

ALGEBRA

Vorlesung im Wintersemester 2025/26
an der
Technischen Universität Chemnitz

Andreas Hohl

Inhaltsverzeichnis

Einleitung	1
1 Einführung und Motivation	3
2 Gruppentheorie	9
2.1 Gruppen und ihre grundlegenden Eigenschaften	9
2.2 Die symmetrische Gruppe	16
2.3 Normalteiler und Quotientengruppen	20
2.4 Der Homomorphiesatz	26
2.5 Gruppenwirkungen	27
2.6 Endliche Gruppen	32
2.7 Die Sylowsätze	35
3 Ringtheorie	41
3.1 Ringe und ihre grundlegenden Eigenschaften	41
3.2 Einheiten und Nullteiler	44
3.3 Ideale und Quotientenringe	46
3.4 Der Polynomring $R[X]$	50
3.5 Euklidische Ringe	56
3.6 Primideale und maximale Ideale	60
3.7 Der Chinesische Restsatz	64
3.8 Primelemente und irreduzible Elemente	67
3.9 Faktorielle Ringe	69
3.10 Quotientenkörper	73
3.11 Irreduzibilität von Polynomen	75
4 Körpererweiterungen	87
4.1 Algebraische Erweiterungen und Minimalpolynome	88
4.2 Von Polynomen zu Körpererweiterungen	98
4.3 Der Fortsetzungssatz	103
4.4 Der algebraische Abschluss	108
5 Galoistheorie	117
5.1 Die Galoisgruppe	117
5.2 Normale Körpererweiterungen	121
5.3 Separable Körpererweiterungen	125
5.4 Der Satz vom primitiven Element	133

5.5	Der Hauptsatz der Galoistheorie	138
5.6	Endliche Körper	148
5.7	Kreisteilungskörper	157
6	Anwendungen	167
6.1	Vorbereitung: Auflösbare Gruppen	167
6.2	Lösungsformeln für Polynomgleichungen	172
6.3	Der Fundamentalsatz der Algebra	180
6.4	Konstruktionen mit Zirkel und Lineal	183
6.5	Ausblick	189
	Englische Begriffe	194
	Literatur	197
	Index	201

Einleitung

Die Mathematiker sind eine Art
Franzosen: redet man zu ihnen,
so übersetzen sie es in ihre
Sprache, und dann ist es alsobald
ganz etwas Anderes.

Johann Wolfgang von Goethe,
Maximen und Reflexionen

Dieses Skript entstand im Rahmen der Vorlesung „Algebra“ im Wintersemester 2025/2026 an der TU Chemnitz. Es behandelt den Stoff eines einführenden Algebra-Kurses im Bachelorstudium mit dem Ziel, die klassische Galoistheorie zu ergründen. Es arbeitet sich daher von der Gruppentheorie über die Theorie von Ringen (und insbesondere Polynomringen in einer Variablen) hin zum Begriff der Körpererweiterungen. Mit dessen Hilfe wird schließlich die moderne Formulierung der Galoistheorie entwickelt, an deren Höhepunkt der Hauptsatz der Galoistheorie steht. Zum Ende werden noch einige Anwendungen der Galoistheorie auf klassische Probleme wie die Lösung von Polynomgleichungen fünften Grades und Konstruktionen mit Zirkel und Lineal aufgezeigt.

Wir orientieren uns dabei zumeist an [3], aber in Teilen auch an klassischen Lehrbüchern wie [1] sowie, insbesondere für die Beweise der Sylowsätze und einige anschauliche Beispiele, an exzellenten Ausarbeitungen wie [2]. Für hilfreiche Anmerkungen danke ich herzlich den Studierenden der TU Chemnitz, die dieses Skript sehr aufmerksam gelesen haben, besonders Joshua Geißler, Joel Hanisch und Lennart Obermüller.

Die Kunst des mathematischen Problemlösens besteht oft auch darin, offene Fragen so umzuformulieren und -interpretieren, dass sie in Verbindung mit schon besser verstandenen Fragen gebracht werden oder gar als Spezialfall einer allgemeineren Theorie erkannt werden können. Die Algebra, die wir hier behandeln werden, und dabei insbesondere die – zu Lebzeiten des Erfinders größtenteils unverstandene – Galoistheorie, sind dafür in der Tat ein hervorragendes Beispiel. Das Vorgehen, das im Goethe-Zitat zu Beginn dieser Einleitung recht unverblümt aufs Korn genommen wird, ist also in Wirklichkeit in vielen Fällen ein wichtiger Teil der Arbeit eines Mathematikers: Man muss Aussagen manchmal in eine andere, bisweilen abstraktere Sprache übersetzen, um eine passende Theorie aufbauen und der Lösung einer Fragestellung näher kommen zu können.

Einleitung

„Andere Sprache“ meint hierbei normalerweise Konzepte und Denkweisen aus einem anderen (oder auch erst noch zu erschaffenden) Teilgebiet der Mathematik. Dabei ist es natürlich in der Regel nicht zwingend nötig, die betroffenen Aussagen in die *französische* Sprache zu übersetzen, mit deren Sprechern Goethe die Mathematiker vergleicht. Nun sind aber die Theorien, um die es hier in großen Teilen geht, maßgeblich von der französischen Mathematik und insbesondere durch die Arbeiten von Évariste Galois (1811–1832) beeinflusst und geformt. Um den Geist der Sprache, der Epoche und der Mathematik dieses Genies durchweg lebendig zu halten, ist jedes Kapitel dieses Skripts mit einem passenden Zitat – zumeist französischen Ursprungs – gespickt.

Als Vorwissen für diese Vorlesung werden – außer eines grundlegenden Verständnisses von Logik, Mengen und Abbildungen – einige Begriffe aus der linearen Algebra vorausgesetzt. Dies beschränkt sich aber weitgehend auf die elementaren Begriffe eines Vektorraums, einer Basis und der Dimension eines Vektorraums.

Konventionen und Notation Wir verwenden die folgenden Standardnotationen:

- $\mathbb{N} = \{1, 2, 3, \dots\}$: natürliche Zahlen (ohne Null)
- $\mathbb{N}_0 := \mathbb{N} \cup \{0\} = \{0, 1, 2, 3, \dots\}$
- \mathbb{Z} : ganze Zahlen
- \mathbb{Q} : rationale Zahlen
- \mathbb{R} : reelle Zahlen
- \mathbb{C} : komplexe Zahlen
- $\#M$: Anzahl der Elemente in der Menge M
- \sqcup : disjunkte Vereinigung, d.h. Vereinigung paarweise disjunkter Mengen
- $a \mid b$: „ a teilt b “, „ a ist ein Teiler von b “

Einführung und Motivation

L'algèbre n'est qu'une géométrie écrite, la géométrie n'est qu'une algèbre figurée.

Algebra ist nichts anderes als
Geometrie in Worten,
Geometrie ist nichts anderes als
Algebra in Bildern.

Sophie Germain

Zahlbereichserweiterungen sind uns aus unserer Schulzeit wohlbekannt. Als Kinder lernen wir zunächst die natürlichen Zahlen \mathbb{N} und die beiden grundlegenden Operationen namens *Addition* und *Multiplikation* kennen, stellen aber während unserer Schulzeit wiederholt fest, dass wir den Zahlbereich erweitern müssen, wenn wir diese Operationen in gewisser Weise auch „rückgängig machen“ möchten. (Mit unserem heutigen Wissen würden wir sagen: „Gleichungen lösen, welche die Addition und Multiplikation beinhalten“.) So führt man zuerst die ganzen Zahlen \mathbb{Z} und später die rationalen Zahlen \mathbb{Q} ein. Letztere bilden einen Körper, haben also aus algebraischer Sicht bereits eine schöne Struktur, es gibt aber immer noch Polynomgleichungen, die in \mathbb{Q} nicht lösbar sind, wie zum Beispiel $x^2 - 2 = 0$.

Die meisten dieser „Probleme“ lösen sich, sobald man zu den reellen Zahlen übergeht. Dahinter steckt eine analytische Konstruktion, die *Vervollständigung* von \mathbb{Q} bezüglich des Absolutbetrags. Dabei erhält man allerdings auch viele Zahlen, die wir uns aus algebraischer Sicht zunächst „gar nicht gewünscht hätten“, nämlich sogenannte *transzendente* Zahlen wie die Kreiszahl π oder die Eulersche Zahl e – sie sind nicht Lösungen irgendeiner polynomiellen Gleichung mit rationalen Koeffizienten. Trotzdem bleibt bei dieser Konstruktion im Wesentlichen eine Gleichung „ungelöst“: Auch in \mathbb{R} hat die Gleichung $x^2 + 1 = 0$ noch keine Lösung.

Abhilfe zur Lösung dieser letzten Gleichung schafft eine weitere Zahlbereichserweiterung – die zu den komplexen Zahlen \mathbb{C} . Das Vorgehen dazu klingt erst

Kapitel 1 Einführung und Motivation

einmal recht gewagt: Man *definiert* (man könnte sagen „erfindet“) einfach eine Lösung dieser Gleichung (als abstraktes Symbol) und nennt sie i . Dann betrachtet man alle Zahlen, die man aus den gewöhnlichen reellen Zahlen und diesem i durch die gewohnten Rechenoperationen (d.h. Addition, Multiplikation sowie Inversenbildung) zusammensetzen kann. Es stellt sich heraus, dass man nur Zahlen von der Form $z = a + bi$ mit $a, b \in \mathbb{R}$ betrachten muss: Höhere Potenzen von i sind nicht notwendig, da sich zum Beispiel $i^2 = -1$, $i^3 = -i$ bereits mit den Basiselementen 1 und i darstellen lassen. Multiplikativ Inverse muss man ebenfalls nicht „künstlich“ einführen, denn zu $z = 1 + i$ ist zum Beispiel $z^{-1} = \frac{1}{2} - \frac{1}{2}i$ ein multiplikativ Inverses. Somit ist die Menge

$$\mathbb{C} := \{a + bi \mid a, b \in \mathbb{R}\}$$

mit den offensichtlich definierten Rechenoperationen $+$ und \cdot ein Körper. (Man schreibt auch $\mathbb{C} = \mathbb{R}[i]$. Diese Notation verstehen wir später genauer.) Er enthält insbesondere jede reelle Zahl, das heißt wir haben eine Teilmengenbeziehung $\mathbb{R} \subseteq \mathbb{C}$. Man sagt deshalb auch, dass \mathbb{C}/\mathbb{R} eine *Körpererweiterung* ist (gelesen „ \mathbb{C} über \mathbb{R} “). Wir nennen \mathbb{C} auch den *Zerfällungskörper* von $X^2 + 1$ über \mathbb{R} , denn er ist die kleinstmögliche Erweiterung von \mathbb{R} , in der das Polynom $X^2 + 1$ alle seine Nullstellen hat. Diese Nullstellen sind offensichtlich die Zahlen $-i$ und i .

Anhand dieser sehr einfachen Körpererweiterung und ähnlicher Beispiele wollen wir uns nun ein paar Begriffe und Argumente ansehen, die uns im Laufe dieser Vorlesung allgemeiner begegnen werden.

Die Galoisgruppe. Wenn man ein Objekt (in diesen Fall eine Körpererweiterung) untersuchen möchte, ist es oft hilfreich, seine Symmetrien zu untersuchen. Hier bedeutet das, dass man sich folgende Frage stellt:

Wie kann man die Nullstellen von $X^2 + 1$ permutieren,
sodass bei jeder Nullstelle die „algebraischen Eigenschaften erhalten bleiben“?¹

Die Antwort ist recht einfach: Natürlich gibt es die Identitätspermutation $\text{id}: \{-i, i\} \rightarrow \{-i, i\}$, gegeben durch

$$\begin{aligned} -i &\mapsto -i \\ i &\mapsto i, \end{aligned}$$

es gibt aber auch die Permutation $\tau: \{-i, i\} \rightarrow \{-i, i\}$ mit

$$\begin{aligned} -i &\mapsto i \\ i &\mapsto -i. \end{aligned}$$

(Es ist „erlaubt“, $-i$ auf i abzubilden, denn beide erfüllen dieselbe „algebraische Eigenschaft“, nämlich diejenige, dass ihr Quadrat gleich -1 ist. Anders gesagt:

¹Diese Formulierung ist nicht besonders präzise, was uns aber für diese Einleitung genügen soll. Genauer müsste man fragen: Welche *Körperautomorphismen* $\varphi: \mathbb{C} \rightarrow \mathbb{C}$ mit $\varphi|_{\mathbb{R}} = \text{id}_{\mathbb{R}}$ gibt es?

Das „kleinstmögliche“ Polynom über \mathbb{R} , welches die Zahl auf Null abbildet, das sogenannte *Minimalpolynom*, ist für $-i$ und i dasselbe, nämlich $X^2 + 1$.)

Es gibt also zwei Abbildungen, die zur obigen Frage passen. Die Menge $\{\text{id}, \tau\}$ dieser beiden Abbildungen ist zusammen mit der Verknüpfung \circ eine Gruppe mit zwei Elementen.² Wir nennen sie die *Galoisgruppe* $\text{Gal}(\mathbb{C}/\mathbb{R})$ der Körpererweiterung.

Die Körpererweiterung \mathbb{R}/\mathbb{Q} ist im Gegensatz dazu nicht so leicht algebraisch zu verstehen. Sie entsteht nicht durch Hinzunahme *eines* neuen Elements, sondern durch Hinzunahme unendlich vieler neuer Elemente (Quadratwurzeln, höhere Wurzeln, aber auch Zahlen, die sich vielleicht nicht durch Wurzelausdrücke darstellen lassen, und sogar *transzendente* Zahlen wie π oder e). In der Realität braucht man aber ja meistens gar nicht *alle* reellen Zahlen: Es ist zwar schön zu wissen, dass es den Körper \mathbb{R} gibt, aber wenn es uns um eine bestimmte Gleichung geht, brauchen wir für ihre Lösung ja nur ein paar einzelne irrationale Zahlen. Es reicht also, sich *Zwischenkörper* anzusehen.

Ein Beispiel ist ganz analog zu dem, was wir oben gesehen haben: Wir betrachten das Polynom $X^2 - 2$ über \mathbb{Q} . Dieses hat zwei Nullstellen, die noch nicht in \mathbb{Q} liegen, nämlich $-\sqrt{2}$ und $\sqrt{2}$. Wir betrachten den Erweiterungskörper

$$\mathbb{Q}[\sqrt{2}] := \{a + b\sqrt{2} \mid a, b \in \mathbb{Q}\}.$$

(Ganz ähnlich wie bei \mathbb{C} überlegt man sich auch hier, dass das ein Körper ist.)

Dies ist also der Zerfällungskörper von $X^2 - 2$ über \mathbb{Q} und seine Galoisgruppe hat zwei Elemente, nämlich die Identitätsabbildung $\text{id}: \{-\sqrt{2}, \sqrt{2}\} \rightarrow \{-\sqrt{2}, \sqrt{2}\}$ mit

$$\begin{aligned} -\sqrt{2} &\mapsto -\sqrt{2} \\ \sqrt{2} &\mapsto \sqrt{2} \end{aligned}$$

sowie die Abbildung, die die beiden Nullstellen vertauscht, also $\tau: \{-\sqrt{2}, \sqrt{2}\} \rightarrow \{-\sqrt{2}, \sqrt{2}\}$ mit

$$\begin{aligned} -\sqrt{2} &\mapsto \sqrt{2} \\ \sqrt{2} &\mapsto -\sqrt{2}. \end{aligned}$$

Auch hier hat die Galoisgruppe $\text{Gal}(\mathbb{Q}[\sqrt{2}]/\mathbb{Q})$ also zwei Elemente.

Etwas spannender wird es, wenn wir den folgenden Körper betrachten:

$$\mathbb{Q}[\sqrt{2}, \sqrt{3}] := \{a + b\sqrt{2} + c\sqrt{3} + d\sqrt{6} \mid a, b, c, d \in \mathbb{Q}\}.$$

(Man beachte, dass man hier den Term $d\sqrt{6}$ unbedingt braucht, sonst wäre die Multiplikation $\sqrt{2} \cdot \sqrt{3}$ nicht definiert und das Ganze sicher kein Körper. Dass

²Diese Gruppe ist im Grunde nichts anderes als (d.h. isomorph zu) $\mathbb{Z}/2\mathbb{Z} = \{0, 1\}$ (mit der Addition als Verknüpfung).

Kapitel 1 Einführung und Motivation

es hier auch multiplikativ Inverse gibt, ist nicht ganz so einfach zu sehen, aber wir glauben das für den Moment einfach mal.) Dies ist der Zerfällungskörper des Polynoms $(X^2 - 2)(X^2 - 3)$ über \mathbb{Q} , dessen Nullstellen $-\sqrt{2}, \sqrt{2}, -\sqrt{3}, \sqrt{3}$ sind. Die Galoisgruppe besteht hier aus vier Elementen, nämlich

id	τ_1	τ_2	τ_3
$-\sqrt{2} \mapsto -\sqrt{2}$	$-\sqrt{2} \mapsto \sqrt{2}$	$-\sqrt{2} \mapsto -\sqrt{2}$	$-\sqrt{2} \mapsto \sqrt{2}$
$\sqrt{2} \mapsto \sqrt{2}$	$\sqrt{2} \mapsto -\sqrt{2}$	$\sqrt{2} \mapsto \sqrt{2}$	$\sqrt{2} \mapsto -\sqrt{2}$
$-\sqrt{3} \mapsto -\sqrt{3}$	$-\sqrt{3} \mapsto -\sqrt{3}$	$-\sqrt{3} \mapsto \sqrt{3}$	$-\sqrt{3} \mapsto \sqrt{3}$
$\sqrt{3} \mapsto \sqrt{3}$	$\sqrt{3} \mapsto \sqrt{3}$	$\sqrt{3} \mapsto -\sqrt{3}$	$\sqrt{3} \mapsto -\sqrt{3}$

Dies sind tatsächlich die einzig möglichen Permutationen mit der gewünschten Eigenschaft, da $\sqrt{2}$ beispielsweise nicht auf $\sqrt{3}$ abgebildet werden kann: Die beiden Elemente erfüllen nicht dieselben „algebraischen Eigenschaften“, denn das erste Element ergibt quadriert die rationale Zahl 2, das zweite aber die Zahl 3. (In anderen Worten: Die beiden Zahlen haben nicht dasselbe Minimalpolynom.)

Die Galoisgruppe ist hier also $\text{Gal}(\mathbb{Q}[\sqrt{2}, \sqrt{3}]/\mathbb{Q}) = \{\text{id}, \tau_1, \tau_2, \tau_3\}$.³

Die Galoisgruppe wird uns im Allgemeinen helfen, die Struktur einer Körpererweiterung besser zu verstehen. Ein kurzer Ausblick auf das Hauptresultat:

Wir haben oben zwei Erweiterungen von \mathbb{Q} betrachtet:

$$\mathbb{Q} \subseteq \mathbb{Q}[\sqrt{2}] \subseteq \mathbb{Q}[\sqrt{2}, \sqrt{3}].$$

Eben haben wir die Galoisgruppe $\text{Gal}(\mathbb{Q}[\sqrt{2}, \sqrt{3}]/\mathbb{Q})$ bestimmt, d.h. wir haben $\mathbb{Q}[\sqrt{2}, \sqrt{3}]$ als Erweiterung von \mathbb{Q} angesehen, nämlich als Zerfällungskörper des Polynoms $(X^2 - 2)(X^2 - 3)$. Wir können $\mathbb{Q}[\sqrt{2}, \sqrt{3}]$ natürlich auch als Erweiterung von $\mathbb{Q}[\sqrt{2}]$ betrachten, d.h. wir starten bereits mit einem größeren Grundkörper. Über $\mathbb{Q}[\sqrt{2}]$ ist $\mathbb{Q}[\sqrt{2}, \sqrt{3}]$ dann der Zerfällungskörper von $X^2 - 3$, d.h. die Zahl $\sqrt{2}$ wird nun nicht mehr als „neue“ Nullstelle betrachtet und darf somit nicht permutiert werden. Als Elemente der Galoisgruppe kommen daher nur die Elemente id und τ_2 von oben in Frage, es gilt also

$$\text{Gal}(\mathbb{Q}[\sqrt{2}, \sqrt{3}]/\mathbb{Q}[\sqrt{2}]) = \{\text{id}, \tau_2\} \subseteq \text{Gal}(\mathbb{Q}[\sqrt{2}, \sqrt{3}]/\mathbb{Q}).$$

Wir beobachten also: „Vergrößern“ wir den Grundkörper, so „verkleinert“ sich die Galoisgruppe, d.h. wir können die neue Galoisgruppe als Untergruppe der ursprünglichen auffassen. Der *Hauptsatz der Galoistheorie* macht dies präzise: Er besagt, dass es (unter den passenden Voraussetzungen) eine 1-zu-1-Beziehung (also eine Bijektion) zwischen Untergruppen der Galoisgruppe und Zwischenkörpern der

³Man kann sich überlegen, dass $\tau_3 = \tau_1 \circ \tau_2$ gilt und dass diese Gruppe isomorph zur additiven Gruppe $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ ist.

Körpererweiterung gibt, dass also jedem Zwischenkörper auf natürliche Weise eine eindeutige Untergruppe der Galoisgruppe entspricht und umgekehrt. Der Hauptsatz erlaubt es uns also, Aussagen über alle möglichen Zwischenkörper zu machen, wenn es uns gelingt, alle möglichen Untergruppen der Galoisgruppe zu verstehen. Dies ist der Grund dafür, dass die Theorie der Gruppen in dieser Vorlesung eine entscheidende Rolle spielt.

Körpertheorie und algebraische Ausdrücke. Nun sehen wir das erste Beispiel eines galoistheoretischen Arguments:

Betrachten wir die Zahl $\alpha := \sqrt{2} + \sqrt{3} \in \mathbb{R}$. Das Minimalpolynom dieses Elements über \mathbb{Q} ist $X^4 - 10X^2 + 1$. (Das ist nicht sofort klar, man kann sich aber überlegen, dass sich dieses Polynom über \mathbb{Q} nicht weiter zerlegen lässt.) Die Menge

$$\mathbb{Q}[\sqrt{2} + \sqrt{3}] := \{a + b\alpha + c\alpha^2 + d\alpha^3 \mid a, b, c, d \in \mathbb{Q}\}$$

ist dann ein Körper (wie wir später zeigen werden). Weiter gilt

$$\mathbb{Q}[\sqrt{2} + \sqrt{3}] \subseteq \mathbb{Q}[\sqrt{2}, \sqrt{3}],$$

denn $\alpha \in \mathbb{Q}[\sqrt{2}, \sqrt{3}]$ und somit auch $\alpha^2, \alpha^3 \in \mathbb{Q}[\sqrt{2}, \sqrt{3}]$, weil letzterer ein Körper ist.

Jetzt kommt die entscheidende Idee: Da sowohl $\mathbb{Q}[\sqrt{2} + \sqrt{3}]$ als auch $\mathbb{Q}[\sqrt{2}, \sqrt{3}]$ jeweils 4-dimensionale \mathbb{Q} -Vektorräume sind, folgt daraus mit unserem Wissen aus der linearen Algebra bereits

$$\mathbb{Q}[\sqrt{2} + \sqrt{3}] = \mathbb{Q}[\sqrt{2}, \sqrt{3}].$$

Damit können wir also folgern, dass sich $\sqrt{2}$ schreiben lässt als rationaler Polynomausdruck der Form

$$\sqrt{2} = a + b(\sqrt{2} + \sqrt{3}) + c(\sqrt{2} + \sqrt{3})^2 + d(\sqrt{2} + \sqrt{3})^3$$

für passende $a, b, c, d \in \mathbb{Q}$, und genauso für $\sqrt{3}$. In anderen Worten: Aus dem Element $\sqrt{2} + \sqrt{3}$ und den rationalen Zahlen kann man nur durch Addition und Multiplikation bereits die Elemente $\sqrt{2}$ und $\sqrt{3}$ einzeln erzeugen. Auch wenn uns das noch nicht sagt, was die Koeffizienten a, b, c, d genau sind, ist das eine Erkenntnis, die wir intuitiv vielleicht nicht erwartet hätten. Sie ergibt sich aber mithilfe der Theorie der Körpererweiterungen durch ein einfaches Lineare-Algebra-Argument.

Klassische Problemstellungen. Warum sind solche Aussagen und Argumente nun wichtig? In vielen klassischen Fragen geht es darum, ob man eine Zahl „in einer bestimmten Form schreiben kann“ oder „mithilfe bestimmter Operationen aus anderen erzeugen kann“.

Ein bekanntes Beispiel ist die Frage nach einer *allgemeinen Lösungsformel für Polynomgleichungen fünften Grades*. Wir kennen die *p-q-Formel* (oder die *Mitternachtsformel*) für quadratische Gleichungen, und für Gleichungen dritten und vierten Grades

sind ähnliche (wenn auch natürlich kompliziertere) Formeln seit dem 16. Jahrhundert bekannt. Für die allgemeine Gleichung fünften Grades gibt es – wie man heute weiß – so eine Formel nicht. Um das zu beweisen, muss man sich überlegen, dass sich die Lösungen im Allgemeinen nicht als Kombination von Wurzelausdrücken aus rationalen Zahlen und den üblichen Rechenoperationen darstellen lassen.

Ein weiteres Beispiel sind Fragen nach der Durchführbarkeit bestimmter *Konstruktionen mit Zirkel und Lineal*⁴. Das bekannteste ist wohl die Unmöglichkeit der *Quadratur des Kreises*. Man kann aber auch zeigen, dass die *Würfelverdopplung*, die *Winkeldreiteilung* oder die *Konstruktion bestimmter regelmäßiger n -Ecke mit Zirkel und Lineal* nicht möglich ist.

Was hat dies nun mit der obigen Frage zu tun? Führt man eine Konstruktion mit Zirkel und Lineal durch, so werden in jedem Konstruktionsschritt Kreise und Geraden miteinander geschnitten. Algebraisch bedeutet das, dass jede neu konstruierte Länge die Lösung einer linearen oder quadratischen Gleichung ist, welche von den vorher konstruierten Längen abhängt. Auch hier ist also die Frage nach der Konstruierbarkeit einer bestimmten Länge nichts anderes als die Frage danach, ob sich die gewünschte Länge sukzessiv als Ausdruck mit Quadratwurzeln und den üblichen Rechenoperationen darstellen lässt.

Die Theorie der Körpererweiterungen und die Erkenntnisse aus der Galoistheorie helfen uns daher, die Lösung all dieser Probleme besser zu verstehen. Diese Probleme wurden zwar nicht erst durch Galois' Erkenntnisse gelöst, die moderne Formulierung der Galoistheorie hat aber dazu beigetragen, sie systematischer und einheitlicher anzugehen.

⁴Die Formulierung „Zirkel und Lineal“ ist etwas irreführend, denn man darf das Lineal nur benutzen, um Strecken zu zeichnen und zu verlängern, man darf damit aber keine Längen abmessen. Das „Lineal“ hat also hier keine Skala.

Gruppentheorie

Wo immer der Mensch Ordnung, Schönheit und Vollkommenheit zu begreifen oder zu schaffen versucht hat, war Symmetrie ihm ein leitendes Prinzip.

Hermann Weyl

2.1 Gruppen und ihre grundlegenden Eigenschaften

Definition 2.1. Eine *Gruppe* (G, \cdot) besteht aus einer Menge G und einer Abbildung

$$\cdot : G \times G \rightarrow G, \quad (g_1, g_2) \mapsto g_1 \cdot g_2,$$

sodass gilt

$$(1) \quad \forall g_1, g_2, g_3 \in G : (g_1 \cdot g_2) \cdot g_3 = g_1 \cdot (g_2 \cdot g_3) \quad (\text{Assoziativitat})$$

und sodass ein Element $e \in G$ existiert mit den folgenden Eigenschaften:

$$(2) \quad \forall g \in G : e \cdot g = g, \quad (\text{Existenz eines Linksneutralen})$$

$$(3) \quad \forall g \in G \exists h \in G : h \cdot g = e. \quad (\text{Existenz von Linksinversen})$$

Die Abbildung \cdot heist *Verknufung* und wird manchmal auch additiv geschrieben (d.h. als „+“ statt „ \cdot “) oder – je nach Kontext – mit anderen Symbolen (z.B. „ \circ “). Insbesondere bei der multiplikativen Schreibweise wird das Verknufungssymbol auch oft weggelassen, d.h. man schreibt gh statt $g \cdot h$.

Da die Verknufung in einer Gruppe nach Axiom (1) assoziativ ist, schreibt man oft einfach $g_1 \cdot g_2 \cdot g_3$ oder $g_1 g_2 g_3$ anstelle von $(g_1 g_2) g_3$ oder $g_1 (g_2 g_3)$, da die beiden letzten Ausdrucke gleich sind.

Oft ist die Verknufung aus dem Kontext klar und man schreibt einfach G fur die Gruppe (G, \cdot) . (Genauso werden wir das auch mit Ringen und Korpern spater handhaben.)

Kapitel 2 Gruppentheorie

Lemma-Definition 2.2. Sei (G, \cdot) eine Gruppe. Dann gilt:

- (i) Für jedes $g \in G$ ist das Element h aus Axiom (3) auch rechtsinvers, d.h. $g \cdot h = e$.
- (ii) Das Element e ist auch rechtsneutral, d.h. $\forall g \in G : g \cdot e = g$.
- (iii) Für jedes $g \in G$ ist das Element h aus Axiom (3) eindeutig bestimmt.
- (iv) Das Element e ist durch die Axiome eindeutig bestimmt.

Wir nennen e das *neutrale Element* von G . Für jedes $g \in G$ bezeichnen wir das zugehörige Element h aus Axiom (3) mit g^{-1} und nennen es das *Inverse* zu g . (Wird die Gruppenverknüpfung additiv geschrieben, dann bezeichnen wir das Inverse meist stattdessen mit $-g$.)

Beweis. (i) Sei $g \in G$ und $h \in G$ ein Linksinverses. Ebenso hat auch h ein Linksinverses $k \in G$. Es gilt also $hg = e$ und $kh = e$ und daraus erhalten wir

$$gh = e(gh) = (kh)(gh) = k(h(gh)) = k((hg)h) = k(eh) = kh = e,$$

also ist h auch ein Rechtsinverses von g .

(ii) Sei $g \in G$ und sei $h \in G$ ein (Rechts- und Links-)Inverses. Dann gilt

$$ge = g(hg) = (gh)g = eg = g,$$

also ist e auch rechtsneutral.

(iii) Sei $g \in G$ und seien $h, h' \in G$ zwei (Links- und Rechts-)Inverse zu g . Dann gilt

$$h = eh = (h'g)h = h'(gh) = h'e = h'.$$

(iv) Seien $e, e' \in G$ zwei (rechts- und links-)neutrale Elemente. Dann gilt $ee' = e$, weil e' neutral ist, es gilt aber auch $ee' = e'$, weil e neutral ist. Also folgt $e = e'$. \square

Es ist leicht zu sehen, dass $e^{-1} = e$ gilt, das neutrale also zu sich selbst invers ist.

Bemerkung 2.3. Natürlich kann man auch algebraische Strukturen mit einer Verknüpfung betrachten, die nicht alle der obigen Gruppenaxiome aus Definition 2.1 erfüllen. Einige gebräuchliche Begriffe möchten wir hier kurz erwähnen:

Ein Paar (G, \cdot) bestehend aus einer Menge G und einer Verknüpfung $G \times G \rightarrow G, (g_1, g_2) \mapsto g_1 \cdot g_2$, an das keine zusätzlichen Bedingungen gestellt werden, heißt *Magma*. Ist zusätzlich das Gruppenaxiom (1) erfüllt, nennen wir es *Halbgruppe*. Falls dazu auch noch das Axiom

$$(2') \quad \exists! e \in G \quad \forall g \in G : e \cdot g = g \cdot e = g \quad \text{(neutrales Element)}$$

gilt, heißt (G, \cdot) ein *Monoid*. Man beachte, dass wir hier (im Gegensatz zum Axiom (2) von oben) die Eindeutigkeit sowie die Links- und Rechtsneutralität von e fordern müssen, da die fehlenden Eigenschaften ohne das Axiom (3) nicht wie in Lemma-Definition 2.2 automatisch folgen.

Insbesondere der Begriff des Monoids wird uns später bei der Definition eines Rings noch einmal nützlich sein.

Lemma 2.4. Sei (G, \cdot) eine Gruppe, dann gilt für beliebige $g, h \in G$

(i) $(g^{-1})^{-1} = g,$

(ii) $(gh)^{-1} = h^{-1}g^{-1}.$

Beweis. (i) Aus Lemma-Definition 2.2 wissen wir, dass $g^{-1}g = gg^{-1} = e$. Ebenso gilt, weil das Element $(g^{-1})^{-1}$ das Inverse zu g^{-1} ist, dass $(g^{-1})^{-1}g^{-1} = g^{-1}(g^{-1})^{-1} = e$. Also folgt insbesondere $g^{-1}g = g^{-1}(g^{-1})^{-1}$ und daraus (durch Multiplikation mit g von links), dass $g = (g^{-1})^{-1}$.

(ii) Wir müssen zeigen, dass $h^{-1}g^{-1}$ das Inverse zu gh ist. Dies rechnet man leicht nach:

$$(h^{-1}g^{-1})(gh) = h^{-1} \underbrace{(g^{-1}g)}_{=e} h = h^{-1}h = e.$$

□

Definition 2.5. Eine Gruppe (G, \cdot) heißt *abelsche Gruppe*, falls gilt:

$$\forall g_1, g_2 \in G : g_1 \cdot g_2 = g_2 \cdot g_1. \quad (\text{Kommutativität})$$

Beispiel 2.6. Einige wichtige und bekannte Beispiele für Gruppen sind:

- $(\mathbb{Z}, +), (\mathbb{Q}, +), (\mathbb{R}, +)$ und $(\mathbb{C}, +),$
- $(\mathbb{Q} \setminus \{0\}, \cdot), (\mathbb{R} \setminus \{0\}, \cdot)$ und $(\mathbb{C} \setminus \{0\}, \cdot),$
- $(\mathbb{Q}_{>0}, \cdot)$ und $(\mathbb{R}_{>0}, \cdot),$
- $(\mathbb{Z}/n\mathbb{Z}, +)$ für $n \in \mathbb{N}$ (siehe auch §2.3),
- die symmetrische Gruppe (S_n, \circ) für $n \in \mathbb{N}$ (siehe auch §2.2).

Beispiele für Monoide, die keine Gruppen sind (d.h. es gibt ein neutrales Element, aber nicht jedes Element besitzt ein Inverses), sind:

- $(\mathbb{N}_0, +),$
- $(\mathbb{Z}, \cdot), (\mathbb{Q}, \cdot), (\mathbb{R}, \cdot)$ und $(\mathbb{C}, \cdot).$

Ähnlich wie bei Vektorräumen in der linearen Algebra möchten wir auch „gute“ Teilmengen einer Gruppe (*Untergruppen*) und „gute“ Abbildungen zwischen Gruppen (*Homomorphismen*) betrachten.

Kapitel 2 Gruppentheorie

Definition 2.7. Sei (G, \cdot) eine Gruppe mit neutralem Element e . Dann heißt eine Teilmenge $H \subseteq G$ **Untergruppe**, falls die folgenden Eigenschaften erfüllt sind:

- (1) $e \in H$,
- (2) $\forall h_1, h_2 \in H : h_1 \cdot h_2 \in H$,
- (3) $\forall h \in H : h^{-1} \in H$.

In diesem Fall bildet die Menge H zusammen mit der (auf H eingeschränkten) Verknüpfung $\cdot : H \times H \rightarrow H$ selbst wieder eine Gruppe (H, \cdot) .

Lemma-Definition 2.8. Sei (G, \cdot) eine Gruppe und $g \in G$ ein Element. Für $k \in \mathbb{N}$ schreiben wir kurz

$$g^k := \underbrace{g \cdot \dots \cdot g}_{k\text{-mal}}$$

Für $k \in \mathbb{Z}, k < 0$, schreiben wir

$$g^{-k} := \underbrace{g^{-1} \cdot \dots \cdot g^{-1}}_{|k|\text{-mal}}$$

und setzen außerdem $g^0 := e$. Dann ist

$$\langle g \rangle := \{g^k \mid k \in \mathbb{Z}\} \subseteq G$$

eine Untergruppe von G und wir nennen sie die *von g erzeugte zyklische Untergruppe* von G .

Wir nennen eine Gruppe G **zyklisch**, falls es ein $g \in G$ gibt mit $G = \langle g \rangle$.

Beweis. Aus der Definition von g^k für $k \in \mathbb{Z}$ sieht man sofort, dass für $k, k' \in \mathbb{Z}$ gilt: $g^k \cdot g^{k'} = g^{k+k'}$ und auch $(g^k)^{-1} = g^{-k}$. Wir prüfen damit für $\langle g \rangle \subseteq G$ die Axiome einer Untergruppe:

- (1) $e = g^0 \in \langle g \rangle$,
- (2) Seien $h_1, h_2 \in \langle g \rangle$, d.h. es gibt $k_1, k_2 \in \mathbb{Z}$, sodass $h_1 = g^{k_1}$ und $h_2 = g^{k_2}$. Dann folgt

$$h_1 \cdot h_2 = g^{k_1} \cdot g^{k_2} = g^{k_1+k_2} \in \langle g \rangle.$$

- (3) Sei $h \in \langle g \rangle$, d.h. es gibt ein $k \in \mathbb{Z}$, sodass $h = g^k$. Dann ist

$$h^{-1} = (g^k)^{-1} = g^{-k} \in \langle g \rangle.$$

□

Ist $(G, +)$ eine additiv geschriebene Gruppe, so schreiben wir normalerweise $k \cdot g$ anstelle von g^k , d.h. $k \cdot g := g + \dots + g$ für $k > 0$ sowie $0 \cdot g := e$ und $k \cdot g := (-g) + \dots + (-g)$ für $k < 0$.

Definition 2.9. Seien (G, \cdot) und $(\tilde{G}, \tilde{\cdot})$ zwei Gruppen. Eine Abbildung $\varphi: G \rightarrow \tilde{G}$ heißt **Gruppenhomomorphismus**, falls gilt:

$$\forall g_1, g_2 \in G : \varphi(g_1 \cdot g_2) = \varphi(g_1) \tilde{\cdot} \varphi(g_2).$$

Wie das nächste Lemma zeigt, kann man aus der Definition bereits folgern, dass Gruppenhomomorphismen das neutrale Element der einen Gruppe auf das der anderen Gruppe abbilden und dass sie das Inverse eines Elements auf das Inverse seines Bildes abbilden.

Lemma 2.10. Sei (G, \cdot) eine Gruppe mit neutralem Element e und sei $(\tilde{G}, \tilde{\cdot})$ eine Gruppe mit neutralem Element \tilde{e} . Sei $\varphi: G \rightarrow \tilde{G}$ ein Gruppenhomomorphismus. Dann gilt:

- (i) $\varphi(e) = \tilde{e}$,
- (ii) $\forall g \in G : \varphi(g^{-1}) = \varphi(g)^{-1}$.

Beweis. (i) Da φ ein Gruppenhomomorphismus ist, gilt

$$\varphi(e) = \varphi(e \cdot e) = \varphi(e) \tilde{\cdot} \varphi(e).$$

Multiplizieren wir diese Gleichung auf beiden Seiten mit $\varphi(e)^{-1}$, so erhalten wir $\tilde{e} = \varphi(e)$.

- (ii) Zu zeigen ist, dass $\varphi(g^{-1})$ ein Inverses (in \tilde{G}) zu $\varphi(g)$ ist. Dies folgt, da φ ein Gruppenhomomorphismus ist, aus

$$\varphi(g^{-1}) \tilde{\cdot} \varphi(g) = \varphi(g^{-1} \cdot g) = \varphi(e) \stackrel{(i)}{=} \tilde{e}.$$

□

Definition 2.11. Sei $\varphi: G \rightarrow \tilde{G}$ ein Gruppenhomomorphismus und sei \tilde{e} das neutrale Element in \tilde{G} . Dann heißt

$$\ker(\varphi) := \{g \in G \mid \varphi(g) = \tilde{e}\} \subseteq G$$

der **Kern** von φ und

$$\text{im}(\varphi) := \{\varphi(g) \mid g \in G\} = \{\tilde{g} \in \tilde{G} \mid \exists g \in G : \tilde{g} = \varphi(g)\} \subseteq \tilde{G}$$

das **Bild** von φ .

Lemma 2.12. Ist $\varphi: G \rightarrow \tilde{G}$ ein Gruppenhomomorphismus, so ist $\ker(\varphi)$ eine Untergruppe von G und $\text{im}(\varphi)$ eine Untergruppe von \tilde{G} .

Beweis. Wir verwenden im Folgenden die Eigenschaften eines Gruppenhomomorphismus.

$\ker(\varphi) \subseteq G$ ist eine Untergruppe, denn:

Kapitel 2 Gruppentheorie

(1) $\varphi(e) = \tilde{e}$, also $e \in \ker(\varphi)$.

(2) Seien $h_1, h_2 \in \ker(\varphi)$, d.h. $\varphi(h_1) = \tilde{e}$ und $\varphi(h_2) = \tilde{e}$. Dann ist

$$\varphi(h_1 h_2) = \varphi(h_1)\varphi(h_2) = \tilde{e}\tilde{e} = \tilde{e},$$

also $h_1 h_2 \in \ker(\varphi)$.

(3) Sei $h \in \ker(\varphi)$, d.h. $\varphi(h) = \tilde{e}$. Dann ist

$$\varphi(h^{-1}) = \varphi(h)^{-1} = \tilde{e}^{-1} = \tilde{e},$$

also $h^{-1} \in \ker(\varphi)$.

$\text{im}(\varphi) \subseteq \tilde{G}$ ist eine Untergruppe, denn:

(1) $\tilde{e} = \varphi(e)$, also $\tilde{e} \in \text{im}(\varphi)$.

(2) Seien $\tilde{h}_1, \tilde{h}_2 \in \text{im}(\varphi)$, d.h. es gibt $g_1, g_2 \in G$ mit $\tilde{h}_1 = \varphi(g_1)$ und $\tilde{h}_2 = \varphi(g_2)$.
Dann ist

$$\tilde{h}_1 \tilde{h}_2 = \varphi(g_1)\varphi(g_2) = \varphi(g_1 g_2),$$

also $\tilde{h}_1 \tilde{h}_2 \in \text{im}(\varphi)$.

(3) Sei $\tilde{h} \in \text{im}(\varphi)$, d.h. es gibt $g \in G$ mit $\tilde{h} = \varphi(g)$. Dann ist

$$\tilde{h}^{-1} = \varphi(g)^{-1} = \varphi(g^{-1}),$$

also $h^{-1} \in \text{im}(\varphi)$.

□

Wir erinnern uns an zwei wichtige Begriffe im Zusammenhang mit (mengen-theoretischen) Abbildungen: Eine Abbildung $f: X \rightarrow Y$ zwischen zwei Mengen X und Y heißt *surjektiv*, falls gilt:

$$\forall y \in Y \exists x \in X : y = f(x).$$

Dies ist offensichtlich genau dann der Fall, wenn $\text{im}(f) = Y$. (Man kann das Bild von f genauso wie oben definieren, auch wenn f kein Gruppenhomomorphismus ist.)

Eine Abbildung heißt *injektiv*, falls gilt:

$$\forall x, x' \in X : (f(x) = f(x') \Rightarrow x = x').$$

Im Fall eines Gruppenhomomorphismus gibt es das folgende einfache Kriterium für Injektivität.

Lemma 2.13. Sei $\varphi: G \rightarrow \tilde{G}$ ein Gruppenhomomorphismus. Dann ist φ injektiv genau dann, wenn $\ker(\varphi) = \{e\}$.

Beweis. Sei $\ker(\varphi) = \{e\}$. Wir wollen zeigen, dass φ injektiv ist. Seien also $g, g' \in G$ mit $\varphi(g) = \varphi(g')$. Dies ist äquivalent zu (wir verwenden die Tatsache, dass φ ein Gruppenhomomorphismus ist)

$$\tilde{e} = \varphi(g)\varphi(g')^{-1} = \varphi(g)\varphi(g'^{-1}) = \varphi(gg'^{-1}).$$

Somit ist also $gg'^{-1} \in \ker(\varphi)$, also nach Voraussetzung $g \cdot g'^{-1} = e$ und dies impliziert $g = g'$. Daher ist φ injektiv.

Sei umgekehrt φ injektiv und sei $g \in \ker(\varphi)$ ein beliebiges Element im Kern, d.h. $\varphi(g) = \tilde{e}$. Es gilt aber auch $\varphi(e) = \tilde{e}$, da φ ein Gruppenhomomorphismus ist, also erhalten wir $\varphi(g) = \varphi(e)$ und somit $g = e$, da φ nach Voraussetzung injektiv ist. Also ist e das einzige Element im Kern von φ und somit $\ker(\varphi) = \{e\}$. \square

Eine Abbildung $f: X \rightarrow Y$ zwischen zwei Mengen X und Y heißt *bijektiv*, wenn sie injektiv und surjektiv ist. Eine solche Abbildung hat dann eine Umkehrabbildung $f^{-1}: Y \rightarrow X$, die jedem y das eindeutige $x \in X$ mit $f(x) = y$ zuordnet. (Wegen der Surjektivität existiert ein solches x , wegen der Injektivität ist es eindeutig.) Eine wichtige Beobachtung ist, dass im Fall von Gruppenhomomorphismen die Umkehrabbildung wieder ein Gruppenhomomorphismus ist.

Definition 2.14. Ein Gruppenhomomorphismus heißt *Gruppenisomorphismus*, falls er bijektiv (also sowohl injektiv als auch surjektiv) ist.

Lemma 2.15. Sei $\varphi: G \rightarrow \tilde{G}$ ein Gruppenisomorphismus. Dann ist die Umkehrabbildung

$$\varphi^{-1}: \tilde{G} \rightarrow G$$

ebenfalls ein Gruppenisomorphismus.

Beweis. Es ist klar, dass φ^{-1} wieder bijektiv ist. Wir müssen also noch zeigen, dass φ^{-1} ein Gruppenhomomorphismus ist. Dazu erinnern wir uns zunächst, dass für ein $\tilde{g} \in \tilde{G}$ das Element $\varphi^{-1}(\tilde{g}) \in G$ ein Element in G ist, welches von φ auf \tilde{g} abgebildet wird (und dieses ist eindeutig).

Seien $\tilde{g}, \tilde{g}' \in \tilde{G}$. Wir wollen zeigen, dass $\varphi^{-1}(\tilde{g})\varphi^{-1}(\tilde{g}') = \varphi^{-1}(\tilde{g}\tilde{g}')$. Seien $g, g' \in G$ die (eindeutigen) Elemente, sodass $\tilde{g} = \varphi(g)$ und $\tilde{g}' = \varphi(g')$. In anderen Worten ist also $\varphi^{-1}(\tilde{g}) = g$ und $\varphi^{-1}(\tilde{g}') = g'$. Außerdem ist (weil φ ein Gruppenhomomorphismus ist)

$$\varphi(gg') = \varphi(g)\varphi(g') = \tilde{g}\tilde{g}',$$

also $\varphi^{-1}(\tilde{g}\tilde{g}') = gg'$. Die rechte Seite ist aber nichts anderes als $\varphi^{-1}(\tilde{g})\varphi^{-1}(\tilde{g}')$ und dies ergibt die gewünschte Gleichung. \square

2.2 Die symmetrische Gruppe

In diesem Abschnitt beschäftigen wir uns mit einem wichtigen Beispiel einer Gruppe, der Gruppe der *Permutationen* einer endlichen Menge.

Lemma-Definition 2.16. Sei $n \in \mathbb{N}$. Dann bildet die Menge

$$S_n := \{\sigma: \{1, \dots, n\} \rightarrow \{1, \dots, n\} \mid \sigma \text{ ist bijektiv}\}$$

der bijektiven Abbildungen von $\{1, \dots, n\}$ nach $\{1, \dots, n\}$ (auch *Permutationen* von $\{1, \dots, n\}$ genannt) zusammen mit der Verknüpfung von Abbildungen eine Gruppe. Wir nennen (S_n, \circ) die *symmetrische Gruppe auf n Elementen*.

Beweis. Es ist leicht zu sehen, dass die Verknüpfung von Abbildungen assoziativ ist, denn seien $\sigma_1, \sigma_2, \sigma_3 \in S_n$, dann gilt für jedes $i \in \{1, \dots, n\}$ zum einen $((\sigma_1 \circ \sigma_2) \circ \sigma_3)(i) = \sigma_1(\sigma_2(\sigma_3(i)))$, zum anderen aber ebenso $(\sigma_1 \circ (\sigma_2 \circ \sigma_3))(i) = \sigma_1(\sigma_2(\sigma_3(i)))$.

Die Identitätsabbildung $\text{id} \in S_n$ ist das neutrale Element und für jedes $\sigma \in S_n$ ist die Umkehrabbildung ein Inverses (diese existiert, da σ bijektiv ist). \square

Auch wenn das Symbol „ \circ “ die Verknüpfung von Abbildungen beschreibt, nennen wir $\sigma_1 \circ \sigma_2$ oft ein *Produkt* von Permutationen und schreiben manchmal sogar einfach $\sigma_1 \sigma_2$.

Elemente $\sigma \in S_n$ werden oft in der Form

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & \dots & n \\ \sigma(1) & \sigma(2) & \sigma(3) & \dots & \sigma(n) \end{pmatrix}$$

geschrieben. Damit sieht man mit etwas elementarer Kombinatorik leicht, dass $\#S_n = n!$, denn möchte man sich einen beliebigen $\sigma \in S_n$ hinschreiben, so kann man zunächst $\sigma(1)$ aus der Menge $\{1, \dots, n\}$ beliebig wählen (hat also n Wahlmöglichkeiten). Das Element $\sigma(2)$ kann man dann nur noch aus der Menge $\{1, \dots, n\} \setminus \{\sigma(1)\}$ wählen, denn σ muss ja eine bijektive Abbildung sein und darf somit jedes Element nur einmal treffen. Es gibt also für $\sigma(2)$ noch $n - 1$ Wahlmöglichkeiten, für $\sigma(3)$ mit demselben Argument noch $n - 2$ usw. Für $\sigma(n)$ hat man schließlich nur noch eine Möglichkeit. Die Anzahl der Elemente, die man so erzeugen kann, ist also gleich $n \cdot (n - 1) \cdot (n - 2) \cdot \dots \cdot 2 \cdot 1 = n!$ und dies ist folglich die Anzahl der Elemente in S_n .

Eine weitere gängige Schreibweise gibt es für spezielle Elemente von S_n , die sogenannten *Zykel*.

Definition 2.17. Sei $k \in \mathbb{N}$. Ein Element $\sigma \in S_n$ heißt *k -Zykel*, falls es paarweise verschiedene Zahlen $a_1, \dots, a_k \in \{1, \dots, n\}$ gibt, sodass gilt:

- Für jedes $j \in \{1, \dots, k - 1\}$ gilt $\sigma(a_j) = a_{j+1}$ und $\sigma(a_k) = a_1$,
- Für jedes $i \in \{1, \dots, n\} \setminus \{a_1, \dots, a_k\}$ gilt $\sigma(i) = i$.

In diesem Fall schreibt man auch kurz $\sigma = (a_1 a_2 \dots a_k)$.

Ein 2-Zykel heißt auch *Transposition*.

Lemma 2.18. Sei $\sigma \in S_n$ ein k -Zykel. Dann gilt $\sigma^k = \text{id}$.

Beweis. Sei $\sigma = (a_1 a_2 \dots a_k)$. Sei $m \in \{1, \dots, k\}$. Mit der Definition eines Zykelns folgt direkt, dass man σ^m folgendermaßen beschreiben kann:

- Für jedes $j \in \{1, \dots, k-m\}$ gilt $\sigma^m(a_j) = a_{j+m}$ und für jedes $j \in \{k-m+1, \dots, k\}$ gilt $\sigma^m(a_j) = a_{j+m-k}$,
- Für jedes $i \in \{1, \dots, n\} \setminus \{a_1, \dots, a_k\}$ gilt $\sigma^m(i) = i$.

Insbesondere folgt (für $m = k$), dass $\sigma^k(i) = i$ für alle $i \in \{1, \dots, n\}$, also $\sigma^k = \text{id}$. \square

Natürlich ist nicht jede Permutation ein Zykel. Ein wichtiges Resultat ist aber, dass sich jedes beliebige Element von S_n zumindest als *Produkt von Zykeln* schreiben lässt. Um die Aussage noch etwas präziser zu fassen, benötigen wir noch einen Begriff.

Definition 2.19. Zwei Zykel $(a_1 a_2 \dots a_k), (b_1 b_2 \dots b_\ell) \in S_n$ heißen *disjunkt*, falls gilt

$$\{a_1, \dots, a_k\} \cap \{b_1, \dots, b_\ell\} = \emptyset.$$

Lemma 2.20. Seien $(a_1 a_2 \dots a_k), (b_1 b_2 \dots b_\ell) \in S_n$ disjunkte Zykel. Dann gilt

$$(a_1 a_2 \dots a_k) \circ (b_1 b_2 \dots b_\ell) = (b_1 b_2 \dots b_\ell) \circ (a_1 a_2 \dots a_k),$$

d.h. disjunkte Zykel kommutieren.

Beweis. Dies ist offensichtlich aus der Definition eines Zykelns. \square

Satz 2.21. Jedes Element $\sigma \in S_n$ lässt sich als Produkt paarweise disjunkter Zykelns schreiben. Eine solche Zerlegung ist bis auf die Reihenfolge der Faktoren eindeutig.

Beweis. Sei $\sigma \in S_n$ ein beliebiges Element. Wir betrachten die Menge der Fixpunkte von σ

$$\text{Fix}(\sigma) := \{i \in \{1, \dots, n\} \mid \sigma(i) = i\},$$

also die Menge der Elemente, die unter σ unverändert bleiben.

Falls $\text{Fix}(\sigma) = \{1, \dots, n\}$ (also falls jedes Element ein Fixpunkt von σ ist), dann ist $\sigma = \text{id}$. In diesem Fall ist σ ein Produkt disjunkter Zykelns, nämlich das leere Produkt.

Falls es einen Nicht-Fixpunkt $i \in \{1, \dots, n\} \setminus \text{Fix}(\sigma)$ gibt, so betrachte die Elemente, auf die i bei sukzessiver Anwendung von σ abgebildet wird:

$$i, \sigma(i), \sigma^2(i), \sigma^3(i), \dots$$

Wir schreiben diese Kette bis zu dem Punkt auf, an dem sich zum ersten Mal eine Zahl wiederholen würde (diese nicht eingeschlossen). Es ist klar, dass das nach

Kapitel 2 Gruppentheorie

endlich vielen Schritten passieren muss, denn wir haben ja nur n verschiedene Zahlen zur Auswahl. Wir erhalten also paarweise verschiedene Elemente

$$i, \sigma(i), \sigma^2(i), \dots, \sigma^\ell(i).$$

Die Zahl $\sigma^{\ell+1}(i)$ kommt dann also unter diesen Elementen bereits vor. Wir wissen auch, welche es ist:

Behauptung: $\sigma^{\ell+1}(i) = i$.

Wäre $\sigma^{\ell+1}(i) = \sigma^j(i)$ für ein $j \in \{1, \dots, \ell\}$, dann können wir σ^{-1} auf diese Gleichung anwenden (denn σ ist bijektiv) und erhalten $\sigma^\ell(i) = \sigma^{j-1}(i)$. Es ist aber $j-1 \in \{0, \dots, \ell-1\}$ und somit $\sigma^{j-1}(i) \in \{i, \sigma(i), \dots, \sigma^{\ell-1}(i)\}$. Dann hätte es also in obiger Kette von Elementen bereits vorher eine Wiederholung gegeben. Widerspruch.

Wir definieren nun den ℓ -Zykel

$$\eta_1 := (i \ \sigma(i) \ \sigma^2(i) \ \dots \ \sigma^\ell(i))$$

und wissen nach der eben bewiesenen Behauptung, dass dieser auf der Menge $\{i, \sigma(i), \sigma^2(i), \dots, \sigma^\ell(i)\}$ mit σ übereinstimmt. Wenn wir dessen Inverses also nun mit σ komponieren, erhalten wir neue Fixpunkte (denn η_1^{-1} macht auf der Menge $\{i, \sigma(i), \sigma^2(i), \dots, \sigma^\ell(i)\}$ rückgängig, was σ gemacht hat, und somit bleiben diese Elemente fix), d.h.

$$\text{Fix}(\eta_1^{-1} \circ \sigma) = \text{Fix}(\sigma) \sqcup \{i, \sigma(i), \sigma^2(i), \dots, \sigma^\ell(i)\}.$$

Die Permutation $\eta_1^{-1} \circ \sigma$ hat nun also mehr Fixpunkte als σ . Falls es immer noch Nicht-Fixpunkte gibt, wiederholen wir dieses Verfahren so lange, bis wir eine Permutation $\eta_m^{-1} \circ \dots \circ \eta_1^{-1} \circ \sigma$ erhalten, für die jedes Element in $\{1, \dots, n\}$ ein Fixpunkt ist. (Dieses Verfahren terminiert, denn es gibt nur endlich viele mögliche Fixpunkte, nämlich die Elemente in $\{1, \dots, n\}$, und in jedem Schritt wird die Zahl der Fixpunkte echt größer.)

Es gilt dann

$$\eta_m^{-1} \circ \dots \circ \eta_1^{-1} \circ \sigma = \text{id}$$

und dies impliziert

$$\sigma = \eta_1 \circ \dots \circ \eta_m.$$

Nach obiger Konstruktion sind die Zyklen η_1, \dots, η_m paarweise disjunkt, denn der neu konstruierte Zykel enthält immer nur Elemente, die noch keine Fixpunkte waren, also noch in keinem vorher konstruierten Zykel enthalten waren.

Nun noch zur Eindeutigkeit (bis auf Reihenfolge) der Zyklen η_1, \dots, η_m : Sei i ein Nicht-Fixpunkt von σ . Dann kommt i in genau einem Zykel η_j vor. (Würde i in keinem der Zyklen vorkommen, wäre es ein Fixpunkt, und da die Zyklen disjunkt sind, kann i nicht in mehreren vorkommen.) Dann muss aber dieser Zykel (damit i

und alle seine sukzessiven Bilder auf die passenden Elemente abgebildet werden) zwingend von der Form $(i \ \sigma(i) \ \sigma^2(i) \ \dots \ \sigma^l(i))$ sein. Also sind die oben konstruierten Zykeln die einzig möglichen. \square

Korollar 2.22. *Jedes Element $\sigma \in S_n$ lässt sich als Produkt von Transpositionen schreiben. Diese können sogar so gewählt werden, dass sie von der Form $(a \ a + 1)$ sind, also zwei benachbarte Zahlen vertauschen.*

Beweis. Nach Satz 2.21 lässt sich σ schreiben als Produkt von Zykeln. Nun überlegt man sich leicht, dass man einen k -Zykel $(a_1 \ a_2 \ \dots \ a_k)$ schreiben kann als

$$(a_1 \ a_2 \ \dots \ a_k) = (a_1 \ a_2) \circ (a_2 \ a_3) \circ (a_3 \ a_4) \circ \dots \circ (a_{k-1} \ a_k).$$

Somit hat σ auch eine Darstellung als Produkt von Transpositionen.

In dieser Zerlegung können noch beliebige Transpositionen vorkommen. Man überlegt sich aber leicht, dass sich eine Transposition der Form $(a \ a + r)$ schreiben lässt als

$$(a \ a + r) = (a + r - 1 \ a + r) \circ \dots \circ (a + 2 \ a + 3) \circ (a + 1 \ a + 2) \circ (a \ a + 1) \circ (a + 1 \ a + 2) \circ (a + 2 \ a + 3) \circ \dots \circ (a + r - 1 \ a + r),$$

also als Produkt von $2r + 1$ Transpositionen, die zwei benachbarte Zahlen vertauschen. \square

Man beachte, dass die Transpositionen in der Aussage von Korollar 2.22, ganz im Gegensatz zu den Zykeln aus Satz 2.21, weder paarweise disjunkt noch eindeutig bestimmt sein müssen!

Zuletzt wollen wir noch kurz eine wichtige Kennzahl einer Permutation erwähnen.

Definition 2.23. Für eine Permutation $\sigma \in S_n$ betrachte die natürliche Zahl

$$\alpha(\sigma) := \#\{(i, j) \in \{1, \dots, n\} \times \{1, \dots, n\} \mid i < j, \sigma(i) > \sigma(j)\}$$

(die Anzahl der *Fehlstände*, also der Paare, deren Reihenfolge durch σ umgekehrt wird). Dann heißt die Zahl

$$\text{sgn}(\sigma) := (-1)^{\alpha(\sigma)}$$

das *Vorzeichen* (oder *Signum*) von σ .

Lemma 2.24. *Die Abbildung*

$$\text{sgn}: S_n \rightarrow \{1, -1\}$$

ist ein Gruppenhomomorphismus (wobei die Verknüpfung auf der rechten Seite die Multiplikation ist).

Kapitel 2 Gruppentheorie

Beweis. Sei $\tau = (a \ a + 1) \in S_n$ eine Transposition, die zwei benachbarte Zahlen vertauscht. Dann ist $\alpha(\tau) = 1$, also $\text{sgn}(\tau) = -1$. Ist nun $\sigma \in S_n$ eine beliebige Permutation, so überlegt man sich leicht, dass $\alpha(\sigma \circ \tau) = \alpha(\sigma) \pm 1$, denn entweder wird genau ein Fehlstand behoben oder genau ein neuer erzeugt. Somit ist also

$$\text{sgn}(\sigma \circ \tau) = (-1)^{\alpha(\sigma) \pm 1} = (-1)^{\alpha(\sigma)} \cdot (-1) = \text{sgn}(\sigma) \cdot \text{sgn}(\tau).$$

Nun ist nach Korollar 2.22 jedes $\sigma \in S_n$ ein Produkt solcher Transpositionen, welche jeweils zwei benachbarte Zahlen vertauschen. Schreiben wir also $\sigma = \tau_1 \circ \dots \circ \tau_k$, so gilt

$$\text{sgn}(\sigma) = \text{sgn}(\tau_1) \cdot \dots \cdot \text{sgn}(\tau_k) = (-1)^k.$$

Seien nun $\sigma_1, \sigma_2 \in S_n$ mit Darstellungen $\sigma_1 = \tau_1 \circ \dots \circ \tau_k$ und $\sigma_2 = \tau'_1 \circ \dots \circ \tau'_\ell$, dann gilt $\text{sgn}(\sigma_1) = (-1)^k$ und $\text{sgn}(\sigma_2) = (-1)^\ell$. Wegen $\sigma_1 \circ \sigma_2 = \tau_1 \circ \dots \circ \tau_k \circ \tau'_1 \circ \dots \circ \tau'_\ell$ ist analog $\text{sgn}(\sigma_1 \circ \sigma_2) = (-1)^{k+\ell}$ und somit gilt

$$\text{sgn}(\sigma_1 \circ \sigma_2) = (-1)^{k+\ell} = (-1)^k \cdot (-1)^\ell = \text{sgn}(\sigma_1) \cdot \text{sgn}(\sigma_2).$$

Daher definiert die Abbildung sgn einen Gruppenhomomorphismus. \square

Definition 2.25. Die *alternierende Gruppe* $A_n \subseteq S_n$ ist definiert als

$$A_n := \ker(\text{sgn}) = \{\sigma \in S_n \mid \text{sgn}(\sigma) = 1\} \subseteq S_n.$$

2.3 Normalteiler und Quotientengruppen

Erinnern wir uns zunächst an das Konzept der *Äquivalenzrelation*:

Definition 2.26. Sei M eine Menge. Eine *Relation* auf M ist eine Teilmenge $R \subseteq M \times M$. Falls $(x, y) \in R$, so schreibt man $x \sim y$.

Eine *Äquivalenzrelation* auf M ist eine Relation auf M , sodass die folgenden Eigenschaften erfüllt sind:

- (1) $\forall x \in M : x \sim x$, (Reflexivität)
- (2) $\forall x, y \in M : (x \sim y \Rightarrow y \sim x)$, (Symmetrie)
- (3) $\forall x, y, z \in M : ((x \sim y \wedge y \sim z) \Rightarrow x \sim z)$. (Transitivität)

Ist $x \in M$, dann heißt die Menge

$$[x] := \{y \in M \mid y \sim x\} \subseteq M$$

die *Äquivalenzklasse* von x . Jedes Element $y \in [x]$ nennen wir *Repräsentant* der Äquivalenzklasse.

Die Menge aller Äquivalenzklassen bezeichnen wir mit

$$M/\sim := \{[x] \mid x \in M\}.$$

Die Abbildung

$$\pi: M \rightarrow M/\sim, \quad x \mapsto [x]$$

heißt *kanonische Projektion*.

Eine Teilmenge $S \subseteq M$ heißt *Repräsentantensystem*, falls die Einschränkung

$$\pi|_S: S \rightarrow M/\sim, \quad s \mapsto [s]$$

bijektiv ist, also falls S aus jeder Äquivalenzklasse genau einen Repräsentanten enthält.

Wir erinnern uns auch an die folgenden einfachen Aussagen über Äquivalenzrelationen.

Lemma 2.27. *Sei \sim eine Äquivalenzrelation auf einer Menge M . Dann gilt:*

- (i) Für $x, y \in M$ gilt entweder $[x] = [y]$ oder $[x] \cap [y] = \emptyset$.
- (ii) Ist S ein Repräsentantensystem, dann ist

$$M = \bigsqcup_{s \in S} [s].$$

Beweis. (i) Falls $[x] \cap [y] \neq \emptyset$, dann gibt es ein $m \in [x] \cap [y]$, d.h. $m \sim x$ und $m \sim y$. Aus der Transitivität folgt dann $x \sim y$ und somit (wieder mit Transitivität) gilt für jedes Element $z \in M$ mit $z \sim x$ auch $z \sim y$ und umgekehrt, also $[x] = [y]$.

- (ii) Es ist klar, dass $\bigcup_{s \in S} [s] \subseteq M$. Für die umgekehrte Inklusion sei $m \in M$. Dann gibt es ein $s \in S$ mit $[m] = [s]$ und somit $m \in [s]$, also folgt $M \subseteq \bigcup_{s \in S} [s]$.

Die Vereinigung ist disjunkt, denn gäbe es $s_1, s_2 \in S$ mit $[s_1] \cap [s_2] \neq \emptyset$, dann wäre nach (i) bereits $[s_1] = [s_2]$. Das ist aber nicht möglich, da S ein Repräsentantensystem ist.

□

Lemma-Definition 2.28. Sei G eine Gruppe und $H \subset G$ eine Untergruppe. Dann definiert

$$g \sim g' :\Leftrightarrow g^{-1}g' \in H$$

eine Äquivalenzrelation auf G .

Für ein $g \in G$ ist die zugehörige Äquivalenzklasse gegeben durch

$$[g] = gH := \{gh \mid h \in H\}.$$

Die Menge gH heißt auch *Linksnebenklasse* von g bezüglich H .

Die Menge der Äquivalenzklassen dieser Äquivalenzrelation notieren wir als

$$G/H := G/\sim = \{gH \mid g \in G\}$$

und nennen sie den *Quotienten* von G modulo H .

Kapitel 2 Gruppentheorie

Beweis. Wir prüfen zunächst die Axiome einer Äquivalenzrelation nach. Seien $g, g', g'' \in G$.

- (1) $g \sim g$, weil $g^{-1}g = e \in H$ (H ist eine Untergruppe).
- (2) Falls $g \sim g'$, also $g^{-1}g' \in H$, dann ist auch $(g^{-1}g')^{-1} = g'^{-1}g \in H$ (nach Definition einer Untergruppe und Lemma 2.4) und daher $g' \sim g$.
- (3) Falls $g \sim g'$ (d.h. $g^{-1}g' \in H$) und $g' \sim g''$ (d.h. $g'^{-1}g'' \in H$), so folgt $(g^{-1}g')(g'^{-1}g'') \in H$, da H eine Untergruppe ist. Wegen

$$(g^{-1}g')(g'^{-1}g'') = g^{-1} \underbrace{(g'g'^{-1})}_{=e} g'' = g^{-1}g''$$

bedeutet das aber genau $g \sim g''$.

Um die Äquivalenzklassen zu bestimmen, bemerken wir Folgendes: Ein Element g' ist (nach Definition) genau dann zu g äquivalent, wenn $g^{-1}g' \in H$. Das ist gleichbedeutend damit, dass es ein Element $h \in H$ gibt mit $g^{-1}g' = h$, d.h. $g' = gh$ für ein $h \in H$. Die Äquivalenzklasse von $[g]$ ist also genau die Menge der Elemente, die sich als gh schreiben lassen für ein $h \in H$, also die Linksnebenklasse gH . \square

Bemerkung 2.29. Man könnte die Konstruktion aus Lemma-Definition 2.28 auch „andersherum“ machen: Wenn man die Äquivalenzrelation definiert als

$$g \sim g' :\Leftrightarrow g'g^{-1} \in H,$$

dann erhält man als Äquivalenzklassen die *Rechtsnebenklassen* $Hg := \{hg \mid h \in H\}$. Die Menge der Äquivalenzklassen G/\sim ist also dann im Allgemeinen nicht dieselbe wie in Lemma-Definition 2.28 (man bezeichnet sie mit $H \setminus G$). Wir werden aber sehen, dass Links- und Rechtsnebenklassen in den Fällen, wo H ein sogenannter *Normalteiler* ist, zusammenfallen (s. Bemerkung 2.36).

Im folgenden Lemma sammeln wir einige wichtige Eigenschaften von Linksnebenklassen. Ein analoges Resultat gilt für Rechtsnebenklassen.

Lemma 2.30. *Sei G eine Gruppe und $H \subseteq G$ eine Untergruppe.*

- (i) *Für beliebige $g_1, g_2 \in G$ gibt es eine Bijektion zwischen g_1H und g_2H . Insbesondere haben alle Linksnebenklassen gleich viele Elemente, falls sie endlich sind.*
- (ii) *Für $g_1, g_2 \in G$ gilt entweder $g_1H = g_2H$ oder $g_1H \cap g_2H = \emptyset$.*
- (iii) *Ist $S \subseteq G$ ein Repräsentantensystem, dann gilt*

$$G = \bigsqcup_{g \in S} gH,$$

d.h. die Gruppe G ist die disjunkte Vereinigung aller Linksnebenklassen.

Beweis. Da wir in Lemma-Definition 2.28 gezeigt haben, dass die Linksnebenklassen die Äquivalenzklassen einer passenden Äquivalenzrelation sind, folgen die Aussagen (ii) und (iii) bereits aus den allgemeinen Eigenschaften von Äquivalenzklassen (Lemma 2.27).

Es bleibt also noch (i) zu zeigen. Seien $g_1, g_2 \in G$ gegeben. Betrachte die Abbildung

$$g_1H \rightarrow g_2H, \quad x \mapsto g_2g_1^{-1}x.$$

Diese ist wohldefiniert, denn sei $x \in g_1H$, d.h. $x = g_1h$ für ein $h \in H$, dann ist $g_2g_1^{-1}x = g_2g_1^{-1}g_1h = g_2h \in g_2H$. Außerdem ist sie bijektiv, denn es gibt eine offensichtliche Umkehrabbildung. \square

Bemerkung 2.31. Während die Eigenschaften (ii) und (iii) aus Lemma 2.30 allgemeingültige Eigenschaften von Äquivalenzklassen beschreiben, ist (i) nicht für jede Äquivalenzrelation wahr: Im Allgemeinen sind Äquivalenzklassen nicht „gleich groß“, dies ist also eine Besonderheit der Äquivalenzrelation, die auf einer Gruppe bezüglich einer Untergruppe gegeben ist.

Man beachte, dass G/H im Allgemeinen nur eine *Menge* ist und selbst a priori keine Gruppenstruktur besitzt. Natürlich möchte man gerne eine (möglichst natürliche) Gruppenstruktur auf G/H definieren. Dazu fällt uns Folgendes ein: Das neutrale Element sollte wohl die Äquivalenzklasse $[e]$ des neutralen Elements von G sein. Die Verknüpfung möchten wir am besten folgendermaßen definieren:

$$G/H \times G/H \rightarrow G/H, ([g_1], [g_2]) \mapsto [g_1] \cdot [g_2] := [g_1g_2].$$

Wir würden also gerne die Verknüpfung zweier Äquivalenzklassen einfach dadurch definieren, indem wir ihre Repräsentanten in der Gruppe G miteinander verknüpfen.

Es stellt sich heraus, dass diese Abbildung nicht immer wohldefiniert ist!

Beispiel 2.32. Sei $G = \text{GL}_2(\mathbb{Q})$ die Gruppe der invertierbaren (2×2) -Matrizen mit rationalen Einträgen und

$$H = \left\{ \begin{pmatrix} a & 0 \\ 0 & b \end{pmatrix} \mid ab \neq 0 \right\} \subset G$$

die Untergruppe der invertierbaren Diagonalmatrizen. Dann betrachten wir die Äquivalenzklasse der Matrix $A = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$ in G/H . Dann ergibt unsere „gewünschte“ Verknüpfungsregel zum einen

$$[A] \cdot [A] = [A \cdot A] = \left[\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \cdot \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \right] = \left[\begin{pmatrix} 1 & 2 \\ 0 & 1 \end{pmatrix} \right].$$

Kapitel 2 Gruppentheorie

Zum anderen liegt aber A in derselben Äquivalenzklasse wie die Matrix $A' = \begin{pmatrix} 1 & 2 \\ 0 & 2 \end{pmatrix}$, denn

$$A^{-1} \cdot A' = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}^{-1} \cdot \begin{pmatrix} 1 & 2 \\ 0 & 2 \end{pmatrix} = \begin{pmatrix} 1 & -1 \\ 0 & 1 \end{pmatrix} \cdot \begin{pmatrix} 1 & 2 \\ 0 & 2 \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 2 \end{pmatrix} \in H.$$

Wenn wir also eine der Matrizen A durch A' ersetzen und das Produkt wieder mithilfe unserer "gewünschten" Regel berechnen, erhalten wir

$$[A'] \cdot [A] = [A' \cdot A] = \left[\begin{pmatrix} 1 & 2 \\ 0 & 2 \end{pmatrix} \cdot \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \right] = \left[\begin{pmatrix} 1 & 3 \\ 0 & 2 \end{pmatrix} \right].$$

Wäre die Verknüpfung jetzt wohldefiniert, dann müsste gelten $[A] \cdot [A] = [A'] \cdot [A]$, da ja $[A] = [A']$ ist. Anders gesagt müssten die beiden Matrizen $\begin{pmatrix} 1 & 2 \\ 0 & 1 \end{pmatrix}$ und $\begin{pmatrix} 1 & 3 \\ 0 & 2 \end{pmatrix}$ also in derselben Äquivalenzklasse liegen. Dies ist aber nicht der Fall, denn

$$\begin{pmatrix} 1 & 2 \\ 0 & 1 \end{pmatrix}^{-1} \cdot \begin{pmatrix} 1 & 3 \\ 0 & 2 \end{pmatrix} = \begin{pmatrix} 1 & -2 \\ 0 & 1 \end{pmatrix} \cdot \begin{pmatrix} 1 & 3 \\ 0 & 2 \end{pmatrix} = \begin{pmatrix} 1 & -1 \\ 0 & 2 \end{pmatrix} \notin H.$$

Die vermeintlich kanonische Gruppenverknüpfung ist also in diesem Fall nicht wohldefiniert und macht G/H nicht zu einer Gruppe.

Man kann also G/H nicht im Allgemeinen auf natürliche Weise zu einer Gruppe machen. Wenn man aber noch eine zusätzliche Bedingung an die Untergruppe H stellt, dann ist die obige Verknüpfung wohldefiniert.

Definition 2.33. Sei G eine Gruppe. Eine Untergruppe $H \subseteq G$ heißt *Normalteiler*, falls gilt:

$$\forall g \in G \forall h \in H : ghg^{-1} \in H.$$

Ist H ein Normalteiler in G , dann schreiben wir $H \triangleleft G$.

Satz 2.34. Sei G eine Gruppe mit neutralem Element e und $H \triangleleft G$ ein Normalteiler. Dann ist die Menge G/H zusammen mit der Verknüpfung

$$\cdot : G/H \times G/H \rightarrow G/H, ([g_1], [g_2]) \mapsto [g_1g_2]$$

eine Gruppe mit neutralem Element $[e]$. Wir nennen G/H die **Quotientengruppe** (oder auch **Faktorgruppe**) von G modulo H .

Beweis. Zu zeigen ist die Wohldefiniertheit der Verknüpfung. Seien also $g_1, g_2 \in G$ zwei beliebige Elemente und $g'_1, g'_2 \in G$ zwei Elemente mit $[g_1] = [g'_1]$ und $[g_2] = [g'_2]$. Dann ist zu zeigen, dass gilt:

$$[g_1g_2] = [g'_1g'_2].$$

Nach Annahme ist $g_1^{-1}g'_1 \in H$ und ebenso $g_2^{-1}g_2 \in H$. Wir schreiben kurz $h := g_1^{-1}g'_1$. Außerdem ist H ein Normalteiler, daher gilt $g_2^{-1}hg'_2 \in H$. (Dazu wählt man in Definition 2.33 das Element g als g_2^{-1} .) Wir nennen dieses Element $h' := g_2^{-1}hg'_2$. Dann gilt

$$(g_1g_2)^{-1}(g'_1g'_2) = g_2^{-1} \underbrace{g_1^{-1}g'_1}_{=h} g'_2 = g_2^{-1} \underbrace{hg'_2}_{=g'_2h'} = \underbrace{g_2^{-1}g'_2}_{\in H} h' \in H.$$

Dies bedeutet, dass $g_1g_2 \sim g'_1g'_2$ und somit ist die Wohldefiniertheit gezeigt. \square

Ein wichtiges Beispiel dafür, wo Normalteiler ganz natürlich auftauchen, beschreibt das folgende Lemma.

Lemma 2.35. *Sei $\varphi: G \rightarrow G'$ ein Gruppenhomomorphismus, dann ist $\ker(\varphi)$ ein Normalteiler in G .*

Beweis. Wir bezeichnen mit e' das neutrale Element in G' . Sei $g \in G$ und $h \in \ker(\varphi)$ (also $\varphi(h) = e'$). Dann müssen wir zeigen, dass $ghg^{-1} \in \ker(\varphi)$. Das folgt einfach aus der folgenden Rechnung:

$$\varphi(ghg^{-1}) = \varphi(g) \underbrace{\varphi(h)}_{=e'} \varphi(g^{-1}) = \varphi(g)\varphi(g)^{-1} = e'.$$

\square

Kerne von Gruppenhomomorphismen sind also immer Normalteiler. Ist $\varphi: G \rightarrow G'$ ein Gruppenhomomorphismus, dann macht es also immer Sinn, über die Gruppe $G/\ker(\varphi)$ zu sprechen.

Umgekehrt ist jeder Normalteiler auch der Kern eines Gruppenhomomorphismus, wie man sich leicht überlegt: Sei G eine Gruppe und $H \triangleleft G$ ein Normalteiler. Dann können wir die Abbildung

$$\pi: G \rightarrow G/H, \quad g \mapsto [g]$$

betrachten (die kanonische Projektion).

Man überlegt sich leicht, dass π ein Gruppenhomomorphismus ist, dass π surjektiv ist und dass $\ker(\pi) = H$ gilt.

Bemerkung 2.36. Wir erwähnen noch zwei einfache Beobachtungen zum Begriff des Normalteilers:

- Ist $H \triangleleft G$ ein Normalteiler, so ist für jedes $g \in G$ die Linksnebenklasse gH identisch mit der Rechtsnebenklasse

$$Hg := \{hg \mid h \in H\} \subseteq G.$$

Dies sieht man wie folgt: Sei $x \in gH$, d.h. $x = gh$ für ein $h \in H$. Da H ein Normalteiler ist, ist $ghg^{-1} \in H$, es gibt also ein $h' \in H$ mit $ghg^{-1} = h'$ bzw. $gh = h'g \in Hg$. Dies zeigt $gH \subseteq Hg$. Die umgekehrte Inklusion beweist man analog.

Kapitel 2 Gruppentheorie

- Ist G eine abelsche Gruppe, dann ist jede Untergruppe $H \subseteq G$ ein Normalteiler.

