Einführung in die Algebra

Andreas Gathmann

Vorlesungsskript TU Kaiserslautern 2010/11

Inhaltsverzeichnis

0. Einleitung und Motivation

Die Vorlesung „Einführung in die Algebra“ verfolgt zwei Ziele. Einerseits wollen wir aus rein algebraischer Sicht das in der Vorlesung „Algebraische Strukturen“ begonnene Studium von Gruppen, Ringen und Körpern fortsetzen. Wir werden demzufolge viele Resultate dieser vorangegangenen Vorlesung benutzen; in diesem Skript verwende ich dazu Referenzen auf mein Skript [G]. Die Ergebnisse der Einführung in die Algebra gehören wie die der Algebraischen Strukturen zum Werkzeugkasten eines jeden Algebraikers; sie werden euch später sicher immer wieder begegnen, wenn ihr vertiefende Vorlesungen im Bereich der Algebra hört.

Andererseits sind diese algebraischen Strukturen ursprünglich natürlich nicht aus purem Interesse an abstrakter Algebra eingeführt worden. Sie dienten vielmehr als Hilfsmittel, um konkrete klassische mathematische Probleme zu lösen, die oftmals sehr anschaulich und geometrisch waren. Im Rahmen dieser Vorlesung werden wir einige dieser klassischen Probleme untersuchen und sie dann nach und nach mit Hilfe der Algebra lösen. Diese anschaulichen und wichtigen Probleme, deren Lösung also das zweite Ziel der „Einführung in die Algebra“ sind, können uns somit im Laufe der Vorlesung als Motivation und Leitfaden dienen. Ich möchte hier einige von ihnen in diesem einführenden Kapitel vorstellen.

Problem 0.1 (Fundamentalsatz der Algebra). Der wohl bekannteste und wichtigste Satz der Algebra ist der sogenannte *Fundamentalsatz der Algebra*, dessen Aussage ihr bereits alle kennt. Er besagt, dass jedes nicht-konstante komplexe Polynom

$$f = t^n + a_{n-1}t^{n-1} + \cdots + a_1 t + a_0 \quad \in \mathbb{C}[t]$$

eine Nullstelle hat, also dass es ein $x \in \mathbb{C}$ gibt mit $f(x) = 0$. Hat man eine solche Nullstelle, so kann man das gegebene Polynom natürlich ohne Rest durch $t - x$ teilen und erhält so ein neues Polynom vom Grad $n-1$, auf das man den Fundamentalsatz erneut anwenden kann. Der Fundamentalsatz ist also äquivalent dazu, dass sich jedes Polynom vom Grad n über $\mathbb{C}$ als Produkt von n *linearen* Polynomen schreiben lässt. Damit hat ein solches Polynom stets n Nullstellen (von denen einige übereinstimmen können).

Den Fundamentalsatz der Algebra kann man auf viele verschiedene Arten beweisen, z. B. mit Hilfe der Topologie oder der Funktionentheorie. Wir werden in dieser Vorlesung einen algebraischen Beweis geben (siehe Satz 7.25).

Problem 0.2 (Auflösbarkeit von Polynomgleichungen). Wir betrachten wieder eine komplexe polynomiale Gleichung

$$t^n + a_{n-1}t^{n-1} + \cdots + a_1 t + a_0 = 0$$

mit $n \geq 1$ und $a_i \in \mathbb{C}$. Wie wir gerade erwähnt haben, hat diese Gleichung nach dem Fundamentalsatz der Algebra genau n Lösungen (von denen einige übereinstimmen können). Für kleines n lassen sich diese Lösungen natürlich leicht explizit angeben: für $n = 1$ hat man einfach

$$t = -a_0,$$

und für $n = 2$ nach der aus der Schule bekannten Formel

$$t = -\frac{a_1}{2} \pm \sqrt{\frac{a_1^2}{4} - a_0}.$$

Für höhere Grade kennt ihr vermutlich keine derartigen Lösungsformeln. In der Schule begnügt man sich z. B. für kubische Polynomgleichungen ja in der Regel mit der Methode, dass man eine Nullstelle „rät“ — sofern dies möglich ist — und diese dann abspaltet, so dass man eine quadratische Gleichung übrig behält, die man dann wieder wie oben lösen kann.

Es gibt jedoch auch für $n = 3$ noch eine explizite Lösungsformel. In der Schule betrachtet man sie in der Regel nicht, weil sie zum einen ein bisschen zu kompliziert ist, um sie sich merken zu können, und sie zum anderen erfordert, dass man dritte Wurzeln aus komplexen Zahlen ziehen kann. Es handelt sich hierbei um die im 16. Jahrhundert gefundene **Cardanische Formel**

$$t = \sqrt[3]{-q + \sqrt{q^2 + p^3}} + \sqrt[3]{-q - \sqrt{q^2 + p^3}}, \qquad (*)$$

wobei

$$p = \frac{3a_1 - a_2^2}{9} \quad \text{und} \quad q = \frac{a_2^3}{27} - \frac{a_1 a_2}{6} + \frac{a_0}{2}$$

(und in $(*)$ die „richtigen" komplexen dritten Wurzeln gewählt werden müssen — für jede der beiden dritten Wurzeln gibt es ja drei Möglichkeiten, aber nur 3 der insgesamt $3 \cdot 3 = 9$ Kombinationsmöglichkeiten liefern in der Tat eine Nullstelle des Polynoms).

In der Tat gibt es auch für den Fall $n = 4$ noch eine (natürlich noch komplizierte) Lösungsformel im obigen Stil, d. h. ein Verfahren, das aus den gegebenen Koeffizienten a_i der Gleichung durch Körperoperationen (Addition, Subtraktion, Multiplikation und Division) und Ziehen beliebiger Wurzeln die exakten Lösungen bestimmt. Diese sogenannte Formel von Ferrari wurde ebenfalls bereits im 16. Jahrhundert gefunden.

Natürlich haben die Mathematiker dann nach entsprechenden Formeln für höhere Grade gesucht — allerdings erfolglos. Es hat sehr lange gedauert, bis Abel im 19. Jahrhundert erkannte, dass es für $n \geq 5$ *keine derartige Lösungsformel geben kann*. Dieses überraschende Resultat benötigt zum Beweis natürlich ganz andere Methoden als im Fall $n \leq 4$, wo man eine konkrete Formel einfach angeben und ihre Korrektheit nachrechnen kann. Obwohl man dies von der Problemstellung her gar nicht vermuten würde, benötigt man hierzu Gruppentheorie. Wir werden in Definition 5.10 und Lemma 5.11 (a) einem Polynom f vom Grad n eine Untergruppe G der symmetrischen Gruppe S_n zuordnen und die Frage, ob sich die Nullstellen von f aus den Koeffizienten durch Körperoperationen und Wurzelziehen bestimmen lassen, in Definition 8.6 und Folgerung 8.12 in eine gewisse Eigenschaft der Untergruppe G übersetzen. Von dieser Eigenschaft können wir in Folgerung 8.10 dann zeigen, dass sie für Untergruppen von S_n für $n \leq 4$ stets erfüllt ist, für $n \geq 5$ jedoch nicht.

Wir sollten aber noch einmal deutlich betonen, dass dies natürlich *nicht* bedeutet, dass Polynomgleichungen vom Grad $n \geq 5$ keine exakten Lösungen besitzen — das wäre ja auch ein Widerspruch zum Fundamentalsatz. Es bedeutet nur, dass sich die exakten Lösungen im Allgemeinen nicht mehr durch Körperoperationen und fortgesetztes Wurzelziehen aus den Koeffizienten des Polynoms berechnen lassen.

Problem 0.3 (Konstruktionen mit Zirkel und Lineal). Ein sehr klassisches (und zunächst geometrisch erscheinendes) Problem ist die Konstruktion bestimmter Objekte in der Ebene mit Zirkel und Lineal, wie ihr sie sicher schon in der Schule durchgeführt habt. Dabei seien die folgenden beiden **Elementarkonstruktionen** erlaubt:

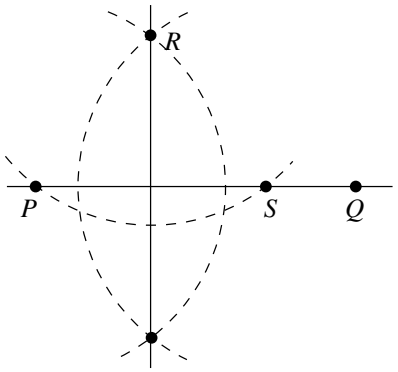
- man zeichnet mit dem Lineal eine Gerade durch P und Q (wobei P und Q zwei bereits konstruierte Punkte sind);
- man zeichnet mit dem Zirkel einen Kreis durch P mit Radius $\overline{QR}$ (wobei P, Q und R drei bereits konstruierte Punkte sind).

Bei diesen beiden Operationen entstehende Schnittpunkte aus Geraden und Kreisen gelten dann als konstruiert.

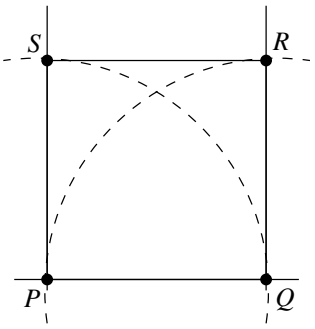
Ein paar Beispiele solcher möglichen Konstruktionen sind:

(a) Gegeben seien eine Gerade PQ und ein Punkt R (der auf der Geraden PQ liegen darf oder auch nicht). Man konstruiere die Gerade durch R, die auf PQ senkrecht steht.

Lösung: Man zeichne einen Kreis um R mit Radius $\overline{PR}$; die beiden Schnittpunkte mit der gegebenen Geraden seien P und S. Mit dem gleichen Radius zeichne man nun zwei Kreise um P und S. Die Verbindungslinie der Schnittpunkte dieser beiden Kreise ist dann die gesuchte Gerade. Die Konstruktion ist im Bild unten links dargestellt.



(a)



(b)

(b) Man konstruiere ein Quadrat.

Lösung: Man starte mit einer beliebigen Strecke $\overline{PQ}$. Dann konstruiere man wie in (a) die Senkrechten zu PQ durch P und Q und trage die Strecke $\overline{PQ}$ auf diesen beiden Senkrechten mit dem Zirkel ab. Die Konstruktion ist im Bild oben rechts dargestellt.

Es gibt aber auch einige geometrische Probleme, deren Lösung mit Zirkel und Lineal trotz jahrhundertelanger Suche nicht gefunden werden konnte, und von denen man erst viel später mit Hilfe der Algebra zeigen konnte, dass sie in der Tat nicht lösbar sind:

(A) (**Quadratur des Kreises**) Zu einem gegebenen Kreis konstruiere man ein Quadrat mit gleichem Flächeninhalt. Dies ist mit Zirkel und Lineal nicht möglich — in der Tat steht der Begriff der „Quadratur des Kreises“ umgangssprachlich ja auch für ein unlösbares Problem. Hat der ursprüngliche Kreis den Radius a und das gesuchte Quadrat die Seitenlänge b, so verlangen wir offensichtlich $\pi a^2 = b^2$, wir wollen aus einer Strecke der Länge a also eine Strecke der Länge $b = \sqrt{\pi}\,a$ konstruieren. Wir werden dieses Problem in Beispiel 2.23 genauer untersuchen.

(B) (**Würfelverdoppelung**) Zu einem gegebenen Würfel konstruiere man einen Würfel doppelten Volumens. (Damit ist gemeint: es sei die Seitenlänge a eines solchen Würfels gegeben; man konstruiere die Seitenlänge $\sqrt[3]{2}\,a$ des Würfels mit dem doppelten Volumen.) Auch diese Konstruktion ist mit Zirkel und Lineal nicht möglich, wie wir in Beispiel 2.23 beweisen werden.

(C) (**Konstruktion des regelmäßigen n-Ecks**) Zu gegebenem n konstruiere man ein regelmäßiges n-Eck mit Zirkel und Lineal (wie wir es z. B. für $n = 4$ in (b) oben getan haben). Wir werden in Folgerung 3.33 und 7.8 sehen, dass dies nur für bestimmte n möglich ist — z. B. ist es für $n = 3, 4, 5, 6, 8, 10$ möglich, für $n = 7$ und $n = 9$ jedoch nicht.

Die Galoistheorie, die zum Beweis solcher Aussagen (und auch für die Lösung der Probleme 0.1 und 0.2) nötig ist und die wir in dieser Vorlesung behandeln werden, stammt aus dem frühen 19. Jahrhundert, ist also ebenfalls schon relativ alt. Dennoch gibt es übrigens immer noch viele Hobbymathematiker, die die Galoistheorie nicht verstehen bzw. ihre Ergebnisse nicht glauben, und die immer noch versuchen, diese Konstruktionsaufgaben zu lösen und auf diese Art berühmt zu werden. An vielen bekannten Universitäten gibt es daher sogar Mitarbeiter, deren Aufgabe es (unter anderem) ist, die dort zahlreich ankommenden Briefe solcher Hobbymathematiker mit ihren angeblichen Lösungen zu beantworten.

Aufgabe 0.4. Auf einem Blatt Papier sei ein gleichseitiges Dreieck gegeben. Konstruiert daraus ein flächengleiches Quadrat mit Zirkel und Lineal.

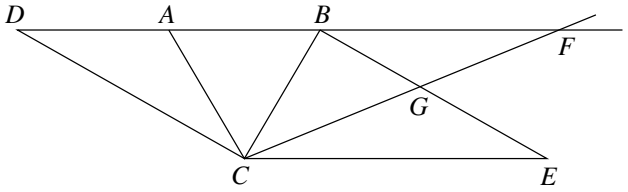
Aufgabe 0.5. In dieser Aufgabe bezeichnen $ABCDE$ im Uhrzeigersinn die Ecken eines regelmäßigen Fünfecks.

(a) Man zeige, dass $\overline{AB}$ die Strecke $\overline{AC}$ im „goldenen Schnitt“ teilt, d. h. dass
$$\frac{\overline{AB}}{\overline{AC}} = \frac{\overline{AC}-\overline{AB}}{\overline{AB}}$$
gilt, und schließe daraus, dass $\overline{AC} = \frac{1}{2}(\sqrt{5}+1)\cdot\overline{AB}$.

(b) Auf einem Blatt Papier sei nur die Strecke $\overline{AB}$ gegeben. Mit Hilfe von (a) konstruiere man daraus das gesamte Fünfeck $ABCDE$ mit Zirkel und Lineal.

Aufgabe 0.6. Stellt euch vor, ihr seid am Fachbereich Mathematik der TU Kaiserslautern angestellt und bekommt einen Brief von einem Hobbymathematiker, der den Unmöglichkeitsbeweis der Würfelverdoppelung mit Zirkel und Lineal nicht versteht und meint, doch eine Lösung gefunden zu haben. Er schreibt:

> Es sei $\overline{AB}$ die gegebene Kantenlänge des ursprünglichen Würfels. Konstruiere den Punkt C so, dass ABC ein gleichseitiges Dreieck ist. Nun sei $D \neq B$ der Punkt auf der Geraden AB mit $\overline{AD} = \overline{AB}$. Vervollständige die Strecken $\overline{BD}$ und $\overline{CD}$ zu einem Parallelogramm $BDCE$. Nun zeichne eine Gerade durch C so, dass $\overline{FG} = \overline{AB}$, wobei F und G die Schnittpunkte dieser Geraden mit AB und BE bezeichnen. Wie man leicht nachrechnet ist dann $\overline{CG} = \sqrt[3]{2}\cdot\overline{AB}$ die gesuchte Kantenlänge des Würfels mit dem doppelten Volumen.



Was schreibt ihr ihm zurück? Liefert seine Konstruktion überhaupt die richtige Lösung, d. h. stimmt es wirklich dass $\overline{CG} = \sqrt[3]{2}\cdot\overline{AB}$? Wenn ja, widerspricht seine Konstruktion dann nicht der in Problem 0.3 (B) angegebenen Unmöglichkeitsaussage?

1. Körper und Körpererweiterungen

Wir beginnen nun mit dem eigentlichen Studium von Gruppen, Ringen und Körpern. Die in der Einleitung vorgestellten Probleme haben dabei zunächst einmal hauptsächlich mit Körpern (und dabei insbesondere mit dem Körper der komplexen Zahlen) zu tun. Auch die geometrisch erscheinenden Fragestellungen zu Konstruktionen mit Zirkel und Lineal aus Problem 0.3 werden wir in Satz 1.12 über gewisse Unterkörper von $\mathbb{C}$ in die Sprache der Algebra übersetzen. Im Gegensatz zu den „Algebraischen Strukturen“, wo wir zunächst Gruppen und später dann Ringe und Körper untersucht haben, wollen wir daher hier den umgekehrten Weg gehen, zuerst Körper studieren und uns erst später genauer mit Gruppen beschäftigen.

Aus den „Algebraischen Strukturen“ wisst ihr sicher noch, was ein Körper ist: eine Menge K mit zwei Verknüpfungen „$+$“ und „$\cdot$“, so dass $(K,+)$ eine abelsche Gruppe (mit neutralem Element $0 = 0_K$) ist, $(K\backslash\{0\},\cdot)$ ebenfalls eine abelsche Gruppe (mit neutralem Element $1 = 1_K$) ist, und das Distributivgesetz gilt [G, Definition 7.6 (b) und Bemerkung 7.7 (b)]. Wir wollen hier nun den in der Praxis besonders wichtigen Fall untersuchen, dass zwei solche Körper ineinander liegen.

Definition 1.1 (Körpererweiterungen)**.** Sind K und L zwei Körper mit $K \subset L$, so heißt K **Teilkörper** bzw. **Unterkörper** von L, und L **Erweiterungskörper** von K. Wir schreiben dies auch als $K \leq L$ oder L/K und sagen, L/K (gesprochen: „L über K“) ist eine **Körpererweiterung**. Im Fall $K \leq Z \leq L$ nennt man Z einen **Zwischenkörper** der Körpererweiterung L/K.

Beachte also, dass L/K für zwei Körper K und L *keine mathematische Konstruktion* wie etwa einen Faktorring bezeichnet, sondern nur eine andere (und letztlich historisch bedingte) Schreibweise für die Relation $K \subset L$ ist.

Beispiel 1.2.

(a) Natürlich gilt $\mathbb{Q} \leq \mathbb{R} \leq \mathbb{C}$.

(b) Für jede Primzahl p wissen wir, dass $\mathbb{Z}_p = \mathbb{Z}/p\mathbb{Z}$ (mit den von $\mathbb{Z}$ induzierten Operationen) ein Körper mit p Elementen ist [G, Satz 7.10]. Diese Körper sind keine Teilkörper von $\mathbb{R}$.

(c) Die Menge der reellen *rationalen Funktionen*

$$\mathbb{R}(t) := \left\{ t \mapsto \frac{f}{g} : \ f,g \in \mathbb{R}[t] \text{ mit } g \neq 0 \right\}$$

ist ein Körper, der $\mathbb{R}$ (als konstante Funktionen) als Unterkörper enthält. Analog kann man $\mathbb{Q}(t)$ und $\mathbb{C}(t)$ als die Körper rationaler oder komplexer rationaler Funktionen definieren.

Bemerkung 1.3.

(a) Ist L ein Körper und $K \subset L$ eine Teilmenge von L, so ist K offensichtlich genau dann ein Unterkörper von L, wenn gilt

- $0,1 \in K$, und
- für alle $x,y \in K$ liegen auch $x+y$, $-x$, $x \cdot y$ und (für $x \neq 0$) x^{-1} in K (d. h. K ist abgeschlossen bezüglich der Körperoperationen).

Dies beweist man genauso wie das Untergruppen- oder Unterringkriterium in den „Algebraischen Strukturen“ [G, Satz 3.3 und 7.23].

(b) Ist $f : K \to L$ ein beliebiger Morphismus von Körpern, so ist f bereits injektiv: ist nämlich $x \in K$ mit $x \neq 0$, so ist nach Definition eines Körperhomomorphismus [G, Definition 7.25 (a)].

$$1 = f(1) = f(x \cdot x^{-1}) = f(x) \cdot f(x^{-1})$$

und damit notwendigerweise $f(x) \neq 0$. Es folgt unmittelbar $\operatorname{Ker} f = \{0\}$, d. h. f ist injektiv. Wir können damit K durch die Abbildung f als Unterkörper von L auffassen. *Jeder Körperhomomorphismus führt also automatisch zu einer Körpererweiterung.*

(c) Es seien L ein Körper sowie $K_i \leq L$ Unterkörper für alle i aus einer beliebigen Indexmenge I. Dann ist nach (a) klar, dass auch der Durchschnitt $\bigcap_{i \in I} K_i$ wieder ein Unterkörper von L ist — da alle K_i die 0 und 1 enthalten sowie abgeschlossen unter den Körperoperationen sind, gilt dies natürlich auch für den Durchschnitt. (Möchte man dies formal aufschreiben, müsste man dies analog zum Fall von Untergruppen in [G, Bemerkung 3.9 (b)] tun.)

Einen einfachen Fall hiervon erhält man, wenn man einfach *alle* Unterkörper von L miteinander schneidet. Dies führt zur folgenden Definition.

Definition 1.4 (Primkörper)**.** Ist L ein Körper, so heißt der Durchschnitt

$$P(L) := \bigcap_{K \leq L} K$$

über alle Teilkörper von L der **Primkörper** von L. Nach Bemerkung 1.3 (c) gilt stets $P(L) \leq L$.

Beispiel 1.5. Wir wollen den Primkörper von $L = \mathbb{R}$ berechnen. Es sei dazu $K \leq \mathbb{R}$ beliebig. Nach Definition eines Teilkörpers sind dann zunächst 0 und 1 in K, wegen der Abgeschlossenheit bezüglich Addition und Subtraktion dann auch $2 = 1+1$, $3 = 1+1+1$, ... und analog alle ganzen Zahlen, und wegen der Abgeschlossenheit bezüglich der Division schließlich auch alle Brüche $\frac{p}{q}$ mit $p, q \in \mathbb{Z}$, $q \neq 0$. Für jeden solchen Teilkörper K gilt also $K \supset \mathbb{Q}$.

Damit muss auch der Durchschnitt $P(\mathbb{R})$ aller dieser Teilkörper $\mathbb{Q}$ umfassen. Andererseits ist aber $\mathbb{Q}$ natürlich einer der Teilkörper von $\mathbb{R}$, über den in der Definition von $P(\mathbb{R})$ der Schnitt gebildet wird. Also folgt auch die umgekehrte Inklusion $P(\mathbb{R}) \subset \mathbb{Q}$ und damit schließlich $P(\mathbb{R}) = \mathbb{Q}$.

Genauso ergibt sich natürlich auch für die komplexen Zahlen $P(\mathbb{C}) = \mathbb{Q}$. Dies ist kein Zufall — es gibt nur sehr wenige verschiedene Möglichkeiten für Primkörper, wie wir gleich in Aufgabe 1.11 sehen werden. Für dieses Resultat benötigen wir noch den Begriff der Charakteristik eines Körpers, der die wohl wichtigste Eigenschaft eines Körpers beschreibt.

Definition 1.6 (Charakteristik eines Körpers)**.** Es sei K ein Körper. Für $n \in \mathbb{Z}$ setzen wir wie üblich

$$n \cdot 1_K := \underbrace{1_K + \cdots + 1_K}_{n\text{-mal}} \quad \in K$$

(wobei dieser Ausdruck für $n < 0$ natürlich als $(-n)$-fache Aufsummierung von -1_K zu verstehen ist). Gibt es ein $n > 0$, so dass $n \cdot 1_K = 0_K$ ist, so heißt das kleinste solche n die **Charakteristik** $\operatorname{char} K$ von K. Andernfalls setzt man $\operatorname{char} K := 0$.

Beispiel 1.7.

(a) Natürlich ist $\operatorname{char}\mathbb{Q} = \operatorname{char}\mathbb{R} = \operatorname{char}\mathbb{C} = 0$ und $\operatorname{char}\mathbb{Z}_p = p$ für alle Primzahlen p.

(b) Ist L/K eine Körpererweiterung, so gilt stets $\operatorname{char} K = \operatorname{char} L$ (da $1_K = 1_L$ und $0_K = 0_L$ ist und somit $n \cdot 1_K = 0_K$ genau dann in K gilt wenn $n \cdot 1_L = 0_L$ in L ist).

Bemerkung 1.8. Möchte man Definition 1.6 „algebraisch eleganter“ ausdrücken, so könnte man dies auch so formulieren: man betrachtet den Ringhomomorphismus $\mathbb{Z} \to K$, $n \mapsto n \cdot 1_K$. Der Kern dieses Morphismus ist ein Ideal von $\mathbb{Z}$ [G, Lemma 8.4] und damit von der Form (m) für ein eindeutig bestimmtes $m \in \mathbb{N}$ [G, Beispiel 8.3 (a)]. Diese Zahl m heißt dann die Charakteristik von K. Beachte, dass diese alternative Definition gleichermaßen in den Fällen $m > 0$ und $m = 0$ funktioniert.

Lemma 1.9. *Ist die Charakteristik eines Körpers ungleich Null, so ist sie eine Primzahl.*

Beweis. Angenommen, K wäre ein Körper mit $\operatorname{char} K = n = p \cdot q$, wobei $1 < p, q < n$. Dann wäre

$$0_K = \underbrace{1_K + \cdots + 1_K}_{n\text{-mal}} = \underbrace{(1_K + \cdots + 1_K)}_{p\text{-mal}} \cdot \underbrace{(1_K + \cdots + 1_K)}_{q\text{-mal}}.$$

Da Körper aber keine Nullteiler außer der 0 besitzen [G, Lemma 7.8 (c)], folgt daraus bereits $p \cdot 1_K = 0_K$ oder $q \cdot 1_K = 0_K$ — im Widerspruch dazu, dass n die *kleinste* positive Zahl mit $n \cdot 1_K = 0_K$ sein soll. Also kann es keine Darstellung $n = p \cdot q$ wie oben geben, d. h. n ist eine Primzahl. □

Bemerkung 1.10. Ob man hauptsächlich Körper der Charakteristik Null oder solche positiver Charakteristik betrachtet, hängt sehr vom jeweiligen Anwendungsgebiet der Algebra ab. So werden wir für die in der Einleitung genannten Probleme hauptsächlich Unterkörper von $\mathbb{C}$, also solche mit Charakteristik Null benötigen, während z. B. in der Gruppentheorie oder Zahlentheorie die Körper mit positiver Charakteristik eine weit größere Rolle spielen. Es ist eine besondere Stärke der Algebra, dass sie in weiten Teilen beide Fälle mit derselben Theorie behandeln kann, obwohl sich Körper mit positiver Charakteristik in der Praxis sehr deutlich von denen mit Charakteristik Null unterscheiden.

Der Zusammenhang zwischen der Charakteristik eines Körpers und seinem Primkörper ist sehr einfach, wie die folgende Aufgabe zeigt.

Aufgabe 1.11. Es sei K ein Körper. Man zeige:

(a) Ist $\operatorname{char} K = 0$, so ist $P(K)$ isomorph zu $\mathbb{Q}$. Jeder Körper der Charakteristik 0 ist also ein Erweiterungskörper von $\mathbb{Q}$.

(b) Ist $\operatorname{char} K = p > 0$, so ist $P(K)$ isomorph zu $\mathbb{Z}_p$. Jeder Körper der Charakteristik $p > 0$ ist also ein Erweiterungskörper von $\mathbb{Z}_p$.

(Hinweis: Untersuche den bereits in Bemerkung 1.8 erwähnten Ringhomomorphismus $\mathbb{Z} \to K$, $n \mapsto n \cdot 1_K$.)

Als Anwendung der gerade eingeführten Begriffe wollen wir nun sehen, wie sich die Probleme der Auflösbarkeit von Polynomgleichungen und der Konstruktionen mit Zirkel und Lineal aus der Einleitung in die Sprache der Körpererweiterungen übersetzen lassen. Bei den Konstruktionen mit Zirkel und Lineal müssen wir dabei zunächst einmal sehen, wie diese überhaupt mit Körpern zusammenhängen. Die Grundidee hierfür ist, die Zeichenebene mit der Ebene der komplexen Zahlen $\mathbb{C}$ zu identifizieren. Wir starten nun mit einer Menge $M \subset \mathbb{C}$ von ursprünglich gegebenen Punkten. Diese Menge wird in der Regel recht klein sein, muss aber natürlich mindestens zwei Punkte enthalten, da sonst überhaupt keine Elementarkonstruktionen wie in Problem 0.3 ausführbar sind (sowohl um eine Gerade als auch um einen Kreis zu zeichnen braucht man ja mindestens zwei Punkte). Wir können die komplexe Ebene daher so mit der Zeichenebene identifizieren, dass die Punkte $0 \in \mathbb{C}$ und $1 \in \mathbb{C}$ in M liegen. Der entscheidende Punkt ist nun, dass die Menge *aller* aus M konstruierbaren Punkte ein Unterkörper von $\mathbb{C}$ ist.

Satz 1.12. *Es sei $M \subset \mathbb{C}$ mit $0, 1 \in M$ gegeben. Weiterhin bezeichne $\hat{M} \subset \mathbb{C}$ die Menge aller aus M mit Zirkel und Lineal konstruierbaren Punkte der Ebene. Dann gilt:*

(a) *$\hat{M}$ ist ein Körper mit $\mathbb{Q} \leq \hat{M} \leq \mathbb{C}$.*

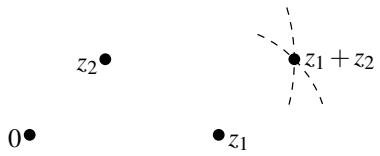
(b) *Ist $z \in \hat{M}$, so liegt auch die zu z konjugiert komplexe Zahl $\bar{z}$ in $\hat{M}$.*

(c) *Ist $z \in \hat{M}$, so liegen auch die beiden komplexen Quadratwurzeln $\pm\sqrt{z}$ in $\hat{M}$.*

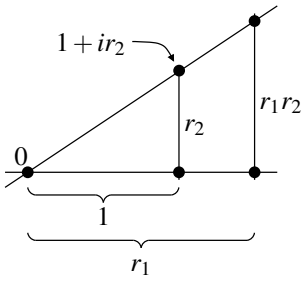
01

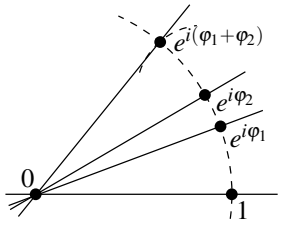
Beweis. Da 0 und 1 nach Voraussetzung in $\hat{M}$ liegen, müssen wir nach Bemerkung 1.3 (a) nur zeigen, dass $\hat{M}$ abgeschlossen unter den Körperoperationen, der komplexen Konjugation und dem Ziehen von Quadratwurzeln ist, d. h. dass sich diese algebraischen Operationen mit Zirkel und Lineal durchführen lassen (dass $\hat{M}$, wie in (a) zusätzlich noch behauptet, ein Erweiterungskörper von $\mathbb{Q}$ ist, folgt aus Aufgabe 1.11 (a)). Wir zeigen diese Abgeschlossenheit exemplarisch für die Addition, die Multiplikation und das Wurzelziehen, da die anderen Fälle analog (bzw. einfacher) sind.

- *Addition:* Es seien $z_1, z_2 \in \hat{M}$, also konstruierbar. Der Punkt $z_1 + z_2$ ist offensichtlich der, der die drei Punkte 0, z_1 und z_2 zu einem Parallelogramm vervollständigt. Diesen kann man konstruieren, indem man einen Kreis um z_1 mit Radius $|z_2|$ (also dem Abstand von 0 nach z_2) und einen um z_2 mit Radius $|z_1|$ (also dem Abstand von 0 nach z_1) zeichnet: der Punkt $z_1 + z_2$ ist dann einer der beiden Schnittpunkte dieser Kreise. Also ist auch $z_1 + z_2 \in \hat{M}$.



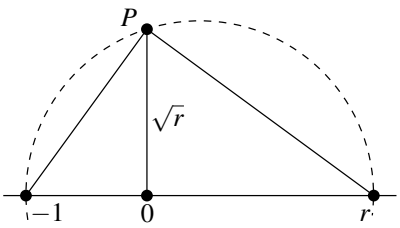
- *Multiplikation:* Es seien wieder $z_1, z_2 \in \hat{M}$ konstruierbar; wir müssen zeigen, dass auch $z_1 z_2$ konstruierbar ist. Dazu stellen wir diese beiden Zahlen in Polarkoordinaten $z_1 = r_1 e^{i\varphi_1}$ und $z_2 = r_2 e^{i\varphi_2}$ dar. Wegen $z_1 z_2 = r_1 r_2 e^{i(\varphi_1+\varphi_2)}$ müssen wir also mit Zirkel und Lineal die Beträge der beiden Zahlen multiplizieren und die Winkel addieren können. Um die Beträge zu multiplizieren (siehe das Bild unten links), zeichnen wir in den Punkten 1 und r_1 zur reellen Achse senkrechte Geraden wie in Problem 0.3 (a). Auf der ersten Senkrechten tragen wir dann nach oben die Länge r_2 ab (d. h. wir konstruieren den Punkt $1+ir_2$). Die Gerade durch 0 und $1+ir_2$ schneidet die zweite Senkrechte dann nach dem Strahlensatz im Punkt $r_1 + ir_1 r_2$, d. h. in einem Punkt, der von r_1 die Länge $r_1 r_2$ hat.

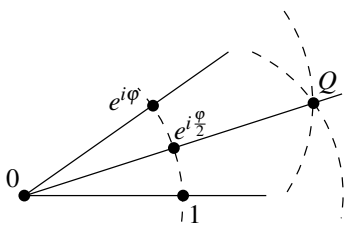




Um die Winkel zu addieren (siehe das Bild oben rechts), zeichnen wir einfach einen Kreis mit Radius 1 um den Nullpunkt und einen mit Radius $|e^{i\varphi_1} - 1|$ (also dem Abstand der bereits konstruierten Punkte 1 und $e^{i\varphi_1}$) um $e^{i\varphi_2}$; einer der Schnittpunkte dieser beiden Kreise definiert dann den Punkt $e^{i(\varphi_1+\varphi_2)}$, also die addierten Winkel.

- *Quadratwurzeln:* Wir arbeiten wieder mit Polarkoordinaten und suchen also zu $z = re^{i\varphi}$ die Zahl $\sqrt{r}\, e^{i\frac{\varphi}{2}}$, d. h. wir müssen die Wurzel aus r sowie zu φ den halben Winkel $\frac{\varphi}{2}$ konstruieren. Für die Wurzel aus r zeichnet man wie im Bild unten links einen Kreis mit Durchmesser $r+1$ von $-1 \in \mathbb{C}$ nach $r \in \mathbb{C}$; es sei P dann der Schnittpunkt dieses Kreises mit der positiven imaginären Achse. Nach bekannter Schulgeometrie ist das Dreieck mit den Eckpunkten P, -1 und r dann rechtwinklig, so dass aus dem Höhensatz folgt, dass die Strecke von 0 nach P gleich der Wurzel aus dem Produkt der Streckenlängen von -1 nach 0 und von 0 nach r, also gleich $\sqrt{r}$ ist.





Für die Winkelhalbierung zeichne man einfach wie im Bild oben rechts zwei Kreise mit Radius 1 und Mittelpunkten 1 sowie $e^{i\varphi}$; ist dann Q ein Schnittpunkt dieser beiden Kreise, so halbiert die Strecke von 0 nach Q offensichtlich den Winkel φ. □

Wir haben die geometrische Frage der Konstruierbarkeit gewisser Punkte der Ebene damit also auf die algebraische Frage zurückgeführt, ob diese Punkte — aufgefasst als komplexe Zahlen — in bestimmten Erweiterungskörpern von $\mathbb{Q}$ bzw. Unterkörpern von $\mathbb{C}$ liegen. Daher sollten wir als

Nächstes nun sehen, wie wir solche Körper zwischen $\mathbb{Q}$ und $\mathbb{C}$ algebraisch am besten beschreiben können.

Die grundlegende Idee hierfür kennt ihr in anderen Fällen bereits aus den „Algebraischen Strukturen“: um Untergruppen einer gegebenen Gruppe G zu konstruieren, kann man eine beliebige Teilmenge $M \subset G$ wählen und die davon erzeugte Untergruppe $\langle M \rangle$ betrachten. Formal kann man $\langle M \rangle$ als den Durchschnitt aller Untergruppen U mit $U \supset M$ definieren; anschaulich ist es einfach die kleinste Untergruppe von G, die M enthält [G, Definition 3.11 und Lemma 3.12]. Analog gibt es in Ringen das von einer Teilmenge erzeugte Ideal, also das kleinste Ideal, das diese gegebene Menge enthält [G, Definition 8.5 und Lemma 8.6].

Ganz genauso können wir nun Körper konstruieren, die zwischen zwei gegebenen Körpern K und L (oben also zwischen $\mathbb{Q}$ und $\mathbb{C}$) liegen:

Definition 1.13 (Körperadjunktion, einfache Körpererweiterungen)**.** Es seien $K \leq L$ Körper und $M \subset L$ eine beliebige Menge. Dann ist

$$K(M) := \bigcap_{\substack{K \leq Z \leq L \\ Z \supset M}} Z,$$

also der Durchschnitt aller Unterkörper von L, die sowohl K als auch die Menge M enthalten, nach Beispiel 1.3 (c) ein Körper mit $K \leq K(M) \leq L$. Anschaulich ist $K(M)$ der kleinste Unterkörper von L, der K und M enthält. Man kann $K(M)$ daher als den von M über K erzeugten Körper bezeichnen. Aus historischen Gründen ist jedoch die Sprechweise üblicher, dass $K(M)$ aus K durch **Adjunktion** der Elemente von M entsteht; man spricht $K(M)$ daher oft als „K adjungiert M“.

Ist $M = \{a_1, \ldots, a_n\}$ eine endliche Menge, so schreibt man statt $K(\{a_1, \ldots, a_n\})$ aus Bequemlichkeit in der Regel $K(a_1, \ldots, a_n)$. Besteht M sogar nur aus einem Element a, so nennt man $K(a)/K$ eine **einfache Körpererweiterung**.

Bemerkung 1.14 (Explizite Formel für Körperadjunktionen)**.** Analog zu [G, Aufgabe 3.14 und Definition 8.5] im Fall von Untergruppen bzw. Idealen kann man auch im Fall von Körpern eine explizite Formel für $K(M)$ hinschreiben. Betrachten wir der Einfachheit halber zunächst eine einfache Körpererweiterung, also $K(a)$ für ein $a \in L$ mit $K \leq L$, so gilt

$$K(a) = \left\{ \frac{f(a)}{g(a)} : \ f, g \in K[t] \text{ mit } g(a) \neq 0 \right\}.$$

Denn einerseits muss jeder Körper, der sowohl K als auch a enthält, wegen der Abgeschlossenheit bezüglich der Körperoperationen alle Ausdrücke der Form $\frac{f(a)}{g(a)}$ mit $f, g \in K[t]$ und $g(a) \neq 0$ enthalten; andererseits ist die rechte Seite der obigen Gleichung aber offensichtlich schon ein Körper, da sie selbst abgeschlossen unter den Körperoperationen ist. Damit ist dies also in der Tat der kleinste Körper, der K und a enthält, d. h. es ist genau $K(a)$.

Beachte, dass die Notation hier konsistent ist mit der Bezeichnung $\mathbb{R}(t)$ für den Körper der rationalen Funktionen über $\mathbb{R}$ aus Beispiel 1.2 (c): dieser wird in der Tat über $\mathbb{R}$ von der Identität $t \mapsto t$ erzeugt.

Adjungiert man zu K eine beliebige Menge M, so erhält man mit der gleichen Begründung wie oben die Aussage, dass $K(M)$ die Menge aller Quotienten von Polynomen (in mehreren Variablen) ist, die Koeffizienten in K haben und für deren Variablen man Werte aus M eingesetzt hat.

Beispiel 1.15. Wenn wir die einfache Körpererweiterung $\mathbb{Q}(\sqrt{2})$ über $\mathbb{Q}$ betrachten, so können wir deren Elemente nach Bemerkung 1.14 als die Menge aller Brüche von Polynomen in $\sqrt{2}$ mit rationalen Koeffizienten schreiben. Es gibt für diesen Körper aber eine viel einfachere Darstellung: wir behaupten, dass

$$\mathbb{Q}(\sqrt{2}) = \{a + b\sqrt{2} : \ a, b \in \mathbb{Q}\}$$

gilt. Um dies zu zeigen, bemerken wir zunächst, dass jeder Körper, der $\mathbb{Q}$ und $\sqrt{2}$ enthält, wegen der Abgeschlossenheit offensichtlich auch die rechte Seite der obigen Gleichung enthalten muss. Analog zur Begründung in Bemerkung 1.14 reicht es also zu zeigen, dass die rechte Seite bereits ein Körper, also abgeschlossen unter den Körperoperationen, ist. Die Abgeschlossenheit bezüglich

Addition und Subtraktion ist hierbei trivial, die bezüglich Multiplikation und Division ergibt sich aus den elementaren Rechnungen

$$(a+b\sqrt{2})(c+d\sqrt{2}) = \underbrace{(ac+2bd)}_{\in\mathbb{Q}} + \underbrace{(ad+bc)}_{\in\mathbb{Q}}\sqrt{2}$$

und

$$\frac{1}{a+b\sqrt{2}} = \frac{a-b\sqrt{2}}{(a+b\sqrt{2})(a-b\sqrt{2})} = \underbrace{\frac{a}{a^2-2b^2}}_{\in\mathbb{Q}} - \underbrace{\frac{b}{a^2-2b^2}}_{\in\mathbb{Q}}\sqrt{2}$$

für alle $a,b,c,d \in \mathbb{Q}$. Wir werden in Lemma 2.10 und Satz 2.14 (b) noch genauer sehen, wie man Körpererweiterungen oft auf viel einfachere Art als in Bemerkung 1.14 explizit beschreiben kann.

Aufgabe 1.16. Es seien L/K eine Körpererweiterung und M_1, M_2 Teilmengen von L. Zeige, dass $(K(M_1))(M_2) = (K(M_2))(M_1) = K(M_1 \cup M_2)$ gilt, d. h. dass es bei der Adjunktion von Mengen nicht auf die Reihenfolge ankommt.

Aufgabe 1.17. Zeige, dass $\mathbb{Q}(\sqrt{2},\sqrt{3}) = \mathbb{Q}(\sqrt{2}+\sqrt{3})$ gilt. Gilt auch $\mathbb{Q}(\sqrt{2},\sqrt{3}) = \mathbb{Q}(\sqrt{2}\cdot\sqrt{3})$?
(Eine Verallgemeinerung dieser Aussage werden wir später in Satz 4.28 beweisen.)

Nachdem wir nun also wissen, wie wir Körpererweiterungen prinzipiell algebraisch beschreiben können, wollen wir jetzt sehen, welche Eigenschaften diese Körpererweiterungen für unsere konkreten Probleme aus der Einleitung haben müssen. Betrachten wir dazu zunächst einmal die Frage der Auflösbarkeit von Polynomgleichungen aus Problem 0.2. Wenn wir die Möglichkeit des Wurzelziehens für einen Moment vernachlässigen und uns fragen würden, ob wir die Nullstellen eines Polynoms $f = t^n + a_{n-1}t^{n-1} + \cdots + a_0$ nur mit Hilfe der Körperoperationen aus den Koeffizienten von f bestimmen können, so könnten wir dies jetzt bereits algebraisch formulieren: dies wäre genau dann der Fall, wenn alle Nullstellen von f in $\mathbb{Q}(a_0,\ldots,a_{n-1})$ liegen — denn dies ist nach Definition 1.13 ja gerade der Körper aller Zahlen, die man aus den Koeffizienten des Polynoms (und unter Verwendung der rationalen Zahlen, die man nach Aufgabe 1.11 (a) immer mit dabei hat) mit den Körperoperationen erzeugen kann.

Wollen wir nun noch zusätzlich Wurzelziehen erlauben, so müssen wir statt $\mathbb{Q}(a_0,\ldots,a_{n-1})$ einfach eine geeignete Körpererweiterung betrachten, in der solche Wurzeln auch vorhanden sind:

Definition 1.18 (Radikalerweiterungen)**.** Es sei L/K eine Körpererweiterung.

(a) Ist $L = K(a)$ für ein $a \in L$, also $L/K = K(a)/K$ eine einfache Körpererweiterung, so heißt $K(a)/K$ eine **einfache Radikalerweiterung**, falls es ein $n \in \mathbb{N}_{>0}$ gibt mit $a^n \in K$. Man spricht in diesem Fall auch von einer **einfachen n-Radikalerweiterung** und kann sich dies so vorstellen, dass $K(a)$ aus K durch Adjunktion einer n-ten Wurzel entsteht.

(b) Ist L/K beliebig, so nennt man L/K eine **Radikalerweiterung**, falls es eine endliche Kette von Körpern

$$K = K_0 \leq K_1 \leq \cdots \leq K_m = L$$

gibt, so dass jedes K_i/K_{i-1} für $i = 1,\ldots,m$ eine einfache Radikalerweiterung ist (d. h. wenn L aus K durch fortgesetzte Adjunktion von Wurzeln entsteht). Ist jede dieser Körpererweiterungen eine einfache n-Radikalerweiterung (für dasselbe n), so nennt man L/K auch eine **n-Radikalerweiterung**.

Beispiel 1.19.

(a) Die Körpererweiterung $\mathbb{Q}(\sqrt{2})/\mathbb{Q}$ aus Beispiel 1.15 ist offensichtlich eine einfache 2-Radikalerweiterung, denn $(\sqrt{2})^2 = 2 \in \mathbb{Q}$.

(b) $\mathbb{Q}(\sqrt{2}, \sqrt[3]{1+\sqrt{2}})/\mathbb{Q}$ ist eine Radikalerweiterung, denn in der Kette

$$\mathbb{Q} \leq \mathbb{Q}(\sqrt{2}) \leq \mathbb{Q}\left(\sqrt{2}, \sqrt[3]{1+\sqrt{2}}\right)$$

ist jeder Schritt eine einfache Radikalerweiterung (im zweiten Schritt wird die dritte Wurzel des Elements $1+\sqrt{2} \in \mathbb{Q}(\sqrt{2})$ adjungiert).

Mit dieser Definition können wir nun unser Problem der Auflösbarkeit von Polynomgleichungen exakt formulieren:

Definition 1.20. Ein komplexes Polynom $f = t^n + a_{n-1}t^{n-1} + \cdots + a_1 t + a_0 \in \mathbb{C}[t]$ heißt **auflösbar**, wenn es eine Radikalerweiterung von $\mathbb{Q}(a_0, \ldots, a_{n-1})$ gibt, die alle Nullstellen von f enthält (also „wenn sich alle Nullstellen von f aus den Koeffizienten mit Hilfe der Körperoperationen und komplexem Wurzelziehen exakt berechnen lassen“).

