LEHRBUCH

Siegfried Bosch

Algebra

10. Auflage

Springer Spektrum

Algebra

Siegfried Bosch

Algebra

10. Auflage

Springer Spektrum

Siegfried Bosch
Mathematisches Institut
Universität Münster
Münster, Deutschland

ISBN 978-3-662-67463-5 ISBN 978-3-662-67464-2 (eBook)
https://doi.org/10.1007/978-3-662-67464-2

Die Deutsche Nationalbibliothek verzeichnet diese Publikation in der Deutschen Nationalbibliografie; detaillierte bibliografische Daten sind im Internet über http://dnb.d-nb.de abrufbar.

Planung/Lektorat: Nikoo Azarm
Springer Spektrum ist ein Imprint der eingetragenen Gesellschaft Springer-Verlag GmbH, DE und ist ein Teil von Springer Nature.
Die Anschrift der Gesellschaft ist: Heidelberger Platz 3, 14197 Berlin, Germany

Vorwort

Das vorliegende Buch bietet eine Einführung in zwei unterschiedliche Themenbereiche der Algebra. Der erste Bereich, auch als *Abstrakte Algebra* bekannt, umfasst die allgemeine Theorie fundamentaler algebraischer Objekte wie z. B. von Gruppen, Ringen und Körpern, also von Begriffsbildungen, die auch weit über die Algebra hinaus in mathematischen Disziplinen von Bedeutung sind. Der zweite Themenbereich ist charakterisiert durch die sogenannte *Galois-Theorie* und deren Anwendungen. Ausgangspunkt dieser Theorie ist aus historischer Sicht das Problem der Auflösung algebraischer Gleichungen, ein Problem, das nach mannigfachen vergeblichen Versuchen zum Auffinden von Lösungsformeln für Gleichungen höheren Grades eine umfassende Klärung durch die brillanten Ideen von E. Galois fand. Erst nach und nach war man in der Lage, die Herangehensweise von Galois in eine fundierte mathematische Theorie umzusetzen, da gleichzeitig verschiedene neuartige algebraische Konzepte als Grundlagen entwickelt und etabliert werden mussten. So ist es zu verstehen, dass das Studium algebraischer Gleichungen für weite Teile der abstrakten Algebra prägend war. Auch im vorliegenden Text werden algebraische Gleichungen häufig als motivierender roter Faden zu erkennen sein.

Um diese Wurzeln besser sichtbar zu machen, beginnt der Text mit einem historischen Abriss zum Problem der Auflösung algebraischer Gleichungen. Ansonsten wird die Thematik der Algebra aus moderner Sicht behandelt. Um ein Höchstmaß an Orientierung zu geben, beginnen die einzelnen Kapitel jeweils mit einigen einführenden Bemerkungen unter dem Titel *Überblick und Hintergrund*, mit der Intention, das jeweilige Thema vorzustellen und zugehörige Höhepunkte in informeller Weise zu erläutern. Der nachfolgende "reguläre" Text geht dann in voller mathematischer Strenge vor; einige Abschnitte, gekennzeichnet durch einen Stern, sind optional. Ich habe mich bemüht, die Dinge in größtmöglicher Einfachheit und Übersicht-

lichkeit darzustellen, inklusive notwendiger Vorbereitungen, jedoch ohne auf simplifizierende Ad-hoc-Lösungen zurückzugreifen. Deshalb sollte das Buch zur Begleitung "jeder" Algebra-Vorlesung geeignet sein, aber sicherlich auch zum Selbststudium, da die Darstellung ohne weitere Vorkenntnisse auskommt, abgesehen von einigen wenigen Grundlagen der Linearen Algebra. Als Neuerung habe ich zum Ende eines jeden Abschnitts unter dem Titel *Lernkontrolle und Prüfungsvorbereitung* einige Fragen und Anforderungen zusammengestellt, die dazu gedacht sind, die dargebotene Theorie erneut und unter leicht verändertem Blickwinkel Revue passieren zu lassen, etwa so wie dies auch in einer mündlichen Examensprüfung geschehen könnte. Dabei sind die mit "+" oder "++" gekennzeichneten Punkte tiefergehender Natur und können zunächst als optional angesehen werden. Ein klassisches Aufgabentraining erfolgt sodann unter dem Titel *Übungsaufgaben*. Hier gibt es in bewährter Weise eine Auswahl an Problemen, die geeignet sind, die Theorie des jeweiligen Abschnitts weiter zu illustrieren und zu vertiefen. Einige dieser Aufgabenstellungen sind *kursiv* gedruckt, um anzudeuten, dass es hierzu Lösungsvorschläge im Anhang gibt.

Mehrfach habe ich Vorlesungen zum Inhalt des Buches gehalten, gewöhnlich in Einheiten von jeweils zwei aufeinander folgenden Semestern. Solche Kurse beschränkten sich im Wesentlichen auf den "Standard"-Stoff, der in den regulären Abschnitten ohne Stern enthalten ist. Dieses Standard-Programm ergibt einen wohl-fundierten und direkten Zugang zur Welt der algebraischen Körpererweiterungen, mit dem Hauptsatz der Galois-Theorie als erstem Höhepunkt. Gleichzeitig werden dabei die zugehörigen grundlegenden Konzepte der abstrakten Algebra erläutert. Nebenbei sei erwähnt, dass die Gruppentheorie in zwei Kapitel aufgeteilt wurde. Der elementare Teil findet sich in Kapitel 1, sowie der mehr fortgeschrittene Teil, der für Anwendungen der Galois-Theorie relevant ist, in Kapitel 5. Bei Bedarf kann man natürlich Kapitel 5 direkt an Kapitel 1 anschließen. Bleibt noch anzumerken, dass die optionalen mit einem Stern versehenen Abschnitte das Standard-Programm komplettieren oder auch, in einigen Fällen, einen ersten Blick auf benachbarte Themen vermitteln, die mehr fortgeschritten sind. Die Thematik der Stern-Abschnitte eignet sich insbesondere zur Behandlung im Rahmen von Seminaren.

Erste Versionen des Manuskripts entstanden in Form von Skripten, die ich den Studierenden in meinen Vorlesungen zur Verfügung gestellt habe. Sie wurden später zu einem Buch zusammengefasst, das erstmals im

Jahre 1993 erschien. Seitdem hat sich das Manuskript der Algebra ständig weiterentwickelt. Einige optionale neue Themen kamen hinzu wie etwa die Auflösung algebraischer Gleichungen vom Grade 3 und 4, aber auch Kummer-Theorie in unterschiedlichen Versionen, einschließlich der benötigten Theorie der Witt-Vektoren. All dies hat nach und nach zu einer vielseitigen Abrundung des behandelten Themenkomplexes geführt.

Die stetige Weiterentwicklung des Buches fußt zu einem erheblichen Teil auf den Rückmeldungen von Studierenden, Lesern, Mitarbeitern und Kollegen. Ihnen allen bin ich zu großem Dank verpflichtet für die mannigfachen Kommentare und Vorschläge, die größtenteils im Rahmen von Neuauflagen berücksichtigt werden konnten. In der vorliegenden Neuauflage habe ich unter dem Aspekt *Lernkontrolle und Prüfungsvorbereitung* erstmals eine textbegleitende Anleitung zur eigenständigen Überprüfung des Lernerfolgs und zur Einstimmung auf Prüfungssituationen realisiert. Nicht zuletzt im Hinblick auf diese Neuerung wurde der gesamte Text weiter optimiert und nochmals einer gründlichen Revision unterzogen.

Abschließend gebührt mein Dank dem Springer-Verlag und seinem Team, welches wie immer für eine mustergültige Herstellung und Ausstattung des Buches gesorgt hat.

Münster, im März 2023 Siegfried Bosch

Inhalt

Einführung

Zur Lösung algebraischer Gleichungen

Der Name "Algebra" ist arabischen Ursprungs (9. Jahrhundert n. Chr.) und bedeutet Rechnen mit Gleichungen, etwa das Zusammenfassen von Termen der Gleichung oder das Verändern der Terme durch gleichartige Manipulationen auf den beiden Seiten der Gleichung. Dabei stellt die Gleichung eine Beziehung dar zwischen bekannten Größen, den sogenannten Koeffizienten, sowie den unbekannten Größen oder Variablen, deren Wert man mit Hilfe der Gleichung ermitteln möchte. Meist interessiert man sich in der Algebra für polynomiale Gleichungen, etwa des Typs

$$2x^3 + 3x^2 + 7x - 10 = 0,$$

wobei x für die unbekannte Größe steht. Eine solche Gleichung wird allgemein als *algebraische* Gleichung für x bezeichnet. Ihr *Grad* ist gegeben durch den Exponenten der höchsten wirklich vorkommenden Potenz von x. Algebraische Gleichungen vom Grad 1 nennt man *linear*. Das Studium linearer Gleichungen oder, allgemeiner, linearer Gleichungssysteme in endlich vielen unbekannten Größen ist ein zentrales Problem der *Linearen Algebra*.

Unter *Algebra* im Sinne dieses Buches wollen wir im Wesentlichen diejenige Theorie verstehen, die aus dem Studium algebraischer Gleichungen einer unbekannten Größe hervorgegangen ist, also in heutiger Sprache die Theorie der Körpererweiterungen mit all ihren abstrakten Begriffsbildungen, auch gruppentheoretischer Art, die insgesamt eine bequeme und präzise

S. Bosch, *Algebra*, https://doi.org/10.1007/978-3-662-67464-2_1

Handhabung algebraischer Gleichungen erst möglich gemacht haben. In der Tat verwendet die moderne Algebra schon auf "elementarem" Niveau in viel stärkerem Maße abstrakte Methoden und Begriffe, als man dies etwa von der Analysis oder der komplexen Funktionentheorie her gewohnt ist. Der Grund hierfür wird in gewisser Weise deutlich, wenn man das Problem der Lösung algebraischer Gleichungen in seiner historischen Entwicklung verfolgt, was wir nachstehend ein wenig tun wollen.

Die Anfänge sind ganz konkreter Natur und konzentrieren sich im Wesentlichen auf das Bearbeiten spezieller zahlenmäßig gegebener "Aufgaben". Eine berühmte Aufgabe aus der griechischen Antike (ca. 600 v. Chr. – 200 n. Chr.) ist z. B. das Problem der Würfelverdoppelung: Gegeben sei ein Würfel mit Kantenlänge 1, man bestimme die Kantenlänge eines Würfels, der doppeltes Volumen besitzt. Zu lösen ist also die algebraische Gleichung $x^3 = 2$, welche vom Grad 3 ist. Heute würden wir die Lösung mit $x = \sqrt[3]{2}$ angeben. Was hat man aber unter $\sqrt[3]{2}$ zu verstehen, wenn man nur rationale Zahlen kennt? Da man keine rationale Zahl finden konnte, deren dritte Potenz 2 ist, hat man sich im Altertum bei solchen Situationen vielfach mit Näherungslösungen begnügt, also etwa versucht, $\sqrt[3]{2}$ mit genügender Genauigkeit rational zu approximieren. Andererseits ist das Problem der Würfelverdoppelung geometrischer Natur, und es liegt nahe, eine geometrische Lösung zu versuchen. Häufig zu finden ist bei den Griechen, z. B. bei Euklid, die Konstruktion mit Zirkel und Lineal, welche Schnittpunkte von Geraden und Kreisen mit ebensolchen Objekten benutzt. Aber auch mit dieser Technik lässt sich $\sqrt[3]{2}$ nicht konstruieren, wie wir heute wissen; vgl. Abschnitt 6.4. Da die Konstruktion mit Zirkel und Lineal nicht immer den gewünschten Erfolg haben konnte, findet man bei den Griechen auch geometrische Konstruktionen unter Verwendung komplizierterer Kurven.

Wenn man einmal akzeptiert hat, dass man zur Lösung algebraischer Gleichungen, etwa mit rationalen Koeffizienten, neben den bekannten "rationalen" Operationen der Addition, Subtraktion, Multiplikation und Division zumindest auch noch das "Wurzelziehen" benötigt, so kann man die Frage stellen, ob eine wiederholte Anwendung dieser Operationen stets ausreicht, um die Lösungen aus den Koeffizienten zu gewinnen. Dies ist die berühmte Frage nach der *Auflösbarkeit algebraischer Gleichungen durch Radikale*. Beispielsweise sind algebraische Gleichungen vom Grad 1 bzw. 2 durch Radikale auflösbar:

$$x^1 + a = 0 \qquad \Longleftrightarrow \qquad x = -a$$

$$x^2 + ax^1 + b = 0 \qquad \Longleftrightarrow \qquad x = -\frac{a}{2} \pm \sqrt{\frac{a^2}{4} - b}$$

Die Auflösung quadratischer Gleichungen wurde im Wesentlichen schon von den Babyloniern (ab ca. Ende des 3. Jahrtausends v. Chr.) unter Verwendung elementargeometrischer Methoden beherrscht, auch wenn bei den konkreten Rechnungen, die uns überliefert sind, Quadratwurzeln meist nur aus Quadratzahlen gezogen werden. Nach Beendigung der babylonischen und der griechischen Periode wurde die Auflösung quadratischer Gleichungen ab ca. dem 9. Jahrhundert n. Chr. insbesondere durch arabische Mathematiker weiter perfektioniert. Diese arbeiteten auch an dem Problem, kubische sowie Gleichungen höheren Grades durch Radikale aufzulösen, konnten hierzu jedoch keinen nennenswerten Beitrag liefern.

Die sensationelle Entdeckung, dass kubische Gleichungen durch Radikale auflösbar sind, gelang erst gegen 1515 dem Italiener S. del Ferro. Er betrachtete eine Gleichung der Form $x^3 + ax = b$ mit $a, b > 0$ und fand als Lösung

$$x = \sqrt[3]{\frac{b}{2} + \sqrt{\left(\frac{b}{2}\right)^2 + \left(\frac{a}{3}\right)^3}} + \sqrt[3]{\frac{b}{2} - \sqrt{\left(\frac{b}{2}\right)^2 + \left(\frac{a}{3}\right)^3}}.$$

Obwohl er wusste, dass Generationen von Mathematikern vor ihm an diesem Problem gescheitert waren, hat del Ferro seine Entdeckung geheim gehalten und nicht veröffentlicht. Wir wissen von seinen Untersuchungen aber aus der *Ars Magna*, einer Art Lehrbuch zur Mathematik, welches G. Cardano im Jahre 1545 publizierte. Cardano hatte von del Ferros Lösungsformel auf Umwegen erfahren und sich die Herleitung selbst überlegt. Weiter erkannte er, dass Gleichungen dritten Grades in der Regel drei Lösungen haben sollten, wobei bemerkenswert ist, dass Cardano weniger Skrupel als seine Zeitgenossen hatte, negative Zahlen zu verwenden. Auch gibt es bei ihm erste Ansätze zur Verwendung komplexer Zahlen. Seinem Schüler L. Ferrari gelang schließlich nach 1545 die Auflösung algebraischer Gleichungen vierten Grades; zu den Formeln vergleiche man Abschnitt 6.1.

In den nächsten zwei Jahrhunderten waren die Fortschritte zur Lösung algebraischer Gleichungen eher gering. F. Viète entdeckte den nach ihm benannten Zusammenhang zwischen den Koeffizienten einer Gleichung und deren Lösungen, welcher sich heute als eine Trivialität darstellt, wenn man die Zerlegung von Polynomen in Linearfaktoren benutzt. Man hatte auch bereits eine gewisse Vorstellung von dem Begriff der Vielfachheit einer

Lösung und vertrat die Auffassung, dass eine algebraische Gleichung n-ten Grades, gezählt mit Vielfachheiten, stets n Lösungen besitzt, so wie es die Beispiele im Idealfall zeigen. Dabei muss man sich allerdings darüber im Klaren sein, dass Letzteres nur eine mehr oder weniger vage Vorstellung war, denn die Natur dieser Lösungen, etwa reell oder komplex oder gar hyperkomplex (also keins von beidem) wurde nicht präzisiert. In diese Zeit fallen auch mehrere vergebliche Versuche, beispielsweise durch G. W. Leibniz, algebraische Gleichungen fünften und höheren Grades allgemein durch Radikale aufzulösen.

Eine gewisse Konsolidierung der Situation deutete sich schließlich mit dem *Fundamentalsatz der Algebra* an. Erste Ansätze zu einem Beweis finden sich 1746 bei J. d'Alembert, weitere Beweise jeweils unterschiedlicher Strenge erfolgten 1749 durch L. Euler, 1772 durch J. L. Lagrange sowie später noch durch C. F. Gauß in seiner Doktorarbeit (1799). Dieser Satz besagt, dass jedes nicht-konstante komplexe Polynom n-ten Grades mit Vielfachheiten gezählt genau n komplexe Nullstellen besitzt, oder mit anderen Worten, dass sich jedes solche Polynom als Produkt von linearen Faktoren schreiben lässt. Auch wenn der Fundamentalsatz der Algebra keinen Beitrag zur expliziten Auflösung algebraischer Gleichungen liefern konnte, so gab er dennoch eine Antwort auf die Frage nach dem Zahlbereich, in welchem Lösungen algebraischer Gleichungen mit rationalen, reellen oder komplexen Koeffizienten zu suchen waren. Auf dieser Basis wurden weitere Fortschritte erzielt, insbesondere von Lagrange. Er unterwarf 1771 die Auflösung algebraischer Gleichungen dritten und vierten Grades einer grundlegenden Revision und bemerkte unter anderem, dass die Kubikwurzeln in del Ferros Formel mit der Nebenbedingung

$$\sqrt[3]{\frac{b}{2}+\sqrt{\left(\frac{b}{2}\right)^2+\left(\frac{a}{3}\right)^3}}\cdot\sqrt[3]{\frac{b}{2}-\sqrt{\left(\frac{b}{2}\right)^2+\left(\frac{a}{3}\right)^3}}=-\frac{a}{3}$$

gewählt werden müssen, damit man nicht 9 mögliche Werte erhält, sondern nur die Werte x_1, x_2, x_3 der wirklichen Lösungen zur betrachteten Gleichung $x^3 + ax = b$. Noch wichtiger aber war die Entdeckung, dass nach Wahl einer nicht-trivialen dritten Einheitswurzel ζ, also einer komplexen Zahl $\zeta \neq 1$ mit $\zeta^3 = 1$, der Ausdruck

$$(x_1 + \zeta x_2 + \zeta^2 x_3)^3$$

bei Permutation der x_i lediglich *zwei* verschiedene Werte annimmt sowie, als Konsequenz, einer quadratischen Gleichung genügt (mit Koeffizienten

aus dem betrachteten Zahlbereich, etwa den rationalen Zahlen). Damit lassen sich die Summen $x_{\pi(1)} + \zeta x_{\pi(2)} + \zeta^2 x_{\pi(3)}$ für beliebige Permutationen π durch Lösen einer quadratischen Gleichung und anschließendes Ausziehen einer Kubikwurzel erhalten. Da man aber andererseits aus diesen Summen x_1, x_2, x_3 mittels rationaler Operationen zurückerhalten kann, ist insgesamt die Auflösung der Gleichung $x^3 + ax = b$ durch Radikale beschrieben. In ähnlicher Weise hat Lagrange auch die Auflösung algebraischer Gleichungen vierten Grades charakterisiert, wobei ebenfalls Permutationen der Lösungen eine wichtige Rolle spielen. Lagrange hat damit erstmalig gruppentheoretische Argumente in die Diskussion eingeführt, ein Ansatz, der letztendlich zur systematischen Klärung des Problems der Auflösung algebraischer Gleichungen durch Galois führte.

In ähnlichem Stile wie Lagrange studierte Gauß 1796 nach Vorarbeiten von A. T. Vandermonde die Lösungen der Gleichung $x^p - 1 = 0$ für Primzahlen $p > 2$, wobei die zugehörigen Permutationen dieser Lösungen unter den Begriff der "zyklischen" Gruppen fallen. Die Methoden von Gauß führten insbesondere zu neuen Erkenntnissen bei der geometrischen Frage, welche regelmäßigen n-Ecke sich mit Zirkel und Lineal konstruieren lassen. In diese Zeit fallen weiter Untersuchungen von P. Ruffini, 1820 von N. H. Abel präzisiert, mit dem Ergebnis, dass die "allgemeine Gleichung" n-ten Grades für $n \geq 5$ nicht durch Radikale auflösbar ist.

Nach derartigen Einzelerfolgen, die im Wesentlichen durch die systematische Ausnutzung von Gruppenargumenten zustande kamen, erschien die Zeit reif zu sein für eine vollständige Klärung des Problems der Auflösung algebraischer Gleichungen. Dieser krönende Abschluss gelang E. Galois mit seinen brillanten Ideen in den Jahren 1830 – 1832. In stärkerem Maße noch als Abel hatte Galois eine sehr präzise Vorstellung von den Zahlbereichen, die etwa aus den rationalen Zahlen durch Hinzunahme von Lösungen algebraischer Gleichungen entstehen; aus heutiger Sicht handelt es sich um eine Vorstufe des Körperbegriffs sowie um die Technik der Adjunktion algebraischer Elemente. Er führte den Begriff der Irreduzibilität einer algebraischen Gleichung ein und zeigte den Satz vom primitiven Element für den Zerfällungskörper L einer algebraischen Gleichung $f(x) = 0$ mit einfachen Lösungen, also für den Körper, der von allen Lösungen $x_1, \ldots, x_r$ einer solchen Gleichung erzeugt wird. Dieser Satz besagt: Es gibt eine irreduzible algebraische Gleichung $g(y) = 0$, so dass L einerseits alle Lösungen $y_1, \ldots, y_s$ dieser Gleichung enthält, sowie andererseits bereits aus

dem Koeffizientenbereich durch Adjunktion eines beliebigen Elementes y_j hervorgeht. Galois' Idee war es nun, die x_i in nahe liegender Weise als Funktionen von y_1 darzustellen, etwa $x_i = h_i(y_1)$, und y_1 dann durch ein beliebiges y_j zu ersetzen. Er zeigte, dass die Elemente $h_i(y_j)$, $i = 1, \ldots, r$, wiederum die sämtlichen Lösungen zu $f(x) = 0$ darstellen, das Ersetzen von y_1 durch y_j also Anlass zu einer Permutation π_j der x_i gibt, und dass die π_j eine Gruppe bilden, nämlich die nach ihm benannte "Galois-Gruppe" zur Gleichung $f(x) = 0$.

Hierauf aufbauend gelangte Galois zu der fundamentalen Einsicht, dass die Teilkörper des Zerfällungskörpers L in gewisser Weise den Untergruppen der zugehörigen Galois-Gruppe G entsprechen, eine Tatsache, die wir heute in verfeinerter Form als "Hauptsatz der Galois-Theorie" bezeichnen. Mittels dieser Erkenntnis konnte Galois zeigen, dass die Gleichung $f(x) = 0$ genau dann durch Radikale auflösbar ist, wenn G eine Kette von Untergruppen $G = G_0 \supset \ldots \supset G_n = \{1\}$ besitzt, so dass G_{i+1} jeweils Normalteiler in G_i und die Faktorgruppe G_i/G_{i+1} zyklisch ist. Wir wollen hier auf weitere Details verzichten und verweisen stattdessen auf die Abschnitte 4.1, 4.3, 4.8 und 6.1, in denen wir diese Aspekte der Galois-Theorie ausführlich darstellen.

Das einfach zu formulierende Problem der Auflösbarkeit algebraischer Gleichungen erfuhr somit durch die genialen Ideen Galois' eine umfassende Klärung. Insbesondere ist zu verstehen, warum dieses Problem über viele Jahrhunderte hinweg dem Zugriff der Mathematiker verwehrt war. Die Lösung besteht nicht aus einer nachvollziehbaren etwa formelmäßigen Bedingung an die Koeffizienten der betrachteten Gleichung; sie erfordert, allein um formuliert werden zu können, eine neue Sprache, also neue Begriffsbildungen und Denkweisen, die erst in einem langwierigen Prozess des Studierens von Beispielen und des Herantastens an die Gegebenheiten gefunden werden mussten. Auch bleibt festzuhalten, dass der eigentliche Nutzen von Galois' Untersuchungen nicht so sehr in dem Beitrag zur Auflösung algebraischer Gleichungen durch Radikale zu sehen ist, sondern vielmehr in der allgemeinen Beziehung, die zwischen algebraischen Gleichungen und den zugehörigen "Galois"-Gruppen besteht. Man kann ja mit dem Hauptsatz der Galois-Theorie sozusagen in gruppentheoretischer Weise die "Natur" der Lösungen beliebiger algebraischer Gleichungen charakterisieren, wodurch im Nachhinein das Problem der Auflösbarkeit durch Radikale viel von seiner ursprünglichen Bedeutung verloren hat.

Und wie wurde Galois' Beitrag von seinen Zeitgenossen aufgenommen? Um hiervon einen Eindruck zu vermitteln, wollen wir einen kurzen Blick auf Galois' Lebenslauf werfen; man vergleiche hierzu auch [10], Abschnitt 7. Evariste Galois wurde 1811 in der Nähe von Paris geboren und starb 1832 im Alter von nur 20 Jahren. Bereits während der Schulzeit beschäftigte er sich mit den Schriften von Lagrange und schrieb eine erste kleinere Arbeit über Kettenbrüche. Zweimal versuchte er, in die angesehene *École Polytechnique* in Paris einzutreten, schaffte aber die Aufnahmeprüfung nicht und musste sich schließlich mit der *École Normale* begnügen. 1829 nahm er dort sein Studium auf, im Alter von 18 Jahren. Im gleichen Jahr legte er der *Académie des Sciences* ein erstes *Mémoire* über die Lösung algebraischer Gleichungen vor. Das Manuskript wurde jedoch nicht beachtet und ging verloren, wie auch ein zweites, das er eine Woche später einreichte. Nachdem 1830 ein weiteres *Mémoire* das gleiche Schicksal erlitten hatte, machte Galois Anfang 1831 einen letzten Versuch und reichte seine Arbeit zur Auflösung algebraischer Gleichungen durch Radikale ein, die wir heute als sein berühmtestes Werk ansehen. Diesmal wurde die Arbeit referiert, aber mit der Begründung der Unausgereiftheit und Unverständlichkeit abgelehnt. Enttäuscht, dass er in der Mathematik keine Anerkennung gewinnen konnte, wandte sich Galois den politischen Ereignissen seiner Zeit zu. Er wurde aufgrund seiner Aktivitäten mehrmals verhaftet und schließlich zu einer Gefängnisstrafe verurteilt. Im Mai 1832 ließ er sich zu einem Duell provozieren, bei dem er den Tod fand. Um sein Werk der Nachwelt zu erhalten, verfasste Galois in der Nacht vor der Austragung des Duells einen Brief an einen Freund, in dem er seine bahnbrechenden Erkenntnisse in programmatischer Form zusammenfasste. Obwohl dieses Programm noch 1832 veröffentlicht werden konnte, wurde die Tragweite von Galois' Untersuchungen nicht unmittelbar erkannt. Man mag über die Gründe spekulieren, zwei Dinge sind aber sicherlich von Bedeutung. Zum einen war Galois ein unbekannter junger Mathematiker, mit einem dubiosen Lebenslauf dazu. Zum anderen aber machte die Charakterisierung der Auflösbarkeit algebraischer Gleichungen für die damalige Zeit offenbar einen derart komplizierten Eindruck, dass man in Galois' unmittelbarer Umgebung nicht darauf vorbereitet war, dies als ernst zu nehmende Lösung des Problems anzuerkennen. Man bedenke auch, dass Lagrange, auf dessen grundlegende Vorarbeiten wir oben hingewiesen haben, bereits 1813 verstorben war.

Wir wollen hier nicht in allen Einzelheiten beschreiben, auf welchen Wegen die Ideen Galois' letztendlich doch ihre Anerkennung und Wertschätzung erfahren haben. Wesentlich war sicherlich, dass J. Liouville ca. 10 Jahre nach Galois' Tod auf dessen Arbeiten stieß und im Jahre 1846 einen Teil des mathematischem Nachlasses von Galois veröffentlichte. So begann in der zweiten Hälfte des 19. Jahrhunderts eine Phase, in der man unter anderem mit dem Verstehen und Ausfeilen von Galois' Ideen beschäftigt war. Man lernte sehr schnell, das Problem der Auflösbarkeit algebraischer Gleichungen durch Radikale in realistischer Weise zu sehen. Es war nur deshalb von so eminent großer Wichtigkeit, weil es den entscheidenden Anreiz geliefert hatte, die Tür zu einer noch umfassenderen Klassifikation der irrationalen Zahlen zu öffnen. Auch begann man nun, sich stärker für das Problem der Transzendenz zu interessieren. Schon 1844 konnte Liouville in konstruktiver Weise die Existenz transzendenter Zahlen zeigen, eine Aussage, die G. Cantor 1874 in noch krasserer Form unter Benutzung eines Mächtigkeitsargumentes erhielt. Weiter gehören zu diesen Untersuchungen die Beweise für die Transzendenz von e im Jahre 1873 durch Ch. Hermite [8] und von π im Jahre 1882 durch F. Lindemann [12]. Einige Aspekte grundsätzlicher Art zum Phänomen der Transzendenz wurden schließlich von E. Steinitz 1910 in seiner Arbeit [15] geklärt.

In den Arbeiten Galois' hatte sich unter anderem gezeigt, dass die Fixierung auf einzelne algebraische Gleichungen eher hinderlich war. Man musste variabel sein und sozusagen mehrere Gleichungen zur selben Zeit betrachten, eventuell auch mit unterschiedlichem Zahlbereich, aus dem die Koeffizienten stammen. Diese Einsicht führte dazu, statt einzelner Gleichungen sogenannte algebraische Körpererweiterungen zu studieren. Als Erster hat wohl R. Dedekind in seinen Vorlesungen 1855 – 1858 in Göttingen die Galois-Theorie konsequent in diesem Sinne dargestellt. Insbesondere interpretierte er Galois-Gruppen als Automorphismengruppen von Körpern und nicht nur als Gruppen, die die Lösungen einer algebraischen Gleichung permutieren. Eine weitere entscheidende Verbesserung der Theorie geht auf L. Kronecker zurück, der 1887 das nach ihm benannte Verfahren zur Konstruktion algebraischer Körpererweiterungen veröffentlichte. Es führte dazu, dass die Galois-Theorie ohne Verwendung des Fundamentalsatzes der Algebra aufgebaut werden konnte und sich somit von der physischen Anwesenheit des Körpers der komplexen Zahlen befreien ließ, z. B. um sie auf endliche Körper zu übertragen.

Mit diesen Entwicklungen sind wir nun schon ziemlich nahe bei den Auffassungen angelangt, die wir auch heute noch in der Theorie der Körpererweiterungen vertreten. Natürlich hat es weitere Komplettierungen, Verbesserungen und Vereinfachungen der Theorie gegeben, die meist im Rahmen von Lehrbüchern dargestellt wurden. Zu nennen sind — in historischer Reihenfolge — die Publikationen von H. Weber [17], B. L. van der Waerden [16], E. Artin [1], [2], sowie als weitere richtungsweisende Lehrbücher N. Bourbaki [5] und S. Lang [11]. Des Weiteren hat auch Emmy Noether ab ca. 1920 wesentlich zur Konsolidierung der "modernen" Algebra beigetragen. Davon zeugen nicht nur ihre Arbeit [13], sondern auch ihre Vorlesungen, auf die beispielsweise in [16] Bezug genommen wird.

Auch wenn die Theorie der algebraischen Gleichungen nunmehr als "fertig" und in einem "optimalen" Gewande erscheinen mag, so möchte ich den Leser dennoch ermutigen, sich von Zeit zu Zeit an den Weg zu erinnern, den das Problem der Lösung dieser Gleichungen durchwandert hat. Nur wenn man sich die enormen Schwierigkeiten bewusst macht, die zu überwinden waren, wird man die faszinierenden Lösungen verstehen und zu schätzen wissen, die die Mathematiker im Laufe von Jahrhunderten in zähem Ringen gefunden haben.

Es sollte nun aber nicht der Eindruck entstehen, dass das Studium algebraischer Gleichungen heute als abgeschlossen zu betrachten wäre. Im Gegenteil, es hat seine natürliche Fortsetzung erfahren mit der Untersuchung von Systemen algebraischer Gleichungen mehrerer unbekannter Größen innerhalb der Algebraischen Geometrie, vgl. [3], oder der Zahlentheorie. Auch hierzu können wir ein einfach formulierbares Problem angeben, welches äußerst lange dem Ansturm der Mathematiker standgehalten hat und erst in jüngerer Vergangenheit gelöst werden konnte, und zwar in den Jahren 1993/94 durch A. Wiles unter Mithilfe von R. Taylor. Es handelt sich um die berühmte *Fermatsche Vermutung*, dass nämlich die Gleichung $x^n + y^n = z^n$ für $n \geq 3$ keine Lösung in ganzen von Null verschiedenen Zahlen besitzt. Man sagt, Fermat habe etwa um 1637 diese Vermutung auf dem Rand einer Seite in seiner Ausgabe von Diophants *Arithmetica* (ca. 250 n. Chr.) vermerkt und hinzugefügt, dass er einen wunderbaren Beweis hierfür habe, der Rand aber zu klein sei, um diesen aufzunehmen.

1. Elementare Gruppentheorie

Überblick und Hintergrund

Der Gruppenbegriff ist im Rahmen dieses Buches in zweierlei Hinsicht von Bedeutung. Einerseits beinhaltet er eine grundlegende mathematische Struktur, die man insbesondere bei Ringen, Körpern, Vektorräumen und Moduln findet, wenn man die dort gegebene Addition als Verknüpfung betrachtet. Gruppen dieses Typs sind stets kommutativ oder, wie man auch sagt, abelsch, benannt nach dem Mathematiker N. H. Abel. Daneben sind für uns aber auch die auf E. Galois zurückgehenden Galois-Gruppen von zentralem Interesse, da diese für die Theorie algebraischer Gleichungen benötigt werden. Galois-Gruppen sind aus einfachster Sicht Permutationsgruppen, also Gruppen, deren Elemente als bijektive Selbstabbildungen einer gegebenen endlichen Menge, etwa $\{1, \ldots, n\}$, aufgefasst werden.

Ein wesentliches Charakteristikum einer Gruppe G ist die Verknüpfungsvorschrift, welche je zwei Elementen $g, h \in G$ ein drittes Element $g \circ h \in G$ zuordnet, als Produkt oder im kommutativen Fall auch als Summe von g und h bezeichnet. Solche Verknüpfungen hatte man beim Rechnen in Zahlbereichen schon immer benutzt, ohne dass man zunächst eine Notwendigkeit sah, die Eigenschaften einer Verknüpfung genauer zu präzisieren. Diese wurden sozusagen als "evident" angesehen. So ist es auch zu verstehen, dass das Auftreten negativer Zahlen als Ergebnis einer Rechnung, etwa bei einer Differenzbildung, noch bis zum Beginn des 17. Jahrhunderts bei manchen Mathematikern als "suspekt" galt, da negative Zahlen eben keine reale Bedeutung zu haben schienen. Mit Beginn des 19. Jahrhunderts je-

S. Bosch, *Algebra*, https://doi.org/10.1007/978-3-662-67464-2_2

doch begann der eigentliche Gruppenbegriff Gestalt anzunehmen, und zwar in dem Maße, wie Verknüpfungsvorschriften auch auf Objekte angewendet wurden, die nicht in natürlicher Weise als Zahlbereichen zugehörig interpretiert werden konnten. Bei der Auflösung algebraischer Gleichungen spielten beispielsweise Permutationsgruppen eine wichtige Rolle. Da es sich hierbei um endliche Gruppen handelt, also um Gruppen mit endlich vielen Elementen, konnte man die Gruppenaxiome noch ohne explizite Erwähnung "inverser Elemente" formulieren, was bei unendlichen Gruppen nicht mehr möglich ist; man vergleiche hierzu etwa Aufgabe 3 aus Abschnitt 1.1. Eine explizite Forderung "inverser Elemente" und damit eine axiomatische Charakterisierung von Gruppen im heutigen Sinne taucht erstmalig im ausgehenden 19. Jahrhundert bei S. Lie und H. Weber auf. Zuvor hatte Lie noch vergeblich versucht, für die von ihm betrachteten "Transformationsgruppen" die Existenz inverser Elemente aus den übrigen Axiomen abzuleiten.

In diesem Kapitel wollen wir in knapper Form einige elementare Grundlagen über Gruppen zusammenstellen, Dinge, die den meisten Lesern sicherlich schon geläufig sein dürften. Neben der Definition einer Gruppe handelt es sich um die Einführung von Normalteilern, der zugehörigen Faktorgruppen sowie um die Diskussion zyklischer Gruppen. Bereits hier spürt man etwas von dem prägenden Einfluss, den die Untersuchungen zur Auflösung algebraischer Gleichungen und insbesondere die Galois-Theorie auf die Gruppentheorie ausgeübt haben. Der Begriff des Normalteilers ist beispielsweise im Zusammenhang mit dem Hauptsatz der Galois-Theorie 4.1/6 entstanden. Denn dieser Satz besagt unter anderem, dass ein Zwischenkörper E zu einer endlichen Galois-Erweiterung L/K genau dann normal über K im Sinne von 3.5/5 ist, wenn die zu E gehörige Untergruppe der Galois-Gruppe $\mathrm{Gal}(L/K)$ die Normalteilereigenschaft besitzt. Auch die Benennung von 1.2/3 als Satz von Lagrange bezieht sich auf gruppentheoretische Argumente, die Lagrange bei seinen Untersuchungen zur Auflösung algebraischer Gleichungen entwickelte.

Weitergehende Resultate über Gruppen und insbesondere Permutationsgruppen, die speziell für Anwendungen in der Galois-Theorie von Interesse sind, werden wir aber erst in Kapitel 5 bringen. Im Übrigen sei hier noch auf den Hauptsatz über endlich erzeugte abelsche Gruppen hingewiesen, der eine Klassifikation dieser Gruppen liefert und dessen Beweis wir in 2.9/9 im Rahmen der Elementarteilertheorie führen werden.

1.1 Gruppen

Es sei M eine beliebige Menge und $M \times M$ ihr kartesisches Produkt mit sich selbst. Unter einer (*inneren*) *Verknüpfung* auf M versteht man eine Abbildung $M \times M \longrightarrow M$. Dabei schreibt man das Bild eines Paares $(a, b) \in M \times M$ meist als "Produkt" $a \cdot b$ oder ab, so dass die Verknüpfung auf M elementweise durch $(a, b) \longmapsto a \cdot b$ charakterisiert werden kann. Die Verknüpfung heißt

assoziativ, falls $(ab)c = a(bc)$ für alle $a, b, c \in M$,

kommutativ, falls $ab = ba$ für alle $a, b \in M$ gilt.

Man nennt ein Element $e \in M$ ein *Einselement* oder *neutrales Element* bezüglich der Verknüpfung auf M, wenn $ea = a = ae$ für alle $a \in M$ gilt. Ein solches Einselement e ist durch diese Eigenschaft eindeutig bestimmt; wir schreiben häufig auch 1 anstelle von e. Eine Menge M mit Verknüpfung $\sigma\colon M \times M \longrightarrow M$ heißt ein *Monoid*, wenn σ assoziativ ist und M ein Einselement bezüglich σ besitzt.

Ist M ein Monoid, so kann man für $a_1, \ldots, a_n \in M$ das Produkt

$$\prod_{i=1}^{n} a_i := a_1 \cdot \ldots \cdot a_n$$

definieren. Da die Verknüpfung assoziativ ist, erübrigt sich eine spezielle Klammerung auf der rechten Seite (was man am besten mit Hilfe eines geschickt angelegten induktiven Arguments beweist). Als Konvention vereinbaren wir noch

$$\prod_{i=1}^{0} a_i := e = \text{ Einselement.}$$

Wie üblich lässt sich zu einem Element $a \in M$ und einem Exponenten $n \in \mathbb{N}$ die n-te Potenz a^n bilden,[1] wobei man aufgrund vorstehender Konvention $a^0 = e$ hat. Ein Element $b \in M$ heißt *invers* zu einem gegebenen Element $a \in M$, wenn $ab = e = ba$ gilt. Es ist dann b eindeutig durch a bestimmt, denn wenn auch $ab' = e = b'a$ gilt, so folgt

$$b = eb = b'ab = b'e = b'.$$

Üblicherweise bezeichnet man das inverse Element zu a, falls es existiert, mit a^{-1}.

[1] $\mathbb{N}$ bezeichnet die natürlichen Zahlen *einschließlich* der 0.

Definition 1. *Eine* Gruppe *ist ein Monoid G, so dass jedes Element von G ein inverses Element besitzt. Im Einzelnen bedeutet dies, man hat eine Menge G mit einer Verknüpfung $G \times G \longrightarrow G$, $(a, b) \longmapsto ab$, welche folgenden Eigenschaften genügt*:

(i) *Die Verknüpfung ist* assoziativ, *d. h. es gilt $(ab)c = a(bc)$ für $a, b, c \in G$.*

(ii) *Es existiert ein* Einselement *in G, d. h. ein Element $e \in G$ mit $ea = a = ae$ für alle $a \in G$.*

(iii) *Zu jedem $a \in G$ gibt es ein* inverses Element, *d. h. ein $b \in G$ mit $ab = e = ba$.*

Die Gruppe heißt kommutativ *oder* abelsch, *falls die Verknüpfung kommutativ ist, d. h. falls*

(iv) *$ab = ba$ für alle $a, b \in G$ gilt.*

Bemerkung 2. *Es genügt, in Definition* 1 *statt* (ii) *und* (iii) *die folgenden etwas schwächeren Bedingungen zu fordern*:

(ii′) *Es existiert ein* links-neutrales Element *in G, d. h. ein Element $e \in G$ mit $ea = a$ für alle $a \in G$.*

(iii′) *Zu jedem $a \in G$ existiert ein* links-inverses Element, *d. h. ein $b \in G$ mit $ba = e$.*

Bezüglich des Nachweises, dass die vorstehenden Bedingungen (ii′) und (iii′) in Verbindung mit (i) bereits zur Definition einer Gruppe ausreichen, verweisen wir auf Aufgabe 1 bzw. auf die im Anhang gegebene Lösung.

Bei einer abelschen Gruppe schreibt man die Verknüpfung oft auch in additiver Form, d. h. man schreibt $a + b$ statt $a \cdot b$ und $\sum a_i$ statt $\prod a_i$, bzw. $n \cdot a$ anstelle einer n-ten Potenz a^n. Entsprechend verwendet man die Bezeichnung $-a$ statt a^{-1} für das inverse Element zu a sowie 0 (*Nullelement*) statt e oder 1 für das neutrale Element. Wir wollen einige Beispiele für Monoide und Gruppen anführen:

(1) $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$, jeweils mit der gewöhnlichen Addition, sind abelsche Gruppen.

(2) $\mathbb{Q}^*$, $\mathbb{R}^*$, $\mathbb{C}^*$, jeweils mit der gewöhnlichen Multiplikation, sind abelsche Gruppen; ebenso die Teilmengen $\mathbb{Q}_{>0} = \{x \in \mathbb{Q}\,;\, x > 0\}$ und $\mathbb{R}_{>0} = \{x \in \mathbb{R}\,;\, x > 0\}$ von $\mathbb{Q}^*$ bzw. $\mathbb{R}^*$. Allgemeiner kann man die aus der Linearen Algebra bekannten Matrizengruppen SL_n oder GL_n mit Ko-

effizienten in $\mathbb{Q}, \mathbb{R}$ oder $\mathbb{C}$ betrachten. Diese sind für $n > 1$ nicht mehr kommutativ.

(3) $\mathbb{N}$ mit Addition, $\mathbb{N}, \mathbb{Z}$ mit Multiplikation sind kommutative Monoide, aber keine Gruppen.

(4) Es sei X eine Menge und $S(X)$ die Menge der bijektiven Abbildungen $X \longrightarrow X$. Dann ist $S(X)$ mit der Komposition von Abbildungen als Verknüpfung eine Gruppe; diese ist nicht abelsch, sofern X aus mindestens 3 Elementen besteht. Für $X = \{1, \ldots, n\}$ setzt man $\mathfrak{S}_n := S(X)$ und nennt dies die *symmetrische Gruppe* bzw. die *Gruppe der Permutationen* der Zahlen $1, \ldots, n$. Elemente $\pi \in \mathfrak{S}_n$ beschreibt man häufig unter expliziter Angabe aller Bilder $\pi(1), \ldots, \pi(n)$ in der Form

$$\begin{pmatrix} 1 & \ldots & n \\ \pi(1) & \ldots & \pi(n) \end{pmatrix}.$$

Indem man die Anzahl der möglichen Anordnungen von $1, \ldots, n$ abzählt, sieht man, dass $\mathfrak{S}_n$ aus genau $n!$ Elementen besteht.

(5) Es sei X eine Menge und G eine Gruppe. Dann ist die Menge aller Abbildungen $X \longrightarrow G$, also $G^X := \mathrm{Abb}(X, G)$, in natürlicher Weise eine Gruppe. Man definiere nämlich für Elemente $f, g \in G^X$ deren Produkt $f \cdot g$ durch $(f \cdot g)(x) := f(x) \cdot g(x)$, also mittels Multiplikation der "Funktionswerte", wobei man die Gruppenverknüpfung von G verwendet. Es heißt G^X auch *Gruppe der G-wertigen Funktionen auf X*. In gleicher Weise können wir die Gruppe $G^{(X)}$ derjenigen Abbildungen $f\colon X \longrightarrow G$ bilden, welche $f(x) = 1$ für fast alle $x \in X$ erfüllen (d. h. für alle $x \in X$, bis auf endlich viele Ausnahmen). Die Gruppen G^X und $G^{(X)}$ sind kommutativ, wenn G kommutativ ist. G^X und $G^{(X)}$ stimmen überein, wenn X endlich ist.

(6) Es sei X eine Indexmenge und $(G_x)_{x \in X}$ eine Familie von Gruppen. Dann wird das mengentheoretische Produkt $\prod_{x \in X} G_x$ zu einer Gruppe, wenn wir die Verknüpfung zweier Elemente $(g_x)_{x \in X}$, $(h_x)_{x \in X} \in \prod_{x \in X} G_x$ komponentenweise erklären durch

$$(g_x)_{x \in X} \cdot (h_x)_{x \in X} := (g_x \cdot h_x)_{x \in X}.$$

Man nennt $\prod_{x \in X} G_x$ das *Produkt* der Gruppen G_x, $x \in X$. Im Fall einer endlichen Menge $X = \{1, \ldots, n\}$ schreibt man hierfür üblicherweise auch $G_1 \times \ldots \times G_n$. Sind die Gruppen G_x Exemplare ein und derselben Gruppe

G, so gilt $\prod_{x\in X} G_x = G^X$ in der Notation des vorstehenden Beispiels. Ist zudem X endlich, etwa $X = \{1, \dots, n\}$, so schreibt man auch G^n statt G^X oder $G^{(X)}$.

Definition 3. *Es sei G ein Monoid. Eine Teilmenge $H \subset G$ heißt* Untermonoid, *wenn H die Bedingungen*

(i) $e \in H$,

(ii) $a, b \in H \Longrightarrow ab \in H$,

erfüllt. Ist G sogar eine Gruppe, so nennt man H eine Untergruppe *von G, wenn zusätzlich gilt*:

(iii) $a \in H \Longrightarrow a^{-1} \in H$.

Eine Untergruppe einer Gruppe G ist also ein Untermonoid, welches abgeschlossen unter Inversenbildung ist.

Man kann die Bedingung (i) bei der vorstehenden Definition einer Untergruppe $H \subset G$ abschwächen zu $H \neq \emptyset$, denn mit (ii) und (iii) folgt dann bereits $e \in H$. Für Monoide ist ein entsprechendes Vorgehen natürlich nicht möglich. Jede Gruppe G besitzt $\{e\}$ und G als *triviale Untergruppen*. Ist $m \in \mathbb{Z}$, so ist $m\mathbb{Z}$, die Menge der ganzzahligen Vielfachen von m, eine Untergruppe der additiven Gruppe $\mathbb{Z}$. Wir werden in 1.3/4 sehen, dass alle Untergruppen in $\mathbb{Z}$ von diesem Typ sind. Allgemeiner kann man die von einem Element a einer Gruppe G erzeugte *zyklische Untergruppe* betrachten. Diese besteht aus allen Potenzen a^n, $n \in \mathbb{Z}$, wobei man $a^n = (a^{-1})^{-n}$ für $n < 0$ setze; man vergleiche hierzu auch Abschnitt 1.3.

Definition 4. *Es seien G, G' Monoide mit den Einselementen e und e'. Ein* Monoidhomomorphismus $\varphi\colon G \longrightarrow G'$ *ist eine Abbildung φ von G nach G' mit*

(i) $\varphi(e) = e'$,

(ii) $\varphi(ab) = \varphi(a)\varphi(b)$ *für alle $a, b \in G$.*

Sind G, G' Gruppen, so heißt φ auch Gruppenhomomorphismus.

Bemerkung 5. *Eine Abbildung $\varphi\colon G \longrightarrow G'$ zwischen Gruppen ist genau dann ein Gruppenhomomorphismus, wenn $\varphi(ab) = \varphi(a)\varphi(b)$ für alle $a, b \in G$ gilt.*

Beweis. Es folgt $\varphi(e) = e'$ aus $\varphi(e) = \varphi(ee) = \varphi(e)\varphi(e)$. □

Bemerkung 6. *Ist* $\varphi\colon G \longrightarrow G'$ *ein Gruppenhomomorphismus, so folgt* $\varphi(a^{-1}) = (\varphi(a))^{-1}$ *für alle* $a \in G$.

Beweis. $e' = \varphi(e) = \varphi(aa^{-1}) = \varphi(a)\varphi(a^{-1})$. □

Ein Gruppenhomomorphismus $\varphi\colon G \longrightarrow G'$ heißt *Isomorphismus*, falls φ ein Inverses besitzt, d. h. falls es einen Gruppenhomomorphismus $\psi\colon G' \longrightarrow G$ mit $\psi \circ \varphi = \mathrm{id}_G$ und $\varphi \circ \psi = \mathrm{id}_{G'}$ gibt. Äquivalent hierzu ist, dass der Homomorphismus φ bijektiv ist. Injektive (bzw. surjektive) Gruppenhomomorphismen $G \longrightarrow G'$ nennt man auch *Monomorphismen* (bzw. *Epimorphismen*). Ein *Endomorphismus* von G ist ein Homomorphismus $G \longrightarrow G$, ein *Automorphismus* von G ein Isomorphismus $G \longrightarrow G$.

Seien $\varphi\colon G \longrightarrow G'$ und $\psi\colon G' \longrightarrow G''$ Gruppenhomomorphismen. Dann ist auch die Komposition $\psi \circ \varphi\colon G \longrightarrow G''$ ein Gruppenhomomorphismus. Weiter kann man zu $\varphi\colon G \longrightarrow G'$ die Untergruppen

$$\ker\varphi = \left\{g \in G\,;\, \varphi(g) = 1\right\} \subset G \qquad (\textit{Kern} \text{ von } \varphi)$$

sowie

$$\mathrm{im}\,\varphi = \varphi(G) \subset G' \qquad (\textit{Bild} \text{ von } \varphi)$$

bilden. Die Injektivität von φ ist äquivalent zu $\ker\varphi = \{1\}$. Im Folgenden seien noch einige Beispiele für Homomorphismen notiert.

(1) Sei G ein Monoid. Für festes $x \in G$ definiert

$$\varphi\colon \mathbb{N} \longrightarrow G, \qquad n \longmapsto x^n,$$

einen Monoidhomomorphismus, wenn man $\mathbb{N}$ als Monoid unter der Addition auffasst. Ist G eine Gruppe, so erhält man in gleicher Weise einen Gruppenhomomorphismus

$$\varphi\colon \mathbb{Z} \longrightarrow G, \qquad n \longmapsto x^n,$$

wobei $x^n := (x^{-1})^{-n}$ für $n < 0$ gesetzt sei. Umgekehrt ist klar, dass jeder Monoidhomomorphismus $\varphi\colon \mathbb{N} \longrightarrow G$ bzw. jeder Gruppenhomomorphismus $\varphi\colon \mathbb{Z} \longrightarrow G$ von dieser Gestalt ist; man setze $x = \varphi(1)$.

(2) Sei G eine Gruppe, $S(G)$ die Gruppe der bijektiven Selbstabbildungen von G. Für $a \in G$ definiere man $\tau_a \in S(G)$ als *Linkstranslation* mit a auf G, d. h.

$$\tau_a \colon G \longrightarrow G, \qquad g \longmapsto ag.$$

Dann ist

$$G \longrightarrow S(G), \qquad a \longmapsto \tau_a,$$

ein injektiver Gruppenhomomorphismus. Man kann daher G mit seinem Bild in $S(G)$ identifizieren, so dass G zu einer Untergruppe von $S(G)$ Anlass gibt. Insbesondere lässt sich eine Gruppe von n Elementen stets als Untergruppe der Permutationsgruppe $\mathfrak{S}_n$ interpretieren, ein Resultat, welches man auch als Satz von Cayley bezeichnet.

Analog zu den Linkstranslationen kann man auch *Rechtstranslationen* auf G erklären. Diese eignen sich ebenfalls dazu, einen injektiven Gruppenhomomorphismus $G \longrightarrow S(G)$ zu konstruieren; vgl. Aufgabe 4.

(3) Sei G eine abelsche Gruppe, $n \in \mathbb{N}$. Dann ist

$$G \longrightarrow G, \qquad g \longmapsto g^n,$$

ein Gruppenhomomorphismus.

(4) Sei G eine Gruppe, $a \in G$. Dann ist

$$\varphi_a \colon G \longrightarrow G, \qquad g \longmapsto aga^{-1},$$

ein sogenannter *innerer Automorphismus* von G. Die Menge $\mathrm{Aut}(G)$ der Automorphismen von G ist unter der Komposition als Verknüpfung eine Gruppe, und die Abbildung $G \longrightarrow \mathrm{Aut}(G)$, $a \longmapsto \varphi_a$, ist ein Gruppenhomomorphismus.

(5) Die reelle Exponentialfunktion definiert einen Gruppenisomorphismus $\mathbb{R} \xrightarrow{\sim} \mathbb{R}_{>0}$. Um dies einzusehen, müssen wir natürlich die aus der Analysis bekannten Eigenschaften der Exponentialfunktion benutzen, insbesondere die Funktionalgleichung $\exp(x + y) = \exp(x) \cdot \exp(y)$.

Lernkontrolle und Prüfungsvorbereitung

1. Was ist ein Monoid, was ist eine Gruppe? Erkläre insbesondere die Begriffe "Einselement" und "inverses Element".
2. Beschreibe einige einfache Beispiele von Monoiden und Gruppen.
3. Gib ein Beispiel einer Gruppe, die nicht kommutativ ist.
4. Was ist ein Untermonoid, was ist eine Untergruppe?

5. Gib einige Beispiele für Untergruppen an und erkläre insbesondere den Begriff einer zyklischen Untergruppe.

6. Was ist ein Monoidhomomorphismus, was ist ein Gruppenhomomorphismus? Wie verhält sich ein Gruppenhomomorphismus bezüglich inverser Elemente? Welche Untergruppen kann man in natürlicher Weise zu einem Gruppenhomomorphismus betrachten?

7. Beschreibe einige einfache Beispiele von Monoid- bzw. Gruppenhomomorphismen.

8. Zeige, dass eine Abbildung $\varphi\colon G \longrightarrow G'$ zwischen Gruppen bereits dann ein Gruppenhomomorphismus ist, wenn $\varphi(ab) = \varphi(a)\varphi(b)$ für alle $a, b \in G$ gilt.

Übungsaufgaben

1. *Führe den Beweis zu Bemerkung* 2.

2. *Die Exponentialfunktion liefert einen Isomorphismus zwischen der additiven Gruppe* $\mathbb{R}$ *und der multiplikativen Gruppe* $\mathbb{R}_{>0}$. *Überlege, ob es auch einen Isomorphismus zwischen der additiven Gruppe* $\mathbb{Q}$ *und der multiplikativen Gruppe* $\mathbb{Q}_{>0}$ *geben kann.*

3. Für ein Monoid G betrachte die folgenden Bedingungen:

   (i) G ist eine Gruppe.

   (ii) Für $a, x, y \in G$ mit $ax = ay$ oder $xa = ya$ folgt stets $x = y$.

   Es gilt (i) $\Longrightarrow$ (ii). Zeige, dass die Umkehrung für endliche Monoide G richtig ist, nicht aber für beliebige Monoide G.

4. Es sei G eine Gruppe. In Analogie zur Notation der Linkstranslation erkläre Rechtstranslationen auf G und konstruiere mit deren Hilfe einen injektiven Gruppenhomomorphismus $G \longrightarrow S(G)$.

5. Es sei X eine Menge mit einer Teilmenge $Y \subset X$. Zeige, dass die Gruppe $S(Y)$ in kanonischer Weise als Untergruppe von $S(X)$ aufgefasst werden kann.

6. Es sei G eine endliche abelsche Gruppe. Dann gilt $\displaystyle\prod_{g \in G} g^2 = 1$.

7. Es sei G eine Gruppe. Für alle $a \in G$ gelte $a^2 = 1$. Zeige, dass G abelsch ist.

8. Es sei G eine Gruppe mit Untergruppen $H_1, H_2 \subset G$. Zeige, dass $H_1 \cup H_2$ genau dann eine Untergruppe von G ist, wenn $H_1 \subset H_2$ oder $H_2 \subset H_1$ gilt.

1.2 Nebenklassen, Normalteiler, Faktorgruppen

Es sei G eine Gruppe, $H \subset G$ eine Untergruppe. Eine *Linksnebenklasse* von H in G ist eine Teilmenge von G der Gestalt

$$aH := \{ah\,;\ h \in H\},$$

wobei $a \in G$.

Satz 1. *Je zwei Linksnebenklassen von H in G sind gleichmächtig*[2]; *verschiedene Linksnebenklassen von H in G sind disjunkt. Insbesondere ist G disjunkte Vereinigung der Linksnebenklassen von H.*

Beweis. Für $a \in G$ ist die Linkstranslation $H \longrightarrow aH$, $h \longmapsto ah$, bijektiv. Folglich sind alle Linksnebenklassen gleichmächtig. Die zweite Behauptung ergibt sich aus folgendem Lemma:

Lemma 2. *Seien aH und bH Linksnebenklassen von H in G. Dann ist äquivalent*:

(i) $aH = bH$.
(ii) $aH \cap bH \neq \emptyset$.
(iii) $a \in bH$.
(iv) $b^{-1}a \in H$.

Beweis. Aus (i) folgt wegen $H \neq \emptyset$ trivialerweise (ii). Ist (ii) gegeben, so existiert ein $c \in aH \cap bH$, etwa $c = ah_1 = bh_2$ mit $h_1, h_2 \in H$. Es folgt $a = bh_2h_1^{-1} \in bH$ und somit (iii) bzw. die hierzu äquivalente Bedingung (iv). Gilt schließlich (iv), so erhält man $a \in bH$ und folglich $aH \subset bH$. Da mit $b^{-1}a$ aber auch das hierzu inverse Element $a^{-1}b$ zu H gehört, folgt entsprechend $bH \subset aH$ und somit $aH = bH$. □

Die Elemente einer Linksnebenklasse aH werden auch als *Repräsentanten* dieser Nebenklasse bezeichnet. Insbesondere ist also a ein Repräsentant der Nebenklasse aH. Für jeden Repräsentanten $a' \in aH$ gilt aufgrund des Lemmas $a'H = aH$. Die Menge der Linksnebenklassen von H in G wird

[2] Zwei Mengen X, Y heißen *gleichmächtig*, wenn es eine bijektive Abbildung $X \longrightarrow Y$ gibt.

mit G/H bezeichnet. Man definiert in analoger Weise die Menge $H\backslash G$ der *Rechtsnebenklassen* von H in G, d. h. der Teilmengen der Gestalt

$$Ha = \{ha\,;\ h \in H\},$$

wobei $a \in G$. Man prüft leicht nach, dass die bijektive Abbildung

$$G \longrightarrow G, \qquad g \longmapsto g^{-1},$$

eine Linksnebenklasse aH auf die Rechtsnebenklasse Ha^{-1} abbildet und somit eine Bijektion

$$G/H \longrightarrow H\backslash G, \qquad aH \longmapsto Ha^{-1},$$

definiert. Insbesondere gelten daher Satz 1 und Lemma 2 (mit den offensichtlichen Modifikationen in Lemma 2) auch für Rechtsnebenklassen. Man bezeichnet die Anzahl der Elemente von G/H bzw. $H\backslash G$ auch als *Index* $(G : H)$ von H in G. Schreiben wir noch $\operatorname{ord} G$ für die Anzahl der Elemente einer Gruppe G, man nennt dies die *Ordnung* von G, so ergibt sich als Folgerung zu Satz 1:

Korollar 3 (Satz von Lagrange). *Sei G eine endliche Gruppe, H eine Untergruppe von G. Dann gilt*

$$\operatorname{ord} G = \operatorname{ord} H \cdot (G : H).$$

Definition 4. *Eine Untergruppe $H \subset G$ heißt* Normalteiler *oder* normale Untergruppe *von G, wenn $aH = Ha$ für alle $a \in G$ gilt, d. h. wenn für jedes $a \in G$ die zugehörigen Links- und Rechtsnebenklassen von H in G übereinstimmen. Man bezeichnet die zu a gehörige Nebenklasse aH bzw. Ha dann auch als die* Restklasse *von a modulo H.*

Die Bedingung $aH = Ha$ lässt sich umschreiben zu $aHa^{-1} = H$. Eine Untergruppe $H \subset G$ ist jedoch bereits dann Normalteiler in G, wenn $aHa^{-1} \subset H$ für alle $a \in G$ gilt (alternativ: $H \subset aHa^{-1}$ für alle $a \in G$). Denn $aHa^{-1} \subset H$ ist gleichbedeutend mit $aH \subset Ha$, ebenso $a^{-1}Ha \subset H$ mit $Ha \subset aH$. Im Übrigen ist jede Untergruppe einer kommutativen Gruppe bereits Normalteiler.

Bemerkung 5. *Für einen Gruppenhomomorphismus* $\varphi\colon G \longrightarrow G'$ *ist* $\ker\varphi$, *der Kern von* φ, *ein Normalteiler in* G.

Beweis. Zunächst ist $\ker\varphi$ eine Untergruppe von G, und es ergibt sich $a\cdot(\ker\varphi)\cdot a^{-1}\subset\ker\varphi$ für alle $a\in G$ mit 1.1/6. □

Wir wollen im Weiteren zeigen, dass es zu jedem Normalteiler $N\subset G$ einen Gruppenhomomorphismus $\varphi\colon G\longrightarrow G'$ mit $\ker\varphi = N$ gibt. Die Idee hierzu ist, auf der Menge der Restklassen G/N eine geeignete Gruppenstruktur zu definieren und für φ die kanonische Projektion $\pi\colon G\longrightarrow G/N$ zu nehmen, welche ein Element $a\in G$ auf die zugehörige Restklasse aN abbildet. Sei also $N\subset G$ ein Normalteiler. Definiert man das Produkt von Teilmengen $X, Y\subset G$ durch

$$X\cdot Y\colon = \{x\cdot y\in G\,;\, x\in X, y\in Y\},$$

so kann man für $a, b\in G$ unter Benutzung der Normalteilereigenschaft von N schreiben:

$$(aN)\cdot(bN) = \{a\}\cdot(Nb)\cdot N = \{a\}\cdot(bN)\cdot N = \{ab\}\cdot(NN) = (ab)N.$$

Es ist also das Produkt zweier Nebenklassen mit Repräsentanten a bzw. b wieder eine Nebenklasse, und zwar mit Repräsentant ab. Wir können daher dieses Produkt als Verknüpfung "$\cdot$" in G/N auffassen, und es folgt unmittelbar aus den Gruppeneigenschaften von G, dass G/N mit dieser Verknüpfung eine Gruppe ist; $N = 1N$ ist das Einselement in G/N, und $a^{-1}N$ ist das inverse Element zu $aN\in G/N$. Im Übrigen ist klar, dass die kanonische Projektion

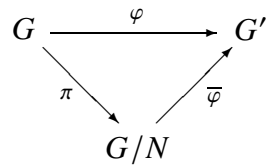
$$\pi\colon G\longrightarrow G/N,\qquad a\longmapsto aN,$$

ein surjektiver Gruppenhomomorphismus mit $\ker\pi = N$ ist. Wir nennen G/N die *Faktor-* oder *Restklassengruppe* von G modulo N.

Für viele Anwendungen ist es wichtig, zu wissen, dass der Gruppenhomomorphismus $\pi\colon G\longrightarrow G/N$ eine sogenannte universelle Eigenschaft erfüllt, welche G/N bis auf kanonische Isomorphie eindeutig charakterisiert:

Satz 6 (Homomorphiesatz). *Es sei* $\varphi\colon G\longrightarrow G'$ *ein Gruppenhomomorphismus und* $N\subset G$ *ein Normalteiler mit* $N\subset\ker\varphi$. *Dann existiert eindeutig*

ein Gruppenhomomorphismus $\overline{\varphi}\colon G/N \longrightarrow G'$ *mit* $\varphi = \overline{\varphi} \circ \pi$, *so dass also das Diagramm*



kommutiert. Es gilt

$$\operatorname{im}\overline{\varphi} = \operatorname{im}\varphi, \qquad \ker\overline{\varphi} = \pi(\ker\varphi), \qquad \ker\varphi = \pi^{-1}(\ker\overline{\varphi}).$$

Insbesondere ist $\overline{\varphi}$ *genau dann injektiv, wenn* $N = \ker\varphi$ *gilt.*

Beweis. Wenn $\overline{\varphi}$ existiert, so folgt

$$\overline{\varphi}(aN) = \overline{\varphi}\big(\pi(a)\big) = \varphi(a)$$

für $a \in G$, also ist $\overline{\varphi}$ eindeutig. Umgekehrt können wir natürlich $\overline{\varphi}$ durch die Gleichung $\overline{\varphi}(aN) = \varphi(a)$ erklären, wenn wir zeigen, dass $\varphi(a)$ unabhängig von der Auswahl des Repräsentanten $a \in aN$ ist. Gelte also $aN = bN$ für zwei Elemente $a, b \in G$. Dann folgt $b^{-1}a \in N \subset \ker\varphi$ und somit $\varphi(b^{-1}a) = 1$, also $\varphi(a) = \varphi(b)$. Dass $\overline{\varphi}$ ein Gruppenhomomorphismus ist, ergibt sich aus der Definition der Gruppenstruktur auf G/N oder, anders ausgedrückt, aus der Tatsache, dass π ein Epimorphismus zwischen Gruppen ist. Existenz und Eindeutigkeit von $\overline{\varphi}$ sind damit geklärt.

Die Gleichung $\ker\varphi = \pi^{-1}(\ker\overline{\varphi})$ folgt aus der Tatsache, dass φ die Komposition von $\overline{\varphi}$ mit π ist. Ferner gilt $\operatorname{im}\overline{\varphi} = \operatorname{im}\varphi$ sowie $\ker\overline{\varphi} = \pi(\ker\varphi)$ aufgrund der Surjektivität von π. □

Korollar 7. *Ist* $\varphi\colon G \longrightarrow G'$ *ein surjektiver Gruppenhomomorphismus, so ist* G' *kanonisch isomorph zu* $G/\ker\varphi$.

Wir wollen als Anwendung von Satz 6 die sogenannten Isomorphiesätze für Gruppen beweisen.

Satz 8 (1. Isomorphiesatz). *Es sei* G *eine Gruppe,* $H \subset G$ *eine Untergruppe und* $N \subset G$ *ein Normalteiler. Dann ist* HN *Untergruppe von* G *mit Normalteiler* N, *und* $H \cap N$ *ist Normalteiler von* H. *Der kanonische Homomorphismus*

$$H/H \cap N \longrightarrow HN/N$$

ist ein Isomorphismus.

Beweis. Unter Benutzung der Normalteilereigenschaft von N zeigt man unmittelbar, dass HN Untergruppe von G mit Normalteiler N ist. Man betrachte dann den Homomorphismus

$$H \hookrightarrow HN \xrightarrow{\pi} HN/N,$$

wobei π die kanonische Projektion bezeichne. Dieser ist surjektiv und besitzt $H \cap N$ als Kern. Somit ist $H \cap N$ Normalteiler in H, und der induzierte Homomorphismus

$$H/H \cap N \longrightarrow HN/N$$

ist nach Satz 6 oder Korollar 7 ein Isomorphismus. □

Satz 9 (2. Isomorphiesatz). *Sei G eine Gruppe, und seien N, H Normalteiler in G mit $N \subset H \subset G$. Dann ist N auch Normalteiler in H, und man kann H/N als Normalteiler von G/N auffassen. Der kanonische Gruppenhomomorphismus*

$$\big(G/N\big)\big/\big(H/N\big) \longrightarrow G/H$$

ist ein Isomorphismus.

Beweis. Wir wollen zunächst überlegen, dass man H/N als Untergruppe von G/N auffassen kann. Man betrachte hierzu den Gruppenhomomorphismus

$$H \hookrightarrow G \xrightarrow{\pi} G/N,$$

wobei π wieder die kanonische Projektion bezeichne. Da dieser Homomorphismus N als Kern besitzt, liefert er mit Satz 6 einen Monomorphismus $H/N \hookrightarrow G/N$, so dass wir H/N mit seinem Bild in G/N identifizieren können.

Als Nächstes beachte man, dass der Kern H der kanonischen Projektion $G \longrightarrow G/H$ den Normalteiler N enthält. Also induziert dieser Epimorphismus gemäß Satz 6 einen Epimorphismus $G/N \longrightarrow G/H$, dessen Kern ein Normalteiler ist und mit dem Bild von H unter der Projektion $G \longrightarrow G/N$ übereinstimmt. Dieses Bild hatten wir gerade mit H/N identifiziert. Wenden wir dann Satz 6 bzw. Korollar 7 nochmals an, so folgt, dass $G/N \longrightarrow G/H$ einen Isomorphismus

$$\big(G/N\big)\big/\big(H/N\big) \xrightarrow{\sim} G/H$$

induziert. □

Lernkontrolle und Prüfungsvorbereitung

1. Was ist eine Linksnebenklasse bzw. eine Rechtsnebenklasse zu einer Untergruppe in einer gegebenen Gruppe? Welche Eigenschaften besitzen solche Nebenklassen? Was sind Repräsentanten von Nebenklassen?
2. Zeige, dass je zwei verschiedene Linksnebenklassen (oder alternativ, Rechtsnebenklassen) einer Untergruppe in einer gegebenen Gruppe disjunkt sind.
3. Was versteht man unter dem Index einer Untergruppe in einer Gruppe?
4. Formuliere den "Satz von Lagrange" und beweise ihn.
5. Was ist ein Normalteiler einer Gruppe? In welchen Situationen treten Normalteiler in natürlicher Weise auf?
6. Es sei N ein Normalteiler in einer Gruppe G. Weiter seien N_1 und N_2 zwei Nebenklassen zu N mit Repräsentanten $a_i \in N_i$ für $i = 1, 2$. Zeige, dass die Nebenklasse zu N mit Repräsentant $a_1 \cdot a_2$ nur von N_1 und N_2 abhängt, nicht aber von der Wahl der Repräsentanten $a_1 \in N_1$ und $a_2 \in N_2$.
7. Beschreibe die Konstruktion der Restklassengruppe G/N für einen Normalteiler N in einer Gruppe G.
8. Formuliere den Homomorphiesatz für Gruppen und beweise ihn.

+9. Formuliere und beweise den 1. Isomorphiesatz für Gruppen.

+10. Formuliere und beweise den 2. Isomorphiesatz für Gruppen.

Übungsaufgaben

1. *Es sei G eine Gruppe und H eine Untergruppe vom Index 2. Zeige, dass H Normalteiler in G ist. Gilt die gleiche Aussage auch für den Fall, dass H vom Index 3 ist?*
2. *Es sei G eine Gruppe und $N \subset G$ ein Normalteiler. Gib eine alternative Konstruktion der Faktorgruppe G/N an. Betrachte hierzu die* Menge $X = G/N$ *der Linksnebenklassen von N in G und zeige die Existenz eines Gruppenhomomorphismus $\varphi\colon G \longrightarrow S(X)$ mit* $\ker\varphi = N$.

3. Es sei X eine Menge, $Y \subset X$ eine Teilmenge, G eine Gruppe und G^X die Gruppe der G-wertigen Funktionen auf X. Zeige, dass die Teilmenge $N := \{f \in G^X \,;\, f(y) = 1 \text{ für alle } y \in Y\}$ einen Normalteiler in G^X bildet mit $G^X/N \simeq G^Y$.

4. Sei $\varphi\colon G \longrightarrow G'$ ein Gruppenhomomorphismus. Zeige:
   (i) Ist $H \subset G$ Untergruppe, so ist $\varphi(H)$ Untergruppe in G'. Die entsprechende Aussage für Normalteiler ist allgemein nur dann richtig, wenn φ surjektiv ist.
   (ii) Ist $H' \subset G'$ Untergruppe (bzw. Normalteiler) in G', so gilt dasselbe für $\varphi^{-1}(H') \subset G$.

5. Es sei G eine endliche Gruppe mit zwei Untergruppen $H_1, H_2 \subset G$, wobei $H_1 \subset H_2$ gelte. Zeige $(G : H_1) = (G : H_2) \cdot (H_2 : H_1)$.

6. Eine Gruppe G enthalte einen Normalteiler N mit der folgenden Maximalitätseigenschaft: Ist $H \subset G$ Untergruppe mit $H \supset N$, so gilt bereits $H = G$ oder $H = N$. Zeige, dass je zwei Untergruppen $H_1, H_2 \subset G$ mit $H_1 \neq \{1\} \neq H_2$ und $H_1 \cap N = H_2 \cap N = \{1\}$ zueinander isomorph sind.

1.3 Zyklische Gruppen

Sei G eine Gruppe und $X \subset G$ eine Teilmenge. Definiert man H als Durchschnitt aller Untergruppen von G, welche X enthalten, so ist H wieder eine Untergruppe von G, und zwar die (eindeutig bestimmte) kleinste Untergruppe von G, welche X enthält. Man sagt, H werde von (den Elementen von) X erzeugt oder, wenn H schon gleich G ist, G werde von X erzeugt. Die von X in G erzeugte Untergruppe H kann auch in konkreter Weise angegeben werden. Sie besteht aus allen Elementen der Form

$$x_1^{\varepsilon_1} \cdot \ldots \cdot x_n^{\varepsilon_n}$$

mit $x_1, \ldots, x_n \in X$ und $\varepsilon_1, \ldots, \varepsilon_n \in \{1, -1\}$, wobei n in $\mathbb{N}$ variieren darf. Die so beschriebenen Elemente bilden offenbar die kleinste Untergruppe von G, die X enthält, und dies ist nach Definition die Gruppe H.

Im Folgenden interessieren wir uns nur für den Fall, dass X aus genau einem Element x besteht. Die Beschreibung der von $x \in G$ erzeugten Untergruppe, für die wir auch die Notation $\langle x \rangle$ verwenden, vereinfacht sich dann:

Bemerkung 1. *Sei x ein Element einer Gruppe G. Dann besteht die von x erzeugte Untergruppe $\langle x\rangle \subset G$ aus allen Potenzen x^n, $n \in \mathbb{Z}$. Mit anderen Worten, $\langle x\rangle$ ist gleich dem Bild des Gruppenhomomorphismus*

$$\mathbb{Z} \longrightarrow G, \qquad n \longmapsto x^n,$$

wobei mit $\mathbb{Z}$ die additive Gruppe der ganzen Zahlen gemeint sei. Insbesondere ist $\langle x\rangle$ kommutativ.

Definition 2. *Eine Gruppe G heißt* zyklisch, *wenn sie von einem Element erzeugt wird. Äquivalent hierzu ist, dass es einen surjektiven Gruppenhomomorphismus $\mathbb{Z} \longrightarrow G$ gibt.*

Man beachte, dass für eine kommutative Gruppe G mit additiv geschriebener Verknüpfung die Abbildung $\mathbb{Z} \longrightarrow G$ aus Bemerkung 1 durch die Vorschrift $n \longmapsto n \cdot x$ gegeben wird. Dabei ist $n \cdot x$ für $n \geq 0$ als n-fache Summe von x aufzufassen und für $n < 0$ als $(-n)$-fache Summe von $-x$. Insbesondere ist damit klar, dass die additive Gruppe $\mathbb{Z}$ von dem Element $1 \in \mathbb{Z}$ erzeugt wird und somit zyklisch ist. Man nennt $\mathbb{Z}$ die *freie zyklische Gruppe*; die Ordnung dieser Gruppe ist unendlich. Für $m \in \mathbb{Z}$ ist aber auch die Untergruppe $m\mathbb{Z}$ aller ganzzahligen Vielfachen von m zyklisch, sie wird von $m = m \cdot 1$ erzeugt. Die Faktorgruppe $\mathbb{Z}/m\mathbb{Z}$ ist ebenfalls zyklisch, sie wird von der Restklasse $1 + m\mathbb{Z}$ erzeugt. Ist $m \neq 0$, etwa $m > 0$, so bezeichnet man $\mathbb{Z}/m\mathbb{Z}$ als *zyklische Gruppe der Ordnung m*. In der Tat besteht $\mathbb{Z}/m\mathbb{Z}$ für $m > 0$ aus genau m Elementen, nämlich aus den Restklassen $0 + m\mathbb{Z}, \ldots, (m-1) + m\mathbb{Z}$. Wir wollen im Folgenden zeigen, dass $\mathbb{Z}$ und die Gruppen des Typs $\mathbb{Z}/m\mathbb{Z}$ bis auf Isomorphie die einzigen zyklischen Gruppen sind. Mit Hilfe des Homomorphiesatzes (in der Version 1.2/7) sieht man, dass eine Gruppe G genau dann zyklisch ist, wenn es einen Isomorphismus $\mathbb{Z}/H \xrightarrow{\sim} G$ gibt, wobei H eine Untergruppe und damit ein Normalteiler von $\mathbb{Z}$ ist. Damit reduziert sich die Bestimmung aller zyklischen Gruppen auf die Bestimmung aller Untergruppen von $\mathbb{Z}$.

Satz 3. *Es sei G eine zyklische Gruppe. Dann gilt*

$$G \simeq \begin{cases} \mathbb{Z}, & \text{falls } \operatorname{ord} G = \infty, \\ \mathbb{Z}/m\mathbb{Z}, & \text{falls } \operatorname{ord} G = m < \infty. \end{cases}$$

Die Gruppen $\mathbb{Z}$ und $\mathbb{Z}/m\mathbb{Z}$ für $m > 0$ ganz sind bis auf Isomorphie die einzigen zyklischen Gruppen.

Zum Beweis des Satzes genügt es, wie wir gesehen haben, folgendes Lemma bereitzustellen:

Lemma 4. *Sei $H \subset \mathbb{Z}$ Untergruppe. Dann existiert ein $m \in \mathbb{Z}$ mit $H = m\mathbb{Z}$. Insbesondere ist jede Untergruppe von $\mathbb{Z}$ zyklisch.*

Beweis. Wir dürfen $H \neq 0$ annehmen, wobei 0 die nur aus dem Nullelement bestehende Untergruppe von $\mathbb{Z}$ bezeichne. Dann gibt es in H positive Elemente; es sei m das kleinste positive Element von H. Wir behaupten $H = m\mathbb{Z}$. Natürlich gilt $m\mathbb{Z} \subset H$. Sei umgekehrt $a \in H$. Indem wir a durch m mit Rest dividieren, erhalten wir $q, r \in \mathbb{Z}$, $0 \leq r < m$, mit $a = qm + r$. Dabei ist $r = a - qm$ Element von H und, da alle positiven Elemente von H größer oder gleich m sind, folgt notwendig $r = 0$. Also gilt $a = qm \in m\mathbb{Z}$ und damit $H \subset m\mathbb{Z}$. Insgesamt ergibt sich $H = m\mathbb{Z}$. □

Satz 5. (i) *Ist G eine zyklische Gruppe, so ist jede Untergruppe $H \subset G$ zyklisch.*

(ii) *Ist $\varphi\colon G \longrightarrow G'$ ein Gruppenhomomorphismus und ist G zyklisch, so sind auch* $\ker \varphi$ *und* $\operatorname{im} \varphi$ *zyklisch.*

Beweis. Es ergibt sich unmittelbar aus der Definition zyklischer Gruppen, dass das Bild einer zyklischen Gruppe unter einem Gruppenhomomorphismus $\varphi\colon G \longrightarrow G'$ wieder zyklisch ist. Da $\ker \varphi$ eine Untergruppe von G ist, bleibt somit lediglich Aussage (i) zu verifizieren. Sei also G zyklisch und $H \subset G$ eine Untergruppe. Weiter sei $\pi\colon \mathbb{Z} \longrightarrow G$ ein Epimorphismus. Dann ist $\pi^{-1}(H)$ eine Untergruppe von $\mathbb{Z}$ und somit gemäß Lemma 4 zyklisch. Es folgt, dass H als Bild von $\pi^{-1}(H)$ unter π wieder zyklisch ist, d. h. Aussage (i) ist bewiesen. □

Sei G eine Gruppe. Für ein Element $a \in G$ definiert man dessen *Ordnung* $\operatorname{ord} a$ als die Ordnung der von a erzeugten zyklischen Untergruppe in G. Wir wissen bereits, dass $\varphi\colon \mathbb{Z} \longrightarrow G, n \longmapsto a^n$, einen Epimorphismus von $\mathbb{Z}$ auf die von a erzeugte zyklische Untergruppe $H \subset G$ definiert. Gilt $\ker \varphi = m\mathbb{Z}$ und ist die Gruppe G endlich, so folgt notwendig $m \neq 0$, etwa $m > 0$, und es ist H isomorph zu $\mathbb{Z}/m\mathbb{Z}$. Also ist m die kleinste positive Zahl mit der Eigenschaft $a^m = 1$, und man sieht, dass H aus genau den (paarweise

verschiedenen) Elementen $1 = a^0, a^1, \ldots, a^{m-1}$ besteht. Insbesondere folgt $\operatorname{ord} a = m$.

Satz 6 (Kleiner Fermatscher Satz). *Sei G eine endliche Gruppe, $a \in G$. Dann ist* $\operatorname{ord} a$ *ein Teiler von* $\operatorname{ord} G$, *und es gilt* $a^{\operatorname{ord} G} = 1$.

Zum *Beweis* wendet man den Satz von Lagrange 1.2/3 auf die von a erzeugte zyklische Untergruppe von G an.

Korollar 7. *Für eine Gruppe G sei $p := \operatorname{ord} G$ eine Primzahl. Dann ist G zyklisch, $G \simeq \mathbb{Z}/p\mathbb{Z}$, und für jedes $a \in G$, $a \neq 1$, folgt* $\operatorname{ord} a = p$. *Insbesondere erzeugt jedes solche a die zyklische Gruppe G.*

Beweis. Sei $a \in G$, $a \neq 1$, und sei $H \subset G$ die von a erzeugte zyklische Gruppe. Da $\operatorname{ord} a = \operatorname{ord} H$ größer als 1 ist, nach Satz 6 aber auch ein Teiler von $p = \operatorname{ord} G$ sein muss, folgt $\operatorname{ord} a = \operatorname{ord} H = p$. Also hat man $H = G$, d. h. G wird von a erzeugt und ist somit zyklisch. Wegen Satz 3 ist G isomorph zu $\mathbb{Z}/p\mathbb{Z}$. □

Lernkontrolle und Prüfungsvorbereitung

1. Es seien $x_1, \ldots, x_n$ Elemente einer Gruppe G. Was bedeutet es, wenn man sagt, G werde von den Elementen $x_1, \ldots, x_n$ erzeugt?
2. Wie lautet die Definition einer zyklischen Gruppe? Wie kann man alternativ zyklische Gruppen unter Nutzung von Gruppenhomomorphismen charakterisieren?
3. Bestimme alle Untergruppen der additiven Gruppe $\mathbb{Z}$. Bestimme alle zyklischen Gruppen (bis auf Isomorphie).
4. Zeige, dass jede Untergruppe einer zyklischen Gruppe wiederum zyklisch ist.
5. Zeige, dass jede Restklassengruppe einer zyklischen Gruppe wiederum zyklisch ist.
6. Was ist die Ordnung $\operatorname{ord} G$ einer Gruppe G? Was ist die Ordnung $\operatorname{ord} a$ eines Elements $a \in G$?
7. Formuliere und beweise den "Kleinen Fermatschen Satz".
8. Zeige, dass jede Gruppe von Primzahlordnung zyklisch und insbesondere kommutativ ist.

Übungsaufgaben

1. *Für $m \in \mathbb{N}-\{0\}$ setze $G_m := \{0, 1, \ldots, m-1\}$. Durch*

$$a \circ b := \text{ der Rest von } a+b \text{ bei Division durch } m$$

wird auf G_m eine Verknüpfung erklärt. Zeige in direkter Weise, dass "$\circ$" eine Gruppenstruktur auf G_m definiert und dass die entstehende Gruppe isomorph zu $\mathbb{Z}/m\mathbb{Z}$ ist.

2. *Bestimme für $m \in \mathbb{N}-\{0\}$ alle Untergruppen von $\mathbb{Z}/m\mathbb{Z}$.*

3. Betrachte $\mathbb{Z}$ als additive Untergruppe von $\mathbb{Q}$ und zeige:
   (i) Jedes Element in $\mathbb{Q}/\mathbb{Z}$ ist von endlicher Ordnung.
   (ii) Für jedes $n \in \mathbb{N} - \{0\}$ besitzt $\mathbb{Q}/\mathbb{Z}$ genau eine Untergruppe der Ordnung n, und diese ist zyklisch.

4. Es seien $m, n \in \mathbb{N} - \{0\}$. Zeige, dass die Gruppen $\mathbb{Z}/mn\mathbb{Z}$ und $\mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$ genau dann isomorph sind, wenn m und n teilerfremd sind. Insbesondere ist ein Produkt zweier endlicher zyklischer Gruppen mit teilerfremden Ordnungen wieder zyklisch.

5. Es sei $\varphi\colon \mathbb{Z}^n \longrightarrow \mathbb{Z}^n$ ein Endomorphismus des n-fachen Produkts der additiven Gruppe $\mathbb{Z}$, wobei $n \in \mathbb{N}$. Zeige: Es ist φ genau dann injektiv, wenn $\mathbb{Z}^n/\operatorname{im}\varphi$ eine endliche Gruppe ist. (*Hinweis*: Betrachte den zu φ gehörigen Homomorphismus von $\mathbb{Q}$-Vektorräumen $\varphi_{\mathbb{Q}}\colon \mathbb{Q}^n \longrightarrow \mathbb{Q}^n$.)

2. Ringe und Polynome

Überblick und Hintergrund

Ein *Ring* ist eine additiv geschriebene abelsche Gruppe R, auf der zusätzlich eine Multiplikation definiert ist, wie etwa beim Ring $\mathbb{Z}$ der ganzen Zahlen. Dabei verlangt man, dass R ein Monoid bezüglich der Multiplikation ist und dass Addition und Multiplikation im Sinne der Distributivgesetze miteinander verträglich sind. Wir werden die Multiplikation in Ringen stets als *kommutativ* voraussetzen, abgesehen von einigen Betrachtungen in Abschnitt 2.1. Bilden die von Null verschiedenen Elemente eines Ringes sogar eine (abelsche) Gruppe bezüglich der Multiplikation, so handelt es sich um einen *Körper*. Die Definition eines Rings geht dem Sinne nach auf R. Dedekind zurück. Bei Dedekind waren Ringe zahlentheoretisch motiviert durch das Rechnen mit ganzen Zahlen in algebraischen Zahlkörpern, also durch das Studium algebraischer Gleichungen mit *ganzzahligen* Koeffizienten. Wir werden jedoch auf Ringe ganzer algebraischer Zahlen nur am Rande eingehen. Wichtiger sind für uns Körper als Koeffizientenbereiche algebraischer Gleichungen sowie Polynomringe über Körpern. Im Folgenden wollen wir den Polynombegriff etwas näher erläutern. Polynome sind bei der Handhabung algebraischer Gleichungen und insbesondere algebraischer Körpererweiterungen von grundlegender Bedeutung.

Wenn man eine algebraische Gleichung

$$(*) \qquad x^n + a_1 x^{n-1} + \ldots + a_n = 0$$

S. Bosch, *Algebra*, https://doi.org/10.1007/978-3-662-67464-2_3

lösen möchte, etwa mit Koeffizienten $a_1, \ldots, a_n$ aus einem Körper K, so liegt es nahe, die unbekannte Größe x zunächst als "variabel" anzusehen. Man betrachtet dann sozusagen die aus den Koeffizienten a_i gebildete Funktion $f(x) = x^n + a_1 x^{n-1} + \ldots + a_n$, welche einem Element x den Funktionswert $f(x)$ zuordnet, und bemüht sich darum, deren Nullstellen zu bestimmen. Dabei muss man streng genommen natürlich den Definitionsbereich festlegen, in dem x variieren darf, beispielsweise K selbst oder für $K = \mathbb{Q}$ auch die reellen oder die komplexen Zahlen. Man nennt $f(x)$ eine *polynomiale Funktion* in x oder in nicht ganz korrekter Sprechweise auch ein *Polynom* in x.

Das Auffinden eines geeigneten Definitionsbereiches, der groß genug ist, um "alle" Nullstellen von f zu enthalten, ist jedoch ein grundsätzliches Problem. Aus historischer Sicht ist an dieser Stelle der Fundamentalsatz der Algebra von entscheidender Bedeutung. Er hat nämlich für $K \subset \mathbb{C}$ zur Folge, dass alle Lösungen von $(*)$ komplexe Zahlen sind. Es ist daher angemessen, $f(x)$ in diesem Falle als polynomiale Funktion auf $\mathbb{C}$ zu interpretieren. Probleme anderer Art ergeben sich, wenn man algebraische Gleichungen mit Koeffizienten aus einem endlichen Körper $\mathbb{F}$ betrachten möchte; vgl. 2.3/6 oder Abschnitt 3.8 zur Definition solcher Körper. Besteht $\mathbb{F}$ etwa aus den Elementen $x_1, \ldots, x_q$, so ist

$$g(x) = \prod_{j=1}^{q} (x - x_j) = x^q + \ldots + (-1)^q x_1 \ldots x_q$$

eine polynomiale Funktion, die auf ganz $\mathbb{F}$ verschwindet, obwohl ihre "Koeffizienten" nicht alle Null sind. Hieraus folgt, dass man je nach betrachtetem Definitionsbereich von der polynomialen Funktion $f(x)$, die einer algebraischen Gleichung $(*)$ zugeordnet ist, nicht unbedingt auf die Koeffizienten der Gleichung $(*)$ zurückschließen kann.

Um solche Schwierigkeiten auszuräumen, rückt man von der Vorstellung ab, ein Polynom sei eine *Funktion* auf einem bestimmten Definitionsbereich und versucht, zwei Gesichtspunkte zu realisieren. Zum einen möchte man, dass Polynome in umkehrbar eindeutiger Weise durch ihre "Koeffizienten" charakterisiert sind. Daneben soll aber auch der Funktionscharakter von Polynomen erhalten bleiben, und zwar in der Weise, dass man in Polynome jeweils Elemente aus beliebigen Körpern (oder Ringen), die den gegebenen Koeffizientenbereich erweitern, einsetzen kann. Dies erreicht man, indem man ein Polynom mit Koeffizienten $a_0, \ldots, a_n$ als formale

Summe $f = \sum_{j=0}^{n} a_j X^j$ erklärt, was letztendlich bedeutet, dass man unter f lediglich die Folge der Koeffizienten $a_0, \ldots, a_n$ zu verstehen hat. Setzt man den Koeffizientenbereich K als Körper (oder auch als Ring) voraus, so kann man in gewohnter Weise Polynome addieren und multiplizieren, indem man die üblichen Rechenregeln formal anwendet. Auf diese Weise bilden die Polynome mit Koeffizienten aus K einen Ring $K[X]$. Zudem kann man Elemente x aus beliebigen Erweiterungskörpern (oder Erweiterungsringen) $K' \supset K$ in Polynome $f \in K[X]$ einsetzen; man ersetze nämlich die Variable X jeweils durch x und betrachte den resultierenden Ausdruck $f(x)$ als Element in K'. Insbesondere können wir von den Nullstellen von f in K' reden. Wir werden diesen Formalismus für Polynome einer Variablen in 2.1 und für Polynome mehrerer Variablen in 2.5 genauer studieren.

Das Problem der Lösung algebraischer Gleichungen mit Koeffizienten aus einem Körper K formuliert sich somit in etwas präziserer Form als Problem, für normierte Polynome mit Koeffizienten in K, also für Polynome des Typs $f = X^n + a_1 X^{n-1} + \ldots + a_n \in K[X]$, die Nullstellen in geeigneten Erweiterungskörpern K' von K zu finden. Bevor man mit der eigentlichen Arbeit hierzu beginnt, ist noch eine nunmehr triviale Bemerkung angebracht: Lässt sich das Polynom f in $K[X]$ als Produkt zweier Polynome $g, h \in K[X]$ schreiben, also $f = gh$, so genügt es zur Bestimmung der Nullstellen von f, die Nullstellen von g und h separat zu bestimmen. Für $x \in K'$ gilt nämlich $f(x) = (gh)(x) = g(x)h(x)$, wie man ohne Schwierigkeiten verifiziert. Da diese Gleichung in einem Körper zu lesen ist, verschwindet f genau dann in x, wenn g oder h dort verschwinden. Man sollte also zur Vereinfachung des Problems die algebraische Gleichung $f(x) = 0$ zu Gleichungen niedrigeren Grades reduzieren, indem man f in $K[X]$ als Produkt normierter Faktoren niedrigeren Grades schreibt. Ist dies nicht mehr möglich, so nennt man f bzw. die algebraische Gleichung $f(x) = 0$ *irreduzibel*.

Diese Überlegungen zeigen insbesondere, dass man Faktorisierungen von Polynomen studieren muss. Wir werden dies in 2.4 tun. Ausgehend von der Tatsache, dass man durch Polynome mit Rest dividieren kann, werden wir zeigen, dass in $K[X]$ in gleicher Weise wie im Ring $\mathbb{Z}$ der ganzen Zahlen der Satz von der eindeutigen Primfaktorzerlegung gilt. Jedes normierte Polynom lässt sich somit in eindeutiger Weise als Produkt normierter irreduzibler Polynome schreiben. Weitere Überlegungen in 2.7 und 2.8 beschäftigen sich im Anschluss hieran mit Kriterien der Irreduzibilität,

also mit der Frage, wie man entscheiden kann, ob ein gegebenes Polynom $f \in K[X]$ irreduzibel ist oder nicht.

Das Studium von Faktorzerlegungen im Polynomring $K[X]$ ist aber auch noch vor einem anderen Hintergrund von großem Interesse. Um dies näher zu erläutern, gehen wir kurz auf den Begriff des *Ideals* eines Rings ein, der mit zu den Grundlagen über Ringe gehört und in 2.2 behandelt wird. Ein Ideal $\mathfrak{a}$ eines Ringes R ist eine additive Untergruppe von R, so dass aus $r \in R$, $a \in \mathfrak{a}$ stets $ra \in \mathfrak{a}$ folgt. Ideale verhalten sich in vielerlei Hinsicht wie Normalteiler bei Gruppen. Insbesondere kann man den Restklassenring $R/\mathfrak{a}$ eines Ringes R nach einem Ideal $\mathfrak{a} \subset R$ bilden, den Homomorphiesatz beweisen usw.; vgl. 2.3. Die Einführung von Idealen erfolgte gegen Ende des 19. Jahrhunderts im Zusammenhang mit Versuchen, den Satz über die eindeutige Primfaktorzerlegung in Ringen ganzer algebraischer Zahlen zu beweisen. Als man eingesehen hatte, dass dieser Satz in solchen Ringen nicht uneingeschränkt gültig ist, hatte man sich eine gewisse Zeit mit Zerlegungen in sogenannte *ideale Zahlen* behelfen wollen. Doch Dedekind bemerkte schließlich, dass man nicht einzelne Elemente faktorisieren sollte, sondern gewisse Teilmengen eines Ringes, die er Ideale nannte. So bewies Dedekind 1894 den Satz über die eindeutige Primfaktorzerlegung für Ideale in Ringen ganzer algebraischer Zahlen. Heute bezeichnet man Ringe ohne Nullteiler, in denen dieser Satz gilt, als *Dedekind-Ringe*.

Für uns ist wichtig, dass der Polynomring $K[X]$ über einem Körper K ein *Hauptidealring* ist, d. h. dass jedes Ideal $\mathfrak{a} \subset K[X]$ von der Form (f) ist, also von einem einzigen Element $f \in K[X]$ erzeugt wird. Dieses Resultat beweisen wir in 2.4/3 und zeigen dann, dass in jedem Hauptidealring der Satz von der eindeutigen Primfaktorzerlegung gilt. Untersuchungen dieser Art führen in direkter Weise zu dem Verfahren von Kronecker, welches wir allerdings erst in 3.4/1 genauer besprechen werden. Das Verfahren gestattet es in einfacher Weise, für eine irreduzible algebraische Gleichung $f(x) = 0$ mit Koeffizienten aus einem Körper K einen Erweiterungskörper K' anzugeben, der eine Lösung dieser Gleichung enthält. Man setze nämlich $K' = K[X]/(f)$, wobei die Restklasse $\overline{X}$ zu $X \in K[X]$ die gewünschte Lösung ist. Wenn auch dieses Verfahren noch keinen Aufschluss über die genauere Struktur des Körpers K' gibt, etwa im Hinblick auf eine Auflösung durch Radikale, so liefert es doch einen wertvollen Beitrag zur Frage der Existenz von Lösungen.

Zur Illustration des Rechnens in Hauptidealringen gehen wir zum Schluss des Kapitels in 2.9 noch auf die sogenannte Elementarteilertheorie ein, ein Thema, das im Grunde genommen der Linearen Algebra zuzuordnen ist. Als Verallgemeinerung von Vektorräumen über Körpern studieren wir dort "Vektorräume" oder, wie man sagt, *Moduln* über Hauptidealringen.

2.1 Ringe, Polynomringe einer Variablen

Definition 1. *Ein* Ring (mit Eins) *ist eine Menge R mit zwei inneren Verknüpfungen, geschrieben als Addition* "+" *und Multiplikation* "$\cdot$", *so dass folgende Bedingungen erfüllt sind*:

(i) *R ist eine kommutative Gruppe bezüglich der Addition.*

(ii) *R ist ein Monoid bezüglich der Multiplikation, d. h. die Multiplikation ist assoziativ, und es existiert in R ein Einselement bezüglich der Multiplikation.*

(iii) *Es gelten die Distributivgesetze, d. h.*

$$(a+b)\cdot c = a\cdot c + b\cdot c, \quad c\cdot(a+b) = c\cdot a + c\cdot b, \quad \text{für } a,b,c \in R.$$

R heißt kommutativ, *falls die Multiplikation kommutativ ist.*[1]

Bei den Distributivgesetzen (iii) haben wir auf der rechten Seite der Gleichungen jeweils auf eine spezielle Klammerung verzichtet. Man vereinbart nämlich, dass wie beim Rechnen mit gewöhnlichen Zahlen das Multiplikationszeichen stärker bindet als das Additionszeichen. Das Nullelement der Addition wird bei Ringen stets mit 0 bezeichnet, das Einselement der Multiplikation mit 1. Dabei ist auch $1 = 0$ zugelassen. Dies ist jedoch nur im Nullring möglich, der lediglich aus dem Nullelement 0 besteht. Man bezeichnet den Nullring meist ebenfalls mit 0, wobei man natürlich streng genommen zwischen 0 als Element und 0 als Ring zu unterscheiden hat. Für das Rechnen in Ringen gelten ähnliche Regeln wie für das Rechnen mit gewöhnlichen Zahlen, z. B.

[1] Wir gehen in diesem Abschnitt zwar auf einige Notationen und Beispiele für nichtkommutative Ringe ein, werden ansonsten aber, wenn nichts anderes gesagt ist, unter einem Ring stets einen *kommutativen* Ring verstehen.

$$0 \cdot a = 0 = a \cdot 0, \qquad (-a) \cdot b = -(ab) = a \cdot (-b), \qquad \text{für } a, b \in R.$$

Man beachte aber, dass etwa aus $ab = ac$ bzw. $a \cdot (b - c) = 0$ (wobei $a \neq 0$) nicht automatisch $b = c$ folgt. Auf letztere Gleichung kann man im Allgemeinen nur in Integritätsringen schließen (siehe weiter unten) oder dann, wenn es zu a ein inverses Element bezüglich der Multiplikation gibt. Bei der Anwendung von Kürzungsregeln in allgemeinen Ringen ist daher Vorsicht geboten.

Ist R ein Ring und $S \subset R$ eine Teilmenge, so nennt man S einen *Unterring* von R, wenn S bezüglich der Addition eine Untergruppe sowie bezüglich der Multiplikation ein Untermonoid von R ist. Insbesondere ist S mit den von R induzierten Verknüpfungen selbst wieder ein Ring. Man nennt das Paar $S \subset R$ auch eine *Ringerweiterung*.

Für einen Ring R bezeichnet man mit

$$R^* = \{a \in R\,;\ \text{es existiert } b \in R \text{ mit } ab = ba = 1\}$$

die Menge der multiplikativ invertierbaren Elemente oder *Einheiten* von R. Man prüft leicht nach, dass R^* eine Gruppe bezüglich der Multiplikation ist. Es heißt R *Schiefkörper*, wenn $R \neq 0$ und $R^* = R - \{0\}$ gilt, d. h. wenn $1 \neq 0$ gilt und weiter jedes von 0 verschiedene Element aus R eine Einheit ist. Ist zusätzlich die Multiplikation von R kommutativ, so heißt R *Körper*. Ein Element a eines Ringes R heißt *Nullteiler*, wenn ein $b \in R - \{0\}$ mit $ab = 0$ oder $ba = 0$ existiert. In Körpern und Schiefkörpern gibt es außer der 0 keine weiteren Nullteiler. Wir nennen einen kommutativen Ring R *nullteilerfrei* oder *Integritätsring*, wenn $R \neq 0$ ist und R nur 0 als Nullteiler besitzt. Im Folgenden seien einige Beispiele für Ringe angeführt.

(1) $\mathbb{Z}$ ist ein Integritätsring, dessen Einheitengruppe aus den Elementen 1 und -1 besteht.

(2) $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$ bilden Körper, die Hamiltonschen Quaternionen $\mathbb{H}$ einen Schiefkörper. Der Vollständigkeit halber sei hier an die Konstruktion von $\mathbb{H}$ erinnert. Man gehe aus von einem 4-dimensionalen $\mathbb{R}$-Vektorraum V mit Basis e, i, j, k. Sodann setze man

$$e^2 = e, \quad ei = ie = i, \quad ej = je = j, \quad ek = ke = k,$$
$$i^2 = j^2 = k^2 = -e,$$
$$ij = -ji = k, \quad jk = -kj = i, \quad ki = -ik = j,$$

und erkläre das Produkt beliebiger Elemente aus V durch $\mathbb{R}$-lineare Ausdehnung. Mit dieser Multiplikation sowie mit der Vektorraumaddition ist V ein (nicht-kommutativer) Ring $\mathbb{H}$, ja sogar ein Schiefkörper, mit e als Einselement. Indem man den Körper $\mathbb{R}$ der reellen Zahlen mit $\mathbb{R}e$ identifiziert, kann man $\mathbb{R}$ als Teilkörper von $\mathbb{H}$ auffassen, d. h. als Unterring, der ein Körper ist. In ähnlicher Weise lässt sich auch $\mathbb{C}$ als Teilkörper von $\mathbb{H}$ deuten.

(3) Es sei K ein Körper. Dann ist $R = K^{n\times n}$, also die Menge aller $(n \times n)$-Matrizen mit Koeffizienten in K, unter der gewöhnlichen Addition und Multiplikation von Matrizen ein Ring mit Einheitengruppe

$$R^* = \{A \in K^{n\times n}\,;\ \det A \neq 0\}.$$

R ist für $n \geq 2$ nicht kommutativ und besitzt in diesem Falle auch von Null verschiedene Nullteiler. Etwas allgemeiner können wir sagen, dass die Menge der Endomorphismen eines Vektorraumes V (oder auch einer abelschen Gruppe G) einen Ring bildet. Dabei ist die Addition von Endomorphismen mit Hilfe der Addition auf V bzw. G definiert, die Multiplikation als Komposition von Endomorphismen.

(4) Sei X eine Menge und R ein Ring. Dann ist R^X, die Menge der R-wertigen Funktionen auf X, ein Ring, wenn man für $f, g \in R^X$ setzt:

$$\begin{aligned} f + g\colon X &\longrightarrow R, \qquad x \longmapsto f(x) + g(x),\\ f \cdot g\colon X &\longrightarrow R, \qquad x \longmapsto f(x) \cdot g(x). \end{aligned}$$

Gilt speziell $X = \{1, \ldots, n\} \subset \mathbb{N}$, so ist R^X mit dem n-fachen kartesischen Produkt $R^n = R \times \ldots \times R$ zu identifizieren, wobei die Ringstruktur von R^n durch die Formeln

$$(*) \qquad \begin{aligned} (x_1, \ldots, x_n) + (y_1, \ldots, y_n) &= (x_1 + y_1, \ldots, x_n + y_n),\\ (x_1, \ldots, x_n) \cdot (y_1, \ldots, y_n) &= (x_1 \cdot y_1, \ldots, x_n \cdot y_n) \end{aligned}$$

beschrieben wird. Null- bzw. Einselement werden gegeben durch die Elemente $0 = (0, \ldots, 0)$ bzw. $1 = (1, \ldots, 1)$. Weiter zeigt die Gleichung $(1, 0, \ldots, 0) \cdot (0, 1, \ldots, 1) = 0$, dass R^n für $n \geq 2$ in der Regel nicht-triviale Nullteiler besitzt, auch wenn R selbst ein Integritätsring ist. Man nennt R^n das n-fache *ringtheoretische Produkt* von R mit sich selbst. Allgemeiner kann das ringtheoretische Produkt

$$P = \prod_{x\in X} R_x$$

einer Familie von Ringen $(R_x)_{x\in X}$ gebildet werden. Addition und Multiplikation auf P werden analog zu den Formeln $(*)$ komponentenweise definiert. Sind die R_x Exemplare ein und desselben Rings R, so stimmen die Ringe $\prod_{x\in X} R_x$ und R^X in natürlicher Weise überein.

Von nun an wollen wir uns auf kommutative Ringe beschränken. Wir werden daher unter einem *Ring*, wenn nichts anderes gesagt ist, stets einen *kommutativen Ring* verstehen. Sei im Folgenden R ein solcher Ring. Als wichtiges Beispiel einer Ringerweiterung von R wollen wir den *Polynomring* $R[X]$ aller Polynome einer Variablen X über R erklären. Wir setzen $R[X] := R^{(\mathbb{N})}$, wobei diese Gleichung zunächst nur im Sinne von Mengen gemeint ist; $R^{(\mathbb{N})}$ bezeichne wie gewohnt die Menge aller Abbildungen $f : \mathbb{N} \longrightarrow R$, für die $f(i) = 0$ für fast alle $i \in \mathbb{N}$ gilt. Indem wir eine Abbildung $f : \mathbb{N} \longrightarrow R$ mit der zugehörigen Folge $(f(i))_{i\in\mathbb{N}}$ der Bilder in R identifizieren, können wir

$$R^{(\mathbb{N})} = \left\{(a_i)_{i\in\mathbb{N}}\,;\ a_i \in R,\ a_i = 0 \text{ für fast alle } i \in \mathbb{N}\right\}$$

schreiben. Um eine Ringstruktur auf $R^{(\mathbb{N})}$ zu erhalten, definieren wir die Addition wie im obigen Beispiel (4) als komponentenweise Addition bzw. als übliche Addition von Abbildungen unter Benutzung der Addition auf R, d. h.

$$(a_i)_{i\in\mathbb{N}} + (b_i)_{i\in\mathbb{N}} := (a_i + b_i)_{i\in\mathbb{N}}.$$

Im Gegensatz hierzu wird die Multiplikation nicht komponentenweise erklärt; wir verwenden eine Konstruktion, wie sie auch der Multiplikation polynomialer Funktionen zugrunde liegt:

$$(a_i)_{i\in\mathbb{N}} \cdot (b_i)_{i\in\mathbb{N}} := (c_i)_{i\in\mathbb{N}}$$

mit

$$c_i := \sum_{\mu+\nu=i} a_\mu b_\nu.$$

Man kann nun nachprüfen, dass $R^{(\mathbb{N})}$ unter den genannten Verknüpfungen einen Ring bildet; das Nullelement wird gegeben durch die Folge $(0, 0, 0, \ldots)$, das Einselement durch die Folge $(1, 0, 0, \ldots)$. Den so gewonnenen Ring bezeichnet man mit $R[X]$ und nennt ihn den *Ring der Polynome in einer Variablen X über R*. Es enthält $R[X]$ in natürlicher Weise den Ring R als Unterring, wenn wir R mit seinem Bild unter der Abbildung

$R \hookrightarrow R[X]$, $a \longmapsto (a, 0, 0, \ldots)$ identifizieren. Dies ist erlaubt, da diese injektive Abbildung die Ringstrukturen auf R und $R[X]$ respektiert, also ein Homomorphismus ist, wie wir sagen werden.

Etwas plausibler wird die Bezeichnung von $R[X]$ als *Polynomring*, wenn man für Elemente in $R[X]$ die übliche Polynomschreibweise verwendet; man schreibt Elemente $(a_i)_{i\in\mathbb{N}} \in R[X]$ nämlich in der Form

$$\sum_{i\in\mathbb{N}} a_i X^i \qquad \text{oder} \qquad \sum_{i=0}^{n} a_i X^i,$$

wobei n so groß gewählt ist, dass $a_i = 0$ für $i > n$ gilt. Die "Variable" X, deren Bedeutung wir sogleich noch genauer erklären werden, ist dabei zu interpretieren als die Folge $(0, 1, 0, 0, \ldots)$. Insbesondere ist X^0 das Einselement in $R[X]$, stimmt also überein mit der Folge $(1, 0, 0, \ldots)$. Multiplikation eines Elements $(a_0, a_1, a_2, \ldots) \in R[X]$ mit der Variablen X bewirkt eine Verschiebung der Komponenten a_i um einen Schritt nach rechts (unter Einfügen von "0" links), also $X \cdot (a_0, a_1, a_2, \ldots) = (0, a_0, a_1, a_2, \ldots)$. Folglich ist X^i für einen Exponent $i \geq 0$ tatsächlich aufzufassen als i-te Potenz $(0, \ldots, 0, 1, 0, \ldots)$ der Variablen X, wobei ausgehend vom Einselement $(1, 0, 0, \ldots)$ die "1" um i Schritte nach rechts verschoben wird. In der Polynomschreibweise werden daher Addition und Multiplikation in $R[X]$ wie gewohnt gegeben durch die Formeln

$$\sum_i a_i X^i + \sum_i b_i X^i = \sum_i (a_i + b_i) X^i,$$
$$\sum_i a_i X^i \cdot \sum_i b_i X^i = \sum_i \Big(\sum_{\mu+\nu=i} a_\mu \cdot b_\nu \Big) X^i.$$

Ist nun $R \subset R'$ eine Ringerweiterung und $f = \sum a_i X^i$ ein Polynom in $R[X]$, so kann man beliebige Elemente $x \in R'$ für die "Variable" X einsetzen und somit den Wert $f(x) = \sum a_i x^i$ von f in x berechnen. Es gibt f also Anlass zu einer wohldefinierten Abbildung $R' \longrightarrow R'$, $x \longmapsto f(x)$, wobei für zwei Polynome $f, g \in R[X]$ stets

$$(f + g)(x) = f(x) + g(x), \qquad (f \cdot g)(x) = f(x) \cdot g(x)$$

gilt. Man bemerke dabei, dass für die rechte Gleichung die Kommutativität der Multiplikation in R' benutzt wird bzw., was ausreicht, die Vertauschbarkeitsrelation $ax = xa$ für $a \in R, x \in R'$. Wir rechnen daher im Polynomring

$R[X]$ mit der "Variablen" X sozusagen wie mit einer universell variierbaren Größe, wobei Gleichungen in $R[X]$ wiederum in Gleichungen übergehen, wenn man für X Einsetzungen im gerade beschriebenen Sinne vornimmt.

Für ein Polynom $f = \sum a_i X^i \in R[X]$ bezeichnet man den i-ten Koeffizienten a_i jeweils als den *Koeffizienten vom Grad i* von f. Weiter definiert man den *Grad* von f durch

$$\operatorname{grad} f := \max\{i\,;\, a_i \neq 0\},$$

mit der Besonderheit, dass dem Nullpolynom 0 der Grad $-\infty$ zugeordnet wird. Gilt ansonsten $\operatorname{grad} f = n \geq 0$, so heißt a_n der höchste Koeffizient oder der Leitkoeffizient von f. Ist dieser 1, so sagt man, f sei *normiert*. Jedes Polynom f in $R[X]-\{0\}$, dessen höchster Koeffizient a_n eine Einheit ist, lässt sich durch Multiplikation mit a_n^{-1} normieren.

Bemerkung 2. *Es sei $R[X]$ der Polynomring einer Variablen X über einem Ring R. Für Polynome $f, g \in R[X]$ gilt dann*

$$\operatorname{grad}(f+g) \leq \max(\operatorname{grad} f, \operatorname{grad} g)$$
$$\operatorname{grad}(f \cdot g) \leq \operatorname{grad} f + \operatorname{grad} g,$$

wobei man sogar $\operatorname{grad}(f \cdot g) = \operatorname{grad} f + \operatorname{grad} g$ *hat, sofern R ein Integritätsring ist.*

Beweis. Die Behauptung ist klar, falls f oder g das Nullpolynom ist. Wir dürfen daher $m = \operatorname{grad} f \geq 0$ sowie $n = \operatorname{grad} g \geq 0$ annehmen, etwa $f = \sum a_i X^i$, $g = \sum b_i X^i$. Dann folgt $a_i + b_i = 0$ für $i > \max(m,n)$, also $\operatorname{grad}(f+g) \leq \max(m,n)$. In ähnlicher Weise ergibt sich $\sum_{\mu+\nu=i} a_\mu b_\nu = 0$ für $i > m+n$ und somit $\operatorname{grad}(f \cdot g) \leq m+n$. Ist jedoch R ein Integritätsring, so schließt man aus $\operatorname{grad} f = m$, $\operatorname{grad} g = n$, dass die Koeffizienten a_m, b_n nicht verschwinden und somit, dass $\sum_{\mu+\nu=m+n} a_\mu b_\nu = a_m b_n$ als Koeffizient vom Grad $m+n$ in $f \cdot g$ nicht verschwindet. Folglich gilt $\operatorname{grad}(f \cdot g) = m+n$. □

Es gibt eine ganze Reihe von Eigenschaften, die sich von einem Ring R auf den Polynomring $R[X]$ vererben. Als einfaches Beispiel behandeln wir die Nullteilerfreiheit.

Bemerkung 3. *Es sei R ein Integritätsring. Dann ist auch der Polynomring $R[X]$ ein Integritätsring. Weiter gilt $(R[X])^* = R^*$.*

Beweis. Man benutze die Formel $\operatorname{grad}(f \cdot g) = \operatorname{grad} f + \operatorname{grad} g$ aus Bemerkung 2. □

Wir wollen schließlich noch zeigen, dass in Polynomringen eine *Division mit Rest* möglich ist, ähnlich wie im Ring $\mathbb{Z}$ der ganzen Zahlen. Dieses Hilfsmittel wird in 2.4 benutzt, um zu zeigen, dass in Polynomringen über Körpern der Satz von der eindeutigen Primfaktorzerlegung gilt.

Satz 4. *Es sei R ein Ring und $g = \sum_{i=0}^{d} a_i X^i \in R[X]$ ein Polynom, dessen höchster Koeffizient a_d eine Einheit in R ist. Dann gibt es zu jedem $f \in R[X]$ eindeutig bestimmte Polynome $q, r \in R[X]$ mit*

$$f = qg + r, \qquad \operatorname{grad} r < d.$$

Beweis. Wir bemerken zunächst, dass stets $\operatorname{grad}(qg) = \operatorname{grad} q + \operatorname{grad} g$ für Polynome $q \in R[X]$ gilt, auch wenn R kein Integritätsring ist. Der höchste Koeffizient a_d von g ist nämlich eine Einheit. Ist daher q vom Grad $n \geq 0$ mit höchstem Koeffizienten c_n, so gilt $c_n a_d \neq 0$. Dies ist aber der höchste Koeffizient von qg, so dass $\operatorname{grad}(qg) = n + d$ folgt.

Nun zur Eindeutigkeit der Division mit Rest. Hat f zwei Darstellungen der gewünschten Art, etwa $f = qg+r = q'g+r'$, so folgt $0 = (q-q')g+(r-r')$ sowie nach vorstehender Überlegung

$$\operatorname{grad}(q - q') + \operatorname{grad} g = \operatorname{grad}(r - r').$$

Da r und r' vom Grad $< d$ sind, gilt dasselbe auch für $r - r'$, und man erhält $\operatorname{grad}(q - q') + \operatorname{grad} g < d$. Dies kann aber wegen $\operatorname{grad} g = d$ nur für $q = q'$ richtig sein. Hieraus ergibt sich insbesondere $r = r'$ und somit die Eindeutigkeit der Division mit Rest.

Um die Existenz der Division mit Rest zu zeigen, schließen wir mit Induktion nach $n = \operatorname{grad} f$. Für $\operatorname{grad} f < d$ setze man $q = 0$ und $r = f$. Gilt andererseits $f = \sum_{i=0}^{n} c_i X^i$ mit $c_n \neq 0$ und $n \geq d$, so ist

$$f_1 = f - c_n a_d^{-1} X^{n-d} g$$

ein Polynom mit $\operatorname{grad} f_1 < n$. Dieses besitzt nach Induktionsvoraussetzung eine Zerlegung $f_1 = q_1 g + r_1$ mit Polynomen $q_1, r_1 \in R[X]$, $\operatorname{grad} r_1 < d$. Dann folgt aber mit

$$f = (q_1 + c_n a_d^{-1} X^{n-d})g + r_1$$

die gewünschte Zerlegung für f. □

Die gerade gegebene Argumentation kann insbesondere als konstruktives Verfahren benutzt werden, um die Division mit Rest im Polynomring $R[X]$ in expliziter Weise durchzuführen, ähnlich wie dies auch im Ring $\mathbb{Z}$ der ganzen Zahlen geschieht. Als Beispiel betrachte man die Polynome

$$f = X^5 + 3X^4 + X^3 - 6X^2 - X + 1, \qquad g = X^3 + 2X^2 + X - 1$$

aus $\mathbb{Z}[X]$:

$$\begin{array}{l}
(X^5 +3X^4 + X^3 -6X^2 - X +1) : (X^3 + 2X^2 + X - 1) = X^2 + X - 2 \\
\underline{X^5 +2X^4 + X^3 - X^2} \\
\quad X^4 \quad -5X^2 - X \\
\quad \underline{X^4 +2X^3 + X^2 - X} \\
\quad -2X^3 -6X^2 \quad +1 \\
\quad \underline{-2X^3 -4X^2 -2X +2} \\
\quad -2X^2 +2X -1
\end{array}$$

Im ersten Schritt subtrahieren wir $X^2 g$ von f, im zweiten dann Xg von $f - X^2 g$ und im dritten $-2g$ von $f - X^2 g - Xg$. Es bleibt $-2X^2 + 2X - 1$ als Rest, so dass wir die Gleichung

$$f = (X^2 + X - 2)g + (-2X^2 + 2X - 1)$$

erhalten.

Abschließend sei angemerkt, dass man die Konstruktion des Polynomrings $R[X]$ in verschiedener Hinsicht verallgemeinern kann. So werden wir beispielsweise in 2.5 Polynomringe in mehreren Variablen definieren. Man kann aber auch von Beginn an die Menge $R^{(\mathbb{N})}$ durch $R^{\mathbb{N}}$ ersetzen, also durch die Menge *aller* Abbildungen von $\mathbb{N}$ nach R. Verfährt man ansonsten wie bei der Konstruktion des Polynomrings $R[X]$, so erhält man den Ring $R[\![X]\!]$ der *formalen Potenzreihen* in einer Variablen X über R. Seine Elemente lassen sich als *unendliche* Reihen $\sum_{i=0}^{\infty} a_i X^i$ darstellen.

Lernkontrolle und Prüfungsvorbereitung

1. Was versteht man unter einem Ring (mit Eins), was ist ein Unterring eines solchen Rings? Wie ist die Einheitengruppe eines Rings definiert? Was ist ein Integritätsring, was ist ein Körper?
2. Gib einige einfache Beispiele von Ringen und bestimme jeweils die zugehörige Einheitengruppe. Welche dieser Ringe sind Integritätsringe bzw. Körper?
3. Erkläre die Konstruktion des Polynomrings $R[X]$ in einer Variablen X über einem (kommutativen) Ring R.

$^{+}$4. Wie ist der Ring der formalen Potenzreihen $R[\![X]\!]$ in einer Variablen X über einem (kommutativen) Ring R erklärt?

5. Was versteht man unter dem Grad eines Polynoms, und wie verhält sich dieser unter der Addition bzw. Multiplikation von Polynomen? Was ist ein normiertes Polynom?
6. Welche speziellen Eigenschaften besitzt die Gradfunktion im Polynomring $R[X]$ über einem Integritätsring R?
7. Sei R ein Integritätsring. Zeige, dass dann auch der Polynomring $R[X]$ ein Integritätsring ist und bestimme die Einheitengruppe $(R[X])^*$.
8. Erläutere das Verfahren der Division mit Rest in Polynomringen.

Übungsaufgaben

1. *Verifiziere, dass für Elemente a, b eines Ringes R stets die Relationen $0 \cdot a = 0$ und $(-a) \cdot b = -(a \cdot b)$ gelten.*
2. *Wir haben den Polynomring $R[X]$ nur für einen kommutativen Ring R definiert. Überlege, inwieweit es sinnvoll ist, Polynomringe auch im Rahmen nicht notwendig kommutativer Ringe zu betrachten.*
3. Führe die in Satz 4 beschriebene Division mit Rest im Polynomring $\mathbb{Z}[X]$ in folgenden Fällen explizit durch:
   (i) $f = 3X^5 + 2X^4 - X^3 + 3X^2 - 4X + 7, \quad g = X^2 - 2X + 1.$
   (ii) $f = X^5 + X^4 - 5X^3 + 2X^2 + 2X - 1, \quad g = X^2 - 1.$
4. Sei K ein Körper und $g \in K[X]$ ein Polynom einer Variablen vom Grad $d > 0$. Beweise die Existenz der sogenannten *g-adischen Entwicklung*: Zu $f \in K[X]$ gibt es eindeutig bestimmte Polynome $a_0, a_1, \ldots \in K[X]$ vom Grad $< d$, $a_i = 0$ für fast alle i, mit $f = \sum_i a_i g^i$.

5. Es sei R ein Ring, der ein *nilpotentes* Element $a \neq 0$ enthalte; nilpotent bedeutet, dass es ein $n \in \mathbb{N}$ mit $a^n = 0$ gibt. Zeige, dass die Einheitengruppe R^* eine echte Untergruppe der Einheitengruppe $(R[X])^*$ ist.
6. Bestimme den kleinsten Unterring von $\mathbb{R}$, welcher $\mathbb{Q}$ und $\sqrt{2}$ enthält, und zeige, dass dieser bereits ein Körper ist.
7. Zeige, dass eine formale Potenzreihe $\sum a_i X^i \in R[\![X]\!]$ über einem Ring R genau dann eine Einheit ist, wenn a_0 eine Einheit in R ist.
8. Beweise, dass die Quaternionen $\mathbb{H}$ aus Beispiel (2) einen Schiefkörper bilden.

2.2 Ideale

Ideale sind für Ringe von ähnlich fundamentaler Bedeutung wie Normalteiler für Gruppen. Ein Normalteiler einer Gruppe ist zugleich auch eine Untergruppe. Dagegen ist ein Ideal eines Ringes im Allgemeinen kein Unterring, denn Ideale enthalten nicht das Einselement der Multiplikation, abgesehen von trivialen Fällen.

Definition 1. *Es sei R ein Ring. Eine Teilmenge $\mathfrak{a} \subset R$ heißt ein* Ideal *in R, wenn gilt*:

(i) $\mathfrak{a}$ *ist eine additive Untergruppe von R.*
(ii) $r \in R, a \in \mathfrak{a} \Longrightarrow ra \in \mathfrak{a}$.

Jeder Ring R enthält stets die sogenannten *trivialen* Ideale, nämlich das *Nullideal* $\{0\}$, auch mit 0 bezeichnet, und das *Einheitsideal* R. Ist R ein Körper, so sind dies die einzigen Ideale in R. Ausgehend von beliebigen Idealen $\mathfrak{a}, \mathfrak{b} \subset R$ kann man die folgenden Ideale bilden:

$$\begin{aligned}
\mathfrak{a} + \mathfrak{b} &:= \{a + b \,;\, a \in \mathfrak{a},\ b \in \mathfrak{b}\},\\
\mathfrak{a} \cdot \mathfrak{b} &:= \left\{ \sum_{i=1}^{<\infty} a_i b_i \,;\, a_i \in \mathfrak{a},\ b_i \in \mathfrak{b} \right\},\\
\mathfrak{a} \cap \mathfrak{b} &:= \{x \,;\, x \in \mathfrak{a} \text{ und } x \in \mathfrak{b}\}.
\end{aligned}$$

Es gilt stets $\mathfrak{a}\cdot\mathfrak{b} \subset \mathfrak{a}\cap\mathfrak{b}$. Im Übrigen kann man in analoger Weise das Produkt von endlich vielen Idealen sowie Summe und Durchschnitt beliebig vieler Ideale bilden. Dabei besteht die Summe $\sum \mathfrak{a}_i$ einer Familie von Idealen

$(\mathfrak{a}_i)_{i\in I}$ aus allen Elementen der Form $\sum a_i$ mit $a_i \in \mathfrak{a}_i$, wobei $a_i = 0$ für fast alle $i \in I$. Für $a \in R$ nennt man $Ra := \{ra\,;\, r \in R\}$ das *von a erzeugte Hauptideal*. Allgemeiner erklärt man für $a_1, \ldots, a_n \in R$ das von diesen Elementen *erzeugte Ideal* in R durch

$$(a_1, \ldots, a_n) := Ra_1 + \ldots + Ra_n = \{r_1a_1 + \ldots + r_na_n\,;\, r_1, \ldots, r_n \in R\}.$$

Es ist dies das kleinste Ideal in R, welches $a_1, \ldots, a_n$ enthält, und zwar in dem Sinne, dass jedes weitere Ideal in R, welches die Elemente $a_1, \ldots, a_n$ enthält, auch das Ideal $(a_1, \ldots, a_n)$ enthält. In analoger Weise kann man das von einer beliebigen Familie $(a_i)_{i\in I}$ von Elementen aus R erzeugte Ideal in R betrachten, nämlich das Ideal $\sum_{i\in I} Ra_i$.

Definition 2. *Es sei $\mathfrak{a}$ ein Ideal eines Ringes R. Eine Familie $(a_i)_{i\in I}$ von Elementen aus $\mathfrak{a}$ wird als* Erzeugendensystem *von $\mathfrak{a}$ bezeichnet, wenn $\mathfrak{a} = \sum_{i\in I} Ra_i$ gilt, wenn also $\mathfrak{a}$ mit dem von der Familie $(a_i)_{i\in I}$ erzeugten Ideal übereinstimmt. Man nennt $\mathfrak{a}$* endlich erzeugt, *wenn $\mathfrak{a}$ ein endliches Erzeugendensystem besitzt. Weiter heißt $\mathfrak{a}$* Hauptideal, *wenn $\mathfrak{a}$ von einem einzigen Element erzeugt wird, wenn es also ein $a \in \mathfrak{a}$ mit $\mathfrak{a} = (a)$ gibt. Ist R Integritätsring und ist jedes Ideal in R Hauptideal, so nennt man R einen* Hauptidealring.

Die trivialen Ideale eines Ringes sind stets Hauptideale. Im Übrigen bilden die Untergruppen der Form $m\mathbb{Z} \subset \mathbb{Z}$ Hauptideale im Integritätsring $\mathbb{Z}$. Da dies gemäß 1.3/4 die einzigen Untergruppen von $\mathbb{Z}$ sind, kann es auch keine weiteren Ideale in $\mathbb{Z}$ geben. Insbesondere folgt:

Satz 3. *$\mathbb{Z}$ ist ein Hauptidealring.*

Erzeugende Elemente von Hauptidealen sind nicht eindeutig bestimmt; man kann sie zumindest durch Einheiten abändern. In Integritätsringen erhält man auf diese Weise aber bereits alle möglichen Erzeugenden eines Hauptideals:

Bemerkung 4. *Zwei Hauptideale $\mathfrak{a} = (a)$, $\mathfrak{b} = (b)$ in einem Integritätsring R stimmen genau dann überein, wenn es eine Einheit $c \in R^*$ mit $b = ca$ gibt.*

Beweis. Es gelte $\mathfrak{a} = \mathfrak{b}$, wobei wir ohne Einschränkung $\mathfrak{a} = \mathfrak{b} \neq 0$ annehmen dürfen. Dann hat man $b \in \mathfrak{a}$, also gibt es ein $c \in R$ mit $b = ca$. Ebenso gibt es wegen $a \in \mathfrak{b}$ ein $c' \in R$ mit $a = c'b$. Damit folgt $b = ca = cc'b$, bzw.

$$(1 - cc')b = 0.$$

Da nun R Integritätsring ist und b wegen $\mathfrak{b} \neq 0$ von Null verschieden sein muss, folgt $cc' = 1$, d. h. c ist eine Einheit. Die umgekehrte Implikation ist trivial. □

Wir nennen zwei Elemente a, b eines Ringes R (zueinander) *assoziiert*, wenn es eine Einheit $c \in R^*$ mit $b = ca$ gibt. Somit können wir sagen, dass in einem Integritätsring zwei Elemente genau dann dasselbe Hauptideal erzeugen, wenn sie assoziiert sind. In allgemeineren Ringen gilt diese Aussage nicht mehr, man vergleiche hierzu Aufgabe 7 in Abschnitt 2.3.

Wir wollen schließlich noch als Beispiel den Polynomring $\mathbb{Z}[X]$ betrachten. Das von X erzeugte Hauptideal beschreibt sich durch

$$(X) = \left\{ \sum a_i X^i \in \mathbb{Z}[X] \; ; \; a_0 = 0 \right\},$$

das von 2 erzeugte Hauptideal durch

$$(2) = \left\{ \sum a_i X^i \in \mathbb{Z}[X] \; ; \; a_i \text{ ist gerade für alle } i \right\}.$$

Da es in $\mathbb{Z}[X]$ keine Nichteinheit gibt, welche sowohl 2 als auch X als Vielfaches besitzt, kann man leicht sehen, dass

$$(2, X) = \left\{ \sum a_i X^i \in \mathbb{Z}[X] \; ; \; a_0 \text{ ist gerade} \right\}$$

ein Ideal in $\mathbb{Z}[X]$ ist, welches kein Hauptideal darstellt. Insbesondere ist $\mathbb{Z}[X]$ kein Hauptidealring.

Lernkontrolle und Prüfungsvorbereitung

1. Wie lautet die Definition eines Ideals in einem Ring? Was versteht man unter den trivialen Idealen? Gib einige weitere Beispiele für Ideale.
2. Welche Möglichkeiten gibt es, aus gegebenen Idealen eines Rings neue zu bilden?

3. Was ist ein Hauptideal, was ist ein Hauptidealring?
4. Welche Ideale gibt es im Ring $\mathbb{Z}$ der ganzen Zahlen?
5. Erkläre den Begriff der Assoziiertheit von Elementen eines Rings. Zeige, dass erzeugende Elemente eines Hauptideals in Integritätsringen bis auf Assoziiertheit eindeutig bestimmt sind.
6. Zeige, dass der Polynomring $\mathbb{Z}[X]$ kein Hauptidealring ist.

Übungsaufgaben

1. *Es seien* $\mathfrak{a} = (a_1, \ldots, a_m)$ *und* $\mathfrak{b} = (b_1, \ldots, b_n)$ *Ideale in einem Ring* R. *Gib Erzeugendensysteme für die Ideale* $\mathfrak{a} + \mathfrak{b}$ *sowie* $\mathfrak{a} \cdot \mathfrak{b}$ *an und diskutiere auch das Ideal* $\mathfrak{a} \cap \mathfrak{b}$.
2. *Überlege, unter welchen Bedingungen die Vereinigung zweier Ideale oder allgemeiner einer Familie von Idealen eines Ringes* R *wieder ein Ideal ist.*
3. *Es sei* K *ein Körper. Betrachte* $K^2 = K \times K$ *als ringtheoretisches Produkt sowie auch als* K*-Vektorraum. Vergleiche die Begriffe Unterring, Ideal und Untervektorraum am Beispiel dieses Ringes.*
4. Betrachte folgende Ideale in $\mathbb{Z}$ und gib jeweils ein erzeugendes Element an:

$$(2) + (3), \qquad (4) + (6), \qquad (2) \cap (3), \qquad (4) \cap (6).$$

5. Sei R ein Ring, X eine Menge und $Y \subset X$ eine Teilmenge. Untersuche, welche der folgenden Teilmengen des Rings R^X der Abbildungen $X \longrightarrow R$ einen Unterring bzw. ein Ideal bilden:

$$\begin{aligned} M_1 &= \{f \in R^X \,;\, f \text{ ist konstant auf } Y\}, \\ M_2 &= \{f \in R^X \,;\, f(Y) = 0\}, \\ M_3 &= \{f \in R^X \,;\, f(y) \neq 0 \text{ für alle } y \in Y\}, \\ M_4 &= \{f \in R^X \,;\, f(y) = 0 \text{ für fast alle } y \in Y\}. \end{aligned}$$

   In welchen Fällen ergeben sich unter geeigneten Bedingungen an Y Hauptideale?
6. Sei R ein Ring. Zeige, dass die Teilmenge

$$\{a \in R \,;\, \text{es existiert ein } n \in \mathbb{N} \text{ mit } a^n = 0\}$$

   ein Ideal in R definiert (das sogenannte *Radikal* oder *Nilradikal* von R).
7. Es sei K ein Körper. Bestimme alle Ideale im Ring der formalen Potenzreihen $K[\![X]\!]$. (Benutze Aufgabe 7 aus Abschnitt 2.1.)

2.3 Ringhomomorphismen, Faktorringe

Der Begriff des Homomorphismus wird in natürlicher Weise auch für Ringe erklärt.

Definition 1. *Es seien R und R' Ringe. Eine Abbildung $\varphi\colon R \longrightarrow R'$ heißt* Ringhomomorphismus, *wenn gilt*:

(i) $\varphi(a+b) = \varphi(a) + \varphi(b)$ *für alle $a, b \in R$, d. h. φ ist ein Gruppenhomomorphismus bezüglich der Addition.*

(ii) $\varphi(a \cdot b) = \varphi(a) \cdot \varphi(b)$ *für alle $a, b \in R$ und $\varphi(1) = 1$, d. h. φ ist ein Monoidhomomorphismus bezüglich der Multiplikation.*

Man verifiziert ohne Schwierigkeiten, dass die Komposition zweier Ringhomomorphismen wieder ein Ringhomomorphismus ist. Wie üblich heißt ein Ringhomomorphismus $\varphi\colon R \longrightarrow R'$ ein *Isomorphismus*, wenn φ ein Inverses besitzt, d. h. wenn es einen Ringhomomorphismus $\psi\colon R' \longrightarrow R$ mit $\psi \circ \varphi = \mathrm{id}_R$ und $\varphi \circ \psi = \mathrm{id}_{R'}$ gibt. Äquivalent hierzu ist, dass der Homomorphismus φ bijektiv ist. Injektive (bzw. surjektive) Ringhomomorphismen $R \longrightarrow R'$ nennt man auch *Monomorphismen* (bzw. *Epimorphismen*). Ein *Endomorphismus* von R ist ein Homomorphismus $R \longrightarrow R$ und ein *Automorphismus* von R ein Isomorphismus $R \xrightarrow{\sim} R$.

Bemerkung 2. *Es sei $\varphi\colon R \longrightarrow R'$ ein Ringhomomorphismus. Dann gilt*:

(i) $\ker \varphi = \{a \in R\,;\, \varphi(a) = 0\}$ *ist ein Ideal in R.*

(ii) $\operatorname{im} \varphi = \varphi(R)$ *ist ein Unterring von R'.*

(iii) *φ induziert einen Gruppenhomomorphismus $R^* \longrightarrow R'^*$ zwischen den Einheitengruppen von R und R'.*

Die Behauptungen sind unmittelbar nachzuprüfen. Man beachte dabei, dass das Bild eines Ringhomomorphismus $\varphi\colon R \longrightarrow R'$ im Allgemeinen kein Ideal in R' ergibt. Handelt es sich bei R und R' um Körper, so spricht man auch von *Körperhomomorphismen*.

Bemerkung 3. *Es sei K ein Körper und R ein Ring, $R \neq 0$. Dann ist jeder Homomorphismus $\varphi\colon K \longrightarrow R$ injektiv. Insbesondere ist jeder Homomorphismus zwischen Körpern injektiv.*

Beweis. Es ist $\ker\varphi$ ein Ideal in K, sogar ein echtes Ideal, denn es gilt $\varphi(1) = 1 \neq 0$. Somit folgt $\ker\varphi = 0$, da ein Körper außer dem Nullideal keine weiteren echten Ideale besitzt. □

Zu jedem Ring R existiert ein Ringhomomorphismus $\mathbb{Z} \longrightarrow R$, der zudem eindeutig bestimmt ist, nämlich als Abbildung, die durch $n \longmapsto n \cdot 1$ gegeben ist. Dabei ist $n \cdot 1$ für $n \geq 0$ als n-fache Summe des Einselementes $1 \in R$ aufzufassen und entsprechend für $n < 0$ als $(-n)$-fache Summe von -1. Für eine Ringerweiterung $R \subset R'$ ist die Inklusionsabbildung $R \hookrightarrow R'$ ein (triviales) Beispiel eines Ringhomomorphismus. Weiter hat man in dieser Situation zu jedem $x \in R'$ einen sogenannten *Einsetzungshomomorphismus*

$$R[X] \longrightarrow R', \qquad f = \sum a_i X^i \longmapsto f(x) = \sum a_i x^i,$$

der ein Ringhomomorphismus ist. Das Einsetzen von Elementen $x \in R'$ in Polynome $f, g \in R[X]$ hatten wir schon in 2.1 besprochen, ebenso die Verträglichkeiten

$$(f+g)(x) = f(x) + g(x), \qquad (f \cdot g)(x) = f(x) \cdot g(x),$$

die für einen Ringhomomorphismus gefordert werden.

Es sei im Folgenden R ein Ring und $\mathfrak{a}$ ein Ideal in R. Wir wollen die Konstruktion der Faktorgruppe G/N einer Gruppe G nach einem Normalteiler N auf die Ringsituation übertragen und einen sogenannten *Faktor-* oder *Restklassenring* $R/\mathfrak{a}$ konstruieren, zusammen mit einem surjektiven Ringhomomorphismus $\pi\colon R \longrightarrow R/\mathfrak{a}$, welcher $\ker\pi = \mathfrak{a}$ erfüllt. Zunächst können wir $R/\mathfrak{a}$ als abelsche Gruppe bilden, indem wir $\mathfrak{a}$ als Untergruppe (und damit als Normalteiler) der additiven Gruppe von R auffassen. Es besteht $R/\mathfrak{a}$ somit aus allen Restklassen der Form $x + \mathfrak{a}$ mit $x \in R$, wobei die Addition in $R/\mathfrak{a}$ durch die Formel

$$(x + \mathfrak{a}) + (y + \mathfrak{a}) = (x + y) + \mathfrak{a}$$

beschrieben wird. Dass diese Verknüpfung wohldefiniert ist und $R/\mathfrak{a}$ zu einer abelschen Gruppe macht, haben wir in 1.2 nachgewiesen. Wir führen nun in analoger Weise eine Multiplikation in $R/\mathfrak{a}$ ein, indem wir für Restklassen $x + \mathfrak{a}$, $y + \mathfrak{a}$ aus $R/\mathfrak{a}$ definieren:

$$(x + \mathfrak{a}) \cdot (y + \mathfrak{a}) := (x \cdot y) + \mathfrak{a}.$$

Um die Wohldefiniertheit dieser Verknüpfung zu überprüfen, zeigen wir, dass die Restklasse $(x \cdot y) + \mathfrak{a}$ nicht von der Wahl der Repräsentanten x, y zu den Restklassen $x+\mathfrak{a}$ und $y+\mathfrak{a}$ abhängt. Hierzu nehmen wir $x'+\mathfrak{a} = x+\mathfrak{a}$ an, also $x' = x + a$ mit $a \in \mathfrak{a}$, und entsprechend $y' + \mathfrak{a} = y + \mathfrak{a}$, also $y' = y + b$ mit $b \in \mathfrak{a}$. Dann ergibt sich $x'y' = xy + ay' + xb \in (xy) + \mathfrak{a}$, d. h.

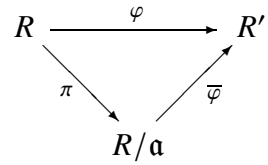
$$(xy) + \mathfrak{a} = (x'y') + \mathfrak{a}.$$

Folglich ist die Multiplikation in $R/\mathfrak{a}$ wohldefiniert, und es ist unmittelbar ersichtlich, dass die Ringeigenschaften sich von R auf $R/\mathfrak{a}$ übertragen. Im Übrigen ist die kanonische Projektion

$$\pi\colon R \longrightarrow R/\mathfrak{a}, \qquad x \longmapsto x + \mathfrak{a},$$

ein Ringhomomorphismus mit $\ker \pi = \mathfrak{a}$, der wie in 1.2/6 eine universelle Eigenschaft erfüllt:

Satz 4 (Homomorphiesatz). *Sei $\varphi\colon R \longrightarrow R'$ ein Ringhomomorphismus und $\mathfrak{a} \subset R$ ein Ideal mit $\mathfrak{a} \subset \ker \varphi$. Dann existiert eindeutig ein Ringhomomorphismus $\overline{\varphi}\colon R/\mathfrak{a} \longrightarrow R'$, so dass das Diagramm*



kommutiert. Es gilt

$$\operatorname{im} \overline{\varphi} = \operatorname{im} \varphi, \qquad \ker \overline{\varphi} = \pi(\ker \varphi), \qquad \ker \varphi = \pi^{-1}(\ker \overline{\varphi}).$$

Insbesondere ist $\overline{\varphi}$ genau dann injektiv, wenn $\mathfrak{a} = \ker \varphi$ gilt.

Korollar 5. *Ist $\varphi\colon R \longrightarrow R'$ ein surjektiver Ringhomomorphismus, so ist R' kanonisch isomorph zu $R/\ker \varphi$.*

Zum *Beweis von Satz* 4 wendet man 1.2/6 auf die additive Gruppe von R an. Sodann hat man nur noch nachzuprüfen, dass der nach 1.2/6 existierende Gruppenhomomorphismus $\overline{\varphi}\colon R/\mathfrak{a} \longrightarrow R'$ bereits ein Ringhomomorphismus ist. Da $\overline{\varphi}$ charakterisiert ist durch die Gleichung

$$\overline{\varphi}(x + \mathfrak{a}) = \varphi(x), \qquad x \in R,$$

ist dies unmittelbar klar. □

Im Übrigen lassen sich die Isomorphiesätze 1.2/8 und 1.2/9, welche wir in Abschnitt 1.2 aus dem Homomorphiesatz 1.2/6 gefolgert hatten, ohne Schwierigkeiten von der Gruppensituation auf die hier betrachtete Ringsituation übertragen bzw. aus dem gerade bewiesenen Homomorphiesatz für Ringe herleiten; man ersetze den Begriff des Normalteilers jeweils durch den Begriff des Ideals in einem Ring.

Als natürliche Beispiele für Restklassenringe können wir die Ringe $\mathbb{Z}/m\mathbb{Z}$ betrachten, die wir in 1.3 lediglich als abelsche Gruppen aufgefasst hatten. Setzen wir $m > 0$ voraus, so ist also $\mathbb{Z}/m\mathbb{Z}$ ein Ring mit m Elementen.

Satz 6. *Für $m \in \mathbb{Z}$, $m > 0$, ist äquivalent*:

(i) *m ist eine Primzahl.*
(ii) *$\mathbb{Z}/m\mathbb{Z}$ ist ein Integritätsring.*
(iii) *$\mathbb{Z}/m\mathbb{Z}$ ist ein Körper.*

Beweis. Wir bezeichnen mit $\overline{x} \in \mathbb{Z}/m\mathbb{Z}$ die zu einem Element $x \in \mathbb{Z}$ gehörige Restklasse modulo $m\mathbb{Z}$. Sei zunächst Bedingung (i) gegeben, also m eine Primzahl. Dann ist $m > 1$ und folglich $\mathbb{Z}/m\mathbb{Z}$ nicht der Nullring. Gilt nun $\overline{a} \cdot \overline{b} = 0$ für zwei Zahlen $a, b \in \mathbb{Z}$, so hat man $ab \in m\mathbb{Z}$, und man sieht, etwa unter Benutzung der Primfaktorzerlegungen für a, b bzw. ab, dass m ein Teiler von a oder b ist. Also ergibt sich $a \in m\mathbb{Z}$ oder $b \in m\mathbb{Z}$, d. h. $\overline{a} = 0$ oder $\overline{b} = 0$, und es ist $\mathbb{Z}/m\mathbb{Z}$ ein Integritätsring, wie in (ii) gefordert.

Weiter folgt aus (ii), dass für jedes $\overline{a} \in \mathbb{Z}/m\mathbb{Z} - \{0\}$ die Abbildung

$$\mathbb{Z}/m\mathbb{Z} \longrightarrow \mathbb{Z}/m\mathbb{Z}, \qquad \overline{x} \longmapsto \overline{a} \cdot \overline{x},$$

injektiv und somit wegen der Endlichkeit von $\mathbb{Z}/m\mathbb{Z}$ sogar bijektiv ist. Insbesondere ist das Einselement von $\mathbb{Z}/m\mathbb{Z}$ im Bild dieser Abbildung enthalten, so dass $\overline{a}$ jeweils ein inverses Element bezüglich der Multiplikation besitzt. Dies bedeutet aber, dass $\mathbb{Z}/m\mathbb{Z}$ ein Körper ist, wie in (iii) gefordert.

Sei schließlich $\mathbb{Z}/m\mathbb{Z}$ wie in (iii) als Körper oder allgemeiner als nullteilerfrei angenommen. Insbesondere folgt dann $\mathbb{Z}/m\mathbb{Z} \neq 0$ und somit $m > 1$. Um zu zeigen, dass m eine Primzahl ist, betrachte man einen Teiler $d \in \mathbb{N}$ von m mit einer Gleichung $m = da$. Es folgt $\overline{d} \cdot \overline{a} = 0$, und die Nullteilerfreiheit von $\mathbb{Z}/m\mathbb{Z}$ ergibt $\overline{d} = 0$ oder $\overline{a} = 0$. Im ersten Fall ist m ein Teiler

von d, d. h. $d = m$, und im zweiten Fall ist m ein Teiler von a, d. h. $a = m$ und somit $d = 1$. Also hat m höchstens sich selbst und 1 als Teiler und ist damit eine Primzahl. □

Für eine Primzahl p ist also $\mathbb{Z}/p\mathbb{Z}$ ein Körper mit p Elementen; man verwendet hierfür die Notation $\mathbb{F}_p$. Mit Teilbarkeitstheorie kann man allgemeiner zeigen, dass für ganze Zahlen $m > 1$ die Einheitengruppe $(\mathbb{Z}/m\mathbb{Z})^*$ aus allen Restklassen $\overline{a}$, $a \in \mathbb{Z}$, besteht, für die a teilerfremd zu m ist. Als Nächstes wollen wir die Aussage von Satz 6 in einen etwas allgemeineren Zusammenhang stellen.

Definition 7. *Es sei R ein Ring.*

(i) *Ein Ideal $\mathfrak{p} \subset R$ heißt* prim *oder* Primideal, *wenn $\mathfrak{p}$ von R verschieden ist und wenn für $a, b \in R$ mit $ab \in \mathfrak{p}$ stets $a \in \mathfrak{p}$ oder $b \in \mathfrak{p}$ folgt.*

(ii) *Ein Ideal $\mathfrak{m} \subset R$ heißt* maximal, *wenn $\mathfrak{m}$ von R verschieden ist und wenn gilt: Ist $\mathfrak{a} \subset R$ ein Ideal mit $\mathfrak{m} \subset \mathfrak{a} \subset R$, so folgt $\mathfrak{a} = \mathfrak{m}$ oder $\mathfrak{a} = R$.*

Beispielsweise ist das Nullideal eines Ringes R genau dann ein Primideal, wenn R ein Integritätsring ist.

Satz 8. *Es sei R ein Ring.*

(i) *Ein Ideal $\mathfrak{p} \subset R$ ist genau dann ein Primideal, wenn $R/\mathfrak{p}$ ein Integritätsring ist.*

(ii) *Ein Ideal $\mathfrak{m} \subset R$ ist genau dann ein maximales Ideal, wenn $R/\mathfrak{m}$ ein Körper ist.*

Insbesondere ist jedes maximale Ideal ein Primideal.

Beweis. Zunächst überlegt man sich, dass $\mathfrak{p}$ genau dann ein echtes Ideal in R ist, wenn der Restklassenring $R/\mathfrak{p}$ nicht der Nullring ist, entsprechend für $\mathfrak{m}$. Aussage (i) ist dann leicht einzusehen. Bezeichnet man mit $\overline{a}, \overline{b} \in R/\mathfrak{p}$ die Restklassen zu Elementen $a, b \in R$, so ist

$$a \cdot b \in \mathfrak{p} \quad \Longrightarrow \quad a \in \mathfrak{p} \text{ oder } b \in \mathfrak{p}$$

offenbar äquivalent zu

$$\overline{a} \cdot \overline{b} = 0 \quad \Longrightarrow \quad \overline{a} = 0 \text{ oder } \overline{b} = 0.$$

Weiter ist Aussage (ii) eine Konsequenz der beiden folgenden Lemmata:

Lemma 9. *Ein Ideal* $\mathfrak{m} \subset R$ *ist genau dann maximal, wenn das Nullideal* $0 \subset R/\mathfrak{m}$ *maximal ist.*

Lemma 10. *Das Nullideal* $0 \subset R$ *eines Ringes* R *ist genau dann maximal, wenn* R *ein Körper ist.*

Beweis von Lemma 9. Sei $\pi\colon R \longrightarrow R/\mathfrak{m}$ die kanonische Projektion. Man prüft leicht nach, dass die Zuordnungen

$$\begin{aligned} R \supset \quad \mathfrak{a} \quad &\longmapsto \pi(\mathfrak{a}) \subset R/\mathfrak{m}, \\ R \supset \pi^{-1}(\mathfrak{b}) &\longleftarrow\!\shortmid\ \mathfrak{b} \quad \subset R/\mathfrak{m}, \end{aligned}$$

eine Bijektion zwischen den Idealen $\mathfrak{a}$ von R mit $\mathfrak{m} \subset \mathfrak{a} \subset R$ und den Idealen $\mathfrak{b} \subset R/\mathfrak{m}$ definieren. Hieraus ist die behauptete Äquivalenz unmittelbar ersichtlich.

Alternativ kann man die Behauptung auch in expliziter Weise verifizieren. Zunächst sei daran erinnert, dass $\mathfrak{m}$ genau dann ein echtes Ideal in R ist, wenn der Restklassenring $R/\mathfrak{m}$ nicht der Nullring ist. Ist nun $\mathfrak{m}$ ein echtes Ideal in R, so ist $\mathfrak{m}$ genau dann maximal, wenn für $a \in R - \mathfrak{m}$ stets $\mathfrak{m} + Ra = R$ gilt, wenn es also zu jedem solchen a Elemente $r \in R$ und $m \in \mathfrak{m}$ mit $ra + m = 1$ gibt. Unter Verwendung der Projektion $\pi\colon R \longrightarrow R/\mathfrak{m}$ sieht man, dass diese Bedingung genau dann erfüllt ist, wenn es zu $\overline{a} \in R/\mathfrak{m} - \{0\}$ stets ein Element $\overline{r} \in R/\mathfrak{m}$ gibt mit $\overline{r} \cdot \overline{a} = 1$, also genau dann, wenn das Nullideal in $R/\mathfrak{m}$ maximal ist. □

Beweis von Lemma 10. Sei $0 \subset R$ maximal und $a \in R$ von 0 verschieden. Dann folgt $aR = R$, und es existiert ein $b \in R$ mit $ab = 1$. Somit hat man $R^* = R - \{0\}$, d. h. R ist ein Körper. Umgekehrt ist unmittelbar klar, dass das Nullideal in einem Körper maximal ist. □

Die Sätze 6 und 8 geben eine vollständige Übersicht über Primideale und maximale Ideale in $\mathbb{Z}$:

Korollar 11. *Ein Ideal in* $\mathbb{Z}$ *ist genau dann prim, wenn es von der Form* $p\mathbb{Z}$ *mit einer Primzahl* p *oder mit* $p = 0$ *ist. Ein Ideal in* $\mathbb{Z}$ *ist genau dann maximal, wenn es ein von Null verschiedenes Primideal ist.*

Man muss lediglich benutzen, dass $\mathbb{Z}$ nach 2.2/3 Hauptidealring ist und dass das Nullideal in einem Integritätsring stets prim ist. Zum Schluss dieses Abschnitts wollen wir noch den sogenannten *Chinesischen Restsatz* beweisen.

Satz 12. *Sei R ein Ring und seien $\mathfrak{a}_1, \ldots, \mathfrak{a}_n \subset R$ paarweise* koprime *Ideale, d. h. es gelte $\mathfrak{a}_i + \mathfrak{a}_j = R$ für $i \neq j$. Ist dann $\pi_i \colon R \longrightarrow R/\mathfrak{a}_i$ jeweils die kanonische Projektion, so ist der Homomorphismus*

$$\varphi \colon R \longrightarrow R/\mathfrak{a}_1 \times \ldots \times R/\mathfrak{a}_n, \qquad x \longmapsto \big(\pi_1(x), \ldots, \pi_n(x)\big),$$

surjektiv und erfüllt $\ker \varphi = \mathfrak{a}_1 \cap \ldots \cap \mathfrak{a}_n$, *induziert also einen Isomorphismus*

$$R\Big/\bigcap_{i=1}^{n} \mathfrak{a}_i \xrightarrow{\sim} \prod_{i=1}^{n} R/\mathfrak{a}_i.$$

Dabei bezeichnet $\prod_{i=1}^{n} R/\mathfrak{a}_i = R/\mathfrak{a}_1 \times \ldots \times R/\mathfrak{a}_n$ das ringtheoretische Produkt der Restklassenringe $R/\mathfrak{a}_i$.

Beweis. Wir wollen zunächst zeigen, dass für $j = 1, \ldots, n$ die Ideale $\mathfrak{a}_j$ und $\bigcap_{i \neq j} \mathfrak{a}_i$ koprim sind, ihre Summe also gleich R ist. Sei im Folgenden ein solcher Index j fest gewählt. Da $\mathfrak{a}_j$ nach Voraussetzung zu den restlichen $\mathfrak{a}_i$ koprim ist, gibt es für $i \neq j$ Elemente $a_i \in \mathfrak{a}_j$, $a_i' \in \mathfrak{a}_i$ mit $a_i + a_i' = 1$. Somit folgt

$$1 = \prod_{i \neq j} (a_i + a_i') \in \mathfrak{a}_j + \prod_{i \neq j} \mathfrak{a}_i \subset \mathfrak{a}_j + \bigcap_{i \neq j} \mathfrak{a}_i,$$

d. h. es gilt $\mathfrak{a}_j + \bigcap_{i \neq j} \mathfrak{a}_i = R$ wie behauptet.

Für $j = 1, \ldots, n$ existieren daher Gleichungen $d_j + e_j = 1$ mit Elementen $d_j \in \mathfrak{a}_j$, $e_j \in \bigcap_{i \neq j} \mathfrak{a}_i$, und es folgt

$$\pi_i(e_j) = \begin{cases} 1 & \text{für} \quad i = j, \\ 0 & \text{für} \quad i \neq j. \end{cases}$$

Damit sieht man unmittelbar ein, dass φ surjektiv ist. Geht man nämlich von einem Element $y = (y_1, \ldots, y_n) \in R/\mathfrak{a}_1 \times \ldots \times R/\mathfrak{a}_n$ aus und wählt jeweils ein π_i-Urbild $x_i \in R$ zu y_i, so gilt

$$\varphi\Big(\sum_{i=1}^{n} x_i e_i\Big) = y.$$

Die Aussage über den Kern von φ ist trivial. Somit folgt die behauptete Isomorphie aus dem Homomorphiesatz. □

Ist $\mathfrak{a}$ ein Ideal in einem Ring R, so sagt man, dass zwei Elemente $x, y \in R$ *kongruent modulo* $\mathfrak{a}$ sind, in Zeichen $x \equiv y \bmod \mathfrak{a}$, wenn x und y dieselbe Restklasse in $R/\mathfrak{a}$ definieren, d. h. wenn $x - y \in \mathfrak{a}$ gilt. Ist dabei $\mathfrak{a}$ ein Hauptideal Ra, so schreibt man statt "mod $\mathfrak{a}$" häufig auch "mod a". Mit dieser Sprechweise können wir die Surjektivität der Abbildung φ in Satz 12 auch folgendermaßen formulieren: Zu $x_1, \ldots, x_n \in R$ gibt es ein $x \in R$ mit $x \equiv x_i \bmod \mathfrak{a}_i$ für $i = 1, \ldots, n$. Für den Ring $\mathbb{Z}$ der ganzen Zahlen hat der Chinesische Restsatz somit folgende Form:

Korollar 13. *Es seien $a_1, \ldots, a_n \in \mathbb{Z}$ paarweise teilerfremd. Dann ist das System simultaner Kongruenzen $x \equiv x_i \bmod a_i$, $i = 1, \ldots, n$, für beliebige Zahlen $x_1, \ldots, x_n \in \mathbb{Z}$ lösbar. Ist x eine Lösung, so ist diese eindeutig bestimmt modulo $a_1 \cdot \ldots \cdot a_n$. Die Gesamtheit der Lösungen bildet daher eine Restklasse des Typs $x + a_1 \cdot \ldots \cdot a_n\mathbb{Z}$.*

Man muss sich nur überlegen, dass für teilerfremde Zahlen $a, a' \in \mathbb{Z}$

$$(a, a') = (1) \quad \text{sowie} \quad (a \cdot a') = (a) \cap (a')$$

gilt; man vergleiche hierzu auch 2.4/13. Im Übrigen liefert der Beweis des Chinesischen Restsatzes auch ein praktisches Verfahren zur Lösung simultaner Kongruenzen. In einem ersten Schritt konstruiert man für $j = 1, \ldots, n$ Zahlen $d_j \in (a_j)$, $e_j \in (\prod_{i \neq j} a_i)$, mit $d_j + e_j = 1$, etwa unter Verwendung des *Euklidischen Algorithmus*; vgl. hierzu 2.4/15. Sodann ist $x = \sum_{i=1}^{n} x_i e_i$ eine Lösung des Systems $x \equiv x_i \bmod a_i$, $i = 1, \ldots, n$, und jede weitere Lösung entsteht durch Addition eines Vielfachen von $\prod_{i=1}^{n} a_i$.

Lernkontrolle und Prüfungsvorbereitung

1. Was ist ein Ringhomomorphismus? Was versteht man bei Polynomringen unter einem Einsetzungshomomorphismus?

2. Sei $\varphi\colon R \longrightarrow R'$ ein Ringhomomorphismus. Zeige, dass sich φ zu einem Homomorphismus der Einheitengruppen $R^* \longrightarrow R'^*$ beschränkt. Definiere den Kern von φ und zeige, dass dieser ein Ideal in R bildet.

3. Betrachte einen Ringhomomorphismus $\varphi\colon K \longrightarrow R$, wobei K ein Körper sei. Was weiß man über $\ker\varphi$ (mit Begründung)?
4. Erläutere die Konstruktion des Restklassenrings $R/\mathfrak{a}$ zu einem Ring R nach einem Ideal $\mathfrak{a} \subset R$.
5. Formuliere den Homomorphiesatz für Ringe und beweise ihn.
6. Bestimme alle Restklassenringe des Rings $\mathbb{Z}$ der ganzen Zahlen. Welche dieser Restklassenringe sind Integritätsringe, welche sind Körper? Erläutere die zugehörigen Beweise.
7. Zeige, dass es zu jeder Primzahl p einen Körper mit p Elementen gibt.
8. Was ist ein Primideal, was ein maximales Ideal in einem Ring? Zeige, dass jedes maximale Ideal ein Primideal ist und gib ein Beispiel eines Primideals, welches nicht maximal ist.
9. Welche Ideale in $\mathbb{Z}$ sind prim, welche sind maximal?
10. Formuliere den Chinesischen Restsatz.

$^{+}$11. Beweise den Chinesischen Restsatz.

$^{+}$12. Formuliere den Chinesischen Restsatz für den Ring $\mathbb{Z}$ der ganzen Zahlen und interpretiere ihn als Resultat über die Lösbarkeit simultaner Kongruenzen in $\mathbb{Z}$.

Übungsaufgaben

1. *Es sei $\varphi\colon R \longrightarrow R'$ ein Ringhomomorphismus. Überlege, welche Aussagen für die Bilder von Idealen $\mathfrak{a} \subset R$ bzw. die Urbilder von Idealen $\mathfrak{a}' \subset R'$ gelten. Untersuche diese Frage insbesondere auch für Primideale und maximale Ideale.*
2. *Betrachte für einen Ring R und ein Element $x \in R$ den Einsetzungshomomorphismus*
$$\varphi_x\colon R[X] \longrightarrow R, \qquad \sum a_i X^i \longmapsto \sum a_i x^i,$$
und beschreibe den Kern von φ_x. Überlege insbesondere, wann dieser ein Primideal bzw. ein maximales Ideal in $R[X]$ ist.
3. Verallgemeinere die Isomorphiesätze 1.2/8 und 1.2/9 auf die Ringsituation, indem Ringe statt Gruppen und Ideale statt Normalteiler betrachtet werden.
4. Sei $\varphi\colon R \longrightarrow R'$ ein Ringhomomorphismus und $x \in R'$. Zeige: Es gibt genau einen Ringhomomorphismus $\Phi\colon R[X] \longrightarrow R'$ mit $\Phi|_R = \varphi$ und $\Phi(X) = x$. Es entsprechen also die Ringhomomorphismen $\Phi\colon R[X] \longrightarrow R'$ mit $\Phi|_R = \varphi$ in bijektiver Weise den Elementen von R'.

5. Sei R ein Integritätsring und $\Phi\colon R[X] \longrightarrow R[X]$ ein Ringhomomorphismus mit $\Phi|_R = \mathrm{id}_R$. Zeige: Φ ist genau dann ein Automorphismus, wenn es $a \in R^*$ und $b \in R$ gibt mit $\Phi(X) = aX + b$.

6. Sei $\mathfrak{p}$ ein Primideal eines Ringes R. Zeige, dass $\mathfrak{p}R[X]$, das von $\mathfrak{p}$ in $R[X]$ erzeugte Ideal, ebenfalls ein Primideal ist.

7. Sei K ein Körper und $K[X,Y] = K[X][Y]$ der Polynomring über K in zwei Variablen X und Y. Im Restklassenring $R = K[X,Y]/(XY^2)$ bezeichne $\overline{X}$ bzw. $\overline{Y}$ jeweils die Restklasse von X bzw. Y. Zeige, dass die Elemente $\overline{X}$ und $\overline{X}+\overline{X}\cdot\overline{Y}$ aus R nicht assoziiert sind, dass die von ihnen in R erzeugten Hauptideale aber übereinstimmen. (*Hinweis*: Betrachte das Ideal aller Elemente $\overline{f} \in R$ mit $\overline{f}\cdot\overline{X} = 0$ bzw. das Ideal aller Elemente $f \in K[X,Y]$ mit $fX \in (XY^2)$.)

8. Sei R ein Ring. Zeige, dass $\{\sum a_i X^i \in R[X]\,;\, a_1 = 0\}$ ein Unterring von $R[X]$ ist und dass dieser isomorph zu $R[X][Y]/(X^2 - Y^3)$ ist.

2.4 Primfaktorzerlegung

Wesentliche Eigenschaften des Ringes $\mathbb{Z}$ der ganzen Zahlen wie auch des Polynomrings $K[X]$ über einem Körper K fußen auf der Tatsache, dass man in diesen Ringen eine Division mit Rest zur Verfügung hat. Wir wollen von Integritätsringen ausgehen, die eine solche Division ermöglichen, und zeigen, dass diese Ringe Hauptidealringe sind. In Hauptidealringen wiederum werden wir die Existenz der eindeutigen Primfaktorzerlegung beweisen.

Definition 1. *Ein Integritätsring R heißt ein* euklidischer Ring, *wenn es eine Abbildung $\delta\colon R{-}\{0\} \longrightarrow \mathbb{N}$ gibt, die in R eine Division mit Rest ermöglicht, und zwar in folgendem Sinne: Zu Elementen $f, g \in R$, $g \neq 0$, gibt es stets Elemente $q, r \in R$ mit*

$$f = qg + r, \quad \textit{wobei } \delta(r) < \delta(g) \textit{ oder } r = 0.$$

Die Abbildung δ wird als eine Grad- *oder* Normabbildung *des euklidischen Rings R bezeichnet.*

Jeder Körper ist aus trivialen Gründen ein euklidischer Ring. Wir wollen aber noch einige interessantere Beispiele betrachten.

(1) $\mathbb{Z}$ ist ein euklidischer Ring mit der gewöhnlichen Division mit Rest, als Gradabbildung $\delta\colon \mathbb{Z}-\{0\} \longrightarrow \mathbb{N}$ kann man die Abbildung $a \longmapsto |a|$ betrachten.

(2) Ist K ein Körper, so ist der Polynomring $K[X]$ mit der gewöhnlichen Polynomdivision mit Rest ein euklidischer Ring, unter der Gradabbildung $\delta\colon K[X]-\{0\} \longrightarrow \mathbb{N}$ gegeben durch $f \longmapsto \operatorname{grad} f$. Man vergleiche hierzu 2.1/4

(3) $\mathbb{Z}[i] := \{x+iy\,;\, x,y \in \mathbb{Z}\} \subset \mathbb{C}$ ist ein euklidischer Ring unter der Gradabbildung

$$\delta\colon \mathbb{Z}[i]-\{0\} \longrightarrow \mathbb{N}, \qquad x+iy \longmapsto x^2+y^2 = |x+iy|^2.$$

Man nennt $\mathbb{Z}[i]$ den *Ring der ganzen Gaußschen Zahlen*. Zur Charakterisierung der Division mit Rest in $\mathbb{Z}[i]$ beachte man, dass der Abstand zweier benachbarter Punkte aus $\mathbb{Z}[i]$ höchstens $\sqrt{2}$ beträgt. Zu Elementen $f, g \in \mathbb{Z}[i]$, $g \neq 0$, gibt es daher $x, y \in \mathbb{Z}$ mit $|fg^{-1}-(x+iy)| \leq \frac{1}{2}\cdot\sqrt{2} < 1$. Setzt man nun $q := (x+iy)$, $r := f - qg$, so hat man $|r| < |g|$, also

$$f = qg + r \quad \text{mit} \quad \delta(r) < \delta(g) \text{ oder } r = 0.$$

(4) Sei $d \neq 0, 1$ eine ganze Zahl, und sei d quadratfrei in dem Sinne, dass d kein Quadrat einer natürlichen Zahl > 1 als Teiler besitzt. Man betrachte zu d den folgenden Unterring von $\mathbb{C}$:

$$R_d = \begin{cases} \mathbb{Z} + \sqrt{d}\cdot\mathbb{Z}, & \text{falls } d \equiv 2,3 \mod 4 \\ \mathbb{Z} + \frac{1}{2}\left(1+\sqrt{d}\right)\cdot\mathbb{Z}, & \text{falls } d \equiv 1 \mod 4 \end{cases}$$

Für $d = -1$ erhält man den oben diskutierten Ring der ganzen Gaußschen Zahlen. Die Ringe R_d sind in der Zahlentheorie von besonderem Interesse. Man möchte wissen, ob R_d faktoriell ist, d. h. ob in R_d jeweils der Satz von der eindeutigen Primfaktorzerlegung gilt. Da ein euklidischer Ring Hauptidealring ist und ein Hauptidealring faktoriell ist, vgl. Satz 2 und Korollar 11, untersucht man in erster Approximation, für welche Werte von d der Ring R_d euklidisch ist. Als Gradabbildung $\delta\colon R_d-\{0\} \longrightarrow \mathbb{N}$ bietet sich hier die sogenannte "Norm" an, gegeben durch $\delta(a+b\sqrt{d}) = |a^2-b^2d|$; zur allgemeinen Definition der Norm vgl. Abschnitt 4.7. Man kann zeigen, dass R_d genau für folgende Werte von d unter dieser Gradabbildung euklidisch ist:

$$d = -1, -2, -3, -7, -11,$$
$$d = 2, 3, 5, 6, 7, 11, 13, 17, 19, 21, 29, 33, 37, 41, 57, 73.$$

Darüber hinaus weiß man, dass R_d für $d < 0$ in noch genau den folgenden Fällen faktoriell ist:

$$d = -19, -43, -67, -163.$$

Für $d > 0$ hingegen ist R_d faktoriell in einer Vielzahl weiterer Fälle. Bezüglich Details konsultiere man etwa H. Hasse [7], §16.6.

Satz 2. *Jeder euklidische Ring ist ein Hauptidealring.*

Beweis. Wir gehen wie in 1.3/4 vor. Sei $\mathfrak{a} \subset R$ ein Ideal; ohne Einschränkung gelte $\mathfrak{a} \neq 0$. Man wähle unter den Elementen a von $\mathfrak{a} - \{0\}$ eines mit der Eigenschaft, dass $\delta(a)$ minimal unter der Gradabbildung δ unseres euklidischen Rings R ist. Dann gilt schon $\mathfrak{a} = (a)$. Ist nämlich $f \in \mathfrak{a}$, $f = qa + r$ mit $\delta(r) < \delta(a)$ oder $r = 0$, so folgt $r = f - qa \in \mathfrak{a}$. Wegen der Minimalität von $\delta(a)$ muss $r = 0$ gelten und somit $f = qa \in (a)$. Dies zeigt $\mathfrak{a} \subset (a)$. Die umgekehrte Inklusion ist trivial, so dass $\mathfrak{a} = (a)$ Hauptideal ist. □

Korollar 3. *Die Ringe $\mathbb{Z}$, $\mathbb{Z}[i]$ sowie der Polynomring $K[X]$ über einem Körper K sind als euklidische Ringe auch Hauptidealringe.*

Als Nächstes wollen wir Primfaktorzerlegungen in Hauptidealringen studieren. Wir sagen, dass in einem Integritätsring R ein Element x das Element y *teilt*, in Zeichen $x \mid y$, wenn es ein $c \in R$ mit $cx = y$ gibt. Äquivalent zu dieser Gleichung ist $y \in (x)$. Ist x kein Teiler von y, so schreibt man $x \nmid y$.

Definition 4. *Es sei R ein Integritätsring und $p \in R$ eine von 0 verschiedene Nichteinheit.*

(i) *p heißt* irreduzibel, *falls für jede Zerlegung $p = xy$ mit $x, y \in R$ gilt: $x \in R^*$ oder $y \in R^*$. Es heißt p* reduzibel, *falls p nicht irreduzibel ist.*

(ii) *p heißt* primes Element *oder* Primelement, *wenn aus $p \mid xy$ mit $x, y \in R$ stets $p \mid x$ oder $p \mid y$ folgt, d. h. mit anderen Worten, wenn das Hauptideal (p) prim ist.*

Im Ring $\mathbb{Z}$ der ganzen Zahlen entsprechen die irreduziblen Elemente abgesehen vom Vorzeichen genau den Primzahlen im üblichen Sinne, während im Polynomring $K[X]$ über einem Körper K insbesondere die linearen Polynome $X - a$ mit $a \in K$ irreduzibel sind. Für $K = \mathbb{C}$ sind hierdurch bis auf Assoziiertheit alle irreduziblen Polynome beschrieben, wie wir später anhand des Fundamentalsatzes der Algebra sehen werden. Im Allgemeinen gibt es jedoch über einem Körper K irreduzible Polynome vom Grad > 1, in $\mathbb{R}[X]$ etwa das Polynom $X^2 + 1$. Im Übrigen werden wir in Satz 6 sehen, dass die Begriffe irreduzibles Element und Primelement in Hauptidealringen übereinstimmen, also insbesondere in $\mathbb{Z}$ bzw. $K[X]$.

Bemerkung 5. *Es sei R ein Integritätsring und $p \in R$ eine von 0 verschiedene Nichteinheit.*

(i) *Wenn (p) ein maximales Ideal in R ist, so ist p ein Primelement.*

(ii) *Wenn p ein Primelement ist, so ist p irreduzibel.*

Beweis. Ist (p) ein maximales Ideal in R, so auch ein Primideal nach 2.3/8, und es folgt, dass p ein Primelement ist. Dies zeigt die Behauptung (i). Zum Nachweis von (ii) sei p als Primelement angenommen. Gilt dann $p = xy$ mit $x, y \in R$, so ergibt sich $p \mid x$ oder $p \mid y$ aufgrund der Primelementeigenschaft von p. Nehmen wir $p \mid x$ an, so existiert also ein $c \in R$ mit $pc = x$, und es folgt $p = xy = pcy$. Da R ein Integritätsring ist, hat man $cy = 1$ und somit $y \in R^*$, d. h. p ist irreduzibel. □

In Hauptidealringen können wir die Aussage der soeben bewiesenen Bemerkung erheblich verschärfen; man vergleiche auch 2.3/6.

Satz 6. *Es sei R ein Hauptidealring und $p \in R$ eine von 0 verschiedene Nichteinheit. Dann ist äquivalent*:

(i) *p ist irreduzibel.*

(ii) *p ist Primelement.*

(iii) *(p) ist maximales Ideal in R.*

Beweis. Unter Benutzung von Bemerkung 5 bleibt nur noch die Implikation von (i) nach (iii) nachzuweisen. Sei also p irreduzibel, und sei $\mathfrak{a} = (a)$ ein Ideal in R mit $(p) \subset (a) \subset R$. Dann existiert ein $c \in R$ mit $p = ac$. Da p

irreduzibel ist, folgt $a \in R^*$ oder $c \in R^*$. Im ersten Fall hat man $(a) = R$ und im zweiten $(a) = (p)$. Somit ist (p) maximal. □

Als Folgerung hierzu können wir leicht die Existenz von Primfaktorzerlegungen in Hauptidealringen beweisen. Es braucht nur eine Faktorisierung in irreduzible Elemente durchgeführt werden.

Satz 7. *Es sei R ein Hauptidealring und $a \in R$ eine von 0 verschiedene Nichteinheit. Dann lässt sich a als Produkt von Primelementen schreiben.*[2]

Beweis. Man fixiere ein Element $a \in R - (R^* \cup \{0\})$. Ist a irreduzibel (und damit prim), so ist nichts zu zeigen. Anderenfalls zerlege man a in das Produkt bc zweier Nichteinheiten aus R. Diese Konstruktion kann man dann für b sowie c wiederholen usw. Zum Beweis des Satzes ist lediglich zu zeigen, dass das Verfahren nach endlich vielen Schritten abbricht. Für die uns interessierenden Ringe $\mathbb{Z}$ und $K[X]$, wobei K ein Körper sei, ist dies unmittelbar klar. In $\mathbb{Z}$ etwa gilt $|b|, |c| < |a|$ bei einer Faktorisierung von a in Nichteinheiten b, c. Entsprechend hat man $\operatorname{grad} b, \operatorname{grad} c < \operatorname{grad} a$ in $K[X]$, wie man mit 2.1/2 sieht. Bei der beschriebenen Zerlegung von a nimmt daher der Betrag bzw. Grad bei jedem Schritt echt ab, so dass das Verfahren nach endlich vielen Schritten abbrechen muss.

Wir wollen hier noch ein Argument angeben, welches auch für einen beliebigen Hauptidealring R zeigt, dass man a in ein (endliches) Produkt irreduzibler Elemente zerlegen kann. Folgende Hilfsaussage wird benötigt:

Lemma 8. *Jeder Hauptidealring R ist ein* noetherscher Ring, *d. h. jede aufsteigende Kette von Idealen $\mathfrak{a}_1 \subset \mathfrak{a}_2 \subset \ldots \subset R$ wird stationär in dem Sinne, dass es ein $n \in \mathbb{N}$ gibt mit $\mathfrak{a}_i = \mathfrak{a}_n$ für alle $i \geq n$.*

Die Aussage ist leicht zu verifizieren. Da die Vereinigung einer aufsteigenden Kette von Idealen wieder ein Ideal ergibt, kann man das Ideal $\mathfrak{a} = \bigcup_{i \geq 1} \mathfrak{a}_i$ bilden; dieses ist ein Hauptideal, etwa $\mathfrak{a} = (a)$. Wegen $a \in \mathfrak{a}$ gibt es ein $n \in \mathbb{N}$ mit $a \in \mathfrak{a}_n$, so dass $(a) \subset \mathfrak{a}_n \subset \mathfrak{a} = (a)$ folgt. Die Idealkette $\mathfrak{a}_1 \subset \mathfrak{a}_2 \subset \ldots$ wird somit bei $\mathfrak{a}_n$ stationär.

[2] Unter einem Produkt von Elementen eines Ringes verstehen wir naturgemäß immer ein *endliches* Produkt.

Nun wollen wir den Allgemeinfall von Satz 7 beweisen. Es sei S die Menge aller Hauptideale in R, die von Elementen $a \in R-(R^* \cup \{0\})$ erzeugt werden, so dass a keine endliche Faktorisierung in irreduzible Elemente zulasse. Zu zeigen ist $S = \emptyset$. Gilt $S \neq \emptyset$, so gibt es aufgrund von Lemma 8 ein maximales Element in S, d. h. ein Element $\mathfrak{a} \in S$ mit der Eigenschaft, dass aus einer echten Inklusion $\mathfrak{a} \subsetneq \mathfrak{b}$ von Idealen in R notwendig folgt, dass $\mathfrak{b}$ nicht zu S gehört. Sei also $\mathfrak{a} = (a)$ ein solches maximales Element. Dann ist das erzeugende Element a reduzibel, etwa $a = a_1 a_2$ mit Nichteinheiten $a_1, a_2 \in R$. Folglich haben wir echte Inklusionen

$$(a) \subsetneq (a_1), \qquad (a) \subsetneq (a_2),$$

und es ergibt sich, dass (a_1) und (a_2) nicht zu S gehören können. Es haben daher a_1 und a_2 Faktorisierungen in irreduzible Elemente, und damit gilt dasselbe auch für das Produkt $a = a_1 a_2$ im Widerspruch zu $(a) \in S$. Somit folgt $S = \emptyset$, und Satz 7 ist bewiesen. □

Zerlegungen in Primelemente wie in Satz 7 erfüllen eine gewisse Eindeutigkeitsaussage.

Lemma 9. *Es sei R ein Integritätsring. Für ein Element $a \in R$ habe man Zerlegungen*

$$a = p_1 \dots p_r = q_1 \dots q_s$$

in Primelemente p_i und irreduzible Elemente q_j. Dann gilt $r = s$, und nach eventueller Umnummerierung der q_j ist p_i assoziiert zu q_i für $i = 1, \dots, r$.

Beweis. Aus $p_1 \mid q_1 \dots q_s$ folgt aufgrund der Primelementeigenschaft von p_1, dass es ein j mit $p_1 \mid q_j$ gibt. Nach Umnummerierung der q_j dürfen wir $j = 1$ annehmen. Es gibt also eine Gleichung $q_1 = \varepsilon_1 p_1$, wobei ε_1 Einheit sein muss, da q_1 irreduzibel ist. Somit folgt

$$p_2 \dots p_r = \varepsilon_1 q_2 \dots q_s,$$

und man kann das Verfahren induktiv fortsetzen, um die Behauptung zu erhalten. □

Satz und Definition 10. *Es sei R ein Integritätsring. Dann ist äquivalent*:

(i) *Jedes $a \in R-(R^* \cup \{0\})$ lässt sich eindeutig (bis auf Assoziiertheit und Reihenfolge) als Produkt von irreduziblen Elementen schreiben.*

(ii) *Jedes* $a \in R - (R^* \cup \{0\})$ *lässt sich als Produkt von Primelementen schreiben.*

Ein Integritätsring R, *der die vorstehenden äquivalenten Bedingungen erfüllt, heißt* faktoriell. *Man sagt auch, dass in* R *der* Satz von der eindeutigen Primfaktorzerlegung *gilt.*

In einem faktoriellen Ring ist ein Element a *genau dann irreduzibel, wenn es prim ist.*

Beweis. Es gelte die Bedingung (i). Wir wollen zeigen, dass dann jedes irreduzible Element von R schon prim ist. Sei also $a \in R$ irreduzibel, und seien $x, y \in R$ mit $a \mid xy$. Zu zeigen ist $a \mid x$ oder $a \mid y$. Hierzu dürfen wir annehmen, dass x und y keine Einheiten sind. Seien $x = x_1 \dots x_r$, $y = y_1 \dots y_s$ Zerlegungen in irreduzible Elemente gemäß (i). Dann folgt $a \mid (x_1 \dots x_r y_1 \dots y_s)$, und die Eindeutigkeitsaussage in (i) hat zur Folge, dass a als irreduzibles Element zu einem x_i oder einem y_j assoziiert ist. Daher gilt $a \mid x$ oder $a \mid y$, und a ist Primelement. Mit dieser Überlegung ist die Implikation von (i) nach (ii) unmittelbar klar. Die Umkehrung folgt mit Lemma 9, da eine Zerlegung in Primelemente nach Bemerkung 5 insbesondere eine Zerlegung in irreduzible Elemente ist.

Wir haben gerade gesehen, dass unter der Bedingung (i) jedes irreduzible Element prim ist, dass also irreduzible Elemente in faktoriellen Ringen prim sind. Die Umkehrung hierzu ergibt sich wiederum aus Bemerkung 5. □

Die Aussage von Satz 7 können wir nun neu formulieren:

Korollar 11. *Jeder Hauptidealring ist faktoriell.*

Körper sind aus trivialen Gründen faktoriell. Aber auch die Ringe $\mathbb{Z}$, $\mathbb{Z}[i]$ sowie der Polynomring $K[X]$ über einem Körper K sind als euklidische Ringe Hauptidealringe und damit faktoriell. Wir werden in 2.7/1 zeigen, dass der Polynomring $R[X]$ über einem faktoriellen Ring R selbst wieder faktoriell ist. Somit kann man sehen, dass etwa der Ring $\mathbb{Z}[X]$ faktoriell ist, obwohl er kein Hauptidealring ist. Gleiches gilt für den Polynomring $K[X,Y] := K[X][Y]$ in zwei Variablen X und Y über einem Körper K.

Es ist üblich, Primfaktorzerlegungen in faktoriellen Ringen R durch Zusammenfassen assoziierter Primelemente zu Potenzen in der Form

$$a = \varepsilon p_1^{\nu_1} \dots p_r^{\nu_r}$$

zu schreiben, wobei ε eine Einheit ist. Formal besitzt dann jedes Element $a \in R - \{0\}$ eine solche Primfaktorzerlegung (mit Exponenten $\nu_i = 0$, wenn a Einheit ist). Um Primfaktorzerlegungen weiter zu standardisieren, kann man in R ein Vertretersystem P von Primelementen auswählen, d. h. eine Teilmenge P bestehend aus Primelementen, so dass P aus jeder Klasse zueinander assoziierter Primelemente genau eines enthält. Dann kann man Primfaktorzerlegungen in R in der Form

$$a = \varepsilon \prod_{p \in P} p^{\nu_p(a)}$$

schreiben, wobei nunmehr $\varepsilon \in R^*$ sowie die Exponenten $\nu_p(a) \in \mathbb{N}$ eindeutig bestimmt sind; natürlich gilt $\nu_p(a) = 0$ für fast alle $p \in P$, so dass das Produkt in Wahrheit endlich ist. In $\mathbb{Z}$ ist es üblich, P als die Menge der (positiven) Primzahlen zu wählen, in $K[X]$ nimmt man für P die Menge aller normierten irreduziblen (oder Prim-) Polynome, d. h. aller irreduziblen Polynome, deren höchster Koeffizient 1 ist.

Wir wollen im Folgenden noch auf die Begriffe größter gemeinsamer Teiler und kleinstes gemeinsames Vielfaches eingehen. Sei R ein Integritätsring, und seien $x_1, \dots, x_n \in R$. Ein Element $d \in R$ heißt *größter gemeinsamer Teiler* von $x_1, \dots, x_n$, wenn gilt:

(i) $d \mid x_i$ für $i = 1, \dots, n$, d. h. d ist gemeinsamer Teiler aller x_i.

(ii) Ist $a \in R$ ein gemeinsamer Teiler der x_i, also $a \mid x_i$ für $i = 1, \dots, n$, so folgt $a \mid d$.

Es ist dann d eindeutig bis auf Assoziiertheit, und man verwendet die Notation $d = \mathrm{ggT}(x_1, \dots, x_n)$. Im Falle $d = 1$ bezeichnet man $x_1, \dots, x_n$ als *teilerfremd*.

Weiter nennt man ein Element $v \in R$ ein *kleinstes gemeinsames Vielfaches* von $x_1, \dots, x_n$, wenn gilt:

(i) $x_i \mid v$ für $i = 1, \dots, n$, d. h. v ist gemeinsames Vielfaches aller x_i.

(ii) Ist $a \in R$ ein gemeinsames Vielfaches der x_i, d. h. gilt $x_i \mid a$ für $i = 1, \dots, n$, so folgt $v \mid a$.

Auch in diesem Falle ist v eindeutig bis auf Assoziiertheit, man schreibt $v = \mathrm{kgV}(x_1, \dots, x_n)$. Wie üblich beweist man:

Satz 12. *Es sei R ein faktorieller Ring. Ist dann P ein Vertretersystem der Primelemente von R und sind*

$$x_i = \varepsilon_i \prod_{p \in P} p^{\nu_p(x_i)}, \qquad i = 1, \ldots, n,$$

Primfaktorzerlegungen von Elementen $x_1, \ldots, x_n \in R - \{0\}$, *so existieren* $\mathrm{ggT}(x_1, \ldots, x_n)$ *und* $\mathrm{kgV}(x_1, \ldots, x_n)$, *und zwar gilt (bis auf Assoziiertheit)*

$$\mathrm{ggT}(x_1, \ldots, x_n) = \prod_{p \in P} p^{\min(\nu_p(x_1), \ldots, \nu_p(x_n))},$$
$$\mathrm{kgV}(x_1, \ldots, x_n) = \prod_{p \in P} p^{\max(\nu_p(x_1), \ldots, \nu_p(x_n))}.$$

In Hauptidealringen lassen sich der größte gemeinsame Teiler und das kleinste gemeinsame Vielfache idealtheoretisch charakterisieren.

Satz 13. *Es seien* $x_1, \ldots, x_n$ *Elemente eines Integritätsrings* R.

(i) *Falls* $(x_1, \ldots, x_n)$, *das von den* x_i *in* R *erzeugte Ideal, ein Hauptideal ist, also von einem Element* $d \in R$ *erzeugt wird, so gilt* $d = \mathrm{ggT}(x_1, \ldots, x_n)$.

(ii) *Falls* $(x_1) \cap \ldots \cap (x_n)$ *ein Hauptideal ist, also von einem Element* $v \in R$ *erzeugt wird, so gilt* $v = \mathrm{kgV}(x_1, \ldots, x_n)$.

Beweis. (i) Es gelte $(x_1, \ldots, x_n) = (d)$. Dann folgt $x_i \in (d)$ und somit $d \mid x_i$ für alle i. Außerdem gibt es wegen $d \in (x_1, \ldots, x_n)$ eine Gleichung $d = \sum_{i=1}^n a_i x_i$ mit gewissen Elementen $a_i \in R$. Hieraus ergibt sich, dass jeder gemeinsame Teiler der x_i auch ein Teiler von d ist, d. h. $d = \mathrm{ggT}(x_1, \ldots, x_n)$.

(ii) Gelte $\bigcap_{i=1}^n (x_i) = (v)$. Dann ist v Element aller Ideale (x_i), also gemeinsames Vielfaches aller x_i. Sei nun a ein weiteres gemeinsames Vielfaches der x_i. Dann folgt $a \in (x_i)$ für alle i, also $a \in \bigcap_{i=1}^n (x_i) = (v)$ und somit $v \mid a$, d. h. $v = \mathrm{kgV}(x_1, \ldots, x_n)$. □

Als Beispiel für eine Anwendung der gerade gegebenen idealtheoretischen Charakterisierung des größten gemeinsamen Teilers und des kleinsten gemeinsamen Vielfachen wollen wir eine spezielle Version des Chinesischen Restsatzes 2.3/12 betrachten. Eine ähnliche Version für den Ring $\mathbb{Z}$ der ganzen Zahlen hatten wir bereits in 2.3/13 kennen gelernt.

Korollar 14. *Es sei* R *ein Hauptidealring und* $a = \varepsilon p_1^{\nu_1} \ldots p_r^{\nu_r}$ *eine Primfaktorzerlegung in* R *mit einer Einheit* ε *und paarweise nicht-assoziierten*

Primelementen p_i. Dann liefert der Chinesische Restsatz 2.3/12 *einen kanonischen Isomorphismus*

$$R/(a) \xrightarrow{\sim} R/(p_1^{\nu_1}) \times \ldots \times R/(p_n^{\nu_n}).$$

Beweis. Mittels der Sätze 12 und 13 sieht man, dass die Hauptideale $(p_1^{\nu_1}), \ldots, (p_r^{\nu_r})$ jeweils paarweise koprim in R sind, denn es gilt $\mathrm{ggT}(p_i^{\nu_i}, p_j^{\nu_j}) = 1$ für $i \neq j$. Ähnlich ergibt sich $(a) = \bigcap_{i=1}^{r}(p_i^{\nu_i})$, denn man hat $a = \mathrm{kgV}(p_1^{\nu_1}, \ldots, p_r^{\nu_r})$. □

In euklidischen Ringen R verfügt man über ein konstruktives Verfahren zur Bestimmung des größten gemeinsamen Teilers zweier Elemente $x, y \in R$, nämlich den *Euklidischen Algorithmus*. Durch iterative Anwendung von Beziehungen des Typs $\mathrm{ggT}(x, y, z) = \mathrm{ggT}(\mathrm{ggT}(x, y), z)$ eignet sich dieses Verfahren auch zur Bestimmung des größten gemeinsamen Teilers von mehr als zwei Elementen.

Satz 15 (Euklidischer Algorithmus). *Es sei R ein euklidischer Ring. Für zwei Elemente $x, y \in R - \{0\}$ betrachte man die Folge $z_0, z_1, \ldots$ in R, die induktiv gegeben ist durch*:

$$\begin{aligned} z_0 &= x, \\ z_1 &= y, \\ z_{i+1} &= \begin{cases} \text{der Rest von } z_{i-1} \text{ bei Division durch } z_i, \text{ falls } z_i \neq 0, \\ 0 \text{ sonst.} \end{cases} \end{aligned}$$

Dann gibt es einen kleinsten Index $n \in \mathbb{N}$ mit $z_{n+1} = 0$. Für dieses n gilt $z_n = \mathrm{ggT}(x, y)$.

