Vorlesungskript

Algebra

SS 2018

Christian Sevenheck

Fakultät für Mathematik

TU Chemnitz

vorläufige Fassung, 6. Juli 2018

Fehler und Bemerkungen bitte an : christian.sevenheck@mathematik.tu-chemnitz.de

Inhaltsverzeichnis

Kapitel 1

Einführung

In diesem Kapitel wollen wir einen Überblick über den in dieser Vorlesung behandelten Stoff geben. Wir werden einige Begriffe „ad hoc“ definieren und einige Sätze ohne Beweis formulieren, alle diese Aussagen werden im späteren Verlauf der Vorlesung sauber behandelt. Hier soll es darum gehen, zu den Hauptergebnissen vorzustoßen und zu skizzieren, welche Hilfsmittel dabei benötigt werden.
Ganz grob gesprochen werden wir fundamentale algebraische Strukturen, wie Gruppen, Ringe und Körper betrachten. Diese spielen in fast allen Teilen der Mathematik eine große Rolle. Der Fokus dieser Vorlesung soll in der Beantwortung von Problemen, die seit der Antike bekannt sind, liegen. Obwohl alle diese Probleme sehr einfach zu formulieren sind, konnten sie erst im 19. Jahrhundert vollständig gelöst werden.
Mehrere dieser klassischen Probleme lassen sich unter dem Stichwort „Konstruktion mit Zirkel und Lineal“ zusammenfassen. Um dies präzise formulieren zu können, beginnen wir mit der folgenden Definition.

Definition 1.1. *Gegeben sei eine Teilmenge $M_0 \subset \mathbb{R}^2$, von der wir*

$$|M_0| := (\text{Anzahl der Elemente von } M_0) \geq 2$$

voraussetzen ($|M_0| = \infty$ ist erlaubt). Wir definieren induktiv Mengen M_i durch folgende Vorschrift: Zeichne beliebige Geraden zwischen 2 Punkten aus M_{i-1} sowie beliebige Kreise um Punkte aus M_{i-1}, welche einen weiteren Punkt aus M_{i-1} auf der Kreislinie enthalten. Dann setze

$$M_i := M_{i-1} \cup \{\text{beliebige Schnittpunkte solcher Geraden und Kreise}\}.$$

Wir sagen, dass ein Punkt $x \in \mathbb{R}^2$ aus der Ausgangsmenge M_0 mit Zirkel und Lineal konstruierbar ist, falls es ein $i \in \mathbb{N} = \{0, 1, 2, \ldots\}$ gibt, so dass $x \in M_i$ ist.

Mit dieser Definition können wir die folgenden Probleme, welche seit der Antike bekannt sind, formulieren.

Definition 1.2. *In den folgenden Konstruktionsproblemen definieren die gegebenen Daten eine Menge $M_0 \subset \mathbb{R}^2$. Das gesuchte Objekt „zu konstruieren“ soll bedeuten, im Sinne von Definition 1.1 eine Menge M_i mit Zirkel und Lineal zu konstruieren, so dass das gesuchte Objekt Teilmenge von M_i ist.*

1. *(Quadratur des Kreises) Kann man aus einem gegebenen Kreis ein Quadrat gleicher Fläche konstruieren ?*

2. *(Delisches Problem) Kann man zu einem Würfel mit vorgegebener Seitenlänge einen Würfel mit doppeltem Volumen konstruieren, d.h., kann man die Seitenlänge diese Würfels konstruieren ?*

3. *(Regelmäßiges n-Eck) Sei $n \in \mathbb{N}$ vorgegeben. Kann man dann ein regelmäßiges n-Eck konstruieren, dessen Eckpunkte in einem gegebenen Kreis liegen ?*

4. *(Winkeldreiteilung) Kann man einen vorgegebenen Winkel dreiteilen?*

Um Antworten auf diese Probleme geben zu können, führen wir jetzt einige Begriffe über Körper und Körpererweiterungen ein, welche im Verlauf der Vorlesung ausführlich diskutiert werden.

Definition 1.3. *Sei $A \subset \mathbb{C} \cong \mathbb{R}^2$ eine Teilmenge. Wir definieren*

$$\mathbb{Q}(A) := \bigcap_{\substack{\mathbb{Q}\subset K\subset\mathbb{C} \\ A\subset K \\ K \text{ Körper}}} K$$

als den kleinsten Körper, welcher $\mathbb{Q}$ und A enthält und in $\mathbb{C}$ liegt. (Es ist leicht zu sehen, dass die oben definierte Menge $\mathbb{Q}(A)$ tatsächlich ein Körper ist). $\mathbb{Q}(A)$ heißt Körpererweiterung von $\mathbb{Q}$.
Allgemeiner kann man für $\mathbb{Q} \subset A \subset B \subset \mathbb{C}$ die Körpererweiterung $\mathbb{Q}(A) \subset \mathbb{Q}(B)$ definieren. $\mathbb{Q}(B)$ ist in natürlicher Weise ein $\mathbb{Q}(A)$-Vektorraum, und man nennt $[\mathbb{Q}(B) : \mathbb{Q}(A)] := \dim_{\mathbb{Q}(A)}(\mathbb{Q}(B))$ den Grad dieser Körpererweiterung.
Falls $A = \{a_1, \ldots, a_k\}$ endlich ist, schreiben wir $\mathbb{Q}(A) = \mathbb{Q}(a_1, \ldots, a_k)$ und sagen, dass $\mathbb{Q}(a_1, \ldots, a_k)$ aus $\mathbb{Q}$ durch Adjunktion von $a_1, \ldots, a_k$ entsteht. Eine Zahl $c \in \mathbb{C}$ heißt algebraisch, *falls $[\mathbb{Q}(c) : \mathbb{Q}] < \infty$ ist, sonst heißt c* transzendent.

Die folgenden Resultate über Körpererweiterungen werden (teilweise) in der Vorlesung bewiesen, und erlauben es, die oben gestellten geometrischen Probleme zu lösen.

Satz 1.4. *1. $\mathbb{Q}(\sqrt{2}) = \mathbb{Q} + \mathbb{Q}\sqrt{2} = \left\{a + b\sqrt{2} \,|\, a, b \in \mathbb{Q}\right\}$, $[\mathbb{Q}(\sqrt{2}) : \mathbb{Q}] = 2$*

2. $\mathbb{Q}(\sqrt[3]{2}) = \mathbb{Q} + \mathbb{Q}\sqrt[3]{2} + \mathbb{Q}(\sqrt[3]{2})^2$, $[\mathbb{Q}(\sqrt[3]{2}) : \mathbb{Q}] = 3$

3. π und $\sqrt{\pi}$ sind transzendent.

4. Für $\alpha \in [0, 2\pi)$ ist $[\mathbb{Q}(\cos\frac{\alpha}{3}, \cos\alpha) : \mathbb{Q}(\cos\alpha)] = 3$.

5. Es ist $[\mathbb{Q}(e^{2\pi i\frac{1}{n}}) : \mathbb{Q}] = \varphi(n)$, hierbei ist $\varphi : \mathbb{N}_{>0} \to \mathbb{N}$ die Eulersche φ-Funktion, *definiert durch*

$$\varphi(n) := \left|\{a \in \{0, \ldots, n-1\} \,|\, \mathrm{ggT}(a, n) = 1\}\right|.$$

Beweis. Wir werden hier nur einige Bemerkungen zu den Beweisen machen, die Details kommen später.

1. Wegen $\mathbb{Q}(\sqrt{2}) = \mathbb{Q} + \mathbb{Q}\sqrt{2}$ ist $\{1, \sqrt{2}\}$ ein Erzeugendensystem des $\mathbb{Q}$-Vektorraumes $\mathbb{Q}(\sqrt{2})$ und auch linear unabhängig, daher ist $\dim_{\mathbb{Q}} \mathbb{Q}(\sqrt{2}) = 2$.

2. Analog zu 1.

3. Dies ist der Satz von Lindemann (1882), den wir in dieser Vorlesung nicht beweisen werden.

4. Es gilt
$$\cos(3x) = 4\cos^3(x) - 3\cos(x),$$
also
$$\cos^3\frac{\alpha}{3} - \frac{3}{4}\cos\frac{\alpha}{3} - \frac{1}{4}\cos\alpha = 0.$$
Also sind alle Potenzen $\cos^k\frac{\alpha}{3}$ für $k > 2$ als Linearkombination von 1, $\cos^2\frac{\alpha}{3}$ und $\cos\frac{\alpha}{3}$ mit Koeffizienten aus $\mathbb{Q}(\cos(\alpha))$ darstellbar. Daher folgt
$$\mathbb{Q}\left(\cos\frac{\alpha}{3}, \cos\alpha\right) = \mathbb{Q}(\cos\alpha)\cdot 1 + \mathbb{Q}(\cos\alpha)\cdot\left(\cos\frac{\alpha}{3}\right) + \mathbb{Q}(\cos\alpha)\cdot\left(\cos^2\frac{\alpha}{3}\right),$$
und daher ist $\left\{1, \cos\frac{\alpha}{3}, \cos^2\frac{\alpha}{3}\right\}$ eine $\mathbb{Q}(\cos\alpha)$-Basis von $\mathbb{Q}\left(\cos\frac{\alpha}{3}, \cos\alpha\right)$.

5. Wir werden später sehen, dass das Polynom

$$\Phi_n(x) := \prod_{\substack{a \text{ mit } 0<a\leq n \\ \mathrm{ggT}(a,n)=1}} \left(x - e^{2\pi i \frac{a}{n}}\right)$$

rationale Koeffizienten hat. Natürlich hat es Grad $\varphi(n)$, und $e^{2\pi i \frac{1}{n}}$ ist eine Nullstelle von Φ_n, außerdem gibt es (wie wir auch später sehen werden) kein Polynom kleineren Grades mit rationalen Koeffizienten, welches $e^{2\pi i \frac{1}{n}}$ als Nullstelle hat. Daraus folgt (auch das kommt später), dass $[\mathbb{Q}(e^{2\pi i \frac{1}{n}}) : \mathbb{Q}] = \varphi(n)$ gilt.

□

Der folgende Satz beantwortet die Fragen aus Definition 1.2.

Satz 1.5. *1. Sei $M \subset \mathbb{R}^2$ gegeben und sei ein Punkt $x \in \mathbb{R}^2$ im Sinne von Definition 1.1 mit Zirkel und Lineal aus M konstruierbar. Dann gilt*

$$[\mathbb{Q}(M \cup \{x\}) : \mathbb{Q}(M)] = 2^m$$

für ein $m \in \mathbb{N}$.

2. Die Quadratur des Kreises ist nicht lösbar.

3. Das Delische Problem ist nicht lösbar

4. Einen Winkel kann man nicht mit Zirkel und Lineal dritteln.

5. Falls das reguläre n-Eck konstruierbar ist, dann gilt $\varphi(n) = 2^m$ für ein $m \in \mathbb{N}$. (Tatsächlich sind diese beiden Bedingungen äquivalent).

Beweis. 1. Das ist der schwierigste Teil dieses Satzes, der Beweis wird am Ende der Vorlesung gegeben.

2. Ein Kreis mit Radius 1 hat Flächeinhalt π, also müßte man ein Quadrat der Seitenlänge $\sqrt{\pi}$ konstruieren, wegen Satz 1.4, 3. ist aber $[\mathbb{Q}(\sqrt{\pi}) : \mathbb{Q}] = \infty$.

3. Analog zum Punkt 2. müsste man hier den Abstand $\sqrt[3]{2}$ konstruieren, aber dies wiederspricht der Aussage $[\mathbb{Q}(\sqrt[3]{2}) : \mathbb{Q}] = 3$, denn 3 ist keine Zweierpotenz.

4. Auch hier folgt aus $[\mathbb{Q}(\cos\frac{\alpha}{3}, \cos\alpha), \mathbb{Q}(\cos\alpha)] = 3$, dass es keine Lösung geben kann.

5. Dies ist eine Konsequenz von $[\mathbb{Q}(e^{2\pi i \frac{1}{n}}) : \mathbb{Q}] = \varphi(n)$, denn das reguläre n-Eck mit Ecken auf einem Kreis mit Radius 1 hat einen Eckpunkt bei $e^{2\pi i \frac{1}{n}} \in \mathbb{C} \cong \mathbb{R}^2$.

□

Wir wollen nun ein zweites fundamentales Problem beschreiben, welches wir in dieser Vorlesung behandeln werden. Es geht um die Lösbarkeit von algebraischen Gleichungen, oder anders formuliert, um die Frage, inwieweit man Formeln zur Berechnung von Nullstellen von Polynomen angeben kann. Wir starten mit der folgenden Definition.

Definition 1.6. *Sei $f(x) = x^n + a_{n-1} \cdot x^{n-1} + \ldots + a_1 \cdot x + a_0 \in \mathbb{Q}[x]$ ein Polynom in einer Variablen mit Koeffizienten aus $\mathbb{Q}$. Die Nullstellen von f seien $x_1, \ldots, x_n \in \mathbb{C}$, d.h., es gilt $f(x) = (x - x_1) \cdot \ldots \cdot (x - x_n)$. Wir sagen, dass f durch Radikale lösbar ist, wenn die Nullstellen $x_1, \ldots, x_n$ aus den Koeffizienten $a_0, \ldots, a_{n-1}$ durch Anwenden der Grundrechenoperationen **und** durch Wurzelziehen bestimmbar sind.*

Für Polynome kleinen Grades kann man explizite Formeln für die Lösungen angeben, dies wollen wir jetzt behandeln, uns dabei aber auf die Fälle $\mathrm{Grad}(f) < 4$ beschränken.

Satz 1.7. *Quadratische Gleichungen $x^2 + px + q = 0$ lassen sich mit der Formel*

$$x_{1,2} = -\frac{p}{2} \pm \sqrt{\frac{p^2}{4} - q} \tag{1.1}$$

lösen.

Beweis. Der Beweis ist natürlich wohlbekannt, aber er ist instruktiv, um die gleich zu behandelnden Formeln für das Lösen von kubischen Gleichungen zu verstehen. Wir ersetzen in der Gleichung $x^2 + px + q = 0$ die Variable x durch $y - \frac{p}{2}$, und erhalten

$$x^2 + px + q = \left(y - \frac{p}{2}\right)^2 + p\left(y - \frac{p}{2}\right) + q = y^2 - \frac{p^2}{4} + q$$

Daher ist $x^2+px+q = 0$ äquivalent zu $y^2 = \frac{p^2}{4} - q$, also $y_{1,2} = \pm\sqrt{\frac{p^2}{4} - q}$ und daher $x_{1,2} = -\frac{p}{2} \pm \sqrt{\frac{p^2}{4} - q}$. □

Im folgenden Satz leiten wir eine ähnliche, aber deutlich kompliziertere Formel für Gleichungen dritten Grades her.

Satz 1.8 (Cardanosche Formeln)**.** *Sei eine Gleichung $x^3 + ax^2 + bx + c = 0$ gegeben. Wir transformieren diese mittels $y := x + \frac{a}{3}$ auf $y^3 + py + q = 0$, mit*

$$p = -\frac{1}{3}a^2 + b, \quad q = \frac{2}{27}a^3 - \frac{1}{3}ab + c$$

Dann sind die Lösungen von $y^3 + py + q = 0$ gegeben durch

$$y_0 = u_0 + v_0, \quad y_1 = u_1 + v_1, \quad y_2 = u_2 + v_2 \tag{1.2}$$

mit

$$\begin{aligned} u_0 &= \sqrt[3]{-\tfrac{q}{2} + \sqrt{\left(\tfrac{q}{2}\right)^2 + \left(\tfrac{p}{3}\right)^3}}, & v_0 &= \sqrt[3]{-\tfrac{q}{2} - \sqrt{\left(\tfrac{q}{2}\right)^2 + \left(\tfrac{p}{3}\right)^3}} \\ u_1 &= u_0 \cdot \zeta, & v_1 &= v_0 \cdot \zeta^2 \\ u_2 &= u_0 \cdot \zeta^2, & v_2 &= v_0 \cdot \zeta \end{aligned} \tag{1.3}$$

wobei $\zeta = e^{2\pi i \frac{1}{3}}$ eine sogenannte primitive dritte Einheitswurzel ist.

Beweis. Wir verwenden die Formel

$$(u+v)^3 = u^3 + 3u^2v + 3uv^2 + v^3 = 3uv(u+v) + (u^3 + v^3)$$

aus der

$$(u+v)^3 + (-3uv) \cdot (u+v) + (-u^3 - v^3) = 0$$

folgt, d.h., die Zahl $u+v$ erfüllt die Gleichung $x^3+px+q = 0$, wenn wir $p = -3uv$ und $q = -u^3 - v^3$ setzen. Umgekehrt sucht man also für gegebene p und q Zahlen u und v, so dass $p = -3uv$ und $q = -u^3 - v^3$ gilt. Wegen $u^3v^3 = \left(-\frac{p}{3}\right)^3$ und $-q = u^3 + v^3$ sind die Zahlen u^3 und v^3 Lösung der quadratischen Gleichung $z^2 + qz - \left(\frac{p}{3}\right)^3 = 0$, also gilt

$$u^3, v^3 = -\frac{q}{2} \pm \sqrt{\left(\frac{q}{2}\right)^2 + \left(\frac{p}{3}\right)^3}$$

und das führt zu den Cardanoschen Formeln, hierbei sind die 3-ten Einheitswurzeln als Faktoren so verteilt, dass für $i = 0, 1, 2$ wirklich $3u_iv_i = -p$ gilt, und nicht nur $u_i^3v_i^3 = \left(-\frac{p}{3}\right)^3$. □

Zu erwähnen bleibt, dass es auch ähnliche Lösungsformeln für Gleichungen vom Grad 4 gibt, welche wir aus Zeitgründen nicht herleiten. Auch in ihnen werden nur Grundrechenoperationen sowie Wurzelziehen verwendet. Wir werden gleich noch einen abstrakten Ansatz kennenlernen, welcher zeigt, dass es für alle Gleichungen vom Grad ≤ 4 solcher Lösungsformeln geben muss.
Wir wollen noch einen wichtigen Begriff einführen, welcher die Struktur der Lösungsmenge von Gleichungen vom Grad 2 oder 3 bestimmt.

Definition-Lemma 1.9 (Diskriminante)**.** *1. Die Diskriminante des Polynoms x^2+px+q ist $D := \frac{p^2}{4}-q$. Wenn $x^2+px+q = (x-x_1)(x-x_2)$ gilt, dann ist $D = \frac{1}{4}(x_1-x_2)^2$, also ist $D=0$ genau dann, wenn $x_1 = x_2$ ist.*

Im Spezialfall, dass $p, q \in \mathbb{R}$ sind, gilt darüber hinaus:

(a) $D \geq 0$ genau dann, wenn $x_1, x_2 \in \mathbb{R}$.

(b) $D \leq 0$ genau dann, wenn $x_1 = \overline{x}_2$.

2. Die Diskriminante des Polynoms x^3+px+q ist $D := \left(\frac{q}{2}\right)^2 + \left(\frac{p}{3}\right)^3$. Seien y_0, y_1, y_2 Lösungen, gegeben durch Formel (1.2), dann ist

$$\sqrt{D} = -\frac{\sqrt{3}}{18} \cdot \sqrt{-1} \cdot (y_0-y_1)(y_0-y_2)(y_1-y_2),$$

insbesondere ist $D=0$ genau dann, wenn es $i \neq j$ mit $y_i = y_j$ gibt.

Seien spezieller $p, q \in \mathbb{R}$, dann gilt

(a) $D \leq 0$ genau dann, wenn alle Lösungen y_i reell sind,

(b) $D > 0$ genau dann, wenn zwei Lösungen komplex konjugiert und nicht reell sind (und die dritte reell ist).

Beweis. 1. Dies ergibt sich sofort aus den Lösungsformeln (Formel (1.1)) für quadratische Gleichungen.

2. Dies ist der Inhalt von Übungsblatt 1., Aufgabe 2.

□

Um die Auflösbarkeit (durch Radikale) von Polynomen bzw. algebraischen Gleichungen beliebigen Grades zu studieren, definieren wir nun ein fundamentales Objekt, welches später (siehe Kapitel 4 und 5) in großer Ausführlichkeit behandelt wird.

Definition 1.10. *Sei $K_1 \subset K_2$ eine Körpererweiterung, d.h., K_1 und K_2 sind Körper, K_1 ist in K_2 enhalten, und die Verknüpfungen $+$ und $\cdot$ sind in beiden Körpern kompatibel. Dann heißt*

$$\mathrm{Gal}(K_2/K_1) := \left\{\phi : K_2 \to K_2 \,|\, \phi \text{ Körperautomorphismus }, \phi_{|K_1} = \mathrm{id}_{K_1}\right\}$$

die Galoisgruppe von K_2/K_1 (mit der Verknüpfung von Automorphismen als Gruppenstruktur).

Der folgende Satz beantwortet die Frage nach der Auflösbarkeit von Polynomgleichungen im Allgemeinen. Wir verschieben den Beweis vollständig auf die hinteren Teile der Vorlesung.

Satz 1.11. *Gegeben $f(x) = x^n + a_{n-1}x^{n-1} + \ldots + a_1x + a_0 = \prod_{i=1}^n (x-x_i)$,*
$a_i \in \mathbb{Q}$, $x_i \in \mathbb{C}$.
Betrachte $\mathbb{Q}(x_1, \ldots, x_n)/\mathbb{Q}$ und Galoisgruppe $\mathrm{Gal}(\mathbb{Q}(x_1, \ldots, x_n)/\mathbb{Q})$. Dann gilt:

1. $\forall \varphi \in \mathrm{Gal}(\mathbb{Q}(x_1, \ldots, x_n)/\mathbb{Q}) : \exists \sigma \in S_n : \varphi(x_i) = x_{\sigma(i)}$

2. *Die durch*

$$\begin{array}{ccc} \mathrm{Gal}(\mathbb{Q}(x_1,\ldots,x_n)/\mathbb{Q}) & \longrightarrow & S_n \\ \varphi & \longmapsto & \sigma \end{array}$$

definierte Abbildung ist ein injektiver Gruppenhomomorphismus (siehe Definition 2.3).

3. *Es seien die folgenden Voraussetzungen erfüllt:*

   (a) n *ist eine Primzahl,*

   (b) f *ist irreduzibel, d.h. falls* $f = g \cdot h$ *für Polynome mit rationalen Koeffizienten, dann ist* $\mathrm{Grad}(g) = 0$ *oder* $\mathrm{Grad}(h) = 0$,

   (c) $x_1, \ldots, x_{n-2} \in \mathbb{R}$,

   (d) $x_{n-1}, x_n \in \mathbb{C}\backslash\mathbb{R}$ *und* $x_{n-1} = \overline{x}_n$.

   Dann gilt $\mathrm{Gal}(\mathbb{Q}(x_1,\ldots,x_n)/\mathbb{Q}) = S_n$.

   Ein Beispiel für ein solches Polynom ist $f(x) = x^5 - 10x + 5$.

4. *Die Nullstellen* $x_1, \ldots, x_n$ *sind durch Grundrechenoperationen und Wurzelziehen aus den Koeffizienten* $a_0, \ldots, a_{n-1}$ *bestimmbar, d.h., f ist durch Radikale lösbar, genau dann, wenn die Gruppe* $\mathrm{Gal}(\mathbb{Q}(x_1,\ldots,x_n)/\mathbb{Q})$ *auflösbar ist (siehe Definition 2.41).*

5. S_n *ist auflösbar für* $n \leq 4$, *und nicht auflösbar für* $n \geq 5$ *(siehe Korollar 2.47).*

6. *Also existieren für Gleichungen vom Grad* $2, 3, 4$ *Lösungsformeln, welche nur Grundrechenoperationen und Wurzelziehen beinhalten, für Gleichungen vom Grad größer oder gleich* 5 *hingegen im Allgemeinen nicht mehr. Beispielweise kann man die Nullstellen von* $f(x) = x^5 - 10x + 5$ *nicht aus den rationalen Zahlen durch (iteriertes) Wurzelziehen und die Grundrechenoperationen bestimmen.*

Kapitel 2

Gruppentheorie

Wir wollen nun mit dem systematischen Aufbau der Theorie beginnen, welche wir zur Lösung der im ersten Kapitel skizzierten Probleme benötigen. Wir werden uns zunächst etwas ausführlicher mit Gruppen beschäftigen, und dabei insbesondere endliche Gruppen und noch spezieller die Permutationsgruppen studieren.

2.1 Gruppen, Homomorphismen und Faktorgruppen

Wir starten mit der Definition einer Gruppe, welche bereits aus der Linearen Algebra bekannt ist.

Definition 2.1. *Sei G eine nichtleere Menge. Eine Verknüpfung auf G ist eine Abbildung*

$$\begin{array}{rcl} G \times G & \longrightarrow & G \\ (a,b) & \longmapsto & a \circ b \end{array}$$

Hierbei ist $\circ$ das Verknüpfungssymbol (für das man auch ein anderes Zeichen wählen kann), dies ist aber nur eine andere Schreibweise für die gegebene Abbildung $G \times G \to G$. Eine Gruppe ist ein Paar $(G, \circ)$ bestehend aus einer nichtleeren Menge G und einer Verknüpfung $\circ$, so dass die folgenden Eigenschaften gelten:

1. *(**Assoziativität**): $\forall a, b, c \in G : a \circ (b \circ c) = (a \circ b) \circ c$.*
2. *(**neutrales Element**): $\exists e \in G : \forall a \in G : a \circ e = e \circ a = a$.*
3. *(**inverses Element**): $\forall a \in G : \exists a' \in G : a \circ a' = a' \circ a = e$.*

Falls noch für alle $a, b, \in G$ gilt, dass $a \circ b = b \circ a$ ist, so nennt man $(G, \circ)$ eine abelsche Gruppe. Oft bezeichnet man eine Gruppe nur mit G, wenn klar ist, welche Verknüpfung gemeint ist.

Wie man leicht zeigt (Übung), ist das inverse Element eines Elementes eindeutig bestimmt, und wird daher mit a^{-1} bezeichnet.
Bei einer abelschen Gruppe wählt man oft das Symbol $+$ für die Verknüpfung und man sagt, die Verknüpfung wird *additiv* geschrieben. Das inverse Element von a heißt dann $-a$, und man setzt für $a \in G$ und für $n \in \mathbb{Z}$

$$\begin{array}{rcll} n \cdot a & := & \underbrace{a + a + \ldots + a}_{n\text{-mal}} & \text{falls} \quad n \in \mathbb{N}\backslash\{0\} \\ n \cdot a & := & -((-n) \cdot a) & \text{falls} \quad -n \in \mathbb{N}\backslash\{0\} \\ 0 \cdot a & := & e & \end{array}$$

Analog schreibt man für beliebige Gruppen die Verknüpfung oft *multiplikativ* (d.h., das Verknüpfungssymbol ist $\cdot$), und dann setzt man $a^n := \underbrace{a \cdot a \cdot \ldots \cdot a}_{n\text{-mal}}$ für $n > 0$, $a^n := (a^{-n})^{-1}$ für $n < 0$ und $a^0 := e$.

Wir diskutieren jetzt Beispiele für Gruppen:

1. Die ganzen Zahlen $\mathbb{Z}$ sind zusammen mit der üblichen Addition eine abelsche Gruppe, geschrieben $(\mathbb{Z}, +)$. Analog sind $(\mathbb{Q}, +)$ (rationale Zahlen), $(\mathbb{R}, +)$ (reelle Zahlen) und $(\mathbb{C}, +)$ (komplexe Zahlen) jeweils zusammen mit der Addition abelsche Gruppen.

2. Sei $\mathbb{Q}^* := \mathbb{Q}\backslash\{0\}$, dann ist $(\mathbb{Q}^*, \cdot)$ eine abelsche Gruppe. Analog definiert man die abelschen Gruppen $(\mathbb{R}^*, \cdot)$ und $(\mathbb{C}^*, \cdot)$. Hingegen bilden $\mathbb{Q}$, $\mathbb{R}$ und $\mathbb{C}$ keine Gruppe bezüglich der Multiplikation, denn 0 hat kein inverses Element.

3. Analog zum letzten Beispiel ist $(\mathbb{Q}_{>0}, \cdot)$ eine abelsche Gruppe, wobei $\mathbb{Q}_{>0} := \{q \in Q \mid q > 0\}$ ist. Genauso erhält man die abelsche Gruppe $(\mathbb{R}_{>0}, \cdot)$.

4. Sei X eine beliebige Menge. Dann sei

$$\mathrm{Bij}(X) := \mathrm{Perm}(X) := \{\psi : X \to X \mid \psi \text{ ist bijektiv}\}$$

   Mit der Verknüpfung von Abbildungen (meistens auch mit $\circ$ bezeichnet) wird $\mathrm{Bij}(X)$ zu einer Gruppe. Falls $X = \{1, 2, \ldots, n\}$, dann schreibt man auch $S_n := \mathrm{Bij}(X)$. Für $|X| > 2$ ist $\mathrm{Bij}(X)$ nicht abelsch, dies gilt also insbesondere für S_n für $n > 2$.

   $(S_n, \circ)$ heißt symmetrische Gruppe, die Elemente von S_n heißen Permutationen. Es gibt verschiedene Arten, eine Permutation darzustellen, häufig schreibt man $\sigma \in S_n$ als

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

   wobei man benutzt, dass eine Abbildung eindeutig durch die Angabe ihrer Bilder bestimmt ist.

5. Sei K ein Körper und

$$\mathrm{Gl}_n(K) := \{A \in \mathrm{Mat}(n \times n, K) \mid \det(A) \neq 0\}$$

   Menge der invertierbaren Matrizen (Einträge aus K).

   Dann ist $(\mathrm{Gl}_n(K), \cdot)$ Gruppe, für $n > 1$ im Allgemeinen nicht-abelsch.

   Falls $|K| = \infty \quad \Longrightarrow \quad \mathrm{Gl}_n(K)$ Beispiel für nicht-abelsche Gruppe mit unendlich vielen Elementen.

Definition 2.2. *Sei $(G, \circ)$ eine Gruppe, und $\emptyset \neq U \subset G$ eine Teilmenge.*
Dann heißt U Untergruppe von G, falls gilt:

1. $\forall a, b \in U \Longrightarrow a \circ b \in U$,
2. $\forall a \in U \Longrightarrow a^{-1} \in U$

Fall $U \subset G$ Untergruppe ist, schreibt man oft kurz $U < G$.

Man sieht leicht: Ist $U \subset G$ eine Untergruppe, so ist $e \in U$, denn wegen $\emptyset \neq U$ gibt es $a \in U$, und dann ist wegen 2. auch $a^{-1} \in U$, und dann wegen 1. auch $e = a \circ a^{-1} \in U$. Genauso leicht zeigt man: Ist $U \subset G$ eine Untergruppe, so ist $(U, \circ)$ eine Gruppe (Übung). Der nächste wichtige Begriff ist der des Gruppenhomomorphismus, welcher es erlaubt, zwei Gruppen miteinander zu vergleichen.

Definition 2.3. *Seien $(G, \circ)$ und $(H, *)$ Gruppen. Eine Abbildung $f : G \longrightarrow H$ heißt Gruppenhomomorphismus, falls gilt*

$$\forall a, b \in G : f(a \circ b) = f(a) * f(b)$$

Sei $f : (G, \circ) \longrightarrow (H, *)$ ein Gruppenhomomorphismus. Dann heißt f ein Gruppenmonomorphismus, falls f injektiv ist, ein Gruppenepimorphismus, falls f surjektiv ist und ein Gruppenisomorphismus, falls f bijektiv ist. Falls $G = H$ und $\circ = *$ ist, so nennt man f einen Gruppenhomomorphismus $f : (G, \circ) \to (G, \circ)$ einen Gruppenendomorphismus, und falls dann f bijektiv ist, einen Gruppenautomorphismus.

Sei $f : G \to H$ ein Gruppenhomomorphismus. Dann definieren wir Kern und Bild von f als

$$\begin{aligned} \ker(f) &:= \{a \in G \mid f(a) = e_H\} \\ \mathrm{Im}(f) &:= f(G) = \{b \in H \mid \exists a \in G, f(a) = b\}, \end{aligned}$$

hierbei ist e_H das neutrale Element von H. Man sieht leicht, dass der Kern eines Gruppenhomomorphismus $f : G \to H$ eine Untergruppe von G und das Bild eine Untergruppe von H ist. Änhlich einfach, aber nützlich ist das folgende Lemma.

Lemma 2.4. *Sei $f : (G, \circ) \to (H, *)$ ein Gruppenhomomorphismus. Dann gilt*

1. *$f(e_G) = e_H$,*
2. *Für alle $a \in G$ ist $f(a)^{-1} = f(a^{-1})$,*
3. *f ist injektiv, d.h., ein Gruppenmonomorphismus,genau dann, wenn $ker(f) = \{e_G\}$ gilt.*

Beweis. Es ist $f(e_G) = f(e_G \circ e_G) = f(e_G) * f(e_G)$, also ist $e_H = f(e_G)$. Dann gilt $e_H = f(e_G) = f(a \circ a^{-1}) = f(a) * f(a^{-1})$, also $f(a^{-1}) = f(a)^{-1}$.
Falls f injektiv ist, muss natürlich $\ker(f) = \{e_G\}$ gelten, weil eben kein weiteres Element aus G auf e_H abgebildet werden kann. Sei andererseits f beliebig und gelte $\ker(f) = \{e_G\}$. Seien $a, b \in G$ mit $f(a) = f(b)$. Dann ist $e_H = f(a) * f(b)^{-1} = f(a \circ b^{-1})$ und also $a \circ b^{-1} \in \ker(f)$, also $a \circ b^{-1} = e_G$ nach Voraussetzung. Somit gilt $a = b$, und f ist injektiv. □

Wir beschließen diesen Abschnitt mit einigen Beispielen für Untergruppen und Gruppenhomomorphismen.

1. Sei $U \subset G$ eine Untergruppe, dann ist die Abbildung $U \to G$, $g \mapsto g$ ein injektiver Gruppenhomomorphismus.

2. Sei G eine Gruppe und $a \in G$. Dann definiert

$$\begin{aligned} \varphi : \mathbb{Z} &\longrightarrow G \\ n &\longmapsto a^n \end{aligned}$$

   einen Gruppenhomomorphismus. Das Bild von φ heißt die von a in G erzeugte Untergruppe und wird manchmal mit $\langle a \rangle$ bezeichnet.

3. Sei $G = \mathbb{Z}$, und $m \in \mathbb{N}$, dann definieren wir

$$m\mathbb{Z} := \{k \cdot m \mid k \in \mathbb{Z}\}$$

   Dann ist $(m\mathbb{Z}, +)$ eine Untergruppe von $(\mathbb{Z}, +)$, denn wenn $km, k'm \in m\mathbb{Z}$ liegen, dann natürlich auch $km + k'm = (k + k')m$ sowie $-km = (-k)m$. Tatsächlich werden wir später zeigen, dass alle Untergruppen von $\mathbb{Z}$ von der Gestalt $m\mathbb{Z}$ sind.

4. Die Abbildung

$$\begin{aligned} \exp : (\mathbb{R}, +) &\longrightarrow (\mathbb{R}_{>0}, \cdot) \\ x &\longmapsto e^x \end{aligned}$$

   ist ein Gruppenhomomorphismus wegen des Exponentialgesetzes $e^{x+y} = e^x \cdot e^y$. Analog ist die komplexe Exponentialfunktion

$$\begin{aligned} \exp : (\mathbb{C}, +) &\longrightarrow (\mathbb{C}^*, \cdot) \\ x &\longmapsto e^x \end{aligned}$$

   ein Gruppenhomomorphismus.

5. Sei G eine Gruppe und $a \in G$. Dann ist die Abbildung

$$\begin{array}{rcl} \gamma_a : G & \longrightarrow & G \\ g & \longmapsto & a \cdot g \cdot a^{-1} \end{array}$$

ein Automorphismus von G, genannt Konjugation mit a. Wie man leicht zeigt (Übung), ist dann die Abbildung

$$\begin{array}{rcl} \Gamma : G & \longrightarrow & \mathrm{Aut}(G) \\ a & \longmapsto & \gamma_a \end{array}$$

ein Gruppenhomomorphismus, hierbei ist $(\mathrm{Aut}(G), \circ)$ die Menge der Automorphismen von G, welche zusammen mit der Komposition eine Gruppe bilden.

6. Für einen Körper K ist die Determinantenabbildung

$$\det : \mathrm{Gl}_n(K) \longrightarrow K^* := K \backslash \{0\} \; ; \; A \mapsto \det(A)$$

wegen der Determinantenmultiplikationsformel $\det(A \cdot B) = \det(A) \cdot \det(B)$ ein Gruppenhomomorphismus. Für alle $a \in K^*$ ist außerdem

$$A := \begin{pmatrix} a & 0 & \dots & 0 \\ 0 & 1 & 0 & 0 \\ \vdots & 0 & \ddots & \vdots \\ 0 & 0 & \dots & 1 \end{pmatrix} \in \mathrm{Gl}_n(K)$$

und es gilt $\det(A) = a$. Daher ist $\det : \mathrm{Gl}_n(K) \to K^*$ surjektiv. Man definiert

$$\mathrm{Sl}_n(K) := \ker(\det) = \{A \in \mathrm{Mat}(n \times n, K) \mid \det(A) = 1\}.$$

Nun wollen wir Untergruppen von gegebenen Gruppen genauer untersuchen. Dazu brauchen wir einen neuen Begriff.

Definition 2.5. *Sei G eine Gruppe und $U \subset G$ eine Untergruppe. Dann heißt für jedes $a \in G$ die Menge*

$$aU := \{a \cdot u \mid u \in U\}$$

die Linksnebenklasse von U in G zu a, analog nennt man

$$Ua := \{u \cdot a \mid u \in U\}$$

die Rechtsnebenklasse von U in G zu a.

Wir formulieren den folgenden Satz für Linksnebenklassen, ein analoges Ergebnis gilt für Rechtsnebenklassen.

Satz 2.6. *1. Sei $a \in G$ und $l_a : G \to G$ definiert durch $l_a(g) := ag$ (dies ist kein Gruppenhomomorphismus). Dann ist l_a eine Bijektion.*

2. Sei $U < G$, dann sind alle Linksnebenklassen von U in G gleichmächtig (d.h., zwischen zwei Linksnebenklassen zu zwei Elementen a und b aus G gibt es eine Bijektion, insbesondere haben sie gleich viele Elemente, falls die Anzahl der Elemente von U endlich ist).

3. Für alle $a, b \in G$ ist entweder $aU = bU$ oder $aU \cap bU = \emptyset$.

4. G ist die disjunkte Vereinigung der Linksnebenklassen von U.

Beweis. 1. Umkehrabbildung zu l_a gegeben durch $l_{a^{-1}}$.

2. Wir haben $aU = l_a(U)$. Also definiert Komposition

$$l_b \circ l_{a^{-1}} : aU \to bU$$

eine Bijektion.

3. Es reicht, die Äquivalenz der Aussagen $aU = bU$ und $aU \cap bU \neq \emptyset$ zu zeigen. Wegen $U \neq \emptyset$ ist die Implikation $aU = bU \Longrightarrow aU \cap bU \neq \emptyset$ klar.

Sei andererseits $aU \cap bU \neq \emptyset$, dann haben wir: $x \in aU \cap bU \Longrightarrow \exists u_1, u_2 \in U : au_1 = bu_2 = x \Longrightarrow a = bu_2u_1^{-1} \Longrightarrow a \in bU \Longrightarrow aU \subset bU$, aber wegen $b = au_1u_2^{-1}$ folgt auch $bU \subset aU$.

4. Dies folgt direkt aus Punkt 3.

□

Wir bezeichnen mit G/U die Menge der Linksnebenklassen von U in G. Für eine endliche Gruppe G bezeichnen wir mit $\mathrm{ord}(G)$ die Anzahl der Elemente von G, genannt die Ordnung von G. Dann haben wir folgende wichtige Konsequenz.

Korollar 2.7 (Satz von Lagrange)**.** *Sei G endlich und $U \subset G$ eine Untergruppe. Dann sind sowohl U als auch G/U endlich und es gilt*

$$\mathrm{ord}(G) = (G : U) \cdot \mathrm{ord}(U),$$

wobei $(G : U)$ die Anzahl der Linksnebenklassen von U in G, also die Anzahl der Elemente von G/U bezeichnet. $(G : U)$ wird der Index von U in G genannt.