Beispiel 1.21. Jedes komplexe Polynom $f = t^2 + a_1 t + a_0$ vom Grad 2 ist auflösbar, denn seine Nullstellen $-\frac{a_1}{2} \pm \sqrt{\frac{a_1^2}{4} - a_0}$ liegen offensichtlich in der Radikalerweiterung $\mathbb{Q}\left(a_0, a_1, \sqrt{\frac{a_1^2}{4} - a_0}\right)$ von $\mathbb{Q}(a_0, a_1)$. Genauso zeigt die Cardanische Formel aus Problem 0.2, dass jedes Polynom vom Grad 3 auflösbar ist. Wie bereits angekündigt werden wir in Aufgabe 8.14 jedoch sehen, dass es auch Polynome gibt, die nicht auflösbar sind.

Nach der Auflösbarkeit von Polynomgleichungen wollen wir nun zum Schluss dieses Kapitels auch die Konstruktionsprobleme mit Zirkel und Lineal aus Problem 0.3 in die Sprache der Algebra übersetzen. Das wesentliche Ergebnis hierfür ist natürlich Satz 1.12, der im Prinzip besagt, dass man Körperoperationen und Quadratwurzelziehen in der komplexen Ebene geometrisch durchführen kann. Die Fragestellung ist hier also sehr ähnlich zur Auflösbarkeit von Polynomgleichungen, nur dass wir in diesem Fall lediglich Quadratwurzeln und nicht beliebige Wurzeln zulassen. Dies führt zu folgendem Satz, der der Definition 1.20 eines auflösbaren Polynoms sehr ähnlich sieht.

Satz 1.22. *Es sei $M \subset \mathbb{C}$ mit $0, 1 \in M$ gegeben. Ein Punkt $z \in \mathbb{C}$ ist genau dann aus M mit Zirkel und Lineal konstruierbar, wenn z in einer 2-Radikalerweiterung von $\mathbb{Q}(M \cup \overline{M})$ liegt. (Hierbei bezeichnet $\overline{M}$ die Menge aller komplex konjugierten Zahlen zu Elementen aus M.)*

Beweis.

„$\Leftarrow$“ ist genau Satz 1.12: Zahlen in einer 2-Radikalerweiterung von $\mathbb{Q}(M \cup \overline{M})$ sind nach Definition 1.18 genau diejenigen, die sich aus M mit Hilfe der Körperoperationen, komplexer Konjugation und Ziehen von Quadratwurzeln erzeugen lassen — und solche Punkte sind nach Satz 1.12 alle mit Zirkel und Lineal konstruierbar.

„$\Rightarrow$“ Es sei $z \in \hat{M}$ mit Zirkel und Lineal konstruierbar. Wir müssen zeigen, dass sich z aus den Punkten von M mit Hilfe der Körperoperationen, der komplexen Konjugation und komplexer Quadratwurzeln ergibt.

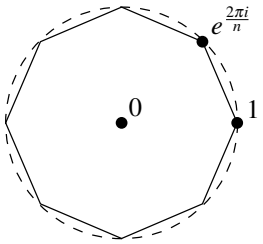
Neue Punkte entstehen bei Elementarkonstruktionen nur dadurch, dass man Schnittpunkte von bereits konstruierten Geraden und / oder Kreisen bestimmt. Geraden und Kreise durch schon konstruierte Punkte werden aber beschrieben durch lineare bzw. quadratische Gleichungen in z und $\bar{z}$, deren Koeffizienten bereits konstruierte Zahlen sind. Die in einer Elementarkonstruktion neu konstruierten Punkte entstehen also stets als Lösungen linearer oder quadratischer Gleichungen mit bereits konstruierten Koeffizienten. Lineare und quadratische Gleichungen lassen sich aber bekanntlich mit Hilfe der Körperoperationen und evtl. Ziehen von Quadratwurzeln lösen. □

Beispiel 1.23 (Konstruktionen mit Zirkel und Lineal, algebraische Fassung)**.** Mit Satz 1.22 können wir die Aufgaben aus Problem 0.3 nun algebraisch formulieren:

(A) (Quadratur des Kreises) In der Ebene sei ein Kreis, o. B. d. A. der Einheitskreis gegeben (der durch den Mittelpunkt 0 und den Punkt 1 auf dem Rand definiert wird). Da dieser Kreis den Flächeninhalt π besitzt, suchen wir also nach einem Quadrat mit Seitenlänge $\sqrt{\pi}$, d. h. wir wollen den Punkt $\sqrt{\pi}$ konstruieren. Nach Satz 1.22 ist die Quadratur des Kreises also genau dann möglich, wenn $\sqrt{\pi}$ in einer 2-Radikalerweiterung von $\mathbb{Q}(0,1) = \mathbb{Q}$ liegt. Offensichtlich ist dies auch äquivalent dazu, dass π in einer 2-Radikalerweiterung von $\mathbb{Q}$ liegt, da man $\sqrt{\pi}$ ja aus π durch Ziehen einer weiteren Quadratwurzel erhält.

(B) (Würfelverdoppelung) Da wir zur Seitenlänge 1 eines Würfels die Seitenlänge $\sqrt[3]{2}$ eines Würfels mit dem doppelten Volumen konstruieren wollen, ist diese Konstruktion analog zu (A) genau dann möglich, wenn $\sqrt[3]{2}$ in einer 2-Radikalerweiterung von $\mathbb{Q}$ liegt.

(C) (Konstruktion des regelmäßigen n-Ecks) Gegeben sei der Mittelpunkt und einer der Eckpunkte des n-Ecks, o. B. d. A. wieder 0 bzw. 1. Offensichtlich genügt es, den ersten weiteren Eckpunkt $e^{\frac{2\pi i}{n}}$ des n-Ecks zu konstruieren, da alle weiteren Eckpunkte dann natürlich rekursiv genauso aus dem jeweils vorhergehenden konstruiert werden können. Also ist die Konstruktion des n-Ecks genau dann möglich, wenn $e^{\frac{2\pi i}{n}}$ in einer 2-Radikalerweiterung von $\mathbb{Q}$ liegt.



Wie schon angekündigt müssen wir also genau wie im Fall der Auflösbarkeit von Polynomgleichungen entscheiden, ob bestimmte Zahlen in gewissen Radikalerweiterungen enthalten sein können oder nicht. Der wesentliche Unterschied besteht darin, dass wir hier nach einer *2-Radikalerweiterung* und nicht nach einer allgemeinen Radikalerweiterung fragen — weil wir beim Auflösen von Gleichungen beliebige Wurzeln zulassen wollen, während man mit Zirkel und Lineal nur Quadratwurzeln ziehen kann.

Bemerkung 1.24. Ist $M \subset \mathbb{C}$ eine Menge mit $0, 1 \in M$, so ergibt sich aus Satz 1.12, dass in jedem Fall alle Punkte der Form $x + iy$ mit $x, y \in \mathbb{Q}$ zu $\hat{M}$ gehören, also konstruierbar sind. Die konstruierbaren Punkte liegen damit „*dicht*“ in der Zeichenebene, d. h. jeder beliebige Punkt der Ebene lässt sich zumindest beliebig genau mit Zirkel und Lineal approximieren.

2. Der Grad von Körpererweiterungen

Wenn wir untersuchen wollen, ob eine gegebene Konstruktion in der Ebene mit Zirkel und Lineal durchführbar ist, haben wir im vorigen Kapitel gesehen, dass wir dazu herausfinden müssen, ob eine bestimmte komplexe Zahl in einer 2-Radikalerweiterung eines gegebenen Körpers liegt oder nicht.

Wie ihr euch vielleicht schon denken könnt, ist dies aber zunächst einmal nicht so einfach herauszufinden, da wir in der Regel ja nicht wissen können, wie diese 2-Radikalerweiterung genau aussieht. In diesem Kapitel wollen wir daher ein *notwendiges* Kriterium für die Existenz einer solchen Erweiterung (und damit für die Durchführbarkeit der Konstruktion) angeben, das sich wesentlich einfacher nachprüfen lässt. Das wesentliche Konzept hierfür ist das des *Grades* einer Körpererweiterung bzw. von Elementen einer Körpererweiterung. Um dies einzuführen, müssen wir untersuchen, ob die Elemente einer Körpererweiterung L/K Nullstellen von Polynomen über K sind, und wenn ja, welchen Grad diese Polynome haben.

Definition 2.1 (Algebraische und transzendente Elemente)**.** Es sei L/K eine Körpererweiterung.

(a) Ein Element $a \in L$ heißt **algebraisch** über K, wenn es ein Polynom $f \in K[t]$ gibt mit $f \neq 0$ und $f(a) = 0$. Andernfalls heißt a **transzendent** über K.

(b) Die Körpererweiterung L/K heißt algebraisch, wenn jedes $a \in L$ algebraisch über K ist. Andernfalls (also wenn es ein über K transzendentes Element in L gibt) heißt L/K transzendent.

Beispiel 2.2.

(a) Die reelle Zahl $\sqrt{2}$ ist offensichtlich algebraisch über $\mathbb{Q}$, denn sie ist Nullstelle des rationalen Polynoms $t^2 - 2$.

(b) Betrachten wir die Körpererweiterung $\mathbb{R}(t)/\mathbb{R}$ aus Beispiel 1.2 (c), so ist das Element $t \in \mathbb{R}(t)$ transzendent über $\mathbb{R}$, denn für Koeffizienten $a_0, \ldots, a_n \in \mathbb{R}$, die nicht alle Null sind, ist $a_n t^n + \cdots + a_1 t + a_0$ niemals 0 in $\mathbb{R}(t)$ (d. h. nie die Nullfunktion).

(c) Ein einfaches Abzählargument ergibt, dass es sehr viele transzendente Zahlen in $\mathbb{R}/\mathbb{Q}$ gibt: die Menge $\mathbb{Q}$ der rationalen Zahlen ist bekanntlich abzählbar. Ein Polynom in $\mathbb{Q}[t]$ vom Grad kleiner als n ist eindeutig durch seine n Koeffizienten in $\mathbb{Q}$ bestimmt; also ist die Menge aller solcher Polynome bijektiv zu $\mathbb{Q}^n$ und damit auch abzählbar. Da jedes solche Polynom (das nicht das Nullpolynom ist) nur endlich viele Nullstellen hat, ist die Menge aller Nullstellen von Polynomen vom Grad kleiner als n ebenfalls abzählbar für alle n. Nimmt man nun die Vereinigung dieser Nullstellenmengen für alle $n \in \mathbb{N}$, so erhält man die Menge aller algebraischen Zahlen und sieht, dass sie als abzählbare Vereinigung abzählbarer Mengen ebenfalls abzählbar sein muss. Die Menge der reellen Zahlen ist aber bekanntlich nicht abzählbar. Also gibt es transzendente Zahlen in $\mathbb{R}/\mathbb{Q}$ — in der Tat sind „die meisten“ Zahlen in $\mathbb{R}$ transzendent über $\mathbb{Q}$.

Trotz dieser Aussage ist es allerdings erstaunlich schwierig, von einer konkreten reellen Zahl nachzuweisen, dass sie transzendent über $\mathbb{Q}$ ist. Lindemann hat Ende des 19. Jahrhunderts bewiesen, dass π und e transzendent über $\mathbb{Q}$ sind; der Beweis hierfür ist jedoch sehr lang und technisch und benutzt Methoden, die wir erst entwickeln müssten und die wir danach für nichts anderes mehr verwenden könnten. Ich möchte ihn euch und mir daher ersparen. Wir werden die Transzendenz von e in dieser Vorlesung auch nicht benötigen, die von π tritt lediglich im Beweis der Unmöglichkeit der Quadratur des Kreises in Beispiel 2.23 auf.

02

Bemerkung 2.3. Es sei L/K eine Körpererweiterung und $a \in L$ algebraisch über K. Dann gibt es unter allen Polynomen in $K[t]$, die a als Nullstelle haben, stets ein *eindeutiges* normiertes Polynom (d. h. der Leitkoeffizient ist 1) mit minimalem Grad. Wären nämlich f und g zwei verschiedene

normierte Polynome minimalen Grades mit Nullstelle a, so wäre $f-g$ ein nicht verschwindendes Polynom kleineren Grades in $K[t]$, das ebenfalls a als Nullstelle hätte (und das man natürlich auch normieren kann). Wir können also definieren:

Definition 2.4 (Minimalpolynom und Grad)**.** Es seien L/K eine Körpererweiterung und $a \in L$.

(a) Ist a algebraisch über K, so heißt das (nach Bemerkung 2.3 eindeutig bestimmte) normierte Polynom über K minimalen Grades mit Nullstelle a das **Minimalpolynom** von a. Wir bezeichnen es mit $m_{a,K} \in K[t]$, bzw. einfach mit m_a, wenn aus dem Zusammenhang klar ist, welcher Grundkörper gemeint ist. Sein Grad wird auch der **Grad** von a über K genannt und als $[a:K]$ geschrieben.

(b) Ist a transzendent über K, so setzen wir formal $[a:K] = \infty$.

Bemerkung 2.5 (Alternative Beschreibung des Minimalpolynoms)**.** Wie in Definition 2.4 seien L/K eine Körpererweiterung und $a \in L$. Wir betrachten die Menge

$$I = \{f \in K[t] : f(a) = 0\} \quad \subset K[t]$$

aller Polynome über K, die a als Nullstelle haben. Man prüft sofort nach, dass I ein Ideal ist. In der Tat behaupten wir, dass

$$I = (m_a) \tag{$*$}$$

gilt, also dass I von m_a erzeugt wird. Den Beweis dieser Aussage kennt ihr bereits aus den „Algebraischen Strukturen“: Dort haben wir nämlich gezeigt, dass man ein Ideal I in einem Hauptidealring stets als das Hauptideal schreiben kann, das von einem Element in $I \setminus \{0\}$ mit minimaler euklidischer Funktion erzeugt wird [G, Satz 10.21]. Wir können den Beweis aber auch hier schnell noch einmal geben:

„$\supset$“ Dies ist klar, denn (jedes Vielfache von) m_a hat natürlich a als Nullstelle.

„$\subset$“ Es sei $f \in K[t]$ mit $f(a) = 0$. Division von f mit Rest durch m_a liefert $f = q m_a + r$ für Polynome $q, r \in K[t]$ mit $\deg r < \deg m_a$. Setzen wir hier den Wert a ein, so erhalten wir $f(a) = q(a)m_a(a) + r(a)$, wegen $f(a) = m_a(a) = 0$ also $r(a) = 0$. Damit ist r ein Polynom mit Nullstelle a und kleinerem Grad als m_a — was nach Definition des Minimalpolynoms nur möglich ist, wenn $r = 0$ das Nullpolynom ist. Dann ist aber $f = q m_a \in (m_a)$.

Dies zeigt die Gleichung $(*)$. Beachte, dass man diese Gleichung auch verwenden könnte, um das Minimalpolynom auf eine andere Art zu *definieren*: als den (eindeutig bestimmten) normierten Erzeuger des Hauptideals aller Polynome über K mit Nullstelle a.

In Worten besagt die Gleichung $(*)$ einfach, dass jedes Polynom über K mit Nullstelle a ein Vielfaches von m_a ist, bzw. dass m_a jedes solche Polynom teilt. Dies werden wir später noch häufiger benötigen.

Minimalpolynome algebraischer Elemente werden im Folgenden eine große Rolle spielen. Wir wollen uns daher als Erstes fragen, wie man sie in der Praxis berechnen kann. Natürlich wird man dazu zunächst nach einem Polynom mit der gewünschten Nullstelle suchen und dieses dann normieren. Dies ist in der Regel nicht kompliziert. Es ist aber oft nur schwer zu entscheiden, ob es sich dabei auch um das Polynom *kleinsten Grades* mit dieser Nullstelle handelt, also ob man wirklich das Minimalpolynom gefunden hat. Um das zu entscheiden, ist das folgende Kriterium sehr nützlich.

Lemma 2.6 („Minimalpolynom=irreduzibel“)**.** *Es seien L/K eine Körpererweiterung, $a \in L$, und $f \in K[t]$ ein normiertes Polynom mit $f(a) = 0$. Dann gilt*

$$f = m_a \quad \Leftrightarrow \quad f \text{ ist irreduzibel in } K[t].$$

Beweis. Beide Richtungen dieser Äquivalenz sind einfach zu zeigen:

„$\Rightarrow$“ Angenommen, $f = m_a$ wäre reduzibel, d. h. $m_a = g \cdot h$ für gewisse Polynome $g, h \in K[t]$ mit $\deg g, \deg h < \deg m_a$. Einsetzen von a liefert $g(a)h(a) = m_a(a) = 0$. Da ein Körper keine Nullteiler hat, muss also $g(a) = 0$ oder $h(a) = 0$ sein. Damit hätten wir in jedem Fall ein

nicht-konstantes Polynom mit Nullstelle a, dessen Grad kleiner als der des Minimalpolynoms ist — was ein Widerspruch ist.

„⇐“ Es sei f irreduzibel und normiert mit $f(a) = 0$. Nach Bemerkung 2.5 ist f dann ein Vielfaches des Minimalpolynoms, also $f = g \cdot m_a$ für ein $g \in K[t]$. Da f aber irreduzibel ist, kann g nur eine Einheit in $K[t]$, also eine Konstante sein. Weil darüber hinaus sowohl f als auch m_a normiert sind, ist diese Konstante sogar gleich 1, und wir erhalten wie gewünscht $f = m_a$. □

Wenn wir dieses Lemma nun benutzen wollen, um Minimalpolynome zu bestimmen, benötigen wir natürlich noch gute Möglichkeiten, wie man einem Polynom ansehen kann, ob es irreduzibel ist oder nicht. Wir begnügen uns hier für den Moment mit dem folgenden einfachen Kriterium, das ihr vermutlich bereits aus den „Algebraischen Strukturen“ kennt — bessere Kriterien werden wir später noch in Kapitel 3 kennen lernen.

Aufgabe 2.7.

(a) Es sei K ein Körper. Zeige, dass ein Polynom $f \in K[t]$ vom Grad 2 oder 3 genau dann irreduzibel ist, wenn es keine Nullstelle hat.

(b) Zeige, dass das Kriterium aus (a) für jeden Grad größer als 3 falsch ist, d. h. gib für jedes $n \geq 4$ ein Beispiel an für einen Körper K sowie ein reduzibles Polynom $f \in K[t]$ vom Grad n ohne Nullstellen.

Aufgabe 2.8. Es sei p eine Primzahl. Wie viele irreduzible Polynome vom Grad 2 gibt es in $\mathbb{Z}_p[t]$?

Mit diesen Ergebnissen können wir nun ein paar Beispiele von Minimalpolynomen und Graden von Elementen konkret angeben.

Beispiel 2.9.

(a) Es sei L/K eine Körpererweiterung und $a \in L$. Offensichtlich ist $[a : K] = 1$ genau dann, wenn $a \in K$ ist — das Minimalpolynom ist in diesem Fall einfach $t - a \in K[t]$.

(b) Wir wollen den Grad von $a = \sqrt{2} \in \mathbb{R}$ über $\mathbb{Q}$ bestimmen. Natürlich ist $t^2 - 2$ ein normiertes rationales Polynom mit Nullstelle a. Da es offensichtlich keine Nullstellen in $\mathbb{Q}$ besitzt, ist es nach Aufgabe 2.7 (a) irreduzibel in $\mathbb{Q}[t]$ und damit nach Lemma 2.6 das Minimalpolynom von a über $\mathbb{Q}$. Damit ist $[\sqrt{2} : \mathbb{Q}] = 2$.

Beachte, dass es beim Minimalpolynom und Grad eines Elements auch entscheidend auf den Grundkörper ankommt: nach (a) ist z. B. $[\sqrt{2} : \mathbb{R}] = 1$ mit Minimalpolynom $m_{\sqrt{2},\mathbb{R}} = t - \sqrt{2}$.

(c) Analog zu (b) ist $t^3 - 2$ das Minimalpolynom von $\sqrt[3]{2}$ über $\mathbb{Q}$, denn es ist ein normiertes Polynom über $\mathbb{Q}$ mit Nullstelle $\sqrt[3]{2}$, das keine Nullstellen in $\mathbb{Q}$ besitzt und damit wiederum nach Aufgabe 2.7 (a) in $\mathbb{Q}[t]$ irreduzibel ist. Also ist $[\sqrt[3]{2} : \mathbb{Q}] = 3$.

(d) Wir wollen das Minimalpolynom (und den Grad) von $a = e^{\frac{2\pi i}{6}}$ über $\mathbb{Q}$ bestimmen. Auch hier sehen wir sofort ein normiertes Polynom über $\mathbb{Q}$ mit Nullstelle a, nämlich $t^6 - 1$. Ist es das Minimalpolynom von a über $\mathbb{Q}$? Nein, denn es lässt sich offensichtlich als

$$t^6 - 1 = (t^3 - 1)(t^3 + 1)$$

faktorisieren, ist damit nicht irreduzibel in $\mathbb{Q}[t]$ und kann demzufolge nach Lemma 2.6 nicht das Minimalpolynom sein. In der Tat ist a ja eine Nullstelle dieses Produkts und muss damit eine Nullstelle von einem der Faktoren sein (dies ist genau das Argument der Richtung „⇒“ vom Beweis von Lemma 2.6). In unserem konkreten Fall ist $a^3 = e^{\pi i} = -1$ und damit a eine Nullstelle von $t^3 + 1$. Ist also $t^3 + 1$ das gesuchte Minimalpolynom? Auch dies ist nicht der Fall, denn $t^3 + 1$ hat noch die rationale Nullstelle -1, was zur weiteren Faktorisierung

$$t^3 + 1 = (t + 1)(t^2 - t + 1)$$

in $\mathbb{Q}[t]$ führt. Hier ist a offensichtlich keine Nullstelle von $t + 1$, also muss es eine von $t^2 - t + 1$ sein. Und dieses Polynom ist nun tatsächlich irreduzibel nach Aufgabe 2.7 (a), denn

es hat in $\mathbb{Q}$ keine Nullstellen mehr (wie eine einfache Berechnung der Nullstellen zeigt). Demnach ist das gesuchte Minimalpolynom $m_a = t^2 - t + 1$ nach Lemma 2.6, es ist also $[e^{\frac{2\pi i}{6}} : \mathbb{Q}] = 2$.

Wir sehen an diesem Beispiel schon, dass wir bei der Berechnung eines Minimalpolynoms aufpassen müssen — das Minimalpolynom eines Elements a ist nicht immer das „erstbeste" oder „einfachste" normierte Polynom mit Nullstelle a, das einem einfällt!

Als erste Anwendung des Gradkonzepts wollen wir nun eine sehr praktische Darstellung einfacher algebraischer Körpererweiterungen zeigen. Wir hatten ja bereits in Bemerkung 1.14 gesehen, dass sich die Elemente einer einfachen Körpererweiterung $K(a)$ immer als Quotienten von Polynomausdrücken in a mit Koeffizienten in K schreiben lassen. Diese explizite Darstellung von $K(a)$ ist jedoch recht kompliziert. Für den konkreten Fall der Körpererweiterung $\mathbb{Q}(\sqrt{2})$ haben wir in Beispiel 1.15 eine viel einfachere Darstellung gefunden, nämlich die Menge aller Ausdrücke der Form $a + b\sqrt{2}$ mit $a, b \in \mathbb{Q}$. Eine solche schöne Darstellung gibt es in der Tat für jede einfache algebraische Körpererweiterung:

Lemma 2.10 (Explizite Darstellung von einfachen algebraischen Körpererweiterungen)**.** *Es sei L/K eine Körpererweiterung und $a \in L$ algebraisch vom Grad $n = [a : K]$. Dann gilt*

$$K(a) \quad = \quad \{f(a) : \ f \in K[t]\} \quad = \quad \{f(a) : \ f \in K[t] \text{ mit } \deg f < n\}.$$

Beweis. Nach Bemerkung 1.14 ist $K(a)$ gleich der Menge $M_0 = \left\{\frac{f(a)}{g(a)} : \ f, g \in K[t] \text{ mit } g(a) \neq 0\right\}$ aller rationalen Ausdrücke in a (mit Koeffizienten in K). Es seien nun $M_1 = \{f(a) : \ f \in K[t]\}$ die Menge aller Polynomausdrücke in a und $M_2 = \{f(a) : \ f \in K[t] \text{ mit } \deg f < n\}$ die Menge aller Polynomausdrücke in a vom Grad kleiner als n. Wir müssen zeigen, dass $M_0 = M_1 = M_2$.

$M_0 = M_1$: Die Inklusion „$\supset$" ist offensichtlich, da jeder Polynomausdruck auch ein rationaler Ausdruck ist. Für die Inklusion „$\subset$" sei $b \in M_0$, also $b = \frac{f(a)}{g(a)}$ für $f, g \in K[t]$ mit $g(a) \neq 0$. Wir wollen den größten gemeinsamen Teiler der Polynome g und m_a mit Hilfe ihrer Primfaktorzerlegungen bestimmen [G, Kapitel 11]. Da das Minimalpolynom m_a nach Lemma 2.6 irreduzibel und damit auch prim ist [G, Bemerkung 11.6], ist m_a selbst der einzige Primfaktor, der in beiden Primfaktorzerlegungen von g und m_a auftreten könnte. Aber m_a kann kein Primfaktor von g sein, da g sonst ein Vielfaches von m_a wäre und somit genau wie m_a den Wert a als Nullstelle haben müsste. Also sind g und m_a teilerfremd, und daher gibt es nach dem Lemma von Bézout Polynome $p, q \in K[t]$ mit $pg + qm_a = 1$ in $K[t]$ [G, Satz 10.13 (b)]. Einsetzen von a liefert dann $p(a)\,g(a) = 1$ in L wegen $m_a(a) = 0$, und wir erhalten wie gewünscht

$$b = \frac{f(a)}{g(a)} = f(a)\,p(a) \in M_1.$$

$M_1 = M_2$: Auch hier ist die Inklusion „$\supset$" wieder klar. Für die Inklusion „$\subset$" sei $b \in M_1$, also $b = f(a)$ für ein $f \in K[t]$. Division von f durch m_a mit Rest [G, Satz 10.19] liefert $f = qm_a + r$ für gewisse $q, r \in K[t]$ mit $\deg r < \deg m_a$. Wegen $m_a(a) = 0$ ist dann $b = f(a) = r(a) \in M_2$. □

Beispiel 2.11. Da $\sqrt{2}$ nach Beispiel 2.9 (b) Grad 2 über $\mathbb{Q}$ hat, ist $\mathbb{Q}(\sqrt{2})$ nach Lemma 2.10 die Menge aller höchstens linearen Polynomausdrücke in $\sqrt{2}$ mit Koeffizienten in $\mathbb{Q}$, also wie in Beispiel 1.15

$$\mathbb{Q}(\sqrt{2}) = \{a + b\sqrt{2} : \ a, b \in \mathbb{Q}\}.$$

Analog ergibt sich aus $[\sqrt[3]{2} : \mathbb{Q}] = 3$ (siehe Beispiel 2.9 (c))

$$\mathbb{Q}(\sqrt[3]{2}) = \{a + b\sqrt[3]{2} + c\sqrt[3]{4} : \ a, b, c \in \mathbb{Q}\}.$$

Diese Darstellung erinnert stark an Linearkombinationen, wie sie in der Linearen Algebra auftreten. In der Tat sieht man sofort, dass man in jeder Körpererweiterung L/K den großen Körper L als einen Vektorraum über dem kleinen Körper K auffassen kann: es gibt ja eine Addition in L (die Vektoraddition), und man kann Elemente von K mit Elementen von L multiplizieren (die Skalarmultiplikation), weil K in L liegt und es in L die Körpermultiplikation gibt. Natürlich folgt aus den Körperaxiomen

auch, dass für diese Vektoraddition und Skalarmultiplikation die für einen Vektorraum geforderten Rechenregeln gelten. Wir können daher definieren:

Definition 2.12 (Grad einer Körpererweiterung)**.** Es sei L/K eine Körpererweiterung. Die Dimension von L als K-Vektorraum wird der **Grad** von L/K genannt und als $[L:K]$ geschrieben. Offensichtlich ist $[L:K] \in \mathbb{N} \cup \{\infty\}$. Ist dieser Grad endlich, also L ein endlich-dimensionaler K-Vektorraum, so nennt man die Körpererweiterung L/K **endlich**.

Beispiel 2.13.

(a) Offensichtlich ist der Grad einer Körpererweiterung L/K genau dann gleich 1, wenn $L = K$ ist.

(b) Nach Beispiel 2.11 ist $[\mathbb{Q}(\sqrt{2}) : \mathbb{Q}] = 2$, denn $\{1, \sqrt{2}\}$ ist eine Basis von $\mathbb{Q}(\sqrt{2})$ als $\mathbb{Q}$-Vektorraum. Genauso ist natürlich $[\mathbb{C} : \mathbb{R}] = 2$, denn $\{1, i\}$ ist eine Basis von $\mathbb{C}$ als $\mathbb{R}$-Vektorraum.

(c) Es sei L/K eine transzendente Körpererweiterung. Dann gibt es ein Element $a \in L$, das transzendent über K ist. Dies bedeutet, dass die Menge $\{1, a, a^2, a^3, \dots\}$ linear unabhängig über K ist, da es ja sonst eine nicht-triviale Linearkombination $\sum_{i=0}^{n} \lambda_i a^i = 0$ mit $\lambda_0, \dots, \lambda_n \in K$ gäbe und a damit Nullstelle eines Polynoms mit Koeffizienten in K wäre. Also ist dann $[L:K] = \infty$.

Anders ausgedrückt bedeutet dies, dass jede endliche Körpererweiterung algebraisch ist. Die Umkehrung gilt hier jedoch nicht, wie wir in Aufgabe 3.11 (b) sehen werden.

Wir können unsere Ergebnisse von Lemma 2.10 und Beispiel 2.11 nun sofort auf den Begriff des Grades einer Körpererweiterung übertragen.

Satz 2.14. *Es seien L/K eine Körpererweiterung und $a \in L$. Dann gilt:*

(a) $[K(a) : K] = [a : K]$.

(b) *Ist a algebraisch vom Grad n über K, so ist $\{1, a, a^2, \dots, a^{n-1}\}$ eine Basis von $K(a)$ als K-Vektorraum.*

(c) *Ist a algebraisch über K, so ist auch $K(a)/K$ algebraisch, d. h. jedes Element von $K(a)$ ist algebraisch über K.*

Beweis. Ist a und damit auch $K(a)$ transzendent über K, so ist $[K(a) : K] = [a : K] = \infty$ nach Beispiel 2.13 (c).

Wir können nun also annehmen, dass a algebraisch vom Grad n über K ist. Nach Lemma 2.10 ist $K(a)$ dann die Menge aller Polynomausdrücke in a vom Grad kleiner als n mit Koeffizienten in K. Dies bedeutet genau, dass $\{1, a, a^2, \dots, a^{n-1}\}$ ein Erzeugendensystem von $K(a)$ als K-Vektorraum ist. In der Tat ist diese Familie auch linear unabhängig über K, denn andernfalls gäbe es ja eine nicht-triviale Linearkombination $\lambda_0 + \lambda_1 a + \dots + \lambda_{n-1} a^{n-1} = 0$ mit $\lambda_0, \dots, \lambda_{n-1} \in K$, d. h. a wäre im Widerspruch zur Definition des Grades eine Nullstelle eines Polynoms über K, dessen Grad kleiner als der des Minimalpolynoms ist. Dies zeigt (b), und damit auch (a).

Für (c) sei $b \in K(a)$ beliebig. Ist wieder $n = [a : K]$, so ist die Familie $\{1, b, b^2, \dots, b^n\}$ dann notwendigerweise linear abhängig über K, denn dies sind $n+1$ Elemente in dem nach (a) n-dimensionalen K-Vektorraum $K(a)$. Es muss also $\lambda_0, \dots, \lambda_n \in K$ geben, die nicht alle Null sind und für die $\lambda_0 + \lambda_1 b + \dots + \lambda_n b^n = 0$ gilt. Dies bedeutet aber genau, dass b algebraisch ist. □

Bemerkung 2.15. Für eine einfache Körpererweiterung $K(a)/K$ gilt also

$$a \text{ algebraisch} \quad \Leftrightarrow \quad K(a)/K \text{ algebraisch} \quad \Leftrightarrow \quad K(a)/K \text{ endlich}$$

(die Äquivalenz der ersten Aussage mit der zweiten ist Satz 2.14 (c), die der ersten mit der dritten Satz 2.14 (a)). Darüber hinaus ist in diesem Fall der Grad von a über K nach Satz 2.14 (a) gleich dem Grad der Körpererweiterung $K(a)$ über K. Die Begriffe „algebraisch“ und „Grad“, die wir sowohl für Elemente als auch für Körpererweiterungen definiert haben, passen in diesem Sinne also zusammen.

Beispiel 2.16. Es sei L/K eine einfache n-Radikalerweiterung, also $L = K(a)$ für ein $a \in L$ mit $a^n \in K$. Dann ist $t^n - a^n$ ein Polynom über K (und nicht nur über L!) mit Nullstelle a. Das Minimalpolynom von a hat also höchstens Grad n. Mit Satz 2.14 (a) folgt demnach $[L:K] = [a:K] \leq n$.

Um mit Graden von Körpererweiterungen rechnen zu können, benötigen wir den folgenden wichtigen Satz, der die Grade zweier „verketteter Körpererweiterungen" miteinander vergleicht.

Satz 2.17 (Gradformel). *Sind $K \leq Z \leq L$ Körper, so gilt $[L:K] = [L:Z] \cdot [Z:K]$.*

03

Beweis. Es seien $\{v_i : i \in I\}$ eine Basis von Z als K-Vektorraum und $\{w_j : j \in J\}$ eine Basis von L als Z-Vektorraum. Wir behaupten, dass $\{v_i \cdot w_j : i \in I, j \in J\}$ eine Basis von L als K-Vektorraum ist (woraus dann offensichtlich die Aussage des Satzes folgt).

Erzeugendensystem: Es sei $a \in L$ beliebig. Da die w_j ein Erzeugendensystem von L als Z-Vektorraum sind, gibt es $\lambda_j \in Z$ mit $a = \sum_j \lambda_j w_j$ (von denen nur endlich viele ungleich Null sind). Andererseits sind die v_i ein Erzeugendensystem von Z als K-Vektorraum, also gibt es auch $\mu_{i,j} \in K$ mit $\lambda_j = \sum_i \mu_{i,j} v_i$. Damit folgt $a = \sum_{i,j} \mu_{i,j} v_i w_j$, d. h. die Produkte $v_i w_j$ erzeugen L über K.

Lineare Unabhängigkeit: Es sei nun $\sum_{i,j} \lambda_{i,j} v_i w_j = 0$ für gewisse $\lambda_{i,j} \in K$ (von denen wieder nur endlich viele ungleich Null sind). Wir schreiben dies als $\sum_j (\sum_i \lambda_{i,j} v_i) w_j = 0$. Weil die Ausdrücke $\sum_i \lambda_{i,j} v_i$ in Z liegen und die w_j eine Basis von L als Z-Vektorraum sind, folgt $\sum_i \lambda_{i,j} v_i = 0$ für alle j. Da nun aber die $\lambda_{i,j}$ in K liegen und die v_i eine Basis von Z als K-Vektorraum sind, folgt sogar $\lambda_{i,j} = 0$ für alle i, j. Also sind die Produkte $v_i w_j$ linear unabhängig. □

Folgerung 2.18. *Es seien L/K eine endliche Körpererweiterung und $a \in L$. Dann ist $[a:K]$ (endlich und) ein Teiler von $[L:K]$.*

Beweis. Die Gradformel für $K \leq K(a) \leq L$ liefert $[L:K] = [L:K(a)] \cdot [K(a):K]$. Nach Satz 2.14 (a) ist nun $[K(a):K] = [a:K]$, also folgt die Behauptung. □

Aufgabe 2.19. Es seien L/K eine Körpererweiterung und $a, b \in L$ algebraisch über K.

(a) Man zeige: Sind $[a:K]$ und $[b:K]$ teilerfremd, so gilt $[K(a,b):K] = [a:K] \cdot [b:K]$.

(b) Bestimme $[K(a,b):K]$, $[a:K]$ und $[b:K]$ für den Fall $L = \mathbb{C}$, $K = \mathbb{Q}$, $a = \sqrt[3]{2}$ und $b = \sqrt[3]{2} e^{\frac{2\pi i}{3}}$.
(Hinweis: Man zeige und benutze $\mathbb{Q}(\sqrt[3]{2}, \sqrt[3]{2} e^{\frac{2\pi i}{3}}) = \mathbb{Q}(\sqrt[3]{2}, e^{\frac{2\pi i}{3}})$.)

Aufgabe 2.20. Bestimme die Minimalpolynome der folgenden reellen Zahlen über $\mathbb{Q}$:

(a) $a = \sqrt{2} + \sqrt{3}$;

(b) $a = \sqrt[3]{\sqrt{5}+2} - \sqrt[3]{\sqrt{5}-2}$. (Was sagt euer Taschenrechner zu dieser Zahl?)

Aufgabe 2.21. Es sei L/K eine endliche Körpererweiterung. Man zeige:

(a) Ist $[L:K]$ eine Primzahl, so gilt $L = K(a)$ für jedes $a \in L \backslash K$. Insbesondere ist L/K dann also eine einfache Körpererweiterung.

(b) Ist $[L:K] = 2$ und $\operatorname{char} K \neq 2$, so ist L/K sogar eine einfache 2-Radikalerweiterung.

Wir wollen unsere Ergebnisse nun auf die Fragen nach der Konstruierbarkeit mit Zirkel und Lineal aus Problem 0.3 anwenden. Da wir in Beispiel 1.23 bereits gesehen hatten, dass wir dazu entscheiden müssen, ob gewisse Zahlen in einer 2-Radikalerweiterung von $\mathbb{Q}$ liegen, müssen wir uns dazu also anschauen, was die Gradformel über 2-Radikalerweiterungen aussagt.

Folgerung 2.22. *Es sei L/K eine 2-Radikalerweiterung. Dann gilt:*

(a) *$[L:K]$ ist (endlich und) eine Zweierpotenz.*

(b) *Für alle $a \in L$ ist $[a:K]$ (endlich und) eine Zweierpotenz.*

Beweis.

(a) Nach Definition 1.18 einer 2-Radikalerweiterung gibt es eine Körperkette

$$K = K_0 \leq K_1 \leq \cdots \leq K_n = L,$$

in der jede Erweiterung K_i/K_{i-1} eine einfache 2-Radikalerweiterung ist, nach Beispiel 2.16 also Grad 1 oder 2 hat. Mit der Gradformel folgt damit

$$[L:K] = [K_n : K_{n-1}] \cdot [K_{n-1} : K_{n-2}] \cdot \cdots \cdot [K_1 : K_0] = 2^m,$$

wobei m die Anzahl der $i = 1, \ldots, n$ ist mit $[K_i : K_{i-1}] = 2$.

(b) ergibt sich mit Folgerung 2.18 unmittelbar aus (a), da jeder Teiler einer Zweierpotenz wieder eine Zweierpotenz ist. □

Beispiel 2.23 (Anwendung auf Konstruktionen mit Zirkel und Lineal)**.**

(A) (Quadratur des Kreises) Wir hatten in Beispiel 2.2 (c) bereits erwähnt, dass π transzendent über $\mathbb{Q}$ ist (was in dieser Vorlesung nicht bewiesen werden soll). Da demnach $[\pi : \mathbb{Q}] = \infty$ gilt, kann π nach Folgerung 2.22 (b) also in keiner 2-Radikalerweiterung von $\mathbb{Q}$ liegen. Aus Beispiel 1.23 wissen wir bereits, dass dies bedeutet, dass die Quadratur des Kreises mit Zirkel und Lineal nicht möglich ist.

(B) (Würfelverdoppelung) Analog zu (A) ist auch $[\sqrt[3]{2} : \mathbb{Q}] = 3$ nach Beispiel 2.9 (c) keine Zweierpotenz. Also kann auch $\sqrt[3]{2}$ nach Folgerung in keiner 2-Radikalerweiterung von $\mathbb{Q}$ liegen, womit sich wiederum aus Beispiel 1.23 ergibt, dass auch die Würfelverdoppelung mit Zirkel und Lineal unmöglich ist.

(C) (Konstruktion des n-Ecks) Um mit unseren bisherigen Ergebnissen Aussagen über die Konstruierbarkeit des regelmäßigen n-Ecks machen zu können, müssten wir nach Beispiel 1.23 den Grad $[e^{\frac{2\pi i}{n}} : \mathbb{Q}]$ bestimmen und überprüfen, für welche n er eine Zweierpotenz ist. Wir haben jedoch in Beispiel 2.9 (d) bereits gesehen, dass dieser Grad nicht so einfach zu berechnen ist. Erst im nächsten Kapitel werden wir in Satz 3.27 (b) und 3.29 in der Lage sein, das Minimalpolynom und damit den Grad von $e^{\frac{2\pi i}{n}}$ über $\mathbb{Q}$ zu bestimmen.

Bemerkung 2.24. Beachte, dass Folgerung 2.22 nur eine *notwendige* Bedingung für die Konstruierbarkeit mit Zirkel und Lineal liefert: der Grad der zu konstruierenden Zahl über $\mathbb{Q}$ muss eine Zweierpotenz sein. Die Umkehrung gilt im Allgemeinen nicht — nicht jede Körpererweiterung, deren Grad eine Zweierpotenz ist, ist eine 2-Radikalerweiterung. Haben wir also eine Zahl, deren Grad über $\mathbb{Q}$ eine Zweierpotenz ist (und dies wird bei manchen Zahlen der Form $e^{\frac{2\pi i}{n}}$ aus Beispiel 2.23 (C) vorkommen), so können wir mit den bisherigen Methoden noch keine Aussage über die Konstruierbarkeit dieser Zahl machen. Dies wird erst später mit Hilfe der Galoistheorie möglich sein (siehe Folgerung 7.8).

Aufgabe 2.25. Diese Aufgabe soll zeigen, wie das Minimalpolynom aus Definition 2.4 (a) mit dem aus den „Grundlagen der Mathematik“ bekannten Minimalpolynom von Matrizen zusammenhängt.

Es seien dazu L/K eine Körpererweiterung und $a \in L$ algebraisch vom Grad n mit Minimalpolynom m_a.

Nach Satz 2.14 (b) ist $K(a)$ ein n-dimensionaler K-Vektorraum mit Basis $B = \{1, a, a^2, \ldots, a^{n-1}\}$. Weiterhin ist $f : K(a) \to K(a)$, $x \mapsto ax$ offensichtlich eine lineare Abbildung.

Bestimme (im Sinne der „Grundlagen der Mathematik“) die Abbildungsmatrix von f bezüglich B sowie das charakteristische Polynom, das Minimalpolynom und alle Eigenwerte dieser Matrix.

(Hinweis: Dies ist eine Nachdenkaufgabe und keine Rechenaufgabe; wenn man sie geschickt angeht, hat sie eine sehr kurze Lösung! Ergebnisse aus den „Grundlagen der Mathematik“ dürfen natürlich verwendet werden.)

Aufgabe 2.26 (Unmöglichkeit der Winkeldreiteilung mit Zirkel und Lineal)**.** Neben den Konstruktionsaufgaben aus Problem 0.3 ist auch die sogenannte **Winkeldreiteilung** ein klassisches Problem,

d. h. die Fragestellung, ob und wie man zu einem gegebenen Winkel φ in der Zeichenebene mit Zirkel und Lineal einen Winkel der Größe $\frac{\varphi}{3}$ konstruieren kann. Wir wollen in dieser Aufgabe sehen, dass diese Winkeldreiteilung im Allgemeinen nicht möglich ist.

Dazu seien in der Zeichenebene die Punkte $M = \{0, 1, e^{i\varphi}\}$, d. h. ein Winkel der Größe φ, gegeben. Man zeige:

(a) Die Dreiteilung des Winkels φ ist mit Zirkel und Lineal genau dann durchführbar, wenn die Lösungen der kubischen Gleichung $4t^3 - 3t = \cos\varphi$ in einer 2-Radikalerweiterung von $\mathbb{Q}(e^{i\varphi})$ liegen.

(b) Die kubische Gleichung $4t^3 - 3t = \frac{1}{3}$ hat keine rationalen Lösungen. *(Hinweis: Mache den Ansatz $t = \frac{p}{q}$ mit teilerfremden $p, q \in \mathbb{Z}$, $q \neq 0$, und führe diese Annahme zu einem Widerspruch.)*

(c) Die Dreiteilung des Winkels $\varphi = \arccos\frac{1}{3}$ ist mit Zirkel und Lineal nicht durchführbar.

Aufgabe 2.27. Es sei L/K eine Körpererweiterung. Man zeige:

(a) Ist $M \subset L$ eine Menge algebraischer Elemente über K, so ist die Körpererweiterung $K(M)/K$ algebraisch.

(b) Sind $a_1, \ldots, a_n \in L$ endlich viele algebraische Elemente über K, so ist die Körpererweiterung $K(a_1, \ldots, a_n)/K$ sogar endlich.

(c) Ist Z ein Körper mit $K \leq Z \leq L$ und sind die Erweiterungen L/Z und Z/K algebraisch, so auch L/K.

3. Irreduzible Polynome und Kreisteilungspolynome

Aus dem letzten Kapitel wissen wir, dass wir zur Berechnung des Grades einer algebraischen Körpererweiterung Minimalpolynome benötigen: ist L/K mit $L = K(a)$ für ein $a \in L$ eine einfache algebraische Körpererweiterung, so ist ihr Grad $[L : K]$ nach Satz 2.14 (a) gleich dem Grad des Minimalpolynoms m_a von a über K. Außerdem haben wir in Lemma 2.6 bereits gesehen, dass m_a dadurch charakterisiert werden kann, dass es ein irreduzibles normiertes Polynom über K mit Nullstelle a ist. Während man normierte Polynome mit Nullstelle a in der Regel leicht finden kann, ist es jedoch in der Praxis oft schwierig zu entscheiden, ob diese Polynome auch irreduzibel sind — dies haben wir in Beispiel 2.9 (d) bereits gesehen. Das einzige Irreduzibilitätskriterium, das wir bisher kennen, ist das Ergebnis aus Aufgabe 2.7 (a), dass ein Polynom vom Grad 2 oder 3 genau dann irreduzibel ist, wenn es keine Nullstellen besitzt.

Dass diese Untersuchung der Irreduzibilität von Polynomen im Allgemeinen ein schwieriges Problem ist, kann man leicht verstehen, wenn man die analoge Situation im Ring $\mathbb{Z}$ der ganzen Zahlen betrachtet. Ihr wisst ja vermutlich, dass es sehr aufwändig ist, von einer (großen) Zahl herauszufinden, ob sie irreduzibel, also eine Primzahl ist. Die Primfaktorzerlegung einer solchen Zahl zu bestimmen ist sogar noch einmal ein ganzes Stück komplizierter; in der Tat ist es die Grundlage vieler moderner Kryptographieverfahren, dass es hierfür kaum effektivere Methoden gibt als ein zeitaufwändiges Durchprobieren aller denkbaren Teiler. Im strukturell noch komplizierteren Polynomring $K[t]$ über einem Körper K wird diese Situation natürlich in der Regel nicht besser. Wir müssen uns daher damit begnügen, in diesem Kapitel ein paar Irreduzibilitätskriterien anzugeben, die zwar in den für uns interessanten Beispielen, insgesamt jedoch nur für „relativ wenige“ Polynome funktionieren. Wir beschränken uns dabei hier auf Polynome über dem Körper $K = \mathbb{Q}$, da dies der für unsere Anwendungen relevante Fall ist.