Beweis. Es sei $\delta\colon R - \{0\} \longrightarrow \mathbb{N}$ die Gradabbildung von R. Nach Definition der Folge $z_0, z_1, \ldots$ hat man für $i > 0$ unter der Bedingung $z_i \neq 0$ eine Gleichung der Form

$$z_{i-1} = q_i z_i + z_{i+1},$$

wobei $\delta(z_{i+1}) < \delta(z_i)$ oder $z_{i+1} = 0$ gilt. Die Folge der Grade $\delta(z_i)$ ist daher für $i > 0$ streng monoton fallend, jedenfalls solange $z_i \neq 0$ gilt und $\delta(z_i)$ erklärt ist. Somit kann $z_i \neq 0$ aber nur für endlich viele $i \in \mathbb{N}$ gelten, und es gibt einen kleinsten Index $n \in \mathbb{N}$ mit $z_{n+1} = 0$. Wegen $z_0 \neq 0 \neq z_1$ ist $n > 0$. Man betrachte nun die Gleichungen

$$
\begin{aligned}
&(\mathrm{E}_0) && z_0 = q_1 z_1 + z_2,\\
&\vdots && \vdots\\
&(\mathrm{E}_{n-2}) && z_{n-2} = q_{n-1} z_{n-1} + z_n,\\
&(\mathrm{E}_{n-1}) && z_{n-1} = q_n z_n.
\end{aligned}
$$

Es folgt $z_n \mid z_{n-1}$ aus (E_{n-1}), dann $z_n \mid z_{n-2}$ aus (E_{n-2}) usw., bis man schließlich $z_n \mid z_1$ und $z_n \mid z_0$ erhält. Es ist also z_n ein gemeinsamer Teiler von x und y. Ist $a \in R$ ein weiterer gemeinsamer Teiler von x und y, so folgt $a \mid z_2$ aus (E_0), dann $a \mid z_3$ aus (E_1) usw., bis man schließlich zu $a \mid z_n$ gelangt. Also ist z_n wie behauptet der größte gemeinsame Teiler von x und y. □

Der Euklidische Algorithmus gestattet es nicht nur, den größten gemeinsamen Teiler d zweier Elemente x, y eines euklidischen Rings R zu bestimmen, sondern er liefert zusätzlich auch eine explizite Darstellung dieses Teilers in der Form $d = ax + by$. Im obigen Beweis erhält man nämlich aus (E_{n-2}) eine Darstellung von $d = z_n$ als Linearkombination in z_{n-2}, z_{n-1}, unter Hinzunahme von (E_{n-3}) als Linearkombination in z_{n-3}, z_{n-2} usw., bis d schließlich unter Benutzung von (E_0) als Linearkombination von $x = z_0$ und $y = z_1$ dargestellt ist. Die Konstruktion einer solchen Darstellung wird z. B. bei dem praktischen Verfahren zur Lösung simultaner Kongruenzen 2.3/13 benötigt, die allgemeine Existenz ist hingegen bereits in Hauptidealringen gegeben, wie wir in Satz 13 gesehen haben.

Abschließend wollen wir noch auf einige Anwendungen der in diesem Abschnitt erzielten Resultate hinweisen. Wir können aus 2.3/8 und Satz 6 nochmals folgern, dass für ein $p \in \mathbb{Z}$, $p > 0$, der Restklassenring $\mathbb{Z}/p\mathbb{Z}$ genau dann ein Körper ist, wenn p eine Primzahl ist. Ebenso ist für einen Körper K der Restklassenring $L = K[X]/(f)$ nach dem von einem Polynom $f \in K[X]$ erzeugten Hauptideal genau dann ein Körper, wenn f irreduzibel ist. Man sieht leicht (vgl. den Beweis zu 3.4/1), dass die Restklasse von X in L nunmehr Nullstelle von f ist. Dabei fasse man K vermöge des kanonischen Homomorphismus $K \longrightarrow L$ (dieser ist nach 2.3/3 injektiv) als Teilkörper von L auf und entsprechend f als Polynom mit Koeffizienten in L. Wir werden dieses auf L. Kronecker zurückgehende Verfahren in 3.4/1 benutzen, um zu einem gegebenen Polynom $f \in K[X] - K$, welches in K keine Nullstelle besitzt, einen Erweiterungskörper L zu konstruieren, so dass f eine Nullstelle in L hat. Beispielsweise sieht man mit Hilfe des Homomorphiesatzes unmittelbar

$$\mathbb{R}[X]/(X^2+1) \simeq \mathbb{C},$$

indem man den Einsetzungshomomorphismus

$$\mathbb{R}[X] \longrightarrow \mathbb{C}, \qquad \sum a_n X^n \longmapsto \sum a_n i^n,$$

betrachtet, der X auf die komplexe Zahl i abbildet. Auf ähnliche Weise zeigt man

$$\mathbb{R}[X]/(X-a) \simeq \mathbb{R}$$

für beliebiges $a \in \mathbb{R}$.

Lernkontrolle und Prüfungsvorbereitung

1. Was ist ein euklidischer Ring? Nenne einige Beispiele euklidischer Ringe.
2. Zeige, dass jeder euklidische Ring ein Hauptidealring ist.
3. Definiere den Ring $\mathbb{Z}[i]$ der ganzen Gaußschen Zahlen und zeige, dass dieser ein Hauptidealring ist.
4. Erläutere die Eigenschaften "irreduzibel" und "prim" für Elemente eines Integritätsrings.
5. Sei p ein Element eines Integritätsrings R mit $p \neq 0$ und $p \notin R^*$. Zeige, dass p ein Primelement ist, falls p in R ein maximales Ideal erzeugt, und weiter, dass p irreduzibel ist, falls p prim ist. Beweise auch die Umkehrungen hierzu für den Fall eines Hauptidealrings R.
6. In einem Hauptidealring R lässt sich jedes Element $a \in R$ mit $a \neq 0$, $a \notin R^*$ als Produkt von Primelementen schreiben. Beweise dies für den Ring $R = \mathbb{Z}$ der ganzen Zahlen und für den Polynomring $R = K[X]$ in einer Variablen über einem Körper K.

+7. Führe den Beweis zu Punkt 6 für beliebige Hauptidealringe R durch.

8. Es sei R ein Integritätsring. Erkläre den Begriff der "Assoziiertheit" für Elemente in R. Zeige, dass je zwei gegebene Zerlegungen eines Elementes $a \in R$ in ein Produkt von Primelementen übereinstimmen, abgesehen von Reihenfolge und Assoziiertheit der Faktoren.
9. Was ist ein faktorieller Ring? Nutze zur Definition "Zerlegungen in Primelemente" oder alternativ "eindeutige Zerlegungen in irreduzible Elemente" und zeige, dass beide Vorgehensweisen äquivalent sind.

10. Zeige, dass der Ring der ganzen Zahlen $\mathbb{Z}$ sowie der Polynomring $K[X]$ in einer Variablen X über einem Körper K Beispiele für faktorielle Ringe sind.

11. Erläutere die Begriffe "größter gemeinsamer Teiler" und "kleinstes gemeinsames Vielfaches" für Elemente $x_1, \ldots, x_n$ eines Integritätsrings R. Charakterisiere diese Bildungen mittels Primfaktorzerlegung in faktoriellen Ringen R.

12. Was versteht man unter der idealtheoretischen Charakterisierung des größten gemeinsamen Teilers bzw. des kleinsten gemeinsamen Vielfachen in Integritätsringen?

+13. Sei R ein euklidischer Ring. Erläutere das Verfahren des "Euklidischen Algorithmus" zur konstruktiven Bestimmung des größten gemeinsamen Teilers zweier Elemente $x, y \in R - \{0\}$.

14. Konstruiere einen Isomorphismus $\mathbb{R}[X]/(X^2+1) \simeq \mathbb{C}$ (mit Begründung).

Übungsaufgaben

1. *Welche Ringe R haben die Eigenschaft, dass der Polynomring $R[X]$ ein Hauptidealring ist*?

2. *Es folgt aus Satz* 13, *dass sich in einem Hauptidealring der größte gemeinsame Teiler und das kleinste gemeinsame Vielfache zweier Elemente stets idealtheoretisch charakterisieren lassen. Untersuche, ob dies auch allgemeiner in faktoriellen Ringen gilt.*

3. Beweise, dass der Unterring $R = \mathbb{Z} + \sqrt{-5} \cdot \mathbb{Z} \subset \mathbb{C}$ nicht faktoriell ist. Betrachte hierzu die Faktorisierungen $6 = 2 \cdot 3 = (1+\sqrt{-5}) \cdot (1-\sqrt{-5})$ und zeige, dass die Elemente $2, 3, (1+\sqrt{-5}), (1-\sqrt{-5})$ jeweils irreduzibel und paarweise nichtassoziiert sind. Handelt es sich bei diesen Elementen um Primelemente?

4. Sei K ein Körper und $R = K[X][Y]/(X^2 - Y^3)$ der Integritätsring aus Aufgabe 8 in 2.3. Zeige: Die Restklassen $\overline{X}$ und $\overline{Y}$ zu den Elementen $X, Y \in K[X][Y]$ sind irreduzibel in R, aber nicht prim.

5. Sei G eine zyklische Gruppe endlicher Ordnung, und seien $a, b \in G$. Dann ist die von a und b in G erzeugte Untergruppe von der Ordnung $\mathrm{kgV}(\mathrm{ord}\, a, \mathrm{ord}\, b)$.

6. Zeige, dass $2 = (1+i)(1-i)$ die Primfaktorzerlegung von 2 in $\mathbb{Z}[i]$ ist.

7. Berechne mit Hilfe des Euklidischen Algorithmus den größten gemeinsamen Teiler der folgenden Polynome aus $\mathbb{Q}[X]$:

$$f = X^3 + X^2 + X - 3, \qquad g = X^6 - X^5 + 6X^2 - 13X + 7.$$

8. Bestimme alle irreduziblen Polynome vom Grad ≤ 3 im Polynomring $\mathbb{F}_2[X]$.

9. Betrachte für eine Primzahl $p \in \mathbb{N}$ die folgende Teilmenge des Körpers $\mathbb{Q}$ der rationalen Zahlen:

$$\mathbb{Z}_p := \{0\} \cup \left\{ \frac{x}{y} \in \mathbb{Q} \,;\, x, y \in \mathbb{Z} - \{0\} \text{ mit } \nu_p(x) - \nu_p(y) \geq 0 \right\}$$

   Zeige: $\mathbb{Z}_p$ ist ein Unterring von $\mathbb{Q}$, ein Hauptidealring, aber kein Körper. Gib alle Einheiten sowie alle Primelemente von $\mathbb{Z}_p$ an.

10. Zeige: Ein Ring R ist genau dann noethersch in dem Sinne, dass jede aufsteigende Kette von Idealen $\mathfrak{a}_1 \subset \mathfrak{a}_2 \subset \ldots \subset R$ stationär wird, wenn jedes Ideal in R ein endliches Erzeugendensystem besitzt.

2.5 Polynomringe in mehreren Variablen

In 2.1 hatten wir zu einem Ring R den Polynomring $R[X]$ in einer Variablen X betrachtet. Durch Iteration könnte man den Polynomring in n Variablen $X_1, \ldots, X_n$ über R konstruieren:

$$R[X_1, \ldots, X_n] := \big(\ldots \big((R[X_1])[X_2] \big) \ldots \big)[X_n].$$

Andererseits ist es möglich, die Definition aus 2.1 in direkter Weise auf den Fall mehrerer Variablen zu verallgemeinern. Und zwar wollen wir im Folgenden für ein kommutatives Monoid M einen "Polynomring" $R[M]$ definieren, derart dass M als das (multiplikative) Monoid der "Monome" in $R[M]$ angesehen werden kann. Für $M = \mathbb{N}$ werden wir auf diese Weise den Polynomring $R[X]$ in einer Variablen erhalten, für $M = \mathbb{N}^n$ den Polynomring $R[X_1, \ldots, X_n]$ in n Variablen und für $M = \mathbb{N}^{(I)}$ den Polynomring $R[\mathfrak{X}]$ in einem durch eine beliebige Indexmenge I indizierten System von Variablen $\mathfrak{X} = (X_i)_{i \in I}$. Dabei betrachte man auf $\mathbb{N}$, $\mathbb{N}^n$, $\mathbb{N}^{(I)}$ jeweils die (komponentenweise) Addition als Monoidverknüpfung.

Es sei im Folgenden M ein beliebiges kommutatives Monoid, dessen Verknüpfung wir als *Addition* schreiben, mit 0 als neutralem Element. Sodann erkläre man $R[M]$ durch

$$R[M] = R^{(M)} = \left\{ (a_\mu)_{\mu \in M} \,;\, a_\mu \in R,\ a_\mu = 0 \text{ für fast alle } \mu \right\}$$

mit den Verknüpfungen

$$(a_\mu)_{\mu\in M} + (b_\mu)_{\mu\in M} := (a_\mu + b_\mu)_{\mu\in M}, \quad (a_\mu)_{\mu\in M} \cdot (b_\mu)_{\mu\in M} := (c_\mu)_{\mu\in M},$$

wobei

$$c_\mu = \sum_{\lambda+\nu=\mu} a_\lambda \cdot b_\nu.$$

Man prüft ohne Schwierigkeiten nach, dass $R[M]$ unter diesen Verknüpfungen ein Ring ist. Dabei ist $0 = (0)_{\mu\in M}$ das Nullelement und $(\delta_{\mu,0})_{\mu\in M}$ das Einselement in $R[M]$; wie üblich bezeichnet $\delta_{\mu,\nu}$ für $\mu, \nu \in M$ das Kronecker-Symbol, d. h. man hat $\delta_{\mu,\nu} = 1$ für $\mu = \nu$ und $\delta_{\mu,\nu} = 0$ für $\mu \neq \nu$. Auch kann man R als Unterring von $R[M]$ auffassen, indem man R mit seinem Bild unter dem Monomorphismus $R \hookrightarrow R[M], a \longmapsto (a \cdot \delta_{\mu,0})_{\mu\in M}$, identifiziert.

Für das Monoid $M = \mathbb{N}$ der natürlichen Zahlen ergibt sich der bereits in 2.1 konstruierte Polynomring einer Variablen $R[X]$. Aber auch in den übrigen Fällen kann man in $R[M]$ eine Polynom-Schreibweise einführen: Für $\nu \in M$ wird $X^\nu := (\delta_{\mu,\nu})_{\mu\in M} \in R[M]$ als das zu ν gehörige *Monom* bezeichnet, wobei $X^\mu \cdot X^\nu = X^{\mu+\nu}$ für Exponenten $\mu, \nu \in M$ gilt. So sieht man, dass die Abbildung $\iota\colon M \longrightarrow R[M], \mu \longmapsto X^\mu$, einen bijektiven Homomorphismus zwischen dem additiven Monoid M und dem multiplikativen Monoid der Monome in $R[M]$ induziert. Sehen wir diese Bijektion als Identifizierung an, so können wir M als Monoid der Monome in $R[M]$ auffassen. Dabei ist zu beachten, dass das Symbol X ohne einen Exponenten $\mu \in M$ normalerweise kein Element von $R[M]$ beschreiben wird, es sein denn, M enthält ein geeignetes Element "1". Wir können dann nämlich $X := X^1$ setzen, wie etwa im Fall des Polynomrings einer Variablen $R[X] = R[M]$ mit $M = \mathbb{N}$.

Unter Verwendung der Monome X^μ, $\mu \in M$, lassen sich die Elemente aus $R[M]$ in der Form $\sum_{\mu\in M} a_\mu X^\mu$ schreiben mit eindeutig bestimmten Koeffizienten $a_\mu \in R$, die für fast alle $\mu \in M$ verschwinden. Genau wie für Polynome einer Variablen X hat man für Addition und Multiplikation die bekannten Formeln:

$$\sum_{\mu\in M} a_\mu X^\mu + \sum_{\mu\in M} b_\mu X^\mu = \sum_{\mu\in M} (a_\mu + b_\mu) X^\mu,$$
$$\sum_{\mu\in M} a_\mu X^\mu \cdot \sum_{\mu\in M} b_\mu X^\mu = \sum_{\mu\in M} \Big(\sum_{\lambda+\nu=\mu} a_\lambda \cdot b_\nu \Big) X^\mu.$$

In gewohnter Weise dient das Nullpolynom $0 = \sum_{\mu \in M} 0 \cdot X^\mu$ als Nullelement und entsprechend X^0 als Einselement in $R[M]$, wobei der Exponent "0" das neutrale Element im Monoid M bezeichnet.

Satz 1 (Universelle Eigenschaft von Polynomringen). *Der Polynomring $R[M]$ über einem Ring R und zu einem kommutativen Monoid M besitzt zusammen mit seinen strukturgebenden Homomorphismen $R \hookrightarrow R[M]$ und $\iota\colon M \longrightarrow R[M]$, $\mu \longmapsto X^\mu$, folgende universelle Abbildungseigenschaft*:

Sei $\varphi\colon R \longrightarrow R'$ ein Ringhomomorphismus und $\sigma\colon M \longrightarrow R'$ ein Monoidhomomorphismus, wobei R' für die Abbildung σ als Monoid unter der Ringmultiplikation aufgefasst werde. Dann existiert ein eindeutig bestimmter Ringhomomorphismus $\Phi\colon R[M] \longrightarrow R'$ mit $\Phi|_R = \varphi$ und $\Phi \circ \iota = \sigma$, bzw. $\Phi(X^\mu) = \sigma(\mu)$ für alle $\mu \in M$.

Beweis. Zum Nachweis der Eindeutigkeitsaussage betrachte man ein Element $\sum_{\mu \in M} a_\mu X^\mu \in R[M]$. Wenn dann ein Homomorphismus Φ mit den geforderten Eigenschaften existiert, so folgt notwendig

$$\Phi\Big(\sum a_\mu X^\mu\Big) = \sum \Phi(a_\mu X^\mu) = \sum \Phi(a_\mu)\Phi(X^\mu) = \sum \varphi(a_\mu)\sigma(\mu).$$

Umgekehrt kann man natürlich, um die Existenzaussage zu erhalten, Φ durch diese Gleichung definieren. Die Eigenschaften eines Ringhomomorphismus prüft man ohne Schwierigkeiten nach, indem man benutzt, dass φ ein Ringhomomorphismus und σ ein Monoidhomomorphismus ist. □

Die in Satz 1 bewiesene Aussage wird als die *universelle Eigenschaft* von Polynomringen bezeichnet, da sie den Polynomring $R[M]$ sozusagen als universellen Ring charakterisiert, der bezüglich kanonischer Homomorphismen über allen ähnlichen Konstrukten mit Koeffizienten aus R und von M induzierten Monomen liegt. Insbesondere charakterisiert die universelle Eigenschaft $R[M]$ bis auf kanonische Isomorphie. Genauer bedeutet dies folgendes: Man gehe aus von einer Ringerweiterung $R \subset S$ und einem Monoidhomomorphismus $\kappa\colon M \longrightarrow S$ mit S als Monoid unter der Ringmultiplikation und nehme an, dass die in Satz 1 beschriebene Abbildungseigenschaft gegeben ist, dass es also zu jedem Ringhomomorphismus $\psi\colon R \longrightarrow R'$ und zu jedem Monoidhomomorphismus $\tau\colon M \longrightarrow R'$ mit R' als Monoid unter der Multiplikation genau einen Ringhomomorphismus

$\Psi\colon S \longrightarrow R'$ mit $\Psi|_R = \psi$ und $\Psi \circ \kappa = \tau$ gibt. Dann sind die Erweiterungen $R \subset R[M]$ und $R \subset S$ kanonisch isomorph.

Wir wollen dies hier kurz begründen, und zwar mit der üblichen Argumentation, die auch für andere universelle Eigenschaften anwendbar ist. Zu $R \hookrightarrow S$ und $\kappa\colon M \longrightarrow S$ korrespondiert aufgrund der universellen Eigenschaft von $R[M]$ ein Ringhomomorphismus $\Phi\colon R[M] \longrightarrow S$, der die Identität auf R fortsetzt und für den $\Phi \circ \iota = \kappa$ gilt. Umgekehrt erhält man aus der universellen Eigenschaft von S und dem Monoidhomomorphismus $\iota\colon M \longrightarrow R[M], \mu \longmapsto X^\mu$, einen Ringhomomorphismus $\Psi\colon S \longrightarrow R[M]$, der die Identität auf R fortsetzt und $\Psi \circ \kappa = \iota$ erfüllt. Sodann gilt

$$(\Phi \circ \Psi) \circ \kappa = \Phi \circ (\Psi \circ \kappa) = \Phi \circ \iota = \kappa = \mathrm{id} \circ \kappa,$$

d. h. $\Phi \circ \Psi$ und die identische Abbildung sind zwei Ringhomomorphismen $S \longrightarrow S$, die die Identität auf R fortsetzen und die unter Komposition mit κ übereinstimmen. Aus der Eindeutigkeitsaussage der universellen Abbildungseigenschaft für S ergibt sich sodann $\Phi \circ \Psi = \mathrm{id}$. Entsprechend schließt man aus der Eindeutigkeitsaussage der universellen Abbildungseigenschaft für $R[M]$ auf die Relation $\Psi \circ \Phi = \mathrm{id}$, und es folgt, dass Φ und Ψ Isomorphismen sind.

Wir wollen nun $M = \mathbb{N}^n$ oder $M = \mathbb{N}^{(I)}$ setzen, also Polynomringe im engeren Sinne betrachten. Im Falle $M = \mathbb{N}^n$ erklären wir für $1 \leq i \leq n$ die i-te "Variable" X_i durch $X^{(0,\ldots,0,1,0,\ldots,0)}$, wobei die 1 im Exponenten gerade an der i-ten Stelle stehe. Für $\mu = (\mu_1, \ldots, \mu_n) \in \mathbb{N}^n$ gilt dann $X^\mu = X_1^{\mu_1} \ldots X_n^{\mu_n}$, und die Elemente von $R[\mathbb{N}^n]$ schreiben sich ausführlicher in der Form

$$\sum_{(\mu_1,\ldots,\mu_n)\in\mathbb{N}^n} a_{\mu_1,\ldots,\mu_n} X_1^{\mu_1} \ldots X_n^{\mu_n}$$

mit eindeutig bestimmten Koeffizienten $a_{\mu_1,\ldots,\mu_n} \in R$, die fast alle verschwinden. Anstelle von $R[\mathbb{N}^n]$ verwenden wir die Notation $R[X_1, \ldots, X_n]$ oder $R[X]$, wobei wir $X = (X_1, \ldots, X_n)$ als ein System von Variablen auffassen. In ähnlicher Weise verfahren wir im Falle von Monoiden der Form $M = \mathbb{N}^{(I)}$ mit einer beliebigen Indexmenge I. Für $i \in I$ sei ε_i dasjenige Element von $\mathbb{N}^{(I)}$, dessen Komponenten alle verschwinden, bis auf diejenige an der Stelle i, die 1 sei. Setzt man dann $X_i = X^{\varepsilon_i}$, so gilt für $\mu = (\mu_i)_{i\in I} \in \mathbb{N}^{(I)}$ stets $X^\mu = \prod_{i\in I} X_i^{\mu_i}$, wobei man beachte, dass fast alle Faktoren dieses Produkts gleich 1 sind, das Produkt in Wahrheit also endlich ist. Die Elemente von $R[\mathbb{N}^{(I)}]$ lassen sich daher in der Form

$$\sum_{\mu\in\mathbb{N}^{(I)}} a_\mu \prod_{i\in I} X_i^{\mu_i}$$

schreiben, und zwar mit eindeutig bestimmten Koeffizienten $a_\mu \in R$, die fast alle verschwinden. Anstelle von $R[\mathbb{N}^{(I)}]$ verwenden wir auch die Notation $R[X_i\,;\, i \in I]$ oder $R[\mathfrak{X}]$ mit $\mathfrak{X} = (X_i)_{i\in I}$. Die Elemente von $R[\mathfrak{X}]$ sind jeweils Polynome in *endlich* vielen Variablen $X_{i_1}, \ldots, X_{i_n}$, und wir können $R[\mathfrak{X}]$ als Vereinigung aller Unterringe des Typs $R[X_{i_1}, \ldots, X_{i_n}]$ auffassen, wobei die Menge $\{i_1, \ldots, i_n\}$ über alle endlichen Teilmengen von I variiert. Insbesondere lassen sich Rechnungen, die nur endlich viele Elemente von $R[\mathfrak{X}]$ betreffen, stets in einem Polynomring in endlich vielen Variablen durchführen.

Wir werden Polynomringe in unendlich vielen Variablen im Wesentlichen nur zur Konstruktion algebraisch abgeschlossener Körper in Abschnitt 3.4 benötigen. Deswegen wollen wir uns im Folgenden der Einfachheit halber auf Polynomringe des Typs $R[X_1, \ldots, X_n]$ beschränken, obwohl die Resultate, die wir nachfolgend beweisen, in entsprechender Version auch für Polynomringe in beliebig vielen Variablen gültig sind. Zunächst stellt man fest, entweder durch direkte Rechnung oder unter Verwendung der universellen Eigenschaft aus Satz 1 (vgl. auch Aufgabe 3), dass man für $n > 0$ stets einen kanonischen Isomorphismus

$$R[X_1, \ldots, X_n] \simeq \big(R[X_1, \ldots, X_{n-1}]\big)[X_n]$$

hat; dabei ist $R[X_1, \ldots, X_{n-1}]$ für $n = 1$ als R zu interpretieren. Dieser Isomorphismus gestattet es in manchen Fällen, Probleme über Polynome in mehreren Variablen in induktiver Weise auf Probleme in einer Variablen zurückzuführen.

Satz 2. *Ist R ein Integritätsring, so auch der Polynomring in endlich vielen Variablen $R[X_1, \ldots, X_n]$.*

Beweis. Wir hatten bereits in 2.1/3 eingesehen, dass die Behauptung im Falle einer Variablen richtig ist. Benutzt man den Isomorphismus

$$R[X_1, \ldots, X_n] \simeq \big(R[X_1, \ldots, X_{n-1}]\big)[X_n],$$

so ergibt sich daraus der Allgemeinfall mit Induktion nach der Anzahl der Variablen.

Man kann aber auch in direkter Weise sehen, dass das Produkt zweier von Null verschiedener Polynome

$$f = \sum a_\mu X^\mu, \quad g = \sum b_\nu X^\nu \quad \in R[X_1, \ldots, X_n]$$

nicht verschwindet, wenn R ein Integritätsring ist. Hierzu ordne man die Indexmenge $\mathbb{N}^n$ lexikographisch, d. h. man schreibe $\mu < \mu'$ für Indizes

$$\mu = (\mu_1, \ldots, \mu_n), \quad \mu' = (\mu'_1, \ldots, \mu'_n) \quad \in \mathbb{N}^n,$$

wenn für ein gewisses i, $1 \le i \le n$,

$$\mu_1 = \mu'_1, \quad \ldots, \quad \mu_{i-1} = \mu'_{i-1}, \quad \mu_i < \mu'_i,$$

gilt. Ist dann $\overline{\mu} \in \mathbb{N}$ maximal (bezüglich lexikographischer Ordnung) unter allen μ mit $a_\mu \neq 0$, ebenso $\overline{\nu}$ maximal mit $b_\nu \neq 0$, so ist der Koeffizient des Monoms $X^{\overline{\mu}+\overline{\nu}}$ in fg gerade $a_{\overline{\mu}} b_{\overline{\nu}}$. Wenn R ein Integritätsring ist, folgt $a_{\overline{\mu}} b_{\overline{\nu}} \neq 0$ und somit $fg \neq 0$. □

Wir schreiben im Folgenden $|\mu| := \mu_1 + \ldots + \mu_n$ für den "Betrag" eines Elementes $\mu = (\mu_1, \ldots, \mu_n) \in \mathbb{N}^n$. Ist $f = \sum a_\mu X^\mu$ ein Polynom in $R[X_1, \ldots, X_n]$, so bezeichnet man für $i \in \mathbb{N}$ mit $f_i := \sum_{|\mu|=i} a_\mu X^\mu$ den *homogenen Bestandteil von f vom Grad i*. Es ist also f Summe seiner homogenen Bestandteile, d. h. $f = \sum_{i=0}^{\infty} f_i$. Man nennt f *homogen*, wenn f gleich einem seiner homogenen Bestandteile ist, genauer *homogen vom Grad i*, wenn $f = f_i$ gilt. Ein homogenes Polynom $f \neq 0$ ist stets homogen von einem eindeutig bestimmten Grad $i \ge 0$, das Nullpolynom jedoch ist homogen von *jedem* Grad $i \ge 0$. Weiter heißt

$$\operatorname{grad} f = \max\{i \in \mathbb{N} \,;\, f_i \neq 0\} = \max\{|\mu| \,;\, a_\mu \neq 0\}$$

der *Totalgrad* von f, wobei $\operatorname{grad} f := -\infty$ gesetzt wird für $f = 0$. Im Falle einer Variablen stimmt der Totalgrad mit dem in 2.1 definierten Grad eines Polynoms überein. Analog zu 2.1/2 erhält man:

Satz 3. *Seien $f, g \in R[X_1, \ldots, X_n]$. Dann gilt*

$$\operatorname{grad}(f+g) \le \max(\operatorname{grad} f, \operatorname{grad} g),$$
$$\operatorname{grad}(f \cdot g) \le \operatorname{grad} f + \operatorname{grad} g$$

und sogar $\operatorname{grad}(f \cdot g) = \operatorname{grad} f + \operatorname{grad} g$, *wenn R ein Integritätsring ist.*

Beweis. Die Abschätzung für $\operatorname{grad}(f+g)$ ist unmittelbar klar, wenn man Polynome in $R[X_1,\dots,X_n]$ als Summe ihrer homogenen Bestandteile schreibt. Gilt weiter $\operatorname{grad} f = r$ und $\operatorname{grad} g = s$, und sind $f = \sum_{i=0}^{r} f_i$, $g = \sum_{i=0}^{s} g_i$ Zerlegungen in homogene Bestandteile, so hat man für Indizes $r, s \geq 0$

$$f \cdot g = f_r \cdot g_s + (\text{homogene Bestandteile vom Grad } < r+s),$$

wobei $f_r \cdot g_s$ der homogene Bestandteil vom Grad $r+s$ in $f \cdot g$ ist. Somit folgt $\operatorname{grad}(f \cdot g) \leq \operatorname{grad} f + \operatorname{grad} g$. Ist R Integritätsring, so hat man mit $f_r, g_s \neq 0$ nach Satz 2 auch $f_r g_s \neq 0$, so dass sich der Grad von fg zu $r+s$ berechnet. □

Als direkte Folgerung ergibt sich:

Korollar 4. *Ist R ein Integritätsring, so gilt*

$$\big(R[X_1,\dots,X_n]\big)^* = R^*.$$

Wir wollen schließlich noch die universelle Eigenschaft aus Satz 1, durch welche Polynomringe bis auf kanonische Isomorphie eindeutig charakterisiert sind, speziell für Polynomringe des Typs $R[X_1,\dots,X_n]$ formulieren. Da ein Monoidhomomorphismus $\sigma\colon \mathbb{N}^n \longrightarrow R'$ bereits durch die Bilder der kanonischen "Erzeugenden" von $\mathbb{N}^n$ bestimmt ist, also durch die Bilder der Elemente des Typs $(0,\dots,0,1,0,\dots,0)$, erhält man aus Satz 1 folgende Version:

Satz 5. *Es sei $\varphi\colon R \longrightarrow R'$ ein Ringhomomorphismus, weiter seien Elemente $x_1,\dots,x_n \in R'$ gegeben. Dann existiert eindeutig ein Ringhomomorphismus $\Phi\colon R[X_1,\dots,X_n] \longrightarrow R'$ mit $\Phi|_R = \varphi$ und $\Phi(X_i) = x_i$ für $i = 1,\dots,n$.*

Setzt man $x = (x_1,\dots,x_n)$ und $x^\mu = x_1^{\mu_1}\dots x_n^{\mu_n}$ für $\mu \in \mathbb{N}^n$, so lässt sich Φ wie im Falle einer Variablen durch

$$\Phi\colon R[X_1,\dots,X_n] \longrightarrow R', \qquad \sum a_\mu X^\mu \longmapsto \sum \varphi(a_\mu) x^\mu,$$

beschreiben. Man nennt Φ einen *Einsetzungs-* oder *Substitutionshomomorphismus*, da für X das Tupel x substituiert wird. Ist speziell R ein Unterring von R' und $\varphi\colon R \hookrightarrow R'$ die kanonische Inklusion, so bezeichnet man für

$f = \sum a_\mu X^\mu \in R[X_1, \ldots, X_n]$ das Bild unter Φ auch mit $f(x) = \sum a_\mu x^\mu$. Gilt $f(x) = 0$, so heißt x eine *Nullstelle* von f. Weiter schreibt man

$$\begin{aligned} R[x] &:= \Phi\big(R[X_1, \ldots, X_n]\big) \\ &= \left\{ \sum a_\mu x^\mu \,;\, a_\mu \in R,\ a_\mu = 0 \text{ für fast alle } \mu \right\} \end{aligned}$$

für das Bild von $R[X_1, \ldots, X_n]$ unter Φ. Es ist $R[x]$ oder in ausführlicher Schreibweise $R[x_1, \ldots, x_n]$ der kleinste Unterring von R', welcher R und alle Komponenten $x_1, \ldots, x_n$ von x enthält. In suggestiver Weise spricht man von $R[x]$ auch als dem Ring aller Polynome in x (besser, aller polynomialen Ausdrücke in x), wobei R als Koeffizientenbereich dient.

Einsetzungshomomorphismen werden im weiteren Verlaufe eine wichtige Rolle spielen. Als Beispiel wollen wir bereits an dieser Stelle auf den Begriff der *Transzendenz* eingehen.

Definition 6. *Sei $R \subset R'$ eine Ringerweiterung und $x = (x_1, \ldots, x_n)$ ein System von Elementen von R'. Das System x heißt* algebraisch unabhängig *oder* transzendent *über R, wenn für ein System von Variablen $X = (X_1, \ldots, X_n)$ der zugehörige Ringhomomorphismus $R[X] \longrightarrow R'$, $f \longmapsto f(x)$, injektiv ist und somit einen Isomorphismus $R[X] \xrightarrow{\sim} R[x]$ induziert. Anderenfalls bezeichnet man x als* algebraisch abhängig *über R.*

Ein über R transzendentes System $x = (x_1, \ldots, x_n)$ hat somit die Eigenschaften eines Systems von Variablen. Wir haben bereits in der Einführung erwähnt, dass z. B. die aus der Analysis bekannten Zahlen e und $\pi \in \mathbb{R}$ jeweils transzendent über $\mathbb{Q}$ sind; Beweise hierfür gehen zurück auf Ch. Hermite [8] und F. Lindemann [12].

Schließlich wollen wir noch auf die *Reduktion der Koeffizienten* von Polynomen hinweisen. Es handelt sich dabei um Homomorphismen, die formal auch unter den Typus der Einsetzungshomomorphismen fallen. Ist $\mathfrak{a} \subset R$ ein Ideal und $\varphi\colon R \longrightarrow R/\mathfrak{a}$ der kanonische Homomorphismus, so kann man gemäß Satz 5 den Homomorphismus $\Phi\colon R[X] \longrightarrow (R/\mathfrak{a})[X]$ betrachten, der φ fortsetzt und X auf X abbildet; dabei sei X eine einzelne Variable oder auch ein System $X = (X_1, \ldots, X_n)$ von Variablen. Man sagt, dass Φ die Koeffizienten von Polynomen aus $R[X]$ modulo dem Ideal $\mathfrak{a}$ reduziert. So führt etwa für eine Primzahl p der Homomorphismus $\mathbb{Z}[X] \longrightarrow \mathbb{Z}/(p)[X]$ Polynome mit ganzzahligen Koeffizienten über in Polynome mit Koeffizienten aus dem Körper $\mathbb{F}_p = \mathbb{Z}/(p)$.

Lernkontrolle und Prüfungsvorbereitung

1. Es sei R ein Ring und M ein kommutatives Monoid. Was versteht man unter dem "Polynomring" $R[M]$? Wie ist der Polynomring $R[X_1, \ldots, X_n]$ in n Variablen $X_1, \ldots, X_n$ über R definiert?
2. Zeige für den Nullring $R = 0$, dass auch der Polynomring $R[X_1, \ldots, X_n]$ in n Variablen $X_1, \ldots, X_n$ über R der Nullring ist.
3. Was versteht man unter der universellen Eigenschaft des Polynomrings $R[X_1, \ldots, X_n]$ in n Variablen über einem Ring R? Gib einen Beweis für diese Eigenschaft. Was versteht man in diesem Zusammenhang unter einem Einsetzungshomomorphismus?
4. Zeige für einen Integritätsring R, dass auch der Polynomring $R[X_1, \ldots, X_n]$ in n Variablen $X_1, \ldots, X_n$ über R ein Integritätsring ist.
5. Was versteht man unter einem homogenen Polynom in n Variablen $X_1, \ldots, X_n$ über einem Ring R?
6. Was versteht man unter dem Totalgrad eines Polynoms in n Variablen $X_1, \ldots, X_n$ über einem Ring R? Wie verhält sich dieser Grad unter Addition bzw. Multiplikation solcher Polynome?
7. Wie berechnet sich die Einheitengruppe $(R[X_1, \ldots, X_n])^*$ eines Polynomrings in n Variablen $X_1, \ldots, X_n$ über einem Integritätsring R?
8. Es sei $R \subset R'$ eine Ringerweiterung und $x = (x_1, \ldots, x_n)$ ein System von Elementen aus R'. Wann wird das System x als algebraisch unabhängig über R bezeichnet?
9. Erläutere das Prinzip der Reduktion von Koeffizienten bei Polynomringen.

Übungsaufgaben

1. *Wir haben für ein kommutatives Monoid M den Polynomring $R[M]$ über einem Ring R definiert. Was ist zu beachten, wenn man $R[M]$ auch für nicht notwendig kommutative Monoide M erklären möchte?*
2. *Untersuche, inwieweit sich die in diesem Abschnitt bewiesenen Resultate für Polynomringe der Form $R[X_1, \ldots, X_n]$ auf Polynomringe in beliebig vielen Variablen $R[\mathfrak{X}]$ verallgemeinern lassen.*
3. *Betrachte für zwei Monoide M, M' das kartesische Produkt $M \times M'$ als Monoid unter komponentenweiser Verknüpfung und zeige, dass es einen kanonischen Ringisomorphismus $R[M][M'] \xrightarrow{\sim} R[M \times M']$ gibt.*

4. Es sei R ein Ring. Betrachte $\mathbb{Z}$ sowie $\mathbb{Z}/m\mathbb{Z}$ für $m > 0$ jeweils als Monoid unter der Addition und zeige:

$$R[\mathbb{Z}] \simeq R[X,Y]\big/(1-XY), \qquad R[\mathbb{Z}/m\mathbb{Z}] \simeq R[X]\big/(X^m-1).$$

5. Sei K ein Körper und $f \in K[X_1,\ldots,X_n]$ ein homogenes Polynom vom Totalgrad $d > 0$. Zeige, dass für jede Primfaktorzerlegung $f = p_1 \ldots p_r$ die Faktoren p_i homogen sind.

6. Betrachte den Polynomring $R[X_1,\ldots,X_n]$ in n Variablen über einem Ring $R \neq 0$ und zeige: Die Anzahl der Monome in $R[X_1,\ldots,X_n]$ vom Totalgrad $d \in \mathbb{N}$ ist
$$\binom{n+d-1}{n-1}.$$

7. Sei K ein Körper und $\varphi\colon K[X_1,\ldots,X_m] \longrightarrow K[X_1,\ldots,X_n]$ ein Ringisomorphismus mit $\varphi|_K = \mathrm{id}_K$. Zeige, es gilt $m = n$.

2.6 Nullstellen von Polynomen

Es sei K ein Körper und $f \in K[X]$ ein von Null verschiedenes Polynom einer Variablen X. Ist $\alpha \in K$ Nullstelle von f, gilt also $f(\alpha) = 0$, so ist das Polynom $X - \alpha$ ein Teiler von f. Denn Division mit Rest von f durch $X - \alpha$ ergibt eine polynomiale Gleichung

$$f = q \cdot (X - \alpha) + c$$

mit $\operatorname{grad} c < 1$, also $c \in K$, und Einsetzen von α zeigt $c = 0$. Es heißt α eine *Nullstelle der Vielfachheit* r, wenn $X - \alpha$ in der Primfaktorzerlegung von f genau mit r-ter Potenz vorkommt. Somit folgt aus Gradgründen:

Satz 1. *Es sei K ein Körper und $f \in K[X]$ ein Polynom vom Grad $n \geq 0$. Dann hat f, gezählt mit Vielfachheiten, höchstens n Nullstellen in K. Die Anzahl ist genau dann gleich n, wenn f in $K[X]$ vollständig in Linearfaktoren zerfällt.*

Insbesondere folgt für $n \in \mathbb{N}$, dass ein Polynom vom Grad $\leq n$ bereits dann das Nullpolynom ist, wenn es mehr als n Nullstellen besitzt. Ist daher K ein unendlicher Körper, so ist für ein Polynom $f \in K[X]$ die Gleichung

$f = 0$ (Nullpolynom) äquivalent zu $f(\alpha) = 0$ für alle $\alpha \in K$ (bzw. für alle α aus einer gegebenen unendlichen Teilmenge von K). Dagegen ist für einen endlichen Körper $\mathbb{F}$ das Polynom

$$f = \prod_{a \in \mathbb{F}} (X - a) \in \mathbb{F}[X]$$

ein vom Nullpolynom verschiedenes Polynom mit $f(\alpha) = 0$ für alle $\alpha \in \mathbb{F}$.

Wir wollen ein Kriterium für das Vorliegen mehrfacher Nullstellen angeben. Hierzu betrachten wir die Abbildung

$$D\colon K[X] \longrightarrow K[X], \qquad \sum_{i=0}^{n} c_i X^i \longmapsto \sum_{i=1}^{n} i c_i X^{i-1},$$

wobei ic_i wie üblich die i-fache Summe von c_i mit sich selbst bezeichnet. Über den Körpern $\mathbb{R}$ oder $\mathbb{C}$ beschreibt D die Bildung der aus der Analysis bekannten Ableitung polynomialer Funktionen. Wir wollen aber auch für den Allgemeinfall zeigen, dass D die Eigenschaften einer "Ableitung" besitzt.

Lemma 2. *Die Abbildung $D\colon K[X] \longrightarrow K[X]$ genügt den Bedingungen einer K-*Derivation, *nämlich*

(i) *D ist K-linear, d. h. für $a, b \in K$, $f, g \in K[X]$ gilt*

$$D(af + bg) = aD(f) + bD(g),$$

(ii) *D erfüllt die Produktregel, d. h. für $f, g \in K[X]$ gilt*

$$D(fg) = fD(g) + gD(f).$$

Beweis. Die K-Linearität von D ist unmittelbar aus der Definition ersichtlich. Um auch die Produktregel für Polynome $f, g \in K[X]$ herzuleiten, bemerken wir zunächst, dass beide Seiten dieser Gleichung symmetrisch in f und g sind. Sodann gilt die Produktregel trivialerweise für Monome $f = X^m$ und $g = X^n$:

$$\begin{aligned} D(X^m \cdot X^n) &= D(X^{m+n}) = (m+n) \cdot X^{m+n-1} \\ &= n \cdot X^m \cdot X^{n-1} + m \cdot X^n \cdot X^{m-1} \\ &= X^m \cdot D(X^n) + X^n \cdot D(X^m) \end{aligned}$$

Seien nun $f_1, f_2, g \in K[X]$ Polynome, so dass die Produktregel für die Paare (f_1, g) und (f_2, g) gilt. Wir können dann unter Nutzung der Linearität von D zeigen, dass diese Regel auch für das Paar $(f_1 + f_2, g)$ gilt:

$$\begin{aligned} D\big((f_1 + f_2) \cdot g\big) &= D(f_1 \cdot g + f_2 \cdot g) = D(f_1 \cdot g) + D(f_2 \cdot g) \\ &= \big(f_1 \cdot D(g) + g \cdot D(f_1)\big) + \big(f_2 \cdot D(g) + g \cdot D(f_2)\big) \\ &= (f_1 + f_2) \cdot D(g) + g \cdot D(f_1 + f_2) \end{aligned}$$

Mit diesen beiden Einzelschritten leitet man die Produktregel nun leicht für Paare des Typs $f, X^n \in K[X]$ her, sowie anschließend für allgemeine Paare $f, g \in K[X]$; man benutze die K-Linearität von D sowie die Symmetrie der Produktregel. □

Statt $D(f)$ schreibt man meist f' und nennt dies die erste *Ableitung* von f.

Satz 3. *Es sei $f \in K[X]$, $f \neq 0$, ein Polynom mit Koeffizienten aus einem Körper K. Eine Nullstelle α von f ist genau dann eine mehrfache Nullstelle (d. h. eine Nullstelle der Vielfachheit ≥ 2), wenn $(f')(\alpha) = 0$ gilt.*

Beweis. Ist $r \geq 1$ die Vielfachheit der Nullstelle α, so gibt es eine Produktzerlegung des Typs $f = (X - \alpha)^r g$ mit $g \in K[X]$, $g(\alpha) \neq 0$. Anwenden der Produktregel aus Lemma 2 auf diese Zerlegung sowie in induktiver Weise auf die Potenz $(X - \alpha)^r$ liefert sodann

$$f' = (X - \alpha)^r g' + r(X - \alpha)^{r-1} g.$$

Daher ist $(f')(\alpha) = 0$ äquivalent zu $r \geq 2$. □

Korollar 4. *Ein Element $\alpha \in K$ ist genau dann eine mehrfache Nullstelle eines Polynoms $f \in K[X] - \{0\}$, wenn α Nullstelle von* $\mathrm{ggT}(f, f')$ *ist.*

Ist z. B. p eine Primzahl, so hat das Polynom $f = X^p - X \in \mathbb{F}_p[X]$ keine mehrfachen Nullstellen. Denn es gilt $f' = -1$, da die p-fache Summe $p \cdot 1$ des Einselementes $1 \in \mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$ verschwindet.

Lernkontrolle und Prüfungsvorbereitung

1. Wie ist die Vielfachheit einer Nullstelle eines Polynoms einer Variablen über einem Körper erklärt? Was ist eine mehrfache Nullstelle?

2. Es sei f ein Polynom einer Variablen vom Grad $n \geq 1$ über einem Körper K, welches n verschiedene Nullstellen in K besitzt. Zeige, dass die Primfaktorzerlegung von f aus n verschiedenen linearen Faktoren besteht.
3. Zeige, dass die Ableitung von Polynomen einer Variablen über einem Körper der Produktregel genügt.
4. Wie lässt sich für Polynome einer Variablen über einem Körper das Vorliegen mehrfacher Nullstellen mit Hilfe der Ableitung charakterisieren?

Übungsaufgaben

1. *Betrachte über einem Körper K mit unendlich vielen Elementen ein Polynom $f \in K[X_1, \ldots, X_n]$, welches auf ganz K^n verschwindet. Zeige $f = 0$, d. h. dass f das Nullpolynom ist.*
2. Sei K ein Körper. Zeige: Zu $n \in \mathbb{N}$, $n > 1$, gibt es in der multiplikativen Gruppe K^* höchstens $n - 1$ Elemente der Ordnung n.
3. Sei K ein Körper. Zeige, es gibt im Polynomring $K[X]$ unendlich viele normierte Primpolynome. Für den Fall, dass jedes nicht-konstante Polynom aus $K[X]$ mindestens eine Nullstelle in K besitzt, zeige weiter, dass K aus unendlich vielen Elementen besteht.
4. Sei K ein Körper und sei $f = X^3 + aX + b \in K[X]$ ein Polynom, welches in $K[X]$ vollständig in Linearfaktoren zerfällt. Zeige: Die Nullstellen von f sind genau dann paarweise verschieden, wenn die "Diskriminante" $\Delta = -4a^3 - 27b^2$ nicht verschwindet.

2.7 Der Satz von Gauß

Ziel dieses Abschnittes ist der Beweis des folgenden Resultats:

Satz 1 (Gauß). *Es sei R ein faktorieller Ring. Dann ist auch der Polynomring in einer Variablen $R[X]$ faktoriell.*

Als direkte Folgerungen erhält man:

Korollar 2. *Ist R ein faktorieller Ring, so ist der Polynomring in endlich vielen Variablen $R[X_1, \ldots, X_n]$ faktoriell.*

Korollar 3. *Ist K ein Körper, so ist der Polynomring in endlich vielen Variablen $K[X_1, \ldots, X_n]$ faktoriell.*

Insbesondere sieht man, dass es faktorielle Ringe gibt, die keine Hauptidealringe sind; man betrachte beispielsweise den Polynomring $K[X, Y]$ in zwei Variablen X, Y über einem Körper K oder den Polynomring einer Variablen $\mathbb{Z}[X]$. Zum Beweis des Satzes von Gauß sind einige Vorbereitungen notwendig. Wir beginnen mit der Konstruktion des *Quotientenkörpers* $Q(R)$ eines Integritätsringes R, wobei wir uns an der Konstruktion rationaler Zahlen als Brüche ganzer Zahlen orientieren. Man betrachte die Menge aller Paare

$$M = \big\{(a, b)\,;\, a \in R,\ b \in R - \{0\}\big\}.$$

Auf M führen wir eine Äquivalenzrelation "$\sim$" ein, indem wir setzen

$$(a, b) \sim (a', b') \quad \Longleftrightarrow \quad ab' = a'b.$$

Die Eigenschaften einer Äquivalenzrelation prüft man leicht nach; es gelten

Reflexivität: $(a, b) \sim (a, b)$ für alle $(a, b) \in M$,
Symmetrie: $(a, b) \sim (a', b') \implies (a', b') \sim (a, b)$,
Transitivität: $(a, b) \sim (a', b'),\ (a', b') \sim (a'', b'') \implies (a, b) \sim (a'', b'')$.

Zum Nachweis der Transitivität etwa führt man folgende Betrachtung durch:

$$\begin{aligned} (a, b) \sim (a', b') \quad &\Longrightarrow \quad ab' = a'b \quad \Longrightarrow \quad ab'b'' = a'bb'', \\ (a', b') \sim (a'', b'') \quad &\Longrightarrow \quad a'b'' = a''b' \quad \Longrightarrow \quad a'bb'' = a''bb', \end{aligned}$$

bzw.

$$(a, b) \sim (a', b'),\ (a', b') \sim (a'', b'') \quad \Longrightarrow \quad ab'b'' = a''bb'.$$

Letztere Gleichung ergibt $ab'' = a''b$, also $(a, b) \sim (a'', b'')$, da R ein Integritätsring ist.

Es ist folglich "$\sim$" eine Äquivalenzrelation und definiert als solche eine Klasseneinteilung auf M; sei

$$Q(R) = M/\!\sim$$

die Menge der Äquivalenzklassen. Für $(a, b) \in M$ bezeichne $\frac{a}{b} \in Q(R)$ die zugehörige Äquivalenzklasse, so dass

$$\frac{a}{b} = \frac{a'}{b'} \quad \Longleftrightarrow \quad ab' = a'b$$

gilt. Man rechnet sofort nach, dass $Q(R)$ unter der gewöhnlichen Addition und Multiplikation von Brüchen

$$\frac{a}{b} + \frac{a'}{b'} = \frac{ab' + a'b}{bb'}, \qquad \frac{a}{b} \cdot \frac{a'}{b'} = \frac{aa'}{bb'},$$

deren Wohldefiniertheit man wie üblich zeigt, ein Körper ist. Es wird $Q(R)$ als *Quotientenkörper* zu R bezeichnet. Weiter ist

$$R \longrightarrow Q(R), \qquad a \longmapsto \frac{a}{1},$$

ein injektiver Ringhomomorphismus, man kann also R als Unterring von $Q(R)$ auffassen. Für $R = \mathbb{Z}$ erhält man natürlich $Q(\mathbb{Z}) = \mathbb{Q}$, also den Körper der rationalen Zahlen. Ist K ein Körper und X eine Variable, so bezeichnet man den Quotientenkörper $Q(K[X])$ als *Körper der rationalen Funktionen* einer Variablen X mit Koeffizienten in K und schreibt $K(X) = Q(K[X])$. Analog betrachtet man rationale Funktionenkörper $K(X_1, \ldots, X_n) = Q(K[X_1, \ldots, X_n])$ in endlich vielen Variablen $X_1, \ldots, X_n$ sowie allgemeiner den Funktionenkörper $K(\mathfrak{X}) = Q(K[\mathfrak{X}])$ in einem System von Variablen $\mathfrak{X} = (X_i)_{i \in I}$.

Die gerade beschriebene Konstruktion des Quotientenkörpers eines Integritätsringes kann in einem allgemeineren Rahmen durchgeführt werden. Man starte mit einem (nicht notwendig nullteilerfreien) Ring R und einem multiplikativen System $S \subset R$, d. h. mit einem multiplikativen Untermonoid von R. Dann kann man ähnlich wie oben den *Bruchring* (im Allgemeinen erhält man keinen Körper)

$$S^{-1}R = \left\{ \frac{a}{s} \,;\, a \in R, s \in S \right\}$$

bilden, wobei man wegen möglicher Nullteiler bezüglich folgender Äquivalenzrelation arbeitet:

$$\frac{a}{s} = \frac{a'}{s'} \quad \Longleftrightarrow \quad \text{es existiert } s'' \in S \text{ mit } as's'' = a'ss''$$

Man schreibt statt $S^{-1}R$ auch R_S und nennt dies die *Lokalisierung* von R nach S. Dabei ist zu beachten, dass die kanonische Abbildung $R \longrightarrow S^{-1}R$

im Allgemeinen einen nicht-trivialen Kern besitzt. Dieser besteht aus allen Elementen $a \in R$, so dass ein $s \in S$ mit $as = 0$ existiert. Im Falle eines Integritätsrings R (dies ist die Situation, die wir im Folgenden hauptsächlich zu betrachten haben) gilt natürlich $Q(R) = S^{-1}R$ für $S := R - \{0\}$.

Bemerkung 4. *Es sei R ein faktorieller Ring, P ein Repräsentantensystem der Primelemente von R. Dann besitzt jedes $\frac{a}{b} \in Q(R)^*$ eine eindeutige Darstellung*

$$\frac{a}{b} = \varepsilon \prod_{p \in P} p^{\nu_p},$$

wobei $\varepsilon \in R^*$ sowie $\nu_p \in \mathbb{Z}$ mit $\nu_p = 0$ für fast alle p. Insbesondere ist $\frac{a}{b} \in R$ äquivalent zu $\nu_p \geq 0$ für alle p.

Beweis. Unter Benutzung der Primfaktorzerlegung für a und b erhält man die Existenz der geforderten Darstellung. Die Eindeutigkeit ergibt sich aus der Eindeutigkeit der Primfaktorzerlegung in R, sofern man Zerlegungen mit $\nu_p \geq 0$ für alle p betrachtet. Auf diesen Fall kann man sich aber durch Multiplikation mit geeigneten nicht-trivialen Elementen aus R beschränken. □

In der Situation von Bemerkung 4 schreiben wir anstelle von ν_p genauer $\nu_p(x)$, falls $x = \frac{a}{b}$, und setzen $\nu_p(0) := \infty$. Für $x, y \in Q(R)$ erhält man dann mit der Eindeutigkeitsaussage in Bemerkung 4 die Gleichung

$$\nu_p(xy) = \nu_p(x) + \nu_p(y).$$

Für Polynome einer Variablen $f = \sum a_i X^i \in Q(R)[X]$ setzen wir weiter

$$\nu_p(f) := \min_i \nu_p(a_i),$$

wobei $f = 0$ äquivalent ist zu $\nu_p(f) = \infty$. Außerdem gehört f genau dann zu $R[X]$, wenn $\nu_p(f) \geq 0$ für alle $p \in P$ gilt. Die folgende Eigenschaft der Funktion $\nu_p(\cdot)$ wird beim Beweis der Faktorialität von $R[X]$ an zentraler Stelle benötigt:

Lemma 5 (Gauß). *Es sei R ein faktorieller Ring und $p \in R$ ein Primelement. Dann gilt für $f, g \in Q(R)[X]$*

$$\nu_p(fg) = \nu_p(f) + \nu_p(g).$$

Beweis. Wie bereits oben bemerkt, ist die Gleichung für konstante Polynome richtig, d. h. für $f, g \in Q(R)$, ja sogar für $f \in Q(R)$ und beliebiges $g \in Q(R)[X]$.

Zum Beweis des Allgemeinfalles darf man $f, g \neq 0$ annehmen. Aufgrund unserer Vorüberlegung darf man weiter ohne Beschränkung der Allgemeinheit f und g mit Konstanten aus $Q(R)^*$ multiplizieren. So kann man sich die Koeffizienten von f als Brüche vorstellen und f mit dem kleinsten gemeinsamen Vielfachen aller auftretenden Nenner multiplizieren, entsprechend für g. Auf diese Weise kann man annehmen, dass f und g Polynome mit Koeffizienten aus R sind. Dividiert man dann noch jeweils durch den größten gemeinsamen Teiler der Koeffizienten von f bzw. g, so erhält man folgende Situation:

$$f, g \in R[X], \qquad \nu_p(f) = 0 = \nu_p(g),$$

und es ist $\nu_p(fg) = 0$ zu zeigen. Hierzu betrachte man den Homomorphismus

$$\Phi\colon R[X] \longrightarrow \big(R/pR\big)[X],$$

welcher die Koeffizienten reduziert. Es besteht $\ker \Phi$ aus allen denjenigen Polynomen in $R[X]$, deren Koeffizienten sämtlich durch p teilbar sind, also

$$\ker \Phi = \big\{ f \in R[X] \,;\, \nu_p(f) > 0 \big\}.$$

Wegen $\nu_p(f) = 0 = \nu_p(g)$ hat man dann $\Phi(f), \Phi(g) \neq 0$. Da mit R/pR nach 2.1/3 auch $(R/pR)[X]$ ein Integritätsring ist, folgt

$$\Phi(fg) = \Phi(f) \cdot \Phi(g) \neq 0,$$

also $\nu_p(fg) = 0$. □

Korollar 6. *Es sei R ein faktorieller Ring und $h \in R[X]$ ein normiertes Polynom. Ist dann $h = f \cdot g$ eine Zerlegung von h in normierte Polynome $f, g \in Q(R)[X]$, so gilt bereits $f, g \in R[X]$.*

Beweis. Es gilt $\nu_p(h) = 0$ sowie $\nu_p(f), \nu_p(g) \leq 0$ für jedes Primelement $p \in R$, da f und g normiert sind. Aus dem Lemma von Gauß folgt

$$\nu_p(f) + \nu_p(g) = \nu_p(h) = 0,$$

so dass sogar $\nu_p(f) = \nu_p(g) = 0$ für alle p und damit $f, g \in R[X]$ gilt. □

Wir nennen ein Polynom $f \in R[X]$ mit Koeffizienten aus einem faktoriellen Ring R *primitiv*, wenn der größte gemeinsame Teiler aller Koeffizienten von f gleich 1 ist, d. h. wenn $\nu_p(f) = 0$ für alle Primelemente $p \in R$ gilt. Beispielsweise sind normierte Polynome in $R[X]$ primitiv. Auch können wir ähnlich wie in Korollar 6 für ein Polynom $h \in R[X]$ und eine Zerlegung $h = f \cdot g$ in ein primitives Polynom $f \in R[X]$ und ein weiteres Polynom $g \in Q(R)[X]$ bereits $g \in R[X]$ schließen.

Wir werden im Folgenden häufiger benutzen, dass sich jedes von 0 verschiedene Polynom $f \in Q(R)[X]$ in der Form $f = a\tilde{f}$ mit einer Konstanten $a \in Q(R)^*$ und einem primitiven Polynom $\tilde{f} \in R[X]$ schreiben lässt. Man setze nämlich

$$a = \prod_{p \in P} p^{\nu_p(f)}, \qquad \tilde{f} = a^{-1} f,$$

wobei P ein Repräsentantensystem der Primelemente in R sei.

Nach diesen Vorbereitungen sind wir nunmehr in der Lage, den eingangs angekündigten Satz von Gauß zu beweisen, wobei wir gleichzeitig auch die Primelemente in $R[X]$ charakterisieren wollen.

Satz 7 (Gauß). *Es sei R ein faktorieller Ring. Dann ist auch $R[X]$ faktoriell. Ein Polynom $q \in R[X]$ ist genau dann ein Primelement in $R[X]$, wenn gilt*:

(i) *q ist Primelement in R oder*

(ii) *q ist primitiv in $R[X]$ und Primelement in $Q(R)[X]$.*

Insbesondere ist ein primitives Polynom $q \in R[X]$ genau dann prim in $R[X]$, wenn es prim in $Q(R)[X]$ ist.

Beweis. Sei zunächst q ein Primelement in R. Dann ist R/qR und somit auch $R[X]/qR[X] \simeq (R/qR)[X]$ ein Integritätsring, woraus folgt, dass q ein Primelement in $R[X]$ ist.

Als Nächstes betrachte man ein primitives Polynom $q \in R[X]$ mit der Eigenschaft, dass q ein Primelement in $Q(R)[X]$ ist. Um nachzuweisen, dass q auch Primelement in $R[X]$ ist, betrachte man $f, g \in R[X]$ mit $q \mid fg$ in $R[X]$. Dann gilt auch $q \mid fg$ in $Q(R)[X]$. Als Primelement in $Q(R)[X]$ teilt q einen der beiden Faktoren, etwa $q \mid f$, und es existiert ein $h \in Q(R)[X]$ mit $f = qh$. Auf letztere Gleichung wenden wir das Lemma von Gauß an. Da q primitiv ist, folgt für jedes Primelement $p \in R$

$$0 \leq \nu_p(f) = \nu_p(q) + \nu_p(h) = \nu_p(h)$$

und somit $h \in R[X]$, also $q \mid f$ in $R[X]$. Insbesondere ist q ein Primelement in $R[X]$.

Es bleibt jetzt noch nachzuweisen, dass $R[X]$ faktoriell ist und dass jedes Primelement in $R[X]$ vom Typ (i) bzw. (ii) ist. Hierfür reicht es, zu zeigen, dass jedes $f \in R[X]$, welches keine Einheit und nicht Null ist, in ein Produkt von Primelementen der gerade diskutierten Gestalt zerfällt. Um dies einzusehen, schreibe man f in der Gestalt $f = a\tilde{f}$, wobei $a \in R$ der größte gemeinsame Teiler aller Koeffizienten von f ist und $\tilde{f}$ folglich primitiv ist. Da a ein Produkt von Primelementen aus R ist, genügt es, zu zeigen, dass das primitive Polynom $\tilde{f}$ Produkt von primitiven Polynomen aus $R[X]$ ist, die prim in $Q(R)[X]$ sind. Sei $\tilde{f} = c\tilde{f}_1 \ldots \tilde{f}_r$ eine Zerlegung in Primelemente aus $Q(R)[X]$, mit einer Konstanten $c \in Q(R)^*$. Nach geeigneter Wahl von c dürfen wir alle $\tilde{f}_i$ als primitiv in $R[X]$ voraussetzen. Dann gilt aufgrund des Lemmas von Gauß für jedes Primelement $p \in R$

$$\nu_p(\tilde{f}) = \nu_p(c) + \nu_p(\tilde{f}_1) + \ldots + \nu_p(\tilde{f}_r)$$

und wegen

$$\nu_p(\tilde{f}) = \nu_p(\tilde{f}_1) = \ldots = \nu_p(\tilde{f}_r) = 0$$

auch $\nu_p(c) = 0$; d. h. c ist Einheit in R. Ersetzt man nun $\tilde{f}_1$ durch $c\tilde{f}_1$, so sieht man, dass $\tilde{f}$ ein Produkt von Primelementen der gewünschten Form ist. □

Lernkontrolle und Prüfungsvorbereitung

1. Wie ist der Quotientenkörper eines Integritätsrings erklärt?
2. Sei R ein faktorieller Ring mit Quotientenkörper $Q(R)$ und sei P ein Repräsentantensystem der Primelemente in R. Zeige, dass sich jedes Element $x \in Q(R)^*$ in eindeutiger Weise als Produkt $\varepsilon \prod_{p \in P} p^{\nu_p(x)}$ schreiben lässt mit einer Einheit $\varepsilon \in R^*$ und ganzzahligen Exponenten $\nu_p(x) \in \mathbb{Z}$. Wie erklärt man $\nu_p(f)$ für ein Primelement $p \in P$ und ein Polynom $f \in Q(R)[X]$?
3. Wie lautet das Lemma von Gauß für Polynome einer Variablen X über dem Quotientenkörper $Q(R)$ eines faktoriellen Rings R? Was ist die Grundidee des Beweises?
4. Es sei R ein faktorieller Ring. Was versteht man unter einem primitiven Polynom in $R[X]$? Sei $h = f \cdot g$ eine Zerlegung eines Polynoms $h \in R[X]$ in ein primitives Polynom $f \in R[X]$ und ein weiteres Polynom $g \in Q(R)[X]$. Zeige, dass dann bereits $g \in R[X]$ gilt.

5. Wie lassen sich die Primelemente im Polynomring einer Variablen $R[X]$ über einem faktoriellen Ring R charakterisieren?

[+]6. Zeige, dass der Polynomring einer Variablen $R[X]$ über einem faktoriellen Ring R ebenfalls faktoriell ist.

7. Zeige, dass der Polynomring $K[X_1, \ldots, X_n]$ in endlich vielen Variablen über einem Körper K faktoriell ist.

Übungsaufgaben

1. *Sei R ein faktorieller Ring und $\Phi\colon R[X] \longrightarrow R[X]$ ein Ringautomorphismus, der sich zu einem Automorphismus $\varphi\colon R \longrightarrow R$ beschränkt. Vergleiche $\nu_p(f)$ mit $\nu_{\varphi(p)}(\Phi(f))$ für Polynome $f \in R[X]$ und Primelemente $p \in R$ und überlege, ob $\Phi(f)$ primitiv ist, wenn f primitiv ist. Zeige für $a \in R$, dass ein Polynom f genau dann primitiv ist, wenn $f(X+a)$ primitiv ist.*

2. *Es sei R ein faktorieller Ring mit Quotientenkörper K und einem Repräsentantensystem von Primelementen P. Bezeichne für $f \in K[X] - \{0\}$ mit $a_f := \prod_{p \in P} p^{\nu_p(f)}$ den "Inhalt" von f. Formuliere die Aussage des Lemmas von Gauß (Lemma 5) in äquivalenter Form unter Benutzung des Inhalts.*

3. Betrachte den rationalen Funktionenkörper $K(X)$ einer Variablen X über einem Körper K, sowie für eine Variable Y den Polynomring $K(X)[Y]$ über dem Körper $K(X)$. Seien $f(Y), g(Y) \in K[Y]$ teilerfremd mit $\operatorname{grad} f(Y) \cdot g(Y) \geq 1$. Zeige, dass $f(Y) - g(Y)X$ irreduzibel in $K(X)[Y]$ ist.

4. Es sei R ein faktorieller Ring. Zeige:
   (i) Ist $S \subset R$ ein multiplikatives System, so ist auch der Bruchring $S^{-1}R$ faktoriell. Wie verhalten sich die Primelemente von R zu denen von $S^{-1}R$?
   (ii) Für Primelemente $p \in R$ setze man $R_p := S_p^{-1}R$ mit $S_p = R - (p)$. Ein Polynom $f \in R[X]$ ist genau dann primitiv, wenn für jedes Primelement $p \in R$ das induzierte Polynom $f_p \in R_p[X]$ primitiv ist.

5. *Universelle Eigenschaft der Bruchringe*: Sei R ein Ring und $S \subset R$ ein multiplikatives System. Zeige: Zu jedem Ringhomomorphismus $\varphi\colon R \longrightarrow R'$ mit $\varphi(S) \subset R'^*$ gibt es genau einen Ringhomomorphismus $\overline{\varphi}\colon S^{-1}R \longrightarrow R'$ mit $\varphi = \overline{\varphi} \circ \tau$; dabei bezeichne $\tau\colon R \longrightarrow S^{-1}R$ den kanonischen Homomorphismus, gegeben durch $a \longmapsto \frac{a}{1}$.

6. *Partialbruchzerlegung*: Es seien $f, g \in K[X]$ Polynome mit Koeffizienten aus einem Körper K, wobei g normiert sei mit Primfaktorzerlegung $g = g_1^{\nu_1} \ldots g_n^{\nu_n}$

und paarweise nicht-assoziierten Primelementen $g_1, \ldots, g_n$. Zeige, dass es im Quotientenkörper $K(X) = Q(K[X])$ eine eindeutige Darstellung

$$\frac{f}{g} = f_0 + \sum_{i=1}^{n} \sum_{j=1}^{\nu_i} \frac{c_{ij}}{g_i^j}$$

mit Polynomen $f_0, c_{ij} \in K[X]$ gibt, wobei $\operatorname{grad} c_{ij} < \operatorname{grad} g_i$. Sind insbesondere die Primfaktoren g_i linear, so haben die c_{ij} Grad 0, sind also Konstanten. (*Hinweis*: Beweise zunächst die Existenz einer Darstellung $fg^{-1} = f_0 + \sum_{i=1}^{n} f_i g_i^{-\nu_i}$ mit $g_i \nmid f_i$ und $\operatorname{grad} f_i < \operatorname{grad} g_i^{\nu_i}$ und wende dann auf f_i die g_i-adische Entwicklung an, siehe Aufgabe 4 aus 2.1.)

2.8 Irreduzibilitätskriterien

Es sei R ein faktorieller Ring und $K = Q(R)$ sein Quotientenkörper. Wir wollen im Folgenden untersuchen, unter welchen Umständen ein gegebenes Polynom $f \in K[X] - \{0\}$ irreduzibel ist (bzw. prim, was in faktoriellen Ringen nach 2.4/10 ja dasselbe bedeutet). Man kann zu f stets ein $c \in K^*$ wählen, so dass $\tilde{f} = cf$ ein primitives Polynom in $R[X]$ ist, und es folgt mit dem Satz von Gauß 2.7/7, dass f bzw. $\tilde{f}$ genau dann irreduzibel in $K[X]$ ist, wenn $\tilde{f}$ irreduzibel in $R[X]$ ist. Somit kann die Irreduzibilität von Polynomen in $K[X]$ auf die Irreduzibilität von primitiven Polynomen in $R[X]$ zurückgeführt werden.

Satz 1 (Eisensteinsches Irreduzibilitätskriterium). *Es sei R ein faktorieller Ring und $f = a_n X^n + \ldots + a_0 \in R[X]$ ein primitives Polynom vom Grad > 0. Weiter sei $p \in R$ ein Primelement mit*

$$p \nmid a_n, \qquad p \mid a_i \text{ für } i < n, \qquad p^2 \nmid a_0.$$

Dann ist f irreduzibel in $R[X]$ und somit gemäß 2.7/7 auch in $Q(R)[X]$.

Beweis. Angenommen, f ist reduzibel in $R[X]$. Dann gibt es eine Zerlegung

$$f = gh \quad \text{mit} \quad g = \sum_{i=0}^{r} b_i X^i, \; h = \sum_{i=0}^{s} c_i X^i,$$

wobei $r + s = n$, $r > 0$, $s > 0$. Es folgt

$$a_n = b_r c_s \neq 0, \qquad p \nmid b_r, \qquad p \nmid c_s,$$
$$a_0 = b_0 c_0, \qquad p \mid b_0 c_0, \qquad p^2 \nmid b_0 c_0,$$

und wir dürfen etwa $p \mid b_0$, $p \nmid c_0$ annehmen. Es sei nun $t < r$ maximal mit $p \mid b_\tau$ für $0 \leq \tau \leq t$. Setzen wir $b_i = 0$ für $i > r$ und $c_i = 0$ für $i > s$, so gilt

$$a_{t+1} = b_0 c_{t+1} + \ldots + b_{t+1} c_0,$$

und es ist a_{t+1} nicht durch p teilbar, denn $b_0 c_{t+1}, \ldots, b_t c_1$ sind durch p teilbar, nicht aber $b_{t+1} c_0$. Es folgt notwendig $t + 1 = n$, aufgrund unserer Voraussetzung über f, und somit $r = n$, $s = 0$ im Widerspruch zu $s > 0$. □

Weiter wollen wir das sogenannte *Reduktionskriterium* beweisen.

Satz 2. *Es sei R ein faktorieller Ring, $p \in R$ ein Primelement und f ein Polynom in $R[X]$ vom Grad > 0, dessen höchster Koeffizient nicht von p geteilt wird. Weiter sei $\Phi\colon R[X] \longrightarrow R/(p)[X]$ der kanonische Homomorphismus, welcher die Koeffizienten reduziert. Dann gilt:*

Ist $\Phi(f)$ irreduzibel in $R/(p)[X]$, so ist f irreduzibel in $Q(R)[X]$. Ist f zusätzlich primitiv, so ist f irreduzibel in $R[X]$.

Beweis. Wir nehmen zunächst $f \in R[X]$ als primitiv an. Ist dann f reduzibel, so gibt es in $R[X]$ eine Zerlegung $f = gh$ mit $\operatorname{grad} g > 0$ und $\operatorname{grad} h > 0$. Dabei kann p nicht den höchsten Koeffizienten von g bzw. h teilen, da p nicht den höchsten Koeffizienten von f teilt. Also gilt

$$\Phi(f) = \Phi(g)\Phi(h)$$

mit nicht-konstanten Polynomen $\Phi(g)$ und $\Phi(h)$, d. h. es ist $\Phi(f)$ reduzibel. Somit impliziert die Irreduzibilität von $\Phi(f)$ diejenige von f in $R[X]$.

Im Allgemeinfall schreiben wir $f = c \cdot \tilde{f}$ mit einer Konstanten $c \in R$ und einem primitiven Polynom $\tilde{f} \in R[X]$, wobei p weder c noch den höchsten Koeffizienten von $\tilde{f}$ teilen kann. Ist dann $\Phi(f)$ irreduzibel, so auch $\Phi(\tilde{f})$, und es folgt, wie wir gerade gesehen haben, dass $\tilde{f}$ irreduzibel in $R[X]$ ist. Hieraus schließt man mit dem Satz von Gauß 2.7/7, dass $\tilde{f}$ und damit auch f irreduzibel in $Q(R)[X]$ sind. □

Man kann übrigens das Eisensteinsche Irreduzibilitätskriterium auch mittels des Reduktionskriteriums beweisen. Hat man nämlich in der Situation von Satz 1 eine Zerlegung $f = gh$ mit Polynomen $g, h \in R[X]$ vom

Grad $< n$, so können wir den Homomorphismus $\Phi\colon R[X] \longrightarrow R/(p)[X]$ anwenden, welcher die Koeffizienten modulo (p) reduziert, und erhalten die Gleichung $\overline{a}_n X^n = \Phi(f) = \Phi(g)\Phi(h)$. Hieraus erkennt man, dass $\Phi(g)$ und $\Phi(h)$, abgesehen von einem konstanten Faktor aus $R/(p)$, jeweils nichttriviale Potenzen von X sind. Man kann nämlich die vorstehende Zerlegung in dem Polynomring $k[X]$ über dem Quotientenkörper k zu $R/(p)$ betrachten, wobei $k[X]$ faktoriell ist. Somit ist der konstante Term von g und h jeweils durch p teilbar, und es folgt, dass der konstante Term von f durch p^2 teilbar ist, im Widerspruch zur Wahl von f.

Wir wollen noch einige konkrete Beispiele für die Anwendung der Irreduzibilitätskriterien angeben:

(1) Es sei k ein Körper, $K := k(t)$ der Körper der rationalen Funktionen in einer Variablen t über k. Dann ist für $n \geq 1$ das Polynom $X^n - t \in K[X]$ irreduzibel. Es ist nämlich $R := k[t]$ faktoriell, $t \in R$ prim und $X^n - t$ ein primitives Polynom in $R[X]$, so dass man das Eisensteinsche Kriterium mit $p := t$ anwenden kann.

(2) Sei $p \in \mathbb{N}$ eine Primzahl. Dann ist $f(X) = X^{p-1} + \ldots + 1$ irreduzibel in $\mathbb{Q}[X]$. Zum Nachweis können wir das Eisensteinsche Kriterium auf das Polynom $f(X+1)$ anwenden, wobei $f(X+1)$ genau dann irreduzibel ist, wenn dies für $f(X)$ gilt. Man hat

$$f(X) = \frac{X^p - 1}{X - 1},$$
$$f(X+1) = \frac{(X+1)^p - 1}{X} = X^{p-1} + \binom{p}{1} X^{p-2} + \ldots + \binom{p}{p-1}.$$

Die Voraussetzungen des Eisensteinschen Kriteriums sind erfüllt wegen $\binom{p}{p-1} = p$ sowie $p \mid \binom{p}{\nu}$ für $\nu = 1, \ldots, p-1$; dabei beachte man, dass

$$\binom{p}{\nu} = \frac{p(p-1)\ldots(p-\nu+1)}{1\ldots\nu}$$

für $\nu = 1, \ldots, p-1$ im Zähler einen Primfaktor p besitzt, im Nenner aber nicht, also durch p teilbar ist.

(3) $f = X^3 + 3X^2 - 4X - 1$ ist irreduzibel in $\mathbb{Q}[X]$. Man fasse f als primitives Polynom in $\mathbb{Z}[X]$ auf und reduziere die Koeffizienten modulo 3. Es bleibt dann zu zeigen, dass das Polynom

$$X^3 - X - 1 \in \mathbb{F}_3[X]$$

irreduzibel ist, was man elementar nachprüfen kann. Allgemeiner kann man zeigen (vgl. Aufgabe 2), dass für p prim das Polynom $X^p - X - 1$ irreduzibel in $\mathbb{F}_p[X]$ ist.

Lernkontrolle und Prüfungsvorbereitung

1. Wie lautet das Eisensteinsche Irreduzibilitätskriterium? Gib einige Beispiele zur Anwendung.
2. Erkläre den Beweis des Eisensteinschen Irreduzibilitätskriteriums.
3. Wie lautet das Reduktionskriterium für Irreduzibilität? Gib einige Beispiele zur Anwendung.
4. Erkläre den Beweis des Reduktionskriteriums für Irreduzibilität.

Übungsaufgaben

1. Zeige, dass folgende Polynome irreduzibel sind:
   (i) $X^4 + 3X^3 + X^2 - 2X + 1 \in \mathbb{Q}[X]$.
   (ii) $2X^4 + 200X^3 + 2000X^2 + 20000X + 20 \in \mathbb{Q}[X]$.
   (iii) $X^2Y + XY^2 - X - Y + 1 \in \mathbb{Q}[X, Y]$.
2. Es sei $p \in \mathbb{N}$ eine Primzahl. Zeige, dass $g = X^p - X - 1$ als Polynom in $\mathbb{F}_p[X]$ irreduzibel ist. (*Hinweis*: g ist invariant unter dem Automorphismus $\tau\colon \mathbb{F}_p[X] \longrightarrow \mathbb{F}_p[X]$, $f(X) \longmapsto f(X+1)$; betrachte die Primfaktorzerlegung von g und lass τ darauf wirken.)

2.9 Elementarteilertheorie*

Als Verallgemeinerung von Vektorräumen über Körpern wollen wir in diesem Abschnitt Moduln über Ringen, speziell über Hauptidealringen, studieren. Wie wir sogleich sehen werden, sind abelsche Gruppen Beispiele für $\mathbb{Z}$-Moduln, also für Moduln über dem Ring $\mathbb{Z}$. Überhaupt ist das Studium abelscher Gruppen, insbesondere die Klassifikation endlich erzeugter abelscher Gruppen, eine nahe liegende Motivation für die hier präsentierte Theorie. Der Hauptsatz für endlich erzeugte Moduln über Hauptidealringen,

der diese Klassifikation liefert, lässt aber auch noch andere interessante Anwendungen zu. Er enthält z. B. als Spezialfall die Normalformentheorie für Endomorphismen endlich-dimensionaler Vektorräume; vgl. Aufgabe 3. Wir werden im Folgenden als zentrales Resultat den sogenannten Elementarteilersatz beweisen. Dieser klärt die Struktur endlich-rangiger Untermoduln von freien Moduln mit Koeffizienten aus einem Hauptidealring. Als Korollar ergibt sich der oben genannte Hauptsatz.

Es sei im Folgenden A zunächst ein beliebiger Ring, später dann ein Hauptidealring. Ein *A-Modul* ist eine abelsche Gruppe M, zusammen mit einer Multiplikation

$$A \times M \longrightarrow M, \qquad (a, x) \longmapsto a \cdot x,$$

die den üblichen "Vektorraum-Axiomen"

$$\begin{aligned} a \cdot (x + y) &= a \cdot x + a \cdot y, \\ (a + b) \cdot x &= a \cdot x + b \cdot x, \\ a \cdot (b \cdot x) &= (ab) \cdot x, \\ 1 \cdot x &= x, \end{aligned}$$

für $a, b \in A$, $x, y \in M$ genügt. *Homomorphismen* zwischen A-Moduln, auch *A-Homomorphismen* genannt, werden ebenso wie in der Theorie der Vektorräume definiert, desgleichen *Untermoduln* eines A-Moduls M sowie der *Restklassenmodul* M/N eines A-Moduls M nach einem Untermodul N. Der Homomorphiesatz 1.2/6 überträgt sich in nahe liegender Weise. Betrachtet man A als Modul über sich selbst, so sind die Ideale in A gerade die Untermoduln von A. Des Weiteren kann man für ein Ideal $\mathfrak{a} \subset A$ den Restklassenring $A/\mathfrak{a}$ als A-Modul auffassen.

Wie wir bereits erwähnt haben, lässt sich jede abelsche Gruppe G als $\mathbb{Z}$-Modul ansehen. Man definiere nämlich die Produktbildung $\mathbb{Z} \times G \longrightarrow G$, $(a, x) \longmapsto ax$, durch $ax = \sum_{i=1}^{a} x$ für $a \geq 0$ und $ax = -(-a)x$ für $a < 0$. Umgekehrt kann man aus jedem $\mathbb{Z}$-Modul M eine abelsche Gruppe G gewinnen, indem man die $\mathbb{Z}$-Multiplikation auf M vergisst. Es ist leicht zu sehen, dass sich auf diese Weise abelsche Gruppen und $\mathbb{Z}$-Moduln bijektiv entsprechen und dass sich diese Korrespondenz auch auf Homomorphismen, Untergruppen und Untermoduln sowie Restklassengruppen und Restklassenmoduln ausdehnt. Als weiteres Beispiel betrachte man einen Vektorraum V über einem Körper K sowie einen K-Endomorphismus $\varphi\colon V \longrightarrow V$. Es

ist V ein Modul über dem Polynomring einer Variablen $K[X]$, wenn man die Multiplikation durch

$$K[X] \times V \longrightarrow V, \qquad \left(\sum a_i X^i, v\right) \longmapsto \sum a_i \varphi^i(v),$$

definiert. Umgekehrt ist jeder $K[X]$-Modul V insbesondere ein K-Vektorraum, wobei man die Multiplikation mit X als K-Endomorphismus $\varphi\colon V \longrightarrow V$ auffassen kann. Auf diese Weise entsprechen die Paare des Typs (V, φ), bestehend aus einem K-Vektorraum V und einem K-Endomorphismus $\varphi\colon V \longrightarrow V$, bijektiv den $K[X]$-Moduln.

Für eine Familie von Untermoduln $M_i \subset M$, $i \in I$, ist deren *Summe* wie üblich als Untermodul

$$M' = \sum_{i\in I} M_i = \left\{\sum_{i\in I} x_i \,;\, x_i \in M_i,\, x_i = 0 \text{ für fast alle } i \in I\right\}$$

von M erklärt. M' wird als die *direkte Summe* der M_i bezeichnet, mit Schreibweise $M' = \bigoplus_{i\in I} M_i$, wenn jedes $x \in M'$ eine Darstellung des Typs $x = \sum_{i\in I} x_i$ mit eindeutig bestimmten Elementen $x_i \in M_i$ besitzt. Eine Summe $M_1 + M_2$ zweier Untermoduln von M ist genau dann direkt, wenn $M_1 \cap M_2 = 0$ gilt. Weiter kann man zu einer Familie $(M_i)_{i\in I}$ von A-Moduln in natürlicher Weise einen A-Modul M bilden, der die direkte Summe der M_i ist. Man setze nämlich

$$M = \left\{(x_i)_{i\in I} \in \prod_{i\in I} M_i \,;\, x_i = 0 \text{ für fast alle } i\right\}$$

und identifiziere M_i jeweils mit dem Untermodul von M, der aus allen Familien $(x_{i'})_{i'\in I}$ mit $x_{i'} = 0$ für $i' \neq i$ besteht.

Eine Familie $(x_i)_{i\in I}$ von Elementen eines A-Moduls M heißt ein *Erzeugendensystem* von M, wenn $M = \sum_{i\in I} Ax_i$ gilt. Besitzt M ein endliches Erzeugendensystem, so heißt M *endlich erzeugt* oder einfach ein *endlicher* Modul.[3] Weiter nennt man das System $(x_i)_{i\in I}$ *frei* oder *linear unabhängig*, wenn aus einer Darstellung $\sum_{i\in I} a_i x_i = 0$ mit Koeffizienten $a_i \in A$ bereits $a_i = 0$ für alle $i \in I$ folgt. Ein freies Erzeugendensystem wird auch *Basis* genannt; jedes $x \in M$ hat dann eine Darstellung $x = \sum_{i\in I} a_i x_i$ mit eindeutig bestimmten Koeffizienten $a_i \in A$. In diesem Falle heißt M ein *freier*

[3] Man beachte den Sprachgebrauch: Im Gegensatz zu einer endlichen Gruppe, einem endlichen Ring oder Körper verlangt man von einem endlichen A-Modul *nicht*, dass dieser nur aus endlich vielen Elementen besteht.

A-Modul. Beispielsweise ist A^n für $n \in \mathbb{N}$ ein freier A-Modul, ebenso $A^{(I)}$ für eine beliebige Indexmenge I.

Legt man anstelle von A einen Körper K als Koeffizientenring zugrunde, so geht die Theorie der A-Moduln über in die Theorie der K-Vektorräume. Überhaupt kann man in einem Modul M über einem Ring A weitgehend genauso rechnen wie in Vektorräumen über Körpern, mit einer Ausnahme, die zu beachten ist: Aus einer Gleichung $ax = 0$ für Elemente $a \in A, x \in M$ kann man meist nicht schließen, dass a oder x verschwinden, da zu $a \neq 0$ im Allgemeinen kein inverses Element a^{-1} in A zur Verfügung steht. Als Konsequenz besitzen A-Moduln, auch endlich erzeugte, nicht notwendig eine Basis. Für ein nicht-triviales Ideal $\mathfrak{a} \subset A$ etwa ist der Restklassenring $A/\mathfrak{a}$ ein Beispiel eines solchen A-Moduls, der nicht frei ist.

Es sei nun A ein *Integritätsring*. Elemente x eines A-Moduls M, zu denen es ein $a \in A - \{0\}$ mit $ax = 0$ gibt, nennt man *Torsionselemente*. Da wir A als Integritätsring vorausgesetzt haben, bilden die Torsionselemente einen Untermodul $T \subset M$, den sogenannten *Torsionsuntermodul*. Im Falle $T = 0$ heißt M *torsionsfrei*, im Falle $T = M$ ein *Torsionsmodul*. Beispielsweise ist jeder freie Modul torsionsfrei und jede endliche abelsche Gruppe, aufgefasst als $\mathbb{Z}$-Modul, ein Torsionsmodul. Weiter definiert man den *Rang* eines A-Moduls M, in Zeichen $\operatorname{rg} M$, als das Supremum aller Anzahlen n, so dass es ein linear unabhängiges System von Elementen $x_1, \ldots, x_n$ in M gibt. Der Rang eines Moduls ist damit ähnlich erklärt wie die Dimension eines Vektorraums. Es ist M genau dann ein Torsionsmodul, wenn der Rang von M verschwindet.

Bezeichnet S das System aller von Null verschiedenen Elemente in A sowie $K = S^{-1}A$ den Quotientenkörper von A, so kann man zu einem A-Modul M stets den K-Vektorraum $S^{-1}M$ konstruieren, indem man wie bei der Bildung von Bruchringen in Abschnitt 2.7 vorgeht. Man betrachte nämlich alle Brüche der Form $\frac{x}{s}$ mit $x \in M$ und $s \in S$, wobei man $\frac{x}{s}$ mit $\frac{x'}{s'}$ identifiziere, sofern es ein $s'' \in S$ mit $s''(s'x - sx') = 0$ gibt. Es ist dann $S^{-1}M$ mit den gewöhnlichen Regeln der Bruchrechnung ein K-Vektorraum, und man verifiziert ohne Schwierigkeiten, dass der Rang von M mit der Dimension von $S^{-1}M$ übereinstimmt. Der Kern der kanonischen Abbildung $M \longrightarrow S^{-1}M, x \longmapsto \frac{x}{1}$, ist gerade der Torsionsuntermodul $T \subset M$.

Im Folgenden setzen wir nun stets voraus, dass A ein *Hauptidealring* ist. Aus technischen Gründen benötigen wir den Begriff der *Länge* eines A-Moduls M, insbesondere eines A-Torsionsmoduls. Hierunter versteht

man das Supremum $l_A(M)$ aller Längen ℓ von Ketten von Untermoduln des Typs

$$0 \subsetneq M_1 \subsetneq M_2 \subsetneq \ldots \subsetneq M_\ell = M.$$

Beispielsweise hat der Null-Modul die Länge 0 und der freie $\mathbb{Z}$-Modul $\mathbb{Z}$ die Länge ∞. Für einen Vektorraum V über einem Körper K stimmt die Länge $l_K(V)$ überein mit der Vektorraumdimension $\dim_K V$.

Lemma 1. (i) *Es sei A ein Hauptidealring und $a \in A$ ein Element mit Primfaktorzerlegung $a = p_1 \ldots p_r$. Dann gilt $l_A(A/aA) = r$.*

(ii) *Ist ein A-Modul M die direkte Summe zweier Untermoduln M' und M'', so gilt $l_A(M) = l_A(M') + l_A(M'')$.*

Beweis. Wir beginnen mit Aussage (ii). Hat man Ketten von Untermoduln

$$0 \subsetneq M'_1 \subsetneq M'_2 \subsetneq \ldots \subsetneq M'_r = M',$$
$$0 \subsetneq M''_1 \subsetneq M''_2 \subsetneq \ldots \subsetneq M''_s = M'',$$

so ist

$$\begin{aligned} 0 \subsetneq M'_1 \oplus 0 \subsetneq M'_2 \oplus 0 \subsetneq \ldots \subsetneq M'_r \oplus 0 \\ \subsetneq M'_r \oplus M''_1 \subsetneq M'_r \oplus M''_2 \subsetneq \ldots \subsetneq M'_r \oplus M''_s = M \end{aligned}$$

eine Kette der Länge $r + s$ in M. Also gilt $l_A(M) \geq l_A(M') + l_A(M'')$. Zum Nachweis der umgekehrten Abschätzung betrachte man eine Kette von Untermoduln

$$0 = M_0 \subsetneq M_1 \subsetneq M_2 \subsetneq \ldots \subsetneq M_\ell = M.$$

Es sei $\pi'' \colon M' \oplus M'' \longrightarrow M''$ die Projektion auf den zweiten Summanden, so dass $\ker \pi'' = M'$. Dann gilt für $0 \leq \lambda < \ell$ jeweils $M_\lambda \cap M' \subsetneq M_{\lambda+1} \cap M'$ oder $\pi''(M_\lambda) \subsetneq \pi''(M_{\lambda+1})$. Hieraus folgt $\ell \leq l_A(M') + l_A(M'')$ und damit die Aussage von (ii).

Nun ist auch Aussage (i) leicht zu verifizieren. Nach Umnummerieren der p_i können wir von einer Primfaktorzerlegung des Typs $a = \varepsilon p_1^{\nu_1} \ldots p_s^{\nu_s}$ ausgehen, mit einer Einheit ε und paarweise nicht-assoziierten Primelementen $p_1, \ldots, p_s$, wobei $r = \nu_1 + \ldots + \nu_s$ gilt. Aufgrund des Chinesischen Restsatzes in der Version 2.4/14 ist A/aA als Ring isomorph zu dem ringtheoretischen Produkt $\prod_{i=1}^s A/p_i^{\nu_i}A$, und im Sinne von A-Moduln schreibt sich diese Zerlegung in additiver Form als

$$A/aA \simeq A/p_1^{\nu_1}A \oplus \ldots \oplus A/p_s^{\nu_s}A.$$

Nach der bereits bewiesenen Aussage (ii) genügt es, den Fall $a = p^\nu$ für ein Primelement $p \in A$ zu betrachten. Die Untermoduln von $A/p^\nu A$ entsprechen bijektiv den Idealen $\mathfrak{a} \subset A$ mit $p^\nu \in \mathfrak{a}$, also, da A Hauptidealring ist, bijektiv den Teilern $p^0, p^1, \ldots, p^\nu$ von p^ν. Da $p^{i+1}A$ jeweils in p^iA echt enthalten ist, ergibt sich $l_A(A/p^\nu) = \nu$, was zu zeigen war. □

Wir behandeln nunmehr den sogenannten *Elementarteilersatz*, der sich als Schlüsselresultat für die Theorie endlich erzeugter Moduln über Hauptidealringen bzw. endlich erzeugter abelscher Gruppen herausstellen wird.

Theorem 2. *Es sei F ein endlicher freier Modul über einem Hauptidealring A sowie $M \subset F$ ein Untermodul vom Rang n. Dann existieren Elemente $x_1, \ldots, x_n \in F$, die Teil einer Basis von F sind, sowie Koeffizienten $\alpha_1, \ldots, \alpha_n \in A - \{0\}$, so dass gilt*:

(i) *$\alpha_1 x_1, \ldots, \alpha_n x_n$ bilden eine Basis von M.*
(ii) *$\alpha_i \mid \alpha_{i+1}$ für $1 \leq i < n$.*

Dabei sind die Elemente $\alpha_1, \ldots, \alpha_n$ bis auf Assoziiertheit eindeutig durch M bestimmt, unabhängig von der Wahl von $x_1, \ldots, x_n$. Man nennt $\alpha_1, \ldots, \alpha_n$ die Elementarteiler *von $M \subset F$.*

Bemerkung 3. *In obiger Situation ist der Untermodul $\bigoplus_{i=1}^n Ax_i \subset F$ eindeutig durch M bestimmt als* Saturierung M_{sat} *von M in F; dabei besteht M_{sat} aus allen Elementen $y \in F$, zu denen es ein $a \neq 0$ in A gibt mit $ay \in M$. Weiter gilt*

$$M_{\text{sat}}/M \simeq \bigoplus_{i=1}^n A/\alpha_i A.$$

Wir wollen zunächst zeigen, dass die Behauptung der Bemerkung eine Konsequenz der Existenzaussage des Theorems ist. Einerseits gilt $\alpha_n \cdot (\bigoplus_{i=1}^n Ax_i) \subset M$, also $\bigoplus_{i=1}^n Ax_i \subset M_{\text{sat}}$. Sei umgekehrt $y \in M_{\text{sat}}$, etwa $ay \in M$ für ein $a \in A - \{0\}$. Man ergänze dann $x_1, \ldots, x_n$ durch Elemente $x_{n+1}, \ldots, x_r$ zu einer Basis von F (was aufgrund der Aussage von Theorem 2 möglich ist) und stelle y als Linearkombination der Basiselemente dar: $y = \sum_{j=1}^r a_j x_j$. Wegen $ay \in M$ ergibt sich $aa_j = 0$ bzw. $a_j = 0$ für

$j = n+1, \ldots, r$, also $y \in \bigoplus_{i=1}^{n} Ax_i$ und somit $M_{\mathrm{sat}} \subset \bigoplus_{i=1}^{n} Ax_i$. Insgesamt folgt $\bigoplus_{i=1}^{n} Ax_i = M_{\mathrm{sat}}$. Um auch die zweite Behauptung von Bemerkung 3 einzusehen, betrachte man für festes i den A-Isomorphismus $A \xrightarrow{\sim} Ax_i$, $a \longmapsto ax_i$. Unter diesem korrespondiert das Ideal $\alpha_i A \subset A$ zu dem Untermodul $A\alpha_i x_i \subset Ax_i$, so dass $Ax_i/A\alpha_i x_i$ isomorph zu $A/\alpha_i A$ ist. Aus dieser Betrachtung ergibt sich leicht die Isomorphie zwischen $(\bigoplus_{i=1}^{n} Ax_i)/M$ und $\bigoplus_{i=1}^{n} A/\alpha_i A$. □

Zum Beweis von Theorem 2 benötigen wir den Begriff des *Inhalts* $\mathrm{cont}(x)$ von Elementen $x \in F$. Um diesen zu definieren, betrachte man eine Basis $y_1, \ldots, y_r$ von F, stelle x als Linearkombination der y_j mit Koeffizienten aus A dar, etwa $x = \sum_{j=1}^{r} c_j y_j$, und setze $\mathrm{cont}(x) = \mathrm{ggT}(c_1, \ldots, c_r)$. Es bezeichnet also $\mathrm{cont}(x)$ im strengen Sinne kein Element aus A, sondern eine Klasse assoziierter Elemente, wobei man $\mathrm{cont}(0) = 0$ hat, auch im Falle $F = 0$. Um zu sehen, dass $\mathrm{cont}(x)$ nicht von der Wahl der Basis $y_1, \ldots, y_r$ von F abhängt, betrachte man den A-Modul F^* aller A-Homomorphismen $F \longrightarrow A$, d. h. aller Linearformen auf F. Die Elemente $\varphi(x)$ mit $\varphi \in F^*$ bilden ein Ideal in A, also ein Hauptideal (c), und wir behaupten $c = \mathrm{cont}(x)$. Um dies zu verifizieren, wähle man eine Gleichung $\mathrm{cont}(x) = \sum_{j=1}^{r} a_j c_j$ mit Koeffizienten $a_j \in A$; vgl. 2.4/13. Ist dann $\varphi_1, \ldots, \varphi_r$ die duale Basis zu $y_1, \ldots, y_r$, definiert durch $\varphi_i(y_j) = 0$ für $i \neq j$ und $\varphi_i(y_i) = 1$, so ergibt sich $\varphi(x) = \mathrm{cont}(x)$ für $\varphi = \sum_{j=1}^{r} a_j \varphi_j$. Da aber andererseits stets $\mathrm{cont}(x) = \mathrm{ggT}(c_1, \ldots, c_r)$ ein Teiler von $\psi(x)$ für $\psi \in F^*$ ist, erhält man $c = \mathrm{cont}(x)$.

Wir wollen die Eigenschaften des Inhalts auflisten, die wir im Folgenden benötigen.

Lemma 4. *In der Situation von Theorem* 2 *gilt*:

(i) *Zu* $x \in F$ *existiert ein* $\varphi \in F^*$ *mit* $\varphi(x) = \mathrm{cont}(x)$.

(ii) *Für* $x \in F$ *und* $\psi \in F^*$ *gilt* $\mathrm{cont}(x) \,|\, \psi(x)$.

(iii) *Es existiert ein* $x \in M$ *mit* $\mathrm{cont}(x) \,|\, \mathrm{cont}(y)$ *für alle* $y \in M$.

Beweis. Es muss nur noch Aussage (iii) gezeigt werden. Hierzu betrachte man die Menge aller Ideale des Typs $\mathrm{cont}(y) \cdot A$, wobei y in M variiert. Unter allen diesen Idealen gibt es ein maximales Element, also eines, welches in keinem Ideal $\mathrm{cont}(y) \cdot A$, $y \in M$, echt enthalten ist. Denn anderenfalls könnte man eine unendliche Folge y_i in M konstruieren mit

$$\operatorname{cont}(y_1) \cdot A \subsetneq \operatorname{cont}(y_2) \cdot A \subsetneq \ldots,$$

im Gegensatz dazu, dass A noethersch ist; vgl. 2.4/8. Es existiert also ein $x \in M$ mit der Eigenschaft, dass $\operatorname{cont}(x) \cdot A$ maximal im obigen Sinne ist. Weiter wähle man $\varphi \in F^*$ mit $\varphi(x) = \operatorname{cont}(x)$. Wir zeigen zunächst

$$(*) \qquad \varphi(x) \,|\, \varphi(y) \text{ für alle } y \in M.$$

Sei $d = \operatorname{ggT}(\varphi(x), \varphi(y))$ für ein $y \in M$, das wir im Folgenden betrachten wollen. Dann gibt es $a, b \in A$ mit $a\varphi(x) + b\varphi(y) = d$, also $\varphi(ax + by) = d$. Aufgrund von (ii) folgt $\operatorname{cont}(ax + by) \mid d$ und wegen $d \mid \varphi(x)$ sogar $\operatorname{cont}(ax + by) \,|\, \operatorname{cont}(x)$. Die Maximalitätseigenschaft von x impliziert dann aber $\operatorname{cont}(ax + by) = \operatorname{cont}(x)$. Somit ist $\varphi(x) = \operatorname{cont}(x)$ ein Teiler von d und wegen $d \,|\, \varphi(y)$ auch ein Teiler von $\varphi(y)$. Dies verifiziert $(*)$.

Um $\operatorname{cont}(x) \,|\, \operatorname{cont}(y)$ zu erhalten, genügt es gemäß (i), für alle $\psi \in F^*$ die Relation $\varphi(x) \mid \psi(y)$ zu zeigen. Da $\varphi(x) \mid \psi(x)$ aufgrund von (ii) gilt sowie $\varphi(x) \,|\, \varphi(y)$ aufgrund von $(*)$, dürfen wir y durch $y - \frac{\varphi(y)}{\varphi(x)}x$ ersetzen und auf diese Weise $\varphi(y) = 0$ annehmen. Indem wir die vorigen Teilbarkeitsrelationen nochmals ausnutzen, können wir weiter ψ durch $\psi - \frac{\psi(x)}{\varphi(x)}\varphi$ ersetzen und damit $\psi(x) = 0$ annehmen. Sei unter diesen Voraussetzungen $d = \operatorname{ggT}(\varphi(x), \psi(y))$, etwa $d = a\varphi(x) + b\psi(y)$ mit $a, b \in A$. Dann gilt

$$(\varphi + \psi)(ax + by) = a\varphi(x) + b\psi(y) = d,$$

d. h. $\operatorname{cont}(ax + by) \,|\, d$. Da nach Definition d ein Teiler von $\varphi(x)$ ist, ergibt sich $\operatorname{cont}(ax + by) \mid \varphi(x)$ und somit $\operatorname{cont}(ax + by) = \varphi(x)$ aufgrund der Maximalitätseigenschaft von x. Hieraus folgt $\varphi(x) \mid d$ und wegen $d \mid \psi(y)$ wie gewünscht $\varphi(x) \,|\, \psi(y)$. □

Wir kommen nun zum eigentlichen *Beweis von Theorem* 2, und zwar werden wir zur Herleitung der Existenzaussage zwei Induktionsbeweise führen, jeweils nach $n = \operatorname{rg} M$. Im ersten zeigen wir, dass jeder Untermodul $M \subset F$ frei ist, und benutzen dies im zweiten Induktionsbeweis, um die im Theorem formulierte Existenzaussage zu gewinnen. Im Falle $n = 0$ gilt auch $M = 0$, da M torsionsfrei ist, und es ist nichts zu zeigen. Sei also $n > 0$. Man wähle gemäß Lemma 4 (iii) ein $x \in M$ mit $\operatorname{cont}(x) \,|\, \operatorname{cont}(y)$ für alle $y \in M$. Es existiert dann ein $\varphi \in F^*$ mit $\varphi(x) = \operatorname{cont}(x)$, vgl. Lemma 4 (i), sowie ein (eindeutig bestimmtes) Element $x_1 \in F$ mit $x = \varphi(x)x_1$. Setzt man nun $F' = \ker \varphi$ und $M' = M \cap F'$, so gilt

$$(*) \qquad F = Ax_1 \oplus F', \qquad M = Ax \oplus M'.$$

Um die Formel für M zu erhalten, wähle man ein Element $y \in M$ und schreibe

$$y = \frac{\varphi(y)}{\varphi(x)}x + \left(y - \frac{\varphi(y)}{\varphi(x)}x\right),$$

wobei der linke Term der Summe zu Ax gehört. In der Tat, da x mit der Eigenschaft $\mathrm{cont}(x) \,|\, \mathrm{cont}(y)$ gewählt wurde und da man zusätzlich $\mathrm{cont}(y) \,|\, \varphi(y)$ aufgrund von Lemma 4 (ii) hat, gilt $\varphi(x) \,|\, \varphi(y)$. Weiter liegt der rechte Term der Summe in M', da er sowohl in M, als auch in $\ker \varphi$ liegt. Insbesondere folgt $M = Ax + M'$. Da $\varphi(x) \neq 0$ wegen $M \neq 0$, ergibt sich $Ax \cap M' = 0$, und wir sehen, dass M die direkte Summe der Untermoduln Ax und M' ist. In gleicher Weise zeigt man die Formel $F = Ax_1 \oplus F'$; man ersetze in vorstehender Argumentation jeweils x durch x_1 und benutze $\varphi(x_1) = 1$.

Aus der Zerlegung $M = Ax \oplus M'$ schließt man wegen $x \neq 0$ insbesondere $\mathrm{rg}\, M' < n$. Dann ist M' nach Induktionsvoraussetzung frei, notwendig vom Rang $n-1$, und es folgt, dass auch M frei ist. Dies beendet unseren ersten Induktionsbeweis.

Den zweiten Induktionsbeweis führen wir in gleicher Weise, bis wir zu den Zerlegungen $(*)$ gelangen. Aus dem ersten Induktionsbeweis wissen wir, dass F' als Untermodul von F frei ist. Wir haben also nach Induktionsvoraussetzung die Aussage von Theorem 2 für den Untermodul $M' \subset F'$ zur Verfügung. Somit existieren Elemente $x_2, \ldots, x_n \in F'$, die sich zu einer Basis von F' ergänzen lassen, sowie Elemente $\alpha_2, \ldots, \alpha_n \in A - \{0\}$ mit $\alpha_i \mid \alpha_{i+1}$ für $2 \leq i < n$ und mit der Eigenschaft, dass $\alpha_2 x_2, \ldots, \alpha_n x_n$ eine Basis von M' bilden. Insgesamt sind dann $x_1, \ldots, x_n$ Teil einer Basis von $F = Ax_1 \oplus F'$, und es bilden $\alpha_1 x_1, \ldots, \alpha_n x_n$ mit $\alpha_1 := \varphi(x)$ eine Basis von $M = Ax \oplus M'$. Für die Existenzaussage in Theorem 2 bleibt daher lediglich noch $\alpha_1 \mid \alpha_2$ nachzuweisen. Hierzu betrachte man eine Linearform $\varphi_2 \in F^*$, welche $\varphi_2(x_2) = 1$ erfüllt. Dann gilt $\mathrm{cont}(x) \mid \mathrm{cont}(\alpha_2 x_2)$ aufgrund der Wahl von x gemäß Lemma 4 (iii) und weiter $\mathrm{cont}(\alpha_2 x_2) \,|\, \varphi(\alpha_2 x_2)$ gemäß Lemma 4 (ii). Es folgt $\varphi(x) \mid \varphi_2(\alpha_2 x_2)$, also $\alpha_1 \mid \alpha_2$. Damit ist die Existenzaussage von Theorem 2 bewiesen.

Es bleibt noch die Eindeutigkeit der α_i nachzuweisen. Im Hinblick auf weitere Anwendungen formulieren wir diese in etwas allgemeinerer Form.

Lemma 5. *Es sei A ein Hauptidealring und $Q \simeq \bigoplus_{i=1}^{n} A/\alpha_i A$ ein A-Modul, wobei $\alpha_1, \ldots, \alpha_n \in A - \{0\}$ Nichteinheiten mit $\alpha_i \mid \alpha_{i+1}$ für $1 \leq i < n$ sind. Dann sind $\alpha_1, \ldots, \alpha_n$ bis auf Assoziiertheit eindeutig durch Q bestimmt.*

Beweis. Aus technischen Gründen invertieren wir die Nummerierung der α_i und betrachten zwei Zerlegungen

$$Q \simeq \bigoplus_{i=1}^{n} A/\alpha_i A \simeq \bigoplus_{j=1}^{m} A/\beta_j A$$

mit $\alpha_{i+1} \mid \alpha_i$ für $1 \leq i < n$ sowie $\beta_{j+1} \mid \beta_j$ für $1 \leq j < m$. Falls es einen Index $k \leq \min\{m, n\}$ mit $\alpha_k A \neq \beta_k A$ gibt, so wähle man k minimal mit dieser Eigenschaft. Da $\alpha_i A = \beta_i A$ für $1 \leq i < k$ und da $\alpha_{k+1}, \ldots, \alpha_n$ sämtlich Teiler von α_k sind, zerlegt sich $\alpha_k Q$ zu

$$\alpha_k Q \simeq \bigoplus_{i=1}^{k-1} \alpha_k \cdot \big(A/\alpha_i A\big) \simeq \Big(\bigoplus_{i=1}^{k-1} \alpha_k \cdot \big(A/\alpha_i A\big)\Big) \oplus \alpha_k \cdot \big(A/\beta_k A\big) \oplus \ldots .$$

Wir benutzen nun Lemma 1. Wegen $l_A(Q) < \infty$ ergibt sich durch Vergleich beider Seiten $l_A(\alpha_k \cdot (A/\beta_k A)) = 0$ und somit $\alpha_k \cdot (A/\beta_k A) = 0$ bzw. $\alpha_k A \subset \beta_k A$. Entsprechend zeigt man $\beta_k A \subset \alpha_k A$ und somit $\alpha_k A = \beta_k A$, im Widerspruch zu unserer Annahme. Es gilt daher $\alpha_i A = \beta_i A$ für alle Indizes i mit $1 \leq i \leq \min\{m, n\}$. Hat man weiter $m \leq n$, so folgt, wiederum unter Benutzung von Lemma 1, dass $\bigoplus_{i=m+1}^{n} A/\alpha_i A$ von der Länge 0 ist, also verschwindet, so dass sich $m = n$ ergibt. □

Abschließend wollen wir noch erläutern, wie die Eindeutigkeitsaussage von Theorem 2 aus vorstehendem Lemma gefolgert werden kann. Man habe also in der Situation des Theorems Elementarteiler $\alpha_1, \ldots, \alpha_n$ mit $\alpha_i \mid \alpha_{i+1}$ sowie $\beta_1, \ldots, \beta_n$ mit $\beta_i \mid \beta_{i+1}$, $1 \leq i < n$. Dann gilt gemäß Bemerkung 3, für deren Beweis wir lediglich die Existenzaussage von Theorem 2 verwendet haben,

$$\bigoplus_{i=1}^{n} A/\alpha_i A \simeq \bigoplus_{i=1}^{n} A/\beta_i A.$$

Da A/aA für Einheiten $a \in A$ verschwindet, folgt aus Lemma 5, dass die Nichteinheiten unter den $\alpha_1, \alpha_2, \ldots$ mit den Nichteinheiten unter den $\beta_1, \beta_2, \ldots$ bis auf Assoziiertheit übereinstimmen. Die restlichen α_i und β_i

sind dann Einheiten. Es gilt daher $\alpha_i A = \beta_i A$ für $1 \le i \le n$, und der Beweis zu Theorem 2 ist beendet. □

Wir wollen jetzt noch eine konstruktive Beschreibung der Elementarteiler angeben, die insbesondere für explizite Berechnungen von Interesse ist.

Satz 6. *Es sei A ein Hauptidealring, F ein endlicher freier A-Modul mit Basis $x_1, \ldots, x_r$ sowie $M \subset F$ ein Untermodul vom Rang n mit den Elementarteilern $\alpha_1, \ldots, \alpha_n$. Weiter seien $z_1, \ldots, z_m \in M$ Elemente, die ein (nicht notwendig freies) Erzeugendensystem von M bilden. Für $j = 1, \ldots, m$ gelte $z_j = \sum_{i=1}^{r} a_{ij} x_i$ mit Koeffizienten $a_{ij} \in A$, und es sei μ_t für $t = 1, \ldots, n$ der größte gemeinsame Teiler aller t-Minoren der Koeffizientenmatrix $D = (a_{ij})$.*[4] *Dann gilt $\mu_t = \alpha_1 \ldots \alpha_t$. Insbesondere folgt $\alpha_1 = \mu_1$ sowie $\alpha_t \mu_{t-1} = \mu_t$ für $t = 2, \ldots, n$.*

Man nennt $\alpha_1, \ldots, \alpha_n$ auch die Elementarteiler der Matrix D.

Beweis. Wir verifizieren die Behauptung zunächst für den Fall $t = 1$. Es ist $(\alpha_1) \subset A$ dasjenige Ideal, welches von allen Elementen des Typs $\varphi(z)$ mit $z \in M$ und $\varphi \in F^*$ erzeugt wird; dies ist unmittelbar aus der Aussage (oder dem Beweis) von Theorem 2 abzulesen. Indem wir auf die Elemente z_j die Linearformen der zu $x_1, \ldots, x_r$ dualen Basis von F^* anwenden, sehen wir, dass dasselbe Ideal auch von allen Koeffizienten a_{ij} erzeugt wird. Dies bedeutet aber, dass α_1 der größte gemeinsame Teiler aller 1-Minoren von D ist.

Um die Aussage für beliebiges t zu erhalten, ist es zweckmäßig, das *t-fache äußere Produkt* $\bigwedge^t F$ zu betrachten. Für unsere Zwecke genügt es, die Basis $x_1, \ldots, x_r$ von F zu fixieren und $\bigwedge^t F$ als freien A-Modul zu erklären, für den die Symbole $x_{i_1} \wedge \ldots \wedge x_{i_t}$ mit $1 \le i_1 < \ldots < i_t \le r$ eine Basis bilden. Für eine Permutation $\pi \in \mathfrak{S}_t$, also eine bijektive Selbstabbildung von $\{1, \ldots, t\}$, setzt man weiter

$$x_{i_{\pi(1)}} \wedge \ldots \wedge x_{i_{\pi(t)}} = (\operatorname{sgn} \pi) \cdot x_{i_1} \wedge \ldots \wedge x_{i_t},$$

wobei $\operatorname{sgn} \pi$ das Signum der Permutation π bezeichnet; vgl. 5.3. Definiert man dann noch $x_{i_1} \wedge \ldots \wedge x_{i_t} = 0$, falls die Indizes i_j nicht paarwei-

[4] Die t-Minoren von D sind die Determinanten der $(t \times t)$-Untermatrizen von D. Da D, aufgefasst als $(r \times m)$-Matrix mit Koeffizienten aus dem Quotientenkörper $Q(A)$, den Rang n hat, gilt $n \le \min(r, m)$.

se verschieden sind, so hat man das sogenannte t-fache "äußere Produkt" $x_{i_1} \wedge \ldots \wedge x_{i_t}$ für beliebige Indizes $i_1, \ldots, i_t \in \{1, \ldots, r\}$ erklärt, also für jeweils t Elemente der Basis $x_1, \ldots, x_r$. Durch A-multilineare Ausdehnung erhält man dann das äußere Produkt $z_1 \wedge \ldots \wedge z_t$ von beliebigen Elementen $z_1, \ldots, z_t \in F$. Nach Konstruktion ist dieses Produkt multilinear und alternierend in den Faktoren. Es ergibt sich beispielsweise für Elemente der Form $z_j = \sum_{i=1}^{r} a_{ij} x_i$

$$\begin{aligned} z_1 \wedge \ldots \wedge z_t &= \Big(\sum_{i=1}^{r} a_{i1} x_i\Big) \wedge \ldots \wedge \Big(\sum_{i=1}^{r} a_{it} x_i\Big) \\ &= \sum_{i_1,\ldots,i_t=1}^{r} a_{i_1 1} \ldots a_{i_t t}\, x_{i_1} \wedge \ldots \wedge x_{i_t} \\ &= \sum_{1 \le i_1 < \ldots < i_t \le r} \Big(\sum_{\pi \in \mathfrak{S}_t} (\operatorname{sgn} \pi) \cdot a_{i_{\pi(1)} 1} \ldots a_{i_{\pi(t)} t}\Big)\, x_{i_1} \wedge \ldots \wedge x_{i_t}, \end{aligned}$$

wobei die Koeffizienten $\sum_{\pi \in \mathfrak{S}_t} (\operatorname{sgn} \pi) \cdot a_{i_{\pi(1)} 1} \ldots a_{i_{\pi(t)} t}$ die t-Minoren der Koeffizientenmatrix von $z_1, \ldots, z_t$ bezüglich der Basis $x_1, \ldots, x_r$ sind. Man kann diese Rechnung übrigens auch dazu verwenden, um einzusehen, dass die obige Definition von $\bigwedge^t F$ zusammen mit dem t-fachen äußeren Produkt von Elementen aus F in natürlicher Weise unabhängig von der Wahl der Basis $x_1, \ldots, x_r$ ist.

Wir betrachten nun wieder die ursprünglich gegebenen Elemente $z_1, \ldots, z_m$ aus M und nehmen zunächst an, dass diese eine Basis von M bilden, genauer, dass $z_i = \alpha_i x_i$ für $i = 1, \ldots, m$ gilt mit Elementen $\alpha_i \in A - \{0\}$, welche der Teilbarkeitsrelation $\alpha_i \mid \alpha_{i+1}$ genügen. Eine solche Situation ist aufgrund des Elementarteilersatzes für $m = n$ durch geeignete Wahl von $x_1, \ldots, x_r$ sowie $z_1, \ldots, z_m$ stets zu realisieren. Man sieht dann, dass das t-fache äußere Produkt $\bigwedge^t M$ in natürlicher Weise ein Untermodul von $\bigwedge^t F$ ist; es bilden nämlich die Elemente $x_{i_1} \wedge \ldots \wedge x_{i_t}$ mit $1 \le i_1 < \ldots i_t \le r$ eine Basis von $\bigwedge^t F$ sowie die Elemente $\alpha_{i_1} \ldots \alpha_{i_t} x_{i_1} \wedge \ldots \wedge x_{i_t}$ mit $1 \le i_1 < \ldots i_t \le m$ eine Basis von $\bigwedge^t M$. Insbesondere erkennt man das Produkt $\alpha_1 \ldots \alpha_t$, etwa aufgrund der bereits für $t = 1$ durchgeführten Betrachtung, als ersten Elementarteiler des Problems $\bigwedge^t M \subset \bigwedge^t F$.

In der Situation des Satzes bilden $z_1, \ldots, z_m$ ein nicht notwendig freies Erzeugendensystem von M. Es folgt, dass die t-fachen äußeren Produkte des Typs $z_{i_1} \wedge \ldots \wedge z_{i_t}$ mit $1 \le i_1 < \ldots < i_t \le m$ den A-Modul $\bigwedge^t M$ erzeugen; man benutze eine Rechnung, wie wir sie oben durchgeführt haben. Aufgrund

des bereits erledigten Falles $t = 1$ berechnet sich der erste Elementarteiler zu $\bigwedge^t M \subset \bigwedge^t F$ als größter gemeinsamer Teiler aller Koeffizienten aus A, die man benötigt, um die Elemente $z_{i_1} \wedge \ldots \wedge z_{i_t}$ als Linearkombinationen der Basiselemente $x_{i_1} \wedge \ldots \wedge x_{i_t}$, $1 \leq i_1 < \ldots i_t \leq r$, darzustellen. Diese Koeffizienten sind aber, wie wir oben gesehen haben, die t-Minoren der Matrix D, d. h. der erste Elementarteiler zu $\bigwedge^t M \subset \bigwedge^t F$ ist μ_t. Andererseits hatten wir diesen Elementarteiler aber schon als $\alpha_1 \ldots \alpha_t$ erkannt, so dass $\mu_t = \alpha_1 \ldots \alpha_t$ folgt. □

Es sei hier noch ein weiteres konstruktives Verfahren angeführt, mit welchem man in der Situation von Satz 6 die Elementarteiler der Matrix $D = (a_{ij})$ bzw. von $M \subset F$ bestimmen kann, und zwar für den Fall, dass A ein *euklidischer Ring* ist. Hierzu betrachte man A^m als freien A-Modul mit der kanonischen Basis $e_1, \ldots, e_m$ sowie den A-Homomorphismus

$$A^m \longrightarrow F, \qquad e_j \longmapsto z_j,$$

welcher bezüglich der Basen $e_1, \ldots, e_m$ von A^m sowie $x_1, \ldots, x_r$ von F durch die Matrix D beschrieben wird. Wir zeigen im Folgenden, dass man D durch elementare Zeilen- und Spaltenumformungen — hiermit meinen wir Vertauschung von Zeilen (bzw. Spalten) sowie Addition eines Vielfachen einer Zeile (bzw. Spalte) zu einer weiteren Zeile (bzw. Spalte) — in die Gestalt

$$\begin{pmatrix} \alpha_1 & 0 & \ldots & 0 & 0 & \ldots & 0 \\ 0 & \alpha_2 & \ldots & 0 & 0 & \ldots & 0 \\ . & . & \ldots & . & . & \ldots & . \\ 0 & 0 & \ldots & \alpha_n & 0 & \ldots & 0 \\ 0 & 0 & \ldots & 0 & 0 & \ldots & 0 \\ . & . & \ldots & . & . & \ldots & . \\ 0 & 0 & \ldots & 0 & 0 & \ldots & 0 \end{pmatrix}$$

mit $\alpha_i \mid \alpha_{i+1}$ für $1 \leq i < n$ bringen kann. Diese Umformungen kann man interpretieren als Multiplikation von links und rechts mit jeweils einer invertierbaren Matrix $S \in A^{(r \times r)}$ bzw. $T \in A^{(m \times m)}$. Die resultierende Matrix SDT beschreibt ebenfalls die Abbildung f, allerdings bezüglich geeigneter anderer Basen $e'_1, \ldots, e'_m$ von A^m und $x'_1, \ldots, x'_r$ von F. Insbesondere folgt, dass M durch $\alpha_1 x'_1, \ldots, \alpha_n x'_n$ erzeugt wird, d. h. $\alpha_1, \ldots, \alpha_n$ sind die Elementarteiler von D bzw. $M \subset F$.

Um nun die Matrix $D = (a_{ij})$ durch elementare Zeilen- und Spaltenumformungen in die gewünschte Gestalt zu bringen, benutzen wir die

Gradabbildung $\delta\colon A-\{0\} \longrightarrow \mathbb{N}$ des euklidischen Rings A. Für $D=0$ ist nichts zu zeigen. Sei also $D \neq 0$. Es ist unsere Strategie, D mittels elementarer Umformungen so abzuändern, dass sich das Minimum

$$d = \min\big\{\delta(a)\,;\ a \text{ ist Koeffizient } \neq 0 \text{ von } D\big\}$$

schrittweise verringert. Da δ Werte in $\mathbb{N}$ annimmt, muss dieses Verfahren nach endlich vielen Schritten abbrechen. Ist dann $a \neq 0$ ein Koeffizient der transformierten Matrix mit minimalem Grad $\delta(a)$, so zeigen wir mittels Division mit Rest, dass a alle anderen Koeffizienten der Matrix teilt; a ist also der erste Elementarteiler von D.

Im Einzelnen gehen wir wie folgt vor. Indem wir Zeilen und Spalten in D vertauschen, können wir $d=\delta(a_{11})$ annehmen, dass also $\delta(a_{11})$ minimal ist unter allen $\delta(a_{ij})$ mit $a_{ij} \neq 0$. Ist eines der Elemente der 1. Spalte, etwa a_{i1}, nicht durch a_{11} teilbar, so teile man a_{i1} mit Rest durch a_{11}, etwa $a_{i1}=qa_{11}+b$ mit $\delta(b)<\delta(a_{11})$, und ziehe das q-fache der 1. Zeile von der i-ten Zeile ab. Als Resultat entsteht an der Position $(i,1)$ das Element b. Das Minimum d der Grade von nichtverschwindenden Koeffizienten von D hat sich daher verringert, und man starte das Verfahren erneut. Entsprechend können wir mit der 1. Zeile verfahren. Da d Werte in $\mathbb{N}$ annimmt, also nicht beliebig oft verringert werden kann, ist nach endlich vielen Schritten jedes Element der 1. Spalte sowie der 1. Zeile ein Vielfaches von a_{11}, und wir können durch Addition von Vielfachen der 1. Zeile zu den restlichen Zeilen der Matrix annehmen, dass $a_{i1}=0$ für $i>1$ gilt. Entsprechend können wir mit der 1. Zeile verfahren und auf diese Weise $a_{i1}=a_{1j}=0$ für $i,j>1$ erreichen. Dabei dürfen wir weiter annehmen, dass das Minimum d mit $\delta(a_{11})$ übereinstimmt; ansonsten ist das Verfahren wiederum neu zu starten.

Existieren nun $i,j>1$ mit $a_{11}\nmid a_{ij}$, so dividiere man a_{ij} mit Rest durch a_{11}, etwa $a_{ij}=qa_{11}+b$, wobei dann $b\neq 0$ mit $\delta(b)<\delta(a_{11})$ gilt. Man addiere die 1. Zeile zur i-ten Zeile und subtrahiere anschließend das q-fache der 1. Spalte von der j-ten Spalte. Auf diese Weise wird, neben anderen Änderungen, a_{ij} durch b ersetzt, wobei nun $\delta(b)<\delta(a_{11})$ gilt und sich das Minimum d der δ-Werte der Koeffizienten erneut verringert hat. Man starte daher das Verfahren erneut. Nach endlich vielen Schritten gelangt man so zu einer Matrix (a_{ij}) mit $a_{i1}=a_{1j}=0$ für $i,j>1$ sowie mit der Eigenschaft, dass a_{11} jedes andere Element a_{ij} mit $i,j>1$ teilt. Man behandele dann in gleicher Weise die Untermatrix $(a_{ij})_{i,j>1}$ von $D=(a_{ij})$, sofern diese

nicht bereits Null ist. Führt man dieses Verfahren in induktiver Weise fort, so gelangt man schließlich nach endlich vielen Schritten zu einer Matrix, auf deren Hauptdiagonale die gesuchten Elementarteiler stehen und deren sonstige Einträge alle verschwinden.

Wir wollen als Nächstes aus dem Elementarteilersatz den *Hauptsatz für endlich erzeugte Moduln über Hauptidealringen* ableiten, wobei wir die Aussage in zwei Teile aufspalten. A sei im Folgenden wieder ein *Hauptidealring*.

Korollar 7. *Es sei M ein endlich erzeugter A-Modul sowie $T \subset M$ der zugehörige Torsionsuntermodul. Dann ist T endlich erzeugt, und es gibt einen freien Untermodul $F \subset M$ mit $M = T \oplus F$, wobei $\operatorname{rg} M = \operatorname{rg} F$. Insbesondere ist M frei, falls M keine Torsion hat.*

Korollar 8. *Es sei M ein endlich erzeugter Torsionsmodul über A sowie $P \subset A$ ein Vertretersystem der Primelemente von A. Für $p \in P$ bezeichne*

$$M_p = \{x \in M\,;\; p^n x = 0 \text{ für geeignetes } n \in \mathbb{N}\}$$

*den sogenannten Untermodul der p-*Torsion *in M. Dann gilt*

$$M = \bigoplus_{p \in P} M_p,$$

wobei M_p für fast alle $p \in P$ verschwindet. Weiter gibt es zu jedem $p \in P$ natürliche Zahlen $1 \leq \nu(p,1) \leq \ldots \leq \nu(p,r_p)$ mit

$$M_p \simeq \bigoplus_{j_p=1}^{r_p} A \,/\, p^{\nu(p,j_p)} A.$$

Die Zahlen $r_p, \nu(p,j_p)$ sind durch die Isomorphie

$$M \simeq \bigoplus_{p \in P} \bigoplus_{j_p=1}^{r_p} A \,/\, p^{\nu(p,j_p)} A$$

eindeutig bestimmt, und es gilt $r_p = 0$ für fast alle p.

In Kombination besagen die beiden Resultate, dass jeder endlich erzeugte A-Modul M zu einer direkten Summe der Form

$$A^d \oplus \bigoplus_{p\in P} \bigoplus_{j_p=1}^{r_p} A/p^{\nu(p,j_p)}A$$

isomorph ist, mit Zahlen d, r_p und $\nu(p, j_p)$ wie oben, die eindeutig durch M bestimmt sind. Dies ist die eigentliche Aussage des Hauptsatzes für endlich erzeugte Moduln über Hauptidealringen. Bevor wir zum Beweis kommen, wollen wir diesen Hauptsatz auch noch speziell für endlich erzeugte $\mathbb{Z}$-Moduln formulieren, als *Hauptsatz über endlich erzeugte abelsche Gruppen*.

Korollar 9. *Es sei G eine endlich erzeugte abelsche Gruppe, P sei die Menge der Primzahlen. Dann gestattet G eine Zerlegung in Untergruppen*

$$G = F \oplus \bigoplus_{p\in P} \bigoplus_{j_p=1}^{r_p} G_{p,j_p},$$

wobei F frei ist, etwa $F \simeq \mathbb{Z}^d$, und G_{p,j_p} zyklisch von p-Potenz-Ordnung, etwa $G_{p,j_p} \simeq \mathbb{Z}/p^{\nu(p,j_p)}\mathbb{Z}$ mit $1 \le \nu(p,1) \le \ldots \le \nu(p,r_p)$. Die Zahlen $d, r_p, \nu(p,j_p)$ sind eindeutig durch G bestimmt, ebenso die Untergruppen $G_p = \bigoplus_{j_p=1}^{r_p} G_{p,j_p}$, wobei r_p für fast alle $p \in P$ verschwindet.

Wenn G eine endlich erzeugte Torsionsgruppe ist, also ein über $\mathbb{Z}$ endlich erzeugter Torsionsmodul, so besitzt G keinen freien Anteil und besteht daher, wie man insbesondere mit Korollar 9 sieht, nur aus endlich vielen Elementen. Umgekehrt ist jede endliche abelsche Gruppe natürlich eine endlich erzeugte Torsionsgruppe.

Nun zum *Beweis von Korollar* 7. Es sei $z_1, \ldots, z_r$ ein Erzeugendensystem des A-Moduls M. Sodann definiere man einen A-Homomorphismus $f\colon A^r \longrightarrow M$, indem man die kanonische Basis von A^r auf $z_1, \ldots, z_r$ abbilde. Dann ist f surjektiv, und es folgt $M \simeq A^r/\ker f$ aufgrund des Homomorphiesatzes. Auf die Situation $\ker f \subset A^r$ können wir nun den Elementarteilersatz anwenden. Es existieren also Elemente $x_1, \ldots, x_r$, die eine Basis von A^r bilden, sowie Elemente $\alpha_1, \ldots, \alpha_n \in A$, $n = \operatorname{rg}(\ker f)$, so dass $\alpha_1 x_1, \ldots, \alpha_n x_n$ eine Basis von $\ker f$ ist. Hieraus ergibt sich

$$M \simeq A^{r-n} \oplus \bigoplus_{i=1}^{n} A/\alpha_i A.$$

Unter dem betrachteten Isomorphismus korrespondiert $\bigoplus_{i=1}^{n} A/\alpha_i A$ zu dem Torsionsuntermodul $T \subset M$, sowie A^{r-n} zu einem freien Modul $F \subset M$, und es gilt $M = T \oplus F$. Im Übrigen ist $T \simeq \bigoplus_{i=1}^{n} A/\alpha_i A$ endlich erzeugt, so dass Korollar 7 bewiesen ist. □

Zum *Beweis von Korollar* 8 nehmen wir M als Torsionsmodul an, so dass M wie im Beweis zu Korollar 7 isomorph zu der direkten Summe $\bigoplus_{i=1}^{n} A/\alpha_i A$ ist. Man zerlege die α_i sodann in Primfaktoren, etwa $\alpha_i = \varepsilon_i \prod_{p \in P} p^{\nu(p,i)}$ mit Einheiten ε_i und Exponenten $\nu(p,i)$, die fast alle verschwinden. Aufgrund des Chinesischen Restsatzes 2.4/14 folgt

$$A/\alpha_i A \simeq \bigoplus_{p \in P} A/p^{\nu(p,i)} A$$

und somit

$$M \simeq \bigoplus_{p \in P} \bigoplus_{i=1}^{n} A/p^{\nu(p,i)} A.$$

In dieser Zerlegung korrespondiert $\bigoplus_{i=1}^{n} A/p^{\nu(p,i)} A$ offenbar gerade zu dem Untermodul $M_p \subset M$ der p-Torsion und ist deshalb eindeutig bestimmt; die Restklasse von p in Restklassenringen der Form $A/p'^r A$ mit $p' \in P - \{p\}$ ist nämlich jeweils eine Einheit. Somit folgt aus obiger Zerlegung insbesondere $M = \bigoplus_{p \in P} M_p$. Verzichtet man nun in der Zerlegung

$$M_p \simeq \bigoplus_{i=1}^{n} A/p^{\nu(p,i)} A$$

auf Terme $A/p^{\nu(p,i)} A$ mit $\nu(p,i) = 0$, die ohnehin trivial sind, und ordnet im Übrigen für fixiertes p die Exponenten $\nu(p,i)$ in aufsteigender Reihenfolge an, etwa

$$M_p \simeq \bigoplus_{j_p=1}^{r_p} A/p^{\nu(p,j_p)} A$$

mit $1 \leq \nu(p,1) \leq \ldots \leq \nu(p,r_p)$, so ergibt sich unter Benutzung der Eindeutigkeitsaussage in Lemma 5 insgesamt die Behauptung von Korollar 8. □

Die in diesem Abschnitt behandelten Methoden und Resultate basieren in grundlegender Weise auf der idealtheoretischen Charakterisierung 2.4/13

des größten gemeinsamen Teilers, also auf einer Charakterisierung, die in Hauptidealringen gilt, nicht jedoch in allgemeineren faktoriellen Ringen; vgl. Abschnitt 2.4, Aufgabe 2. Aus diesem Grunde ist eine Übertragung der Elementarteilertheorie auf endlich erzeugte Moduln etwa über faktoriellen Ringen nicht möglich.

Lernkontrolle und Prüfungsvorbereitung

A sei stets ein Hauptidealring.

1. Was versteht man unter einem A-Modul? Wie kann man eine abelsche Gruppe als $\mathbb{Z}$-Modul auffassen? Wie kann man einen Vektorraum über einem Körper K zusammen mit einem K-Endomorphismus $V \longrightarrow V$ als Modul über dem Polynomring $K[X]$ auffassen?

2. Was versteht man unter einem Erzeugendensystem eines A-Moduls, was unter einem endlichen A-Modul? Was versteht man unter einer Basis eines A-Moduls, was unter einem freien A-Modul? Besitzt jeder A-Modul eine Basis?

3. Was versteht man unter einem Torsionselement in einem A-Modul M? Zeige, dass die Torsionselemente von M einen Untermodul bilden, den sogenannten Torsionsuntermodul von M. Wann nennt man M einen Torsionsmodul? Gib einige Beispiele für Torsionsmoduln.

4. Wie ist der Rang eines A-Moduls definiert? Gib ein Beispiel eines A-Moduls $M \neq 0$, dessen Rang 0 ist.

5. Was versteht man unter der Länge eines A-Moduls? Wie verhält sich die Länge bei direkten Summen von A-Moduln?

6. Wie berechnet sich für ein Primelement $p \in A$ und einen Exponenten $\nu \in \mathbb{N}$ die Länge von $A/p^\nu A$, aufgefasst als A-Modul?

7. Wie kann man allgemeiner für ein Element $a \neq 0$ in A die Länge von A/aA als A-Modul berechnen?

8. Wie lautet der Elementarteilersatz für einen Untermodul M eines endlichen freien A-Moduls F? Was versteht man unter der Saturierung M_{sat} von M in F? Wie lässt sich M_{sat} mit Hilfe des Elementarteilersatzes charakterisieren?

+9. Es sei F ein endlicher freier A-Modul und F^* der A-Modul aller A-Homomorphismen $F \longrightarrow A$. Definiere den Inhalt $\text{cont}(x)$ für Elemente $x \in F$. Wie lässt sich $\text{cont}(x)$ unter Nutzung von Elementen $\varphi \in F^*$ charakterisieren?

$^{++}$10. Es sei F ein endlicher freier A-Modul und $M \subset F$ ein Untermodul. Zeige, dass ein $x \in M$ existiert mit $\mathrm{cont}(x) \,|\, \mathrm{cont}(y)$ für alle $y \in M$. Zeige weiter, dass M endlich und frei ist.

$^{++}$11. Führe den Induktionsbeweis der Existenzaussage des Elementarteilersatzes für einen Untermodul M eines endlichen freien A-Moduls F.

$^{+}$12. Beweise die Eindeutigkeitsaussage des Elementarteilersatzes für einen Untermodul M eines endlichen freien A-Moduls F.

$^{+}$13. Was versteht man unter den Elementarteilern einer Matrix mit Koeffizienten aus A? Wie lassen sich diese Elementarteiler mit Hilfe von Minoren der Matrix charakterisieren?

$^{+}$14. Wie kann man die Elementarteiler einer Matrix mit Koeffizienten aus einem euklidischen Ring in konstruktiver Weise bestimmen?

15. Wie lautet der Hauptsatz für endlich erzeugte Moduln über Hauptidealringen und wie kann man diesen aus dem Elementarteilersatz folgern?

16. Formuliere den Hauptsatz für endliche abelsche Gruppen.

Übungsaufgaben

A sei stets ein Hauptidealring.

1. *Betrachte eine Zerlegung $M = T \oplus F$ eines endlich erzeugten A-Moduls M in einen Torsionsmodul T und einen freien Modul F und diskutiere die Eindeutigkeit einer solchen Zerlegung. Studiere dasselbe Problem für eine Zerlegung der Form $M = M' \oplus M''$ mit $M' \simeq A/p^r A$ sowie $M'' \simeq A/p^s A$ für ein Primelement $p \in A$.*

2. *Ein torsionsfreier A-Modul ist frei, sofern er endlich erzeugt ist. Gilt dies auch für beliebige torsionsfreie A-Moduln*?

3. *Leite die Normalformentheorie für Endomorphismen von Vektorräumen endlicher Dimension über einem Körper aus Korollar* 8 *ab.*

4. Bestimme die Elementarteiler der folgenden Matrix:

$$\begin{pmatrix} 2 & 6 & 8 \\ 3 & 1 & 2 \\ 9 & 5 & 4 \end{pmatrix} \in \mathbb{Z}^{(3\times 3)}$$

5. Es seien $a_{11}, \ldots, a_{1n} \in A$ Elemente mit $\mathrm{ggT}(a_{11}, \ldots, a_{1n}) = 1$. Zeige, es gibt Elemente $a_{ij} \in A$, $i = 2, \ldots, n$, $j = 1, \ldots, n$, so dass die Matrix $(a_{ij})_{i,j=1,\ldots,n}$ in $A^{(n\times n)}$ invertierbar ist.

6. Es sei $f\colon L \longrightarrow M$ ein A-Homomorphismus zwischen endlich erzeugten freien A-Moduln. Zeige:
   (i) Es existiert ein freier Untermodul $F \subset L$ mit $L = \ker f \oplus F$.
   (ii) Es existieren Basen $x_1, \ldots, x_m$ von L und $y_1, \ldots, y_n$ von M sowie Elemente $\alpha_1, \ldots, \alpha_r \in A - \{0\}$, $r \leq \min\{m, n\}$, mit der Eigenschaft, dass $f(x_i) = \alpha_i y_i$ für $i = 1, \ldots, r$ und $f(x_i) = 0$ für $i > r$ gilt. Zusätzlich kann man $\alpha_i \,|\, \alpha_{i+1}$ für $1 \leq i < r$ erreichen.
7. Gib ein einfaches Argument an, mit dessen Hilfe sich die Aussage von Theorem 2 auf endlich-rangige Untermoduln M von (nicht notwendig endlich-rangigen) freien A-Moduln F verallgemeinern lässt.

3. Algebraische Körpererweiterungen

Überblick und Hintergrund

Zunächst wollen wir erklären, auf welche Weise algebraische Gleichungen mit algebraischen Körpererweiterungen zusammenhängen. Wir beginnen mit dem nahe liegenden Fall einer algebraischen Gleichung mit rationalen Koeffizienten, etwa $f(x) = 0$, wobei $f \in \mathbb{Q}[X]$ ein normiertes Polynom vom Grad ≥ 1 ist. Die Frage, was man unter den Lösungen einer solchen Gleichung zu verstehen hat und wie man mit diesen rechnet, wollen wir erst einmal zurückstellen, indem wir den Fundamentalsatz der Algebra als bekannt annehmen. Wir benutzen also, dass es in $\mathbb{C}$ eine Nullstelle α zu f gibt, wobei dann $f(\alpha) = 0$ als eine in $\mathbb{C}$ gültige Gleichung aufzufassen ist. Um die "Natur" der Nullstelle α besser beschreiben zu können, ist man allerdings darum bemüht, einen möglichst kleinen Zahlbereich zu konstruieren, in dem die Gleichung $f(\alpha) = 0$ gelesen werden kann. Ein solcher Bereich wird z. B. durch den kleinsten Unterring von $\mathbb{C}$ gegeben, der $\mathbb{Q}$ und α enthält, also durch

$$\mathbb{Q}[\alpha] = \big\{g(\alpha)\,;\, g \in \mathbb{Q}[X]\big\}.$$

Unter Benutzung des Epimorphismus $\varphi\colon \mathbb{Q}[X] \longrightarrow \mathbb{Q}[\alpha]$, $g \longmapsto g(\alpha)$, ist leicht zu sehen, dass $\mathbb{Q}[\alpha]$ sogar ein *Körper* ist. $\mathbb{Q}[X]$ ist nämlich ein Hauptidealring. Folglich ist $\ker\varphi$ ein Hauptideal, etwa $\ker\varphi = (q)$, wobei q wegen $f \in \ker\varphi$ nicht verschwindet und somit als normiertes Polynom in $\mathbb{Q}[X]$ angenommen werden kann. Der Homomorphiesatz 2.3/5 liefert dann

S. Bosch, *Algebra*, https://doi.org/10.1007/978-3-662-67464-2_4

zu φ einen Isomorphismus $\mathbb{Q}[X]/(q) \xrightarrow{\sim} \mathbb{Q}[\alpha]$, und man sieht mit 2.3/8 (i) und 2.4/4 (ii), dass q ein Primelement ist, das sogenannte *Minimalpolynom* zu α. Ist f irreduzibel, so folgt $f = q$ mittels Teilbarkeitstheorie. Das Ideal (q) ist nach 2.4/6 maximal in $\mathbb{Q}[X]$, so dass $\mathbb{Q}[\alpha] \simeq \mathbb{Q}[X]/(q)$ in der Tat ein Körper ist. Man sagt, $\mathbb{Q}[\alpha]$ entsteht aus $\mathbb{Q}$ durch *Adjunktion* der Nullstelle α. In gleicher Weise kann man weitere Nullstellen von f (oder von anderen Polynomen mit Koeffizienten aus $\mathbb{Q}[\alpha]$) zu $\mathbb{Q}[\alpha]$ adjungieren.

Aus diesen Überlegungen ergeben sich einige wichtige Schlussfolgerungen. Zunächst erkennt man, dass $\mathbb{Q}[\alpha]$ als $\mathbb{Q}$-Vektorraum von endlicher Dimension ist, dass also $\mathbb{Q} \subset \mathbb{Q}[\alpha]$ eine *endliche* Körpererweiterung ist; vgl. 3.2/6. Dies impliziert unter Benutzung eines einfachen Dimensionsarguments aus der Linearen Algebra, dass *jedes* Element von $\mathbb{Q}[\alpha]$ Lösung einer algebraischen Gleichung mit Koeffizienten aus $\mathbb{Q}$ ist, dass also $\mathbb{Q} \subset \mathbb{Q}[\alpha]$ eine *algebraische* Körpererweiterung ist, wie wir sagen werden; vgl. 3.2/7. Damit wird klar, dass man mit der Erweiterung $\mathbb{Q} \subset \mathbb{Q}[\alpha]$ sozusagen eine ganze Klasse verwandter algebraischer Gleichungen gleichzeitig behandelt.

Im Folgenden wollen wir nun $f \in \mathbb{Q}[X]$ als *irreduzibel* voraussetzen; $\alpha_1, \ldots, \alpha_n \in \mathbb{C}$ seien die Nullstellen von f. Wir haben dann für $i = 1, \ldots, n$ einen Isomorphismus $\mathbb{Q}[\alpha_i] \simeq \mathbb{Q}[X]/(f)$, wie oben konstruiert, unter dem α_i jeweils zu der Restklasse von X korrespondiert. Insbesondere gibt es zu je zwei Indizes i, j einen Isomorphismus $\sigma_{ij} \colon \mathbb{Q}[\alpha_i] \xrightarrow{\sim} \mathbb{Q}[\alpha_j]$ mit $\sigma_{ij}(\alpha_i) = \alpha_j$. Wir sehen also, dass alle Nullstellen von f in gewisser Weise "gleichartig" sind. Die genannten Isomorphismen lassen bereits einen ersten Ausblick auf die Galois-Theorie der Gleichung $f(x) = 0$ zu. In dem Spezialfall, wo der Teilkörper $L = \mathbb{Q}[\alpha_i] \subset \mathbb{C}$ unabhängig von i ist, bilden die σ_{ij} Automorphismen von L, und diese sind gerade die Elemente der Galois-Gruppe zur Gleichung $f(x) = 0$. Im Allgemeinfall betrachtet man statt $\mathbb{Q}[\alpha_i]$ den sogenannten *Zerfällungskörper* $L = \mathbb{Q}[\alpha_1, \ldots, \alpha_n]$ von f, der aus $\mathbb{Q}$ durch Adjunktion aller Nullstellen von f entsteht. Man kann dann mit Hilfe des Satzes vom primitiven Element 3.6/12 zeigen, dass es ein irreduzibles Polynom $g \in \mathbb{Q}[X]$ mit Nullstellen $\beta_1, \ldots, \beta_r \in \mathbb{C}$ gibt, so dass $L = \mathbb{Q}[\beta_j]$ für $j = 1, \ldots, r$ gilt. Wir sind daher in der Situation des soeben betrachteten Spezialfalles, und man kann die Galois-Gruppe zur Gleichung $f(x) = 0$ durch die entsprechende Gruppe der Gleichung $g(x) = 0$ erklären.

Bis jetzt haben wir uns lediglich auf Körpererweiterungen von $\mathbb{Q}$ beschränkt. Wie kann man aber vorgehen, wenn man $\mathbb{Q}$ durch einen beliebigen

Körper K ersetzen möchte? Im Prinzip sind keine Änderungen nötig, wie wir in diesem Kapitel sehen werden. Man braucht lediglich einen gewissen Ersatz für den Fundamentalsatz der Algebra. Hierzu charakterisieren wir in 3.2 zunächst endliche und algebraische Körpererweiterungen, ohne dass wir von konkreten algebraischen Gleichungen ausgehen, die wir lösen möchten; eine Verallgemeinerung der Theorie auf Ringerweiterungen findet man in 3.3. Sodann beschäftigen wir uns in 3.4 mit dem Problem, zu einer irreduziblen algebraischen Gleichung $f(x) = 0$ mit $f \in K[X]$ einen Erweiterungskörper L von K zu konstruieren, der eine Nullstelle α von f enthält. Ist L ein solcher Körper, so kann man wie oben den Körper $K[\alpha]$ betrachten; dieser ist isomorph zu $K[X]/(f)$, da f irreduzibel ist. Umgekehrt kann man aber auch L durch $K[X]/(f)$ erklären, wobei die Restklasse von X eine Nullstelle zu f ist; dies ist das *Verfahren von Kronecker*, vgl. 3.4/1. Das Verfahren von Kronecker erlaubt es, in sukzessiver Weise Nullstellen von Polynomen zu K zu adjungieren. Hat man etwa eine Nullstelle α_1 von f zu K adjungiert, so besteht in $K[\alpha_1][X]$ eine Zerlegung der Form $f = (X - \alpha_1)f_1$, und man kann in einem nächsten Schritt zu $K[\alpha_1]$ eine Nullstelle α_2 von f_1 adjungieren usw. Auf diese Weise erhält man nach endlich vielen Schritten einen Zerfällungskörper L zu f, d. h. einen Erweiterungskörper von K, über dem f vollständig in Linearfaktoren zerfällt und der durch Adjunktion sämtlicher Nullstellen von f zu K entsteht.

Obwohl das Verfahren von Kronecker ausreicht, um algebraische Gleichungen handhaben zu können, ist es in vielerlei Hinsicht wünschenswert, einen "echten" Ersatz für den Fundamentalsatz der Algebra zu haben. So konstruieren wir in 3.4 einen sogenannten *algebraischen Abschluss* $\overline{K}$ von K, indem wir nach einer auf E. Artin zurückgehenden Methode *alle* Nullstellen von Polynomen aus $K[X]$ auf einen Schlag zu K adjungieren. Der Körper $\overline{K}$ ist algebraisch über K und hat die Eigenschaft, dass jedes nicht-konstante Polynom in $\overline{K}[X]$ vollständig in Linearfaktoren zerfällt. Diese Konstruktion ermöglicht es uns, in einem gewissen Sinne von "den" Nullstellen von f zu sprechen. Insbesondere ist dann die Konstruktion von Zerfällungskörpern zu einer Familie von Polynomen in 3.5 kein Problem mehr, und wir gelangen zu der Notation *normaler Körpererweiterungen*, einer Vorstufe der Galois-Erweiterungen.

Es bleibt noch auf das Phänomen der *Inseparabilität* hinzuweisen, welches auftritt, wenn man statt Erweiterungskörpern von $\mathbb{Q}$ solche von Körpern K einer Charakteristik > 0 behandelt. Dabei bezeichnet die Charakteristik

von K die kleinste natürliche Zahl $p > 0$ mit $p \cdot 1 = 0$, bzw. man setzt $p = 0$, falls eine solche Zahl nicht existiert; vgl. 3.1. Ein Polynom $f \in K[X]$ heißt *separabel*, wenn es (in einem algebraischen Abschluss von K) lediglich einfache Nullstellen besitzt, und *rein inseparabel*, wenn es genau eine Nullstelle besitzt, die dann notwendig grad f als Vielfachheit hat. Irreduzible Polynome über Körpern der Charakteristik 0 sind stets separabel, im Allgemeinen jedoch nicht über Körpern der Charakteristik > 0. Allgemeiner führen wir die Charakterisierung separabler algebraischer Körpererweiterungen in 3.6 durch und als Gegenstück dazu die Behandlung rein inseparabler Körpererweiterungen in 3.7. Von Interesse sind insbesondere die Resultate 3.7/4 und 3.7/5, welche eine Aufspaltung algebraischer Körpererweiterungen in einen separablen und einen rein inseparablen Anteil ermöglichen. Als Beispiel studieren wir dann noch in 3.8 spezielle Körper der Charakteristik > 0, nämlich endliche Körper.

Das Kapitel schließt in 3.9 mit einem Ausblick auf die Anfänge der Algebraischen Geometrie, also auf die Theorie der algebraischen Gleichungen in mehreren unbekannten Größen.

3.1 Die Charakteristik eines Körpers

Ist K ein Ring, so gibt es genau einen Ringhomomorphismus

$$\varphi\colon \mathbb{Z} \longrightarrow K.$$

Dieser ist gegeben durch $n \longmapsto n \cdot 1$ und induziert aufgrund des Homomorphiesatzes für Ringe 2.3/4 einen Monomorphismus $\mathbb{Z}/\ker\varphi \hookrightarrow K$, wobei $\ker\varphi$ nach 2.4/3 ein Hauptideal ist. Handelt es sich bei K um einen Integritätsring, etwa einen Körper, so ist auch $\mathbb{Z}/\ker\varphi$ ein Integritätsring und somit $\ker\varphi$ ein Primideal. Dann ist $\ker\varphi$ entweder das Nullideal oder aber ein Ideal, welches von einer Primzahl p erzeugt wird, vgl. 2.3/11. Dementsprechend bezeichnet man 0 oder p als die *Charakteristik* des Integritätsrings oder Körpers K.

Definition 1. *Es sei K ein Körper* (*oder allgemeiner ein Integritätsring*) *und $\varphi\colon \mathbb{Z} \longrightarrow K$ der kanonische Ringhomomorphismus. Ist dann $p \in \mathbb{N}$ ein erzeugendes Element des Hauptideals* $\ker\varphi$, *so heißt p die* Charakteristik *von K, in Zeichen $p = \operatorname{char} K$.*

Die Körper $\mathbb{Q}, \mathbb{R}, \mathbb{C}$ haben alle die Charakteristik 0, wohingegen für eine Primzahl p der Körper mit p Elementen $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$ die Charakteristik p hat. Wir nennen einen Unterring T eines Körpers K einen *Teilkörper* (oder auch K einen *Oberkörper* von T), wenn T selbst ein Körper ist. Natürlich gilt dann $\operatorname{char} K = \operatorname{char} T$. Da der Durchschnitt von Teilkörpern eines Körpers K wieder ein Teilkörper ist, enthält K einen eindeutig bestimmten kleinsten Teilkörper P als Durchschnitt aller in K enthaltenen Teilkörper. Es wird P als *Primkörper* von K bezeichnet.

Satz 2. *Es sei K ein Körper und $P \subset K$ der Primkörper von K. Dann gilt*:

(i) $\operatorname{char} K = p > 0 \Longleftrightarrow P \simeq \mathbb{F}_p$ *mit p prim.*

(ii) $\operatorname{char} K = 0 \Longleftrightarrow P \simeq \mathbb{Q}$.

Daher gibt es bis auf Isomorphie nur die Primkörper $\mathbb{F}_p$ mit p prim sowie $\mathbb{Q}$.

Beweis. Es gilt $\operatorname{char} \mathbb{F}_p = p$ und $\operatorname{char} \mathbb{Q} = 0$. Wegen $\operatorname{char} P = \operatorname{char} K$ folgt dann $\operatorname{char} K = p$ aus $P \simeq \mathbb{F}_p$ und $\operatorname{char} K = 0$ aus $P \simeq \mathbb{Q}$. Dies begründet in (i) und (ii) jeweils die Implikation "$\Longleftarrow$".

Zum Beweis der umgekehrten Implikationen betrachte man den kanonischen Ringhomomorphismus $\varphi\colon \mathbb{Z} \longrightarrow K$; dieser faktorisiert durch den Primkörper $P \subset K$, d. h. es gilt $\operatorname{im}\varphi \subset P$. Ist $\operatorname{char} K$ eine Primzahl p, so gilt $\ker\varphi = (p)$, und es ist das Bild $\operatorname{im}\varphi \simeq \mathbb{Z}/(p)$ nach 2.3/6 oder 2.4/6 ein Körper. Da P der kleinste Teilkörper von K ist, folgt $\operatorname{im}\varphi = P$ und somit $P \simeq \mathbb{F}_p$. Gilt andererseits $\operatorname{char} K = 0$, so ist $\operatorname{im}\varphi$ isomorph zu $\mathbb{Z}$. Also ist der Quotientenkörper $Q(\operatorname{im}\varphi)$ ein zu $\mathbb{Q}$ isomorpher Teilkörper von P, so dass $P = Q(\operatorname{im}\varphi) \simeq \mathbb{Q}$ gilt. □

Wir wollen noch darauf hinweisen, dass in einem Körper der Charakteristik $p > 0$ die binomische Formel für p-Potenzen eine besonders einfache Gestalt annimmt.

Bemerkung 3. *Sei p eine Primzahl und R ein Integritätsring der Charakteristik p (oder allgemeiner ein Ring mit $p \cdot 1 = 0$). Dann gilt für $a, b \in R$ und $r \in \mathbb{N}$*

$$(a+b)^{p^r} = a^{p^r} + b^{p^r}, \qquad (a-b)^{p^r} = a^{p^r} - b^{p^r}.$$

Beweis. Mit vollständiger Induktion reduziert man die Aussage leicht auf den Fall $r = 1$. Nun hatten wir aber in Abschnitt 2.8 folgende Teilbarkeitsbeziehungen gezeigt:

$$p \mid \binom{p}{\nu}, \qquad \nu = 1, \ldots, p-1.$$

Die aufgeführten Binomialkoeffizienten verschwinden also in R. Damit folgen dann die behaupteten Formeln im Falle $r = 1$, wenn man noch benutzt, dass für gerades p, also für $p = 2$, in R die Gleichung $1 = -1$ gilt. □

Ist K ein Körper der Charakteristik $p > 0$, so zeigt Bemerkung 3, dass die Abbildung

$$\sigma \colon K \longrightarrow K, \qquad a \longmapsto a^p,$$

verträglich mit der Addition auf K ist. Sie definiert einen Körperhomomorphismus, den sogenannten *Frobenius-Homomorphismus* von K.

Lernkontrolle und Prüfungsvorbereitung

1. Wie ist die Charakteristik eines Körpers oder eines Integritätsrings definiert?
2. Was versteht man unter dem Primkörper eines gegebenen Körpers? Welche Primkörper gibt es?
3. Was versteht man unter dem Frobenius-Homomorphismus eines Körpers der Charakteristik $p > 0$? Beweise die zugehörige binomische Formel für den Exponent p.

Übungsaufgaben

1. *Gibt es Homomorphismen zwischen Körpern unterschiedlicher Charakteristik? Betrachte dasselbe Problem auch für Integritätsringe.*
2. Gibt es einen Körper mit 6 Elementen? Gibt es einen Integritätsring mit 6 Elementen?
3. Es sei K ein endlicher Körper mit multiplikativer Gruppe K^*. Zeige, dass $H = \{a^2 \,;\, a \in K^*\}$ eine Untergruppe von K^* ist mit

$$H = \begin{cases} K^*, \text{ falls } \operatorname{char} K = 2, \\ \text{Untergruppe in } K^* \text{ vom Index 2, falls } \operatorname{char} K > 2. \end{cases}$$

4. Es sei K ein Körper mit $\operatorname{char} K > 0$. Zeige, dass der Frobenius-Homomorphismus $\sigma\colon K \longrightarrow K$ ein Automorphismus ist, falls K endlich ist. Gilt dies auch ohne die Endlichkeitsbedingung an K?
5. Berechne den Frobenius-Homomorphismus von $\mathbb{F}_p$.

3.2 Endliche und algebraische Körpererweiterungen

Unter einer *Körpererweiterung* wollen wir ein Paar von Körpern $K \subset L$ verstehen, wobei K ein Teilkörper von L sei. Wir werden in dieser Situation auch etwas ungenauer sagen, L sei ein Erweiterungskörper bzw. eine "Körpererweiterung" von K. Insbesondere können wir die Multiplikation auf L einschränken zu einer Multiplikation $K \times L \longrightarrow L$ und auf diese Weise L als K-Vektorraum auffassen. Körpererweiterungen $K \subset L$ werden häufig in der Form L/K geschrieben, wenn eine Verwechslung mit Faktorgruppen- oder Faktorringkonstruktionen ausgeschlossen ist. Zu Körpererweiterungen L/K werden wir insbesondere *Zwischenkörper* betrachten, d. h. Körper E mit $K \subset E \subset L$.

Definition 1. *Es sei $K \subset L$ eine Körpererweiterung. Dann bezeichnet man die Vektorraumdimension $[L : K] := \dim_K L$ als den* Grad *der Körpererweiterung bzw. als den Grad von L über K. Die Körpererweiterung heißt* endlich *oder* unendlich, *je nachdem ob $[L : K]$ endlich oder unendlich ist.*

Offenbar ist $L = K$ äquivalent zu $[L : K] = 1$.

Satz 2 (Gradsatz). *Es seien $K \subset L \subset M$ Körpererweiterungen. Dann gilt*

$$[M : K] = [M : L] \cdot [L : K].$$

Beweis. Die Gleichung ist symbolisch zu verstehen, wenn einer der Grade unendlich ist. Wir nehmen jedoch zunächst an, dass beide Grade $[M : L]$ und $[L : K]$ endlich sind. In diesem Fall wähle man Vektorraumbasen $x_1, \ldots, x_m$ von L über K und $y_1, \ldots, y_n$ von M über L. Um die Beziehung $[M : K] = [M : L] \cdot [L : K] = mn$ herzuleiten, rechnen wir nach, dass die Elemente $x_i y_j$, $i = 1, \ldots m$, $j = 1, \ldots, n$, eine Vektorraumbasis von M über K bilden. Dazu zeigen wir in einem ersten Schritt, dass aus der

linearen Unabhängigkeit der x_i über K sowie der y_j über L die lineare Unabhängigkeit der $x_i y_j$ über K folgt. Seien also $c_{ij} \in K$ gegeben mit $\sum_{ij} c_{ij} x_i y_j = 0$. Die linke Seite schreiben wir dann als Linearkombination in den y_j mit Koeffizienten in L und erhalten

$$\sum_{j=1}^{n} \Big(\sum_{i=1}^{m} c_{ij} x_i \Big) y_j = 0.$$

Da die Elemente y_j linear unabhängig über L sind, ergibt sich $\sum_i c_{ij} x_i = 0$ für alle j. Ebenso folgt $c_{ij} = 0$ für alle i und j, da die x_i linear unabhängig über K sind. Also sind die $x_i y_j$ linear unabhängig über K.

Genauso einfach kann man sehen, dass die $x_i y_j$ ein Erzeugendensystem von M über K bilden. Jedes $z \in M$ hat nämlich eine Darstellung als Linearkombination $z = \sum_{j=1}^{n} c_j y_j$ mit Koeffizienten $c_j \in L$, da die y_j ein Erzeugendensystem von M über L bilden. Weiter gibt es für jedes j eine Darstellung $c_j = \sum_{i=1}^{m} c_{ij} x_i$ mit Koeffizienten $c_{ij} \in K$, da die x_i ein Erzeugendensystem von L über K bilden. Es folgt

$$z = \sum_{j=1}^{n} \sum_{i=1}^{m} c_{ij} x_i y_j,$$

und man sieht, dass die $x_i y_j$ ein Erzeugendensystem, insgesamt also eine Basis von M über K bilden.

Es bleibt noch der Fall zu behandeln, wo die Erweiterungen M/L und L/K nicht beide endlich sind. Im ersten Schritt des Beweises haben wir für über K linear unabhängige Elemente $x_1, \ldots, x_m \in L$ und für über L linear unabhängige Elemente $y_1, \ldots, y_n \in M$ gezeigt, dass die Produkte $x_i y_j$ linear unabhängig über K sind. Mit anderen Worten, aus $[L : K] \geq m$ und $[M : L] \geq n$ folgt $[M : K] \geq mn$. Daher ist $[M : K]$ unendlich, falls einer der Grade $[M : L]$ oder $[L : K]$ unendlich ist. □

Korollar 3. *Sind $K \subset L \subset M$ Körpererweiterungen und ist der Grad $p = [M : K]$ prim, so folgt $L = K$ oder $L = M$.*

Beispiele für endliche Körpererweiterungen vom Grad 2 sind die Erweiterungen $\mathbb{R} \subset \mathbb{C}$ oder $\mathbb{Q} \subset \mathbb{Q}[\sqrt{2}]$, wobei wir $\mathbb{Q}[\sqrt{2}]$ als Unterring von $\mathbb{R}$ auffassen. Andererseits sind die Erweiterungen $\mathbb{Q} \subset \mathbb{R}$ sowie

$K \subset K(X) = Q(K[X])$ für einen beliebigen Körper K und eine Variable X unendlich.

Definition 4. *Sei $K \subset L$ eine Körpererweiterung und $\alpha \in L$. Es heißt α* algebraisch *über K, wenn α eine algebraische Gleichung*

$$\alpha^n + c_1\alpha^{n-1} + \ldots + c_n = 0$$

mit Koeffizienten $c_1, \ldots, c_n \in K$ erfüllt, mit anderen Worten, wenn der Kern des Substitutionshomomorphismus

$$\varphi\colon K[X] \longrightarrow L, \qquad g \longmapsto g(\alpha),$$

von Null verschieden ist. Anderenfalls heißt α transzendent *über K. Schließlich nennt man L* algebraisch *über K, wenn jedes $\alpha \in L$ algebraisch über K ist.*

Beispielsweise ist für $q \in \mathbb{Q}$, $q \geq 0$, und $n \in \mathbb{N} - \{0\}$ die n-te Wurzel $\sqrt[n]{q} \in \mathbb{R}$ algebraisch über $\mathbb{Q}$, denn es ist $\sqrt[n]{q}$ Nullstelle des Polynoms $X^n - q$. Ebenso ist die komplexe Zahl $e^{2\pi i/n}$ als "n-te Wurzel der Eins" algebraisch über $\mathbb{Q}$. Im Allgemeinen ist es jedoch nicht einfach zu entscheiden, ob eine gegebene komplexe Zahl z algebraisch über $\mathbb{Q}$ ist oder nicht, insbesondere dann, wenn z mit Methoden der Analysis konstruiert wird; man vergleiche etwa das Problem der Transzendenz der Zahlen e und π, welches bereits in der Einführung erwähnt wurde.

Bemerkung 5. *Ist $K \subset L$ eine Körpererweiterung und $\alpha \in L$ algebraisch über K, so existiert ein eindeutig bestimmtes normiertes Polynom kleinsten Grades $f \in K[X]$ mit $f(\alpha) = 0$. Es gilt* $\ker\varphi = (f)$ *für den Kern des Substitutionshomomorphismus*

$$\varphi\colon K[X] \longrightarrow L, \qquad g \longmapsto g(\alpha).$$

Insbesondere ist f prim und somit irreduzibel. Man nennt f das Minimalpolynom *von α über K.*

Beweis. Es ist $K[X]$ ein Hauptidealring, vgl. 2.4/3. Folglich wird $\ker\varphi$ von einem Polynom $f \in K[X]$ erzeugt, und es gilt $f \neq 0$ aufgrund der Algebraizität von α. Als erzeugendes Element von $\ker\varphi$ ist f eindeutig

bis auf eine multiplikative Konstante aus K^*. Normieren wir daher f, so ist f eindeutig bestimmt; f ist das normierte Polynom kleinsten Grades in $K[X]$ mit $f(\alpha) = 0$. Da $\operatorname{im}\varphi$ als Unterring von L ein Integritätsring ist sowie aufgrund des Homomorphiesatzes 2.3/5 isomorph zu $K[X]/(f)$ ist, erkennt man f als prim bzw. irreduzibel; vgl. 2.3/8 und 2.4/6. □

Satz 6. *Es sei $K \subset L$ eine Körpererweiterung und $\alpha \in L$ algebraisch über K mit Minimalpolynom $f \in K[X]$. Bezeichnet $K[\alpha]$ den von α und K erzeugten Unterring von L, also das Bild unter dem Homomorphismus $\varphi\colon K[X] \longrightarrow L$, $g \longmapsto g(\alpha)$, so induziert φ einen Isomorphismus $K[X]/(f) \xrightarrow{\sim} K[\alpha]$.*

Hieraus folgt insbesondere, dass $K[\alpha]$ ein Körper ist, und zwar eine endliche Körpererweiterung von K vom Grade $[K[\alpha] : K] = \operatorname{grad} f$.

Beweis. Es gilt $K[\alpha] = \operatorname{im}\varphi \simeq K[X]/(f)$ aufgrund des Homomorphiesatzes. Da $\ker\varphi = (f)$ ein von Null verschiedenes Primideal in $K[X]$ ist, sieht man mit 2.4/6, dass dieses Ideal sogar maximal ist. Somit sind $K[X]/(f)$ und $K[\alpha]$ Körper.

Es bleibt noch

$$\dim_K K[X]/(f) = \operatorname{grad} f$$

zu zeigen. Sei etwa $f = X^n + c_1X^{n-1} + \ldots + c_n$, also $\operatorname{grad} f = n$. Die Division mit Rest durch f ist eindeutig in $K[X]$ in dem Sinne, dass es zu jedem $g \in K[X]$ eindeutig bestimmte Polynome $q, r \in K[X]$ gibt mit

$$g = qf + r, \qquad \operatorname{grad} r < n;$$

vgl. 2.1/4. Ist $\overline{X} \in K[X]/(f)$ die Restklasse zu $X \in K[X]$, so zeigt dies, dass jedes Element aus $K[X]/(f)$, aufgefasst als K-Vektorraum, eindeutig darstellbar ist als Linearkombination von $\overline{X}^0, \ldots, \overline{X}^{n-1}$ mit Koeffizienten in K. Letzteres besagt aber, dass $\overline{X}^0, \ldots, \overline{X}^{n-1}$ eine K-Basis von $K[X]/(f)$ bilden oder, wenn wir den Isomorphismus $K[\alpha] \simeq K[X]/(f)$ benutzen, dass $\alpha^0, \ldots, \alpha^{n-1}$ eine K-Basis von $K[\alpha]$ bilden. Es folgt $\dim_K K[X]/(f) = \dim_K K[\alpha] = n$. □

Wir wollen ein nahe liegendes Beispiel betrachten. Es sei p eine Primzahl und $n \in \mathbb{N} - \{0\}$. Dann ist $\sqrt[n]{p} \in \mathbb{R}$ algebraisch über $\mathbb{Q}$, also ist $\mathbb{Q}[\sqrt[n]{p}]$ eine endliche Körpererweiterung von $\mathbb{Q}$. Das Polynom $f = X^n - p \in \mathbb{Q}[X]$ ist irreduzibel aufgrund des Eisensteinschen Irreduzibilitätskriteriums 2.8/1

und hat $\sqrt[n]{p}$ als Nullstelle. Daher muss f als normiertes Polynom schon das Minimalpolynom von $\sqrt[n]{p}$ sein. Folglich gilt

$$\left[\mathbb{Q}\left[\sqrt[n]{p}\right] : \mathbb{Q}\right] = \operatorname{grad} f = n,$$

und man sieht insbesondere, dass die Erweiterung $\mathbb{R}/\mathbb{Q}$ nicht endlich sein kann.

Satz 7. *Jede endliche Körpererweiterung $K \subset L$ ist algebraisch.*

Beweis. Gelte etwa $[L : K] = n$, und sei $\alpha \in L$. Es sind dann die $n + 1$ Elemente $\alpha^0, \ldots, \alpha^n$ linear abhängig über K. Folglich gibt es eine nichttriviale Gleichung

$$c_0\alpha^0 + \ldots + c_n\alpha^n = 0$$

mit Koeffizienten $c_i \in K$, aus der man durch Normieren des höchsten nichttrivialen Koeffizienten eine algebraische Gleichung für α gewinnt. □

Die Umkehrung der Aussage dieses Satzes ist nicht richtig, wie wir weiter unten sehen werden. Es gibt algebraische Körpererweiterungen, die nicht endlich sind.

Ist $K \subset L$ eine Körpererweiterung und $\mathfrak{A} = (\alpha_i)_{i\in I}$ ein System von Elementen aus L (oder eine Teilmenge von L), so kann man den von $\mathfrak{A}$ über K erzeugten Teilkörper $K(\mathfrak{A}) \subset L$ betrachten. Dies ist der kleinste Teilkörper von L, welcher K und alle Elemente α_i enthält, d. h. $K(\mathfrak{A})$ ist der Durchschnitt aller Teilkörper von L, die K sowie alle α_i enthalten. Zu einer Körpererweiterung $K \subset L$ gibt es stets ein System $\mathfrak{A}$ von Elementen aus L mit $L = K(\mathfrak{A})$; beispielsweise nehme man für $\mathfrak{A}$ das System aller Elemente aus L. Den von endlich vielen Elementen $\alpha_1, \ldots, \alpha_n \in L$ über K erzeugten Teilkörper $K(\alpha_1, \ldots, \alpha_n) \subset L$ wollen wir explizit beschreiben. Er enthält notwendig den Ring $K[\alpha_1, \ldots, \alpha_n]$ aller polynomialen Ausdrücke $f(\alpha_1, \ldots, \alpha_n)$ zu Polynomen $f \in K[X_1, \ldots, X_n]$ und damit dessen Quotientenkörper, so dass

$$K(\alpha_1, \ldots, \alpha_n) = Q\big(K[\alpha_1, \ldots, \alpha_n]\big)$$

gilt. Es besteht also $K(\alpha_1, \ldots, \alpha_n)$ aus allen Quotienten der Form

$$\frac{f(\alpha_1, \ldots, \alpha_n)}{g(\alpha_1, \ldots, \alpha_n)}$$

mit $f, g \in K[X_1, \ldots, X_n]$, $g(\alpha_1, \ldots, \alpha_n) \neq 0$. Für ein beliebiges System $\mathfrak{A} = (\alpha_i)_{i \in I}$ von Elementen aus L lässt sich der Körper $K(\mathfrak{A})$ in gleicher Weise beschreiben, indem man Polynome aus $K[\mathfrak{X}]$ mit einem System $\mathfrak{X} = (X_i)_{i \in I}$ von Variablen benutzt. Alternativ kann man sich aber $K(\mathfrak{A})$ auch als Vereinigung aller Teilkörper des Typs $K(\alpha_{i_1}, \ldots, \alpha_{i_s})$ mit $i_1, \ldots, i_s \in I$ vorstellen.

Definition 8. *Eine Körpererweiterung $K \subset L$ heißt* einfach, *wenn es ein Element $\alpha \in L$ mit $L = K(\alpha)$ gibt. Der Grad $[K(\alpha) : K]$ wird auch als der* Grad *von α über K bezeichnet.*

Eine Körpererweiterung L/K heißt endlich erzeugt, *wenn es endlich viele Elemente $\alpha_1, \ldots, \alpha_n \in L$ mit $L = K(\alpha_1, \ldots, \alpha_n)$ gibt.*

Satz 9. *Es sei $L = K(\alpha_1, \ldots, \alpha_n)$ eine endlich erzeugte Körpererweiterung von K. Sind dann $\alpha_1, \ldots, \alpha_n$ algebraisch über K, so gilt*:

(i) $L = K(\alpha_1, \ldots, \alpha_n) = K[\alpha_1, \ldots, \alpha_n]$.

(ii) *L ist eine endliche und damit insbesondere algebraische Körpererweiterung von K.*

Beweis. Wir schließen mit Induktion nach n. Der Fall $n = 1$ wurde bereits in Satz 6 behandelt. Sei also $n > 1$. Nach Induktionsvoraussetzung dürfen wir annehmen, dass $K[\alpha_1, \ldots, \alpha_{n-1}]$ eine endliche Körpererweiterung von K ist. Weiter folgt aus Satz 6, dass $K[\alpha_1, \ldots, \alpha_n]$ eine endliche Körpererweiterung von $K[\alpha_1, \ldots, \alpha_{n-1}]$ ist. Dann ist $K[\alpha_1, \ldots, \alpha_n]$ nach Satz 2 auch endlich über K, also nach Satz 7 insbesondere algebraisch über K. Da $K[\alpha_1, \ldots, \alpha_n]$ bereits ein Körper ist, stimmt $K(\alpha_1, \ldots, \alpha_n)$ mit $K[\alpha_1, \ldots, \alpha_n]$ überein. □

Der Satz beinhaltet insbesondere die nicht offensichtliche Aussage, dass eine einfache Körpererweiterung L/K, die von einem algebraischen Element erzeugt wird, selbst algebraisch ist, was bedeutet, dass *jedes* Element von L algebraisch über K ist. Unter Benutzung dieser Tatsache kann man beispielsweise leicht sehen, dass für $n \in \mathbb{N} - \{0\}$ die reelle Zahl $\cos \frac{\pi}{n}$ algebraisch über $\mathbb{Q}$ ist. Es ist nämlich $\cos \frac{\pi}{n} = \frac{1}{2}(e^{\pi i/n} + e^{-\pi i/n})$ enthalten in $\mathbb{Q}(e^{\pi i/n})$, wobei das Element $e^{\pi i/n}$ als $2n$-te Wurzel der 1 algebraisch über $\mathbb{Q}$ ist. Da eine endliche Körpererweiterung L/K stets endlich erzeugt ist, etwa von einer K-Basis von L, erhält man als Zusammenfassung der Sätze 7 und 9:

Korollar 10. *Es sei $K \subset L$ eine Körpererweiterung. Dann ist äquivalent*:
(i) *L/K ist endlich.*
(ii) *L wird über K von endlich vielen algebraischen Elementen erzeugt.*
(iii) *L ist endlich erzeugte algebraische Körpererweiterung von K.*

Ist $\mathfrak{A} = (\alpha_i)_{i \in I}$ ein Erzeugendensystem einer Körpererweiterung L/K, so ist L die Vereinigung aller Teilkörper des Typs $K(\alpha_{i_1}, \ldots, \alpha_{i_s})$ mit Indizes $i_1, \ldots, i_s \in I$. Insbesondere folgt mit Korollar 10, dass L/K algebraisch ist, sofern alle α_i algebraisch über K sind. Somit ergibt sich folgende Charakterisierung (nicht notwendig endlich erzeugter) algebraischer Körpererweiterungen:

Korollar 11. *Es sei $K \subset L$ eine Körpererweiterung. Dann ist äquivalent*:
(i) *L/K ist algebraisch.*
(ii) *L wird über K von algebraischen Elementen erzeugt.*

Wir wollen schließlich noch zeigen, dass der Begriff der algebraischen Körpererweiterung in nahe liegender Weise transitiv ist.

Satz 12. *Es seien $K \subset L \subset M$ Körpererweiterungen. Ist $\alpha \in M$ algebraisch über L und ist L/K algebraisch, so ist α auch algebraisch über K. Insbesondere ist die Erweiterung M/K genau dann algebraisch, wenn M/L und L/K algebraisch sind.*

Beweis. Sei $f = X^n + c_1 X^{n-1} + \ldots + c_n \in L[X]$ das Minimalpolynom von α über L. Dann ist α schon über dem Teilkörper $K(c_1, \ldots, c_n)$ von L algebraisch, was gemäß Satz 6

$$\big[K(c_1, \ldots, c_n, \alpha) : K(c_1, \ldots, c_n)\big] < \infty$$

bedeutet. Da man aber nach Satz 9

$$\big[K(c_1, \ldots, c_n) : K\big] < \infty$$

hat, ergibt sich aus Satz 2

$$\big[K(c_1, \ldots, c_n, \alpha) : K\big] < \infty.$$

Dann ist $K(c_1, \ldots, c_n, \alpha)$ algebraisch über K nach Satz 7, insbesondere also α algebraisch über K.

Die gerade gegebene Argumentation zeigt, dass M/K algebraisch ist, sofern M/L und L/K algebraisch sind. Die Umkehrung hierzu ist trivial.

□

Zum Schluss wollen wir noch ein Beispiel einer algebraischen Körpererweiterung angeben, die nicht endlich ist, sich also auch nicht endlich erzeugen lässt. Man setze

$$L = \{\alpha \in \mathbb{C}\,;\ \alpha \text{ ist algebraisch über } \mathbb{Q}\}.$$

Zunächst ist L ein Erweiterungskörper von $\mathbb{Q}$, denn mit $\alpha, \beta \in L$ hat man auch $\mathbb{Q}(\alpha, \beta) \subset L$; vgl. Korollar 12. Nach Definition ist $L/\mathbb{Q}$ algebraisch. Weiter gilt $[L : \mathbb{Q}] = \infty$, da L etwa $\mathbb{Q}(\sqrt[n]{p})$ für $n \in \mathbb{N} - \{0\}$ und p prim als Teilkörper enthält und da, wie wir gesehen haben, $\mathbb{Q}(\sqrt[n]{p})$ den Grad n über $\mathbb{Q}$ hat. Man schreibt $L = \overline{\mathbb{Q}}$ und nennt $\overline{\mathbb{Q}}$ den *algebraischen Abschluss* von $\mathbb{Q}$ in $\mathbb{C}$.

Lernkontrolle und Prüfungsvorbereitung

1. Was ist eine Körpererweiterung, was versteht man unter dem Grad einer Körpererweiterung? Was ist eine endliche Körpererweiterung?
2. Formuliere den Gradsatz für Körpererweiterungen und beweise ihn.
3. Es sei L/K eine Körpererweiterung, deren Grad $[L\colon K]$ eine Primzahl ist. Welche Zwischenkörper gibt es zu L/K?
4. Es sei L/K eine Körpererweiterung. Wann heißt ein Element $\alpha \in L$ algebraisch über K, wann transzendent? Wann heißt die Erweiterung L/K algebraisch?
5. Zeige, dass die Erweiterung $\mathbb{C}/\mathbb{Q}$ Zwischenkörper L von beliebig großem Grad $[L\colon \mathbb{Q}]$ besitzt.
6. Zeige, dass jede endliche Körpererweiterung algebraisch ist. Gib ein Beispiel dafür, dass die Umkehrung hierzu nicht richtig ist.
7. Sei L/K eine Körpererweiterung und seien $\alpha_1, \ldots, \alpha_n \in L$. Erkläre die Symbole $K[\alpha_1, \ldots, \alpha_n]$ und $K(\alpha_1, \ldots, \alpha_n)$. Wann nennt man L/K eine einfache Körpererweiterung, wann eine endlich erzeugte Körpererweiterung?
8. Zeige, dass jede einfache Körpererweiterung, die von einem algebraischen Element erzeugt wird, algebraisch ist. Im Einzelnen ist Folgendes gefragt: Es sei L/K eine Körpererweiterung und $\alpha \in L$ ein Element, welches algebraisch

über K ist. Definiere das Minimalpolynom von α über K und beschreibe den von α erzeugten Zwischenkörper $K(\alpha)$ zur Erweiterung L/K. Bestimme den Grad $[K(\alpha) : K]$ und zeige, dass die Erweiterung $K(\alpha)/K$ algebraisch ist.

9. Sei L/K eine Körpererweiterung, und seien $\alpha, \beta \in L$ algebraisch über K. Zeige, dass dann auch $\alpha + \beta$ algebraisch über K ist. Zeige allgemeiner, dass die Menge aller Elemente $\alpha \in L$, so dass α algebraisch über K ist, einen Zwischenkörper zu L/K bildet, der algebraisch über K ist.

10. Es sei L/K eine Körpererweiterung, und seien $\alpha_1, \ldots, \alpha_n \in L$ algebraisch über K. Zeige $K(\alpha_1, \ldots, \alpha_n) = K[\alpha_1, \ldots, \alpha_n]$ und weiter, dass die Erweiterung $K(\alpha_1, \ldots, \alpha_n)/K$ endlich und insbesondere algebraisch ist.

+11. Die Körpererweiterung L/K werde von Elementen erzeugt, die algebraisch über K sind. Zeige, dass L/K algebraisch ist.

+12. Seien $K \subset L \subset M$ Körpererweiterungen. Zeige, dass M/K genau dann algebraisch ist, wenn die Erweiterungen M/L und L/K algebraisch sind. Gilt dieselbe Aussage auch für "endlich" anstelle von "algebraisch"?

Übungsaufgaben

1. *Es sei L/K eine Körpererweiterung. Überlege im Detail, wie man zeigt, dass mit zwei Elementen $\alpha, \beta \in L$ auch deren Summe $\alpha + \beta$ algebraisch über K ist.*

2. *Charakterisiere algebraische Körpererweiterungen mittels endlicher Körpererweiterungen.*

3. *Begründe, dass jedes Element aus $\mathbb{C} - \overline{\mathbb{Q}}$ transzendent über $\overline{\mathbb{Q}}$ ist.*

4. Sei L/K eine endliche Körpererweiterung, so dass $p = [L : K]$ prim ist. Zeige: Es existiert ein $\alpha \in L$ mit $L = K(\alpha)$.

5. Sei L/K eine endliche Körpererweiterung vom Grad $[L : K] = 2^k$ und sei $f \in K[X]$ ein Polynom vom Grad 3, welches in L eine Nullstelle hat. Zeige, f hat bereits eine Nullstelle in K.

6. Zeige: Eine Körpererweiterung L/K ist genau dann algebraisch, wenn jeder Unterring R mit $K \subset R \subset L$ bereits ein Körper ist.

7. Sei L/K eine endliche Körpererweiterung. Zeige:
   (i) Für $\alpha \in L$ stimmt das Minimalpolynom von α über K überein mit dem Minimalpolynom des K-Vektorraumhomomorphismus $\varphi_\alpha \colon L \longrightarrow L$, $x \longmapsto \alpha x$.
   (ii) Gilt $L = K(\alpha)$, so stimmt das Minimalpolynom von α über K mit dem charakteristischen Polynom von φ_α überein.

(iii) Für $\alpha \in L$ nennt man das charakteristische Polynom von φ_α auch das *Körperpolynom* von α bezüglich der Erweiterung L/K. Dieses ist stets eine Potenz des Minimalpolynoms von α über K.

8. Sei $\alpha \in \mathbb{C}$ mit $\alpha^3 + 2\alpha - 1 = 0$. Es ist α algebraisch über $\mathbb{Q}$. Bestimme das Minimalpolynom von α sowie dasjenige von $\alpha^2 + \alpha$, jeweils über $\mathbb{Q}$.

9. Sei K ein Körper und x ein Element eines Erweiterungskörpers von K, so dass x transzendent über K ist. Zeige: Für $n \in \mathbb{N} - \{0\}$ ist x^n transzendent über K, und es gilt $[K(x) : K(x^n)] = n$.

10. Sei L/K eine Körpererweiterung und $\alpha \in L$ algebraisch über K. Zeige: Für $n \in \mathbb{N} - \{0\}$ gilt $[K(\alpha^n) : K] \geq \frac{1}{n}[K(\alpha) : K]$.

11. Sei K ein Körper und $K(X)$ der Funktionenkörper einer Variablen über K. Sei $q = f/g \in K(X) - K$ mit teilerfremden Polynomen $f, g \in K[X]$. Zeige, dass q transzendent über K ist und dass

$$\big[K(X) : K(q)\big] = \max(\operatorname{grad} f, \operatorname{grad} g)$$

gilt. Bestimme das Minimalpolynom von X über $K(q)$. (*Hinweis*: Benutze Aufgabe 3 aus Abschnitt 2.7.)

12. Sei L/K eine Körpererweiterung. Zeige: Zwei Elemente $\alpha, \beta \in L$ sind genau dann algebraisch über K, wenn $\alpha + \beta$ und $\alpha \cdot \beta$ algebraisch über K sind.

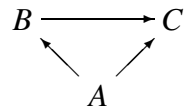
13. Es seien $\alpha, \beta \in \mathbb{C}$ sowie $m, n \in \mathbb{N}$ mit $\mathrm{ggT}(m, n) = 1$, so dass $\alpha^m = 2$, $\beta^n = 3$ gilt. Zeige $\mathbb{Q}(\alpha, \beta) = \mathbb{Q}(\alpha \cdot \beta)$ und bestimme das Minimalpolynom von $\alpha \cdot \beta$ über $\mathbb{Q}$.

3.3 Ganze Ringerweiterungen*

Wir wollen im Folgenden zeigen, dass die in Abschnitt 3.2 behandelte Theorie endlicher bzw. algebraischer Körpererweiterungen in vielerlei Hinsicht als Spezialfall der hier zu behandelnden Theorie ganzer Ringerweiterungen anzusehen ist. Sollte man allerdings lediglich an Körpererweiterungen interessiert sein, so sei angemerkt, dass der allgemeinere Rahmen der Ringtheorie auch für diese Situation neue Einsichten liefert, wie z. B. Korollar 8 zeigen wird. Als technisches Hilfsmittel hatten wir in 3.2 Vektorräume über Körpern benutzt. Entsprechend werden wir bei der Behandlung von Ringerweiterungen mit Moduln operieren. Zur Definition von Moduln über Ringen sei auf Abschnitt 2.9 verwiesen.

Zu einer Ringerweiterung $R \subset R'$ kann man stets die Inklusionsabbildung $R \hookrightarrow R'$ als Ringhomomorphismus betrachten. Wir werden im Folgenden statt von Ringerweiterungen allgemeiner von Ringhomomorphismen ausgehen. Für jeden Ringhomomorphismus $\varphi\colon A \longrightarrow B$ lässt sich B in natürlicher Weise als A-Modul auffassen; man multipliziere Elemente $a \in A$ mit Elementen $b \in B$, indem man jeweils das Produkt $\varphi(a)b$ in B bilde. Es wird φ als *endlich* bezeichnet, wenn B unter φ ein endlicher A-Modul ist; in anderer Sprechweise sagen wir auch, B sei endlich über A oder, falls φ eine Inklusionsabbildung ist, die Erweiterung $A \hookrightarrow B$ sei endlich. Weiter heiße φ, bzw. B über A, bzw. die Ringerweiterung $A \hookrightarrow B$ *von endlichem Typ*, wenn es einen Epimorphismus $\Phi\colon A[X_1, \ldots, X_n] \longrightarrow B$ eines Polynomrings in endlich vielen Variablen über A nach B gibt, der φ fortsetzt. Jeder endliche Ringhomomorphismus ist insbesondere auch von endlichem Typ. Dass ein Homomorphismus $\varphi\colon A \longrightarrow B$ von endlichem Typ ist, können wir auch dadurch charakterisieren, dass es Elemente $x_1, \ldots, x_n \in B$ mit $B = \varphi(A)[x_1, \ldots, x_n]$ gibt. Dabei ist $\varphi(A)[x_1, \ldots, x_n] \subset B$, wie in 2.5 erklärt, der Unterring aller Ausdrücke $f(x_1, \ldots, x_n)$ zu Polynomen $f \in \varphi(A)[X_1, \ldots, X_n]$. Wir werden diesen Ring der Einfachheit halber auch mit $A[x_1, \ldots, x_n]$ bezeichnen.

In der vorstehenden Situation wird häufig die Terminologie der Algebren benutzt. Eine *Algebra* B über einem Ring A ist nichts anderes als ein Ringhomomorphismus $A \longrightarrow B$. Insbesondere kann man also von (modul-)endlichen A-Algebren sprechen oder auch von A-Algebren von endlichem Typ. Am Rande sei noch erwähnt, dass man unter einem Homomorphismus zwischen zwei A-Algebren B und C nicht lediglich einen beliebigen Ringhomomorphismus $B \longrightarrow C$ versteht, sondern einen solchen, der mit den definierenden Homomorphismen $A \longrightarrow B$ und $A \longrightarrow C$ verträglich ist, so dass also das Diagramm



kommutiert.

Es ist klar, dass eine Körpererweiterung $K \subset L$ genau dann endlich ist, wenn sie als Ringerweiterung endlich ist. Man beachte allerdings, dass eine entsprechende Aussage für endlich erzeugte Körpererweiterungen bzw. Ringerweiterungen von endlichem Typ nicht gilt. Es ist $K \subset L$ zwar als

Körpererweiterung endlich erzeugt, sofern $K \subset L$ als Ringerweiterung von endlichem Typ ist. Die Umkehrung hierzu ist jedoch nicht allgemein richtig, wie wir am Ende dieses Abschnittes noch erläutern werden. Wir wollen nun zunächst den Begriff der algebraischen Körpererweiterung auf Ringerweiterungen übertragen.

Lemma 1. *Man betrachte einen Ringhomomorphismus $\varphi\colon A \longrightarrow B$ sowie ein Element $b \in B$. Dann ist äquivalent*:

(i) *Es existiert eine* ganze Gleichung *von b über A, d. h. eine Gleichung der Form $f(b) = 0$ mit einem normierten Polynom $f \in A[X]$.*

(ii) *Der Unterring $A[b] \subset B$ ist als A-Modul endlich erzeugt.*

(iii) *Es existieren endlich viele Elemente $m_1, \ldots, m_n \in B$, welche einen A-Untermodul $M = \sum_{i=1}^{n} Am_i \subset B$ mit $1 \in M$ und $bM \subset M$ erzeugen.*

Beweis. Wir beginnen mit der Implikation (i) $\Longrightarrow$ (ii). Es existiere also eine Gleichung $f(b) = 0$ mit einem normierten Polynom $f \in A[X]$, etwa

$$b^n + a_1 b^{n-1} + \ldots + a_n = 0.$$

Damit ist b^n ein Element des A-Moduls $M = \sum_{i=0}^{n-1} Ab^i$, und es folgt per Induktion $b^i \in M$ für alle $i \in \mathbb{N}$, also $A[b] \subset M$ bzw. $A[b] = M$. Es ist dann $A[b]$ ein endlich erzeugter A-Modul, d. h. es gilt (ii).

Die Implikation (ii) $\Longrightarrow$ (iii) ist trivial, es bleibt also nur noch die Implikation (iii) $\Longrightarrow$ (i) zu verifizieren. Sei $M = \sum_{i=1}^{n} Am_i \subset B$ ein endlich erzeugter A-Untermodul von B mit $1 \in M$ und $bM \subset M$. Aufgrund letzterer Inklusion existiert dann ein Gleichungssystem

$$\begin{aligned} bm_1 &= a_{11}m_1 + \ldots + a_{1n}m_n, \\ &\ldots \\ &\ldots \\ &\ldots \\ bm_n &= a_{n1}m_1 + \ldots + a_{nn}m_n, \end{aligned}$$

mit Koeffizienten $a_{ij} \in A$. Dieses lässt sich in Matrixform zusammenfassen zu

$$\Delta \cdot \begin{pmatrix} m_1 \\ \vdots \\ m_n \end{pmatrix} = 0,$$

mit der Matrix $\Delta = (\delta_{ij} b - a_{ij})_{i,j=1,\dots,n} \in B^{n\times n}$, wobei δ_{ij} das Kronecker-Symbol bezeichnet; $\delta_{ij} = 1$ für $i = j$ sowie $\delta_{ij} = 0$ für $i \neq j$. Wir verwenden nun die "Cramersche Regel", d. h. die Beziehung

$$(*) \qquad \Delta^* \cdot \Delta = (\det \Delta) \cdot E;$$

vgl. etwa [4], Satz 4.4/3. Dabei ist $\Delta^* \in B^{n\times n}$ die zu Δ adjungierte Matrix sowie $E \in B^{n\times n}$ die Einheitsmatrix. Diese Gleichung wird in der Linearen Algebra für Matrizen mit Koeffizienten aus einem Körper bewiesen und gilt aber auch in der hier benötigten allgemeineren Version über einem Ring B. Es stellt $(*)$ nämlich, wenn man links und rechts etwa die Koeffizienten der auftauchenden Matrizen betrachtet, ein System polynomialer Identitäten zwischen den Koeffizienten von Δ dar. Diese Identitäten lassen sich allgemein, indem man die Koeffizienten c_{ij} von Δ als Variablen ansieht, über dem Ring $\mathbb{Z}[c_{ij}]$ formulieren und aus dem bekannten, in der Linearen Algebra behandelten Körperfall ableiten, wenn man zum Quotientenkörper $\mathbb{Q}(c_{ij})$ übergeht.