Beweis. Natürlich folgt aus $\mathrm{ord}(G) < \infty$, dass $|U| < \infty$ gilt. Andererseits ist dann wegen Satz 2.6, 4. auch G/U endlich, und wegen Punkt 2. und Punkt 4. in Satz 2.6 gilt die zu beweisende Formel. □

Es ist leicht zu sehen, dass die bijektive Abbildung $G \to G, g \mapsto g^{-1}$ die Linksnebenklasse aU auf die Rechtsnebenklasse Ua^{-1} abbildet und eine Bijektion $G/U \longrightarrow U\backslash G := \{Ug \mid g \in G\}$ der Menge der Linksnebenklassen auf die Menge der Rechtsnebenklassen induziert. Daher gelten alle obigen Aussagen auch entsprechend für Rechtsnebenklassen.
Wir wollen jetzt die Menge der Linksnebenklassen in natürlicher Weise mit einer Gruppenstruktur versehen. Dies ist jedoch nicht immer möglich, sondern nur unter einer Zusatzbedingung an die gegebene Untergruppe U.

Definition 2.8. *Sei $U < G$ eine Untergruppe, dann heißt U Normalteiler von G, falls für alle $a \in G$ gilt: $aU = Ua$, d.h., falls Recht- und Linksnebenklassen zu a von U in G übereinstimmen. Man schreibt dann auch $U \lhd G$.*

Eine äquivialente Definition eines Normalteilers ist, dass $aUa^{-1} = U$ für alle $a \in G$ gilt, tatsächlich ist hierzu die Aussage, dass für alle $a \in G$ die Inklusion $aUa^{-1} \subset U$ gilt, äquivalent, denn dies ist dasselbe wie $aU \subset Ua$, aber wenn dies für alle Gruppenelemente a gelten soll, dann folgt auch $a^{-1}U \subset Ua^{-1}$, also $Ua \subset aU$.
Man sieht sofort, dass alle Untergruppen U einer abelschen Gruppe G auch Normalteiler von G sind. Eine wichtige weitere Quelle für Normalteiler sind Gruppenhomomorphismen, wie die folgende Aussage zeigt.

Lemma 2.9. *Sei $f : G \to H$ ein Gruppenhomomorphismus, dann ist $U := \ker(f)$ ein Normalteiler in G.*

Beweis. Wie schon oben erwähnt, gilt $\ker(f) < G$. Sei jetzt $a \in G$, dann ist zu zeigen, dass $a \cdot \ker(f) \cdot a^{-1} \subset \ker(f)$ gilt, dass also für alle $g \in \ker(f)$ auch das Element $a \cdot g \cdot a^{-1}$ im Kern von f liegt. Da aber f ein Gruppenhomomorphismus ist, gilt $f(a \cdot g \cdot a^{-1}) = f(a) \cdot f(g) \cdot f(a)^{-1} = f(a) \cdot e_H \cdot f(a)^{-1} = e_H$. □

Wir kommen nun zur angekündigten Konstruktion einer Gruppenstruktur auf G/U. Hierfür führen wir folgende Schreibweise ein: Für eine Gruppe G und Teilmengen $X, Y \subset G$ sei $X \cdot Y := \{x \cdot y \,|x \in X, y \in Y\}$. Analog definiert man das Produkt mehrerer Mengen. Ist dann $U \lhd G$ ein Normalteiler, gilt für alle $a, b \in G$ die folgende Gleichheit von Teilmengen von G:

$$(aU) \cdot (bU) = \{a\} \cdot (Ub) \cdot U \overset{(*)}{=} \{a\} \cdot (bU) \cdot U = \{a \cdot b\} \cdot U \cdot U = (ab) \cdot U, \tag{2.1}$$

wobei die Gleichheit $(*)$ aus der Normalteilereigenschaft von U folgt. Für die letzte Gleichheit benutzt man $U \cdot U \subset U$ (gilt, weil, $U < G$) und $U \subset U \cdot \{e_G\} \subset U \cdot U$. Dies bedeutet, das die Verknüpfung

$$\begin{aligned} G/U \times G/U &\longrightarrow G/U \\ (aU, bU) &\longmapsto (ab)U \end{aligned}$$

wohldefiniert ist. Genauer, sei $aU = a'U$, dann ist $(aU) \cdot (bU) = (a'U) \cdot (bU)$ und daher wegen Gleichung (2.1) eben auch $(ab) \cdot U = (a'b) \cdot U$. Das gleiche Argument gilt für Nebenklassen $bU = b'U$. Da die so definierte Verknüpfung auf G/U von der gegeben Verknüpfung auf G definiert wird, erfüllt sie die Gruppenaxiome und wir haben damit folgende Aussage.

Satz 2.10. *Sei G eine Gruppe und $U \lhd G$ ein Normalteiler, dann definiert die Verknüpfung $(aU, bU) \mapsto (ab)U$ eine Gruppenstruktur auf der Menge G/U der Linksnebenklassen von U in G.*
Sei $\pi : G \longrightarrow G/U$ die Abbildung gegeben durch $g \mapsto gU$, dann ist π ein Gruppenhomomorphismus bezüglich der gegebenen Verknüpfung auf G und der gerade definierten Verknüpfung auf G/U. π ist surjektiv, und wir haben $\ker(\pi) = U$.

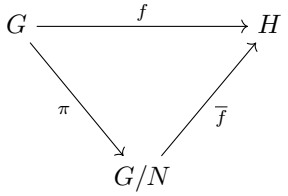
Beweis. Das π ein Gruppenhomomorphismus ist, folgt direkt daraus, dass die Verknüpfung auf G/U durch die Verknüpfung auf G definiert wird. Die Surjektivität gilt, weil jedes Element $aU \in G/U$ als Urbild $a \in G$ hat. Das neutrale Element der Gruppe G/U ist nach der obigen Definition der Verknüpfung auf G/U gerade die Nebenklasse $e_G U = U$, also ist $\ker(\pi) = U$. □

In der obigen Situation nennt man G/U die Faktor- oder Restklassen- oder Quotientengruppe von G nach U. Man sieht leicht: G/U ist die Menge der Äquivalenzklassen der Relation $a \sim b \;\Leftrightarrow ab^{-1} \in U$. Daher schreibt man die Elemente von G/U, also die Nebenklassen aU von U in G oft auch als Restklassen, also z.B. $[a]$, oder auch $\overline{a}$. Ein wichtiges Beispiel der obigen Konstruktion ist der Fall $G = \mathbb{Z}$, dies ist eine abelsche Gruppe, also sind alle Untergruppen automatische Normalteiler. Sei $m \in \mathbb{N}$, dann ist mit $U = m\mathbb{Z}$ also die Quotientengruppe $G/U = \mathbb{Z}/m\mathbb{Z}$ definiert. Dies ist eine endliche Gruppe, wir haben

$$\mathbb{Z}/m\mathbb{Z} = \{[0], [1], \ldots, [m-1]\}$$

Das folgende Lemma zeigt, dass die oben konstruierten Faktorgruppen eine sogenannte universelle Eigenschaft haben

Satz 2.11 (Homomorphiesatz)**.** *Sei ein Gruppenhomomorphismus $f : G \to H$ gegeben. Sei $N \lhd G$ ein Normalteiler, welcher in* $\ker(f)$ *enthalten ist. Dann existiert ein eindeutig bestimmter Gruppenhomomorphismus $\overline{f} : G/N \to H$, so dass das folgende Diagramm kommutativ ist:*



so dass also $f = \overline{f} \circ \pi$ gilt. Dann ist außerdem

$$\mathrm{Im}(f) = \mathrm{Im}(\overline{f}) \qquad \ker(\overline{f}) = \pi(\ker(f)) \qquad \ker(f) = \pi^{-1}(\ker(\overline{f}))$$

Außerdem ist $\overline{f}$ injektiv, genau dann, wenn $N = \ker(f)$ gilt. Falls f surjektiv ist, so existiert also ein kanonischer (d.h., nicht von irgendwelchen Wahlen abhängender) Gruppenisomorphismus $G/\ker(f) \cong H$.

Beweis. Wir zeigen zunächst die Existenz von $\overline{f}$: Man definiert einfach $\overline{f}(aN) := f(a)$, und jetzt ist zu zeigen, dass diese Definition nicht von der Wahl des Repräsentanten a der Nebenklasse aN abhängt. Sei also $b \in aN$, dann ist $ba^{-1} \in N \subset \ker(f)$, also $f(ab^{-1}) = f(a)f(b)^{-1} = e_H$, also $f(a) = f(b)$, und somit ist $\overline{f}$ wohldefiniert. Natürlich ist $\overline{f}$ mit dieser Definition ein Gruppenhomomorphismus, weil die Gruppenstruktur auf G/N durch die von G definiert wird, und weil f ein Gruppenhomomorphismus ist. Ebenfalls folgt aus der Definition von $\overline{f}$, dass $f(a) = \overline{f}(aN) = (\overline{f} \circ \pi)(a)$ für alle $a \in G$ gilt, also $f = \overline{f} \circ \pi$, und damit ist $\overline{f}$ auch eindeutig bestimmt.
Da π surjektiv ist, folgt sofort $\mathrm{Im}(f) = \mathrm{Im}(\overline{f})$, aber auch $\ker(\overline{f}) = \pi(\ker(f))$. Schließlich ist $\ker(f) = \pi^{-1}(\ker(\overline{f}))$ eine direkte Konsequenz der Kommutativität $f = \overline{f} \circ \pi$. $N = \ker(f)$ ist wegen $\ker(\overline{f}) = \pi(\ker(f))$ zur Injektivität von $\overline{f}$ äquivalent. Ist dann noch f surjektiv, so auch $\overline{f}$ (wegen $\mathrm{Im}(f) = \mathrm{Im}(\overline{f})$), also liefert $\overline{f}$ den gesuchten Isomorphismus. □

Korollar 2.12 (1. Isomorphiesatz)**.** *Sei G eine Gruppe und $H < G$, $N \lhd G$. Dann gilt*

1. *$HN < G$*
2. *$N \lhd HN$*
3. *$H \cap N \lhd H$*
4. *Die Abbildung*

$$\begin{array}{ccc} H/H \cap N & \longrightarrow & HN/N \\ h & \longmapsto & h \cdot 1 \end{array}$$

ist ein Gruppenisomorphismus.

Beweis.

1. Seien $h_1, h_2 \in H$,$n_1, n_2 \in N$, dann ist

$$(h_1n_1)(h_2n_2) \in h_1n_1h_2N \overset{N \lhd G}{=} h_1n_1Nh_2 \subset h_1Nh_2 \overset{N \lhd G}{=} h_1h_2N \subset HN.$$

   Außerdem ist $(h_1n_1)^{-1} = n_1^{-1} \cdot h_1^{-1} \in Nh_1^{-1} = h_1^{-1}N \subset HN$, also ist HN Untergruppe von G.

2. Der offensichtliche injektive Gruppenhomomorphismus $N \hookrightarrow HN$ identifiziert N mit einer Untergruppe von HN. Zu zeigen ist, dass diese (welche wir auch mit N bezeichnen) auch ein Normalteiler von HN ist. Dies folgt direkt aus der Normalteilereigenschaft von N in G.

3. Betrachte den Gruppenhomomorphismus $f : H \hookrightarrow HN \twoheadrightarrow HN/N$, welcher durch die Komposition der injektiven Abbildung $H \hookrightarrow HN; h \mapsto h \cdot 1$ mit der (surjektiven) kanonischen Projektion $HN \twoheadrightarrow HN/N$ gegeben ist. Jetzt zeigen wir $\ker(f) = H \cap N$, dann gilt $H \cap N \lhd H$ wegen Lemma 2.9. Offensichtlich ist $\ker(f) \supset H \cap N$, sei andererseits $h \in \ker(f)$, d.h., die Restklasse von $h \cdot 1$ in HN/N ist das Einselement dieser Faktorgruppe, dann muss $h \in N$ liegen.

4. Da für alle $n \in N$ gilt, dass $nN = N$ ist, kann man jede Restklasse $[h \cdot n] \in HN/N$, also eine Linksnebenklasse $hnN = hN$ durch ein Element $h = h \cdot 1 \in HN$ repräsentieren, also ist $f : H \to HN/N$ surjektiv. Damit induziert es nach Satz 2.11 einen Isomorphismus $\overline{f} : H/\ker(f) \to HN/N$, und wir haben eben $\ker(f) = H \cap N$ bewiesen.

□

Wir zitieren noch den 2. Isomorphiesatz, dessen Beweis eine Übungsaufgabe ist.

Satz 2.13 (2. Isomorphiesatz)**.** *$H \lhd G$, $K \lhd G$, sei $K \subset H$, dann $H/K \lhd G/K$ und*

$$(G/K)/(H/K) \cong G/H.$$

Eine wichtige Klasse von Gruppen sind die zyklischen Gruppen, welche wir jetzt studieren wollen. Wir hatten schon erwähnt, dass die von einem Element x in einer gegebenen Gruppe G erzeugte Untergruppe die Gruppe ist, welche aus allen x^n für $n \in \mathbb{Z}$ besteht, und mit $\langle x \rangle$ bezeichnet wird. Allgemeiner definieren wir:

Definition 2.14. *Eine Gruppe G heißt zyklisch, wenn es einen surjektiven Gruppenhomomorphismus $\varphi : \mathbb{Z} \longrightarrow G$ gibt. Dann heißt $\varphi(1)$ der Erzeuger von G.*

Natürlich ist die Gruppe $(\mathbb{Z}, +)$ selbst zyklisch. Die wichtigsten, und, wie wir gleich sehen werden, bis auf Isomorphie auch die einzigen Beispiele für endliche zyklische Gruppen sind die Quotienten $\mathbb{Z}/m\mathbb{Z}$ für $m \in \mathbb{N}$. Zur Erinnerung:

$$\mathbb{Z}/m\mathbb{Z} = \{[0], [1], [2], \ldots, [m-2], [m-1]\}$$

Diese Quotientengruppen werden auch mit C_m bezeichnet.
Die Restklasse $[m]$ ist bereits wieder gleich der Restklasse $[0]$, allgemeiner ist $[a] = [b]$ in $\mathbb{Z}/m\mathbb{Z}$ genau dann, wenn $a - b$ durch m teilbar ist. Die Verknüpfung auf $\mathbb{Z}/m\mathbb{Z}$ ist, da von der Addition auf $\mathbb{Z}$ induziert, einfach die Addition von zwei Repräsentanten, modulo m genommen.
Der folgende Satz klassifiziert nun alle zyklischen Gruppen bis auf Isomorphie.

Satz 2.15. *1. Sei $U < \mathbb{Z}$ eine Untergruppe, dann ist $U = m\mathbb{Z}$ für ein $m \in \mathbb{N}$.*

2. Sei G eine zyklische Gruppe. Dann gilt

$$G \cong \begin{cases} \mathbb{Z} & \text{falls} \quad \operatorname{ord}(G) = \infty \\ \mathbb{Z}/m\mathbb{Z} & \text{falls} \quad \operatorname{ord}(G) = m \end{cases}$$

3. Sei G zyklisch mit $\operatorname{ord}(G) = m$. Dann existiert für jedes $k|m$ genau eine Untergruppe $U < G$ mit $\operatorname{ord}(U) = k$ (und $(G : U) = \frac{m}{k}$), U ist ebenfalls zyklisch, d.h. $U \cong \mathbb{Z}/k\mathbb{Z}$. Dies sind die einzigen Untergruppen von G.

Beweis. 1. Falls U die Untergruppe ist, die nur die $0 \in \mathbb{Z}$ enthält, dann ist die Aussage offensichtlich richtig, mit $m = 0$. Sei also $\{0\} \subsetneq U < \mathbb{Z}$ gegeben, und sei $m \in U \cap \mathbb{N}_{>0}$ minimal gewählt. Man beachte, dass es wegen der Untergruppeneigenschaft positive Element in U geben muss. Wir zeigen nun, dass dann $U = m\mathbb{Z}$ gelten muss. Zunächst folgt wieder aus $U < \mathbb{Z}$, dass $m\mathbb{Z} \subset U$ gilt. Sei andererseits $a \in U$ vorgegeben, dann dividieren wir a mit Rest durch m, d.h., es gibt $q \in \mathbb{Z}$ und $r \in \mathbb{N}$ mit $r < m$, so dass $a = q \cdot m + r$ ist. Dann folgt aus $r = a - qm$, dass auch $r \in U$ gilt, aber wegen $r < m$ und der angenommenen Minimalität von m in $U \cap \mathbb{N}_{>0}$ muss dann $r = 0$ gelten. Also ist $a = qm \in m\mathbb{Z}$.

2. Sei G zyklisch, dann folgt aus Satz 2.11, dass $G \cong \mathbb{Z}/U$, wobei U eine Untergruppe von $\mathbb{Z}$ ist. Nach Punkt 1. ist dann $U = m\mathbb{Z}$, und jetzt ist $m = 0$, falls $\operatorname{ord}(G) = \infty$, dann folgt $G \cong \mathbb{Z}$, und sonst ist $G \cong \mathbb{Z}/m\mathbb{Z}$, mit $m = \operatorname{ord}(G)$.

3. Wir wissen schon, dass $G \cong \mathbb{Z}/m\mathbb{Z}$ gilt, d.h., wir können uns auf das Studium von Untergruppen von $\mathbb{Z}/m\mathbb{Z}$ beschränken. Sei $k|m$, d.h., es gibt $n \in \mathbb{Z}$ mit $m = k \cdot n$. Dann ist offensichtlich die Teilmenge

$$\{[0], [n], [2n], \ldots, [m-n] = [(k-1) \cdot n]\}$$

eine zyklische Untergruppe von $\mathbb{Z}/m\mathbb{Z}$ der Ordnung k. Sie ist isomorph zu $\mathbb{Z}/k\mathbb{Z}$, und hat wegen des Satzes von Lagrange (Korollar 2.7) den Index $\frac{m}{k}$. Es bleibt zu zeigen, dass es keine anderen Untergruppen in $\mathbb{Z}/m\mathbb{Z}$ geben kann. Sei also $U < \mathbb{Z}/m\mathbb{Z}$ beliebig, setze

$$l := \min_{s \in \mathbb{N}_{>0}} ([s] \in U)$$

Offensichtlich gilt dann $\langle [l] \rangle \subset U$. Sei andererseits $[s] \in U$, dann gilt $l|s$, denn sonst dividieren wir s mit Rest durch l, d.h., es gibt $q \in \mathbb{N}$ mit $s = ql + r$, mit $0 < r < l$, aber dann ist notwendig $[r] \in U$, was der Minimalität von l wiederspricht. Also ist l ein Teiler von s, und daher $[s] \in \langle [l] \rangle$, so dass $U = \langle [l] \rangle$ gilt.

□

Für eine beliebige Gruppe G und ein Element $g \in G$ bezeichnen wir mit $\mathrm{ord}(g)$ (Ordnung von g) die Ordnung der von g erzeugten Untergruppe, also

$$\mathrm{ord}(g) := \min\left(k \in \mathbb{N}_{>0} \,|\, g^k = 1\right)$$

Dann gilt der sogenannte *kleine Satz von Fermat*.

Satz 2.16. *Sei G eine endliche Gruppe und $g \in G$, dann gilt $\mathrm{ord}(g) \,|\, \mathrm{ord}(G)$ und insbesondere ist $g^{\mathrm{ord}(G)} = 1$.*

Beweis. Wir setzen $H := \langle g \rangle$ (dann ist $\mathrm{ord}(g) = \mathrm{ord}(H)$) und benutzen den Satz von Lagrange (Korollar 2.7), dann folgt $\mathrm{ord}(g) \,|\, \mathrm{ord}(G)$, und dann ist die erste Aussage offensichtlich, und die zweite folgt sofort aus der ersten. □

Die folgende einfache Konsequenz ist ein erster Schritt in der Klassifikation von gewissen endlichen Gruppen.

Korollar 2.17. *Sei G eine endliche Gruppe mit $\mathrm{ord}(G) = p$, p Primzahl. Dann ist G zyklisch, also isomorph zu $\mathbb{Z}/\mathbb{Z}p$. Jedes Element in $G\backslash\{1\}$ ist ein Erzeugendes von G.*

Beweis. Sei $g \in G\backslash\{1\}$, dann ist $\mathrm{ord}(g) \neq 1$, und aus dem Satz von Langrange folgt, dass $\mathrm{ord}(g)|p$ gilt, also muss $\mathrm{ord}(g) = p = \mathrm{ord}(G)$ und damit also $\langle g \rangle = G$ sein. Daher ist G zyklisch, und jedes $g \in G\backslash\{1\}$ ist ein Erzeuger. □

2.2 Gruppenwirkungen, Sylowsätze und Klassifikation von Gruppen kleiner Ordnung

Ziel diese Abschnittes ist es, den in vielen Bereichen der Mathematik zentralen Begriff einer Gruppenwirkung (oder Gruppenaktion bzw. Gruppenoperation) einzuführen. Eine Gruppe operiert insbesondere durch Konjugation auf sich selbst und das Studium dieser Gruppenwirkung führt zu den Sylow-Sätzen, welche wir zur Klassifikation von Gruppen kleiner Ordnung benutzen werden.

Definition 2.18. *Sei G eine Gruppe und X eine Menge. Eine Abbildung*

$$G \times X \longrightarrow X,$$

geschrieben $(g, x) \mapsto g \cdot x$, heißt Gruppenwirkung (Gruppenaktion, Gruppenoperation), falls gilt

1. $\forall x \in X : 1 \cdot x = x$,
2. $\forall g, h \in G, x \in X : (gh) \cdot x = g \cdot (h \cdot x)$.

In diesem Fall sagt man, dass die Gruppe G auf der Menge X operiert.
Sei eine Gruppenwirkung $G \times X \to X$ und ein Element $x \in X$ vorgegeben. Dann heisst

1. $G \cdot x := \{g \cdot x \,|\, g \in G\}$ *die Bahn (oder der Orbit) von x unter G und*
2. $G_x := \{g \in G \,|\, g \cdot x = x\}$ *die Isotropiegruppe von x. G_x ist eine Untergruppe von G (Übung, leicht).*

Die Bahnen einer Gruppenaktion haben die folgende schöne Eigenschaft.

Lemma 2.19. *Sei $G \times X \to X$ eine Gruppenaktion, dann ist X disjunkte Vereinigung ihrer Bahnen.*

Beweis. Zu zeigen ist, dass für $x, y \in X$ entweder $Gx \cap Gy = \emptyset$ oder $Gx = Gy$ gilt. Sei also $a \in Gx \cap Gy$, dann ist $a = g \cdot x$ und $a = h \cdot y$ mit $g, h \in G$, also gilt $x = g^{-1}hy$ und daher $x \in Gy$ und also auch $Gx \subset Gy$. Analog zeigt man $Gx \supset Gy$, also $Gx = Gy$. □

Wir illustrieren diesen Begriff mit einigen Beispielen:

1. Sei $X = \mathbb{R}$ und $G = (\mathbb{R}\backslash\{0\}, \cdot)$ oder auch $G = (\mathbb{R}_{>0}, \cdot)$, dann operiert G (in beiden Fällen) durch Multiplikation auf X, d.h., man hat die Gruppenoperation

$$\begin{array}{rcl} G \times X & \longrightarrow & X \\ (r, x) & \longmapsto & r \cdot x \end{array}$$

   Für $G = \mathbb{R}\backslash\{0\}$ hat die Gruppenoperation zwei Orbits, nämlich $G \cdot 0$ und $G \cdot 1 = \mathbb{R}\backslash\{0\}$, für $G = \mathbb{R}_{\geq 0}$ gibt es die Orbits $G \cdot 0$, $G \cdot 1 = \mathbb{R}_{>0}$ und $G \cdot (-1) = \mathbb{R}_{<0}$. In beiden Fällen ist $G_x = \{1\}$ für alle $x \in \mathbb{R}\backslash\{0\}$ und $G_0 = G$.

2. Für eine beliebige Menge X sei $G < S(X)$ eine Untergruppe der Permutationsgruppe von X. Dann bekommt man in natürlicher Art und Weise die Gruppenoperation

$$\begin{array}{rcl} G \times X & \longrightarrow & X \\ (\varphi, x) & \longmapsto & \varphi(x) \end{array}$$

   Hier hängen die Orbits natürlich von der Wahl von G ab, z.B. hat man für $G = S(X)$ nur einen Orbit und für $G = \{\mathrm{id}\}$ ist jedes Element von X ein eigener Orbit.

3. Jede Gruppe operiert auf sich selbst durch Konjugation, also durch die Abbildung:

$$\begin{array}{rcl} G \times G & \longrightarrow & G \\ (a, g) & \longmapsto & a^{-1}ga \end{array}$$

   Wir haben weiter oben in den Beispielen nach Lemma 2.4 schon den zugehörigen Homomorphismus $G \to \mathrm{Aut}(G); a \longmapsto \big(\gamma_a : g \mapsto a^{-1}ga\big)$ kennengelernt. Sein Bild sind die sogenannten *inneren Automorphismen* von G.

   Die Orbits dieser Gruppenwirkung heißen Konjugationsklassen. Man sieht leicht, dass die Relation $g \sim h$ *genau dann, wenn* g *und* h *in der gleichen Konjugationklasse liegen*, eine Äquivalenzrelation ist. Allgemeiner ist natürlich für eine beliebige Gruppenwirkung $G \times X \to X$ die Relation $x \sim y$ genau dann, wenn $Gx = Gy$ eine Äquivalenzrelation.

Das folgende Lemma ist nützlich zum Verständnis der Bahnen einer Gruppenwirkung.

Lemma 2.20. *Sei $G \times X \to X$ eine Gruppenwirkung und $x \in X$. Dann existiert eine Bijektion $G/G_x \xrightarrow{\cong} Gx$ von der Menge der Linksnebenklassen von G_x in G auf den Orbit von $x \in X$.*

Beweis. Betrachte die surjektive Abbildung

$$\begin{array}{rcl} \varphi : G & \longrightarrow & Gx \\ g & \longmapsto & gx \end{array}$$

Dann gilt $\varphi(g) = \varphi(h)$ genau dann, wenn $gx = hx$, also $h^{-1}gx = x$ also $h^{-1}g \in G_x$, und diese letzte Aussage ist zu $gG_x = hG_x$ äquivalent, mit anderen Worten, g und h liegen in derselben Linksnebenklasse bezüglich der Untergruppe G_x. Dies induziert (vergleiche den Beweis des Homorphiesatzes 2.11) eine Bijektion $G/G_x \to Gx$. □

Als Konsequenz erhalten wir die sogenannte Bahnengleichung.

Satz 2.21. *Eine Gruppe G operiere auf einer* endlichen *Menge X. Sei $x_1, \ldots, x_n$ ein Vertretersystem der Bahnen dieser Operation, d.h., die Menge X ist disjunkte Vereinigung der Bahnen $Gx_1, \ldots, Gx_n$. Dann gilt*

$$|X| = \sum_{i=1}^{n} |Gx_i| = \sum_{i=1}^{n} (G : G_{x_i})$$

Die wichtigste Anwendung dieses Satzes ist der Fall $X = G$, bei dem G auf sich selbst durch Konjugation operiert. Hierfür benötigen wir noch die folgenden Begriffe.

Definition 2.22. *Sei G eine Gruppe und $S \subset G$ eine Menge, dann nennen wir:*

$$Z_S := \{g \in G \,|\, gs = sg \; \forall s \in S\} \quad \text{den Zentralisator von } S \text{ in } G$$

$$N_S := \{g \in G \,|\, gS = Sg\} \quad \text{den Normalisator von } S \text{ in } G$$

$$Z(G) := Z_G = \{g \in G \,|\, gs = sg \; \forall s \in G\} \quad \text{das Zentrum von } G$$

Man sieht leicht, dass Z_S und N_S Untergruppen von G sind, andererseits ist wegen $gZ(G) = Z(G)g$ für alle $g \in G$ das Zentrum ein Normalteiler von G.

Wir folgern jetzt aus der Bahnengleichung für Gruppenoperationen die sogenannte Klassengleichung für endliche Gruppen. Hierzu betrachten wir die Konjugationsoperation $G \times G \to G; (a, g) \mapsto a^{-1}ga$.

Satz 2.23 (Klassengleichung)**.** *Sei G endlich und $x_1, \ldots, x_n$ ein Vertretersystem der Bahnen in $G\backslash Z(G)$. Dann gilt*

$$\operatorname{ord}(G) = \operatorname{ord}(Z(G)) + \sum_{i=1}^{n} (G : Z_{\{x_i\}})$$

Beweis. Für $g \in Z(G)$ ist natürlich $a^{-1}ga = g$, also bestehen die Bahnen von Elementen aus $Z(G)$ nur aus einem Element. Außerdem operiert G auf dem Komplement $G\backslash Z(G)$, und hier hat man nach der Bahnengleichung für die Anzahl der Elemente einer Bahn $|Gx_i| = (G : G_{x_i})$. Aber offensichtlich ist

$$G_{x_i} = \left\{a \in G \,|\, a^{-1}x_i a = x_i\right\} = \{a \in G \,|\, x_i a = ax_i\} = Z_{\{x_i\}}.$$

□

Im folgenden wollen wir spezieller endliche Gruppen untersuchen, deren Ordnung eine Primzahlpotenz ist. Hierzu führen wir zunächst einige neue Namen ein.

Definition 2.24. *Sei G eine endliche Gruppe und p eine Primzahl.*

1. *G heißt p-*Gruppe*, falls $\operatorname{ord}(G) = p^k$ ist für ein $k \in \mathbb{N}$.*
2. *Sei $H < G$, dann heißt H eine p-Sylowgruppe, falls H eine p-Gruppe ist und falls $p \nmid (G : H)$, d.h., falls sich $\operatorname{ord}(G)$ schreiben läßt als $\operatorname{ord}(G) = p^k \cdot m$, mit $p^k = \operatorname{ord}(H)$ und $p \nmid m$.*

Wir diskutieren nun etwas die Struktur von p- bzw. p-Sylowgruppen.

Lemma 2.25. *Sei G eine p-Gruppe (p Primzahl) mit $\operatorname{ord}(G) = p^k$, $k > 0$. Dann gilt $p|\operatorname{ord}(Z(G))$, also insbesondere ist $Z(G) \neq \{1\}$.*

Beweis. Wir verwenden die Klassengleichung (Satz 2.23). Es reicht, zu zeigen, dass $p|(G : Z_{\{x_i\}})$ für alle $i \in \{1, \ldots, n\}$ gilt, denn dann folgt wegen $p|\operatorname{ord}(G)$ auch $p|\operatorname{ord}(Z(G))$.
Aus dem Satz von Lagrange wissen wir schon, dass $(G : Z_{\{x_i\}})|\operatorname{ord}(G)$, also $(G : Z_{\{x_i\}})|p^k$ gilt. Andererseits ist $x_i \notin Z(G)$, und daraus folgt, dass $Z_{\{x_i\}} \subsetneq G$ gilt, also $(G : Z_{\{x_i\}}) > 1$. Dann muss aber $(G : Z_{\{x_i\}}) = p^l$ für $1 \leq l \leq k$ sein, und dann folgt insbesondere $p|(G : Z_{\{x_i\}})$. □

Korollar 2.26. *Sei wieder G eine p-Gruppe der Ordnung p^k, p Primzahl. Dann existiert eine absteigende Kette von Untergruppen*

$$G = G_k \supset G_{k-1} \supset \ldots \supset G_0 = \{1\}.$$

mit $\operatorname{ord}(G_l) = p^l$ und $G_{l-1} \lhd G_l$ für $l = 1, \ldots, k$.
Also existiert zu jedem l eine Untergruppe $H < G$ mit $\operatorname{ord}(H) = p^l$ und insbesondere gibt es für $k \geq 1$ immer ein Element der Ordnung p in G.

Beweis. Der Beweis wird mit Induktion über k geführt. Für $k = 0$ ist die Aussage klar. Sei also $k > 0$. Dann gilt $Z(G) \neq \{1\}$ nach Lemma 2.25, sei also $a \in Z(G)\backslash\{1\}$. Wegen $\mathrm{ord}(a)|p^k$ ist notwendig $\mathrm{ord}(a) = p^r$ für ein $1 \leq r \leq k$. Setze dann $b := a^{(p^{r-1})}$, dann ist natürlich $b \in Z(G)$, und $\mathrm{ord}(b) = p$. Die von b erzeugte Untergruppe $\langle b\rangle$ ist wegen $b \in Z(G)$ ein Normalteiler in G. Betrachte $\overline{G} := G/\langle b\rangle$, dann ist $\mathrm{ord}(\overline{G}) = p^{k-1}$, wir können also hier die Induktionsvoraussetzung anwenden. Es existiert also eine Kette von Untergruppen

$$\overline{G} = \overline{G}_{k-1} \supset \overline{G}_{k-2} \supset \ldots \supset \overline{G}_0 = \{1\}$$

mit $\mathrm{ord}(\overline{G}_l) = p^l$ und $\overline{G}_{l-1} \lhd \overline{G}_l$ für $l = 1, \ldots, k-1$. Sei $\pi : G \to \overline{G}$ die kanonische Projektion, dann definieren wir $G_{l+1} := \pi^{-1}(\overline{G}_l)$ (und $G_0 := \{1\}$), und dann ist $\mathrm{ord}(G_l) = p^l$ und wir erhalten die gesuchte Kette von Untergruppen

$$G = G_k \supset G_{k-1} \supset \ldots \supset G_0 = \{1\}\,.$$

□

Für das nächste Ergebnis benötigen wir den einfachen, aber sehr nützlichen Begriff des Produktes von Gruppen.

Definition 2.27. *Sei I eine (möglicherweise unendliche) Menge, und $G_i, i \in I$ eine durch I parametrisierte Familie von Gruppen. Dann ist die Menge $\prod_{i\in I} G_i$ mit der (sogenannten komponentenweisen) Verknüpfung*

$$(a_i)_{i\in I} \cdot (b_i)_{i\in I} := (a_i \cdot b_i)_{i\in I}$$

eine Gruppe, genannt direktes Produkt der Gruppen G_i. Falls $I = \{1, \ldots, n\}$ ist, schreibt man auch $\prod_{i\in I} G_i = G_1 \times \ldots \times G_n$.

Korollar 2.28. *Sei $\mathrm{ord}(G) = p^2$, p Primzahl. Dann gilt*

1. *G ist abelsch.*
2. $$G \cong \mathbb{Z}/p^2\mathbb{Z} \qquad \text{oder} \qquad G \cong \mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z}$$

Beweis. 1. Aus dem obigen Lemma 2.25 folgt $p|\mathrm{ord}(Z(G))$, folglich gibt es nur die zwei Fälle $\mathrm{ord}(Z(G)) = p$ und $\mathrm{ord}(Z(G)) = p^2$. Im zweiten Fall ist $Z(G) = G$ und dann ist G natürlich abelsch. Wir nehmen also an, dass $\mathrm{ord}(Z(G)) = p$ gelte, insbesondere ist dann $Z(G) \subsetneq G$, d.h., G wäre nicht abelsch. Es muss dann aber der Quotient $G/Z(G)$ wegen Korollar 2.17 eine zyklische Gruppe der Ordnung p sein. Wir zeigen jetzt, dass daraus schon folgt, dass G abelsch ist (insbesondere ist die Annahme $\mathrm{ord}(Z(G)) = p$ also falsch): Sei $a \in G$ so gewählt, dass $G/Z(G) = \langle\overline{a}\rangle$ gilt. Seien $g, h \in G$ mit $\overline{g} = \overline{a}^m$ und $\overline{h} = \overline{a}^n$, dann existieren $b, c \in Z(G)$ mit $g = a^m \cdot b$ und $h = a^n \cdot c$. Dann ist aber

$$gh = a^m b a^n c \overset{b\in Z(G)}{=} a^{m+n} bc \qquad hg = a^n c a^m b \overset{c\in Z(G)}{=} a^{n+m} cb \overset{c\in Z(G)}{=} a^{n+m} bc,$$

also $gh = hg$, und daher ist G abelsch.

2. Es gibt nach Korollar 2.26 ein Element $a \in G$ mit $\mathrm{ord}(a) = p$, wähle weiterhin ein $b \in G\backslash\langle a\rangle$. Jetzt muss $\mathrm{ord}(b) \in \{p, p^2\}$ gelten, falls $\mathrm{ord}(b) = p^2$ ist, dann ist $G = \langle b\rangle \cong \mathbb{Z}/p^2\mathbb{Z}$. Sei also $\mathrm{ord}(b) = p$, und betrachte die Abbildung

$$\begin{aligned} \varphi : \langle a\rangle \times \langle b\rangle &\longmapsto G \\ (a^m, b^n) &\longmapsto a^m \cdot b^n \end{aligned}$$

Wegen Punkt 1. ist G abelsch, also ist φ ein Gruppenhomomorphismus. Aus der Wahl $b \notin \langle a\rangle$ folgt, dass $\langle a\rangle \cap \langle b\rangle \subsetneq \langle a\rangle$, aber dann ist $\langle a\rangle \cap \langle b\rangle = \{1\}$. Hieraus folgt die Injektivität von φ. Nun gilt aber offensichtlich

$$\mathrm{ord}(\langle a\rangle \times \langle b\rangle) = p^2 = \mathrm{ord}(G),$$

daher muss φ auch surjektiv, also ein Gruppenisomorphismus sein. Wegen $\mathrm{ord}(a) = \mathrm{ord}(b) = p$ gilt natürlich $\langle a\rangle \cong \langle b\rangle \cong \mathbb{Z}/p\mathbb{Z}$.

□

Bemerkung: Wir werden im Abschnitt 3.4 allgemeiner die Struktur von endlich erzeugten abelschen Gruppen studieren. Wenn man also Teil 1. des obigen Korollars bewiesen hat, dann kann man aus den Ergebnissen dieses Kapitels direkt Teil 2. ableiten.
Wir kommen nun zu den Sylowsätzen.

Satz 2.29 (Sylowsätze)**.** *Sei p eine Primzahl, G eine endliche Gruppe mit* $\mathrm{ord}(G) = n$ *und sei $n = p^k \cdot m$, $p \nmid m$.*

1. *Für jede p-Untergruppe $H < G$ (d.h.,* $\mathrm{ord}(H) = p^l$*) existiert eine p-Sylowgruppe $S \subset G$ mit $H \subset S$.*
2. *Für jede p-Sylowgruppe S von G (zur Erinnerung:* $\mathrm{ord}(S) = p^k$*) gilt: Alle zu S konjugierten Untergruppen sind p-Sylowgruppen. Umgekehrt sind alle p-Sylowgruppen konjugiert.*
3. *Sei s_p die Anzahl der p-Sylowgruppen von G, dann gilt*

$$s_p | m \qquad \text{und} \qquad s_p \equiv 1 \mod (p)$$

Insbesondere ist also $s_p > 0$, d.h. aus 3. folgt insbesondere die Existenz einer p-Sylowgruppe $S < G$.

Für den Beweis der Sylowsätze formulieren wir zunächst folgende Hilfsaussage.