Bemerkung 3.1. Die meisten Strategien, um die Irreduzibilität eines Polynoms in $\mathbb{Q}[t]$ zu zeigen, verfahren in zwei Schritten:

(a) zunächst führt man die Frage nach der Irreduzibilität in $\mathbb{Q}[t]$ durch geeignetes „Wegkürzen der Nenner“ auf die Irreduzibilität in $\mathbb{Z}[t]$ zurück;

(b) die Irreduzibilität in $\mathbb{Z}[t]$ zeigt man dann, indem man die Koeffizienten des Polynoms modulo einer Primzahl p reduziert und so zum oft einfacher zu behandelnden Polynomring $\mathbb{Z}_p[t]$ über dem Körper $\mathbb{Z}_p$ übergeht.

Beachte, dass der erste Teil (a) dabei nicht nur bedeutet, dass man das betrachtete Polynom f mit einer geeigneten Zahl multipliziert, so dass es in $\mathbb{Z}[t]$ liegt: auch bei einem Polynom in $\mathbb{Z}[t]$ ist es natürlich noch etwas anderes, ob man nach der Irreduzibilität in $\mathbb{Q}[t]$ oder in $\mathbb{Z}[t]$ fragt — denn es wäre ja prinzipiell denkbar, dass man zwar eine nicht-triviale Zerlegung $f = g \cdot h$ mit rationalen, aber nicht mit ganzzahligen Polynomen g und h findet, so dass f dann zwar irreduzibel in $\mathbb{Z}[t]$, aber nicht in $\mathbb{Q}[t]$ wäre.

Es stellt sich jedoch heraus, dass die Situation hier besonders schön ist und ein derartiger Fall nicht auftreten kann: eine Zerlegungsmöglichkeit eines ganzzahligen Polynoms über $\mathbb{Q}$ führt immer auch schon zu einer Zerlegungsmöglichkeit über $\mathbb{Z}$. Dies zeigt der folgende Satz, der damit den Punkt (a) der oben beschriebenen Strategie bereits klärt.

Satz 3.2 (Lemma von Gauß). *Ist ein nicht-konstantes Polynom $f \in \mathbb{Z}[t]$ irreduzibel in $\mathbb{Z}[t]$, so auch in $\mathbb{Q}[t]$.*

Beweis. Angenommen, f wäre reduzibel in $\mathbb{Q}[t]$. Wir zeigen in zwei Schritten, dass f dann auch reduzibel in $\mathbb{Z}[t]$ ist.

1. Behauptung: ist f reduzibel in $\mathbb{Q}[t]$, so gibt es ein $\lambda \in \mathbb{N}_{>0}$, so dass sich λf als Produkt nicht-konstanter Polynome in $\mathbb{Z}[t]$ schreiben lässt. Dies sieht man sofort ein: haben wir eine Zerlegung $f = g \cdot h$ mit nicht-konstanten Polynomen $g, h \in \mathbb{Q}[t]$, so gibt es natürlich $\mu, \nu \in \mathbb{N}_{>0}$, so dass $\mu g, \nu h \in \mathbb{Z}[t]$ gilt (man wähle z. B. für μ und ν das kleinste gemeinsame Vielfache der in den Koeffizienten von g bzw. h auftretenden Nenner). Mit $\lambda := \mu\nu$ erhalten wir dann die gewünschte Zerlegung $\lambda f = (\mu g)(\nu h)$ in $\mathbb{Z}[t]$.

2. Behauptung: lässt sich λf für ein $\lambda \in \mathbb{N}_{>1}$ als Produkt nicht-konstanter Polynome in $\mathbb{Z}[t]$ schreiben, so gilt dies auch für $\lambda' f$ für ein geeignetes $\lambda' < \lambda$ in $\mathbb{N}_{>0}$. Für den Beweis dieser Behauptung sei also $\lambda f = g \cdot h$ für nicht-konstante $g, h \in \mathbb{Z}[t]$. Wegen $\lambda > 1$ können wir einen Primfaktor p von λ wählen und $\lambda' := \frac{\lambda}{p} \in \mathbb{N}_{>0}$ setzen, so dass wir die Zerlegung $p\lambda' f = gh$ in $\mathbb{Z}[t]$ erhalten. Wir betrachten diese Gleichung nun in $\mathbb{Z}_p[t]$, d. h. reduzieren alle Koeffizienten der Polynome modulo p. Bezeichnet $\overline{f} \in \mathbb{Z}_p[t]$ das Polynom, das man aus $f \in \mathbb{Z}[t]$ erhält, indem man alle Koeffizienten durch ihre Restklassen in $\mathbb{Z}_p$ ersetzt (und analog für die anderen auftretenden Polynome), so bekommen wir also die Zerlegung

$$\overline{p} \cdot \overline{\lambda'} \cdot \overline{f} = \overline{g} \cdot \overline{h} \quad \in \mathbb{Z}_p[t].$$

Aber natürlich ist $\overline{p} = \overline{0}$ in $\mathbb{Z}_p[t]$, und damit erhalten wir $\overline{g} \cdot \overline{h} = \overline{0}$ in $\mathbb{Z}_p[t]$. Da $\mathbb{Z}_p[t]$ nach [G, Lemma 9.9 (b)] als Polynomring über einem Körper ein Integritätsring ist, ist dies nur möglich, wenn bereits einer der Faktoren gleich Null ist. Es sei also ohne Beschränkung der Allgemeinheit $\overline{g} = \overline{0}$ in $\mathbb{Z}_p[t]$. Dies bedeutet aber gerade, dass alle Koeffizienten von g durch p teilbar sind. Das Polynom $g' := \frac{g}{p}$ liegt damit ebenfalls in $\mathbb{Z}[t]$, und wir erhalten aus $\lambda f = g \cdot h$ nach Division durch p wie gewünscht die Zerlegung $\lambda' f = g' \cdot h$ in $\mathbb{Z}[t]$ mit $\lambda' < \lambda$. Dies zeigt auch die 2. Behauptung.

Die Aussage des Satzes ergibt sich nun offensichtlich aus der Kombination der beiden Schritte: nach der 1. Behauptung gibt es zunächst ein $\lambda \in \mathbb{N}_{>0}$, so dass λf ein Produkt nicht-konstanter Polynome in $\mathbb{Z}[t]$ ist, und durch fortgesetzte Anwendung der 2. Behauptung können wir diese Zahl λ dann so lange reduzieren, bis sie gleich 1 ist. □

Bemerkung 3.3. Der Beweis von Satz 3.2 zeigt sogar noch etwas mehr: ist $f \in \mathbb{Z}[t]$ reduzibel in $\mathbb{Q}[t]$, d. h. können wir $f = g \cdot h$ für gewisse nicht-konstante Polynome $g, h \in \mathbb{Q}[t]$ schreiben, so gibt es auch eine Zerlegung $f = g' \cdot h'$ mit $g', h' \in \mathbb{Z}[t]$, *wobei g' und h' aus g bzw. h durch Multiplikation mit einer rationalen Zahl entstehen.* In den beiden Schritten des Beweises werden die beiden Polynome der ursprünglichen Zerlegung über $\mathbb{Q}$ nämlich lediglich mit konstanten Faktoren multipliziert, um die letztendlich gewünschte Zerlegung über $\mathbb{Z}$ zu erhalten. Aus dieser Beobachtung erhalten wir das folgende nützliche Resultat.

Folgerung 3.4. *Es seien $f, g, h \in \mathbb{Q}[t]$ normierte Polynome mit $f = g \cdot h$. Gilt dann $f \in \mathbb{Z}[t]$, so liegen auch g und h bereits in $\mathbb{Z}[t]$.*

Beweis. Nach Bemerkung 3.3 gibt es $g', h' \in \mathbb{Z}[t]$, die sich von g bzw. h nur um einen konstanten Faktor unterscheiden und für die $f = g' \cdot h'$ gilt. Da der Leitkoeffizient 1 von f dabei gleich dem Produkt der ganzzahligen Leitkoeffizienten von g' und h' ist, können die Leitkoeffizienten von g' und h' außerdem nur 1 oder -1 sein. Weil g und h aber nach Voraussetzung den Leitkoeffizienten 1 haben, bedeutet dies gerade, dass $g' = \pm g$ und $h' = \pm h$ gelten muss. Mit $g', h' \in \mathbb{Z}[t]$ ergibt sich damit auch wie behauptet $g, h \in \mathbb{Z}[t]$. □

Insbesondere erhalten wir damit das folgende Kriterium, das oft bei der Suche von Nullstellen ganzzahliger Polynome hilft und das euch vielleicht in der einen oder anderen Form schon aus der Schule bekannt war.

Folgerung 3.5 (Ganzzahligkeit von Nullstellen)**.** *Es sei $f = t^n + a_{n-1}t^{n-1} + \cdots + a_0 \in \mathbb{Z}[t]$ ein normiertes Polynom. Ist $x \in \mathbb{Q}$ eine Nullstelle von f, so gilt bereits $x \in \mathbb{Z}$, und x ist ein Teiler von a_0.*

Beweis. Ist $x \in \mathbb{Q}$ eine Nullstelle von f, so können wir diese bekanntlich abspalten [G, Lemma 11.15] und $f = (t - x)\, g$ für ein normiertes Polynom $g = t^m + b_{m-1}t^{m-1} + \cdots + b_0 \in \mathbb{Q}[t]$ schreiben. Nach Folgerung 3.4 folgt dann $t - x, g \in \mathbb{Z}[t]$ und damit insbesondere $x \in \mathbb{Z}$. Vergleichen wir schließlich noch die konstanten Koeffizienten, so sehen wir außerdem $a_0 = -x\, b_0$ und damit $x \,|\, a_0$. □

Bemerkung 3.6. Aufgrund von Satz 3.2 können wir uns für den Nachweis der Irreduzibilität ganzzahliger Polynome über $\mathbb{Q}[t]$ also vollständig auf den Ring $\mathbb{Z}[t]$ zurückziehen, d. h. die Irreduzibilität lediglich in $\mathbb{Z}[t]$ überprüfen. Beachte jedoch, dass in $\mathbb{Z}[t]$ nicht alle konstanten Polynome, sondern nur die Polynome ± 1 Einheiten sind. So ist also z. B. das Polynom $2t \in \mathbb{Z}[t]$ reduzibel, da es das Produkt der Nichteinheiten 2 und t ist. Reduzibilität in $\mathbb{Z}[t]$ bedeutet also nicht notwendigerweise, dass sich das Polynom als Produkt zweier *nicht-konstanter* Polynome schreiben lässt. Um derartige Probleme zu umgehen, wollen wir uns im Folgenden auf normierte Polynome beschränken. Normierte Polynome über $\mathbb{Z}[t]$ können offensichtlich keine Konstante ungleich ± 1 als Teiler haben, so dass in diesem Fall die Reduzibilität über $\mathbb{Z}[t]$ wirklich äquivalent dazu ist, dass sich das Polynom als Produkt von nicht-konstanten Polynomen schreiben lässt.

Wir wollen im Folgenden nun zwei einfache Irreduzibilitätskriterien angeben. Wie schon in Bemerkung 3.1 (b) angekündigt ergeben sich beide (analog zum Beweis von Satz 3.2) durch Reduktion modulo einer Primzahl.

Lemma 3.7 (Irreduzibilität durch Reduktion modulo p)**.** *Es sei $f \in \mathbb{Z}[t]$ ein normiertes Polynom. Gibt es eine Primzahl p, so dass das Polynom $\overline{f} \in \mathbb{Z}_p[t]$ irreduzibel in $\mathbb{Z}_p[t]$ ist, so ist bereits f irreduzibel in $\mathbb{Z}[t]$ (und damit nach Satz 3.2 auch in $\mathbb{Q}[t]$).*

Beweis. Wäre f reduzibel in $\mathbb{Z}[t]$, nach Bemerkung 3.6 also $f = g \cdot h$ für nicht-konstante $g, h \in \mathbb{Z}[t]$, so wäre natürlich auch $\overline{f} = \overline{g} \cdot \overline{h}$ reduzibel in $\mathbb{Z}_p[t]$. □

Beispiel 3.8. Man prüft leicht nach, dass das Polynom $f = t^4 + t^3 + t^2 + t + 1 \in \mathbb{Z}_2[t]$ irreduzibel ist [G, Aufgabe 11.8 (a)] — z. B. indem man explizit nachrechnet, dass die Polynome in $\mathbb{Z}_2[t]$ vom Grad 1 und 2 (von denen es ja nur sehr wenige gibt) alle keine Teiler von f sind. Also ist nach Lemma 3.7 jedes normierte ganzzahlige Polynom, dessen Reduktion modulo 2 gleich f ist (d. h. jedes Polynom $t^4 + a_3t^3 + a_2t^2 + a_1t + a_0 \in \mathbb{Z}[t]$ mit ungeraden $a_0, \ldots, a_3$) irreduzibel in $\mathbb{Z}[t]$ und auch in $\mathbb{Q}[t]$.

Satz 3.9 (Irreduzibilitätskriterium von Eisenstein). *Es sei $f = t^n + a_{n-1}t^{n-1} + \cdots + a_1t + a_0 \in \mathbb{Z}[t]$ ein normiertes Polynom. Gibt es eine Primzahl p, so dass $p \mid a_i$ für alle $i = 0, \ldots, n-1$ sowie $p^2 \nmid a_0$ gilt, so ist f irreduzibel in $\mathbb{Z}[t]$ (und damit nach Satz 3.2 auch in $\mathbb{Q}[t]$).*

Beweis. Angenommen, f wäre reduzibel in $\mathbb{Z}[t]$, nach Bemerkung 3.6 also von der Form $f = g \cdot h$ für gewisse nicht-konstante $g, h \in \mathbb{Z}[t]$. Ein Vergleich der Leitkoeffizienten liefert sofort, dass g und h dann Leitkoeffizient ± 1 haben müssen und damit ohne Beschränkung der Allgemeinheit als normiert vorausgesetzt werden können.

Wir reduzieren die Gleichung $f = g \cdot h$ nun wieder modulo p. Da p nach Voraussetzung alle Koeffizienten $a_0, \ldots, a_{n-1}$ von f teilt, folgt $\overline{f} = t^n$ und damit $\overline{g} \cdot \overline{h} = t^n$ in $\mathbb{Z}_p[t]$. Weil es in $\mathbb{Z}_p[t]$ nach [G, Satz 11.9] eine eindeutige Primfaktorzerlegung gibt und t in $\mathbb{Z}_p[t]$ als irreduzibles Polynom natürlich prim ist [G, Bemerkung 11.6], ist t demnach der einzige Primfaktor, der in $\overline{g}$ und $\overline{h}$ auftreten kann, d. h. es ist $\overline{g} = t^k$ und $\overline{h} = t^l$ für gewisse $k, l \geq 1$.

Insbesondere bedeutet dies nun, dass die konstanten Koeffizienten von g und h gleich 0 modulo p, also durch p teilbar sein müssen. Damit ist dann der konstante Koeffizient von f, der ja wegen $f = g \cdot h$ das Produkt der konstanten Koeffizienten von g und h ist, aber durch p^2 teilbar, was ein Widerspruch zur Voraussetzung ist. □

Beispiel 3.10. Es seien p eine Primzahl und $n \in \mathbb{N}_{>0}$. Dann ist das normierte Polynom $t^n - p$ nach dem Kriterium von Eisenstein aus Satz 3.9 sowohl in $\mathbb{Z}[t]$ als auch in $\mathbb{Q}[t]$ irreduzibel. Da es außerdem $\sqrt[n]{p}$ als Nullstelle hat, ist es nach Lemma 2.6 das Minimalpolynom von $\sqrt[n]{p}$ über $\mathbb{Q}$. Also gilt stets $[\sqrt[n]{p} : \mathbb{Q}] = n$. Dies verallgemeinert die Ergebnisse von Beispiel 2.9 (b) und (c).

Aufgabe 3.11. Zu einer Körpererweiterung L/K bezeichne $\overline{K}^L \subset L$ die Menge aller Elemente von L, die über K algebraisch sind. Man zeige:

(a) $\overline{K}^L$ ist ein Körper.

(b) Die Körpererweiterung $\overline{\mathbb{Q}}^{\mathbb{R}}/\mathbb{Q}$ ist algebraisch, aber nicht endlich.

Aufgabe 3.12 (Varianten des Irreduzibilitätskriteriums von Eisenstein)**.** Es sei $f = t^n + a_{n-1}t^{n-1} + \cdots + a_0 \in \mathbb{Z}[t]$ ein ganzzahliges normiertes Polynom vom Grad $n \geq 2$, so dass kein Teiler von a_0 eine Nullstelle von f ist. Man zeige, dass f dann irreduzibel in $\mathbb{Z}[t]$ und damit auch in $\mathbb{Q}[t]$ ist, wenn eine der folgenden beiden Bedingungen gilt:

(a) $p \,|\, a_i$ für alle $i = 0, \ldots, n-2$ sowie $p^2 \nmid a_0$;

(b) $p \,|\, a_i$ für alle $i = 0, \ldots, n-1$ sowie $p^2 \nmid a_1$.

04

Für den Rest dieses Kapitels wollen wir nun mit Hilfe der bisherigen Resultate die Minimalpolynome und Grade der Zahlen $e^{\frac{2\pi i}{n}}$ über $\mathbb{Q}$ bestimmen. Damit kommen wir dann auch bei unserer Frage nach der Konstruierbarkeit mit Zirkel und Lineal weiter — da wir ja aus Beispiel 1.23 (C) schon wissen, dass das regelmäßige n-Eck genau dann mit Zirkel und Lineal konstruierbar ist, wenn $e^{\frac{2\pi i}{n}}$ in einer 2-Radikalerweiterung liegt, und dies nach Folgerung 2.22 (b) höchstens dann möglich ist, wenn $[e^{\frac{2\pi i}{n}} : \mathbb{Q}]$ eine Zweierpotenz ist.

Da die komplexen Zahlen der Form $e^{\frac{2\pi i}{n}}$, oder allgemeiner die Lösungen der Gleichung $t^n - 1 = 0$, in der Praxis eine wichtige Rolle spielen, werden wir ihnen zunächst einen speziellen Namen geben.

Definition 3.13 (Einheitswurzeln)**.** Es sei $n \in \mathbb{N}_{>0}$. Wir setzen

$$E_n := \{z \in \mathbb{C} : z^n = 1\} = \left\{e^{\frac{2\pi i k}{n}} : k \in \mathbb{Z}\right\} = \left\{e^{\frac{2\pi i k}{n}} : k = 0, \ldots, n-1\right\}$$

und nennen die Elemente von E_n die **n-ten Einheitswurzeln**. Die Elemente der Teilmenge

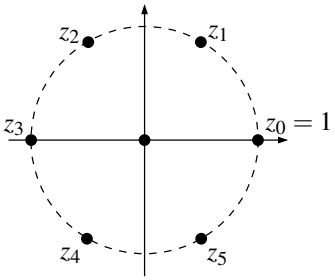
$$E_n' := \{z \in E_n : z^k \neq 1 \text{ für alle } k \text{ mit } 1 \leq k < n\},$$

also die n-ten Einheitswurzeln, für die n auch die kleinste Potenz ist, bei der wieder 1 herauskommt, werden **primitive n-te Einheitswurzeln** genannt.

Beispiel 3.14.

(a) Für $n = 1$ ist offensichtlich ist $E_1 = E_1' = \{1\}$. Für $n = 2$ ergibt sich $E_2 = \{1, -1\}$ sowie $E_2' = \{-1\}$.

(b) Das Bild rechts zeigt die sechs 6-ten Einheitswurzeln $z_k := e^{\frac{2\pi i k}{6}}$ für $k = 0, \ldots, 5$. Von ihnen sind genau z_1 und z_5 primitiv — denn es ist ja $z_0^1 = z_2^3 = z_3^2 = z_4^3 = 1$, wohingegen alle Potenzen z_1^m und z_5^m für $m = 1, \ldots, 5$ ungleich 1 sind.



Bemerkung 3.15.

(a) Offensichtlich ist E_n zusammen mit der Multiplikation eine Untergruppe von $(\mathbb{C}^*, \cdot) = (\mathbb{C}\backslash\{0\}, \cdot)$. In der Tat ist sie genau das Bild des Gruppenhomomorphismus

$$f : (\mathbb{Z}, +) \to (\mathbb{C}^*, \cdot), \quad k \mapsto e^{\frac{2\pi i k}{n}}.$$

Da der Kern von f genau $n\mathbb{Z}$ ist, folgt aus dem Homomorphiesatz [G, Satz 6.17], dass die Abbildung

$$g : (\mathbb{Z}_n, +) \to (E_n, \cdot), \quad \overline{k} \mapsto e^{\frac{2\pi i k}{n}}$$

ein Gruppenisomorphismus ist: die Gruppe E_n der n-ten Einheitswurzeln ist isomorph zu $\mathbb{Z}_n$.

(b) Man kann leicht sehen, welche Einheitswurzeln primitiv sind: es sei dazu $z = e^{\frac{2\pi ik}{n}} \in E_n$. Dann gilt

$$\begin{aligned}
z \in E_n' &\Leftrightarrow \text{die Ordnung von } z \text{ in } \mathbb{C}^* \text{ ist } n && \text{(Definition 3.13)}\\
&\Leftrightarrow \text{die Ordnung von } \overline{k} \text{ in } \mathbb{Z}_n \text{ ist } n && \text{((a))}\\
&\Leftrightarrow \langle \overline{k} \rangle = \mathbb{Z}_n && \text{([G, Lemma 5.14])}\\
&\Leftrightarrow \overline{1} \in \langle \overline{k} \rangle = \{\overline{ak} : a \in \mathbb{Z}\}\\
&\Leftrightarrow \overline{k} \text{ ist eine Einheit in } \mathbb{Z}_n\\
&\Leftrightarrow \operatorname{ggt}(k,n) = 1 && \text{([G, Folgerung 10.31]).}
\end{aligned}$$

Unter dem Isomorphismus aus (a) entsprechen die primitiven n-ten Einheitswurzeln $E_n' \subset E_n$ also genau den Einheiten $\mathbb{Z}_n^* \subset \mathbb{Z}_n$; insbesondere ist damit $|E_n'| = |\mathbb{Z}_n^*|$. In Beispiel 3.14 (b) für $n = 6$ waren dies genau $e^{1 \cdot \frac{2\pi i}{6}}$ und $e^{5 \cdot \frac{2\pi i}{6}}$, entsprechend den Einheiten $\overline{1}$ und $\overline{5}$ in $\mathbb{Z}_6$, bzw. entsprechend den zu 6 teilerfremden Zahlen 1 und 5 in $\{0,\dots,5\}$.

Mit Hilfe der primitiven Einheitswurzeln können wir nun bereits die Polynome definieren, die sich später als die Minimalpolynome von $e^{\frac{2\pi i}{n}}$ herausstellen werden:

Definition 3.16 (Kreisteilungspolynome)**.** Für $n \in \mathbb{N}_{>0}$ heißt

$$\Phi_n := \prod_{z \in E_n'} (t - z) \quad \in \mathbb{C}[t]$$

das **n-te Kreisteilungspolynom**.

Beispiel 3.17. Aus Beispiel 3.14 erhalten wir z. B.

$$\begin{aligned}
\Phi_1 &= t - 1,\\
\Phi_2 &= t + 1,\\
\Phi_6 &= \left(t - e^{\frac{2\pi i}{6}}\right)\left(t - e^{5 \cdot \frac{2\pi i}{6}}\right) = t^2 - t + 1.
\end{aligned}$$

Für größere n ist die Berechnung von Φ_n direkt nach Definition 3.16 oft recht umständlich. Die folgende rekursive Formel ist hier in der Regel nützlicher.

Lemma 3.18 (Rekursive Formel für die Kreisteilungspolynome)**.** *Für alle $n \in \mathbb{N}_{>0}$ ist E_n die disjunkte Vereinigung aller E_d' mit $d \mid n$. Insbesondere gilt also*

$$t^n - 1 \;= \prod_{d \mid n} \Phi_d \quad \in \mathbb{C}[t].$$

Beweis. Nach Bemerkung 3.15 (b) ist E_d' genau die Menge aller Elemente der Ordnung d in $\mathbb{C}^*$. Insbesondere ist die Vereinigung aller E_d' also disjunkt.

Ist nun $z \in E_n$, so ist die Ordnung d von z nach [G, Folgerung 5.15 (a)] ein Teiler von $|E_n| = n$, also ist dann auch $z \in E_d'$ für ein $d \mid n$. Ist umgekehrt $z \in E_d'$ für ein $d \mid n$, so folgt mit $z^d = 1$ natürlich auch $z^n = 1$ und damit $z \in E_n$. Insgesamt zeigt dies, dass E_n die disjunkte Vereinigung aller E_d' mit $d \mid n$ ist.

Die behauptete Gleichheit von Polynomen folgt nun unmittelbar, da auf beiden Seiten offensichtlich das (eindeutig bestimmte) normierte Polynom vom Grad n mit den Nullstellen E_n steht. □

Beispiel 3.19.

(a) Für $n = 6$ liefert Lemma 3.18 die disjunkte Zerlegung $E_6 = E_6' \cup E_3' \cup E_2' \cup E_1'$. Dies hatten wir in Beispiel 3.14 (b) auch schon direkt gesehen: mit der dortigen Bezeichnung $z_k = e^{\frac{2\pi ik}{6}}$ für $k = 0,\dots,5$ ist $E_6 = \{z_0,\dots,z_5\}$, $E_6' = \{z_1, z_5\}$, $E_3' = \{z_2, z_4\}$, $E_2' = \{z_3\}$ und $E_1' = \{z_0\}$.

(b) Ist p eine Primzahl, so liefert die Formel aus Lemma 3.18

$$t^p - 1 = \Phi_p \cdot \Phi_1 = \Phi_p \cdot (t-1)$$

und damit nach der endlichen geometrischen Reihe

$$\Phi_p = \frac{t^p - 1}{t-1} = t^{p-1} + t^{p-2} + \cdots + t + 1.$$

(c) Allgemeiner kann man für alle $n \in \mathbb{N}_{>0}$ die Formel aus Lemma 3.18 zu der Gleichung

$$\Phi_n = (t^n - 1) \Big/ \prod_{\substack{d \mid n \\ d < n}} \Phi_d$$

umstellen, mit der man alle Φ_n leicht durch rekursive Polynomdivision berechnen kann.

Aufgabe 3.20. Man zeige:

(a) $\Phi_{p^r}(t) = \Phi_p(t^{p^{r-1}})$ für jede Primzahl p und alle $r \geq 1$;

(b) $\Phi_{2n}(t) = \Phi_n(-t)$ für alle ungeraden $n > 1$.

Obwohl Definition 3.16 komplexe Zahlen benutzt und damit a priori komplexe Polynome liefert, haben sich alle unsere bisher berechneten Kreisteilungspolynome in den Beispielen 3.17 und 3.19 (b) als ganzzahlig herausgestellt. Dies ist kein Zufall, wie der folgende Satz zeigt.

Satz 3.21 (Ganzzahligkeit der Kreisteilungspolynome)**.** *Für alle $n \in \mathbb{N}_{>0}$ gilt $\Phi_n \in \mathbb{Z}[t]$.*

Beweis. Wir zeigen die Behauptung mit Induktion über n; der Induktionsanfang für $n = 1$ ist klar wegen $\Phi_1 = t - 1$.

Für den Induktionsschritt sei nun $n \in \mathbb{N}_{>1}$. Nach Induktionsvoraussetzung ist dann

$$f_n := \prod_{\substack{d \mid n \\ d < n}} \Phi_d \quad \in \mathbb{Z}[t]$$

ein normiertes ganzzahliges Polynom. Wir können nun $t^n - 1$ in $\mathbb{Q}[t]$ mit Rest durch f_n dividieren und erhalten

$$t^n - 1 = q f_n + r \quad \in \mathbb{Q}[t]$$

für gewisse $q, r \in \mathbb{Q}[t]$ mit $\deg r < \deg f_n$. Außerdem ergibt Lemma 3.18

$$t^n - 1 = \Phi_n f_n \quad \in \mathbb{C}[t].$$

Subtraktion dieser beiden Gleichungen voneinander liefert nun

$$(\Phi_n - q) f_n = r \quad \in \mathbb{C}[t],$$

nach der Gradformel [G, Lemma 9.9 (a)] also $\deg(\Phi_n - q) + \deg f_n = \deg r$. Wegen $\deg r < \deg f_n$ ist dies aber nur dann möglich, wenn $\deg(\Phi_n - q) = \deg r = -\infty$, also $\Phi_n - q = r = 0$ ist. Insbesondere ist damit $\Phi_n = q \in \mathbb{Q}[t]$. Aus der Gleichung $t^n - 1 = \Phi_n f_n$ in $\mathbb{Q}[t]$ ergibt sich dann mit Folgerung 3.4 auch sofort $\Phi_n \in \mathbb{Z}[t]$. □

Bemerkung 3.22. Berechnet man z. B. mit Hilfe der Rekursionsformel aus Lemma 3.18 einmal einige Kreisteilungspolynome, so stellt man schnell fest, dass die Koeffizienten dieser Polynome nicht nur ganzzahlig, sondern „sehr oft“ sogar nur 0, 1 oder -1 sind — allerdings mit einer kaum zu durchschauenden Verteilung. So ist z. B.

$$\Phi_{42} = t^{12} + t^{11} - t^9 - t^8 + t^6 - t^4 - t^3 + t + 1.$$

In der Tat ist das erste(!) Kreisteilungspolynom, das überhaupt einen Koeffizienten vom Betrag größer als 1 besitzt,

$$\begin{aligned}\Phi_{105} = {} & t^{48} + t^{47} + t^{46} - t^{43} - t^{42} - 2t^{41} - t^{40} - t^{39} + t^{36} + t^{35} + t^{34} + t^{33} + t^{32} + t^{31} - t^{28} - t^{26} \\ & - t^{24} - t^{22} - t^{20} + t^{17} + t^{16} + t^{15} + t^{14} + t^{13} + t^{12} - t^9 - t^8 - 2t^7 - t^6 - t^5 + t^2 + t + 1.\end{aligned}$$

Dennoch kann man ebenfalls zeigen, dass die Menge aller in den Kreisteilungspolynomen auftretenden Koeffizienten unbeschränkt ist.

Fassen wir unsere bisherigen Ergebnisse zu den Kreisteilungspolynomen zusammen, so wissen wir also, dass Φ_n ein normiertes, ganzzahliges (und damit insbesondere rationales) Polynom mit Nullstelle $e^{\frac{2\pi i}{n}}$ ist. Um zu zeigen, dass Φ_n wirklich das Minimalpolynom von $e^{\frac{2\pi i}{n}}$ ist, bleibt also nach Lemma 2.6 nur noch seine Irreduzibilität zu zeigen. Allerdings ist leider keines unserer bisherigen Irreduzibilitätskriterien auf die Kreisteilungspolynome anwendbar; wir müssen hierfür also einen neuen Beweis angeben. Wie unsere bisherigen Kriterien benutzt auch dieser (nicht ganz einfache) Beweis Reduktion modulo einer Primzahl. Er verwendet die folgenden beiden Hilfsaussagen, die wir beide später in dieser Vorlesung noch einmal wiedersehen werden.

Lemma 3.23 (Rechenregeln für Potenzen in $\mathbb{Z}_p$)**.** *Für $a \in \mathbb{Z}_p$ und $f, g \in \mathbb{Z}_p[t]$ gelten die folgenden einfachen Rechenregeln:*

(a) $(f+g)^p = f^p + g^p$;

(b) $a^p = a$;

(c) $f(t^p) = f(t)^p$.

Beweis.

(a) Nach der binomischen Formel gilt zunächst natürlich

$$(f+g)^p = \sum_{i=0}^{p} \binom{p}{i} f^i g^{p-i} = f^p + g^p + \sum_{i=1}^{p-1} \binom{p}{i} f^i g^{p-i}.$$

Nun ist p aber für $i = 1, \ldots, p-1$ ein Teiler des Binomialkoeffizienten

$$\binom{p}{i} = \frac{p \cdot (p-1) \cdot \cdots \cdot (p-i+1)}{1 \cdot 2 \cdot \cdots \cdot i},$$

da p zwar im Zähler, aber nicht im Nenner dieses Bruches auftritt. Also ist dieser Binomialkoeffizient gleich Null in $\mathbb{Z}_p$, woraus die Behauptung folgt.

(b) Für $a = 0$ ist die Aussage natürlich klar. Andernfalls ist $a \in \mathbb{Z}_p^*$ eine Einheit, da $\mathbb{Z}_p$ ein Körper ist. Wegen $|\mathbb{Z}_p^*| = |p-1|$ folgt aus dem kleinen Satz von Fermat [G, Folgerung 5.15 (b)] also $a^{p-1} = 1$ und damit $a^p = a$.

(c) Ist $f = \sum_n a_n t^n$, so folgt

$$f(t)^p = \Big(\sum_n a_n t^n\Big)^p \overset{(a)}{=} \sum_n a_n^p t^{pn} \overset{(b)}{=} \sum_n a_n t^{pn} = f(t^p). \qquad \square$$

Lemma 3.24 (Formale Ableitungen)**.** *Für ein Polynom $f = \sum_n a_n t^n \in K[t]$ über einem Körper K betrachten wir die **formale Ableitung** $f' := \sum_n n a_n t^{n-1}$. Für diese gilt:*

(a) *Für alle $f, g \in K[t]$ ist $(f+g)' = f' + g'$ und $(fg)' = f'g + fg'$.*

(b) *Ist $f \in K[t]$ ein Polynom, das teilerfremd zu seiner formalen Ableitung f' ist, so hat f keine mehrfachen Faktoren in seiner Primfaktorzerlegung (und damit insbesondere keine mehrfachen Nullstellen).*

Beweis.

(a) Dies ergibt sich durch einfaches Nachrechnen, siehe z. B. [G, Aufgabe 9.10].

(b) Angenommen, f hätte einen mehrfachen Faktor in seiner Primfaktorzerlegung, d. h. es wäre $f = g^2 h$ für $g, h \in K[t]$ mit $\deg g > 0$. Anwenden der Differentiationsregeln aus (a) ergibt dann

$$f' = 2gg'h + g^2 h' = g(2g'h + gh'),$$

woraus wir sehen, dass f und f' im Widerspruch zur Annahme den gemeinsamen Teiler g haben. $\square$

Bemerkung 3.25. Die Rechenregeln aus Lemma 3.24 (a) sind euch für reelle Polynome und die in der Analysis definierte Ableitung natürlich bereits aus der Schule bzw. aus den „Grundlagen der Mathematik“ bekannt. Auch die Aussage aus Teil (b) habt ihr dort vielleicht schon einmal gesehen — zumindest wohl in der Form, dass mehrfache Nullstellen eines Polynoms auch Nullstellen seiner Ableitung sind. Die besondere Aussage in Lemma 3.24 ist, dass dies nicht nur über $\mathbb{R}$, sondern für die nun rein formal definierte Ableitung auch über jedem beliebigen Körper gilt. In der Tat werden wir dieses Resultat im Beweis der Irreduzibilität der Kreisteilungspolynome für die endlichen Körper $\mathbb{Z}_p$ anwenden, und zwar für das folgende Beispiel.

Beispiel 3.26. Wir betrachten das Polynom $f = t^n - 1$ über einem Körper K. Offensichtlich ist $f' = nt^{n-1}$.

(a) Ist $\operatorname{char} K$ kein Teiler von n (z. B. im Fall $\operatorname{char} K = 0$), so ist $n \neq 0$ in K und damit $f' \neq 0$. Da die Primfaktorzerlegung von f' dann t als einzigen Primfaktor enthält und dieser offensichtlich kein Teiler von f ist, sind f und f' teilerfremd. Nach Lemma 3.24 (b) hat f in diesem Fall also keine mehrfachen Faktoren. Für $K = \mathbb{C}$ wussten wir dies bereits, denn da hat $t^n - 1$ ja genau die n verschiedenen Linearfaktoren $t - z$ für $z \in E_n$.

(b) Ist $\operatorname{char} K = p > 0$ ein Teiler von n, so ist $f' = 0$ das Nullpolynom. Damit sind f und f' nicht teilerfremd (jeder Teiler von f ist ja auch einer von f'), d. h. Lemma 3.24 (b) ist nicht anwendbar. In der Tat kann es dann auch passieren, dass f mehrfache Faktoren besitzt: für $n = p > 2$ und $K = \mathbb{Z}_p$ zum Beispiel ist $f = t^p - 1 = (t-1)^p$ nach Lemma 3.23 (a).

Mit diesen beiden Hilfsaussagen können wir nun wie angekündigt zeigen, dass Φ_n das Minimalpolynom von $e^{\frac{2\pi i}{n}}$ ist.

Satz 3.27 (Irreduzibilität der Kreisteilungspolynome)**.** *Es sei $n \in \mathbb{N}_{>0}$. Dann gilt:*

(a) *Ist $z \in E_n$ eine n-te Einheitswurzel und $m \in \mathbb{N}_{>0}$ mit $\operatorname{ggt}(m,n) = 1$, so haben z und z^m dasselbe Minimalpolynom über $\mathbb{Q}$.*

(b) *$e^{\frac{2\pi i}{n}}$ hat das Minimalpolynom Φ_n über $\mathbb{Q}$. Insbesondere ist Φ_n also irreduzibel in $\mathbb{Q}[t]$.*

Beweis.

(a) Wir betrachten zunächst den Spezialfall, dass $m = p$ eine Primzahl ist. Es seien f und g die Minimalpolynome von z bzw. z^p in $\mathbb{Q}[t]$. Wir machen einen Widerspruchsbeweis und nehmen also an, dass $f \neq g$.

(1) Natürlich ist $t^n - 1 \in \mathbb{Z}[t]$ ein normiertes Polynom mit Nullstellen z und z^p. Nach Bemerkung 2.5 sind die Minimalpolynome f und g dann Teiler von $t^n - 1$. Da sie irreduzibel sind und wir sie als verschieden angenommen haben, gilt also $t^n - 1 = f \cdot g \cdot h$ für ein (ebenfalls normiertes) Polynom $h \in \mathbb{Q}[t]$. Mit Folgerung 3.4 sehen wir, dass dann sogar $f, g, h \in \mathbb{Z}[t]$ gelten muss. Wir können die Gleichung also modulo p reduzieren und erhalten $t^n - 1 = \overline{f} \cdot \overline{g} \cdot \overline{h}$ in $\mathbb{Z}_p[t]$. Da nach Voraussetzung $p \nmid n$ gilt, hat nun $t^n - 1$ nach Beispiel 3.26 (a) keine mehrfachen Nullstellen in $\mathbb{Z}_p[t]$. Damit müssen $\overline{f}$ und $\overline{g}$ in $\mathbb{Z}_p[t]$ offensichtlich teilerfremd sein, denn ein gemeinsamer Teiler von ihnen wäre ja ein quadratischer Teiler von $t^n - 1 \in \mathbb{Z}_p[t]$.

(2) Andererseits ist z nach Konstruktion von g auch eine Nullstelle von $g(t^p)$. Also muss das Minimalpolynom f von z nach Bemerkung 2.5 ein Teiler von $g(t^p)$ sein, d. h. es gibt ein Polynom $k \in \mathbb{Q}[t]$ mit $g(t^p) = f \cdot k$. Wir haben f und g (und damit auch $g(t^p)$) aber oben schon als ganzzahlige Polynome erkannt, und damit ist nach Folgerung 3.4 auch $k \in \mathbb{Z}[t]$. Wir können unsere Gleichung also wieder modulo p reduzieren und erhalten nach Lemma 3.23 (c)

$$\overline{f} \cdot \overline{k} = \overline{g(t^p)} = \overline{g}^p \quad \in \mathbb{Z}_p[t].$$

Dies ist aber nur möglich, wenn jeder Primfaktor von $\overline{f}$ auch einer von $\overline{g}$ ist — im Widerspruch zum Resultat von (1). Dies zeigt die Behauptung (a) für den Fall, dass $m = p$ eine Primzahl ist.

Fortgesetzte Anwendung dieses Ergebnisses liefert nun sofort, dass auch die Zahlen z und $z^{p_1 \cdots p_r} = ((z^{p_1}) \cdots)^{p_r}$ das gleiche Minimalpolynom haben, sofern die Primzahlen $p_1, \ldots, p_r$ keine Teiler von n sind. Da sich jede Zahl m mit $\operatorname{ggt}(m,n) = 1$ als Produkt derartiger Primzahlen schreiben lässt, folgt damit die Behauptung (a).

(b) Das Minimalpolynom von $z = e^{\frac{2\pi i}{n}}$ muss nach (a) auch alle z^m mit $\operatorname{ggt}(m,n) = 1$ als Nullstellen haben. Dies sind nach Bemerkung 3.15 (b) aber genau die primitiven Einheitswurzeln. Damit kann der Grad des Minimalpolynoms von z nicht kleiner als $|E_n'|$ sein. Da dies nach Definition 3.16 aber genau der Grad von Φ_n ist, sehen wir, dass Φ_n wirklich das normierte Polynom minimalen Grades mit Nullstelle z, also das Minimalpolynom von z ist. Insbesondere ist Φ_n nach Lemma 2.6 damit irreduzibel in $\mathbb{Q}[t]$. □

Bemerkung 3.28. Da Φ_n die primitiven n-ten Einheitswurzeln als Nullstellen hat, normiert und nach Satz 3.27 (b) auch irreduzibel in $\mathbb{Q}[t]$ ist, sehen wir als leichte Verallgemeinerung von Satz 3.27 (b), dass Φ_n nicht nur das Minimalpolynom von $e^{\frac{2\pi i}{n}}$, sondern sogar von jeder primitiven n-ten Einheitswurzel ist.

Nachdem wir nun die Minimalpolynome Φ_n der Einheitswurzeln $e^{\frac{2\pi i}{n}}$ kennen, wollen wir natürlich auch noch den Grad dieser Polynome bestimmen. Dieser ist nach Konstruktion genau $|E_n'|$, also $|\mathbb{Z}_n^*|$ nach Bemerkung 3.15 (b). Wenn ihr die Vorlesung „Elementare Zahlentheorie“ schon gehört habt, wisst ihr bereits, was hierbei herauskommt:

Satz 3.29 (Grad der Kreisteilungspolynome)**.** *Es sei $n \in \mathbb{N}_{>0}$ eine natürliche Zahl mit Primfaktorzerlegung $n = p_1^{k_1} \cdot \cdots \cdot p_r^{k_r}$ (für verschiedene Primzahlen $p_1, \ldots, p_r$). Dann gilt für jede primitive n-te Einheitswurzel z*

$$[z : \mathbb{Q}] = \deg \Phi_n = |E_n'| = |\mathbb{Z}_n^*| = \varphi(n),$$

*wobei φ die **Eulersche φ-Funktion***

$$\varphi(n) := \prod_{i=1}^{r} (p_i - 1)\, p_i^{k_i - 1}$$

ist.

Beweis. Die erste Gleichheit ist Bemerkung 3.28, die zweite folgt aus Definition 3.16, und die dritte aus Bemerkung 3.15 (b). Es bleibt also nur noch die letzte Gleichheit, d. h. die Anzahl der Einheiten in $\mathbb{Z}_n$ zu berechnen. Wir tun dies in zwei Schritten:

1. Fall: $n = p^k$ ist eine Primzahlpotenz. Die *Nichteinheiten* von $\mathbb{Z}_n$ sind dann genau $\overline{m}$ für alle $m = 0, \ldots, p^k - 1$, die einen gemeinsamen Teiler mit p^k haben [G, Folgerung 10.31]. Dies sind genau die Vielfachen von p, also die p^{k-1} Zahlen $m = i\,p$ mit $i = 0, \ldots, p^{k-1} - 1$. Damit folgt $|\mathbb{Z}_{p^k}^*| = n - p^{k-1} = (p-1)\,p^{k-1}$.

2. Fall: $n = p_1^{k_1} \cdot \cdots \cdot p_r^{k_r}$ ist eine beliebige natürliche Zahl. Nach dem chinesischen Restsatz [G, Satz 11.22] gilt dann

$$\mathbb{Z}_n \cong \mathbb{Z}_{p_1^{k_1}} \times \cdots \times \mathbb{Z}_{p_r^{k_r}}.$$

Da ein Element in einem Produktring nach Definition der Ringstruktur offensichtlich genau dann eine Einheit ist, wenn jede Komponente eine Einheit ist, folgt daraus auch

$$\mathbb{Z}_n^* \cong \left(\mathbb{Z}_{p_1^{k_1}}\right)^* \times \cdots \times \left(\mathbb{Z}_{p_r^{k_r}}\right)^*$$

Nach dem 1. Fall ergibt sich hieraus sofort die behauptete Formel $|\mathbb{Z}_n^*| = \varphi(n)$. □

05

Aufgabe 3.30. Man zeige: ist $n > 2$, so gilt $\left[z + \frac{1}{z} : \mathbb{Q}\right] = \frac{1}{2}\varphi(n)$ für jede primitive n-te Einheitswurzel z.

Wie bereits angekündigt hat Satz 3.29 natürlich eine unmittelbare Anwendung auf die Frage nach der Konstruierbarkeit des regelmäßigen n-Ecks mit Zirkel und Lineal. Dazu müssen wir nach Beispiel 2.23 (C) herausfinden, wann $[e^{\frac{2\pi i}{n}} : \mathbb{Q}] = \varphi(n)$ eine Zweierpotenz ist.

Lemma 3.31. *Es sei $n \in \mathbb{N}_{>0}$. Dann ist $\varphi(n)$ genau dann eine Zweierpotenz, wenn n von der Form*

$$n = 2^m \cdot p_1 \cdot \cdots \cdot p_r$$

ist, wobei $r, m \geq 0$ gilt und $p_1, \ldots, p_r$ verschiedene Primzahlen der Form $p_i = 2^{2^{a_i}} + 1$ mit $a_1, \ldots, a_r \in \mathbb{N}$ sind.

Beweis. Hat n die angegebene Form, so ist nach Satz 3.29

$$\varphi(n) = \begin{cases} \prod_{i=1}^r 2^{2^{a_i}} & \text{für } m = 0, \\ 2^{m-1} \cdot \prod_{i=1}^r 2^{2^{a_i}} & \text{für } m > 0 \end{cases}$$

eine Zweierpotenz. Hat umgekehrt n die allgemeine Primfaktorzerlegung $n = p_1^{k_1} \cdot \cdots \cdot p_r^{k_r}$ und ist

$$\varphi(n) = \prod_{i=1}^r (p_i - 1)\, p_i^{k_i - 1}$$

eine Zweierpotenz, so können ungerade Primfaktoren wegen des Faktors $p_i^{k_i-1}$ in $\varphi(n)$ offensichtlich nur einfach auftreten, und wegen des Faktors $p_i - 1$ müssen sie von der Form $p_i = 2^{b_i} + 1$ für gewisse $b_i \in \mathbb{N}_{>0}$ sein.