Unter Benutzung von $(*)$ ergibt sich

$$(\det \Delta) \cdot \begin{pmatrix} m_1 \\ \vdots \\ m_n \end{pmatrix} = \Delta^* \cdot \Delta \cdot \begin{pmatrix} m_1 \\ \vdots \\ m_n \end{pmatrix} = 0,$$

d. h. $(\det \Delta) \cdot m_i = 0$ für $i = 1, \dots, n$. Da sich das neutrale Element der Multiplikation $1 \in B$ als Linearkombination der m_i mit Koeffizienten aus A darstellen lässt, folgt $\det \Delta = (\det \Delta) \cdot 1 = 0$. Damit ist

$$\det(\delta_{ij} X - a_{ij})$$

ein normiertes Polynom in $A[X]$, welches wie gewünscht b als Nullstelle hat. □

Definition 2. *Sei $\varphi\colon A \longrightarrow B$ ein Ringhomomorphismus. Ein Element $b \in B$ heißt* ganz *über A bezüglich φ, wenn b und φ die äquivalenten Bedingungen von Lemma 1 erfüllen. Weiter sagt man, B sei* ganz *über A bzw. φ sei* ganz, *wenn jedes $b \in B$ ganz über A in dem vorstehend beschriebenen Sinne ist.*

Es ist offensichtlich, dass "Ganzheit" im Falle einer Körpererweiterung dem Begriff "algebraisch" entspricht. Durch den Beweis der in Lemma 1

genannten Äquivalenzen haben wir bereits die wesentlichen Zusammenhänge zwischen ganzen und endlichen Ringerweiterungen geklärt. Wir wollen einige spezielle Folgerungen explizit formulieren, und zwar handelt es sich um die Verallgemeinerung der Resultate 3.2/7, 3.2/9 und 3.2/12.

Korollar 3. *Jeder endliche Ringhomomorphismus $A \longrightarrow B$ ist ganz.*

Beweis. Man benutze Bedingung (iii) aus Lemma 1 mit $M = B$ zur Charakterisierung der Ganzheit von $A \longrightarrow B$. □

Korollar 4. *Es sei $\varphi\colon A \longrightarrow B$ ein Ringhomomorphismus von endlichem Typ, so dass etwa $B = A[b_1, \ldots, b_r]$ gelte. Sind dann die Elemente $b_1, \ldots, b_r \in B$ ganz über A, so ist $A \longrightarrow B$ endlich und insbesondere ganz.*

Beweis. Man betrachte die Kette von Ringerweiterungen

$$\varphi(A) \subset \varphi(A)[b_1] \subset \ldots \subset \varphi(A)[b_1, \ldots, b_r] = B.$$

Jede Teilerweiterung ist nach Lemma 1 endlich, und man schließt hieraus per Induktion leicht, dass dann auch B über A endlich ist. Für den Induktionsschritt multipliziere man die Elemente eines Modulerzeugendensystems von B über $\varphi(A)[b_1, \ldots, b_{r-1}]$ mit denen eines entsprechenden Systems von $\varphi(A)[b_1, \ldots, b_{r-1}]$ über A. Insgesamt erhält man dann ein Modulerzeugendensystem von B über A; man vergleiche hierzu auch die Argumentation im Beweis zu 3.2/2. □

Korollar 5. *Sind $A \longrightarrow B$, $B \longrightarrow C$ zwei endliche* (*bzw. ganze*) *Ringhomomorphismen, so ist auch deren Komposition $A \longrightarrow C$ endlich* (*bzw. ganz*).

Beweis. Der Fall "endlich" ergibt sich mit derselben Argumentation wie im Beweis zu Korollar 4. Seien nun $A \longrightarrow B$ und $B \longrightarrow C$ ganz, und sei $c \in C$. Dann erfüllt c eine ganze Gleichung über B:

$$c^n + b_1 c^{n-1} + \ldots + b_n = 0, \qquad b_1, \ldots, b_n \in B.$$

Hieraus folgt, dass $c \in C$ ganz über $A[b_1, \ldots, b_n]$ ist. Nach Korollar 4 ist also die Erweiterung $A[b_1, \ldots, b_n] \longrightarrow A[b_1, \ldots, b_n, c]$ endlich. Ebenfalls nach Korollar 4 ist $A \longrightarrow A[b_1, \ldots, b_n]$ endlich, so dass insgesamt

$A \longrightarrow A[b_1, \ldots, b_n, c]$ endlich ist. Dann ist dieser Homomorphismus aber auch ganz, vgl. Korollar 3, so dass insbesondere c ganz über A ist. Indem man c in C variieren lässt, sieht man, dass $A \longrightarrow C$ ganz ist. □

Wir wollen noch einen Satz beweisen, der von fundamentaler Bedeutung für das Studium von Algebren von endlichem Typ über Körpern ist. Ein analoges Resultat für Körpererweiterungen, nämlich die Aufspaltung einer beliebigen Körpererweiterung in einen rein transzendenten und einen algebraischen Teil, werden wir erst in 7.1 behandeln.

Theorem 6 (Noetherscher Normalisierungssatz). *Es sei K ein Körper und $K \hookrightarrow B$ eine von Null verschiedene K-Algebra von endlichem Typ. Dann existiert ein über K algebraisch unabhängiges System von Elementen $x_1, \ldots, x_r \in B$ (vgl. 2.5/6), so dass B endlich über dem Unterring $K[x_1, \ldots, x_r] \subset B$ ist.*

Mit anderen Worten, es existiert ein endlicher und injektiver Homomorphismus $K[X_1, \ldots, X_r] \hookrightarrow B$, wobei $K[X_1, \ldots, X_r]$ ein Polynomring in endlich vielen Variablen über K ist.

Beweis. Es sei $B = K[b_1, \ldots, b_n]$ für gewisse Elemente $b_1, \ldots, b_n \in B$. Sind $b_1, \ldots, b_n$ algebraisch unabhängig über K, so ist nichts zu zeigen. Seien also $b_1, \ldots, b_n$ algebraisch abhängig über K. Dann existiert eine nicht-triviale Relation der Form

$$(*) \qquad \sum_{(\nu_1 \ldots \nu_n) \in I} a_{\nu_1 \ldots \nu_n} b_1^{\nu_1} \ldots b_n^{\nu_n} = 0$$

mit Koeffizienten $a_{\nu_1 \ldots \nu_n} \in K^*$, wobei sich die Summation über eine endliche Menge I von n-Tupeln $(\nu_1, \ldots, \nu_n) \in \mathbb{N}^n$ erstreckt. Man führe nun neue Elemente $x_1, \ldots, x_{n-1} \in B$ ein, und zwar

$$x_1 = b_1 - b_n^{s_1}, \quad \ldots, \quad x_{n-1} = b_{n-1} - b_n^{s_{n-1}},$$

mit gewissen Exponenten $s_1, \ldots, s_{n-1} \in \mathbb{N} - \{0\}$, deren Wahl noch zu präzisieren ist. Es gilt dann

$$B = K[b_1, \ldots, b_n] = K[x_1, \ldots, x_{n-1}, b_n].$$

Indem man $b_i = x_i + b_n^{s_i}$, $i = 1, \ldots, n-1$, in die Relation $(*)$ einsetzt und Potenzen $b_i^{\nu_i} = (x_i + b_n^{s_i})^{\nu_i}$ aufspaltet in $b_n^{s_i \nu_i}$ sowie Terme niedrigeren Grades in b_n, ergibt sich eine neue Relation der Form

$$(**) \qquad \sum_{(\nu_1 \ldots \nu_n) \in I} a_{\nu_1 \ldots \nu_n} b_n^{s_1\nu_1 + \ldots + s_{n-1}\nu_{n-1} + \nu_n} + f(x_1, \ldots, x_{n-1}, b_n) = 0.$$

Dabei ist $f(x_1, \ldots, x_{n-1}, b_n)$ ein polynomialer Ausdruck in b_n mit Koeffizienten in $K[x_1, \ldots, x_{n-1}]$, wobei der zugehörige Grad in b_n echt kleiner ist als das Maximum aller Zahlen $s_1\nu_1 + \ldots + s_{n-1}\nu_{n-1} + \nu_n$ mit $(\nu_1, \ldots, \nu_n) \in I$. Wie man leicht einsehen kann, lassen sich die Zahlen $s_1, \ldots, s_{n-1} \in \mathbb{N}$ so wählen, dass die in $(**)$ auftauchenden Exponenten $s_1\nu_1 + \ldots + s_{n-1}\nu_{n-1} + \nu_n$ zu Indextupeln $(\nu_1, \ldots, \nu_n) \in I$ alle verschieden sind. Man wähle nämlich $t \in \mathbb{N}$ größer als das Maximum aller $\nu_1, \ldots, \nu_n$ mit $(\nu_1, \ldots, \nu_n) \in I$ und setze

$$s_1 = t^{n-1}, \ldots, s_{n-1} = t^1.$$

Fasst man nun $(**)$ als polynomiale Gleichung in b_n mit Koeffizienten aus $K[x_1, \ldots, x_{n-1}]$ auf, so überwiegt ein Term der Form ab_n^N mit einem Koeffizienten $a \in K^*$ dem Grade nach alle anderen Terme. Wir erhalten daher nach Multiplikation mit a^{-1} aus $(**)$ eine ganze Gleichung von b_n über $K[x_1, \ldots, x_{n-1}]$, und es folgt mit Korollar 4, dass die Erweiterung $K[x_1, \ldots, x_{n-1}] \hookrightarrow B$ endlich ist. Sind nun $x_1, \ldots, x_{n-1}$ algebraisch unabhängig über K, so ist man fertig. Ansonsten wendet man das beschriebene Verfahren erneut an, und zwar nunmehr auf den Ring $K[x_1, \ldots, x_{n-1}]$. In dieser Weise fährt man fort, bis man schließlich zu einem über K algebraisch unabhängigen System $x_1, \ldots, x_r$ gelangt. Dass die Erweiterung $K[x_1, \ldots, x_r] \hookrightarrow B$ endlich ist, ergibt sich mit Korollar 5. □

Man kann zeigen, dass die Zahl r in der Aussage des Noetherschen Normalisierungssatzes eindeutig bestimmt ist; es ist r die sogenannte *Dimension* des Ringes B. Für den Fall, dass B ein Integritätsring ist, lässt sich die Eindeutigkeit von r leicht auf eine entsprechende Eindeutigkeitsaussage über den Transzendenzgrad von Körpererweiterungen, vgl. 7.1/5, zurückführen. Wir wollen dies im Vorgriff auf 7.1 hier kurz erklären. Ist nämlich für über K algebraisch unabhängige Elemente $x_1, \ldots, x_r \in B$ die Erweiterung $K[x_1, \ldots, x_r] \hookrightarrow B$ endlich, so ist der Quotientenkörper $Q(B)$ algebraisch über der rein transzendenten Erweiterung $K(x_1, \ldots, x_r)$ von K. Folglich bilden $x_1, \ldots, x_r$ eine Transzendenzbasis von $Q(B)/K$, vgl. 7.1/2, und es gilt $\operatorname{transgrad}_K Q(B) = r$.

Wir wollen als Anwendung des Noetherschen Normalisierungssatzes noch zeigen, dass, wie bereits eingangs erwähnt, eine endlich erzeugte

Körpererweiterung nicht unbedingt eine Ringerweiterung von endlichem Typ zu sein braucht. Wir beginnen mit einem Hilfsresultat.

Lemma 7. *Es sei $A \hookrightarrow B$ eine ganze Erweiterung von Integritätsringen. Ist dann einer der Ringe A oder B ein Körper, so auch der andere.*

Beweis. Sei A ein Körper und $b \neq 0$ ein Element von B. Es erfüllt dann b eine ganze Gleichung über A, etwa

$$b^n + a_1 b^{n-1} + \ldots + a_n = 0, \qquad a_1, \ldots, a_n \in A.$$

Indem wir im Quotientenkörper von B mit einer geeigneten Potenz von b^{-1} multiplizieren, können wir $a_n \neq 0$ voraussetzen. Dann folgt wegen $a_n^{-1} \in A$

$$b^{-1} = -a_n^{-1}(b^{n-1} + a_1 b^{n-2} + \ldots + a_{n-1}) \in B,$$

und B ist Körper.

Ist umgekehrt B ein Körper, so betrachte man ein Element $a \in A$, $a \neq 0$. Dann erfüllt $a^{-1} \in B$ eine ganze Gleichung über A, etwa

$$a^{-n} + a_1 a^{-n+1} + \ldots + a_n = 0, \qquad a_1, \ldots, a_n \in A,$$

und es folgt

$$a^{-1} = -a_1 - a_2 a - \ldots - a_n a^{n-1} \in A,$$

d. h. A ist ein Körper. □

Korollar 8. *Man betrachte eine Körpererweiterung $K \subset L$, derart dass $L = K[x_1, \ldots, x_n]$ für gewisse Elemente $x_1, \ldots, x_n \in L$ gilt, d. h. die Ringerweiterung $K \subset L$ sei von endlichem Typ. Dann ist die Erweiterung $K \subset L$ bereits endlich.*

Beweis. Aufgrund des Noetherschen Normalisierungssatzes gibt es über K algebraisch unabhängige Elemente $y_1, \ldots, y_r$ in L, so dass die Ringerweiterung $K[y_1, \ldots, y_r] \hookrightarrow L$ endlich ist. Mit L ist nach Lemma 7 auch $K[y_1, \ldots, y_r]$ ein Körper. Ein Polynomring über K in r Variablen kann für $r > 0$ aber niemals ein Körper sein. Also folgt notwendig $r = 0$, und es ist die Erweiterung $K \hookrightarrow L$ bereits endlich. □

Eine Situation wie in Korollar 8 lässt sich leicht herstellen, wenn man Polynomringe modulo maximaler Ideale betrachtet.

Korollar 9. *Es sei $K[X_1, \ldots, X_n]$ der Polynomring in n Variablen über einem Körper K und $\mathfrak{m} \subset K[X_1, \ldots, X_n]$ ein maximales Ideal. Dann ist die kanonische Abbildung $K \longrightarrow K[X_1, \ldots, X_n]/\mathfrak{m} = L$ endlich und folglich L/K eine endliche Körpererweiterung.*

Beweis. Es gilt $L = K[x_1, \ldots, x_n]$, wobei $x_i \in L$ jeweils die Restklasse der Variablen X_i bezeichne. Weiter ist L ein Körper, da $\mathfrak{m}$ ein maximales Ideal in $K[X_1, \ldots, X_n]$ ist. Daher können wir mit Korollar 8 schließen, dass L/K eine endliche Körpererweiterung ist. □

Betrachten wir zu einem Körper K den Funktionenkörper $K(X)$ in einer Variablen X über K, so ist die Körpererweiterung $K(X)/K$ zwar endlich erzeugt, nämlich von der Variablen X, aber nach Korollar 8 als Ringerweiterung nicht von endlichem Typ, da der Grad $[K(X) : K]$ unendlich ist. Damit haben wir eingesehen, dass, wie eingangs bemerkt, die Eigenschaften "endlich erzeugt" und "von endlichem Typ" bei Körpererweiterungen im Allgemeinen nicht äquivalent sind.

Lernkontrolle und Prüfungsvorbereitung

1. Es sei A ein Ring. Was versteht man unter einer A-Algebra, was unter einem Homomorphismus von A-Algebren? Was ist eine A-Algebra von endlichem Typ? Charakterisiere diese Bildungen mittels Ringhomomorphismen.
2. Es sei $A \longrightarrow B$ ein Ringhomomorphismus. Wann bezeichnet man ein Element $b \in B$ als "ganz" über A, wann einen Homomorphismus $A \longrightarrow B$ als "ganz"? Gib einfache Definitionen, die analog sind zur Eigenschaft "algebraisch" bei Körpererweiterungen.
3. Erkläre für einen Ringhomomorphismus $A \longrightarrow B$ die fundamentalen äquivalenten Bedingungen, die man zur Charakterisierung der Ganzheit von Elementen $b \in B$ über A bzw. für die Ganzheit von $A \longrightarrow B$ nutzen kann.

[+]4. Beweise die Äquivalenz der unter Punkt 3 angesprochenen Bedingungen zur Charakterisierung der Ganzheit von Ringhomomorphismen.

5. Zeige, dass jeder endliche Ringhomomorphismus ganz ist.
6. Sei $B = A[b_1, \ldots, b_r]$ eine Algebra von endlichem Typ über einem Ring A, wobei die Elemente $b_1, \ldots, b_r \in B$ ganz über A seien. Zeige, dass B eine endliche und insbesondere ganze A-Algebra ist.

+7. Zeige, dass die Komposition von endlichen bzw. ganzen Ringhomomorphismen wieder endlich bzw. ganz ist.

8. Formuliere den Noetherschen Normalisierungssatz.

++9. Erkläre den Beweis des Noetherschen Normalisierungssatzes.

10. Betrachte einen injektiven Ringhomomorphismus $A \hookrightarrow B$ und zeige, dass A und B Körper sind, sobald dies für A oder B zutrifft.

11. Es sei L/K eine Körpererweiterung, die als Ringerweiterung von endlichem Typ ist. Zeige, dass L/K dann bereits eine endliche Körpererweiterung ist.

12. Sei $\mathfrak{m} \subset K[X_1, \ldots, X_n]$ ein maximales Ideal im Polynomring in n Variablen über einem Körper K. Zeige, dass der Restklassenring $L = K[X_1, \ldots, X_n]/\mathfrak{m}$ in kanonischer Weise eine endliche Körpererweiterung von K ist.

13. Begründe für eine Körpererweiterung L/K, dass die Eigenschaften "endlich erzeugt" im Sinne von Körpererweiterungen und "von endlichem Typ" im Sinne von Ringerweiterungen nicht äquivalent sind.

Übungsaufgaben

1. *Es sei $A \subset B$ eine ganze Ringerweiterung. Diskutiere die Frage, ob man zu einem Element $b \in B$ "das" Minimalpolynom über A erklären kann. Betrachte als Beispiel die Erweiterung*

$$A = \left\{ \sum c_i X^i \in K[X] \,;\, c_1 = 0 \right\} \subset K[X] = B,$$

wobei $K[X]$ der Polynomring einer Variablen über einem Körper K sei.

2. Für einen Ringhomomorphismus $A \longrightarrow B$ bezeichne $\overline{A}$ die Menge derjenigen Elemente aus B, die ganz über A sind. Zeige, dass $\overline{A}$ ein Unterring von B ist, mit der Eigenschaft, dass $A \longrightarrow B$ sich zu einem ganzen Homomorphismus $A \longrightarrow \overline{A}$ beschränkt. Es heißt $\overline{A}$ der *ganze Abschluss* von A in B.

3. Es sei A ein faktorieller Ring. Zeige, dass A ganz abgeschlossen in seinem Quotientenkörper ist, d. h. dass der ganze Abschluss von A in $Q(A)$ im Sinne von Aufgabe 2 mit A übereinstimmt.

4. Es sei $\varphi\colon A \hookrightarrow A'$ eine ganze Ringerweiterung. Zeige, dass für jedes maximale Ideal $\mathfrak{m}' \subset A'$ auch das Ideal $\varphi^{-1}(\mathfrak{m}') \subset A$ maximal ist und dass es umgekehrt zu jedem maximalen Ideal $\mathfrak{m} \subset A$ ein maximales Ideal $\mathfrak{m}' \subset A'$ mit $\varphi^{-1}(\mathfrak{m}') = \mathfrak{m}$ gibt. (*Hinweis*: Betrachte zu einem maximalen Ideal $\mathfrak{m} \subset A$ das multiplikative System $S = A - \mathfrak{m}$, sowie die zugehörigen Bruchringe $S^{-1}A$ und $S^{-1}A'$ gemäß Abschnitt 2.7. Es darf zudem benutzt werden, dass jeder von Null verschiedene Ring ein maximales Ideal besitzt; vgl. 3.4/6.)

3.4 Algebraischer Abschluss eines Körpers

Ziel dieses Abschnittes ist es, zu einem Körper K einen algebraischen Abschluss, d. h. einen minimalen algebraischen Erweiterungskörper $\overline{K}$ zu konstruieren, so dass jedes nicht-konstante Polynom aus $\overline{K}[X]$ eine Nullstelle in $\overline{K}$ besitzt. Wir beginnen mit dem bereits verschiedentlich erwähnten *Verfahren von Kronecker*, welches es erlaubt, zu einem nicht-konstanten Polynom $f \in K[X]$ einen endlich algebraischen Erweiterungskörper L/K zu konstruieren, derart dass f eine Nullstelle in L besitzt.

Satz 1. *Sei K ein Körper und $f \in K[X]$ ein Polynom vom Grad ≥ 1. Dann existiert eine endliche algebraische Körpererweiterung $K \subset L$, so dass f eine Nullstelle in L besitzt. Ist f irreduzibel, so kann man $L := K[X]/(f)$ setzen.*

Beweis. Man kann f als irreduzibel annehmen; ansonsten betrachte man eine Primfaktorzerlegung von f und ersetze f durch einen seiner irreduziblen Faktoren. Es ist dann (f) gemäß 2.4/6 ein maximales Ideal in $K[X]$ und folglich $L := K[X]/(f)$ ein Körper. Man bilde nun die Komposition

$$K \hookrightarrow K[X] \xrightarrow{\pi} K[X]/(f) = L,$$

wobei π der kanonische Epimorphismus sei. Der resultierende Homomorphismus $K \longrightarrow L$ ist als Homomorphismus zwischen Körpern injektiv, und wir können L als Erweiterungskörper von K auffassen, indem wir K mit seinem Bild unter $K \longrightarrow L$ identifizieren. Man setze nun $x := \pi(X)$. Mit $f = \sum_{i=0}^{n} c_i X^i$ folgt dann

$$f(x) = \sum_{i=0}^{n} c_i x^i = \sum_{i=0}^{n} c_i \pi(X)^i = \pi\Big(\sum_{i=0}^{n} c_i X^i\Big) = \pi(f) = 0,$$

d. h. x ist Nullstelle von f. Somit ist x algebraisch über K, und es gilt $L = K(x)$. Nimmt man f als normiert an, so erkennt man f als das Minimalpolynom von x über K, und es ergibt sich mit 3.2/6, dass L/K eine endliche Körpererweiterung vom Grad $n = \operatorname{grad} f$ ist. □

Bei dem Verfahren von Kronecker sagt man, dass L aus K durch *Adjunktion einer Nullstelle x* von f konstruiert wird. Die Nullstelle x von f wird

sozusagen "erzwungen", indem man ausgehend von $K[X]$ den Restklassenring $L = K[X]/(f)$ bildet. Man kann dann über L einen Linearfaktor von f abspalten und das Verfahren wiederholen. Nach endlich vielen Schritten gelangt man so zu einem Erweiterungskörper K' von K, über dem f komplett in Linearfaktoren zerfällt. Im Prinzip müsste man dieses Verfahren für alle nicht-konstanten Polynome in $K[X]$ gleichzeitig anwenden, um einen algebraischen Abschluss von K zu konstruieren.

Definition 2. *Ein Körper K heißt* algebraisch abgeschlossen, *falls jedes nicht-konstante Polynom f aus $K[X]$ eine Nullstelle in K besitzt oder, mit anderen Worten, falls f in $K[X]$ vollständig in Linearfaktoren zerfällt. Letzteres bedeutet, dass f eine Darstellung $f = c\prod_i(X - \alpha_i)$ mit einer Konstanten $c \in K^*$ sowie Nullstellen $\alpha_i \in K$ besitzt.*

Bemerkung 3. *Ein Körper K ist genau dann algebraisch abgeschlossen, wenn er keine echten algebraischen Körpererweiterungen L/K zulässt.*

Beweis. Sei zunächst K algebraisch abgeschlossen und sei $K \subset L$ eine algebraische Körpererweiterung. Wählen wir dann ein Element $\alpha \in L$ mit zugehörigem Minimalpolynom $f \in K[X]$, so zerfällt f über K in Linearfaktoren, ist also linear, da irreduzibel. Dies ergibt $\alpha \in K$ und somit $L = K$. Ist umgekehrt bekannt, dass K keine echten algebraischen Erweiterungen zulässt, so betrachte man ein Polynom $f \in K[X]$ mit grad $f \geq 1$. Nach dem Verfahren von Kronecker lässt sich eine algebraische Erweiterung L/K konstruieren, so dass f eine Nullstelle in L hat. Aufgrund unserer Annahme gilt dann $L = K$, so dass f schon eine Nullstelle in K hat. Damit sieht man, dass K algebraisch abgeschlossen ist. □

Theorem 4. *Zu jedem Körper K gibt es einen algebraisch abgeschlossenen Erweiterungskörper L.*

Zum Beweis verwenden wir die Existenz maximaler Ideale in Ringen $R \neq 0$, ein Resultat, das wiederum auf dem sogenannten Zornschen Lemma beruht. Das Zornsche Lemma ist tief im Bereich der Mengenlehre verwurzelt, so dass wir hier von einem Beweis absehen wollen und uns darauf beschränken, seine Aussage zu erklären, einschließlich der benötigten Begriffsbildungen.

Es sei M eine Menge. Eine (*partielle*) *Ordnung* auf M ist eine Relation $\leq$,[1] so dass gilt:

$$\begin{aligned} x \leq x \text{ für alle } x \in M \qquad & \text{(Reflexivität)} \\ x \leq y,\ y \leq z \implies x \leq z \qquad & \text{(Transitivität)} \\ x \leq y,\ y \leq x \implies x = y \qquad & \text{(Antisymmetrie)} \end{aligned}$$

Die Ordnung heißt *total* oder *streng*, wenn für je zwei Elemente $x, y \in M$ stets $x \leq y$ oder $y \leq x$ gilt, d. h. wenn alle Elemente aus M miteinander vergleichbar sind.

Die gewöhnliche Größenrelation $\leq$ zwischen reellen Zahlen stellt eine totale Ordnung auf $\mathbb{R}$ dar. Man kann aber auch von einer Menge X ausgehen und M als Potenzmenge von X definieren. Dann ist die Inklusion von Teilmengen in X eine partielle Ordnung auf M. Diese ist im Allgemeinen nicht total, da für $U, U' \subset X$ weder $U \subset U'$ noch $U' \subset U$ zu gelten braucht. In ähnlicher Weise kann man für einen Ring R die Menge M aller echten Ideale $\mathfrak{a} \subsetneq R$ mit der Inklusion als Ordnung betrachten. Es ist $\mathfrak{a}$ genau dann ein maximales Ideal in R, wenn $\mathfrak{a}$ maximales Element von M ist. Wir wollen diese Sprechweise präzisieren, indem wir für eine Menge M mit partieller Ordnung $\leq$ und ein Element $a \in M$ erklären:

a heißt *größtes* Element von M, wenn $x \leq a$ für alle $x \in M$ gilt.

a heißt *maximales* Element von M, wenn aus $a \leq x$ mit $x \in M$ stets $a = x$ folgt.

a heißt *obere Schranke* für eine Teilmenge $N \subset M$, wenn $x \leq a$ für alle $x \in N$ gilt.

Gibt es in M ein größtes Element a, so ist a das einzige maximale Element in M; es ist a als größtes Element eindeutig bestimmt. Im Allgemeinen gibt es jedoch in einer partiell geordneten Menge M verschiedene maximale Elemente und damit kein größtes Element.

Lemma 5 (Zorn). *Es sei M eine partiell geordnete Menge. Jede (bezüglich der induzierten Ordnung) total geordnete Teilmenge von M habe eine obere Schranke in M. Dann besitzt M ein maximales Element.*[2]

[1] Eine Relation auf M ist eine Teilmenge $R \subset M \times M$, wobei wir im vorliegenden Fall $x \leq y$ anstelle von $(x, y) \in R$ schreiben.

[2] Man beachte: Die leere Teilmenge in M ist total geordnet und besitzt daher aufgrund der Voraussetzung des Lemmas eine obere Schranke in M. Insbesondere wird auf diese Weise $M \neq \emptyset$ gefordert.

Bezüglich einer elementaren Herleitung der Aussage sei auf [11], Appendix 2, §2, verwiesen. Man muss allerdings hinzufügen, dass das Lemma von Zorn axiomatischen Charakter hat. Es ist äquivalent zum sogenannten Auswahlaxiom, welches besagt, dass das Produkt einer nicht-leeren Familie nicht-leerer Mengen nicht leer ist. Als Anwendung wollen wir zeigen:

Satz 6. *Es sei R ein Ring und $\mathfrak{a} \subsetneq R$ ein echtes Ideal. Dann besitzt R ein maximales Ideal $\mathfrak{m}$ mit $\mathfrak{a} \subset \mathfrak{m}$. Insbesondere besitzt also jeder Ring $R \neq 0$ ein maximales Ideal.*

Beweis. Es sei M die Menge der echten Ideale $\mathfrak{b} \subsetneq R$, welche $\mathfrak{a}$ umfassen. Dann ist M partiell geordnet bezüglich der Inklusion von Idealen. Das Ideal $\mathfrak{a}$ gehört zu M, also gilt $M \neq \emptyset$. Des Weiteren besitzt jede total geordnete Teilmenge $N \subset M$ eine obere Schranke in M. Sei nämlich N eine solche Teilmenge, wobei wir $N \neq \emptyset$ annehmen dürfen. Dann ist $\mathfrak{c} = \bigcup_{\mathfrak{b} \in N} \mathfrak{b}$ ein echtes Ideal in R, welches $\mathfrak{a}$ umfasst, wie man leicht unter Benutzung der totalen Ordnung auf N verifiziert, also als Element von M obere Schranke zu N. Folglich besitzt M nach dem Lemma von Zorn ein maximales Element und somit R ein maximales Ideal $\mathfrak{m}$ mit $\mathfrak{a} \subset \mathfrak{m}$. □

Beweis zu Theorem 4. Wir sind nun in der Lage, zu einem Körper K die Existenz eines algebraisch abgeschlossenen Oberkörpers L nachzuweisen. Das Verfahren, welches wir benutzen, verwendet den Polynomring in unendlich vielen Variablen über K und geht zurück auf E. Artin. In einem ersten Schritt konstruieren wir einen Erweiterungskörper L_1 von K, so dass jedes Polynom $f \in K[X]$ mit $\operatorname{grad} f \geq 1$ eine Nullstelle in L_1 besitzt. Hierzu betrachten wir ein System $\mathfrak{X} = (X_f)_{f \in I}$ von Variablen, indiziert durch die Indexmenge

$$I = \big\{ f \in K[X] \,;\ \operatorname{grad} f \geq 1 \big\},$$

sowie den Polynomring $K[\mathfrak{X}]$. In $K[\mathfrak{X}]$ liegt das Ideal

$$\mathfrak{a} = \big(f(X_f) \,;\ f \in I \big),$$

erzeugt von der Familie der Polynome $f(X_f)$, wobei die Variable X in f jeweils durch X_f ersetzt ist. Wir behaupten, dass $\mathfrak{a}$ ein echtes Ideal in $K[\mathfrak{X}]$ ist. Angenommen, dies ist nicht der Fall. Dann gilt $1 \in \mathfrak{a}$, und es gibt eine Gleichung

$$\sum_{i=1}^{n} g_i f_i(X_{f_i}) = 1$$

mit $f_1, \ldots, f_n \in I$ und $g_1, \ldots, g_n \in K[\mathfrak{X}]$. Nun existiert aber, wenn wir etwa das Verfahren von Kronecker auf die Polynome f_i anwenden, ein Erweiterungskörper K' von K, so dass jedes f_i eine Nullstelle α_i in K' hat. Wir dürfen dann in obiger Gleichung α_i für X_{f_i} substituieren, $i = 1, \ldots, n$, indem wir den Einsetzungshomomorphismus $K[\mathfrak{X}] \longrightarrow K'$ betrachten, der für X_{f_i} jeweils α_i einsetzt und für die restlichen Variablen einen beliebigen Wert aus K', etwa 0. Dann ergibt sich 0 auf der linken Seite der Gleichung, im Widerspruch zu 1 auf der rechten. Es ist somit $\mathfrak{a}$ ein echtes Ideal in $K[\mathfrak{X}]$, wie behauptet.

Man wähle nun gemäß Satz 6 ein maximales Ideal $\mathfrak{m} \subset K[\mathfrak{X}]$, welches das Ideal $\mathfrak{a}$ enthält. Dann ist $L_1 = K[\mathfrak{X}]/\mathfrak{m}$ ein Körper. Fasst man L_1 bezüglich der kanonischen Abbildungen

$$K \hookrightarrow K[\mathfrak{X}] \longrightarrow K[\mathfrak{X}]/\mathfrak{m} = L_1$$

als Erweiterungskörper von K auf, so sieht man ähnlich wie beim Verfahren von Kronecker, dass für $f \in I$ die zu $X_f \in K[\mathfrak{X}]$ gehörige Restklasse $\overline{X}_f$ in $K[\mathfrak{X}]/\mathfrak{m}$ eine Nullstelle von $f \in K[X]$ ist. Die Nullstellen sind formal bei der Restklassenbildung modulo $\mathfrak{a}$ bzw. $\mathfrak{m}$ erzwungen worden.

Um den Beweis von Theorem 4 zu beenden, verfahren wir folgendermaßen. Durch Iteration der gerade beschriebenen Konstruktion erhält man eine Körperkette

$$K = L_0 \subset L_1 \subset L_2 \subset \ldots,$$

so dass jedes Polynom $f \in L_n[X]$ mit $\operatorname{grad} f \geq 1$ eine Nullstelle in L_{n+1} hat. Es ist dann

$$L = \bigcup_{n=0}^{\infty} L_n$$

als Vereinigung einer aufsteigenden Kette von Körpern selbst wieder ein Körper, und wir behaupten, dass L algebraisch abgeschlossen ist. Sei nämlich $f \in L[X]$ mit $\operatorname{grad} f \geq 1$. Dann gibt es, da f nur endlich viele von 0 verschiedene Koeffizienten hat, ein $n \in \mathbb{N}$ mit $f \in L_n[X]$. Es folgt, dass f eine Nullstelle in L_{n+1} und damit in L hat. Somit ist L algebraisch abgeschlossen, die Aussage von Theorem 4 also bewiesen. □

Es soll hier vermerkt werden, dass in der Situation des vorstehenden Beweises bereits $L = L_1$ gilt; vgl. Aufgabe 10 in Abschnitt 3.7. Um dies einzusehen, sind allerdings Hilfsmittel erforderlich, die uns im Moment noch nicht zur Verfügung stehen.

Korollar 7. *Es sei K ein Körper. Dann gibt es einen algebraisch abgeschlossenen Oberkörper $\overline{K}$ von K, so dass $\overline{K}$ algebraisch über K ist*; *man nennt $\overline{K}$ einen* algebraischen Abschluss *von K.*

Beweis. Wenn man die soeben durchgeführte Konstruktion eines algebraisch abgeschlossenen Erweiterungskörpers L zu K verfolgt, so kann man leicht feststellen, dass L algebraisch über K ist und somit die Eigenschaften eines algebraischen Abschlusses von K besitzt. Es wird nämlich die Erweiterung L_n/L_{n-1} nach Konstruktion jeweils von einer Familie algebraischer Elemente erzeugt, so dass L_n/L_{n-1} gemäß 3.2/11 algebraisch ist. Dann folgt auf induktive Weise mit 3.2/12, dass alle L_n algebraisch über K sind, d. h. es ist L als Vereinigung der L_n algebraisch über K.

Man kann für einen beliebigen algebraisch abgeschlossenen Erweiterungskörper L von K aber auch folgendermaßen vorgehen. Man setze

$$\overline{K} = \big\{\alpha \in L\,;\ \alpha \text{ ist algebraisch über } K\big\}.$$

Es ist dann $\overline{K}$ ein Körper, also ein algebraischer Erweiterungskörper von K, da mit $\alpha, \beta \in \overline{K}$ auch $K(\alpha, \beta) \subset \overline{K}$ gilt. Weiter ist $\overline{K}$ algebraisch abgeschlossen, denn ist $f \in \overline{K}[X]$ mit $\operatorname{grad} f \geq 1$, so hat f eine Nullstelle γ in L. Letztere ist algebraisch über $\overline{K}$ und mit 3.2/12 algebraisch über K, so dass sich $\gamma \in \overline{K}$ ergibt. □

Als Beispiel können wir hier die (noch nicht bewiesene) Tatsache anführen, dass $\mathbb{C}$ ein algebraischer Abschluss von $\mathbb{R}$ ist. Weiter können wir einen algebraischen Abschluss $\overline{\mathbb{Q}}$ von $\mathbb{Q}$ erklären durch

$$\overline{\mathbb{Q}} = \big\{\alpha \in \mathbb{C}\,;\ \alpha \text{ ist algebraisch über } \mathbb{Q}\big\}.$$

Es gilt dann $\overline{\mathbb{Q}} \neq \mathbb{C}$, da $\mathbb{C}$ auch Elemente wie e oder π besitzt, die transzendent, also nicht algebraisch über $\mathbb{Q}$ sind. Die Ungleichung $\overline{\mathbb{Q}} \neq \mathbb{C}$ lässt sich andererseits auch durch ein Mächtigkeitsargument begründen, wenn man benutzt, dass der algebraische Abschluss eines Körpers bis auf (nichtkanonische) Isomorphie eindeutig ist (siehe Korollar 10). Es ist nämlich $\mathbb{C}$

von überabzählbarer Mächtigkeit, während die explizite Konstruktion eines algebraischen Abschlusses von $\mathbb{Q}$ mit dem Beweis zu Theorem 4 zeigt, dass $\overline{\mathbb{Q}}$ abzählbar ist.

Wir wollen abschließend noch zeigen, dass je zwei algebraische Abschlüsse eines Körpers K isomorph sind (wobei es im Allgemeinen verschiedene solcher Isomorphismen gibt). Hierzu müssen wir das Problem der Fortsetzbarkeit von Körperhomomorphismen $K \longrightarrow L$ auf algebraische Erweiterungen K'/K studieren. Wir wollen aber bereits an dieser Stelle darauf hinweisen, dass die nachstehend in Lemma 8 und Satz 9 bewiesenen Resultate nicht nur für die Frage der Eindeutigkeit des algebraischen Abschlusses von Interesse sind, sondern beispielsweise bei der Charakterisierung separabler Erweiterungen in 3.6 sowie für die Galois-Theorie in 4.1 eine fundamentale Rolle spielen.

Wir benötigen noch eine bequeme Notation für den Transport von Polynomen mittels Homomorphismen. Ist $\sigma\colon K \longrightarrow L$ ein Körperhomomorphismus und $K[X] \longrightarrow L[X]$ der induzierte Homomorphismus der Polynomringe, so bezeichnen wir für $f \in K[X]$ das Bild in $L[X]$ mit f^σ. Es folgt unmittelbar, dass für jede Nullstelle $\alpha \in K$ von f deren Bild $\sigma(\alpha)$ eine Nullstelle von f^σ ist.

Lemma 8. *Es sei K ein Körper und $K' = K(\alpha)$ eine einfache algebraische Körpererweiterung von K mit Minimalpolynom $f \in K[X]$ zu α. Weiter sei $\sigma\colon K \longrightarrow L$ ein Körperhomomorphismus.*

(i) *Ist $\sigma'\colon K' \longrightarrow L$ ein Körperhomomorphismus, welcher σ fortsetzt, so ist $\sigma'(\alpha)$ Nullstelle von f^σ.*

(ii) *Umgekehrt gibt es zu jeder Nullstelle $\beta \in L$ von $f^\sigma \in L[X]$ genau eine Fortsetzung $\sigma'\colon K' \longrightarrow L$ von σ mit $\sigma'(\alpha) = \beta$.*

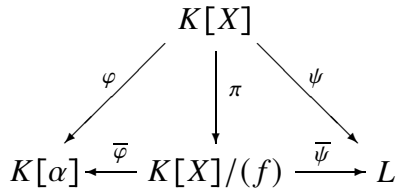
Insbesondere ist die Anzahl der verschiedenen Fortsetzungen σ' von σ gleich der Anzahl der verschiedenen Nullstellen von f^σ in L, also $\leq \operatorname{grad} f$.

Beweis. Für jede Fortsetzung $\sigma'\colon K' \longrightarrow L$ von σ folgt aus $f(\alpha) = 0$ notwendig $f^\sigma(\sigma'(\alpha)) = \sigma'(f(\alpha)) = 0$. Da weiter $K' = K[\alpha]$ nach 3.2/9 gilt, ist eine Fortsetzung $\sigma'\colon K' \longrightarrow L$ von σ schon eindeutig durch das Bild $\sigma'(\alpha)$ bestimmt.

Es bleibt noch zu zeigen, dass zu gegebener Nullstelle $\beta \in L$ von f^σ eine Fortsetzung $\sigma'\colon K' \longrightarrow L$ zu σ existiert mit $\sigma'(\alpha) = \beta$. Hierzu betrachte man die Substitutionshomomorphismen

$$\varphi\colon K[X] \longrightarrow K[\alpha], \qquad g \longmapsto g(\alpha),$$
$$\psi\colon K[X] \longrightarrow L, \qquad g \longmapsto g^{\sigma}(\beta).$$

Es gilt $(f) = \ker\varphi$ nach 3.2/5 sowie $(f) \subset \ker\psi$ wegen $f^{\sigma}(\beta) = 0$. Bezeichnet $\pi\colon K[X] \longrightarrow K[X]/(f)$ die kanonische Projektion, so erhält man aufgrund des Homomorphiesatzes 2.3/4 ein kommutatives Diagramm



mit eindeutig bestimmten Homomorphismen $\overline{\varphi}$ und $\overline{\psi}$. Da $\overline{\varphi}$ ein Isomorphismus ist, erkennt man $\sigma' := \overline{\psi} \circ \overline{\varphi}^{-1}$ als Fortsetzung von σ mit $\sigma'(\alpha) = \beta$. □

Satz 9. *Es sei $K \subset K'$ eine algebraische Körpererweiterung und $\sigma\colon K \longrightarrow L$ ein Körperhomomorphismus mit Bild in einem algebraisch abgeschlossenen Körper L. Dann gibt es zu σ eine Fortsetzung $\sigma'\colon K' \longrightarrow L$. Ist zusätzlich K' algebraisch abgeschlossen und L algebraisch über $\sigma(K)$, so ist jede Fortsetzung σ' von σ ein Isomorphismus.*

Beweis. Die wesentliche Arbeit wurde bereits in Lemma 8 geleistet, wir müssen lediglich noch das Lemma von Zorn anwenden. Sei also M die Menge aller Paare (F, τ), bestehend aus einem Zwischenkörper F, $K \subset F \subset K'$, und einer Fortsetzung $\tau\colon F \longrightarrow L$ von σ. Es ist dann M partiell geordnet unter der Größenrelation $\leq$, wenn wir $(F, \tau) \leq (F', \tau')$ setzen, falls $F \subset F'$ und $\tau'|_F = \tau$ gilt. Da (K, σ) zu M gehört, ist M nicht leer. Außerdem folgt mit dem üblichen Vereinigungsargument, dass jede total geordnete Teilmenge von M eine obere Schranke besitzt. Somit sind die Voraussetzungen zum Lemma von Zorn erfüllt, also enthält M ein maximales Element (F, τ). Es gilt dann notwendig $F = K'$, denn sonst könnte man ein Element $\alpha \in K' - F$ wählen und τ mit Hilfe von Lemma 8 fortsetzen zu $\tau'\colon F(\alpha) \longrightarrow L$, im Widerspruch zur Maximalität von (F, τ). Damit ist die Existenz der gewünschten Fortsetzung $\sigma'\colon K' \longrightarrow L$ von σ nachgewiesen.

Ist nun zusätzlich K' algebraisch abgeschlossen, so ist auch $\sigma'(K')$ algebraisch abgeschlossen. Ist weiter L algebraisch über $\sigma(K)$, so insbesondere

auch über $\sigma'(K')$, und es folgt $\sigma'(K') = L$ mit Bemerkung 3. Da Körperhomomorphismem stets injektiv sind, ist σ' ein Isomorphismus. □

Korollar 10. *Es seien $\overline{K}_1$ und $\overline{K}_2$ zwei algebraische Abschlüsse eines Körpers K. Dann existiert ein K-Isomorphismus $\overline{K}_1 \xrightarrow{\sim} \overline{K}_2$, d. h. ein Isomorphismus, welcher die Identität $K \longrightarrow K$ fortsetzt.*

Wir wollen hier noch hervorheben, dass Satz 9 keinerlei Eindeutigkeitsaussage für Fortsetzungen $\sigma' \colon K' \longrightarrow L$ zu $\sigma \colon K \longrightarrow L$ längs einer algebraischen Körpererweiterung K'/K beinhaltet, ein Phänomen, dass wir in 3.6 zur Definition des Separabilitätsgrads von K'/K nutzen werden. In der Tat, im Allgemeinen wird es mehrere "gleichwertige" solcher Fortsetzungen σ' geben, wie bereits das Beispiel einer einfachen algebraischen Erweiterung K'/K in Lemma 8 gezeigt hat. Als Konsequenz gibt es in der Situation von Korollar 10 auch keinen kanonischen Isomorphismus zwischen algebraischen Abschlüssen von K, abgesehen von Spezialfällen.

Lernkontrolle und Prüfungsvorbereitung

1. Erläutere das Verfahren von Kronecker, welches es erlaubt, zu einem Körper K und einem Polynom $f \in K[X]$ vom Grad ≥ 1 eine endliche Körpererweiterung L/K zu konstruieren, derart dass f eine Nullstelle in L besitzt.
2. Wann bezeichnet man einen Körper als algebraisch abgeschlossen? Gib verschiedene Charakterisierungen dieser Eigenschaft.
3. Erkläre die Aussage des Lemmas von Zorn.
4. Zeige, dass jeder Ring $R \neq 0$ ein maximales Ideal besitzt.
5. Zeige, dass jeder Körper K einen algebraischen Abschluss besitzt, also einen algebraisch abgeschlossen Erweiterungskörper, der algebraisch über K ist.
6. Es sei K'/K eine algebraische Körpererweiterung und $\sigma \colon K \longrightarrow L$ ein Homomorphismus zwischen Körpern. Diskutiere die Möglichkeit, σ zu einem Körperhomomorphismus $\sigma' \colon K' \longrightarrow L$ fortzusetzen. Beginne mit dem Fall einer einfachen algebraischen Körpererweiterung K'/K und charakterisiere hier auch die Anzahl der verschiedenen Fortsetzungen.
7. Es seien $\overline{K}_1$ und $\overline{K}_2$ algebraische Abschlüsse eines Körpers K. Zeige, dass es einen Isomorphismus $\overline{K}_1 \xrightarrow{\sim} \overline{K}_2$ gibt, welcher die Identität auf K fortsetzt.

Übungsaufgaben

1. *Es sei $f \in \mathbb{Q}[X]$ ein Polynom vom Grad > 1. Warum ist es leichter, eine Nullstelle von f im "Sinne der Algebra" zu konstruieren als im "Sinne der Analysis"?*
2. *Warum lässt sich die Existenz eines algebraischen Abschlusses $\overline{K}$ zu einem Körper K nicht auf folgende Weise begründen: Man betrachte sämtliche algebraischen Erweiterungen von K. Da für eine bezüglich der Inklusion total geordnete Familie $(K_i)_{i\in I}$ algebraischer Erweiterungen von K auch deren Vereinigung $\bigcup_{i\in I} K_i$ eine algebraische Erweiterung von K ist, liefert das Lemma von Zorn die Existenz einer maximalen algebraischen Erweiterung, also eines algebraischen Abschlusses von K.*
3. *Warum sollte man verschiedene algebraische Abschlüsse eines Körpers K unterscheiden und nicht von "dem" algebraischen Abschluss von K reden?*
4. Sei K ein Körper und $f \in K[X]$ ein Polynom vom Grad > 0. Zeige: Ist $\mathfrak{m} \subset K[X]$ ein maximales Ideal mit $f \in \mathfrak{m}$, so kann man $L = K[X]/\mathfrak{m}$ als algebraischen Erweiterungskörper von K auffassen, wobei f eine Nullstelle in L hat. Es stimmt L überein mit demjenigen Erweiterungskörper, den man bei Anwendung des Verfahrens von Kronecker auf einen geeigneten irreduziblen Faktor von f erhalten würde.
5. Sei $\overline{K}$ ein algebraischer Abschluss eines Körpers K. Zeige: Ist K abzählbar, so auch $\overline{K}$.
6. Zeige, dass jeder algebraisch abgeschlossene Körper unendlich viele Elemente besitzt.
7. Sei L/K eine endliche Körpererweiterung vom Grad $[L : K] = n$. Für ein Element $\alpha \in L$ gebe es Automorphismen $\sigma_i \colon L \longrightarrow L$, $i = 1, \ldots, n$, mit $\sigma_i|_K = \mathrm{id}_K$ und $\sigma_i(\alpha) \neq \sigma_j(\alpha)$ für $i \neq j$. Beweise: $L = K(\alpha)$.
8. Sei $\overline{\mathbb{Q}}$ ein algebraischer Abschluss von $\mathbb{Q}$. Bestimme alle Homomorphismen $\mathbb{Q}(\sqrt[4]{2}, i) \longrightarrow \overline{\mathbb{Q}}$ sowie deren Bilder.

3.5 Zerfällungskörper

Wir beginnen in diesem Abschnitt mit einigen Vorbereitungen zur Galois-Theorie. Als Hilfsmittel verwenden wir dabei die im vorigen Abschnitt bewiesene Existenz algebraisch abgeschlossener Körper sowie die Resultate 3.4/8 und 3.4/9 über die Fortsetzung von Körperhomomorphismen. Sind

L/K und L'/K zwei Körpererweiterungen und ist $\sigma\colon L \longrightarrow L'$ ein Homomorphismus, so nennen wir σ einen *K-Homomorphismus*, wenn σ eine Fortsetzung der Identität $K \longrightarrow K$ ist.

Definition 1. *Es sei $\mathfrak{F} = (f_i)_{i\in I}$, $f_i \in K[X]$, eine Familie nicht-konstanter Polynome mit Koeffizienten aus einem Körper K. Ein Erweiterungskörper L von K heißt* Zerfällungskörper *(über K) der Familie $\mathfrak{F}$, wenn gilt*:

(i) *Jedes f_i zerfällt über L vollständig in Linearfaktoren.*

(ii) *Die Körpererweiterung L/K wird von den Nullstellen der f_i erzeugt.*

Im einfachsten Fall hat man $\mathfrak{F} = (f)$ mit einem einzigen Polynom $f \in K[X]$. Ist $\overline{K}$ ein algebraischer Abschluss von K und sind $a_1, \ldots, a_n$ die Nullstellen von f in $\overline{K}$, so ist $L = K(a_1, \ldots, a_n)$ ein Zerfällungskörper von f über K. In gleicher Weise zeigt man, dass Zerfällungskörper für beliebige Familien $\mathfrak{F}$ von nicht-konstanten Polynomen $f_i \in K[X]$ existieren: Man wähle einen algebraischen Abschluss $\overline{K}$ von K und definiere L als denjenigen Teilkörper von $\overline{K}$, welcher über K von allen Nullstellen der f_i erzeugt wird. Besteht die Familie $\mathfrak{F}$ nur aus endlich vielen Polynomen $f_1, \ldots, f_n$, so ist jeder Zerfällungskörper des Produktes $f_1 \cdot \ldots \cdot f_n$ auch Zerfällungskörper von $\mathfrak{F}$ und umgekehrt.

Satz 2. *Es seien L_1, L_2 zwei Zerfällungskörper einer Familie $\mathfrak{F}$ nicht-konstanter Polynome $f_i \in K[X]$ mit Koeffizienten aus einem Körper K. Wählt man dann einen algebraischen Abschluss $\overline{L}_2$ von L_2, so beschränkt sich jeder K-Homomorphismus $\overline{\sigma}\colon L_1 \longrightarrow \overline{L}_2$ zu einem Isomorphismus $\sigma\colon L_1 \xrightarrow{\sim} L_2$.*

In der Situation des Satzes lässt sich die Inklusion $K \hookrightarrow \overline{L}_2$ gemäß 3.4/9 zu einem K-Homomorphismus $\overline{\sigma}\colon L_1 \longrightarrow \overline{L}_2$ fortsetzen, wobei eine solche Fortsetzung $\overline{\sigma}$ allerdings, wie zum Schluss von 3.4 erläutert, normalerweise nicht eindeutig bestimmt sein wird. Immerhin folgt jedoch, dass L_1 und L_2 über K isomorph sind, so dass wir als direkte Folgerung von Satz 2 vermerken können:

Korollar 3. *Es seien K ein Körper und L_1, L_2 zwei Zerfällungskörper einer Familie nicht-konstanter Polynome aus $K[X]$. Dann gibt es einen K-Isomorphismus $L_1 \xrightarrow{\sim} L_2$.*

Beweis von Satz 2. Wir nehmen zunächst an, dass $\mathfrak{F}$ nur aus einem einzigen Polynom f besteht, wobei wir f als normiert voraussetzen dürfen. Sind $a_1, \ldots, a_n$ die Nullstellen von f in L_1 und $b_1, \ldots, b_n$ die Nullstellen von f in $L_2 \subset \overline{L}_2$, so gilt

$$f^{\overline{\sigma}} = \prod \big(X - \overline{\sigma}(a_i)\big) = \prod (X - b_i).$$

Daher bildet $\overline{\sigma}$ die Menge der a_i bijektiv auf die Menge der b_i ab, und es folgt

$$L_2 = K(b_1, \ldots, b_n) = K\big(\overline{\sigma}(a_1), \ldots, \overline{\sigma}(a_n)\big) = \overline{\sigma}(L_1),$$

d. h. $\overline{\sigma}$ beschränkt sich zu einem K-Isomorphismus $\sigma\colon L_1 \longrightarrow L_2$, wie behauptet.

Mit dem soeben bewiesenen Spezialfall folgt die Behauptung des Satzes auch für endliche Familien $\mathfrak{F}$, indem wir L_1 und L_2 als Zerfällungskörper des Produkts aller Polynome aus $\mathfrak{F}$ auffassen. Hieraus wiederum ergibt sich der Allgemeinfall unmittelbar, da L_1 und L_2 als Vereinigung von Zerfällungskörpern zu endlichen Teilfamilien von $\mathfrak{F}$ darstellbar sind. □

Wir wollen die Eigenschaft eines Körpers, Zerfällungskörper einer Familie von Polynomen aus $K[X]$ zu sein, durch äquivalente Bedingungen charakterisieren und im Anschluss hieran den Begriff normaler Körpererweiterungen einführen.

Theorem 4. *Es sei K ein Körper und L ein algebraischer Erweiterungskörper von K. Dann ist äquivalent*:

(i) *Jeder K-Homomorphismus $L \longrightarrow \overline{L}$ in einen algebraischen Abschluss $\overline{L}$ von L beschränkt sich zu einem Automorphismus von L.*

(ii) *Es ist L Zerfällungskörper einer Familie von Polynomen aus $K[X]$.*

(iii) *Jedes irreduzible Polynom aus $K[X]$, welches in L eine Nullstelle besitzt, zerfällt über L vollständig in Linearfaktoren.*

Definition 5. *Eine algebraische Körpererweiterung $K \subset L$ heißt* normal, *wenn die äquivalenten Bedingungen von Theorem* 4 *erfüllt sind.*

Beweis von Theorem 4. Wir beginnen mit der Implikation von (i) nach (iii). Sei also $f \in K[X]$ irreduzibel und $a \in L$ eine Nullstelle von f. Ist $b \in \overline{L}$ eine weitere Nullstelle von f, so erhalten wir unter Benutzung von 3.4/8 einen K-Homomorphismus $\sigma\colon K(a) \longrightarrow \overline{L}$ mit $\sigma(a) = b$. Es

lässt sich dann σ gemäß 3.4/9 zu einem K-Homomorphismus $\sigma' : L \longrightarrow \overline{L}$ fortsetzen. Ist nun Bedingung (i) gegeben, so gilt $\sigma'(L) = L$ und somit $b = \sigma'(a) \in L$. Folglich sind alle Nullstellen von f bereits in L enthalten, und f zerfällt über L in Linearfaktoren.

Als Nächstes zeigen wir, dass (iii) die Bedingung (ii) impliziert. Sei $(a_i)_{i\in I}$ eine Familie von Elementen aus L, so dass die a_i die Körpererweiterung L/K erzeugen. Sei jeweils f_i das Minimalpolynom von a_i über K. Da alle f_i gemäß (iii) über L vollständig in Linearfaktoren zerfallen, ist L Zerfällungskörper der Familie $\mathfrak{F} = (f_i)_{i\in I}$.

Sei schließlich Bedingung (ii) gegeben, also L Zerfällungskörper einer Familie $\mathfrak{F}$ von Polynomen aus $K[X]$, und sei $\sigma : L \longrightarrow \overline{L}$ ein K-Homomorphismus. Dann ist mit L auch $\sigma(L)$ Zerfällungskörper von $\mathfrak{F}$, und es folgt $\sigma(L) = L$, da beide Körper Teilkörper von $\overline{L}$ sind; vgl. hierzu auch Satz 2. □

Aus trivialen Gründen ist eine Erweiterung vom Typ $\overline{K}/K$ normal, wobei $\overline{K}$ ein algebraischer Abschluss eines Körpers K sei. Im Übrigen sind Körpererweiterungen vom Grad 2 normal, da ein Polynom über einem Körper K bereits dann in Linearfaktoren zerfällt, wenn es in K eine Nullstelle besitzt. Weiter sieht man mit Bedingung (ii) von Theorem 4:

Bemerkung 6. *Ist $K \subset L \subset M$ eine Kette algebraischer Körpererweiterungen und ist M/K normal, so auch M/L.*

Der Begriff der normalen Körpererweiterung verhält sich jedoch *nicht* transitiv. Obwohl $\mathbb{Q}(\sqrt{2})/\mathbb{Q}$ und $\mathbb{Q}(\sqrt[4]{2})/\mathbb{Q}(\sqrt{2})$ normal sind, da vom Grad 2, ist die Körpererweiterung $\mathbb{Q}(\sqrt[4]{2})/\mathbb{Q}$ nicht normal. Das Polynom $X^4 - 2$ etwa ist irreduzibel über $\mathbb{Q}$ und hat in $\mathbb{Q}(\sqrt[4]{2})$ die Nullstelle $\sqrt[4]{2}$. Es kann aber über $\mathbb{Q}(\sqrt[4]{2})$ nicht vollständig in Linearfaktoren zerfallen, da die komplexe Nullstelle $i \cdot \sqrt[4]{2}$ nicht zu $\mathbb{Q}(\sqrt[4]{2}) \subset \mathbb{R}$ gehört.

Für Anwendungen ist es oft nützlich, zu wissen, dass man zu einer algebraischen Körpererweiterung L/K eine *normale Hülle* bilden kann. Hierunter versteht man einen Erweiterungskörper L' von L, wobei L'/L algebraisch und L'/K normal ist mit der Eigenschaft, dass kein echter Teilkörper von L' diese Bedingungen erfüllt. Es ist also L' ein "minimaler" Erweiterungskörper von L, so dass L'/K normal ist.

Satz 7. *Es sei L/K eine algebraische Körpererweiterung.*

(i) *Zu L/K existiert eine normale Hülle L'/K, und zu je zwei solcher normaler Hüllen L'_1, L'_2 gibt es stets einen L-Isomorphismus $L'_1 \xrightarrow{\sim} L'_2$.*

(ii) *Es ist L'/K endlich, falls L/K endlich ist.*

(iii) *Ist M/L eine algebraische Körpererweiterung mit der Eigenschaft, dass M/K normal ist, so kann man L' mit $L \subset L' \subset M$ wählen. Als Teilkörper von M ist L' eindeutig bestimmt. Ist $(\sigma_i)_{i\in I}$ das System aller K-Homomorphismen von L nach M, so gilt $L' = K(\sigma_i(L); i \in I)$. Man bezeichnet L' auch als die* normale Hülle *von L in M.*

Beweis. Es gelte $L = K(\mathfrak{A})$, wobei $\mathfrak{A} = (a_j)_{j\in J}$ eine Familie von Elementen aus L sei. Sei f_j jeweils das Minimalpolynom von a_j über K. Ist dann M ein algebraischer Erweiterungskörper von L, so dass M/K normal ist (man kann für M etwa einen algebraischen Abschluss von L wählen), so zerfallen die Polynome f_j gemäß Theorem 4 (iii) in $M[X]$ vollständig in Linearfaktoren. Sei L' der von den Nullstellen der f_j über K erzeugte Teilkörper von M, d. h. es ist L' ein Zerfällungskörper der f_j. Dann gilt $L \subset L' \subset M$, und es ist L'/K offenbar eine normale Hülle von L/K. Nach Konstruktion ist L'/K endlich, falls L/K endlich ist. Umgekehrt überlegt man, dass für eine normale Hülle L'/K zu L/K der Körper L' notwendigerweise einen Zerfällungskörper der f_j enthält, also wegen der Minimalitätsforderung selbst schon ein Zerfällungskörper der f_j über K ist.

Zum Nachweis der zusätzlichen Aussage in (i) betrachte man zwei normale Hüllen L'_1/K und L'_2/K zu L/K. Es sind dann L'_1 und L'_2 Zerfällungskörper der f_j über K mit $L \subset L'_i$, also auch Zerfällungskörper der f_j über L. Aus Korollar 3 folgt die Existenz eines L-Isomorphismus $L'_1 \longrightarrow L'_2$. Dies impliziert die Aussage in (i) und mit Theorem 4 (i) auch die Eindeutigkeitsaussage in (iii).

Um die in (iii) behauptete spezielle Gestalt von L' als Teilkörper von M zu verifizieren, betrachte man einen K-Homomorphismus $\sigma\colon L \longrightarrow M$. Dieser überführt die Nullstellen der f_j wiederum in Nullstellen der f_j, vgl. 3.4/8. Da L' über K von diesen Nullstellen erzeugt wird, ergibt sich $K(\sigma_i(L); i \in I) \subset L'$. Umgekehrt können wir zu jeder Nullstelle $a \in L'$ eines Polynoms f_j ebenfalls gemäß 3.4/8 einen K-Homomorphismus $K(a_j) \longrightarrow L'$ durch $a_j \longmapsto a$ definieren, diesen mittels 3.4/9 zu einem K-Automorphismus eines algebraischen Abschlusses von L' fortsetzen sowie anschließend aufgrund der Normalität von L'/K zu ei-

nem K-Homomorphismus $\sigma\colon L \longrightarrow L'$ beschränken. Somit erhalten wir $a \in K(\sigma_i(L); i \in I)$, woraus sich insgesamt die gewünschte Beziehung $L' = K(\sigma_i(L); i \in I)$ ergibt. □

Lernkontrolle und Prüfungsvorbereitung

1. Es sei K ein Körper. Was versteht man unter einem Zerfällungskörper einer Familie nicht-konstanter Polynome in $K[X]$? Wie lassen sich solche Zerfällungskörper konstruieren?
2. Was ist ein K-Homomorphismus zwischen Erweiterungen eines Körpers K?
3. Es sei K ein Körper und f ein nicht-konstantes Polynom in $K[X]$. Zeige, dass je zwei Zerfällungskörper von f über K isomorph sind. Wie lässt sich dieses Resultat auf Familien nicht-konstanter Polynome in $K[X]$ erweitern?
4. Es sei L/K eine algebraische Körpererweiterung, so dass L Zerfällungskörper einer Familie nicht-konstanter Polynome in $K[X]$ ist. Sei $g \in K[X]$ ein irreduzibles Polynom, welches in L eine Nullstelle habe. Begründe in direkter Weise, dass g über L vollständig in Linearfaktoren zerfällt.
5. Erkläre die äquivalenten definierenden Bedingungen für normale algebraische Körpererweiterungen (mit Begründung)?
6. Welche einfachen Beispiele normaler Körpererweiterungen gibt es?
7. Es sei $K \subset L \subset M$ eine Kette algebraischer Körpererweiterungen. Zeige, dass M/L normal ist, falls M/K normal ist. Ist dann auch L/K normal? Umgekehrt, seien M/L und L/K normal. Ist dann auch M/K normal?
8. Was versteht man unter einer normalen Hülle einer algebraischen Körpererweiterung L/K? Wie lässt sich diese z. B. in einem algebraischen Abschluss von K realisieren?

Übungsaufgaben

1. *Gib eine genaue Begründung dafür, dass Körpererweiterungen vom Grad* 2 *stets normal sind.*
2. *Es sei K ein Körper und L ein Zerfällungskörper eines nicht-konstanten Polynoms $f \in K[X]$. Begründe nochmals im Detail, warum jedes in $K[X]$ irreduzible Polynom g, welches in L eine Nullstelle besitzt, über L schon vollständig in Linearfaktoren zerfällt.*

3. *Es sei K ein Körper und L ein Zerfällungskörper der Familie aller nichtkonstanten Polynome in $K[X]$. Erkläre, warum L bereits ein algebraischer Abschluss von K ist.*

4. Zeige für eine endliche Körpererweiterung L/K, dass die Bedingung (i) aus Theorem 4 äquivalent zu folgender Bedingung ist:

   (i′) Jeder K-Homomorphismus $L \longrightarrow L'$ in eine endliche Körpererweiterung L' von L beschränkt sich zu einem Automorphismus von L.

   Ersetze in Theorem 4 Bedingung (i) durch (i′) und skizziere für endliche Erweiterungen L/K einen Beweis dieses Theorems, der auf die Benutzung der Existenz eines algebraischen Abschlusses von K verzichtet.

5. Betrachte $L = \mathbb{Q}(\sqrt[4]{2}, i)$ als Erweiterungskörper von $\mathbb{Q}$.

   (i) Zeige, dass L ein Zerfällungskörper des Polynoms $X^4 - 2$ über $\mathbb{Q}$ ist.

   (ii) Bestimme den Grad von L über $\mathbb{Q}$ sowie alle $\mathbb{Q}$-Automorphismen von L.

   (iii) Zeige $L = \mathbb{Q}(\sqrt[4]{2}+i)$ unter Verwendung von Aufgabe 7 aus Abschnitt 3.4.

6. Bestimme einen Zerfällungskörper L des Polynoms X^4+2X^2-2 über $\mathbb{Q}$ sowie den Grad $[L : \mathbb{Q}]$.

7. Ist die Körpererweiterung $\mathbb{Q}\left(\sqrt{2+\sqrt{2}}\right)/\mathbb{Q}$ normal?

8. Es sei K ein Körper und $f \in K[X]$ ein Polynom vom Grad $n > 0$. Sei L ein Zerfällungskörper von f über K. Zeige:

   (i) $[L : K]$ ist ein Teiler von $n!$.

   (ii) Gilt $[L : K] = n!$, so ist f irreduzibel.

9. Bestimme einen Zerfällungskörper L der Familie $\{X^4 + 1, X^5 + 2\}$ über $\mathbb{Q}$ sowie den Grad $[L : \mathbb{Q}]$.

10. Betrachte das Polynom $f = X^6-7X^4+3X^2+3$ in $\mathbb{Q}[X]$ und in $\mathbb{F}_{13}[X]$. Zerlege f jeweils in seine irreduziblen Faktoren und bestimme einen Zerfällungskörper von f über $\mathbb{Q}$ bzw. $\mathbb{F}_{13}$.

11. Es seien $K(\alpha)/K$ und $K(\beta)/K$ einfache algebraische Körpererweiterungen mit den Minimalpolynomen f von α bzw. g von β über K. Zeige: f ist genau dann irreduzibel über $K(\beta)$, wenn g irreduzibel über $K(\alpha)$ ist. Die Irreduzibilität ist gegeben, wenn grad f und grad g teilerfremd sind.

12. Sei L/K eine normale algebraische Körpererweiterung und $f \in K[X]$ ein normiertes irreduzibles Polynom. In $L[X]$ sei $f = f_1 \dots f_r$ die Primfaktorzerlegung von f, wobei die f_i normiert seien. Zeige, dass es zu je zwei Faktoren $f_i, f_j, i \neq j$, dieser Zerlegung einen K-Automorphismus $\sigma\colon L \longrightarrow L$ gibt mit $f_j = f_i^{\sigma}$.

13. Seien L/K und L'/K normale algebraische Körpererweiterungen, und sei L'' ein Körper, der L und L' als Teilkörper enthält.
    (i) Zeige, dass $(L \cap L')/K$ eine normale algebraische Körpererweiterung ist.
    (ii) Benutze die Idee aus (i), um einen alternativen Beweis zur Existenz normaler Hüllen von algebraischen Körpererweiterungen zu geben.

3.6 Separable Körpererweiterungen

Ist K ein Körper, so ist es zweckmäßig, die Nullstellen von Polynomen $f \in K[X]$ in einem algebraischen Abschluss $\overline{K}$ von K zu betrachten. Da $\overline{K}$ bis auf K-Isomorphie eindeutig ist, können viele Aussagen über Nullstellen von Polynomen f unabhängig von der Wahl von $\overline{K}$ formuliert werden; z. B. macht es Sinn, zu sagen, f habe nur einfache Nullstellen oder f habe mehrfache Nullstellen. Nicht-konstante Polynome, deren Nullstellen sämtlich einfach sind, nennen wir *separabel*.

Lemma 1. *Es sei K ein Körper und $f \in K[X]$ ein nicht-konstantes Polynom.*
(i) *Die mehrfachen Nullstellen von f (in einem algebraischen Abschluss $\overline{K}$ von K) stimmen überein mit den gemeinsamen Nullstellen von f und seiner Ableitung f' oder, äquivalent hierzu, mit den Nullstellen von* $\mathrm{ggT}(f, f')$.
(ii) *Ist f irreduzibel, so hat f genau dann mehrfache Nullstellen, wenn die Ableitung f' verschwindet.*

Beweis. Aussage (i) ist eine Konsequenz von 2.6/4, zumindest wenn K bereits algebraisch abgeschlossen ist (in Abschnitt 2.6 wurden Nullstellen von Polynomen $f \in K[X]$ stets in K, noch nicht in einem algebraischen Abschluss von K betrachtet). Für den Allgemeinfall genügt es dann, zu bemerken, dass ein in $K[X]$ gebildeter größter gemeinsamer Teiler $d = \mathrm{ggT}(f, f')$ zugleich auch größter gemeinsamer Teiler von f und f' in $\overline{K}[X]$ ist. Um Letzteres einzusehen, benutze man die idealtheoretische Charakterisierung des größten gemeinsamen Teilers in Hauptidealringen 2.4/13. Aus der Gleichung

$$d \cdot K[X] = f \cdot K[X] + f' \cdot K[X]$$

ergibt sich nämlich $d \cdot \overline{K}[X] = f \cdot \overline{K}[X] + f' \cdot \overline{K}[X]$, was $d = \mathrm{ggT}(f, f')$ auch in $\overline{K}[X]$ bedeutet.

Zum Nachweis von (ii) wähle man f irreduzibel, außerdem sei f normiert. Ist dann $a \in \overline{K}$ eine Nullstelle von f, so erkennt man f als das Minimalpolynom von a über K. Nach Teil (i) ist a genau dann eine mehrfache Nullstelle von f, wenn a auch Nullstelle von f' ist. Da aber $\operatorname{grad} f' < \operatorname{grad} f$ gilt und f das Minimalpolynom von a ist, kann a nur dann eine Nullstelle von f' sein, wenn f' das Nullpolynom ist. □

Im Falle $\operatorname{char} K = 0$ gilt für nicht-konstante Polynome $f \in K[X]$ stets $f' \neq 0$. Daher zeigt Aussage (ii) des Lemmas, dass irreduzible Polynome in Charakteristik 0 immer separabel sind. Andererseits gibt es in Charakteristik > 0 irreduzible Polynome, die nicht separabel sind. Es sei etwa p eine Primzahl, t eine Variable und $K = \mathbb{F}_p(t) = Q(\mathbb{F}_p[t])$. Dann ist $X^p - t$ als Polynom in $K[X]$ aufgrund des Eisensteinschen Irreduzibilitätskriteriums 2.8/1 irreduzibel, wegen $f' = pX^{p-1} = 0$ aber nicht separabel. Wir wollen insbesondere den Fall positiver Charakteristik etwas genauer untersuchen.

Satz 2. *Es sei K ein Körper und $f \in K[X]$ irreduzibel.*

(i) *Falls* $\operatorname{char} K = 0$, *so ist f separabel.*

(ii) *Falls* $\operatorname{char} K = p > 0$, *so wähle man $r \in \mathbb{N}$ maximal mit der Eigenschaft, dass f ein Polynom in X^{p^r} ist, d. h. dass es ein $g \in K[X]$ mit $f(X) = g(X^{p^r})$ gibt. Dann hat jede Nullstelle von f die Vielfachheit p^r, und es ist g ein irreduzibles Polynom, welches separabel ist. Die Nullstellen von f sind gerade die p^r-ten Wurzeln der Nullstellen von g.*

Beweis. Der Fall $\operatorname{char} K = 0$ wurde bereits diskutiert. Wir dürfen daher $\operatorname{char} K = p > 0$ annehmen. Weiter sei

$$f = \sum_{i=0}^{n} c_i X^i, \qquad f' = \sum_{i=1}^{n} i c_i X^{i-1}.$$

Dann ist $f' = 0$ gleichbedeutend mit $ic_i = 0$ für $i = 1, \ldots, n$. Da ic_i genau dann verschwindet, wenn $p \mid i$ oder $c_i = 0$ gilt, ist f' genau dann das Nullpolynom, wenn es ein $h \in K[X]$ mit $f(X) = h(X^p)$ gibt.

Es sei nun $f(X) = g(X^{p^r})$, wie in Aussage (ii) beschrieben. Wenden wir obige Überlegung auf g anstelle von f an, so folgt $g' \neq 0$ aus der Maximalität von r. Außerdem ist mit f auch g irreduzibel, so dass g nach Lemma 1 (ii) separabel ist. Sei nun $\overline{K}$ ein algebraischer Abschluss von K und

$$g = \prod_i (X - a_i), \qquad a_i \in \overline{K},$$

wobei wir f und somit auch g als normiert angenommen haben. Sind dann $c_i \in \overline{K}$ mit $c_i^{p^r} = a_i$, so folgt unter Benutzung von 3.1/3

$$f = \prod_i (X^{p^r} - c_i^{p^r}) = \prod_i (X - c_i)^{p^r},$$

d. h. alle Nullstellen von f haben die Ordnung p^r. □

Wir wollen nun den Separabilitätsbegriff allgemeiner für algebraische Körpererweiterungen erklären.

Definition 3. *Es sei $K \subset L$ eine algebraische Körpererweiterung. Ein Element $\alpha \in L$ heißt* separabel *über K, wenn α Nullstelle eines separablen Polynoms aus $K[X]$ ist oder, was hierzu äquivalent ist, wenn das Minimalpolynom von α über K separabel ist. Es heißt L* separabel *über K, wenn jedes Element $\alpha \in L$ im vorstehenden Sinne separabel über K ist.*

Ein Körper K heißt *vollkommen* oder *perfekt*, wenn jede algebraische Erweiterung von K separabel ist. Daher können wir aus Satz 2 (i) als direkte Folgerung ablesen:

Bemerkung 4. *In Charakteristik 0 ist jede algebraische Körpererweiterung separabel, d. h. Körper der Charakteristik 0 sind vollkommen.*

Wir haben bereits gesehen, dass für p prim und t eine Variable das Polynom $X^p - t \in \mathbb{F}_p(t)[X]$ irreduzibel, aber nicht separabel ist. Somit ist der Körper $\mathbb{F}_p(t)[X]/(X^p - t)$ nicht separabel über $\mathbb{F}_p(t)$. In äquivalenter Weise können wir sagen, dass die algebraische Körpererweiterung $\mathbb{F}_p(t)/\mathbb{F}_p(t^p)$ nicht separabel ist, denn $X^p - t^p$ ist als irreduzibles Polynom in $\mathbb{F}_p(t^p)[X]$ das Minimalpolynom von t über $\mathbb{F}_p(t^p)$.

Wir wollen im Folgenden separable algebraische Körpererweiterungen genauer charakterisieren. Insbesondere wollen wir zeigen, dass eine algebraische Körpererweiterung bereits dann separabel ist, wenn sie von separablen Elementen erzeugt wird. Als technisches Hilfsmittel benötigen wir die Notation des Separabilitätsgrades, in Analogie zum "gewöhnlichen" Grad einer Körpererweiterung.

Definition 5. *Für eine algebraische Körpererweiterung $K \subset L$ bezeichne* $\mathrm{Hom}_K(L, \overline{K})$ *die Menge der K-Homomorphismen von L in einen algebraischen Abschluss $\overline{K}$ von K. Dann erklärt man den* Separabilitätsgrad *von L über K als die Anzahl der Elemente von* $\mathrm{Hom}_K(L, \overline{K})$; *in Zeichen*:

$$[L : K]_s := \#\,\mathrm{Hom}_K(L, \overline{K}).$$

Es folgt mit 3.4/10, dass die Definition des Separabilitätsgrades unabhängig von der Wahl des algebraischen Abschlusses $\overline{K}$ von K ist. Zunächst wollen wir den Separabilitätsgrad für einfache algebraische Körpererweiterungen berechnen.

Lemma 6. *Es sei $K \subset L = K(\alpha)$ eine einfache algebraische Körpererweiterung, $f \in K[X]$ sei das Minimalpolynom von α über K.*

(i) *Der Separabilitätsgrad $[L : K]_s$ ist gleich der Anzahl der verschiedenen Nullstellen von f in einem algebraischen Abschluss von K.*

(ii) *Es ist α genau dann separabel über K, wenn $[L : K] = [L : K]_s$ gilt.*

(iii) *Gilt* $\mathrm{char}\, K = p > 0$, *und ist p^r die Vielfachheit der Nullstelle α von f (vgl. Satz 2 (ii)), so folgt $[L : K] = p^r [L : K]_s$.*

Beweis. Aussage (i) ist eine Umformulierung von 3.4/8. Zum Nachweis von (ii) sei $n = \mathrm{grad}\, f$. Es ist α genau dann separabel, wenn f keine mehrfachen Nullstellen, also insgesamt n verschiedene Nullstellen hat, bzw. gemäß (i), wenn $n = [L : K]_s$ gilt. Mit 3.2/6 hat man aber $[L : K] = \mathrm{grad}\, f = n$, so dass α genau dann separabel ist, wenn $[L : K] = [L : K]_s$ gilt. Aussage (iii) schließlich ist eine direkte Konsequenz von Satz 2 (ii). □

Um den Separabilitätsgrad für beliebige algebraische Erweiterungen handhaben zu können, brauchen wir ein Analogon zum Gradsatz 3.2/2.

Satz 7 (Gradsatz für Separabilitätsgrad). *Es seien $K \subset L \subset M$ algebraische Körpererweiterungen. Dann gilt*

$$[M : K]_s = [M : L]_s \cdot [L : K]_s.$$

Beweis. Man wähle einen algebraischen Abschluss $\overline{K}$ von M. Sodann folgt $K \subset L \subset M \subset \overline{K}$, und $\overline{K}$ ist zugleich auch ein algebraischer Abschluss von

K und L. Weiter gelte

$$\mathrm{Hom}_K(L,\overline{K}) = \{\sigma_i\,;\, i \in I\}, \qquad \mathrm{Hom}_L(M,\overline{K}) = \{\tau_j\,;\, j \in J\},$$

wobei die σ_i sowie die τ_j jeweils paarweise verschieden seien. Man setze nun die K-Homomorphismen $\sigma_i\colon L \longrightarrow \overline{K}$ mittels 3.4/9 zu K-Automorphismen $\overline{\sigma}_i\colon \overline{K} \longrightarrow \overline{K}$ fort. Die behauptete Gradformel ist dann eine Konsequenz aus den beiden folgenden Aussagen, die wir nachweisen werden:

(1) Die Abbildungen $\overline{\sigma}_i \circ \tau_j\colon M \longrightarrow \overline{K}$, $i \in I$, $j \in J$, sind paarweise verschieden.

(2) $\mathrm{Hom}_K(M,\overline{K}) = \{\overline{\sigma}_i \circ \tau_j\,;\, i \in I, j \in J\}$.

Um Behauptung (1) zu verifizieren, betrachte man eine Gleichung des Typs $\overline{\sigma}_i \circ \tau_j = \overline{\sigma}_{i'} \circ \tau_{j'}$. Dann folgt, da τ_j und $\tau_{j'}$ sich auf L zur Identität beschränken, $\sigma_i = \sigma_{i'}$ bzw. $i = i'$. Hieraus ergibt sich $\tau_j = \tau_{j'}$ wegen $\overline{\sigma}_i = \overline{\sigma}_{i'}$ und somit $j = j'$. Die in (1) genannten Abbildungen sind daher paarweise verschieden. Da es sich außerdem um K-Homomorphismen handelt, bleibt zum Nachweis von (2) lediglich noch zu zeigen, dass jeder K-Homomorphismus $\tau\colon M \longrightarrow \overline{K}$ von der in (1) beschriebenen Form ist. Für $\tau \in \mathrm{Hom}_K(M,\overline{K})$ gilt $\tau|_L \in \mathrm{Hom}_K(L,\overline{K})$, also gibt es ein $i \in I$ mit $\tau|_L = \sigma_i$. Dann ist $\overline{\sigma}_i^{-1} \circ \tau \in \mathrm{Hom}_L(M,\overline{K})$, d. h. es gibt ein $j \in J$ mit $\overline{\sigma}_i^{-1} \circ \tau = \tau_j$. Somit gilt $\tau = \overline{\sigma}_i \circ \tau_j$, und (2) ist klar. □

Da algebraische Körpererweiterungen in Charakteristik 0 stets separabel sind (Bemerkung 4), lässt sich durch induktive Anwendung der in 3.2/2 und Satz 7 angegebenen Gradformeln folgendes Resultat aus Lemma 6 gewinnen:

Satz 8. *Es sei $K \subset L$ eine endliche Körpererweiterung.*

(i) *Falls* $\mathrm{char}\, K = 0$, *so folgt* $[L:K] = [L:K]_s$.

(ii) *Falls* $\mathrm{char}\, K = p > 0$, *so existiert ein Exponent* $r \in \mathbb{N}$, *derart dass* $[L:K] = p^r[L:K]_s$.

Insbesondere gilt $1 \leq [L:K]_s \leq [L:K]$, *und es ist* $[L:K]_s$ *stets ein Teiler von* $[L:K]$.

Wir können nun endliche separable Körpererweiterungen mit Hilfe des Separabilitätsgrades charakterisieren.

Theorem 9. *Es sei $K \subset L$ eine endliche Körpererweiterung. Dann ist äquivalent*:

(i) *L/K ist separabel.*

(ii) *Es gibt über K separable Elemente $a_1, \ldots, a_n$, die L/K erzeugen, so dass also $L = K(a_1, \ldots, a_n)$ gilt.*

(iii) $[L : K]_s = [L : K]$.

Beweis. Die Implikation von (i) nach (ii) ist trivial. Ist $a \in L$ separabel über K, so auch über jedem Zwischenkörper zu L/K. Somit lässt sich die Implikation von (ii) nach (iii) mit Hilfe der Gradformeln aus 3.2/2 und Satz 7 auf den Fall einer einfachen Körpererweiterung zurückführen. Diesen Fall haben wir aber in Lemma 6 (ii) bereits behandelt.

Nun zur Implikation von (iii) nach (i). Sei $a \in L$, und sei $f \in K[X]$ das Minimalpolynom von a über K. Um zu zeigen, dass a separabel über K ist, dass also f separabel ist, bleibt wegen Bemerkung 4 nur der Fall $\operatorname{char} K = p > 0$ zu betrachten. Nach Satz 2 (ii) gibt es ein $r \in \mathbb{N}$, so dass jede Nullstelle von f die Vielfachheit p^r besitzt. Es folgt

$$\big[K(a) : K\big] = p^r \cdot \big[K(a) : K\big]_s$$

mit Lemma 6. Unter Benutzung der Gradformeln aus 3.2/2 und Satz 7 sowie der Abschätzung zwischen Grad und Separabilitätsgrad in Satz 8 ergibt sich dann

$$\begin{aligned} \big[L : K\big] &= \big[L : K(a)\big] \cdot \big[K(a) : K\big] \\ &\geq \big[L : K(a)\big]_s \cdot p^r \cdot \big[K(a) : K\big]_s = p^r \cdot \big[L : K\big]_s. \end{aligned}$$

Gilt nun $[L : K]_s = [L : K]$, so folgt notwendig $r = 0$, d. h. alle Nullstellen von f sind einfach. Mithin ist a separabel über K. Dies zeigt, dass (iii) Bedingung (i) impliziert. □

Korollar 10. *Es sei $K \subset L$ eine algebraische Körpererweiterung und $\mathfrak{A}$ eine Familie von Elementen aus L, so dass die Körpererweiterung L/K von $\mathfrak{A}$ erzeugt wird. Dann ist äquivalent*:

(i) *L/K ist separabel.*

(ii) *Jedes $a \in \mathfrak{A}$ ist separabel über K.*

Ist eine der beiden Bedingungen erfüllt, so gilt $[L : K] = [L : K]_s$.

Beweis. Jedes Element $a \in L$ ist enthalten in einem Teilkörper der Form $K(a_1, \ldots, a_n)$ mit $a_1, \ldots, a_n \in \mathfrak{A}$. Damit ist die Äquivalenz von (i) und (ii)

eine direkte Konsequenz aus Theorem 9. Ist weiter L/K separabel, so gilt im Falle der Endlichkeit von $[L : K]$ die Gleichung $[L : K] = [L : K]_s$, ebenfalls aufgrund von Theorem 9. Sei nun L/K separabel mit $[L : K] = \infty$. Dann ist auch jeder Zwischenkörper E von L/K separabel über K, und für $[E : K] < \infty$ folgt $[E : K] = [E : K]_s$, so dass man unter Benutzung des Gradsatzes 7 die Abschätzung $[L : K]_s \geq [E : K]$ erhält. Da es zu L/K Zwischenkörper E beliebig großen Grades über K gibt, hat man $[L : K]_s = \infty = [L : K]$. □

Korollar 11. *Es seien $K \subset L \subset M$ algebraische Körpererweiterungen. Es ist M/K genau dann separabel, wenn M/L und L/K separabel sind.*

Beweis. Es ist nur zu zeigen, dass aus der Separabilität von M/L und L/K die Separabilität von M/K folgt. Sei $a \in M$ mit Minimalpolynom $f \in L[X]$ über L. Sei L' derjenige Zwischenkörper zu L/K, der über K von den Koeffizienten von f erzeugt wird. Da M/L separabel ist, ist f separabel. Somit ist $L'(a)/L'$ separabel und ebenfalls L'/K, da L/K separabel ist. Im Übrigen sind $L'(a)/L'$ und L'/K endlich, und es folgt unter Benutzung der Gradformeln

$$\begin{aligned}\big[L'(a) : K\big]_s &= \big[L'(a) : L'\big]_s \cdot \big[L' : K\big]_s \\ &= \big[L'(a) : L'\big] \cdot \big[L' : K\big] = \big[L'(a) : K\big],\end{aligned}$$

d. h. $L'(a)$ ist separabel über K. Insbesondere ist dann a separabel über K. □

Abschließend wollen wir noch den sogenannten *Satz vom primitiven Element* beweisen, der eine Aussage über endliche separable Körpererweiterungen macht.

Satz 12. *Es sei L/K eine endliche Körpererweiterung, etwa von der Form $L = K(a_1, \ldots, a_r)$. Sind dann die Elemente $a_2, \ldots, a_r$ separabel über K, so existiert ein* primitives Element *zu L/K, d. h. ein Element $a \in L$ mit $L = K(a)$. Insbesondere besitzt jede endliche separable Körpererweiterung ein primitives Element.*

Beweis. Wir wollen zunächst annehmen, dass K nur endlich viele Elemente besitzt. Dann ist wegen $[L : K] < \infty$ auch L endlich. Insbesondere ist die

multiplikative Gruppe L^* endlich und folglich zyklisch, wie wir weiter unten in Satz 14 zeigen werden. Ein Element $a \in L$, welches L^* als zyklische Gruppe erzeugt, erzeugt auch L als Erweiterungskörper von K. Bei diesem Argument wird keine Separabilitätsvoraussetzung benutzt; es ist allerdings L/K automatisch separabel, wenn K ein endlicher Körper ist, wie wir in 3.8/4 sehen werden.

Es bleibt noch der Fall zu betrachten, wo K unendlich viele Elemente besitzt. Mit Hilfe eines Induktionsarguments reduziert man die Behauptung auf den Fall $L = K(a, b)$; wir dürfen also annehmen, dass L von zwei Elementen a, b über K erzeugt wird, wobei b separabel über K ist. Sei dann $n = [L : K]_s$ und seien $\sigma_1, \ldots, \sigma_n$ die paarweise verschiedenen Elemente von $\mathrm{Hom}_K(L, \overline{K})$, wobei wie üblich $\overline{K}$ einen algebraischen Abschluss von K bezeichne. Man betrachte dann das Polynom

$$P = \prod_{i \neq j} \Big[\big(\sigma_i(a) - \sigma_j(a)\big) \; + \; \big(\sigma_i(b) - \sigma_j(b)\big) \cdot X \Big].$$

Es ist $P \in \overline{K}[X]$ nicht das Nullpolynom; denn für $i \neq j$ hat man notwendig $\sigma_i(a) \neq \sigma_j(a)$ oder $\sigma_i(b) \neq \sigma_j(b)$, da ansonsten σ_i wegen $L = K[a, b]$ mit σ_j übereinstimmen müsste. Weil K unendlich viele Elemente besitzt, P aber nur endlich viele Nullstellen haben kann, gibt es ein $c \in K$ mit $P(c) \neq 0$. Letzteres impliziert, dass die Elemente

$$\sigma_i(a) + c\sigma_i(b) = \sigma_i(a + cb) \in \overline{K}, \qquad i = 1, \ldots, n,$$

paarweise verschieden sind. Es ist dann $L' = K(a + cb)$ eine einfache Körpererweiterung von K mit Separabilitätsgrad

$$[L' : K]_s \geq n = [L : K]_s.$$

Wegen $L' \subset L$ hat man $[L' : K]_s \leq [L : K]_s$ und somit notwendig $[L' : K]_s = [L : K]_s$. Wir wollen zeigen, dass sogar $L' = L$ gilt, woraus sich die Einfachheit der Erweiterung L/K ergibt. Das Element $b \in L$ ist nach Voraussetzung separabel über K, also auch über L', so dass $[L'(b) : L']_s = [L'(b) : L']$ gilt. Weiter liefert die Gradformel in Satz 7 die Abschätzung

$$\big[L : K\big]_s \geq \big[L'(b) : K\big]_s = \big[L'(b) : L'\big]_s \cdot \big[L' : K\big]_s = \big[L'(b) : L'\big] \cdot \big[L : K\big]_s,$$

aus der sich $[L'(b) : L'] = 1$ ergibt. Das bedeutet aber $L'(b) = L'$ und somit $b \in L' = K(a + cb)$. Dann hat man aber auch $a \in K(a + cb)$, also $L = K(a, b) = L'$, d. h. L ist einfache Körpererweiterung von K. □

Es bleibt noch nachzutragen, dass die multiplikative Gruppe eines endlichen Körpers zyklisch ist. Wir beginnen mit einem gruppentheoretischen Hilfsresultat.

Lemma 13. *Es seien a, b Elemente endlicher Ordnung in einer abelschen Gruppe G. Sei* $\operatorname{ord} a = m$ *und* $\operatorname{ord} b = n$. *Dann existiert in G ein Element der Ordnung* $\mathrm{kgV}(m, n)$.

Genauer, wählt man ganzzahlige Zerlegungen $m = m_0 m'$, $n = n_0 n'$ mit $\mathrm{kgV}(m, n) = m_0 n_0$ *und* $\mathrm{ggT}(m_0, n_0) = 1$, *so ist $a^{m'} b^{n'}$ ein Element der Ordnung* $\mathrm{kgV}(m, n)$. *Insbesondere besitzt also ab die Ordnung mn, falls m und n teilerfremd sind.*

Beweis. Wir nehmen zunächst m, n als teilerfremd an und zeigen, dass ab die Ordnung mn besitzt. Natürlich gilt $(ab)^{mn} = (a^m)^n (b^n)^m = 1$. Andererseits erhält man aus $(ab)^t = 1$ die Beziehung $a^{nt} = a^{nt} b^{nt} = 1$, und es folgt $m \mid t$ wegen $\mathrm{ggT}(m, n) = 1$. Ebenso ergibt sich $n \mid t$ und damit $mn \mid t$, also insgesamt $\operatorname{ord}(ab) = mn$.

Im Allgemeinfall wähle man Zerlegungen $m = m_0 m'$, $n = n_0 n'$ mit $\mathrm{kgV}(m, n) = m_0 n_0$ und $\mathrm{ggT}(m_0, n_0) = 1$. Hierzu betrachte man etwa eine Primfaktorzerlegung $p_1^{\nu_1} \cdot \ldots \cdot p_r^{\nu_r}$ von $\mathrm{kgV}(m, n)$ und definiere m_0 als das Produkt aller Primpotenzen $p_i^{\nu_i}$, welche m teilen, sowie n_0 als das Produkt aller Primpotenzen $p_i^{\nu_i}$, die m nicht teilen. Es folgt $m_0 \mid m$ sowie $n_0 \mid n$, und die resultierenden Zerlegungen $m = m_0 m'$, $n = n_0 n'$ erfüllen offenbar die Bedingungen $\mathrm{kgV}(m, n) = m_0 n_0$ und $\mathrm{ggT}(m_0, n_0) = 1$.

Da nun $a^{m'}$ die Ordnung m_0 und $b^{n'}$ die Ordnung n_0 hat, berechnet sich die Ordnung von $a^{m'} b^{n'}$ aufgrund des eingangs behandelten Spezialfalls wie gewünscht zu $m_0 n_0$. □

Satz 14. *Es sei K ein Körper und H eine endliche Untergruppe der multiplikativen Gruppe K^*. Dann ist H zyklisch.*

Beweis. Es sei $a \in H$ ein Element maximaler Ordnung m und H_m die Untergruppe aller Elemente aus H, deren Ordnung ein Teiler von m ist.

Alle Elemente von H_m sind dann Nullstellen des Polynoms $X^m - 1$, so dass H_m höchstens m Elemente enthalten kann. Andererseits enthält H_m die von a erzeugte zyklische Gruppe $\langle a \rangle$, und deren Ordnung ist m. Somit folgt $H_m = \langle a \rangle$, und H_m ist zyklisch. Wir behaupten, dass bereits $H = H_m$ gilt. Gibt es nämlich ein Element $b \in H$, welches nicht zu H_m gehört, dessen Ordnung n also kein Teiler von m ist, so besitzt H aufgrund von Lemma 13 ein Element der Ordnung $\mathrm{kgV}(m, n) > m$. Dies aber widerspricht der Wahl von a. □

Lernkontrolle und Prüfungsvorbereitung

1. Seien K ein Körper, $\overline{K}$ ein algebraischer Abschluss von K und $f \in K[X]$ ein nicht-konstantes Polynom und mit Ableitung f'. Zeige, dass die mehrfachen Nullstellen von f in $\overline{K}$ mit den gemeinsamen Nullstellen von f und f' in $\overline{K}$ übereinstimmen. Zeige weiter, dass diese Nullstellen gerade die Nullstellen von $\mathrm{ggT}(f, f')$ sind, wobei der größte gemeinsame Teiler wahlweise in $K[X]$ oder in $\overline{K}[X]$ gebildet werden kann.

2. Zeige, dass ein irreduzibles Polynom $f \in K[X]$ mit Koeffizienten aus einem Körper K genau dann mehrfache Nullstellen besitzt (in einem algebraischen Abschluss von K), wenn seine Ableitung f' das Nullpolynom ist.

3. Was versteht man unter einem separablen Polynom? Zeige, dass über einem Körper der Charakteristik 0 jedes irreduzible Polynom separabel ist.

4. Es sei K ein Körper der Charakteristik $p > 0$ und $f \in K[X]$ ein irreduzibles Polynom. Wie lässt sich das Vorliegen mehrfacher Nullstellen von f (in einem algebraischen Abschluss von K) an der Form von f ablesen?

5. Sei L/K eine algebraische Körpererweiterung. Wann nennt man ein Element $\alpha \in L$ separabel über K? Wann heißt die Erweiterung L/K separabel? Wann bezeichnet man einen Körper K als vollkommen?

6. Zeige, dass Körper der Charakteristik 0 vollkommen sind. Gib ein einfaches Beispiel einer algebraischen Körpererweiterung, die nicht separabel ist.

7. Was versteht man unter dem Separabilitätsgrad $[L\colon K]_s$ einer algebraischen Körpererweiterung L/K? Wie berechnet sich der Separabilitätsgrad speziell für eine einfache algebraische Körpererweiterung $K(\alpha)/K$?

8. Wie lautet der Gradsatz für den Separabilitätsgrad? Wie kann man diesen beweisen?

9. Sei L/K eine endliche algebraische Körpererweiterung. Welche Beziehung besteht zwischen dem Separabilitätsgrad $[L\colon K]_s$ und dem Grad $[L\colon K]$ (mit Begründung)?

10. Es sei L/K eine einfache algebraische Körpererweiterung, die von einem Element $\alpha \in L$ erzeugt werde. Zeige, dass die Erweiterung L/K genau dann separabel ist, wenn α separabel über K ist.

11. Es sei L/K eine endliche algebraische Körpererweiterung. Wie lässt sich die Separabilität von L/K durch äquivalente Bedingungen charakterisieren (mit Begründung)? Welche dieser Äquivalenzen bleiben auch für beliebige algebraische Körpererweiterungen gültig?

12. Betrachte zu einer algebraischen Körpererweiterung L/K die Menge E aller Elemente $\alpha \in L$, die separabel über K sind. Zeige, dass E ein Körper ist und dass die Erweiterung E/K separabel ist.

13. Es seien $K \subset L \subset M$ algebraische Körpererweiterungen. Zeige, dass M/K genau dann separabel ist, wenn M/L und L/K separabel sind.

14. Wie lautet der Satz vom primitiven Element für algebraische Körpererweiterungen?

+15. Gib einen Beweis für den Satz vom primitiven Element.

Übungsaufgaben

1. *Begründe nochmals im Detail, dass für eine algebraische Körpererweiterung L/K und zwei über K separable Elemente $a, b \in L$ auch deren Summe $a + b$ separabel über K ist. Genauer lässt sich zeigen, dass die über K separablen Elemente von L einen Zwischenkörper zu L/K bilden. Es handelt sich um die sogenannte* separable Hülle *von K in L.*

2. *Es sei K ein Körper und $f \in K[X]$ ein nicht-konstantes Polynom. Warum hängt die Aussage, f habe mehrfache Nullstellen in einem algebraischen Abschluss $\overline{K}$ von K, nicht von der Wahl von $\overline{K}$ ab*?

3. *Der Beweis zu Satz* 12 *beinhaltet ein praktisches Verfahren zur Bestimmung primitiver Elemente bei endlichen separablen Körpererweiterungen. Skizziere dieses Verfahren.*

4. Es seien $K \subset L \subset M$ algebraische Körpererweiterungen, wobei M/K normal sei. Zeige: $[L : K]_s = \#\operatorname{Hom}_K(L, M)$.

5. Betrachte für eine gegebene Primzahl p den Funktionenkörper $L = \mathbb{F}_p(X, Y)$ in zwei Variablen über $\mathbb{F}_p$ sowie den Frobenius-Homomorphismus $\sigma\colon L \longrightarrow L$, $a \longmapsto a^p$. Sei $K = \sigma(L)$ das Bild unter σ. Berechne die Grade $[L : K]$ und $[L : K]_s$ und zeige, dass die Körpererweiterung L/K nicht einfach ist.

6. Sei L/K eine Körpererweiterung in Charakteristik $p > 0$. Zeige, dass ein über K algebraisches Element $\alpha \in L$ genau dann separabel über K ist, wenn $K(\alpha) = K(\alpha^p)$ gilt.

7. Eine algebraische Körpererweiterung L/K ist genau dann einfach, wenn sie nur endlich viele Zwischenkörper zulässt. Beweise diese Aussage in folgenden Schritten:

   (i) Diskutiere zunächst den Fall, wo K endlich ist, so dass wir K im Folgenden als unendlich annehmen dürfen.

   (ii) Sei $L = K(\alpha)$ und sei $f \in K[X]$ das Minimalpolynom von α über K. Die Menge der Zwischenkörper von L/K lässt sich identifizieren mit einer Teilmenge der Teiler von f, aufgefasst als Polynom in $L[X]$.

   (iii) Es möge L/K nur endlich viele Zwischenkörper zulassen. Um zu zeigen, dass L/K einfach ist, reduziere auf den Fall, wo L über K von zwei Elementen α, β erzeugt wird. Für $L = K(\alpha, \beta)$ schließlich betrachte zu Konstanten $c \in K$ die Körper $K(\alpha + c\beta)$.

8. Sei K ein endlicher Körper. Zeige, dass das Produkt aller Elemente aus K^* den Wert -1 ergibt. Folgere als Anwendung für Primzahlen p die Teilbarkeitsrelation $p \mid ((p-1)! + 1)$.

3.7 Rein inseparable Körpererweiterungen

Im vorigen Abschnitt haben wir für algebraische Körpererweiterungen L/K den Separabilitätsgrad $[L : K]_s$ eingeführt, wobei gemäß 3.6/8 die Abschätzung $1 \leq [L : K]_s \leq [L : K]$ gilt. Ist L/K endlich, so ist die Erweiterung genau dann separabel, wenn $[L : K]_s = [L : K]$ gilt. In diesem Abschnitt betrachten wir als anderes Extrem Körpererweiterungen mit der Eigenschaft $[L : K]_s = 1$. Da Körpererweiterungen in Charakteristik 0 stets separabel sind, setzen wir in diesem Abschnitt generell voraus, dass K ein *Körper der Charakteristik* $p > 0$ ist.

Wir nennen ein Polynom $f \in K[X]$ *rein inseparabel*, wenn es (in einem algebraischen Abschluss $\overline{K}$ von K) genau eine Nullstelle α hat. Da das Minimalpolynom $m_\alpha \in K[X]$ zu α ein Teiler von f ist, sieht man

per Induktion nach dem Grad von f, dass f abgesehen von einem Faktor aus K^* eine Potenz von m_α ist, also eine Potenz eines irreduziblen rein inseparablen Polynoms. Ist weiter $h \in K[X]$ ein normiertes irreduzibles Polynom, welches rein inseparabel ist, so sieht man unter Benutzung von 3.1/3 und 3.6/2 (ii), dass h von der Form $X^{p^n} - c$ mit $n \in \mathbb{N}$ und $c \in K$ ist. Umgekehrt ist klar, dass alle Polynome dieses Typs rein inseparabel sind. Die normierten rein inseparablen Polynome in $K[X]$ sind daher gerade die Potenzen von Polynomen des Typs $X^{p^n} - c$.

Definition 1. *Es sei $K \subset L$ eine algebraische Körpererweiterung. Ein Element $\alpha \in L$ heißt* rein inseparabel *über K, wenn α Nullstelle eines rein inseparablen Polynoms aus $K[X]$ ist oder, was hierzu äquivalent ist, wenn das Minimalpolynom von α über K von der Form $X^{p^n} - c$ mit $n \in \mathbb{N}$ und $c \in K$ ist. Es heißt L* rein inseparabel *über K, wenn jedes $\alpha \in L$ rein inseparabel über K in dem vorstehenden Sinne ist.*

Es folgt unmittelbar aus der Definition, dass rein inseparable Erweiterungen stets normal sind. Die triviale Erweiterung K/K ist die einzige Körpererweiterung, welche separabel und rein inseparabel zugleich ist. Die Erweiterung $\mathbb{F}_p(t)/\mathbb{F}_p(t^p)$ aus dem vorigen Abschnitt ist ein Beispiel für eine nicht-triviale rein inseparable Körpererweiterung.

Satz 2. *Es sei $K \subset L$ eine algebraische Körpererweiterung. Dann ist äquivalent*:

(i) *L ist rein inseparabel über K.*

(ii) *Es existiert eine Familie $\mathfrak{A} = (a_i)_{i \in I}$ über K rein inseparabler Elemente aus L mit $L = K(\mathfrak{A})$.*

(iii) $[L : K]_s = 1$.

(iv) *Zu jedem $a \in L$ gibt es ein $n \in \mathbb{N}$ mit $a^{p^n} \in K$.*

Beweis. Die Implikation von (i) nach (ii) ist trivial. Ist Bedingung (ii) gegeben, so genügt es zum Nachweis von (iii), zu zeigen, dass für $i \in I$ stets $[K(a_i) : K]_s = 1$ gilt; denn ein K-Homomorphismus $L \longrightarrow \overline{K}$ in einen algebraischen Abschluss $\overline{K}$ von K ist bereits durch die Bilder der a_i festgelegt. Das Minimalpolynom eines jeden Elementes a_i ist aber von der Form $X^{p^n} - c$, hat also lediglich eine Nullstelle in $\overline{K}$, so dass mit 3.4/8 wie gewünscht $[K(a_i) : K]_s = 1$ folgt.

Wir nehmen nun Bedingung (iii) an und leiten (iv) hieraus ab. Sei $a \in L$. Dann gilt

$$\big[L : K(a)\big]_s \cdot \big[K(a) : K\big]_s = \big[L : K\big]_s = 1$$

und somit $[K(a) : K]_s = 1$. Dies bedeutet, dass das Minimalpolynom von a über K nur eine einzige Nullstelle besitzt, also nach 3.6/2 von der Form $X^{p^n} - c$ ist. Daher gilt $a^{p^n} \in K$. Umgekehrt ergibt sich aus $a^{p^n} \in K$, dass a Nullstelle eines rein inseparablen Polynoms der Form $X^{p^n} - c \in K[X]$ ist, also eines Polynoms mit einer einzigen Nullstelle. Dann hat aber das Minimalpolynom von a auch lediglich eine Nullstelle, und a ist rein inseparabel über K. Dies zeigt, dass aus (iv) Bedingung (i) folgt. □

Korollar 3. *Es seien $K \subset L \subset M$ algebraische Körpererweiterungen. Dann sind M/L und L/K genau dann rein inseparabel, wenn M/K rein inseparabel ist.*

Beweis. $[M : K]_s = [M : L]_s \cdot [L : K]_s$, vgl. 3.6/7. □

Wir wollen nun noch beweisen, dass man eine algebraische Körpererweiterung stets in einen separablen und einen rein inseparablen Anteil zerlegen kann, wobei dies im Falle normaler Erweiterungen auf zwei Weisen geschehen kann.

Satz 4. *Es sei L/K eine algebraische Körpererweiterung. Dann existiert eindeutig ein Zwischenkörper K_s zu L/K, so dass L/K_s rein inseparabel und K_s/K separabel ist. Es ist K_s die* separable Hülle *von K in L, d. h.*

$$K_s = \big\{a \in L\,;\ a \text{ separabel über } K\big\},$$

und es gilt $[L : K]_s = [K_s : K]$. Ist L/K normal, so auch K_s/K.

Satz 5. *Es sei L/K eine* normale *algebraische Körpererweiterung. Dann existiert eindeutig ein Zwischenkörper K_i zu L/K, so dass L/K_i separabel und K_i/K rein inseparabel ist.*

Beweis zu Satz 4. Wir setzen

$$K_s = \big\{a \in L\,;\ a \text{ separabel über } K\big\}.$$

Dann ist K_s ein Körper, denn für $a, b \in K_s$ ist $K(a, b)$ nach 3.6/9 eine separable Erweiterung von K, so dass $K(a, b) \subset K_s$. Es ist also K_s die größte in L enthaltene separable Erweiterung von K. Sei nun $a \in L$ und $f \in K_s[X]$ das Minimalpolynom von a über K_s. Dann gibt es nach 3.6/2 aufgrund der Irreduzibilität von f ein $r \in \mathbb{N}$ sowie ein irreduzibles separables Polynom $g \in K_s[X]$ mit $f(X) = g(X^{p^r})$. Insbesondere ist g das Minimalpolynom von $c = a^{p^r}$ über K_s, und c ist separabel über K_s, also nach 3.6/11 auch über K. Dann muss aber $c \in K_s$ gelten, d. h. g ist linear, und es folgt $f = X^{p^r} - c$. Somit ist a rein inseparabel über K_s und daher L/K_s rein inseparabel.

Aus der reinen Inseparabilität von L/K_s und der Separabilität von K_s/K folgt die behauptete Gradgleichung:

$$[L : K]_s = [L : K_s]_s \cdot [K_s : K]_s = [K_s : K].$$

Um die Eindeutigkeit von K_s nachzuweisen, betrachte man einen Zwischenkörper K' zu L/K, so dass L/K' rein inseparabel und K'/K separabel ist. Dann gilt $K' \subset K_s$ nach Definition von K_s, und die Erweiterung K_s/K' ist separabel. Sie ist zugleich aber auch rein inseparabel, da L/K' rein inseparabel ist. Daher folgt $K_s = K'$, d. h. K_s ist eindeutig bestimmt.

Es bleibt noch nachzuweisen, dass mit L/K auch K_s/K normal ist. Man betrachte einen K-Homomorphismus $\sigma\colon K_s \longrightarrow \overline{L}$ in einen algebraischen Abschluss $\overline{L}$ von L hinein, wobei wir $\overline{L}$ auch als algebraischen Abschluss von K auffassen können. Es setzt sich dann σ gemäß 3.4/9 zu einem K-Homomorphismus $\sigma'\colon L \longrightarrow \overline{L}$ fort. Wenn L/K normal ist, beschränkt sich σ' zu einem K-Automorphismus von L. Die Eindeutigkeitsaussage für K_s zeigt dann, dass sich σ zu einem K-Automorphismus von K_s beschränkt, d. h. K_s/K ist normal. □

Beweis zu Satz 5. Da L/K normal ist, können wir K-Homomorphismen von L in einen algebraischen Abschluss $\overline{L}$ von L mit den K-Automorphismen von L identifizieren. Die K-Automorphismen von L bilden eine Gruppe G. Es sei

$$K_i = \{a \in L\,;\, \sigma(a) = a \text{ für alle } \sigma \in G\}$$

die Fixmenge unter G; man prüft unmittelbar nach, dass K_i ein Körper ist. Da sich jeder K-Homomorphismus $K_i \longrightarrow \overline{L}$ nach 3.4/9 zu einem K-Homomorphismus $L \longrightarrow \overline{L}$ fortsetzt und die Fortsetzung K_i definitionsgemäß festlässt, folgt $\#\operatorname{Hom}_K(K_i, \overline{L}) = 1$. Indem man $\overline{L}$ als algebraischen Abschluss von K auffasst, schließt man hieraus, dass K_i/K rein inseparabel

ist. Genauer sieht man aufgrund der Äquivalenz von (i) und (iii) in Satz 2, dass K_i die größte rein inseparable Erweiterung von K ist, die in L enthalten ist. Um zu sehen, dass L/K_i separabel ist, betrachte man ein Element $a \in L$ sowie ein maximales System von Elementen $\sigma_1, \ldots, \sigma_r \in G$ mit der Eigenschaft, dass $\sigma_1(a), \ldots, \sigma_r(a)$ paarweise verschieden sind. Ein solches endliches System existiert stets, auch dann, wenn G nicht endlich ist; denn für $\sigma \in G$ ist $\sigma(a)$ jeweils Nullstelle des Minimalpolynoms von a über K. Im Übrigen bemerke man, dass das Element a notwendigerweise unter den $\sigma_i(a)$ vorkommt. Jedes $\sigma \in G$ induziert eine bijektive Selbstabbildung auf der Menge $\{\sigma_1(a), \ldots, \sigma_r(a)\}$, und es folgt, dass das Polynom

$$f = \prod_{i=1}^{r} \big(X - \sigma_i(a)\big)$$

Koeffizienten in K_i hat, da diese unter G festgelassen werden. Es ist also a Nullstelle eines separablen Polynoms aus $K_i[X]$ und damit a separabel über K_i, so dass insgesamt L/K_i separabel ist. Die Eindeutigkeitsaussage für K_i folgt ähnlich wie in Satz 4 aus der Tatsache, dass K_i der größte Zwischenkörper zu L/K ist, der rein inseparabel über K ist. □

Lernkontrolle und Prüfungsvorbereitung

K sei stets ein Körper der Charakteristik $p > 0$.

1. Wann bezeichnet man ein Polynom aus $K[X]$ als rein inseparabel? Welche rein inseparablen Polynome gibt es in $K[X]$?

2. Sei L/K eine algebraische Körpererweiterung. Wann bezeichnet man ein Element $\alpha \in L$ als rein inseparabel über K? Wann nennt man die Erweiterung L/K rein inseparabel? Gib ein Beispiel einer nicht-trivialen rein inseparablen algebraischen Körpererweiterung L/K.

3. Der Körper K sei endlich, d. h. es bestehe K nur aus endlich vielen Elementen. Zeige, dass der Frobenius-Homomorphismus $K \longrightarrow K$, $a \longmapsto a^p$, surjektiv ist und dass K keine echte rein inseparable algebraische Körpererweiterung L/K zulässt.

4. Zeige, dass eine algebraische Körpererweiterung L/K genau dann rein inseparabel ist, wenn $[L\colon K]_s = 1$ gilt. Welche weiteren äquivalenten Charakterisierungen der reinen Inseparabilität gibt es?

5. Seien M/L und L/K algebraische Körpererweiterungen. Zeige, dass M/K genau dann rein inseparabel ist, wenn dies für M/L und L/K gilt.

6. Sei L/K eine algebraische Körpererweiterung, welche separabel und rein inseparabel zugleich sei. Zeige $L = K$.

7. Sei L/K eine algebraische Körpererweiterung. Erkläre die Konstruktion der separablen Hülle K_s von K in L und zeige, dass die Erweiterung L/K_s rein inseparabel ist. Welche Eindeutigkeitsaussage gilt? Zeige weiter, dass K_s/K normal ist, wenn dies für L/K gilt.

+8. Sei L/K eine normale algebraische Körpererweiterung. Zeige, dass es einen eindeutig bestimmten Zwischenkörper K_i zu L/K gibt, derart dass L/K_i separabel und K_i/K rein inseparabel ist.

Übungsaufgaben

1. *Sei L/K eine Körpererweiterung, und seien $\alpha, \beta \in L$ rein inseparabel über K. Zeige in expliziter Weise, dass dann auch $\alpha + \beta$ und $\alpha \cdot \beta$ rein inseparabel über K sind.*

2. *Für eine endliche Körpererweiterung L/K definiert man den Inseparabilitätsgrad durch $[L : K]_i = [L : K] \cdot [L : K]_s^{-1}$. Welcher Nachteil ergibt sich, wenn man die Resultate dieses Abschnitts über rein inseparable Körpererweiterungen mit Hilfe des Inseparabilitätsgrads anstelle des Separabilitätsgrads formulieren und beweisen möchte?*

3. *Begründe für eine einfache algebraische Körpererweiterung L/K in direkter Weise den aus Satz 4 bekannten Sachverhalt, dass es einen Zwischenkörper K_s mit L/K_s rein inseparabel und K_s/K separabel gibt.*

4. Sei K ein Körper der Charakteristik $p > 0$. Zeige, dass der Frobenius-Homomorphismus $\sigma\colon K \longrightarrow K$, $a \longmapsto a^p$, genau dann surjektiv ist, wenn K vollkommen ist.

5. Sei L/K eine Körpererweiterung, und sei $\alpha \in L$ separabel über K sowie $\beta \in L$ rein inseparabel über K. Zeige:
   (i) $K(\alpha, \beta) = K(\alpha + \beta)$,
   (ii) $K(\alpha, \beta) = K(\alpha \cdot \beta)$, falls $\alpha \neq 0 \neq \beta$.

6. Sei K ein Körper der Charakteristik $p > 0$. Zeige:
   (i) Zu $n \in \mathbb{N}$ existiert ein Erweiterungskörper $K^{p^{-n}}$ von K mit folgenden Eigenschaften: Für $a \in K^{p^{-n}}$ gilt $a^{p^n} \in K$, und zu jedem $b \in K$ gibt es ein $a \in K^{p^{-n}}$ mit $a^{p^n} = b$.

(ii) Es ist $K^{p^{-n}}$ eindeutig bis auf kanonische Isomorphie, und man hat kanonische Einbettungen $K \subset K^{p^{-1}} \subset K^{p^{-2}} \subset \ldots$

(iii) Es ist $K^{p^{-\infty}} = \bigcup_{i=0}^{\infty} K^{p^{-i}}$ vollkommen.

Man nennt $K^{p^{-\infty}}$ auch den *rein inseparablen Abschluss* von K.

7. Sei L/K eine algebraische Körpererweiterung. Zeige:

   (i) Mit K ist auch L vollkommen.

   (ii) Ist L vollkommen und L/K endlich, so ist auch K vollkommen.

   Gib ein Beispiel an, welches zeigt, dass Aussage (ii) im Allgemeinen nicht richtig ist, wenn man auf die Endlichkeit von L/K verzichtet.

8. Sei L/K eine separable algebraische Körpererweiterung. Zeige die Äquivalenz folgender Aussagen:

   (i) Jedes nicht-konstante separable Polynom in $L[X]$ zerfällt vollständig in Linearfaktoren.

   (ii) Bei Wahl eines algebraischen Abschlusses $\overline{K}$ von K und einer K-Einbettung $L \hookrightarrow \overline{K}$ ist die Erweiterung $\overline{K}/L$ rein inseparabel.

   Zeige, dass es zu einem Körper K stets eine algebraische Erweiterung $L = K_{\text{sep}}$ mit den vorstehenden Eigenschaften gibt und dass diese bis auf K-Isomorphie eindeutig ist. Man nennt K_{sep} einen *separabel algebraischen Abschluss* von K.

9. Sei L/K eine normale algebraische Körpererweiterung der Charakteristik > 0. Betrachte die Zwischenkörper K_s und K_i aus den Sätzen 4 und 5 und zeige: $L = K_s(K_i) = K_i(K_s)$.

10. Sei L/K eine algebraische Körpererweiterung mit der Eigenschaft, dass jedes irreduzible Polynom aus $K[X]$ mindestens eine Nullstelle in L habe. Zeige, dass L ein algebraischer Abschluss von K ist.

3.8 Endliche Körper

Die endlichen Körper $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$, wobei p eine Primzahl ist, sind uns bereits geläufig. Es sind dies gerade die Primkörper der Charakteristik > 0; vgl. 3.1/2. Wir wollen im Folgenden für jede echte Potenz q von p, also für $q = p^n$ mit $n > 0$, einen Körper $\mathbb{F}_q$ mit q Elementen konstruieren. Dabei beachte man, dass ein solcher Körper für $n > 1$ grundverschieden von dem Restklassenring $\mathbb{Z}/p^n\mathbb{Z}$ sein muss, da $\mathbb{Z}/p^n\mathbb{Z}$ für $n > 1$ Nullteiler besitzt und somit kein Körper ist.

Lemma 1. *Es sei $\mathbb{F}$ ein endlicher Körper. Dann gilt $p = \operatorname{char}\mathbb{F} > 0$, und $\mathbb{F}$ enthält $\mathbb{F}_p$ als Primkörper. Weiter besteht $\mathbb{F}$ aus genau $q = p^n$ Elementen, wobei $n = [\mathbb{F} : \mathbb{F}_p]$. Es ist $\mathbb{F}$ Zerfällungskörper des Polynoms $X^q - X$ über $\mathbb{F}_p$; die Erweiterung $\mathbb{F}/\mathbb{F}_p$ ist daher normal.*

Beweis. Mit $\mathbb{F}$ ist auch der zugehörige Primkörper endlich, also von der Form $\mathbb{F}_p$ mit $p = \operatorname{char}\mathbb{F} > 0$. Weiter ergibt sich aus der Endlichkeit von $\mathbb{F}$, dass der Grad $n = [\mathbb{F} : \mathbb{F}_p]$ endlich ist, und man sieht, etwa durch Ausnutzung eines Isomorphismus von $\mathbb{F}_p$-Vektorräumen $\mathbb{F} \xrightarrow{\sim} (\mathbb{F}_p)^n$, dass $\mathbb{F}$ aus $q = p^n$ Elementen besteht. Die multiplikative Gruppe $\mathbb{F}^*$ hat dann die Ordnung $q - 1$, und jedes Element aus $\mathbb{F}^*$ ist Nullstelle des Polynoms $X^{q-1} - 1$, jedes Element aus $\mathbb{F}$ folglich Nullstelle des Polynoms $X^q - X$. Es besteht daher $\mathbb{F}$ aus insgesamt $q = p^n$ Nullstellen von $X^q - X$, d. h. aus sämtlichen Nullstellen dieses Polynoms. Somit zerfällt $X^q - X$ über $\mathbb{F}$ vollständig in Linearfaktoren, und man erkennt, dass $\mathbb{F}$ Zerfällungskörper des Polynoms $X^q - X \in \mathbb{F}_p[X]$ ist. □

Theorem 2. *Es sei p eine Primzahl. Zu jedem $n \in \mathbb{N} - \{0\}$ existiert ein Erweiterungskörper $\mathbb{F}_q/\mathbb{F}_p$ mit $q = p^n$ Elementen. Es ist $\mathbb{F}_q$ bis auf Isomorphie eindeutig charakterisiert als Zerfällungskörper des Polynoms $X^q - X$ über $\mathbb{F}_p$; es besteht $\mathbb{F}_q$ gerade aus den q Nullstellen von $X^q - X$.*

Jeder endliche Körper der Charakteristik p ist isomorph zu genau einem endlichen Körper des Typs $\mathbb{F}_q$.

Beweis. Man setze $f = X^q - X$. Wegen $f' = -1$ hat das Polynom f keine mehrfachen Nullstellen, also insgesamt q einfache Nullstellen in einem algebraischen Abschluss $\overline{\mathbb{F}}_p$ von $\mathbb{F}_p$. Sind dann $a, b \in \overline{\mathbb{F}}_p$ zwei Nullstellen von f, so gilt aufgrund der binomischen Formel 3.1/3

$$(a \pm b)^q = a^q \pm b^q = a \pm b,$$

so dass $a \pm b$ wiederum Nullstelle von f ist. Außerdem folgt für $b \neq 0$

$$(ab^{-1})^q = a^q (b^q)^{-1} = ab^{-1},$$

d. h. die q Nullstellen von f in $\overline{\mathbb{F}}_p$ bilden einen Körper mit q Elementen, nämlich den (in $\overline{\mathbb{F}}_p$ gebildeten) Zerfällungskörper von f über $\mathbb{F}_p$. Dies zeigt die Existenz eines Körpers der Charakteristik p mit $q = p^n$ Elementen. Die Eindeutigkeitsaussagen folgen mit Lemma 1. □

Im Folgenden sei p stets eine Primzahl. Wenn man mit endlichen Körpern der Charakteristik $p > 0$ arbeitet, so wählt man meist einen algebraischen Abschluss $\overline{\mathbb{F}}_p$ von $\mathbb{F}_p$ und stellt sich vor, dass die Körper $\mathbb{F}_{p^n}$ für $n \in \mathbb{N} - \{0\}$ mittels 3.4/9 in $\overline{\mathbb{F}}_p$ eingebettet sind. Als normale Erweiterung von $\mathbb{F}_p$ gibt $\mathbb{F}_{p^n}$ dann aufgrund von 3.5/4 (i) Anlass zu einem eindeutig bestimmten Teilkörper von $\overline{\mathbb{F}}_p$.

Korollar 3. *Man bette die Körper $\mathbb{F}_q$ mit $q = p^n$, $n \in \mathbb{N} - \{0\}$, in einen algebraischen Abschluss $\overline{\mathbb{F}}_p$ von $\mathbb{F}_p$ ein. Es ist dann $\mathbb{F}_q \subset \mathbb{F}_{q'}$ für $q = p^n$ und $q' = p^{n'}$ äquivalent zu $n \mid n'$. Die Erweiterungen des Typs $\mathbb{F}_q \subset \mathbb{F}_{q'}$ sind bis auf Isomorphie die einzigen Erweiterungen zwischen endlichen Körpern der Charakteristik p.*

Beweis. Es gelte $\mathbb{F}_q \subset \mathbb{F}_{q'}$ und $m = [\mathbb{F}_{q'} : \mathbb{F}_q]$. Dann hat man

$$p^{n'} = \#\mathbb{F}_{q'} = (\#\mathbb{F}_q)^m = p^{mn},$$

also $n \mid n'$. Gilt umgekehrt $n' = mn$, so folgt für $a \in \mathbb{F}_q$, also für $a \in \overline{\mathbb{F}}_p$ mit $a^q = a$, in rekursiver Weise $a^{q'} = a^{(q^m)} = (a^q)^{(q^{m-1})} = a^{(q^{m-1})} = a$, d. h. $\mathbb{F}_q \subset \mathbb{F}_{q'}$. Dass es bis auf Isomorphie keine anderen Erweiterungen zwischen endlichen Körpern der Charakteristik p gibt, folgt aus dem Fortsetzungssatz 3.4/9. Ist etwa $\mathbb{F} \subset \mathbb{F}'$ eine Erweiterung endlicher Körper der Charakteristik p, so kann man die Inklusion $\mathbb{F}_p \subset \overline{\mathbb{F}}_p$ fortsetzen zu einem Homomorphismus $\mathbb{F} \longrightarrow \overline{\mathbb{F}}_p$ und diesen wiederum zu einem Homomorphismus $\mathbb{F}' \longrightarrow \overline{\mathbb{F}}_p$, so dass man sich modulo Isomorphie auf den Fall $\mathbb{F} \subset \mathbb{F}' \subset \overline{\mathbb{F}}_p$ beschränken kann. □

Korollar 4. *Jede algebraische Erweiterung eines endlichen Körpers ist normal und separabel. Insbesondere sind endliche Körper vollkommen.*

Beweis. Sei $\mathbb{F} \subset K$ eine algebraische Körpererweiterung, $\mathbb{F}$ endlich. Ist zunächst K ebenfalls endlich, etwa $K = \mathbb{F}_q$ mit $q = p^n$, so ist K als Zerfällungskörper des separablen Polynoms $X^q - X$ normal und separabel über $\mathbb{F}_p$ bzw. $\mathbb{F}$. Im Allgemeinfall lässt sich K durch endliche Erweiterungen von $\mathbb{F}$ ausschöpfen. □

Wir haben bereits in 3.6/14 gesehen, dass die multiplikative Gruppe eines endlichen Körpers zyklisch ist; wir können also vermerken:

Satz 5. *Es sei q eine Potenz einer Primzahl. Dann ist die multiplikative Gruppe von $\mathbb{F}_q$ zyklisch von der Ordnung $q-1$.*

Zum Abschluss wollen wir für eine endliche Erweiterung $\mathbb{F}_{q'}/\mathbb{F}_q$ vom Grad n die Automorphismengruppe $\mathrm{Aut}_{\mathbb{F}_q}(\mathbb{F}_{q'})$ bestimmen, also deren Galois-Gruppe, wie wir im nächsten Kapitel sagen werden; es sei $q = p^r$, $q' = q^n = p^{rn}$. Wählen wir einen algebraischen Abschluss $\overline{\mathbb{F}}_p$ von $\mathbb{F}_q$, so gilt aufgrund der Normalität von $\mathbb{F}_{q'}/\mathbb{F}_q$

$$\mathrm{Aut}_{\mathbb{F}_q}(\mathbb{F}_{q'}) = \mathrm{Hom}_{\mathbb{F}_q}(\mathbb{F}_{q'}, \overline{\mathbb{F}}_p)$$

sowie aufgrund der Separabilität von $\mathbb{F}_{q'}/\mathbb{F}_q$

$$\#\,\mathrm{Aut}_{\mathbb{F}_q}(\mathbb{F}_{q'}) = [\mathbb{F}_{q'} : \mathbb{F}_q]_s = [\mathbb{F}_{q'} : \mathbb{F}_q] = n.$$

Man betrachte nun den aus 3.1 bekannten *Frobenius-Homomorphismus*

$$\sigma\colon \mathbb{F}_{q'} \longrightarrow \mathbb{F}_{q'}, \qquad a \longmapsto a^p,$$

von $\mathbb{F}_{q'}$; bezüglich der Verträglichkeit von σ mit der Addition siehe 3.1/3. Die r-te Potenz σ^r lässt $\mathbb{F}_q$ invariant und wird der *relative Frobenius-Homomorphismus* über $\mathbb{F}_q$ genannt. Es hat $\sigma^r \in \mathrm{Aut}_{\mathbb{F}_q}(\mathbb{F}_{q'})$ eine Ordnung $\leq n$, denn $a^{(p^{rn})} = a$ für alle $a \in \mathbb{F}_{q'}$. Wäre nun $\mathrm{ord}\,\sigma^r < n$, bzw. $e := \mathrm{ord}\,\sigma < rn$, so wären alle $a \in \mathbb{F}_{q'}$ bereits Nullstelle des Polynoms $X^{(p^e)} - X$, im Widerspruch zu $\#\mathbb{F}_{q'} = p^{rn} > p^e$. Somit haben wir gezeigt, dass $\mathrm{Aut}_{\mathbb{F}_q}(\mathbb{F}_{q'})$ zyklisch von der Ordnung n ist und vom relativen Frobenius-Homomorphismus σ^r erzeugt wird. Mit Korollar 3 ergibt sich deshalb:

Satz 6. *Es sei $\mathbb{F}_q$ ein endlicher Körper, $q = p^r$, sowie $\mathbb{F}/\mathbb{F}_q$ eine endliche Körpererweiterung vom Grad n. Dann ist $\mathrm{Aut}_{\mathbb{F}_q}(\mathbb{F})$ zyklisch von der Ordnung n und wird erzeugt vom relativen Frobenius-Homomorphismus $\mathbb{F} \longrightarrow \mathbb{F}$, $a \longmapsto a^q$.*

Lernkontrolle und Prüfungsvorbereitung

1. Es sei $\mathbb{F}$ ein endlicher Körper. Was versteht man unter dem Primkörper $\mathbb{F}_p$ von $\mathbb{F}$? Was weiß man über die Anzahl der Elemente von $\mathbb{F}$? Wie lässt sich die Erweiterung $\mathbb{F}/\mathbb{F}_p$ charakterisieren?

2. Es sei p eine Primzahl. Für welche Exponenten $n \in \mathbb{N}$ ist der Restklassenring $\mathbb{Z}/p^n\mathbb{Z}$ ein Körper (mit Begründung)?
3. Konstruiere zu einer Primzahl p und einem Exponenten $n > 0$ einen Körper $\mathbb{F}_q$ mit $q = p^n$ Elementen. Wieviele Körper mit q Elementen gibt es (bis auf Isomorphie)?
4. Wähle einen algebraischen Abschluss $\overline{\mathbb{F}}_p$ von $\mathbb{F}_p$ und zeige, dass sich jeder endliche Körper der Charakteristik p mit einem eindeutig bestimmten Teilkörper $\mathbb{F} \subset \overline{\mathbb{F}}_p$ identifizieren lässt. Wann gilt $\mathbb{F} \subset \mathbb{F}'$ für zwei solche endlichen Teilkörper $\mathbb{F} \subset \overline{\mathbb{F}}_p$ und $\mathbb{F}' \subset \overline{\mathbb{F}}_p$?
5. Zeige, dass jede algebraische Erweiterung eines endlichen Körpers normal und separabel ist.
6. Was weiß man über die multiplikative Gruppe $\mathbb{F}^*$ eines endlichen Körpers $\mathbb{F}$?

+7. Gib den Beweis für das Resultat unter Punkt 6.

8. Was versteht man unter dem relativen Frobenius-Homomorphismus über einem endlichen Körper $\mathbb{F}_q$, wobei q eine Primpotenz sei. Bestimme für eine Erweiterung endlicher Körper $\mathbb{F}'_{q'}/\mathbb{F}_q$ die Gruppe aller $\mathbb{F}_q$-Automorphismen von $\mathbb{F}'_{q'}$.

Übungsaufgaben

1. *Überlege, warum die Erweiterungen $\mathbb{F}_p(t)/\mathbb{F}_p(t^p)$ für p prim und t eine Variable die "einfachsten" Beispiele von nicht-separablen Körpererweiterungen sind.*
2. *Es seien $\mathbb{F}, \mathbb{F}'$ Teilkörper eines Körpers L. Überlege, warum $\mathbb{F} = \mathbb{F}'$ gilt, wenn $\mathbb{F}$ und $\mathbb{F}'$ endlich sind und gleich viele Elemente besitzen.*
3. Zeige für p prim und $n \in \mathbb{N} - \{0\}$:
   (i) Ein irreduzibles Polynom $f \in \mathbb{F}_p[X]$ ist genau dann ein Teiler von $X^{p^n} - X$, wenn grad f ein Teiler von n ist.
   (ii) $X^{p^n} - X \in \mathbb{F}_p[X]$ ist das Produkt über alle irreduziblen normierten Polynome $f \in \mathbb{F}_p[X]$ mit der Eigenschaft, dass grad f ein Teiler von n ist.
4. Zeige, dass $\mathbb{F}_{p^\infty} = \bigcup_{n=0}^{\infty} \mathbb{F}_{p^{n!}}$ ein algebraischer Abschluss von $\mathbb{F}_p$ ist.
5. Sei $\overline{\mathbb{F}}_p$ ein algebraischer Abschluss von $\mathbb{F}_p$. Zeige, dass es außer den Potenzen des Frobenius-Homomorphismus noch weitere Automorphismen von $\overline{\mathbb{F}}_p$ gibt. (*Hinweis*: Untersuche für eine Primzahl ℓ zunächst die Automorphismen von $\bigcup_{\nu=0}^{\infty} \mathbb{F}_{q_\nu}$, wobei $q_\nu = p^{\ell^\nu}$.)

3.9 Anfänge der Algebraischen Geometrie*

Bisher haben wir uns nur für Nullstellen von Polynomen einer Variablen interessiert. Im Folgenden wollen wir Nullstellen von Polynomen in mehreren Variablen mit Koeffizienten aus einem Körper K untersuchen und damit einen kleinen Ausblick auf das umfangreiche Gebiet der Algebraischen Geometrie geben; vgl. hierzu auch [3]. Wie der Name schon andeutet, kommen in der Algebraischen Geometrie zusätzlich zu der abstrakt algebraischen Seite geometrische Argumente mit ins Spiel. Dies hängt damit zusammen, dass Nullstellenmengen von Polynomen in mehreren Variablen im Allgemeinen eine komplizierte Struktur tragen und nicht mehr endlich sind.

Es sei im Folgenden $X = (X_1, \ldots, X_n)$ ein System von Variablen sowie $\overline{K}$ ein algebraischer Abschluss des betrachteten Körpers K. Für eine beliebige Teilmenge E des Polynomrings $K[X] = K[X_1, \ldots, X_n]$ bezeichne dann

$$V(E) = \left\{x \in \overline{K}^n \,;\, f(x) = 0 \text{ für alle } f \in E\right\}$$

die Menge der gemeinsamen Nullstellen in $\overline{K}^n$ aller Polynome aus E; wir nennen $V(E)$ eine *über K definierte algebraische Teilmenge* von $\overline{K}^n$. Umgekehrt kann man zu einer Teilmenge $U \subset \overline{K}^n$ das zugehörige Ideal

$$I(U) = \left\{f \in K[X] \,;\, f(U) = 0\right\}$$

aller Polynome f betrachten, die auf U verschwinden. Es ist $I(U)$ ein Ideal in $K[X]$, wie man leicht nachprüft. Auch gilt stets $V(E) = V(\mathfrak{a})$, wenn $\mathfrak{a}$ das von E in $K[X]$ erzeugte Ideal bezeichnet, denn $\mathfrak{a}$ besteht aus allen endlichen Summen der Form $\sum f_i e_i$ mit $f_i \in K[X]$, $e_i \in E$. Die Bildungen $V(\cdot)$ und $I(\cdot)$ erfüllen einige elementare Eigenschaften:

Lemma 1. *Für Ideale $\mathfrak{a}_1, \mathfrak{a}_2$ bzw. eine Familie $(\mathfrak{a}_i)_{i\in I}$ von Idealen in $K[X]$ sowie Teilmengen $U_1, U_2 \subset \overline{K}^n$ gilt*:

(i) $\mathfrak{a}_1 \subset \mathfrak{a}_2 \Longrightarrow V(\mathfrak{a}_1) \supset V(\mathfrak{a}_2)$.
(ii) $U_1 \subset U_2 \Longrightarrow I(U_1) \supset I(U_2)$.
(iii) $V(\sum_i \mathfrak{a}_i) = \bigcap_i V(\mathfrak{a}_i)$.
(iv) $V(\mathfrak{a}_1 \cdot \mathfrak{a}_2) = V(\mathfrak{a}_1 \cap \mathfrak{a}_2) = V(\mathfrak{a}_1) \cup V(\mathfrak{a}_2)$.

Beweis. Die Aussagen (i) bis (iii) sind einfach nachzurechnen; wir zeigen nur, wie man (iv) erhält. Wegen

$$\mathfrak{a}_1 \cdot \mathfrak{a}_2 \subset \mathfrak{a}_1 \cap \mathfrak{a}_2 \subset \mathfrak{a}_i, \qquad i = 1, 2,$$

schließt man mit (i) sofort

$$V(\mathfrak{a}_1 \cdot \mathfrak{a}_2) \supset V(\mathfrak{a}_1 \cap \mathfrak{a}_2) \supset V(\mathfrak{a}_1) \cup V(\mathfrak{a}_2).$$

Sei andererseits $x \in \overline{K}^n - (V(\mathfrak{a}_1) \cup V(\mathfrak{a}_2))$. Für $i = 1, 2$ gibt es dann wegen $x \notin V(\mathfrak{a}_i)$ jeweils ein $f_i \in \mathfrak{a}_i$ mit $f_i(x) \neq 0$. Da $f_1 f_2$ zu $\mathfrak{a}_1 \cdot \mathfrak{a}_2$ gehört, aber $(f_1 f_2)(x) = f_1(x) \cdot f_2(x)$ nicht verschwindet, ergibt sich $x \notin V(\mathfrak{a}_1 \cdot \mathfrak{a}_2)$ bzw.

$$V(\mathfrak{a}_1 \cdot \mathfrak{a}_2) \subset V(\mathfrak{a}_1) \cup V(\mathfrak{a}_2)$$

und damit Aussage (iv). □

Hauptziel dieses Abschnitts ist die Herleitung einiger tieferliegender Eigenschaften der Bildungen $V(\cdot)$ und $I(\cdot)$. Zunächst wollen wir zeigen, dass es zu jeder Teilmenge $E \subset K[X]$ endlich viele Elemente $f_1, \ldots, f_r \in E$ mit $V(E) = V(f_1, \ldots, f_r)$ gibt. Jede über K definierte algebraische Teilmenge von $\overline{K}^n$ ist also als Nullstellengebilde *endlich* vieler Polynome aus $K[X]$ darstellbar. Zur Begründung reicht es, zu zeigen, dass das von E in $K[X]$ erzeugte Ideal $\mathfrak{a}$ bereits endlich erzeugt ist. Ein Ring, in dem jedes Ideal endlich erzeugt ist, wird als *noetherscher Ring* bezeichnet.

Satz 2 (Hilbertscher Basissatz). *Es sei R ein noetherscher Ring. Dann ist auch der Polynomring $R[Y]$ in einer Variablen Y noethersch. Insbesondere ist der Polynomring $K[X] = K[X_1, \ldots, X_n]$ in endlich vielen Variablen über einem Körper K noethersch.*

In 2.4/8 hatten wir einen Ring R als noethersch bezeichnet, wenn jede aufsteigende Kette von Idealen $\mathfrak{a}_1 \subset \mathfrak{a}_2 \subset \ldots \subset R$ nach endlich vielen Schritten stationär wird. Wir wollen zunächst zeigen, dass diese Bedingung äquivalent dazu ist, dass jedes Ideal in R endlich erzeugt ist. Zu einer Kette der genannten Art betrachte man nämlich das Ideal $\mathfrak{a} = \bigcup_i \mathfrak{a}_i$. Besitzt dieses ein endliches Erzeugendensystem $f_1, \ldots, f_r$, so sind alle f_ρ und damit $\mathfrak{a}$ bereits in einem der $\mathfrak{a}_i$ enthalten. Die Idealkette ist daher ab dieser Stelle stationär. Ist umgekehrt $\mathfrak{a} \subset R$ ein Ideal, welches nicht endlich erzeugt ist, so gilt für endlich viele Elemente $f_1, \ldots, f_r \in \mathfrak{a}$ stets $(f_1, \ldots, f_r) \neq \mathfrak{a}$, d. h. man kann in $\mathfrak{a}$ mit einer induktiven Konstruktion eine unendliche echt aufsteigende Kette von Idealen finden.

Beweis zu Satz 2. Es sei R ein noetherscher Ring und $\mathfrak{a} \subset R[Y]$ ein Ideal. Für $i \in \mathbb{N}$ definiere man $\mathfrak{a}_i \subset R$ als Menge aller Elemente $a \in R$, so dass es ein Polynom der Form

$$aY^i + \text{ Terme niedrigeren Grades in } Y$$

in $\mathfrak{a}$ gibt. Man verifiziert ohne Schwierigkeiten, dass jedes $\mathfrak{a}_i$ ein Ideal in R ist und dass man eine aufsteigende Kette

$$\mathfrak{a}_0 \subset \mathfrak{a}_1 \subset \ldots \subset R$$

erhält; für $f \in \mathfrak{a}$ gilt nämlich auch $Yf \in \mathfrak{a}$. Da der Ring R noethersch ist, wird diese Kette stationär, etwa an der Stelle des Ideals $\mathfrak{a}_{i_0}$. Für $i = 0, \ldots, i_0$ wähle man nun Polynome $f_{ij} \in \mathfrak{a}$ mit $\operatorname{grad} f_{ij} = i$, so dass für festes i die höchsten Koeffizienten a_{ij} der f_{ij} jeweils das Ideal $\mathfrak{a}_i$ erzeugen. Wir behaupten, dass die Polynome f_{ij} das Ideal $\mathfrak{a}$ erzeugen. Sei also $g \in \mathfrak{a}$, wobei wir $g \neq 0$ annehmen dürfen. Weiter sei $d = \operatorname{grad} g$ und $a \in R$ der höchste Koeffizient von g; man setze $i = \min\{d, i_0\}$. Es gilt dann $a \in \mathfrak{a}_i$, und man hat folglich eine Darstellung

$$a = \sum_j c_j a_{ij}, \qquad c_j \in R.$$

Das Polynom

$$g_1 = g - Y^{d-i} \cdot \sum_j c_j f_{ij}$$

gehört wieder zu $\mathfrak{a}$, sein Grad ist aber kleiner als der Grad d von g, da der Koeffizient von Y^d nunmehr verschwindet. Für $g_1 \neq 0$ lässt sich das Verfahren mit g_1 anstelle von g fortsetzen usw. Auf diese Weise gelangt man nach endlich vielen Schritten zu einem Polynom g_s mit $g_s = 0$. Es folgt, dass g eine Linearkombination der f_{ij} mit Koeffizienten in $R[Y]$ ist. Also erzeugen die f_{ij} das Ideal $\mathfrak{a}$. □

Zu einem Ideal $\mathfrak{a}$ eines Ringes R kann man stets sein *Radikal*

$$\operatorname{rad} \mathfrak{a} = \left\{a \in R;\ \text{es existiert ein } n \in \mathbb{N} \text{ mit } a^n \in \mathfrak{a}\right\}$$

bilden. Unter Anwendung der binomischen Formel sieht man leicht, dass das Radikal von $\mathfrak{a}$ wieder ein Ideal in R ist. Ideale mit der Eigenschaft $\mathfrak{a} = \operatorname{rad} \mathfrak{a}$

heißen *reduziert*. Für jede Teilmenge $U \subset \overline{K}^n$ ist das Ideal $I(U) \subset K[X]$ reduziert; denn ein Polynom $f \in K[X]$ verschwindet genau dann in einem Punkt $x \in \overline{K}^n$, wenn irgendeine Potenz f^r mit $r > 0$ dort verschwindet. Wir wollen etwas genauer die Korrespondenz zwischen Idealen in $K[X]$ und algebraischen Mengen in $\overline{K}^n$ untersuchen.

Satz 3. *Die Zuordnungen $I(\cdot)$ und $V(\cdot)$ definieren zueinander inverse, inklusionsumkehrende Bijektionen*

$$\big\{\text{algebraische Teilmengen} \subset \overline{K}^n\big\} \underset{V}{\overset{I}{\rightleftarrows}} \big\{\text{reduzierte Ideale} \subset K[X]\big\},$$

wobei auf der linken Seite genauer über K definierte algebraische Teilmengen von $\overline{K}^n$ gemeint sind.

Zum *Beweis* sind die beiden Beziehungen

$$V\big(I(U)\big) = U, \qquad I\big(V(\mathfrak{a})\big) = \mathfrak{a},$$

für algebraische Teilmengen $U \subset \overline{K}^n$ bzw. reduzierte Ideale $\mathfrak{a} \subset K[X]$ zu zeigen. Die erste Gleichung ist elementarer Natur. Gelte etwa $U = V(\mathfrak{a})$ für ein Ideal $\mathfrak{a} \subset K[X]$. Zu zeigen ist $V(I(V(\mathfrak{a}))) = V(\mathfrak{a})$. Da alle Polynome aus $\mathfrak{a}$ auf $V(\mathfrak{a})$ verschwinden, folgt $\mathfrak{a} \subset I(V(\mathfrak{a}))$ und somit $V(\mathfrak{a}) \supset V(I(V(\mathfrak{a})))$. Andererseits verschwinden alle Polynome aus $I(V(\mathfrak{a}))$ auf $V(\mathfrak{a})$, man hat also $V(\mathfrak{a}) \subset V(I(V(\mathfrak{a})))$ bzw. $V(I(V(\mathfrak{a}))) = V(\mathfrak{a})$. Die Gleichung $I(V(\mathfrak{a})) = \mathfrak{a}$ schließlich ist Konsequenz des sogenannten *Hilbertschen Nullstellensatzes*:

Theorem 4 (Hilbertscher Nullstellensatz). *Es sei $\mathfrak{a}$ ein Ideal des Polynomrings $K[X] = K[X_1, \ldots, X_n]$ und $V(\mathfrak{a})$ die Menge der Nullstellen von $\mathfrak{a}$ in $\overline{K}^n$. Dann gilt $I(V(\mathfrak{a})) = \operatorname{rad} \mathfrak{a}$. Mit anderen Worten, ein Polynom $f \in K[X]$ verschwindet genau dann auf $V(\mathfrak{a})$, wenn eine Potenz f^r zu $\mathfrak{a}$ gehört.*

Wir leiten zunächst ein Lemma her, das man auch als schwache Form des Hilbertschen Nullstellensatzes bezeichnet.

Lemma 5. *Es sei $A = K[x_1, \ldots, x_n] \neq 0$ ein Ring von endlichem Typ über einem Körper K. Dann setzt sich die Inklusion $K \hookrightarrow \overline{K}$ zu einem K-Homomorphismus $A \longrightarrow \overline{K}$ fort.*

Beweis. Man wähle ein maximales Ideal $\mathfrak{m} \subset A$ und betrachte die kanonische Abbildung $K \longrightarrow A/\mathfrak{m}$. Da es sich bei $A/\mathfrak{m}$ um einen Körper handelt, der über K im ringtheoretischen Sinne von endlichem Typ ist, sieht man mit 3.3/8, dass $A/\mathfrak{m}$ eine endliche Körpererweiterung von K ist. Nach 3.4/9 gibt es dann einen K-Homomorphismus $A/\mathfrak{m} \longrightarrow \overline{K}$, und die Komposition der Projektion $A \longrightarrow A/\mathfrak{m}$ mit dieser Abbildung ergibt den gewünschten K-Homomorphismus von A nach $\overline{K}$. □

Nun zum *Beweis* von Theorem 4. Da alle Polynome aus $\mathfrak{a}$ auf $V(\mathfrak{a})$ verschwinden, gilt $\mathfrak{a} \subset I(V(\mathfrak{a}))$, und es folgt sogar $\operatorname{rad}\mathfrak{a} \subset I(V(\mathfrak{a}))$, da Ideale des Typs $I(U)$ reduziert sind. Wir nehmen an, dass es ein $f \in I(V(\mathfrak{a}))$ gibt mit $f^r \notin \mathfrak{a}$ für alle $r \in \mathbb{N}$. Dann hat das multiplikative System $S = \{1, f, f^2, \ldots\}$ einen leeren Schnitt mit $\mathfrak{a}$. Aufgrund des Zornschen Lemmas 3.4/5 (oder, alternativ, da $K[X]$ noethersch ist) existiert ein Ideal $\mathfrak{p} \subset K[X]$, welches maximal unter allen Idealen $\mathfrak{q} \subset K[X]$ ist, für die $\mathfrak{a} \subset \mathfrak{q}$ und $\mathfrak{q} \cap S = \emptyset$ gilt. Es ist $\mathfrak{p}$ ein Primideal. Seien nämlich $a, b \in K[X] - \mathfrak{p}$. Nach Definition von $\mathfrak{p}$ müssen die Ideale $(a, \mathfrak{p})$ und $(b, \mathfrak{p})$, die von a und $\mathfrak{p}$ bzw. b und $\mathfrak{p}$ in $K[X]$ erzeugt werden, jeweils einen nicht-leeren Schnitt mit S haben, so dass

$$S \cap (ab, \mathfrak{p}) \supset S \cap \big((a, \mathfrak{p}) \cdot (b, \mathfrak{p})\big) \neq \emptyset$$

gilt. Es folgt $ab \notin \mathfrak{p}$, d. h. $\mathfrak{p}$ ist ein Primideal.

Wir betrachten nun $A = K[X]/\mathfrak{p}$ als Ringerweiterung von endlichem Typ über K. Es sei $\tilde{f} \in A$ die Restklasse von f. Da $f \notin \mathfrak{p}$ nach Wahl von $\mathfrak{p}$ und da A ein Integritätsring ist, können wir im Quotientenkörper $Q(A)$ den Unterring $A[\tilde{f}^{-1}]$ definieren. Nach Lemma 5 gibt es einen K-Homomorphismus $A[\tilde{f}^{-1}] \longrightarrow \overline{K}$, so dass wir durch Komposition mit kanonischen Abbildungen insgesamt einen K-Homomorphismus

$$\varphi\colon K[X] \longrightarrow A \hookrightarrow A[\tilde{f}^{-1}] \longrightarrow \overline{K}$$

erhalten. Wir können φ als denjenigen Homomorphismus ansehen, der Polynome aus $K[X]$ im Punkt $x = (\varphi(X_1), \ldots, \varphi(X_n)) \in \overline{K}^n$ auswertet. Da nach Konstruktion $\mathfrak{a} \subset \mathfrak{p} \subset \ker\varphi$ gilt, hat man $x \in V(\mathfrak{a})$. Andererseits kann aber $f(x) = \varphi(f)$ als Bild der Einheit $\tilde{f} \in A[\tilde{f}^{-1}]$ nicht verschwinden, im Widerspruch zu $f \in I(V(\mathfrak{a}))$. Folglich ist die Annahme, dass keine Potenz von f zu $\mathfrak{a}$ gehört, nicht haltbar. □

Im Falle eines algebraisch abgeschlossenen Körpers K besitzen die durch maximale Ideale $\mathfrak{m} \subset K[X]$ definierten algebraischen Teilmengen von K^n eine besonders einfache Gestalt:

Korollar 6. *Sei K ein algebraisch abgeschlossener Körper. Ein Ideal $\mathfrak{m}$ des Polynomrings $K[X] = K[X_1, \ldots, X_n]$ ist genau dann maximal, wenn es von der Form $\mathfrak{m} = (X_1 - x_1, \ldots, X_n - x_n)$ mit einem Punkt $x = (x_1, \ldots, x_n) \in K^n$ ist. Insbesondere gilt dann $V(\mathfrak{m}) = \{x\}$ und $I(x) = \mathfrak{m}$.*

Ist K also algebraisch abgeschlossen, so entsprechen die maximalen Ideale in $K[X]$ unter der in Satz 3 beschriebenen Korrespondenz genau den Punkten von K^n.

Beweis. Es ist $(X_1, \ldots, X_n) \subset K[X]$ ein maximales Ideal, da der Restklassenring $K[X]/(X_1, \ldots, X_n)$ isomorph zu K ist. Mit einer Variablentransformation erkennt man, dass Ideale des Typs $(X_1 - x_1, \ldots, X_n - x_n) \subset K[X]$ mit $x = (x_1, \ldots, x_n) \in K^n$ ebenfalls maximal sind. Sei nun umgekehrt ein maximales Ideal $\mathfrak{m} \subset K[X]$ gegeben. Nach Lemma 5 gibt es einen K-Homomorphismus $K[X]/\mathfrak{m} \longrightarrow K$, der dann notwendig ein Isomorphismus ist, da $K[X]/\mathfrak{m}$ bereits eine Körpererweiterung von K ist. Wir erhalten also einen Epimorphismus $K[X] \longrightarrow K$ mit Kern $\mathfrak{m}$. Sei jeweils $x_i \in K$ das Bild von X_i. Dann gilt $X_i - x_i \in \mathfrak{m}$ für alle i, und es folgt, da $(X_1 - x_1, \ldots, X_n - x_n)$ maximal in $K[X]$ ist, dass dieses Ideal mit $\mathfrak{m}$ übereinstimmt. Die restlichen Behauptungen ergeben sich nun leicht aus der gerade beschriebenen Charakterisierung der maximalen Ideale in $K[X]$. □

Für einen nicht notwendig algebraisch abgeschlossenen Körper K kann man zeigen, dass ein Ideal in $K[X]$ genau dann maximal ist, wenn es die Gestalt $I(\{x\})$ mit einem Punkt $x \in \overline{K}^n$ hat, vgl. Aufgabe 2. Allerdings ist $\{x\}$ nicht notwendig eine über K definierte algebraische Menge in $\overline{K}^n$. Auch ist x im Allgemeinen nicht eindeutig durch das zugehörige maximale Ideal $I(\{x\}) \subset K[X]$ bestimmt. Beispielsweise überführt jeder K-Automorphismus $\sigma\colon \overline{K} \longrightarrow \overline{K}$ den Punkt $x = (x_1, \ldots, x_n)$ in einen Punkt $\sigma(x) := (\sigma(x_1), \ldots, \sigma(x_n))$, für den dann $I(\{x\}) = I(\{\sigma(x)\})$ gilt. Die kleinste über K definierte algebraische Menge in $\overline{K}^n$, die x enthält, ist $V(I\{x\})$, und man kann zeigen, dass dies die Menge aller $\sigma(x)$ ist, wobei σ die K-Automorphismen von $\overline{K}$ durchläuft.

Betrachtet man die Polynome aus $K[X]$ als $\overline{K}$-wertige Funktionen auf $\overline{K}^n$, so kann man diese bei Vorgabe eines Ideals $\mathfrak{a} \subset K[X]$ einschränken auf die algebraische Menge $V(\mathfrak{a})$. Dieser Einschränkungsprozess definiert einen Ringhomomorphismus $K[X] \longrightarrow \mathrm{Abb}(V(\mathfrak{a}), \overline{K})$, dessen Kern das Ideal $\mathfrak{a}$ enthält. Somit lassen sich die Elemente des Restklassenrings $K[X]/\mathfrak{a}$ in kanonischer Weise als "Funktionen" auf $V(\mathfrak{a})$ auffassen; man nennt $K[X]/\mathfrak{a}$ auch den zu $\mathfrak{a}$ gehörigen Ring *polynomialer Funktionen* auf der algebraischen Menge $V(\mathfrak{a})$. Bei dieser Sicht ist jedoch etwas Vorsicht geboten, denn die Abbildung $K[X]/\mathfrak{a} \longrightarrow \mathrm{Abb}(V(\mathfrak{a}), \overline{K})$ wird im Allgemeinen nicht injektiv sein. Nilpotente Elemente aus $K[X]/\mathfrak{a}$ induzieren beispielsweise stets die Nullfunktion auf $V(\mathfrak{a})$, und man folgert aus dem Hilbertschen Nullstellensatz, dass dies auch die einzigen Elemente in $K[X]/\mathfrak{a}$ mit dieser Eigenschaft sind. Der Kern der Abbildung $K[X] \longrightarrow \mathrm{Abb}(V(\mathfrak{a}), \overline{K})$ ist nämlich das Ideal $\operatorname{rad}\mathfrak{a}$, womit sich der Kern der induzierten Abbildung $K[X]/\mathfrak{a} \longrightarrow \mathrm{Abb}(V(\mathfrak{a}), \overline{K})$ als das Radikal des Nullideals in $K[X]/\mathfrak{a}$ ergibt. Letzteres besteht aus allen nilpotenten Elementen von $K[X]/\mathfrak{a}$.

Lernkontrolle und Prüfungsvorbereitung

K sei ein Körper, $\overline{K}$ ein algebraischer Abschluss von K und $X = (X_1, \ldots, X_n)$ ein System von Variablen.

1. Was versteht man unter einer über K definierten algebraischen Teilmenge von $\overline{K}^n$, was unter dem zugehörigen Ideal in $K[X]$? Erkläre die Zuordnungen $V(\cdot)$ und $I(\cdot)$.
2. Welche allgemeinen Eigenschaften gelten für die Zuordnungen $V(\cdot)$ und $I(\cdot)$?
3. Wie lautet der Hilbertsche Basissatz?

$^+$4. Skizziere den Beweis des Hilbertschen Basissatzes.

5. Definiere das Radikal $\operatorname{rad}\mathfrak{a}$ eines Ideals $\mathfrak{a}$ in einem Ring R und zeige, dass dies wiederum ein Ideal in R ist.
6. Wie lautet der Hilbertsche Nullstellensatz?
7. Was versteht man unter der schwachen Form des Hilbertschen Nullstellensatzes?

$^+$8. Skizziere den Beweis des Hilbertschen Nullstellensatzes.

9. Welche fundamentale Beziehung besteht zwischen den Zuordnungen $V(\cdot)$ und $I(\cdot)$? Erkläre die zugehörigen Beweise.

10. Bestimme für einen algebraisch abgeschlossenen Körper K die Struktur der maximalen Ideale im Polynomring $K[X_1, \ldots, X_n]$.

Übungsaufgaben

Betrachte weiterhin einen Körper K, einen zugehörigen algebraischen Abschluss $\overline{K}$, sowie ein System von Variablen $X = (X_1, \ldots, X_n)$.

1. *Für Teilmengen $E \subset K[X]$ und $U \subset K^n$ sei definiert*:

$$V_K(E) = \{x \in K^n \,;\, f(x) = 0 \text{ für alle } f \in E\},$$
$$I(U) = \{f \in K[X] \,;\, f(U) = 0\}.$$

Überlege, welche der Resultate aus diesem Abschnitt gültig bleiben und welche nicht, wenn man Nullstellen von Polynomen $f \in K[X]$ lediglich in K^n und nicht in $\overline{K}^n$ betrachtet, also die Bildung $V_K(\cdot)$ anstelle von $V(\cdot)$ benutzt.

2. Betrachte zu Punkten $x \in \overline{K}^n$ jeweils den Einsetzungshomomorphismus $h_x \colon K[X] \longrightarrow \overline{K}$, $f \longmapsto f(x)$. Zeige, dass die Ideale des Typs $\ker h_x$ gerade die maximalen Ideale in $K[X]$ sind.

3. Sei $\mathfrak{m} \subset K[X]$ ein maximales Ideal. Zeige: Es gilt $\mathfrak{m} = (f_1, \ldots, f_n)$ mit Polynomen $f_1, \ldots, f_n$, wobei f_i jeweils ein normiertes Polynom in X_i mit Koeffizienten in $K[X_1, \ldots, X_{i-1}]$ ist.

4. Es sei $U \subset \overline{K}^n$ eine über K definierte algebraische Teilmenge. Man nennt U *irreduzibel* über K, wenn es keine Zerlegung $U = U_1 \cup U_2$ mit über K definierten algebraischen Teilmengen $U_1, U_2 \subsetneq U$ gibt. Zeige:
   (i) $U \subset \overline{K}^n$ ist genau dann irreduzibel über K, wenn das zugehörige Ideal $I(U) \subset K[X]$ prim ist.
   (ii) Es existiert eine Zerlegung $U = U_1 \cup \ldots \cup U_r$ von U in irreduzible über K definierte algebraische Teilmengen. Für unverkürzbare Zerlegungen sind die $U_1, \ldots, U_r$ eindeutig bestimmt, abgesehen von der Reihenfolge.

5. Es sei A eine K-Algebra von endlichem Typ. Zeige, dass A ein *Jacobson-Ring* ist, d. h. dass jedes reduzierte Ideal $\mathfrak{a} \subsetneq A$ Durchschnitt maximaler Ideale ist.

4. Galois-Theorie

Überblick und Hintergrund

In Kapitel 3 haben wir gesehen, dass zu einem Körper K stets ein algebraischer Abschluss $\overline{K}$ existiert und dass dieser bis auf K-Isomorphie eindeutig bestimmt ist. Gehen wir daher von einer algebraischen Gleichung $f(x) = 0$ mit einem nicht-konstanten Polynom $f \in K[X]$ aus, so zerfällt f über $\overline{K}$ vollständig in Linearfaktoren, und man kann sagen, dass $\overline{K}$ "sämtliche" Lösungen der algebraischen Gleichung $f(x) = 0$ enthält. Der Teilkörper $L \subset \overline{K}$, der über K von allen diesen Lösungen erzeugt wird, ist ein Zerfällungskörper von f, wobei die Erweiterung L/K endlich sowie gemäß 3.5/5 normal ist. Ersatzweise können wir einen Zerfällungskörper L zu f auch mit Hilfe des Verfahrens von Kronecker konstruieren, indem wir sukzessive alle Lösungen von $f(x) = 0$ zu K adjungieren. Die Struktur der Erweiterung L/K ist zu klären, wenn man Aussagen über die "Natur" der Lösungen von $f(x) = 0$ machen möchte, z. B. wenn man die Gleichung, wie in der Einführung angesprochen, durch Radikale auflösen möchte.

An dieser Stelle setzt nun die Galois-Theorie mit ihren gruppentheoretischen Begriffsbildungen ein. Und zwar betrachtet man die Gruppe $\mathrm{Aut}_K(L)$ aller K-Automorphismen von L, wobei weiterhin L ein Zerfällungskörper des Polynoms $f \in K[X]$ sei. Ist L/K separabel und damit eine *Galois-Erweiterung*, so bezeichnet man $\mathrm{Aut}_K(L)$ auch als *Galois-Gruppe* zu L/K und schreibt hierfür $\mathrm{Gal}(L/K)$. Jeder K-Automorphismus $L \longrightarrow L$ induziert eine bijektive Selbstabbildung auf der Menge der Nullstellen von f und ist durch die Bilder dieser Nullstellen auch eindeutig bestimmt. Man kann

S. Bosch, *Algebra*, https://doi.org/10.1007/978-3-662-67464-2_5

daher die Elemente von $\mathrm{Aut}_K(L)$ mit den entsprechenden Permutationen der Nullstellen von f identifizieren. Fasst man $\overline{K}$ als algebraischen Abschluss von L auf, so wird mit 3.5/4 klar, dass man $\mathrm{Aut}_K(L)$ auch als Menge aller K-Homomorphismen $L \longrightarrow \overline{K}$ interpretieren kann, wobei sich diese Homomorphismen mit Hilfe der Resultate 3.4/8 und 3.4/9 in konkreter Weise beschreiben lassen. Man nehme beispielsweise an, dass f keine mehrfachen Nullstellen hat oder, allgemeiner, dass L als Zerfällungskörper von f separabel über K ist. Dann ist die Erweiterung L/K aufgrund des Satzes vom primitiven Element 3.6/12 einfach, etwa $L = K(\alpha)$, und das Minimalpolynom $g \in K[X]$ zu α zerfällt nach 3.5/4 über L vollständig in Linearfaktoren. Für die zugehörigen Nullstellen $\alpha_1, \ldots, \alpha_n \in L$ gilt jeweils $L = K(\alpha_i)$, und es gibt nach 3.4/8 zu jedem i einen eindeutig bestimmten Automorphismus $\sigma_i \in \mathrm{Aut}_K(L)$ mit $\sigma_i(\alpha) = \alpha_i$, den wir durch $h(\alpha) \longmapsto h(\alpha_i)$ für Polynome $h \in K[X]$ beschreiben können. Die Galois-Gruppe $\mathrm{Gal}(L/K)$ besteht dann aus den Elementen $\sigma_1, \ldots, \sigma_n$, wobei deren Anzahl n gleich dem Grad von g bzw. dem Grad der Erweiterung L/K ist. In dieser konkreten Weise hat bereits Galois die nach ihm benannten Gruppen eingeführt.

Als erstes grundlegendes Resultat der Galois-Theorie beweisen wir in Abschnitt 4.1 den sogenannten *Hauptsatz der Galois-Theorie*. Er besagt für eine endliche Galois-Erweiterung L/K, dass die Untergruppen H der zugehörigen Galois-Gruppe $\mathrm{Gal}(L/K)$ mittels $H \longmapsto L^H$ bzw. $E \longmapsto \mathrm{Aut}_E(L)$ in bijektiver Weise den Zwischenkörpern E von L/K entsprechen; dabei sei $L^H \subset L$ der Teilkörper derjenigen Elemente, die unter allen Automorphismen aus H invariant sind. Weiter ist ein Zwischenkörper E zu L/K genau dann normal über K, wenn $\mathrm{Aut}_E(L)$ als Untergruppe von $\mathrm{Gal}(L/K)$ ein Normalteiler ist. Man kann daher die Galois-Gruppe $\mathrm{Gal}(L/K)$ in gewisser Weise als ein Abbild der Erweiterung L/K ansehen. Insbesondere reduziert sich das Problem, alle Zwischenkörper zu L/K zu bestimmen, auf das prinzipiell einfachere Problem, die Untergruppen von $\mathrm{Gal}(L/K)$ zu bestimmen.

In Abschnitt 4.2 verallgemeinern wir den Hauptsatz der Galois-Theorie auf nicht notwendig endliche Galois-Erweiterungen, indem wir Galois-Gruppen nach W. Krull als topologische Gruppen interpretieren und hier speziell die *abgeschlossenen* Untergruppen betrachten. Insbesondere bestimmen wir in diesem Abschnitt die absolute Galois-Gruppe $\mathrm{Gal}(\overline{\mathbb{F}}/\mathbb{F})$ eines endlichen Körpers $\mathbb{F}$, wobei $\overline{\mathbb{F}}$ ein algebraischer Abschluss zu $\mathbb{F}$ sei. In 4.3 schließlich zeigen wir an einigen Beispielen, wie die Galois-Gruppe

einer algebraischen Gleichung in konkreten Fällen bestimmt werden kann. Hier beweisen wir auch, dass die allgemeine Gleichung n-ten Grades die volle Permutationsgruppe $\mathfrak{S}_n$ als Galois-Gruppe besitzt. Die zugehörige Problemstellung leitet über zum Hauptsatz über symmetrische Polynome, den wir in einer ersten Version in 4.3/5 sowie in detaillierterer Weise in 4.4/1 herleiten. Als Anwendung gehen wir auf die Diskriminante eines Polynoms f ein, deren Wert anzeigt, ob f eine mehrfache Nullstelle hat oder nicht. In diesem Zusammenhang behandeln wir als mögliches Hilfsmittel zur Berechnung der Diskriminante auch die Resultante zweier Polynome.

Die Abschnitte 4.5 – 4.8 dienen im Wesentlichen dazu, die Charakterisierung der Auflösbarkeit algebraischer Gleichungen vorzubereiten, wobei eine abschließende Behandlung allerdings erst in Kapitel 6 erfolgen wird. Wir untersuchen in 4.5 und 4.8 sogenannte *Radikalerweiterungen*, d. h. Erweiterungen, die durch Adjunktion von Lösungen reiner Gleichungen des Typs $x^n - c = 0$ entstehen. Im Falle $c = 1$ handelt es sich um die Adjunktion von n-ten *Einheitswurzeln*, also n-ter Wurzeln der 1, sowie ansonsten, wenn man voraussetzt, dass der Koeffizientenkörper K die n-ten Einheitswurzeln bereits enthält, um das Studium *zyklischer Erweiterungen*, d. h. von Galois-Erweiterungen mit zyklischer Galois-Gruppe. Gewisse Modifikationen sind zu berücksichtigen, wenn die Charakteristik des betrachteten Körpers K ein Teiler von n ist. Als Hilfsmittel beweisen wir in 4.6 den Satz über die *lineare Unabhängigkeit von Charakteren* und studieren anschließend in 4.7 die *Norm* und *Spur* von endlichen Körpererweiterungen. E. Artin hat diese Techniken aus der Linearen Algebra zur Grundlage seines Aufbaus der Galois-Theorie gemacht, vgl. [1] und [2], wohingegen wir in Abschnitt 4.1 einen mehr konventionellen Zugang gewählt haben.

In den Abschnitten 4.9 und 4.10 verallgemeinern wir die Charakterisierung zyklischer Erweiterungen auf gewisse Klassen abelscher Erweiterungen. Es handelt sich um die nach E. Kummer benannte Theorie der *Kummer-Erweiterungen* zu einem gegebenen Exponenten n. In 4.9 nehmen wir zunächst an, dass die Charakteristik des betrachteten Körpers kein Teiler von n ist; dies ist der einfachste Fall. Anschließend entwickeln wir in 4.10 die Kummer-Theorie mehr von einem axiomatischen Standpunkt aus und wenden sie insbesondere an, um für $p = \operatorname{char} K > 0$ Kummer-Erweiterungen zu einem Exponenten der Form p^r zu studieren. Als wesentliches Hilfsmittel führen wir dazu den auf E. Witt zurückgehenden Kalkül der *Witt-Vektoren* ein.

Wir beschließen das Kapitel in 4.11 mit einem Beispiel aus der Descent-Theorie. Es geht hier für eine endliche Galois-Erweiterung L/K darum, in der Art des Hauptsatzes der Galois-Theorie K-Vektorräume mittels Invariantenbildung durch L-Vektorräume mit zugehörigen "Galois-Automorphismen" zu beschreiben.

4.1 Galois-Erweiterungen

In 3.5 hatten wir eine algebraische Körpererweiterung L/K normal genannt, wenn L Zerfällungskörper einer Familie von Polynomen aus $K[X]$ ist oder, in äquivalenter Weise, wenn jedes irreduzible Polynom aus $K[X]$, welches in L eine Nullstelle besitzt, über L vollständig in Linearfaktoren zerfällt, vgl. 3.5/4 (ii) und (iii). Im Weiteren wird die noch verbleibende charakterisierende Eigenschaft 3.5/4 (i) für normale Erweiterungen eine tragende Rolle spielen: Nach Wahl eines algebraischen Abschlusses $\overline{L}$ von L beschränkt sich jeder K-Homomorphismus $L \longrightarrow \overline{L}$ zu einem Automorphismus von L. Indem wir $\overline{L}$ als algebraischen Abschluss $\overline{K}$ von K auffassen, können wir also die Menge $\mathrm{Hom}_K(L, \overline{K})$ aller K-Homomorphismen von L nach $\overline{K}$ mit der Gruppe $\mathrm{Aut}_K(L)$ der K-Automorphismen von L identifizieren. In diesem Zusammenhang sei erwähnt, dass man zwei Elemente $a, b \in L$ als (*über K*) *konjugiert* bezeichnet, wenn es einen Automorphismus $\sigma \in \mathrm{Aut}_K(L)$ mit $\sigma(a) = b$ gibt; wir werden diese Terminologie jedoch nur selten benutzen.

Definition 1. *Eine algebraische Körpererweiterung L/K heißt* galoissch *bzw. eine* Galois-Erweiterung, *wenn sie normal und separabel ist. Die Automorphismengruppe* $\mathrm{Gal}(L/K) := \mathrm{Aut}_K(L)$ *wird dann als die* Galois-Gruppe *der Galois-Erweiterung L/K bezeichnet.*

Normale Körpererweiterungen werden in der Literatur teilweise auch als *quasi-galoissche* Erweiterungen bezeichnet. Bildet man über einem Körper K den Zerfällungskörper eines separablen Polynoms mit Koeffizienten aus K, so erhält man ein Beispiel für eine endliche Galois-Erweiterung. Weiter haben wir in 3.8/4 gesehen, dass jede algebraische Erweiterung $\mathbb{F}/\mathbb{F}_q$ eines endlichen Körpers $\mathbb{F}_q$ eine Galois-Erweiterung ist; q sei eine Primpotenz. Für eine *endliche* Erweiterung $\mathbb{F}/\mathbb{F}_q$ ist die zugehörige Galois-Gruppe $\mathrm{Gal}(\mathbb{F}/\mathbb{F}_q)$ zyklisch von der Ordnung $n = [\mathbb{F} : \mathbb{F}_q]$ und wird von

dem relativen Frobenius-Homomorphismus $\mathbb{F} \longrightarrow \mathbb{F}$, $a \longmapsto a^q$ erzeugt; vgl. 3.8/6.

Bemerkung 2. *Es sei L/K eine Galois-Erweiterung und E ein Zwischenkörper zu L/K. Dann gilt*:

(i) *Die Erweiterung L/E ist galoissch, und die zugehörige Galois-Gruppe* $\mathrm{Gal}(L/E)$ *ist in natürlicher Weise eine Untergruppe von* $\mathrm{Gal}(L/K)$.

(ii) *Ist auch E/K galoissch, so beschränkt sich jeder K-Automorphismus von L zu einem K-Automorphismus von E, und die Abbildung* $\mathrm{Gal}(L/K) \longrightarrow \mathrm{Gal}(E/K)$, $\sigma \longmapsto \sigma|_E$, *ist ein surjektiver Gruppenhomomorphismus mit Kern* $\mathrm{Gal}(L/E)$, *induziert also einen Isomorphismus*

$$\mathrm{Gal}(L/K)\big/\,\mathrm{Gal}(L/E) \xrightarrow{\sim} \mathrm{Gal}(E/K).$$

Insbesondere ist $\mathrm{Gal}(L/E)$ *in diesem Falle ein Normalteiler in* $\mathrm{Gal}(L/K)$.

Beweis. Es folgt mit 3.5/6 und 3.6/11, dass die Erweiterung L/E galoissch ist. Da jeder E-Automorphismus von L insbesondere ein K-Automorphismus ist, erkennt man $\mathrm{Gal}(L/E)$ als Untergruppe von $\mathrm{Gal}(L/K)$. Ist nun auch E/K galoissch, so beschränkt sich jeder K-Automorphismus von L nach 3.5/4 (i) zu einem K-Automorphismus von E. Auf diese Weise erhält man einen Gruppenhomomorphismus $\mathrm{Gal}(L/K) \longrightarrow \mathrm{Gal}(E/K)$ mit Kern $\mathrm{Gal}(L/E)$, der gemäß 3.4/9 surjektiv ist; man benutze dabei, dass L/K normal ist. Weiter sieht man, dass $\mathrm{Gal}(L/E)$ als Kern eines Gruppenhomomorphismus ein Normalteiler in $\mathrm{Gal}(L/K)$ ist. □

Als Nächstes wollen wir die Automorphismengruppe einer normalen Körpererweiterung mit der Definition des Separabilitätsgrads in Verbindung bringen.

Bemerkung 3. *Für eine normale Körpererweiterung L/K gilt*

$$\mathrm{ord}\,\mathrm{Aut}_K(L) = [L : K]_s \leq [L : K].$$

Ist die Erweiterung L/K endlich, so besteht in vorstehender Abschätzung genau dann Gleichheit, also $\mathrm{ord}\,\mathrm{Aut}_K(L) = [L : K]$, *wenn L/K separabel ist.*

Beweis. Der Separabilitätsgrad $[L : K]_s$ ist gemäß 3.6/5 definiert als Anzahl der K-Homomorphismen $L \longrightarrow \overline{K}$ in einen algebraischen Abschluss $\overline{K}$ von

K bzw. L. Da L/K als normal vorausgesetzt ist, beschränken sich alle diese Homomorphismen zu K-Automorphismen von L, vgl. 3.5/4, und wir erhalten die Beziehung $\operatorname{ord} \operatorname{Aut}_K(L) = [L : K]_s$. Gemäß 3.6/8 gilt weiter $[E : K]_s \leq [E : K]$ für Zwischenkörper E zu L/K, die endlich über K sind. Indem man L/K gegebenenfalls durch Zwischenkörper dieses Typs ausschöpft, folgert man $[L : K]_s \leq [L : K]$. Ist schließlich L/K endlich, so wende man 3.6/9 an, um zu sehen, dass $[L : K]_s = [L : K]$ äquivalent zur Separabilität von L/K ist. □

Eine wichtige Eigenschaft von Galois-Erweiterungen L/K ist in der Tatsache begründet, dass K jeweils der Invarianten- oder Fixkörper zur Galois-Gruppe $\operatorname{Gal}(L/K)$ ist, d. h. dass K aus allen denjenigen Elementen von L besteht, die unter allen Automorphismen aus $\operatorname{Gal}(L/K)$ invariant sind. Um diese Aussage, die zentraler Teil des Hauptsatzes der Galois-Theorie ist, beweisen zu können, studieren wir zunächst einmal Fixkörper, die mit Hilfe von Automorphismengruppen gebildet werden.

Satz 4. *Es sei L ein Körper und G eine Untergruppe von* $\operatorname{Aut}(L)$, *der Automorphismengruppe von L. Weiter setze man*

$$K = L^G = \{a \in L \,;\, \sigma(a) = a \text{ für alle } \sigma \in G\};$$

dies ist der sogenannte Fixkörper *in L unter G.*

(i) *Ist G endlich, so ist L/K eine endliche Galois-Erweiterung vom Grad $[L : K] = \operatorname{ord} G$ mit Galois-Gruppe* $\operatorname{Gal}(L/K) = G$.

(ii) *Ist G nicht endlich, L/K aber algebraisch, so ist L/K eine unendliche Galois-Erweiterung mit einer Galois-Gruppe* $\operatorname{Gal}(L/K)$, *welche G als Untergruppe enthält.*

Beweis. Man überlegt sich leicht, dass $K = L^G$ in der Tat ein Teilkörper von L ist. Sei nun G endlich bzw. L/K algebraisch. Um zu sehen, dass L/K separabel algebraisch ist, betrachte man ein Element $a \in L$ sowie ein maximales System von Elementen $\sigma_1, \ldots, \sigma_r \in G$ mit der Eigenschaft, dass $\sigma_1(a), \ldots, \sigma_r(a)$ paarweise verschieden sind. Ein solches endliches System existiert stets, auch dann, wenn G nicht endlich ist, die Erweiterung L/K aber algebraisch ist; im letzteren Falle ist nämlich $\sigma(a)$ für $\sigma \in G$ jeweils Nullstelle des Minimalpolynoms von a über K. Im Übrigen bemerke man, dass das Element a notwendigerweise unter den $\sigma_i(a)$ vorkommt. Jedes

$\sigma \in G$ induziert eine Selbstabbildung auf der Menge $\{\sigma_1(a), \ldots, \sigma_r(a)\}$, die notwendig bijektiv ist, und es folgt, dass das Polynom

$$f = \prod_{i=1}^{r} \big(X - \sigma_i(a)\big)$$

Koeffizienten in K hat, da diese unter G festgelassen werden. Es ist also a Nullstelle des separablen Polynoms $f \in K[X]$ und damit separabel über K, so dass insgesamt L/K separabel algebraisch ist. Weiter ist L/K normal, da L Zerfällungskörper über K aller Polynome f des obigen Typs ist. Damit sieht man, dass L/K eine Galois-Erweiterung ist.

Sei nun $n = \operatorname{ord} G$, wobei wir auch $n = \infty$ zulassen. Dann folgt mit vorstehender Argumentation $[K(a) : K] \leq n$ für jedes $a \in L$. Hieraus ergibt sich $[L : K] \leq n$, wenn man den Satz vom primitiven Element 3.6/12 auf Teilkörper von L anwendet, die endlich über K sind. Da G offenbar auch Untergruppe von $\operatorname{Aut}_K(L) = \operatorname{Gal}(L/K)$ ist, hat man nach Bemerkung 3

$$n = \operatorname{ord} G \leq \operatorname{ord} \operatorname{Gal}\big(L/K\big) \leq [L : K] \leq n$$

und deshalb $\operatorname{ord} G = [L : K]$. Im Falle $n < \infty$ ergibt sich außerdem $G = \operatorname{Gal}(L/K)$. □

Korollar 5. *Es sei L/K eine normale algebraische Körpererweiterung mit Automorphismengruppe $G = \operatorname{Aut}_K(L)$. Dann gilt*:

(i) *L/L^G ist eine Galois-Erweiterung mit Galois-Gruppe G.*

(ii) *Ist L/K separabel und damit galoissch, so hat man $L^G = K$.*

(iii) *Sei* $\operatorname{char} K > 0$. *Dann ist L^G rein inseparabel über K, und die Kette $K \subset L^G \subset L$ stimmt überein mit der Kette $K \subset K_i \subset L$ aus* 3.7/5.

Beweis. Wir können mit Satz 4 schließen, dass L/L^G eine Galois-Erweiterung ist. Die zugehörige Galois-Gruppe ist in diesem Falle G, denn es gilt $\operatorname{Aut}_{L^G}(L) = \operatorname{Aut}_K(L)$. Weiter folgt aus der Definition von L^G die Gleichung $[L^G : K]_s = 1$. Ist nämlich $\overline{K}$ ein algebraischer Abschluss von K, der L enthält, so setzt sich jeder K-Homomorphismus $L^G \longrightarrow \overline{K}$ gemäß 3.4/9 zu einem K-Homomorphismus $L \longrightarrow \overline{K}$ fort bzw. aufgrund der Normalität von L/K zu einem K-Automorphismus von L; alle K-Automorphismen von L sind aber auf L^G trivial. Also gilt $[L^G : K]_s = 1$. Ist nun L/K separabel, so auch L^G/K, und es folgt $L^G = K$ wegen $[L^G : K] = [L^G : K]_s = 1$.

Ist andererseits L/K (im Falle $\operatorname{char} K > 0$) nicht separabel, so erkennt man L^G/K nach 3.7/2 als rein inseparabel. Dass die Kette $K \subset L^G \subset L$ mit derjenigen aus 3.7/5 übereinstimmt, ergibt sich aus der Konstruktion bzw. der Eindeutigkeitsaussage in 3.7/5. □

Theorem 6 (Hauptsatz der Galois-Theorie). *Zu einer Galois-Erweiterung L/K mit Galois-Gruppe $\operatorname{Gal}(L/K)$ betrachte man die Abbildungen*

$$\begin{aligned} \big\{\text{Untergruppen von } \operatorname{Gal}(L/K)\big\} &\underset{\Psi}{\overset{\Phi}{\rightleftarrows}} \big\{\text{Zwischenkörper von } L/K\big\}, \\ H &\longmapsto L^H, \\ \operatorname{Gal}\big(L/E\big) &\longmapsfrom E, \end{aligned}$$

welche einer Untergruppe $H \subset \operatorname{Gal}(L/K)$ den Fixkörper L^H, bzw. einem Zwischenkörper E von L/K die Gruppe $\operatorname{Gal}(L/E)$ der Galois-Erweiterung L/E zuordnen.

(i) *Es gilt*

$$H \subset \operatorname{Gal}(L/L^H), \qquad L^{\operatorname{Gal}(L/E)} = E$$

für Untergruppen $H \subset \operatorname{Gal}(L/K)$ und Zwischenkörper E zu L/K. Insbesondere folgt $\Phi \circ \Psi = \mathrm{id}$, und es ist Φ surjektiv, Ψ injektiv.

(ii) *Ist die Erweiterung L/K zusätzlich* endlich, *so ergibt sich sogar*

$$H = \operatorname{Gal}(L/L^H)$$

und damit $\Psi \circ \Phi = \mathrm{id}$. In diesem Falle sind die Zuordnungen Φ, Ψ bijektiv und zueinander invers, definieren also eine bijektive Beziehung zwischen den Untergruppen von $\operatorname{Gal}(L/K)$ und den Zwischenkörpern von L/K.

(iii) *Ist $H \subset \operatorname{Gal}(L/K)$ ein Normalteiler, so ist die Erweiterung L^H/K normal und damit galoissch.*

(iv) *Umgekehrt, ist E ein Zwischenkörper zu L/K und ist E/K normal, so ist $\operatorname{Gal}(L/E)$ ein Normalteiler in $\operatorname{Gal}(L/K)$. Es besitzt nämlich der surjektive Gruppenhomomorphismus aus Bemerkung 2*

$$\begin{aligned} \operatorname{Gal}(L/K) &\longrightarrow \operatorname{Gal}\big(E/K\big), \\ \sigma &\longmapsto \sigma|_E, \end{aligned}$$

die Gruppe $\operatorname{Gal}(L/E)$ als Kern und induziert folglich einen Isomorphismus

$$\operatorname{Gal}(L/K)\big/\operatorname{Gal}(L/E) \xrightarrow{\sim} \operatorname{Gal}\big(E/K\big).$$

Die Inklusion $H \subset \mathrm{Gal}(L/L^H)$ aus Theorem 6 (i) ist im Allgemeinen echt, wenn die Erweiterung L/K nicht endlich ist. Im nachfolgenden Abschnitt 4.2 werden wir $\mathrm{Gal}(L/K)$ mit einer geeigneten Topologie versehen, bezüglich der $\mathrm{Gal}(L/L^H)$ als topologischer Abschluss von H zu sehen ist.

Bemerkung 7. *Die Zuordnungen* Φ, Ψ *aus Theorem* 6 *lassen sich auf die sogenannten* "abgeschlossenen" *Untergruppen von* $\mathrm{Gal}(L/K)$ *einschränken, d. h. auf Untergruppen* $H \subset \mathrm{Gal}(L/K)$ *mit* $H = \mathrm{Gal}(L/L^H)$. *Man erhält dann eine bijektive Beziehung zwischen den abgeschlossenen Untergruppen in* $\mathrm{Gal}(L/K)$ *und den Zwischenkörpern von* L/K, *auch wenn* L/K *nicht endlich ist*; *vgl.* 4.2/3.

Beweis zu Theorem 6 *und Bemerkung* 7. Wir gehen von einer nicht notwendig endlichen Galois-Erweiterung L/K aus. Die Inklusion $H \subset \mathrm{Gal}(L/L^H)$ für Untergruppen $H \subset \mathrm{Gal}(L/K)$ ist trivial. Ist andererseits E ein Zwischenkörper von L/K, so ist L/E galoissch, und die Galois-Gruppe $H = \mathrm{Gal}(L/E)$ ist eine Untergruppe von $\mathrm{Gal}(L/K)$; vgl. Bemerkung 2. Mit Korollar 5 (ii) folgt dann $E = L^H$, so dass man $\Phi \circ \Psi = \mathrm{id}$ schließen kann. Behauptung (i) ist damit klar. Weiter folgt, dass die Einschränkung $\Phi|_{\mathrm{im}\,\Psi}$ von Φ auf das Bild von Ψ bijektiv und invers zu Ψ ist, also die Relation $\Psi \circ \Phi|_{\mathrm{im}\,\Psi} = \mathrm{id}$ erfüllt. Die Abbildungen $\Phi|_{\mathrm{im}\,\Psi}$ und Ψ definieren daher bijektive und zueinander inverse Abbildungen zwischen $\mathrm{im}\,\Psi$ und der Menge der Zwischenkörper von L/K. Nun gehört eine Untergruppe $H \subset \mathrm{Gal}(L/K)$ aber offenbar genau dann zu $\mathrm{im}\,\Psi$, wenn sie der Relation $H = \Psi \circ \Phi(H)$ genügt, also der Relation $H = \mathrm{Gal}(L/L^H)$. In der Tat, ist H von dieser Form, so gilt natürlich $H \in \mathrm{im}\,\Psi$. Hat man umgekehrt $H \in \mathrm{im}\,\Psi$, etwa $H = \Psi(E)$ für einen Zwischenkörper E von L/K, so folgt

$$H = \Psi(E) = \Psi \circ (\Phi \circ \Psi)(E) = (\Psi \circ \Phi) \circ \Psi(E) = \Psi \circ \Phi(H)$$

wegen $\Phi \circ \Psi = \mathrm{id}$. Dies begründet die Aussage von Bemerkung 7.

Ist nun die Erweiterung L/K endlich, so ist auch die zugehörige Galois-Gruppe $\mathrm{Gal}(L/K)$ endlich; vgl. Bemerkung 3. Weiter ist jede Untergruppe $H \subset \mathrm{Gal}(L/K)$ endlich, und es folgt $H = \mathrm{Gal}(L/L^H)$ mit Satz 4. Somit ergibt sich $\Psi \circ \Phi = \mathrm{id}$ im Falle der Endlichkeit von L/K, d. h. Φ und Ψ sind dann bijektiv und zueinander invers. Dies erledigt Behauptung (ii).

Ist weiter H ein Normalteiler in $\mathrm{Gal}(L/K)$, so wähle man einen algebraischen Abschluss $\overline{L}$ von L; dies ist zugleich auch ein algebraischer Abschluss

von K und L^H. Um die Normalität von L^H/K nachzuweisen, betrachte man einen K-Homomorphismus $\sigma\colon L^H \longrightarrow \overline{L}$. Es ist dann $\sigma(L^H) = L^H$ zu zeigen. Um dies zu erreichen, setze man zunächst σ mittels 3.4/9 zu einem K-Homomorphismus $\sigma'\colon L \longrightarrow \overline{L}$ fort. Da L/K normal ist, beschränkt sich σ' zu einem Automorphismus von L, d. h. wir können σ als K-Homomorphismus $L^H \longrightarrow L$ interpretieren. Sei nun $b \in \sigma(L^H)$, etwa $b = \sigma(a)$ mit $a \in L^H$. Zum Nachweis von $b \in L^H$ hat man zu zeigen, dass b von allen Automorphismen aus H festgelassen wird. Sei also $\tau \in H$. Dann gibt es wegen $H\sigma = \sigma H$ (der Normalteilereigenschaft von H) zu τ ein Element $\tau' \in H$ mit $\tau \circ \sigma = \sigma \circ \tau'$, und es gilt wegen $a \in L^H$

$$\tau(b) = \tau \circ \sigma(a) = \sigma \circ \tau'(a) = \sigma(a) = b,$$

d. h. $b \in L^H$. Somit folgt $\sigma(L^H) \subset L^H$. Indem wir $\sigma^{-1}\colon \sigma(L^H) \longrightarrow L^H$ gemäß 3.4/9 zu einem K-Homomorphismus $\rho\colon L^H \longrightarrow \overline{L}$ fortsetzen, ergibt sich in gleicher Weise $\rho(L^H) \subset L^H$ und damit $\sigma(L^H) = L^H$. Dies erledigt Aussage (iii). Bezüglich Aussage (iv) verweisen wir auf Bemerkung 2. □

Wir wollen einige Folgerungen aus dem Hauptsatz der Galois-Theorie ziehen.

Korollar 8. *Jede endliche separable Körpererweiterung L/K besitzt nur endlich viele Zwischenkörper.*

Beweis. Indem wir zu einer normalen Hülle von L/K übergehen, vgl. 3.5/7, können wir voraussetzen, dass L/K endlich und galoissch ist. Dann korrespondieren die Zwischenkörper von L/K in bijektiver Weise zu den Untergruppen der endlichen Gruppe $\mathrm{Gal}(L/K)$. □

Um das nächste Resultat formulieren zu können, erklären wir für Teilkörper E, E' eines Körpers L das *Kompositum* $E \cdot E'$ als den kleinsten Teilkörper von L, der E und E' enthält. Man gewinnt $E \cdot E'$, indem man alle Elemente von E' zu E oder auch alle Elemente von E zu E' adjungiert, d. h. $E \cdot E' = E(E') = E'(E)$.

Korollar 9. *Es sei L/K eine endliche Galois-Erweiterung. Zu Zwischenkörpern E, E' von L/K betrachte man $H = \mathrm{Gal}(L/E)$ und $H' = \mathrm{Gal}(L/E')$ als Untergruppen von* $\mathrm{Gal}(L/K)$. *Dann gilt*:

(i) $E \subset E' \Longleftrightarrow H \supset H'$.

(ii) $E \cdot E' = L^{H \cap H'}$.

(iii) $E \cap E' = L^{H''}$, *wobei* H'' *die von* H *und* H' *in* $\mathrm{Gal}(L/K)$ *erzeugte Untergruppe ist, also die kleinste Untergruppe in* $\mathrm{Gal}(L/K)$, *die* H *und* H' *enthält*; *vgl.* 1.3.

Beweis. (i) Gilt $E \subset E'$, so ist jeder E'-Automorphismus von L auch ein E-Automorphismus, d. h. es gilt $H = \mathrm{Gal}(L/E) \supset \mathrm{Gal}(L/E') = H'$. Umgekehrt folgt aus $H \supset H'$ die Inklusion $E = L^H \subset L^{H'} = E'$.

(ii) Es gilt $E \cdot E' \subset L^{H \cap H'}$ sowie $\mathrm{Gal}(L/E \cdot E') \subset H \cap H'$. Aus letzterer Inklusion folgt mit (i) sofort $E \cdot E' \supset L^{H \cap H'}$.

(iii) Es gilt $L^{H''} = L^H \cap L^{H'} = E \cap E'$. □

Definition 10. *Eine Galois-Erweiterung* L/K *heißt* abelsch (*bzw*. zyklisch), *wenn die Gruppe* $\mathrm{Gal}(L/K)$ *abelsch* (*bzw*. *zyklisch*) *ist*.

Beispiele zyklischer und somit abelscher Galois-Erweiterungen lassen sich leicht angeben. Mit 3.8/4 und 3.8/6 sieht man, dass jede Erweiterung zwischen endlichen Körpern eine zyklische Galois-Erweiterung darstellt.

Korollar 11. *Es sei* L/K *eine abelsche* (*bzw*. *zyklische*) *Galois-Erweiterung*. *Dann ist für jeden Zwischenkörper* E *von* L/K *auch* E/K *eine abelsche* (*bzw*. *zyklische*) *Galois-Erweiterung*.