Lemma 2.30. *Sei G eine endliche Gruppe mit* $\mathrm{ord}(G) = n = p^k \cdot m$ *(hier wird nicht $p \nmid m$ vorausgesetzt). Sei s die Anzahl der (p-)Untergruppen $H < G$ mit Ordnung* $\mathrm{ord}(H) = p^k$*. Dann gilt*

$$s \equiv \binom{n-1}{p^k - 1} = \frac{1}{m}\binom{n}{p^k} \qquad \mod \quad (p).$$

Beweis. Die zweite Gleichung gilt wegen

$$\frac{m \cdot p^k}{p^k} \cdot \binom{n-1}{p^k - 1} = \binom{n}{p^k}.$$

Wir zeigen jetzt, dass

$$s \cdot m \equiv \binom{n}{p^k} \qquad \mod \quad (m \cdot p)$$

gilt. Hierzu definieren wir eine Menge X, welche Teilmenge der Potenzmenge $\mathcal{P}(G)$ ist, also deren Elemente Teilmengen von G sind, nämlich

$$X := \left\{ U \subset G \,|\, |U| = p^k \right\}.$$

Da man genau $\binom{n}{p^k}$ Möglichkeiten hat, p^k Elemente aus n Elementen auszuwählen, gilt

$$|X| = \binom{n}{p^k}.$$

Wir betrachten die Wirkung von G auf X, welche durch

$$\varphi : G \times X \quad \longrightarrow \quad X$$

$$(g, U) \quad \longmapsto \quad gU$$

definiert wird, wobei hier $gU := \{g \cdot u \,|\, u \in U\}$ analog zur Definition von Linksnebenklassen erklärt ist, obwohl U nicht notwendig eine Untergruppe von G ist. Man beachte: gU ist eine Teilmenge von G, aber

ein Element von X (weil eben $|gU| = p^k$ gilt). Die Wirkung φ von G auf X hat Bahnen, und wir schreiben für die Bahn eines Elementes $U \in X$ hier $G(U)$ (weil die Standardbezeichnung GU zu Verwirrung führen würde). Wir betrachten jetzt für $U \in X$ die Isotropiegruppe

$$G_U = \{g \in G \,|\, gU = U\},$$

dann können wir eine neue Gruppenoperation definieren, nämlich von der Gruppe G_U auf der Menge U:

$$\begin{aligned} \psi : G_U \times U &\longrightarrow U \\ (g, u) &\longmapsto gu \end{aligned}$$

Wieder interessieren uns die Bahnen der Wirkung ψ: für ein $u \in U$ ist die Bahn $G_U u = \{g \cdot u \,|\, g \in G_U\}$ nichts anderes als die Rechtnebenklasse von G_U in G zu u. Wegen Satz 2.6 ist also U disjunkte Vereinigung von gewissen Rechtsnebenklassen von G_U (natürlich nur von Rechtsnebenklassen zu Elementen aus U). Alle diese Nebenklassen haben $\mathrm{ord}(G_U)$-viele Elemente, dies impliziert $\mathrm{ord}(G_U) \Big| |U|$, aber wegen $|U| = p^k$ folgt $\mathrm{ord}(G_U) = p^l$ für ein $l \in \{0, \ldots, k\}$. Man beachte, dass die Ordnung von G_U (weil G_U Untergruppe von G ist) natürlich die Ordnung von G teilen muss, aber daraus würde a priori nicht $\mathrm{ord}(G_U)|p^k$ folgen. Wir bemerken noch, dass im Fall $l = k$ die gesamte Menge U nur aus einem einzigen G_U-Orbit besteht, d.h., dann gilt $U = G_U u$ für ein $u \in U$, also ist dann U selbst eine Rechtsnebenklasse von G_U in U.
Wir kehren nun wieder zum Studium der Wirkung φ von G auf der Menge X der p^k-elementigen Teilmengen von G zurück. Sei $U_1, \ldots, U_r$ ein Vertretersystem der G-Bahnen, dann gilt wegen der Bahnengleichung (Satz 2.21), dass

$$\binom{n}{p^k} = |X| = \sum_{i=1}^{r} |G(U_i)| = \sum_{i=1}^{r} (G : G_{U_i})$$

Wie wir eben gesehen haben, ist $\mathrm{ord}(G_{U_i}) = p^{l_i}$ für ein $l_i \in \{0, \ldots, k\}$, also (wegen dem Satz von Langrange), $(G : G_{U_i}) = p^{k-l_i} \cdot m$. Falls $l_i < k$, ist also $(G : G_{U_i})$ notwendig durch $m \cdot p$ teilbar. Wir setzen jetzt

$$I := \{i \in \{1, \ldots, r\} \,|\, l_i = k\}$$

dann haben wir

$$\begin{aligned} |I| \cdot m &= \textstyle\sum_{i \in I} (G : G_{U_i}) \\ &= \textstyle\sum_{i=1}^{r} (G : G_{U_i}) - \sum_{i \notin I} (G : G_{U_i}) \\ &= \textstyle\binom{n}{p^k} - \sum_{i \notin I} (G : G_{U_i}) \end{aligned}$$

wobei die erste Gleichung folgt, weil $(G : G_{U_i}) = m$ ist, falls $i \in I$ gilt.
Da, wie oben bemerkt, für all $i \notin I$ gilt, dass $mp \,|\, (G : G_{U_i})$ ist, folgt schließlich

$$|I| \cdot m \equiv \binom{n}{p^k} \mod (m \cdot p).$$

Es bleibt zu zeigen, dass

$$|I| = \left|\left\{H < G \,|\, \mathrm{ord}(H) = p^k\right\}\right|$$

gilt, um den Beweis des Lemmas abzuschließen. Um dies zu beweisen, zeigen wir, dass es eine Bijektion

$$\alpha : \left\{H < G \,|\, \mathrm{ord}(H) = p^k\right\} \longrightarrow \{i \in \{1, \ldots, r\} \,|\, \mathrm{ord}(G_{U_i}) = p^k\} = I$$

gibt. Sei $H < G$ mit $\mathrm{ord}(H) = p^k$, dann folgt $(G : H) = m$. Betrachten wir dann die G-Bahn $G(H)$ des Elementes H in der Menge X (bezüglich der Operation φ), dann ist

$$G(H) = \{gH \,|\, g \in G\} \subset X$$

d.h., $G(H)$ identifiziert sich mit der Menge G/H der Linksnebenklassen von H, folglich ist $|G(H)| = (G : H) = m$, dann muss aber diese Bahn eine der Bahnen $G(U_i)$ mit $i \in I$ sein. Also können wir $\alpha(H) := i$ setzen. Hat man zwei p-Untergruppen $H_1, H_2 < G$ mit $\mathrm{ord}(H_1) = \mathrm{ord}(H_2) = p^k$, so dass $G(H_1) = G(H_2)$ gilt, dann gibt es $g \in G$ mit $gH_1 = H_2$, also insbesondere existiert $h \in H_1$ mit $gh = 1$ und daher ist $g = h^{-1}$, also notwendig $g \in H_1$, und deshalb $H_1 = H_2$. Folglich ist α injektiv.
Sei nun $U_i, i \in I$ gegeben. Wegen $\mathrm{ord}(G_{U_i}) = p^k$ ist, wie oben festgestellt, U_i eine einzelne G_{U_i}-Bahn (also eine einzelne Bahn der Wirkung ψ), also $U_i = G_{U_i}u_i$ für ein $u_i \in U_i$. Weil u_i^{-1} natürlich ein Element in G ist, gilt

$$G(U_i) = G(u_i^{-1}U_i) = G(u_i^{-1}G_{U_i}u_i)$$

Damit gilt für die Untergruppe $H := u_i^{-1}G_{U_i}u_i < G$ (mit $\mathrm{ord}(H) = \mathrm{ord}(G_{U_i}) = p^k$), dass $G(H) = G(U_i)$ ist, mit anderen Worten, wir haben $\alpha(H) = i$ nach der obigen Definition von α, und damit ist α auch surjektiv. Dies beendet den Beweis des Lemmas. □

Beweis der Sylowsätze. Wir zeigen zunächst, dass die Anzahl s_p der p-Sylowgruppen die Kongruenzgleichung $s_p \equiv 1 \mod (p)$ erfüllt. Hierzu wenden wir Lemma 2.30 zwei Mal an: Einmal auf die zu untersuchende Gruppe G mit $\mathrm{ord}(G) = p^k \cdot m$, $p \nmid m$, sowie auf die zyklische Gruppe der selben Ordnung $n = p^k \cdot m$. Zunächst besagt Lemma 2.30, dass die Anzahl s_p der p-Sylowgruppen die Relation

$$s_p \equiv \frac{1}{m}\binom{p^k m}{p^k} \mod (p)$$

erfüllt. Andererseits wissen wir aus Satz 2.15, dass es genau eine Untergruppe von $\mathbb{Z}/n\mathbb{Z}$ der Ordnung p^k gibt, diese Anzahl ist nach Lemma 2.30 aber ebenfalls kongruent $\frac{1}{m}\binom{n}{p^k}$ modulo p, also haben wir die Relation

$$\frac{1}{m}\binom{p^k m}{p^k} \equiv 1 \mod (p)$$

so dass wir $s_p \equiv 1 \mod (p)$ erhalten. Insbesondere muss G also eine p-Sylowgruppe $S < G$ enthalten.
Punkt 1. des zu zeigenden Satzes ist die etwas stärkere Aussage, dass jede p-Untergruppe $H < G$ sogar in einer Sylowgruppe enthalten ist. Sei also $H < G$ mit $\mathrm{ord}(H) = p^l$, $l \in \{1, \ldots, k\}$ gegeben und betrachte die Wirkung von H auf G/S, definiert durch

$$\begin{aligned} \gamma : H \times G/S &\longrightarrow G/S \\ (h, gS) &\longmapsto (hg)S \end{aligned}$$

Wähle ein Vertretersystem $x_1, \ldots, x_t$ der Bahnen von γ, dann sagt wieder die Bahnengleichung, dass

$$|G/S| = \sum_{i=1}^{t} |Hx_i|$$

gilt. Es ist $|G/S| = (G : S) = p^k m/p^k = m$, und $|Hx_i| = (H : H_{x_i})$ nach Lemma 2.20, also $|Hx_i| \big| \mathrm{ord}(H)$ und damit ist $|Hx_i|$ eine p-Potenz. Wäre $|Hx_i| > 0$ für alle $i \in \{1, \ldots, t\}$, dann hätten wir $p \big| |G/S|$, was $p \nmid m$ widerspricht. Also existiert ein x_i mit $Hx_i = \{x_i\}$. x_i ist eine Linksnebenklasse von S in G, also $x_i = gS$ für ein $g \in G$, und $Hx_i = \{x_i\}$ bedeutet dann $hgS = gS$ für alle $h \in H$. Wegen $1 \in S$ impliziert dies, dass $hg \in gS$ oder, $h \in gSg^{-1}$ für alle $h \in H$ gilt. Dann muss also $H \subset gSg^{-1}$ sein. Nun haben wir aber $|gSg^{-1}| = |S| = p^k$, d.h., auch gSg^{-1} ist eine p-Sylowgruppe, und damit haben wir gezeigt, dass H immer in einer Sylowgruppe enthalten ist.
Als nächstes beweisen wir Punkt 2. Wie wir eben schon gesehen haben, ist mit S auch jede zu S konjugierte Untergruppe eine p-Sylowgruppe. Sei S' eine andere p-Sylowgruppe, dann folgt wie eben, dass $S' \subset gSg^{-1}$ gilt, für ein $g \in G$. Aber wegen $\mathrm{ord}(S') = \mathrm{ord}(S) = \mathrm{ord}(gSg^{-1}) = p^k$ ist dann schon $S' = gSg^{-1}$, also sind alle p-Sylowgruppen konjugiert.

Schlußendlich ist noch die Aussage $s_p|m$ zu zeigen. Wir bezeichnen analog zum letzten Lemma mit X die Menge der p-Sylowgruppen von G, und betrachten die Konjugationswirkung

$$\begin{aligned} G \times X &\longrightarrow X \\ (g, S) &\longmapsto gSg^{-1} \end{aligned}$$

dann sagt Punkt 2., dass diese Wirkung transitiv ist, d.h., dass es nur einen Orbit gibt. Sei

$$G_S = \{g \in G \,|\, gSg^{-1} = S\} \subset G$$

die Isotropiegruppe einer gegebenen Sylowgruppe S (G_S ist natürlich nichts anderes als der Normalisator N_S von S in G), dann ist nach Lemma 2.20 $s_p = |X| = (G : G_S) = \mathrm{ord}(G)/\mathrm{ord}(G_S)$, und somit folgt $s_p|\mathrm{ord}(G)$. Falls jetzt $s_p = 1$ ist, dann gilt natürlich $s_p|m$, falls $s_p > 1$ und $s \nmid m$, dann folgt $s_p|p^k$, aber dann ist $s_p = p^l$ mit $l \in \{1, \ldots, k\}$, und dann wäre $p|s_p$, was $s_p \equiv 1 \mod (p)$ widerspricht, somit muss $s_p|m$ gelten. □

Als nächstes wollen wir eine Klassifikation von Gruppen gewisser (kleiner) Ordnungen aus den Sylowsätze ableiten.
Wir haben schon gesehen (Korollar 2.17), dass Gruppen mit Primzahlordnung zyklisch und daher bis auf Isomorphie eindeutig bestimmt sind. Eine weitere Quelle zyklischer Gruppen sind durch den folgenden Satz gegeben.

Satz 2.31. *Seien p, q Primzahlen mit $p < q$ und $p \nmid (q-1)$. Dann ist jede Gruppe G der Ordnung pq zyklisch, also isomorph zu $\mathbb{Z}/(pq)\mathbb{Z}$.*

Beweis. Wie oben bezeichne s_p bzw. s_q die Anzahl der p- bzw. q-Sylowgruppen von G, dann ist nach dem 3. Sylowsatz $s_q \in \{1, p\}$ und $s_q \equiv 1 \mod (q)$. Wegen $p < q$ ist damit der Fall $s_q = p$ ausgeschlossen, und wir haben $s_q = 1$. Jetzt wenden wir den 3. Sylowsatz auf s_p an, und erhalten analog $s_p \in \{1, q\}$ sowie $s_p \equiv 1 \mod (p)$. Angenommen, wir hätten $s_p = q$, dann würde p die Zahl $s_p - 1 = q - 1$ teilen, was nach Voraussetzung ausgeschlossen ist, also $s_p = 1$. Es gibt also genau eine p- und genau eine q-Sylowgruppe. Dann hat jedes Element außerhalb dieser Untergruppen die Ordnung pq. Es muss aber Elemente ausserhalb dieser Untergruppen geben, denn beide zusammen haben $p+q-1$ Elemente, und das Komplement hat dann $pq - (p + q - 1) = (p - 1)(q - 1) \geq (q - 1) \geq 4$ Elemente. Weil also Elemente der Ordnung pq existieren, ist G zyklisch. □

Der nächste Satz behandelt eine andere Klasse von Gruppen.

Satz 2.32. *Sei p eine Primzahl, $p > 2$ und G eine Gruppe der Ordnung $2p$. Dann ist G zyklisch oder isomorph zur Diedergruppe D_p.*

Beweis. Aus dem 3. Sylowsatz folgt wie im Beweis des letzten Satz, dass $s_p = 1$ sein muss, d.h., es gibt genau eine Untergruppe U der Ordnung p in G. Dann ist notwendig $U \lhd G$, denn jede zu U konjugierte Untergruppe hätte auch p Elemente, muss also gleich U sein. Andererseits ist U als Gruppe von Primzahlordnung natürlich zyklisch, sei also $U = \langle x \rangle$, mit $\mathrm{ord}(x) = p$. Natürlich können wir auch aus dem 3. Sylowsatz folgern, dass es eine Untergruppe der Ordnung 2 geben muss, diese heiße V und ist natürlich auch zyklisch, d.h. $V = \langle y \rangle$, mit $\mathrm{ord}(y) = 2$.
Da U ein Normalteiler ist, folgt $y \cdot x \cdot y^{-1} \in U$, also gibt es $b \in \{0, \ldots, p-1\}$ mit $y \cdot x \cdot y^{-1} = x^b$. Man kann jetzt die Relationen zwischen den Potenzen von x und y berechnen, genauer, man zeigt, dass

$$\begin{aligned} y^r x^s y^t &= x^r y^{t+s} \\ y^r x^s y x^t &= x^{r+1} y^{sb+t} \end{aligned}$$

für alle $r \in \{0, 1\}$ und $s, t \in \{0, \ldots, p-1\}$ gilt. Daraus läßt sich $x = x^{(b^2)}$ schlußfolgern, also $x^{b^2-1} = 1$, also folgt wegen $\mathrm{ord}(x) = p$, dass $p|(b^2 - 1)$, d.h. $p|b-1$ oder $p|b+1$ gelten muss, und hieraus folgt $b \in \{1, p-1\}$.

Für $b = 1$ folgt $y \cdot x = x \cdot y$, und dann ist G abelsch, und man prüft, dass $G \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z} \cong \mathbb{Z}/2p\mathbb{Z}$ ist. Für $b = p - 1$ kann man auch explizit nachrechnen, dass G isomorph zu D_p ist, wobei x einer Drehung um $2\pi i/p$ und y einer Spiegelung an der Spiegelachse, welche durch die Punkte $0 \in \mathbb{C}$ und $2\pi i/p \in \mathbb{C}$ geht, entspricht. □

Wir erwähnen die folgende Klassifikation von Gruppen der Ordnung kleiner gleich 15, von der wir einen Großteil aus den bisherigen Ergebnissen ableiten können.

Satz 2.33. *Die folgende Tabelle gibt die Isomorphieklassen für Gruppen bis zur Ordnung* 15*.*

Ordnung	**Isomorphieklassen**
1	$\{e\}$
2	$S_2 \cong \mathbb{Z}/2\mathbb{Z}$
3	$\mathbb{Z}/3\mathbb{Z}$
4	$\mathbb{Z}/4\mathbb{Z}, \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$
5	$\mathbb{Z}/5\mathbb{Z}$
6	$\mathbb{Z}/6\mathbb{Z} \cong \mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}, D_3 \cong S_3$
7	$\mathbb{Z}/7\mathbb{Z}$
8	$\mathbb{Z}/8\mathbb{Z}, \mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}, \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}, D_4$, Quarternionengruppe
9	$\mathbb{Z}/9\mathbb{Z}, \mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}$
10	$\mathbb{Z}/10\mathbb{Z} \cong \mathbb{Z}/5\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}, D_5$
11	$\mathbb{Z}/11\mathbb{Z}$
12	$\mathbb{Z}/12\mathbb{Z} \cong \mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z}, \mathbb{Z}/6\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \cong \mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}, D_6, A_4, S_3 \times \mathbb{Z}/2\mathbb{Z}$
13	$\mathbb{Z}/13\mathbb{Z}$
14	$\mathbb{Z}/14\mathbb{Z} \cong \mathbb{Z}/7\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}, D_7$
15	$\mathbb{Z}/15\mathbb{Z}$

Beweis. Für $n \in \{1, \ldots, 15\}$ mit n Primzahl existiert nach Korollar 2.17 nur die zyklische Gruppe mit Ordnung n, und diese ist isomorph zu $\mathbb{Z}/n\mathbb{Z}$. Analog folgt für $n = 15$ aus Satz 2.31, dass eine Gruppe der Ordnung 15 nur zyklisch sein kann. Für $n \in \{6, 10, 14\}$ verwenden wir analog Satz 2.32 und erhalten die zyklische Gruppe und die Diedergruppe als Isomorphietyp. Die einzigen Fälle, die wir nicht beweisen sind $n = 8$ und $n = 12$. Die Gruppe A_4 wird gleich in Definition 2.39 eingeführt.
Bemerkung: Wir haben in der Tabelle benutzt, dass für teilerfremde Zahlen a, b gilt, dass $\mathbb{Z}/a\mathbb{Z} \times \mathbb{Z}/b\mathbb{Z} \cong \mathbb{Z}/(ab)\mathbb{Z}$ gilt. Diese Aussage ist eine einfache Konsequenz des *Chinesischen Restsatzes*, welchen wir im im Abschnitt 3.4 behandeln werden, kann aber natürlich auch direkt bewiesen werden. □

2.3 Permutationsgruppen und Auflösbarkeit

Wir wollen uns nun ausführlicher mit *Permutationsgruppen* beschäftigen. Die erreichten Ergebnisse werden wir später zur Frage der Lösbarkeit algebraischer Gleichungen benutzen. Zur Erinnerung: Für $X = \{1, \ldots, n\}$ heißt die Gruppe $(\mathrm{Bij}(X), \circ)$ die symmetrische Gruppe und wird mit S_n bezeichnet. Elemente $\sigma \in S_n$ schreibt man

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

Man sieht leicht, dass $\mathrm{ord}(S_n) = n!$ ist: Für $\sigma(1)$ gibt es genau n Möglichkeiten, nämlich die Zahlen $1, \ldots, n$, $\sigma(2)$ ist (da σ eine Bijektion sein soll) ein Element aus $\{1, \ldots, n\} \backslash \{\sigma(1)\}$, daher gibt es $n - 1$ Möglichkeiten usw.
Die folgenden speziellen Permutationen spielen im weiteren Verlauf eine große Rolle.

Definition 2.34. *Eine Permutation $\sigma \in S_n$ heißt Zyklus, falls es Zahlen $a_1, \ldots, a_k \in \{1, \ldots, n\}$ gibt mit*

$$\begin{aligned} \sigma(a_i) &= a_{i+1} \quad \forall i \in \{1, \ldots, k-1\} \\ \sigma(a_k) &= a_1 \\ \sigma(l) &= l \qquad \forall l \notin \{a_1, \ldots, a_k\}. \end{aligned}$$

Wir schreiben dann $\sigma = (a_1\, a_2\, \ldots\, a_k)$. Ein Zyklus, bei dem $k = 2$ ist (also $\sigma = (a_1\, a_2)$) heißt Transposition. Für einen Zyklus $\sigma = (a_1\, a_2\, \ldots\, a_k)$ heißt die Menge $\{a_1, \ldots, a_k\}$ der Träger $Tr(\sigma)$ von σ. Alternativ kann man für eine beliebige Permutation $\sigma \in S_n$ den Träger definieren als

$$\mathrm{Tr}(\sigma) := \{k \in \{1, \ldots, n\} \mid \sigma(k) \neq k\},$$

und natürlich stimmen für einen Zyklus beide Definitionen überein.

Zyklen sind gut geeignet, um Elemente oder Untergruppen der symmetrischen Gruppe effizient aufschreiben zu können. Betrachte beispielweise die abelsche symmetrische Gruppe S_2, dann gilt

$$S_2 = \{\mathrm{id}, (1\,2)\} = \{\mathrm{id}, (2\,1)\},$$

weil natürlich für jede Transposition $(a\,b) = (b\,a)$ gilt. Weiterhin ist

$$S_3 = \{\mathrm{id}, (1\,2), (1\,3), (2\,3), (1\,2\,3), (1\,3\,2)\}.$$

Wir wollen die Untergruppen von S_3 bestimmen: Nach dem Satz von Lagrange können nur Untergruppen der Ordnungen 1, 2, 3 und 6 auftreten. Genauer gilt

Ordnung	**Untergruppen**
1	$\{\mathrm{id}\}$
2	$\{\mathrm{id}, (1\,2)\}, \{\mathrm{id}, (1\,3)\}, \{\mathrm{id}, (2\,3)\}$
3	$\{\mathrm{id}, (1\,2\,3), (1\,3\,2)\} = A_3$
6	S_3

Die Bezeichnung A_3 wird weiter unten in Definition 2.39 eingeführt.
Wir werde gleich sehen, dass sich alle Permutationen in geeigneter Weise aus Zyklen aufbauen lassen. Zunächst führen wir den folgenden, für die Untersuchung der symmetrischen Gruppen wichtigen Begriff ein.

Definition 2.35. *Sei $\sigma \in S_n$. Das Vorzeichen oder Signum von σ ist definiert als*

$$\mathrm{sign}(\sigma) := (-1)^{|\mathrm{Fehlstände}(\sigma)|}.$$

Hierbei ist

$$\mathrm{Fehlstände}(\sigma) := \left\{(i,j) \in \{1, \ldots, n\}^2 \mid i < j,\ \sigma(i) > \sigma(j)\right\}.$$

Eine Permutation σ mit $\mathrm{sign}(\sigma) = 1$ heißt gerade, eine mit $\mathrm{sign}(\sigma) = -1$ nennt man ungerade.

Die folgende Aussage gibt einen ersten Hinweis, wie man das Vorzeichen berechnen kann.

Satz 2.36. *Sei $\sigma \in S_n$, dann gilt:*

$$\mathrm{sign}(\sigma) = \prod_{j<i} \frac{\sigma(j) - \sigma(i)}{j - i}.$$

Die Abbildung

$$\begin{aligned} \mathrm{sign} : S_n &\longrightarrow \{1, -1\} \\ \sigma &\longmapsto \mathrm{sign}(\sigma) \end{aligned}$$

definiert einen Gruppenhomomorphismus $\sigma : (S_n, \circ) \to (\{1, -1\}, \cdot)$.

Beweis. Zunächst beweisen wir folgende Aussage: Sei $A \subset \{(j,i) \,|\, j,i \in \{1,\dots,n\}, i \neq j\}$ eine Menge, welche zu jedem Paar (a,b) mit $a \neq b$, entweder (a,b) oder (b,a) enthält. Dann ist

$$\operatorname{sign}(\sigma) = \prod_{(j,i)\in A} \frac{\sigma(j)-\sigma(i)}{j-i}. \tag{2.2}$$

Zum Beweis bemerken wir zunächst, dass gilt:

$$\prod_{(j,i)\in A} |j-i| = \prod_{i<j} (j-i).$$

Andererseits kann man auch die Menge $A' := \{(\sigma(j),\sigma(i)) \,|\, (j,i) \in A\}$ betrachten, diese hat wieder die Eigenschaft, dass zu jedem Paar (a,b) mit $a \neq b$, entweder (a,b) oder (b,a) in A' liegt. Daher gilt

$$\prod_{(j,i)\in A'} |j-i| = \prod_{(j,i)\in A} |\sigma(j)-\sigma(i)| = \prod_{i<j} (j-i),$$

und deshalb ist

$$\left| \prod_{(j,i)\in A} \frac{\sigma(j)-\sigma(i)}{j-i} \right| = 1.$$

Außerdem gilt

$$\text{Vorzeichen}\left(\frac{\sigma(j)-\sigma(i)}{j-i}\right) = \begin{cases} +1 & \text{falls } (i,j) \text{ bzw. } (j,i) \text{ kein Fehlstand} \\ -1 & \text{falls } (i,j) \text{ bzw. } (j,i) \text{ Fehlstand} \end{cases}$$

Damit ist Formel (2.2) bewiesen. Insbesondere können wir den Fall $A = \{(j,i) \,|\, j < i\}$ betrachten, und erhalten den Spezialfall

$$\operatorname{sign}(\sigma) = \prod_{j<i} \frac{\sigma(j)-\sigma(i)}{j-i}.$$

Zum Beweis der zweiten Aussage des Satzes seien also $\sigma, \tau \in S_n$, dann gilt:

$$\begin{aligned} \operatorname{sign}(\sigma\circ\tau) &= \prod_{j<i} \tfrac{\sigma(\tau(j))-\sigma(\tau(i))}{j-i} \\ &= \prod_{j<i} \tfrac{\sigma(\tau(j))-\sigma(\tau(i))}{\tau(j)-\tau(i)} \cdot \prod_{j<i} \tfrac{\tau(j)-\tau(i)}{j-i} \\ &= \operatorname{sign}(\sigma)\cdot\operatorname{sign}(\tau). \end{aligned}$$

Hierbei folgt die Gleichheit

$$\prod_{j<i} \frac{\sigma(\tau(j))-\sigma(\tau(i))}{\tau(j)-\tau(i)} = \operatorname{sign}(\sigma)$$

aus Gleichung (2.2) für den Fall $A = \{(\tau(j),\tau(i)) \,|\, j < i\}$. □

Um Vorzeichen von Elementen von S_n zu berechnen, benutzt man insbesondere zyklische Permutationen. Nicht jede Permutation ist ein Zyklus, aber die folgende Aussage zeigt, dass man jede Permutation aus Zyklen aufbauen kann.

Satz 2.37. *1. Seien $\sigma_1, \sigma_2 \in S_n$ Zyklen mit $\operatorname{Tr}(\sigma_1) \cap \operatorname{Tr}(\sigma_2) = \emptyset$. Zur Erinnerung*

$$\operatorname{Tr}(\sigma) = \{i \in \{1,\dots,n\} \,|\, \sigma(i) \neq i\}$$

für alle $\sigma \in S_n$. Dann gilt $\sigma_1 \circ \sigma_2 = \sigma_2 \circ \sigma_1$.

2. *Sei $\sigma \in S_n$. Dann existieren (bis auf Vertauschung) eindeutige Zyklen $\sigma_1, \ldots, \sigma_r$ mit paarweise disjunkten Trägern, so dass $\sigma = \sigma_1 \circ \ldots \circ \sigma_r$ gilt.*

3. *Für $\sigma \in S_n$ existieren (nicht eindeutig bestimmte) Transpositionen $\tau_1, \ldots, \tau_s$ mit $\sigma = \tau_1 \circ \ldots \circ \tau_s$.*

Beweis. 1. Das ist klar, da sich Zyklen mit disjunktem Träger „gegenseitig nicht beeinflussen".

2. Sei $H := \langle \sigma \rangle$ die von σ erzeugte zyklische Untergruppe von S_n. Diese operiert in natürlicher Weise auf der Menge $\{1, \ldots, n\}$, einfach, weil H eine Untergruppe von S_n ist (siehe Beispiel 2. nach Lemma 2.19). Nach Lemma 2.19 ist dann $\{1, \ldots, n\}$ disjunkte Vereinigung der Bahnen dieser Gruppenoperation. Wir betrachten jetzt alle Bahnen $B_1, \ldots, B_k$, welche aus mindestens 2 Elementen bestehen. Jede dieser Bahnen hat dann die Form
$$B_i = \{x_i, \sigma(x_i), \ldots, \sigma^{r_i - 1}(x_i)\}$$
wobei $x_i \in B_i$ und $r_i = |B_i|$ ist. Dann definieren wir den Zyklus $Z_i := (x_i\ \sigma(x_i)\ \ldots\ \sigma^{r_i-1}(x_i))$, und man sieht sofort, dass
$$\sigma = Z_1 \circ \ldots \circ Z_k$$
ist. Die Träger der Zyklen sind gerade die Bahnen B_i, also paarweise disjunkt. Andererseits gibt jede Zerlegung von σ in Zyklen mit paarweise disjunkten Trägern eine Zerlegung von $\{1, \ldots, n\}$ in H-Bahnen, da letztere eindeutig ist, muss auch die Zyklenzerlegung eindeutig sein (immer bis auf Reihenfolge, welche wegen 1. in der Produktdarstellung $\sigma = Z_1 \circ \ldots \circ Z_k$ keine Rolle spielt).

3. Man rechnet leicht nach, dass man die folgende Darstellung eines Zyklus als Produkt von Transpositionen hat:
$$(a_1\ \ldots\ a_k) = (a_1\ a_2) \circ (a_2\ a_3) \circ \ldots \circ (a_{k-1}\ a_k), \tag{2.3}$$
und dann ergibt sich die zu zeigende Aussage aus Teil 2.

□

Wir diskutieren einige einfache Beispiele zur Berechnung der Zyklenzerlegung: Sei $\sigma \in S_6$ mit
$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 3 & 5 & 6 & 4 & 2 & 1 \end{pmatrix}.$$
Anders geschrieben ist diese Permutation gegeben durch $1 \to 3 \to 6 \to 1$, $2 \to 5 \to 2$, $4 \to 4$, also ist
$$\sigma = (1\ 3\ 6)(2\ 5)(4) = (1\ 3\ 6)(2\ 5) = (2\ 5)(1\ 3\ 6) = (5\ 2)(3\ 6\ 1).$$
Ein weiteres Beispiel: Sei $\psi = (1\ 2\ 3)(1\ 3\ 4\ 5)(2\ 4\ 6\ 7) \in S_7$. Man hat folgende Abbildungsschritte: $1 \to 1$, $2 \to 5 \to 2$, $3 \to 4 \to 6 \to 7 \to 3$, also ist
$$\psi = (2\ 5)(3\ 4\ 6\ 7) = (3\ 4\ 6\ 7)(2\ 5).$$
Bemerkung: Bei der Komposition von Zyklen, werden diese von rechts abgearbeitet (wie allgemein bei der Komposition von Abbildungen), aber innerhalb eines Zykels läuft man von links nach rechts.
Als Konsequenz des vorherigen Satzes erhalten wir eine einfache Methode der Berechnung des Vorzeichens einer Permutation.

Korollar 2.38. 1. *Sei $\sigma = (a_1\ \ldots\ a_k)$ ein Zyklus der Länge k (d.h., $|\mathrm{Tr}(\sigma)| = k$), dann ist* $\mathrm{sign}(\sigma) = (-1)^{k-1}$.

2. *Sei $\sigma \in S_n$ beliebig, und gelte die Zerlegung*
$$\sigma = \sigma_1 \circ \ldots \circ \sigma_r,$$
wobei σ_i Zyklen der Länge k_i sind, dann ist $\mathrm{sign}(\sigma) = \prod_{i=1}^{r} (-1)^{k_i - 1}$.

Beweis. 1. Wegen Formel (2.3) reicht es, zu zeigen, dass $\operatorname{sign}((a\,b)) = -1$ für eine beliebige Transposition $(a\,b)$ gilt. Die Aussage ist offensichtlich, falls $a+1=b$ ist. Sei andererseits $a<b$ beliebig, dann ist (Übung: nachrechnen)

$$(a\,b) = (a\;a+1) \circ (a+1\;a+2) \circ \ldots \circ (b-1\;b) \circ (b-2\;b-1) \circ \ldots \circ (a+1\;a+2) \circ (a\;a+1)$$

In dieser Formel stehen auf der rechten Seite $2\cdot(b-a)-1$, also eine ungerade Anzahl von Transpositionen, welche jeweils das Vorzeichen -1 haben, also ist $\operatorname{sign}((a\;b)) = -1$, wie gewünscht.

2. Dies ist klar, weil das Vorzeichen nach Satz 2.36 ein Gruppenhomomorphismus ist.

□

Für die weiteren Untersuchungen ist die folgende Untergruppe von S_n von besonderer Bedeutung.

Definition 2.39. *Die Gruppe*

$$A_n := \ker(\operatorname{sign} : S_n \longrightarrow \{1,-1\}) = \{\sigma \in S_n \mid \operatorname{sign}(\sigma) = 1\}$$

heißt alternierende Gruppe. A_n ist als Kern eines Gruppenhomomorphismus ein Normalteiler in S_n. Für $n>1$ folgt wegen aus dem Homomorphiesatz (Satz 2.11), dass $S_n/A_n \cong \{1,-1\}$, also ist $(S_n : A_n) = 2$.

Gleich werden wir die Frage der Auflösbarkeit (Definition 2.41) untersuchen, hierbei spielt das folgende Ergebnis eine zentrale Rolle.

Lemma 2.40. *Für $n \geq 3$ wird A_n von den 3-Zykeln erzeugt, d.h., jedes Element von A_n ist ein Produkt von Zyklen der Länge 3.*

Beweis. Sei $n \geq 3$ und seien paarweise verschiedene Zahlen $a_1, a_2, a_3 \in \{1,\ldots,n\}$ gegeben. Dann gilt

$$(a_1\,a_2) \circ (a_2\,a_3) = (a_1\,a_2\,a_3),$$

und analog für paarweise verschiedene Zahlen $a_1, a_2, a_3, a_4 \in \{1,\ldots,n\}$ ist

$$(a_1\,a_2) \circ (a_3\,a_4) = (a_1\,a_3\,a_2) \circ (a_1\,a_3\,a_4).$$

Nun verwenden wir die Tatsache (Satz 2.37, 3.), dass sich jede Permutation als Produkt von Transpositionen darstellen lässt. Ist die Permutation gerade, so muss sie Produkt einer geraden Anzahl von Transpositionen sein. Jeweils zwei solcher Transpositionen kann man mit den obigen Formeln (und der Tatsache, dass $(a_1\,a_2)\circ(a_1\,a_2) = \mathrm{id}$ gilt), als Produkt von 3 Zyklen schreiben, also ist auch die gegeben Permutation aus A_n ein Produkt von 3-Zyklen. □

Für spätere Anwendungen in der Galoistheorie benötigen wir den Begriff der Auflösung einer Gruppe, den wir jetzt einführen. Insbesondere werden wir dann die Auflösbarkeit von symmetrischen Gruppen untersuchen.

Definition 2.41. *Sei G eine Gruppe, dann heißt eine Kette von Untergruppen*

$$G = G_0 \supset G_1 \supset \ldots \supset G_n = \{1\}$$

eine Normalreihe, falls $G_i \lhd G_{i-1}$ für alle $i = 1,\ldots,n$ gilt. G heißt auflösbar, falls es eine Normalreihe mit abelschen *Quotienten G_{i-1}/G_i besitzt.*

Selbstverständlich sind alle abelschen Gruppen auflösbar, denn der Quotient einer abelschen Gruppe ist natürlich wieder abelsch. Die Problemstellung beim Nachweis der Auflösbarkeit besteht gerade darin, für eine gegebenen Gruppe, welche selbst nicht abelsch ist, geeignete Normalteiler zu konstruieren, so dass der Quotient der abelsch wird. Hierzu sind die folgende Begriffe nützlich.

Definition 2.42. *Sei G eine Gruppe.*

1. *Für $a, b \in G$ heißt $[a,b] := aba^{-1}b^{-1}$ der Kommutator von a und b.*
2. *Für Untergruppen $H_1, H_2 < G$ sei $[H_1, H_2]$ die von allen Elementen $[a,b]$ mit $a \in H_1, b \in H_2$ erzeugte Untergruppe von G. Insbesondere nennt man $[G,G]$ die Kommutatoruntergruppe von G.*
3. *Der i-te iterierte Kommutator D^iG ist induktiv definiert durch*

$$D^0G := G \qquad \text{und} \qquad D^{i+1}G := [D^iG, D^iG]$$

Wir haben zunächst die folgenden einfachen Aussagen über Kommutatoren.

Lemma 2.43. *1. $[G,G]$ ist die Menge aller endlichen Produkte von Kommutatoren von Elementen aus G.*

2. $[G,G]$ ist Normalteiler in G. Genauer ist $[G,G]$ der (bezüglich der Inklusion) kleinste Normalteiler N von G, so dass der Quotient G/N abelsch ist.

Beweis. 1. Zu zeigen ist, dass das Inverse eines Kommutators wieder ein Kommutator ist, dies gilt wegen

$$[a,b]^{-1} = \left(aba^{-1}b^{-1}\right)^{-1} = bab^{-1}a^{-1} = [b,a].$$

2. $[G,G] \lhd G$ folgt aus der folgenden Rechnung, welche für alle $a, b, g \in G$ gilt.

$$g[a,b]g^{-1} = gaba^{-1}b^{-1}g^{-1} = (gag^{-1})(gbg^{-1})(ga^{-1}g^{-1})(gb^{-1}g^{-1}) =$$

$$(gag^{-1})(gbg^{-1})(gag^{-1})^{-1}(gbg^{-1})^{-1} = [(gag^{-1}), (gbg^{-1})] \in [G,G]$$

Betrachte nun den Quotienten $G/[G,G]$, dann gilt für alle $a, b \in G$, dass

$$\overline{a} \cdot \overline{b} \cdot \overline{a}^{-1} \cdot \overline{b}^{-1} = \overline{a \cdot a^{-1} \cdot b \cdot b^{-1}} = \overline{1}$$

ist, also gilt $\overline{a} \cdot \overline{b} = \overline{b} \cdot \overline{a}$, d.h., ist $G/[G,G]$ ist abelsch. Wir wollen nun noch zeigen, dass $[G,G]$ tatsächlich der bezüglich der Inklusion kleinste Normalteiler N ist, so dass der Quotient G/N abelsch ist. Sei also $N \lhd G$ ein beliebiger Normalteiler und sei G/N abelsch. Nach Definition wird $[G,G]$ von allen Kommutatoren $[a,b]$ erzeugt. Angenommen, es gäbe einen Kommutator $[a,b]$, welcher nicht in N liegt, dann gilt notwendigerweise $\overline{a}\overline{b} \neq \overline{b}\overline{a}$ in G/N, und dann wäre G/N nicht abelsch, was einen Widerspruch zur Annahme darstellt. Somit gilt $[a,b] \in N$ für alle $a, b \in G$. Da der Normalteiler $[G,G]$ von allen Kommutatoren $[a,b]$ erzeugt wird, folgt demnach $[G,G] \subset N$. Also muss für alle $N \lhd G$, so dass G/N abelsch ist, $[G,G] \subset N$ gelten. Folglich ist $[G,G]$ der kleinste Normalteiler N, so dass G/N abelsch ist.

□

Auflösbarkeit von Gruppen kann man nun folgendermaßen charakterisieren.

Satz 2.44. *G ist auflösbar genau dann, wenn es ein $n \in \mathbb{N}$ gibt mit $D^nG = \{1\}$.*

Beweis. Sei zunächst $D^nG = \{1\}$ für ein $n \in \mathbb{N}$, dann haben wir die Normalreihe

$$\{1\} = D^nG \lhd D^{n-1}G \lhd \ldots \lhd D^1G = [G,G] \lhd D^0G = G$$

und die Quotienten $D^{i-1}G/D^iG = D^{i-1}G/[D^{i-1}G, D^{i-1}G]$ sind nach Lemma 2.43, 2. abelsch.
Sei andererseits eine Normalreihe

$$\{1\} = G_n \lhd G_{n-1} \lhd \ldots G_1 \lhd G_0 = G$$

mit abelschen Quotienten gegeben. Wir zeigen induktiv, dass $D^iG \subset G_i$ gelten muss, dann folgt die Aussage des Satzes wegen $D^nG \subset G_n = \{1\}$. Für $i = 0$ ist die Behauptung klar, sei also $D^iG \subset G_i$ für $i < n$. Da G_i/G_{i+1} abelsch ist, muss also wegen Lemma 2.43, 2. die Inklusion $[G_i, G_i] \subset G_{i+1}$ gelten, und dann ist

$$D^{i+1}G = [D^iG, D^iG] \subset [G_i, G_i] \subset G_{i+1},$$

wie gefordert. □

Für spätere Anwendungen benötigen wir noch eine Präzisierung des eben gezeigten Resultats.