Es bleibt also nur noch zu zeigen, dass eine Zahl der Form $2^b + 1$ nur dann eine Primzahl sein kann, wenn b selbst eine Zweierpotenz ist. Nehmen wir also an, b wäre keine Zweierpotenz. Dann könnten wir b als $b = qc$ mit ungeradem $q > 1$ und geeignetem $c < b$ schreiben. Setzen wir in der Identität

$$x^q - y^q = (x - y) \cdot (x^{q-1} + x^{q-2}y + \cdots + xy^{q-2} + y^{q-1})$$

dann $x = 2^c$ und $y = -1$ ein, so ist die linke Seite gleich $2^b + 1$, und auf der rechten Seite haben wir den nicht-trivialen Faktor $x - y = 2^c + 1$. Also kann $2^b + 1$ dann nicht prim sein, was zu zeigen war. □

Bemerkung 3.32 (Fermatsche Primzahlen)**.** Die in Lemma 3.31 auftretenden Primzahlen der Form $2^{2^a} + 1$ für $a \in \mathbb{N}$ nennt man **Fermatsche Primzahlen**. Die ersten Zahlen dieser Form sind

a	0	1	2	3	4
$2^{2^a} + 1$	3	5	17	257	65537

und dies sind in der Tat alles Primzahlen. Als man die Zahlen der Form $2^{2^a} + 1$ zuerst untersucht hat (und numerisch nicht weiter als bis $a = 4$ gekommen ist, weil es Taschenrechner ja noch nicht gab), hat man mit „naiver Induktion“ aus der obigen Tabelle vermutet, dass alle Zahlen dieser Form Primzahlen sind. Heute wissen wir es jedoch besser: schon $2^{2^5} + 1 = 4294967297 = 641 \cdot 6700417$ ist zusammengesetzt, und in der Tat hat man bisher noch *gar keine* weitere Primzahl der Form $2^{2^a} + 1$ für $a > 4$ gefunden.

Folgerung 3.33 (Notwendige Bedingung für die Konstruierbarkeit des n-Ecks)**.** *Das regelmäßige n-Eck ist höchstens dann mit Zirkel und Lineal konstruierbar, wenn n von der Form*

$$n = 2^m \cdot p_1 \cdot \cdots \cdot p_r$$

für ein $m \geq 0$ und verschiedene Fermatsche Primzahlen $p_1, \ldots, p_r$ ist.

Beweis. Nach Beispiel 1.23 (C) ist das regelmäßige n-Eck genau dann mit Zirkel und Lineal konstruierbar, wenn $e^{\frac{2\pi i}{n}}$ in einer 2-Radikalerweiterung von $\mathbb{Q}$ liegt. Dies ist nach Folgerung 2.22 (b) aber höchstens dann möglich, wenn der Grad $[e^{\frac{2\pi i}{n}} : \mathbb{Q}]$ eine Zweierpotenz ist. Da dieser Grad nach Satz 3.29 gleich $\varphi(n)$ ist, folgt die Behauptung also aus Lemma 3.31. □

Bemerkung 3.34. Die ersten n-Ecke, die nach dem Kriterium aus Folgerung 3.33 nicht mit Zirkel und Lineal konstruierbar sind, sind $n = 7$, 9, 11, 13 und 14. In allen anderen Fällen mit $n \leq 17$ ist $\varphi(n)$ nach Lemma 3.31 eine Zweierpotenz — was bedeutet, dass wir dann mit unseren bisherigen Ergebnissen noch keine Aussage über die Konstruierbarkeit machen können. Erst in Folgerung 7.8 werden wir mit Hilfe der Galoistheorie sehen, dass die Bedingung in Folgerung 3.33 in der Tat auch

hinreichend ist und alle n-Ecke, für die $\varphi(n)$ eine Zweierpotenz ist, auch wirklich mit Zirkel und Lineal konstruiert werden können.

4. Zerfällungskörper

In den bisherigen Kapiteln der Vorlesung haben wir sehr ausführlich einfache algebraische Körpererweiterungen behandelt. In der Regel hatten wir dazu eine Körpererweiterung L/K mit einem über K algebraischen Element $a \in L$, und haben dann den Körper $K(a)$ mit Hilfe des Minimalpolynoms von a studiert, also mit dem eindeutig bestimmten normierten irreduziblen Polynom $f \in K[t]$ mit Nullstelle a

Wir wollen in diesem Kapitel nun in gewissem Sinne den umgekehrten Weg gehen und uns fragen: haben wir einen Körper K und ein irreduzibles Polynom $f \in K[t]$, finden wir dann immer einen Erweiterungskörper L von K, in dem f eine Nullstelle $a \in L$ besitzt? Oder vielleicht sogar einen Erweiterungskörper, in dem f komplett in Linearfaktoren zerfällt?

Eine solche Frage ist sehr natürlich und tritt z. B. bei der Konstruktion der komplexen Zahlen auf. Versetzt euch doch einmal in die Zeit zurück, als ihr den Körper der komplexen Zahlen noch nicht kanntet. Ihr stellt fest, dass man in $\mathbb{R}$ aus -1 keine Wurzel ziehen kann, dass eine solche Wurzel für viele Anwendungen aber sehr nützlich wäre. Ihr würdet also gerne von $\mathbb{R}$ zu einem größeren Körper übergehen, in dem eine Wurzel aus -1 existiert, d. h. in dem das Polynom t^2+1 eine Nullstelle besitzt. Aber gibt es so etwas überhaupt? Typischerweise fällt die Antwort auf diese Frage in Form des Körpers $\mathbb{C}$ dann in der Schule oder in den „Grundlagen der Mathematik“ irgendwann vom Himmel; man definiert $\mathbb{C}$ dort in der Regel zunächst als $\mathbb{R}^2$ mit einer recht unmotiviert aussehenden Multiplikation und beweist erst einmal, dass man so einen Erweiterungskörper von $\mathbb{R}$ erhält. Und im Nachhinein stellt man dann irgendwann fest, dass dieser Erweiterungskörper auch „zufällig“ das Problem der Wurzel aus -1 löst — aus der Konstruktion von $\mathbb{C}$ war das aber sicher nicht offensichtlich.

Wir wollen dieses Problem nun systematisch angehen und sehen, wie man ganz gezielt zu einem gegebenen Polynom über einem Körper immer einen Erweiterungskörper finden kann, in dem das Polynom eine Nullstelle hat oder sogar in Linearfaktoren zerfällt. Wir betrachten zunächst einmal den einfacheren Fall einer einzelnen Nullstelle und definieren uns einen Begriff für das, was wir suchen.

Definition 4.1 (Stammkörper)**.** Es sei $f \in K[t]$ ein irreduzibles Polynom über einem Körper K. Ein Erweiterungskörper L von K heißt **Stammkörper** von f (über K), wenn es ein $a \in L$ gibt mit $f(a) = 0$ und $L = K(a)$.

Bemerkung 4.2.

(a) Kennen wir bereits einen Erweiterungskörper Z von K, in dem f eine Nullstelle a besitzt, so ist $L = K(a) \leq Z$ offensichtlich ein Stammkörper von f.

(b) Die Bedingung $L = K(a)$ in Definition 4.1 können wir als eine Art Minimalitätsforderung auffassen: wir wollen zu K nur die gewünschte Nullstelle a und nicht noch weitere unnötige Elemente adjungieren. Dies wird in Bemerkung 4.9 dafür sorgen, dass der Stammkörper eines Polynoms (bis auf Isomorphie) eindeutig bestimmt ist.

(c) Ist L ein Stammkörper von $f \in K[t]$ und a wie in Definition 4.1, so ist f nach Lemma 2.6 bis auf einen konstanten Faktor das Minimalpolynom von a. Insbesondere gilt also

$$[L : K] = [K(a) : K] = [a : K] = \deg f$$

nach der Voraussetzung $L = K(a)$ und Satz 2.14 (a). Wir sehen also bereits, dass alle Stammkörper von f denselben Grad über K haben müssen.

Beispiel 4.3.

(a) Betrachten wir das Polynom $f = t^2 + 1 \in \mathbb{R}[t]$ und gehen wir davon aus, dass wir den Körper $\mathbb{C}$ der komplexen Zahlen bereits kennen, so ist $\mathbb{R}(i) = \mathbb{C}$ nach Bemerkung 4.2 (a) ein Stammkörper von f über $\mathbb{R}$. Genauso ist $\mathbb{Q}(\sqrt{2}) \leq \mathbb{R}$ ein Stammkörper von $t^2 - 2$ über $\mathbb{Q}$.

(b) Es sei $K = \mathbb{Z}_2$. Da das Polynom $t^2 + t + 1 \in \mathbb{Z}_2[t]$ offensichtlich keine Nullstelle in $\mathbb{Z}_2$ hat, ist es nach Aufgabe 2.7 (a) irreduzibel. In diesem Fall kennen wir momentan noch keinen Stammkörper von f — schon allein deswegen, weil wir bisher noch überhaupt keinen Erweiterungskörper von $\mathbb{Z}_2$ kennen.

Wir wollen nun sehen, wie man zu einem gegebenen irreduziblen Polynom mit Hilfe von Faktorringen von Polynomringen stets einen Stammkörper konstruieren kann. Ist $f \in K[t]$ ein Polynom, so bezeichne dazu wie üblich $(f) = \{af : a \in K[t]\}$ das von f erzeugte Ideal in $K[t]$ und $K[t]/(f)$ den zugehörigen Faktorring [G, Beispiel 8.8 (a) und Satz 8.10].

Lemma 4.4 (Existenz von Stammkörpern)**.** *Es sei $f \in K[t]$ ein nicht-konstantes Polynom über einem Körper K. Dann gilt:*

(a) *Der Ring $K[t]/(f)$ ist genau dann ein Körper, wenn f irreduzibel ist.*

(b) *Ist f irreduzibel, so ist $L = K[t]/(f)$ ein Stammkörper von f; in ihm ist $\bar{t}$ ein Element mit $f(\bar{t}) = 0$ und $L = K(\bar{t})$.*

Beweis.

(a) „⇒“: Angenommen, f wäre reduzibel, d. h. es wäre $f = g \cdot h$ für nicht-konstante Polynome $g, h \in K[t]$. Im Faktorring $K[t]/(f)$ wäre dann $\overline{g} \cdot \overline{h} = \overline{f} = \overline{0}$, während $\overline{g}$ und $\overline{h}$ ungleich $\overline{0}$ sind, da g und h offensichtlich keine Vielfachen von f sind. Also besitzt $K[t]/(f)$ nicht-triviale Nullteiler und kann damit kein Körper sein [G, Lemma 7.8 (c)].

„⇐“: Es sei nun f irreduzibel. Da $K[t]/(f)$ in jedem Fall bereits ein Ring ist, bleibt nur noch zu zeigen, dass jedes Element $\overline{g} \neq \overline{0}$ in $K[t]/(f)$ ein multiplikatives Inverses besitzt. Beachte dazu, dass f und g in $K[t]$ teilerfremd sind: Da f nach Voraussetzung irreduzibel und damit prim ist [G, Bemerkung 11.6], könnte ohnehin nur f selbst der einzige gemeinsame Primfaktor von f und g sein — aber dann wäre g ein Vielfaches von f und damit $\overline{g} = \overline{0}$ in $K[t]/(f)$. Nach dem Lemma von Bézout [G, Satz 10.13 (b)] gibt es also Polynome p und q mit $pf + qg = 1$ in $K[t]$, d. h. $\overline{q} \cdot \overline{g} = \overline{1}$ in $K[t]/(f)$. Damit besitzt $\overline{g}$ wie gewünscht ein multiplikatives Inverses $\overline{q}$ in $K[t]/(f)$.

(b) Nach (a) ist L ein Körper. Der offensichtliche Morphismus $K \to L$, $a \mapsto \overline{a}$ ist nach Bemerkung 1.3 (b) injektiv und macht L damit zu einem Erweiterungskörper von K. Weiterhin gilt nach Konstruktion natürlich $f(\bar{t}) = \overline{f} = \overline{0} \in L$. Darüber hinaus erzeugen K und t zusammen den Polynomring $K[t]$ und damit auch $L = K[t]/(f)$, d. h. es ist $L = K(\bar{t})$. □

Beispiel 4.5. Wir betrachten noch einmal den Körper $K = \mathbb{Z}_2$ mit dem irreduziblen Polynom $f = t^2 + t + 1 \in \mathbb{Z}_2[t]$ aus Beispiel 4.3 (b). Nach Lemma 4.4 (b) ist dann $L := \mathbb{Z}_2[a]/(a^2 + a + 1)$ ein Stammkörper von f, in dem $\overline{a}$ eine Nullstelle von f ist. Beachte, dass wir hier im Polynomring eine andere formale Variable a als sonst üblich gewählt haben, damit gleich keine Verwirrung auftritt, wenn wir auch Polynome über L betrachten, die wir dann wieder mit der formalen Variablen t schreiben wollen: im Polynomring $L[t]$ über dem Koeffizientenkörper $L = \mathbb{Z}_2[a]/(a^2 + a + 1)$ ist $\overline{a}$ nun eine Konstante und kein lineares Polynom!

Wenn $\overline{a}$ eine Nullstelle von f über L ist, muss man diese natürlich abspalten und f damit über L als Produkt von zwei linearen Faktoren schreiben können. In der Tat zeigt eine einfache Rechnung in

$L[t]$, dass

$$\begin{aligned}(t-\overline{a})\,(t-\overline{a}-\overline{1}) &= t^2-(\overline{2}\cdot\overline{a}+\overline{1})t+\overline{a^2+a}\\ &= t^2-(\overline{2}\cdot\overline{a}+\overline{1})t-\overline{1} && (\overline{a^2+a+1}=\overline{0}\text{ in }L)\\ &= t^2+t+\overline{1} && (\operatorname{char}L=\operatorname{char}K=2\text{ nach Beispiel 1.7 (b)})\\ &= f.\end{aligned}$$

Damit zerfällt f also in der Tat über L in Linearfaktoren; die Nullstellen von f in L sind $\overline{a}$ und $\overline{a}+\overline{1}$.

Bemerkung 4.6. Bei Rechnungen in Stammkörpern der Form $L=K[t]/(f)$ wie in Lemma 4.4 lässt man in der Notation oft die Querstriche zur Bezeichnung der Restklassen im Faktorring weg, wenn dies nicht zu Verwirrungen führen kann. In Beispiel 4.5 wären mit dieser Konvention also alle Querstriche überflüssig, und a (statt $\overline{a}$) wäre dort dann ein Element in dem Erweiterungskörper L mit $a^2+a+1=0$ (statt $\overline{a^2+a+1}=\overline{0}$). Dies macht die Formeln einfacher lesbar und kann auch durch die Tatsache motiviert werden, dass wir ja K als Unterkörper von L identifizieren wollen und es dann merkwürdig wäre, Elemente von K ohne und solche von L mit Querstrich zu schreiben.

Aufgabe 4.7. In dieser Aufgabe wollen wir eine Verallgemeinerung der Aussage aus Lemma 4.4 (a) herleiten, die allgemein die Frage beantwortet, wann ein Faktorring R/I sogar ein Körper ist.

Dazu heiße ein Ideal $I\neq R$ in einem Ring R ein **maximales Ideal**, wenn für jedes Ideal $J\supsetneq I$ bereits folgt, dass $J=R$. Man zeige:

(a) Der Ring R/I ist genau dann ein Körper, wenn I ein maximales Ideal ist.

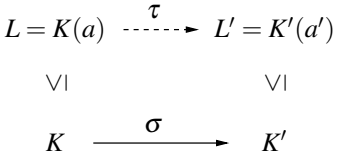
(b) Ist R ein Hauptidealring, so ist ein Ideal $I=(a)$ für eine Nichteinheit $a\neq 0$ genau dann ein maximales Ideal, wenn a irreduzibel ist.

Im Fall des Polynomrings $R=K[t]$ über einem Körper K ergibt sich aus (a) und (b) offensichtlich genau Lemma 4.4 (a). Welche euch bereits bekannte Aussage ergibt sich im Fall $R=\mathbb{Z}$?

Nach der Existenz von Stammkörpern wollen wir nun auch deren Eindeutigkeit (bis auf Isomorphie) zeigen. Wir beweisen dazu eine etwas allgemeinere Aussage, die wir später noch mehrfach benötigen werden.

Lemma 4.8 (Eindeutigkeit von Stammkörpern)**.** *Es seien $\sigma: K\to K'$ ein Körperisomorphismus, $f\in K[t]$ ein irreduzibles Polynom über K und $f'=\sigma(f)\in K'[t]$ das zugehörige Polynom über K'. Ferner seien $L=K(a)$ ein Stammkörper von f über K mit $f(a)=0$ und $L'=K'(a')$ ein Stammkörper von f' über K' mit $f'(a')=0$.*

Dann gibt es genau einen Körperisomorphismus $\tau: L\to L'$ mit $\tau|_K=\sigma$ und $\tau(a)=a'$.



Beweis. Die Eindeutigkeit von τ sieht man schnell ein: jedes Element von $L=K(a)$ lässt sich nach Lemma 2.10 als Polynom $\sum_n \lambda_n a^n$ mit Koeffizienten in K schreiben. Da τ ein Körperhomomorphismus ist und auf K sowie a durch $\tau|_K=\sigma$ und $\tau(a)=a'$ festgelegt ist, muss ein solches Element von τ zwangsläufig auf

$$\tau\Big(\sum_n \lambda_n a^n\Big)=\sum_n \tau(\lambda_n)\,\tau(a)^n=\sum_n \sigma(\lambda_n)\,(a')^n$$

abgebildet werden. Damit ist τ also eindeutig festgelegt, d. h. es kann höchstens einen Körperhomomorphismus mit den geforderten Eigenschaften geben.

Für die Existenz von τ betrachten wir den Ringhomomorphismus $F: K[t]\to L$, $g\mapsto g(a)$. Wiederum nach Lemma 2.10 ist F surjektiv; der Kern hingegen ist

$$\operatorname{Ker}F=\{g\in K[t]: g(a)=0\}=(f)$$

nach Bemerkung 2.5, da f wegen Bemerkung 4.2 (c) bis auf einen konstanten Faktor das Minimalpolynom von a ist. Nach dem Homomorphiesatz [G, Satz 8.12] ist die Abbildung

$$G : K[t]/(f) \to L, \quad \overline{g} \mapsto g(a)$$

also ein Körperisomorphismus; offensichtlich bildet er $\overline{t}$ auf a und Elemente von $K \leq K[t]/(f)$ auf sich selbst ab. Genauso gibt es auf der anderen Seite einen Körperisomorphismus $G' : K'[t]/(f') \to L'$ mit $G'(\overline{t}) = a'$ und $G'|_{K'} = \mathrm{id}$. Die Verkettung τ der drei Isomorphismen

$$K(a) \xrightarrow{G^{-1}} K[t]/(f) \longrightarrow K'[t]/(f') \xrightarrow{G'} K'(a')$$

hat dann die gewünschten Eigenschaften, wobei der mittlere Isomorphismus einfach die Abbildung $\overline{g} \mapsto \overline{\sigma(g)}$ ist, die ein Polynom über K mit σ in ein Polynom über K' umwandelt. □

Bemerkung 4.9. Der wichtigste Fall von Lemma 4.8 ist der, in dem σ die Identität, also $K = K'$ und $f = f'$ ist. Das Lemma besagt dann, dass es zu zwei beliebigen Stammkörpern $L = K(a)$ und $L' = K(a')$ eines irreduziblen Polynoms $f \in K[t]$ immer einen Isomorphismus $\tau : K(a) \to K(a')$ gibt mit $\tau|_K = \mathrm{id}$ und $\tau(a) = a'$. Der Stammkörper eines Polynoms ist also bis auf Isomorphie eindeutig bestimmt; wir können damit in Zukunft von *dem* Stammkörper anstatt von *einem* Stammkörper von f sprechen. In der Tat haben wir sogar etwas mehr gesehen, nämlich dass es einen Isomorphismus zwischen den Stammkörpern gibt, *der auf dem Ursprungskörper K die Identität ist*. Man sagt dafür auch, dass die Stammkörper **K-isomorph** bzw. **isomorph über** K sind.

Beispiel 4.10.

(a) Wir betrachten in Lemma 4.8 (bzw. Bemerkung 4.9) den Fall $K = K' = \mathbb{R}$ mit $\sigma = \mathrm{id}$ und $f = f' = t^2 + 1$. Nach Beispiel 4.3 (a) ist $L = L' = \mathbb{C}$ dann ein Stammkörper von f. Allerdings hat f die zwei Nullstellen i und $-i$, und damit können wir im Lemma $a = i$ und $a' = -i$ wählen. Wir erhalten so die Aussage, dass es genau einen Körperisomorphismus $\tau : \mathbb{C} \to \mathbb{C}$ mit $\tau|_{\mathbb{R}} = \mathrm{id}$ und $\tau(i) = -i$ gibt. Diesen Körperisomorphismus kennt ihr natürlich bereits: es ist einfach die komplexe Konjugation $\tau(z) = \overline{z}$.

(b) Es sei $f = t^3 - 2 \in \mathbb{Q}[t]$. Drei Stammkörper von f sind dann z. B.

(i) $\mathbb{Q}(\sqrt[3]{2})$ (als Teilkörper von $\mathbb{R}$) nach Bemerkung 4.2 (a);

(ii) $\mathbb{Q}\left(\sqrt[3]{2}e^{\frac{2\pi i}{3}}\right)$ (als Teilkörper von $\mathbb{C}$) mit demselben Argument;

(iii) $\mathbb{Q}[t]/(t^3 - 2)$ nach Lemma 4.4 (b).

Diese drei Körper sehen zunächst alle verschieden aus: (i) und (ii) sind verschiedene Teilkörper von $\mathbb{C}$ (da (i) nur reelle Zahlen enthält, (ii) jedoch nicht), und der Körper (iii) ist ohnehin auf eine ganz andere Art definiert. Dennoch sagt Bemerkung 4.9, dass diese drei Körper als Stammkörper von f isomorph über $\mathbb{Q}$ sind.

Die algebraische Art, sich diese Aussage vorzustellen, ist einfach, dass es sich in allen drei Fällen um den Körper handelt, der aus $\mathbb{Q}$ entsteht, indem man ein Element adjungiert, dessen dritte Potenz gleich 2 ist. Wo dieses Element herkommt, spielt dabei keine Rolle — es kann ein konkretes Element in einem schon bekannten Erweiterungskörper von $\mathbb{Q}$ sein (wie $\sqrt[3]{2} \in \mathbb{R}$ oder $\sqrt[3]{2}e^{\frac{2\pi i}{3}} \in \mathbb{C}$ in (i) bzw. (ii)), oder einfach ein formales Element t wie in (iii), von dem man durch Übergang zu einem geeigneten Faktorring einfach verlangt, dass $t^3 - 2 = 0$ gilt.

Bemerkung 4.11 (Konstruktion von $\mathbb{C}$ aus $\mathbb{R}$)**.** Mit unserem Wissen über Stammkörper wollen wir noch einmal das Problem aus der Einleitung dieses Kapitels betrachten, wie man aus dem Körper $\mathbb{R}$ der reellen Zahlen den Körper $\mathbb{C}$ der komplexen Zahlen konstruieren kann, ohne dass die Definition von $\mathbb{C}$ dabei vom Himmel fällt und man erst im Nachhinein überprüfen muss, dass sie wirklich das Gewünschte leistet, nämlich eine Wurzel aus -1 einführt.

Wenn man in ingenieurswissenschaftliche Bücher schaut, werden die komplexen Zahlen dort oft so eingeführt: man nehme einfach an, dass es ein Element i mit $i^2 = -1$ gibt, und rechne damit dann ganz normal weiter, als wäre nichts Besonderes passiert. Als angehende Mathematiker würdet ihr dazu nun vermutlich sagen, dass das so nicht geht: wenn man bisher nur die reellen Zahlen kennt,

ist $i^2 = -1$ einfach nur eine widersprüchliche und damit unerlaubte Annahme und keinesfalls eine Definition. Das stimmt natürlich eigentlich auch, und daher definiert man die komplexen Zahlen in den „Grundlagen der Mathematik“ ja auch nicht so.

Der Algebraiker hingegen sieht die Sache etwas anders und kann die Sichtweise der Ingenieure zu einer mathematisch korrekten Definition $\mathbb{C} := \mathbb{R}[i]/(i^2+1)$ machen — denn dies ist haargenau die Übersetzung ins Algebraische der Idee „man nehme zu $\mathbb{R}$ ein formales Element i hinzu, für das $i^2 = -1$ gelte, und rechne damit ganz normal (mit den Körperaxiomen) weiter“. Und in der Tat wissen wir ja jetzt auch, dass wir auf diese Art exakt die üblichen komplexen Zahlen erhalten: denn $\mathbb{R}[i]/(i^2+1)$ ist nach Lemma 4.4 (b) ein Stammkörper des Polynoms t^2+1, der zum Stammkörper $\mathbb{C}$ (siehe Beispiel 4.3 (a)) nach Bemerkung 4.9 isomorph ist.

06

Wir wollen die Idee von Stammkörpern nun dahingehend ausweiten, dass wir Erweiterungskörper suchen, in denen ein gegebenes Polynom nicht nur eine Nullstelle hat, sondern sogar komplett in Linearfaktoren zerfällt. Die Definition, die in diesem Sinne Definition 4.1 entspricht, ist die folgende.

Definition 4.12 (Zerfällungskörper)**.** Es sei $f \in K[t]$ mit $f \neq 0$ ein Polynom über einem Körper K. Ein Erweiterungskörper L von K heißt **Zerfällungskörper** von f (über K), wenn es $\lambda \in K$ und $a_1, \dots, a_n \in L$ gibt mit

$$f = \lambda\,(t-a_1)\cdot\dots\cdot(t-a_n) \in L[t] \quad \text{und} \quad L = K(a_1,\dots,a_n).$$

Bemerkung 4.13. Die folgenden beiden Eigenschaften sind völlig analog zu denen von Stammkörpern in Bemerkung 4.2:

(a) Kennen wir bereits einen Erweiterungskörper Z von K, in dem f in Linearfaktoren zerfällt, also $f = \lambda\,(t-a_1)\cdot\dots\cdot(t-a_n)$ mit $\lambda \in K$ und $a_1,\dots,a_n \in Z$ gilt, so ist $L = K(a_1,\dots,a_n) \leq Z$ offensichtlich ein Zerfällungskörper von f über K. Dies ist z. B. in der Regel der Fall, wenn $K = \mathbb{Q}$ ist und wir eine Zerlegung in Linearfaktoren über $Z = \mathbb{C}$ hinschreiben können.

(b) Die Bedingung $L = K(a_1,\dots,a_n)$ in Definition 4.12 ist eine Art Minimalitätsforderung, die besagt, dass wir zu K nicht noch mehr Elemente adjungieren wollen, als wir für die Zerlegung in Linearfaktoren unbedingt benötigen. Wie schon bei den Stammkörpern wird dies in Satz 4.16 zur Eindeutigkeit von Zerfällungskörpern führen.

Beispiel 4.14.

(a) Das Polynom $f = t^3 - 2 \in \mathbb{Q}[t]$ hat offensichtlich die komplexen Nullstellen $\sqrt[3]{2} \cdot e^{\frac{2\pi i k}{3}}$ für $k = 0,1,2$. Nach Bemerkung 4.13 (a) ist also

$$\mathbb{Q}\big(\sqrt[3]{2}, \sqrt[3]{2}\,e^{\frac{2\pi i}{3}}, \sqrt[3]{2}\,e^{\frac{4\pi i}{3}}\big) = \mathbb{Q}\big(\sqrt[3]{2}, e^{\frac{2\pi i}{3}}\big) \leq \mathbb{C}$$

ein Zerfällungskörper von f über $\mathbb{Q}$.

(b) Es sei $f \in K[t]$ ein irreduzibles Polynom vom Grad 2 und L sein Stammkörper. Da f in L eine Nullstelle hat und diese dann natürlich als Linearfaktor abspaltet, zerfällt f damit in L auch bereits in Linearfaktoren. Für irreduzible quadratische Polynome fallen die Begriffe Stammkörper und Zerfällungskörper also zusammen. So ist z. B. für das in Beispiel 4.5 betrachteten Polynom $f = t^2+t+1 \in \mathbb{Z}_2[t]$ sein Stammkörper $L = \mathbb{Z}_2[a]/(a^2+a+1)$ auch bereits ein Zerfällungskörper.

Für Polynome höheren Grades ist dies natürlich nicht so — hier kann man im Stammkörper zwar eine oder evtl. auch mehrere Nullstellen abspalten, aber es bleibt in der Regel noch ein Restpolynom übrig, auf das man die Stammkörperkonstruktion rekursiv erneut anwenden muss, bis schließlich das gesamte Polynom in Linearfaktoren zerfällt. Auf diese Art kann man dann wie im folgenden Satz zu jedem Polynom einen Zerfällungskörper konstruieren.

Satz 4.15 (Existenz von Zerfällungskörpern)**.** *Es seien K ein Körper und $f \in K[t]$ ein Polynom mit $f \neq 0$ und $n = \deg f$. Dann besitzt f einen Zerfällungskörper vom Grad höchstens $n!$.*

Beweis. Wir zeigen die Aussage mit Induktion über n; für $n = 0$ ist K selbst offensichtlich ein Zerfällungskörper von f.

Für den Induktionsschritt sei nun f ein Polynom vom Grad n. Wir wählen einen irreduziblen Faktor g von f; in seinem Stammkörper $L = K(a)$ ist a dann eine Nullstelle von g und damit auch von f. Beachte, dass $[L : K] = \deg g \leq \deg f = n$ nach Bemerkung 4.2 (c).

In L spaltet f also die Nullstelle a ab, d. h. wir können $f = (t-a)\,h$ für ein $h \in L[t]$ mit $\deg h = n-1$ schreiben. Nach Induktionsvoraussetzung besitzt h nun einen Zerfällungskörper Z über L, d. h. es ist $h = \lambda\,(t-a_2)\cdot\,\cdots\,(t-a_n)$ für gewisse $\lambda \in K$ und $a_2,\ldots,a_n \in Z$ mit $Z = L(a_2,\ldots,a_n)$ und $[Z : L] \leq (n-1)!$. Damit ist aber $f = \lambda\,(t-a)\,(t-a_2)\cdot\,\cdots\,(t-a_n) \in Z[t]$, d. h. $Z = L(a_2,\ldots,a_n) = K(a,a_2,\ldots,a_n)$ ist ein Zerfällungskörper von f über K. Nach der Gradformel aus Satz 2.17 gilt ferner wie behauptet $[Z : K] = [Z : L]\cdot[L : K] \leq (n-1)!\cdot n = n!$. □

Genau wie bei Stammkörpern wollen wir nun auch für Zerfällungskörper noch ihre Eindeutigkeit zeigen. Ganz analog zum Beweis ihrer Existenz in Satz 4.15 zeigt man auch diese Eindeutigkeit rekursiv aus der entsprechenden Aussage über Stammkörper in Lemma 4.8.

Satz 4.16 (Eindeutigkeit von Zerfällungskörpern)**.** *Es seien $\sigma : K \to K'$ ein Körperisomorphismus, $f \in K[t]$ ein Polynom mit $f \neq 0$ und $f' = \sigma(f) \in K'[t]$ das zugehörige Polynom über K'. Ferner seien L und L' Zerfällungskörper von f bzw. f' über K bzw. K'.*

Dann gibt es einen Isomorphismus $\tau : L \to L'$ mit $\tau|_K = \sigma$.

$$\begin{array}{ccc} L & \overset{\tau}{\dashrightarrow} & L' \\ \vee| & & \vee| \\ K & \xrightarrow{\sigma} & K' \end{array}$$

Beweis. Wir zeigen die Aussage wieder mit Induktion über $n = \deg f = \deg f'$. Für $n = 0$ haben f und f' keine Nullstellen, also muss $L = K$ und $L' = K'$ gelten und wir können $\tau = \sigma$ wählen.

Für den Induktionsschritt sei nun n beliebig. Wir wählen einen irreduziblen Faktor g von f. Nach Voraussetzung zerfällt f und damit auch g über L in Linearfaktoren; insbesondere gibt es also ein $a \in L$ mit $f(a) = g(a) = 0$. Genauso ist $g' = \sigma(g)$ ein irreduzibler Faktor von f', und es gibt ein $a' \in L'$ mit $f'(a') = g'(a') = 0$.

Nach Bemerkung 4.2 (a) sind nun $K(a) \leq L$ und $K'(a') \leq L'$ Stammkörper von g bzw. g'. Aufgrund von Lemma 4.8 finden wir also einen Isomorphismus $\varphi : K(a) \to K'(a')$ mit $\varphi|_K = \sigma$ und $\varphi(a) = a'$, d. h. wir können das untere Rechteck im Diagramm unten rechts vervollständigen.

Da a eine Nullstelle von f in $K(a)$ ist, können wir nun $f = (t-a)\,h \in K(a)[t]$ für ein Polynom h vom Grad $n-1$ schreiben. Dann ist L als Zerfällungskörper von f über K offensichtlich auch ein Zerfällungskörper von h über $K(a)$, denn beide entstehen aus K durch Adjunktion von a sowie der Nullstellen von h. Genauso ist L' ein Zerfällungskörper über $K'(a')$ vom entsprechenden Polynom $h' = \varphi(h)$ mit $f' = (t-a')\,h' \in K'(a')[t]$. Nach Induktionsvoraussetzung, angewendet auf den Isomorphismus φ und das Polynom h, können wir also auch das obere Rechteck im Diagramm rechts vervollständigen, d. h. wir finden wie gewünscht einen Isomorphismus $\tau : L \to L'$ mit $\tau|_{K(a)} = \varphi$, insbesondere also mit $\tau|_K = \sigma$.

$$\begin{array}{ccc} L & \overset{\tau}{\dashrightarrow} & L' \\ \vee| & & \vee| \\ K(a) & \overset{\varphi}{\dashrightarrow} & K'(a') \\ \vee| & & \vee| \\ K & \xrightarrow{\sigma} & K' \end{array}$$

□

Bemerkung 4.17.

(a) Wenden wir Satz 4.16 auf den Fall $K = K'$, $\sigma = \mathrm{id}$ und damit $f = f'$ an, so sehen wir wie in Bemerkung 4.9 im Fall von Stammkörpern, dass es zu zwei Zerfällungskörpern L und L' eines Polynoms $f \in K[t]$ mit $f \neq 0$ stets einen K-Isomorphismus $\tau : L \to L'$ gibt. Der Zerfällungskörper eines Polynoms ist also bis auf K-Isomorphie eindeutig bestimmt. Wir können in diesem Sinne damit in Zukunft von *dem* Zerfällungskörper statt von *einem* Zerfällungskörper von f reden.

(b) Im Gegensatz zur analogen Aussage über Stammkörper in Lemma 4.8 ist der K-Isomorphismus $\tau : L \to L'$ in Satz 4.16 nicht eindeutig. Dies liegt daran, dass wir im Beweis des

Satzes für das Element $a \in L$ eine Nullstelle $a' \in L'$ von g' als das Bild von a unter τ wählen konnten — wofür es in der Regel natürlich mehrere Möglichkeiten gibt. In der Tat ist die Nichteindeutigkeit dieses Isomorphismus einer der Schlüsselpunkte der Galoistheorie, die wir in Kapitel 5 untersuchen werden (siehe z. B. Definition 5.1 (b)).

Aufgabe 4.18. Berechne für die folgenden Polynome $f \in K[t]$ ihren Zerfällungskörper L sowie den Grad $[L : K]$:

(a) $t^p - q \in \mathbb{Q}[t]$ für zwei Primzahlen p und q;

(b) $t^{15} + 6 \in \mathbb{Q}[t]$;

(c) $t^4 + 2 \in \mathbb{Z}_3[t]$.

Aufgabe 4.19. Es sei L der Zerfällungskörper eines Polynoms $f \in K[t]$ mit $f \neq 0$ über einem Körper K. Ferner seien $g \in K[t]$ ein irreduzibles Polynom und Z der Zerfällungskörper von $f \cdot g$. Da dann offensichtlich auch f und g in Z in Linearfaktoren zerfallen, können wir insbesondere L als Teilkörper von Z auffassen.

Man zeige:

(a) Sind $a, b \in Z$ zwei Nullstellen von g, so sind die Teilkörper $L(a)$ und $L(b)$ von Z isomorph über K.

(b) Hat g eine Nullstelle in L, so zerfällt g in L bereits in Linearfaktoren.

Zum Abschluss dieses Kapitels wollen wir noch zwei Anwendungen von Zerfällungskörpern behandeln. Die erste besteht darin, dass wir nun endliche Körper, also Körper mit nur endlich vielen Elementen, besser untersuchen können. Bisher kannten wir als „systematische Beispiele“ für solche endlichen Körper nur die Körper $\mathbb{Z}_p$ für eine Primzahl p. Wir hatten allerdings in Beispiel 4.5 mit dem Stammkörper $K = \mathbb{Z}_2[a]/(a^2 + a + 1)$ von $t^2 + t + 1 \in \mathbb{Z}_2[t]$ auch schon ein Beispiel für einen endlichen Körper gesehen, der nicht von dieser Form ist: nach Bemerkung 4.2 (c) ist $[K : \mathbb{Z}_2] = 2$, d. h. K ist ein 2-dimensionaler $\mathbb{Z}_2$-Vektorraum. Als $\mathbb{Z}_2$-Vektorraum ist K also isomorph zu $\mathbb{Z}_2^2$ und hat demzufolge 4 Elemente. Damit ist K ein endlicher Körper, der sicher nicht von der Form $\mathbb{Z}_p$ für eine Primzahl p sein kann.

Mit unseren Ergebnissen über Zerfällungskörper können wir nun in der Tat bis auf Isomorphie *alle* endlichen Körper konkret angeben. Wir benötigen dazu zuerst ein kleines Lemma, das die mögliche Anzahl $|K|$ von Elementen eines endlichen Körpers K wesentlich einschränkt.

Lemma 4.20. *Es sei K ein endlicher Körper. Dann ist $|K| = p^r$ für eine Primzahl p und ein $r \in \mathbb{N}_{>0}$, und die Charakteristik von K ist p.*

Beweis. Es sei $P(K) \leq K$ der Primkörper von K aus Definition 1.4. Nach Aufgabe 1.11 ist dieser Primkörper durch die Charakteristik von K eindeutig bestimmt:

- Ist $\operatorname{char} K = 0$, so ist $P(K) = \mathbb{Q}$. Also ist K dann ein Erweiterungskörper von $\mathbb{Q}$ und kann damit insbesondere nicht endlich sein. Dieser Fall tritt also für endliche Körper nicht auf.
- Ist $\operatorname{char} K = p$ eine Primzahl, so ist $P(K) = \mathbb{Z}_p$, d. h. K ist ein Erweiterungskörper von $\mathbb{Z}_p$ und damit auch ein $\mathbb{Z}_p$-Vektorraum der Dimension $r := [K : \mathbb{Z}_p]$. Natürlich muss diese Dimension endlich sein, da K sonst kein endlicher Körper wäre. Damit ist K als $\mathbb{Z}_p$-Vektorraum (nicht jedoch als Ring!) isomorph zu $\mathbb{Z}_p^r$, und es folgt $|K| = p^r$. □

Das bemerkenswerte Resultat ist nun, dass es zu jeder Primzahlpotenz wie in Lemma 4.20 *genau einen* Körper mit dieser Anzahl von Elementen gibt. Wir definieren diese Körper zunächst, und zeigen danach, dass dies wirklich die Körper sind, die wir suchen.

Definition 4.21 (Endliche Körper)**.** Es sei $q = p^r$ für eine Primzahl p und ein $r \in \mathbb{N}_{>0}$. Wir definieren $\mathbb{F}_q$ als den Zerfällungskörper des Polynoms $t^q - t$ über $\mathbb{Z}_p$ (der Buchstabe F steht für „field“, das englische Wort für Körper).

Beispiel 4.22.

(a) Ist p eine Primzahl, so ist $\mathbb{F}_p$ nach Definition der Zerfällungskörper von $f = t^p - t$ über $\mathbb{Z}_p$. Nun gilt nach Lemma 3.23 (b) aber $a^p = a$ für alle $a \in \mathbb{Z}_p$, d. h. jedes Element $a \in \mathbb{Z}_p$ ist Nullstelle von f. Da f Grad p hat, zerfällt f damit schon über $\mathbb{Z}_p$ in Linearfaktoren — es ist nämlich $f = \prod_{a\in\mathbb{Z}_p}(t-a)$. Also ist $\mathbb{Z}_p$ bereits der Zerfällungskörper von f, d. h. es ist $\mathbb{F}_p \cong \mathbb{Z}_p$.

(b) Der Körper $\mathbb{F}_4$ ist nach Definition der Zerfällungskörper von

$$f = t^4 - t = t\,(t^3-1) = t\,(t-1)\,(t^2+t+1)$$

über $\mathbb{Z}_2$, und damit auch der Zerfällungskörper von t^2+t+1 über $\mathbb{Z}_2$. Mit Beispiel 4.14 (b) ist also $\mathbb{F}_4 = \mathbb{Z}_2[a]/(a^2+a+1)$. Beachte, dass (wie vor Lemma 4.20 schon bemerkt) $[\mathbb{F}_4 : \mathbb{Z}_2] = 2$ und damit $|\mathbb{F}_4| = |\mathbb{Z}_2^2| = 4$ gilt, d. h. $\mathbb{F}_4$ ist ein Körper mit 4 Elementen.

Aufgabe 4.23. Berechne eine Multiplikationstafel für den Körper $\mathbb{F}_4$.

Wir wollen nun sehen, dass $\mathbb{F}_q$ in der Tat für jede Primzahlpotenz q ein Körper mit q Elementen ist. Beachte, dass dies ganz und gar nicht offensichtlich ist, da wir für den Grad des Zerfällungskörpers im Allgemeinen ja nur die Abschätzung aus Satz 4.15 haben.

Lemma 4.24. *Für jede Primzahlpotenz q gilt $|\mathbb{F}_q| = q$.*

Beweis. Ist $q = p^r$, so ist $\mathbb{F}_q$ zunächst einmal nach Definition der Zerfällungskörper von $f = t^q - t$ über $\mathbb{Z}_p$, d. h. wir haben eine Zerlegung

$$t^q - t = \prod_{i=1}^{q}(t-a_i),$$

wobei $N := \{a_1,\dots,a_q\} \subset \mathbb{F}_q$ genau die Menge der Nullstellen von f in $\mathbb{F}_q$ ist. Wir wollen zunächst zeigen, dass diese Nullstellen auch wirklich alle verschieden sind. Nach Lemma 3.24 (b) genügt es dazu zu sehen, dass f teilerfremd zu seiner formalen Ableitung f' ist. Da diese formale Ableitung in unserem konkreten Fall gleich $f' = qt^{q-1} - 1 = -1$ ist (beachte, dass $q = 0$ in $\mathbb{Z}_p$ gilt), ist dies aber offensichtlich. Also sind die Nullstellen von f alle verschieden, d. h. es ist $|N| = q$.

Wir müssen also nur noch sehen, dass $N = \mathbb{F}_q$ gilt. Dazu zeigen wir mit dem Kriterium aus Bemerkung 1.3 (a) zunächst, dass N ein Körper ist:

- $0, 1 \in N$, denn diese beiden Elemente sind offensichtlich Nullstellen von f.
- Es seien $a_i, a_j \in N$, also $a_i^q = a_i$ und $a_j^q = a_j$. Beachte, dass wegen $\operatorname{char}\mathbb{F}_q = p$ mit demselben Argument wie im Beweis von Lemma 3.23 (a) gilt, dass

  $$(x+y)^p = \sum_{i=0}^{p}\binom{p}{i}x^i y^{p-i} = x^p + y^p$$

  für alle $x, y \in \mathbb{F}_q$, denn $p \mid \binom{p}{i}$ und damit $\binom{p}{i} = 0 \in \mathbb{F}_q$ für $0 < i < p$. Damit erhalten wir

  $$\begin{aligned}
  (a_i+a_j)^q &= (((a_i+a_j)^p)^p\cdots)^p = a_i^q + a_j^q = a_i + a_j && \text{und damit } a_i+a_j \in N;\\
  (-a_i)^q &= -a_i^q = -a_i && \text{und damit } -a_i \in N;\\
  (a_i a_j)^q &= a_i^q a_j^q = a_i a_j && \text{und damit } a_i a_j \in N;\\
  (a_i^{-1})^q &= (a_i^q)^{-1} = a_i^{-1} && \text{und damit } a_i^{-1} \in N \text{ für } a_i \neq 0.
  \end{aligned}$$

Also ist N ein Körper. Natürlich muss er damit den Primkörper $\mathbb{Z}_p$ enthalten und ist daher der kleinste Körper, der $\mathbb{Z}_p$ und $a_1,\dots,a_q$ enthält, d. h. gleich $\mathbb{Z}_p(a_1,\dots,a_q) = \mathbb{F}_q$. Damit ist $|\mathbb{F}_q| = |N| = q$. □

Mit diesen Ergebnissen erhalten wir nun die angekündigte vollständige Klassifikation der endlichen Körper.

Folgerung 4.25 (Klassifikation endlicher Körper)**.** *Die endlichen Körper sind bis auf Isomorphie genau die Körper $\mathbb{F}_q$ für eine Primzahlpotenz q.*

Beweis. Die Körper $\mathbb{F}_q$ sind nach Lemma 4.24 natürlich endliche Körper, die paarweise verschieden sind, da sie unterschiedlich viele Elemente haben.

Ist umgekehrt K ein beliebiger endlicher Körper, so gilt zunächst $|K| = q = p^r$ für eine Primzahl p und ein $r \in \mathbb{N}_{>0}$ nach Lemma 4.20, und der Primkörper von K ist $\mathbb{Z}_p$ nach Aufgabe 1.11 (b). Ferner hat die Einheitengruppe $K^* = K \backslash \{0\}$ von K dann $q-1$ Elemente. Nach dem kleinen Satz von Fermat [G, Folgerung 5.15 (b)] gilt also $a^{q-1} = 1$ für alle $a \in K^*$ und damit $a^q = a$ für alle $a \in K$.

Insgesamt ist K also ein Erweiterungskörper von $\mathbb{Z}_p$, in dem das Polynom $t^q - t$ in Linearfaktoren zerfällt, da es ja alle q Elemente $a_1, \dots, a_q$ von K als Nullstellen hat. Weil in K natürlich auch $\mathbb{Z}_p(a_1, \dots, a_q) = K$ gilt, ist K damit der (nach Bemerkung 4.17 (a) eindeutig bestimmte) Zerfällungskörper $\mathbb{F}_q$ von $t^q - t$ über $\mathbb{Z}_p$. □

Aufgabe 4.26. Es seien p eine Primzahl und $m, n \in \mathbb{N}_{>0}$. Zeige, dass $\mathbb{F}_{p^m}$ genau dann (bis auf Isomorphie) in $\mathbb{F}_{p^n}$ enthalten ist, wenn $m \mid n$ gilt.

Aufgabe 4.27. Es sei $f \in \mathbb{Z}_p[t]$ ein irreduzibles Polynom vom Grad n. Man zeige:

(a) In $\mathbb{F}_{p^n}$ zerfällt f in Linearfaktoren.

(b) $f \mid t^{p^n} - t$ in $\mathbb{Z}_p[t]$.