Beweis. Sei E ein Zwischenkörper zu L/K. Dann ist $H = \mathrm{Gal}(L/E)$ als Untergruppe von $\mathrm{Gal}(L/K)$ ein Normalteiler, da zyklische Gruppen insbesondere abelsch sind. Weiter ist E galoissch über K nach Theorem 6 (iii), wobei sich die Galois-Gruppe $\mathrm{Gal}(E/K)$ nach 6 (iv) zu $\mathrm{Gal}(L/K)/\mathrm{Gal}(L/E)$ berechnet. Dieser Quotient ist abelsch bzw. zyklisch, wenn $\mathrm{Gal}(L/K)$ die entsprechende Eigenschaft hat. □

Satz 12. *Es sei* L/K *eine Körpererweiterung mit Zwischenkörpern* E, E', *so dass* E/K *und* E'/K *endliche Galois-Erweiterungen sind. Dann gilt*:

(i) $E \cdot E'$ *ist endlich und galoissch über* K, *und der Homomorphismus*

$$\varphi\colon\ \mathrm{Gal}\big(E \cdot E'/E\big) \longrightarrow \mathrm{Gal}\big(E'/E \cap E'\big),$$
$$\sigma \longmapsto \sigma|_{E'},$$

ist bijektiv.

(ii) *Der Homomorphismus*

$$\psi\colon \operatorname{Gal}\bigl(E\cdot E'/K\bigr) \longrightarrow \operatorname{Gal}\bigl(E/K\bigr)\times\operatorname{Gal}\bigl(E'/K\bigr),$$
$$\sigma \longmapsto (\sigma|_E, \sigma|_{E'}),$$

ist injektiv. Gilt $E\cap E'=K$, so ist ψ auch surjektiv und damit bijektiv.

Beweis. Wir beginnen mit Aussage (i). Zunächst folgt aus der Beziehung $E\cdot E' = K(E,E')$, dass $E\cdot E'$ normal, separabel und endlich über K ist, da E/K und E'/K diese Eigenschaften besitzen. Weiter ist φ injektiv, denn für $\sigma\in\operatorname{Gal}(E\cdot E'/E)$ gilt $\sigma|_E=\mathrm{id}$, und für $\sigma\in\ker\varphi$ gilt zusätzlich $\sigma|_{E'}=\mathrm{id}$, also $\sigma=\mathrm{id}$. Für die Surjektivität von φ nutzen wir den Hauptsatz und betrachten die Gleichung

$$(E')^{\operatorname{im}\varphi} = (E\cdot E')^{\operatorname{Gal}(E\cdot E'/E)}\cap E' = E\cap E';$$

diese impliziert $\operatorname{im}\varphi=\operatorname{Gal}(E'/E\cap E')$, wie gewünscht.

Die Injektivität von ψ in Aussage (ii) ist leicht einzusehen, denn jeder K-Automorphismus $\sigma\in\ker\psi$ ist trivial auf E und E', somit also auch auf $E\cdot E'$. Zum Nachweis der Surjektivität von ψ nehmen wir $E\cap E'=K$ an. Sei $(\sigma,\sigma')\in\operatorname{Gal}(E/K)\times\operatorname{Gal}(E'/K)$. Nach (i) lässt sich $\sigma'\in\operatorname{Gal}(E'/K)$ fortsetzen zu $\tilde\sigma'\in\operatorname{Gal}(E\cdot E'/K)$ mit $\tilde\sigma'|_E=\mathrm{id}$. Entsprechend lässt sich auch σ fortsetzen zu $\tilde\sigma\in\operatorname{Gal}(E\cdot E'/K)$ mit $\tilde\sigma|_{E'}=\mathrm{id}$. Es ist dann $\tilde\sigma\circ\tilde\sigma'$ ein Urbild zu (σ,σ') unter ψ, denn es gilt

$$(\tilde\sigma\circ\tilde\sigma')|_E = \tilde\sigma|_E\circ\tilde\sigma'|_E = \sigma$$

und

$$(\tilde\sigma\circ\tilde\sigma')|_{E'} = \tilde\sigma|_{E'}\circ\tilde\sigma'|_{E'} = \sigma'.$$

□

Lernkontrolle und Prüfungsvorbereitung

1. Wann bezeichnet man eine algebraische Körpererweiterung L/K als Galois-Erweiterung? Was versteht man in diesem Falle unter der Galois-Gruppe von L/K?
2. Erkläre einige Beispiele von endlichen Galois-Erweiterungen L/K mit zugehörigen Galois-Gruppen, wobei K einer der Körper $\mathbb{Q}$, $\mathbb{R}$ oder ein endlicher Körper sei.

3. Zeige, dass eine endliche normale Körpererweiterung L/K genau dann eine Galois-Erweiterung ist, wenn $\operatorname{ord} \operatorname{Aut}_K(L) = [L\colon K]$ gilt.

4. Wie lautet der Hauptsatz der Galois-Theorie? Erkläre insbesondere für eine Galois-Erweiterung L/K, wie man einer Untergruppe der Galois-Gruppe $\operatorname{Gal}(L/K)$ einen Zwischenkörper zu L/K und umgekehrt einem Zwischenkörper von L/K eine Untergruppe von $\operatorname{Gal}(L/K)$ zuordnet.

5. Welche Verbindung besteht zwischen Normalteilern im Sinne der Gruppentheorie und normalen algebraischen Körpererweiterungen?

6. Es sei L/K eine Galois-Erweiterung und E ein Zwischenkörper, derart dass E/K normal sei. Zeige, dass E/K galoissch ist und beweise, dass die Einschränkung von K-Automorphismen von L auf E einen surjektiven Gruppenhomomorphismus $\operatorname{Gal}(L/K) \longrightarrow \operatorname{Gal}(E/K)$ mit Kern $\operatorname{Gal}(L/E)$ erklärt.

7. Es sei L/K eine Galois-Erweiterung und $H \subset \operatorname{Gal}(L/K)$ ein Normalteiler. Zeige, dass die Erweiterung L^H/K normal ist.

+8. Es sei L ein Körper und G eine endliche Untergruppe der Automorphismengruppe $\operatorname{Aut}(L)$ von L. Definiere den Fixkörper L^G in L unter G und zeige, dass L/L^G eine endliche Galois-Erweiterung vom Grad $[L\colon L^G] = \operatorname{ord} G$ und mit Galois-Gruppe $\operatorname{Gal}(L/L^G) = G$ ist. Wie lässt sich dieses Resultat auf nicht notwendig endliche Untergruppen $G \subset \operatorname{Aut}(L)$ verallgemeinern?

9. Verwende das Resultat von Punkt 8 zum Beweis des Hauptsatzes der Galois-Theorie.

++10. Es sei L/K eine Galois-Erweiterung. Zeige, dass die Zwischenkörper zu L/K bijektiv zu den Untergruppen $H \subset \operatorname{Gal}(L/K)$ korrespondieren, welche der Relation $H = \operatorname{Gal}(L/L^H)$ genügen.

11. Warum besitzt eine endliche separable Körpererweiterung nur endlich viele Zwischenkörper?

12. Sei L/K eine endliche Galois-Erweiterung mit Zwischenkörpern E und E'. Zeige, dass $E \subset E'$ äquivalent zu $\operatorname{Gal}(L/E) \supset \operatorname{Gal}(L/E')$ ist.

13. Wann heißt eine Galois-Erweiterung abelsch, wann zyklisch?

14. Es sei L/K eine abelsche Galois-Erweiterung. Zeige, dass für jeden Zwischenkörper E zu L/K auch E/K eine abelsche Galois-Erweiterung ist. Beweise dasselbe Resultat für "zyklisch" anstelle der Bedingung "abelsch".

15. Es seien E/K und E'/K endliche Galois-Erweiterungen, deren Kompositum $E \cdot E'$ man in einem gemeinsamen Oberkörper bilden kann. Vergleiche die Galois-Gruppe $\operatorname{Gal}(E \cdot E'/E)$ mit $\operatorname{Gal}(E'/E \cap E')$ sowie $\operatorname{Gal}(E \cdot E'/K)$ mit dem Produkt $\operatorname{Gal}(E/K) \times \operatorname{Gal}(E'/K)$.

Übungsaufgaben

1. *Welche Einsichten liefert der Hauptsatz der Galois-Theorie bezüglich endlicher algebraischer Körpererweiterungen*?
2. *Wie müsste der Hauptsatz der Galois-Theorie lauten, wenn man ihn für endliche quasi-galoissche Körpererweiterungen formulieren wollte*?
3. *Zeige, dass eine algebraische Körpererweiterung L/K genau dann galoissch ist, wenn K der Fixkörper unter der Automorphismengruppe* $\mathrm{Aut}_K(L)$ *ist.*
4. Konstruiere einen Körper L mit einer Untergruppe $G \subset \mathrm{Aut}(L)$, derart dass L/L^G keine Galois-Erweiterung ist.
5. Es sei L/K eine endliche Galois-Erweiterung und $H \subset \mathrm{Gal}(L/K)$ eine Untergruppe.
   (i) Sei $\alpha \in L$ und sei für $\sigma \in \mathrm{Gal}(L/K)$ die Gleichung $\sigma(\alpha) = \alpha$ äquivalent zu $\sigma \in H$. Zeige $L^H = K(\alpha)$.
   (ii) Begründe, dass es zu H stets ein $\alpha \in L$ wie in (i) gibt.
6. Es sei K ein Körper, $f \in K[X]$ ein irreduzibles separables Polynom und L ein Zerfällungskörper von f über K, so dass also L/K eine endliche Galois-Erweiterung ist. Zeige: Ist L/K abelsch, so gilt $L = K(\alpha)$ für jede Nullstelle $\alpha \in L$ von f.
7. Sei L ein algebraisch abgeschlossener Körper und $\sigma \in \mathrm{Aut}(L)$. Sei $K = L^\sigma$ der Fixkörper unter σ. Zeige, dass jede endliche Körpererweiterung von K eine zyklische Galois-Erweiterung ist.
8. Betrachte zu einer Galois-Erweiterung L/K ein Element $\alpha \in L - K$ sowie einen Zwischenkörper K', der maximal mit der Bedingung $\alpha \notin K'$ ist. Zeige: Ist E ein Zwischenkörper zu L/K' mit $[E : K'] < \infty$, so ist E/K' eine zyklische Galois-Erweiterung.
9. Sei K ein Körper und $\overline{K}$ ein algebraischer Abschluss. Zeige:
   (i) Ist E_i, $i \in I$, eine Familie von Zwischenkörpern zu $\overline{K}/K$ mit der Eigenschaft, dass E_i/K jeweils eine abelsche Galois-Erweiterung ist, so ist auch $K(\bigcup_{i\in I} E_i)$ eine abelsche Galois-Erweiterung von K.
   (ii) Es existiert eine maximale abelsche Galois-Erweiterung K_{ab}/K. Diese ist charakterisiert durch die folgenden Eigenschaften: (a) Es ist K_{ab}/K abelsche Galois-Erweiterung. (b) Für jede weitere abelsche Galois-Erweiterung L/K ist L isomorph über K zu einem Zwischenkörper von K_{ab}/K.
   (iii) Je zwei maximale abelsche Galois-Erweiterungen sind über K isomorph.

10. Es sei L/K eine endliche Galois-Erweiterung. Weiter seien L_1, L_2 Zwischenkörper zu L/K, welche zu den Untergruppen $H_1, H_2 \subset \mathrm{Gal}(L/K)$ korrespondieren mögen. Zeige: Für $\sigma \in \mathrm{Gal}(L/K)$ ist $\sigma(L_1) = L_2$ äquivalent zu der Gleichung $\sigma H_1 \sigma^{-1} = H_2$.
11. Zeige, dass $L = \mathbb{Q}(\sqrt{p_1}, \ldots, \sqrt{p_n})$ für paarweise verschiedene Primzahlen $p_1, \ldots, p_n$ eine abelsche Galois-Erweiterung von $\mathbb{Q}$ mit Galois-Gruppe $(\mathbb{Z}/2\mathbb{Z})^n$ ist. (*Hinweis*: Beachte, dass für $a \in \mathbb{Q}$ mit $\sqrt{a} \in L$ und für $\sigma \in \mathrm{Gal}(L/\mathbb{Q})$ stets $\sigma(\sqrt{a}) = \pm\sqrt{a}$ gilt. Allgemeiner werden Erweiterungen des Typs $L/\mathbb{Q}$ im Rahmen der sogenannten multiplikativen *Kummer-Theorie* behandelt; siehe 4.9.)

4.2 Proendliche Galois-Gruppen*

Im vorigen Abschnitt hatten wir die Galois-Theorie im Wesentlichen für endliche Körpererweiterungen entwickelt, ohne auf speziellere Techniken für den unendlichen Fall einzugehen. Wir wollen dies hier nachholen und einige Zusatzüberlegungen anstellen, die speziell für nicht-endliche Galois-Erweiterungen von Interesse sind. Sei also L/K eine beliebige Galois-Erweiterung. Dann können wir das System $\mathfrak{L} = (L_i)_{i\in I}$ aller Zwischenkörper von L/K betrachten, die *endlich* und galoissch über K sind. Es bezeichne $f_i\colon \mathrm{Gal}(L/K) \longrightarrow \mathrm{Gal}(L_i/K)$ jeweils den Restriktionshomomorphismus gemäß 4.1/2. Jedes $\sigma \in \mathrm{Gal}(L/K)$ bestimmt dann eine Familie von Galois-Automorphismen $(\sigma_i)_{i\in I}$, indem wir $\sigma_i = \sigma|_{L_i} = f_i(\sigma)$ setzen. Dabei gilt $\sigma_j|_{L_i} = \sigma_i$ für $L_i \subset L_j$. Hat man umgekehrt eine Familie $(\sigma_i)_{i\in I} \in \prod_{i\in I} \mathrm{Gal}(L_i/K)$, welche vorstehende Verträglichkeitsrelation erfüllt, so definiert diese eindeutig ein Element $\sigma \in \mathrm{Gal}(L/K)$. Hierfür sind zwei Gegebenheiten verantwortlich: Zum einen ist L die Vereinigung aller $L_i \in \mathfrak{L}$, denn für $a \in L$ ist die normale Hülle von $K(a)$ in L/K eine endliche Galois-Erweiterung, welche a enthält; vgl. 3.5/7. Insbesondere ist jedes $\sigma \in \mathrm{Gal}(L/K)$ eindeutig durch seine Restriktionen auf die L_i festgelegt. Zum anderen gibt es zu je zwei endlichen Galois-Erweiterungen $L_i, L_j \in \mathfrak{L}$ stets ein $L_k \in \mathfrak{L}$ mit $L_i \cup L_j \subset L_k$, nämlich das Kompositum $L_i \cdot L_j = K(L_i, L_j)$. Ist daher (σ_i) ein System von Galois-Automorphismen mit $\sigma_j|_{L_i} = \sigma_i$ für $L_i \subset L_j$, so ergeben die σ_i eine wohldefinierte Abbildung $\sigma\colon L \longrightarrow L$. Diese ist ein K-Automorphismus, da es zu $a, b \in L$, etwa $a \in L_i$, $b \in L_j$, stets einen Index k mit $a, b \in L_k$ gibt und da σ_k ein K-Automorphismus ist.

Es sei nun $H \subset \mathrm{Gal}(L/K)$ eine Untergruppe. Ähnlich wie oben beschrieben, kann man zu H die Restriktionen $H_i = f_i(H) \subset \mathrm{Gal}(L_i/K), i \in I$, bilden. Ein Element $a \in L$ ist genau dann invariant unter H, wenn es invariant unter einem (oder alternativ, unter allen) H_i mit $a \in L_i$ ist. Allerdings ist H im Gegensatz zur obigen Situation im Allgemeinen nicht eindeutig durch die Restriktionen H_i bestimmt; man betrachte als Beispiel etwa die absolute Galois-Gruppe eines endlichen Körpers, welche wir am Ende dieses Abschnitts berechnen. Diese Unbestimmtheit von H ist der eigentliche Grund dafür, dass sich der Teil 4.1/6 (ii) des Hauptsatzes der Galois-Theorie nur in modifizierter Form auf unendliche Galois-Erweiterungen übertragen lässt. Eine gewisse Hüllenbildung von Untergruppen in $\mathrm{Gal}(L/K)$ ist erforderlich, vgl. 4.1/7, und diese lässt sich am einfachsten unter Zuhilfenahme topologischer Begriffsbildungen beschreiben.

Es sei daran erinnert, dass eine *Topologie* auf einer Menge X aus einem System $\mathfrak{T} = (U_i)_{i \in I}$ von Teilmengen von X besteht, den sogenannten *offenen* Mengen, so dass folgende Bedingungen erfüllt sind:

(i) $\emptyset, X$ sind offen.

(ii) Die Vereinigung beliebig vieler offener Teilmengen von X ist offen.

(iii) Der Durchschnitt endlich vieler offener Teilmengen von X ist offen.

Das Paar $(X, \mathfrak{T})$ (meist einfach mit X bezeichnet) heißt ein *topologischer Raum*. Für einen Punkt $x \in X$ bezeichnet man offene Mengen $U \subset X$, die x enthalten, auch als *offene Umgebungen* von x. Komplemente offener Teilmengen von X werden *abgeschlossene* Teilmengen von X genannt. Weiter kann man zu jeder Teilmenge $S \subset X$ den *Abschluss* $\overline{S}$ betrachten. Dies ist der Durchschnitt aller abgeschlossenen Teilmengen von X, die S enthalten, oder, mit anderen Worten, die kleinste abgeschlossene Teilmenge von X, die S enthält. Sie besteht aus allen denjenigen Punkten $x \in X$, so dass $U \cap S \neq \emptyset$ für jede offene Umgebung U von x gilt. Wie üblich nennt man eine Abbildung topologischer Räume $(X', \mathfrak{T}') \longrightarrow (X, \mathfrak{T})$ *stetig*, wenn das Urbild einer $\mathfrak{T}$-offenen Teilmenge von X stets $\mathfrak{T}'$-offen in X' ist, oder in äquivalenter Weise, wenn das Urbild einer $\mathfrak{T}$-abgeschlossenen Teilmenge von X stets $\mathfrak{T}'$-abgeschlossen in X' ist.

Um eine Topologie auf einer Menge X zu definieren, kann man von einem beliebigen System $\mathfrak{B}$ von Teilmengen von X ausgehen und die hiervon erzeugte Topologie betrachten. Um diese zu konstruieren, vergrößert man $\mathfrak{B}$ zunächst zu einem System $\mathfrak{B}'$, indem man die spezielle Teilmenge $X \subset X$ hinzunimmt sowie alle endlichen Durchschnitte von Teilmengen von X, die

zu $\mathfrak{B}$ gehören. Sodann bezeichnet man eine Teilmenge $U \subset X$ als offen, wenn sie Vereinigung von Mengen aus $\mathfrak{B}'$ ist; mit anderen Worten, wenn es zu jedem $x \in U$ ein $V \in \mathfrak{B}'$ gibt mit $x \in V \subset U$. Man sieht leicht, dass man auf diese Weise eine Topologie $\mathfrak{T}$ auf X erhält. Man nennt $\mathfrak{T}$ die von $\mathfrak{B}$ *erzeugte Topologie* auf X. Es ist $\mathfrak{T}$ die *gröbste Topologie* auf X, bezüglich welcher die Elemente von $\mathfrak{B}$ offen in X sind; d. h. jede weitere Topologie $\mathfrak{T}'$ mit letzterer Eigenschaft ist *feiner* als $\mathfrak{T}$ in dem Sinne, dass jede $\mathfrak{T}$-offene Teilmenge von X auch $\mathfrak{T}'$-offen ist. Im Übrigen prüft man leicht nach, dass die Vergrößerung von $\mathfrak{B}$ zu $\mathfrak{B}'$ überflüssig ist, wenn X bereits Vereinigung aller Elemente aus $\mathfrak{B}$ ist und wenn der Durchschnitt zweier Elemente $U, V \in \mathfrak{B}$ stets wieder eine Vereinigung von Teilmengen von X ist, die zu $\mathfrak{B}$ gehören.

Als Anwendung des gerade beschriebenen Konstruktionsverfahrens können wir das *Produkt* einer Familie topologischer Räume $(X_i)_{i\in I}$ definieren. Man betrachte nämlich auf dem gewöhnlichen kartesischen Produkt $\prod_{i\in I} X_i$ diejenige Topologie, die von allen Teilmengen des Typs $\prod_{i\in I} U_i$ erzeugt wird, wobei U_i offen in X_i ist und $U_i = X_i$ für fast alle $i \in I$ gilt. Dies ist die gröbste Topologie, für die alle Projektionen auf die Faktoren X_i stetig sind. Im Übrigen benötigen wir noch den Begriff der *Restriktion* der Topologie eines topologischen Raumes X auf eine Teilmenge $V \subset X$. Hierunter versteht man die Topologie auf V, deren offene Mengen gerade die Schnitte der offenen Mengen von X mit V sind. Man spricht dann auch von der von X auf V *induzierten Topologie*.

Wir kehren nun zu der ursprünglich betrachteten Galois-Erweiterung L/K zurück und betrachten wieder das System $\mathfrak{L} = (L_i)_{i\in I}$ aller in L gelegenen endlichen Galois-Erweiterungen von K sowie die zugehörigen Restriktionen $f_i\colon \operatorname{Gal}(L/K) \longrightarrow \operatorname{Gal}(L_i/K)$. Für jedes $i \in I$ versehen wir die endliche Gruppe $\operatorname{Gal}(L_i/K)$ mit der diskreten Topologie; dies ist diejenige Topologie, bezüglich der alle Teilmengen von $\operatorname{Gal}(L_i/K)$ offen sind. Sodann betrachten wir auf $\operatorname{Gal}(L/K)$ die gröbste Topologie, so dass alle Restriktionen $f_i\colon \operatorname{Gal}(L/K) \longrightarrow \operatorname{Gal}(L_i/K)$ stetig sind. Da $\operatorname{Gal}(L_i/K)$ jeweils die diskrete Topologie trägt, ist dies die von allen Fasern der Abbildungen f_i erzeugte Topologie.[1]

[1] Unter den Fasern einer Abbildung $f\colon X \longrightarrow Y$ versteht man die Urbilder $f^{-1}(y)$ von Punkten $y \in Y$.

Bemerkung 1. (i) *Eine Teilmenge* $U \subset \mathrm{Gal}(L/K)$ *ist genau dann offen, wenn es zu jedem Element* $\sigma \in U$ *einen Index* $i \in I$ *gibt mit* $f_i^{-1}(f_i(\sigma)) \subset U$.

(ii) *Eine Teilmenge* $A \subset \mathrm{Gal}(L/K)$ *ist genau dann abgeschlossen, wenn für jedes* $\sigma \in \mathrm{Gal}(L/K) - A$ *ein* $i \in I$ *mit* $f_i^{-1}(f_i(\sigma)) \cap A = \emptyset$ *existiert.*

(iii) *Für eine Teilmenge* $S \subset \mathrm{Gal}(L/K)$ *besteht der Abschluss* $\overline{S}$ *aus allen Elementen* $\sigma \in \mathrm{Gal}(L/K)$, *so dass* $f_i^{-1}(f_i(\sigma)) \cap S \neq \emptyset$ *für alle* $i \in I$.

Beweis. Wir begründen nur Aussage (i), die restlichen beiden Behauptungen sind formale Folgerungen hieraus. Sei $\mathfrak{B}$ das System der Fasern der Restriktionen f_i, $i \in I$. Aufgrund der Beschreibung der von einem System von Teilmengen einer Menge X erzeugten Topologie haben wir lediglich zu zeigen, dass wir $\mathfrak{B}$, wie oben ausgeführt, nicht durch Hinzunahme endlicher Durchschnitte von Elementen aus $\mathfrak{B}$ zu einem System $\mathfrak{B}'$ zu vergrößern brauchen, d. h. dass für zwei Automorphismen $\sigma_i \in \mathrm{Gal}(L_i/K)$, $\sigma_j \in \mathrm{Gal}(L_j/K)$ der Durchschnitt $f_i^{-1}(\sigma_i) \cap f_j^{-1}(\sigma_j)$ Vereinigung gewisser Fasern von Restriktionsabbildungen $f_k\colon \mathrm{Gal}(L/K) \longrightarrow \mathrm{Gal}(L_k/K)$ ist. Um dies nachzuweisen, wähle man einen Index $k \in I$ mit $L_i \cup L_j \subset L_k$. Da f_i die Komposition von f_k mit der Restriktionsabbildung $\mathrm{Gal}(L_k/K) \longrightarrow \mathrm{Gal}(L_i/K)$ ist, sieht man, dass $f_i^{-1}(\sigma_i)$ Vereinigung von Fasern der Restriktion $f_k\colon \mathrm{Gal}(L/K) \longrightarrow \mathrm{Gal}(L_k/K)$ ist. Entsprechendes gilt für $f_j^{-1}(\sigma_j)$, und es folgt, dass auch $f_i^{-1}(\sigma_i) \cap f_j^{-1}(\sigma_j)$ Vereinigung von Fasern von f_k ist. □

Mit Hilfe von Bemerkung 1 kann man leicht sehen, dass $\mathrm{Gal}(L/K)$ eine *topologische Gruppe* ist. Man versteht hierunter eine Gruppe G mit einer Topologie, derart dass die Gruppenverknüpfung $G \times G \longrightarrow G$ sowie die Inversenbildung $G \longrightarrow G$ stetig sind. Dabei versieht man $G \times G$ natürlich mit der Produkttopologie. Zur weiteren Illustration der Topologie auf $\mathrm{Gal}(L/K)$ wollen wir zeigen:

Bemerkung 2. *Es ist* $\mathrm{Gal}(L/K)$ *als topologische Gruppe kompakt und total unzusammenhängend.*

Bevor wir den Beweis beginnen, sei daran erinnert, dass ein topologischer Raum X *quasi-kompakt* heißt, wenn jede offene Überdeckung von X eine endliche Teilüberdeckung enthält. Weiter heißt X *kompakt*, wenn X quasi-kompakt und *hausdorffsch* ist. Letzteres bedeutet, dass es zu $x, y \in X$

disjunkte offene Teilmengen $U, V \subset X$ mit $x \in U$, $y \in V$ gibt. Schließlich heißt X *total unzusammenhängend*, wenn für jede Teilmenge $A \subset X$, die mehr als ein Element enthält, zwei offene Teilmengen $U, V \subset X$ existieren mit $A \subset U \cup V$ sowie $U \cap A \neq \emptyset \neq V \cap A$ und $U \cap A \cap V = \emptyset$. Trägt X beispielsweise die diskrete Topologie, so ist X hausdorffsch und total unzusammenhängend. Ist X zusätzlich endlich, so ist X auch kompakt.

Beweis zu Bemerkung 2. Die zu betrachtenden Restriktionsabbildungen $f_i\colon \operatorname{Gal}(L/K) \longrightarrow \operatorname{Gal}(L_i/K)$ induzieren einen injektiven Homomorphismus

$$\operatorname{Gal}\big(L/K\big) \hookrightarrow \prod_{i\in I} \operatorname{Gal}\big(L_i/K\big),$$

den wir im Folgenden als Inklusion verstehen. Es ist $\prod \operatorname{Gal}(L_i/K)$ als Produkt endlicher diskreter, also kompakter topologischer Räume aufgrund des Satzes von Tychonoff selbst wieder kompakt (eine Tatsache, die man in der hier vorliegenden speziellen Situation auch elementar nachprüfen kann). Da $\prod \operatorname{Gal}(L_i/K)$ auf $\operatorname{Gal}(L/K)$ die gegebene Topologie induziert, haben wir zum Nachweis der Kompaktheit von $\operatorname{Gal}(L/K)$ lediglich zu zeigen, dass diese Gruppe abgeschlossen in $\prod \operatorname{Gal}(L_i/K)$ ist. Um dies einzusehen, betrachte man einen Punkt $(\sigma_i) \in \prod \operatorname{Gal}(L_i/K)$, der nicht zu $\operatorname{Gal}(L/K)$ gehört, für den es also zwei Indizes $j, j' \in I$ mit $L_j \subset L_{j'}$ gibt, so dass $\sigma_{j'}|_{L_j} \neq \sigma_j$. Dann bildet aber die Menge aller $(\sigma_i') \in \prod \operatorname{Gal}(L_i/K)$, für die $\sigma_j' = \sigma_j$ und $\sigma_{j'}' = \sigma_{j'}$ gilt, eine offene Umgebung des Punktes (σ_i), welche $\operatorname{Gal}(L/K)$ nicht trifft. Folglich ist $\operatorname{Gal}(L/K)$ abgeschlossen in $\prod \operatorname{Gal}(L_i/K)$.

Um zu sehen, dass $\operatorname{Gal}(L/K)$ total unzusammenhängend ist, genügt es zu zeigen, dass $\prod \operatorname{Gal}(L_i/K)$ als Produkt diskreter Gruppen total unzusammenhängend ist. Seien etwa (σ_i) und (σ_i') zwei verschiedene Elemente von $\prod \operatorname{Gal}(L_i/K)$. Dann existiert ein Index $j \in I$ mit $\sigma_j \neq \sigma_j'$. Man definiere nun offene Teilmengen $V = \prod V_i$ und $V' = \prod V_i'$ in $\prod \operatorname{Gal}(L_i/K)$ durch

$$V_i = \begin{cases} \operatorname{Gal}(L_i/K) & \text{für } i \neq j \\ \{\sigma_j\} & \text{für } i = j \end{cases}, \qquad V_i' = \begin{cases} \operatorname{Gal}(L_i/K) & \text{für } i \neq j \\ \operatorname{Gal}(L_j/K) - \{\sigma_j\} & \text{für } i = j \end{cases}.$$

Dann gilt $(\sigma_i) \in V$, $(\sigma_i') \in V'$ sowie $\prod \operatorname{Gal}(L_i/K) = V \cup V'$ und $V \cap V' = \emptyset$. Hieraus sieht man unmittelbar, dass $\prod \operatorname{Gal}(L_i/K)$ die definierende Eigenschaft eines total unzusammenhängenden topologischen Raumes erfüllt.

□

Wir wollen uns nun der Verallgemeinerung des Hauptsatzes der Galois-Theorie 4.1/6 auf beliebige Galois-Erweiterungen zuwenden.

Satz 3. *Es sei L/K eine beliebige Galois-Erweiterung. Dann beschränken sich die Abbildungen Φ und Ψ aus* 4.1/6 *zu Abbildungen*

$$\left\{\begin{matrix}\text{abgeschlossene Untergruppen}\\ \text{von } \mathrm{Gal}(L/K)\end{matrix}\right\} \underset{\Psi}{\overset{\Phi}{\rightleftarrows}} \{\text{Zwischenkörper von } L/K\},$$

$$\begin{aligned} H &\longmapsto L^H,\\ \mathrm{Gal}(L/E) &\longmapsfrom E, \end{aligned}$$

die bijektiv und zueinander invers sind.

Die wesentliche Arbeit des Beweises wurde bereits in Abschnitt 4.1 geleistet, man vergleiche 4.1/7. Es bleibt lediglich noch nachzuweisen, dass eine Untergruppe $H \subset \mathrm{Gal}(L/K)$ genau dann abgeschlossen ist, wenn $H = \mathrm{Gal}(L/L^H)$ gilt. Letzteres ergibt sich aus folgendem Resultat:

Lemma 4. *Es sei $H \subset \mathrm{Gal}(L/K)$ eine Untergruppe und L^H der Fixkörper unter H. Dann ist $\mathrm{Gal}(L/L^H)$ als Untergruppe von $\mathrm{Gal}(L/K)$ gerade der Abschluss von H. Insbesondere ist H genau dann abgeschlossen in $\mathrm{Gal}(L/K)$, wenn $H = \mathrm{Gal}(L/L^H)$ gilt.*

Beweis. Wir betrachten wieder das System $(L_i)_{i\in I}$ aller Zwischenkörper von L/K mit der Eigenschaft, dass L_i/K endlich und galoissch ist, sowie die Restriktionsabbildungen $f_i\colon \mathrm{Gal}(L/K) \longrightarrow \mathrm{Gal}(L_i/K)$. Sei $H_i = f_i(H)$. Da ein Element $a \in L_i$ genau dann invariant unter H ist, wenn es invariant unter H_i ist, gilt $L^H \cap L_i = L_i^{H_i}$, also $L^H = \bigcup_{i\in I} L_i^{H_i}$. Ist $H' \subset \mathrm{Gal}(L/K)$ eine weitere Untergruppe von $\mathrm{Gal}(L/K)$ und setzt man $H_i' = f_i(H')$, so folgt mit 4.1/4 oder 4.1/6, dass $L^H = L^{H'}$ äquivalent ist zu den Gleichungen $H_i = H_i'$, $i \in I$. Nun ist aber $H' := \bigcap_{i\in I} f_i^{-1}(H_i)$ offenbar die größte Untergruppe in $\mathrm{Gal}(L/K)$ mit $f_i(H') = H_i$ für alle $i \in I$, also mit $L^{H'} = L^H$. Folglich gilt $H' = \mathrm{Gal}(L/L^H)$.

Andererseits berechnet sich der Abschluss $\overline{H}$ von H gemäß Bemerkung 1 (iii) zu

$$\begin{aligned}\overline{H} &= \left\{\sigma \in \mathrm{Gal}\big(L/K\big)\ ;\ f_i^{-1}\big(f_i(\sigma)\big) \cap H \neq \emptyset \text{ für alle } i \in I\right\}\\ &= \left\{\sigma \in \mathrm{Gal}\big(L/K\big)\ ;\ f_i(\sigma) \in H_i \text{ für alle } i \in I\right\}\\ &= \bigcap_{i\in I} f_i^{-1}(H_i)\\ &= H',\end{aligned}$$

und es folgt, dass die Galois-Gruppe $\mathrm{Gal}(L/L^H)$ mit dem Abschluss der Untergruppe $H \subset \mathrm{Gal}(L/K)$ übereinstimmt. □

In der Situation von Satz 3 können die offenen Untergruppen von $\mathrm{Gal}(L/K)$ wie folgt charakterisiert werden:

Korollar 5. *Es sei L/K eine Galois-Erweiterung und H eine Untergruppe von* $\mathrm{Gal}(L/K)$. *Dann ist äquivalent*:

(i) *H ist offen in* $\mathrm{Gal}(L/K)$.

(ii) *H ist abgeschlossen in* $\mathrm{Gal}(L/K)$, *und der Fixkörper L^H ist endlich über K.*

Beweis. Sei zunächst H offen in $\mathrm{Gal}(L/K)$. Dann ist H auch abgeschlossen in $\mathrm{Gal}(L/K)$, denn mit H sind alle Links- bzw. Rechtsnebenklassen von H offen, also auch das Komplement von H in $\mathrm{Gal}(L/K)$. Weiter existiert aufgrund von Bemerkung 1 (i) eine endliche Galois-Erweiterung L'/K in L, so dass H den Kern der Restriktionsabbildung $\mathrm{Gal}(L/K) \longrightarrow \mathrm{Gal}(L'/K)$, also $\mathrm{Gal}(L/L')$ enthält. Mit Satz 3 folgt dann $L^H \subset L^{\mathrm{Gal}(L/L')} = L'$, und es ist L^H endlich über K, da dies für L' gilt.

Ist umgekehrt H abgeschlossen und L^H/K endlich, so können wir die normale Hülle $L' \subset L$ zu L^H/K betrachten. Diese ist ebenfalls endlich über K; vgl. 3.5/7. Es ist dann $\mathrm{Gal}(L/L')$ gemäß Bemerkung 1 (i) offen in $\mathrm{Gal}(L/K)$, und es gilt $\mathrm{Gal}(L/L') \subset \mathrm{Gal}(L/L^H) = H$, wiederum mit Satz 3. Insbesondere ist H offen in $\mathrm{Gal}(L/K)$. □

Bei der konkreten Untersuchung unendlicher Galois-Erweiterungen L/K ist es oftmals von Vorteil, die Galois-Gruppe $\mathrm{Gal}(L/K)$ als projektiven Limes über die endlichen Galois-Gruppen $\mathrm{Gal}(L_i/K)$ anzusehen, wobei wiederum $(L_i)_{i\in I}$ das System aller Zwischenkörper zu L/K bezeichne,

die endlich und galoissch über K sind. Wir wollen den Formalismus des projektiven Limes hier kurz erklären.

Wir gehen dazu von einer partiell geordneten Indexmenge I mit Ordnungsrelation $\leq$ aus; vgl. Abschnitt 3.4. Für jedes Paar von Indizes $i, j \in I$ mit $i \leq j$ habe man einen Homomorphismus von Gruppen $f_{ij} \colon G_j \longrightarrow G_i$, so dass gilt:

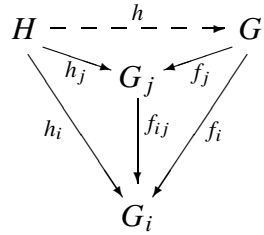
(i) $f_{ii} = \mathrm{id}_{G_i}$ für alle $i \in I$.

(ii) $f_{ik} = f_{ij} \circ f_{jk}$ falls $i \leq j \leq k$.

Ein solches System $(G_i, f_{ij})_{i,j \in I}$ heißt *projektives System* von Gruppen. In ähnlicher Weise definiert man auch projektive Systeme von Mengen oder von Mengen mit speziellen Strukturen. Beispielsweise verlangt man für ein projektives System von topologischen Gruppen, dass alle f_{ij} stetige Homomorphismen sind. Eine Gruppe G zusammen mit Homomorphismen $f_i \colon G \longrightarrow G_i$, so dass $f_i = f_{ij} \circ f_j$ für $i \leq j$ gilt, heißt *projektiver Limes* des Systems (G_i, f_{ij}), wenn folgende universelle Eigenschaft erfüllt ist:

Sind $h_i \colon H \longrightarrow G_i$, $i \in I$, Gruppenhomomorphismen, welche der Bedingung $h_i = f_{ij} \circ h_j$ für $i \leq j$ genügen, so existiert eindeutig ein Gruppenhomomorphismus $h \colon H \longrightarrow G$ mit $h_i = f_i \circ h$ für alle $i \in I$.

Die Bedingung wird durch folgendes kommutative Diagramm verdeutlicht:



Falls ein projektiver Limes G existiert, so ist er bis auf kanonische Isomorphie eindeutig bestimmt. Dies ist so wie bei jedem Objekt, das mit Hilfe einer universellen Eigenschaft definiert wird. Die Begründung ist wie folgt: Ist in obiger Situation neben (G, f_i) auch (H, h_i) ein projektiver Limes von (G_i, f_{ij}), so gibt es außer $h \colon H \longrightarrow G$ auch einen Homomorphismus $g \colon G \longrightarrow H$ mit den in obigem Diagramm ausgedrückten Verträglichkeiten. Nutzt man die Eindeutigkeitsbedingung in der Definition aus, so erkennt man, dass die Abbildungen $g \circ h, \mathrm{id}_H \colon H \longrightarrow H$ übereinstimmen, sowie ebenfalls die Abbildungen $h \circ g, \mathrm{id}_G \colon G \longrightarrow G$. Es sind also h und g invers zueinander. Man schreibt $G = \varprojlim_{i \in I} G_i$ für den projektiven Limes

des Systems (G_i, f_{ij}), wobei man die Homomorphismen f_i, sofern diese in offensichtlicher Weise definiert sind, meist nicht explizit angibt.

Ist (G_i, f_{ij}) ein projektives System *topologischer* Gruppen, und ist (G, f_i) ein projektiver Limes im Sinne gewöhnlicher Gruppen, so versehe man G mit der gröbsten Topologie, für die alle Homomorphismen f_i stetig sind. Dies ist diejenige Topologie, welche von allen Urbildern $f_i^{-1}(U)$ offener Mengen $U \subset G_i$ erzeugt wird; man spricht auch von dem *projektiven Limes* der Topologien auf den G_i. Unter dieser Topologie ist G ein projektiver Limes von (G_i, f_{ij}) im Sinne topologischer Gruppen.

Es sei am Rande erwähnt, dass es zum projektiven Limes als duale Notation den Begriff des *induktiven* (oder *direkten*) *Limes* $\varinjlim$ gibt. Man erhält die Definition eines induktiven Systems, bzw. eines induktiven Limes, indem man in den Definitionen für projektive Systeme bzw. Limiten die Richtung sämtlicher Abbildungspfeile umkehrt. Zusätzlich verlangt man noch, dass die Indexmenge I *gerichtet* ist in dem Sinne, dass es zu $i, j \in I$ stets einen Index $k \in I$ gibt mit $i, j \leq k$. Projektive und induktive Limiten von Gruppen (bzw. Mengen oder Ringen etc.) existieren stets, wie man leicht nachprüft. Wir interessieren uns hier nur für den projektiven Fall:

Bemerkung 6. *Es sei (G_i, f_{ij}) ein projektives System von Gruppen.*

(i) *Die Untergruppe*

$$G = \left\{(x_i)_{i\in I}\ ;\ f_{ij}(x_j) = x_i \text{ für } i \leq j\right\} \subset \prod_{i\in I} G_i,$$

zusammen mit den von den Projektionen auf die einzelnen Faktoren induzierten Gruppenhomomorphismen $f_i\colon G \longrightarrow G_i$ bildet einen projektiven Limes zu (G_i, f_{ij}).

Insbesondere definiert jedes System $(x_i)_{i\in I} \in \prod_{i\in I} G_i$ mit $f_{ij}(x_j) = x_i$ für $i \leq j$ eindeutig ein Element $x \in \varprojlim_{i\in I} G_i$.

(ii) *Ist (G_i, f_{ij}) ein projektives System topologischer Gruppen, und ist G wie in* (i), *so ist die Restriktion der Produkt-Topologie von $\prod_{i\in I} G_i$ auf G gerade der projektive Limes der Topologien auf den G_i.*

Zum *Beweis* verwendet man die universelle Eigenschaft des kartesischen Produkts, dass nämlich Gruppenhomomorphismen $H \longrightarrow \prod_{i\in I} G_i$ mittels Projektion von $\prod_{i\in I} G_i$ auf die Faktoren G_i in bijektiver Weise den Systemen von Gruppenhomomorphismen $(H \longrightarrow G_i)_{i\in I}$ entsprechen.

Im konkreten Fall einer Galois-Erweiterung L/K mit $\mathfrak{L} = (L_i)_{i\in I}$ als System der Zwischenkörper, die endlich und galoissch über K sind, führe man auf I eine partielle Ordnung ein, indem man $i \leq j$ durch $L_i \subset L_j$ erkläre. Weiter setze man $G_i = \mathrm{Gal}(L_i/K)$ für $i \in I$, und es sei $f_{ij}\colon \mathrm{Gal}(L_j/K) \longrightarrow \mathrm{Gal}(L_i/K)$ für $i \leq j$ jeweils die Restriktionsabbildung. Dann ist (G_i, f_{ij}) ein projektives System von Gruppen bzw. (diskreten) topologischen Gruppen, und es gilt:

Satz 7. *Die Restriktionsabbildungen* $f_i\colon \mathrm{Gal}(L/K) \longrightarrow \mathrm{Gal}(L_i/K)$ *definieren die Galois-Gruppe* $\mathrm{Gal}(L/K)$ *als projektiven Limes des Systems* $(\mathrm{Gal}(L_i/K), f_{ij})$, *also*

$$\mathrm{Gal}\big(L/K\big) = \varprojlim_{i\in I} \mathrm{Gal}\big(L_i/K\big).$$

Dies gilt im Sinne gewöhnlicher Gruppen wie auch im Sinne topologischer Gruppen.

Beweis. Es genügt, die definierende universelle Eigenschaft eines projektiven Limes gewöhnlicher Gruppen zu verifizieren; die Topologie auf $\mathrm{Gal}(L/K)$ stimmt dann per definitionem mit dem projektiven Limes der Topologien der Gruppen $\mathrm{Gal}(L_i/K)$ überein. Seien also $h_i\colon H \longrightarrow \mathrm{Gal}(L_i/K)$ Gruppenhomomorphismen, die mit den Einschränkungsabbildungen f_{ij} verträglich sind. Zum Nachweis der Eindeutigkeitsaussage betrachten wir einen Gruppenhomomorphismus $h\colon H \longrightarrow \mathrm{Gal}(L/K)$ mit $h_i = f_i \circ h$ für alle $i \in I$. Man wähle ein Element $x \in H$ und schreibe abkürzend $\sigma = h(x)$, $\sigma_i = h_i(x)$. Die Relation $h_i = f_i \circ h$ impliziert dann $\sigma_i = \sigma|_{L_i}$. Da L die Vereinigung der L_i ist, sieht man, dass $\sigma = h(x)$ eindeutig durch die $\sigma_i = h_i(x)$ bestimmt ist. Andererseits lässt sich diese Erkenntnis zur Konstruktion eines Homomorphismus $h\colon H \longrightarrow \mathrm{Gal}(L/K)$ der gewünschten Form ausnutzen. Sind nämlich die $\sigma_i = h_i(x)$ jeweils als Bild eines Elementes $x \in H$ gegeben, so zeigen die Relationen $h_i = f_{ij} \circ h_j$ für $i \leq j$, also für $L_i \subset L_j$, dass $\sigma_i = \sigma_j|_{L_i}$ gilt. Da $L = \bigcup_{i\in I} L_i$ und da es zu $i, j \in I$ stets ein $k \in I$ mit $i, j \leq k$, d. h. mit $L_i \cup L_j \subset L_k$ gibt, sieht man, dass sich die σ_i zu einem wohldefinierten Automorphismus $\sigma \in \mathrm{Gal}(L/K)$ zusammensetzen. Indem wir jeweils $x \in H$ auf das entsprechende $\sigma \in \mathrm{Gal}(L/K)$ abbilden, erhalten wir einen Gruppenhomomorphismus $h\colon H \longrightarrow \mathrm{Gal}(L/K)$ der gewünschten Art. Somit erfüllt $\mathrm{Gal}(L/K)$ die Eigenschaften eines projektiven Limes des Systems $(\mathrm{Gal}(L_i/K))_{i\in I}$. □

Man sagt in der Situation von Satz 7, $\mathrm{Gal}(L/K)$ sei eine *proendliche Gruppe*, also projektiver Limes von endlichen (diskreten) Gruppen. Es sei hier noch angemerkt, dass es zur Bestimmung des projektiven Limes eines projektiven Systems $(G_i, f_{ij})_{i,j\in I}$ mit *gerichteter* Indexmenge I ausreicht, diesen Limes über ein sogenanntes *kofinales Teilsystem* zu bilden. Dabei nennen wir ein Teilsystem $(G_i, f_{ij})_{i,j\in I'}$ von $(G_i, f_{ij})_{i,j\in I}$ kofinal, wenn es zu $i \in I$ stets ein $i' \in I'$ mit $i \leq i'$ gibt. Ist also $(L_i)_{i\in I'}$ ein Teilsystem des Systems $(L_i)_{i\in I}$ aller Zwischenkörper von L/K, die endlich und galoissch über K sind, und gibt es zu jedem $i \in I$ ein $i' \in I'$ mit $L_i \subset L_{i'}$, so ist $\mathrm{Gal}(L/K)$ bereits der projektive Limes über die Galois-Gruppen $\mathrm{Gal}(L_i/K)$, $i \in I'$. Dabei benutze man, dass die Indexmenge I in diesem Fall gerichtet ist, denn zu Indizes $i, j \in I$ gibt es stets einen Index $k \in I$ mit $L_i \cup L_j \subset L_k$.

Zum Abschluss wollen wir noch ein Beispiel für die Berechnung einer unendlichen Galois-Gruppe geben. Es sei p eine Primzahl und $\overline{\mathbb{F}}$ ein algebraischer Abschluss des Körpers $\mathbb{F}_p$ mit p Elementen. Jede endliche Erweiterung von $\mathbb{F}_p$ ist dann von der Form $\mathbb{F}_q$ mit einer Potenz $q = p^n$, vgl. 3.8/2, und wir können uns alle Körper $\mathbb{F}_q$ in $\overline{\mathbb{F}}$ eingebettet denken, vgl. 3.4/9 und 3.8/3. Für ein festes $q = p^n$ soll die Galois-Gruppe $\mathrm{Gal}(\overline{\mathbb{F}}/\mathbb{F}_q)$ berechnet werden, die sogenannte *absolute Galois-Gruppe* von $\mathbb{F}_q$. Hierzu betrachten wir das System aller endlichen Galois-Erweiterungen von $\mathbb{F}_q$, also nach 3.8/3 und 3.8/4 das System $(\mathbb{F}_{q^i})_{i\in\mathbb{N}-\{0\}}$. Dann gilt nach Satz 7

$$\mathrm{Gal}\big(\overline{\mathbb{F}}/\mathbb{F}_q\big) = \varprojlim_{i\in\mathbb{N}-\{0\}} \mathrm{Gal}\big(\mathbb{F}_{q^i}/\mathbb{F}_q\big).$$

Zur weiteren Berechnung studieren wir das projektive System von Galois-Gruppen auf der rechten Seite vorstehender Gleichung genauer. Hierzu bezeichne $\sigma\colon \overline{\mathbb{F}} \longrightarrow \overline{\mathbb{F}}$, $a \longmapsto (a^p)^n = a^q$, die n-te Potenz des Frobenius-Homomorphismus von $\overline{\mathbb{F}}$; ähnlich wie in Abschnitt 3.8 nennt man σ den *relativen Frobenius-Homomorphismus* über $\mathbb{F}_q$. Es ist $\mathbb{F}_q \subset \overline{\mathbb{F}}$ gerade der Zerfällungskörper des Polynoms $X^q - X$ über $\mathbb{F}_p$, vgl. 3.8/2, also der Fixkörper unter der von σ erzeugten zyklischen Untergruppe von $\mathrm{Gal}(\overline{\mathbb{F}}/\mathbb{F}_p)$. Die Restriktion von σ auf eine endliche Erweiterung $\mathbb{F}_{q^i}$ von $\mathbb{F}_q$ werde mit σ_i bezeichnet. Man sieht dann mit 3.8/3 bzw. 3.8/6:

Bemerkung 8. (i) *Es ist* $\mathrm{Gal}(\mathbb{F}_{q^i}/\mathbb{F}_q)$ *zyklisch von der Ordnung* i, *erzeugt von der Restriktion* σ_i *des relativen Frobenius-Homomorphismus über* $\mathbb{F}_q$.

(ii) *Es gilt* $\mathbb{F}_{q^i} \subset \mathbb{F}_{q^j}$ *genau dann, wenn* i *ein Teiler von* j *ist. Ist Letzteres der Fall, so bildet die Restriktion* $\mathrm{Gal}(\mathbb{F}_{q^j}/\mathbb{F}_q) \longrightarrow \mathrm{Gal}(\mathbb{F}_{q^i}/\mathbb{F}_q)$ *das erzeugende Element* σ_j *auf das erzeugende Element* σ_i *ab.*

Wir sehen also, dass wir zur Bestimmung von $\varprojlim \mathrm{Gal}(\mathbb{F}_{q^i}/\mathbb{F}_q)$ den projektiven Limes über das System $(\mathbb{Z}/i\mathbb{Z})_{i\in\mathbb{N}-\{0\}}$ bilden müssen. Dabei ist als Ordnungsrelation auf $\mathbb{N}-\{0\}$ die Teilbarkeitsrelation zu verwenden. Weiter betrachte man für $i \mid j$ als verbindenden Homomorphismus $f_{ij}\colon \mathbb{Z}/j\mathbb{Z} \longrightarrow \mathbb{Z}/i\mathbb{Z}$ denjenigen, der die Restklasse $\overline{1} \in \mathbb{Z}/j\mathbb{Z}$ auf die Restklasse $\overline{1} \in \mathbb{Z}/i\mathbb{Z}$ überführt. Somit folgt:

Satz 9. *Es existiert ein eindeutig bestimmter Isomorphismus topologischer Gruppen*

$$\mathrm{Gal}\big(\overline{\mathbb{F}}/\mathbb{F}_q\big) \simeq \varprojlim_{i\in\mathbb{N}-\{0\}} \mathbb{Z}/i\mathbb{Z},$$

unter welchem der relative Frobenius-Homomorphismus $\sigma \in \mathrm{Gal}(\overline{\mathbb{F}}/\mathbb{F}_q)$ *zu dem System der Restklassen* $\overline{1} \in \mathbb{Z}/i\mathbb{Z}$, $i \in \mathbb{N}-\{0\}$, *korrespondiert.*

Wir schreiben $\widehat{\mathbb{Z}} = \varprojlim_{i\in\mathbb{N}-\{0\}} \mathbb{Z}/i\mathbb{Z}$ (wobei wir diesen Limes auch als einen projektiven Limes von *Ringen* bzw. *topologischen Ringen*[2] auffassen können) und sehen, dass dies bis auf kanonische Isomorphie die absolute Galois-Gruppe eines jeden *endlichen* Körpers ist. Weiter ist $\mathbb{Z}$ in kanonischer Weise eine Untergruppe von $\widehat{\mathbb{Z}}$, denn die Projektionen $\mathbb{Z} \longrightarrow \mathbb{Z}/i\mathbb{Z}$ geben Anlass zu einem injektiven Homomorphismus $\mathbb{Z} \longrightarrow \widehat{\mathbb{Z}}$. Und zwar korrespondiert $\mathbb{Z}$ zu der vom relativen Frobenius-Homomorphismus $\sigma \in \mathrm{Gal}(\overline{\mathbb{F}}/\mathbb{F}_q)$ erzeugten freien zyklischen Gruppe $\langle\sigma\rangle$. Da die Projektionen $\mathbb{Z} \longrightarrow \mathbb{Z}/i\mathbb{Z}$ alle surjektiv sind, liegt $\mathbb{Z}$ dicht in $\widehat{\mathbb{Z}}$, und es erzeugt σ eine dichte Untergruppe in $\mathrm{Gal}(\overline{\mathbb{F}}/\mathbb{F}_q)$, d. h. eine Untergruppe, deren Abschluss bereits ganz $\mathrm{Gal}(\overline{\mathbb{F}}/\mathbb{F}_q)$ ist. Dies ergibt sich im Übrigen auch aus der Aussage von Lemma 4, da $\mathbb{F}_q$ als Fixkörper $\overline{\mathbb{F}}^{\langle\sigma\rangle}$ interpretiert werden kann. Wir werden im Weiteren sehen, dass $\mathbb{Z}$ eine echte Untergruppe von $\widehat{\mathbb{Z}}$ darstellt, ja dass $\mathbb{Z}$ sogar wesentlich "kleiner" als $\widehat{\mathbb{Z}}$ ist. Insbesondere folgt hieraus, dass der relative Frobenius-Homomorphismus σ eine Untergruppe in $\mathrm{Gal}(\overline{\mathbb{F}}/\mathbb{F}_q)$ erzeugt, die nicht abgeschlossen ist.

[2] Für einen topologischen Ring verlangt man, dass dieser bezüglich der Addition eine topologische Gruppe ist und dass außerdem die Ringmultiplikation stetig ist.

Es ist $\widehat{\mathbb{Z}}$, wie die Notation bereits andeutet, in gewisser Hinsicht als ein Abschluss des Ringes $\mathbb{Z}$ anzusehen, wobei allerdings auch andere Abschlüsse von $\mathbb{Z}$ denkbar sind. Beispielsweise kann man sich bei der Bildung des projektiven Limes der $\mathbb{Z}/i\mathbb{Z}$ darauf beschränken, die Zahl i nur in einer gewissen Teilmenge von $\mathbb{N} - \{0\}$ variieren zu lassen. Für eine Primzahl ℓ etwa bezeichnet man den projektiven Limes topologischer Ringe

$$\mathbb{Z}_\ell = \varprojlim_{\nu \in \mathbb{N}} \mathbb{Z}/\ell^\nu\mathbb{Z}$$

als Ring der *ganzen ℓ-adischen Zahlen*. In unserer Situation sind diese Ringe nützlich, da ihre Struktur einfacher zu beschreiben ist als diejenige von $\widehat{\mathbb{Z}}$, andererseits $\widehat{\mathbb{Z}}$ aber mit Hilfe der Ringe $\mathbb{Z}_\ell$ interpretiert werden kann:

Satz 10. *Es existiert ein kanonischer Isomorphismus von topologischen Ringen*

$$\widehat{\mathbb{Z}} = \varprojlim_{i \in \mathbb{N}-\{0\}} \mathbb{Z}/i\mathbb{Z} \simeq \prod_{\ell \text{ prim}} \mathbb{Z}_\ell.$$

Beweis. Wir zeigen, dass $P := \prod_{\ell \text{ prim}} \mathbb{Z}_\ell$, zusammen mit noch zu definierenden kanonischen Homomorphismen $f_i \colon P \longrightarrow \mathbb{Z}/i\mathbb{Z}$, die Eigenschaften eines projektiven Limes des Systems $(\mathbb{Z}/i\mathbb{Z})_{i \in \mathbb{N}-\{0\}}$ erfüllt. Sei $i \in \mathbb{N}-\{0\}$ mit Primfaktorzerlegung $i = \prod_\ell \ell^{\nu_\ell(i)}$, wobei natürlich fast alle Exponenten $\nu_\ell(i)$ verschwinden. Aufgrund des Chinesischen Restsatzes in der Version 2.4/14 ist der kanonische Homomorphismus

$$(*) \qquad \mathbb{Z}/i\mathbb{Z} \longrightarrow \prod_{\ell \text{ prim}} \mathbb{Z}/\ell^{\nu_\ell(i)}\mathbb{Z}$$

ein Isomorphismus, so dass wir einen kanonischen Homomorphismus

$$f_i \colon P \longrightarrow \prod_{\ell \text{ prim}} \mathbb{Z}/\ell^{\nu_\ell(i)}\mathbb{Z} \xrightarrow{\sim} \mathbb{Z}/i\mathbb{Z}$$

erhalten. Variiert i in $\mathbb{N}-\{0\}$, so sind die vorstehenden Homomorphismen $f_i \colon P \longrightarrow \mathbb{Z}/i\mathbb{Z}$ für $i \mid j$ mit den Projektionen $f_{ij} \colon \mathbb{Z}/j\mathbb{Z} \longrightarrow \mathbb{Z}/i\mathbb{Z}$ verträglich. Im Übrigen sieht man anhand der Definition der f_i, dass die Topologie von P gerade die gröbste Topologie ist, für die alle f_i stetig sind. Wir brauchen also lediglich noch zu zeigen, dass (P, f_i) ein projektiver Limes von $(\mathbb{Z}/i\mathbb{Z}, f_{ij})$ im Sinne gewöhnlicher Ringe ist.

Hierzu wähle man einen Ring R und betrachte für $i \in \mathbb{N} - \{0\}$ Ringhomomorphismen $h_i \colon R \longrightarrow \mathbb{Z}/i\mathbb{Z}$, die mit den f_{ij} verträglich sind. Indem man Isomorphismen des Typs $(*)$ benutzt, erhält man hieraus für jede Primzahl ℓ einen Homomorphismus $h_{i,\ell} \colon R \longrightarrow \mathbb{Z}/\ell^{\nu_\ell(i)}\mathbb{Z}$, wobei die $h_{i,\ell}$ mit den Restriktionshomomorphismen des projektiven Systems $(\mathbb{Z}/\ell^\nu\mathbb{Z})_{\nu\in\mathbb{N}}$ verträglich sind. Folglich definieren die $h_{i,\ell}$, wenn wir i variieren lassen, einen Ringhomomorphismus $h_\ell \colon R \longrightarrow \varprojlim_{\nu\in\mathbb{N}} \mathbb{Z}/\ell^\nu\mathbb{Z}$ und somit, wenn auch ℓ variiert, insgesamt einen Ringhomomorphismus $h \colon R \longrightarrow P$, welcher der Bedingung $h_i = f_i \circ h$ genügt. Nun sind aber die $h_{i,\ell}$ eindeutig durch die h_i bestimmt, und es folgt, dass auch h eindeutig durch die h_i bestimmt ist. □

Wir können also zusammenfassen:

Theorem 11. *Sei $\mathbb{F}$ ein endlicher Körper und $\overline{\mathbb{F}}$ ein algebraischer Abschluss. Dann existiert ein kanonischer Isomorphismus topologischer Gruppen*

$$\mathrm{Gal}\big(\overline{\mathbb{F}}/\mathbb{F}\big) \simeq \prod_{\ell \text{ prim}} \mathbb{Z}_\ell,$$

wobei der relative Frobenius-Homomorphismus $\sigma \in \mathrm{Gal}(\overline{\mathbb{F}}/\mathbb{F})$ zu dem Element $(1, 1, \ldots.) \in \prod_{\ell \text{ prim}} \mathbb{Z}_\ell$ korrespondiert. Hierbei sei 1 jeweils das Einselement in $\mathbb{Z}_\ell$, wenn wir $\mathbb{Z}_\ell$ als Ring auffassen.

Insbesondere ist hieraus abzulesen, dass die freie zyklische Untergruppe $\mathbb{Z} \subset \mathrm{Gal}(\overline{\mathbb{F}}/\mathbb{F})$, welche durch den relativen Frobenius-Homomorphismus σ erzeugt wird, "wesentlich kleiner" als die gesamte Galois-Gruppe ist. Es ist $\mathbb{Z}$ sogar "wesentlich kleiner" als der Ring der ganzen ℓ-adischen Zahlen $\mathbb{Z}_\ell$ für eine Primzahl ℓ. Man kann nämlich in einfacher Weise sehen (und dies rechtfertigt die Bezeichnung ℓ-adische Zahlen), dass die Elemente von $\mathbb{Z}_\ell$ bijektiv den formal gebildeten unendlichen Reihen $\sum_{\nu=0}^{\infty} c_\nu \ell^\nu$ mit ganzzahligen Koeffizienten c_ν, $0 \leq c_\nu \leq \ell - 1$, entsprechen. Damit ist $\mathbb{Z}_\ell$ überabzählbar, wie das von den reellen Zahlen bekannte Cantorsche Diagonalargument zeigt. Im Gegensatz dazu ist $\mathbb{Z}$ abzählbar.

Lernkontrolle und Prüfungsvorbereitung

1. Gib die Definition eines topologischen Raums X. Was versteht man unter den offenen bzw. abgeschlossenen Teilmengen von X? Wie ist der Abschluss

einer Teilmenge von X erklärt? Was versteht man für eine Teilmenge $V \subset X$ unter der von X auf V induzierten Topologie? Was ist eine stetige Abbildung topologischer Räume?

2. Es sei X eine Menge und $\mathfrak{B}$ ein System von Teilmengen von X. Wie ist die von $\mathfrak{B}$ auf X erzeugte Topologie erklärt?

3. Wie ist das Produkt einer Familie topologischer Räume erklärt?

4. Es sei L/K eine Galois-Erweiterung. Definiere die zugehörige Galois-Gruppe $\mathrm{Gal}(L/K)$ als topologische Gruppe. Charakterisiere insbesondere die offenen und die abgeschlossenen Teilmengen von $\mathrm{Gal}(L/K)$ sowie den Abschluss von Teilmengen $S \subset \mathrm{Gal}(L/K)$.

5. Zeige, dass eine Galois-Erweiterung L/K genau dann endlich ist, wenn die Topologie der zugehörigen Galois-Gruppe $\mathrm{Gal}(L/K)$ diskret ist.

+6. Zeige für eine Galois-Erweiterung L/K, dass die zugehörige Galois-Gruppe $\mathrm{Gal}(L/K)$ kompakt und total unzusammenhängend ist.

7. Zeige für eine Galois-Erweiterung L/K, dass eine Untergruppe $H \subset \mathrm{Gal}(L/K)$ genau dann abgeschlossen ist, wenn $H = \mathrm{Gal}(L/L^H)$ gilt.

8. Formuliere den Hauptsatz der Galois-Theorie für beliebige Galois-Erweiterungen L/K.

9. Es sei L/K eine Galois-Erweiterung und $H \subset \mathrm{Gal}(L/K)$ eine Untergruppe. Zeige: Ist H offen in $\mathrm{Gal}(L/K)$, so auch abgeschlossen und weiter, dass H genau dann offen in $\mathrm{Gal}(L/K)$ ist, wenn H abgeschlossen ist und der Fixkörper L^H endlich über K ist.

10. Erkläre den Formalismus projektiver Systeme und projektiver Limiten von Gruppen. Zeige, dass ein projektives System von Gruppen bzw. topologischen Gruppen stets einen projektiven Limes besitzt.

11. Zeige für eine Galois-Erweiterung L/K, dass sich die Galois-Gruppe $\mathrm{Gal}(L/K)$ als projektiver Limes von Galois-Gruppen des Typs $\mathrm{Gal}(L'/K)$ interpretieren lässt, wobei L' alle Zwischenkörper von L/K durchläuft, die endlich und galoissch über K sind.

+12. Bestimme die absolute Galois-Gruppe $\mathrm{Gal}(\overline{\mathbb{F}}/\mathbb{F})$ eines endlichen Körpers $\mathbb{F}$.

+13. Definiere den Ring $\mathbb{Z}_\ell$ der ganzen ℓ-adischen Zahlen für eine Primzahl ℓ. Stelle einen Zusammenhang her zwischen den Ringen $\mathbb{Z}_\ell$ für $\ell \in \mathbb{N}$ prim und der absoluten Galois-Gruppe eines endlichen Körpers $\mathbb{F}$.

Übungsaufgaben

1. *Präzisiere noch einmal die grundlegende Idee, welche in relativ einfacher Weise eine Verallgemeinerung des Hauptsatzes der Galois-Theorie auf unendliche Galois-Erweiterungen möglich macht.*
2. *Überlege, warum man unendliche Galois-Gruppen nicht als rein abstrakte Gruppen, sondern eher als topologische bzw. proendliche Gruppen sehen sollte.*
3. Es sei X eine Menge, weiter sei $(X_i)_{i\in I}$ ein System von Teilmengen von X. Für Indizes $i, j \in I$ mit $X_j \subset X_i$ bezeichne f_{ij} die Inklusionsabbildung $X_j \longrightarrow X_i$.
   (i) Schreibe $i \leq j$, falls $X_j \subset X_i$, und zeige: (X_i, f_{ij}) ist ein projektives System von Mengen, und es gilt: $\varprojlim_{i\in I} X_i = \bigcap_{i\in I} X_i$.
   (ii) Schreibe $i \leq j$, falls $X_i \subset X_j$, und nimm an, dass die Indexmenge I bezüglich $\leq$ gerichtet ist. (Letzteres ist in diesem Zusammenhang allerdings ohne Bedeutung.) Zeige, dass (X_i, f_{ji}) ein induktives System von Mengen ist und dass gilt: $\varinjlim_{i\in I} X_i = \bigcup_{i\in I} X_i$.
4. Zeige, dass jedes induktive System von Gruppen einen (induktiven) Limes besitzt.
5. Es sei K ein Körper sowie $\overline{K}$ ein algebraischer Abschluss von K. Zeige, dass die absolute Galois-Gruppe $\mathrm{Gal}(\overline{K}/K)$ bis auf Isomorphie nicht von der Wahl von $\overline{K}$ abhängt.
6. Es sei L/K eine Körpererweiterung und $(L_i)_{i\in I}$ ein System von Zwischenkörpern, so dass L_i galoissch über K ist und es zu $i, j \in I$ jeweils ein $k \in I$ mit $L_i \cup L_j \subset L_k$ gibt. Weiter sei L' der kleinste Teilkörper von L, welcher alle L_i enthält. Zeige, dass L'/K galoissch ist und dass $\mathrm{Gal}(L'/K) = \varprojlim \mathrm{Gal}(L_i/K)$ im Sinne topologischer Gruppen gilt.
7. Es sei L/K eine Galois-Erweiterung sowie E ein Zwischenkörper mit der Eigenschaft, dass auch E/K galoissch ist. Zeige:
   (i) Die Restriktionsabbildung $\varphi\colon\ \mathrm{Gal}(L/K) \longrightarrow \mathrm{Gal}(E/K)$ ist stetig.
   (ii) Es trägt $\mathrm{Gal}(E/K)$ die Quotiententopologie bezüglich φ, d. h. eine Teilmenge $V \subset \mathrm{Gal}(E/K)$ ist genau dann offen, wenn $\varphi^{-1}(V)$ offen in $\mathrm{Gal}(L/K)$ ist.
8. Kann es eine Galois-Erweiterung L/K mit $\mathrm{Gal}(L/K) \simeq \mathbb{Z}$ geben?
9. Betrachte die Situation von Theorem 11 und bestimme
   (i) für eine Primzahl ℓ den Fixkörper zu $\mathbb{Z}_\ell$, aufgefasst als Untergruppe von $\mathrm{Gal}(\overline{\mathbb{F}}/\mathbb{F})$, sowie
   (ii) alle Zwischenkörper von $\overline{\mathbb{F}}/\mathbb{F}$.

10. Betrachte für eine Primzahl ℓ den Ring $\mathbb{Z}_\ell = \varprojlim_\nu \mathbb{Z}/\ell^\nu\mathbb{Z}$ der ganzen ℓ-adischen Zahlen. Für ein Element $a \in \mathbb{Z}_\ell$ bezeichne $v(a)$ das Maximum aller Zahlen $\nu \in \mathbb{N}$, so dass die Restklasse von a in $\mathbb{Z}/\ell^\nu\mathbb{Z}$ verschwindet; setze $v(a) = \infty$ für $a = 0$. Definiere weiter den sogenannten *ℓ-adischen Betrag* von a durch $|a|_\ell = \ell^{-v(a)}$ und zeige für $a, b \in \mathbb{Z}_\ell$:

    (i) $|a|_\ell = 0 \iff a = 0$,

    (ii) $|a \cdot b|_\ell = |a|_\ell \cdot |b|_\ell$,

    (iii) $|a + b|_\ell \le \max\{|a|_\ell, |b|_\ell\}$.

11. Beweise, dass der ℓ-adische Betrag $|\cdot|_\ell$ aus Aufgabe 10 die Topologie von $\mathbb{Z}_\ell$ definiert (in dem Sinne, dass eine Teilmenge $U \subset \mathbb{Z}_\ell$ genau dann offen ist, wenn es zu jedem Punkt von U eine ℓ-adische ε-Umgebung gibt, die noch ganz in U enthalten ist). Beweise weiter die Gleichung $(1-\ell)^{-1} = \sum_{i=0}^{\infty} \ell^i$, wobei die Konvergenz in nahe liegender Weise bezüglich des ℓ-adischen Betrags zu verstehen ist. Mit einem ähnlichen Argument kann man zeigen, dass jedes $a \in \mathbb{Z}_\ell$ mit $|a|_\ell = 1$ Einheit in $\mathbb{Z}_\ell$ ist.

4.3 Die Galois-Gruppe einer Gleichung

Es sei K ein Körper und $f \in K[X]$ ein nicht-konstantes Polynom. Weiter sei L ein Zerfällungskörper von f über K. Ist dann f separabel, so ist L/K eine endliche Galois-Erweiterung, und man nennt $\mathrm{Gal}(L/K)$ die Galois-Gruppe von f über K bzw., in suggestiver Terminologie, die Galois-Gruppe der Gleichung $f(x) = 0$.

Satz 1. *Es sei $f \in K[X]$ ein separables Polynom vom Grade $n > 0$ mit Zerfällungskörper L über K. Sind dann $\alpha_1, \ldots, \alpha_n \in L$ die Nullstellen von f, so definiert*

$$\begin{aligned} \varphi\colon \mathrm{Gal}\big(L/K\big) &\longrightarrow S\big(\{\alpha_1, \ldots, \alpha_n\}\big) \simeq \mathfrak{S}_n, \\ \sigma &\longmapsto \sigma|_{\{\alpha_1,\ldots,\alpha_n\}}, \end{aligned}$$

einen injektiven Gruppenhomomorphismus der Galois-Gruppe zu L/K in die Gruppe der Permutationen von $\alpha_1, \ldots, \alpha_n$, bzw. in die Gruppe $\mathfrak{S}_n$ der Permutationen von n Elementen. Auf diese Weise lässt sich $\mathrm{Gal}(L/K)$ als Untergruppe von $\mathfrak{S}_n$ auffassen, und man sieht, dass $[L : K] = \mathrm{ord}\,\mathrm{Gal}(L/K)$ ein Teiler von $\mathrm{ord}\,\mathfrak{S}_n = n!$ ist.

f ist genau dann irreduzibel, wenn $\mathrm{Gal}(L/K)$ transitiv *auf der Menge der Nullstellen* $\{\alpha_1, \ldots, \alpha_n\}$ *operiert, d. h. wenn es zu je zwei dieser Nullstellen* α_i, α_j *einen Automorphismus* $\sigma \in \mathrm{Gal}(L/K)$ *mit* $\sigma(\alpha_i) = \alpha_j$ *gibt. Insbesondere ist dies der Fall für* $[L : K] = n!$ *bzw. für* $\mathrm{Gal}(L/K) \simeq \mathfrak{S}_n$.

Beweis. Sei $\sigma \in \mathrm{Gal}(L/K)$. Da σ die Koeffizienten von f festlässt, bildet σ Nullstellen von f wieder auf Nullstellen von f ab. Da weiter σ injektiv ist, induziert es auf $\{\alpha_1, \ldots, \alpha_n\}$ eine injektive und damit bijektive Selbstabbildung, also eine Permutation. Dies bedeutet, dass die Abbildung φ wohldefiniert ist. Im Übrigen ist φ injektiv, denn ein K-Homomorphismus aus $\mathrm{Gal}(L/K)$ ist wegen $L = K(\alpha_1, \ldots, \alpha_n)$ bereits eindeutig durch seine Werte auf den Elementen $\alpha_1, \ldots, \alpha_n$ bestimmt.

Nehmen wir nun f als irreduzibel an, so existiert gemäß 3.4/8 zu je zwei Nullstellen α_i, α_j von f ein K-Homomorphismus $\sigma\colon K(\alpha_i) \longrightarrow K(\alpha_j)$ mit $\sigma(\alpha_i) = \alpha_j$. Dieser setzt sich nach 3.4/9 zu einem K-Homomorphismus $\sigma'\colon L \longrightarrow \overline{L}$ fort; $\overline{L}$ sei ein algebraischer Abschluss von L. Da die Erweiterung L/K aber normal ist, beschränkt sich σ' zu einem K-Automorphismus von L, also zu einem Element $\sigma'' \in \mathrm{Gal}(L/K)$, und es gilt nach Konstruktion $\sigma''(\alpha_i) = \alpha_j$.

Ist andererseits f reduzibel und $f = gh$ eine echte Zerlegung in $K[X]$, so bildet jedes $\sigma \in \mathrm{Gal}(L/K)$ die Nullstellen von g bzw. h wieder in sich ab. Da aber f nach Voraussetzung separabel ist, müssen die Nullstellen von g paarweise verschieden von denjenigen von h sein, und es folgt, dass σ nicht transitiv auf der Menge der Nullstellen von f operieren kann. □

Da jede endliche Galois-Erweiterung L/K aufgrund des Satzes vom primitiven Element 3.6/12 einfach ist und L somit Zerfällungskörper eines Polynoms aus $K[X]$ vom Grad $n = [L : K]$ ist, folgt insbesondere:

Korollar 2. *Ist L/K eine endliche Galois-Erweiterung vom Grad n, so lässt sich* $\mathrm{Gal}(L/K)$ *als Untergruppe der Permutationsgruppe* $\mathfrak{S}_n$ *auffassen.*

Man sieht hierbei auch, dass die Galois-Gruppe $\mathrm{Gal}(L/K)$ in der Situation von Satz 1 im Allgemeinen eine echte Untergruppe von $\mathfrak{S}_n$ ist. Ist nämlich $f \in K[X]$ das Minimalpolynom eines primitiven Elements zu L/K und n sein Grad, so gilt für $n > 2$ die Abschätzung $\mathrm{ord}(\mathrm{Gal}(L/K)) = n < n! = \mathrm{ord}\,\mathfrak{S}_n$. Daher gibt es im Rahmen von Satz 1 in

der Regel Permutationen der Nullstellen von f, die nicht zu einem Galois-Automorphismus von L/K korrespondieren.

Wir wollen nun in einigen speziellen Fällen die Galois-Gruppe eines Polynoms $f \in K[X]$ berechnen.

(1) Man betrachte $f = X^2 + aX + b \in K[X]$, wobei f keine Nullstelle in K habe. Dann ist f irreduzibel in $K[X]$ und, sofern $\operatorname{char} K \neq 2$ oder $a \neq 0$ gilt, auch separabel. Adjungieren wir zu K eine Nullstelle α von f, so ist der resultierende Körper $L = K(\alpha)$ bereits ein Zerfällungskörper von f über K, d. h. L/K ist eine Galois-Erweiterung vom Grad 2. Die Galois-Gruppe $\operatorname{Gal}(L/K)$ hat die Ordnung 2 und ist notwendigerweise zyklisch.

(2) Es sei $\operatorname{char} K \neq 2, 3$ und $f = X^3 + aX + b \in K[X]$. Jedes andere normierte Polynom dritten Grades $X^3 + c_1X^2 + \ldots \in K[X]$ lässt sich durch die Substitution $X \longmapsto X - c$ mit $c = \frac{1}{3}c_1$ auf die obige Gestalt bringen; Zerfällungskörper sowie Galois-Gruppe des Polynoms ändern sich dabei nicht. Wir nehmen an, dass f keine Nullstelle in K hat. Dann ist f irreduzibel in $K[X]$ und aufgrund der Voraussetzung über $\operatorname{char} K$ auch separabel. Sei L ein Zerfällungskörper von f über K und $\alpha \in L$ eine Nullstelle von f. Es ist $K(\alpha)/K$ eine Erweiterung vom Grad 3, und für den Grad $[L : K]$ ergeben sich die Werte 3 oder 6, je nachdem ob $K(\alpha)$ bereits ein Zerfällungskörper von f ist oder nicht. Entsprechend ist $\operatorname{Gal}(L/K)$ von der Ordnung 3 oder 6, wobei wir diese Gruppe gemäß Satz 1 als Untergruppe von $\mathfrak{S}_3$ auffassen wollen. Im ersten Fall ist $\operatorname{Gal}(L/K)$ zyklisch von der Ordnung 3; jedes von der Identität verschiedene Element $\sigma \in \operatorname{Gal}(L/K)$ ist ein erzeugendes Element, da aus $\operatorname{ord}\sigma > 1$ und $(\operatorname{ord}\sigma)|3$ schon $\operatorname{ord}\sigma = 3$ folgt. Im zweiten Fall ergibt sich $\operatorname{Gal}(L/K) = \mathfrak{S}_3$ wegen $\operatorname{ord}\operatorname{Gal}(L/K) = 6 = \operatorname{ord}\mathfrak{S}_3$.

Wir wollen eine Methode angeben, um zu testen, welcher der beiden Fälle vorliegt. Sind $\alpha_1, \alpha_2, \alpha_3 \in L$ die Nullstellen von f, so setze man

$$\delta = (\alpha_1 - \alpha_2)(\alpha_2 - \alpha_3)(\alpha_1 - \alpha_3).$$

Man nennt $\Delta = \delta^2$ die *Diskriminante* des Polynoms f; vgl. auch Abschnitt 4.4. Da Δ unter den Automorphismen aus $\operatorname{Gal}(L/K)$ invariant bleibt, hat man $\Delta \in K$; eine leichte Rechnung ergibt in unserem speziellen Fall

$$\Delta = -4a^3 - 27b^2.$$

Wendet man einen Automorphismus $\sigma \in \operatorname{Gal}(L/K)$ auf δ an, so ändern sich bei den Faktoren von δ möglicherweise die Vorzeichen. Es gilt daher

$\sigma(\delta) = \pm\delta$, je nachdem ob σ zu einer geraden oder ungeraden Permutation in $\mathfrak{S}_3$ korrespondiert. (Eine Permutation $\pi \in \mathfrak{S}_n$ heißt gerade bzw. ungerade, falls

$$\operatorname{sgn}(\pi) = \prod_{i<j} \frac{\pi(i) - \pi(j)}{i - j},$$

das Signum von π, den Wert 1 bzw. -1 hat; die Funktion sgn ist multiplikativ, d. h. es gilt $\operatorname{sgn}(\pi \circ \pi') = \operatorname{sgn}(\pi) \cdot \operatorname{sgn}(\pi')$ für $\pi, \pi' \in \mathfrak{S}_n$; vgl. auch 5.3.)

Die geraden Permutationen in $\mathfrak{S}_n$ bilden eine Untergruppe, die sogenannte alternierende Gruppe $\mathfrak{A}_n$. Es ist $\mathfrak{A}_n$ als Kern des surjektiven Gruppenhomomorphismus

$$\mathfrak{S}_n \longrightarrow \{1, -1\}, \qquad \pi \longmapsto \operatorname{sgn}(\pi),$$

für $n > 1$ ein Normalteiler vom Index 2 in $\mathfrak{S}_n$. Außerdem sieht man, dass alle Permutationen $\pi \in \mathfrak{S}_n$, deren Ordnung ungerade ist, zu $\mathfrak{A}_n$ gehören müssen. Insbesondere ist $\mathfrak{A}_3$ die einzige Untergruppe von $\mathfrak{S}_3$ der Ordnung 3. Somit gelten folgende Äquivalenzen:

$$\begin{aligned}
& \operatorname{ord} \operatorname{Gal}(L/K) = 3 \\
\iff\ & \operatorname{Gal}(L/K) \subset \mathfrak{S}_3 \text{ besteht nur aus geraden Permutationen} \\
\iff\ & \delta \in K \\
\iff\ & \Delta \text{ besitzt eine Quadratwurzel in } K
\end{aligned}$$

Man kann also entscheiden, ob $\operatorname{Gal}(L/K)$ die Ordnung 3 oder 6 hat, indem man testet, ob die Diskriminante eine Quadratwurzel in K besitzt oder nicht.

Beispielsweise ist $f = X^3 - X + 1 \in \mathbb{Q}[X]$ irreduzibel (da f in $\mathbb{Z}[X]$ keinen linearen Faktor abspaltet). Für einen Zerfällungskörper L von f über $\mathbb{Q}$ gilt $\operatorname{Gal}(L/\mathbb{Q}) = \mathfrak{S}_3$, da $\sqrt{\Delta} = \sqrt{-23} \notin \mathbb{Q}$.

(3) Schließlich wollen wir noch einige spezielle irreduzible Polynome 4. Grades betrachten, und zwar irreduzible normierte Polynome $f \in \mathbb{Q}[X]$, deren lineare und kubische Terme trivial sind. Jedes solche Polynom lässt sich in der Form $f = (X^2 - a)^2 - b$ schreiben, wobei wir zunächst $b > a^2$ voraussetzen wollen. Als konkrete Beispiele mögen die Polynome $X^4 - 2$ oder $X^4 - 4X^2 - 6$ dienen. Die Nullstellen von f in $\mathbb{C}$ sind

$$\alpha = \sqrt{a + \sqrt{b}}, \qquad -\alpha, \qquad \beta = \sqrt{a - \sqrt{b}}, \qquad -\beta,$$

wobei zu beachten ist, dass aufgrund unserer Voraussetzung $\sqrt{b} > |a|$ gilt, also α reell ist, im Gegensatz zu β als Quadratwurzel einer negativen reellen Zahl. Der Zerfällungskörper von f in $\mathbb{C}$ ist $L = \mathbb{Q}(\alpha, \beta)$, und wir wollen zunächst den Grad $[L : \mathbb{Q}]$ bestimmen. Es hat α als Nullstelle von f den Grad 4 über $\mathbb{Q}$, also gilt $[\mathbb{Q}(\alpha) : \mathbb{Q}] = 4$. Weiter ist β als Quadratwurzel des Elementes $a - \sqrt{b} \in \mathbb{Q}(\alpha)$ vom Grad ≤ 2 über $\mathbb{Q}(\alpha)$. Da $\mathbb{Q}(\alpha)$ in $\mathbb{R}$ enthalten ist, nicht aber β, ist β notwendig vom Grad 2 über $\mathbb{Q}(\alpha)$, und es ergibt sich $[L : \mathbb{Q}] = [\mathbb{Q}(\alpha, \beta) : \mathbb{Q}] = 8$.

Es soll nun die Galois-Gruppe $\mathrm{Gal}(L/\mathbb{Q})$ berechnet werden. Dazu fassen wir $\mathrm{Gal}(L/\mathbb{Q})$ im Sinne von Satz 1 als Untergruppe der Permutationsgruppe $S(\{\alpha, -\alpha, \beta, -\beta\})$ der Nullstellen von f auf. Wir wissen bereits, dass $L/\mathbb{Q}$ den Grad 8 hat, $\mathrm{Gal}(L/\mathbb{Q})$ also die Ordnung 8 besitzt. Weiter erfüllt jedes $\sigma \in \mathrm{Gal}(L/\mathbb{Q})$ als Körperhomomorphismus die Relationen $\sigma(-\alpha) = -\sigma(\alpha), \sigma(-\beta) = -\sigma(\beta)$. Nun gibt es aber gerade 8 Permutationen in $S(\{\alpha, -\alpha, \beta, -\beta\})$, welche diese Bedingungen erfüllen. Denn will man eine solche Permutation definieren, so hat man zur Festlegung von $\sigma(\alpha)$ insgesamt 4 Möglichkeiten, wobei $\sigma(-\alpha)$ durch die Relation $\sigma(-\alpha) = -\sigma(\alpha)$ erklärt werden muss. Sodann bleiben zur Festlegung von $\sigma(\beta)$ noch 2 Möglichkeiten, wobei wiederum $\sigma(-\beta)$ durch die Relation $\sigma(-\beta) = -\sigma(\beta)$ festgelegt ist. Damit gibt es genau 8 Permutationen in $S(\{\alpha, -\alpha, \beta, -\beta\})$, welche die Relationen $\sigma(-\alpha) = -\sigma(\alpha)$, $\sigma(-\beta) = -\sigma(\beta)$ erfüllen, und es folgt, dass dies gerade die Elemente von $\mathrm{Gal}(L/\mathbb{Q})$ sind. Um die Gruppe $\mathrm{Gal}(L/\mathbb{Q})$ explizit zu beschreiben, betrachte man die beiden Elemente $\sigma, \tau \in \mathrm{Gal}(L/\mathbb{Q})$, welche durch

$$\begin{aligned} \sigma: &\quad \alpha \longmapsto \beta, \quad \beta \longmapsto -\alpha, \\ \tau: &\quad \alpha \longmapsto -\alpha, \quad \beta \longmapsto \beta \end{aligned}$$

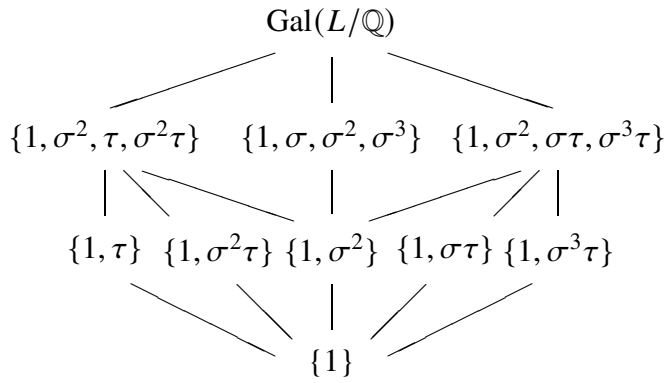
gegeben sind. Die von σ erzeugte Untergruppe $\langle\sigma\rangle \subset \mathrm{Gal}(L/\mathbb{Q})$ ist zyklisch von der Ordnung 4, somit also Normalteiler in $\mathrm{Gal}(L/\mathbb{Q})$, da vom Index 2. Weiter hat τ die Ordnung 2. Da $\tau \notin \langle\sigma\rangle$, ergibt sich

$$\mathrm{Gal}(L/\mathbb{Q}) = \langle\sigma, \tau\rangle = \langle\sigma\rangle \cup \tau\langle\sigma\rangle = \langle\sigma\rangle \cup \langle\sigma\rangle\tau,$$

bzw. in noch expliziterer Schreibweise

$$\mathrm{Gal}(L/\mathbb{Q}) = \{1, \sigma, \sigma^2, \sigma^3, \tau, \sigma\tau, \sigma^2\tau, \sigma^3\tau\}.$$

Zur Beschreibung der Gruppenstruktur in $\mathrm{Gal}(L/\mathbb{Q})$ genügt es nachzuprüfen, dass σ und τ die Relation $\tau\sigma = \sigma^3\tau$ erfüllen. Es lassen sich nun leicht alle Untergruppen von $\mathrm{Gal}(L/\mathbb{Q})$ angeben, man hat folgendes Schema:



Aufgrund des Hauptsatzes der Galois-Theorie 4.1/6 entsprechen die Untergruppen von $\mathrm{Gal}(L/\mathbb{Q})$ eindeutig den Zwischenkörpern von $L/\mathbb{Q}$. Letztere lassen sich bestimmen, indem man geeignete Elemente vom Grad 2 oder 4 in L betrachtet, die unter obigen Gruppen invariant sind.

Als Gegenstück zu vorstehender Situation wollen wir noch die Galois-Gruppe des Polynoms $f = X^4 - 4X^2 + 16 \in \mathbb{Q}[X]$ berechnen. Auch in diesem Fall ist f von der Form $(X^2-a)^2-b$, wobei aber $a = 2$ und $b = -12$ nicht die obige Abschätzung $b > a^2$ erfüllen. Die Nullstellen von f in $\mathbb{C}$ berechnen sich zu

$$\alpha = 2e^{2\pi i/12}, \qquad -\alpha, \qquad \beta = 2e^{-2\pi i/12}, \qquad -\beta,$$

bzw.

$$2\zeta, \qquad 2\zeta^7, \qquad 2\zeta^{11}, \qquad 2\zeta^5,$$

wobei $\zeta = e^{2\pi i/12}$ als Quadratwurzel von $\frac{1}{2}+\frac{1}{2}i\sqrt{3}$ und entsprechend $e^{-2\pi i/12}$ als Quadratwurzel von $\frac{1}{2} - \frac{1}{2}i\sqrt{3}$ anzusehen ist. Adjungieren wir daher eine Nullstelle von f zu $\mathbb{Q}$, etwa α, so folgt, dass $L = \mathbb{Q}(\alpha) = \mathbb{Q}(\zeta)$ Zerfällungskörper von f über $\mathbb{Q}$ ist. Somit hat die Galois-Gruppe von $L/\mathbb{Q}$ die Ordnung 4. Die einzelnen Automorphismen werden beschrieben durch

$$\begin{aligned}
\sigma_1 &: \quad \zeta \longmapsto \zeta, \\
\sigma_2 &: \quad \zeta \longmapsto \zeta^5, \\
\sigma_3 &: \quad \zeta \longmapsto \zeta^7, \\
\sigma_4 &: \quad \zeta \longmapsto \zeta^{11},
\end{aligned}$$

mit den Relationen $\sigma_1 = \mathrm{id}$, $\sigma_2^2 = \sigma_3^2 = \sigma_4^2 = \mathrm{id}$ sowie $\sigma_2 \circ \sigma_3 = \sigma_4$, wobei $\mathrm{Gal}(L/\mathbb{Q})$ kommutativ ist. Es folgt $\mathrm{Gal}(L/\mathbb{Q}) \simeq \mathbb{Z}/2\mathbb{Z}\times\mathbb{Z}/2\mathbb{Z}$. In $\mathrm{Gal}(L/\mathbb{Q})$

gibt es außer den trivialen Untergruppen lediglich die Untergruppen $\langle\sigma_2\rangle$, $\langle\sigma_3\rangle$, $\langle\sigma_4\rangle$, welche im Sinne des Hauptsatzes der Galois-Theorie 4.1/6 zu den Zwischenkörpern $\mathbb{Q}(\zeta^3), \mathbb{Q}(\zeta^2), \mathbb{Q}(\sqrt{3})$ von $L/\mathbb{Q}$ korrespondieren; man beachte $\sqrt{3} = \zeta + \zeta^{11}$. Bis auf die trivialen Zwischenkörper $\mathbb{Q}$ und L sind dies also die einzigen Zwischenkörper von $L/\mathbb{Q}$. Erweiterungen des Typs $L/\mathbb{Q}$ werden wir in Abschnitt 4.5 noch ausführlicher studieren. Es entsteht L aus $\mathbb{Q}$ durch Adjunktion einer sogenannten *primitiven* 12-ten Einheitswurzel ζ und wird entsprechend als *Kreisteilungskörper* bezeichnet.

(4) Als letztes Beispiel wollen wir die sogenannte *allgemeine Gleichung* n-ten Grades behandeln. Hierzu wählen wir einen Körper k und betrachten darüber den Körper L der rationalen Funktionen in endlich vielen Variablen $T_1, \ldots, T_n$, also

$$L = k(T_1, \ldots, T_n) = Q\big(k[T_1, \ldots, T_n]\big).$$

Jede Permutation $\pi \in \mathfrak{S}_n$ definiert einen Automorphismus von L, indem man π auf die Variablen $T_1, \ldots, T_n$ anwendet:

$$\begin{aligned} k(T_1, \ldots, T_n) &\longrightarrow k(T_1, \ldots, T_n), \\ \frac{g(T_1, \ldots, T_n)}{h(T_1, \ldots, T_n)} &\longmapsto \frac{g(T_{\pi(1)}, \ldots, T_{\pi(n)})}{h(T_{\pi(1)}, \ldots, T_{\pi(n)})}. \end{aligned}$$

Der zugehörige Fixkörper $K = L^{\mathfrak{S}_n}$ heißt Körper der *symmetrischen rationalen Funktionen* in n Variablen mit Koeffizienten in k. Es ist L/K nach 4.1/4 eine Galois-Erweiterung vom Grad $n!$ mit Galois-Gruppe $\mathfrak{S}_n$.

Um die "Gleichung" der Erweiterung L/K angeben zu können, wählen wir eine Polynomvariable X und betrachten das Polynom

$$\begin{aligned} f(X) &= \prod_{i=1}^{n} (X - T_i) \\ &= \sum_{j=0}^{n} (-1)^j \cdot s_j(T_1, \ldots, T_n) \cdot X^{n-j} \in k[T_1, \ldots, T_n][X]. \end{aligned}$$

Dabei heißt s_j, gewonnen durch Ausmultiplizieren der Faktoren $X - T_i$ und durch Sammeln der Koeffizienten von $(-1)^j X^{n-j}$, das *j-te elementarsymmetrische Polynom* (bzw. die *j-te elementarsymmetrische Funktion*) in $T_1, \ldots, T_n$, wobei

$$
\begin{aligned}
s_0 &= 1,\\
s_1 &= T_1 + \ldots + T_n,\\
s_2 &= T_1T_2 + T_1T_3 + \ldots + T_{n-1}T_n,\\
&\ldots\\
s_n &= T_1 \ldots T_n.
\end{aligned}
$$

Als Polynom in $L[X]$ hat f bereits Koeffizienten in K, da f durch die Aktion von $\mathfrak{S}_n$ invariant gelassen wird. Sodann folgt $k(s_1, \ldots, s_n) \subset K$, und es ist L ein Zerfällungskörper von f über $k(s_1, \ldots, s_n)$ bzw. K. Im Übrigen schließt man mittels Satz 1 aus grad $f = n$ und $[L : K] = n!$, dass f *irreduzibel* in $K[X]$ ist.

Satz 3. *Jede symmetrische rationale Funktion aus $L = k(T_1, \ldots, T_n)$ lässt sich über k auf genau eine Weise als rationale Funktion in den elementarsymmetrischen Polynomen $s_1, \ldots, s_n$ darstellen. Mit anderen Worten, es gilt*:

(i) $K = L^{\mathfrak{S}_n} = k(s_1, \ldots, s_n)$.

(ii) *$s_1, \ldots, s_n$ sind algebraisch unabhängig über k.*

Beweis. Zum Nachweis von (i) beachte man

$$[L : K] = \operatorname{ord} \mathfrak{S}_n = n!$$

sowie $k(s_1, \ldots, s_n) \subset K$. Es reicht deshalb zu zeigen, dass

$$\big[L : k(s_1, \ldots, s_n)\big] \leq n!$$

gilt. Letztere Abschätzung aber folgt aus Satz 1, da L Zerfällungskörper von $f = \prod(X - T_i)$ über $k(s_1, \ldots, s_n)$ ist.

Um zu zeigen, dass das System der elementarsymmetrischen Polynome $s_1, \ldots, s_n$ algebraisch unabhängig über k ist, betrachten wir den Körper $k(S_1, \ldots, S_n)$ aller rationalen Funktionen in n Variablen $S_1, \ldots, S_n$, sowie einen Zerfällungskörper $\tilde{L}$ des Polynoms

$$\tilde{f}(X) = \sum_{j=0}^{n} (-1)^j \cdot S_j \cdot X^{n-j} \in k(S_1, \ldots, S_n)[X],$$

wobei formal $S_0 = 1$ gesetzt werde. Seien $t_1, \ldots, t_n$ die Nullstellen von $\tilde{f}$ in $\tilde{L}$, mit Mehrfachnennungen entsprechend den eventuellen Vielfachheiten dieser Nullstellen. Es gilt dann

$$\tilde{L} = k(S_1, \ldots, S_n)(t_1, \ldots, t_n) = k(t_1, \ldots, t_n),$$

da sich die Elemente $S_1, \ldots, S_n$ als elementarsymmetrische Funktionen in $t_1, \ldots, t_n$ darstellen, insbesondere also zu $k(t_1, \ldots, t_n)$ gehören. Der Homomorphismus

$$k[T_1, \ldots, T_n] \longrightarrow k[t_1, \ldots, t_n], \qquad \sum a_\nu T^\nu \longmapsto \sum a_\nu t^\nu,$$

bildet nun elementarsymmetrische Funktionen in $T_1, \ldots, T_n$ auf ebensolche in den Elementen $t_1, \ldots, t_n$ ab und beschränkt sich daher zu einem Homomorphismus

$$k[s_1, \ldots, s_n] \longrightarrow k[S_1, \ldots, S_n], \qquad \sum a_\nu s^\nu \longmapsto \sum a_\nu S^\nu.$$

Da $S_1, \ldots, S_n$ Variablen sind, ist diese Abbildung notwendig injektiv und damit ein Isomorphismus. Dies zeigt, dass $s_1, \ldots, s_n$ als Variablen angesehen werden können und folglich algebraisch unabhängig über k sind. □

Die gerade verwendete Idee, allgemeine Polynome, also Polynome mit Variablen als Koeffizienten zu betrachten, führt uns in direkter Weise zur allgemeinen Gleichung n-ten Grades. Man bezeichnet nämlich für Variablen $S_1, \ldots, S_n$ das Polynom

$$p(X) = X^n + S_1 X^{n-1} + \ldots + S_n \in k(S_1, \ldots, S_n)[X]$$

als das *allgemeine Polynom* n-ten Grades über k. Dementsprechend wird die zugehörige Gleichung $p(x) = 0$ traditionsgemäß als *allgemeine Gleichung* n-ten Grades bezeichnet. Wir wollen die Galois-Gruppe von $p(X)$ bestimmen, indem wir zeigen, dass wir $p(X)$ modulo Isomorphismen mit dem oben diskutierten Polynom $f(X)$ identifizieren dürfen.

Satz 4. *Es sei $p(X) \in k(S_1, \ldots, S_n)[X]$ das allgemeine Polynom n-ten Grades, wie oben definiert. Dann ist $p(X)$ separabel und irreduzibel und besitzt $\mathfrak{S}_n$ als Galois-Gruppe.*

Beweis. Zum rationalen Funktionenkörper $L = k(T_1, \ldots, T_n)$ in n Variablen $T_1, \ldots, T_n$ über k betrachten wir den Fixkörper

$$K = L^{\mathfrak{S}_n} = k(s_1, \ldots, s_n)$$

aller symmetrischen rationalen Funktionen; vgl. Satz 3. Da die elementarsymmetrischen Polynome $s_1, \ldots, s_n$ algebraisch unabhängig über k sind, können wir sie als Variablen ansehen und daher einen k-Isomorphismus

$$k(S_1, \ldots, S_n) \xrightarrow{\sim} k(s_1, \ldots, s_n) = K$$

mittels $S_j \longmapsto (-1)^j s_j$ erklären. Interpretieren wir diesen als Identifizierung, so wird hierbei $p(X)$ in das bekannte Polynom

$$f(X) = \sum_{j=0}^{n} (-1)^j \cdot s_j \cdot X^{n-j} = \prod_{j=0}^{n} (X - T_j) \in K[X]$$

überführt, welches wir oben studiert haben. Genauso wie f ist p dann separabel und irreduzibel und besitzt $\mathfrak{S}_n$ als Galois-Gruppe. Weiter ergibt sich L als Zerfällungskörper von p über $k(S_1, \ldots, S_n)$. □

In Analogie zu den symmetrischen rationalen Funktionen kann man auch symmetrische *Polynome* studieren, wobei wir im Folgenden über einem beliebigen Ring R als Koeffizientenbereich arbeiten wollen. Ein Polynom $f \in R[T_1, \ldots, T_n]$ heißt *symmetrisch*, wenn es von allen Automorphismen von $R[T_1, \ldots, T_n]$ festgelassen wird, die durch Permutationen $\pi \in \mathfrak{S}_n$ der Variablen $T_1, \ldots, T_n$ gegeben sind. Die elementarsymmetrischen Polynome $s_0, \ldots, s_n$, wie oben erklärt, sind spezielle Beispiele solcher symmetrischer Polynome. Wir beweisen nachfolgend den sogenannten *Hauptsatz über symmetrische Polynome*, der als Analogon zu Satz 3 zu sehen ist. Eine detailliertere Version dieses Satzes bringen wir in 4.4/1.

Satz 5 (Hauptsatz über symmetrische Polynome). *Zu einem symmetrischen Polynom $f \in R[T_1, \ldots, T_n]$ mit Koeffizienten aus einem Ring R gibt es genau ein Polynom $g \in R[S_1, \ldots, S_n]$ in n Variablen $S_1, \ldots, S_n$, so dass $f = g(s_1, \ldots, s_n)$ gilt.*

Beweis. Wir beginnen mit einigen Vorbereitungen und führen auf $\mathbb{N}^n$ die sogenannte *lexikographische Ordnung* ein, wobei wir $\nu < \nu'$ für zwei Tupel $\nu = (\nu_1, \ldots, \nu_n)$ und $\nu' = (\nu'_1, \ldots, \nu'_n)$ aus $\mathbb{N}^n$ schreiben, wenn es ein $i_0 \in \{1, \ldots, n\}$ gibt mit

$$\nu_i = \nu'_i \quad \text{für} \quad i = 1, \ldots, i_0 - 1 \quad \text{sowie} \quad \nu_{i_0} < \nu'_{i_0}.$$

Ist dann $f = \sum_{\nu \in \mathbb{N}^n} c_\nu T^\nu \in R[T_1, \ldots, T_n]$ ein nicht-triviales Polynom, so besitzt die Menge $\{\nu \in \mathbb{N}^n \,;\, c_\nu \neq 0\}$ ein wohlbestimmtes lexikographisch größtes Element μ. Dieses wird als *lexikographischer Grad* von f bezeichnet, in Zeichen $\mu = \text{lexgrad}(f)$, und man nennt $\text{Lt}(f) = c_\mu T^\mu$ den *Leitterm* von f, wobei wir für die Zwecke dieses Beweises hier immer den Leitterm im Sinne der lexikographischen Ordnung meinen.

Die Leitterme der elementarsymmetrischen Polynome $s_0, \ldots, s_n$ aus $R[T_1, \ldots, T_n]$ gestalten sich recht einfach,

$$\begin{aligned}
\text{Lt}(s_0) &= \text{Lt}(1) &&= 1,\\
\text{Lt}(s_1) &= \text{Lt}(T_1 + \ldots + T_n) &&= T_1,\\
\text{Lt}(s_2) &= \text{Lt}(T_1T_2 + T_1T_3 + \ldots T_{n-1}T_n) &&= T_1T_2,\\
&\ldots &&\ldots\\
\text{Lt}(s_n) &= \text{Lt}(T_1 \ldots T_n) &&= T_1 \ldots T_n,
\end{aligned}$$

also insgesamt

$$\text{Lt}(s_i) = T_1 \ldots T_i, \qquad i = 0, \ldots, n.$$

Außerdem benötigen wir noch die Gestalt der Leitterme von Monomen in den elementarsymmetrischen Funktionen $s_1, \ldots, s_n$, etwa des Typs $s_1^{\nu_1} \ldots s_n^{\nu_n}$ mit Exponenten $\nu_i \in \mathbb{N}$. Eine leichte Rechnung ergibt:

$$(*)\quad \text{Lt}(s_1^{\nu_1} \ldots s_n^{\nu_n}) = \text{Lt}(s_1)^{\nu_1} \ldots \text{Lt}(s_n)^{\nu_n} = T_1^{\nu_1+\ldots+\nu_n} \cdot T_2^{\nu_2+\ldots+\nu_n} \cdot \ldots \cdot T_n^{\nu_n}$$

Um nun die Existenzaussage des Satzes zu beweisen, betrachten wir ein nicht-triviales symmetrisches Polynom $f = \sum_{\nu \in \mathbb{N}^n} c_\nu T^\nu \in R[T_1, \ldots, T_n]$ mit lexikographischem Grad $\text{lexgrad}(f) = \mu = (\mu_1, \ldots, \mu_n)$ und Leitterm $\text{Lt}(f) = c_\mu T^\mu$. Dann gilt $\mu_1 \geq \mu_2 \geq \ldots \geq \mu_n$ aufgrund der Symmetrieeigenschaft, und es ist

$$f_1 = c_\mu s_1^{\mu_1-\mu_2} s_2^{\mu_2-\mu_3} \ldots s_n^{\mu_n} \in R[T_1, \ldots, T_n]$$

ein symmetrisches und homogenes Polynom vom Totalgrad

$$(\mu_1 - \mu_2) + 2(\mu_2 - \mu_3) + 3(\mu_3 - \mu_4) + \ldots + n\mu_n = \sum_{i=1}^{n} \mu_i = |\mu| \leq \text{grad}(f),$$

welches, ebenso wie f, nach obiger Rechnung $(*)$ mit $c_\mu T^\mu$ als Leitterm beginnt. Folglich gilt

$$\operatorname{lexgrad}(f - f_1) < \operatorname{lexgrad}(f), \qquad \operatorname{grad}(f - f_1) \leq \operatorname{grad}(f),$$

falls f von f_1 verschieden ist. In letzterem Falle kann man den gerade durchgeführten Schritt wiederholen, indem man f durch $f - f_1$ ersetzt. In rekursiver Weise erhält man daher eine Folge $f_1, f_2, \ldots \in R[s_1, \ldots, s_n]$, derart dass der lexikographische Grad der Elemente

$$f,\ f - f_1,\ f - f_1 - f_2,\ \ldots \in R[T_1, \ldots, T_n]$$

schrittweise abnimmt. Da gleichzeitig der Totalgrad durch $\operatorname{grad}(f)$ beschränkt ist, kann der lexikographische Grad nur endlich viele Werte in $\mathbb{N}^n$ annehmen, und es ist offensichtlich, dass die Folge nach endlich vielen Schritten mit dem Nullpolynom endet. Insgesamt ergibt sich eine Darstellung von f als Polynom in den elementarsymmetrischen Polynomen $s_1, \ldots, s_n$.

Zum Nachweis der Eindeutigkeitsaussage reicht es, ein Polynom $g \neq 0$ in $R[S_1, \ldots, S_n]$ zu betrachten und hierfür $g(s_1, \ldots, s_n) \neq 0$ zu zeigen, wobei letzterer Ausdruck in $R[T_1, \ldots, T_n]$ zu lesen ist. Ist etwa $a_\nu S_1^{\nu_1} S_2^{\nu_2} \ldots S_n^{\nu_n}$ ein nicht-trivialer Term von g, so schreiben wir die Exponenten $\nu_1, \ldots, \nu_n$ in der Form $\mu_1 - \mu_2, \mu_2 - \mu_3, \ldots, \mu_n$ mit einem wohlbestimmten Tupel $(\mu_1, \ldots, \mu_n) \in \mathbb{N}^n$, also

$$a_\nu S_1^{\nu_1} S_2^{\nu_2} \ldots S_n^{\nu_n} = a_\nu S_1^{\mu_1 - \mu_2} S_2^{\mu_2 - \mu_3} \ldots S_n^{\mu_n},$$

und ersetzen die Variablen S_i durch die elementarsymmetrischen Funktionen s_i. Sodann berechnet sich der Leitterm des resultierenden Ausdrucks gemäß $(*)$ zu

$$\operatorname{Lt}(a_\nu s_1^{\mu_1 - \mu_2} s_2^{\mu_2 - \mu_3} \ldots s_n^{\mu_n}) = a_\nu T_1^{\mu_1} T_2^{\mu_2} \ldots T_n^{\mu_n},$$

und wir können unter allen Tupeln $\mu = (\mu_1, \ldots, \mu_n) \in \mathbb{N}^n$, die in der beschriebenen Art zu nicht-trivialen Termen von g korrespondieren, eines wählen, etwa $\tilde{\mu}$, das bezüglich der lexikographischen Ordnung auf $\mathbb{N}^n$ maximal ist. Sei $\tilde{\nu}$ das eindeutig bestimmte Tupel in $\mathbb{N}^n$, aus dem $\tilde{\mu}$ gewonnen wurde. Dann folgt

$$\operatorname{Lt}(a_{\tilde{\nu}} s_1^{\tilde{\nu}_1} s_2^{\tilde{\nu}_2} \ldots s_n^{\tilde{\nu}_n}) = a_{\tilde{\nu}} T_1^{\tilde{\mu}_1} T_2^{\tilde{\mu}_2} \ldots T_n^{\tilde{\mu}_n},$$

und dieser Leitterm kann sich in $g(s_1, \ldots, s_n)$ wegen der Maximalität von $\tilde{\mu}$ nicht wegheben. Also ergibt sich $g(s_1, \ldots, s_n) \neq 0$, wie gewünscht. □

Der Beweis des Hauptsatzes über symmetrische Polynome beinhaltet insbesondere ein sehr effektives Verfahren, mit dem man zu einem konkret gegebenen symmetrischen Polynom f leicht das Polynom g mit $f = g(s_1, \ldots, s_n)$ berechnen kann. Bezüglich praktischer Beispiele konsultiere man etwa Abschnitt 6.2. Wir müssen dort spezielle symmetrische Polynome, die im Zusammenhang mit der Auflösung algebraischer Gleichungen vom Grad 3 und 4 auftreten, als Polynome in den elementarsymmetrischen Polynomen schreiben. Im nachfolgenden Abschnitt 4.4 werden wir uns noch genauer mit symmetrischen Polynomen und deren Darstellung mittels elementarsymmetrischer Polynome beschäftigen. Insbesondere nutzen wir den Hauptsatz zur Definition der Diskriminante eines Polynoms; siehe auch 4.4/3. Im Übrigen sei erwähnt, dass die Charakterisierung symmetrischer rationaler Funktionen gemäß Satz 3 auch als Korollar zum Hauptsatz über symmetrische Polynome hergeleitet werden kann.

Lernkontrolle und Prüfungsvorbereitung

1. Es sei K ein Körper und f ein separables Polynom vom Grade $n > 0$ in $K[X]$. Was versteht man unter der Galois-Gruppe G der Gleichung $f(x) = 0$? Zeige, dass man G als Untergruppe der Permutationsgruppe $\mathfrak{S}_n$ auffassen kann und dass f irreduzibel ist, falls $G \simeq \mathfrak{S}_n$ gilt.

2. Ist in der Situation von Punkt 1 die Bedingung $G \simeq \mathfrak{S}_n$ notwendig, damit f irreduzibel ist (mit Begründung)?

3. Es sei K ein Körper mit $\operatorname{char} K \neq 2, 3$ und $f \in K[X]$ ein nicht-konstantes Polynom vom Grad ≤ 3, welches in K keine Nullstelle besitze. Zeige, dass f irreduzibel und separabel ist und diskutiere, welche Gestalt die Galois-Gruppe der Gleichung $f(x) = 0$ über K annehmen kann.

4. Betrachte ein Polynom dritten Grades $f = X^3 + aX + b$ über einem Körper K der Charakteristik $\neq 2, 3$, welches in K keine Nullstelle habe. Definiere die Diskriminante Δ von f und zeige, dass die Galois-Gruppe G der Gleichung $f(x) = 0$ genau dann die Ordnung 3 besitzt, wenn Δ eine Quadratwurzel in K hat.

5. Fasse die Galois-Gruppe G in der Situation von Punkt 4 als Untergruppe der Permutationsgruppe $\mathfrak{S}_3$ auf und definiere die alternierende Gruppe $\mathfrak{A}_3 \subset \mathfrak{S}_3$. Zeige $G = \mathfrak{A}_3$, falls die Diskriminante Δ eine Quadratwurzel in K besitzt sowie $G = \mathfrak{S}_3$, falls Letzteres nicht der Fall ist.

6. Wie ist der Körper der symmetrischen rationalen Funktionen in n Variablen über einem Körper k erklärt? Charakterisiere diesen mittels elementarsymmetrischer Polynome (mit Begründung).

7. Was versteht man unter der allgemeinen Gleichung n-ten Grades $p(x) = 0$ bzw. unter dem allgemeinen Polynom n-ten Grades p? Zeige, dass p irreduzibel und separabel ist und die volle Permutationsgruppe $\mathfrak{S}_n$ als Galois-Gruppe besitzt.

8. Wie lautet der Hauptsatz über symmetrische Polynome?

9. Es sei R ein Ring und $f \in R[T_1, \ldots, T_n]$ ein nicht-triviales Polynom in n Variablen $T_1, \ldots, T_n$. Was versteht man unter dem lexikographischen Grad von f? Wie ist der lexikographische Leitterm $\mathrm{Lt}(f)$ definiert?

10. Berechne in der Situation von Punkt 9 die lexikographischen Leitterme der elementarsymmetrischen Polynome $s_0, \ldots, s_n \in R[T_1, \ldots, T_n]$.

+11. Wie beweist man den Hauptsatz über symmetrische Polynome? Skizziere auch das zugehörige praktische Verfahren zur Darstellung symmetrischer Polynome mittels elementarsymmetrischer Polynome.

Übungsaufgaben

1. *Begründe, dass es zu jeder endlichen Gruppe G eine Galois-Erweiterung L/K mit $\mathrm{Gal}(L/K) \simeq G$ gibt.*

2. Sei $L \subset \mathbb{C}$ ein Teilkörper, so dass $L/\mathbb{Q}$ eine zyklische Galois-Erweiterung vom Grad 4 ist. Zeige: Es besitzt $L/\mathbb{Q}$ genau einen echten Zwischenkörper E, und für diesen gilt $E \subset \mathbb{R}$.

3. Es sei K ein Körper der Charakteristik $\neq 2$ und $f \in K[X]$ ein separables irreduzibles Polynom mit Nullstellen $\alpha_1, \ldots, \alpha_n$ in einem Zerfällungskörper L von f über K. Die Galois-Gruppe von f sei zyklisch von gerader Ordnung. Zeige:

   (i) Die Diskriminante $\Delta = \prod_{i<j}(\alpha_i - \alpha_j)^2$ besitzt keine Quadratwurzel in K.

   (ii) Es gibt genau einen Zwischenkörper E zu L/K mit $[E : K] = 2$, nämlich $E = K(\sqrt{\Delta})$.

4. Es seien $\alpha, \beta \in \mathbb{C}$ zwei Nullstellen des Polynoms $(X^3 - 2)(X^2 + 3) \in \mathbb{Q}[X]$ mit $\alpha \neq \beta, \alpha \neq -\beta$. Zeige für $L = \mathbb{Q}(\alpha, \beta)$, dass $L/\mathbb{Q}$ eine Galois-Erweiterung ist, und bestimme die Galois-Gruppe sowie alle Zwischenkörper zu L/K.

5. Betrachte $L = \mathbb{Q}\left(\frac{1+i}{\sqrt{2}}\right)$ als Teilkörper von $\mathbb{C}$ und zeige, dass $L/\mathbb{Q}$ eine Galois-Erweiterung ist. Bestimme die zugehörige Galois-Gruppe sowie alle Zwischenkörper von $L/\mathbb{Q}$.
6. Bestimme die Galois-Gruppen folgender Polynome aus $\mathbb{Q}[X]$:
   (i) $X^3 + 6X^2 + 11X + 7$,
   (ii) $X^3 + 3X^2 - 1$,
   (iii) $X^4 + 2X^2 - 2$.
7. Bestimme Zerfällungskörper und Galois-Gruppe des Polynoms $X^4 - 5$ über $\mathbb{Q}$ bzw. $\mathbb{Q}(i)$ sowie alle Zwischenkörper der auftretenden Erweiterungen.
8. Bestimme die Galois-Gruppen der folgenden Polynome:
   (i) $X^4 - X^2 - 3 \in \mathbb{F}_5[X]$,
   (ii) $X^4 + 7X^2 - 3 \in \mathbb{F}_{13}[X]$.
9. Schreibe das Polynom $T_1^4 + T_2^4 \in R[T_1, T_2]$ über einem Ring R als Polynom in den zugehörigen elementarsymmetrischen Polynomen.
10. Sei $f \in R[T_1, \ldots, T_n]$ ein symmetrisches Polynom über einem Ring R und $f = g(s_1, \ldots, s_n)$ seine Darstellung als Polynom in den zugehörigen elementarsymmetrischen Polynomen. Zeige, dass der Totalgrad von g gleich dem Grad von f als Polynom in T_1 über $R[T_2, \ldots, T_n]$ als Koeffizientenring ist.

4.4 Symmetrische Polynome, Diskriminante, Resultante*

In diesem Abschnitt beschäftigen wir uns nochmals mit dem Hauptsatz über symmetrische Polynome 4.3/5 und nutzen zum Beweis eine alternative Methode, die insbesondere aus modultheoretischer Sicht neue Informationen liefert. Als Anwendung soll die Diskriminante eines Polynoms studiert und mit Hilfe der Resultante charakterisiert werden. Die Diskriminante eines normierten Polynoms $f \in K[X]$ mit Koeffizienten aus einem Körper K verschwindet genau dann, wenn f in einem algebraischen Abschluss $\overline{K}$ von K mehrfache Nullstellen besitzt; vgl. Bemerkung 3. In ähnlicher Weise zeigt das Verschwinden der Resultante zweier normierter Polynome $f, g \in K[X]$ an, dass f und g eine gemeinsame Nullstelle in $\overline{K}$ haben; vgl. Korollar 8.

Wir verwenden im Folgenden Methoden der Linearen Algebra und benötigen insbesondere den Begriff des Moduls über einem Ring als Verallgemeinerung von Vektorräumen über Körpern, vgl. Abschnitt 2.9. Es

genügt zu wissen, dass für eine Ringerweiterung $R \subset R'$ oder allgemeiner einen Ringhomomorphismus $\varphi\colon R \longrightarrow R'$ eine additive Untergruppe $M \subset R'$ ein *R-Modul* genannt wird, wenn für $r \in R, x \in M$ stets $\varphi(r)x \in M$ gilt; dabei schreibe man abkürzend rx für $\varphi(r)x$. Insbesondere kann man R' als R-Modul auffassen. Ein System $(x_i)_{i\in I}$ von Elementen aus M heißt ein *freies Erzeugendensystem* von M, wenn jedes $x \in M$ eine Darstellung $x = \sum_{i\in I} r_i x_i$ mit eindeutig bestimmten Koeffizienten $r_i \in R$ besitzt, die fast alle verschwinden. Freie Erzeugendensysteme von Moduln entsprechen im Grunde genommen den Basen von Vektorräumen, sie existieren aber nur in Spezialfällen, da man nicht-triviale Linearkombinationen, etwa des Typs $r_1x_1 + \ldots r_nx_n = 0$ mit $r_i \in R$ und $x_i \in M$, nicht notwendig nach einem der x_i auflösen kann, z. B. wenn r_i zwar nicht Null aber keine Einheit ist.

Es sei im Folgenden $R[T_1, \ldots, T_n]$ der Polynomring in n Variablen T_i über einem Ring R. Wie in Abschnitt 4.3 interpretieren wir die Permutationsgruppe $\mathfrak{S}_n$ als eine Gruppe von Automorphismen von $R[T_1, \ldots, T_n]$, indem wir zu $\pi \in \mathfrak{S}_n$ jeweils den zugehörigen R-Automorphismus

$$\begin{aligned} R[T_1, \ldots, T_n] &\longrightarrow R[T_1, \ldots, T_n], \\ f(T_1, \ldots, T_n) &\longmapsto f(T_{\pi(1)}, \ldots, T_{\pi(n)}), \end{aligned}$$

betrachten. Ein Polynom $f \in R[T_1, \ldots, T_n]$ heißt *symmetrisch*, wenn es von allen $\pi \in \mathfrak{S}_n$ festgelassen wird. Als Beispiele für symmetrische Polynome kennen wir bereits die elementarsymmetrischen Polynome

$$\begin{aligned} s_0 &= 1, \\ s_1 &= T_1 + \ldots + T_n, \\ s_2 &= T_1T_2 + T_1T_3 + \ldots + T_{n-1}T_n, \\ &\ldots \\ s_n &= T_1 \ldots T_n, \end{aligned}$$

welche unter Zuhilfenahme einer weiteren Variablen X durch die Gleichung

$$\prod_{i=1}^{n}(X - T_i) = \sum_{j=0}^{n}(-1)^j s_j X^{n-j} \tag{1}$$

erklärt sind. Die symmetrischen Polynome in $R[T_1, \ldots, T_n]$ bilden einen Unterring, welcher R sowie alle s_j enthält.

Satz 1 (Hauptsatz über symmetrische Polynome). *Seien $s_1, \ldots, s_n$ die elementarsymmetrischen Polynome im Polynomring $R[T] = R[T_1, \ldots, T_n]$ in n Variablen T_i über einem Ring R.*

(i) *Der Unterring der symmetrischen Polynome in $R[T]$ wird gegeben durch $R[s_1, \ldots, s_n]$, d. h. jedes symmetrische Polynom in $R[T]$ ist ein Polynom in den elementarsymmetrischen Polynomen $s_1, \ldots, s_n$.*

(ii) *Die Elemente $s_1, \ldots, s_n \in R[T]$ sind algebraisch unabhängig über R (im Sinne von 2.5/6).*

(iii) *Sei $N \subset \mathbb{N}^n$ die Menge aller n-Tupel $\nu = (\nu_1, \ldots, \nu_n)$ mit $0 \leq \nu_i < i$ für $1 \leq i \leq n$. Dann ist das System $(T^\nu)_{\nu \in N}$ ein freies Modulerzeugendensystem der Länge $n!$ von $R[T]$ über $R[s_1, \ldots, s_n]$.*

Beweis. Wir schließen mit Induktion nach n. Der Fall $n = 1$ ist trivial, da dann $s_1 = T_1$ gilt und jedes Polynom in $R[T_1]$ symmetrisch ist. Sei also $n > 1$, und seien $s'_0, \ldots, s'_{n-1}$ die elementarsymmetrischen Polynome in $R[T_1, \ldots, T_{n-1}]$. Dann gilt unter Zuhilfenahme einer Variablen X

$$\sum_{j=0}^{n} (-1)^j s_j X^{n-j} = \prod_{i=1}^{n} (X - T_i) = (X - T_n) \cdot \sum_{j=0}^{n-1} (-1)^j s'_j X^{n-1-j},$$

d. h. man hat die Relationen

$$s_j = s'_j + s'_{j-1} T_n, \qquad 1 \leq j \leq n-1, \tag{2}$$

sowie $s'_0 = s_0 = 1$ und $s'_{n-1} T_n = s_n$. Hieraus folgt induktiv, dass sich auch $s'_1, \ldots, s'_{n-1}$ als Linearkombinationen der $s_1, \ldots, s_{n-1}$ mit Koeffizienten in $R[T_n]$ darstellen lassen, und es gilt

$$R[s'_1, \ldots, s'_{n-1}, T_n] = R[s_1, \ldots, s_{n-1}, T_n]. \tag{3}$$

Wir behaupten weiter:

$$\begin{gathered} \textit{Die Systeme } s'_1, \ldots, s'_{n-1}, T_n \textit{ sowie } s_1, \ldots, s_{n-1}, T_n \\ \textit{sind algebraisch unabhängig über } R. \end{gathered} \tag{4}$$

Indem wir R durch $R[T_n]$ ersetzen, können wir nach Induktionsvoraussetzung schließen, dass $s'_1, \ldots, s'_{n-1}$ algebraisch unabhängig über $R[T_n]$ sind bzw. dass $s'_1, \ldots, s'_{n-1}, T_n$ algebraisch unabhängig über R sind. Es ist daher lediglich die entsprechende Aussage für $s_1, \ldots, s_{n-1}, T_n$ zu zeigen.

Sei nun f ein nicht-triviales Polynom in $n-1$ Variablen mit Koeffizienten in $R[T_n]$, so dass $f(s_1,\dots,s_{n-1})$ als Element von $R[T_1,\dots,T_n]$ verschwindet. Da T_n kein Nullteiler in $R[T_1,\dots,T_n]$ ist, dürfen wir annehmen, dass nicht alle Koeffizienten von f durch T_n teilbar sind. Man wende nun den Homomorphismus $\tau\colon R[T_1,\dots,T_n] \longrightarrow R[T_1,\dots,T_{n-1}]$ an, welcher 0 anstelle von T_n substituiert. Aufgrund der Relationen (2) gilt dann $\tau(s_j) = s'_j$ für $j = 1,\dots,n-1$. Da nicht alle Koeffizienten von f durch T_n teilbar sind, also unter τ auf 0 abgebildet werden, erhalten wir aus $f(s_1,\dots,s_{n-1}) = 0$ eine nicht-triviale Relation des Typs $g(s'_1,\dots,s'_{n-1}) = 0$ in $R[T_1,\dots,T_{n-1}]$. Dies widerspricht aber der Tatsache, dass $s'_1,\dots,s'_{n-1}$ nach Induktionsvoraussetzung algebraisch unabhängig über R sind. Behauptung (4) ist somit bewiesen.

Wir beginnen nun mit der Herleitung der einzelnen Aussagen des Hauptsatzes. Zum Nachweis von (i) betrachte man ein symmetrisches Polynom f aus $R[T_1,\dots,T_n]$. Da mit f auch alle homogenen Bestandteile von f symmetrisch sind, dürfen wir f als homogen von einem gewissen Grad $m > 0$ ansehen. Es ist f invariant unter allen Permutationen der Variablen $T_1,\dots,T_{n-1}$ und gehört daher nach Induktionsvoraussetzung zu $R[s'_1,\dots,s'_{n-1},T_n]$, also nach (3) zu $R[s_1,\dots,s_{n-1},T_n]$. Man stelle nun f in der Form

$$f = \sum f_i T_n^i \tag{5}$$

mit Koeffizienten $f_i \in R[s_1,\dots,s_{n-1}]$ dar. Dann ist jeder Koeffizient f_i als Polynom in $T_1,\dots,T_n$ symmetrisch und, wie wir behaupten, außerdem homogen vom Grad $m-i$. Um dies einzusehen, schreibe man die f_i in expliziter Weise als Summe von Termen des Typs $cs_1^{\nu_1}\dots s_{n-1}^{\nu_{n-1}}$. Als Polynom in $T_1,\dots,T_n$ ist ein solcher Term homogen vom Grad $\sum_{j=1}^{n-1} j\nu_j$, dem sogenannten *Gewicht* dieses Terms. Nach Multiplikation mit T_n^i ergibt sich daraus ein homogenes Polynom, und zwar vom Grad $i + \sum_{j=1}^{n-1} j\nu_j$. Bezeichnen wir daher mit f'_i die Summe aller Terme $cs_1^{\nu_1}\dots s_{n-1}^{\nu_{n-1}}$ in f_i vom Gewicht $m-i$, so folgt $f = \sum f'_i T_n^i$, denn f ist homogen vom Grade m. Da aber $s_1,\dots,s_{n-1},T_n$ aufgrund von (4) algebraisch unabhängig über R sind, ist die Darstellung (5) eindeutig, d. h. es gilt $f_i = f'_i$, und f_i ist als Polynom in $T_1,\dots,T_n$ homogen vom Grad $m-i$.

Insbesondere ist $f_0 \in R[s_1,\dots,s_{n-1}]$ symmetrisch und homogen vom Grad m in $T_1,\dots,T_n$. Gilt in (5) bereits $f = f_0$, so sind wir fertig. Ansonsten betrachte man die Differenz $f - f_0$. Diese ist ebenfalls symmetrisch und

homogen vom Grad m in $T_1, \ldots, T_n$, und es wird $f - f_0$ nach Konstruktion von T_n geteilt. Aufgrund der Symmetrie wird dann $f - f_0$ auch vom Produkt $s_n = T_1 \ldots T_n$ geteilt, und wir können

$$f = f_0 + g s_n \tag{6}$$

schreiben, wobei g symmetrisch und homogen von einem Grad $< m$ in $T_1, \ldots, T_n$ ist. Induktion nach m liefert schließlich $f \in R[s_1, \ldots, s_n]$.

Nun zum Nachweis von Aussage (ii). Da T_n eine Nullstelle des Polynoms (1) ist, erhalten wir

$$(-1)^{n+1} s_n = \sum_{j=0}^{n-1} (-1)^j s_j T_n^{n-j} = T_n^n - s_1 T_n^{n-1} + \ldots + (-1)^{n-1} s_{n-1} T_n.$$

In dieser Situation wenden wir für $A = R[s_1, \ldots, s_{n-1}]$, $X = T_n$ und $h = s_n$ folgendes Resultat an, welches wir weiter unten beweisen werden:

Lemma 2. *Sei $A[X]$ der Polynomring einer Variablen X über einem Ring A. Weiter sei $h = c_0 X^n + c_1 X^{n-1} + \ldots + c_n$ ein Polynom in $A[X]$, dessen höchster Koeffizient c_0 eine Einheit in A ist. Dann besitzt jedes $f \in A[X]$ eine Darstellung $f = \sum_{i=0}^{n-1} f_i X^i$ mit eindeutig bestimmten Koeffizienten $f_i \in A[h]$ und jedes f_i eine Darstellung $f_i = \sum_{j \geq 0} a_{ij} h^j$ mit eindeutig bestimmten Koeffizienten $a_{ij} \in A$.*

Es ist also h algebraisch unabhängig über A, und $X^0, X^1, \ldots, X^{n-1}$ bilden ein freies Erzeugendensystem von $A[X]$ als Modul über $A[h]$.

Insbesondere folgt, dass s_n algebraisch unabhängig über dem Ring $R[s_1, \ldots, s_{n-1}]$ ist, also aufgrund der algebraischen Unabhängigkeit von $s_1, \ldots, s_{n-1}$, vgl. (4), dass $s_1, \ldots, s_n$ algebraisch unabhängig über R sind. Aussage (ii) ist damit klar. Ebenso einfach können wir Aussage (iii) aus dem Lemma folgern. Nach Induktionsvoraussetzung bildet

$$\mathfrak{F}' = \left\{ T_1^{\nu_1} \ldots T_{n-1}^{\nu_{n-1}} \,;\, 0 \leq \nu_i < i \text{ für } 1 \leq i \leq n-1 \right\},$$

ein freies Erzeugendensystem von $R[T_1, \ldots, T_n]$, aufgefasst als Modul über $R[s_1, \ldots, s_{n-1}, T_n]$; dabei betrachte man $R[T_n]$ als Koeffizientenring und wende (3) an. Aufgrund des obigen noch zu beweisenden Lemmas bildet weiter $\mathfrak{F}'' = \{T_n^0, \ldots, T_n^{n-1}\}$ ein freies Erzeugendensystem von $R[s_1, \ldots, s_{n-1}, T_n]$ über $R[s_1, \ldots, s_n]$. Eine Standardrechnung zeigt dann,

dass $\mathfrak{F} = \{a'a'' ; a' \in \mathfrak{F}', a'' \in \mathfrak{F}''\}$ ein freies Erzeugendensystem von $R[T_1, \ldots, T_n]$ über $R[s_1, \ldots, s_n]$ ist. □

Es bleibt noch der *Beweis zu Lemma* 2 nachzutragen. Zu zeigen ist, dass jedes $f \in A[X]$ eine Darstellung

$$f = \sum_{i=0}^{n-1} \Big(\sum_{j \geq 0} a_{ij} h^j \Big) X^i = \sum_{j \geq 0} \Big(\sum_{i=0}^{n-1} a_{ij} X^i \Big) h^j$$

mit eindeutig bestimmten Koeffizienten $a_{ij} \in A$, bzw. eine Darstellung

$$f = \sum_{j \geq 0} r_j h^j \tag{7}$$

mit eindeutig bestimmten Polynomen $r_j \in A[X]$ mit $\operatorname{grad} r_j < n$ besitzt. Hierzu verwenden wir die Division mit Rest durch h. Diese steht in $A[X]$ zur Verfügung, da der höchste Koeffizient von h eine Einheit in A ist; vgl. 2.1/4. Daher existieren Zerlegungen

$$f_0 = f = f_1 h + r_0, \qquad f_1 = f_2 h + r_1, \qquad f_2 = f_3 h + r_2, \qquad \ldots$$

mit geeigneten Polynomen $r_0, r_1, \ldots \in A[X]$ vom Grad $< n$, sowie Polynomen $f_0, f_1, \ldots \in A[X]$, deren Grad schrittweise abnimmt, bis wir schließlich bei einem Index j mit $\operatorname{grad} f_j < n = \operatorname{grad} h$ und damit $f_j = r_j$ landen. Indem man die vorstehenden Gleichungen zusammensetzt, ergibt sich die Existenz der Darstellung (7). Zum Nachweis der Eindeutigkeit geht man von einer Darstellung $0 = \sum_{j \geq 0} r_j h^j$ aus. Aufgrund der Eindeutigkeit der Division mit Rest folgert man aus der Zerlegung

$$0 = r_0 + h \cdot \sum_{j > 0} r_j h^{j-1}$$

$r_0 = 0$ und $\sum_{j>0} r_j h^{j-1} = 0$. Mit Induktion ergibt sich $r_j = 0$ für alle j. □

Aus dem Beweis zu Satz 1 können wir ein weiteres praktisches Konstruktionsverfahren zur Darstellung symmetrischer Polynome mittels elementarsymmetrischer Polynome ablesen, welches allerdings etwas komplizierter als das im Beweis zu 4.3/5 gegebene Verfahren erscheint. Substituiert

man in der Gleichung $f = f_0(s_1, \ldots, s_{n-1}) + g s_n$, vgl. (6), den Wert 0 für T_n, so ergibt sich unter Benutzung von (2)

$$f(T_1, \ldots, T_{n-1}, 0) = f_0(s'_1, \ldots, s'_{n-1}).$$

Dies bedeutet, dass der im Beweis beschriebene Konstruktionsschritt das Problem, f als Polynom in den elementarsymmetrischen Polynomen $s_1, \ldots, s_n$ darzustellen, auf folgende Teilprobleme reduziert:

(a) Man betrachte das symmetrische Polynom $f(T_1, \ldots, T_{n-1}, 0)$ in $n-1$ Variablen und schreibe es als Polynom $f_0(s'_1, \ldots, s'_{n-1})$ in den elementarsymmetrischen Polynomen $s'_1, \ldots, s'_{n-1}$ in $T_1, \ldots, T_{n-1}$ mit Koeffizienten in R.

(b) Man ersetze $s'_1, \ldots, s'_{n-1}$ in f_0 durch die entsprechenden elementarsymmetrischen Polynome $s_1, \ldots, s_{n-1}$ in $T_1, \ldots, T_n$, dividiere die Differenz $f - f_0(s_1, \ldots, s_{n-1})$ durch s_n und schreibe den resultierenden Ausdruck $s_n^{-1} \cdot (f - f_0(s_1, \ldots, s_{n-1}))$ als Polynom in den elementarsymmetrischen Polynomen $s_1, \ldots, s_n$.

Mit (a) reduzieren wir die Anzahl der Variablen, mit (b) den Grad des zu behandelnden Polynoms. Man gelangt daher nach endlich vielen Schritten der beschriebenen Art zu der gewünschten Darstellung von f.

Als Anwendung von Satz 1 kann man insbesondere die Aussage 4.3/3 ableiten, dass nämlich jede symmetrische rationale Funktion in n Variablen $T_1, \ldots, T_n$ mit Koeffizienten aus einem Körper k eine rationale Funktion mit Koeffizienten aus k in den elementarsymmetrischen Polynomen $s_1, \ldots, s_n$ ist. Hierzu betrachte man eine symmetrische rationale Funktion $q \in k(T_1, \ldots, T_n)$, etwa $q = f/g$ mit Polynomen $f, g \in k[T_1, \ldots, T_n]$. Indem wir den Bruch f/g erweitern, dürfen wir g durch $\prod_{\pi \in \mathfrak{S}_n} \pi(g)$ ersetzen und damit g als symmetrisch annehmen. Dann ist aber auch $f = q \cdot g$ symmetrisch. Folglich ist q ein Quotient symmetrischer Polynome und damit gemäß Satz 1 (i) eine rationale Funktion in $s_1, \ldots, s_n$. Im Übrigen gibt das freie Erzeugendensystem aus Satz 1 (iii) Anlass zu einer konkreten Basis von $k(T_1, \ldots, T_n)$ über $k(s_1, \ldots, s_n)$.

Als weitere Anwendung des Hauptsatzes über symmetrische Polynome wollen wir die *Diskriminante* eines normierten Polynoms behandeln. Wir betrachten zunächst den Fall $R = \mathbb{Z}$. In der Situation des Hauptsatzes ist

$$\prod_{i<j} (T_i - T_j)^2$$

ein symmetrisches Polynom in $T_1, \ldots, T_n$ und folglich aufzufassen als Polynom $\Delta = \Delta(s_1, \ldots, s_n)$ in den elementarsymmetrischen Polynomen $s_1, \ldots, s_n$. Man nennt Δ die Diskriminante des Polynoms

$$\prod_{i=1}^{n}(X - T_i) = \sum_{j=0}^{n}(-1)^j s_j X^{n-j},$$

wobei X als Variable über dem Koeffizientenring $\mathbb{Z}[T_1, \ldots, T_n]$ zu sehen ist. Um nun für einen beliebigen Koeffizientenring R und ein normiertes Polynom $f = X^n + c_1 X^{n-1} + \ldots + c_n \in R[X]$ die Diskriminante zu definieren, setzen wir

$$\Delta_f = \Delta\big(-c_1, c_2, \ldots, (-1)^n c_n\big).$$

Es ist also Δ_f gleich dem Bild von Δ unter dem Ringhomomorphismus

$$\varphi\colon \mathbb{Z}[s_1, \ldots, s_n] \longrightarrow R, \qquad s_j \longmapsto (-1)^j c_j,$$

welcher den kanonischen Homomorphismus $\mathbb{Z} \longrightarrow R$ fortsetzt. Dabei beachte man, dass die elementarsymmetrischen Polynome $s_1, \ldots, s_n$ algebraisch unabhängig über $\mathbb{Z}$ sind, und wir deshalb $\mathbb{Z}[s_1, \ldots, s_n]$ als Polynomring in den n "Variablen" $s_1, \ldots, s_n$ ansehen dürfen. Die Existenz und Eindeutigkeit von φ ergibt sich deshalb aus 2.5/5. Man kann die Definition der Diskriminante Δ_f auch im Falle $n = 0$, also für das normierte Polynom $f = 1$ durchführen und erhält $\Delta_f = 1$ (da leere Produkte per definitionem den Wert 1 haben). Insgesamt bleibt festzustellen, dass die Diskriminante Δ_f ein Element des Koeffizientenrings R ist, welches in polynomialer Weise von den Koeffizienten des betrachteten Polynoms f abhängt.

Bemerkung 3. *Es sei $f = X^n + c_1 X^{n-1} + \ldots + c_n \in R[X]$ ein normiertes Polynom einer Variablen X mit Diskriminante Δ_f über einem Ring R. Ist dann $f = \prod_{i=1}^{n}(X - \alpha_i)$ eine Faktorisierung über einem Erweiterungsring R' von R, so gilt*

$$\Delta_f = \prod_{i<j}(\alpha_i - \alpha_j)^2.$$

Beweis. Man betrachte den Ringhomomorphismus

$$\varphi\colon \mathbb{Z}[T_1, \ldots, T_n] \longrightarrow R', \qquad T_i \longmapsto \alpha_i,$$

welcher den kanonischen Homomorphismus $\mathbb{Z} \longrightarrow R$ fortsetzt. Dieser transportiert das Polynom $F = \prod_{i=1}^{n}(X - T_i)$ in das Polynom $F^{\varphi} = f$, also gilt $\varphi(s_j) = (-1)^j c_j$ und somit $\varphi(\Delta_F) = \Delta_f$. Daher ergibt sich

$$\Delta_f = \varphi\Big(\prod_{i<j}(T_i - T_j)^2\Big) = \prod_{i<j}(\alpha_i - \alpha_j)^2,$$

was zu zeigen war. □

Insbesondere folgt für einen Körper K, dass die Diskriminante Δ_f eines normierten Polynoms $f \in K[X]$ genau dann verschwindet, wenn f in einem algebraischen Abschluss von K mehrfache Nullstellen hat. Dies ist wiederum äquivalent dazu, dass f und die zugehörige Ableitung f' gemeinsame Nullstellen haben; vgl. 2.6/3. Wir wollen im Folgenden genauer zeigen, dass die Diskriminante Δ_f bis auf das Vorzeichen mit der Resultante $\operatorname{res}(f, f')$ übereinstimmt. Diese Beziehung bietet insbesondere für die konkrete Berechnung von Diskriminanten einige Vorteile.

Als Nächstes soll nun die Resultante $\operatorname{res}(f, g)$ zweier Polynome f, g definiert werden. Seien

$$f = a_0X^m + a_1X^{m-1} + \ldots + a_m, \qquad g = b_0X^n + b_1X^{n-1} + \ldots + b_n$$

zwei Polynome einer Variablen X mit Koeffizienten in einem Ring R. Da wir nicht verlangen, dass a_0 und b_0 von 0 verschieden sind, bezeichnen wir m bzw. n auch als *formalen Grad* von f bzw. g sowie das Paar (m, n) als formalen Grad von (f, g). Man definiert nun die *Resultante* $\operatorname{res}(f, g)$ zum formalen Grad (m, n) als Determinante der folgenden Matrix mit $m + n$ Zeilen und Spalten

$$(*) \qquad \begin{array}{c} \vartriangle \\ \vert \\ n \\ \vert \\ \triangledown \\ \vartriangle \\ \vert \\ m \\ \vert \\ \triangledown \end{array} \begin{pmatrix} a_0 & a_1 & . & . & . & a_m & & & \\ & a_0 & a_1 & . & . & . & a_m & & \\ & & \multicolumn{5}{c}{\dotfill} & & \\ & & & a_0 & a_1 & . & . & . & a_m & \\ & & & & a_0 & a_1 & . & . & . & a_m \\ b_0 & b_1 & . & . & . & b_n & & & & \\ & b_0 & b_1 & . & . & . & b_n & & & \\ & & \multicolumn{5}{c}{\dotfill} & & \\ & & & b_0 & b_1 & . & . & . & b_n & \\ & & & & b_0 & b_1 & . & . & . & b_n \end{pmatrix},$$

also

$$\operatorname{res}(f,g) = \det(*),$$

wobei an den nicht durch Elemente oder Punkte besetzten Stellen jeweils Nullen einzufügen sind. Im Trivialfall $m = n = 0$ erkläre man die Determinante der leeren Matrix als 1. Wird der formale Grad von f bzw. g nicht explizit erwähnt, so interpretiert man diesen für $f \neq 0 \neq g$ gewöhnlich als den Grad von f bzw. g. Mit Hilfe der üblichen Regeln für das Rechnen mit Determinanten[3] ergibt sich unmittelbar:

Bemerkung 4. (i) $\operatorname{res}(f,g) = (-1)^{m\cdot n} \operatorname{res}(g,f)$.

(ii) $\operatorname{res}(af, bg) = a^n b^m \operatorname{res}(f,g)$ *für Konstanten* $a, b \in R$.

(iii) *Es sei* $\varphi\colon R \longrightarrow R'$ *ein Ringhomomorphismus. Dann gilt für die mit* φ *von* $R[X]$ *nach* $R'[X]$ *transportierten Polynome* f^φ, g^φ *die Relation* $\operatorname{res}(f^\varphi, g^\varphi) = \varphi(\operatorname{res}(f,g))$.

Sei nun S die transponierte Matrix zu $(*)$, d. h. die Matrix, die durch Spiegelung von $(*)$ an seiner Hauptdiagonalen gewonnen wird. Wir wollen S als Matrix gewisser einfach zu beschreibender R-linearer Abbildungen interpretieren und entsprechend $\operatorname{res}(f,g)$ als Determinante solcher Abbildungen charakterisieren. Hierzu bezeichne man für $i \in \mathbb{N}$ mit $R[X]_i$ den R-Modul aller Polynome in $R[X]$ vom Grad $< i$.

Lemma 5. *Seien* $f, g \in R[X]$ *Polynome wie vorstehend beschrieben.*

(i) *Fixiert man auf* $R[X]_i$ *jeweils* $X^{i-1}, \ldots, X^0$ *als freies R-Erzeugendensystem, so beschreibt die zu* $(*)$ *transponierte Matrix S die R-lineare Abbildung*

$$\Phi\colon R[X]_n \times R[X]_m \longrightarrow R[X]_{m+n}, \qquad (u,v) \longmapsto uf + vg.$$

(ii) *Ist f normiert vom Grad m, so ist neben* $\mathfrak{F} = (X^{m+n-1}, \ldots, X^0)$ *auch* $\mathfrak{F}' = (fX^{n-1}, \ldots, fX^0, X^{m-1}, \ldots, X^0)$ *ein freies R-Erzeugendensystem von* $R[X]_{m+n}$. *Die Übergangsmatrix zwischen beiden Systemen hat Determinante* 1.

[3] Formale Regeln für das Rechnen mit Determinanten bleiben gültig, wenn man statt Koeffizienten aus einem Körper allgemeiner Koeffizienten aus einem Ring R zulässt. Man fasse nämlich die benötigten Koeffizienten, etwa $c_1, \ldots, c_r$, zunächst als Variablen auf und stelle fest, dass die betreffende Regel über dem Körper $\mathbb{Q}(c_1, \ldots, c_r)$ bzw. dem Unterring $\mathbb{Z}[c_1, \ldots, c_r]$ gilt. Sodann kann man diese mittels geeigneter Ringhomomorphismen in beliebige Ringe R transportieren.

(iii) *Ist f normiert vom Grad m, so ist* $\operatorname{res}(f,g)$ *gleich der Determinante des R-Endomorphismus* $\Phi' \colon R[X]_{m+n} \longrightarrow R[X]_{m+n}$, *welcher* $X^{m-1},\dots,X^0$ *jeweils mit g multipliziert und im Übrigen* $fX^{n-1},\dots,fX^0$ *festlässt.*

Beweis. Aussage (i) ist unmittelbar klar, die Koeffizientenvektoren der Φ-Bilder zu

$$(X^{n-1},0),\dots,(X^0,0),(0,X^{m-1}),\dots,(0,X^0)$$

stimmen überein mit den Zeilen der Matrix $(*)$, also mit den Spalten der Matrix S.

Nun zu Aussage (ii). Stellt man das System $\mathfrak{F}'$ mit Hilfe des freien Erzeugendensystems $\mathfrak{F}$ dar, so ist die zugehörige Koeffizientenmatrix eine Dreiecksmatrix, deren Diagonalelemente alle 1 sind; man beachte dabei, dass f als normiert vorausgesetzt ist. Die Übergangsmatrix hat daher Determinante 1 und ist invertierbar.

Um (iii) einzusehen, prüfe man nach, dass die Abbildung Φ' gerade durch die Matrix S beschrieben wird, wenn wir auf dem Urbildraum $\mathfrak{F}'$ als freies Erzeugendensystem fixieren und auf dem Bildraum $\mathfrak{F}$. Um die Determinante von Φ' zu berechnen, müssen wir auf Urbild- und Bildraum jeweils dasselbe freie Erzeugendensystem zugrunde legen, also etwa auf dem Urbildraum von $\mathfrak{F}'$ zu $\mathfrak{F}$ wechseln. Nach (ii) hat die Übergangsmatrix Determinante 1, also gilt $\det\Phi' = \det S = \operatorname{res}(f,g)$. □

Wir wollen einige Folgerungen aus dem Lemma ziehen.

Satz 6. *Falls $m+n \geq 1$, so gibt es Polynome $p,q \in R[X]$,* $\operatorname{grad} p < n$, $\operatorname{grad} q < m$, *mit* $\operatorname{res}(f,g) = pf + qg$.

Beweis. Wir benutzen die Abbildung Φ aus Lemma 5 und zeigen, dass das konstante Polynom $\operatorname{res}(f,g) \in R[X]$ zum Bild von Φ gehört. Um dies einzusehen, benutzen wir die "Cramersche Regel"

$$S \cdot S^* = (\det S) \cdot E,$$

wobei S^* die adjungierte Matrix zu S bezeichnet sowie E die Einheitsmatrix mit $m+n$ Zeilen und Spalten; vgl. [4], Satz 4.4/3, und die Verallgemeinerung, die wir im Beweis zu 3.3/1 gegeben haben. In der Sprache

der R-linearen Abbildungen bedeutet die obige Gleichung: Es existiert eine R-lineare Abbildung $\Phi^*\colon R[X]_{m+n} \longrightarrow R[X]_m \times R[X]_n$, deren Komposition mit $\Phi\colon R[X]_m \times R[X]_n \longrightarrow R[X]_{m+n}$ die Abbildung $(\det S)\cdot \mathrm{id}$ ergibt. Insbesondere gehört das konstante Polynom $\Phi \circ \Phi^*(1) = \det S = \mathrm{res}(f,g)$ zum Bild von Φ, woraus sich die behauptete Gleichung ergibt. □

In der Situation des Satzes folgt insbesondere, dass die Resultante $\mathrm{res}(f,g)$ verschwindet, wenn f und g eine gemeinsame Nullstelle besitzen. Allerdings kann die Resultante auch noch in weiteren Fällen verschwinden, z. B. wenn die höchsten Koeffizienten a_0, b_0 von f und g beide Null sind. Wir wollen nun eine Interpretation der Resultante geben, welche als Schlüssel zur Herleitung weiterer wichtiger Eigenschaften dient.

Satz 7. *Es sei $f \in R[X]$ ein normiertes Polynom vom Grad m. Fasst man den Restklassenring $A = R[X]/(f)$ als R-Modul unter der kanonischen Abbildung $R \longrightarrow R[X]/(f)$ auf, so bilden die Potenzen $x^{m-1}, \ldots, x^0$, wobei x die Restklasse zu X bezeichne, ein freies R-Modulerzeugendensystem von A. Sei weiter $g \in R[X]$ ein Polynom vom Grad $\leq n$ und $g(x)$ die Restklasse von g in A. Dann gilt für die Resultante zum formalen Grad (m,n)*

$$\mathrm{res}(f,g) = \mathrm{N}_{A/R}\big(g(x)\big),$$

wobei $\mathrm{N}_{A/R}(g(x))$ die Norm *von $g(x)$ ist, d. h. die Determinante der R-linearen Abbildung $A \longrightarrow A$, $a \longmapsto g(x)\cdot a$.*

Insbesondere ist $\mathrm{res}(f,g)$ *in dieser Situation unabhängig von der Wahl des formalen Grades n von g.*

Beweis. Da f normiert ist, steht in $R[X]$ die Division mit Rest zur Verfügung; vgl. 2.1/4. Diese ist eindeutig, also induziert die Projektion $R[X] \longrightarrow A$ einen Isomorphismus $R[X]_m \xrightarrow{\sim} A$ von R-Moduln. Somit bilden die Elemente $x^{m-1}, \ldots, x^0$ als Bilder von $X^{m-1}, \ldots, X^0$ ein freies Erzeugendensystem von A über R. Dies begründet die erste Behauptung. Um die zweite zu erhalten, benutzen wir die Abbildung Φ' aus Lemma 5 (iii). Die Projektion $R[X]_{m+n} \longrightarrow A$ hat als Kern den R-Modul $fR[X]_n$. Da Φ' diesen Kern in sich abbildet, induziert Φ' eine R-lineare Abbildung $\overline{\Phi'}\colon A \longrightarrow A$; dies ist offenbar gerade die Multiplikation mit $g(x)$, wie man aus der Definition von Φ' abliest. Da Φ' sich auf $fR[X]_n$ zur identischen Abbildung beschränkt, gilt $\det \Phi' = \det \overline{\Phi'}$, d. h. man hat $\mathrm{res}(f,g) = \mathrm{N}_{A/R}(g(x))$ mit Lemma 5 (iii). □

Korollar 8. *Es seien f, g nicht-triviale Polynome mit Koeffizienten in einem Körper K. Weiter sei* $\operatorname{grad} f = m$ *sowie* $\operatorname{grad} g \leq n$. *Dann ist äquivalent*:

(i) *Die Resultante* $\operatorname{res}(f, g)$ *zum formalen Grad* (m, n) *ist von Null verschieden.*

(ii) *Ist $\overline{K}$ ein algebraischer Abschluss von K, so haben f und g keine gemeinsame Nullstelle in $\overline{K}$.*

Beweis. Nach Bemerkung 4 dürfen wir f als normiert annehmen. Gelte zunächst $\operatorname{res}(f, g) \neq 0$. Dann ist nach Satz 7 die Determinante der Multiplikation mit $g(x)$ auf $K[X]/(f)$ nicht Null, also invertierbar. Es folgt, dass die Multiplikation mit $g(x)$ invertierbar ist, dass also $g(x)$ eine Einheit in $K[X]/(f)$ ist. Somit erzeugen f und g das Einheitsideal in $K[X]$, und es können diese Polynome keine gemeinsame Nullstelle besitzen. Seien nun f und g ohne gemeinsame Nullstelle in $\overline{K}$. Es sind dann f, g teilerfremd in $\overline{K}[X]$ und somit auch in $K[X]$. Daher existiert eine Gleichung der Form $uf + vg = 1$ mit Polynomen $u, v \in K[X]$, und man sieht, dass $g(x)$ eine Einheit ist. Die Multiplikation mit $g(x)$ auf $K[X]/(f)$ ist also invertierbar, die zugehörige Determinante nicht Null, und es folgt $\operatorname{res}(f, g) \neq 0$ mit Satz 7. □

Korollar 9. *Seien $f, g \in R[X]$ Polynome vom Grad m bzw. $\leq n$, wobei f eine Zerlegung $f = \alpha \prod_{i=1}^{m} (X - \alpha_i)$ besitze mit einer Konstanten $\alpha \in R$ sowie Nullstellen $\alpha_1, \ldots, \alpha_m$ aus einem Erweiterungsring R' zu R. Dann gilt für die Resultante zum formalen Grad (m, n)*

$$\operatorname{res}(f, g) = \alpha^n \prod_{i=1}^{m} g(\alpha_i).$$

Besitzt auch g eine Zerlegung $g = \beta \prod_{j=1}^{n} (X - \beta_j)$ mit einer Konstanten $\beta \in R$ sowie Nullstellen $\beta_1, \ldots, \beta_n \in R'$, so folgt zudem

$$\operatorname{res}(f, g) = \alpha^n \prod_{i=1}^{m} g(\alpha_i) = \alpha^n \beta^m \prod_{\substack{1 \leq i \leq m \\ 1 \leq j \leq n}} (\alpha_i - \beta_j).$$

Beweis. Aufgrund von Bemerkung 4 können wir $R = R'$ und $\alpha = 1$ annehmen (sowie $\beta = 1$ in der Zerlegung von g), so dass f ein normiertes

Polynom ist, welches in $R[X]$ vollständig in Linearfaktoren zerfällt. Man prüft nun leicht nach, dass $\operatorname{res}(X - \alpha_i, g) = g(\alpha_i)$ gilt, entweder indem man die Definition der Resultante in direkter Weise verifiziert oder Satz 7 verwendet. Weiter schließt man aus der Multiplikativität der Norm von Elementen in $R[X]/(f)$ über R bzw. der Multiplikativität der Determinante, dass man für Polynome $g_1, g_2 \in R[X]$ die Relation

$$\operatorname{res}(f, g_1 g_2) = \operatorname{res}(f, g_1) \cdot \operatorname{res}(f, g_2)$$

hat. Unter Benutzung von Bemerkung 4 (i) folgt hieraus für Polynome f_1, f_2 aus $R[X]$ mit $\operatorname{grad} f_i \leq m_i$ die Relation

$$\operatorname{res}(f_1 f_2, g) = \operatorname{res}(f_1, g) \cdot \operatorname{res}(f_2, g),$$

wobei die Resultanten zu den formalen Graden $(m_1 + m_2, n)$ bzw. (m_1, n) und (m_2, n) gebildet werden. Wendet man letztere Gleichung wiederholt auf die Faktorisierung von f an, so erhält man die gewünschten Formeln. □

Wir wollen nun noch auf die bereits angekündigte Charakterisierung der Diskriminante mittels der Resultante eingehen.

Korollar 10. *Es sei $f \in R[X]$ ein normiertes Polynom vom Grad $m > 0$ und f' seine Ableitung. Dann besteht zwischen der Diskriminante Δ_f und der Resultante* $\operatorname{res}(f, f')$ *zum formalen Grad $(m, m-1)$ die Beziehung*

$$\Delta_f = (-1)^{m(m-1)/2} \operatorname{res}(f, f').$$

Für $A = R[X]/(f)$ und $x \in A$ als Restklasse zu $X \in R[X]$ gilt

$$\Delta_f = (-1)^{m(m-1)/2} \mathrm{N}_{A/R}\big(f'(x)\big).$$

Beweis. Die zweite Formel folgt mit Satz 7 aus der ersten. Um die erste Formel zu erhalten, dürfen wir R aufgrund der Definition der Diskriminante sowie nach Bemerkung 4 (iii) erweitern. Wir können somit annehmen, dass f über R vollständig in Linearfaktoren zerfällt. Man ersetze nämlich ähnlich wie beim Verfahren von Kronecker 3.4/1 den Ring R durch $R' = R[X]/(f)$. Es hat dann f zumindest eine Nullstelle in R', nämlich die Restklasse $\overline{x}$ zu X. Sodann dividiert man den Linearfaktor $X - \overline{x}$ aus f aus und erhält ein

normiertes Polynom vom Grad $m-1$, welches man in gleicher Weise weiterbehandelt. Nach endlich vielen Schritten erhält man einen Erweiterungsring von R, über dem f vollständig in Linearfaktoren zerfällt.

Es gelte also $f = \prod_{i=1}^{m}(X-\alpha_i)$. Sodann folgt mit Korollar 9

$$\operatorname{res}(f,f') = \prod_{i=1}^{m} f'(\alpha_i).$$

Aufgrund der Produktregel ergibt sich

$$f' = \sum_{i=1}^{m}(X-\alpha_1)\dots(X-\alpha_{i-1})(X-\alpha_{i+1})\dots(X-\alpha_m)$$

und somit

$$f'(\alpha_i) = (\alpha_i-\alpha_1)\dots(\alpha_i-\alpha_{i-1})(\alpha_i-\alpha_{i+1})\dots(\alpha_i-\alpha_m).$$

Dies bedeutet aber

$$\begin{aligned}\operatorname{res}(f,f') &= \prod_{i\neq j}(\alpha_i-\alpha_j) = (-1)^{m(m-1)/2}\prod_{i<j}(\alpha_i-\alpha_j)^2\\ &= (-1)^{m(m-1)/2}\Delta_f,\end{aligned}$$

wie behauptet. □

Insbesondere beinhaltet Korollar 10 eine explizite Formel zur Berechnung der Diskriminante. Als einfaches Beispiel wollen wir die Diskriminante des Polynoms $f = X^3 + aX + b \in R[X]$ bestimmen, welche wir (für den Fall eines Körpers $K = R$) in Abschnitt 4.3 zum Studium der Galois-Gruppe von f bereits verwendet haben. Es gilt nach Korollar 10

$$\Delta_f = -\operatorname{res}(f,f') = -\det\begin{pmatrix}1&0&a&b&0\\0&1&0&a&b\\3&0&a&0&0\\0&3&0&a&0\\0&0&3&0&a\end{pmatrix}.$$

Um den Rechenaufwand in Grenzen zu halten, sollte man das 3-fache der 1. Zeile von der 3. Zeile subtrahieren sowie das 3-fache der 2. Zeile von der 4. Zeile. Dies ergibt

$$\Delta_f = -\det\begin{pmatrix} -2a & -3b & 0 \\ 0 & -2a & -3b \\ 3 & 0 & a \end{pmatrix} = -4a^3 - 27b^2.$$

Nach dem gleichen Verfahren zeigt man für $m \geq 2$, dass die Diskriminante des Polynoms $f = X^m + aX + b$ folgenden Wert hat:

$$\Delta_f = (-1)^{m(m-1)/2}\big((1-m)^{m-1}a^m + m^m b^{m-1}\big)$$

Relativ einfach gestaltet sich auch noch der Fall $f = X^4 + aX^2 + bX + c$; man erhält

$$\Delta_f = 144ab^2c - 128a^2c^2 - 4a^3b^2 + 16a^4c - 27b^4 + 256c^3.$$

Hier reduziert man ähnlich wie in den vorstehenden Beispielen die Berechnung der entsprechenden 7-reihigen Determinante mittels elementarer Zeilenumformungen auf eine 4-reihige Determinante.

Es sei abschließend noch darauf hingewiesen, dass man Diskriminanten üblicherweise in einem etwas allgemeineren Rahmen betrachtet. Sei $R \subset A$ eine Erweiterung von Ringen, so dass A als R-Modul ein endliches freies Erzeugendensystem $e_1, \ldots, e_n$ besitzt. Wie in der Theorie der Vektorräume lässt sich dann für jede R-lineare Abbildung $\varphi\colon A \longrightarrow A$ deren *Spur* definieren. Wird etwa φ bezüglich eines freien R-Erzeugendensystems von A durch die Matrix $(a_{ij}) \in R^{n\times n}$ beschrieben, so gilt $\operatorname{Spur}\varphi = \sum_{i=1}^n a_{ii} \in R$. Insbesondere kann man für $a \in A$ die R-lineare Abbildung "Multiplikation mit a"

$$\varphi_a\colon A \longrightarrow A, \qquad x \longmapsto ax,$$

betrachten. Man bezeichnet deren Spur mit $\operatorname{Sp}_{A/R}(a)$ und nennt dies die *Spur von a* bezüglich der Erweiterung A/R; vgl. auch Abschnitt 4.7.

Ist nun $x_1, \ldots, x_n$ ein System von Elementen in A, so betrachtet man die Matrix $(\operatorname{Sp}_{A/R}(x_i x_j))_{i,j=1,\ldots,n} \in R^{n\times n}$ und definiert die *Diskriminante* von $x_1, \ldots, x_n$ bezüglich der Ringerweiterung $R \subset A$ durch

$$D_{A/R}(x_1, \ldots, x_n) = \det\big(\operatorname{Sp}_{A/R}(x_i x_j)\big)_{i,j=1,\ldots,n}.$$

Es besteht dann folgender Zusammenhang zwischen der Diskriminante eines Polynoms und der Diskriminante eines Systems von Elementen:

Satz 11. *Es sei $f \in R[X]$ ein normiertes Polynom vom Grad $n > 0$. Wie in Satz 7 betrachte man $A = R[X]/(f)$ als R-Modul mit $x^0, \ldots, x^{n-1}$ als*

freiem Erzeugendensystem; $x \in A$ *sei die Restklasse zu* $X \in R[X]$. *Dann gilt*

$$\Delta_f = D_{A/R}(x^0, \ldots, x^{n-1}).$$

Beweis. Wir beginnen mit einem Reduktionsschritt, der zeigt, dass man die Gleichung nur für gewisse Ringe R und Polynome f nachweisen muss. Sei $\tau\colon \hat{R} \longrightarrow R$ ein Ringhomomorphismus, und sei $\hat{f} \in \hat{R}[X]$ ein normiertes Polynom vom Grad n, welches bezüglich des von τ induzierten Homomorphismus $\hat{R}[X] \longrightarrow R[X]$ ein Urbild zu $f \in R[X]$ bilde. Dann gibt τ Anlass zu einem Ringhomomorphismus

$$\tau'\colon \hat{A} = \hat{R}[X]\big/(\hat{f}) \longrightarrow R[X]\big/(f) = A.$$

Schreiben wir $\hat{x}$ für die Restklasse von X in $\hat{R}[X]/(\hat{f})$, so bilden die Potenzen $\hat{x}^0, \ldots, \hat{x}^{n-1}$ ein freies Erzeugendensystem von $\hat{A}$ als $\hat{R}$-Modul, genau wie auch $x^0, \ldots, x^{n-1}$ ein freies Erzeugendensystem von A als R-Modul bilden. Weiter gilt $\tau'(\hat{x}^i) = x^i$ für $i = 0, \ldots, n-1$. Wir wollen die Multiplikation mit einem Element $\hat{a} \in \hat{A}$, also die $\hat{R}$-lineare Abbildung $\varphi_{\hat{a}}\colon \hat{A} \longrightarrow \hat{A}$, mit der entsprechenden R-linearen Abbildung $\varphi_a\colon A \longrightarrow A$ vergleichen, wobei $a = \tau'(\hat{a})$ gelte. Da τ' ein Ringhomomorphismus ist, sieht man, dass die beschreibende Matrix M_a zu φ_a (bezüglich des freien Erzeugendensystems $x^0, \ldots, x^{n-1}$) aus der entsprechenden Matrix $M_{\hat{a}}$ zu $\varphi_{\hat{a}}$ gewonnen wird, indem man $M_{\hat{a}}$ mit τ von $\hat{R}^{n\times n}$ nach $R^{n\times n}$ transportiert. Deshalb folgt $\mathrm{Sp}_{A/R}(a) = \tau(\mathrm{Sp}_{\hat{A}/\hat{R}}(\hat{a}))$ sowie insbesondere

$$D_{A/R}(x^0, \ldots, x^{n-1}) = \tau\big(D_{\hat{A}/\hat{R}}(\hat{x}^0, \ldots, \hat{x}^{n-1})\big), \qquad \Delta_f = \tau(\Delta_{\hat{f}}),$$

Letzeres aufgrund der Definition der Diskriminante eines Polynoms. Ist also die Behauptung des Satzes für $\hat{R}$ und $\hat{f}$ bekannt, so auch für R und f.

Man betrachte nun das Diagramm von Ring- bzw. Körpererweiterungen

$$\begin{array}{ccc} \mathbb{Z}[T_1, \ldots, T_n] & \subset & \mathbb{Q}(T_1, \ldots, T_n) \\ \bigcup & & \bigcup \\ \mathbb{Z}[s_1, \ldots, s_n] & \subset & \mathbb{Q}(s_1, \ldots, s_n), \end{array}$$

wobei $s_1, \ldots, s_n$ die elementarsymmetrischen Polynome in $T_1, \ldots, T_n$ seien. Weiter sei $f = X^n + c_1X^{n-1} + \ldots + c_n \in R[X]$ ein normiertes Polynom über einem Ring R. Dann lässt sich ein Ringhomomorphismus

$\mathbb{Z}[s_1, \ldots, s_n] \longrightarrow R$ durch $s_j \longmapsto (-1)^j c_j$ definieren, und es folgt aufgrund unserer Vorüberlegung, dass wir die Behauptung des Satzes nur für $R = \mathbb{Z}[s_1, \ldots, s_n]$ und $f = \sum_{j=0}^{n} (-1)^j s_j X^{n-j}$ beweisen brauchen. Außerdem können wir, da $\mathbb{Z}[s_1, \ldots, s_n]$ ein Unterring von $\mathbb{Q}(s_1, \ldots, s_n)$ ist, sogar $R = \mathbb{Q}(s_1, \ldots, s_n)$ annehmen, wobei f irreduzibel in $\mathbb{Q}(s_1, \ldots, s_n)[X]$ ist, wie wir in 4.3 gesehen haben. Insgesamt genügt es daher, den Fall zu betrachten, wo $R = K$ ein Körper und f ein normiertes irreduzibles Polynom in $K[X]$ ist. Insbesondere ist $L = A = K[X]/(f)$ dann ein endlich-algebraischer Erweiterungskörper von K. Diese Situation wollen wir im Folgenden als gegeben annehmen.

Nach Definition gilt

$$D_{L/K}(x^0, \ldots, x^{n-1}) = \det\bigl(\mathrm{Sp}_{L/K}(x^{i+j})\bigr)_{i,j=0,\ldots,n-1}.$$

Zur Berechnung von $\mathrm{Sp}_{L/K}(x^{i+j})$ zerlegen wir f über einem algebraischen Abschluss von L in Linearfaktoren, etwa $f = \prod_{k=1}^{n}(X - \alpha_k)$, und machen einen Vorgriff auf Abschnitt 4.7. Nach 4.7/4 gilt nämlich

$$\mathrm{Sp}_{L/K}(x^{i+j}) = \sum_{k=1}^{n} \alpha_k^{i+j}.$$

Ist $V = (\alpha_{i+1}^j)_{i,j=0,\ldots,n-1}$ die Vandermondesche Matrix zu $\alpha_1, \ldots, \alpha_n$, so folgt

$$\bigl(\mathrm{Sp}_{L/K}(x^{i+j})\bigr)_{i,j=0,\ldots,n-1} = V^t \cdot V,$$

und wegen $\det V = \prod_{i<j}(\alpha_j - \alpha_i)$ ergibt sich

$$D_{L/K}(x^0, \ldots, x^{n-1}) = (\det V)^2 = \prod_{i<j}(\alpha_i - \alpha_j)^2 = \Delta_f.$$

□

Lernkontrolle und Prüfungsvorbereitung

1. Wie lautet die erweiterte modultheoretische Version des Hauptsatzes über symmetrische Polynome?
2. Sei $f \in R[X]$ ein normiertes Polynom vom Grad $n > 0$ über einem Ring R. Zeige, dass $X^0, \ldots, X^{n-1}$ ein freies Erzeugendensystem von $R[X]$ als Modul über dem Unterring $R[f]$ bilden, wobei f algebraisch unabhängig über R ist.

+3. Skizziere den Beweis zu Punkt 1.

4. Sei R ein Ring und $f \in R[X]$ ein normiertes Polynom. Definiere die Diskriminante von f.

5. Zeige für ein normiertes Polynom $f \in K[X]$ über einem Körper K, dass die Diskriminante Δ_f genau dann verschwindet, wenn f in einem algebraischen Abschluss von K mehrfache Nullstellen besitzt.

6. Definiere die Resultante zweier Polynome mit Koeffizienten aus einem gegebenen Ring R.

7. Es sei f ein normiertes Polynom mit Koeffizienten aus einem Ring R. Setze $A = R[X]/(f)$ und charakterisiere die Resultante $\operatorname{res}(f, g)$ für Polynome $g \in R[X]$ mit Hilfe der Norm $\mathrm{N}_{A/R}$ von A über R.

+8. Führe den Beweis zu Punkt 7.

9. Es seien f, g nicht-triviale Polynome vom Grad m bzw. $\leq n$ mit Koeffizienten aus einem Körper K. Nutze Punkt 7, um zu zeigen, dass f und g genau dann eine gemeinsame Nullstelle in einem algebraischen Abschluss von K haben, wenn die Resultante $\operatorname{res}(f, g)$ zum formalen Grad (m, n) verschwindet.

10. Wie lässt sich die Diskriminante eines normierten Polynoms vom Grad > 0 mit Hilfe der Resultante von f und seiner Ableitung f' beschreiben?

+11. Es sei $R \subset A$ eine Ringerweiterung, so dass A als R-Modul ein freies Erzeugendensystem der Länge n besitzt. Erkläre die Diskriminante für Systeme $(x_1, \ldots, x_n)$ von Elementen aus A und stelle den Zusammenhang her zur Diskriminante von Polynomen in $R[X]$.

Übungsaufgaben

1. *Welche Rolle spielt der Hauptsatz über symmetrische Polynome, wenn man für Polynome des Typs $f = X^n + a_1 X^{n-1} + \ldots + a_n$ deren Diskriminante Δ_f definieren möchte? Warum sollte man symmetrische Polynome mit Koeffizienten aus einem Ring betrachten, selbst wenn man die Diskriminante nur für Polynome über Körpern benötigt?*

2. Betrachte den Polynomring $R[T_1, T_2, T_3]$ über einem Ring R und schreibe das symmetrische Polynom $T_1^3 + T_2^3 + T_3^3$ als Polynom in den zugehörigen elementarsymmetrischen Polynomen.

3. Es sei R ein Ring. Verifiziere die folgenden Formeln für Diskriminanten Δ_f zu Polynomen $f \in R[X]$:
   (i) $f = X^2 + aX + b$,
   $\Delta_f = a^2 - 4b$.
   (ii) $f = X^m + aX + b$ für $m \geq 2$.
   $\Delta_f = (-1)^{m(m-1)/2}((1-m)^{m-1}a^m + m^m b^{m-1})$.
   (iii) $f = X^3 + aX^2 + bX + c$,
   $\Delta_f = a^2b^2 + 18abc - 4a^3c - 4b^3 - 27c^2$.
   (iv) $f = X^4 + aX^2 + bX + c$,
   $\Delta_f = 144ab^2c - 128a^2c^2 - 4a^3b^2 + 16a^4c - 27b^4 + 256c^3$.
4. Es sei R ein Ring. Bestimme für zwei Polynome $f, g \in R[X]$ vom formalen Grad (m, n) die zugehörige Resultante $\operatorname{res}(f, g)$ in folgenden Fällen:
   (i) $g = g_0 \in R$ (konstantes Polynom), $m = 0$.
   (ii) $g = g_0 \in R$ (konstantes Polynom), $m = 1$.
   (iii) $f = a_0X + a_1$, $g = b_0X + b_1$, $m = n = 1$.
5. Zeige:
$$\operatorname{res}(a_0X^2 + a_1X + a_2, b_0X^2 + b_1X + b_2) = (a_0b_2 - a_2b_0)^2 + (a_1b_2 - a_2b_1)(a_1b_0 - a_0b_1).$$
6. Sei R ein Ring, und seien $f, g \in R[X]$ normierte Polynome. Zeige:
$$\Delta_{fg} = \Delta_f \cdot \Delta_g \cdot \operatorname{res}(f, g)^2.$$
7. Es sei R ein Ring und $f \in R[X]$ ein normiertes Polynom. Zeige für $c \in R$, dass die Polynome f und $g = f(X + c)$ dieselbe Diskriminante haben.

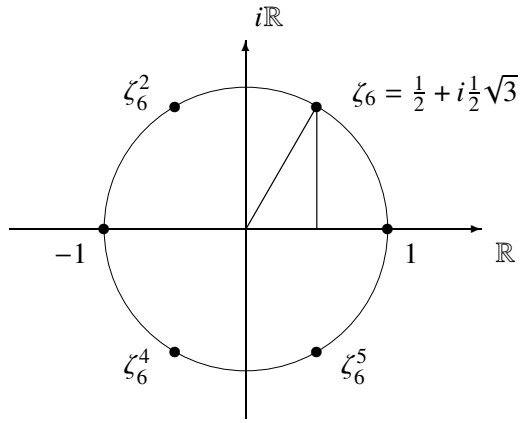
4.5 Einheitswurzeln

Wir fixieren in diesem Abschnitt einen Körper K sowie einen algebraischen Abschluss $\overline{K}$. Für $n \in \mathbb{N} - \{0\}$ bezeichnet man die Nullstellen des Polynoms $X^n - 1$ als *n-te Einheitswurzeln* (in $\overline{K}$), sie bilden eine Untergruppe $U_n \subset \overline{K}^*$. Falls $\operatorname{char} K = 0$ oder, allgemeiner, falls $\operatorname{char} K$ kein Teiler von n ist, so haben $X^n - 1$ und seine Ableitung $D(X^n - 1) = nX^{n-1}$ keine gemeinsamen Nullstellen. Folglich ist $X^n - 1$ in diesem Falle separabel, d. h. es gilt $\operatorname{ord} U_n = n$. Ansonsten betrachte man im Falle positiver Charakteristik

$p = \operatorname{char} K > 0$ eine Zerlegung $n = p^r n'$ mit $p \nmid n'$. Das Polynom $X^{n'} - 1$ ist aus den oben genannten Gründen separabel, und seine Nullstellen stimmen wegen $X^n - 1 = (X^{n'} - 1)^{p^r}$ mit denjenigen von $X^n - 1$ überein. Folglich gilt $U_n = U_{n'}$ und damit insbesondere $\operatorname{ord} U_n = n'$. Man kann sich daher bei der Betrachtung der Gruppen U_n auf den Fall $\operatorname{char} K \nmid n$ beschränken. Hauptziel ist im Folgenden das Studium von Körpern, die aus K durch Adjunktion von Einheitswurzeln entstehen. Zunächst können wir mit 3.6/14 feststellen:

Satz 1. *Es sei $n \in \mathbb{N} - \{0\}$ mit $\operatorname{char} K \nmid n$. Dann ist die Gruppe U_n der n-ten Einheitswurzeln in $\overline{K}$ zyklisch von der Ordnung n.*

Man nennt eine Einheitswurzel $\zeta \in U_n$ eine *primitive n-te Einheitswurzel*, wenn ζ die Gruppe U_n erzeugt. Beispielsweise sind $1, i, -1, -i$ die 4-ten Einheitswurzeln in $\mathbb{C}$, wobei i und $-i$ primitive 4-te Einheitswurzeln darstellen. Alle Einheitswurzeln in $\mathbb{C}$ sind vom Betrag 1, liegen also auf der Kreislinie $\{z \in \mathbb{C}\,;\, |z| = 1\}$. Unter Benutzung der komplexen Exponentialfunktion lassen sich die n-ten Einheitswurzeln in $\mathbb{C}$ in einfacher Weise beschreiben. Es sind dies gerade die Potenzen der primitiven n-ten Einheitswurzel $\zeta_n = e^{2\pi i/n}$, wobei wir den Fall $n = 6$ hier zeichnerisch illustrieren wollen:



In Anbetracht des komplexen Falls sagt man, dass die n-ten Einheitswurzeln "den (Einheits-)Kreis teilen". Man nennt daher Körper, die aus $\mathbb{Q}$ durch Adjunktion einer Einheitswurzel entstehen, auch *Kreisteilungskörper*.

Bemerkung 2. *Es seien $m, n \in \mathbb{N} - \{0\}$ teilerfremd. Dann ist die Abbildung*

$$h\colon U_m \times U_n \longrightarrow U_{mn}, \qquad (\zeta, \eta) \longmapsto \zeta\eta,$$

ein Isomorphismus von Gruppen. Ist $\zeta_m \in U_m$ eine primitive m-te und $\zeta_n \in U_n$ eine primitive n-te Einheitswurzel, so ist $\zeta_m\zeta_n$ eine primitive mn-te Einheitswurzel.

Beweis. Wir dürfen annehmen, dass char K kein Teiler von mn ist. Da U_m und U_n Untergruppen von U_{mn} sind, ist h ein wohldefinierter Homomorphismus kommutativer Gruppen. Weiter sind U_m und U_n gemäß Satz 1 zyklisch von den Ordnungen m bzw. n. Ist nun $\zeta_m \in U_m$ eine primitive m-te und $\zeta_n \in U_n$ eine primitive n-te Einheitswurzel, so besitzt $(\zeta_m, \zeta_n) \in U_m \times U_n$ nach 3.6/13 als Produkt der Elemente $(\zeta_m, 1)$ und $(1, \zeta_n)$ die Ordnung mn, erzeugt also die Gruppe $U_m \times U_n$. Ebenfalls nach 3.6/13 hat $\zeta_m\zeta_n \in U_{mn}$ die Ordnung mn, ist also eine primitive mn-te Einheitswurzel und erzeugt somit U_{mn}. Es folgt, dass h ein Isomorphismus ist. □

Als Nächstes wollen wir die primitiven unter den n-ten Einheitswurzeln genauer studieren. Um deren Anzahl zu beschreiben, benötigen wir die sogenannte Eulersche φ-Funktion.

Definition 3. *Für $n \in \mathbb{N}-\{0\}$ bezeichne $\varphi(n)$ die Ordnung der multiplikativen Gruppe $(\mathbb{Z}/n\mathbb{Z})^*$, also der Einheitengruppe des Restklassenrings $\mathbb{Z}/n\mathbb{Z}$. Es heißt $\varphi\colon \mathbb{N} - \{0\} \longrightarrow \mathbb{N}$ die* Eulersche φ-Funktion.

Bemerkung 4. (i) *Für $n \in \mathbb{N}-\{0\}$ gilt*

$$(\mathbb{Z}/n\mathbb{Z})^* = \big\{\overline{a} \in \mathbb{Z}/n\mathbb{Z}\,;\; a \in \mathbb{Z} \text{ mit } \operatorname{ggT}(a,n) = 1\big\},$$
$$\varphi(n) = \#\big\{a \in \mathbb{N}\,;\; 0 \le a < n \text{ und } \operatorname{ggT}(a,n) = 1\big\}.$$

(ii) *Für teilerfremde Zahlen $m, n \in \mathbb{N} - \{0\}$ gilt $\varphi(mn) = \varphi(m)\varphi(n)$. Diese Eigenschaft wird auch als* Multiplikativität der φ-Funktion *bezeichnet.*

(iii) *Für eine Primfaktorzerlegung $n = p_1^{\nu_1} \dots p_r^{\nu_r}$ mit paarweise verschiedenen Primzahlen p_ρ sowie Exponenten $\nu_\rho > 0$ gilt*

$$\varphi(n) = \prod_{\rho=1}^{r} p_\rho^{\nu_\rho - 1}(p_\rho - 1).$$

Beweis. Sei $a \in \mathbb{Z}$. Es gilt $\operatorname{ggT}(a,n) = 1$ genau dann, wenn $a\mathbb{Z} + n\mathbb{Z} = \mathbb{Z}$ gilt, d. h. genau dann, wenn es $c, d \in \mathbb{Z}$ gibt mit $ac + nd = 1$; vgl. 2.4/13.

Letzteres ist äquivalent dazu, dass die Restklasse von a in $\mathbb{Z}/n\mathbb{Z}$ eine Einheit ist. Mit dieser Überlegung ergibt sich Aussage (i).

Zum Nachweis von (ii) benutze man den Chinesischen Restsatz in der Version 2.4/14. Aufgrund dieses Satzes hat man für teilerfremde natürliche Zahlen einen Ringisomorphismus

$$\mathbb{Z}/mn\mathbb{Z} \xrightarrow{\sim} \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$$

und dann auch einen Isomorphismus zwischen den zugehörigen Einheitengruppen

$$(\mathbb{Z}/mn\mathbb{Z})^* \xrightarrow{\sim} (\mathbb{Z}/m\mathbb{Z})^* \times (\mathbb{Z}/n\mathbb{Z})^*,$$

woraus die Multiplikativität der φ-Funktion folgt.

Um (iii) zu erhalten, kann man (ii) anwenden. Es ist dann nur $\varphi(p^\nu)$ für eine Primzahl p und einen positiven Exponenten ν zu bestimmen. Da die Produkte $0 \cdot p, 1 \cdot p, \ldots, (p^{\nu-1} - 1) \cdot p$ gerade alle natürlichen Zahlen d mit $0 \leq d < p^\nu$ darstellen, die nicht zu p^ν teilerfremd sind, folgt mit (i) wie gewünscht

$$\varphi(p^\nu) = p^\nu - p^{\nu-1} = p^{\nu-1}(p-1).$$

□

Satz 5. *Sei $n \in \mathbb{N}$. Ein Element $\overline{a}$ erzeugt die additive zyklische Gruppe $\mathbb{Z}/n\mathbb{Z}$ genau dann, wenn $\overline{a}$ Einheit im Ring $\mathbb{Z}/n\mathbb{Z}$ ist. Ist $n \neq 0$, so enthält $\mathbb{Z}/n\mathbb{Z}$ genau $\varphi(n)$ Elemente, welche $\mathbb{Z}/n\mathbb{Z}$ als zyklische Gruppe erzeugen.*

Beweis. Es wird $\mathbb{Z}/n\mathbb{Z}$ genau dann von $\overline{a}$ erzeugt, wenn die Restklasse $\overline{1}$ zu $1 \in \mathbb{Z}$ in der von $\overline{a}$ erzeugten zyklischen Gruppe liegt. Letzteres ist genau dann der Fall, wenn es ein $r \in \mathbb{Z}$ gibt mit $\overline{1} = r \cdot \overline{a} = \overline{r} \cdot \overline{a}$, d. h. wenn $\overline{a}$ Einheit ist. □

Korollar 6. *Sei K ein Körper und $n \in \mathbb{N} - \{0\}$ mit $\operatorname{char} K \nmid n$. Dann enthält die Gruppe U_n der n-ten Einheitswurzeln genau $\varphi(n)$ primitive n-te Einheitswurzeln. Ist $\zeta \in U_n$ primitive n-te Einheitswurzel, so ist ζ^r für $r \in \mathbb{Z}$ genau dann primitive n-te Einheitswurzel, wenn die Restklasse von r modulo n eine Einheit in $\mathbb{Z}/n\mathbb{Z}$ ist, d. h. wenn $\operatorname{ggT}(r, n) = 1$ gilt.*

Beweis. Aufgrund von Satz 1 ist U_n isomorph zu $\mathbb{Z}/n\mathbb{Z}$; es besitzt also U_n nach Satz 5 genau $\varphi(n)$ primitive n-te Einheitswurzeln. Ist nun $\zeta \in U_n$ eine

primitive n-te Einheitswurzel, so ist der Homomorphismus $\mathbb{Z}/n\mathbb{Z} \longrightarrow U_n$, der die Restklasse $\overline{1} \in \mathbb{Z}/n\mathbb{Z}$ auf ζ abbildet, ein Isomorphismus. Für $r \in \mathbb{Z}$ ist ζ^r genau dann eine primitive n-te Einheitswurzel, wenn das Urbild in $\mathbb{Z}/n\mathbb{Z}$, also die Restklasse $\overline{r}$, die Gruppe $\mathbb{Z}/n\mathbb{Z}$ erzeugt, d. h. genau dann, wenn $\overline{r}$ eine Einheit ist; vgl. Satz 5. □

Ist $\zeta_n \in \overline{K}$ eine primitive n-te Einheitswurzel, so enthält der Körper $K(\zeta_n)$ sämtliche n-ten Einheitswurzeln, ist also als Zerfällungskörper des Polynoms $X^n - 1 \in K[X]$ *normal* über K. Da $X^n - 1$ für $\operatorname{char} K \nmid n$ zudem separabel ist, erkennt man $K(\zeta_n)/K$ als endliche Galois-Erweiterung. Im Falle $K = \mathbb{Q}$ heißt $\mathbb{Q}(\zeta_n)$ der *n-te Kreisteilungskörper*.

Satz 7. *Es sei K ein Körper und $\zeta_n \in \overline{K}$ eine primitive n-te Einheitswurzel mit* $\operatorname{char} K \nmid n$. *Dann gilt*:

(i) *$K(\zeta_n)/K$ ist eine endliche abelsche Galois-Erweiterung von einem Grad, der $\varphi(n)$ teilt.*

(ii) *Jedes $\sigma \in \operatorname{Gal}(K(\zeta_n)/K)$ induziert durch Einschränkung einen Automorphismus der Gruppe U_n der n-ten Einheitswurzeln, und die Abbildung*

$$\psi\colon \operatorname{Gal}\big(K(\zeta_n)/K\big) \longrightarrow \operatorname{Aut}(U_n), \qquad \sigma \longmapsto \sigma|_{U_n},$$

ist ein Monomorphismus von Gruppen.

(iii) *Die Automorphismengruppe $\operatorname{Aut}(U_n)$ ist kanonisch isomorph zur multiplikativen Gruppe $(\mathbb{Z}/n\mathbb{Z})^*$, und zwar vermöge der Abbildung*

$$(\mathbb{Z}/n\mathbb{Z})^* \longrightarrow \operatorname{Aut}(U_n), \qquad \overline{r} \longmapsto (\zeta \longmapsto \zeta^r),$$

die wohldefiniert ist.

Beweis. Wir wissen bereits, dass $K(\zeta_n)/K$ eine endliche Galois-Erweiterung ist. Unter Verwendung der Aussagen (ii) und (iii) lässt sich die Galois-Gruppe $\operatorname{Gal}(K(\zeta_n)/K)$ als Untergruppe von $(\mathbb{Z}/n\mathbb{Z})^*$ auffassen, so dass wir diese als abelsch mit einer Ordnung erkennen, die $\operatorname{ord}(\mathbb{Z}/n\mathbb{Z})^* = \varphi(n)$ teilt. Behauptung (i) folgt somit aus (ii) und (iii).

Zum Nachweis von (ii) beachte man, dass ein Galois-Automorphismus $\sigma \in \operatorname{Gal}(K(\zeta_n)/K)$ die Nullstellen von $X^n - 1$ wiederum auf ebensolche abbildet. Da σ zudem multiplikativ und injektiv ist, erkennt man, dass $\sigma|_{U_n}$ einen Automorphismus der endlichen Gruppe U_n darstellt. Somit definiert $\sigma \longmapsto \sigma|_{U_n}$ einen Gruppenhomomorphismus $\operatorname{Gal}(K(\zeta_n)/K) \longrightarrow \operatorname{Aut}(U_n)$,

und dieser ist injektiv, da ein Automorphismus $\sigma \in \mathrm{Gal}(K(\zeta_n)/K)$, welcher $\zeta_n \in U_n$ festlässt, bereits mit der Identität übereinstimmt.

Für Aussage (iii) schließlich nutzen wir die Eigenschaft, dass U_n zyklisch von der Ordnung n ist, also isomorph zu $\mathbb{Z}/n\mathbb{Z}$ ist. Sodann ist zu zeigen, dass die Abbildung

$$\psi' \colon (\mathbb{Z}/n\mathbb{Z})^* \longrightarrow \mathrm{Aut}(\mathbb{Z}/n\mathbb{Z}), \qquad \overline{r} \longmapsto (\overline{a} \longmapsto r \cdot \overline{a}),$$

ein wohldefinierter Isomorphismus von Gruppen ist, wobei wir mit $\overline{r}$ bzw. $\overline{a}$ die Restklassen in $\mathbb{Z}/n\mathbb{Z}$ zu Elementen $r, a \in \mathbb{Z}$ bezeichnen. Zunächst erkennt man ψ' als wohldefiniert wegen $r \cdot \overline{a} = \overline{ra} = \overline{r} \cdot \overline{a}$. Weiter ist klar, dass die Multiplikation mit einer Einheit $\overline{r} \in (\mathbb{Z}/n\mathbb{Z})^*$ einen Automorphismus der additiven Gruppe $\mathbb{Z}/n\mathbb{Z}$ ergibt und dass ψ' somit injektiv ist. Um einzusehen, dass ψ' auch surjektiv ist, betrachte man einen Automorphismus ρ der additiven Gruppe $\mathbb{Z}/n\mathbb{Z}$. Gilt dann $\rho(\overline{1}) = \overline{r}$, so ergibt sich für $a \in \mathbb{Z}$

$$\rho(\overline{a}) = \rho(\overline{1} \cdot a) = \rho(\overline{1}) \cdot a = \overline{r} \cdot \overline{a},$$

und man erkennt ρ als Multiplikation mit $\overline{r}$. Da eine solche Multiplikation nur für eine Einheit $\overline{r}$ surjektiv ist, folgt $\overline{r} \in (\mathbb{Z}/n\mathbb{Z})^*$ und somit $\rho = \psi'(\overline{r})$, d. h. ψ' ist surjektiv. □

Satz 8. *Es sei $\zeta_n \in \overline{\mathbb{Q}}$ eine primitive n-te Einheitswurzel. Dann ist der n-te Kreisteilungskörper $\mathbb{Q}(\zeta_n)$ eine endliche Galois-Erweiterung über $\mathbb{Q}$ vom Grad $[\mathbb{Q}(\zeta_n) : \mathbb{Q}] = \varphi(n)$ mit Galois-Gruppe*

$$\mathrm{Gal}\big(\mathbb{Q}(\zeta_n)/\mathbb{Q}\big) \xrightarrow{\sim} \mathrm{Aut}(U_n) \simeq (\mathbb{Z}/n\mathbb{Z})^*.$$

Beweis. Ist $f \in \mathbb{Q}[X]$ das Minimalpolynom von ζ_n über $\mathbb{Q}$, so gilt $[\mathbb{Q}(\zeta_n) : \mathbb{Q}] = \mathrm{grad}\, f$, und wir haben lediglich $\mathrm{grad}\, f = \varphi(n)$ zu zeigen, denn die Charakterisierung der Galois-Gruppe $\mathrm{Gal}(\mathbb{Q}(\zeta_n)/\mathbb{Q})$ ist dann eine Konsequenz von Satz 7. Zunächst gilt

$$\big[\mathbb{Q}(\zeta_n) : \mathbb{Q}\big] = \mathrm{grad}\, f \leq \varphi(n),$$

ebenfalls aufgrund von Satz 7.

Wir wollen zeigen, dass jede primitive n-te Einheitswurzel $\zeta \in U_n$ Nullstelle von f ist, was dann aufgrund von Korollar 6 wie gewünscht

grad $f = \varphi(n)$ impliziert. Um dies nachzuweisen, beachte man, dass f als Minimalpolynom von ζ_n ein Teiler von $X^n - 1$ ist. Es gibt also ein Polynom $h \in \mathbb{Q}[X]$ mit

$$X^n - 1 = f \cdot h.$$

Da f nach Definition normiert ist, gilt Gleiches auch für h, und es folgt $f, h \in \mathbb{Z}[X]$ nach 2.7/6.