Beispiel 2.37. Ein wichtiges Beispiel für eine Quotientengruppe kennen wir bereits: Sei $n \in \mathbb{N}$, dann ist

$$n\mathbb{Z} := \{x \cdot n \mid x \in \mathbb{Z}\} = \{\dots, -3n, -2n, -n, 0, n, 2n, 3n, \dots\} \triangleleft \mathbb{Z}$$

ein Normalteiler. (Man sieht leicht, dass $n\mathbb{Z} \subseteq \mathbb{Z}$ eine Untergruppe ist. Da \mathbb{Z} eine abelsche Gruppe ist, ist jede Untergruppe dann automatisch ein Normalteiler, wie in Bemerkung 2.36 beobachtet.)

Dann ist $\mathbb{Z}/n\mathbb{Z}$ mit der von \mathbb{Z} induzierten Addition also eine Gruppe, deren Elemente von der Form

$$[a] = a + n\mathbb{Z} = \{a + x \cdot n \mid x \in \mathbb{Z}\} = \{\dots, a - 3n, a - 2n, a - n, a, a + n, a + 2n, a + 3n, \dots\}$$

für $a \in \mathbb{Z}$ sind. (Dies sind einfach die Nebenklassen von $n\mathbb{Z}$ in \mathbb{Z} , die hier aber additiv als $a + n\mathbb{Z}$ geschrieben werden.)

Rechnen wir in $\mathbb{Z}/n\mathbb{Z}$, so schreiben wir oft auch $a \equiv b \pmod{n}$ für $[a] = [b]$. Dies bedeutet, dass a und b äquivalent modulo n sind, dass sie also bei Division durch n denselben Rest haben.

2.4 Der Homomorphiesatz

Der Homomorphiesatz (hier für Gruppen, aber es gibt analog Versionen z.B. für Ringe und Vektorräume) ermöglicht es uns, das Konzept des Quotienten zu benutzen, um aus Homomorphismen Isomorphismen zu konstruieren. Er wird uns an verschiedenen Stellen nützlich sein.

Satz 2.38 (Homomorphiesatz). Sei $\varphi: G \rightarrow G'$ ein Gruppenhomomorphismus. Dann definiert

$$\bar{\varphi}: G/\ker(\varphi) \rightarrow G', \quad [g] \mapsto \varphi(g)$$

einen injektiven Gruppenhomomorphismus.

Beweis. Wir schreiben e für das neutrale Element in G und e' für das neutrale Element in G' .

Zunächst zeigen wir, dass obige Vorschrift eine wohldefinierte Abbildung beschreibt: Seien $g_1, g_2 \in G$ mit $[g_1] = [g_2]$. Dies bedeutet, dass wir schreiben können $g_2 = g_1 h$ für ein $h \in \ker(\varphi)$. Also gilt

$$\varphi(g_2) = \varphi(g_1 h) = \varphi(g_1) \underbrace{\varphi(h)}_{=e'} = \varphi(g_1).$$

Damit ist $\bar{\varphi}$ wohldefiniert.

Die Tatsache, dass $\bar{\varphi}$ ein Gruppenhomomorphismus ist, folgt direkt aus der Tatsache, dass φ ein Gruppenhomomorphismus ist und die Gruppenstruktur auf $G/\ker(\varphi)$ durch die von G induziert ist.

Es bleibt noch zu zeigen, dass $\bar{\varphi}$ injektiv ist, also dass $\ker(\bar{\varphi}) = \{[e]\}$: Sei also $[g] \in \ker(\bar{\varphi})$ beliebig, d.h. $\bar{\varphi}([g]) = e'$. Nach Definition ist aber $\bar{\varphi}([g]) = \varphi(g)$, also folgt $\varphi(g) = e'$ und somit $g \in \ker(\varphi)$. Dies bedeutet aber $[g] = [e]$. \square

Korollar 2.39. *Ist $\varphi: G \rightarrow G'$ ein surjektiver Gruppenhomomorphismus, dann ist*

$$\bar{\varphi}: G/\ker(\varphi) \rightarrow G', \quad [g] \mapsto \varphi(g)$$

ein Gruppenisomorphismus.

Für einen beliebigen Gruppenhomomorphismus $\varphi: G \rightarrow G'$ erhält man daher einen Gruppenisomorphismus $G/\ker(\varphi) \cong \text{im}(\varphi)$.

Beweis. Ist φ surjektiv, dann überträgt sich diese Eigenschaft auf $\bar{\varphi}$, wie man folgendermaßen sieht: Sei $g' \in G'$ beliebig. Da φ surjektiv ist, gibt es ein $g \in G$ mit $\varphi(g) = g'$. Daher gilt $\bar{\varphi}([g]) = g'$, also haben wir ein Element $[g] \in G/\ker(\varphi)$ gefunden, welches auf g' abgebildet wird.

Somit ist $\bar{\varphi}$ sowohl injektiv (wie in Satz 2.38 gezeigt) als auch surjektiv und daher ein Gruppenisomorphismus.

Falls φ ein beliebiger Gruppenhomomorphismus ist, können wir seinen Wertebereich auf sein Bild $\text{im}(\varphi)$ einschränken, d.h. wir betrachten den Gruppenhomomorphismus $G \rightarrow \text{im}(\varphi), g \mapsto \varphi(g)$. Wir nennen diesen Gruppenhomomorphismus ebenfalls φ , denn er ist durch dieselbe Abbildungsvorschrift wie φ gegeben und hat auch denselben Kern wie φ . Dieser ist nach Definition surjektiv und somit liefert der erste Teil des Korollars einen Isomorphismus $G/\ker(\varphi) \cong \text{im}(\varphi)$. \square

2.5 Gruppenwirkungen

Wie schon das Zitat am Anfang dieses Kapitels andeutet, kommen Gruppen oft im Zusammenhang mit Symmetrien vor. Genauer gesagt werden die Elemente einer Gruppe als Symmetrieoperationen aufgefasst, die auf einem Objekt (einer Menge, die selber keine Gruppe sein muss), *wirken* können.

Ein Beispiel haben wir bereits gesehen: die (passenderweise schon so bezeichnete) symmetrische Gruppe S_n . Elemente σ dieser Menge kann man als Abbildungen $\{1, \dots, n\} \rightarrow \{1, \dots, n\}$ verstehen, d.h. sie *operieren* auf der Menge $\{1, \dots, n\}$.

Wir führen dieses Konzept jetzt allgemeiner ein.

Definition 2.40. Sei G eine Gruppe mit neutralem Element e und X eine Menge. Eine Abbildung

$$\Phi: G \times X \rightarrow X$$

heißt **Gruppenwirkung** (oder **Gruppenoperation**), wenn die folgenden Eigenschaften erfüllt sind:

- (1) $\forall x \in X : \Phi(e, x) = x,$
- (2) $\forall g_1, g_2 \in G \forall x \in X : \Phi(g_1, \Phi(g_2, x)) = \Phi(g_1 g_2, x).$

Kapitel 2 Gruppentheorie

Bemerkung 2.41. Wir schreiben oft einfach gx oder $g \cdot x$ für $\Phi(g, x)$ und lesen „ g wird angewendet/wirkt/operiert auf x “. Die beiden Bedingungen in Definition 2.40 sind dann so zu lesen:

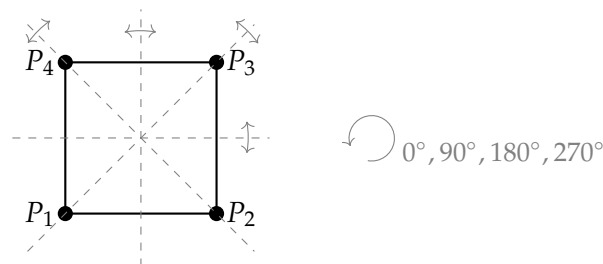
- (1) $ex = x$, d.h. wendet man das neutrale Element von G auf ein beliebiges $x \in X$ an, so bleibt x unverändert.
- (2) $g_1(g_2x) = (g_1g_2)x$, d.h. wendet man nacheinander zwei Gruppenelemente auf ein $x \in X$ an, so kann man sie auch zuerst in G verknüpfen und dann auf x anwenden und man erhält dasselbe Ergebnis.

Beispiel 2.42. Einige einfache Beispiele für Gruppenwirkungen sind die folgenden:

- Wie bereits erwähnt, wirkt die Gruppe S_n auf der Menge $\{1, \dots, n\}$.
- Die Gruppe $G = GL_n(\mathbb{R})$ der invertierbaren $(n \times n)$ -Matrizen wirkt auf \mathbb{R}^n durch Matrix-Vektor-Multiplikation.
- Die Gruppe D_4 ist die Symmetriegruppe des Quadrats. Ihre Elemente sind die Drehungen um 0° , 90° , 180° und 270° , die Spiegelungen an den beiden senkrecht auf den Seiten stehenden Symmetrieachsen sowie die Spiegelungen an den beiden Diagonalen.

Die Gruppe D_4 wirkt auf der Menge $\{P_1, P_2, P_3, P_4\}$ der Ecken des Quadrats.

Alternativ kann man D_4 auch als die Gruppe derjenigen orthogonalen (2×2) -Matrizen betrachten, die das Quadrat mit Mittelpunkt $(0, 0)$ auf sich selbst abbilden.



Ähnlich kann man auch die Symmetriegruppe D_n des regelmäßigen n -Ecks definieren.

- Jede Gruppe G wirkt auf sich selbst durch Konjugation:

$$G \times G \rightarrow G, \quad (g, x) \mapsto gxg^{-1}.$$

Man kann eine Gruppenwirkung auch etwas anders verstehen. Analog zur symmetrischen Gruppe S_n kann man zunächst den folgenden Begriff einführen.

Lemma-Definition 2.43. Sei X eine Menge. Dann ist die Menge

$$S(X) := \{\sigma: X \rightarrow X \mid \sigma \text{ ist bijektiv}\}$$

zusammen mit der Verknüpfung \circ von Abbildungen eine Gruppe, deren neutrales Element die Identitätsabbildung $\text{id}: X \rightarrow X$ ist.

Beweis. Der Beweis ist vollkommen analog zum Beweis von Lemma-Definition 2.16. \square

Es gilt also insbesondere $S_n = S(\{1, \dots, n\})$.

Lemma 2.44. Sei G eine Gruppe und X eine Menge. Eine Gruppenwirkung $\Phi: G \times X \rightarrow X$ induziert einen Gruppenhomomorphismus

$$\varphi: G \rightarrow S(X),$$

der ein Element $g \in G$ auf die Bijektion $\varphi_g: X \rightarrow X, x \mapsto gx = \Phi(g, x)$ abbildet.

Umgekehrt gilt: Ist $\varphi: G \rightarrow S(X)$ ein Gruppenhomomorphismus, dann induziert dieser eine Gruppenwirkung

$$\Phi: G \times X \rightarrow X$$

durch die Vorschrift $\Phi(g, x) := (\varphi(g))(x)$.

Beweis. Sei $\Phi: G \times X \rightarrow X$ eine Gruppenwirkung. Dann ist die Abbildung

$$\varphi: G \rightarrow S(X), \quad g \mapsto (\varphi_g: X \rightarrow X, x \mapsto gx)$$

ein Gruppenhomomorphismus:

Zunächst vergewissern wir uns, dass φ wohldefiniert ist, dass also für beliebiges $g \in G$ die Abbildung φ_g wirklich bijektiv ist. Dies ist der Fall, denn $\varphi_{g^{-1}}$ ist eine Umkehrabbildung, wie man leicht nachrechnet: Sei $x \in X$, dann gilt

$$(\varphi_{g^{-1}} \circ \varphi_g)(x) = \varphi_{g^{-1}}(\varphi_g(x)) = \varphi_{g^{-1}}(gx) = g^{-1}(gx) = (g^{-1}g)x = ex = x.$$

(Hier haben wir in der vierten und sechsten Gleichheit die Eigenschaften einer Gruppenwirkung verwendet.)

Nun prüfen wir noch die definierende Eigenschaft eines Gruppenhomomorphismus nach: Seien $g_1, g_2 \in G$, dann ist für jedes $x \in X$

$$\varphi_{g_1 g_2}(x) = (g_1 g_2)x = g_1(g_2 x) = g_1(\varphi_{g_2}(x)) = \varphi_{g_1}(\varphi_{g_2}(x))$$

(in der zweiten Gleichheit wurde verwendet, dass Φ eine Gruppenwirkung ist), also gilt $\varphi_{g_1 g_2} = \varphi_{g_1} \circ \varphi_{g_2}$ oder (anders geschrieben) $\varphi(g_1 g_2) = \varphi(g_1)\varphi(g_2)$.

Sei umgekehrt $\varphi: G \rightarrow S(X)$ ein Gruppenhomomorphismus, dann ist

$$\Phi: G \times X \rightarrow X, \quad (g, x) \mapsto gx := (\varphi(g))(x)$$

eine Gruppenwirkung, denn

Kapitel 2 Gruppentheorie

(1) Für $x \in X$ ist $\Phi(e, x) = (\varphi(e))(x) = \text{id}_X(x) = x$.

(Die Gleichheit $\varphi(e) = \text{id}_X$ gilt, weil nach Voraussetzung φ ein Gruppenhomomorphismus ist.)

(2) Für $g_1, g_2 \in G$ und $x \in X$ ist

$$\begin{aligned} g_1(g_2x) &= (\varphi(g_1))(g_2x) = (\varphi(g_1))((\varphi(g_2))(x)) \\ &= (\varphi(g_1) \circ \varphi(g_2))(x) = \varphi(g_1g_2)(x) \\ &= (g_1g_2)x. \end{aligned}$$

(Die vierte Gleichheit benutzt hier die Tatsache, dass φ ein Gruppenhomomorphismus ist.) \square

Definition 2.45. Sei $G \times X \rightarrow X$ eine Gruppenwirkung und sei $x \in X$. Dann heißt die Teilmenge

$$Gx := \{gx \mid g \in G\} \subseteq X$$

die *Bahn* (oder der *Orbit*) von x .

Außerdem nennen wir die Untergruppe

$$G_x := \{g \in G \mid gx = x\} \subseteq G$$

die *Standgruppe* (oder auch die *Isotropiegruppe* oder den *Stabilisator*) von x .

Bemerkung 2.46. Es ist leicht zu sehen, dass $G_x \subseteq G$ wirklich eine Untergruppe ist: Offensichtlich gilt $e \in G_x$ wegen $ex = x$. Außerdem gilt für zwei Elemente $g_1, g_2 \in G_x$ (d.h. $g_1x = x$ und $g_2x = x$) auch $(g_1g_2)x = g_1(g_2x) = g_1x = x$, also $g_1g_2 \in G_x$.

Eine Gruppenwirkung $G \times X \rightarrow X$ liefert auf natürliche Weise eine Äquivalenzrelation auf X , deren Äquivalenzklassen die Bahnen sind.

Lemma-Definition 2.47. Sei $G \times X \rightarrow X$ eine Gruppenwirkung. Dann definiert

$$x \sim y :\Leftrightarrow \exists g \in G : y = gx$$

eine Äquivalenzrelation auf X . Für jedes $x \in X$ ist dann die zugehörige Äquivalenzklasse die Bahn von x , also $[x] = Gx$.

Beweis. Obige Vorschrift definiert eine Äquivalenzrelation auf X :

(1) Sei $x \in X$, dann ist $x = ex$, also $x \sim x$.

(2) Seien $x, y \in X$ mit $x \sim y$, d.h. $y = gx$ für ein $g \in G$. Dann ist

$$g^{-1}y = g^{-1}(gx) = (g^{-1}g)x = ex = x,$$

also $y \sim x$.

- (3) Seien $x, y, z \in X$ mit $x \sim y$ und $y \sim z$, d.h. $y = gx$ und $z = g'y$ für bestimmte $g, g' \in G$. Dann ist $z = g'y = g'(gx) = (gg')x$, also $x \sim z$.

Für $x \in X$ ist nach Definition

$$[x] = \{y \in X \mid x \sim y\} = \{y \in X \mid \exists g \in G : y = gx\} = Gx.$$

□

Beispiel 2.48. Man kann sich überlegen, dass die ersten drei Gruppenwirkungen aus Beispiel 2.42 jeweils nur eine einzige Bahn haben (und diese ist folglich gleich der ganzen Menge X) – je zwei Elemente aus der Menge X werden durch Anwendung mindestens eines Gruppenelements aufeinander abgebildet. Gibt es nur eine einzige Bahn, so nennen wir die Gruppenwirkung *transitiv*.

Das letzte Beispiel ist etwas interessanter. Betrachten wir es für $G = \text{GL}_n(\mathbb{R})$, also die Gruppenwirkung

$$\text{GL}_n(\mathbb{R}) \times \text{GL}_n(\mathbb{R}) \rightarrow \text{GL}_n(\mathbb{R}), \quad (S, A) \mapsto SAS^{-1}.$$

Ist A eine Matrix, so besteht die Bahn von A aus allen zu A ähnlichen Matrizen.

Satz 2.49 (Bahnensatz). *Sei $G \times X \rightarrow X$ eine Gruppenoperation und $X \neq \emptyset$. Dann haben wir für jedes $x \in X$ eine bijektive Abbildung*

$$G/G_x \rightarrow Gx, \quad [g] \mapsto gx.$$

Beweis. Sei $x \in X$. Zunächst ist obige Abbildung wohldefiniert, denn seien $g, g' \in G$ mit $[g] = [g']$, d.h. $g^{-1}g' \in G_x$, dann gibt es also ein $h \in G_x$ (d.h. $hx = x$) mit $g' = gh$. Folglich ist

$$g'x = (gh)x = g \underbrace{(hx)}_{=x} = gx.$$

Die Abbildung ist offensichtlich surjektiv nach Definition von Gx . Sie ist auch injektiv, denn seien $g_1, g_2 \in G$ mit $g_1x = g_2x$, dann gilt

$$(g_1^{-1}g_2)x = g_1^{-1}(g_2x) = g_1^{-1}(g_1x) = (g_1^{-1}g_1)x = ex = x,$$

also $g_1^{-1}g_2 \in G_x$ und somit $[g_1] = [g_2]$ in G/G_x . □

Falls die operierende Gruppe und die Menge, auf der sie operiert, endlich sind, erhalten wir daraus auch einen nützlichen Zusammenhang zwischen der Größe der Bahn und dem Index der Standgruppe, die sogenannte *Bahnengleichung*. Diese wird im nächsten Abschnitt bewiesen (Korollar 2.56).

2.6 Endliche Gruppen

In dem Fall, dass die Gruppe, mit der wir arbeiten, endlich viele Elemente hat, können wir einige nützliche Formeln für die Anzahl der Elemente im Zusammenhang mit Untergruppen und Quotienten angeben.

Definition 2.50. Sei G eine endliche Gruppe (also eine Gruppe mit endlich vielen Elementen). Dann bezeichnen wir mit $\#G$ oder $|G|$ die Anzahl der Elemente in G und nennen sie die *Ordnung* von G .

Für ein Element $g \in G$ heißt

$$\text{ord}(g) := \#\langle g \rangle$$

die *Ordnung* von g .

Ist $H \subseteq G$ eine Untergruppe, dann nennen wir die Anzahl der Nebenklassen

$$(G : H) := \#(G/H)$$

den *Index* von H in G .

Die Ordnung eines Elements lässt sich auch anders charakterisieren.

Lemma 2.51. Sei G eine endliche Gruppe und $g \in G$. Dann ist

$$\text{ord}(g) = \min\{\ell \in \mathbb{N} \mid g^\ell = e\}.$$

Beweis. Wir überlegen uns zuerst, dass es ein $k \in \mathbb{N}$ gibt mit $g^k = e$, dass also die Menge auf der rechten Seite nicht leer ist: Da G endlich ist, ist auch die Untergruppe

$$\langle g \rangle = \{g^k \mid k \in \mathbb{Z}\} \subseteq G$$

endlich. Es gibt also $k, k' \in \mathbb{N}$, $k \neq k'$ mit $g^k = g^{k'}$. Dann ist aber $g^{k-k'} = e$ und daher $\ell = |k - k'|$ eine natürliche Zahl mit $g^\ell = e$. Sei nun $m := \min\{\ell \in \mathbb{N} \mid g^\ell = e\}$. (Das Minimum existiert, da die Menge nicht leer und als Teilmenge der natürlichen Zahlen nach unten beschränkt ist.)

Dann sind die Elemente $e = g^0, g = g^1, g^2, \dots, g^{m-1}$ paarweise verschieden, denn sonst gäbe es (mit demselben Argument wie oben) eine natürliche Zahl m' zwischen 1 und $m - 1$ mit $g^{m'} = e$, was unmöglich ist, denn m ist die kleinste solche natürliche Zahl.

Nun ist aber $g^m = e$, also sind alle g^k mit $k \geq m$ bereits in obiger Liste enthalten. Ebenso ist $g^{m-1} \cdot g = g^m = e$, also $g^{-1} = g^{m-1}$, also sind auch alle g^k mit $k < 0$ bereits in obiger Liste enthalten. Also ist $\langle g \rangle = \{e, g, g^2, \dots, g^{m-1}\}$ und somit

$$\text{ord}(g) = \#\langle g \rangle = m.$$

□

Wir ziehen zunächst zwei kurze Schlussfolgerungen aus dem zuvor allgemein Gezeigten.

Lemma 2.52. *Sei G eine endliche Gruppe und $H \subseteq G$ eine Untergruppe. Sei weiter S ein Repräsentantensystem für G/H (d.h. für die Äquivalenzrelation aus Lemma-Definition 2.28). Dann gilt:*

- (i) $(G : H) = \#S$,
- (ii) $\forall g \in G : \#(gH) = \#H$.

Beweis. (i) Nach Definition eines Repräsentantensystems ist die Abbildung $S \rightarrow G/H, g \mapsto [g]$ bijektiv, also haben Definitions- und Zielbereich gleich viele Elemente.

- (ii) Nach Lemma 2.30(i) gibt es Bijektionen zwischen allen Nebenklassen, also gilt $\#(gH) = \#(eH) = \#H$.

□

Der folgende Satz von Lagrange ist nun eine einfache Konsequenz.

Satz 2.53 (Satz von Lagrange). *Sei G eine endliche Gruppe und H eine Untergruppe. Dann gilt*

$$\#G = (G : H) \cdot \#H.$$

Beweis. Sei S ein Repräsentantensystem. Aus Lemma 2.30(iii) wissen wir, dass $G = \bigsqcup_{g \in S} gH$, also gilt $\#G = \sum_{g \in S} \#(gH)$. Aus Lemma 2.52 wissen wir aber, dass $\#(gH) = \#H$ für alle $g \in G$ gilt (also insbesondere für alle $g \in S$). Somit folgt

$$\#G = \sum_{g \in S} \#(gH) = \sum_{g \in S} \#H = \#S \cdot \#H = (G : H) \cdot \#H,$$

wobei wir im letzten Schritt noch Lemma 2.52(i) benutzt haben. □

Wir beweisen noch ein paar einfache, aber wichtige Folgerungen aus dem Satz von Lagrange.

Korollar 2.54. *Sei G eine endliche Gruppe.*

- (i) *Ist $H \subseteq G$ eine Untergruppe, dann gilt*

$$\#H \mid \#G,$$

d.h. die Ordnung der Untergruppe ist ein Teiler der Ordnung von G .

- (ii) *Ist $g \in G$, dann gilt*

$$\text{ord}(g) \mid \#G.$$

- (iii) *Für jedes $g \in G$ gilt $g^{\#G} = e$.*

Kapitel 2 Gruppentheorie

Beweis. (i) ist eine direkte Konsequenz aus Satz 2.53.

(ii) folgt aus (i) mit $H = \langle g \rangle$, denn nach Definition ist $\text{ord}(g) = \#\langle g \rangle$.

(iii) Nach Satz 2.53 ist $\#G = (G : \langle g \rangle) \cdot \#\langle g \rangle = (G : \langle g \rangle) \cdot \text{ord}(g)$. Daher folgt mit Lemma 2.51

$$g^{\#G} = (g^{\text{ord}(g)})^{(G:\langle g \rangle)} = e^{(G:\langle g \rangle)} = e.$$

□

Korollar 2.55. Sei G eine Gruppe und $\#G = p$ eine Primzahl. Dann ist G zyklisch.

Beweis. Sei $g \in G$ ein Element mit $g \neq e$ (dieses existiert, da $p \geq 2$.) Dann gilt nach Korollar 2.54, dass $\text{ord}(g) \mid \#G = p$. Da $g \neq e$, ist außerdem $\text{ord}(g) \neq 1$, also folgt $\text{ord}(g) = p$. Somit ist $\langle g \rangle = G$, denn $\langle g \rangle$ ist eine Untergruppe von G , die genauso viele Elemente wie G enthält. Also ist G eine zyklische Gruppe. □

Aus dem Bahnsatz (Satz 2.49) ergeben sich zusammen mit dem Satz von Lagrange die folgenden expliziten Formeln.

Korollar 2.56 (Bahnformel und Bahngleichung). Sei G eine endliche Gruppe, X eine endliche Menge und $G \times X \rightarrow X$ eine Gruppenwirkung. Dann gilt für jedes $x \in X$ die Gleichheit

$$\#(Gx) \cdot \#(G_x) = \#G.$$

Ist weiter S ein Repräsentantensystem der zugehörigen Äquivalenzrelation wie in Lemma-Definition 2.47, dann gilt

$$\#X = \sum_{x \in S} (G : G_x).$$

Beweis. Da nach Definition des Index gilt $(G : G_x) = \#(G/G_x)$, folgt $\#(Gx) = (G : G_x)$ direkt aus Satz 2.49 und somit die erste Gleichung mit Satz 2.53.

Aus Lemma 2.27 und Lemma-Definition 2.47 wissen wir, dass gilt

$$X = \bigsqcup_{x \in S} [x] = \bigsqcup_{x \in S} Gx$$

und somit

$$\#X = \sum_{x \in S} \#(Gx).$$

Zusammen mit der oben erwähnten Gleichheit $\#(Gx) = (G : G_x)$ folgt also die gewünschte zweite Gleichung. □

Wir wissen aus dem Satz von Lagrange nun, dass die Ordnung eines Elements die Gruppenordnung teilt. Wir wissen aber nicht, dass es zu jedem Teiler der Gruppenordnung auch ein passendes Element mit dieser Ordnung gibt, was im Allgemeinen auch falsch ist. Der folgende wichtige Satz sagt aber zumindest für die Primteiler der Gruppenordnung die Existenz solcher Elemente voraus.

Satz 2.57 (Satz von Cauchy). *Sei G eine endliche Gruppe und p eine Primzahl mit $p \mid \#G$. Dann gibt es ein Element $g \in G$ mit $\text{ord}(g) = p$.*

Beweis. Wir betrachten die Menge

$$M = \{(g_1, \dots, g_p) \in G \times \dots \times G \mid g_1 \cdot g_2 \cdot \dots \cdot g_p = e\}.$$

Sie besteht also aus p -Tupeln von Elementen in G , deren Produkt das neutrale Element ergibt. Auf dieser Menge betrachten wir nun die folgende Wirkung der Gruppe $\mathbb{Z}/p\mathbb{Z}$:

$$\mathbb{Z}/p\mathbb{Z} \times M \rightarrow M, \quad ([k], (g_1, \dots, g_p)) \mapsto (g_{k+1}, \dots, g_p, g_1, \dots, g_k).$$

Das Element $[k] \in \mathbb{Z}/p\mathbb{Z}$ (dargestellt durch eine Zahl $k \in \{0, \dots, p-1\}$) permutiert das Tupel also zyklisch. (Es ist einfach zu sehen, dass dies tatsächlich eine Gruppenoperation definiert.)

Behauptung: Für jede Bahn dieser Gruppenwirkung gilt $\#(\mathbb{Z}/p\mathbb{Z}(g_1, \dots, g_p)) \in \{1, p\}$.

Nach Korollar 2.56 ist die Bahnlänge $\#(\mathbb{Z}/p\mathbb{Z}(g_1, \dots, g_p))$ ein Teiler der Ordnung $\#\mathbb{Z}/p\mathbb{Z} = p$ und kann somit nur 1 oder p sein, da p Primzahl ist.

Bahnen mit nur einem Element müssen offensichtlich aus einem Element der Form (g, \dots, g) bestehen (d.h. alle Einträge sind gleich). Davon gibt es mindestens eines, nämlich (e, \dots, e) , denn dieses erfüllt offensichtlich die Bedingung, dass das Produkt aller Einträge das neutrale Element ist.

Wir bezeichnen mit c die Anzahl der Bahnen mit nur einem Element. Nach obigem Argument gilt $c \neq 0$. Außerdem bezeichnen wir mit d die Anzahl der Bahnen, die aus p verschiedenen Elementen bestehen.

Da M die disjunkte Vereinigung aller Bahnen ist (denn Bahnen sind Äquivalenzklassen, siehe Lemma 2.27 und Lemma-Definition 2.47), muss gelten $\#M = c + d \cdot p$.

Die Menge M hat $(\#G)^{p-1}$ Elemente, denn um ein Element $(g_1, \dots, g_p) \in M$ zu erhalten, kann man $g_1, \dots, g_{p-1} \in G$ frei wählen (wofür man jeweils $\#G$ Möglichkeiten hat) und das Element g_p ist dann eindeutig festgelegt als $g_p = (g_1 \cdots \dots \cdot g_{p-1})^{-1}$. Insbesondere gilt also $p \mid \#M$, da nach Voraussetzung $p \mid \#G$ gilt.

Daher muss wegen $c = \#M - d \cdot p$ auch gelten $p \mid c$. Da wir bereits gezeigt haben, dass $c \neq 0$, folgt $c > 1$, es gibt also mindestens ein Tupel $(g, \dots, g) \in M$, welches aus einem Element $g \neq e$ besteht. Dieses erfüllt dann also $g^p = e$ und somit folgt $\text{ord}(g) \mid p$, was aber wegen $g \neq e$ bereits $\text{ord}(g) = p$ bedeutet. Damit haben wir ein Element $g \in G$ der Ordnung p gefunden. \square

2.7 Die Sylowsätze

Als Anwendung von Gruppenwirkungen wollen wir nun noch die sogenannten Sylowsätze (benannt nach dem Mathematiker Ludwig Sylow) kennenlernen. Sie

Kapitel 2 Gruppentheorie

können uns unter anderem helfen zu verstehen, welche Untergruppen eine gegebene endliche Gruppe besitzt (oder eben nicht besitzt).

Definition 2.58. Sei p eine Primzahl und G eine endliche Gruppe mit $p \mid \#G$. Schreibe $\#G = p^n \cdot m$ mit $p \nmid m$ und $n \in \mathbb{N}$. Dann nennen wir eine Untergruppe $H \subseteq G$ eine p -**Untergruppe**, falls $\#H = p^s$ für ein $s \in \mathbb{N}$. Eine Untergruppe $H \subseteq G$ heißt p -**Sylowgruppe**, falls $\#H = p^n$.

Es stellt sich natürlich sofort die Frage, ob es solche p -Sylowgruppen immer gibt, ob möglicherweise mehrere existieren (und es zwischen diesen dann ein Zusammenhang gibt) und falls ja, wie viele davon existieren. Diese Fragen klären die drei *Sylowsätze*.

Satz 2.59 (Erster Sylowsatz). Sei G eine endliche Gruppe und p eine Primzahl mit $p \mid \#G$. Dann gibt es eine p -Sylowgruppe in G .

Satz 2.60 (Zweiter Sylowsatz). Sei G eine endliche Gruppe und p eine Primzahl mit $p \mid \#G$. Dann gilt:

- (i) Ist $H \subseteq G$ eine p -Untergruppe, dann gibt es eine p -Sylowgruppe $P \subseteq G$ mit $H \subseteq P$.
- (ii) Sind $P, P' \subseteq G$ zwei p -Sylowgruppen, dann gibt es ein $g \in G$, sodass gilt

$$P' = gPg^{-1},$$

d.h. je zwei p -Sylowgruppen sind zueinander konjugiert (und insbesondere zueinander isomorph).

Satz 2.61 (Dritter Sylowsatz). Sei G eine endliche Gruppe und p eine Primzahl mit $p \mid \#G$. Sei $\#G = p^n \cdot m$ mit $p \nmid m$ und $n \in \mathbb{N}$. Sei $s_p \in \mathbb{N}$ die Anzahl der p -Sylowgruppen in G . Dann gilt

$$s_p \equiv 1 \pmod{p} \quad \text{und} \quad s_p \mid m.$$

Bevor wir die Sätze beweisen, führen wir noch den folgenden Begriff ein.

Lemma-Definition 2.62. Sei G eine Gruppe und $H \subseteq G$ eine Untergruppe. Dann ist die Teilmenge

$$N_G(H) := \{g \in G \mid gHg^{-1} = H\} \subseteq G$$

eine Untergruppe von G mit $H \subseteq N_G(H)$. Es gilt sogar $H \triangleleft N_G(H)$, d.h. H ist ein Normalteiler in $N_G(H)$. Wir nennen $N_G(H)$ den **Normalisator** von H in G .

Beweis. $N_G(H)$ ist eine Untergruppe von G , denn:

- (1) $eHe^{-1} = eHe = H$, also $e \in N_G(H)$,

(2) Seien $g_1, g_2 \in N_G(H)$, d.h. $g_1 H g_1^{-1} = H$ und $g_2 H g_2^{-1} = H$, dann folgt auch

$$(g_1 g_2) H \underbrace{(g_1 g_2)^{-1}}_{=g_2^{-1} g_1^{-1}} = g_1 (g_2 H g_2^{-1}) g_1^{-1} = g_1 H g_1^{-1} = H,$$

also $g_1 g_2 \in N_G(H)$.

(3) Sei $g \in N_G(H)$, d.h. $g H g^{-1} = H$. Durch Umformen dieser Gleichung sieht man, dass auch $g^{-1} H (g^{-1})^{-1} = g^{-1} H g = H$, also $g^{-1} \in N_G(H)$.

Es gilt weiter $H \subseteq N_G(H)$, denn: Sei $h \in H$, dann gilt offensichtlich $h H h^{-1} \subseteq H$ (da H eine Gruppe ist). Auch die umgekehrte Inklusion $H \subseteq h H h^{-1}$ gilt, denn jedes Element $k \in H$ können wir schreiben als

$$k = h \underbrace{h^{-1} k h}_{\in H} h^{-1} \in h H h^{-1}.$$

Daher ist $h H h^{-1} = H$ und somit $h \in N_G(H)$.

Nach Definition eines Normalteilers ist dann auch klar, dass $H \triangleleft N_G(H)$ ein Normalteiler ist. \square

Im Beweis der Sylowsätze wird uns auch folgende Konsequenz aus der Bahngleichung nützlich sein.

Lemma 2.63. Sei G eine Gruppe, p eine Primzahl und $\#G = p^i$ für ein $i \in \mathbb{N}$. Sei X eine Menge und $G \times X \rightarrow X$ eine Gruppenwirkung und schreibe

$$\text{Fix}_G(X) := \{x \in X \mid \forall g \in G : g \cdot x = x\}$$

für die Menge der Fixpunkte dieser Gruppenwirkung. Dann gilt

$$\#X \equiv \#\text{Fix}_G(X) \pmod{p}.$$

Beweis. Wir erinnern uns an die Bahngleichung

$$\#X = \sum_{x \in S} (G : G_x),$$

wobei $S \subseteq X$ ein Repräsentantensystem der durch die Gruppenwirkung gegebenen Äquivalenzrelation ist (siehe Lemma-Definition 2.47).

Ein Element $x \in X$ ist genau ein Element von $\text{Fix}_G(X)$, wenn $G_x = G$ (also wenn x unter allen Gruppenelement invariant bleibt) oder (äquivalent) $Gx = \{x\}$ (also die Bahn von x nur aus dem Element x selbst besteht). Insbesondere muss jeder Fixpunkt der Gruppenwirkung ein Element von S sein, denn er ist der einzige Repräsentant seiner eigenen Äquivalenzklasse. Es gilt also $\text{Fix}_G(X) \subseteq S$.

Kapitel 2 Gruppentheorie

Für $x \in S \setminus \text{Fix}_G(X)$ ist hingegen $G_x \subsetneq G$ eine echte Untergruppe von G . Da $\#G = p^i$, muss folglich mit Satz 2.53 gelten: $\#G_x = p^j$ für ein $j \in \mathbb{N}_0$, $j < i$, und somit $(G : G_x) = p^{i-j}$, also $p \mid (G : G_x)$. Daher ist

$$\#X = \sum_{x \in \text{Fix}_G(X)} (G : G_x) + \underbrace{\sum_{x \in S \setminus \text{Fix}_G(X)} (G : G_x)}_{\equiv 0 \pmod{p}} \equiv \sum_{x \in \text{Fix}_G(X)} (G : G_x) \pmod{p}.$$

□

Beweis von Satz 2.59 (Erster Sylowsatz). Sei $\#G = p^n \cdot m$ mit $p \nmid m$. Wir zeigen nun induktiv die folgende allgemeinere Aussage:

Für jedes $i \in \{0, \dots, n\}$ hat G eine Untergruppe mit p^i Elementen.

(Für $i = n$ ergibt dies offensichtlich die gewünschte Aussage des ersten Sylowsatzes.) Für $i = 0$ ist diese Aussage klar, denn die triviale Untergruppe $\{e\}$ (mit $p^0 = 1$ Elementen) existiert immer.

Sei nun $i \in \{0, \dots, n-1\}$ und sei eine Untergruppe $H \triangleleft G$ mit $\#H = p^i$ gegeben. Dann wollen wir zeigen, dass es auch eine Untergruppe $H' \triangleleft G$ mit $\#H' = p^{i+1}$ gibt.

Wir betrachten die Menge $G/H = \{gH \mid g \in G\}$ der Linksnebenklassen (siehe Lemma-Definition 2.28, diese ist nicht unbedingt eine Gruppe, da H kein Normalteiler sein muss). Auf dieser Menge ist eine Gruppenwirkung der Gruppe H gegeben durch

$$H \times (G/H) \mapsto G/H, \quad (h, gH) \mapsto (hg)H.$$

Nach Lemma 2.63, angewendet auf diese Gruppenwirkung, gilt dann

$$\#(G/H) \equiv \#\text{Fix}_H(G/H) \pmod{p}.$$

Die Menge $\text{Fix}_H(G/H)$ besteht aus denjenigen Nebenklassen gH , sodass für alle $h \in H$ gilt $hgH = gH$. Dies lässt sich umformen zu $g^{-1}hgH = H$ und dies ist gleichbedeutend mit $g^{-1}hg \in H$. Da dies für alle $h \in H$ gelten soll, folgt also $g^{-1}Hg \subseteq H$, und weil $g^{-1}Hg$ und H gleich viele Elemente haben, bedeutet dies $g^{-1}Hg = H$. Wir haben daher

$$\text{Fix}_H(G/H) = \{gH \mid g \in G \text{ und } g^{-1}Hg = H\} = \{gH \mid g \in N_G(H)\}.$$

Die Fixpunkte sind also diejenigen Nebenklassen, die von Elementen aus dem Normalisator $N_G(H)$ repräsentiert werden. Anders geschrieben bedeutet dies, dass $\text{Fix}_H(G/H) = N_G(H)/H$. Diese Menge ist also insbesondere eine Gruppe, denn nach Lemma-Definition 2.62 ist H immer ein Normalteiler in $N_G(H)$.

Wegen obiger Formel aus Lemma 2.63 gilt dann $p \mid \#(N_G(H)/H)$, denn $\#H = p^i$ für ein $i < n$ und $\#G = p^n \cdot m$, also $p \mid \#(G/H) = \frac{\#G}{\#H} = p^{n-i} \cdot m$. Daher gibt es nach dem Satz von Cauchy (Satz 2.57) ein Element $[\tilde{g}] \in N_G(H)/H$ der Ordnung p .

Nun betrachten wir die kanonische Projektion

$$\pi: N_G(H) \rightarrow N_G(H)/H, \quad g \mapsto [g]$$

und definieren die Untergruppe $H' := \pi^{-1}(\langle [\tilde{g}] \rangle)$. Diese hat $p \cdot p^i = p^{i+1}$ Elemente, denn sie ist nichts anderes als die disjunkte Vereinigung der Äquivalenzklassen $[e], [\tilde{g}], [\tilde{g}^2], \dots, [\tilde{g}^{p-1}]$ und jede dieser Äquivalenzklassen (Nebenklassen) hat genauso viele Elemente wie H , nämlich p^i .

Somit haben wir eine Untergruppe der Ordnung p^{i+1} gefunden und die gewünschte Aussage ist gezeigt. \square

Beweis von Satz 2.60 (Zweiter Sylowsatz). Der Teil (i) folgt bereits aus unserem Beweis des ersten Sylowsatzes: Starten wir mit einer p -Gruppe H , so können wir mit dem obigen Argument eine Gruppe H' konstruieren, die $p \cdot \#H$ Elemente hat. Außerdem ist leicht zu sehen, dass $H \subseteq H'$ (denn $[e] = H$). Falls H' noch keine p -Sylowgruppe ist, kann man sukzessive so weiter machen, bis man bei einer p -Sylowgruppe ankommt, die dann natürlich immer noch H enthält.

Wir zeigen also noch Teil (ii): Seien $P, P' \subseteq G$ zwei p -Sylowgruppen. Betrachte die Menge G/P der Linksnebenklassen und die Gruppenwirkung

$$P' \times (G/P) \rightarrow G/P, \quad h' \cdot (gP) \mapsto (h'g)P,$$

für die nach Lemma 2.63 gilt

$$\#(G/P) \equiv \#\text{Fix}_{P'}(G/P) \pmod{p}.$$

Da P eine p -Sylowgruppe ist, gilt $p \nmid \#(G/P) = \frac{\#G}{\#P}$. Somit ist auch $\#\text{Fix}_{P'}(G/P) \not\equiv 0 \pmod{p}$, also gibt es mindestens einen Fixpunkt der obigen Gruppenwirkung.

Sei gP für ein passendes $g \in G$ ein solcher Fixpunkt. Es gilt dann also $h'gP = gP$ für alle $h' \in P'$. Dies impliziert dann (ähnlich wie in dem Argument im Beweis des ersten Sylowsatzes), dass $g^{-1}P'g = P$, was zu zeigen war. \square

Beweis von Satz 2.61 (Dritter Sylowsatz). Sei \mathfrak{S} die Menge aller p -Sylowgruppen in G . Sei P eine beliebige p -Sylowgruppe. Dann betrachten wir die Gruppenwirkung

$$P \times \mathfrak{S} \rightarrow \mathfrak{S}, \quad (h, Q) \mapsto hQh^{-1}.$$

Ein Fixpunkt dieser Gruppenwirkung ist eine p -Sylowgruppe Q , sodass $hQh^{-1} = Q$ für alle $h \in P$. Es gilt dann also $P \subseteq N_G(Q)$ und natürlich auch $Q \subseteq N_G(Q)$. Daher sind P und Q auch p -Sylowgruppen in $N_G(Q)$, denn wir haben $N_G(Q) \subseteq G$ und somit $\#N_G(Q) \mid \#G$, es kann also in $\#N_G(Q)$ keine größere Potenz von p vorkommen als in $\#G$.

Nach dem zweiten Sylowsatz gibt es also ein $g \in N_G(Q)$ mit $gQg^{-1} = P$. Allerdings ist nach Definition des Normalisators (Lemma-Definition 2.62) bereits $gQg^{-1} = Q$, also folgt $Q = P$. Es gibt also nur einen einzigen Fixpunkt der obigen Gruppenwirkung, nämlich $P \in \mathfrak{S}$.

Nach Lemma 2.63 gilt wieder

$$\#\mathfrak{S} \equiv \#\text{Fix}_P(\mathfrak{S}) \pmod{p}$$

und dies ist nichts anderes als die gesuchte Formel $s_p \equiv 1 \pmod{p}$.

Kapitel 2 Gruppentheorie

Betrachte nun die Gruppenwirkung

$$G \times \mathfrak{S} \rightarrow \mathfrak{S}, \quad (g, Q) \mapsto gQg^{-1}.$$

Nach dem zweiten Sylowsatz sind alle Elemente von \mathfrak{S} konjugiert zueinander (bzgl. eines Elements von G) und somit hat diese Gruppenwirkung nur eine einzige Bahn. Sei $P \in \mathfrak{S}$ ein beliebiges Element, dann ist $GP = \mathfrak{S}$, also ergibt die Bahnformel in diesem Fall $\#\mathfrak{S} \cdot \#(G_P) = \#G$ und folglich gilt $s_p = \#\mathfrak{S} \mid \#G = p^n \cdot m$. Da wir aber schon gezeigt haben, dass $s_p \equiv 1 \pmod{p}$, gilt $p \nmid s_p$, also folgt $s_p \mid m$ wie gewünscht. \square

Mithilfe der Sylowsätze kann man oft die Struktur kleiner Gruppen verstehen. Ein Beispiel gibt der folgende Satz.

Satz 2.64. *Sei G eine Gruppe mit $\#G = pq$, wobei p und q Primzahlen sind mit $p < q$ und $p \nmid (q - 1)$. Dann ist G zyklisch, also $G \cong \mathbb{Z}/(pq)\mathbb{Z}$.*

Beweis. Nach dem dritten Sylowsatz gilt $s_p \in \{1, q\}$ und $s_p \equiv 1 \pmod{p}$ (wobei s_p die Anzahl der p -Sylowgruppen in G bezeichnet) sowie $s_q \in \{1, p\}$ und $s_q \equiv 1 \pmod{q}$. Aus letzterem folgt daher wegen $p < q$, dass $s_q = 1$, es gibt also genau eine q -Sylowgruppe in G . Falls $s_p = q$ wäre, dann wäre $q \equiv 1 \pmod{p}$, also $p \mid (q - 1)$, was ein Widerspruch zur Voraussetzung ist, also ist auch $s_p = 1$.

Sei P die eindeutige p -Sylowgruppe und sei Q die eindeutige q -Sylowgruppe. Dann sind beide nach Korollar 2.55 zyklisch, d.h. jedes Element außer e in P hat die Ordnung p und jedes Element außer e in Q hat die Ordnung q . Insbesondere haben die beiden Gruppen nur das Element e gemeinsam. Sei nun $g \in G \setminus (P \cup Q)$ ein Element, das außerhalb beider Sylowgruppen liegt. Ein solches gibt es, denn $\#(G \setminus (P \cup Q)) = pq - (p + q - 1) = (p - 1)(q - 1) \geq q - 1 > 0$. Es gilt dann $\text{ord}(g) \mid \#G = pq$, aber $\text{ord}(g) \notin \{p, q\}$, sonst wäre $\langle g \rangle$ eine weitere p - bzw. q -Sylowgruppe. Also gilt $\text{ord}(g) = pq$ und somit ist $G = \langle g \rangle$ zyklisch. \square

Dieses Korollar sagt uns insbesondere, dass es beispielsweise nur eine einzige (nämlich die zyklische) Gruppe von Ordnung 15, 33 und 35 gibt.

Ringtheorie

Ah ! vous voilà bien, vous autres, mangeurs d' x ! Vous croyez avoir tout dit quand vous avez dit : l'algèbre.

Ah! Seht doch, was seid Ihr für Buchstabenfresser! Ihr meint, mit Eurer Algebra Alles fertig zu bringen.

Jules Verne
Autour de la Lune

3.1 Ringe und ihre grundlegenden Eigenschaften

In diesem Abschnitt werden wir das Konzept eines Rings näher kennenlernen. Im Gegensatz zu einer Gruppe, auf denen es nur *eine* Verknüpfung gibt, besitzt ein Ring *zwei* Rechenoperationen, die üblicherweise als Addition und Multiplikation bezeichnet werden und die „gewohnten“ Rechenregeln erfüllen sollen, die wir schon seit unseren ersten Rechenerfahrungen mit natürlichen Zahlen kennen.

Definition 3.1. Ein *Ring* $(R, +, \cdot)$ besteht aus einer Menge R und zwei Abbildungen

$$+ : R \times R \rightarrow R, \quad (r_1, r_2) \mapsto r_1 + r_2$$

(genannt Addition) und

$$\cdot : R \times R, \quad (r_1, r_2) \mapsto r_1 \cdot r_2$$

(genannt Multiplikation), sodass die folgenden Eigenschaften erfüllt sind:

- (1) $(R, +)$ ist eine abelsche Gruppe,

Kapitel 3 Ringtheorie

$$(2) \forall r, s, t \in R : (r \cdot s) \cdot t = r \cdot (s \cdot t), \quad (\text{Assoziativität der Multiplikation})$$

$$(3) \forall r, s, t \in R :$$

$$r \cdot (s + t) = (r \cdot s) + (r \cdot t)$$

und

$$(r + s) \cdot t = (r \cdot t) + (s \cdot t).$$

(Distributivgesetze)

Das neutrale Element der Addition bezeichnen wir mit $0 \in R$.

Bemerkung 3.2. Wie bereits bei Gruppen schreiben wir meistens die Multiplikation ohne Punkt, d.h. wir schreiben nur rs statt $r \cdot s$. Außerdem benutzen wir, um Klammern zu sparen, die übliche „Punkt-vor-Strich“-Konvention (d.h. wir denken uns Klammern um multiplikative Ausdrücke). Damit schreibt sich das erste Distributivgesetz zum Beispiel als

$$r(s + t) = rs + rt.$$

Auch hier unterschlagen wir oft in der Notation die Verknüpfungen $+$ und \cdot und sagen meist einfach „ R ist ein Ring“.

In dieser Vorlesung werden wir uns nur mit Ringen beschäftigen, bei denen die Multiplikation kommutativ ist und zudem ein neutrales Element hat. Wir fügen den obigen Eigenschaften also noch diese beiden hinzu.

Definition 3.3. Ein Ring $(R, +, \cdot)$ heißt **Ring mit Eins**, falls es ein Element $1 \in R$ gibt, sodass für alle $r \in R$ gilt: $1 \cdot r = r \cdot 1 = r$.

Ein Ring $(R, +, \cdot)$ heißt **kommutativer Ring**, falls für alle $r, s \in R$ gilt: $r \cdot s = s \cdot r$.

Erfüllt ein Ring beide der soeben definierten Eigenschaften, so nennen wir ihn einen **kommutativen Ring mit Eins**.

Beispiel 3.4. Wir kennen bereits einige kommutative Ringe mit Eins:

- $(\mathbb{Z}, +, \cdot)$, $(\mathbb{Q}, +, \cdot)$, $(\mathbb{R}, +, \cdot)$, $(\mathbb{C}, +, \cdot)$,
- $(\mathbb{Z}/n\mathbb{Z}, +, \cdot)$ (siehe dazu auch §3.3),
- $(K[X], +, \cdot)$, der Ring der Polynome mit Koeffizienten in einem Körper K (siehe dazu auch §3.4)

Ein nichtkommutativer Ring ist beispielsweise $(\text{Mat}(n \times n, \mathbb{Q}), +, \cdot)$, der Ring der $(n \times n)$ -Matrizen mit Einträgen in \mathbb{Q} (für ein $n \in \mathbb{N}$ mit $n \geq 2$).

Bemerkung 3.5. Wir wollen kurz den Zusammenhang mit den Begriffen aus Bemerkung 2.3 herstellen: Das Axiom (2) in Definition 3.1 kann man auch so formulieren:

$$(2) (R, \cdot) \text{ ist eine Halbgruppe.}$$

Ein Ring mit Eins ist dann ein Ring, bei dem (R, \cdot) sogar ein Monoid ist. Das neutrale Element der Multiplikation bezeichnen wir immer (wie bereits in Definition 3.3 getan) mit 1.

Wenn wir wie im Folgenden mit verschiedenen Ringen arbeiten, werden wir in der Notation nicht zwischen den Verknüpfungen oder neutralen Elementen unterscheiden, d.h. sind R und S zwei Ringe, schreiben wir sowohl $+$ als auch \cdot sowie 0 und 1 für die entsprechenden Verknüpfungen und Elemente in R und S , da aus dem Kontext immer zweifellos ersichtlich ist, in welchem Ring ein Term zu lesen ist. Es ist trotzdem sinnvoll, sich ab und an daran zu erinnern, dass diese Symbole verschiedene Objekte bezeichnen können.

Auch hier wollen wir Abbildungen betrachten, die sich im Bezug auf die Ringstruktur gut verhalten.

Definition 3.6. Seien R und S zwei kommutative Ringe mit Eins. Eine Abbildung $\varphi: R \rightarrow S$ heißt *Ringhomomorphismus*, falls die folgenden Eigenschaften erfüllt sind:

- (1) $\forall r_1, r_2 \in R : \varphi(r_1 + r_2) = \varphi(r_1) + \varphi(r_2)$,
- (2) $\forall r_1, r_2 \in R : \varphi(r_1 \cdot r_2) = \varphi(r_1) \cdot \varphi(r_2)$,
- (3) $\varphi(1) = 1$.

Ein bijektiver Ringhomomorphismus heißt *Ringisomorphismus*.

In der letzten Bedingung (3) bezeichnen die beiden Elemente „1“ natürlich zwei verschiedene neutrale Elemente der Multiplikation. Man könnte also ausführlicher schreiben: $\varphi(1_R) = 1_S$, wobei 1_R die Eins in R und 1_S die Eins in S ist. Da die Bedeutung der Symbole aber meist unmissverständlich aus dem Kontext klar wird, werden wir dies in der Regel nicht tun.

Natürlich soll ein Ringhomomorphismus auch das neutrale Element der Addition auf das neutrale Element der Addition abbilden. Man könnte sich also wundern, warum dies in obiger Definition nicht aufgeführt ist. Es stellt sich aber heraus, dass diese Eigenschaft bereits aus den anderen Axiomen folgt (ähnlich wie bei Lemma 2.10(i)).

Lemma 3.7. Ist $\varphi: R \rightarrow S$ ein Ringhomomorphismus, so gilt $\varphi(0) = 0$.

Beweis. Ein Ringhomomorphismus $\varphi: R \rightarrow S$ ist wegen Axiom (1) aus Definition 3.6 insbesondere ein Gruppenhomomorphismus zwischen den (additiven) Gruppen $(R, +)$ und $(S, +)$. Somit bildet er nach Lemma 2.10 das neutrale Element der Addition auf das neutrale Element der Addition ab. \square

Wir merken an, dass dasselbe Argument für die Bedingung $\varphi(1) = 1$ nicht funktioniert, da (R, \cdot) und (S, \cdot) im Allgemeinen keine Gruppen sind – es gibt in einem Ring nicht unbedingt multiplikativ Inverse! Somit kann das Axiom (3) in Definition 3.6 nicht weggelassen werden.

Kapitel 3 Ringtheorie

Spezielle Beispiele für Ringe sind Körper, deren Definition wir hier schon einmal erwähnen, da sie im weiteren Verlauf der Vorlesung eine prominente Rolle spielen werden.

Definition 3.8. Ein *Körper* $(K, +, \cdot)$ besteht aus einer Menge K und zwei Verknüpfungen $+, \cdot : K \times K \rightarrow K$, sodass gilt:

- (1) $(K, +, \cdot)$ ist ein kommutativer Ring mit Eins,
- (2) $0 \neq 1$,
- (3) $\forall x \in K \setminus \{0\} \exists y \in K : xy = 1$.

Sind K_1, K_2 zwei Körper, so heißt ein Ringhomomorphismus $\varphi : K_1 \rightarrow K_2$ auch *Körperhomomorphismus*. Ein bijektiver Körperhomomorphismus heißt *Körperisomorphismus*. Ist K ein Körper, so heißt ein Körperisomorphismus $\varphi : K \rightarrow K$ auch *Körperautomorphismus* von K .

Ein Körper ist also ein kommutativer Ring mit Eins, in dem jedes Element, welches nicht 0 ist, ein multiplikatives Inverses hat. Außerdem wird gefordert, dass die beiden neutralen Elemente 0 und 1 voneinander verschieden sind. Dies ist nötig, um den pathologischen Fall des sogenannten *Nullrings* $R = \{0\}$ auszuschließen, den wir nicht als Körper betrachten wollen. (Dieser ist ein kommutativer Ring mit Eins, aber in ihm fallen die neutralen Elemente der Addition und der Multiplikation zusammen, d.h. $0 = 1$. Er ist der einzige Ring mit dieser Eigenschaft.)

3.2 Einheiten und Nullteiler

In einem Ring mit Eins hat im Allgemeinen nicht jedes Element ein multiplikativ Inverses. Diejenigen Elemente, die ein solches Inverses besitzen, wollen wir nun untersuchen.

Definition 3.9. Sei R ein kommutativer Ring mit Eins. Ein Element $r \in R$ heißt *Einheit*, falls es ein multiplikatives Inverses besitzt, also falls es ein $s \in R$ gibt mit $rs = 1$. Die Teilmenge aller Einheiten in R bezeichnen wir mit R^\times .

Bemerkung 3.10. Die Bedingung (3) in Definition 3.8 kann mit diesem neuen Begriff der Einheit auch so geschrieben werden:

$$(3) \quad K^\times = K \setminus \{0\}.$$

Das neutrale Element der Addition 0 hat, falls $0 \neq 1$ ist, niemals ein multiplikatives Inverses, wie man sich leicht überlegt: Für jedes $s \in R$ gilt

$$0 \cdot s = (0 + 0) \cdot s = 0 \cdot s + 0 \cdot s.$$

Von dieser Gleichung können wir auf beiden Seiten $0 \cdot s$ abziehen und erhalten $0 = 0 \cdot s$. Gäbe es also ein $s \in R$ mit $0 \cdot s = 1$, so wäre das ein Widerspruch zu $0 \neq 1$. Eine ähnliche, aber allgemeinere Aussage beweisen wir gleich in Lemma 3.14.

Beispiel 3.11. • $\mathbb{Z}^\times = \{-1, +1\}$,

- $(\mathbb{Z}[i])^\times = \{1, -1, i, -i\}$, wobei $\mathbb{Z}[i] = \{a + bi \mid a, b \in \mathbb{Z}\}$ den Ring der *gaußschen Zahlen* bezeichnet.

Lemma 3.12. Seien R und S zwei kommutative Ringe mit Eins. Ist $\varphi: R \rightarrow S$ ein Ringhomomorphismus, dann gilt $\varphi(R^\times) \subseteq S^\times$, in anderen Worten: φ bildet Einheiten auf Einheiten ab, d.h. für jedes $r \in R^\times$ ist $\varphi(r) \in S^\times$.

Beweis. Sei $r \in R^\times$, d.h. es gibt ein $r' \in R$ mit $rr' = 1$. Dann ist

$$1 = \varphi(1) = \varphi(rr') = \varphi(r)\varphi(r'),$$

also hat auch $\varphi(r)$ ein Inverses und daher $\varphi(r) \in S^\times$.

(Bemerkung: Insbesondere folgt aus diesem Beweis, dass gilt $\varphi(r^{-1}) = \varphi(r)^{-1}$, falls r^{-1} existiert.) \square

Eine weitere interessante Klasse von Elementen sind solche, die selbst nicht Null sind, aus denen sich die Null als Produkt mit anderen Nicht-Null-Elementen zusammensetzen lässt.

Definition 3.13. Sei R ein Ring. Ein Element $r \in R$ heißt *Nullteiler*, falls es ein $r' \in R \setminus \{0\}$ gibt mit $rr' = 0$ oder $r'r = 0$.

Ein Ring, in dem das Element 0 der einzige Nullteiler ist, heißt *nullteilerfrei*.

Ein nullteilerfreier kommutativer Ring mit Eins, in dem $0 \neq 1$ gilt, heißt *Integritätsbereich*.

Ein Integritätsbereich ist also ein Ring, in dem das oben beschriebene Phänomen, nämlich dass das Produkt zweier Nicht-Null-Elemente Null ergibt, nicht auftritt.

Das folgende Lemma zeigt, dass die beiden Klassen von Elementen, die wir in diesem Abschnitt eingeführt haben (nämlich Einheiten und Nullteiler), sich gegenseitig ausschließen, dass also kein Element gleichzeitig beide Eigenschaften erfüllen kann.

Lemma 3.14. Sei R ein kommutativer Ring mit Eins. Ist $r \in R^\times$, so ist r kein Nullteiler. Insbesondere ist also jeder Körper ein Integritätsbereich.

Beweis. Sei $r \in R^\times$, d.h. es gibt $r' \in R$ mit $rr' = r'r = 1$. Sei $r'' \in R$ ein Element mit $rr'' = 0$. Dann ist

$$0 = r' \cdot 0 = r'(rr'') = (r'r)r'' = 1 \cdot r'' = r''.$$

Also ist $r'' = 0$ das einzige Element mit $rr'' = 0$ und daher ist r kein Nullteiler. \square

3.3 Ideale und Quotientenringe

Ähnlich wie bei Gruppen und Vektorräumen gibt es auch bei Ringen den Begriff des *Unterrings*. Dieser wird uns aber nicht wirklich nützlich sein, weshalb wir ihn an dieser Stelle auch gar nicht definieren wollen. Stattdessen führen wir nun eine wesentlich wichtigere Art von Unterobjekt eines Rings ein.

Definition 3.15. Sei R ein kommutativer Ring. Eine Teilmenge $\mathfrak{a} \subseteq R$ heißt *Ideal*, falls gilt

- (1) $0 \in \mathfrak{a}$,
- (2) $\forall x, y \in \mathfrak{a} : x + y \in \mathfrak{a}$,
- (3) $\forall r \in R \forall x \in \mathfrak{a} : r \cdot x \in \mathfrak{a}$.

Ist \mathfrak{a} ein Ideal in R , so schreiben wir $\mathfrak{a} \triangleleft R$. Wir nennen ein Ideal *echt*, falls $\mathfrak{a} \neq R$.

Beispiel 3.16. • In jedem kommutativen Ring R gibt es das Nullideal $\{0\} \triangleleft R$ und das Ideal, das aus allen Elementen des Rings besteht $R \triangleleft R$.

(Falls R ein Körper ist, so sind dies die einzigen beiden Ideale, wie wir gleich in Korollar 3.19 sehen werden.)

- $2\mathbb{Z} \triangleleft \mathbb{Z}$ oder allgemeiner $n\mathbb{Z} \triangleleft \mathbb{Z}$ für jedes $n \in \mathbb{Z}$.

Lemma 3.17. Seien R und S kommutative Ringe mit Eins und sei $\varphi : R \rightarrow S$ ein Ringhomomorphismus. Dann ist $\ker(\varphi) \triangleleft R$ ein Ideal.

Beweis. (1) $\varphi(0) = 0$, also $0 \in \ker(\varphi)$

(2) Seien $x, y \in \ker(\varphi)$, d.h. $\varphi(x) = \varphi(y) = 0$. Dann ist $\varphi(x + y) = \varphi(x) + \varphi(y) = 0 + 0 = 0$, also $x + y \in \ker(\varphi)$.

(3) Sei $r \in R$ und $x \in \ker(\varphi)$, d.h. $\varphi(x) = 0$. Dann ist $\varphi(rx) = \varphi(r)\varphi(x) = \varphi(r) \cdot 0 = 0$, also $rx \in \ker(\varphi)$. □

Lemma 3.18. Sei R ein kommutativer Ring mit Eins. Ist $\mathfrak{a} \triangleleft R$ ein Ideal und gilt $\mathfrak{a} \cap R^\times \neq \emptyset$, so ist $\mathfrak{a} = R$.

Beweis. Sei $x \in \mathfrak{a} \cap R^\times$, d.h. x ist ein Element von \mathfrak{a} und zugleich eine Einheit in R . Daher gibt es ein $y \in R$ mit $xy = 1$. Nach Axiom (3) aus Definition 3.15 gilt dann aber

$$1 = y \cdot x \in \mathfrak{a}$$

und somit auch für jedes beliebige $r \in R$

$$r = r \cdot 1 \in \mathfrak{a},$$

also $\mathfrak{a} = R$. □

Korollar 3.19. *Ist K ein Körper, so sind $\{0\}$ und K die einzigen Ideale in K .*

Beweis. Die Teilmenge $\{0\} \subset K$ ist offensichtlich ein Ideal. Falls $\mathfrak{a} \triangleleft K$ ein Ideal ist, das mehr als ein Element enthält, gilt aber automatisch $\mathfrak{a} \cap K^\times \neq \emptyset$, denn $K^\times = K \setminus \{0\}$ (jedes Element außer der 0 ist eine Einheit). Damit ist mit Lemma 3.18 bereits $\mathfrak{a} = K$. \square

Korollar 3.20. *Sei K ein Körper, S ein kommutativer Ring mit Eins, in dem $0 \neq 1$ gilt, und $\varphi: K \rightarrow S$ ein Ringhomomorphismus. Dann ist φ injektiv. Insbesondere ist jeder Körperhomomorphismus injektiv.*

Beweis. Wegen Lemma 3.17 ist $\ker(\varphi) \triangleleft K$ ein Ideal und wegen Korollar 3.19 muss dann $\ker(\varphi) = \{0\}$ oder $\ker(\varphi) = K$ gelten. In letzterem Fall wäre aber $\varphi(1) = 0 \neq 1$, was den Axiomen eines Ringhomomorphismus widerspricht. Somit muss gelten $\ker(\varphi) = \{0\}$ und folglich ist φ injektiv. \square

Die Notation $\mathfrak{a} \triangleleft R$ deutet schon an, dass Ideale in gewisser Weise in der Ringtheorie die Rolle spielen sollen, die Normalteiler in der Gruppentheorie gespielt haben. In der Tat sind Ideale genau die Unterobjekte, bezüglich derer man Quotientenringe bilden kann.

Lemma-Definition 3.21. *Sei R ein kommutativer Ring und $\mathfrak{a} \triangleleft R$ ein Ideal. Dann betrachten wir die Äquivalenzrelation auf R gegeben durch*

$$r \sim r' :\Leftrightarrow r' - r \in \mathfrak{a}.$$

Die Menge der Äquivalenzklassen bezeichnen wir mit $R/\mathfrak{a} := R/\sim$. Durch die Vorschriften

$$\begin{aligned} + : R/\mathfrak{a} \times R/\mathfrak{a} &\rightarrow R/\mathfrak{a}, & ([r_1], [r_2]) &\mapsto [r_1] + [r_2] := [r_1 + r_2], \\ \cdot : R/\mathfrak{a} \times R/\mathfrak{a} &\rightarrow R/\mathfrak{a}, & ([r_1], [r_2]) &\mapsto [r_1] \cdot [r_2] := [r_1 \cdot r_2], \end{aligned}$$

werden zwei wohldefinierte Verknüpfungen definiert, die R/\mathfrak{a} zu einem kommutativen Ring machen. Wir nennen $(R/\mathfrak{a}, +, \cdot)$ den **Quotientenring** (oder **Faktorring**) von R modulo \mathfrak{a} .

Ist R ein kommutativer Ring mit Eins, so auch R/\mathfrak{a} .

Die kanonische Projektion

$$\pi: R \rightarrow R/\mathfrak{a}, \quad r \mapsto [r]$$

ist ein surjektiver Ringhomomorphismus.

Beweis. • Wohldefiniertheit von der Addition:

Da $(R, +)$ eine abelsche Gruppe ist und $(\mathfrak{a}, +)$ eine Untergruppe, ist $(\mathfrak{a}, +)$ auch automatisch ein Normalteiler in $(R, +)$ (jede Untergruppe einer abelschen Gruppe ist Normalteiler). Somit ist die Addition auf R/\mathfrak{a} wohldefiniert nach Satz 2.34.

- Wohldefiniertheit der Multiplikation:

Seien $r_1, r'_1, r_2, r'_2 \in R$ mit $[r_1] = [r'_1]$ und $[r_2] = [r'_2]$, d.h. $r'_1 - r_1 \in \mathfrak{a}$ und $r'_2 - r_2 \in \mathfrak{a}$. Dann müssen wir zeigen, dass $[r_1 r_2] = [r'_1 r'_2]$, d.h. $r'_1 r'_2 - r_1 r_2 \in \mathfrak{a}$. Dies folgt mit einem kleinen Trick (indem man einen Term hinzufügt und wieder subtrahiert):

$$\begin{aligned} r'_1 r'_2 - r_1 r_2 &= r'_1 r'_2 - \underbrace{r'_1 r_2 + r'_1 r_2 - r_1 r_2}_{=0} \\ &= \underbrace{r'_1}_{\in R} \underbrace{(r'_2 - r_2)}_{\in \mathfrak{a}} + \underbrace{(r'_1 - r_1)}_{\in \mathfrak{a}} \underbrace{r_2}_{\in R} \in \mathfrak{a}. \end{aligned}$$

Hier haben wir in der letzten Zeile die Axiome (3) und (2) aus Definition 3.15 verwendet: Multipliziert man ein Element des Ideals mit einem beliebigen Element des Rings, so erhält man wiederum ein Element des Ideals, und die Summe zweier Idealelemente ist ebenfalls wieder ein Element im Ideal.

Da Addition und Multiplikation auf R/\mathfrak{a} durch die Verknüpfungen auf R induziert sind, ist dann klar, dass die Axiome eines Rings auch für R/\mathfrak{a} erfüllt sind. Außerdem sieht man sofort, dass $[1]$ ein neutrales Element der Multiplikation in R/\mathfrak{a} ist, wenn 1 ein solches in R ist.

Die gewünschten Eigenschaften der kanonischen Projektion sind nach Definition ebenfalls klar. \square

Ganz analog zu Gruppen sieht man auch hier, dass der folgende Homomorphiesatz gilt.

Satz 3.22 (Homomorphiesatz für Ringe). *Seien R und S kommutative Ringe mit Eins und sei $\varphi: R \rightarrow S$ ein Ringhomomorphismus, dann ist*

$$\bar{\varphi}: R/\ker(\varphi) \rightarrow S, \quad [r] \mapsto \varphi(r)$$

ein injektiver Ringhomomorphismus.

Wir führen jetzt noch einen speziellen Typ von Idealen ein.

Lemma-Definition 3.23. Sei R ein kommutativer Ring und $a \in R$. Dann ist die Teilmenge

$$(a) := R \cdot a := \{ra \mid r \in R\} \subseteq R$$

ein Ideal und wir nennen es das von a erzeugte **Hauptideal**.

Ein Ideal $\mathfrak{a} \triangleleft R$ heißt **Hauptideal**, falls es ein $a \in R$ gibt mit $\mathfrak{a} = (a)$.

Sind allgemeiner $a_1, \dots, a_k \in R, k \in \mathbb{N}$, so ist die Menge

$$(a_1, \dots, a_k) := R \cdot a_1 + \dots + R \cdot a_k := \{r_1 a_1 + \dots + r_k a_k \mid r_1, \dots, r_k \in R\}$$

ein Ideal und heißt das **von a_1, \dots, a_k erzeugte Ideal**.

Beweis. Die erste Konstruktion ist ein Spezialfall der zweiten (für $k = 1$). Seien also $a_1, \dots, a_k \in R$, dann gilt:

- (1) $0 \cdot a_1 + \dots + 0 \cdot a_k = 0$, also $0 \in (a_1, \dots, a_k)$.
- (2) Seien $x, y \in (a_1, \dots, a_k)$, d.h. $x = r_1 a_1 + \dots + r_k a_k$, $y = r'_1 a_1 + \dots + r'_k a_k$ für bestimmte $r_1, \dots, r_k, r'_1, \dots, r'_k \in R$. Dann gilt (mit Kommutativität der Addition und Distributivität in R)

$$x + y = (r_1 + r'_1)a_1 + \dots + (r_k + r'_k)a_k \in (a_1, \dots, a_k).$$

- (3) Sei $r \in R$ und $x \in (a_1, \dots, a_k)$, d.h. $x = r_1 a_1 + \dots + r_k a_k$ für $r_1, \dots, r_k \in R$. Dann ist (mit Distributivität und Assoziativität der Multiplikation in R)

$$r \cdot x = (r r_1)a_1 + \dots + (r r_k)a_k \in (a_1, \dots, a_k).$$

Also ist $(a_1, \dots, a_k) \triangleleft R$ ein Ideal. □

Natürlich muss nicht jedes Ideal in einem Ring R von der Form (a_1, \dots, a_k) sein und noch weniger von der Form (a) für einen einzigen Erzeuger a . Falls letzteres aber der Fall ist, erhält der Ring einen besonderen Namen.

Definition 3.24. Ein kommutativer Ring R , in dem jedes Ideal $\mathfrak{a} \triangleleft R$ ein Hauptideal ist, heißt **Hauptidealring**. Ist R zusätzlich ein Integritätsbereich, so nennen wir ihn **Hauptidealbereich**.

Ein kommutativer Ring heißt **noethersch**, falls jedes Ideal endlich erzeugt ist, d.h. falls es für jedes Ideal $\mathfrak{a} \triangleleft R$ endlich viele Elemente $a_1, \dots, a_k \in R$ gibt, sodass $\mathfrak{a} = (a_1, \dots, a_k)$.

Mit dem Ring der ganzen Zahlen kennen wir bereits ein Beispiel für einen Hauptidealbereich.

Lemma 3.25. *Der Ring \mathbb{Z} ist ein Hauptidealbereich.*

Beweis. Offensichtlich ist \mathbb{Z} ein Integritätsbereich, denn er ist kommutativ mit Eins, es gilt $0 \neq 1$ und er ist nullteilerfrei.

Das Nullideal $\{0\} \triangleleft \mathbb{Z}$ ist ein Hauptideal, denn $\{0\} = (0)$. Sei nun $\mathfrak{a} \triangleleft R$ ein Ideal mit $\mathfrak{a} \neq \{0\}$. Dann betrachte $a := \min\{z \in \mathfrak{a} \mid z > 0\}$ die kleinste positive Zahl in \mathfrak{a} .

Behauptung: $\mathfrak{a} = (a)$.

Die Inklusion $(a) \subseteq \mathfrak{a}$ ist nach Definition klar, denn $a \in \mathfrak{a}$ und somit auch $ra \in \mathfrak{a}$ für jedes $r \in R$. Für die andere Inklusion sei $b \in \mathfrak{a}$ ein beliebiges Element. Dann ergibt die Division mit Rest, dass wir schreiben können

$$b = qa + r$$

Kapitel 3 Ringtheorie

für ein $q \in \mathbb{Z}$ und ein $r \in \{0, \dots, a-1\}$. Das bedeutet aber, dass

$$r = \underbrace{b}_{\in \mathfrak{a}} - \underbrace{q}_{\in R} \cdot \underbrace{a}_{\in \mathfrak{a}} \in \mathfrak{a},$$

da \mathfrak{a} ein Ideal ist. Da aber a als die kleinste positive Zahl in \mathfrak{a} gewählt war, ist $r \in \{1, \dots, a-1\}$ nicht möglich, es muss also $r = 0$ gelten. Dann ist aber $b = qa \in (a)$ und die Behauptung ist gezeigt.

Daher ist \mathfrak{a} ein Hauptideal und \mathbb{Z} ein Hauptidealring. □

3.4 Der Polynomring $R[X]$

Wir beschäftigen uns nun mit einem wichtigen Beispiel eines Rings, das uns in dieser Vorlesung noch oft begegnen wird: Dem Polynomring in einer Variablen über einem Körper.

Wir werden sehen, dass dieser sich in vielerlei Hinsicht wie der Ring \mathbb{Z} der ganzen Zahlen verhält. Später (in §3.5) werden wir lernen, dass dies der Tatsache geschuldet ist, dass beide Ringe sogenannte *euklidische Ringe* sind.

Zunächst definieren wir den Polynomring (etwas allgemeiner über einem kommutativen Ring).

Definition 3.26. Ist R ein kommutativer Ring, dann heißt ein formaler Ausdruck

$$\sum_{i=0}^n a_i X^i = a_n X^n + a_{n-1} X^{n-1} + \dots + a_2 X^2 + a_1 X + a_0$$

mit $n \in \mathbb{N}_0$ und $a_0, \dots, a_n \in R$ (wobei $a_n \neq 0$, falls $n \neq 0$) ein *Polynom* in einer Variablen über R . (Hierbei sind X, X^2, \dots nur formale Symbole.)

Die Menge aller solchen Polynome bezeichnen wir mit

$$R[X] := \left\{ \sum_{i=0}^n a_i X^i \mid n \in \mathbb{N}_0; a_0, \dots, a_n \in R; a_n \neq 0, \text{ falls } n \neq 0 \right\}.$$

Zusammen mit der natürlichen Addition, gegeben durch

$$\sum_{i=0}^n a_i X^i + \sum_{i=0}^m b_i X^i := \sum_{i=0}^{\max(n,m)} (a_i + b_i) X^i$$

(wobei wir setzen $a_i := 0$ für $i > n$, falls $m > n$, bzw. $b_i := 0$ für $i > m$, falls $n > m$) und der natürlichen Multiplikation, gegeben durch

$$\left(\sum_{i=0}^n a_i X^i \right) \cdot \left(\sum_{j=0}^m b_j X^j \right) := \sum_{k=0}^{n+m} \left(\sum_{i=0}^k a_i b_{k-i} \right) X^k$$

bildet $R[X]$ einen kommutativen Ring. Er heißt der *Polynomring* in einer Variablen über R .

Bemerkung 3.27. Einige zusätzliche Überlegungen und Erläuterungen zu dieser Definition:

- Die Bemerkung bei der Definition der Addition bedeutet einfach Folgendes: Falls wir zwei Polynome addieren möchten, die nicht dieselbe höchste Potenz von X besitzen, also z.B.

$$\sum_{i=0}^n a_i X^i = a_n X^n + \dots + a_0 \quad \text{und} \quad \sum_{i=0}^m b_i X^i = b_m X^m + \dots + b_0$$

mit $m > n$, dann „füllen wir das erste Polynom auf“, indem wir Terme mit Koeffizienten $a_i = 0$ als führende Terme hinzufügen, also schreiben

$$\sum_{i=0}^n a_i X^i = a_n X^n + \dots + a_0 = 0 \cdot X^m + \dots + 0 \cdot X^{n+1} + a_n X^n + \dots + a_0.$$

Nun haben beide Polynome dieselbe Anzahl an Termen und wir können sie addieren, indem wir die Koeffizienten vor jedem X^i addieren.

- Die Formel für die Multiplikation kann man auch so schreiben:

$$\left(\sum_{i=0}^n a_i X^i \right) \cdot \left(\sum_{j=0}^m b_j X^j \right) := \sum_{k=0}^{n+m} \left(\sum_{\substack{i,j \in \mathbb{N}_0 \\ i+j=k}} a_i b_j \right) X^k.$$

- Die Bedingung, dass $a_n \neq 0$ für Polynome mit $n \neq 0$ ist technischer Natur: Sie bedeutet, dass wir ein Polynom (zumindest hier in der Definition) immer so aufschreiben, dass es vor der höchsten Potenz von X einen Koeffizienten hat, der nicht Null ist, es also keine „überflüssigen“ führenden Terme gibt. Falls wir das nicht tun, hätten wir für jedes Polynom viele verschiedene Darstellungen und die Menge $R[X]$ würde jedes Polynom unendlich oft enthalten. Für die Formeln der Addition und Multiplikation bedeutet dies: Nachdem man die Addition oder Multiplikation ausgeführt hat, muss man, falls dabei führende Terme mit Koeffizient 0 entstanden sein sollten, diese wieder wegstreichen.
- Die Formeln für die Addition und Multiplikation ergeben sich, indem man X wie ein Element eines Rings behandelt und einfach die üblichen Rechengesetze (Kommutativität, Assoziativität, Distributivität) anwendet – daher die Bezeichnung „natürliche“ Addition und Multiplikation. Aus diesem Grund erfüllen diese Operationen auch automatisch alle Eigenschaften, die es braucht, damit $(R[X], +, \cdot)$ ein kommutativer Ring wird. (Dies kann man leicht nachprüfen.)

Kapitel 3 Ringtheorie

- Das neutrale Element der Addition ist das Polynom $0 \in R[X]$ (d.h. das Polynom mit $n = 0, a_0 = 0$).
- Ist R ein kommutativer Ring mit Eins, so ist auch $R[X]$ ein kommutativer Ring mit Eins. Das neutrale Element der Multiplikation in $R[X]$ ist dann das Polynom $1 \in R[X]$ (d.h. das Polynom mit $n = 0, a_0 = 1$).

Definition 3.28. Sei R ein kommutativer Ring und sei $f(X) = \sum_{i=0}^n a_i X^i \in R[X] \setminus \{0\}$. Dann heißt

$$\deg(f) := \max\{i \mid a_i \neq 0\}$$

der *Grad* von f . Ist $n = \deg(f)$, dann nennen wir a_n den *Leitkoeffizienten* von f . Wir setzen auch $\deg(0) := -\infty$.