Für die zweite Anwendung von Zerfällungskörpern erinnern wir uns noch einmal an Aufgabe 1.17, in der wir gezeigt haben, dass man die Körpererweiterung $\mathbb{Q}(\sqrt{2}, \sqrt{3})$, bei der man eigentlich zwei Elemente zu $\mathbb{Q}$ adjungiert hat, auch als einfache Körpererweiterung $\mathbb{Q}(\sqrt{2}+\sqrt{3})$ schreiben kann. Da einfache Körpererweiterungen oft schöner zu behandeln sind als allgemeine (siehe z. B. Satz 2.14), wollen wir uns fragen, ob man vielleicht *jede* Körpererweiterung als einfache Körpererweiterung schreiben kann. In der Tat stellt sich heraus, dass dies zumindest für endliche Erweiterungen in Charakteristik 0 immer möglich ist.

Satz 4.28 (Satz vom primitiven Element). *Es sei L/K eine endliche Körpererweiterung mit $\operatorname{char} K = 0$. Dann ist L/K einfach, d. h. es gibt ein $c \in L$ mit $L = K(c)$. (Ein solches c wird dann oft auch primitives Element genannt.)*

07

Bevor wir diesen Satz beweisen, benötigen wir noch eine Vorbemerkung.

Bemerkung 4.29 (ggt von Polynomen über verschiedenen Körpern)**.** Es seien $f, g \in K[t]$ zwei Polynome über einem Körper K, die nicht beide gleich 0 sind. Ferner sei $L \geq K$ ein Erweiterungskörper von K, so dass wir f und g also auch als Polynome über L auffassen können.

In dieser Situation können wir den (nach [G, Notation 10.30 (b)] eindeutig bestimmten) normierten größten gemeinsamen Teiler $\operatorname{ggt}(f, g)$ dieser beiden Polynome natürlich sowohl über K als auch über L ausrechnen. Da sich $\operatorname{ggt}(f, g)$ aber mit Hilfe des euklidischen Algorithmus durch fortgesetzte Polynomdivision berechnen lässt [G, Satz 10.26] und die Division zweier Polynome in $K[t]$ mit Rest nach Konstruktion offensichtlich nicht davon abhängt, ob man sie als Elemente von $K[t]$ oder $L[t]$ auffasst [G, Satz 10.19], sehen wir, dass der größte gemeinsame Teiler $\operatorname{ggt}(f, g)$ in der Tat davon unabhängig ist, ob man ihn über K oder L berechnet hat.

Beachte, dass dieses Ergebnis nicht mehr ganz so offensichtlich ist, wenn man sich $\operatorname{ggt}(f, g)$ als Produkt der sowohl in f als auch in g auftretenden Primfaktoren (mit den entsprechenden Potenzen) vorstellt, da die Primfaktorzerlegungen von f und g natürlich durchaus davon abhängen, ob man sie über K oder über L betrachtet.

Durch Kombination dieses Ergebnisses mit Lemma 3.24 (b) erhalten wir nun ein einfaches und wichtiges Kriterium dafür, dass ein Polynom in seinem Zerfällungskörper keine mehrfachen Nullstellen hat:

Folgerung 4.30. *Es sei f ein nicht-konstantes irreduzibles Polynom über einem Körper K mit $\operatorname{char} K = 0$. Dann hat f in keinem Erweiterungskörper von K mehrfache Nullstellen.*

Beweis. Wegen $\operatorname{char} K = 0$ ist die formale Ableitung f' von f nicht das Nullpolynom (beachte, dass dies in positiver Charakteristik im Allgemeinen falsch ist, da z. B. das Polynom t^p über $\mathbb{Z}_p$ die formale Ableitung 0 hat). Damit sind f und f' in K teilerfremd: da f irreduzibel ist, könnte höchstens f ein gemeinsamer Teiler von f und f' sein — was aber unmöglich ist, da $f' \neq 0$ kleineren Grad als f hat und somit nicht f als Teiler haben kann. Also ist $\operatorname{ggt}(f,f') = 1$ in K, und nach Bemerkung 4.29 daher auch in jedem Erweiterungskörper $L \geq K$. Damit hat f nach Lemma 3.24 (b) keine mehrfachen Faktoren, insbesondere also auch keine mehrfachen Nullstellen in L. □

Kommen wir nun aber zum Beweis des Satzes vom primitiven Element:

Beweis von Satz 4.28. Da L/K eine endliche Körpererweiterung ist, können wir in jedem Fall $L = K(a_1,\dots,a_n)$ für gewisse Erzeuger $a_1,\dots,a_n \in L$ schreiben, die algebraisch über K sind. Mit Induktion über n genügt es dann offensichtlich zu zeigen, dass wir stets zwei Erzeuger zu einem zusammenfassen können. Mit anderen Worten können wir also annehmen, dass $L = K(a,b)$ von zwei Elementen erzeugt wird, und müssen dann zeigen, dass es ein $c \in L$ gibt mit $K(a,b) = K(c)$.

Dazu seien f und g die Minimalpolynome von a bzw. b sowie Z der Zerfällungskörper von $f \cdot g$. Dann zerfallen in Z auch f und g in Linearfaktoren, d. h. wir können

$$f = \prod_{i=1}^{r} (t - a_i) \qquad \text{und} \qquad g = \prod_{j=1}^{s} (t - b_j)$$

für gewisse $a_1,\dots,a_r,b_1,\dots,b_s \in Z$ schreiben. Beachte, dass die $a_1,\dots,a_r$ sowie die $b_1,\dots,b_s$ nach Folgerung 4.30 verschieden sind, da f und g als Minimalpolynome irreduzibel sind. Außerdem können wir diese Nullstellen so nummerieren, dass $a_1 = a$ und $b_1 = b$ gilt.

Wir wählen nun ein $\lambda \in K$, so dass

$$a_1 + \lambda b_1 \neq a_i + \lambda b_j \qquad \text{für alle } i = 1,\dots,r \text{ und } j = 2,\dots,s \tag{$*$}$$

gilt. Beachte, dass dies immer möglich ist: es sind ja nur die endlich vielen Werte $\frac{a_i - a_1}{b_1 - b_j}$ für λ ausgeschlossen, aber K enthält wegen $\operatorname{char} K = 0$ nach Aufgabe 1.11 (a) den Primkörper $P(K) = \mathbb{Q}$ und hat damit unendlich viele Elemente. Für ein solches λ setzen wir dann

$$c := a + \lambda b \quad \in L$$

und behaupten, dass dann $K(a,b) = K(c)$ gilt. Die Inklusion $K(c) \subset K(a,b)$ ist dabei natürlich offensichtlich.

Um die andere Inklusion zu sehen, betrachten wir das aus f durch Variablensubstitution entstehende Hilfspolynom

$$h(t) := f(c - \lambda t) \quad \in K(c)[t]$$

(beachte, dass c in der Regel nicht in K liegt und h damit nur über $K(c)$ definiert ist). Für dieses Polynom gilt nach Konstruktion einerseits

$$h(b_1) = f(c - \lambda b_1) = f(a_1) = f(a) = 0,$$

andererseits aber

$$h(b_j) = f(c - \lambda b_j) = f(\underbrace{a_1 + \lambda b_1 - \lambda b_j}_{\neq a_i \text{ für alle } i \text{ nach } (*)}) \neq 0$$

für $j = 2,\dots,s$, da die $a_1,\dots,a_r$ ja die einzigen Nullstellen von f sind. Damit können wir nun leicht den größten gemeinsamen Teiler von g und h in Z ablesen: die Primfaktorzerlegung von g enthält die (verschiedenen) Faktoren $t - b_j$ für $j = 1,\dots,s$ jeweils einfach, während die von h den Faktor $t - b_1$ wegen $h(b_1) = 0$ enthält, die anderen $t - b_j$ für $j = 2,\dots,s$ wegen $h(b_j) \neq 0$ jedoch nicht. Also ist $\operatorname{ggt}(g,h) = t - b_1 = t - b$ in Z.

Da g und h beide über $K(c)$ definiert sind, gilt nach Bemerkung 4.29 damit aber auch $\operatorname{ggt}(g,h) = t - b$ über $K(c)$. Insbesondere ist damit $t - b$ ein Polynom über $K(c)$, d. h. es ist $b \in K(c)$ und damit auch $a = c - \lambda b \in K(c)$. Also ergibt sich auch die Inklusion $K(a,b) \subset K(c)$ und somit wie behauptet $K(a,b) = K(c)$. □

Beispiel 4.31. Der Beweis von Satz 4.28 ist konstruktiv: er besagt, dass wir zu einer Körpererweiterung $K(a,b)$ in Charakteristik 0 konkret ein Element c mit $K(a,b) = K(c)$ finden, indem wir eine „nahezu beliebige" Linearkombination $c = a + \lambda b$ für ein $\lambda \in K$ wählen — wir müssen lediglich die Bedingung $(*)$ im Beweis des Satzes sicher stellen, wobei $a_1 = a, a_2, \ldots, a_r$ und $b_1 = b, b_2, \ldots, b_s$ die Nullstellen der Minimalpolynome von a und b in einem geeigneten Erweiterungskörper sind.

Betrachten wir einmal konkret das Beispiel $\mathbb{Q}(\sqrt{2}, \sqrt{3})$ aus Aufgabe 1.17, d. h. $a = \sqrt{2}$ und $b = \sqrt{3}$, dann sind die Minimalpolynome dieser Elemente gleich $f = t^2 - 2$ bzw. $g = t^2 - 3$, und davon die Nullstellen in $\mathbb{C}$ wiederum $a_1 = \sqrt{2}$, $a_2 = -\sqrt{2}$, $b_1 = \sqrt{3}$, $b_2 = -\sqrt{3}$. Nach $(*)$ müssen wir also nur überprüfen, dass

$$\lambda \neq \frac{\pm\sqrt{2} - \sqrt{2}}{2\sqrt{3}}$$

ist — was bei $\lambda \in \mathbb{Q}$ für alle $\lambda \neq 0$ erfüllt ist. Damit gilt

$$\mathbb{Q}(\sqrt{2}, \sqrt{3}) = \mathbb{Q}(\sqrt{2} + \lambda\sqrt{3})$$

für alle $\lambda \in \mathbb{Q} \backslash \{0\}$. Für den Spezialfall $\lambda = 1$ hatten wir dies in Aufgabe 1.17 bereits direkt überprüft.

5. Galoisgruppen

Nach dem Studium von Zerfällungskörpern im letzten Kapitel wollen wir nun wieder zu unseren Problemen aus der Einleitung zurückkehren. Dazu erinnern wir uns zunächst noch einmal kurz daran, was wir z. B. über die Konstruktion des regelmäßigen n-Ecks mit Zirkel und Lineal bereits wissen: nach Beispiel 1.23 (C) ist das n-Eck genau dann konstruierbar, wenn $z = e^{\frac{2\pi i}{n}}$ in einer 2-Radikalerweiterung von $\mathbb{Q}$ liegt, d. h. wenn es eine Kette

$$\mathbb{Q} = K_0 \leq K_1 \leq \cdots \leq K_m = L$$

von Unterkörpern von $\mathbb{C}$ gibt, so dass $z \in L$ und jedes K_i/K_{i-1} für $i = 1, \ldots, m$ eine einfache 2-Radikalerweiterung ist (bzw. nach Aufgabe 2.21 (b) einfach Grad 2 hat).

Wir haben in Folgerung 2.22 (a) gezeigt, dass eine *notwendige* Bedingung hierfür ist, dass der Grad $[z : \mathbb{Q}]$ eine Zweierpotenz ist. Diesen Grad haben wir in Satz 3.29 dann auch konkret berechnet — er ist gerade der Wert $\varphi(n)$ der Eulerschen φ-Funktion.

Wir wollen nun sehen, ob wir auch *hinreichende* Kriterien für die Konstruierbarkeit angeben können, die sich ähnlich leicht nachprüfen lassen. Nach Satz 3.29 ist für $n = 17$ z. B. $\varphi(n) = 16 = 2^4$ eine Zweierpotenz; unser notwendiges Kriterium ist damit in diesem Fall erfüllt. Wir müssen jetzt also herausfinden, ob wir eine Kette

$$\mathbb{Q} = K_0 \leq K_1 \leq K_2 \leq K_3 \leq K_4 = \mathbb{Q}\left(e^{\frac{2\pi i}{17}}\right)$$

von Körpern mit $[K_i : K_{i-1}] = 2$ für $i = 1, \ldots, 4$ finden können. Dies ist jedoch nicht so einfach. Wir benötigen dazu offensichtlich genauere Informationen über die Zwischenkörper von $\mathbb{Q}(z)/\mathbb{Q}$, also über die Körper Z mit $\mathbb{Q} \leq Z \leq \mathbb{Q}(z)$.

Die Idee der Galoistheorie ist nun, die Frage nach *Zwischenkörpern einer gegebenen Körpererweiterung* auf die Frage nach *Untergruppen einer gegebenen Gruppe* zurückzuführen. Die Anzahl der Elemente der Gruppen entsprechen dabei den Graden der Körpererweiterung. Im Fall des 17-Ecks werden wir also eine gewisse Gruppe G mit 16 Elementen haben und untersuchen müssen, ob es eine Kette von Untergruppen

$$G = U_0 \geq U_1 \geq U_2 \geq U_3 \geq U_4 = \{e\}$$

gibt, deren Anzahl Elemente genau 16, 8, 4, 2 bzw. 1 ist. Da endliche Gruppen viel einfacher zu behandeln sind als Körpererweiterungen, werden wir unser Problem schließlich auf diese Art lösen können. In der Tat werden wir in Aufgabe 5.4 sehen, dass die Gruppe G im Fall des 17-Ecks einfach $\mathbb{Z}_{16}$ ist. Von dieser Gruppe können wir natürlich alle Untergruppen leicht angeben [G, Aufgabe 6.28 (a)] und insbesondere sehen, dass dort eine Untergruppenkette

$$\mathbb{Z}_{16} = \langle \overline{1} \rangle \geq \langle \overline{2} \rangle \geq \langle \overline{4} \rangle \geq \langle \overline{8} \rangle \geq \{\overline{0}\}$$

wie oben existiert — woraus wir dann mit Hilfe der Galoistheorie schließen können, dass auch die oben erwähnte Kette von Zwischenkörpern von $\mathbb{Q}(z)/\mathbb{Q}$ existiert und das 17-Eck damit konstruierbar ist.

Wir wollen diesen Zusammenhang zwischen Untergruppen und Zwischenkörpern nun in diesem und dem folgenden Kapitel konkret konstruieren. Da unsere Anwendungen der Galoistheorie letztlich bei Körpererweiterungen von $\mathbb{Q}$ liegen, werden wir uns dabei auf den Fall von (endlichen) Körpererweiterungen in Charakteristik 0 beschränken. Galoistheorie funktioniert zwar auch in positiver Charakteristik, jedoch ist sie dort komplizierter, da dort einige Sätze nicht gelten, die uns im Folgenden das Leben einfacher machen werden (wie z. B. der Satz 4.28 vom primitiven Element oder die Äquivalenz von galoisschen und normalen Körpererweiterungen in Satz 5.8). Wir vereinbaren also:

In Kapitel 5 und 6 seien alle Körpererweiterungen endlich und von Charakteristik 0.

Um mit unserem Programm zu beginnen, werden wir nun als Erstes angeben, wie wir überhaupt einem Körper bzw. einer Körpererweiterung eine Gruppe zuordnen wollen.

Definition 5.1 (Automorphismengruppe und Galoisgruppe)**.** Es sei L/K eine Körpererweiterung.

(a) Wir bezeichnen mit $\mathrm{Aut}(L)$ die Menge aller Körperisomorphismen $\sigma : L \to L$. Der Name kommt daher, dass man Isomorphismen mit gleichem Start- und Zielraum auch als **Automorphismen** bezeichnet. Offensichtlich ist $\mathrm{Aut}(L)$ mit der Verkettung von Abbildungen eine Gruppe. Man nennt sie die **Automorphismengruppe** von L.

(b) Wichtiger für uns ist die entsprechende relative Version: die Menge

$$\mathrm{Gal}(L/K) := \mathrm{Aut}(L/K) := \{\sigma : L \to L \text{ Körperisomorphismus mit } \sigma|_K = \mathrm{id}\}$$

der Automorphismen von L, die alle Elemente von K fest lassen (also die Menge aller K-Automorphismen in der Sprechweise von Bemerkung 4.9). Auch dies ist zusammen mit der Verkettung von Abbildungen offensichtlich eine Gruppe. Man nennt sie die **Galoisgruppe** bzw. Automorphismengruppe von L/K (in der Literatur sind beide Bezeichnungen üblich).

Das Ziel dieses Kapitels ist es, diese Galoisgruppen von Körpererweiterungen zu studieren. Dazu werden wir natürlich gleich auch einige Beispiele von Galoisgruppen sehen. Um diese einfacher berechnen zu können, benötigen wir jedoch zunächst ein Lemma.

Lemma 5.2 (Eigenschaften von Galoisgruppen)**.** *Es sei L/K eine Körpererweiterung (gemäß unserer Konvention endlich und von Charakteristik 0). Dann gilt:*

(a) *Es sei $f \in K[t]$ und $a \in L$ mit $f(a) = 0$. Für jedes Element der Galoisgruppe $\sigma \in \mathrm{Gal}(L/K)$ gilt dann auch $f(\sigma(a)) = 0$. (Man sagt: die Elemente der Galoisgruppe bilden Nullstellen auf Nullstellen ab.)*

(b) *Ist $L = K(a)$ und f das Minimalpolynom von a, so gibt es eine Bijektion*

$$\begin{aligned} \{\textit{Nullstellen von } f \textit{ in } L\} &\overset{1:1}{\longleftrightarrow} \mathrm{Gal}(L/K) \\ b &\longmapsto \textit{der eindeutig bestimmte Isomorphismus } \sigma : L \to L \\ &\qquad \textit{mit } \sigma|_K = \mathrm{id} \textit{ und } \sigma(a) = b \\ \sigma(a) &\longmapsfrom \sigma. \end{aligned}$$

(c) $|\mathrm{Gal}(L/K)| \leq [L : K]$. *(Insbesondere sind Galoisgruppen also stets endliche Gruppen.)*

Beweis.

(a) Es sei $f = c_n t^n + \cdots + c_1 t + c_0$ mit $c_0, \ldots, c_n \in K$. Dann gilt

$$\begin{aligned} f(\sigma(a)) &= c_n \sigma(a)^n + \cdots + c_1 \sigma(a) + c_0 \\ &= \sigma(c_n)\,\sigma(a)^n + \cdots + \sigma(c_1)\sigma(a) + \sigma(c_0) && (\sigma|_K = \mathrm{id}) \\ &= \sigma(c_n a^n + \cdots + c_1 a + c_0) && (\sigma \text{ Körperhomomorphismus}) \\ &= \sigma(f(a)) = \sigma(0) = 0. \end{aligned}$$

(b) Wir müssen zeigen, dass die beiden angegebenen Abbildungen existieren.

Für die Abbildung „$\longmapsto$“ betrachten wir eine Nullstelle b von f in L. Dann ist $K(b) \leq L$ nach Bemerkung 4.2 (a) ein Stammkörper von f, nach Bemerkung 4.2 (c) ist demzufolge $[K(b) : K] = \deg f = [K(a) : K] = [L : K]$. Mit der Gradformel aus Satz 2.17, angewendet auf $K \leq K(b) \leq L$, bedeutet dies $[L : K(b)] = 1$ und damit $K(b) = L$.

Die Eindeutigkeit von Stammkörpern aus Lemma 4.8 besagt daher nun, dass es genau einen Isomorphismus σ von $K(a) = L$ nach $K(b) = L$ mit $\sigma|_K = \mathrm{id}$ und $\sigma(a) = b$ gibt. Also existiert die im Lemma angegebene Abbildung „$\longmapsto$“.

Die Abbildung „$\longmapsfrom$“ existiert, da jedes $\sigma \in \mathrm{Gal}(L/K)$ die Nullstelle a von f nach (a) wieder auf eine Nullstelle von f abbildet.

Nach Konstruktion ist klar, dass die beiden Abbildungen invers zueinander sind.

(c) Nach dem Satz 4.28 vom primitiven Element können wir annehmen, dass $L = K(a)$ eine einfache Körpererweiterung ist. Ist f das Minimalpolynom von a, so ist $\mathrm{Gal}(L/K)$ nach (b) bijektiv zur Menge der Nullstellen von f in L. Also hat $\mathrm{Gal}(L/K)$ höchstens $\deg f$ Elemente. Da nach Bemerkung 4.2 (c) ferner $\deg f = [L:K]$ gilt, folgt die Behauptung. □

Beispiel 5.3. Wir wollen nun mit Hilfe von Lemma 5.2 (b) einige Galoisgruppen konkret berechnen. Dazu müssen wir offensichtlich die gegebene Körpererweiterung L/K als einfache Körpererweiterung $K(a)/K$ schreiben, das Minimalpolynom f von a bestimmen, und untersuchen, welche bzw. wie viele Nullstellen f in L besitzt.

(a) Es sei $L/K = \mathbb{C}/\mathbb{R} = \mathbb{R}(i)/\mathbb{R}$ (vgl. Beispiel 4.10 (a)). Das Minimalpolynom von i ist natürlich $f = t^2+1$, und dieses Polynom hat in L zwei Nullstellen, nämlich i und $-i$. Also hat die Galoisgruppe $\mathrm{Gal}(\mathbb{C}/\mathbb{R})$ nach Lemma 5.2 (b) zwei Elemente $\sigma_0, \sigma_1 : \mathbb{C} \to \mathbb{C}$, die eindeutig bestimmt sind durch

$$\begin{aligned} & \sigma_0|_{\mathbb{R}} = \mathrm{id} \quad \text{und} \quad \sigma_0(i) = i \\ \text{bzw.} \quad & \sigma_1|_{\mathbb{R}} = \mathrm{id} \quad \text{und} \quad \sigma_1(i) = -i. \end{aligned}$$

In der Tat kann man hier einfach sehen, dass diese Angaben σ_0 und σ_1 eindeutig bestimmen: für jedes $z = x+iy \in \mathbb{C}$ mit $x, y \in \mathbb{R}$ ist ja

$$\begin{aligned} & \sigma_0(x+iy) = \sigma_0(x) + \sigma_0(i)\,\sigma_0(y) = x+iy \\ \text{und} \quad & \sigma_1(x+iy) = \sigma_1(x) + \sigma_1(i)\,\sigma_1(y) = x-iy, \end{aligned}$$

also ist σ_0 die Identität und σ_1 die komplexe Konjugation. Als Gruppe gilt offensichtlich $\mathrm{Gal}(\mathbb{C}/\mathbb{R}) = \{\sigma_0, \sigma_1\} \cong \mathbb{Z}_2$, wobei die Identität σ_0 das neutrale Element ist. Insbesondere gilt hier in Lemma 5.2 (c) also die Gleichheit $|\mathrm{Gal}(\mathbb{C}/\mathbb{R})| = 2 = [\mathbb{C}:\mathbb{R}]$, da das quadratische Polynom f in $\mathbb{C}$ wirklich zwei (verschiedene) Nullstellen besitzt.

(b) Es sei $L/K = \mathbb{Q}(\sqrt[3]{2})/\mathbb{Q}$. Hier hat das Minimalpolynom $f = t^3 - 2$ von $\sqrt[3]{2}$ nur die Nullstelle $\sqrt[3]{2}$ in L, da die anderen beiden (komplexen) Nullstellen $\sqrt[3]{2}\,e^{\frac{2\pi i}{3}}$ und $\sqrt[3]{2}\,e^{\frac{4\pi i}{3}}$ nicht reell sind und somit nicht im Körper $\mathbb{Q}(\sqrt[3]{2}) \leq \mathbb{R}$ liegen können. Also ist das einzige Element in der Galoisgruppe nach Lemma 5.2 (b) die Identität auf L, d. h. $\mathrm{Gal}(\mathbb{Q}(\sqrt[3]{2})/\mathbb{Q})$ ist die triviale Gruppe mit nur einem Element. Insbesondere gilt nun in Lemma 5.2 (c) eine echte Ungleichung $|\mathrm{Gal}(\mathbb{Q}(\sqrt[3]{2})/\mathbb{Q})| = 1 < 3 = [\mathbb{Q}(\sqrt[3]{2}) : \mathbb{Q}]$, da das kubische Minimalpolynom $t^3 - 2$ keine drei Nullstellen in $\mathbb{Q}(\sqrt[3]{2})$ besitzt.

(c) Es sei $L/K = \mathbb{Q}(e^{\frac{2\pi i}{n}})/\mathbb{Q}$ für ein $n \in \mathbb{N}_{>0}$. Nach Satz 3.27 (b) ist das Minimalpolynom f von $e^{\frac{2\pi i}{n}}$ gerade das n-te Kreisteilungspolynom Φ_n aus Definition 3.16. Die Nullstellen dieses Polynoms sind nach Konstruktion genau die primitiven n-ten Einheitswurzeln E_n', also nach Bemerkung 3.15 (b) die komplexen Zahlen $e^{\frac{2\pi ik}{n}}$ für alle k mit $\mathrm{ggt}(k,n) = 1$ bzw. $\overline{k} \in \mathbb{Z}_n^*$. Diese liegen natürlich alle im Körper L, denn L ist ja multiplikativ abgeschlossen und $e^{\frac{2\pi ik}{n}}$ gerade die k-te Potenz von $e^{\frac{2\pi i}{n}}$.

Also ist $\mathrm{Gal}(L/K)$ nach Lemma 5.2 (b) bijektiv zur Menge E_n' der primitiven n-ten Einheitswurzeln bzw. zu $\mathbb{Z}_n^*$: zu jedem k mit $\mathrm{ggt}(k,n) = 1$ gehört ein Element σ_k von $\mathrm{Gal}(L/K)$, das durch

$$\sigma_k|_{\mathbb{Q}} = \mathrm{id} \quad \text{und} \quad \sigma_k(e^{\frac{2\pi i}{n}}) = e^{\frac{2\pi ik}{n}} \qquad (*)$$

eindeutig bestimmt ist. Insbesondere gilt hier in Lemma 5.2 (c) also wieder die Gleichheit: es ist $|\mathrm{Gal}(L/K)| = |E_n'| = \varphi(n) = [L:K]$ nach Satz 3.29.

Um auch noch die Gruppenstruktur der Galoisgruppe zu verstehen, müssen wir schließlich noch die Verknüpfungstabelle der σ_k berechnen. Dies ist sehr einfach: haben wir k, l mit $\mathrm{ggt}(k,n) = \mathrm{ggt}(l,n) = 1$, so gilt nach $(*)$

$$(\sigma_k \circ \sigma_l)(e^{\frac{2\pi i}{n}}) = \sigma_k(e^{\frac{2\pi il}{n}}) = \sigma_k(e^{\frac{2\pi i}{n}})^l = (e^{\frac{2\pi ik}{n}})^l = e^{\frac{2\pi ikl}{n}}$$

und damit $\sigma_k \circ \sigma_l = \sigma_{k \cdot l}$. Diese Gleichung bedeutet aber genau, dass die Abbildung

$$\mathbb{Z}_n^* \to \mathrm{Gal}(L/K), \quad \bar{k} \mapsto \sigma_k$$

ein Gruppenhomomorphismus ist. Da wir diese Abbildung oben schon als bijektiv erkannt haben, ist sie also sogar ein Isomorphismus, und wir erhalten als Resultat, dass

$$\mathrm{Gal}\left(\mathbb{Q}(e^{\frac{2\pi i}{n}})/\mathbb{Q}\right) \cong \mathbb{Z}_n^*.$$

Aufgabe 5.4. Zeige, dass die Gruppen $\mathbb{Z}_{17}^*$ und $\mathbb{Z}_{16}$ isomorph sind, und dass mit Beispiel 5.3 (c) demnach

$$\mathrm{Gal}\left(\mathbb{Q}(e^{\frac{2\pi i}{17}})/\mathbb{Q}\right) \cong \mathbb{Z}_{16}$$

gilt. (Wenn ihr die Vorlesung „Elementare Zahlentheorie“ bereits gehört habt, werdet ihr dies bereits wissen, da ihr dort dann allgemein bewiesen habt, dass die Gruppe $\mathbb{Z}_p^*$ für jede Primzahl p zyklisch mit $p-1$ Elementen und somit isomorph zu $\mathbb{Z}_{p-1}$ ist.)

Aufgabe 5.5. Es sei L/K eine algebraische, aber nicht notwendig endliche Körpererweiterung. Beweise, dass jeder K-Homomorphismus $\varphi : L \to L$ (also jeder Körperhomomorphismus $\varphi : L \to L$ mit $\varphi|_K = \mathrm{id}$) bereits ein K-Isomorphismus ist.

08

Wir hatten in der Einleitung zu diesem Kapitel ja schon erwähnt, dass in unserer Galois-Korrespondenz zwischen Untergruppen und Zwischenkörpern letztlich die Ordnungen der Gruppen den Graden der Körpererweiterungen entsprechen sollen. Daher werden für uns in Zukunft besonders die Körpererweiterungen L/K interessant sein, bei denen in der Beziehung $|\mathrm{Gal}(L/K)| \leq [L:K]$ aus Lemma 5.2 (c) die Gleichheit gilt. Wir geben diesen Erweiterungen zunächst einen besonderen Namen.

Definition 5.6 (Galoissche Körpererweiterung)**.** Eine Körpererweiterung L/K heißt **galoissch**, wenn $|\mathrm{Gal}(L/K)| = [L:K]$.

Beispiel 5.7. Wie wir in Beispiel 5.3 gesehen haben, sind die Körpererweiterungen $\mathbb{C}/\mathbb{R}$ und $\mathbb{Q}(e^{\frac{2\pi i}{n}})/\mathbb{Q}$ für $n \in \mathbb{N}_{>0}$ galoissch, $\mathbb{Q}(\sqrt[3]{2})/\mathbb{Q}$ jedoch nicht.

Zur Eigenschaft „galoissch“ einer Körpererweiterung gibt es einige äquivalente Bedingungen. Die wichtigsten von ihnen, die auch in der Praxis häufig verwendet werden, sind die folgenden.

Satz 5.8 (Äquivalente Bedingungen zu „galoissch“)**.** *Es sei L/K eine Körpererweiterung (wie üblich endlich und von Charakteristik 0). Dann sind die folgenden Eigenschaften äquivalent:*

(a) *L/K ist galoissch.*

(b) *L ist der Zerfällungskörper eines Polynoms über K.*

(c) *Ist $g \in K[t]$ ein irreduzibles Polynom, das eine Nullstelle in L besitzt, so zerfällt g in L bereits in Linearfaktoren. (Körpererweiterungen mit dieser Eigenschaft werden in der Literatur oft als **normal** bezeichnet.)*

Beweis. Nach dem Satz 4.28 vom primitiven Element können wir annehmen, dass $L = K(a)$ eine einfache Körpererweiterung ist. Es sei $f \in K[t]$ das Minimalpolynom von a, so dass L also der Stammkörper von f ist. Wir zeigen die Äquivalenz der angegebenen Aussagen durch einen Ringschluss.

„(a) $\Rightarrow$ (b)“: Die Anzahl der Nullstellen von f in L ist gleich

$$\begin{aligned} & |\mathrm{Gal}(L/K)| && \text{(Lemma 5.2 (b))} \\ = {} & [L:K] && \text{(Voraussetzung)} \\ = {} & \deg f && \text{(Bemerkung 4.2 (c)).} \end{aligned}$$

Insbesondere muss f damit über L in Linearfaktoren zerfallen. Da a eine Nullstelle von f ist, ist L also der Zerfällungskörper von f.

„(b) $\Rightarrow$ (c)“: Dies ist genau die Aussage von Aufgabe 4.19 (b).

„(c) $\Rightarrow$ (a)“: Das irreduzible Polynom f hat natürlich die Nullstelle a in L und zerfällt nach Voraussetzung damit über L in Linearfaktoren. Diese Linearfaktoren sind nach Folgerung 4.30 auch alle verschieden. Also hat f genau $\deg f$ Nullstellen in L. Nach Lemma 5.2 (b) und Bemerkung 4.2 (c) gilt damit $|\mathrm{Gal}(L/K)| = \deg f = [L:K]$, d. h. L/K ist galoissch. □

Bemerkung 5.9.

(a) Der Beweis der Richtung „(a) $\Rightarrow$ (b)“ in Satz 5.8 zeigt zusätzlich, dass es eine weitere äquivalente Bedingung für eine galoissche Körpererweiterung L/K ist, dass L der Zerfällungskörper eines *irreduziblen* Polynoms über K ist.

(b) In positiver Charakteristik ist die Aussage von Satz 5.8 falsch. Man kann z. B. zeigen, dass die Begriffe „galoissch“ und „normal“ dort in der Regel verschieden sind — was auch erklärt, warum es hierfür zwei verschiedene Namen gibt.

Da die für uns später besonders wichtigen galoisschen Körpererweiterungen nach Satz 5.8 genau die Zerfällungskörper von Polynomen sind, führen wir nun eine weitere Notation ein, die einem Polynom direkt die Galoisgruppe seines Zerfällungskörpers zuordnet. Gleichzeitig gibt uns dies im folgenden Lemma auch eine gute Möglichkeit, wie wir uns solche Galoisgruppen anschaulich vorstellen können.

Definition 5.10 (Galoisgruppe eines Polynoms)**.** Es sei $f \in K[t]$ ein Polynom über einem Körper K mit $f \neq 0$. Ist L der Zerfällungskörper von f (der nach Satz 5.8 galoissch über K ist), so definieren wir die **Galoisgruppe** von f als $\mathrm{Gal}(f) := \mathrm{Gal}(L/K)$.

Lemma 5.11 (Galoisgruppen als Untergruppen von S_n)**.** *Es sei $f \in K[t]$ ein Polynom über einem Körper K mit $n := \deg f \in \mathbb{N}_{>0}$. Dann gilt:*

(a) *Jedes Element von $\mathrm{Gal}(f)$ permutiert die Nullstellen von f in seinem Zerfällungskörper. Auf diese Art ist $\mathrm{Gal}(f)$ isomorph zu einer Untergruppe der symmetrischen Gruppe S_n.*

(b) *Ist f irreduzibel, so ist die Ordnung $|\mathrm{Gal}(f)|$ der Galoisgruppe von f ein Vielfaches von n.*

Beweis. Es seien L der Zerfällungskörper von f und $a_1, \dots, a_m$ mit $m \leq n$ die verschiedenen Nullstellen von f in L, so dass also $L = K(a_1, \dots, a_m)$.

(a) Beachte, dass jedes Element $\sigma \in \mathrm{Gal}(f)$ als Körperisomorphismus $\sigma : L \to L$ bijektiv ist und Nullstellen von f nach Lemma 5.2 (a) wieder auf Nullstellen von f abbildet. Also induziert ein solches σ eine Permutation der Nullstellen von f, d. h. wir erhalten eine Abbildung

$$\begin{aligned} \mathrm{Gal}(f) &\to S_m \\ \sigma &\mapsto \text{die Permutation } \tau \in S_m \text{ mit } \sigma(a_i) = a_{\tau(i)} \text{ für } i = 1, \dots, m. \end{aligned}$$

Diese Abbildung ist ein Gruppenhomomorphismus, denn wird unter ihr σ auf τ und σ' auf τ' abgebildet, so ist

$$(\sigma \circ \sigma')(a_i) = \sigma(a_{\tau'(i)}) = a_{(\tau \circ \tau')(i)},$$

d. h. $\sigma \circ \sigma'$ wird auf $\tau \circ \tau'$ abgebildet. Außerdem ist sie injektiv, denn ist $\sigma \in \mathrm{Gal}(f)$ mit $\sigma(a_i) = a_i$ für alle $i = 1, \dots, m$, so ist σ die Identität auf K und allen a_i und damit auch auf dem davon erzeugten Körper $K(a_1, \dots, a_m) = L$.

Nach dem Homomorphiesatz [G, Satz 6.17] ist $\mathrm{Gal}(f)$ also isomorph zu einer Untergruppe von S_m, und wegen $S_m \leq S_n$ damit auch zu einer Untergruppe von S_n.

(b) Nach Lemma 2.18 ist $[a_1 : K]$ ein Teiler von $[L : K]$. Nun ist aber einerseits $[a_1 : K] = \deg f = n$, da f irreduzibel und damit bis auf Normierung das Minimalpolynom von a_1 ist, und andererseits $[L : K] = |\mathrm{Gal}(L/K)| = |\mathrm{Gal}(f)|$, da L/K als Zerfällungskörper nach Satz 5.8 galoissch ist. Also ist n wie behauptet ein Teiler von $|\mathrm{Gal}(f)|$. □

Beispiel 5.12. Das Polynom $f = t^3 - 2$ hat offensichtlich die drei Nullstellen

$$a_1 = \sqrt[3]{2}, \quad a_2 = \sqrt[3]{2}e^{\frac{2\pi i}{3}}, \quad a_3 = \sqrt[3]{2}e^{\frac{4\pi i}{3}}$$

in $\mathbb{C}$. Sein Zerfällungskörper ist also nach Aufgabe 4.18 (a)

$$L = \mathbb{Q}(a_1, a_2, a_3) = \mathbb{Q}\left(\sqrt[3]{2}, e^{\frac{2\pi i}{3}}\right)$$

und hat Grad $[L : \mathbb{Q}] = 6$ über $\mathbb{Q}$. Da diese Körpererweiterung nach Satz 5.8 galoissch ist, ist also $|\mathrm{Gal}(f)| = |\mathrm{Gal}(L/\mathbb{Q})| = [L : \mathbb{Q}] = 6$. Mit der Interpretation aus Lemma 5.11 (a) bedeutet dies genau, dass $\mathrm{Gal}(f) \cong S_3$ gelten muss, also dass man jede Permutation der drei Nullstellen von f durch einen $\mathbb{Q}$-Automorphismus von L erzeugen kann. Die Permutation $(2\ 3) \in S_3$ erhält man z. B. genau durch die komplexe Konjugation $\sigma \in \mathrm{Gal}(L/\mathbb{Q})$, $\sigma(z) = \overline{z}$, denn es ist ja $\sigma(a_1) = \overline{a_1} = a_1$, $\sigma(a_2) = \overline{a_2} = a_3$ und $\sigma(a_3) = \overline{a_3} = a_2$.

Allgemein besagt Lemma 5.11 für ein irreduzibles Polynom f vom Grad 3, dass $\mathrm{Gal}(f)$ isomorph zu einer Untergruppe von S_3 ist, deren Ordnung ein Vielfaches von 3 ist. Nach [G, Beispiel 5.16] sind die einzigen solchen Untergruppen die symmetrische Gruppe S_3 selbst sowie die alternierende Gruppe $A_3 = \{\mathrm{id}, (1\ 2\ 3), (1\ 3\ 2)\}$. Wiederum nach der Interpretation aus Lemma 5.11 (a) liegt der Unterschied dieser beiden Fälle darin, dass sich im Fall $\mathrm{Gal}(f) \cong A_3$ nicht jede Permutation der Nullstellen von f durch einen $\mathbb{Q}$-Automorphismus von L realisieren lässt. Wie aber kann man in der Praxis für ein gegebenes Polynom feststellen, ob dies der Fall ist? Die Antwort auf diese Frage gibt der folgende Satz. Er ist zwar einerseits sehr konkret, andererseits aber auch überraschend komplex, und soll hier vor allem als Beispiel dafür dienen, welche Art von Überlegungen man anstellen muss, um Galoisgruppen explizit zu berechnen.

Satz 5.13 (Galoisgruppen irreduzibler Polynome vom Grad 3)**.** *Es sei $f = t^3 + \lambda_2 t^2 + \lambda_1 t + \lambda_0 \in \mathbb{Q}[t]$ ein normiertes irreduzibles Polynom vom Grad 3. Wir definieren die **Diskriminante** von f als*

$$\Delta := \lambda_1^2\lambda_2^2 - 4\lambda_1^3 - 4\lambda_0\lambda_2^3 + 18\lambda_0\lambda_1\lambda_2 - 27\lambda_0^2 \quad \in \mathbb{Q}.$$

Dann ist $\Delta \neq 0$, und es gilt:

(a) *Ist Δ ein Quadrat in $\mathbb{Q}$, also $\Delta = z^2$ für ein $z \in \mathbb{Q}$, so ist $\mathrm{Gal}(f) \cong A_3$.*

(b) *Ist Δ kein Quadrat in $\mathbb{Q}$, so ist $\mathrm{Gal}(f) \cong S_3$.*

Beweis. Da f irreduzibel ist, hat f nach Folgerung 4.30 drei verschiedene komplexe Nullstellen a_1, a_2, a_3. Offensichtlich gilt dann

$$t^3 + \lambda_2 t^2 + \lambda_1 t + \lambda_0 = (t - a_1)(t - a_2)(t - a_3),$$

woraus man durch Ausmultiplizieren und Koeffizientenvergleich die drei Gleichungen

$$\begin{aligned} \lambda_2 &= -a_1 - a_2 - a_3, \\ \lambda_1 &= a_1a_2 + a_2a_3 + a_3a_1, \\ \lambda_0 &= -a_1a_2a_3 \end{aligned}$$

erhält. Einsetzen dieser Ausdrücke in die Diskriminante von f zeigt nach einer elementaren, aber sehr langen Rechnung, dass

$$\Delta = (a_1 - a_2)^2(a_2 - a_3)^2(a_3 - a_1)^2.$$

Für ein geeignetes $z \in \mathbb{C}$ mit $z^2 = \Delta$ gilt also

$$z = (a_1 - a_2)(a_2 - a_3)(a_3 - a_1). \qquad (*)$$

Da die drei Nullstellen von f verschieden sind, ist ferner $\Delta \neq 0$ und damit auch $z \neq 0$.

(a) Es sei nun $z \in \mathbb{Q}$. Angenommen, die Transposition $(1\ 2)$ wäre in der Galoisgruppe von f, d. h. es gäbe einen $\mathbb{Q}$-Automorphismus σ des Zerfällungskörpers $\mathbb{Q}(a_1, a_2, a_3)$ mit $\sigma(a_1) = a_2$, $\sigma(a_2) = a_1$ und $\sigma(a_3) = a_3$. Wenden wir σ auf die Gleichung $(*)$ an, erhalten wir dann

$$\sigma(z) = (\sigma(a_1) - \sigma(a_2))(\sigma(a_2) - \sigma(a_3))(\sigma(a_3) - \sigma(a_1))$$

und damit

$$z = (a_2 - a_1)(a_1 - a_3)(a_3 - a_2),$$

durch Vergleich mit $(*)$ also $z = -z$, was wegen $z \neq 0$ ein Widerspruch ist. Also ist $(1\ 2) \notin \mathrm{Gal}(f)$, d. h. $\mathrm{Gal}(f)$ ist nicht die gesamte Gruppe S_3 und muss nach Beispiel 5.12 damit isomorph zu A_3 sein.

(b) Ist dagegen $z \notin \mathbb{Q}$, so folgt $[z : \mathbb{Q}] = 2$ wegen $z^2 = \Delta \in \mathbb{Q}$. Aber z liegt wegen der Gleichung $(*)$ offensichtlich im Zerfällungskörper $\mathbb{Q}(a_1, a_2, a_3)$ von f. Damit muss der Grad des Zerfällungskörpers nach Folgerung 2.18 durch 2 teilbar sein. Dies schließt $\mathrm{Gal}(f) \cong A_3$ aus, und nach Beispiel 5.12 bleibt nur noch die Möglichkeit $\mathrm{Gal}(f) \cong S_3$. □

Beispiel 5.14.

(a) Irreduzible kubische Polynome der Form $t^3 - a \in \mathbb{Q}[t]$ haben nach Satz 5.13 stets die Galoisgruppe S_3, denn ihre Diskriminante $\Delta = -27a^2$ ist negativ und damit nie ein Quadrat in $\mathbb{Q}$. In der Tat funktioniert für solche Polynome auch stets das Argument aus Beispiel 5.12, um zu sehen, dass ihre Galoisgruppe S_3 ist.

(b) Im Gegensatz dazu hat das rationale Polynom $f = t^3 - 3t + 1$ die Diskriminante

$$\Delta = -4 \cdot (-3)^3 - 27 \cdot 1^2 = 81 = 9^2,$$

die ein Quadrat in $\mathbb{Q}$ ist. Da f außerdem keine Nullstellen in $\mathbb{Q}$ hat und damit nach Aufgabe 2.7 (a) irreduzibel ist, ist also $\mathrm{Gal}(f) \cong A_3$ nach Satz 5.13.

Wir sehen hier also schon, dass es eine besondere Bedingung ist, dass $\mathrm{Gal}(f) \cong A_3$ gilt. Für die „meisten“ irreduziblen kubischen Polynome über $\mathbb{Q}$ wird die Diskriminante kein Quadrat und die Galoisgruppe daher S_3 sein.

Bemerkung 5.15 (Diskriminanten)**.** Diskriminanten wie in Satz 5.13 kann man nicht nur für kubische Polynome konstruieren. Ist etwa $f = t^n + \lambda_{n-1}t^{n-1} + \cdots + \lambda_1 t + \lambda_0 \in \mathbb{Q}[t]$ ein normiertes Polynom vom Grad n mit (nicht notwendig verschiedenen) Nullstellen $a_1, \ldots, a_n \in \mathbb{C}$, so setzt man

$$\Delta := \prod_{1 \leq i < j \leq n} (a_i - a_j)^2.$$

Offensichtlich ist Δ genau dann gleich Null, wenn f mehrfache Nullstellen in $\mathbb{C}$ besitzt. Die Quadrate in der obigen Formel bewirken, dass Δ unabhängig von der Nummerierung der Nullstellen ist und damit nur von f abhängt. In der Tat kann man zeigen, dass Δ stets ein Polynom in den Koeffizienten $\lambda_0, \ldots, \lambda_{n-1}$ von f und damit insbesondere eine rationale Zahl ist (siehe Aufgabe 6.13 (a)). Für $n = 2$ ist z. B.

$$t^2 + \lambda_1 t + \lambda_0 = (t - a_1)(t - a_2),$$

also

$$\lambda_1 = -a_1 - a_2 \quad \text{und} \quad \lambda_0 = a_1 a_2,$$

und damit

$$\Delta = (a_1 - a_2)^2 = a_1^2 - 2a_1a_2 + a_2^2 = \lambda_1^2 - 4\lambda_0.$$

Dies ist natürlich genau der aus der Lösungsformel für quadratische Gleichungen bekannte Term, der entscheidet, ob es eine oder zwei Lösungen gibt bzw. ob diese Lösungen reell oder komplex sind.

Mit ähnlichen Methoden wie im Beweis von Satz 5.13 kann man nun zeigen, dass die Galoisgruppe $\mathrm{Gal}(f)$ eines irreduziblen Polynoms vom Grad n genau dann eine Untergruppe der alternierenden Gruppe A_n ist, wenn seine Diskriminante Δ ein Quadrat in $\mathbb{Q}$ ist — in Aufgabe 6.13 (a) werden wir zumindest eine Richtung dieser Äquivalenz zeigen.