Sei nun p eine Primzahl mit $p \nmid n$. Dann ist ζ_n^p nach Korollar 6 eine primitive n-te Einheitswurzel, und wir behaupten, dass ζ_n^p eine Nullstelle von f ist. Ist dies nicht der Fall, gilt also $f(\zeta_n^p) \neq 0$, so folgt $h(\zeta_n^p) = 0$. Mit anderen Worten, ζ_n ist Nullstelle von $h(X^p)$. Hieraus ergibt sich wiederum $f | h(X^p)$, etwa $h(X^p) = f \cdot g$, wobei man unter Verwendung von 2.7/6 wie oben sieht, dass g ein normiertes Polynom in $\mathbb{Z}[X]$ ist. Wir wenden nun den Homomorphismus "Reduktion der Koeffizienten modulo p" an,

$$\mathbb{Z}[X] \longrightarrow \mathbb{Z}/p\mathbb{Z}[X] = \mathbb{F}_p[X], \qquad \sum c_i X^i \longmapsto \sum \overline{c}_i X^i,$$

welcher die kanonische Projektion $\mathbb{Z} \longrightarrow \mathbb{Z}/p\mathbb{Z}$ fortsetzt. Dann zeigt die Gleichung $\overline{h}^p = \overline{h}(X^p) = \overline{f} \cdot \overline{g}$, dass $\overline{h}$ und $\overline{f}$ nicht teilerfremd in $\mathbb{F}_p[X]$ sind. Folglich hat das Polynom $X^n - 1 = \overline{f} \cdot \overline{h} \in \mathbb{F}_p[X]$ mehrfache Nullstellen in einem algebraischen Abschluss von $\mathbb{F}_p$. Dies steht aber im Widerspruch zu $p \nmid n$, so dass die obige Annahme $f(\zeta_n^p) \neq 0$ nicht haltbar ist. Folglich ist ζ_n^p Nullstelle von f.

Ist nun ζ eine beliebige primitive n-te Einheitswurzel, so bleibt noch zu zeigen, dass ζ Nullstelle von f ist. Gilt etwa $\zeta = \zeta_n^m$, so folgt $\mathrm{ggT}(m, n) = 1$ aufgrund von Korollar 6. Man kann daher ζ aus ζ_n durch sukzessives Bilden von Primpotenzen gewinnen, wobei die primen Exponenten alle teilerfremd zu n sind. Eine wiederholte Anwendung des obigen Argumentes zeigt daher $f(\zeta) = 0$. □

Für teilerfremde Zahlen $m, n \in \mathbb{N} - \{0\}$ und primitive m-te, n-te und (mn)-te Einheitswurzeln $\zeta_m, \zeta_n, \zeta_{mn} \in \overline{\mathbb{Q}}$ liefert die im Beweis zu Bemerkung 4 (ii) benutzte Zerlegung

$$(\mathbb{Z}/mn\mathbb{Z})^* \xrightarrow{\sim} (\mathbb{Z}/m\mathbb{Z})^* \times (\mathbb{Z}/n\mathbb{Z})^*$$

in Verbindung mit Satz 8 eine Zerlegung von Galois-Gruppen

$$\mathrm{Gal}\big(\mathbb{Q}(\zeta_{mn})/\mathbb{Q}\big) \xrightarrow{\sim} \mathrm{Gal}\big(\mathbb{Q}(\zeta_m)/\mathbb{Q}\big) \times \mathrm{Gal}\big(\mathbb{Q}(\zeta_m)/\mathbb{Q}\big).$$

Wir wollen diese noch etwas genauer charakterisieren.

Korollar 9. *Es seien* $\zeta_m, \zeta_n \in \overline{\mathbb{Q}}$ *primitive m-te bzw. n-te Einheitswurzeln mit* $\mathrm{ggT}(m,n) = 1$. *Dann gilt*

$$\mathbb{Q}(\zeta_m) \cap \mathbb{Q}(\zeta_n) = \mathbb{Q},$$

und die Abbildung

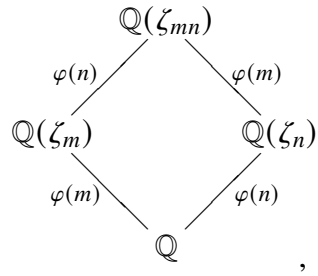
$$\begin{aligned} \mathrm{Gal}\big(\mathbb{Q}(\zeta_m,\zeta_n)/\mathbb{Q}\big) &\longrightarrow \mathrm{Gal}\big(\mathbb{Q}(\zeta_m)/\mathbb{Q}\big) \times \mathrm{Gal}\big(\mathbb{Q}(\zeta_n)/\mathbb{Q}\big), \\ \sigma &\longmapsto (\sigma|_{\mathbb{Q}(\zeta_m)}, \sigma|_{\mathbb{Q}(\zeta_n)}), \end{aligned}$$

ist ein Isomorphismus.

Beweis. Aus Bemerkung 2 folgt, dass $\zeta_{mn} = \zeta_m\zeta_n$ eine primitive mn-te Einheitswurzel ist. Somit berechnet sich das Kompositum von $\mathbb{Q}(\zeta_m)$ und $\mathbb{Q}(\zeta_n)$ zu

$$\mathbb{Q}(\zeta_m) \cdot \mathbb{Q}(\zeta_n) = \mathbb{Q}(\zeta_{mn}).$$

Man hat dann folgendes Diagramm von Körpererweiterungen



,

wobei die Grade von $\mathbb{Q}(\zeta_{mn})$, $\mathbb{Q}(\zeta_m)$ und $\mathbb{Q}(\zeta_n)$ über $\mathbb{Q}$ nach Satz 8 durch $\varphi(mn)$, $\varphi(m)$ und $\varphi(n)$ gegeben sind und wobei

$$\big[\mathbb{Q}(\zeta_{mn}) : \mathbb{Q}(\zeta_m)\big] = \varphi(n), \qquad \big[\mathbb{Q}(\zeta_{mn}) : \mathbb{Q}(\zeta_n)\big] = \varphi(m)$$

gilt, da $\varphi(mn) = \varphi(m) \cdot \varphi(n)$. Sei nun $L = \mathbb{Q}(\zeta_m) \cap \mathbb{Q}(\zeta_n)$. Benutzt man $\mathbb{Q}(\zeta_{mn}) = \mathbb{Q}(\zeta_m, \zeta_n)$, so wird klar, dass ζ_m über $\mathbb{Q}(\zeta_n)$ den Grad $\varphi(m)$, also über L einen Grad $\geq \varphi(m)$ hat. Aus der Abschätzung

$$\varphi(m) = \big[\mathbb{Q}(\zeta_m) : \mathbb{Q}\big] = \big[\mathbb{Q}(\zeta_m) : L\big] \cdot \big[L : \mathbb{Q}\big] \geq \varphi(m) \cdot \big[L : \mathbb{Q}\big]$$

ergibt sich jedoch $[L : \mathbb{Q}] = 1$ und daher $L = \mathbb{Q}$. Somit wird 4.1/12 (ii) anwendbar, und es folgt, dass die zu betrachtende Abbildung einen Isomorphismus zwischen $\mathrm{Gal}(\mathbb{Q}(\zeta_{mn})/\mathbb{Q})$ und dem kartesischen Produkt der Galois-Gruppen $\mathrm{Gal}(\mathbb{Q}(\zeta_m)/\mathbb{Q})$ und $\mathrm{Gal}(\mathbb{Q}(\zeta_n)/\mathbb{Q})$ definiert. □

Wir wollen nun das Polynom $X^n - 1$, dessen Nullstellen die n-ten Einheitswurzeln sind, in die sogenannten Kreisteilungspolynome zerlegen.

Definition 10. *Es sei K ein Körper. Für $n \in \mathbb{N} - \{0\}$ mit* $\mathrm{char}\, K \nmid n$ *seien $\zeta_1, \ldots, \zeta_{\varphi(n)}$ die primitiven n-ten Einheitswurzeln in $\overline{K}$. Dann heißt*

$$\Phi_n = \prod_{i=1}^{\varphi(n)} (X - \zeta_i)$$

das n-te Kreisteilungspolynom *über K.*

Satz 11. (i) *Φ_n ist ein normiertes separables Polynom in $K[X]$ vom Grad $\varphi(n)$.*

(ii) *Für $K = \mathbb{Q}$ gilt $\Phi_n \in \mathbb{Z}[X]$, und Φ_n ist irreduzibel in $\mathbb{Z}[X]$ bzw. $\mathbb{Q}[X]$.*

(iii) $X^n - 1 = \prod_{d|n, d>0} \Phi_d$.

(iv) *Ist $\Phi_n \in \mathbb{Z}[X]$ das n-te Kreisteilungspolynom über $\mathbb{Q}$, so gewinnt man das n-te Kreisteilungspolynom über einem Körper K mit* $\mathrm{char}\, K \nmid n$ *aus Φ_n durch Anwenden des kanonischen Homomorphismus $\mathbb{Z} \longrightarrow K$ auf die Koeffizienten von Φ_n.*

Beweis. Da Φ_n keine mehrfachen Nullstellen hat, ist für (i) nur zu begründen, dass Φ_n Koeffizienten in K besitzt. Es ist $L = K(\zeta_1) = K(\zeta_1, \ldots, \zeta_{\varphi(n)})$ aufgrund von Satz 7 eine endliche Galois-Erweiterung von K. Im Übrigen gilt $\Phi_n \in L[X]$ nach Definition. Da jeder Galois-Automorphismus $\sigma \in \mathrm{Gal}(L/K)$ eine primitive n-te Einheitswurzel wieder in eine solche überführt, also eine Permutation auf der Menge der primitiven n-ten Einheitswurzeln induziert, ist Φ_n invariant unter $\mathrm{Gal}(L/K)$, und es folgt $\Phi_n \in K[X]$ mit 4.1/5 (ii).

Es sei nun $K = \mathbb{Q}$. Da jede primitive n-te Einheitswurzel ζ vom Grad $\varphi(n)$ über $\mathbb{Q}$ ist und da $\Phi_n \in \mathbb{Q}[X]$ ein normiertes Polynom vom Grad

$\varphi(n)$ ist mit $\Phi_n(\zeta) = 0$, ist Φ_n bereits das Minimalpolynom von ζ über $\mathbb{Q}$, insbesondere also irreduzibel. Aus $\Phi_n \mid (X^n - 1)$ und der Normiertheit von Φ_n schließt man dann $\Phi_n \in \mathbb{Z}[X]$ mit Hilfe von 2.7/6. Natürlich ist Φ_n auch irreduzibel in $\mathbb{Z}[X]$, vgl. 2.7/7, so dass Aussage (ii) klar ist.

Die Formel in (iii) schließlich wird gewonnen durch Zusammenfassen von Faktoren in der Zerlegung

$$X^n - 1 = \prod_{\zeta \in U_n} (X - \zeta).$$

Bezeichnet nämlich P_d für $d \in \mathbb{N} - \{0\}$ die Menge der primitiven d-ten Einheitswurzeln in $\overline{K}$, so ist U_n die disjunkte Vereinigung aller P_d, $d \mid n$, $d > 0$. Folglich erhält man

$$X^n - 1 = \prod_{d|n, d>0} \prod_{\zeta \in P_d} (X - \zeta) = \prod_{d|n, d>0} \Phi_d.$$

Zum Beweis von Aussage (iv) verwenden wir für das n-te Kreisteilungspolynom die Bezeichnungen Φ_n bzw. $\tilde{\Phi}_n$, je nachdem, ob wir über $\mathbb{Q}$ oder über einem sonstigen Körper K arbeiten. Zu zeigen ist, dass der kanonische Homomorphismus $\tau\colon \mathbb{Z}[X] \longrightarrow K[X]$ das Polynom Φ_n auf $\tilde{\Phi}_n$ abbildet, d. h. dass $\tau(\Phi_n) = \tilde{\Phi}_n$ gilt. Letztere Relation beweisen wir mit Induktion nach n. Für $n = 1$ besteht die Gleichung

$$\tau(\Phi_1) = X - 1 = \tilde{\Phi}_1.$$

Sei also $n > 1$. Dann haben wir über $\mathbb{Z}$

$$X^n - 1 = \Phi_n \cdot \prod_{d|n, 0<d<n} \Phi_d$$

sowie über K

$$X^n - 1 = \tilde{\Phi}_n \cdot \prod_{d|n, 0<d<n} \tilde{\Phi}_d.$$

Unter Benutzung der Induktionsvoraussetzung und der Nullteilerfreiheit von $K[X]$ ergibt sich wie gewünscht $\tau(\Phi_n) = \tilde{\Phi}_n$. □

Ausgehend von $\Phi_1 = X - 1$ kann man die Kreisteilungspolynome mit Hilfe der Formel in Satz 11 (iii) rekursiv berechnen. Im Falle $K = \mathbb{Q}$ stellt diese Formel sogar die Primfaktorzerlegung von $X^n - 1$ in $\mathbb{Z}[X]$ oder $\mathbb{Q}[X]$

dar, denn die Faktoren Φ_d sind gemäß (ii) irreduzibel. Für eine Primzahl p etwa hat man

$$X^p - 1 = \Phi_1 \cdot \Phi_p,$$

so dass

$$\Phi_p = X^{p-1} + X^{p-2} + \ldots + 1$$

folgt. Sind weiter p und q zwei verschiedene Primzahlen, so gilt

$$X^{pq} - 1 = \Phi_1 \cdot \Phi_p \cdot \Phi_q \cdot \Phi_{pq}$$

und daher

$$\Phi_{pq} = \frac{X^{pq} - 1}{(X-1) \cdot (X^{p-1} + \ldots + 1) \cdot (X^{q-1} + \ldots + 1)}.$$

Beispielsweise erhält man

$$\Phi_6 = \frac{X^6 - 1}{(X-1) \cdot (X+1) \cdot (X^2 + X + 1)} = X^2 - X + 1.$$

Wir wollen hier die ersten 12 Kreisteilungspolynome explizit auflisten:

$$\begin{aligned}
\Phi_1 &= X - 1 \\
\Phi_2 &= X + 1 \\
\Phi_3 &= X^2 + X + 1 \\
\Phi_4 &= X^2 + 1 \\
\Phi_5 &= X^4 + X^3 + X^2 + X + 1 \\
\Phi_6 &= X^2 - X + 1 \\
\Phi_7 &= X^6 + X^5 + X^4 + X^3 + X^2 + X + 1 \\
\Phi_8 &= X^4 + 1 \\
\Phi_9 &= X^6 + X^3 + 1 \\
\Phi_{10} &= X^4 - X^3 + X^2 - X + 1 \\
\Phi_{11} &= X^{10} + X^9 + X^8 + X^7 + X^6 + X^5 + X^4 + X^3 + X^2 + X + 1 \\
\Phi_{12} &= X^4 - X^2 + 1
\end{aligned}$$

Man könnte aufgrund der vorstehenden Beispiele vermuten, dass 1 und -1 die einzigen von Null verschiedenen ganzen Zahlen sind, die als

Koeffizienten der Kreisteilungspolynome auftauchen können. Eine solche Vermutung ist aber nicht haltbar, es ist z. B.

$$\begin{aligned}\Phi_{105} = {} & X^{48} + X^{47} + X^{46} - X^{43} - X^{42} - 2X^{41} - X^{40} - X^{39} \\ & + X^{36} + X^{35} + X^{34} + X^{33} + X^{32} + X^{31} \\ & - X^{28} - X^{26} - X^{24} - X^{22} - X^{20} \\ & + X^{17} + X^{16} + X^{15} + X^{14} + X^{13} + X^{12} \\ & - X^9 - X^8 - 2X^7 - X^6 - X^5 + X^2 + X + 1\end{aligned}$$

das erste Kreisteilungspolynom, welches nicht ausschließlich Koeffizienten vom Betrag ≤ 1 besitzt. Die drei nächsten sind Φ_{165}, Φ_{195} und Φ_{210}, wobei hier, wie auch bei Φ_{105}, die Koeffizienten sämtlich vom Betrag ≤ 2 sind. Man weiß allerdings aufgrund eines Resultats von I. Schur, dass die Koeffizienten der Kreisteilungspolynome nicht beschränkt sind. Für $n = p_1 \cdot \ldots \cdot p_m$, wobei $p_1 < \ldots < p_m$ Primzahlen mit $p_m < p_1 + p_2$ seien, ist nämlich der Koeffizient von X^{p_m} in Φ_n gerade $1 - m$, und man kann mit Hilfe zahlentheoretischer Argumente zeigen, dass es für ungerades m stets Primzahlen $p_1, \ldots, p_m$ mit den vorstehenden Eigenschaften gibt.

Abschließend wollen wir noch speziell auf den Fall endlicher Körper eingehen. Hierzu betrachten wir eine Primpotenz q sowie den Körper $\mathbb{F}_q$ mit q Elementen. Es sei daran erinnert, vgl. 3.8/6, dass die Galois-Gruppe einer endlichen Erweiterung $\mathbb{F}/\mathbb{F}_q$ stets zyklisch von der Ordnung $[\mathbb{F} : \mathbb{F}_q]$ ist und vom relativen Frobenius-Homomorphismus $\mathbb{F} \longrightarrow \mathbb{F}$, $a \longmapsto a^q$ erzeugt wird.

Satz 12. *Für eine Primpotenz q sei $\mathbb{F}_q$ der Körper mit q Elementen. Weiter sei $\zeta \in \overline{\mathbb{F}}_q$ eine primitive n-te Einheitswurzel, wobei* $\mathrm{ggT}(n, q) = 1$ *gelte.*

(i) *Die Injektion* $\psi\colon \mathrm{Gal}(\mathbb{F}_q(\zeta)/\mathbb{F}_q) \hookrightarrow \mathrm{Aut}(U_n)$ *aus Satz* 7 (ii) *bildet den relativen Frobenius-Homomorphismus von $\mathbb{F}_q(\zeta)/\mathbb{F}_q$ unter der Identifizierung* $\mathrm{Aut}(U_n) \simeq (\mathbb{Z}/n\mathbb{Z})^*$ *auf die zu q gehörige Restklasse $\overline{q} \in (\mathbb{Z}/n\mathbb{Z})^*$ ab. Insbesondere induziert ψ einen Isomorphismus zwischen* $\mathrm{Gal}(\mathbb{F}_q(\zeta)/\mathbb{F}_q)$ *und der Untergruppe $\langle \overline{q} \rangle \subset (\mathbb{Z}/n\mathbb{Z})^*$.*

(ii) *Der Grad $[\mathbb{F}_q(\zeta) : \mathbb{F}_q]$ stimmt überein mit der Ordnung von $\overline{q}$ in $(\mathbb{Z}/n\mathbb{Z})^*$.*

(iii) *Das n-te Kreisteilungspolynom Φ_n ist genau dann irreduzibel in $\mathbb{F}_q[X]$, wenn $\overline{q}$ die Gruppe $(\mathbb{Z}/n\mathbb{Z})^*$ erzeugt.*

Beweis. Der relative Frobenius-Homomorphismus über $\mathbb{F}_q$ ist auch auf U_n durch die Abbildung $\zeta \longrightarrow \zeta^q$ gegeben und korrespondiert daher unter dem kanonischen Isomorphismus $\mathrm{Aut}(U_n) \simeq (\mathbb{Z}/n\mathbb{Z})^*$ aus Satz 7 (iii) zu der Restklasse $\overline{q} \in (\mathbb{Z}/n\mathbb{Z})^*$. Weiter ist Aussage (ii) eine Konsequenz von (i), denn es gilt

$$\big[\mathbb{F}_q(\zeta) : \mathbb{F}_q\big] = \operatorname{ord} \mathrm{Gal}\big(\mathbb{F}_q(\zeta)/\mathbb{F}_q\big) = \operatorname{ord}\langle\overline{q}\rangle = \operatorname{ord}\overline{q}.$$

Zum Nachweis von (iii) schließlich beachte man, dass Φ_n genau dann irreduzibel ist, wenn $[\mathbb{F}_q(\zeta) : \mathbb{F}_q] = \operatorname{grad}\Phi_n = \varphi(n)$ gilt. Letzteres ist nach (ii) äquivalent zu der Bedingung, dass $\overline{q}$ die Gruppe $(\mathbb{Z}/n\mathbb{Z})^*$ erzeugt. □

Das n-te Kreisteilungspolynom Φ_n kann also höchstens dann irreduzibel über einem endlichen Körper $\mathbb{F}_q$ sein, wenn die Gruppe $(\mathbb{Z}/n\mathbb{Z})^*$ zyklisch ist. Beispielsweise ist $(\mathbb{Z}/n\mathbb{Z})^*$ zyklisch für eine Primzahl $n = p$, vgl. 3.6/14, oder allgemeiner auch für eine Potenz $n = p^r$ einer Primzahl $p \neq 2$, vgl. Aufgabe 7.

Lernkontrolle und Prüfungsvorbereitung

1. Definiere für einen Körper K und einen Index $n \in \mathbb{N}-\{0\}$ die Gruppe U_n der n-ten Einheitswurzeln in einem algebraischen Abschluss $\overline{K}$ von K. Bestimme die Ordnung von U_n und zeige, dass U_n zyklisch ist.
2. Was versteht man unter einem Kreisteilungskörper, was unter einer primitiven Einheitswurzel?
3. Für teilerfremde Zahlen $m, n \in \mathbb{N}-\{0\}$ sei ζ_m eine primitive m-te und ζ_n eine primitive n-te Einheitswurzel. Zeige, dass $\zeta_m\zeta_n$ eine primitive mn-te Einheitswurzel ist.
4. Gib die Definition der Eulerschen φ-Funktion und zeige, wie sich $\varphi(n)$ für $n \in \mathbb{N}-\{0\}$ berechnen lässt, ausgehend von einer Primfaktorzerlegung von n.
5. Betrachte die zyklische Gruppe $\mathbb{Z}/n\mathbb{Z}$ für $n \in \mathbb{N}$. Charakterisiere die erzeugenden Elemente von $\mathbb{Z}/n\mathbb{Z}$, bestimme deren Anzahl und beschreibe die Automorphismen von $\mathbb{Z}/n\mathbb{Z}$.
6. Es sei K ein Körper, $\overline{K}$ ein algebraischer Abschluss von K und $\zeta_n \in \overline{K}$ eine primitive n-te Einheitswurzel, wobei $n \nmid \operatorname{char} K$. Stelle einen Zusammenhang her zwischen der Gruppe $U_n \subset \overline{K}$ der n-ten Einheitswurzeln und der Gruppe $\mathbb{Z}/n\mathbb{Z}$, sowie zwischen der Galois-Gruppe $\mathrm{Gal}(K(\zeta_n)/K)$ und den Automorphismengruppen von U_n und $\mathbb{Z}/n\mathbb{Z}$.

7. Betrachte den n-ten Kreisteilungskörper $\mathbb{Q}(\zeta_n)$ für ein $n \in \mathbb{N}-\{0\}$ und bestimme den Grad $[\mathbb{Q}(\zeta_n) : \mathbb{Q}]$ sowie die Galoisgruppe $\mathrm{Gal}(\mathbb{Q}(\zeta_n)/\mathbb{Q})$.

⁺8. Zeige für teilerfremde Zahlen $m, n \in \mathbb{N} - \{0\}$ und primitive m-te bzw. n-te Einheitswurzeln $\zeta_m, \zeta_n \in \overline{\mathbb{Q}}$, dass $\mathbb{Q}(\zeta_m) \cap \mathbb{Q}(\zeta_n) = \mathbb{Q}$ gilt sowie $\mathrm{Gal}(\mathbb{Q}(\zeta_m, \zeta_n)/\mathbb{Q}) \simeq \mathrm{Gal}(\mathbb{Q}(\zeta_m)/\mathbb{Q}) \times \mathrm{Gal}(\mathbb{Q}(\zeta_n)/\mathbb{Q})$.

9. Was versteht man unter einem Kreisteilungspolynom? Welche Eigenschaften besitzen diese Polynome über $\mathbb{Q}$ sowie über einem beliebigen Körper K?

⁺10. Betrachte einen endlichen Körper $\mathbb{F}_q$ mit q Elementen, eine primitive n-te Einheitswurzel $\zeta_n \in \overline{\mathbb{F}}_q$ sowie die Gruppe $U_n \subset \overline{\mathbb{F}}_q$ aller n-ten Einheitswurzeln, wobei $\mathrm{ggT}(n, q) = 1$. Identifiziere die Automorphismengruppe $\mathrm{Aut}(U_n)$ mit $(\mathbb{Z}/n\mathbb{Z})^*$ und charakterisiere die Galois-Gruppe $\mathrm{Gal}(\mathbb{F}_q(\zeta_n)/\mathbb{F}_q)$ als Untergruppe von $(\mathbb{Z}/n\mathbb{Z})^*$.

Übungsaufgaben

1. *Betrachte eine primitive n-te Einheitswurzel ζ über einem Körper K sowie das n-te Kreisteilungspolynom $\Phi_n \in K[X]$, wobei* $\mathrm{char}\, K \nmid n$. *Zeige, dass Φ_n über K in $\varphi(n)/s$ verschiedene irreduzible Faktoren vom* $\mathrm{Grad}\ s = [K(\zeta) : K]$ *zerfällt.*

2. *Es sei $\zeta_m \in \overline{\mathbb{Q}}$ eine primitive m-te Einheitswurzel. Überlege, für welche n das n-te Kreisteilungspolynom Φ_n irreduzibel über $\mathbb{Q}(\zeta_m)$ ist.*

3. Zeige für $n \in \mathbb{N}$, $n > 0$, dass $\varphi(n) = n \cdot \prod_{p \mid n,\ p \text{ prim}} (1 - p^{-1})$ gilt.

4. Bestimme die Galois-Gruppe des Polynoms $X^5 - 1 \in \mathbb{F}_7[X]$.

5. Es sei ζ eine primitive 12-te Einheitswurzel über $\mathbb{Q}$. Bestimme alle Zwischenkörper von $\mathbb{Q}(\zeta)/\mathbb{Q}$.

6. Es sei p eine Primzahl, so dass $p - 1 = \prod_{\nu=1}^{n} p_\nu$ ein Produkt von paarweise verschiedenen Primfaktoren p_ν ist. Sei $\zeta_p \in \overline{\mathbb{Q}}$ eine primitive p-te Einheitswurzel. Zeige, dass $\mathbb{Q}(\zeta_p)/\mathbb{Q}$ eine zyklische Galois-Erweiterung ist und dass es genau 2^n verschiedene Zwischenkörper zu $\mathbb{Q}(\zeta_p)/\mathbb{Q}$ gibt.

7. Es sei p eine ungerade Primzahl. Zeige, dass die Gruppe $(\mathbb{Z}/p^r\mathbb{Z})^*$ für $r > 0$ zyklisch ist und schließe hieraus, dass der p^r-te Kreisteilungskörper $\mathbb{Q}(\zeta_{p^r})$ eine zyklische Galois-Erweiterung von $\mathbb{Q}$ darstellt. (*Hinweis*: Betrachte den kanonischen Homomorphismus $(\mathbb{Z}/p^r\mathbb{Z})^* \longrightarrow (\mathbb{Z}/p\mathbb{Z})^*$ sowie dessen Kern W und zeige induktiv, dass die Restklasse zu $1 + p$ ein Element der Ordnung p^{r-1} in W ist, W also insbesondere zyklisch ist.)

8. Verifiziere, dass die Kreisteilungspolynome Φ_n folgenden Formeln genügen:
   (i) $\Phi_{p^r}(X) = \Phi_p(X^{p^{r-1}})$, für p prim, $r > 0$.
   (ii) $\Phi_n(X) = \Phi_{p_1 \dots p_s}(X^{p_1^{r_1-1} \cdots p_s^{r_s-1}})$, wobei $n = p_1^{r_1} \dots p_s^{r_s}$ eine Primfaktorzerlegung mit paarweise verschiedenen Primzahlen p_ν und mit Exponenten $r_\nu > 0$ sei.
   (iii) $\Phi_{2n}(X) = \Phi_n(-X)$, für $n \geq 3$ ungerade.
   (iv) $\Phi_{pn}(X) = \dfrac{\Phi_n(X^p)}{\Phi_n(X)}$, für p prim mit $p \nmid n$.
9. Bestimme sämtliche Einheitswurzeln, die in den Körpern $\mathbb{Q}(\sqrt{2})$, $\mathbb{Q}(i)$, $\mathbb{Q}(i\sqrt{2})$ bzw. $\mathbb{Q}(i\sqrt{3})$ enthalten sind.

4.6 Lineare Unabhängigkeit von Charakteren

In diesem und dem nächsten Abschnitt besprechen wir einige Methoden der Linearen Algebra, die für die Galois-Theorie wichtig sind und die wir zur Untersuchung zyklischer Erweiterungen in 4.8 verwenden werden. In besonderem Maße hat E. Artin diesen "linearen" Standpunkt in der Galois-Theorie vertreten. Beispielsweise hat er in [1], [2] "lineare" Methoden benutzt, um einen alternativen Aufbau der Galois-Theorie zu geben. Für uns geht es zunächst um die Untersuchung von Charakteren; diese werden im Weiteren in der Form von Homomorphismen $K^* \longrightarrow L^*$ zwischen den multiplikativen Gruppen zweier Körper K und L vorkommen. Ziel des Abschnitts ist es, zu zeigen, dass verschiedene Charaktere linear unabhängig sind.

Definition 1. *Ist G eine Gruppe und K ein Körper, so heißt ein Homomorphismus $\chi\colon G \longrightarrow K^*$ ein K-wertiger* Charakter *von G.*

Zu einer Gruppe G und einem Körper K existiert stets der *triviale* Charakter $G \longrightarrow K^*$, der jedes $g \in G$ auf das Einselement $1 \in K^*$ abbildet. Im Übrigen bilden die K-wertigen Charaktere von G eine Gruppe, wenn man zur Verknüpfung von Charakteren die Gruppenstruktur von K^* verwendet. So ist das Produkt zweier Charaktere $\chi_1, \chi_2\colon G \longrightarrow K^*$ erklärt durch

$$\chi_1 \cdot \chi_2\colon G \longrightarrow K^*, \qquad g \longmapsto \chi_1(g) \cdot \chi_2(g).$$

Die K-wertigen Charaktere von G kann man insbesondere als Elemente des K-Vektorraums $\mathrm{Abb}(G,K)$ aller Abbildungen von G nach K auffassen, so dass man von der linearen Unabhängigkeit von Charakteren sprechen kann.

Satz 2 (E. Artin). *Verschiedene Charaktere $\chi_1,\ldots,\chi_n$ einer Gruppe G mit Werten in einem Körper K sind linear unabhängig in* $\mathrm{Abb}(G,K)$.

Beweis. Wir schließen indirekt und nehmen an, dass die Aussage des Satzes falsch ist. Dann gibt es ein minimales $n\in\mathbb{N}$, so dass ein linear abhängiges System von Charakteren $\chi_1,\ldots,\chi_n$ existiert. Dabei gilt $n\geq 2$, da jeder Charakter Werte in K^* annimmt, also von der Nullabbildung verschieden ist. Sei nun

$$a_1\chi_1+\ldots+a_n\chi_n=0$$

eine nicht-triviale Relation in $\mathrm{Abb}(G,K)$ mit Koeffizienten $a_i\in K$. Aufgrund der Minimalität von n gilt dann $a_i\neq 0$ für alle i, und man hat

$$a_1\chi_1(gh)+\ldots+a_n\chi_n(gh)=0$$

für $g,h\in G$. Man wähle speziell g mit $\chi_1(g)\neq\chi_2(g)$; dies ist möglich wegen $\chi_1\neq\chi_2$. Variiert nun h in G, so sieht man, dass

$$a_1\chi_1(g)\cdot\chi_1+\ldots+a_n\chi_n(g)\cdot\chi_n=0$$

eine neue nicht-triviale Relation in $\mathrm{Abb}(G,K)$ ist. Durch Kombination mit der ursprünglichen Relation, die man mit $\chi_1(g)$ multipliziere, ergibt sich

$$a_2\big(\chi_1(g)-\chi_2(g)\big)\chi_2+\ldots+a_n\big(\chi_1(g)-\chi_n(g)\big)\chi_n=0.$$

Dies ist eine Relation der Länge $n-1$, die wegen $a_2(\chi_1(g)-\chi_2(g))\neq 0$ nicht-trivial ist. Somit erhält man einen Widerspruch zur Minimalität von n, und der Satz ist bewiesen. □

Man kann den vorstehenden Satz in vielfältigen Situationen anwenden. Ist etwa L/K eine algebraische Körpererweiterung, so ergibt sich, dass $\mathrm{Aut}_K(L)$ ein linear unabhängiges System im L-Vektorraum der Abbildungen $L\longrightarrow L$ darstellt; man schränke hierzu K-Homomorphismen $L\longrightarrow L$ zu Gruppenhomomorphismen $L^*\longrightarrow L^*$ ein.

Korollar 3. *Es sei L/K eine endliche separable Körpererweiterung mit K-Basis $x_1, \ldots, x_n$ von L. Sind dann $\sigma_1, \ldots, \sigma_n$ die K-Homomorphismen von L in einen algebraischen Abschluss $\overline{K}$ von K, so sind die Vektoren*

$$\begin{aligned} \xi_1 &= \big(\sigma_1(x_1), \ldots, \sigma_1(x_n)\big), \\ &\cdots \\ &\cdots \\ &\cdots \\ \xi_n &= \big(\sigma_n(x_1), \ldots, \sigma_n(x_n)\big), \end{aligned}$$

linear unabhängig über $\overline{K}$.

Beweis. Aus der linearen Abhängigkeit der ξ_i würde die lineare Abhängigkeit der σ_i folgen. Es sind die σ_i jedoch wegen Satz 2 linear unabhängig. □

Als weiteres Beispiel kann man Charaktere der Form

$$\mathbb{Z} \longrightarrow K^*, \qquad \nu \longmapsto a^\nu,$$

betrachten, wobei $a \in K^*$ fest gewählt ist. Hat man etwa paarweise verschiedene Elemente $a_1, \ldots, a_n \in K^*$ sowie weitere Elemente $c_1, \ldots, c_n \in K$ mit

$$c_1 a_1^\nu + \ldots + c_n a_n^\nu = 0$$

für alle $\nu \in \mathbb{Z}$, so folgt $c_1 = \ldots = c_n = 0$ mit Satz 2.

Lernkontrolle und Prüfungsvorbereitung

1. Es sei G eine Gruppe und K ein Körper. Was versteht man unter einem K-wertigen Charakter von G? Gib einige Beispiele für solche Charaktere.
2. Zeige, dass verschiedene Charaktere einer Gruppe G mit Werten in einem Körper K linear unabhängig sind. In welchem Vektorraum ist diese lineare Unabhängigkeit zu verstehen?
3. Sei L/K eine endliche separable Körpererweiterung vom Grad n. Sei $x_1, \ldots, x_n$ eine K-Basis von L und seien $\sigma_1, \ldots, \sigma_n$ die K-Homomorphismen von L in einen algebraischen Abschluss $\overline{K}$ von K. Zeige $\det(\sigma_i(x_j))_{\substack{i=1,\ldots,n \\ j=1,\ldots,n}} \neq 0$.
4. Sei K ein Körper. Für fest gewählte Elemente $a_1, \ldots, a_n \in K^*$ und Koeffizienten $c_1, \ldots, c_n \in K$ gelte $\sum_{i=1}^n c_i a_i^\nu = 0$ für alle Exponenten $\nu \in \mathbb{Z}$, wobei die a_i paarweise verschieden seien. Zeige $c_1 = \ldots = c_n = 0$.

Übungsaufgaben

1. *Es sei G eine zyklische Gruppe und $\mathbb{F}$ ein endlicher Körper. Beschreibe alle $\mathbb{F}$-wertigen Charaktere von G und bestimme insbesondere deren Anzahl.*

2. Es seien L/K und M/K Körpererweiterungen sowie $\sigma_1, \ldots, \sigma_r$ verschiedene K-Homomorphismen von L nach M. Zeige, dass es Elemente $x_1, \ldots, x_r \in L$ gibt, so dass die Vektoren $\xi_i = (\sigma_i(x_1), \ldots, \sigma_i(x_r)) \in M^r$, $i = 1, \ldots, r$, linear unabhängig über M sind, ähnlich wie in Korollar 3. (*Hinweis*: Betrachte die Abbildung $L \longrightarrow M^r$, $x \longmapsto (\sigma_1(x), \ldots, \sigma_r(x))$, und zeige, dass M^r als M-Vektorraum vom Bild dieser Abbildung erzeugt wird.)

3. Es seien L/K und M/K Körpererweiterungen sowie $\sigma_1, \ldots, \sigma_r$ verschiedene K-Homomorphismen von L nach M. Betrachte ein Polynom f in $M[X_1, \ldots, X_r]$ mit $f(\sigma_1(x), \ldots, \sigma_r(x)) = 0$ für alle $x \in L$ und zeige unter Verwendung von Aufgabe 2: Besitzt K unendlich viele Elemente, so gilt $f = 0$. (*Hinweis*: Wähle $x_1, \ldots, x_r \in L$ wie in Aufgabe 2 und zeige, dass $g(Y_1, \ldots, Y_r) = f(\sum_{i=1}^r \sigma_1(x_i)Y_i, \ldots, \sum_{i=1}^r \sigma_r(x_i)Y_i)$ das Nullpolynom ist.)

4.7 Norm und Spur

In der Linearen Algebra definiert man Determinante und Spur von Endomorphismen endlich-dimensionaler Vektorräume. Wir wollen diese Begriffe im Folgenden verwenden und erinnern deshalb zunächst noch einmal daran. Es sei K ein Körper, V ein n-dimensionaler K-Vektorraum und $\varphi\colon V \longrightarrow V$ ein Endomorphismus. Dann definiert man zu φ das *charakteristische Polynom*

$$\chi_\varphi(X) = \det(X \cdot \mathrm{id} - \varphi) = \sum_{i=0}^{n} c_i X^{n-i},$$

wobei $(-1)^n c_n = \det\varphi$ die *Determinante* und $-c_1 = \mathrm{Spur}\,\varphi$ die *Spur* von φ ist. Stellt man φ bezüglich einer Basis von V durch eine Matrix dar, etwa durch $A = (a_{ij}) \in K^{n\times n}$, so gilt

$$\det\varphi = \det A = \sum_{\pi\in\mathfrak{S}_n} \mathrm{sgn}(\pi) a_{1,\pi(1)} \ldots a_{n,\pi(n)},$$

$$\mathrm{Spur}\,\varphi = \mathrm{Spur}\,A = \sum_{i=1}^{n} a_{ii}.$$

Für zwei Endomorphismen $\varphi, \psi : V \longrightarrow V$ sowie Konstanten $a, b \in K$ gelten die Regeln

$$\begin{aligned} \operatorname{Spur}(a\varphi + b\psi) &= a \operatorname{Spur}\varphi + b \operatorname{Spur}\psi, \\ \det(\varphi \circ \psi) &= \det\varphi \cdot \det\psi. \end{aligned}$$

Definition 1. *Es sei L/K eine endliche Körpererweiterung. Für $a \in L$ betrachte man*

$$\varphi_a : L \longrightarrow L, \qquad x \longmapsto ax,$$

als K-Vektorraumendomorphismus von L. Dann heißen

$$\operatorname{Sp}_{L/K}(a) := \operatorname{Spur}\varphi_a, \qquad \operatorname{N}_{L/K}(a) := \det\varphi_a$$

Spur *bzw.* Norm *von a bezüglich der Körpererweiterung L/K.*

Es ist also $\operatorname{Sp}_{L/K} : L \longrightarrow K$ ein K-Vektorraumhomomorphismus oder, genauer, eine Linearform auf L, wobei L als K-Vektorraum aufgefasst werde. Entsprechend ist $\operatorname{N}_{L/K} : L^* \longrightarrow K^*$ ein Gruppenhomomorphismus, also ein Charakter auf L^* mit Werten in K. Beispielsweise gilt

$$\operatorname{N}_{\mathbb{C}/\mathbb{R}}(z) = |z|^2.$$

Ist nämlich $z = x + iy$ die Zerlegung von z in Real- und Imaginärteil, so wird die Multiplikation mit z auf $\mathbb{C}$ bezüglich der $\mathbb{R}$-Basis $1, i$ durch die Matrix

$$\begin{pmatrix} x & -y \\ y & x \end{pmatrix}$$

dargestellt. Wir wollen im Folgenden einige allgemeine Methoden zur Berechnung von Spur und Norm beschreiben.

Lemma 2. *Es sei L/K eine endliche Körpererweiterung vom Grad n.*

(i) *Für $a \in K$ gilt*

$$\operatorname{Sp}_{L/K}(a) = na, \qquad \operatorname{N}_{L/K}(a) = a^n.$$

(ii) *Für $a \in L$ und $L = K(a)$ mit $X^n + c_1 X^{n-1} + \ldots + c_n$ als Minimalpolynom von a über K gilt*

$$\operatorname{Sp}_{L/K}(a) = -c_1, \qquad \operatorname{N}_{L/K}(a) = (-1)^n c_n.$$

Beweis. Für $a \in K$ wird die Abbildung $\varphi_a \colon L \longrightarrow L$ durch das a-fache der Einheitsmatrix in $K^{n\times n}$ beschrieben. Als Konsequenz ergeben sich die beiden Formeln in (i). Im Falle $a \in L$ und $L = K(a)$ ist das Minimalpolynom von a zugleich auch das Minimalpolynom von φ_a und damit aus Gradgründen schon das charakteristische Polynom von φ_a. Die Formeln in (ii) ergeben sich deshalb aus der Beschreibung von $\operatorname{Spur}\varphi_a$ und $\det\varphi_a$ durch die Koeffizienten des charakteristischen Polynoms von φ_a. □

Die beiden Spezialfälle von Lemma 2 lassen sich kombinieren und ermöglichen dann eine allgemeine Berechnung von Norm und Spur.

Lemma 3. *Sei L/K eine endliche Körpererweiterung. Für $a \in L$ und $s = [L : K(a)]$ gilt*

$$\mathrm{Sp}_{L/K}(a) = s \cdot \mathrm{Sp}_{K(a)/K}(a), \qquad \mathrm{N}_{L/K}(a) = \big(\mathrm{N}_{K(a)/K}(a)\big)^s.$$

Beweis. Man wähle eine K-Basis $x_1, \ldots, x_r$ von $K(a)$ sowie eine $K(a)$-Basis $y_1, \ldots, y_s$ von L. Dann bilden die Produkte $x_i y_j$ eine K-Basis von L. Es sei nun $A \in K^{r\times r}$ diejenige Matrix, welche bezüglich der Basis $x_1, \ldots, x_r$ die Multiplikation mit a auf $K(a)$ beschreibt. Dann wird bezüglich der $x_i y_j$ die Multiplikation mit a auf L durch die Matrix

$$C = \begin{pmatrix} A & & 0 \\ & \ddots & \\ 0 & & A \end{pmatrix}$$

beschrieben, welche aus s Kästchen A und Nullen sonst besteht. Somit folgt

$$\begin{aligned} \mathrm{Sp}_{L/K}(a) = \operatorname{Spur} C = s \cdot \operatorname{Spur} A = s \cdot \mathrm{Sp}_{K(a)/K}(a), \\ \mathrm{N}_{L/K}(a) = \det C = (\det A)^s = \big(\mathrm{N}_{K(a)/K}(a)\big)^s. \end{aligned}$$

□

Satz 4. *Sei L/K eine endliche Körpererweiterung mit $[L : K] = qr$, wobei $r = [L : K]_s$ der Separabilitätsgrad von L/K ist.* (*Man nennt q auch den* Inseparabilitätsgrad *von L/K.*) *Sind dann $\sigma_1, \ldots, \sigma_r$ sämtliche K-Homomorphismen von L in einen algebraischen Abschluss $\overline{K}$ von K, so gilt für $a \in L$*

$$\mathrm{Sp}_{L/K}(a) = q \sum_{i=1}^{r} \sigma_i(a),$$
$$\mathrm{N}_{L/K}(a) = \Big(\prod_{i=1}^{r} \sigma_i(a)\Big)^q.$$

Ist L/K im Falle $p = \mathrm{char}\, K > 0$ nicht separabel, so ist q eine nicht-triviale Potenz von p, und es folgt $\mathrm{Sp}_{L/K}(a) = 0$ für alle $a \in L$.

Bevor wir den Beweis führen, seien noch die Transitivitätsformeln für Spur und Norm angeführt, welche wir gemeinsam mit Satz 4 beweisen werden.

Satz 5. *Es sei $K \subset L \subset M$ eine Kette endlicher Körpererweiterungen. Dann gilt*

$$\mathrm{Sp}_{M/K} = \mathrm{Sp}_{L/K} \circ \mathrm{Sp}_{M/L}, \qquad \mathrm{N}_{M/K} = \mathrm{N}_{L/K} \circ \mathrm{N}_{M/L}.$$

Beweis der Sätze 4 *und* 5. In der Situation von Satz 4 setzen wir für Elemente $a \in L$

$$\mathrm{Sp}'_{L/K}(a) = q \sum_{i=1}^{r} \sigma_i(a),$$
$$\mathrm{N}'_{L/K}(a) = \Big(\prod_{i=1}^{r} \sigma_i(a)\Big)^q.$$

Zu zeigen ist dann $\mathrm{Sp}_{L/K} = \mathrm{Sp}'_{L/K}$ und $\mathrm{N}_{L/K} = \mathrm{N}'_{L/K}$. Wir betrachten hierzu die Spezialfälle aus Lemma 2 und schließen mit den Transitivitätsformeln auf den Allgemeinfall.

Sei zunächst $a \in K$. Wegen $[L : K] = qr$ und $\sigma_i(a) = a$ für alle i gilt nach Lemma 2

$$\mathrm{Sp}_{L/K}(a) = [L : K] \cdot a = q(ra) = \mathrm{Sp}'_{L/K}(a),$$
$$\mathrm{N}_{L/K}(a) = a^{[L:K]} = (a^r)^q = \mathrm{N}'_{L/K}(a).$$

Wir betrachten nun den zweiten Spezialfall aus Lemma 2 und nehmen $L = K(a)$ an. Sei

$$X^n + c_1 X^{n-1} + \ldots + c_n \in K[X]$$

das Minimalpolynom von a über K mit $n = qr$. Dieses Polynom hat über $\overline{K}$ gemäß 3.4/8 und 3.6/2 die Faktorisierung

$$\prod_{i=1}^{r} \big(X - \sigma_i(a)\big)^q.$$

Folglich gilt nach Lemma 2

$$\mathrm{Sp}_{L/K}(a) = -c_1 = q \sum_{i=1}^{r} \sigma_i(a) = \mathrm{Sp}'_{L/K}(a),$$
$$\mathrm{N}_{L/K}(a) = (-1)^n c_n = \Big(\prod_{i=1}^{r} \sigma_i(a)\Big)^q = \mathrm{N}'_{L/K}(a).$$

Wir sehen also, dass Sp und Sp′ sowie N und N′ in den Spezialfällen von Lemma 2 übereinstimmen.

Ist nun $a \in L$ beliebig, so betrachte man die Kette $K \subset K(a) \subset L$. Dann gilt aufgrund der Lemmata 2 und 3 sowie aufgrund der bereits behandelten Spezialfälle:

$$\begin{aligned}
\mathrm{Sp}_{L/K}(a) &= [L : K(a)] \cdot \mathrm{Sp}_{K(a)/K}(a) = \mathrm{Sp}_{K(a)/K}\big([L : K(a)] \cdot a\big) \\
&= \mathrm{Sp}_{K(a)/K}\big(\mathrm{Sp}_{L/K(a)}(a)\big) \\
&= \mathrm{Sp}'_{K(a)/K}\big(\mathrm{Sp}'_{L/K(a)}(a)\big), \\
\mathrm{N}_{L/K}(a) &= \big(\mathrm{N}_{K(a)/K}(a)\big)^{[L:K(a)]} = \mathrm{N}_{K(a)/K}\big(a^{[L:K(a)]}\big) \\
&= \mathrm{N}_{K(a)/K}\big(\mathrm{N}_{L/K(a)}(a)\big) \\
&= \mathrm{N}'_{K(a)/K}\big(\mathrm{N}'_{L/K(a)}(a)\big).
\end{aligned}$$

Es genügt daher zum Nachweis von Satz 4, die Transitivitätsformeln aus Satz 5 für Sp′ und N′ zu beweisen. Dieselben Formeln gelten dann aufgrund von Satz 4 auch für Sp und N.

Es sei also $K \subset L \subset M$ eine Kette endlicher Körpererweiterungen wie in Satz 5. Indem wir M in den algebraischen Abschluss $\overline{K}$ von K einbetten, können wir annehmen, dass die Kette in $\overline{K}$ liegt. Gilt nun

$$[L : K] = q_1 [L : K]_s, \qquad [M : L] = q_2 [M : L]_s,$$

so folgt aufgrund der Gradsätze 3.2/2 und 3.6/7

$$[M : K] = q_1 q_2 [M : K]_s.$$

Es gelte weiter

$$\mathrm{Hom}_K(L, \overline{K}) = \{\sigma_1, \ldots, \sigma_r\}, \qquad \mathrm{Hom}_L(M, \overline{K}) = \{\tau_1, \ldots, \tau_s\},$$

wobei die σ_i bzw. τ_j jeweils paarweise verschieden seien. Wählen wir dann Fortsetzungen $\sigma_i' \colon \overline{K} \longrightarrow \overline{K}$ der σ_i, so ergibt sich wie im Beweis zu 3.6/7

$$\mathrm{Hom}_K(M, \overline{K}) = \{\sigma_i' \circ \tau_j \,;\, i = 1, \ldots, r,\ j = 1, \ldots, s\}$$

mit paarweise verschiedenen Elementen $\sigma_i' \circ \tau_j$, und wir können für $a \in M$ die gewünschten Transitivitätsformeln ausrechnen:

$$\begin{aligned} \mathrm{Sp}'_{M/K}(a) &= q_1 q_2 \sum_{i,j} \sigma_i' \circ \tau_j(a) \\ &= q_1 \sum_i \sigma_i' \Big(q_2 \sum_j \tau_j(a) \Big) \\ &= \mathrm{Sp}'_{L/K}\big(\mathrm{Sp}'_{M/L}(a)\big), \end{aligned}$$

entsprechend für $\mathrm{N}'_{M/K}(a)$. Dabei dürfen wir streng genommen die letzte Zeile allerdings nur dann schreiben, wenn wir wissen, dass $\mathrm{Sp}'_{M/L}(a)$ ein Element von L ist oder, was ausreicht, wenn $\mathrm{Sp}'_{M/L}(a) = \mathrm{Sp}_{M/L}(a)$ gilt. In der beim Beweis von Satz 4 benötigten Situation ist diese Gleichung aber gegeben, so dass wir den Beweis von Satz 4 beenden können. Anschließend folgen die allgemeinen Transitivitätsformeln in Satz 5 unter Benutzung von Satz 4. □

Als unmittelbare Folgerung erhält man aus Satz 4:

Korollar 6. *Es sei L/K eine endliche Galois-Erweiterung. Dann sind $\mathrm{Sp}_{L/K}$ und $\mathrm{N}_{L/K}$ mit den Galois-Automorphismen von L/K verträglich, d. h. es gilt*

$$\mathrm{Sp}_{L/K}(a) = \mathrm{Sp}_{L/K}\big(\sigma(a)\big), \qquad \mathrm{N}_{L/K}(a) = \mathrm{N}_{L/K}\big(\sigma(a)\big)$$

für alle $a \in L$, $\sigma \in \mathrm{Gal}(L/K)$.

Wir wollen noch einige weitere Folgerungen aus Satz 4 ziehen. Ist L/K eine endliche Körpererweiterung, so können wir L als K-Vektorraum auffassen und die symmetrische Bilinearform

$$\mathrm{Sp}\colon L \times L \longrightarrow K, \qquad (x, y) \longmapsto \mathrm{Sp}_{L/K}(xy),$$

betrachten. Diese verschwindet nach Satz 4 identisch, wenn L/K nicht separabel ist.

Satz 7. *Eine endliche Körpererweiterung L/K ist genau dann separabel, wenn die K-lineare Abbildung $\mathrm{Sp}_{L/K}\colon L \longrightarrow K$ nicht-trivial und damit surjektiv ist. Ist L/K separabel, so ist die symmetrische Bilinearform*

$$\mathrm{Sp}\colon L \times L \longrightarrow K, \qquad (x, y) \longmapsto \mathrm{Sp}_{L/K}(xy),$$

nicht ausgeartet. Mit anderen Worten, Sp *induziert dann einen Isomorphismus*

$$L \longrightarrow \hat{L}, \qquad x \longmapsto \mathrm{Sp}(x, \cdot),$$

von L auf seinen Dualraum $\hat{L}$.

Beweis. Wir nehmen an, dass L/K separabel ist. Sind dann $\sigma_1, \ldots, \sigma_r$ die K-Homomorphismen von L in einen algebraischen Abschluss von K, so gilt

$$\mathrm{Sp}_{L/K} = \sigma_1 + \ldots + \sigma_r$$

nach Satz 4, und der Satz 4.6/2 über die lineare Unabhängigkeit von Charakteren impliziert, dass $\mathrm{Sp}_{L/K}$ nicht identisch verschwindet. Sei nun x ein Element des Kerns von $L \longrightarrow \hat{L}$, so dass also $\mathrm{Sp}(x, \cdot) = 0$ gilt. Es folgt dann $\mathrm{Sp}_{L/K}(xL) = 0$ und damit notwendig $x = 0$, da ansonsten $\mathrm{Sp}_{L/K}$ wegen $xL = L$ identisch verschwinden würde. Somit ist die Abbildung $L \longrightarrow \hat{L}$ injektiv und wegen $\dim L = \dim \hat{L} < \infty$ auch surjektiv. □

Korollar 8. *Es sei L/K eine endliche separable Körpererweiterung mit K-Basis $x_1, \ldots, x_n$ von L. Dann existiert eine eindeutig bestimmte K-Basis $y_1, \ldots, y_n$ von L mit $\mathrm{Sp}_{L/K}(x_i y_j) = \delta_{ij}$ für $i, j = 1, \ldots, n$.*

Beweis. Man benutze Existenz und Eindeutigkeit der dualen Basis zu $x_1, \ldots, x_n$. □

Lernkontrolle und Prüfungsvorbereitung

1. Sei L/K eine endliche Körpererweiterung. Definiere die Spur und Norm bezüglich dieser Erweiterung, also $\mathrm{Sp}_{L/K}(a)$ und $\mathrm{N}_{L/K}(a)$ für Elemente $a \in L$.
2. Bestimme $\mathrm{Sp}_{\mathbb{C}/\mathbb{R}}(z)$ und $\mathrm{N}_{\mathbb{C}/\mathbb{R}}(z)$ für Elemente $z \in \mathbb{C}$.

3. Sei L/K eine endliche Körpererweiterung und $a \in L$. Berechne $\mathrm{Sp}_{L/K}(a)$ und $N_{L/K}(a)$ für den Spezialfall $a \in K$. Beschreibe weiter $\mathrm{Sp}_{L/K}(a)$ und $\mathrm{N}_{L/K}(a)$ unter Zuhilfenahme des Minimalpolynoms von a über K, falls $L = K(a)$ gilt. Welche Charakterisierung von Spur und Norm ergibt sich daraus im Allgemeinfall?

4. Es sei L/K eine endliche Körpererweiterung und $\overline{K}$ ein algebraischer Abschluss von K. Beschreibe $\mathrm{Sp}_{L/K}(a)$ und $\mathrm{N}_{L/K}(a)$ für Elemente $a \in L$ unter Verwendung der K-Homomorphismen $L \longrightarrow \overline{K}$.

5. Wie lauten die sogenannten Transitivitätsformeln für die Spur und die Norm?

+6. Gib die Beweise zu den Punkten 4 und 5.

7. Zeige für eine endliche Galois-Erweiterung L/K, dass $\mathrm{Sp}_{L/K}(a)$ und $N_{L/K}(a)$ verträglich sind mit der Anwendung von Automorphismen aus $\mathrm{Gal}(L/K)$ auf Elemente $a \in L$.

8. Zeige, dass eine endliche Körpererweiterung L/K genau dann separabel ist, wenn die Linearform $\mathrm{Sp}_{L/K} \colon L \longrightarrow K$ nicht trivial ist. Im letzteren Falle ist $\mathrm{Sp} \colon L \times L \longrightarrow K$ eine nicht ausgeartete Bilinearform.

Übungsaufgaben

1. *Es sei L/K eine Körpererweiterung vom Grad $n < \infty$. Beschreibe die Eigenschaften der Menge* $\{a \in L\,;\ \mathrm{Sp}_{L/K}(a) = 0\}$.

2. *Es sei $\mathbb{F}'/\mathbb{F}$ eine Erweiterung endlicher Körper. Beschreibe Kern und Bild der zugehörigen Normabbildung* $\mathrm{N} \colon \mathbb{F}'^{*} \longrightarrow \mathbb{F}^{*}$.

3. Es sei K ein Körper und $L = K(a)$ eine einfache algebraische Körpererweiterung mit Minimalpolynom $f \in K[X]$ zu a. Zeige, dass $f(x) = \mathrm{N}_{L/K}(x - a)$ für $x \in K$ gilt.

4. Es seien m, n teilerfremde positive ganze Zahlen. Ist dann L/K eine Körpererweiterung vom Grad m, so hat jedes Element $a \in K$, welches eine n-te Wurzel in L besitzt, bereits eine n-te Wurzel in K.

5. Sei L/K eine endliche Galois-Erweiterung mit K-Basis $x_1, \ldots, x_n$. Zeige für eine Untergruppe $H \subset \mathrm{Gal}(L/K)$, dass der zugehörige Fixkörper L^H durch $L^H = K(\mathrm{Sp}_{L/L^H}(x_1), \ldots, \mathrm{Sp}_{L/L^H}(x_n))$ gegeben ist.

6. Es sei L/K eine endliche Körpererweiterung der Charakteristik $p > 0$. Zeige $\mathrm{Sp}_{L/K}(a^p) = (\mathrm{Sp}_{L/K}(a))^p$ für Elemente $a \in L$.

4.8 Zyklische Erweiterungen

Für die Auflösung algebraischer Gleichungen durch Radikale muss man zu einem gegebenen Körper K Erweiterungen studieren, die durch Adjunktion einer n-ten Wurzel eines Elementes $c \in K$ entstehen. Ziel dieses Abschnittes ist es, solche Erweiterungen Galois-theoretisch zu charakterisieren. Dabei wählen wir als Grundlage den berühmten Satz 90 von D. Hilbert [9], welchen wir zunächst behandeln wollen. Es sei daran erinnert, dass eine Galois-Erweiterung L/K *zyklisch* genannt wird, wenn die Galois-Gruppe $\mathrm{Gal}(L/K)$ zyklisch ist.

Theorem 1 (Hilbert 90). *Es sei L/K eine endliche zyklische Galois-Erweiterung, $\sigma \in \mathrm{Gal}(L/K)$ sei ein erzeugendes Element. Für $b \in L$ ist dann äquivalent*:

(i) $\mathrm{N}_{L/K}(b) = 1$.

(ii) *Es existiert ein $a \in L^*$ mit $b = a \cdot \sigma(a)^{-1}$.*

Beweis. Gilt $b = a \cdot \sigma(a)^{-1}$ mit $a \in L^*$, so folgt unter Benutzung von 4.7/6

$$\mathrm{N}_{L/K}(b) = \frac{\mathrm{N}_{L/K}(a)}{\mathrm{N}_{L/K}\big(\sigma(a)\big)} = 1.$$

Sei umgekehrt $b \in L$ gegeben mit $\mathrm{N}_{L/K}(b) = 1$, und sei $n = [L : K]$. Aufgrund der linearen Unabhängigkeit von Charakteren 4.6/2 sieht man dann, dass

$$\sigma^0 + b\sigma^1 + b \cdot \sigma(b) \cdot \sigma^2 + \ldots + b \cdot \sigma(b) \cdot \ldots \cdot \sigma^{n-2}(b) \cdot \sigma^{n-1}$$

als Abbildung $L^* \longrightarrow L$ nicht die Nullabbildung ist. Somit existiert ein $c \in L^*$ mit

$$a := c + b\sigma(c) + b \cdot \sigma(b) \cdot \sigma^2(c) + \ldots + b \cdot \sigma(b) \cdot \ldots \cdot \sigma^{n-2}(b) \cdot \sigma^{n-1}(c) \neq 0.$$

Anwenden von σ und anschließende Multiplikation mit b ergibt

$$b \cdot \sigma(a) = b\sigma(c) + b \cdot \sigma(b) \cdot \sigma^2(c) + \ldots + b \cdot \sigma(b) \cdot \ldots \cdot \sigma^{n-1}(b) \cdot \sigma^n(c) = a,$$

da man $\sigma^n = \mathrm{id}$ und $b \cdot \sigma(b) \cdot \ldots \cdot \sigma^{n-1}(b) = \mathrm{N}_{L/K}(b) = 1$ wegen 4.7/4 hat. □

Man kann das vorstehende Theorem auch in den allgemeineren Rahmen der Galois-Kohomologie einordnen. Dies wollen wir im Folgenden andeuten; bezüglich weiterer Details konsultiere man etwa Serre [14], Chap. VII, X. Wir betrachten im Folgenden eine Gruppe G, eine abelsche Gruppe A sowie eine Aktion von G auf A, worunter wir hier einen Gruppenhomomorphismus $G \longrightarrow \mathrm{Aut}(A)$ verstehen wollen. Ausgehend von einer endlichen (nicht notwendig zyklischen) Galois-Erweiterung L/K ist für uns der Fall $G = \mathrm{Gal}(L/K)$ sowie etwa $A = L^*$ von Interesse, wobei $G \longrightarrow \mathrm{Aut}(L^*)$ der kanonische Homomorphismus sei. Bezeichnen wir für $\sigma \in G$ und $a \in A$ mit $\sigma(a)$ jeweils das Bild von a unter dem zu σ gehörigen Automorphismus von A, so können wir die folgenden Untergruppen der abelschen Gruppe $\mathrm{Abb}(G, A)$ aller Abbildungen $f\colon G \longrightarrow A$ definieren:

$$Z^1(G,A) = \Big\{ f\ ;\ f(\sigma\circ\sigma') = \sigma\big(f(\sigma')\big)\cdot f(\sigma) \text{ für alle } \sigma,\sigma' \in G \Big\},$$

$$B^1(G,A) = \Big\{ f\ ;\ \text{es gibt } a \in A \text{ mit } f(\sigma) = a\cdot\sigma(a)^{-1} \text{ für alle } \sigma \in G \Big\}.$$

Die Gruppe $B^1(G,A)$ der sogenannten 1-*Koränder* ist eine Untergruppe von $Z^1(G,A)$, der Gruppe der 1-*Kozyklen*, und man nennt die Restklassengruppe

$$H^1(G,A) := Z^1(G,A)\,\big/\,B^1(G,A)$$

die *erste Kohomologiegruppe* von G mit Werten in A. Die kohomologische Version von Hilberts Satz 90 lautet dann:

Theorem 2. *Ist L/K eine endliche Galois-Erweiterung mit Galois-Gruppe G, so gilt $H^1(G, L^*) = \{1\}$, d. h. jeder 1-Kozyklus ist bereits ein 1-Korand.*

Beweis. Sei $f\colon G \longrightarrow L^*$ ein 1-Kozyklus. Für $c \in L^*$ bilde man die sogenannte Poincaré-Reihe

$$b = \sum_{\sigma'\in G} f(\sigma')\cdot\sigma'(c).$$

Aufgrund der linearen Unabhängigkeit von Charakteren 4.6/2 kann man c so wählen, dass $b \neq 0$ ist. Man hat dann für beliebiges $\sigma \in G$

$$\begin{aligned}\sigma(b) &= \sum_{\sigma'\in G} \sigma\big(f(\sigma')\big)\cdot(\sigma\circ\sigma')(c)\\ &= \sum_{\sigma'\in G} f(\sigma)^{-1}\cdot f(\sigma\circ\sigma')\cdot(\sigma\circ\sigma')(c) = f(\sigma)^{-1}\cdot b,\end{aligned}$$

d. h. f ist ein 1-Korand. □

Um aus Theorem 2 Hilberts Satz 90 in der ursprünglich gegebenen Version zu erhalten, betrachte man eine zyklische Galois-Erweiterung L/K vom Grad n und wähle ein erzeugendes Element σ der Galois-Gruppe $\mathrm{Gal}(L/K)$. Man zeigt dann für $b \in L^*$ mit $\mathrm{N}_{L/K}(b) = 1$, dass $f\colon G \longrightarrow L^*$, gegeben durch

$$\begin{aligned} \sigma^0 &\longmapsto 1, \\ \sigma^1 &\longmapsto b, \\ &\dots \\ \sigma^{n-1} &\longmapsto b \cdot \sigma(b) \cdot \ldots \cdot \sigma^{n-2}(b), \end{aligned}$$

ein 1-Kozyklus und damit gemäß Theorem 2 ein 1-Korand ist.

Wir wollen Hilberts Satz 90 benutzen, um zyklische Erweiterungen genauer zu charakterisieren.

Satz 3. *Es sei L/K eine Körpererweiterung und n eine natürliche Zahl > 0 mit* $\mathrm{char}\, K \nmid n$. *Weiter enthalte K eine primitive n-te Einheitswurzel.*

(i) *Ist L/K eine zyklische Galois-Erweiterung vom Grad n, so gilt $L = K(a)$ für ein Element $a \in L$, dessen Minimalpolynom über K von der Form $X^n - c$ mit $c \in K$ ist.*

(ii) *Gilt umgekehrt $L = K(a)$ für ein Element $a \in L$, das Nullstelle eines Polynoms der Form $X^n - c \in K[X]$ ist, so ist L/K eine zyklische Galois-Erweiterung von K. Weiter ist $d = [L : K]$ ein Teiler von n, und es gilt $a^d \in K$, so dass $X^d - a^d \in K[X]$ das Minimalpolynom von a über K ist.*

Beweis. Es sei $\zeta \in K$ eine primitive n-te Einheitswurzel. Ist nun L/K eine zyklische Erweiterung vom Grad n, so gilt $\mathrm{N}_{L/K}(\zeta^{-1}) = \zeta^{-n} = 1$ mit 4.7/2, und es existiert aufgrund von Hilberts Satz 90 ein Element $a \in L^*$ mit $\sigma(a) = \zeta a$; dabei sei σ ein erzeugendes Element von $\mathrm{Gal}(L/K)$. Man hat dann

$$\sigma^i(a) = \zeta^i a, \qquad i = 0, \dots, n-1.$$

Insbesondere sind die Elemente $\sigma^0(a), \dots, \sigma^{n-1}(a)$ paarweise verschieden, so dass $[K(a) : K] \geq n$ folgt, bzw. $L = K(a)$ wegen $K(a) \subset L$ und

$[L : K] = n$.[4] Es gilt nun

$$\sigma(a^n) = \sigma(a)^n = \zeta^n a^n = a^n,$$

d. h. $a^n \in K$. Somit ist a Nullstelle des Polynoms

$$X^n - a^n \in K[X].$$

Da a über K vom Grad n ist, handelt es sich hierbei notwendigerweise bereits um das Minimalpolynom von a über K. Damit ist die Aussage (i) klar.

Nun zu Aussage (ii). Es gelte $L = K(a)$, wobei a Nullstelle eines Polynoms der Form $X^n - c \in K[X]$ sei. Der Fall $a = 0$ ist trivial, wir dürfen deshalb $a \neq 0$ annehmen. Dann sind $\zeta^0 a, \ldots, \zeta^{n-1} a$ insgesamt n verschiedene Nullstellen von $X^n - c$, so dass $L = K(a)$ ein Zerfällungskörper dieses Polynoms über K ist. Da es sich bei $X^n - c$ wegen $\operatorname{char} K \nmid n$ um ein separables Polynom handelt, ist L/K sogar eine Galois-Erweiterung. Für $\sigma \in \operatorname{Gal}(L/K)$ ist mit a auch $\sigma(a)$ eine Nullstelle von $X^n - c$. Daher existiert zu σ jeweils eine n-te Einheitswurzel $w_\sigma \in U_n$ mit $\sigma(a) = w_\sigma a$, und man stellt fest, dass

$$\operatorname{Gal}(L/K) \longrightarrow U_n, \qquad \sigma \longmapsto w_\sigma,$$

ein injektiver Gruppenhomomorphismus ist. Aufgrund des Satzes von Lagrange 1.2/3 ist $d := [L : K] = \operatorname{ord}(\operatorname{Gal}(L/K))$ ein Teiler von $n = \operatorname{ord} U_n$. Da U_n gemäß 4.5/1 zyklisch ist, hat auch jede Untergruppe von U_n diese Eigenschaft, insbesondere ist daher $\operatorname{Gal}(L/K)$ zyklisch. Erzeugt nun $\sigma \in \operatorname{Gal}(L/K)$ diese zyklische Gruppe der Ordnung d, so ist w_σ eine primitive d-te Einheitswurzel, und es gilt

$$\sigma(a^d) = \sigma(a)^d = w_\sigma^d a^d = a^d,$$

d. h. $a^d \in K$. Dann ist a Nullstelle von $X^d - a^d \in K[X]$, und dieses Polynom ist aus Gradgründen bereits das Minimalpolynom von $a \in L$ über K. □

Wir behandeln nun noch eine additive Form von Hilberts Satz 90. Auch hierzu gibt es eine Galois-kohomologische Verallgemeinerung, vgl. Aufgabe 5.

[4] Wir haben hier mit Hilfe von Hilberts Satz 90 ein spezielles erzeugendes Element der Körpererweiterung L/K erhalten. Dass L/K eine einfache Körpererweiterung ist, folgt indessen auch aus dem Satz vom primitiven Element 3.6/12.

Theorem 4 (Hilbert 90, additive Form). *Es sei L/K eine endliche zyklische Galois-Erweiterung, $\sigma \in \mathrm{Gal}(L/K)$ sei ein erzeugendes Element. Für Elemente $b \in L$ ist dann äquivalent*:

(i) $\mathrm{Sp}_{L/K}(b) = 0$.

(ii) *Es existiert ein $a \in L$ mit $b = a - \sigma(a)$.*

Beweis. Wir kopieren den Beweis zu Theorem 1. Für $b = a - \sigma(a)$ mit $a \in L$ folgt unter Benutzung von 4.7/6

$$\mathrm{Sp}_{L/K}(b) = \mathrm{Sp}_{L/K}(a) - \mathrm{Sp}_{L/K}\big(\sigma(a)\big) = 0.$$

Sei umgekehrt $b \in L$ gegeben mit $\mathrm{Sp}_{L/K}(b) = 0$, und sei $n = [L : K]$. Da die Spurfunktion $\mathrm{Sp}_{L/K}$ nicht identisch verschwindet, gibt es ein $c \in L$ mit $\mathrm{Sp}_{L/K}(c) \neq 0$; vgl. 4.7/7. Man definiere $a \in L$ durch

$$\begin{aligned} a \cdot \big(\mathrm{Sp}_{L/K}(c)\big) = {} & b \cdot \sigma(c) + \big(b + \sigma(b)\big) \cdot \sigma^2(c) + \ldots \\ & + \big(b + \sigma(b) + \ldots + \sigma^{n-2}(b)\big) \cdot \sigma^{n-1}(c). \end{aligned}$$

Anwenden von σ ergibt dann

$$\begin{aligned} \sigma(a) \cdot \big(\mathrm{Sp}_{L/K}(c)\big) = {} & \sigma(b)\sigma^2(c) + \big(\sigma(b) + \sigma^2(b)\big) \cdot \sigma^3(c) + \ldots \\ & + \big(\sigma(b) + \sigma^2(b) + \ldots + \sigma^{n-1}(b)\big) \cdot \sigma^n(c) \end{aligned}$$

und, indem wir

$$\begin{aligned} \mathrm{Sp}_{L/K}(b) &= b + \sigma(b) + \ldots + \sigma^{n-1}(b) = 0, \\ \mathrm{Sp}_{L/K}(c) &= c + \sigma(c) + \ldots + \sigma^{n-1}(c), \end{aligned}$$

benutzen, vgl. 4.7/4,

$$\begin{aligned} \big(a - \sigma(a)\big) \cdot \mathrm{Sp}_{L/K}(c) &= b\sigma(c) + b\sigma^2(c) + \ldots + b\sigma^{n-1}(c) \\ &\quad - \big(\sigma(b) + \sigma^2(b) + \ldots + \sigma^{n-1}(b)\big) \cdot \sigma^n(c) \\ &= b \cdot \big(\sigma(c) + \sigma^2(c) + \ldots + \sigma^{n-1}(c) + c\big) \\ &= b \cdot \mathrm{Sp}_{L/K}(c), \end{aligned}$$

d. h. $b = a - \sigma(a)$. □

Wir wollen die additive Form von Hilberts Satz 90 dazu verwenden, um im Falle $p = \mathrm{char}\, K > 0$ zyklische Erweiterungen vom Grad p zu studieren, ein Fall, der in Satz 3 nicht enthalten ist.

Theorem 5 (Artin-Schreier). *Es sei L/K eine Körpererweiterung in Charakteristik $p > 0$.*

(i) *Ist L/K eine zyklische Galois-Erweiterung vom Grad p, so gilt $L = K(a)$ für ein Element $a \in L$, dessen Minimalpolynom über K von der Form $X^p - X - c$ mit $c \in K$ ist.*

(ii) *Gilt umgekehrt $L = K(a)$ für ein Element $a \in L$, das Nullstelle eines Polynoms der Form $X^p - X - c \in K[X]$ ist, so ist L/K eine zyklische Galois-Erweiterung. Es zerfällt $X^p - X - c$ über K entweder vollständig in Linearfaktoren oder aber dieses Polynom ist irreduzibel. Im letzteren Falle ist L/K eine zyklische Galois-Erweiterung vom Grad p.*

Beweis. Sei zunächst L/K zyklisch vom Grad p. Gemäß 4.7/2 gilt dann $\mathrm{Sp}_{L/K}(c) = 0$ für alle $c \in K$. Insbesondere gibt es aufgrund der additiven Form von Hilberts Satz 90 ein $a \in L$ mit $\sigma(a) - a = 1$; dabei sei $\sigma \in \mathrm{Gal}(L/K)$ ein erzeugendes Element. Es folgt

$$\sigma^i(a) = a + i, \qquad i = 0, \ldots, p-1.$$

Da $\sigma^0(a), \ldots, \sigma^{p-1}(a)$ paarweise verschieden sind, hat a mindestens den Grad p über K, so dass sich $[K(a) : K] \geq p$, also $L = K(a)$ ergibt. Weiter gilt

$$\sigma(a^p - a) = \sigma(a)^p - \sigma(a) = (a+1)^p - (a+1) = a^p - a$$

und somit $c := a^p - a \in K$. Es ist also a eine Nullstelle des Polynoms $X^p - X - c$, und dieses Polynom ist aus Gradgründen das Minimalpolynom von a über K.

Es sei nun umgekehrt $L = K(a)$, wobei a eine Nullstelle eines Polynoms der Gestalt $f = X^p - X - c \in K[X]$ sei. Mit a ist dann auch $a + 1$ Nullstelle dieses Polynoms, d. h.

$$a, a+1, \ldots, a+p-1 \in L$$

sind die p verschiedenen Nullstellen von f. Hat also f eine Nullstelle in K, so liegen alle Nullstellen von f in K, und f zerfällt über K vollständig in Linearfaktoren. Das gleiche Argument zeigt, dass L ein Zerfällungskörper des separablen Polynoms f über K ist, die Erweiterung L/K also galoissch ist. Im Trivialfall $L = K$ ist sie auch zyklisch. Sei nun f ohne Nullstelle in K. Wir behaupten, dass dann f bereits irreduzibel über K ist. Ist dies nämlich

nicht der Fall, so existiert eine Zerlegung $f = gh$ in zwei nicht-konstante normierte Polynome g und h. Über L hat man die Faktorisierung

$$f = \prod_{i=0}^{p-1} (X - a - i),$$

und g besteht aus gewissen dieser Faktoren. Sei $d = \operatorname{grad} g$. Der Koeffizient von X^{d-1} in g hat die Gestalt $-da + j$ mit einem gewissen Element j aus dem Primkörper $\mathbb{F}_p \subset K$. Aus $-da + j \in K$ und $p \nmid d$ folgt dann $a \in K$, so dass f eine Nullstelle in K haben würde, was wir aber ausgeschlossen hatten. Folglich ist f irreduzibel, wenn f keine Nullstelle in K hat. Wählt man dann $\sigma \in \operatorname{Gal}(L/K)$ mit $\sigma(a) = a + 1$, vgl. 3.4/8, so hat σ eine Ordnung $\geq p$, und wegen $\operatorname{ord} \operatorname{Gal}(L/K) = \operatorname{grad} f = p$ ist L/K eine zyklische Erweiterung vom Grad p. □

Lernkontrolle und Prüfungsvorbereitung

1. Was versteht man unter einer zyklischen Galois-Erweiterung?
2. Wie lautet der berühmte Satz 90 von D. Hilbert?
3. [+] Führe den Beweis zu Hilberts Satz 90.
4. Erläutere die kohomologische Version von Hilberts Satz 90.
5. [+] Führe den Beweis zur kohomologischen Version von Hilberts Satz 90.
6. Benutze Hilberts Satz 90 zur Charakterisierung zyklischer Galois-Erweiterungen L/K mit einem Grad, der prim zu $\operatorname{char} K$ ist.
7. Erläutere die additive Version von Hilberts Satz 90.
8. [+] Führe den Beweis zur additiven Form von Hilberts Satz 90.
9. Erläutere das Theorem von Artin-Schreier zur Charakterisierung zyklischer Galois-Erweiterungen L/K vom Grade $p = \operatorname{char} K > 0$.

Übungsaufgaben

1. *Betrachte in der Situation von Theorem* 1 *zu einem Element* $b \in L^*$ *Elemente* $a \in L^*$ *mit* $b = a \cdot \sigma(a)^{-1}$. *Welche Eindeutigkeitsaussage lässt sich formulieren*? *Untersuche dieselbe Frage auch für die Situation von Theorem* 4.
2. *Überlege, was die Aussage von Hilberts Satz* 90 *für die Erweiterung* $\mathbb{C}/\mathbb{R}$ *bedeutet.*

3. Es sei L ein Zerfällungskörper eines Polynoms des Typs $X^n - a$ über einem Körper K mit $\operatorname{char} K \nmid n$. Ist die Erweiterung L/K stets zyklisch? Diskutiere insbesondere den Fall $K = \mathbb{Q}$.

4. Für eine endliche Galois-Erweiterung L/K mit zugehöriger Galois-Gruppe $G = \mathrm{Gal}(L/K)$ zeige $H^1(G, \mathrm{GL}(n, L)) = \{1\}$. (*Hinweis*: Behandle nur den Fall, wo K unendlich viele Elemente besitzt, und gehe wie im Beweis zu Theorem 2 vor, unter Benutzung von Aufgabe 3 aus Abschnitt 4.6. Beachte bei der Definition von $H^1(G, \mathrm{GL}(n, L))$, dass dieses Objekt zunächst als "Kohomologiemenge" aufgefasst werden muss, da die Gruppe $\mathrm{GL}(n, L)$ für $n > 1$ nicht abelsch ist. Es ist also zunächst nicht klar, dass die zu betrachtende Gruppe der 1-Koränder einen Normalteiler in der Gruppe der 1-Kozyklen bildet, die Menge der Restklassen also wiederum eine Gruppe ist.)

5. Für eine endliche Galois-Erweiterung L/K mit zugehöriger Galois-Gruppe $G = \mathrm{Gal}(L/K)$ zeige $H^1(G, L) = 0$, wobei L als additive Gruppe mit der kanonischen Aktion von G aufzufassen ist. (*Hinweis*: Verwende eine additive Version des Beweises zu Theorem 2.)

6. Zeige unter Verwendung von Hilberts Satz 90, dass für zwei Zahlen $a, b \in \mathbb{Q}$ genau dann $a^2 + b^2 = 1$ gilt, wenn es $m, n \in \mathbb{Z}$ gibt mit

$$a = \frac{m^2 - n^2}{m^2 + n^2}, \qquad b = \frac{2mn}{m^2 + n^2}.$$

4.9 Multiplikative Kummer-Theorie*

Eine Galois-Erweiterung L/K heißt bekanntlich *abelsch*, wenn die zugehörige Galois-Gruppe $G = \mathrm{Gal}(L/K)$ abelsch ist. Sie heißt *abelsch vom Exponenten d* für eine natürliche Zahl $d > 0$, wenn G eine abelsche Gruppe vom Exponenten d ist, d. h. wenn G abelsch ist und man $\sigma^d = 1$ für jedes $\sigma \in G$ hat, wobei d minimal mit dieser Eigenschaft gewählt ist. Als Verallgemeinerung zyklischer Erweiterungen wollen wir im Folgenden abelsche Erweiterungen mit Exponenten studieren, die jeweils Teiler einer vorgegebenen Zahl $n \in \mathbb{N} - \{0\}$ sind. Solche Erweiterungen werden auch als *Kummer-Erweiterungen* bezeichnet, zu Ehren von E. Kummer, der sich hiermit aus zahlentheoretischem Anlass beschäftigte.[5]

[5] Genauer wird eine abelsche Erweiterung L/K mit einem Exponent $d > 0$ als *Kummer-Erweiterung* bezeichnet, wenn $\operatorname{char} K \nmid d$ gilt und K die Gruppe U_d aller d-ten Einheitswurzeln enthält.

Wir setzen zunächst $\operatorname{char} K \nmid n$ voraus und weiter, dass K die Gruppe U_n aller n-ten Einheitswurzeln enthält. Für $c \in K$ bezeichne $K(c^{1/n})$ eine Erweiterung, welche durch Adjunktion einer n-ten Wurzel zu c aus K entsteht. Man beachte dabei, dass $c^{1/n}$ in einem algebraischen Abschluss von K nur bis auf eine n-te Einheitswurzel eindeutig bestimmt ist, dass aber der Körper $K(c^{1/n})$ wohldefiniert ist als Zerfällungskörper des Polynoms $X^n - c$, da K bereits alle n-ten Einheitswurzeln enthält. Gemäß 4.8/3 ist $K(c^{1/n})/K$ eine zyklische Erweiterung von einem Grad, der n teilt. Für eine Teilmenge $C \subset K$ sei allgemeiner $K(C^{1/n})$ diejenige Galoiserweiterung, die aus K durch Adjunktion aller n-ten Wurzeln $c^{1/n}$ mit $c \in C$ entsteht. Man kann dann $K(C^{1/n})$ als Kompositum aller Erweiterungen $K(c^{1/n})$ mit $c \in C$ auffassen. Insbesondere setzen sich die nach 4.1/2 existierenden Einschränkungsabbildungen $\operatorname{Gal}(K(C^{1/n})/K) \longrightarrow \operatorname{Gal}(K(c^{1/n})/K)$ zu einem Monomorphismus

$$\operatorname{Gal}\big(K(C^{1/n})\,/\,K\big) \longrightarrow \prod_{c \in C} \operatorname{Gal}\big(K(c^{1/n})\,/\,K\big)$$

zusammen, und man erkennt $K(C^{1/n})/K$ als (nicht notwendig endliche) abelsche Erweiterung mit einem Exponenten, der n teilt. Wir werden dies allerdings weiter unten in Satz 1 (i) nochmals in direkter Weise einsehen, ohne auf die in 4.8/3 gegebene Charakterisierung zyklischer Erweiterungen Bezug zu nehmen.

Im Folgenden sei G_C die Galois-Gruppe der Erweiterung $K(C^{1/n})/K$. Für $\sigma \in G_C$ und eine n-te Wurzel $c^{1/n}$ eines Elementes $c \in C$ ist dann $\sigma(c^{1/n})$ ebenfalls eine n-te Wurzel zu c. Es existiert daher eine n-te Einheitswurzel $w_\sigma \in U_n$ mit $\sigma(c^{1/n}) = w_\sigma c^{1/n}$. Wie man leicht nachprüft, ist $w_\sigma = \sigma(c^{1/n}) \cdot c^{-1/n}$ unabhängig von der speziellen Wahl der n-ten Wurzel $c^{1/n}$ zu c. Wir erhalten deshalb eine wohldefinierte Paarung

$$\langle \cdot, \cdot \rangle \colon G_C \times C \longrightarrow U_n, \qquad (\sigma, c) \longmapsto \frac{\sigma(c^{1/n})}{c^{1/n}}.$$

Im Folgenden wollen wir C als Untergruppe von K^* voraussetzen. Dann ist $\langle \cdot, \cdot \rangle$ insbesondere bimultiplikativ, denn es gilt

$$\langle \sigma \circ \tau, c \rangle = \frac{\sigma \circ \tau(c^{1/n})}{c^{1/n}} = \frac{\sigma \circ \tau(c^{1/n})}{\tau(c^{1/n})} \cdot \frac{\tau(c^{1/n})}{c^{1/n}} = \langle \sigma, c \rangle \cdot \langle \tau, c \rangle,$$

$$\langle \sigma, c \cdot c' \rangle = \frac{\sigma(c^{1/n} c'^{1/n})}{c^{1/n} c'^{1/n}} = \frac{\sigma(c^{1/n})}{c^{1/n}} \cdot \frac{\sigma(c'^{1/n})}{c'^{1/n}} = \langle \sigma, c \rangle \cdot \langle \sigma, c' \rangle,$$

für $\sigma, \tau \in G_C$ und $c, c' \in C$. Weiter hat man $\langle \sigma, c^n \rangle = 1$ für $\sigma \in G_C$ und $c \in K^*$. Setzen wir daher voraus, dass $C \subset K^*$ eine Untergruppe ist, welche die Gruppe K^{*n} aller n-ten Potenzen von Elementen aus K^* enthält, so faktorisiert $\langle \cdot, \cdot \rangle$ zu einer bimultiplikativen Abbildung

$$G_C \times C/K^{*n} \longrightarrow U_n, \qquad (\sigma, \overline{c}) \longmapsto \frac{\sigma(c^{1/n})}{c^{1/n}},$$

die wir ebenfalls mit $\langle \cdot, \cdot \rangle$ bezeichnen.

Satz 1. *Wie oben betrachte man einen Körper K und eine natürliche Zahl $n > 0$ mit* $\operatorname{char} K \nmid n$ *und $U_n \subset K^*$. Weiter sei $C \subset K^*$ eine Untergruppe mit $K^{*n} \subset C$. Dann gilt*:

(i) *Es ist $K(C^{1/n})/K$ eine abelsche Galois-Erweiterung mit einem Exponenten, der n teilt. Sei G_C die zugehörige Galois-Gruppe.*

(ii) *Die bimultiplikative Abbildung*

$$\langle \cdot, \cdot \rangle \colon G_C \times C/K^{*n} \longrightarrow U_n, \qquad (\sigma, \overline{c}) \longmapsto \frac{\sigma(c^{1/n})}{c^{1/n}}$$

ist nicht ausgeartet, induziert also Monomorphismen

$$\begin{aligned} \varphi_1 \colon \quad & G_C \longrightarrow \operatorname{Hom}\big(C/K^{*n}, U_n\big), & \sigma &\longmapsto \langle \sigma, \cdot \rangle, \\ \varphi_2 \colon \quad & C/K^{*n} \longrightarrow \operatorname{Hom}(G_C, U_n), & \overline{c} &\longmapsto \langle \cdot, \overline{c} \rangle, \end{aligned}$$

in die Gruppe aller Homomorphismen $C/K^{*n} \longrightarrow U_n$ bzw. $G_C \longrightarrow U_n$. Genauer, φ_1 ist ein Isomorphismus, und es induziert φ_2 einen Isomorphismus $C/K^{*n} \xrightarrow{\sim} \operatorname{Hom}_{\text{stet}}(G_C, U_n)$ auf die Gruppe aller stetigen Homomorphismen $G_C \longrightarrow U_n$.[6]

(iii) *Es ist $K(C^{1/n})/K$ genau dann endlich, wenn $(C : K^{*n})$ endlich ist. Im letzteren Fall ist neben φ_1 auch die Abbildung φ_2 aus* (ii) *ein Isomorphismus, und es gilt $[K(C^{1/n}) : K] = (C : K^{*n})$.*

Beweis. Behauptung (i) folgt aus der Injektivität von φ_1 in (ii). Zum Nachweis dieser Injektivität betrachte man ein $\sigma \in G_C$ mit $\sigma(c^{1/n}) = c^{1/n}$ für

[6] Dabei werde G_C als topologische Gruppe wie in Abschnitt 4.2 betrachtet; U_n versehe man mit der diskreten Topologie. Ein Homomorphismus $f \colon G_C \longrightarrow U_n$ ist also genau dann stetig, wenn $H = \ker f$ eine offene Untergruppe in G_C ist, d. h. gemäß 4.2/3 und 4.2/5, wenn es eine endliche Galois-Erweiterung K'/K in $K(C^{1/n})$ gibt mit $H = \operatorname{Gal}(K(C^{1/n})/K')$ oder, alternativ, mit $H \supset \operatorname{Gal}(K(C^{1/n})/K')$.

alle $c \in C$. Offenbar folgt dann $\sigma(a) = a$ für alle Elemente $a \in K(C^{1/n})$ und somit $\sigma = \mathrm{id}$, d. h. φ_1 ist injektiv. Sei andererseits $c \in C$ mit $\sigma(c^{1/n}) = c^{1/n}$ für alle $\sigma \in G_C$. Dies ergibt $c^{1/n} \in K$ und daher $c \in K^{*n}$, so dass auch φ_2 injektiv ist.

Als Nächstes zeigen wir Behauptung (iii) und benutzen dabei, dass die Homomorphismen φ_1, φ_2 aus (ii) bereits als injektiv erkannt sind. Aus der Endlichkeit von $[K(C^{1/n}) : K]$ bzw. G_C folgt diejenige von $\mathrm{Hom}(G_C, U_n)$ und damit unter Benutzung der Injektivität von φ_2 auch die Endlichkeit von C/K^{*n}. Umgekehrt impliziert die Endlichkeit von C/K^{*n} diejenige von $\mathrm{Hom}(C/K^{*n}, U_n)$ und damit von G_C, da φ_1 injektiv ist, also von $[K(C^{1/n}) : K]$. Im Falle der Endlichkeit bestehen, wie wir sogleich in Lemma 2 zeigen werden, (nicht-kanonische) Isomorphismen

$$C/K^{*n} \xrightarrow{\sim} \mathrm{Hom}\big(C/K^{*n}, U_n\big), \qquad G_C \xrightarrow{\sim} \mathrm{Hom}(G_C, U_n).$$

Deshalb zeigt die Abschätzung

$$\begin{aligned}\big[K(C^{1/n}) : K\big] = \operatorname{ord} G_C &\le \operatorname{ord} \mathrm{Hom}\big(C/K^{*n}, U_n\big) = \operatorname{ord} C/K^{*n} \\ &\le \operatorname{ord} \mathrm{Hom}(G_C, U_n) = \operatorname{ord} G_C = \big[K(C^{1/n}) : K\big]\end{aligned}$$

die gewünschte Gleichung $[K(C^{1/n}) : K] = (C : K^{*n})$. Insbesondere sind φ_1 und φ_2 dann Isomorphismen, so dass Satz 1 für $[K(C^{1/n}) : K] < \infty$ bzw. $(C : K^{*n}) < \infty$ vollständig bewiesen ist.

Im nicht-endlichen Fall betrachten wir das System $(C_i)_{i\in I}$ aller Untergruppen von C mit $C_i \supset K^{*n}$ und $(C_i : K^{*n}) < \infty$. Dann gilt $C = \bigcup_{i\in I} C_i$ sowie $K(C^{1/n}) = \bigcup_{i\in I} K(C_i^{1/n})$, wenn man sich alle diese Körper als Teilkörper eines algebraischen Abschlusses von K vorstellt. Für jedes $i \in I$ haben wir ein kommutatives Diagramm

$$\begin{array}{ccc} G_C & \xrightarrow{\varphi_1} & \mathrm{Hom}\big(C/K^{*n}, U_n\big) \\ \big\downarrow & & \big\downarrow \\ G_{C_i} & \xrightarrow{\varphi_{1,i}} & \mathrm{Hom}\big(C_i/K^{*n}, U_n\big), \end{array}$$

wobei die vertikale Abbildung links die Einschränkung von Galois-Automorphismen auf $K(C^{1/n})/K$ zu solchen auf $K(C_i^{1/n})/K$ darstellt (vgl. 4.1/2) und die vertikale Abbildung rechts durch Einschränkung von Homomorphismen $C/K^{*n} \longrightarrow U_n$ auf C_i/K^{*n} entsteht. Wie wir gesehen haben, sind

die Abbildungen $\varphi_{1,i}$ alle bijektiv. Starten wir daher mit einem Homomorphismus $f\colon C/K^{*n} \longrightarrow U_n$, so existieren eindeutig bestimmte Elemente $\sigma_i \in G_{C_i}$ mit $\varphi_{1,i}(\sigma_i) = f|_{C_i/K^{*n}}$, und man überprüft leicht, dass sich die σ_i zu einem Galois-Automorphismus $\sigma \in G_C$ mit $\varphi_1(\sigma) = f$ zusammensetzen. Folglich ist φ_1 surjektiv und damit bijektiv.

Um die entsprechende Aussage für φ_2 zu erhalten, betrachte man für $i \in I$ das kommutative Diagramm

$$\begin{array}{ccc} C_i/K^{*n} & \xrightarrow{\varphi_{2,i}} & \mathrm{Hom}(G_{C_i}, U_n) \\ \downarrow & & \downarrow \\ C/K^{*n} & \xrightarrow{\varphi_2} & \mathrm{Hom}(G_C, U_n), \end{array}$$

wobei die vertikale Abbildung links die kanonische Inklusion ist und diejenige rechts durch die bereits oben betrachtete Restriktion $G_C \longrightarrow G_{C_i}$ induziert wird. Da jeder stetige Homomorphismus $f\colon G_C \longrightarrow U_n$ von einem Homomorphismus des Typs $f_i\colon G_{C_i} \longrightarrow U_n$ induziert wird und da $\varphi_{2,i}$ bijektiv ist, ergibt sich auch die Behauptung für φ_2 in (ii). □

Es bleibt noch die Existenz der benutzten Dualitäts-Isomorphismen nachzuweisen, wobei U_n gemäß 4.5/1 zyklisch von der Ordnung n, also isomorph zu $\mathbb{Z}/n\mathbb{Z}$ ist.

Lemma 2. *Es sei H eine endliche abelsche Gruppe mit einem Exponenten, der eine gegebene Zahl $n \in \mathbb{N} - \{0\}$ teilt. Dann existiert ein (nichtkanonischer) Isomorphismus $H \xrightarrow{\sim} \mathrm{Hom}(H, \mathbb{Z}/n\mathbb{Z})$.*

Beweis. Da $\mathrm{Hom}(\cdot, \mathbb{Z}/n\mathbb{Z})$ mit endlichen direkten Summen verträglich ist, können wir den Hauptsatz über endlich erzeugte abelsche Gruppen 2.9/9 anwenden und dementsprechend H als zyklisch von einer Ordnung d mit $d \mid n$ annehmen. Es ist dann also ein Isomorphismus

$$\mathbb{Z}/d\mathbb{Z} \xrightarrow{\sim} \mathrm{Hom}\big(\mathbb{Z}/d\mathbb{Z}, \mathbb{Z}/n\mathbb{Z}\big)$$

zu konstruieren.

Wir reduzieren zunächst auf den Fall $d = n$. In der Lösung zu Aufgabe 2 aus Abschnitt 1.3 hatten wir gesehen, dass es zu jedem Teiler d von n genau eine Untergruppe $H_d \subset \mathbb{Z}/n\mathbb{Z}$ der Ordnung d gibt und dass diese wiederum zyklisch ist. Für $d' \mid d$ gilt dann natürlich $H_{d'} \subset H_d$, und es folgt, dass jeder

Homomorphismus $\mathbb{Z}/d\mathbb{Z} \longrightarrow \mathbb{Z}/n\mathbb{Z}$ durch H_d faktorisiert. Deshalb ist die kanonische Abbildung $\mathrm{Hom}(\mathbb{Z}/d\mathbb{Z}, H_d) \longrightarrow \mathrm{Hom}(\mathbb{Z}/d\mathbb{Z}, \mathbb{Z}/n\mathbb{Z})$ ein Isomorphismus. Wegen $H_d \simeq \mathbb{Z}/d\mathbb{Z}$ genügt es folglich, einen Isomorphismus $\mathbb{Z}/d\mathbb{Z} \longrightarrow \mathrm{Hom}(\mathbb{Z}/d\mathbb{Z}, \mathbb{Z}/d\mathbb{Z})$ anzugeben. Nun ist aber

$$\mathbb{Z} \longrightarrow \mathrm{Hom}\big(\mathbb{Z}/d\mathbb{Z}, \mathbb{Z}/d\mathbb{Z}\big), \qquad 1 \longmapsto \mathrm{id},$$

offenbar ein Epimorphismus mit Kern $d\mathbb{Z}$ und induziert somit einen Isomorphismus der gewünschten Art. □

Theorem 3. *Es sei K ein Körper und $n > 0$ eine natürliche Zahl mit* $\mathrm{char}\, K \nmid n$ *und $U_n \subset K^*$. Dann sind die Abbildungen*

$$\left\{ \begin{array}{c} \text{Untergruppen } C \subset K^* \\ \text{mit } K^{*n} \subset C \end{array} \right\} \underset{\Psi}{\overset{\Phi}{\rightleftarrows}} \left\{ \begin{array}{c} \text{abelsche Erweiterungen } L/K \\ \text{mit Exponenten, die } n \text{ teilen} \end{array} \right\}$$

$$\begin{aligned} C &\longmapsto K(C^{1/n}), \\ L^{*n} \cap K^* &\longmapsto L, \end{aligned}$$

inklusionserhaltend, bijektiv und zueinander invers.[7] *In dieser Situation wird die Galois-Gruppe G_C einer Erweiterung $K(C^{1/n})/K$ charakterisiert durch den Isomorphismus*

$$\varphi_1 \colon G_C \longrightarrow \mathrm{Hom}\big(C/K^{*n}, U_n\big), \qquad \sigma \longmapsto \langle \sigma, \cdot \rangle,$$

aus Satz 1 (ii). *Falls C/K^{*n} endlich ist, so sind* $\mathrm{Hom}(C/K^{*n}, U_n)$ *und damit auch $G_C = \mathrm{Gal}(K(C^{1/n})/K)$ isomorph zu C/K^{*n}.*

Beweis. Aufgrund von Satz 1 und Lemma 2 bleibt lediglich zu zeigen, dass die Abbildungen Φ, Ψ bijektiv und zueinander invers sind. Wir beginnen mit der Beziehung $\Psi \circ \Phi = \mathrm{id}$ und betrachten eine Untergruppe $C \subset K^*$ mit $C \supset K^{*n}$, wobei wir zunächst $(C : K^{*n}) < \infty$ annehmen. Setzen wir dann $C' = K(C^{1/n})^{*n} \cap K^*$, so gilt $C \subset C'$ und weiter $K(C^{1/n}) = K(C'^{1/n})$. Mit Satz 1 (iii) folgt hieraus $C = C'$.

Ist nun der Index $(C : K^{*n})$ nicht notwendig endlich, so können wir die gerade durchgeführte Argumentation auf alle Untergruppen $C_i \subset C$

[7] Damit wir von der *Menge* aller abelschen Erweiterungen von K sprechen können, fassen wir solche Erweiterungen stets als Teilkörper eines fest gewählten algebraischen Abschlusses $\overline{K}$ von K auf.

anwenden, die über K^{*n} von endlichem Index sind. Da C Vereinigung dieser Untergruppen ist und außerdem $K(C^{1/n}) = \bigcup_i K(C_i^{1/n})$ gilt, ergibt sich auch in diesem Fall $C = K(C^{1/n})^{*n} \cap K^*$ und somit $\Psi \circ \Phi = \mathrm{id}$.

Um zu sehen, dass auch $\Phi \circ \Psi = \mathrm{id}$ gilt, betrachten wir eine abelsche Erweiterung L/K mit einem Exponenten, der n teilt. Mit $C = L^{*n} \cap K^*$ haben wir dann $K(C^{1/n}) \subset L$, und es ist zu zeigen, dass beide Körper übereinstimmen. Indem wir L als Vereinigung endlicher Galois- und dann notwendig abelscher Erweiterungen darstellen, dürfen wir ohne Einschränkung L/K als endlich voraussetzen. Wir betrachten nun den nach 4.1/2 existierenden Epimorphismus

$$q\colon\ \mathrm{Gal}\big(L/K\big) \longrightarrow G_C, \qquad \sigma \longmapsto \sigma|_{K(C^{1/n})}.$$

Es genügt zu zeigen, dass der assoziierte Homomorphismus

$$q^*\colon\ \mathrm{Hom}\big(G_C, U_n\big) \longrightarrow \mathrm{Hom}\big(\mathrm{Gal}(L/K), U_n\big), \qquad f \longmapsto f \circ q,$$

ein Isomorphismus ist. Denn dann haben die Galois-Gruppen zu den Erweiterungen $K(C^{1/n})/K$ und L/K aufgrund von Lemma 2 gleiche Ordnungen, und wir können daraus $[L : K] = [K(C^{1/n}) : K]$ sowie $L = K(C^{1/n})$ schließen.

Zunächst ist q^* aufgrund der Surjektivität von q injektiv. Um zu sehen, dass q^* auch surjektiv ist, betrachte man einen Homomorphismus $g\colon\ \mathrm{Gal}(L/K) \longrightarrow U_n$. Es gilt dann für $\sigma, \sigma' \in \mathrm{Gal}(L/K)$

$$g(\sigma \circ \sigma') = g(\sigma) \cdot g(\sigma') = \sigma \circ g(\sigma') \cdot g(\sigma).$$

In der Sprache von Abschnitt 4.8 ist g ein 1-Kozyklus und gemäß 4.8/2 auch ein 1-Korand, d. h. es existiert ein Element $a \in L^*$ mit $g(\sigma) = a \cdot \sigma(a)^{-1}$ für alle $\sigma \in \mathrm{Gal}(L/K)$. Dabei gilt notwendigerweise $a^n \in C = L^{*n} \cap K^*$, also $a \in K(C^{1/n})$, denn aus $g(\sigma)^n = 1$ ergibt sich $\sigma(a^n) = \sigma(a)^n = a^n$. Führen wir nun den Homomorphismus

$$f\colon G_C \longrightarrow U_n, \qquad \sigma \longmapsto a \cdot \sigma(a)^{-1}$$

ein, so gilt offenbar $g = f \circ q = q^*(f)$, und es folgt, wie behauptet, die Surjektivität von q^*. □

Ist L/K in der Situation von Theorem 3 eine abelsche Erweiterung mit einem Exponenten, der n teilt, so kann man leicht eine K-Basis von

L/K wie folgt angeben. Man setze $C = L^{*n} \cap K^*$ und betrachte ein System $(c_i)_{i\in I}$ von Elementen aus C, welches ein Repräsentantensystem von C/K^{*n} bildet. Dann ist $(c_i^{1/n})_{i\in I}$ bei beliebiger Wahl der n-ten Wurzeln eine K-Basis von L/K. In der Tat, dieses System ist offenbar ein K-Erzeugendensystem von L/K. Zudem besteht es im Falle $[L : K] < \infty$ aus genau $(C : K^{*n}) = [L : K]$ Elementen, ist also auch linear unabhängig. Indem wir L durch endliche abelsche Erweiterungen von K ausschöpfen, sehen wir, dass $(c_i^{1/n})_{i\in I}$ linear unabhängig und damit eine K-Basis von L ist.

Lernkontrolle und Prüfungsvorbereitung

1. Was versteht man unter einer abelschen Körpererweiterung vom Exponenten d für eine natürliche Zahl $d > 0$, was unter einer Kummer-Erweiterung?
2. Es sei K ein Körper und $n > 0$ eine natürliche Zahl, so dass $\operatorname{char} K \nmid n$ gilt und K die Gruppe U_n der n-ten Einheitswurzeln enthält. Betrachte eine Untergruppe $C \subset K^*$, welche die Gruppe K^{*n} aller n-ten Potenzen von Elementen aus K^* enthält. Definiere die Erweiterung $K(C^{1/n})/K$ und begründe, dass dies eine abelsche Erweiterung von einem Exponenten d ist, der n teilt.
3. Definiere in der Situation von Punkt 2 die in der Kummer-Theorie betrachtete Paarung $\langle\cdot,\cdot\rangle\colon \operatorname{Gal}(K(C^{1/n})/K) \times C/K^{*n} \longrightarrow U_n$ und zeige, dass diese bimultiplikativ ist.
4. Welche Eigenschaften besitzt die Paarung von Punkt 3? Diskutiere insbesondere die zugehörigen Homomorphismen

$$\begin{aligned} \varphi_1\colon \operatorname{Gal}\big(K(C^{1/n})/K\big) &\longrightarrow \operatorname{Hom}\big(C/K^{*n}, U_n\big), & \sigma &\longmapsto \langle\sigma,\cdot\rangle,\\ \varphi_2\colon \quad C/K^{*n} &\longrightarrow \operatorname{Hom}\big(\operatorname{Gal}\big(K(C^{1/n})/K\big), U_n\big), & \overline{c} &\longmapsto \langle\cdot,\overline{c}\rangle. \end{aligned}$$

5. Wie steht in der Situation von Punkt 4 die Endlichkeit von $K(C^{1/n})/K$ in Relation zur Endlichkeit von C/K^{*n}? Wie berechnet sich im Falle der Endlichkeit die Galois-Gruppe der Erweiterung $K(C^{1/n})/K$?

+6. Führe die Beweise zu den Punkten 4 und 5.

7. Wie lassen sich in der Situation von Punkt 2 die abelschen Erweiterungen L/K von einem Index d charakterisieren, der n teilt? Was weiß man jeweils über die zugehörige Galois-Gruppe von L/K?

+8. Führe die Beweise zu Punkt 7 aus.

Übungsaufgaben

K sei ein Körper, $\overline{K}$ ein algebraischer Abschluss von K und $n > 0$ eine natürliche Zahl mit $\operatorname{char} K \nmid n$, derart dass K eine primitive n-te Einheitswurzel enthält.

1. *Folgere die in* 4.8/3 *gegebene Charakterisierung zyklischer Erweiterungen von K aus der Kummer-Theorie.*
2. *Betrachte in $\overline{K}$ alle abelschen Erweiterungen L/K mit einem Exponenten, der n teilt, und zeige, dass es hierunter eine größte Erweiterung L_n/K gibt. Wie lässt sich die Galois-Gruppe* $\operatorname{Gal}(L_n/K)$ *charakterisieren*?
3. Setze $K = \mathbb{Q}$ und $n = 2$ in der Situation von Aufgabe 2. Zeige, dass dann $L_2 = \mathbb{Q}(i, \sqrt{2}, \sqrt{3}, \sqrt{5}, \ldots)$ gilt und bestimme die Galois-Gruppe der Erweiterung $L_2/\mathbb{Q}$.
4. Betrachte für $c, c' \in K^*$ die Zerfällungskörper $L, L' \subset \overline{K}$ der Polynome $X^n - c$ und $X^n - c'$ über K. Zeige, es gilt genau dann $L = L'$, wenn es eine zu n teilerfremde Zahl $r \in \mathbb{N}$ gibt mit $c^r \cdot c' \in K^{*n}$.
5. Zeige: Für jede endliche Galois-Erweiterung L/K gibt es einen kanonischen Isomorphismus von Gruppen

$$(L^{*n} \cap K^*) \big/ K^{*n} \xrightarrow{\sim} \operatorname{Hom}\big(\operatorname{Gal}(L/K), U_n\big).$$

4.10 Allgemeine Kummer-Theorie, Witt-Vektoren*

Im vorigen Abschnitt haben wir für einen Körper K die Kummer-Theorie zu einem Exponenten n mit $\operatorname{char} K \nmid n$ entwickelt. In ähnlicher Weise kann man für $p = \operatorname{char} K > 0$ die Kummer-Theorie zum Exponenten p, auch als *Artin-Schreier-Theorie* bezeichnet, sowie allgemeiner die Kummer-Theorie zu einem Exponenten p^r mit $r \geq 1$ behandeln, die auf E. Witt zurückgeht. Allen diesen Theorien liegt ein allgemeines Gerüst zugrunde, sozusagen eine allgemeine Kummer-Theorie, die wir zunächst in ihren Grundzügen erläutern wollen. Es sei K_s ein separabel algebraischer Abschluss von K, den wir uns etwa in einem algebraischen Abschluss von K als Teilkörper aller über K separablen Elemente vorstellen können; die Charakteristik von K unterliege dabei im Moment noch keinerlei Einschränkung. Es ist K_s/K eine Galois-Erweiterung; die zugehörige Galois-Gruppe $G = \operatorname{Gal}(K_s/K)$ wird auch als die *absolute Galois-Gruppe* von K bezeichnet. Wir fassen sie als topologische Gruppe im Sinne von Abschnitt 4.2 auf.

Kummer-Theorie. — Für eine Kummer-Theorie über K benötigt man zunächst einmal einen stetigen G-Modul A. Hierunter versteht man eine abelsche Gruppe A mit einer stetigen G-Aktion

$$G \times A \longrightarrow A, \qquad (\sigma, a) \longmapsto \sigma(a),$$

welche die Gruppenstruktur von A respektiert; auf A betrachte man dabei die diskrete Topologie. Bezüglich der Definition von Gruppenaktionen sei auf 5.1/1 und 5.1/2 verwiesen. Insbesondere kann man sich eine Aktion der betrachteten Art als einen Homomorphismus $G \longrightarrow \operatorname{Aut} A$ vorstellen; $\sigma(a)$ ist dann zu interpretieren als das Bild von a unter dem mittels $G \longrightarrow \operatorname{Aut} A$ durch σ induzierten Automorphismus $A \longrightarrow A$. Im Übrigen bedeutet die Stetigkeitsbedingung, dass für jedes Element $a \in A$ die Untergruppe

$$G(A/a) = \big\{\sigma \in G \,;\, \sigma(a) = a\big\}$$

offen in G ist. Gemäß 4.2/5 ist dies äquivalent dazu, dass $G(A/a)$ abgeschlossen in G und der Fixkörper $K_s^{G(A/a)}$ endlich über K ist.

Aufgrund des Hauptsatzes der Galois-Theorie 4.2/3 korrespondieren die Zwischenkörper von K_s/K in bijektiver Weise zu den abgeschlossenen Untergruppen von G, und zwar mittels der Abbildung $L \longmapsto \operatorname{Gal}(K_s/L)$. Wir können daher einem Zwischenkörper L von K_s/K bzw. einer abgeschlossenen Untergruppe $\operatorname{Gal}(K_s/L) \subset G$ die Fixgruppe

$$A_L = \big\{a \in A \,;\, \sigma(a) = a \text{ für alle } \sigma \in \operatorname{Gal}(K_s/L)\big\}$$

zuordnen. Ist L galoissch über K oder, äquivalent dazu, $\operatorname{Gal}(K_s/L)$ ein Normalteiler in G, so sieht man leicht, dass sich die G-Aktion auf A zu einer G-Aktion auf A_L beschränkt. Wir erhalten damit eine Aktion von $G/\operatorname{Gal}(K_s/L)$ auf A_L, wobei wir diesen Quotienten gemäß 4.1/7 mit $\operatorname{Gal}(L/K)$ identifizieren dürfen. Für eine Galois-Erweiterung L/K erhält man daher eine Aktion der zugehörigen Galois-Gruppe $\operatorname{Gal}(L/K)$ auf A_L, so dass insbesondere die Kohomologiegruppe $H^1(\operatorname{Gal}(L/K), A_L)$ wie in Abschnitt 4.8 erklärt werden kann. Als essentielle Grundlage jeglicher Kummer-Theorie zu einem gegebenen Exponent n verlangt man die Gültigkeit der kohomologischen Version von Hilberts Satz 90, etwa in folgender Form:

(**Hilbert 90**) *Es sei L/K eine zyklische Galoiserweiterung von einem Grad, der n teilt. Dann gilt $H^1(\operatorname{Gal}(L/K), A_L) = 0$.*

Natürlich ist diese Aussage nicht automatisch erfüllt, sie dient sozusagen als Axiom, auf dem die Kummer-Theorie basiert.

Umgekehrt zum obigen Vorgehen können wir von einer Teilmenge $\Delta \subset A$ ausgehen und die Gruppe

$$G\big(A/\Delta\big) = \big\{\sigma \in G\,;\, \sigma(a) = a \text{ für alle } a \in \Delta\big\}$$

betrachten. Diese ist wegen $G(A/\Delta) = \bigcap_{a\in\Delta} G(A/a)$ abgeschlossen in G, da alle Gruppen $G(A/a)$ aufgrund der Stetigkeit von A als G-Modul offen, also auch abgeschlossen in G sind. Folglich ist $G(A/\Delta)$ zu interpretieren als absolute Galois-Gruppe eines wohlbestimmten Zwischenkörpers $K(\Delta)$ zu K_s/K, nämlich von

$$K(\Delta) = K_s^{G(A/\Delta)} = \big\{\alpha \in K_s\,;\, \sigma(\alpha) = \alpha \text{ für alle } \sigma \in G(A/\Delta)\big\}.$$

Die Kummer-Theorie zu einem gegebenen Exponenten n beruht weiter auf der speziellen Wahl eines surjektiven G-Homomorphismus $\wp\colon A \longrightarrow A$, dessen Kern, im Folgenden mit μ_n bezeichnet, eine zyklische Untergruppe der Ordnung n mit $\mu_n \subset A_K$ ist. Dabei verlangt man von einem G-Homomorphismus, dass er verträglich mit der G-Aktion ist, also $\sigma(\wp(a)) = \wp(\sigma(a))$ für $\sigma \in G$ und $a \in A$ erfüllt.

Die in Abschnitt 4.9 behandelte multiplikative Kummer-Theorie ordnet sich auf natürliche Weise in den Rahmen der hier vorgestellten allgemeinen Kummer-Theorie ein: Man betrachte die multiplikative Gruppe $A = K_s^*$ mit der natürlichen Aktion der Galois-Gruppe G und mit $\wp\colon A \longrightarrow A$, $a \longmapsto a^n$, als G-Homomorphismus, wobei man $\operatorname{char} K \nmid n$ annehme. Diese Voraussetzung bewirkt, dass $\mu_n = \ker \wp$ als Gruppe U_n der n-ten Einheitswurzeln zyklisch von der Ordnung n ist. Mit den oben eingeführten Bezeichnungen gilt dann $A_L = L^*$ für Zwischenkörper L zu K_s/K sowie $K(\wp^{-1}(C)) = K(C^{1/n})$ für $C \subset K^*$, wobei wir in Abschnitt 4.9 $U_n \subset K^*$, also $\mu_n \subset A_K$ vorausgesetzt hatten. In 4.9/3 ergab sich dann eine Charakterisierung abelscher Erweiterungen mit Exponenten, die n teilen, im Stile des Hauptsatzes der Galois-Theorie, und zwar mittels der Untergruppen $C \subset A_K$, die $\wp(A_K)$ enthalten. Der Beweis erforderte Hilberts Satz 90 in der Version 4.8/2.

Wir wollen nun zeigen, dass sich die Resultate 4.9/1 und 4.9/3 ohne Schwierigkeiten auf die Situation der allgemeinen Kummer-Theorie übertragen lassen. Man betrachte hierzu eine Teilmenge $C \subset A_K$, sowie die Untergruppe $G(A/\wp^{-1}(C)) \subset G$ und den zugehörigen Zwischenkörper

$K(\wp^{-1}(C))$ von K_s/K. Die Gruppenverknüpfung auf A werde additiv geschrieben. Da für $\sigma \in G$ und $a \in \wp^{-1}(C)$ die Gleichungen

$$\wp \circ \sigma(a) = \sigma \circ \wp(a) = \wp(a) \qquad \text{bzw.} \qquad \sigma(a) - a \in \ker \wp = \mu_n$$

bestehen, schränkt sich jeder Automorphismus $\sigma \in G$ zu einer Bijektion $\wp^{-1}(C) \longrightarrow \wp^{-1}(C)$ ein, und man erkennt, dass $G(A/\wp^{-1}(C))$ als Kern dieser Einschränkungsabbildung ein Normalteiler in G ist. Gemäß 4.2/3 bzw. 4.1/7 ist dann $K(\wp^{-1}(C))/K$ eine Galois-Erweiterung, sogar eine abelsche Erweiterung, wie wir weiter unten sehen werden. Sei G_C die zugehörige Galois-Gruppe, wobei sich diese nach 4.1/7 mit dem Quotienten $G/G(A/\wp^{-1}(C))$ identifizieren lässt.

Für $c \in C$ und $a \in \wp^{-1}(c)$ hängt die Differenz $\sigma(a) - a \in \mu_n$ im Allgemeinen von c ab, nicht aber von der Wahl eines speziellen Urbilds $a \in \wp^{-1}(c)$, denn für ein weiteres Element $a' \in \wp^{-1}(c)$, etwa $a' = a + i$ mit $i \in \ker \wp = \mu_n$, gilt

$$\sigma(a') - a' = \big(\sigma(a) + \sigma(i)\big) - (a + i) = \sigma(a) - a.$$

Daher ist die Abbildung

$$\langle \cdot, \cdot \rangle \colon G_C \times C \longrightarrow \mu_n, \qquad (\sigma, c) \longmapsto \sigma(a) - a \qquad \text{mit } a \in \wp^{-1}(c),$$

wohldefiniert, und wir erhalten ähnlich wie in Abschnitt 4.9 eine in beiden Variablen homomorphe Paarung

$$\langle \cdot, \cdot \rangle \colon G_C \times C/\wp(A_K) \longrightarrow \mu_n, \quad (\sigma, \overline{c}) \longmapsto \sigma(a) - a \quad \text{mit } a \in \wp^{-1}(c),$$

wenn wir uns auf Untergruppen $C \subset A_K$ mit $\wp(A_K) \subset C$ beschränken.

Theorem 1. *Es sei G die absolute Galois-Gruppe eines Körpers K. Weiter betrachte man einen stetigen G-Modul A mit einem surjektiven G-Homomorphismus $\wp \colon A \longrightarrow A$, dessen Kern μ_n eine endliche zyklische Untergruppe der Ordnung n von A_K sei. Für zyklische Galois-Erweiterungen L/K, deren Grad n teilt, habe man $H^1(\mathrm{Gal}(L/K), A_L) = 0$. Dann gilt*:

(i) *Die Abbildungen*

$$\left\{ \begin{array}{c} \text{Untergruppen } C \subset A_K \\ \text{mit } \wp(A_K) \subset C \end{array} \right\} \underset{\Psi}{\overset{\Phi}{\rightleftarrows}} \left\{ \begin{array}{c} \text{abelsche Erweiterungen } L/K \\ \text{mit Exponenten, die } n \text{ teilen} \end{array} \right\}$$

$$\begin{aligned} C &\longmapsto K\big(\wp^{-1}(C)\big), \\ \wp(A_L) \cap A_K &\longmapsto L, \end{aligned}$$

sind inklusionserhaltend, bijektiv und zueinander invers, wobei wir abelsche Erweiterungen von K stets als Teilkörper von K_s auffassen.

(ii) *Für Untergruppen $C \subset A_K$ mit $\wp(A_K) \subset C$ ist die bihomomorphe Abbildung*

$$\langle \cdot, \cdot \rangle \colon G_C \times C/\wp(A_K) \longrightarrow \mu_n, \quad (\sigma, \overline{c}) \longmapsto \sigma(a) - a \quad \text{mit } a \in \wp^{-1}(c),$$

nicht ausgeartet, induziert also Monomorphismen

$$\begin{aligned} \varphi_1 \colon \quad & G_C \longrightarrow \mathrm{Hom}\big(C/\wp(A_K), \mu_n\big), & \sigma &\longmapsto \langle \sigma, \cdot \rangle, \\ \varphi_2 \colon \quad & C/\wp(A_K) \longrightarrow \mathrm{Hom}\big(G_C, \mu_n\big), & \overline{c} &\longmapsto \langle \cdot, \overline{c} \rangle. \end{aligned}$$

Genauer, φ_1 ist ein Isomorphismus, und es induziert φ_2 einen Isomorphismus $C/\wp(A_K) \xrightarrow{\sim} \mathrm{Hom}_{\mathrm{stet}}(G_C, \mu_n)$ auf die Gruppe aller stetigen Homomorphismen $G_C \longrightarrow \mu_n$.

(iii) *Es ist die Erweiterung $K(\wp^{-1}(C))/K$ genau dann endlich, wenn der Index $(C : \wp(A_K))$ endlich ist. Im Falle der Endlichkeit ist neben φ_1 auch φ_2 in* (ii) *ein Isomorphismus. Sodann folgt $[K(\wp^{-1}(C)) : K] = (C : \wp(A_K))$, und die Galois-Gruppe $G_C = \mathrm{Gal}(K(\wp^{-1}(C))/K)$ ist gemäß* 4.9/2 *isomorph zu $C/\wp(A_K)$.*

Beweis. Ähnlich wie beim Beweis zu 4.9/1 beginnen wir mit der Injektivität von φ_1 und φ_2. Sei also $\sigma \in G_C$ ein Element mit $\langle \sigma, \overline{c} \rangle = 0$ für alle $c \in C$. Es folgt dann $\sigma(a) = a$ für alle $a \in \wp^{-1}(C)$, bzw. wenn wir einen Repräsentanten $\sigma' \in G$ zu σ wählen, $\sigma'(a) = a$ für alle $a \in \wp^{-1}(C)$. Dies bedeutet aber $\sigma' \in G(A/\wp^{-1}(C))$. Somit ist σ trivial und φ_1 injektiv. Sei andererseits $c \in C$ mit $\langle \sigma, \overline{c} \rangle = 0$ für alle $\sigma \in G_C$, d. h. mit $\sigma(a) - a = 0$ für alle $\sigma \in G_C$ und für Urbilder $a \in \wp^{-1}(c)$. Jedes solche a ist dann invariant unter G_C bzw. G, und es ergibt sich $a \in A_K$ bzw. $c = \wp(a) \in \wp(A_K)$. Folglich ist φ_2 injektiv. Aus der Injektivität von φ_1 schließt man insbesondere, dass für eine Untergruppe $C \subset A_K$ mit $C \supset \wp(A_K)$ die Erweiterung $K(\wp^{-1}(C))/K$ abelsch von einem Exponenten ist, der n teilt. Die Abbildung Φ in (i) ist daher wohldefiniert.

Als nächsten Schritt hat man die Aussagen in (iii) zu beweisen. Da die Exponenten von G_C und $C/\wp(A_K)$ aufgrund der Injektivität von φ_1 und φ_2 jeweils n teilen, kann man dabei wortwörtlich wie im Beweis zu 4.9/1 (iii) vorgehen. Um weiter aus (iii) die in (ii) behaupteten Isomorphieeigenschaften für φ_1 und φ_2 zu gewinnen, betrachtet man das System $(C_i)_{i \in I}$ aller Untergruppen in C, die von endlichem Index über $\wp(A_K)$ sind. Es gilt

$$C = \sum_{i\in I} C_i, \qquad G\big(A/\wp^{-1}(C)\big) = \bigcap_{i\in I} G\big(A/\wp^{-1}(C_i)\big)$$

und folglich

$$G\Big(K_s/K\big(\wp^{-1}(C)\big)\Big) = \bigcap_{i\in I} G\Big(K_s/K\big(\wp^{-1}(C_i)\big)\Big),$$

so dass wir $K(\wp^{-1}(C))$ als Kompositum der Körper $K(\wp^{-1}(C_i))$ erkennen. Da das System $(C_i)_{i\in I}$ gerichtet ist, es also zu $i, j \in I$ stets einen Index $k \in I$ mit $C_i, C_j \subset C_k$ gibt, haben wir sogar $K(\wp^{-1}(C)) = \bigcup_{i\in I} K(\wp^{-1}(C_i))$. Unter Verwendung dieser Eigenschaft überträgt sich nun die weitere Argumentation aus dem Beweis zu 4.9/1 (ii) ohne Probleme, und es folgen die in (ii) behaupteten Isomorphieeigenschaften von φ_1 und φ_2.

Auch beim Beweis von Aussage (i) orientieren wir uns an dem entsprechenden Vorbild in Abschnitt 4.9, d. h. am Beweis zu 4.9/3. Wir beginnen mit der Gleichung $\Psi \circ \Phi = \mathrm{id}$ und betrachten eine Untergruppe $C \subset A_K$ mit $C \supset \wp(A_K)$. Man setze $L = K(\wp^{-1}(C))$. Zu zeigen ist, dass $C' = \wp(A_L) \cap A_K$ mit C übereinstimmt. Nach Definition ist $A_L \subset A$ die Fixgruppe zu $G(A/\wp^{-1}(C))$, so dass $\wp^{-1}(C) \subset A_L$ bzw. $C \subset \wp(A_L) \cap A_K = C'$ folgt. Außerdem gilt $G(A/A_L) = G(A/\wp^{-1}(C))$ und somit

$$L = K\big(\wp^{-1}(C)\big) \subset K\big(\wp^{-1}(C')\big) \subset K(A_L) = L,$$

insbesondere also $L = K(\wp^{-1}(C)) = K(\wp^{-1}(C'))$. Ist nun C von endlichem Index über $\wp(A_K)$, so erhält man unmittelbar $C = C'$ aus (iii). Ansonsten betrachten wir wieder das gerichtete System $(C_i)_{i\in I}$ aller Untergruppen in C, die von endlichem Index über $\wp(A_K)$ sind. Dann ist, wie wir gesehen haben, auch das System aller Körper $L_i = K(\wp^{-1}(C_i))$ gerichtet, und es gilt $L = \bigcup_{i\in I} L_i$. Im Übrigen behaupten wir:

$$(*) \qquad A_L = \bigcup_{i\in I} A_{L_i}.$$

Natürlich gilt $A_L \supset \bigcup_{i\in I} A_{L_i}$. Umgekehrt betrachte man ein Element $a \in A_L$ sowie die zugehörige Untergruppe $G(A/a) \subset G$, welche a festlässt. Diese ist offen in G, da die Aktion von G auf A stetig ist. Gemäß 4.2/5 korrespondiert $G(A/a)$ zu einem Zwischenkörper E von K_s/K, der endlich über K ist. Es gilt sogar $E \subset L$, denn man hat $G(A/a) \supset G(A/A_L)$, wobei die Gruppe

$G(A/A_L)$ mit $G(A/\wp^{-1}(C))$ übereinstimmt. Da das System $(L_i)_{i\in I}$ gerichtet ist, existiert somit ein Index $j \in I$ mit $E \subset L_j$. Insbesondere folgt

$$a \in A_E \subset A_{L_j} \subset \bigcup_{i\in I} A_{L_i}$$

und damit die behauptete Gleichung $(*)$.

Im Übrigen gilt aber $\wp(A_{L_i}) \cap A_K = C_i$ für alle i, da die Indizes $(C_i : \wp(A_K))$ endlich sind. Mit $(*)$ folgt daraus $\wp(A_L) \cap A_K = C$, also $\Psi \circ \Phi = \mathrm{id}$.

Um zu sehen, dass auch $\Phi \circ \Psi = \mathrm{id}$ gilt, betrachten wir eine abelsche Erweiterung L/K mit einem Exponenten, der n teilt. Für $C = \wp(A_L) \cap A_K$ gilt dann $\wp^{-1}(C) \subset A_L$. Es wird also $\wp^{-1}(C)$ durch $\mathrm{Gal}(K_s/L)$ festgelassen, und man hat folglich $K(\wp^{-1}(C)) \subset L$. Zu zeigen ist, dass hier sogar Gleichheit besteht. Um dies zu erreichen, schreiben wir L als Kompositum endlicher und dann notwendig abelscher Galoiserweiterungen L'/K. Jede dieser Erweiterungen L'/K lässt sich wiederum als Kompositum endlich vieler zyklischer Erweiterungen schreiben. Hierzu hat man lediglich in der Galois-Gruppe $H = \mathrm{Gal}(L'/K)$ Untergruppen H_j zu finden, derart dass H/H_j jeweils zyklisch ist und $\bigcap_j H_j = \{1\}$ gilt; dies ist aber unter Benutzung des Hauptsatzes über endlich erzeugte abelsche Gruppen 2.9/9 ohne Probleme möglich. Somit ist L Kompositum einer Familie $(L_i)_{i\in I}$ endlicher *zyklischer* Erweiterungen, und es genügt offenbar, $L_i \subset K(\wp^{-1}(C_i))$ mit $C_i = \wp(A_{L_i}) \cap A_K$ zu zeigen. Mit anderen Worten, wir dürfen L/K als endliche zyklische Erweiterung mit einem Exponenten annehmen, der n teilt.

Sei also L/K eine solche Erweiterung. Für $C = \wp(A_L) \cap A_K$ betrachten wir dann den Epimorphismus

$$q\colon \mathrm{Gal}\big(L/K\big) \longrightarrow G_C, \qquad \sigma \longmapsto \sigma|_{K(\wp^{-1}(C))},$$

sowie den zugehörigen Homomorphismus

$$q^*\colon \mathrm{Hom}\big(G_C, \mu_n\big) \longrightarrow \mathrm{Hom}\big(\mathrm{Gal}(L/K), \mu_n\big), \qquad f \longmapsto f \circ q.$$

Es genügt zu zeigen, dass q^* ein Isomorphismus ist, denn dann ergibt sich mit 4.9/2 die Beziehung $\mathrm{ord}\,\mathrm{Gal}(L/K) = \mathrm{ord}\, G_C$ und aus Gradgründen also $L = K(\wp^{-1}(C))$.

Zunächst ist q^* injektiv, da q surjektiv ist. Um zu sehen, dass q^* auch surjektiv ist, betrachte man ein Element des Bildbereichs, also einen Homomorphismus $g\colon \mathrm{Gal}(L/K) \longrightarrow \mu_n$. Es ist g wegen

$$g(\sigma \circ \sigma') = g(\sigma) + g(\sigma') = \sigma \circ g(\sigma') + g(\sigma), \qquad \sigma, \sigma' \in \mathrm{Gal}\big(L/K\big),$$

ein 1-Kozyklus bezüglich der Aktion von $\mathrm{Gal}(L/K)$ auf A_L, also nach unserer Voraussetzung über $H^1(\mathrm{Gal}(L/K), A_L)$ auch ein 1-Korand. Daher existiert ein Element $a \in A_L$ mit $g(\sigma) = a - \sigma(a)$ für alle $\sigma \in \mathrm{Gal}(L/K)$. Benutzen wir nun $\ker \wp = \mu_n$, so folgt $\sigma \circ \wp(a) = \wp \circ \sigma(a) = \wp(a)$ für $\sigma \in \mathrm{Gal}(L/K)$ und damit $\wp(a) \in \wp(A_L) \cap A_K = C$. Offenbar gilt dann $g = f \circ q = q^*(f)$ mit

$$f\colon G_C \longrightarrow \mu_n, \qquad \sigma \longmapsto a - \sigma(a),$$

und man sieht, dass q^* surjektiv ist. □

Als konkrete Situation, in der das Theorem anwendbar ist, haben wir in Abschnitt 4.9 die Kummer-Theorie zu einem Exponenten n mit $\mathrm{char}\, K \nmid n$ studiert. Wir setzen von nun an $p = \mathrm{char}\, K > 0$ voraus und wollen im Weiteren auf die Kummer-Theorie zu Exponenten der Form $n = p^r$ eingehen. Der Fall $n = p$ (Artin-Schreier-Theorie) ist recht simpel. Wir betrachten die additive Gruppe $A = K_s$ mit der kanonischen Aktion von G als G-Modul sowie mit

$$\wp\colon A \longrightarrow A, \qquad a \longmapsto a^p - a,$$

als G-Homomorphismus. Es ist dann $\mu_p = \ker \wp$ der Primkörper in $A_K = K$, also eine zyklische Untergruppe der Ordnung p in A_K wie gefordert. Um die Anwendbarkeit von Theorem 1 zu garantieren, ist lediglich Hilberts Satz 90 bereitzustellen. Wir werden dies weiter unten mit Satz 11 in allgemeinerem Rahmen tun.

Witt-Vektoren. — Die Kummer-Theorie für beliebige Exponenten der Form $n = p^r$, $r \geq 1$, ist aufwendiger und benötigt den von E. Witt [19] eingeführten Kalkül der *Witt-Vektoren*, den wir im Folgenden behandeln wollen. Die Witt-Vektoren zu einer Primzahl p und mit Koeffizienten aus einem Ring R bilden einen Ring $W(R)$, den sogenannten *Witt-Ring* zu R, der im Folgenden zu definieren ist. Dabei setzt man $W(R) = R^{\mathbb{N}}$, um $W(R)$ als *Menge* zu charakterisieren. Summe und Produkt von Elementen $x, y \in W(R)$ werden durch Ausdrücke der Form

$$x + y = \big(S_n(x, y)\big)_{n\in\mathbb{N}}, \qquad x \cdot y = \big(P_n(x, y)\big)_{n\in\mathbb{N}}$$

erklärt, wobei $S_n(x,y), P_n(x,y)$ für $n \in \mathbb{N}$ Polynome in $x_0,\dots,x_n$ und $y_0,\dots,y_n$ mit Koeffizienten aus $\mathbb{Z}$ sind,[8] also Polynome in den ersten $n+1$ Komponenten von x bzw. y. Wenn $p = p\cdot 1$ in R invertierbar ist, werden wir sehen, dass $W(R)$ als Ring isomorph zu $R^{\mathbb{N}}$ mit komponentenweiser Addition und Multiplikation ist.

Um nun die Polynome $S_n, P_n \in \mathbb{Z}[X_0,\dots,X_n,Y_0,\dots,Y_n]$ für alle $n\in\mathbb{N}$ zu erklären, betrachten wir die sogenannten *Witt-Polynome*

$$W_n = \sum_{i=0}^{n} p^i X_i^{p^{n-i}} = X_0^{p^n} + pX_1^{p^{n-1}} + \ldots + p^n X_n \in \mathbb{Z}[X_0,\dots,X_n],$$

die als Schlüssel zur Theorie der Witt-Vektoren dienen. Für diese Polynome gelten die Rekursionsformeln

$$(*) \qquad W_n = W_{n-1}(X_0^p,\dots,X_{n-1}^p) + p^n X_n, \qquad n>0,$$

und man sieht per Induktion, dass sich X_n jeweils als Polynom in $W_0,\dots,W_n$ mit Koeffizienten in $\mathbb{Z}[\frac{1}{p}]$ schreiben lässt, etwa

$$X_0 = W_0, \qquad X_1 = p^{-1}W_1 - p^{-1}W_0^p, \qquad \dots$$

Lemma 2. *Der durch Einsetzen von $W_0,\dots,W_n$ erklärte Endomorphismus*

$$\begin{aligned}\omega_n\colon \mathbb{Z}[\tfrac{1}{p}][X_0,\dots,X_n] &\longrightarrow \mathbb{Z}[\tfrac{1}{p}][X_0,\dots,X_n],\\ f(X_0,\dots,X_n) &\longmapsto f(W_0,\dots,W_n),\end{aligned}$$

ist bijektiv. Insbesondere geben die Abbildungen ω_n, $n\in\mathbb{N}$, Anlass zu einem Automorphismus

$$\begin{aligned}\omega\colon \mathbb{Z}[\tfrac{1}{p}][X_0,X_1,\dots] &\longrightarrow \mathbb{Z}[\tfrac{1}{p}][X_0,X_1,\dots],\\ f(X_0,X_1,\dots) &\longmapsto f(W_0,W_1,\dots).\end{aligned}$$

Beweis. In der Tat, ω_n ist surjektiv, da sich die $X_0,\dots,X_n$ als Polynome in den $W_0,\dots,W_n$ schreiben lassen. Dann ist ω_n aus allgemeinen Gründen aber auch injektiv; man erweitere etwa die Koeffizienten von $\mathbb{Z}[\frac{1}{p}]$ zu $\mathbb{Q}$ und wende 7.1/9 an.

[8] Die Multiplikation von Elementen aus $\mathbb{Z}$ mit Elementen aus R sei wie üblich erklärt, etwa unter Zuhilfenahme des kanonischen Homomorphismus $\mathbb{Z}\longrightarrow R$.

Wir wollen zusätzlich noch auf direkte Weise zeigen, dass ω_n injektiv ist, und gehen hierbei mit Induktion nach n vor. Der Fall $n = 0$ ist wegen $W_0 = X_0$ trivial. Sei also $n > 0$ und sei

$$f = \sum_{i=0}^{r} f_i \cdot X_n^i, \qquad f_i \in \mathbb{Z}[\tfrac{1}{p}][X_0, \ldots, X_{n-1}],$$

ein nicht-triviales Polynom in $X_0, \ldots, X_n$ mit Koeffizienten in $\mathbb{Z}[\frac{1}{p}]$, etwa mit $f_r \neq 0$. Dann gilt

$$\omega_n(f) = \sum_{i=0}^{r} f_i(W_0, \ldots, W_{n-1}) \cdot W_n^i,$$

wobei alle $f_i(W_0, \ldots, W_{n-1})$ Polynome in $X_0, \ldots, X_{n-1}$ sind und wobei $f_r(W_0, \ldots, W_{n-1})$ nach Induktionsvoraussetzung nicht verschwindet. Wir denken uns nun $\omega_n(f)$ als Polynom in X_n mit Koeffizienten aus $\mathbb{Z}[\frac{1}{p}][X_0, \ldots, X_{n-1}]$ geschrieben. Da $p^n X_n$ der einzige Term von W_n ist, der die Variable X_n in nicht-trivialer Potenz enthält, beginnt $\omega_n(f)$ mit dem Produkt $p^{nr} f_r(W_0, \ldots, W_{n-1}) \cdot X_n^r$ als höchstem Term, und es folgt $\omega_n(f) \neq 0$, d. h. ω_n ist injektiv. □

Wir werden im Folgenden die Polynome W_n häufig auch als Elemente des Polynomrings $\mathbb{Z}[X_0, X_1, \ldots]$ auffassen, so dass für Punkte $x \in R^{\mathbb{N}}$ mit Komponenten aus einem beliebigen Ring R die Werte $W_n(x)$ Sinn machen.

Lemma 3. *Es sei p in R invertierbar. Dann ist die Abbildung*

$$w\colon W(R) = R^{\mathbb{N}} \longrightarrow R^{\mathbb{N}}, \qquad x \longmapsto \big(W_n(x)\big)_{n\in\mathbb{N}},$$

bijektiv.

Beweis. In der Situation von Lemma 2 sind die Umkehrabbildungen ω_n^{-1} und ω^{-1} ebenso wie ω_n und ω aufgrund der universellen Eigenschaft von Polynomringen 2.5/5 bzw. 2.5/1 Einsetzungshomomorphismen. Es existieren daher Polynome $\widetilde{W}_n \in \mathbb{Z}[\frac{1}{p}][X_0, \ldots, X_n]$ mit

$$W_n(\widetilde{W}_0, \ldots, \widetilde{W}_n) = X_n, \qquad \widetilde{W}_n(W_0, \ldots, W_n) = X_n$$

für $n \in \mathbb{N}$. Da p in R invertierbar ist, dehnt sich der kanonische Homomorphismus $\mathbb{Z} \longrightarrow R$ (auf eindeutige Weise) zu einem Homomorphismus

$\mathbb{Z}[\frac{1}{p}] \longrightarrow R$ aus, und es bleiben die vorstehenden Relationen bestehen, wenn man $\mathbb{Z}[\frac{1}{p}]$ durch R als Koeffizientenring ersetzt. Hieraus folgt dann unmittelbar, dass die geforderte Abbildung w eine Umkehrabbildung besitzt und also bijektiv ist.

Alternativ kann man auch

$$R^{\mathbb{N}} \longrightarrow \mathrm{Hom}\Big(\mathbb{Z}[\tfrac{1}{p}][X_0, X_1, \dots], R\Big), \qquad x \longmapsto \big(f \longmapsto f(x)\big),$$

als Identifizierung ansehen und $w\colon R^{\mathbb{N}} \longrightarrow R^{\mathbb{N}}$ als Abbildung

$$\begin{aligned}\mathrm{Hom}\Big(\mathbb{Z}[\tfrac{1}{p}][X_0, X_1, \dots], R\Big) &\longrightarrow \mathrm{Hom}\Big(\mathbb{Z}[\tfrac{1}{p}][X_0, X_1, \dots], R\Big),\\ \varphi &\longmapsto \varphi \circ \omega,\end{aligned}$$

interpretieren, welche durch den Isomorphismus ω aus Lemma 2 induziert wird; $\mathrm{Hom}(C, R)$ bezeichnet dabei für Ringe C und R die Menge aller Ringhomomorphismen $C \longrightarrow R$. □

Ist also R ein Ring, in dem p invertierbar ist, so können wir, ausgehend von $R^{\mathbb{N}}$ als Ring mit komponentenweiser Addition "$+_c$" und komponentenweiser Multiplikation "$\cdot_c$", Verknüpfungen "+" und "$\cdot$" auf $W(R)$ durch die Formeln

$$x + y = w^{-1}\big(w(x) +_c w(y)\big), \qquad x \cdot y = w^{-1}\big(w(x) \cdot_c w(y)\big),$$

erklären. Es ist unmittelbar klar, dass $W(R)$ mit diesen Verknüpfungen ein Ring ist. In der Tat, die Verknüpfungen auf $W(R)$ sind gerade so definiert, dass die Abbildung $w\colon W(R) \longrightarrow R^{\mathbb{N}}$ ein Isomorphismus von Ringen wird.

Man kann sich nun leicht davon überzeugen, dass sich die n-ten Komponenten einer Summe $x + y$ oder eines Produkts $x \cdot y$ von Elementen $x, y \in W(R)$ in polynomialer Weise aus den i-ten Komponenten von x und y mit $i \leq n$ berechnen lassen. w ist nämlich durch polynomiale Ausdrücke dieser Art mit Koeffizienten in $\mathbb{Z}$ gegeben, w^{-1} durch ebensolche mit Koeffizienten in $\mathbb{Z}[\frac{1}{p}]$, so dass man insgesamt Koeffizienten in $\mathbb{Z}[\frac{1}{p}]$ benötigt. Allerdings werden wir sogleich sehen, dass bereits Koeffizienten aus $\mathbb{Z}$ genügen, um die Verknüpfungen "+" und "$\cdot$" auf $W(R)$ zu charakterisieren. Dies wird uns in die Lage versetzen, den Witt-Ring $W(R)$ auch für solche Ringe R zu definieren, in denen p nicht invertierbar ist. Wir beginnen mit einer Hilfsaussage über Witt-Polynome.

Lemma 4. *Es sei R ein Ring, in dem $p = p \cdot 1$ kein Nullteiler sei. Für Elemente $a_0, \ldots, a_n, b_0, \ldots, b_n \in R$ und $r \in \mathbb{N} - \{0\}$ ist dann äquivalent*:

(i) $a_i \equiv b_i \bmod (p^r)$ *für* $i = 0, \ldots, n$.

(ii) $W_i(a_0, \ldots, a_i) \equiv W_i(b_0, \ldots, b_i) \bmod (p^{r+i})$ *für* $i = 0, \ldots, n$.

Beweis. Wir gehen mit Induktion nach n vor, wobei der Fall $n = 0$ klar ist. Sei also $n > 0$. Nach Induktionsvoraussetzung sind die Bedingungen (i) und (ii) äquivalent für $n - 1$ anstelle von n. Ist daher (i) oder (ii) erfüllt, so dürfen wir in jedem Falle beide Bedingungen für $i = 0, \ldots, n-1$ als gegeben annehmen. Potenzieren der Kongruenzen in (i) mit p ergibt

$$a_i^p \equiv b_i^p \mod (p^{r+1}), \qquad i = 0, \ldots, n-1,$$

da $r \geq 1$ gilt und p die Binomialkoeffizienten $\binom{p}{1}, \ldots, \binom{p}{p-1}$ teilt. Nach Induktionsvoraussetzung folgt hieraus insbesondere

$$W_{n-1}(a_0^p, \ldots, a_{n-1}^p) \equiv W_{n-1}(b_0^p, \ldots, b_{n-1}^p) \mod (p^{r+n})$$

und unter Benutzung der Rekursionsformeln $(*)$

$$W_n(a_0, \ldots, a_n) - W_n(b_0, \ldots, b_n) \equiv p^n a_n - p^n b_n \mod (p^{r+n}).$$

Folglich ist die Kongruenz

$$W_n(a_0, \ldots, a_n) \equiv W_n(b_0, \ldots, b_n) \mod (p^{r+n})$$

äquivalent zu $p^n a_n \equiv p^n b_n \bmod (p^{r+n})$, also zu $a_n \equiv b_n \bmod (p^r)$, da p kein Nullteiler in R ist. □

Lemma 5. *Es sei $\Phi \in \mathbb{Z}[\zeta, \xi]$ ein Polynom in den Variablen ζ und ξ. Dann existieren eindeutig Polynome $\varphi_n \in \mathbb{Z}[X_0, \ldots, X_n, Y_0, \ldots, Y_n]$, $n \in \mathbb{N}$, mit*

$$W_n(\varphi_0, \ldots, \varphi_n) = \Phi\big(W_n(X_0, \ldots, X_n), W_n(Y_0, \ldots, Y_n)\big).$$

für alle n.

Beweis. Wir setzen $\mathfrak{X} = (X_0, X_1, \ldots)$ sowie $\mathfrak{Y} = (Y_0, Y_1, \ldots)$ und betrachten das kommutative Diagramm

$$\begin{array}{ccc} \mathbb{Z}[\frac{1}{p}][\mathfrak{X}] & \xrightarrow{\omega} & \mathbb{Z}[\frac{1}{p}][\mathfrak{X}] \\ {\scriptstyle\tau}\downarrow & & \downarrow{\scriptstyle\tau'} \\ \mathbb{Z}[\frac{1}{p}][\mathfrak{X},\mathfrak{Y}] & \xrightarrow{\omega\otimes\omega} & \mathbb{Z}[\frac{1}{p}][\mathfrak{X},\mathfrak{Y}], \end{array}$$

welches durch

$$\begin{aligned} \omega: &\quad X_n \longmapsto W_n, \\ \omega\otimes\omega: &\quad X_n \longmapsto W_n(X_0,\dots,X_n),\ Y_n \longmapsto W_n(Y_0,\dots,Y_n), \\ \tau: &\quad X_n \longmapsto \Phi(X_n,Y_n), \\ \tau': &\quad = (\omega\otimes\omega)\circ\tau\circ\omega^{-1}, \end{aligned}$$

festgelegt ist. Man beachte dabei, dass ω gemäß Lemma 2 ein Isomorphismus ist und damit Gleiches auch für $\omega\otimes\omega$ gilt. Insbesondere ist τ' wohldefiniert und eindeutig durch die Kommutativität des Diagramms bestimmt, also durch die Gleichung $\tau'\circ\omega = (\omega\otimes\omega)\circ\tau$. Setzen wir daher $\varphi_n = \tau'(X_n)$, so sind die φ_n eindeutig bestimmte Polynome aus $\mathbb{Z}[\frac{1}{p}][X_0,\dots,X_n,Y_0,\dots,Y_n]$ mit

$$W_n(\varphi_0,\dots,\varphi_n) = \Phi\big(W_n(X_0,\dots,X_n), W_n(Y_0,\dots,Y_n)\big), \qquad n\in\mathbb{N}.$$

Zum Beweis der Aussage des Lemmas ist daher lediglich noch zu zeigen, dass alle Polynome φ_n Koeffizienten in $\mathbb{Z}$ haben.

Um Letzteres einzusehen, verwenden wir Induktion nach n. Für $n=0$ ergibt sich wegen $W_0 = X_0$ unmittelbar $\varphi_0 = \Phi$, und es besitzt φ_0 somit Koeffizienten in $\mathbb{Z}$. Sei nun $n>0$. Nach Induktionsvoraussetzung dürfen wir annehmen, dass $\varphi_0,\dots,\varphi_{n-1}$ Koeffizienten in $\mathbb{Z}$ haben. Man betrachte dann das Element

$$W_n(\varphi_0,\dots,\varphi_n) = \tau'\circ\omega(X_n) = (\omega\otimes\omega)\circ\tau(X_n),$$

welches aufgrund der Definition von ω und τ ein Polynom in $\mathfrak{X}$ und $\mathfrak{Y}$ mit Koeffizienten in $\mathbb{Z}$ darstellt. Gleiches gilt unter Benutzung der Induktionsvoraussetzung für $W_{n-1}(\varphi_0^p,\dots,\varphi_{n-1}^p)$. Die Rekursionsformel $(*)$ ergibt nun

$$W_n(\varphi_0,\dots,\varphi_n) = W_{n-1}(\varphi_0^p,\dots,\varphi_{n-1}^p) + p^n\varphi_n,$$

und es genügt

$$W_n(\varphi_0,\dots,\varphi_n) \equiv W_{n-1}(\varphi_0^p,\dots,\varphi_{n-1}^p) \mod (p^n)$$

zu zeigen, um einzusehen, dass φ_n Koeffizienten in $\mathbb{Z}$ besitzt.

Für Polynome $\varphi \in \mathbb{Z}[\mathfrak{X},\mathfrak{Y}]$ gilt $\varphi^p \equiv \varphi(\mathfrak{X}^p,\mathfrak{Y}^p) \bmod (p)$, wie man leicht anhand des Reduktionshomomorphismus $\mathbb{Z}[\mathfrak{X},\mathfrak{Y}] \longrightarrow \mathbb{F}_p[\mathfrak{X},\mathfrak{Y}]$ und mittels 3.1/3 nachweist; $\mathfrak{X}^p$ bzw. $\mathfrak{Y}^p$ sei das System aller p-ten Potenzen der Komponenten von $\mathfrak{X}$ bzw. $\mathfrak{Y}$. Insbesondere hat man

$$\varphi_i^p \equiv \varphi_i(\mathfrak{X}^p,\mathfrak{Y}^p) \mod (p), \qquad i = 0,\dots,n-1,$$

woraus mit Lemma 4

$$W_{n-1}(\varphi_0^p,\dots,\varphi_{n-1}^p) \equiv W_{n-1}\big(\varphi_0(\mathfrak{X}^p,\mathfrak{Y}^p),\dots,\varphi_{n-1}(\mathfrak{X}^p,\mathfrak{Y}^p)\big) \bmod (p^n)$$

folgt. Unter Ausnutzung der Kommutativität des obigen Diagramms und der Rekursionsformel $(*)$ ergibt sich dann folgende Kongruenz modulo (p^n):

$$\begin{aligned} W_n(\varphi_0,\dots,\varphi_n) &= \Phi\big(W_n(\mathfrak{X}),W_n(\mathfrak{Y})\big) \\ &\equiv \Phi\big(W_{n-1}(\mathfrak{X}^p),W_{n-1}(\mathfrak{Y}^p)\big) \\ &= W_{n-1}\big(\varphi_0(\mathfrak{X}^p,\mathfrak{Y}^p),\dots,\varphi_{n-1}(\mathfrak{X}^p,\mathfrak{Y}^p)\big) \\ &\equiv W_{n-1}(\varphi_0^p,\dots,\varphi_{n-1}^p) \end{aligned}$$

Es folgt, wie oben erläutert, dass φ_n Koeffizienten in $\mathbb{Z}$ besitzt. □

Wir wenden Lemma 5 speziell auf die Polynome

$$\Phi(\zeta,\xi) = \zeta + \xi \quad \text{bzw.} \quad \Phi(\zeta,\xi) = \zeta \cdot \xi$$

an und erhalten anstelle der φ_n zugehörige Polynome

$$S_n, P_n \in \mathbb{Z}[X_0,\dots,X_n,Y_0,\dots,Y_n], \qquad n \in \mathbb{N};$$

beispielsweise gilt

$$\begin{aligned} S_0 &= X_0 + Y_0, & S_1 &= X_1 + Y_1 + \tfrac{1}{p}\big(X_0^p + Y_0^p - (X_0+Y_0)^p\big), \\ P_0 &= X_0 \cdot Y_0, & P_1 &= X_1 Y_0^p + X_0^p Y_1 + p X_1 Y_1. \end{aligned}$$

Die Polynome S_n, P_n sollen nun für beliebige Ringe R zur Definition der Addition und Multiplikation im zugehörigen Witt-Ring $W(R)$ benutzt werden. Und zwar setzen wir $W(R) = R^{\mathbb{N}}$ im Sinne von Mengen und versehen $W(R)$ mit den Verknüpfungen

$$x + y = \big(S_n(x,y)\big)_{n\in\mathbb{N}}, \quad x \cdot y = \big(P_n(x,y)\big)_{n\in\mathbb{N}}, \quad x, y \in W(R).$$

Aufgrund von Lemma 5 gelten dann für

$$w\colon W(R) \longrightarrow R^{\mathbb{N}}, \qquad x \longmapsto \big(W_n(x)\big)_{n\in\mathbb{N}},$$

die Verträglichkeitsrelationen

$$w(x+y) = w(x) +_c w(y), \quad w(x\cdot y) = w(x) \cdot_c w(y), \quad x, y \in W(R),$$

d. h. w ist ein Ringhomomorphismus, sofern wir gezeigt haben, dass $W(R)$ unter den Verknüpfungen "+" und "·" ein Ring ist. Nun ist aber, wie wir aus Lemma 3 wissen, w bijektiv, falls p in R invertierbar ist. In diesen Fällen gilt daher

$$x + y = w^{-1}\big(w(x) +_c w(y)\big), \quad x \cdot y = w^{-1}\big(w(x) \cdot_c w(y)\big), \quad x, y \in W(R),$$

und wir sehen, wie bereits oben erläutert, dass $W(R)$ dann in der Tat ein Ring unter den Verknüpfungen "+" und "·" ist, $w\colon W(R) \longrightarrow R^{\mathbb{N}}$ also ein Isomorphismus von Ringen ist.

Satz 6. *Es sei R ein beliebiger Ring. Dann ist $W(R)$ unter den aus den Polynomen S_n, P_n gewonnenen Verknüpfungen "+" und "·" ein Ring mit folgenden Eigenschaften*:

(i) $(0,0,\ldots) \in W(R)$ *ist das Nullelement und* $(1,0,0,\ldots) \in W(R)$ *das Einselement.*

(ii) $w\colon W(R) \longrightarrow R^{\mathbb{N}}, x \longmapsto (W_n(x))_{i\in\mathbb{N}}$, *ist ein Ringhomomorphismus, sogar ein Isomorphismus, falls p in R invertierbar ist.*

(iii) *Für jeden Ringhomomorphismus $f\colon R \longrightarrow R'$ ist die induzierte Abbildung*

$$W(f)\colon W(R) \longrightarrow W(R'), \qquad (a_n)_{n\in\mathbb{N}} \longmapsto \big(f(a_n)\big)_{n\in\mathbb{N}},$$

ebenfalls ein Ringhomomorphismus.

Beweis. Sei zunächst p in R invertierbar. Dann ist, wie wir gesehen haben, $W(R)$ ein Ring und $w\colon W(R) \longrightarrow R^{\mathbb{N}}$ ein Isomorphismus von Ringen. Da man offenbar

$$w(0,0,\ldots) = (0,0,\ldots), \qquad w(1,0,0,\ldots) = (1,1,1,\ldots)$$

hat, ist $(0, 0, \ldots)$ das Nullelement und $(1, 0, 0, \ldots)$ das Einselement in $W(R)$.

Wir wollen insbesondere den Fall $R = \mathbb{Z}[\frac{1}{p}][\mathfrak{X}, \mathfrak{Y}, \mathfrak{Z}]$ mit Systemen von Variablen

$$\mathfrak{X} = (X_0, X_1, \ldots), \qquad \mathfrak{Y} = (Y_0, Y_1, \ldots), \qquad \mathfrak{Z} = (Z_0, Z_1, \ldots)$$

betrachten. Dann können $\mathfrak{X}, \mathfrak{Y}, \mathfrak{Z}$ als Elemente von $W(R)$ interpretiert werden, und die Assoziativitäts-Bedingungen

$$(\mathfrak{X} + \mathfrak{Y}) + \mathfrak{Z} = \mathfrak{X} + (\mathfrak{Y} + \mathfrak{Z}), \qquad (\mathfrak{X} \cdot \mathfrak{Y}) \cdot \mathfrak{Z} = \mathfrak{X} \cdot (\mathfrak{Y} \cdot \mathfrak{Z})$$

stellen gewisse Polynom-Identitäten in den S_n bzw. P_n dar, wobei lediglich Koeffizienten aus $\mathbb{Z}$ ins Spiel kommen. Diese Identitäten bestehen daher bereits im Polynomring $\mathbb{Z}[\mathfrak{X}, \mathfrak{Y}, \mathfrak{Z}]$. Mit den weiteren Ringaxiomen kann man entsprechend verfahren, wobei man Lemma 5 mit $\Phi(\zeta, \xi) = -\zeta$ anwendet, um zu sehen, dass die Addition in $W(R)$ eine mittels Koeffizienten aus $\mathbb{Z}$ erklärte Inversenbildung besitzt. Als Konsequenz ergibt sich, dass die betrachteten Verknüpfungen sozusagen in generischer Weise die Axiome einer Ringstruktur erfüllen, zu deren Beschreibung lediglich Koeffizienten aus $\mathbb{Z}$ benötigt werden. Setzt man nun für die Variablen Werte aus einem beliebigen Ring R ein, so behalten die Verknüpfungen "+" und "·" die Eigenschaften einer Ringstruktur, und man erkennt folglich $W(R)$ auch für allgemeine Ringe R wiederum als einen Ring.

Es bleibt noch Behauptung (iii) zu zeigen. Unter Benutzung der universellen Eigenschaft von Polynomringen 2.5/1 können wir $W(R)$ für beliebiges R mit der Menge $\mathrm{Hom}(\mathbb{Z}[\mathfrak{X}], R)$ aller Homomorphismen $\mathbb{Z}[\mathfrak{X}] \longrightarrow R$ identifizieren und entsprechend $W(R) \times W(R)$ mit $\mathrm{Hom}(\mathbb{Z}[\mathfrak{X}, \mathfrak{Y}], R)$. Addition und Multiplikation auf $W(R)$ sind dann zu interpretieren als diejenigen Abbildungen

$$\mathrm{Hom}\big(\mathbb{Z}[\mathfrak{X}, \mathfrak{Y}], R\big) \longrightarrow \mathrm{Hom}\big(\mathbb{Z}[\mathfrak{X}], R\big), \qquad \varphi \longmapsto \varphi \circ g,$$

die durch

$$g \colon \mathbb{Z}[\mathfrak{X}] \longrightarrow \mathbb{Z}[\mathfrak{X}, \mathfrak{Y}], \qquad X_n \longmapsto S_n \text{ bzw. } X_n \longmapsto P_n,$$

induziert werden. Zu einem Ringhomomorphismus $f \colon R \longrightarrow R'$ erhält man dann, sowohl für die Addition wie auch für die Multiplikation, auf kanonische Weise ein kommutatives Diagramm

$$\begin{array}{ccc} \mathrm{Hom}\big(\mathbb{Z}[\mathfrak{X},\mathfrak{Y}],R\big) & \longrightarrow & \mathrm{Hom}\big(\mathbb{Z}[\mathfrak{X}],R\big) \\ \downarrow & & \downarrow \\ \mathrm{Hom}\big(\mathbb{Z}[\mathfrak{X},\mathfrak{Y}],R'\big) & \longrightarrow & \mathrm{Hom}\big(\mathbb{Z}[\mathfrak{X}],R'\big), \end{array}$$

wobei die vertikalen Abbildungen durch Komposition mit f erklärt sind und im Übrigen als Abbildung

$$W(f)\colon W(R) \longrightarrow W(R'), \qquad (a_n)_{n\in\mathbb{N}} \longmapsto \big(f(a_n)\big)_{n\in\mathbb{N}},$$

bzw. deren kartesisches Produkt mit sich selber interpretiert werden können. Die Kommutativität des Diagramms beinhaltet dann die Homomorphieeigenschaft für $W(f)$. □

Man nennt $W(R)$ den *Witt-Ring* zum Ring R und dessen Elemente *Witt-Vektoren* mit Koeffizienten aus R. Für $a \in W(R)$ bezeichnet man $w(a)$ auch als den Vektor der *Neben-* oder *Geisterkomponenten* von a, da das Rechnen mit diesen Komponenten (zumindest im Falle, wo p in R invertierbar ist) die Ringstruktur von $W(R)$ bestimmt, diese Komponenten selbst aber in $W(R)$ nicht direkt in Erscheinung treten.

Wir wollen noch einige einfache Regeln für das Rechnen im Witt-Ring $W(R)$ anführen und betrachten dazu wiederum den Homomorphismus $w\colon W(R) \longrightarrow R^{\mathbb{N}}$. Zunächst gilt offenbar

$$w\big((\alpha\cdot\beta,0,0,\ldots)\big) = w\big((\alpha,0,0,\ldots)\big)\cdot w\big((\beta,0,0,\ldots)\big)$$

für Elemente $\alpha,\beta \in R$, denn man hat $W_n(\gamma,0,0,\ldots) = \gamma^{p^n}$ für $\gamma \in R$. Hieraus folgt die Regel

$$(\alpha,0,0,\ldots)\cdot(\beta,0,0,\ldots) = (\alpha\cdot\beta,0,0,\ldots)$$

für die Multiplikation in $W(R)$, zunächst für den Fall, dass p in R invertierbar ist, und dann mit einer Argumentation wie im Beweis zu Satz 6 auch für beliebige Ringe R. In gleicher Weise beweist man die Zerlegungsregel

$$(a_0,a_1,\ldots) = (a_0,\ldots,a_n,0,0,\ldots) + (0,\ldots,0,a_{n+1},a_{n+2},\ldots)$$

für die Addition in $W(R)$. Von besonderem Interesse ist im Weiteren die Multiplikation mit p in $W(R)$, insbesondere für den Fall, dass $p\cdot 1 = 0$ in R gilt. Wählt man etwa $R = \mathbb{F}_p$ und betrachtet ein Element $a \in W(\mathbb{F}_p)$, so erhält man $w(p\cdot a) = p\cdot w(a) = 0$, obwohl die p-Multiplikation in $W(\mathbb{F}_p)$ nicht trivial ist, wie wir sogleich sehen werden. Insbesondere folgt hieraus,

dass der Homomorphismus $w\colon W(\mathbb{F}_p) \longrightarrow \mathbb{F}_p^{\mathbb{N}}$ nicht injektiv sein kann. Mit anderen Worten, Elemente aus $W(\mathbb{F}_p)$ sind nicht eindeutig durch ihre Geisterkomponenten festgelegt.

Zur Behandlung der p-Multiplikation in $W(R)$ führen wir den sogenannten *Frobenius-Operator*

$$F\colon W(R) \longrightarrow W(R), \qquad (a_0, a_1, \ldots) \longmapsto (a_0^p, a_1^p, \ldots),$$

sowie den *Verschiebungsoperator*

$$V\colon W(R) \longrightarrow W(R), \qquad (a_0, a_1, \ldots) \longmapsto (0, a_0, a_1, \ldots),$$

ein. Beide Operatoren sind miteinander vertauschbar, was $V \circ F = F \circ V$ bedeutet. Außerdem ist der Frobenius-Operator $F\colon W(R) \longrightarrow W(R)$ für Ringe R mit $p \cdot 1 = 0$ ein Ringhomomorphismus. In diesem Falle ist nämlich $R \longrightarrow R$, $a \longmapsto a^p$, ein Ringhomomorphismus und induziert somit einen Ringhomomorphismus $W(R) \longrightarrow W(R)$, der gerade mit F übereinstimmt. Der Verschiebungsoperator V besitzt keine solche Eigenschaft, er ist aber stets additiv. Um dies zu verifizieren, darf man ähnlich wie im Beweis zu Satz 6 annehmen, dass p in R invertierbar ist. Dann ist $w\colon W(R) \longrightarrow R^{\mathbb{N}}$ ein Isomorphismus, und es gilt $W_{n+1}(V(a)) = pW_n(a)$ bzw.

$$w\big(V(a)\big) = \big(0, pW_0(a), pW_1(a), \ldots\big),$$

was besagt, dass V mittels w in die Abbildung

$$R^{\mathbb{N}} \longrightarrow R^{\mathbb{N}}, \qquad (x_0, x_1, \ldots) \longmapsto (0, px_0, px_1, \ldots),$$

transformiert wird. Diese ist offenbar komponentenweise additiv.

Wir können nun die p-Multiplikation auf $W(R)$, die wir im Folgenden auch einfach mit p bezeichnen, wie folgt beschreiben:

Lemma 7. *Für $a \in W(R)$ bezeichne $(p{\cdot}a)$ die p-fache Summe von a in $W(R)$ und $(p \cdot a)_n$ die n-te Komponente hiervon. Entsprechend sei $(V \circ F(a))_n$ die n-te Komponente von $V \circ F(a)$. Dann gilt*

$$\big(V \circ F(a)\big)_n \equiv \big(p \cdot a\big)_n \mod (p), \qquad n \in \mathbb{N}.$$

Hat man insbesondere $p \cdot 1 = 0$ in R, so besteht die Beziehung

$$V \circ F = F \circ V = p.$$

Beweis. Mit der üblichen Argumentation dürfen wir annehmen, dass p kein Nullteiler in R ist. Die behaupteten Kongruenzen sind dann gemäß Lemma 4 äquivalent zu

$$W_n\big(V \circ F(a)\big) \equiv W_n(p \cdot a) \mod p^{n+1}, \qquad n \in \mathbb{N}.$$

Nun gilt aber aufgrund der Rekursionsformeln $(*)$

$$W_n\big(V \circ F(a)\big) = W_n\big(F \circ V(a)\big) \equiv W_{n+1}\big(V(a)\big) \mod p^{n+1}$$

und weiter

$$W_{n+1}\big(V(a)\big) = p \cdot W_n(a) = W_n(p \cdot a).$$

Dabei hatten wir die Gleichheit links in vorstehender Formel bereits weiter oben benutzt, um zu zeigen, dass V additiv ist. Die Gleichheit rechts folgt aus der Tatsache, dass $w\colon W(R) \longrightarrow R^{\mathbb{N}}$ homomorph ist, so dass sich insgesamt die gewünschten Kongruenzen ergeben. □

Im Hinblick auf die Kummer-Theorie zur Charakteristik p und zu einem Exponenten p^r benötigen wir Ringe von Witt-Vektoren *endlicher Länge* $r \geq 1$. Bisher sind wir von der Menge $R^{\mathbb{N}}$ ausgegangen und haben sozusagen Witt-Vektoren unendlicher Länge betrachtet. Man kann sich aber auch auf Vektoren $(a_0, \ldots, a_{r-1}) \in R^r$ der Länge r beschränken. Da die Polynome S_n, P_n nur Variablen X_i, Y_i mit Indizes $i \leq n$ enthalten, induzieren diese Polynome wiederum Verknüpfungen auf R^r, und man zeigt wie im Falle von Witt-Vektoren unendlicher Länge, dass man eine Ring-Struktur auf R^r erhält. Der resultierende Ring wird mit $W_r(R)$ bezeichnet und heißt Ring der *Witt-Vektoren der Länge* r über R. Die Aussagen von Satz 6 übertragen sich dem Sinne nach, wobei $W_1(R)$ kanonisch isomorph zu R ist. Bezeichnet V wie oben den Verschiebungsoperator auf $W(R)$, so ist die Projektion

$$W(R) \longrightarrow W_r(R), \qquad (a_0, a_1, \ldots) \longmapsto (a_0, \ldots, a_{r-1})$$

ein surjektiver Ringhomomorphismus mit Kern

$$V^r W(R) = \big\{(a_0, a_1, \ldots) \in W(R)\,;\, a_0 = \ldots = a_{r-1} = 0\big\},$$

induziert also einen Isomorphismus $W(R)/V^r W(R) \xrightarrow{\sim} W_r(R)$. Insbesondere ist $V^r W(R)$ ein Ideal in $W(R)$. Dabei bemerke man, dass $V^r\colon W(R) \longrightarrow W(R)$ ein injektiver Homomorphismus additiver Gruppen

ist, der $V^k W(R)$ für $k \in \mathbb{N}$ auf $V^{r+k}W(R)$ abbildet und daher zu einem r-fachen Verschiebungsoperator $V_k^r \colon W_k(R) \longrightarrow W_{r+k}(R)$ Anlass gibt. Letzterer ist ebenfalls ein injektiver Homomorphismus additiver Gruppen. Offenbar gilt

$$\operatorname{im} V_k^r = \big\{(a_0, \ldots, a_{r+k-1}) \in W_{r+k}(R) \,;\, a_0 = \ldots = a_{r-1} = 0\big\},$$

und dieses Bild stimmt überein mit dem Kern der Projektion

$$W_{r+k}(R) \longrightarrow W_r(R), \qquad (a_0, \ldots, a_{r+k-1}) \longmapsto (a_0, \ldots, a_{r-1}).$$

Es folgt, dass V_k^r einen Isomorphismus $W_{r+k}(R)/V_k^r W_k(R) \xrightarrow{\sim} W_r(R)$ induziert oder, mit anderen Worten, Anlass zu einer exakten Sequenz abelscher Gruppen

$$0 \longrightarrow W_k(R) \xrightarrow{V_k^r} W_{r+k}(R) \longrightarrow W_r(R) \longrightarrow 0$$

gibt. Alternativ können wir auf $W_r(R)$ auch die Abbildung

$$W_r(R) \xrightarrow{V_r^1} W_{r+1}(R) \longrightarrow W_r(R), \quad (a_0, \ldots, a_{r-1}) \longmapsto (0, a_0, \ldots, a_{r-2}),$$

als Verschiebungsoperator betrachten. Dieser Operator, im Folgenden wieder mit V bezeichnet, ist additiv, und es besitzt V^k für $0 \leq k \leq r$ gerade

$$V^{r-k} W_r(R) = \big\{(a_0, \ldots, a_{r-1}) \in W_r(R) \,;\, a_0 = \ldots = a_{r-k-1} = 0\big\}$$

als Kern.

Kummer-Theorie zum Exponent p^r. — Wir wollen nun zur Kummer-Theorie zu einem Exponenten p^r, $r \geq 1$, zurückkehren und betrachten hierfür einen Körper K der Charakteristik $p > 0$ mit separabel algebraischem Abschluss K_s und absoluter Galois-Gruppe G. Jeder Galois-Automorphismus $\sigma \colon K_s \longrightarrow K_s$ induziert dann einen Automorphismus von Ringen

$$W_r(K_s) \longrightarrow W_r(K_s), \qquad (a_0, \ldots, a_{r-1}) \longmapsto \big(\sigma(a_0), \ldots, \sigma(a_{r-1})\big).$$

Insgesamt ergibt sich ein Homomorphismus $G \longrightarrow \operatorname{Aut}(W_r(K_s))$, der eine Aktion von G auf $W_r(K_s)$ darstellt. Diese Aktion ist stetig, da die Aktion von G auf den einzelnen Komponenten von $W_r(K_s)$ stetig ist. Schreiben wir also im Folgenden A für die additive Gruppe von $W_r(K_s)$, so ist A mit

einer stetigen G-Aktion versehen, wobei in der Notation der allgemeinen Kummer-Theorie $A_L = W_r(L)$ für Zwischenkörper L zu K_s/K gilt.

Es bildet nun

$$\wp\colon A \longrightarrow A, \qquad a \longmapsto F(a) - a,$$

einen Endomorphismus von A, der mit der G-Aktion verträglich ist.

Theorem 8. *Für* $\operatorname{char} K = p > 0$ *erfüllt* $A = W_r(K_s)$ *als G-Modul zusammen mit dem G-Homomorphismus*

$$\wp\colon A \longrightarrow A, \qquad a \longmapsto F(a) - a,$$

die Voraussetzungen von Theorem 1 *zur Kummer-Theorie vom Exponenten* p^r *über* K.

Wir führen den Nachweis in einzelnen Schritten durch.

Lemma 9. $\wp$ *ist surjektiv*.

Beweis. Im Falle $r = 1$ gilt $A = W_1(K_s) = K_s$, und wir haben die Abbildung

$$\wp\colon K_s \longrightarrow K_s, \qquad \alpha \longmapsto \alpha^p - \alpha,$$

zu betrachten. Diese ist surjektiv, da Polynome des Typs $X^p - X - c$ mit $c \in K_s$ stets separabel sind. Ansonsten überlegt man sich für $r \geq 1$, dass $\wp$ mit dem Verschiebungsoperator wie auch mit der Projektion $W_r(K_s) \longrightarrow W_1(K_s)$ verträglich ist. Für $r > 1$ hat man daher ein kommutatives Diagramm

$$\begin{array}{ccccccccc}
0 & \longrightarrow & W_{r-1}(K_s) & \xrightarrow{V^1_{r-1}} & W_r(K_s) & \longrightarrow & W_1(K_s) & \longrightarrow & 0 \\
 & & \wp\downarrow & & \wp\downarrow & & \wp\downarrow & & \\
0 & \longrightarrow & W_{r-1}(K_s) & \xrightarrow{V^1_{r-1}} & W_r(K_s) & \longrightarrow & W_1(K_s) & \longrightarrow & 0,
\end{array}$$

und man schließt aus der Surjektivität von $\wp$ auf $W_1(K_s)$ und auf $W_{r-1}(K_s)$ leicht die Surjektivität auf $W_r(K_s)$. □

Weiter ist für die Kummer-Theorie der Kern von $\wp$ zu bestimmen. Wir fassen im Folgenden $\mathbb{F}_p$ als Primkörper unseres Körpers K auf.

Lemma 10. *Es gilt* $\ker \wp = W_r(\mathbb{F}_p)$, *und diese Gruppe ist zyklisch von der Ordnung* p^r. *Sie wird erzeugt vom Einselement* $e \in W_r(\mathbb{F}_p)$.

Beweis. Die Lösungen in K_s der Gleichung $x^p = x$ bestehen gerade aus den Elementen des Primkörpers $\mathbb{F}_p \subset K_s$. Deshalb gilt $\ker \wp = W_r(\mathbb{F}_p)$. Dies ist eine Gruppe der Ordnung p^r, und wir behaupten, dass das Einselement $e = (1, 0, \ldots, 0) \in W_r(\mathbb{F}_p)$ diese Ordnung besitzt. In der Tat, die Ordnung von e ist ein Teiler von p^r, also eine p-Potenz. Unter Benutzung der Formel $V \circ F = p$ aus Lemma 7 schiebt jede Multiplikation mit p die Komponente 1 in e um eine Stelle nach rechts, so dass sich tatsächlich p^r als Ordnung von e ergibt. □

Um nun Theorem 1 anwenden zu können und damit eine Charakterisierung der abelschen Erweiterungen mit einem Exponenten, der p^r teilt, zu gewinnen, bleibt noch die Gültigkeit von Hilberts Satz 90 nachzuweisen.

Satz 11. *Sei* L/K *eine endliche Galois-Erweiterung in Charakteristik* $p > 0$ *mit Galois-Gruppe* G. *Auf dem Ring der Witt-Vektoren* $W_r(L)$ *gegebener Länge* r *betrachte man die komponentenweise Aktion von* G. *Dann gilt*

$$H^1\big(G, W_r(L)\big) = 0,$$

d. h. jeder 1*-Kozyklus ist bereits ein* 1*-Korand.*

Beweis. Wir gehen ähnlich wie in 4.8/2 vor, müssen aber zusätzlich die Spurabbildung

$$\mathrm{Sp}_{L/K} \colon W_r(L) \longrightarrow W_r(K), \qquad a \longmapsto \sum_{\sigma \in G} \sigma(a),$$

benutzen. Da jedes $\sigma \in G$ einen $W_r(K)$-Automorphismus von $W_r(L)$ definiert, sieht man unmittelbar, dass die Spurbildung $W_r(K)$-linear ist. Im Übrigen ist $\mathrm{Sp}_{L/K}$ mit der Projektion $W_r(L) \longrightarrow W_1(L) = L$ verträglich, wobei die Spurbildung auf $W_1(L)$ gemäß 4.7/4 mit der gewöhnlichen Spurabbildung $\mathrm{Sp}_{L/K} \colon L \longrightarrow K$ übereinstimmt. Wir wollen mittels Induktion nach r zeigen, dass $\mathrm{Sp}_{L/K} \colon W_r(L) \longrightarrow W_r(K)$ surjektiv ist.

Im Falle $r = 1$ haben wir es mit der gewöhnlichen Spurabbildung für endliche Körpererweiterungen zu tun, und die Behauptung ergibt sich mit 4.7/7. Ansonsten können wir benutzen, dass die Spurbildung auf $W_r(L)$

offenbar mit dem Verschiebungsoperator verträglich ist und wir daher für $r > 1$ ein kommutatives Diagramm

$$\begin{array}{ccccccccc} 0 & \longrightarrow & W_{r-1}(L) & \xrightarrow{V^1_{r-1}} & W_r(L) & \longrightarrow & W_1(L) & \longrightarrow & 0 \\ & & \mathrm{Sp}_{L/K}\downarrow & & \mathrm{Sp}_{L/K}\downarrow & & \mathrm{Sp}_{L/K}\downarrow & & \\ 0 & \longrightarrow & W_{r-1}(K) & \xrightarrow{V^1_{r-1}} & W_r(K) & \longrightarrow & W_1(K) & \longrightarrow & 0 \end{array}$$

erhalten. Die Spurbildung auf dem Niveau von $W_1(L)$ ist surjektiv. Daher impliziert die Surjektivität der Spurbildung auf dem Niveau von $W_{r-1}(L)$ wie gewünscht diejenige auf dem Niveau von $W_r(L)$. Insbesondere existiert ein Element $a \in W_r(L)$ mit $\mathrm{Sp}_{L/K}(a) = 1$.

Sei nun $f\colon G \longrightarrow W_r(L)$ ein 1-Kozyklus. Wir betrachten die Poincaré-Reihe

$$b = \sum_{\sigma' \in G} f(\sigma') \cdot \sigma'(a)$$

und erhalten für beliebiges $\sigma \in G$

$$\begin{aligned} \sigma(b) &= \sum_{\sigma' \in G} \sigma\big(f(\sigma')\big) \cdot (\sigma \circ \sigma')(a) \\ &= \sum_{\sigma' \in G} \big(f(\sigma \circ \sigma') - f(\sigma)\big) \cdot (\sigma \circ \sigma')(a) \\ &= \sum_{\sigma' \in G} f(\sigma \circ \sigma') \cdot (\sigma \circ \sigma')(a) - \sum_{\sigma' \in G} f(\sigma) \cdot (\sigma \circ \sigma')(a) \\ &= b - f(\sigma) \cdot \mathrm{Sp}_{L/K}(a) = b - f(\sigma), \end{aligned}$$

d. h. f ist ein 1-Korand. □

Theorem 8 ist damit bewiesen.

Lernkontrolle und Prüfungsvorbereitung

Kummer-Theorie

1. Erkläre das Grundgerüst und die zugehörigen Bedingungen der allgemeinen Kummer-Theorie. Wie passt sich die im Abschnitt 4.9 behandelte multiplikative Kummer-Theorie in diesen Rahmen ein?

2. Es sei K ein Körper und K_s ein separabel algebraischer Abschluss von K. Setze $G = \mathrm{Gal}(K_s/K)$ und betrachte im Sinne der allgemeinen Kummer-Theorie für eine gegebene natürliche Zahl $n > 0$ einen stetigen G-Modul A sowie einen surjektiven G-Homomorphismus $\wp\colon A \longrightarrow A$, dessen Kern μ_n eine zyklische Untergruppe der Ordnung n in A_K bilde. Definiere für eine Untergruppe $C \subset A_K$, welche $\wp(A_K)$ enthalte, die in der allgemeinen Kummer-Theorie verwendete Paarung $\langle\cdot,\cdot\rangle\colon\ \mathrm{Gal}(K(\wp^{-1}(C))/K)\times C/\wp(A_K) \longrightarrow \mu_n$ und erläutere deren Eigenschaften.

3. Sei Hilberts Satz 90 in der Situation von Punkt 2 gegeben. Welche Eigenschaften besitzt die Paarung von Punkt 2? Diskutiere insbesondere die zugehörigen Homomorphismen

$$\varphi_1\colon \mathrm{Gal}\big(K(\wp^{-1}(C))\,/K\big) \longrightarrow \mathrm{Hom}\big(C/\wp(A_K), \mu_n\big), \qquad \sigma \longmapsto \langle\sigma,\cdot\rangle,$$
$$\varphi_2\colon \qquad C/\wp(A_K) \longrightarrow \mathrm{Hom}\big(\mathrm{Gal}(K(\wp^{-1}(C))\,/K), \mu_n\big),\ \ \overline{c} \longmapsto \langle\cdot,\overline{c}\rangle.$$

4. Wie steht in der Situation von Punkt 3 die Endlichkeit von $K(\wp^{-1}(C))/K$ in Relation zur Endlichkeit von $C/\wp(A_K)$? Wie berechnet sich im Falle der Endlichkeit die Galois-Gruppe der Erweiterung $K(\wp^{-1}(C))/K$?

+5. Skizziere die Beweise zu den Punkten 3 und 4.

Witt-Vektoren. — Sei p eine fest gewählte Primzahl.

6. Definiere die Witt-Polynome $W_n \in \mathbb{Z}[X_0, \ldots, X_n]$, $n \in \mathbb{N}$, zur Primzahl p und leite die zugehörigen Rekursionsformeln her.

7. Betrachte für $n \in \mathbb{N}$ den Endomorphismus ω_n auf $\mathbb{Z}[\frac{1}{p}][X_0, \ldots, X_n]$, der für die Variablen $X_0, \ldots, X_n$ die Witt-Polynome $W_0, \ldots, W_n$ einsetzt und zeige, dass dies ein Automorphismus ist. Zeige weiter, dass sich die ω_n zu einem Automorphismus ω auf $\mathbb{Z}[\frac{1}{p}][X_0, X_1, \ldots]$ zusammensetzen.

8. Betrachte für einen Ring R die Abbildung $w\colon R^{\mathbb{N}} \longrightarrow R^{\mathbb{N}}$, welche einer Folge $x \in R^{\mathbb{N}}$ die Folge $(W_n(x))_{n\in\mathbb{N}}$ seiner "Geisterkomponenten" zuordnet, und zeige, dass diese bijektiv ist, falls $p = p \cdot 1$ in R invertierbar ist.

9. Betrachte die Abbildung $w\colon R^{\mathbb{N}} \longrightarrow R^{\mathbb{N}}$ aus Punkt 8 und führe auf dem Bildbereich $R^{\mathbb{N}}$ eine Ringstruktur mittels komponentenweiser Addition und Multiplikation ein. Erkläre die allgemeine Strategie, die man zur Definition des Witt-Rings $W(R)$ verfolgt, indem man nämlich auf dem Urbildbereich $R^{\mathbb{N}}$ eine Ringstruktur erklärt, so dass w ein Homomorphismus von Ringen ist, sogar ein Isomorphismus, wenn $p = p \cdot 1$ in R invertierbar ist.

+10. Welche fundamentalen Hilfsresultate sind zu beweisen, wenn man für einen Ring R den Witt-Ring $W(R)$ gemäß Punkt 9 definieren möchte.

11. Sei R ein Ring. Leite die Multiplikationsregel und die Zerlegungsregel im Witt-Ring $W(R)$ her. Wie lauten das Nullelement und das Einselement in $W(R)$?

12. Definiere für einen Ring R den Frobenius-Operator und den Verschiebungsoperator auf dem Ring $W(R)$ der Witt-Vektoren. Leite die typischen Eigenschaften dieser Operatoren her und kläre insbesondere die Relation zur p-Multiplikation auf $W(R)$.

13. Gib ein Beispiel eines Ringes R, welches zeigt, dass ein Vektor $a \in W(R)$ im Allgemeinen nicht eindeutig durch seine Geisterkomponenten festgelegt ist.

14. Beschreibe den Formalismus der Witt-Vektoren endlicher Länge über einem Ring R.

Kummer-Theorie zum Exponent p^r

15. Erkläre, wie man Witt-Vektoren endlicher Länge für die Kummer-Theorie zu einer Primpotenz p^r als Exponent nutzen kann.

[+]16. Formuliere Hilberts Satz 90 im Zusammenhang mit Punkt 15 und führe dessen Beweis aus.

Übungsaufgaben

1. *Charakterisiere innerhalb der allgemeinen Kummer-Theorie zu einem Exponenten n alle zyklischen Erweiterungen von einem Grad, der n teilt.*

2. *Es sei K ein vollkommener Körper der Charakteristik $p > 0$. Beweise folgende Eigenschaften des Witt-Rings $W(K)$:*

   (i) *Die Abbildung*

   $$K^* \longrightarrow W(K)^*, \qquad \alpha \longmapsto (\alpha, 0, 0, \ldots),$$

   ist ein Monomorphismus multiplikativer Gruppen. Gilt eine ähnliche Aussage auch für die additive Gruppe K?

   (ii) *Die kanonische Abbildung $W(K) \longrightarrow \varprojlim W(K)/p^n W(K)$ ist ein Isomorphismus von Ringen. Insbesondere stimmt $W(\mathbb{F}_p)$ überein mit dem Ring $\mathbb{Z}_p$ der ganzen p-adischen Zahlen; vgl. Abschnitt* 4.2.

   (iii) *$W(K)$ ist ein Hauptidealring mit $p \cdot W(K) = V^1 W(K)$ als maximalem Ideal. Alle weiteren nicht-trivialen Ideale in $W(K)$ sind Potenzen dieses maximalen Ideals und sind daher von der Form $p^n \cdot W(K) = V^n W(K)$.*

3. Es sei p prim und $q = p^r$ eine nicht-triviale Potenz von p. Zeige:
   (i) Jedes $a \in W(\mathbb{F}_q)$ hat eine Darstellung
   $$a = \sum_{i \in \mathbb{N}} c_i p^i$$
   mit eindeutig bestimmten Koeffizienten $c_i \in \mathbb{F}_q$; dabei ist c_i jeweils als Witt-Vektor $(c_i, 0, 0, \ldots) \in W(\mathbb{F}_q)$ zu interpretieren.
   (ii) $W(\mathbb{F}_q) = \mathbb{Z}_p[\zeta]$ für eine primitive $(q-1)$-te Einheitswurzel ζ.

   Bestimme schließlich den Grad des Quotientenkörpers $Q(W(\mathbb{F}_q))$ über $Q(\mathbb{Z}_p)$.
4. Es sei G die absolute Galois-Gruppe eines Körpers K. Betrachte in der Notation der allgemeinen Kummer-Theorie für einen G-Modul A die Abbildungen
   $$\Phi\colon \Delta \longmapsto G(A/\Delta), \qquad \Psi\colon H \longmapsto A^H,$$
   für Untergruppen $\Delta \subset A$ und $H \subset G$ und zeige:
   $$\Phi \circ \Psi \circ \Phi(\Delta) = \Phi(\Delta), \qquad \Psi \circ \Phi \circ \Psi(H) = \Psi(H).$$

4.11 Galois-Descent*

Es sei K'/K eine Körpererweiterung. Ist V ein K-Vektorraum, etwa mit Basis $(v_i)_{i \in I}$, so kann man durch Koeffizientenerweiterung aus V einen K'-Vektorraum $V' = V \otimes_K K'$ konstruieren, etwa indem man $(v_i)_{i \in I}$ als Basis vorgibt, nun aber Koeffizienten in K' zulässt. Man sagt, V sei eine *K-Form* von V'. In ähnlicher Weise lässt sich aus einem K-Homomorphismus $\varphi\colon V \longrightarrow W$ durch Koeffizientenerweiterung ein K'-Homomorphismus $\varphi'\colon V' \longrightarrow W'$ gewinnen. Gegenstand der Descent-Theorie ("Abstiegs"-Theorie) zu K'/K ist das umgekehrte Problem. Man möchte K-Vektorräume und ihre Homomorphismen durch die entsprechenden Objekte über K' beschreiben, wobei man auf letzteren gewisse Zusatzstrukturen, sogenannte *Descent-Daten* betrachtet. Es ist zwar einfach, zu K'-Vektorräumen V', W' jeweils K-Formen V, W anzugeben. Damit aber ein K'-Homomorphismus $\varphi'\colon V' \longrightarrow W'$ bei vorgegebenen K-Formen V, W zu V', W' als über K definiert, d. h. als Koeffizientenerweiterung eines K-Homomorphismus $\varphi\colon V \longrightarrow W$ angesehen werden kann, ist es erforderlich, dass φ' die auf V' und W' gegebenen Descent-Daten respektiert.

Wir werden hier Descent-Theorie nur für den Fall durchführen, wo K Fixkörper unter einer endlichen Gruppe von Automorphismen von K' ist, also für endliche Galois-Erweiterungen K'/K; vgl. 4.1/4. Die erforderlichen Descent-Daten lassen sich dann mit Hilfe von Gruppenaktionen beschreiben. Es sei noch angefügt, dass man Descent-Theorie in der Algebraischen Geometrie unter sehr viel allgemeineren Bedingungen betreibt; man vergleiche hierzu die grundlegende Abhandlung von Grothendieck [6], oder auch [3], Chap. 4.

Bevor wir mit der eigentlichen Descent-Theorie beginnen, wollen wir den Prozess der Koeffizientenerweiterung bei Vektorräumen auf eine solide Basis stellen, indem wir Tensorprodukte einführen. Wir diskutieren hier nur den benötigten Spezialfall, in allgemeinerem Rahmen werden Tensorprodukte noch in Abschnitt 7.2 behandelt.

Definition 1. *Es sei K'/K eine Körpererweiterung und V ein K-Vektorraum. Ein* Tensorprodukt *von K' mit V über K ist ein K'-Vektorraum V' zusammen mit einer K-linearen Abbildung $\tau\colon V \longrightarrow V'$, so dass folgende universelle Eigenschaft gilt*:

Ist $\varphi\colon V \longrightarrow W'$ eine K-lineare Abbildung in einen K'-Vektorraum W', so existiert eindeutig ein K'-Homomorphismus $\varphi'\colon V' \longrightarrow W'$ mit $\varphi = \varphi' \circ \tau$, also eine K'-lineare "Ausdehnung" φ' von φ.

Tensorprodukte sind aufgrund der definierenden universellen Eigenschaft bis auf kanonische Isomorphie eindeutig bestimmt. Man schreibt in vorstehender Situation $K' \otimes_K V$ oder $V \otimes_K K'$ anstelle von V', je nachdem, ob man V' unter der skalaren Multiplikation mit Elementen aus K' als Links- oder als Rechtsvektorraum ansehen möchte. Weiter ist es üblich, für $(a, v) \in K' \times V$ das Produkt $a \cdot \tau(v)$ auch mit $a \otimes v$ zu bezeichnen. Man nennt $a \otimes v$ einen *Tensor*; die Elemente aus $K' \otimes_K V$ sind endliche Summen solcher Tensoren, wie sich weiter unten ergeben wird. Entsprechendes gilt, wenn man V' als Rechtsvektorraum interpretiert.