Es ist leicht zu sehen, wie sich der Grad beim Addieren oder Multiplizieren von Polynomen verhält.

Lemma 3.29. Sei R ein kommutativer Ring und seien $f(X), g(X) \in R[X] \setminus \{0\}$. Wir schreiben $(f + g)(X) := f(X) + g(X)$ und $(f \cdot g)(X) = f(X) \cdot g(X)$. Dann gilt:

- (i) $\deg(f + g) \leq \max\{\deg(f), \deg(g)\}$,
- (ii) $\deg(f \cdot g) \leq \deg(f) + \deg(g)$.

Falls der Leitkoeffizient von $f(X)$ oder $g(X)$ kein Nullteiler ist (also insbesondere, falls R nullteilerfrei ist), gilt sogar $\deg(f \cdot g) = \deg(f) + \deg(g)$.

Beweis. Die Aussagen (i) und (ii) ergeben sich direkt aus den Formeln für Addition und Multiplikation (siehe Definition 3.26): Schreibt man die Polynome $f(X) = \sum_{i=0}^n a_i X^i$ und $g(X) = \sum_{i=0}^m b_i X^i$ so auf, dass $n = \deg(f)$ bzw. $m = \deg(g)$ (es also keine führenden Terme mit Koeffizienten gleich Null gibt), dann kommt in der Summe $f + g$ höchstens die Potenz $X^{\max\{n,m\}}$ und im Produkt $f \cdot g$ höchstens die Potenz X^{n+m} vor.

Der höchste Term im Produkt $(f \cdot g)(X)$ lautet dann $a_n b_m X^{n+m}$. Es sind außerdem $a_n, b_m \neq 0$ (sonst wären n und m nicht die Grade von f und g). Ist also mindestens eines dieser beiden Elemente kein Nullteiler, so folgt $a_n b_m \neq 0$ und damit $\deg(f \cdot g) = n + m$. \square

Aus diesen Formeln erhalten wir als direkte Konsequenz die wichtige Aussage, dass sich die Nullteilerfreiheit vom Koeffizientenring auf den Polynomring überträgt.

Korollar 3.30. Ist R nullteilerfrei, so ist auch $R[X]$ nullteilerfrei. Insbesondere ist $R[X]$ ein Integritätsbereich, wenn R ein Integritätsbereich ist.

Beweis. Sei R nullteilerfrei und sei $f(X) \in R[X]$ ein Nullteiler, d.h. es gibt ein $g(X) \in R[X] \setminus \{0\}$ mit $f(X) \cdot g(X) = 0$. Falls $f(X) \neq 0$, dann wäre $\deg(f) \geq 0$ und da auch $\deg(g) \geq 0$ gilt, wäre daher nach Lemma 3.29 auch $\deg(f \cdot g) = \deg(f) + \deg(g) \geq 0$.

Das würde aber bedeuten $f(X) \cdot g(X) \neq 0$. Also folgt, dass $f(X) = 0$ der einzige Nullteiler in $R[X]$ ist. Daher ist $R[X]$ nullteilerfrei. \square

Über einem Integritätsbereich können wir nun außerdem die Einheiten im Polynomring beschreiben.

Korollar 3.31. *Sei R ein Integritätsbereich, dann gilt $(R[X])^\times = R^\times$, d.h. die einzigen Einheiten sind diejenigen konstanten Polynome, die den Einheiten in R entsprechen.*

Beweis. Sei $f(X) \in (R[X])^\times$, d.h. es gibt ein $g(X) \in R[X]$ (welches nicht das Nullpolynom sein kann) mit $f(X) \cdot g(X) = 1$. Nach Lemma 3.29 gilt dann $0 = \deg(1) = \deg(f \cdot g) = \deg(f) + \deg(g)$ und dies ist nur möglich, wenn $\deg(f) = \deg(g) = 0$. Es sind also $f(X)$ und $g(X)$ konstante Polynome, deren Produkt 1 ergibt, also insbesondere $f(X) \in R^\times$. Dies zeigt $(R[X])^\times \subseteq R^\times$ und die umgekehrte Inklusion ist klar. \square

Eine Besonderheit des Polynomrings (die wir aus \mathbb{Z} kennen, aber die in allgemeinen Ringen nicht verfügbar ist), ist die Existenz einer *Division mit Rest*, zumindest für gewisse Elemente.

Lemma 3.32. *Sei R ein kommutativer Ring mit Eins und seien $f(X), g(X) \in R[X]$ zwei Polynome mit $g(X) \neq 0$ und sei der Leitkoeffizient von g eine Einheit in R , d.h. wir können schreiben*

$$g(X) = \sum_{i=0}^m b_i X^i = b_m X^m + \dots + b_1 X + b_0$$

mit $b_m \in R^\times$.

Dann gibt es eindeutig bestimmte Polynome $q(X), r(X) \in R[X]$ mit

$$f(X) = q(X) \cdot g(X) + r(X) \quad \text{und} \quad \deg(r) < \deg(g).$$

Beweis. Wir beweisen zunächst die Existenz (das ist im Grunde der wohlbekannte Algorithmus zur Polynomdivision):

Ist $\deg(f) < \deg(g)$, so sind wir fertig, denn dann können wir setzen $q(X) := 0$ und $r(X) := f(X)$.

Falls $\deg(f) \geq \deg(g)$, dann können wir ein passendes Vielfaches von $g(X)$ subtrahieren: Sei $f(X) = \sum_{i=0}^n a_i X^i$ und $g(X) = \sum_{i=0}^m b_i X^i$ mit $\deg(f) = n$ und $\deg(g) = m$. Dann betrachten wir

$$\tilde{f}(X) := f(X) - \frac{a_n}{b_m} X^{n-m} \cdot g(X).$$

Hierbei bezeichnet $\frac{a_n}{b_m}$ das Element $a_n \cdot b_m^{-1} \in R$, welches existiert, da $b_m \in R^\times$ nach Voraussetzung eine Einheit ist. Es gilt dann $\deg(\tilde{f}) < \deg(f)$, denn der Faktor $\frac{a_n}{b_m} X^{n-m}$ ist gerade so gewählt, dass der führende Term in der Differenz wegfällt. Ist nun $\deg(\tilde{f}) < \deg(g)$, so sind wir fertig, denn dann setzen wir $q(X) := \frac{a_n}{b_m} X^{n-m}$

Kapitel 3 Ringtheorie

und $r(X) := \tilde{f}(X)$. Andernfalls verringern wir den Grad weiter, indem wir von \tilde{f} ein passendes Vielfaches von $g(X)$ abziehen, sodass die Differenz einen kleineren Grad als $\tilde{f}(X)$ hat. Dies wiederholen wir so oft, bis der Grad der Differenz kleiner als der von $g(X)$ ist.

Zuletzt noch zur Eindeutigkeit: Sind $q(X), r(X), q'(X), r'(X) \in R[X]$ mit $\deg(r) < \deg(g)$ und $\deg(r') < \deg(g)$ und

$$f(X) = q(X) \cdot g(X) + r(X) = q'(X) \cdot g(X) + r'(X).$$

Dann ist also $(q - q')(X) \cdot g(X) = (r' - r)(X)$. Nach Lemma 3.29 haben wir $\deg(r' - r) \leq \max\{\deg(r), \deg(r')\} < \deg(g)$. Andererseits haben wir aber auch $\deg((q - q') \cdot g) \geq \deg(g)$, falls $(q - q')(X) \neq 0$, da der führende Koeffizient von $g(X)$ eine Einheit und somit (nach Lemma 3.14) kein Nullteiler ist. Da das nicht möglich ist, muss also gelten $q(X) = q'(X)$ und damit auch $r(X) = r'(X)$. \square

In einem Polynomring $K[X]$, wobei K ein Körper ist, kann man für zwei Polynome $f(X), g(X) \in K[X]$ also immer eine Polynomdivision durchführen, wenn $g(X) \neq 0$, denn die zweite Bedingung ist automatisch erfüllt: Der Leitkoeffizient von g ist ein Element in $K \setminus \{0\}$ und jedes solche Element ist eine Einheit. Dies liefert uns sofort eine wichtige Eigenschaft des Polynomrings über einem Körper.

Korollar 3.33. *Sei K ein Körper. Dann ist $K[X]$ ein Hauptidealbereich.*

Beweis. Nach Korollar 3.30 ist $K[X]$ ein Integritätsbereich.

Da wir in $K[X]$ für alle Elemente $f(X), g(X) \in K[X]$ mit $g(X) \neq 0$ die Division mit Rest zur Verfügung haben, funktioniert der Beweis, dass $K[X]$ ein Hauptidealring ist, analog zu Lemma 3.25:

Das Nullideal $\{0\} = (0) \triangleleft K[X]$ ist ein Hauptideal. Für ein beliebiges Ideal $\alpha \triangleleft K[X]$ mit $\alpha \neq \{0\}$ sei $g(X) \in \alpha \setminus \{0\}$ ein Element mit minimalem Grad. Ist dann $f(X) \in \alpha$ ein beliebiges Element, so können wir schreiben

$$f(X) = q(X) \cdot g(X) + r(X)$$

für gewisse $q(X), r(X) \in K[X]$ mit $\deg(r) < \deg(g)$. Aus dieser Formel folgt aber $r(X) \in \alpha$ und dies ist nur möglich (da $g(X)$ minimalen Grad in $\alpha \setminus \{0\}$ hat), wenn $r(X) = 0$, also $f(X) = q(X) \cdot g(X)$. Somit ist $\alpha = (g(X))$ ein Hauptideal. \square

Auch wenn die Variable X als formale Variable betrachtet wird, kann man sie natürlich als „Platzhalter“ betrachten, an dessen Stelle Elemente des Rings eingesetzt werden können. Die folgende Bemerkung fasst dies etwas präziser.

Bemerkung 3.34. Ein Polynom $f(X) = \sum_{i=0}^n a_i X^i \in R[X]$ induziert eine Abbildung

$$R \rightarrow R, \quad r \mapsto f(r) := \sum_{i=0}^n a_i r^i.$$

Das Element $f(r)$ entsteht also einfach, indem man im (formalen) Ausdruck $f(X)$ die Variable X durch das Element r ersetzt und die Operationen (Summe, Produkt und Potenzieren, d.h. iteriertes Multiplizieren mit sich selbst) mit den gegebenen Rechenoperationen in R ausführt. Man beachte, dass diese Abbildung im Allgemeinen *kein* Ringhomomorphismus ist.

Fixieren wir ein Element $a \in R$, so erhalten wir außerdem die Abbildung

$$\text{ev}_a: R[X] \rightarrow R, \quad f(X) \mapsto f(a),$$

den *Einsetzungshomomorphismus*. Dieser ist ein Ringhomomorphismus (wie man sich leicht überlegt).

Der Unterschied in der Philosophie dieser beiden Abbildungen ist also der folgende: Im ersten Fall halten wir das Polynom $f(X)$ fest und setzen alle möglichen $r \in R$ ein, während wir im zweiten Fall das Element $a \in R$ fixieren und in alle möglichen Polynome $f(X) \in R[X]$ einsetzen. Eine andere Schreibweise für $f(a)$ ist also $\text{ev}_a(f(X))$ („ $f(X)$ ausgewertet bei a “).

Definition 3.35. Sei $f(X) \in R[X]$ ein Polynom. Wir nennen $a \in R$ eine *Nullstelle* von f , falls $f(a) = 0$.

Über diesen Begriff der Nullstelle erhalten wir aus obigem Lemma 3.32 direkt die folgende Konsequenz.

Korollar 3.36. Sei R ein kommutativer Ring mit Eins und $0 \neq 1$ und sei $f(X) \in R[X]$ ein Polynom mit $\deg(f) \geq 1$. Ist $a \in R$ eine Nullstelle von $f(X)$, dann gibt es ein $q(X) \in R[X]$ mit

$$f(X) = (X - a) \cdot q(X).$$

Ist R ein Integritätsbereich, so hat $f(X)$ höchstens $\deg(f)$ viele verschiedene Nullstellen.

Beweis. Nach Lemma 3.32 (mit $g(X) := X - a$, das die dort geforderten Eigenschaften erfüllt), gibt es $q(X), r(X) \in R[X]$, sodass $f(X) = q(X) \cdot (X - a) + r(X)$ und $\deg(r) < \deg(X - a) = 1$. Es muss also insbesondere $r(X)$ ein konstantes Polynom sein, d.h. $r(X) = c$ für ein $c \in R$. Setzen wir auf beiden Seiten a für X ein, erhalten wir

$$\underbrace{f(a)}_{=0} = q(a) \cdot 0 + \underbrace{r(a)}_{=c}.$$

Es folgt also, dass $r(X) = 0$ das Nullpolynom ist und somit $f(X) = (X - a) \cdot q(X)$.

Sei nun R ein Integritätsbereich und seien $a_1, \dots, a_k \in R$ paarweise verschiedene Nullstellen von $f(X)$, dann können wir nach obiger Aussage schreiben $f(X) = (X - a_1) \cdot q(X)$ für ein $q(X) \in R[X]$. Setzen wir a_2 in diese Gleichung ein, erhalten wir

$$\underbrace{f(a_2)}_{=0} = \underbrace{(a_2 - a_1)}_{\neq 0} \cdot q(a_2).$$

Kapitel 3 Ringtheorie

Da R ein Integritätsbereich ist, ist $a_2 - a_1 \neq 0$ kein Nullteiler und somit muss gelten $q(a_2) = 0$. Genauso zeigen wir $q(a_3) = q(a_k) = 0$. Wir können also schreiben $q(X) = (X - a_2) \cdot q'(X)$ für ein $q'(X) \in R[X]$, welches dann wiederum a_3, \dots, a_k als Nullstellen hat. Sukzessive erhalten wir also

$$f(X) = (X - a_1) \cdot \dots \cdot (X - a_k) \cdot \tilde{q}(X)$$

für ein $\tilde{q}(X) \in R[X]$. Da wir vorausgesetzt haben $\deg(f) \geq 1$, gilt $f(X) \neq 0$ und daher $\tilde{q}(X) \neq 0$. Wegen Lemma 3.29 folgt dann $\deg(f) = \deg(X - a_1) + \dots + \deg(X - a_k) + \deg(\tilde{q}) \geq k$, also kann es höchstens $\deg(f)$ verschiedene Nullstellen von $f(X)$ geben. \square

3.5 Euklidische Ringe

Wie bereits im letzten Abschnitt angedeutet, sind \mathbb{Z} und $K[X]$ zwei Beispiele eines allgemeineren Konzeptes, das wir nun entwickeln wollen.

Definition 3.37. Ein Integritätsbereich R heißt *euklidischer Ring*, falls es eine Abbildung (die *Gradfunktion*)

$$d: R \setminus \{0\} \rightarrow \mathbb{N}_0$$

gibt, sodass folgende Eigenschaft erfüllt ist:

$$\forall a \in R \forall b \in R \setminus \{0\} \exists q, r \in R : a = qb + r \wedge (r = 0 \vee d(r) < d(b)).$$

(Division mit Rest)

Ein euklidischer Ring besitzt also eine Division mit Rest, bei welcher der Rest – in einer passenden Funktion d gemessen – „kleiner“ als der Divisor ist. (Hierbei nennen wir a den *Dividenden* und b den *Divisor*.)

Beispiel 3.38. Einige wichtige Beispiele für euklidische Ringe sind:

- \mathbb{Z} mit der Gradfunktion $d(x) := |x|$ (gegeben durch den Absolutbetrag),
- $K[X]$ für einen Körper K , mit der Gradfunktion $d(f) := \deg(f)$,
- jeder Körper K (denn die Division geht dann immer auf),
- der Ring der Gaußschen Zahlen $\mathbb{Z}[i] := \{a + bi \mid a, b \in \mathbb{Z}\}$, mit der Gradfunktion $d(a + bi) := a^2 + b^2$. (Es ist nicht offensichtlich, dass dies ein euklidischer Ring ist, siehe Übungen).

Mit demselben Argument wie in Lemma 3.25 und Korollar 3.33 lässt sich auch der folgende allgemeine Satz beweisen.

Satz 3.39. *Jeder euklidische Ring ist ein Hauptidealbereich.*

Beweis. Sei R ein euklidischer Ring mit Gradfunktion d . Sei $\mathfrak{a} \triangleleft R$ ein beliebiges Ideal. Falls $\mathfrak{a} = (0)$ das Nullideal ist, ist \mathfrak{a} offensichtlich ein Hauptideal.

Andernfalls betrachte die Menge aller Werte, die die Gradfunktion d auf $\mathfrak{a} \setminus \{0\}$ annimmt, also die Menge $d(\mathfrak{a} \setminus \{0\}) \subseteq \mathbb{N}$. Da diese Menge nichtleer ist, hat sie ein kleinstes Element. Wir wählen ein Element $a \in \mathfrak{a} \setminus \{0\}$, sodass $d(a)$ minimal ist.

Ist nun $x \in \mathfrak{a}$ ein beliebiges anderes Element, dann gibt es $q, r \in R$ mit $x = qa + r$ und sodass entweder $r = 0$ oder $d(r) < d(a)$. Wir sehen aber, dass

$$r = \underbrace{x}_{\in \mathfrak{a}} - \underbrace{q}_{\in R} \cdot \underbrace{a}_{\in \mathfrak{a}} \in \mathfrak{a},$$

$\underbrace{\hspace{10em}}_{\in \mathfrak{a}}$

daher ist $d(r) < d(a)$ nicht möglich, denn wir haben a so gewählt, dass es den kleinsten Grad unter allen Elementen von $\mathfrak{a} \setminus \{0\}$ annimmt. Es muss also $r = 0$ gelten und somit ist $x = qa$ ein Vielfaches von a . Da dies für alle Elemente $x \in \mathfrak{a}$ gilt, folgt, dass $\mathfrak{a} = (a)$ das von a erzeugte Hauptideal ist. \square

Wir definieren nun einen Begriff, den wir aus den ganzen Zahlen gut kennen.

Definition 3.40. Sei R ein kommutativer Ring mit Eins und seien $x, y \in R$ zwei Elemente, von denen mindestens eines nicht 0 ist. Ein Element $d \in R \setminus \{0\}$ heißt ein *größter gemeinsamer Teiler* von x und y , falls gilt

- (1) $d \mid x$ und $d \mid y$,
- (2) $\forall s \in R : (s \mid x \wedge s \mid y) \Rightarrow s \mid d$.

Wir schreiben dann auch $d = \text{ggT}(x, y)$.

Bemerkung 3.41. Diese Definition lässt sich ganz einfach auch zu einer Definition eines größten gemeinsamen Teilers von mehr als zwei Elementen verallgemeinern. Alle Aussagen, die wir über den ggT von zwei Elementen im weiteren Verlauf der Vorlesung machen werden, verallgemeinern sich ebenfalls leicht auf mehrere (aber endlich viele) Elemente.

Die Bedingung (2) besagt dass jeder gemeinsame Teiler s von x und y auch ein Teiler von d ist. Dies rechtfertigt die Bezeichnung „größter gemeinsame Teiler“, denn d „enthält“ jeden anderen gemeinsamen Teiler von x und y .

Beachte, dass weder die Existenz noch die Eindeutigkeit von größten gemeinsamen Teilern im Allgemeinen gegeben ist. Nicht jedes Paar von Elementen $x, y \in R$ wie oben hat notwendigerweise einen größten gemeinsamen Teiler. Wir werden aber später Ringe studieren, in denen die Existenz immer gegeben ist, die sogenannten *faktoriellen Ringe*.

Man beachte weiter, dass in der Definition von *einem*, nicht *dem* größten gemeinsamen Teiler die Rede ist. In \mathbb{Z} ist zum Beispiel sowohl 2 als auch -2 ein größter gemeinsamer Teiler von 6 und 8. In \mathbb{Z} „bevorzugen“ wir meistens positive Zahlen,

Kapitel 3 Ringtheorie

so eine kanonische Wahl eines „besten“ größten gemeinsamen Teilers gibt es aber in allgemeineren Ringen nicht unbedingt. Die Schreibweise $d = \text{ggT}(x, y)$ ist daher mit Vorsicht zu lesen (und zu verwenden)!

Das folgende Lemma klärt die Frage, wie eindeutig der größte gemeinsame Teiler ist, wenn R ein Integritätsbereich ist, nämlich eindeutig bis auf Multiplikation mit einer Einheit.

Lemma 3.42. *Sei R ein Integritätsbereich und seien $x, y \in R$ zwei Elemente wie in Definition 3.40. Ist $d \in R$ ein größter gemeinsamer Teiler von x und y und ist $\varepsilon \in R^\times$ eine beliebige Einheit, so ist auch $d' := \varepsilon d$ ein größter gemeinsamer Teiler von x und y . Umgekehrt gilt auch: Sind $d, d' \in R$ zwei größte gemeinsame Teiler von x und y , so existiert eine Einheit $\varepsilon \in R^\times$, sodass gilt $d' = \varepsilon d$.*

Beweis. Sei $d = \text{ggT}(x, y)$ und $d' = \varepsilon d$ für ein $\varepsilon \in R^\times$. Dann ist auch $d' = \text{ggT}(x, y)$, denn:

- (1) Da $d \mid x$, gibt es ein $r \in R$ mit $x = rd$. Folglich ist $x = r\varepsilon\varepsilon^{-1}d$ und somit auch $e \mid x$. Ganz analog zeigt man, dass $e \mid y$ aus $d \mid y$ folgt.
- (2) Sei $s \in R$ mit $s \mid x$ und $s \mid y$, dann folgt $s \mid d$, da d ein größter gemeinsamer Teiler ist. Das bedeutet, dass $d = rs$ für ein $r \in R$. Dann ist aber auch $d' = \varepsilon d = \varepsilon rs$, also auch $s \mid d'$.

Seien umgekehrt $d, d' \in R$ größte gemeinsame Teiler von x und y , dann folgt aus der Bedingung (2) aus Definition 3.40 zum einen $d' \mid d$ (betrachte diese Bedingung für d und wähle $s = d'$), zum anderen aber auch $d \mid d'$ (betrachte die Bedingung für d' und wähle $s = d$). Es gibt also $r \in R$ mit $d = rd'$ und es gibt auch $r' \in R$ mit $d' = r'd$. Setzen wir dies zusammen, erhalten wir

$$d = rd' = rr'd,$$

woraus folgt $0 = d - rr'd = (1 - rr')d$. Da $d \neq 0$ und R ein Integritätsbereich ist, muss gelten $1 - rr' = 0$, also $rr' = 1$. Dies bedeutet aber, dass r und r' Einheiten sind, wir können also wählen $\varepsilon := r' \in R^\times$ und damit gilt $d' = \varepsilon d$. \square

Oben haben wir den Begriff des größten gemeinsamen Teilers für Integritätsbereiche betrachtet. Ist R sogar ein euklidischer Ring, erhalten wir die folgende schöne Aussage.

Lemma 3.43 (Lemma von Bézout). *Sei R ein euklidischer Ring und seien $x, y \in R$ zwei Elemente, von denen mindestens eines nicht 0 ist. Dann existiert ein größter gemeinsamer Teiler $d = \text{ggT}(x, y)$ von x und y und es gibt Elemente $a, b \in R$ mit*

$$d = ax + by. \qquad \qquad \qquad (\text{Bézout-Darstellung})$$

Bevor wir dieses Lemma beweisen, beschreiben wir ein wichtiges Rechenverfahren, das wir für den Beweis verwenden werden, das aber auch unabhängig davon nützlich ist: den *euklidischen Algorithmus*. Mit seiner Hilfe lässt sich durch sukzessives Teilen mit Rest der größte gemeinsame Teiler zweier Elemente (zum Beispiel zweier ganzer Zahlen) bestimmen.

Euklidischer Algorithmus 3.44. Sei R ein euklidischer Ring und seien $x, y \in R$ zwei Elemente mit $y \neq 0$. Dann können wir eine Division mit Rest (mit y als Divisor) durchführen:

$$x = q_1 \cdot y + r_1$$

für $q_1, r_1 \in R$ mit $r = 0$ oder $d(r_1) < d(y)$. Falls diese Division noch nicht „aufgeht“, also falls $r \neq 0$, dann führen wir eine weitere Division mit Rest mit den Elementen y und r_1 durch:

$$y = q_2 \cdot r_1 + r_2.$$

Es gilt hier dann $r_2 = 0$ oder $d(r_2) < d(r_1)$. Dies wiederholen wir nun: Solange der Rest nicht Null ist, führen wir eine weitere Division mit Rest durch, wobei wir als Dividend den Divisor der vorherigen Division und als Divisor den Rest der vorherigen Division verwenden. Da der Grad des Restes in jedem Schritt echt kleiner wird, erreicht man irgendwann den Punkt, an dem die Division aufgeht, der Rest also Null ist. Man hat also insgesamt eine Abfolge von Divisionen mit Rest wie folgt:

$$\begin{array}{rcl} x & = & q_1 \cdot y + r_1 \\ y & \leftarrow & = q_2 \cdot r_1 + r_2 \\ r_1 & \leftarrow & = q_3 \cdot r_2 + r_3 \\ & & \vdots \\ r_{n-3} & = & q_{n-1} \cdot r_{n-2} + r_{n-1} \\ r_{n-2} & \leftarrow & = q_n \cdot r_{n-1} + r_n \\ r_{n-1} & \leftarrow & = q_{n+1} \cdot r_n + 0 \end{array}$$

Nun überlegt man sich leicht folgende zwei Tatsachen:

- Der letzte nicht-verschwindende Rest r_n ist ein sowohl ein Teiler von x als auch von y :

Aus der letzten Zeile folgt, dass $r_n \mid r_{n-1}$. Damit erhält man aus der vorletzten Zeile, dass r_{n-2} ein Vielfaches von r_n ist, also $r_n \mid r_{n-2}$. Verfolgt man dieses

Kapitel 3 Ringtheorie

Argument durch alle Zeilen bis ganz nach oben, hat man schließlich auch $r_n \mid y$ und $r_n \mid x$.

- Für jeden gemeinsamen Teiler s von x und y gilt $s \mid r_n$:

Seien $s \mid x$ und $s \mid y$, dann folgt aus der ersten Zeile $r_1 = x - q_1 \cdot y$, also gilt auch $s \mid r_1$. Die zweite Zeile ergibt wiederum $r_2 = y - q_2 \cdot r_1$, also ist auch r_2 ein Vielfaches von s , d.h. $s \mid r_2$. Verfolgt man dieses Argument bis zur vorletzten Zeile nach unten, erhält man $s \mid r_n$.

Insgesamt ist also $r_n = \text{ggT}(x, y)$ ein größter gemeinsamer Teiler von x und y und der euklidische Algorithmus gibt uns ein explizites Verfahren zu seiner Berechnung.

Beweis von Lemma 3.43. Der Euklidische Algorithmus 3.44 zeigt konstruktiv (also sogar mit Angabe einer expliziten Konstruktion) die Existenz eines größten gemeinsamen Teilers $d := r_n = \text{ggT}(x, y)$ von x und y . (Falls $y = 0$, muss man ggf. die Rollen von x und y vertauschen.)

Betrachte nun noch einmal die Kette von Divisionen mit Rest aus dem Algorithmus. Lösen wir die vorletzte Zeile nach $d = r_n$ auf, erhalten wir

$$d = r_{n-2} - q_n \cdot r_{n-1}.$$

Das Element d lässt sich also schreiben als Linearkombination von r_{n-1} und r_{n-2} (mit Koeffizienten in R). Lösen wir nun die drittletzte Zeile nach r_{n-1} auf, erhalten wir $r_{n-1} = r_{n-3} - q_{n-1} \cdot r_{n-2}$. Setzen wir dies in obige Gleichung für d ein, so sehen wir, dass sich d als Linearkombination von r_{n-2} und r_{n-3} (mit Koeffizienten aus R) darstellen lässt. Führen wir dies mit allen Gleichungen bis ganz oben durch, so erhalten wir schließlich eine Gleichung, die d als Linearkombination von x und y schreibt. Dies ist eine gesuchte Bézout-Darstellung. \square

Der soeben gegebene Beweis liefert auch eine explizite Methode zur Bestimmung einer Bézout-Darstellung, ist also wiederum konstruktiv.

3.6 Primideale und maximale Ideale

Wir haben gesehen, dass man den Quotienten eines Rings bezüglich eines Ideals bilden kann und diese Konstruktion wieder einen Ring liefert. Man kann sich nun fragen, welche Bedingungen das Ideal erfüllen muss, damit der Quotientenring möglichst gute Eigenschaften hat, also zum Beispiel ein Integritätsbereich oder sogar ein Körper ist – wir erinnern uns: Ziel dieser Vorlesung ist ja das Verständnis von Körpern und ihrer Erweiterungen. Diesen Fragen werden wir jetzt auf den Grund gehen.

Definition 3.45. Sei R ein kommutativer Ring. Ein Ideal $\mathfrak{a} \triangleleft R$ heißt *Primideal*, falls $\mathfrak{a} \neq R$ und falls gilt

$$xy \in \mathfrak{a} \Rightarrow x \in \mathfrak{a} \vee y \in \mathfrak{a}.$$

Beispiel 3.46. • Das Ideal $(0) \triangleleft R$ ist genau dann ein Primideal, wenn R ein Integritätsbereich ist.

- Das Ideal $(n) = n\mathbb{Z} \triangleleft \mathbb{Z}$ ist genau dann ein Primideal, wenn n eine Primzahl ist.
- Sei K ein Körper.

Das Ideal $(X) = X \cdot K[X] \triangleleft K[X]$ der Polynome ohne konstanten Term ist ein Primideal. Ebenso ist $(X - a) \triangleleft K[X]$ ein Primideal für alle $a \in K$.

Das Ideal $(X^2) \triangleleft K[X]$ ist kein Primideal.

Satz 3.47. Ist R ein kommutativer Ring und $\mathfrak{a} \triangleleft R$ ein Ideal, so ist R/\mathfrak{a} genau dann ein nullteilerfreier Ring, wenn \mathfrak{a} ein Primideal ist.

Beweis. Der Ring R/\mathfrak{a} hat genau dann (echte) Nullteiler, wenn es $[x], [y] \in R/\mathfrak{a}$ gibt mit $[x] \neq [0]$ und $[y] \neq 0$, aber $[xy] = [0]$. Anders ausgedrückt bedeutet dies, dass es $x, y \in R$ gibt mit $x, y \notin \mathfrak{a}$, aber $xy \in \mathfrak{a}$. Dies wiederum ist gleichbedeutend damit, dass \mathfrak{a} kein Primideal ist. \square

Definition 3.48. Sei R ein kommutativer Ring. Ein Ideal $\mathfrak{a} \triangleleft R$ heißt *maximales Ideal*, falls $\mathfrak{a} \neq R$ und falls gilt

$$\mathfrak{b} \triangleleft R \wedge \mathfrak{a} \subseteq \mathfrak{b} \subseteq R \Rightarrow \mathfrak{a} = \mathfrak{b},$$

also falls jedes echte Ideal, welches \mathfrak{a} enthält, bereits gleich \mathfrak{a} ist.

Bemerkung 3.49. Die obige Bedingung bedeutet, dass es kein echtes Ideal gibt, das wirklich größer als \mathfrak{a} ist. Man könnte das äquivalent auch so formulieren: Jedes Ideal, welches mehr Elemente als \mathfrak{a} enthält, ist dann der ganze Ring (also nicht mehr echt). Die Bedingung in Definition 3.48 ist also äquivalent zu

$$\mathfrak{b} \triangleleft R \wedge \mathfrak{a} \subsetneq \mathfrak{b} \subseteq R \Rightarrow \mathfrak{b} = R.$$

Beispiel 3.50. • Ist $p \in \mathbb{N}$ eine Primzahl, dann ist $(p) = p\mathbb{Z} \triangleleft \mathbb{Z}$ ein maximales Ideal, denn ist $\mathfrak{b} = (n) \triangleleft \mathbb{Z}$ ein echt größeres Ideal (jedes Ideal in \mathbb{Z} ist ein Hauptideal), d.h. $(p) \subsetneq (n)$, dann folgt $n \mid p$ (aber nicht $n = \pm p$, sonst wären die beiden Ideale gleich). Dann muss aber $n = \pm 1$ gelten. Also ist $(n) = (1) = \mathbb{Z}$.

Das Ideal $4\mathbb{Z} \triangleleft \mathbb{Z}$ ist hingegen nicht maximal, denn es gilt $4\mathbb{Z} \subsetneq 2\mathbb{Z} \subsetneq \mathbb{Z}$. (Ebenso verhält es sich mit allen anderen Idealen $n\mathbb{Z}$, wobei n keine Primzahl ist.)

Satz 3.51. Ist R ein kommutativer Ring mit Eins und $\mathfrak{a} \triangleleft R$ ein Ideal, so ist R/\mathfrak{a} genau dann ein Körper, wenn \mathfrak{a} ein maximales Ideal ist.

Kapitel 3 Ringtheorie

Beweis.

\mathfrak{a} maximales Ideal $\Rightarrow R/\mathfrak{a}$ Körper:

Sei \mathfrak{a} ein maximales Ideal und sei $[x] \in R/\mathfrak{a}$ ein Element mit $[x] \neq [0]$. Dann müssen wir zeigen, dass es ein multiplikatives Inverses zu $[x]$ gibt.

Es gilt $x \notin \mathfrak{a}$ (wegen $[x] \neq [0]$), wir betrachten daher das Ideal

$$\mathfrak{b} := \mathfrak{a} + R \cdot x := \{a + rx \mid a \in \mathfrak{a}, r \in R\}.$$

Dieses Ideal erfüllt $\mathfrak{a} \subsetneq \mathfrak{b} \subseteq R$ und somit folgt $\mathfrak{b} = R$ (da \mathfrak{a} ein maximales Ideal ist, siehe Bemerkung 3.49). Insbesondere ist also $1 \in \mathfrak{b}$, und da sich jedes Element in \mathfrak{b} in der Form $a + rx$ schreiben lässt, gibt es also ein $a \in \mathfrak{a}$ und ein $r \in R$ mit

$$1 = a + rx.$$

Lesen wir diese Gleichung nun in R/\mathfrak{a} , so erhalten wir

$$[1] = \underbrace{[a]}_{=[0]} + [r][x] = [r][x],$$

also ist r ein multiplikativ Inverses zu $[x]$. Da dies für jedes $[x]$ funktioniert, ist R/\mathfrak{a} ein Körper.

R/\mathfrak{a} Körper $\Rightarrow \mathfrak{a}$ maximales Ideal:

Sei R/\mathfrak{a} ein Körper, d.h. jedes $[x] \in R/\mathfrak{a}$ mit $[x] \neq [0]$ besitzt ein multiplikativ Inverses. Wir müssen zeigen, dass \mathfrak{a} ein maximales Ideal ist. Sei dafür $\mathfrak{b} \triangleleft R$ ein Ideal mit $\mathfrak{a} \subsetneq \mathfrak{b} \subseteq R$. Es gibt also ein $x \in \mathfrak{b}$ mit $x \notin \mathfrak{a}$. Wegen letzterem gilt also für die Restklasse $[x] \in R/\mathfrak{a}$, dass $[x] \neq [0]$, also hat $[x]$ ein multiplikativ Inverses $[y] \in R/\mathfrak{a}$, für das also $[xy] = [1]$ bzw. $[1 - xy] = [0]$ gilt. Anders gesagt gibt es ein $y \in R$ mit $1 - xy \in \mathfrak{a}$ und daher auch $1 - xy \in \mathfrak{b}$. Folglich ist also

$$1 = \underbrace{1 - xy}_{\in \mathfrak{b}} + \underbrace{x}_{\in \mathfrak{b}} \cdot \underbrace{y}_{\in R} \in \mathfrak{b}$$

und somit $\mathfrak{b} = R$, weshalb \mathfrak{a} ein maximales Ideal ist (siehe Bemerkung 3.49). \square

Korollar 3.52. Sei R ein kommutativer Ring mit Eins. Dann ist jedes maximale Ideal $\mathfrak{m} \triangleleft R$ ein Primideal.

Beweis. Nach Satz 3.51 ist R/\mathfrak{m} ein Körper, also insbesondere nullteilerfrei. Daher ist \mathfrak{m} nach Satz 3.47 ein Primideal. \square

Einschub: Das Lemma von Zorn Im Beweis des folgenden Satzes (und auch später in dieser Vorlesung noch einmal) werden wir das *Lemma von Zorn* verwenden, welches wir hier kurz formulieren.

Zunächst ein paar Begriffe:

- Eine *partiell geordnete Menge* ist eine Menge M zusammen mit einer Relation \leq auf M , für die gilt:

- (1) $\forall x \in M : x \leq x$, (Reflexivität)
- (2) $\forall x, y, z \in M : (x \leq y \wedge y \leq z) \Rightarrow x \leq z$, (Transitivität)
- (3) $\forall x, y \in M : (x \leq y \wedge y \leq x) \Rightarrow x = y$. (Antisymmetrie)

Sei nun (M, \leq) immer eine partiell geordnete Menge.

- Eine Teilmenge $T \subseteq M$ heißt *total geordnet*, falls gilt:

$$\forall x, y \in T : x \leq y \vee y \leq x.$$

- Eine *obere Schranke* einer Teilmenge $A \subseteq M$ ist ein Element $s \in M$, sodass gilt:

$$\forall x \in A : x \leq s.$$

(Man beachte, dass das Element s nicht in A liegen muss!)

- Ein *maximales Element* von M ist ein Element $m \in M$, sodass gilt:

$$\forall x \in M : m \leq x \Rightarrow m = x.$$

Lemma 3.53 (Lemma von Zorn). *Sei (M, \leq) eine partiell geordnete Menge, sodass jede total geordnete Teilmenge eine obere Schranke in M besitzt. Dann gibt es ein maximales Element in M .*

Wir werden das Lemma von Zorn nicht beweisen. Man kann zeigen, dass es äquivalent zum Auswahlaxiom ist.

Der folgende Satz illustriert eine Anwendung des Lemmas von Zorn.

Satz 3.54. *Sei R ein kommutativer Ring mit Eins und $\mathfrak{a} \triangleleft R$ ein echtes Ideal. Dann gibt es ein maximales Ideal $\mathfrak{m} \triangleleft R$ mit $\mathfrak{a} \subseteq \mathfrak{m}$.*

Beweis. Wir betrachten die Menge aller echten Ideale, die \mathfrak{a} enthalten:

$$M := \{\mathfrak{b} \triangleleft R \mid \mathfrak{a} \subseteq \mathfrak{b} \subsetneq R\}.$$

Diese Menge ist partiell geordnet durch die Relation $\mathfrak{b} \leq \mathfrak{b}' :\Leftrightarrow \mathfrak{b} \subseteq \mathfrak{b}'$.

Damit wir das Lemma von Zorn anwenden können, müssen wir noch die folgende Behauptung zeigen.

Behauptung: Eine beliebige totalgeordnete Teilmenge $K \subseteq M$ hat eine obere Schranke in M .

Diese obere Schranke ist gegeben durch

$$\tilde{\mathfrak{b}} := \bigcup_{\mathfrak{b} \in K} \mathfrak{b}.$$

Es ist noch zu zeigen, dass dies wirklich ein Element in M ist, also dass $\tilde{\mathfrak{b}}$ ein echtes Ideal in R ist und dass $\mathfrak{a} \subseteq \tilde{\mathfrak{b}}$.

Kapitel 3 Ringtheorie

$\tilde{b} \triangleleft R$: Seien $x, y \in \tilde{b}$. Nach Definition von \tilde{b} gibt es also $b, b' \in K$ mit $x \in b$ und $y \in b'$. Außerdem gilt, da K totalgeordnet ist, $b \subseteq b'$ oder $b' \subseteq b$. Wir nehmen ohne Beschränkung der Allgemeinheit $b \subseteq b'$ an. Dann ist also $x, y \in b'$ und daher $x + y \in b'$, denn b' ist ein Ideal. Da aber $b' \subseteq \tilde{b}$, erhalten wir wie gewünscht $x + y \in \tilde{b}$. Genauso erhalten wir für beliebiges $r \in R$, dass $rx \in b$ und daher $rx \in \tilde{b}$.

$\tilde{b} \neq R$: Da für jedes $b \in K$ gilt, dass $b \neq R$, also insbesondere $1 \notin b$, folgt auch $1 \notin \tilde{b}$ und somit $\tilde{b} \neq R$.

$\mathfrak{a} \subseteq \tilde{b}$: Es gilt $\mathfrak{a} \subseteq b$ für alle $b \in K$, daher auch $\mathfrak{a} \subseteq \tilde{b}$.

Damit ist die Behauptung bewiesen.

Das Lemma von Zorn sagt uns nun also, dass die Menge M ein maximales Element hat, dass es also ein echtes Ideal in R gibt, welches \mathfrak{a} enthält und welches auch alle anderen Ideale, in denen \mathfrak{a} enthalten ist, enthält. Dieses maximale Element von M ist daher ein maximales Ideal in R mit $\mathfrak{a} \subseteq \mathfrak{m}$. \square

3.7 Der Chinesische Restsatz

Wir werden jetzt einen berühmten und grundlegenden Satz kennenlernen, der uns in seiner Version über den ganzen Zahlen ($R = \mathbb{Z}$) eine ganz alltägliche Frage beantwortet: Kennt man von einer Zahl $x \in \mathbb{Z}$ nur die Reste bei Division mit Rest durch gewisse andere Zahlen a_1, \dots, a_n (d.h. nur die Restklassen $[a] \in \mathbb{Z}/a_j\mathbb{Z}$), inwieweit legen diese Informationen die Zahl a bereits fest?

Wir werden diesen Satz in zwei Versionen (einer expliziteren und einer abstrakteren, aber dafür etwas allgemeineren und ringtheoretisch nützlichen) formulieren. Dazu benötigen wir zunächst einen neuen Begriff.

Definition 3.55. Sei R ein kommutativer Ring mit Eins. Dann heißen zwei Ideale $\mathfrak{a}, \mathfrak{b} \triangleleft R$ *teilerfremd*, falls gilt:

$$\mathfrak{a} + \mathfrak{b} = R.$$

Hierbei ist $\mathfrak{a} + \mathfrak{b} := \{a + b \mid a \in \mathfrak{a}, b \in \mathfrak{b}\}$.

Beispiel 3.56. Der Begriff *teilerfremd* ist motiviert durch Teilerfremdheit im Ring der ganzen Zahlen:

Sind $(n), (m) \triangleleft \mathbb{Z}$ zwei Ideale und n, m sind teilerfremde Zahlen (d.h. $\text{ggT}(n, m) = 1$), dann gibt es eine Bézout-Darstellung $an + bm = 1$. Dies bedeutet aber, dass $1 \in (n) + (m)$, also $(n) + (m) = R$.

Umgekehrt kann man sich überlegen, dass $(n) + (m) \subseteq (\text{ggT}(n, m))$. Sind also n und m nicht teilerfremd, so ist $(n) + (m) \neq R$.

Notation 3.57. Bevor wir den Chinesischen Restsatz formulieren, klären wir noch kurz folgende Notation:

Ist R ein Ring und \mathfrak{a} ein Ideal, so schreiben wir für eine Äquivalenzklasse $[x] \in R/\mathfrak{a}$ manchmal auch „ $x \bmod \mathfrak{a}$ “, um zu betonen, bezüglich welches Ideals die Restklasse betrachtet wird. (Eine weitere verbreitete Schreibweise ist $[x] = x + \mathfrak{a}$.) Dies wird insbesondere wichtig sein, da wir in den folgenden Sätzen oft mehrere verschiedene Quotienten von R gleichzeitig betrachten.

Genauso schreiben wir

$$x \equiv y \pmod{\mathfrak{a}}$$

anstelle von $[x] = [y]$ für zwei Elemente $x, y \in R$, um zu betonen, dass sie modulo \mathfrak{a} äquivalent sind.

Satz 3.58 (Chinesischer Restsatz über simultane Kongruenzen). *Sei R ein kommutativer Ring mit Eins und seien $\mathfrak{a}_1, \dots, \mathfrak{a}_n \triangleleft R$ paarweise teilerfremde Ideale in R . Seien $x_1, \dots, x_n \in R$ beliebige Elemente. Dann gibt es ein $x \in R$, sodass gilt*

$$\begin{aligned} x &\equiv x_1 \pmod{\mathfrak{a}_1} \\ x &\equiv x_2 \pmod{\mathfrak{a}_2} \\ &\vdots \\ x &\equiv x_n \pmod{\mathfrak{a}_n}. \end{aligned}$$

Beweis. Wir zeigen zunächst die folgende Hilfsaussage.

Behauptung: Für jedes $j \in \{1, \dots, n\}$ gibt es ein $s_j \in R$ mit

$$\begin{aligned} s_j &\equiv 1 \pmod{\mathfrak{a}_j}, \\ s_j &\equiv 0 \pmod{\mathfrak{a}_i} \quad \text{für alle } i \in \{1, \dots, n\}, i \neq j. \end{aligned}$$

Sei also $j \in \{1, \dots, n\}$ fest gewählt. Für jedes $k \in \{1, \dots, n\}$ mit $k \neq j$ sind die Ideale \mathfrak{a}_k und \mathfrak{a}_j teilerfremd, d.h. wir können Elemente $a_k \in \mathfrak{a}_k$ und $b_k \in \mathfrak{a}_j$ wählen mit $a_k + b_k = 1$. Dann setzen wir

$$s_j := \prod_{\substack{k \in \{1, \dots, n\} \\ k \neq j}} a_k \in R.$$

Dieses Element erfüllt

$$s_j = \prod_{\substack{k \in \{1, \dots, n\} \\ k \neq j}} (1 - b_k) \equiv \prod_{\substack{k \in \{1, \dots, n\} \\ k \neq j}} 1 = 1 \pmod{\mathfrak{a}_j},$$

da $b_k \in \mathfrak{a}_j$ und somit $b_k \equiv 0 \pmod{\mathfrak{a}_j}$. Außerdem gilt für jedes $i \in \{1, \dots, n\}$ mit $i \neq j$

$$s_j = \underbrace{a_i}_{\in \mathfrak{a}_i} \cdot \underbrace{\prod_{\substack{k \in \{1, \dots, n\} \\ k \neq j, k \neq i}} a_k}_{\in R} \in \mathfrak{a}_i,$$

also $s_j \equiv 0 \pmod{\mathfrak{a}_i}$. Somit erfüllt dieses s_j die gewünschten Eigenschaften.

Kapitel 3 Ringtheorie

Wir benutzen jetzt die Elemente s_j aus der Behauptung und setzen

$$x := x_1s_1 + x_2s_2 + \dots + x_ns_n.$$

Dies ist ein gesuchtes Element, denn es gilt offensichtlich

$$x \equiv x_k \pmod{a_k}$$

für jedes $k \in \{1, \dots, n\}$. □

Satz 3.59 (Chinesischer Restsatz als Ringisomorphismus). *Sei R ein kommutativer Ring mit Eins und seien $a_1, \dots, a_n \triangleleft R$ paarweise teilerfremde Ideale in R , dann definiert*

$$\begin{aligned} \Psi: R / \bigcap_{j=1}^n a_j &\rightarrow R/a_1 \times R/a_2 \times \dots \times R/a_n \\ x \pmod{\bigcap_{j=1}^n a_j} &\mapsto (x \pmod{a_1}, x \pmod{a_2}, \dots, x \pmod{a_n}) \end{aligned}$$

einen Isomorphismus von Ringen.

Beweis. Die Abbildung

$$\psi: R \rightarrow R/a_1 \times R/a_2 \times \dots \times R/a_n, \quad x \mapsto (x \pmod{a_1}, x \pmod{a_2}, \dots, x \pmod{a_n})$$

ist ein Ringhomomorphismus (denn sie ist komponentenweise die kanonische Projektion $R \rightarrow R/a_j$). Satz 3.58 besagt gerade, dass ψ surjektiv ist. Außerdem ist ihr Kern

$$\begin{aligned} \ker(\psi) &= \{x \in R \mid x \equiv 0 \pmod{a_j} \text{ für alle } j \in \{1, \dots, n\}\} \\ &= \{x \in R \mid x \in a_j \text{ für alle } j \in \{1, \dots, n\}\} \\ &= \bigcap_{j=1}^n a_j. \end{aligned}$$

Daher ist die induzierte Abbildung

$$\Psi = \bar{\psi}: R / \bigcap_{j=1}^n a_j \rightarrow R/a_1 \times R/a_2 \times \dots \times R/a_n$$

nach dem Homomorphiesatz (Satz 3.22) ein Ringisomorphismus. □

Beispiel 3.60. Denken wir noch einmal darüber nach, was der Chinesische Restsatz nun genau über \mathbb{Z} aussagt: Gesucht sei eine (noch unbekannte) ganze Zahl $x \in \mathbb{Z}$, sodass

$$\begin{aligned} x &\equiv x_1 \pmod{a_1} \\ x &\equiv x_2 \pmod{a_2} \\ &\vdots \\ x &\equiv x_n \pmod{a_n} \end{aligned}$$

für bestimmte (bekannte) $x_1, \dots, x_n \in \mathbb{Z}$ sowie paarweise teilerfremde $a_1, \dots, a_n \in \mathbb{Z}$. Dann gibt es eine Zahl $x \in \mathbb{Z}$, die alle diese Kongruenzen erfüllt (nach Satz 3.58). Diese Zahl ist nicht eindeutig. Nach Satz 3.59 gehört sie aber zu einem eindeutig bestimmten Element in $\mathbb{Z}/\bigcap_{j=1}^n (a_j)$. Man überlegt sich leicht, dass $\bigcap_{j=1}^n (a_j) = (a_1 \cdot \dots \cdot a_n)$. Das Element x ist also eindeutig bis auf Vielfache der Zahl $a_1 \cdot \dots \cdot a_n$. Der Beweis von Satz 3.58 gibt uns auch eine Methode, wie wir ein solches x finden, nämlich indem wir Bézout-Darstellungen für je zwei Elemente a_i und a_j bestimmen, welche wir wiederum mit dem Euklidischen Algorithmus 3.44 berechnen können.

3.8 Primelemente und irreduzible Elemente

Eine wichtige Eigenschaft der ganzen Zahlen ist die Existenz einer eindeutigen Zerlegung in Primfaktoren für jedes Element. Um solche Eigenschaften für allgemeinere Ringe zu untersuchen, muss man sich zunächst überlegen, welche Elemente die Rolle der Primzahlen übernehmen sollen.

Definition 3.61. Sei R ein kommutativer Ring mit Eins.

Ein Element $p \in R$ heißt **Primelement**, falls $p \neq 0$ und $p \notin R^\times$ und falls für alle $x, y \in R$ gilt

$$p \mid xy \Rightarrow (p \mid x \vee p \mid y).$$

Ein Element $\pi \in R$ heißt **irreduzibel**, falls $\pi \neq 0$ und $\pi \notin R^\times$ und falls für alle $x, y \in R$ gilt

$$\pi = xy \Rightarrow (x \in R^\times \vee y \in R^\times).$$

Bemerkung 3.62. Beide Definitionen entsprechen unserer Vorstellung von „Primzahlen“ in \mathbb{Z} : Die Definition eines Primelements besagt, dass, wenn p ein Produkt zweier Elemente teilt, es dann bereits einen der Faktoren teilen muss (da sich p als „Primzahl“ eben nicht weiter „aufspalten“ und auf die beiden Faktoren „verteilen“ kann). Die Definition eines irreduziblen Elements besagt, dass sich p nicht als Produkt zweier anderer Elemente schreiben lässt, außer auf triviale Weise, wenn einer der Faktoren eine Einheit ist (man kann ja in \mathbb{Z} zum Beispiel immer schreiben $3 = 3 \cdot 1$ oder $3 = (-3) \cdot (-1)$, aber das soll eben nicht als „echte“ Zerlegung gelten).

In \mathbb{Z} sind die beiden Definitionen also äquivalent, d.h. jedes Primelement ist irreduzibel und umgekehrt. Im Allgemeinen sind die beiden Begriffe aber verschieden und wir werden im Folgenden untersuchen, wie sie zusammenhängen.

Lemma 3.63. Ein Element $r \in R$ ist genau dann ein Primelement, wenn $r \neq 0$ und $(r) \triangleleft R$ ein Primideal ist.

Beweis. Man überlegt sich, dass $r \mid x$ gleichbedeutend ist mit $x \in (r)$. Damit sieht man, dass die Definition eines Primelements und die Definition eines Primideals (Definition 3.45) für den Fall $\mathfrak{a} = (r)$ äquivalent sind. Es ist nur der Fall $r = 0$ auszuschließen, da dieser in Definition 3.45 erlaubt ist. \square

Lemma 3.64. Sei R ein Integritätsbereich. Ist $p \in R$ ein Primelement, so ist p irreduzibel.

Kapitel 3 Ringtheorie

Beweis. Sei $p \in R$ ein Primelement. Wir nehmen an, dass sich p schreiben lässt als Produkt $p = xy$ für gewisse $x, y \in R$. Es gilt dann offensichtlich $p \mid xy$ (jedes Element teilt sich selbst). Da p ein Primelement ist, folgt also $p \mid x$ oder $p \mid y$. Wir nehmen ohne Beschränkung der Allgemeinheit an, dass $p \mid y$, dass es also ein $r \in R$ gibt mit $y = rp$. Dann folgt $p = xy = xrp$ und somit

$$0 = p - xrp = (1 - xr)p.$$

Da R ein Integritätsbereich und p ein Primelement, also insbesondere $p \neq 0$ ist, folgt daraus $1 - xr = 0$ und somit $1 = xr$, also ist $x \in R^\times$ eine Einheit. Dies beweist, dass p irreduzibel ist. \square

Nun wollen wir eine Aussage ähnlich zu Lemma 3.63 auch für irreduzible Elemente formulieren. Für die „genau dann“-Richtung benötigen wir hier aber eine zusätzliche Annahme, nämlich dass R ein Hauptidealring ist.

Lemma 3.65. *Ist $\pi \in R \setminus \{0\}$ ein Element, sodass $(\pi) \triangleleft R$ ein maximales Ideal ist, so ist π irreduzibel.*

Ist R ein Hauptidealring, so gilt auch die Umkehrung: Ist $\pi \in R$ irreduzibel, dann ist $(\pi) \triangleleft R$ ein maximales Ideal.

Beweis. Sei $(\pi) \triangleleft R$ ein maximales Ideal. Wir wollen zeigen, dass π irreduzibel ist. Sei also $\pi = xy$ für gewisse $x, y \in R$. Betrachte dann das Ideal $(y) \triangleleft R$. Wegen $\pi = xy$ gilt $\pi \in (y)$ und somit

$$(\pi) \subseteq (y) \subseteq R.$$

Nun ist (π) aber ein maximales Ideal, also muss entweder $(\pi) = (y)$ oder $(y) = R$ gelten. (Es gibt keine echten Ideale zwischen (π) und R .)

Im ersten Fall folgt also $y \in (\pi)$, d.h. es gibt ein $r \in R$ mit $y = r\pi$. Daraus ergibt sich $\pi = xy = xr\pi$, also

$$0 = \pi - xr\pi = (1 - xr)\pi.$$

Da R ein Integritätsbereich ist und $\pi \neq 0$, folgt $1 - xr = 0$, also $1 = xr$. Dies impliziert $x \in R^\times$.

Im zweiten Fall gilt $(y) = R$, also insbesondere $1 \in (y)$. Es gibt also ein $r \in R$ mit $ry = 1$, also ist $y \in R^\times$.

Sei umgekehrt $\pi \in R$ ein irreduzibles Element und sei R nun zusätzlich ein Hauptidealring. Dann wollen wir zeigen, dass $(\pi) \triangleleft R$ ein maximales Ideal ist. Sei also $\mathfrak{a} \triangleleft R$ ein weiteres Ideal mit

$$(\pi) \subseteq \mathfrak{a} \subsetneq R.$$

Da R ein Hauptidealring ist, können wir schreiben $\mathfrak{a} = (a)$ für ein $a \in R$. Da $(\pi) \subseteq (a)$, gilt insbesondere $\pi \in (a)$, also existiert ein $r \in R$ mit $\pi = ra$. Da π irreduzibel ist, folgt nun $r \in R^\times$ oder $a \in R^\times$. Letzteres ist aber nicht möglich, denn wäre $a \in R^\times$, dann wäre auch $1 \in (a)$, also $(a) = R$, was wir oben ausgeschlossen haben. Also muss

$r \in R^\times$ eine Einheit sein. Dann ist aber $a = r^{-1}\pi$, also $a \in (\pi)$ und somit $(a) \subseteq (\pi)$. Damit haben wir insgesamt $(\pi) = (a)$ und dies zeigt, dass (π) ein maximales Ideal ist. \square

Korollar 3.66. *Ist R ein Hauptidealring, so ist jedes irreduzible Element $\pi \in R$ ein Primelement.*

Beweis. Ist $\pi \in R$ irreduzibel, so ist $(\pi) \triangleleft R$ nach Lemma 3.65 ein maximales Ideal (hier geht die Voraussetzung ein, dass R ein Hauptidealring ist). Somit ist $(\pi) \triangleleft R$ auch ein Primideal nach Korollar 3.52 und folglich ist π nach Lemma 3.63 ein Primelement. \square

Insbesondere haben wir also nun gesehen, dass in einem Hauptidealbereich (d.h. in einem Ring, der sowohl Integritätsbereich als auch Hauptidealring ist) die Begriffe *Primelement* und *irreduzibles Element* zusammenfallen. Allgemeiner gilt dies noch in einer größeren Klasse von Ringen, die wir im folgenden Abschnitt einführen werden.

3.9 Faktorielle Ringe

Wir wollen jetzt Ringe definieren und untersuchen, in denen eine Art „eindeutige Primfaktorzerlegung“ existiert.

Definition 3.67. Ein *faktorieller Ring* ist ein Integritätsbereich R , in dem folgende Eigenschaft erfüllt ist: Für jedes $r \in R \setminus (\{0\} \cup R^\times)$ gibt es eine Zerlegung

$$r = \pi_1 \cdot \dots \cdot \pi_m$$

in ein Produkt irreduzibler Elemente $\pi_1, \dots, \pi_m \in R$, wobei diese irreduziblen Elemente bis auf ihre Reihenfolge und Multiplikation mit Einheiten eindeutig bestimmt sind.

Bemerkung 3.68. Wir machen uns kurz Gedanken, was diese „Eindeutigkeit bis auf Reihenfolge und Multiplikation mit Einheiten“ genau bedeutet. Gemeint ist damit das Folgende: Hat man für ein Element $r \in R$ zwei Zerlegungen

$$r = \pi_1 \cdot \dots \cdot \pi_m = \tilde{\pi}_1 \cdot \dots \cdot \tilde{\pi}_n$$

in irreduzible Elemente $\pi_1, \dots, \pi_m, \tilde{\pi}_1, \dots, \tilde{\pi}_n \in R$, dann muss gelten:

- (a) $n = m$, d.h. die Zerlegungen bestehen aus gleich vielen Faktoren und
- (b) man kann die Faktoren $\tilde{\pi}_1, \dots, \tilde{\pi}_n$ so umnummerieren, dass es Einheiten $\varepsilon_1, \dots, \varepsilon_m \in R^\times$ gibt mit

$$\pi_1 = \varepsilon_1 \cdot \tilde{\pi}_1, \dots, \pi_m = \varepsilon_m \cdot \tilde{\pi}_m.$$

Kapitel 3 Ringtheorie

Um dieses „bis auf Multiplikation mit Einheiten“ etwas kürzer zu schreiben, benutzt man manchmal den folgenden Begriff: Zwei Elemente $r, r' \in R$ heißen *assoziert*, falls es ein $\varepsilon \in R^\times$ gibt mit $r = \varepsilon \cdot r'$. Man schreibt dann $r \sim r'$. (Wie man leicht sieht, definiert dies eine Äquivalenzrelation auf R .)

Die Bedingung (b) von oben lässt sich dann auch so formulieren:

$$\exists \sigma \in S_m \forall i \in \{1, \dots, m\} : \pi_i \sim \tilde{\pi}_{\sigma(i)}.$$

In obiger Definition wird eine Zerlegung in irreduzible Elemente gefordert. Die folgenden beiden Sätze zeigen aber, dass man den Begriff des faktoriellen Rings auch mithilfe von Primelementen definieren kann und dass in faktoriellen Ringen die Begriffe „prim“ und „irreduzibel“ zusammenfallen.

Satz 3.69. *Sei R ein Integritätsbereich, sodass es für jedes Element $r \in R \setminus (\{0\} \cup R^\times)$ eine Zerlegung*

$$r = p_1 \cdot \dots \cdot p_m$$

in ein Produkt von Primelementen $p_1, \dots, p_m \in R$ gibt. Dann ist R ein faktorieller Ring.

Beachte, dass in diesem Satz nur eine Zerlegung, nicht aber irgendeine Form von Eindeutigkeit gefordert wird!

Beweis. Sei $r \in R \setminus (\{0\} \cup R^\times)$, dann gibt es nach Voraussetzung eine Zerlegung

$$r = p_1 \cdot \dots \cdot p_m$$

für Primelemente $p_1, \dots, p_m \in R$. Da Primelemente nach Lemma 3.64 auch irreduzibel sind, folgt sofort, dass dies auch eine Zerlegung in ein Produkt irreduzibler Elemente ist. Zu zeigen ist also noch die Eindeutigkeit der irreduziblen Faktoren (bis auf Reihenfolge und Multiplikation mit Einheiten) wie in Definition 3.67.

Sei also $r = \pi_1 \cdot \dots \cdot \pi_n$ eine andere Zerlegung von r in ein Produkt irreduzibler Elemente $\pi_1, \dots, \pi_n \in R$ (diese müssen nun nicht unbedingt prim sein). Da $p_1 \cdot \dots \cdot p_m = \pi_1 \cdot \dots \cdot \pi_n$, gilt $p_1 \mid \pi_1 \cdot \dots \cdot \pi_n$, und da p_1 ein Primelement ist, folgt $p_1 \mid \pi_j$ für ein $j \in \{1, \dots, n\}$. Wir können die π_j so umnummerieren, dass $p_1 \mid \pi_1$ gilt (denn wir wollen am Ende ja nur Eindeutigkeit bis auf Reihenfolge). Es gibt dann also ein $r \in R$ mit $\pi_1 = r p_1$ und somit muss $r \in R^\times$ oder $p_1 \in R^\times$, da π_1 irreduzibel ist. Da Primelemente aber nach Definition niemals Einheiten sind, kommt nur $r \in R^\times$ in Frage. Es folgt also $p_1 \sim \pi_1$ und

$$p_1 \cdot \dots \cdot p_m = r p_1 \cdot \pi_2 \cdot \dots \cdot \pi_n.$$

Hier können wir p_1 auf beiden Seiten kürzen (da R ein Integritätsbereich ist). Außerdem können wir $r \pi_2$ in π_2 umbenennen (da wir uns am Ende ja nur für Eindeutigkeit bis auf Einheiten interessieren) und erhalten

$$p_2 \cdot \dots \cdot p_m = \pi_2 \cdot \dots \cdot \pi_n.$$

Nun wiederholen wir dies so oft, bis alle Faktoren verbraucht sind. In jedem Schritt erhalten wir (nach evtl. Umnummerierung) $p_j \sim \pi_j$ und man sieht leicht, dass $m = n$ sein muss, da sonst am Ende auf einer Seite nur eine Einheit, auf der anderen Seite aber ein irreduzibles Element übrigbleiben würde, was nicht möglich ist, da irreduzible Elemente nach Definition keine Einheiten sind.

Insgesamt haben wir somit gezeigt, dass die beiden Zerlegungen die gleiche Anzahl an Faktoren enthalten und die Faktoren paarweise zueinander assoziiert sind, sich also nur durch Reihenfolge und Multiplikation mit Einheiten unterscheiden. \square

Satz 3.70. *Sei R ein faktorieller Ring, dann ist jedes irreduzible Element ein Primelement.*

Beweis. Sei $\pi \in R$ irreduzibel und seien $x, y \in R$ mit $\pi \mid xy$. Dann gibt es also ein $r \in R$ mit $r\pi = xy$. Falls $x = 0$ oder $y = 0$, folgt direkt $\pi \mid x$ oder $\pi \mid y$. Falls $x \in R^\times$ oder $y \in R^\times$, folgt $\pi \mid y$ oder $\pi \mid x$. Andernfalls können wir, da R faktoriell ist, schreiben $x = \pi_1 \cdot \dots \cdot \pi_m$, $y = \rho_1 \cdot \dots \cdot \rho_n$, $r = \sigma_1 \cdot \dots \cdot \sigma_k$ für (bis auf Reihenfolge und Multiplikation mit Einheiten) eindeutige irreduzible Faktoren. Es gilt also

$$\sigma_1 \cdot \dots \cdot \sigma_k \cdot \pi = \pi_1 \cdot \dots \cdot \pi_m \cdot \rho_1 \cdot \dots \cdot \rho_n.$$

Da alle Faktoren auf der linken und rechten Seite irreduzibel sind und Zerlegungen in irreduzible Faktoren in R eindeutig (bis auf die bekannten Ambiguitäten) sind, folgt, dass $\pi \sim \pi_i$ für ein $i \in \{1, \dots, m\}$ oder $\pi \sim \rho_j$ für ein $j \in \{1, \dots, n\}$. Ersteres bedeutet aber $\pi \mid x$, zweiteres bedeutet $\pi \mid y$. Somit ist π ein Primelement.

(Bemerkung: Das Element r könnte auch eine Einheit sein, dann gibt es keine Zerlegung $r = \sigma_1 \cdot \dots \cdot \sigma_k$, aber das Argument funktioniert trotzdem.) \square

Beispiele für faktorielle Ringe kennen wir bereits, denn unsere beiden wichtigsten Beispiele \mathbb{Z} und $K[X]$ sind nach dem folgenden Satz faktorielle Ringe.

Satz 3.71. *Jeder Hauptidealbereich ist ein faktorieller Ring.*

Beweis. Sei R ein Hauptidealbereich und sei $r \in R \setminus (R^\times \cup \{0\})$ ein beliebiges Element. Wir müssen zeigen, dass r eine Zerlegung in Primelemente hat, dann folgt mit Satz 3.69, dass R faktoriell ist. Nach Korollar 3.66 ist jedes irreduzible Element in R auch prim, also genügt es zu zeigen, dass r eine Zerlegung in irreduzible Elemente besitzt (ohne über die Eindeutigkeit nachdenken zu müssen). Wir zeigen zunächst eine Hilfsaussage.

Behauptung: Jedes Element $r \in R \setminus (R^\times \cup \{0\})$ hat mindestens einen irreduziblen Teiler.

Angenommen, dies wäre nicht der Fall. Dann wäre r selbst nicht irreduzibel (sonst wäre es ein irreduzibler Teiler von sich selbst), also kann man schreiben $r = xy$ für gewisse $x, y \in R \setminus R^\times$, wobei auch x und y nicht irreduzibel sind

Kapitel 3 Ringtheorie

und selbst wiederum keine irreduziblen Teiler haben (sonst hätte ja auch r einen solchen). Dann setzen wir $a_1 := x$ und haben

$$(r) \subsetneq (a_1).$$

(Gleichheit kann nicht eintreten, da $y \notin R^\times$.)

Dasselbe Argument können wir nun mit a_1 statt r durchführen: Wir zerlegen $a_1 = x'y'$ passend und erhalten $(a_1) \subsetneq (a_2)$. Sukzessive haben wir also eine unendliche aufsteigende Kette von Idealen

$$(r) \subsetneq (a_1) \subsetneq (a_2) \subsetneq (a_3) \subsetneq \dots$$

Die Vereinigung $\mathfrak{a} := \bigcup_{i=1}^{\infty} (a_i) \subseteq R$ ist wieder ein Ideal. (Dass die Vereinigung aller Ideale in einer aufsteigenden Kette wieder ein Ideal ist, haben wir auch im Beweis von Satz 3.54 schon einmal nachgeprüft.) Nun ist aber R ein Hauptidealring, also gilt $\mathfrak{a} = (a)$ für ein $a \in R$. Da \mathfrak{a} die Vereinigung aller (a_i) ist, muss gelten $a \in (a_i)$ für ein bestimmtes $i \in \mathbb{N}$. Es gilt dann aber

$$(a) \subseteq (a_i) \subsetneq (a_{i+1}) \subseteq \mathfrak{a} = (a).$$

Das ist ein Widerspruch.

Nach der eben gezeigten Behauptung hat also r einen irreduziblen Teiler, wir können also schreiben $r = \pi_1 \cdot b_1$ für ein irreduzibles $\pi_1 \in R$ und ein $b_1 \in R$. Ist nun $b_1 \in R^\times$, dann sind wir fertig, denn dann ist auch $\pi_1 \cdot b_1$ irreduzibel und wir haben eine Zerlegung von r in irreduzible Faktoren gefunden. Andernfalls können wir b_1 (wieder nach der obigen Behauptung) weiter zerlegen in $b_1 = \pi_2 \cdot b_2$ für irreduzibles $\pi_2 \in R$ und $b_2 \in R$. Man erhält also sukzessive eine Zerlegung

$$r = \pi_1 \cdot \pi_2 \cdot \dots \cdot \pi_m \cdot b_m.$$

Wir müssen uns nur noch überlegen, dass dieser Prozess terminiert, dass also nach endlich vielen Schritten $b_m \in R^\times$ gilt und wir somit die gewünschte Zerlegung von r in irreduzible Elemente erhalten haben: Würde nie $b_m \in R^\times$ gelten, so hätten wir eine aufsteigende Kette von Idealen

$$(b_1) \subsetneq (b_2) \subsetneq (b_3) \subsetneq \dots$$

(denn für jedes $i \in \mathbb{N}$ ist $b_i = \pi_{i+1} b_{i+1}$ mit $\pi_{i+1} \notin R^\times$). Solch eine unendliche Kette von Idealen kann es aber (mit dem gleichen Argument wie im Beweis der obigen Behauptung) nicht geben. \square

Faktorielle Ringe sind also allgemeiner als Hauptideal- und euklidische Ringe. Sie erlauben uns aber immer noch, einen größten gemeinsamen Teiler zweier Elemente zu finden.

Lemma 3.72. Sei R ein faktorieller Ring. Seien $x, y \in R$ zwei Elemente, von denen mindestens eines nicht 0 ist. Dann gibt es einen größten gemeinsamen Teiler von x und y .

Beweis. Falls eines der beiden Elemente gleich 0 ist (sagen wir $y = 0$), dann ist $\text{ggT}(x, y) = x$.

Falls beide ungleich 0 sind, aber eines der beiden Elemente eine Einheit ist, gilt $\text{ggT}(x, y) = 1$.

Andernfalls (wenn also $x, y \in R \setminus (\{0\} \cup R^\times)$), gibt es Zerlegungen von x und y in ein Produkt irreduzibler Elemente. Natürlich kann derselbe Faktor in solch einer Zerlegung auch mehrmals vorkommen (oder es können mehrere Faktoren assoziiert zueinander sein). In diesem Fall fassen wir gleiche Faktoren zu einer Potenz zusammen (und sorgen durch geschicktes Hin- und Herschieben von Einheiten dafür, dass die irreduziblen Faktoren paarweise nicht zueinander assoziiert sind) und schreiben

$$x = \pi_1^{\mu_1} \cdot \dots \cdot \pi_m^{\mu_m}, \quad y = \varepsilon \cdot \pi_1^{\nu_1} \cdot \dots \cdot \pi_m^{\nu_m},$$

wobei $\pi_1, \dots, \pi_m \in R$ irreduzibel sind und $\varepsilon \in R^\times$ eine Einheit ist. Man beachte, dass wir hier in beiden Darstellungen dieselben Faktoren π_1, \dots, π_m verwenden (aber natürlich mit möglicherweise unterschiedlichen Potenzen). Dies können wir tun, indem wir einfach alle Faktoren, die in einer der beiden Zerlegungen eigentlich nicht auftauchen, mit $\nu_i = 0$ im Exponenten hinzufügen.

Der größte gemeinsame Teiler von x und y ist dann gegeben durch

$$d := \pi_1^{\min\{\mu_1, \nu_1\}} \cdot \dots \cdot \pi_m^{\min\{\mu_m, \nu_m\}},$$

wie man sich leicht überlegt. □

Bemerkung 3.73. Neben dem größten gemeinsamen Teiler gibt es auch den Begriff des *kleinsten gemeinsamen Vielfachen* (kgV), den man in einem allgemeinen kommutativen Ring mit Eins definieren kann: Sind $x, y \in R \setminus \{0\}$, so heißt ein Element $m \in R$ *kleinstes gemeinsames Vielfaches* von x und y , geschrieben $m = \text{kgV}(x, y)$, falls gilt:

- (1) $x \mid m$ und $y \mid m$,
- (2) $\forall s \in R : (x \mid s \wedge y \mid s) \Rightarrow m \mid s$.

Ähnlich wie im gerade bewiesenen Lemma 3.72 kann man auch sehen, dass kleinste gemeinsame Vielfache zweier Elemente $x, y \neq 0$ in einem faktoriellen Ring immer existieren. Man muss dazu im Beweis einfach alle Minima durch Maxima ersetzen.

3.10 Quotientenkörper

Blicken wir auf die Definition eines Körpers zurück, so stellen wir fest, dass es einem Integritätsbereich – falls er nicht selbst schon ein Körper ist – nur an einer Eigenschaft fehlt, um ein Körper zu sein: der Existenz von multiplikativ Inversen für

Kapitel 3 Ringtheorie

jedes Element außer der Null. Bei der Zahlbereichserweiterung von \mathbb{Z} nach \mathbb{Q} haben wir uns diese Inversen einfach „erfunden“, nämlich indem wir eine rationale Zahl als Bruch $\frac{a}{b}$ aus zwei ganzen Zahlen schreiben, wobei der Nenner nun eine beliebige ganze Zahl außer der Null sein darf. Diese Konstruktion funktioniert tatsächlich für jeden Integritätsbereich.

Lemma-Definition 3.74. Sei R ein Integritätsbereich. Auf der Menge $R \times (R \setminus \{0\})$ wird durch

$$(a, b) \sim (a', b') :\Leftrightarrow ab' = a'b$$

eine Äquivalenzrelation definiert.

Ist $(a, b) \in R \times (R \setminus \{0\})$, so schreiben wir

$$\frac{a}{b} := [(a, b)]$$

für die zugehörige Äquivalenzklasse und bezeichnen mit

$$\text{Quot}(R) := (R \times (R \setminus \{0\})) / \sim$$

die Menge der Äquivalenzklassen. Auf ihr wird durch

$$\frac{a}{b} + \frac{c}{d} := \frac{ad + bc}{bd} \quad \text{und} \quad \frac{a}{b} \cdot \frac{c}{d} := \frac{ac}{bd}$$

eine Addition und Multiplikation definiert, welche $\text{Quot}(R)$ zu einem Körper machen. Wir nennen $\text{Quot}(R)$ den *Quotientenkörper* von R .

Beweis. Die gegebene Relation ist eine Äquivalenzrelation, denn für beliebige Elemente $(a, b), (a', b'), (a'', b'') \in R \times (R \setminus \{0\})$ gilt:

- (1) $(a, b) \sim (a, b)$, weil $ab = ab$.
- (2) Falls $(a, b) \sim (a', b')$, d.h. $ab' = a'b$, dann gilt offensichtlich auch $(a', b') \sim (a, b)$.
- (3) Falls $(a, b) \sim (a', b')$ und $(a', b') \sim (a'', b'')$, d.h. $ab' = a'b$ und $a'b'' = a''b'$, dann folgt

$$(ab'')b' = (ab')b'' = (a'b)b'' = b(a'b'') = b(a''b') = (a''b)b',$$

also $(ab'' - a''b)b' = 0$. Da $b' \neq 0$ und R ein Integritätsbereich ist, folgt daraus $ab'' - a''b = 0$ und somit $(a, b) \sim (a'', b'')$.

Die Addition ist wohldefiniert: Seien $(a, b), (a', b'), (c, d), (c', d') \in R \times (R \setminus \{0\})$ mit $(a, b) \sim (a', b')$ und $(c, d) \sim (c', d')$ (d.h. $ab' = a'b$ und $cd' = c'd$), dann gilt auch $\frac{ad+bc}{bd} = \frac{a'd'+b'c'}{b'd'}$, denn

$$(ad + bc)b'd' = ab'dd' + bb'cd' = a'bdd' + bb'c'd = (a'd' + b'c')bd.$$

Ebenso ist die Multiplikation wohldefiniert, denn in derselben Situation wie eben gilt $\frac{ac}{bd} = \frac{a'c'}{b'd'}$ wegen

$$ac \cdot b'd' = ab'cd' = a'bc'd = a'c' \cdot bd.$$

□

Das neutrale Element der Addition in $\text{Quot}(R)$ ist offensichtlich $0 := \frac{0}{1}$, das neutrale Element der Multiplikation ist $1 := \frac{1}{1}$.

Genau wie wir das aus dem Beispiel $\mathbb{Z} \subseteq \mathbb{Q}$ kennen, finden wir auch in der allgemeinen Konstruktion den ursprünglichen Ring in seinem Quotientenkörper wieder, nämlich als diejenigen Elemente, die „keinen Nenner haben“ (d.h. bei denen 1 im Nenner steht).

Lemma 3.75. *Ist R ein Integritätsbereich, so ist*

$$R \rightarrow \text{Quot}(R), \quad r \mapsto \frac{r}{1}$$

ein injektiver Ringhomomorphismus.

Beweis. Mit der Definition der Addition und Multiplikation von Elementen des Quotientenkörpers folgt sofort, dass die Abbildung ein Ringhomomorphismus ist.

Die Abbildung ist injektiv, denn seien $r_1, r_2 \in R$ mit $\frac{r_1}{1} = \frac{r_2}{1}$, dann bedeutet dies, dass in R die Gleichung $r_1 \cdot 1 = r_2 \cdot 1$ gilt, also $r_1 = r_2$. \square

3.11 Irreduzibilität von Polynomen

In diesem Abschnitt sei R immer ein faktorieller Ring (falls nicht anders erwähnt) und $Q := \text{Quot}(R)$ sein Quotientenkörper.

Wir werden später, in der Theorie der Körpererweiterungen, oft sogenannte *Minimalpolynome* bestimmen, also „kleinstmögliche“ Polynome mit einer bestimmten Eigenschaft. Wie wir sehen werden, sind diese immer irreduzibel, weshalb wir in diesem Abschnitt noch einige Kriterien kennenlernen werden, die uns helfen, festzustellen, ob ein gegebenes Polynom irreduzibel ist – dies ist im Allgemeinen keine einfache Aufgabe!

Oft werden wir Polynome über einem Körper, zum Beispiel Polynome in $\mathbb{Q}[X]$, auf Irreduzibilität untersuchen müssen. Oft werden diese Polynome zufällig ganzzahlige Koeffizienten haben (also in $\mathbb{Z}[X]$ liegen), und es stellt sich heraus, dass es dann etwas einfacher ist, Irreduzibilität in $\mathbb{Z}[X]$ zu untersuchen und sich dann zu überlegen, ob und wie wir daraus Irreduzibilität in $\mathbb{Q}[X]$ folgern können.

Wir arbeiten hier natürlich nicht nur mit \mathbb{Z} und \mathbb{Q} , sondern allgemein mit einem faktoriellen Ring R und seinem Quotientenkörper Q . Ein Polynom in $R[X]$ können wir auf natürliche Weise als Polynom in $Q[X]$ auffassen: Die natürliche Abbildung $R[X] \rightarrow Q[X]$, induziert von der natürlichen Abbildung $R \rightarrow Q, r \mapsto \frac{r}{1}$ (siehe Lemma-Definition 3.74), ist ein injektiver Ringhomomorphismus.

Wir wollen zuerst den Zusammenhang zwischen Irreduzibilität in $R[X]$ und Irreduzibilität in $Q[X]$ ergründen. A priori ist das nicht klar: In $Q[X]$ gibt es ja mehr Elemente als in $R[X]$. Wenn sich ein Polynom also in $R[X]$ nicht weiter zerlegen lässt (bzw. nur auf triviale Weise, wenn einer der beiden Faktoren eine Einheit ist), müsste das nicht automatisch bedeuten, dass es auch in $Q[X]$ unzerlegbar ist. Wir werden sehen, dass das aber tatsächlich der Fall ist.