Satz 2.45. *1. Sei G eine endliche und auflösbare Gruppe. Sei $G = G_0 \supsetneq G_1 \supsetneq \ldots \supsetneq G_n = \{1\}$ eine Normalreihe mit abelschen Quotienten. Dann existiert eine Verfeinerung dieser Normalreihe, deren Quotienten zyklisch von Primzahlordnung sind.*

2. Sei G eine Gruppe und $H < G$. Falls G auflösbar ist, so auch H. Falls $H \lhd G$ gilt, dann ist G auflösbar genau dann, wenn H und G/H auflösbar sind.

Beweis. 1. Angenommen, G_i/G_{i+1} sei nicht zyklisch von Primzahlordnung. Wähle ein $\overline{a} \in G_i/G_{i+1}$ mit $\overline{a} \neq 1$ und $\langle\overline{a}\rangle \subsetneq G_i/G_{i+1}$. Dann ist $\langle\overline{a}\rangle \lhd G_i/G_{i+1}$, und wir setzen $H := \pi^{-1}(\langle\overline{a}\rangle)$, wobei $\pi : G_i \to G_i/G_{i+1}$ die kanonische Projektion ist. Es gilt dann $H \lhd G_i$, und $G_{i+1} \lhd H$. Damit können wir die Normalreihe zu

$$G = G_0 \supsetneq G_1 \supsetneq \ldots \supsetneq G_i \supsetneq H \supsetneq G_{i+1} \supsetneq \ldots \supsetneq G_n = \{1\}$$

verfeinern, und diese verfeinerte Normalreihe hat ebenfalls abelsche Quotienten (denn H/G_{i+1} ist eine Untergruppe und G_i/H ist eine Quotientengruppe der abelschen Gruppe G_i/G_{i+1}). Indem man dieses Verfahren wiederholt, erreicht man nach endlich vielen Schritten, dass die Quotienten der konstruierten Normalreihen zyklisch von Primzahlordnung sind.

2. Wir verwenden das Kriterium aus Satz 2.44. Falls G auflösbar ist, folgt wegen $D^n H \subset D^n G$, dass auch H auflösbar ist. Sei nun H ein Normalteiler ist G und $\pi : G \to G/H$ die kanonische Projektion. Man prüft leicht nach, dass dann $D^i(\pi(G)) = \pi(D^i G)$ gilt. Wenn also G auflösbar ist, so auch G/H. Seien andererseits H sowie G/H auflösbar. Es gibt dann ein $n \in \mathbb{N}$, so dass $D^n H = \{1\}$ und $D^n G/H = \{1\}$ gilt. Damit folgt $\pi(D^n G) = D^n(G/H) = \{1\}$, d.h. $D^n G \subset H$. Dann ist $D^{2n} G = D^n(D^n G) \subset D^n H = \{1\}$, und damit ist nach Satz 2.44 auch G auflösbar.

□

Zur Anwendung des eben bewiesenen Kriteriums für Auflösbarkeit berechnen wir Kommutatorgruppen von symmetrischen und alternierenden Gruppen.

Lemma 2.46. *Wir haben*

$$[S_n, S_n] = A_n \qquad \forall n \geq 2$$

$$[A_n, A_n] = \begin{cases} \{1\} & \text{für } n = 2, 3 \\ V_4 & \text{für } n = 4 \\ A_n & \text{für } n \geq 5 \end{cases}$$

Hierbei ist V_4 die sogenannte Kleinsche Vierergruppe, definiert durch

$$V_4 := \{\mathrm{id}\,, (12)(34), (13)(24), (14)(23)\} \subset A_4 \subset S_4.$$

Man prüft leicht nach, dass $V_4 \lhd A_4$ gilt (Übung). Ebenso leicht sieht man, dass $V_4 \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ gilt, insbesondere ist V_4 abelsch.

Beweis. Wir berechnen zunächst die Kommutatorgruppe von S_n: Wegen $S_n/A_n \cong \mathbb{Z}/2\mathbb{Z}$ ist dieser Quotient abelsch, und dann muss Lemma 2.43, 2. in $[S_n, S_n]$ in A_n enthalten sein, im Fall $n = 2$ wegen $A_2 = \{1\}$ gilt dann sogar die Gleichheit. Es bleibt also noch $A_n \subset [S_n, S_n]$ für $n \geq 3$ zu zeigen. Wir wissen schon, dass jedes Element in A_n für $n \geq 3$ ein Produkt von 3-Zyklen ist, aber andererseits ist wegen

$$(a_1\, a_2\, a_3) = (a_1\, a_3)(a_2\, a_3)(a_3\, a_1)(a_3\, a_2) = (a_1\, a_3)(a_2\, a_3)(a_1\, a_3)^{-1}(a_2\, a_3)^{-1}$$

jeder 3-Zyklus ein Kommutator, also ist jedes Element in A_n ein Produkt von Kommutatoren und damit wegen 2.43, 1. ein Element von $[S_n, S_n]$.
Zur Berechung von $[A_n, A_n]$ bemerken wir zunächst, dass $A_2 \cong \{1\}$, und $A_3 \cong \mathbb{Z}/3\mathbb{Z}$, also abelsch sind. Daher ist für $n = 2, 3$ der Kommutator $[A_n, A_n]$ trivial.
Klar ist auch, dass $[A_4, A_4] \subset V_4$ gilt, weil der Quotient A_4/V_4 Ordnung 3 hat und also abelsch ist. Andererseits gilt für paarweise verschiedene Elements $a_1, a_2, a_3, a_4 \in \{1, \ldots, 4\}$, dass

$$(a_1\, a_2)(a_3\, a_4) = (a_1\, a_2\, a_3)(a_1\, a_2\, a_4)(a_1\, a_2\, a_3)^{-1}(a_1\, a_2\, a_4)^{-1}$$

ist, also folgt auch $V_4 \subset [A_4, A_4]$.
Es bleibt die Gleichung $[A_n, A_n] = A_n$ für $n \geq 5$, d.h., die Inklusion $A_n \subset [A_n, A_n]$ zu zeigen. Erneut reicht es, zu zeigen, dass jeder 3-Zyklus ein Produkt von Kommutatoren ist, allerdings müssen diese Kommutatoren von Elementen in A_n sein (die obige Gleichung $(a_1\, a_2\, a_3) = (a_1\, a_3)(a_2\, a_3)(a_1\, a_3)^{-1}(a_2\, a_3)^{-1}$ liefert nur die Inklusion $A_n \subset [S_n, S_n]$). Sei also $(a_1\, a_2\, a_3)$ ein 3-Zyklus in A_n, $n \geq 5$. Dann gibt es $a_4, a_5 \in \{1, \ldots, n\}$, so dass die Menge $\{a_1, a_2, a_3, a_4, a_5\}$ fünf Elemente hat, d.h., so dass die Zahlen $a_1, \ldots, a_5$ paarweise verschieden sind. Dann gilt

$$(a_1\, a_2\, a_3) = (a_1\, a_2\, a_4)(a_1\, a_3\, a_5)(a_1\, a_2\, a_4)^{-1}(a_1\, a_3\, a_5)^{-1}$$

und wegen $\operatorname{sign}(a_1\, a_2\, a_4) = \operatorname{sign}(a_1\, a_3\, a_5) = 1$ ist also $A_n \subset [A_n, A_n]$. □

Wir erhalten die folgende wichtige Konsequenz.

Korollar 2.47. *Für $n \geq 5$ sind sowohl A_n als auch S_n nicht auflösbar. Für $n \leq 4$ sind S_n und A_n auflösbar.*

Beweis. Für $n \geq 5$ ist die Kommutatorreihe $D^i S_n$ nach dem eben bewiesenen Lemma 2.46 gegeben durch

$$D^0 S_n = S_n \supset D^1 S_n = A_n \supset D^2 S_n = A_n \supset \ldots \supset D^i S_n = A_n \supset \ldots$$

so dass wegen des Auflösbarkeitskriteriums (Satz 2.44) weder S_n noch A_n auflösbar sein können.
Für $n \leq 4$ liefern die Kommutatorreihen $D^i S_n$ direkt Normalreihen mit abelschen Quotienten, nämlich:

$$S_2 \supset \{1\}$$

$$S_3 \supset A_3 \supset \{1\}$$

$$S_4 \supset A_4 \supset V_4 = [A_4, A_4] \supset \{1\}$$

Das die Quotienten abelsch sind, kann man auch konkret daran erkennen, dass alle auftretenden Indizes von Untergruppen kleiner gleich 3 sind, aber alle Gruppen der Ordnung höchstens drei sind abelsch. □

Zum Abschluss dieses Kapitels machen wir noch eine Bemerkung zum wichtigen Begriff der *einfachen* Gruppen. Wir haben diesen in der obigen Argumentation vermieden, aber er passt gut hierher.

Definition 2.48. *Ein Gruppe G heißt einfach, falls aus $N \lhd G$ folgt, dass $N = \{1\}$ oder $N = G$ ist.*

Wir haben oben gezeigt, dass A_n für $n \geq 5$ keine echten Normalteiler N haben kann, so dass A_n/N abelsch ist. Tatsächlich gibt es aber überhaupt keine echten Normalteiler von A_n, $n \geq 5$ (der Beweis funktioniert ähnlich), und daher ist A_n für $n \geq 5$ einfach.
Die einfachen endlichen Gruppen sind alle klassifiziert, es existierten 18 unendliche Serien (z.B. die Gruppen $\mathbb{Z}/p\mathbb{Z}$ für Primzahlen p und eben die Gruppen A_n für $n \geq 5$), sowie 26 einzelne (sporadische) Gruppen (die größte ist die sogenannte Monster-Gruppe und hat ca. 10^{54} Elemente). Wir erwähnen noch die folgenden Ergebnisse zur Klassifikation einfacher Gruppen.

Satz 2.49. *1. Die einzigen einfachen abelschen Gruppen ungerader Ordnung sind die sind die Gruppen $\mathbb{Z}/p\mathbb{Z}$ für eine Primzahl $p > 2$.*

2. *Die einzigen endlichen einfachen Gruppen ungerader Ordnung sind die Gruppen $\mathbb{Z}/p\mathbb{Z}$ für eine Primzahl $p > 2$.*

Beweis. 1. Sei G endlich, abelsch und einfach und $\mathrm{ord}(G) > 1$, dann gibt es ein $a \in G\backslash\{1\}$. Da G abelsch ist, gilt $\langle a\rangle \lhd G$, da aber G einfach sein soll, muss $\langle a\rangle = G$ gelten, und dann ist G zyklisch von Primzahlordnung.

2. Dies ist der Satz von Feit-Thompson, welcher hier nicht beweisen wird.

□

Kapitel 3

Ringe

Eine ganz zentrale algebraische Struktur sind Ringe, welchen wir uns in diesem Kapitel widmen. Die zwei wichtigsten Beispiele sind der Ring der ganzen Zahlen, und der Polynomring über einem Körper. Analog zu der Quotientenkonstruktion für Gruppen werden wir Quotienten- bzw. Faktorringe definieren, und dies liefert ein Konstruktionsverfahren für neue Ringe, und, manchmal, für Körper. Dies werden wir in den späteren Kapiteln intensiv benutzen.
Wir werden außerdem die Konstruktion des Quotientenkörpers studieren (und allgemeiner Lokalisierungen von Ringen), dies ist die natürliche Verallgemeinerung der Konstruktion von $\mathbb{Q}$ aus $\mathbb{Z}$. Schließlich werden wir Moduln über Hauptidealringen studieren, und damit einige der Ergebnisse über endliche abelsche Gruppen des letzten Kapitels verallgemeinern können.

3.1 Ringe und Ideale

Wir beginnen mit der wichtigsten Definition dieses Kapitels.

Definition 3.1. *Ein Ring ist ein Tripel $(R, +, \cdot)$, bestehend aus einer nicht-leeren Menge R und zwei Verknüpfungen*

$$+ : R \times R \longrightarrow R$$

$$\cdot : R \times R \longrightarrow R$$

welche die folgenden Eigenschaften erfüllen:

1. *$(R, +)$ ist eine abelsche Gruppe (deren neutrales Element wir mit 0 bezeichnen).*
2. *$\cdot$ ist assoziativ, d.h. $\forall a, b, c \in R : (a \cdot b) \cdot c = a \cdot (b \cdot c)$*
3. *Es gelten die Distributivgesetze, d.h., für alle $a, b, c \in R$ ist*
   (a) *$a \cdot (b + c) = a \cdot b + a \cdot c$*
   (b) *$(a + b) \cdot c = a \cdot c + b \cdot c$*

Existiert ein Element $1 \in R$, welches $1 \cdot a = a \cdot 1 = a$ erfüllt, dann heißt 1 Eins oder Einselement (es ist wegen $1 = 1 \cdot 1' = 1'$ eindeutig), und R heißt Ring mit Eins oder unitärer Ring.
Falls für alle $a, b \in R$ gilt, dass $a \cdot b = b \cdot a$ ist, so nennt man R einen kommutativen Ring.

Nach der obigen Definition ist $(R, +)$ eine abelsche Gruppe. Hingegen ist R zusammen mit der Verknüpfung $\cdot$ keine Gruppe, weil beliebige Elemente von R keine multiplikativen Inversen haben müssen. Daher definiert man:

Definition 3.2. *Sei R ein unitärer Ring und $\{0\} \subsetneq R$, dann bezeichne*

$$R^* := \{r \in R \,|\, \exists s \in R : rs = 1\}$$

die Menge der invertierbaren Elemente von R. Dann ist $(R^*, \cdot)$ eine Gruppe, genannt die Einheitengruppe von R.

Wir können jetzt die wohlbekannte Definition eines Körpers als ein Spezialfall der Defintion eines Ringes als einfache Aussage umformulieren.

Lemma 3.3. *Ein kommutativer Ring R mit 1 ist ein Körper genau dann, wenn $R^* = R\backslash\{0\}$ gilt.*

Beweis. $R^* = R\backslash\{0\}$ bedeutet, dass jedes Element von $R\backslash\{0\}$ invertierbar ist, aber dann ist (da R kommutativ sein soll), $(R\backslash\{0\}, \cdot)$ eine abelsche Gruppe, und dies ist genau das fehlende Axiom, welches $(R, +, \cdot)$ zu einem Körper macht. □

Wir zeigen jetzt die folgenden elementaren Eigenschaften von Ringen.

Lemma 3.4. *Sei R ein Ring, dann gilt*

1. $\forall a \in R : 0 \cdot a = a \cdot 0 = 0$
2. *Ist R unitär, und gilt $|R| > 1$, so ist $1 \neq 0$.*
3. $\forall a, b \in R : (-a) \cdot b = -(ab) = a \cdot (-b)$ *sowie* $(-a) \cdot (-b) = ab$.
4. *Falls R ein Körper ist, dann folgt* $a \cdot b = 0 \implies a = 0$ oder $b = 0$

Beweis.

1. $a \cdot 0 = a \cdot (0 + 0) = a \cdot 0 + a \cdot 0$, also folgt $a \cdot 0 = 0$, analog zeigt man $0 \cdot a = 0$.
2. Sei $a \in R\backslash\{0\}$, dann folgt aus 1., dass $a \cdot 0 = 0 \neq a$ ist, aber $a \cdot 1 = a$, also kann nicht $1 = 0$ gelten.
3. Wir haben $(-a) \cdot b + a \cdot b = (-a + a) \cdot b = 0 \cdot b \overset{1.}{=} 0$, also ist $(-a) \cdot b = -(ab)$, und analog sieht man, dass $a \cdot (-b) = -(ab)$ gilt.

   Genauso: $(-a) \cdot (-b) + a \cdot (-b) = (-a + a) \cdot (-b) = 0 \implies (-a) \cdot (-b) = -(a \cdot (-b))$, und wir wissen schon, dass $a \cdot (-b) = -(ab)$ ist, also folgt $(-a) \cdot (-b) = a \cdot b$.
4. Sei $a \cdot b = 0$ und $a \neq 0$, dann gilt $b = 1 \cdot b \overset{R \text{ Körper}}{=} (a^{-1} \cdot a) \cdot b = a^{-1} \cdot (a \cdot b) = a^{-1} \cdot 0 \overset{1.}{=} 0$.

□

Die letzte Eigenschaft, welche für Körper gilt, kann man auch für allgemeinere Ring betrachten, und diese Klasse von Ringen ist so wichtig, dass sie einen eigenen Namen hat.

Definition 3.5. *Sei R ein kommutativer Ring mit 1. Ein Element $a \in R$ heißt Nullteiler, falls es ein $b \in R$ mit $b \neq 0$ gibt, so dass $a \cdot b = 0$ ist. Natürlich ist $0 \in R$ immer ein Nullteiler, und falls R ein Körper ist, gibt es auch keine anderen. Der Ring R heißt* nullteilerfrei *oder* Integritätsring*, falls R außer 0 keine weiteren Nullteiler enthält.*
Man zeigt leicht, dass in einem Integritätsring R die Kürzungsregel

$$a \cdot b = a \cdot c \quad \implies b = c$$

für alle $a \neq 0$ gilt.

Wir diskutieren jetzt einige einfache Beispiele für Ringe.

1. Alle Körper sind kommutative Ringe mit 1, insbesondere sind also $\mathbb{Q}$, $\mathbb{R}$ und $\mathbb{C}$ mit der gewöhnlichen Addition und Multiplikation Ringe (und, wie eben schon erwähnt, auch Integritätsringe).

2. $(\mathbb{Z}, +, \cdot)$ ist ein Ring, sogar ein Integritätsring, aber kein Körper, denn nur 1 und -1 haben ein inverses Element bezüglich $\cdot$, d.h. $\mathbb{Z}^* = \{1, -1\} \subsetneq \mathbb{Z}\backslash\{0\}$.

3. Sei R ein beliebiger Ring und $n \in \mathbb{N}_{>0}$, dann ist die Menge der quadratischen $n \times n$-Matrizen

$$\mathrm{Mat}(n \times n, R) := \left\{ (a_{ij})_{i,j \in \{1,\ldots,n\}} \,|\, a_{ij} \in R \right\}$$

mit Einträgen aus R zusammen mit der Addition und der Multiplikation von Matrizen ein Ring. Wir haben

$$\mathrm{Mat}(n \times n, R)^* = \mathrm{Gl}_n(R) := \{A \in \mathrm{Mat}(n \times n, R) \,|\, \det(A) \in R^*\}.$$

Diese letzte Aussage folgt wie in der linearen Algebra aus der Formel für die inverse Matrix, d.h.

$$A^{-1} = \frac{1}{\det(A)} \cdot A^{\#},$$

wobei $A^{\#} := (a_{ij}^{\#})_{i,j \in \{1,\ldots,n\}}$ die Komplementärmatrix ist mit

$$a_{ji}^{\#} := (-1)^{i+j} \det(A^{(i,j)}),$$

hier ist $A^{(i,j)}$ die Matrix, welche man aus A durch Streichen der i-ten Zeile und der j-ten Spalte erhält.

Man beachte, dass zum Beispiel Matrizen mit ganzzahligen Einträgen nur dann in $\mathrm{Mat}(n \times n, \mathbb{Z})$ invertierbar sind, wenn ihre Determinante gleich 1 oder -1 ist. Hingegen sind sie natürlich in $\mathrm{Mat}(n \times n, \mathbb{Q})$ invertierbar, wenn ihre Determinante ungleich Null ist.

Wir haben $\mathrm{Mat}(1 \times 1, R) = R$ und entsprechend $\mathrm{Gl}_1 R = R^*$. Daher ist $\mathrm{Mat}(1 \times 1, R)$ kommutativ, falls R kommutativ ist (z.B. falls R ein Körper ist). Hingegen ist für $n > 1$ der Ring $\mathrm{Mat}(n \times n, R)$ im Allgemeinen nicht kommutativ, selbst wenn R kommutativ (z.B. ein Körper) ist.

4. Die einelementige Menge $\{0\}$ ist ein Ring mit der trivialen Addition $+$ und mit $\cdot = +$. Es ist sogar ein unitärer Ring mit $1 = 0$, und, wie wir im Punkt 2. des letzten Lemmas gesehen haben, der einzige unitäre Ring, in dem $1 = 0$ gilt.

5. Sei X eine beliebige Menge, R ein Ring, dann definiere

$$R^X := \{f : X \to R\}$$

als die Menge der Funktionen von X mit Werten in R. Dann ist R^X mit der sogenannten punktweisen Addition und Multiplikation

$$(f + g) : X \longrightarrow R;\ x \longmapsto f(x) + g(x)$$

$$(f \cdot g) : X \longrightarrow R;\ x \longmapsto f(x) \cdot g(x)$$

ein Ring, hierbei ist $0_{R^X} : X \to R;\ x \mapsto 0$. Falls R unitär ist, dann auch R^X, mit $1_{R^X} : X \to R;\ x \mapsto 1$.

R^X ist im Allgemeinen kein Integritätsring, selbst wenn R einer ist. Als Beispiel betrachten wir $X = \mathbb{R}$ (und R beliebig), und die beiden Funktionen

$$f(x) := \begin{cases} 1 & x \in \mathbb{Q} \\ 0 & x \notin \mathbb{Q} \end{cases}$$

$$g(x) := \begin{cases} 0 & x \in \mathbb{Q} \\ 1 & x \notin \mathbb{Q} \end{cases}$$

Dann ist offensichtlich weder f noch g die Nullfunktion $0_{\mathbb{R}} \in R^{\mathbb{R}}$, aber $f \cdot g = 0_{\mathbb{R}}$, denn $(f \cdot g)(x) = f(x) \cdot g(x) = 0 \in R$ für alle $x \in \mathbb{R}$.

Um die Notationen etwas zu vereinfachen, wollen wir im weiteren Verlauf, sofern nicht explizit etwas anderes gesagt wird, unter einem Ring immer einen *kommutativen Ring mit* 1 verstehen.
Wir diskutieren jetzt ein weiteres wichtiges Beispiel für Ringe, welches im weiteren Verlauf eine überragende Bedeutung haben wird, nämlich die Polynomringe.

Definition 3.6. *Sei R ein Ring und x ein formales Symbol. Dann setzen wir $(R[[x]],+) := (R^{\mathbb{N}},+)$, d.h., wir betrachten die Menge der Abbildungen $\mathbb{N} \to R$, zusammen mit der oben definierten Addition. Eine Abbildung $f : \mathbb{N} \to R$ schreiben wir als formale Potenzreihe in x, d.h.:*

$$f = \sum_{i=0}^{\infty} f(i) \cdot x^i$$

Wir definieren nun eine neue Multiplikation auf $R[[x]]$, welche gegeben ist durch

$$\left(\sum_{i=0}^{\infty} a_i x^i\right) \cdot \left(\sum_{j=0}^{\infty} b_j x^j\right) = \left(\sum_{k=0}^{\infty} c_i x^k\right)$$

mit $c_k = \sum_{i=0}^{k} a_i \cdot b_{k-i}$. Dann ist $(R[[x]],+,\cdot)$ ein Ring, genannt der Ring der formalen Potenzreihen in einer Variablen (nämlich x) über R (d.h., mit Koeffizienten aus R).
Betrachte nun die Teilmenge

$$R[x] := R^{(\mathbb{N})} := \left\{ f \in R[[x]] = R^{\mathbb{N}} \mid \exists n \in \mathbb{N} : f(i) = 0 \ \forall i > n \right\}.$$

Man prüft leicht, dass sich die Verknüpfungen $+$ und $\cdot$ von $R[[x]]$ auf $R[x]$ einschränken. Dann ist auch $(R[x],+,\cdot)$ ein Ring, genannt der Polynomring in x über R. Wir definieren den Grad eines Polynoms als $f = a_n x^n + \ldots + a_1 x + a_0 \in R[x]$

$$\deg(f) = \max_{i \in \mathbb{N}} (a_i \neq 0).$$

Das Nullpolynom (also das Nullelement in $R[x]$) hat nach Definition Grad $-\infty$. Falls $f = a_k x^k + \ldots + a_0$ mit $a_k \neq 0$ (dann ist also $\deg(f) = k$) heißt a_k Leitkoeffizient von f. Ist $a_k = 1$, dann heißt f unitär.
Für $n \in \mathbb{N}$ und formale Symbole $x_1, \ldots, x_n$ definiert man induktiv

$$\begin{aligned} R[x_1,\ldots,x_n] &:= R[x_1,\ldots,x_{n-1}][x_n] \\ R[[x_1,\ldots,x_n]] &:= R[[x_1,\ldots,x_{n-1}]][[x_n]] \end{aligned}$$

als den Polynomring bzw. den formalen Potenzreihenring in den Variablen $x_1, \ldots, x_n$. Hierbei muss man zeigen, dass diese Definition nicht von der Reihenfolge der Variablen $x_1, \ldots, x_n$ abhängt (Übung).

Wir haben die folgenden elementaren Eigenschaften von Polynomringen.

Lemma 3.7. *Sei R ein Ring und $f, g \in R[x]$. Dann gilt:*

1. $\deg(f+g) \leq \max(\deg(f), \deg(g))$,
2. $\deg(f \cdot g) \leq \deg(f) + \deg(g)$,
3. *Falls R ein Integritätsring ist, gilt* $\deg(f \cdot g) = \deg(f) + \deg(g)$,
4. *Sei R ein Integritätsring, dann ist auch $R[x]$ ein Integritätsring, und wir haben $(R[x])^* = R^*$.*

Für die Aussagen über den Grad soll $-\infty + n = -\infty$ für alle $n \in \mathbb{N} \cup \{-\infty\}$ gelten.

Beweis. Falls f oder g gleich dem Nullpolynom sind, stimmen die ersten drei Aussagen offensichtlich. Sei also $n = \deg(f) \geq 0$ und $m = \deg(g) \geq 0$, und wir schreiben $f = \sum_{i=0}^{n} a_i x^i$, sowie $g = \sum_{j=0}^{m} b_j x^j$. Dann ist aber $a_k = b_k = 0$ für alle $k > \max(m, n)$, also auch $a_k + b_k = 0$, und daher $\deg(f+g) \leq \max(\deg(f), \deg(g))$. Analog gilt: Für $k > m + n$ ist $i > n$ oder $k - i > m$ für alle $i \in \{0, \ldots, k\}$, also $a_i \cdot b_{k-i} = 0$, also $\sum_{i+j=k} a_i b_j = 0$, und daher $\deg(f \cdot g) \leq \deg(f) + \deg(g)$. Außerdem ist der Leitkoeffizient von $f \cdot g$ gleich $a_n \cdot b_m$, wobei nach Definition $a_n \neq 0$ und $b_m \neq 0$ gilt. Ist R ein Integritätsring, folgt daraus $a_n \cdot b_m \neq 0$, d.h., wir haben $\deg(f \cdot g) = \deg(f) + \deg(g)$.
Es bleibt, die letzte Aussage zu zeigen: Angenommen, $R[x]$ sei kein Integritätsring, dann existiert also ein Nullteiler $f \in R[x] \backslash \{0\}$, also gibt es $g \in R[x] \backslash \{0\}$ mit $f \cdot g = 0$. Dann gilt, da R Integritätsring ist, aufgrund von Punkt 3., dass

$$-\infty = \deg(0) = \deg(f \cdot g) = \deg(f) + \deg(g).$$

Dies ist ein Widerspruch, da wegen $f, g \in R[x] \backslash \{0\}$ $\deg(f) \geq 0, \deg(g) \geq 0$ gelten muss. Also ist $R[x]$ ein Integritätsring.
Die Inklusion $R^* \subset (R[x])^*$ ist klar, zu zeigen ist die umgekehrte Richtung. Sei also ein invertierbares Polynom $f \in (R[x])^*$ gegeben, dann gibt es ein $g \in R[x]$ mit $f \cdot g = 1$, aber wegen $\deg(1) = 0$ muss dann $\deg(f) = \deg(g) = 0$ gelten, aber das bedeutet $f, g \in R$ und daher auch $f \in R^*$. □

Um mehr Strukturtheorie von Ringen erarbeiten zu können, benötigen wir Begriffe, die es erlauben, zwei Ringe in Beziehung zueinander zu setzen.

Definition 3.8. *Sei R ein Ring, hier nicht notwending kommutativ oder mit* 1.

1. *Eine Teilmenge $U \subset R$ heißt Unterring, falls $(U, +) < (R, +)$ und falls U abgeschlossen unter der Multiplikation $\cdot$ in R ist, falls also $U \cdot U \subset U$ gilt. Klar ist, dass ein Unterring U mit den induzierten Verknüpfungen $+$ und $\cdot$ ein Ring ist.*

   Ist U ein Unterring von R, dann nennt man R auch eine Ringerweiterung von U. Der für uns in dieser Vorlesung wichtigste Spezialfall davon ist der, bei dem sowohl U als auch R Körper sind, dann heißt $R \supset U$ eine Körpererweiterung *(diese werden ab Kapitel 4 ausführlich studiert).*

2. *Sei S ein weiterer Ring (eventuell nicht-kommutativ), dann heißt eine Abbildung $f : R \to S$ ein Ringhomomorphismus, falls $f : (R, +) \to (S, +)$ ein Gruppenhomomorphismus ist und falls*

$$f(a \cdot b) = f(a) \cdot f(b) \quad \forall a, b, \in R$$

   gilt. Falls darüber hinaus R und S unitär sind, soll auch noch $f(1_R) = 1_S$ gelten.

3. *Eine Teilmenge $I \subset R$ heißt Links- (bzw. Rechts-)ideal, falls $(I, +) < (R, +)$ ist und falls für alle $a \in I, r \in R$ gilt, dass $r \cdot a \in I$ (bzw. $a \cdot r \in I$) ist (mit anderen Worten $R \cdot I \subset I$ bzw. $I \cdot R \subset I$).*

   Man beachte, dass mit dieser Definition ein Ideal immer ein Unterring ist, aber das ein Unterring nicht notwendig ein Ideal sein muss.

4. *Ist $I \subset R$ sowohl Links- als auch Rechtsideal, so heißt I Ideal von R. Beachte, dass die Menge der Links- und Rechtsideale in kommutativen Ringen übereinstimmen.*

Das folgende Lemma liefert Beispiele für Unterringe und Ideale, wobei wir ab jetzt wieder annehmen, dass alle Ringe kommutativ mit 1 sind.

Lemma 3.9. *Sei $f : R \to S$ ein Ringhomomorphismus. Dann ist* $\ker(f) = \{a \in R \mid f(a) = 0\}$ *ein Ideal in R und* $\mathrm{Im}(f) = \{b \in S \mid \exists a \in R : f(a) = b\}$ *ein Unterring in S (aber im Allgemeinen kein Ideal).*

Beweis. Wir wissen bereits, dass $(\ker(f), +) < (R, +)$ gilt. Für $a \in \ker(f)$ und $r \in R$ gilt nun wegen der Homomorphismuseigenschaft von f

$$f(r \cdot a) = f(r) \cdot f(a) = f(r) \cdot 0 = 0,$$

und damit ist $r \cdot a \in \ker(f)$, also bildet $\ker(f)$ ein Ideal von R.
Analog wissen wir schon, dass $(\mathrm{Im}(f), +) < (S, +)$ gilt. Seien andererseits Elemente $b, b' \in \mathrm{Im}(f)$ gegeben, dann gibt es $a, a' \in R$ mit $f(a) = b$ und $f(a') = b'$. Dann gilt aber $b \cdot b' = f(a) \cdot f(a') = f(a \cdot a')$, also ist $b \cdot b' \in \mathrm{Im}(f)$. Also ist $\mathrm{Im}(f)$ sogar ein Unterring von S. Ist f surjektiv, dann ist $\mathrm{Im}(f)$ natürlich sogar ein Ideal (nämlich ganz S), aber im Allgemeinen gilt dies nicht, z.B ist $\mathbb{Q}$ als Körper ein Ring, und die injektive Abbildung $\mathbb{Z} \hookrightarrow \mathbb{Q}, x \mapsto x$ ist ein Ringhomomorphismus. $\mathbb{Z}$ ist natürlich ein Unterring von $\mathbb{Q}$, aber kein Ideal, denn für $q = \frac{1}{3}$ und $n = 2$ gilt $q \in \mathbb{Q}$, $n \in \mathbb{Z}$ aber $q \cdot n \notin \mathbb{Z}$. □

Das folgende Lemma zeigt erste wichtige Eigenschaften von und Beispiele für Ideale.

Lemma 3.10. *Sei R ein Ring, dann sind $\{0\}$ und R Ideale. Für ein Ideal $I \subset R$ gilt*

$$I = R \iff 1 \in I \iff \exists a \in R^* \cap I$$

Beweis. Man rechnet direkt nach, dass $\{0\}$ und R die Idealbedingungen erfüllen. Falls $I = R$ ist, folgt natürlich $1 \in I$, und (da 1 immer eine Einheit ist) auch die Bedingung $\exists a \in R^* : a \in I$. Falls andererseits eine Einheit $a \in R^*$ mit $a \in I$ existiert, dann gibt es $a^{-1} \in R$, und aus der Idealbedingung folgt, dass $a^{-1} \cdot a = 1 \in I$ gilt. Dann ist aber für alle $r \in R$ auch $r \cdot 1 = r \in I$, so dass $I = R$ folgt. □

Wir benutzen den Polynomring, um ein einfache, aber nützliche Beispiele von Ringhomomomorphismen angeben zu können.

Lemma 3.11. *Sei R ein Ring, $R[x]$ der Polynomring in einer Variablen über R, und sei $R \subset R'$ eine gegebene Ringerweiterung (zur Erinnerung: sowohl R als auch R' sind kommutativ mit 1). Dann gilt*

1. *Die Abbildung*
$$\begin{aligned} R &\longrightarrow R[x] \\ a &\longmapsto a \cdot x^0 \end{aligned}$$
ist ein injektiver Ringhomomorphismus.

2. *Für alle $c \in R'$ ist die Abbildung*
$$\begin{aligned} R[x] &\longrightarrow R' \\ f &\longmapsto f(c) \in R' \end{aligned}$$
ein Ringhomomorphismus, genannt Einsetzungshomomorphismus. Hierbei ist für $f = a_n x^n + \ldots + a_0$ die Einsetzung $f(c)$ definiert als $f(c) = a_n \cdot c^n + \ldots a_1 \cdot c + a_0 \in R'$.

Beweis. 1. Dies ergibt sich einfach aus der Definition der Ringstruktur auf $R[x]$.

2. Man sieht sofort, dass $f(c) + g(c) = (f + g)(c)$ für alle $f, g \in R[x]$ und $c \in R'$ gilt. Andererseits haben wir für $f = \sum_{i=0}^{n} a_i x^i$ und $g = \sum_{j=0}^{m} b_j x^j$, dass

$$f(c) \cdot g(c) = \left(\sum_{i=0}^{n} a_i c^i \right) \cdot \left(\sum_{j=0}^{m} b_j c^j \right) =$$

$$\sum_{i=0}^{n} \sum_{j=0}^{m} a_i c^i b_j c^j = \sum_{i=0}^{n} \sum_{j=0}^{m} a_i b_j c^{i+j} = (f \cdot g)(c)$$

Man beachte, das bei der dritten Gleicheit der obigen Rechnung wirklich die Kommutativität von R' verwendet wird. Das Element $1 \cdot x^0$, also das Einselement in $R[x]$ wird durch die Einsetzungsabbildung natürlich auf $1 \in R'$ abgebildet, so dass diese Abbildung also ein Ringhomomorphismus ist.

□

Das folgende einfache Lemma (dessen Beweis eine Übungsaufgabe ist) zeigt, wie man aus gegebenen Idealen neue konstruieren kann.

Lemma 3.12. *Sei R ein Ring, $\mathfrak{a}, \mathfrak{b} \subset R$ Ideale, und $a_1, \ldots, a_n \in R$ Elemente von R.*

1. *Die Menge*
$$\mathfrak{a} + \mathfrak{b} := \{a + b \,|\, a \in \mathfrak{a}, b \in \mathfrak{b}\}$$
ist ein Ideal in R.

2. *Die Menge $\mathfrak{a} \cap \mathfrak{b}$ ist ein Ideal in R.*

3. *Die Menge*
$$\mathfrak{a} \cdot \mathfrak{b} := \left\{ \sum_{i=1}^{k} x_i \cdot y_i \,|\, k \in \mathbb{N}, x_i \in \mathfrak{a}, y_i \in \mathfrak{b} \right\}$$
ist ein Ideal in R.

4. *Die Menge*
$$(a_1, \ldots, a_n) := R \cdot a_1 + \ldots R \cdot a_n := \left\{ \sum_{i=1}^{n} r_i \cdot a_i \,|\, r_i \in R \right\}$$
ist ein Ideal in R, genannt das von den Elementen $a_1, \ldots, a_n$ erzeugte Ideal. Es ist das kleinste Ideal von R (bezüglich der Inklusion), welches $a_1, \ldots, a_n$ enthält. Es gilt $(a_1, \ldots, a_n) = (a_1) + \ldots + (a_n)$.

5. *Analog ist für eine (evenutell unendliche) Familie $(a_i)_{i \in I}$ die Menge*
$$(\{a_i \,|\, i \in I\}) := \left\{ \sum_{i \in I} r_i a_i \,|\, r_i = 0 \text{ für fast alle } i \in I \right\}$$
ein Ideal in R. Hier und später steht „fast alle“ für „alle bis auf endlich viele“ Elemente.

Für ein gegebenes Ideal möchte man andererseits die möglichen Erzeugendensysteme studieren.

Definition 3.13. *Sei R ein Ring und $\mathfrak{a} \subset R$ ein Ideal. Dann heißt eine Familie $(a_i)_{i \in I}$ von Elementen von R ein Erzeugendensystem von $\mathfrak{a}$, falls $\mathfrak{a} = (\{a_i \,|\, i \in I\})$ gilt. Ist $|I| < \infty$, d.h., gilt $\mathfrak{a} = (a_1, \ldots, a_n)$ für Elemente $a_1, \ldots, a_n \in R$, dann heißt $\mathfrak{a}$ endlich erzeugt. Ist darüber hinaus $n = 1$, d.h., gilt $\mathfrak{a} = (a_1)$, dann heißt $\mathfrak{a}$ ein Hauptideal. Ein Ring R, in dem alle Ideale endlich erzeugt sind, heißt* noethersch. *Ein Ring, in dem alle Ideale Hauptideale sind, heißt* Hauptidealring.

Fast alle in dieser Vorlesung vorkommenden Ringe werden noethersch sein. Im nächsten Lemma diskutieren wir einige wichtige Hauptidealringe (und „Nicht-Hauptidealringe“).

Lemma 3.14. 1. *Der Ring $\mathbb{Z}$ ist ein Hauptidealring, mit den einzigen Idealen $(m) = m\mathbb{Z} \subset \mathbb{Z}$ für $m \in \mathbb{N}$.*

2. *Sei K ein Körper, dann ist der Polynomring $K[x]$ ein Hauptidealring.*

3. *Der Ring $\mathbb{Z}[x]$ ist kein Hauptidealring.*

Beweis. 1. Klar ist, dass $m\mathbb{Z}$ nicht nur eine Untergruppe in $\mathbb{Z}$, sondern auch ein Ideal ist, und zwar genau das von m erzeugte (Haupt-)ideal. Andererseits wissen wir aus Satz 2.15, dass $m\mathbb{Z} < \mathbb{Z}$ die einzigen Untergruppen von $\mathbb{Z}$ sind, aber jedes Ideal in einem Ring ist insbesondere eine Untergruppe bezüglich der Addition. Daher sind $m\mathbb{Z}$ die einzigen Ideale in $\mathbb{Z}$, und demnach ist $\mathbb{Z}$ ein Hauptidealring.

2. Den Beweis dieser Aussage verschieben wir auf Satz 3.27.

3. Betrachte das Ideal $(2, x) \subset \mathbb{Z}[x]$. Es gilt dann

$$(2, x) = \left\{ \sum_{i=0}^{n} a_i x_i \,|, n \in \mathbb{N}, a_i \in \mathbb{Z}, 2|a_0 \right\}.$$

Sowohl die Inklusion $\subset$ als auch die Inklusion $\supset$ folgen aus

$$(x) = \left\{ \sum_{i=1}^{n} a_i x_i \,|, n \in \mathbb{N}, a_i \in \mathbb{Z} \right\}.$$

Angenommen, $(2, x)$ wäre ein Hauptideal, d.h., wir hätten $(2, x) = (f)$ für ein $f \in \mathbb{Z}[x]$. Dann würde $2 \in (f)$ und $x \in (f)$ gelten, also $2 = f \cdot g$ und $x = f \cdot h$ mit $g, h \in \mathbb{Z}[x]$. Wegen $\deg(2) = 0$ folgt aus $2 = fg$, dass $f, g \in \mathbb{Z}$ ist. Die obige konkrete Beschreibung des Ideals $(2, x)$ zeigt $(2, x) \subsetneq \mathbb{Z}[x]$, also $f \notin \{1, -1\}$, daher muss $f \in \{2, -2\}$ gelten. Dies widerspricht aber der Gleichung $x = f \cdot h$ (denn der Leitkoeffizient von x ist 1 und daher nicht durch 2 teilbar).