Bemerkung 2. *In der Situation von Definition* 1 *existiert das Tensorprodukt $V' = K' \otimes_K V$ stets.*

Beweis. Man wähle eine K-Basis $(v_i)_{i\in I}$ von V und betrachte $V' = K'^{(I)}$ als K'-Vektorraum mit der kanonischen Basis $(e_i)_{i\in I}$. Indem wir für $i \in I$ den

Basisvektor $v_i \in V$ auf den Basisvektor $e_i \in K'^{(I)}$ abbilden, erhalten wir eine injektive K-lineare Abbildung $\tau\colon V \longrightarrow V'$. Es sei nun $\varphi\colon V \longrightarrow W'$ eine K-lineare Abbildung in einen beliebigen K'-Vektorraum W'. Ist dann $\varphi'\colon V' \longrightarrow W'$ eine K'-lineare Abbildung mit $\varphi = \varphi' \circ \tau$, so folgt notwendig $\varphi'(e_i) = \varphi'(\tau(v_i)) = \varphi(v_i)$. Somit ist φ' auf der K'-Basis (e_i) von V' und damit auf ganz V' eindeutig durch φ bestimmt. Umgekehrt kann man natürlich durch $e_i \longmapsto \varphi(v_i)$ sowie K'-lineare Ausdehnung eine K'-lineare Abbildung $\varphi'\colon V' \longrightarrow W'$ erklären, welche $\varphi = \varphi' \circ \tau$ erfüllt. Somit ist V' zusammen mit τ ein Tensorprodukt von K' mit V über K. □

Der Beweis zeigt, dass $V' = K' \otimes_K V$ in der Tat aus V entsteht, indem man die "Koeffizienten von V ausdehnt". Wir können nämlich V mit einem K-Untervektorraum von $K' \otimes_K V$ identifizieren, indem wir die (injektive) K-lineare Abbildung $\tau\colon V \longrightarrow V' = K' \otimes_K V$ verwenden. Im Beweis wurde, ausgehend von der K-Basis $(v_i)_{i\in I}$ von V, das Tensorprodukt $K' \otimes_K V$ als K'-Vektorraum mit dieser Basis erklärt. Die universelle Eigenschaft des Tensorprodukts, die wir nachgewiesen haben, zeigt sofort, dass das Ergebnis unabhängig von der Wahl der Basis $(v_i)_{i\in I}$ von V ist. Man kann weiter in direkter Weise sehen, dass sich jeder K-Homomorphismus $\varphi\colon V \longrightarrow W$ zwischen K-Vektorräumen V und W eindeutig zu einem K'-Homomorphismus $K' \otimes \varphi\colon K' \otimes_K V \longrightarrow K' \otimes_K W$ ausdehnt. Letzteres folgt aber auch formal aus der universellen Eigenschaft des Tensorprodukts, denn

$$V \longrightarrow K' \otimes_K W, \qquad v \longmapsto 1 \otimes \varphi(v),$$

ist eine K-lineare Abbildung und korrespondiert somit zu einem K'-Homomorphismus $K' \otimes \varphi\colon K' \otimes_K V \longrightarrow K' \otimes_K W$.[9]

Wir können nun die eingangs bereits benutzten Begriffe "K-Form" und "definiert über K" präzisieren. Dazu betrachte man eine beliebige Körpererweiterung K'/K. Ein K-Untervektorraum V eines K'-Vektorraumes V' heißt eine *K-Form* von V', wenn die zu $V \hookrightarrow V'$ gehörige K'-lineare Abbildung $K' \otimes_K V \longrightarrow V'$ ein Isomorphismus ist. Fixieren wir eine K-Form V von V', so können wir vorstehenden Isomorphismus als Identifizierung ansehen. Ein K'-Untervektorraum $U' \subset V'$ heißt dann *über K definiert*, wenn U' die K'-Ausdehnung eines K-Untervektorraumes $U \subset V$ ist oder,

[9] Im Rahmen allgemeiner Tensorprodukte ist es üblich, anstelle von $K' \otimes \varphi$ die Bezeichnung $\mathrm{id}_{K'} \otimes \varphi$ zu benutzen. Es handelt sich um das Tensorprodukt zweier K-linearer Abbildungen, nämlich der Identität auf K' und der Abbildung φ; vgl. Abschnitt 7.2.

mit anderen Worten, wenn es einen K-Untervektorraum $U \hookrightarrow V$ gibt, so dass die induzierte K'-lineare Abbildung $K' \otimes_K U \longrightarrow K' \otimes_K V = V'$ (diese ist stets injektiv!) $K' \otimes_K U$ mit U' identifiziert. Insbesondere sieht man, dass U dann eine K-Form von U' ist. Schließlich heißt ein K'-Homomorphismus $\varphi' \colon V' \longrightarrow W'$ zwischen K'-Vektorräumen mit K-Formen V und W *über K definiert*, wenn φ' Ausdehnung eines K-Homomorphismus $\varphi \colon V \longrightarrow W$ ist, d. h. wenn es einen K-Homomorphismus $\varphi \colon V \longrightarrow W$ gibt, so dass φ' bezüglich der Identifizierungen $V' = K' \otimes_K V$ und $W' = K' \otimes_K W$ mit $K' \otimes \varphi$ übereinstimmt.

Wir wollen nun auf den Fall einer endlichen Galois-Erweiterung K'/K hinarbeiten und setzen zunächst voraus, dass K der Fixkörper bezüglich einer Untergruppe $G \subset \mathrm{Aut}(K')$ ist; vgl. 4.1/4. Ist dann V' ein K'-Vektorraum mit K-Form V, wobei wir V' mit $K' \otimes_K V$ identifizieren, so lässt sich für jedes $\sigma \in G$ die K-lineare Abbildung $f_\sigma \colon K' \otimes_K V \longrightarrow K' \otimes_K V$ betrachten, welche durch $a \otimes v \longmapsto \sigma(a) \otimes v$ charakterisiert ist. Fixiert man nämlich eine K-Basis $(v_i)_{i \in I}$ von V, so kann man diese auch als K'-Basis von V' auffassen, und man kann f_σ durch

$$f_\sigma \colon V' \longrightarrow V', \qquad \sum a_i v_i \longmapsto \sum \sigma(a_i) v_i$$

erklären. Wir nennen f_σ eine *σ-lineare Abbildung*, denn es gelten die Relationen

$$f_\sigma(v' + w') = f_\sigma(v') + f_\sigma(w'), \qquad f_\sigma(a'v') = \sigma(a') f_\sigma(v'),$$

für $v', w' \in V'$ und $a' \in K'$. Weiter gilt $f_\sigma \circ f_\tau = f_{\sigma\tau}$ für $\sigma, \tau \in G$ sowie $f_\varepsilon = \mathrm{id}_{V'}$ für das Einselement $\varepsilon \in G$. Dies bedeutet, dass die Abbildungen f_σ eine Aktion

$$G \times V' \longrightarrow V', \qquad (\sigma, v) \longmapsto f_\sigma(v),$$

von G auf V' im Sinne von 5.1/1 definieren. Man nennt $f = (f_\sigma)_{\sigma \in G}$ die zur K-Form V von V' gehörige *kanonische G-Aktion*.

Satz 3. *Es sei K'/K eine Körpererweiterung, so dass K der Fixkörper unter einer Gruppe G von Automorphismen von K' ist. V' sei ein K'-Vektorraum mit K-Form V und zugehöriger G-Aktion f.*

(i) *Ein Element $v \in V'$ gehört genau dann zu V, wenn $f_\sigma(v) = v$ für alle $\sigma \in G$ gilt.*

(ii) *Ein K'-Untervektorraum $U' \subset V'$ ist genau dann über K definiert, wenn $f_\sigma(U') \subset U'$ für alle $\sigma \in G$ gilt.*

(iii) *Ein K'-Homomorphismus $\varphi' \colon V' \longrightarrow W'$ zwischen K'-Vektorräumen mit K-Formen V, W und zugehörigen G-Aktionen f, g ist genau dann über K definiert, wenn φ' mit allen Automorphismen $\sigma \in G$ verträglich ist, wenn also für alle $\sigma \in G$ und $v \in V'$ die Beziehung $\varphi'(f_\sigma(v)) = g_\sigma(\varphi'(v))$ gilt.*

Beweis. Aussage (i) ist leicht einzusehen. Bezüglich einer K-Basis $(v_i)_{i\in I}$ von V gelte $v = \sum_i a_i v_i$ mit Koeffizienten $a_i \in K'$. Wegen $f_\sigma(v) = \sum_i \sigma(a_i) v_i$ ist v genau dann invariant unter allen f_σ, wenn die Koeffizienten a_i invariant unter allen $\sigma \in G$ sind, d. h. wenn alle a_i zu K gehören und somit v Element von V ist. Genauso einfach lässt sich Aussage (iii) erhalten. Die dort angegebene Bedingung ist offenbar notwendig. Umgekehrt impliziert diese Bedingung unter Benutzung von (i) aber auch $\varphi'(V) \subset W$.

Nun zum Beweis von (ii). Die Bedingung $f_\sigma(U') \subset U'$ für $\sigma \in G$ ist trivialerweise notwendig. Um zu sehen, dass sie auch hinreichend ist, betrachte man eine K-Basis $(v_i)_{i\in I}$ von V sowie die Restklassen $\overline{v}_i$ zu den v_i in $W' = V'/U'$. Es existiert dann ein Teilsystem $(\overline{v}_i)_{i\in I'}$ des Systems aller $\overline{v}_i$, welches eine K'-Basis von W' bildet. Wir können daher $W = \sum_{i\in I'} K\overline{v}_i$ als K-Form von W' auffassen sowie auf W' die zu W gehörige kanonische G-Aktion g einführen. Es ist dann die Projektion $\varphi' \colon V' \longrightarrow W'$ bereits über K definiert. Um dies einzusehen, beachte man, dass jedes $v \in V'$ eine Darstellung

$$v = u + \sum_{i\in I'} a_i v_i$$

mit einem Element $u \in U'$ und Koeffizienten $a_i \in K'$ besitzt. Hieraus ergibt sich für $\sigma \in G$ wegen $f_\sigma(U') \subset U' = \ker \varphi'$ und $f_\sigma(v_i) = v_i$ sofort die Gleichung $\varphi'(f_\sigma(v)) = g_\sigma(\varphi'(v))$; d. h. φ' ist gemäß (iii) über K definiert. Man erkennt dann unschwer, dass mit φ' auch $U' = \ker \varphi'$ über K definiert ist. □

Wir wollen nun zeigen, dass man K-Formen eines Vektorraumes mittels Gruppenaktionen charakterisieren kann.

Satz 4. *Es sei K'/K eine Körpererweiterung, so dass K der Fixkörper unter einer Gruppe G von Automorphismen von K' ist. Weiter sei V' ein*

K'-Vektorraum. Für jedes $\sigma \in G$ sei $f_\sigma \colon V' \longrightarrow V'$ eine σ-lineare Abbildung mit $f_\sigma \circ f_\tau = f_{\sigma\tau}$ für $\sigma, \tau \in G$ und $f_\varepsilon = \mathrm{id}_{V'}$ für das Einselement $\varepsilon \in G$. Die Elemente f_σ definieren also eine Aktion f von G auf V'. Sei $V \subset V'$ die Fixmenge unter G. Dann gilt:

(i) *V ist ein K-Untervektorraum von V', und die von $\lambda \colon V \hookrightarrow V'$ induzierte K'-lineare Abbildung $\lambda' \colon K' \otimes_K V \longrightarrow V'$ ist injektiv.*

(ii) *Ist G endlich, so ist λ' surjektiv und somit bijektiv. V ist dann also eine K-Form von V'.*

Beweis. Da V eine K-Form von $K' \otimes_K V$ ist, können wir die zugehörige Aktion h von G auf $K' \otimes_K V$ betrachten; man definiere $h_\sigma \colon K' \otimes_K V \longrightarrow K' \otimes_K V$ durch $a \otimes v \longmapsto \sigma(a) \otimes v$. Dann ist λ' kompatibel mit den Aktionen h und f, denn es gilt

$$\lambda'\big(h_\sigma(a \otimes v)\big) = \lambda'\big(\sigma(a) \otimes v\big) = \sigma(a)v = f_\sigma(av) = f_\sigma\big(\lambda'(a \otimes v)\big).$$

Als Konsequenz folgt $h_\sigma(\ker \lambda') \subset \ker \lambda'$, d. h. $\ker \lambda'$ ist nach Satz 3 (ii) über K definiert. Es existiert daher ein K-Untervektorraum $U \subset V$, dessen K'-Ausdehnung in $K' \otimes_K V$ mit $\ker \lambda'$ übereinstimmt. Für $u \in U$ gilt aber $u = \lambda(u) = \lambda'(u) = 0$, also $u = 0$, und es ergibt sich, dass λ' injektiv ist. Aussage (i) ist damit klar.

Zum Nachweis von (ii) setzen wir G als endlich voraus. Es genügt zu zeigen, dass jede Linearform $\varphi' \colon V' \longrightarrow K'$, welche auf V verschwindet, schon auf ganz V' verschwindet. Sei also φ' eine solche Linearform mit $\varphi'(V) = 0$, und sei $v \in V'$. Dann sind für beliebiges $a \in K'$ die Elemente $v_a = \sum_{\sigma \in G} f_\sigma(av)$ sämtlich invariant unter der Aktion von G auf V', gehören also zu V. Wegen $\varphi'(V) = 0$ ergibt sich daraus $\sum_{\sigma \in G} \sigma(a)\varphi'(f_\sigma(v)) = 0$ für alle $a \in K'$. Fassen wir vorstehende Summe als Linearkombination der Charaktere $\sigma \in G$ auf, so folgt aus dem Satz 4.6/2 über die lineare Unabhängigkeit von Charakteren, dass die Koeffizienten $\varphi'(f_\sigma(v)) \in K'$ verschwinden. Für $\sigma = \varepsilon$ (Einselement von G) ergibt sich insbesondere $\varphi'(v) = 0$. Jede Linearform auf V', welche auf V trivial ist, ist somit auch auf V' trivial. □

Wir können also zusammenfassend aus den Sätzen 3 und 4 ablesen, dass für eine endliche Galois-Erweiterung K'/K mit Galois-Gruppe G die Theorie der K-Vektorräume äquivalent zu der Theorie der K'-Vektorräume mit G-Aktionen der beschriebenen Art ist. Dabei korrespondieren die

K-Homomorphismen von K-Vektorräumen zu denjenigen K'-Homomorphismen entsprechender K'-Objekte, die mit den jeweiligen G-Aktionen verträglich sind. Die G-Aktionen spielen also die Rolle der eingangs erwähnten Descent-Daten.

Es sei abschließend auch noch darauf hingewiesen, dass wir im Beweis von Satz 4 (ii) die lineare Unabhängigkeit von Charakteren 4.6/2 in ähnlicher Weise benutzt haben wie im Beweis der kohomologischen Version von Hilberts Satz 90, vgl. 4.8/2. In der Tat liefert 4.8/2 für eine endliche Galois-Erweiterung K'/K gerade die Aussage von Satz 4 im Falle $\dim_{K'} V' = 1$ bzw. $V' = K'$. Man rechnet nämlich leicht nach, dass für festes $v \in K'^*$ die Abbildung

$$G \longrightarrow K'^*, \qquad \sigma \longmapsto \frac{f_\sigma(v)}{v},$$

ein 1-Kozyklus und somit nach 4.8/2 ein 1-Korand ist. Es existiert deshalb ein Element $a \in K'^*$ mit $f_\sigma(v) \cdot v^{-1} = a \cdot \sigma(a)^{-1}$, und es folgt

$$f_\sigma(av) = \sigma(a) \cdot f_\sigma(v) = av,$$

d. h. $av \in V'$ ist ein Element, welches von allen f_σ festgelassen wird. Man sieht nun leicht, dass $V = K \cdot av$ die Fixmenge unter der Aktion von G auf V' ist, diese Menge also eine K-Form von V' darstellt.

Lernkontrolle und Prüfungsvorbereitung

1. Betrachte einen K-Vektorraum V und eine Körpererweiterung K'/K. Definiere das Tensorprodukt $K' \otimes_K V$ als K'-Vektorraum und beweise die Existenz solcher Tensorprodukte.

2. Es sei K'/K eine Körpererweiterung und $\varphi : V \longrightarrow W$ ein K-Homomorphismus zwischen K-Vektorräumen. Zeige, wie man φ zu einem K'-Homomorphismus zwischen den zugehörigen K'-Vektorräumen $K' \otimes_K V \longrightarrow K' \otimes_K W$ ausdehnen kann.

3. Es sei K'/K eine Körpererweiterung. Was versteht man unter einer K-Form eines K'-Vektorraums V'? Sei $\varphi' \colon V' \longrightarrow W'$ ein K'-Homomorphismus zwischen K'-Vektorräumen mit K-Formen V und W. Wann bezeichnet man φ' bezüglich dieser K-Formen als definiert über K? Wann bezeichnet man einen K'-Untervektorraum $U' \subset V'$ bezüglich einer K-Form von V' als definiert über K?

4. Es sei K'/K eine Galois-Erweiterung mit Galois-Gruppe G und V' ein K'-Vektorraum mit K-Form V. Erkläre den Begriff einer G-Aktion auf V' und beschreibe das Zusammenspiel von solchen G-Aktionen mit den unter Punkt 3 diskutierten Begriffsbildungen.
5. Es sei K'/K eine endliche Galois-Erweiterung mit Galois-Gruppe G, sowie V' ein K'-Vektorraum. Charakterisiere die K-Formen von V' mittels G-Aktionen auf V'.
6. Diskutiere Punkt 5 im Falle $\dim_{K'} V' = 1$ aus der Sicht der kohomologischen Version von Hilberts Satz 90 für endliche Galois-Erweiterungen.

Übungsaufgaben

1. *Es sei K'/K eine Körpererweiterung und A eine K-Algebra, d. h. ein Ring mit einem Homomorphismus $K \longrightarrow A$. Zeige, dass $A \otimes_K K'$ in natürlicher Weise eine K'-Algebra ist.*
2. *Führe einen alternativen Beweis zu Satz* 4 *und verifiziere Aussage* (i) *in direkter Weise mit einem induktiven Argument. Zum Nachweis von* (ii) *wähle eine K-Basis $\alpha_1, \ldots, \alpha_n$ von K' und zeige, dass jedes $v \in V'$ eine Darstellung der Form*
$$v = \sum_{i=1}^{n} c_i \Big(\sum_{\sigma \in G} f_\sigma(\alpha_i v) \Big)$$
mit Koeffizienten $c_i \in K'$ besitzt.
3. Es sei K'/K eine Körpererweiterung, so dass K der Fixkörper unter einer Gruppe G von Automorphismen von K' ist. Weiter sei V' ein K'-Vektorraum. Für $\sigma \in G$ bezeichne V'_σ den K'-Vektorraum, welcher als additive Gruppe mit V' übereinstimmt, dessen Multiplikation aber durch die Vorschrift $a \cdot v := \sigma(a)v$ gegeben ist, wobei das Produkt rechts im Sinne des K'-Vektorraums V' zu verstehen ist. Betrachte die Diagonaleinbettung $\lambda\colon V' \longrightarrow \prod_{\sigma \in G} V'_\sigma$ als K-lineare Abbildung sowie die induzierte K'-lineare Abbildung
$$\Lambda\colon V' \otimes_K K' \longrightarrow \prod_{\sigma \in G} V'_\sigma$$
und zeige: Λ ist injektiv und im Falle $[K' : K] < \infty$ sogar bijektiv. (*Hinweis*: Definiere eine geeignete Aktion von G auf $\prod_{\sigma \in G} V'_\sigma$, so dass V' die zugehörige Fixmenge ist.)
4. Es sei K'/K eine Körpererweiterung und V ein K-Vektorraum. Betrachte die K-linearen Abbildungen

$$\begin{aligned} V &\longrightarrow V \otimes_K K', & v &\longmapsto v \otimes 1, \\ V \otimes_K K' &\longrightarrow V \otimes_K K' \otimes_K K', & v \otimes a &\longmapsto v \otimes a \otimes 1, \\ V \otimes_K K' &\longrightarrow V \otimes_K K' \otimes_K K', & v \otimes a &\longmapsto v \otimes 1 \otimes a, \end{aligned}$$

und zeige, dass das Diagramm

$$V \to V \otimes_K K' \rightrightarrows V \otimes_K K' \otimes_K K'$$

exakt in dem Sinne ist, dass die Abbildung links injektiv ist und ihr Bild gleich dem Kern der Differenz der beiden Abbildungen rechts ist.

5. Es sei K'/K eine endliche Galois-Erweiterung mit Galois-Gruppe G. In der Situation von Aufgabe 4 setze $V' = V \otimes_K K'$ und identifiziere $V' \otimes_K K'$ mit $\prod_{\sigma \in G} V'_\sigma$ im Sinne von Aufgabe 3. Beschreibe nunmehr die beiden Abbildungen $V' \rightrightarrows \prod_{\sigma \in G} V'_\sigma$ aus Aufgabe 4 auf möglichst einfache Weise.

5. Fortführung der Gruppentheorie

Überblick und Hintergrund

Wir wollen an dieser Stelle noch einmal auf das Problem der Lösung algebraischer Gleichungen zurückkommen. Sei also $f \in K[X]$ ein normiertes Polynom mit Koeffizienten aus einem Körper K, und sei L ein Zerfällungskörper von f, wobei wir die Erweiterung L/K als separabel voraussetzen wollen. Wenn wir die algebraische Gleichung $f(x) = 0$ durch Radikale auflösen möchten, so bedeutet dies, dass wir eine Körperkette des Typs

$$(*) \qquad K = K_0 \subsetneq K_1 \subsetneq \ldots \subsetneq K_r$$

mit $L \subset K_r$ finden müssen, wobei K_{i+1} jeweils aus K_i durch Adjunktion einer gewissen Wurzel eines Elementes aus K_i entsteht. Denn genau dann können wir die Lösungen von $f(x) = 0$, welche die Erweiterung L/K ja erzeugen, mittels rationaler Operationen und mittels "Wurzelziehen" aus den Elementen von K gewinnen. Vereinfachend wollen wir im Folgenden annehmen, dass die Erweiterung K_r/K galoissch ist. Dann ist eine Körperkette des Typs $(*)$ aufgrund des Hauptsatzes der Galois-Theorie 4.1/6 zu einer Kette von Untergruppen

$$(**) \qquad \mathrm{Gal}(K_r/K) = G_0 \supsetneq G_1 \supsetneq \ldots \supsetneq G_r = \{1\}$$

äquivalent. Zudem haben wir in 4.5 und 4.8 Erweiterungen, die durch Adjunktion n-ter Wurzeln entstehen, Galois-theoretisch charakterisiert. Wenn wir uns auf Körper der Charakteristik 0 beschränken und annehmen, dass

S. Bosch, *Algebra*, https://doi.org/10.1007/978-3-662-67464-2_6

K genügend viele Einheitswurzeln enthält, so folgt mit 4.8/3 und 4.1/6, dass eine Körperkette des Typs $(*)$ genau dann durch sukzessive Adjunktion von Wurzeln entsteht, wenn die zugehörige Kette $(**)$ die folgenden Eigenschaften besitzt: G_{i+1} ist jeweils ein Normalteiler in G_i und die Restklassengruppen G_i/G_{i+1} sind zyklisch. Genauer werden wir in 6.1 auch ohne die Bedingung an die Einheitswurzeln sehen, dass die Gleichung $f(x) = 0$ dann und nur dann durch Radikale auflösbar ist, wenn sich eine Kette $(**)$ mit den genannten Eigenschaften für die Galois-Gruppe $\mathrm{Gal}(L/K)$ finden lässt.

Die vorstehenden Überlegungen zeigen, dass man das Problem der Auflösbarkeit algebraischer Gleichungen mittels der Galois-Theorie auf ein gruppentheoretisches Problem reduzieren kann. Beispielsweise sieht man unter Anwendung des Hauptsatzes über endlich erzeugte abelsche Gruppen 2.9/9, dass algebraische Gleichungen mit abelscher Galois-Gruppe stets auflösbar sind. Um hier aber zu allgemeineren Ergebnissen zu gelangen, ist es notwendig, die Theorie der endlichen (nicht notwendig kommutativen) Gruppen weiter auszubauen. Insbesondere müssen wir diejenigen Gruppen G charakterisieren, die eine Kette von Untergruppen des Typs $(**)$ besitzen, und zwar mit der Eigenschaft, dass G_{i+1} jeweils ein Normalteiler in G_i ist und die Restklassengruppen G_i/G_{i+1} zyklisch sind. Wir bezeichnen G in diesem Falle als *auflösbar*, wobei wir anstelle von "zyklisch" in äquivalenter Weise die Bedingung "abelsch" für die Quotienten G_i/G_{i+1} verlangen werden; vgl. 5.4/3 und 5.4/7.

Wir beginnen jedoch in 5.1 auf ganz elementare Weise mit *Gruppenaktionen*. Prototyp einer solchen Aktion ist die Interpretation der Galois-Gruppe einer algebraischen Gleichung $f(x) = 0$ als Gruppe von Permutationen der zugehörigen Lösungen; vgl. 4.3/1. Als Anwendung beweisen wir in 5.2 die nach L. Sylow benannten Sätze über endliche Gruppen. Diese machen Aussagen über die Existenz von Untergruppen, deren Ordnung eine Primpotenz ist. Insbesondere kann man die Sylowschen Sätze in Spezialfällen auch dazu benutzen, um zu testen, ob eine gegebene Gruppe auflösbar ist oder nicht. Sodann haben wir in 5.3 einige Grundlagen über Permutationsgruppen zusammengestellt, und in 5.4 schließlich behandeln wir auflösbare Gruppen. Dort zeigen wir insbesondere, dass die symmetrische Gruppe $\mathfrak{S}_n$ für $n \geq 5$ nicht auflösbar ist, woraus sich in 6.1 ergeben wird, dass die allgemeine Gleichung n-ten Grades für $n \geq 5$ nicht durch Radikale auflösbar ist.

5.1 Gruppenaktionen

Im Kapitel über Galois-Theorie haben wir bereits verschiedentlich mit Gruppenaktionen gearbeitet. Allerdings wurde dabei der Begriff einer Aktion nicht explizit eingeführt, da es sich ausschließlich um konkret gegebene Aktionen einer Galois-Gruppe auf einem Körper oder den Nullstellen eines Polynoms handelte. Im Folgenden wollen wir jedoch den konkreten Rahmen verlassen und einige allgemeine kombinatorische Eigenschaften von Gruppenaktionen herleiten.

Definition 1. *Es sei G eine (multiplikativ geschriebene) Gruppe und X eine Menge. Eine* Operation *oder* Aktion *von G auf X ist eine Abbildung*

$$G \times X \longrightarrow X, \qquad (g,x) \longmapsto g \cdot x,$$

welche folgende Bedingungen erfüllt:

(i) $1 \cdot x = x$ *für das Einselement* $1 \in G$ *und für* $x \in X$.

(ii) $(gh) \cdot x = g \cdot (h \cdot x)$ *für* $g, h \in G, x \in X$.

Wir führen zunächst einige Beispiele für Gruppenaktionen an.

(1) Es sei G eine Gruppe und X eine Menge. Dann gibt es stets die triviale Operation von G auf X, gegeben durch die Abbildung

$$G \times X \longrightarrow X, \qquad (g,x) \longmapsto x.$$

(2) Es sei X eine Menge und $S(X)$ die Gruppe der bijektiven Abbildungen $X \longrightarrow X$. Ist dann $G \subset S(X)$ eine Untergruppe, so operiert G auf X vermöge der Abbildung

$$G \times X \longrightarrow X, \qquad (\sigma,x) \longmapsto \sigma(x).$$

Insbesondere kann man für eine Galois-Erweiterung L/K die Aktion der Galois-Gruppe $\mathrm{Gal}(L/K) = \mathrm{Aut}_K(L)$ auf L betrachten. Diese Aktion wurde in Kapitel 4 über Galois-Theorie bereits ausführlich studiert.

(3) Für jede Gruppe G ist die Gruppenmultiplikation

$$G \times G \longrightarrow G, \qquad (g,h) \longmapsto gh,$$

eine Aktion von G auf sich selbst. Man sagt, G operiert durch Linkstranslation auf sich, wobei man, wie bereits früher erwähnt, unter der *Linkstranslation* mit $g \in G$ die Abbildung

$$\tau_g \colon G \longrightarrow G, \qquad h \longmapsto gh,$$

versteht. Analog kann man unter Benutzung der Rechtstranslation eine Aktion von G auf sich definieren, und zwar mittels

$$G \times G \longrightarrow G, \qquad (g, h) \longmapsto hg^{-1}.$$

Dabei heißt

$$\tau'_g \colon G \longrightarrow G, \qquad h \longmapsto hg,$$

für $g \in G$ die *Rechtstranslation* mit g auf G.

(4) Zu jeder Gruppe G gibt es weiter die sogenannte *Konjugationsoperation*

$$G \times G \longrightarrow G, \qquad (g, h) \longmapsto ghg^{-1}.$$

Die Abbildung

$$\mathrm{int}_g = \tau_g \circ \tau'_{g^{-1}} \colon G \longrightarrow G, \qquad h \longmapsto ghg^{-1},$$

ist ein Gruppenautomorphismus von G, die sogenannte *Konjugation* mit g. Automorphismen der Form int_g heißen *innere Automorphismen* von G ("int" steht für "interior"), wobei die kanonische Abbildung $G \longrightarrow \mathrm{Aut}(G)$, $g \longmapsto \mathrm{int}_g$, ein Gruppenhomomorphismus ist. Zwei Elemente $h, h' \in G$ heißen *konjugiert*, wenn es ein $g \in G$ mit $h' = \mathrm{int}_g(h)$ gibt. Ebenso nennt man zwei Untergruppen $H, H' \subset G$ *konjugiert*, wenn es ein $g \in G$ mit $H' = \mathrm{int}_g(H)$ gibt. Konjugiertheit von Elementen oder Untergruppen in G ist eine Äquivalenzrelation. Natürlich ist die Konjugationsoperation die triviale Aktion, wenn G kommutativ ist.

Ähnlich wie in (3) kann man für jede Gruppenaktion

$$G \times X \longrightarrow X$$

die (Links-)Translation mit einem Element $g \in G$ erklären, und zwar als Abbildung

$$\tau_g \colon X \longrightarrow X, \qquad x \longmapsto g \cdot x.$$

Die Familie der Translationen $(\tau_g)_{g\in G}$ beschreibt eine gegebene Aktion von G auf X vollständig. Es ist $G \longrightarrow S(X),\ g \longmapsto \tau_g$, ein Gruppenhomomorphismus, wie man leicht nachrechnet. Umgekehrt gibt jeder Gruppenhomomorphismus $\varphi\colon G \longrightarrow S(X)$ ähnlich wie in Beispiel (2) Anlass zu einer Aktion von G auf X, nämlich zu

$$G \times X \longrightarrow X, \qquad (g,x) \longmapsto \varphi(g)(x).$$

Beide Zuordnungen sind zueinander invers, so dass gilt:

Bemerkung 2. *Es sei G eine Gruppe und X eine Menge. Dann entsprechen die Gruppenaktionen $G \times X \longrightarrow X$ vermöge der obigen Zuordnung in bijektiver Weise den Gruppenhomomorphismen $G \longrightarrow S(X)$.*

Betrachtet man für eine Gruppe G die Aktion $G \times G \longrightarrow G$ vermöge Linkstranslation, so ist der zugehörige Homomorphismus $G \longrightarrow S(G)$ injektiv; denn $\tau_g = \tau_{g'}$ ist äquivalent zu $g = g'$. Insbesondere kann man G als Untergruppe von $S(G)$ auffassen.

Definition 3. *Es sei $G \times X \longrightarrow X$ eine Aktion einer Gruppe G auf einer Menge X. Für Punkte $x \in X$ führt man folgende Notationen ein*:

(i) $Gx := \{gx\ ;\ g \in G\}$ *heißt* Orbit *oder* Bahn *von x unter G.*

(ii) $G_x := \{g \in G\ ;\ gx = x\}$ *heißt* Isotropiegruppe *von x; es ist G_x eine Untergruppe von G.*

Dass G_x wirklich eine Untergruppe von G ist, rechnet man leicht nach. Denn G_x enthält das Einselement von G, und für $g, h \in G$ mit $gx = x = hx$ ergibt sich

$$(gh^{-1})x = (gh^{-1})(hx) = g\big(h^{-1}(hx)\big) = g\big((h^{-1}h)x\big) = gx = x.$$

Bemerkung 4. *Es sei $G \times X \longrightarrow X$ eine Aktion einer Gruppe G auf einer Menge X. Sind dann x, y zwei Punkte einer G-Bahn in X, so sind die Isotropiegruppen G_x, G_y zueinander konjugiert.*

Beweis. Es genügt, den Fall $y \in Gx$ zu betrachten. Sei also $h \in G$ mit $y = hx$. Für $g \in G_x$ gilt dann

$$(hgh^{-1})y = (hgh^{-1})hx = h(gx) = hx = y,$$

also $hgh^{-1} \in G_y$ und somit $hG_xh^{-1} \subset G_y$. Aus $x = h^{-1}y$ leitet man entsprechend $h^{-1}G_yh \subset G_x$ her, so dass $G_y = hG_xh^{-1}$ folgt. □

Weiter wollen wir zeigen, dass für zwei Bahnen $Gx, Gy \subset X$ aus $Gx \cap Gy \neq \emptyset$ bereits $Gx = Gy$ folgt. Ist nämlich $z \in Gx \cap Gy$, etwa $z = gx = hy$ mit $g, h \in G$, so hat man $x = g^{-1}z = g^{-1}hy$ und damit $Gx \subset Gy$. Analog ergibt sich $Gx \supset Gy$ und somit $Gx = Gy$. Folglich gilt:

Bemerkung 5. *Ist $G \times X \longrightarrow X$ eine Aktion einer Gruppe G auf einer Menge X, so ist X disjunkte Vereinigung der Bahnen unter G.*

Ein Element x einer Bahn B zu einer Aktion $G \times X \longrightarrow X$ wird auch als *Vertreter* dieser Bahn bezeichnet. Analog versteht man unter einem *Vertretersystem* einer Familie $(B_i)_{i\in I}$ paarweise disjunkter Bahnen eine Familie $(x_i)_{i\in I}$ von Elementen aus X, so dass jeweils $x_i \in B_i$ gilt. Die Aktion $G \times X \longrightarrow X$ heißt *transitiv*, wenn es genau eine G-Bahn gibt.

Wir wollen die Bahnen unter einer Gruppenaktion noch genauer charakterisieren. Wie üblich sei $\operatorname{ord} M$ die Anzahl der Elemente einer Menge M sowie $(G : H)$ der Index einer Untergruppe H in einer Gruppe G.

Bemerkung 6. *Sei $G \times X \longrightarrow X$ eine Gruppenaktion. Für $x \in X$ induziert die Abbildung $G \longrightarrow X$, $g \longmapsto gx$, eine Bijektion $G/G_x \xrightarrow{\sim} Gx$ von der* Menge *der Linksnebenklassen von G modulo der Isotropiegruppe G_x auf die Bahn von x unter G. Insbesondere gilt*

$$\operatorname{ord} Gx = \operatorname{ord} G/G_x = (G : G_x).$$

Beweis. Man betrachte die surjektive Abbildung

$$\varphi\colon G \longrightarrow Gx, \qquad g \longmapsto gx.$$

Für $g, h \in G$ hat man dann

$$\begin{aligned}\varphi(g) = \varphi(h) &\iff gx = hx \iff h^{-1}gx = x \iff h^{-1}g \in G_x\\ &\iff gG_x = hG_x.\end{aligned}$$

Folglich induziert φ, ähnlich wie bei dem Homomorphiesatz 1.2/7, eine Bijektion $G/G_x \xrightarrow{\sim} Gx$. □

Als direkte Folgerung ergibt sich aus den Bemerkungen 5 und 6:

Satz 7 (Bahnengleichung). *Es sei $G \times X \longrightarrow X$ eine Aktion einer Gruppe G auf einer endlichen Menge X sowie $x_1, \ldots, x_n$ ein Vertretersystem der Bahnen von X. Dann folgt*

$$\operatorname{ord} X = \sum_{i=1}^{n} \operatorname{ord} Gx_i = \sum_{i=1}^{n} (G : G_{x_i}).$$

Wir werden die Bahnengleichung insbesondere für $X = G$ und die Konjugationsoperation $G \times G \longrightarrow G$ anwenden. Im Folgenden sei G eine Gruppe und $S \subset G$ eine Teilmenge. Dann erklärt man den *Zentralisator* von S in G durch

$$Z_S = \big\{x \in G \,;\, xs = sx \text{ für alle } s \in S\big\},$$

das *Zentrum* von G als Zentralisator von G, also durch

$$Z = Z_G = \big\{x \in G \,;\, xs = sx \text{ für alle } s \in G\big\},$$

sowie den *Normalisator* von S in G durch

$$N_S = \big\{x \in G \,;\, xS = Sx\big\}.$$

Bemerkung 8. *Mit den oben eingeführten Bezeichnungen gilt*:

(i) *Z ist ein Normalteiler in G.*

(ii) *Z_S und N_S sind Untergruppen in G.*

(iii) *Ist S eine Untergruppe von G, so ist N_S die größte aller Untergruppen $H \subset G$ mit der Eigenschaft, dass S ein Normalteiler in H ist.*

Die Aussagen sind alle leicht nachzuprüfen. Wir gehen hier nur auf den Fall Z_S in (ii) ein. Besteht S aus genau einem Element s, so ist $Z_S = N_S$ die Isotropiegruppe von s unter der Konjugationsoperation von G. Für allgemeines S ist deshalb $Z_S = \bigcap_{s \in S} Z_{\{s\}}$ Untergruppe von G. Im Übrigen gilt stets $Z_S \subset N_S$.

Satz 9 (Klassengleichung). *Es sei G eine endliche Gruppe mit Zentrum Z und $x_1, \ldots, x_n$ ein Vertretersystem der Bahnen in $G - Z$ unter der Konjugationsoperation von G auf sich. Dann gilt*

$$\operatorname{ord} G = \operatorname{ord} Z + \sum_{i=1}^{n} \big(G : Z_{\{x_i\}}\big).$$

Beweis. Für $x \in Z$ besteht die Bahn unter der Konjugationsoperation von G lediglich aus dem Element x. Für $x \in G - Z$ hingegen kann die Bahn von x mit $G/Z_{\{x\}}$ identifiziert werden, vgl. Bemerkung 6. Die Behauptung ergibt sich damit aus der Bahnengleichung. □

Abschließend wollen wir noch zwei Resultate über das Zentrum Z einer Gruppe G erwähnen. Da Z gerade der Kern des Homomorphismus

$$G \longrightarrow \mathrm{Aut}(G), \qquad g \longmapsto \mathrm{int}_g,$$

ist, gilt aufgrund des Homomorphiesatzes 1.2/7:

Bemerkung 10. *Die Gruppe der inneren Automorphismen von G ist isomorph zu G/Z.*

Bemerkung 11. *Ist G/Z zyklisch, so ist G abelsch.*

Beweis. Sei $a \in G$, so dass G/Z von der Restklasse $\overline{a}$ zu a erzeugt wird. Sind nun $g, h \in G$ mit Restklassen $\overline{g} = \overline{a}^m$, $\overline{h} = \overline{a}^n$, so gibt es Elemente $b, c \in Z$ mit $g = a^m b$, $h = a^n c$. Dann folgt

$$gh = a^m b a^n c = a^{m+n} bc, \qquad hg = a^n c a^m b = a^{m+n} cb = a^{m+n} bc,$$

d. h. insgesamt $gh = hg$. □

Lernkontrolle und Prüfungsvorbereitung

1. Erläutere die Definition einer Gruppenaktion auf einer Menge und nenne einige Beispiele. Betrachte insbesondere für eine Gruppe deren Konjugationsoperation sowie deren innere Automorphismen.
2. Zeige, dass die Gruppenaktionen einer Gruppe G auf einer Menge X in bijektiver Weise den Gruppenhomomorphismen $G \longrightarrow S(X)$ in die Gruppe der bijektiven Selbstabbildungen von X entsprechen.
3. Betrachte eine Aktion $G \times X \longrightarrow X$ einer Gruppe G auf einer Menge X. Definiere für Punkte $x \in X$ die zugehörige Bahn Gx von x sowie die Isotropiegruppe G_x zu x. Zeige, dass X die disjunkte Vereinigung der Bahnen unter G ist und dass je zwei Isotropiegruppen zu Punkten aus ein und derselben Bahn zueinander konjugiert sind.

4. Zeige in der Situation von Punkt 3, dass es für $x \in X$ eine kanonische Bijektion $G/G_x \longrightarrow Gx$ gibt.
5. Erläutere die Bahnengleichung für Gruppenaktionen und beweise diese.
6. Es sei G eine Gruppe und S eine Teilmenge von G. Definiere den Zentralisator von S in G, das Zentrum von G sowie den Normalisator von S in G und kläre die Eigenschaften dieser Begriffsbildungen.
7. Erläutere die Klassengleichung für die Konjugationsoperation einer Gruppe auf sich und beweise diese.
8. Zeige für eine Gruppe G und deren Zentrum Z, dass die Gruppe der inneren Automorphismen von G zu G/Z isomorph ist.
9. Sei G eine Gruppe mit Zentrum Z. Zeige, dass G abelsch ist, wenn G/Z zyklisch ist.

Übungsaufgaben

1. *Es sei G eine endliche Gruppe und $H \subset G$ eine Untergruppe. Betrachte die Aktion von H auf G vermöge Linkstranslation (bzw. Rechtstranslation) und interpretiere die zugehörige Bahnengleichung im Sinne der elementaren Gruppentheorie.*
2. *Es sei L/K eine endliche Galois-Erweiterung mit Galois-Gruppe G. Betrachte die natürliche Aktion von G auf L und interpretiere für $a \in L$ die Isotropiegruppe G_a sowie die Bahn Ga im Sinne der Galois-Theorie. Bestimme auch die Ordnungen von G_a und Ga.*
3. Es sei G eine Gruppe und X die Menge aller Untergruppen von G. Zeige:
   (i) $G \times X \longrightarrow X$, $(g, H) \longmapsto gHg^{-1}$, definiert eine Aktion von G auf X.
   (ii) Die Bahn eines Elementes $H \in X$ besteht genau dann nur aus H, wenn H ein Normalteiler in G ist.
   (iii) Ist die Ordnung von G Potenz einer Primzahl p, so unterscheidet sich die Anzahl der Untergruppen in G von der Anzahl der Normalteiler in G um ein Vielfaches von p.
4. Es sei G eine endliche Gruppe, H eine Untergruppe und N_H ihr Normalisator. Zeige für $M := \bigcup_{g \in G} gHg^{-1}$:
   (i) $\operatorname{ord} M \leq (G : N_H) \cdot \operatorname{ord} H$
   (ii) Falls $H \neq G$, so gilt auch $M \neq G$.

5. Es sei G eine Gruppe, H eine Untergruppe sowie N_H bzw. Z_H der zugehörige Normalisator bzw. Zentralisator von H in G. Zeige, dass Z_H ein Normalteiler in N_H ist und dass die Gruppe N_H/Z_H isomorph zu einer Untergruppe der Automorphismengruppe $\mathrm{Aut}(H)$ ist.

6. *Lemma von Burnside*: Es sei $G \times X \longrightarrow X$ eine Aktion einer endlichen Gruppe G auf einer Menge X. Bezeichne mit X/G die Menge der Bahnen und für ein Element $g \in G$ mit $X^g = \{x \in X\,;\, gx = x\}$ die Menge aller Elemente in X, die von g festgelassen werden. Zeige

$$\mathrm{ord}(X/G) = \frac{1}{\mathrm{ord}\, G} \cdot \sum_{g \in G} \mathrm{ord}\, X^g.$$

5.2 Sylow-Gruppen

In Abschnitt 2.9 haben wir mit dem Hauptsatz 2.9/9 eine genaue Analyse der Struktur endlich erzeugter und insbesondere endlicher abelscher Gruppen gegeben. Wir wollen im Folgenden endliche Gruppen ohne Kommutativitätsvoraussetzung studieren und als Hauptziel die nach L. Sylow benannten Sätze beweisen, welche Aussagen über die Existenz von Untergruppen mit gewissen Eigenschaften machen. Als zentrale Begriffe führen wir zunächst p-Gruppen sowie p-Sylow-Untergruppen endlicher Gruppen ein.

Definition 1. *Es sei G eine endliche Gruppe sowie p eine Primzahl.*

(i) *G heißt* p-Gruppe, *wenn die Ordnung von G eine p-Potenz ist.*

(ii) *Eine Untergruppe $H \subset G$ heißt* p-Sylow-Gruppe, *wenn H eine p-Gruppe ist und p nicht den Index $(G : H)$ teilt, wenn es also $k, m \in \mathbb{N}$ mit $\mathrm{ord}\, H = p^k$, $\mathrm{ord}\, G = p^k m$ und $p \nmid m$ gibt* (*vgl.* 1.2/3).

Elemente von p-Gruppen haben aufgrund des Satzes von Lagrange 1.2/3 stets eine p-Potenz als Ordnung. Ebenso folgt mit 1.2/3, dass eine p-Sylow-Gruppe niemals echt in einer p-Untergruppe von G enthalten sein kann, also stets eine maximale p-Gruppe in G ist. Die Umkehrung hierzu wird sich erst als Folgerung aus den Sylowschen Sätzen ergeben, vgl. Korollar 11. Die triviale Untergruppe $\{1\} \subset G$ ist ein Beispiel einer p-Gruppe und für $p \nmid \mathrm{ord}\, G$ sogar einer p-Sylow-Gruppe in G. Im Übrigen kann man etwa aus dem Hauptsatz 2.9/9 ablesen, dass es in einer endlichen *abelschen* Gruppe G zu einer Primzahl p mit $p \mid \mathrm{ord}\, G$ genau eine p-Sylow-Gruppe $S_p \neq \{1\}$

gibt und dass G die direkte Summe aller dieser Sylow-Gruppen ist. Obwohl wir dieses Resultat im Weiteren nicht benötigen, wollen wir zur Illustration die Existenz von Sylow-Untergruppen im Falle endlicher abelscher Gruppen zunächst einmal vom elementaren Standpunkt aus behandeln. Das nachfolgend formulierte Resultat ist später allerdings auch in einfacher Weise aus den Sylowschen Sätzen abzuleiten; man vergleiche hierzu Aufgabe 1.

Bemerkung 2. *Es sei G eine endliche* abelsche *Gruppe und p eine Primzahl. Dann ist*

$$S_p = \left\{a \in G\,;\; a^{p^t} = 1 \text{ für geeignetes } t \in \mathbb{N}\right\}$$

die einzige p-Sylow-Gruppe in G.

Beweis. Zunächst ist zu zeigen, dass S_p eine Untergruppe von G ist. Seien also $a, b \in S_p$, etwa $a^{p^{t'}} = 1$, $b^{p^{t''}} = 1$. Dann gilt für $t = \max(t', t'')$ aufgrund der Kommutativität von G

$$(ab^{-1})^{p^t} = a^{p^t} \cdot b^{-p^t} = 1,$$

und somit $ab^{-1} \in S_p$, d. h. S_p ist eine Untergruppe von G. Nach Konstruktion enthält S_p jede p-Untergruppe von G; denn S_p besteht aus allen Elementen von G, deren Ordnung eine p-Potenz ist. Wenn wir also zeigen, dass S_p eine p-Sylow-Gruppe in G ist, so ist diese auch eindeutig bestimmt.

Es bleibt somit noch nachzuweisen, dass S_p eine p-Sylow-Gruppe ist. Wir gehen mit Induktion nach $n = \operatorname{ord} G$ vor. Im Falle $n = 1$ ist nichts zu zeigen; sei also $n > 1$. Man wähle ein Element $x \neq 1$ in G. Indem wir x durch eine geeignete Potenz ersetzen, können wir annehmen, dass $q = \operatorname{ord} x$ prim ist. Man betrachte dann zu der von x erzeugten zyklischen Untergruppe $\langle x\rangle \subset G$ die Projektion $\pi\colon G \longrightarrow G' = G/\langle x\rangle$, wobei aufgrund des Satzes von Lagrange 1.2/3 die Gleichung $\operatorname{ord} G' = \frac{1}{q} \operatorname{ord} G$ gilt.

Ist $S'_p \subset G'$ die Untergruppe aller Elemente von G', deren Ordnung eine p-Potenz ist, so wissen wir nach Induktionsvoraussetzung, dass S'_p eine p-Sylow-Gruppe in G' ist. Weiter hat man $\pi(S_p) \subset S'_p$, und wir wollen zeigen, dass sogar $\pi(S_p) = S'_p$ gilt. Hierfür betrachte man ein Element $\overline{a} \in S'_p$ mit π-Urbild $a \in G$. Ist p^t die Ordnung von $\overline{a}$, so folgt $a^{p^t} \in \langle x\rangle$, also $a^{p^t q} = 1$. Für $p = q$ ergibt dies bereits $a \in S_p$. Andererseits existiert für $p \neq q$ aufgrund der Teilerfremdheit von p und q eine Gleichung $rp^t + sq = 1$ mit ganzen Zahlen r, s, und es folgt

$$\pi(a^{sq}) = \overline{a}^{sq} = \overline{a}^{rp^t}\overline{a}^{sq} = \overline{a}^{rp^t+sq} = \overline{a}$$

mit $a^{sq} \in S_p$, denn es gilt $a^{p^t q} = 1$. Wir sehen daher, dass π in jedem Falle eine surjektive Abbildung $\pi_p \colon S_p \longrightarrow S'_p$ induziert, und zwar mit $\ker \pi_p = \langle x \rangle \cap S_p$.

Gelte nun $n = \operatorname{ord} G = p^k m$ mit $p \nmid m$. Für $p = q$ hat man, wie oben berechnet, $\operatorname{ord} G' = \frac{1}{p} \operatorname{ord} G = p^{k-1}m$ sowie nach Induktionsvoraussetzung $\operatorname{ord} S'_p = p^{k-1}$. Da weiter in diesem Falle $\langle x \rangle \subset S_p$ und folglich $\ker \pi_p = \langle x \rangle$ gilt, induziert π_p einen Isomorphismus $S_p/\langle x \rangle \xrightarrow{\sim} S'_p$. Nach 1.2/3 ergibt sich $\operatorname{ord} S_p = p \cdot \operatorname{ord} S'_p = p^k$, und wir sehen, dass S_p eine p-Sylow-Gruppe in G ist. Sei nun $p \neq q$. Dann folgt entsprechend $\operatorname{ord} G' = p^k \cdot \frac{m}{q}$ und $\operatorname{ord} S'_p = p^k$. Da $\langle x \rangle$ kein Element enthalten kann, dessen Ordnung eine echte p-Potenz ist, hat man $\ker \pi_p = \langle x \rangle \cap S_p = \{1\}$ und folglich einen Isomorphismus $S_p \xrightarrow{\sim} S'_p$. Es ergibt sich deshalb $\operatorname{ord} S_p = \operatorname{ord} S'_p = p^k$, und S_p ist auch in diesem Falle eine p-Sylow-Gruppe in G. □

Im Allgemeinfall ist die Theorie der p-Gruppen bzw. p-Sylow-Gruppen komplizierter. p-Gruppen der Ordnung p sind zyklisch und damit abelsch. Auch p-Gruppen der Ordnung p^2 sind noch abelsch, wie wir sogleich in Satz 5 sehen werden. Diese Aussage lässt sich allerdings nicht auf p-Gruppen zu höheren p-Potenzen verallgemeinern. Stattdessen gilt:

Satz 3. *Es sei p prim und G eine p-Gruppe der Ordnung p^k, $k \geq 1$. Dann teilt p die Ordnung des Zentrums Z von G, insbesondere gilt also $Z \neq \{1\}$.*

Beweis. Man betrachte die Klassengleichung 5.1/9 für die Konjugationsoperation von G auf sich:

$$\operatorname{ord} G = \operatorname{ord} Z + \sum_{i=1}^{n} \big(G : Z_{\{x_i\}}\big)$$

Dabei sei $x_1, \ldots, x_n$ ein Vertretersystem der G-Bahnen in $G - Z$. Der Index $(G : Z_{\{x_i\}})$ ist nach 1.2/3 jeweils eine p-Potenz, da $\operatorname{ord} G$ eine p-Potenz ist. Es ist $(G : Z_{\{x_i\}})$ sogar eine echte p-Potenz, da $Z_{\{x_i\}}$ wegen $x_i \notin Z$ eine echte Untergruppe von G ist. Folglich erhält man $p \mid \operatorname{ord} Z$. □

Die Aussage des Satzes ist oftmals für Induktionsbeweise nutzbar, wir geben ein Beispiel:

Korollar 4. *Es sei p eine Primzahl und G eine p-Gruppe der Ordnung p^k. Dann gibt es eine absteigende Kette von Untergruppen*

$$G = G_k \supset G_{k-1} \supset \ldots \supset G_0 = \{1\},$$

derart dass $\operatorname{ord} G_\ell = p^\ell$ *gilt und $G_{\ell-1}$ für $\ell = 1, \ldots, k$ jeweils ein Normalteiler in G_ℓ ist.*[1]

Insbesondere existiert zu jedem Teiler p^ℓ von p^k eine p-Untergruppe $H \subset G$ mit $\operatorname{ord} H = p^\ell$, *und es besitzt G für $k \geq 1$ ein Element der Ordnung p.*

Beweis. Wir schließen mit Induktion nach k. Der Fall $k = 0$ ist trivial, gelte also $k > 0$. Dann ist das Zentrum $Z \subset G$ nach Satz 3 nicht trivial, und wir können ein Element $a \neq 1$ in Z wählen. Ist p^r dessen Ordnung, so hat $a^{p^{r-1}}$ die Ordnung p. Wir dürfen also ohne weiteres $\operatorname{ord} a = p$ annehmen. Da a im Zentrum von G liegt, ist die von a erzeugte Untergruppe $\langle a \rangle \subset G$ sogar ein Normalteiler in G. Dann besitzt $\overline{G} = G/\langle a \rangle$ gemäß 1.2/3 die Ordnung p^{k-1}, und wir können auf diese Gruppe die Induktionsvoraussetzung anwenden. Es existiert also eine Kette von Untergruppen

$$\overline{G} = \overline{G}_k \supset \overline{G}_{k-1} \supset \ldots \supset \overline{G}_1 = \{1\}, \qquad \operatorname{ord} \overline{G}_\ell = p^{\ell-1},$$

so dass $\overline{G}_{\ell-1}$ für $\ell = 2, \ldots, k$ jeweils ein Normalteiler in $\overline{G}_\ell$ ist. Man betrachte nun die Projektion $\pi\colon G \longrightarrow G/\langle a \rangle$ und setze $G_\ell = \pi^{-1}(\overline{G}_\ell)$ für $\ell = 1, \ldots, k$. Dann ist

$$G = G_k \supset G_{k-1} \supset \ldots \supset G_1 \supset \{1\}$$

offenbar eine Kette von Untergruppen in G mit den gewünschten Eigenschaften. □

Satz 5. *Es sei p eine Primzahl und G eine Gruppe der Ordnung p^2. Dann ist G abelsch. Genauer gilt*

$$G \simeq \mathbb{Z}/p^2\mathbb{Z} \quad \textit{oder} \quad G \simeq \mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z}.$$

Beweis. Wir zeigen zunächst, dass G abelsch ist. Aus Satz 3 ergibt sich $p \,|\, \operatorname{ord} Z$ für das Zentrum Z von G. Also ist die Ordnung von Z gleich p

[1] Die Quotienten $G_\ell/G_{\ell-1}$ sind von der Ordnung p und damit zyklisch sowie insbesondere abelsch. Jede endliche p-Gruppe G ist daher *auflösbar* im Sinne der Definition 5.4/3.

oder p^2. Im Falle $\operatorname{ord} Z = p^2$ gilt $G = Z$, d. h. G ist abelsch. Nehmen wir dagegen $\operatorname{ord} Z = p$ an, so kann G nicht abelsch sein. Allerdings ist dann G/Z zyklisch von der Ordnung p, so dass G nach 5.1/11 doch abelsch sein müsste im Widerspruch zu $\operatorname{ord} Z = p$.

Man benutze nun Korollar 4 und wähle ein Element $a \in G$ mit $\operatorname{ord} a = p$; sei $b \in G$ aus dem Komplement der von a erzeugten zyklischen Untergruppe $\langle a \rangle \subset G$. Dann hat b die Ordnung p oder p^2, wobei im letzteren Falle G von b erzeugt wird, also $G = \langle b \rangle \simeq \mathbb{Z}/p^2\mathbb{Z}$ gilt. Gelte deshalb $\operatorname{ord} b = p$. Wir behaupten, dass die Abbildung

$$\varphi\colon \langle a \rangle \times \langle b \rangle \longrightarrow G, \qquad (a^i, b^j) \longmapsto a^i b^j,$$

ein Gruppenisomorphismus ist. Zunächst ist φ ein Gruppenhomomorphismus, da G bereits als abelsch erkannt ist. Da weiter $\langle a \rangle \cap \langle b \rangle$ wegen $b \notin \langle a \rangle$ eine echte Untergruppe von $\langle b \rangle$ ist, hat man $\langle a \rangle \cap \langle b \rangle = \{1\}$, d. h. φ ist injektiv. Dann ist φ aber wegen

$$\operatorname{ord}\big(\langle a \rangle \times \langle b \rangle\big) = p^2 = \operatorname{ord} G$$

auch bijektiv, und mit $\langle a \rangle \simeq \mathbb{Z}/p\mathbb{Z} \simeq \langle b \rangle$ folgt $G \simeq \mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z}$. Alternativ hätten wir natürlich auch den Hauptsatz über endlich erzeugte abelsche Gruppen 2.9/9 anwenden können. □

Als Nächstes sollen die Sylowschen Sätze bewiesen werden, die wir in folgendem Theorem zusammenfassen:

Theorem 6 (Sylowsche Sätze). *Es sei G eine endliche Gruppe und p eine Primzahl.*

(i) *Es enthält G eine p-Sylow-Gruppe. Genauer existiert zu jeder p-Untergruppe $H \subset G$ eine p-Sylow-Gruppe $S \subset G$ mit $H \subset S$.*

(ii) *Ist $S \subset G$ eine p-Sylow-Gruppe, so auch jede zu S konjugierte Untergruppe von G. Umgekehrt sind je zwei p-Sylow-Gruppen in G zueinander konjugiert.*

(iii) *Für die Anzahl s der p-Sylow-Gruppen in G gilt*

$$s \mid \operatorname{ord} G, \qquad s \equiv 1 \mod (p).$$

Wir gliedern den Beweis des Theorems in einzelne Schritte auf und beginnen mit einem grundlegenden Lemma, welches wir im weiteren Sinne nach H. Wielandt [18] herleiten.

Lemma 7. *Es sei G eine endliche Gruppe der Ordnung $n = p^k m$, wobei p prim, aber nicht notwendig teilerfremd zu m sei. Dann gilt für die Anzahl s der p-Untergruppen $H \subset G$ mit* $\operatorname{ord} H = p^k$ *die Kongruenz*

$$s \equiv \binom{n-1}{p^k-1} = \frac{1}{m}\binom{n}{p^k} \mod (p).$$

Beweis. Wir bezeichnen mit X die Menge aller Teilmengen von G, welche aus genau p^k Elementen bestehen. Es gilt

$$\operatorname{ord} X = \binom{n}{p^k},$$

und G operiert auf X durch "Linkstranslation" vermöge

$$G \times X \longrightarrow X, \qquad (g, U) \longmapsto gU = \{gu\,;\, u \in U\}.$$

Abweichend von unserer bisherigen Notation werde die G-Bahn eines Elementes $U \in X$ im Folgenden mit $G(U)$ bezeichnet; G_U ist wie gewöhnlich die Isotropiegruppe zu U. Fasst man U im ursprünglichen Sinne als Teilmenge von G auf, so induziert die Linkstranslation von G auf sich selbst eine Aktion von G_U auf U. Es besteht daher U aus gewissen Rechtsnebenklassen von G_U in G. Diese sind paarweise disjunkt und besitzen alle genau $\operatorname{ord} G_U$ Elemente, so dass $\operatorname{ord} G_U$ notwendig ein Teiler von $\operatorname{ord} U = p^k$, also von der Form $p^{k'}$ mit $k' \leq k$ ist. Insbesondere ist U genau dann selbst eine Rechtsnebenklasse von G_U, wenn $\operatorname{ord} G_U = p^k$ gilt.

Es sei nun $(U_i)_{i\in I}$ ein System von Elementen aus X, welches ein Vertretersystem aller G-Bahnen von X bildet. Dann gilt aufgrund der Bahnengleichung 5.1/7

$$\binom{n}{p^k} = \operatorname{ord} X = \sum_{i\in I} \operatorname{ord} G(U_i) = \sum_{i\in I} (G : G_{U_i}).$$

Wir wollen diese Gleichung weiter auswerten, indem wir modulo (pm) rechnen. Wie wir gesehen haben, ist G_{U_i} eine p-Gruppe einer Ordnung p^{k_i} mit $k_i \leq k$, wobei der Satz von Lagrange 1.2/3 dann $(G : G_{U_i}) = p^{k-k_i} m$ ergibt. Setzen wir nun $I' = \{i \in I\,;\, k_i = k\}$, so folgt

$$(\operatorname{ord} I') \cdot m = \sum_{i\in I'} (G : G_{U_i}) \equiv \binom{n}{p^k} \mod (pm),$$

und es genügt zum Beweis des Lemmas zu zeigen, dass ord I' mit der Anzahl s aller p-Untergruppen $H \subset G$ der Ordnung p^k übereinstimmt. Denn dann erhalten wir $s \equiv \frac{1}{m}\binom{n}{p^k} \bmod (p)$, wobei die Gleichheit $\binom{n-1}{p^k-1} = \frac{1}{m}\binom{n}{p^k}$ aufgrund der Zerlegung $n = p^k m$ besteht.

Um ord $I' = s$ nachzuweisen, erinnern wir uns daran, dass ein Index $i \in I$ genau dann zu I' gehört, wenn ord $G(U_i) = (G : G_{U_i}) = m$ gilt, die Bahn $G(U_i)$ also aus genau m Elementen besteht. Man kann nun für p-Untergruppen $H \subset G$ der Ordnung p^k die G-Bahn $G(H) \subset X$ betrachten; diese besteht jeweils aus den Linksnebenklassen von H in G, also aufgrund des Satzes von Lagrange 1.2/3 aus genau m Elementen. Verschiedene solche Untergruppen $H, H' \subset G$ geben dabei zu verschiedenen G-Bahnen Anlass, denn aus $gH = H'$ für ein Element $g \in G$ folgt wegen $1 \in H'$ unmittelbar $g \in H$ und damit $H = H'$. Andererseits kann man leicht einsehen, dass jede G-Bahn $G(U_i)$, $i \in I'$, vom Typ $G(H)$ mit einer p-Untergruppe $H \subset G$ der Ordnung p^k ist. Für $i \in I'$ gilt nämlich ord $G_{U_i} = p^k$, und es ist, wie wir oben gesehen haben, U_i eine Rechtsnebenklasse von G_{U_i} in G, etwa $U_i = G_{U_i} \cdot u_i$ mit $u_i \in U_i$. Für die G-Bahn von U_i in X folgt dann

$$G(U_i) = G(u_i^{-1} \cdot U_i) = G(u_i^{-1} \cdot G_{U_i} \cdot u_i),$$

wobei nunmehr $H = u_i^{-1} \cdot G_{U_i} \cdot u_i$ eine p-Untergruppe in G der Ordnung p^k ist. Somit entsprechen die Elemente $i \in I'$ in bijektiver Weise den p-Untergruppen $H \subset G$ der Ordnung p^k, und die Aussage des Lemmas ist bewiesen. □

In einer zyklischen Gruppe der Ordnung n gibt es zu jedem Teiler d von n genau eine Untergruppe der Ordnung d; vgl. 1.3, Aufgabe 2 und deren Lösung im Anhang. Somit ergibt sich in der Situation von Lemma 7 die nicht-triviale Relation

$$\binom{n-1}{p^k-1} = \frac{1}{m}\binom{n}{p^k} \equiv 1 \mod (p),$$

und wir erhalten folgende partielle Verallgemeinerung von Korollar 4:

Satz 8. *Es sei G eine endliche Gruppe und p^k eine Primpotenz, welche ein Teiler von* ord G *ist. Weiter bezeichne s die Anzahl der p-Untergruppen $H \subset G$ der Ordnung p^k. Dann gilt $s \equiv 1 \bmod (p)$ und folglich $s \neq 0$.*

Ist k maximal mit $p^k \mid \operatorname{ord} G$, so folgt, dass G mindestens eine p-Sylow-Gruppe enthält, wobei die Anzahl dieser Untergruppen kongruent 1 modulo p ist; siehe Aufgabe 4 für einen alternativen Beweis dieses Resultats.

Lemma 9. *Es sei G eine endliche Gruppe, $H \subset G$ eine p-Untergruppe und $S \subset G$ eine p-Sylow-Gruppe. Dann existiert ein Element $g \in G$ mit $H \subset gSg^{-1}$.*

Beweis. Wir versehen die Menge G/S der Linksnebenklassen von S in G mit der H-Aktion

$$H \times G/S \longrightarrow G/S, \qquad (h, gS) \longmapsto (hg)S,$$

und wenden den Satz von Lagrange 1.2/3 in Verbindung mit 5.1/6 und der Bahnengleichung 5.1/7 an. Da es sich bei H um eine p-Gruppe handelt, ist die Ordnung einer jeden H-Bahn in G/S als Teiler von $\operatorname{ord} H$ eine p-Potenz. Da andererseits aber p kein Teiler von $\operatorname{ord} G/S$ sein kann, muss es mindestens eine H-Bahn geben, deren Ordnung p^0, also 1 ist. Dann besteht diese H-Bahn aus genau einer Nebenklasse gS, und es gilt $hgS = gS$ für alle $h \in H$, woraus wegen $1 \in S$ sofort $hg \in gS$ bzw. $h \in gSg^{-1}$ und damit $H \subset gSg^{-1}$ folgt. □

Da die Abbildung $G \longrightarrow G$, $x \longmapsto gxg^{-1}$, für $g \in G$ ein Automorphismus ist, folgt in der Situation von Lemma 9 unmittelbar, dass mit S auch gSg^{-1} eine p-Sylow-Gruppe in G ist. Ist $H \subset G$ eine weitere p-Sylow-Gruppe, so ergibt sich aus der Inklusion $H \subset gSg^{-1}$ wegen $\operatorname{ord} H = \operatorname{ord} S = \operatorname{ord} gSg^{-1}$ bereits $H = gSg^{-1}$, so dass Satz 8 und Lemma 9 insgesamt die Behauptungen von Theorem 6 implizieren, abgesehen von der Aussage $s \mid \operatorname{ord} G$ in (iii). Dieser noch fehlende Teil ergibt sich aber unter Benutzung des Satzes von Lagrange 1.2/3 aus folgendem Resultat:

Lemma 10. *Es sei G eine endliche Gruppe und S eine p-Sylow-Gruppe in G. Bezeichnet dann N_S den Normalisator von S in G, so gibt der Index $(G : N_S)$ gerade die Anzahl der p-Sylow-Gruppen in G an.*

Beweis. Es sei X die Menge der p-Sylow-Gruppen in G. Da alle p-Sylow-Gruppen zueinander konjugiert sind, ist die Konjugationsoperation

$$G \times X \longrightarrow X, \qquad (g, S') \longmapsto gS'g^{-1},$$

transitiv. Insbesondere gilt nach 5.1/6

$$\operatorname{ord} X = (G : G_S),$$

und es stimmt G_S als Isotropiegruppe bezüglich der Konjugationsoperation mit dem Normalisator N_S überein. □

Die Sylowschen Sätze in der Form von Theorem 6 sind damit bewiesen. Wir wollen nun noch einige Folgerungen aus diesen Sätzen ziehen.

Korollar 11. *Es sei G eine endliche Gruppe und p eine Primzahl. Dann gilt*:

(i) *Für $p \mid \operatorname{ord} G$ enthält G ein Element der Ordnung p.*

(ii) *G ist genau dann eine p-Gruppe, wenn es zu jedem $a \in G$ ein $t \in \mathbb{N}$ mit $a^{p^t} = 1$ gibt.*

(iii) *Eine Untergruppe $H \subset G$ ist genau dann eine p-Sylow-Gruppe, wenn sie maximale p-Gruppe in G ist.*

Beweis. Behauptung (i) ist eine Konsequenz von Satz 8 oder auch von Theorem 6 (i) in Verbindung mit Korollar 4.

Zum Nachweis von (ii) nehme man an, dass jedes Element $a \in G$ eine p-Potenz als Ordnung besitzt. Ist $\operatorname{ord} G$ keine p-Potenz, so wähle man eine von p verschiedene Primzahl q, welche $\operatorname{ord} G$ teilt. Wie wir gesehen haben, enthält G dann ein Element der Ordnung q, im Widerspruch zu unserer Annahme. Also ist $\operatorname{ord} G$ eine p-Potenz und damit G eine p-Gruppe. Umgekehrt hat natürlich jedes $a \in G$ eine p-Potenz als Ordnung, wenn G eine p-Gruppe ist, da die Ordnung eines Elementes $a \in G$ aufgrund des Satzes von Lagrange 1.2/3 ein Teiler von $\operatorname{ord} G$ ist.

Ebenfalls sieht man mit 1.2/3, dass jede p-Sylow-Gruppe in G eine maximale p-Untergruppe ist. Die Umkehrung hierzu folgt aus Theorem 6 (i), so dass auch Behauptung (iii) klar ist. □

Bei kleinen Gruppenordnungen sind die unter Theorem 6 (iii) genannten Bedingungen für die Anzahl der p-Sylow-Gruppen oftmals ausreichend, um Informationen zur Struktur einer Gruppe G zu erhalten. Gibt es z. B. zu einer Primzahl p nur eine einzige p-Sylow-Gruppe in G, so ist dies automatisch ein Normalteiler, da alle p-Sylow-Gruppen zueinander konjugiert sind. Wir gehen nachfolgend auf einen einfachen Fall einer solchen Argumentation ein, die sich beispielsweise auf Gruppen der Ordnung 15 anwenden lässt.

Satz 12. *Es seien p, q Primzahlen mit $p < q$ und $p \nmid (q-1)$. Dann ist jede Gruppe G der Ordnung pq zyklisch.*

Beweis. Sei s die Anzahl der p-Sylow-Gruppen in G. Dann gilt $s \mid \operatorname{ord} G$ bzw. $s \mid pq$ sowie $s \equiv 1(p)$ nach Theorem 6 (iii). Letzteres bedeutet $p \nmid s$ und somit $s \mid q$. Da $q = s \equiv 1(p)$ wegen $p \nmid (q-1)$ ausgeschlossen ist, gilt notwendig $s = 1$. Es gibt also genau eine p-Sylow-Gruppe S_p in G. Diese ist invariant unter Konjugation mit Elementen aus G und daher ein Normalteiler in G. Ist s' die Anzahl der q-Sylow-Gruppen in G, so folgt entsprechend $s' \mid p$. Der Fall $s' = p$ scheidet wieder aus, da $p = s' \equiv 1(q)$ nicht mit $p < q$ vereinbar wäre. Also gilt $s' = 1$, und es existiert genau eine q-Sylow-Gruppe S_q in G. Diese ist ebenfalls ein Normalteiler in G. Da S_p und S_q nur die triviale Gruppe $\{1\}$ als echte Untergruppe besitzen, gilt $S_p \cap S_q = \{1\}$.

Wir behaupten nun, dass die Abbildung

$$\varphi\colon S_p \times S_q \longrightarrow G, \qquad (a,b) \longmapsto ab,$$

ein Isomorphismus von Gruppen ist. Dann ist G, etwa nach dem Chinesischen Restsatz in der Version 2.4/14, als kartesisches Produkt zweier zyklischer Gruppen teilerfremder Ordnungen selbst wieder zyklisch. Zunächst müssen wir zeigen, dass φ ein Gruppenhomomorphismus ist. Es gilt für $a \in S_p$, $b \in S_q$

$$aba^{-1}b^{-1} = (aba^{-1})b^{-1} \in S_q,$$

aber auch

$$aba^{-1}b^{-1} = a(ba^{-1}b^{-1}) \in S_p.$$

Somit hat man

$$aba^{-1}b^{-1} \in S_p \cap S_q = \{1\}$$

und deshalb $ab = ba$. Elemente aus S_p kommutieren also mit Elementen aus S_q.

Für $a, a' \in S_p$ und $b, b' \in S_q$ gilt daher

$$\begin{aligned}\varphi\big((a,b)\cdot(a',b')\big) &= \varphi(aa', bb') = aa'bb' \\ &= aba'b' = \varphi(a,b)\cdot\varphi(a',b'),\end{aligned}$$

d. h. φ ist Gruppenhomomorphismus. Wegen $S_p \cap S_q = \{1\}$ ist φ injektiv und sogar bijektiv, denn die Ordnungen von $S_p \times S_q$ und G sind gleich. □

Lernkontrolle und Prüfungsvorbereitung

1. Sei p eine Primzahl. Wann nennt man eine endliche Gruppe G eine p-Gruppe? Was versteht man unter einer p-Sylow-Gruppe in G?
2. Wie lassen sich für eine endliche abelsche Gruppe G deren p-Sylow-Gruppen beschreiben (mit Begründung)?
3. Sei G eine nicht-triviale p-Gruppe. Zeige, dass das Zentrum Z von G nicht-trivial ist.
4. Sei G eine p-Gruppe. Zeige, dass es zu jedem Teiler n von $\operatorname{ord} G$ eine Untergruppe $H \subset G$ der Ordnung n gibt.
5. Sei G eine Gruppe der Ordnung p^2. Zeige, dass G abelsch ist.
6. Wie lauten die Sylowschen Sätze?

+7. Wie lautet das fundamentale Lemma zum Beweis der Sylowschen Sätze, welches die Anzahl der p-Untergruppen $H \subset G$ gegebener Ordnung klärt? Skizziere dessen Beweis.

+8. Erkläre den Beweis der Sylowschen Sätze unter Nutzung von Punkt 7.

9. Zeige, dass eine Untergruppe H einer Gruppe G genau dann eine p-Sylow-Gruppe ist, wenn H eine maximale p-Gruppe in G ist.
10. Seien p, q Primzahlen mit $p < q$ und $p \nmid (q-1)$. Zeige, dass jede Gruppe der Ordnung pq zyklisch ist.

Übungsaufgaben

1. *Welche Informationen liefern die Sylowschen Sätze im Falle endlicher abelscher Gruppen.*
2. *Es sei $\varphi\colon G \longrightarrow G'$ ein Homomorphismus endlicher Gruppen. Versuche, Beziehungen zwischen den Sylow-Gruppen in G und denjenigen in G' herzustellen.*
3. Es sei G eine endliche Gruppe und $H \subset G$ eine p-Untergruppe für eine Primzahl p. Zeige: Ist H ein Normalteiler in G, so ist H in jeder p-Sylow-Gruppe von G enthalten.
4. Sei G eine endliche Gruppe. Zeige mittels eines alternativen Arguments, dass $s \equiv 1 \mod (p)$ für die Anzahl s der p-Sylow-Gruppen in G gilt. (*Hinweis*: Sei X die Menge der p-Sylow-Gruppen in G. Zeige $X \neq \emptyset$ mittels Lemma 7 und wähle $S \in X$. Zeige, dass S der einzige Fixpunkt unter der Konjugationsoperation von S auf X ist. Wende dazu Lemma 9 an.)

5. Es sei $\mathrm{GL}(n, K)$ die Gruppe der invertierbaren $(n \times n)$-Matrizen über einem endlichen Körper K der Charakteristik $p > 0$. Zeige, dass die oberen Dreiecksmatrizen, deren Diagonalelemente sämtlich 1 sind, eine p-Sylow-Gruppe in $\mathrm{GL}(n, K)$ bilden.
6. Zeige, dass jede Gruppe der Ordnung 30 bzw. 56 eine nicht-triviale normale Sylow-Gruppe besitzt.
7. Zeige, dass jede Gruppe der Ordnung 45 abelsch ist.
8. Zeige, dass jede Gruppe G der Ordnung 36 einen nicht-trivialen Normalteiler besitzt. (*Hinweis*: Betrachte die Aktion von G auf der Menge der 3-Sylow-Gruppen in G.)
9. Zeige, dass jede Gruppe G mit $\operatorname{ord} G < 60$ zyklisch ist oder einen nicht-trivialen Normalteiler besitzt.

5.3 Permutationsgruppen

Wir wollen im Folgenden für $n \in \mathbb{N}$ die Gruppe $\mathfrak{S}_n$ der bijektiven Selbstabbildungen von $\{1, \ldots, n\}$ etwas genauer untersuchen. Die Fälle $n = 0$ und $n = 1$ sind dabei formal nicht ausgeschlossen, haben aber keinerlei besondere Bedeutung. $\mathfrak{S}_0$ besteht als Gruppe der bijektiven Selbstabbildungen der leeren Menge nur aus dem Einselement, genau wie auch $\mathfrak{S}_1$ als Gruppe der bijektiven Selbstabbildungen einer einelementigen Menge.

Wie wir bereits wissen, bezeichnet man $\mathfrak{S}_n$ auch als *symmetrische Gruppe* oder *Permutationsgruppe* von $\{1, \ldots, n\}$, wobei $\operatorname{ord} \mathfrak{S}_n = n!$ gilt und $\mathfrak{S}_n$ in natürlicher Weise auf $\{1, \ldots, n\}$ operiert. Elemente $\pi \in \mathfrak{S}_n$ schreibt man häufig in der Form

$$\begin{pmatrix} 1 & \ldots & n \\ \pi(1) & \ldots & \pi(n) \end{pmatrix},$$

insbesondere dann, wenn die Bilder $\pi(1), \ldots, \pi(n)$ in expliziter Weise gegeben sind. Eine Permutation $\pi \in \mathfrak{S}_n$ heißt ein *Zyklus*, wenn es paarweise verschiedene Zahlen $x_1, \ldots, x_r \in \{1, \ldots, n\}$ gibt, $r \geq 2$, mit

$$\begin{aligned} \pi(x_i) &= x_{i+1} \quad \text{für} \quad 1 \leq i < r, \\ \pi(x_r) &= x_1, \\ \pi(x) &= x \quad \text{für} \quad x \in \{1, \ldots, n\} - \{x_1, \ldots, x_r\}. \end{aligned}$$

In dieser Situation nennt man π genauer einen *r-Zyklus* und verwendet für π die Schreibweise $(x_1, \ldots, x_r)$. Zwei Zyklen $(x_1, \ldots, x_r)$ und $(y_1, \ldots, y_s)$ heißen *fremd*, wenn

$$\{x_1, \ldots, x_r\} \cap \{y_1, \ldots, y_s\} = \emptyset$$

gilt. Ein 2-Zyklus heißt auch *Transposition*.

Satz 1. *Sei $n \geq 2$.*

(i) *Sind $\pi_1, \pi_2 \in \mathfrak{S}_n$ fremde Zyklen, so gilt $\pi_1 \circ \pi_2 = \pi_2 \circ \pi_1$.*

(ii) *Jedes $\pi \in \mathfrak{S}_n$ ist Produkt paarweise fremder Zyklen. Diese sind eindeutig durch π bestimmt (bis auf die Reihenfolge).*

(iii) *Jedes $\pi \in \mathfrak{S}_n$ ist Produkt von Transpositionen.*

Beweis. Aussage (i) ist trivial. In der Situation von (ii) sei $H = \langle \pi \rangle$ die von π erzeugte zyklische Untergruppe von $\mathfrak{S}_n$. Die natürliche Operation von H auf $\{1, \ldots, n\}$ liefert eine Unterteilung in disjunkte Bahnen. Seien $B_1, \ldots, B_\ell$ diejenigen unter diesen Bahnen, die aus mindestens zwei Elementen bestehen, also mit $r_\lambda = \operatorname{ord} B_\lambda \geq 2$. Wählt man dann jeweils $x_\lambda \in B_\lambda$, so erhält man

$$B_\lambda = \left\{x_\lambda, \pi(x_\lambda), \ldots, \pi^{r_\lambda - 1}(x_\lambda)\right\}$$

und

$$\pi = \prod_{\lambda=1}^{\ell} \left(x_\lambda, \pi(x_\lambda), \ldots, \pi^{r_\lambda - 1}(x_\lambda)\right),$$

also eine Zerlegung von π in paarweise fremde Zyklen, wobei die Reihenfolge bei der Produktbildung gemäß (i) ohne Belang ist. Umgekehrt ist leicht zu erkennen, dass jede Darstellung von π als Produkt paarweise fremder Zyklen in der gerade beschriebenen Art zu der Zerlegung von $\{1, \ldots, n\}$ in seine H-Bahnen korrespondiert. Hieraus folgt die Eindeutigkeitsaussage.

Aussage (iii) schließlich ergibt sich mit Hilfe der Zerlegung

$$(x_1, \ldots, x_r) = (x_1, x_2) \circ (x_2, x_3) \circ \ldots \circ (x_{r-1}, x_r)$$

aus (ii). □

Für eine Permutation $\pi \in \mathfrak{S}_n$ definiert man das *Signum* durch

$$\operatorname{sgn} \pi = \prod_{i<j} \frac{\pi(i) - \pi(j)}{i - j} \,.$$

Das Signum kann die Werte 1 und -1 annehmen. Es heißt π eine *gerade* oder *ungerade* Permutation, je nachdem ob $\operatorname{sgn}\pi$ positiv oder negativ ist. Bei der Bildung des Signums wird sozusagen in multiplikativer Weise modulo 2 gezählt, für wie viele 2-elementige Teilmengen $\{i,j\} \subset \{1,\dots,n\}$ die Abbildung π die zwischen i und j bestehende Größenrelation umkehrt. Das obige Produkt darf daher allgemeiner über irgendeine Menge I von Paaren (i,j) natürlicher Zahlen mit $1 \le i,j \le n$ gebildet werden, mit der Maßgabe, dass die Zuordnung $(i,j) \longmapsto \{i,j\}$ eine Bijektion zwischen I und der Menge der 2-elementigen Teilmengen von $\{1,\dots,n\}$ definiert.

Bemerkung 2. *Die Abbildung* $\operatorname{sgn}\colon \mathfrak{S}_n \longrightarrow \{1,-1\}$ *ist ein Gruppenhomomorphismus.*

Beweis. Seien $\pi,\pi' \in \mathfrak{S}_n$. Dann gilt

$$\begin{aligned}\operatorname{sgn}\pi\circ\pi' &= \prod_{i<j} \frac{\pi\circ\pi'(i)-\pi\circ\pi'(j)}{i-j}\\ &= \prod_{i<j} \frac{\pi\circ\pi'(i)-\pi\circ\pi'(j)}{\pi'(i)-\pi'(j)} \cdot \frac{\pi'(i)-\pi'(j)}{i-j}\\ &= \operatorname{sgn}\pi\cdot\operatorname{sgn}\pi'.\end{aligned}$$

□

Für eine Transposition aus $\mathfrak{S}_n$ berechnet sich das Signum zu -1. Zerlegen wir daher eine Permutation $\pi \in \mathfrak{S}_n$ gemäß Satz 1 (iii) in ein Produkt von Transpositionen, etwa $\pi = \tau_1 \circ \ldots \circ \tau_\ell$, so gilt $\operatorname{sgn}\pi = (-1)^\ell$, und die Restklasse von ℓ modulo 2 ist eindeutig durch π bestimmt. Insbesondere ist π eine gerade oder ungerade Permutation, je nachdem ob π ein Produkt einer geraden oder ungeraden Anzahl von Transpositionen ist. Aus Bemerkung 2 folgt weiter, dass

$$\mathfrak{A}_n = \ker\operatorname{sgn} = \big\{\pi \in \mathfrak{S}_n\,;\ \operatorname{sgn}\pi = 1\big\},$$

die Menge der geraden Permutationen, für $n > 1$ einen Normalteiler vom Index 2 in $\mathfrak{S}_n$ bildet. Man nennt $\mathfrak{A}_n$ die *alternierende Gruppe*.

Satz 3. *Für* $n \ge 3$ *besteht* $\mathfrak{A}_n$ *aus allen Permutationen* $\pi \in \mathfrak{S}_n$, *die sich als Produkt von* 3*-Zyklen schreiben lassen.*

Beweis. Seien $x_1, x_2, x_3, x_4 \in \{1, \ldots, n\}$. Sind dann x_1, x_2, x_3 paarweise verschieden, so hat man die Formel

$$(x_1, x_2) \circ (x_2, x_3) = (x_1, x_2, x_3).$$

Sind weiter x_1, x_2, x_3, x_4 paarweise verschieden, so gilt

$$(x_1, x_2) \circ (x_3, x_4) = (x_1, x_3, x_2) \circ (x_1, x_3, x_4).$$

Die erste Gleichung impliziert, dass jeder 3-Zyklus zu $\mathfrak{A}_n$ gehört und damit auch jedes Produkt von 3-Zyklen. Beide Gleichungen zusammen zeigen, dass jedes Produkt einer geraden Anzahl von Transpositionen, also jedes Element von $\mathfrak{A}_n$, ein Produkt von 3-Zyklen ist. □

Wir wollen nun noch einige konkrete Permutationsgruppen bzw. Untergruppen von Permutationsgruppen diskutieren.

(1) Zunächst ist $\mathfrak{S}_2$ eine Gruppe der Ordnung 2; daher ergibt sich $\mathfrak{S}_2 \simeq \mathbb{Z}/2\mathbb{Z}$.

(2) Die Gruppe $\mathfrak{S}_3$ hat die Ordnung 6. Man kann sie interpretieren als *Diedergruppe* D_3, d. h. als Gruppe der Spiegelungen und Drehungen eines gleichseitigen Dreiecks (3 Drehungen, 3 Spiegelungen). Es enthält $\mathfrak{S}_3$ nur Elemente der Ordnung 1, 2 und 3, aber kein Element der Ordnung 6. Folglich ist $\mathfrak{S}_3$ eine von der zyklischen Gruppe $\mathbb{Z}/6\mathbb{Z}$ verschiedene Gruppe. Da jede abelsche Gruppe der Ordnung 6 zu dem Produkt $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}$ isomorph und somit aufgrund des Chinesischen Restsatzes 2.4/14 zyklisch ist, erkennt man $\mathfrak{S}_3$ als nicht-abelsche Gruppe der Ordnung 6 (was man natürlich auch in direkter Weise nachprüfen kann).

(3) Für $n \geq 3$ erklärt man die *Diedergruppe* D_n als Gruppe der Bewegungen eines regelmäßigen n-Ecks. Nummeriert man dessen Eckpunkte fortlaufend mit $1, \ldots, n$, so wird D_n als Untergruppe von $\mathfrak{S}_n$ von den Permutationen

$$\sigma = (1, \ldots, n), \qquad \tau = \begin{pmatrix} 1 & 2 & 3 & \ldots & n \\ 1 & n & n-1 & \ldots & 2 \end{pmatrix}$$

erzeugt. Hierbei entspricht σ einer Drehung des regelmäßigen n-Ecks um den Winkel $2\pi/n$ und τ einer Spiegelung an der Symmetrieachse durch den Punkt 1. Es gilt $\operatorname{ord} D_n = 2n$; die von σ erzeugte zyklische Untergruppe

von D_n ist ein Normalteiler vom Index 2. In ähnlicher Weise definiert man Bewegungsgruppen für Tetraeder, Würfel, Oktaeder, Dodekaeder und Ikosaeder.

(4) Im Hinblick auf spätere Anwendungen wollen wir noch die sogenannte *Kleinsche Vierergruppe* $\mathfrak{V}_4 \subset \mathfrak{S}_4$ einführen:

$$\mathfrak{V}_4 = \big\{\mathrm{id},\ (1,2)(3,4),\ (1,3)(2,4),\ (1,4)(2,3)\big\}$$

Es gilt

$$\mathfrak{V}_4 \subset \mathfrak{A}_4 \subset \mathfrak{S}_4,$$

wobei man leicht nachprüft, vgl. Aufgabe 6, dass $\mathfrak{V}_4$ ein Normalteiler in $\mathfrak{S}_4$ ist. Im Übrigen ist $\mathfrak{V}_4$ isomorph zu $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$.

Lernkontrolle und Prüfungsvorbereitung

1. Definiere die symmetrische Gruppe $\mathfrak{S}_n$ zu einem Index $n \in \mathbb{N}$. Erkläre auch die Bezeichnungen "Zyklus" und "Transposition".
2. Zeige, dass $\mathfrak{S}_n$ die Ordnung $n!$ besitzt.
3. Zeige, dass jede Permutation $\pi \in \mathfrak{S}_n$ ein Produkt von Transpositionen ist.
4. Definiere das Signum $\operatorname{sgn}\pi$ einer Permutation $\pi \in \mathfrak{S}_n$ und erkläre, wie sich dieses berechnen lässt.
5. Definiere die alternierende Gruppe $\mathfrak{A}_n$ und zeige, dass diese für $n > 1$ einen Normalteiler vom Index 2 in $\mathfrak{S}_n$ bildet.
6. Zeige, dass $\mathfrak{A}_n$ für $n \geq 3$ aus allen Permutationen $\pi \in \mathfrak{S}_n$ besteht, die sich als Produkt von 3-Zyklen schreiben lassen.
7. Erläutere einige mögliche geometrische Interpretationen für Permutationsgruppen und deren Untergruppen und zeige insbesondere, dass $\mathfrak{S}_3$ nicht abelsch ist.
8. Definiere die Kleinsche Vierergruppe $\mathfrak{V}_4 \subset \mathfrak{S}_4$ und zeige, dass diese einen Normalteiler vom Index 3 in $\mathfrak{A}_4$ und vom Index 6 in $\mathfrak{S}_4$ bildet, sowie isomorph zu $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ ist.

Übungsaufgaben

1. *Transpositionen in $\mathfrak{S}_n$ werden auch als Vertauschungen bezeichnet. Zeige in direkter Weise, dass für $n \geq 2$ jedes $\pi \in \mathfrak{S}_n$ als Produkt von Transpositionen geschrieben werden kann.*
2. *Gib für eine Primzahl p explizit eine p-Sylow-Gruppe in $\mathfrak{S}_p$ an.*

3. Es sei $\pi \in \mathfrak{S}_n$ ein r-Zyklus. Zeige $\operatorname{sgn}\pi = (-1)^{r-1}$.

4. Für eine Permutation $\pi \in \mathfrak{S}_n$ bezeichne $\langle\pi\rangle \subset \mathfrak{S}_n$ die zugehörige zyklische Untergruppe. Weiter sei m die Anzahl der $\langle\pi\rangle$-Bahnen bezüglich der natürlichen Aktion von $\langle\pi\rangle$ auf $\{1,\dots n\}$. Zeige: $\operatorname{sgn}\pi = (-1)^{n-m}$.

5. Schreibe die folgenden Permutationen als Produkt von Zyklen und berechne jeweils das Signum:

$$\begin{pmatrix}1&2&3&4\\3&4&1&2\end{pmatrix} \in \mathfrak{S}_4, \qquad \begin{pmatrix}1&2&3&4&5&6&7&8\\3&1&4&5&2&6&8&7\end{pmatrix} \in \mathfrak{S}_8.$$

6. Betrachte einen r-Zyklus $\pi = (x_1,\dots,x_r) \in \mathfrak{S}_n$ und zeige für beliebiges $\sigma \in \mathfrak{S}_n$

$$\sigma \circ \pi \circ \sigma^{-1} = \big(\sigma(x_1),\dots,\sigma(x_r)\big).$$

   Folgere als Anwendung, dass die Kleinsche Vierergruppe ein Normalteiler in $\mathfrak{S}_4$ ist.

7. Zeige für $n \geq 2$, dass die Zyklen $(1,2)$ und $(1,2,\dots,n)$ die Gruppe $\mathfrak{S}_n$ erzeugen.

8. Zeige für $n \geq 3$, dass die alternierende Gruppe $\mathfrak{A}_n$ von den Zyklen $(1,2,3)$, $(1,2,4),\dots,(1,2,n)$ erzeugt wird. Folgere hieraus, dass ein Normalteiler $N \subset \mathfrak{A}_n$, welcher einen 3-Zyklus enthält, bereits mit $\mathfrak{A}_n$ übereinstimmt.

5.4 Auflösbare Gruppen

Zur Charakterisierung auflösbarer Gruppen wollen wir den Begriff des Kommutators verwenden. Sind a, b zwei Elemente einer Gruppe G, so bezeichnet man $[a,b] = aba^{-1}b^{-1}$ als den *Kommutator* von a und b. In ähnlicher Weise können wir für zwei Untergruppen $H, H' \subset G$ den Kommutator $[H,H']$ bilden, indem wir die von allen Kommutatoren $[a,b]$ mit $a \in H$, $b \in H'$ *erzeugte* Untergruppe in G betrachten. Speziell für $H = H' = G$ erhält man die sogenannte *Kommutatorgruppe* $[G,G]$ von G. Es ist G genau dann abelsch, wenn $[G,G] = \{1\}$ gilt.

Bemerkung 1. (i) *Es besteht* $[G,G]$ *aus allen* (*endlichen*) *Produkten von Kommutatoren aus* G.

(ii) $[G,G]$ *ist ein Normalteiler in* G, *und zwar der kleinste unter allen Normalteilern* $N \subset G$, *so dass* G/N *abelsch ist.*

Beweis. Für $a, b \in G$ gilt

$$[a,b]^{-1} = (aba^{-1}b^{-1})^{-1} = bab^{-1}a^{-1} = [b,a].$$

Daher bilden die endlichen Produkte von Kommutatoren eine Untergruppe von G, und zwar die Kommutatorgruppe $[G,G]$. Weiter hat man für $a, b, g \in G$

$$\begin{aligned} g[a,b]g^{-1} &= gaba^{-1}b^{-1}g^{-1} = (gag^{-1})(gbg^{-1})(gag^{-1})^{-1}(gbg^{-1})^{-1} \\ &= [gag^{-1}, gbg^{-1}]. \end{aligned}$$

Dies zeigt, dass $[G,G]$ ein Normalteiler in G ist. Bezeichnen wir für $x \in G$ mit $\overline{x}$ jeweils die Restklasse in $G/[G,G]$, so zeigt die Gleichung

$$\overline{a} \cdot \overline{b} \cdot \overline{a}^{-1} \cdot \overline{b}^{-1} = \overline{aba^{-1}b^{-1}} = 1,$$

dass $G/[G,G]$ abelsch ist. Ist $N \subset G$ ein Normalteiler mit der Eigenschaft, dass G/N abelsch ist, so enthält N notwendigerweise alle Kommutatoren $[a,b]$ von Elementen $a, b \in G$. Dann gilt aber $[G,G] \subset N$, d. h. es ist $[G,G]$ der kleinste aller Normalteiler $N \subset G$ mit der Eigenschaft, dass G/N abelsch ist. □

Wir wollen einige spezielle Kommutatoren berechnen, die wir später benötigen werden.

Bemerkung 2. *Es gilt*:

$$[\mathfrak{S}_n, \mathfrak{S}_n] = \mathfrak{A}_n \text{ für } n \geq 2,$$

$$[\mathfrak{A}_n, \mathfrak{A}_n] = \begin{cases} \{1\} & \text{für } n = 2, 3, \\ \mathfrak{V}_4 & \text{für } n = 4, \\ \mathfrak{A}_n & \text{für } n \geq 5. \end{cases} \qquad \text{(Kleinsche Vierergruppe)}$$

Beweis. Wir beginnen mit der Berechnung von $[\mathfrak{S}_n, \mathfrak{S}_n]$. Die Faktorgruppe $\mathfrak{S}_n/\mathfrak{A}_n \simeq \mathbb{Z}/2\mathbb{Z}$ ist abelsch. Folglich hat man $[\mathfrak{S}_n, \mathfrak{S}_n] \subset \mathfrak{A}_n$ nach Bemerkung 1 und insbesondere $[\mathfrak{S}_2, \mathfrak{S}_2] = \mathfrak{A}_2$ wegen $\mathfrak{A}_2 = \{1\}$. Zum Nachweis der Inklusion $[\mathfrak{S}_n, \mathfrak{S}_n] \supset \mathfrak{A}_n$ für $n \geq 3$ benutzen wir, dass jedes Element aus $\mathfrak{A}_n$ ein Produkt von 3-Zyklen ist, vgl. 5.3/3. Jeder 3-Zyklus $(x_1, x_2, x_3) \in \mathfrak{S}_n$ ist aber aufgrund der Gleichung

$$(x_1, x_2, x_3) = (x_1, x_3)(x_2, x_3)(x_1, x_3)^{-1}(x_2, x_3)^{-1}$$

ein Kommutator. Somit erhält man $[\mathfrak{S}_n, \mathfrak{S}_n] \supset \mathfrak{A}_n$ und daher insgesamt $[\mathfrak{S}_n, \mathfrak{S}_n] = \mathfrak{A}_n$.

Als Nächstes bemerken wir, dass die Gruppen $\mathfrak{A}_2$ und $\mathfrak{A}_3$ von der Ordnung 1 bzw. 3 und damit abelsch sind. Folglich ist die Kommutatorgruppe $[\mathfrak{A}_n, \mathfrak{A}_n]$ für $n = 2, 3$ trivial. Sei nun $n \geq 5$, und sei (x_1, x_2, x_3) ein 3-Zyklus in $\mathfrak{S}_n$. Wählt man dann $x_4, x_5 \in \{1, \ldots, n\}$, so dass $x_1, \ldots, x_5$ paarweise verschieden sind, so hat man

$$(x_1, x_2, x_3) = (x_1, x_2, x_4)(x_1, x_3, x_5)(x_1, x_2, x_4)^{-1}(x_1, x_3, x_5)^{-1}.$$

Da $\mathfrak{A}_n$ gemäß 5.3/3 aus allen endlichen Produkten von 3-Zyklen besteht, ist also jedes Element aus $\mathfrak{A}_n$ ein Produkt von Kommutatoren aus $\mathfrak{A}_n$, so dass $\mathfrak{A}_n \subset [\mathfrak{A}_n, \mathfrak{A}_n]$ und damit $[\mathfrak{A}_n, \mathfrak{A}_n] = \mathfrak{A}_n$ gilt.

Es bleibt noch $[\mathfrak{A}_4, \mathfrak{A}_4] = \mathfrak{B}_4$ nachzurechnen. Es ist $[\mathfrak{A}_4, \mathfrak{A}_4]$ gemäß Bemerkung 1 (ii) der kleinste Normalteiler in $\mathfrak{A}_4$ mit abelscher Faktorgruppe. Da $\mathfrak{A}_4/\mathfrak{B}_4$ von der Ordnung 3, also abelsch ist, ergibt sich $[\mathfrak{A}_4, \mathfrak{A}_4] \subset \mathfrak{B}_4$. Andererseits hat man für paarweise verschiedene Elemente $x_1, \ldots, x_4 \in \{1, \ldots, 4\}$ die Gleichung

$$(x_1, x_2)(x_3, x_4) = (x_1, x_2, x_3)(x_1, x_2, x_4)(x_1, x_2, x_3)^{-1}(x_1, x_2, x_4)^{-1},$$

welche besagt, dass $\mathfrak{B}_4 = \{\mathrm{id},\ (1,2)(3,4),\ (1,3)(2,4),\ (1,4)(2,3)\}$ in $[\mathfrak{A}_4, \mathfrak{A}_4]$ enthalten ist. □

Im Folgenden wollen wir den Begriff des Kommutators zur Charakterisierung sogenannter auflösbarer Gruppen verwenden. Hierzu definieren wir für eine Gruppe G und $i \in \mathbb{N}$ den *i-ten iterierten Kommutator* D^iG induktiv durch

$$D^0G = G \quad \text{und} \quad D^{i+1}G = [D^iG, D^iG].$$

Somit erhält man eine Kette

$$G = D^0G \supset D^1G \supset \ldots \supset D^iG \supset \ldots$$

von Untergruppen von G, wobei stets $D^{i+1}G$ ein Normalteiler in D^iG ist. Außerdem ist $D^iG/D^{i+1}G$ abelsch. Allgemeiner benutzt man Ketten mit diesen Eigenschaften zur Definition auflösbarer Gruppen:

Definition 3. *Es sei G eine Gruppe. Eine Kette von Untergruppen*

$$G = G_0 \supset G_1 \supset \ldots \supset G_n = \{1\}$$

heißt eine Normalreihe *von G, wenn G_{i+1} jeweils ein Normalteiler in G_i ist. Die Restklassengruppen G_i/G_{i+1}, $i = 0, \ldots, n-1$, werden als die* Faktoren *der Normalreihe bezeichnet.*

Es heißt G auflösbar, *wenn G eine Normalreihe mit abelschen Faktoren besitzt.*

Satz 4. *Eine Gruppe G ist genau dann auflösbar, wenn es eine natürliche Zahl n mit $D^nG = \{1\}$ gibt.*

Beweis. Sei zunächst G auflösbar und

$$G = G_0 \supset G_1 \supset \ldots \supset G_n = \{1\}$$

eine Normalreihe mit abelschen Faktoren. Wir zeigen dann mit Induktion $D^iG \subset G_i$ für $i = 0, \ldots, n$. Für $i = 0$ ist diese Beziehung trivialerweise richtig. Gelte nun $D^iG \subset G_i$ für ein $i < n$. Aus der Tatsache, dass G_i/G_{i+1} abelsch ist, ergibt sich $[G_i, G_i] \subset G_{i+1}$, vgl. Bemerkung 1 (ii). Somit hat man

$$D^{i+1}G = [D^iG, D^iG] \subset [G_i, G_i] \subset G_{i+1}$$

und damit die gewünschte Inklusion. Insbesondere folgt

$$D^nG \subset G_n = \{1\}.$$

Ist umgekehrt $D^nG = \{1\}$ bekannt, so ist

$$G = D^0G \supset D^1G \supset \ldots \supset D^nG = \{1\}$$

eine Normalreihe mit abelschen Faktoren. □

Wir wollen einige Beispiele betrachten. Trivialerweise ist jede kommutative Gruppe auflösbar.

Bemerkung 5. *Die symmetrische Gruppe $\mathfrak{S}_n$ ist auflösbar für $n \leq 4$, nicht aber für $n \geq 5$.*

Beweis. Für $n \leq 4$ hat man für $\mathfrak{S}_n$ folgende Normalreihen mit abelschen Faktoren:

$$\mathfrak{S}_2 \supset \{1\},$$
$$\mathfrak{S}_3 \supset \mathfrak{A}_3 \supset \{1\},$$
$$\mathfrak{S}_4 \supset \mathfrak{A}_4 \supset \mathfrak{B}_4 \supset \{1\}.$$

Dass die Faktoren dieser Normalreihen abelsch sind, kann man leicht einsehen. Die Gruppen $\mathfrak{S}_2$, $\mathfrak{S}_3/\mathfrak{A}_3$ und $\mathfrak{S}_4/\mathfrak{A}_4$ sind zyklisch von der Ordnung 2, die Gruppen $\mathfrak{A}_3$ und $\mathfrak{A}_4/\mathfrak{B}_4$ zyklisch von der Ordnung 3, so dass die Kommutativität in diesen Fällen klar ist. Weiter ist die Kleinsche Vierergruppe $\mathfrak{B}_4$ ebenfalls kommutativ. Daher ist $\mathfrak{S}_n$ für $n \leq 4$ auflösbar. Für $n \geq 5$ gilt $[\mathfrak{S}_n, \mathfrak{S}_n] = \mathfrak{A}_n$ sowie $[\mathfrak{A}_n, \mathfrak{A}_n] = \mathfrak{A}_n$, vgl. Bemerkung 2, so dass $\mathfrak{S}_n$ in diesem Fall nicht auflösbar sein kann. □

Bemerkung 6. *Für eine Primzahl p ist jede* (*endliche*) *p-Gruppe*, *also jede Gruppe der Ordnung p^n mit $n \in \mathbb{N}$*, *auflösbar*.

Dies wurde bereits in 5.2/4 bewiesen. Als Nächstes wollen wir eine spezielle Charakterisierung der Auflösbarkeit endlicher Gruppen geben, welche insbesondere für die Auflösung algebraischer Gleichungen von Interesse sein wird.

Satz 7. *Es sei G eine endliche auflösbare Gruppe. Dann lässt sich in G jede echt absteigende Normalreihe mit abelschen Faktoren zu einer Normalreihe verfeinern, deren Faktoren zyklisch von Primzahlordnung sind.*

Beweis. Es sei $G_0 \supset \ldots \supset G_n$ eine echt absteigende Normalreihe von G mit abelschen Faktoren. Ist dann einer der Faktoren, etwa G_i/G_{i+1} nicht zyklisch von Primzahlordnung, so wähle man ein nicht-triviales Element $\overline{a} \in G_i/G_{i+1}$. Indem man zu einer geeigneten Potenz von $\overline{a}$ übergeht, kann man annehmen, dass $\operatorname{ord} \overline{a}$ prim ist. Die von $\overline{a}$ erzeugte zyklische Gruppe $\langle \overline{a} \rangle$ ist dann echt in G_i/G_{i+1} enthalten, da letztere Gruppe nicht zyklisch von Primzahlordnung ist. Das Urbild von $\langle \overline{a} \rangle$ in G_i unter der Projektion $G_i \longrightarrow G_i/G_{i+1}$ ergibt daher eine Gruppe H mit

$$G_i \supsetneq H \supsetneq G_{i+1}.$$

Da $\langle \overline{a} \rangle$ ein Normalteiler in der (abelschen) Gruppe G_i/G_{i+1} ist, ist dessen Urbild H ein Normalteiler in G_i. Außerdem ist G_{i+1} ein Normalteiler in H. Wir

können also die Normalreihe $G_0 \supset \ldots \supset G_n$ durch Einfügen von H zwischen G_i und G_{i+1} zu einer neuen Normalreihe verfeinern. Letztere hat ebenfalls abelsche Faktoren, denn man hat eine Injektion $H/G_{i+1} \hookrightarrow G_i/G_{i+1}$ sowie einen Epimorphismus $G_i/G_{i+1} \longrightarrow G_i/H$, wobei G_i/G_{i+1} abelsch ist. Wiederholt man das Verfahren der Verfeinerung, so gelangt man aufgrund der Endlichkeit von G nach endlich vielen Schritten zu einer Normalreihe, deren Faktoren zyklisch von Primzahlordnung sind. □

Satz 8. *Es sei G eine Gruppe und $H \subset G$ eine Untergruppe. Ist G auflösbar, so auch H. Ist H ein Normalteiler in G, so ist G genau dann auflösbar, wenn H und G/H auflösbar sind.*

Beweis. Sei zunächst G auflösbar. Dann ist wegen $D^i H \subset D^i G$ auch H auflösbar. Ist weiter H ein Normalteiler in G, so kann man den kanonischen Epimorphismus $\pi\colon G \longrightarrow G/H$ betrachten. Für diesen gilt $D^i(\pi(G)) = \pi(D^i(G))$, wie man leicht verifiziert, und es ist mit G auch $G/H = \pi(G)$ auflösbar.

Seien nun umgekehrt H und G/H auflösbar, wobei $D^n H = \{1\}$ und $D^n(G/H) = \{1\}$ gelte. Dann folgt

$$\pi(D^n G) = D^n(G/H) = \{1\},$$

d. h. $D^n G \subset H$ und weiter $D^{2n} G \subset D^n H = \{1\}$. Somit ist G auflösbar. □

Korollar 9. *Sind $G_1, \ldots, G_n$ Gruppen, so ist das kartesische Produkt $\prod_{i=1}^n G_i$ genau dann auflösbar, wenn alle G_i auflösbar sind.*

Beweis. Man schließe induktiv. Für $n = 2$ wende man Satz 8 auf die Projektion $G_1 \times G_2 \longrightarrow G_2$ an, welche G_1 als Kern besitzt. □

Lernkontrolle und Prüfungsvorbereitung

1. Es sei G eine Gruppe. Definiere den Kommutator $[a, b]$ für zwei Elemente $a, b \in G$ sowie den Kommutator $[H, H']$ für zwei Untergruppen $H, H' \subset G$. Welche Eigenschaften besitzt der Kommutator $[G, G]$?
2. Berechne die Kommutatoren $[\mathfrak{S}_n, \mathfrak{S}_n]$ und $[\mathfrak{A}_n, \mathfrak{A}_n]$ für $n \geq 2$.
3. Wann bezeichnet man eine Gruppe als auflösbar?

4. Sei G eine Gruppe. Definiere für $n \in \mathbb{N}$ den n-ten iterierten Kommutator zu G und charakterisiere die Auflösbarkeit von G mit Hilfe dieser Kommutatoren.
5. Für welche Indizes $n \in \mathbb{N}$ ist die symmetrische Gruppe $\mathfrak{S}_n$ auflösbar?
6. Zeige für eine Primzahl p, dass jede p-Gruppe auflösbar ist.
7. Sei G eine Gruppe und $H \subset G$ ein Normalteiler. Zeige, dass G genau dann auflösbar ist, wenn H und G/H auflösbar sind.

Übungsaufgaben

1. *Wir haben in Bemerkung* 1 *gesehen, dass für eine Gruppe G der Kommutator $[G, G]$ gleich dem kleinsten aller Normalteiler $N \subset G$ mit abelschem Quotienten G/N ist. Leite allgemeiner eine entsprechende Aussage für Kommutatoren der Form $[G, H]$ her, wobei H ein Normalteiler bzw. lediglich eine Untergruppe in G sei.*
2. Es seien p, q verschiedene Primzahlen. Zeige, dass jede Gruppe der Ordnung pq auflösbar ist.
3. Es sei G eine endliche Gruppe. Zeige:
   (i) Sind H, H' normale auflösbare Untergruppen in G, so auch $H \cdot H'$.
   (ii) Es existiert eine eindeutig bestimmte größte normale auflösbare Untergruppe in G. Diese ist invariant unter allen Automorphismen von G.
4. Zeige, dass jede Gruppe der Ordnung < 60 auflösbar ist.
5. Zeige, dass die alternierende Gruppe $\mathfrak{A}_5$ keinen nicht-trivialen Normalteiler besitzt.
6. Es sei T die Untergruppe der oberen Dreiecksmatrizen in $\mathrm{GL}(n, K)$, der Gruppe der invertierbaren $(n \times n)$-Matrizen über einem Körper K. Zeige, dass T auflösbar ist.
7. Betrachte zu einer Gruppe G die Untergruppen $C^i(G)$, welche induktiv durch $C^1(G) = G$ und $C^{i+1}(G) = [G, C^i(G)]$ definiert sind. Es heißt G *nilpotent*, wenn es ein $n \in \mathbb{N}$ mit $C^n(G) = \{1\}$ gibt. Zeige: Jede nilpotente Gruppe ist auflösbar.
8. Betrachte in der Notation von Aufgabe 6 für $K \neq \mathbb{F}_2$ die Gruppe der oberen Dreiecksmatrizen $T \subset \mathrm{GL}(n, K)$ sowie die Untergruppe $T_1 \subset T$ aller Dreiecksmatrizen, deren Diagonalelemente 1 sind. Zeige, dass T_1 nilpotent (vgl. Aufgabe 7) ist, nicht aber T. Es ist daher T ein Beispiel einer auflösbaren Gruppe, die nicht nilpotent ist.

6. Anwendungen der Galois-Theorie

Überblick und Hintergrund

Inzwischen sind wir in der Gruppen- und Körpertheorie zu einem gewissen Abschluss gelangt und wollen nun zeigen, wie die Galois-Theorie zur Lösung einiger berühmter klassischer Fragestellungen eingesetzt werden kann. Wir beginnen in 6.1 mit dem Problem der Auflösbarkeit algebraischer Gleichungen durch Radikale, also mit demjenigen Problem, das E. Galois zur Entwicklung seiner "Galois"-Theorie motiviert hat, und beweisen, dass für ein normiertes separables Polynom f mit Koeffizienten aus einem Körper K die algebraische Gleichung $f(x) = 0$ genau dann durch Radikale auflösbar ist, wenn die zugehörige Galois-Gruppe im gruppentheoretischen Sinne auflösbar ist.

Die grundsätzliche Beweisidee hierzu ist einfach zu erklären. Man reduziert das Problem auf der Körperseite auf den Fall, dass K genügend viele Einheitswurzeln enthält und betrachtet Erweiterungen von K, die durch Adjunktion eines *Radikals* entstehen, also einer Nullstelle eines Polynoms des Typs $X^n - c \in K[X]$ für $\operatorname{char} K \nmid n$ oder im Falle $p = \operatorname{char} K > 0$ auch des Typs $X^p - X - c \in K[X]$. Dies sind im Wesentlichen die zyklischen Galois-Erweiterungen von K; vgl. 4.8/3 und 4.8/5. Entsprechend benutzt man auf der Seite der Galois-Gruppen, dass die zyklischen Gruppen sozusagen die "Bausteine" der auflösbaren endlichen Gruppen darstellen; vgl. 5.4/7. Dabei werden für $p = \operatorname{char} K > 0$ auch die Nullstellen von Polynomen des Typs $X^p - X - c \in K[X]$ als "Radikale" bezeichnet, da nur so die Charakterisierung auflösbarer (separabler) algebraischer Gleichungen mittels auflösbarer

S. Bosch, *Algebra*, https://doi.org/10.1007/978-3-662-67464-2_7

Galois-Gruppen für Körper positiver Charakteristik gültig bleibt. Man bedenke hierbei auch, dass für $p = \operatorname{char} K > 0$ Polynome des Typs $X^p - c$ nicht separabel sind, ihre Nullstellen also nicht mit Galois-theoretischen Methoden behandelt werden können. Weiter gehen wir in 6.1/11 noch auf eine notwendige Bedingung für die Auflösbarkeit irreduzibler algebraischer Gleichungen von Primzahlgrad ein, welche man insbesondere zur Konstruktion nicht-auflösbarer algebraischer Gleichungen verwenden kann. Auch dieses Kriterium geht auf E. Galois zurück. Zur rechnerischen Illustration des Auflösbarkeitsproblems behandeln wir anschließend in Abschnitt 6.2 die expliziten Auflösungsformeln für algebraische Gleichungen vom Grad 3 und 4.

Als zweite Anwendung bringen wir in 6.3 einen Galois-theoretischen Beweis des Fundamentalsatzes der Algebra. Dieser Satz bietet aus algebraischer Sicht einige Tücken, wie auch die Beweise der ersten Stunde zeigen. Dies hängt damit zusammen, dass der Körper $\mathbb{C}$ der komplexen Zahlen zwar aus den reellen Zahlen $\mathbb{R}$ in algebraischer Weise durch Adjunktion einer Quadratwurzel zu -1 gewonnen werden kann, dass aber zur Konstruktion von $\mathbb{R}$ Methoden benutzt werden, die im Grunde genommen der Analysis zuzurechnen sind. Daher hat man für Polynome $f \in \mathbb{C}[X]$ nur geringe Chancen, deren Nullstellen in algebraischer Weise als Elemente von $\mathbb{C}$ zu konstruieren. Stattdessen gehen wir indirekt vor. Wenn $\mathbb{C}$ nicht algebraisch abgeschlossen ist, so gibt es nach dem Satz von Kronecker eine nichttriviale Erweiterung $L/\mathbb{C}$, die man als Galois-Erweiterung annehmen kann. Wir zeigen dann mittels Galois-Theorie und unter Benutzung der Tatsache, dass reelle Polynome ungeraden Grades stets eine reelle Nullstelle haben, dass man $L/\mathbb{C}$ vom Grad 2 annehmen darf. Eine solche Erweiterung kann aber nicht existieren; dies erkennt man unmittelbar, wenn man ausnutzt, dass positive reelle Zahlen eine Quadratwurzel in $\mathbb{R}$ und folglich alle komplexen Zahlen eine Quadratwurzel in $\mathbb{C}$ besitzen. Wie man sieht, stützt man sich auch bei dieser Schlussweise auf gewisse "analytische" Gegebenheiten der reellen Zahlen.

Als weitere Anwendung diskutieren wir in 6.4 Konstruktionen mit Zirkel und Lineal in der komplexen Zahlenebene. Eine genaue Analyse der Konstruktionsschritte, die man mit solchen Mitteln ausführen kann, zeigt, dass man beginnend mit den Punkten $0, 1 \in \mathbb{C}$ lediglich Punkte $z \in \mathbb{C}$ konstruieren kann, zu denen es eine Galois-Erweiterung $L/\mathbb{Q}$ mit $z \in L$ gibt, wobei der Grad $[L : \mathbb{Q}]$ eine Potenz von 2 ist. Insbesondere ist dann

z algebraisch über $\mathbb{Q}$, mit einem Grad, der ebenfalls eine Potenz von 2 ist. So kann etwa die Konstruierbarkeit der Kubikwurzel $\sqrt[3]{2}$ ausgeschlossen werden, und es folgt als Beispiel, dass das antike Problem der Würfelverdoppelung mit Zirkel und Lineal nicht lösbar ist. Im Übrigen werden wir auf die Untersuchungen von C. F. Gauß zur Konstruierbarkeit regelmäßiger n-Ecke eingehen.

6.1 Auflösbarkeit algebraischer Gleichungen

Wenn auch die Formeln zur Auflösung algebraischer Gleichungen vom Grad 2 als simpel erscheinen mögen, so machen die entsprechenden Formeln für die Grade 3 und 4, die wir in Abschnitt 6.2 herleiten werden, bereits unmissverständlich klar, dass es sich bei der Auflösung algebraischer Gleichungen um ein kompliziertes Problem handelt. Im Übrigen werden wir sehen, dass es ab Grad 5 derartige allgemeine Auflösungsformeln aus prinzipiellen Gründen nicht mehr geben kann. Um die Hintergründe genauer analysieren zu können, wollen wir zunächst den Begriff der Auflösbarkeit algebraischer Gleichungen präzisieren.

Definition 1. *Eine endliche Körpererweiterung L/K heißt* durch Radikale auflösbar, *wenn es zu L einen Erweiterungskörper E sowie eine Körperkette*

$$K = E_0 \subset E_1 \subset \ldots \subset E_m = E$$

gibt, so dass E_{i+1} jeweils aus E_i durch Adjunktion eines Elements des folgenden Typs entsteht, nämlich einer

(1) *Einheitswurzel oder*
(2) *Nullstelle eines Polynoms $X^n - a \in E_i[X]$ mit* $\operatorname{char} K \nmid n$ *oder*
(3) *Nullstelle eines Polynoms des Typs $X^p - X - a \in E_i[X]$, wobei $p = \operatorname{char} K > 0$ gelte.*

Es ist L/K dann notwendig separabel.

Hauptziel dieses Abschnitts ist es, die Auflösbarkeit von Körpererweiterungen durch Radikale mit Hilfe der Auflösbarkeit von Galois-Gruppen (vgl. 5.4/3) zu charakterisieren.

Definition 2. *Eine endliche Körpererweiterung L/K heißt* auflösbar, *wenn es einen Oberkörper $E \supset L$ gibt, so dass E/K eine endliche Galois-Erweiterung mit auflösbarer Galois-Gruppe* $\mathrm{Gal}(E/K)$ *gemäß* 5.4/3 *ist.*

Wir wollen hier sogleich an den Hauptsatz der Galois-Theorie 4.1/6 erinnern und festhalten, wie sich für eine endliche Galois-Erweiterung L/K die Auflösbarkeit der Galois-Gruppe $\mathrm{Gal}(L/K)$ auf die Struktur der Erweiterung L/K auswirkt.

Bemerkung 3. *Es sei L/K eine endliche Galois-Erweiterung. Dann ist äquivalent*:

(i) *Es existiert eine Normalreihe*

$$\mathrm{Gal}(L/K) = G_0 \supset G_1 \supset \ldots \supset G_n = \{1\}$$

mit abelschen Faktoren G_i/G_{i+1} für $i = 0, \ldots, n-1$.

(ii) *Es existiert eine Körperkette*

$$K = K_0 \subset K_1 \subset \ldots \subset K_n = L$$

so dass K_{i+1}/K_i für $i = 0, \ldots, n-1$ jeweils eine endliche abelsche Galois-Erweiterung ist.

Beweis. Wir verwenden im Folgenden wiederholt den Hauptsatz der Galois-Theorie, ohne dies bei den einzelnen Schritten explizit zu erwähnen. Ist eine Normalreihe von $\mathrm{Gal}(L/K)$ wie in (i) gegeben, so setze man $K_i = L^{G_i}$ für $i = 0, \ldots, n$. Dies ergibt eine Körperkette $K = K_0 \subset K_1 \subset \ldots \subset K_n = L$ wie in (ii), und zwar mit $G_i = \mathrm{Gal}(L/K_i)$. Indem wir K_{i+1} als Zwischenkörper zu L/K_i betrachten und benutzen, dass $G_{i+1} = \mathrm{Gal}(L/K_{i+1})$ ein Normalteiler in G_i ist, erkennen wir K_{i+1}/K_i als Galois-Erweiterung mit Galois-Gruppe G_i/G_{i+1}. Dieser Quotient ist abelsch, so dass K_{i+1}/K_i jeweils eine abelsche Galois-Erweiterung ist.

Sei nun umgekehrt eine Körperkette wie in (ii) gegeben. Wir setzen dann $G_i = \mathrm{Gal}(L/K_i)$ für $i = 0, \ldots, n$ und erhalten eine Kette von Untergruppen $\mathrm{Gal}(L/K) = G_0 \supset G_1 \supset \ldots \supset G_n = \{1\}$ wie in (i). Indem wir wieder K_{i+1} als Zwischenkörper von L/K_i ansehen und benutzen, dass K_{i+1}/K_i eine endliche abelsche Galois-Erweiterung ist, ergibt sich, dass $G_{i+1} = \mathrm{Gal}(L/K_{i+1})$ ein Normalteiler in $G_i = \mathrm{Gal}(L/K_i)$ ist, und zwar mit abelschem Quotienten $\mathrm{Gal}(K_{i+1}/K_i) = G_i/G_{i+1}$. □

Man beachte bei Definition 2, dass eine Galois-Erweiterung L/K genau dann auflösbar ist, wenn die Galois-Gruppe $\mathrm{Gal}(L/K)$ auflösbar ist. Können wir nämlich L/K zu einer endlichen Galois-Erweiterung E/K mit auflösbarer Galois-Gruppe vergrößern, so ist $\mathrm{Gal}(L/K)$ nach 4.1/2 ein Quotient von $\mathrm{Gal}(E/K)$ und somit nach 5.4/8 ebenfalls auflösbar.

Die beiden Auflösbarkeitsbegriffe lassen sich in nahe liegender Weise auf algebraische Gleichungen übertragen. Ist f ein nicht-konstantes (separables) Polynom mit Koeffizienten aus einem Körper K, so wähle man einen Zerfällungskörper L von f über K. Wir sagen dann, dass die algebraische Gleichung $f(x) = 0$ *über K auflösbar* bzw. *durch Radikale auflösbar* ist, wenn die Erweiterung L/K die entsprechende Eigenschaft besitzt.

Als Nächstes wollen wir einige mehr oder weniger elementare Eigenschaften der beiden Auflösbarkeitsbegriffe behandeln.

Lemma 4. *Es sei L/K eine endliche Körpererweiterung sowie F ein beliebiger Erweiterungskörper von K. Man bette L mittels eines K-Homomorphismus in einen algebraischen Abschluss $\overline{F}$ von F ein, vgl.* 3.4/9, *und bilde das Kompositum FL in $\overline{F}$. Ist dann L/K auflösbar* (*bzw. galoissch mit auflösbarer Galois-Gruppe*, *bzw. durch Radikale auflösbar*, *bzw. ausschöpfbar durch eine Körperkette des in Definition* 1 *genannten Typs*), *so gilt dasselbe auch für die Erweiterung FL/F.*

Lemma 5. *Für eine Kette endlicher Körpererweiterungen $K \subset L \subset M$ ist M/K genau dann auflösbar* (*bzw. durch Radikale auflösbar*), *wenn M/L und L/K auflösbar* (*bzw. durch Radikale auflösbar*) *sind.*

Beweis zu Lemma 4. Sei zunächst L/K auflösbar. Indem wir L vergrößern, dürfen wir L/K als galoissch mit auflösbarer Galois-Gruppe $\mathrm{Gal}(L/K)$ annehmen. Dann ist auch $FL = F(L)$ eine endliche Galois-Erweiterung von F. Da jedes $\sigma \in \mathrm{Gal}(FL/F)$ den Körper K festlässt, ist $\sigma(L)$ wieder algebraisch über K. Es folgt sogar $\sigma(L) = L$ mittels 3.5/4 (i), so dass man einen Restriktionshomomorphismus

$$\mathrm{Gal}\big(FL/F\big) \longrightarrow \mathrm{Gal}\big(L/K\big)$$

erhält. Dieser ist wegen $FL = F(L)$ injektiv, so dass die Auflösbarkeit von $\mathrm{Gal}(FL/F)$ bzw. FL/F aus 5.4/8 folgt. Ist andererseits L/K durch Radikale auflösbar bzw. durch eine Körperkette des in Definition 1 genannten Typs ausschöpfbar, so gilt dies natürlich auch für die Erweiterung FL/F. □

Beweis zu Lemma 5. Wir beginnen wieder mit der Eigenschaft "auflösbar". Sei zunächst M/K auflösbar. Indem wir M vergrößern, dürfen wir M/K als galoissch mit auflösbarer Galois-Gruppe annehmen. Dann ist definitionsgemäß auch L/K auflösbar. Da weiter $\mathrm{Gal}(M/L)$ in natürlicher Weise als Untergruppe von $\mathrm{Gal}(M/K)$ aufzufassen ist, folgt unter Verwendung von 5.4/8, dass auch M/L auflösbar ist.

In der Kette $K \subset L \subset M$ seien nun M/L und L/K auflösbar. In einem ersten Schritt wollen wir zeigen, dass beide Erweiterungen als Galois-Erweiterungen mit auflösbaren Galois-Gruppen angenommen werden dürfen. Hierzu wähle man eine endliche Erweiterung L' zu L, so dass L'/K galoissch mit auflösbarer Galois-Gruppe ist. Unter Benutzung von Lemma 4 dürfen wir dann L durch L' und M durch das Kompositum $L'M$ (in einem algebraischen Abschluss von M) ersetzen. Weiter finden wir eine endliche Erweiterung M' von $L'M$, so dass M'/L' galoissch mit auflösbarer Galois-Gruppe ist. Indem wir weiter $L'M$ durch M' ersetzen, können wir im Folgenden annehmen, dass M/L und L/K jeweils galoissch mit auflösbarer Galois-Gruppe sind.

Da M wohl separabel, aber nicht notwendig galoissch über K ist, gehen wir zu einer normalen Hülle M' von M/K über; vgl. 3.5/7. Es ist dann M'/K eine endliche Galois-Erweiterung. Zur Konstruktion von M' betrachten wir alle K-Homomorphismen $\sigma\colon M \longrightarrow \overline{M}$ in einen algebraischen Abschluss $\overline{M}$ von M und definieren M' als das Kompositum aller $\sigma(M)$. Da L/K galoissch ist, hat man $\sigma(L) = L$ für alle σ, und es folgt, dass jede Erweiterung $\sigma(M)/L$ eine zu M/L isomorphe Galois-Erweiterung ist. Wir behaupten, dass die Galois-Gruppe $\mathrm{Gal}(M'/K)$ und damit die Erweiterung M/K auflösbar ist. Um dies einzusehen, betrachte man die surjektive Restriktionsabbildung

$$\mathrm{Gal}\big(M'/K\big) \longrightarrow \mathrm{Gal}\big(L/K\big),$$

welche $\mathrm{Gal}(M'/L)$ als Kern hat; vgl. 4.1/2 (ii). Da $\mathrm{Gal}(L/K)$ auflösbar ist, haben wir gemäß 5.4/8 lediglich zu zeigen, dass $\mathrm{Gal}(M'/L)$ auflösbar ist. Letztere Gruppe lässt sich aber unter Benutzung von 4.1/12 (ii) als Untergruppe des kartesischen Produktes

$$\prod_{\sigma \in \mathrm{Hom}_K(M,\overline{M})} \mathrm{Gal}\big(\sigma(M)/L\big)$$

auffassen. Alle Gruppen $\mathrm{Gal}(\sigma(M)/L) = \mathrm{Gal}(\sigma(M)/\sigma(L))$ sind kanonisch isomorph zu $\mathrm{Gal}(M/L)$ und daher auflösbar. Dann ist auch das karte-

sische Produkt dieser Gruppen auflösbar, vgl. 5.4/9, und man sieht mit 5.4/8, dass $\mathrm{Gal}(M'/L)$ auflösbar ist. Dies beendet den Beweis von Lemma 5 für die Eigenschaft "auflösbar".

Es bleibt noch der Fall "durch Radikale auflösbar" zu betrachten. Ist M/K durch Radikale auflösbar, so gilt dies trivialerweise auch für die Erweiterungen M/L und L/K. Sind umgekehrt M/L und L/K durch Radikale auflösbar, so wähle man eine Erweiterung L'/L, so dass die Erweiterung L'/K durch eine Kette des in Definition 1 genannten Typs ausgeschöpft werden kann. Man bilde dann in einem algebraischen Abschluss von M das Kompositum $L'M$, wobei $L'M/L'$ gemäß Lemma 4 ebenfalls durch Radikale auflösbar ist. Trivialerweise ist dann $L'M/K$ durch Radikale auflösbar, und es folgt, dass auch M/K durch Radikale auflösbar ist. □

Theorem 6. *Eine endliche Körpererweiterung L/K ist genau dann auflösbar, wenn sie durch Radikale auflösbar ist.*

Beweis. Sei zunächst L/K als auflösbar vorausgesetzt. Indem wir L vergrößern, dürfen wir L/K als galoissch mit auflösbarer Galois-Gruppe annehmen. Sei weiter m das Produkt aller Primzahlen $q \neq \mathrm{char}\, K$, welche den Grad $[L : K]$ teilen, und sei F ein Erweiterungskörper von K, der durch Adjunktion einer primitiven m-ten Einheitswurzel entsteht. Die Erweiterung F/K ist dann per definitionem durch Radikale auflösbar. Indem wir das Kompositum von F und L in einem algebraischen Abschluss von K bilden, können wir die Kette

$$K \subset F \subset FL$$

betrachten, und es genügt zu zeigen (vgl. Lemma 5), dass FL/F durch Radikale auflösbar ist. Dabei wissen wir nach Lemma 4, dass FL/F auflösbar ist, ja sogar eine Galois-Erweiterung mit auflösbarer Galois-Gruppe ist, da wir die entsprechende Eigenschaft für L/K vorausgesetzt haben. Man wähle nun eine Normalreihe

$$\mathrm{Gal}\big(FL/F\big) = G_0 \supset G_1 \supset \ldots \supset G_n = \{1\}$$

mit Faktoren, die zyklisch von Primzahlordnung sind; vgl. 5.4/7. Aufgrund des Hauptsatzes der Galois-Theorie 4.1/6 bzw. Bemerkung 3 korrespondiert hierzu eine Körperkette

$$F = F_0 \subset F_1 \subset \ldots \subset F_n = FL,$$

wobei F_{i+1}/F_i jeweils eine zyklische Galois-Erweiterung mit Primzahlgrad, etwa p_i, ist. Bemerkt man nun, dass $[FL : F]$, etwa unter Benutzung von 4.1/12 (i), ein Teiler von $[L : K]$ ist, so erkennt man für $p_i \neq \operatorname{char} K$, dass die Primzahl p_i ein Teiler von m ist. Folglich enthält F und damit F_i eine primitive p_i-te Einheitswurzel. Nach 4.8/3 entsteht dann F_{i+1} aus F_i durch Adjunktion einer Nullstelle eines Polynoms des Typs $X^{p_i} - a \in F_i[X]$. Andererseits sieht man für $p_i = \operatorname{char} K$ mit 4.8/5, dass F_{i+1} aus F_i durch Adjunktion einer Nullstelle eines Polynoms des Typs $X^{p_i} - X - a \in F_i[X]$ gewonnen wird. Insgesamt ergibt sich, dass FL/F und somit auch L/K durch Radikale auflösbar ist.

Es sei nun L/K durch Radikale auflösbar. Dann existiert eine Körperkette $K = K_0 \subset K_1 \subset \ldots \subset K_n$ mit $L \subset K_n$, so dass die Erweiterung K_{i+1}/K_i jeweils vom Typ (1), (2) oder (3) im Sinne von Definition 1 ist. Indem wir L vergrößern, dürfen wir $L = K_n$ annehmen. Um nun zu zeigen, dass L/K auflösbar ist, reicht es gemäß Lemma 5, zu zeigen, dass jede Erweiterung K_{i+1}/K_i auflösbar ist. Mit anderen Worten, wir dürfen annehmen, dass die Erweiterung L/K von der Form (1), (2) oder (3) in Definition 1 ist. Nun sind aber Erweiterungen des Typs (1) nach 4.5/7 und des Typs (3) nach 4.8/5 abelsche bzw. zyklische Galois-Erweiterungen und damit auflösbar. Sei also L/K eine Erweiterung des Typs (2), d. h. es entstehe L aus K durch Adjunktion einer Nullstelle eines Polynoms $X^n - c \in K[X]$ mit $\operatorname{char} K \nmid n$. Ist F/K eine Erweiterung, die von einer primitiven n-ten Einheitswurzel erzeugt wird, so bilde man das Kompositum von F und L in einem algebraischen Abschluss von L und betrachte die Kette $K \subset F \subset FL$. Dann ist F/K nach 4.5/7 als abelsche Galois-Erweiterung auflösbar sowie FL/F nach 4.8/3 eine zyklische Galois-Erweiterung, also ebenfalls auflösbar. Mit Lemma 5 ist FL/K und somit auch L/K auflösbar, was zu zeigen war. □

Korollar 7. *Es sei L/K eine separable Körpererweiterung vom Grad ≤ 4. Dann ist L/K auflösbar, insbesondere also auch durch Radikale auflösbar.*

Beweis. Aufgrund des Satzes vom primitiven Element 3.6/12 ist L/K eine einfache Körpererweiterung, etwa $L = K(a)$. Sei $f \in K[X]$ das Minimalpolynom von a über K, und sei L' ein Zerfällungskörper von f über K. Dann gilt $\operatorname{grad} f = [L : K] \leq 4$, und es lässt sich $\operatorname{Gal}(L'/K)$ nach 4.3/1 als Untergruppe von $\mathfrak{S}_4$ auffassen. Da $\mathfrak{S}_4$ und alle ihre Untergruppen auflösbar sind (vgl. 5.4/5 und 5.4/8), sind auch L'/K und L/K auflösbar. □

Korollar 8. *Es existieren endliche separable Körpererweiterungen, die nicht durch Radikale auflösbar sind. Beispielsweise ist die allgemeine Gleichung n-ten Grades für $n \geq 5$ nicht durch Radikale auflösbar.*

Zum *Beweis* genügt es zu wissen, dass die allgemeine Gleichung n-ten Grades für $n \geq 2$ die volle Permutationsgruppe $\mathfrak{S}_n$ als Galois-Gruppe besitzt; vgl. Abschnitt 4.3, Beispiel (4). Da $\mathfrak{S}_n$ gemäß 5.4/5 für $n \geq 5$ nicht auflösbar ist, sieht man mit Theorem 6, dass die zugehörige Erweiterung L/K in diesem Falle nicht durch Radikale auflösbar sein kann. □

Wir wollen das Beispiel (4) aus Abschnitt 4.3 noch einmal rekapitulieren. Man ging dort von einem Körper k aus und betrachtete den rationalen Funktionenkörper $L = k(T_1, \ldots, T_n)$ in den Variablen $T_1, \ldots, T_n$. Auf L ließ man die Gruppe $\mathfrak{S}_n$ durch Permutieren der T_i operieren, wobei sich L als Galois-Erweiterung über dem zugehörigen Fixkörper K mit Galois-Gruppe $\mathrm{Gal}(L/K) = \mathfrak{S}_n$ herausstellte. Der Fixkörper selbst ergab sich als Körper $K = k(s_1, \ldots, s_n)$, wobei $s_1, \ldots, s_n$ die elementarsymmetrischen Polynome in $T_1, \ldots, T_n$ sind. Weiter hatten wir gesehen, dass L ein Zerfällungskörper des Polynoms $f = X^n - s_1 X^{n-1} + \ldots + (-1)^n s_n \in K[X]$ ist. Da die Elemente $s_1, \ldots, s_n \in K$ aufgrund des Hauptsatzes über symmetrische Polynome 4.3/5 bzw. 4.4/1 algebraisch unabhängig über k sind, kann man die Koeffizienten $-s_1, \ldots, (-1)^n s_n$ auch als Variablen über k ansehen. Somit kann man im Fall $n \geq 5$ sagen, dass für Variablen $c_1, \ldots, c_n$ über k die *allgemeine Gleichung n-ten Grades* $x^n + c_1 x^{n-1} + \ldots + c_n = 0$ über dem rationalen Funktionenkörper $K = k(c_1, \ldots, c_n)$ nicht durch Radikale auflösbar ist.

Konkreter kann man natürlich die Frage stellen, ob es auch über dem Körper $\mathbb{Q}$ Gleichungen gibt, die nicht durch Radikale auflösbar sind. Einige Aspekte dieser Fragestellung sollen im Folgenden studiert werden, wobei wir allerdings nur Gleichungen von Primzahlgrad betrachten werden. Wir beginnen mit zwei Hilfsresultaten über Permutationen, welche wir anschließend auf Galois-Gruppen anwenden wollen.

Lemma 9. *Für eine Primzahl p sei $G \subset \mathfrak{S}_p$ eine Untergruppe, welche transitiv auf $\{1, \ldots, p\}$ operiere. Dann enthält G eine Untergruppe H der Ordnung p. Ist G auflösbar, so ist H eindeutig bestimmt und insbesondere ein Normalteiler in G.*

Beweis. Da G transitiv auf $\{1,\dots,p\}$ operiert, gibt es bei dieser Operation lediglich eine G-Bahn. Diese besteht aus p Elementen, und man sieht etwa mit 5.1/6, dass p ein Teiler von $\operatorname{ord} G$ ist. Da p^2 kein Teiler von $p!$ ist, also die Ordnung von $\mathfrak{S}_p$ nicht teilt, kann p^2 auch kein Teiler von $\operatorname{ord} G$ sein. Es enthält G daher eine Untergruppe H der Ordnung p, nämlich eine p-Sylow-Gruppe, vgl. 5.2/6.

Nehmen wir nun an, dass G auflösbar ist, so gibt es nach 5.4/7 eine Normalreihe $G = G_0 \supsetneq \dots \supsetneq G_n = \{1\}$, deren Faktoren zyklisch von Primzahlordnung sind. Wir wollen per Induktion zeigen, dass G_i für $i < n$ jeweils transitiv auf $\{1,\dots,p\}$ operiert. Für $i = 0$ ist dies vorausgesetzt, sei also $i > 0$. Da G_i ein Normalteiler in G_{i-1} ist, ergibt sich für $g \in G_{i-1}$ und $x \in \{1,\dots,p\}$ die Gleichung $g(G_i x) = G_i(gx)$. Dies bedeutet, dass G_{i-1} auf den G_i-Bahnen von $\{1,\dots,p\}$ operiert und, wenn wir nach Induktionsvoraussetzung annehmen, dass G_{i-1} transitiv auf $\{1,\dots,p\}$ operiert, dass alle G_i-Bahnen von $\{1,\dots,p\}$ die gleiche Ordnung haben. Sind also $B_1,\dots,B_r$ die Bahnen der Aktion von G_i auf $\{1,\dots,p\}$, so folgt $p = \sum_{\rho=1}^{r} \operatorname{ord} B_\rho = r \cdot \operatorname{ord} B_1$, woraus sich $r = 1$ oder $\operatorname{ord} B_1 = 1$ ergibt. Für $i < n$ ist aber $G_i \neq \{1\}$ und daher $\operatorname{ord} B_\rho > 1$, so dass $r = 1$ folgt. Es gibt also nur eine Bahn bezüglich der Aktion von G_i, d. h. G_i operiert transitiv auf $\{1,\dots,p\}$. Als Konsequenz enthält G_i für $i < n$ stets eine Untergruppe der Ordnung p, wie wir oben gezeigt haben. Insbesondere ist daher G_{n-1} selbst von der Ordnung p, denn $G_{n-1} \simeq G_{n-1}/G_n$ ist von Primzahlordnung.

Mittels wiederholter Anwendung des Satzes von Lagrange 1.2/3 zeigt man $\operatorname{ord} G = \prod_{i=0}^{n-1} \operatorname{ord} G_i/G_{i+1}$. Da p ein Teiler von $\operatorname{ord} G$ ist, nicht aber p^2, gilt $p \neq \operatorname{ord} G_i/G_{i+1}$ für $i = 0,\dots,n-2$. Ausgehend von $H \subset G_0$ schließt man hieraus in induktiver Weise $H \subset G_i$ für $i = 0,\dots,n-1$. Hat man nämlich $H \subset G_i$ für ein $i \leq n-2$, so ist die kanonische Abbildung

$$H \hookrightarrow G_i \longrightarrow G_i/G_{i+1}$$

wegen $p \nmid \operatorname{ord} G_i/G_{i+1}$ trivial, und es folgt $H \subset G_{i+1}$. Insbesondere erhält man $H \subset G_{n-1}$ und damit $H = G_{n-1}$. Dies zeigt die Eindeutigkeit von H. Dann ist H aber auch invariant unter der Konjugation mit Elementen aus G und folglich ein Normalteiler in G. □

Lemma 10. *Es sei G in der Situation von Lemma 9 eine auflösbare Gruppe. Besitzt dann ein Element $\sigma \in G$ als bijektive Selbstabbildung von $\{1,\dots,p\}$ zwei verschiedene Fixpunkte, so folgt $\sigma = \mathrm{id}$.*

Beweis. Nach Lemma 9 gibt es in G einen Normalteiler H der Ordnung p. Notwendigerweise ist H dann zyklisch von der Ordnung p und wird von einem Element $\pi \in G \subset \mathfrak{S}_p$ erzeugt. Indem man π als Produkt elementfremder Zyklen schreibt, vgl. 5.3/1 (ii), und $\operatorname{ord} \pi = p$ benutzt, sieht man, dass π ein p-Zyklus ist, etwa $\pi = (0, \ldots, p-1)$, wobei wir aus schreibtechnischen Gründen $\mathfrak{S}_p$ als Gruppe der Permutationen der Elemente $0, \ldots, p-1$ auffassen. Sei nun $\sigma \in G$ eine Permutation mit zwei verschiedenen Fixpunkten. Durch Umnummerieren können wir dann annehmen, dass einer dieser Fixpunkte das Element 0 ist. Seien also $0, i$ mit $0 < i < p$ zwei Fixpunkte von σ. Da H ein Normalteiler in G ist, gehört das Element

$$\sigma \circ \pi \circ \sigma^{-1} = \big(\sigma(0), \ldots, \sigma(p-1)\big)$$

wiederum zu H, lässt sich also als Potenz π^r mit $0 \leq r < p$ schreiben, etwa

$$\big(\sigma(0), \ldots, \sigma(p-1)\big) = \big(0, \overline{r \cdot 1}, \ldots, \overline{r \cdot (p-1)}\,\big),$$

wobei $\overline{r \cdot j}$ jeweils den Rest in $\{0, \ldots, p-1\}$ bezeichnet, wenn man $r \cdot j$ durch p teilt. Wegen $\sigma(0) = 0$ und $\sigma(i) = i$ folgt $\overline{r \cdot i} = i$, bzw. $\overline{r} \cdot \overline{i} = \overline{r \cdot i} = \overline{i}$ in $\mathbb{Z}/p\mathbb{Z}$. Hieraus ergibt sich $\overline{r} = 1$ und damit $r = 1$, denn $\overline{i}$ ist wegen $0 < i < p$ eine Einheit in $\mathbb{Z}/p\mathbb{Z}$. Somit hat man $\sigma = \mathrm{id}$. □

Wir wollen nun die Aussage von Lemma 10 im Sinne der Galois-Theorie interpretieren.

Satz 11. *Es sei K ein Körper und $f \in K[X]$ ein irreduzibles separables Polynom von primem Grad p. Die zugehörige Galois-Gruppe sei auflösbar. Ist dann L ein Zerfällungskörper von f über K und sind $\alpha, \beta \in L$ zwei verschiedene Nullstellen von f, so gilt $L = K(\alpha, \beta)$.*

Beweis. Es ist L/K eine Galois-Erweiterung mit $G = \mathrm{Gal}(L/K)$ als Galois-Gruppe, die zugleich die Galois-Gruppe des Polynoms f ist. Jedes Element $\sigma \in G$ induziert eine Permutation der Nullstellen $\alpha_1, \ldots, \alpha_p$ von f, und wir können G deshalb als Untergruppe der Permutationsgruppe $\mathfrak{S}_p$ auffassen, vgl. 4.3/1. Da f irreduzibel ist, gibt es zu je zwei Nullstellen α, β von f ein $\sigma \in G$ mit $\sigma(\alpha) = \beta$, und die Aktion von G auf $\{\alpha_1, \ldots, \alpha_p\}$ ist transitiv. Außerdem ist G nach Voraussetzung auflösbar, erfüllt also die Voraussetzungen zu Lemma 10. Gilt daher $\alpha \neq \beta$ und ist $\sigma \in G$ ein Automorphismus von L, welcher auf $K(\alpha, \beta)$ trivial ist, so hat σ als

Permutation von $\alpha_1, \ldots, \alpha_p$ zwei verschiedene Fixpunkte, nämlich α und β, und ist folglich die Identität. Deshalb ergibt sich $\mathrm{Gal}(L/K(\alpha,\beta)) = \{1\}$ und somit $L = K(\alpha,\beta)$ aufgrund des Hauptsatzes der Galois-Theorie 4.1/6. □

Mittels Satz 11 kann man nun eine ganze Reihe von nicht-auflösbaren endlichen Körpererweiterungen von $\mathbb{Q}$ konstruieren. Ist nämlich $f \in \mathbb{Q}[X]$ irreduzibel mit primem Grad $p \geq 5$ und besitzt f mindestens zwei reelle sowie eine nicht-reelle Nullstelle in $\mathbb{C}$, so kann die Gleichung $f(x) = 0$ nicht auflösbar sein. Anderenfalls könnte man nämlich mit Satz 11 schließen, dass der Zerfällungskörper von f in $\mathbb{C}$ reell ist, im Widerspruch zu der Tatsache, dass f nicht-reelle Nullstellen besitzt. Als Beispiel betrachte man etwa für Primzahlen $p \geq 5$ das Polynom $f = X^p - 4X + 2 \in \mathbb{Q}[X]$. Dieses ist irreduzibel aufgrund des Eisensteinschen Irreduzibilitätskriteriums 2.8/1. Weiter sieht man mittels Kurvendiskussion, dass f genau 3 reelle Nullstellen hat. Folglich ist die zugehörige Galois-Gruppe nicht auflösbar. Speziell für $p = 5$ kann man dies auch anders einsehen, indem man zeigt, dass die Galois-Gruppe G zu $f = X^5 - 4X + 2$ isomorph zu $\mathfrak{S}_5$ ist. Fassen wir G nämlich gemäß 4.3/1 als Untergruppe von $\mathfrak{S}_5$ auf, so enthält G etwa nach Lemma 9 ein Element der Ordnung 5, also einen 5-Zyklus. Weiter permutiert die komplexe Konjugation die beiden nicht-reellen Nullstellen von f, wobei die 3 übrigen Nullstellen invariant bleiben, da sie reell sind. Es enthält daher G auch eine Transposition. Dann folgt aber bereits $G = \mathfrak{S}_5$; vgl. Aufgabe 7 aus Abschnitt 5.3. Mit dieser Argumentation kann man allgemeiner zeigen, dass es zu jeder Primzahl p ein irreduzibles Polynom $f \in \mathbb{Q}[X]$ vom Grad p gibt, dessen zugehörige Galois-Gruppe isomorph zu $\mathfrak{S}_p$ ist; vgl. Aufgabe 5.

Lernkontrolle und Prüfungsvorbereitung

1. Wann heißt eine endliche Körpererweiterung "auflösbar" und wann "durch Radikale auflösbar"?

2. Es sei G eine endliche auflösbare Gruppe. Zeige, dass G eine Normalreihe besitzt mit Faktoren, die zyklisch von Primzahlordnung sind.

3. Eine endliche Körpererweiterung L/K ist genau dann auflösbar, wenn sie durch Radikale auflösbar ist. Beweise dieses Resultat unter der vereinfachenden Annahme, dass K "genügend viele" Einheitswurzeln enthält.

[+]4. Sei L/K eine endliche Körpererweiterung, sowie F ein beliebiger Erweiterungskörper von K, so dass das Kompositum FL in einem gemeinsamen Oberkörper von L und F gebildet werden kann. Sei L/K auflösbar bzw. durch Radikale auflösbar. Zeige, dass dies dann auch für die Erweiterung FL/F gilt.

[+]5. Es sei $K \subset L \subset M$ eine Kette endlicher Körpererweiterungen. Zeige, dass M/K genau dann auflösbar bzw. durch Radikale auflösbar ist, wenn dies für die Erweiterungen M/L und L/K gilt.

6. Behandle den Allgemeinfall zu Punkt 3 unter Benutzung von Punkt 4 und 5.

7. Zeige, dass jede separable Körpererweiterung vom Grad ≤ 4 durch Radikale auflösbar ist.

8. Erkläre, was man unter der allgemeinen Gleichung n-ten Grades versteht. Zeige, dass diese für $n \geq 5$ nicht durch Radikale auflösbar ist.

[+]9. Sei p eine Primzahl und $G \subset \mathfrak{S}_p$ eine Untergruppe, die transitiv auf $\{1, \ldots, p\}$ operiert und auflösbar ist. Zeige, dass G genau eine p-Sylow-Gruppe besitzt und dass diese ein Normalteiler der Ordnung p in G ist.

[+]10. Sei G wie in Punkt 9, und sei $\sigma \in G$ ein Element, welches als bijektive Selbstabbildung von $\{1, \ldots, p\}$ zwei verschiedene Fixpunkte hat. Zeige $\sigma = \mathrm{id}$.

11. Sei f ein irreduzibles separables Polynom von primem Grad p über einem Körper K. Die Galois-Gruppe der Gleichung $f(x) = 0$ sei auflösbar. Zeige unter Benutzung von Punkt 9 und 10: Sind α, β zwei verschiedene Nullstellen von f in einem Zerfällungskörper L von f, so gilt $L = K(\alpha, \beta)$.

12. Konstruiere mittels Punkt 11 Beispiele von irreduziblen Polynomen $f \in \mathbb{Q}[X]$, deren zugehörige Galois-Gruppe nicht auflösbar ist.

Übungsaufgaben

1. *Es sei K ein Körper und $f \in K[X]$ ein nicht-konstantes separables Polynom. Sei K_0 der kleinste Teilkörper von K, der alle Koeffizienten von f enthält. Welche Beziehung besteht zwischen der Auflösbarkeit der Gleichung $f(x) = 0$ über K und über K_0?*

2. *Es sei K ein Körper und $f \in K[X]$ ein separables nicht-konstantes Polynom. In älterer Terminologie nennt man die algebraische Gleichung $f(x) = 0$* metazyklisch, *wenn sie sich auf eine Kette zyklischer Gleichungen zurückführen lässt. Genauer bedeutet dies folgendes: Ist L ein Zerfällungskörper von f über K, so gibt es eine Körperkette $K = K_0 \subset K_1 \subset \ldots \subset K_n$ mit $L \subset K_n$ und der Eigenschaft, dass K_{i+1}/K_i jeweils eine Galois-Erweiterung zu einer zyklischen*

Gleichung ist, also mit zyklischer Galois-Gruppe. Zeige, dass die Gleichung $f(x) = 0$ *genau dann metazyklisch ist, wenn sie auflösbar* (*bzw. durch Radikale auflösbar*) *ist.*

3. Bestimme die Galois-Gruppe des Polynoms

$$X^7 - 8X^5 - 4X^4 + 2X^3 - 4X^2 + 2 \in \mathbb{Q}[X]$$

und entscheide, ob diese auflösbar ist oder nicht.

4. Entscheide, ob die Gleichung

$$X^7 + 4X^5 - \tfrac{10}{11}X^3 - 4X + \tfrac{2}{11} = 0$$

mit Koeffizienten aus $\mathbb{Q}$ durch Radikale auflösbar ist oder nicht.

5. Zeige, dass es zu jeder Primzahl $p \geq 5$ ein irreduzibles Polynom $f_p \in \mathbb{Q}[X]$ mit $\operatorname{grad} f_p = p$ gibt, dessen zugehörige Galois-Gruppe (über $\mathbb{Q}$) isomorph zu $\mathfrak{S}_p$ ist. (*Hinweis*: Starte mit einem separablen Polynom $h_p \in \mathbb{Q}[X]$ vom Grade p, welches genau zwei nicht-reelle Nullstellen besitzt, und approximiere h_p durch ein geeignetes irreduzibles Polynom f_p. Benutze dabei, dass sich die Nullstellen von h_p bei stetiger Abänderung der Koeffizienten von h_p ebenfalls in stetiger Weise ändern.)

6. Betrachte für eine Primzahl p die Gruppe $S(\mathbb{F}_p)$ der bijektiven Selbstabbildungen $\mathbb{F}_p \longrightarrow \mathbb{F}_p$ des Körpers $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$. Ein Element $\sigma \in S(\mathbb{F}_p)$ heiße *linear*, wenn es $a, b \in \mathbb{F}_p$ gibt mit $\sigma(x) = ax + b$ für alle $x \in \mathbb{F}_p$, wobei dann notwendigerweise $a \neq 0$ folgt. Eine Untergruppe $G \subset S(\mathbb{F}_p)$ heiße *linear*, wenn alle Elemente $\sigma \in G$ linear sind. Schließlich nennen wir eine Untergruppe $G \subset \mathfrak{S}_p$ *linear*, wenn es eine Bijektion $\{1, \ldots, p\} \longrightarrow \mathbb{F}_p$ gibt, unter welcher G zu einer linearen Untergruppe von $\mathfrak{S}_p$ korrespondiert. Zeige:

   (i) Ist $\sigma \in S(\mathbb{F}_p)$ linear und besitzt σ mindestens zwei verschiedene Fixpunkte, so gilt $\sigma = \mathrm{id}$.

   (ii) Jede Untergruppe $G \subset \mathfrak{S}_p$, welche auflösbar ist und transitiv auf $\{1, \ldots, p\}$ operiert, ist linear.

   (iii) Jede lineare Untergruppe $G \subset \mathfrak{S}_p$ ist auflösbar.

   (iv) Die Galois-Gruppe eines irreduziblen Polynoms vom Grad p ist linear, sofern sie auflösbar ist.

6.2 Algebraische Gleichungen vom Grad 3 und 4*

Es sei K ein Körper, $f \in K[X]$ ein separables normiertes Polynom und L ein Zerfällungskörper von f über K. Wie wir gesehen haben, ist die algebraische Gleichung $f(x) = 0$ genau dann durch Radikale auflösbar, wenn die zugehörige Galois-Gruppe $\mathrm{Gal}(L/K)$ auflösbar im gruppentheoretischen Sinne ist. Letzteres ist äquivalent zur Existenz einer Normalreihe

$$\mathrm{Gal}\big(L/K\big) = G_0 \supset G_1 \supset \ldots \supset G_r = \{1\}$$

mit (endlichen) zyklischen Faktoren; vgl. 5.4/7. Gehen wir nun von einer solchen Normalreihe aus, so korrespondiert hierzu aufgrund des Hauptsatzes der Galois-Theorie 4.1/6 eine Körperkette

$$K = E_0 \subset E_1 \subset \ldots \subset E_r = L,$$

derart dass E_i/E_{i-1} für $i = 1, \ldots, r$ eine zyklische Erweiterung mit Galois-Gruppe G_{i-1}/G_i ist. Den Schlüssel zur Auflösung der Gleichung $f(x) = 0$ liefert in dieser Situation die in 4.8/3 (i) gegebene Charakterisierung zyklischer Erweiterungen: Unter der Voraussetzung, dass E_{i-1} eine Einheitswurzel der Ordnung $n_i = [E_i : E_{i-1}]$ enthält und $\mathrm{char}\, K$ den Grad n_i nicht teilt, entsteht E_i aus E_{i-1} durch Adjunktion einer n_i-ten Wurzel eines Elementes $c_i \in E_i$, wobei c_i allerdings in nicht-konstruktiver Weise mit Hilfe von Hilberts Satz 90 bestimmt wird.

Um nun für konkretes f zu Lösungsformeln der Gleichung $f(x) = 0$ zu gelangen, müssen wir wie beschrieben vorgehen und gleichzeitig versuchen, die auftauchenden Körpererweiterungen explizit zu beschreiben. Wir interessieren uns lediglich für Polynome f der Grade 2, 3 und 4 und fassen dementsprechend die zugehörige Galois-Gruppe $\mathrm{Gal}(L/K)$ als Untergruppe von $\mathfrak{S}_2$, $\mathfrak{S}_3$ bzw. $\mathfrak{S}_4$ auf. Für diese Permutationsgruppen stehen folgende Normalreihen mit zyklischen Faktoren zur Verfügung:

$$\begin{gathered}\mathfrak{S}_2 \supset \mathfrak{A}_2 = \{1\},\\ \mathfrak{S}_3 \supset \mathfrak{A}_3 \supset \{1\},\\ \mathfrak{S}_4 \supset \mathfrak{A}_4 \supset \mathfrak{V}_4 \supset \mathfrak{Z} \supset \{1\}.\end{gathered}$$

Dabei bezeichnet $\mathfrak{A}_n$ jeweils die alternierende Gruppe, $\mathfrak{V}_4$ die Kleinsche Vierergruppe, sowie $\mathfrak{Z}$ eine zyklische Untergruppe der Ordnung 2 in $\mathfrak{V}_4$; vgl. Abschnitt 5.3.

Es seien nun $x_1, \ldots, x_n \in L$ die Nullstellen von f. Wir können die Galois-Gruppe $\mathrm{Gal}(L/K)$ dann als Untergruppe von $\mathfrak{S}_n$ auffassen. Nehmen wir für einen Moment $\mathrm{Gal}(L/K) = \mathfrak{S}_n$ an und betrachten $\mathfrak{A}_n$ als Untergruppe von $\mathrm{Gal}(L/K)$, so lässt sich der zugehörige Zwischenkörper E_1 von L/K relativ leicht explizit beschreiben. Man nennt $\Delta = \delta^2$ mit

$$\delta = \prod_{i<j} (x_i - x_j)$$

die *Diskriminante* des Polynoms f; vgl. Abschnitt 4.4. Es gilt $\Delta \neq 0$, da f als separabel vorausgesetzt war. Weiter ist Δ invariant unter allen Permutationen $\pi \in \mathfrak{S}_n$ und gehört folglich zu K. In Abschnitt 4.4, vgl. insbesondere 4.4/10, haben wir genauer gezeigt, wie man Δ aus den Koeffizienten von f berechnen kann. Gilt $\mathrm{char}\, K \neq 2$, so ist im Übrigen die Quadratwurzel δ zu Δ genau dann invariant unter einer Permutation $\pi \in \mathfrak{S}_n$, wenn π gerade ist, also zu $\mathfrak{A}_n$ gehört. Dies bedeutet $K(\sqrt{\Delta}) \subset L^{\mathfrak{A}_n} = E_1$ und wegen $\sqrt{\Delta} \notin K$ sogar $K(\sqrt{\Delta}) = E_1$. Der Schritt $\mathfrak{S}_n \supset \mathfrak{A}_n$ wird folglich für $\mathrm{char}\, K \neq 2$ auf der Körperseite durch die Adjunktion einer Quadratwurzel der Diskriminante Δ realisiert.

Nach diesen allgemeinen Betrachtungen wollen wir uns nun den speziellen Auflösungsformeln für algebraische Gleichungen $f(x) = 0$ vom Grad ≤ 4 zuwenden, wobei wir f als nicht notwendig irreduzibel oder separabel annehmen. Voraussetzungen an die Charakteristik von K werden aber garantieren, dass der Zerfällungskörper L von f stets separabel und damit galoissch über K ist. Wir beginnen mit einem Polynom $f \in K[X]$ *zweiten Grades*, etwa

$$f = X^2 + aX + b,$$

wobei $\mathrm{char}\, K \neq 2$ gelte. Man könnte wie üblich schnell mit Hilfe der quadratischen Ergänzung zum Ziel gelangen. Wir wollen aber, wie oben angedeutet, die Diskriminante benutzen. Es sei also L ein Zerfällungskörper von f über K, und x_1, x_2 seien die Nullstellen von f in L. Die Diskriminante von f berechnet sich zu $\Delta = a^2 - 4b$. Es ist dann $\delta = x_1 - x_2$ eine Quadratwurzel zu Δ, und es gilt $x_1 + x_2 = -a$, also

$$x_1 = \tfrac{1}{2}(-a + \delta), \qquad x_2 = \tfrac{1}{2}(-a - \delta),$$

bzw.

$$x_{1/2} = -\frac{a}{2} \pm \sqrt{\frac{a^2}{4} - b}.$$

Dies sind die bekannten Lösungsformeln für quadratische Gleichungen.

Als Nächstes wollen wir ein Polynom $f \in K[X]$ *dritten Grades* betrachten, etwa

$$f = X^3 + aX^2 + bX + c,$$

wobei wir $\operatorname{char} K \neq 2, 3$ voraussetzen. Mittels kubischer Ergänzung, man ersetze X durch $X - \frac{1}{3}a$, können wir annehmen, dass f von der etwas einfacheren Gestalt

$$f = X^3 + pX + q$$

ist. L sei wieder ein Zerfällungskörper von f, und x_1, x_2, x_3 seien die Nullstellen von f in L. Die Diskriminante von f bestimmt sich zu $\Delta = -4p^3 - 27q^2$; vgl. die Rechnung im Anschluss an 4.4/10. Zur Lösung der Gleichung $f(x) = 0$ ist es nützlich, sich zunächst den Fall $\operatorname{Gal}(L/K) = \mathfrak{S}_n$ anzuschauen, den wir als den *generischen Fall* bezeichnen. Unsere Rechnungen sind jedoch, wie wir sehen werden, für beliebige Galois-Gruppen $\operatorname{Gal}(L/K)$ gültig.

Gemäß der Normalreihe $\mathfrak{S}_3 \supset \mathfrak{A}_3 \supset \{1\}$ adjungieren wir zunächst zu K eine Quadratwurzel

$$\delta = (x_1 - x_2)(x_1 - x_3)(x_2 - x_3) = \sqrt{\Delta}$$

der Diskriminante Δ. Im generischen Fall, den wir für einen Moment verfolgen wollen, ist $L/K(\delta)$ dann eine zyklische Galois-Erweiterung vom Grad 3. Motiviert durch die Voraussetzungen in 4.8/3 (i) adjungieren wir weiter eine primitive dritte Einheitswurzel ζ zu $K(\delta)$ bzw. K und setzen der Einfachheit halber von nun an $\zeta \in K$ voraus. Es entsteht dann $L/K(\delta)$ durch Adjunktion einer dritten Wurzel eines Elementes aus $K(\delta)$. Eine Zurückverfolgung der Konstruktionen in 4.8/3 und 4.8/1 zeigt, dass man diese Wurzel als sogenannte *Lagrangesche Resolvente*

$$(\zeta, x) = x + \zeta\sigma(x) + \zeta^2\sigma^2(x)$$

mit einem geeigneten Element $x \in L$ wählen kann; σ ist dabei ein erzeugendes Element der zyklischen Gruppe $\operatorname{Gal}(L/K(\delta))$.

Da ein spezielles Element x wie gerade beschrieben nicht in kanonischer Weise zur Verfügung steht, nutzen wir die Nullstellen x_1, x_2, x_3, um "Resolventen" durch

$$(1,x) = x_1 + x_2 + x_3 = 0,$$
$$(\zeta,x) = x_1 + \zeta x_2 + \zeta^2 x_3,$$
$$(\zeta^2,x) = x_1 + \zeta^2 x_2 + \zeta x_3$$

zu erklären; zur Motivation dürfen wir uns $x = x_1, \sigma(x) = x_2$ und $\sigma^2(x) = x_3$ vorstellen. Indem wir benutzen, dass die primitiven dritten Einheitswurzeln

$$\zeta = -\tfrac{1}{2} + \tfrac{1}{2}\sqrt{-3}, \qquad \zeta^2 = -\tfrac{1}{2} - \tfrac{1}{2}\sqrt{-3} \tag{0}$$

Nullstellen des Kreisteilungspolynoms $\Phi_3 = X^2 + X + 1 \in \mathbb{Z}[X]$ sind, können wir die Nullstellen x_1, x_2, x_3 von f wie folgt ausdrücken:

$$\begin{aligned} x_1 &= \tfrac{1}{3}\big((\zeta,x) + (\zeta^2,x)\big), \\ x_2 &= \tfrac{1}{3}\big(\zeta^2(\zeta,x) + \zeta(\zeta^2,x)\big), \\ x_3 &= \tfrac{1}{3}\big(\zeta(\zeta,x) + \zeta^2(\zeta^2,x)\big). \end{aligned} \tag{1}$$

Unser Ziel ist es daher, die genannten Resolventen zu bestimmen. Da die Erweiterung $L/K(\delta)$ im generischen Fall $\mathfrak{A}_3$ als Galois-Gruppe besitzt, sind die dritten Potenzen der Resolventen (ζ,x), (ζ^2,x) invariant unter $\mathrm{Gal}(L/K(\delta))$ und folglich enthalten in $K(\delta)$. Wir wollen dies auch durch Rechnung nachprüfen. Mit

$$\begin{aligned} \delta &= (x_1 - x_2)(x_1 - x_3)(x_2 - x_3) \\ &= x_1^2 x_2 + x_2^2 x_3 + x_3^2 x_1 - x_1^2 x_3 - x_2^2 x_1 - x_3^2 x_2 \end{aligned}$$

und (0) ergibt sich unabhängig vom generischen Fall

$$\begin{aligned} (\zeta,x)^3 &= x_1^3 + x_2^3 + x_3^3 + 3\zeta(x_1^2 x_2 + x_2^2 x_3 + x_3^2 x_1) \\ &\quad + 3\zeta^2(x_1^2 x_3 + x_2^2 x_1 + x_3^2 x_2) + 6x_1x_2x_3 \\ &= \textstyle\sum_i x_i^3 - \frac{3}{2}\sum_{i\neq j} x_i^2 x_j + 6x_1x_2x_3 + \frac{3}{2}\sqrt{-3}\cdot\delta. \end{aligned}$$

Dabei ist die spezielle Wahl der Quadratwurzel $\sqrt{-3}$ ohne Belang. Ersetzen von $\sqrt{-3}$ durch $-\sqrt{-3}$ bewirkt eine Vertauschung der Größen ζ und ζ^2 bzw. (ζ,x) und (ζ^2,x). Insbesondere lässt sich $(\zeta^2,x)^3$ berechnen, indem man in der obigen Formel $\sqrt{-3}$ durch $-\sqrt{-3}$ ersetzt.

Wir wollen $(\zeta,x)^3$ als symmetrische Funktion in x_1, x_2, x_3 auffassen und durch die elementarsymmetrischen Polynome

$$\sigma_1 = s_1(x_1, x_2, x_3) = x_1 + x_2 + x_3 = 0,$$
$$\sigma_2 = s_2(x_1, x_2, x_3) = x_1x_2 + x_1x_3 + x_2x_3 = p,$$
$$\sigma_3 = s_3(x_1, x_2, x_3) = x_1x_2x_3 = -q$$

ausdrücken, um eine Darstellung in den Koeffizienten p, q der betrachteten Gleichung zu erhalten. Dabei benutzen wir das Verfahren aus dem Beweis zu Satz 4.3/5.

$$\begin{array}{rcl}
(\zeta, x)^3 & = & \sum_i x_i^3 - \frac{3}{2}\sum_{i\neq j} x_i^2x_j + 6x_1x_2x_3 + \frac{3}{2}\sqrt{-3}\cdot\delta \\
\sigma_1^3 & = & \sum_i x_i^3 + 3\sum_{i\neq j} x_i^2x_j + 6x_1x_2x_3 \\
\hline
 & & -\frac{9}{2}\sum_{i\neq j} x_i^2x_j + \frac{3}{2}\sqrt{-3}\cdot\delta \\
-\frac{9}{2}\sigma_1\sigma_2 & = & -\frac{9}{2}\sum_{i\neq j} x_i^2x_j - \frac{27}{2}x_1x_2x_3 \\
\hline
 & & \frac{27}{2}x_1x_2x_3 + \frac{3}{2}\sqrt{-3}\cdot\delta \\
\frac{27}{2}\sigma_3 & = & \frac{27}{2}x_1x_2x_3 \\
\hline
 & & \frac{3}{2}\sqrt{-3}\cdot\delta
\end{array}$$

Folglich erhält man $(\zeta, x)^3 = \sigma_1^3 - \frac{9}{2}\sigma_1\sigma_2 + \frac{27}{2}\sigma_3 + \frac{3}{2}\sqrt{-3}\cdot\delta$, mithin wegen $\sigma_1 = 0$ und $\sigma_3 = -q$

$$(\zeta, x)^3 = -\tfrac{27}{2}q + \tfrac{3}{2}\sqrt{-3}\cdot\delta = -\tfrac{27}{2}q + 27\sqrt{(\tfrac{p}{3})^3 + (\tfrac{q}{2})^2}, \tag{2}$$

sowie entsprechend

$$(\zeta^2, x)^3 = -\tfrac{27}{2}q - \tfrac{3}{2}\sqrt{-3}\cdot\delta = -\tfrac{27}{2}q - 27\sqrt{(\tfrac{p}{3})^3 + (\tfrac{q}{2})^2}. \tag{3}$$

Die Resolventen (ζ, x) und (ζ^2, x) sind durch diese Gleichungen bis auf eine dritte Einheitswurzel bestimmt. Die Gleichungen (1) für x_1, x_2, x_3 zeigen weiter, dass man (ζ, x) durch $\zeta(\zeta, x)$ ersetzen darf, wenn man gleichzeitig (ζ^2, x) durch $\zeta^2(\zeta^2, x)$ ersetzt. Dies lässt vermuten, dass die dritten Wurzeln beim Lösen der Gleichungen (2) und (3) nicht unabhängig voneinander gewählt werden dürfen, wenn man mittels (1) zu Lösungen der Gleichung $x^3 + px + q = 0$ gelangen möchte. In der Tat, es besteht die Beziehung

$$\begin{aligned}
(\zeta, x)(\zeta^2, x) &= (x_1 + \zeta x_2 + \zeta^2 x_3)(x_1 + \zeta^2 x_2 + \zeta x_3) \\
&= x_1^2 + x_2^2 + x_3^2 + (\zeta + \zeta^2)(x_1x_2 + x_1x_3 + x_2x_3) \\
&= \sigma_1^2 - 3\sigma_2 = -3\sigma_2 = -3p,
\end{aligned}$$

welche diesen Sachverhalt bestätigt. Folglich können wir feststellen:

Satz 1 (Cardanosche Formeln). *Es sei K ein Körper der Charakteristik* $\operatorname{char} K \neq 2, 3$. *Für $p, q \in K$ werden die Lösungen der algebraischen Gleichung $x^3 + px + q = 0$ gegeben durch*

$$x_1 = u + v, \qquad x_2 = \zeta^2 u + \zeta v, \qquad x_3 = \zeta u + \zeta^2 v.$$

Dabei ist $\zeta \in \overline{K}$ eine beliebige primitive dritte Einheitswurzel, sowie

$$u = \sqrt[3]{-\frac{q}{2} + \sqrt{\left(\frac{p}{3}\right)^3 + \left(\frac{q}{2}\right)^2}}, \qquad v = \sqrt[3]{-\frac{q}{2} - \sqrt{\left(\frac{p}{3}\right)^3 + \left(\frac{q}{2}\right)^2}},$$

wobei die dritten Wurzeln mit der Nebenbedingung $uv = -\frac{1}{3}p$ zu wählen sind.

Beweis. Ersetzt man bei den vorstehenden Ausdrücken u, v durch $\zeta u, \zeta^2 v$ bzw. $\zeta^2 u, \zeta v$, so bewirkt dies lediglich eine Permutation von x_1, x_2, x_3. Wir dürfen daher ohne Einschränkung $u = \frac{1}{3}(\zeta, x)$ sowie $v = \frac{1}{3}(\zeta^2, x)$ annehmen. Die im Satz angegebenen Größen x_1, x_2, x_3 stimmen dann aufgrund der Formeln (1) mit den Lösungen der Gleichung $x^3 + px + q = 0$ überein. □

Wir wollen schließlich noch ein Polynom *vierten Grades* $f \in K[X]$ betrachten, etwa

$$f = X^4 + pX^2 + qX + r,$$

wobei wir wiederum $\operatorname{char} K \neq 2, 3$ voraussetzen. Der Allgemeinfall lässt sich wie üblich durch eine Substitution des Typs $X \longmapsto X - \frac{1}{4}c$ auf diesen Spezialfall zurückführen. Es seien x_1, x_2, x_3, x_4 die Nullstellen von f in einem Zerfällungskörper L von f über K; diese erfüllen dann die Relation $x_1 + x_2 + x_3 + x_4 = 0$. Ähnlich wie bei Polynomen dritten Grades orientieren wir uns bei unseren Überlegungen an dem *generischen Fall* $\operatorname{Gal}(L/K) = \mathfrak{S}_4$. Zusätzlich sei hierbei vorausgesetzt, dass x_1, x_2, x_3 algebraisch unabhängig über dem Primkörper von K sind. Dieser generische Fall wird beispielsweise realisiert, wenn wir die allgemeine Gleichung vierten Grades auf die hier betrachtete Form transformieren. Man beachte jedoch, dass die nachfolgend ausgeführten Rechnungen unabhängig von diesen speziellen Voraussetzungen gültig sind.

Im generischen Fall können wir die bereits oben erwähnte Normalreihe

$$\mathfrak{S}_4 \supset \mathfrak{A}_4 \supset \mathfrak{B}_4 \supset \mathfrak{Z} \supset \{1\}$$

sowie die hierzu korrespondierende Körperkette

$$K \subset L^{\mathfrak{A}_4} \subset L^{\mathfrak{B}_4} \subset L^3 \subset L$$

betrachten. Wie üblich gilt $L^{\mathfrak{A}_4} = K(\delta)$ für eine Quadratwurzel δ der Diskriminante Δ von f, wobei man

$$\Delta = 144pq^2r - 128p^2r^2 - 4p^3q^2 + 16p^4r - 27q^4 + 256r^3$$

mittels 4.4/10 ausrechnet. Wir werden dies allerdings nicht weiter benötigen. Die Erweiterung $L^{\mathfrak{B}_4}/L^{\mathfrak{A}_4}$ ist vom Grad 3 und wird erzeugt durch ein beliebiges Element aus $L^{\mathfrak{B}_4}$, welches nicht zu $L^{\mathfrak{A}_4}$ gehört, beispielsweise von

$$z_1 = (x_1 + x_2)(x_3 + x_4) \in L.$$

Um dies einzusehen, beachte man, dass z_1 nicht von der Permutation $(1,2,3) \in \mathfrak{A}_4$ festgelassen wird. Andererseits ist z_1 invariant unter allen Elementen in $\mathfrak{B}_4$ und, zusätzlich, unter den Permutationen $(1,2)$, $(3,4)$, $(1,3,2,4)$ und $(1,4,2,3)$. Insgesamt handelt es sich dabei um die Elemente der Isotropiegruppe von z_1 in $\mathfrak{S}_4$. Mittels 5.1/6 sehen wir sodann, dass die Bahn von z_1 in $\mathfrak{S}_4$ aus genau den folgenden drei Elementen besteht:

$$\begin{aligned} z_1 &= (x_1 + x_2)(x_3 + x_4), \\ z_2 &= (x_1 + x_3)(x_2 + x_4), \\ z_3 &= (x_1 + x_4)(x_2 + x_3). \end{aligned}$$

Insbesondere sind z_1, z_2, z_3 die Wurzeln einer Gleichung dritten Grades mit Koeffizienten aus K, nämlich von

$$z^3 - b_1z^2 + b_2z - b_3 = 0,$$

wobei b_1, b_2, b_3 die elementarsymmetrischen Polynome in z_1, z_2, z_3 sind, also[1]

[1] Bei den nachfolgenden Summationen variieren die Indizes jeweils in $\{1,2,3,4\}$. Unterschiedliche Indizes dürfen innerhalb einer Summe nur *paarweise verschiedene* Werte annehmen.

$$
\begin{aligned}
b_1 &= z_1 + z_2 + z_3 &&= 2\sum_{i<j} x_i x_j,\\
b_2 &= z_1z_2 + z_1z_3 + z_2z_3 &&= \sum_{i<j} x_i^2x_j^2 + 3\sum_{\substack{i\\ j<k}} x_i^2x_jx_k + 6x_1x_2x_3x_4,\\
b_3 &= z_1z_2z_3 &&= \sum_{i,j,k} x_i^3x_j^2x_k + 2\sum_{\substack{i\\ j<k<l}} x_i^3x_jx_kx_l\\
& && \quad + 2\sum_{i<j<k} x_i^2x_j^2x_k^2 + 4\sum_{\substack{i<j\\ k<l}} x_i^2x_j^2x_kx_l.
\end{aligned}
$$

Es sind b_1, b_2, b_3 symmetrische Funktionen in x_1, x_2, x_3, x_4, und wir wollen diese als Funktionen in den elementarsymmetrischen Polynomen

$$
\begin{aligned}
\sigma_1 &= s_1(x_1,x_2,x_3,x_4) = \textstyle\sum_i x_i &&= 0,\\
\sigma_2 &= s_2(x_1,x_2,x_3,x_4) = \textstyle\sum_{i<j} x_ix_j &&= p,\\
\sigma_3 &= s_3(x_1,x_2,x_3,x_4) = \textstyle\sum_{i<j<k} x_ix_jx_k &&= -q,\\
\sigma_4 &= s_4(x_1,x_2,x_3,x_4) = x_1x_2x_3x_4 &&= r
\end{aligned}
$$

schreiben, damit wir die b_i durch die Koeffizienten p, q, r unserer Gleichung ausdrücken können. Zunächst gilt $b_1 = 2\sigma_2 = 2p$. Für b_2 führen wir folgende Rechnung durch, wobei wir wieder das Verfahren aus dem Beweis zu Satz 4.3/5 benutzen:

$$
\begin{array}{rl}
b_2 = & \displaystyle\sum_{i<j} x_i^2x_j^2 \;+\; 3\sum_{\substack{i\\ j<k}} x_i^2x_jx_k \;+\; 6x_1x_2x_3x_4\\
\sigma_2^2 = & \displaystyle\sum_{i<j} x_i^2x_j^2 \;+\; 2\sum_{\substack{i\\ j<k}} x_i^2x_jx_k \;+\; 6x_1x_2x_3x_4\\
\hline
 & \displaystyle\sum_{\substack{i\\ j<k}} x_i^2x_jx_k\\
\sigma_1\sigma_3 = & \displaystyle\sum_{\substack{i\\ j<k}} x_i^2x_jx_k \;+\; 4x_1x_2x_3x_4\\
\hline
 & -\;4x_1x_2x_3x_4\\
-4\sigma_4 = & -\;4x_1x_2x_3x_4\\
\hline
 & 0
\end{array}
$$

Dies ergibt $b_2 = \sigma_2^2 + \sigma_1\sigma_3 - 4\sigma_4 = p^2 - 4r$ wegen $\sigma_1 = 0$. Schließlich stellen wir noch b_3 mittels $\sigma_1, \sigma_2, \sigma_3, \sigma_4$ dar:

$$
\begin{aligned}
b_3 &= \sum_{i,j,k} x_i^3 x_j^2 x_k + 2 \sum_{\substack{i \\ j<k<l}} x_i^3 x_j x_k x_l + 2 \sum_{i<j<k} x_i^2 x_j^2 x_k^2 + 4 \sum_{\substack{i<j \\ k<l}} x_i^2 x_j^2 x_k x_l \\
\sigma_1\sigma_2\sigma_3 &= \sum_{i,j,k} x_i^3 x_j^2 x_k + 3 \sum_{\substack{i \\ j<k<l}} x_i^3 x_j x_k x_l + 3 \sum_{i<j<k} x_i^2 x_j^2 x_k^2 + 8 \sum_{\substack{i<j \\ k<l}} x_i^2 x_j^2 x_k x_l \\
\hline
& \quad - \sum_{\substack{i \\ j<k<l}} x_i^3 x_j x_k x_l \quad - \sum_{i<j<k} x_i^2 x_j^2 x_k^2 \quad - 4 \sum_{\substack{i<j \\ k<l}} x_i^2 x_j^2 x_k x_l \\
-\sigma_1^2\sigma_4 &= \quad - \sum_{\substack{i \\ j<k<l}} x_i^3 x_j x_k x_l \qquad\qquad\quad - 2 \sum_{\substack{i<j \\ k<l}} x_i^2 x_j^2 x_k x_l \\
\hline
& \qquad\qquad\qquad - \sum_{i<j<k} x_i^2 x_j^2 x_k^2 \quad - 2 \sum_{\substack{i<j \\ k<l}} x_i^2 x_j^2 x_k x_l \\
-\sigma_3^2 &= \qquad\qquad\qquad - \sum_{i<j<k} x_i^2 x_j^2 x_k^2 \quad - 2 \sum_{\substack{i<j \\ k<l}} x_i^2 x_j^2 x_k x_l \\
\hline
& \qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad 0
\end{aligned}
$$

Hieraus folgt $b_3 = \sigma_1\sigma_2\sigma_3 - \sigma_1^2\sigma_4 - \sigma_3^2 = -q^2$, wiederum wegen $\sigma_1 = 0$, und wir erkennen unabhängig von den Voraussetzungen des generischen Falls z_1, z_2, z_3 als die Lösungen der Gleichung

$$z^3 - 2pz^2 + (p^2 - 4r)z + q^2 = 0.$$

Diese Gleichung wird auch als *kubische Resolvente* der Gleichung vierten Grades bezeichnet; ihre Lösungen z_1, z_2, z_3 können mittels der Cardanoschen Formeln bestimmt werden.

Im generischen Fall, den wir im Folgenden weiter betrachten, erkennt man $\mathfrak{V}_4$ als diejenige Untergruppe von $\mathfrak{S}_4$, welche die Elemente z_1, z_2, z_3 festlässt. Dies bedeutet $\mathrm{Gal}(L/K(z_1, z_2, z_3)) = \mathfrak{V}_4$ sowie $K(z_1, z_2, z_3) = L^{\mathfrak{V}_4}$. Um nun von $K(z_1, z_2, z_3)$ zu L zu gelangen, sind zwei Quadratwurzeln zu adjungieren, etwa gemäß der Kette $\mathfrak{V}_4 \supset \mathfrak{Z} \supset \{1\}$. Es ist $x_1 + x_2$ invariant unter den Elementen (1) und $(1,2)(3,4)$ von $\mathfrak{V}_4$, nicht aber unter den übrigen Elementen von $\mathfrak{V}_4$. Folglich besitzt $x_1 + x_2$ den Grad 2 über $K(z_1, z_2, z_3)$. In der Tat, unabhängig hiervon gilt

$$(x_1 + x_2)(x_3 + x_4) = z_1, \qquad x_1 + x_2 + x_3 + x_4 = 0,$$

also

$$x_1 + x_2 = \sqrt{-z_1}, \qquad x_3 + x_4 = -\sqrt{-z_1},$$

bei Wahl einer geeigneten Quadratwurzel zu $-z_1$. Entsprechend hat man

$$\begin{aligned} x_1 + x_3 &= \sqrt{-z_2}, & x_2 + x_4 &= -\sqrt{-z_2}, \\ x_1 + x_4 &= \sqrt{-z_3}, & x_2 + x_3 &= -\sqrt{-z_3}, \end{aligned}$$

sowie als Konsequenz

$$\begin{aligned} x_1 &= \tfrac{1}{2}(\ \ \sqrt{-z_1} + \sqrt{-z_2} + \sqrt{-z_3}), \\ x_2 &= \tfrac{1}{2}(\ \ \sqrt{-z_1} - \sqrt{-z_2} - \sqrt{-z_3}), \\ x_3 &= \tfrac{1}{2}(-\sqrt{-z_1} + \sqrt{-z_2} - \sqrt{-z_3}), \\ x_4 &= \tfrac{1}{2}(-\sqrt{-z_1} - \sqrt{-z_2} + \sqrt{-z_3}). \end{aligned}$$

Ähnlich wie bei den kubischen Gleichungen ergibt sich die Frage nach der speziellen Wahl der benötigten Wurzeln zu $-z_1, -z_2, -z_3$. Es gilt

$$\begin{aligned} (x_1 + x_2)(x_1 + x_3)(x_1 + x_4) &= x_1^2(x_1 + x_2 + x_3 + x_4) + \textstyle\sum_{i<j<k} x_i x_j x_k \\ &= \textstyle\sum_{i<j<k} x_i x_j x_k \\ &= -q. \end{aligned}$$

Wir sehen also, dass wir zur Beschreibung der Nullstellen x_1, x_2, x_3, x_4 die Quadratwurzeln $\sqrt{-z_1}, \sqrt{-z_2}, \sqrt{-z_3}$ mit der Nebenbedingung

$$\sqrt{-z_1} \cdot \sqrt{-z_2} \cdot \sqrt{-z_3} = -q$$

wählen müssen. Als Konsequenz erhalten wir:

Satz 2. *Es sei K ein Körper mit* $\operatorname{char} K \neq 2, 3$. *Für $p, q, r \in K$ werden die Lösungen der algebraischen Gleichung $x^4 + px^2 + qx + r = 0$ gegeben durch*

$$\begin{aligned} x_1 &= \tfrac{1}{2}(\ \ \sqrt{-z_1} + \sqrt{-z_2} + \sqrt{-z_3}), \\ x_2 &= \tfrac{1}{2}(\ \ \sqrt{-z_1} - \sqrt{-z_2} - \sqrt{-z_3}), \\ x_3 &= \tfrac{1}{2}(-\sqrt{-z_1} + \sqrt{-z_2} - \sqrt{-z_3}), \\ x_4 &= \tfrac{1}{2}(-\sqrt{-z_1} - \sqrt{-z_2} + \sqrt{-z_3}). \end{aligned}$$

Dabei sind z_1, z_2, z_3 die Lösungen der kubischen Resolvente

$$z^3 - 2pz^2 + (p^2 - 4r)z + q^2 = 0,$$

und es sind die Quadratwurzeln mit der Nebenbedingung

$$\sqrt{-z_1} \cdot \sqrt{-z_2} \cdot \sqrt{-z_3} = -q$$

zu wählen.

Abschließend bemerken wir noch, dass wegen

$$\begin{aligned} z_1 - z_2 &= -(x_1 - x_4)(x_2 - x_3), \\ z_1 - z_3 &= -(x_1 - x_3)(x_2 - x_4), \\ z_2 - z_3 &= -(x_1 - x_2)(x_3 - x_4) \end{aligned}$$

die Diskriminante von X^4+pX^2+qX+r mit der Diskriminante der kubischen Resolvente $X^3 - 2pX^2 + (p^2 - 4r)X + q^2$ übereinstimmt.

Lernkontrolle und Prüfungsvorbereitung

1. Sei f ein separables Polynom mit Koeffizienten aus einem Körper K, und seien $x_1, \ldots, x_n$ die Nullstellen von f in einem Zerfällungskörper L/K. Für die Galois-Gruppe zu L/K gelte $\mathrm{Gal}(L/K) = \mathfrak{S}_n$. Beschreibe die Erweiterung $L^{\mathfrak{A}_n}/K$ mittels der Diskriminante Δ von f.
2. Leite die Lösungsformeln für quadratische Gleichungen unter Nutzung der Diskriminante her wie in Punkt 1.
3. Beschreibe die Normalreihe in $\mathfrak{S}_3$, an der man sich bei der Lösung algebraischer Gleichungen dritten Grades orientiert. Erkläre die Problematik, die sich ergibt, wenn man die Normalreihe in eine formelmäßige Beschreibung der zugehörigen Erweiterungen auf der Körperseite umsetzen möchte.

+4. Skizziere in Fortführung von Punkt 3 das Vorgehen zur Auflösung algebraischer Gleichungen dritten Grades mittels geeigneter Resultanten, deren dritte Potenzen eine quadratische Gleichung über dem Grundkörper erfüllen, und erläutere insbesondere die Cardanoschen Formeln.

5. Von welcher Normalreihe in $\mathfrak{S}_4$ geht man aus, wenn man eine algebraische Gleichung $f(x) = 0$ vom Grad 4 auflösen möchte? Erkläre den entscheidenden Schritt in dieser Reihe, der zum Auffinden der kubischen Resolvente führt.

+6. Skizziere in Fortführung von Punkt 5 die Auflösung algebraischer Gleichungen vierten Grades.

Übungsaufgaben

1. *Es sei K ein Teilkörper von $\mathbb{R}$. Weiter seien $f, g \in K[X]$ normierte irreduzible Polynome vierten bzw. dritten Grades, derart dass $g(z) = 0$ die kubische Resolvente der algebraischen Gleichung $f(x) = 0$ ist (unter der Annahme, dass der kubische Term von f trivial ist). Berechne die Galois-Gruppe der Gleichung $f(x) = 0$ unter der Voraussetzung, dass f keine reellen Nullstellen hat.*
2. Es sei K ein Körper und L ein Zerfällungskörper eines normierten Polynoms vierten Grades $f \in K[X]$, wobei wir annehmen, dass der kubische Term von f trivial ist. Weiter sei L' mit $K \subset L' \subset L$ ein Zerfällungskörper der kubischen Resolvente zu f. Interpretiere die Galois-Gruppe $G = \mathrm{Gal}(L/K)$ als Untergruppe von $\mathfrak{S}_4$ und zeige, dass $G \cap \mathfrak{V}_4$ ein Normalteiler in G ist mit $\mathrm{Gal}(L'/K) = G/(G \cap \mathfrak{V}_4)$.

6.3 Der Fundamentalsatz der Algebra

Konkrete Untersuchungen zur algebraischen Struktur der Körper $\mathbb{R}$ und $\mathbb{C}$ haben in der Vergangenheit entscheidende Anstöße zur Entwicklung der Theorie der Körper und ihrer Erweiterungen gegeben. Wir wollen hier zunächst auf den *Fundamentalsatz der Algebra* eingehen, dessen Herleitung mit Methoden der Algebra auf Euler und Lagrange zurückgeht. Alternativ lässt sich dieser Satz beispielsweise auch mit Mitteln der komplexen Funktionentheorie beweisen.

Theorem 1. *Der Körper $\mathbb{C}$ der komplexen Zahlen ist algebraisch abgeschlossen.*

Zum *Beweis* müssen wir uns auf gewisse Eigenschaften des Körpers $\mathbb{R}$ der reellen Zahlen stützen, und zwar werden wir benutzen:

Jedes Polynom $f \in \mathbb{R}[X]$ ungeraden Grades hat mindestens eine Nullstelle in $\mathbb{R}$.

Jedes $a \in \mathbb{R}$, $a \geq 0$, hat eine Quadratwurzel in $\mathbb{R}$.

Letztere Eigenschaft hat zur Folge, wie wir zeigen wollen, dass jedes Polynom 2. Grades aus $\mathbb{C}[X]$ eine Nullstelle in $\mathbb{C}$ hat. Es genügt hierzu zu zeigen, dass jedes $z \in \mathbb{C}$ eine Quadratwurzel in $\mathbb{C}$ besitzt. Sei also $z = x + iy \in \mathbb{C}$ mit $x, y \in \mathbb{R}$. Um z in der Form

$$z = x + iy = (a + ib)^2 = a^2 - b^2 + 2iab$$

mit $a, b \in \mathbb{R}$ schreiben zu können, sind die Gleichungen

$$x = a^2 - b^2, \qquad y = 2ab,$$

in a, b zu lösen. Diese Gleichungen sind, abgesehen von der Wahl des Vorzeichens von a und b, äquivalent zu

$$a^2 = \frac{1}{2}x \pm \frac{1}{2}\sqrt{x^2 + y^2}, \qquad b^2 = -\frac{1}{2}x \pm \frac{1}{2}\sqrt{x^2 + y^2},$$

wobei $\pm$ bedeutet, dass man für beide Gleichungen einheitlich entweder das Plus- oder das Minuszeichen auswählt. Allerdings ist das Minuszeichen entbehrlich, da a^2 und b^2 keine negativen Werte annehmen können. Benutzen wir daher, dass nicht-negative reelle Zahlen jeweils eine Quadratwurzel in $\mathbb{R}$ besitzen, so folgt die Existenz der gewünschten Lösungen a und b.

Zum Nachweis der algebraischen Abgeschlossenheit von $\mathbb{C}$ betrachte man eine Körperkette $\mathbb{R} \subset \mathbb{C} \subset L$, wobei $L/\mathbb{C}$ endlich sei. Zu zeigen ist $L = \mathbb{C}$. Indem wir L vergrößern, dürfen wir ohne Beschränkung der Allgemeinheit annehmen, dass $L/\mathbb{R}$ eine Galois-Erweiterung ist. Sei $G = \mathrm{Gal}(L/\mathbb{R})$ die zugehörige Galois-Gruppe, und gelte

$$\big[L : \mathbb{R}\big] = \operatorname{ord} G = 2^k m \quad \text{mit} \quad 2 \nmid m.$$

Es folgt $k \geq 1$, und G enthält aufgrund von 5.2/6 eine 2-Sylow-Gruppe H, also eine Untergruppe der Ordnung 2^k. Für den Fixkörper L^H unter der Aktion von H auf L hat man dann aufgrund des Hauptsatzes der Galois-Theorie 4.1/6

$$\big[L : L^H\big] = 2^k \quad \text{bzw.} \quad \big[L^H : \mathbb{R}\big] = m.$$

Da aber jedes reelle Polynom ungeraden Grades eine Nullstelle in $\mathbb{R}$ hat, ergibt sich beispielsweise unter Benutzung des Satzes vom primitiven Element 3.6/12 notwendig $m = 1$. Damit ist L vom Grad 2^k über $\mathbb{R}$, also vom Grad 2^{k-1} über $\mathbb{C}$; außerdem ist $L/\mathbb{C}$ eine Galois-Erweiterung. Indem wir nun 5.2/4 anwenden, erhalten wir im Falle $L \neq \mathbb{C}$ bzw. $k \geq 2$ eine Untergruppe $H' \subset G' = \mathrm{Gal}(L/\mathbb{C})$ der Ordnung 2^{k-2}. Für den Fixkörper $L^{H'}$ gilt dann $[L : L^{H'}] = 2^{k-2}$ und somit $[L^{H'} : \mathbb{C}] = 2$, was aber nicht sein kann, da jedes komplexe Polynom 2. Grades eine Nullstelle in $\mathbb{C}$ besitzt. Folglich muss $L = \mathbb{C}$ gelten, und $\mathbb{C}$ ist algebraisch abgeschlossen. □

Der gerade vorgeführte Beweis des Fundamentalsatzes der Algebra benutzt die Theorie der Sylow-Gruppen. Im Unterschied hierzu wird in Aufgabe 2 ein direkter Beweis vorgeschlagen, der ohne diese Theorie auskommt. Des Weiteren sei hier noch erwähnt, dass der Körper $\mathbb{R}$ der reellen Zahlen als Teilkörper von $\mathbb{C}$ aus rein algebraischer Sicht keineswegs eindeutig bestimmt ist, da es Automorphismen von $\mathbb{C}$ gibt, die $\mathbb{R}$ nicht wieder in sich selbst abbilden, vgl. etwa Aufgabe 2 aus Abschnitt 7.1. Dass aber $\mathbb{C}$ als algebraischer Abschluss von $\mathbb{R}$ den Grad 2 über $\mathbb{R}$ besitzt, hat tiefere Gründe, wie folgendes auf E. Artin zurückgehende Resultat zeigt.