Kapitel 3 Ringtheorie

Umgekehrt gibt es in Q aber mehr Einheiten als in R . Es könnte also passieren, dass sich ein Polynom $f(X) \in R[X]$ zerlegen lässt als $f(X) = c \cdot g(X)$ für ein $g(X) \in R[X]$ und ein $c \in R \subseteq R[X]$, welches keine Einheit ist (man klammert also aus den Koeffizienten von $f(X)$ einen gemeinsamen Teiler aus). Dann ist das Polynom in $R[X]$ nicht irreduzibel, aber in $Q[X]$ möglicherweise schon, da $c \in Q$ eine Einheit ist. Um dieses letzte Phänomen zu vermeiden, beschränken wir uns in der Regel auf *primitive* Polynome.

Definition 3.76. Sei $f(X) = \sum_{i=0}^n a_i X^i \in R[X]$ ein Polynom mit $f(X) \neq 0$. Dann nennen wir

$$\text{Inh}(f) := \text{ggT}(a_0, \dots, a_n)$$

den *Inhalt* von f . Ist $\text{Inh}(f) = 1$, so heißt $f(X)$ *primitiv*.

Man sieht also direkt, dass insbesondere normierte Polynome immer primitiv sind und die oben bereits erwähnten Minimalpolynome werden diese Bedingung immer erfüllen.

Bemerkung 3.77. Streng genommen müsste man auch hier von *einem* Inhalt von f sprechen, denn der größte gemeinsame Teiler ist ja nur bis auf Multiplikation mit Einheiten definiert. Dies sollte man also immer im Hinterkopf behalten – für die meisten Aussagen, die wir über den Inhalt machen werden (wie beispielsweise Teilbarkeitsrelationen) spielt diese Uneindeutigkeit aber glücklicherweise keine Rolle.

Eine grundlegende und nichttriviale Eigenschaft des Inhalts von Polynomen zeigt das *Lemma von Gauß*. Bevor wir es formulieren, führen wir noch ein wichtiges Konzept ein, welches uns in diesem Abschnitt noch einmal prominent begegnen wird.

Lemma-Definition 3.78. Sei $p \in R$ ein Primelement und $(p) \triangleleft R$ das davon erzeugte Hauptideal. Für $r \in R$ schreiben wir $\bar{r} := [r] \in R/(p)$ für die Äquivalenzklasse von r in $R/(p)$. Dann ist die Abbildung

$$R[X] \rightarrow R/(p)[X], \quad f(X) = \sum_{i=0}^n a_i X^i \mapsto \bar{f}(X) := \sum_{i=0}^n \bar{a}_i X^i$$

ein surjektiver Ringhomomorphismus und heißt *Reduktion modulo p* .

Beweis. Wir wissen, dass die kanonische Projektion $R \rightarrow R/(p)$ ein surjektiver Ringhomomorphismus ist. Da die Definition der Addition und Multiplikation für Polynome nur die Operationen aus dem zugrundeliegenden Koeffizientenring verwendet, folgt sofort, dass auch die fragliche Abbildung $R[X] \rightarrow R/(p)[X]$ ein Ringhomomorphismus ist. Die Surjektivität folgt ebenfalls sofort. \square

Lemma 3.79 (Lemma von Gauß). *Seien $f(X), g(X) \in R[X] \setminus \{0\}$ Polynome. Dann gilt*

$$\text{Inh}(f \cdot g) = \text{Inh}(f) \cdot \text{Inh}(g).$$

Insbesondere ist $f \cdot g$ primitiv, wenn sowohl f als auch g primitiv ist.

Beweis. Wir beweisen zunächst die folgenden Aussagen. Seien $f(X), g(X) \in R[X]$.

Behauptung 1: f und g sind primitiv $\Rightarrow f \cdot g$ ist primitiv.

Wir beweisen die Kontraposition ($f \cdot g$ nicht primitiv $\Rightarrow f$ oder g nicht primitiv).

Ist $f \cdot g$ nicht primitiv, dann ist $d = \text{Inh}(f \cdot g)$ keine Einheit, es gibt also ein Primelement $p \in R$ mit $p \mid d$, da R ein faktorieller Ring ist. Dies bedeutet, dass p ein Teiler jedes einzelnen Koeffizienten von $f \cdot g$ ist. Betrachten wir also die Reduktion modulo p für ein solches Primelement, so gilt

$$\overline{f \cdot g}(X) = \bar{0} \in R/(p)[X].$$

Nun ist die Reduktion modulo p ein Ringhomomorphismus, also gilt auch $\bar{f}(X) \cdot \bar{g}(X) = \bar{0} \in R/(p)[X]$. Der Ring $R/(p)$ ist aber ein Integritätsbereich, da p ein Primelement und $(p) \triangleleft R$ daher ein Primideal ist (siehe Lemma 3.63 und Satz 3.47). Folglich ist auch $R/(p)[X]$ ein Integritätsbereich (siehe Korollar 3.30), also muss gelten $\bar{f}(X) = \bar{0}$ oder $\bar{g}(X) = \bar{0}$. Dies bedeutet aber, dass $p \mid \text{Inh}(f)$ oder $p \mid \text{Inh}(g)$, also ist eines dieser beiden Polynome nicht primitiv.

Behauptung 2: Ist $c \in R \setminus \{0\}$, dann gilt: $\text{Inh}(c \cdot f) = c \cdot \text{Inh}(f)$.

Dies ist klar aus der Beschreibung des größten gemeinsamen Teilers in Lemma 3.72: Sei $f(X) = \sum_{i=0}^n a_i X^i$ und seien p_1, \dots, p_k alle Primfaktoren, die in c, a_0, \dots, a_n vorkommen. Schreibe

$$\begin{aligned} c &= p_1^{\mu_1} \cdot \dots \cdot p_k^{\mu_k} \\ a_0 &= p_1^{\nu_{01}} \cdot \dots \cdot p_k^{\nu_{0k}} \\ a_1 &= p_1^{\nu_{11}} \cdot \dots \cdot p_k^{\nu_{1k}} \\ &\vdots \\ a_n &= p_1^{\nu_{n1}} \cdot \dots \cdot p_k^{\nu_{nk}} \end{aligned}$$

mit Exponenten aus \mathbb{N}_0 .

Dann ist

$$\begin{aligned} \text{Inh}(c \cdot f) &= \text{ggT}(c \cdot a_0, \dots, c \cdot a_n) \\ &= \text{ggT}(p_1^{\mu_1 + \nu_{01}} \cdot \dots \cdot p_k^{\mu_k + \nu_{0k}}, \dots, p_1^{\mu_1 + \nu_{n1}} \cdot \dots \cdot p_k^{\mu_k + \nu_{nk}}) \\ &= p_1^{\min\{\mu_1 + \nu_{01}, \dots, \mu_1 + \nu_{n1}\}} \cdot \dots \cdot p_k^{\min\{\mu_k + \nu_{0k}, \dots, \mu_k + \nu_{nk}\}} \\ &= p_1^{\mu_1 + \min\{\nu_{01}, \dots, \nu_{n1}\}} \cdot \dots \cdot p_k^{\mu_k + \min\{\nu_{0k}, \dots, \nu_{nk}\}} \\ &= p_1^{\mu_1} \cdot \dots \cdot p_k^{\mu_k} \cdot p_1^{\min\{\nu_{01}, \dots, \nu_{n1}\}} \cdot \dots \cdot p_k^{\min\{\nu_{0k}, \dots, \nu_{nk}\}} \\ &= c \cdot \text{ggT}(a_0, \dots, a_n) = c \cdot \text{Inh}(f). \end{aligned}$$

Kapitel 3 Ringtheorie

Sind nun $f(X), g(X) \in R[X] \setminus \{0\}$, dann sei $d := \text{Inh}(f)$ und $e := \text{Inh}(g)$. Betrachte die Polynome

$$\tilde{f}(X) := \frac{1}{d}f(X), \quad \tilde{g}(X) := \frac{1}{e}g(X).$$

Diese liegen immer noch in $R[X]$ und sind nun primitiv (das folgt z.B. auch aus Behauptung 2). Daher sind mit Behauptung 1 auch das Produkt $\tilde{f} \cdot \tilde{g}$ primitiv. Es gilt außerdem

$$f(X) \cdot g(X) = d \cdot \tilde{f}(X) \cdot e \cdot \tilde{g}(X) = (de) \cdot (\tilde{f} \cdot \tilde{g})(X).$$

Also ist nach Behauptung 2 nun

$$\text{Inh}(f \cdot g) = (de) \cdot \underbrace{\text{Inh}(\tilde{f} \cdot \tilde{g})}_{=1} = d \cdot e = \text{Inh}(f) \cdot \text{Inh}(g).$$

□

Mithilfe des Lemmas von Gauß können wir den folgenden Satz beweisen, der Teilbarkeit in $R[X]$ mit Teilbarkeit in $Q[X]$ in Verbindung bringt.

Satz 3.80. Sind $f(X), g(X) \in R[X]$, wobei g primitiv ist, und ist $q(X) \in Q[X]$, sodass gilt $f(X) = q(X) \cdot g(X)$, dann folgt bereits $q(X) \in R[X]$.

Beweis. Falls $q(X) = 0$, so ist die Aussage offensichtlich wahr. Sei nun also $q(X) \neq 0$ (dann ist automatisch $f(X) \neq 0$, denn g ist primitiv und somit ebenfalls nicht das Nullpolynom). Die Koeffizienten von $q(X)$ sind Elemente im Quotientenkörper $Q = \text{Quot}(R)$. Wenn wir dieses Polynom also mit einem passenden Element $\beta \in R \setminus \{0\}$ multiplizieren, liegen all seine Koeffizienten in R . Dafür kann man zum Beispiel für β das Produkt aller Nenner der Koeffizienten von $q(X)$ nehmen oder (besser) ihren *Hauptnenner*, d.h. das kleinste gemeinsame Vielfache all dieser Nenner (dieses existiert, da R faktoriell ist, siehe Bemerkung 3.73). Es gibt also ein $\beta \in R \setminus \{0\}$ mit

$$\beta \cdot q(X) \in R[X].$$

Wir haben daher die Gleichung

$$\underbrace{\beta f(X)}_{\in R[X]} = \underbrace{\beta q(X)}_{\in R[X]} \cdot \underbrace{g(X)}_{\in R[X]}$$

und Lemma 3.79 impliziert dann

$$\text{Inh}(\beta f) = \text{Inh}(\beta q) \cdot \text{Inh}(g),$$

aber auch $\text{Inh}(\beta f) = \beta \text{Inh}(f)$. Da nach Voraussetzung g primitiv ist, also $\text{Inh}(g) = 1$ gilt, erhalten wir $\text{Inh}(\beta q) = \beta \cdot \text{Inh}(f)$, also $\beta \mid \text{Inh}(\beta q)$ in R . Schreiben wir

$$\beta q(X) = \sum_{i=0}^n a_i X^i \in R[X],$$

dann gilt also $\beta \mid \text{ggT}(a_0, \dots, a_n)$, also insbesondere $\beta \mid a_i$ für alle $i \in \{0, \dots, n\}$. Es gibt also $b_0, \dots, b_n \in R$ mit $a_i = \beta \cdot b_i$ für jedes i , also gilt

$$\beta q(X) = \sum_{i=0}^n (\beta b_i) X^i = \beta \underbrace{\sum_{i=0}^n b_i X^i}_{\in R[X]}$$

und daraus folgt (da $R[X]$ ein Integritätsbereich ist und $\beta \neq 0$)

$$q(X) = \sum_{i=0}^n b_i X^i \in R[X].$$

□

Dieser Satz besagt also insbesondere, dass für zwei Polynome $f(X), g(X) \in R[X]$, wobei g primitiv sei, eine Teilbarkeitsrelation $g(X) \mid f(X)$ in $Q[X]$ automatisch eine Teilbarkeitsrelation $g(X) \mid f(X)$ in $R[X]$ impliziert. Daraus können wir nun die Aussage folgern, nach der wir gesucht haben, nämlich dass für ein primitives Polynom die Irreduzibilität über R und über Q äquivalent sind.

Satz 3.81. Sei $f(X) \in R[X]$ ein primitives Polynom, dann gilt:

$$f(X) \text{ ist irreduzibel über } R[X] \Leftrightarrow f(X) \text{ ist irreduzibel über } Q[X].$$

Beweis. Wir beweisen beide Richtungen nacheinander.

\Rightarrow : Sei $f(X)$ irreduzibel in $R[X]$. Seien $g(X), h(X) \in Q[X]$, sodass $f(X) = g(X) \cdot h(X)$. (Insbesondere ist dann weder $g(X)$ noch $h(X)$ das Nullpolynom, da f primitiv und daher $f(X) \neq 0$.) Dann wollen wir zeigen, dass einer der beiden Faktoren eine Einheit in $Q[X]$ ist.

Es gibt ein Element $\beta \in R \setminus \{0\}$, sodass

$$\beta \cdot g(X) \in R[X]$$

(zum Beispiel kann man für β den Hauptnenner der Koeffizienten von $g(X)$ nehmen). Wir schreiben $d := \text{Inh}(\beta \cdot g)$, dann sind alle Koeffizienten von $\beta \cdot g(X)$ durch d teilbar (in R) und $\frac{1}{d} \cdot \beta \cdot g(X) \in R[X]$ ist ein primitives Polynom. Es gibt dann eine Zerlegung

$$\underbrace{f(X)}_{\in R[X]} = \underbrace{\frac{\beta}{d} g(X)}_{\substack{\in R[X] \\ \text{und primitiv}}} \cdot \underbrace{\frac{d}{\beta} h(X)}_{\in Q[X]}, \quad (*)$$

die a priori in $Q[X]$ ist, aber nach Satz 3.80 muss dann bereits gelten

$$\frac{d}{\beta} h(X) \in R[X].$$

Die Zerlegung (*) ist also bereits eine Zerlegung in $R[X]$ und da $f(X)$ dort irreduzibel ist, muss einer der beiden Faktoren eine Einheit, also insbesondere ein Polynom vom Grad 0 sein. Folglich muss auch eines der beiden Polynome $g(X)$ und $h(X)$ vom Grad 0 sein und ist somit eine Einheit in $Q[X]$. Also ist $f(X)$ auch irreduzibel in $Q[X]$.

\Leftarrow : Sei $f(X)$ irreduzibel in $Q[X]$. Seien $g(X), h(X) \in R[X]$, sodass $f(X) = g(X) \cdot h(X)$. Wir wollen zeigen, dass $g(X)$ oder $h(X)$ eine Einheit in $R[X]$ ist.

Wir können die Zerlegung $f(X) = g(X) \cdot h(X)$ auch in $Q[X]$ lesen und wegen der Irreduzibilität ist einer der Faktoren, o.B.d.A. sagen wir $g(X)$, eine Einheit in $Q[X]$, also $g(X) = c$ ist ein konstantes Polynom mit $c \in Q^\times = Q \setminus \{0\}$. Da aber $g(X) \in R[X]$ vorausgesetzt ist, muss gelten $c \in R \setminus \{0\}$. Aus dem Lemma von Gauß und weil f primitiv ist, erhalten wir

$$1 = \text{Inh}(f) = \text{Inh}(g \cdot h) = \text{Inh}(c \cdot h) = c \cdot \text{Inh}(h),$$

also ist $c \in R^\times$ eine Einheit in R und somit $g(X)$ eine Einheit in $R[X]$. Daher ist $f(X)$ auch irreduzibel in $R[X]$. \square

Da wir nun wissen, dass wir für ein primitives Polynom $f(X) \in R[X]$ nur die Irreduzibilität in $R[X]$ testen müssen und damit die Irreduzibilität in $Q[X]$ automatisch folgern können, stellt sich natürlich noch die Frage, wie man für ein solches $f(X)$ feststellt, ob es in $R[X]$ irreduzibel ist. Dafür gibt es drei wichtige Kriterien, die wir im Folgenden beweisen. Wir beginnen mit einem sehr einfachen.

Lemma 3.82 (Nullstellenkriterium). *Sei R ein Integritätsbereich und $f(X) \in R[X]$ ein normiertes Polynom.*

(i) *Ist $\deg(f) = 1$, so ist $f(X)$ irreduzibel.*

(ii) *Ist $\deg(f) \in \{2, 3\}$, dann gilt:*

$$f(X) \text{ ist irreduzibel in } R[X] \Leftrightarrow f(X) \text{ hat keine Nullstelle in } R.$$

Beweis. (i) Ist $f(X) = g(X)h(X)$ für $g(X), h(X) \in R[X]$, dann gilt $\deg(g) + \deg(h) = 1$, also ist $g \in R$ oder $h \in R$ ein konstantes Polynom, o.B.d.A. sagen wir $g = a \in R$ und $h(X) = bX + c \in R[X]$. Dann folgt aber $a \cdot b = 1$, da $f(X)$ normiert ist und somit $g(X) = a \in R^\times = (R[X])^\times$. Also ist $f(X)$ irreduzibel.

(ii) Wir zeigen beide Richtungen nacheinander:

\Rightarrow : Sei $f(X) \in R[X]$ irreduzibel. Hätte $f(X)$ eine Nullstelle $a \in R$, so könnte man nach Korollar 3.36 schreiben

$$f(X) = (X - a) \cdot g(X)$$

für ein $g(X) \in R[X]$. Da R ein Integritätsbereich ist, gilt nach Lemma 3.29 außerdem $\deg(g) = \deg(f) - 1 \geq 1$. Somit hätten wir $f(X)$ in ein Produkt

zweier nicht-konstanter Polynome (also Nichteinheiten) zerlegt, dies ist aber ein Widerspruch zur Voraussetzung, dass $f(X)$ irreduzibel ist. Daher hat $f(X)$ keine Nullstelle.

⇐: Es habe $f(X)$ keine Nullstelle in R . Angenommen, $f(X)$ wäre nicht irreduzibel, dann könnte man schreiben

$$f(X) = g(X) \cdot h(X)$$

für zwei Polynome $g(X), h(X) \in R[X]$, die keine Einheiten sind. Es wäre dann also $\deg(g), \deg(h) \geq 1$, aber auch $\deg(g) + \deg(h) = \deg(f) \in \{2, 3\}$ nach Lemma 3.29. Dies bedeutet aber, dass einer der Faktoren Grad 1 haben müsste, o.B.d.A. sagen wir daher $g(X) = aX + b$. Da $f(X)$ normiert ist, würde dann folgen $a \in R^\times$ (denn sein Produkt mit dem Leitkoeffizienten von $h(X)$ muss gleich 1 sein). Also hätte $g(X)$ und damit $f(X)$ eine Nullstelle, nämlich $-a^{-1}b \in R$, was der Voraussetzung widerspricht. Somit ist $f(X)$ irreduzibel. □

Satz 3.83 (Reduktionskriterium). *Sei R ein faktorieller Ring und $p \in R$ ein Primelement. Sei $f(X) = \sum_{i=0}^n a_i X^i \in R[X]$ ein primitives Polynom mit $p \nmid a_n$, sodass $\bar{f}(X) \in R/(p)[X]$ irreduzibel ist. Dann ist $f(X)$ irreduzibel in $R[X]$ (und damit in $Q[X]$).*

Beweis. Wir nehmen an, dass $f(X)$ nicht irreduzibel in $R[X]$ ist, und versuchen dies zum Widerspruch zu führen. In diesem Fall gibt es Polynome $g(X), h(X) \in R[X]$ mit $f(X) = g(X) \cdot h(X)$ und $g(X), h(X) \notin (R[X])^\times = R^\times$. Beide Polynome $g(X)$ und $h(X)$ müssen dann auch nicht-konstant sein, denn wäre beispielsweise $g(X) = b$ für ein $b \in R$, so gälte $b \cdot \text{Inh}(h) = \text{Inh}(b \cdot h) = \text{Inh}(g \cdot h) = \text{Inh}(f) = 1$ (nach dem Lemma von Gauß und weil f primitiv ist), also wäre $b \in R^\times$, was ausgeschlossen war.

Schreiben wir nun $g(X) = \sum_{i=0}^k b_i X^i$ und $\sum_{i=0}^m c_i X^i$ (mit $k + m = n$), dann muss für die Leitkoeffizienten gelten $b_k \cdot c_m = a_n$. Also gilt $p \nmid b_k$ und $p \nmid c_m$.

Wenden wir auf die Zerlegung $f(X) = g(X) \cdot h(X)$ nun die Reduktion modulo p an, erhalten wir eine Zerlegung

$$\bar{f}(X) = \bar{g}(X) \cdot \bar{h}(X)$$

in $R/(p)[X]$. Der Leitkoeffizient von $\bar{g}(X)$ ist $\bar{b}_k = [b_k] \in R/(p)$ und wegen $p \nmid b_k$ gilt $[b_k] \neq [0]$ und somit $\deg(\bar{g}) \geq 1$. Es ist also $\bar{g}(X)$ keine Einheit (beachte, dass $(R/(p)[X])^\times = (R/(p))^\times = (R/(p)) \setminus \{0\}$). Ebenso ist $\bar{h}(X)$ keine Einheit und daher ist $\bar{f}(X)$ nicht irreduzibel in $R/(p)[X]$, ein Widerspruch. □

Bemerkung 3.84. Dieses Kriterium ist hilfreich, denn Irreduzibilität in $R/(p)[X]$ ist oft recht einfach zu prüfen: Zum Beispiel gibt es in $\mathbb{Z}/p\mathbb{Z}[X]$ viel weniger Polynome von einem bestimmtem Grad als in $\mathbb{Z}[X]$, einfach deshalb, weil es in $\mathbb{Z}/p\mathbb{Z}$ weniger (nämlich nur endlich viele) Elemente gibt. Man kann sich also gegebenenfalls alle

Kapitel 3 Ringtheorie

möglichen Teiler eines Polynoms aufschreiben und (mithilfe der Polynomdivision) testen, ob es einen Teiler gibt, der dann eine nichttriviale Zerlegung liefert. Falls nicht, ist das Polynom irreduzibel.

Es ist wichtig, zu beobachten, dass die Umkehrung von Satz 3.83 *nicht* gilt: Ein Polynom kann irreduzibel in $R[X]$ sein, obwohl die Reduktion $\bar{f}(X)$ modulo p reduzibel ist: Beispielsweise ist $f(X) = X^3 + 3X + 2 \in \mathbb{Z}[X]$ irreduzibel (denn es hat keine Nullstelle in \mathbb{Z}), aber die Reduktion modulo 3 ist $\bar{f}(X) = X^3 + \bar{2} = (X - \bar{1})(X^2 + X + \bar{1}) \in \mathbb{Z}/3\mathbb{Z}[X]$, also reduzibel.

Man muss manchmal mehrere Primelemente p ausprobieren, bevor man eines findet, bezüglich dessen die Reduktion modulo p irreduzibel ist – sobald man eines gefunden hat, folgt ja mit dem obigen Satz die Irreduzibilität des ursprünglichen Polynoms.

Es kann aber sogar passieren, dass ein Polynom zwar irreduzibel ist, es aber gar kein Primelement p gibt, bezüglich dessen die Reduktion modulo p irreduzibel ist. In diesem Fall bringt uns das Reduktionskriterium also nicht weiter und man ist auf andere Kriterien angewiesen.

Satz 3.85 (Eisenstein-Kriterium). *Sei R ein faktorieller Ring und $p \in R$ ein Primelement. Sei $f(X) = \sum_{i=0}^n a_i X^i \in R[X]$ ein primitives Polynom, sodass*

$$p \nmid a_n, \quad p \mid a_i \quad \text{für alle } i \in \{0, \dots, n-1\}, \quad p^2 \nmid a_0.$$

Dann ist $f(X)$ irreduzibel in $R[X]$ (und damit auch in $Q[X]$).

Beweis. Wir nehmen an, dass $f(X)$ nicht irreduzibel ist, also $f(X) = g(X) \cdot h(X)$ für Polynome $g(X), h(X) \in R[X]$, welche keine Einheiten sind. Dann müssen $g(X)$ und $h(X)$ automatisch nicht-konstant sein, da $f(X)$ primitiv ist. (Dieses Argument haben wir am Anfang des Beweises von Satz 3.83 ausgeführt). Also gilt auch $\deg(f) \geq 2$.

Wenden wir die Reduktion modulo p an, so erhalten wir wegen der vorausgesetzten Teilbarkeitsrelationen

$$\bar{f}(X) = \bar{a}_n X^n \in R/(p)[X]$$

mit $\bar{a}_n \neq \bar{0}$. Schreiben wir $g(X) = \sum_{i=0}^k b_i X^i$ und $h(X) = \sum_{i=0}^m c_i X^i$ (mit $k, m \geq 1$ und $k + m = n$), so gilt außerdem

$$\bar{f}(X) = \bar{g}(X) \cdot \bar{h}(X) = \left(\sum_{i=0}^k \bar{b}_i X^i \right) \cdot \left(\sum_{i=0}^m \bar{c}_i X^i \right).$$

Insbesondere gilt für die Leitkoeffizienten $\bar{a}_n = \bar{b}_k \cdot \bar{c}_m$ und damit $\bar{b}_k, \bar{c}_m \neq \bar{0}$.

Behauptung: $\bar{b}_0 = \bar{c}_0 = \bar{0}$.

Angenommen, $\bar{b}_0 \neq \bar{0}$. Wir bezeichnen mit $j \in \{0, \dots, m\}$ den kleinsten Index, sodass $\bar{c}_j \neq \bar{0}$. Dann hat das Produkt $\bar{g}(X) \cdot \bar{h}(X) = \bar{f}(X)$ einen Term der Form

$\overline{b_0 c_j X^j}$, dessen Koeffizient nicht Null ist (denn $R/(p)$ ist ein Integritätsbereich). Da aber $j \leq m < n$ gilt, ist das ein Widerspruch. Ebenso ist $\overline{c_0} \neq 0$ nicht möglich.

Aus der Behauptung folgt $p \mid b_0$ und $p \mid c_0$, also $p^2 \mid b_0 c_0 = a_0$, was ein Widerspruch zur Voraussetzung ist. Damit ist $f(X)$ irreduzibel in $R[X]$. \square

Bemerkung 3.86. In Satz 3.83 und Satz 3.85 haben wir vorausgesetzt, dass die Polynome $f(X) \in R[X]$ primitiv sind. Fordert man das nicht, so kann man, wenn die anderen Voraussetzungen erfüllt sind, immer noch folgern, dass $f(X)$ irreduzibel in $Q[X]$ ist: Man kann nämlich schreiben $f(X) = \text{Inh}(f) \cdot \tilde{f}(X)$ für ein primitives Polynom $\tilde{f}(X) \in R[X]$. Man überlegt sich leicht, dass letzteres immer noch die Voraussetzungen der Sätze erfüllt, wenn $f(X)$ sie erfüllt, und man erhält somit, dass $\tilde{f}(X)$ irreduzibel in $R[X]$ und $Q[X]$ ist. Da $\text{Inh}(f)$ eine Einheit in Q ist, ist $f(X)$ ebenfalls irreduzibel in $Q[X]$. Falls $\text{Inh}(f)$ aber keine Einheit in R ist, ist $f(X)$ nicht irreduzibel in $R[X]$.

Zu guter Letzt erwähnen wir noch einen weiteren Kniff, mit dem man sich manchmal die Untersuchung der Irreduzibilität etwas leichter machen.

Lemma 3.87. *Sei R ein kommutativer Ring mit Eins, $a \in R$ ein Element und $f(X) \in R[X]$ ein Polynom. Dann gilt*

$$f(X) \text{ ist irreduzibel in } R[X] \Leftrightarrow f(X + a) \text{ ist irreduzibel in } R[X].$$

Beweis. Die Abbildung

$$R[X] \rightarrow R[X], \quad f(X) \mapsto f(X + a)$$

ist ein Ringisomorphismus (die Umkehrabbildung ist gegeben durch $f(X) \mapsto f(X - a)$). Ist also $f(X) = g(X) \cdot h(X)$ eine Zerlegung in zwei Nichteinheiten, so ist auch $f(X + a) = g(X + a) \cdot h(X + a)$ eine Zerlegung in zwei Nichteinheiten, da ein Ringhomomorphismus Einheiten auf Einheiten abbildet (siehe Lemma 3.12). \square

Zum Abschluss dieses Kapitels wollen wir den folgenden wichtigen Satz formulieren, der nun aus unseren bisherigen Resultaten (und insbesondere aus Satz 3.80, der auch selbst manchmal als „Satz von Gauß“ bezeichnet wird) folgt.

Satz 3.88 (Satz von Gauß). *Sei R ein faktorieller Ring. Dann ist auch $R[X]$ ein faktorieller Ring. Ein Polynom $p(X) \in R[X]$ ist genau dann ein Primelement in $R[X]$, wenn eine der folgenden Bedingungen erfüllt ist:*

- (i) $q(X) = p$ ist ein konstantes Polynom für ein Primelement $p \in R$,
- (ii) $q(X)$ ist primitiv und ein Primelement in $Q[X]$, wobei $Q := \text{Quot}(R)$ den Quotientenkörper von R bezeichnet.

Beweis. Wir zeigen den Satz in mehreren Schritten.

Kapitel 3 Ringtheorie

Behauptung 1: Ist $p \in R$ ein Primelement, so ist auch das konstante Polynom $p \in R[X]$ ein Primelement.

Sei $p \in R$ ein Primelement und seien $f(X), g(X) \in R[X]$ Polynome, sodass $p \mid f(X)g(X)$. Angenommen, $p \nmid f(X)$ und $p \nmid g(X)$, d.h. es gibt Koeffizienten von $f(X)$ und $g(X)$, welche von p nicht geteilt werden. Schreibe $f(X) = \sum_{i=0}^n a_i X^i$ und $g(X) = \sum_{j=0}^m b_j X^j$ und seien $r \in \{0, \dots, n\}, s \in \{0, \dots, m\}$ die kleinsten Indizes, sodass $p \nmid a_r$ und $p \nmid b_s$ in R gilt. Da p ein Primelement in R ist, gilt auch $p \nmid a_r b_s$. Schreiben wir nun $f(X)g(X) = \sum_{k=0}^{n+m} c_k X^k$, dann wäre $c_{r+s} = \sum_{l=0}^{r+s} a_l b_{r+s-l}$. Jeder Summand außer $a_r b_s$ hat hier p als Teiler, also würde gelten $p \mid c_{r+s}$ und folglich $p \mid f(X)g(X)$ in $R[X]$. Widerspruch. Also gilt $p \mid f(X)$ oder $p \mid g(X)$ und damit ist p auch ein Primelement in $R[X]$.

Behauptung 2: Ist $q(X) \in R[X]$ ein Primelement mit $\deg(q) = 0$, so ist $q(X) = p$ für ein Primelement $p \in R$.

Wegen $\deg(q) = 0$ gilt auf jeden Fall $q(X) = r$ für ein $r \in R$. Da $q(X)$ prim ist, folgt für alle $f(X), g(X) \in R[X]$ aus $r \mid f(X)g(X)$ bereits, dass $r \mid f(X)$ oder $r \mid g(X)$. Insbesondere gilt diese Eigenschaft für alle *konstanten* Polynome $f(X)$ und $g(X)$. Dies bedeutet dann genau, dass r ein Primelement in R ist.

Behauptung 3: Ist $q(X) \in R[X]$ primitiv und ein Primelement in $Q[X]$, so ist $q(X)$ ein Primelement in $R[X]$.

Seien $f(X), g(X) \in R[X]$, sodass $q(X) \mid f(X)g(X)$ in $R[X]$. Dann gilt auch $q(X) \mid f(X)g(X)$ in $Q[X]$ und es folgt, dass $q(X) \mid f(X)$ oder $q(X) \mid g(X)$ in $Q[X]$, da $q(X)$ nach Voraussetzung ein Primelement in $Q[X]$ ist. Da $q(X)$ primitiv ist, folgt dann mit Satz 3.80 auch, dass $q(X) \mid f(X)$ oder $q(X) \mid g(X)$ in $R[X]$. Somit ist $q(X)$ ein Primelement in $R[X]$.

Behauptung 4: Ist $f(X) \in R[X]$ ein Primelement und $\deg(f) \geq 1$, so ist $f(X)$ auch ein Primelement in $Q[X]$.

Nach Lemma 3.64 ist $f(X) \in R[X]$ irreduzibel. Damit ist $f(X) \in Q[X]$ irreduzibel (siehe Satz 3.81, wobei man sich ähnlich wie in Bemerkung 3.86 überlegt, dass für diese Richtung Primitivität nicht notwendig ist). Da Q ein Körper und daher $Q[X]$ ein Hauptidealbereich ist, ist somit $f(X) \in Q[X]$ nach Korollar 3.66 auch ein Primelement.

Die obigen vier Behauptungen beweisen zusammen den zweiten Teil des Satzes: Ein $q(X) \in R[X]$ ist prim genau dann, wenn die Eigenschaften (i) oder (ii) erfüllt sind.

Behauptung 5: Ist $f(X) \in R[X]$ irreduzibel, so ist es auch ein Primelement in $R[X]$.

Ist $f(X)$ irreduzibel in $R[X]$, so auch in $Q[X]$ (mit demselben Argument wie oben) und somit ein Primelement in $Q[X]$. Seien nun $g(X), h(X) \in R[X]$ mit $f(X) \mid g(X)h(X)$, so gilt diese Teilbarkeitsrelation auch in $Q[X]$ lesen.

Da $f(X)$ ein Primelement in $Q[X]$ ist, folgt $f(X) \mid g(X)$ oder $f(X) \mid h(X)$ in $Q[X]$, o.B.d.A. sagen wir $f(X) \mid g(X)$. Es gibt also ein $q(X) \in Q[X]$ mit $g(X) = q(X)f(X)$. Da $f(X)$ irreduzibel in $R[X]$ ist, ist es insbesondere primitiv und somit folgt mit Satz 3.80 bereits $q(X) \in R[X]$, also gilt auch $f(X) \mid g(X)$ in $R[X]$. Somit ist $f(X)$ auch ein Primelement in $R[X]$.

Behauptung 6: Jedes $f(X) \in R[X] \setminus (\{0\} \cup R^\times)$ hat eine Zerlegung als Produkt von Primelementen.

Wir beweisen dies per Induktion nach dem Grad von $f(X)$:

Induktionsanfang: Ist $\deg(f) = 0$, so hat $f(X)$ eine Zerlegung als Produkt von Primelementen, denn $f(X) = r$ für ein $r \in R$ und R ist ein faktorieller Ring, dessen Primelemente auch prim in $R[X]$ sind (siehe Behauptung 1).

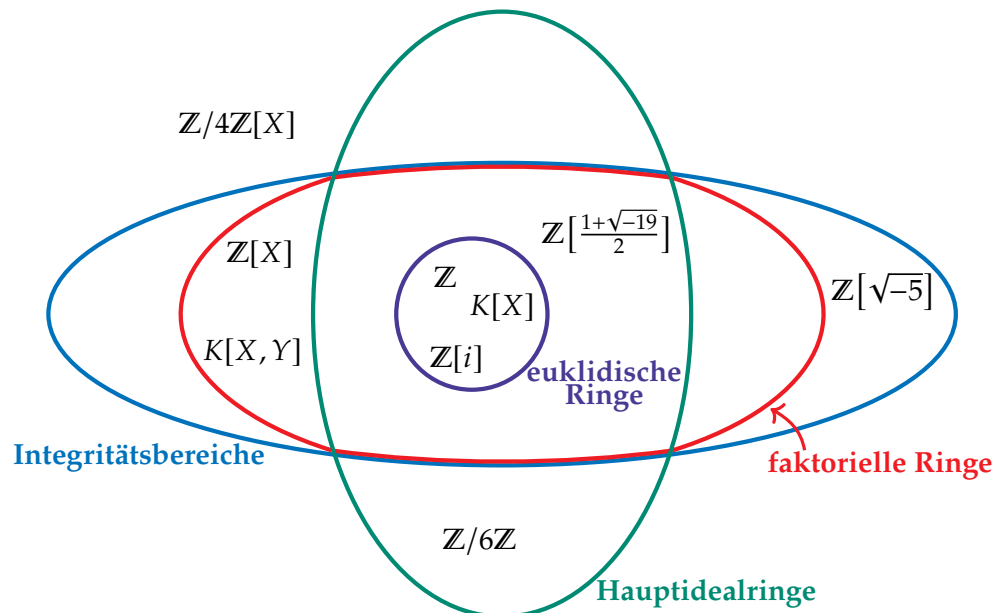
Induktionsvoraussetzung: Für ein beliebiges, aber festes $n \in \mathbb{N}_0$ sei bekannt, dass sich jedes $f(X) \in R[X] \setminus (\{0\} \cup R^\times)$ mit $\deg(f) \leq n$ als Produkt von Primelementen in $R[X]$ darstellen lässt.

Induktionsschritt: Sei $f(X) \in R[X] \setminus (\{0\} \cup R^\times)$ mit $\deg(f) = n + 1$. Wir schreiben $f(X) = \text{Inh}(f) \cdot \tilde{f}(X)$ für ein primitives Polynom $\tilde{f}(X) \in R[X]$. Wie im Induktionsanfang können wir $\text{Inh}(f)$ als Produkt von Primelementen schreiben. Es bleibt also noch zu zeigen, dass $\tilde{f}(X)$ ein Produkt von Primelementen ist. Falls $\tilde{f}(X)$ irreduzibel ist, ist die Aussage klar, denn nach Behauptung 5 ist $\tilde{f}(X)$ dann auch prim und somit als Produkt (mit nur einem Faktor) von Primelementen darstellbar. Ist $\tilde{f}(X)$ hingegen nicht irreduzibel, so können wir schreiben $\tilde{f}(X) = g(X)h(X)$ für gewisse $g(X), h(X) \in R[X]$, welche keine Einheiten sind. Außerdem sind $g(X)$ und $h(X)$ beide nicht konstant, denn $\tilde{f}(X)$ ist primitiv. Folglich gilt $\deg(g), \deg(h) < \deg(\tilde{f})$ und somit lassen sich beide nach Induktionsvoraussetzung als Produkt von Primelementen schreiben, was uns eine Darstellung von $\tilde{f}(X)$ als Produkt von Primelementen und schließlich eine solche von $f(X)$ liefert.

Wegen Satz 3.69 impliziert die Behauptung 6, dass $R[X]$ ein faktorieller Ring ist. \square

Kapitel 3 Ringtheorie

Wir haben in diesem Kapitel viele Eigenschaften und Begrifflichkeiten im Zusammenhang mit (kommutativen) Ringen (mit Eins) gesehen. Das folgende Bild¹ veranschaulicht die Zusammenhänge zwischen diesen Konzepten noch einmal:



Die Abbildung zeigt die verschiedenen Klassen von Ringen, die wir kennengelernt haben, sowie Beispiele von Ringen, die zu bestimmten dieser Klassen (nicht) gehören. Zum Beispiel sind alle Ringe innerhalb der blauen Linie Integritätsbereiche und $\mathbb{Z}[\sqrt{-5}]$ ist ein Integritätsbereich, der aber kein faktorieller Ring ist. Zudem sieht man, dass alle Hauptidealbereiche (d.h. Ringe, die sowohl Hauptidealringe als auch Integritätsbereiche sind), automatisch faktoriell sind (das war die Aussage von Satz 3.71) und dass alle Euklidischen Ringe Hauptidealbereiche sind (Satz 3.39). In dieser Abbildung bezeichnet K immer einen (beliebigen) Körper.

¹Dieses Bild ist inspiriert durch eine entsprechende Veranschaulichung in einer Vorlesung von Marco Hien.

Körpererweiterungen

L'Algèbre est généreuse, elle donne souvent plus qu'on ne lui demande.

Die Algebra ist großzügig, sie gibt oft mehr, als man von ihr verlangt.

Jean-Baptiste le Rond d'Alembert

Wir kommen jetzt zum Hauptthema dieser Vorlesung: den Körpererweiterungen. Bevor wir sie definieren, sammeln wir noch einmal kurz die wichtigsten Erkenntnisse über Körper, die sich aus dem letzten Kapitel ergeben:

- Körper sind Integritätsbereiche.
Sie sind sogar euklidische Ringe (was aber nicht wirklich interessant ist, denn die Division mit Rest geht immer auf) und damit auch Hauptidealbereiche (auch das ist nicht sehr spannend, da es nur die Ideale $\{0\} = (0)$ und $K = (1)$ gibt) und faktorielle Ringe (es gibt aber keine irreduziblen Elemente, da jedes Element entweder 0 oder eine Einheit ist).
- Körperhomomorphismen sind immer injektiv.
- Der Polynomring $K[X]$ über einem Körper K ist ein euklidischer Ring (und damit automatisch Integritäts- sowie Hauptidealbereich und faktorieller Ring).

Für die folgenden Abschnitte setzen wir das Wissen aus der Linearen Algebra voraus (in Wirklichkeit benötigen wir aber nur die Definition eines Vektorraums, einer Basis und der Dimension.)

4.1 Algebraische Erweiterungen und Minimalpolynome

Definition 4.1. Sei L ein Körper, dann heißt eine Teilmenge $L \subseteq K$ ein *Teilkörper* (oder *Unterkörper*) von L , falls K abgeschlossen unter der Addition und Multiplikation ist und falls $(K, +, \cdot)$ wieder ein Körper ist.

Der Körper L heißt dann ein *Erweiterungskörper* von K und das Paar $K \subseteq L$ heißt *Körpererweiterung*. Wir schreiben für gewöhnlich L/K (gelesen „ L über K “).

Beispiel 4.2. • Jeder Körper K ist ein Erweiterungskörper von sich selbst: K/K

- bekannte Körpererweiterungen: \mathbb{C}/\mathbb{R} , \mathbb{R}/\mathbb{Q} , \mathbb{C}/\mathbb{Q}
- Betrachte eine Zahl $d \in \mathbb{Z}$, welche keine Quadratzahl ist (d.h. $d \neq x^2$ für alle $x \in \mathbb{Z}$). Wähle dann eine Zahl $\sqrt{d} \in \mathbb{C}$ mit $(\sqrt{d})^2 = d$ und betrachte die Menge

$$\mathbb{Q}(\sqrt{d}) := \{a + b\sqrt{d} \mid a, b \in \mathbb{Q}\} \subseteq \mathbb{C}.$$

Diese ist ein Teilkörper von \mathbb{C} . Um zu sehen, dass es tatsächlich multiplikativ Inverse in $\mathbb{Q}(\sqrt{d})$ gibt, muss man kurz nachdenken: Man sieht aber leicht, dass gilt

$$\frac{1}{a + b\sqrt{d}} = \frac{a - b\sqrt{d}}{a^2 - b^2d} = \frac{a}{a^2 - b^2d} - \frac{b}{a^2 - b^2d}\sqrt{d} \in \mathbb{Q}(\sqrt{d}).$$

Eine einfache Beobachtung ist das folgende Lemma, das es uns ermöglichen wird, unser Wissen aus der Linearen Algebra einzusetzen, um Körpererweiterungen zu studieren.

Lemma 4.3. *Ist L/K eine Körpererweiterung, so ist L auf natürliche Weise ein K -Vektorraum. Die Addition $+$: $L \times L \rightarrow L$ ist dabei durch die Addition auf dem Körper L gegeben, die Skalarmultiplikation \cdot : $K \times L \rightarrow L$ ist gegeben durch Einschränkung der Multiplikation auf dem Körper L .*

Beweis. Da L ein Körper ist, ist $(L, +)$ eine abelsche Gruppe. Die Eigenschaften, die die Skalarmultiplikation eines Vektorraums erfüllen muss, folgen aus dem Assoziativgesetz der Multiplikation sowie dem Distributivgesetz und der Eigenschaft der Eins im Körper L . \square

Nun möchten wir gerne messen, wie „groß“ eine Körpererweiterung ist, also wie groß L im Vergleich zu K ist. Für die „Größe“ eines Vektorraums haben wir in der Linearen Algebra bereits einen guten Begriff kennengelernt, nämlich die *Dimension*.

Definition 4.4. Sei L/K eine Körpererweiterung. Diese heißt *endlich*, falls L ein endlichdimensionaler K -Vektorraum ist. In diesem Fall definieren wir den *Körpergrad* (oder *Erweiterungsgrad*) von L über K als

$$[L : K] := \dim_K(L).$$

Bemerkung 4.5. Eine einfache Beobachtung ist die folgende: Für eine endliche Körpererweiterung L/K ist der Körpergrad $[L : K]$ immer mindestens 1, denn K ist in L enthalten, sodass L niemals der nulldimensionale K -Vektorraum $\{0\}$ sein kann. Die kleinste Körpererweiterung ist die triviale (d.h. $L = K$) und in diesem Fall gilt $[L : K] = [K : K] = \dim_K K = 1$.

Beispiel 4.6. Sei $d \in \mathbb{Z} \setminus \{0, 1\}$ wie in Beispiel 4.2 eine quadratfreie Zahl. Dann bilden die Elemente 1 und \sqrt{d} eine Basis von $\mathbb{Q}(\sqrt{d})$ über \mathbb{Q} : Offensichtlich sind sie ein Erzeugendensystem (nach Definition von $\mathbb{Q}(\sqrt{d})$). Es bleibt noch sich zu vergewissern, dass sie auch linear unabhängig über \mathbb{Q} sind. Seien also $a, b \in \mathbb{Q}$ mit $a \cdot 1 + b \cdot \sqrt{d} = 0$. Schreiben wir $a = \frac{m}{n}$ und $b = \frac{m'}{n'}$ für passende $m, n, m', n' \in \mathbb{Z}$ und formen die vorherige Gleichung um, so erhalten wir

$$m^2 n'^2 = m'^2 n^2 d.$$

Daraus würde aber folgen, dass jeder Primfaktor in d in einer geraden Potenz vorkommen muss (denn auf der linken Seite dieser Gleichung und auch in $m'^2 n^2$ kommt jeder Primfaktor in einer geraden Potenz vor). Da d aber quadratfrei und nicht 1 ist, ist dies nur möglich, wenn bereits $m = m' = 0$ ist, also $a = b = 0$. Somit sind die Elemente 1 und \sqrt{d} linear unabhängig über \mathbb{Q} und es folgt

$$[\mathbb{Q}(\sqrt{d}) : \mathbb{Q}] = \dim_{\mathbb{Q}} \mathbb{Q}(\sqrt{d}) = 2.$$

Natürlich kann man (und werden wir oft) mehrere Körpererweiterungen nacheinander oder, anders gesagt, einen weiteren Körper zwischen einem Grundkörper und seinem Erweiterungskörper betrachten. Wir möchten uns an dieser Stelle kurz Gedanken machen, wie sich der Körpergrad in einem solchen Fall verhält.

Definition 4.7. Sei L/K eine Körpererweiterung. Ein Teilkörper $M \subseteq L$ mit $K \subseteq M$ heißt *Zwischenkörper* von L/K .

Satz 4.8. Sei M ein Zwischenkörper einer endlichen Körpererweiterung L/K . Dann gilt

$$[L : K] = [L : M] \cdot [M : K].$$

Beweis. Wir schreiben $r := [L : M] = \dim_M L$ und $s := [M : K] = \dim_K M$. Sei dann (ℓ_1, \dots, ℓ_r) eine Basis von L als M -Vektorraum und sei (m_1, \dots, m_s) eine Basis von M als K -Vektorraum.

Wir wollen aus diesen beiden Basen eine Basis von L über K konstruieren. Wegen $K \subseteq M \subseteq L$ können wir all diese Elemente als Elemente in L auffassen und dort addieren und multiplizieren. Die Idee für die K -Basis von L ist nun, alle paarweisen Produkte von ℓ_i und m_j zu betrachten, also die Familie $(\ell_1 m_1, \ell_1 m_2, \dots, \ell_1 m_s, \ell_2 m_1, \dots, \ell_r m_s)$.

Behauptung: Die Familie $(m_j \ell_i)_{i=1, \dots, r; j=1, \dots, s}$ ist eine Basis von L als K -Vektorraum.

Kapitel 4 Körpererweiterungen

Zunächst vergewissern wir uns, dass die Familie ein Erzeugendensystem von L über K bildet: Sei $\ell \in L$ beliebig, dann können wir schreiben

$$\ell = \sum_{i=1}^r \mu_i \ell_i$$

für bestimmte $\mu_1, \dots, \mu_r \in M$, da die ℓ_i eine Basis von L über M bilden. Jedes μ_i kann man aber wiederum schreiben als Linearkombination

$$\mu_i = \sum_{j=1}^s a_{ij} m_j$$

für bestimmte $a_{ij} \in K$, da die m_j eine Basis von M über K bilden. Insgesamt ist also

$$\ell = \sum_{i=1}^r \sum_{j=1}^s a_{ij} m_j \ell_i$$

eine K -Linearkombination der $m_j \ell_i$, welche somit ein Erzeugendensystem von L über K bilden.

Dann müssen wir noch die lineare Unabhängigkeit nachprüfen: Seien $a_{ij} \in K$ (für $i \in \{1, \dots, r\}$ und $j \in \{1, \dots, s\}$) sodass

$$\sum_{i=1}^r \sum_{j=1}^s a_{ij} m_j \ell_i = 0.$$

Wir können das (indem wir die Distributivität in L ausnutzen) auch schreiben als

$$\sum_{i=1}^r \underbrace{\left(\sum_{j=1}^s a_{ij} m_j \right)}_{\in M} \ell_i = 0$$

und somit folgt, dass für alle $i \in \{1, \dots, r\}$ gelten muss

$$\sum_{j=1}^s a_{ij} m_j = 0,$$

denn die ℓ_i bilden eine Basis von L über M . Nun bilden aber wiederum die m_j eine Basis von M über K und daher folgt aus der letzten Gleichung, dass $a_{ij} = 0$ für jedes $i \in \{1, \dots, r\}$ und $j \in \{1, \dots, s\}$. Somit ist die Familie der $m_j \ell_i$ auch linear unabhängig über L und insgesamt eine Basis von L über K .

Die Basis $(m_j \ell_i)_{i=1, \dots, r; j=1, \dots, s}$ hat offensichtlich $r \cdot s$ Elemente und somit folgt wie gewünscht

$$[L : K] = \dim_K L = r \cdot s = [L : M] \cdot [M : K].$$

□

Die eben bewiesene Gradformel kann – passend gelesen – auch für unendliche Erweiterungen verstanden werden (denn unser Beweis funktioniert auch für Basen mit unendlich vielen Elementen): Sobald eine der Erweiterung L/M oder M/K nicht endlich ist, ist auch L/K nicht endlich.

Das Beispiel $\mathbb{Q}(\sqrt{d})$ von oben gibt uns schon einen guten Ausblick auf die Art von Erweiterungen, die wir später studieren werden: Wir nehmen einen bekannten Körper und „fügen ein Element hinzu“ (oder auch mehrere Elemente). Die Notation (mit runden Klammern um das „neue“ Element) werden wir gleich noch genauer kennenlernen, hier war das erst einmal einfach eine Schreibweise.

Lemma-Definition 4.9. Sei L/K eine Körpererweiterung und sei $S \subseteq L$ eine beliebige Teilmenge. Dann gibt es einen *eindeutigen kleinsten Zwischenkörper, der S enthält*, d.h. genau einen **Zwischenkörper $K(S)$** (d.h. $K \subseteq K(S) \subseteq L$), sodass $S \subseteq K(S)$ und sodass für jeden Zwischenkörper M von L/K mit $S \subseteq M$ gilt: $K(S) \subseteq M$.

Ist $S = \{\alpha_1, \dots, \alpha_r\}$ eine endliche Menge, so schreiben wir auch kurz $K(\alpha_1, \dots, \alpha_r)$ statt $K(S) = K(\{\alpha_1, \dots, \alpha_r\})$.

Eine Körpererweiterung der Form $K(\alpha)/K$ heißt *einfache Erweiterung*.

Beweis. Sei $I := \{M \text{ Zwischenkörper von } L/K \text{ mit } S \subseteq M\}$ die Menge aller Zwischenkörper, die S enthalten.

Behauptung: Ein kleinstmöglicher Zwischenkörper, der S enthält, ist der Schnitt all dieser Körper, also

$$K(S) := \bigcap_{M \in I} M.$$

Zunächst muss man sich überlegen, dass dies wirklich ein (Zwischen-)Körper ist: Seien $x, y \in K(S) = \bigcap_{M \in I} M$, dann sind also $x, y \in M$ für alle $M \in I$. Da jedes M ein Körper ist, sind also $x + y, xy \in M$ für alle $M \in I$ und folglich $x + y, xy \in K(S) = \bigcap_{M \in I} M$. Wegen $K \subseteq M$ für alle $M \in I$ gilt auch $K \subseteq K(S) = \bigcap_{M \in I} M$, also insbesondere $0, 1, -1 \in K(S)$. Außerdem ist für jedes $x \in K(S) = \bigcap_{M \in I} M$ auch $-x, x^{-1} \in K(S) = \bigcap_{M \in I} M$, denn jedes $M \in I$ ist ein Körper und enthält die additiv und multiplikativ Inversen. Folglich ist also $K(S)$ ein Körper und es ist klar, dass $K \subseteq K(S) \subseteq L$.

Nach Konstruktion ist außerdem klar, dass $S \subseteq K(S)$ (denn $S \subseteq M$ für alle $M \in I$) und dass für jedes $M \in I$ gilt: $K(S) \subseteq M$. Der so konstruierte Körper $K(S)$ erfüllt also die gewünschten Eigenschaften und die Behauptung – also die Existenz eines kleinstmöglichen Zwischenkörpers, der S enthält – ist gezeigt.

Es bleibt noch, die Eindeutigkeit eines solchen $K(S)$ zu zeigen: Seien $\widetilde{K(S)}$ und $\overline{K(S)}$ zwei Körper mit den gewünschten Eigenschaften. Dann gilt aber $\widetilde{K(S)} \subseteq \overline{K(S)}$ (denn $K(S)$ ist ein kleinstmöglicher Körper der S enthält und $\overline{K(S)}$ ist ein anderer Körper, der S enthält), aber ebenso $K(S) \subseteq \widetilde{K(S)}$ (gleiches Argument mit vertauschten Rollen). Also folgt $K(S) = \overline{K(S)}$. \square

Wir lesen $K(S)$ oft als „ K adjungiert S “, oder für ein einzelnes Element: $K(\alpha)$ als „ K adjungiert α “, da diese Körper durch *Adjunktion* (Hinzunahme) der Elemente

Kapitel 4 Körpererweiterungen

in S entstehen. Das bedeutet natürlich nicht, dass $K(S)$ nur aus den Elementen von K und S besteht, sondern auch aus allen anderen Elementen, die notwendig sind, damit $K(S)$ wieder ein Körper wird (zum Beispiel Summen und Produkte von Elementen aus K und S , Inverse solcher Elemente etc.)

Definition 4.10. Sei L/K eine Körpererweiterung und sei $\alpha \in L$. Dann heißt der Ringhomomorphismus

$$K[X] \rightarrow L, \quad f(X) \mapsto f(\alpha)$$

der *Einsetzungshomomorphismus* von α auf $K[X]$.

Das Bild dieses Homomorphismus bezeichnen wir mit $K[\alpha]$, es ist also

$$K[\alpha] := \{f(\alpha) \in L \mid f(X) \in K[X]\} \subseteq L.$$

Im Gegensatz zu $K(\alpha)$ aus Lemma-Definition 4.9, welches ja nach Definition ein Körper war, ist $K[\alpha]$ a priori kein Körper (und wird es im Allgemeinen auch nicht sein). In $K[\alpha]$ gibt es nämlich nicht unbedingt multiplikativ Inverse.

Dafür können wir uns die Elemente in $K[\alpha]$ – im Gegensatz zu denen von $K(\alpha)$ – recht gut vorstellen: Elemente in $K[\alpha]$ sind von der Form $b_n\alpha^n + b_{n-1}\alpha^{n-1} + \dots + b_1\alpha + b_0$ für Koeffizienten $b_0, \dots, b_n \in K$, also polynomielle Ausdrücke in α mit Koeffizienten in K . Eine Division ist also in gewissem Sinne zunächst „nicht vorgesehen“. Wir haben aber in Beispiel 4.2 bereits gesehen, dass sich manchmal auch nur mithilfe polynomieller Ausdrücke Inverse finden lassen. Dies ist genau dann der Fall, wenn α ein *algebraisches Element* ist. Wir werden sehen, dass in diesem Fall die beiden Mengen $K(\alpha)$ und $K[\alpha]$ gleich sind, also insbesondere auch $K[\alpha]$ ein Körper ist.

Lemma 4.11. Sei L/K eine Körpererweiterung und sei $\alpha \in L$. Dann gilt

$$K[\alpha] \subseteq K(\alpha).$$

Genauer gilt: $K[\alpha]$ ist ein K -Untervektorraum und ein Unterring von $K(\alpha)$.

Beweis. Jedes Element $x \in K[\alpha]$ ist von der Form $x = f(\alpha) = a_m\alpha^m + \dots + a_1\alpha + a_0$ für $a_0, \dots, a_m \in K$. Es ist also x ein Element in L , welches sich durch Addition und Multiplikation aus Elementen von K und dem Element α zusammensetzen lässt. Da $K(\alpha)$ ein Körper (und somit abgeschlossen unter Addition und Multiplikation) ist, der K und α enthält, muss er also auch $f(\alpha)$ enthalten. \square

Definition 4.12. Sei L/K eine Körpererweiterung. Ein Element $\alpha \in L$ heißt *algebraisch über K* , falls es ein Polynom $f(X) \in K[X] \setminus \{0\}$ gibt mit $f(\alpha) = 0$. Andernfalls heißt α *transzendent*.

Wie üblich sagen wir, dass α eine *Nullstelle von $f(X)$* ist, wenn $f(\alpha) = 0$ gilt.

Beispiel 4.13. • Jedes Element $\alpha \in K$ ist algebraisch über K , denn α ist eine Nullstelle von $f(X) = X - \alpha \in K[X]$.

(Achtung: Für $\alpha \in L \setminus K$ ist α natürlich auch eine Nullstelle des Polynoms $X - \alpha$, aber dieses Polynom kommt in diesem Fall nicht für $f(X)$ in Frage, um zu zeigen, dass α algebraisch **über K** ist, denn seine Koeffizienten liegen nicht alle in K !)

- $\sqrt{3} \in \mathbb{R}$ ist algebraisch über \mathbb{Q} , denn wir können $f(X) = X^2 - 3$ wählen. Alternativ können wir zum Beispiel auch $f(X) = X^4 - 9$ wählen oder jedes andere rationale Polynom wählen, welches $X^2 - 3$ als Teiler hat.
- Zahlen wie $\pi \in \mathbb{R}$ (Kreiszahl) und $e \in \mathbb{R}$ (eulersche Zahl) sind transzendent über \mathbb{Q} , denn sie sind nicht Nullstelle irgendeines Polynoms mit rationalen Koeffizienten. Dies ist aber nicht einfach zu zeigen.

Wie wir im zweiten Beispiel oben gesehen haben, ist das Polynom $f(X)$ aus Definition 4.12 natürlich nicht eindeutig, wir wollen es aber natürlich im besten Fall möglichst klein und ohne „überflüssige Faktoren“ wählen – das ist die Idee des *Minimalpolynoms*.

Lemma-Definition 4.14. Sei L/K eine Körpererweiterung und $\alpha \in L$ algebraisch über K . Dann existiert ein eindeutiges normiertes Polynom $p(X) \in K[X]$ von minimalem Grad mit $p(\alpha) = 0$. Dieses nennen wir das *Minimalpolynom von α* .

Es gilt dann auch: Ist $f(X) \in K[X]$ ein beliebiges Polynom mit $f(\alpha) = 0$, so gilt $p(X) \mid f(X)$.

Beweis. Betrachte die Menge

$$P := \{f(X) \in K[X] \setminus \{0\} \mid f(\alpha) = 0\}$$

aller Polynome in $K[X]$, die nicht das Nullpolynom sind und α als Nullstelle haben. Da α algebraisch ist, gibt es mindestens ein solches Polynom, d.h. $P \neq \emptyset$. Da der Grad eines Polynoms eine natürliche Zahl (oder 0) ist und somit nach unten beschränkt, gibt es ein Polynom in P mit minimalem Grad. Wir wählen ein solches Polynom. Falls es nicht normiert ist, dividieren wir es durch seinen Leitkoeffizienten. Damit erhalten wir ein normiertes Polynom $p(X)$, welches immer noch α als Nullstelle hat, von minimalem Grad. Dies zeigt die Existenz eines solchen Polynoms.

Ein solches Polynom $p(X)$ erfüllt dann auch die gewünschte Eigenschaft: Sei $f(X) \in K[X]$ ein Polynom mit $f(\alpha) = 0$, dann erhalten wir mittels Polynomdivision

$$f(X) = q(X)p(X) + r(X)$$

für $q(X), r(X) \in K[X]$ mit $\deg(r) < \deg(p)$. Setzen wir in diese Gleichung α ein, so erhalten wir

$$0 = q(\alpha) \cdot 0 + r(\alpha),$$

also $r(\alpha) = 0$. Nach Konstruktion von $p(X)$ kann es aber (außer dem Nullpolynom) kein Polynom kleineren Grades geben, welches α als Nullstelle hat, somit muss gelten $r(X) = 0$. Dann folgt aber $f(X) = q(X)p(X)$, also $p(X) \mid f(X)$.

Kapitel 4 Körpererweiterungen

Es bleibt noch die Eindeutigkeit von $p(X)$ zu beweisen: Seien $p(X), \tilde{p}(X) \in K[X]$ zwei normierte Polynome minimalen Grades mit $p(\alpha) = 0$. Dann gilt nach dem eben Gezeigten, dass $\tilde{p}(X) \mid p(X)$, aber auch $p(X) \mid \tilde{p}(X)$. Die beiden Polynome können sich also höchstens um Multiplikation mit einer Einheit unterscheiden. Da aber beide normiert sind, muss $p(X) = \tilde{p}(X)$ gelten. \square

Lemma 4.15. *Sei L/K eine Körpererweiterung und $\alpha \in L$ algebraisch über K . Dann ist das Minimalpolynom $p(X) \in K[X]$ von α irreduzibel.*

Umgekehrt gilt: Ist $f(X) \in K[X]$ ein irreduzibles, normiertes Polynom mit $f(\alpha) = 0$, dann ist $f(X)$ das Minimalpolynom von α .

Beweis. Wäre $p(X)$ nicht irreduzibel, dann könnte man schreiben $p(X) = f(X)g(X)$ für $f(X), g(X) \in K[X]$, wobei keines der beiden Polynome $f(X)$ und $g(X)$ eine Einheit (also ein konstantes Polynom $\neq 0$) ist. Das bedeutet also, dass sowohl $\deg(f) < \deg(p)$ als auch $\deg(g) < \deg(p)$. Aus $0 = p(\alpha) = f(\alpha) \cdot g(\alpha)$ folgt dann aber $f(\alpha) = 0$ oder $g(\alpha) = 0$, denn der Körper K (in dem sich diese Gleichung abspielt) ist ein Integritätsbereich. Dies ist aber ein Widerspruch, da $p(X)$ das Minimalpolynom von α ist und es somit kein (nicht verschwindendes) Polynom kleineren Grades geben kann, welches α als Nullstelle hat.

Sei umgekehrt $f(X) \in K[X]$ ein irreduzibles Polynom mit $f(\alpha) = 0$ und sei $p(X) \in K[X]$ das Minimalpolynom von α . Dann gilt nach Lemma-Definition 4.14, dass $p(X) \mid f(X)$, also $f(X) = p(X)g(X)$ für ein $g(X) \in K[X]$. Da aber $f(X)$ irreduzibel ist, folgt, dass $g(X) \in (K[X])^\times = K^\times$ eine Einheit ist (denn $p(X)$ kann keine Einheit sein, da es eine Nullstelle hat). Da sowohl $f(X)$ als auch $g(X)$ normiert sind, folgt $g(X) = 1$ und $f(X) = p(X)$. \square

Satz 4.16. *Sei L/K eine Körpererweiterung und $\alpha \in L$ ein Element. Dann sind die folgenden Aussagen äquivalent:*

- (i) α ist algebraisch über K .
- (ii) $K[\alpha]$ ist ein Körper.
- (iii) $K[\alpha] = K(\alpha)$.
- (iv) $K(\alpha)/K$ ist eine endliche Körpererweiterung.

Beweis. Wir führen einen Ringschluss durch.

(i) \Rightarrow (ii): Wir müssen zeigen, dass in $K[\alpha]$ jedes Element außer der 0 ein multiplikativ Inverses besitzt. Zunächst beobachten wir, dass $K[\alpha]$ ein endlichdimensionaler K -Vektorraum ist: Sei $p(X) \in K[X]$ das Minimalpolynom von α und schreibe

$$p(X) = X^n + b_{n-1}X^{n-1} + \dots + b_1X + b_0.$$

Sei jetzt $x \in K[\alpha]$ ein beliebiges Element, d.h. $x = f(\alpha)$ für ein $f(X) \in K[X]$. Dann erhalten wir durch Polynomdivision

$$f(X) = q(X)p(X) + r(X)$$

für $q(X), r(X) \in K[X]$ mit $\deg(r) < \deg(p)$, also $r(X) = c_{n-1}X^{n-1} + \dots + c_1X + c_0$ für gewisse $c_0, \dots, c_{n-1} \in K$. Setzen wir α in diese Gleichung ein, erhalten wir

$$f(\alpha) = \underbrace{q(\alpha)}_{=0} p(\alpha) + r(\alpha) = r(\alpha) = c_{n-1}\alpha^{n-1} + \dots + c_1\alpha + c_0,$$

also $x = f(\alpha) \in \text{Span}_K(1, \alpha, \alpha^2, \dots, \alpha^{n-1})$.

Somit ist die Familie $(1, \alpha, \alpha^2, \dots, \alpha^{n-1})$ ein Erzeugendensystem von $K[\alpha]$ als K -Vektorraum, insbesondere ist $K[\alpha]$ ein endlichdimensionaler K -Vektorraum.

Sei nun $x \in K[\alpha] \setminus \{0\}$ beliebig. Dann ist die Abbildung

$$L \rightarrow L, \quad \ell \mapsto x \cdot \ell$$

injektiv (sogar bijektiv), da x in L ein multiplikativ Inverses hat und es somit eine Umkehrabbildung gibt. (Wir betrachten hier $x \in K[\alpha] \setminus \{0\} \subseteq L$ kurzzeitig als Element in L .)

Schränken wir diese Abbildung nun auf $K[\alpha]$ ein, so liegt ihr Bild wieder in $K[\alpha]$, da $K[\alpha]$ unter Multiplikation abgeschlossen ist und $x \in K[\alpha]$. Wir erhalten also die Abbildung

$$\varphi: K[\alpha] \rightarrow K[\alpha], \quad v \mapsto x \cdot v.$$

Diese ist immer noch injektiv, da sie die Einschränkung einer injektiven Abbildung ist. Außerdem ist diese Abbildung ein K -Vektorraumhomomorphismus (also eine K -lineare Abbildung), denn mithilfe der Eigenschaften von Addition und Multiplikation (die aus dem Körper L kommen) haben wir für alle $v, v_1, v_2 \in K[\alpha]$ und $\kappa \in K$:

$$\begin{aligned} \varphi(v_1 + v_2) &= x \cdot (v_1 + v_2) = x \cdot v_1 + x \cdot v_2 = \varphi(v_1) + \varphi(v_2), \\ \varphi(\kappa v) &= x \cdot (\kappa \cdot v) = \kappa \cdot (x \cdot v) = \kappa \varphi(v). \end{aligned}$$

Wir wissen aber aus der linearen Algebra, dass eine injektive lineare Abbildung zwischen zwei endlichdimensionalen Vektorräumen gleicher Dimension bereits auch surjektiv ist, somit ist $\text{im}(\varphi) = K[\alpha]$, also insbesondere $1 \in \text{im}(\varphi)$. Es gibt also ein $v \in K[\alpha]$ mit $x \cdot v = 1$, also hat x in $K[\alpha]$ ein multiplikativ Inverses.

(ii) \Rightarrow (iii): Es ist immer $K[\alpha] \subseteq K(\alpha)$, wie in Lemma 4.11 gezeigt. Nun ist $K(\alpha)$ nach Definition der kleinste Zwischenkörper von L/K , der K und α enthält. Wenn also $K[\alpha]$ bereits ein Körper ist (der ja auch K und α enthält), dann muss gelten $K[\alpha] = K(\alpha)$.

Kapitel 4 Körpererweiterungen

(iii) \Rightarrow (iv): Ist $\alpha = 0$, so gilt $K(\alpha) = K$, also ist die Körpererweiterung offensichtlich endlich. Nehmen wir also nun an, dass $\alpha \neq 0$. Wegen $K[\alpha] = K(\alpha)$ ist $K[\alpha]$ ein Körper. Es gibt also insbesondere ein multiplikativ Inverses zu α , also ein Element $y \in K[\alpha]$ mit $\alpha \cdot y = 1$. Wir können schreiben $y = g(\alpha)$ für ein Polynom $g(X) \in K[X]$. Dann ist also

$$\alpha \cdot g(\alpha) = 1$$

und folglich $\alpha \cdot g(\alpha) - 1 = 0$. Das Polynom $f(X) := X \cdot g(X) - 1 \in K[X] \setminus \{0\}$ hat daher α als Nullstelle und somit ist α algebraisch über K . Wir haben in „(i) \Rightarrow (ii)“ bereits gezeigt, dass $K[\alpha]$ für ein algebraisches Element α ein endlichdimensionaler K -Vektorraum ist, also folgt hier

$$[K(\alpha) : K] = \dim_K K(\alpha) \stackrel{(iii)}{=} \dim_K K[\alpha] < \infty.$$

(iv) \Rightarrow (i): Sei $[K(\alpha) : K] = \dim_K K(\alpha) < \infty$ gegeben. Dann haben wir auch $\dim_K K[\alpha] < \infty$, denn nach Lemma 4.11 ist $K[\alpha]$ ein Untervektorraum von $K(\alpha)$. Wir bezeichnen diese Dimension mit $n := \dim_K K[\alpha]$ und betrachten die Familie $(1, \alpha, \alpha^2, \dots, \alpha^n)$ von $n + 1$ Elementen im K -Vektorraum $K[\alpha]$. Diese muss also linear abhängig sein, d.h. es gibt $b_0, \dots, b_n \in K$, sodass nicht alle b_j gleich 0 sind und sodass

$$b_0 \cdot 1 + b_1 \cdot \alpha + \dots + b_n \cdot \alpha^n = 0.$$

Folglich hat das Polynom $f(X) := b_n X^n + \dots + b_1 X + b_0 \in K[X]$ das Element α als Nullstelle, weshalb α algebraisch über K ist.

□

Wir fassen eine Aussage aus dem Beweisschritt „(i) \Rightarrow (ii)“ noch etwas präziser.

Korollar 4.17. Sei L/K eine Körpererweiterung und $\alpha \in L$ algebraisch mit Minimalpolynom $p(X) \in K[X]$. Sei $n := \deg(p)$. Dann ist die Familie $(1, \alpha, \alpha^2, \dots, \alpha^{n-1})$ eine Basis von $K[\alpha]$ als K -Vektorraum und somit auch $[K(\alpha) : K] = \deg(p)$.

Beweis. Im Beweisschritt „(i) \Rightarrow (ii)“ von Satz 4.16 haben wir bereits gesehen, dass die Familie $(1, \alpha, \alpha^2, \dots, \alpha^{n-1})$ ein Erzeugendensystem ist. Es fehlt also noch die lineare Unabhängigkeit: Seien $c_0, \dots, c_{n-1} \in K$ mit

$$c_0 \cdot 1 + \dots + c_{n-1} \cdot \alpha^{n-1} = 0.$$

Dann ist also α eine Nullstelle des Polynoms $g(X) = c_{n-1} X^{n-1} + \dots + c_1 X + c_0 \in K[X]$ mit $\deg(g) = n - 1$. Da aber $p(X)$ mit $\deg(p) = n$ das Minimalpolynom von α ist, kann es außer dem Nullpolynom kein Polynom kleineren Grades geben, welches α als Nullstelle hat. Folglich muss gelten $g(X) = 0$, also $c_0 = \dots = c_{n-1} = 0$, und somit ist die Familie $(1, \alpha, \alpha^2, \dots, \alpha^{n-1})$ linear unabhängig.

Für den Körpergrad gilt dann (da wir nach Satz 4.16 bereits $K(\alpha) = K[\alpha]$ wissen)

$$[K(\alpha) : K] = \dim_K K(\alpha) = \dim_K K[\alpha] = n = \deg(p).$$

□

Den Begriff *algebraisch* kann man nicht nur für ein einzelnes Element, sondern auch für eine Körpererweiterung definieren.

Definition 4.18. Eine Körpererweiterung L/K heißt *algebraisch*, wenn jedes Element $\alpha \in L$ algebraisch über K ist (im Sinne der Definition 4.12).

Eine interessante und wichtige Aussage ist dann die folgende.

Korollar 4.19. Ist L/K eine endliche Körpererweiterung, so ist L/K algebraisch.

Beweis. Sei $[L : K] < \infty$ und sei $\alpha \in L$ ein beliebiges Element. Dann betrachten wir den Zwischenkörper $K(\alpha) \in L$. Dieser ist ein Untervektorraum von L und daher gilt

$$\dim_K K(\alpha) \leq \dim_K L = [L : K] < \infty$$

und nach Satz 4.16 ist damit α algebraisch über K . □

Satz 4.20. Sind $K \subseteq M \subseteq L$ Körpererweiterungen und sind L/M und M/K algebraisch, so ist auch L/K algebraisch.

Beweis. Sei $\alpha \in L$ beliebig. Wir müssen zeigen, dass α algebraisch über K ist. Nach Voraussetzung, dass L/M algebraisch ist, wissen wir a priori, dass α algebraisch über M ist, dass es also ein Polynom $f(X) \in M[X]$ gibt mit $f(\alpha) = 0$. Wir schreiben

$$f(X) = \mu_m X^m + \mu_{m-1} X^{m-1} + \dots + \mu_1 X + \mu_0$$

mit Koeffizienten $\mu_0, \dots, \mu_m \in M$.

Da nach Voraussetzung auch M/K algebraisch ist, sind all diese Koeffizienten μ_i algebraisch über K . Wir betrachten den Zwischenkörper $K(\mu_0, \dots, \mu_m)$ von L/K . Dieser ist endlich über K , denn wendet man wiederholt die Gradformel an, erhält man

$$\begin{aligned} [K(\mu_0, \dots, \mu_m) : K] &= [K(\mu_0, \dots, \mu_m) : K(\mu_0, \dots, \mu_{m-1})] \cdot [K(\mu_0, \dots, \mu_{m-1}) : K] \\ &= \dots \\ &= \underbrace{[K(\mu_0, \dots, \mu_m) : K(\mu_0, \dots, \mu_{m-1})]}_{< \infty} \cdot \dots \cdot \underbrace{[K(\mu_0) : K]}_{< \infty} \\ &< \infty. \end{aligned}$$

Außerdem ist α algebraisch über $K(\mu_0, \dots, \mu_m)$ (denn das Polynom $f(X)$ liegt in $K(\mu_0, \dots, \mu_m)[X]$). Also ist auch

$$[K(\mu_0, \dots, \mu_m, \alpha) : K(\mu_0, \dots, \mu_m)] < \infty$$

Kapitel 4 Körpererweiterungen

und somit (wieder mit der Gradformel) insgesamt

$$[K(\mu_0, \dots, \mu_m, \alpha) : K] = [K(\mu_0, \dots, \mu_m, \alpha) : K(\mu_0, \dots, \mu_m)] \cdot [K(\mu_0, \dots, \mu_m) : K] < \infty.$$

Nach Korollar 4.19 ist dann jedes Element in $K(\mu_0, \dots, \mu_m, \alpha)$ und somit insbesondere α algebraisch über K . \square

Wir beschließen diesen Abschnitt mit einer Aussage, die uns im Folgenden sehr nützlich sein wird: Wir haben oben gesehen, dass Körpererweiterungen, bei denen nur ein einzelnes, algebraisches Element adjungiert wird, besonders schöne Eigenschaften haben. Das nächste Lemma gibt uns noch eine etwas abstraktere Sichtweise auf solche Erweiterungen.

Lemma 4.21. *Sei L/K eine Körpererweiterung und $\alpha \in L$ algebraisch. Sei $p(X)$ das Minimalpolynom von α über K . Dann haben wir einen Körperisomorphismus*

$$K(\alpha) \cong K[X]/(p(X)).$$

Beweis. Da α algebraisch ist, gilt $K(\alpha) = K[\alpha]$ (Satz 4.16) und letzteres ist nach Definition 4.10 das Bild des Einsetzungshomomorphismus

$$\text{ev}_\alpha: K[X] \rightarrow L, \quad f(X) \mapsto f(\alpha).$$

Wir haben also eine surjektive Abbildung $\text{ev}_\alpha: K[X] \rightarrow K[\alpha], f(X) \mapsto f(\alpha)$. Der Kern dieser Abbildung ist die Menge (sogar das Ideal) aller Polynome, die α als Nullstelle haben. Nach Lemma-Definition 4.14 sind das aber genau die Polynome, die Vielfache von $p(X)$ sind, also ist $\ker(\text{ev}_\alpha) = (p(X))$, das von $p(X)$ erzeugte Hauptideal in $K[X]$. Nach dem Homomorphiesatz für Ringe (Satz 3.22) induziert ev_α also einen Isomorphismus

$$K[X]/(p(X)) \xrightarrow{\cong} K[\alpha], \quad [f(X)] \mapsto f(\alpha).$$

\square

Wir merken noch an, dass man leicht sehen kann, dass der Quotientenring $K[X]/(p(X))$ ein Körper ist – auch ohne zu wissen, dass er isomorph zu $K(\alpha)$ ist: Das Minimalpolynom ist irreduzibel (Lemma 4.15), daher ist das Ideal $(p(X)) \triangleleft K[X]$ ein maximales Ideal (Lemma 3.65) und somit der Quotient $K[X]/(p(X))$ ein Körper (Satz 3.51).

4.2 Von Polynomen zu Körpererweiterungen

Schauen wir noch einmal kurz auf Lemma 4.21 zurück: Wir haben dort gesehen, dass es einen Isomorphismus gibt zwischen $K(\alpha)$ und $K[X]/(p(X))$. Dem Element α auf der linken Seite entspricht die Äquivalenzklasse $[X]$, des Polynoms X auf der rechten Seite. Beide erfüllen dieselbe Eigenschaft: Auf der linken Seite gilt

$p(\alpha) = 0$, auf der rechten Seite gilt $p([X]) = [p(X)] = 0$. Auf den ersten Blick wirkt die rechte Seite komplizierter und vielleicht unnötig abstrakt. Sie hat aber einen entscheidenden Vorteil: Während man auf der linken Seite das Element α bereits kennen muss, um den Körper $K(\alpha)$ zu konstruieren, kann man die rechte Seite auch konstruieren, wenn man nur $p(X)$ gegeben hat, aber vielleicht noch keine Nullstelle kennt.

In anderen Worten: Bisher haben wir immer angenommen, dass wir einen größeren Körper L kennen, in dem es das Element α schon gibt und dann den Zwischenkörper $K(\alpha)$ konstruiert. Was aber tun wir, wenn wir nur den Körper K haben und ein Polynom, das in K noch keine Nullstelle hat? Dann wollen wir K so erweitern, dass unser Polynom eine Nullstelle besitzt. Das erinnert uns an die Konstruktion der komplexen Zahlen \mathbb{C} : Wir müssen eine Lösung i der Gleichung $X^2 + 1 = 0$ „erfinden“ (als reines Symbol) und zu \mathbb{R} hinzufügen.

Satz 4.22. Sei K ein Körper und sei $f(X) \in K[X]$ ein irreduzibles Polynom mit $\deg(f) \geq 1$. Dann gibt es eine endliche Körpererweiterung L/K , sodass $f(X)$ eine Nullstelle in L hat. Explizit ist eine solche Erweiterung gegeben durch

$$L := K[T]/(f(T)).$$

Beweis. Wir verwenden hier zunächst die Variable T anstelle von X , um sie später von der Polynomvariablen X zu unterscheiden.

Da $f(T)$ irreduzibel ist, ist $(f(T)) \triangleleft K[T]$ ein maximales Ideal und somit $L := K[T]/(f(T))$ ein Körper (siehe auch den letzten Absatz im vorherigen Abschnitt).

Die Abbildung

$$K \rightarrow K[T]/(f(T)), \quad a \mapsto [a],$$

die ein Element a des Körpers auf die Äquivalenzklasse des konstanten Polynoms a abbildet, ist ein Körperhomomorphismus (wie man leicht sieht) und damit automatisch injektiv nach Korollar 3.20. Es gilt also $K \subseteq L$ und L/K ist eine Körpererweiterung.