□

Der Vollständigkeit halber sei noch erwähnt, dass Polynomringe in mehreren Variablen, auch über einem Körper, also z.B. $K[x, y]$ keine Hauptidealringe sind. Zum Beispiel kann man sich überlegen, dass das Ideal $(x, y) \subset K[x, y]$ nicht von einem Element erzeugt werden kann.
Ideale spielen in Ringen eine ähnlich Rolle wie Normalteiler in Gruppen. Insbesondere können wir die Konstruktion der Quotienten- oder Faktorgruppe auch für Ringe durchführen.

Definition-Lemma 3.15. *Sei R ein Ring und $I \subset R$ ein Ideal. Insbesondere ist $(I, +) \lhd (R, +)$ (weil $(R, +)$ abelsch ist), und wir können die Faktorgruppe $(R/I, +)$ betrachten. Dann definieren wir eine Multiplikation*

$$\begin{array}{rcl} R/I \times R/I & \longrightarrow & R/I \\ ([a] = a + I, [b] = b + I) & \longmapsto & (a \cdot b) + I = [a \cdot b] \end{array}$$

Dann ist $(R/I, +, \cdot)$ ein Ring, mit $0_{R/I} = 0 + I$ und $1_{R/I} = 1 + I$. Die kanonische Projektion $\pi : R \to R/I, a \mapsto [a]$ ist ein (surjektiver) Ringhomomorphismus.

Beweis. Zu zeigen ist lediglich, dass die Multiplikation auf R/I wohldefiniert ist, alle anderen Eigenschaften folgen automatisch. Sei also $a' \in [a]$ und $b' \in [b]$, d.h. es gibt $x, y \in I$ mit $x = a' - a, y = b' - b$, dann ist $a' \cdot b' = (a + x) \cdot (b + y) = ab + xb + ay + xy \in a \cdot b + I$, also ist $[a' \cdot b'] = [a \cdot b]$. Man beachte, dass dieses Argument wirklich benutzt, dass I ein zweiseitiges Ideal ist (was aufgrund unserer allgemeinen Annahme, dass R kommutativ ist, natürlich in jedem Fall erfüllt ist). □

Als nächstes zeigen wir eine Variante des Homomorphiesatzes für Ringe.

Satz 3.16. *Sei $f : R \to S$ ein Ringhomomorphismus, und $I \subset R$ ein Ideal, welches $I \subset \ker(f)$ erfüllt. Sei $\pi : R \to R/I$ die kanonische Projektionsabbildung. Dann existiert ein eindeutig bestimmter Ringhomomorphismus $\overline{f} : R/I \to S$, welcher $f = \overline{f} \circ \pi$ erfüllt, und so dass gilt*

$$\begin{array}{rcl} \mathrm{Im}(f) & = & \mathrm{Im}(\overline{f}) \\ \ker(\overline{f}) & = & \pi(\ker(f)) \\ \ker(f) & = & \pi^{-1}\left(\ker(\overline{f})\right) \end{array}$$

Insbesondere gilt: Ist f surjektiv, dann ist der Faktorring $R/\ker(f)$ kanonisch isomorph zum Ring S.

Beweis. Wir wissen schon aus dem Homomorphisatz für Gruppen (Satz 2.11), dass die gesuchte Abbildung $\overline{f}$ als Gruppenhomomorphismus $(R/I,+) \to (S,+)$ existiert und alle gewünschten Eigenschaften hat. Zu zeigen bleibt, dass $\overline{f}$ auch ein Ringhomomorphismus ist. Wir haben

$$\overline{f}([a]\cdot[b]) = \overline{f}\left(\pi(a)\cdot\pi(b)\right) = \overline{f}\left(\pi(a\cdot b)\right) = f(a\cdot b) = f(a)\cdot f(b) =$$

$$\overline{f}(\pi(a))\cdot\overline{f}(\pi(b)) = \overline{f}([a])\cdot\overline{f}([b])$$

□

Für viele Anwendungen ist es wichtig, zu verstehen, wie die Ideale eines gegebenen Ringes R mit denen eines Faktorringes R/J für ein fest gewähltes Ideal $J \subset R$ zusammenhängen. Dies liefert der folgende Satz.

Satz 3.17. *Sei R ein Ring, $J \subset R$ ein Ideal und $\pi : R \twoheadrightarrow R/J$ die kanonische Projektion. Dann existieren die folgenden beiden bijektiven Abbildungen, welche invers zueinander sind.*

$$\begin{array}{ccc} \{\text{Ideale } I \text{ in } R \text{ mit } J \subset I\} & \xrightarrow{\alpha} & \{\text{Ideale } I' \text{ in } R/J\} \\ I & \mapsto & \pi(I) \end{array}$$

$$\begin{array}{ccc} \{\text{Ideale } I \text{ in } R \text{ mit } J \subset I\} & \xleftarrow{\beta} & \{\text{Ideale } I' \text{ in } R/J\} \\ \pi^{-1}(I') & \mapsfrom & I' \end{array}$$

Beweis. Dieser Beweis ist eine Übung. □

Wir kommen nun zur Definition von zwei speziellen Typen von Idealen, welche im weiteren Verlauf sehr wichtig werden.

Definition 3.18. *Sei R ein Ring und $I \subsetneq R$ ein Ideal. Dann heißt I*

1. *ein* maximales *Ideal, falls für alle Ideale $K \subset R$ mit $I \subsetneq K$ gilt, dass $K = R$ ist,*
2. prim *oder ein* Primideal*, falls für alle $a, b \in R$ mit $a \cdot b \in I$ gilt, dass $a \in I$ oder $b \in I$ ist.*

Quotientenringe nach maximalen oder Primidealen haben besondere Eigenschaften.

Satz 3.19. *Sei R ein Ring und $I \subsetneq R$ ein Ideal.*

1. *I ist maximal genau dann, wenn die einzigen Ideale von R/I das Nullideal und der ganze Ring R/I sind.*
2. *I ist maximal genau dann, wenn R/I ein Körper ist.*
3. *I ist ein Primideal genau dann, wenn R/I ein Integritätsring ist.*
4. *Falls I maximal ist, dann ist I ein Primideal.*

Beweis. 1. I ist maximal genau dann, wenn für alle Ideale K mit $I \subset K \subset R$ gilt, dass entweder $K = I$ oder $K = R$ gilt. Nach Satz 3.17 entsprechen Ideale K mit $I \subset K \subset R$ aber genau den Idealen K' in R/I, und $K = I$ bzw. $K = R$ entspricht dem Fall $K' = (0)$ bzw. $K' = R/I$.

2. Sei S ein beliebiger Ring. Falls das Nullideal (0) maximal in S ist, dann folgt $(0) \subsetneq S$, und es gibt dann $a \in S\backslash\{0\}$, aber dann ist wegen $(0) \subsetneq (a)$ notwendig $(a) = S$, also $1 \in (a)$, d.h., es existiert $b \in R$ mit $a \cdot b = 1$, also ist a invertierbar. Dann ist also S notwendig ein Körper.

   Wir wenden diese Überlegung jetzt auf den Quotientenring R/I an, für den wir nach Punkt 1. wissen, dass das Nullideal maximal ist genau dann, wenn $I \subset R$ maximal ist. Dies gibt die gewünschte Äquivalenz.

3. Sei I ein Primideal, dann ist insbesondere $I \subsetneq R$, also $R/I \neq (0)$. Sei $[a], [b] \in R/I$ mit $[a] \cdot [b] = 0$, dann ist $a \cdot b \in I$, aber dann muss $a \in I$ oder $b \in I$ gelten, weil eben I ein Primideal ist. Daher hat man $[a] = 0$ oder $[b] = 0$.

   Die andere Richtung zeigt man genauso, mit den jeweils umgekehrten Implikationen.

4. Wenn I maximal ist, dann sagt Punkt 2., dass R/I ein Körper ist, dieser ist natürlich insbesondere ein Integritätsring, und dann folgt aus Punkt 3., dass I ein Primideal sein muss.

□

Eine einfach, aber nützliche Konsequenz aus dieser Argumentation ist die folgende Aussage.

Korollar 3.20. *Sei $\varphi : R \to S$ ein Ringhomomorphismus mit $\varphi(1) \neq 0$ und sei R ein Körper. Dann ist φ injektiv. Insbesondere sind also nicht-triviale Körperhomomorphismen immer injektiv.*

Beweis. φ ist injektiv genau dann, wenn $\ker(\varphi) = (0)$ ist. Der Kern von φ ist aber nach Lemma 3.9 ein Ideal in R, und wegen $\varphi(1) \neq 0$ gilt $ker(\varphi) \subsetneq R$. Da aber R ein Körper ist, hat R entsprechend der Argumentation im Beweis des letzten Satzes nur die Ideale R und (0), so dass $\ker(\varphi) = (0)$ folgt. □

Der Ring $\mathbb{Z}$ hat, wie wir im Lemma 3.14 gesehen haben, nur die Ideale $(m) = m\mathbb{Z}$. In diesem Fall ist es leicht, festzustellen, ob diese Ideale maximal bzw. prim sind.

Lemma 3.21. *Sei $m \in \mathbb{N}_{>0}$, dann sind äquivalent:*

1. *m ist eine Primzahl,*
2. *(m) ist ein Primideal, d.h. $\mathbb{Z}/m\mathbb{Z}$ ist ein Integritätsring,*
3. *(m) ist ein maximales Ideal, d.h., $\mathbb{Z}/m\mathbb{Z}$ ist ein Körper.*

Beweis.

1. ⇒ 2. m ist eine Primzahl, d.h. $m > 1$, also $m\mathbb{Z} \subsetneq \mathbb{Z}$. Falls $a \cdot b \in (m)$, dann ist $a \cdot b = m \cdot k$ für ein $k \in \mathbb{Z}$. Daher ist $m|a$ oder $m|b$ (Primfaktorzerlegung in $\mathbb{Z}$), und es folgt $a \in (m)$ oder $b \in (m)$.

2. ⇒ 3. Sei $\mathbb{Z}/m\mathbb{Z}$ ein Integritätsring, und betrachte für ein beliebiges Element $[a] \in \mathbb{Z}/m\mathbb{Z}$ mit $[a] \neq [0]$ den Gruppenhomomorphismus

$$\begin{array}{ccc} (\mathbb{Z}/m\mathbb{Z}, +) & \longrightarrow & (\mathbb{Z}/m\mathbb{Z}, +) \\ [b] & \longmapsto & [a] \cdot [b] \end{array}$$

Man beachte, dass dies *kein* Ringhomomorphismus ist. Da $\mathbb{Z}/m\mathbb{Z}$ keine Nullteiler enthält, ist der Kern dieser Abbildung gleich $\{[0]\}$, also ist sie injektiv, und daher, weil es eine Abbildung zwischen endlichen Mengen mit derselben Anzahl von Elementen ist, auch surjektiv. Also existiert ein $[b] \in \mathbb{Z}/m\mathbb{Z}$ mit $[a] \cdot [b] = [1]$, d.h., $\mathbb{Z}/m\mathbb{Z}$ ist ein Körper.

3. ⇒ 1. Angenommen, m wäre keine Primzahl, d.h., es gibt $a, b \in \mathbb{N}_{>1}$ mit $m = a \cdot b$. Wegen $a > 1$ ist dann notwendig $(a) \subsetneq \mathbb{Z}$, aber wegen $b > 1$ folgt $a < m$ und daher ist $(m) \subsetneq (a)$, also kann (m) kein maximales Ideal sein.

□

Für eine Primzahl p bezeichnet man den Körper $(\mathbb{Z}/p\mathbb{Z}, +, \cdot)$ mit $\mathbb{F}_p$. Dies sind die einfachsten Beispiele für endliche Körper. Wir werden später in Kapitel 4 alle endlichen Körper klassifizieren.
Zum Abschluss dieses Abschnitts betrachten wir noch eine „Ring-Version“ einer klassischen Aussage der elementaren Zahlentheorie, nämlich den Chinesischen Restsatz. Hierzu benötigen wir zunächst die ganz einfache Definition des Produktes von Ringen, die wir in ähnlicher Art und Weise schon für Gruppen diskutiert hatten (siehe Definition 2.27).

Definition-Lemma 3.22. *Seien $R_1, \ldots, R_k$ Ringe (wie immer kommutativ mit 1). Dann ist das kartesische Produkt $R_1 \times \ldots \times R_k$ ein kommutativer Ring mit 1, und es gilt $(R_1 \times \ldots \times R_k)^* = R_1^* \times \ldots \times R_k^*$.*

Beweis. Übung. □

Mit dieser Notation haben wir den folgenden Satz.

Satz 3.23 (Chinesischer Restsatz)**.** *Sei R ein Ring und seien $\mathfrak{a}_1, \ldots, \mathfrak{a}_n$ Ideale, so dass für alle $i, j \in \{1, \ldots, n\}$ mit $i \neq j$ gilt, dass $\mathfrak{a}_i + \mathfrak{a}_j = R$ ist. Wir schreiben $\pi_i : R \to R/\mathfrak{a}_i$ für die kanonische Restklassenprojektion. Dann ist der Ringhomomorphismus*

$$\begin{aligned} \psi : R &\longrightarrow \prod_{i=1}^{n} R/\mathfrak{a}_i \\ x &\longmapsto (\pi_1(x), \ldots, \pi_n(x)) \end{aligned}$$

surjektiv mit $\ker(\psi) = \mathfrak{a}_1 \cap \ldots \cap \mathfrak{a}_n$, d.h., ψ induziert mit Hilfe des Homomorphiesatzes für Ringe (Satz 3.16) einen Ringisomorphismus.

$$\frac{R}{\bigcap_{i=1}^{n} \mathfrak{a}_i} \longrightarrow \prod_{i=1}^{n} \frac{R}{\mathfrak{a}_i}$$

Beweis. Wir beweisen zunächst folgende Hilfsaussage: Sei $j \in \{1, \ldots, n\}$, dann gilt

$$\mathfrak{a}_j + \bigcap_{i \neq j} \mathfrak{a}_i = R \tag{3.1}$$

Zum Beweis dieser Gleichung fixieren wir $j \in \{1, \ldots, n\}$, dann gilt für alle $i \in \{1, \ldots, n\}\backslash\{j\}$, dass $\mathfrak{a}_j + \mathfrak{a}_i = R$ ist, also gibt es für alle solche $i \in \{1, \ldots, n\}\backslash\{j\}$ Elemente $a_i \in \mathfrak{a}_j$ (Achtung: die Indizierung ist bewusst so gewählt) und $a_i' \in \mathfrak{a}_i$ mit $1 = a_i + a_i'$. Dann gilt aber

$$1 = \prod_{i \in \{1,\ldots,n\}\backslash\{j\}} (a_i + a_i') = \sum_{i \in \{1,\ldots,n\}\backslash\{j\}} r_i \cdot a_i + \prod_{i \in \{1,\ldots,n\}\backslash\{j\}} a_i'$$

für gewisse $r_i \in R$, hierbei entsteht die zweite Gleichung durch Ausmultiplizieren des Ausdrucks $\prod_{i \in \{1,\ldots,n\}\backslash\{j\}} (a_i + a_i')$. Jetzt ist aber $\sum_{i \in \{1,\ldots,n\}\backslash\{j\}} r_i a_i \in \mathfrak{a}_j$ und

$$\prod_{i \in \{1,\ldots,n\}\backslash\{j\}} a_i' \in \prod_{i \in \{1,\ldots,n\}\backslash\{j\}} \mathfrak{a}_i \subset \bigcap_{i \in \{1,\ldots,n\}\backslash\{j\}} \mathfrak{a}_i,$$

und dies beweist die Behauptung.
Wegen Gleichung (3.1) finden wir also für alle $j \in \{1, \ldots, n\}$ Elemente $d_j \in \mathfrak{a}_j$ und $e_j \in \bigcap_{i \neq j} \mathfrak{a}_i$, so dass $d_j + e_j = 1$ ist. Es gilt dann $\pi_i(e_j) = 0$ für alle $i \in \{1, \ldots, n\}\backslash\{j\}$ und $\pi_j(e_j) = \pi_j(1 - d_j) = \pi_j(1)$.

Sei nun $(y_1, \ldots, y_n) \in \prod_{i=1}^{n} R/\mathfrak{a}_i$ vorgegeben. Wir wählen beliebige Urbilder $x_i \in R$ mit $\pi_i(x_i) = y_i$, und definieren

$$x := \sum_{i=1}^{n} x_i \cdot e_i.$$

Dann gilt

$$\psi(x) = \left(\pi_1 \left(\sum_{i=1}^{n} x_i \cdot e_i \right), \ldots, \pi_n \left(\sum_{i=1}^{n} x_i \cdot e_i \right) \right) = (\pi_1(x_1)\pi_1(e_1), \ldots, \pi_1(x_n)\pi_n(e_n)) = (y_1, \ldots, y_n),$$

d.h., ψ ist surjektiv. Andererseits gilt $\psi(x) = 0$ genau dann, wenn $\pi_1(x) = \ldots = \pi_n(x) = 0$ ist, d.h., wenn $x \in \mathfrak{a}_i$ für alle $i = \{1, \ldots, n\}$ gilt, und dies heißt nichts anderes als $x \in \bigcap_{i=1}^{n} \mathfrak{a}_i$. □

Für den Ring $R = \mathbb{Z}$ liefert der Chinesische Restsatz eine bekannte Aussage über die Lösbarkeit von Kongruenzgleichungssystemen.

Korollar 3.24. *Seien $a_1, \ldots, a_n \in \mathbb{Z}$ paarweise teilerfremde Zahlen. Dann existiert für alle $x_1, \ldots, x_n \in \mathbb{Z}$ eine Lösung $x \in \mathbb{Z}$ des Kongruenzensystems*

$$\begin{aligned} x &\equiv x_1 \mod (a_1) \\ &\vdots \\ x &\equiv x_n \mod (a_n) \end{aligned}$$

Sind $x, x' \in \mathbb{Z}$ zwei Lösungen dieses Systems, so folgt $x \equiv x' \mod (a_1 \cdot \ldots \cdot a_n)$.

Beweis. Wir betrachten die Ideale $\mathfrak{a}_i := (a_i) \subset \mathbb{Z}$. Um den eben bewiesenen Chinesischen Restsatz benutzen zu können, müssen wir die Bedingung $\mathfrak{a}_i + \mathfrak{a}_j = \mathbb{Z}$ nachweisen. Da $\mathbb{Z}$ ein Hauptidealring ist, gilt $\mathfrak{a}_i + \mathfrak{a}_j = (m)$ für ein $m \in \mathbb{N}$. Es ist $(a_i) \subset (a_i) + (a_j) = (m)$ und $(a_j) \subset (a_i) + (a_j) = (m)$, also teilt m sowohl a_i als auch a_j. Letztere sind teilerfremd, also ist $m = 1$, und wir haben $\mathfrak{a}_i + \mathfrak{a}_j = \mathbb{Z}$. Wir können also Satz 3.23 anwenden, die Surjektivitität der Abbildung ψ liefert die Existenz des Elementes x, und die zweite Aussage folgt aus $\ker(\psi) = \bigcap_{i=1}^{n} \mathfrak{a}_i$, wenn man berücksichtigt, dass für $i \neq j$ gilt, dass $(a_i \cdot a_j) = (a_i) \cap (a_j)$ gilt (Die Inklusion $\subset$ ist klar, sei $m \in (a_i) \cap (a_j)$, d.h., $a_i | m$ und $a_j | m$, aber wegen $\mathrm{ggT}(a_i, a_j) = 1$ folgt $a_i \cdot a_j | m$ und daher $m \in (a_i \cdot a_j)$).

□

Wir notieren noch die folgende schöne Konsequenz des Chinesischen Restsatzes.

Korollar 3.25. *Sei $m \in \mathbb{N}_{>0}$ und betrachte die Quotientenringe $\mathbb{Z}/m\mathbb{Z}$. Dann gilt:*

$$(\mathbb{Z}/m\mathbb{Z})^* = \{a \in \{0, \ldots, m-1\} \mid \mathrm{ggT}(a, m) = 1\}$$

Wir definieren die Eulersche φ-Funktion $\varphi : \mathbb{N}_{>0} \to \mathbb{N}_{>0}$ durch

$$\varphi(m) := |(\mathbb{Z}/m\mathbb{Z})^*| = |\{a \in \{0, \ldots, m-1\} \mid \mathrm{ggT}(a, m) = 1\}|.$$

Dann gilt:

1. *Für eine Primzahl p ist $\varphi(p^k) = (p-1)p^{k-1}$.*
2. *Sei $n_1, n_2 \in \mathbb{N}_{>0}$ mit $\mathrm{ggT}(n_1, n_2) = 1$. Dann ist $\varphi(n_1 \cdot n_2) = \varphi(n_1) \cdot \varphi(n_2)$.*

3. *Sei $m \in \mathbb{Z}$ und $m = p_1^{k_1} \cdot \ldots \cdot p_l^{k_l}$ die Zerlegung von m in Potenzen von Primzahlen $p_1, \ldots, p_l$. Dann ist*

$$\begin{aligned} \varphi(m) &= \varphi(p_1^{k_1} \cdot \ldots \cdot p_l^{k_l}) = \varphi(p_1^{k_1}) \cdot \ldots \cdot \varphi(p_l^{k_l}) = (p_1 - 1) \cdot p_1^{k_1 - 1} \cdot \ldots \cdot (p_l - 1) \cdot p_l^{k_l - 1} \\ &= m \cdot \prod_{i=1}^{l} \left(1 - \frac{1}{p_i}\right) = m \cdot \prod_{p \mid m} \left(1 - \frac{1}{p}\right). \end{aligned}$$

Beweis. Die erste Aussage kann man als Übung leicht selbst verifizieren. Zum Beweis der Aussagen über die Eulersche φ-Funktion:

1. Von den Zahlen $0, 1, \ldots, p^k - 1$ sind genau die p^{k-1} Zahlen $p \cdot 0, p \cdot 1, \ldots p \cdot (p^{k-1} - 1)$ durch p teilbar. Die anderen sind nicht durch p teilbar und daher teilerfremd zu p^k. Ihre Anzahl ist $p^k - p^{k-1} = (p-1)p^{k-1}$.

2. Aus Satz 3.23 folgt, dass
$$\frac{\mathbb{Z}}{(n_1 \cdot n_2)\mathbb{Z}} \cong \frac{\mathbb{Z}}{n_1\mathbb{Z}} \times \frac{\mathbb{Z}}{n_2\mathbb{Z}}$$
(als Ringe) gilt. Lemma 3.22 liefert
$$\left(\frac{\mathbb{Z}}{(n_1 \cdot n_2)\mathbb{Z}}\right)^* \cong \left(\frac{\mathbb{Z}}{n_1\mathbb{Z}}\right)^* \times \left(\frac{\mathbb{Z}}{n_2\mathbb{Z}}\right)^*$$
als Gruppen, und hieraus folgt, dass
$$\varphi(n_1 \cdot n_2) = \left|\left(\frac{\mathbb{Z}}{(n_1 \cdot n_2)\mathbb{Z}}\right)^*\right| = \left|\left(\frac{\mathbb{Z}}{n_1\mathbb{Z}}\right)^*\right| \times \left|\left(\frac{\mathbb{Z}}{n_2\mathbb{Z}}\right)^*\right| = \varphi(n_1) \cdot \varphi(n_2)$$
ist.

3. Folgt aus 1. und 2.

□

3.2 Euklidische Ringe und faktorielle Ringe

Wir wollen jetzt das bekannte Konzept der Polynomdivision verallgemeinern und eine Klasse von Ringen betrachten, in welchen in einem abstrakten Sinn eine solche Division mit Rest möglich ist.

Definition 3.26. *Sei R ein Integritätsring und sei $\omega : R\backslash\{0\} \to \mathbb{N}$ eine Abbildung. Dann heißt R ein* euklidischer Ring*, falls für alle $f, g \in R$ mit $g \neq 0$ Elemente $q, r \in R$ existieren, so dass gilt*

$$f = q \cdot g + r$$

und so dass $\omega(r) < \omega(g)$ gilt, falls $r \neq 0$ ist.
Dann heißt ω die Gradfunktion *von R.*

Wir diskutieren einige typische Beispiele für euklidische Ringe.

1. Ein Körper K ist zusammen mit der trivialen Abbildung $\omega = 0$ ein euklidischer Ring.

2. Für einen Körper K ist der Polynomring $K[x]$ ein euklidischer Ring, wobei $\omega = \deg$ ist. Dies folgt aus der bekannten Division mit Rest für Polynome, welche exakt die in der obigen Definition geforderten Eigenschaften hat.

3. Der Ring $\mathbb{Z}$ ist ein euklidischer Ringe, mit $\omega(m) := |m|$.

4. Gaußsche Zahlen: Betrachte
$$\mathbb{Z}[i] := \{a + ib \,|\, a, b \in \mathbb{Z}\} \subset \mathbb{C},$$
dann prüft man leicht, dass $\mathbb{Z}[i]$ ein Unterring von $\mathbb{C}$ ist. Definiere weiterhin:
$$\begin{aligned} \omega : \mathbb{Z}[i]\backslash\{0\} &\longrightarrow \mathbb{N} \\ a + ib &\longmapsto |a + ib|^2 = a^2 + b^2. \end{aligned}$$
Um zu zeigen, dass $\mathbb{Z}[i]$ bezüglich ω ein euklidischer Ring ist, wählen wir $f, g \in \mathbb{Z}[i]$ mit $g \neq 0$. Dann können wir natürlich den Quotienten $\frac{f}{g}$ als Element von $\mathbb{C}$ betrachten. Angenommen, es gäbe ein $q \in \mathbb{Z}[i]$ mit
$$\left| \frac{f}{g} - q \right| < 1. \tag{3.2}$$
Dann folgt $|f - g \cdot q| < |g|$, also $|f - g \cdot q|^2 < |g|^2$, und damit ist $f = g \cdot q + r$, mit $r := f - g \cdot q$, und es gilt entweder $r = 0$ oder $\omega(r) = |r|^2 < |g|^2 = \omega(g)$. Wir müssen also Gleichung (3.2) beweisen. Klar ist: Für alle Zahlen $x, y \in \mathbb{R}$ existieren Zahlen $a, b \in \mathbb{Z}$ mit $|x - a| \leq \frac{1}{2}$, $|y - b| \leq \frac{1}{2}$. Dann folgt aber für $z := x + iy$, dass
$$|z - (a + ib)|^2 = |(x - a) + i(y - b)|^2 \leq 2 \cdot \frac{1}{4} < 1,$$
gilt. Dies kann man auf $z := f/g$ anwenden, und erhält die Existenz von $q := a + ib \in \mathbb{Z}[i]$ mit den gewünschten Eigenschaften.

Der nächste Satz liefert eine fundamentale Konsequenz der Eigenschaft, ein euklidischer Ring zu sein.

Satz 3.27. *Sei R ein euklidischer Ring, dann ist R auch ein Hauptidealring.*

Beweis. Sei $\{0\} \subsetneq I \subset R$ ein Ideal. Wir wählen ein $b \in I\backslash\{0\}$ so, dass $\omega(b)$ minimal wird. Da ω eine Funktion mit Werten in $\mathbb{N}$ ist, existiert natürlich so ein b, auch wenn es im Allgemeinen nicht eindeutig bestimmt ist. Dann gilt wegen $b \in I$ natürlich $(b) \subset I$. Sei andererseits $a \in I$ beliebig vorgegeben, dann wissen wir (weil R euklidisch ist), dass es $q, r \in R$ gibt mit $a = q \cdot b + r$ und so dass entweder $r = 0$ oder $\omega(r) < \omega(b)$ ist. Der letzte Fall kann aber nicht eintreten: Wegen $r = a - q \cdot b$ ist $r \in I$, und $\omega(r) < \omega(b)$ würde dann der Minimalität von $\omega(b)$ widersprechen. Also ist $r = 0$, d.h., $a = q \cdot b$, und daher $a \in (b)$. Wir erhalten also $I = (b)$, damit ist I ein Hauptideal, und also R ein Hauptidealring. □

Wir erhalten als Konsequenz, dass die folgenden Ringe Hauptidealringe sind: $\mathbb{Z}$ (das wussten wir schon, siehe Lemma 3.14), $K[x]$ (dies war auch in Lemma 3.14 angekündigt worden), $\mathbb{Z}[i]$. Desweiteren sehen wir aus diesem Satz, dass der Ring $\mathbb{Z}[x]$ kein euklidischer Ring sein kann.

Definition 3.28. *Sei R ein Ring mit $1 \neq 0$. Dann heißen zwei Elemente $a, b \in R$ assoziiert, falls es ein $c \in R^*$ gibt mit $a = b \cdot c$ (Leicht: Assoziiertheit ist ein eine Äquivalenzrelation). Man schreibt auch $a \sim b$. Desweiteren sagt man, dass ein Element $a \in R$ ein Element $p \in R$ teilt, geschrieben $a|p$, falls es $b \in R$ gibt mit $p = a \cdot b$.*
Falls R ein Integritätsring R und $p \in R\backslash(R^* \cup \{0\})$ ist, dann heißt p

1. irreduzibel*, falls für alle $a, b \in R$ mit $p = a \cdot b$ gilt, dass $a \in R^*$ (also $p \sim b$) oder $b \in R^*$ (also $p \sim a$) ist,*

2. prim *oder* Primelement*, falls für alle $a, b \in R$ aus $p|a \cdot b$ schon $p|a$ oder $p|b$ folgt (äquivalent dazu: (p) ist ein Primideal).*

Wir zeigen zunächst einige elementare Eigenschaften dieser Begriffe.

Lemma 3.29. *1. In $\mathbb{Z}$ sind irreduzible und Primelemente gleich, nämlich genau die Zahlen p und $-p$, falls p Primzahl ist.*

2. *Wenn ein Hauptideal (m) maximal ist, dann ist m prim.*

3. *Ein Primelement p ist irreduzibel.*

Beweis. 1. Klar.

2. Ein maximales Ideal ist nach Lemma 3.19 ein Primideal, falls es ein Hauptideal ist, wird es von einem Primelement erzeugt.

3. Sei $p \in R$ prim, und sei $p = a \cdot b$, dann gilt insbesondere $p|a \cdot b$, also folgt (weil p Primelement ist), dass $p|a$ oder $p|b$ gilt. Sei $a = p \cdot x$, dann ist $p = (p \cdot x) \cdot b$. Weil R ein Integritätsring ist, impliziert die Kürzungsregel (Definition 3.5), dass $x \cdot b = 1$ gilt, also ist $b \in R^*$. Analog folgt aus $p|b$, dass $a \in R^*$ ist, also ist p irreduzibel.

□

In Hauptidealringen gilt sogar die Umkehrung der Aussage 2. des letzten Lemmas.

Lemma 3.30. *Sei R ein Hauptidealring und $p \in R$, dann sind die folgenden Bedingungen äquivalent:*

1. *(p) ist ein maximales Ideal in R,*

2. *p ist prim,*

3. *p ist irreduzibel.*

Beweis. Die Implikationen 1. $\Rightarrow$ 2. $\Rightarrow$ 3. sind nach Satz 3.19 klar, es bleibt 3. $\Rightarrow$ 1. zu zeigen. Dies machen wir indirekt, angenommen, p ist irreduzibel und (p) nicht maximal, dann existiert, weil R Hauptidealring ist, $q \in R$ mit $(p) \subsetneq (q) \subsetneq R$. Es gibt dann $x \in R$ mit $p = xq$. Da p aber irreduzibel sein soll, ist $x \in R^*$ oder $q \in R^*$. Ersteres widerspricht $(p) \subsetneq (q)$, und letzteres ist wegen $(q) \subsetneq R$ unmöglich. □

Bemerkung: Insbesondere folgt aus Satz 3.27, dass ein Ideal (f) in $K[x]$ genau dann ein maximales Ideal ist, wenn f ein irreduzibles Polynom ist. Dann ist aber der Quotientenring $L := K[x]/(f)$ ein Körper (Satz 3.19). Betrachte die Komposition φ der kanonischen Inklusion $K \hookrightarrow K[x]$ mit der kanonischen Projektion $K[x] \twoheadrightarrow K[x]/(f)$, da f irreduzibel also insbesondere keine Einheit ist, folgt $1 \notin (f)$, und wir haben $\varphi(1) \neq 0$. Dann ist φ also ein nicht-trivialer Körperhomomorphismus $K \to L$, und dieser ist nach Korollar 3.20 automatisch injektiv, d.h., wir können K als Unterkörper von L auffassen. Insbesondere können wir den Einsetzungshomomorphismus (siehe Lemma 3.11) für das Polynom f und das Element $[x] \in L$ betrachten, und erhalten, dass dieses Element eine Nullstelle von f ist. Dieses Verfahren und allgemeiner die Möglichkeit, Körpererweiterungen als Quotienten von Polynomringen zu konstruieren werden wir im Kapitel 4 noch ausführlich studieren. Als einfaches Beispiel sei hier nur erwähnt, dass der Homomorphismus

$$\begin{array}{ccc} \mathbb{R}[x]/(x^2+1) & \longrightarrow & \mathbb{C} \\ x & \longmapsto & i \end{array}$$

ein Körperisomorphismus ist.
Eine der wichtigsten Aussagen der elementaren Zahlentheorie ist, dass sich jede natürlich Zahl im Wesentlichen (d.h., bis auf Reihenfolge) eindeutig als ein Produkt von Primzahlpotenzen schreiben läßt. Dies wollen wir jetzt im allgemeineren Kontext von Integritätsringen studieren.

Definition 3.31. *Ein Integritätsring R heißt faktorieller Ring (oder ZPE-Ring), falls für jedes $a \in R\backslash\{0\}$ irreduzible Elemente $p_1, \ldots, p_r$ sowie eine Einheit $c \in R^*$ existieren, so dass $a = c \cdot p_1 \cdot \ldots \cdot p_r$ gilt, und falls diese Zerlegung in folgendem Sinne eindeutig ist: Seien $a = c \cdot p_1 \cdot \ldots \cdot p_r$ und $a = c' \cdot q_1 \cdot \ldots \cdot q_s$ zwei derartige Zerlegungen, dann ist $r = s$ und es existiert eine Permutation $\tau \in S_r$ mit $p_i \sim q_{\tau(i)}$ für alle $i \in \{1, \ldots, r\}$. Mit anderen Worten: Bis auf Umordnung und Multiplikation mit Einheiten sind Zerlegungen in irreduzible Elemente eindeutig.*

Die oben erwähnte Aussage aus der elementaren Zahlentheorie sagt also, dass der Ring $\mathbb{Z}$ faktoriell ist.
Im Allgemeinen ist die Eindeutigkeit der Zerlegung in irreduzible Elemente natürlich schwer zu prüfen. Daher ist die folgende Umformulierung nützlich.

Satz 3.32. *Sei R ein Integritätsring.*

1. *Falls R faktoriell ist, dann ist jedes irreduzible Element auch prim (also sind wegen Lemma 3.29 in faktoriellen Ringen die beiden Begriffe äquivalent).*
2. *R ist faktoriell genau dann, wenn für jedes $a \in R\backslash(R^* \cup \{0\})$ Primelemente $p_1, \dots p_r$ und $c \in R^*$ existieren, so dass $a = c \cdot p_1 \cdot \ldots \cdot p_r$ gilt. Achtung: Hier wird keine Eindeutigkeit gefordert !*

Beweis. 1. Sei $a \in R$ irreduzibel, und $x, y \in R$, so dass $a|xy$ gilt. Wir wollen jetzt $a|x$ oder $a|y$ zeigen. Falls x oder y Einheiten oder gleich Null sind, dann ist die Aussage klar, also nehmen wir $x, y \in R\backslash(R^* \cup \{0\})$ an. Da R faktoriell ist, existieren Zerlegungen $x = c \cdot x_1 \cdot \ldots \cdot x_r$ und $y = c' \cdot y_1 \cdot \ldots \cdot y_s$, wobei x_i und y_j irreduzibel und c und c' Einheiten sind. Wegen $a|xy$ existiert also $z \in R$ mit $az = xy$, und wir können auch z zerlegen als $z = c'' \cdot z_1 \cdot \ldots \cdot z_t$ mit $c'' \in R^*$ und z_k irreduzibel, so dass wir die Gleichheit

$$c'' \cdot a \cdot z_1 \cdot \ldots \cdot z_t = (c \cdot c') \cdot x_1 \cdot \ldots \cdot x_r \cdot y_1 \cdot \ldots \cdot y_s$$

bekommen, wegen der Eindeutigkeit der Zerlegung in irreduzible Elemente ist dann also a assoziiert zu einem x_i oder einem y_j, und daher haben wir $a|x$ oder $a|y$.

2. Falls R faktoriell ist, wissen wir aus der Definition, dass sich jedes Element, welches nicht Null und keine Einheit ist, in ein Produkt von irreduziblen Elementen (und Einheiten) zerlegen lässt, aber diese irreduziblen Elemente sind nach Punkt 1. auch prim. Daher ist die eine Richtung der Äquivalenz bewiesen.

   Für die andere Richtung nehmen wir an, dass sich jedes $a \in R\backslash(R^* \cup \{0\})$ als $a = c \cdot a_1 \cdot \ldots \cdot a_r$ mit $c \in R^*$ und a_i prim schreiben läßt. Da alle a_i auch irreduzibel sind, liefert dies insbesondere eine Zerlegung in irreduzible Elemente. Der Hauptpunkt ist nun, zu zeigen, dass man dann auch die Eindeutigkeit der Zerlegung in irreduzible Elemente automatisch erhält. Nehmen wir also an, es gäbe noch eine Zerlegung $a = c' \cdot b_1 \cdot \ldots \cdot b_s$ mit $c' \in R^*$ und b_j irreduzibel, also

$$c \cdot a_1 \cdot \ldots \cdot a_r = c' \cdot b_1 \cdot \ldots \cdot b_s,$$

   dann folgt $a_i|c' \cdot b_1 \cdot \ldots \cdot b_s$ für alle $i \in \{1, \dots, r\}$. Also gilt $a_1|c'$ oder $a_1|b_j$ für ein $j \in \{1, \dots, s\}$. Ersteres ist ausgeschlossen, da $a_1 \notin R^*$. Also existiert $d \in R$ mit $a_1 \cdot d = b_j$. Aus der Tatsache, dass b_j irreduzibel und $a_1 \notin R^*$ ist, folgt $d \in R^*$, also ist $a_1 \sim b_j$. R ist ein Integritätsring, also sagt die Kürzungsregel, dass

$$a_2 \cdot \ldots \cdot a_r = c'' \cdot \prod_{k \in \{1,\dots,s\}\backslash\{j\}} b_k$$

   für ein $c'' \in R^*$, und dann folgt induktiv, dass alle Elemente a_i zu Elementen b_k assoziiert sind, insbesondere, dass $s = r$ gilt.

□

Wir folgern als nächstes, dass Hauptidealringe (insbesondere euklidische Ringe) faktoriell sind.

Satz 3.33. *1. Ein Ring ist noethersch genau dann, wenn jede aufsteigende Kette von Idealen*

$$\mathfrak{a}_1 \subset \mathfrak{a}_2 \subset \ldots \subset R$$

stationär wird, d.h., wenn es ein $n \in \mathbb{N}$ gibt mit $\mathfrak{a}_k = \mathfrak{a}_n$ für alle $k \geq n$. Insbesondere gilt diese Eigenschaft also für Hauptidealringe.

2. *Ein Hauptidealring ist faktoriell.*

Beweis. 1. Nach Definition ist ein Ring R noethersch, wenn jedes Ideal I endlich erzeugt ist, wenn es also $a_1, \ldots, a_l \in R$ mit $I = (a_1, \ldots a_l)$ gibt. Sei jetzt R noethersch und eine aufsteigende Kette $\mathfrak{a}_1 \subset \mathfrak{a}_2 \subset \ldots R$ gegeben, dann ist die Vereinigung $I = \bigcup_{i \geq 1} \mathfrak{a}_i$ ein Ideal, also endlich erzeugt, d.h. $I = (a_1, \ldots, a_l)$. Für alle $i \in \{1, \ldots, l\}$ existiert dann ein $j \in \mathbb{N}_{>0}$ mit $a_i \in \mathfrak{a}_j$ und daher gibt es $n \in \mathbb{N}_{>0}$ mit $a_1, \ldots, a_l \in \mathfrak{a}_n$, aber dann gilt schon $I = a_n$, und dann ist $\mathfrak{a}_k = I = \mathfrak{a}_n$ für alle $k \geq n$.