Bemerkung 5.16. Wie man aus Satz 5.13 schon erahnen kann, ist es im Allgemeinen nicht einfach, die Galoisgruppe eines gegebenen Polynoms zu berechnen — in der Tat wird man für die konkrete Berechnung von Galoisgruppen in der Regel Computeralgebrasysteme einsetzen. Die umgekehrte Frage, wie man zu einer gegebenen Untergruppe $G \leq S_n$ ein Beispiel eines rationalen Polynoms f vom Grad n mit Galoisgruppe G finden kann, und ob ein solches überhaupt für alle G existiert,

ist sogar ein bis heute noch ungelöstes Problem! Es wird im Rahmen der sogenannten *inversen Galoistheorie* untersucht.

Zum Abschluss dieses Kapitels wollen wir nun noch ein paar wichtige Eigenschaften galoisscher Körpererweiterungen angeben.

Lemma 5.17 (Eigenschaften galoisscher Körpererweiterungen)**.**

(a) *Jede Körpererweiterung vom Grad* 2 *ist galoissch.*

(b) *Sind* $K \leq Z \leq L$ *Körper und ist* L/K *galoissch, so auch* L/Z*.*

Beweis.

(a) Nach dem Satz 4.28 vom primitiven Element ist $L = K(a)$ für ein a mit $[a : K] = 2$. Ist f das Minimalpolynom von a, so spaltet f in L natürlich die Nullstelle a ab und zerfällt damit bereits in Linearfaktoren, da es ja ein quadratisches Polynom ist. Also ist L der Zerfällungskörper von f. Damit ist L/K nach Satz 5.8 galoissch.

(b) Ist L/K galoissch, so ist L nach Satz 5.8 der Zerfällungskörper eines Polynoms über K. Dann ist L aber natürlich auch der Zerfällungskörper desselben Polynoms über Z. Wiederum nach Satz 5.8 ist damit auch L/Z galoissch. □

Beachte, dass sich die Eigenschaft „galoissch“ bei verketten Körpererweiterungen also zunächst etwas ungewohnt verhält: sind $K \leq Z \leq L$ Körper und ist die große Körpererweiterung L/K galoissch, so ist es nach Lemma 5.17 (b) auch die „obere“ L/Z. Unter welchen Bedingungen dann auch die „untere“ Erweiterung Z/K galoissch ist, werden wir in Satz 6.14 noch sehen. Definitiv nicht gilt jedoch die Eigenschaft, die man vielleicht als Erstes vermutet hätte, nämlich die Transitivität:

Bemerkung 5.18 (Nicht-Transitivität der Eigenschaft „galoissch“)**.** Sind $K \leq Z \leq L$ Körper und Z/K und L/Z galoissch, so muss deswegen nicht notwendig auch L/K galoissch sein. Dies zeigt das Beispiel $\mathbb{Q} \leq \mathbb{Q}(\sqrt{2}) \leq \mathbb{Q}(\sqrt[4]{2})$: nach Beispiel 3.10 ist $[\mathbb{Q}(\sqrt{2}) : \mathbb{Q}] = 2$ und $[\mathbb{Q}(\sqrt[4]{2}) : \mathbb{Q}] = 4$, mit der Gradformel aus Satz 2.14 also $[\mathbb{Q}(\sqrt[4]{2}) : \mathbb{Q}(\sqrt{2})] = 2$. Also sind zunächst einmal die beiden Körpererweiterungen $\mathbb{Q}(\sqrt{2})/\mathbb{Q}$ und $\mathbb{Q}(\sqrt[4]{2})/\mathbb{Q}(\sqrt{2})$ nach Lemma 5.17 (a) galoissch. Aber die zusammengesetzte Körpererweiterung $\mathbb{Q}(\sqrt[4]{2})/\mathbb{Q}$ ist nach Satz 5.8 nicht galoissch, denn das Polynom $t^4 - 2 \in \mathbb{Q}[t]$ hat in $\mathbb{Q}(\sqrt[4]{2})$ zwar die Nullstelle $\sqrt[4]{2}$, zerfällt dort aber nicht in Linearfaktoren, da z. B. die komplexe Nullstelle $\sqrt[4]{2}\,i$ nicht im reellen Körper $\mathbb{Q}(\sqrt[4]{2})$ liegt.

Aufgabe 5.19.

(a) Zeige, dass die Körpererweiterung $\mathbb{Q}(\sqrt{2}, \sqrt{3})/\mathbb{Q}$ galoissch mit Galoisgruppe $\mathbb{Z}_2 \times \mathbb{Z}_2$ ist.

(b) Gib ein Beispiel für einen Erweiterungskörper L von $\mathbb{Q}$ an, so dass $L/\mathbb{Q}$ galoissch mit Galoisgruppe $\mathbb{Z}_4$ ist.

(c) Gib ein Beispiel für einen Erweiterungskörper L von $\mathbb{Q}$ an, so dass $L/\mathbb{Q}$ Galoisgruppe $\mathbb{Z}_2 \times \mathbb{Z}_2$ hat, aber *nicht* galoissch ist.

Aufgabe 5.20. Es seien $n \in \mathbb{N}_{>0}$ und $K \leq \mathbb{C}$ ein Körper mit $e^{\frac{2\pi i}{n}} \in K$.

Man zeige: Ist L/K eine einfache n-Radikalerweiterung, so ist L/K galoissch, und die Galoisgruppe $\mathrm{Gal}(L/K)$ ist isomorph zu einer Untergruppe von $\mathbb{Z}_n$.

Aufgabe 5.21 (Translationssatz)**.** Es seien $K \leq L \leq Z$ Körper und $a \in Z$. Man zeige:

Ist die Körpererweiterung $K(a)/K$ galoissch, so ist auch $L(a)/L$ galoissch, und es gilt

$$\mathrm{Gal}(L(a)/L) \cong \mathrm{Gal}(K(a)/(K(a) \cap L)) \leq \mathrm{Gal}(K(a)/K).$$

(Hinweis: Es ist nützlich zu zeigen, dass a über L und $K(a) \cap L$ dasselbe Minimalpolynom hat.)

09

6. Der Hauptsatz der Galoistheorie

Im letzten Kapitel haben wir jeder Körpererweiterung L/K eine Gruppe zugeordnet, nämlich die Galoisgruppe $\mathrm{Gal}(L/K)$ aller K-Automorphismen von L. Wir wollen nun das eigentliche Hauptresultat der Galoistheorie beweisen, das wir bereits am Anfang von Kapitel 5 angekündigt hatten: dass im Fall einer galoisschen Körpererweiterung die Zwischenkörper von L/K bijektiv den Untergruppen von $\mathrm{Gal}(L/K)$ entsprechen. Auch in diesem Kapitel seien dazu noch alle Körpererweiterungen endlich und von Charakteristik 0.

Eine Richtung dieser Bijektion können wir mit unseren bisherigen Methoden schon konstruieren, nämlich die Zuordnung einer Untergruppe von $\mathrm{Gal}(L/K)$ zu einem Zwischenkörper von L/K.

Notation 6.1 (Zwischenkörper $\mapsto$ Untergruppe)**.** Es sei L/K eine Körpererweiterung. Wir bezeichnen mit $\mathscr{Z}$ die Menge der Zwischenkörper von L/K und mit $\mathscr{U}$ die Menge der Untergruppen von $\mathrm{Gal}(L/K)$. Ist $Z \in \mathscr{Z}$ ein Zwischenkörper und $\sigma \in \mathrm{Gal}(L/Z)$ ein Automorphismus von L, der Z fest lässt, so lässt σ natürlich auch den kleineren Körper K fest und liegt damit auch in $\mathrm{Gal}(L/K)$. Also ist $\mathrm{Gal}(L/Z)$ eine Untergruppe von $\mathrm{Gal}(L/K)$, und wir erhalten so eine Abbildung

$$\begin{aligned} \Psi: \quad \mathscr{Z} &\longrightarrow \mathscr{U} \\ Z &\longmapsto \mathrm{Gal}(L/Z). \end{aligned}$$

Für die umgekehrte Richtung, also um einer Untergruppe einen Zwischenkörper zuzuordnen, benötigen wir die folgende Konstruktion.

Definition 6.2 (Fixkörper)**.** Es seien L ein Körper und $G \leq \mathrm{Aut}(L)$ eine Untergruppe der Automorphismengruppe von L. Dann heißt

$$L^G := \{a \in L : \ \sigma(a) = a \text{ für alle } \sigma \in G\}$$

der **Fixkörper** von G in L (man prüft sofort nach, dass dies in der Tat ein Unterkörper von L ist).

Beispiel 6.3. Es seien $L = \mathbb{C}$ und $G = \{\mathrm{id}_{\mathbb{C}}, \sigma\}$, wobei $\sigma : \mathbb{C} \to \mathbb{C}$, $z \mapsto \bar{z}$ die komplexe Konjugation ist. Dann ist G offensichtlich eine Gruppe von Automorphismen von $\mathbb{C}$. Der zugehörige Fixkörper besteht aus den Elementen von $\mathbb{C}$, die von allen Automorphismen in G festgehalten werden, also

$$\begin{aligned} L^G &= \{z \in \mathbb{C} : \ \mathrm{id}(z) = z \text{ und } \sigma(z) = z\} \\ &= \{z \in \mathbb{C} : \ \bar{z} = z\} \\ &= \mathbb{R}. \end{aligned}$$

Notation 6.4 (Untergruppe $\mapsto$ Zwischenkörper)**.** Mit den Bezeichnungen aus Notation 6.1 sei nun $G \in \mathscr{U}$ eine Untergruppe von $\mathrm{Gal}(L/K)$. Da dann alle Elemente von G Automorphismen von L sind, die K fest lassen, enthält der Fixkörper L^G natürlich K und ist damit ein Zwischenkörper von L/K. Wir haben also eine Abbildung

$$\begin{aligned} \Phi: \quad \mathscr{U} &\longrightarrow \mathscr{Z} \\ G &\longmapsto L^G. \end{aligned}$$

Beispiel 6.5. Für die Körpererweiterung $L/K = \mathbb{C}/\mathbb{R}$ ist $G := \mathrm{Gal}(\mathbb{C}/\mathbb{R}) = \{\mathrm{id}, \sigma\}$ nach Beispiel 5.3 (a), wobei $\sigma : \mathbb{C} \to \mathbb{C}$, $z \mapsto \bar{z}$ wie in Beispiel 6.3 die komplexe Konjugationsabbildung ist. Da $\mathbb{C}/\mathbb{R}$ als Körpererweiterung vom Grad 2 nach der Gradformel aus Satz 2.17 keine echten Zwischenkörper haben kann, ist die Menge der Zwischenkörper dieser Körpererweiterung gleich $\mathscr{Z} = \{\mathbb{R}, \mathbb{C}\}$. Andererseits ist die Galoisgruppe $\mathrm{Gal}(\mathbb{C}/\mathbb{R})$ isomorph zu $\mathbb{Z}_2$ und hat damit nur die trivialen Untergruppen, d. h. die Menge der Untergruppen von $\mathrm{Gal}(\mathbb{C}/\mathbb{R})$ ist $\mathscr{U} = \{G, \{\mathrm{id}\}\}$. Die Abbildungen Ψ

und Φ aus den Notationen 6.1 und 6.4 sind nun

$$\begin{aligned} \Psi: \quad \mathscr{Z} &\longrightarrow \mathscr{U} \\ \mathbb{R} &\longmapsto \mathrm{Gal}(\mathbb{C}/\mathbb{R}) = G \\ \mathbb{C} &\longmapsto \mathrm{Gal}(\mathbb{C}/\mathbb{C}) = \{\mathrm{id}\} \end{aligned}$$

und nach Beispiel 6.3

$$\begin{aligned} \Phi: \quad \mathscr{U} &\longrightarrow \mathscr{Z} \\ G &\longmapsto \mathbb{C}^G = \mathbb{R} \\ \{\mathrm{id}\} &\longmapsto \mathbb{C}^{\{\mathrm{id}\}} = \mathbb{C}. \end{aligned}$$

Die Abbildungen Ψ und Φ sind hier also invers zueinander. Unser Ziel ist es zu zeigen, dass dies für jede galoissche Körpererweiterung der Fall ist. Die Hauptarbeit hierfür steckt in dem folgenden vorbereitenden Lemma.

Lemma 6.6 (Lemma von Artin). *Es seien L ein Körper und $G \leq \mathrm{Aut}(L)$ eine endliche Gruppe von Automorphismen von L. Ist dann $K = L^G$ der Fixkörper von G, so gilt*

$$[L:K] \leq |G|.$$

(In der Tat werden wir in Bemerkung 6.8 noch sehen, dass sogar immer die Gleichheit gilt.)

Beweis. Es sei $G = \{\sigma_1, \dots, \sigma_n\}$ mit $n = |G|$. Nach Definition des Grades einer Körpererweiterung müssen wir zeigen, dass die Dimension von L als K-Vektorraum höchstens gleich n ist, d. h. dass je $n+1$ Elemente $a_1, \dots, a_{n+1} \in L$ linear abhängig über K sind.

Dazu betrachten wir für solche $a_1, \dots, a_{n+1}$ das lineare Gleichungssystem

$$\sum_{i=1}^{n+1} \sigma_j(a_i) \cdot x_i = 0 \qquad \text{für alle } j = 1, \dots, n \tag{1}$$

in den Variablen $x_1, \dots, x_{n+1} \in L$. Da dies ein System mit n Gleichungen in $n+1$ Variablen ist, besitzt es eine nicht-triviale Lösung. Wir wählen nun eine solche nicht-triviale Lösung, die mit maximal vielen Nullen beginnt und so normiert ist, dass der nächste Eintrag gleich 1 ist, d. h. so dass

$$x_1 = \dots = x_s = 0 \quad \text{und} \quad x_{s+1} = 1 \tag{2}$$

für ein $s \geq 0$ gilt und keine nicht-triviale Lösung mit $x_1 = \dots = x_{s+1} = 0$ existiert.

Wir behaupten zunächst, dass für jedes $\sigma \in G$ dann auch $(\sigma(x_1), \dots, \sigma(x_{n+1}))$ eine Lösung des Gleichungssystems (1) ist. In der Tat rechnet man dies leicht nach: für alle $j = 1, \dots, n$ ist

$$\sum_{i=1}^{n+1} \sigma_j(a_i) \cdot \sigma(x_i) = \sigma\left(\sum_{i=1}^{n+1} (\sigma^{-1} \circ \sigma_j)(a_i) \cdot x_i \right) = \sigma(0) = 0,$$

da ja $\sigma^{-1} \circ \sigma_j \in G$ gilt und der Ausdruck in der großen Klammer damit genau eine der linken Seiten des Gleichungssystems (1) ist. Weil σ als Körperhomomorphismus die Elemente 0 und 1 festhält, gilt nach (2) auch für diese Lösung

$$\sigma(x_1) = \dots = \sigma(x_s) = 0 \quad \text{und} \quad \sigma(x_{s+1}) = 1. \tag{3}$$

Nun bilden die Lösungen des Gleichungssystems (1) aber natürlich einen Vektorraum. Damit ist auch die Differenz $(y_1, \dots, y_{n+1}) := (x_1 - \sigma(x_1), \dots, x_{n+1} - \sigma(x_{n+1}))$ unserer beiden gefundenen Lösungen eine Lösung von (1) — und für diese gilt nach (2) und (3) offensichtlich

$$y_1 = \dots = y_{s+1} = 0.$$

Wegen der Maximalität von s unter den nicht-trivialen Lösungen von (1) bedeutet dies, dass $(y_1, \dots, y_{n+1}) = (0, \dots, 0)$ die triviale Lösung sein muss. Also gilt $y_i = 0$, d. h. $\sigma(x_i) = x_i$ für alle $i = 1, \dots, n+1$.

Da dies für alle $\sigma \in G$ gilt, liegen alle x_i im Fixkörper $K = L^G$ von G. Die Gleichung

$$\sum_{i=1}^{n+1} a_i \cdot x_i = 0,$$

die (für $\sigma_j = \mathrm{id}$) ja im Gleichungssystem (1) enthalten ist, besagt damit gerade, dass die $a_1, \ldots, a_{n+1}$ linear abhängig über K sind. Damit ist die Dimension von L als K-Vektorraum höchstens gleich n. □

Mit dem Lemma von Artin können wir neben den Bedingungen aus Satz 5.8 nun noch eine weitere angeben, die äquivalent dazu ist, dass eine Körpererweiterung L/K galoissch ist — nämlich dass K ein Fixkörper (von irgendeiner Gruppe) in L ist.

Folgerung 6.7 („galoissch = Fixkörper“)**.** *Für eine Körpererweiterung L/K gilt*

$$L/K \text{ galoissch} \quad \Longleftrightarrow \quad K = L^G \text{ für ein } G \leq \mathrm{Aut}(L).$$

In diesem Fall ist dann $\mathrm{Gal}(L/K) = G$.

Beweis.

„⇐“ Es sei $K = L^G$ für ein $G \leq \mathrm{Aut}(L)$. Beachte, dass dann $G \leq \mathrm{Gal}(L/K)$ gelten muss, da nach der Definition des Fixkörpers jedes Element von G den Körper K fest lässt. Andererseits gilt für die Ordnungen der Gruppen G und $\mathrm{Gal}(L/K)$ aber auch

$$\begin{aligned} |\mathrm{Gal}(L/K)| &\leq [L:K] && \text{(Lemma 5.2 (c))} \\ &\leq |G| && \text{(Lemma 6.6 von Artin)} \end{aligned}$$

(beachte, dass G als Untergruppe von $\mathrm{Gal}(L/K)$ endlich und das Lemma von Artin daher anwendbar ist). Zusammen ist dies natürlich nur möglich, wenn $G = \mathrm{Gal}(L/K)$ und $|\mathrm{Gal}(L/K)| = [L:K]$ (und auch $[L:K] = |G|$) gilt. Also ist L/K galoissch, und wir haben auch bereits die Zusatzbehauptung in der Folgerung gezeigt.

„⇒“ Wir betrachten den Fixkörper $L^{\mathrm{Gal}(L/K)}$, der wie in Notation 6.4 erläutert ein Zwischenkörper von L/K ist. Nach dem bereits bewiesenen Teil „⇐“ ist die Körpererweiterung $L/L^{\mathrm{Gal}(L/K)}$ galoissch mit Galoisgruppe $\mathrm{Gal}(L/K)$. Damit folgt

$$\begin{aligned} [L : L^{\mathrm{Gal}(L/K)}] &= |\mathrm{Gal}(L/K)| && (L/L^{\mathrm{Gal}(L/K)} \text{ galoissch} \\ & && \text{mit Galoisgruppe } \mathrm{Gal}(L/K)) \\ &= [L:K] && (L/K \text{ galoissch nach Voraussetzung}) \\ &= [L : L^{\mathrm{Gal}(L/K)}] \cdot [L^{\mathrm{Gal}(L/K)} : K] && \text{(Gradformel aus Satz 2.17).} \end{aligned}$$

Also ist $[L^{\mathrm{Gal}(L/K)} : K] = 1$ und damit $K = L^{\mathrm{Gal}(L/K)}$ wie behauptet ein Fixkörper. □

Bemerkung 6.8 (Gleichheit im Lemma von Artin)**.** Ist L ein Körper und $K = L^G$ der Fixkörper einer endlichen Gruppe $G \leq \mathrm{Aut}(L)$, so haben wir im Beweis des Teils „⇐“ von Folgerung 6.7 gesehen, dass dann $[L:K] = |G|$ gilt. Im Lemma 6.6 von Artin gilt also sogar immer die Gleichheit. Wir haben dort nur deswegen nur die schwächere Aussage $[L:K] \leq |G|$ gezeigt, um den Beweis kürzer und übersichtlicher zu halten.

Wir haben nun alle Vorbereitungen getroffen, um die bereits angekündigte Korrespondenz zwischen Zwischenkörpern einer galoisschen Körpererweiterung L/K und Untergruppen ihrer Galoisgruppe $\mathrm{Gal}(L/K)$ zu beweisen.

Folgerung 6.9 (**Hauptsatz der Galoistheorie**)**.** *Es sei L/K eine galoissche Körpererweiterung. Wie in den Notationen 6.1 und 6.4 bezeichne $\mathscr{Z}$ die Menge der Zwischenkörper von L/K und $\mathscr{U}$ die Menge der Untergruppen von* $\mathrm{Gal}(L/K)$.

(a) *Die Abbildungen* Ψ *und* Φ *aus den Notationen 6.1 und 6.4 liefern eine Bijektion*

$$\begin{array}{rcll} & \mathscr{Z} & \overset{1:1}{\longleftrightarrow} & \mathscr{U} \\ & Z & \longmapsto & \mathrm{Gal}(L/Z) \quad = \Psi(Z) \\ \Phi(G) = & L^G & \longmapsto & G. \end{array}$$

(b) *Die Korrespondenz aus (a) dreht Inklusionen um:*

$$\begin{aligned} &\text{für } Z_1, Z_2 \in \mathscr{Z} \text{ mit } Z_1 \leq Z_2 \text{ gilt } \Psi(Z_2) \leq \Psi(Z_1); \\ &\text{für } G_1, G_2 \in \mathscr{U} \text{ mit } G_1 \leq G_2 \text{ gilt } \Phi(G_2) \leq \Phi(G_1). \end{aligned}$$

(c) *In der Korrespondenz aus (a) entsprechen die Grade der Zwischenkörper den Ordnungen der Untergruppen: sind* $Z \in \mathscr{Z}$ *und* $G \in \mathscr{U}$ *mit* $G = \Psi(Z)$ *(also* $Z = \Phi(G)$*), so gilt*

$$[L : Z] = |G|.$$

Beweis.

(a) Wir müssen zeigen, dass $\Psi \circ \Phi = \mathrm{id}$ und $\Phi \circ \Psi = \mathrm{id}$.

Für $\Psi \circ \Phi = \mathrm{id}$ sei $G \in \mathscr{U}$, also $G \leq \mathrm{Gal}(L/K)$. Nach dem Zusatz in Folgerung 6.7 ist dann $\mathrm{Gal}(L/Z) = G$ für den Fixkörper $Z = L^G$. Damit gilt

$$G \overset{\Phi}{\longmapsto} L^G = Z \overset{\Psi}{\longmapsto} \mathrm{Gal}(L/Z) = G.$$

Also ist $\Psi \circ \Phi = \mathrm{id}$. Beachte, dass wir für diesen Teil *nicht* benötigt haben, dass die Körpererweiterung L/K galoissch ist!

Für $\Phi \circ \Psi = \mathrm{id}$ sei $Z \in \mathscr{Z}$, also $K \leq Z \leq L$. Nach Lemma 5.17 (b) ist mit L/K auch L/Z galoissch. Folgerung 6.7 angewendet auf L/Z ergibt also $Z = L^G$ mit $G = \mathrm{Gal}(L/Z)$. Damit haben wir

$$Z \overset{\Psi}{\longmapsto} \mathrm{Gal}(L/Z) = G \overset{\Phi}{\longmapsto} L^G = Z,$$

und somit auch $\Phi \circ \Psi = \mathrm{id}$.

(b) Beide Aussagen sind unmittelbar aus den Definitionen klar:

- Ist $Z_1 \leq Z_2$, so erfüllt jeder Isomorphismus $\sigma : L \to L$ mit $\sigma|_{Z_2} = \mathrm{id}$ natürlich auch $\sigma|_{Z_1} = \mathrm{id}$. Damit gilt dann $\mathrm{Gal}(L/Z_2) \leq \mathrm{Gal}(L/Z_1)$.
- Ist $G_1 \leq G_2$, so wird jedes Element von L, das von den Automorphismen in G_2 fest gelassen wird, natürlich insbesondere auch von denen in G_1 fest gelassen. Also gilt dann $L^{G_2} \leq L^{G_1}$.

(c) Wegen $Z = L^G$ ist dies exakt die Aussage aus Bemerkung 6.8. □

10

Beispiel 6.10. Es sei L/K die Körpererweiterung des Zerfällungskörpers von $f = t^3 - 2$ über $\mathbb{Q}$ aus Beispiel 5.12, also $K = \mathbb{Q}$ und

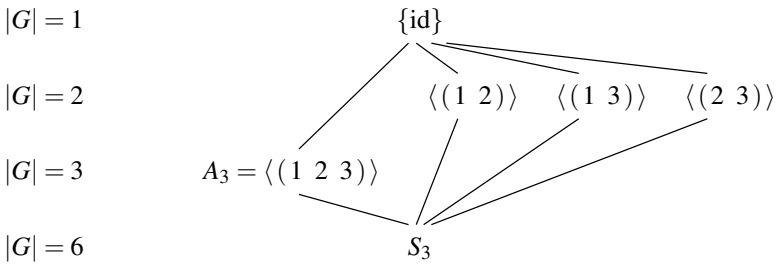
$$L = \mathbb{Q}(a_1, a_2, a_3) = \mathbb{Q}\left(\sqrt[3]{2}, e^{\frac{2\pi i}{3}}\right),$$

wobei

$$a_1 = \sqrt[3]{2}, \quad a_2 = \sqrt[3]{2}\, e^{\frac{2\pi i}{3}}, \quad a_3 = \sqrt[3]{2}\, e^{\frac{4\pi i}{3}}$$

die Nullstellen von f in $\mathbb{C}$ sind. Wir hatten in Beispiel 5.12 bereits gesehen, dass L/K galoissch mit Galoisgruppe $\mathrm{Gal}(L/K) = S_3$ ist, wobei die Elemente von S_3 genau den möglichen Permutationen der drei Nullstellen a_1, a_2, a_3 entsprechen. Auf diese Körpererweiterung wollen wir nun den Hauptsatz der Galoistheorie aus Folgerung 6.9 anwenden.

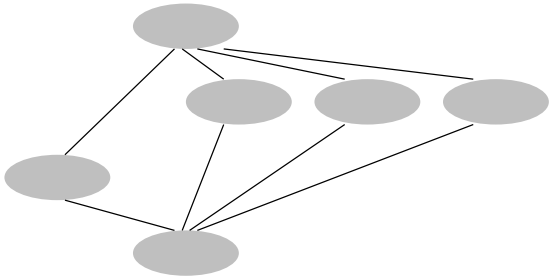
Üblicherweise beginnt man dabei mit der Menge $\mathscr{U}$ der Untergruppen von $\mathrm{Gal}(L/K)$, da man über diese in der Regel zunächst mehr weiß als über die Menge $\mathscr{Z}$ der Zwischenkörper von L/K. In unserem Fall hier sind z. B. alle Untergruppen von $\mathrm{Gal}(L/K) = S_3$ aus den „Algebraischen Strukturen“ bekannt [G, Beispiel 5.16]; sie sind im folgenden Diagramm dargestellt.



Man nennt eine solche Darstellung ein *Untergruppendiagramm* von $\mathrm{Gal}(L/K) = S_3$. Wir haben die Untergruppen dabei von oben nach unten nach aufsteigender Ordnung sortiert; zwei Untergruppen sind dabei durch Linien miteinander verbunden, wenn die oben stehende eine Untergruppe der unten stehenden ist. In unserem einfachen Fall ist dabei keine echte Untergruppe in einer anderen enthalten, so dass alle Linien entweder im obersten Punkt $\{\mathrm{id}\}$ beginnen oder im untersten Punkt S_3 enden — dies kann in einem komplizierteren Beispiel aber natürlich anders sein.

Die Korrespondenz zwischen diesen Untergruppen und den Zwischenkörpern von L/K aus dem Hauptsatz der Galoistheorie in Folgerung 6.9 besagt nun zunächst, dass die Zwischenkörper von L/K in exakt das gleiche Schema passen, dass das *Zwischenkörperdiagramm* also wie im folgenden Bild aussehen muss.

$$[L:Z] = 1 \ \Rightarrow\ [Z:K] = 6$$
$$[L:Z] = 2 \ \Rightarrow\ [Z:K] = 3$$
$$[L:Z] = 3 \ \Rightarrow\ [Z:K] = 2$$
$$[L:Z] = 6 \ \Rightarrow\ [Z:K] = 1$$



Dabei bedeuten die Linien diesmal, dass der unten stehende Körper ein Teilkörper des oben stehenden ist. Teil (a) des Hauptsatzes besagt dabei zunächst nur, dass diese Zwischenkörper in 1:1-Beziehung zu den Untergruppen aus dem obigen Diagramm stehen. Teil (b) zeigt, dass die Linien zwischen den einzelnen Positionen in beiden Diagrammen gleich sind, und Teil (c) besagt, dass die Zeilenstruktur in beiden Diagrammen übereinstimmt, wobei die Ordnung $|G|$ der Untergruppe nun als Grad $[L:Z]$ von L über dem zugehörigen Zwischenkörper interpretiert werden muss. Die jeweiligen Grade $[Z:K]$ ergeben sich daraus dann natürlich wegen $[L:K] = 6$ mit der Gradformel aus Satz 2.17.

Welche Zwischenkörper stehen nun an den einzelnen Stellen dieses Diagramms? Klar ist natürlich, dass ganz oben der Zwischenkörper mit $[L:Z] = 1$, also $Z = L = \mathbb{Q}\big(\sqrt[3]{2}, e^{\frac{2\pi i}{3}}\big)$ steht, und ganz unten der mit $[Z:K] = 1$, also $Z = K = \mathbb{Q}$. Um den ersten Eintrag in der zweiten Zeile zu bestimmen, müssen wir gemäß der Abbildung Φ in Folgerung 6.9 (a) den Fixkörper $L^{\langle(1\ 2)\rangle}$ bestimmen. Nun entspricht das Element $(1\ 2)$ in S_3 aber gerade dem Automorphismus $\sigma : L \to L$ mit $\sigma(a_1) = a_2$, $\sigma(a_2) = a_1$ und $\sigma(a_3) = a_3$. Also ist a_3 und damit auch $\mathbb{Q}(a_3)$ offensichtlich im Fixkörper $L^{\langle(1\ 2)\rangle}$ enthalten. Da dieser gesuchte Fixkörper gemäß unserem Diagramm Grad 3 über $\mathbb{Q}$ hat und der Grad von $\mathbb{Q}(a_3)$ über $\mathbb{Q}$ bereits 3 ist, gilt sogar schon $L^{\langle(1\ 2)\rangle} = \mathbb{Q}(a_3)$: dies ist der gesuchte Eintrag im Zwischenkörperdiagramm. Auf die gleiche Art sieht man, dass die beiden anderen Einträge dieser Zeile $\mathbb{Q}(a_2)$ und $\mathbb{Q}(a_1)$ sind.

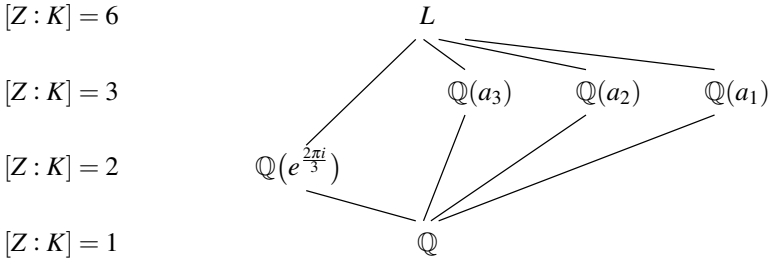
Für den Eintrag in der dritten Zeile müssen wir analog den Fixkörper $L^{\langle(1\ 2\ 3)\rangle}$ berechnen. Hier entspricht das Element $(1\ 2\ 3)$ von S_3 dem Automorphismus $\sigma : L \to L$ mit $\sigma(a_1) = a_2$, $\sigma(a_2) = a_3$ und $\sigma(a_3) = a_1$. Keine der drei Nullstellen von f liegt also im gesuchten Fixkörper. Allerdings ist

diesmal

$$\sigma\left(e^{\frac{2\pi i}{3}}\right) = \sigma\left(\frac{a_2}{a_1}\right) = \frac{\sigma(a_2)}{\sigma(a_1)} = \frac{a_3}{a_2} = e^{\frac{2\pi i}{3}}$$

und damit $\mathbb{Q}\left(e^{\frac{2\pi i}{3}}\right) \leq L^{\langle (1\ 2\ 3)\rangle}$. Wie oben ist nun aber $[\mathbb{Q}\left(e^{\frac{2\pi i}{3}}\right) : \mathbb{Q}] = 2 = [L^{\langle (1\ 2\ 3)\rangle} : \mathbb{Q}]$ und damit bereits $L^{\langle (1\ 2\ 3)\rangle} = \mathbb{Q}\left(e^{\frac{2\pi i}{3}}\right)$ — dies ist also der noch fehlende Eintrag im Diagramm.

Insgesamt haben wir jetzt also das folgende Zwischenkörperdiagramm erhalten.



Natürlich ist die Existenz aller dieser Zwischenkörper in diesem einfachen Fall schon aus der ursprünglichen Definition

$$L = \mathbb{Q}(a_1, a_2, a_3) = \mathbb{Q}\left(\sqrt[3]{2}, e^{\frac{2\pi i}{3}}\right)$$

offensichtlich gewesen. Der Hauptsatz der Galoistheorie besagt allerdings nun, dass dies auch wirklich die einzigen Zwischenkörper der betrachteten Körpererweiterung sind.

In komplizierteren Fällen sind die Zwischenkörper natürlich meistens nicht so einfach zu sehen wie in dem obigen Beispiel. Wir wollen in der folgenden Aufgabe daher ein Verfahren entwickeln, mit dem man den zu einer Untergruppe gehörenden Fixkörper auf einfache Weise explizit berechnen kann.

Aufgabe 6.11 (Berechnung von Fixkörpern)**.** Es sei L/K eine galoissche Körpererweiterung. Nach dem Satz 4.28 vom primitiven Element können wir sie als einfache Körpererweiterung schreiben, also $L = K(a)$ für ein $a \in L$.

Für eine Untergruppe $G \leq \mathrm{Gal}(L/K)$ setzen wir nun

$$f := \prod_{\sigma \in G} (t - \sigma(a)) \quad \in L[t].$$

Ferner seien $\lambda_0, \ldots, \lambda_n \in L$ die Koeffizienten von f, also $f = \sum_{i=0}^{n} \lambda_i t^i$. Ist dann $Z = L^G$ der zu G gehörige Zwischenkörper von L/K in der Galois-Korrespondenz, so zeige man:

(a) $f \in Z[t]$.

(b) f ist das Minimalpolynom von a über Z und über $K(\lambda_0, \ldots, \lambda_n)$.

(c) $Z = K(\lambda_0, \ldots, \lambda_n)$.

Aufgabe 6.12. Bestimme für die folgenden Körpererweiterungen L/K das Untergruppendiagramm von $\mathrm{Gal}(L/K)$ und das Zwischenkörperdiagramm von L/K:

(a) $\mathbb{Q}(\sqrt{2}, \sqrt{3})/\mathbb{Q}$;

(b) $\mathbb{Q}(e^{\frac{2\pi i}{7}})/\mathbb{Q}$.

Aufgabe 6.13. Zu einem Polynom $f \in K[t]$ über einem Körper K sei $L = K(a_1, \ldots, a_n)$ der Zerfällungskörper, wobei $a_1, \ldots, a_n$ die (verschiedenen) Nullstellen von f in L sind. Bekanntlich ist dann $\mathrm{Gal}(L/K) \leq S_n$. Wir setzen

$$z := \prod_{i<j} (a_i - a_j).$$

Man zeige:

(a) Die sogenannte *Diskriminante* z^2 (siehe auch Bemerkung 5.15) liegt in K.

(b) Ist $\mathrm{Gal}(L/K) \leq A_n$, dann ist sogar $z \in K$.

Zum Abschluss dieses Kapitels wollen wir noch eine zusätzliche Aussage über die Galois-Korrespondenz beweisen, die in der Literatur häufig noch als Teil des Hauptsatzes angesehen wird. Ist Z ein Zwischenkörper einer galoisschen Körpererweiterung L/K, so haben wir in Lemma 5.17 (b) gesehen, dass dann auch die „obere“ Erweiterung L/Z galoissch ist. Man kann sich nun natürlich fragen, unter welchen Bedingungen auch die „untere“ Erweiterung Z/K galoissch ist. Auf der anderen Seite kann man für eine Untergruppe $G \leq \mathrm{Gal}(L/K)$ untersuchen, ob G vielleicht sogar ein Normalteiler in $\mathrm{Gal}(L/K)$ ist. Wir wollen nun zeigen, dass sich diese beiden Eigenschaften in der Galois-Korrespondenz genau entsprechen (die Eigenschaft (c) im folgenden Satz, die ebenfalls dazu äquivalent ist, ist eine eher technische Bedingung, die wir hier nur aufführen, da sie im Beweis benötigt wird).

Satz 6.14 (Ergänzung zum Hauptsatz der Galoistheorie)**.** *Es sei L/K eine galoissche Körpererweiterung. Ferner sei Z ein Zwischenkörper von L/K, der in der Galois-Korrespondenz aus Folgerung 6.9 der Untergruppe $G \leq \mathrm{Gal}(L/K)$ entspricht, also $Z = L^G$ und $G = \mathrm{Gal}(L/Z)$. Dann sind äquivalent:*

(a) *Z/K ist galoissch.*

(b) *$G \trianglelefteq \mathrm{Gal}(L/K)$ ist ein Normalteiler.*

(c) *Für alle $\sigma \in \mathrm{Gal}(L/K)$ gilt $\sigma(Z) \subset Z$ (und damit nach Aufgabe 5.5 sogar $\sigma(Z) = Z$).*

In diesem Fall ist dann $\mathrm{Gal}(Z/K) \cong \mathrm{Gal}(L/K)/G$.

Beweis.

(a) $\Rightarrow$ (c): Da Z/K galoissch ist, ist Z nach Satz 5.8 der Zerfällungskörper eines Polynoms $f \in K[t]$, also $Z = K(a_1, \ldots, a_n)$ mit den Nullstellen $a_1, \ldots, a_n$ von f in Z. Ist nun $\sigma \in \mathrm{Gal}(L/K)$, so bildet σ die Menge $\{a_1, \ldots, a_n\}$ dieser Nullstellen nach Lemma 5.2 (a) auf sich ab. Also folgt $\sigma(a_i) \in K(a_1, \ldots, a_n) = Z$ für alle $i = 1, \ldots, n$ und damit auch $\sigma(Z) \subset Z$.

(b) $\Rightarrow$ (c): Es seien $\sigma \in \mathrm{Gal}(L/K)$ und $\tau \in G = \mathrm{Gal}(L/Z)$. Dann gilt für alle $a \in \sigma(Z)$

$$(\sigma \circ \tau \circ \sigma^{-1})(a) = (\sigma \circ \tau)(\underbrace{\sigma^{-1}(a)}_{\in Z}) = \sigma(\sigma^{-1}(a)) = a,$$

da τ das Element $\sigma^{-1}(a) \in Z$ fest lässt. Es ist dann also $\sigma \circ \tau \circ \sigma^{-1} \in \mathrm{Gal}(L/\sigma(Z))$. Weil G nach Voraussetzung ein Normalteiler in $\mathrm{Gal}(L/K)$ ist, folgt also für alle $\sigma \in \mathrm{Gal}(L/K)$

$$\mathrm{Gal}(L/Z) = \sigma \circ G \circ \sigma^{-1} \subset \mathrm{Gal}(L/\sigma(Z)),$$

d. h. die nach der Galois-Korrespondenz zum Zwischenkörper Z gehörige Untergruppe $\mathrm{Gal}(L/Z)$ ist in der zum Zwischenkörper $\sigma(Z)$ gehörigen Untergruppe $\mathrm{Gal}(L/\sigma(Z))$ enthalten. Nach dem Hauptsatz der Galoistheorie aus Folgerung 6.9 gilt für die Zwischenkörper selbst dann die umgekehrte Inklusion $\sigma(Z) \subset Z$.

(c) $\Rightarrow$ (a) und (b): Für alle $\sigma \in \mathrm{Gal}(L/K)$ gilt nach Voraussetzung $\sigma(Z) = Z$, d. h. wir können σ zu einem K-Automorphismus von Z einschränken. Es gibt also einen Gruppenhomomorphismus

$$F : \mathrm{Gal}(L/K) \to \mathrm{Gal}(Z/K), \quad \sigma \mapsto \sigma|_Z$$

mit Kern

$$\mathrm{Ker}\, F = \{\sigma \in \mathrm{Gal}(L/K) : \ \sigma|_Z = \mathrm{id}\} = \mathrm{Gal}(L/Z) = G.$$

Insbesondere ist $G = \mathrm{Gal}(L/Z)$ damit als Kern eines Morphismus ein Normalteiler in $\mathrm{Gal}(L/K)$ [G, Lemma 6.7], was (b) zeigt. Außerdem folgt

$$\begin{aligned}
[L:K] &= |\mathrm{Gal}(L/K)| && (L/K \text{ galoissch}) \\
&= |\mathrm{Gal}(L/K)/\mathrm{Gal}(L/Z)| \cdot |\mathrm{Gal}(L/Z)| && (\text{Satz von Lagrange [G, Satz 5.10]}) \\
&= |\mathrm{Im}\, F| \cdot |\mathrm{Gal}(L/Z)| && (\text{Homomorphiesatz [G, Satz 6.17]}) \\
&\leq |\mathrm{Gal}(Z/K)| \cdot |\mathrm{Gal}(L/Z)| && (\mathrm{Im}\, F \leq \mathrm{Gal}(Z/K)) \\
&\leq [Z:K] \cdot [L:Z] && (\text{Lemma 5.2 (c)}) \\
&= [L:K]. && (\text{Gradformel aus Satz 2.17})
\end{aligned}$$

Also muss hier überall die Gleichheit gelten. Insbesondere ist damit $|\mathrm{Gal}(Z/K)| = [Z:K]$ (d. h. Z/K ist galoissch, was (a) zeigt) und $\mathrm{Im}\, F = \mathrm{Gal}(Z/K)$ (was mit dem Homomorphiesatz [G, Satz 6.17] den Isomorphismus $\mathrm{Gal}(Z/K) \cong \mathrm{Gal}(L/K)/G$, also die Zusatzbehauptung zeigt). □

Beispiel 6.15. Wir betrachten noch einmal das Beispiel 6.10 des Zerfällungskörpers von $t^3 - 2$ über $\mathbb{Q}$ und überprüfen dort die Äquivalenz (a) $\Leftrightarrow$ (b) aus Satz 6.14:

(a) Die Untergruppe $A_3 = \langle (1\ 2\ 3) \rangle$ von S_3 ist nach [G, Beispiel 6.8] als Kern der Signumsabbildung ein Normalteiler. Auf der anderen Seite ist der zugehörige Zwischenkörper $\mathbb{Q}\left(e^{\frac{2\pi i}{3}}\right)$ nach Lemma 5.17 (a) galoissch über $\mathbb{Q}$, da diese Körpererweiterung Grad 2 hat.

(b) Die Untergruppe $\langle (1\ 2) \rangle$ von S_3 ist nach [G, Beispiel 6.6 (c)] kein Normalteiler. Dementsprechend ist auch der zugehörige Zwischenkörper $\mathbb{Q}(a_3)$ nicht galoissch über $\mathbb{Q}$: in ihm hat das irreduzible Polynom $t^3 - 2 \in \mathbb{Q}[t]$ nämlich eine Nullstelle a_3, zerfällt aber nicht in Linearfaktoren (siehe Satz 5.8). Dasselbe Argument gilt natürlich auch für die beiden anderen zweielementigen Untergruppen von S_3.

Beispiel 6.16. Es sei Z ein Zwischenkörper einer galoisschen Körpererweiterung L/K mit $[Z:K] = 2$, also $[L:Z] = \frac{1}{2}[L:K] = \frac{1}{2}|\mathrm{Gal}(L/K)|$. Für die zugehörige Untergruppe $G = \mathrm{Gal}(L/Z)$ gilt dann nach Folgerung 6.9 (c) also $|G| = \frac{1}{2}|\mathrm{Gal}(L/K)|$.

Beachte, dass in diesem Fall die Körpererweiterung Z/K nach Lemma 5.17 (a) immer galoissch ist. Auf der anderen Seite ist die Untergruppe $G \leq \mathrm{Gal}(L/K)$ dann nach [G, Aufgabe 6.9 (a)] auch stets ein Normalteiler, da sie genau halb so viele Elemente hat wie $\mathrm{Gal}(L/K)$. In diesem Fall kannten wir die Äquivalenz von (a) und (b) in Satz 6.14 also schon vorher.

Die folgende Aufgabe zeigt, wie man ein ähnliches Normalteilerkriterium mit Hilfe der Galoistheorie in eines für Zwischenkörper umschreiben kann:

Aufgabe 6.17. Es sei L/K eine galoissche Körpererweiterung und $G \leq \mathrm{Gal}(L/K)$ eine Untergruppe. Aus [G, Aufgabe 6.9 (b)] wissen wir, dass G ein Normalteiler von $\mathrm{Gal}(L/K)$ ist, wenn es keine andere Untergruppe von $\mathrm{Gal}(L/K)$ gibt, die genau so viele Elemente wie G hat.

Welche entsprechende Aussage über Zwischenkörper von L/K erhält man hieraus aus der Galois-Korrespondenz mit Hilfe von Satz 6.14? Kannst du diese Aussage auch direkt ohne Verwendung von Satz 6.14 beweisen?

Aufgabe 6.18. Es sei G die Galoisgruppe eines irreduziblen Polynoms vom Grad n über einem Körper K.

Man zeige: Ist G abelsch, so gilt $|G| = n$.

Gilt auch die Umkehrung?

7. Gruppentheorie und die Sätze von Sylow

In den letzten beiden Kapiteln haben wir mit Hilfe der Galoistheorie die Frage nach Zwischenkörpern einer gegebenen Körpererweiterung auf die Frage nach Untergruppen einer gegebenen Gruppe zurückgeführt. Wir wollen nun also Gruppen untersuchen und uns dabei insbesondere fragen, ob und wie man in einer (endlichen) Gruppe Untergruppen einer gegebenen Ordnung finden kann. Im Gegensatz zur direkten Suche nach Zwischenkörpern wird sich dies in der Tat als deutlich einfacher herausstellen.

Man kann diese Fragestellung in gewissem Sinne als eine „Umkehrung des Satzes von Lagrange“ bezeichnen: ist G eine endliche Gruppe und $U \leq G$ eine Untergruppe, so besagt dieser Satz ja bekanntlich, dass $|U|$ stets ein Teiler von $|G|$ ist [G, Satz 5.10]. Wir wollen uns jetzt die umgekehrte Frage stellen: ist n ein Teiler von $|G|$, gibt es dann immer eine Untergruppe $U \leq G$ mit $|U| = n$? Wie wir in Aufgabe 7.36 noch sehen werden, ist die Antwort auf diese Frage im Allgemeinen nein. Wir werden in diesem Kapitel aber einige hinreichende Kriterien angeben, die die Existenz einer solchen Untergruppe sicher stellen, und die für die Behandlung unserer Probleme aus Kapitel 0 genügen werden.

Am einfachsten wäre diese Frage natürlich zu beantworten, wenn man eine Klassifikation aller Gruppen hätte, also eine vollständige (und halbwegs überschaubare) Liste aller Gruppen modulo Isomorphie. In diesem Fall müsste man ja einfach nur alle Gruppen der gegebenen Ordnung in dieser Liste durchgehen und explizit nachprüfen, ob in diesen Fällen eine Untergruppe der gewünschten Ordnung existiert oder nicht.