Satz 2. *Es sei K ein Körper, $\overline{K}$ ein algebraischer Abschluss von K sowie $i \in \overline{K}$ ein Element mit $i^2 = -1$. Aus $[\overline{K} : K] < \infty$ folgt dann $\overline{K} = K(i)$. Ist zusätzlich $\overline{K}/K$ eine echte Erweiterung, so gilt außerdem* $\operatorname{char} K = 0$.

Beweis. Der Grad $[\overline{K} : K]$ sei endlich. Aufgrund der algebraischen Abgeschlossenheit von $\overline{K}$ ist die Erweiterung $\overline{K}/K$ normal, und wir behaupten, dass $\overline{K}/K$ sogar galoissch ist. Setzen wir etwa $\operatorname{char} K = p > 0$ voraus, so gibt es nach 3.7/4 einen Zwischenkörper L zu $\overline{K}/K$, so dass $\overline{K}/L$ rein inseparabel und L/K separabel ist. Man betrachte dann den Frobenius-Homomorphismus $\sigma\colon \overline{K} \longrightarrow \overline{K}$, $x \longmapsto x^p$, wobei σ aufgrund der algebraischen Abgeschlossenheit von $\overline{K}$ ein Automorphismus ist. Da $\sigma(L) \subset L$ gilt und der Grad

$$\big[\overline{K} : L\big] = \big[\sigma(\overline{K}) : \sigma(L)\big] = \big[\overline{K} : \sigma(L)\big]$$

endlich ist, ergibt sich $\sigma(L) = L$. Dies bedeutet aber, dass L keine echte rein inseparable Erweiterung gestattet, d. h. man hat $L = \overline{K}$, und $\overline{K}/K$ ist galoissch.

Dann ist auch $\overline{K}/K(i)$ eine endliche Galois-Erweiterung, und wir haben zu zeigen, dass diese Erweiterung trivial ist. Angenommen, Letzteres ist nicht der Fall, so gibt es eine Untergruppe in $\operatorname{Gal}(\overline{K}/K(i))$, deren Ordnung prim ist; man benutze etwa 5.2/8 bzw. 5.2/11. Für den zugehörigen Fixkörper $L \subset \overline{K}$ ist dann der Grad $[\overline{K} : L]$ ebenfalls prim, etwa $[\overline{K} : L] = \ell$, und es ist $\overline{K}/L$ eine zyklische Galois-Erweiterung vom Grad ℓ. Wir wollen zunächst $p = \operatorname{char} K > 0$ annehmen und den Fall $\ell = p$ behandeln. Nach 4.8/5 (i) gilt dann $\overline{K} = L(a)$ mit einem Element $a \in \overline{K}$, dessen Minimalpolynom über L vom Typ $X^p - X - c$ ist. Um einen Widerspruch zu erhalten, betrachten wir die Abbildung $\tau\colon \overline{K} \longrightarrow \overline{K}$, $x \longmapsto x^p - x$. Diese ist surjektiv, da $\overline{K}$ algebraisch

abgeschlossen ist. Wegen $\mathrm{Sp}_{\overline{K}/L}(x^p) = (\mathrm{Sp}_{\overline{K}/L}(x))^p$, man verwende etwa 4.7/4, ergibt sich die Beziehung

$$\mathrm{Sp}_{\overline{K}/L} \circ \tau = \tau|_L \circ \mathrm{Sp}_{\overline{K}/L} .$$

Da außer τ auch $\mathrm{Sp}_{\overline{K}/L}$ surjektiv ist, vgl. 4.7/7, sieht man, dass auch $\tau|_L$ surjektiv sein muss. Dann besitzt aber $X^p - X - c$ eine Nullstelle in L, im Widerspruch dazu, dass dieses Polynom das Minimalpolynom von a über L ist.

Der prime Grad $\ell = [\overline{K} : L]$ sei nun von der Charakteristik von K verschieden. Wählt man eine primitive ℓ-te Einheitswurzel ζ_ℓ in $\overline{K}$, so hat diese nach 4.5/7 einen Grad $< \ell$ über L. Mit Hilfe des Gradsatzes 3.2/2 folgt dann aber bereits $\zeta_\ell \in L$, und wir können 4.8/3 (i) anwenden. Es gilt also $\overline{K} = L(a)$ für ein Element $a \in \overline{K}$, dessen Minimalpolynom über L vom Typ $X^\ell - c$ ist. Es sei nun $\alpha \in \overline{K}$ eine ℓ-te Wurzel zu a, d. h. es gelte $\alpha^\ell = a$. Dann folgt aufgrund der Multiplikativität der Norm von $\overline{K}$ über L sowie unter Benutzung von 4.7/2 (ii)

$$\mathrm{N}_{\overline{K}/L}(\alpha)^\ell = \mathrm{N}_{\overline{K}/L}(\alpha^\ell) = \mathrm{N}_{\overline{K}/L}(a) = (-1)^{\ell+1} c.$$

Für ungerades ℓ ist daher $\mathrm{N}_{\overline{K}/L}(\alpha) \in L$ eine ℓ-te Wurzel zu c, was aber der Irreduzibilität des Polynoms $X^\ell - c \in L[X]$ widerspricht. Im Falle $\ell = 2$ schließlich ist $\mathrm{N}_{\overline{K}/L}(\alpha) \in L$ eine Quadratwurzel zu $-c$. Dann gibt es aber wegen $i \in L$ auch zu c eine Quadratwurzel in L, was in gleicher Weise der Irreduzibilität des Polynoms $X^2 - c \in L[X]$ widerspricht. Wir haben also insgesamt einen Widerspruch erhalten und somit $\overline{K} = K(i)$ bewiesen.

Es gelte nun $K \subsetneq K(i) = \overline{K}$; insbesondere ist also -1 kein Quadrat in K. Zum Nachweis von $\mathrm{char}\, K = 0$ zeigen wir, dass die Summe zweier Quadrate in K wieder ein Quadrat in K ergibt. Seien also $a, b \in K$. Dann besitzt $a+ib$ eine Quadratwurzel in $K(i)$, etwa $x + iy$, und es gilt $x^2 - y^2 + 2ixy = a + ib$. Dies ergibt $a = x^2 - y^2$, $b = 2xy$ und somit

$$a^2 + b^2 = (x^2 - y^2)^2 + 4x^2y^2 = (x^2 + y^2)^2.$$

Per Induktion sieht man dann, dass die Summe endlich vieler Quadrate aus K wieder ein Quadrat in K ist. Da aber in einem Körper positiver Charakteristik das Element -1 als mehrfache Summe des Einselementes $1 = 1^2$ darstellbar ist, -1 in unserem Falle aber kein Quadrat in K ist, gilt notwendig $\mathrm{char}\, K = 0$. □

Lernkontrolle und Prüfungsvorbereitung

1. Auf welche Eigenschaften des Körpers $\mathbb{R}$ der reellen Zahlen greift man zurück, wenn man den Fundamentalsatz der Algebra mit Mitteln der Algebra beweisen möchte? Begründe diese Eigenschaften aus Sicht der Analysis.

2. Welche algebraischen Konsequenzen haben die unter Punkt 1 angesprochenen Eigenschaften von $\mathbb{R}$? Setze diese zusammen, um einen Beweis des Fundamentalsatzes der Algebra zu gewinnen.

3. Es sei K ein Körper und $\overline{K}$ ein algebraischer Abschluss von K, wobei $\overline{K} = K(i)$ mit einer Quadratwurzel i zu -1 gelte. Zeige, dass die Summe zweier Quadrate in K wieder ein Quadrat in K ergibt.

+4. Stelle die Tatsache, dass die Erweiterung $\mathbb{C}/\mathbb{R}$ vom Grad 2 ist, in einen allgemeinen Zusammenhang. Genauer, sei K ein Körper und $\overline{K}$ ein algebraischer Abschluss von K, so dass die Erweiterung $\overline{K}/K$ endlich ist. Zeige $\overline{K} = K$ für $\operatorname{char} K > 0$ sowie $\overline{K} = K(i)$ in Charakteristik 0, wobei i eine Quadratwurzel von -1 sei.

Übungsaufgaben

1. *Welche Argumentation verwendet man beim Beweis der in Theorem* 1 *benutzten Eigenschaften der reellen Zahlen, dass nämlich jedes reelle Polynom ungeraden Grades eine Nullstelle in* $\mathbb{R}$ *hat und dass jedes* $a \in \mathbb{R}$, $a \geq 0$, *eine Quadratwurzel in* $\mathbb{R}$ *besitzt*?

2. Es sei $f \in \mathbb{R}[X]$ ein nicht-konstantes Polynom vom Grad $n = 2^k m$ mit $2 \nmid m$. Beweise mittels Induktion nach k, dass f eine Nullstelle in $\mathbb{C}$ besitzt, und folgere hieraus den Fundamentalsatz der Algebra. (*Hinweis*: Zerlege das Polynom f, welches als normiert angenommen werde, über einem algebraischen Abschluss $\overline{\mathbb{R}}$ von $\mathbb{R}$ in Linearfaktoren, etwa $f = \prod_{\nu=1}^{n}(X - \alpha_\nu)$, setze $\alpha_{\mu\nu} = \alpha_\mu + \alpha_\nu + b\alpha_\mu\alpha_\nu$ für beliebiges $b \in \mathbb{R}$ an und verwende die Induktionsvoraussetzung für das Polynom $g = \prod_{\mu<\nu}(X - \alpha_{\mu\nu})$. Die in Aufgabe 1 spezifizierten Eigenschaften von $\mathbb{R}$ dürfen dabei benutzt werden.)

3. Es sei K ein Körper und $X^n - c \in K[X]$ ein Polynom vom Grad $n \geq 2$ mit $c \neq 0$. Zeige in Verallgemeinerung der im Beweis zu Satz 2 benutzten Methoden, dass $X^n - c$ genau dann irreduzibel ist, wenn c für keinen Primteiler p von n eine p-te Potenz in K ist und wenn zusätzlich im Falle $4 \mid n$ das Element c nicht von der Form $c = -4a^4$ mit $a \in K$ ist. (*Hinweis*: Studiere zunächst den Fall, dass n eine Primpotenz ist.)

6.4 Konstruktionen mit Zirkel und Lineal

In diesem Abschnitt werden wir die Galois-Theorie auf geometrische Konstruktionsprobleme in der komplexen Zahlenebene $\mathbb{C}$ anwenden. Wir gehen von einer Teilmenge $M \subset \mathbb{C}$ aus (später setzt man meist $M = \{0, 1\}$) und sagen, ein Punkt $z \in \mathbb{C}$ *lasse sich mit Zirkel und Lineal aus M konstruieren*, wenn M sich durch endlich viele *elementare Konstruktionsschritte* zu einer Teilmenge $M' \subset \mathbb{C}$ mit $z \in M'$ vergrößern lässt. Dabei lassen wir folgende drei Typen von elementaren Konstruktionsschritten zu:

(1) *Man betrachte zwei nicht-parallele Geraden g_1 und g_2 in $\mathbb{C}$, welche jeweils durch Punkte $z_1, z_2 \in M$ bzw. $z_3, z_4 \in M$ festgelegt sind, und füge zu M den Schnittpunkt von g_1 mit g_2 hinzu.*

(2) *Man betrachte eine Kreislinie K in $\mathbb{C}$ um einen Punkt $z_1 \in M$ mit einem Radius, der durch den Abstand $|z_3 - z_2|$ zweier Punkte $z_2, z_3 \in M$ gegeben wird, sowie eine Gerade g, die durch zwei Punkte z_4, $z_5 \in M$ definiert wird, und füge zu M alle Schnittpunkte von K mit g hinzu.*

(3) *Man betrachte zwei nicht-identische Kreislinien K_1 und K_2 in $\mathbb{C}$ mit Mittelpunkten $z_1, z_2 \in M$ sowie Radien $|z_4 - z_3|$ bzw. $|z_6 - z_5|$, die durch Abstände zwischen Punkten $z_3, z_4, z_5, z_6 \in M$ gegeben werden. Man füge die Schnittpunkte von K_1 mit K_2 zu M hinzu.*

Wir bezeichnen mit $\mathfrak{K}(M)$ die Menge aller mit Zirkel und Lineal aus M konstruierbaren Punkte in $\mathbb{C}$, wobei wir stets $0, 1 \in M$ voraussetzen wollen. Ist dann $\overline{M}$ das Bild von M unter der komplexen Konjugation[2] $\mathbb{C} \longrightarrow \mathbb{C}$, $z \longmapsto \overline{z}$, so gilt offenbar $\mathfrak{K}(M) = \mathfrak{K}(M \cup \overline{M})$, da man zu jedem $z \in M - \mathbb{R}$ den konjugierten Punkt $\overline{z}$ durch Spiegeln an der reellen Achse mit Zirkel und Lineal aus M konstruieren kann. Für z rein imaginär, also mit Realteil $\operatorname{Re} z = 0$, ergibt sich $\overline{z}$ als Schnittpunkt der Geraden durch 0 und z mit dem Kreis um 0 mit Radius $|z| = |z - 0|$. Ansonsten betrachtet man den Kreis um z mit Radius $|z|$. Dieser hat zwei Schnittpunkte z_1, z_2 mit der Geraden durch 0 und 1, und man erhält $\overline{z}$ als Schnittpunkt der Kreise um z_1 und z_2, ebenfalls mit Radius $|z|$.

Um die Menge $\mathfrak{K}(M)$ mittels algebraischer Körpererweiterungen zu charakterisieren, gehen wir von dem kleinsten Teilkörper in $\mathbb{C}$ aus, der M

[2] Wir verwenden in diesem Abschnitt die Notation $\overline{M}$ für das Bild von M unter der Konjugationsabbildung, auch wenn M ein Körper ist; ein algebraischer Abschluss eines solchen Körpers $M \subset \mathbb{C}$, üblicherweise mit $\overline{M}$ bezeichnet, wird nicht benötigt.

und $\overline{M}$ enthält. Dies ist der Körper $\mathbb{Q}(M \cup \overline{M})$, der aus $\mathbb{Q}$ durch Adjunktion von $M \cup \overline{M}$ entsteht.

Satz 1. *Sei $M \subset \mathbb{C}$ mit $0, 1 \in M$, und sei $z \in \mathbb{C}$. Dann ist äquivalent*:

(i) $z \in \mathfrak{K}(M)$.

(ii) *Es gibt eine Körperkette $\mathbb{Q}(M \cup \overline{M}) = L_0 \subset L_1 \subset \ldots \subset L_n \subset \mathbb{C}$ mit $z \in L_n$ und $[L_i : L_{i-1}] = 2$ für $i = 1, \ldots, n$.*

(iii) *z ist enthalten in einer Galois-Erweiterung L von $\mathbb{Q}(M \cup \overline{M})$, deren Grad $[L : \mathbb{Q}(M \cup \overline{M})]$ eine Potenz von 2 ist.*

Als direkte Folgerung ergibt sich hieraus:

Korollar 2. *Sei $M \subset \mathbb{C}$ mit $0, 1 \in M$. Es ist $\mathfrak{K}(M)$ ein algebraischer Erweiterungskörper von $\mathbb{Q}(M \cup \overline{M})$. Der Grad jedes Elementes $z \in \mathfrak{K}(M)$ über $\mathbb{Q}(M \cup \overline{M})$ ist eine Potenz von 2.*

Beweis von Satz 1. Wir beginnen mit der Implikation von (i) nach (ii) und zeigen zunächst, dass wir M als Körper mit $M = \overline{M}$ und $i \in M$ annehmen können, für die komplexe Zahl $i \in \mathbb{C}$. Die komplexe Konjugation beschränkt sich nämlich zu einem Automorphismus des Körpers $L_0 = \mathbb{Q}(M \cup \overline{M})$, so dass $L_0 = \overline{L}_0$ gilt. Dann ist $L_1 = L_0(i)$ ein Erweiterungskörper von L_0 vom Grade ≤ 2 mit $L_1 = \overline{L}_1$ und $i \in L_1$. Weiter gilt $\mathfrak{K}(M) \subset \mathfrak{K}(L_1)$ und $\mathbb{Q}(L_1 \cup \overline{L}_1) = L_1$, und es genügt, die Implikation von (i) nach (ii) für L_1 anstelle von M nachzuweisen. Mit anderen Worten, wir dürfen M als Körper mit $M = \overline{M}$ und $i \in M$ annehmen.

Aus dieser Voraussetzung ergibt sich, dass für einen Punkt $z \in M$ auch sein Realteil $\operatorname{Re} z = \frac{1}{2}(z + \overline{z})$, sein Imaginärteil $\operatorname{Im} z = \frac{1}{2i}(z - \overline{z})$ sowie das Quadrat $|z|^2 = z\overline{z}$ seines Betrages zu M gehören. Sei nun $z \in \mathfrak{K}(M)$. Es reicht, den Fall zu betrachten, wo sich z durch einen einzigen elementaren Konstruktionsschritt aus M gewinnen lässt, und zu zeigen, dass z in M oder in einem Erweiterungskörper $L = M(\sqrt{\Delta})$ enthalten ist, der aus M durch Adjunktion einer Quadratwurzel aus einer nicht-negativen Zahl $\Delta \in M \cap \mathbb{R}$ gewonnen wird. Wegen $L = \overline{L}$ und $i \in L$, erhält man hieraus mit Induktion den Allgemeinfall.

Wir betrachten zunächst einen Konstruktionsschritt des Typs (1). Dann ergibt sich z als Schnittpunkt zweier Geraden

$$g_1 = \{z_1 + t(z_2 - z_1)\,;\, t \in \mathbb{R}\},$$
$$g_2 = \{z_3 + t'(z_4 - z_3)\,;\, t' \in \mathbb{R}\},$$

mit $z_1, z_2, z_3, z_4 \in M$, d. h. wir haben die Gleichung

$$z_1 + t(z_2 - z_1) = z_3 + t'(z_4 - z_3)$$

nach den Parametern $t, t' \in \mathbb{R}$ aufzulösen. Eine Aufspaltung dieser Gleichung in Real- und Imaginärteil ergibt ein System von zwei linearen Gleichungen in den Unbekannten t, t' mit Koeffizienten in $\mathbb{R} \cap M$, welches genau eine Lösung $(t_0, t_0') \in \mathbb{R}^2$ besitzt. Da sich die Lösung (t_0, t_0') beispielsweise mit der Cramerschen Regel aus den Koeffizienten des Gleichungssystems berechnen lässt, erhält man $t_0, t_0' \in \mathbb{R} \cap M$ und daher

$$z = z_1 + t_0(z_2 - z_1) = z_3 + t_0'(z_4 - z_3) \in M,$$

so dass in diesem Falle keine Erweiterung von M notwendig ist.

Als Nächstes nehmen wir an, dass z aus M durch einen Konstruktionsschritt des Typs (2) gewonnen wird. Es ist z also Schnittpunkt einer Kreislinie

$$K = \{\zeta \in \mathbb{C}\,;\, |\zeta - z_1|^2 = |z_3 - z_2|^2\}$$

mit einer Geraden

$$g = \{z_4 + t(z_5 - z_4)\,;\, t \in \mathbb{R}\},$$

wobei $z_1, \ldots, z_5 \in M$. Um sämtliche Schnittpunkte von K mit g zu berechnen, ist die Gleichung

$$|z_4 + t(z_5 - z_4) - z_1|^2 = |z_3 - z_2|^2$$

nach t aufzulösen. Hierbei handelt es sich um eine quadratische Gleichung in t, und zwar mit Koeffizienten, die sich aus den Real- und Imaginärteilen von $z_1, \ldots, z_5$ mit rationalen Operationen berechnen lassen, also zu $\mathbb{R} \cap M$ gehören. Die Gleichung lässt sich dann in der Form $t^2 + at + b = 0$ mit Koeffizienten $a, b \in M \cap \mathbb{R}$ schreiben, wobei der betrachtete Schnittpunkt $z \in K \cap g$ zu einer reellen Lösung t_0 von $t^2 + at + b = 0$ korrespondiert. Für die Diskriminante $\Delta = a^2 - 4b$ der Gleichung gilt dann $\Delta \geq 0$, und es folgt $t_0 \in (M \cap \mathbb{R})(\sqrt{\Delta})$ sowie $z = z_4 + t_0(z_5 - z_4) \in L$, wenn wir $L = M(\sqrt{\Delta})$ setzen.

Es bleibt noch ein Konstruktionsschritt des Typs (3) zu betrachten. Sei z also Schnittpunkt zweier nicht-identischer Kreise

$$K_1 = \{\zeta \in \mathbb{C}\,;\, |\zeta - z_1|^2 = r_1^2\},$$
$$K_2 = \{\zeta \in \mathbb{C}\,;\, |\zeta - z_2|^2 = r_2^2\},$$

wobei $r_1 = |z_4 - z_3|$, $r_2 = |z_6 - z_5|$, $z_1, \ldots, z_6 \in M$. Dann genügt z den Gleichungen

$$z\overline{z} - z\overline{z}_1 - \overline{z}z_1 + z_1\overline{z}_1 = r_1^2,$$
$$z\overline{z} - z\overline{z}_2 - \overline{z}z_2 + z_2\overline{z}_2 = r_2^2,$$

bzw., wenn man subtrahiert, einer Gleichung des Typs

$$az + \overline{az} + b = 0 \quad \text{bzw.} \quad 2\mathrm{Re}(az) + b = 0$$

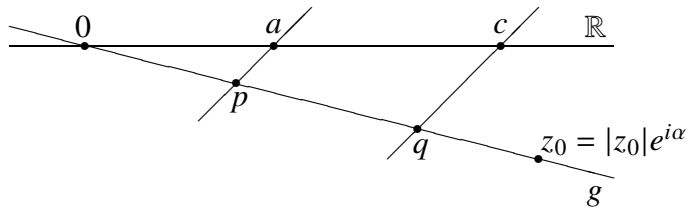
mit $a = \overline{z}_2 - \overline{z}_1 \in M$ und $b \in M \cap \mathbb{R}$. Da die Mittelpunkte von K_1 und K_2 verschieden sein müssen, gilt $a \neq 0$, und es handelt sich bei der letzten Gleichung um eine Geradengleichung für z. Die zugehörige Gerade g enthält die Punkte $\frac{-b}{2a}, \frac{-b+i}{2a} \in M$, und die Schnittpunkte von g mit K_1 bzw. K_2 stimmen überein mit denjenigen von K_1 und K_2. Indem wir also g mit K_1 oder K_2 schneiden, können wir wie bei einem Konstruktionsschritt des Typs (2) weiterschließen. Der Beweis der Implikation (i) $\Longrightarrow$ (ii) ist damit abgeschlossen.

Für die umgekehrte Implikation (ii) $\Longrightarrow$ (i) genügt es zu zeigen, dass $\mathfrak{K}(M)$ (unter der Voraussetzung $0, 1 \in M$) ein Teilkörper von $\mathbb{C}$ ist, der $M \cup \overline{M}$ und damit $\mathbb{Q}(M \cup \overline{M})$ enthält und für den mit z auch jede der beiden Quadratwurzeln $\pm\sqrt{z}$ zu $\mathfrak{K}(M)$ gehört. Um dies einzusehen, erinnern wir an die Beziehung $\mathfrak{K}(M) = \mathfrak{K}(M \cup \overline{M})$ und zeigen nachfolgende Aussagen, von denen wir einige nur aus beweistechnischen Gründen aufgelistet haben:

(a) $z_1, z_2 \in \mathfrak{K}(M) \Longrightarrow z_1 + z_2 \in \mathfrak{K}(M)$
(b) $z \in \mathfrak{K}(M) \Longrightarrow -z \in \mathfrak{K}(M)$
(c) $z \in \mathfrak{K}(M) \Longrightarrow |z| \in \mathfrak{K}(M)$
(d) $e^{\pi i/3} = \frac{1}{2} + \frac{1}{2} \cdot i\sqrt{3} \in \mathfrak{K}(M)$
(e) $z_1, z_2 \in \mathfrak{K}(M) \Longrightarrow |z_1||z_2| \in \mathfrak{K}(M)$
(f) $z \in \mathfrak{K}(M), z \neq 0 \Longrightarrow |z|^{-1} \in \mathfrak{K}(M)$

(g) $z_1, z_2 \in \mathfrak{K}(M) \Longrightarrow z_1 z_2 \in \mathfrak{K}(M)$
(h) $z \in \mathfrak{K}(M), z \neq 0 \Longrightarrow z^{-1} \in \mathfrak{K}(M)$
(i) $z \in \mathfrak{K}(M) \Longrightarrow \pm\sqrt{z} \in \mathfrak{K}(M)$

Jede der vorstehenden Implikationen kann man mit Hilfe einfacher geometrischer Konstruktionen verifizieren. Für (a) verwende man die Interpretation der Addition komplexer Zahlen als Vektoraddition. Der "Vektor" $z_1 + z_2$ korrespondiert zu der Diagonalen des von den "Vektoren" z_1, z_2 aufgespannten Parallelogramms. Für (b) spiegele man z am Nullpunkt, es liegt $-z$ auf der Geraden durch 0 und z (man nehme $z \neq 0$ an) sowie auf der Kreislinie um 0 mit Radius $|z| = |z - 0|$. In (c) interpretiere man entsprechend $|z|$ als Schnittpunkt der reellen Achse mit der Kreislinie um 0 mit Radius $|z|$. Eigenschaft (d) benötigen wir zum Nachweis von (e) und (f), um zu sehen, dass $\mathfrak{K}(M)$ außer den Punkten $0, 1$ noch einen weiteren, nicht-reellen Punkt enthält; man errichte über der Strecke von 0 nach 1 ein gleichseitiges Dreieck der Seitenlänge 1. Die Spitze, als Schnittpunkt der Kreise um 0 bzw. 1 mit Radius 1, ist dann die primitive sechste Einheitswurzel $e^{\pi i/3} = \frac{1}{2} + \frac{1}{2} \cdot i\sqrt{3}$. In der Situation (e) und (f) schließlich nehme man $z_1 \neq 0 \neq z_2$ an und betrachte folgende Figur:



Um diese zu erhalten, wähle man einen Punkt $z_0 = |z_0|e^{i\alpha}$ in $M - \mathbb{R}$ mit $\operatorname{Re} z_0 > 0$, z. B. $z_0 = e^{\pi i/3}$, und betrachte die Gerade g durch 0 und z_0. Auf g kann man dann die Punkte $p = e^{i\alpha}$ und $q = |z_2|e^{i\alpha}$ betrachten, sowie auf der reellen Achse den Punkt $a = |z_1|$. Alle diese Punkte gehören zu $\mathfrak{K}(M)$, wie man leicht verifiziert. Auf der reellen Achse betrachte man noch den Punkt c, den man als Schnittpunkt von $\mathbb{R}$ mit der Parallelen zu $g_{a,p}$ durch q gewinnt; dabei sei $g_{a,p}$ die durch a und p festgelegte Gerade. Auch c gehört zu $\mathfrak{K}(M)$, wie man anhand elementarer Konstruktionen sofort nachprüft; man fälle etwa von q aus das Lot auf die Gerade $g_{a,p}$ und errichte auf diesem Lot die Senkrechte in q. Dann gilt nach dem Strahlensatz

$$|q| \cdot |p|^{-1} = |c| \cdot |a|^{-1},$$

also wegen $|q| = |z_2|$, $|p| = 1$ und $|a| = |z_1|$

$$|c| = |a| \cdot |q| = |z_1| \cdot |z_2|$$

und somit $|z_1| \cdot |z_2| \in \mathfrak{K}(M)$. Indem man die Parallele zu $g_{a,p}$ durch $1 \in \mathbb{R}$ konstruiert, erhält man als Schnittpunkt mit g eine komplexe Zahl vom Betrag $|z_1|^{-1}$, wobei $|z_1|^{-1} \in \mathfrak{K}(M)$ gemäß (c). Da sich bei der Multiplikation komplexer Zahlen die Beträge multiplizieren und die Argumente addieren, hat man zum Nachweis von (g) bzw. (h) lediglich noch die Winkeladdition bzw. -negation elementargeometrisch durchzuführen, was aber ohne Probleme möglich ist. Da auch die Winkelhalbierung elementargeometrisch durchführbar ist, bleibt für (i) nur noch zu zeigen, dass für $z \in \mathfrak{K}(M) - \{0\}$ auch $\sqrt{|z|}$ konstruierbar ist. Hierzu betrachte man auf der reellen Achse die Strecke von $-|z|$ bis 1 und errichte hierüber den Halbkreis des Thales. Diesen schneide man mit der Senkrechten auf der reellen Achse, die man in 0 errichtet. Als Schnittpunkt ergibt sich nach dem Höhensatz für rechtwinklige Dreiecke eine komplexe Zahl vom Betrag $\sqrt{|z|}$. Damit ist gezeigt, dass $\mathfrak{K}(M)$ ein Teilkörper von $\mathbb{C}$ ist und dass $\mathfrak{K}(M)$ abgeschlossen ist unter der Bildung von Quadratwurzeln. Die Äquivalenz der Bedingungen (i) und (ii) ist also bewiesen.

Es bleibt noch die Äquivalenz zwischen (ii) und (iii) zu begründen; sei zunächst Bedingung (ii) gegeben. Zu L_n als Körpererweiterung von $K = \mathbb{Q}(M \cup \overline{M})$ lässt sich die normale Hülle L in $\mathbb{C}$ bilden; vgl. 3.5/7. Sind $\sigma_1, \ldots, \sigma_r$ die verschiedenen K-Homomorphismen von L_n nach $\mathbb{C}$, so ist L derjenige Körper, der über K von allen $\sigma_i(L_n)$, $i = 1, \ldots, r$, erzeugt wird. Da L_n aus K durch sukzessive Adjunktion von Quadratwurzeln entsteht, gilt dasselbe für jedes $\sigma_i(L_n)$ und daher auch für L. Somit ist L/K eine Galois-Erweiterung, deren Grad eine Potenz von 2 ist. Wegen $z \in L_n \subset L$ ist Bedingung (iii) erfüllt.

Ist umgekehrt Bedingung (iii) gegeben, so ist die Galois-Gruppe $\mathrm{Gal}(L/K)$ eine 2-Gruppe und daher nach 5.4/6 auflösbar. Folglich besitzt $\mathrm{Gal}(L/K)$ eine Normalreihe, deren Faktoren zyklisch von der Ordnung 2 sind, vgl. 5.4/7. Zu einer solchen Kette korrespondiert dann aber aufgrund des Hauptsatzes der Galois-Theorie 4.1/6 eine Körperkette wie in Bedingung (ii) gefordert. □

Die Aussage des gerade bewiesenen Satzes ist oft nützlich, um zu zeigen, dass gewisse Größen bzw. Punkte der komplexen Zahlenebene nicht durch

Konstruktion mit Zirkel und Lineal aus einer gegebenen Menge $M \subset \mathbb{C}$ erhalten werden können. Ein berühmtes Beispiel hierzu ist das Problem der *Quadratur des Kreises*, welches darin besteht, einen Kreis, gegeben durch Mittelpunkt und Radius, durch Konstruktion mit Zirkel und Lineal in ein flächengleiches Quadrat zu verwandeln. Man betrachte etwa den Kreis mit Radius 1 um 0. Sein Flächeninhalt wird durch die Zahl π gegeben. Ein flächengleiches Quadrat hat somit die Kantenlänge $\sqrt{\pi}$. Das Problem der Quadratur des Kreises besteht also darin, zu entscheiden, ob $\sqrt{\pi}$ zu $\mathfrak{K}(\{0,1\})$ gehört oder nicht. Gemäß Korollar 2 bildet $\mathfrak{K}(\{0,1\})$ einen algebraischen Erweiterungskörper von $\mathbb{Q}$. Man weiß aber, wie F. Lindemann bereits 1882 in [12] gezeigt hat, dass die Zahlen π bzw. $\sqrt{\pi}$ transzendent über $\mathbb{Q}$ sind. Es ist also $\sqrt{\pi}$ nicht mit Zirkel und Lineal aus $\{0,1\}$ konstruierbar und somit die Quadratur des Kreises nicht lösbar. In der Vergangenheit sind durch Konstruktion mit Zirkel und Lineal oftmals sehr gute Näherungslösungen für π bzw. $\sqrt{\pi}$ gefunden worden, die dann in Unkenntnis der Sachlage verschiedentlich als Lösung des Problems der Quadratur des Kreises angesehen wurden.

Ein weiteres klassisches Problem, dessen Unlösbarkeit sich herausstellt, ist das Problem der *Würfelverdoppelung*: Kann man das Volumen eines Würfels durch Konstruktion mit Zirkel und Lineal verdoppeln? Man gehe etwa von einem Würfel der Kantenlänge 1 aus. Verdoppelung des Volumens führt zu einem Würfel der Kantenlänge $\sqrt[3]{2}$. Nach Korollar 2 gehört aber $\sqrt[3]{2}$ nicht zu $\mathfrak{K}(\{0,1\})$, da der Grad von $\sqrt[3]{2}$ über $\mathbb{Q}$ keine Potenz von 2 ist. In ähnlicher Weise behandelt man auch das Problem der Winkeldreiteilung; vgl. hierzu Aufgabe 2.

Wir wollen uns schließlich noch mit dem Problem der *Konstruktion regelmäßiger n-Ecke* beschäftigen. Wichtige Lösungsbeiträge hierzu gehen auf C. F. Gauß zurück. Das Problem besteht darin, zu entscheiden, ob für eine gegebene natürliche Zahl $n \geq 3$ die n-te primitive Einheitswurzel $e^{2\pi i/n}$ zu $\mathfrak{K}(\{0,1\})$ gehört oder nicht. Im Beweis zu Satz 1 hatten wir bereits $e^{\pi i/3} \in \mathfrak{K}(\{0,1\})$ gesehen. Das regelmäßige 6-Eck ist deshalb mit Zirkel und Lineal konstruierbar. Allgemeiner gilt:

Satz 3. *Sei $n \geq 3$ eine natürliche Zahl. Das regelmäßige n-Eck ist genau dann mit Zirkel und Lineal konstruierbar, wenn $\varphi(n)$ eine Potenz von 2 ist; dabei ist φ die Eulersche φ-Funktion* (*vgl.* 4.5/3).

Beweis. Es sei ζ_n eine primitive n-te Einheitswurzel über $\mathbb{Q}$. Dann ist $\mathbb{Q}(\zeta_n)/\mathbb{Q}$ nach 4.5/8 eine abelsche Galois-Erweiterung vom Grad $\varphi(n)$. Nehmen wir zunächst an, dass das regelmäßige n-Eck konstruierbar ist, also $\zeta_n \in \mathfrak{K}(\{0,1\})$ gilt, so ist nach Korollar 2 der Grad von ζ_n über $\mathbb{Q}$ und damit $\varphi(n)$ eine Potenz von 2. Weiß man umgekehrt, dass $\varphi(n) = [\mathbb{Q}(\zeta_n) : \mathbb{Q}]$ eine Potenz von 2 ist, ergibt sich $\zeta_n \in \mathfrak{K}(\{0,1\})$, indem man die Implikation von (iii) nach (i) in Satz 1 ausnutzt. □

Unter Benutzung von 4.5/4 (iii) berechnet man leicht folgende Werte der φ-Funktion:

n	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	...
$\varphi(n)$	2	2	4	2	*6*	4	*6*	4	*10*	4	*12*	*6*	8	8	16	...

Kursivdruck in der Zeile für $\varphi(n)$ deutet Nicht-Konstruierbarkeit des regelmäßigen n-Ecks an. Das regelmäßige 7-Eck ist das erste nicht-konstruierbare n-Eck in dieser Liste; der Beweis der Nicht-Konstruierbarkeit geht auf Gauß zurück. Gauß war es auch, der als Erster ein Verfahren für die (recht aufwendige) Konstruktion des regelmäßigen 17-Ecks fand; man beachte, dass $\varphi(17) = 16$ eine Potenz von 2 ist.

Wir wollen abschließend noch auf den Zusammenhang zwischen der Konstruierbarkeit des regelmäßigen n-Ecks und der Zerlegung von n in Fermatsche Primzahlen eingehen.

Definition 4. *Für $\ell \in \mathbb{N}$ heißt $F_\ell = 2^{2^\ell} + 1$ die* ℓ-te Fermatsche Zahl. *Eine* Fermatsche Primzahl *ist eine Primzahl, die zugleich eine Fermatsche Zahl ist, also eine Primzahl der Form $2^{2^\ell} + 1$.*

Es sind $F_0 = 3$, $F_1 = 5$, $F_2 = 17$, $F_3 = 257$, $F_4 = 65537$ Primzahlen, also Fermatsche Primzahlen. Dies sind die einzigen Fermatschen Zahlen, von denen man bisher weiß, dass sie prim sind.

Satz 5. *Sei $n \geq 2$. Dann ist äquivalent*:

(i) *$\varphi(n)$ ist eine Potenz von* 2.

(ii) *Es existieren verschiedene Fermatsche Primzahlen $p_1, \ldots, p_r$ sowie eine natürliche Zahl $m \in \mathbb{N}$ mit $n = 2^m p_1 \ldots p_r$.*

Beweis. Für eine Primzahl p ist $\varphi(p^m) = (p-1)p^{m-1}$ genau dann eine Potenz von 2, wenn $p = 2$ gilt oder wenn $p^{m-1} = 1$, also $m = 1$ gilt und $p - 1$ eine Potenz von 2 ist. Somit folgt die Aussage des Satzes aufgrund der Multiplikativität der φ-Funktion mit folgendem Lemma:

Lemma 6. *Eine Primzahl $p \geq 3$ ist genau dann eine Fermatsche Zahl, wenn $p - 1$ eine Potenz von 2 ist.*

Beweis. Für jede Fermatsche Zahl p ist nach Definition $p - 1$ eine Potenz von 2. Sei umgekehrt $p - 1$ eine Potenz von 2, etwa $p = (2^{2^\ell})^r + 1$ mit ungeradem r. Gilt dann $r > 1$, so können wir p aufgrund der Formel

$$1 + a^r = 1 - (-a)^r = \big(1 - (-a)\big)\big((-a)^{r-1} + (-a)^{r-2} + \ldots + 1\big)$$

echt zerlegen in der Form

$$(2^{2^\ell})^r + 1 = (2^{2^\ell} + 1)\big((2^{2^\ell})^{r-1} - \ldots + 1\big).$$

Da aber p eine Primzahl ist, ergibt sich $r = 1$. □

Zusammenfassend stellt sich heraus, dass das regelmäßige n-Eck genau dann mit Zirkel und Lineal konstruierbar ist, wenn n von der Form $n = 2^m p_1 \ldots p_r$ mit paarweise verschiedenen Fermatschen Primzahlen $p_1, \ldots, p_r$ sowie einer natürlichen Zahl m ist.

Lernkontrolle und Prüfungsvorbereitung

1. Was ist mit "Konstruktion mittels Zirkel und Lineal" gemeint? Erkläre insbesondere die zugelassenen elementaren Konstruktionsschritte.
2. Für eine Menge $M \subset \mathbb{C}$ mit $0, 1 \in M$ bezeichne $\mathfrak{K}(M)$ die Menge der aus M mittels Zirkel und Lineal konstruierbaren Punkte in $\mathbb{C}$. Charakterisiere die Menge $\mathfrak{K}(M)$ mit Methoden der Körper- bzw. Galois-Theorie.
3. Begründe, dass man in der Situation von Punkt 2 die Menge M als Körper annehmen kann, der die komplexe Zahl i als Quadratwurzel von -1 enthält und der invariant unter der komplexen Konjugation ist.
4. Erkläre in der Situation von Punkt 2 die Korrespondenz zwischen den elementaren Konstruktionsschritten und geeigneten Körpererweiterungen vom Grad ≤ 2.

5. Zeige in der Situation von Punkt 2, dass $\mathfrak{K}(M)$ ein Körper ist, der abgeschlossen unter der Adjunktion von Quadratwurzeln zu Elementen aus $\mathfrak{K}(M)$ ist und der invariant unter der komplexen Konjugation ist.
6. Setze die vorhergehenden Punkte zusammen zu einem Beweis zu Punkt 2.
7. Beschreibe die klassischen Probleme der Quadratur des Kreises, der Würfelverdoppelung und der Winkeldreiteilung.
8. Zeige, wie man die Konstruierbarkeit mit Zirkel und Lineal für regelmäßige n-Ecke mittels der Eulerschen φ-Funktion charakterisieren kann. Gib die kleinsten vier Werte für n an, so dass das regelmäßige n-Eck *nicht* mit Zirkel und Lineal konstruierbar ist.
9. Führe die Konstruktion des regelmäßigen 6-Ecks mittels Zirkel und Lineal durch.
10. Was ist eine Fermatsche Zahl, was eine Fermatsche Primzahl? Welche Fermatschen Primzahlen sind bekannt?
11. Welche Rolle spielen die Fermatschen Primzahlen für die Konstruierbarkeit regelmäßiger n-Ecke mittels Zirkel und Lineal?

Übungsaufgaben

1. *Es sei $M \subset \mathbb{C}$ eine Teilmenge mit $0, 1 \in M$. Diskutiere die Frage, ob ein Element $z \in \mathbb{C}$ bereits dann zu $\mathfrak{K}(M)$ gehört, wenn sein Grad über $\mathbb{Q}(M \cup \overline{M})$ eine Potenz von 2 ist. Betrachte insbesondere für $M = \{0, 1\}$ den Fall, wo z vom Grad 4 über $\mathbb{Q}$ ist.*
2. *Überlege, ob das Problem der Winkeldreiteilung mit Zirkel und Lineal lösbar ist.*
3. Betrachte für $M = \{0, 1\}$ die Erweiterung $\mathfrak{K}(M)/\mathbb{Q}$ und zeige:
   (i) $\mathfrak{K}(M)/\mathbb{Q}$ ist eine unendliche Galois-Erweiterung.
   (ii) $\mathfrak{K}(M)$ ist darstellbar als Vereinigung einer aufsteigenden Kette von Galois-Erweiterungen von $\mathbb{Q}$, deren Grad jeweils eine Potenz von 2 ist.
   (iii) Beschreibe die Gruppe $\mathrm{Gal}(\mathfrak{K}(M)/\mathbb{Q})$ unter Verwendung des projektiven Limes, vgl. Abschnitt 4.2.
4. Beschreibe die Konstruktion mit Zirkel und Lineal für das regelmäßige 5-Eck.

7. Transzendente Erweiterungen

Überblick und Hintergrund

Ausgehend von den rationalen Zahlen erkannte man schon frühzeitig, dass gewisse "Zahlen" wie etwa $\sqrt{2}$ nicht rational, also *irrational* sind. Man sprach von den *Irrationalitäten* und versuchte insbesondere, diese zu klassifizieren. Die Galois-Theorie lieferte dann erstmals einen Zugang zu den algebraischen unter den irrationalen Zahlen, also zu denjenigen, die einer nicht-trivialen algebraischen Gleichung mit Koeffizienten aus $\mathbb{Q}$ genügen. Kurze Zeit später konnte man zeigen, dass die algebraischen nur den "kleineren" Teil aller irrationalen Zahlen ausmachen, die "allermeisten" aber keiner nicht-trivialen algebraischen Gleichung mit Koeffizienten aus $\mathbb{Q}$ genügen und somit *transzendent* sind, wie man sagte.

Für eine über $\mathbb{Q}$ transzendente Zahl wie etwa π ist die einfache Körpererweiterung $\mathbb{Q}(\pi)/\mathbb{Q}$ leicht zu beschreiben: Der Monomorphismus $\mathbb{Q}[X] \hookrightarrow \mathbb{Q}(\pi)$, $X \longmapsto \pi$, induziert einen Isomorphismus $\mathbb{Q}(X) \xrightarrow{\sim} \mathbb{Q}(\pi)$, wobei $\mathbb{Q}(X)$ der Funktionenkörper in der Variablen X über $\mathbb{Q}$ ist, also der Quotientenkörper zu $\mathbb{Q}[X]$. Wie kann man aber für kompliziertere Teilkörper $L \subset \mathbb{C}$ oder gar für $L = \mathbb{C}$ die Struktur der Erweiterung $L/\mathbb{Q}$ aus algebraischer Sicht beschreiben? Eine verblüffend einfache Antwort auf diese Frage gab E. Steinitz in seiner grundlegenden Arbeit [15]. Und zwar existiert zu einer beliebigen Körpererweiterung L/K ein System $\mathfrak{x} = (x_i)_{i\in I}$ von Elementen aus L, so dass $\mathfrak{x}$ die Eigenschaften eines Systems von *Variablen* über K hat und L algebraisch über dem "Funktionenkörper" $K(\mathfrak{x})$ ist. Dabei wird das System $\mathfrak{x}$ als eine *Transzendenzbasis* zu L/K bezeichnet, wobei jedoch

S. Bosch, *Algebra*, https://doi.org/10.1007/978-3-662-67464-2_8

zu beachten ist, dass der Zwischenkörper $K(\mathfrak{x})$ im Allgemeinen von der Wahl von $\mathfrak{x}$ abhängt. Steinitz zeigte, dass sich Transzendenzbasen in etwa so wie Basen von Vektorräumen verhalten, und insbesondere, dass je zwei Transzendenzbasen einer Körpererweiterung L/K von gleicher Mächtigkeit sind. Wir werden diese Theorie in Abschnitt 7.1 genauer behandeln.

Die Untersuchung von Körpererweiterungen L/K ohne Algebraizitätsvoraussetzung ist nicht nur vor dem Hintergrund der Erweiterung $\mathbb{C}/\mathbb{Q}$ von Interesse, sondern insbesondere auch aus algebraisch-geometrischer Sicht. Ist K ein Körper mit algebraischem Abschluss $\overline{K}$, so kann man die Elemente des Polynomrings $K[X_1, \ldots, X_n]$ als (Polynom-)Funktionen auf $\overline{K}^n$ interpretieren; vgl. 3.9. Entsprechend geben die Elemente des "Funktionen"-Körpers $K(X_1, \ldots, X_n)$ zu gebrochen rationalen "Funktionen" auf $\overline{K}^n$ Anlass; denn für Quotienten $h \in K(X_1, \ldots, X_n)$, etwa $h = f/g$ mit $f, g \in K[X_1, \ldots, X_n]$, $g \neq 0$, und für Punkte $z \in \overline{K}^n$ mit $g(z) \neq 0$ ist $h(z) = f(z)/g(z)$ als Element von $\overline{K}$ wohldefiniert. Allgemeiner können wir über K endlich erzeugte Erweiterungskörper $L = K(x_1, \ldots, x_n)$ in dieser Weise als Körper von gebrochen rationalen Funktionen interpretieren. Man betrachte nämlich zu einem gegebenen Erzeugendensystem $x_1, \ldots, x_n$ den Unterring $A = K[x_1, \ldots, x_n] \subset L$ und benutze eine Darstellung $A \simeq K[X_1, \ldots, X_n]/\mathfrak{p}$ von A als Restklassenring eines Polynomrings nach einem Primideal $\mathfrak{p}$. Wie in 3.9 kann man dann die Elemente von A als polynomiale Funktionen auf der Nullstellenmenge $V(\mathfrak{p}) \subset \overline{K}^n$ des Ideals $\mathfrak{p}$ ansehen und entsprechend die Elemente von $L = Q(A)$ als gebrochen rationale Funktionen auf $V(\mathfrak{p})$. Wir werden in 7.3 insbesondere die Begriffe *separabel* und rein inseparabel bzw. *primär*, wie wir sagen werden, von algebraischen auf beliebige Körpererweiterungen ausdehnen und plausibel machen, dass diese Eigenschaften zu konkreten geometrischen Eigenschaften der zugehörigen algebraischen Mengen $V(\mathfrak{p})$ korrespondieren; man vergleiche hierzu insbesondere den Schluss von Abschnitt 7.3 und die dortige Aufgabe 4.

Um *separable* und *primäre* Körpererweiterungen in 7.3 handhaben zu können, benötigt man eine gute Kenntnis des Tensorprodukts. Wir haben Tensorprodukte zwar schon in 4.11 in speziellem Rahmen behandelt, doch ist es nunmehr notwendig, die zugehörigen Grundlagen in allgemeinerer Form zu entwickeln; wir tun dies in 7.2. In Abschnitt 7.4 schließlich geben wir eine Charakterisierung separabler Körpererweiterungen mittels Techniken der Differentialrechnung. Die benutzten Methoden sind allerdings rein

algebraischer Natur und vermeiden auf diese Weise den Limesbegriff der Analysis.

7.1 Transzendenzbasen

In 2.5/6 hatten wir für Ringerweiterungen $R \subset R'$ die algebraische Unabhängigkeit bzw. Transzendenz von endlichen Systemen von Elementen aus R' eingeführt. Zunächst erinnern wir noch einmal an diese Definition, wobei wir uns auf Körper beschränken.

Definition 1. *Es sei L/K eine beliebige Körpererweiterung. Ein System $(x_1, \ldots, x_n)$ von Elementen aus L wird als* algebraisch unabhängig *oder* transzendent *über K bezeichnet, wenn aus einer Gleichung des Typs $f(x_1, \ldots, x_n) = 0$ mit einem Polynom $f \in K[X_1, \ldots, X_n]$ stets $f = 0$ folgt, d. h. wenn der Substitutionshomomorphismus*

$$\begin{aligned} K[X_1, \ldots, X_n] &\longrightarrow L, \\ \sum c_{\nu_1 \ldots \nu_n} X_1^{\nu_1} \ldots X_n^{\nu_n} &\longmapsto \sum c_{\nu_1 \ldots \nu_n} x_1^{\nu_1} \ldots x_n^{\nu_n}, \end{aligned}$$

injektiv ist.

Ein System $\mathfrak{X} = (x_i)_{i \in I}$ von (beliebig vielen) Elementen aus L heißt algebraisch unabhängig *oder* transzendent *über K, wenn jedes endliche Teilsystem von $\mathfrak{X}$ im obigen Sinne algebraisch unabhängig über K ist.*

Ist also $\mathfrak{X} = (x_i)_{i \in I}$ ein über K algebraisch unabhängiges System von Elementen aus L, so kann man die x_i in Bezug auf den Körper K als *Variablen* ansehen. Insbesondere ist der von $\mathfrak{X}$ erzeugte Körper $K(\mathfrak{X})$ der Funktionenkörper in den Variablen x_i, $i \in I$, also der Quotientenkörper des Polynomrings $K[\mathfrak{X}]$.

Definition 2. *Es sei L/K eine Körpererweiterung und $\mathfrak{X}$ ein über K algebraisch unabhängiges System von Elementen aus L. Man nennt $\mathfrak{X}$ eine* Transzendenzbasis *von L/K, wenn L algebraisch über $K(\mathfrak{X})$ ist. Gilt bereits $L = K(\mathfrak{X})$, so bezeichnet man L/K als eine* rein transzendente *Körpererweiterung.*

Satz 3. *Es sei L/K eine Körpererweiterung. Ein System $\mathfrak{X}$ von Elementen aus L ist genau dann eine Transzendenzbasis von L/K, wenn $\mathfrak{X}$ ein maximales über K algebraisch unabhängiges System in L ist. Insbesondere besitzt jede Körpererweiterung L/K eine Transzendenzbasis.*

Beweis. Sei zunächst $\mathfrak{X}$ ein maximales über K algebraisch unabhängiges System in L. Dann folgt aus der Maximalität von $\mathfrak{X}$, dass jedes Element aus L algebraisch über $K(\mathfrak{X})$ ist, dass also $\mathfrak{X}$ eine Transzendenzbasis von L/K ist. Für $x \in L$ ist nämlich das System, welches aus $\mathfrak{X}$ durch Hinzufügen von x entsteht, nicht mehr algebraisch unabhängig über K. Es existiert also ein endliches Teilsystem $(x_1, \ldots, x_n)$ von $\mathfrak{X}$ sowie ein nicht-triviales Polynom $f \in K[X_1, \ldots, X_{n+1}]$ mit $f(x_1, \ldots, x_n, x) = 0$. Da die Elemente $x_1, \ldots, x_n$ algebraisch unabhängig über K sind, kommt X_{n+1} in f von mindestens erster Potenz vor. Dies bedeutet aber, dass x algebraisch über $K(x_1, \ldots, x_n)$ und somit über $K(\mathfrak{X})$ ist. Es ist daher L algebraisch über $K(\mathfrak{X})$ und folglich $\mathfrak{X}$ eine Transzendenzbasis von L/K. Da L aufgrund des Zornschen Lemmas 3.4/5 stets ein maximales über K algebraisch unabhängiges System enthält, sieht man insbesondere, dass L/K eine Transzendenzbasis besitzt.

Sei nun umgekehrt $\mathfrak{X}$ als algebraisch unabhängig über K und $L/K(\mathfrak{X})$ als algebraisch angenommen. Dann ist $\mathfrak{X}$ notwendigerweise ein maximales über K algebraisch unabhängiges System in L. □

Als Nächstes wollen wir überlegen, dass man ein System algebraisch unabhängiger Elemente von L durch Hinzunahme von geeigneten Elementen aus einem Erzeugendensystem von L/K zu einer Transzendenzbasis ergänzen kann. Dieses "Austauschargument" werden wir anschließend benutzen, um zu zeigen, dass je zwei Transzendenzbasen von L/K gleiche Mächtigkeit besitzen.

Lemma 4. *Es sei L/K eine Körpererweiterung sowie $\mathfrak{Y}$ ein System von Elementen aus L. Ist dann L algebraisch über $K(\mathfrak{Y})$ und $\mathfrak{X}' \subset L$ ein über K algebraisch unabhängiges System von Elementen aus L, so lässt sich $\mathfrak{X}'$ durch Hinzunahme von Elementen aus $\mathfrak{Y}$ zu einer Transzendenzbasis $\mathfrak{X}$ von L/K vergrößern.*

Insbesondere lässt sich dies auf das leere System $\mathfrak{X}' \subset L$ anwenden, und es folgt, dass man eine Transzendenzbasis von L/K aus $\mathfrak{Y}$ auswählen kann.

Beweis. Man benutze das Zornsche Lemma 3.4/5 und wähle ein maximales Teilsystem $\mathfrak{X}'' \subset \mathfrak{Y}$ mit der Eigenschaft, dass das zusammengesetzte System $\mathfrak{X} = \mathfrak{X}' \cup \mathfrak{X}''$ algebraisch unabhängig über K ist. Ähnlich wie im Beweis zu Satz 3 ist dann jedes $y \in \mathfrak{Y}$ algebraisch über $K(\mathfrak{X})$. Es folgt, dass $K(\mathfrak{X}, \mathfrak{Y})$ algebraisch über $K(\mathfrak{X})$ ist. Dasselbe gilt dann auch für L, und man erkennt $\mathfrak{X}$ als Transzendenzbasis von L/K. □

Theorem 5. *Je zwei Transzendenzbasen einer Körpererweiterung L/K besitzen gleiche Mächtigkeit.*

Bevor wir zum Beweis des Theorems kommen, wollen wir kurz erklären, wie man Mächtigkeiten von Mengen vergleicht. Insbesondere wollen wir zwei Hilfsresultate beweisen, die im Falle unendlicher Transzendenzbasen benötigt werden. Dabei gehen wir allerdings nicht auf die formale Definition der Mächtigkeit oder Kardinalität einer Menge mittels Ordinalzahlen ein (die wir im Grunde genommen auch gar nicht kennen müssen), sondern verweisen diesbezüglich auf die Mengenlehre. Bisher haben wir der Bequemlichkeit halber für eine Menge M die Anzahl $\operatorname{ord} M$ der Elemente stets in naiver Weise aufgefasst. So bedeutet $\operatorname{ord} M = \infty$ lediglich, dass M aus unendlich vielen Elementen besteht, also nicht endlich ist. Im Gegensatz hierzu unterscheidet man bei der Mächtigkeit zwischen verschiedenen Graden der Unendlichkeit. Man nennt zwei Mengen M und N *gleichmächtig* oder *von gleicher Kardinalität* und schreibt $\operatorname{card} M = \operatorname{card} N$, wenn es eine Bijektion $M \longrightarrow N$ gibt. Hilfsweise verwenden wir auch die Notation $\operatorname{card} M \leq \operatorname{card} N$, wenn es eine Injektion $M \hookrightarrow N$ oder, in äquivalenter Weise, eine Surjektion $N \longrightarrow M$ gibt, sofern $M \neq \emptyset$. Dass eine Kette $\operatorname{card} M \leq \operatorname{card} N \leq \operatorname{card} M$ bereits $\operatorname{card} M = \operatorname{card} N$ impliziert, ist im Falle nicht-endlicher Mächtigkeiten keineswegs offensichtlich; es handelt sich um die Aussage des Satzes von Schröder-Bernstein, die wir sogleich beweisen werden. Wie gewohnt bedeutet $\operatorname{card} M = n$ (bzw. $\operatorname{card} M \leq n$) für eine natürliche Zahl n, dass M aus genau (bzw. höchstens) n Elementen besteht.

Lemma 6 (Satz von Schröder-Bernstein). *Für zwei Mengen M und N gebe es Injektionen $\sigma\colon M \hookrightarrow N$ und $\tau\colon N \hookrightarrow M$. Dann existiert eine Bijektion $\rho\colon M \longrightarrow N$.*

Beweis. Es sei $M' \subset M$ die Menge aller Elemente $x \in M$, welche für jedes $n \in \mathbb{N}$ die Eigenschaft

$$x \in (\tau \circ \sigma)^n(M) \quad \Longrightarrow \quad x \in (\tau \circ \sigma)^n \circ \tau(N)$$

besitzen. Ein Element $x \in M$ gehört also genau dann zu M', wenn eine fortgesetzte Urbildbildung der Form

$$x,\ \tau^{-1}(x),\ \sigma^{-1}\tau^{-1}(x),\ \tau^{-1}\sigma^{-1}\tau^{-1}(x),\ \ldots$$

entweder unendlich oft möglich ist oder aber bei einem Element in N endet. Man erkläre sodann eine Abbildung $\rho\colon M \longrightarrow N$ durch

$$\rho(x) = \begin{cases} \tau^{-1}(x) & \text{für } x \in M', \\ \sigma(x) & \text{für } x \notin M'. \end{cases}$$

Es ist ρ injektiv, denn die Einschränkungen $\rho|_{M'}$ und $\rho|_{M-M'}$ sind injektiv, und aus $\rho(x) = \rho(y)$ mit $x \in M'$, $y \in M - M'$ ergibt sich $\sigma(y) = \tau^{-1}(x)$, also $\tau \circ \sigma(y) = x \in M'$ und damit $y \in M'$ im Widerspruch zur Wahl von y. Weiter ist ρ auch surjektiv. Zu $z \in N$ betrachte man nämlich $x = \tau(z)$. Für $x \in M'$ gilt dann die Gleichung $\rho(x) = \tau^{-1}(x) = z$. Für $x \notin M'$ aber besitzt z ein Urbild $y = \sigma^{-1}(z) = \sigma^{-1}(\tau^{-1}(x))$, da anderenfalls x zu M' gehören müsste. Wegen $x \notin M'$ gilt auch $y \notin M'$, und folglich $\rho(y) = \sigma(y) = z$. □

Lemma 7. *Jede unendliche Menge M ist eine disjunkte Vereinigung abzählbar unendlicher Mengen.*

Beweis. Man betrachte die Menge X aller Paare (A, Z), wobei A eine unendliche Teilmenge von M ist und Z eine disjunkte Zerlegung von A in abzählbar unendliche Teilmengen, also ein System von abzählbar unendlichen disjunkten Teilmengen von A, die A überdecken. Da M unendlich ist, gilt $X \neq \emptyset$. Wir schreiben $(A, Z) \leq (A', Z')$ für zwei solche Paare, wenn A in A' enthalten und Z ein Teilsystem von Z' ist. Somit haben wir auf X eine partielle Ordnung definiert, und es ist unmittelbar klar, dass jede total geordnete Teilmenge von X eine obere Schranke in X besitzt. Nach dem Lemma von Zorn 3.4/5 gibt es daher in X ein maximales Element $(\overline{A}, \overline{Z})$. Nun ist aber die Differenz $M - \overline{A}$ aufgrund der Maximalitätseigenschaft von $(\overline{A}, \overline{Z})$ endlich. Indem wir ein beliebiges Element der Zerlegung $\overline{Z}$ um $M - \overline{A}$ vergrößern, erhalten wir insgesamt wie gewünscht eine Zerlegung von M in disjunkte abzählbar unendliche Teilmengen. □

Nun können wir den *Beweis von Theorem* 5 führen. Seien $\mathfrak{X}$ und $\mathfrak{Y}$ zwei Transzendenzbasen von L/K, wobei wir die beiden Systeme für

die Zwecke dieses Beweises als Teilmengen von L ansehen wollen. Zunächst setzen wir $\mathfrak{X}$ als endlich voraus, etwa $\mathfrak{X} = \{x_1, \ldots, x_n\}$, und zeigen $\operatorname{card} \mathfrak{Y} \leq \operatorname{card} \mathfrak{X}$ mit Induktion nach $n = \operatorname{card} \mathfrak{X}$. Aus Symmetriegründen ergibt sich daraus $\operatorname{card} \mathfrak{Y} = \operatorname{card} \mathfrak{X}$. Der Induktionsbeginn $n = 0$ ist trivial, denn dann ist L/K algebraisch. Sei also $n > 0$. In diesem Falle ist L/K nicht mehr algebraisch und folglich $\mathfrak{Y}$ nicht leer. Es existiert also ein Element $y \in \mathfrak{Y}$, und man kann das System $\{y\}$ gemäß Lemma 4 durch Hinzunahme von Elementen aus $\mathfrak{X}$ zu einer Transzendenzbasis $\mathfrak{Z}$ von L/K ergänzen. Dann gilt notwendig $\operatorname{card} \mathfrak{Z} \leq n$, da $\mathfrak{X}$ als maximales über K algebraisch unabhängiges System nicht zusammen mit y in $\mathfrak{Z}$ enthalten sein kann. Nun enthalten aber $\mathfrak{Y}$ und $\mathfrak{Z}$ gemeinsam das Element y. Folglich sind $\mathfrak{Y} - \{y\}$ und $\mathfrak{Z} - \{y\}$ zwei Transzendenzbasen von L über $K(y)$. Benutzt man $\operatorname{card}(\mathfrak{Z} - \{y\}) < \operatorname{card} \mathfrak{Z} \leq n$, so ergibt sich also nach Induktionsvoraussetzung $\operatorname{card}(\mathfrak{Y} - \{y\}) \leq \operatorname{card}(\mathfrak{Z} - \{y\})$ und somit $\operatorname{card} \mathfrak{Y} \leq \operatorname{card} \mathfrak{Z} \leq n = \operatorname{card} \mathfrak{X}$.

Die gerade durchgeführte Argumentation zeigt, dass je zwei Transzendenzbasen $\mathfrak{X}$ und $\mathfrak{Y}$ zu L/K entweder endlich, und dann von gleicher Kardinalität, oder aber beide unendlich sind. Um den Beweis abzuschließen, betrachten wir jetzt noch den Fall, dass $\mathfrak{X}$ und $\mathfrak{Y}$ unendlich sind. Jedes $x \in \mathfrak{X}$ ist algebraisch über $K(\mathfrak{Y})$. Es gibt daher zu $x \in \mathfrak{X}$ eine endliche Teilmenge $\mathfrak{Y}_x \subset \mathfrak{Y}$, so dass x bereits algebraisch über $K(\mathfrak{Y}_x)$ ist. Da L für ein echtes Teilsystem $\mathfrak{Y}' \subsetneq \mathfrak{Y}$ nicht algebraisch über $K(\mathfrak{Y}')$ sein kann, gilt $\bigcup_{x \in \mathfrak{X}} \mathfrak{Y}_x = \mathfrak{Y}$. Man benutze nun die Inklusionen $\mathfrak{Y}_x \hookrightarrow \mathfrak{Y}$, um eine surjektive Abbildung $\coprod_{x \in \mathfrak{X}} \mathfrak{Y}_x \longrightarrow \mathfrak{Y}$ der disjunkten Vereinigung aller $\mathfrak{Y}_x$ nach $\mathfrak{Y}$ zu definieren. Dann gilt $\operatorname{card} \mathfrak{Y} \leq \operatorname{card}(\coprod_{x \in \mathfrak{X}} \mathfrak{Y}_x)$ und sogar $\operatorname{card} \mathfrak{Y} \leq \operatorname{card} \mathfrak{X}$, wenn wir die Gleichung $\operatorname{card}(\coprod_{x \in \mathfrak{X}} \mathfrak{Y}_x) = \operatorname{card} \mathfrak{X}$ verifizieren können. Besteht $\mathfrak{X}$ nur aus abzählbar unendlich vielen Elementen, so kann man diese Gleichung durch einfaches "Abzählen" nachprüfen. Den Allgemeinfall führt man aber leicht hierauf zurück, da $\mathfrak{X}$ nach Lemma 7 als unendliche Menge eine disjunkte Vereinigung abzählbar unendlicher Teilmengen ist. Somit erhält man $\operatorname{card} \mathfrak{Y} \leq \operatorname{card} \mathfrak{X}$ und aus Symmetriegründen auch $\operatorname{card} \mathfrak{X} \leq \operatorname{card} \mathfrak{Y}$. Hieraus folgt $\operatorname{card} \mathfrak{X} = \operatorname{card} \mathfrak{Y}$ unter Benutzung von Lemma 6. □

Das soeben bewiesene Resultat gestattet es uns, für beliebige Körpererweiterungen L/K den *Transzendenzgrad* $\operatorname{transgrad}_K L$ zu definieren, und zwar als die Mächtigkeit einer Transzendenzbasis von L/K. Algebraische

Erweiterungen sind stets vom Transzendenzgrad 0, während für einen Polynomring $K[X_1, \ldots, X_n]$ der Quotientenkörper $K(X_1, \ldots, X_n)$ eine rein transzendente Erweiterung vom Transzendenzgrad n über K darstellt. Allgemeiner ist für ein beliebiges System $\mathfrak{X}$ von Variablen der Quotientenkörper $K(\mathfrak{X})$ des Polynomrings $K[\mathfrak{X}]$ eine rein transzendente Erweiterung von K vom Transzendenzgrad $\operatorname{card} \mathfrak{X}$. Da K-Isomorphismen Transzendenzbasen wieder in ebensolche überführen, sieht man:

Korollar 8. *Zu zwei rein transzendenten Körpererweiterungen L/K und L'/K gibt es genau dann einen K-Isomorphismus $L \xrightarrow{\sim} L'$, wenn L und L' vom gleichen Transzendenzgrad über K sind.*

Hieraus ergibt sich insbesondere, dass es keinen K-Isomorphismus zwischen Polynomringen $K[X_1, \ldots, X_m]$ und $K[Y_1, \ldots, Y_n]$ unterschiedlicher Variablenanzahlen m und n geben kann. Die beiden Quotientenkörper wären sonst nämlich isomorphe Körpererweiterungen von K, hätten aber unterschiedliche Transzendenzgrade, was unmöglich ist. Wir wollen dieses Argument noch in etwas sorgfältigerer Weise auswerten.

Korollar 9. *Sei $\varphi\colon K[X_1, \ldots, X_m] \longrightarrow K[Y_1, \ldots, Y_n]$ ein K-Homomorphismus zwischen Polynomringen, so dass jede Variable $Y \in \{Y_1, \ldots, Y_n\}$ eine Gleichung des Typs*

$$Y^r + c_1 Y^{r-1} + \ldots + c_r = 0, \qquad c_1, \ldots, c_r \in \operatorname{im} \varphi,$$

erfüllt (d. h. φ ist ganz im Sinne von Abschnitt 3.3; *vgl.* 3.3/4). *Dann folgt $m \geq n$. Ferner ist φ genau dann injektiv, wenn $m = n$ gilt.*

Beweis. Es sei R das Bild von φ. Als Unterring von $K[Y_1, \ldots, Y_n]$ ist dies ein Integritätsring, so dass wir $K(Y_1, \ldots, Y_n)$ als Erweiterungskörper von $Q(R)$ ansehen können. Da $K(Y_1, \ldots, Y_n) = Q(R)(Y_1, \ldots, Y_n)$ gilt und die Elemente $Y_1, \ldots, Y_n$ gemäß unserer Voraussetzung algebraisch über $Q(R)$ sind, ist die Erweiterung $K(Y_1, \ldots, Y_n)/Q(R)$ algebraisch. Es haben daher $Q(R)$ und $K(Y_1, \ldots, Y_n)$ denselben Transzendenzgrad über K, nämlich n. Da andererseits die Variablen $X_1, \ldots, X_m$ zu Elementen $x_1, \ldots, x_m \in Q(R)$ Anlass geben, die die Erweiterung $Q(R)/K$ erzeugen, ergibt sich $m \geq n$ mit Lemma 4.

Es ist φ genau dann injektiv, wenn die Elemente $x_1, \ldots, x_m \in Q(R)$ algebraisch unabhängig über K sind, d. h. wenn $\operatorname{transgrad}_K Q(R) = m$ gilt.

Da wir aber bereits $\operatorname{transgrad}_K Q(R) = n$ gezeigt haben, ist wie behauptet die Injektivität von φ äquivalent zu $m = n$. □

Wir wollen noch für eine Körperkette $K \subset L \subset M$ darauf hinweisen, dass sich der Transzendenzgrad additiv verhält:

$$\operatorname{transgrad}_K M = \operatorname{transgrad}_K L + \operatorname{transgrad}_L M.$$

Dies verifiziert man leicht, indem man Transzendenzbasen $\mathfrak{X}$ und $\mathfrak{Y}$ von L/K und M/L betrachtet und zeigt, dass dann $\mathfrak{X} \cup \mathfrak{Y}$ eine Transzendenzbasis von M/K ist. Die Summe der Kardinalitäten von $\mathfrak{X}$ und $\mathfrak{Y}$ ist per definitionem die Kardinalität der (disjunkten) Vereinigung $\mathfrak{X} \cup \mathfrak{Y}$.

Zum Schluss wollen wir noch zeigen, dass für eine rein transzendente Erweiterung L/K der algebraische Abschluss von K in L stets mit K übereinstimmt, dass K also algebraisch abgeschlossen in L ist.

Bemerkung 10. *Es sei L/K eine rein transzendente Körpererweiterung. Dann ist jedes $x \in L - K$ transzendent über K.*

Beweis. Man betrachte ein über K algebraisches Element $x \in L$ sowie eine Transzendenzbasis $\mathfrak{X}$ von L/K mit $L = K(\mathfrak{X})$. Dann existiert ein endliches Teilsystem $(x_1, \ldots, x_r)$ von $\mathfrak{X}$ mit $x \in K(x_1, \ldots, x_r)$. Um $x \in K$ zu zeigen, dürfen wir folglich $\mathfrak{X}$ als endlich ansehen, etwa $\mathfrak{X} = (x_1, \ldots, x_r)$. Sei nun

$$f = X^n + c_1 X^{n-1} + \ldots + c_n \in K[X]$$

das Minimalpolynom von $x \in L = K(\mathfrak{X})$ über K, wobei wir $x \neq 0$ und somit $c_n \neq 0$ annehmen dürfen. Indem wir $K[\mathfrak{X}]$ als Polynomring in den Variablen $x_1, \ldots, x_r$ interpretieren, sehen wir mit 2.7/3, dass dieser Ring faktoriell ist. Wir können deshalb x als gekürzten Bruch zweier teilerfremder Elemente schreiben, $x = g/h$ mit $g, h \in K[\mathfrak{X}]$, $h \neq 0$. Die Gleichung $f(x) = 0$ liefert dann

$$g^n + c_1 g^{n-1} h + \ldots + c_n h^n = 0.$$

Jedes Primelement $q \in K[\mathfrak{X}]$, welches h teilt, teilt somit auch g, und es folgt, dass h eine Einheit in $K[\mathfrak{X}]$ ist, also $h \in K^*$. In gleicher Weise zeigt man $g \in K^*$, so dass sich insgesamt $x \in K$ ergibt. □

Lernkontrolle und Prüfungsvorbereitung

1. Es sei L/K eine Körpererweiterung. Wann bezeichnet man ein System $\mathfrak{X}$ von Elementen aus L als transzendent über K? Was ist eine Transzendenzbasis von L/K. Wann bezeichnet man die Erweiterung L/K als rein transzendent?
2. Zeige, dass jede Körpererweiterung L/K eine Transzendenzbasis besitzt.
3. Es sei L/K eine Körpererweiterung und $\mathfrak{Y}$ ein System von Elementen aus L, so dass L algebraisch über $K(\mathfrak{Y})$ ist. Sei weiter $\mathfrak{X}'$ ein System von Elementen aus L, welches transzendent über K ist. Zeige, dass sich $\mathfrak{X}'$ durch Hinzunahme von Elementen aus $\mathfrak{Y}$ zu einer Transzendenzbasis von L/K vergrößern lässt.
4. Wie lautet der Satz von Schröder-Bernstein?

+5. Beweise den Satz von Schröder-Bernstein.

+6. Zeige, dass jede unendliche Menge eine disjunkte Vereinigung abzählbar unendlicher Teilmengen ist.

7. Nutze die Resultate aus Punkt 4 und 6, um zu zeigen, dass je zwei Transzendenzbasen einer Körpererweiterung L/K gleiche Mächtigkeit besitzen.
8. Sei $\varphi\colon K[X_1,\ldots,X_m] \longrightarrow K[Y_1,\ldots,Y_n]$ ein ganzer Ringhomomorphismus zwischen Polynomringen über einem Körper K. Zeige $m \geq n$ und weiter, dass genau dann $m = n$ gilt, wenn φ injektiv ist.
9. Sei L/K eine rein transzendente Körpererweiterung. Zeige, dass jedes Element $x \in L - K$ transzendent über K ist.

Übungsaufgaben

1. *Vergleiche den Begriff der Transzendenzbasis einer Körpererweiterung L/K mit dem Begriff der Basis eines Vektorraums.*
2. *Zeige, dass es Automorphismen von $\mathbb{C}$ gibt, die $\mathbb{R}$ nicht in sich selbst abbilden, sowie weiter, dass $\mathbb{C}$ zu sich selbst isomorphe echte Teilkörper enthält.*
3. Zeige, dass der Transzendenzgrad von $\mathbb{R}/\mathbb{Q}$ gleich der Kardinalität von $\mathbb{R}$ ist.
4. Zeige, dass jeder Körper der Charakteristik 0 Vereinigung von Teilkörpern ist, die isomorph zu Teilkörpern von $\mathbb{C}$ sind.
5. Es sei L/K eine Körpererweiterung und $\mathfrak{X}$ ein über K algebraisch unabhängiges System von Elementen aus L. Zeige, dass für jeden über K algebraischen Zwischenkörper K' zu L/K das System $\mathfrak{X}$ algebraisch unabhängig über K' ist.
6. Es sei L/K eine endlich erzeugte Körpererweiterung. Zeige, dass dann auch für jeden Zwischenkörper L' zu L/K die Erweiterung L'/K endlich erzeugt ist.

7.2 Tensorprodukte*

In Abschnitt 4.11 hatten wir bereits eine vereinfachte Version des Tensorprodukts kennen gelernt. Wir wollen nunmehr Tensorprodukte etwas grundsätzlicher studieren, und zwar im Hinblick auf Anwendungen bei separablen bzw. primären Körpererweiterungen in Abschnitt 7.3. Dabei beginnen wir mit dem Tensorprodukt von Moduln; zur Definition eines Moduls über einem Ring sei auf Abschnitt 2.9 verwiesen.

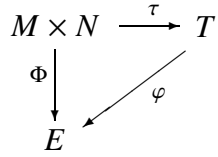
Im Folgenden seien M, N Moduln über einem Ring R. Ist E ein weiterer R-Modul, so nennt man eine Abbildung $\Phi\colon M \times N \longrightarrow E$ wie üblich *R-bilinear*, wenn für alle $x \in M$, $y \in N$ die Abbildungen

$$\begin{aligned} \Phi(x,\cdot)\colon N &\longrightarrow E, \qquad z \longmapsto \Phi(x,z), \\ \Phi(\cdot,y)\colon M &\longrightarrow E, \qquad z \longmapsto \Phi(z,y), \end{aligned}$$

jeweils *R-linear*, d. h. Homomorphismen von R-Moduln sind. Ein Tensorprodukt von M mit N über dem Ring R ist nun ein R-Modul T, derart dass die R-bilinearen Abbildungen von $M \times N$ in einen beliebigen R-Modul E in umkehrbar eindeutiger Weise durch die R-linearen Abbildungen $T \longrightarrow E$ beschrieben werden:

Definition 1. *Ein* Tensorprodukt *zweier R-Moduln M und N über einem Ring R ist gegeben durch einen R-Modul T zusammen mit einer R-bilinearen Abbildung $\tau\colon M \times N \longrightarrow T$, welche folgende universelle Eigenschaft besitzt*:

Zu jeder R-bilinearen Abbildung $\Phi\colon M \times N \longrightarrow E$ in einen R-Modul E existiert eine eindeutig bestimmte R-lineare Abbildung $\varphi\colon T \longrightarrow E$ mit $\Phi = \varphi \circ \tau$, so dass also das Diagramm



kommutiert.

Tensorprodukte sind aufgrund der definierenden universellen Eigenschaft bis auf kanonische Isomorphie eindeutig bestimmt. Ihre Existenz ist stets gesichert, wie wir sogleich beweisen werden. In der Situation von

Definition 1 schreibt man meist $M \otimes_R N$ anstelle von T. Außerdem ist es üblich, für $x \in M$, $y \in N$ das Bild von (x, y) unter der bilinearen Abbildung $\tau\colon M \times N \longrightarrow T$ mit $x \otimes y$ zu bezeichnen; Elemente des Typs $x \otimes y$ heißen *Tensoren* in $M \otimes_R N$. Unter Benutzung dieser Notation beschreibt sich die R-bilineare Abbildung τ durch

$$M \times N \longrightarrow M \otimes_R N, \qquad (x, y) \longmapsto x \otimes y.$$

Insbesondere sind also Tensoren R-bilinear in den beiden Faktoren, d. h. es gilt

$$\begin{aligned}&(ax + a'x') \otimes (by + b'y')\\ &= ab(x \otimes y) + ab'(x \otimes y') + a'b(x' \otimes y) + a'b'(x' \otimes y')\end{aligned}$$

für $a, a', b, b' \in R,\ x, x' \in M,\ y, y' \in N$. In vielen Fällen wird die definierende R-bilineare Abbildung $\tau\colon M \times N \longrightarrow M \otimes_R N$ nicht explizit erwähnt. Man bezeichnet dann $M \otimes_R N$ als Tensorprodukt von M und N über R und geht von der "Kenntnis" der Tensoren $x \otimes y$ in $M \otimes_R N$ aus, mit deren Hilfe man die Abbildung τ rekonstruieren kann.

Satz 2. *Das oben definierte Tensorprodukt $T = M \otimes_R N$ existiert für beliebige R-Moduln M und N.*

Beweis. Die Konstruktionsidee ist recht einfach. Wir beginnen mit dem von allen Paaren $(x, y) \in M \times N$ erzeugten freien R-Modul, also mit $R^{(M\times N)}$, und dividieren durch den kleinsten Untermodul Q, so dass die Restklassen zu den Elementen des Typs (x, y) die Eigenschaften von Tensoren erhalten.[1] Dies bedeutet, wir konstruieren den Untermodul $Q \subset R^{(M\times N)}$, der von allen Elementen

$$\begin{gathered}(x + x', y) - (x, y) - (x', y),\\ (x, y + y') - (x, y) - (x, y'),\\ (ax, y) - a(x, y),\\ (x, ay) - a(x, y)\end{gathered}$$

mit $a \in R, x, x' \in M, y, y' \in N$ erzeugt wird, und betrachten den Quotienten $T = R^{(M\times N)}/Q$. Die kanonische Abbildung $\tau\colon M \times N \longrightarrow T$, welche ein

[1] (x, y) korrespondiert hier zu demjenigen Element $(r_{m,n})_{m\in M, n\in N}$ in $R^{(M\times N)}$, welches unter Verwendung des Kronecker-Symbols durch $r_{m,n} = \delta_{m,x}\delta_{n,y}$ definiert ist.

Paar (x, y) auf die Restklasse zu (x, y) in T abbildet, ist dann R-bilinear. Wir wollen zeigen, dass τ die universelle Eigenschaft eines Tensorprodukts aus Definition 1 erfüllt. Sei also $\Phi\colon M \times N \longrightarrow E$ eine R-bilineare Abbildung in einen R-Modul E. Hieraus erhält man in kanonischer Weise eine R-lineare Abbildung $\hat{\varphi}\colon R^{(M\times N)} \longrightarrow E$, indem man $\hat{\varphi}(x, y) = \Phi(x, y)$ für die Basiselemente des Typs $(x, y) \in R^{(M\times N)}$ verlangt sowie $\hat{\varphi}$ insgesamt durch R-lineare Ausdehnung erklärt. Aus der R-Bilinearität von Φ schließt man dann, dass $\ker \hat{\varphi}$ alle obigen erzeugenden Elemente von Q enthält, dass also $\hat{\varphi}$ eine R-lineare Abbildung $\varphi\colon R^{(M\times N)}/Q \longrightarrow E$ mit $\Phi = \varphi \circ \tau$ induziert. Letztere ist durch die Relation $\Phi = \varphi \circ \tau$ eindeutig bestimmt, denn die Restklassen $\overline{(x, y)}$ der Basiselemente $(x, y) \in R^{(M\times N)}$ erzeugen $R^{(M\times N)}/Q$ als R-Modul, und es gilt wegen $\Phi = \varphi \circ \tau$ notwendig

$$\varphi\big(\overline{(x, y)}\big) = \varphi\big(\tau(x, y)\big) = \Phi(x, y).$$

Also ist φ auf einem Erzeugendensystem des R-Moduls $T = R^{(M\times N)}/Q$ eindeutig festgelegt und damit insgesamt eindeutig. □

Für die Handhabung von Tensorprodukten ist deren explizite Konstruktion, wie sie im Beweis zu Satz 2 ausgeführt wurde, nur von geringem Interesse. In den allermeisten Fällen ist es einfacher und übersichtlicher, die benötigten Eigenschaften aus der definierenden universellen Eigenschaft des Tensorprodukts abzuleiten. Aus der Konstruktion von $M \otimes_R N$ sieht man beispielsweise, dass sich jedes Element $z \in M \otimes_R N$ als endliche Summe von Tensoren schreiben lässt, etwa $z = \sum_{i=1}^{n} x_i \otimes y_i$. Dies ergibt sich aber auch unmittelbar aus der universellen Eigenschaft von $M \otimes_R N$, da der von allen Tensoren in $M \otimes_R N$ erzeugte Untermodul ebenfalls die universelle Eigenschaft eines Tensorprodukts von M und N über R besitzt. Zu der Notation der Tensoren sei noch bemerkt, dass für einen Tensor $x \otimes y$ stets das zugehörige Tensorprodukt $M \otimes_R N$ angegeben werden muss, in dem dieser Tensor gebildet wird, es sei denn, dies ist aus dem Zusammenhang klar. Für einen Untermodul $M' \subset M$ ist nämlich das Tensorprodukt $M' \otimes_R N$ nicht notwendig ein Untermodul von $M \otimes_R N$. Im Allgemeinen gibt es von Null verschiedene Tensoren $x \otimes y$ in $M' \otimes_R N$, die als Tensoren in $M \otimes_R N$ verschwinden. Man betrachte etwa den Tensor $2 \otimes 1$ in $(2\mathbb{Z}) \otimes_{\mathbb{Z}} (\mathbb{Z}/2\mathbb{Z})$ sowie in $\mathbb{Z} \otimes_{\mathbb{Z}} (\mathbb{Z}/2\mathbb{Z})$; dieses Beispiel werden wir weiter unten noch genauer diskutieren.

In vielen Fällen ist es bequem, zur Beschreibung einer R-linearen Abbildung $M \otimes_R N \longrightarrow E$ von einem Tensorprodukt in einen R-Modul E

lediglich die Bilder der Tensoren $x \otimes y \in M \otimes_R N$ in E anzugeben; es wird nämlich, wie wir wissen, $M \otimes_R N$ als R-Modul von diesen Tensoren erzeugt. Dabei ist allerdings zu beachten, dass die Bilder der Tensoren aus $M \otimes_R N$ nicht in beliebiger Weise vorgegeben werden dürfen, sondern die Regeln der R-Bilinearität erfüllen müssen. Zu einer Familie $(z_{x,y})_{x\in M, y\in N}$ von Elementen aus E existiert genau dann eine R-lineare Abbildung $M \otimes_R N \longrightarrow E$ mit $x\otimes y \longmapsto z_{x,y}$, wenn $(x, y) \longmapsto z_{x,y}$ eine R-bilineare Abbildung $M\times N \longrightarrow E$ definiert.

Bemerkung 3. *Zu R-Moduln M, N, P existieren kanonische R-Isomorphismen*

$$\begin{aligned} R \otimes_R M &\xrightarrow{\sim} M, & a \otimes x &\longmapsto ax, \\ M \otimes_R N &\xrightarrow{\sim} N \otimes_R M, & x \otimes y &\longmapsto y \otimes x, \\ (M \otimes_R N) \otimes_R P &\xrightarrow{\sim} M \otimes_R (N \otimes_R P), & (x \otimes y) \otimes z &\longmapsto x \otimes (y \otimes z), \end{aligned}$$

welche durch die angegebenen Abbildungsvorschriften eindeutig charakterisiert sind.

Beweis. In allen drei Fällen geht man ähnlich vor. Man zeigt zunächst, dass die auf den Tensoren erklärte Abbildungsvorschrift zu einer wohldefinierten R-linearen Abbildung führt und konstruiert dann in nahe liegender Weise eine hierzu inverse Abbildung. Wir führen dies nur für den ersten Isomorphismus aus. Da die Abbildung $R\times M \longrightarrow M$, $(a, x) \longmapsto ax$, R-bilinear ist, gibt sie Anlass zu einer R-linearen Abbildung $\varphi\colon R \otimes_R M \longrightarrow M$, $a \otimes x \longmapsto ax$. Um eine hierzu inverse Abbildung anzugeben, betrachte man die R-lineare Abbildung $\psi\colon M \longrightarrow R \otimes_R M$, $x \longmapsto 1 \otimes x$. Dann gilt $\varphi \circ \psi(x) = x$ für alle $x \in M$ und entsprechend $\psi \circ \varphi(a \otimes x) = \psi(ax) = 1 \otimes ax = a \otimes x$ für alle Tensoren $a \otimes x$ in $R \otimes_R M$. Es folgt $\varphi \circ \psi = \mathrm{id}$ und $\psi \circ \varphi = \mathrm{id}$, d. h. φ ist ein Isomorphismus mit $\varphi^{-1} = \psi$. □

Dieselbe Beweisidee liefert die Vertauschbarkeit von Tensorprodukten mit direkten Summen:

Bemerkung 4. *Es sei $(M_i)_{i\in I}$ eine Familie von R-Moduln sowie N ein weiterer R-Modul. Dann gibt es einen kanonischen Isomorphismus*

$$\Big(\bigoplus_{i\in I} M_i\Big) \otimes_R N \xrightarrow{\sim} \bigoplus_{i\in I} (M_i \otimes_R N), \quad (x_i)_{i\in I} \otimes y \longmapsto (x_i \otimes y)_{i\in I},$$

welcher durch die angegebene Abbildungsvorschrift eindeutig charakterisiert ist. Tensorprodukte kommutieren also mit direkten Summen.

Als Nächstes betrachten wir zwei R-lineare Abbildungen $\varphi\colon M \longrightarrow M'$ und $\psi\colon N \longrightarrow N'$ und definieren deren Tensorprodukt als R-lineare Abbildung $\varphi \otimes \psi\colon M \otimes_R N \longrightarrow M' \otimes_R N'$ durch $x \otimes y \longmapsto \varphi(x) \otimes \psi(y)$. Dies ist möglich, da durch $(x, y) \longmapsto \varphi(x) \otimes \psi(y)$ eine R-bilineare Abbildung $M \times N \longrightarrow M' \otimes_R N'$ gegeben wird. Insbesondere kann man das Tensorprodukt $\varphi \otimes \mathrm{id}\colon M \otimes_R N \longrightarrow M' \otimes_R N$ von φ mit der identischen Abbildung auf N bilden; man sagt, die Abbildung $\varphi\colon M \longrightarrow M'$ werde mit N tensoriert. Um das Verhalten von R-linearen Abbildungen bei Tensorieren mit einem R-Modul N zu studieren, benutzen wir den Begriff der *exakten Sequenz*. Hierunter versteht man eine Folge R-linearer Abbildungen

$$M_1 \xrightarrow{\varphi_1} M_2 \xrightarrow{\varphi_2} \ldots \xrightarrow{\varphi_{r-1}} M_r,$$

so dass $\operatorname{im}\varphi_i = \ker\varphi_{i+1}$ für $i = 1, \ldots, r-2$ gilt.

Satz 5. *Es sei*

$$M' \xrightarrow{\varphi} M \xrightarrow{\psi} M'' \longrightarrow 0$$

eine exakte Sequenz von R-Moduln. Dann ist für jeden R-Modul N auch die tensorierte Sequenz

$$M' \otimes_R N \xrightarrow{\varphi\otimes\mathrm{id}} M \otimes_R N \xrightarrow{\psi\otimes\mathrm{id}} M'' \otimes_R N \longrightarrow 0$$

exakt.

Beweis. Zunächst gilt $(\psi \otimes \mathrm{id}) \circ (\varphi \otimes \mathrm{id}) = (\psi \circ \varphi) \otimes \mathrm{id} = 0$ wegen $\psi \circ \varphi = 0$, d. h. wir haben $\operatorname{im}(\varphi \otimes \mathrm{id}) \subset \ker(\psi \otimes \mathrm{id})$. Daher induziert $\psi \otimes \mathrm{id}$ eine R-lineare Abbildung

$$\overline{\psi}\colon (M \otimes_R N) \big/ \operatorname{im}(\varphi \otimes \mathrm{id}) \longrightarrow M'' \otimes_R N,$$

und es genügt zu zeigen, dass $\overline{\psi}$ ein Isomorphismus ist. Um eine inverse Abbildung zu $\overline{\psi}$ zu konstruieren, benutzen wir die Surjektivität von ψ und wählen zu jedem $x'' \in M''$ ein Element $\iota(x'') \in M$ mit $\psi(\iota(x'')) = x''$; die resultierende Abbildung $\iota\colon M'' \longrightarrow M$ ist lediglich eine Abbildung zwischen *Mengen*. Man betrachte nun die Abbildung

$$\sigma\colon M'' \times N \longrightarrow (M \otimes_R N) \big/ \operatorname{im}(\varphi \otimes \mathrm{id}), \qquad (x'', y) \longmapsto \overline{\iota(x'') \otimes y},$$

wobei $\overline{\iota(x'') \otimes y}$ die Restklasse von $\iota(x'') \otimes y$ in $(M \otimes_R N)/\operatorname{im}(\varphi \otimes \mathrm{id})$ bezeichne. Wir behaupten, dass σ eine R-bilineare Abbildung ist. Nur die Linearität im ersten Argument ist nachzuprüfen, und diese folgt, wenn wir zeigen können, dass das Element $\overline{\iota(x'') \otimes y}$ unabhängig von der Wahl des Urbildes $\iota(x'') \in M$ zu $x'' \in M''$ ist. Um diese Unabhängigkeit einzusehen, betrachte man zwei Urbilder $x_1, x_2 \in M$ zu x''. Es gilt dann $x_1 - x_2 \in \operatorname{im}\varphi$, etwa $x_1 - x_2 = \varphi(x')$, da die Sequenz $M' \to M \to M'' \to 0$ exakt ist. Hieraus folgt aber

$$\overline{x_1 \otimes y} - \overline{x_2 \otimes y} = \overline{\varphi(x') \otimes y} = \overline{(\varphi \otimes \mathrm{id})(x' \otimes y)} = 0,$$

wie behauptet. Mithin ist σ wie oben definiert eine R-bilineare Abbildung, und man sieht, dass die induzierte R-lineare Abbildung

$$M'' \otimes_R N \longrightarrow (M \otimes_R N)/\operatorname{im}(\varphi \otimes \mathrm{id})$$

invers zu $\overline{\psi}$ ist. □

Als Folgerung zu Satz 5 kann man für R-Moduln M, N sowie einen Untermodul $M' \subset M$ das Tensorprodukt $(M/M') \otimes_R N$ konkretisieren. Aus der kanonischen exakten Sequenz

$$M' \xrightarrow{\varphi} M \xrightarrow{\psi} M/M' \longrightarrow 0$$

ergibt sich die exakte Sequenz

$$M' \otimes_R N \xrightarrow{\varphi\otimes\mathrm{id}} M \otimes_R N \xrightarrow{\psi\otimes\mathrm{id}} (M/M') \otimes_R N \longrightarrow 0,$$

man erhält also einen Isomorphismus

$$(M/M') \otimes_R N \xrightarrow{\sim} (M \otimes_R N)/\operatorname{im}(\varphi \otimes \mathrm{id}), \quad \overline{x} \otimes y \longmapsto \overline{x \otimes y}.$$

An dieser Stelle sei darauf hingewiesen, dass aus der Injektivität von φ im Allgemeinen nicht die Injektivität der tensorierten Abbildung $\varphi \otimes \mathrm{id}$ folgt, d. h. man kann $M' \otimes_R N$ im Allgemeinen nicht bezüglich $\varphi \otimes \mathrm{id}$ als Untermodul von $M \otimes_R N$ auffassen. So ist die von der Inklusion $2\mathbb{Z} \hookrightarrow \mathbb{Z}$ induzierte Abbildung $2\mathbb{Z} \otimes_{\mathbb{Z}} (\mathbb{Z}/2\mathbb{Z}) \longrightarrow \mathbb{Z} \otimes_{\mathbb{Z}} (\mathbb{Z}/2\mathbb{Z})$ die Nullabbildung, da in $\mathbb{Z} \otimes_{\mathbb{Z}} (\mathbb{Z}/2\mathbb{Z})$ alle Tensoren der Form $2a \otimes \overline{b}$ auch in der

Form $a \otimes 2\overline{b}$ geschrieben werden können und deshalb verschwinden, wobei $2\mathbb{Z} \otimes_{\mathbb{Z}} (\mathbb{Z}/2\mathbb{Z}) \simeq \mathbb{Z} \otimes_{\mathbb{Z}} (\mathbb{Z}/2\mathbb{Z}) \simeq \mathbb{Z}/2\mathbb{Z}$ von Null verschieden ist.

Man nennt einen R-Modul N *flach*, wenn für jeden injektiven Homomorphismus von R-Moduln $M' \hookrightarrow M$ die zugehörige mit N tensorierte Abbildung $M' \otimes_R N \longrightarrow M \otimes_R N$ injektiv ist. Hierzu ist äquivalent, dass exakte Sequenzen des Typs $0 \to M' \to M \to M'' \to 0$ bei Tensorieren mit N exakt bleiben. Aus den Bemerkungen 3 und 4 ergibt sich beispielsweise:

Bemerkung 6. *Freie R-Moduln sind flach, insbesondere also jeder Vektorraum über einem Körper.*

Wir wollen als Nächstes für R-Moduln den Prozess der Koeffizientenerweiterung erklären. Sei $f : R \longrightarrow R'$ ein Ringhomomorphismus. Indem wir R' bezüglich f als R-Modul auffassen, können wir für jeden R-Modul M das Tensorprodukt $M \otimes_R R'$ bilden. Dieses ist per definitionem ein R-Modul, wobei sich die R-Modulstruktur von $M \otimes_R R'$ sogar zu einer R'-Modulstruktur fortsetzen lässt. Und zwar erkläre man das Produkt eines Elementes $a \in R'$ mit einem Tensor $(x \otimes b) \in M \otimes_R R'$ durch $x \otimes (ab)$. Hierbei beachte man, dass die Abbildung

$$M \times R' \longrightarrow M \otimes_R R', \qquad (x, b) \longmapsto x \otimes (ab),$$

R-bilinear ist, also eine R-lineare Abbildung

$$M \otimes_R R' \longrightarrow M \otimes_R R', \qquad x \otimes b \longmapsto x \otimes (ab),$$

induziert. Letztere ist gerade die Multiplikation mit a. Unter Benutzung der Rechenregeln für Tensoren sieht man unmittelbar, dass die so definierte Produktbildung den Eigenschaften einer R'-Modulstruktur genügt. Man sagt, der R'-Modul $M \otimes_R R'$ entstehe aus M durch *Erweiterung der Koeffizienten*. Auch überzeugt man sich leicht davon, dass die hier gegebene Definition der Koeffizientenerweiterung mit derjenigen aus Abschnitt 4.11 übereinstimmt, wo wir lediglich Vektorräume über Körpern betrachtet haben; man vergleiche auch Aufgabe 1.

Bemerkung 7. *Es seien $R \longrightarrow R' \longrightarrow R''$ Ringhomomorphismen sowie M ein R-Modul. Dann existiert ein kanonischer Isomorphismus von R''-Moduln*

$$(M \otimes_R R') \otimes_{R'} R'' \xrightarrow{\sim} M \otimes_R R'', \quad (x \otimes a') \otimes a'' \longmapsto x \otimes (a'a''),$$

welcher durch die angegebene Abbildungsvorschrift eindeutig charakterisiert ist.

Beweis. Zunächst induziert $R' \longrightarrow R''$, aufgefasst als R-lineare Abbildung, durch Tensorieren mit M eine R'-lineare Abbildung

$$\sigma\colon M \otimes_R R' \longrightarrow M \otimes_R R'',$$

und es ist

$$(M \otimes_R R') \times R'' \longrightarrow M \otimes_R R'', \qquad (x, a'') \longmapsto a'' \cdot \sigma(x),$$

eine wohldefinierte R'-bilineare Abbildung, welche die zu betrachtende Abbildung $(M \otimes_R R') \otimes_{R'} R'' \longrightarrow M \otimes_R R''$ induziert. Letztere ist R''-linear, wie man anhand der Tensoren leicht nachrechnet. Um eine inverse Abbildung zu konstruieren, betrachte man die R-bilineare Abbildung

$$M \times R'' \longrightarrow (M \otimes_R R') \otimes_{R'} R'', \qquad (x, a'') \longmapsto (x \otimes 1) \otimes a'',$$

sowie die zugehörige Abbildung $M \otimes_R R'' \longrightarrow (M \otimes_R R') \otimes_{R'} R''$. □

Wir werden den Prozess der Koeffizientenerweiterung speziell für Ringhomomorphismen des Typs $R \longrightarrow R_S$ benutzen, wobei $S \subset R$ ein multiplikatives System sei; hierbei bezeichnet R_S die Lokalisierung von R nach S, d. h. $R_S = S^{-1}R$ in der Notation von Abschnitt 2.7. Man kann also zu einem R-Modul M stets den R_S-Modul $M \otimes_R R_S$ betrachten. Andererseits lässt sich aber zu M auch ein R_S-Modul durch Lokalisieren konstruieren. Man betrachte nämlich die Menge aller Brüche $\frac{x}{s}$ mit $x \in M$, $s \in S$ und identifiziere jeweils $\frac{x}{s}$ mit einem weiteren Bruch $\frac{x'}{s'}$, falls es ein $s'' \in S$ mit $s''(s'x - sx') = 0$ gibt. Die resultierende Menge ist dann unter den gewöhnlichen Regeln der Bruchrechnung ein R_S-Modul; dieser wird mit M_S bezeichnet.

Satz 8. *Es sei $S \subset R$ ein multiplikatives System.*

(i) *Die kanonische Abbildung $R \longrightarrow R_S$ ist flach, d. h. R_S ist unter dieser Abbildung ein flacher R-Modul.*

(ii) *Zu jedem R-Modul M gibt es einen kanonischen Isomorphismus von R- bzw. R_S-Moduln*

$$M \otimes_R R_S \xrightarrow{\sim} M_S, \qquad x \otimes \frac{a}{s} \longmapsto \frac{ax}{s},$$

welcher durch die angegebene Abbildungsvorschrift eindeutig charakterisiert ist.

Beweis. Wir beginnen mit Aussage (ii). Die Abbildung

$$M \times R_S \longrightarrow M_S, \qquad \left(x, \frac{a}{s}\right) \longmapsto \frac{ax}{s},$$

ist wohldefiniert, wie man leicht einsieht, und darüber hinaus R-bilinear, gibt also Anlass zu einer eindeutig bestimmten R-linearen Abbildung $\varphi\colon M \otimes_R R_S \longrightarrow M_S$ mit der in (ii) gegebenen Abbildungsvorschrift. Letztere zeigt zudem, dass φ sogar R_S-linear ist. Andererseits prüft man leicht nach, dass

$$\psi\colon M_S \longrightarrow M \otimes_R R_S, \qquad \frac{x}{s} \longmapsto x \otimes \frac{1}{s},$$

eine wohldefinierte R-lineare Abbildung ist, die invers zu φ ist, d. h. φ ist ein Isomorphismus.

Nun ist Aussage (i) leicht zu begründen. Sei $\sigma\colon M' \longrightarrow M$ eine Injektion von R-Moduln. Indem wir (ii) anwenden, genügt es zu zeigen, dass die natürliche von σ induzierte Abbildung $\sigma_S\colon M'_S \longrightarrow M_S$, $\frac{x}{s} \longmapsto \frac{\sigma(x)}{s}$ injektiv ist. Sei also $\frac{x}{s}$ ein Element in M'_S, dessen Bild in M_S verschwindet. Dann existiert gemäß der Definition von M_S ein $s'' \in S$ mit $\sigma(s''x) = s''\sigma(x) = 0$. Aus der Injektivität von σ folgt $s''x = 0$ und somit $\frac{x}{s} = 0$, d. h. σ_S ist injektiv. □

Schließlich wollen wir für zwei Ringhomomorphismen $f\colon R \longrightarrow R'$ und $g\colon R \longrightarrow R''$ das Tensorprodukt $R' \otimes_R R''$ betrachten, wobei wir es hier allerdings vorziehen, R' und R'' als *R-Algebren* zu bezeichnen (vgl. Abschnitt 3.3), um auf die explizite Erwähnung der Homomorphismen f und g verzichten zu können. Das Tensorprodukt $R' \otimes_R R''$ ist von links ein R'-Modul und von rechts ein R''-Modul, und wir wollen zeigen, dass $R' \otimes_R R''$ außerdem eine R-Algebra ist. Hierzu werde auf $R' \otimes_R R''$ durch

$$(a \otimes b) \cdot (c \otimes d) = (ac) \otimes (bd)$$

eine Ringmultiplikation erklärt. Um zu zeigen, dass diese wohldefiniert ist, betrachten wir zu einem Element $z = \sum_{i=1}^{r} c_i \otimes d_i \in R' \otimes_R R''$ die Abbildung

$$R' \times R'' \longrightarrow R' \otimes_R R'', \qquad (a, b) \longmapsto a \cdot z \cdot b = \sum_{i=1}^{r} (ac_i) \otimes (bd_i).$$

Diese ist wohldefiniert und R-bilinear, da wir wissen, dass $R' \otimes_R R''$ sowohl ein R'-Modul als auch ein R''-Modul ist. Somit erhalten wir die "Multiplikation" mit z als R-lineare Abbildung

$$R' \otimes_R R'' \longrightarrow R' \otimes_R R'', \qquad a \otimes b \longmapsto a \cdot z \cdot b.$$

Indem wir z variieren lassen, ergibt sich eine Abbildung

$$(R' \otimes_R R'') \times (R' \otimes_R R'') \longrightarrow R' \otimes_R R'',$$

welche durch

$$(a \otimes b, c \otimes d) \longmapsto (ac) \otimes (bd)$$

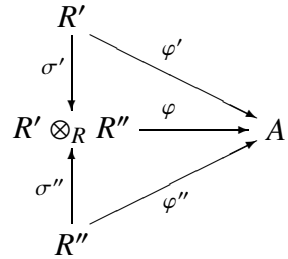
charakterisiert ist und aufgrund der Bilinearitätseigenschaften von Tensoren die Forderungen einer Ringmultiplikation erfüllt. Schließlich definiert man durch $a \longmapsto (a \cdot 1) \otimes 1 = 1 \otimes (a \cdot 1)$ einen Ringhomomorphismus $R \longrightarrow R' \otimes_R R''$, welcher das Tensorprodukt $R' \otimes_R R''$ als R-Algebra erklärt.

Das Tensorprodukt $R' \otimes_R R''$ zweier R-Algebren R' und R'' ist ausgestattet mit den beiden kanonischen R-Algebrahomomorphismen

$$\sigma' \colon R' \longrightarrow R' \otimes_R R'', \qquad a' \longmapsto a' \otimes 1,$$
$$\sigma'' \colon R'' \longrightarrow R' \otimes_R R'', \qquad a'' \longmapsto 1 \otimes a'',$$

welche, wie nachfolgendes Lemma zeigt, das Tensorprodukt $R' \otimes_R R''$ als R-Algebra eindeutig charakterisieren.

Lemma 9. *Die oben genannten Abbildungen $\sigma' \colon R' \longrightarrow R' \otimes_R R''$, $\sigma'' \colon R'' \longrightarrow R' \otimes_R R''$ erfüllen folgende universelle Eigenschaft: Zu je zwei R-Algebrahomomorphismen $\varphi' \colon R' \longrightarrow A$ und $\varphi'' \colon R'' \longrightarrow A$ in eine R-Algebra A gibt es genau einen R-Algebrahomomorphismus $\varphi \colon R' \otimes_R R'' \longrightarrow A$, so dass das Diagramm*



kommutiert. Dabei ist φ charakterisiert durch $a' \otimes a'' \longmapsto \varphi'(a') \cdot \varphi''(a'')$.

Besitzen φ', φ'' die gleiche universelle Eigenschaft wie σ', σ'', so ist φ ein Isomorphismus. Das Tensorprodukt $R' \otimes_R R''$ ist daher als R-Algebra durch die genannte universelle Eigenschaft eindeutig charakterisiert.

Beweis. Um die Eindeutigkeit von φ zu zeigen, betrachte man einen Tensor $a' \otimes a'' \in R' \otimes_R R''$. Es gilt dann

$$\varphi(a' \otimes a'') = \varphi\big((a' \otimes 1) \cdot (1 \otimes a'')\big) = \varphi(a' \otimes 1) \cdot \varphi(1 \otimes a'') = \varphi'(a') \cdot \varphi''(a''),$$

d. h. φ ist eindeutig auf allen Tensoren in $R' \otimes_R R''$ und damit auf ganz $R' \otimes_R R''$. Umgekehrt kann man aber auch die Abbildung

$$R' \times R'' \longrightarrow A, \qquad (a', a'') \longmapsto \varphi'(a') \cdot \varphi''(a''),$$

betrachten. Diese ist R-bilinear und induziert daher eine R-lineare Abbildung $\varphi\colon R' \otimes_R R'' \longrightarrow A$. Dass φ ein R-Algebrahomomorphismus mit den geforderten Eigenschaften ist, rechnet man unmittelbar nach. □

Satz 10. *Es sei R' eine R-Algebra und $\mathfrak{X}$ ein System von Variablen sowie $\mathfrak{a} \subset R[\mathfrak{X}]$ ein Ideal. Dann gibt es kanonische Isomorphismen*

$$\begin{aligned} R[\mathfrak{X}] \otimes_R R' &\xrightarrow{\sim} R'[\mathfrak{X}], & f \otimes a' &\longmapsto a'f, \\ \big(R[\mathfrak{X}]/\mathfrak{a}\big) \otimes_R R' &\xrightarrow{\sim} R'[\mathfrak{X}]\big/\mathfrak{a}R'[\mathfrak{X}], & \overline{f} \otimes a' &\longmapsto \overline{a'f}, \end{aligned}$$

welche durch die angegebenen Abbildungsvorschriften eindeutig charakterisiert sind.

Beweis. Die kanonischen Homomorphismen $\varphi'\colon R[\mathfrak{X}] \longrightarrow R'[\mathfrak{X}]$ und $\varphi''\colon R' \longrightarrow R'[\mathfrak{X}]$ geben aufgrund von Lemma 9 Anlass zu einem R-Algebrahomomorphismus

$$\varphi\colon R[\mathfrak{X}] \otimes_R R' \longrightarrow R'[\mathfrak{X}], \qquad f \otimes a' \longmapsto a'f.$$

Andererseits lässt sich der Ringhomomorphismus $R' \longrightarrow R[\mathfrak{X}] \otimes_R R'$, $a' \longmapsto 1 \otimes a'$, gemäß 2.5/5 durch $\mathfrak{X} \longmapsto \mathfrak{X} \otimes 1$ zu einem Ringhomomorphismus $\psi\colon R'[\mathfrak{X}] \longrightarrow R[\mathfrak{X}] \otimes_R R'$ fortsetzen. Man stellt dann fest, dass ψ invers zu φ ist, dass also φ ein Isomorphismus ist. Die weitere in der Behauptung genannte Isomorphie ergibt sich hieraus unter Benutzung von Satz 5. □

Zum Abschluss wollen wir die gewonnenen Resultate nutzen, um Tensorprodukte von Körpern zu behandeln. Für Körpererweiterungen L/K und K'/K ist das Tensorprodukt $L \otimes_K K'$ im Allgemeinen jedoch kein Körper mehr; vgl. etwa Aufgabe 7. Dennoch ist $L \otimes_K K'$ eine von Null verschiedene K-Algebra, die L und K' als Unteralgebren enthält. Die kanonischen Abbildungen

$$L \simeq L \otimes_K K \longrightarrow L \otimes_K K', \qquad K' \simeq K \otimes_K K' \longrightarrow L \otimes_K K'$$

sind aufgrund der Flachheit von L/K und K'/K injektiv.

Bemerkung 11. *Es sei K'/K eine Körpererweiterung und $f \in K[X]$ ein Polynom einer Variablen X. Dann gilt*

$$\big(K[X]/fK[X]\big) \otimes_K K' \simeq K'[X]\big/fK'[X].$$

Ist weiter $f = p_1^{\nu_1} \dots p_r^{\nu_r}$ eine Primfaktorzerlegung in $K'[X]$ mit paarweise nicht-assoziierten Primpolynomen $p_i \in K'[X]$, so folgt

$$\big(K[X]/fK[X]\big) \otimes_K K' \simeq \prod_{i=1}^{r} K'[X]\big/p_i^{\nu_i}K'[X].$$

Beweis. Man benutze Satz 10 in Verbindung mit dem Chinesischen Restsatz 2.4/14. □

Ist L/K eine einfache algebraische Körpererweiterung, etwa $L = K(a)$ mit Minimalpolynom $f \in K[X]$ zu a, und ist K'/K irgendeine Körpererweiterung, so ergibt sich in der Situation von Bemerkung 11, dass

$$K(a) \otimes_K K' \simeq K'[X]\big/fK'[X] \simeq \prod_{i=1}^{r} K'[X]\big/p_i^{\nu_i}K'[X]$$

genau dann wieder ein Körper ist, wenn f über K' irreduzibel ist. Im Allgemeinen wird $K(a) \otimes_K K'$ jedoch Nullteiler besitzen und sogar nicht-triviale nilpotente Elemente haben, d. h. Elemente $z \neq 0$, zu denen es einen Exponenten $n \in \mathbb{N}$ mit $z^n = 0$ gibt. Es enthält $K(a) \otimes_K K'$ genau dann von Null verschiedene nilpotente Elemente, wenn mindestens einer der obigen Exponenten ν_i größer als 1 ist. Dies bedeutet insbesondere, dass f in diesem Fall kein separables Polynom sein kann.

Bemerkung 12. *Es sei K ein Körper und $K(\mathfrak{X})/K$ eine rein transzendente Körpererweiterung mit erzeugender Transzendenzbasis $\mathfrak{X}$. Dann gibt es zu jeder Körpererweiterung K'/K kanonische Homomorphismen*

$$K(\mathfrak{X}) \otimes_K K' \xrightarrow{\sim} K'[\mathfrak{X}]_S \hookrightarrow K'(\mathfrak{X})$$

wobei $K'[\mathfrak{X}]_S$ die Lokalisierung des Polynomrings $K'[\mathfrak{X}]$ nach dem multiplikativen System $S = K[\mathfrak{X}] - \{0\}$ bezeichnet. Insbesondere ist $K(\mathfrak{X}) \otimes_K K'$ ein Integritätsring.

Beweis. Wir fassen $K(\mathfrak{X})$ als Lokalisierung $K[\mathfrak{X}]_S$ des Polynomrings $K[\mathfrak{X}]$ nach dem multiplikativen System $S = K[\mathfrak{X}] - \{0\}$ auf. Mit Satz 10 gilt $K[\mathfrak{X}] \otimes_K K' \simeq K'[\mathfrak{X}]$, sowie nach Bemerkung 7 und Satz 8

$$\begin{aligned} K(\mathfrak{X}) \otimes_K K' &\simeq K[\mathfrak{X}]_S \otimes_K K' \\ &\simeq K[\mathfrak{X}]_S \otimes_{K[\mathfrak{X}]} \left(K[\mathfrak{X}] \otimes_K K'\right) \\ &\simeq K[\mathfrak{X}]_S \otimes_{K[\mathfrak{X}]} K'[\mathfrak{X}] \\ &\simeq K'[\mathfrak{X}]_S. \end{aligned}$$

Es ist somit $K(\mathfrak{X}) \otimes_K K'$ als Unterring des Quotientenkörpers von $K'[\mathfrak{X}]$ ein Integritätsring. □

Wir wollen nun noch auf eine Eigenschaft von Tensorprodukten eingehen, die es in vielen Fällen erlaubt, gewisse Endlichkeitsbedingungen zu realisieren. Es handelt sich um die Verträglichkeit von Tensorprodukten mit direkten Limiten, vgl. Aufgabe 8, eine Eigenschaft, die wir an dieser Stelle der Einfachheit halber nur in einem Spezialfall formulieren.

Lemma 13. *Es seien A und A' Algebren über einem Körper K. Für Unteralgebren $A_0 \subset A$ und $A'_0 \subset A'$ ist dann $A_0 \otimes_K A'_0$ in kanonischer Weise eine Unteralgebra von $A \otimes_K A'$. Sind weiter $(A_i)_{i\in I}$, $(A'_j)_{j\in J}$ gerichtete[2] Systeme von Unteralgebren von A bzw. A' mit $A = \bigcup_{i\in I} A_i$ und $A' = \bigcup_{j\in J} A'_j$, so ist $(A_i \otimes_K A'_j)_{i\in I, j\in J}$ ein gerichtetes System von Unteralgebren von $A \otimes_K A'$ mit*

$$A \otimes_K A' = \bigcup_{i\in I, j\in J} (A_i \otimes_K A'_j).$$

[2] *Gerichtet* bedeutet für das System $(A_i)_{i\in I}$, dass zu $i, i' \in I$ stets ein $k \in I$ mit $A_i \cup A_{i'} \subset A_k$ existiert, entsprechend für die übrigen Systeme; vgl. auch 4.2.

Beweis. Die Inklusionen $A_0 \hookrightarrow A$ und $A'_0 \hookrightarrow A'$ induzieren aufgrund der Flachheit von K-Algebren Injektionen

$$A_0 \otimes_K A'_0 \hookrightarrow A_0 \otimes_K A' \hookrightarrow A \otimes_K A'.$$

Insbesondere folgt daher für $i \in I$, $j \in J$, dass die Tensorprodukte $A_i \otimes_K A'_j$ Unteralgebren von $A \otimes_K A'$ sind. Sei nun $z \in A \otimes_K A'$. Dann ist z darstellbar als endliche Summe $z = \sum_{\rho=1}^{r} x_\rho \otimes y_\rho$ mit $x_\rho \in \bigcup_{i\in I} A_i$ und $y_\rho \in \bigcup_{j\in J} A'_j$. Da $(A_i)_{i\in I}$ und $(A'_j)_{j\in J}$ gerichtet sind, gibt es Indizes $i \in I$, $j \in J$ mit $x_1, \ldots, x_r \in A_i$ und $y_1, \ldots, y_r \in A'_j$, d. h. es gilt $z \in A_i \otimes_K A'_j$. □

Als Beispiel betrachte man zu zwei Körpererweiterungen L/K und L'/K jeweils die gerichteten Systeme $(L_i)_{i\in I}$ bzw. $(L'_j)_{j\in J}$ aller über K *endlich* erzeugten Teilkörper $L_i \subset L$ bzw. $L'_j \subset L'$. Dann gilt $L \otimes_K L' = \bigcup_{i\in I, j\in J}(L_i \otimes_K L'_j)$ aufgrund von Lemma 13. Möchte man nun eine gewisse Eigenschaft wie etwa die Nullteilerfreiheit für $L \otimes_K L'$ beweisen, so sieht man, dass $L \otimes_K L'$ genau dann nullteilerfrei ist, wenn alle $L_i \otimes_K L'_j$ dies sind. Auf diese Weise kann man die Behandlung beliebiger Körpererweiterungen auf den Fall endlich erzeugter Körpererweiterungen zurückführen. Wir werden von dieser Möglichkeit im nachfolgenden Abschnitt mehrfach Gebrauch machen.

Lernkontrolle und Prüfungsvorbereitung

R sei stets ein Ring.

1. Es seien M und N zwei R-Moduln. Was versteht man unter einer R-bilinearen Abbildung $M \times N \longrightarrow E$ in einen R-Modul E? Wie ist das Tensorprodukt $M \otimes_R N$ definiert? Welche Elemente eines Tensorprodukts werden als Tensoren bezeichnet?
2. Beweise, dass das Tensorprodukt zweier R-Moduln stets existiert.
3. Erkläre und verifiziere für R-Moduln M, N und P die kanonischen Isomorphismen $R \otimes_R M \simeq M$, $M \otimes_R N \simeq N \otimes_R M$ und $(M \otimes_R N) \otimes_R P \simeq M \otimes_R (N \otimes_R P)$.
4. Zeige, dass das Tensorprodukt von R-Moduln mit der Bildung direkter Summen verträglich ist.
5. Es sei $M' \longrightarrow M \longrightarrow M'' \longrightarrow 0$ eine exakte Sequenz von R-Moduln. Zeige, dass man durch Tensorieren mit einem R-Modul N hieraus wiederum eine exakte Sequenz von R-Moduln erhält.

6. Was versteht man unter einem flachen R-Modul? Nenne einige Beispiele für flache R-Moduln und für solche, die nicht flach sind.
7. Sei $R \longrightarrow R'$ ein Ringhomomorphismus. Wie lassen sich für einen gegebenen R-Modul M die Koeffizienten aus R zu Koeffizienten aus R' erweitern?
8. Es seien $R \longrightarrow R' \longrightarrow R''$ Ringhomomorphismen. Erkläre und verifiziere für einen gegebenen R-Modul M den kanonischen Isomorphismus von R''-Moduln $(M \otimes_R R') \otimes_{R'} R'' \xrightarrow{\sim} M \otimes_R R''$.
9. Betrachte zu einem multiplikativen System $S \subset R$ die Lokalisierung R_S von R und zeige, dass R_S ein flacher R-Modul ist. Erkläre und verifiziere für einen R-Modul M und seine Lokalisierung M_S nach S den kanonischen Isomorphismus $M \otimes_R R_S \xrightarrow{\sim} M_S$.
10. Erkläre den Begriff einer R-Algebra. Zeige, dass das Tensorprodukt zweier R-Algebren in kanonischer Weise wieder eine R-Algebra ist. Durch welche universelle Eigenschaft ist das Tensorprodukt zweier R-Algebren charakterisiert (mit Begründung)?
11. Sei R' eine R-Algebra und $\mathfrak{X}$ ein System von Variablen. Erkläre und verifiziere den kanonischen Isomorphismus $R[\mathfrak{X}] \otimes_R R' \xrightarrow{\sim} R'[\mathfrak{X}]$, sowie dessen Verträglichkeit bezüglich Restklassenbildung nach Idealen $\mathfrak{a} \subset R[\mathfrak{X}]$.
12. Es sei L/K eine rein transzendente Körpererweiterung. Zeige, dass das Tensorprodukt $L \otimes_K K'$ ein Integritätsring ist. Für eine weitergehende Aussage siehe Aufgabe 7.
13. Erläutere und begründe für Algebren über einem Körper K die Verträglichkeit von Tensorprodukten des Typs $A \otimes_K A'$ mit dem direkten Limes über aufsteigende gerichtete Systeme von Unteralgebren in A und A'.

Übungsaufgaben

R sei stets ein Ring.

1. *Betrachte für eine R-Algebra R' und einen R-Modul M das Tensorprodukt $M \otimes_R R'$ und zeige, dass dieses als R'-Modul, zusammen mit der R-linearen Abbildung $\tau\colon M \longrightarrow M \otimes_R R'$, $x \longmapsto x \otimes 1$, eindeutig durch folgende universelle Eigenschaft charakterisiert ist: Zu jeder R-linearen Abbildung $\Phi\colon M \longrightarrow E$ in einen R'-Modul E gibt es genau eine R'-lineare Abbildung $\varphi\colon M \otimes_R R' \longrightarrow E$ mit $\Phi = \varphi \circ \tau$.*
2. *Beweise die Existenz des Tensorprodukts $R' \otimes_R R''$ zweier R-Algebren in direkter Weise, und zwar durch Konstruktion einer R-Algebra T, die der universellen Eigenschaft aus Lemma 9 genügt.*

3. Es sei R' eine R-Algebra. Zeige: Ist M ein flacher R-Modul, so ist $M \otimes_R R'$ als R'-Modul flach.

4. Es sei M ein R-Modul. Zeige:
   (i) Ist M flach und ist $a \in R$ kein Nullteiler in R, so folgt aus einer Gleichung $ax = 0$ mit $x \in M$ stets $x = 0$.
   (ii) Ist R ein Hauptidealring, so ist M genau dann ein flacher R-Modul, wenn M *torsionsfrei* ist, d. h. wenn aus $ax = 0$ mit $a \in R$, $x \in M$ stets $a = 0$ oder $x = 0$ folgt.

5. Betrachte zwei R-Algebren R', R'' sowie zwei Ideale $\mathfrak{a}' \subset R'$, $\mathfrak{a}'' \subset R''$ und zeige $(R'/\mathfrak{a}') \otimes_R (R''/\mathfrak{a}'') \simeq (R' \otimes_R R'')/(\mathfrak{a}', \mathfrak{a}'')$. Dabei sei $(\mathfrak{a}', \mathfrak{a}'')$ das von den Bildern $\sigma'(\mathfrak{a}')$ und $\sigma''(\mathfrak{a}'')$ unter den kanonischen R-Algebrahomomorphismen $\sigma' \colon R' \longrightarrow R' \otimes_R R''$, $\sigma'' \colon R'' \longrightarrow R' \otimes_R R''$ erzeugte Ideal.

6. Betrachte zu einer normalen algebraischen Körpererweiterung L/K der Charakteristik $p > 0$ gemäß 3.7/4 und 3.7/5 den separablen Abschluss K_s sowie den rein inseparablen Abschluss K_i von K in L und zeige, dass die kanonische Abbildung $K_s \otimes_K K_i \longrightarrow L$, $a \otimes b \longmapsto ab$, ein Isomorphismus ist.

7. Es seien L/K und K'/K endlich erzeugte Körpererweiterungen, wobei L/K rein transzendent von einem Transzendenzgrad > 0 sei. Zeige: $L \otimes_K K'$ ist genau dann ein Körper, wenn die Erweiterung K'/K algebraisch ist.

8. Es seien $(M_i)_{i \in I}$, $(N_i)_{i \in I}$ zwei induktive Systeme von R-Moduln (vgl. Abschnitt 4.2). Zeige, dass $(M_i \otimes_R N_i)_{i \in I}$ in natürlicher Weise ein induktives System von R-Moduln bildet und dass es einen kanonischen Isomorphismus von R-Moduln

$$(\varinjlim M_i) \otimes_R (\varinjlim N_i) \xrightarrow{\sim} \varinjlim (M_i \otimes_R N_i)$$

   gibt.

7.3 Separable, primäre und reguläre Erweiterungen*

In diesem Abschnitt sollen gewisse Typen von nicht notwendig algebraischen Körpererweiterungen studiert werden, die sich mittels Tensorprodukten charakterisieren lassen. Wir beginnen mit separablen Körpererweiterungen und erinnern zunächst daran, dass das *Radikal* $\operatorname{rad} R$ eines Ringes R aus allen Elementen $z \in R$ besteht, zu denen es ein $n \in \mathbb{N}$ mit $z^n = 0$ gibt. Man nennt R *reduziert*, wenn $\operatorname{rad} R = 0$ gilt.

Bemerkung 1. *Es sei L/K eine* algebraische *Körpererweiterung. Dann ist äquivalent*:

(i) *Es ist L/K separabel im Sinne von Definition* 3.6/3.

(ii) *Für jede Körpererweiterung K'/K ist $L \otimes_K K'$ reduziert.*

Beweis. Sei zunächst L/K als separabel vorausgesetzt. Unter Benutzung von 7.2/13 dürfen wir annehmen, dass die Erweiterung L/K endlich erzeugt und somit von endlichem Grad ist. Dann gibt es aufgrund des Satzes vom primitiven Element 3.6/12 ein $a \in L$ mit $L = K(a)$, und es folgt mit 7.2/11 aus der Separabilität von a über K, dass $L \otimes_K K'$ für jede Erweiterung K'/K reduziert ist. Dies zeigt, dass (ii) aus (i) folgt. Sei nun umgekehrt (ii) gegeben, wobei wir K' speziell als einen algebraischen Abschluss von K wählen. Sei $a \in L$. Da K'/K flach ist, ergibt die Inklusion $K(a) \hookrightarrow L$ eine Inklusion $K(a) \otimes_K K' \hookrightarrow L \otimes_K K'$, so dass $K(a) \otimes_K K'$ reduziert ist. Dann hat aber das Minimalpolynom von a über K gemäß 7.2/11 lediglich einfache Nullstellen, und es folgt, dass a separabel über K ist. Indem man diesen Schluss für jedes $a \in L$ durchführt, sieht man, dass L/K separabel ist. □

Da die Bedingung (ii) in Bemerkung 1 auch für nicht-algebraische Erweiterungen L/K sinnvoll ist, können wir die Separabilität beliebiger Körpererweiterungen wie folgt erklären:

Definition 2. *Eine Körpererweiterung L/K heißt* separabel, *wenn für jede Körpererweiterung K'/K das Tensorprodukt $L \otimes_K K'$ reduziert ist.*

Bemerkung 1 besagt also mit anderen Worten, dass eine Körpererweiterung L/K genau dann separabel im Sinne von 3.6/3 ist, wobei dann L/K als *algebraisch* vorauszusetzen ist, wenn sie separabel im Sinne von Definition 2 ist. Als prominentes Beispiel einer Klasse separabler nicht-algebraischer Erweiterungen können wir vermerken:

Bemerkung 3. *Jede rein transzendente Körpererweiterung L/K ist separabel.*

Beweis. Man benutze 7.2/12. □

Als Nächstes wollen wir einige einfache Eigenschaften separabler Körpererweiterungen zusammenstellen.

Satz 4. *Es sei M/K eine Körpererweiterung.*

(i) *Ist M/K separabel, so ist für jeden Zwischenkörper L zu M/K auch die Erweiterung L/K separabel.*[3]

(ii) *M/K ist genau dann separabel, wenn L/K für alle über K endlich erzeugten Zwischenkörper $L \subset M$ separabel ist.*

(iii) *Sind für einen Zwischenkörper L zu M/K die Erweiterungen M/L und L/K separabel, so auch M/K.*

Beweis. Sei M/K separabel. Ist dann K'/K eine beliebige Körpererweiterung, so induziert die Inklusion $L \hookrightarrow M$ aufgrund der Flachheit von K'/K eine Inklusion $L \otimes_K K' \hookrightarrow M \otimes_K K'$, und man sieht, dass mit $M \otimes_K K'$ auch $L \otimes_K K'$ reduziert ist. Aus der Separabilität von M/K folgt also diejenige von L/K. Weiter folgt aus 7.2/13, dass M/K genau dann separabel ist, wenn L/K für alle über K endlich erzeugten Zwischenkörper separabel ist. Damit sind die Behauptungen (i) und (ii) klar.

Um die Behauptung (iii) zu verifizieren, nehmen wir M/L und L/K als separabel an. Sei wiederum K'/K eine beliebige Körpererweiterung. Es ist dann $R = L \otimes_K K'$ von Null verschieden und reduziert. Wir benötigen als Hilfsresultat, dass das Nullideal in R Durchschnitt von Primidealen ist. Um dies einzusehen, betrachte man ein Element $s \neq 0$ in R sowie das von s erzeugte multiplikative System $S = \{s^0, s^1, \ldots\}$. Da R reduziert ist, gilt $0 \notin S$. Indem man wie im Beweis zu 3.4/6 vorgeht, konstruiert man mit Hilfe des Lemmas von Zorn 3.4/5 ein Ideal $\mathfrak{p} \subset R$, welches maximal mit der Bedingung $\mathfrak{p} \cap S = \emptyset$ ist und stellt fest, dass $\mathfrak{p}$ ein Primideal ist. Es gibt also zu jedem $s \neq 0$ ein Primideal $\mathfrak{p} \subset R$ mit $s \notin \mathfrak{p}$, d. h. das Nullideal in R ist Durchschnitt von Primidealen, etwa $0 = \bigcap_{j \in J} \mathfrak{p}_j$.

Für $j \in J$ sei Q_j der Quotientenkörper zu $R/\mathfrak{p}_j$. Dann induzieren die kanonischen Homomorphismen $R \longrightarrow R/\mathfrak{p}_j \hookrightarrow Q_j$ für $j \in J$ eine Injektion $R \hookrightarrow \prod_{j \in J} Q_j$ sowie aufgrund der Flachheit von M/L eine Injektion $M \otimes_L R \hookrightarrow M \otimes_L \prod_{j \in J} Q_j$. Wir benutzen nun, dass die Abbildung

[3] Man beachte, dass M/L nicht notwendig separabel ist, wenn dies für M/K gilt; vgl. Aufgabe 1.

$$(*) \qquad M \otimes_L \prod_{j\in J} Q_j \longrightarrow \prod_{j\in J}(M \otimes_L Q_j), \quad x \otimes (q_j)_{j\in J} \longmapsto (x \otimes q_j)_{j\in J},$$

injektiv ist, eine Eigenschaft, die wir weiter unten noch gesondert zeigen werden. Da wegen der Separabilität von M/L die Tensorprodukte $M \otimes_L Q_j$ sämtlich reduziert sind, ergibt sich die Reduziertheit von $M \otimes_L R$ und unter Benutzung des Isomorphismus

$$M \otimes_L R = M \otimes_L (L \otimes_K K') \xrightarrow{\sim} M \otimes_K K'$$

aus 7.2/7 auch die Reduziertheit von $M \otimes_K K'$, so dass insgesamt die Separabilität von M/K folgt.

Um nun die Injektivität der Abbildung $(*)$ nachzuweisen, benutzen wir, dass M eine L-Vektorraumbasis $(y_i)_{i\in I}$ besitzt. Da Tensorprodukte mit direkten Summen kommutieren, vgl. 7.2/4, schreibt sich jedes Element $z \in M \otimes_L \prod_{j\in J} Q_j$ in der Form $z = \sum_{i\in I} y_i \otimes (q_{ij})_{j\in J}$ mit eindeutig bestimmten Elementen $q_{ij} \in Q_j$, wobei fast alle Terme in dieser Summe verschwinden. Letzteres bedeutet, dass es nur für endlich viele $i \in I$ Indizes $j \in J$ mit $q_{ij} \neq 0$ gibt. In ähnlicher Weise können wir Elemente aus $\prod_{j\in J}(M \otimes_L Q_j)$ eindeutig als Familien von endlichen Summen $\sum_{i\in I} y_i \otimes q_{ij}$, $j \in J$, schreiben, also von Summen mit nur endlich vielen von Null verschiedenen Termen. Dies bedeutet, dass es zu jedem $j \in J$ höchstens endlich viele Indizes $i \in I$ mit $q_{ij} \neq 0$ gibt. Nehmen wir insbesondere I und J als unendlich an, so kann man Elemente $(\sum_{i\in I} y_i \otimes q_{ij})_{j\in J}$ in $\prod_{j\in J}(M \otimes_L Q_j)$ konstruieren mit der Eigenschaft, dass $q_{ij} \neq 0$ für unendlich viele Indizes $i \in I$ gilt, sowie für gewisse Indizes $j \in J$, die jeweils von i abhängen. Da die Abbildung $(*)$ ein Element der Form $\sum_{i\in I} y_i \otimes (q_{ij})_{j\in J}$ auf das Element $(\sum_{i\in I} y_i \otimes q_{ij})_{j\in J}$ abbildet, sieht man, dass $(*)$ stets injektiv, im Allgemeinen aber nicht surjektiv ist. □

Definition 5. *Eine Körpererweiterung L/K heißt* separabel erzeugt, *wenn es eine Transzendenzbasis $\mathfrak{X}$ von L/K gibt, so dass L separabel* (*algebraisch*) *über $K(\mathfrak{X})$ ist. In diesem Fall heißt $\mathfrak{X}$ eine* separierende Transzendenzbasis *von L/K.*

Da jede Körpererweiterung L/K eine Transzendenzbasis besitzt, vgl. 7.1/3, sieht man, dass Körpererweiterungen im Falle $\operatorname{char} K = 0$ stets separabel erzeugt sind. Weiter folgert man aus Satz 4 (iii) in Verbindung mit Bemerkung 3 unmittelbar:

Korollar 6. *Jede separabel erzeugte Körpererweiterung L/K, insbesondere also jede Körpererweiterung in Charakteristik* 0, *ist separabel.*

Unser nächstes Ziel ist es, für endlich erzeugte Körpererweiterungen die Umkehrung zu beweisen. Hierzu erinnern wir daran, dass man zu einem Körper K der Charakteristik $p > 0$ den Körper $K^{p^{-i}}$ aller p^i-ten Wurzeln aus Elementen von K bilden kann. Man hat dann kanonische Inklusionen

$$K = K^{p^{-0}} \subset K^{p^{-1}} \subset K^{p^{-2}} \subset \ldots,$$

und es ist $K^{p^{-\infty}} = \bigcup_{i=0}^{\infty} K^{p^{-i}}$ der rein inseparable Abschluss von K, ein Körper, der vollkommen und rein inseparabel über K ist; vgl. Aufgabe 6 aus Abschnitt 3.7.

Satz 7. *Es sei K ein Körper der Charakteristik $p > 0$ sowie L ein Erweiterungskörper. Dann ist äquivalent*:

(i) *L/K ist separabel.*

(ii) *$L \otimes_K K^{p^{-\infty}}$ ist reduziert.*

(iii) *Für jede endliche Körpererweiterung K'/K mit $K' \subset K^{p^{-1}}$ ist $L \otimes_K K'$ reduziert.*

(iv) *Sind $a_1, \ldots, a_r \in L$ linear unabhängig über K, so auch die Elemente $a_1^p, \ldots, a_r^p$.*

(v) *Jeder über K endlich erzeugte Teilkörper $L' \subset L$ ist separabel über K erzeugt.*

Ist L/K endlich erzeugt, etwa $L = K(x_1, \ldots, x_n)$, so lässt sich im Falle der Separabilität das System der x_i zu einer separierenden Transzendenzbasis von L/K verkleinern.

Beweis. Die Implikation (i) $\Longrightarrow$ (ii) ist trivial. Weiter folgt die Implikation (ii) $\Longrightarrow$ (iii) aus der Flachheit von L/K, da in der Situation von (iii) jedes K' ein Teilkörper von $K^{p^{-\infty}}$ und somit $L \otimes_K K'$ ein Unterring von $L \otimes_K K^{p^{-\infty}}$ ist.

Zum Nachweis von (iii) $\Longrightarrow$ (iv) betrachte man über K linear unabhängige Elemente $a_1, \ldots, a_r \in L$ sowie Elemente $c_1, \ldots, c_r \in K$ mit $\sum_{i=1}^r c_i a_i^p = 0$. Dann kann man jeweils die p-te Wurzel $c_i^{p^{-1}} \in K^{p^{-1}}$ zu c_i bilden sowie den Körper $K' = K(c_1^{p^{-1}}, \ldots, c_r^{p^{-1}}) \subset K^{p^{-1}}$ erklären. Dieser ist endlich über K. Man setze nun $z = \sum_{i=1}^r a_i \otimes c_i^{p^{-1}} \in L \otimes_K K'$. Da

$$z^p = \sum_{i=1}^{r} a_i^p \otimes c_i = \sum_{i=1}^{r} (c_i a_i^p) \otimes 1 = \Big(\sum_{i=1}^{r} c_i a_i^p\Big) \otimes 1 = 0$$

gilt und $L \otimes_K K'$ reduziert ist, erhält man $z = 0$. Nun sind aber die Elemente $a_1 \otimes 1, \ldots, a_r \otimes 1$ in $L \otimes_K K'$ linear unabhängig über K', denn $(\bigoplus_{i=1}^{r} Ka_i) \otimes_K K'$ ist aufgrund der Flachheit von K'/K ein Untervektorraum von $L \otimes_K K'$, und es gilt

$$\Big(\bigoplus_{i=1}^{r} Ka_i\Big) \otimes_K K' \xrightarrow{\sim} \bigoplus_{i=1}^{r} (Ka_i \otimes_K K')$$

aufgrund von 7.2/4. Somit folgt aus $z = 0$, dass alle Koeffizienten $c_i^{p^{-1}}$ bzw. alle c_i verschwinden, und man sieht, dass $a_1^p, \ldots, a_r^p$ linear unabhängig über K sind.

Sei nun Bedingung (iv) erfüllt. Um (v) hieraus abzuleiten, dürfen wir L/K als endlich erzeugt annehmen, etwa $L = K(x_1, \ldots, x_n)$. Wir zeigen mit Induktion nach n, dass L/K separabel erzeugt ist. Der Induktionsanfang $n = 0$ ist trivial. Sei also im Folgenden $n > 0$. Wir betrachten ein maximales über K algebraisch unabhängiges Teilsystem von $x_1, \ldots, x_n$, etwa $x_1, \ldots, x_t$ mit $t \leq n$. Dann bildet $x_1, \ldots, x_t$ eine Transzendenzbasis von L/K. Im Falle $n = t$ ist nichts zu zeigen. Sei also $t < n$, und sei $f \in K[X_1, \ldots, X_{t+1}]$ ein nicht-triviales Polynom minimalen Gesamtgrades d mit $f(x_1, \ldots, x_{t+1}) = 0$. Falls nun f sogar ein Polynom in $X_1^p, \ldots, X_{t+1}^p$ ist, so ist f von der Form $f = \sum_{\nu \in I} c_\nu (X^p)^\nu$ mit Koeffizienten $c_\nu \in K$ und einer endlichen Indexmenge $I \subset \mathbb{N}^{t+1}$, wobei wir $c_\nu \neq 0$ für alle $\nu \in I$ annehmen wollen. Die p-ten Potenzen $(x_1^{\nu_1})^p \ldots (x_{t+1}^{\nu_{t+1}})^p$, $\nu \in I$, sind also linear abhängig über K, und Gleiches gilt gemäß (iv) auch für die Monome $x_1^{\nu_1} \ldots x_{t+1}^{\nu_{t+1}}$. Wir erhalten daher eine Relation $g(x_1, \ldots, x_{t+1}) = 0$ mit einem nicht-trivialen Polynom $g \in K[X_1, \ldots, X_{t+1}]$, dessen Gesamtgrad $< d$ ist. Dies ist aber nach Wahl von d ausgeschlossen, so dass notwendig $f \notin K[X_1^p, \ldots, X_{t+1}^p]$ folgt. Es existiert daher eine Variable X_i mit der Eigenschaft, dass f kein Polynom in X_i^p ist. Somit ist $h = f(x_1, \ldots, x_{i-1}, X_i, x_{i+1}, \ldots, x_{t+1})$ ein nicht-triviales Polynom in X_i mit Koeffizienten in $K[x_1, \ldots, x_{i-1}, x_{i+1}, \ldots, x_{t+1}]$, welches x_i annulliert und dessen Ableitung nicht identisch verschwindet. Als Konsequenz sieht man, dass L algebraisch über $K(x_1, \ldots, x_{i-1}, x_{i+1}, \ldots, x_{t+1})$ ist, und wegen $\mathrm{transgrad}_K(L) = t$, dass $x_1, \ldots, x_{i-1}, x_{i+1}, \ldots, x_{t+1}$ eine Transzendenzbasis von L/K bilden, also insbesondere algebraisch unabhängig über K sind. Aufgrund der Minimalität des Grades von f ist h

als Polynom mit Koeffizienten in $K[x_1, \ldots, x_{i-1}, x_{i+1}, \ldots, x_{t+1}]$ irreduzibel und primitiv. Da der Polynomring in X_i über diesem Koeffizientenbereich nach 2.7/3 faktoriell ist, ist h prim und somit auch ein Primelement in $K(x_1, \ldots, x_{i-1}, x_{i+1}, \ldots, x_{t+1})[X_i]$; vgl. 2.7/7. Da außerdem die Ableitung von h nicht verschwindet, ist h nach 3.6/1 separabel. Somit ist x_i separabel algebraisch über dem Körper $K(x_1, \ldots, x_{i-1}, x_{i+1}, \ldots, x_{t+1})$ und damit insbesondere separabel algebraisch über $K(x_1, \ldots, x_{i-1}, x_{i+1}, \ldots, x_n)$. Letzterer Körper ist nun nach Induktionsvoraussetzung über K separabel erzeugt, so dass dann auch $L = K(x_1, \ldots, x_n)$ insgesamt über K separabel erzeugt ist. Dies beendet den Nachweis der Implikation (iv) $\Longrightarrow$ (v). Das beschriebene Verfahren zeigt insbesondere, dass man für $L = K(x_1, \ldots, x_n)$ das System der x_i zu einer separierenden Transzendenzbasis von L/K verkleinern kann.

Die Implikation (v) $\Longrightarrow$ (i) schließlich ergibt sich aus Satz 4 (ii) und Korollar 6. □

Ist K in der Situation von Satz 7 bereits vollkommen, so gestattet K keine echten rein inseparablen Körpererweiterungen, d. h. es gilt $K = K^{p^{-\infty}}$. In Verbindung mit Korollar 6 ergibt sich daher:

Korollar 8. *Jede Körpererweiterung L/K eines vollkommenen Körpers K ist separabel.*

Als Nächstes wollen wir zwei weitere Klassen von Körpererweiterungen betrachten, die *primären* und die *regulären* Körpererweiterungen, wobei man die primären Erweiterungen als eine Verallgemeinerung rein inseparabler algebraischer Erweiterungen deuten kann; man benutze etwa die unten in Satz 13 gegebene Charakterisierung primärer Erweiterungen. Wir nennen einen Ring R *irreduzibel*, wenn sein Radikal $\operatorname{rad} R$ ein Primideal ist.

Definition 9. *Eine Körpererweiterung L/K heißt* primär (*bzw.* regulär), *wenn für jede beliebige Körpererweiterung K'/K das Tensorprodukt $L \otimes_K K'$ irreduzibel* (*bzw. ein Integritätsring*) *ist.*[4] *Die Erweiterung L/K ist also genau dann regulär, wenn sie separabel und primär ist.*[5]

[4] In der Literatur wird eine Körpererweiterung L/K meist dann als primär bezeichnet, wenn K separabel abgeschlossen in L ist. Diese Bedingung ist äquivalent zu der hier gegebenen, vgl. Satz 13.

[5] Man benutze, dass ein Ring genau dann ein Integritätsring ist, wenn sein Nullideal prim ist.

Dass in Charakteristik $p > 0$ zumindest einfache rein inseparable Erweiterungen L/K Beispiele primärer Körpererweiterungen sind, lässt sich leicht aus 7.2/11 ablesen. Gilt nämlich $L = K(a)$ und ist $f = X^{p^r} - c \in K[X]$ das Minimalpolynom von a über K, so folgt $L \otimes_K K' \simeq K'[X]/(f)$. Über einem algebraischen Abschluss $\overline{K}'$ zu K' besitzt f die Zerlegung $f = (X-a)^{p^r}$, wobei wir a mit der entsprechenden Nullstelle von f in $\overline{K}'$ identifiziert haben. Es folgt dann $\mathrm{rad}(\overline{K}'[X]/(f)) = (X-a)/(f)$, so dass $\mathrm{rad}(L \otimes_K \overline{K}')$ prim ist. Da aber die Inklusion $K' \hookrightarrow \overline{K}'$ aufgrund der Flachheit von L/K eine Injektion $L \otimes_K K' \hookrightarrow L \otimes_K \overline{K}'$ induziert, sieht man, dass mit $\mathrm{rad}(L \otimes_K \overline{K}')$ auch dessen Schnitt mit $L \otimes_K K'$, also das Radikal von $L \otimes_K K'$ prim ist. Letzteres bedeutet, dass L/K primär ist.

Ähnlich wie für separable Körpererweiterungen wollen wir einige elementare Eigenschaften primärer und regulärer Körpererweiterungen zusammenstellen.

Bemerkung 10. *Jede rein transzendente Körpererweiterung L/K ist regulär und damit insbesondere primär.*

Beweis. Man benutze 7.2/12. □

Satz 11. *Es sei M/K eine Körpererweiterung.*

(i) *Ist M/K primär (bzw. regulär), so ist für jeden Zwischenkörper L zu M/K die Erweiterung L/K primär (bzw. regulär).*

(ii) *M/K ist genau dann primär (bzw. regulär), wenn L/K für alle über K endlich erzeugten Zwischenkörper $L \subset M$ primär (bzw. regulär) ist.*

(iii) *Sind für einen Zwischenkörper L zu M/K die Erweiterungen M/L und L/K primär (bzw. regulär), so auch M/K.*

Beweis. Die Eigenschaft regulär ist für Körpererweiterungen als Kombination von separabel und primär erklärt. Somit dürfen wir uns auf primäre Erweiterungen beschränken, denn die behaupteten Aussagen wurden in Satz 4 bereits für separable Erweiterungen bewiesen. Ist L ein Zwischenkörper zu M/K sowie K' ein beliebiger Erweiterungskörper von K, so induziert die Inklusion $L \hookrightarrow M$ eine Injektion $L \otimes_K K' \hookrightarrow M \otimes_K K'$, denn K'/K ist flach. Da für jede Ringerweiterung $R \subset R'$ und jedes Primideal $\mathfrak{p}' \subset R'$ der Schnitt $R \cap \mathfrak{p}'$ ein Primideal in R ist und da $\mathrm{rad}\, R = R \cap \mathrm{rad}\, R'$ gilt, sieht man unmittelbar, dass mit M/K auch L/K primär ist. Ist umgekehrt L/K

für jeden über K endlich erzeugten Zwischenkörper L zu M/K primär, so folgt unter Benutzung von 7.2/13, dass auch M/K primär ist. Die Aussagen (i) und (ii) sind somit klar.

Zum Nachweis von (iii) betrachte man einen Zwischenkörper L zu M/K und nehme die Erweiterungen M/L und L/K als primär an. Für eine beliebige Körpererweiterung K'/K ist sodann $R = (L \otimes_K K')/\mathrm{rad}(L \otimes_K K')$ ein Integritätsring; der zugehörige Quotientenkörper werde mit Q bezeichnet. Weiter besteht folgende Sequenz von Homomorphismen:

$$M \otimes_K K' \xrightarrow{\sim} M \otimes_L (L \otimes_K K') \xrightarrow{\varphi} M \otimes_L R \xrightarrow{\psi} M \otimes_L Q$$

Die erste Abbildung ist der Isomorphismus aus 7.2/7, die weiteren entstehen aus den kanonischen Abbildungen $L \otimes_K K' \longrightarrow R \hookrightarrow Q$ durch Tensorieren mit M über L. Dabei schließt man aus 7.2/5 sowie unter Benutzung der Flachheit von M/L, dass $\ker \varphi$ mit dem Tensorprodukt $M \otimes_L \mathrm{rad}(L \otimes_K K')$ zu identifizieren ist, also nur nilpotente Elemente enthält, und dass ψ injektiv ist. Um zu sehen, dass $\mathrm{rad}(M \otimes_K K')$ ein Primideal ist, betrachte man Elemente $a, b \in M \otimes_L (L \otimes_K K')$, deren Produkt ab nilpotent ist. Dann ist $(\psi \circ \varphi)(ab) = (\psi \circ \varphi)(a) \cdot (\psi \circ \varphi)(b)$ nilpotent in $M \otimes_L Q$. Da M/L primär ist, muss einer der beiden Faktoren, etwa $(\psi \circ \varphi)(a)$ nilpotent sein. Da $\ker \psi \circ \varphi = \ker \varphi$ aus nilpotenten Elementen besteht, ist a selbst nilpotent. Insbesondere folgt, dass $\mathrm{rad}(M \otimes_K K')$ prim ist. □

Wir wollen im weiteren Verlauf zeigen, dass eine Körpererweiterung L/K bereits dann primär bzw. regulär ist, wenn das Tensorprodukt $L \otimes_K K'$ für alle *algebraischen* Körpererweiterungen K'/K irreduzibel bzw. nullteilerfrei ist. Als Hilfsmittel benötigen wir folgendes Schlüsselresultat:

Lemma 12. *Ein Tensorprodukt $A \otimes_K A'$ von Algebren A und A' über einem* algebraisch abgeschlossenen *Körper K ist genau dann ein Integritätsring, wenn A und A' Integritätsringe sind.*

Beweis. Sei zunächst $A \otimes_K A'$ ein Integritätsring. Dann gilt $A \otimes_K A' \neq 0$, und dies impliziert $A \neq 0$ und $A' \neq 0$. Somit sind die Strukturabbildungen $K \longrightarrow A, K \longrightarrow A'$ injektiv. Wegen der Flachheit von A und A' über K sind auch die tensorierten Abbildungen

$$A \simeq A \otimes_K K \longrightarrow A \otimes_K A', \qquad A' \simeq K \otimes_K A' \longrightarrow A \otimes_K A'$$

injektiv, und es folgt, dass A und A' Integritätsringe sind. Dasselbe Argument zeigt $A \otimes_K A' \neq 0$, wenn $A \neq 0$ und $A' \neq 0$ gilt.

Um nachzuweisen, dass $A \otimes_K A'$ ein Integritätsring ist, sofern dies für A und A' gilt, greifen wir auf die geometrischen Methoden aus Abschnitt 3.9 zurück; insbesondere benutzen wir den Hilbertschen Nullstellensatz 3.9/4. Seien also A und A' Integritätsringe. Indem wir 7.2/13 benutzen, dürfen wir annehmen, dass A und A' endlich erzeugte K-Algebren sind, also von der Form

$$A \simeq K[X]/\mathfrak{p}, \qquad A' \simeq K[Y]/\mathfrak{q},$$

mit Variablen $X = (X_1, \ldots, X_r)$, $Y = (Y_1, \ldots, Y_s)$ und Primidealen $\mathfrak{p}$, $\mathfrak{q}$. Weiter hat man nach 7.2/10 einen kanonischen Isomorphismus

$$\big(K[X]/\mathfrak{p}\big) \otimes_K \big(K[Y]/\mathfrak{q}\big) \xrightarrow{\sim} K[X,Y]\big/(\mathfrak{p},\mathfrak{q}), \qquad \overline{f} \otimes \overline{g} \longmapsto \overline{fg}.$$

Es seien nun $U = V(\mathfrak{p}) \subset K^r$ und $U' = V(\mathfrak{q}) \subset K^s$ die zu $\mathfrak{p}$ und $\mathfrak{q}$ gehörigen algebraischen Teilmengen von K^r bzw. K^s. Dann gilt $U \times U' = V(\mathfrak{p},\mathfrak{q})$, d. h. $U \times U'$ ist die zu dem Ideal $(\mathfrak{p},\mathfrak{q}) \subset K[X,Y]$ gehörige algebraische Menge. Da alle Polynome aus $\mathfrak{p}$ auf U trivial sind, faktorisiert der Einsetzungshomomorphismus $K[X] \longrightarrow K$, $f \longmapsto f(x)$, für $x \in U$ über $A \simeq K[X]/\mathfrak{p}$, liefert also einen Einsetzungshomomorphismus $A \longrightarrow K$. Wir können daher, wie zum Ende von Abschnitt 3.9 erläutert, die Elemente von A als "Funktionen" auf U ansehen. Aufgrund des Hilbertschen Nullstellensatzes 3.9/4 verschwindet eine Funktion $f \in A$ genau dann auf ganz U, wenn $f \in \operatorname{rad} A$ gilt, wenn also f nilpotent ist. In unserem Falle ist allerdings $\mathfrak{p}$ ein Primideal und folglich $A = K[X]/\mathfrak{p}$ ein Integritätsring, so dass $f(U) = 0$ äquivalent zu $f = 0$ ist. In ähnlicher Weise betrachten wir die Elemente aus A' als Funktionen auf U' sowie die Elemente aus $A \otimes_K A'$ als Funktionen auf $U \times U'$.

In einem ersten Schritt wollen wir zeigen, dass $A \otimes_K A'$ reduziert ist, dass also aus $g(U \times U') = 0$ mit $g \in A \otimes_K A'$ stets $g = 0$ folgt. Hierfür benötigen wir zu Punkten $x \in U$ das Tensorprodukt des Einsetzungshomomorphismus $A \longrightarrow K$, $a \longmapsto a(x)$, mit A', also die Abbildung

$$\sigma_x \colon A \otimes_K A' \longrightarrow A', \qquad \sum a_i \otimes a_i' \longmapsto \sum a_i(x) \cdot a_i',$$

sowie in einem späteren Stadium auch noch die analoge Abbildung

$$\tau_y \colon A \otimes_K A' \longrightarrow A, \qquad \sum a_i \otimes a_i' \longmapsto \sum a_i \cdot a_i'(y),$$

zu Punkten $y \in U'$. Weiter wähle man eine K-Basis $(e'_i)_{i\in I}$ von A'. Gemäß 7.2/4 hat dann jedes $g \in A \otimes_K A'$ eine Darstellung $g = \sum_{i\in I} g_i \otimes e'_i$ mit eindeutig bestimmten Elementen $g_i \in A$. Nach diesen Vorbereitungen betrachte man nun ein nilpotentes Element $g \in A \otimes_K A'$ mit der Darstellung $g = \sum_{i\in I} g_i \otimes e'_i$. Es verschwindet g auf $U \times U'$, und folglich gilt dasselbe für die Funktionen $\sigma_x(g) = \sum_{i\in I} g_i(x) \cdot e'_i$ auf U', und zwar für jedes $x \in U$. Da A' reduziert ist, folgt $g_i(x) = 0$ für alle $x \in U$. Da auch A reduziert ist, ergibt sich $g_i = 0$ für alle $i \in I$ und somit $g = 0$. Also ist $A \otimes_K A'$ reduziert.

In ähnlicher Weise können wir zeigen, dass $A \otimes_K A'$ sogar ein Integritätsring ist. Seien $f, g \in A \otimes_K A'$, $f \neq 0$, mit $f \cdot g = 0$, wobei wiederum $g = \sum_{i\in I} g_i \otimes e'_i$ gelte. Aus

$$\sigma_x(f) \cdot \sum_{i\in I} g_i(x) \cdot e'_i = \sigma_x(f) \cdot \sigma_x(g) = \sigma_x(fg) = 0$$

und der Nullteilerfreiheit von A' schließt man dann $\sigma_x(g) = 0$ bzw. $g_i(x) = 0$ für alle $x \in U$ mit $\sigma_x(f) \neq 0$, d. h. für alle diejenigen $x \in U$, zu denen es ein $y \in U'$ mit $f(x, y) \neq 0$ gibt. Dies bedeutet, dass $f \cdot (g_i \otimes 1)$ für alle $i \in I$ auf $U \times U'$ verschwindet, d. h. es gilt $f \cdot (g_i \otimes 1) = 0$, wie wir oben gesehen haben. Weiter hat man

$$\tau_y(f) \cdot g_i = \tau_y\big(f \cdot (g_i \otimes 1)\big) = 0$$

für $y \in U'$. Wegen $f \neq 0$ gibt es Punkte $(x, y) \in U \times U'$ mit $f(x, y) \neq 0$, also insbesondere mit $\tau_y(f) \neq 0$. Da A nullteilerfrei ist, folgt $g_i = 0$ für alle $i \in I$ und somit $g = 0$. □

Satz 13. *Es sei L/K eine Körpererweiterung. Dann ist äquivalent*:

(i) *L/K ist primär.*

(ii) *Für jede endliche separable Erweiterung K'/K ist $L \otimes_K K'$ irreduzibel.*

(iii) *K ist separabel abgeschlossen in L, d. h. jedes Element $a \in L$, welches separabel algebraisch über K ist, gehört bereits zu K.*

Beweis. Die Implikation (i) $\Longrightarrow$ (ii) ist trivial. Sei also Bedingung (ii) gegeben, und sei $a \in L$ separabel algebraisch über K. Ist $f \in K[X]$ das Minimalpolynom zu a, so zerfällt dieses Polynom über L in ein Produkt von irreduziblen Faktoren, etwa $f = f_1 \dots f_r$, wobei aufgrund der Separabilität von f keine mehrfachen Primfaktoren auftreten können. Deshalb gilt für $K' = K(a)$ nach 7.2/11

$$L \otimes_K K' \simeq \prod_{i=1}^{r} L[X]/(f_i),$$

d. h. es ist $L \otimes_K K'$ ein endliches Produkt von Körpern. Insbesondere ist $\mathrm{rad}(L \otimes_K K')$ das Nullideal. Da dieses Ideal aber nach Voraussetzung ein Primideal ist, gilt notwendig $r = 1$. Also ist f irreduzibel in $L[X]$. Nun ist aber $a \in L$ eine Nullstelle von f, so dass man in $L[X]$ eine Gleichung der Form $f = (X - a) \cdot g$ hat. Aus der Irreduzibilität von f ergibt sich $g = 1$ und folglich $a \in K$. Somit ist K separabel abgeschlossen in L.

Sei nun Bedingung (iii) erfüllt. Um zu zeigen, dass $L \otimes_K K'$ für Körpererweiterungen K'/K irreduzibel ist, betrachten wir zunächst eine endliche separable Erweiterung K'/K. Nach dem Satz vom primitiven Element 3.6/12 ist K'/K eine einfache Erweiterung, etwa $K' = K(a)$. Sei $f \in K[X]$ das Minimalpolynom von a über K. Dieses ist irreduzibel über K, aber auch über L. Ist nämlich $f = g \cdot h$ eine Zerlegung mit normierten Polynomen $g, h \in L[X]$, so sind die Koeffizienten von g und h als Elemente eines Zerfällungskörpers von f über K separabel algebraisch über K. Es gilt also bereits $g, h \in K[X]$, und aus der Irreduzibilität von f über K folgt $g = 1$ oder $h = 1$, d. h. f ist irreduzibel über L. Nun hat man aber $L \otimes_K K' \simeq L[X]/(f)$ nach 7.2/11, was zeigt, dass $L \otimes_K K'$ ein Körper ist.

In einem nächsten Schritt betrachten wir im Falle positiver Charakteristik eine endliche rein inseparable Körpererweiterung K''/K', wobei wie soeben K'/K endlich und separabel sei. Da wir im Anschluss an Definition 9 gesehen haben, dass einfache rein inseparable Erweiterungen primär sind, folgt mit Satz 11 (iii), dass auch K''/K' primär ist. Daher ist $L \otimes_K K'' \simeq (L \otimes_K K') \otimes_{K'} K''$ irreduzibel, und wir sehen auf diese Weise, dass $L \otimes_K K''$ für alle endlichen Erweiterungen K''/K irreduzibel ist. Ist nun $\overline{K}$ ein algebraischer Abschluss zu K, so ist auch $L \otimes_K \overline{K}$ irreduzibel. Mittels 7.2/13 lässt sich das Radikal $\mathrm{rad}(L \otimes_K \overline{K})$ nämlich als Vereinigung aller Radikale $\mathrm{rad}(L \otimes_K K'')$ zu endlichen Erweiterungen K''/K mit $K'' \subset \overline{K}$ interpretieren.

Hieraus folgt nun unter Benutzung von Lemma 12 leicht, dass $L \otimes_K K'$ für beliebige Erweiterungen K'/K irreduzibel und L/K somit primär ist. Man wähle nämlich einen algebraischen Abschluss $\overline{K'}$ zu K' und betrachte die von $K' \hookrightarrow \overline{K'}$ induzierte Injektion $L \otimes_K K' \hookrightarrow L \otimes_K \overline{K'}$. Es genügt zu zeigen, dass $L \otimes_K \overline{K'}$ irreduzibel ist. Nun haben wir aber gerade gesehen, dass $L \otimes_K \overline{K}$ irreduzibel ist, wenn $\overline{K}$ den algebraischen Abschluss von K in $\overline{K'}$ bezeichnet. Da das Tensorprodukt

$$\big((L \otimes_K \overline{K}) \big/ \operatorname{rad}(L \otimes_K \overline{K})\big) \otimes_{\overline{K}} \overline{K}'$$

nach Lemma 12 ein Integritätsring ist, sieht man wie im Beweis zu Satz 11 (iii), dass $L \otimes_K \overline{K}'$ irreduzibel ist. □

Aus den gewonnenen Resultaten für separable und primäre Körpererweiterungen lässt sich durch Kombination eine entsprechende Charakterisierung regulärer Körpererweiterungen ableiten.

Satz 14. *Es sei L/K eine Körpererweiterung. Dann ist äquivalent*:

(i) *L/K ist regulär.*

(ii) *Für jede endliche Erweiterung K'/K ist $L \otimes_K K'$ ein Integritätsring.*

(iii) *L/K ist separabel und K ist algebraisch abgeschlossen in L.*

Beweis. Ein Ring R ist genau dann ein Integritätsring, wenn das Nullideal $0 \subset R$ prim ist. Letzteres ist äquivalent dazu, dass das Radikal $\operatorname{rad} R$ einerseits prim ist und andererseits verschwindet. Dies zeigt die Äquivalenz von (i) und (ii), wenn man die Sätze 7 und 13 benutzt.

Um auch die Äquivalenz von (i) und (iii) zu erhalten, gehe man zunächst von einer regulären Erweiterung L/K aus. Dann ist nach Satz 11 (i) auch der algebraische Abschluss von K in L regulär über K. Es genügt also, den Fall zu betrachten, wo L/K algebraisch ist. Hier ergibt sich aber aus Bemerkung 1 und Satz 13 sofort $L = K$ und damit (iii). Ist umgekehrt Bedingung (iii) gegeben, so folgt (i) wiederum mit Satz 13. □

Wir wollen abschließend noch auf eine geometrische Anwendung der gewonnenen Resultate hinweisen. In der Situation von Abschnitt 3.9 betrachte man einen Körper K sowie einen algebraischen Abschluss $\overline{K}$. Weiter sei $U \subset \overline{K}^n$ eine über K definierte algebraische Teilmenge von $\overline{K}^n$, die *irreduzibel* sei, d. h. wir verlangen, dass das zugehörige Ideal $\mathfrak{p} = I_K(U) \subset K[X_1, \ldots, X_n]$ prim sei; man vergleiche hierzu auch die geometrische Interpretation der Irreduzibilität in Aufgabe 4 aus Abschnitt 3.9. Dann lässt sich U auch als über $\overline{K}$ definierte algebraische Teilmenge von $\overline{K}^n$ auffassen, und man kann das zugehörige Ideal $I_{\overline{K}}(U)$ in $\overline{K}[X_1, \ldots, X_n]$ betrachten, welches sich aufgrund des Hilbertschen Nullstellensatzes 3.9/4 zu $I_{\overline{K}}(U) = \operatorname{rad}(\mathfrak{p}\overline{K}[X_1, \ldots, X_n])$ berechnet. Es heißt *U geometrisch reduziert*, wenn $I_{\overline{K}}(U) = \mathfrak{p}\overline{K}[X_1, \ldots, X_n]$ gilt, d. h. wenn das Ideal $\mathfrak{p}\overline{K}[X_1, \ldots, X_n]$ reduziert ist. Weiter heißt *U geometrisch irreduzibel*, wenn

$I_{\overline{K}}(U) = \mathrm{rad}(\mathfrak{p}\overline{K}[X_1, \ldots, X_n])$ prim ist, wenn also U als über $\overline{K}$ definierte algebraische Menge irreduzibel ist. Mit Aufgabe 4 sieht man, dass U genau dann geometrisch reduziert (bzw. geometrisch irreduzibel, bzw. geometrisch reduziert und geometrisch irreduzibel) ist, wenn für den Quotientenkörper Q zu $K[X_1, \ldots, X_n]/\mathfrak{p}$ die Erweiterung Q/K separabel (bzw. primär, bzw. regulär) ist.

Lernkontrolle und Prüfungsvorbereitung

1. Definiere das Radikal $\mathrm{rad}\, R$ eines Rings R und zeige, dass R genau dann ein Integritätsring ist, wenn $\mathrm{rad}\, R$ ein Primideal mit $\mathrm{rad}\, R = 0$ ist.
2. Wann bezeichnet man eine allgemeine Körpererweiterung als separabel? Gib die Definition und zeige, dass diese kompatibel mit der gewöhnlichen Definition ist, die man für algebraische Körpererweiterungen kennt.
3. Zeige, dass jede rein transzendente Körpererweiterung separabel ist.
4. Wie lässt sich die Separabilität einer Körpererweiterung M/K in Beziehung setzen zur Separabilität von M/L bzw. L/K für Zwischenkörper L zu M/K (mit Begründung)?
5. Wann bezeichnet man eine Körpererweiterung L/K als separabel erzeugt? Was versteht man unter einer separierenden Transzendenzbasis von L/K?
6. Zeige, dass jede separabel erzeugte Körpererweiterung separabel ist, insbesondere also jede Körpererweiterung in Charakteristik 0.
7. Konstruiere zu einem Körper K seinen rein inseparablen Abschluss $K^{p^{-\infty}}$.

+8. Zeige, dass eine Körpererweiterung L/K genau dann separabel ist, wenn das Tensorprodukt $L \otimes_K K^{p^{-\infty}}$ reduziert ist.

9. Zeige, dass jede Körpererweiterung eines vollkommenen Körpers separabel ist.

+10. Zeige, dass eine endlich erzeugte Körpererweiterung L/K genau dann separabel ist, wenn sie separabel erzeugt ist.

11. Definiere primäre bzw. reguläre Körpererweiterungen und begründe, dass eine Körpererweiterung genau dann regulär ist, wenn sie separabel und primär ist.
12. Zeige, dass jede rein transzendente Körpererweiterung regulär und insbesondere primär ist.

13. Wie lassen sich die Eigenschaften "primär" bzw. "regulär" einer Körpererweiterung M/K für Zwischenkörper L in Beziehung setzen zu den entsprechenden Eigenschaften der Erweiterungen M/L bzw. L/K (mit Begründung)?

$^{+}$14. Zeige, dass das Tensorprodukt $A \otimes_K A'$ zweier K-Algebren über einem algebraisch abgeschlossenen Körper K genau dann ein Integritätsring ist, wenn A und A' selbst Integritätsringe sind.

$^{+}$15. Zeige, dass eine Körpererweiterung L/K genau dann primär ist, wenn für jede endliche separable Erweiterung K'/K das Tensorprodukt $L \otimes_K K'$ irreduzibel ist und dass Letzteres genau dann der Fall ist, wenn K separabel abgeschlossen in L ist.

16. Zeige, dass eine Körpererweiterung L/K genau dann regulär ist, wenn für jede endliche Erweiterung K'/K das Tensorprodukt $L \otimes_K K'$ ein Integritätsring ist und dass Letzteres genau dann der Fall ist, wenn L/K separabel und K algebraisch abgeschlossen in L ist.

Übungsaufgaben

1. *Es seien $K \subset L \subset M$ Körpererweiterungen, wobei M/K separabel (bzw. primär, bzw. regulär) sei. Wir haben gesehen, dass dann auch die Erweiterung L/K separabel (bzw. primär, bzw. regulär) ist. Kann man eine entsprechende Aussage auch für die Erweiterung M/L machen?*

2. *Eine Körpererweiterung L/K ist genau dann primär, wenn K in L separabel abgeschlossen ist. Lassen sich im Falle $p = \operatorname{char} K > 0$ separable Erweiterungen L/K in ähnlicher Weise charakterisieren, etwa indem man fordert, dass aus $a \in L$ mit $a^p \in K$ bereits $a \in K$ folgt, oder, dass der algebraische Abschluss von K in L separabel über K ist?*

3. *Konstruiere ein Beispiel einer separablen Körpererweiterung, die nicht separabel erzeugt ist.*

4. Es sei $K[X]$ der Polynomring über einem Körper K in endlich vielen Variablen $X_1, \ldots, X_n$. Betrachte ein Primideal $\mathfrak{p} \subset K[X]$, den zugehörigen Quotientenkörper $Q = Q(K[X]/\mathfrak{p})$ sowie einen algebraischen Abschluss $\overline{K}$ zu K und zeige:

   (i) Die Erweiterung Q/K ist genau dann separabel, wenn das Ideal $\mathfrak{p}\overline{K}[X]$ in $\overline{K}[X]$ reduziert ist.

   (ii) Die Erweiterung Q/K ist genau dann primär, wenn das Ideal $\operatorname{rad}(\mathfrak{p}\overline{K}[X])$ ein Primideal in $\overline{K}[X]$ ist.

(iii) Die Erweiterung Q/K ist genau dann regulär, wenn das Ideal $\mathfrak{p}\overline{K}[X]$ ein Primideal in $\overline{K}[X]$ ist.

5. Es sei K ein Körper und $\overline{K}$ ein algebraischer Abschluss. Zeige, dass eine Erweiterung L/K genau dann regulär ist, wenn $L \otimes_K \overline{K}$ ein Körper ist.

6. Es sei K ein vollkommener Körper. Zeige: Sind A, A' zwei reduzierte K-Algebren, so ist auch das Tensorprodukt $A \otimes_K A'$ reduziert.

7. Sei K ein Körper der Charakteristik $p > 0$. Ein System $x = (x_1, \ldots, x_n)$ von Elementen aus $K^{p^{-1}}$ heißt *p-frei* über K, wenn sich die Erweiterung $K(x)/K$ nicht von weniger als n Elementen erzeugen lässt. Zeige:

   (i) Ein System von n Elementen $x_1, \ldots, x_n \in K^{p^{-1}}$ ist genau dann p-frei über K, wenn die von $X_i \longmapsto x_i$ induzierte kanonische Abbildung $K[X_1, \ldots, X_n]/(X_1^p - x_1^p, \ldots, X_n^p - x_n^p) \longrightarrow K(x)$ ein Isomorphismus ist.

   (ii) Eine Körpererweiterung L/K ist genau dann separabel, wenn folgende Bedingung gilt: Sind $x_1, \ldots, x_n \in K$ p-frei über K^p, so sind diese Elemente auch p-frei über L^p.

7.4 Kalkül der Differentiale*

Ziel dieses Abschnitts ist die Charakterisierung separabler Körpererweiterungen mit Mitteln der Differentialrechnung. Die benutzten Methoden fußen allerdings nicht auf dem Limesbegriff der Infinitesimalrechnung, sondern sind rein algebraischer Natur. Sie finden ihre natürliche Fortsetzung beim Studium sogenannter étaler bzw. glatter Morphismen innerhalb der Algebraischen Geometrie; vgl. etwa [3], Chap. 8. Im Folgenden sei R stets ein Ring.

Definition 1. *Eine* R-Derivation *einer R-Algebra A in einen A-Modul M ist eine R-lineare Abbildung $\delta\colon A \longrightarrow M$, welche der "Produktregel"*

$$\delta(fg) = f \cdot \delta(g) + g \cdot \delta(f), \qquad f, g \in A,$$

genügt. Allgemein versteht man unter einer Derivation *eine $\mathbb{Z}$-Derivation.*

Für $r \in R$ gilt stets $\delta(r \cdot 1) = 0$. Außerdem folgert man aus der Produktregel leicht die "Quotientenregel"

$$\delta\Big(\frac{f}{g}\Big) = \frac{g\delta(f) - f\delta(g)}{g^2}$$

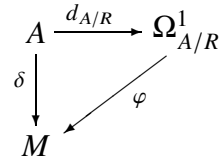
für Elemente $f, g \in A$, wobei g eine Einheit in A ist. Die Menge aller R-Derivationen $\delta\colon A \longrightarrow M$ bildet einen A-Modul, den wir mit $\mathrm{Der}_R(A, M)$ bezeichnen, bzw. mit $\mathrm{Der}(A, M)$, falls $R = \mathbb{Z}$ gesetzt ist. Ist beispielsweise $A = R[X]$ der Polynomring einer Variablen über R, so sieht man wie in 2.6/2, dass die formale Differentiation von Polynomen

$$\frac{d}{dX}\colon R[X] \longrightarrow R[X], \qquad f(X) \longmapsto f'(X),$$

der Produktregel genügt und daher eine R-Derivation von $R[X]$ in sich darstellt. Auch zeigt die Produktregel, dass eine beliebige R-Derivation $\delta\colon R[X] \longrightarrow R[X]$ bereits eindeutig durch die Angabe des Elements $\delta(X)$ bestimmt ist. Daher erkennt man $\mathrm{Der}_R(R[X], R[X])$ als den freien $R[X]$-Modul, der von der Derivation $\frac{d}{dX}$ erzeugt wird.

Satz 2. *Es sei A eine R-Algebra. Dann existiert ein A-Modul $\Omega^1_{A/R}$ zusammen mit einer R-Derivation $d_{A/R}\colon A \longrightarrow \Omega^1_{A/R}$, so dass das Paar $(\Omega^1_{A/R}, d_{A/R})$ folgende universelle Eigenschaft besitzt*:

Zu jeder R-Derivation $\delta\colon A \longrightarrow M$ in einen A-Modul M gibt es eine eindeutig bestimmte A-lineare Abbildung $\varphi\colon \Omega^1_{A/R} \longrightarrow M$ mit $\delta = \varphi \circ d_{A/R}$, so dass also das Diagramm



kommutativ ist. Das Paar $(\Omega^1_{A/R}, d_{A/R})$ ist durch diese Eigenschaft bis auf kanonische Isomorphie eindeutig bestimmt. Man nennt $(\Omega^1_{A/R}, d_{A/R})$ bzw. $\Omega^1_{A/R}$ den Modul der relativen Differentialformen (*vom Grad* 1) *von A über R.*

Beweis. Wir behandeln zunächst den Fall $A = R[\mathfrak{X}]$ mit einem System $\mathfrak{X}$ von (beliebig vielen) Variablen X_i, $i \in I$. Es sei $\Omega^1_{A/R} = A^{(I)}$ der von I erzeugte freie A-Modul, wobei wir für das zu $i \in I$ korrespondierende Basiselement von $\Omega^1_{A/R}$ im Folgenden die Notation dX_i verwenden werden,

also $\Omega^1_{A/R} = \bigoplus_{i\in I} A \cdot dX_i$. Bildet man die partiellen Ableitungen von Elementen $f \in A$ nach den Variablen X_i, und zwar im formalen Sinne, so überzeugt man sich wie in 2.6/2 davon, dass

$$d_{A/R}\colon A \longrightarrow \Omega^1_{A/R}, \qquad f \longmapsto \sum_{i\in I} \frac{\partial f}{\partial X_i} dX_i,$$

eine R-Derivation mit $d_{A/R}(X_i) = dX_i$ ist und weiter, dass $(\Omega^1_{A/R}, d_{A/R})$ die universelle Eigenschaft eines Moduls der relativen Differentialformen von A über R erfüllt. Ist nämlich $\delta\colon A \longrightarrow M$ eine R-Derivation in einen beliebigen A-Modul M, so erkläre man eine A-lineare Abbildung $\varphi\colon \Omega^1_{A/R} \longrightarrow M$ durch $\varphi(dX_i) = \delta(X_i)$ für $i \in I$. Dann ist $\varphi \circ d_{A/R}$ eine R-Derivation von A nach M, welche auf den Variablen X_i, $i \in I$, mit δ übereinstimmt. Aufgrund der A-Linearität und der Produktregel ergibt sich hieraus für $f \in A$ die Gleichung

$$\delta(f) = \sum_{i\in I} \frac{\partial f}{\partial X_i}\delta(X_i) = \sum_{i\in I} \frac{\partial f}{\partial X_i}\varphi(dX_i) = \varphi \circ d_{A/R}(f),$$

also $\delta = \varphi \circ d_{A/R}$. Da aus dieser Beziehung notwendig $\varphi(dX_i) = \delta(X_i)$ folgt, ist φ auch eindeutig bestimmt.

Im Allgemeinfall können wir A von der Form $R[\mathfrak{X}]/\mathfrak{a}$ annehmen mit einem System $\mathfrak{X}$ von Variablen und einem Ideal $\mathfrak{a} \subset R[\mathfrak{X}]$. Folglich genügt es zu zeigen:

Lemma 3. *Es sei A eine R-Algebra und $\mathfrak{a} \subset A$ ein Ideal. Man setze $B = A/\mathfrak{a}$. Ist dann $(\Omega^1_{A/R}, d_{A/R})$ der Modul der relativen Differentialformen von A über R, so ist*

$$\Omega = \Omega^1_{A/R} \big/ \big(\mathfrak{a}\Omega^1_{A/R} + A d_{A/R}(\mathfrak{a})\big)$$

zusammen mit der von $d_{A/R}\colon A \longrightarrow \Omega^1_{A/R}$ induzierten R-linearen Abbildung $d\colon B \longrightarrow \Omega$ der Modul der relativen Differentialformen von B über R.

Beweis. Zunächst stellt man fest, dass Ω ein B-Modul ist. Da weiter $d_{A/R}$ die Eigenschaften einer R-Derivation besitzt, gilt dasselbe für d. Um die universelle Eigenschaft für d zu zeigen, betrachte man eine R-Derivation $\overline{\delta}\colon B \longrightarrow M$ in einen B-Modul M. Dann ist die Komposition $\delta = \overline{\delta} \circ \pi$ mit der Projektion $\pi\colon A \longrightarrow A/\mathfrak{a} = B$ eine R-Derivation von A nach M,

wobei wir M bezüglich $\pi\colon A \longrightarrow B$ als A-Modul auffassen. Die universelle Eigenschaft von $d_{A/R}\colon A \longrightarrow \Omega^1_{A/R}$ bewirkt, dass δ eindeutig über eine A-lineare Abbildung $\varphi\colon \Omega^1_{A/R} \longrightarrow M$ faktorisiert. Da $\delta(\mathfrak{a}) = 0$ gilt und M ein Modul über B ist, hat man notwendig $\varphi(\mathfrak{a}\Omega^1_{A/R} + Ad_{A/R}(\mathfrak{a})) = 0$. Somit induziert φ eine B-lineare Abbildung $\overline{\varphi}\colon \Omega \longrightarrow M$ mit $\overline{\delta} = \overline{\varphi} \circ d$. Dass $\overline{\varphi}$ durch diese Gleichung eindeutig bestimmt ist, folgt aus der Eindeutigkeit von φ. Lemma 3 und Satz 2 sind also bewiesen. □

Der obige Satz besagt insbesondere, dass $\varphi \longmapsto \varphi \circ d_{A/R}$ eine A-lineare Bijektion

$$\mathrm{Hom}_A\big(\Omega^1_{A/R}, M\big) \longrightarrow \mathrm{Der}_R\big(A, M\big)$$

zwischen den A-Modulhomomorphismen $\Omega^1_{A/R} \longrightarrow M$ und den R-Derivationen von A nach M definiert. Weiter sieht man aus der universellen Eigenschaft von $\Omega^1_{A/R}$ unmittelbar, dass $\Omega^1_{A/R}$ von allen Differentialen zu Elementen aus A, d. h. von allen Elementen des Typs $d_{A/R}(f)$, $f \in A$, erzeugt wird. Genauer zeigt die im Beweis zu Satz 2 gegebene Argumentation:

Satz 4. *Es sei A eine R-Algebra und $x = (x_i)_{i\in I}$ ein System von Elementen von A mit $A = R[x]$. Dann gilt*:

(i) *$(d_{A/R}(x_i))_{i\in I}$ ist ein A-Erzeugendensystem von $\Omega^1_{A/R}$.*

(ii) *Ist $x = (x_i)_{i\in I}$ algebraisch unabhängig über R, so bildet das System $(d_{A/R}(x_i))_{i\in I}$ eine Basis von $\Omega^1_{A/R}$; insbesondere ist $\Omega^1_{A/R}$ dann frei.*

Als Nächstes wollen wir zeigen, dass zu einem Homomorphismus von R-Algebren $\tau\colon A \longrightarrow B$ stets eine kanonische exakte Sequenz von B-Moduln

$$\Omega^1_{A/R} \otimes_A B \xrightarrow{\ \alpha\ } \Omega^1_{B/R} \xrightarrow{\ \beta\ } \Omega^1_{B/A} \longrightarrow 0$$

korrespondiert. Um die Abbildung α zu erklären, betrachte man die Komposition von $\tau\colon A \longrightarrow B$ mit der R-Derivation $d_{B/R}\colon B \longrightarrow \Omega^1_{B/R}$. Fasst man $\Omega^1_{B/R}$ mittels τ als A-Modul auf, so ist $d_{B/R} \circ \tau$ eine R-Derivation von A. Nach Definition von $\Omega^1_{A/R}$ faktorisiert diese über eine A-lineare Abbildung

$$\Omega^1_{A/R} \longrightarrow \Omega^1_{B/R}, \qquad d_{A/R}(f) \longmapsto d_{B/R}\big(\tau(f)\big),$$

und letztere induziert eine B-lineare Abbildung

$$\alpha\colon \Omega^1_{A/R} \otimes_A B \longrightarrow \Omega^1_{B/R}, \qquad d_{A/R}(f) \otimes b \longmapsto b \cdot d_{B/R}\big(\tau(f)\big).$$

Zur Definition von β schließlich beachte man, dass sich jede A-Derivation von B insbesondere als R-Derivation von B auffassen lässt, so dass man aufgrund der universellen Eigenschaft von $\Omega^1_{B/R}$ eine wohldefinierte B-lineare Abbildung

$$\beta\colon \Omega^1_{B/R} \longrightarrow \Omega^1_{B/A}, \qquad d_{B/R}(g) \longmapsto d_{B/A}(g),$$

erhält.

Satz 5. *Ist $\tau\colon A \longrightarrow B$ ein Homomorphismus von R-Algebren, so ist die Sequenz*

$$\Omega^1_{A/R} \otimes_A B \xrightarrow{\ \alpha\ } \Omega^1_{B/R} \xrightarrow{\ \beta\ } \Omega^1_{B/A} \longrightarrow 0,$$

die durch $d_{A/R}(f) \otimes b \overset{\alpha}{\longmapsto} b \cdot d_{B/R}(\tau(f))$, $d_{B/R}(g) \overset{\beta}{\longmapsto} d_{B/A}(g)$ gegeben wird, exakt.

Beweis. Da $\Omega^1_{B/A}$ von allen Elementen des Typs $d_{B/A}(g)$, $g \in B$, erzeugt wird, und da $\beta(d_{B/R}(g)) = d_{B/A}(g)$ gilt, ist β surjektiv. Weiter gilt $\beta \circ \alpha = 0$, und es genügt zum Nachweis von $\operatorname{im}\alpha = \ker\beta$ zu zeigen, dass $\Omega^1_{B/R}/\operatorname{im}\alpha$ zusammen mit der von $d_{B/R}$ induzierten Abbildung $d\colon B \longrightarrow \Omega^1_{B/R}/\operatorname{im}\alpha$ der Modul der relativen Differentialformen von B über A ist. Um dies einzusehen, betrachte man folgendes kommutative Diagramm:

$$\begin{array}{ccccc} A & \xrightarrow{d_{A/R}\otimes 1} & \Omega^1_{A/R} \otimes_A B & & \\ {\scriptstyle\tau}\downarrow & & \downarrow{\scriptstyle\alpha} & & \\ d\colon B & \xrightarrow{d_{B/R}} & \Omega^1_{B/R} & \longrightarrow & \Omega^1_{B/R}/\operatorname{im}\alpha \end{array}$$

Zunächst ist $d\colon B \longrightarrow \Omega^1_{B/R}/\operatorname{im}\alpha$ eine A-Derivation, da dies nach Definition eine R-Derivation ist und da $d_{B/R}(\tau(f)) \in \operatorname{im}\alpha$ für alle $f \in A$ gilt. Ist nun $\delta\colon B \longrightarrow M$ eine A-Derivation von B in einen B-Modul M, so ist dies insbesondere eine R-Derivation. Also existiert eine eindeutig bestimmte B-lineare Abbildung $\varphi\colon \Omega^1_{B/R} \longrightarrow M$ mit $\delta = \varphi \circ d_{B/R}$. Da δ eine

A-Derivation ist, gilt $\delta \circ \tau = 0$ und folglich $\varphi \circ \alpha = 0$, was aber bedeutet, dass φ durch eine B-lineare Abbildung $\overline{\varphi}\colon \Omega^1_{B/R}/\operatorname{im}\alpha \longrightarrow M$ faktorisiert. Nach Konstruktion gilt $\delta = \overline{\varphi} \circ d$, wobei $\overline{\varphi}$ durch diese Gleichung eindeutig bestimmt ist. □

Wir wollen die exakte Sequenz aus Satz 5 in einem Spezialfall auswerten.

Satz 6. *Es sei A eine R-Algebra und $S \subset A$ ein multiplikatives System. Ist dann $\tau\colon A \longrightarrow A_S$ die kanonische Abbildung von A in die Lokalisierung nach S, so ist die zugehörige Abbildung*

$$\alpha\colon \Omega^1_{A/R} \otimes_A A_S \longrightarrow \Omega^1_{A_S/R}, \qquad d_{A/R}(f) \otimes a \longmapsto a \cdot d_{A_S/R}\big(\tau(f)\big),$$

bijektiv. Insbesondere gilt $\Omega^1_{A_S/A} = 0$.

Beweis. Die Gleichung $\Omega^1_{A_S/A} = 0$ ergibt sich leicht aus der Bijektivität von α; man verwende Satz 5 oder setze $R = A$ und benutze $\Omega^1_{A/A} = 0$. Es bleibt also lediglich zu zeigen, dass α bijektiv ist. Hierzu identifiziert man $\Omega^1_{A/R} \otimes_A A_S$ mit dem A_S-Modul $(\Omega^1_{A/R})_S$, vgl. 7.2/8, und zeigt, dass $(\Omega^1_{A/R})_S$ zusammen mit der Abbildung

$$d\colon A_S \longrightarrow (\Omega^1_{A/R})_S, \qquad \frac{f}{s} \longmapsto \frac{s d_{A/R}(f) - f d_{A/R}(s)}{s^2},$$

die universelle Eigenschaft des Moduls der relativen Differentialformen von A_S über R besitzt. Zunächst ist nachzurechnen, dass d wohldefiniert ist. Gelte etwa $\frac{f}{s} = \frac{f'}{s'}$ für $f, f' \in A$ und $s, s' \in S$. Dann gibt es ein $s'' \in S$, so dass die Gleichung $s''(s'f - sf') = 0$ in A besteht. Hieraus folgt

$$(s'f - sf') \cdot d_{A/R}(s'') + s'' \cdot d_{A/R}(s'f - sf') = 0,$$

und man sieht durch Multiplikation mit s'', dass $d_{A/R}(s'f - sf')$ in $(\Omega^1_{A/R})_S$ verschwindet, d.h. es gilt $s'\delta(f) - s\delta(f') = f'\delta(s) - f\delta(s')$, wobei δ die Komposition von $d_{A/R}$ mit der kanonischen Abbildung $\Omega^1_{A/R} \longrightarrow (\Omega^1_{A/R})_S$ bezeichne. Dass $d : A_S \longrightarrow (\Omega^1_{A/R})_S$ wohldefiniert ist, ergibt sich dann aus folgender Rechnung:

$$\begin{aligned}
&s'^2\big(s\delta(f) - f\delta(s)\big) - s^2\big(s'\delta(f') - f'\delta(s')\big)\\
&= ss'\big(s'\delta(f) - s\delta(f')\big) - s'^2 f\delta(s) + s^2 f'\delta(s')\\
&= ss'\big(f'\delta(s) - f\delta(s')\big) - s'^2 f\delta(s) + s^2 f'\delta(s')\\
&= s'(sf' - s'f)\delta(s) + s(sf' - s'f)\delta(s')\\
&= 0
\end{aligned}$$

Als Nächstes rechnet man in nahe liegender Weise aus, dass d eine Derivation ist, was wir hier aber nicht ausführen wollen. Zum Testen der universellen Eigenschaft betrachte man schließlich eine R-Derivation $\delta\colon A_S \longrightarrow M$ in einen A_S-Modul M. Es ist dann $\delta\circ\tau$ eine R-Derivation von A nach M, d. h. es existiert eine A-lineare Abbildung $\varphi\colon \Omega^1_{A/R} \longrightarrow M$ mit $\delta\circ\tau = \varphi\circ d_{A/R}$. Durch A_S-lineare Ausdehnung erhält man hieraus eine A_S-lineare Abbildung $\varphi_S\colon (\Omega^1_{A/R})_S \longrightarrow M$ mit $\delta = \varphi_S\circ d$, wobei φ_S durch diese Gleichung eindeutig bestimmt ist. □

Im Folgenden soll die Theorie der Differentialformen auf *Körpererweiterungen* angewendet werden. Wir wollen in einigen speziellen Fällen den Modul der relativen Differentialformen $\Omega^1_{L/K}$ zu einer Körpererweiterung L/K berechnen. Im Prinzip kann dies unter Benutzung von Lemma 3 und Satz 6 geschehen. In technischer Hinsicht ist es jedoch im Allgemeinen einfacher, statt $\Omega^1_{L/K}$ dessen Dualraum, nämlich den L-Vektorraum $\mathrm{Der}_K(L,L) \simeq \mathrm{Hom}_L(\Omega^1_{L/K}, L)$ zu berechnen. Man hat stets eine kanonische Injektion von L-Vektorräumen

$$\Omega^1_{L/K} \hookrightarrow \mathrm{Hom}_L\big(\mathrm{Der}_K(L,L), L\big), \qquad d_{L/K}(x) \longmapsto \big(\delta \longmapsto \delta(x)\big),$$

und diese ist bijektiv, wenn einer der Räume $\Omega^1_{L/K}$ oder $\mathrm{Der}_K(L,L)$ von endlicher Dimension über L ist.

Satz 7. *Es sei L/K eine Körpererweiterung und $x = (x_j)_{j\in J}$ ein Erzeugendensystem dieser Erweiterung. Für ein System von Variablen $\mathfrak{X} = (X_j)_{j\in J}$ definiere man durch $X_j \longmapsto x_j$ einen K-Homomorphismus $\pi\colon K[\mathfrak{X}] \longrightarrow L$, und es sei $(f_i)_{i\in I}$ ein Erzeugendensystem von* $\ker\pi$. *Weiter betrachte man eine Derivation $\delta\colon K \longrightarrow V$ in einen L-Vektorraum V sowie ein System $(v_j)_{j\in J}$ von Elementen aus V. Dann ist äquivalent*:

(i) *δ setzt sich zu einer Derivation $\delta'\colon L \longrightarrow V$ mit $\delta'(x_j) = v_j$ für $j \in J$ fort.*

(ii) *Es gilt*

$$f_i^\delta(x) + \sum_{j\in J} \frac{\partial f_i}{\partial X_j}(x) \cdot v_j = 0, \qquad i \in I.$$

Dabei bezeichne f^δ *für* $f \in K[\mathfrak{X}]$ *das "Polynom" in* $V[\mathfrak{X}] := V \otimes_K K[\mathfrak{X}]$, *welches man durch Anwenden von* δ *auf die Koeffizienten von* f *erhält, also* $f^\delta = \sum_\nu \delta(c_\nu)\mathfrak{X}^\nu$ *für* $f = \sum_\nu c_\nu \mathfrak{X}^\nu$.

Existiert eine Fortsetzung wie in (i), *so ist diese eindeutig bestimmt.*

Beweis. Ist Bedingung (i) gegeben, so gilt für Polynome $f = \sum_\nu c_\nu \mathfrak{X}^\nu$ aus $K[\mathfrak{X}]$ die Gleichung

$$\delta'\big(f(x)\big) = \sum_\nu \delta(c_\nu)x^\nu + \sum_\nu c_\nu \delta'(x^\nu) = f^\delta(x) + \sum_{j\in J} \frac{\partial f}{\partial X_j}(x) \cdot v_j,$$

d. h. δ' ist als Fortsetzung zu δ durch die Gleichungen $\delta'(x_j) = v_j$, $j \in J$, eindeutig auf $K[x]$ festgelegt. Verwendet man dann für Elemente $a, b \in K[x]$, $b \neq 0$, die Quotientenregel

$$\delta'\Big(\frac{a}{b}\Big) = \frac{b\delta'(a) - a\delta'(b)}{b^2},$$

so ergibt sich dieselbe Eindeutigkeitsaussage für δ' auf ganz $K(x)$; alternativ kann man hierfür auch Satz 6 verwenden. Im Übrigen sieht man, dass die Gleichungen aus (ii) gelten, da $f_i(x)$ für alle $i \in I$ verschwindet.