Gelte andererseits, dass jede Kette $\mathfrak{a}_1 \subset \mathfrak{a}_2 \subset \ldots R$ stationär wird, und sei ein Ideal $I \subset R$ gegeben. Angenommen, I wäre nicht endlich erzeugt, dann existieren Elemente $a_1, a_2, \ldots$ mit $a_{i+1} \notin (a_1, \ldots, a_i)$, und dann liefert $(a_1) \subsetneq (a_1, a_2) \subsetneq \ldots$ eine aufsteigende Kette von Idealen, welche nicht stationär wird.

Ein Hauptidealring hat nach Definition nur Ideale, welche von einem, insbesondere also von endlich vielen Elementen erzeugt werden, d.h., er ist noethersch. Daher gilt in Hauptidealringen, dass aufsteigende Idealketten stationär werden.

2. Nach dem letzten Satz reicht es, zu zeigen, dass jedes Element, welches nicht Null und keine Einheit ist, sich in irreduzible Faktoren zerlegen läßt (denn diese sind nach Lemma 3.30 automatisch prim). Sei S die Menge aller (Haupt-)Ideale, welche von Elementen erzeugt werden, die sich nicht in irreduzible Faktoren zerlegen lassen. Wir wollen $S = \emptyset$ zeigen. Angenommen, $S \neq \emptyset$, dann enthält die Menge S ein bezüglich der Inklusion maximales Element $\mathfrak{a}$: wäre dies nicht so, würde man eine aufsteigende Idealkette $\mathfrak{a}_1 \subsetneq \mathfrak{a}_2 \subsetneq \ldots$ mit $\mathfrak{a}_i \in S$ konstruieren können, diese müsste aber wegen 1. stationär werden, aber dann gäbe es ein maximales Element.

Sei also $\mathfrak{a} = (a)$ ein maximales Element in S, dann ist $a \notin R^*$ und nicht irreduzibel nach Konstruktion, man kann also $a = b \cdot c$ mit $b, c \in R \backslash R^*$ schreiben. Dann folgt $(a) \subsetneq (b)$ und $(a) \subsetneq (c)$. Es muss dann (wegen der Maximalität von (a)) gelten, dass $(b) \notin S$ und $(c) \notin S$ ist. Dies bedeutet aber, dass sowohl b als auch c eine Zerlegung in irreduzible Elemente haben, dann hat aber auch a solch eine Zerlegung, und dies ist ein Widerspruch zu $(a) \in S$.

□

Zum Abschluss dieses Abschnittes wollen wir uns noch der Verallgemeinerung des für die ganzen Zahlen wohlbekannten *Euklidischen Algorithmus* widmen. Hierzu wählen wir für einen gegebenen faktoriellen Ring R zunächst ein Vertretersystem $P \subset R$ der Äquivalenzklassen aller *irreduziblen- bzw. Primelemente* bezüglich der Äquivalenzrelation ($a \sim b \Leftrightarrow a$ assoziiert zu b), dann läßt sich jedes $a \in R \backslash \{0\}$ *eindeutig* zerlegen als

$$a = c \cdot \prod_{p \in P} p^{\nu_p(a)}, \tag{3.3}$$

mit $c \in R^*$, $\nu_p(a) \in \mathbb{N}$ und so dass fast alle $\nu_p(a)$ gleich Null sind. Beispielsweise wählt man für $R = \mathbb{Z}$ häufig $P = \{\text{Primzahlen}\}$ (d.h., $a \in P \Longrightarrow a > 0$), und für $R = K[x]$ wählt man $P = \{\text{irreduzible unitäre Polynome}\}$. Wir definieren nun für allgemeine Integritätsringe zwei für den Fall $R = \mathbb{Z}$ schon bekannte Begriffe.

Definition 3.34. *Sei R ein Integritätsring und $a_1, \ldots, a_n$ Elemente von R.*

1. *Ein Element $d \in R$ heißt* größter gemeinsamer Teiler *(ggT) von $a_1, \ldots, a_n$ falls $d|a_i$ für $i \in \{1, \ldots, n\}$ gilt und falls für alle $x \in R$ aus $x|a_i$ für $i \in \{1, \ldots, n\}$ folgt, dass $x|d$ ist.*

2. *Ein Element $v \in R$ heißt* kleinstes gemeinsames Vielfaches *(kgV) von $a_1, \ldots, a_n$ falls $a_i|v$ für $i \in \{1, \ldots, n\}$ gilt und falls für alle $y \in R$ aus $a_i|y$ für $i \in \{1, \ldots, n\}$ folgt, dass $v|y$ gilt.*

Die Berechnung des größten gemeinsamen Teilers bzw. des kleinsten gemeinsamen Vielfachen funktioniert in faktoriellen Ringen analog zur Berechung in $\mathbb{Z}$, wenn man die Zerlegung in Primelemente kennt, genauer gilt der folgende Satz, dessen Beweis völlig gleich zum Fall $R = \mathbb{Z}$ verläuft.

Satz 3.35. *Sei R faktoriell und $P \subset R$ wie oben ein Vertretersystem der Primelemente, und seien Elemente $a_1, \ldots, a_n$ vorgegeben. Dann existieren der größte gemeinsame Teiler und das kleinste gemeinsame Vielfache*

von $a_1, \ldots, a_n$, diese sind bis auf Einheiten eindeutig bestimmt, und es gilt

$$\begin{aligned} \mathrm{ggT}(a_1, \ldots, a_n) &= \prod_{p \in P} p^{\min(\nu_p(a_1), \ldots, \nu_p(a_n))} \\ \mathrm{kgV}(a_1, \ldots, a_n) &= \prod_{p \in P} p^{\max(\nu_p(a_1), \ldots, \nu_p(a_n))} \end{aligned}$$

Wir können den größten gemeinsamen Teiler und das kleinste gemeinsame Vielfache auch idealtheoretisch charakterisieren, wie das folgende Lemma zeigt.

Lemma 3.36. *Sei R ein Integritätsring, und $a_1, \ldots, a_n \in R$. Dann gilt*

1. *Wenn $(a_1, \ldots, a_n) = (d)$ gilt, dann ist $d = \mathrm{ggT}(a_1, \ldots, a_n)$.*
2. *Wenn $(a_1) \cap \ldots \cap (a_n) = (v)$ gilt, dann ist $v = \mathrm{kgV}(a_1, \ldots, a_n)$.*

Beweis. 1. Wegen $a_i \in (d)$ gilt $d | a_i$. Falls $x \in R$ existiert mit $x | a_i$ für alle $i \in \{1, \ldots, n\}$, dann folgt $x | \lambda_1 a_1 + \ldots + \lambda_n a_n$ für alle $\lambda_1, \ldots, \lambda_n \in R$. Aber wegen $d \in (a_1, \ldots, a_n)$ existieren $\lambda_1, \ldots, \lambda_n \in R$ mit $d = \lambda_1 a_1 + \ldots + \lambda_n a_n$, also haben wir $x | d$.

2. Wegen $v \in (a_i)$ für alle $i \in \{1, \ldots, n\}$ gilt offensichtlich $a_i | v$. Falls es ein anderes Element $y \in R$ mit $a_i | y$ für alle $i \in \{1, \ldots, n\}$ gibt, dann ist $y \in (a_i)$ und daher $y \in (a_1) \cap \ldots \cap (a_n) = (v)$, dies impliziert $v | y$.

□

Wir kommen jetzt zum oben erwähnten Euklidischen Algorithmus, mit dem man in euklidischen Ringen den größten gemeinsamen Teiler auch praktisch bestimmen kann.

Satz 3.37. *Sei R ein euklidischer Ring, und $a, b \in R \backslash \{0\}$. Definiere eine Folge von Elementen $(d_i)_{i \in \mathbb{N}}$ in R durch*

$$\begin{aligned} d_0 &:= a \\ d_1 &:= b \\ d_{i+1} &:= \begin{cases} \text{Rest der Division von } d_{i-1} \text{ durch } d_i & \text{falls } d_i \neq 0 \\ 0 & \text{sonst} \end{cases} \end{aligned}$$

Dann gilt

$$\mathrm{ggT}(a, b) = d_{\min(k \mid d_{k+1} = 0)}.$$

Beweis. Sei wie oben ω die Gradfunktion des euklidischen Ringes R. Dann gilt nach der Definition der Division mit Rest in R, dass für alle $i \in \mathbb{N}$ entweder $d_{i+1} = 0$ oder $\omega(d_{i+1}) < \omega(d_i)$ ist, d.h., die Folge $(\omega(d_i))$ ist bis zum Erreichen des Wertes 0 streng monoton fallend, und daher muss das Minimum $n := \min(k \mid d_{k+1} = 0)$ existieren. Wegen $a \neq 0$, $b \neq 0$ ist $n > 0$.
Es gilt $d_n | d_i$ für alle $i \in \{0, 1, \ldots, n\}$, dies sieht man per absteigender Induktion: Nach Konstruktion gibt es $q_n \in R$ mit $d_n \cdot q_n = d_{n-1}$, also haben wir $d_n | d_{n-1}$. Für alle $i \in \{1, \ldots, n-1\}$ ist $d_{i+1} + q_i \cdot d_i = d_{i-1}$ also folgt aus $d_n | d_{i+1}$ und $d_n | d_i$, dass auch $d_n | d_{i-1}$ gilt. Insbesondere erhalten wir also $d_n | a$ und $d_n | b$. Andererseits folgt für jedes $x \in R$, welches $x | a$ und $x | b$ erfüllt, dass es auch $x | d_i$ für alle $i \in \{0, 1, \ldots, n\}$ erfüllen muss (diesmal per aufsteigender Induktion wieder unter Verwendung der Gleichung $d_{i+1} + q_i \cdot d_i = d_{i-1}$), und daher gilt $x | d_n$, und wir erhalten $d_n = \mathrm{ggT}(a, b)$. □

3.3 Lokalisierungen, Quotientenkörper und der Satz von Gauß

Das Hauptziel dieses Abschnitts ist der Satz von Gauß (Satz 3.43), welcher zeigt, dass Polynomringe faktoriell sind. Zur Vorbereitung benötigen wir eine auch sonst sehr nützliche Konstruktionen, nämlich die Lokalisierung von Ringen und als Anwendung die Konstruktion von Quotientenkörpern.

Lemma 3.38. *Sei R ein Ring, und $S \subset R\backslash\{0\}$ ein multiplikativ abgeschlossenes System, d.h. es ist $1 \in S$ und für alle $b, d \in S$ gilt $b \cdot d \in S$. Dann sei eine Relation $\sim$ auf $R \times S$ definiert durch*

$$(a, b) \sim (c, d) \quad \Longleftrightarrow \quad \exists \lambda \in S : \lambda\,(ad - bc) = 0$$

für alle $a, c \in R$ und $b, d \in S$. Dann ist $\sim$ eine Äquivalenzrelation.

Beweis. Reflexivität und Symmetrie sind offensichtlich. Zu zeigen ist die Transitivität. Seien $(a, x), (b, y), (c, z) \in R \times S$ gegeben, mit $(a, x) \sim (b, y)$ und $(b, y) \sim (c, z)$. Dann existieren $\lambda, \mu \in S$ mit $\lambda(ay - bx) = \mu(bz - cy) = 0$. Wir erhalten $\lambda \cdot \mu \cdot z \cdot (ay - bx) = 0$ und $\mu \cdot \lambda \cdot x \cdot (bz - cy) = 0$, also $\lambda \cdot \mu \cdot z \cdot a \cdot y - \mu \cdot \lambda \cdot x \cdot c \cdot y = 0$, also $\lambda \cdot \mu \cdot y(az - xc) = 0$, und da S multiplikativ abgeschlossen ist, gilt $\lambda \cdot \mu \cdot y \in S$, also insgesamt $(a, x) \sim (c, z)$. □

Sei nun R ein Ring und S multiplikativ abgeschlossen. Dann bezeichnen wir mit $S^{-1}R$ die Menge der Äquivalenzklassen der Relation $\sim$. Für eine Klasse $(a, b) \in S^{-1}R$ schreiben wir auch $\frac{a}{b}$. Wir definieren die folgenden Verknüpfungen auf $S^{-1}R$:

$$\frac{a}{b} + \frac{c}{d} = \frac{ad+bc}{bd}$$

$$\frac{a}{b} \cdot \frac{c}{d} = \frac{ac}{bd},$$

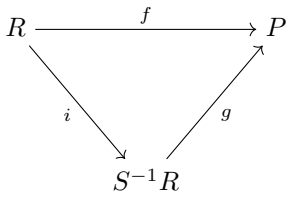
Dann gilt:

Satz 3.39. *Die Menge $S^{-1}R$ ist mit den obigen Verknüpfungen ein (kommutativer) Ring mit Nullelement $\frac{0}{1}$ und Einselement $\frac{1}{1}$. Wir nennen $S^{-1}R$ Bruchring oder Lokalisierung (des Ringes R nach dem multiplikativen System S).*
Die kanonische Abbildung

$$i : R \longrightarrow S^{-1}R$$

$$r \longmapsto \frac{r}{1}$$

ist ein Ringhomomorphismus, welcher die folgende universelle Eigenschaft hat. Für jeden Ringhomomorphismus $f : R \to P$, so dass $f(S) \subset P^*$ gilt, existiert ein eindeutig bestimmter Ringhomomorphismus $g : S^{-1}R \to P$, so dass $f = g \circ i$ gilt, s.h., so dass das Diagramm



kommutiert.

Beweis. Zunächst haben wir zu zeigen, dass die Verknüpfungen + und · auf $S^{-1}R$ wohldefiniert sind. Seien $\frac{a}{b} = \frac{a'}{b'}$, d.h., es gibt $\lambda \in S$ mit $\lambda\,(ab' - a'b) = 0$. Wir wollen jetzt zeigen, dass

$$\frac{ad + bc}{bd} = \frac{a'd + b'c}{b'd}$$

gilt. Wir haben

$$0 = d^2 \cdot \lambda \cdot (ab' - a'b) = \lambda \cdot \left(ab'd^2 + bcb'd - a'bd^2 - b'bdc\right) =$$

$$\lambda\left((ad + bc) \cdot (b'd) - (bd) \cdot (a'd - b'c)\right),$$

und dies zeigt die gewünschte Gleichheit. Analog folgt

$$0 = \lambda \cdot c \cdot d \cdot (ab' - a'b) = \lambda\,(acb'd - bda'c)\,,$$

und daher gilt $\frac{ac}{bd} = \frac{a'c}{b'd}$. Somit sind die beiden Verknüpfungen wohldefiniert, und man kann ganz leicht die Ringaxiome nachprüfen. Ebenso leicht zeigt man, dass i ein Ringhomomorphismus ist.
Wir müssen nun noch die universelle Eigenschaft von i zeigen.
Wir beweisen zunächst die Eindeutigkeit von g. Wegen $f = g \circ i$ muss für alle $a \in R$ die Gleichung $f(a) = g(i(a)) = g(\frac{a}{1})$ gelten. Nach der obigen Definition der Multiplikation in $S^{-1}R$ ist

$$\frac{s}{1} \cdot \frac{1}{s} = \frac{s \cdot 1}{1 \cdot s} = \frac{s}{s} = 1 \in S^{-1}R$$

für alle $s \in S$. Daher ist

$$1 = g(1) = g\left(\frac{s}{1}\right) \cdot g\left(\frac{1}{s}\right) = f(s) \cdot g\left(\frac{1}{s}\right).$$

Somit muss $g\left(\frac{1}{s}\right) = f(s)^{-1}$ gelten, man beachte, dass $f(s)^{-1}$ existiert, da nach Voraussetzung $f(s) \in P^*$ gilt. Andererseits haben alle Elemente von $S^{-1}R$ die Form $\frac{a}{b}$ für $a \in R$, $b \in S$ und es gilt

$$g\left(\frac{a}{b}\right) = g\left(\frac{a}{1}\right) \cdot g\left(\frac{1}{b}\right) = f(a) \cdot f(b)^{-1},$$

und somit ist der Homomorphismus g (falls er existiert), eindeutig durch f bestimmt.
Nun zeigen wir die Existenz von g: Man definiert $g : S^{-1}R \to P$ durch $g\left(\frac{a}{b}\right) := f(a) \cdot f(b)^{-1}$, hier wird wieder verwendet, dass $f(b)$ eine Einheit in P ist. Zu zeigen ist, dass die dadurch gegebene Abbildung wohldefiniert ist: Sei $a' \in R$, $b' \in S$ mit $\frac{a}{b} = \frac{a'}{b'}$, d.h., es gibt $\lambda \in S$ mit $\lambda(ab' - ba') = 0$, dann ist $f(\lambda) \cdot (f(a)f(b') - f(b)f(a')) = 0$, aber nach Voraussetzung ist $f(\lambda) \in P^*$, also folgt $f(a)f(b') - f(b)f(a') = 0$, also $f(a)f(b)^{-1} = f(a')f(b')^{-1}$. Man prüft leicht, dass die so definierte Abbildung $g : S^{-1}R \to P$ auch ein Ringhomomorphismus ist. □

Die folgenden Beispiele sind die Situationen, in denen Lokalisierungen meist verwendet werden.

1. Sei $\mathfrak{p} \subset R$ ein Primideal, dann ist $S := R\backslash\mathfrak{p}$ multiplikativ abgeschlossen ($0 \in \mathfrak{p}$, also $0 \notin S$; $\mathfrak{p} \subsetneq R$, also $1 \notin \mathfrak{p}$, also $1 \in S$; $a \notin \mathfrak{p}, b \notin \mathfrak{p} \;\Rightarrow\; a \cdot b \notin \mathfrak{p}$, da $\mathfrak{p}$ Primideal), und man schreibt $R_\mathfrak{p}$ für den Bruchring $S^{-1}R$ und nennt $R_\mathfrak{p}$ die Lokalisierung von R nach dem Primideal $\mathfrak{p}$.

2. Sei R ein Integritätsring, dann ist $(0) \subset R$ ein Primideal, und wir können die Lokalisierung $R_{(0)}$ betrachten, also den Bruchring $S^{-1}R$, wobei $S := R\backslash\{0\}$ ist. Dies ist ein *Körper*: Sei $\frac{a}{b} \in S^{-1}R$ mit $\frac{a}{b} \neq 0$, d.h. $a \neq 0$, dann ist $a \in S$ und wir haben auch $\frac{b}{a} \in S^{-1}R\backslash\{0\}$ und $\frac{a}{b} \cdot \frac{b}{a} = 1$, also ist $\frac{a}{b}$ invertierbar. Man nennt $R_{(0)}$ den Quotientenkörper von R, und bezeichnet ihn mit $Q(R)$.

   Man bemerke, dass sich in diesem Fall die Äquivalenzrelation $\sim$, welche $Q(R)$ definiert, zu

   $$(a, b) \sim (c, d) \quad \Leftrightarrow ad = bc$$

   vereinfacht. Es folgt, dass der kanonische Ringhomomorphismus $i : R \to Q(R)$ injektiv ist, denn $(a, 1) \sim (0, 1)$ impliziert $a = 0$. Wir können also R immer als Unterring seines Quotientenkörpers $Q(R)$ auffassen, indem wir ein Element $a \in R$ mit $\frac{a}{1} \in Q(R)$ identifizieren.

   Für $R = \mathbb{Z}$ erhalten wir $Q(\mathbb{Z}) = \mathbb{Q}$, und falls K ein beliebiger Körper ist, dann schreiben wir $K(x_1, \ldots, x_n)$ für den Quotientenkörper des Polynomringes $K[x_1, \ldots, x_n]$. Der Körper $K(x_1, \ldots, x_n)$ heißt auch Körper der *rationalen Funktionen* in den Variablen $x_1, \ldots, x_n$ (über K).

3. Sei $f \in R\backslash\{0\}$, dann ist die Menge $S := \{f^i \mid i \in \mathbb{N}\}$ offensichtlich ein multiplikatives System, und wir bezeichnen den Bruchring $S^{-1}R$ mit R_f. Er besteht aus allen Brüchen $\frac{a}{f^i}$ für $i \in \mathbb{N}$.

Wir können jetzt die Primfaktorzerlegung in faktoriellen Ringen (Definition 3.31 und Satz 3.32) auf deren Quotientenkörper ausdehnen.

Lemma 3.40. *Sei R faktoriell, und sei wie in Satz 3.35 $P \subset R$ ein Vertretersystem der irreduziblen (oder primen) Elemente von R. Dann besitzt jedes Element $\frac{a}{b} \in Q(R)$ eine eindeutige Darstellung*

$$\frac{a}{b} = c \cdot \prod_{p \in P} p^{\nu_p(\frac{a}{b})},$$

wobei $c \in R^*$, $\nu_p(\frac{a}{b}) \in \mathbb{Z}$ (beachte: bei der Zerlegung in Formel (3.3) war $\nu_p(a) \in \mathbb{N}$ vorausgesetzt) und so dass für fast alle $p \in P$ die Zahl $\nu_p(\frac{a}{b})$ Null ist. Hierbei soll für $\nu_p(\frac{a}{b}) < 0$ der Ausdruck $p^{\nu_p(\frac{a}{b})}$ das zu $p^{-\nu_p(\frac{a}{b})} \in R$ inverse Element in $Q(R)$ bedeuten. Es gilt also insbesondere $\frac{a}{b} \in R$ genau dann, wenn $\nu_p(\frac{a}{b}) \geq 0$ für alle $p \in P$ ist.

Beweis. Wir betrachten die Primfaktorzerlegungen für die Elemente $a, b \in R$ aus Formel (3.3), dies liefert die Existenz der gewünschten Zerlegung für $\frac{a}{b}$. Zur Eindeutigkeit: Angenommen, wir hätten

$$\frac{a}{b} = c \cdot \prod_{p \in P} p^{\nu_p(\frac{a}{b})} \quad \text{und} \quad \frac{a}{b} = c' \cdot \prod_{p \in P} p^{\nu'_p(\frac{a}{b})},$$

dann multiplizieren wir die Gleichung

$$c \cdot \prod_{p \in P} p^{\nu_p(\frac{a}{b})} = c' \cdot \prod_{p \in P} p^{\nu'_p(\frac{a}{b})}$$

mit dem Ausdruck $\prod_{p \in P} p^{m_p}$, wobei

$$m_p := \begin{cases} -\min(\nu_p(\frac{a}{b}), \nu'_p(\frac{a}{b})) & \text{falls} \quad \min(\nu_p(\frac{a}{b}), \nu'_p(\frac{a}{b})) < 0 \\ 0 & \text{sonst} \end{cases}$$

Wir erhalten dann

$$c \cdot \prod_{p \in P} p^{m_p + \nu_p(\frac{a}{b})} = c' \cdot \prod_{p \in P} p^{m_p + \nu'_p(\frac{a}{b})},$$

und nun sind die Ausrücke auf der rechten und auf der linken Seite dieser Gleichung Elemente von R und wir können die Eindeutigkeit der Primfaktorzerlegung in R benutzen, d.h., wir erhalten, dass $c = c'$ sowie $m_p + \nu_p(\frac{a}{b}) = m_p + \nu'_p(\frac{a}{b})$ ist, und dies impliziert natürlich $\nu_p(\frac{a}{b}) = \nu'_p(\frac{a}{b})$. □

Eine Notation: Wir schreiben für das Element 0 eines faktoriellen Ringes $\nu_p(0) = \infty$.
Wir wollen nun zu den Vorbereitungen des Satzes von Gauß kommen. Hierzu betrachten wir für einen faktoriellen Ring R den Polynomring $Q(R)[x]$ über dem Körper $Q(R)$. Für $f = \sum_{i=0}^{n} a_i x^i \in Q(R)[x]$ und $p \in R$ prim setzen wir

$$\nu_p(f) := \min_{i=0,\ldots,n} (\nu_p(a_i)) \in \mathbb{Z}$$

Klar ist, dass dann $f = 0$ gilt genau dann, wenn $\nu_p(f) = \infty$ ist und f in $R[x]$ liegt genau dann, wenn $\nu_p(f) \geq 0$ gilt.

Lemma 3.41 (Lemma von Gauß)**.** *Sei R faktoriell und $f, g \in Q(R)[x]$. Dann gilt*

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

Beweis. Wir führen den Beweis zunächst in einem Spezialfall durch: Sei $f = a_0 \in Q(R)$ ein konstantes Polynom, und $g = \sum_{j=0}^{m} b_j x^i \in Q(R)[x]$, dann ist

$$\begin{aligned} \nu_p(f \cdot g) &= \nu_p(a_0 \cdot g) \\ &= \min_{j=0,\ldots,m} (\nu_p(a_0 \cdot b_j)) = \min_{j=0,\ldots,m} (\nu_p(a_0) + \nu_p(b_j)) \\ &= \nu_p(a_0) + \min_{j=0,\ldots,m} (\nu_p(b_j)) = \nu_p(a_0) + \nu_p(g). \end{aligned}$$

Für $\deg(f) = 0$ ist der Satz damit bewiesen. Seien nun $f = \sum_{i=0}^{n} a_i x^i \in Q(R)[x]$ beliebig und g wie oben. Dann gibt es ein Element $r \in R$, so dass $r \cdot a_i, r \cdot b_j \in R$ für alle i und j gilt, d.h., so dass $r \cdot f, r \cdot g \in R[x]$ ist. Dann haben wir, wie eben gezeigt, $\nu_p(r \cdot f \cdot r \cdot g) = 2\nu_p(r) + \nu_p(f \cdot g)$. Somit können wir uns darauf beschränken, die Gleichung $\nu_p(f \cdot g) = \nu_p(f) + \nu_p(g)$ für Elemente f, g von $R[x]$ zu zeigen. Sei jetzt $d := \mathrm{ggT}(a_0, \ldots, a_n)$, d.h., es gibt ein $f_1 \in R[x]$, so dass $f = d \cdot f_1$ gilt und so, dass die Koeffizienten von f_1 keinen gemeinsamen Teiler mehr haben. Dies bedeutet, dass es für alle $p \in P$ (mindestens) einen Koeffizienten von f_1 gibt, welcher nicht von p geteilt wird, also ist $\nu_p(f_1) = 0$. Da wieder $\nu_p(f) = \nu_p(d) + \nu_p(f_1)$ gilt, können wir uns also ein weiteres Mal einschränken: Wir müssen die Gleichung $\nu_p(f \cdot g) = \nu_p(f) + \nu_p(g)$ nur unter der Zusatzannahme $\nu_p(f) = \nu_p(g) = 0$ zeigen, d.h., wir müssen unter dieser Annahme zeigen, dass $\nu_p(f \cdot g) = 0$ gilt. Betrachte die Projektion $R \to R/(p)$, und den dadurch induzierten Ringhomomorphismus

$$\begin{array}{rcl} \varphi : R[x] & \longrightarrow & (R/(p))[x] \\ \sum_{i=0}^{n} a_i x^i & \longmapsto & \sum_{i=0}^{n} [a_i] x^i, \end{array}$$

wobei $[a_i]$ die Restklasse in $R/(p)$ von $a_i \in R$ ist. Der Kern von φ sind alle Polynome, deren sämtliche Koeffizienten durch p teilbar sind, anders gesagt

$$\ker(\varphi) = \{ f \in R[x] \mid \nu_p(f) > 0 \}.$$

Wir haben also $f, g \notin \ker(\varphi)$, d.h., $\varphi(f) \neq 0, \varphi(g) \neq 0$. p ist ein Primelement in R also ist (p) ein Primideal, und daher (Satz 3.19) ist $R/(p)$ ein Integritätsring. Wegen Lemma 3.7 ist dann auch $(R/(p))[x]$ ein Integritätsring, und es folgt $\varphi(f \cdot g) = \varphi(f) \cdot \varphi(g) \neq 0$, aber dies bedeutet, dass $\nu_p(f \cdot g) = 0$ ist, wie gefordert. □

Als Konsequenz erhalten wir

Korollar 3.42. *Sei R faktoriell und $f \in R[x]$ ein unitäres Polynom. Seien $g, h \in Q(R)[x]$ ebenfalls unitär, so dass $f = g \cdot h$ gilt. Dann sind g und h bereits Elemente von $R[x]$.*

Beweis. Da $f = a_n x^n + \cdot + a_0 \in R[x]$ ist mit $a_n = 1$, folgt $\nu_p(f) = 0$ für alle $p \in P$, und analog haben wir $\nu_p(g) \leq 0, \nu_p(h) \leq 0$. Wegen des letzten Lemmas ist $\nu_p(f) = \nu_p(g) + \nu_p(h)$, und dies impliziert $\nu_p(g) = \nu_p(h) = 0$, also $g, h \in R[x]$. □

Wir nennen ein Polynom $f = a_n x^n + \ldots + x_0 \in R[x]$ (R soll wieder ein faktorieller Ring sein) *primitiv*, falls $\mathrm{ggT}(a_0, \ldots, a_n) = 1$ gilt, d.h., wenn $\nu_p(f) = 0$ für alle $p \in P$ ist. Für ein beliebiges Polynom $g = b_m x^m + \ldots + b_0 \in Q(R)[x]$ setzen wir $q := \prod_{p \in P} p^{\nu_p(g)}$, dann ist $g' := q^{-1} \cdot g$ ein Element von $R[x]$ und primitiv, denn es gilt $\nu_p(g') = 0$ für alle $p \in P$.
Wir haben nun alle Hilfsmittel zur Verfügung, um den Satz von Gauß zu zeigen, welcher die Teilbarkeitstheorie in Polynomringen beschreibt.

Satz 3.43 (Satz von Gauß)**.** *Sei R ein faktorieller Ring. Dann ist auch $R[x]$ faktoriell. Ein Element $f \in R[x]$ ist ein Primelement in $R[x]$ genau dann, wenn*

1. *f ein Primelement in R* ***oder***
2. *wenn f primitiv und ein Primelement in $Q(R)[x]$ ist.*

Falls f also ein primitives Polynom in $R[x]$ ist (dann kann es insbesondere kein Primelement in R sein), dann ist f irreduzibel in $R[x]$ genau dann, wenn es irreduzibel in $Q(R)[x]$ ist.

Beweis. Zunächst ist klar, dass ein Primelement $p \in R$ auch in $R[x]$ prim ist: Wir haben $(R/(p))[x] \cong R[x]/(p)$, ist p prim, dann ist $R/(p)$ und mit Lemma 3.7 auch $(R/(p))[x]$ ein Integritätsring, also auch $R[x]/(p)$ und (p) ist ein Primideal in $R[x]$, also ist p ein Primelement in $R[x]$.
Sei andererseits $f \in R[x]$ primitiv und ein Primelement in $Q(R)[x]$. Wir wollen zeigen, dass f dann auch in $R[x]$ ein Primelement ist. Seien $g, h \in R[x]$ gegeben mit $f | g \cdot h$. Natürlich gilt $f | g \cdot h$ auch in $Q(R)[x]$, und

da f in $Q(R)[x]$ ein Primelement sein soll, gibt es also ein $r \in Q(R)[x]$ mit $g = f \cdot r$ oder $h = f \cdot r$. Ohne Beschränkung der Allgemeinheit nehmen wir den ersten Fall an, dann müssen wir zeigen, dass $r \in R[x]$ gilt. Wir verwenden das Lemma von Gauß (Lemma 3.41), und erhalten $\nu_p(g) = \nu_p(f) + \nu_p(r)$ für alle $p \in P$. Wegen $g, f \in R[x]$ ist $\nu_p(g), \nu_p(f) \geq 0$, aber f ist sogar primitiv, d.h., $\nu_p(f) = 0$, und daher ist auch $\nu_p(r) \geq 0$ für alle $p \in P$. Dies aber bedeutet $r \in R[x]$, wie gewünscht.
Wir zeigen nun, dass $R[x]$ faktoriell ist und nur die Primelemente in 1. und 2. hat. Sei $f \in R[x] \setminus (R^* \cup \{0\})$ gegeben, dann müssen wir nach Satz 3.32 beweisen, dass sich f in ein Produkt von Primelementen des Typs 1. und 2. zerlegen läßt. Wir können f schreiben als $f = d \cdot f'$, wobei d der größte gemeinsame Teiler der Koeffizienten von f und f' primitiv ist. Da R faktoriell ist, zerlegt sich d in ein Produkt von Primelementen des Typs 1. Wir müssen also nur noch zeigen, dass primitive Polynome $f' \in R[x]$ eine Zerlegung in primitive Polynome in $R[x]$, welche in $Q(R)[x]$ prim sind, besitzen. $Q(R)$ ist ein Körper, also ist nach Lemma 3.14 (bewiesen in Satz 3.27) $Q(R)[x]$ ein Hauptidealring, also nach Satz 3.33 faktoriell. Wir haben also eine Zerlegung $f' = c \cdot q_1 \dots q_r$ mit $c \in (Q(R)[x])^* = Q(R) \setminus \{0\}$ und so dass q_i ien Primelement in $Q(R)[x]$ ist. Wir haben schon gesehen, dass zu jedem $q_i \in Q(R)[x]$ ein $d_i \in Q(R)^*$ existiert, so dass $\widetilde{q}_i := d_i^{-1} \cdot q_i$ ein primitives Polynom in $R[x]$ ist. Betrachte die Zerlegung

$$f' = d \cdot \widetilde{q}_1 \cdot \ldots \cdot \widetilde{q}_r \quad \text{mit} \quad d := c \cdot d_1 \cdot \ldots \cdot d_n.$$

Die Elemente $\widetilde{q}_i$ sind primitiv und in $Q(R)[x]$ zu q_i assoziiert, also insbesondere prim in $Q(R)[x]$, d.h., vom Typ 2. Es bleibt zu zeigen, dass $d \in R$ liegt. Wir wissen aber aus dem Lemma von Gauß, dass $\nu_p(f') = \nu_p(d) + \nu_p(\widetilde{q}_1) + \ldots + \nu_p(\widetilde{q}_r)$ ist, und daher weil f' und alle $\widetilde{q}_i$ primitiv sind, haben wir $\nu_p(f') = \nu_p(\widetilde{q}_1) = \ldots = \nu_p(\widetilde{q}_r) = 0$, also auch $\nu_p(d) = 0$ für alle $p \in P$. Damit ist $d \in R$ und sogar $d \in R^*$ (betrachte die Primelementezerlegung von d, wenn $\nu_p(d) = 0$ für alle $p \in P$ gilt, ist d notwendig eine Einheit). □

Als Anwendung diskutieren wir nun noch einige Kriterien, mit denen man in der Praxis prüfen kann, ob ein gegebenes Polynom irreduzibel ist. Das erste Kriterium nutzt die Reduktion der Koeffizienten eines Polynoms modulo eines Primelementes des Ringes R.

Satz 3.44. *Sei R faktoriell und $p \in R$ prim. Sei $f = a_n x^n + \ldots + a_0 \in R[x] \setminus \{0\}$ ein Polynom, so dass $p \nmid a_n$ gilt. Wir betrachten wieder den Ringhomomorphismus $\varphi : R[x] \to (R/(p))[x]$, welcher die Koeffizienten modulo (p) reduziert. Dann gilt: Ist $\varphi(f)$ irreduzibel in $(R/(p))[x]$, so ist f irreduzibel in $Q(R)[x]$. Ist f primitiv und ist $\varphi(f)$ irreduzibel in $(R/(p))[x]$, so ist f sogar irreduzibel in $R[x]$.*

Beweis. Der wesentliche Fall ist der, dass f primitiv ist. Dies nehmen wir zunächst an. Wir zeigen die Kontraposition der Aussage, sei daher f reduzibel mit $f = g \cdot h$, $g, h \in R[x]$, $\deg(g), \deg(h) > 0$. Dann ist das Produkt der Leitkoeffizienten von g und h gerade der Leitkoeffizient von f, dieser wird nicht von p geteilt, also kann p auch nicht die Leitkoeffizienten von g und h teilen. Dies impliziert, dass $\deg(\varphi(g)) = \deg(g) > 0$ und $\deg(\varphi(h)) = \deg(h) > 0$, und die Gleichung $\varphi(f) = \varphi(g) \cdot \varphi(h)$ zeigt, dass f reduzibel in $(R/(p))[x]$ ist, was zu zeigen war.
Falls nun $f = c \cdot f'$ mit primitivem $f' \in R[x]$ und $c \in R \setminus \{0\}$ ist, dann teilt p weder c noch den Leitkoeffizienten von f'. Nach Voraussetzung wissen wir, dass $\varphi(f)$ in $(R/(p))[x]$ irreduzibel ist, aber dies gilt natürlich genauso für $\varphi(f')$. Wie gerade gezeigt, ist dann f' in $R[x]$ irreduzibel, und der Satz von Gauß sagt uns, dass dann f' auch in $Q(R)[x]$ irreduzibel sein muss. In $Q(R)[x]$ sind aber f und f' assoziiert, und daher ist f irreduzibel in $Q(R)[x]$. □

Das zweite wichtige Hilfsmittel zu Prüfen der Zerlegbarkeit von Polynomen ist das Eisensteinsche Irreduzibilitätskriterium.

Satz 3.45. *Sei R faktoriell und $f = a_n x^n + \ldots + a_0 \in R[x]$ primitiv mit $\deg(f) = n$. Sei $p \in R$ ein Primelement mit $p \nmid a_n$, $p | a_i$ für alle $i \in \{0, 1, \ldots, n-1\}$ und $p^2 \nmid a_0$. Dann ist f irreduzibel in $R[x]$ (und daher auch in $Q(R)[x]$).,*

Beweis. Sei eine Zerlegung $f = g \cdot h$ mit $g, h \in R[x]$ gegeben. Wieder betrachten wir den Homomorphismus $\varphi : R[x] \to (R/(p))[x]$. Aus den Voraussetzungen folgt, dass $\varphi(g) \cdot \varphi(h) = \varphi(f) = [a_n] \cdot x^n \neq 0$ gilt. Wir

können diese Gleichung auch in dem faktoriellen Ring $Q\left(R/(p)\right)[x]$ lesen, und hier besitzen $\varphi(g)$ und $\varphi(h)$ eine eindeutige Zerlegung in irreduzible Elemente. Da deren Produkt gleich $[a_n] \cdot x^n$ ist, sind also $\varphi(g)$ und $\varphi(h)$ bis auf Faktoren aus $R/(p)$ Potenzen von x. Wir wissen außerdem, dass $\deg(\varphi(g)) + \deg(\varphi(h)) = n = \deg(g) + \deg(h)$ gilt. Also ist entweder $\deg(g) = 0, \deg(h) = n$ bzw. $\deg(g) = n, \deg(h) = 0$, und dann ist die Aussage bewiesen, oder $\deg(g), \deg(h) \in \{1, \ldots, n-1\}$. Dann müssen aber die Absolutkoeffizenten (also die Koeffizienten von x^0) von g und h durch p teilbar sein (denn sonst hätte eines der Bilder $\varphi(g)$ oder $\varphi(h)$ einen nichtverschwindenden Absolutkoeffizienten und wäre keine Potenz von x), und dann gilt $p^2 | a_0$, was ein Widerspruch darstellt. □

3.4 Moduln über Hauptidealringen

In diesem Abschnitt wollen wir zum einen den fundamentalen Bergiff eines Moduls über einem Ring kennenlernen. Er verallgemeinert den Begriff des Vektorraums, führt aber zu ein Fülle neuer Phänomene. Wir diskutieren einige elementare Eigenschaften von Moduln, und studieren dann den Spezialfall von endlich erzeugten Moduln über Hauptidealringen, welche eine vollständige Klassifikation erlauben. Diesen Klassifikationssatz kann man insbesondere auf endlich erzeugte abelsche Gruppen (gesehen als Moduln über $\mathbb{Z}$) anwenden, und erhält einige Resultate, welche wir zum Teil (mit elementareren Methoden) schon im Kaptiel 2 hergeleitet hatten.
Wir beginnen mit der Definition eines Moduls, wobei wir uns auf den Fall von kommutativen Ringen mit 1 beschränken.

Definition 3.46. *Sei R ein kommutativer Ring mit 1.*

1. *Ein R-Modul ist eine abelsche Gruppe $(M, +)$ zusammen mit einer skalaren Multiplikation $\cdot : R \times M \to M$, welche die üblichen Vektorraum-Axiome erfüllt, d.h., es gilt für alle $a, b \in R$, $x, y \in M$.*

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

2. *Sei $(x_i)_{i \in I}$ ein System von Elementen eines R-Moduls M. Es heißt Erzeugendensystem, falls gilt:*

$$\forall x \in M : \exists J \subset I \text{ endlich und } (a_i)_{i \in J}, a_i \in R \text{ so daß } x = \sum_{i \in J} a_i x_i$$

Es heißt frei oder linear unabhängig, falls für alle endlichen Teilmengen J von I gilt:

$$0 = \sum_{i \in J} a_i x_i \implies a_i = 0 \ \ \forall i \in J$$

Es heißt Basis, falls es ein freies Erzeugendensystem ist.