Behauptung: Das Element $\alpha := [T] \in L$ ist eine Nullstelle des Polynoms $f(X)$.

Etwas präziser bedeutet diese Behauptung Folgendes: Wir schreiben $f(X) = b_n X^n + b_{n-1} X^{n-1} + \dots + b_1 X + b_0 \in K[X]$ (wobei $\deg(f) = n$, also $b_n \neq 0$). In diesem Polynom können wir die Koeffizienten $b_j \in K$ als Elemente in L auffassen (also durch $[b_j] \in L = K[T]/(f(T))$ ersetzen, d.h. wir wenden die Einbettung $K \hookrightarrow L$ von oben an) und für die Variable X das Element $\alpha = [T] \in L = K[T]/(f(T))$ einsetzen. Die Behauptung ist dann, dass dies 0 ergibt, genauer gesagt das neutrale Element der Addition in L , also $[0] \in L = K[T]/(f(T))$.

Dies können wir leicht nachrechnen:

$$\begin{aligned} f(\alpha) &= f([T]) = [b_n] \cdot [T]^n + [b_{n-1}] \cdot [T]^{n-1} + \dots + [b_1] \cdot [T] + [b_0] \\ &= [b_n T^n + b_{n-1} T^{n-1} + \dots + b_1 T + b_0] \\ &= [f(T)] = [0]. \end{aligned}$$

□

Nach Konstruktion hat dieser Erweiterungskörper aus Satz 4.22 jetzt, wo die Nullstelle von $f(X)$ einen Namen bekommen hat, eine Beschreibung wie im vorigen Abschnitt: Er entsteht durch Adjunktion einer einzelnen Nullstelle zu K .

Korollar 4.23. Sei K ein Körper, $f(X) \in K[X]$ ein irreduzibles Polynom mit $\deg(f) \geq 1$ und $L := K[T]/(f(T))$. Sei $\alpha := [T] \in L$ eine Nullstelle von $f(X)$ in L . Dann gilt: $K(\alpha) = L$.

Beweis. A priori ist $K(\alpha)$ ein Zwischenkörper von L/K , also $K(\alpha) \subseteq L$. Andererseits ist jedes Element in L von der Form $[g(T)] = g([T]) = g(\alpha)$ für ein $g(X) \in K[X]$, also nach Definition ein Element von $K[\alpha]$. Somit gilt auch $K \subseteq K[\alpha]$ und damit die Gleichheit $K[\alpha] = L$. □

Wir können jetzt also einen Körper konstruieren, der *eine* Nullstelle eines zuvor nullstellenfreien Polynoms $f(X)$ enthält. Der Körper $L = K[T]/(f(T))$ enthält aber möglicherweise noch nicht *alle* Nullstellen von $f(X)$, sodass man in $L[X]$ zwar $f(X) = (X - \alpha) \cdot g(X)$ für ein $\alpha \in L$ und ein $g(X) \in L[X]$ schreiben kann, aber $f(X)$ möglicherweise noch nicht komplett in Linearfaktoren zerfällt. Man muss die Konstruktion aus Satz 4.22 also eventuell wiederholt anwenden, um einen Körper zu erhalten, der K erweitert und zusätzlich alle Nullstellen von $f(X)$ erhält, aber eben auch „nicht mehr als das“. Ein solcher Körper bekommt einen eigenen Namen.

Definition 4.24. Sei K ein Körper und $f(X) \in K[X]$ ein Polynom mit $\deg(f) \geq 1$. Ein Erweiterungskörper L von K heißt **Zerfällungskörper von f** , falls gilt:

- (1) $f(X) \in K[X] \subseteq L[X]$ zerfällt in $L[X]$ in Linearfaktoren, d.h. es gibt paarweise verschiedene Elemente $\alpha_1, \dots, \alpha_m \in L$ ($m \in \mathbb{N}$) und es gibt $v_1, \dots, v_m \in \mathbb{N}$ und $c \in K$, sodass

$$f(X) = c \cdot \prod_{j=1}^m (X - \alpha_j)^{v_j} = c \cdot (X - \alpha_1)^{v_1} \cdot \dots \cdot (X - \alpha_m)^{v_m}.$$

- (2) L wird von den Nullstellen von $f(X)$ erzeugt, d.h. sind $\alpha_1, \dots, \alpha_m \in L$ die (paarweise verschiedenen) Nullstellen von $f(X)$ und betrachtet man den Zwischenkörper $K[\alpha_1, \dots, \alpha_m] \subseteq L$, so gilt bereits

$$K[\alpha_1, \dots, \alpha_m] = L.$$

Ein Zerfällungskörper von f ist also eine minimal mögliche Körpererweiterung, in der $f(X)$ genügend Nullstellen hat, um in Linearfaktoren zu zerfallen. Einen solchen Zerfällungskörper kann man immer konstruieren, indem man die Konstruktion aus Satz 4.22, wie oben angedeutet, geschickt und wiederholt anwendet.

Satz 4.25. Ist K ein Körper und $f(X) \in K[X]$ ein Polynom mit $\deg(f) \geq 1$, dann gibt es einen Zerfällungskörper Z/K von f .

Beweis. Zunächst muss $f(X)$ nicht irreduzibel sein, sodass wir die Konstruktion aus Satz 4.22 nicht direkt anwenden können. Das Polynom $f(X)$ hat aber sicher einen irreduziblen Faktor, d.h. wir können es schreiben als

$$f(X) = f_1(X) \cdot g(X)$$

für $f_1(X), g(X) \in K[X]$, wobei $f_1(X)$ irreduzibel ist. (Dies ist möglich, da $K[X]$ ein faktorieller Ring ist, d.h. man kann jedes Element in irreduzible Faktoren zerlegen, von denen $f_1(X)$ einer ist und alle anderen hier in $g(X)$ zusammengefasst werden.) Dann definieren wir den Körper

$$K_1 := K[T]/(f_1(T)),$$

der dann eine Nullstelle α_1 von $f_1(X)$ (also auch eine Nullstelle von $f(X)$) enthält und tatsächlich gilt $K_1 = K[\alpha_1]$.

Betrachten wir das Polynom $f(X)$ nun also in $K_1[X]$, so können wir den Linearfaktor $(X - \alpha_1)$ abspalten, evtl. mehrfach, wir können also schreiben

$$f(X) = (X - \alpha_1)^{v_1} \cdot \tilde{f}(X),$$

für ein $v_1 \in \mathbb{N}$ und ein Polynom $\tilde{f}(X) \in K_1[X]$, sodass $\tilde{f}(X)$ keine Nullstelle bei α_1 hat. Es gilt dann $\deg(\tilde{f}) = \deg(f) - v_1 < \deg(f)$.

Falls $\tilde{f}(X)$ nicht bereits ein konstantes Polynom ist, wiederholen wir nun diesen Vorgang mit dem Polynom $\tilde{f}(X)$ und nun über dem neuen Grundkörper K_1 anstelle von K : Wir schreiben es als

$$\tilde{f}(X) = f_2(X) \cdot \tilde{g}(X)$$

für $f_2(X), \tilde{g}(X) \in K_1[X]$ mit irreduziblem $f_2(X)$. (Das geht, denn auch $K_1[X]$ ist ein faktorieller Ring.) Mit der Konstruktion aus Satz 4.22 finden wir einen Körper K_2 , der eine Nullstelle α_2 von $f_2(X)$ (also insbesondere eine weitere Nullstelle unseres ursprünglichen $f(X)$) enthält. Anders gesagt gilt $K_2 = K[\alpha_1, \alpha_2]$ und man kann diese Nullstelle wieder abspalten, d.h.

$$f(X) = (X - \alpha_1)^{v_1} \cdot (X - \alpha_2)^{v_2} \cdot \tilde{\tilde{f}}(X)$$

für ein $v_2 \in \mathbb{N}$ und ein Polynom $\tilde{\tilde{f}}(X) \in K_2[X]$, welches keine Nullstelle bei α_1 und α_2 hat und außerdem $\deg \tilde{\tilde{f}} = \deg(f) - v_1 - v_2 < \deg(\tilde{f})$ erfüllt.

Nun wiederholen wir dasselbe mit $\tilde{\tilde{f}}(X)$ (falls es nicht bereits vom Grad 0 ist) und führen dieses Vorgehen so oft fort, bis wir nach endlich vielen Schritten bei einem Körper $K_r = K[\alpha_1, \dots, \alpha_r]$ ankommen, über dem gilt

$$f(X) = c \cdot (X - \alpha_1)^{v_1} \cdot (X - \alpha_2)^{v_2} \cdot \dots \cdot (X - \alpha_m)^{v_m}$$

Kapitel 4 Körpererweiterungen

für eine Konstante $c \in K_m$. (In Wirklichkeit ist dann automatisch $c \in K$, denn multipliziert man die rechte Seite aus, wird c zum Leitkoeffizienten des Polynoms und $f(X)$ hat Koeffizienten in K .) Dieser Zustand wird nach endlich vielen Schritten erreicht, da der Grad des „Restpolynoms“ (d.h. von $\tilde{f}(X)$, $\tilde{\tilde{f}}(X)$ etc.) in jedem Schritt echt kleiner wird und somit nach endlich vielen Schritten außer der Linearfaktoren nur noch ein konstantes Polynom c übrigbleibt.

Der gesuchte Körper Z ist dann K_r , denn dieser ist offensichtlich ein Zerfällungskörper von $f(X)$. \square

Im eben bewiesenen Satz wurde die Existenz eines (abstrakten) Zerfällungskörpers bewiesen. Es ist zunächst nicht klar, ob Zerfällungskörper in gewisser Weise eindeutig sind, weshalb wir von *einem* und nicht *dem* Zerfällungskörper sprechen. (Die Frage der Eindeutigkeit wird in Korollar 4.38 noch einmal aufgegriffen.)

Falls $f(X) \in K[X]$ aber ein Polynom ist und wir bereits einen größeren Körper L mit $K \subseteq L$ kennen, in dem $f(X)$ in Linearfaktoren zerfällt, so können wir von *dem* Zerfällungskörper Z von f in L sprechen. Dieser ist dann gegeben durch $Z = K[\alpha_1, \dots, \alpha_n]$, wenn $\alpha_1, \dots, \alpha_n$ alle Nullstellen von $f(X)$ in L sind. Oft (wie auch im folgenden Beispiel) sind wir in dieser Situation, wenn wir Polynome in $\mathbb{Q}[X]$ betrachten und wir den Körper \mathbb{C} bereits kennen.

Beispiel 4.26. Betrachten wir das Polynom $f(X) = X^3 - 2 \in \mathbb{Q}[X]$ und versuchen wir seinen Zerfällungskörper zu verstehen. Das Polynom ist irreduzibel (nach dem Eisenstein-Kriterium). Wir kennen die Nullstellen von $f(X)$ in \mathbb{C} , nämlich die reelle Nullstelle $\alpha_1 = \sqrt[3]{2}$ sowie die beiden komplexen Nullstellen $\alpha_2 = \sqrt[3]{2} \cdot e^{\frac{2\pi i}{3}}$ und $\alpha_3 = \sqrt[3]{2} \cdot e^{\frac{4\pi i}{3}}$.

Ein Zerfällungskörper ist also $Z := \mathbb{Q}[\alpha_1, \alpha_2, \alpha_3]$. Welchen Körpergrad hat diese Erweiterung von \mathbb{Q} ?

Bauen wir diesen Körper Schritt für Schritt auf: Wir haben eine Kette von Körpererweiterungen

$$K \subseteq K_1 = \mathbb{Q}[\alpha_1] \subseteq K_2 = \mathbb{Q}[\alpha_1, \alpha_2] \subseteq Z = K_3 = \mathbb{Q}[\alpha_1, \alpha_2, \alpha_3].$$

Oft zeichnet man sich dies auch vertikal als sogenannten *Körperturm* auf:

$$\begin{array}{c} Z = K_3 = \mathbb{Q}[\alpha_1, \alpha_2, \alpha_3] \\ | \\ K_2 = \mathbb{Q}[\alpha_1, \alpha_2] \\ | \\ K_1 = \mathbb{Q}[\alpha_1] \\ | \\ \mathbb{Q} \end{array}$$

Kapitel 4 Körpererweiterungen

Eine partielle Antwort darauf wird uns der Fortsetzungssatz geben, der beschreibt, wie sich Körperhomomorphismen unter bestimmten Bedingungen von einer Etage auf die darüberliegende Etage erweitern lassen.

Lemma-Definition 4.27. Sei $\varphi: K \rightarrow K'$ ein Körperhomomorphismus. Dann ist die Abbildung

$$K[X] \rightarrow K'[X], \quad f(X) = \sum_{i=0}^n a_i X^i \mapsto f^\varphi(X) := \sum_{i=0}^n \varphi(a_i) X^i$$

ein Ringhomomorphismus.

Ist φ ein Körperisomorphismus, so ist diese Abbildung ein Ringisomorphismus. In diesem Fall ist ein Polynom $f(X) \in K[X]$ genau dann irreduzibel, wenn $f^\varphi(X) \in K'[X]$ irreduzibel ist.

Beweis. Es ist zu prüfen, dass $(f + g)^\varphi(X) = f^\varphi(X) + g^\varphi(X)$ und $(f \cdot g)^\varphi(X) = f^\varphi(X)g^\varphi(X)$ gilt und dass $1^\varphi = 1$. All dies folgt leicht aus der Voraussetzung, dass φ ein Körperhomomorphismus ist.

Falls φ ein Körperhomomorphismus ist (dessen Inverses wir mit f^{-1} bezeichnen), so ist der Ringhomomorphismus $K'[X] \rightarrow K[X], g(X) \mapsto g^{\varphi^{-1}}(X)$ offensichtlich eine Umkehrabbildung von $K[X] \rightarrow K'[X], f(X) \mapsto f^\varphi(X)$. Letztere ist als ein Ringisomorphismus. Sei nun $f(X) \in K[X]$ irreduzibel. Dann wollen wir zeigen, dass auch $f^\varphi(X) \in K'[X]$ irreduzibel ist. Sei also $f^\varphi(X) = g(X)h(X)$ für bestimmte $g(X), h(X) \in K'[X]$. Dann wenden wir die Umkehrabbildung an und erhalten

$$f(X) = g^{\varphi^{-1}}(X) \cdot h^{\varphi^{-1}}(X).$$

Da $f(X)$ irreduzibel ist, muss aber $g^{\varphi^{-1}}(X)$ oder $h^{\varphi^{-1}}(X)$ eine Einheit in $K[X]$ sein. Dann ist aber auch $g(X)$ oder $h(X)$ eine Einheit in $K'[X]$, da ein Ringisomorphismus Einheiten (und nur diese) auf Einheiten abbildet. Analog zeigt man, dass aus der Irreduzibilität von $f^\varphi(X)$ die Irreduzibilität von $f(X)$ folgt. \square

Lemma 4.28. Seien K und K' zwei Körper und $\varphi: K \rightarrow K'$ ein Körperhomomorphismus. Sei $f(X) \in K[X]$ ein Polynom und sei L/K eine Körpererweiterung, sodass es eine Nullstelle $\alpha \in L$ von $f(X)$ gibt. Sei weiter L'/K' eine Körpererweiterung und $\tilde{\varphi}: L \rightarrow L'$ ein Körperhomomorphismus mit $\tilde{\varphi}|_K = \varphi$. Grafisch sei also die folgende Situation gegeben:

$$\begin{array}{ccc} \alpha \in L & \xrightarrow{\tilde{\varphi}} & L' \\ | & & | \\ K & \xrightarrow{\varphi} & K'. \end{array}$$

Dann ist $\tilde{\varphi}(\alpha)$ eine Nullstelle von $f^\varphi(X) \in K'[X]$.

Beweis. Dies können wir direkt nachrechnen: Schreibe $f(X) = \sum_{i=0}^n a_i X^i$ und beachte, dass $a_i \in K$ und somit $\tilde{\varphi}(a_i) = \varphi(a_i)$. Dann ist

$$f^\varphi(\tilde{\varphi}(\alpha)) = \sum_{i=0}^n \varphi(a_i)(\tilde{\varphi}(\alpha))^i = \sum_{i=0}^n \tilde{\varphi}(a_i)(\tilde{\varphi}(\alpha))^i = \tilde{\varphi}\left(\sum_{i=0}^n a_i \alpha^i\right) = \tilde{\varphi}(f(\alpha)) = \tilde{\varphi}(0) = 0,$$

wobei wir verwendet haben, dass $\tilde{\varphi}$ ein Körperhomomorphismus ist und α eine Nullstelle von $f(X)$. \square

Insbesondere bedeutet die Aussage von Lemma 4.28 Folgendes für den Fall $K = K'$.

Korollar 4.29. *Sind L/K und L'/K zwei verschiedene algebraische Erweiterungen desselben Grundkörpers K und ist $\tilde{\varphi}: L \rightarrow L'$ ein Körperhomomorphismus mit $\tilde{\varphi}(x) = x$ für jedes $x \in K$, dann haben für jedes $\alpha \in L$ die Elemente $\alpha \in L$ und $\tilde{\varphi}(\alpha) \in L'$ dasselbe Minimalpolynom.*

Beweis. Wir wenden Lemma 4.28 für den Fall $\varphi = \text{id}_K$ an: Sei $\alpha \in L$ und sei $p(X) \in K[X]$ das Minimalpolynom von α über K . Dann ist $\tilde{\varphi}(\alpha)$ eine Nullstelle von $p^{\text{id}_K}(X) = p(X)$. Da $p(X)$ irreduzibel ist, ist es nach Lemma 4.15 automatisch auch das Minimalpolynom von $\tilde{\varphi}(\alpha)$. \square

Satz 4.30 (Fortsetzungssatz für einfache Erweiterungen). *Seien K und K' zwei Körper und $\varphi: K \rightarrow K'$ ein Körperhomomorphismus. Sei $f(X) \in K[X]$ ein irreduzibles Polynom. Sei weiter L/K eine Körpererweiterung und $\alpha \in L$ eine Nullstelle von $f(X)$ sowie L'/K' eine Körpererweiterung und $\beta \in L'$ eine Nullstelle von $f^\varphi(X)$. Dann gibt es einen eindeutigen Körperhomomorphismus $\tilde{\varphi}: K[\alpha] \rightarrow K'[\beta]$ mit $\tilde{\varphi}|_K = \varphi$ und $\tilde{\varphi}(\alpha) = \beta$.*

Grafisch veranschaulicht:

$$\begin{array}{ccc} L & & L' \\ | & & | \\ K[\alpha] & \xrightarrow{\exists! \tilde{\varphi}} & K'[\beta] \\ | & & | \\ K & \xrightarrow{\varphi} & K' \end{array}$$

Außerdem gilt: Ist φ ein Körperisomorphismus, so ist auch $\tilde{\varphi}$ ein Körperisomorphismus.

Beweis. Da $f(X)$ irreduzibel ist, ist $\frac{1}{a_m} f(X)$ das Minimalpolynom von α , wobei $a_m \neq 0$ der Leitkoeffizient von $f(X) = \sum_{i=0}^m a_i X^i$ ist. Außerdem bezeichnen wir mit $p(X) \in K'[X]$ das Minimalpolynom von β . Dann gibt es nach Lemma 4.21 Körperisomorphismen

$$\sigma_\alpha: K[\alpha] \xrightarrow{\cong} K[X]/(f(X)) \quad \text{und} \quad \sigma_\beta: K'[\beta] \xrightarrow{\cong} K'[X]/(p(X)).$$

Unter diesen Isomorphismen entspricht das Element α der Äquivalenzklasse $[X]$ des Polynoms $X \in K[X]$ und das Element β der Äquivalenzklasse $[X]$ des Polynoms $X \in K'[X]$.

Kapitel 4 Körpererweiterungen

Behauptung: Die Vorschrift

$$\psi: K[X]/(f(X)) \rightarrow K'[X]/(p(X)), \quad [g(X)] \mapsto [g^\varphi(X)]$$

definiert einen (wohldefinierten) Körperhomomorphismus.

Die Axiome eines Körperhomomorphismus sind klar (wie auch in Lemma-Definition 4.27). Es bleibt also noch die Wohldefiniertheit zu zeigen. Wir bemerken zuerst, dass nach Voraussetzung $f^\varphi(\beta) = 0$ gilt und daher $p(X) \mid f^\varphi(X)$ folgt. Wir können also schreiben $f^\varphi(X) = h(X) \cdot p(X)$ für ein $h(X) \in K'[X]$.

Seien nun $g_1(X), g_2(X) \in K[X]$, sodass $[g_1(X)] = [g_2(X)]$ in $K[X]/(f(X))$, d.h. $g_2(X) = g_1(X) + q(X) \cdot f(X)$ für ein $q(X) \in K[X]$. Dann ist

$$\begin{aligned} g_2^\varphi(X) &= g_1^\varphi(X) + q^\varphi(X) \cdot f^\varphi(X) \\ &= g_1^\varphi(X) + q^\varphi(X) \cdot h(X) \cdot p(X) \end{aligned}$$

und somit $[g_1^\varphi(X)] = [g_2^\varphi(X)]$ in $K'[X]/(p(X))$.

Offensichtlich bildet der Körperhomomorphismus ψ aus der obigen Behauptung eine Äquivalenzklasse $[c]$ eines konstanten Polynoms $c \in K$ auf die Äquivalenzklasse $[\varphi(c)]$ des konstanten Polynoms $\varphi(c) \in K'$ ab. Außerdem ist $\psi([X]) = [X]$. Setzen wir ihn nun also passend mit den Isomorphismen σ_α und σ_β zusammen, so erhalten wir den gesuchten Körperhomomorphismus

$$\tilde{\varphi} := \sigma_\beta^{-1} \circ \psi \circ \sigma_\alpha: K[\alpha] \xrightarrow{\sigma_\alpha} K[X]/(f(X)) \xrightarrow{\psi} K'[X]/(p(X)) \xrightarrow{\sigma_\beta^{-1}} K'[\beta]$$

mit $\tilde{\varphi}|_K = \varphi$ und $\tilde{\varphi}(\alpha) = \beta$. Dies beweist die Existenz von $\tilde{\varphi}$.

Zur Eindeutigkeit: Jedes Element von $K[\alpha]$ ist von der Form $g(\alpha) = b_n \alpha^n + \dots + b_1 \alpha + b_0$ für $b_0, \dots, b_n \in K$. Ist also $\tilde{\varphi}: K[\alpha] \rightarrow K'[\beta]$ ein Körperhomomorphismus mit $\tilde{\varphi}|_K = \varphi$ und $\tilde{\varphi}(\alpha) = \beta$, dann ist automatisch

$$\begin{aligned} \tilde{\varphi}(b_n \alpha^n + \dots + b_1 \alpha + b_0) &= \tilde{\varphi}(b_n) \tilde{\varphi}(\alpha)^n + \dots + \tilde{\varphi}(b_1) \tilde{\varphi}(\alpha) + \tilde{\varphi}(b_0) \\ &= \varphi(b_n) \beta^n + \dots + \varphi(b_1) \beta + \varphi(b_0), \end{aligned}$$

die beiden Bedingungen legen das Bild jedes Elementes von $K[\alpha]$ unter $\tilde{\varphi}$ also bereits eindeutig fest.

Es bleibt noch zu zeigen, dass $\tilde{\varphi}$ ein Isomorphismus ist, wenn φ ein solcher ist: Ist φ ein Isomorphismus, so ist auch der entsprechende Ringhomomorphismus aus Lemma-Definition 4.27 ein Isomorphismus (es gibt eine offensichtliche Umkehrabbildung, die von φ^{-1} induziert ist). Es ist dann $f^\varphi(X)$ irreduzibel und somit das Minimalpolynom von β . Dann überlegt man sich leicht, dass die obige Abbildung $\psi: K[X]/(f(X)) \rightarrow K'[X]/(f^\varphi(X))$ ebenfalls ein Isomorphismus ist und folglich auch die Abbildung $\tilde{\varphi} = \sigma_\beta^{-1} \circ \psi \circ \sigma_\alpha$. \square

Konkret bedeutet der Fortsetzungssatz im Fall $\varphi = \text{id}_K$ wieder Folgendes: Sind α, β zwei verschiedene Nullstellen eines irreduziblen Polynoms $f(X)$, so gibt es einen eindeutigen Körperisomorphismus $K[\alpha] \cong K[\beta]$, der auf K die Identität ist und α auf β abbildet.

Denken wir zurück an die Situation aus Beispiel 4.26: Versuchen wir, den Körperturm auf zwei verschiedene Weisen aufzubauen:

$$\begin{array}{ccc}
 \mathbb{Q}[\alpha_1, \alpha_2, \alpha_3] & & \mathbb{Q}[\alpha_2, \alpha_3, \alpha_1] \\
 \parallel & & \parallel \\
 \mathbb{Q}[\alpha_1, \alpha_2] & & \mathbb{Q}[\alpha_2, \alpha_3] \\
 | & & | \\
 \mathbb{Q}[\alpha_1] & & \mathbb{Q}[\alpha_2] \\
 | & & | \\
 \mathbb{Q} & \xrightarrow{\text{id}} & \mathbb{Q}
 \end{array}$$

Die Identitätsabbildung im „Erdgeschoss“ lässt sich nach dem Fortsetzungssatz eindeutig zu einem Körperisomorphismus $\tilde{\varphi}: \mathbb{Q}[\alpha_1] \rightarrow \mathbb{Q}[\alpha_2]$ mit $\tilde{\varphi}(\alpha_1) = \alpha_2$ fortsetzen, denn α_1 und α_2 haben dasselbe Minimalpolynom über \mathbb{Q} , nämlich $X^3 - 2$. Diesen Körperisomorphismus $\tilde{\varphi}$ können wir dann wiederum zu einem $\tilde{\tilde{\varphi}}: \mathbb{Q}[\alpha_1, \alpha_2] \rightarrow \mathbb{Q}[\alpha_2, \alpha_3]$ mit $\tilde{\tilde{\varphi}}(\alpha_2) = \alpha_3$ fortsetzen, denn das Minimalpolynom von α_2 über $\mathbb{Q}[\alpha_1]$ ist $f(X) = X^2 + \alpha_1 X + \alpha_1^2$ und das Minimalpolynom von α_3 über $\mathbb{Q}[\alpha_2]$ ist $X^2 + \alpha_2 X + \alpha_2^2 = f^{\tilde{\varphi}}(X)$. Da der letzte Schritt im Körperturm trivial ist, haben wir damit durch wiederholte Anwendung des Fortsetzungssatzes einen Körperautomorphismus des Zerfällungskörpers $Z = \mathbb{Q}[\alpha_1, \alpha_2, \alpha_3] = \mathbb{Q}[\alpha_2, \alpha_3, \alpha_1]$ erhalten. Dieser entspricht der Identität auf \mathbb{Q} und bildet die Nullstellen wie folgt ab: $\alpha_1 \mapsto \alpha_2, \alpha_2 \mapsto \alpha_3, \alpha_3 \mapsto \alpha_1$. (Die letzte Eigenschaft kann man sehen, wenn man sich überlegt, dass $\alpha_3 = \frac{\alpha_2^2}{\alpha_1}$ gilt und $\tilde{\tilde{\varphi}}$ ein Körperhomomorphismus ist.) Ein solcher Körperautomorphismus ist also nicht anderes als eine Permutation der Nullstellen, beschreibt also eine gewisse „innere Symmetrie“ der Lösungen einer Polynomgleichung.

Man beachte aber, dass die Bedingung im Bezug auf das Minimalpolynom (also die Bedingung an α und β in Satz 4.30) essentiell ist: Zum Beispiel lässt sich der Fortsetzungssatz nicht auf folgende Situation anwenden:

$$\begin{array}{ccc}
 \mathbb{Q}[\sqrt{2}, \sqrt{3}] & & \mathbb{Q}[\sqrt{3}, \sqrt{2}] \\
 | & & | \\
 \mathbb{Q}[\sqrt{2}] & & \mathbb{Q}[\sqrt{3}] \\
 | & & | \\
 \mathbb{Q} & \xrightarrow{\text{id}} & \mathbb{Q}
 \end{array}$$

Kapitel 4 Körpererweiterungen

(Dieses Diagramm zeigt zwei mögliche Wege, den Zerfällungskörper des Polynoms $(X^2 - 2)(X^2 - 3)$ aufzubauen.) Es gibt keinen Körperhomomorphismus $\tilde{\varphi}: \mathbb{Q}[\sqrt{2}] \rightarrow \mathbb{Q}[\sqrt{3}]$ mit $\tilde{\varphi}|_{\mathbb{Q}} = \text{id}$ und $\tilde{\varphi}(\sqrt{2}) = \sqrt{3}$. Gäbe es einen solchen, so müsste gelten

$$3 = (\sqrt{3})^2 = (\tilde{\varphi}(\sqrt{2}))^2 = \tilde{\varphi}((\sqrt{2})^2) = \tilde{\varphi}(2) = 2,$$

was offensichtlich ein Widerspruch in \mathbb{Q} ist. Wir sehen also, dass nicht immer jede beliebige Permutation der Nullstellen erlaubt ist.

Das Verständnis, welche solchen Körperautomorphismen es gibt (also welche „inneren algebraischen Symmetrien“ ein Zerfällungskörper hat), liefert uns viele Informationen über die zugehörige Körpererweiterung. Dies ist die Grundidee der Galoistheorie, die wir in Kapitel 5 studieren werden.

4.4 Der algebraische Abschluss

In vielen Beispielen haben wir bereits ausgenutzt, dass ein Polynom zwar vielleicht über einem bestimmten Grundkörper (meist \mathbb{Q}) keine Nullstelle besitzt, dass wir aber zumindest bereits einen größeren Körper kennen, in dem eine Nullstelle existiert. Dies konnten wir deshalb machen, weil wir die komplexen Zahlen \mathbb{C} kennen und diese eine besondere Eigenschaft haben: Sie sind *algebraisch abgeschlossen* – ein Begriff, den wir nun definieren.

Definition 4.31. (i) Ein Körper K heißt *algebraisch abgeschlossen*, falls jedes Polynom $f(X) \in K[X]$ mit $\deg(f) \geq 1$ eine Nullstelle in K besitzt.

(ii) Sei K ein Körper, dann heißt ein Körper Ω mit $K \subseteq \Omega$ ein *algebraischer Abschluss* von K , falls Ω algebraisch abgeschlossen ist und Ω/K eine algebraische Körpererweiterung ist.

Bemerkung 4.32. Es ist leicht zu sehen, dass ein algebraisch abgeschlossener Körper K automatisch *alle* Nullstellen jedes Polynoms $f(X) \in K[X]$ mit $\deg(f) \geq 1$ enthält – genauer gesagt: Jedes Polynom $f(X) \in K[X]$ zerfällt in Linearfaktoren: Ist $f(X)$ ein solches Polynom, dann gibt es nach Definition der algebraischen Abgeschlossenheit eine Nullstelle $\alpha \in K$ von $f(X)$, falls $\deg(f) \geq 1$ (andernfalls sind wir schon fertig). Nach Korollar 3.36 können wir also schreiben $f(X) = (X - \alpha) \cdot g(X)$ für ein $g(X) \in K[X]$ mit $\deg(g) = \deg(f) - 1$. Falls $\deg(g) \geq 1$ (also $g(X)$ noch kein konstantes Polynom ist), besitzt es – wieder wegen der algebraischen Abgeschlossenheit von K – eine Nullstelle in K , welche wir wiederum als Linearfaktor abspalten können. Dies setzen wir solange fort, bis wir $f(X)$ also Produkt von Linearfaktoren und einer Konstanten ausgedrückt haben.

Eine weitere leichte Beobachtung ist die folgende: Ist L/K eine algebraische Körpererweiterung und ist Ω ein algebraischer Abschluss von L , dann ist Ω auch ein algebraischer Abschluss von K . Dies ist klar, denn Ω ist nach Definition algebraisch abgeschlossen, die Erweiterung Ω/K ist algebraisch (denn L/K ist algebraisch nach

Voraussetzung und Ω/L ist algebraisch nach Definition) und Ω enthält eine Nullstelle von jedem Polynom in $K[X]$ (denn es enthält sogar eine Nullstelle von jedem Polynom in $L[X]$).

Beispiel 4.33. • Der Körper \mathbb{C} der komplexen Zahlen ist algebraisch abgeschlossen. Er ist ein algebraischer Abschluss von \mathbb{R} .

- \mathbb{C} ist kein algebraischer Abschluss von \mathbb{Q} , denn nicht jedes Element von \mathbb{C} ist algebraisch über \mathbb{Q} (z.B. sind die Zahlen π und e transzendent). Den algebraischen Abschluss von \mathbb{Q} bezeichnet man oft mit $\overline{\mathbb{Q}}$ und nennt ihn den *Körper der algebraischen Zahlen*.
- Der Körper $\mathbb{F}_2 := \mathbb{Z}/2\mathbb{Z}$ ist nicht algebraisch abgeschlossen. Beispielsweise hat das Polynom $X^2 + X + 1 \in \mathbb{F}_2[X]$ keine Nullstelle in \mathbb{F}_2 .
- Ebenso ist jeder andere Körper mit nur endlich vielen Elementen nicht algebraisch abgeschlossen: Sei $K = \{\alpha_1, \dots, \alpha_n\}$, dann hat das Polynom $f(X) := (X - \alpha_1) \cdot \dots \cdot (X - \alpha_n) + 1 \in K[X]$ offensichtlich keine Nullstelle in K , denn für jedes $\alpha_i \in K$ ist $f(\alpha_i) = 1 \neq 0$.

Tatsächlich hat jeder Körper einen algebraischen Abschluss. Das Ziel dieses Abschnitts ist es, den folgenden Satz zu beweisen.

Satz 4.34. *Ist K ein Körper, dann existiert ein algebraischer Abschluss Ω von K .*

Wir beweisen zuvor eine etwas schwächere Aussage.

Lemma 4.35. *Ist K ein Körper, so gibt es eine algebraische Körpererweiterung L/K , sodass jedes Polynom $f(X) \in K[X]$ mit $\deg(f) \geq 1$ eine Nullstelle in L hat.*

Beweis. Es sei $I := \{f(X) \in K[X] \mid \deg(f) \geq 1\}$ die Menge aller Polynome vom Grad ≥ 1 , also all derjenigen Polynome, die in dem zu konstruierenden L eine Nullstelle haben sollen.

In Satz 4.22 haben wir gesehen, wie man einen Körper so erweitert, dass er eine Nullstelle *eines* (irreduziblen) Polynoms enthält, nämlich indem man den Polynomring $K[X]$ in *einer* Variablen betrachtet und den Quotientenring bezüglich eines maximalen Ideals bildet.

Hier wollen wir dem Körper K nun Nullstellen aller (unendlich vielen) Polynome in I hinzufügen. Dazu wenden den folgenden „Trick“ an: Wir betrachten den Polynomring in (unendlich vielen) Variablen, wobei wir für jedes der Element $f \in I$ eine formale Variable X_f einführen. Dieser Ring wird mit

$$K[X_f \mid f \in I]$$

bezeichnet.

Beschreiben wir ihn etwas genauer. Dazu führen wir die folgende Notation ein:

$$\mathbb{N}_0^I := \{\gamma: I \rightarrow \mathbb{N}_0 \mid \gamma(f) = 0 \text{ für alle bis auf endlich viele } f \in I\}.$$

Kapitel 4 Körpererweiterungen

Ein Element $\gamma \in \mathbb{N}_0^I$ gibt uns also für endlich viele $f \in I$ eine natürliche Zahl $\gamma(f)$ vor. Wir kürzen ab:

$$\mathbf{X}^\gamma := \prod_{f \in I} X_f^{\gamma(f)}.$$

(Das ist also ein Produkt von endlich vielen X_f in den entsprechenden Potenzen, die durch γ vorgegeben werden.)

Die Menge $K[X_f \mid f \in I]$ ist dann definiert als die Menge von Elemente der Form

$$\sum_{\gamma \in \mathbb{N}_0^I} a_\gamma \mathbf{X}^\gamma,$$

mit Koeffizienten $a_\gamma \in K$, sodass $a_\gamma = 0$ für alle bis auf endlich viele $\gamma \in \mathbb{N}_0^I$. Die Ringstruktur ist durch die Verknüpfungen

$$\begin{aligned} \left(\sum_{\gamma \in \mathbb{N}_0^I} a_\gamma \mathbf{X}^\gamma \right) + \left(\sum_{\gamma \in \mathbb{N}_0^I} b_\gamma \mathbf{X}^\gamma \right) &:= \sum_{\gamma \in \mathbb{N}_0^I} (a_\gamma + b_\gamma) \mathbf{X}^\gamma, \\ \left(\sum_{\gamma \in \mathbb{N}_0^I} a_\gamma \mathbf{X}^\gamma \right) \cdot \left(\sum_{\gamma \in \mathbb{N}_0^I} b_\gamma \mathbf{X}^\gamma \right) &:= \sum_{\gamma \in \mathbb{N}_0^I} \left(\sum_{\substack{\alpha, \beta \in \mathbb{N}_0^I \\ \alpha + \beta = \gamma}} a_\alpha b_\beta \right) \mathbf{X}^\gamma. \end{aligned}$$

(Man überlegt sich leicht, dass diese wohldefiniert sind und die Ringaxiome erfüllen. Dies sind im Grunde die „natürlichen“ Verknüpfungen, ähnlich wie beim Polynomring in einer Variablen.)

In diesem Ring betrachten wir nun das Ideal

$$\mathfrak{a} := (f(X_f) \mid f \in I) \triangleleft K[X_f \mid f \in I],$$

welches von all den Polynomen $f(X_f)$ mit $f \in I$ erzeugt wird. Konkret bedeutet das: Ein Element von \mathfrak{a} ist eine endliche Summe

$$\sum_{k=1}^n g_k(X_f \mid f \in I) \cdot f_k(X_{f_k})$$

für bestimmte $f_1, \dots, f_k \in I$ und $g_1, \dots, g_k \in K[X_f \mid f \in I]$.

Behauptung: Das Ideal $\mathfrak{a} \triangleleft K[X_f \mid f \in I]$ ist ein echtes Ideal, d.h. es gilt $\mathfrak{a} \neq K[X_f \mid f \in I]$.

Wäre $\mathfrak{a} = K[X_f \mid f \in I]$, so wäre $1 \in \mathfrak{a}$, d.h. wir könnten das konstante Polynom $1 \in K[X_f \mid f \in I]$ schreiben als endliche Summe

$$1 = \sum_{k=1}^n g_k(X_f \mid f \in I) \cdot f_k(X_{f_k})$$

für passende $f_1, \dots, f_n \in I$ und $g_1, \dots, g_n \in K[X_f \mid f \in I]$. Sei nun Z ein Zerfällungskörper von $f_1(X) \cdot \dots \cdot f_n(X)$ über K (den es nach Satz 4.25 gibt) und sei $\alpha_k \in Z$ eine Nullstelle von $f_k(X)$ für jedes $k \in \{1, \dots, n\}$. Dann lesen wir den obigen Ausdruck

$$\sum_{k=1}^n g_k(X_f \mid f \in I) \cdot f_k(X_{f_k})$$

als Element in $Z[X_f \mid f \in I]$ und setzen für X_{f_k} jeweils α_k ein. Dann erhalten wir $1 = 0$, ein Widerspruch.

Da \mathfrak{a} also ein echtes Ideal in $K[X_f \mid f \in I]$ ist, gibt es nach Satz 3.54 ein maximales Ideal $\mathfrak{m} \triangleleft K[X_f \mid f \in I]$ mit $\mathfrak{a} \subseteq \mathfrak{m}$. Wir definieren jetzt den Quotienten

$$L := K[X_f \mid f \in I]/\mathfrak{m}.$$

Da \mathfrak{m} ein maximales Ideal ist, ist L ein Körper (siehe Satz 3.51). Außerdem überlegt man sich leicht, dass die Abbildung $K \rightarrow L, x \mapsto [x]$, die $x \in K$ auf die Äquivalenzklasse des konstanten Polynoms x schickt, ein Körperhomomorphismus ist und somit injektiv (nach Korollar 3.20). Damit ist also K in L enthalten und somit L eine Körpererweiterung von K . Um zu sehen, dass L die gesuchte Körpererweiterung ist, prüfen wir noch zwei Eigenschaften.

Behauptung: Jedes Polynom $f(X) \in K[X]$ mit $\deg(f) \geq 1$ hat eine Nullstelle in L .

Sei $f(X)$ ein solches Polynom (d.h. $f \in I$). Offensichtlich ist $\alpha_f := [X_f] \in L$ eine Nullstelle von $f(X)$, denn wegen $f(X_f) \in \mathfrak{m}$ gilt

$$f(\alpha_f) = f([X_f]) = [f(X_f)] = [0].$$

Behauptung: L/K ist eine algebraische Körpererweiterung.

Wir müssen zeigen, dass jedes Element $\alpha \in L$ algebraisch über K ist. Sei also $\alpha = [g(X_f \mid f \in I)]$ ein beliebiges Element von L , also eine Äquivalenzklasse modulo \mathfrak{a} eines Polynoms $g \in K[X_f \mid f \in I]$. Obwohl letzterer Polynomring unendlich viele Variablen hat, kommen in jedem konkreten Polynom nur endlich viele verschiedene Variablen X_f vor, so also auch in g . Seien X_{f_1}, \dots, X_{f_m} die Variablen, die in g tatsächlich vorkommen und $f_1, \dots, f_m \in I$ die zugehörigen Polynome. Es ist dann also $g = g(X_{f_1}, \dots, X_{f_m})$ ein Polynom in endlich vielen Variablen. Dann betrachte die Elemente

$$\beta_k := [X_{f_k}] \in L$$

für $k \in \{1, \dots, m\}$. Es gilt dann

$$\alpha = [g(X_{f_1}, \dots, X_{f_m})] = g([X_{f_1}], \dots, [X_{f_m}]) = g(\beta_1, \dots, \beta_m) \in K[\beta_1, \dots, \beta_m].$$

Kapitel 4 Körpererweiterungen

Da jedes Element β_k algebraisch über K ist (es ist eine Nullstelle des Polynoms $f_k(X)$), folgt

$$[K(\beta_1, \dots, \beta_m) : K] < \infty$$

(durch endlich viele Anwendungen von Satz 4.16) und daher ist insbesondere α algebraisch über K nach Korollar 4.19.

□

Mithilfe dieses Lemmas können wir nun die Existenz eines algebraischen Abschlusses beweisen. Man könnte zunächst denken, dass wir mit dem Lemma eigentlich schon fertig sind und einen algebraischen Abschluss von K konstruiert haben. Der Körper L aus dem Lemma ist aber selbst noch nicht unbedingt der gesuchte algebraische Abschluss von K , denn in L haben nur (nichtkonstante) Polynome aus $K[X]$ sicher eine Nullstelle, nicht aber zwangsläufig alle nichtkonstanten Polynome aus $L[X]$.

Beweis von Satz 4.34. Zu unserem Ausgangskörper K können wir nach Lemma 4.35 einen algebraischen Erweiterungskörper L_1 definieren, in dem jedes Polynom $f(X) \in K[X]$ mit $\deg(f) \geq 1$ eine Nullstelle hat. Dieser Körper hat nach demselben Lemma wieder einen algebraischen Erweiterungskörper L_2 , in dem jedes Polynom $f(X) \in L_1[X]$ mit $\deg(f) \geq 1$ eine Nullstelle besitzt. Führen wir dies so weiter, erhalten wir also eine Kette von algebraischen Körpererweiterungen

$$K \subseteq L_1 \subseteq L_2 \subseteq L_3 \subseteq \dots,$$

wobei jeweils in L_{k+1} jedes Polynom $f \in L_k[X]$ mit $\deg(f) \geq 1$ eine Nullstelle besitzt (für jedes $k \in \mathbb{N}$). Wir definieren dann

$$\Omega := \bigcup_{k=1}^{\infty} L_k.$$

Dies ist unser gesuchter algebraischer Abschluss von K , wie die folgenden Behauptungen zeigen.

Behauptung 1: Ω ist ein Körper.

Jedes Körperaxiom stellt Bedingungen an eine endliche Anzahl an Elementen aus Ω (z.B. sind die Assoziativgesetze Bedingungen an drei beliebige Elemente). Sind also endlich viele Elemente gegeben, für die eine Bedingung geprüft werden soll, so gibt es ein L_m in der Kette, in dem alle diese endlich vielen Elemente enthalten sind. In L_m gilt aber das entsprechende Axiom, da wir wissen, dass L_m ein Körper ist.

Behauptung 2: Ω/K ist algebraisch.

Da jedes $\alpha \in \Omega$ bereits in einem L_k in der Kette enthalten ist und L_k/K nach Lemma 4.35 und Satz 4.20 eine algebraische Erweiterung ist, ist α algebraisch über K und somit insgesamt Ω/K eine algebraische Körpererweiterung.

Behauptung 3: Ω ist algebraisch abgeschlossen.

Sei $f(X) \in \Omega[X]$ ein Polynom mit $\deg(f) \geq 1$. Schreiben wir $f(X) = \sum_{i=0}^n a_i X^i$, dann gibt es einen Körper L_m in der Kette, in dem die (endlich vielen) Koeffizienten a_0, \dots, a_n enthalten sind. Also ist $f(X) \in L_m[X]$ und somit hat $f(X)$ eine Nullstelle in $L_{m+1} \subseteq \Omega$. \square

Wir beweisen nun eine Variante des Fortsetzungssatzes (der in Satz 4.30 nur für einfache Erweiterungen formuliert war) für beliebige algebraische Körpererweiterungen. Dies ist möglich unter der Voraussetzung, dass es im Zielbereich des erweiterten Homomorphismus „genügend Nullstellen gibt“.

Satz 4.36 (Fortsetzungssatz in algebraisch abgeschlossene Körper). *Sei $\varphi: K \rightarrow L'$ ein Körperhomomorphismus, wobei L' algebraisch abgeschlossen ist. Sei L/K eine algebraische Körpererweiterung. Dann gibt es einen Körperhomomorphismus $\tilde{\varphi}: L \rightarrow L'$ mit $\tilde{\varphi}|_K = \varphi$.*

Grafisch veranschaulicht:

$$\begin{array}{ccc} L & & \\ | & \searrow \exists \tilde{\varphi} & \\ K & \xrightarrow{\varphi} & L' \end{array}$$

Beweis. Betrachte die Menge

$$\mathcal{M} := \{(M, \psi) \mid K \subseteq M \subseteq L, \psi: M \rightarrow L' \text{ Körperhomomorphismus mit } \psi|_K = \varphi\}$$

Diese Menge enthält also Paare bestehend aus einem Zwischenkörper M von L/K und einem Homomorphismus $\psi: M \rightarrow L'$, welcher φ erweitert.

Unser Ziel ist zu zeigen, dass \mathcal{M} ein maximales Element (M, ψ) mit $M = L$ hat, dass sich φ also tatsächlich auf ganz L (und nicht nur auf einen Zwischenkörper) fortsetzen lässt. Dazu wenden wir das Lemma von Zorn an. Wir betrachten die partielle Ordnung auf \mathcal{M} definiert durch

$$(M, \psi) \leq (M', \psi') :\Leftrightarrow M \subseteq M' \text{ und } \psi'|_M = \psi.$$

Jede totalgeordnete Teilmenge von (\mathcal{M}, \leq) hat eine obere Schranke in \mathcal{M} , denn man kann alle Zwischenkörper, die in der totalgeordneten Menge vorkommen, zu einem neuen Zwischenkörper vereinigen und außerdem alle Abbildung von diesen Zwischenkörpern nach L' zu einem neuen Körperhomomorphismus von dieser Vereinigung nach L' zusammensetzen. Daher gibt es nach dem Lemma von Zorn ein maximales Element $(M, \psi) \in \mathcal{M}$.

Falls nun $M \neq L$, so gibt es ein $\alpha \in L \setminus M$. Sei $f(X) \in M[X]$ das Minimalpolynom von α über M . Nach dem Fortsetzungssatz für einfache Erweiterungen (Satz 4.30) gibt es dann einen Körperhomomorphismus $\tilde{\psi}: M[\alpha] \rightarrow L'[\beta]$, wobei $\beta \in L'$ eine Nullstelle von $f^\psi(X) \in L'[X]$ ist (eine solche gibt es, da L' algebraisch abgeschlossen

Kapitel 4 Körpererweiterungen

ist). Wir haben also das Diagramm

$$\begin{array}{ccc}
 L & & \\
 | & & \\
 M[\alpha] & \xrightarrow{\tilde{\psi}} & L'[\beta] = L' \\
 | & & \parallel \\
 M & \xrightarrow{\psi} & L' \\
 | & & \parallel \\
 K & \xrightarrow{\varphi} & \Omega
 \end{array}$$

und somit wäre $(M[\alpha], \tilde{\psi}) \in \mathcal{M}$ mit $(M, \psi) \leq (M[\alpha], \tilde{\psi})$, was ein Widerspruch zur Maximalität von (M, ψ) ist.

Folglich muss gelten $M = L$ und damit ist $\varphi := \psi$ der gesuchte Körperhomomorphismus. \square

Korollar 4.37. *Der algebraische Abschluss eines Körpers K ist eindeutig bis auf Isomorphie, d.h. sind Ω und Ω' zwei algebraische Abschlüsse von K , so gibt es einen Körperisomorphismus $\psi: \Omega \rightarrow \Omega'$ mit $\psi|_K = \text{id}_K$.*

Beweis. Wir wenden Satz 4.36 auf die Körper $L = \Omega$ und $L' = \Omega'$ sowie $\varphi: K \rightarrow \Omega', x \mapsto x$ an. Wir erhalten dann einen Körperhomomorphismus $\tilde{\varphi}: \Omega \rightarrow \Omega'$ mit $\tilde{\varphi}|_K = \text{id}_K$. Es bleibt noch zu zeigen, dass dieser ein Isomorphismus ist. Nach Korollar 3.20 ist $\tilde{\varphi}$ injektiv und somit ist Ω isomorph zu $\tilde{\varphi}(\Omega)$, welcher daher wieder ein algebraisch abgeschlossener Körper und ein Teilkörper von Ω' ist. Da Ω'/K algebraisch ist, ist auch $\Omega'/\tilde{\varphi}(\Omega)$ algebraisch. Dies bedeutet aber, dass jedes $\alpha \in \Omega'$ Nullstelle eines Polynoms über $\tilde{\varphi}(\Omega)$ ist. Da dieser Körper aber algebraisch abgeschlossen ist, enthält er bereits alle Nullstellen solcher Polynome und daher folgt $\tilde{\varphi}(\Omega) = \Omega'$, also ist $\tilde{\varphi}$ auch surjektiv und damit der gesuchte Isomorphismus $\psi := \tilde{\varphi}$. \square

Ebenfalls unter Verwendung des obigen Fortsetzungssatzes können wir nun noch eine Frage beantworten, die wir uns schon im letzten Kapitel gestellt haben: Wie eindeutig ist ein Zerfällungskörper eines Polynoms eigentlich? Die Antwort ist wie erwartet: Auch wenn man den Zerfällungskörper auf unterschiedliche Arten und Weisen aufbauen kann, gelangt man auf allen Wegen zu zueinander isomorphen Körpern.

Korollar 4.38. *Sei K ein Körper und $f(X) \in K[X]$ ein Polynom mit $\deg(f) \geq 1$. Sind L_1 und L_2 Zerfällungskörper von f , so gibt es einen Körperisomorphismus $\phi: L_1 \rightarrow L_2$ mit $\phi|_K = \text{id}_K$.*

Beweis. Wir schreiben $f(X) = \sum_{i=0}^n a_i X^i$ mit Koeffizienten $a_0, \dots, a_n \in K$ und $a_n \neq 0$.

Da L_1 ein Zerfällungskörper von f ist können wir schreiben

$$f(X) = c \cdot (X - \alpha_1) \cdot \dots \cdot (X - \alpha_n) \in L_1[X]$$

für $c = a_n \in K$ und $\alpha_1, \dots, \alpha_n \in L_1$. Es gilt dann außerdem $L_1 = K[\alpha_1, \dots, \alpha_n]$.

Ebenso gilt, da L_2 ein Zerfällungskörper von f ist, dass

$$f(X) = c \cdot (X - \beta_1) \cdot \dots \cdot (X - \beta_n) \in L_2[X]$$

für $c = a_n \in K$ und $\beta_1, \dots, \beta_n \in L_2$ und $L_2 = K[\beta_1, \dots, \beta_n]$.

Nun sei Ω_2 ein algebraischer Abschluss von L_2 . Dann gilt $K \subseteq L_2 \subseteq \Omega_2$, also haben wir einen Körperhomomorphismus $\varphi: K \rightarrow \Omega_2, x \mapsto x$. Da L_1/K eine algebraische Körpererweiterung ist, gibt es nach Satz 4.36 eine Fortsetzung $\tilde{\varphi}: L_1 \rightarrow \Omega_2$.

Behauptung: Es gilt $\text{im}(\tilde{\varphi}) = L_2$.

Betrachten wir das Polynom $f(X) \in L_1[X]$. Da alle seine Koeffizienten a_0, \dots, a_n in K liegen, gilt $f^{\tilde{\varphi}}(X) = f(X)$, also

$$f^{\tilde{\varphi}}(X) = c \cdot (X - \beta_1) \cdot \dots \cdot (X - \beta_n) \in L_2[X].$$

Andererseits ist die Abbildung $f(X) \mapsto f^{\tilde{\varphi}}(X)$ ein Ringhomomorphismus (Lemma-Definition 4.27), man kann sie also auch einzeln auf jeden Linearfaktor von $f(X) = c \cdot (X - \alpha_1) \cdot \dots \cdot (X - \alpha_n)$ anwenden und erhält

$$f^{\tilde{\varphi}}(X) = c \cdot (X - \tilde{\varphi}(\alpha_1)) \cdot \dots \cdot (X - \tilde{\varphi}(\alpha_n)) \in L_2[X].$$

Da nun aber der Polynomring $L_2[X]$ faktoriell ist (Satz 3.39 und Satz 3.71), ist die Zerlegung in Linearfaktoren bis auf Reihenfolge eindeutig. Die $\tilde{\varphi}(\alpha_i)$ und die β_j aus den beiden obigen Zerlegungen von $f^{\tilde{\varphi}}(X)$ müssen sich also bijektiv entsprechen, genauer gesagt:

$$\exists \sigma \in S_n \forall i \in \{1, \dots, n\} : \tilde{\varphi}(\alpha_i) = \beta_{\sigma(i)}.$$

Sei nun $\gamma \in L_1 = K[\alpha_1, \dots, \alpha_n]$, also ist γ ein polynomieller Ausdruck in den α_i mit Koeffizienten in K , d.h.

$$\gamma = \sum_{i_1, \dots, i_n=0}^m b_{i_1, \dots, i_n} \alpha_1^{i_1} \cdot \dots \cdot \alpha_n^{i_n}$$

mit $a_{i_1, \dots, i_n} \in K$. Dann ist

$$\tilde{\varphi}(\gamma) = \sum_{i_1, \dots, i_n=0}^m b_{i_1, \dots, i_n} \beta_{\sigma(1)}^{i_1} \cdot \dots \cdot \beta_{\sigma(n)}^{i_n}$$

ein polynomieller Ausdruck in den β_j mit Koeffizienten in K , also $\tilde{\varphi}(\gamma) \in K[\beta_1, \dots, \beta_n] = L_2$. Also ist $\text{im}(\tilde{\varphi}) \subseteq L_2$. (Hierzu beachte man, dass $\tilde{\varphi}(b_{i_1, \dots, i_n}) = b_{i_1, \dots, i_n}$, da $b_{i_1, \dots, i_n} \in K$.)

Kapitel 4 Körpererweiterungen

Umgekehrt lässt sich aber jedes $\delta \in L_2 = K[\beta_1, \dots, \beta_n]$ schreiben also polynomieller Ausdruck

$$\delta = \sum_{i_1, \dots, i_n=0}^m d_{i_1, \dots, i_n} \beta_1^{i_1} \cdot \dots \cdot \beta_n^{i_n}$$

und man sieht leicht, dass δ im Bild von $\tilde{\varphi}$ liegt, denn

$$\delta = \tilde{\varphi} \left(\sum_{i_1, \dots, i_n=0}^m d_{i_1, \dots, i_n} \alpha_{\sigma^{-1}(1)}^{i_1} \cdot \dots \cdot \alpha_{\sigma^{-1}(n)}^{i_n} \right).$$

Also ist auch $L_2 \subseteq \text{im}(\tilde{\varphi})$.

Schränken wir also den Zielbereich von $\tilde{\varphi}: L_1 \rightarrow \Omega_2$ auf sein Bild $\text{im}(\tilde{\varphi}) = L_2$ ein, erhalten wir einen Körperisomorphismus (die Surjektivität ist dann klar, die Injektivität folgt wie gewohnt automatisch für Körperhomomorphismen, siehe Korollar 3.20). Da er eine Fortsetzung unseres ursprünglichen φ ist, gilt natürlich auch $\tilde{\varphi}|_K = \text{id}_K$. Somit ist $\phi := \tilde{\varphi}$ wie gewünscht ein Körperisomorphismus zwischen den beiden Zerfällungskörpern. \square

Galoistheorie

Eh bien, mon vieux Barbicane,
répondit Michel, on m'eût plutôt
coupé la tête, en commençant par
les pieds, que de me faire
résoudre ce problème-là !
– Parce que tu ne sais pas
l'algèbre, répliqua
tranquillement Barbicane.

Mein werthester Barbicane,
erwiderte Michel, eher hätte man
mir, von den Füßen angefangen,
den Kopf abgeschnitten, als daß
ich diese Aufgabe zu lösen
vermocht hätte!
– Weil Du nichts von Algebra
verstehst, entgegnete ruhig
Barbicane.

Jules Verne
Autour de la Lune

5.1 Die Galoisgruppe

Wie schon in der Einleitung angekündigt, besteht die revolutionäre Idee der Galoistheorie darin, Polynomgleichungen über die Symmetrien ihrer Nullstellen zu verstehen. In unserer bisher entwickelten Sprache bedeutet das, dass wir Körpererweiterungen (und insbesondere Zerfällungskörper von Polynomen) über ihre „inneren Symmetrien“, d.h. Körperautomorphismen, die den Grundkörper erhalten, verstehen möchten. (Am Ende des Abschnitts 4.3 haben wir Beispiele für solche Körperautomorphismen gesehen.) Der Vorteil ist, dass diese Körperautomorphismen eine Gruppe bilden und wir somit gruppentheoretische Methoden verwenden können, um sie zu studieren.

Kapitel 5 Galoistheorie

Definition 5.1. Sei K ein Körper und seien L/K und L'/K Körpererweiterungen. Ein Körperhomomorphismus $\varphi: L \rightarrow L'$ mit $\varphi|_K = \text{id}_K$ heißt **K -Homomorphismus**. Die Menge aller K -Homomorphismen von L nach L' bezeichnen wir mit $\text{Hom}_K(L, L')$.

Ist L/K eine Körpererweiterung, dann heißt ein Körperisomorphismus $\varphi: L \rightarrow L$, welcher $\varphi|_K = \text{id}_K$ erfüllt, **K -Automorphismus** von L . Wir bezeichnen die Menge aller K -Automorphismen von L mit $\text{Aut}_K(L)$.

Definition 5.2. Sei L/K eine Körpererweiterung. Dann heißt

$$\begin{aligned} \text{Gal}(L/K) &:= \text{Aut}_K(L) \\ &:= \{ \sigma: L \rightarrow L \mid \sigma \text{ ist ein Körperautomorphismus mit } \sigma|_K = \text{id}_K \} \end{aligned}$$

(zusammen mit der Verknüpfung von Abbildungen und der Identität $\text{id}_L: L \rightarrow L$ als neutrales Element) die **Galoisgruppe** von L/K .

Beispiel 5.3. Überlegen wir uns, wie diese Galoisgruppe in einem ganz konkreten Fall aussieht: Sei $L \subseteq \mathbb{C}$ der Zerfällungskörper des Polynoms $f(X) = X^4 - 5 \in \mathbb{Q}[X]$. Die Nullstellen dieses Polynoms kennen wir, sie sind

$$\alpha_1 = \sqrt[4]{5}, \quad \alpha_2 = -\sqrt[4]{5}, \quad \alpha_3 = i\sqrt[4]{5}, \quad \alpha_4 = -i\sqrt[4]{5},$$

also ist $L = \mathbb{Q}[\alpha_1, \alpha_2, \alpha_3, \alpha_4] \subseteq \mathbb{C}$. Da $\alpha_2 = -\alpha_1$ und $\alpha_4 = -\alpha_3$ gilt, sieht man sofort, dass $L = \mathbb{Q}[\alpha_1, \alpha_3]$. Man hat also einen Körperturm bestehend aus einfachen Erweiterungen

$$\begin{array}{c} L = \mathbb{Q}[\alpha_1, \alpha_3] \\ | \\ \mathbb{Q}[\alpha_1] \\ | \\ \mathbb{Q} \end{array}$$

Natürlich kann man ebenso schreiben $L = \mathbb{Q}[\alpha_2, \alpha_4]$, $L = \mathbb{Q}[\alpha_2, \alpha_3]$ etc.

Welche Körperautomorphismen $\sigma: L \rightarrow L$ mit $\sigma|_{\mathbb{Q}} = \text{id}$ gibt es nun? In anderen Worten: Können wir alle Möglichkeiten beschreiben, wie sich die Identität $\text{id}_{\mathbb{Q}}: \mathbb{Q} \rightarrow \mathbb{Q}$ zu einem Körperautomorphismus von L fortsetzen lässt? Die Antwort ist „Ja“: Dies können wir, indem wir sukzessive den Fortsetzungssatz (Satz 4.30) auf obigen Körperturm anwenden!

Starten wir also mit der Identität

$$\mathbb{Q} \xrightarrow{\text{id}} \mathbb{Q}$$

Wir wollen den Definitionsbereich auf $\mathbb{Q}[\alpha_1]$ erweitern. Nach Lemma 4.28 und Satz 4.30 können wir das genau dann tun (und dann sogar eindeutig), wenn wir α_1

auf eine Nullstelle des Polynoms $f^{\text{id}}(X) = f(X) = X^4 - 5$ abbilden. Es gibt also für jedes $k \in \{1, 2, 3, 4\}$ eine eindeutige Fortsetzung $\tilde{\varphi}$ wie im folgenden Diagramm

$$\begin{array}{ccc} \mathbb{Q}[\alpha_1] & \xrightarrow{\tilde{\varphi}} & \mathbb{Q}[\alpha_k] \\ | & & | \\ \mathbb{Q} & \xrightarrow{\text{id}} & \mathbb{Q} \end{array}$$

mit $\tilde{\varphi}(\alpha_1) = \alpha_k$.

Jetzt wollen wir den Definitionsbereich weiter vergrößern, und zwar auf ganz $L = \mathbb{Q}[\alpha_1, \alpha_3]$. Zuerst müssen wir uns überlegen, wie das Minimalpolynom von α_3 über $\mathbb{Q}[\alpha_1]$ aussieht: Über $\mathbb{Q}[\alpha_1]$ können wir sicher die Linearfaktoren $(X - \sqrt[4]{5})$ und $(X + \sqrt[4]{5})$ abspalten und erhalten

$$X^4 - 5 = (X - \sqrt[4]{5})(X + \sqrt[4]{5})(X^2 + \sqrt{5}).$$

Das Polynom $g(X) := X^2 + \sqrt{5} \in \mathbb{Q}[\alpha_1][X]$ ist irreduzibel nach Lemma 3.82, denn seine Nullstellen sind $\alpha_3, \alpha_4 \notin \mathbb{R}$, aber $\mathbb{Q}[\alpha_1] \subseteq \mathbb{R}$. Somit ist $g(X)$ das Minimalpolynom von α_3 über $\mathbb{Q}[\alpha_1]$.

Wollen wir die Körperhomomorphismen $\tilde{\varphi}$ also auf $\mathbb{Q}[\alpha_1, \alpha_2]$ erweitern, so ist dies genau dann möglich, wenn wir α_3 auf eine Nullstelle des Polynoms $g^{\tilde{\varphi}}(X)$ abbilden. Da $g(X) = X^2 + \sqrt{2} = X^2 + \alpha_1^2$ und $\tilde{\varphi}(\alpha_1) = \alpha_k$, erhalten wir $g^{\tilde{\varphi}}(X) = X^2 + \alpha_k^2$. Die Nullstellen dieses Polynoms sind $\pm i\alpha_k$. Worauf wir α_3 abbilden dürfen, hängt also davon ab, worauf wir α_1 im ersten Schritt abgebildet haben. Wir erhalten dann für jedes $\beta \in \{i\alpha_k, -i\alpha_k\}$ eine Fortsetzung $\tilde{\tilde{\varphi}}$

$$\begin{array}{ccc} L = \mathbb{Q}[\alpha_1, \alpha_3] & \xrightarrow{\tilde{\tilde{\varphi}}} & \mathbb{Q}[\alpha_k, \beta] = L \\ | & & | \\ \mathbb{Q}[\alpha_1] & \xrightarrow{\tilde{\varphi}} & \mathbb{Q}[\alpha_k] \\ | & & | \\ \mathbb{Q} & \xrightarrow{\text{id}} & \mathbb{Q} \end{array}$$

mit $\tilde{\tilde{\varphi}}(\alpha_1) = \alpha_k$ und $\tilde{\tilde{\varphi}}(\alpha_3) = \beta$. Es ist leicht zu sehen, dass der Zielkörper $\mathbb{Q}[\alpha_k, \beta]$ ebenfalls gleich L ist, also erhalten wir auf diese Weise ein Element der Galoisgruppe.

Insgesamt können wir also alle möglichen Fälle – also alle Elemente der Galoisgruppe $\text{Gal}(L/\mathbb{Q})$ – wie folgt auflisten:

- Im ersten Schritt wird $k = 1$ gewählt (d.h. $\alpha_1 \mapsto \alpha_1$), dann müssen wir $\beta \in \{i\alpha_1, -i\alpha_1\} = \{\alpha_3, \alpha_4\}$ wählen. Es gibt also die beiden \mathbb{Q} -Automorphismen von L , die gegeben sind durch

$$\begin{array}{ll} \sigma_1 = \text{id}: \alpha_1 \mapsto \alpha_1 & \sigma_2: \alpha_1 \mapsto \alpha_1 \\ & \alpha_3 \mapsto \alpha_4 \end{array}$$

Kapitel 5 Galoistheorie

- Im ersten Schritt wird $k = 2$ gewählt (d.h. $\alpha_1 \mapsto \alpha_2$), dann müssen wir $\beta \in \{i\alpha_2, -i\alpha_2\} = \{\alpha_4, \alpha_3\}$ wählen. Es gibt also die beiden \mathbb{Q} -Automorphismen von L , die gegeben sind durch

$$\begin{array}{ll} \sigma_3: \alpha_1 \mapsto \alpha_2 & \sigma_4: \alpha_1 \mapsto \alpha_2 \\ \alpha_3 \mapsto \alpha_3 & \alpha_3 \mapsto \alpha_4 \end{array}$$

- Im ersten Schritt wird $k = 3$ gewählt (d.h. $\alpha_1 \mapsto \alpha_3$), dann müssen wir $\beta \in \{i\alpha_3, -i\alpha_3\} = \{\alpha_2, \alpha_1\}$ wählen. Es gibt also die beiden \mathbb{Q} -Automorphismen von L , die gegeben sind durch

$$\begin{array}{ll} \sigma_5: \alpha_1 \mapsto \alpha_3 & \sigma_6: \alpha_1 \mapsto \alpha_3 \\ \alpha_3 \mapsto \alpha_1 & \alpha_3 \mapsto \alpha_2 \end{array}$$

- Im ersten Schritt wird $k = 4$ gewählt (d.h. $\alpha_1 \mapsto \alpha_4$), dann müssen wir $\beta \in \{i\alpha_4, -i\alpha_4\} = \{\alpha_1, \alpha_2\}$ wählen. Es gibt also die beiden \mathbb{Q} -Automorphismen von L , die gegeben sind durch

$$\begin{array}{ll} \sigma_7: \alpha_1 \mapsto \alpha_4 & \sigma_8: \alpha_1 \mapsto \alpha_4 \\ \alpha_3 \mapsto \alpha_1 & \alpha_3 \mapsto \alpha_2 \end{array}$$

Es gibt also genau 8 verschiedene \mathbb{Q} -Automorphismen von L und somit ist

$$\text{Gal}(L/\mathbb{Q}) = \{\sigma_1, \dots, \sigma_8\}.$$

Auch wenn oben immer nur angegeben wurde, worauf α_1 und α_3 abgebildet werden, kann man natürlich einfach herausfinden, worauf die anderen Nullstellen α_2 und α_4 jeweils abgebildet werden: Sehen wir uns zum Beispiel den Fall σ_3 an. Da σ_3 ein Körperhomomorphismus ist, gilt

$$\sigma_3(\alpha_2) = \sigma_3(-\alpha_1) = -\sigma_3(\alpha_1) = -\alpha_2 = \alpha_1.$$

Ebenso findet man heraus, dass $\sigma_3(\alpha_4) = \alpha_4$. Möchte man also alle Nullstellen „erwähnen“, könnte man die Abbildung auch ausführlicher beschreiben durch

$$\begin{array}{l} \sigma_3: \alpha_1 \mapsto \alpha_2 \\ \alpha_2 \mapsto \alpha_1 \\ \alpha_3 \mapsto \alpha_3 \\ \alpha_4 \mapsto \alpha_4 \end{array}$$

und ebenso für alle anderen Elemente der Galoisgruppe. Man sieht also (wie bereits in den Beispielen am Ende von Abschnitt 4.3), dass ein Element der Galoisgruppe eines Zerfällungskörpers von $f(X)$ einer Permutation der Nullstellen von $f(X)$ entspricht, dass aber nicht jede beliebige Permutation vorkommen kann.

Das Hauptresultat dieses Kapitels wird der *Hauptsatz der Galoistheorie* sein, der eine Korrespondenz zwischen solchen Galoisgruppen und gewissen Körpererweiterungen herstellt. Dieser Satz wird natürlich nicht für beliebige Körpererweiterungen gültig sein, sondern nur für solche, die man heute als *Galoiserweiterungen* bezeichnet. Um diese definieren zu können, sehen wir uns in den nächsten beiden Abschnitten noch zwei neue Begriffe im Zusammenhang mit Körpererweiterungen an: Normalität und Separabilität.

Zu diesen Begriffen eine kurze Motivation: Eine normale Erweiterung ist, wie wir sehen werden, nichts anderes als ein Zerfällungskörper. Wenn wir uns also im Hauptsatz auf normale Erweiterungen beschränken müssen, bedeutet das, dass dieser Satz nur für Zerfällungskörper gilt und nicht für Erweiterungen, die nur „manche“ (und nicht alle) Nullstellen eines Polynoms enthalten. Damit können wir aber gut leben, denn insbesondere für unsere Hauptanwendung (das Verständnis der Lösbarkeit von Polynomgleichungen) sind Zerfällungskörper genau die Objekte, die uns interessieren.

Eine separable Erweiterung ist eine, bei der jedes Minimalpolynom nur einfache (und niemals mehrfache) Nullstellen besitzt. Wie wir aber sehen werden, ist dies zum Beispiel für Erweiterungen von \mathbb{Q} immer der Fall, sodass diese Bedingung insbesondere in der Anwendung, die Évariste Galois im Sinn hatte (nämlich der Lösbarkeit von Polynomgleichungen über den rationalen Zahlen) keine Einschränkung bedeutet.

5.2 Normale Körpererweiterungen

Definition 5.4. Eine algebraische Körpererweiterung L/K heißt *normal*, falls gilt: Jedes irreduzible Polynom $f(X) \in K[X]$, welches eine Nullstelle $\alpha \in L$ besitzt, zerfällt in $L[X]$ bereits in Linearfaktoren, d.h. es gibt (nicht notwendigerweise verschiedene) $\alpha_1, \dots, \alpha_m \in L$ (wobei $m = \deg(f)$) und $c \in K$, sodass

$$f(X) = c \cdot \prod_{i=1}^m (X - \alpha_i).$$

Wichtige Beispiele von normalen Körpererweiterungen kennen wir bereits, nämlich Zerfällungskörper von Polynomen. Dass diese wirklich normal sind (und in Wahrheit die einzigen Beispiele normaler Körpererweiterungen sind), zeigt der folgende Satz.

Satz 5.5. Sei L/K eine endliche Körpererweiterung. Dann ist L/K genau dann normal, wenn L Zerfällungskörper eines Polynoms $f(X) \in K[X]$ ist.

Beweis. Sei $f(X) \in K[X]$ und sei L ein Zerfällungskörper von f , d.h. es ist $L = K[\beta_1, \dots, \beta_m]$, wobei $\beta_1, \dots, \beta_m \in L$ Elemente sind, sodass

$$f(X) = c \cdot \prod_{i=1}^m (X - \beta_i)$$

Kapitel 5 Galoistheorie

für ein $c \in K$. Sei weiter $g(X) \in K[X]$ ein irreduzibles Polynom, das eine Nullstelle $\alpha \in L$ besitzt. Wir zeigen, dass dann $g(X)$ in $L[X]$ bereits in Linearfaktoren zerfällt:

Sei Ω ein algebraischer Abschluss von L , dann können wir in $\Omega[X]$ schreiben

$$g(X) = a \cdot \prod_{i=1}^n (X - \alpha_i)$$

für gewisse $\alpha_1, \dots, \alpha_n \in \Omega$ (die Nullstellen von $g(X)$) und ein $a \in K$. Sei dabei $\alpha_1 = \alpha \in L$. Wir wollen zeigen, dass auch für jedes $i \in \{2, \dots, n\}$ gilt: $\alpha_i \in L$.

Sei also $i \in \{2, \dots, n\}$. Dann gibt es nach dem Fortsetzungssatz für einfache Erweiterungen (Satz 4.30 angewendet für $\varphi = \text{id}_K$) einen Körperhomomorphismus

$$\tilde{\varphi}: K[\alpha] \rightarrow K[\alpha_i]$$

mit $\tilde{\varphi}|_K = \text{id}_K$ und $\tilde{\varphi}(\alpha) = \alpha_i$. Da $K[\alpha_i] \subseteq L \subseteq \Omega$, können wir diesen auch als Körperhomomorphismus $K[\alpha] \rightarrow \Omega$ betrachten. Nach Satz 4.36 können wir letzteren dann weiter fortsetzen zu einem Körperhomomorphismus

$$\hat{\varphi}: L \rightarrow \Omega,$$

für den natürlich immer noch $\hat{\varphi}|_K = \text{id}_K$ und $\hat{\varphi}(\alpha) = \alpha_i$ gilt.

Wegen $\alpha \in L = K[\beta_1, \dots, \beta_m]$ können wir α über K als polynomiellen Ausdruck in den β_1, \dots, β_m schreiben, also

$$\alpha = \sum_{i_1, \dots, i_m=0}^N a_{i_1, \dots, i_m} \beta_1^{i_1} \cdot \dots \cdot \beta_m^{i_m}$$

für ein $n \in \mathbb{N}$ und Koeffizienten $a_{i_1, \dots, i_m} \in K$. Folglich ist

$$\alpha_i = \hat{\varphi}(\alpha) = \sum_{i_1, \dots, i_m=0}^N a_{i_1, \dots, i_m} \hat{\varphi}(\beta_1)^{i_1} \cdot \dots \cdot \hat{\varphi}(\beta_m)^{i_m}.$$

Nun sind aber wegen Lemma 4.28 die Elemente $\hat{\varphi}(\beta_1), \dots, \hat{\varphi}(\beta_m)$ wiederum Nullstellen von $f(X)$, d.h. jedes $\hat{\varphi}(\beta_i)$ ist gleich einem der Elemente β_1, \dots, β_m und somit ist α_i wieder ein polynomieller Ausdruck in β_1, \dots, β_m . In anderen Worten: $\alpha_i \in K[\beta_1, \dots, \beta_m] = L$.

Folglich enthält L alle Nullstellen von $g(X)$ und damit ist L/K normal.

Sei nun umgekehrt L/K eine normale, endliche Körpererweiterung. Dann gibt es Elemente $\beta_1, \dots, \beta_k \in L$ mit $L = K[\beta_1, \dots, \beta_k]$. (Wäre dies nicht der Fall, d.h. müsste man unendlich viele β_i zu K adjungieren, um L zu erhalten, so wäre L/K nicht endlich.) Für jedes $j \in \{1, \dots, k\}$ sei nun $f_j(X) \in K[X]$ das Minimalpolynom von β_j über K .

Behauptung: L ist ein Zerfällungskörper des Polynoms $f(X) := \prod_{j=1}^k f_j(X) \in K[X]$.

Wir prüfen die Bedingungen aus der Definition eines Zerfällungskörpers (Definition 4.24) nach:

- (1) Das Polynom $f(X)$ zerfällt über L in Linearfaktoren, denn jedes der irreduziblen Polynome $f_j(X)$ besitzt nach Definition mindestens eine Nullstelle in L und zerfällt daher in Linearfaktoren, weil L/K normal ist.
- (2) Seien $\gamma_1, \dots, \gamma_N \in L$ alle Nullstellen von $f(X)$ in L . Dann gilt

$$K[\gamma_1, \dots, \gamma_N] \subseteq L = K[\beta_1, \dots, \beta_k]$$

(da $K \subseteq L$ und $\gamma_j \in L$), aber auch

$$L = K[\beta_1, \dots, \beta_k] \subseteq K[\gamma_1, \dots, \gamma_N]$$

(da die β_i bereits unter den γ_j vorkommen). Also ist $L = K[\gamma_1, \dots, \gamma_N]$.

□

Bemerkung 5.6. Wir haben den Begriff des Zerfällungskörpers immer nur für ein Polynom betrachtet (Definition 4.24). Man kann diese Definition leicht verallgemeinern und den Zerfällungskörper einer (möglicherweise unendlichen) Menge von Polynomen definieren. Dann gibt es auch eine allgemeinere Version von Satz 5.5 ohne das Adjektiv „endlich“: Eine Körpererweiterung ist genau dann normal, wenn sie Zerfällungskörper einer Menge von Polynomen ist.

In diesem Sinne sind also Zerfällungskörper wirklich die *einzig* normalen Körpererweiterungen, auch wenn sie unendlich sind. Wir werden darauf hier nicht näher eingehen, weil wir uns in der Galoistheorie am Ende hauptsächlich für endliche algebraische Erweiterungen interessieren.

Eine wichtige Beobachtung ist die folgende Eigenschaft.

Lemma 5.7. *Sei L/K eine normale Körpererweiterung und sei M ein Zwischenkörper von L/K (d.h. $K \subseteq M \subseteq L$). Dann ist auch L/M eine normale Körpererweiterung.*

Beweis. Sei $f(X) \in M[X]$ ein irreduzibles Polynom und sei $\alpha \in L$ eine Nullstelle, d.h. $f(\alpha) = 0$. Wir können schreiben $f(X) = \sum_{i=0}^n a_i X^i$ mit $a_n \neq 0$. Normieren wir dieses Polynom noch, so erhalten wir das Minimalpolynom $g(X) := \frac{1}{a_n} f(X)$ von α über M .

Da L/K normal (also insbesondere algebraisch) ist, ist α auch algebraisch über K . Wir bezeichnen mit $p(X) \in K[X]$ das Minimalpolynom von α über K . Wir können $p(X)$ auch als Polynom in $M[X]$ auffassen. Dort ist dann also $g(X)$ das Minimalpolynom von α und $p(X)$ ein Polynom mit $p(\alpha) = 0$ und somit folgt mit Lemma-Definition 4.14, dass $g(X) \mid p(X)$ in $M[X]$, also auch $f(X) \mid p(X)$.