Für *abelsche* Gruppen führt diese Strategie in der Tat zum Erfolg: hier können wir eine Klassifikation aller endlichen Gruppen konkret angeben und dadurch dann einfach sehen, dass für jede dieser Gruppen G zu einem gegebenen Teiler n von $|G|$ auch immer eine Untergruppe der Ordnung n existiert. Da es nicht mehr Aufwand ist, werden wir diese Klassifikation nicht nur für *endliche* abelsche Gruppen durchführen, sondern sogar für alle, die von endlich vielen Elementen erzeugt werden können.

Definition 7.1 (Endlich erzeugte Gruppen)**.** Eine Gruppe G heißt **endlich erzeugt**, wenn es endlich viele Elemente $a_1, \ldots, a_k$ gibt mit $G = \langle a_1, \ldots, a_k \rangle$.

Beispiel 7.2.

(a) Natürlich ist jede endliche Gruppe endlich erzeugt (nämlich z. B. von allen ihren Elementen).

(b) Für alle $k \in \mathbb{N}_{>0}$ ist die Gruppe $\mathbb{Z}^k$ endlich erzeugt, nämlich z. B. von den k Einheitsvektoren $(1,0,\ldots,0), \ldots, (0,\ldots,0,1)$.

(c) Die Gruppe $\mathbb{R}$ ist nicht endlich erzeugt: sind $a_1, \ldots, a_k \in \mathbb{R}$, so ist

$$\langle a_1, \ldots, a_k \rangle = \{n_1 a_1 + \cdots + n_k a_k : n_1, \ldots, n_k \in \mathbb{Z}\} \quad \subset \mathbb{R}.$$

Diese Menge ist aber stets abzählbar und kann somit nicht gleich der überabzählbaren Menge $\mathbb{R}$ sein.

Die Hauptarbeit der angekündigten Klassifikation endlich erzeugter abelscher Gruppen steckt in dem folgenden Lemma. Dazu erinnern wir uns zunächst daran, dass eine Gruppe *zyklisch* heißt, wenn sie von *einem* Element erzeugt werden kann [G, Definition 6.20], und dass diese zyklischen Gruppen genau $\mathbb{Z}$ und $\mathbb{Z}_n$ für $n \in \mathbb{N}_{>0}$ sind [G, Satz 6.21 (a)]. Wir wollen nun sehen, dass eine abelsche Gruppe, die von endlich vielen Elementen erzeugt werden kann, einfach ein Produkt von solchen zyklischen Gruppen ist.

Lemma 7.3. *Jede endlich erzeugte abelsche Gruppe ist ein (endliches) Produkt zyklischer Gruppen.*

Beweis. Es sei G eine abelsche Gruppe, die von k Elementen erzeugt werden kann. Wie bei abelschen Gruppen üblich schreiben wir die Gruppenverknüpfung in G als „+“. Wir zeigen die Aussage des Lemmas nun mit Induktion über k. Der Induktionsanfang für $k = 1$ ist dabei klar, denn dann ist G ja bereits selbst zyklisch.

Für den Induktionsschritt sei nun also $k > 1$. Wir wählen $a_1, \dots, a_k \in G$ und $n_1, \dots, n_k \in \mathbb{Z}$ mit den folgenden drei Eigenschaften:

(a) $G = \langle a_1, \dots, a_k \rangle$;

(b) $n_1 a_1 + \dots + n_k a_k = 0 \in G$;

(c) $|n_1| \neq 0$ ist minimal.

Ausführlich bedeutet Bedingung (c) also, dass es keine andere Wahl $a'_1, \dots, a'_k \in G$ und $n'_1, \dots, n'_k \in \mathbb{Z}$ gibt, für die ebenfalls (a) und (b) gilt, aber $0 \neq |n'_1| < |n_1|$ ist. Da G nach Voraussetzung von k Elementen erzeugt werden kann, ist eine solche Wahl mit $|n_1| \neq 0$ nur dann unmöglich, wenn es zwischen beliebigen Erzeugern $a_1, \dots, a_k$ überhaupt keine nicht-trivialen Relationen der Form (b) gibt. Dann ist für fest gewählte Erzeuger $a_1, \dots, a_k$ von G aber

$$\mathbb{Z}^k \to G,\ (n_1, \dots, n_k) \mapsto n_1 a_1 + \dots + n_k a_k$$

ein Gruppenisomorphismus, d. h. $G \cong \mathbb{Z}^k$ ist ein k-faches Produkt der zyklischen Gruppe $\mathbb{Z}$ und wir sind fertig.

Wir können also annehmen, dass wir eine Wahl von $a_1, \dots, a_k$ und $n_1, \dots, n_k$ mit den obigen drei Eigenschaften getroffen haben. Durch evtl. Multiplikation der $n_1, \dots, n_k$ mit -1 können wir weiterhin ohne Einschränkung $n_1 > 0$ annehmen.

Wir behaupten nun, dass n_1 ein Teiler von $n_2, \dots, n_k$ ist. Aus Symmetriegründen reicht es natürlich, dies für n_2 zu zeigen. Nach Division mit Rest können wir $n_2 = q n_1 + r$ mit $q \in \mathbb{Z}$ und $0 \leq r < n_1$ schreiben und erhalten aus (b)

$$n_1 a_1 + (q n_1 + r) a_2 + n_3 a_3 + \dots + n_k a_k = 0,$$

also

$$r a_2 + n_1 (a_1 + q a_2) + n_3 a_3 + \dots + n_k a_k = 0.$$

Nun ist aber $\langle a_2, a_1 + q a_2, a_3, \dots, a_k \rangle = \langle a_1, \dots, a_k \rangle = G$, und damit sind $a_2, a_1 + q a_2, a_3, \dots, a_k$ Erzeuger von G, die mit den Koeffizienten $r, n_1, n_3, \dots, n_k$ die Bedingungen (a) und (b) erfüllen. Wegen $0 \leq r < n_1$ muss nach der Minimalitätsforderung (c) also $r = 0$ gelten, d. h. $n_1 \,|\, n_2$.

Da n_1 ein Teiler von $n_2, \dots, n_k$ ist, können wir nun das Element

$$a'_1 := a_1 + \frac{n_2}{n_1} a_2 + \dots + \frac{n_k}{n_1} a_k \quad \in G$$

betrachten. Natürlich ist dann auch $\langle a'_1, a_2, \dots, a_k \rangle = \langle a_1, \dots, a_k \rangle = G$. Der Morphismus

$$F : \langle a'_1 \rangle \times \langle a_2, \dots, a_k \rangle \to G, \quad (u, v) \mapsto u + v$$

ist also surjektiv. Er ist aber auch injektiv: es sei $F(u,v) = 0$ mit $u = m_1 a'_1$ und $v = m_2 a_2 + \dots + m_k a_k$. Nach Konstruktion von a'_1 sowie (b) ist $n_1 a'_1 = 0$, aufgrund der Minimalitätsbedingung (c) jedoch $n a'_1 \neq 0$ für $0 < n < n_1$. Also ist $\langle a'_1 \rangle \cong \mathbb{Z}_{n_1}$, und wir können in der Darstellung für u ohne Einschränkung $0 \leq m_1 < n_1$ annehmen. Dann besagt $F(u,v) = u + v = 0$ aber

$$m_1 a'_1 + m_2 a_2 + \dots + m_k a_k = 0,$$

was wiederum wegen der Minimalitätsbedingung (c) aufgrund von $0 \leq m_1 < n_1$ nur für $m_1 = 0$ möglich ist. Damit ist $u = 0$, mit $F(u,v) = u + v = 0$ also auch $v = 0$, d. h. F ist auch injektiv.

Aufgrund des Isomorphismus F ist G also isomorph zum Produkt der zyklischen Gruppe $\langle a'_1 \rangle$ mit $\langle a_2, \dots, a_k \rangle$. Da dieser zweite Faktor von $k-1$ Elementen erzeugt werden kann, ist er nach Induktionsvoraussetzung ein endliches Produkt zyklischer Gruppen. Damit ist auch G wie behauptet ein endliches Produkt zyklischer Gruppen. □

11

Mit diesem Lemma können wir nun wie angekündigt alle endlich erzeugten abelschen Gruppen klassifizieren.

Folgerung 7.4 (**Hauptsatz über endlich erzeugte abelsche Gruppen**). *Es sei G eine endlich erzeugte abelsche Gruppe. Dann gibt es eindeutig bestimmte $r,m \in \mathbb{N}$ und bis auf die Reihenfolge eindeutige (aber nicht notwendig verschiedene) Primzahlpotenzen $p_1^{k_1},\dots,p_m^{k_m}$, so dass*

$$G \cong \mathbb{Z}^r \times \mathbb{Z}_{p_1^{k_1}} \times \cdots \times \mathbb{Z}_{p_m^{k_m}}.$$

Beweis. Für die Existenz einer solchen Darstellung genügt es nach Lemma 7.3, eine zyklische Gruppe zu betrachten, also $G = \mathbb{Z}$ oder $G = \mathbb{Z}_n$ für ein $n \in \mathbb{N}_{>0}$. Für $G = \mathbb{Z}$ ist natürlich nichts zu zeigen; für $\mathbb{Z}_n$ dagegen gilt nach dem chinesischen Restsatz [G, Satz 11.22]

$$\mathbb{Z}_n \cong \mathbb{Z}_{p_1^{k_1}} \times \cdots \times \mathbb{Z}_{p_m^{k_m}},$$

wenn $p_1^{k_1} \cdot \cdots \cdot p_m^{k_m}$ die Primfaktorzerlegung von n ist.

Die Eindeutigkeit der Darstellung ergibt sich aus Teil (b) der folgenden Aufgabe. □

Aufgabe 7.5 (Eindeutigkeit im Hauptsatz über endlich erzeugte abelsche Gruppen)**.**

(a) Es sei $G = \mathbb{Z}^r \times \mathbb{Z}_{p_1^{k_1}} \times \cdots \times \mathbb{Z}_{p_n^{k_n}}$ für gewisse $r,n,k_1,\dots,k_n \in \mathbb{N}$ und (nicht notwendig verschiedene) Primzahlen $p_1,\dots,p_n$. Zeige, dass für alle $k \in \mathbb{N}$ und jede Primzahl p

$$\log_p |G/p^k G| = kr + \sum_{i:\, p_i = p} \min\{k, k_i\}$$

gilt, wobei wie üblich $p^k G = \{p^k x :\ x \in G\}$ und $\log_p$ der Logarithmus zur Basis p ist.

(b) Wir betrachten nun eine beliebige Gruppe G, die isomorph zu einer Gruppe der Form $\mathbb{Z}^r \times \mathbb{Z}_{p_1^{k_1}} \times \cdots \times \mathbb{Z}_{p_n^{k_n}}$ wie in (a) ist. Zeige, dass dann r, n und alle Primzahlpotenzen $p_1^{k_1},\dots,p_n^{k_n}$ (bis auf die Reihenfolge) durch G eindeutig bestimmt sind.

Bemerkung 7.6. Mit Folgerung 7.4 können wir insbesondere leicht alle endlichen abelschen Gruppen einer gegebenen Ordnung n angeben, indem wir n auf alle möglichen Arten als Produkt von (nicht notwendig verschiedenen) Primzahlpotenzen schreiben. So erhalten wir zum Beispiel:

(a) Es gibt genau zwei abelsche Gruppen der Ordnung 12, nämlich

$$\mathbb{Z}_4 \times \mathbb{Z}_3 \quad \text{und} \quad \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_3$$

(dass diese beiden Gruppen nicht isomorph sind, sieht man hier auch direkt ohne Aufgabe 7.5 (b), da die erste ein Element der Ordnung 4 besitzt, die zweite jedoch nicht). Die erste dieser beiden Gruppen ist nach dem chinesischen Restsatz isomorph zu $\mathbb{Z}_{12}$.

(b) Ist n ein Produkt von paarweise verschiedenen Primzahlen, so gibt es nur eine abelsche Gruppe der Ordnung n (nämlich $\mathbb{Z}_n$).

Mit Hilfe der Klassifikation aus Folgerung 7.4 können wir nun für abelsche Gruppen leicht die in der Einleitung zu diesem Kapitel genannte Frage nach der Existenz von Untergruppen einer gegebenen Ordnung beantworten.

Folgerung 7.7 (Untergruppen in abelschen Gruppen)**.** *Es sei G eine endliche abelsche Gruppe und $n \in \mathbb{N}_{>0}$ ein Teiler von $|G|$. Dann gibt es eine Untergruppe $U \leq G$ mit $|U| = n$.*

Beweis. Nach Folgerung 7.4 dürfen wir mit den dortigen Bezeichnungen $G = \mathbb{Z}_{p_1^{k_1}} \times \cdots \times \mathbb{Z}_{p_m^{k_m}}$ mit $|G| = p_1^{k_1} \cdot \cdots \cdot p_m^{k_m}$ annehmen. Da n ein Teiler dieser Zahl ist, können wir n natürlich (nicht notwendig eindeutig) in der Form $n = p_1^{a_1} \cdot \cdots \cdot p_m^{a_m}$ mit $a_i \leq k_i$ für alle i schreiben. Nun ist aber für alle i

$$U_i := \langle\, p_i^{k_i - a_i} \,\rangle = \{r \cdot p_i^{k_i - a_i} :\ 0 \leq r < {p_i}^{a_i}\}$$

eine Untergruppe von $\mathbb{Z}_{p_i^{k_i}}$ der Ordnung $p_i^{a_i}$. Also ist $U_1 \times \cdots \times U_m \leq G$ wie gewünscht eine Untergruppe der Ordnung n. □

Übertragen wir dieses Ergebnis nun mit Hilfe der Galoistheorie auf Körpererweiterungen, können wir damit also im Fall einer galoisschen Körpererweiterung mit abelscher Galoisgruppe die Existenz von Zwischenkörpern mit gegebenem Grad zeigen. Dies ermöglicht es uns z. B. schon, die Frage nach der Konstruierbarkeit des regelmäßigen n-Ecks mit Zirkel und Lineal nun endgültig zu lösen, indem wir zeigen, dass die in Folgerung 3.33 gefundene notwendige Bedingung für die Konstruierbarkeit auch hinreichend ist.

Folgerung 7.8 (Konstruierbarkeit des n-Ecks)**.** *Das regelmäßige n-Eck ist genau dann mit Zirkel und Lineal konstruierbar, wenn n von der Form*

$$n = 2^m \cdot p_1 \cdot \cdots \cdot p_r$$

für ein $m \geq 0$ und verschiedene Fermatsche Primzahlen $p_1, \ldots, p_r$ ist (also für Primzahlen der Form $p_i = 2^{2^{a_i}} + 1$ mit $a_i \in \mathbb{N}$).

Beweis. Aus Folgerung 3.33 wissen wir bereits, dass das n-Eck höchstens dann konstruierbar sein kann, wenn n von der angegebenen Form ist.

Es sei nun also n von dieser Form. Die Körpererweiterung $\mathbb{Q}\left(e^{\frac{2\pi i}{n}}\right)/\mathbb{Q}$ ist nach Beispiel 5.3 (c) und 5.7 galoissch mit Galoisgruppe $G = \mathbb{Z}_n^*$. Ihre Ordnung ist nach Satz 3.29 gleich $|\mathbb{Z}_n^*| = \varphi(n)$ und damit nach Lemma 3.31 für das betrachtete n eine Zweierpotenz 2^r für ein $r \in \mathbb{N}$. Da $G = \mathbb{Z}_n^*$ natürlich abelsch ist, können wir mit Folgerung 7.7 also rekursiv eine Untergruppenkette

$$G = U_0 \geq U_1 \geq \cdots \geq U_r = \{e\}$$

mit $|U_k| = 2^{r-k}$ für $k = 0, \ldots, r$ finden. Nach der Galois-Korrespondenz aus Folgerung 6.9 erhalten wir nun mit $Z_k := \mathbb{Q}\left(e^{\frac{2\pi i}{n}}\right)^{U_k}$ eine entsprechende Kette von Zwischenkörpern

$$\mathbb{Q} = Z_0 \leq Z_1 \leq \cdots \leq Z_r = \mathbb{Q}\left(e^{\frac{2\pi i}{n}}\right)$$

mit $\left[\mathbb{Q}\left(e^{\frac{2\pi i}{n}}\right) : Z_k\right] = 2^{r-k}$, nach der Gradformel aus Satz 2.17 also $[Z_k : Z_{k-1}] = 2$ für alle $k = 1, \ldots, r$. Damit ist Z_k/Z_{k-1} gemäß Aufgabe 2.21 (b) für alle i eine einfache 2-Radikalerweiterung. Also ist $\mathbb{Q}\left(e^{\frac{2\pi i}{n}}\right)$ nach Definition 1.18 (b) eine 2-Radikalerweiterung von $\mathbb{Q}$. Da sie natürlich das Element $e^{\frac{2\pi i}{n}}$ enthält, ist das n-Eck damit wie in Beispiel 1.23 (C) erläutert mit Zirkel und Lineal konstruierbar. □

Wir wollen nun sehen, in wie weit wir auch im nicht-abelschen Fall Aussagen zur Klassifikation von Gruppen und zur Existenz von Untergruppen gegebener Ordnung machen können. Natürlich ist dies hier viel schwieriger, und die Ergebnisse werden auch deutlich schwächer ausfallen als im abelschen Fall. Zur Vorbereitung müssen wir zunächst etwas ausholen und das Konzept der Gruppenoperation auf einer Menge einführen.

Definition 7.9 (Gruppenoperationen)**.** Es seien $(G, \cdot)$ eine Gruppe und M eine Menge. Eine **Gruppenoperation** von G auf M ist eine Abbildung

$$* : G \times M \to M, \quad (a, x) \mapsto a * x,$$

so dass

(a) $e * x = x$ für alle $x \in M$ (wobei $e \in G$ wie üblich das neutrale Element bezeichnet);

(b) $a * (b * x) = (a \cdot b) * x$ für alle $a, b \in G$ und $x \in M$.

Bemerkung 7.10. Genau wie bei Gruppenverknüpfungen kann man eine Gruppenoperation natürlich auch mit einem anderen Symbol als „$*$“ bezeichnen. Oft verwendet man für eine Gruppenoperation sogar das gleiche Symbol „$\cdot$“ wie für die Gruppenverknüpfung, weil dadurch, ob zwei Elemente von G miteinander verknüpft werden oder eines von G mit einem von M, ja in der Regel bereits eindeutig erkennbar ist, ob die Gruppenverknüpfung oder die Gruppenoperation gemeint ist. Da man eine Gruppenoperation außerdem auch so auffassen kann, dass ein Gruppenelement a eine

Funktion ist, die einem Element $x \in M$ ein Element $a * x \in M$ zuordnet (daher kommt natürlich auch die Sprechweise, dass G auf M operiert), sieht man in der Literatur auch oft die Schreibweise $a(x)$ für $a * x$. Wir werden in diesem Skript jedoch ausschließlich die Schreibweise $a * x$ verwenden, da diese wohl am wenigsten zu Verwirrungen führen kann.

Beispiel 7.11 (Permutationen als Gruppenoperation)**.** Es seien $G \leq S_n$ eine Untergruppe der symmetrischen Gruppe und $M = \{1, \ldots, n\}$. Dann operiert G auf M einfach dadurch, dass man eine Permutation aus G auf eine Zahl in M anwendet, d. h. indem wir

$$\sigma * i := \sigma(i) \quad \in M$$

für $\sigma \in G$ und $i \in M$ setzen. Die Eigenschaften (a) und (b) aus Definition 7.9 sind dabei natürlich offensichtlich, denn es ist ja $\mathrm{id}(i) = i$ und $\sigma(\tau(i)) = (\sigma \circ \tau)(i)$ für alle $i \in M$ und $\sigma, \tau \in G \leq S_n$.

In der Tat ist dies ein sehr „typisches“ Beispiel für eine Gruppenoperation — denn die folgende Bemerkung zeigt, dass die Elemente von G im Fall einer Operation auf einer Menge M immer als Permutationen auf M operieren.

Bemerkung 7.12 (Gruppenoperationen als Morphismen in die symmetrische Gruppe)**.** Es sei G eine Gruppe, die auf einer Menge M operiert. Für ein festes $a \in G$ ist dann die Abbildung

$$\sigma_a : M \to M,\ x \mapsto a * x$$

bijektiv mit Umkehrabbildung $\sigma_{a^{-1}}$, denn nach Definition 7.9 gilt für alle $x \in M$

$$\sigma_{a^{-1}}(\sigma_a(x)) = a^{-1} * (a * x) = (a^{-1} \cdot a) * x = e * x = x$$

und analog auch $\sigma_a(\sigma_{a^{-1}}(x)) = x$. Wir erhalten so also eine Abbildung

$$G \to S(M),\ a \mapsto \sigma_a$$

der Gruppe G in die symmetrische Gruppe $S(M)$ aller bijektiven Abbildungen von M in sich [G, Konstruktion 2.1]. Diese Abbildung ist sogar ein Gruppenhomomorphismus, denn nach Definition 7.9 gilt für alle $x \in M$ und $a, b \in G$

$$\sigma_a(\sigma_b(x)) = a * (b * x) = (a \cdot b) * x = \sigma_{a \cdot b}(x)$$

und damit $\sigma_a \circ \sigma_b = \sigma_{a \cdot b}$. Eine Operation einer Gruppe G auf einer Menge M bestimmt also einen Morphismus von G in die symmetrische Gruppe $S(M)$. Im Fall von Beispiel 7.11, wo eine Untergruppe $G \leq S_n$ der symmetrischen Gruppe durch Permutation auf $M = \{1, \ldots, n\}$ operiert, ist dieser Morphismus offensichtlich gerade die Einbettung $G \to S_n = S(M)$.

In der Tat bestimmt auch umgekehrt ein Morphismus von G in die symmetrische Gruppe $S(M)$ eine Gruppenoperation von G auf M, wie die folgende einfache Aufgabe zeigt.

Aufgabe 7.13. Es seien G eine Gruppe und M eine Menge. Zeige, dass eine Gruppenoperation von G auf M „dasselbe“ ist wie ein Morphismus von G in die symmetrische Gruppe $S(M)$, d. h. dass die Konstruktion aus Bemerkung 7.12 eine bijektive Abbildung

$$\{\text{Gruppenoperationen von } G \text{ auf } M\} \overset{1:1}{\longleftrightarrow} \{\text{Morphismen } G \to S(M)\}$$

liefert.

Wir werden später in Konstruktion 7.18 und im Beweis der Sätze 7.29 und 7.30 noch weitere für uns relevante Gruppenoperationen kennen lernen. Zunächst einmal wollen wir jedoch ein paar Begriffe einführen, mit denen man Gruppenoperationen untersuchen kann.

Definition 7.14 (Bahnen, Fixgruppen und Fixpunkte)**.** Es sei G eine Gruppe, die auf einer Menge M operiert. Für ein festes $x \in M$ heißt dann

(a) $G * x := \{a * x :\ a \in G\} \subset M$ die **Bahn** von x;

(b) $G_x := \{a \in G :\ a * x = x\} \leq G$ die **Fixgruppe** oder der **Stabilisator** von x (man prüft sofort nach, dass dies in der Tat eine Untergruppe von G ist);

(c) x ein **Fixpunkt** der Operation, falls $a*x=x$ für alle $a\in G$. Offensichtlich ist dies äquivalent zu $G*x=\{x\}$ und zu $G_x=G$.

Beispiel 7.15. Es sei $\sigma\in S_4$ der 3-Zykel $\sigma=(1\ 2\ 3)$. Wie in Beispiel 7.11 operiere die Gruppe $G=\langle\sigma\rangle=\{\mathrm{id},\sigma,\sigma^2\}\leq S_4$ auf der Menge $M=\{1,2,3,4\}$ durch Permutation. Die Elemente in G vertauschen also die Zahlen $1,2,3\in M$ zyklisch und lassen das Element $4\in M$ fest. In der Sprechweise von Definition 7.14 bedeutet dies:

(a) Die Bahn des Elements $1\in M$ ist $G*1=\{\mathrm{id}(1),\sigma(1),\sigma^2(1)\}=\{1,2,3\}$. Da von den Elementen von G nur die Identität das Element 1 fest lässt, ist die zugehörige Fixgruppe $G_1=\{\mathrm{id}\}$. Natürlich ist 1 kein Fixpunkt der Gruppenoperation. Dieselben Aussagen gelten analog für die Elemente 2 und 3 von M.

(b) Die Bahn des Elements $4\in M$ ist $G*4=\{\mathrm{id}(4),\sigma(4),\sigma^2(4)\}=\{4\}$. Hier ist also die zugehörige Fixgruppe $G_4=G$, und 4 ist ein Fixpunkt der Gruppenoperation.

Bemerkung 7.16 (Bahnen als Äquivalenzklassen)**.** Die Gruppe G operiere wieder auf der Menge M. Wir definieren eine Relation $\sim$ auf M durch

$$y\sim x \quad :\Leftrightarrow \quad \text{es gibt ein } a\in G \text{ mit } y=a*x.$$

Man prüft sofort nach, dass dies eine Äquivalenzrelation ist [G, Definition 5.1]. Außerdem ist die Äquivalenzklasse eines Elements $x\in M$, also die Menge der Elemente $y\in M$ mit $y\sim x$, nach Konstruktion natürlich genau die Bahn $G*x$. Insbesondere ist M also stets die disjunkte Vereinigung aller Bahnen der Gruppenoperation [G, Lemma 5.3 (b)].

Die wichtigste Eigenschaft einer Gruppenoperation ist die sogenannte Bahnengleichung, die wir jetzt beweisen wollen.

Satz 7.17 (**Bahnengleichung**)**.** *Eine endliche Gruppe G operiere auf einer endlichen Menge M. Dann gilt:*

(a) *Für alle $x\in M$ ist $|G|=|G_x|\cdot|G*x|$.*

(b) *Ist $\{x_1,\dots,x_n\}\subset M$ ein Repräsentantensystem der Bahnen, d. h. sind $G*x_1,\dots,G*x_n$ genau die verschiedenen Bahnen der Gruppenoperation, so gilt*

$$|M|=\sum_{i=1}^{n}|G*x_i|=\sum_{i=1}^{n}\frac{|G|}{|G_{x_i}|}.$$

Beweis.

(a) Wie üblich bezeichne G/G_x die Menge der Linksnebenklassen von G_x in G [G, Definition 5.6]. Beachte, dass dies keine Gruppe ist, da die Fixgruppe G_x in der Regel kein Normalteiler in G ist. Das brauchen wir aber auch nicht, denn wir behaupten lediglich, dass die Abbildung

$$G/G_x\to G*x,\quad \overline{a}\mapsto a*x$$

wohldefiniert und bijektiv ist. In der Tat gilt für alle $a,b\in G$

$$\begin{aligned}\overline{a}=\overline{b}\in G/G_x &\Leftrightarrow a^{-1}b\in G_x && \text{(Definition von } G/G_x)\\ &\Leftrightarrow (a^{-1}b)*x=x && \text{(Definition der Fixgruppe } G_x)\\ &\Leftrightarrow b*x=a*x.\end{aligned}$$

Lesen wir diese Äquivalenz in der Richtung „$\Rightarrow$“, so ergibt sich, dass die oben genannte Abbildung wohldefiniert ist. Lesen wir die Äquivalenz in der Richtung „$\Leftarrow$“, so bedeutet dies genau die Injektivität. Außerdem ist die Abbildung natürlich surjektiv, denn nach Definition der Bahn ist ja jedes Element von $G*x$ von der Form $a*x$ für ein $a\in G$.

Also ist die obige Abbildung bijektiv, d. h. es ist insbesondere $|G/G_x|=|G*x|$. Mit dem Satz von Lagrange [G, Satz 5.10] ergibt sich also die Behauptung $|G|=|G_x|\cdot|G/G_x|=|G_x|\cdot|G*x|$.

(b) Dies folgt nun sofort aus Bemerkung 7.16 und Teil (a) des Satzes. □

Wir werden nun eine für uns im Folgenden besonders wichtige Gruppenoperation kennen lernen, nämlich die Gruppenkonjugation. Eine Besonderheit dieser Operation ist, dass eine Gruppe G hierbei auf sich selbst operiert, d. h. in der Notation von Definition 7.9 die Menge M gleich der Gruppe G ist. Demzufolge liegen auch die Bahnen und Fixgruppen dieser Operation beide in G, während sonst ja die Bahnen in M und die Fixgruppen in G liegen. Da die Gruppenkonjugation besonders wichtig ist, haben die Begriffe aus Definition 7.14 für diesen Fall alle einen besonderen Namen.

Konstruktion 7.18 (Gruppenkonjugation)**.** Es sei G eine Gruppe.

(a) Die Vorschrift
$$b * a := bab^{-1} \quad \text{für } a, b \in G$$
definiert eine Gruppenoperation von G auf sich selbst, denn für alle $a, b, c \in G$ ist
$$e * a = eae^{-1} = a \quad \text{und} \quad c * (b * a) = cbab^{-1}c^{-1} = (cb)a(cb)^{-1} = (cb) * a.$$
Sie wird als **Konjugation** bezeichnet. Die Bahnen dieser Operation nennt man die **Konjugationsklassen** von G. Zwei Elemente $a_1, a_2 \in G$ heißen **konjugiert** zueinander, wenn sie in derselben Konjugationsklasse liegen, also wenn es ein $b \in G$ gibt mit $a_2 = ba_1b^{-1}$.

(b) Für ein $a \in G$ heißt die Fixgruppe von a bezüglich der Konjugation
$$G_a = \{b \in G : \ bab^{-1} = a\} = \{b \in G : \ ba = ab\} \quad \leq G$$
(also die Menge der Gruppenelemente, die mit dem gegebenen a kommutieren) der **Zentralisator** von a in G. Er wird mit $C_G(a)$ bezeichnet, bzw. (wenn die zugrunde liegende Gruppe aus dem Zusammenhang klar ist) einfach mit $C(a)$.

(c) Die Menge der Fixpunkte der Konjugation
$$Z(G) := \{a \in G : \ bab^{-1} = a \text{ für alle } b \in G\} = \{a \in G : \ ba = ab \text{ für alle } b \in G\}$$
(also die Menge der Gruppenelemente, die mit allen anderen Elementen kommutieren) heißt das **Zentrum** von G. Offensichtlich ist G genau dann abelsch, wenn $Z(G) = G$ ist. Man prüft leicht nach, dass $Z(G)$ eine Untergruppe von G ist [G, Aufgabe 3.6 (e)]. In der Tat ist sogar jede Untergruppe U des Zentrums ein Normalteiler von G, denn für alle $u \in U$ und $a \in G$ gilt ja $aua^{-1} = u \in U$.

Beispiel 7.19 (Konjugationsklassen in S_n)**.** Im Fall der symmetrischen Gruppe S_n haben die Konjugationsklassen eine besonders einfache Interpretation. Es sei dazu $\sigma \in S_n$ eine Permutation, deren Zykelzerlegung aus disjunkten Zykeln der Längen $k_1, \ldots, k_m$ mit $k_1 + \cdots + k_m = n$ besteht [G, Konstruktion 2.10], also
$$\sigma = (a_{1,1} \ \cdots \ a_{1,k_1}) \ \cdots \ (a_{m,1} \ \cdots \ a_{m,k_m})$$
für $a_{i,j}$ mit $\{a_{i,j} : 1 \leq i \leq m, 1 \leq j \leq k_i\} = \{1, \ldots, n\}$. Ist nun $\tau \in S_n$ beliebig und setzen wir $b_{i,j} := \tau(a_{i,j})$, so ergibt einfaches Nachrechnen, dass
$$\tau\sigma\tau^{-1} = (b_{1,1} \ \cdots \ b_{1,k_1}) \ \cdots \ (b_{m,1} \ \cdots \ b_{m,k_m}). \qquad (*)$$
Die zu σ konjugierten Permutationen haben in ihrer Zykelzerlegung also Zykel der gleichen Längen wie σ. Haben wir umgekehrt eine Permutation wie auf der rechten Seite von $(*)$, die aus Zykeln der gleichen Länge wie σ besteht, so können wir durch $\tau(a_{i,j}) := b_{i,j}$ ein Element $\tau \in S_n$ definieren, für das die Gleichung $(*)$ gilt. Die Konjugationsklasse von σ besteht also genau aus allen Permutationen, deren Zykelzerlegung aus disjunkten Zykeln der Längen $k_1, \ldots, k_m$ besteht. So ist z. B. die Konjugationsklasse von $(1 \ \ 2)$ in S_n genau die Menge aller Transpositionen (hier ist $k_1 = 2$ und $k_2 = \cdots = k_m = 1$ für $m = n - 1$).

12

Bemerkung 7.20 (Klassengleichung)**.** Es sei G eine Gruppe. Wenden wir die Bahnengleichung aus Satz 7.17 auf die Konjugationsoperation aus Konstruktion 7.18 an, so erhalten wir offensichtlich
$$|G| = \sum_{i=1}^{n} \frac{|G|}{|C(a_i)|},$$

wobei $a_1, \dots, a_n$ ein Repräsentantensystem der Konjugationsklassen ist. Typischerweise formuliert man diese Gleichung etwas um, indem man aus dieser Summe alle Terme herauszieht, die den Wert 1 haben. Dies sind genau die i mit $C(a_i) = G$, also für die a_i mit allen Gruppenelementen kommutiert und damit $a_i \in Z(G)$ gilt. Umgekehrt kommt natürlich auch jedes Element des Zentrums unter den a_i vor, da jedes solche Element seine eigene Konjugationsklasse bildet. Wir erhalten damit die sogenannte **Klassengleichung**

$$|G| = |Z(G)| + \sum_{i=1}^{m} \underbrace{\frac{|G|}{|C(a_i)|}}_{>1}$$

für G, wobei wir die obigen Repräsentanten der Konjugationsklassen jetzt so nummeriert haben, dass $a_1, \dots, a_m$ genau die Klassen mit mehr als einem Element repräsentieren und $a_{m+1}, \dots, a_n$ im Zentrum von G liegen.

Als erste Anwendung unseres Studiums von Gruppenoperationen können wir nun ein kleines Resultat zur Klassifikation beliebiger (d. h. nicht notwendig abelscher) Gruppen zeigen. Wir wissen ja bereits, dass es zu einer Primzahl p bis auf Isomorphie nur eine Gruppe mit p Elementen gibt, nämlich $\mathbb{Z}_p$. Ein ähnliches Ergebnis können wir nun für Gruppen zeigen, deren Ordnung ein Primzahlquadrat ist.

Aufgabe 7.21 (Klassifikation der Gruppen der Ordnung p^2)**.** Es sei G eine Gruppe mit $|G| = p^2$ für eine Primzahl p.

(a) Zeige mit Hilfe der Klassengleichung, dass $|Z(G)| = p^2$.

(b) Zeige, dass $G \cong \mathbb{Z}_{p^2}$ oder $G \cong \mathbb{Z}_p \times \mathbb{Z}_p$.

Als weitere Anwendung der Klassengleichung wollen wir nun wieder zum Problem der Existenz von Untergruppen einer gegebenen Ordnung zurück kommen. Wie wir in Aufgabe 7.36 noch sehen werden, ist es — im Gegensatz zum abelschen Fall in Folgerung 7.7 — für eine beliebige endliche Gruppe G und einen Teiler n von $|G|$ im Allgemeinen nicht mehr richtig, dass G dann eine Untergruppe der Ordnung n besitzt. Allerdings können wir die Existenz einer solchen Untergruppe zumindest noch dann zeigen, wenn n eine Primzahlpotenz ist.

Satz 7.22 (**1. Satz von Sylow**)**.** *Es sei G eine endliche Gruppe. Ferner seien p eine Primzahl und $k \in \mathbb{N}_{>0}$, so dass p^k ein Teiler von $|G|$ ist. Dann gibt es eine Untergruppe $U \leq G$ mit $|U| = p^k$.*

Beweis. Wir zeigen die Aussage mit Induktion über $|G|$; für $|G| = 1$ ist natürlich nichts zu zeigen. Für den Induktionsschritt unterscheiden wir zwei Fälle:

(a) $p \mid |Z(G)|$: Da das Zentrum $Z(G)$ eine abelsche Gruppe ist, gibt es nach Folgerung 7.7 eine Untergruppe $N \leq Z(G) \leq G$ mit $|N| = p$. Im Fall $k = 1$ können wir dann also natürlich $U = N$ wählen und sind fertig.

Andernfalls können wir die Faktorgruppe G/N betrachten, da N nach Konstruktion 7.18 (c) als Untergruppe des Zentrums sogar ein Normalteiler in G ist. Wegen $p^k \mid |G|$ gilt dann $p^{k-1} \mid \frac{1}{p} \cdot |G| = |G/N|$. Nach Induktionsvoraussetzung gibt es also eine Untergruppe $V \leq G/N$ mit $|V| = p^{k-1}$. Ist dann $\pi : G \to G/N$, $a \mapsto \overline{a}$ die Restklassenabbildung, so ist $U := \pi^{-1}(V)$ eine Untergruppe von G mit $U/N = V$, also wie gewünscht $|U| = |N| \cdot |V| = p \cdot p^{k-1} = p^k$.

(b) $p \nmid |Z(G)|$: Wegen $p \mid |G|$ und $p \nmid |Z(G)|$ muss es nach der Klassengleichung

$$|G| = |Z(G)| + \sum_{i=1}^{m} \underbrace{\frac{|G|}{|C(a_i)|}}_{>1}$$

aus Bemerkung 7.20 (mit den dortigen Notationen) ein $i = 1, \dots, m$ geben mit $p \nmid \frac{|G|}{|C(a_i)|}$. Da dieser Quotient also keinen Primfaktor p mehr enthält, folgt mit $p^k \mid |G|$ auch $p^k \mid |C(a_i)|$.

Wegen $\frac{|G|}{|C(a_i)|} > 1$, also $|C(a_i)| < |G|$, finden wir nun nach Induktionsvoraussetzung eine Untergruppe $U \leq C(a_i) \leq G$ mit $|U| = p^k$. □

Mit Hilfe der Galois-Korrespondenz erhalten wir aus diesem Satz nun natürlich sofort eine analoge Aussage über die Existenz von Zwischenkörpern.

Folgerung 7.23 (Existenz von Zwischenkörpern)**.** *Es sei L/K eine galoissche Körpererweiterung von Charakteristik 0. Ferner seien p prim und $k \in \mathbb{N}_{>0}$ mit $p^k \mid [L:K]$. Dann gibt es einen Zwischenkörper Z von L/K mit $[L:Z] = p^k$.*

Beweis. Weil L/K galoissch ist, ist $|\mathrm{Gal}(L/K)| = [L:K]$, d. h. nach Voraussetzung ist p^k ein Teiler von $|\mathrm{Gal}(L/K)|$. Der 1. Satz von Sylow liefert also die Existenz einer Untergruppe $U \leq \mathrm{Gal}(L/K)$ mit $|U| = p^k$. Nach dem Hauptsatz der Galoistheorie aus Folgerung 6.9 gibt es nun einen zugehörigen Zwischenkörper $Z = L^U$ von L/K mit $[L:Z] = |U| = p^k$. □

Dieses Resultat ermöglicht es uns nun, wie in Problem 0.1 der Einleitung angekündigt einen algebraischen Beweis des Fundamentalsatzes der Algebra zu geben. Allerdings ist dieser Beweis nicht wirklich vollständig algebraisch, sondern verwendet auch ein Hilfsresultat aus der Analysis — was aber auch so sein muss, da die besonderen Eigenschaften von $\mathbb{R}$ gegenüber $\mathbb{Q}$ (z. B. die Vollständigkeit) und damit auch die von $\mathbb{C} = \mathbb{R}(i)$ gegenüber $\mathbb{Q}(i)$ (wo ja z. B. das Polynom $t^2 - 2$ nicht in Linearfaktoren zerfällt) nun einmal analytischer und nicht algebraischer Natur sind. Im folgenden Lemma stellen wir bereit, was wir aus der Analysis benötigen.

Lemma 7.24.

(a) *Es gibt keinen Erweiterungskörper L von $\mathbb{R}$ mit $[L:\mathbb{R}] = q$ für ein ungerades $q > 1$.*

(b) *Es gibt keinen Erweiterungskörper L von $\mathbb{C}$ mit $[L:\mathbb{C}] = 2$.*

Beweis.

(a) Angenommen, es gäbe einen Körper $L \geq \mathbb{R}$ mit $[L:\mathbb{R}] = q > 1$ ungerade. Nach dem Satz 4.28 vom primitiven Element ist $L = \mathbb{R}(a)$ für ein $a \in L$. Das Minimalpolynom f von a über $\mathbb{R}$ ist dann natürlich nach Lemma 2.6 und Satz 2.14 (a) irreduzibel und hat Grad q. Nun wissen wir aber aus dem Zwischenwertsatz der Analysis, dass ein solches reelles Polynom ungeraden Grades immer eine Nullstelle in $\mathbb{R}$ besitzt, da $f(x)$ für $x \to \infty$ und $x \to -\infty$ unterschiedliche Vorzeichen hat. Also spaltet f über $\mathbb{R}$ einen Linearfaktor ab und kann damit nicht über $\mathbb{R}$ irreduzibel sein, was ein Widerspruch ist.

(b) Wir nehmen nun an, dass $L \geq \mathbb{C}$ mit $[L:\mathbb{C}] = 2$. Wie in Teil (a) ist dann $L = \mathbb{C}(a)$ für ein $a \in L$; das Minimalpolynom f von a über $\mathbb{C}$ ist wieder irreduzibel und hat diesmal Grad 2. Nach der bekannten Lösungsformel für quadratische Gleichungen (und weil in $\mathbb{C}$ jede Zahl eine Quadratwurzel besitzt) hat f dann aber eine Nullstelle in $\mathbb{C}$, zerfällt also über $\mathbb{C}$ in Linearfaktoren und kann damit nicht irreduzibel sein, was wieder ein Widerspruch ist. □

Satz 7.25 (Fundamentalsatz der Algebra). *Jedes komplexe Polynom zerfällt über $\mathbb{C}$ in Linearfaktoren. (Insbesondere hat also jedes nicht-konstante komplexe Polynom eine Nullstelle in $\mathbb{C}$.)*

Beweis. Es sei $f \in \mathbb{C}[t]$. Es genügt zu zeigen, dass das reelle Polynom $g := f \cdot \overline{f} \in \mathbb{R}[t]$ über $\mathbb{C}$ in Linearfaktoren zerfällt, da dies wegen der eindeutigen Primfaktorzerlegung in $\mathbb{C}[t]$ [G, Satz 11.9] dann natürlich auch für f gelten muss.

Wir betrachten nun den Zerfällungskörper L von g über $\mathbb{C}$. Da wir diesen auch als Zerfällungskörper von $(t^2+1)\,g$ über $\mathbb{R}$ schreiben können, sind die Körpererweiterungen $L/\mathbb{C}$ und $L/\mathbb{R}$ nach Satz 5.8 galoissch. Wir wollen zeigen, dass $L = \mathbb{C}$ ist, also dass g bereits über $\mathbb{C}$ in Linearfaktoren zerfällt.

Dazu schreiben wir den Grad der Körpererweiterung $L/\mathbb{R}$ als $[L:\mathbb{R}] = q \cdot 2^k$ für ein ungerades q — jede natürliche Zahl lässt sich ja so schreiben. Da $L/\mathbb{R}$ galoissch ist, gibt es nun nach Folgerung 7.23 einen Zwischenkörper $\mathbb{R} \leq Z \leq L$ mit $[L:Z] = 2^k$, nach der Gradformel aus Satz 2.17 also $[Z:\mathbb{R}] = q$. Dies ist nach Lemma 7.24 (a) aber nur möglich für $q = 1$.

Wir haben also $[L:\mathbb{R}] = 2^k$ und damit $[L:\mathbb{C}] = 2^{k-1}$. Wäre nun $k \geq 2$, so gäbe es wiederum nach Folgerung 7.23 einen Zwischenkörper $\mathbb{C} \leq Z' \leq L$ mit $[L:Z'] = 2^{k-2}$, also $[Z':\mathbb{C}] = 2$. Dies ist nach Lemma 7.24 (b) aber unmöglich. Also ist $k = 1$, d. h. $[L:\mathbb{C}] = 1$ und damit $L = \mathbb{C}$. □

Bemerkung 7.26 (Algebraische Erweiterungen von $\mathbb{C}$)**.** Eine äquivalente Formulierung des Fundamentalsatzes der Algebra ist, dass es keine (echte) algebraische Körpererweiterung von $\mathbb{C}$ gibt: ist $L/\mathbb{C}$ eine algebraische Körpererweiterung und $a \in L$ beliebig, so ist das Minimalpolynom von a über $\mathbb{C}$ irreduzibel und damit nach dem Fundamentalsatz linear; also ist $[a:\mathbb{C}] = 1$ und damit bereits $a \in \mathbb{C}$. Auf ähnliche Art zeigt man, dass die einzige echte algebraische Körpererweiterung von $\mathbb{R}$ der Körper der komplexen Zahlen ist.

Beachte aber, dass es natürlich (viele) *transzendente* Körpererweiterungen von $\mathbb{C}$ gibt, z. B. den Körper der rationalen komplexen Funktionen aus Beispiel 1.2 (c).

Im 1. Satz von Sylow (siehe Satz 7.22) haben wir gesehen, dass zu einer endlichen Gruppe G und einer Primzahlpotenz p^k mit $p^k \mid |G|$ stets eine Untergruppe U von G mit $|U| = p^k$ existiert. Für viele Anwendungen wäre es nun nützlich, noch weitere Angaben über diese Untergruppen machen zu können, z. B. über deren Anzahl. Wenn wir z. B. wüssten, dass es genau eine Untergruppe der Ordnung p^k gibt, so wüssten wir damit nach [G, Aufgabe 6.9 (b)] auch schon, dass diese ein Normalteiler sein muss.

Für derartige Fragen gibt es noch zwei weitere Sätze von Sylow, die wir jetzt zum Abschluss dieses Kapitels behandeln wollen. Sie werden im wesentlichen mit dem gleichen Argument bewiesen; die Aufteilung in zwei Sätze hat hier lediglich historische Gründe. Besonders starke Aussagen machen sie über die Untergruppen $U \leq G$ mit $|U| = p^k$, für die p^k die maximale Potenz von p ist, die $|G|$ teilt. Derartigen Untergruppen gibt man daher einen besonderen Namen.

Definition 7.27 (p-Gruppen und p-Sylowgruppen)**.** Es sei G eine Gruppe.

(a) Ist $|G| = p^k$ für eine Primzahl p und ein $k \in \mathbb{N}_{>0}$, so heißt G eine **p-Gruppe**.

(b) Es sei $|G| = q\,p^k$ für eine Primzahl p, ein $k \in \mathbb{N}_{>0}$ und ein q mit $p \nmid q$, d. h. der Primfaktor p tritt in $|G|$ genau mit der Vielfachheit k auf. Dann heißt eine Untergruppe $U \leq G$ mit $|U| = p^k$ (also eine p-Untergruppe von G mit maximal möglicher Ordnung) eine **p-Sylowgruppe** bzw. **p-Sylowuntergruppe** von G. Die Menge aller p-Sylowgruppen von G wird mit $\mathrm{Syl}_p(G)$ bezeichnet.

Bemerkung 7.28. Nach dem 1. Satz von Sylow (siehe Satz 7.22) ist offensichtlich $\mathrm{Syl}_p(G) \neq \emptyset$ für jeden Primteiler p der Ordnung einer endlichen Gruppe G.