3. *Ein R-Modul M heißt endlich erzeugt, falls er ein endliches Erzeugendensystem besitzt. Er heißt frei falls er eine Basis besitzt.*

4. *Der Rang eines R-Moduls M, geschrieben* $\operatorname{rang}(M)$*, ist das Supremum der Längen aller Systeme linear unabhängiger Elemente.*

5. *Homomorphismen, Isomorphismen von R-Moduln, R-Untermoduln und Produkte von R-Moduln werden wie bei Vektorräumen definiert.*

6. *Ist $N \subset M$ ein R-Untermodul von M, dann ist auch M/N (nach Satz 2.10 eine abelsche Gruppe) ein R-Modul, der Quotientenmodul von M nach N.*

7. *Seien M_1, M_2 R-Untermoduln von M. Dann ist M per Definition die direkte Summe, geschrieben $M = M_1 \oplus M_2$ wenn gilt: $M = M_1 + M_2$ und $M_1 \cap M_2 = \{0\}$.*

Wir notieren kurz die wichtigsten Eigenschaften und Beispiele für Moduln.

Lemma 3.47. *1. Sei K ein Körper, dann ist ein K-Modul dasselbe wie ein K-Vektorraum.*

2. *G ist eine abelsche Gruppe $\iff$ G ist ein $\mathbb{Z}$-Modul:*
   „$\Longleftarrow$“: klar, denn ein $\mathbb{Z}$-Modul ist eine abelsche Gruppe.
   „$\Longrightarrow$“: die skalare Multiplikation $\mathbb{Z} \times G \to G$ ist definiert durch

$$\begin{aligned} n \cdot x &:= \underbrace{x + \ldots + x}_{n \text{ Summanden}} \quad n \geq 1 \\ 0 \cdot x &:= 0 \\ (-n) \cdot x &:= \underbrace{(-x) + \ldots + (-x)}_{n \text{ Summanden}} \quad n \geq 1 \end{aligned}$$

   Man zeigt leicht: Alle Axiome in Definition 3.46 sind erfüllt.

3. *Ein kommutativer Ring R mit 1 ist selbst ein R-Modul. Seine Untermoduln sind genau die Ideale von R.*

4. *Sei R ein Integritätsring und M ein R-Modul. Die Menge $\mathrm{Tor}(M) := \{x \in M \mid \exists a \in R\backslash\{0\}, a \cdot x = 0\}$ ist ein R-Untermodul. Sie heißt Torsionsuntermodul oder Torsionsmodul von M. Ein Modul M heißt Torsionsmodul, falls $M = \mathrm{Tor}(M)$ gilt, dies ist äquivalent zu $\mathrm{rang}(M) = 0$. (Achtung: Im Gegensatz zu Vektorräumen, also Moduln über einem Körper, folgt aus $\mathrm{rang}(M) = 0$ nicht, dass $M = 0$ ist.)*

   Eine alternative Beschreibung des Torsionsuntermoduls erhält man, in dem man $S := R\backslash\{0\}$ setzt, und die Menge $S^{-1}M$ betrachtet: Dies ist die Menge der Äquivalenzklassen der folgenden Relation auf $M \times S$:

$$(m, s) \sim (m', s') \quad \iff \quad \exists \lambda \in S : \lambda\,(s' \cdot m - s \cdot m') = 0.$$

   und wir schreiben wieder $\frac{m}{s}$ für solch eine Äquivalenzklasse. Man prüft leicht, dass dann $S^{-1}M$ zu einem Vektorraum über der Quotientenkörper $S^{-1}R = Q(R)$ wird. Wir haben den kanonischen R-Modulhomomorphismus $\iota : M \to S^{-1}M$, welcher m auf $\frac{m}{1}$ abbildet, und es gilt

$$\ker(\iota) = \mathrm{Tor}(M)$$

5. *Sei $R = K$ ein Körper. Dann ist M frei und $\mathrm{Tor}(M) = \{0\}$.*

6. *Für den Fall $R = \mathbb{Z}$ ist $\mathrm{Tor}(M) = \{x \in M \mid \mathrm{ord}(x) < \infty\} \subset M$.*

7. *Sei M ein freier R-Modul. Dann haben je zwei Basen von M gleich viele, nämlich $\mathrm{rang}(M)$, Elemente. Falls $\mathrm{rang}(M) < \infty$, dann ist $M \cong R^{\mathrm{rang}(M)}$ als R-Modul.*

Beweis. Übung. □

Für die weiteren Untersuchungen in diesem Abschnitt brauchen wir den Begriff der Länge eines Moduls.

Definition 3.48. *Sei R ein Ring und M ein R-Modul. Dann ist die Länge von M, geschrieben $l_R(M)$ das Supremum über die Länge l aller Ketten von R-Untermoduln von M des Typs*

$$\{0\} \subsetneq M_1 \subsetneq M_2 \subsetneq \ldots \subsetneq M_l = M$$

Falls $l_R(M) < \infty$ gilt, dann heißt M ein artinscher Modul. *Ein Ring R heißt artinsch, falls er als Modul über sich selbst artinsch ist.*

Wir benötigen die folgenden einfachen Eigenschaften der Länge.

Lemma 3.49. *1. Sei $M = M' \oplus M''$, dann ist $l_R(M' \oplus M'') = l_R(M') + l_R(M'')$.*

2. Sei R ein Hauptidealring (dann ist R nach Satz 3.33 insbesondere ein faktorieller Ring), sei $a \in R$, und sei $a = p_1 \cdot \ldots \cdot p_r$ eine Zerlegung in Primelemente (man beachte, dass hier Primelemente mehrfach vorkommen können und dass die Zahl r ist nach Satz 3.32 eindeutig bestimmt ist). Dann ist $l_R(R/(a)) = r$.

Beweis. 1. Seien Ketten von Untermoduln

$$0 \subsetneq M'_1 \subsetneq \ldots \subsetneq M'_r = M'$$

$$0 \subsetneq M''_1 \subsetneq \ldots \subsetneq M''_s = M''$$

gegeben, dann ist

$$0 \subsetneq M'_1 \oplus 0 \subsetneq \ldots \subsetneq M'_r \oplus 0 \subsetneq M'_r \oplus M''_1 \subsetneq \ldots \subsetneq M'_r \oplus M''_r = M$$

eine Kette von Untermoduln von M, und wir erhalten $l_R(M') + l_R(M'') \leq l_R(M)$. Wir müssen die umgekehrte Abschätzung beweisen. Sei also eine beliebige Kette

$$0 \subsetneq M_1 \subsetneq \ldots \subsetneq M_l = M$$

gegeben, dann folgt für alle $i \in \{1, \ldots, l\}$, dass $M_i \cap M' \subsetneq M_{i+1} \cap M'$ oder $\pi_2(M_i) \subsetneq \pi_2(M_{i+1})$ gilt, wobei $\pi_2 : M \twoheadrightarrow M''$ die kanonische Projektion auf den zweiten Summanden ist (so dass $\ker(\pi_2) = M'$ gilt). Wäre nämlich $M_i \cap M_1 = M_{i+1} \cap M'$ und $\pi_2(M_i) = \pi_2(M_{i+1})$, dann hätten wir $M_i = M_{i+1}$. Hieraus folgt, dass $l_R(M) \leq l_R(M') + l_R(M'')$ gilt, und damit ist die gewünschte Gleichheit bewiesen.

2. Wir können die Primelement $p_1, \ldots, p_r$ umnummerieren, so dass $a = c \cdot p_1^{\nu_1} \cdot \ldots \cdot p_s^{\nu_s}$, mit $s \leq r$, $c \in R^*$ derart ist, dass $p_i \nsim p_j$ für $i, j \in \{1, \ldots s\}$, $i \neq j$ ist (insbesondere haben wir $r = \nu_1 + \ldots + \nu_s$). Dann folgt aus dem Chinesischen Restsatz (Satz 3.23), dass

$$R/(a) = \bigoplus_{i=1}^{s} R/(p_i^{\nu_i})$$

gilt, wegen 1. kann man sich also auf den Beweis im Fall $s = 1$ einschränken.

Die R-Untermoduln von $R/(p_1^{\nu_1})$ sind genau die Ideale von $R/(p_1^{\nu_1})$ und diese entsprechen nach Satz 3.17 den Idealen von $\mathfrak{a} \subset R$ mit $p_1^{\nu_1} \in \mathfrak{a}$. Da R ein Hauptidealring ist, sind diese von der Form p^i mit $i \leq \nu_1$. Andererseits gilt $(p^{i+1}) \subsetneq (p^i)$, daher ist die Länge von $R/(p_1^{\nu_1})$ gleich ν_1.

□

Als Folgerung erhalten wir folgendes Lemma, welches wir später zum Beweis der Eindeutigkeitsaussage des Elementarteilersatzes verwenden werden.

Lemma 3.50. *Sei R ein Hauptidealring und Q ein R-Modul, so dass es einen R-Modulisomorphismus*

$$Q \cong \bigoplus_{i=1}^{n} \frac{R}{(a_i)}$$

gibt, wobei $a_1, \ldots, a_n \in R \backslash (R^* \cup \{0\})$ mit $a_{i+1} | a_i$ für alle $i \in \{1, \ldots, n-1\}$. Dann sind die Elemente $a_1, \ldots, a_n$ bis auf Assoziiertheit eindeutig durch Q bestimmt. (Man beachte: Später wird häufig die Bedingung $a_i | a_{i+1}$ benutzt, diese ist aber durch Umordnen der Summanden der Zerlegung äquivalent zur hier benutzten Bedingung, wir verwenden die Bedingung $a_{i+1} | a_i$, weil sich im Beweis die Indizes damit besser anordnen lassen).

Beweis. Seien zwei Zerlegungen

$$Q \cong \bigoplus_{i=1}^{n} \frac{R}{(a_i)} \cong \bigoplus_{j=1}^{m} \frac{R}{(b_j)}$$

mit von Null verschiedenen Nicht-Einheiten a_i, b_j gegeben, so dass $a_{i+1}|a_i$ für alle $i \in \{1, \dots, n-1\}$ und $b_{j+1}|b_j$ für alle $j \in \{1, \dots, m-1\}$ gilt. Angenommen, die Zerlegungen seien nicht (bis auf Einheiten) gleich, dann gibt es $k = \min\{j \leq \min(m,n) \,|\, (a_j) \neq (b_j)\}$. Wir betrachten jetzt den R-Untermodul $a_k \cdot Q$ von Q. Dann haben wir

$$a_k \cdot Q \cong \bigoplus_{j=1}^{m} a_k \cdot \tfrac{R}{(b_j)} \overset{(*)}{\cong} \left(\bigoplus_{j=1}^{k-1} a_k \cdot \tfrac{R}{(a_j)}\right) \oplus \left(\bigoplus_{j=k}^{m} a_k \cdot \tfrac{R}{(b_j)}\right)$$

$$a_k \cdot Q \cong \bigoplus_{i=1}^{n} a_k \cdot \tfrac{R}{(a_i)} \cong \left(\bigoplus_{i=1}^{k-1} a_k \cdot \tfrac{R}{(a_i)}\right) \oplus \left(\bigoplus_{i=k}^{n} a_k \cdot \tfrac{R}{(a_i)}\right) \overset{(**)}{\cong} \left(\bigoplus_{i=1}^{k-1} a_k \cdot \tfrac{R}{(a_i)}\right)$$

Hierbei folgt $(*)$ aus $a_i = b_i$ für alle $i \in \{1, \dots, k-1\}$ und $(**)$ folgt aus $a_i|a_k$ für alle $i \in \{k, k+1, \dots, n\}$. Wir verwenden jetzt Lemma 3.49, wegen $l_R(Q) < \infty$ folgt durch Vergleich der beiden Darstellungen von $l_R(a_k \cdot Q)$, dass $l_R(a_k \cdot \frac{R}{(b_k)}) = 0$, also $a_k \cdot \frac{R}{(b_k)} = 0$ ist, dies bedeutet aber $(b_k) \subset (a_k)$. Mit dem gleichen Argument kann man die andere Inklusion zeigen, und damit ist $(a_k) = (b_k)$ im Widerspruch zu unserer Annahme. Wir erhalten also $(a_j) = (b_j)$ für alle $j \leq \min(m,n)$. Sei ohne Beschränkung der Allgemeinheit $m \leq n$, dann liefert erneute Anwendung von Lemma 3.49, dass $l_R\left(\oplus_{i=m+1}^{n} \frac{R}{(a_i)}\right) = 0$ ist, also folgt $m = n$. □

Nach diesem Vorbereitungen kommen wir jetzt zum sogenannten Elementarteilersatz. Ab jetzt werden wir nur noch Moduln über Hauptidealringen betrachten, weil die zentralen Aussagen nur in diesem Fall stimmen. Die folgende Aussage ist das wesentliche Hilfsmittel beim nachfolgenden Klassifizierungssatz für endlich erzeugte Moduln über Hauptidealringen (Satz 3.54).

Satz 3.51 (Elementarteilersatz)**.** *Sei R ein Hauptidealring und F ein freier R-Modul. Sei $M \subset F$ ein Untermodul mit* $\operatorname{rang}(M) = n$. *Dann gibt es Elemente $x_1, \dots, x_n \in F$ (aber im Allgemeinen $x_i \notin M$), welche Teil einer Basis von F sind, sowie Koeffizienten $a_1, \dots, a_n \in R\backslash\{0\}$, so dass gilt:*

1. *$a_1 \cdot x_1, \dots, a_n \cdot x_n$ bilden eine Basis von M (insbesondere ist M frei).*
2. *$a_i|a_{i+1}$ für alle $i \in \{1, \dots, n-1\}$.*

Die Elemente $a_1, \dots, a_n \in R$ sind bis auf Multiplikation mit Einheiten eindeutig bestimmt (und unabhängig von der Wahl von $x_1, \dots, x_n$). Sie heißen die Elementarteiler von $M \subset F$.
Setze $M_{\text{sat}} := \{y \in F \,|\, \exists a \in R\backslash\{0\} : ay \in M\}$ (die Saturierung *von M), dann ist $M \subset M_{\text{sat}}$, und es gilt $M_{\text{sat}} = \oplus_{i=1}^{n} Rx_i$. Also sind zwar nicht die Elemente $x_1, \dots, x_n$, wohl aber der von ihnen erzeugte Untermodul von F eindeutig durch M bestimmt. Außerdem gilt*

$$\frac{M_{\text{sat}}}{M} \cong \bigoplus_{i=1}^{n} \frac{R}{(a_i)} \tag{3.4}$$

Zum Beweis benötigen wir zunächst einen Begriff.

Definition-Lemma 3.52. *Sei $x \in F$, und $y_1, \dots, y_r$ eine Basis von F. Sei $x = \sum_{i=1}^{r} \lambda_i \cdot y_i$, dann definieren wir den* Inhalt *von x als* $\operatorname{cont}(x) := \operatorname{ggT}(\lambda_1, \dots, \lambda_r)$ *(beachte, dass damit der Inhalt eines Elements nur bis auf Einheiten definiert ist). Dann gilt*

1. $\operatorname{cont}(x)$ *ist wohldefiniert, d.h., die obige Definition hängt nicht von der Wahl der Basis $y_1, \dots, y_r$ von F ab.*
2. *Sei F^* die Menge aller R-Modulhomomorphismen von F nach R (siehe Beweis unten), dann existiert für alle $x \in F$ ein $\varphi \in F^*$ mit $\varphi(x) = \operatorname{cont}(x)$.*

3. *Für alle $x \in F$ und $\varphi \in F^*$ gilt* $\mathrm{cont}(x)|\varphi(x)$.

4. *Sei $M \subset F$ ein Untermodul, dann existiert ein $x \in M$ so dass* $\mathrm{cont}(x)|\mathrm{cont}(y)$ *für alle $y \in M$ gilt.*

Beweis. 1. Wir betrachten wie in der Formulierung des Lemmas den R-Modul $F^* := \mathrm{Hom}_R(F, R)$ aller R-Modulhomomorphismen von F nach R (genannt der zu F duale Modul). Für festes $x \in F$ ist die Menge $\{\varphi(x) \,|\, \varphi \in F^*\}$ ein Ideal in R (es heiße I), also von der Form $I = (c)$ für ein $c \in R$. Die Behauptung ist, dass dann $c = \mathrm{cont}(x)$ gilt:

Zunächst verifiziert man leicht, dass F^* selbst ein freier R-Modul vom Rang r ist, es ist nämlich $\varphi_1, \ldots, \varphi_r$ mit $\varphi_i(y_j) = \delta_{ij}$ eine Basis von F^*. Sei nun also $x \in F$ fest gewählt, und schreibe $x = \sum_{i=1}^r \lambda_i y_i$, dann gibt es wegen $\mathrm{cont}(x) = \mathrm{ggT}(\lambda_1, \ldots, \lambda_r)$ Koeffizienten $c_1, \ldots, c_r \in R$ mit $\mathrm{cont}(x) = \sum_{i=1}^r c_i \cdot \lambda_i$ (siehe Lemma 3.36). Setzen wir dann $\varphi = \sum_{i=1}^r c_i \cdot \varphi_i$, dann gilt $\varphi(x) = \mathrm{cont}(x)$, also $\mathrm{cont}(x) \in I$, d.h. wir haben $c|\mathrm{cont}(x)$. Andererseits gilt für jede Linearform $\psi \in F^*$, dass $\psi(x)$ sich als Linearkombination der Elemente $\lambda_1, \ldots, \lambda_r$ schreiben läßt, aber wegen $\mathrm{cont}(x) = \mathrm{ggT}(\lambda_1, \ldots, \lambda_r)$. gilt dann $\mathrm{cont}(x)|\psi(x)$, und daher haben wir auch $\mathrm{cont}(x)|c$.

2. Dies folgt sofort aus der bewiesenen Gleichheit $I = (\mathrm{cont}(x))$.

3. Auch dies folgt aus $I = (\mathrm{cont}(x))$.

4. Sei X die Menge aller (Haupt)-Ideale in R der Form $(\mathrm{cont}(x))$ für alle $x \in M$. Dann existiert in X ein bezüglich der Inklusion von Idealen maximales Element, andernfalls gäbe es eine unendliche Kette

$$(\mathrm{cont}(x_1)) \subsetneq (\mathrm{cont}(x_2)) \subsetneq \ldots,$$

im Widerspruch (siehe Satz 3.33) zu der Tatsache, dass R noethersch ist. Sei $x \in M$ ein Element, so dass $(\mathrm{cont}(x))$ in X ein maximales Element ist. Wir wollen zeigen, dass dann $\mathrm{cont}(x)|\mathrm{cont}(y)$ für alle $y \in M$ gilt. Zunächst gibt es wegen Punkt 2. ein $\varphi \in F^*$ mit $\varphi(x) = \mathrm{cont}(x)$. Wir beweisen zuerst:

$$\varphi(x)|\varphi(y) \quad \forall y \in M \tag{3.5}$$

Sei $d := \mathrm{ggT}(\varphi(x), \varphi(y))$, dann existieren $a, b \in R$ mit $d = a\varphi(x) + b\varphi(y)$, aber dann ist $d = \varphi(ax + by)$. Wir wenden Punkt 3. auf das Element $ax + by \in F$ an, und erhalten $\mathrm{cont}(ax + by)|d$, aber wegen $d|\varphi(x)$ folgt dann $\mathrm{cont}(ax + by)|\mathrm{cont}(x)$. Da aber das Ideal $I = (\mathrm{cont}(x))$ maximal gewählt war, ist notwendig $\mathrm{cont}(ax + by) = \mathrm{cont}(x)$. Damit haben wir $\mathrm{cont}(x)|d$ und mit $d|\varphi(y)$ folgt schließlich $\varphi(x)|\varphi(y)$ und damit ist Formel (3.5) bewiesen.

Wir wollen nun aus der Teilbarkeitsrelation (3.5) die Relation $\mathrm{cont}(x)|\mathrm{cont}(y)$ ableiten. Es reicht, zu zeigen, dass für alle $\psi \in F^*$ die Relation $\varphi(x)|\psi(y)$ gilt, denn nach Punkt 2. existiert ein $\psi \in F^*$ mit $\mathrm{cont}(y) = \psi(y)$. Wenn wir Punkt 3. auf das Element $x \in M$ anwenden, erhalten wir, dass $\varphi(x)|\psi(x)$ gilt, also haben wir $\varphi(x)|\psi(y)$ genau dann, wenn $\varphi(x)|(\psi(y) - \mu \cdot \psi(x))$ für irgendein $\mu \in R$ gilt, und dies ist äquivalent dazu, dass $\varphi(x)|\psi(y - \mu x)$ gilt. Andererseits sagt (3.5), dass $\varphi(x)|\varphi(y)$ ist. Wir können also insbesondere y durch $y - \frac{\varphi(y)}{\varphi(x)} \cdot x$ ersetzen, und uns daher auf den Beweis der Relation $\varphi(x)|\psi(y)$ für alle $\psi \in F^*$ und alle $y \in M$ mit $\varphi(y) = 0$ einschränken.

Mit exakt derselben Argumentation können wir ψ durch $\psi - \frac{\psi(x)}{\varphi(x)} \cdot \varphi$ ersetzen: zunächst folgt aus $\varphi(x)|\psi(x)$, dass $\psi - \frac{\psi(x)}{\varphi(x)} \cdot \varphi$ als Element von F^* existiert, und dann ist wegen $\varphi(x)|\varphi(y)$ die Teilbarkeit $\varphi(x)|\psi(y)$ äquivalent zu $\varphi(x)|(\psi - \mu'\varphi)(y)$ für irgendein $\mu' \in R$. Wir haben also das Problem auf den Beweis von $\varphi(x)|\psi(y)$ für alle $\psi \in F^*$ mit $\psi(x) = 0$ und alle $y \in M$ mit $\varphi(y) = 0$ reduziert.

Dann setzen wir $d := \mathrm{ggT}(\varphi(x), \psi(y))$ und schreiben $d = a\varphi(x) + b\psi(y)$, mit $a, b \in R$. Es folgt

$$(\varphi + \psi)(ax + by) = a\varphi(x) + b\psi(y)) = d$$

und damit (wegen Punkt 3. angewandt auf $ax + by$) $\mathrm{cont}(ax + by)|d$. Wegen $d|\varphi(x)$ erhalten wir $\mathrm{cont}(ax + by)|\varphi(x)$, und die Maximalität von $(\mathrm{cont}(x))$ liefert $\varphi(x) = \mathrm{cont}(ax + by)$, und daher $\varphi(x)|d$ und, wegen $d|\psi(y)$, schlußendlich $\varphi(x)|\psi(y)$, wie gefordert.

□

Beweis des Elementarteilersatzes. Wir führen zwei Induktionsbeweise: Im ersten wird gezeigt, dass M frei ist. Die Induktion erfolgt über $n = \operatorname{rang}(M)$. Für $n = 0$ ist nichts zu zeigen, denn M ist als Untermodul eines freien Moduls (über einem Hauptidealring, insbesondere also über einem Integritätsring) torsionsfrei und daher impliziert $n = 0$, dass $M = 0$ ist. Sei also $n > 0$ beliebig und sei $x \in M$ entsprechend Lemma 3.52, Punkt 4., so gewählt, dass $\operatorname{cont}(x)|\operatorname{cont}(y)$ für alle $y \in M$ gilt. Sei weiterhin (Lemma 3.52, Punkt 2.) $\varphi \in F^*$ mit $\operatorname{cont}(x) = \varphi(x)$. Dann gibt es ein eindeutig bestimmtes $x_1 \in F$ mit $x = \varphi(x) \cdot x_1$ (z.B. kann man, wenn $z_1, \ldots, z_r$ irgendeine Basis von F mit $x = \sum_{i=1}^r \lambda_i z_i$ und $\operatorname{cont}(x) = \operatorname{ggT}(\lambda_1, \ldots, \lambda_r)$ ist, einfach $x_1 = \sum_{i=1}^r \frac{\lambda_i}{\operatorname{cont(x)}} z_i$ setzen, und man sieht leicht, dass dann x_1 nicht von der Wahl der Basis abhängt, weil schon $\operatorname{cont}(x)$ nicht von der Wahl einer Basis abhängt). Setze $F' := \ker(\varphi)$, dann ist $F = R \cdot x_1 \oplus F'$: Für alle $y \in F$ schreiben wir

$$y = \varphi(y) \cdot x_1 + (y - \varphi(y) \cdot x_1),$$

dann ist wegen $\varphi(x_1) = 1$ der zweite Term ein Element von F', dies zeigt $F = Rx_1 + F'$ und andererseits ist $\varphi(x_1) = 1 \neq 0$, also ist $Rx_1 \cap F' = 0$. Wir setzen weiter $M' := M \cap F'$, dann zeigt man analog, dass $M = Rx \oplus M'$ gilt: Schreibe für $y \in M$

$$y = \frac{\varphi(y)}{\varphi(x)} \cdot x + \left(y - \frac{\varphi(y)}{\varphi(x)} \cdot x \right),$$

dann ist der erste Term wegen $\varphi(x)|\varphi(y)$ (siehe Lemma 3.52) in Rx, und der zweite liegt sowohl in F' als auch in M, also in M'. Somit haben wir $M = Rx + M'$. Da $\varphi(x) \neq 0$ gilt (wegen $M \neq 0$), folgt auch hier $M' \cap Rx = 0$, und die Summe ist direkt, d.h., $M = Rx \oplus M'$. Wegen $x \neq 0$ ist notwendig $\operatorname{rang}(M') < n$, und damit muss M unter Anwendung der Induktionsannahme frei sein.
Im zweiten Induktionsbeweis wollen wir die Basis $a_1 \cdot x_1, \ldots, a_n \cdot x_n$ von M konstruieren. Wir führen den Beweis zunächst genauso wie eben, bis wir die Zerlegungen

$$F = Rx_1 \oplus F' \quad \text{sowie} \quad M = Rx \oplus M'$$

gewonnen haben. Jetzt ist F' als Untermodul von F frei (wie eben bewiesen), und wir können die Induktionsannahme auf den Untermodul M' des freien R-Moduls F anwenden. Wir haben dann $x_2, \ldots, x_n \in F'$, welche zu einer Basis von F' ergänzt werden können, sowie Elemente $a_2, \ldots, a_n \in R$, so dass $a_2 \cdot x_2, \ldots, a_n \cdot x_n$ eine Basis von M' ist (und so dass $a_i | a_{i+1}$ für $i \in \{2, \ldots, n-1\}$ gilt). Setze $a_1 := \varphi(x)$, dann ist $a_1 \cdot x_1, a_2 \cdot x_2, \ldots, a_n \cdot x_n$ eine Basis von M, und wir müssen $a_1 | a_2$ zeigen. Sei $\varphi_2 \in F^*$ mit $\varphi_2(x_2) = 1$, dann folgt wieder aus dem Beweis zum Punkt 4. des letzten Lemmas, dass $\varphi(x) | \varphi_2(a_2 \cdot x_2)$ gilt, also $a_1 | a_2$.
Als nächstes zeigen wir die Eindeutigkeit des Moduls $\oplus_{i=1}^n Rx_i$, genauer, die Aussage $M_{\text{sat}} = \oplus_{i=1}^n Rx_i$: Klar ist, dass $M \subset M_{\text{sat}}$ gilt. Da $a_i | a_n$ für alle $i \in \{1, \ldots, n\}$ ist, haben wir $a_n (\oplus_{i=1}^n Rx_i) \subset M$, also $\oplus_{i=1}^n Rx_i \subset M_{\text{sat}}$. Sei nun $y \in M_{\text{sat}}$ gegeben, d.h., es gibt $a \in R \backslash \{0\}$ mit $a \cdot y \in M$. Wähle eine Ergänzung $x_{n+1}, \ldots, x_r$ zu einer Basis $x_1, \ldots, x_r$ von F, und schreibe $y = \sum_{i=1}^r \lambda_i \cdot x_i$, dann gilt wegen $a \cdot y \in M$, dass $a \cdot \lambda_i = 0$ für alle $i \in \{n+1, \ldots, r\}$ ist. Dies impliziert (da R ein Integritätsring ist), dass $\lambda_i = 0$ für alle $i \in \{n+1, \ldots, r\}$ ist, und wir erhalten $y \in \oplus_{i=1}^n Rx_i$, also $M_{\text{sat}} = \oplus_{i=1}^n Rx_i$. Um die Gleichung (3.4) zu zeigen, betrachten wir für alle $i \in \{1, \ldots, n\}$ den Isomorphismus von R-Moduln $R \to R \cdot x_i$, welcher R (gesehen als R-Modul vom Rang 1 über sich selbst) auf den von x_i erzeugten R-Untermodul von M abbildet. Das Ideal (a_i) wird unter diesem Isomorphismus auf den R-Untermodul $(a_i) \cdot x_i$ von $R \cdot x_i$ abgebildet und wir haben $(R \cdot x_i)/((a_i) \cdot x_i) \cong R/(a_i)$. Damit ergibt sich der Isomorphismus

$$\frac{M_{\text{sat}}}{M} = \frac{\oplus_{i=1}^n Rx_i}{M} = \bigoplus_{i=1}^n \frac{R \cdot x_i}{(a_i) \cdot x_i} = \bigoplus_{i=1}^n \frac{R}{(a_i)}$$

Schlußendlich ist noch die Eindeutigkeit der Elemente $a_1, \ldots, a_n$ zu zeigen. Seien also für den gegebenen Modul M Elementarteiler $a_1, \ldots, a_n$ und $b_1, \ldots, b_n$ mit $a_i | a_{i+1}$ und $b_i | b_{i+1}$ für $i \in \{1, \ldots, n-1\}$ gegeben. Die eben bewiesene Aussage liefert

$$\bigoplus_{i=1}^n \frac{R}{(a_i)} \cong \bigoplus_{j=1}^n \frac{R}{(b_j)}$$

In dieser Gleichung können wir alle Summanden, bei denen a_i oder b_j Einheiten sind, vernachlässigen, denn dann ist der entsprechende Quotient gleich Null. Das Lemma 3.50 liefert nun, dass die Nicht-Einheiten unter den a_i und b_i paarweise assoziiert sind, und alle anderen Elemente sind Einheiten und per Definition (paarweise) assoziiert. Dies liefert die gewünschte Eindeutigkeitsaussage. □

Bevor wir den schon erwähnten Klassifizierungssatz formulieren und beweisen, wollen wir zunächst ein praktisches Verfahren zur Bestimmung der Elementarteiler kennenlernen. Hierbei beschränken wir uns auf den Fall, dass R ein euklidischer Ring ist (wegen Satz 3.27 ist er dann auch ein Hauptidealring), dies umfasst insbesondere den wichtigen Fall $R = \mathbb{Z}$.

Satz 3.53. *Sei R ein euklidischer Ring mit Gradfunktion $\omega : R\backslash\{0\} \to \mathbb{N}$. Sei $A \in \mathrm{Mat}(t \times s, R)$ gegeben, dann existieren eindeutig (bis auf Einheiten) bestimmte $a_1, \ldots, a_n \in R\backslash\{0\}$ mit $a_i | a_{i+1}$ für $i \in \{1, \ldots, n-1\}$ sowie (nicht eindeutig bestimmte) Matrizen $B \in \mathrm{Gl}(t, R)$, $C \in \mathrm{Gl}(s, R)$ so dass*

$$B \cdot A \cdot C := \begin{pmatrix} a_1 & & & & & 0 & 0 \\ & \ddots & & & & \vdots & 0 \\ & & \ddots & & & \vdots & \vdots \\ & & & \ddots & & \vdots & \vdots \\ & & & & \ddots & 0 & 0 \\ 0 & \cdots & \cdots & \cdots & 0 & a_n & \cdots \\ 0 & 0 & \cdots & 0 & 0 & \vdots & 0_{t-n,s-n} \end{pmatrix}$$

gilt.

Beweis. Die abstrakte Existenz der Matrizen B und C folgt aus dem Elementarteilersatz (Übung), aber hier wollen wir einen konstruktiven Beweis geben. Wir bemerken nur, dass die Elementarteiler des Moduls $\mathrm{Im}(\varphi)$, wobei $\varphi : R^s \to R^t$ die durch Linksmultiplikation mit der Matrix A gegebene Abbildung ist, genau die Elemente $a_1, \ldots, a_n$ sind.
Wir führen an der Matrix A Zeilen- bzw. Spaltenumformungen durch, welche durch Links- bzw. Rechtsmultiplikation mit sogenannten Elementarmartrizen gegeben werden. Diese sind (für den Fall der Spaltenumformungen):

1. Vertauschen der i-ten und der j-ten Spalte. Dies wird durch Rechtsmultiplikation mit der Elementarmatrix
$$\begin{pmatrix} 1 & & & & & & & & \\ & \ddots & & & & & & & \\ & & 1 & & & & & & \\ & & & 0 & \cdots & \cdots & \cdots & 1 & & & \\ & & & \vdots & 1 & & & \vdots & & & i \\ & & & \vdots & & \ddots & & \vdots & & & \\ & & & \vdots & & & 1 & \vdots & & & j \\ & & & 1 & \cdots & \cdots & \cdots & 0 & & & \\ & & & & & & & & 1 & & \\ & & & & & & & & & \ddots & \\ & & & & & & & & & & 1 \end{pmatrix}$$
erreicht.
2. $\lambda \in R$, Addieren des λ-fachen der j-ten Spalte zur i-ten Spalte. Dies ist durch Rechtsmultiplikation

mit der folgenden Elementarmatrix zu erreichen.

$$\begin{pmatrix} 1 & & & & & & & & & & \\ & \ddots & & & & & & & & & \\ & & 1 & & & & & & & & \\ & & & 1 & & & & & & & \\ & & & \vdots & 1 & & & & & & \\ & & & \vdots & & \ddots & & & & & \\ & & & \vdots & & & 1 & & & & \\ & & & \lambda & \dots & \dots & \dots & 1 & & & \\ & & & & & & & & 1 & & \\ & & & & & & & & & \ddots & \\ & & & & & & & & & & 1 \end{pmatrix} \begin{matrix} \\ \\ \\ \\ i \\ \\ \\ \\ j \\ \\ \\ \end{matrix}$$

3. Für alle $\lambda \in R^*$: i-te Spalte mit λ multiplizieren.

$$\begin{pmatrix} 1 & & & & & & \\ & \ddots & & & & & \\ & & 1 & & & & \\ & & & \lambda & & & \\ & & & & 1 & & \\ & & & & & \ddots & \\ & & & & & & 1 \end{pmatrix} \begin{matrix} \\ \\ \\ \\ i \\ \\ \\ \end{matrix}$$

Alle diese Matrizen liegen in $\mathrm{Gl}(s, R)$, ihr Produkt liefert die oben gesuchte Matrix C, analog geben die Zeilenumformungen die Matrix $B \in \mathrm{Gl}(t, R)$.
Nun zur Beschreibung des Elementarteileralgorithmus.

(1. Schritt) Mit Spaltenumformungen wird die Zahl $\alpha_{11} := \mathrm{ggT}(a_{11}, a_{12}, \dots, a_{1s})$ an die Position $(1,1)$ gebracht und Nullen an der Position $(1, j)$ für $j > 1$ erzeugt

$$\left(\begin{array}{c|ccc} \alpha_{11} & 0 & \dots & 0 \\ \hline * & & & \\ \vdots & & * & \\ * & & & \end{array}\right)$$

(2. Schritt) Analog mit Zeilenumformungen für die erste Zeile

$$\left(\begin{array}{c|ccc} \widetilde{\alpha}_{11} & * & \dots & * \\ \hline 0 & & & \\ \vdots & & * & \\ 0 & & & \end{array}\right)$$

Hierbei ist $\omega(\widetilde{\alpha}_{11}) \leq \omega(\alpha_{11})$, falls $\omega(\widetilde{\alpha}_{11}) = \omega(\alpha_{11})$, dann sind $\widetilde{\alpha}_{11}$ und α_{11} assoziiert, und wir erhalten die Matrix

$$\left(\begin{array}{c|ccc} \widetilde{\alpha}_{11} & 0 & \dots & 0 \\ \hline 0 & & & \\ \vdots & & * & \\ 0 & & & \end{array}\right) =: \widetilde{A}.$$

Dann machen wir direkt mit dem 4. Schritt weiter.

(3. Schritt) Abwechselnd ersten und zweiten Schritt wiederholen. Nach endlich vielen Schritten muss $\omega(\widetilde{\alpha}_{11}) = \omega(\alpha_{11})$ gelten, und wir haben

$$\left(\begin{array}{c|ccc} \widetilde{\alpha}_{11} & 0 & \dots & 0 \\ \hline 0 & & & \\ \vdots & & * & \\ 0 & & & \end{array}\right) =: \widetilde{A}$$

(4. Schritt) Hier unterscheidet man 2 Fälle.

(1. Fall) $\widetilde{\alpha}_{11}$ teilt nicht alle Einträge von $\widetilde{A}$. Dann addiert man eine Zeile, deren Einträge nicht alle von $\widetilde{a}_{11}$ geteilt werden, zur ersten Zeile von $\widetilde{A}$. Danach beginnt man wieder mit dem ersten Schritt. Nach endlich vielen Schritten erreicht man den 2. Fall.

(2. Fall) $\widetilde{a}_{11}$ teilt alle Einträge von $\widetilde{A}$. Setze dann $a_1 := \widetilde{a}_{11}$. Ab nun betrachtet man die $(t-1)\times(s-1)$ Matrix A', so dass:

$$\widetilde{A} = \left(\begin{array}{c|c} a_1 & 0_{1,s-1} \\ \hline 0_{t-1,1} & A' \end{array}\right)$$

und beginnt wieder mit dem ersten Schritt mit der Matrix A'

Nach endlich vielen Schritten hat man erreicht, dass

$$B \cdot A \cdot C = \left(\begin{array}{ccc|c} a_1 & & & 0 \\ & \ddots & & \vdots \\ & & a_n & 0 \\ \hline 0 & \dots & 0 & 0_{t-n,s-n} \end{array}\right)$$

mit $a_i | a_{i+1}$, $B \in \mathrm{Gl}(t, R)$ und $C \in \mathrm{Gl}(s, R)$.

□

Zur Illustration dienen die folgenden Beispiele.

1.
$$\begin{pmatrix} 2 & 6 & 8 \\ 3 & 1 & 2 \\ 9 & 5 & 4 \end{pmatrix} \xrightarrow{Sp.} \begin{pmatrix} 6 & 2 & 8 \\ 1 & 3 & 2 \\ 5 & 9 & 4 \end{pmatrix} \xrightarrow{Z.} \begin{pmatrix} 1 & 3 & 2 \\ 6 & 2 & 8 \\ 5 & 9 & 4 \end{pmatrix} \xrightarrow{Z.}$$
$$\begin{pmatrix} 1 & 3 & 2 \\ 0 & -16 & -4 \\ 0 & -6 & -6 \end{pmatrix} \xrightarrow{Sp.} \begin{pmatrix} 1 & 0 & 0 \\ 0 & 2 & 14 \\ 0 & -6 & -6 \end{pmatrix} \xrightarrow{Z.} \begin{pmatrix} 1 & 0 & 0 \\ 0 & 2 & 14 \\ 0 & 0 & 36 \end{pmatrix} \xrightarrow{Sp.}$$
$$\begin{pmatrix} 1 & 0 & 0 \\ 0 & 2 & 0 \\ 0 & 0 & 36 \end{pmatrix}$$

Die Elementarteiler sind in diesem Beispiel also die Zahlen 1, 2 und 36.

2.
$$\begin{pmatrix} 12 & 6 \\ 4 & 2 \end{pmatrix} \xrightarrow{Z.} \begin{pmatrix} 0 & 0 \\ 4 & 2 \end{pmatrix} \xrightarrow{Z.,Sp.} \begin{pmatrix} 2 & 0 \\ 0 & 0 \end{pmatrix}$$

Hier hat man nur den Elementarteiler 2.

3.

$$\begin{pmatrix} 4 & 6 \\ 6 & 8 \end{pmatrix} \xrightarrow{Sp.} \begin{pmatrix} 4 & 2 \\ 6 & 2 \end{pmatrix} \xrightarrow{Sp.} \begin{pmatrix} 0 & 2 \\ 2 & 2 \end{pmatrix} \xrightarrow{Z.}$$

$$\begin{pmatrix} 0 & 2 \\ 2 & 0 \end{pmatrix} \xrightarrow{Z./Sp.} \begin{pmatrix} 2 & 0 \\ 0 & 2 \end{pmatrix}$$

In diesem Beispiel tritt die Zahl 2 zweimal als Elementarteiler auf.