Da L/K aber normal ist, zerfällt $p(X)$ in $L[X]$ in Linearfaktoren und folglich zerfällt auch $f(X)$ über $L[X]$ in Linearfaktoren. Somit ist L/M normal. □

Als Nächstes beweisen wir noch eine interessante Eigenschaft normaler Erweiterungen, die wir uns unbewusst bereits einmal zunutze gemacht haben: Erinnern wir uns kurz zurück an Beispiel 5.3. Dort haben wir den Fortsetzungssatz angewendet, um die Galoisgruppe eines Zerfällungskörpers (also einer normalen Körpererweiterung) zu bestimmen. Dabei lieferte uns der Fortsetzungssatz zunächst Körperisomorphismen $L = \mathbb{Q}[\alpha_1, \alpha_3] \rightarrow \mathbb{Q}[\alpha_k, \beta]$. Auf den ersten Blick sieht das also gar nicht unbedingt wie ein Element der Galoisgruppe aus, weil wir befürchten müssen, dass im Definitions- und Zielbereich unterschiedliche Körper stehen (d.h. der Zielbereich eventuell Elemente enthält, die L nicht enthält). In Beispiel 5.3 haben wir aber festgestellt, dass auch der Zielbereich dieser Abbildungen gleich dem Körper L war, dass diese Abbildungen also wirklich Körperautomorphismen von L und somit Elemente der Galoisgruppe waren. Das folgende Lemma zeigt, dass dies kein Zufall war, sondern dass für normale Erweiterungen Körperhomomorphismen in a priori größere Körper in Wahrheit immer Elemente der Galoisgruppe sind.

Lemma 5.8. *Sei L/K eine normale Körpererweiterung und Ω ein algebraisch abgeschlossener Körper mit $L \subseteq \Omega$. Dann gilt*

$$\text{Hom}_K(L, \Omega) = \text{Aut}_K(L),$$

d.h. für jeden K -Homomorphismus $\psi: L \rightarrow \Omega$ gilt $\text{im}(\psi) = L$ und somit ist ψ auch ein Automorphismus von L .

Beweis. Sei $\psi: L \rightarrow \Omega$ ein K -Homomorphismus.

Behauptung: Es gilt $\text{im}(\psi) = L$.

Wir zeigen zunächst, dass $\text{im}(\psi) \subseteq L$: Sei $\alpha \in L$, dann ist α algebraisch über K , denn L/K ist insbesondere eine algebraische Erweiterung. Sei also $p(X) \in K[X]$ das Minimalpolynom von α über K . Nach Lemma 4.28 (für den Fall $\varphi = \text{id}_K$) ist $\psi(\alpha) \in \Omega$ ebenfalls eine Nullstelle von $p(X)$. Da L/K normal ist und mit $\alpha \in L$ bereits eine Nullstelle von $p(X)$ in L liegt, liegen alle Nullstellen von $p(X)$ (und insbesondere $\psi(\alpha)$) bereits in L .

Nun zeigen wir noch, dass $L \subseteq \text{im}(\psi)$: Sei $\beta \in L$. Dann ist β algebraisch über K und wir bezeichnen mit $q(X) \in K[X]$ sein Minimalpolynom. Sei $Z \subseteq L$ ein Zerfällungskörper von $q(X)$ (d.h. $Z := K[\beta, \beta_2, \beta_3, \dots, \beta_k]$, wobei $\beta, \beta_2, \dots, \beta_k$ mit $k = \deg(q)$ die Nullstellen von $q(X)$ in L sind; beachte, dass $q(X)$ über L in Linearfaktoren zerfällt, da L normal ist und wir bereits wissen, dass $\beta \in L$). Dann gilt $\text{im}(\psi|_Z) \subseteq Z$, mit derselben Begründung wie im ersten Teil des Beweises dieser Behauptung, denn Z ist Zerfällungskörper und daher ist Z/K normal. Es ist also $\psi|_Z: Z \rightarrow Z$ ein Körperhomomorphismus und daher injektiv. Andererseits ist diese Abbildung auch eine lineare Abbildung zwischen zwei endlichdimensionalen K -Vektorräumen, also folgt aus der Injektivität auch die Surjektivität. Somit ist auch $\beta \in \text{im}(\psi)$.

Nach obiger Behauptung ist ψ also tatsächlich ein surjektiver K -Homomorphismus $L \rightarrow L$ und als Körperhomomorphismus automatisch injektiv, also insgesamt ein K -Automorphismus von L , wie gewünscht. \square

5.3 Separable Körpererweiterungen

Der zweite Begriff, den wir uns ansehen müssen, hat mit der Vielfachheit von Nullstellen zu tun. In dem Verfahren, das wir zur Bestimmung der Galoisgruppe angewendet haben (Beispiel 5.3), haben wir die (verschiedenen) Nullstellen $\alpha_1, \alpha_2, \dots$ durchnummeriert, den Körperturm aufgebaut und den Fortsetzungssatz wiederholt verwendet. In diesem Verfahren spielt es keine Rolle, wie oft jede Nullstelle in unserem Polynom vorkommt. In anderen Worten: Es gibt also potentiell Informationen über unser Polynom (nämlich die Vielfachheiten der Nullstellen), die von der Galoisgruppe „nicht bemerkt werden“. Um das zu verhindern (wir möchten ja, dass die Galoisgruppe möglichst alles über unser Polynom „weiß“), beschränken wir uns auf Erweiterungen, bei denen die Minimalpolynome nur einfache Nullstellen haben.

Definition 5.9. Sei L/K eine algebraische Körpererweiterung und sei Ω ein algebraischer Abschluss von L . Dann definieren wir:

- Ein Polynom $f(X) \in K[X]$ mit $\deg(f) \geq 1$ heißt *separabel*, falls es in Ω keine mehrfachen Nullstellen hat, d.h. wenn in $\Omega[X]$ gilt

$$f(X) = c \cdot \prod_{i=1}^m (X - \alpha_i)$$

für ein $c \in K$ und paarweise verschiedene $\alpha_1, \dots, \alpha_m \in \Omega$.

- Ein Element $\alpha \in L$ heißt *separabel*, wenn sein Minimalpolynom $p(X) \in K[X]$ separabel ist.
- Die Körpererweiterung L/K heißt *separabel*, falls jedes Element $\alpha \in L$ separabel ist. Andernfalls nennen wir L/K *inseparabel*.

Bemerkung 5.10. Man könnte sich fragen, ob diese Begriffe wohldefiniert sind, denn wir beginnen mit den Worten „sei Ω ein algebraischer Abschluss von L “. Es könnte also sein, dass für einen bestimmten algebraischen Abschluss von L ein Polynom $f(X) \in K[X]$ separabel ist, für einen anderen aber nicht. Dies ist aber nicht der Fall, denn nach Korollar 4.37 sind je zwei algebraische Abschlüsse K -isomorph und daraus kann man folgern, dass paarweise verschiedene Nullstellen in einem algebraischen Abschluss auch paarweise verschiedenen Nullstellen in einem anderen algebraischen Abschluss entsprechen. Die Definition von Separabilität hängt also nicht davon ab, welchen algebraischen Abschluss man wählt – das ist auch gut so, aber natürlich eine wichtige Beobachtung.

Wie kann man nun nachprüfen, ob ein gegebenes Polynom mehrfache Nullstellen besitzt oder nicht? Ein hilfreiches Kriterium dazu benutzt den folgenden Begriff, welcher offensichtlich motiviert ist durch den Ableitungsbegriff aus der Analysis.

Definition 5.11. Sei K ein Körper. Wir nennen die Abbildung

$$D: K[X] \rightarrow K[X], \quad f(X) = \sum_{i=0}^n a_i X^i \mapsto Df(X) := f'(X) := \sum_{i=1}^n i a_i X^{i-1}$$

die *formale Ableitung*.

Bemerkung 5.12. Es ist leicht zu sehen, dass die formale Ableitung eine K -lineare Abbildung ist (also ein Vektorraumendomorphismus des K -Vektorraums $K[X]$). Sie ist aber kein Ringhomomorphismus, denn es gilt nicht $(f \cdot g)'(X) = f'(X) \cdot g'(X)$. Stattdessen gilt – wie wir es von einer Abbildung erwarten würden, die „Ableitung“ heißt – die Produktregel (auch *Leibniz-Regel* genannt)

$$(f \cdot g)'(X) = f'(X) \cdot g(X) + f(X) \cdot g'(X).$$

Diese kann man auch direkt mit der obigen Definition für alle $f(X), g(X) \in K[X]$ beweisen (Übungsaufgabe). Wir werden dies hier nicht ausführen, wir werden die Produktregel aber im Folgenden benutzen.

Außerdem bemerken wir noch: Hat man eine Körpererweiterung L/K und ein Polynom $f(X) \in K[X]$, dann kann man $f(X)$ auch als Polynom in $L[X]$ auffassen und es ist egal, ob die formale Ableitung in $K[X]$ oder in $L[X]$ berechnet wird. Auch dies sieht man leicht, wenn man sich die Formel für $f'(X)$ ansieht.

Mithilfe der formalen Ableitung hat man die folgende Beobachtung.

Lemma 5.13. Sei K ein Körper und Ω ein algebraischer Abschluss von K . Sei $f(X) \in K[X]$ und sei $\alpha \in \Omega$ eine Nullstelle von f . Dann ist α genau dann eine mehrfache Nullstelle von f (d.h. $(X - \alpha)^2 \mid f(X)$ in $\Omega[X]$), wenn α auch eine Nullstelle von f' ist.

Beweis. Sei $\alpha \in \Omega$ eine mehrfache Nullstelle von $f(X) \in K[X]$. Dann können wir in $\Omega[X]$ den Linearfaktor $X - \alpha$ mehrmals abspalten, also schreiben

$$f(X) = (X - \alpha)^m \cdot g(X)$$

für ein $m \geq 2$ und ein $g(X) \in \Omega[X]$. Nach der Produktregel gilt dann

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

(Hier haben wir verwendet, dass die formale Ableitung des Polynoms $(X - \alpha)^m$ gleich dem Polynom $m(X - \alpha)^{m-1}$ ist – auch diese Formel erwarten wir von einer „Ableitung“ und dies kann leicht mithilfe der Definition der formalen Ableitung nachgeprüft werden (Übungsaufgabe).)

Setzen wir in das Polynom $f'(X)$ nun α ein, so erhalten wir $f'(\alpha) = 0$, da $m - 1 \geq 1$, also der Linearfaktor $X - \alpha$ in jedem Summanden mindestens einmal vorkommt. Also ist α auch eine Nullstelle von f' .

Sei umgekehrt $f'(\alpha) = 0$. Angenommen, α wäre nur eine einfache Nullstelle von f , d.h. $f(X) = (X - \alpha) \cdot g(X)$, wobei $g(\alpha) \neq 0$. Dann haben wir ähnlich wie vorher

$$f'(X) = 1 \cdot g(X) + (X - \alpha) \cdot g'(X)$$

in $\Omega[X]$. Setzen wir nun α in diese Gleichung ein, erhalten wir $0 = g(\alpha)$ und dies ist ein Widerspruch. Folglich ist α eine mehrfache Nullstelle von f . \square

Daraus ergibt sich also folgende Idee: Wenn man testen möchte, ob ein Polynom separabel ist oder mehrfache Nullstellen hat, so kann man das Polynom mit seiner formalen Ableitung vergleichen und untersuchen, ob beide einen „gemeinsamen Anteil“ (z.B. gemeinsame Nullstellen) haben. Genauer ist dieses Kriterium im nächsten Korollar formuliert.

Korollar 5.14. Sei $f(X) \in K[X]$ mit $\deg(f) \geq 1$. Dann gilt:

$$f(X) \text{ ist separabel} \Leftrightarrow \text{ggT}(f(X), f'(X)) = 1 \text{ in } K[X].$$

Beweis. Wir beweisen beide Richtungen nacheinander. Es sei Ω ein algebraischer Abschluss von K .

\Rightarrow : Sei $f(X)$ separabel. Angenommen, es wäre $\text{ggT}(f(X), f'(X)) \neq 1$, d.h. die Polynome $f(X)$ und $f'(X)$ haben einen gemeinsamen Teiler $h(X) \in K[X]$, welcher keine Einheit ist. Dann wäre insbesondere $\deg(h) \geq 1$, also hat $h(X)$ eine Nullstelle in Ω . Diese wäre dann eine gemeinsame Nullstelle von f und f' und somit nach Lemma 5.13 eine mehrfache Nullstelle von f . Dies ist ein Widerspruch zur Separabilität von $f(X)$.

\Leftarrow : Sei $\text{ggT}(f(X), f'(X)) = 1$. Wäre f nicht separabel, dann hätte $f(X)$ eine mehrfache Nullstelle $\alpha \in \Omega$, die dann auch eine Nullstelle von $f'(X)$ wäre. Da Ω/K eine algebraische Körpererweiterung ist (Ω ist ein algebraischer Abschluss von K), ist α algebraisch über K . Wir bezeichnen mit $p(X) \in K[X]$ sein Minimalpolynom. Dann gilt wegen $f(\alpha) = 0$ und $f'(\alpha) = 0$, dass $p(X) \mid f(X)$ und $p(X) \mid f'(X)$ in $K[X]$. Folglich gilt auch

$$p(X) \mid \text{ggT}(f(X), f'(X)).$$

Da aber $\deg(p) \geq 1$, ist $p(X)$ keine Einheit und kann somit kein Teiler von $\text{ggT}(f(X), f'(X)) = 1$ sein. Widerspruch.

\square

Kapitel 5 Galoistheorie

Aus diesem Kriterium können wir direkt eine weitere Folgerung ableiten, die uns in sehr vielen Fällen bereits sagt, dass ein irreduzibles Polynom keine mehrfachen Nullstellen haben kann.

Wir definieren zunächst kurz den Begriff der Charakteristik eines Körpers. Dazu erinnern wir uns an die Schreibweise

$$n \cdot 1 := \underbrace{1 + \dots + 1}_{n\text{-mal}}$$

für eine natürliche Zahl $n \in \mathbb{N}$ (siehe auch Abschnitt 2.1).

Lemma-Definition 5.15. Sei K ein Körper. Dann nennen wir die Zahl

$$\text{char}(K) := \begin{cases} 0 & \text{falls } \forall n \in \mathbb{N} : n \cdot 1 \neq 0 \\ \min\{n \in \mathbb{N} \mid n \cdot 1 = 0\} & \text{sonst} \end{cases}$$

die *Charakteristik* von K . Ist $\text{char}(K) \neq 0$, so ist $\text{char}(K)$ immer eine Primzahl.

Beweis. Wäre $\text{char}(K) = n \in \mathbb{N}$ und n keine Primzahl, so könnten wir schreiben $n = a \cdot b$ für $a, b \in \mathbb{N} \setminus \{1\}$, also wäre in K

$$0 = k \cdot 1 = (a \cdot b) \cdot 1 = (a \cdot 1) \cdot (b \cdot 1)$$

und somit $a \cdot 1 = 0$ oder $b \cdot 1 = 0$, denn K ist als Körper nullteilerfrei. Dann wäre aber n nicht die kleinste natürliche Zahl mit $n \cdot 1 = 0$ gewesen, ein Widerspruch. \square

Bemerkung 5.16. Man kann die Charakteristik auch folgendermaßen verstehen:

Wir betrachten den eindeutig bestimmten Gruppenhomomorphismus

$$\varphi: \mathbb{Z} \rightarrow K.$$

(Davon gibt es genau einen, denn es muss gelten $\varphi(0) = 0$ und $\varphi(1) = 1$ und somit auch $\varphi(n) = \varphi(1 + \dots + 1) = \varphi(1) + \dots + \varphi(1) = n \cdot 1$ für $n \in \mathbb{N}$ und $\varphi(-n) = -\varphi(n) = -n \cdot 1$.)

Der Kern $\ker(\varphi)$ ist ein Ideal in \mathbb{Z} . Da \mathbb{Z} ein Hauptidealbereich ist, ist also $\ker(\varphi) = (n)$ für ein $n \in \mathbb{N}_0$ (eigentlich $n \in \mathbb{Z}$, aber wir können annehmen, dass $n \geq 0$ und damit ist dieses n eindeutig). Wir nennen dieses n dann die Charakteristik von K .

Man kann sich dann überlegen, dass $\ker(\varphi)$ sogar ein Primideal ist und damit ist $\text{char}(K) = 0$ oder $\text{char}(K) \in \mathbb{N}$ eine Primzahl.

Nun also zur angekündigten Folgerung über Separabilität.

Korollar 5.17. Sei K ein Körper $f(X) \in K[X]$ ein irreduzibles Polynom mit $\deg(f) \geq 1$. Falls $\text{char}(K) \nmid \deg(f)$, so ist $f(X)$ separabel.

Beweis. Wir schreiben $f(X) = \sum_{i=0}^n a_i X^i$ mit $n = \deg(f) \geq 1$ und $a_n \neq 0$.

Behauptung: Es gilt $n \neq 0$ in K .

Falls $\text{char}(K) = 0$, ist dies klar, denn dann ist $n = n \cdot 1 \in K$ niemals Null (für beliebige natürliche Zahlen $n \in \mathbb{N}$).

Falls $\text{char}(K) \neq 0$, haben wir nach Voraussetzung, dass $n = \deg(f)$ kein Vielfaches von $\text{char}(K)$ ist und somit ist $n = n \cdot 1$ nicht Null.

Die formale Ableitung von $f(X)$ ist

$$f'(X) = \sum_{i=1}^n i a_i X^{i-1}.$$

mit Leitkoeffizient $n a_n$. Wegen $n \neq 0$ und $a_n \neq 0$ ist also $n a_n \neq 0$ in K und somit $\deg(f') \geq 0$, also $f'(X) \neq 0$. Da $f(X)$ irreduzibel ist, kann es aber keine Teiler von kleinerem Grad haben, die keine Einheiten sind und daher muss gelten

$$\text{ggT}(f(X), f'(X)) = 1,$$

also ist $f(X)$ nach Korollar 5.14 separabel. \square

Die Voraussetzung $\text{char}(K) \nmid \deg(f)$ ist insbesondere immer dann erfüllt, wenn $\text{char}(K) = 0$. Über solchen Körpern ist also dann jedes nichtkonstante irreduzible Polynom (und somit jede algebraische Körpererweiterung) separabel. Körper mit dieser Eigenschaft bekommen einen eigenen Namen.

Definition 5.18. Ein Körper K heißt *vollkommen* (oder *perfekt*), falls jede algebraische Körpererweiterung L/K separabel ist.

Korollar 5.19 (aus Korollar 5.17). *Jeder Körper K mit $\text{char}(K) = 0$ ist vollkommen.*

Wie auch bei der Normalität wollen wir uns auch kurz beim Begriff der Separabilität Gedanken darüber machen, wie sich diese Eigenschaft im Bezug auf Zwischenkörper verhält.

Lemma 5.20. *Sei L/K eine Körpererweiterung und M mit $K \subseteq M \subseteq L$ ein Zwischenkörper. Ist L/K separabel, so sind auch L/M und M/K separabel.*

Beweis. Zunächst zur Separabilität von L/M :

Sei $\alpha \in L$ ein Element. Da L/K separabel und daher insbesondere algebraisch ist, ist α algebraisch über K und somit auch über M . Sei $f(X) \in K[X]$ sein Minimalpolynom über K und $g(X) \in M[X]$ sein Minimalpolynom über M . Dann können wir $f(X)$ ebenfalls als Polynom in $M[X]$ auffassen, welches α als Nullstelle hat und daher gilt nach Lemma 4.15 $g(X) \mid f(X)$ in $M[X]$. Da nach Voraussetzung L/K separabel ist, hat $f(X)$ in einem algebraischen Abschluss Ω nur einfache Nullstellen, was somit auch für $g(X)$ gelten muss. Daher ist L/M separabel.

Nun noch zur Separabilität von M/K :

Kapitel 5 Galoistheorie

Sei $\beta \in M$ und sei $p(X) \in K[X]$ sein Minimalpolynom über K , welches existiert, da M/K endlich und somit algebraisch ist. Dann ist β auch ein Element von L und somit zerfällt sein Minimalpolynom $p(X)$ in einem algebraischen Abschluss Ω in Linearfaktoren mit paarweise verschiedenen Nullstellen, da L/K separabel ist. Somit ist auch M/K separabel. \square

Wir versuchen nun zu „messen“, wie separabel (oder inseparabel) eine Körpererweiterung ist.

Definition 5.21. Sei L/K eine endliche Körpererweiterung und sei Ω ein algebraischer Abschluss von L . Dann nennen wir die Zahl

$$[L : K]_{\text{sep}} := \#\text{Hom}_K(L, \Omega)$$

den *Separabilitätsgrad* von L/K .

A priori wissen wir noch gar nicht, dass $\text{Hom}_K(L, \Omega)$ endlich viele Elemente hat, dass also $[L : K]_{\text{sep}}$ für endliche Erweiterungen wirklich eine natürliche Zahl ist. Dies wird sich mit Satz 5.24 klären: Dieser besagt, dass der Separabilitätsgrad nie größer als der Körpergrad sein kann, und damit wird obige Definition a posteriori gerechtfertigt.

Bemerkung 5.22. Versuchen wir uns kurz klarzumachen, was dieser neue Begriff bedeutet:

Zunächst könnten wir uns fragen, warum wir hier $\text{Hom}_K(L, \Omega)$ betrachten und nicht $\text{Aut}_K(L)$. Wir haben gesehen, dass die beiden Mengen gleich sind, wenn die Erweiterung L/K normal ist (Lemma 5.8). Andernfalls sagen uns aber die Automorphismen eventuell nichts Interessantes: In den „Zwischenetagen“ in Beispiel 5.3 – also bevor wir beim ganzen Zerfällungskörper ankommen, der normal ist – sind Definitions- und Zielbereich nicht gleich, man kann diese Informationen also nicht als Automorphismen fassen, sondern nur als Körperhomomorphismen von einem Körper in einen anderen (und o.B.d.A. weiter in den algebraischen Abschluss). Daher ist $\text{Hom}_K(L, \Omega)$ hier die richtige Wahl.

Nun denken wir der Einfachheit halber an eine einfache Erweiterung $K[\alpha]/K$ und versuchen uns den Unterschied zwischen dem Körpergrad $[K[\alpha] : K]$ und dem Separabilitätsgrad $[K[\alpha] : K]_{\text{sep}}$ klarzumachen:

Sei $p(X) \in K[X]$ das Minimalpolynom von α . Seien $\alpha_1, \dots, \alpha_m$ die paarweise verschiedenen Nullstellen von $p(X)$ im algebraischen Abschluss Ω . Diese treten möglicherweise mehrfach auf. Wir schreiben also in $\Omega[X]$

$$p(X) = \prod_{j=1}^m (X - \alpha_j)^{v_j}$$

für $v_1, \dots, v_m \in \mathbb{N}$.

Dann ist nach Korollar 4.17 der Körpergrad

$$[K[\alpha] : K] = \deg(p) = \sum_{j=1}^m v_j$$

(also der Grad von $p(X)$, oder anders gesagt: die Nullstellen von $p(X)$ mit Vielfachheit gezählt).

Andererseits ist der Separabilitätsgrad $[K[\alpha] : K]_{\text{sep}}$ die Anzahl der möglichen K -Homomorphismen $K[\alpha] \rightarrow \Omega$. Nach Lemma 4.28 muss dabei α auf eines der Elemente $\alpha_1, \dots, \alpha_m$ abgebildet werden und nach dem Fortsetzungssatz gibt es auch für jedes $j \in \{1, \dots, m\}$ genau einen solchen K -Homomorphismus mit $\alpha \mapsto \alpha_j$. Wir sehen also, dass

$$[K[\alpha] : K]_{\text{sep}} = \#\text{Hom}_K(K[\alpha], \Omega) = m$$

(also die Anzahl der Nullstellen von $p(X)$, ohne Vielfachheit gezählt).

Wir sehen also insbesondere, dass im Fall einer einfachen Erweiterung $K[\alpha]/K$ der Separabilitätsgrad immer kleiner oder gleich dem Körpergrad ist und dass Gleichheit genau dann eintritt, wenn das Minimalpolynom von α separabel ist.

Es liegt also die Vermutung nahe, dass auch im Allgemeinen Körpergrad und Separabilitätsgrad genau dann übereinstimmen, wenn es sich um eine separable Erweiterung handelt (wenn es also keine mehrfachen Nullstellen in Minimalpolynomen gibt). Dies ist in der Tat der Fall. Bevor wir diese Aussage beweisen können, zeigen wir noch eine Gradformel für den Separabilitätsgrad.

Satz 5.23. *Sei M ein Zwischenkörper einer endlichen Körpererweiterung L/K . Sind die Separabilitätsgrade $[L : M]_{\text{sep}}$ und $[M : K]_{\text{sep}}$ endlich, so gilt*

$$[L : K]_{\text{sep}} = [L : M]_{\text{sep}} \cdot [M : K]_{\text{sep}}.$$

Beweis. Es sei Ω ein algebraischer Abschluss von L (und somit von K und M). Wir führen (nur für diesen Beweis) die folgende Schreibweise ein: Sei $\tau \in \text{Hom}_K(M, \Omega)$, dann schreiben wir

$$\text{Hom}_\tau(L, \Omega) := \{\sigma \in \text{Hom}_K(L, \Omega) \mid \sigma|_M = \tau\}$$

für die Menge der K -Homomorphismen $\sigma : L \rightarrow \Omega$, deren Einschränkung auf M mit dem gegebenen τ übereinstimmt.

Offensichtlich liegt jedes $\sigma \in \text{Hom}_K(L, \Omega)$ in genau einem $\text{Hom}_\tau(L, \Omega)$ für ein bestimmtes $\tau \in \text{Hom}_K(M, \Omega)$ (nämlich $\tau := \sigma|_M$). Also haben wir eine disjunkte Zerlegung

$$\text{Hom}_K(L, \Omega) = \bigsqcup_{\tau \in \text{Hom}_K(M, \Omega)} \text{Hom}_\tau(L, \Omega).$$

Kapitel 5 Galoistheorie

Behauptung: Für jedes $\tau \in \text{Hom}_K(M, \Omega)$ ist $\#\text{Hom}_\tau(L, \Omega) = \#\text{Hom}_M(L, \Omega)$.

Sei $\tau \in \text{Hom}_K(M, \Omega)$ beliebig. Dann lässt sich τ nach Satz 4.36 zu einem Körperhomomorphismus $\tilde{\tau} \in \text{Hom}_K(\Omega, \Omega)$ mit $\tilde{\tau}|_M = \tau$ fortsetzen. Dieser ist als Körperhomomorphismus injektiv und mit folgendem Argument sogar surjektiv: Sei $\alpha \in \Omega$, sei $p(X) \in K[X]$ sein Minimalpolynom über K und sei Z der Zerfällungskörper in Ω von $p(X)$. Die Erweiterung Z/K ist also nach Satz 5.5 normal und somit gilt mit Lemma 5.8

$$\tilde{\tau}|_Z \in \text{Hom}_K(Z, \Omega) = \text{Aut}_K(Z),$$

somit gibt es ein $\beta \in Z \subseteq \Omega$ mit $\tilde{\tau}(\beta) = \alpha$.

Wir definieren nun die Abbildung

$$\text{Hom}_M(L, \Omega) \rightarrow \text{Hom}_\tau(L, \Omega), \quad \sigma \mapsto \tilde{\tau} \circ \sigma.$$

Diese ist wohldefiniert, denn wenn $\sigma \in \text{Hom}_M(L, \Omega)$, d.h. $\sigma(m) = m$ für alle $m \in M$, so folgt $(\tilde{\tau} \circ \sigma)(m) = \tilde{\tau}(\sigma(m)) = \tilde{\tau}(m) = \tau(m)$, d.h. $\tilde{\tau} \circ \sigma \in \text{Hom}_\tau(L, \Omega)$. Sie ist außerdem bijektiv, denn offensichtlich ist eine Umkehrabbildung gegeben durch

$$\text{Hom}_\tau(L, \Omega) \rightarrow \text{Hom}_M(L, \Omega), \quad \sigma \mapsto \tilde{\tau}^{-1} \circ \sigma.$$

(Wir haben oben gezeigt, dass $\tilde{\tau}$ bijektiv ist.)

Also gilt wie behauptet $\#\text{Hom}_\tau(L, \Omega) = \#\text{Hom}_M(L, \Omega)$.

Mit der obigen Zerlegung und der eben gezeigten Behauptung bekommen wir also

$$\begin{aligned} [L : K]_{\text{sep}} &= \#\text{Hom}_K(L, \Omega) \\ &= \sum_{\tau \in \text{Hom}_K(M, \Omega)} \#\text{Hom}_\tau(L, \Omega) = \sum_{\tau \in \text{Hom}_K(M, \Omega)} \#\text{Hom}_M(L, \Omega) \\ &= \#\text{Hom}_K(M, \Omega) \cdot \#\text{Hom}_M(L, \Omega) \\ &= [M : K]_{\text{sep}} \cdot [L : M]_{\text{sep}}. \end{aligned} \quad \square$$

Satz 5.24. Sei L/K eine endliche Körpererweiterung. Dann hat man

$$[L : K]_{\text{sep}} \leq [L : K]$$

und es gilt

$$[L : K]_{\text{sep}} = [L : K] \Leftrightarrow L/K \text{ ist separabel.}$$

Beweis. Da L/K endlich ist, gibt es Elemente $\alpha_1, \dots, \alpha_m \in L$, sodass wir schreiben können $L = K[\alpha_1, \dots, \alpha_m]$.

In Bemerkung 5.22 haben wir uns bereits überlegt, dass für einfache Erweiterungen der Separabilitätsgrad (der die paarweise verschiedenen Nullstellen des Minimalpolynoms ohne Vielfachheiten zählt) immer kleiner oder gleich dem Körpergrad (der dem Grad des Minimalpolynoms, also der Anzahl der Nullstellen

mit Vielfachheiten gezählt, entspricht) ist. Wir können also die Erweiterung L/K in mehrere einfache Erweiterungen zerlegen und erhalten mit den Gradformeln für den Separabilitätsgrad (Satz 5.23) und den Körpergrad (Satz 4.8)

$$\begin{aligned} [L : K]_{\text{sep}} &= [K[\alpha_1, \dots, \alpha_m] : K]_{\text{sep}} \\ &= [K[\alpha_1, \dots, \alpha_m] : K[\alpha_1, \dots, \alpha_{m-1}]]_{\text{sep}} \cdots [K[\alpha_1] : K]_{\text{sep}} \\ &\leq [K[\alpha_1, \dots, \alpha_m] : K[\alpha_1, \dots, \alpha_{m-1}]] \cdots [K[\alpha_1] : K] \quad (\star) \\ &= [K[\alpha_1, \dots, \alpha_m] : K] = [L : K]. \end{aligned}$$

Damit ist der erste Teil des Satzes (die Ungleichung) bewiesen. Wir zeigen noch die Äquivalenz.

\Leftarrow : Ist L/K separabel, so sind nach Lemma 5.20 auch alle Zwischenerweiterungen im oben verwendeten Körperturm

$$K \subseteq K[\alpha_1] \subseteq K[\alpha_1, \alpha_2] \subseteq \dots \subseteq K[\alpha_1, \dots, \alpha_m] = L$$

separabel. Folglich sind die Minimalpolynome der α_i in jeder der einfachen Zwischenerweiterungen jeweils separabel (haben also in einem algebraischen Abschluss Ω von L nur einfache Nullstellen). Nach unseren Überlegungen aus Bemerkung 5.22 gilt somit Gleichheit von Separabilitätsgrad und Körpergrad in jedem Zwischenschritt und somit Gleichheit in (\star) .

\Rightarrow : Sei $[L : K]_{\text{sep}} = [L : K]$. Wäre L/K inseparabel, so gäbe es ein $\alpha \in L$, sodass das Minimalpolynom von α über K nicht separabel ist. Dann wäre aber (wie wir uns in Bemerkung 5.22 überlegt haben)

$$[K[\alpha] : K]_{\text{sep}} < [K[\alpha] : K],$$

also mit den Gradformeln und der Ungleichung aus dem ersten Teil des Satzes

$$[L : K]_{\text{sep}} = \underbrace{[L : K[\alpha]]_{\text{sep}}}_{\leq [L : K[\alpha]]} \cdot \underbrace{[K[\alpha] : K]_{\text{sep}}}_{< [K[\alpha] : K]} < [L : K[\alpha]] \cdot [K[\alpha] : K] = [L : K],$$

ein Widerspruch zur Voraussetzung $[L : K]_{\text{sep}} = [L : K]$. Folglich ist L/K separabel.

□

5.4 Der Satz vom primitiven Element

Wir beantworten jetzt noch eine Frage, die uns vielleicht auf dem Weg hierhin schon einmal in den Sinn kam: Gegeben eine Körpererweiterung L/K , wann kann man $L = K[\alpha]$ schreiben für ein einzelnes $\alpha \in L$? In anderen Worten: Wann ist L/K eine

einfache Erweiterung? Ob es ein solches α gibt, sieht man einer Erweiterung im Allgemeinen nicht einfach an: Beispielsweise könnte man denken, dass die Körpererweiterung $\mathbb{Q}[\sqrt{2}, \sqrt{3}]/\mathbb{Q}$ nicht einfach ist, da sie (in dieser Darstellung) durch Adjunktion zweier Elemente zum Grundkörper \mathbb{Q} entsteht. Wir haben aber in der Einführung (Kapitel 1) gezeigt, dass gilt:

$$\mathbb{Q}[\sqrt{2}, \sqrt{3}] = \mathbb{Q}[\sqrt{2} + \sqrt{3}].$$

(Mittlerweile verstehen wir die Argumente dort auch besser, es lohnt sich also, das erste Kapitel und insbesondere Seite 7 noch einmal zu lesen.)

Die Erweiterung ist also in Wirklichkeit eine einfache Erweiterung und entsteht durch Adjunktion eines einzelnen Elementes. Ein solches Element bekommt einen speziellen Namen.

Definition 5.25. Sei L/K eine Körpererweiterung. Ein Element $\gamma \in L$ heißt *primitives Element* für die Körpererweiterung L/K , falls $L = K[\gamma]$.

Wie kann man nun aber allgemein herausfinden, ob eine gegebene Erweiterung sich auch durch Adjunktion eines einzelnen Elementes aus dem Grundkörper erzeugen lässt, ob also so ein primitives Element überhaupt existiert? Die Antwort darauf gibt der folgende Satz.

Satz 5.26 (Satz vom primitiven Element (für unendliche Körper)). *Sei K ein Körper mit unendlich vielen Elementen. Ist L/K eine endliche, separable Körpererweiterung, so gibt es ein primitives Element für L/K . In anderen Worten: Dann existiert ein $\gamma \in L$, sodass $L = K[\gamma]$.*

Beweis. Da L/K endlich ist, gibt es a priori $\alpha_1, \dots, \alpha_m \in L$, sodass $L = K[\alpha_1, \dots, \alpha_m]$.

Wir zeigen zunächst, dass der Satz für $m = 2$ gilt: Sei also $L = K[\alpha_1, \alpha_2]$. Sei Ω ein algebraischer Abschluss von L . Nach Voraussetzung ist L/K endlich separabel, also hat die Menge $\text{Hom}_K(L, \Omega)$ nur endlich viele Elemente (nämlich nach Satz 5.24 genau so viele wie der Körpergrad $n = [L : K]$). Wir schreiben

$$\text{Hom}_K(L, \Omega) = \{\sigma_1, \dots, \sigma_n\},$$

wobei $\sigma_1, \dots, \sigma_n$ die paarweise verschiedenen Elemente von $\text{Hom}_K(L, \Omega)$ sind. Für jedes $i \in \{1, \dots, n\}$ sind dann $\sigma_i(\alpha_1)$ und $\sigma_i(\alpha_2)$ Elemente von Ω und wir können das Polynom

$$f(X) := \prod_{i=1}^n \prod_{\substack{j=1 \\ j \neq i}}^n \left((\sigma_i(\alpha_1) - \sigma_j(\alpha_1))X + \sigma_i(\alpha_2) - \sigma_j(\alpha_2) \right) \in \Omega[X]$$

betrachten.

Behauptung: Es gibt ein $x \in K$ mit $f(x) \neq 0$.

Zunächst überlegen wir uns, dass $f(X) \in \Omega[X]$ nicht das Nullpolynom ist: Wäre nämlich $f(X) = 0$, so müsste bereits einer der Linearfaktoren

$$(\sigma_i(\alpha_1) - \sigma_j(\alpha_1))X + \sigma_i(\alpha_2) - \sigma_j(\alpha_2)$$

das Nullpolynom sein (denn $\Omega[X]$ ist ein Integritätsbereich). Das würde aber bedeuten, dass es $i, j \in \{1, \dots, n\}$ gibt mit $i \neq j$, sodass $\sigma_i(\alpha_1) = \sigma_j(\alpha_1)$ und $\sigma_i(\alpha_2) = \sigma_j(\alpha_2)$. Dann wären aber die Abbildungen σ_i und σ_j gleich, denn $L = K[\alpha_1, \alpha_2]$ und daher ist jedes Element $\sigma \in \text{Hom}_K(L, \Omega)$ eindeutig durch die Werte $\sigma(\alpha_1)$ und $\sigma(\alpha_2)$ (sowie die Bedingung $\sigma(x) = x$ für alle $x \in K$) bestimmt. Nach Voraussetzung ist aber $\sigma_i \neq \sigma_j$, also erhalten wir einen Widerspruch und daher kann $f(X)$ nicht das Nullpolynom sein.

Da nun $f(X)$ nicht das Nullpolynom ist, hat es in Ω nur endlich viele Nullstellen. Somit kann es auch höchstens endlich viele Nullstellen in $K \subseteq \Omega$ haben (eventuell auch gar keine). Da aber K nach Voraussetzung unendlich viele Elemente besitzt, gibt es sicher ein $x \in K$ mit $f(x) \neq 0$.

Sei nun $x \in K$ mit $f(x) \neq 0$. Beachten wir, dass $\sigma_i(x) = x$ gilt und die σ_i Körperhomomorphismen sind, so können wir schreiben

$$\begin{aligned} f(x) &= \prod_{i=1}^n \prod_{\substack{j=1 \\ j \neq i}}^n \left((\sigma_i(\alpha_1) - \sigma_j(\alpha_1))x + \sigma_i(\alpha_2) - \sigma_j(\alpha_2) \right) \\ &= \prod_{i=1}^n \prod_{\substack{j=1 \\ j \neq i}}^n \left((\sigma_i(\alpha_1)x + \sigma_i(\alpha_2)) - (\sigma_j(\alpha_1)x + \sigma_j(\alpha_2)) \right) \\ &= \prod_{i=1}^n \prod_{\substack{j=1 \\ j \neq i}}^n \left((\sigma_i(\alpha_1)\sigma_i(x) + \sigma_i(\alpha_2)) - (\sigma_j(\alpha_1)\sigma_j(x) + \sigma_j(\alpha_2)) \right) \\ &= \prod_{i=1}^n \prod_{\substack{j=1 \\ j \neq i}}^n (\sigma_i(\alpha_1x + \alpha_2) - \sigma_j(\alpha_1x + \alpha_2)). \end{aligned}$$

Wenn dieser Ausdruck nun also nicht Null ist, muss auch jeder der Faktoren

$$\sigma_i(\alpha_1x + \alpha_2) - \sigma_j(\alpha_1x + \alpha_2)$$

für $i \neq j$ ungleich Null sein. Es sind also die Elemente

$$\sigma_1(\alpha_1x + \alpha_2), \dots, \sigma_n(\alpha_1x + \alpha_2) \in \Omega$$

paarweise verschieden.

Behauptung: Das Element $\alpha_1x + \alpha_2 \in L = K[\alpha_1, \alpha_2]$ ist ein primitives Element für L/K .

Wir müssen zeigen, dass $K[\alpha_1x + \alpha_2] = K[\alpha_1, \alpha_2]$. Wegen $\alpha_1x + \alpha_2 \in K[\alpha_1, \alpha_2]$ haben wir sicher

$$K \subseteq K[\alpha_1x + \alpha_2] \subseteq K[\alpha_1, \alpha_2] = L.$$

Da die Elemente $\sigma_i(\alpha_1x + \alpha_2) \in \Omega$ für $i \in \{1, \dots, n\}$ paarweise verschieden sind, sind die Abbildungen

$$\sigma_i|_{K[\alpha_1x + \alpha_2]}: K[\alpha_1x + \alpha_2] \rightarrow \Omega$$

ebenfalls paarweise verschieden. Anders gesagt: Es gibt mindestens n verschiedene Elemente in $\text{Hom}_K(K[\alpha_1x + \alpha_2], \Omega)$, d.h. $[K[\alpha_1x + \alpha_2] : K]_{\text{sep}} \geq n$. Nun beachten wir noch, dass $K[\alpha_1x + \alpha_2]/K$ ebenfalls separabel ist, da L/K separabel ist (Lemma 5.20), also gilt mit Satz 5.24

$$[K[\alpha_1x + \alpha_2] : K] = [K[\alpha_1x + \alpha_2] : K]_{\text{sep}} \geq n = [L : K].$$

Also ist $K[\alpha_1x + \alpha_2]$ ein Zwischenkörper von L/K , der mindestens denselben Körpergrad wie L über K hat und damit folgt $K[\alpha_1x + \alpha_2] = L$.

Damit ist der Satz für den Fall $m = 2$ bewiesen.

Für den allgemeinen Fall $m \geq 2$ gehen wir induktiv vor. (Für $m = 0$ und $m = 1$ ist der Satz offensichtlich trivial, sodass wir darauf hier nicht eingehen müssen.)

Induktionsanfang: $m = 2$ (soeben bewiesen).

Induktionsvoraussetzung: Es sei bekannt, dass für beliebiges, aber festes $m \geq 2$ jede endliche Körpererweiterung L/K mit $L = K[\alpha_1, \dots, \alpha_m]$ ein primitives Element besitzt, also ein $\gamma \in L$ mit $L = K[\gamma]$.

Induktionsschluss: Sei $L = K[\alpha_1, \dots, \alpha_{m+1}]$. Dann ist

$$L = (K[\alpha_1, \dots, \alpha_m])[\alpha_{m+1}].$$

Nach Induktionsvoraussetzung gibt es ein $\gamma \in K[\alpha_1, \dots, \alpha_m] \subseteq L$ mit

$$K[\alpha_1, \dots, \alpha_m] = K[\gamma].$$

Dann haben wir also

$$L = (K[\gamma])[\alpha_{m+1}] = K[\gamma, \alpha_{m+1}].$$

Nach dem Induktionsanfang (denn nun sind wir wieder im Fall $m = 2$) gibt es dann wiederum ein $\tilde{\gamma} \in L$ mit $L = K[\tilde{\gamma}]$, also ein primitives Element für L/K .

□

Bemerkung 5.27. • Wir haben in Satz 5.26 vorausgesetzt, dass der Grundkörper K unendlich viele Elemente hat. Auch ohne diese Voraussetzung (also über endlichen Körpern) gilt der Satz, man muss ihn dann aber anders beweisen. Kennt man ein paar grundlegende Aussagen über endliche Körper, so ist der Beweis in diesem Fall aber sehr kurz – wir gehen darauf in einem späteren Abschnitt ein, wo wir uns etwas ausführlicher mit endlichen Körpern beschäftigen werden.

- Die Aussage des Satzes vom primitiven Element klingt zunächst sehr nützlich: Jeder endliche separable Erweiterungskörper $L = K[\alpha_1, \dots, \alpha_m]$ von K ist von der Form $L = K[\gamma]$ für ein einzelnes Element $\gamma \in L$. Da für einfache Erweiterungen zum Teil schönere oder direktere Aussagen gelten (siehe z.B. Satz 4.16 und Satz 4.30), könnte uns das auf den ersten Blick das Leben oft einfacher machen. In der Praxis ist das aber selten der Fall: Zwar können wir schreiben $L = K[\gamma]$, aber das hilft uns nur, wenn wir das Element γ und sein Minimalpolynom über K wirklich gut verstehen:
 - Der Satz vom primitiven Element sagt uns a priori nur, dass ein primitives Element γ existiert, er sagt uns aber nicht, wie dieses γ aussieht. Aus dem Beweis können wir aber ablesen, wie wir ein solches γ theoretisch finden können: Falls wir eine Darstellung $L = K[\alpha_1, \dots, \alpha_m]$ gegeben haben, dann kann man ein passendes γ als Linearkombination der $\alpha_1, \dots, \alpha_m$ mit Koeffizienten in K finden, und es gibt nur endlich viele solche Linearkombinationen, die nicht funktionieren. Man könnte also eine beliebige Linearkombination (zum Beispiel $\gamma := \alpha_1 + \dots + \alpha_m$) ansetzen und testen, ob diese bereits ein primitives Element ist. Dazu muss man das Minimalpolynom $p(X) \in K[X]$ von γ über K bestimmen und sehen, ob $\deg(p) = [L : K]$ gilt. Falls das nicht der Fall ist, nimmt man eine andere Linearkombination und macht so weiter, bis man eine passende gefunden hat. Das ist aber im Allgemeinen eine schwierige Aufgabe!
 - Selbst wenn man ein passendes γ gefunden hat, wird dieses meist wesentlich schwieriger zu handhaben sein als die einzelnen α_i , denn das Minimalpolynom von γ hat dann einen höheren Grad als die Minimalpolynome der α_i . Es kann dann also kompliziert sein, es zu finden, seine Irreduzibilität zu beweisen oder etwas über seine Nullstellen auszusagen.

Es ist daher für explizite Berechnungen oft einfacher, mit den Elementen α_i zu arbeiten und den Fortsetzungssatz sukzessive im Körperturm $K \subseteq K[\alpha_1] \subseteq K[\alpha_1, \alpha_2] \subseteq \dots \subseteq K[\alpha_1, \dots, \alpha_m]$ anzuwenden.

- Aus theoretischer Sicht kann es hingegen natürlich durchaus nützlich sein, zu wissen, dass sich L in der Form $K[\gamma]$ schreiben lässt. Außerdem vergegenwärtigt uns der Satz vom primitiven Element noch einmal die Bedeutung des Begriffs der Separabilität, den wir im letzten Abschnitt kennengelernt haben.

5.5 Der Hauptsatz der Galoistheorie

Wir haben nun alle Zutaten, um das lange versprochene Hauptresultat zu formulieren und zu beweisen – den Hauptsatz der Galoistheorie. Dazu zunächst noch zwei Definitionen.

Definition 5.28. Eine algebraische Körpererweiterung L/K heißt *galoissch* (oder *Galoiserweiterung*), wenn sie normal und separabel ist.

Dieser Begriff hat eine einfache, aber wichtige Konsequenz.

Lemma 5.29. Sei L/K eine endliche Galoiserweiterung. Dann ist $\text{Gal}(L/K)$ eine endliche Gruppe. Genauer gilt

$$\#\text{Gal}(L/K) = [L : K].$$

Beweis. Da L/K sowohl endlich als auch normal und separabel ist, haben wir

$$\#\text{Gal}(L/K) = \#\text{Aut}_K(L) = \#\text{Hom}_K(L, \Omega) = [L : K]_{\text{sep}} = [L : K],$$

wobei wir im ersten Schritt die Definition der Galoisgruppe (Definition 5.2), im zweiten Schritt Lemma 5.8, im dritten Schritt die Definition des Separabilitätsgrades (Definition 5.21) und im letzten Schritt Satz 5.24 verwendet haben. \square

Lemma-Definition 5.30. Sei L ein Körper und $H \subseteq \text{Aut}(L)$ eine Untergruppe der Gruppe der Körperautomorphismen von L . Dann ist

$$L^H := \{\ell \in L \mid \forall \varphi \in H: \varphi(\ell) = \ell\}$$

ein Teilkörper von L . Wir nennen ihn den *Fixkörper* von L unter H .

Ist L/K eine Körpererweiterung und $H \subseteq \text{Gal}(L/K) = \text{Aut}_K(L)$, so ist L^H ein Zwischenkörper von L/K .

Beweis. L^H ist offensichtlich ein Körper, denn jedes $\varphi \in H$ ist ein Körperautomorphismus von L und somit gilt:

(1) $0 \in L^H$ und $1 \in L^H$, denn für jedes $\varphi \in H$ gilt $\varphi(0) = 0$ und $\varphi(1) = 1$.

(2) Sind $\ell_1, \ell_2 \in L^H$, d.h. $\varphi(\ell_1) = \ell_1$ und $\varphi(\ell_2) = \ell_2$ für alle $\varphi \in H$, so gilt auch

$$\varphi(\ell_1 + \ell_2) = \varphi(\ell_1) + \varphi(\ell_2) = \ell_1 + \ell_2$$

und analog $\varphi(\ell_1 \cdot \ell_2) = \ell_1 \cdot \ell_2$ für alle $\varphi \in H$, also $\ell_1 + \ell_2, \ell_1 \cdot \ell_2 \in L^H$.

(3) Ist $\ell \in L^H$, d.h. $\varphi(\ell) = \ell$ für alle $\varphi \in H$, und ist $\ell \neq 0$, dann gilt auch $\varphi(-\ell) = -\ell$ und $\varphi(\ell^{-1}) = \ell^{-1}$, also $-\ell, \ell^{-1} \in L^H$.

Da offensichtlich $L^H \subseteq L$ gilt, ist L^H ein Teilkörper von L .

Sei nun $H \subseteq \text{Gal}(L/K)$. Dann gilt für alle $\varphi \in H$ und alle $x \in K$, dass $\varphi(x) = x$. Folglich ist $K \subseteq L^H$ und daher ist L^H ein Zwischenkörper von L/K . \square

Bemerkung 5.31. Mit der Sprache der Gruppentheorie können wir noch etwas anders über den Fixkörper nachdenken: Die Galoisgruppe $\text{Gal}(L/K)$ wirkt auf dem Körper L (denn jedes Element der Galoisgruppe ist ein Automorphismus von L , kann also ganz natürlich auf Elemente von L angewendet werden). Man hat also eine Gruppenwirkung

$$\text{Gal}(L/K) \times L \rightarrow L, \quad (\varphi, \ell) \mapsto \varphi(\ell).$$

Auch jede Untergruppe $H \subseteq \text{Gal}(L/K)$ wirkt somit auf L , denn man kann die Gruppenwirkung einfach einschränken und erhält

$$H \times L \rightarrow L, \quad (\varphi, \ell) \mapsto \varphi(\ell).$$

In unserer Notation aus Lemma 2.63 ist dann der Fixkörper nichts anderes als die Menge der Fixpunkte dieser Gruppenwirkung, wir haben also

$$L^H = \text{Fix}_H(L).$$

Bei einer allgemeinen Gruppenwirkung $G \times X \rightarrow X$ muss X nur eine Menge sein. In diesem Fall ist $X = L$ ein Körper und wir haben bewiesen, dass dann die Menge der Fixpunkte auch wieder einen Körper bildet.

Satz 5.32 (Hauptsatz der Galoistheorie). *Sei L/K eine endliche Galoiserweiterung und sei $\text{Gal}(L/K)$ ihre Galoisgruppe. Betrachte die folgenden beiden Mengen:*

$$\begin{aligned} \mathcal{ZK}(L/K) &:= \{M \subseteq L \mid M \text{ ist Zwischenkörper von } L/K\}, \\ \mathcal{UG}(L/K) &:= \{H \subseteq \text{Gal}(L/K) \mid H \text{ ist Untergruppe}\}. \end{aligned}$$

Dann sind die beiden Abbildungen

$$\begin{array}{ccc} & \Psi & \\ \mathcal{ZK}(L/K) & \xrightarrow{\quad} & \mathcal{UG}(L/K) \\ & \Phi & \\ M & \longmapsto & \text{Gal}(L/M) \\ L^H & \longleftarrow & H \end{array}$$

bijektiv und zueinander invers.
Außerdem gilt:

- (i) Sind $M, M' \in \mathcal{ZK}(L/K)$ mit $M \subseteq M'$, dann gilt $\text{Gal}(L/M) \supseteq \text{Gal}(L/M')$.
Sind $H, H' \in \mathcal{UG}(L/K)$ mit $H \subseteq H'$, dann gilt $L^H \supseteq L^{H'}$.
- (ii) Für $M \in \mathcal{ZK}(L/K)$ gilt

$$[M : K] = (\text{Gal}(L/K) : \text{Gal}(L/M)).$$

Kapitel 5 Galoistheorie

(iii) Für einen Zwischenkörper $M \in \mathcal{ZK}(L/K)$ ist die Körpererweiterung M/K genau dann normal, wenn $\text{Gal}(L/M) \triangleleft \text{Gal}(L/K)$ ein Normalteiler ist.

In diesem Fall ist die Abbildung

$$\text{Gal}(L/K)/\text{Gal}(L/M) \rightarrow \text{Gal}(M/K), \quad [\sigma] \mapsto \sigma|_M$$

ein Gruppenisomorphismus.

Beweis. Wir zeigen, dass die obigen Abbildungen $\Psi(M) = \text{Gal}(L/M)$ und $\Phi(H) = L^H$ invers zueinander (und damit insbesondere bijektiv) sind. Dazu müssen wir zeigen, dass $\Phi(\Psi(M)) = M$ für alle Zwischenkörper M von L/K und $\Psi(\Phi(H)) = H$ für alle Untergruppen $H \subseteq \text{Gal}(L/K)$.

Sei zunächst M ein Zwischenkörper von L/K . Wir zeigen $\Phi(\Psi(M)) = M$, d.h. $L^{\text{Gal}(L/M)} = M$, indem wir beide Inklusionen prüfen.

\supseteq : Diese Inklusion ist einfach: Sei $m \in M$, dann ist sicher $\sigma(m) = m$ für alle $\sigma \in \text{Gal}(L/M)$ (nach Definition der Galoisgruppe: diese besteht nur aus Automorphismen, welche Elemente des Grundkörpers unverändert lassen). Also ist $m \in L^{\text{Gal}(L/M)}$.

\subseteq : Sei $y \in L^{\text{Gal}(L/M)}$, d.h. $y \in L$ ist ein Element mit $\sigma(y) = y$ für alle $\sigma \in \text{Gal}(L/M)$. Wir müssen zeigen, dass dann bereits $y \in M$.

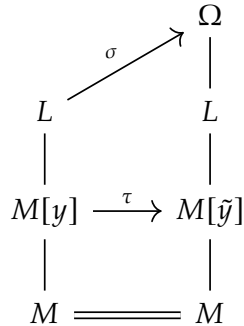
Nehmen wir an, dies wäre nicht der Fall, also $y \in L \setminus M$. Um einen Widerspruch zu erhalten, müssen wir ein Element $\sigma \in \text{Gal}(L/M)$ finden, sodass $\sigma(y) \neq y$.

Sei $p(X) \in M[X]$ das Minimalpolynom von y über M . Dann machen wir folgende Beobachtungen:

- $\deg(p) \geq 2$, denn wegen $y \notin M$ ist sicher $M[y] \neq M$, also folgt $\deg(p) = [M[y] : M] > 1$.
- $p(X)$ hat mindestens eine weitere, von y verschiedene Nullstelle in L , denn: L/K ist nach Voraussetzung galoissch, also normal und separabel. Somit ist nach Lemma 5.7 und Lemma 5.20 auch L/M normal und separabel. Weil $y \in L$ eine Nullstelle von $p(X)$ ist, muss somit $p(X)$ in $L[X]$ bereits in Linearfaktoren zerfallen (wegen Normalität). Außerdem sind die Nullstellen von $p(X)$ in L paarweise verschieden (wegen Separabilität) und wegen $\deg(p) \geq 2$ gibt es davon mindestens zwei.

Sei also $\tilde{y} \in L$ eine weitere Nullstelle von $p(X)$ mit $\tilde{y} \neq y$. Nach dem Fortsetzungssatz für einfache Erweiterungen (Satz 4.30) gibt es dann einen eindeutigen Körperhomomorphismus $\tau: M[y] \rightarrow M[\tilde{y}]$ mit $\tau|_M = \text{id}_M$. Nach dem Fortsetzungssatz in algebraisch abgeschlossene Körper (Satz 4.36) lässt sich dieser weiter fortsetzen zu einem Körperhomomorphismus $\sigma: L \rightarrow \Omega$ (wobei

Ω ein algebraischer Abschluss von L ist). Grafisch dargestellt:



Da aber L/M normal ist, ist σ nach Lemma 5.8 in Wirklichkeit bereits ein Körperautomorphismus von L , also ein Element der Galoisgruppe $\text{Gal}(L/M)$. Es gilt aber $\sigma(y) = \tilde{y} \neq y$ und dies ist der gewünschte Widerspruch. Folglich muss $y \in M$ gelten.

Sei nun $H \subseteq \text{Gal}(L/K)$ eine Untergruppe. Wir zeigen $\Psi(\Phi(H)) = H$, d.h. $\text{Gal}(L/L^H) = H$.

Die Inklusion $H \subseteq \text{Gal}(L/L^H)$ ist leicht zu sehen: Sei $\varphi \in H$. Dann gilt nach Definition von L^H , dass $\varphi(\ell) = \ell$ für alle $\varphi \in H$ und alle $\ell \in L^H$. In anderen Worten: Der Körperautomorphismus $\varphi: L \rightarrow L$ erfüllt $\varphi|_{L^H} = \text{id}_{L^H}$, also $\varphi \in \text{Gal}(L/L^H)$. Um die Gleichheit der beiden Gruppen zu zeigen, bemerken wir zuerst, dass $\text{Gal}(L/L^H)$ (und somit auch H) nach Lemma 5.29 eine endliche Gruppe ist, denn L/L^H ist eine endliche Galoiserweiterung.

Behauptung: $\#\text{Gal}(L/L^H) \leq \#H$.

Da L/K galoissch ist, ist auch L/L^H galoissch (Lemma 5.7 und Lemma 5.20), also ist nach Lemma 5.29 die Behauptung äquivalent zur Ungleichung

$$[L : L^H] \leq \#H.$$

Da L/L^H endlich und separabel ist, können wir den Satz vom primitiven Element anwenden: Es gibt also ein $\gamma \in L$, sodass $L = L^H[\gamma]$. Wir bezeichnen mit $p(X) \in L^H[X]$ das Minimalpolynom von γ über L^H . Es gilt also $\deg(p) = [L : L^H]$.

Weiter betrachten wir die Menge

$$A := \{\sigma(\gamma) \mid \sigma \in H\}$$

und das Polynom, das genau die Elemente von A als Nullstellen hat:

$$f(X) := \prod_{\alpha \in A} (X - \alpha) \in L[X].$$

(Dies ergibt Sinn, denn H ist eine endliche Gruppe und somit ist A eine endliche Menge. Es gilt nämlich $\#A \leq \#H$, denn mehrere $\sigma(\gamma)$ für verschiedene $\sigma \in H$ könnten gleich sein. Beachte zudem, dass $f(X)$ nur einfache Nullstellen besitzt, da jedes Element in A nur einmal „benutzt“ wird, selbst wenn verschiedene $\sigma \in H$ dasselbe $\sigma(\gamma)$ liefern.)

Dieses Polynom ist in Wahrheit nicht nur ein Polynom in $L[X]$, sondern hat bereits Koeffizienten in L^H , wie wir nun zeigen: Sei $\tau \in H$ und betrachten wir das Polynom

$$f^\tau(X) = \prod_{\alpha \in A} (X - \tau(\alpha)).$$

Dieses hat also als Nullstellen die Elemente $\tau(\alpha)$ für alle $\alpha \in A$. Die Nullstellenmenge ist also

$$\tau(A) = \{\tau(\alpha) \mid \alpha \in A\} = \{\tau(\sigma(\gamma)) \mid \sigma \in H\}.$$

Es ist aber

$$\tau(A) = \{\tau(\sigma(\gamma)) \mid \sigma \in H\} = \{\tilde{\sigma}(\gamma) \mid \tilde{\sigma} \in \tau H\} = \{\tilde{\sigma}(\gamma) \mid \tilde{\sigma} \in H\} = A,$$

denn $\tau \in H$ und somit ist $\tau H = \text{id} \cdot H = H$ (wir erinnern uns an Lemma-Definition 2.28). Die Polynome $f(X)$ und $f^\tau(X)$ haben also die gleichen (und nur einfache) Nullstellen und sind somit gleich. Schreiben wir $f(X) = \sum_{i=0}^n a_i X^i$ für bestimmte $a_i \in L$, dann ist $f^\tau(X) = \sum_{i=0}^n \tau(a_i) X^i$. Wegen der eben gezeigten Gleichheit $f(X) = f^\tau(X)$ muss also dann $\tau(a_i) = a_i$ für alle $i \in \{1, \dots, n\}$ gelten, also $a_i \in L^H$ für alle $i \in \{1, \dots, n\}$. Damit haben wir gezeigt, dass $f(X) \in L^H[X]$.

Wir haben also nun ein Polynom $f(X) \in L^H[X]$ gefunden, welches γ als Nullstelle hat (denn $\gamma = \text{id}(\gamma) \in A$). Dann muss das Minimalpolynom $p(X)$ von γ über L^H ein Teiler von $f(X)$ sein, d.h. $p(X) \mid f(X)$ in $L^H[X]$. Also ist wie behauptet

$$[L : L^H] = \deg(p) \leq \deg(f) = \#A \leq \#H.$$

Insgesamt ist also $H \subseteq \text{Gal}(L/L^H)$ eine Untergruppe mit mindestens so vielen Elementen wie $\text{Gal}(L/L^H)$ und damit folgt $H = \text{Gal}(L/L^H)$.

Nun beweisen wir noch die Zusätze (i)–(iii):

(i) Dies folgt direkt aus den Definitionen:

Sind M, M' zwei Zwischenkörper von L/K mit $M \subseteq M'$, so haben wir sicher $\text{Gal}(L/M') \subseteq \text{Gal}(L/M)$ (jeder Körperautomorphismus von L , der M' die Identität ist, ist dies insbesondere auf M).

Ebenso offensichtlich ist die folgende Aussage: Sind $H, H' \subseteq \text{Gal}(L/K)$ zwei Untergruppen mit $H \subseteq H'$, dann ist $L^{H'} \subseteq L^H$ (bleibt ein Element von L unter allen Gruppenelementen von H' unverändert, so tut es dies insbesondere unter allen Gruppenelementen von H).

(ii) Wir betrachten den Körperturm

$$[L:K] \begin{array}{c} L \\ \left| \begin{array}{l} [L:M] \\ M \\ [M:K] \end{array} \right. \\ K \end{array}$$

Nach Satz 4.8 gilt also

$$[M : K] = \frac{[L : K]}{[L : M]}.$$

Nach Voraussetzung ist L/K endlich und galoissch. Dies gilt somit auch für L/M (nach Lemma 5.7 und Lemma 5.20). Mit Lemma 5.29 folgt dann also

$$[M : K] = \frac{\#\text{Gal}(L/K)}{\#\text{Gal}(L/M)} = (\text{Gal}(L/K) : \text{Gal}(L/M)),$$

wobei der letzte Schritt aus dem Satz von Lagrange folgt (Satz 2.53).

(iii) Sei M ein Zwischenkörper von L/K . Wir zeigen zuerst:

$$M/K \text{ ist normal} \Leftrightarrow \text{Gal}(L/M) \text{ ist Normalteiler in } \text{Gal}(L/K).$$

\Rightarrow : Sei M/K normal. Seien $\sigma \in \text{Gal}(L/K)$ und $\varphi \in \text{Gal}(L/M)$ beliebig. Dann müssen wir zeigen, dass $\sigma \circ \varphi \circ \sigma^{-1} \in \text{Gal}(L/M)$. Sicher ist $\sigma \circ \varphi \circ \sigma^{-1}$ ein Körperautomorphismus von L , also ist noch zu zeigen, dass

$$\forall m \in M : (\sigma \circ \varphi \circ \sigma^{-1})(m) = m.$$

Sei also $m \in M$ beliebig und sei $f(X) \in K[X]$ das Minimalpolynom von m über K . Dann ist nach Lemma 4.28 das Element $\sigma^{-1}(m) \in L$ ebenfalls eine Nullstelle von $f(X)$. Da aber M/K normal ist und das irreduzible Polynom $f(X)$ bereits eine Nullstelle in M hat, muss auch $\sigma^{-1}(m) \in M$ gelten. Dann können wir berechnen

$$(\sigma \circ \varphi \circ \sigma^{-1})(m) = \sigma(\underbrace{\varphi(\sigma^{-1}(m))}_{\in M}) = \sigma(\sigma^{-1}(m)) = m,$$

da wir wissen, dass $\varphi|_M = \text{id}_M$. Somit ist $\text{Gal}(L/M) \triangleleft \text{Gal}(L/K)$ ein Normalteiler.

\Leftarrow : Sei nun $\text{Gal}(L/M) \triangleleft \text{Gal}(L/K)$ ein Normalteiler und sei $f(X) \in K[X]$ ein irreduzibles Polynom mit einer Nullstelle $\alpha \in M$. In $L[X]$ zerfällt $f(X)$ in Linearfaktoren, da L/K normal ist, und wir müssen zeigen, dass dies

auch in $M[X]$ der Fall ist. Sei also $\beta \in L$ eine beliebige Nullstelle von $f(X)$. Dann ist zu zeigen, dass $\beta \in M$.

Nach der bereits gezeigten Bijektion (erster Teil des Hauptsatzes der Galoistheorie) ist $M = L^{\text{Gal}(L/M)}$, d.h. es reicht zu zeigen, dass $\varphi(\beta) = \beta$ für alle $\varphi \in \text{Gal}(L/M)$.

Bevor wir dies zeigen, überlegen wir uns noch Folgendes: Mit Satz 4.30 und Satz 4.36 können wir die Identitätsabbildung auf K fortsetzen zu einem Körperautomorphismus $\sigma: L \rightarrow L$ mit $\sigma(\beta) = \alpha$, d.h.

$$\begin{array}{ccc} L & \xrightarrow{\sigma} & L \\ | & & | \\ K[\beta] & \longrightarrow & K[\alpha] \\ | & & | \\ K & \xlongequal{\quad} & K \end{array}$$

(Ähnlich wie im Diagramm auf Seite 141 ist $\sigma: L \rightarrow \Omega$ a priori ein Körperhomomorphismus in einen algebraischen Abschluss von L , aber mit Lemma 5.8 ist dieser dann wegen der Normalität von L/K bereits ein Körperautomorphismus von L .)

Sei nun $\varphi \in \text{Gal}(L/M)$. Da $\text{Gal}(L/M)$ ein Normalteiler in $\text{Gal}(L/K)$ ist, folgt dann $\sigma \circ \varphi \circ \sigma^{-1} \in \text{Gal}(L/M)$, also insbesondere $(\sigma \circ \varphi \circ \sigma^{-1})(m) = m$ für alle $m \in M$. Wir erhalten also

$$\alpha = (\sigma \circ \varphi \circ \sigma^{-1})(\alpha) = \sigma(\underbrace{\varphi(\sigma^{-1}(\alpha))}_{=\beta}) = \sigma(\varphi(\beta))$$

und somit $\varphi(\beta) = \sigma^{-1}(\alpha) = \beta$, was zu zeigen war.

Sei nun $\text{Gal}(L/M)$ ein Normalteiler in $\text{Gal}(L/K)$ (und damit automatisch M/K eine normale Erweiterung nach dem eben Gezeigten). Dann ist (nach Satz 2.34) $\text{Gal}(L/K)/\text{Gal}(L/M)$ eine Gruppe und wir beweisen nun noch, dass

$$\text{Gal}(L/K)/\text{Gal}(L/M) \rightarrow \text{Gal}(M/K), \quad [\sigma] \mapsto \sigma|_M$$

ein Isomorphismus von Gruppen ist.

Betrachte dazu zunächst die Abbildung

$$\rho: \text{Gal}(L/K) \rightarrow \text{Gal}(M/K), \quad \sigma \mapsto \sigma|_M.$$

Diese ist wohldefiniert: Ist $\sigma \in \text{Gal}(L/K)$, d.h. σ ist ein Körperautomorphismus von L mit $\sigma|_K = \text{id}_K$, so ist zunächst $\sigma|_M: M \rightarrow L$ ein Körperhomomorphismus. Sei Ω ein algebraischer Abschluss von L (und damit auch von M). Dann

können wir $\sigma|_M$ auch als Körperhomomorphismus von M nach Ω auffassen und es gilt mit Lemma 5.8

$$\sigma|_M \in \text{Hom}_K(M, L) \subseteq \text{Hom}_K(M, \Omega) = \text{Aut}_K(M) = \text{Gal}(M/K).$$

Offensichtlich ist die Abbildung ρ ein Gruppenhomomorphismus. Sie ist außerdem surjektiv, denn jedes $\tau \in \text{Gal}(M/K)$ kann nach Satz 4.36 zu einem $\sigma \in \text{Gal}(L/K)$ fortgesetzt werden. (Hier verwenden wir wieder – wie bereits zweimal im Beweis des Hauptsatzes – das Argument, dass die Fortsetzung zunächst von der Form $\sigma: L \rightarrow \Omega$ ist, aber mit Lemma 5.8 bereits $\sigma \in \text{Aut}_K(L) = \text{Gal}(L/K)$ gilt.)

Der Kern dieses Gruppenhomomorphismus ist nun

$$\ker(\rho) = \{\sigma \in \text{Gal}(L/K) \mid \sigma|_M = \text{id}_M\} = \text{Gal}(L/M)$$

und daher ist nach dem Homomorphiesatz (Satz 2.38)

$$\bar{\rho}: \text{Gal}(L/K)/\text{Gal}(L/M) \rightarrow \text{Gal}(M/K), \quad [\sigma] \mapsto \sigma|_M$$

ein Gruppenisomorphismus.

Der Hauptsatz der Galoistheorie ist hiermit bewiesen. \square

Bemerkung 5.33. Der Hauptsatz der Galoistheorie beantwortet also eine natürliche Frage:

Gegeben eine Körpererweiterung L/K , so haben wir die Galoisgruppe $\text{Gal}(L/K)$. Betrachten wir nun eine Zwischenerweiterung M , so können wir die Galoisgruppe $\text{Gal}(L/M)$ betrachten und diese ist natürlicherweise eine Untergruppe von $\text{Gal}(L/K)$. Man fragt sich sofort, ob man auf diese Weise alle möglichen Untergruppen von $\text{Gal}(L/K)$ erhält und ob dieselbe Untergruppe für mehrere verschiedene Zwischenerweiterungen auftreten kann. In anderen Worten:

Ist die Abbildung, die einem Zwischenkörper M die Untergruppe $\text{Gal}(L/M)$ zuordnet, eine bijektive Abbildung?

Der Hauptsatz der Galoistheorie beantwortet diese Frage mit „Ja“, falls L/K eine endliche Galoiserweiterung ist.

Der Hauptsatz sagt uns aber noch mehr:

- Er sagt uns explizit, wie die Umkehrabbildung aussieht.
- Er sagt uns, dass sich die Teilmengenrelationen umkehren (Punkt (i)), d.h. je größer der Zwischenkörper wird, desto kleiner wird die Untergruppe und umgekehrt.
- Er stellt einen Zusammenhang zwischen dem Grad der Zwischenerweiterung und dem Index der entsprechenden Untergruppe her (Punkt (ii)).

- Er erklärt uns, was gewisse Eigenschaften einer Zwischenerweiterung für die Eigenschaften der zugehörigen Untergruppe bedeuten (Punkt (iii)): Ist die Zwischenerweiterung normal über K , so ist die entsprechende Untergruppe sogar ein Normalteiler und umgekehrt.

Ein solcher Satz ist (wie viele Äquivalenzen in der Mathematik) deshalb nützlich, weil er eine Verbindung zwischen zwei verschiedenen Teilgebieten der Algebra herstellt: Der Gruppentheorie und der Körpertheorie. Wenn wir also etwas über eine bestimmte Körpererweiterung verstehen möchten, können wir von nun an auch gruppentheoretische Argumente bemühen. Beispielsweise könnte es schwierig sein, direkt mithilfe der Körpertheorie festzustellen, ob die Erweiterung normal ist. Möglicherweise ist es aber nicht so kompliziert, festzustellen, ob die Galoisgruppe ein Normalteiler ist, da wir uns mittlerweile in der Gruppentheorie recht gut auskennen. Wir können unser körpertheoretisches Problem also mithilfe des Hauptsatzes in ein gruppentheoretisches „übersetzen“. Dies wird auch in Beispiel 5.35 illustriert.

Bemerkung 5.34. Strenggenommen haben wir den Hauptsatz bisher nur für Körper mit unendlich vielen Elementen bewiesen: Wir haben im Beweis nämlich den Satz vom primitiven Element verwendet. Dieser gilt zwar für jede endliche separable Körpererweiterung, aber wir haben ihn bisher nur für unendliche Körper bewiesen (siehe Satz 5.26). Der Beweis des Hauptsatzes ist also in voller Allgemeinheit erst dann komplett, wenn wir den Satz vom primitiven Element auch für endliche Körper bewiesen haben, was im nächsten Abschnitt passieren wird.

Beispiel 5.35. Wir möchten uns eine explizite Anwendung des Hauptsatzes von Galois ansehen, nämlich im Fall unseres (bereits öfter bemühten) Körpers $L = \mathbb{Q}[\sqrt{2}, \sqrt{3}]$. Angenommen, man möchte alle Zwischenkörper von $\mathbb{Q}[\sqrt{2}, \sqrt{3}]/\mathbb{Q}$ bestimmen. Wir wissen, dass $\mathbb{Q}[\sqrt{2}]$ und $\mathbb{Q}[\sqrt{3}]$ Zwischenkörper sind, und denken wir noch einen Moment länger nach, fällt uns vielleicht noch der Zwischenkörper $\mathbb{Q}[\sqrt{6}]$ ein. Wie können wir aber herausfinden, ob das *alle* Zwischenkörper sind? Dazu nutzen wir jetzt den Hauptsatz der Galoistheorie: Dieser ist hier anwendbar, da $\mathbb{Q}[\sqrt{2}, \sqrt{3}]/\mathbb{Q}$ eine endliche Galoiserweiterung ist ($\mathbb{Q}[\sqrt{2}, \sqrt{3}]$ ist Zerfällungskörper und \mathbb{Q} ist vollkommen). Der Hauptsatz besagt dann, dass es genauso viele Zwischenkörper gibt wie es Untergruppen von $\text{Gal}(\mathbb{Q}[\sqrt{2}, \sqrt{3}]/\mathbb{Q})$ gibt, und dass die Zwischenkörper genau die Fixkörper dieser Untergruppen sind. Sehen wir uns also die Galoisgruppe an. Diese hat vier Elemente

$$\text{Gal}(\mathbb{Q}[\sqrt{2}, \sqrt{3}]/\mathbb{Q}) = \{\sigma_1, \sigma_2, \sigma_3, \sigma_4\}$$

und diese sind gegeben durch

$$\begin{array}{ll} \sigma_1 = \text{id}: \sqrt{2} \mapsto \sqrt{2} & \sigma_2: \sqrt{2} \mapsto -\sqrt{2} \\ \sqrt{3} \mapsto \sqrt{3} & \sqrt{3} \mapsto \sqrt{3} \\ \\ \sigma_3: \sqrt{2} \mapsto \sqrt{2} & \sigma_4: \sqrt{2} \mapsto -\sqrt{2} \\ \sqrt{3} \mapsto -\sqrt{3} & \sqrt{3} \mapsto -\sqrt{3} \end{array}$$

(Wir erinnern uns, dass ein Element der Galoisgruppe eindeutig bestimmt ist, wenn wir wissen, worauf die Elemente $\sqrt{2}$ und $\sqrt{3}$ abgebildet werden.)

Man überlegt sich leicht, dass $\text{Gal}(\mathbb{Q}[\sqrt{2}, \sqrt{3}]/\mathbb{Q})$ die folgenden fünf Untergruppen hat:

$$H_1 = \{\sigma_1\}, \quad H_2 = \{\sigma_1, \sigma_2\}, \quad H_3 = \{\sigma_1, \sigma_3\}, \quad H_4 = \{\sigma_1, \sigma_4\}, \quad H_5 = \{\sigma_1, \sigma_2, \sigma_3, \sigma_4\}.$$

Dies sind alle Untergruppen und somit gibt es die folgenden fünf Zwischenkörper:

$$L^{H_1} = L, \quad L^{H_2} = \mathbb{Q}[\sqrt{3}], \quad L^{H_3} = \mathbb{Q}[\sqrt{2}], \quad L^{H_4} = \mathbb{Q}[\sqrt{6}], \quad L^{H_5} = \mathbb{Q}.$$

Diese zu bestimmen, ist nicht besonders schwierig: Ein Element $x \in L$ lässt sich eindeutig als Linearkombination $x = a + b\sqrt{2} + c\sqrt{3} + d\sqrt{6}$ mit $a, b, c, d \in \mathbb{Q}$ schreiben. Wenn wir jetzt beispielsweise den Fixkörper L^{H_2} bestimmen möchten, müssen wir herausfinden, welche Elemente unter σ_2 unverändert bleiben (dies ist das einzige „interessante“ Element von H_2 , denn unter $\sigma_1 = \text{id}$ bleibt sowieso alles unverändert). Wir müssen also die Gleichung $\sigma_2(x) = x$ betrachten. Wir wissen, dass $\sigma_2|_{\mathbb{Q}} = \text{id}_{\mathbb{Q}}$ und dass $\sigma_2(\sqrt{2}) = -\sqrt{2}$, $\sigma_2(\sqrt{3}) = \sqrt{3}$ sowie $\sigma_2(\sqrt{6}) = \sigma_2(\sqrt{2}\sqrt{3}) = -\sqrt{2}\sqrt{3} = -\sqrt{6}$. Also lautet die zu lösende Gleichung

$$a - b\sqrt{2} + c\sqrt{3} - d\sqrt{6} = a + b\sqrt{2} + c\sqrt{3} + d\sqrt{6}$$

und damit folgt $b = d = 0$, da die Elemente $1, \sqrt{2}, \sqrt{3}, \sqrt{6}$ eine Basis von L über \mathbb{Q} bilden. Der Fixkörper besteht also aus Elementen der Form $a + c\sqrt{3}$, also haben wir $L^{H_2} = \mathbb{Q}[\sqrt{3}]$.

Es gibt also tatsächlich nur die oben bereits erratenen Zwischenkörper von $\mathbb{Q}[\sqrt{2}, \sqrt{3}]/\mathbb{Q}$.

Auch bei der Bestimmung eines primitiven Elements können wir uns die Galoisgruppe zunutze machen. In der Einführung (Kapitel 1) haben wir erwähnt, dass $\mathbb{Q}[\sqrt{2}, \sqrt{3}] = \mathbb{Q}[\sqrt{2} + \sqrt{3}]$ gilt. Dies kann man zeigen, indem man ein irreduzibles Polynom vom Grad 4 bestimmt, welches $\sqrt{2} + \sqrt{3}$ als Nullstelle hat. Dann ist $\mathbb{Q}[\sqrt{2} + \sqrt{3}]$ ein Zwischenkörper von $\mathbb{Q}[\sqrt{2}, \sqrt{3}]/\mathbb{Q}$, der denselben Erweiterungsgrad wie $\mathbb{Q}[\sqrt{2}, \sqrt{3}]$ über \mathbb{Q} hat und somit müssen die beiden gleich sein. Das ist machbar,

Kapitel 5 Galoistheorie

aber man muss etwas arbeiten, um zu zeigen, dass das Polynom $X^4 - 10X^2 + 1$ irreduzibel ist (keines unserer Irreduzibilitätskriterien lässt sich hier anwenden, man muss das also „von Hand“ prüfen).

Wir geben hier ein alternatives Argument, um $\mathbb{Q}[\sqrt{2}, \sqrt{3}] = \mathbb{Q}[\sqrt{2} + \sqrt{3}]$ zu zeigen: Die Galoisgruppe $\text{Gal}(\mathbb{Q}[\sqrt{2}, \sqrt{3}]/\mathbb{Q})$ haben wir oben bestimmt. Es ist bekannt (Lemma 4.28), dass für $\sigma \in \text{Gal}(\mathbb{Q}[\sqrt{2}, \sqrt{3}]/\mathbb{Q})$ das Element $\sigma(\sqrt{2} + \sqrt{3})$ dasselbe Minimalpolynom wie $\sqrt{2} + \sqrt{3}$ über \mathbb{Q} hat. Es müssen also die vier Elemente

$$\begin{aligned}\sigma_1(\sqrt{2} + \sqrt{3}) &= \sqrt{2} + \sqrt{3}, & \sigma_2(\sqrt{2} + \sqrt{3}) &= -\sqrt{2} + \sqrt{3} \\ \sigma_3(\sqrt{2} + \sqrt{3}) &= \sqrt{2} - \sqrt{3}, & \sigma_4(\sqrt{2} + \sqrt{3}) &= -\sqrt{2} - \sqrt{3}\end{aligned}$$

dasselbe Minimalpolynom über \mathbb{Q} haben. Da diese Elemente paarweise verschieden sind, bedeutet dies, dass das Minimalpolynom von $\sqrt{2} + \sqrt{3}$ mindestens den Grad 4 haben muss. Damit folgt, dass $\mathbb{Q}[\sqrt{2}, \sqrt{3}] = \mathbb{Q}[\sqrt{2} + \sqrt{3}]$, ohne dass wir hier das Minimalpolynom wirklich ausrechnen und seine Irreduzibilität zeigen mussten!