Satz 7.29 (2. Satz von Sylow). *Es seien G eine Gruppe und p ein Primteiler von $|G|$. Dann gilt:*

(a) *Jede p-Untergruppe von G ist in einer p-Sylowuntergruppe von G enthalten.*

(b) *Alle p-Sylowgruppen von G sind zueinander konjugiert, d. h. für alle $S_1, S_2 \in \mathrm{Syl}_p(G)$ gibt es ein $a \in G$ mit $S_2 = aS_1a^{-1}$.*

Satz 7.30 (3. Satz von Sylow). *Es seien wieder G eine endliche Gruppe und p ein Primteiler von $|G|$. Wir schreiben die Ordnung von G als $|G| = q\,p^k$ für ein $k \in \mathbb{N}_{>0}$ und ein q mit $p \nmid q$. Dann gilt für die Anzahl $s_p := |\mathrm{Syl}_p(G)|$ der p-Sylowgruppen in G:*

(a) $s_p = 1 \mod p$;

(b) $s_p \mid q$.

Beweis von Satz 7.29 und 7.30. Es sei $|G| = q\,p^k$ für eine Primzahl p, ein $k \in \mathbb{N}_{>0}$ und ein q mit $p \nmid q$. Der Beweis beider Sätze besteht im wesentlichen aus einer zweimaligen geschickten Anwendung der Bahnengleichung für geeignete Gruppenoperationen.

Als Erstes lassen wir die Gruppe G durch Konjugation auf der Menge $\mathrm{Syl}_p(G)$ aller p-Sylowgruppen in G operieren, d. h. als $a * U := aUa^{-1}$ für $a \in G$ und $U \in \mathrm{Syl}_p(G)$ (beachte, dass aUa^{-1} nach [G,

Aufgabe 3.7 (a) und Lemma 5.9] in der Tat eine Untergruppe derselben Ordnung wie U, also ebenfalls eine p-Sylowgruppe ist). Für eine im Folgenden fest gewählte p-Sylowgruppe $S \in \mathrm{Syl}_p(G)$ sei nun $\Omega = \{aSa^{-1} : a \in G\} \subset \mathrm{Syl}_p(G)$ die Bahn von S unter dieser Konjugationsoperation. Natürlich ist die Aussage von Satz 7.29 (b) letztlich, dass bereits $\Omega = \mathrm{Syl}_p(G)$ ist, aber das wissen wir momentan noch nicht. Allerdings wissen wir nach der Bahnengleichung aus Satz 7.17 (a), dass

$$|G| = |G_S| \cdot |\Omega| \tag{1}$$

gilt, wobei $G_S = \{a \in G : aSa^{-1} = S\} = \{a \in G : aS = Sa\}$ die Fixgruppe von S ist. Nun ist aber $aS = Sa = S$ für alle $a \in S$, und damit $S \leq G_S$. Nach dem Satz von Lagrange [G, Satz 5.10] ist $|S| = p^k$ also ein Teiler von $|G_S|$. Alle Primfaktoren p von $|G|$ stecken in der Gleichung (1) damit bereits in $|G_S|$, und wir sehen, dass

$$p \nmid |\Omega|. \tag{2}$$

Wir kommen nun zur zweiten bereits angekündigten Gruppenoperation. Hierfür sei H eine beliebige p-Untergruppe von G, die wir wieder durch Konjugation auf p-Sylowgruppen operieren lassen — allerdings diesmal nur auf der Menge Ω aller p-Sylowgruppen, die man aus dem fest gewählten S durch Konjugation mit beliebigen Gruppenelementen erreichen kann. Die Bahnengleichung aus Satz 7.17 (b) lautet für diese Operation

$$|\Omega| = \sum_{i=1}^{n} \frac{|H|}{|H_{S_i}|}, \tag{3}$$

wobei $S_1, \ldots, S_n \in \Omega$ ein Repräsentantensystem der Bahnen und $H_{S_i} = \{a \in H : aS_ia^{-1} = S_i\}$ ist. Da H eine p-Gruppe ist, ist jeder Summand auf der rechten Seite dieser Gleichung eine Potenz von p, also entweder gleich $p^0 = 1$ oder durch p teilbar. Da $|\Omega|$ nach (2) aber nicht durch p teilbar ist, muss demnach mindestens einmal ein Summand 1 vorkommen, d. h. wir sehen:

$$\text{für jede } p\text{-Gruppe } H \text{ in } G \text{ gibt es ein } S_i \in \Omega \text{ mit } H_{S_i} = H. \tag{4}$$

Für ein solches S_i ist also $aS_ia^{-1} = S_i$ für alle $a \in H$. Nach [G, Aufgabe 6.11] folgt hieraus, dass HS_i eine Untergruppe von G ist. Ihre Ordnung ist nach der Produktformel [G, Aufgabe 5.5 (c)] gleich $\frac{|H| \cdot |S_i|}{|H \cap S_i|}$, also insbesondere eine Potenz von p, da H und S_i beides p-Gruppen sind. Damit ist HS_i eine p-Untergruppe von G, die die maximale p-Untergruppe S_i enthält. Es muss demnach $HS_i = S_i$ und damit insbesondere $H \leq HS_i = S_i$ gelten. Also haben wir:

$$\text{für jedes } H \text{ und } S_i \text{ wie in (4) ist } H \leq S_i. \tag{5}$$

Wir können nun alle unsere Ergebnisse zusammensetzen, um den 2. und 3. Satz von Sylow zu beweisen: ist H eine beliebige p-Untergruppe von G, so liegt H nach (4) und (5) in einer p-Sylowgruppe $S_i \in \Omega$, was Satz 7.29 (a) zeigt. Im Spezialfall, wenn H selbst eine p-Sylowgruppe ist und damit genauso viele Elemente wie S_i hat, ist dann natürlich sogar $H = S_i$. Insbesondere ist dann also schon $H \in \Omega$, also $H = aSa^{-1}$ für ein $a \in G$, was Satz 7.29 (b) und außerdem $\Omega = \mathrm{Syl}_p(G)$ beweist. Wir haben demnach $s_p = |\mathrm{Syl}_p(G)| = |\Omega|$. Darüber hinaus gilt für eine p-Sylowgruppe H dann natürlich nur für ein S_i, dass $H \leq S_i$ (nämlich für $S_i = H$). Nach (5) gilt also auch nur für dieses eine S_i, dass $H_{S_i} = H$ und der zugehörige Summand in (3) damit gleich 1 ist. Also hat in (3) genau ein Summand den Wert 1, während alle anderen durch p teilbar sind, d. h. es gilt $s_p = |\Omega| = 1 \mod p$ und damit Satz 7.30 (a). Nach (1) ist schließlich $s_p = |\Omega| \mid |G| = q\,p^k$; da s_p wegen $s_p = 1 \mod p$ keinen Primfaktor p enthalten kann also $s_p \mid q$, d. h. Satz 7.30 (b). □

Beispiel 7.31. Wir betrachten die 3-Sylowgruppen in der symmetrischen Gruppe S_4. Wegen $|S_4| = 24 = 2^3 \cdot 3$ haben diese jeweils 3 Elemente. Sie sind also zyklisch [G, Satz 6.21 (b)] und werden damit von jeweils einem Element der Ordnung 3, also einem 3-Zykel erzeugt. Die verschiedenen 3-Sylowgruppen von S_4 sind damit

$$U_1 = \langle (1\ 2\ 3) \rangle = \{\mathrm{id}, (1\ 2\ 3), (1\ 3\ 2)\}, \qquad U_2 = \langle (1\ 2\ 4) \rangle = \{\mathrm{id}, (1\ 2\ 4), (1\ 4\ 2)\},$$
$$U_3 = \langle (1\ 3\ 4) \rangle = \{\mathrm{id}, (1\ 3\ 4), (1\ 4\ 3)\}, \qquad U_4 = \langle (2\ 3\ 4) \rangle = \{\mathrm{id}, (2\ 3\ 4), (2\ 4\ 3)\}.$$

Wir hatten in Beispiel 7.19 bereits gesehen, dass alle 3-Zykel und damit auch alle $U_1, \dots, U_4$ zueinander konjugiert sind — was Satz 7.29 (b) in diesem Fall bestätigt. Gemäß Satz 7.30 erfüllt die Anzahl $s_3 = 4$ der 3-Sylowgruppen auch $s_3 = 1 \mod 3$ und $s_3 \mid 2^3 = 8$.

13

Wie bereits angekündigt können wir nun in den Fällen, in denen wir aus dem 3. Satz von Sylow wissen, dass es genau eine Untergruppe einer gegebenen Ordnung gibt, darauf schließen, dass diese dann auch ein Normalteiler sein muss. Dies ist z. B. für die folgenden Gruppenordnungen der Fall.

Folgerung 7.32 (Existenz von Normalteilern)**.** *Es sei G eine Gruppe mit $|G| = q\,p^k$ für ein $k \in \mathbb{N}_{>0}$ und zwei verschiedene Primzahlen p, q mit $q \neq 1 \mod p$. Dann besitzt G genau eine p-Sylowuntergruppe (der Ordnung p^k), und diese ist ein Normalteiler in G.*

Beweis. Nach Satz 7.30 (b) ist die Anzahl s_p der p-Sylowgruppen von G ein Teiler von q und kann damit nur 1 oder q sein. Gleichzeitig gilt nach Satz 7.30 (a) aber auch $s_p = 1 \mod p$; wegen $q \neq 1 \mod p$ ist $s_p = q$ also unmöglich. Damit gibt es genau eine p-Sylowuntergruppe $U \leq G$. Nach [G, Aufgabe 6.9 (b)] ist diese dann auch ein Normalteiler (denn für alle $a \in G$ ist aUa^{-1} wieder eine p-Sylowuntergruppe von G und muss damit gleich U sein). □

Mit Hilfe dieser Existenzaussage für Normalteiler können wir nun für eine weitere Klasse von Gruppenordnungen eine Klassifikation angeben.

Folgerung 7.33 (Klassifikation der Gruppen der Ordnung pq mit $p \neq 1 \mod q$ und $q \neq 1 \mod p$)**.** *Es sei G eine Gruppe mit $|G| = pq$ für zwei verschiedene Primzahlen p, q mit $p \neq 1 \mod q$ und $q \neq 1 \mod p$. Dann ist $G \cong \mathbb{Z}_{pq}$.*

Beweis. Nach Folgerung 7.32 gibt es Normalteiler $U_p, U_q \trianglelefteq G$ mit $|U_p| = p$ und $|U_q| = q$. Beachte, dass $U_p \cap U_q = \{e\}$ gilt, da $|U_p \cap U_q|$ nach dem Satz von Lagrange [G, Satz 5.10] ein Teiler von p und q sein muss.

Wir behaupten nun, dass die Abbildung

$$f : U_p \times U_q \to G, \quad (a,b) \mapsto ab$$

ein Isomorphismus ist.

- f ist ein Morphismus: für alle $a, a' \in U_p$ und $b, b' \in U_q$ ist
$$f((a,b)\cdot(a',b')) = f(aa', bb') = aa'bb' \qquad \text{und} \qquad f(a,b)\cdot f(a',b') = aba'b'.$$
Wir müssen zeigen, dass diese beiden Elemente gleich sind, also dass $a'b = ba'$, d. h. $a'ba'^{-1}b^{-1} = e$ gilt. Da $b \in U_q$ und U_q ein Normalteiler in G ist, ist $a'ba'^{-1} \in U_q$ und damit auch $a'ba'^{-1}b^{-1} \in U_q$. Umgekehrt ist genauso $ba'^{-1}b^{-1} \in U_p$ und damit auch $a'ba'^{-1}b^{-1} \in U_p$. Also ist $a'ba'^{-1}b^{-1} \in U_p \cap U_q = \{e\}$, d. h. f ist ein Morphismus.
- f ist injektiv: ist $(a,b) \in U_p \times U_q$ mit $f(ab) = ab = e$, so ist $a = b^{-1} \in U_p \cap U_q = \{e\}$, also $(a,b) = (e,e)$. Damit ist $\operatorname{Ker} f = \{(e,e)\}$, d. h. f ist injektiv.
- f ist surjektiv: dies folgt nun aus der Injektivität, da $|U_p \times U_q| = |G| = pq$.

Damit ist $G \cong U_p \times U_q$. Da U_p und U_q als Gruppen von Primzahlordnung isomorph zu $\mathbb{Z}_p$ bzw. $\mathbb{Z}_q$ sind [G, Satz 6.21 (b)], ist G also isomorph zu $\mathbb{Z}_p \times \mathbb{Z}_q$ und damit nach dem chinesischen Restsatz [G, Satz 11.22] auch zu $\mathbb{Z}_{pq}$. □

Beispiel 7.34. Nach Folgerung 7.33 ist jede Gruppe der Ordnung $15 = 3 \cdot 5$ isomorph zu $\mathbb{Z}_{15}$, denn $3 \neq 1 \mod 5$ und $5 \neq 1 \mod 3$. Für Gruppen der Ordnung $6 = 2 \cdot 3$ hingegen macht Folgerung 7.33 keine Aussage, da $3 = 1 \mod 2$ — und in der Tat gibt es hier neben $\mathbb{Z}_6$ ja auch noch die nicht-abelsche Gruppe S_3.

Aufgabe 7.35 (Klassifikation der Gruppen der Ordnung $2p$)**.** Es sei G eine Gruppe mit $|G| = 2p$ für eine ungerade Primzahl p. Man zeige:

(a) Hat G kein Element der Ordnung $2p$, so gibt es Elemente $a, b \in G$ mit $\operatorname{ord} a = p$, $\operatorname{ord} b = 2$ und $ba = a^{-1}b$.

(b) G ist entweder isomorph zu $\mathbb{Z}_{2p}$ oder zur Diedergruppe D_{2p} aus [G, Aufgabe 3.16].

Aufgabe 7.36. Zeige, dass A_4 keine Untergruppe der Ordnung 6 besitzt. (Wegen $|A_4| = 12$ ist dies also ein Beispiel dafür, dass zu einer endlichen Gruppe G und einem $n \mid |G|$ nicht notwendig eine Untergruppe $U \leq G$ mit $|U| = n$ existieren muss).

Bemerkung 7.37 (Klassifikation endlicher Gruppen)**.** Wir wollen jetzt noch einmal die Ergebnisse zur Klassifikation endlicher Gruppen zusammenfassen, die wir mit unseren bisherigen Methoden erzielen konnten. Ist G eine endliche Gruppe der Ordnung n, so wissen wir:

- Ist $n = p$ eine Primzahl, so ist $G \cong \mathbb{Z}_p$ [G, Satz 6.21 (b)].
- Ist $n = p^2$ ein Primzahlquadrat, so ist $G \cong \mathbb{Z}_{p^2}$ oder $G \cong \mathbb{Z}_p \times \mathbb{Z}_p$ (Aufgabe 7.21).
- Ist $n = 2p$ für eine ungerade Primzahl p, so ist G isomorph zu $\mathbb{Z}_{2p}$ oder zur Diedergruppe D_{2p} (Aufgabe 7.35).
- Ist $n = pq$ für zwei verschiedene Primzahlen p und q mit $p \neq 1 \mod q$ und $q \neq 1 \mod p$, so ist $G \cong \mathbb{Z}_{pq}$ (Folgerung 7.33).

Für andere Gruppenordnungen ist die grobe Faustregel, dass mit zunehmender Anzahl von (nicht notwendig verschiedenen) Primfaktoren in n sowohl die Anzahl der Gruppen der Ordnung n als auch der Aufwand für den Klassifikationsbeweis schnell ansteigt. In der Tat ist eine Klassifikation endlicher Gruppen für beliebige Gruppenordnungen derzeit nicht bekannt — und aufgrund der Struktur der bisher bekannten Ergebnisse auch kaum zu erwarten. Für „kleine“ Gruppenordnungen (bis etwa 1000) kann man allerdings noch mit einer Mischung aus Computeralgebra und theoretischen Methoden eine vollständige Liste aller Gruppen erzeugen. Die folgende Tabelle zeigt beispielhaft für alle $n < 100$ die Anzahlen der Gruppen der Ordnung n [BE]. Es ist sicher erstaunlich, dass eine so einfache und grundlegende mathematische Struktur wie die einer Gruppe zu solch einer unüberschaubaren Klassifikation führt!

n	0	1	2	3	4	5	6	7	8	9
0		1	1	1	2	1	2	1	5	2
10	2	1	5	1	2	1	14	1	5	1
20	5	2	2	1	15	2	2	5	4	1
30	4	1	51	1	2	1	14	1	2	2
40	14	1	6	1	4	2	2	1	52	2
50	5	1	5	1	15	2	13	2	2	1
60	13	1	2	4	267	1	4	1	5	1
70	4	1	50	1	2	3	4	1	6	1
80	52	15	2	1	15	1	2	1	12	1
90	10	1	4	2	2	1	231	1	5	2

8. Einfache und auflösbare Gruppen

Wir haben am Ende des letzten Kapitels in Bemerkung 7.37 gesehen, dass es praktisch aussichtslos ist, alle endlichen Gruppen klassifizieren zu wollen. Wenn wir ein übersichtlicheres Resultat haben möchten, müssen wir uns also weiter einschränken und nur bestimmte endliche Gruppen untersuchen. Natürlich sollten wir diese Einschränkung aber so vornehmen, dass das Ergebnis hinterher trotzdem noch möglichst vielseitig anwendbar ist.

Die Idee hierfür ist die folgende. Angenommen, wir haben eine endliche Gruppe G, die wir klassifizieren bzw. untersuchen wollen. Wenn G nun einen nicht-trivialen Normalteiler U besitzt, können wir statt G auch erst einmal die kleineren Gruppen U und G/U untersuchen. Da G dann ja die disjunkte Vereinigung aller Nebenklassen von U ist und die Gruppe dieser Nebenklassen gerade G/U ist, können wir in diesem Sinne sagen, dass sich G aus den Gruppen U und G/U „zusammensetzt". Es ist zwar nicht richtig, dass man aus U und G/U die Gruppe G wieder bis auf Isomorphie zurück gewinnen kann, aber dennoch kann man so natürlich viele Informationen über G erhalten, wenn man U und G/U genau kennt.

Diese Strategie lässt sich nun rekursiv fortsetzen: wenn U oder G/U selbst wieder nicht-triviale Normalteiler besitzen, kann man diese wie oben dazu benutzen, um sich auch U oder G/U als aus kleineren Bestandteilen zusammengesetzt vorzustellen. Das Verfahren endet erst bei Gruppen, die keine nicht-trivialen Normalteiler mehr besitzen und die sich daher nicht mehr weiter auf diese Art aufspalten lassen. Gruppen dieser Art bezeichnet man als *einfach* (auch wenn wir in Bemerkung 8.5 noch sehen werden, dass auch diese einfachen Gruppen durchaus sehr kompliziert sein können). In obigem Sinne kann man dann also sagen, dass sich jede endliche Gruppe in einfache Bestandteile zerlegen lässt und es daher für viele Anwendungen ausreicht, die einfachen Gruppen zu klassifizieren.

Wir wollen daher nun kurz diese einfachen Gruppen untersuchen — zumal sie auch eng mit den auflösbaren Gruppen zusammenhängen, die wir später noch für die Untersuchung der Auflösbarkeit von Polynomen aus Problem 0.2 benötigen.

Definition 8.1 (Einfache Gruppen)**.** Eine Gruppe G heißt **einfach**, wenn G keinen nicht-trivialen Normalteiler besitzt, also wenn es kein $U \trianglelefteq G$ gibt mit $U \neq \{e\}$ und $U \neq G$.

Beispiel 8.2. Es sei G eine endliche Gruppe.

(a) Ist $|G| = p$ eine Primzahl, also $G \cong \mathbb{Z}_p$ [G, Satz 6.21 (b)], so besitzt G nach dem Satz von Lagrange [G, Satz 5.10] nicht einmal eine nicht-triviale Untergruppe. Also ist G dann natürlich einfach.

(b) Ist $|G| = q\,p^k$ für ein $k \in \mathbb{N}_{>0}$ und zwei verschiedene Primzahlen p und q mit $q \neq 1 \mod p$, so besitzt G nach Folgerung 7.32 einen Normalteiler der Ordnung p^k und ist somit nicht einfach.

(c) Ist $|G| = 36$, so ist G nicht einfach: nach dem 3. Satz von Sylow aus Satz 7.30 gilt für die Anzahl s_3 der 3-Sylowgruppen von G, dass $s_3 = 1 \mod 3$ und $s_3 \,|\, 4$, also $s_3 = 1$ oder $s_3 = 4$. Wir unterscheiden nun diese beiden Fälle:

- Ist $s_3 = 1$, so ist die einzige 3-Sylowgruppe von G nach [G, Aufgabe 6.9 (b)] ein Normalteiler in G.
- Ist $s_3 = 4$, so operiert G durch Konjugation auf der Menge $\mathrm{Syl}_3(G)$ der 3-Sylowgruppen von G und definiert damit nach Bemerkung 7.12 einen Gruppenhomomorphismus $f : G \to S(\mathrm{Syl}_3(G)) = S_4$. Wegen $|G| = 36 > 24 = |S_4|$ kann dieser natürlich nicht injektiv sein, d. h. es ist $\mathrm{Ker}\, f \neq \{e\}$. Es ist aber auch $\mathrm{Ker}\, f \neq G$, denn andernfalls wäre die Konjugationsoperation trivial, also $aUa^{-1} = U$ für alle $a \in G$ und jede

3-Sylowgruppe U — im Widerspruch zum 2. Satz von Sylow aus Satz 7.29 (b). Da Kerne von Gruppenhomomorphismen immer Normalteiler sind [G, Lemma 6.7], ist $\operatorname{Ker} f$ also ein nicht-trivialer Normalteiler in G.

Aufgabe 8.3. Zeige, dass Gruppen der folgenden Ordnungen nicht einfach sein können:

(a) 42;

(b) 30;

(c) 27.

Wer besonders fleißig ist, kann sogar für jede Zahl $n < 60$, die keine Primzahl ist, zeigen, dass eine Gruppe der Ordnung n nicht einfach sein kann. Hierfür werden keine anderen Methoden benötigt als die in den Fällen (a), (b), (c) oben sowie die aus Beispiel 8.2.

Wie wir jetzt sehen werden, ist damit die kleinste einfache Gruppe, deren Ordnung keine Primzahl ist, die alternierende Gruppe A_5 mit 60 Elementen [G, Beispiel 6.19 (a)].

Satz 8.4. *Die alternierende Gruppe A_5 ist einfach.*

Beweis. Angenommen, es gäbe einen nicht-trivialen Normalteiler $U \trianglelefteq A_5$. Wir unterscheiden drei Fälle:

(a) $|U|$ ist ein Vielfaches von 5. Dann enthält U nach dem 1. Satz von Sylow aus Satz 7.22 eine Untergruppe V der Ordnung 5, also eine 5-Sylowgruppe von A_5. Ist nun $\sigma = (a\ b\ c\ d\ e) \in A_5$ ein 5-Zykel (beachte, dass dieser nach [G, Aufgabe 4.6] auch wirklich Signum 1 hat und damit in A_5 liegt), so ist $\langle \sigma \rangle$ ebenfalls eine 5-Sylowgruppe von A_5 und damit nach Satz 7.29 (b) von der Form $\tau V \tau^{-1}$ für ein $\tau \in A_5$. Damit folgt aber

$$\sigma \in \langle \sigma \rangle = \tau V \tau^{-1} \leq \tau U \tau^{-1} = U,$$

d. h. U enthält sämtliche 5-Zykel. Da man 5-Zykel immer in der Form $(a\ b\ c\ d\ e)$ mit $a = 1$ schreiben kann und jede Permutation der anderen vier Elemente dann einen anderen Zykel liefert, gibt es genau $4! = 24$ solche 5-Zykel. Also enthält U mit der Identität und den 5-Zykeln schon einmal mindestens 25 Elemente.

Da $|U|$ nach dem Satz von Lagrange aber auch ein Teiler von $|A_5| = 60$ sein muss, kommt nur noch $|U| = 30$ in Frage. Damit ist auch 3 ein Teiler von $|U|$, und wir können das obige Argument für die 5-Sylowgruppen wörtlich genauso auch für die 3-Sylowgruppen anwenden, um zu sehen, dass U auch alle 3-Zykel $(a\ b\ c)$ enthalten muss. Die Anzahl solcher 3-Zykel ist $2 \cdot \binom{5}{3} = 20$, da es $\binom{5}{3}$ Möglichkeiten gibt, die Zahlen a, b, c aus der Menge $\{1, \ldots, 5\}$ auszuwählen und es für jede solche Wahl dann genau zwei verschiedene 3-Zykel $(a\ b\ c)$ und $(a\ c\ b)$ gibt. Insgesamt hat U nun also mit der Identität, den 5-Zykeln und den 3-Zykeln schon mindestens $1 + 24 + 20 = 45$ Elemente, im Widerspruch zu $|U| = 30$. Also ist dieser erste Fall, in dem $|U|$ ein Vielfaches von 5 ist, unmöglich.

(b) $|U|$ ist ein Vielfaches von 3. Dies führt man genauso zum Widerspruch wie in Fall (a), nur dass man hier zuerst die 3-Sylowgruppen und danach die 5-Sylowgruppen betrachtet.

(c) $|U|$ ist weder ein Vielfaches von 5 noch von 3. Als Teiler von $|A_5| = 60$ kommen für $|U|$ dann nur noch 2 und 4 in Frage. In jedem Fall enthält U wiederum nach dem 1. Satz von Sylow eine Untergruppe und damit auch ein Element der Ordnung 2. Da die Elemente der Ordnung 2 in A_5 genau die Doppeltranspositionen $(a\ b)(c\ d)$ sind, können wir ohne Einschränkung annehmen, dass $(1\ 2)(3\ 4) \in U$. Dann liegen aber auch die hierzu in A_5 konjugierten Elemente in U, also z. B.

$$(1\ 2\ 5)(1\ 2)(3\ 4)(1\ 2\ 5)^{-1} = (5\ 2)(3\ 4),$$
$$(2\ 1\ 5)(1\ 2)(3\ 4)(2\ 1\ 5)^{-1} = (1\ 5)(3\ 4),$$
$$(3\ 4\ 5)(1\ 2)(3\ 4)(3\ 4\ 5)^{-1} = (1\ 2)(5\ 4).$$

Zusammen mit der Identität muss U also mindestens 5 Elemente enthalten, im Widerspruch zu $|U| \leq 4$.

Insgesamt erhalten wir also in jedem Fall einen Widerspruch. Damit kann A_5 keinen nicht-trivialen Normalteiler besitzen. □

Bemerkung 8.5 (Klassifikation einfacher Gruppen)**.** Wir hatten in Bemerkung 7.37 gesehen, dass die Klassifikation aller endlichen Gruppen modulo Isomorphie praktisch ein aussichtsloses Unterfangen ist. Beschränkt man sich nun mit dem Hintergrund der Einleitung zu diesem Kapitel auf einfache Gruppen, so wird die Situation sofort deutlich überschaubarer: so haben wir z. B. in Beispiel 8.2 und Aufgabe 8.3 gesehen, dass die einfachen Gruppen mit weniger als 60 Elementen genau die zyklischen Gruppen $\mathbb{Z}_p$ von Primzahlordnung sind — während die Tabelle in Bemerkung 7.37 ja zeigt, dass es ohne die Einschränkung der Einfachheit auch für diese kleinen Gruppenordnungen bereits sehr viel mehr verschiedene Gruppen gibt.

In der Tat ist die Klassifikation der einfachen endlichen Gruppen inzwischen ein gelöstes Problem. Wann genau das Problem endgültig gelöst wurde, lässt sich allerdings gar nicht so genau sagen, da sich das gesamte Resultat über unzählige Forschungsarbeiten aus der 2. Hälfte des 20. Jahrhunderts erstreckt, in denen in den ersten Jahren nach der Veröffentlichung immer mal wieder kleine Fehler entdeckt wurden, die dann nachträglich noch korrigiert werden mussten. Auch das Ergebnis der Klassifikation ist so kompliziert, dass wir es hier gar nicht vollständig angeben, sondern nur kurz skizzieren können:

(a) Die zyklischen Gruppen $\mathbb{Z}_p$ für eine Primzahl p sind einfach (siehe Beispiel 8.2 (a)). Man sagt, dass sie eine *Serie* einfacher Gruppen bilden.

(b) Die kleinste einfache Gruppe, die nicht von dieser Form ist, ist die alternierende Gruppe A_5 mit 60 Elementen (siehe Aufgabe 8.3 und Satz 8.4). In der Tat kann man zeigen, dass alle alternierenden Gruppen A_n für $n \geq 5$ einfach sind und damit eine weitere Serie einfacher Gruppen bilden.

(c) Die kleinste einfache Gruppe, die nicht von der Form (a) oder (b) ist, hat Ordnung 168. Es handelt sich hierbei um die multiplikative Gruppe

$$\{A \in \mathrm{Mat}(2 \times 2, \mathbb{Z}_7) : \det A = 1\}/\{E, -E\}$$

aller invertierbaren 2×2-Matrizen mit Determinante 1 über dem Körper $\mathbb{Z}_7$, modulo dem von der negativen Einheitsmatrix erzeugten Normalteiler. Auch dieses Beispiel führt gleich zu einer ganzen Serie einfacher Gruppen, wenn man die Größe der quadratischen Matrizen variiert oder den Grundkörper $\mathbb{Z}_7$ durch einen anderen endlichen Körper ersetzt. Man kann sogar noch auf geeignete Art die Bedingungen an die Matrizen durch andere ersetzen (z. B. $\det A = 1$ durch $A^T \cdot A = E$, so dass man also nur orthogonale Matrizen betrachtet) und erhält so nicht nur eine, sondern insgesamt 16 solcher Serien von einfachen „Matrixgruppen“.

(d) Die kleinste einfache Gruppe, die nicht von der Form (a), (b) oder (c) ist, hat Ordnung 7920. Man wird nun wohl befürchten (und hat dies sicher auch getan, solange man die Klassifikation der einfachen Gruppen noch nicht vollständig gefunden hatte), dass dieses Prinzip immer so weiter geht: immer neue und komplizierter werdende Serien, und immer wieder die nächste Ausnahme. Dem ist allerdings nicht so: das erstaunliche Resultat ist nun, dass es nur noch genau 26 einfache Gruppen gibt, die nicht in die Serien (a), (b) oder (c) passen. Diese Gruppen werden *sporadische Gruppen* genannt. Die größte von ihnen hat übrigens die Ordnung

$$808017424794512875886459904961710757005754368000000000$$

und wird als *Monstergruppe* bezeichnet, während die zweitgrößte mit der Ordnung

$$4154781481226426191177580544000000$$

das *Baby-Monster* genannt wird.

Nach den einfachen Gruppen kommen wir nun zum eng verwandten Konzept der auflösbaren Gruppen. Wie bereits erwähnt wird dies dann letztlich genau der Begriff sein, der in der Gruppentheorie der Auflösbarkeit von Polynomen entspricht.

Definition 8.6 (Auflösbare Gruppen)**.** Eine endliche Gruppe G heißt **auflösbar**, wenn es eine Kette

$$\{e\} = G_0 \trianglelefteq G_1 \trianglelefteq \cdots \trianglelefteq G_n = G$$

von Untergruppen von G gibt, so dass G_{i-1} für alle $i = 1, \ldots, n$ ein Normalteiler in G_i ist und die zugehörigen Faktorgruppen G_i/G_{i-1} abelsch sind.

Bemerkung 8.7.

(a) Beachte bei der Schreibweise von Definition 8.6, dass die Normalteilereigenschaft im Allgemeinen nicht transitiv ist! Die Gruppen in der Kette müssen also z. B. keine Normalteiler in G, sondern lediglich in der jeweils nächsten Gruppe der Kette sein.

(b) Im Sinne der Einleitung zu diesem Kapitel kann man auch bei einer auflösbaren Gruppe sagen, dass sie sich mit der Notation aus Definition 8.6 aus den einzelnen Bestandteilen G_i/G_{i-1} „zusammensetzt“. Man kann sich eine auflösbare Gruppe daher als eine Gruppe vorstellen, die sich in abelsche Anteile aufspalten lässt. Da wir die abelschen Gruppen ja im Hauptsatz über endlich erzeugte abelsche Gruppen aus Folgerung 7.4 vollständig klassifiziert haben, ist diese Aufspaltung hier also besonders einfach.

Beispiel 8.8.

(a) Natürlich ist jede abelsche Gruppe G auflösbar, da wir hier ja die triviale Kette $\{e\} \trianglelefteq G$ nehmen können.

(b) Die symmetrische Gruppe S_3 ist auflösbar, denn in der Kette

$$\{\mathrm{id}\} \trianglelefteq A_3 \trianglelefteq S_3$$

sind A_3 (mit 3 Elementen) und S_3/A_3 (mit 2 Elementen) als Gruppen von Primzahlordnung beide zyklisch [G, Satz 6.21 (b)] und damit insbesondere abelsch.

(c) Ist G einfach und nicht abelsch, so kann G nicht auflösbar sein: die triviale Kette wie in (a) ist dann ja nicht zulässig, und andere kann es nicht geben, da G überhaupt keine nicht-trivialen Normalteiler besitzt. Insbesondere folgt aus Satz 8.4 also, dass die alternierende Gruppe A_5 nicht auflösbar ist.

Um weitere Beispiele auflösbarer und nicht auflösbarer Gruppen einfacher angeben zu können, brauchen wir zunächst ein paar einfache Eigenschaften auflösbarer Gruppen.

Aufgabe 8.9 (Eigenschaften auflösbarer Gruppen)**.** Es sei G eine endliche Gruppe. Man zeige:

(a) G ist genau dann auflösbar, wenn es eine Kette

$$\{e\} = G_0 \trianglelefteq G_1 \trianglelefteq \cdots \trianglelefteq G_n = G$$

gibt, so dass $|G_i/G_{i-1}|$ für alle i eine Primzahl ist.

(Hinweis: Zeige mit Hilfe von Folgerung 7.7, dass sich eine Kette mit abelschen Quotienten wie in Definition 8.6 stets zu einer Kette verfeinern lässt, in der die Quotienten Primzahlordnung haben.)

(b) Ist G auflösbar und $U \leq G$, so ist auch U auflösbar.

(c) Ist $U \trianglelefteq G$, so ist G genau dann auflösbar, wenn U und G/U auflösbar sind.

Folgerung 8.10.

(a) *Jede Gruppe mit weniger als* 60 *Elementen ist auflösbar.*

(b) *Die symmetrischen und alternierenden Gruppen S_n und A_n sind genau für $n \leq 4$ auflösbar.*

Beweis.

(a) Es sei G eine Gruppe mit $|G| = n < 60$. Wir zeigen mit Induktion über n, dass G auflösbar ist; der Induktionsanfang für $n = 1$ ist natürlich trivial.

Ist n eine Primzahl, so ist $G \cong \mathbb{Z}_n$ [G, Satz 6.21 (b)], also insbesondere abelsch und damit auch auflösbar. Andernfalls ist G nach Aufgabe 8.3 nicht einfach und besitzt daher einen nicht-trivialen Normalteiler U. Nach Induktionsvoraussetzung sind U und G/U dann auflösbar, mit Aufgabe 8.9 (c) also auch G.

(b) Der Fall $n \leq 4$ wird durch (a) abgedeckt. Für $n \geq 5$ hingegen enthalten sowohl S_n als auch A_n die alternierende Gruppe A_5 als Untergruppe. Da A_5 nach Beispiel 8.8 (c) nicht auflösbar ist, können nach Aufgabe 8.9 (b) also auch S_n und A_n für $n \geq 5$ nicht auflösbar sein. □

Wir wollen nun unsere Ergebnisse zu auflösbaren Gruppen anwenden, um Aussagen über die Auflösbarkeit von Polynomen zu beweisen. Es sei dazu $f = t^n + a_{n-1}t^{n-1} + \cdots + a_1 t + a_0 \in \mathbb{C}[t]$ ein komplexes Polynom und $K = \mathbb{Q}(a_0, \ldots, a_{n-1})$. Wir erinnern uns daran, dass wir f in Definition 1.20 auflösbar genannt haben, wenn sich alle Nullstellen von f aus K mit Hilfe der Körperoperationen und komplexem Wurzelziehen exakt berechnen lassen, also wenn es eine Radikalerweiterung

$$K = K_0 \leq K_1 \leq \cdots \leq K_n = L$$

von K in $\mathbb{C}$ gibt, so dass L alle Nullstellen und damit den Zerfällungskörper von f über K enthält.

Formal sieht dieses Kriterium fast genauso aus wie das der Konstruierbarkeit mit Zirkel und Lineal in Beispiel 1.23. Allerdings besteht ein wesentlicher Unterschied darin, dass wir im Fall der Konstruktionen mit Zirkel und Lineal nur 2-Radikalerweiterungen zugelassen haben, was zu der einfachen numerischen Bedingung geführt hat, dass der Grad von L (und damit auch von allen Elementen von L) über K eine Zweierpotenz sein musste (siehe Folgerung 2.22 und Beispiel 2.23). Im nun vorliegenden Fall der Auflösbarkeit haben wir dagegen keine solche Gradbeschränkung und können daher auch kein analoges einfaches numerisches Kriterium für die Auflösbarkeit von f erwarten.

Die entscheidende Beobachtung zur Lösung dieses Problems ist nun, dass eine einfache m-Radikalerweiterung nach Aufgabe 5.20 stets eine *abelsche* Galoisgruppe besitzt (zumindest unter der technischen Zusatzvoraussetzung, dass der Grundkörper bereits die m-ten Einheitswurzeln enthält — wir werden gleich aber sehen, dass diese Voraussetzung kein größeres Problem darstellt). Wir wollen nun zeigen, dass die obige Kette von Zwischenkörpern auf diese Art mit Hilfe der Galoistheorie einer Kette von Gruppen entspricht, von denen jeweils der Quotient von zwei aufeinander folgenden eine abelsche Gruppe ist — was also genau zum Konzept von auflösbaren Gruppen führt.

Lemma 8.11. *Es seien $K \leq L \leq \mathbb{C}$ Körper, so dass L/K eine Radikalerweiterung ist. Ferner sei Z ein Zwischenkörper von L/K, der galoissch über K ist. Dann ist die Galoisgruppe* $\mathrm{Gal}(Z/K)$ *auflösbar.*

Beweis. Nach Definition 1.18 einer Radikalerweiterung gibt es eine Kette

$$K = K_0 \leq K_1 \leq \cdots \leq K_n = L, \qquad (*)$$

so dass jedes K_j/K_{j-1} eine einfache Radikalerweiterung ist.

Als ersten Reduktionsschritt wollen wir zunächst zeigen, dass wir annehmen dürfen, dass jede Körpererweiterung K_j/K_{j-1} in dieser Kette zusätzlich galoissch mit abelscher Galoisgruppe ist. Es sei dazu K_j/K_{j-1} eine einfache m_j-Radikalerweiterung. Mit $m := m_1 \cdot \cdots \cdot m_n$ und $z := e^{\frac{2\pi i}{m}}$ betrachten wir nun statt $(*)$ die Kette

$$K = K_0 \leq K_0(z) \leq K_1(z) \leq \cdots \leq K_n(z) = L(z),$$

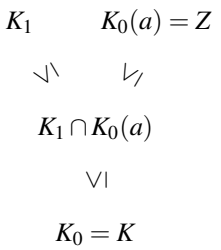
in der wir als Erstes die m-te Einheitswurzel adjungieren. Natürlich sind hier weiterhin alle Körpererweiterungen einfache Radikalerweiterungen (die erste, neue Erweiterung $K_0(z)/K_0$ ist offensichtlich eine einfache m-Radikalerweiterung), und Z ist immer noch ein Zwischenkörper von $L(z)/K$. Weiterhin ist nun jede Körpererweiterung in dieser Kette galoissch mit abelscher Galoisgruppe:

- für die erste Erweiterung $K_0(z)/K_0$ folgt dies aus dem Translationssatz aus Aufgabe 5.21, da $\mathbb{Q}(z)/\mathbb{Q}$ nach Beispiel 5.3 (c) galoissch mit abelscher Galoisgruppe $\mathbb{Z}_m^*$ ist;

- für alle anderen Erweiterungen der Kette ergibt sich dies aus Aufgabe 5.20, die besagt, dass $K_j(z)/K_{j-1}(z)$ galoissch mit abelscher Galoisgruppe (nämlich einer Untergruppe von $\mathbb{Z}_{m_j}$) ist, da $K_{j-1}(z)$ mit $e^{\frac{2\pi i}{m}}$ insbesondere auch die m_j-te Einheitswurzel enthält.

Wir können der Einfachheit halber also annehmen, dass die ursprüngliche Kette $(*)$ bereits so gewählt war, dass jede Körpererweiterung galoissch mit abelscher Galoisgruppe ist. Darüber hinaus können wir nach dem Satz 4.28 vom primitiven Element annehmen, dass $Z = K(a)$ für ein $a \in Z$.

Wir zeigen die Behauptung des Lemmas nun mit Induktion über n; der Induktionsanfang für $n = 0$ ist trivial. Es sei also $n > 0$. Wir betrachten wie im Bild rechts dargestellt den Körper $K_1 \cap K_0(a)$ als Zwischenkörper der beiden Erweiterungen K_1/K_0 und Z/K.



Wir beginnen mit der linken Erweiterung K_1/K_0, die nach unserem Reduktionsschritt galoissch mit abelscher Galoisgruppe ist. Die in der Galois-Korrespondenz zum Zwischenkörper $K_1 \cap K_0(a)$ gehörige Untergruppe von $\mathrm{Gal}(K_1/K_0)$ ist damit natürlich automatisch ein Normalteiler. Nach Satz 6.14 ist die im Bild untere Körpererweiterung $K_1 \cap K_0(a)/K_0$ damit ebenfalls galoissch, und ihre Galoisgruppe ist als Faktorgruppe der abelschen Gruppe $\mathrm{Gal}(K_1/K_0)$ ebenfalls abelsch.

Wir gehen nun zur rechten Körpererweiterung Z/K über, die ja nach Voraussetzung des Lemmas galoissch ist. Da wir die untere Körpererweiterung $K_1 \cap K_0(a)/K_0$ gerade als galoissch erkannt haben, können wir wiederum mit Satz 6.14 schließen, dass die zum Zwischenkörper $K_1 \cap K_0(a)$ gehörige Untergruppe $\mathrm{Gal}(Z/K_1 \cap K_0(a))$ von $\mathrm{Gal}(Z/K)$ ein Normalteiler ist, und dass

$$\mathrm{Gal}(K_1 \cap K_0(a)/K_0) \;=\; \mathrm{Gal}(Z/K) \;/\; \mathrm{Gal}(Z/K_1 \cap K_0(a)).$$

Um die Auflösbarkeit von $\mathrm{Gal}(Z/K)$ zu beweisen, genügt es nach Aufgabe 8.9 (c) also, die Auflösbarkeit der beiden Gruppen $\mathrm{Gal}(K_1 \cap K_0(a)/K_0)$ und $\mathrm{Gal}(Z/K_1 \cap K_0(a))$ zu zeigen:

- $\mathrm{Gal}(K_1 \cap K_0(a)/K_0)$ ist nach Beispiel 8.8 (a) auflösbar, denn von dieser Gruppe haben wir oben ja bereits gesehen, dass sie abelsch ist.
- $\mathrm{Gal}(Z/K_1 \cap K_0(a)) = \mathrm{Gal}(K_0(a)/K_1 \cap K_0(a))$ ist nach dem Translationssatz aus Aufgabe 5.21 isomorph zu $\mathrm{Gal}(K_1(a)/K_1)$. Diese Gruppe ist nun aber nach Induktionsvoraussetzung auflösbar, denn $K_1(a)$ ist einerseits nach Aufgabe 5.21 galoissch über K_1, und andererseits ein Zwischenkörper der $(n-1)$-stufigen Radikalerweiterung $K_1 \leq \cdots \leq K_n = L$.

Damit ist $\mathrm{Gal}(Z/K)$ auflösbar. □

Folgerung 8.12 (Auflösbarkeit von Polynomen und Gruppen)**.** *Es seien $f = t^n + a_{n-1}t^{n-1} + \cdots + a_1 t + a_0 \in \mathbb{C}[t]$ ein komplexes Polynom und $K = \mathbb{Q}(a_0, \ldots, a_{n-1})$. Ist f dann auflösbar im Sinne von Definition 1.20, so ist die Galoisgruppe des Zerfällungskörpers von f über K auflösbar im Sinne von Definition 8.6.*

Beweis. Es sei $Z \leq \mathbb{C}$ der Zerfällungskörper von f über K. Weil f auflösbar ist, ist Z nach Definition 1.20 in einer Radikalerweiterung L von K enthalten. Da Z als Zerfällungskörper außerdem nach Satz 5.8 galoissch über K ist, folgt die Behauptung nun sofort aus Lemma 8.11. □

Beispiel 8.13. Es sei $f \in \mathbb{Q}[t]$ ein rationales Polynom vom Grad $n \geq 5$. Nach Lemma 5.11 (a) ist die Galoisgruppe $\mathrm{Gal}(f)$ dann eine Untergruppe von S_n. Ist sogar $\mathrm{Gal}(f) = S_n$, so ist $\mathrm{Gal}(f)$ damit nach Folgerung 8.10 (b) nicht auflösbar, d. h. nach Folgerung 8.12 ist dann auch f nicht auflösbar. In der Tat ist dies für die meisten Polynome vom Grad $n \geq 5$ der Fall. Die folgende Aufgabe gibt ein konkretes Beispiel dafür.

Aufgabe 8.14 (Beispiel für ein nicht-auflösbares Polynom)**.** Für das Polynom $f = t^5 - 80t + 2 \in \mathbb{Q}[t]$ zeige man:

(a) f ist irreduzibel und hat genau drei reelle Nullstellen.

(b) $\mathrm{Gal}(f)$ ist isomorph zu einer Untergruppe $U \leq S_5$ mit $(1\ 2\ 3\ 4\ 5) \in U$ und $(1\ 2) \in U$.

(c) $\mathrm{Gal}(f) \cong S_5$.

Nach Beispiel 8.13 ist f damit also nicht auflösbar.

Bemerkung 8.15. Man kann zeigen, dass in Folgerung 8.12 auch die Umkehrung gilt, dass ein Polynom also genau dann auflösbar ist, wenn sein Zerfällungskörper eine auflösbare Galoisgruppe besitzt [B, Kapitel 6.1]. Da Untergruppen von S_n für $n \leq 4$ nach Folgerung 8.10 (a) stets auflösbar sind, bedeutet dies also, dass Polynome vom Grad höchstens 4 immer auflösbar sind — was man aber natürlich auch schon ohne die Hilfe der Galoistheorie wusste, da in diesen Fällen nach Problem 0.2 ja konkrete Lösungsformeln existieren.

14

Literatur

[B] S. Bosch, *Algebra*, Springer (2006)

[BE] H. Besche und B. Eick: *The groups of order at most 1000 except 512 and 768*, J. Symb. Comput. **27** (4), 405–413 (1999)

[G] A. Gathmann: *Algebraische Strukturen*, Vorlesungsskript TU Kaiserslautern (2019/20), https://www.mathematik.uni-kl.de/~gathmann/ags

Index