Sei nun Bedingung (ii) gegeben. Dann kann man, wie leicht nachzurechnen ist, eine Derivation $\hat\delta\colon K[\mathfrak{X}] \longrightarrow V$ durch

$$\hat\delta(f) = f^\delta(x) + \sum_{j\in J} \frac{\partial f}{\partial X_j}(x) \cdot v_j$$

erklären; hierbei fasse man V unter Verwendung der gegebenen Abbildung $\pi\colon K[\mathfrak{X}] \longrightarrow L$ als $K[\mathfrak{X}]$-Modul auf. Speziell gilt $\hat\delta(f_i) = 0$ für alle $i \in I$ aufgrund der Gleichungen in (ii). Mit Hilfe der Produktregel sieht man dann $\hat\delta(gf_i) = 0$ für beliebiges $g \in K[\mathfrak{X}]$, so dass $\hat\delta$ auf dem von $(f_i)_{i\in I}$ in $K[\mathfrak{X}]$ erzeugten Ideal verschwindet, also auf dem Kern der Abbildung $\pi\colon K[\mathfrak{X}] \longrightarrow L$, $\mathfrak{X} \longmapsto x$. Somit induziert $\hat\delta$ eine Derivation $\overline{\delta}\colon K[x] \longrightarrow V$, die δ fortsetzt. Man kann dann die Quotientenregel oder Satz 6 benutzen, um $\overline{\delta}$ zu einer Derivation $\delta'\colon K(x) \longrightarrow V$ fortzusetzen. □

Der gerade bewiesene Satz 7 liefert ein nützliches Hilfsmittel zur Berechnung von $\Omega^1_{L/K}$ bzw. $\mathrm{Der}_K(L, L)$, indem er insbesondere zeigt, wie die Fortsetzungen der trivialen Derivation $K \longrightarrow L$ zu bestimmen sind. Man wird jedoch im Allgemeinen die Erweiterung L/K durch Zwischenkörper unterteilen, etwa $K \subset L' \subset L$, und zunächst die K-Derivationen von L' bestimmen. Anschließend muss man dann etwas über die Fortsetzbarkeit von K-Derivationen auf L' zu K-Derivationen auf L wissen, um insgesamt Informationen über die K-Derivationen von L zu erhalten. Dies ist der typische Fall für eine Anwendung von Satz 7. Alternativ kann man für eine Kette $K \subset L' \subset L$ auch die exakte Sequenz aus Satz 5 benutzen. Hierbei ist es wünschenswert, dass die Abbildung $\alpha\colon \Omega^1_{L'/K} \otimes_{L'} L \longrightarrow \Omega^1_{L/K}$ injektiv ist, was jedoch im Allgemeinen nicht automatisch der Fall ist. Man kann zeigen, dass die Injektivität der Abbildung α äquivalent zu der Bedingung ist, dass jede K-Derivation $L' \longrightarrow L$ eine Fortsetzung zu einer K-Derivation $L \longrightarrow L$ besitzt; vgl. Aufgabe 3.

Wir wollen nun die Aussage von Satz 7 zu Aussagen über Moduln von Differentialformen umformulieren.

Korollar 8. *Es sei L/K eine rein transzendente Körpererweiterung mit erzeugender Transzendenzbasis $(x_j)_{j\in J}$. Dann ist $(d_{L/K}(x_j))_{j\in J}$ eine Basis des L-Vektorraums $\Omega^1_{L/K}$.*

Beweis. Man benutze die Sätze 4 und 6. Alternativ kann man zumindest für eine endliche Transzendenzbasis $(x_j)_{j\in J}$ die Aussage von Satz 7 anwenden. □

Korollar 9. *Es sei L/K eine separable algebraische Körpererweiterung. Dann setzt sich jede Derivation $\delta\colon K \longrightarrow V$ in einen L-Vektorraum V eindeutig zu einer Derivation $\delta'\colon L \longrightarrow V$ fort, und es gilt $\Omega^1_{L/K} = 0$.*

Beweis. Sei $\delta\colon K \longrightarrow V$ eine Derivation in einen L-Vektorraum V, und sei L' ein Zwischenkörper zu L/K, so dass L'/K endlich ist. Dann ist L'/K nach dem Satz vom primitiven Element 3.6/12 einfach, etwa $L' = K(x)$ mit einem Element $x \in L$ und Minimalpolynom $f \in K[X]$ zu x. Sei $v \in V$. Die Bedingung aus Satz 7 für die Fortsetzbarkeit von δ zu einer Derivation $\delta'\colon K(x) \longrightarrow V$ mit $\delta'(x) = v$ lautet dann

$$f^\delta(x) + f'(x) \cdot v = 0.$$

Da f separabel ist, kann die Ableitung f' zu f nicht das Nullpolynom sein. Weiter gilt $f'(x) \neq 0$, da f' einen kleineren Grad als das Minimalpolynom f zu x hat. Daher ist v durch obige Gleichung eindeutig bestimmt, und es folgt, dass sich δ auf eindeutige Weise zu einer Derivation $\delta' \colon L' \longrightarrow V$ fortsetzt.

Hieraus kann man leicht folgern, dass sich δ auf eindeutige Weise zu einer Derivation $\delta' \colon L \longrightarrow V$ fortsetzt. Für jeden Zwischenkörper L' zu L/K, der endlich über K ist, können wir δ nämlich wie eben beschrieben zu einer Derivation $\delta' \colon L' \longrightarrow V$ fortsetzen. Da jede solche Fortsetzung eindeutig durch δ bestimmt ist und da L durch Teilkörper des Typs L' ausgeschöpft werden kann, ergibt sich insgesamt die eindeutige Fortsetzbarkeit von δ zu einer Derivation $L \longrightarrow V$.

Insbesondere setzt sich die triviale Derivation $K \longrightarrow L$ lediglich zur trivialen Derivation $L \longrightarrow L$ fort, woraus sich $\mathrm{Der}_K(L, L) = 0$ und somit $\Omega^1_{L/K} = 0$ ergibt. □

Die Fortsetzung von Derivationen ist in der Situation von Satz 7 besonders dann ein Problem, wenn die Erweiterung L/K nicht separabel ist.

Korollar 10. *Es sei K ein Körper der Charakteristik $p > 0$ und L/K eine rein inseparable Körpererweiterung vom Grad p, etwa $L = K(x)$ mit Minimalpolynom $f = X^p - c \in K[X]$ zu x. Weiter sei $\delta \colon K \longrightarrow V$ eine Derivation in einen L-Vektorraum V. Dann gilt*:

(i) *Ist $\delta' \colon L \longrightarrow V$ eine Derivation, die δ fortsetzt, so gilt $\delta(c) = 0$.*

(ii) *Hat man umgekehrt $\delta(c) = 0$, so existiert zu $v \in V$ genau eine Derivation $\delta' \colon L \longrightarrow V$ mit $\delta'(x) = v$, die δ fortsetzt. Insbesondere bildet $d_{L/K}(x)$ eine L-Basis von $\Omega^1_{L/K}$.*

Beweis. Mit Satz 7 schließen wir, dass sich δ genau dann zu einer Derivation $\delta' \colon L \longrightarrow V$ mit $\delta'(x) = v$ fortsetzen lässt, wenn die Gleichung

$$-\delta(c) + px^{p-1} \cdot v = 0$$

erfüllt ist, wenn also $\delta(c) = 0$ gilt. Im Falle der Fortsetzbarkeit kann allerdings der Wert $\delta'(x) = v$ beliebig vorgegeben werden. Somit ist $\mathrm{Der}_K(L, L)$ von Dimension 1 über L, und Gleiches gilt für $\Omega^1_{L/K}$, wobei $d_{L/K}(x)$ eine Basis bildet. □

Wir können nun die angestrebte Charakterisierung separabler Körpererweiterungen herleiten, wobei wir uns auf endlich erzeugte Erweiterungen beschränken wollen.

Theorem 11. *Es sei L/K eine endlich erzeugte Körpererweiterung, etwa des Typs $L = K(y_1, \ldots, y_r)$. Dann gilt*

$$\operatorname{transgrad}_K L \leq \dim_L \Omega^1_{L/K} \leq r,$$

wobei $\operatorname{transgrad}_K L = \dim_L \Omega^1_{L/K}$ *äquivalent zur Separabilität von L/K ist.*

Korollar 12. *Eine endlich erzeugte Körpererweiterung L/K ist genau dann separabel algebraisch, wenn $\Omega^1_{L/K} = 0$ gilt.*

Korollar 13. *Es sei L/K eine separable und endlich erzeugte Körpererweiterung. Für Elemente $x_1, \ldots, x_n \in L$ ist dann äquivalent:*

(i) *$x_1, \ldots, x_n$ bilden eine separierende Transzendenzbasis von L/K.*

(ii) *$d_{L/K}(x_1), \ldots, d_{L/K}(x_n)$ bilden eine L-Basis von $\Omega^1_{L/K}$.*

Die Aussage von Korollar 12 ist ein Spezialfall der Aussage von Theorem 11, deshalb die Bezeichnung "Korollar". Aus beweistechnischer Sicht ist Korollar 12 jedoch ein vorbereitendes Lemma, auf das wir uns im Beweis zu Theorem 11 stützen werden.

Wir beginnen daher mit dem *Beweis zu Korollar* 12. Ist L/K separabel algebraisch, so gilt stets $\Omega^1_{L/K} = 0$; vgl. Korollar 9. Sei also umgekehrt $\Omega^1_{L/K} = 0$ bekannt, was äquivalent zu $\operatorname{Der}_K(L, L) = 0$ ist. Man wähle eine Transzendenzbasis $x_1, \ldots, x_n$ von L/K. Dann ist L eine endliche algebraische Erweiterung von $K(x_1, \ldots, x_n)$. Ist diese Erweiterung sogar separabel, so sehen wir mit den Korollaren 8 und 9, dass $\operatorname{Der}_K(L, L)$ von der Dimension n über L ist. Folglich gilt $n = 0$, und L/K ist separabel algebraisch.

Sei nun für $p = \operatorname{char} K > 0$ die Erweiterung $K(x_1, \ldots, x_n) \subset L$ nicht separabel. Dann gibt es einen Zwischenkörper L' zu L/K, so dass L/L' rein inseparabel vom Grad p ist. Gemäß Korollar 10 existiert eine nicht-triviale L'-Derivation $L \longrightarrow L$, also insbesondere eine nicht-triviale K-Derivation $L \longrightarrow L$. Dies steht aber im Widerspruch zu $\operatorname{Der}_K(L, L) = 0$, so dass der inseparable Fall nicht auftreten kann. Korollar 12 ist damit bewiesen. □

Beweis zu Theorem 11. Es folgt mit den Sätzen 4 und 6, dass $\Omega^1_{L/K}$ von den Elementen $d_{L/K}(y_1), \ldots, d_{L/K}(y_r)$ erzeugt wird, also ergibt sich $\dim_L \Omega^1_{L/K} \leq r$. Man wähle nun Elemente $x_1, \ldots, x_n \in L$ aus, so dass die Differentialformen $d_{L/K}(x_1), \ldots, d_{L/K}(x_n)$ eine Basis von $\Omega^1_{L/K}$ bilden. Sei $L' = K(x_1, \ldots, x_n)$. In der exakten Sequenz

$$\Omega^1_{L'/K} \otimes_{L'} L \xrightarrow{\alpha} \Omega^1_{L/K} \xrightarrow{\beta} \Omega^1_{L/L'} \longrightarrow 0$$

aus Satz 5 ist dann die Abbildung α surjektiv, so dass $\Omega^1_{L/L'} = 0$ folgt. Die Erweiterung L/L' ist also, wie wir gesehen haben, separabel algebraisch, und es folgt

$$\operatorname{transgrad}_K L = \operatorname{transgrad}_K L' \leq n = \dim_L \Omega^1_{L/K}.$$

Im Falle der Gleichheit sind $x_1, \ldots, x_n$ notwendig algebraisch unabhängig über K, so dass die Erweiterung L/K separabel erzeugt und damit separabel ist; vgl. 7.3/6. Ist umgekehrt L/K eine endlich erzeugte separable Körpererweiterung vom Transzendenzgrad n, so ist L/K nach 7.3/7 separabel erzeugt, und es ergibt sich aus den Korollaren 8 und 9, dass $\operatorname{Der}_K(L, L)$ und folglich ebenfalls $\Omega^1_{L/K}$ von der Dimension n über L sind. □

Beweis zu Korollar 13. Man betrachte die exakte Sequenz

$$\Omega^1_{L'/K} \otimes_{L'} L \xrightarrow{\alpha} \Omega^1_{L/K} \xrightarrow{\beta} \Omega^1_{L/L'} \longrightarrow 0$$

aus Satz 5 mit $L' = K(x_1, \ldots, x_n)$. Wenn $x_1, \ldots, x_n$ eine separierende Transzendenzbasis von L/K bilden, so gilt $\Omega^1_{L/L'} = 0$ nach Korollar 12 oder Korollar 9. Die Abbildung α ist also surjektiv. Sie ist aber sogar bijektiv, denn es gilt $\dim_L(\Omega^1_{L'/K} \otimes_{L'} L) = n$ nach Korollar 8 sowie $\dim \Omega^1_{L/K} = n$ nach Theorem 11. Da $d_{L'/K}(x_1), \ldots, d_{L'/K}(x_n)$ eine Basis von $\Omega^1_{L'/K}$ bilden, gilt dasselbe aufgrund der Bijektivität von α für die Bilder in $\Omega^1_{L/K}$.

Ist umgekehrt $d_{L/K}(x_1), \ldots, d_{L/K}(x_n)$ eine Basis von $\Omega^1_{L/K}$, so schließt man wie im Beweis zu Theorem 11, dass $x_1, \ldots, x_n$ eine separierende Transzendenzbasis von L/K bilden. □

Die Aussage von Korollar 13 zeigt erneut, indem man Satz 4 in Verbindung mit Satz 6 benutzt, dass man bei einer separablen, endlich erzeugten Körpererweiterung L/K ein Erzeugendensystem stets zu einer separierenden Transzendenzbasis verkleinern kann.

Lernkontrolle und Prüfungsvorbereitung

1. Was versteht man unter einer R-Derivation einer R-Algebra A in einen A-Modul M? Gib ein Beispiel einer R-Derivation für den Fall, dass A ein Polynomring über R ist, in einer oder mehreren Variablen.
2. Leite für eine Derivation die Quotientenregel aus der Produktregel her.
3. Erkläre für eine R-Algebra A den Modul $\Omega^1_{A/R}$ der relativen Differentialformen von A über R. Wie lautet die universelle Eigenschaft von $\Omega^1_{A/R}$? Beweise die Existenz des Differentialmoduls $\Omega^1_{A/R}$.
4. Es sei A eine R-Algebra und $x = (x_i)_{i\in I}$ ein System von Elementen aus A, welches A als R-Algebra erzeugt. Zeige, dass x ein Erzeugendensystem von $\Omega^1_{A/R}$ als A-Modul induziert. Was weiß man genauer für den Fall, dass x algebraisch unabhängig über R ist?
5. Sei $\tau\colon A \longrightarrow B$ ein Homomorphismus von R-Algebren. Zeige, dass τ eine kanonische exakte Sequenz auf dem Niveau der Differentialmoduln induziert.
6. Es sei A eine R-Algebra. Zeige, dass die Bildung des Differentialmoduls $\Omega^1_{A/R}$ verträglich mit dem Übergang von A zu einer Lokalisierung A_S ist, für ein multiplikatives System $S \subset A$.
7. In welchen Fällen kann man für eine Körpererweiterung L/K den Differentialmodul $\Omega^1_{L/K}$ als Dualraum des L-Vektorraums der Derivationen $\mathrm{Der}_K(L,L)$ deuten?

+8. Betrachte eine Körpererweiterung L/K und eine Derivation $\delta\colon K \longrightarrow V$ in einen L-Vektorraum V. Charakterisiere die Fortsetzbarkeit von δ zu einer Derivation $\delta'\colon L \longrightarrow V$ durch geeignete Bedingungen (mit Begründung).

9. Es sei L/K eine rein transzendente Körpererweiterung. Wie gelangt man von einer erzeugenden Transzendenzbasis von L/K zu einer L-Basis von $\Omega^1_{L/K}$?
10. Es sei L/K eine separable algebraische Körpererweiterung. Zeige, dass sich jede Derivation $\delta\colon K \longrightarrow V$ in einen L-Vektorraum V eindeutig zu einer Derivation $\delta'\colon L \longrightarrow V$ fortsetzen lässt und dass $\Omega^1_{L/K} = 0$ gilt.
11. Kläre für einen Körper der Charakteristik $p > 0$ die Fortsetzbarkeit von Derivationen bezüglich einer rein inseparablen Körpererweiterung vom Grad p.
12. Kläre für eine endlich erzeugte Körpererweiterung L/K die Beziehungen zwischen dem Transzendenzgrad $\mathrm{transgrad}_K L$, der Dimension $\dim_L \Omega^1_{L/K}$ und der Anzahl der Erzeugenden von L/K.
13. Wie lässt sich für eine endlich erzeugte Körpererweiterung L/K die Separabilität mittels $\Omega^1_{L/K}$ charakterisieren? Was bedeutet hierbei $\Omega^1_{L/K} = 0$?

14. Es sei L/K eine endlich erzeugte separable Körpererweiterung. Zeige, dass gegebene Elemente $x_1, \ldots, x_n \in L$ genau dann eine separierende Transzendenzbasis von L/K bilden, wenn sie zu einer L-Basis von $\Omega^1_{L/K}$ Anlass geben.

Übungsaufgaben

1. *Ist für beliebige Körpererweiterungen L/K die Bedingung $\Omega^1_{L/K} = 0$ äquivalent dazu, dass L/K separabel algebraisch ist*?

2. Es sei L/K eine Körpererweiterung in Charakteristik 0. Zeige, dass sich jede Derivation $K \longrightarrow V$ in einen L-Vektorraum V zu einer Derivation $L \longrightarrow V$ fortsetzt.

3. Betrachte zu Körpererweiterungen $R \subset K \subset L$ die Abbildung

$$\alpha \colon \Omega^1_{K/R} \otimes_K L \longrightarrow \Omega^1_{L/R}, \qquad d_{K/R}(x) \otimes a \longmapsto a \cdot d_{L/R}(x).$$

   Zeige, dass α genau dann injektiv ist, wenn sich jede R-Derivation $K \longrightarrow L$ zu einer R-Derivation $L \longrightarrow L$ fortsetzt.

4. Es sei L/K eine endlich erzeugte Körpererweiterung, $L = K(x_1, \ldots, x_n)$. Der Kern des K-Homomorphismus $K[X_1, \ldots, X_n] \longrightarrow L$, $X_i \longmapsto x_i$, werde von Polynomen $f_1, \ldots, f_r \in K[X_1, \ldots, X_n]$ erzeugt, welche der Bedingung

$$\operatorname{rg}\left(\frac{\partial f_i}{\partial X_j}(x)\right)_{\substack{i=1\ldots r\\ j=1\ldots n}} = r$$

   genügen. Zeige, dass L/K eine separable Erweiterung vom Transzendenzgrad $n - r$ ist.

5. Es sei L/K eine Körpererweiterung in Charakteristik $p > 0$ mit $L^p \subset K$. Weiter sei $(x_i)_{i \in I}$ eine *p-Basis* von L/K, d. h. ein p-freies System (vgl. Aufgabe 7 aus Abschnitt 7.3), welches die Erweiterung L/K erzeugt, und sei $\delta \colon K \longrightarrow V$ eine Derivation in einen L-Vektorraum V. Zeige für $c_i = x_i^p$:

   (i) Wenn eine Derivation $\delta' \colon L \longrightarrow V$ existiert, die δ fortsetzt, dann gilt $\delta(c_i) = 0$ für alle $i \in I$.

   (ii) Gilt umgekehrt $\delta(c_i) = 0$ für alle $i \in I$, so gibt es zu einem System $(v_i)_{i \in I}$ von Elementen aus V genau eine Fortsetzung $\delta' \colon L \longrightarrow V$ von δ mit $\delta'(x_i) = v_i$ für alle i.

   (iii) Die Differentialformen $d_{L/K}(x_i)$, $i \in I$, bilden eine L-Basis von $\Omega^1_{L/K}$.

6. Zeige, dass eine Körpererweiterung L/K genau dann separabel ist, wenn sich jede Derivation $K \longrightarrow L$ zu einer Derivation $L \longrightarrow L$ fortsetzt. (*Hinweis*: Benutze Aufgabe 2 sowie in Charakteristik $p > 0$ Aufgabe 5 in Verbindung mit der Charakterisierung separabler Erweiterungen aus Aufgabe 7 in Abschnitt 7.3.)

Anhang

Lösungshinweise zu den Aufgaben

Aufgaben, die im Text in *Kursiv-Druck* erscheinen, sind speziell dazu gedacht, das Verständnis des gebotenen Stoffes zu erleichtern und zum Nachdenken anzuregen. Im Gegensatz zu den restlichen Übungsaufgaben mehr klassischen Typs handelt es sich überwiegend um Fragestellungen, die sich gut für eine Diskussion in Form eines Gesprächs eignen. Nur zu diesen Aufgaben werden nachfolgend Lösungshinweise und Erläuterungen gegeben.

1.1, Aufg. 1. Natürlich implizieren die Bedingungen (ii) und (iii) aus 1.1/1 die Bedingungen (ii′) und (iii′) aus 1.1/2. Sei umgekehrt G eine Menge mit einer assoziativen Verknüpfung, derart dass es ein links-neutrales Element $e \in G$ gibt, sowie zu jedem Element $a \in G$ ein links-inverses Element $b \in G$. Wir zeigen zunächst, dass b stets auch rechts-invers zu a ist. Gelte also $ba = e$. Dann existiert zu b ein links-inverses Element c, so dass also $cb = e$ gilt. Hieraus folgt aber

$$ab = eab = cbab = cb = e,$$

d. h. wenn b ein links-inverses Element zu a ist, so ist b auch rechts-invers zu a. Mithin ist Bedingung 1.1/1 (iii) erfüllt. Es bleibt nun noch zu zeigen, dass das links-neutrale Element $e \in G$ auch rechts-neutral ist. Sei also $a \in G$. Ist dann $b \in G$ ein links-inverses Element zu a, so ist b gleichzeitig auch rechts-invers zu a, wie wir gesehen haben, und es folgt 1.1/1 (ii) mit

$$ae = aba = ea = a.$$

S. Bosch, *Algebra*, https://doi.org/10.1007/978-3-662-67464-2

1.1, Aufg. 2. Wir werden zeigen, dass es aufgrund unterschiedlicher gruppentheoretischer Gegebenheiten keinen Isomorphismus zwischen $\mathbb{Q}$ und $\mathbb{Q}_{>0}$ geben kann. Zu jedem $x \in \mathbb{Q}$ gibt es ein $y \in \mathbb{Q}$ mit $x = y + y$, nämlich $y = \frac{1}{2}x$. Die entsprechende Aussage aber, dass es zu jedem $x \in \mathbb{Q}_{>0}$ ein $y \in \mathbb{Q}_{>0}$ mit $x = y \cdot y$ gibt, ist falsch. Denn zu $x = 2$ gibt es bekanntermaßen keine rationale Zahl y, deren Quadrat 2 ist; dies beweist man unter Benutzung der eindeutigen Primfaktorzerlegung ganzer Zahlen. Hat man nun aber einen Isomorphismus $\varphi\colon \mathbb{Q} \longrightarrow \mathbb{Q}_{>0}$, so gibt es aufgrund der Surjektivität insbesondere ein Element $a \in \mathbb{Q}$ mit $\varphi(a) = 2$. Mit $b = \frac{1}{2}a$ folgt dann $\varphi(b)^2 = \varphi(2b) = \varphi(a) = 2$, im Widerspruch dazu, dass 2 keine rationale Quadratwurzel besitzt.

1.2, Aufg. 1. Da H vom Index 2 in G ist, zerfällt G in zwei disjunkte Linksnebenklassen zu H. Eine davon ist H, die andere stimmt überein mit dem Komplement von H in G, welches wir mit H' bezeichnen wollen. Die gleiche Argumentation gilt auch für die Rechtsnebenklassen zu H, so dass H' sowohl eine Links- als auch eine Rechtsnebenklasse zu H ist. Sei nun $a \in G$. Für $a \in H$ gilt trivialerweise $aH = Ha$. Hat man aber $a \notin H$, so sind die beiden Nebenklassen aH und Ha jeweils verschieden von H, stimmen also mit H' überein, so dass auch in diesem Falle $aH = Ha$ gilt. Somit ist H Normalteiler in G.

Um zu sehen, dass eine Untergruppe vom Index 3 nicht notwendig ein Normalteiler zu sein braucht, betrachte man die symmetrische Gruppe $\mathfrak{S}_3$. Sei $\sigma \in \mathfrak{S}_3$ diejenige Permutation, welche die Zahlen 1 und 2 vertauscht sowie 3 festlässt. Es ist dann $H := \{\mathrm{id}, \sigma\} \subset \mathfrak{S}_3$ eine Untergruppe der Ordnung 2, also nach dem Satz von Lagrange 1.2/3 wegen $\operatorname{ord} \mathfrak{S}_3 = 6$ eine Untergruppe vom Index 3. Sei nun $\tau \in \mathfrak{S}_3$ die Permutation, welche 1 festlässt und 2 mit 3 vertauscht. Dann vertauscht $\tau \circ \sigma \circ \tau^{-1}$ die Zahlen 1 und 3 und lässt 2 fest, gehört also nicht zu H. Somit hat man $\tau H \neq H\tau$, d. h. H ist kein Normalteiler in $\mathfrak{S}_3$.

1.2, Aufg. 2. Wir wollen zunächst nur annehmen, dass N eine Untergruppe in G ist. Dann bildet die Linkstranslation $\tau_g\colon G \longrightarrow G, a \longmapsto ga$, mit einem Element $g \in G$ Linksnebenklassen zu N wieder auf ebensolche ab, induziert also eine Abbildung $\overline{\tau}_g\colon X \longrightarrow X$, die wir durch $aN \longmapsto gaN$ beschreiben können. Da aus $gaN = ga'N$ mit $a, a' \in G$ die Gleichung $aN = a'N$ folgt, ist $\overline{\tau}_g$ injektiv. Andererseits schließt man aus der Surjektivität von τ_g aber auch die Surjektivität von $\overline{\tau}_g$, so dass $\overline{\tau}_g$ sogar bijektiv ist, also $\overline{\tau}_g \in S(X)$ gilt. Die Zuordnung $g \longmapsto \overline{\tau}_g$ definiert daher eine Abbildung $\varphi\colon G \longrightarrow S(X)$,

und dies ist sogar ein Gruppenhomomorphismus, wie man aus der Relation $\tau_{gg'} = \tau_g \circ \tau_{g'}$ für $g, g' \in G$ schließt. Wir wollen nun den Kern von φ bestimmen. Für $g \in G$ gilt genau dann $g \in \ker\varphi$, wenn $\overline{\tau}_g \colon X \longrightarrow X$ die identische Abbildung ist, d. h. wenn $gaN = aN$ für alle $a \in G$ gilt. Letztere Gleichung ist äquivalent zu $ga \in aN$ bzw. zu $g \in aNa^{-1}$, so dass wir $\ker\varphi = \bigcap_{a\in G} aNa^{-1}$ erhalten. Ist nun N Normalteiler in G, so gilt jeweils $aNa^{-1} = N$ und folglich $\ker\varphi = N$. Setzen wir dann noch $\overline{G} = \varphi(G)$, so haben wir gezeigt, dass es zu jedem Normalteiler $N \subset G$ eine Gruppe $\overline{G}$ mit einem surjektiven Gruppenhomomorphismus $p \colon G \longrightarrow \overline{G}$ gibt, welcher $\ker p = N$ erfüllt.

Wir könnten nun $\overline{G}$ als "die" Faktorgruppe von G nach N bezeichnen. Insbesondere würde das Sinn machen, wenn wir unter $\overline{G}$ die oben konkret konstruierte Untergruppe $\varphi(G) \subset S(G)$ verstehen würden. Aber es ist vorteilhafter, hier einen etwas allgemeineren Standpunkt einzunehmen und ein beliebiges Paar $(\overline{G}, p)$, wobei $p \colon G \longrightarrow \overline{G}$ ein surjektiver Gruppenhomomorphismus mit $\ker p = N$ ist, als "Faktorgruppe" von G nach N zu bezeichnen. Für ein solches $p \colon G \longrightarrow \overline{G}$ lässt sich genauso wie für den in Abschnitt 1.2 konkret konstruierten surjektiven Gruppenhomomorphismus $\pi \colon G \longrightarrow G/N$ der Homomorphiesatz 1.2/6 herleiten; die Beweisführung ist dieselbe. Als Konsequenz erhält man, dass alle "Faktorgruppen" $(\overline{G}, p)$ zueinander kanonisch isomorph sind, insbesondere auch zu der konkret konstruierten "Faktorgruppe" $(G/N, \pi)$.

1.3, Aufg. 1. Zunächst stellt man fest, dass die Verknüpfung "$\circ$" kommutativ ist. Um die Assoziativität nachzuprüfen, wähle man Elemente $a, b, c \in G_m$. Nach Definition der Verknüpfung "$\circ$" gibt es Zahlen $q, q' \in \mathbb{Z}$ mit

$$a + b = qm + (a \circ b), \qquad (a \circ b) + c = q'm + \big((a \circ b) \circ c\big),$$

woraus

$$a + b + c = (q + q')m + \big((a \circ b) \circ c\big)$$

folgt. Dies bedeutet, dass $(a \circ b) \circ c$ der Rest von $a + b + c$ bei Division durch m ist. Analog sieht man, dass auch $a \circ (b \circ c)$ gleich dem Rest von $a + b + c$ bei Division durch m ist. Also gilt $(a \circ b) \circ c = a \circ (b \circ c)$, d. h. die Verknüpfung "$\circ$" ist assoziativ. Die übrigen Axiome sind leicht einzusehen: 0 ist ein neutrales Element bezüglich "$\circ$", und für $a \in G_m$, $a \neq 0$, ist $m - a$ ein inverses Element zu a. Also ist G_m eine kommutative Gruppe.

Um zu sehen, dass G_m isomorph zu $\mathbb{Z}/m\mathbb{Z}$ ist, betrachten wir die Bijektion $\iota \colon G_m \longrightarrow \mathbb{Z}/m\mathbb{Z}$, $a \longmapsto a + m\mathbb{Z}$. Da sich für $a, b \in G_m$ die Zahlen

$a \circ b$ und $a + b$ höchstens um ein Vielfaches von m unterscheiden, gilt $(a \circ b) + m\mathbb{Z} = (a + b) + m\mathbb{Z}$ und folglich $\iota(a \circ b) = \iota(a) + \iota(b)$. Somit ist ι ein Isomorphismus von Gruppen.

1.3, Aufg. 2. Man betrachte den durch $a \longmapsto a+m\mathbb{Z}$ gegebenen Epimorphismus $\pi\colon \mathbb{Z} \longrightarrow \mathbb{Z}/m\mathbb{Z}$. Ist dann $\overline{H} \subset \mathbb{Z}/m\mathbb{Z}$ eine Untergruppe, so ist $\pi^{-1}(\overline{H})$ eine Untergruppe von $\mathbb{Z}$, welche $m\mathbb{Z}$ enthält. Da umgekehrt das Bild $\pi(H)$ einer Untergruppe $H \subset \mathbb{Z}$ stets eine Untergruppe in $\mathbb{Z}/m\mathbb{Z}$ ergibt, überlegt man sich leicht, dass die Zuordnung $\overline{H} \longmapsto \pi^{-1}(\overline{H})$ eine Bijektion zwischen den Untergruppen $\overline{H} \subset \mathbb{Z}/m\mathbb{Z}$ und denjenigen Untergruppen $H \subset \mathbb{Z}$ definiert, die $m\mathbb{Z}$ enthalten.

Wir wollen zunächst alle Untergruppen $H \subset \mathbb{Z}$ bestimmen, die $m\mathbb{Z}$ enthalten. Sei etwa H eine solche Untergruppe. Nach 1.3/4 ist H zyklisch, etwa $H = d\mathbb{Z}$. Aus der Inklusion $m\mathbb{Z} \subset d\mathbb{Z}$ folgt, dass m eine Darstellung $m = cd$ mit $c \in \mathbb{Z}$ hat, also d ein Teiler von m ist. Umgekehrt hat man natürlich für jeden Teiler d von m die Inklusion $m\mathbb{Z} \subset d\mathbb{Z}$, so dass die Untergruppen von $\mathbb{Z}$, welche $m\mathbb{Z}$ enthalten, gerade die Gruppen des Typs $d\mathbb{Z}$ sind, wobei d ein Teiler von m ist. Da das erzeugende Element d einer Untergruppe $d\mathbb{Z} \subset \mathbb{Z}$ bis auf das Vorzeichen eindeutig bestimmt ist, entsprechen diese Gruppen in bijektiver Weise den positiven Teilern von m.

Um nun alle Untergruppen von $\mathbb{Z}/m\mathbb{Z}$ zu erhalten, brauchen wir lediglich den Epimorphismus π auf die gerade bestimmten Untergruppen $d\mathbb{Z}$ anzuwenden, wobei also d die positiven Teiler von m durchläuft. Da $d\mathbb{Z}$ zyklisch ist mit erzeugendem Element d, ist das Bild $\pi(d\mathbb{Z})$ ebenfalls zyklisch, mit erzeugendem Element $\pi(d) = d + m\mathbb{Z}$. Die Ordnung dieser Gruppe bestimmt sich zu $\frac{m}{d}$, also ist der Index von $\pi(d\mathbb{Z})$ in $\mathbb{Z}/m\mathbb{Z}$ gleich d; vgl. 1.2/3. Somit können wir formulieren: Zu jedem positiven Teiler d von m gibt es genau eine Untergruppe $\overline{H} \subset \mathbb{Z}/m\mathbb{Z}$ vom Index d, nämlich die von $d + m\mathbb{Z}$ erzeugte zyklische Untergruppe, und es gibt außer den Untergruppen dieses Typs keine weiteren in $\mathbb{Z}/m\mathbb{Z}$. Indem wir benutzen, dass jede zyklische Gruppe der Ordnung m isomorph zu $\mathbb{Z}/m\mathbb{Z}$ ist, können wir auch sagen: In einer zyklischen Gruppe der Ordnung m gibt es zu jedem positiven Teiler d von m genau eine Untergruppe vom Index d und, unter Benutzung von 1.2/3, genau eine Untergruppe der Ordnung d.

Abschließend sei bemerkt, dass man dieses Resultat auch in direkter Weise ohne die Betrachtung entsprechender Untergruppen von $\mathbb{Z}$ gewinnen kann, wenn man Eigenschaften des größten gemeinsamen Teilers ganzer Zahlen benutzt. Ein wesentlicher Schritt des Beweises besteht darin, zu zei-

gen, dass eine gegebene Untergruppe $H \subset \mathbb{Z}/m\mathbb{Z}$ bereits von der Restklasse $\overline{d}$ eines geeigneten Teilers d von m erzeugt wird. Um dies einzusehen, wähle man Elemente $a_1, \ldots, a_r \in \mathbb{Z}$, deren Restklassen $\overline{a}_1, \ldots, \overline{a}_r \in \mathbb{Z}/m\mathbb{Z}$ die Gruppe H erzeugen. Sei d der größte gemeinsame Teiler der Elemente $a_1, \ldots, a_r, m$. Es gibt dann eine Gleichung des Typs $d = c_1a_1 + \ldots + c_ra_r + cm$ mit Koeffizienten $c_1, \ldots, c_r, c \in \mathbb{Z}$, vgl. etwa 2.4/13, und man kann hieraus schließen, dass H bereits von der Restklasse $\overline{d}$ zu d erzeugt wird.

2.1, Aufg. 1. Man erhält $0 \cdot a + 0 \cdot a = (0 + 0) \cdot a = 0 \cdot a$ und somit $0 \cdot a = 0$ für alle $a \in R$, indem man das Distributivgesetz anwendet. Weiter gilt $a \cdot b + (-a) \cdot b = (a + (-a)) \cdot b = 0 \cdot b = 0$, d. h. es ist $(-a) \cdot b$ invers zu $a \cdot b$ bezüglich der Addition, also $(-a) \cdot b = -(a \cdot b)$.

2.1, Aufg. 2. Bei der in 2.1 beschriebenen Konstruktion des Polynomrings $R[X]$ wurde nicht benutzt, dass der Ring R kommutativ ist. Wir können also für jeden nicht notwendig kommutativen Ring R den Polynomring $R[X]$ bilden, wobei die resultierende Multiplikation in $R[X]$ der Eigenschaft $aX = Xa$ für $a \in R$ genügt. Ist weiter $R \subset R'$ eine Erweiterung nicht notwendig kommutativer Ringe, so können wir in gewohnter Weise Elemente $x \in R'$ in Polynome aus $R[X]$ einsetzen. Für $f, g \in R[X]$ und $x \in R'$ gilt dann $(f + g)(x) = f(x) + g(x)$, aber die Gleichung $(f \cdot g)(x) = f(x) \cdot g(x)$ ist in der Regel nur dann erfüllt, wenn x mit den Elementen aus R vertauschbar ist, wenn also $ax = xa$ für $a \in R$ gilt. Wählt man insbesondere $x \in R$ und betrachtet die triviale Erweiterung $R \subset R$, so wird ersichtlich, dass man Polynomringe, wie sie in 2.1 definiert wurden, nur im Falle eines *kommutativen* Koeffizientenrings R verwenden sollte. Der Ring R', dessen Elemente man in Polynome aus $R[X]$ einsetzen möchte, braucht jedoch nicht unbedingt kommutativ zu sein. Es genügt, wenn die Elemente aus R mit denjenigen aus R' vertauschbar sind.

2.2, Aufg. 1. Aus $\mathfrak{a} = \sum_{i=1}^{m} Ra_i$ und $\mathfrak{b} = \sum_{j=1}^{n} Rb_j$ ergibt sich natürlich $\mathfrak{a} + \mathfrak{b} = \sum_{i=1}^{m} Ra_i + \sum_{j=1}^{n} Rb_j$, d. h. $a_1, \ldots, a_m, b_1, \ldots, b_n$ erzeugen das Ideal $\mathfrak{a} + \mathfrak{b}$. Als Nächstes wollen wir zeigen, dass die Elemente a_ib_j, $i = 1, \ldots, m$, $j = 1, \ldots, n$, ein Erzeugendensystem von $\mathfrak{a} \cdot \mathfrak{b}$ bilden. Sei $\mathfrak{q}$ das von diesen Elementen erzeugte Ideal. Da stets $a_ib_j \in \mathfrak{a} \cdot \mathfrak{b}$ gilt, folgt $\mathfrak{q} \subset \mathfrak{a} \cdot \mathfrak{b}$. Um die umgekehrte Inklusion zu zeigen, betrachte man ein Element $z \in \mathfrak{a} \cdot \mathfrak{b}$. Dann ist z eine endliche Summe der Form $z = \sum_\lambda \alpha_\lambda\beta_\lambda$ mit Elementen $\alpha_\lambda \in \mathfrak{a}$, $\beta_\lambda \in \mathfrak{b}$, und es gibt Elemente $c_{\lambda i}, d_{\lambda j} \in R$ mit $\alpha_\lambda = \sum_{i=1}^{m} c_{\lambda i}a_i$ sowie $\beta_\lambda = \sum_{j=1}^{n} d_{\lambda j}b_j$. Daraus ergibt sich aber $\alpha_\lambda\beta_\lambda = \sum_{i,j} c_{\lambda i}d_{\lambda j}a_ib_j \in \mathfrak{q}$ und somit $z \in \mathfrak{q}$. Also gilt $\mathfrak{q} = \mathfrak{a} \cdot \mathfrak{b}$, und die a_ib_j erzeugen das Ideal $\mathfrak{a} \cdot \mathfrak{b}$.

Für das Ideal $\mathfrak{a} \cap \mathfrak{b}$ kann man nicht in so einfacher Weise ein Erzeugendensystem aus den a_i und den b_j konstruieren. Als Beispiel betrachte man den Fall $R = \mathbb{Z}$. Es wird dann $\mathfrak{a}$ vom größten gemeinsamen Teiler a aller a_i erzeugt und entsprechend $\mathfrak{b}$ vom größten gemeinsamen Teiler b aller b_j; Aussagen dieses Typs werden beispielsweise in 2.4/13 bewiesen. Weiter wird das Ideal $\mathfrak{a} \cap \mathfrak{b}$ vom kleinsten gemeinsamen Vielfachen von a und b erzeugt; vgl. hierzu ebenfalls 2.4/13. Diese Beschreibung eines erzeugenden Elementes von $\mathfrak{a} \cap \mathfrak{b}$ gilt jedoch nur in Hauptidealringen, in allgemeineren Ringen ist die Lage wesentlich unübersichtlicher.

2.2, Aufg. 2. Es seien $\mathfrak{a}, \mathfrak{b}$ Ideale eines Rings R. Wir behaupten, dass $\mathfrak{a} \cup \mathfrak{b}$ genau dann ein Ideal in R ist, wenn $\mathfrak{a} \subset \mathfrak{b}$ oder $\mathfrak{b} \subset \mathfrak{a}$ gilt. Ist eine dieser Inklusionen gegeben, etwa $\mathfrak{a} \subset \mathfrak{b}$, so ist natürlich $\mathfrak{a} \cup \mathfrak{b} = \mathfrak{b}$ ein Ideal in R. Hat man umgekehrt $\mathfrak{a} \subsetneq \mathfrak{b}$ und $\mathfrak{b} \subsetneq \mathfrak{a}$, so existiert ein Element $a \in \mathfrak{a}$, welches nicht zu $\mathfrak{b}$ gehört, sowie ein Element $b \in \mathfrak{b}$, welches nicht zu $\mathfrak{a}$ gehört. Hieraus folgt, dass $a + b$ weder in $\mathfrak{a}$ noch in $\mathfrak{b}$ enthalten sein kann, so dass $\mathfrak{a} \cup \mathfrak{b}$ nicht abgeschlossen unter der Addition ist, also insbesondere kein Ideal sein kann. Unsere Behauptung ist also bewiesen.

Für eine Familie $(\mathfrak{a}_i)_{i \in I}$ von Idealen in R, die aus mehr als zwei Elementen besteht, kann man nicht so leicht entscheiden, ob die Vereinigung $\mathfrak{a} = \bigcup_{i \in I} \mathfrak{a}_i$ wieder ein Ideal ist. Natürlich ist $\mathfrak{a}$ abgeschlossen unter der Multiplikation mit Elementen aus R sowie unter der Inversenbildung bezüglich der Addition. Daher ist nur zu testen, ob $\mathfrak{a}$ abgeschlossen unter der Addition ist, d. h. ob für $a, b \in \mathfrak{a}$ stets $a + b \in \mathfrak{a}$ gilt. Eine hinreichende Bedingung hierfür ist z. B., dass es zu je zwei Indizes $i, j \in I$ und Elementen $a \in \mathfrak{a}_i$, $b \in \mathfrak{a}_j$ stets einen Index $k \in I$ mit $a, b \in \mathfrak{a}_k$ gibt. So ist beispielsweise die Vereinigung einer aufsteigenden Folge von Idealen $\mathfrak{a}_1 \subset \mathfrak{a}_2 \subset \ldots$ wieder ein Ideal.

2.2, Aufg. 3. Am einfachsten ist es, alle Ideale im Ring K^2 zu bestimmen. Wir behaupten, dass es außer 0, $K \times 0$, $0 \times K$, K^2 keine weiteren Ideale in K^2 gibt. Um dies zu zeigen, betrachte man ein Ideal $\mathfrak{a} \subset K^2$. Falls $\mathfrak{a}$ ein Element (a, b) mit $a \neq 0 \neq b$ enthält, so gilt $(1, 1) = (a^{-1}, b^{-1})(a, b) \in \mathfrak{a}$, d. h. $\mathfrak{a}$ enthält das Einselement von K^2, und es gilt $\mathfrak{a} = K^2$. Gibt es in $\mathfrak{a}$ aber kein Element (a, b) mit $a \neq 0 \neq b$, so besteht $\mathfrak{a}$ nur aus Elementen des Typs $(a, 0)$ oder $(0, b)$. Wegen $(a, 0) + (0, b) = (a, b)$, können die Elemente $(a, 0)$ und $(0, b)$ in nicht-trivialer Form nicht gleichzeitig in $\mathfrak{a}$ auftreten. Wir dürfen daher etwa annehmen, dass alle Elemente von $\mathfrak{a}$ von der Form $(a, 0)$ sind. Dann ist $\mathfrak{a}$ entweder das Nullideal, oder es gibt in $\mathfrak{a}$ ein Element

$(a,0)$ mit $a \neq 0$. Im letzteren Fall hat man $(1,0) = (a^{-1},1)(a,0) \in \mathfrak{a}$ und folglich $\mathfrak{a} = K \times 0$.

Insbesondere ist ersichtlich, dass alle Ideale auch Untervektorräume von K^2 sind. Dass dies so ist, hat einen allgemeinen Grund. Betrachten wir nämlich die sogenannte Diagonaleinbettung $K \longrightarrow K^2$, $a \longmapsto (a,a)$, so können wir K mit seinem Bild Δ in K^2 identifizieren und $K = \Delta$ auf diese Weise als Unterring von K^2 auffassen. Für Elemente $a \in K$ und $v \in K^2$ liefert dann das Produkt av im Sinne von K^2 als K-Vektorraum dasselbe, als wenn wir av im Sinne der Ringmultiplikation von K^2 berechnen. Da Ideale abgeschlossen unter der Multiplikation mit K^2 sind, sieht man nochmals ein, dass jedes Ideal in K^2 ein K-Untervektorraum von K^2 ist. Gleiches können wir aber auch für jeden Unterring von K^2 schließen, sofern dieser die Diagonale Δ enthält. Aus Dimensionsgründen gibt es daher keinen Unterring von K^2, der in echter Weise zwischen Δ und K^2 gelegen ist. Im Übrigen sehen wir auch, dass Δ ein Beispiel eines Untervektorraums von K^2 ist, der nicht zugleich die Eigenschaften eines Ideals hat. Es ist Δ übrigens der einzige echte Untervektorraum, der zugleich ein Unterring von K^2 ist.

Abgesehen von dem Fall, wo K nur aus zwei Elementen besteht, kann man zeigen, dass es außer den genannten Untervektorräumen noch weitere in K^2 gibt. Auch wird es außer Δ im Allgemeinen noch weitere echte Unterringe von K^2 geben, insbesondere solche, die in Δ enthalten sind.

2.3, Aufg. 1. Das Bild $\varphi(\mathfrak{a})$ eines Ideals $\mathfrak{a} \subset R$ ist zwar eine Untergruppe von R', aber im Allgemeinen kein Ideal, da $\varphi(\mathfrak{a})$ nicht unter der Multiplikation mit Elementen aus R' abgeschlossen zu sein braucht. Als Beispiel betrachte man den Ringhomomorphismus $\mathbb{Z} \hookrightarrow \mathbb{Q}$. Für $m \geq 1$ ist $m\mathbb{Z}$ ein Ideal in $\mathbb{Z}$, nicht aber in $\mathbb{Q}$, denn $\mathbb{Q}$ besitzt als Körper lediglich die trivialen Ideale. Anders ist die Situation, wenn man $\varphi\colon R \longrightarrow R'$ als *surjektiv* voraussetzt. In diesem Fall ist das Bild $\varphi(\mathfrak{a})$ eines Ideals $\mathfrak{a} \subset R$ stets ein Ideal in R'. Um beispielsweise die Abgeschlossenheit von $\varphi(\mathfrak{a})$ unter der Multiplikation mit Elementen aus R' zu zeigen, betrachte man Elemente $r' \in R'$, $a' \in \varphi(\mathfrak{a})$ sowie Urbilder $r \in R$, $a \in \mathfrak{a}$. Dann gilt $ra \in \mathfrak{a}$ und deshalb auch $r'a' = \varphi(ra) \in \varphi(\mathfrak{a})$. Wir wollen noch untersuchen, in welchen Fällen das Ideal $\varphi(\mathfrak{a})$ prim oder maximal in R' ist. Hierzu bilde man die Komposition $\psi\colon R \longrightarrow R' \longrightarrow R'/\varphi(\mathfrak{a})$ von φ mit der kanonischen Projektion $R' \longrightarrow R'/\varphi(\mathfrak{a})$, natürlich unter der Voraussetzung, dass φ surjektiv ist. Es ist dann ψ als Komposition surjektiver Ringhomomorphismen wieder ein surjektiver Ringhomomorphismus. Sein Kern berechnet sich zu $\mathfrak{a} + \ker\varphi$,

so dass $R'/\varphi(\mathfrak{a})$ aufgrund von 2.3/5 zu $R/(\mathfrak{a}+\ker\varphi)$ isomorph ist. Wir können daher unter Benutzung von 2.3/8 schließen, dass $\varphi(\mathfrak{a})$ genau dann prim (bzw. maximal) ist, wenn $R'/\varphi(\mathfrak{a})$ ein Integritätsring (bzw. Körper) ist, d. h. genau dann, wenn $\mathfrak{a}+\ker\varphi$ prim (bzw. maximal) in R ist. Insbesondere ist für jedes prime (bzw. maximale) Ideal $\mathfrak{a}$, welches $\ker\varphi$ umfasst, das Bild $\varphi(\mathfrak{a})$ ebenfalls prim (bzw. maximal).

Als Nächstes wollen wir das Urbild $\mathfrak{a}=\varphi^{-1}(\mathfrak{a}')$ eines Ideals $\mathfrak{a}'\subset R'$ betrachten, wobei φ jetzt wieder ein beliebiger Ringhomomorphismus sei. Man verifiziert dann ohne Schwierigkeiten, dass $\mathfrak{a}$ ein Ideal in R ist. Die Abgeschlossenheit unter der Multiplikation mit R ergibt sich wie folgt: Sind $r\in R$ und $a\in\mathfrak{a}$, so gilt $\varphi(ra)=\varphi(r)\varphi(a)\in\mathfrak{a}'$, also $ra\in\varphi^{-1}(\mathfrak{a}')=\mathfrak{a}$. Um zu erkennen, wann $\mathfrak{a}$ prim oder maximal in R ist, betrachte man wieder die Komposition $\psi\colon R\longrightarrow R'\longrightarrow R'/\mathfrak{a}'$, welche nunmehr $\ker\psi=\mathfrak{a}$ erfüllt. Nach 2.3/4 induziert ψ einen injektiven Homomorphismus $\overline{\psi}\colon R/\mathfrak{a}\longrightarrow R'/\mathfrak{a}'$. Indem wir 2.3/8 anwenden, können wir wie folgt schließen: Ist $\mathfrak{a}'$ prim in R', so ist $R'/\mathfrak{a}'$ ein Integritätsring, folglich auch $R/\mathfrak{a}$ und somit $\mathfrak{a}$ ein Primideal in R. Dieselbe Schlussweise funktioniert jedoch nicht für maximale Ideale anstelle von Primidealen, da die Abbildung $\overline{\psi}$ nicht surjektiv zu sein braucht. In der Tat ist das Urbild $\mathfrak{a}\subset R$ eines maximalen Ideals $\mathfrak{a}'\subset R'$ nicht notwendig wieder maximal. Man betrachte etwa die Inklusionsabbildung $\mathbb{Z}\hookrightarrow\mathbb{Q}$, sowie das Ideal $\mathfrak{a}'=0$. Dieses ist maximal in $\mathbb{Q}$, sein Urbild $\mathfrak{a}=0$ aber nicht maximal in $\mathbb{Z}$.

Im Falle der Surjektivität von φ kann man mit der gegebenen Argumentation übrigens auch einsehen, dass die Ideale in R' in bijektiver Weise denjenigen Idealen in R entsprechen, die $\ker\varphi$ enthalten, und weiter, dass sich bei dieser Korrespondenz jeweils Primideale bzw. maximale Ideale entsprechen.

2.3, Aufg. 2. Wir wollen zeigen, dass $\ker\varphi_x$ gleich dem von $X-x$ erzeugten Hauptideal $(X-x)$ ist. Natürlich gilt $X-x\in\ker\varphi_x$. Umgekehrt können wir auf ein beliebiges Element $f\in\ker\varphi_x$ die Division mit Rest 2.1/4 anwenden und $f=q(X-x)+r$ mit einem Polynom $r\in R[X]$ vom Grad <1 schreiben, d. h. mit einem konstanten Polynom r. Da aber $\varphi_x(r)=\varphi_x(f)=0$ gilt, erhält man $r=0$ und somit $f\in(X-x)$. Insgesamt folgt $\ker\varphi_x=(X-x)$.

Aufgrund der Surjektivität von φ_x erhält man mit Hilfe des Homomorphiesatzes 2.3/5 einen Isomorphismus $R[X]/\ker\varphi_x\xrightarrow{\sim}R$. Nach 2.3/8 ist daher $\ker\varphi_x$ genau dann prim, wenn R ein Integritätsring ist und genau dann maximal, wenn R ein Körper ist.

2.4, Aufg. 1. Es sei R ein Ring. Wir wollen zeigen, dass der Polynomring $R[X]$ genau dann ein Hauptidealring ist, wenn R ein Körper ist. Die Bedingung ist hinreichend, wie wir in 2.4/3 gesehen haben. Sei also $R[X]$ als Hauptidealring angenommen. Insbesondere ist dann $R[X]$ und somit auch R ein Integritätsring. Wir wollen zunächst nachweisen, dass das Element X irreduzibel in $R[X]$ ist. Hierzu betrachte man eine Zerlegung $X = fg$ mit Polynomen $f, g \in R[X]$. Aufgrund der Gradgleichung in 2.1/2 folgt dann $\operatorname{grad} f + \operatorname{grad} g = 1$, also etwa $\operatorname{grad} f = 0$ und $\operatorname{grad} g = 1$. Das Polynom f ist daher konstant, d. h. definiert ein Element in R, und das Produkt von f mit dem Koeffizienten vom Grad 1 in g ergibt 1 aufgrund der Gleichung $X = fg$. Dies bedeutet aber, dass f eine Einheit in R bzw. $R[X]$ ist, und es folgt die Irreduzibilität von X.

Sei nun $\varphi\colon R[X] \longrightarrow R$, $h \longmapsto h(0)$, der Einsetzungshomomorphismus, der 0 anstelle der Variablen X substituiert. Dieser ist surjektiv mit $\ker \varphi = (X)$ und induziert somit einen Isomorphismus $R[X]/(X) \simeq R$ aufgrund des Homomorphiesatzes 2.3/5. Da X irreduzibel ist, schließt man mit 2.4/6, dass das Ideal (X) maximal in $R[X]$ ist. Dann ist aber $R[X]/(X) \simeq R$ nach 2.3/8 ein Körper.

2.4, Aufg. 2. Es sei R ein faktorieller Ring. Wenn das von zwei Elementen x, y in R erzeugte Ideal stets ein Hauptideal ist, so folgt mit einem induktiven Argument, dass jedes *endlich* erzeugte Ideal in R ein Hauptideal ist. In Verbindung mit der Faktorialität von R sieht man dann, dass *jedes* Ideal in R ein Hauptideal ist, dass R also ein Hauptidealring ist. Falls nämlich ein Ideal $\mathfrak{a} \subset R$ existiert, das nicht endlich erzeugt ist, so findet man in $\mathfrak{a}$ eine Folge von Elementen $a_1, a_2, \ldots$ mit

$$(a_1) \subsetneq (a_1, a_2) \subsetneq (a_1, a_2, a_3) \subsetneq \ldots$$

Da jedes dieser Ideale als endlich erzeugtes Ideal ein Hauptideal ist, können wir diese Idealkette auch in der Form

$$(x_1) \subsetneq (x_2) \subsetneq (x_3) \subsetneq \ldots$$

schreiben, wobei jeweils x_{i+1} ein echter Teiler von x_i ist. Dies bedeutet, dass die Anzahl der Primfaktoren, in die x_{i+1} zerfällt, um mindestens 1 geringer sein muss als die Anzahl der Primfaktoren von x_i. Folglich kann eine unendliche Kette des obigen Typs nicht existieren, jedes Ideal in R ist daher endlich erzeugt und somit ein Hauptideal. Die idealtheoretische

Charakterisierung des größten gemeinsamen Teilers ist also generell nur in Hauptidealringen möglich.

Anders ist dies beim kleinsten gemeinsamen Vielfachen v zweier Elemente $x, y \in R$. Es gilt nämlich $(x) \cap (y) = (v)$, auch wenn R lediglich ein faktorieller Ring ist. Dies ist leicht zu begründen. Da v ein Vielfaches von x und y ist, hat man $(x) \cap (y) \supset (v)$. Ist andererseits $a \in (x) \cap (y)$, also gemeinsames Vielfaches von x und y, so ist a nach Definition von v auch Vielfaches von v, und es folgt $a \in (v)$ bzw. $(x) \cap (y) \subset (v)$.

2.5, Aufg. 1. Es sei R ein (kommutativer) Ring und M ein nicht notwendig kommutatives Monoid. Dann lässt sich der Polynomring $R[M]$ wie in 2.5 konstruieren, denn dort wurde an keiner Stelle benutzt, dass M kommutativ ist. Vorsicht ist allerdings geboten, wenn man die Verknüpfung von M weiterhin additiv schreibt. Wenn nämlich M nicht kommutativ ist, so gibt es Elemente $\mu, \nu \in M$ mit $\mu + \nu \neq \nu + \mu$. Insbesondere ist dann das Produkt $X^\mu \cdot X^\nu = X^{\mu+\nu}$ verschieden von dem Produkt $X^\nu \cdot X^\mu = X^{\nu+\mu}$, so dass $R[M]$ im Allgemeinen kein kommutativer Ring mehr ist. Entsprechend sollte man auch in 2.5/1 nicht nur kommutative Erweiterungsringe R' von R zulassen, sondern allgemeiner Ringe R', deren Elemente mit denen von R vertauschbar sind. Die Aussage von 2.5/1 sowie der Beweis bleiben ohne Änderungen gültig.

2.5, Aufg. 2. Die Resultate 2.5/2, 2.5/3 und 2.5/4 bleiben wortwörtlich gültig, wenn man statt $R[X_1, \ldots, X_n]$ den Polynomring $R[\mathfrak{X}]$ in einem beliebigen System $\mathfrak{X} = (X_i)_{i \in I}$ von Variablen X_i betrachtet. Als Argument kann man anführen, dass die Elemente von $R[\mathfrak{X}]$ jeweils Polynome in endlich vielen Variablen X_i sind und dass es deshalb genügt, die entsprechenden Aussagen für Polynomringe in endlich vielen Variablen zu kennen. Man betrachte beispielsweise die Aussage von 2.5/4. Zunächst gilt $R^* \subset (R[\mathfrak{X}])^*$, denn jede Einheit in R ist auch Einheit in $R[\mathfrak{X}]$. Ist umgekehrt f Einheit in $R[\mathfrak{X}]$, so gibt es ein $g \in R[\mathfrak{X}]$ mit $fg = 1$. Da f und g jeweils Polynome in endlich vielen Variablen sind, lässt sich die Gleichung $fg = 1$ auch in einem Unterring der Form $R[X_{i_1}, \ldots, X_{i_n}] \subset R[\mathfrak{X}]$ lesen. Also ist f Einheit in $R[X_{i_1}, \ldots, X_{i_n}]$, und wir können benutzen, dass f dann schon eine Einheit in R ist.

Auch 2.5/5 lässt sich auf Systeme von beliebig vielen Variablen verallgemeinern: Sei $\varphi\colon R \longrightarrow R'$ ein Ringhomomorphismus und $(x_i)_{i \in I}$ ein System von Elementen aus R'. Dann gibt es genau einen Ringhomomorphismus $\Phi\colon R[X_i\,;\, i \in I] \longrightarrow R'$ mit $\Phi|_R = \varphi$ und $\Phi(X_i) = x_i$ für alle

$i \in I$. Man kann diese Aussage aus 2.5/5 ableiten, indem man Fortsetzungen von φ des Typs $R[X_{i_1}, \ldots, X_{i_n}] \longrightarrow R'$ mit $X_{i_j} \longmapsto x_{i_j}$ betrachtet und deren Eindeutigkeit benutzt. Natürlicher ist es jedoch, zu bemerken, dass ein Monoidhomomorphismus $\mathbb{N}^{(I)} \longrightarrow R'$ durch die Angabe der Bilder der Elemente $e_j = (\delta_{ij})_{i \in I}$, $j \in I$, eindeutig bestimmt ist und dass man diese Bilder beliebig vorgeben darf. Dann kann man 2.5/1 benutzen.

2.5, Aufg. 3. Wir schließen unter wiederholter Anwendung von 2.5/1. Es sei $\Phi' \colon R[M] \longrightarrow R[M \times M']$ derjenige Ringhomomorphismus, der durch die kanonische Abbildung $R \hookrightarrow R[M \times M']$ sowie durch den Monoidhomomorphismus $M \longrightarrow R[M \times M']$, $\mu \longmapsto X^{(\mu,0)}$, gegeben wird. Weiter gibt es einen Homomorphismus $\Phi \colon R[M][M'] \longrightarrow R[M \times M']$, der Φ' fortsetzt und ansonsten durch $M' \longrightarrow R[M \times M']$, $\nu \longmapsto X^{(0,\nu)}$, beschrieben wird. In umgekehrter Weise können wir einen Ringhomomorphismus $\Psi \colon R[M \times M'] \longrightarrow R[M][M']$ durch die kanonische Abbildung $R \hookrightarrow R[M] \hookrightarrow R[M][M']$ sowie den Monoidhomomorphismus $M \times M' \longrightarrow R[M][M']$, $(\mu, \nu) \longmapsto X^{\mu} \cdot X^{\nu}$, definieren. Wir behaupten, dass Φ und Ψ zueinander invers sind, dass also die Gleichungen $\Phi \circ \Psi = \mathrm{id}$ und $\Psi \circ \Phi = \mathrm{id}$ gelten. Es sind $\Phi \circ \Psi$ und die identische Abbildung jeweils Ringhomomorphismen $R[M \times M'] \longrightarrow R[M \times M']$, die die kanonische Abbildung $R \hookrightarrow R[M \times M']$ fortsetzen und die Vorschrift $X^{(\mu,\nu)} \longmapsto X^{(\mu,\nu)}$ erfüllen, also zu dem Monoidhomomorphismus $M \times M' \longrightarrow R[M \times M']$, $(\mu, \nu) \longmapsto X^{(\mu,\nu)}$, korrespondieren. Die Eindeutigkeitsaussage in 2.5/1 liefert daher $\Phi \circ \Psi = \mathrm{id}$. Auf ähnliche Weise erhält man $\Psi \circ \Phi = \mathrm{id}$, zunächst eingeschränkt auf $R[M]$ und sodann auf ganz $R[M][M']$.

2.6, Aufg. 1. Wir schließen mit Induktion nach n und stellen das Polynom $f \in K[X_1, \ldots, X_n]$ in der Form $f = \sum_{i=0}^{\infty} f_i X_n^i$ dar, mit Polynomen $f_i \in K[X_1, \ldots, X_{n-1}]$. Dabei sei $n \geq 1$. Für $x = (x_1, \ldots, x_n) \in K^n$ gilt dann $f(x) = \sum_{i=0}^{\infty} f_i(x') x_n^i$ mit $x' = (x_1, \ldots, x_{n-1})$. Hat man nun $f(x) = 0$ für alle $x \in K^n$, so verschwindet für jedes $x' \in K^{n-1}$ das Polynom einer Variablen $\sum_{i=0}^{\infty} f_i(x') X_n^i \in K[X_n]$ auf ganz K. Nach 2.6/1 verschwinden die Koeffizienten $f_i(x')$, so dass man also $f_i(x') = 0$ für alle $i \in \mathbb{N}$ und alle $x' \in K^{n-1}$ hat. Im Falle $n > 1$ ergibt sich dann nach Induktionsvoraussetzung $f_i = 0$ für alle i und somit $f = 0$.

2.7, Aufg. 1. Zunächst überlegt man sich, dass das Bild $\varphi(p)$ eines Primelements $p \in R$ wieder ein Primelement ist. Gehen wir daher von einer Primfaktorzerlegung $x = p_1 \ldots p_n$ eines Elementes $x \in R$ aus, so ergibt

sich $\varphi(x) = \varphi(p_1) \dots \varphi(p_n)$ als Primfaktorzerlegung des Bildes $\varphi(x)$. Insbesondere gilt $\nu_{\varphi(p)}(\varphi(x)) = \nu_p(x)$ für $x \in R$. Wir wollen zeigen, dass allgemeiner die Gleichung $\nu_{\varphi(p)}(\Phi(f)) = \nu_p(f)$ gilt, und zwar für alle Primelemente $p \in R$ und alle Polynome $f \in R[X]$. Indem man neben Φ auch Φ^{-1} betrachtet, genügt es, für Polynome $f \neq 0$ nachzuweisen, dass stets $\nu_{\varphi(p)}(\Phi(f)) \geq \nu_p(f)$ gilt. Hat man etwa $\nu_p(f) = r \geq 0$, so kann man $\tilde{f} = p^{-r} f$ als Polynom in $R[X]$ auffassen. Es folgt $\Phi(\tilde{f}) \in R[X]$ und daher $\nu_{\varphi(p)}(\Phi(\tilde{f})) \geq 0$. Da aber $\Phi(f) = \Phi(p^r \tilde{f}) = \varphi(p)^r \Phi(\tilde{f})$ gilt, ergibt sich $\nu_{\varphi(p)}(\Phi(f)) \geq r = \nu_p(f)$, was zu zeigen war. Unter der Bedingung, dass $\varphi(p)$ stets zu p assoziiert ist, z. B. für $\varphi = \Phi|_R = \mathrm{id}$ erhält man sogar $\nu_p(\Phi(f)) = \nu_p(f)$ für alle Primelemente $p \in R$.

Ein Polynom $f \in R[X]$ ist genau dann primitiv, wenn $\nu_p(f) = 0$ für alle Primelemente $p \in R$ gilt. Da φ ein Isomorphismus von R ist, induziert φ eine Bijektion auf der Menge der Klassen assoziierter Primelemente. Insbesondere folgt aus der Gleichung $\nu_{\varphi(p)}(\Phi(f)) = \nu_p(f)$, dass $\Phi(f)$ genau dann primitiv ist, wenn f primitiv ist. Als Beispiel können wir die Abbildung $\Phi\colon R[X] \longrightarrow R[X]$, $f \longmapsto f(X+a)$, betrachten. Es folgt, dass ein Polynom $f \in R[X]$ genau dann primitiv ist, wenn $f(X+a)$ primitiv ist.

2.7, Aufg. 2. Das Lemma von Gauß besagt, dass für Primelemente $p \in R$ und für Polynome $f, g \in K[X]$ die Formel $\nu_p(fg) = \nu_p(f) + \nu_p(g)$ gilt. Hieraus folgt für $f, g \neq 0$

$$\prod_{p \in P} p^{\nu_p(fg)} = \prod_{p \in P} p^{\nu_p(f)} \cdot \prod_{p \in P} p^{\nu_p(g)},$$

d. h. $a_{fg} = a_f \cdot a_g$ als Formel für den Inhalt. Umgekehrt schließt man aus dieser Formel $\nu_p(a_{fg}) = \nu_p(a_f) + \nu_p(a_g)$ für $p \in P$. Da der Inhalt a_h eines Polynoms $h \neq 0$ durch die Beziehung $\nu_p(a_h) = \nu_p(h)$ charakterisiert ist, ergibt sich wiederum $\nu_p(fg) = \nu_p(f) + \nu_p(g)$. Für $f, g \neq 0$ ist die Aussage des Lemmas von Gauß somit äquivalent zu der Formel $a_{fg} = a_f \cdot a_g$.

2.9, Aufg. 1. Ist $M = T \oplus F$ eine Zerlegung in einen Torsionsmodul T und einen freien Modul F, so ist T eindeutig bestimmt als "der" Torsionsuntermodul von M. Im Gegensatz hierzu ist F, abgesehen von den Fällen $T = 0$ und $T = M$, nicht eindeutig bestimmt. Ändert man nämlich die Elemente einer Basis von F in beliebiger Weise durch Torsionselemente ab, so erhält man einen freien Untermodul $F' \subset M$, der ebenfalls $T \oplus F' = M$ erfüllt.

Keine Eindeutigkeit besteht auch bei nicht-trivialen Zerlegungen des Typs $M = M' \oplus M''$ mit $M' \simeq A/p^r A$ und $M'' \simeq A/p^s A$, wobei p

ein Primelement sei. Beispielsweise kann man M im Falle $r = s = 1$ als (A/p)-Vektorraum auffassen. Es ist dann $M = M' \oplus M''$ eine direkte Summenzerlegung eines 2-dimensionalen (A/p)-Vektorraums in zwei 1-dimensionale Unterräume. Eine solche Zerlegung ist aber niemals eindeutig bestimmt.

2.9, Aufg. 2. Es ist $\mathbb{Q}$ ein torsionsfreier $\mathbb{Z}$-Modul vom Rang 1, der nicht frei ist. Wäre $\mathbb{Q}$ nämlich ein freier $\mathbb{Z}$-Modul, so würde es ein $x \in \mathbb{Q}$ mit $\mathbb{Q} = \mathbb{Z}x$ geben. Eine solche Gleichung kann aber nicht bestehen. Gilt etwa $x = \frac{a}{b}$ mit teilerfremden Zahlen $a, b \in \mathbb{Z}$, $a, b \neq 0$, so folgt $\frac{a}{2b} \notin \mathbb{Z}x$.

2.9, Aufg. 3. Es sei K ein Körper und V ein endlich-dimensionaler K-Vektorraum mit einem K-Endomorphismus $\varphi\colon V \longrightarrow V$. Ein Untervektorraum $U \subset V$ heißt *φ-invariant*, wenn $\varphi(U) \subset U$ gilt, und *φ-zyklisch*, wenn es ein $u \in U$ gibt, so dass die Folge $u, \varphi(u), \varphi^2(u), \ldots$ ein K-Erzeugendensystem von U bildet; insbesondere ist U dann φ-invariant. Weiter wird ein φ-invarianter Untervektorraum $U \subset V$ als *φ-irreduzibel* bezeichnet, wenn U sich nicht in eine direkte Summe zweier echter φ-invarianter Untervektorräume zerlegen lässt. In der Normalformentheorie zeigt man in einem ersten Schritt, dass V in eine direkte Summe φ-irreduzibler Untervektorräume zerfällt und dass jeder φ-irreduzible Untervektorraum φ-zyklisch ist. Wir wollen dies zunächst aus 2.9/8 folgern; vgl. auch [4], 6.3–6.5.

Hierzu fasse man V wie in 2.9 beschrieben als $K[X]$-Modul auf, indem man die Multiplikation mit X auf V durch Anwenden von φ erkläre. Ein $K[X]$-Untermodul $U \subset V$ ist dann nichts anderes als ein φ-invarianter K-Untervektorraum, ein von einem Element erzeugter $K[X]$-Untermodul nichts anderes als ein φ-zyklischer K-Untervektorraum. Ein φ-irreduzibler Untervektorraum von V ist daher ein $K[X]$-Untermodul von V, der sich nicht in eine direkte Summe zweier echter $K[X]$-Untermoduln zerlegen lässt.

Da V als K-Vektorraum endlich erzeugt ist, gilt dasselbe auch für V als $K[X]$-Modul, und es ist V ein $K[X]$-Torsionsmodul. Wir können also 2.9/8 anwenden und erhalten nach Wahl eines Vertretersystems P der Primpolynome in $K[X]$ eine Zerlegung

$$V \simeq \bigoplus_{p \in P} \bigoplus_{\nu_p=1}^{r_p} K[X]/(p^{n(p,\nu_p)})$$

mit eindeutig bestimmten Zahlen $r_p, n(p, \nu_p) \in \mathbb{N}$, wobei r_p für fast alle $p \in P$ verschwindet. In der Sprache der Vektorräume ist dies eine Zerle-

gung von V in eine direkte Summe φ-zyklischer Untervektorräume, und man schließt aus der Eindeutigkeitsaussage in 2.9/8, dass die auftretenden Unterräume sogar φ-irreduzibel sind, bzw. allgemeiner, dass jeder φ-irreduzible Unterraum φ-zyklisch ist. Damit ist das oben angegebene Resultat bewiesen.

Man kann nun noch spezielle Matrizen betrachten, die den Endomorphismus φ bezüglich geeigneter K-Basen von V beschreiben. Man betrachte hierzu eine Zerlegung $V = \bigoplus_{i=1}^{s} V_i$ in φ-irreduzible Untervektorräume und wähle eine Basis von V, indem man geeignete Basen der einzelnen V_i zusammensetzt. Die zugehörige Matrix von φ ist dann eine "Diagonalmatrix" in dem Sinne, dass auf der "Diagonalen" die beschreibenden Matrizen der Endomorphismen $\varphi_i = \varphi|_{V_i}$ stehen, ansonsten nur jeweils Elemente 0. Es genügt daher, V als φ-irreduzibel anzunehmen, etwa $V = K[X]/(p^n)$ mit einem Primelement $p \in P$. Bezeichnet $\overline{X} \in K[X]/(p^n)$ die Restklasse zu X, so bilden die Elemente $1, \overline{X}, \overline{X}^2, \ldots, \overline{X}^{m-1}$ mit $m = n \cdot (\operatorname{grad} p)$ eine K-Basis von V, und die zu φ gehörige Matrix ist von der Gestalt

$$\begin{pmatrix} 0 & 0 & \ldots & 0 & 0 & -c_m \\ 1 & 0 & \ldots & 0 & 0 & -c_{m-1} \\ . & . & \ldots & . & . & . \\ . & . & \ldots & . & . & . \\ 0 & 0 & \ldots & 1 & 0 & -c_2 \\ 0 & 0 & \ldots & 0 & 1 & -c_1 \end{pmatrix}$$

mit $p^n = X^m + c_1 X^{m-1} + \ldots + c_m$ als Minimalpolynom zu φ. Dies ist die sogenannte *allgemeine Normalform* der Matrix zu φ. Ist p vom Grad 1, also $p = X - c$, so kann man auch $1, \overline{X} - c, (\overline{X} - c)^2, \ldots, (\overline{X} - c)^{n-1}$ als K-Basis von V nehmen. Die zu φ gehörige Matrix hat dann die Form

$$\begin{pmatrix} \mathrm{c} & 0 & \ldots & 0 & 0 \\ 1 & \mathrm{c} & \ldots & 0 & 0 \\ . & . & \ldots & . & . \\ 0 & 0 & \ldots & \mathrm{c} & 0 \\ 0 & 0 & \ldots & 1 & \mathrm{c} \end{pmatrix}$$

Dies ist die sogenannte *Jordansche Normalform* der Matrix zu φ.

3.1, Aufg. 1. Es sei $\sigma\colon R \longrightarrow R'$ ein Homomorphismus zwischen Integritätsringen R, R' der Charakteristik p bzw. p'. Betrachtet man dann die Homomorphismen $\varphi\colon \mathbb{Z} \longrightarrow R$, $n \longmapsto n \cdot 1$, und $\varphi'\colon \mathbb{Z} \longrightarrow R'$, $n \longmapsto n \cdot 1$,

so gilt $\ker \varphi = p\mathbb{Z}$ und $\ker \varphi' = p'\mathbb{Z}$. Da φ' als Homomorphismus von $\mathbb{Z}$ nach R' eindeutig bestimmt ist, folgt $\varphi' = \sigma \circ \varphi$ und somit $\ker \varphi \subset \ker \varphi'$ bzw. $p' \mid p$. Weiter hat man $\ker \varphi = \ker \varphi'$ bzw. $p = p'$, falls σ injektiv ist. Da Körperhomomorphismen stets injektiv sind, sieht man insbesondere, dass es zwischen Körpern unterschiedlicher Charakteristik keine Homomorphismen geben kann.

Andererseits liefert $\mathbb{Z} \longrightarrow \mathbb{Z}/p'\mathbb{Z}$ für p' prim ein Beispiel eines Homomorphismus zwischen Integritätsringen der Charakteristik 0 bzw. p'. Dies ist aber auch der einzige Fall "gemischter" Charakteristik, der auftreten kann. Ist nämlich wie oben $\sigma\colon R \longrightarrow R'$ ein Homomorphismus zwischen Integritätsringen der Charakteristik p und p', so gilt $p' \mid p$, wie wir gesehen haben. Da p und p' (positive) Primzahlen sind, sofern sie nicht verschwinden, ergibt sich für $p \neq p'$ notwendig $p = 0$.

3.2, Aufg. 1. Wir betrachten also eine Körpererweiterung L/K und zwei über K algebraische Elemente $\alpha, \beta \in L$. Um zu zeigen, dass $\alpha + \beta$ algebraisch über K ist, könnte man versuchen, aus den beiden Minimalpolynomen zu α und β in expliziter Weise ein nicht-triviales Polynom zu konstruieren, welches $\alpha + \beta$ annulliert. Die Erfahrung zeigt jedoch, dass ein solches Verfahren wenig praktikabel ist. Ein oberflächlicher Grund hierfür liegt darin, dass man in einem Ausdruck $f(\alpha + \beta)$ mit einem Polynom $f \in K[X]$ vom Grad ≥ 2 die Größen α und β im Allgemeinen nicht "trennen" kann, etwa indem man $f(\alpha + \beta)$ als Summe eines Polynoms in α und eines Polynoms in β schreibt. Als Beispiel betrachte man die Körpererweiterung $\mathbb{C}/\mathbb{Q}$ sowie die algebraischen Zahlen $\alpha = \sqrt{2}$ und $\beta = \sqrt{3}$. Das Minimalpolynom zu α ist $X^2 - 2$, dasjenige zu β ist $X^2 - 3$. Verfährt man etwa nach der Methode von Aufgabe 7 aus Abschnitt 3.2, so erhält man $X^4 - 10X^2 + 1$ als Minimalpolynom zu $\alpha + \beta$, also ein Polynom, das in keinem "offensichtlichen" Zusammenhang zu den Polynomen $X^2 - 2$ und $X^2 - 3$ steht.

So bleibt kein anderer Weg, als zum Beweis der Algebraizität von $\alpha + \beta$ die in Abschnitt 3.2 entwickelte Theorie zu verwenden. Wir wissen nach 3.2/6, dass $K(\alpha)/K$ und $K(\alpha, \beta)/K(\alpha)$ endliche Körpererweiterungen sind. Aufgrund des Gradsatzes 3.2/2 ist dann auch $K(\alpha, \beta)/K$ endlich und somit nach 3.2/7 algebraisch. Insbesondere folgt, dass $\alpha + \beta \in K(\alpha, \beta)$ algebraisch über K ist.

3.2, Aufg. 2. Wir haben in 3.2/7 gezeigt, dass jede endliche Körpererweiterung algebraisch ist. Weiter zeigt das Beispiel des algebraischen Abschlusses $\overline{\mathbb{Q}}$ von $\mathbb{Q}$ in $\mathbb{C}$, dass die Umkehrung dieses Satzes nicht richtig ist. Wir können

aber sagen, dass eine Körpererweiterung L/K genau dann algebraisch ist, wenn es eine Familie $(L_i)_{i\in I}$ von Zwischenkörpern zu L/K mit $L = \bigcup_{i\in I} L_i$ gibt, derart dass L_i/K jeweils endlich ist. In der Tat, ist letztere Bedingung gegeben und ist $\alpha \in L$, so existiert ein Index $i \in I$ mit $\alpha \in L_i$. Folglich ist α algebraisch über K und entsprechend L algebraisch über K. Ist umgekehrt L/K algebraisch, so ist L Vereinigung der Zwischenkörper $K(\alpha)$, wobei α in L variiert. $K(\alpha)/K$ ist endlich nach 3.2/6.

Weiter wollen wir noch zeigen, dass man die Algebraizität einer Körpererweiterung L/K durch folgende Bedingung charakterisieren kann: Jeder über K endlich erzeugte Teilkörper L' von L ist endlich über K. Ist nämlich L/K algebraisch und L' ein über K endlich erzeugter Teilkörper von L, so ist L'/K nach 3.2/9 endlich. Die angegebene Bedingung ist also notwendig. Sie ist aber auch hinreichend. In der Tat, für jedes $\alpha \in L$ ist die Körpererweiterung $K(\alpha)/K$ einfach und damit endlich erzeugt. Ist nun $K(\alpha)/K$ stets endlich, so auch algebraisch gemäß 3.2/7, und wir sehen, dass L/K algebraisch ist.

3.2, Aufg. 3. Angenommen, es gibt ein Element $\alpha \in \mathbb{C}$, welches nicht im algebraischen Abschluss $\overline{\mathbb{Q}}$ von $\mathbb{Q}$ in $\mathbb{C}$ enthalten ist und dennoch algebraisch über $\overline{\mathbb{Q}}$ ist. Dann ist α nach 3.2/12 algebraisch über $\mathbb{Q}$, muss also doch schon in $\overline{\mathbb{Q}}$ enthalten sein, im Widerspruch zur Wahl von α.

3.3, Aufg. 1. Zu $b \in B$ betrachte man in gewohnter Weise den Homomorphismus $\varphi\colon A[Y] \longrightarrow B$, der die Inklusion $A \hookrightarrow B$ fortsetzt und Y auf b abbildet. Da b eine ganze Gleichung über A erfüllt, enthält $\ker\varphi$ insbesondere normierte Polynome. Wir können daher unter allen normierten Polynomen in $\ker\varphi$ eines mit minimalem Grad wählen, etwa f. Handelt es sich bei A um einen Körper K, so ist f eindeutig durch b bestimmt. Denn dann ist $\ker\varphi$ ein Hauptideal, und es wird $\ker\varphi$ von f erzeugt. Als Erzeuger eines Hauptideals ist f eindeutig bis auf eine Einheit in $K[Y]$, d. h. bis auf eine Konstante in K^*. Setzt man daher f als normiert voraus, so ist f eindeutig durch b bestimmt.

Im Allgemeinfall ist $\ker\varphi$ jedoch kein Hauptideal in $A[Y]$. Es gibt dann meist verschiedene normierte Polynome minimalen Grades in $\ker\varphi$, und wir können keines von diesen als "das" Minimalpolynom von b über A bezeichnen. Für das Beispiel $A = \{\sum c_i X^i \in K[X]\,;\, c_1 = 0\} \subset K[X] = B$ aus der Aufgabenstellung sind etwa

$$Y^2 - X^2, \qquad Y^2 + X^2Y - (X^3 + X^2)$$

zwei verschiedene normierte Polynome minimalen Grades in $A[Y]$, welche das Element $b := X$ annullieren. Keines von beiden erzeugt das Ideal $\ker \varphi$.

3.4, Aufg. 1. Wir nehmen an, dass das Polynom $f \in \mathbb{Q}[X]$ irreduzibel ist; ansonsten müssten wir f durch einen irreduziblen Faktor ersetzen. Wir wissen dann aufgrund des Verfahrens von Kronecker, Satz 3.4/1, dass wir $\mathbb{Q}[X]/(f)$ als Erweiterungskörper von $\mathbb{Q}$ auffassen können, wobei die Restklasse $\overline{X}$ der Variablen X eine Nullstelle von f ist. Wir haben also $\mathbb{Q}$ sozusagen minimal erweitert mit der alleinigen Intention, eine Nullstelle zu f zu bekommen und ohne den erhaltenen Erweiterungskörper in Relation zu den reellen oder komplexen Zahlen zu setzen. Im Gegensatz hierzu konstruiert man in der Analysis zu $\mathbb{Q}$ zunächst mit topologischen Argumenten den Körper $\mathbb{R}$ sowie hieraus den Körper $\mathbb{C}$ der komplexen Zahlen. Erst dann interessiert man sich für Nullstellen von Polynomen in diesen speziellen Körpern. Bei der Konstruktion solcher Nullstellen spielen Näherungsverfahren und Grenzprozesse eine wesentliche Rolle, da man die definitionsgemäßen Gegebenheiten von $\mathbb{R}$ bzw. $\mathbb{C}$, insbesondere deren Vollständigkeit, ausnutzen muss. Hat man schließlich eine Nullstelle $a \in \mathbb{C}$ zu f gefunden, so lässt sich der Homomorphismus $\mathbb{Q} \longrightarrow \mathbb{C}$ gemäß 3.4/8 zu einem Homomorphismus $\mathbb{Q}[X]/(f) \longrightarrow \mathbb{C}$ fortsetzen, indem wir $\overline{X}$ auf a abbilden.

3.4, Aufg. 2. Man benötigt für die Anwendung des Lemmas von Zorn eine partiell geordnete *Menge*. Im Allgemeinen ist jedoch die "Gesamtheit" aller algebraischen Erweiterungen von K keine Menge.

Die vorgeschlagene Argumentation lässt sich jedoch dem Sinne nach retten, wenn man einige mengentheoretische Vorsichtsmaßnahmen trifft. Wir betrachten hierzu die Potenzmenge P von K und fassen K mittels der Abbildung $K \longrightarrow P$, $a \longmapsto \{a\}$, als Teilmenge von P auf. Es sei dann M die Menge aller Paare (L, κ), bestehend aus einer Menge L mit $K \subset L \subset P$ und einer Körperstruktur κ auf L, welche die gegebene Körperstruktur auf K fortsetzt und L als algebraische Erweiterung von K erklärt. M ist auf natürliche Weise partiell geordnet, und zwar schreiben wir $(L, \kappa) \leq (L', \kappa')$, falls $L \subset L'$ gilt und sich κ' auf L zu κ beschränkt. Mit dem üblichen Vereinigungsargument ergibt sich sofort, dass jede total geordnete Teilmenge von M eine obere Schranke in M besitzt. Somit können wir aus dem Lemma von Zorn 3.4/5 folgern, dass M ein maximales Element enthält. Dieses werde mit (L_1, κ_1) bezeichnet; es stellt eine algebraische Erweiterung von K dar.

Wir behaupten, dass (L_1, κ_1) bereits ein algebraischer Abschluss von K ist, falls K aus unendlich vielen Elementen besteht. Hierzu ist zu zeigen,

dass (L_1, κ_1) keine echten algebraischen Erweiterungen gestattet. Sei also E eine algebraische Erweiterung von (L_1, κ_1); dies ist dann insbesondere eine algebraische Erweiterung von K. Wir verwenden nun einige Kenntnisse über Kardinalitäten von Mengen und benutzen, dass K und $K[X]$ (für nicht-endliches K) gleichmächtig sind, damit also die gleiche Kardinalität besitzen wie die Mengen L_1 und E; letztere sind nämlich darstellbar als Vereinigung von Nullstellenmengen von Polynomen aus $K[X]$. Nun hat aber P als Potenzmenge von K eine echt größere Kardinalität als K bzw. E. Gleiches gilt für $P - L_1$, und es lässt sich daher die Inklusion $L_1 \hookrightarrow P$ zu einer injektiven Abbildung $E \hookrightarrow P$ fortsetzen. Dies liefert ein Element $(L_2, \kappa_2) \in M$ mit $(L_1, \kappa_1) \leq (L_2, \kappa_2)$. Aus der Maximalität von (L_1, κ_1) folgt dann $L_1 = L_2$, bzw. $(L_1, \kappa_1) = E$, d. h. (L_1, κ_1) ist ein algebraischer Abschluss von K. Für endliche Körper K kann man die Argumentation in nahe liegender Weise modifizieren, indem man von K zu einer unendlichen Obermenge K' übergeht und P als Potenzmenge von K' erklärt.

3.4, Aufg. 3. Zwei algebraische Abschlüsse $\overline{K}_1$ und $\overline{K}_2$ eines Körpers K sind zwar über K isomorph, aber es gibt im Allgemeinen verschiedene K-Isomorphismen $\overline{K}_1 \xrightarrow{\sim} \overline{K}_2$, d. h. solche, die K festlassen; man vgl. hierzu 3.4/8 sowie das Konstruktionsverfahren im Beweis zu 3.4/9. Würden wir von "dem" algebraischen Abschluss $\overline{K}$ von K sprechen, so würden wir damit eine Identifizierung aller möglichen algebraischen Abschlüsse von K unterstellen, d. h. wir würden für je zwei solche Abschlüsse $\overline{K}_i$ und $\overline{K}_j$ einen speziellen Isomorphismus $\varphi_{ij} : \overline{K}_i \xrightarrow{\sim} \overline{K}_j$ mit $\varphi_{ij}|_K = \mathrm{id}_K$ auswählen, wobei für je drei Indizes i, j, k die Verträglichkeitsrelation $\varphi_{ik} = \varphi_{jk} \circ \varphi_{ij}$ erfüllt sein müsste. Da es im Allgemeinen aber keine kanonischen Wahlen für solche K-Isomorphismen gibt, ist eine Identifizierung der algebraischen Abschlüsse von K sehr problematisch.

3.5, Aufg. 1. Es sei L/K eine Körpererweiterung vom Grad 2. Ist dann $a \in L - K$, so gilt $1 < [K(a) : K] \leq 2$, also $[K(a) : K] = 2$ und somit $L = K(a)$. Sei $f \in K[X]$ das Minimalpolynom von a über K. Es ist dann a Nullstelle von f, so dass der Linearfaktor $X - a$ in $L[X]$ ein Teiler von f ist. Es folgt, dass f über L vollständig in Linearfaktoren zerfällt. Sind a, b die beiden Nullstellen von f, so gilt $L = K(a) = K(a, b)$, d. h. L ist Zerfällungskörper von f über K und damit normal über K.

3.5, Aufg. 2. Man betrachte also einen Zerfällungskörper L eines nicht-konstanten Polynoms $f \in K[X]$ sowie ein irreduzibles Polynom $g \in K[X]$, welches in L eine Nullstelle b hat. Um zu sehen, dass L bereits sämtliche

Nullstellen von g enthält, wählen wir einen algebraischen Abschluss $\overline{L}$ von L. Seien $b_1, \ldots, b_r \in \overline{L}$ die verschiedenen Nullstellen von g. Nach 3.4/8 gibt es zu jedem $i = 1, \ldots, r$ einen K-Homomorphismus $\sigma_i \colon K(b) \longrightarrow \overline{L}$ mit $\sigma_i(b) = b_i$, und wir können σ_i nach 3.4/9 zu einem K-Homomorphismus $\sigma_i' \colon L \longrightarrow \overline{L}$ fortsetzen.

Es reicht, $\sigma_i'(L) \subset L$ für $i = 1, \ldots, r$ zu zeigen, denn dann sind alle Nullstellen $b_1, \ldots, b_r$ von g in L enthalten, und es folgt, dass g über L vollständig in Linearfaktoren zerfällt. Da σ_i' den Körper K festlässt, bildet es Nullstellen von f auf Nullstellen von f ab. Da aber L über K von allen Nullstellen von f in $\overline{L}$ erzeugt wird, gilt $\sigma_i'(L) \subset L$, wie gewünscht.

3.5, Aufg. 3. Sei $\overline{K}$ ein algebraischer Abschluss von L; es ist dann $\overline{K}$ auch ein algebraischer Abschluss von K, da L/K algebraisch ist. Sei $a \in \overline{K}$ mit Minimalpolynom $f \in K[X]$. Da f nicht konstant ist und L Zerfällungskörper aller nicht-konstanten Polynome in $K[X]$ ist, zerfällt f über L vollständig in Linearfaktoren, so dass $a \in L$ gilt. Damit folgt $L = \overline{K}$, d. h. L ist ein algebraischer Abschluss von K.

3.6, Aufg. 1. Wir gehen ähnlich wie in 3.2, Aufgabe 1 vor. Es ist $a \in L$ separabel über K, also gilt $[K(a) : K]_s = [K(a) : K]$ nach 3.6/6. Weiter ist $b \in L$ separabel über K, also insbesondere auch über $K(a)$, und es gilt entsprechend $[K(a,b) : K(a)]_s = [K(a,b) : K(a)]$. Nun wende man die Gradsätze 3.2/2 und 3.6/7 an und schließe $[K(a,b) : K]_s = [K(a,b) : K]$. Um zu sehen, dass $a + b \in K(a,b)$ separabel über K ist, kann man die Implikation von (iii) nach (i) in 3.6/9 benutzen. Möchte man allerdings weiter in der Theorie zurückgehen und dieses Resultat nicht verwenden, so betrachte man alternativ die Erweiterungen $K \subset K(a+b) \subset K(a,b)$. Man hat

$$\begin{aligned} [K(a,b) : K] &= [K(a,b) : K(a+b)] \cdot [K(a+b) : K] \\ [K(a,b) : K]_s &= [K(a,b) : K(a+b)]_s \cdot [K(a+b) : K]_s. \end{aligned}$$

Die beiden Terme links haben den gleichen Wert. Da der Separabilitätsgrad höchstens gleich dem gewöhnlichen Grad ist, vgl. 3.6/6, gilt Gleichheit auch zwischen den entsprechenden Termen auf der rechten Seite, also insbesondere $[K(a+b) : K]_s = [K(a+b) : K]$. Hieraus folgt wiederum mit 3.6/6, dass $a + b$ separabel über K ist.

Entsprechende Betrachtungen kann man natürlich auch für $a - b$, ab und im Falle $b \neq 0$ für ab^{-1} durchführen. Auf diese Weise sieht man, dass die über K separablen Elemente von L einen Zwischenkörper zu L/K bilden.

3.6, Aufg. 2. Seien $\overline{K}_1$ und $\overline{K}_2$ zwei algebraische Abschlüsse von K. Gemäß 3.4/10 gibt es einen K-Isomorphismus $\sigma\colon \overline{K}_1 \xrightarrow{\sim} \overline{K}_2$. Sei f ein normiertes Polynom in $K[X]$. Sind dann

$$f = \prod_{i=1}^{m} (X - a_i)^{r_i}, \qquad f = \prod_{i=1}^{n} (X - b_i)^{s_i},$$

die Zerlegungen von f in Potenzen paarweise verschiedener Linearfaktoren, jeweils in $\overline{K}_1[X]$ bzw. $\overline{K}_2[X]$, so transportiert σ aufgrund der Eindeutigkeit der Primfaktorzerlegung die erste Zerlegung in die zweite. Es gilt dann $m = n$ und nach eventueller Umnummerierung der b_i auch $\sigma(a_i) = b_i$ für $i = 1, \ldots, m$ sowie $r_i = s_i$. Es hat also f genau dann mehrfache Nullstellen in $\overline{K}_1$, wenn dies in $\overline{K}_2$ gilt.

3.6, Aufg. 3. Wir betrachten eine endliche separable Körpererweiterung L/K, wobei wir uns hier nur für den Fall interessieren, wo K unendlich viele Elemente enthält. Mittels Rekursion kann man sich auf den Fall $L = K(a, b)$ beschränken. Es seien f und g die Minimalpolynome von a bzw. b über K sowie L' ein Zerfällungskörper von f, g über L. Dann ist L' auch Zerfällungskörper von f, g über K, und zwar die normale Hülle von L/K; vgl. 3.5/7. Im Beweis zu 3.6/12 betrachtet man sämtliche K-Homomorphismen $\sigma_1, \ldots, \sigma_n$ von L in einen algebraischen Abschluss $\overline{K}$ von K. Dabei dürfen wir $L' \subset \overline{K}$ annehmen, und es folgt mit 3.5/4, dass die Bilder der σ_i bereits in L' enthalten sind. Mit anderen Worten, es genügt, eine normale Hülle L'/K zu L/K zu bestimmen und alle K-Homomorphismen $\sigma_1, \ldots, \sigma_n$ von L nach L' zu betrachten. Wählt man dann $c \in K$ mit der Eigenschaft, dass für $i \neq j$ stets $\sigma_i(a + cb) \neq \sigma_j(a + cb)$ gilt, so folgt $K(a, b) = K(a + cb)$.

3.7, Aufg. 1. Die Elemente $\alpha, \beta \in L$ seien als rein inseparabel über K vorausgesetzt. Dies bedeutet nach 3.7/2, dass es Gleichungen $\alpha^{p^m} = c$ sowie $\beta^{p^n} = d$ mit Elementen $c, d \in K$ gibt. Dabei dürfen wir, indem wir eventuell eine der beiden Gleichungen geeignet potenzieren, sogar $m = n$ annehmen. Mit der binomischen Formel 3.1/3 folgt dann $(\alpha + \beta)^{p^m} = \alpha^{p^m} + \beta^{p^m} = c + d$. Im Übrigen gilt $(\alpha\beta)^{p^m} = cd$. So sieht man, wiederum mit 3.7/2, dass $\alpha + \beta$ und $\alpha\beta$ rein inseparabel über K sind. Alternativ kann man 3.7/2 nutzen und ähnlich wie in Aufgabe 1 aus Abschnitt 3.2 oder Aufgabe 1 aus Abschnitt 3.6 argumentieren.

3.7, Aufg. 2. Eine rein inseparable Erweiterung L/K lässt sich charakterisieren durch die Gleichung $[L : K]_s = 1$. Alternativ könnten wir auch

$[L : K]_i = [L : K]$ schreiben, allerdings nur für den Fall, dass der Grad $[L : K]$ *endlich* ist. Will man also den Inseparabilitätsgrad anstelle des Separabilitätsgrades verwenden, so muss man sich, ähnlich wie bei der Diskussion separabler Erweiterungen in Abschnitt 3.6, bei Gradbetrachtungen stets auf endlich erzeugte Erweiterungen beschränken.

3.7, Aufg. 3. Sei $K(a)/K$ eine einfache algebraische Körpererweiterung mit Minimalpolynom $f \in K[X]$ von a über K. Wie in 3.6/2 findet man ein $g \in K[X]$ mit $f(X) = g(X^{p^r})$, wobei r maximal gewählt sei. Es ist dann g ein separables Polynom, und zwar das Minimalpolynom von a^{p^r} über K. Es folgt, dass $K(a)/K(a^{p^r})$ rein inseparabel ist und $K(a^{p^r})/K$ separabel.

3.8, Aufg. 1. Körper der Charakteristik 0 sind vollkommen (3.6/4), ebenso endliche Körper oder allgemeiner Körper, die algebraisch über endlichen Körpern sind (3.8/4). Um ein Beispiel einer inseparablen Körpererweiterung zu konstruieren, muss man daher von einem unendlichen Körper K der Charakteristik $p > 0$ ausgehen, der nicht algebraisch über seinem Primkörper $\mathbb{F}_p$ ist. Die einfachste Möglichkeit hierzu ist der Funktionenkörper $K = \mathbb{F}_p(t)$ in einer Variablen t. Adjungieren wir zu K eine p-te Wurzel aus t, so erhalten wir eine rein inseparable Körpererweiterung von K. Unter Benutzung des Frobenius-Homomorphismus lässt sich diese beschreiben als $\mathbb{F}_p(t)/\mathbb{F}_p(t^p)$.

3.8, Aufg. 2. Ist $\mathbb{F}$ ein endlicher Körper der Charakteristik $p > 0$ mit $q = p^n$ Elementen, so ist $\mathbb{F}$ Zerfällungskörper des Polynoms $X^q - X$ über $\mathbb{F}_p$. Genauer besteht $\mathbb{F}$ aus den q Nullstellen dieses Polynoms. Damit ist $\mathbb{F}$ als Teilkörper eines Körpers L durch die Anzahl seiner Elemente eindeutig charakterisiert.

3.9, Aufg. 1. Wir haben zu Beginn von Abschnitt 3.9 nicht benutzt, dass die Nullstellen der entsprechenden Polynome über einem *algebraisch abgeschlossenen* Körper betrachtet werden. So bleibt insbesondere die Aussage von 3.9/1 gültig, wenn man $\overline{K}$ durch K und $V(\cdot)$ durch $V_K(\cdot)$ ersetzt. Auch ergibt sich aus 3.9/2, dass algebraische Mengen des Typs $V_K(E)$ stets durch endlich viele Polynome in $K[X]$ definiert werden, also von der Form $V_K(f_1, \ldots, f_r)$ sind. In 3.9/3 erhält man die Relation $V_K(I(U)) = U$ für Teilmengen $U \subset K^n$ des Typs $U = V_K(\mathfrak{a})$ mit einem Ideal $\mathfrak{a} \subset K[X]$. Die Gleichung $I(V(\mathfrak{a})) = \mathfrak{a}$ für reduzierte Ideale $\mathfrak{a} \subset K[X]$ jedoch, welche sozusagen die Aussage des Hilbertschen Nullstellensatzes 3.9/4 darstellt, lässt sich nicht übertragen. Man betrachte etwa für $K = \mathbb{R}$ und $n = 1$ das Ideal

$\mathfrak{a} = (X^2+1) \subset \mathbb{R}[X]$. Dann gilt $V_{\mathbb{R}}(\mathfrak{a}) = \emptyset$ und somit $I(V_{\mathbb{R}}(\mathfrak{a})) = \mathbb{R}[X] \neq \mathfrak{a}$. Beim Hilbertschen Nullstellensatz kann man also nicht darauf verzichten, die Nullstellen in einem algebraisch abgeschlossenen Körper zu betrachten.

4.1, Aufg. 1. Ist L/K eine endliche Galois-Erweiterung, so entsprechen aufgrund des Hauptsatzes der Galois-Theorie 4.1/6 die Zwischenkörper von L/K bijektiv den Untergruppen der Galois-Gruppe $\mathrm{Gal}(L/K)$. Dies haben wir in 4.1/8 benutzt, um einzusehen, dass jede endliche separable Körpererweiterung nur endlich viele Zwischenkörper besitzt, ein Resultat, das für nicht-separable (endliche) Erweiterungen seine Gültigkeit verliert. Da die Zwischenkörper von L/K gemäß 4.1/6 als Fixkörper zu den Untergruppen von $\mathrm{Gal}(L/K)$ interpretiert werden können, lassen sich diese bei genügend guter Kenntnis der Galois-Automorphismen sowie der Gruppenstruktur von $\mathrm{Gal}(L/K)$ explizit berechnen. Hiermit verbunden ist ein weiterer Aspekt der Galois-Theorie. Äquivalent zu der Vorgabe einer endlichen Galois-Erweiterung L/K ist die Vorgabe des Körpers L sowie einer endlichen Gruppe G von Automorphismen von L, nämlich der Galois-Gruppe von L/K, wobei dann $K = L^G$ gilt; vgl. 4.1/4 und 4.1/6. Wir werden diese Sicht im Abschnitt 4.11 über Galois-Descent noch weiter vertiefen.

4.1, Aufg. 2. Es sei L/K eine endliche quasi-galoissche Körpererweiterung mit Automorphismengruppe $G = \mathrm{Aut}_K(L)$. Dann ist L/L^G gemäß 4.1/5 (i) eine Galois-Erweiterung mit Galois-Gruppe G. Weiter ist $L^G = K_i$ (im Falle $\mathrm{char}\, K > 0$) die maximale rein inseparable Erweiterung von K in L; vgl. 3.7/5 und 4.1/5 (iii). Man kann daher die Aussage von 4.1/6 verallgemeinern, indem man sagt, dass die Untergruppen von G in der in 4.1/6 beschriebenen Art bijektiv denjenigen Zwischenkörpern von L/K entsprechen, welche die maximale rein inseparable Erweiterung K_i als Teilkörper enthalten.

4.1, Aufg. 3. Ist L/K eine Galois-Erweiterung und $\mathrm{Gal}(L/K) = \mathrm{Aut}_K(L)$ die zugehörige Galois-Gruppe, so folgt mit 4.1/5 (ii), dass K der Fixkörper unter der Automorphismengruppe $\mathrm{Aut}_K(L)$ ist. Die Umkehrung hierzu ergibt sich mit 4.1/4.

4.2, Aufg. 1. Ist L/K eine Galois-Erweiterung beliebigen Grades, so lässt sich L als Vereinigung über das System $(L_i)_{i\in I}$ aller Zwischenkörper zu L/K auffassen, die endlich und galoissch über K sind; man vergleiche hierzu den Beginn von Abschnitt 4.2. Als Konsequenz hierzu ist ein Element $a \in L$, etwa $a \in L_i$, genau dann invariant unter einer Untergruppe $H \subset \mathrm{Gal}(L/K)$, wenn a invariant unter dem Bild $H_i = f_i(H)$ bezüglich

der Restriktionsabbildung $f_i\colon \mathrm{Gal}(L/K) \longrightarrow \mathrm{Gal}(L_i/K)$ ist. Mit anderen Worten, es gilt $L^H \cap L_i = L_i^{H_i}$, also $L^H = \bigcup_{i\in I} L_i^{H_i}$. Gehen wir in umgekehrter Weise von einem Zwischenkörper E zu L/K aus, so können wir zu E die Untergruppe $H = \mathrm{Gal}(L/E)$ von $\mathrm{Gal}(L/K)$ betrachten. Es gilt $H = \bigcap_{i\in I} f_i^{-1}(\mathrm{Gal}(L_i/L_i \cap E))$ sowie $f_i(H) = \mathrm{Gal}(L_i/L_i \cap E)$, wobei man letztere Gleichung unter Verwendung des Fortsetzungsarguments 3.4/9 nachweist. Mit diesen Formeln wird die Galois-Theorie von L/K sozusagen zurückgeführt auf die Galois-Theorien der Erweiterungen L_i/K. Benutzt man den Hauptsatz 4.1/6 für diese Erweiterungen, so erhält man für einen Zwischenkörper E zu L/K mit Galois-Gruppe $H = \mathrm{Gal}(L/E)$ wegen $f_i(H) = \mathrm{Gal}(L_i/L_i \cap E)$ sofort $L^H \cap L_i = E \cap L_i$, also $L^H = E$. Geht man umgekehrt von einer Untergruppe $H \subset \mathrm{Gal}(L/K)$ aus und bildet deren Fixkörper L^H, so ergibt sich $\mathrm{Gal}(L/L^H) = \bigcap_{i\in I} f_i^{-1}(f_i(H))$, eine Gruppe, die H umfasst und im Allgemeinen von H verschieden ist. In diesem Punkt unterscheidet sich die allgemeine Version 4.2/3 des Hauptsatzes der Galois-Theorie von der Version 4.1/6 für endliche Galois-Erweiterungen.

4.2, Aufg. 2. Wir haben soeben erklärt, dass die Galois-Theorie einer Galois-Erweiterung L/K charakterisiert ist durch die Galois-Theorien der Erweiterungen L_i/K, $i \in I$, wobei $(L_i)_{i\in I}$ das System derjenigen Zwischenkörper zu L/K ist, die endlich und galoissch über K sind. Von daher gesehen ist es natürlich, einen Galois-Automorphismus $\sigma\colon L \longrightarrow L$ mit dem System seiner Beschränkungen $(\sigma|_{L_i})_{i\in I}$ zu identifizieren. Verfolgt man diesen Standpunkt in konsequenter Weise, so gelangt man zu der Interpretation von $\mathrm{Gal}(L/K)$ als projektivem Limes der Galois-Gruppen $\mathrm{Gal}(L_i/K)$, also von $\mathrm{Gal}(L/K)$ als proendlicher Gruppe. Somit trägt $\mathrm{Gal}(L/K)$ in natürlicher Weise eine Topologie, die von den diskreten Topologien auf den Gruppen $\mathrm{Gal}(L_i/K)$ induziert wird. Wie wir in 4.2/3 bzw. 4.2/4 gesehen haben, ist diese Topologie geeignet, um diejenigen Untergruppen in $\mathrm{Gal}(L/K)$ zu beschreiben, die als Galois-Gruppen $\mathrm{Gal}(L/E)$ zu Zwischenkörpern E von L/K interpretiert werden können; dies sind nämlich gerade die abgeschlossenen Untergruppen von $\mathrm{Gal}(L/K)$. Kennt man allerdings für eine unendliche Galois-Erweiterung L/K die zugehörige Galois-Gruppe $\mathrm{Gal}(L/K)$ lediglich als rein abstrakte Gruppe, ohne dass Anhaltspunkte über die zugehörige Topologie gegeben sind, so ist dies im Sinne der Galois-Theorie von L/K nur von relativ geringem Wert. Beim Studium von unendlichen Galois-Gruppen $\mathrm{Gal}(L/K)$ hat man die Wahl, ob man deren Topologie in direkter Weise einführt, vgl. etwa 4.2/1, oder ob man lieber den Formalismus

projektiver Limiten benutzt. Letzteres ist meist von Vorteil bei konkreten Berechnungen, vgl. etwa 4.2/11.

4.3, Aufg. 1. Jede Gruppe G lässt sich als Untergruppe der Gruppe der bijektiven Selbstabbildungen $G \longrightarrow G$ auffassen, indem man ein Element $a \in G$ jeweils mit der zugehörigen Linkstranslation $\tau_a \colon G \longrightarrow G, g \longmapsto ag$, identifiziert. Zur Lösung der Aufgabe ist daher lediglich zu zeigen, dass jede Untergruppe G einer Permutationsgruppe $\mathfrak{S}_n$ als Galois-Gruppe realisiert werden kann. Letzteres ist aber in einfacher Weise möglich. Man betrachte den rationalen Funktionenkörper $L = k(T_1, \ldots, T_n)$ in n Variablen $T_1, \ldots, T_n$ über einem Konstantenkörper k. Ähnlich wie bei der Betrachtung der allgemeinen Gleichung n-ten Grades lässt sich G als Untergruppe der Automorphismengruppe von L auffassen, indem man die Elemente von G jeweils als Permutationen der Variablen $T_1, \ldots, T_n$ interpretiert. Es ist dann L/L^G nach 4.1/4 eine Galois-Erweiterung mit Galois-Gruppe G. Viel schwieriger und teilweise noch ungelöst ist allerdings die Frage, ob eine gegebene endliche Gruppe stets als Galois-Gruppe einer Erweiterung $L/\mathbb{Q}$ zu realisieren ist.

4.4, Aufg. 1. Die Diskriminante Δ_f eines normierten Polynoms f mit Koeffizienten aus einem Ring R soll der Intention nach in gewissem Sinne ein Maß für den Abstand der Nullstellen von f liefern, selbst wenn letztere erst nach Erweiterung von R auftreten; vgl. 4.4/3. Es stellt sich dabei das Problem der Berechnung von Δ_f. Man könnte versuchen, R so zu erweitern, dass f vollständig in Linearfaktoren zerfällt, um anschließend das Produkt über die Quadrate der Differenzen der Nullstellen von f zu berechnen. Dieses Verfahren ist im Allgemeinen jedoch wenig praktikabel, man denke nur an die Probleme, die auftreten, wenn man Polynome mit Koeffizienten aus $\mathbb{Q}, \mathbb{R}$ oder $\mathbb{C}$ in konkreter Weise faktorisieren möchte. Stattdessen führt man die Rechnung in einem "universellen" Fall aus und zeigt, dass sich diese mittels Ringhomomorphismen in alle anderen Situationen übertragen lässt. Man betrachtet nämlich speziell das Polynom $f = \prod_{i=1}^{n}(X - T_i)$ in der Variablen X über dem Koeffizientenring $\mathbb{Z}[T_1, \ldots, T_n]$. An dieser Stelle wird der Hauptsatz über elementarsymmetrische Funktionen 4.4/1 verwendet, um die Diskriminante Δ_f als ganzzahliges Polynom in den Koeffizienten von f, nämlich den elementarsymmetrischen Polynomen $s_1, \ldots, s_n$, darzustellen. Die resultierende Identität kann anschließend mittels Ringhomomorphismen in allgemeine Koeffizientenbereiche transportiert werden. Auf diese

Weise erhält man eine Formel für Δ_f, die in jedem Koeffizientenbereich gültig ist.

Beschränkt man sich beim Hauptsatz über elementarsymmetrische Polynome 4.4/1 auf Polynome mit Koeffizienten aus einem Körper K, so muss man das allgemeine Polynom $f = \prod_{i=1}^{n}(X - T_i)$ als ein Polynom in X mit Koeffizienten in $K[T_1, \ldots, T_n]$ sehen. Man erhält dann Δ_f als Polynom in $s_1, \ldots, s_n$, nunmehr aber mit Koeffizienten, von denen man nur weiß, dass sie in K liegen. Für Körper unterschiedlicher Charakteristik besteht dann keine Chance mehr, die verschiedenen Darstellungen für Δ_f zueinander in Relation zu setzen.

4.5, Aufg. 1. Sei $\Phi_n = g_1 \ldots g_r$ die Primfaktorzerlegung des Kreisteilungspolynoms $\Phi_n \in K[X]$, wobei die Faktoren $g_1, \ldots, g_r$ aufgrund der Separabilität von Φ_n paarweise verschieden sind. Da die Nullstellen der g_i gerade aus den primitiven n-ten Einheitswurzeln bestehen, können wir jedes g_i als Minimalpolynom über K einer primitiven n-ten Einheitswurzel auffassen. Alle diese Einheitswurzeln erzeugen den gleichen Erweiterungskörper von K, nämlich $K(\zeta)$, d. h. es folgt $\operatorname{grad} g_i = [K(\zeta) : K] = s$ für alle i. Da Φ_n den Grad $\varphi(n)$ besitzt, gilt $r = \varphi(n)/s$ wie behauptet.

4.5, Aufg. 2. Man wähle $m, n \in \mathbb{N} - \{0\}$ und primitive m-te bzw. n-te Einheitswurzeln $\zeta_m, \zeta_n \in \overline{\mathbb{Q}}$. Da ζ_n eine Nullstelle von Φ_n ist, erhält man die Abschätzung $[\mathbb{Q}(\zeta_m, \zeta_n) : \mathbb{Q}(\zeta_m)] \leq \operatorname{grad} \Phi_n = \varphi(n)$, und es folgt, dass Φ_n genau dann irreduzibel über $\mathbb{Q}(\zeta_m)$ ist, wenn die Beziehung $[\mathbb{Q}(\zeta_m, \zeta_n) : \mathbb{Q}(\zeta_m)] = \varphi(n)$ gilt, d. h. unter Benutzung von $[\mathbb{Q}(\zeta_m) : \mathbb{Q}] = \varphi(m)$, wenn $[\mathbb{Q}(\zeta_m, \zeta_n) : \mathbb{Q}] = \varphi(m) \cdot \varphi(n)$ gilt. Um diese Gleichung weiter zu untersuchen, berechnen wir den Grad von $\mathbb{Q}(\zeta_m, \zeta_n)/\mathbb{Q}$. Sei $k = \operatorname{kgV}(m, n)$. Dann enthält $\mathbb{Q}(\zeta_m, \zeta_n)$ gemäß 3.6/13 eine primitive k-te Einheitswurzel ζ, und es folgt $\mathbb{Q}(\zeta_m, \zeta_n) = \mathbb{Q}(\zeta)$, also $[\mathbb{Q}(\zeta_m, \zeta_n) : \mathbb{Q}] = \varphi(k)$.

Somit ergibt sich aus unseren Überlegungen, dass Φ_n genau dann irreduzibel über $\mathbb{Q}(\zeta_m)$ ist, wenn $\varphi(\operatorname{kgV}(m, n)) = \varphi(m) \cdot \varphi(n)$ gilt. Wir wählen nun wie in 3.6/13 Zerlegungen $m = m_0 m'$ und $n = n_0 n'$ mit $\operatorname{kgV}(m, n) = m_0 n_0$ und $\operatorname{ggT}(m_0, n_0) = 1$. Aufgrund von 4.5/4 folgt dann

$$\varphi\big(\operatorname{kgV}(m, n)\big) = \varphi(m_0) \cdot \varphi(n_0) \leq \varphi(m) \cdot \varphi(n),$$

wobei Gleichheit lediglich für $\varphi(m_0) = \varphi(m)$ und $\varphi(n_0) = \varphi(n)$ besteht. Mit der expliziten Formel in 4.5/4 (iii) sieht man weiter, dass $\varphi(m_0) = \varphi(m)$

äquivalent zu $m' \in \{1, 2\}$ ist. Entsprechendes gilt für die Zerlegung $n = n_0 n'$, und es folgt, dass Φ_n genau dann irreduzibel über $\mathbb{Q}(\zeta_m)$ ist, wenn $\mathrm{ggT}(m, n) \in \{1, 2\}$ gilt.

4.6, Aufg. 1. Es ist $\mathbb{F}$ von der Form $\mathbb{F}_q$, wobei q Potenz einer Primzahl p ist. Die multiplikative Gruppe von $\mathbb{F}_q$ ist nach 3.8/5 zyklisch von der Ordnung $q - 1$. Wir haben also alle Gruppenhomomorphismen $G \longrightarrow \mathbb{Z}/(q-1)\mathbb{Z}$ zu bestimmen. Sei ζ ein erzeugendes Element von G, und sei ζ zunächst von unendlicher Ordnung. Dann lässt sich für jedes $a \in \mathbb{Z}/(q-1)\mathbb{Z}$ in eindeutiger Weise ein Gruppenhomomorphismus $G \longrightarrow \mathbb{Z}/(q-1)\mathbb{Z}$ durch $\zeta \longmapsto a$ definieren. In diesem Falle gibt es also $q - 1$ Charaktere auf G mit Werten in $\mathbb{F}^*$.

Sei nun G eine zyklische Gruppe endlicher Ordnung $m > 0$. Ist dann $G \longrightarrow \mathbb{Z}/(q-1)\mathbb{Z}$ ein Homomorphismus mit Bild a von ζ, so gilt $m \cdot a = 0$. Umgekehrt lässt sich zu jedem Element $a \in \mathbb{Z}/(q-1)\mathbb{Z}$, dessen Ordnung ein Teiler von m ist, ein Homomorphismus $G \longrightarrow \mathbb{Z}/(q-1)\mathbb{Z}$ durch $\zeta \longmapsto a$ definieren. Somit korrespondieren die gesuchten Homomorphismen in bijektiver Weise zu den Elementen von $\mathbb{Z}/(q-1)\mathbb{Z}$, deren Ordnung ein Teiler von m ist. Eine elementare Rechnung zeigt, dass deren Anzahl gleich $\mathrm{ggT}(m, q-1)$ ist.

4.7, Aufg. 1. Betrachten wir L als K-Vektorraum, so können wir die Abbildung $\mathrm{Sp}_{L/K} \colon L \longrightarrow K$ als Linearform auf L ansehen. Folglich ist der Kern dieser Abbildung, also die Menge $\{a \in L\,;\ \mathrm{Sp}_{L/K}(a) = 0\}$, ein K-Untervektorraum von L. Ist L/K separabel, so ist die Linearform $\mathrm{Sp}_{L/K}$ nicht trivial und daher $\ker \mathrm{Sp}_{L/K}$ ein $(n-1)$-dimensionaler K-Untervektorraum von L. Ist dagegen L/K nicht separabel, so ist $\mathrm{Sp}_{L/K}$ die Nullabbildung, und es gilt $\ker \mathrm{Sp}_{L/K} = L$.

4.7, Aufg. 2. Sei n der Grad der Erweiterung $\mathbb{F}'/\mathbb{F}$, also etwa $\mathbb{F} = \mathbb{F}_q$, $\mathbb{F}' = \mathbb{F}_{q'}$ mit Primpotenzen q und q', wobei $q' = q^n$. Wir wollen zunächst zeigen, dass die Normabbildung $\mathrm{N} \colon \mathbb{F}'^* \longrightarrow \mathbb{F}^*$ surjektiv ist. Berücksichtigen wir, dass die Galois-Gruppe $\mathrm{Gal}(\mathbb{F}'/\mathbb{F})$ vom relativen Frobenius-Homomorphismus $a \longmapsto a^q$ erzeugt wird, so berechnet sich die Norm eines Elementes $a \in \mathbb{F}'$ zu

$$\mathrm{N}(a) = a \cdot a^q \cdot a^{q^2} \cdot \ldots \cdot a^{q^{n-1}} = a^{\frac{q^n-1}{q-1}},$$

und man sieht insbesondere $\mathrm{N}(a)^{q-1} = a^{q^n-1} = 1$. Wir benutzen nun, dass die Gruppe $\mathbb{F}'^*$ zyklisch ist, also von einem Element α der Ordnung $q^n - 1$

erzeugt wird. Dann ist $\mathrm{N}(\alpha) = \alpha^{\frac{q^n-1}{q-1}} \in \mathbb{F}$ von der Ordnung $q-1$, also erzeugendes Element der zyklischen Gruppe $\mathbb{F}^*$. Als Gruppenhomomorphismus ist $\mathrm{N}\colon \mathbb{F}'^* \longrightarrow \mathbb{F}^*$ damit surjektiv. Weiter erkennt man, dass der Kern von N aus allen Elementen α^r besteht mit $(q-1) \mid r$ oder, mit anderen Worten, aus allen Elementen, die $(q-1)$-te Potenz eines Elementes aus $\mathbb{F}'^*$ sind.

4.8, Aufg. 1. Es sei L/K eine endliche zyklische Galois-Erweiterung mit erzeugendem Element $\sigma \in \mathrm{Gal}(L/K)$. Zu $b \in L^*$ habe man $a, a' \in L^*$ mit $b = a\sigma(a)^{-1} = a'\sigma(a')^{-1}$. Dann ergibt sich $\sigma(a/a') = a/a'$ und somit $a/a' \in K^*$. Umgekehrt gilt für $a/a' \in K^*$ natürlich $a\sigma(a)^{-1} = a'\sigma(a')^{-1}$. Ist daher $b \in L^*$ mit $\mathrm{N}_{L/K}(b) = 1$ gegeben, so ist das nach 4.8/1 existierende Element $a \in L^*$ mit $b = a\sigma(a)^{-1}$ eindeutig bis auf eine multiplikative Konstante aus K^*. Genauso zeigt man in der Situation von 4.8/4, dass zu gegebenem $b \in L$ mit $\mathrm{Sp}_{L/K}(b) = 0$ das zugehörige Element $a \in L$ mit $b = a - \sigma(a)$ eindeutig ist bis auf eine additive Konstante aus K.

4.8, Aufg. 2. Die Galois-Gruppe $\mathrm{Gal}(\mathbb{C}/\mathbb{R})$ ist zyklisch von der Ordnung 2, sie wird erzeugt von der komplexen Konjugation $\mathbb{C} \longrightarrow \mathbb{C}$, $z \longmapsto \overline{z}$. Für $z \in \mathbb{C}$ folgt daher $\mathrm{N}_{\mathbb{C}/\mathbb{R}}(z) = z\overline{z} = |z|^2$. Gelte nun $\mathrm{N}_{\mathbb{C}/\mathbb{R}}(z) = 1$, d. h. es liege z auf dem Rand des Einheitskreises um 0. Hilberts Theorem 90 besagt dann, dass es ein $x \in \mathbb{C}^*$ mit $z = x/\overline{x}$ gibt, wobei wir sogar $x\overline{x} = |x|^2 = 1$ annehmen dürfen. Es gilt dann $z = x^2$, d. h. x ist eine Quadratwurzel von z.

4.9, Aufg. 1. Wir betrachten zunächst eine zyklische Erweiterung L/K vom Grad n; sei $C = L^n \cap K^*$. Es gilt $L = K(C^{1/n})$ aufgrund von 4.9/3 und $n = [L : K] = (C : K^{*n})$ aufgrund von 4.9/1. Die Galois-Gruppe $G_C = \mathrm{Gal}(L/K)$ ist zyklisch von der Ordnung n. Gleiches gilt dann nach 4.9/3 für $\mathrm{Hom}(C/K^{*n}, U_n)$ und nach 4.9/2 für C/K^{*n}. Wählt man nun ein Element $c \in C$, dessen Restklasse die Gruppe C/K^{*n} erzeugt, so folgt $L = K(c^{1/n})$, d. h. die Erweiterung L/K entsteht durch Adjunktion einer Nullstelle a des Polynoms $X^n - c \in K[X]$. Dieses Polynom ist aus Gradgründen irreduzibel und ist folglich das Minimalpolynom von a über K.

Sei nun umgekehrt L/K eine Erweiterung, die durch Adjunktion einer Nullstelle a eines Polynoms des Typs $X^n - c$ entsteht, wobei wir $c \in K^*$ voraussetzen wollen. Bezeichnet dann C die von c und K^{*n} in K^* erzeugte Untergruppe, so gilt $L = K(C^{1/n})$, und es ist L/K gemäß 4.9/3 eine abelsche Erweiterung mit Galois-Gruppe $\mathrm{Hom}(C/K^{*n}, U_n)$ bzw. C/K^{*n}, da letztere Gruppe endlich ist. Die Gruppe C/K^{*n} ist sogar zyklisch, da sie von der Restklasse zu c erzeugt wird, und wir sehen, dass die Erweiterung L/K

zyklisch ist. Da $c^n \in K^{*n}$ gilt, ist C/K^{*n} zyklisch von einer Ordnung d, die n teilt. Folglich gilt $c^d \in K^{*n}$, also $a^d \in K$, und man sieht ähnlich wie oben, dass $X^d - a^d$ das Minimalpolynom von a über K ist.

4.9, Aufg. 2. Es ist $C = K^*$ die größte aller Untergruppen von K^*, die K^{*n} enthalten, und es folgt aus 4.9/3, dass entsprechend $L_n = K(K^{*1/n})$ die größte abelsche Erweiterung von K ist mit einem Exponent, der n teilt. Da jeder Homomorphismus $K^* \longrightarrow U_n$ notwendig trivial auf K^{*n} ist, ergibt sich $\mathrm{Gal}(L_n/K) = \mathrm{Hom}(K^*, U_n)$, wiederum mit 4.9/3.

4.10, Aufg. 1. Wir nehmen an, dass wir uns in der Situation von Theorem 4.10/1 befinden und behaupten, dass eine Körpererweiterung L/K genau dann zyklisch von einem Grad ist, der n teilt, wenn es ein Element $\alpha \in A$ mit $\wp(\alpha) \in A_K$ und $L = K(\alpha)$ gibt. Die Argumentation ist wie in Aufgabe 1 aus Abschnitt 4.9. Sei zunächst L/K eine zyklische Erweiterung mit einem Grad, der n teilt. Gemäß 4.10/1 gilt dann $L = K(\wp^{-1}(C))$ mit $C = \wp(A_L) \cap A_K$, und man hat einen Isomorphismus $C/\wp(A_K) \xrightarrow{\sim} \mathrm{Hom}(G_C, \mu_n)$, wobei G_C die Galois-Gruppe zu L/K ist. G_C ist nach Annahme zyklisch von einer Ordnung, die n teilt. Aufgrund von 4.9/2 folgt Gleiches auch für $C/\wp(A_K)$ und wir können ein Element $c \in C$ finden, dessen Restklasse $C/\wp(A_K)$ erzeugt. Ist dann $\alpha \in \wp^{-1}(c)$ ein Urbild, so wird $\wp^{-1}(C)$ von α und A_K erzeugt, und es folgt wie gewünscht $L = K(\alpha)$.

Sei umgekehrt $L = K(\alpha)$ mit einem $\alpha \in A$, welches $\wp(\alpha) \in A_K$ erfüllt. Dann folgt $L = K(\wp^{-1}(C))$ mit C erzeugt von $\wp(\alpha)$ und $\wp(A_K)$, und es ist $C/\wp(A_K)$ zyklisch, erzeugt von der Restklasse zu $\wp(\alpha)$. Hieraus schließt man mit 4.10/1, dass L/K eine abelsche Erweiterung von einem Exponenten ist, der n teilt, und in Verbindung mit 4.9/2, dass L/K sogar zyklisch ist.

4.10, Aufg. 2. Es ist K vollkommen und folglich der Frobenius-Homomorphismus $K \longrightarrow K$ ein Isomorphismus. Gleiches gilt dann auch für den Frobenius-Operator $F\colon W(K) \longrightarrow W(K)$. Insbesondere impliziert die Gleichung $V \circ F = p$ aus 4.10/7 bereits $p \cdot W(K) = V^1 W(K)$.

Zur Behauptung in (i) erinnern wir an die in Abschnitt 4.10 angegebene Formel

$$(\alpha, 0, 0, \ldots) \cdot (\beta, 0, 0, \ldots) = (\alpha \cdot \beta, 0, 0, \ldots)$$

für die Multiplikation in $W(K)$. Sie besagt gerade, dass die zu betrachtende Abbildung $K \longrightarrow W(K)$, $\alpha \longmapsto (\alpha, 0, 0, \ldots)$, multiplikativ ist

und sich insbesondere zu einem Monomorphismus multiplikativer Gruppen $K^* \longrightarrow W(K)^*$ einschränkt. Auf der anderen Seite aber kann es keine nicht-triviale Abbildung $K \longrightarrow W(K)$ geben, die additiv ist, denn die Multiplikation mit p auf K ist die Nullabbildung, auf $W(K)$ hingegen, abgesehen vom Frobenius-Operator, der Verschiebungsoperator.

Als Nächstes behandeln wir Behauptung (ii). Zu zeigen ist, dass $W(K)$ mit den Projektionen $W(K) \longrightarrow W(K)/V^n W(K)$ ein projektiver Limes des projektiven Systems

$$W(K)/V^0 W(K) \longleftarrow W(K)/V^1 W(K) \longleftarrow W(K)/V^2 W(K) \longleftarrow \ldots$$

ist. Wir verifizieren hierzu die definierende universelle Eigenschaft aus Abschnitt 4.2. Sei also R ein Ring und $(h_n)_{n\in\mathbb{N}}$ ein System von Ringhomomorphismen $h_n\colon R \longrightarrow W(K)/V^n W(K)$, welches mit allen Projektionen

$$W(K)/V^{i+1} W(K) \longrightarrow W(K)/V^i W(K), \qquad i \in \mathbb{N},$$

verträglich ist. Dann faktorisieren die h_n in eindeutiger Weise über $W(K)$, und zwar vermöge der Abbildung

$$h\colon R \longrightarrow W(K), \qquad x \longmapsto \big(h_1(x)_0, h_2(x)_1, h_3(x)_2, \ldots\big),$$

wobei $h_{n+1}(x)_n$ für $n \in \mathbb{N}$ jeweils die Komponente mit Index n des Elements $h_{n+1}(x) \in W(K)/V^{n+1} W(K)$ bezeichne. Dass h sogar ein Ringhomomorphismus ist, ergibt sich aus formaler Argumentation im Sinne projektiver Limites oder durch explizites Ausnutzen der Definition der Ringstruktur auf $W(K)$ mittels der Polynome S_n, P_n. Der erste Teil von Behauptung (ii) ist damit bewiesen, und es folgt mit 4.10/10 auch leicht der zweite Teil, dass nämlich $W(\mathbb{F}_p)$ mit $\mathbb{Z}_p$ übereinstimmt.

Zum Nachweis von (iii) betrachten wir die kanonische Projektion $W(K) \longrightarrow W_1(K) = K$. Diese ist ein Epimorphismus mit zugehörigem Kern $V^1 W(K) = p \cdot W(K)$, und es folgt, dass $p \cdot W(K)$ ein maximales Ideal in $W(K)$ ist. Wir behaupten weiter, dass dieses Ideal das einzige maximale Ideal in $W(K)$ ist, ja dass die Einheitengruppe $W(K)^*$ mit $W(K) - V^1 W(K)$ übereinstimmt. Sei also $a \in W(K) - V^1 W(K)$. Um zu zeigen, dass a eine Einheit ist, dürfen wir ohne Einschränkung a durch eine Einheit des Typs $(\alpha, 0, 0, \ldots)$ mit $\alpha \in K^*$ abändern; vgl. (i). Auf diese Weise können wir a von der Form $1 - p \cdot c$ annehmen mit $c \in W(K)$. Man überzeugt sich nun leicht davon, indem man die Gleichung $p^r \cdot W(K) = V^r W(K)$ benutzt, dass

$b = \sum_{i\in\mathbb{N}} p^i \cdot c^i$ als ein wohldefiniertes Element in $W(K)$ aufgefasst werden kann; das Bild einer jeden endlichen Summe $\sum_{i=0}^{s} p^i \cdot c^i$ unter der Projektion $W(K) \longrightarrow W(K)/V^n W(K)$ ist nämlich unabhängig von s für $s \geq n$. Weiter ergibt sich aufgrund der Formel für die geometrische Reihe, dass $a \cdot b$ unter jeder Projektion $W(K) \longrightarrow W(K)/V^n W(K)$ auf das Einselement abgebildet wird, dass also $a \cdot b = 1$ in $W(K)$ gilt.

Wir haben damit $W(K) - p \cdot W(K) = W(K) - V^1 W(K)$ als Einheitengruppe von $W(K)$ erkannt. Weiter gibt es zu jedem $a \in W(K)$ mit $a \neq 0$ eine eindeutig bestimmte natürliche Zahl $n \in \mathbb{N}$ mit $a \in V^n W(K) - V^{n+1} W(K)$. Wir können dann $a = p^n \cdot a'$ schreiben, wobei $a' \in W(K) - V^1 W(K)$, also mit einer Einheit $a' \in W(K)^*$. Da p wegen $p^n \cdot W(K) = V^n(K)$ nicht nilpotent sein kann, ist $W(K)$ insbesondere ein Integritätsring. Im Übrigen gilt für jedes nicht-triviale Ideal $\mathfrak{a} \subset W(K)$ offenbar

$$\mathfrak{a} = (p^n) \quad \text{mit} \quad n = \min\{i \in \mathbb{N}\,;\, p^i \in \mathfrak{a}\},$$

d. h. $W(K)$ ist ein Hauptidealring. Hinzugefügt sei, dass Hauptidealringe mit genau einem nicht-trivialen maximalen Ideal auch als *diskrete Bewertungsringe* bezeichnet werden. $W(K)$ ist daher ein solcher diskreter Bewertungsring.

4.11, Aufg. 1. Man wähle eine K-Vektorraumbasis $(a_i)_{i\in I}$ von A. Es ist dann $(a_i \otimes 1)_{i\in I}$ eine K'-Vektorraumbasis von $A \otimes_K K'$, jedes Element aus $A \otimes_K K'$ hat also eine Darstellung $\sum_{i\in I} a_i \otimes c_i$ mit eindeutig bestimmten Elementen $c_i \in K'$, wobei $c_i = 0$ für fast alle Indizes $i \in I$ gilt. Um nun die Multiplikation auf $A \otimes_K K'$ mit einem Element $\sum_{j\in I} a_j \otimes c'_j$ zu erklären, gehen wir schrittweise vor und definieren zunächst die (Rechts-) Multiplikation mit einem Term $a_j \otimes c'_j$:

$$\varphi_{a_j,c'_j} \colon A \otimes_K K' \longrightarrow A \otimes_K K', \qquad \sum_{i\in I} a_i \otimes c_i \longmapsto \sum_{i\in I} a_i a_j \otimes c_i c'_j.$$

Anschließend erhält man die Multiplikation mit $\sum_{j\in I} a_j \otimes c'_j$ als Summe der Abbildungen φ_{a_j,c'_j}. Auf diese Weise ergibt sich eine Abbildung

$$(A \otimes_K K') \times (A \otimes_K K') \longrightarrow A \otimes_K K',$$

welche durch die Vorschrift $(a \otimes c, a' \otimes c') \longmapsto aa' \otimes cc'$ charakterisiert ist, wie man leicht nachprüft. Hiermit lassen sich die Eigenschaften einer Ringmultiplikation in direkter Weise verifizieren, indem man die entsprechenden

Eigenschaften für A und K' benutzt. Weiter ist $A \otimes_K K'$ eine K'-Algebra vermöge des Ringhomomorphismus $K' \longrightarrow A \otimes_K K'$, $c \longmapsto 1 \otimes c$.

4.11, Aufg. 2. Zum Nachweis von Aussage 4.11/4 (i) genügt es zu zeigen, dass für jeden K-Untervektorraum $V_0 \subset V$ von endlicher Dimension die durch $\lambda\colon V \hookrightarrow V'$ gegebene zugehörige K'-lineare Abbildung $\lambda'_0\colon K' \otimes_K V_0 \longrightarrow V'$ injektiv ist. Wir verifizieren Letzteres mit Induktion nach $r = \dim_K V_0$. Für $r = 0$ ist nichts zu zeigen. Sei also $r > 0$. Dann existiert ein von Null verschiedener Vektor $x \in V_0$, und wir können den K-Vektorraum V_0/Kx als Teil der Fixmenge zu der von f auf $V'/K'x$ induzierten Aktion betrachten. Nach Induktionsvoraussetzung ist die kanonische K'-lineare Abbildung $K' \otimes_K (V_0/Kx) \longrightarrow V'/K'x$ injektiv, und eine leichte Rechnung zeigt, dass dann auch $\lambda'_0\colon K' \otimes_K V_0 \longrightarrow V'$ injektiv ist.

Nun zum Beweis von 4.11/4 (ii). Es gilt $f_\sigma(\alpha_i v) = \sigma(\alpha_i) f_\sigma(v)$, also

$$\sum_{\sigma\in G} f_\sigma(\alpha_i v) = \sum_{\sigma\in G} \sigma(\alpha_i) f_\sigma(v), \qquad i = 1, \ldots, n.$$

Da die Matrix $(\sigma(\alpha_i))_{\sigma\in G, i=1\ldots n} \in (K')^{n\times n}$ gemäß 4.6/3 invertierbar ist, lassen sich die Elemente $f_\sigma(v)$, $\sigma \in G$, insbesondere also v, als K'-Linearkombination der Elemente $v_i = \sum_{\sigma\in G} f_\sigma(\alpha_i v)$, $i = 1, \ldots, n$, darstellen. Die v_i werden unter der Aktion von G auf V' festgelassen, gehören also zu V. Hieraus ergibt sich die Surjektivität der Abbildung $\lambda'\colon K' \otimes_K V \longrightarrow V'$ in direkter Weise.

5.1, Aufg. 1. Die H-Bahn eines Elementes $g \in G$ unter der Linkstranslation mit H, also unter der Aktion $H \times G \longrightarrow G$, $(h, g) \longmapsto hg$, wird gegeben durch die Rechtsnebenklasse Hg. Ist $\{g_1, \ldots, g_r\}$ ein Vertretersystem der Rechtsnebenklassen von G modulo H, so lautet die Bahnengleichung $\operatorname{ord} G = \sum_{i=1}^{r} \operatorname{ord}(Hg_i)$. Die Anzahl r der Rechtsnebenklassen zu H ist gleich dem Index $(G : H)$. Weiter besitzen alle Rechtsnebenklassen Hg_i gleiche Mächtigkeit. Folglich können wir die Bahnengleichung zu obiger Aktion in der Form $\operatorname{ord} G = (G : H) \cdot \operatorname{ord} H$ schreiben. Dies ist aber gerade die Formel, welche durch den Satz von Lagrange 1.2/3 gegeben wird. Betrachtet man statt der Linkstranslation die Rechtstranslation mit H, genauer die Aktion $H \times G \longrightarrow G$, $(h, g) \longmapsto gh^{-1}$, so sind die zugehörigen H-Bahnen von der Form gH, stellen also die Linksnebenklassen zu H dar. Auch in diesem Falle stimmt die zugehörige Bahnengleichung mit der Formel aus 1.2/3 überein.

5.1, Aufg. 2. Da ein Galois-Automorphismus $\sigma \in \mathrm{Gal}(L/K)$ ein Element $a \in L$ genau dann festlässt, wenn es den Körper $K(a)$ festlässt, ergibt sich die Isotropiegruppe zu a als $G_a = \mathrm{Gal}(L/K(a))$. Weiter besteht die Bahn Ga aus allen über K (im Sinne der Galois-Theorie) zu a konjugierten Elementen; vgl. 4.1. Ist etwa $f \in K[X]$ das Minimalpolynom von a über K, so sind dies gerade die Nullstellen von f. Es bildet nämlich jedes $\sigma \in \mathrm{Gal}(L/K)$ die Menge der Nullstellen von f wieder in sich ab. Andererseits zerfällt f wegen der Normalität von L/K in $L[X]$ vollständig in Linearfaktoren (vgl. 3.5/4 und 3.5/5), und es gibt zu jeder Nullstelle $a' \in L$ von f ein $\sigma \in \mathrm{Gal}(L/K)$ mit $\sigma(a) = a'$ (vgl. 3.4/8 und 3.4/9). Insbesondere gelten unter Benutzung der Separabilität von L/K die Gleichungen $\mathrm{ord}\, Ga = \mathrm{grad}\, f = [K(a) : K]$ und $\mathrm{ord}\, G_a = [L : K(a)]$.

5.2, Aufg. 1. Es sei G eine endliche abelsche Gruppe und p eine Primzahl. Theorem 5.2/6 (i) liefert dann die Existenz einer p-Sylow-Gruppe $S \subset G$. Da alle p-Sylow-Gruppen in G nach 5.2/6 (ii) zueinander konjugiert sind, G aber abelsch ist, sieht man, dass S die einzige p-Sylow-Gruppe in G ist. Es folgt dann durch erneute Anwendung von 5.2/6 (i), dass S von der in 5.2/2 beschriebenen Gestalt ist. Theorem 5.2/6 liefert also die Erkenntnis, dass die Elemente aus G, deren Ordnung eine p-Potenz ist, eine p-Sylow-Gruppe in G bilden, eine Tatsache, die wir in 5.2/2 auf elementare Weise eingesehen haben.

5.2, Aufg. 2. Ist $S \subset G$ eine p-Sylow-Gruppe, so enthält das Bild $\varphi(S)$ nur Elemente, deren Ordnung eine p-Potenz ist. Nach 5.2/11 ist $\varphi(S)$ daher eine p-Gruppe, und es folgt mit 5.2/6, dass es in G' eine p-Sylow-Gruppe S' mit $\varphi(S) \subset S'$ gibt. Ist φ injektiv, etwa $\varphi\colon G \hookrightarrow G'$, so gilt notwendig $S' \cap G = S$, denn es ist $S' \cap G$ eine p-Gruppe in G, die S enthält. Mit anderen Worten, ist $G \subset G'$ eine Untergruppe, so sind die p-Sylow-Gruppen von G Einschränkungen (gewisser) p-Sylow-Gruppen von G'. Ist allerdings G ein Normalteiler in G', so ist für jede p-Sylow-Gruppe $S' \subset G'$ auch deren Einschränkung $S' \cap G$ eine p-Sylow-Gruppe in G. Es ist nämlich $S' \cap G$ eine p-Gruppe und somit enthalten in einer p-Sylow-Untergruppe S von G. Dann ist S eine p-Gruppe in G', und es gibt ein $g \in G'$ mit $gSg^{-1} \subset S'$, vgl. 5.2/9. Aufgrund der Normalität von G gilt $gSg^{-1} \subset G$, und man erkennt gSg^{-1} wegen $\mathrm{ord}\, S = \mathrm{ord}\, gSg^{-1}$ als p-Sylow-Gruppe von G. Da aber gSg^{-1} in dem Schnitt $S' \cap G$ liegt und letztere Gruppe eine p-Gruppe ist, ergibt sich $S' \cap G = gSg^{-1}$, d. h. es ist $S' \cap G$ eine p-Sylow-Gruppe in G.

Wir wollen noch den Fall untersuchen, wo $\varphi\colon G \longrightarrow G'$ surjektiv ist. Sei wiederum $S \subset G$ eine p-Sylow-Gruppe. Wir behaupten, dass dann $H' = \varphi(S)$ eine p-Sylow-Gruppe in G' ist. Um dies einzusehen, betrachte man die Aktion von G durch Linkstranslation auf der *Menge* der Linksnebenklassen G'/H'. Diese Aktion ist transitiv, hat also nur eine einzige Bahn. Bezeichnet H die Isotropiegruppe der Klasse H' in G'/H', so gilt $S \subset H$ sowie $\operatorname{ord} G/H = \operatorname{ord} G'/H'$ aufgrund der Bahnengleichung. Aus $p \nmid \operatorname{ord}(G/S)$ folgt dann $p \nmid \operatorname{ord}(G/H)$ und somit $p \nmid \operatorname{ord}(G'/H')$. Also ist H' als p-Gruppe bereits eine p-Sylow-Gruppe in G'. Das Bild einer p-Sylow-Gruppe $S \subset G$ ist damit stets eine p-Sylow-Gruppe in G', und man kann leicht unter Benutzung der Konjugationsoperation einsehen, dass umgekehrt auch jede p-Sylow-Gruppe in G' Bild einer p-Sylow-Gruppe von G ist.

5.3, Aufg. 1. Eine Permutation $\pi \in \mathfrak{S}_n$ ist eine bijektive Selbstabbildung der Menge $\{1, \ldots, n\}$. Wir können uns dabei vorstellen, dass π die Zahlen $1, \ldots, n$ "permutiert", d. h. sie in eine andere Reihenfolge bringt, nämlich $\pi(1), \ldots, \pi(n)$. Eine Transposition vertauscht dabei in der Zahlenreihe $1, \ldots, n$ genau zwei Elemente. Nun ist es aber plausibel, dass man ausgehend von $1, \ldots, n$ diese Zahlen in eine beliebige Reihenfolge bringen kann, indem man in sukzessiver Weise jeweils zwei Elemente vertauscht. Nichts anderes als dies besagt die Aussage, dass jedes $\pi \in \mathfrak{S}_n$ Produkt von Transpositionen ist.

Wir wollen noch erläutern, wie man vorstehende Idee in einen strengen Beweis umsetzen kann. Wir benutzen Induktion nach n. Der Induktionsanfang $n = 1$ ist trivial, da $\mathfrak{S}_1$ nur das Einselement enthält und da wir letzteres als das leere Produkt ansehen können. Sei also $n > 1$. Existiert dann ein $i \in \{1, \ldots, n\}$ mit $\pi(i) = i$, so gibt π durch Einschränkung Anlass zu einer bijektiven Selbstabbildung π' von $\{1, \ldots, i-1, i+1, \ldots, n\}$. Nach Induktionsvoraussetzung ist π' ein Produkt von Transpositionen, und die gleiche Aussage gilt für π. Existiert andererseits ein Index $i \in \{1, \ldots, n\}$ mit $\pi(i) \neq i$, so lässt $(i, \pi(i)) \circ \pi$ das Element i fest, ist also nach dem eben Gezeigten ein Produkt von Transpositionen, etwa $(i, \pi(i)) \circ \pi = \tau_1 \circ \ldots \circ \tau_r$. Hieraus folgt $\pi = (i, \pi(i)) \circ \tau_1 \circ \ldots \circ \tau_r$, d. h. π ist Produkt von Transpositionen.

5.3, Aufg. 2. Es sei $\pi \in \mathfrak{S}_p$ ein p-Zyklus, etwa $\pi = (1, \ldots, p)$. Dann ist die von π erzeugte zyklische Gruppe $\langle \pi \rangle$ eine p-Sylow-Gruppe in $\mathfrak{S}_p$. Ihre Ordnung ist nämlich p, und es gilt $p \nmid (\mathfrak{S}_p : \langle \pi \rangle)$ wegen $(\mathfrak{S}_p : \langle \pi \rangle) = (p-1)!$.

5.4, Aufg. 1. Es sei H zunächst ein Normalteiler in G. Mit der Gleichung $g[a,b]g^{-1} = [gag^{-1}, gbg^{-1}]$, vgl. den Beweis zu 5.4/1, folgt dann, dass $[G,H]$ ein Normalteiler in G ist. Wir behaupten, dass $[G,H]$ der kleinste aller Normalteiler $N \subset G$ ist, so dass das Bild von H in G/N im Zentrum von G/N liegt. In der Tat, das Bild von H in $G/[G,H]$ ist elementweise mit allen Restklassen von Elementen $g \in G$ vertauschbar, also liegt das Bild von H im Zentrum von $G/[G,H]$. Ist umgekehrt $N \subset G$ ein Normalteiler mit dieser Eigenschaft, so gehören alle Kommutatoren $[a,b]$ mit $a \in G$ und $b \in H$ zu N, so dass $[G,H] \subset N$ gilt. Unsere Behauptung ist also verifiziert. Ist nun H lediglich eine Untergruppe, so liefert obiger Schluss noch folgende Aussage: Ist $N \subset G$ ein Normalteiler mit der Eigenschaft, dass das Bild von H im Zentrum von G/N liegt, so gilt $[G,H] \subset N$.

6.1, Aufg. 1. Ist $f(x) = 0$ auflösbar über K, so kann man im Allgemeinen nichts über die Auflösbarkeit dieser Gleichung über K_0 sagen. Beispielsweise gibt es algebraische Gleichungen $f(x) = 0$ über $\mathbb{Q}$, die nicht auflösbar sind, wie wir am Ende von Abschnitt 6.1 gesehen haben. Im Gegensatz hierzu ist eine solche Gleichung über einem Zerfällungskörper von f oder über einem algebraischen Abschluss von $\mathbb{Q}$ auflösbar. Umgekehrt impliziert aber die Auflösbarkeit der Gleichung $f(x) = 0$ über K_0 die Auflösbarkeit über K. Ist nämlich L ein Zerfällungskörper von f über K sowie $L_0 \subset L$ ein Zerfällungskörper von f über K_0, so hat man aufgrund von 3.5/4 eine kanonische Einschränkungsabbildung $\mathrm{Gal}(L/K) \longrightarrow \mathrm{Gal}(L_0/K_0)$, und diese ist injektiv, da die Erweiterungen L/K und L_0/K_0 jeweils von den Nullstellen von f erzeugt werden. Mit $\mathrm{Gal}(L_0/K_0)$ ist daher nach 5.4/8 auch $\mathrm{Gal}(L/K)$ auflösbar.

6.1, Aufg. 2. Die Gleichung $f(x) = 0$ werde zunächst als metazyklisch vorausgesetzt. Dann existiert zu dem Zerfällungskörper L von f über K eine Körperkette $K = K_0 \subset K_1 \subset \ldots \subset K_n$ mit $L \subset K_n$, so dass K_{i+1}/K_i jeweils eine (endliche) zyklische und daher auflösbare Galois-Erweiterung ist. Mit 6.1/5 folgt hieraus, dass auch die Erweiterungen K_n/K und L/K auflösbar sind.

Sei umgekehrt die Gleichung $f(x) = 0$ als auflösbar angenommen. Dann ist die Galois-Gruppe $\mathrm{Gal}(L/K)$ auflösbar, und es gibt zu $\mathrm{Gal}(L/K)$ nach 5.4/7 eine Normalreihe mit zyklischen Faktoren. Anwenden des Hauptsatzes der Galois-Theorie 4.1/6 in Verbindung mit dem Satz vom primitiven Element 3.6/12 zeigt daher, dass die Gleichung $f(x) = 0$ metazyklisch ist.

Also ist "metazyklisch" äquivalent zu "auflösbar". Die weitere Äquivalenz zu "durch Radikale auflösbar" folgt mit 6.1/6.

6.2, Aufg. 1. Gemäß der Theorie in Abschnitt 6.2 betrachten wir die Körperkette

$$K \subset K\big(\sqrt{\Delta}\big) \subset L' \subset L,$$

wobei L' ein Zerfällungskörper zu g und L ein Zerfällungskörper zu f über K sei; Δ sei die gemeinsame Diskriminante von f bzw. g. Die Galois-Gruppe $G = \mathrm{Gal}(L/K)$ operiert auf den Nullstellen $x_1, \ldots, x_4 \in L$ von f und kann hierdurch als Untergruppe von $\mathfrak{S}_4$ aufgefasst werden. Wir wissen bereits, dass Δ genau dann eine Quadratwurzel in K besitzt, wenn G nur gerade Permutationen auf den x_i induziert, wenn also $G \subset \mathfrak{A}_4$ gilt. Folglich ist der Grad von $K(\sqrt{\Delta})$ über K gleich 1 oder 2, je nachdem ob $G \subset \mathfrak{A}_4$ oder $G \not\subset \mathfrak{A}_4$ gilt.

Die komplexe Konjugation $\mathbb{C} \longrightarrow \mathbb{C}$, $z \longmapsto \overline{z}$, beschränkt sich auf L zu einem nicht-trivialen Element in G, und man sieht, dass die Nullstellen von f sich in zwei Paare komplex konjugierter Größen aufteilen, etwa mit $x_2 = \overline{x}_1$ und $x_4 = \overline{x}_3$. Für die Nullstellen

$$z_1 = (x_1 + x_2)(x_3 + x_4),\ z_2 = (x_1 + x_3)(x_2 + x_4),\ z_3 = (x_1 + x_4)(x_2 + x_3)$$

von g schließt man daher $z_1 \in \mathbb{R}$ sowie $z_2, z_3 \geq 0$, wobei allerdings aufgrund der Irreduzibilität von g keines der Elemente z_i verschwinden darf. Insbesondere folgt $L' \subset \mathbb{R}$. Die Irreduzibilität von g impliziert weiter, dass der Grad von L/K von 3 geteilt wird, der Grad von $L'/K(\sqrt{\Delta})$ also in jedem Falle 3 sein muss.

Wir behaupten nun, dass die Galois-Gruppe $H = \mathrm{Gal}(L/K(\sqrt{\Delta}))$ mit $\mathfrak{A}_4$ übereinstimmt. Natürlich gilt $H \subset \mathfrak{A}_4$. Weiter bemerken wir, dass die komplexe Konjugation wegen $L' \subset \mathbb{R}$ ein nicht-triviales Element in $\mathrm{Gal}(L/L')$ induziert, so dass der Grad $[L : L']$ von 2 geteilt wird, also mindestens 2 ist. Die Ordnung $\mathrm{ord}\, H = [L : K(\sqrt{\Delta})]$ ist daher mindestens 6, also entweder 6 oder 12, und es genügt, wenn wir den Fall $\mathrm{ord}\, H = 6$ ausschließen können. Nehmen wir einmal $\mathrm{ord}\, H = 6$ an. Es gibt dann in H aufgrund der Sylowschen Sätze, vgl. 5.2/6, genau eine 3-Sylow-Gruppe. Außerdem zeigt die Kette $K(\sqrt{\Delta}) \subset L' \subset L$, wobei notwendig $[L : L'] = 2$ gelten muss, dass es in H einen Normalteiler der Ordnung 2 gibt. Letzterer ist eine 2-Sylow-Gruppe in H und als Normalteiler auch die einzige 2-Sylow-Gruppe, die H enthalten kann. Dann zeigt aber der Beweis von 5.2/12, dass H zyklisch

von der Ordnung 6 ist, im Gegensatz dazu, dass es in $\mathfrak{S}_4$ nur Elemente der Ordnung 1, 2, 3 oder 4 gibt. Wir sehen damit, dass ord $H = 12$ gelten muss, und wir erhalten $\mathrm{Gal}(L/K(\sqrt{\Delta})) = \mathfrak{A}_4$ wie behauptet.

Zusammenfassend ergibt sich $\mathrm{Gal}(L/K) = \mathfrak{A}_4$, falls Δ ein Quadrat in K ist, und ansonsten $\mathrm{Gal}(L/K) \supsetneq \mathfrak{A}_4$, also $\mathrm{Gal}(L/K) = \mathfrak{S}_4$, wenn Δ kein Quadrat in K ist. Wir geben noch ein Beispiel an, welches die behandelte Situation illustriert. Man betrachte die algebraische Gleichung $f(x) = 0$ mit

$$f = X^4 + X^2 + X + 1 \in \mathbb{Q}[X].$$

Offenbar hat f keine reellen Nullstellen und ist auch irreduzibel. Die kubische Resolvente wird gegeben durch

$$g = X^3 - 2X^2 - 3X + 1 \in \mathbb{Q}[X]$$

und ist ebenfalls irreduzibel. Weiter berechnet sich die Diskriminante von f bzw. g zu

$$\Delta = 144 - 128 - 4 + 16 - 27 + 256 = 257.$$

Da 257 kein Quadrat in $\mathbb{Q}$ ist, erkennen wir $\mathfrak{S}_4$ als Galois-Gruppe der Gleichung $f(x) = 0$.

6.3, Aufg. 1. Die im Beweis zu 6.3/1 benutzten Eigenschaften der reellen Zahlen sind mit rein algebraischen Methoden, wie wir sie in diesem Buch entwickeln, nicht zu verifizieren. Dies ist nicht verwunderlich, denn wir haben bis jetzt die reellen Zahlen als "bekannt" angesehen und insbesondere auf eine präzise Charakterisierung verzichtet. Ohnehin ist das Studium der reellen Zahlen sowie der reellwertigen Funktionen eher dem Bereich der Analysis als dem der Algebra zuzuordnen. Wir begründen deshalb die geforderten Eigenschaften mit Mitteln der Infinitesimalrechnung. Sei also $f = X^n + a_1 X^{n-1} + \ldots + a_n$ ein Polynom ungeraden Grades in $\mathbb{R}[X]$. Indem wir für $x \in \mathbb{R}$, $x \neq 0$, die Zerlegung

$$f(x) = x^n(1 + a_1 x^{-1} + \ldots + a_n x^{-n})$$

benutzen, können wir

$$\lim_{x\to\infty} f(x) = \infty, \qquad \lim_{x\to-\infty} f(x) = -\infty$$

schließen. Folglich besitzt $f(x)$ als stetige reellwertige Funktion aufgrund des Zwischenwertsatzes eine Nullstelle in $\mathbb{R}$. Aus einem ähnlichen Grund gibt es zu jedem $a \in \mathbb{R}$, $a \geq 0$, eine Quadratwurzel in $\mathbb{R}$. Man betrachte nämlich die Funktion $g(x) = x^2 - a$. Auch sie besitzt aufgrund des Zwischenwertsatzes wegen $g(0) \leq 0$ sowie $\lim_{x\to\infty} g(x) = \infty$ eine Nullstelle in $\mathbb{R}$.

6.4, Aufg. 1. Man setze $K = \mathbb{Q}(M \cup \overline{M})$. Aus 6.4/1 folgt unter Benutzung des Gradsatzes 3.2/2, dass für jedes $z \in \mathfrak{K}(M)$ der Grad $[K(z) : K]$ eine Potenz von 2 ist. Sei nun umgekehrt $z \in \mathbb{C}$ ein Element mit dieser Eigenschaft. Ist dann die Erweiterung $K(z)/K$ galoissch, so ergibt sich $z \in \mathfrak{K}(M)$ mit 6.4/1. Allgemein gilt allerdings $z \in \mathfrak{K}(M)$ nur dann, wenn z in einem galoisschen Erweiterungskörper von K enthalten ist, dessen Grad über K eine Potenz von 2 ist. Bezeichnet L den von allen Konjugierten zu z über K erzeugten Körper, also den Zerfällungskörper des Minimalpolynoms von z über K, so ist vorstehende Eigenschaft äquivalent zu der Bedingung, dass der Grad $[L : K]$ eine Potenz von 2 ist. Nun gibt es aber durchaus Fälle, wo $[K(z) : K]$ eine Potenz von 2 ist, nicht aber $[L : K]$. Beispielsweise gibt es irreduzible algebraische Gleichungen vom Grad 4 mit Galois-Gruppe $\mathfrak{S}_4$, wie wir sogleich sehen werden. Man kann daher aus der Tatsache, dass $[K(z) : K]$ eine Potenz von 2 ist, im Allgemeinen nicht auf $z \in \mathfrak{K}(M)$ schließen.

Um solche Beispiele explizit anzugeben, setze man $M = \{0, 1\}$ und betrachte ein Polynom des Typs $f = X^4 - pX - 1 \in \mathbb{Q}[X]$ mit einer Primzahl p. Es ist f irreduzibel. Um dies einzusehen, genügt es zu zeigen, dass f als Polynom in $\mathbb{Z}[X]$ irreduzibel ist, vgl. 2.7/7. Letzteres verifiziert man in direkter Weise, indem man nachrechnet, dass eine Zerlegung von f über $\mathbb{Z}$ in ein lineares und ein kubisches bzw. zwei quadratische Polynome unmöglich ist. Seien nun $\alpha_1, \ldots, \alpha_4$ die Nullstellen von f in $\mathbb{C}$ und sei $L = \mathbb{Q}(\alpha_1, \ldots, \alpha_4)$ der Zerfällungskörper von f in $\mathbb{C}$. Die explizite Auflösung von Gleichungen 4-ten Grades in Abschnitt 6.1 zeigt dann, dass die Größen

$$\beta_1 = (\alpha_1 + \alpha_2)(\alpha_3 + \alpha_4),\ \beta_2 = (\alpha_1 + \alpha_3)(\alpha_2 + \alpha_4),\ \beta_3 = (\alpha_1 + \alpha_4)(\alpha_2 + \alpha_3)$$

die Nullstellen der kubischen Resolvente von f sind, nämlich des Polynoms $g = X^3 + 4X + p^2$. Ähnlich wie bei f stellt man fest, dass auch dieses Polynom irreduzibel über $\mathbb{Q}$ ist. Als Konsequenz sehen wir, dass L Elemente vom Grad 3 über $\mathbb{Q}$ enthält und dass folglich der Grad $[L : \mathbb{Q}]$ keine Potenz von 2 sein kann. Es gilt daher $\alpha_1, \ldots, \alpha_4 \notin \mathfrak{K}(\{0, 1\})$, obwohl jedes α_i vom Grad 4 über

$\mathbb{Q}$ ist. Man kann übrigens leicht einsehen, dass die Galois-Gruppe $\mathrm{Gal}(L/\mathbb{Q})$ die volle Gruppe $\mathfrak{S}_4$ ergibt, wenn wir die Elemente $\sigma \in \mathrm{Gal}(L/\mathbb{Q})$ als Permutationen der Wurzeln $\alpha_1, \ldots, \alpha_4$ interpretieren. Als Untergruppe von $\mathfrak{S}_4$ besitzt $\mathrm{Gal}(L/\mathbb{Q})$ eine Ordnung, die ein Teiler von 24 ist. Da aber L sowohl Elemente vom Grad 3 als auch vom Grad 4 enthält, ist die Ordnung mindestens 12. Somit hat man entweder $\mathrm{Gal}(L/\mathbb{Q}) = \mathfrak{S}_4$, oder aber es ist $\mathrm{Gal}(L/\mathbb{Q})$ eine Untergruppe vom Index 2 und damit ein Normalteiler in $\mathfrak{S}_4$. Im letzteren Fall folgt $\mathrm{Gal}(L/\mathbb{Q}) = \mathfrak{A}_4$, da jeder Normalteiler vom Index 2 zu einer abelschen Faktorgruppe führt und da $[\mathfrak{S}_4, \mathfrak{S}_4] = \mathfrak{A}_4$ gilt; vgl. 5.4/1 und 5.4/2. Nun besitzt aber die Diskriminante

$$\Delta_g = (\beta_1 - \beta_2)^2(\beta_1 - \beta_3)^2(\beta_2 - \beta_3)^2 = -4 \cdot 4^3 - 27p^4$$

des Polynoms g keine Quadratwurzel in $\mathbb{Q}$; zu der Formel für Δ_g konsultiere man Beispiel (2) in 4.3 oder den Schluss von 4.4. Folglich kann $\mathrm{Gal}(L/\mathbb{Q})$ nicht ausschließlich gerade Permutationen der $\beta_1, \beta_2, \beta_3$ induzieren, und man sieht unter Benutzung der Definition der β_i, dass $\mathrm{Gal}(L/\mathbb{Q})$ dann auch nicht nur aus geraden Permutationen der $\alpha_1, \alpha_2, \alpha_3, \alpha_4$ bestehen kann. Somit folgt $\mathrm{Gal}(L/\mathbb{Q}) = \mathfrak{S}_4$, wie behauptet.

6.4, Aufg. 2. Es ist $\zeta_3 = e^{2\pi i/3}$ eine primitive dritte Einheitswurzel in $\mathbb{C}$. Wie wir wissen, man vergleiche etwa 6.4/3, gilt $\zeta_3 \in \mathfrak{K}(\{0, 1\})$. Wäre nun die Winkeldreiteilung generell mit Zirkel und Lineal durchführbar, so müsste sich auch die primitive 9-te Einheitswurzel $\zeta_9 = e^{2\pi i/9}$ mit Zirkel und Lineal konstruieren lassen. Dies ist aber wegen $\varphi(9) = 6$ nach 6.4/3 unmöglich. Die Winkeldreiteilung ist daher im Allgemeinen nicht mit Zirkel und Lineal durchführbar. Dies ist auch nicht verwunderlich, denn das Problem der Dreiteilung eines Winkels φ korrespondiert zur Lösung der Gleichung $z^3 - e^{i\varphi} = 0$ bzw., wenn wir nur den Realteil dieser Gleichung betrachten und $z\overline{z} = 1$ benutzen, zur Lösung von $4x^3 - 3x - \cos\varphi = 0$. Es ist also eine Gleichung dritten Grades zu lösen, und dies ist im Allgemeinen nicht mit Zirkel und Lineal möglich.

7.1, Aufg. 1. Es sei L/K eine Körpererweiterung und $\mathfrak{X} = (x_i)_{i \in I}$ eine Transzendenzbasis. Das System $\mathfrak{X}$ ist dann insbesondere algebraisch unabhängig über K, d. h. man kann $\mathfrak{X}$ als ein System von Variablen sowie den Unterring $K[\mathfrak{X}] \subset L$ als Polynomring in den Variablen x_i auffassen. Hieraus folgt natürlich, dass das System $\mathfrak{X}$ linear unabhängig über K ist, wenn wir L als K-Vektorraum interpretieren. Aber man kann auch sehen, dass $\mathfrak{X}$ niemals $K[\mathfrak{X}]$ oder gar L als K-Vektorraum erzeugen kann. Deshalb kann eine

Transzendenzbasis von L/K niemals gleichzeitig eine K-Vektorraumbasis von L sein.

Trotzdem besteht eine große begriffliche Analogie zwischen Basen von Vektorräumen und Transzendenzbasen von Körpererweiterungen. Unter dieser Analogie korrespondiert "lineare Unabhängigkeit" eines Systems $\mathfrak{X}$ von Elementen eines K-Vektorraums V zu "algebraischer Unabhängigkeit" eines Systems $\mathfrak{X}$ von Elementen einer Körpererweiterung L/K. Eine Basis von V ist ein linear unabhängiges System $\mathfrak{X} \subset V$, welches V als K-Vektorraum erzeugt. Entsprechend ist eine Transzendenzbasis von L/K ein algebraisch unabhängiges System $\mathfrak{X} \subset L$, welches die Erweiterung L/K in dem Sinne "erzeugt", dass $L/K(\mathfrak{X})$ algebraisch ist. Genau wie bei Vektorräumen lassen sich Transzendenzbasen als maximale algebraisch unabhängige Systeme (vgl. 7.1/3) bzw. als minimale "Erzeugendensysteme" im vorstehenden Sinne charakterisieren. Auch der Beweis zu 7.1/5, nämlich dass je zwei Transzendenzbasen von L/K gleiche Mächtigkeit besitzen, ist im Vektorraumfall in gleicher Weise gültig.

Aber auch hier sind der Analogie Grenzen gesetzt. So dehnt sich jede Bijektion $\mathfrak{X} \longrightarrow \mathfrak{Y}$ zwischen zwei Basen von V auf genau eine Weise zu einem K-Automorphismus von V aus. Die entsprechende Aussage für Transzendenzbasen von L/K ist falsch, sowohl im Hinblick auf die Existenzaussage wie auch auf die Eindeutigkeitsaussage. Beispielsweise bilden für eine einfache transzendente Erweiterung $L = K(X)$ die Elemente X und X^2 jeweils eine Transzendenzbasis von L/K, und es gibt auch einen K-Isomorphismus $K(X) \longrightarrow K(X^2)$, der X auf X^2 abbildet. Aber dieser Isomorphismus setzt sich nicht zu einem K-Automorphismus von $K(X)$ fort, da X in $K(X)$ keine Quadratwurzel besitzt. Ist andererseits L ein algebraischer Abschluss von $K(X)$, so setzt sich die Identität auf $K(X)$ zwar zu einem K-Automorphismus von L fort. Dieser ist jedoch nicht eindeutig bestimmt, da es nicht-triviale $K(X)$-Automorphismen von L gibt.

7.1, Aufg. 2. Wir wollen zunächst zeigen, dass $\mathbb{C}$ Automorphismen besitzt, die $\mathbb{R}$ nicht festlassen. Hierzu wähle man ein Element $x \in \mathbb{R}$, etwa $x = \pi$, welches transzendent über $\mathbb{Q}$ ist. Nach 7.1/4 besitzt die Erweiterung $\mathbb{C}/\mathbb{Q}$ eine Transzendenzbasis $\mathfrak{X}$ mit $x \in \mathfrak{X}$. Da auch das Element $ix \in \mathbb{C}$ transzendent über $\mathbb{Q}$ ist, gibt es weiter eine Transzendenzbasis $\mathfrak{Y}$ von $\mathbb{C}/\mathbb{Q}$ mit $ix \in \mathfrak{Y}$. Nach 7.1/5 besitzen $\mathfrak{X}$ und $\mathfrak{Y}$ gleiche Mächtigkeit. Es existiert also eine Bijektion $\mathfrak{X} \longrightarrow \mathfrak{Y}$, wobei wir $x \longmapsto ix$ annehmen dürfen. Diese Bijektion setzt sich fort zu einem $\mathbb{Q}$-Isomorphismus $\mathbb{Q}(\mathfrak{X}) \xrightarrow{\sim} \mathbb{Q}(\mathfrak{Y})$. Da $\mathbb{C}$

ein algebraisch abgeschlossener Körper ist, der algebraisch über $\mathbb{Q}(\mathfrak{X})$ und $\mathbb{Q}(\mathfrak{Y})$ ist, kann man $\mathbb{C}$ als algebraischen Abschluss sowohl von $\mathbb{Q}(\mathfrak{X})$ wie auch von $\mathbb{Q}(\mathfrak{Y})$ auffassen. Folglich sind

$$\sigma\colon \mathbb{Q}(\mathfrak{X}) \hookrightarrow \mathbb{C}, \qquad \tau\colon \mathbb{Q}(\mathfrak{X}) \xrightarrow{\sim} \mathbb{Q}(\mathfrak{Y}) \hookrightarrow \mathbb{C}$$

zwei algebraische Abschlüsse von $\mathbb{Q}(\mathfrak{X})$. Aufgrund von 3.4/10 existiert dann ein Automorphismus $\varphi\colon \mathbb{C} \longrightarrow \mathbb{C}$ mit $\tau = \varphi \circ \sigma$. Da nach Konstruktion $\varphi(x) = ix$ gilt, ist φ ein Automorphismus von $\mathbb{C}$, der $\mathbb{R}$ wie gewünscht nicht festlässt. Es ist daher $\varphi(\mathbb{R})$ ein zu $\mathbb{R}$ isomorpher, aber von $\mathbb{R}$ verschiedener Teilkörper von $\mathbb{C}$.

Um zu sehen, dass $\mathbb{C}$ zu sich selbst isomorphe echte Teilkörper enthält, verfahren wir ähnlich. Wir wählen eine Transzendenzbasis $\mathfrak{X}$ von $\mathbb{C}/\mathbb{Q}$ und benutzen, dass $\mathfrak{X}$ aus unendlich vielen Elementen besteht; vgl. hierzu Aufgabe 3 aus 7.1. Dann existiert eine injektive Abbildung $\mathfrak{X} \hookrightarrow \mathfrak{X}$, welche nicht surjektiv ist. Man benutze hierzu etwa, wie in 7.1/7 gezeigt, dass $\mathfrak{X}$ eine disjunkte Vereinigung abzählbarer Teilmengen von $\mathfrak{X}$ ist. Die betrachtete Injektion $\mathfrak{X} \longrightarrow \mathfrak{X}$ setzt sich zu einer Injektion $\iota\colon \mathbb{Q}(\mathfrak{X}) \hookrightarrow \mathbb{Q}(\mathfrak{X})$ fort, wobei $\mathbb{Q}(\mathfrak{X})$ nicht algebraisch über dem Bild von ι ist. Wiederum kann man die beiden Homomorphismen

$$\sigma\colon \mathbb{Q}(\mathfrak{X}) \hookrightarrow \mathbb{C}, \qquad \tau\colon \mathbb{Q}(\mathfrak{X}) \overset{\iota}{\hookrightarrow} \mathbb{Q}(\mathfrak{X}) \hookrightarrow \mathbb{C}$$

betrachten. Es ist $\mathbb{C}$ ein algebraischer Abschluss von $\mathbb{Q}(\mathfrak{X})$ bezüglich der Injektion σ, nicht aber bezüglich τ. Indem wir 3.4/9 benutzen, erhalten wir einen $\mathbb{Q}(\mathfrak{X})$-Homomorphismus $\varphi\colon \mathbb{C} \hookrightarrow \mathbb{C}$ mit $\tau = \varphi \circ \sigma$. Da $\mathbb{C}$ nicht algebraisch über dem Bild von τ ist, kann φ nicht surjektiv sein. Folglich ist $\varphi(\mathbb{C})$ ein echter Teilkörper von $\mathbb{C}$, der zu $\mathbb{C}$ isomorph ist.

7.2, Aufg. 1. Sei $\Phi\colon M \longrightarrow E$ eine R-lineare Abbildung in einen R'-Modul E. Es ist lediglich zu zeigen, dass es zu Φ eine eindeutig bestimmte R'-lineare Abbildung $\varphi\colon M \otimes_R R' \longrightarrow E$ gibt mit $x \otimes 1 \longmapsto \Phi(x)$ für $x \in M$. Um die Existenz von φ einzusehen, betrachte man die R-bilineare Abbildung $M \times R' \longrightarrow E$, $(x, a) \longmapsto a\Phi(x)$. Diese induziert gemäß der universellen Eigenschaft des Tensorprodukts eine R-lineare Abbildung $\varphi\colon M \otimes_R R' \longrightarrow E$, welche eindeutig durch $\varphi(x \otimes a) = a\Phi(x)$ für $a \in R'$ und $x \in M$ charakterisiert ist. Anhand dieser Eigenschaft sieht man sofort, dass φ als Abbildung zwischen R'-Moduln sogar R'-linear ist. Ist umgekehrt $\psi\colon M \otimes_R R' \longrightarrow E$ eine R'-lineare Abbildung mit $\psi(x \otimes 1) = \Phi(x)$ für

$x \in M$, so stimmt ψ auf allen Tensoren der Form $x \otimes 1$ mit φ überein. Da diese Tensoren aber $M \otimes_R R'$ als R'-Modul erzeugen, folgt $\varphi = \psi$.

7.2, Aufg. 2. Wir behandeln zunächst den Fall freier Polynomringe, also etwa $R' = R[\mathfrak{X}]$ und $R'' = R[\mathfrak{Y}]$ mit Systemen $\mathfrak{X}, \mathfrak{Y}$ von Variablen. Es folgt, dass der Polynomring $R[\mathfrak{X}, \mathfrak{Y}]$ mit den kanonischen Injektionen $\sigma' \colon R[\mathfrak{X}] \longrightarrow R[\mathfrak{X}, \mathfrak{Y}]$ und $\sigma'' \colon R[\mathfrak{Y}] \longrightarrow R[\mathfrak{X}, \mathfrak{Y}]$ die universelle Eigenschaft aus 7.2/9 erfüllt. Ein R-Algebrahomomorphismus $R[\mathfrak{X}, \mathfrak{Y}] \longrightarrow A$ ist nämlich eindeutig durch die Vorgabe der Bilder zu $\mathfrak{X}$ und $\mathfrak{Y}$ bestimmt. Im Allgemeinfall lassen sich R' und R'' als Restklassenringe freier Polynomringe darstellen, etwa $R' = R[\mathfrak{X}]/\mathfrak{a}$ und $R'' = R[\mathfrak{Y}]/\mathfrak{b}$. Wir behaupten, dass $R[\mathfrak{X}, \mathfrak{Y}]/(\mathfrak{a}, \mathfrak{b})$ zusammen mit den kanonischen Abbildungen $\sigma' \colon R[\mathfrak{X}]/\mathfrak{a} \longrightarrow R[\mathfrak{X}, \mathfrak{Y}]/(\mathfrak{a}, \mathfrak{b})$ und $\sigma'' \colon R[\mathfrak{Y}]/\mathfrak{b} \longrightarrow R[\mathfrak{X}, \mathfrak{Y}]/(\mathfrak{a}, \mathfrak{b})$ die universelle Eigenschaft aus 7.2/9 erfüllt. Sind nämlich $\varphi' \colon R[\mathfrak{X}] \longrightarrow A$, $\varphi'' \colon R[\mathfrak{Y}] \longrightarrow A$ zwei R-Algebrahomomorphismen mit $\mathfrak{a} \subset \ker \varphi'$ und $\mathfrak{b} \subset \ker \varphi''$, so gilt für den resultierenden R-Algebrahomomorphismus $\varphi \colon R[\mathfrak{X}, \mathfrak{Y}] \longrightarrow A$ die Relation $(\mathfrak{a}, \mathfrak{b}) \subset \ker \varphi$.

7.3, Aufg. 1. Die Frage ist in allen Fällen negativ zu beantworten. Als Beispiel einer regulären Körpererweiterung betrachte man eine rein transzendente Erweiterung $K(X)/K$ mit einer Variablen X. Im Falle $\operatorname{char} K = 2$ ist die Erweiterung $K(X)/K(X^2)$ rein inseparabel und damit nicht separabel. Im Falle $\operatorname{char} K \neq 2$ dagegen ist diese Erweiterung separabel algebraisch und folglich nicht primär.

7.3, Aufg. 2. Auch diese Frage ist negativ zu beantworten. Um ein Beispiel zu konstruieren, wähle man einen Körper k der Charakteristik $p > 0$ und betrachte zu Variablen X, Y, Z die rein transzendente Erweiterung $k(X, Y, Z)$ sowie die folgenden Teilkörper:

$$K = k(X^p, Y^p), \qquad L = k(X^p, Y^p, Z)(t) \qquad \text{mit} \qquad t = X + YZ.$$

Wir wollen zeigen, dass die Erweiterung L/K nicht separabel ist, obwohl K algebraisch abgeschlossen in L ist. Zunächst beachte man, dass sich die Erweiterung L/K in die rein transzendente Erweiterung $K(Z)/K$ und die rein inseparable Erweiterung $L/K(Z)$ vom Grad p zerlegt; es ist $t^p - (X^p + Y^p Z^p) = 0$ die irreduzible Gleichung von t über $K(Z)$. Um zu sehen, dass L/K nicht separabel ist, betrachte man die Elemente $t^p, 1^p, Z^p$. Wie aus vorstehender Gleichung folgt, sind diese linear abhängig über K. Wäre nun die Erweiterung L/K separabel, so müssten nach 7.3/7 (iv) auch

die Elemente $t, 1, Z$ linear abhängig über K sein, und dies würde $t \in K(Z)$ nach sich ziehen, was aber nicht der Fall ist. Folglich ist L/K nicht separabel.

Somit bleibt noch zu zeigen, dass K in L algebraisch abgeschlossen ist. Sei etwa $a \in L$ algebraisch über K. Dann gilt $a^p \in K(Z)$. Da aber jedes Element aus $K(Z)-K$ transzendent über K ist (vgl. 7.1/10), muss bereits $a^p \in K$ gelten, und es folgt $a \in k(X,Y)$. Angenommen, a ist kein Element von K. Dann gilt $a \notin K(Z)$ und wegen $[L : K(Z)] = p$ bereits $K(Z)(a) = L$. Nun kann man aber den Körper $K(Z)(a)$ auch in der Form $K(a)(Z)$ konstruieren, indem man zunächst das algebraische Element a zu K adjungiert, sowie anschließend das transzendente Element Z. Insbesondere lässt sich daher das Element $t = X + YZ \in L = K(a)(Z)$ als Quotient zweier Polynome aus $K(a)[Z] \subset k(X,Y)[Z]$ schreiben, etwa $X + YZ = f(Z)g(Z)^{-1}$. Indem wir auf der rechten Seite durch Potenzen von Z kürzen, können wir $g(0) \neq 0$ annehmen. Es folgt $X = f(0)g(0)^{-1} \in K(a)$. Dann gehört aber mit t auch YZ zu $K(a)(Z)$ und somit Y zu $K(a)$. Hieraus ergibt sich $K(a) = k(X,Y)$, was aber nicht sein kann, da a lediglich den Grad p über $K = k(X^p, Y^p)$ hat. Daher ist K wie behauptet algebraisch abgeschlossen in L.

7.3, Aufg. 3. Es sei K ein vollkommener Körper der Charakteristik $p > 0$, etwa $K = \mathbb{F}_p$, sowie X eine Variable. Man betrachte zu $K(X)$ den rein inseparablen Abschluss $L = K(X)^{p^{-\infty}}$. Dann ist L/K vom Transzendenzgrad 1, und wir behaupten, dass diese Erweiterung separabel, aber nicht separabel erzeugt ist. Um dies einzusehen, beachte man, dass L durch die aufsteigende Folge der Körper $K(X)^{p^{-i}} = K(X^{p^{-i}})$, $i \in \mathbb{N}$, ausgeschöpft wird. Da $K(X^{p^{-i}})$ jeweils rein transzendent über K mit $X^{p^{-i}}$ als Transzendenzbasis ist, ergibt sich mit 7.2/13 und 7.3/3 die Separabilität von L/K.

Wir gehen nun indirekt vor und nehmen an, dass L/K separabel erzeugt ist. Dann existiert ein über K transzendentes Element $x \in L$, so dass L separabel algebraisch über $K(x)$ ist. Da x aber in einem der Körper $K(X^{p^{-i}})$ enthalten sein muss, hat man eine Kette $K(x) \subset K(X^{p^{-i}}) \subset L$. Wenn nun $L/K(x)$ separabel algebraisch ist, so gilt dasselbe nach 3.6/11 auch für $L/K(X^{p^{-i}})$. Damit ergibt sich aber ein Widerspruch, denn es ist $X^{p^{-i-1}}$ offenbar rein inseparabel vom Grad p über $K(X^{p^{-i}})$. Somit ist die Erweiterung L/K nicht separabel erzeugt.

7.4, Aufg. 1. Die Charakterisierung separabel algebraischer Erweiterungen L/K durch die Bedingung $\Omega^1_{L/K} = 0$ ist nur gültig für endlich erzeugte Körpererweiterungen. Ist beispielsweise K ein nicht vollkommener Körper der Charakteristik $p > 0$ und $L = K^{p^{-\infty}}$ seine vollkommene Hülle (oder

ein algebraischer Abschluss), so ist die Erweiterung L/K nicht separabel. Da andererseits jedes Element von L eine p-te Wurzel in L besitzt, ist jede Derivation auf L trivial. Dies bedeutet aber insbesondere $\Omega^1_{L/K} = 0$.

Literatur

1. Artin, E.: Foundations of Galois Theory. New York University Lecture Notes. New York University, New York 1938
2. Artin, E.: Galois Theory. Notre Dame Mathematical Lectures, Number 2. University of Notre Dame Press, Notre Dame 1942 (deutsche Übersetzung der 2. Auflage: Galoissche Theorie. Harri Deutsch, Zürich 1965)
3. Bosch, S.: Algebraic Geometry and Commutative Algebra. Universitext, Springer, London 2013, 2022
4. Bosch, S.: Lineare Algebra. Springer, Berlin–Heidelberg–New York 2001, 2003, 2006, 2008, 2014, 2021
5. Bourbaki, N.: Eléments de Mathématique, Algèbre, Chap. 1-10. Hermann, Paris 1947 . . .
6. Grothendieck, A.: Technique de descente et théorèmes d'existence en géométrie algébrique: I. Généralités. Descente par morphismes fidèlement plats. Séminaire Bourbaki 12, no. 190, 1959/60
7. Hasse, H.: Vorlesungen über Zahlentheorie, Grundlehren der mathematischen Wissenschaften, Bd. 59. Springer, Berlin–Göttingen–Heidelberg–New York 1964
8. Hermite, Ch.: Sur la fonction exponentielle. C. R. Acad. Sci. Paris 77 (1873)
9. Hilbert, D.: Die Theorie der algebraischen Zahlkörper. Jahresbericht der Deutschen Mathematikervereinigung, Bd. 4, 175-546 (1897)
10. Kiernan, B. M.: The Development of Galois Theory from Lagrange to Artin. Archive for History of Exact Sciences, Vol. 8, 40-154 (1971/72)
11. Lang, S.: Algebra. Addison Wesley 1965, 1984, 1993 (Rev. 3rd ed. 2002, Graduate Texts in Mathematics, Springer)
12. Lindemann, F.: Über die Zahl π. Math. Ann. 20, 213-225 (1882)
13. Noether, E.: Idealtheorie in Ringbereichen. Math. Ann. 83, 24-66 (1921)

S. Bosch, *Algebra*, https://doi.org/10.1007/978-3-662-67464-2

14. Serre, J.-P.: Corps locaux. Hermann, Paris 1968
15. Steinitz, E.: Algebraische Theorie der Körper. Crelles Journal 137, 167–309 (1910)
16. van der Waerden, B. L.: Moderne Algebra. Springer, Berlin 1930/31; weitere Auflagen 1936, 1950, 1955, 1960, 1964, 1966 (ab 1955 unter dem Titel "Algebra")
17. Weber, H.: Lehrbuch der Algebra, 2 Bde. Vieweg, Braunschweig 1895/96
18. Wielandt, H.: Ein Beweis für die Existenz der Sylowgruppen. Archiv der Mathematik 10, 401–402 (1959)
19. Witt, E.: Zyklische Körper und Algebren der Charakteristik p vom Grad p^n. Struktur diskret bewerteter perfekter Körper mit vollkommenem Restklassenkörper der Charakteristik p, Crelles Journal 176, 126 –140 (1937)

Symbolverzeichnis

$\mathbb{N}$	natürliche Zahlen, einschließlich 0
$\mathbb{Z}$	ganze Zahlen
$\mathbb{Q}, \mathbb{Q}_{>0}$	rationale bzw. positive rationale Zahlen
$\mathbb{R}, \mathbb{R}_{>0}$	reelle bzw. positive reelle Zahlen
$\mathbb{C}$	komplexe Zahlen
$G^X, G^{(X)}$	G-wertige Funktionen auf X 15
τ_a	Linkstranslation mit a 17
aH, Ha	Nebenklassen einer Untergruppe H 20
$G/H, H\backslash G$	Menge der Nebenklassen modulo H 21
$(G : H)$	Index einer Untergruppe H 21
$\operatorname{ord} G$	Ordnung einer Gruppe 21
G/N	Restklassengruppe nach einem Normalteiler N 22
$\langle x \rangle$	von einem Element erzeugte Untergruppe 26
$\operatorname{ord} a$	Ordnung eines Elementes 28
R^*	Einheitengruppe eines Rings 36
$\mathbb{H}$	Hamiltonsche Quaternionen 36
$R^X, R^{(X)}$	R-wertige Funktionen auf X 37
$R[X]$	Polynomring einer Variablen X 38
$\operatorname{grad} f$	Grad eines Polynoms 40
$R[\![X]\!]$	Ring formaler Potenzreihen 42
$\mathfrak{a} + \mathfrak{b}$	Summe von Idealen 44
$\mathfrak{a} \cdot \mathfrak{b}$	Produkt von Idealen 44
$\mathfrak{a} \cap \mathfrak{b}$	Durchschnitt von Idealen 44
$(a_1, \ldots, a_n)$	von $a_1, \ldots, a_n$ erzeugtes Ideal 45
$R/\mathfrak{a}$	Restklassenring modulo eines Ideals $\mathfrak{a}$ 49

S. Bosch, *Algebra*, https://doi.org/10.1007/978-3-662-67464-2

$\mathbb{F}_p$	Körper mit p Elementen 52
$x \equiv y \bmod \mathfrak{a}$	Kongruenz 55
$x \mid y$	x teilt y 59
$x \nmid y$	x teilt nicht y 59
$\nu_p(a)$	Exponent zum Primfaktor p 64
$\mathrm{ggT}(x_1, \ldots, x_n)$	größter gemeinsamer Teiler von $x_1, \ldots, x_n$ 64
$\mathrm{kgV}(x_1, \ldots, x_n)$	kleinstes gemeinsames Vielfaches von $x_1, \ldots, x_n$ 64
$R[M]$	Polynomring zu einem Monoid M 70
$R[X_1, \ldots, X_n]$	Polynomring in n Variablen 70
$R[\mathfrak{X}]$	Polynomring in einem System $\mathfrak{X}$ von Variablen 70
$\mathrm{grad}\, f$	Totalgrad eines Polynoms 75
$R[x]$	kleinster Unterring, der R und x enthält 77
$D(f), f'$	Ableitung eines Polynoms 81
$Q(R)$	Quotientenkörper eines Integritätsrings 84
$K(X), K(\mathfrak{X})$	rationale Funktionenkörper 84
$S^{-1}R, R_S$	Lokalisierung eines Rings R 84
$\nu_p(x), \nu_p(f)$	Exponenten zum Primfaktor p 85
M/N	Restklassenmodul nach einem Untermodul N 94
$\sum_{i \in I} M_i$	Summe von Moduln 95
$\bigoplus_{i \in I} M_i$	direkte Summe von Moduln 95
$\mathrm{rg}\, M$	Rang eines Moduls 96
$S^{-1}M$	Lokalisierung eines Moduls M 96
$l_A(M)$	Länge eines Moduls 97
M_{sat}	Saturierung eines Untermoduls 98
$\mathrm{cont}(x)$	Inhalt eines Elementes 99
$\bigwedge^t F$	t-faches äußeres Produkt eines freien Moduls 103
$\mathrm{char}\, K$	Charakteristik eines Körpers 116
L/K	Körpererweiterung 119
$[L : K]$	Grad einer Körpererweiterung 119
$K(\mathfrak{A})$	von einem System $\mathfrak{A}$ über K erzeugter Körper 123
$K(\alpha_1, \ldots, \alpha_n)$	von $\alpha_1, \ldots, \alpha_n$ über K erzeugter Körper 123
$\overline{\mathbb{Q}}$	algebraischer Abschluss von $\mathbb{Q}$ 126
$A[x_1, \ldots, x_n]$	von $x_1, \ldots, x_n$ über A erzeugter Ring 129
$\overline{K}$	algebraischer Abschluss eines Körpers 143
f^σ	mit σ transportiertes Polynom 144
$\mathrm{Hom}_K(L, \overline{K})$	Menge der K-Homomorphismen $L \longrightarrow \overline{K}$ 157
$[L : K]_s$	Separabilitätsgrad einer Körpererweiterung 157
$\#H$	Anzahl der Elemente einer Menge 157
$\mathbb{F}_q$	Körper mit $q = p^n$ Elementen 172
$V(E), V(\mathfrak{a})$	algebraische Mengen zu $E, \mathfrak{a}$ 176

$I(U)$	Verschwindungsideal zu U 176
$\operatorname{rad}\mathfrak{a}$	Radikal eines Ideals 178
$\operatorname{Aut}_K(L)$	Gruppe der K-Automorphismen von L 188
$\operatorname{Gal}(L/K)$	Galois-Gruppe zu L/K 188
L^G	Fixkörper zu G 190
$E \cdot E'$	Kompositum von Körpern 194
$\varprojlim_{i\in I} G_i$	projektiver Limes 206
$\varinjlim_{i\in I} G_i$	induktiver Limes 207
$\mathbb{Z}_\ell$	Ring der ganzen ℓ-adischen Zahlen 211
$s_0, \ldots, s_n$	elementarsymmetrische Polynome in n Variablen 221
$\operatorname{lexgrad}(f)$	lexikographischer Grad eines Polynoms 225
$\operatorname{Lt}(f)$	lexikographischer Leitterm eines Polynoms 225
Δ_f	Diskriminante eines Polynoms 236
$\operatorname{res}(f, g)$	Resultante zweier Polynome 237
$\operatorname{N}_{A/R}\big(g(x)\big)$	Norm der Multiplikation mit $g(x)$ 240
$\operatorname{Sp}_{A/R}(a)$	Spur der Multiplikation mit a 244
$D_{A/R}(x_1, \ldots, x_n)$	Diskriminante von $x_1, \ldots, x_n$ 244
U_n	Gruppe der n-ten Einheitswurzeln 248
$\varphi(n)$	Eulersche φ-Funktion 250
Φ_n	n-tes Kreisteilungspolynom 256
$\operatorname{Sp}_{L/K}(a)$	Spur eines Elementes 266
$\operatorname{N}_{L/K}(a)$	Norm eines Elementes 266
$H^1(G, A)$	1. Kohomologiegruppe von G mit Werten in A 274
$W(R)$	Witt-Ring 296
$W_n(X_0, \ldots, X_n)$	Witt-Polynom 296
F	Frobenius-Operator 305
V	Verschiebungsoperator 305
$K' \otimes_K V$	Tensorprodukt 314
$a \otimes v$	Tensor 314
τ_g, τ'_g	Translationen mit g 326
int_g	Konjugation mit g 326
Gx	Bahn zu x 327
G_x	Isotropiegruppe zu x 327
Z_S	Zentralisator von S 329
Z, Z_G	Zentrum von G 329
N_S	Normalisator von S 329
$\mathfrak{S}_n$	Permutationsgruppe 343
$(x_1, \ldots, x_r)$	Zyklus 344
$\operatorname{sgn}\pi$	Signum einer Permutation 344
$\mathfrak{A}_n$	alternierende Gruppe 345

$\mathfrak{B}_4$	Kleinsche Vierergruppe 347
$[a, b]$	Kommutator zweier Elemente 348
$[H, H']$	Kommutator zweier Untergruppen 348
$D^i G$	i-ter iterierter Kommutator 350
$\mathfrak{K}(M)$	mit Zirkel und Lineal konstruierbare Punkte 385
F_ℓ	ℓ-te Fermatsche Zahl 392
$\operatorname{card} M$	Kardinalität einer Menge 399
$\operatorname{transgrad}_K L$	Transzendenzgrad einer Körpererweiterung 401
$M \otimes_R N$	Tensorprodukt von Moduln 406
$x \otimes y$	Tensor 406
M_S	Lokalisierung eines Moduls 412
$\operatorname{rad} R$	Radikal eines Rings 420
$K^{p^{-\infty}} = \bigcup_{i=0}^{\infty} K^{p^{-i}}$	rein inseparabler Abschluss von K 424
$\operatorname{Der}_R(A, M)$	A-Modul von Derivationen 436
$(\Omega^1_{A/R}, d_{A/R})$	Modul von Differentialformen 436

Namen- und Sachverzeichnis

S. Bosch, *Algebra*, https://doi.org/10.1007/978-3-662-67464-2