Die Argumente in diesem Beispiel funktionieren übrigens ganz analog, wenn wir statt \mathbb{Q} einen beliebigen Körper K mit $\text{char}(K) \neq 2$ ersetzen und statt $\sqrt{2}$ und $\sqrt{3}$ zwei Wurzeln \sqrt{a} und \sqrt{b} , wobei a, b und ab keine Quadrate in K sein sollen. Dann gibt es ebenfalls genau die fünf Zwischenkörper wie oben und $\sqrt{a} + \sqrt{b}$ ist ein primitives Element von $K[\sqrt{a}, \sqrt{b}]/K$.

5.6 Endliche Körper

Wir beschäftigen uns jetzt noch mit einer wichtigen und interessanten Klasse von Körpern, nämlich solchen mit endlich vielen Elementen. Auch wenn wir bisher in unseren Überlegungen zur Körper- und Galoistheorie meistens an Beispiele über \mathbb{Q} oder Teilkörper von \mathbb{C} , also insbesondere an Körper der Charakteristik 0 gedacht haben, galten unsere Resultate natürlich auch für endliche Körper. Diese spielen in vielen Anwendungen, beispielsweise in der Kryptographie, aber auch in der Geometrie eine wichtige Rolle. Auch in dieser Vorlesung haben wir bereits gesehen, wie endliche Körper uns helfen können, selbst wenn wir uns eigentlich für Objekte über den rationalen Zahlen interessieren (siehe das Reduktionskriterium Satz 3.83).

Einige Eigenschaften endlicher Körper wollen wir nun näher untersuchen. Insbesondere werden wir lernen, dass solche Körper ebenfalls vollkommen sind und dass für sie der Satz vom primitiven Element gilt.

Die einfachsten Beispiele endlicher Körper sind die Körper $\mathbb{F}_p := \mathbb{Z}/p\mathbb{Z}$ für eine Primzahl p . Es sind aber nicht die einzigen, denn natürlich kann man zum Beispiel Körpererweiterungen von \mathbb{F}_p betrachten.

Lemma 5.36. *Sei K ein endlicher Körper, dann gilt:*

- (i) $\text{char}(K) = p$ für eine Primzahl p ,

- (ii) K ist eine Körpererweiterung von \mathbb{F}_p ,
 (iii) $\#K = p^k$ für ein $k \in \mathbb{N}$.

Beweis. (i) Nach Lemma-Definition 5.15 ist $\text{char}(K)$ entweder eine Primzahl oder Null. Letzteres kann aber nicht der Fall sein, denn ein Körper der Charakteristik 0 hat unendlich viele Elemente, weil dann die Elemente $n \cdot 1$ für alle $n \in \mathbb{N}$ paarweise verschieden sind.

- (ii) Wir betrachten die Abbildung

$$\varphi: \mathbb{Z} \rightarrow K, \quad n \mapsto n \cdot 1.$$

Diese ist ein Ringhomomorphismus und es gilt

$$\ker(\varphi) = p\mathbb{Z},$$

also erhalten wir mit dem Homomorphiesatz (Satz 2.38) einen injektiven Körperhomomorphismus

$$\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z} \rightarrow K,$$

bezüglich dessen wir \mathbb{F}_p also als Teilkörper von K betrachten können. (Beachte, dass es *genau eine* Möglichkeit gibt, \mathbb{F}_p als Teilkörper von K zu betrachten, denn die Abbildung φ ist wegen $\varphi(1) = 1$ eindeutig bestimmt.)

- (iii) Da wir nach (ii) die Körpererweiterung K/\mathbb{F}_p haben, ist K ein \mathbb{F}_p -Vektorraum. Es muss außerdem gelten, dass $[K : \mathbb{F}_p] = \dim_{\mathbb{F}_p} K < \infty$, denn wäre K ein unendlichdimensionaler \mathbb{F}_p -Vektorraum, so hätte K unendlich viele Elemente. Also gilt

$$\#K = (\#\mathbb{F}_p)^{[K:\mathbb{F}_p]} = p^{[K:\mathbb{F}_p]}$$

(denn jedes Element in K ist eine Linearkombination der Basiselemente und für jedes der $[K : \mathbb{F}_p]$ Basiselemente gibt es p mögliche Koeffizienten). □

Die Anzahl der Elemente eines endlichen Körpers ist also immer eine Primzahlpotenz p^k . Das ist schon einmal eine recht große Einschränkung: Es kann also zum Beispiel keinen Körper mit 6 Elementen geben. Umgekehrt fragt man sich nun sofort: Gibt es für jede Primzahlpotenz p^k einen Körper mit p^k Elementen? Diese Frage beantwortet Satz 5.39 unten. Bevor wir ihn formulieren können, führen wir noch eine wichtige Abbildung ein.

Lemma-Definition 5.37. Sei K ein Körper mit $\text{char}(K) = p$ für eine Primzahl p . Dann definieren wir die Abbildung

$$\text{Frob}: K \rightarrow K, \quad x \mapsto x^p.$$

Sie ist ein Körperhomomorphismus mit $\text{Frob}|_{\mathbb{F}_p} = \text{id}_{\mathbb{F}_p}$ und heißt der **Frobenius-homomorphismus** auf K .

Ist $K = \overline{\mathbb{F}_p}$ ein algebraischer Abschluss von \mathbb{F}_p , so ist $\text{Frob}: \overline{\mathbb{F}_p} \rightarrow \overline{\mathbb{F}_p}$ sogar ein Körperautomorphismus, also gilt $\text{Frob} \in \text{Gal}(\overline{\mathbb{F}_p}/\mathbb{F}_p)$.

Kapitel 5 Galoistheorie

Beweis. Fast alle Eigenschaften eines Körperhomomorphismus sind klar: Es gilt offensichtlich $\text{Frob}(0) = 0^p = 0$, $\text{Frob}(1) = 1^p = 1$ und $\text{Frob}(x \cdot y) = (x \cdot y)^p = x^p \cdot y^p$ für alle $x, y \in K$. Es fehlt noch zu zeigen, dass $\text{Frob}(x + y) = (x + y)^p = x^p + y^p$ für beliebige $x, y \in K$. Nach dem binomischen Lehrsatz haben wir zunächst

$$(x + y)^p = \sum_{k=0}^p \binom{p}{k} x^k y^{p-k}.$$

Man sieht leicht, dass $p \mid \binom{p}{k}$ für $k \in \{1, \dots, p-1\}$, denn

$$\binom{p}{k} = \frac{p!}{(p-k)!k!} = \frac{p \cdot (p-1) \cdot \dots \cdot (p-k+1)}{k \cdot (k-1) \cdot \dots \cdot 1}$$

und somit kann der Faktor p im Zähler nicht durch einen Faktor im Nenner ausgelöscht werden, da p eine Primzahl ist und somit keine nichttrivialen Teiler kleiner als p besitzt. Folglich verschwinden in K alle Terme außer die für $k=0$ und $k=p$, also ist $(x+y)^p = x^p + y^p$ und somit ist $\text{Frob}: K \rightarrow K$ ein Körperhomomorphismus.

Nun zeigen wir, dass $\text{Frob}|_{\mathbb{F}_p} = \text{id}_{\mathbb{F}_p}$. Sei also $x \in \mathbb{F}_p$. Falls $x=0$, so ist offensichtlich $\text{Frob}(0) = 0^p = 0$. Falls $x \neq 0$, dann ist also $x \in \mathbb{F}_p^\times$ eine Einheit in \mathbb{F}_p . Die Einheiten \mathbb{F}_p^\times bilden zusammen mit der Multiplikation eine Gruppe und es ist $\#\mathbb{F}_p^\times = p-1$. Also haben wir $x^{p-1} = 1$ nach Korollar 2.54(iii). Multiplizieren wir diese Gleichung mit x , erhalten wir $x^p = x$, also $\text{Frob}(x) = x$.

Ist nun $K = \overline{\mathbb{F}_p}$, so ist K algebraisch abgeschlossen, also hat das Polynom $X^p - y$ für jedes $y \in \overline{\mathbb{F}_p}$ eine Nullstelle in $\overline{\mathbb{F}_p}$. Dies bedeutet, dass es für jedes $y \in \overline{\mathbb{F}_p}$ ein $x \in \overline{\mathbb{F}_p}$ gibt mit $x^p = y$ und somit ist $\text{Frob}: \overline{\mathbb{F}_p} \rightarrow \overline{\mathbb{F}_p}$ surjektiv. Da Körperhomomorphismen immer injektiv sind und wir bereits $\text{Frob}|_{\mathbb{F}_p} = \text{id}_{\mathbb{F}_p}$ gezeigt haben, folgt dann $\text{Frob} \in \text{Aut}_{\mathbb{F}_p}(\overline{\mathbb{F}_p}) = \text{Gal}(\overline{\mathbb{F}_p}/\mathbb{F}_p)$. \square

An dieser Stelle möchten wir einen berühmten Satz erwähnen, dessen (mit unseren gruppentheoretischen Vorkenntnissen sehr kurzen!) Beweis wir gerade im Vorübergehen im zweiten Absatz des Beweises von Lemma-Definition 5.37 gegeben haben.

Satz 5.38 (Kleiner fermatscher Satz). *Sei $p \in \mathbb{N}$ eine Primzahl. Dann gilt für jede ganze Zahl $a \in \mathbb{Z}$ die Kongruenz*

$$a^p \equiv a \pmod{p}.$$

Nun zeigen wir die Existenz und einige Eigenschaften von endlichen Körpern mit beliebigen Primpotenzordnungen.

Satz 5.39. *Sei p eine Primzahl, $\overline{\mathbb{F}_p}$ ein algebraischer Abschluss von \mathbb{F}_p und $k \in \mathbb{N}$. Wir schreiben $q := p^k$. Dann gibt es genau einen Zwischenkörper K von $\overline{\mathbb{F}_p}/\mathbb{F}_p$ mit $\#K = q = p^k$. Für diesen gilt:*

- (i) K ist Zerfällungskörper des Polynoms $f(X) = X^q - X \in \mathbb{F}_p[X]$.

- (ii) K/\mathbb{F}_p ist eine Galoisweiterung.
- (iii) Die Galoisgruppe $\text{Gal}(K/\mathbb{F}_p)$ ist eine zyklische Gruppe, erzeugt durch den Frobenius-homomorphismus, es gilt also

$$\text{Gal}(K/\mathbb{F}_p) = \langle \text{Frob} \rangle = \{\text{Frob}^0 = \text{id}_K, \text{Frob}, \text{Frob}^2, \dots, \text{Frob}^{q-1}\}.$$

Beweis. Wir betrachten die Menge aller Nullstellen von $f(X) = X^q - X$ im algebraischen Abschluss

$$K := \{x \in \overline{\mathbb{F}_p} \mid x^q = x\} \subseteq \overline{\mathbb{F}_p}.$$

Es gilt sicher $\mathbb{F}_p \subseteq K$, denn für $x \in \mathbb{F}_p$ gilt $x^p = x$ (siehe Lemma-Definition 5.37) und somit

$$x^q = x^{p^k} = (x^p)^{p^{k-1}} = x^{p^{k-1}} = (x^p)^{p^{k-2}} = x^{p^{k-2}} = \dots = x^p = x.$$

Weiter ist $\#K = q$, wie man folgendermaßen sieht: Das Polynom $f(X) = X^q - X$ hat als formale Ableitung das Polynom $f'(X) = qX^{q-1} - 1 = -1$ (denn der Leitkoeffizient $q = p^k$ ist gleich Null in \mathbb{F}_p). Also ist $\text{ggT}(f(X), f'(X)) = 1$ und somit ist $f(X)$ nach Korollar 5.14 separabel. Es hat also q paarweise verschiedene Nullstellen.

Die Menge K ist ein Körper, denn:

- (1) $0 \in K$ und $1 \in K$, denn $0^q = 0$ und $1^q = 1$.
- (2) Sind $x, y \in K$, d.h. $x^q = x$ und $y^q = y$, dann folgt induktiv

$$\begin{aligned} (x + y)^q &= (x + y)^{p^k} = ((x + y)^p)^{p^{k-1}} = (x^p + y^p)^{p^{k-1}} = ((x^p + y^p)^p)^{p^{k-2}} \\ &= ((x^p)^p + (y^p)^p)^{p^{k-2}} = (x^{p^2} + y^{p^2})^{p^{k-2}} = \dots = \\ &= x^{p^k} + y^{p^k} = x^q + y^q = x + y, \end{aligned}$$

wobei wir wiederholt verwendet haben, dass für alle $a, b \in K$ gilt $(a + b)^p = a^p + b^p$ (dass also die Frobeniusabbildung ein Körperhomomorphismus ist, siehe Lemma-Definition 5.37).

Außerdem folgt

$$(x \cdot y)^q = x^q \cdot y^q = x \cdot y.$$

Insgesamt gilt also $x + y, x \cdot y \in K$.

- (3) Sei $x \in K$, d.h. $x^q = x$, dann folgt

$$(-x)^q = (-1)^q x^q = (-1)^q x.$$

Falls q ungerade ist, bedeutet dies also $(-x)^q = -x$. Falls q gerade ist, bedeutet dies $p = 2$ (denn p muss eine Primzahl sein) und somit gilt $-1 = 1$ in K , also haben wir auch in diesem Fall $(-x)^q = x = -x$. Insgesamt ist also immer $-x \in K$.

Außerdem haben wir $(x^{-1})^q = (x^q)^{-1} = x^{-1}$, also auch $x^{-1} \in K$.

Der Körper K ist also ein Zwischenkörper mit q Elementen. Damit ist die Existenz eines solchen bewiesen.

Wir zeigen nun die Eindeutigkeit: Sei M ein beliebiger anderer Zwischenkörper von $\overline{\mathbb{F}_p}/\mathbb{F}_p$ mit q Elementen. Dann bilden die Einheiten $M^\times = M \setminus \{0\}$ mit der Multiplikation eine Gruppe mit $q-1$ Elementen und somit folgt mit Korollar 2.54(iii), dass $x^{q-1} = 1$ für alle $x \in M^\times$, also $x^q = x$ für alle $x \in M^\times$ (und damit für alle $x \in M$, denn für $x = 0$ gilt diese Gleichheit ja sowieso). Es folgt also $M \subseteq K$ und da beide Körper endlich sind und die gleiche Anzahl an Elementen haben, folgt $M = K$.

Jetzt noch zu den drei Eigenschaften von K :

- (i) K enthält alle Nullstellen von $X^q - X$. Andererseits enthält K aber *ausschließlich* die Nullstellen $\alpha_1, \dots, \alpha_q$ von f , also gilt $K = \mathbb{F}_p[\alpha_1, \dots, \alpha_q]$ und somit ist K der Zerfällungskörper in $\overline{\mathbb{F}_p}$ von $f(X)$.
- (ii) Da K ein Zerfällungskörper eines Polynoms in $\mathbb{F}_p[X]$ ist, ist K/\mathbb{F}_p eine normale Erweiterung. Außerdem ist $K = \mathbb{F}_p[\alpha_1, \dots, \alpha_q]$, also können wir K sukzessive durch Adjunktion eines Elementes α_i aus \mathbb{F}_p erhalten, d.h. den Körperturm

$$\mathbb{F}_p \subseteq \mathbb{F}_p[\alpha_1] \subseteq \mathbb{F}_p[\alpha_1, \alpha_2] \subseteq \dots \subseteq K$$

betrachten. Da $f(X)$ separabel ist, sind in diesem Körperturm auch alle Minimalpolynome der α_i separabel, denn sie müssen Teiler von $f(X)$ sein. Somit stellt man mit einer ähnlichen Rechnung wie im Beweis von Satz 5.24 fest, dass $[L : K]_{\text{sep}} = [L : K]$ (denn für einfache Erweiterungen wissen wir ja bereits aus Bemerkung 5.22, dass diese Gleichheit gilt, wenn das Minimalpolynom separabel ist). Folglich ist K/\mathbb{F}_p auch separabel nach Satz 5.24 und damit eine Galoiserweiterung.

- (iii) Zunächst ist der Frobeniushomomorphismus ein (injektiver) Körperhomomorphismus $\text{Frob}: K \rightarrow K$. Er ist aber auch eine \mathbb{F}_p -lineare Abbildung zwischen zwei endlichdimensionalen \mathbb{F}_p -Vektorräumen gleicher Dimension, denn für $a \in \mathbb{F}_p$ und $x \in K$ gilt wegen $\text{Frob}|_{\mathbb{F}_p} = \text{id}_{\mathbb{F}_p}$

$$\text{Frob}(a \cdot x) = \text{Frob}(a) \cdot \text{Frob}(x) = a \cdot \text{Frob}(x).$$

Somit ist er, wie wir aus der linearen Algebra wissen, auch surjektiv und somit ein Körperautomorphismus, also $\text{Frob} \in \text{Gal}(K/\mathbb{F}_p)$. Wir können also die Untergruppe

$$\langle \text{Frob} \rangle = \{\text{id}_K = \text{Frob}^0, \text{Frob}, \text{Frob}^2, \dots\} \subseteq \text{Gal}(K/\mathbb{F}_p)$$

betrachten.

Behauptung: $\text{Gal}(K/\mathbb{F}_p) = \langle \text{Frob} \rangle$.

Nach Korollar 2.54(ii) gilt $\text{ord}(\text{Frob}) \mid \#\text{Gal}(K/\mathbb{F}_p) = [K : \mathbb{F}_p] = k$. Falls $\text{ord}(\text{Frob}) = k$ ist, ist die Aussage gezeigt. Angenommen, $\text{ord}(\text{Frob}) < k$. Dann gäbe es also $j < k$ mit $\text{Frob}^j = \text{id}_K$, also wäre für jedes $x \in K$

$$\text{Frob}^j(x) = x^{p^j} = x.$$

Das würde aber bedeuten, dass jedes Element in K eine Nullstelle des Polynoms $X^{p^j} - X$ ist. Letzteres kann aber aus Gradgründen nur p^j verschiedene Nullstellen haben, während $\#K = p^k > p^j$. Dies ist ein Widerspruch und somit folgt $\text{Gal}(K/\mathbb{F}_p) = \langle \text{Frob} \rangle$.

□

Aus dem obigen Satz erhalten wir direkt eine wichtige Eigenschaft endlicher Körper, die wir in Korollar 5.19 bereits für Körper der Charakteristik 0 gezeigt haben.

Korollar 5.40. *Jeder endliche Körper ist vollkommen.*

Beweis. Sei K ein endlicher Körper und sei L/K eine beliebige algebraische Körpererweiterung. Wir müssen zeigen, dass L/K separabel ist. In anderen Worten: Wir müssen zeigen, dass das Minimalpolynom eines jeden $\alpha \in L$ über K separabel ist. Sei also $\alpha \in L$ beliebig und betrachte die Erweiterung $K[\alpha]/K$. Sei $\overline{\mathbb{F}_p}$ ein algebraischer Abschluss von L (und somit auch von $\mathbb{F}_p \subseteq L$), dann ist $K[\alpha]$ ein endlicher Körper in $\overline{\mathbb{F}_p}$ und somit nach Satz 5.39 die Erweiterung $K[\alpha]/\mathbb{F}_p$ separabel. Folglich ist nach Lemma 5.20 auch $K[\alpha]/K$ separabel, also hat das Minimalpolynom von α über K nur einfache Nullstellen. □

Bemerkung 5.41. Die Aussage von Satz 5.39 besagt, dass es für jedes $q = p^k$ einen eindeutigen Körper mit q Elementen innerhalb eines gewählten algebraischen Abschlusses $\overline{\mathbb{F}_p}$ gibt. Wählt man also verschiedene algebraische Abschlüsse, so erhält man auch erstmal verschiedene Körper mit q Elementen (es macht keinen Sinn zu sagen, dass sie „gleich“ sind, denn sie leben in unterschiedlichen Mengen). Da diese nach Satz 5.39 jedoch alle Zerfällungskörper des Polynoms $f(X) = X^q - X$ sind, sind sie zueinander isomorph, wie in Korollar 4.38 gezeigt. Man kann also sagen: Es gibt *bis auf Isomorphie* einen eindeutigen Körper mit q Elementen.

Im Folgenden arbeiten wir weiterhin in einem vorgegebenen algebraischen Abschluss $\overline{\mathbb{F}_p}$, sodass wir uns über das „bis auf Isomorphie“ keine Gedanken machen müssen.

Für den Rest dieses Abschnitts sei p eine fest gewählte Primzahl und $\overline{\mathbb{F}_p}$ ein fest gewählter algebraischer Abschluss von \mathbb{F}_p .

Definition 5.42. Ist $q = p^k$ für ein $k \in \mathbb{N}$, so bezeichnen wir den eindeutigen Körper mit q Elementen in $\overline{\mathbb{F}_p}$ (welcher nach Satz 5.39 existiert) mit $\mathbb{F}_q = \mathbb{F}_{p^k}$.

Bemerkung 5.43. Achtung: Für eine Primzahl war $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$. Die Notation \mathbb{F}_q bezeichnet aber allgemeiner den (eindeutigen) **Körper** mit q Elementen. Wenn q also keine Primzahl ist, so gilt **nicht (!)** $\mathbb{F}_q = \mathbb{Z}/q\mathbb{Z}$, denn das wäre kein Körper! Stattdessen ist \mathbb{F}_q eine Erweiterung von \mathbb{F}_p .

Ist beispielsweise $p = 2$ und $q = 4 = 2^2$, so ist

$$\mathbb{F}_4 \cong \mathbb{F}_2[X]/(X^2 + X + 1),$$

Kapitel 5 Galoistheorie

also $\mathbb{F}_4 = \mathbb{F}_2[\alpha]$, wobei α ein Element mit Minimalpolynom $X^2 + X + 1$ ist (letzteres ist irreduzibel in $\mathbb{F}_2[X]$).

Wir beweisen nun den Satz vom primitiven Element für endliche Körper. Dazu brauchen wir als Vorbereitung den folgenden Satz, der besagt, dass die Einheiten eines endlichen Körpers eine zyklische Gruppe bilden. Der Satz ist hier noch etwas allgemeiner formuliert, weil wir ihn später noch einmal in einem anderen Zusammenhang verwenden werden.

Satz 5.44. *Ist K ein Körper und $H \subseteq K^\times$ eine endliche Untergruppe seiner (multiplikativen) Einheitengruppe. Dann ist H zyklisch.*

Beweis. Wir beweisen zunächst eine Hilfsaussage.

Hilfsbehauptung: Ist G eine abelsche Gruppe und sind $a, b \in G$ Elemente mit $\text{ggT}(\text{ord}(a), \text{ord}(b)) = 1$, so gilt $\text{ord}(ab) = \text{ord}(a) \cdot \text{ord}(b)$.

Es bezeichne $e \in G$ das neutrale Element. Wir verwenden im Folgenden wiederholt ein einfaches Argument, welches wir aus den Übungen (Blatt 2, Aufgabe 3) kennen: Ist $g \in G$ und gilt $g^n = e$ für ein $n \in \mathbb{N}$, so gilt $\text{ord}(g) \mid n$.

Damit also zum Beweis der Hilfsaussage: Es ist

$$(ab)^{\text{ord}(a) \cdot \text{ord}(b)} = \underbrace{(a^{\text{ord}(a)})^{\text{ord}(b)}}_{=e} \cdot \underbrace{(b^{\text{ord}(b)})^{\text{ord}(a)}}_{=e} = e,$$

also $\text{ord}(ab) \mid \text{ord}(a) \cdot \text{ord}(b)$.

Andererseits gilt: Schreiben wir $k = \text{ord}(ab)$, dann ist $e = (ab)^k = a^k b^k$. Durch Umformung erhalten wir $a^k = b^{-k}$. Wir wissen, dass $\text{ord}(a^k) \mid \text{ord}(a)$ und mit der gerade gesehenen Gleichheit gilt auch $\text{ord}(a^k) = \text{ord}(b^{-k}) = \text{ord}(b^k) \mid \text{ord}(b)$. Nach Voraussetzung sind $\text{ord}(a)$ und $\text{ord}(b)$ teilerfremd, also folgt $\text{ord}(a^k) = 1$ und somit $a^k = e$ und $b^k = a^{-k} = e$. Also muss gelten $\text{ord}(a) \mid k$ und $\text{ord}(b) \mid k$ und folglich $\text{ord}(a) \cdot \text{ord}(b) \mid k = \text{ord}(ab)$, da $\text{ord}(a)$ und $\text{ord}(b)$ teilerfremd sind.

Sei nun $H \subseteq K^\times$ eine endliche Untergruppe und wähle ein Element $g \in H$ mit maximaler Ordnung. (Ein solches gibt es – wenn auch eventuell nicht eindeutig –, da H nur endlich viele Elemente hat.) Wir wollen zeigen, dass $H = \langle g \rangle$ gilt. Da wir wissen, dass $\langle g \rangle \subseteq H$ eine Untergruppe ist, reicht es zu zeigen, dass $\#\langle g \rangle \geq \#H$.

Behauptung: Ist $x \in H$ ein beliebiges Element, so gilt $\text{ord}(x) \mid \text{ord}(g)$.

Wir nehmen an, dies wäre nicht der Fall. Dann gibt es also ein $x \in H$ mit $\text{ord}(x) \nmid \text{ord}(g)$. Es ist dann also sicher $\text{ord}(x) > 1$.

Wir schreiben $d := \text{ggT}(\text{ord}(x), \text{ord}(g))$. Dann können wir die Ordnung von x zerlegen als $\text{ord}(x) = d \cdot m$, wobei dann gilt $\text{ggT}(m, \text{ord}(g)) = 1$ und $m > 1$ (denn wir haben ja angenommen, dass $\text{ord}(x)$ kein Teiler von $\text{ord}(g)$ ist, also

kann nicht $\text{ord}(x) = d$ gelten.) Es gilt dann $\text{ord}(x^d) = m$ und somit nach obiger Hilfsbehauptung

$$\text{ord}(x^d g) = \text{ord}(x^d) \cdot \text{ord}(g) = m \text{ord}(g) > \text{ord}(g),$$

was nicht möglich ist, da $x^d g \in H$, aber g als ein Element mit maximaler Ordnung gewählt wurde. Widerspruch.

Wir schreiben nun $n := \text{ord}(g)$. Nach obiger Behauptung gilt also $x^n = 1$ für alle $x \in H$. Da $H \subseteq K^\times$ und das Polynom $X^n - 1$ im Körper K nur höchstens n verschiedene Nullstellen haben kann, gilt $\#H \leq n = \text{ord}(g) = \#\langle g \rangle$, wie gewünscht. Somit ist $H = \langle g \rangle$ und daher H zyklisch. \square

Satz 5.45 (Satz vom primitiven Element (für endliche Körper)). *Sei K ein endlicher Körper. Ist L/K eine endliche Körpererweiterung (die dann nach Korollar 5.40 auch separabel ist), so gibt es ein primitives Element für L/K . In anderen Worten: Dann existiert ein $\gamma \in L$, sodass $L = K[\gamma]$.*

Beweis. Der Körper L ist eine endliche Erweiterung von K , also selbst ein endlicher Körper. Nach Satz 5.44 ist die Einheitengruppe L^\times dann zyklisch. Wir können also ein $\gamma \in L^\times$ finden, sodass jedes andere $x \in L^\times$ sich in der Form $x = \gamma^k$ für ein $k \in \mathbb{Z}$ schreibt. Damit gilt natürlich $K[\gamma] \subseteq L$, denn L enthält sowohl K als auch γ , aber auch $L \subseteq K[\gamma]$, denn jedes Element in L ist entweder 0 oder eine Potenz von γ . \square

Damit ist der Hauptsatz der Galoistheorie nun auch für endliche Körper vollständig bewiesen.

Zu guter Letzt wollen wir uns noch überlegen, wie verschiedene endliche Körper (die wir nach Satz 5.39 nun alle kennen) miteinander zusammenhängen. Tatsächlich können wir die Relationen zwischen endlichen Körper (in einem fest gegebenen algebraischen Abschluss $\overline{\mathbb{F}_p}$) sehr genau beschreiben.

Lemma 5.46. *Man hat eine Inklusion $\mathbb{F}_{p^k} \subseteq \mathbb{F}_{p^\ell}$ genau dann, wenn $k \mid \ell$.*

Beweis. Zu zeigen ist, dass ein endlicher Körper \mathbb{F}_{p^ℓ} den endlichen Körper \mathbb{F}_{p^k} genau dann enthält, wenn k ein Teiler von ℓ ist. In anderen Worten: Die Zwischenkörper von $\mathbb{F}_{p^\ell}/\mathbb{F}_p$ sind genau die \mathbb{F}_{p^k} für $k \mid \ell$. Um dies zu beweisen, wenden wir den Hauptsatz der Galoistheorie an. (Dies dürfen wir, da $\mathbb{F}_{p^\ell}/\mathbb{F}_p$ nach Satz 5.39 eine endliche Galoiserweiterung ist.)

Die Galoisgruppe von $\mathbb{F}_{p^\ell}/\mathbb{F}_p$ ist nach Satz 5.39

$$\text{Gal}(\mathbb{F}_{p^\ell}/\mathbb{F}_p) = \langle \text{Frob} \rangle = \{\text{id}_{\mathbb{F}_{p^\ell}}, \text{Frob}, \text{Frob}^2, \dots, \text{Frob}^{\ell-1}\},$$

wobei $\text{Frob}: \mathbb{F}_{p^\ell} \rightarrow \mathbb{F}_{p^\ell}, x \mapsto x^p$ der Frobeniushomomorphismus ist. Wenn wir also alle Zwischenkörper von $\mathbb{F}_{p^\ell}/\mathbb{F}_p$ finden möchten, können wir nach dem Hauptsatz der Galoistheorie auch alle Untergruppen von $\text{Gal}(\mathbb{F}_{p^\ell}/\mathbb{F}_p)$ bestimmen und davon die Fixkörper berechnen.

Kapitel 5 Galoistheorie

Die zyklische Gruppe $\langle \text{Frob} \rangle$ hat für jede natürliche Zahl d mit $d \mid \ell$ (und nur für solche) eine Untergruppe mit d Elementen.

(Diese ist sogar eindeutig und wir können sie explizit hinschreiben: Ist $\ell = d \cdot k$, so ist $H_d = \langle \text{Frob}^k \rangle$ die eindeutige Untergruppe von $\langle \text{Frob} \rangle$ mit d Elementen.)

Ist $H_d \subseteq \text{Gal}(\mathbb{F}_{p^\ell}/\mathbb{F}_p)$ eine Untergruppe mit d Elementen und $M := \mathbb{F}_{p^\ell}^{H_d}$ der zugehörige Fixkörper, so gilt nach dem Hauptsatz der Galoistheorie

$$\text{Gal}(\mathbb{F}_{p^\ell}/M) = \text{Gal}(\mathbb{F}_{p^\ell}/\mathbb{F}_{p^\ell}^{H_d}) = H_d$$

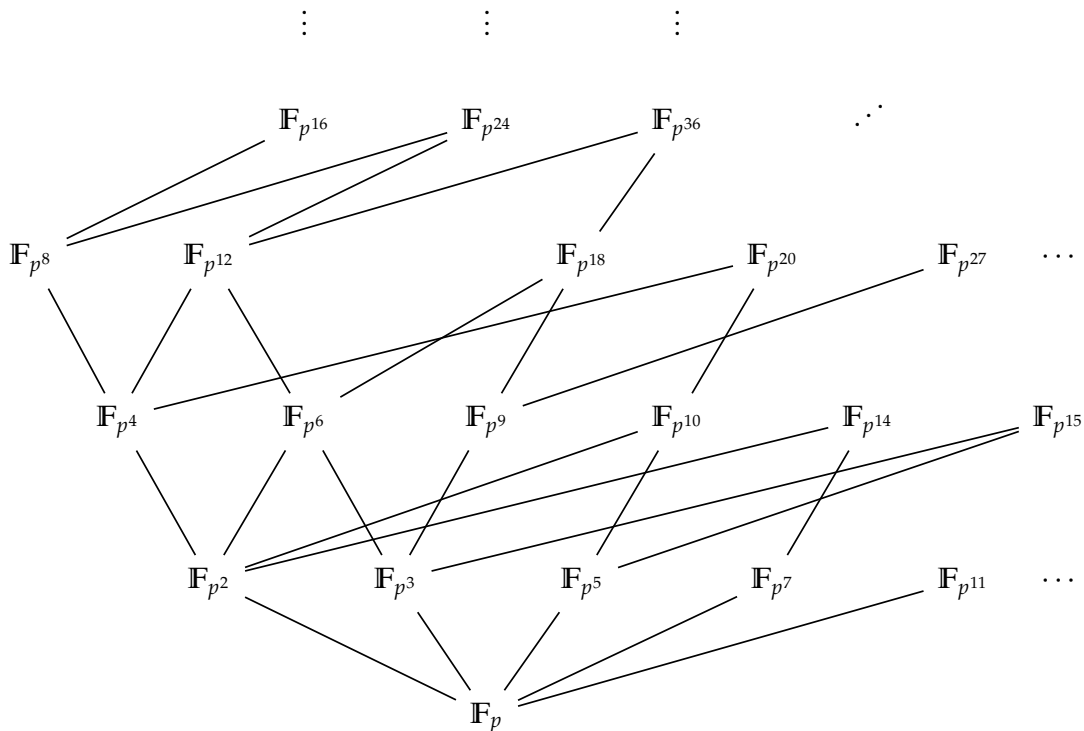
und aus Punkt (ii) im Hauptsatz der Galoistheorie folgt

$$[M : \mathbb{F}_p] = (\text{Gal}(\mathbb{F}_{p^\ell}/\mathbb{F}_p) : \text{Gal}(\mathbb{F}_{p^\ell}/M)) = (\text{Gal}(\mathbb{F}_{p^\ell}/\mathbb{F}_p) : H_d) = \frac{\#\text{Gal}(\mathbb{F}_{p^\ell}/\mathbb{F}_p)}{\#H_d} = \frac{\ell}{d}.$$

Somit ist M eine Erweiterung vom Grad $k := \frac{\ell}{d}$ über \mathbb{F}_p und somit nach Satz 5.39 gleich dem Körper \mathbb{F}_{p^k} .

Durchläuft d alle möglichen Teiler von ℓ , so durchläuft auch $k = \frac{\ell}{d}$ alle möglichen Teiler von ℓ und damit ist das Lemma gezeigt. \square

Man kann sich also das folgende Diagramm aller endlichen Körpererweiterungen von \mathbb{F}_p (für ein festgelegtes p) auszeichnen. Es zeigt die Körpererweiterungen von \mathbb{F}_p , also die endlichen Körper mit p^k Elementen für $k \in \mathbb{N}$ (in einem festgelegten algebraischen Abschluss). Sind zwei Körper (eventuell auch über einen längeren Pfad) verbunden, bedeutet dies, dass der kleinere im größeren enthalten ist, dass es sich also um eine Körpererweiterung handelt.



5.7 Kreisteilungskörper

In diesem Abschnitt sehen wir uns noch weitere wichtige Beispiele für Körpererweiterungen an, nämlich solche, die durch Adjunktion von Einheitswurzeln entstehen. Dazu zunächst eine Definition dieses Begriffs.

Lemma-Definition 5.47. Sei Ω ein Körper und $n \in \mathbb{N}$.

Eine Nullstelle in Ω des Polynoms $\Phi_n(X) = X^n - 1 \in \Omega[X]$ heißt *n-te Einheitswurzel*. Die Menge der *n*-ten Einheitswurzeln bezeichnen wir mit

$$\mu_n(\Omega) := \{\zeta \in \Omega \mid \zeta^n = 1\} \subseteq \Omega^\times.$$

Sie ist eine zyklische Untergruppe der multiplikativen Gruppe (Ω^\times, \cdot) der Einheiten von Ω .

Kapitel 5 Galoistheorie

Ein Element $\zeta \in \mu_n(\Omega)$ mit $\text{ord}(\zeta) = n$ heißt *primitive n -te Einheitswurzel*. Eine solche existiert also genau dann, wenn $\#\mu_n(\Omega) = n$.

Beweis. Zunächst bilden die Einheitswurzeln eine Teilmenge der Einheiten von Ω , denn offensichtlich ist das Element $0 \in \Omega$ keine n -te Einheitswurzel. Es ist weiter $\mu_n(\Omega) \subseteq \Omega^\times$ eine Untergruppe, denn:

(1) $1 \in \mu_n(\Omega)$, da $1^n = 1$.

(2) Sind $\zeta_1, \zeta_2 \in \mu_n(\Omega)$, d.h. $\zeta_1^n = \zeta_2^n = 1$, dann folgt

$$(\zeta_1 \zeta_2)^n = \zeta_1^n \zeta_2^n = 1 \cdot 1 = 1,$$

also $\zeta_1 \zeta_2 \in \mu_n(\Omega)$.

(3) Ist $\zeta \in \mu_n(\Omega)$, d.h. $\zeta^n = 1$, dann gilt

$$(\zeta^{-1})^n = (\zeta^n)^{-1} = 1^{-1} = 1,$$

also $\zeta^{-1} \in \mu_n(\Omega)$.

Da das Polynom $X^n - 1$ nur höchstens n Nullstellen haben kann, ist $\mu_n(\Omega)$ endlich und somit nach Satz 5.44 eine zyklische Gruppe. Ein Erzeuger dieser zyklischen Gruppe hat die Ordnung n , wenn $\#\mu_n(\Omega) = n$ und ist in diesem Fall also eine primitive n -te Einheitswurzel. Ist hingegen $\#\mu_n(\Omega) < n$, so kann es kein Element der Ordnung n und somit keine primitive n -te Einheitswurzel in Ω geben. \square

Wir haben in dieser Definition den Körper Ω genannt, weil wir meistens in algebraisch abgeschlossenen Körpern nach Einheitswurzeln suchen werden. Prinzipiell kann Ω aber hier erst einmal ein beliebiger Körper sein.

Beispiel 5.48. Ist $\Omega = \mathbb{C}$, so sind die Elemente $e^{\frac{2\pi i}{n} \cdot k} \in \mathbb{C}$ für $k \in \mathbb{Z}$ die n -ten Einheitswurzeln. Tatsächlich reicht es, die Indizes $k \in \{0, \dots, n-1\}$ zu betrachten, denn für alle anderen Werte von k wiederholen sich die Einheitswurzeln (beachte $e^0 = e^{2\pi i} = 1$). Schreiben wir also $\zeta = e^{\frac{2\pi i}{n}}$, so gilt

$$\mu_n(\mathbb{C}) = \{1, \zeta, \zeta^2, \dots, \zeta^{n-1}\} = \langle \zeta \rangle.$$

Das Element $\zeta = e^{\frac{2\pi i}{n}}$ ist also eine primitive n -te Einheitswurzel. Es kann aber auch noch andere geben:

Wenn $\text{ord}(\zeta) = n$ gilt, so ist $\text{ord}(\zeta^k) = n$ genau dann, wenn $\text{ggT}(k, n) = 1$. (Dies überlegt man sich leicht, wurde aber auch in den Übungen bereits bewiesen, siehe Blatt 2, Aufgabe 3.)

Beispielsweise sind also im Fall $n = 8$ die komplexen Einheitswurzeln

$$e^{\frac{2\pi i}{8}}, e^{\frac{6\pi i}{8}}, e^{\frac{10\pi i}{8}}, e^{\frac{14\pi i}{8}} \in \mu_n(\mathbb{C})$$

die primitiven Einheitswurzeln. Jede davon könnte also als Erzeuger ζ verwendet werden.

Falls Ω ein anderer Körper als \mathbb{C} ist, aber es immer noch n verschiedene Einheitswurzeln gibt, geht alles genauso: Ist $\zeta \in \mu_n(\Omega)$ primitiv, so auch ζ^k für jedes k mit $\text{ggT}(k, n) = 1$. Es gibt also genauso viele primitive n -te Einheitswurzeln wie es teilerfremde Elemente zu n zwischen 1 und $n - 1$ gibt. Diese Zahl ist uns vielleicht schon einmal begegnet: Diese zu n teilerfremden Elemente sind auch genau die Einheiten in $\mathbb{Z}/n\mathbb{Z}$. Da diese Zahl öfter vorkommt, gibt es für sie eine spezielle Notation.

Definition 5.49. Die Abbildung

$$\varphi: \mathbb{N} \rightarrow \mathbb{N}, \quad n \mapsto \varphi(n) := \#(\mathbb{Z}/n\mathbb{Z})^\times = \#\{j \in \{1, \dots, n-1\} \mid \text{ggT}(j, n) = 1\}$$

heißt *Eulersche φ -Funktion*.

Lemma 5.50. Die Eulersche φ -Funktion hat die folgende Eigenschaft: Für zwei teilerfremde Zahlen $m, n \in \mathbb{N}$ gilt $\varphi(m \cdot n) = \varphi(m) \cdot \varphi(n)$.

Beweis. Nach dem Chinesischen Restsatz (Satz 3.59) haben wir für teilerfremde $m, n \in \mathbb{N}$ einen Ringisomorphismus

$$\mathbb{Z}/(mn)\mathbb{Z} \cong \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}.$$

Da ein solcher Einheiten auf Einheiten abbildet, erhalten wir daraus einen Gruppenisomorphismus

$$(\mathbb{Z}/(mn)\mathbb{Z})^\times \cong (\mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z})^\times.$$

Nun ist die Multiplikation im Ring $\mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$ komponentenweise definiert und daher ist ein Element $([a], [b]) \in \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$ genau dann invertierbar, wenn sowohl $[a] \in \mathbb{Z}/m\mathbb{Z}$ als auch $[b] \in \mathbb{Z}/n\mathbb{Z}$ invertierbar sind, denn nur dann gibt es $([c], [d]) \in \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$, sodass $([a], [b]) \cdot ([c], [d]) = ([1], [1])$ das neutrale Element der Multiplikation ergibt. Dies bedeutet, dass

$$(\mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z})^\times = (\mathbb{Z}/m\mathbb{Z})^\times \times (\mathbb{Z}/n\mathbb{Z})^\times$$

und somit ist

$$\begin{aligned} \varphi(mn) &= \#(\mathbb{Z}/(mn)\mathbb{Z})^\times = \#((\mathbb{Z}/m\mathbb{Z})^\times \times (\mathbb{Z}/n\mathbb{Z})^\times) = \#(\mathbb{Z}/m\mathbb{Z})^\times \cdot \#(\mathbb{Z}/n\mathbb{Z})^\times \\ &= \varphi(m) \cdot \varphi(n). \end{aligned}$$

□

Wir wollen jetzt Körpererweiterungen studieren, die durch Adjunktion von Einheitswurzeln entstehen.

Definition 5.51. Sei K ein Körper, Ω ein algebraisch abgeschlossener Körper mit $K \subseteq \Omega$ und $n \in \mathbb{N}$. Sei Z_n der Zerfällungskörper des Polynoms $X^n - 1 \in K[X]$ in Ω . Dann nennen wir Z_n den n -ten *Kreisteilungskörper* zu K (in Ω).

Wie bereits bei den endlichen Körpern setzt diese Definition die Wahl eines algebraischen Abschlusses voraus. Wir gehen also im Folgenden immer davon aus, dass wir in einem fest gewählten algebraisch abgeschlossenen größeren Körper arbeiten. Für den Fall $K = \mathbb{Q}$ werden das dann natürlich die komplexen Zahlen \mathbb{C} sein.

Satz 5.52. *Sei K ein Körper und $n \in \mathbb{N}$ mit $\text{char}(K) \nmid n$. Sei Ω ein algebraischer Abschluss von K und Z_n der n -te Kreisteilungskörper (zu K in Ω). Dann gilt*

- (i) $\mu_n(Z_n)$ ist eine zyklische Gruppe der Ordnung n . Es gibt also eine primitive n -te Einheitswurzel in Z_n .
- (ii) Ist $\zeta \in \mu_n(Z_n)$ eine primitive Einheitswurzel, so gilt $Z_n = K[\zeta]$.
- (iii) Z_n/K ist eine Galoiserweiterung.

Beweis. (i) Die formale Ableitung des Polynoms $f(X) = X^n - 1$ ist $f'(X) = nX^{n-1}$, welches wegen $\text{char}(K) \nmid n$ nicht das Nullpolynom ist und offensichtlich auch keine gemeinsamen Nullstellen mit $f(X)$ hat. Somit ist $f(X)$ separabel (siehe Lemma 5.13). Es gibt also n paarweise verschiedene Nullstellen und dies bedeutet nichts anderes als $\#\mu_n(Z_n) = n$. Folglich gibt es, da $\mu_n(Z_n)$ zyklisch ist, (mindestens) eine primitive n -te Einheitswurzel, denn jeder Erzeuger ist eine solche.

- (ii) Ist ζ eine primitive n -te Einheitswurzel, so gilt $\mu_n(Z_n) = \{1, \zeta, \zeta^2, \dots, \zeta^{n-1}\}$, also ist $Z_n = K[1, \zeta, \zeta^2, \dots, \zeta^{n-1}] = K[\zeta]$.
- (iii) Nach Definition ist Z_n ein Zerfällungskörper, also Z_n/K normal. Außerdem ist Z_n eine einfache Erweiterung von K und das Minimalpolynom von ζ ist separabel (denn es muss ein Teiler des separablen Polynoms $X^n - 1$ sein). Somit gilt nach Bemerkung 5.22 bereits $[Z_n : K]_{\text{sep}} = [Z_n : K]$ und daher ist Z_n/K separabel nach Satz 5.24.

□

Bemerkung 5.53. Die Voraussetzung $\text{char}(K) \nmid n$ ist tatsächlich wichtig: Ist zum Beispiel $K = \mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$ und betrachten wir das Polynom $X^p - 1$ (das ist also der Fall $\text{char}(K) = p = n$), so gilt $X^p - 1 = (X - 1)^p$. Das Polynom ist also nicht separabel, sondern hat in diesem Fall sogar p -mal dieselbe Nullstelle. Es gibt also hier nicht p verschiedene p -te Einheitswurzeln und somit auch keine primitive, die Schlussfolgerung des obigen Satzes ist daher für diese Situation falsch.

Ein Kreisteilungskörper ist also meist von der Form $Z_n = K[\zeta]$ für eine primitive Einheitswurzel $\zeta \in \mu_n(Z_n)$. Um seine Eigenschaften besser zu verstehen, also beispielsweise den Körpergrad $[K[\zeta] : K]$ und die Galoisgruppe $\text{Gal}(K[\zeta]/K)$, müssen wir das Minimalpolynom von ζ über K kennen. Die erste (naive) Idee wäre, zu denken, dass dieses Minimalpolynom $X^n - 1$ ist. Das ist natürlich hochgradig falsch, denn dieses Polynom hat die Nullstelle 1, ist also sicher nicht irreduzibel!

Aber selbst das Polynom $\frac{X^n-1}{X-1}$, welches alle n -ten Einheitswurzeln außer der 1 als Nullstellen hat, ist im Allgemeinen nicht das Minimalpolynom. Für den Fall $K = \mathbb{Q}$ werden wir gleich sehen, dass das Minimalpolynom dasjenige Polynom ist, welches nur die *primitiven* n -ten Einheitswurzeln als Nullstellen hat. Dieses bekommt einen besonderen Namen.

Definition 5.54. Sei $n \in \mathbb{N}$. Seien $\zeta_1, \dots, \zeta_{\varphi(n)} \in \mu_n(\mathbb{Z}_n)$ die primitiven n -ten Einheitswurzeln. Dann heißt das Polynom

$$\Phi_n(X) = \prod_{i=1}^{\varphi(n)} (X - \zeta_i) \in \mathbb{Z}_n[X]$$

das n -te *Kreisteilungspolynom* über K .

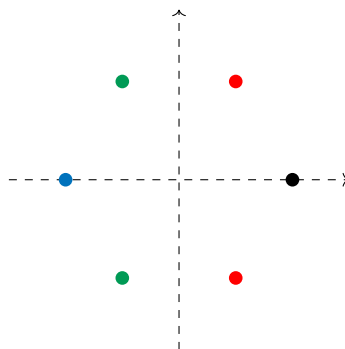
Lemma 5.55. Sei K ein Körper und $n \in \mathbb{N}$ mit $\text{char}(K) \nmid n$, dann gilt

$$X^n - 1 = \prod_{d \in \mathbb{N}, d|n} \Phi_d(X),$$

d.h. das Polynom $X^n - 1$ ist das Produkt aller Kreisteilungspolynome $\Phi_d(X)$ für alle natürlichen Teiler d von n . (Beachte, dass dies auch $d = 1$ und $d = n$ einschließt.)

Beweis. Wie in Satz 5.52 gezeigt, besitzt $X^n - 1$ paarweise verschiedene Nullstellen. Für jede solche Nullstelle ζ gilt $\text{ord}(\zeta) \mid \#\mu_n(\mathbb{Z}_n) = n$, also ist ζ eine primitive d -te Einheitswurzel für $d = \text{ord}(\zeta)$, also eine Nullstelle von $\Phi_d(X)$ für ein passendes d mit $d \mid n$. Also zerlegt sich $X^n - 1$ wie behauptet. \square

Beispiel 5.56. Machen wir uns die Zerlegung aus Lemma 5.55 kurz am Beispiel $K = \mathbb{C}$ und $n = 6$ klar: Es gibt 6 Einheitswurzeln, die im folgenden Bild veranschaulicht sind:



Jede dieser sechsten Einheitswurzeln ist eine primitive d -te Einheitswurzel für ein bestimmtes (und genau ein) d mit $d \mid 6$. Man kann dann die zugehörigen Kreisteilungspolynome für jedes solche d bestimmen, zum Beispiel, indem man die zugehörigen Linearfaktoren multipliziert. Die folgende Tabelle zeigt all diese Polynome sowie die zugehörigen Nullstellen.

Kapitel 5 Galoistheorie

d	Kreisteilungspolynom	primitive d -te Einheitswurzeln
1	$\Phi_1(X) = X - 1$	1
2	$\Phi_2(X) = X + 1$	-1
3	$\Phi_3(X) = X^2 + X + 1$	$e^{\frac{4\pi i}{6}} = -\frac{1}{2} + \frac{1}{2}\sqrt{3}i, e^{\frac{8\pi i}{6}} = -\frac{1}{2} - \frac{1}{2}\sqrt{3}i$
6	$\Phi_6(X) = X^2 - X + 1$	$e^{\frac{2\pi i}{6}} = \frac{1}{2} + \frac{1}{2}\sqrt{3}i, e^{\frac{10\pi i}{6}} = \frac{1}{2} - \frac{1}{2}\sqrt{3}i$

Damit ist die Zerlegung $X^6 - 1 = \Phi_1(X) \cdot \Phi_2(X) \cdot \Phi_3(X) \cdot \Phi_6(X)$ in diesem Beispiel verstanden.

Wenn nun $\Phi_n(X)$ ein Kandidat für das Minimalpolynom einer primitiven Einheitswurzel ζ über K sein soll, muss es auf jeden Fall Koeffizienten in K haben – nach Definition liegt es ja zunächst in $Z_n[X]$. Dies ist auch tatsächlich der Fall.

Lemma 5.57. *Sei K ein Körper und $n \in \mathbb{N}$ eine natürliche Zahl mit $\text{char}(K) \nmid n$. Dann gilt $\Phi_n(X) \in K[X]$.*

Beweis. Betrachte die Galoisgruppe $\text{Gal}(Z_n/K)$. Ist $\sigma \in \text{Gal}(Z_n/K)$ und ist ζ eine primitive n -te Einheitswurzel, so ist $\sigma(\zeta)$ wieder eine Nullstelle von $X^n - 1$ (da $\sigma|_K = \text{id}_K$) und außerdem gilt $\text{ord}(\sigma(\zeta)) = \text{ord}(\zeta)$, da σ ein Isomorphismus ist. Also ist $\sigma(\zeta)$ wieder eine primitive n -te Einheitswurzel. Die Abbildung σ induziert also eine bijektive Abbildung von der Menge $\{\zeta_1, \dots, \zeta_{\varphi(n)}\}$ der primitiven n -ten Einheitswurzeln in Z_n auf sich selbst (also eine Permutation dieser primitiven Einheitswurzeln). Daher gilt für jedes $\sigma \in \text{Gal}(Z_n/K)$

$$\Phi_n^\sigma(X) = \prod_{i=1}^{\varphi(n)} (X - \sigma(\zeta_i)) = \prod_{i=1}^{\varphi(n)} (X - \zeta_i) = \Phi_n(X).$$

In anderen Worten: Das Polynom $\Phi_n(X)$ und somit alle seine Koeffizienten bleiben invariant unter allen $\sigma \in \text{Gal}(Z_n/K)$, das Polynom $\Phi_n(X)$ hat also Koeffizienten in $Z_n^{\text{Gal}(Z_n/K)}$ und nach dem Hauptsatz der Galoistheorie ist dies der Körper K . \square

Korollar 5.58. *In der Situation von Satz 5.52 gilt: $[Z_n : K] \leq \varphi(n)$.*

Beweis. Wir haben in Satz 5.52 bereits gezeigt, dass $Z_n = K[\zeta]$ für eine primitive n -te Einheitswurzel ζ . Daher gilt $[Z_n : K] = \deg(p)$, wobei $p(X) \in K[X]$ das Minimalpolynom von ζ über K ist. Nach Lemma 5.57 ist $\Phi_n(X) \in K[X]$ ein Polynom, welches ζ als Nullstelle hat. Somit muss gelten $p(X) \mid \Phi_n(X)$ und daher $\deg(p) \leq \deg(\Phi_n) = \varphi(n)$. \square

Wir spezialisieren jetzt auf den Fall $K = \mathbb{Q}$ und zeigen, dass dort wirklich Gleichheit im letzten Korollar gilt, dass also $\Phi_n(X)$ das Minimalpolynom der primitiven Einheitswurzeln ist und sogar ganzzahlige Koeffizienten hat.

Satz 5.59. *Sei $n \in \mathbb{N}$ und sei $\Phi_n(X) \in \mathbb{Q}[X]$ das n -te Kreisteilungspolynom über \mathbb{Q} . Dann gilt $\Phi_n(X) \in \mathbb{Z}[X]$ und $\Phi_n(X)$ ist irreduzibel in $\mathbb{Q}[X]$ und in $\mathbb{Z}[X]$. Insbesondere ist $\Phi_n(X)$ das Minimalpolynom einer beliebigen primitiven n -ten Einheitswurzel in \mathbb{C} über \mathbb{Q} .*

Beweis. Wir zeigen zunächst induktiv, dass $\Phi_n(X)$ ganzzahlige Koeffizienten hat.

Induktionsanfang: Für $n = 1$ ist offensichtlich $\Phi_1(X) = X - 1 \in \mathbb{Z}[X]$.

Induktionsvoraussetzung: Für ein beliebiges, aber festes $n \in \mathbb{N}$ sei bereits bekannt, dass $\Phi_k(X) \in \mathbb{Z}[X]$ für alle $k \in \mathbb{N}$ mit $k \leq n - 1$.

Induktionsschritt: Es ist nun zu zeigen, dass $\Phi_n(X) \in \mathbb{Z}[X]$. Wir wissen nach Lemma 5.55, dass

$$X^n - 1 = \Phi_n(X) \cdot \prod_{d \in \mathbb{N}, d|n, d \neq n} \Phi_d(X).$$

Es ist offensichtlich $X^n - 1 \in \mathbb{Z}[X]$ und nach Induktionsvoraussetzung auch $\prod_{d \in \mathbb{N}, d|n, d \neq n} \Phi_d(X) \in \mathbb{Z}[X]$. Außerdem ist letzteres Polynom primitiv (sein Leitkoeffizient ist 1) und daher folgt mit Satz 3.80, dass $\Phi_n(X) \in \mathbb{Z}[X]$.

Sei nun $\zeta \in \mathbb{C}$ eine fest gewählte primitive n -te Einheitswurzel und sei $p(X) \in \mathbb{Q}[X]$ ihr Minimalpolynom über \mathbb{Q} . Da ζ eine Nullstelle von $\Phi_n(X)$ ist, gilt sicher $p(X) \mid \Phi_n(X)$. Um zu zeigen, dass beide Polynome gleich sind, müssen wir zeigen, dass jede primitive n -te Einheitswurzel eine Nullstelle von $p(X)$ ist. Jede primitive n -te Einheitswurzel lässt sich schreiben als ζ^m für ein $m \in \mathbb{N}$ mit $\text{ggT}(m, n) = 1$. Wir zeigen zunächst einen einfachen Fall.

Behauptung: Ist $p \in \mathbb{N}$ eine Primzahl mit $p \nmid n$ und ζ eine primitive n -te Einheitswurzel mit Minimalpolynom $p(X)$ über \mathbb{Q} , so gilt $p(\zeta^p) = 0$.

Wir schreiben $X^n - 1 = p(X) \cdot g(X)$ für ein $g(X) \in \mathbb{Q}[X]$. Vergewissern wir uns und zunächst, dass alle Polynome in dieser Gleichung in Wirklichkeit ganzzahlig sind: Sei $c \in \mathbb{Z}$ ein Hauptnenner aller Koeffizienten von $g(X)$, sodass also $c \cdot g(X) \in \mathbb{Z}[X]$ ein primitives Polynom ist. Dann ist also

$$\underbrace{X^n - 1}_{\in \mathbb{Z}[X]} = \frac{1}{c} \cdot p(X) \cdot \underbrace{c \cdot g(X)}_{\in \mathbb{Z}[X], \text{primitiv}},$$

also nach Satz 3.80 auch $\frac{1}{c} \cdot p(X) \in \mathbb{Z}[X]$ und daher $p(X) \in \mathbb{Z}[X]$. Mit demselben Argument folgt dann aus

$$\underbrace{X^n - 1}_{\in \mathbb{Z}[X]} = \underbrace{p(X)}_{\in \mathbb{Z}[X]} \cdot g(X)$$

auch $g(X) \in \mathbb{Z}[X]$, denn $p(X)$ ist als Minimalpolynom normiert und somit primitiv.

Nehmen wir nun an, ζ^p wäre keine Nullstelle von $p(X)$. Da aber ζ^p eine Nullstelle von $X^n - 1$ ist, müsste dann gelten $g(\zeta^p) = 0$. Dann wäre ζ also eine Nullstelle des Polynoms $h(X) := g(X^p)$. Also würde wieder folgen $p(X) \mid h(X)$,

also $h(X) = p(X) \cdot q(X)$ für ein $q(X) \in \mathbb{Q}[X]$, für welches mit demselben Argument wie oben wieder $q(X) \in \mathbb{Z}[X]$ gilt. Wenden wir Reduktion modulo p an (siehe Lemma-Definition 3.78), so erhalten wir

$$\bar{p}(X) \cdot \bar{q}(X) = \bar{h}(X) = \bar{g}(X^p) = (\bar{g}(X))^p.$$

Hierbei haben wir im letzten Schritt verwendet, dass sich diese Rechnung im Polynomring $\mathbb{F}_p[X]$ abspielt: Dieser hat die Charakteristik p und somit ist Potenzieren mit p ein Ringhomomorphismus, der die Koeffizienten in \mathbb{F}_p unverändert lässt (ähnlich wie in Lemma-Definition 5.37).

Somit müsste gelten $\text{ggT}(\bar{p}(X), \bar{g}(X)) \neq 1$ und daher hätte das Polynom $X^n - 1 = \bar{p}(X) \cdot \bar{g}(X)$ mehrfache Nullstellen in $\bar{\mathbb{F}}_p$, wäre also nicht separabel. Wegen unserer Voraussetzung $\text{char}(\mathbb{F}_p) = p \nmid n$ ist das aber ein Widerspruch, denn wir haben im Beweis von Satz 5.52 gezeigt, dass $X^n - 1 \in \mathbb{F}_p[X]$ separabel ist. Folglich ist ζ^p eine Nullstelle von $p(X)$.

Ist nun ζ eine primitive n -te Einheitswurzel mit Minimalpolynom $p(X)$ und ζ^m für ein $m \in \mathbb{N}$ mit $\text{ggT}(m, n) = 1$ eine beliebige andere primitive n -te Einheitswurzel, so können wir die eben gezeigte Behauptung mehrmals anwenden: Sei $m = p_1 \cdot \dots \cdot p_k$ die Primfaktorzerlegung von m , dann gilt für jeden Primfaktor $p_i \nmid n$. Dann ist also nach der Behauptung ζ^{p_1} eine Nullstelle von $p(X)$, also ist $p(X)$ auch das Minimalpolynom von $\zeta' := \zeta^{p_1}$. Nun wenden wir die Behauptung erneut auf ζ' und p_2 an und erhalten, dass auch $\zeta'' := (\zeta')^{p_2} = \zeta^{p_1 p_2}$ eine Nullstelle von $p(X)$ ist. Führen wir dies fort, ergibt sich schließlich wie gewünscht, dass $p(\zeta^m) = 0$.

Insgesamt hat also das Minimalpolynom $p(X)$ von ζ über \mathbb{Q} alle primitiven n -ten Einheitswurzeln als Nullstellen und muss somit mit $\Phi_n(X)$ übereinstimmen. Letzteres ist somit irreduzibel in $\mathbb{Q}[X]$ und (da es normiert und somit primitiv ist) auch in $\mathbb{Z}[X]$ nach Satz 3.81. \square

Zusammenfassend kann den Fall $K = \mathbb{Q}$ also folgendermaßen beschreiben.

Korollar 5.60. Sei $n \in \mathbb{N}$ und $\zeta \in \mathbb{C}$ eine primitive n -te Einheitswurzel. Dann ist $\mathbb{Q}[\zeta]/\mathbb{Q}$ eine endliche Galoiserweiterung mit $[\mathbb{Q}[\zeta]/\mathbb{Q}] = \varphi(n)$ und man hat einen Gruppenisomorphismus

$$(\mathbb{Z}/n\mathbb{Z})^\times \rightarrow \text{Gal}(\mathbb{Q}[\zeta]/\mathbb{Q}), \quad [j] \mapsto (\sigma_j: \zeta \mapsto \zeta^j).$$

Beweis. Dass $\mathbb{Q}[\zeta]/\mathbb{Q}$ eine endliche Galoiserweiterung ist, folgt direkt aus Satz 5.52. Nach Satz 5.59 ist außerdem $\Phi_n(X)$ das Minimalpolynom von ζ über \mathbb{Q} , sodass $[\mathbb{Q}[\zeta]/\mathbb{Q}] = \deg(\Phi_n) = \varphi(n)$ folgt. Die Elemente der Galoisgruppe bestimmt man leicht mit dem Fortsetzungssatz (Satz 4.30): Ein Element der Galoisgruppe bildet ζ wieder auf eine (beliebige) Nullstelle von $\Phi_n(X)$ ab, also auf eine primitive n -te Einheitswurzel. Dadurch ist ein Element der Galoisgruppe dann auch eindeutig bestimmt. Die primitiven n -ten Einheitswurzeln sind genau die ζ^j mit $\text{ggT}(j, n) = 1$, also $[j] \in (\mathbb{Z}/n\mathbb{Z})^\times$, also ist die Abbildung

$$(\mathbb{Z}/n\mathbb{Z})^\times \rightarrow \text{Gal}(\mathbb{Q}[\zeta]/\mathbb{Q}), \quad [j] \mapsto (\sigma_j: \zeta \mapsto \zeta^j)$$

wohldefiniert und bijektiv. Sie ist außerdem ein Gruppenhomomorphismus, denn sind $[j], [j'] \in (\mathbb{Z}/n\mathbb{Z})^\times$, so gilt $\sigma_j \circ \sigma_{j'} = \sigma_{jj'}$, denn

$$(\sigma_j \circ \sigma_{j'})(\zeta) = \sigma_j(\sigma_{j'}(\zeta)) = \sigma_j(\zeta^{j'}) = (\sigma_j(\zeta))^{j'} = (\zeta^j)^{j'} = \zeta^{jj'} = \sigma_{jj'}(\zeta).$$

□

Anwendungen

Tant que l'Algèbre et la Géométrie ont été séparées, leurs progrès ont été lents et leurs usages bornés ; mais lorsque ces deux sciences se sont réunies, elles se sont prêtées des forces mutuelles et ont marché ensemble d'un pas rapide vers la perfection.

Solange Algebra und Geometrie getrennt waren, waren ihr Fortschritt langsam und ihr Nutzen begrenzt; doch als diese beiden Wissenschaften sich vereinten, leihten sie sich gegenseitig ihre Stärken und gingen gemeinsam raschen Schrittes der Perfektion entgegen.

Joseph Louis Lagrange

6.1 Vorbereitung: Auflösbare Gruppen

Bevor wir endlich verstehen können, wie die Galoistheorie uns zeigt, dass es keine Lösungsformel für Polynomgleichungen vom Grad $n \geq 5$ geben kann, müssen wir noch einen neuen Begriff in der Gruppentheorie kennenlernen und untersuchen, dessen Name bereits andeutet, dass er mit dem erwähnten Problem zusammenhängt.

Kapitel 6 Anwendungen

Definition 6.1. Eine Gruppe G mit neutralem Element e heißt *auflösbar*, falls es eine Kette von Untergruppen

$$G = G_0 \supseteq G_1 \supseteq G_2 \supseteq \dots \supseteq G_N = \{e\}$$

gibt, sodass für alle $j \in \{1, \dots, N\}$ die folgenden beiden Eigenschaften erfüllt sind:

- (1) $G_j \triangleleft G_{j-1}$ ist ein Normalteiler,
- (2) G_{j-1}/G_j ist eine abelsche Gruppe.

Eine solche Kette von Untergruppe heißt auch *Normalreihe*.

Bemerkung 6.2. Aus der Definition ist sofort klar, dass jede abelsche Gruppe auflösbar ist, denn wir können die Kette

$$G = G_0 \supseteq G_1 = \{e\}$$

betrachten. (Der Quotient G_0/G_1 ist die Gruppe G selbst und somit abelsch.)

Für nicht-abelsche Gruppen müssen wir längere Ketten betrachten. Die Idee hinter dieser Definition ist, dass man eine Gruppe, die nicht kommutativ ist, durch abelsche Gruppen „approximieren“ möchte. Natürlich kann es auch sein, dass es für bestimmte Gruppen solch eine Kette nicht gibt, es ist also nicht jede Gruppe auflösbar.

Definition 6.3. Sei G eine Gruppe.

Für zwei Elemente $g, h \in G$ nennen wir das Element

$$[g, h] := ghg^{-1}h^{-1} \in G$$

den *Kommutator* von g und h .

Wir bezeichnen mit $[G, G]$ die Untergruppe von G , die von allen Elementen $[g, h]$ für beliebige $g, h \in G$ erzeugt wird (d.h. die kleinste Untergruppe von G , die all diese Kommutatoren $[g, h]$ enthält), und nennen sie die *Kommutatoruntergruppe* (oder *abgeleitete Gruppe*) von G .

Man schreibt auch $G^{(0)} := G$ und $G^{(1)} := [G, G]$ und definiert rekursiv für $j \geq 2$ den j -ten *iterierten Kommutator*

$$G^{(j)} := [G^{(j-1)}, G^{(j-1)}].$$

Dadurch erhält man die Kette von Untergruppen

$$G = G^{(0)} \supseteq G^{(1)} \supseteq G^{(2)} \supseteq \dots$$

Diese heißt *Kommutatorreihe* von G .

Lemma 6.4. Sei G eine Gruppe. Dann ist $[G, G] \triangleleft G$ ein Normalteiler und $G/[G, G]$ eine abelsche Gruppe.

Außerdem gilt: Ist $H \subseteq G$ eine Untergruppe, sodass G/H abelsch ist, so folgt $[G, G] \subseteq H$. Die Kommutatoruntergruppe $[G, G]$ ist also die kleinste Untergruppe von G , sodass der Quotient abelsch ist.

Beweis. Wir machen zunächst folgende Beobachtung: Für beliebige $g, h \in G$ und $t \in G$ gilt

$$\begin{aligned} t[g, h]t^{-1} &= tghg^{-1}h^{-1}t^{-1} = tg \underbrace{(t^{-1}t)}_{=e} h \underbrace{(t^{-1}t)}_{=e} g^{-1} \underbrace{(t^{-1}t)}_{=e} h^{-1}t^{-1} \\ &= (tgt^{-1})(tht^{-1})(tg^{-1}t^{-1})(th^{-1}t^{-1}) \\ &= (tgt^{-1})(tht^{-1})(tgt^{-1})^{-1}(tht^{-1})^{-1} \\ &= [tgt^{-1}, tht^{-1}]. \end{aligned}$$

Sei nun $a \in [G, G]$ beliebig, d.h. $a = [g_1, h_1] \cdot [g_2, h_2] \cdot \dots \cdot [g_m, h_m]$ ist ein endliches Produkt von Kommutatoren für bestimmte $g_1, \dots, g_m, h_1, \dots, h_m \in G$, und sei $t \in G$. Dann ist mit obiger Überlegung

$$\begin{aligned} tat^{-1} &= t[g_1, h_1] \cdot [g_2, h_2] \cdot \dots \cdot [g_m, h_m]t^{-1} \\ &= t[g_1, h_1]t^{-1} \cdot t[g_2, h_2]t^{-1} \cdot \dots \cdot t[g_m, h_m]t^{-1} \\ &= [tg_1t^{-1}, th_1t^{-1}] \cdot [tg_2t^{-1}, th_2t^{-1}] \cdot \dots \cdot [tg_mt^{-1}, th_mt^{-1}] \end{aligned}$$

ebenfalls ein Produkt von Kommutatoren von Elementen aus G , also ein Element von $[G, G]$. Folglich ist $[G, G] \triangleleft G$ ein Normalteiler.

Zur Kommutativität überlegt man sich zunächst Folgendes: Eine Gruppe ist genau dann abelsch, wenn jeder Kommutator gleich dem neutralen Element ist, denn $ghg^{-1}h^{-1} = e$ ist äquivalent zu $gh = hg$.

Sind nun $g, h \in G$ beliebig, dann gilt $[g, h] = ghg^{-1}h^{-1} \in [G, G]$, also ist die Äquivalenzklasse von $[g, h]$ in $G/[G, G]$ gleich der Äquivalenzklasse des neutralen Elements, d.h. $[ghg^{-1}h^{-1}] = [e]$. Daraus folgt $[gh] = [hg]$, also ist $G/[G, G]$ abelsch.

Umgekehrt gilt: Wenn G/H für eine Untergruppe $H \subseteq G$ abelsch sein soll, muss für alle $[g], [h] \in G/H$ gelten:

$$[e] = [[g], [h]] = [g][h][g]^{-1}[h]^{-1} = [ghg^{-1}h^{-1}] = [[g, h]],$$

d.h. die Äquivalenzklasse jedes Kommutators muss gleich der Äquivalenzklasse des neutralen Elements in G/H sein. Dies bedeutet aber, dass alle Kommutatoren $[g, h]$ für beliebige $g, h \in G$ in H liegen müssen, also $[G, G] \subseteq H$. \square

Bemerkung 6.5. Wegen obiger Beobachtung heißt die Gruppe $G/[G, G]$ auch die **Abelianisierung** von G , denn sie ist der „minimalinvasivste“ Quotient von G , der abelsch ist.

Kapitel 6 Anwendungen

Man fragt sich nun, wie man für eine gegebene Gruppe prüfen kann, ob diese auflösbar ist. Dazu müsste man eine Normalreihe wie in Definition 6.3 finden. Als Kandidat für eine solche kann man die Kommutatorreihe testen. Was macht man aber, wenn diese nicht „funktioniert“, also nicht die passenden Eigenschaften hat? (Nach Lemma 6.4 hat sie fast alle gewünschten Eigenschaften, aber es könnte zum Beispiel sein, dass sie nicht endet, also niemals bei der trivialen Untergruppe $\{e\}$ „ankommt“.) Der folgende Satz erlöst uns von diesem Problem: Er besagt nämlich, dass es dann auch keine andere Normalreihe gibt. Wenn also die Kommutatorreihe nicht endet, so kann die Gruppe nicht auflösbar sein.

Satz 6.6. *Eine Gruppe G mit neutralem Element $e \in G$ ist genau dann auflösbar, wenn es ein $N \in \mathbb{N}$ gibt mit $G^{(N)} = \{e\}$.*

Beweis. Eine Richtung ist einfach: Falls es ein $N \in \mathbb{N}$ mit $G^{(N)} = \{e\}$ gibt, so ist die Kommutatorreihe eine Kette wie in Definition 6.3, also ist G auflösbar.

Sei nun umgekehrt G eine auflösbare Gruppe, d.h. es gibt eine Kette von Untergruppen

$$G = G_0 \supseteq G_1 \supseteq G_2 \supseteq \dots \supseteq G_N = \{e\},$$

wobei für $G_j \triangleleft G_{j-1}$ ein Normalteiler und G_{j-1}/G_j abelsch ist jedes $j \in \{1, \dots, N\}$. Dann haben wir den folgenden Zusammenhang zwischen dieser Kette und der Kommutatorreihe.

Behauptung: Für jedes $j \in \{1, \dots, N\}$ gilt $G^{(j)} \subseteq G_j$.

Wir beweisen dies induktiv.

Induktionsanfang: Da G/G_1 abelsch ist, wissen wir aus Lemma 6.4, dass $[G, G] \subseteq G_1$, in anderen Worten: $G^{(1)} \subseteq G_1$.

Induktionsvoraussetzung: Für ein beliebiges, aber festes $j \in \{1, \dots, N-1\}$ sei bereits bekannt, dass $G^{(j)} \subseteq G_j$.

Induktionsschluss: Da G_j/G_{j+1} abelsch ist, gilt $[G_j, G_j] \subseteq G_{j+1}$ (wieder nach Lemma 6.4). Daraus erhalten wir mit der Induktionsvoraussetzung

$$G^{(j+1)} = [G^{(j)}, G^{(j)}] \subseteq [G_j, G_j] \subseteq G_{j+1}.$$

Nach dieser Behauptung ist also insbesondere $G^{(N)} \subseteq G_N = \{e\}$ und damit $G^{(N)} = \{e\}$ (die triviale Gruppe besitzt nur diese eine Untergruppe). \square

Korollar 6.7. *Ist G eine auflösbare Gruppe und $H \triangleleft G$ ein Normalteiler, so ist G/H eine auflösbare Gruppe.*

Beweis. Zuerst untersuchen wir, wie die iterierten Kommutatoren von G/H mit denen von G zusammenhängen. Wir bezeichnen mit $\pi: G \rightarrow G/H, g \mapsto [g]$ die kanonische Projektion.

Behauptung: Für jedes $j \in \mathbb{N}_0$ gilt $(G/H)^{(j)} = \pi(G^{(j)})$.

Dies zeigen wir induktiv.

Induktionsanfang: Für $j = 0$ ist offensichtlich $(G/H)^{(0)} = G/H = \pi(G) = \pi(G^{(0)})$.

Induktionsvoraussetzung: Sei die Aussage bereits für ein beliebiges, aber festes $j \in \mathbb{N}_0$ gezeigt.

Induktionsschluss: Mit der Definition des iterierten Kommutators und der Induktionsvoraussetzung rechnet man leicht

$$\begin{aligned} (G/H)^{(j+1)} &= [(G/H)^{(j)}, (G/H)^{(j)}] = [\pi(G^{(j)}), \pi(G^{(j)})] \\ &= \pi([G^{(j)}, G^{(j)}]) = \pi(G^{(j+1)}). \end{aligned}$$

Hierbei verwenden wir beim Übergang von der ersten zur zweiten Zeile auch, dass π ein Gruppenhomomorphismus ist: Es ist also egal, ob man zuerst den Kommutator berechnet (also bestimmte Verknüpfungen in der Gruppe ausführt) und dann π anwendet oder umgekehrt.

Da nach Voraussetzung nun G auflösbar ist, gibt es nach Satz 6.6 ein $N \in \mathbb{N}$ mit $G^{(N)} = \{e\}$. Mit der eben bewiesenen Behauptung ist dann $(G/H)^{(N)} = \pi(G^{(N)}) = \pi(\{e\}) = \{\{e\}\}$. Somit ist (wieder mit Satz 6.6) auch G/H auflösbar. \square

Wir untersuchen nun noch eine wichtige Gruppe auf Auflösbarkeit: die symmetrische Gruppe. Das folgende Resultat gibt uns bereits einen Hinweis darauf, warum sich bei der Lösbarkeit von Polynomgleichungen ab Grad 5 etwas ändert.

Lemma 6.8. *Die symmetrische Gruppe S_n ist auflösbar für $n \leq 4$, aber nicht auflösbar für $n \geq 5$.*

Beweis. Die Gruppen S_1 und S_2 sind abelsch und daher auflösbar (siehe Bemerkung 6.2).

Für die Gruppe S_3 betrachte die Kette

$$S_3 \supseteq A_3 \supseteq \{\text{id}\}.$$

Es gilt:

- $A_3 \triangleleft S_3$ ist ein Normalteiler, wie man leicht prüft.
- S_3/A_3 ist eine Gruppe mit 2 Elementen und daher isomorph zu $\mathbb{Z}/2\mathbb{Z}$ also abelsch.
- $A_3/\{e\} \cong A_3$ ist eine Gruppe mit 3 Elementen, also isomorph zu $\mathbb{Z}/3\mathbb{Z}$ und daher abelsch.

Kapitel 6 Anwendungen

Also ist S_3 auflösbar.

Für die Gruppe S_4 betrachte die Kette

$$S_4 \supseteq A_4 \supseteq V \supseteq \{\text{id}\},$$

wobei $V := \{\text{id}, (12)(34), (13)(24), (14)(23)\}$ die *kleinsche Vierergruppe* ist.

Es gilt:

- $A_4 \triangleleft S_4$ und $V \triangleleft A_4$ sind jeweils Normalteiler, wie man leicht prüft.
- S_4/A_4 ist eine Gruppe mit 2 Elementen und daher isomorph zu $\mathbb{Z}/2\mathbb{Z}$ also abelsch.
- A_4/V ist eine Gruppe mit $\frac{\#A_4}{\#V} = \frac{12}{4} = 3$ Elementen, also isomorph zu $\mathbb{Z}/3\mathbb{Z}$ und daher abelsch.
- $V/\{e\} \cong V$ ist eine abelsche Gruppe, denn es gilt $V \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$.

Also ist S_4 auflösbar. (Anmerkung: Die beiden obigen Ketten für S_3 und S_4 sind auch tatsächlich die jeweiligen Kommutatorreihen, was wir hier aber nicht bewiesen haben.)

Nun zur Gruppe S_n für $n \geq 5$.

Behauptung: Ist $n \geq 5$ und $G \subseteq S_n$ eine Untergruppe, die jeden 3-Zykel $(a_1 a_2 a_3) \in S_n$ enthält. Dann enthält auch $[G, G]$ alle 3-Zykel.

Sei $(a_1 a_2 a_3) \in G$ ein beliebiger 3-Zykel und seien $a_4, a_5 \in \{1, \dots, n\}$ zwei weitere Elemente, sodass a_1, a_2, a_3, a_4, a_5 paarweise verschieden sind. Dann rechnet man leicht nach, dass gilt

$$(a_1 a_2 a_3) = (a_1 a_2 a_4) \circ (a_1 a_3 a_5) \circ (a_1 a_2 a_4)^{-1} \circ (a_1 a_3 a_5)^{-1}.$$

Also lässt sich $(a_1 a_2 a_3)$ als Kommutator von 3-Zykeln schreiben (die alle nach Voraussetzung auch in G liegen) und somit ist $(a_1 a_2 a_3) \in [G, G]$.

Wenden wir die Behauptung wiederholt an, erkennen wir dass alle iterierten Kommutatoren $(S_n)^{(j)}$ alle 3-Zykel enthalten. Es kann also niemals $(S_n)^{(N)} = \{\text{id}\}$ gelten und somit ist S_n nach Satz 6.6 nicht auflösbar. \square

6.2 Lösungsformeln für Polynomgleichungen

Wir wenden uns jetzt endlich dem Problem der Lösungsformel für Polynomgleichungen höheren Grades zu. Aus unserer Schulzeit kennen wir alle die Lösungsformel für quadratische Gleichungen: Die Lösungen eines Polynoms $f(X) = aX^2 + bX + c$ mit $a, b, c \in \mathbb{Q}$ lassen sich einfach mithilfe der Formel

$$x_{1,2} = \frac{-b \pm \sqrt{b^2 - 4ac}}{2a}$$

berechnen. Auch für Gleichungen dritten und vierten Grades gibt es ähnliche (wenn auch natürlicherweise komplizierte) Formeln (gefunden im 16. Jahrhundert von Gerolamo Cardano und Lodovico Ferrari).

Wir wollen nun verstehen, warum es für Polynomgleichungen fünften und höheren Grades keine solche Lösungsformel geben kann. Wir beschränken uns in diesem Abschnitt auf Körper der Charakteristik 0 und meist auf den Grundkörper \mathbb{Q} . Für Körper positiver Charakteristik müsste man einige Details anpassen.

Definition 6.9. Sei K ein Körper der Charakteristik 0 und $f(X) \in K[X]$ ein Polynom. Wir sagen, dass $f(X)$ *durch Radikale auflösbar* ist, wenn es eine Folge von Körpererweiterungen

$$K = K_0 \subseteq K_1 \subseteq K_2 \subseteq \dots \subseteq K_N$$

gibt, sodass $f(X)$ in K_N in Linearfaktoren zerfällt (also K_N einen Zerfällungskörper von $f(X)$ enthält) und sodass für jedes $j \in \{1, \dots, N\}$ die Erweiterung K_j von der Form

$$K_j = K_{j-1}[\alpha_j]$$

ist, wobei $\alpha_j \in K_j$ eine Nullstelle eines Polynoms $X^{m_j} - \gamma_j \in K_{j-1}[X]$ für ein $m_j \in \mathbb{N}$ und ein $\gamma_j \in K_{j-1}$ ist.

Bemerkung 6.10. Denken wir kurz darüber nach, was diese Definition konkret bedeutet:

Jedes Element α_j ist Nullstelle eines Polynoms der Form $X^{m_j} - \gamma_j$. Wir könnten also auch schreiben $\alpha_j = \sqrt[m_j]{\gamma_j}$, wobei $\sqrt[m_j]{\gamma_j}$ eine fest gewählte Wurzel des obigen Polynoms bezeichnet. In anderen Worten: In jedem Erweiterungsschritt adjungiert man eine (höhere) Wurzel eines Ausdruckes, den es im vorherigen Körper bereits gab.

Ist also beispielsweise $K = \mathbb{Q}$ der Grundkörper, so könnte $\alpha_1 = \sqrt{3}$ sein, also ist jedes Element in K_1 von der Form $a + b\sqrt{3}$ für $a, b \in \mathbb{Q}$. Dann könnte beispielsweise $\alpha_2 = \sqrt[3]{2 + 5\sqrt{3}}$ sein, also wäre jedes Element in K_2 von der Form $x + y\alpha_2 + z\alpha_2^2$ für $x, y, z \in K_1$, also von der Form

$$(a_1 + b_1\sqrt{3}) + (a_2 + b_2\sqrt{3}) \cdot \sqrt[3]{2 + 5\sqrt{3}} + (a_3 + b_3\sqrt{3}) \cdot \left(\sqrt[3]{2 + 5\sqrt{3}}\right)^2$$

für $a_1, b_1, a_2, b_2, a_3, b_3 \in \mathbb{Q}$. Dies kann man noch mehrere Male weiterführen, aber es ist klar, dass die entstehenden Körper immer Elemente haben, die polynomielle Ausdrücke sind, in denen nur rationale Zahlen vorkommen sowie Wurzeln, unter denen wiederum polynomielle Ausdrücke aus rationalen Zahlen und Wurzeln stehen, unter denen abermals polynomielle Ausdrücke . . . (Dies kann man endlich oft so weiterführen.)

Anders ausgedrückt: Die Elemente von K_N sind Ausdrücke, die man mithilfe der rationalen Zahlen, der vier Grundrechenarten sowie Wurzeln aufschreiben kann. Ein Element, das sich auf diese Weise schreiben lässt, nennen wir auch *Radikal* (vom lateinischen Wort *radix* für Wurzel).

Kapitel 6 Anwendungen

(Dass auch Division in diesen Ausdrücken erlaubt ist, sieht man nicht sofort: Da aber alle vorkommenden Elemente algebraisch sind, gilt in jedem Schritt $K[\alpha_j] = K(\alpha_j)$, es können also auch Quotienten zweier Elemente wieder als Polynomausdrücke geschrieben werden. Divisionen sind also „zulässig“, aber nicht unbedingt notwendig.)

Die obige Definition bedeutet daher – wie der Begriff „durch Radikale auflösbar“ schon andeutet –, dass jede Nullstelle von $f(X)$ sich als ein solches Radikal schreiben lässt.

Wir werden uns im Folgenden auf den Grundkörper $K = \mathbb{Q}$ konzentrieren und nehmen daher an, dass sich alle Erweiterungen im Körper \mathbb{C} abspielen. Das folgende Lemma zeigt, dass sich die Bedingungen aus Definition 6.9 noch verschärfen lassen, wenn man die Folge von Körpererweiterungen „geschickt“ konstruiert.

Lemma 6.11. *Sei $f(X) \in \mathbb{Q}[X]$ ein Polynom und sei $Z \subseteq \mathbb{C}$ sein Zerfällungskörper in \mathbb{C} . Dann gilt: Ist $f(X) \in \mathbb{Q}[X]$ durch Radikale auflösbar, so gibt es eine Folge*

$$\mathbb{Q} \subseteq L_0 \subseteq L_1 \subseteq L_2 \subseteq \dots \subseteq L_N$$

von Körpererweiterungen (in \mathbb{C}), sodass gilt:

- $Z \subseteq L_N$,
- für jedes $j \in \{1, \dots, N\}$ gilt $L_j = L_{j-1}[\alpha_j]$, wobei $\alpha_j \in L_j$ eine Nullstelle eines Polynoms $X^{m_j} - \gamma_j$ für ein $m_j \in \mathbb{N}$ und ein $\gamma_j \in L_{j-1}$ ist,
- $L_0 = \mathbb{Q}[\zeta]$, wobei $\zeta \in \mathbb{C}$ eine m -te Einheitswurzel für ein $m \in \mathbb{N}$ ist,
- für jedes $j \in \{1, \dots, N\}$ ist L_j/L_{j-1} eine normale Körpererweiterung,
- die Erweiterung L_N/\mathbb{Q} ist normal.

Beweis. Nach Voraussetzung ist $f(X) \in \mathbb{Q}[X]$ durch Radikale auflösbar. Sei also

$$\mathbb{Q} = K_0 \subseteq K_1 \subseteq K_2 \subseteq \dots \subseteq K_N$$

eine Folge von Körpererweiterungen wie in Definition 6.9.

Zunächst können wir sie so modifizieren, dass jeder Schritt dieser Folge eine normale Körpererweiterung ist:

Für $j \in \{1, \dots, N\}$ gibt es nach Definition ein $m_j \in \mathbb{N}$ und ein $\gamma_j \in K_{j-1}$, sodass $K_j = K_{j-1}[\alpha_j]$, wobei α_j eine Nullstelle von $X^{m_j} - \gamma_j$ ist. Setze $m := \prod_{j=1}^N m_j$ sowie $\zeta := e^{\frac{2\pi i}{m}}$ und definiere für jedes $j \in \{0, \dots, N\}$ den Körper

$$\tilde{K}_j := K_j[\zeta].$$

Dann haben wir eine Folge

$$\mathbb{Q} \subseteq \tilde{K}_0 = \mathbb{Q}[\zeta] \subseteq \tilde{K}_1 \subseteq \tilde{K}_2 \subseteq \dots \subseteq \tilde{K}_N.$$

Diese Folge erfüllt immer noch die Forderungen aus Definition 6.9, denn es gilt

$$\tilde{K}_j = K_j[\zeta] = K_{j-1}[\alpha_j, \zeta] = \tilde{K}_{j-1}[\alpha_j].$$

Nun ist aber \tilde{K}_0/\mathbb{Q} normal (siehe Satz 5.52). Außerdem ist für $j \in \{1, \dots, N\}$ die Erweiterung $\tilde{K}_j/\tilde{K}_{j-1}$ normal: Die Nullstellen (in \mathbb{C}) des Polynoms $X^{m_j} - \gamma_j$ sind

$$\alpha_j, \xi\alpha_j, \dots, \xi^{m_j-1}\alpha_j,$$

wobei $\xi = e^{\frac{2\pi i}{m_j}}$. Der Zerfällungskörper dieses Polynoms über \tilde{K}_{j-1} ist also

$$\begin{aligned} \tilde{K}_{j-1}[\alpha_j, \xi\alpha_j, \dots, \xi^{m_j-1}\alpha_j] &= \tilde{K}_{j-1}[\alpha_j, \xi] = K_{j-1}[\zeta, \alpha_j, \xi] = K_{j-1}[\zeta, \alpha_j] \\ &= \tilde{K}_{j-1}[\alpha_j] = \tilde{K}_j. \end{aligned}$$

Hier folgt der dritte Schritt aus der Tatsache, dass ξ wegen $m_j \mid m$ bereits eine Potenz von ζ ist. Also ist \tilde{K}_j der Zerfällungskörper von $X^{m_j} - \gamma_j$ über \tilde{K}_{j-1} und somit die Erweiterung $\tilde{K}_j/\tilde{K}_{j-1}$ normal.

Es sind nun also alle bis auf die letzte Forderung an die Folge von Körpererweiterungen erfüllt. Nun modifizieren wir die Körper \tilde{K}_j weiter, sodass schließlich auch noch die Gesamterweiterung L_N/\mathbb{Q} normal ist. Dazu gehen wir induktiv vor:

Die Erweiterung $\tilde{K}_0 = \mathbb{Q}[\zeta]/\mathbb{Q}$ ist bereits normal (Satz 5.52) und wir setzen $L_0 := \tilde{K}_0$.

Die Erweiterung $\tilde{K}_1 = L_0[\alpha_1]/\mathbb{Q}$ ist möglicherweise noch nicht normal. Betrachte das Minimalpolynom $p(X) \in \mathbb{Q}[X]$ von α über \mathbb{Q} . Seien β_1, \dots, β_d seine Nullstellen in \mathbb{C} . Dann betrachte die Folge von Erweiterungen

$$\mathbb{Q} \subseteq L_0 \subseteq L_0[\beta_1] \subseteq L_0[\beta_1, \beta_2] \subseteq \dots \subseteq L_0[\beta_1, \dots, \beta_d]. \quad (\diamond_1)$$

Der Körper $L'_1 := L_0[\beta_1, \dots, \beta_d]$ enthält \tilde{K}_1 , da α_1 unter den β_1, \dots, β_d vorkommt. Die Erweiterung L'_1/\mathbb{Q} ist außerdem normal, denn L_0/\mathbb{Q} ist normal, also Zerfällungskörper eines Polynoms $f(X) \in \mathbb{Q}[X]$, also ist L'_1 nun Zerfällungskörper des Polynoms $f(X) \cdot p(X)$ über \mathbb{Q} .

Behauptung: Jedes β_i für $i \in \{1, \dots, d\}$ ist Nullstelle eines Polynoms $X^{m_1} - \eta_i$ für ein $\eta_i \in L_0$.

Sei $i \in \{1, \dots, N\}$ beliebig. Nach dem Fortsetzungssatz gibt es einen Körperhomomorphismus $\tilde{\varphi}: L_0[\alpha_1] \rightarrow L_0[\beta_i]$ mit $\tilde{\varphi}|_{\mathbb{Q}} = \text{id}_{\mathbb{Q}}$. (Genauer: Mit Satz 4.30 erhält man zunächst einen Körperhomomorphismus $\varphi: \mathbb{Q}[\alpha_1] \rightarrow \mathbb{Q}[\beta_i]$ und durch sukzessive Anwendung des Fortsetzungssatzes lässt sich dieser fortsetzen zu einem solchen $\tilde{\varphi}$.)

Da L_0/\mathbb{Q} normal ist, gilt wegen Lemma 5.8, dass $\text{Hom}_{\mathbb{Q}}(L_0, \Omega) = \text{Aut}_{\mathbb{Q}}(L_0)$. Dies bedeutet also, dass $\tilde{\varphi}(x) \in L_0$ für jedes $x \in L_0$. Da α_1 eine Nullstelle von $X^{m_1} - \gamma_1$ ist, ist β_i nach Lemma 4.28 eine Nullstelle von $X^{m_1} - \tilde{\varphi}(\gamma_1)$, also eine m_1 -te Wurzel von $\eta_1 := \tilde{\varphi}(\gamma_1) \in L_0$ wie gewünscht.

Kapitel 6 Anwendungen

Außerdem sind in der Folge (\diamond_1) alle Erweiterungsschritte normal. (Dies folgt wie oben, als wir gezeigt haben, dass $\tilde{K}_j/\tilde{K}_{j-1}$ normal ist, nämlich einfach daraus, dass ζ in allen Körpern enthalten ist und daher jeder Körper bereits ein Zerfällungskörper über dem nächstkleineren ist.) Somit ist (\diamond_1) in gewisser Weise eine „verbesserte Version“ von $\mathbb{Q} \subseteq \tilde{K}_0 \subseteq \tilde{K}_1$.

Nun gehen wir sukzessive weiter so vor. Wir betrachten das Minimalpolynom von α_2 über \mathbb{Q} und adjungieren zu L'_1 nach und nach seine Nullstellen $\delta_1, \dots, \delta_e$ hinzu, erhalten also eine Folge

$$\mathbb{Q} \subseteq L_0 \subseteq L_0[\beta_1] \subseteq \dots \subseteq L_0[\beta_1, \dots, \beta_d] = L'_1 \subseteq L'_1[\delta_1] \subseteq \dots \subseteq L'_1[\delta_1, \dots, \delta_e] = L'_2. \quad (\diamond_2)$$

Wieder können wir zeigen, dass L'_2/\mathbb{Q} normal ist, dass $\tilde{K}_2 \subseteq L'_2$ gilt und dass jeder Schritt dieser Folge eine normale Erweiterung ist und durch Adjunktion einer m_2 -ten Wurzel eines Elements L'_1 entsteht. Die Folge (\diamond_2) ist somit eine „verbesserte Version“ von $\mathbb{Q} \subseteq \tilde{K}_0 \subseteq \tilde{K}_1 \subseteq \tilde{K}_2$.

Führen wir dies weiter, erhalten wir schließlich eine (sehr lange) Folge (\diamond_N) , die mit einem Körper L'_N endet, der \tilde{K}_N und somit Z enthält und alle gewünschten Eigenschaften erfüllt. \square

Mit dieser „verfeinerten“ Folge von Körpererweiterungen können wir den folgenden Satz beweisen, der uns einen Zusammenhang zwischen der Auflösbarkeit von Polynomen und der Auflösbarkeit von Gruppen gibt.

Satz 6.12. Sei $f(X) \in \mathbb{Q}[X]$ ein Polynom mit $\deg(f) \geq 1$ und sei $Z \subseteq \mathbb{C}$ der Zerfällungskörper von f . Dann gilt: Ist $f(X)$ durch Radikale auflösbar, so ist $\text{Gal}(Z/\mathbb{Q})$ eine auflösbare Gruppe.

Beweis. Sei

$$\mathbb{Q} \subseteq L_0 = \mathbb{Q}(\zeta) \subseteq L_1 \subseteq L_2 \subseteq \dots \subseteq L_N$$

eine Folge von Körpererweiterungen wie in Lemma 6.11.

Betrachte die Gruppe $G := \text{Gal}(L_N/\mathbb{Q})$. Weiter definieren wir für $j \in \{0, \dots, N\}$ die Untergruppen

$$H_j := \text{Gal}(L_N/L_j) \subseteq G.$$

Nach dem Hauptsatz der Galoistheorie (Satz 5.32(i)) haben wir eine Kette

$$G \supseteq H_0 \supseteq H_1 \supseteq \dots \supseteq H_N = \{e\}.$$

Diese ist eine Normalreihe wie in Definition 6.3, denn:

- (1) Für jedes $j \in \{1, \dots, N\}$ ist $H_j \triangleleft H_{j-1}$ ein Normalteiler nach Satz 5.32(iii), denn L_j/L_{j-1} ist eine normale Erweiterung. Außerdem ist $H_0 \triangleleft G$ ein Normalteiler, da $L_0 = \mathbb{Q}[\zeta]/\mathbb{Q}$ eine normale Erweiterung ist.

- (2) Der Quotient G/H_0 ist eine abelsche Gruppe, denn es gilt nach dem Hauptsatz (Satz 5.32(iii))

$$G/H_0 = \text{Gal}(L_N/\mathbb{Q})/\text{Gal}(L_N/\mathbb{Q}[\zeta]) \cong \text{Gal}(\mathbb{Q}[\zeta]/\mathbb{Q})$$

und diese Gruppe ist abelsch nach Korollar 5.60.

Außerdem ist für jedes $j \in \{1, \dots, N\}$ der Quotient H_{j-1}/H_j eine abelsche Gruppe, denn: Nach dem Hauptsatz (Satz 5.32(iii)) ist

$$H_{j-1}/H_j = \text{Gal}(L_N/L_{j-1})/\text{Gal}(L_N/L_j) \cong \text{Gal}(L_j/L_{j-1}).$$

Außerdem wissen wir, dass $L_j = L_{j-1}[\alpha_j]$ gilt für eine Nullstelle α_j des Polynoms $X^{m_j} - \gamma_j$. Jede andere Nullstelle dieses Polynoms hat dann die Form $\zeta^k \cdot \alpha_j$ für ein $k \in \mathbb{N}$. Somit hat auch jede Nullstelle des Minimalpolynoms von α_j über L_{j-1} diese Form (denn dieses Minimalpolynom ist ein Teiler von $X^{m_j} - \gamma_j$). Ein Element der Galoisgruppe bildet also α_j auf ein Element $\zeta^k \cdot \alpha_j$ ab (und ist dadurch eindeutig bestimmt). In anderen Worten: Für ein Element $\sigma \in \text{Gal}(L_j/L_{j-1})$ ist $\frac{\sigma(\alpha_j)}{\alpha_j}$ eine m -te Einheitswurzel. Wir können daher die Abbildung

$$\text{Gal}(L_j/L_{j-1}) \rightarrow \mu_m(L_j), \quad \sigma \mapsto \frac{\sigma(\alpha_j)}{\alpha_j} \quad (\circ)$$

betrachten. Diese ist ein Gruppenhomomorphismus, denn für zwei Elemente $\sigma_1, \sigma_2 \in \text{Gal}(L_j/L_{j-1})$ mit $\sigma_1(\alpha_j) = \zeta^{k_1} \alpha_j$ und $\sigma_2(\alpha_j) = \zeta^{k_2} \alpha_j$ folgt

$$(\sigma_1 \circ \sigma_2)(\alpha_j) = \sigma_1(\sigma_2(\alpha_j)) = \sigma_1(\zeta^{k_2} \alpha_j) = \sigma_1(\zeta^{k_2}) \cdot \sigma_1(\alpha_j) = \zeta^{k_2} \cdot \zeta^{k_1} \alpha_j = \zeta^{k_1+k_2} \alpha_j,$$

wobei der vorletzte Schritt verwendet, dass $\zeta \in L_{j-1}$ und $\sigma_1|_{L_{j-1}} = \text{id}_{L_{j-1}}$. Folglich erhalten wir

$$\frac{(\sigma_1 \circ \sigma_2)(\alpha_j)}{\alpha_j} = \frac{\zeta^{k_1+k_2} \alpha_j}{\alpha_j} = \frac{\zeta^{k_1} \alpha_j}{\alpha_j} \cdot \frac{\zeta^{k_2} \alpha_j}{\alpha_j} = \frac{\sigma_1(\alpha_j)}{\alpha_j} \cdot \frac{\sigma_2(\alpha_j)}{\alpha_j}.$$

Die Abbildung (\circ) ist außerdem injektiv, denn ihr Kern besteht aus denjenigen $\sigma \in \text{Gal}(L_j/L_{j-1})$, für die gilt $\frac{\sigma(\alpha_j)}{\alpha_j} = 1$, also $\sigma(\alpha_j) = \alpha_j$. Das einzige solche Element der Galoisgruppe ist aber $\sigma = \text{id}_{L_j}$. Somit ist (\circ) injektiv und mithilfe dieser Abbildung kann $\text{Gal}(L_j/L_{j-1})$ als Untergruppe von $\mu_m(L_j)$ aufgefasst werden. Letztere ist aber abelsch und somit ist auch $\text{Gal}(L_j/L_{j-1})$ eine abelsche Gruppe.

Wir haben also gezeigt, dass die Gruppe $G = \text{Gal}(L_N/\mathbb{Q})$ auflösbar ist.

Nun gilt $Z \subseteq L_N$, und da Z der Zerfällungskörper über \mathbb{Q} von $f(X)$ ist, ist Z/\mathbb{Q} normal. Folglich ist (wieder nach dem Hauptsatz, Satz 5.32(iii))

$$\text{Gal}(L_N/Z) \triangleleft G$$

Kapitel 6 Anwendungen

ein Normalteiler und es gibt einen Isomorphismus

$$\text{Gal}(Z/\mathbb{Q}) \cong G/\text{Gal}(L_N/Z).$$

Daher ist auch $\text{Gal}(Z/\mathbb{Q})$ auflösbar nach Korollar 6.7. \square

Nun fehlt also nur noch ein Schritt: Wenn wir Polynome finden, sodass die Galoisgruppe ihres Zerfällungskörpers nicht auflösbar ist, dann können die Polynome nicht durch Radikale auflösbar sein und daher kann es natürlich keine allgemeingültige „Lösungsformel“ (welche ja ein Ausdruck aus Grundrechenarten und Wurzeln sein soll) geben.

Lemma 6.13. Sei $f(X) \in \mathbb{Q}[X]$ ein irreduzibles Polynom und sei $n := \deg(f)$ eine Primzahl. Sei $Z \subseteq \mathbb{C}$ der Zerfällungskörper von f über \mathbb{Q} . Falls $f(X)$ genau $n - 2$ reelle Nullstellen besitzt, so ist $\text{Gal}(Z/\mathbb{Q}) \cong S_n$.

Beweis. Seien $\alpha_1, \dots, \alpha_n \in \mathbb{C}$ die Nullstellen von $f(X)$ und seien diese so nummeriert, dass $\alpha_3, \dots, \alpha_n \in \mathbb{R}$ und $\alpha_1, \alpha_2 \in \mathbb{C} \setminus \mathbb{R}$. Die Nullstellen sind paarweise verschieden, da $f(X)$ separabel ist (siehe Korollar 5.19).

Wir wissen außerdem: Zu jeder Nullstelle ist auch die komplex konjugierte eine Nullstelle, denn schreiben wir $f(X) = \sum_{i=0}^n a_i X^i$ mit $a_i \in \mathbb{Q} \subseteq \mathbb{R}$, dann folgt aus $f(\alpha) = 0$, dass auch

$$0 = \overline{f(\alpha)} = \overline{\sum_{i=0}^n a_i \alpha^i} = \sum_{i=0}^n \overline{a_i \alpha^i} = \sum_{i=0}^n \overline{a_i} \overline{\alpha^i} = \sum_{i=0}^n a_i \overline{\alpha}^i = f(\overline{\alpha}).$$

Folglich muss gelten $\alpha_2 = \overline{\alpha_1}$.

Ein Element der Galoisgruppe $\text{Gal}(Z/\mathbb{Q})$ ist eindeutig dadurch bestimmt, worauf die Elemente $\alpha_1, \dots, \alpha_n$ abgebildet werden (und diese müssen jeweils wieder auf Nullstellen von $f(X)$ abgebildet werden.) Jedes Element dieser Galoisgruppe lässt sich also mit einer gewissen Permutation der Nullstellenmenge $\{\alpha_1, \dots, \alpha_n\}$ identifizieren. (Dies hatten wir bereits am Ende von Abschnitt 4.3 und in Beispiel 5.3 gesehen.) In anderen Worten: Die Gruppe $\text{Gal}(Z/\mathbb{Q})$ ist isomorph zu einer Untergruppe von S_n , und wir wollen zeigen, dass sie die ganze S_n ist.

Zwei Elemente der Galoisgruppe $\text{Gal}(Z/\mathbb{Q})$ kennen wir bereits:

- Es gibt ein Element der Ordnung 2 in $\text{Gal}(Z/\mathbb{Q})$: Nach obiger Beobachtung ist die komplexe Konjugation

$$Z = \mathbb{Q}[\alpha_1, \dots, \alpha_n] \rightarrow Z = \mathbb{Q}[\alpha_1, \dots, \alpha_n], \quad z \mapsto \bar{z}$$

offensichtlich ein Körperautomorphismus (sie vertauscht nur die Elemente α_1 und α_2 in den Ausdrücken $z = \sum_{i_1, \dots, i_n=0}^k b_{i_1, \dots, i_n} \alpha_1^{i_1} \cdot \dots \cdot \alpha_n^{i_n}$).

- Es gibt ein Element der Ordnung p in $\text{Gal}(Z/\mathbb{Q})$: Betrachten wir die Zwischen-erweiterung $\mathbb{Q}[\alpha_1]$ von Z/\mathbb{Q} , so haben wir

$$[\mathbb{Q}[\alpha_1] : \mathbb{Q}] = \deg(f) = n,$$

da $f(X)$ das Minimalpolynom von α_1 über \mathbb{Q} ist. Außerdem gilt nach Lemma 5.29

$$[Z : \mathbb{Q}] = \#\text{Gal}(Z/\mathbb{Q}),$$

denn Z/\mathbb{Q} ist eine endliche Galois-erweiterung. Folglich erhalten wir (aus Satz 4.8)

$$n \mid \#\text{Gal}(Z/\mathbb{Q})$$

und damit sagt uns der Satz von Cauchy (Satz 2.57), dass es ein Element der Ordnung n in $\#\text{Gal}(Z/\mathbb{Q})$ gibt, denn n ist nach Voraussetzung eine Primzahl.

Die Galoisgruppe $\text{Gal}(Z/\mathbb{Q})$ ist also isomorph zu einer Untergruppe $H \subseteq S_n$, die ein Element der Ordnung 2 und ein Element der Ordnung n enthält. Da sich jedes Element als Produkt disjunkter Zyklen schreiben lässt (Satz 2.21), muss das Element von Ordnung p ein p -Zykel sein. Das Element von Ordnung 2 ist ein 2-Zykel, denn es vertauscht (wie wir oben gesehen haben) genau zwei Nullstellen und lässt die anderen unverändert. Durch eventuelle Umnummerierung der Menge $\{1, \dots, n\}$ können wir annehmen, dass der 2-Zykel von der Form $\tau = (12)$ ist und der n -Zykel von der Form $\sigma = (1 a_2 a_3 \dots a_n)$ mit $\{a_2, \dots, a_n\} = \{2, \dots, n\}$. Dann enthält die Gruppe H auch alle Elemente σ^j für $j \in \mathbb{N}$ und es gibt ein $k \in \{1, \dots, n-1\}$, sodass $\sigma^j = (12 b_3 \dots b_n)$ mit $\{b_3, \dots, b_n\} = \{3, \dots, n\}$ ist. (Dies gilt, da für $j \in \{1, \dots, n-1\}$ gilt $\text{ord}(\sigma^j) \mid \text{ord}(\sigma) = n$, und da n eine Primzahl ist, bedeutet dies, dass σ^j immer noch ein n -Zykel ist.) Nach eventuell nochmaliger Umnummerierung der Menge $\{3, \dots, n\}$ ist H also eine Untergruppe der S_n , welche die beiden Elemente (12) und $(12 \dots n)$ enthält.

Nun prüft man leicht, dass sich jede Nachbarschaftsvertauschung aus diesen beiden Elementen zusammensetzen lässt, denn es gilt für jedes $k \in \{1, \dots, n-1\}$

$$(12 \dots n)^{k-1} \circ (12) \circ (12 \dots n)^{-(k-1)} = (k \ k+1).$$

Hat man alle Nachbarschaftsvertauschnungen, so kann man aber nach Korollar 2.22 jedes andere Element von S_n daraus zusammensetzen. Also ist $H = S_n$ und somit $\text{Gal}(Z/\mathbb{Q}) \cong S_n$. \square

Solche irreduziblen Polynome mit $n-2$ reellen und zwei nichtreellen Nullstellen gibt es auch tatsächlich: Man betrachte zum Beispiel das Polynom $f(X) = X^5 - 777X + 7$. Dieses ist irreduzibel nach Eisenstein und mit unseren Kenntnissen aus der Analysis können wir leicht feststellen, dass dieses Polynom genau drei reelle Nullstellen besitzt. Wir haben also insgesamt das folgende Resultat bewiesen.

Korollar 6.14. *Es gibt Polynome $f(X) \in \mathbb{Q}[X]$ mit $\deg(f) = 5$, die nicht in Radikale auflösbar sind.*

Kapitel 6 Anwendungen

Insbesondere kann es also keine Lösungsformel für Polynomgleichungen fünften Grades geben, welche die Lösungen einer beliebigen Polynomgleichung fünften Grades mithilfe von rationalen Zahlen, den vier Grundrechenarten sowie Wurzelausdrücken beschreibt.

Bemerkung 6.15. Wir möchten noch ein paar Details zum Problem der Lösungsformeln für Polynomgleichungen erwähnen, auf die wir in diesem Abschnitt nicht näher eingegangen sind.

- Natürlich gilt Korollar 6.14 auch für Polynome $f(X)$ mit $\deg(f) = n$ für jede andere Primzahl $n \geq 5$, denn man kann ähnlich einfach Beispiele mit genau $n - 2$ reellen Nullstellen finden.

Auch für alle anderen Zahlen $n \geq 5$, die keine Primzahlen sind, kann man zeigen, dass es Polynome vom Grad n gibt, deren Galoisgruppe gleich S_n und somit nicht auflösbar ist. Es gibt also für $n \geq 5$ nie eine allgemeine Lösungsformel für Polynomgleichungen n -ten Grades.

- Es gilt auch die Umkehrung von Satz 6.12: Falls die Galoisgruppe des Zerfällungskörpers von f auflösbar ist, so ist $f(X)$ durch Radikale auflösbar, d.h. die Nullstellen von $f(X)$ lassen sich als Ausdrücke schreiben, die nur rationale Zahlen, Grundrechenarten und Wurzeln beinhalten.

Die Unmöglichkeit, eine allgemeine Lösungsformel zu finden, schließt also nicht aus, dass manche Polynomgleichungen sehr wohl Lösungen haben, die sich als Radikale schreiben lassen.

- Die Frage nach der Auflösbarkeit durch Radikale ist nicht ganz identisch mit der Frage nach einer Lösungsformel, denn unter einer Lösungsformel stellen wir uns eine Formel vor, die mithilfe der vier Grundrechenarten und Wurzeln die Lösungen **aus den Koeffizienten** von $f(X)$ berechnet. Wenn ein Polynom aber durch Radikale auflösbar ist, bedeutet dies zunächst nur, dass sich die Lösungen als Radikale schreiben lassen, in denen irgendwelche rationalen Zahlen, aber nicht zwingend nur die Koeffizienten vorkommen dürfen.

Für unseren Widerspruchsbeweis ist das aber natürlich kein Problem: Wenn es überhaupt keinen Radikalausdruck für die Nullstellen gibt, gibt es natürlich auch keine solche Lösungsformel.

6.3 Der Fundamentalsatz der Algebra

Als weitere Anwendung der Galoistheorie geben wir einen Beweis des Fundamentalsatzes der Algebra. Dieser besagt, dass über den komplexen Zahlen jedes Polynom in Linearfaktoren zerfällt.

Es gibt viele interessante Beweise dieses Satzes mit Methoden aus unterschiedlichen Teilgebieten der Mathematik, wie zum Beispiel aus der Topologie oder der Funktionentheorie. Einen rein algebraischen Beweis gibt es hingegen nicht, denn

der Satz macht eine Aussage speziell über den Körper \mathbb{C} , der wiederum eine (algebraische) Erweiterung des Körpers \mathbb{R} ist. Letzterer wird aber mit analytischen Methoden konstruiert (als Vervollständigung von \mathbb{Q}), der Beweis muss also irgendwann Eigenschaften nutzen, welche sich aus dieser Konstruktion ergeben.

Wir werden die folgende Aussage über Polynome mit reellen Koeffizienten benutzen, die sich einfach aus dem Zwischenwertsatz ergibt:

Jedes Polynom $f(X) \in \mathbb{R}[X]$ von ungeradem Grad besitzt eine Nullstelle in \mathbb{R} .

Außerdem werden wir die folgende Eigenschaft der komplexen Zahlen nutzen.

Lemma 6.16. *Es gibt keine Körpererweiterung L/\mathbb{C} mit $[L : \mathbb{C}] = 2$.*

Beweis. Ein Erweiterungskörper L vom Grad 2 über \mathbb{C} würde sich schreiben lassen als $L = \mathbb{C}[\alpha]$ für ein $\alpha \in L$. Für das Minimalpolynom $f(X) \in \mathbb{C}[X]$ von α über \mathbb{C} würde dann gelten $\deg(f) = 2$.

Nun hat aber das Polynom $f(X) = X^2 + pX + q \in \mathbb{C}[X]$ bereits zwei Nullstellen in \mathbb{C} , nämlich

$$z_{1,2} = -\frac{p}{2} \pm \sqrt{\left(\frac{p}{2}\right)^2 - q},$$

wobei $\sqrt{\left(\frac{p}{2}\right)^2 - q}$ eine (von zwei) komplexen Wurzeln aus $\left(\frac{p}{2}\right)^2 - q$ bezeichnet. Dies folgt, da jede komplexe Zahl eine Wurzel besitzt und man somit die Lösungsformel für quadratische Gleichungen (p - q -Formel) auch über \mathbb{C} gilt.

Somit ist ein Polynom vom Grad 2 niemals irreduzibel, also gibt es kein solches L wie oben behauptet. \square

Mit diesen beiden Aussagen (die letztendlich auf der reellen Analysis beruhen) und unserem Wissen aus der Gruppen- und Galoistheorie können wir nun den Fundamentalsatz der Algebra beweisen.

Satz 6.17 (Fundamentalsatz der Algebra). *Jedes Polynom $f(X) \in \mathbb{C}[X]$ mit $\deg(f) \geq 1$ besitzt eine Nullstelle in \mathbb{C} .*

Insbesondere zerfällt jedes solche Polynom in $\mathbb{C}[X]$ also in Linearfaktoren und der Körper \mathbb{C} ist algebraisch abgeschlossen.

Beweis. Sei $f(X) \in \mathbb{C}[X]$ ein Polynom. Wir nehmen an, dass $f(X)$ keine Nullstelle in \mathbb{C} besitzt. Sei Ω ein algebraischer Abschluss von \mathbb{C} , sei $\alpha \in \Omega$ eine Nullstelle von f und betrachte den Körper $\mathbb{C}[\alpha]$. Wir können $\mathbb{C}[\alpha] = \mathbb{R}[i, \alpha]$ auch als Erweiterungskörper von \mathbb{R} betrachten. Die Erweiterung $\mathbb{C}[\alpha]/\mathbb{R}$ ist möglicherweise nicht normal. Deshalb betrachten wir eine leicht abgeänderte Körpererweiterung: Sei $p(X) \in \mathbb{R}[X]$ das Minimalpolynom von α über \mathbb{R} und bezeichne mit L den

Kapitel 6 Anwendungen

Zerfällungskörper von $p(X) \cdot (X^2 + 1)$ über \mathbb{R} . Dann ist L/\mathbb{R} eine endliche Galoiserweiterung (denn Zerfällungskörper bilden immer normale Erweiterungen nach Satz 5.5 und Separabilität folgt aus Korollar 5.19). Wir haben also den Körperturm

$$\begin{array}{c} L \\ | \\ \mathbb{C} \\ 2 | \\ \mathbb{R} \end{array}$$

Daraus sehen wir mit der Gradformel (Satz 4.8), dass $2 \mid [L : \mathbb{R}]$ gilt. Wir schreiben $[L : \mathbb{R}] = 2^k \cdot m$ für ein $k \in \mathbb{N}$ und eine ungerade Zahl $m \in \mathbb{N}$. Dann gilt auch $\#\text{Gal}(L/\mathbb{R}) = [L : \mathbb{R}] = 2^k \cdot m$ nach Lemma 5.29. Nach dem ersten Sylowsatz (Satz 2.59) gibt es dann eine 2-Sylowgruppe $H \subseteq \text{Gal}(L/\mathbb{R})$, also eine Untergruppe mit $\#H = 2^k$.

Nun betrachten wir den Fixkörper L^H . Dann gilt nach dem Hauptsatz der Galoistheorie (Satz 5.32)

$$[L^H : \mathbb{R}] = (\text{Gal}(L/\mathbb{R}) : \text{Gal}(L/L^H)) = (\text{Gal}(L/\mathbb{R})/H) = \frac{\#\text{Gal}(L/\mathbb{R})}{\#H} = \frac{2^k \cdot m}{2^k} = m.$$

Behauptung: Es gilt $L^H = \mathbb{R}$, also $m = 1$.

Sei $y \in L^H$ ein Element und sei $p(X) \in \mathbb{R}[X]$ das Minimalpolynom von y über \mathbb{R} . Dann können wir den Zwischenkörper $\mathbb{R}[y]$ von L^H/\mathbb{R} betrachten und es gilt nach der Gradformel

$$\deg(p) = [\mathbb{R}[y] : \mathbb{R}] \mid [L^H : \mathbb{R}] = m,$$

also ist $\deg(p)$ ungerade. Jedes Polynom in $\mathbb{R}[X]$ von ungeradem Grad hat aber eine Nullstelle in \mathbb{R} und kann daher nur dann irreduzibel sein, wenn $\deg(p) = 1$ ist. Das bedeutet aber $[\mathbb{R}[y] : \mathbb{R}] = 1$ und daher $y \in \mathbb{R}$. Da dies für alle $y \in L^H$ gilt, folgt $L^H = \mathbb{R}$ und somit $m = [L^H : \mathbb{R}] = 1$.

Nun wissen wir also, dass $\#\text{Gal}(L/\mathbb{R}) = 2^k$ und daher

$$\#\text{Gal}(L/\mathbb{C}) = [L : \mathbb{C}] = \frac{[L : \mathbb{R}]}{[\mathbb{C} : \mathbb{R}]} = \frac{2^k}{2} = 2^{k-1}.$$

Behauptung: Es gilt $[L : \mathbb{C}] = 1$, also $L = \mathbb{C}$.

Falls $k \geq 2$ wäre, gäbe es eine Untergruppe $\tilde{H} \subseteq \text{Gal}(L/\mathbb{C})$ mit $\#\tilde{H} = 2^{k-2}$. (Dies haben wir im Beweis des ersten Sylowsatzes (Satz 2.59) gezeigt: Es gibt nicht nur immer eine p -Sylowgruppe, sondern auch eine Gruppe mit p^i Elementen für jede nicht-maximale p -Potenz, die die Gruppenordnung teilt.) Dann gilt

(wieder mit dem Hauptsatz der Galoistheorie) für den Fixkörper $L^{\tilde{H}}$, welcher ein Zwischenkörper von L/\mathbb{C} ist:

$$[L^{\tilde{H}} : \mathbb{C}] = (\text{Gal}(L/\mathbb{C}) : \text{Gal}(L/L^{\tilde{H}})) = (\text{Gal}(L/\mathbb{C}) : \tilde{H}) = \frac{\#\text{Gal}(L/\mathbb{C})}{\#\tilde{H}} = \frac{2^{k-1}}{2^{k-2}} = 2.$$

Dies ist aber nicht möglich, wie wir in Lemma 6.16 gesehen haben. Somit ist also $k = 1$ und daraus folgt die Behauptung.

Wir haben also insgesamt gezeigt, dass $L = \mathbb{C}$, also insbesondere $\alpha \in \mathbb{C}$. Somit hat das Polynom $f(X)$, mit dem wir angefangen haben, eine Nullstelle in \mathbb{C} .

□

6.4 Konstruktionen mit Zirkel und Lineal

Ein klassisches Problem, das bereits auf die antike Mathematik zurückgeht, ist die Frage nach der Durchführbarkeit bestimmter geometrischer Konstruktionen allein mit Zirkel und Lineal.

Genauer bedeutet „Konstruieren mit Zirkel und Lineal“ klassischerweise Folgendes:

Es sei eine Menge von Punkten in einer Ebene gegeben (typischerweise stellen wir uns die zweidimensionale Ebene als komplexe Zahlenebene vor und die gegebenen Punkte sind die Zahlen 0 und 1). Dann kann man folgende Objekte zeichnen:

- (L) Mit dem Lineal: Verbinden zweier bereits gegebener oder bereits konstruierter Punkte durch eine Gerade.
- (Z) Mit dem Zirkel: Zeichnen eines Kreises, dessen Mittelpunkt ein gegebener oder bereits konstruierter Punkt ist und dessen Kreislinie durch einen weiteren gegebenen oder bereits konstruierten Punkt verläuft.

Man erhält dann neue Punkte, indem man

- (I) zwei Geraden wie in (L),
- (II) eine Gerade wie in (L) und einen Kreis wie in (Z) oder
- (III) zwei Kreise wie in (Z)

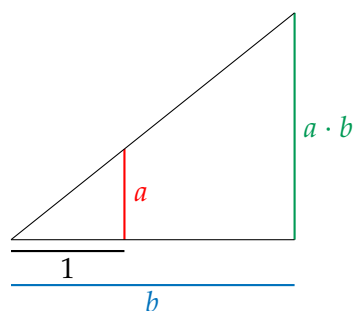
miteinander schneidet. Diese Schnittpunkte gelten dann als „bereits konstruiert“ und man kann mit ihnen weiterarbeiten, indem man wiederum Schritte vom Typ (I), (II) und (III) mit ihnen ausführt.

Lemma 6.18. *Sind die Zahlen $0, 1 \in \mathbb{C}$ sowie zwei beliebige $z, z' \in \mathbb{C}$ gegeben, so lassen sich die Zahlen $z + z', z \cdot z', -z, \frac{1}{z}, i$ (die imaginäre Einheit), $\text{Re}(z), \text{Im}(z), \bar{z}$ (das komplex Konjugierte von z) sowie ein Element $y \in \mathbb{C}$ mit $y^2 = z$ daraus in endlich vielen Schritten vom Typ (I), (II) und (III) konstruieren.*

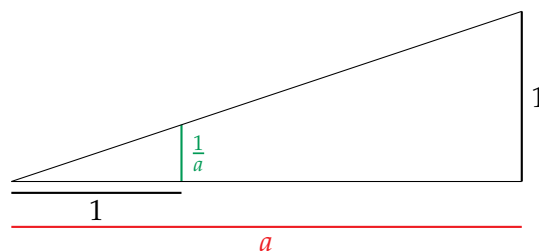
Kapitel 6 Anwendungen

Beweisskizze. Dass $z + z'$ sowie $-z$ aus 0 , z und z' konstruiert werden können, überlegt man sich leicht.

Wir bemerken, dass sich jede komplexe Zahl in der Form $ae^{i\varphi}$ schreiben lässt für $a, \varphi \in \mathbb{R}$ und dass gilt $ae^{i\varphi} \cdot be^{i\psi} = (ab)e^{i(\varphi+\psi)}$. Um $z \cdot z'$ zu konstruieren, genügt es daher, zu zeigen, dass sich Winkel addieren lassen (dies ist einfach) und dass sich aus zwei positiven reellen Zahlen a und b (sowie einer Strecke der Länge 1) eine Strecke mit der Länge $a \cdot b$ konstruieren lässt. Dabei könnte das folgende Bild helfen (in welchem der Strahlensatz zum Einsatz kommt):



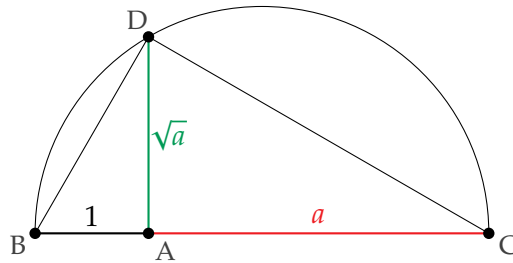
Ebenso reicht es wegen $(ae^{i\varphi})^{-1} = a^{-1}e^{-i\varphi}$, aus einer Strecke der Länge $a \in \mathbb{R}$ (und einer Strecke der Länge 1) eine Strecke der Länge a^{-1} zu konstruieren, um zu zeigen, dass z_1^{-1} aus den gegebenen Daten konstruierbar ist. Dabei hilft dieses Bild:



Die Zahl i lässt sich aus den Zahlen 0 und 1 leicht konstruieren und somit auch $\operatorname{Re}(z)$ und $\operatorname{Im}(z)$ für ein gegebenes $z \in \mathbb{C}$ (einfach durch Projektion auf die reelle bzw. imaginäre Achse). Damit erhält man dann aber auch $\bar{z} = z - 2\operatorname{Im}(z)$.

Schließlich zur Quadratwurzel: Ist $z = ae^{i\varphi}$, so ist eine solche gegeben durch $y = \sqrt{a}e^{i\frac{\varphi}{2}}$. Es genügt also zu zeigen, dass man Winkel halbieren kann (das ist einfach) und dass man aus einer Strecke der Länge $a \in \mathbb{R}$ (und der Strecke der Länge 1) eine Strecke der Länge \sqrt{a} konstruieren kann. Dazu betrachtet man das

folgende Bild:



(Um zu sehen, dass die grüne Strecke wirklich die Länge \sqrt{a} hat, macht man sich klar, dass alle drei Dreiecke in diesem Bild ähnlich zueinander sind und somit gilt $\frac{AD}{1} = \frac{a}{AD}$.) \square

Insbesondere bedeutet dieses Lemma also, dass

Definition 6.19. Eine Zahl $z \in \mathbb{C}$ heißt *konstruierbar*, falls sich der zu z gehörige Punkt in der komplexen Zahlenebene in endlich vielen Schritten mit Operationen der Form (I), (II) und (III) aus den Punkten 0 und 1 konstruieren lässt.

Das obige Lemma 6.18 bedeutet also insbesondere, dass jedes $x \in \mathbb{Q}$ konstruierbar ist (und sogar jedes $z \in \mathbb{Q}[i]$). Man kann aber mit seiner Hilfe noch ein wesentlich genaueres Kriterium für Konstruierbarkeit angeben.

Satz 6.20. Eine Zahl $z \in \mathbb{C}$ ist genau dann konstruierbar, wenn es eine Folge von Körpererweiterungen

$$\mathbb{Q} = K_0 \subseteq K_1 \subseteq K_2 \subseteq \dots \subseteq K_N$$

gibt, sodass $z \in K_N$ und sodass für jedes $j \in \{1, \dots, N\}$ gilt $[K_j : K_{j-1}] = 2$.

Beweis. Ist $z \in \mathbb{C}$ konstruierbar, so entsteht es durch endlich viele Schritte der Form (I), (II) und (III) aus den Zahlen 0 und 1 (und damit o.B.d.A. aus den Zahlen in \mathbb{Q}).

Da die Zahl i konstruierbar ist, sind mit Lemma 6.18 sicher alle Elemente des Körpers $K_1 := \mathbb{Q}[i]$ konstruierbar. Von diesem ausgehend führt man einen der obigen Konstruktionsschritte aus, um einen neuen Punkt α zu erhalten. Damit hat man dann o.B.d.A. auch alle Zahlen in $K_2 := K_1[\alpha]$ konstruiert (wieder wegen Lemma 6.18). Mit diesen kann man einen weiteren Konstruktionsschritt durchführen und erhält ein Element β , womit dann gezeigt ist, dass alle Elemente in $K_3 := K_2[\beta]$ konstruierbar sind. Dies führt man so lange fort, bis man z konstruiert hat. Man bekommt also insgesamt eine Folge

$$\mathbb{Q} \subseteq K_1 = \mathbb{Q}[i] \subseteq K_2 = \mathbb{Q}[i, \alpha] \subseteq K_3 = \mathbb{Q}[i, \alpha, \beta] \subseteq \dots \subseteq K_N$$

mit $z \in K_N$.

Man muss noch zeigen, dass die Erweiterungen in dieser Folge jeweils Grad 1 oder 2 haben, d.h. dass die „neue Zahl“ $z \in \mathbb{C}$, die man mit Schritten vom Typ (I), (II) und (III) jeweils konstruiert, ein Minimalpolynom vom Grad 1 oder 2 über

Kapitel 6 Anwendungen

dem vorhergehenden Körper hat. Für die Erweiterung $\mathbb{Q}[i]/\mathbb{Q}$ ist das klar. Für alle weiteren Schritte überlegt man sich dies wie folgt:

Sei M ein Körper, welcher i enthält und in dem zu jedem Element auch das komplex Konjugierte enthalten ist (und damit automatisch auch der Real- und Imaginärteil jedes Elementes wieder in M liegt). Wir zeigen, dass für ein $z \in \mathbb{C}$, welches sich aus Elementen von M konstruieren lässt, die Erweiterung $M[z]/M$ entweder trivial oder von Grad 2 ist und dass $M[z]$ wieder abgeschlossen unter komplexer Konjugation ist.

- (I) Schneidet man zwei Geraden durch Punkte $z_1, z_2 \in M$ und $z_3, z_4 \in M$, so muss man das Gleichungssystem

$$\begin{aligned}z &= z_1 + t(z_2 - z_1) \\z &= z_3 + t'(z_4 - z_3)\end{aligned}$$

für reelle Parameter $t, t' \in \mathbb{R}$ lösen. Dies entspricht einem linearen System mit zwei Gleichungen über \mathbb{R} (indem man die beiden rechten Seiten gleichsetzt und Real- um Imaginärteile miteinander vergleicht). Damit sind dann t, t' und somit z bereits im Körper M , also ist $M[z] = M$, also $[M[z] : M] = 1$. (Man kann diesen Erweiterungsschritt also auch einfach weglassen.)

- (II) Schneidet man eine Gerade durch zwei Punkte $z_1, z_2 \in M$ mit einem Kreis mit Mittelpunkt $z_3 \in M$ durch $z_4 \in M$, so muss man das Gleichungssystem

$$\begin{aligned}z &= z_1 + t(z_2 - z_1) \\|z - z_3|^2 &= |z_4 - z_3|^2\end{aligned}$$

für einen reellen Parameter $t \in \mathbb{R}$ lösen. Setzt man die rechte Seite der ersten Gleichung für z in der zweiten Gleichung ein, so erhält man

$$|z_1 + t(z_2 - z_1) - z_3|^2 = |z_4 - z_3|^2$$

und man überlegt sich, dass dies eine quadratische Gleichung für t mit reellen Koeffizienten aus M ist. Damit hat das Minimalpolynom von t über M höchstens Grad 2 und folglich ist $[M[z] : M] = [M[t] : M] \leq 2$.

Außerdem ist t (falls ein passendes existiert, also falls sich Kreis und Gerade tatsächlich schneiden) reell. Ist $f(X) = X^2 + pX + q \in \mathbb{R}[X]$ das Minimalpolynom von t über M , so ist also die Diskriminante $p^2 - 4q \geq 0$, also ist $M[z] = M[t] = M[\sqrt{p^2 - 4q}]$ und es ist leicht zu sehen, dass dieser Körper (wegen $\sqrt{p^2 - 4q} \in \mathbb{R}$) abgeschlossen unter komplexer Konjugation ist.

- (III) Schneidet man einen Kreis mit Mittelpunkt $z_1 \in M$ durch $z_2 \in M$ mit einem Kreis mit Mittelpunkt $z_3 \in M$ durch $z_4 \in M$, so muss man das Gleichungssystem

$$\begin{aligned}|z - z_1|^2 &= |z_2 - z_1|^2 \\|z - z_3|^2 &= |z_4 - z_3|^2\end{aligned}$$

lösen. Dies lässt sich umformen zu

$$\begin{aligned} |z|^2 - z\bar{z}_1 - \bar{z}z_1 + |z_1|^2 &= |z_2 - z_1|^2 \\ |z|^2 - z\bar{z}_3 - \bar{z}z_3 + |z_3|^2 &= |z_4 - z_3|^2 \end{aligned}$$

und subtrahiert man die erste Gleichung von der zweiten, erhält man in der zweiten Zeile

$$z(\bar{z}_1 - \bar{z}_3) + \bar{z}(z_1 - z_3) + |z_3|^2 - |z_1|^2 = |z_4 - z_3|^2,$$

was wiederum äquivalent ist zu

$$2\operatorname{Re}(az) = b$$

mit $a = \bar{z}_1 - \bar{z}_3$ und $b = |z_4 - z_3|^2 + |z_1|^2 - |z_3|^2 \in \mathbb{R}$. Man sieht leicht, dass die Lösung dieser Gleichung die Gerade $z = \frac{1}{a}(\frac{b}{2} + t \cdot i)$ mit $t \in \mathbb{R}$ ist. (Der Term $\frac{b}{2} + t \cdot i$ beschreibt sicher eine Gerade, und Multiplikation mit einer komplexen Zahl ergibt wieder eine Gerade.) Diese verläuft zum Beispiel durch die Punkte $\frac{b}{2a}$ und $\frac{b+i}{2a}$, welche beide in M liegen. Somit kann der Fall (III) auch als Spezialfall von (II) aufgefasst werden, dem Schnitt eines Kreises mit einer Geraden, die alle durch Punkte in M gegeben sind, also gelten auch hier die gewünschten Eigenschaften.

Sei nun umgekehrt bekannt, dass es eine Folge von Körpererweiterungen

$$\mathbb{Q} = K_0 \subseteq K_1 \subseteq K_2 \subseteq \dots \subseteq K_N$$

gibt mit $z \in K_N$ und sodass $[K_j : K_{j-1}] = 2$ für jedes $j \in \{1, \dots, N\}$. Dann gilt also $K_j = K_{j-1}[\alpha_j]$ für ein $\alpha_j \in K_j$, dessen Minimalpolynom über K_{j-1} Grad 2 hat. Sei $f(X) = X^2 + pX + q \in K_{j-1}[X]$ dieses Minimalpolynom. Dann ist

$$\alpha_j = -\frac{p}{2} + \sqrt{\left(\frac{p}{2}\right)^2 - q} \quad \text{oder} \quad \alpha_j = -\frac{p}{2} - \sqrt{\left(\frac{p}{2}\right)^2 - q}.$$

Da $\left(\frac{p}{2}\right)^2 - q \in K_{j-1}$, ist dieses Element nach Lemma 6.18 aus den Elementen von K_{j-1} in endlich vielen Schritten der Form (I), (II) und (III) erhalten werden kann. Insgesamt bedeutet dies also, dass jedes Element in K_N (und damit insbesondere z) in endlich vielen Schritten vom Typ (I), (II) und (III) aus Zahlen in \mathbb{Q} konstruierbar ist, also ist z eine konstruierbare Zahl. \square

Korollar 6.21. Die folgenden Konstruktionen sind mit Zirkel und Lineal unmöglich:

- (i) die Quadratur des Kreises, d.h. eine Konstruktion, die zu einem gegebenen Kreis ein Quadrat gleichen Flächeninhalts konstruiert,
- (ii) die Winkeldreiteilung, d.h. eine Konstruktion, mit deren Hilfe man einen beliebigen Winkel in drei gleiche Teile teilen kann,

Kapitel 6 Anwendungen

(iii) die Würfelverdoppelung (das sogenannte Delische Problem), d.h. eine Konstruktion, die zu einem gegebenen Würfel einen Würfel doppelten Volumens konstruiert.

Außerdem gilt:

(iv) Das regelmäßige n -Eck (mit Ecken auf dem Einheitskreis) ist genau dann mit Zirkel und Lineal konstruierbar, wenn $\varphi(n)$ eine Potenz von 2 ist.

Beweis. (i) Wäre die Quadratur des Kreises möglich, so ließe sich aus dem Einheitsquadrat ein Kreis mit Flächeninhalt 1 konstruieren. Dieser hätte also den Radius $\frac{1}{\sqrt{\pi}}$, man hätte dann also eine Strecke der Länge $\frac{1}{\sqrt{\pi}}$ konstruiert und somit wäre auch π konstruierbar. Die Kreiszahl π ist aber transzendent¹ über \mathbb{Q} und somit in keiner algebraischen (und daher keiner endlichen) Erweiterung von \mathbb{Q} enthalten.

(ii) Wäre die Winkeldreiteilung für beliebige Winkel möglich, so könnte man auch den Winkel $\alpha = \frac{\pi}{3} = 60^\circ$ dreiteilen. Da gleichseitige Dreiecke (und somit dieser Winkel) mit Zirkel und Lineal leicht konstruierbar sind, wäre dann auch der Winkel $\frac{\alpha}{3} = \frac{\pi}{9} = 20^\circ$ konstruierbar und somit die Zahl $\cos(\frac{\pi}{9})$. Man kann zeigen (oder einer trigonometrischen Formelsammlung entnehmen), dass

$$\cos(3x) = 4(\cos(x))^3 - 3\cos(x),$$

und setzt man $x = \frac{\pi}{9}$ und verwendet $\cos(\frac{\pi}{3}) = \frac{1}{2}$, so sieht man, dass $\cos(\frac{\pi}{9})$ Nullstelle des Polynoms

$$8X^3 - 6X - 1$$

ist. Dieses ist irreduzibel in $\mathbb{Z}[X]$, denn wäre es dort reduzibel, so müsste es eine ganzzahlige Nullstelle geben und diese wäre ein Teiler von 1. Man kann aber leicht testen, dass 1 und -1 keine Nullstellen sind. Da das Polynom auch primitiv ist, ist es auch irreduzibel in $\mathbb{Q}[X]$ und somit das Minimalpolynom von $\cos(\frac{\pi}{9})$ über \mathbb{Q} , es gilt also $[\mathbb{Q}[\cos(\frac{\pi}{9})] : \mathbb{Q}] = 3$. Damit kann $\cos(\frac{\pi}{9})$ nicht in einer Erweiterung von \mathbb{Q} vom Grad 2^N enthalten sein. Mit Satz 6.20 bedeutet dies also einen Widerspruch zur angenommenen Konstruierbarkeit von $\cos(\frac{\pi}{9})$.

(iii) Wäre die Würfelverdoppelung möglich, so könnte man aus einer gegebenen Seitenlänge a die Länge $a \cdot \sqrt[3]{2}$ konstruieren. Dann wäre also die Zahl $\sqrt[3]{2}$ konstruierbar. Es gilt aber $[\mathbb{Q}[\sqrt[3]{2}] : \mathbb{Q}] = 3$ und somit kann $\sqrt[3]{2}$ nicht in einem Erweiterungskörper von \mathbb{Q} vom Grad 2^N enthalten sein, ein Widerspruch zur Aussage von Satz 6.20.

(iv) Offensichtlich ist das regelmäßige n -Eck genau dann konstruierbar, wenn die Zahl $\zeta_n := e^{\frac{2\pi i}{n}}$ konstruierbar ist.

¹Dass $\pi \in \mathbb{R}$ transzendent über \mathbb{Q} ist, es also kein Polynom $f(X) \in \mathbb{Q}[X]$ gibt, welches π als Nullstelle hat, haben wir hier nicht bewiesen. Dieses Resultat heißt *Satz von Lindemann*.

Eine Richtung der Behauptung ist recht einfach: Ist ζ_n konstruierbar, so folgt nach Satz 6.20, dass $\varphi(n) = [\mathbb{Q}[\zeta_n] : \mathbb{Q}]$ ein Teiler von 2^N ist, also ist $\varphi(n)$ selbst eine Potenz von 2.

Sei nun umgekehrt bekannt, dass $\varphi(n) = 2^k$ eine Potenz von 2 ist. Wir schreiben $L := \mathbb{Q}[\zeta_n]$. Wir wissen, dass L/\mathbb{Q} eine endliche Galoiserweiterung ist (Satz 5.52) und wir betrachten die Galoisgruppe $G := \text{Gal}(L : \mathbb{Q})$. Über diese wissen wir nach Lemma 5.29, dass $\#G = [L : \mathbb{Q}] = 2^k$. Dann folgt mit sukzessiver Anwendung des ersten Sylowsatzes (Satz 2.59), dass es eine Kette von Untergruppen

$$G \supseteq H_1 \supseteq H_2 \supseteq \dots \supseteq H_k = \{\text{id}\}$$

gibt, wobei $\#H_j = 2^{k-j}$. Außerdem folgt aus dem zweiten und dritten Sylowsatz, dass $H_1 \triangleleft G$ und $H_{j+1} \triangleleft H_j$ für $j \in \{1, \dots, N-1\}$ jeweils Normalteiler sind.

Nach dem Hauptsatz der Galoistheorie erhält man dann eine Kette von Fixkörpern

$$\mathbb{Q} = L^G \subseteq L^{H_1} \subseteq L^{H_2} \subseteq \dots \subseteq L^{H_k} = L.$$

Es gilt weiter $[L^{H_1} : L^G] = (G : H_1) = 2$ und $[L^{H_{j+1}} : L^{H_j}] = (H_j : H_{j+1}) = 2$ für $j \in \{1, \dots, N-1\}$ (wieder nach dem Hauptsatz der Galoistheorie, genauer Satz 5.32(iii), und der obigen Normalteilereigenschaft). Dies ist also eine Folge von Körpererweiterungen wie in Satz 6.20 und es gilt $\zeta_n \in L$, also ist ζ_n konstruierbar. □

Bemerkung 6.22. Man kann (mit wenig Aufwand) auch zeigen, dass die Bedingung „ $\varphi(n)$ ist eine Potenz von 2“ äquivalent ist zu

$$n = 2^m \cdot p_1 \cdot \dots \cdot p_r,$$

wobei $m \in \mathbb{N}_0$ und p_1, \dots, p_r paarweise verschiedene *Fermatsche Primzahlen* sind, d.h. Primzahlen, die sich in der Form $2^{2^l} + 1$ schreiben lassen.

Die einzigen bekannten Fermatschen Primzahlen sind 3, 5, 17, 257 und 65537.

6.5 Ausblick

Auch wenn wir in diesem Kurs viele Konzepte der Algebra kennengelernt haben, gibt es natürlich noch unzählige andere Aspekte zu entdecken. Dieser abschließende Abschnitt soll daher einen kurzen Ausblick auf weiterführende Fragen sowie wichtige Resultate, Themen und Konzepte geben, welche die Algebra für zukünftige Kurse und Studien bereithält.

Zunächst gibt es in der Galoistheorie, mit der wir uns intensiv beschäftigt haben, noch viele weitere interessante Probleme:

- **Unendliche Galoistheorie:** Der Hauptsatz der Galoistheorie, den wir bewiesen haben (Satz 5.32), gilt nur für den Fall einer *endlichen* Galoiserweiterung. Betrachtet man den Fall einer Körpererweiterung L/K , die galoissch, aber möglicherweise nicht endlich ist, so kann man auch in dieser Situation eine Korrespondenz zwischen *bestimmten* (nicht allen!) Untergruppen der Galoisgruppe $G := \text{Gal}(L/K)$ und den Zwischenkörpern von L/K beweisen. Um das Resultat zu formulieren, muss man aber die Galoisgruppe etwas genauer studieren: Auf dieser lässt sich eine *Topologie* definieren (also im Grunde eine Vorschrift, welche Teilmengen man offen oder abgeschlossen nennt). Der verallgemeinerte Hauptsatz liefert dann eine Bijektion

$$\{\text{Zwischenkörper von } L/K\} \xrightleftharpoons[\phi]{\psi} \{\text{abgeschlossene Untergruppen von } G\}.$$

- **Inverse Galoistheorie:** In der Galoistheorie haben wir gelernt, dass man einer Körpererweiterung L/K ihre Galoisgruppe $\text{Gal}(L/K) = \text{Aut}_K(L)$ zuordnen kann. Die umgekehrte Frage lautet: Gibt es zu jeder Gruppe G eine Körpererweiterung L/K , sodass $\text{Gal}(L/K)$ isomorph zu G ist? In anderen Worten: Kommt jede Gruppe als Galoisgruppe vor? Falls man den Grundkörper $K = \mathbb{Q}$ festlegt, ist diese Frage bis heute nicht allgemein gelöst: Man weiß zum Beispiel, dass jede endliche auflösbare Gruppe und jede symmetrische Gruppe S_n als Galoisgruppe einer Erweiterung L/\mathbb{Q} vorkommt. Es ist aber nicht bekannt, ob dies für alle endlichen Gruppen der Fall ist.

Die Ring- und Galoistheorie finden zudem reichlich Anwendung in der **Zahlentheorie**, wo zum Beispiel algebraische Zahlkörper (d.h. endliche Erweiterungen von \mathbb{Q}) und endliche Körper, aber auch Eigenschaften von Primzahlen, p -adische Zahlen und vieles mehr studiert werden.

Auch in der Gruppentheorie gibt es noch einige wichtige grundlegende Resultate, zum Beispiel das Folgende:

- **Klassifikation endlich erzeugter abelscher Gruppen:** Wir haben gesehen, dass es nicht immer leicht ist, festzustellen, welche Gruppen mit einer bestimmten Anzahl an Elementen es gibt. Beschränkt man sich auf *abelsche* Gruppen, die zudem *endlich erzeugt* sind, so gibt es aber einen sehr schönen Klassifikationssatz, der uns sagt, welche solchen Gruppen es gibt. Hierbei heißt eine Gruppe G *endlich erzeugt*, wenn es endlich viele Elemente $g_1, \dots, g_n \in G$ gibt, sodass sich jedes Element als endliches Produkt darstellen lässt, in dem ausschließlich diese Elemente (möglicherweise mehrfach) vorkommen.

Satz (Hauptsatz über endlich erzeugte abelsche Gruppen). *Sei G eine endlich erzeugte abelsche Gruppe, dann gibt es einen Gruppenisomorphismus*

$$G \cong \mathbb{Z}^r \times \mathbb{Z}/q_1\mathbb{Z} \times \dots \times \mathbb{Z}/q_m\mathbb{Z}$$

für ein $r \in \mathbb{N}_0$ und Primzahlpotenzen $q_1 = p_1^{k_1}, \dots, q_m = p_m^{k_m}$ (für ein $m \in \mathbb{N}_0$ und $k_1, \dots, k_m \in \mathbb{N}$). Hierbei müssen die Primzahlen p_1, \dots, p_m nicht paarweise verschieden sein. Die Zahlen q_1, \dots, q_m sind außerdem bis auf Reihenfolge eindeutig bestimmt.

Beim Studium von Ringen haben wir uns in dieser Vorlesung auf *kommutative* Ringe konzentriert. Eine spannende Frage ist also, welche Resultate es für nichtkommutative Ringe gibt. Dies ist relevant, denn viele Ringe, die wir in mathematischen Problemstellungen antreffen, sind nicht kommutativ (z.B. Ringe von Matrizen, Quaternionen, Differentialoperatoren etc.).

Ein Konzept, welches in der weiterführenden Algebra eine große Rolle spielt, ist das eines Moduls:

- **Moduln über Ringen:** Sei R ein Ring mit Eins. Dann kann man den Begriff eines *R-Moduls*² definieren: Dazu kopiert man die Definition eines K -Vektorraums aus der linearen Algebra und ersetzt überall den Körper K durch den Ring R . Da ein Ring R in der Regel kein Körper ist, sind R -Moduln im Allgemeinen schwieriger zu handhaben als Vektorräume. (Andererseits kann man das auch positiv betrachten und sagen, dass Moduln „flexibler“ sind als Vektorräume, denn nicht jede Menge, die uns begegnet, ist ein Körper oder ein Vektorraum.)

Ist R ein Hauptidealbereich, so hat man für R -Moduln ein ähnliches Resultat wie für endlich erzeugte abelsche Gruppen oben.

Satz (Klassifikation endlich erzeugter Moduln über Hauptidealbereichen). Sei R ein Hauptidealbereich und sei M ein endlich erzeugter R -Modul. Dann gibt es einen Isomorphismus von R -Moduln

$$M \cong R^r \times R/(d_1) \times \dots \times R/(d_\ell)$$

für ein $r \in \mathbb{N}_0$ und Elemente $d_1, \dots, d_\ell \in R$ (für ein $\ell \in \mathbb{N}_0$), welche die Teilbarkeitsrelationen $d_1 \mid d_2 \mid \dots \mid d_\ell$ erfüllen. Die Elemente d_1, \dots, d_ℓ sind eindeutig bis auf Multiplikation mit Einheiten bestimmt und heißen die Elementarteiler von M .

Tatsächlich ist der obige Satz über endlich erzeugte abelsche Gruppen ein Spezialfall dieses Satzes über endlich erzeugte R -Moduln: Man kann sich leicht überlegen, dass eine abelsche Gruppe dasselbe ist wie ein \mathbb{Z} -Modul. Um von den q_1, \dots, q_m im obigen Satz zu den d_1, \dots, d_ℓ zu gelangen, nutzt man geschickt den Chinesischen Restsatz.

Ein sehr mächtiges Instrument, das verschiedenen algebraischen (und auch anderen) Strukturen ein gemeinsames Fundament gibt, ist in der höheren Algebra heute unabdingbar:

²Die Betonung im Wort „Modul“ liegt auf der ersten Silbe, der Plural lautet „Moduln“.

- **Kategorientheorie:** Wir haben in unserer bisherigen mathematischen Laufbahn viele verschiedene Arten („Kategorien“) von Strukturen kennengelernt, z.B. Gruppen, Ringe, Vektorräume, Moduln, topologische Räume, etc. In all diesen Theorien gibt es einen Begriff von „guten“ (d.h. strukturerhaltenden) Abbildungen, z.B. Gruppenhomomorphismen, Ringhomomorphismen, lineare Abbildungen, Modulhomomorphismen, stetige Abbildungen etc.

Die Kategorientheorie liefert uns eine einheitliche Sprache für viele dieser Fälle: Man spricht allgemein dann einfach von „Objekten“ und „Morphismen“ und man definiert und untersucht (ohne sich auf eine konkrete aus den obigen Theorien zu beziehen) Begriffe wie beispielsweise den Kern und das Bild einer Abbildung, Quotienten und Produkte, welche ja in vielen dieser konkreten Fälle eine Rolle spielen und bisher jedes Mal neu definiert werden mussten. All diese Begriffe sind in Wirklichkeit Spezialfälle des Konzeptes eines sogenannten *Limes*³. Man kann nun durch kategorientheoretische Argumente (manchmal auch als *general abstract nonsense* bezeichnet) Eigenschaften solcher Konstruktionen beweisen, und erhält diese dann automatisch für viele spezielle Kategorien, in denen es entsprechende Begriffe gibt.

Auch von einem praktischeren Standpunkt kann man sich vielen algebraischen Konzepten nähern: Oft haben wir Existenzaussagen gesehen (für ein Element einer Gruppe mit einer vorgegebenen Ordnung, für ein primitives Element, für einen größten gemeinsamen Teiler, für Basen von Körpererweiterungen oder Minimalpolynome), ohne genau anzugeben, wie man diese explizit bestimmen kann. Es ist daher in vielen Fällen notwendig, sich zu überlegen, ob es beispielsweise Algorithmen gibt, mit denen sich solche algebraischen Objekte konkret berechnen lassen. Dabei können auch Computeralgebrasysteme eine wichtige Rolle spielen.

Wichtige Anwendungen der Algebra finden sich schließlich auch in der Geometrie, denn geometrische Objekte werden oft untersucht, indem man ihnen eine Gruppe zuordnet, aus der man etwas über ihre Geometrie lernen kann. Die **algebraische Geometrie** untersucht geometrische Objekte, die als Nullstellenmengen von Polynomen (in mehreren Variablen) entstehen. In der modernen Formulierung der algebraischen Geometrie spielen die Begriffe von Prim- und maximalen Idealen eine wichtige Rolle. Dabei ergeben sich viele Bezüge zu anderen Gebieten, denn das Studium der algebraischen Geometrie ist auch eng verwoben mit der analytischen Geometrie, der Topologie, der Funktionentheorie sowie der Differentialgeometrie.

³Dem Begriff eines Limes in der Kategorientheorie sind wir – ohne es zu wissen – bereits begegnet: Der algebraische Abschluss eines Körpers K ist der Limes (oder genauer: der Kolimes) aller algebraischen Erweiterungen von K . Zum Beispiel ist der algebraische Abschluss $\overline{\mathbb{F}_p}$ des endlichen Körpers \mathbb{F}_p der Kolimes des Diagramms auf Seite 157.

Englische Begriffe

abelsche Gruppe	abelian group
abgeleitete Gruppe	derived subgroup
Ableitung	derivative
algebraisch	algebraic
alternierende Gruppe	alternating group
Äquivalenzrelation	equivalence relation
auflösbar (durch Radikale)	solvable (in radicals)
Bahn	orbit
Bild	image
Charakteristik	characteristic
Chinesischer Restsatz	Chinese Remainder Theorem
disjunkt	disjoint
Einheit	unit
Einheitswurzel	root of unity
einfach	simple
endlich	finite
euklidischer Ring	Euclidean domain
faktorieller Ring	unique factorization domain (UFD)
Fixkörper	fixed field
Fixpunkt	fixed point
Grad	degree
größter gemeinsamer Teiler (ggT)	greatest common divisor (gcd)
Gruppe	group
Gruppenwirkung	group action
Hauptideal	principal ideal
Hauptidealbereich (HIB)	principal ideal domain (PID)
Hauptidealring (HIR)	principal ideal ring (PIR)
Homomorphismus	homomorphism
Ideal	ideal
Identität	identity
Index	index
Integritätsbereich	integral domain
irreduzibel	irreducible

Isomorphismus	isomorphism
Kern	kernel
kleinstes gemeinsames Vielfaches (kgV)	least common multiple (lcm)
kommutativ	commutative
konstruierbar	constructible
Körper	field
Körpererweiterung	field extension
Kreisteilungskörper/-polynom	cyclotomic field/polynomial
Lösung	solution
maximales Ideal	maximal ideal
Minimalpolynom	minimal polynomial
Nebenklasse	coset
noethersch	Noetherian
normal	normal
Normalisator	normalizer
Normalteiler	normal subgroup
Nullstelle	root (of a polynomial)/zero
Nullteiler	zero divisor
Polynom	polynomial
Primideal	prime ideal
primitiv	primitive
Quotientengruppe/-ring	quotient (or factor) group/ring
Quotientenkörper	field of fractions
Ring	ring
Ring mit Eins	unital ring/ring with identity
separabel	separable
Standgruppe	stabilizer/isotropy group
symmetrische Gruppe	symmetric group
Untergruppe	subgroup
vollkommen	perfect
Zerfallungskörper	splitting field
Zirkel und Lineal	ruler/straightedge and compass
Zykel	cycle

Literatur

- [1] Siegfried Bosch. *Algebra*, 9. Auflage. Springer-Verlag, Berlin 2020.
- [2] Keith Conrad. Expository Papers: *The Sylow theorems, Applications of Galois theory*. Verfügbar unter <https://kconrad.math.uconn.edu/blurbs>.
- [3] Marco Hien. *Algebra*. Springer-Verlag, Berlin 2021.

Index

- abgeleitete Gruppe, 168
- Ableitung
 - formale, 126
- algebraisch abgeschlossener Körper, 108
- algebraische Körpererweiterung, 97
- algebraischer Abschluss, 108
- algebraisches Element, 92
- alternierende Gruppe, 20
- Äquivalenzklasse, 20
- Äquivalenzrelation, 20
- assozierte Elemente, 70
- auflösbar, 168
 - durch Radikale, 173
- Bahn, 30
- Bahngleichung, 34
- Bahnformel, 34
- Bézout
 - Lemma von, 58
- Bézout-Darstellung, 58
- Bild, 13
- Cauchy
 - Satz von, 35
- Charakteristik, 128
- Chinesischer Restsatz
 - als Ringhomomorphismus, 66
 - über simultane Kongruenzen, 65
- disjunkte Zykel, 17
- einfache Körpererweiterung, 91
- Einheit, 44
- Einheitswurzel, 157
 - primitive, 158
- Einsetzungshomomorphismus, 55, 92
- Eisenstein-Kriterium, 82
- Element
 - primitives, 134
- endliche Körpererweiterung, 88
- Erweiterungskörper, 88
- Erweiterungsgrad, 88
- euklidischer Algorithmus, 59
- euklidischer Ring, 56
- Eulersche φ -Funktion, 159
- Faktorgruppe, 24
- faktorieller Ring, 69
- Faktorring, 47
- Fixkörper, 138
- Fixpunkt (einer Gruppenwirkung), 37
- formale Ableitung, 126
- Fortsetzungssatz
 - für einfache Erweiterungen, 105
 - in algebraisch abgeschlossene Körper, 113
- Frobeniushomomorphismus, 149
- Fundamentalsatz der Algebra, 181
- Galoiserweiterung, 138
- Galoisgruppe, 118
- Gauß
 - Lemma von, 76
 - Satz von, 83
- Grad
 - einer Körpererweiterung, 88
 - eines Polynoms, 52
- Gradfunktion, 56
- größter gemeinsamer Teiler (ggT), 57
- Gruppe, 9
 - abelsche, 11
 - abgeleitete, 168

Index

- alternierende, 20
- auflösbare, 168
- symmetrische, 16
- zyklische, 12
- Gruppenhomomorphismus, 13
- Gruppenisomorphismus, 15
- Gruppenoperation, 27
- Gruppenwirkung, 27
- Hauptideal, 48
- Hauptidealbereich, 49
- Hauptidealring, 49
- Hauptsatz der Galoistheorie, 139
- Homomorphiesatz
 - für Gruppen, 26
 - für Ringe, 48
- Homomorphismus
 - von Gruppen, 13
 - von Körpern, 44
 - von Ringen, 43
- Ideal, 46
 - Haupt-, 48
 - maximales, 61
 - Prim-, 60
 - von Elementen erzeugtes, 48
- Index, 32
- Inhalt, 76
- Integritätsbereich, 45
- irreduzibel, 67
- Isotropiegruppe, 30
- kanonische Projektion, 21
- Kern, 13
- kleinstes gemeinsames Vielfaches (kgV), 73
- kommutativer Ring, 42
 - mit Eins, 42
- Kommutator, 168
- Kommutatorreihe, 168
- Kommutatoruntergruppe, 168
- konstruierbare Zahl, 185
- Konstruktionen mit Zirkel und Lineal, 183
- Körper, 44
 - algebraisch abgeschlossener, 108
 - vollkommener/perfekter, 129
- Körperautomorphismus, 44
- Körpererweiterung, 88
 - algebraische, 97
 - einfache, 91
 - endliche, 88
 - galoissche, 138
 - normale, 121
 - separable, 125
- Körpergrad, 88
- Kreisteilungskörper, 159
- Kreisteilungspolynom, 161
- Lagrange
 - Satz von, 33
- Leitkoeffizient, 52
- Lemma von Bézout, 58
- Lemma von Gauß, 76
- Lemma von Zorn, 63
- maximales Ideal, 61
- Minimalpolynom, 93
- Nebenklasse, 21
- noetherscher Ring, 49
- normale Körpererweiterung, 121
- Normalisator, 36
- Normalreihe, 168
- Nullstellenkriterium, 80
- Nullteiler, 45
- nullteilerfrei, 45
- Orbit, 30
- Ordnung
 - einer Gruppe, 32
 - eines Elements, 32
- perfekter Körper, 129
- Permutation, 16
- Polynom, 50
- Polynomring, 51
- Primelement, 67
- Primideal, 60
- primitives Element, 134

Satz vom ..., 134, 155
primitives Polynom, 76
Projektion, 21

Quotientengruppe, 24
Quotientenkörper, 74
Quotientenring, 47

Radikale
 durch ... auflösbar, 173

Reduktion modulo p , 76
Reduktionskriterium, 81
Relation, 20
Repräsentant, 20
Repräsentantensystem, 21
Ring, 41
 euklidischer, 56
 faktorieller, 69
 Hauptideal-, 49
 kommutativer, 42
 mit Eins, 42
 noetherscher, 49
 nullteilerfreier, 45
 Polynom-, 51
Ringhomomorphismus, 43
Ringisomorphismus, 43

Satz vom primitiven Element, 134,
 155
Satz von Cauchy, 35

Satz von Gauß, 83
Satz von Lagrange, 33
separabel, 125
Separabilitätsgrad, 130
Signum, 19
Stabilisator, 30
Standgruppe, 30
Sylowgruppe, 36
Sylowsätze, 36
symmetrische Gruppe, 16

Teilkörper, 88
Transposition, 16
transzendent, 92

Untergruppe, 12
 zyklische, 12
Unterkörper, 88

vollkommener Körper, 129
Vorzeichen (einer Permutation), 19

Zerfällungskörper, 100
Zirkel und Lineal, 183
Zorn
 Lemma von, 63
Zwischenkörper, 89
Zykel, 16
 disjunkte, 17
zyklische Gruppe, 12