Als Anwendung des Elementarteilersatzes erhalten wir das oben schon erwähnte Klassifikationsresultat.

Satz 3.54. *Sei R ein Hauptidealring, und N ein endlich erzeugter R-Modul. Dann existieren bis auf Einheiten eindeutig bestimmte Elemente $a_1, \ldots, a_n \in R$ mit $a_i | a_{i+1}$ für alle $i \in \{1, \ldots, n-1\}$ sowie ein Modulisomorphismus*

$$N \cong R^l \bigoplus \left(\bigoplus_{i=1}^{n} \frac{R}{(a_i)} \right)$$

Es ist $\mathrm{Tor}(N) = \bigoplus_{i=1}^{n} \frac{R}{(a_i)}$ *und* $\mathrm{rang}(N) = l$.

Beweis. Sei $z_1, \ldots, z_k$ ein Erzeugendensystem von N. Dann definiert

$$\begin{array}{rcl} \varphi : R^k & \longrightarrow & N \\ (b_1, \ldots, b_k) & \longmapsto & \sum_{i=1}^{k} b_i \cdot z_i \end{array}$$

einen surjektiven Modulhomomorphismus, d.h., es gilt nach dem Homomorphiesatz für Moduln, dass $N \cong R^k / \ker(\varphi)$. Wir wenden jetzt den Elementarteilersatz (Satz 3.51) auf den Untermodul $M := \ker(\varphi)$ des freien Moduls R^k an. Es gibt also eine Basis $x_1, \ldots, x_k$ von R^k, sowie Elementarteiler $a_1, \ldots, a_n \in R$ $(n \leq k)$ mit $a_i | a_{i+1}$, so dass $a_1 \cdot x_1, \ldots, a_n \cdot x_n$ eine Basis von $\ker(\varphi)$ bilden. Wir haben also

$$N \cong \frac{R^k}{\oplus_{i=1}^{n} R(a_i \cdot x_i)} \cong \frac{\oplus_{i=1}^{k} R x_i}{\oplus_{i=1}^{n} R(a_i \cdot x_i)} \cong \frac{\oplus_{i=1}^{n} R x_i}{\oplus_{i=1}^{n} R(a_i \cdot x_i)} \oplus R^{n-k} \cong \bigoplus_{i=1}^{n} \frac{R}{(a_i)} \oplus R^{n-k}$$

und offensichtlich ist $\bigoplus_{i=1}^{n} \frac{R}{(a_i)}$ gerade der Torsionsuntermodul $\mathrm{Tor}(N)$ und daher $\mathrm{rang}(N) = k - n =: l$. $\square$

Wir haben im Lemma 3.47 gesehen, dass abelsche Gruppen nichts anderes als $\mathbb{Z}$-Moduln sind. Daher gibt der letzte Satz insbesondere eine Klassifikation von endlich erzeugten abelschen Gruppen. Insbesondere liefert dieser Satz also die Aussage, dass eine endliche abelsche Gruppe immer isomorph zu einem Produkt von zyklischen Gruppen der Form $\mathbb{Z}/a_1\mathbb{Z} \times \ldots \times \mathbb{Z}/a_n\mathbb{Z}$ mit $a_i | a_{i+1}$ ist, dies hatten wir in Kapitel 2 gelegentlich schon verwendet.

Kapitel 4

Körpererweiterungen

In diesem und dem nächsten Kapitel werden wir eine der zentralen Konstruktionen dieser Vorlesung genau studieren, nämlich Körpererweiterungen. Wie im einleitenden Kapitel 1 bereits angedeutet, ist dies das entscheidende Hilfsmittel zur Lösung der aus der Antike stammenden Konstruktionsprobleme und der Frage nach der Auflösbarkeit algebraischer Gleichungen.

4.1 Endliche und algebraische Körpererweiterungen

In diesem Abschnitt behandeln wir die Grundbegriffe der Körpertheorie. Insbesondere lernen wir endliche und algebraische Körpererweiterungen kennen, und konstruieren den sogenannten algebraischen Abschluss eines Körpers.
Wir wiederholen zunächst eine aus den Übungen bekannte Invariante eines Körpers, oder allgemeiner eines Integritätsringes, nämlich seine Charakteristik.

Definition 4.1. *Sei R ein Integritätsring, und $\varphi : \mathbb{Z} \to R$ gegeben durch*

$$\varphi(n) := n \cdot 1_R := \begin{cases} \underbrace{1_R + \ldots + 1_R}_{n\text{-mal}} & \text{falls} \quad n > 0 \\ 0 & \text{falls} \quad n = 0 \\ \underbrace{-1_R - \ldots - 1_R}_{-n\text{-mal}} & \text{falls} \quad n < 0 \end{cases}$$

Dann ist φ ein Ringhomomorphismus, und $\ker(\varphi) = (p)$ für eine Zahl $p \in \mathbb{N}$, genannt die Charakteristik von R, geschrieben $\operatorname{char}(R)$. Wegen des Homomorphiesatzes ist $\mathbb{Z}/\ker(\varphi)$ zu einem Unterring von R (nämlich zu $\operatorname{Im}(\varphi)$) isomorph und daher auch ein Integritätsring, also ist $p = 0$ oder $\mathbb{Z}/(p)$ ist wegen Satz 3.21 ein Körper, und daher ist p eine Primzahl.

Wir diskutieren die Charakteristiken von einigen Beispielen.

1. Die Charakteristik der Körper $\mathbb{Q}$, $\mathbb{R}$ und $\mathbb{C}$ ist gleich 0, denn $n \cdot 1$ ist für $n \neq 0$ niemals gleich 0 in diesen Körpern.

2. Der Körper $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$ hat die Charakteristik p (für p Primzahl).

3. Sei $R = \mathbb{F}_p[x]$ und $f \in R$ ein irreduzibles Polynom. Dann ist $L := R/(f)$ ein Körper (siehe die Bemerkung nach Lemma 3.30), und es gilt $\operatorname{char}(L) = p$. Wir werden später alle endlichen Körper klassifizieren, und es stellt sich heraus, dass diese alle aus den Körpern $\mathbb{F}_p$ als Quotienten von R konstruiert werden können.

Wir wenden uns nun dem Studium von Körpererweiterungen zu. Wie schon mehrfach erwähnt (siehe z.B. die Definition 3.8) nennt man eine Inklusion $K \subset L$ von zwei Körpern eine Körpererweiterung, wenn K ein Unterkörper von L ist. Manchmal sagt man auch, dass L Oberkörper von K ist, und man schreibt $L \supset K$ oder L/K. Häufig hat man auch eine Inklusion dreier Körper $K \subset E \subset L$, und dann sagt man, dass E ein Zwischenkörper der Körpererweiterung $K \subset L$ ist. Wir definieren nun eine wichtige Invariante einer solchen Erweiterung.

Definition 4.2. *Sei $L \supset K$ eine Körpererweiterung, dann schränkt sich die Multiplikation auf L zu einer Skalarmultiplikation*

$$K \times L \longrightarrow L$$

ein, und dann ist L in natürlicher Weise ein K-Vektorraum. Wir nennen $[L : K] := \dim_K(L) \in \mathbb{N}_{>0} \cup \{\infty\}$ den Grad der Körpererweiterung $L \supset K$. Die Körpererweiterung $L \supset K$ heißt endlich, falls $[L : K] < \infty$ ist, ansonsten heißt sie unendlich. Es gilt: $[L : K] = 1 \iff L = K$ (leicht, Übung).

Ein wichtiges Hilfsmittel zum Bestimmen des Grades von Körpererweiterungen ist der sogenannte Gradsatz.

Satz 4.3. *Seien $K \subset E \subset L$ Körpererweiterungen. Dann gilt*

$$[L : K] = [L : E] \cdot [E : K],$$

falls alle drei Grade endlich sind. $[L : K]$ ist unendlich genau dann, wenn einer der beiden Grade $[L : E]$ oder $[E : K]$ unendlich ist.

Beweis. Angenommen, alle drei Grade seien endlich. Wähle eine K-Basis $x_1, \ldots, x_n$ von E und eine E-Basis $y_1, \ldots, y_m$ von L. Wir behaupten, dass dann $(x_i \cdot y_j)_{i \in \{1,\ldots,n\}, j \in \{1,\ldots,m\}}$ eine K-Basis von L ist. Sei $z \in L$, dann existiert eine (eindeutig bestimmte) Darstellung $z = \sum_{j=1}^{m} \mu_j \cdot y_j$ mit $\mu_j \in E$. Für jedes $j \in \{1, \ldots, m\}$ gibt es wiederum eine (ebenfalls eindeutige) Darstellung $\mu_j = \sum_{i=1}^{n} \lambda_{ij} \cdot x_i$ mit $\lambda_{ij} \in K$, also haben wir

$$z = \sum_{i \in \{1,\ldots,n\}, j \in \{1,\ldots,m\}} \lambda_{ij} \cdot (x_i \cdot y_j),$$

also ist die Menge $(x_i \cdot y_j)$ ein K-Erzeugendensystem von L. Die lineare Unabhängigkeit folgt eigentlich schon aus der oben erwähnten Eindeutigkeit, aber man kann sie auch noch einmal explizit zeigen: Sei

$$\sum_{i \in \{1,\ldots,n\}, j \in \{1,\ldots,m\}} \lambda_{ij}(x_i \cdot y_j) = 0,$$

dann ist

$$0 = \sum_{j=1}^{m} \left(\sum_{i=1}^{n} \lambda_{ij} \cdot x_i \right) \cdot y_j,$$

und weil (y_j) eine E-Basis von L, also insbesondere linear unabhängig ist, folgt $\sum_{i=1}^{n} \lambda_{ij} \cdot x_i = 0$ für alle $j \in \{1, \ldots, m\}$. Weil aber auch (x_i) eine K-Basis von E, also auch linear unabhängig sind, impliziert dies $\lambda_{ij} = 0$ für alle i, j, und damit ist die Familie $(x_i \cdot y_j)$ linear unabhängig über K und also eine K-Basis von L.
Betrachte nun beliebige Elemente $x_1, \ldots, x_n \in E$ und $y_1, \ldots, y_m \in L$. Falls $(x_1, \ldots, x_m)$ über K linear unabhängig sind und falls $(y_1, \ldots, y_m)$ über E linear unabhängig sind, dann sind, wie eben gesehen, $(x_i \cdot y_j)$ über K linear unabhängig. Dies bedeutet, dass aus $[E : K] \geq n$ und $[L : E] \geq m$ stets $[L : K] \geq m \cdot n$ folgt, ist also $[E : K] = \infty$ oder $[L : E] = \infty$, dann haben wir $[L : K] = \infty$. □

Wir betrachten die folgenden Beispiele für Grade von Körpererweiterungen:

1. $\mathbb{C}$ ist eine endliche Körpererweiterung von $\mathbb{R}$, mit $[\mathbb{C} : \mathbb{R}] = 2$, z.B. ist $1, i$ eine $\mathbb{R}$-Basis von $\mathbb{C}$.
2. Es ist $[\mathbb{R} : \mathbb{Q}] = \infty$, siehe Korollar 4.7 unten.

3. Sei K ein beliebiger Körper, dann ist $K \subset Q(K[x])$ eine Körpererweiterung, und es gilt $[Q(K[x]) : K] = \infty$ (denn falls $[Q(K[x]) : K] < \infty$, dann wäre auch der K-Vektorraum $K[x]$ über K endlichdimensional, was nicht der Fall ist).

4. Eine leichte Konsequenz des Gradsatzes ist, dass eine endliche Körpererweiterung $[L : K]$, deren Grad eine Primzahl ist, keinen echten Zwischenkörper enthalten kann.

Wir behandeln einen zweiten fundamentalen Begriff für Körpererweiterungen.

Definition 4.4. *Sei $L \supset K$ eine Körpererweiterung. Ein Element $\alpha \in L$ heißt* algebraisch *über K, falls es ein unitäres Polynom $f \in K[x]$ gibt, so dass $f(\alpha) = 0$ ist. Mit anderen Worten, es existieren Koeffizienten $a_0, a_1, \ldots, a_{n-1} \in K$, so dass α die Gleichung*

$$\alpha^n + a_{n-1} \cdot \alpha^{n-1} + \ldots + a_1 \cdot \alpha + a_0 = 0$$

erfüllt. Eine dritte äquivalente Formulierung benutzt den Einsetzungshomomorphismus (siehe Lemma 3.11)

$$K[x] \to L, g \mapsto g(\alpha)$$

α ist algebraisch genau dann, wenn dieser Homomorphismus nicht injektiv ist.
Falls α nicht algebraisch über K ist, dann heißt α transzendent *über K. Die Körpererweiterung $L \supset K$ heißt algebraisch, wenn alle $\alpha \in L$ algebraisch über K sind.*

Ein wichtiger Begriff im Zusammenhang mit algebraischen Körpererweiterungen ist der des Minimalpolynoms.

Lemma 4.5. *Sei $L \supset K$ eine Körpererweiterung und $\alpha \in L$ algebraisch über K. Dann existiert ein eindeutig bestimmtes unitäres Polynom kleinsten Grades $f \in K[x]$, genannt Minimalpolynom von α, welches $f(\alpha) = 0$ erfüllt. Wir schreiben zur Abkürzung oft $f = \mathrm{MinPol}_K(\alpha)$. f ist irreduzibel in $K[x]$.*

Beweis. Betrachte erneut den Einsetzungshomomorphismus $\varphi : K[x] \to L$, $g \mapsto g(\alpha)$. Nach Voraussetzung ist $\ker(\varphi) \neq 0$, also ist $\ker(\varphi)$ ein Hauptideal, da $K[x]$ ein Hauptidealring ist. Es gibt einen eindeutig bestimmten unitären Erzeuger $f = \mathrm{MinPol}_K(\alpha)$ von $\ker(\varphi)$, und da $K[x]/(f)$ ein Unterring von L, insbesondere also ein Integritätsring ist, muss f prim, also irreduzibel sein. □

Wir können die Aussage des letzten Lemmas noch präzisieren.

Lemma 4.6. *Sei $L \supset K$ eine Körpererweiterung, und $\alpha \in L$ ein über K algebraisches Element mit Minimalpolynom $f = \mathrm{MinPol}_K(\alpha) \in K[x]$. Sei $K[\alpha]$ das Bild des Einsetzungshomomorphismus $K[x] \to L$ gegeben durch $g \mapsto g(\alpha)$, dann ist $K[\alpha] \supset K$ eine endliche Körpererweiterung vom Grad $\deg(f)$. Wir schreiben für $K[\alpha]$ auch $K(\alpha)$ (dies ist ein Spezialfall einer allgemeineren Notation, siehe Definition 4.9 weiter unten).*

Beweis. Das Ideal (f) (der Kern des Einsetzungshomomorphismus), ist, wie im ein letzten Lemma gezeigt, ein Primideal. Aber dann ist $(f) \subset K[x]$ nach Lemma 3.30 sogar ein maximales Ideal, und daher ist $\mathrm{Im}(\varphi) \cong K[x]/(f)$ ein Körper.
Zur Berechnung des Grades der Körpererweiterung $K[\alpha] \supset K$ nehmen wir $\deg(f) = n$ an, d.h., $f = x^n + a_{n-1} \cdot x^{n-1} + \ldots + a_0$ mit $a_i \in K$. Dann behaupten wir, dass die Restklassen $1, [x], \ldots, [x^{n-1}]$ eine K-Basis von $K[x]/(f)$ bilden. Sei eine beliebige Restklasse $[g] \in K[x]/(f)$ gegeben, dann wird diese repräsentiert von $g \in K[x]$ und dann liefert Division mit Rest $g = q \cdot f + r$ mit $\deg(r) < n$ und so dass $[g] = [r]$ ist. Dann liegt aber $[r]$ im von $1, [x], \ldots, [x^{n-1}]$ erzeugten K-Untervektorraum von $K[x]/(f)$, also bilden diese Klassen ein Erzeugendensystem von $K[x]/(f)$.
Es bleibt zu zeigen, dass diese Elemente über K linear unabhängig sind. Angenommen, wir hätten eine Relation $\sum_{i=0}^{n-1} \lambda_i [x^i] = 0$ mit $\lambda_i \in K$ gegeben, dann folgt $\sum_{i=0}^{n-1} \lambda_i x^i \in (f)$, d.h., f ist ein Teiler des Polynoms $\sum_{i=0}^{n-1} \lambda_i x^i$. Wegen $\deg(f) = n$ kann dann nur $a_i = 0$ für $i \in \{0, \ldots, n-1\}$ gelten.
Man beachte, dass die durch den Einsetzungshomomorphismus induzierte Abbildung $K[x]/(f) \xrightarrow{\cong} K[\alpha]$ das Monom $[x^i]$ auf das Element $[\alpha^i]$ abbildet, d.h., $[1], [\alpha], \ldots, [\alpha^{n-1}]$ ist eine K-Basis von $K[\alpha]$.

□

Als Anwendung haben wir die folgende Aussage.

Korollar 4.7. *Es ist* $[\mathbb{R} : \mathbb{Q}] = \infty$.

Beweis. Sei p eine Primzahl und $n \in \mathbb{N}$. Dann ist die Zahl $\sqrt[n]{p} \in \mathbb{R}$ algebraisch über $\mathbb{Q}$, denn sie ist Nullstelle von $f = x^n - p \in \mathbb{Q}[x]$. Das Eisensteinsche Irreduzibilitätskriterium (Satz 3.45) liefert, dass f irreduzibel in $\mathbb{Q}[x]$ ist, und natürlich ist f unitär. Also haben wir $f = \mathrm{MinPol}_{\mathbb{Q}}(\sqrt[n]{p})$, und daher ist wegen des letzten Lemmas $[\mathbb{Q}(\sqrt[n]{p}) : \mathbb{Q}] = n$. Da alle Zahlen $\sqrt[n]{p}$ in $\mathbb{R}$ liegen (und daher $[\mathbb{R} : \mathbb{Q}] \geq [\mathbb{Q}(\sqrt[n]{p}) : \mathbb{Q}] = n$ für alle $n \in \mathbb{N}$ gilt), kann $\mathbb{R}$ nicht endlich über $\mathbb{Q}$ sein. □

Wir wollen als nächstes die Beziehung zwischen endlichen und algebraischen Körpererweiterungen untersuchen.

Satz 4.8. *Sei $L \supset K$ eine endliche Körpererweiterung. Dann ist L algebraisch über K.*

Beweis. Wir haben zu zeigen, dass alle Elemente $\alpha \in L$ algebraisch über K sind. Da $[L : K] = n < \infty$ ist, sind die $n + 1$ Elemente $1, \alpha, \alpha^2, \ldots, \alpha^n$ linear abhängig, d.h., es gibt $\lambda_0, \lambda_1, \ldots, \lambda_n \in K$, welche nicht alle gleich 0 sind, mit

$$\lambda_n \cdot \alpha^n + \ldots + \lambda_0 = 0$$

Sei $k = \max\{i \in \{0, \ldots, n\} \mid \lambda_i \neq 0\}$, dann können wir diese diese Gleichung durch λ_k dividieren. Wir erhalten

$$\alpha^k + \frac{\lambda_{k-1}}{\lambda_k}\alpha^{k-1} + \ldots + \frac{\lambda_0}{\lambda_k} = 0$$

und entsprechend Definition 4.4 ist α damit algebraisch über K. □

Im allgemeinen ist eine algebraische Körpererweiterung nicht endlich. Um dies besser verstehen zu können, brauchen wir eine neue Bezeichnung.

Definition 4.9. *Sei $L \supset K$ eine Körpererweiterung*

1. *Sei $S \subset L$ eine Teilmenge, setze*

$$K(S) := \bigcap_{\substack{\text{Zwischenkörper } K \subset E \subset L \\ S \subset E}} E.$$

   Dann ist $K(S)$ ein Körper, genauer, ein Zwischenkörper von $K \subset L$ (leicht, Übung). $K(S)$ ist der kleinste Unterkörper von L, welcher K und S enthält (auch leicht, Übung).

2. *L heißt endlich erzeugt über K, falls S eine endliche Menge und $L = K(S)$ ist.*

3. *$L \supset K$ heißt eine einfache Körpererweiterung, falls $L = K(S)$ mit $|S| = 1$, d.h., falls es ein $\alpha \in L$ gibt mit $L = K(\alpha)$.*

Wir haben weiter oben für ein algebraisches Element $\alpha \in L$ den Zwischenkörper $K[\alpha]$ eingeführt und diesen auch mit $K(\alpha)$ bezeichnet. Man prüft leicht nach, dass $K[\alpha]$ tatsächlich der kleinste Erweiterungskörper von K ist, welcher α enthält, daher sind für den Fall $S = \{\alpha\}$ die beiden Definitionen konsistent.
Allgemeiner gilt: Ist $L \supset K$ endlich erzeugt, d.h. $L = K(\alpha_1, \ldots, \alpha_n)$ für Elemente $\alpha_1, \ldots, \alpha_n$, dann ist

$$Q(K[\alpha_1, \ldots, \alpha_n]) = L$$

wobei $K[\alpha_1, \ldots, \alpha_n]$ das Bild des Einsetzungshomomorphismus $K[x_1, \ldots, x_n] \to L$ bezeichnet. Um dies zu zeigen, überlegt man sich zuerst, dass notwendig $K[\alpha_1, \ldots, \alpha_n] \subset L$ gilt, denn die Elemente von $K[\alpha_1, \ldots, \alpha_n]$ sind nach Definition Polynome in $\alpha_1, \ldots, \alpha_n$, und alle diese müssen in L enthalten sein, da $\alpha_1, \ldots, \alpha_n$ in L enthalten und L ein Körper ist. Dann muss aber schon $Q(K[\alpha_1, \ldots, \alpha_n]) \subset L$ gelten, denn auch die

Quotienten zweier Elemente aus L (das zweite ungleich 0) müssen wieder in L enthalten sein. Nach Definition ist aber $L = K(\alpha_1, \ldots, \alpha_n)$ der kleinste Teilkörper von L der K und alle $\alpha_1, \ldots, \alpha_n$ enthält, dann folgt aber $Q(K[\alpha_1, \ldots, \alpha_n]) \supset L$, denn natürlich enthält $Q(K[\alpha_1, \ldots, \alpha_n])$ sowohl K als auch die Elemente $\alpha_1, \ldots, \alpha_n$. Wir können jetzt den Zusammenhang zwischen den verschiedenen Typen von Körpererweiterungen genauer charakterisieren.

Satz 4.10. *Sei $L \supset K$ eine Körpererweiterung, dann sind äquivalent:*

1. *$L \supset K$ ist eine endliche Körpererweiterung.*
2. *Es gibt algebraische Elemente $\alpha_1, \ldots, \alpha_n \in L$ mit $L = K(\alpha_1, \ldots, \alpha_n)$.*
3. *L ist endlich über K erzeugt und algebraisch.*

Beweis. **1. ⇒ 2.** Sei $[L : K] = n$ und sei $\alpha_1, \ldots, \alpha_n$ eine Basis von L als K-Vektorraum. Dann gilt natürlich $K(\alpha_1, \ldots, \alpha_n) \subset L$, aber da sich jedes Element aus L als Linearkombination (mit Koeffizienten aus K) von $\alpha_1, \ldots, \alpha_n$ darstellen lässt, ist natürlich insbesondere $L \subset K(\alpha_1, \ldots, \alpha_n)$. Wegen Satz 4.8 sind dann die Elemente $\alpha_1, \ldots, \alpha_n$ alle algebraisch über K.

2. ⇒ 1. Wir zeigen die folgende Aussage per Induktion über n:

Sei $L = K(\alpha_1, \ldots, \alpha_n)$ und α_i algebraisch für $i = 1, \ldots, n$, dann ist $L = K[\alpha_1, \ldots, \alpha_n]$ und $[L : K] < \infty$.

Der Fall $n = 1$ ist genau der Inhalt von Lemma 4.6 und der Bemerkung nach Definition 4.9. Sei also $L' := K[\alpha_1, \ldots, \alpha_{n-1}] = K(\alpha_1, \ldots, \alpha_{n-1})$ endlich über K. Da α_n algebraisch über K ist, ist es natürlich insbesondere algebraisch über L', und wir können wieder Lemma 4.6 anwenden, welches uns liefert, dass $L'[\alpha_n] = K[\alpha_1, \ldots, \alpha_n]$ eine endliche Körpererweiterung von L' ist. Insbesondere ist $K[\alpha_1, \ldots, \alpha_n] = K(\alpha_1, \ldots, \alpha_n)$ und wegen dem Gradsatz (Satz 4.3) ist dann auch $[L : K] < \infty$.

2. ⇒ 3. Wir haben gerade gesehen (in 2. ⇒ 1.), dass unter der Voraussetzung 2. die Erweiterung $L \supset K$ auch endlich ist. Dann ist sie wegen Satz 4.8 aber auch algebraisch.

3. ⇒ 2. L ist nach Voraussetzung endlich erzeugt. Wenn wir aber schon wissen, dass $L \supset K$ algebraisch ist, dann sind natürlich insbesondere die Erzeuger von L algebraische Elemente über K.

□

Im allgemeinen muss eine algebraische Körpererweiterung nicht endlich sein, falls sie nämlich von unendlich vielen algebraischen Elementen erzeugt wird. Genauer gilt der folgende Satz.

Satz 4.11. *Sei $L \supset K$ eine Körpererweiterung, dann sind äquivalent:*

1. *$L \supset K$ ist algebraisch.*
2. *$L = K(S)$ für eine Teilmenge $S \subset L$, so dass jedes $\alpha \in S$ algebraisch über K ist.*

Beweis. **1. ⇒ 2.** Dies ist offensichtlich, denn wir können einfach $S = L$ wählen.

2. ⇒ 1. Sei $T \subset S$ mit $|T| < \infty$. Dann ist nach Satz 4.10 die Erweiterung $K(T)$ algebraisch über K. Andererseits haben wir

$$L = K(S) \overset{!}{=} \bigcup_{T \subset S; |T| < \infty} K(T)$$

also ist auch L algebraisch über K.

□

Als Konsequenz erhalten wir, dass die Eigenschaft einer Körpererweiterung, algebraisch zu sein, sich transitiv bezüglich Zwischenkörpern verhält (für die Endlichkeit folgt dies aus dem Gradsatz 4.3).

Korollar 4.12. *Seien $K \subset E \subset L$ Körpererweiterungen, und sei $E \supset K$ algebraisch. Falls ein Element $\alpha \in L$ algebraisch über E ist, dann ist es auch algebraisch über K.*
Insbesondere ist die Körpererweiterung $L \supset K$ algebraisch genau dann, wenn sowohl $L \supset E$ als auch $E \supset K$ algebraisch sind.

Beweis. Wenn α algebraisch über E ist, dann existiert $\mathrm{MinPol}_E(\alpha) = f = x^n + a_{n-1} \cdot x^{n-1} + \ldots + a_0 \in E[x]$. Wir betrachten den Unterkörper $K(a_0, \ldots, a_{n-1})$ von E, und es ist klar, dass α auch algebraisch über $K(a_0, \ldots, a_{n-1})$ ist. Da $K(a_0, \ldots, a_{n-1}, \alpha) = K(a_0, \ldots, a_{n-1})(\alpha) \supset K(a_0, \ldots, a_{n-1})$ eine einfache Körpererweiterung ist, folgt aus Lemma 4.6, dass

$$[K(a_0, \ldots, a_{n-1}, \alpha) : K(a_0, \ldots, a_{n-1})] < \infty$$

gilt. Andererseits ist nach Satz 4.10 die Erweiterung $K(a_0, \ldots, a_{n-1}) \supset K$ endlich, also sagt der Gradsatz, dass auch $[K(a_0, \ldots, a_{n-1}, \alpha) : K] < \infty$ ist. Dann folgt aus Satz 4.8, dass $K(a_0, \ldots, a_{n-1}, \alpha)$ algebraisch über K ist, also ist auch das Element α algebraisch über K. □

Unser nächstes Ziel ist eine fundamentale Konstruktion der Körpertheorie. Wir haben weiter oben gesehen, dass algebraische Erweiterungen aus Elementen bestehen, welche Nullstellen von Polynomen mit Koeffizienten im Grundkörper sind. Im Umkehrschluss sieht man also, dass man den Koeffizientenkörper eines Polynoms gegebenenfalls erweitern muss, damit dieses Polynom Nullstellen hat. Das Ziel ist es nun, einen Körper zu konstruieren, in dem alle Polynome eine maximale Anzahl von Nullstellen haben. Dieser wird der algebraische Abschluss genannt. Hierzu betrachten wir zunächst ein Beispiel. Definiere

$$L := \{\alpha \in \mathbb{C} \mid \alpha \text{ ist algebraisch über } \mathbb{Q}\}$$

Dann ist $L \subset \mathbb{C}$, und L ist ein Körper, denn für $\alpha, \beta \in L$ ist $\mathbb{Q}(\alpha, \beta)$ (wieder nach Satz 4.10) algebraisch über $\mathbb{Q}$, also $\mathbb{Q}(\alpha, \beta) \subset L$ und damit sind $\alpha + \beta, \alpha \cdot \beta \in L$.
Nach dem Fundamentalsatz der Algebra, welchen wir im nächsten Kapitel beweisen werden (Satz 5.13), zerfällt jedes Polynom mit Koeffizienten in $\mathbb{Q}$ über $\mathbb{C}$ in Linearfaktoren, und dann sind die Nullstellen dieses Polynoms per Definition algebraisch über $\mathbb{Q}$, also Elemente von L. L ist daher der algebraische Abschluss von $\mathbb{Q}$, genannt Körper der algebraischen Zahlen, und geschrieben $\overline{\mathbb{Q}}$.
Um die Konstruktion eines algebraischen Abschlusses allgemein durchführen zu können, konstruieren wir zunächst Erweiterungskörper, in denen ein vorgegebenes Polynom eine Nullstelle hat.

Satz 4.13 (Verfahren von Kronecker)**.** *Sei K ein Körper, $f \in K[x]$ mit $\deg(f) > 0$. Dann gibt es einen Erweiterungskörper $L \supset K$ und ein $\alpha \in L$ mit $f(\alpha) = 0$. Falls f irreduzibel in $K[x]$ ist, dann kann man $L = K[x]/(f)$ wählen.*

Beweis. Für den Fall, dass f irreduzibel in $K[x]$ ist, haben wir das Verfahren schon in der Bemerkung nach Lemma 3.30 skizziert: Wir wissen, dass f dann prim ist, das Ideal (f) ist ein Prim- und daher (weil $K[x]$ ein Hauptidealring ist) auch ein maximales Ideal, und deshalb ist $K[x]/(f)$ ein Körper. Die Komposition

$$\begin{array}{ccccc} K & \hookrightarrow & K[x] & \overset{\pi}{\twoheadrightarrow} & K[x]/(f) \\ c & \longmapsto & c \cdot x^0 & & \\ & & g & \longmapsto & [g] \end{array}$$

ist ein Körperhomomorphismus und daher injektiv, wir können also K als Unterkörper von $L := K[x]/(f)$ auffassen. Wir setzen $\alpha := [x] = \pi(x) \in L$, sei $f = \sum_{i=0}^{n} a_i x^i$, dann ist

$$f(\alpha) = \sum_{i=0}^{n} a_i \cdot \alpha^i = \sum_{i=0}^{n} a_i \cdot \pi(x)^i = \pi\left(\sum_{i=0}^{n} a_i \cdot x^i\right) = \pi(f) = 0.$$

Falls f reduzibel ist, und g einer der irreduziblen Faktoren, können wir mit dem eben Gesagten eine Erweiterung $L \supset K$ konstruieren, welche eine Nullstelle von g enthält, aber diese ist dann natürlich auch eine Nullstelle von f. □

Es ist klar, dass die Aussage dieses Satzes eigentlich stärker ist: Wenn wir einen Körper $L \supset K$ konstruiert haben, so dass f in L eine Nullstelle hat, dann können wir über $L[x]$ einen Linearfaktor von f abspalten, und danach das Verfahren wiederholen. Man sieht also, dass man für jeden Körper K und jedes $f \in K[x]$ einen Erweiterungskörper L konstruieren kann, über dem f in Linearfaktoren zerfällt. Die Frage, der wir uns jetzt widmen, ist, ob man diese Konstruktion auch simultan für alle $f \in K[x]$ durchführen kann. Dazu zunächst ein Begriff.

Definition 4.14. *Ein Körper K heißt algebraisch abgeschlossen, falls für alle $f \in K[x]$ mit $\deg(f) > 0$ ein $\alpha \in K$ existiert, so dass $f(\alpha) = 0$ ist. Iterativ sieht man, dass dann f in $K[x]$ in Linearfaktoren zerfällt, d.h.,*

$$f = c \cdot \prod_{i=1}^{\deg(f)} (x - \alpha_i)$$

mit $c \in K \backslash \{0\}$.

Wir haben die folgende mengentheoretische Charakterisierung von algebraisch abgeschlossenen Körpern.

Lemma 4.15. *K ist algebraisch abgeschlossen, falls er keine echten algebraischen Erweiterungen besitzt, d.h., falls für jede algebraische Körpererweiterung $L \supset K$ gilt, dass $L = K$ ist.*

Beweis. Angenommen, K ist algebraisch abgeschlossen, und sei $L \supset K$ eine algebraische Körpererweiterung. Wähle ein $\alpha \in L$, dann zerfällt $\mathrm{MinPol}_K(\alpha) \in K[x]$ schon in $K[x]$ in Linearfaktoren. Andererseits ist $\mathrm{MinPol}_K(\alpha)$ irreduzibel in $K[x]$, daher muss $\deg(\mathrm{MinPol}_K(\alpha)) = 1$ und daher ist $\alpha \in K$ sein.
Für die andere Implikation nehmen wir an, dass K keine echten algebraischen Erweiterungen besitzt. Sei $f \in K[x]$ mit $\deg(f) > 1$. Mit Hilfe des Kronecker-Verfahrens (Satz 4.13) finden wir eine *algebraische* Erweiterung $L \supset K$, so dass f in L eine Nullstelle hat. Dann folgt aus der Annahme, dass $L = K$ ist, und diese Nullstelle liegt schon in K. □

Bevor wir zur Konstruktion von algebraisch abgeschlossenen Körpern kommen, benötigen wir ein technisches Hilfsmittel, welches uns auch später noch von Nutzen sein wird.

Lemma 4.16. *1. (Zornsches Lemma) Sei M eine partiell geordnete Menge, d.h., es gibt eine Relation $R \subset M \times M$, geschrieben $x \leq y$ für $x, y \in M$, $(x, y) \in R$, so das gilt*

$$x \leq x \quad \forall x \in M$$

$$x \leq y, y \leq z \implies x \leq z$$

$$x \leq y, y \leq x \implies x = y$$

Eine solche Ordnung heißt total, wenn für alle $x, y \in M$ $x \leq y$ oder $y \leq x$ gilt. Für eine Teilmenge $N \subset M$ heißt ein Element $a \in M$ obere Schranke, falls $x \leq a$ für alle $x \in N$ gilt. Ein Element $a \in M$ heißt maximales Element, falls für alle $x \in M$ aus $a \leq x$ folgt, dass $a = x$ ist. Dann gilt: Angenommen, jede total geordnete Teilmenge N von M habe eine obere Schranke, dann besitzt M ein maximales Element.

Bemerke, dass $N = \emptyset$ total geordnet ist. Unter der Voraussetzung des Zornschen Lemmas muss es daher eine obere Schranke $a \in M$ von $N = \emptyset$ geben muss, insbesondere ist dann also $M \neq \emptyset$.

2. Sei R ein Ring und $I \subsetneq R$ ein Ideal. Dann gibt es ein maximales Ideal $\mathbf{m} \subsetneq R$ mit $I \subset \mathbf{m}$

Beweis. 1. Das Zornsche Lemma läßt sich nicht beweisen, man kann nur zeigen, dass es zu anderen Aussagen, z.B. zum sogenannten Auswahlaxiom äquivalent ist. Dies soll hier nicht ausgeführt werden.

2. Wir verwenden Teil 1. Sei
$$M = \{J \subsetneq R \text{ Ideal } | I \subset J\}$$
dann ist M bezüglich der Inklusion von Idealen partiell geordnet und wegen $I \in M$ nicht leer. Sei $N \subset M$ total geordnet, dann definieren wir:
$$\widetilde{J} := \bigcup_{J \in N} J.$$
Man kann zeigen (hier geht ein, dass N total geordnet ist), dass $\widetilde{J} \subset R$ ein Ideal ist, natürlich gilt $I \subset \widetilde{J}$, also ist $\widetilde{J} \in M$, und es ist natürliche eine obere Schranke für N. Also sind die Voraussetzungen von Teil 1. erfüllt, und M besitzt ein maximales Element, aber dies ist natürlich gerade ein maximales Ideal $\mathbf{m} \subsetneq R$ mit $I \subset \mathbf{m}$.

□

Satz 4.17. *Sei K ein Körper, dann existiert ein algebraisch abgeschlossener Erweiterungskörper $L \supset K$.*

Für den Beweis dieses Satzes benötigen wir eine Erweiterung des Begriffs des Polynomringes, nämlich auf Polynome in unendlich vielen Variablen. Aus Zeitgründen geben wir hier eine leicht informelle Definition, welche sich aber (analog zu unserer Definition von Polynomringen in endlich vielen Variablen, siehe 3.6) präzisieren lässt.

Definition 4.18. *Sei R ein Ring und sei ein System von Variablen $(x_i)_{i \in S}$ gegeben, hierbei kann $|S|$ auch unendlich sein. Wie in Definition 3.6 betrachten wir*
$$\mathbb{N}^{(S)} := \{f : S \to \mathbb{N} \,|\, f(s) = 0 \text{ für fast alle } s \in S\},$$
und wir schreiben Elemente von $\mathbb{N}^{(S)}$ als Tupel $I = (i_s)_{s \in S}$, wobei $i_s \in \mathbb{N}$ ist und $i_s = 0$ für fast alle $s \in S$ gilt.
Dann definieren wir $R[(x_i)_{i \in S}]$ als die Menge aller formalen Summen
$$\sum_{I \in \mathbb{N}^{(S)}} a_I \cdot \underline{x}^I,$$
hierbei ist $a_I \in R$, es gilt $a_I = 0$ für fast alle $I \in \mathbb{N}^{(S)}$ und es ist $\underline{x}^I := \prod_{s \in S} x_s^{i_s}$.
Wir erhalten analog zur Definition 3.6 eine Addition und eine Multiplikation auf $R[(x_i)_{i \in S}]$ durch die Formeln
$$\begin{aligned} \textstyle\sum_{I \in \mathbb{N}^{(S)}} a_I \cdot \underline{x}^I + \sum_{I \in \mathbb{N}^{(S)}} b_I \cdot \underline{x}^I &:= \sum_{I \in \mathbb{N}^{(S)}} (a_I + b_I) \cdot \underline{x}^I \\ \left(\textstyle\sum_{I \in \mathbb{N}^{(S)}} a_I \cdot \underline{x}^I\right) \cdot \left(\sum_{I \in \mathbb{N}^{(S)}} b_I \cdot \underline{x}^I\right) &:= \sum_{I \in \mathbb{N}^{(S)}} c_I \cdot \underline{x}^I, \end{aligned}$$
hierbei ist $c_I := \sum_{J+K=I} a_J \cdot b_K$ und die Vektoren $J, K \in \mathbb{N}^{(S)}$ werden komponentenweise addiert.
Man prüft, dass dann $R[(x_i)_{i \in S}]$ ein kommutativer Ring mit 1 ist, genannt der Polynomring in (eventuell unendlich vielen) durch S indizierten Variablen.

Beweis von Satz 4.17. Wir definieren die Menge
$$S := \{f \in K[x] \,|\, \deg(f) > 0\},$$
und betrachten den Polynomring $K[(x_f)_{f \in S}]$. Setze $\mathfrak{a} := (f(x_f)_{f \in S})$. Wir zeigen jetzt zunächst, dass $\mathfrak{a}$ ein echtes Ideal in $K[(x_f)_{f \in S}]$, das also $\mathfrak{a} \subsetneq K[(x_f)_{f \in S}]$ ist. Angenommen, dies wäre nicht so, dann hätten wir $1 \in \mathfrak{a}$, und nach der Definition des von einer Teilmenge eines Ringes erzeugten Ideals gibt es dann Polynome $f_1, \ldots, f_k \in S$ (d.h. $\deg(f_i) > 0$) und Polynome $g_1, \ldots, g_k \in K[(x_f)_{f \in S}]$ mit
$$\sum_{i=1}^{k} g_i \cdot f_i(x_{f_i}) = 1$$

(Man beachte: Das Ideal $\mathfrak{a}$ wird von unendlich vielen Elementen erzeugt, aber jedes Element dieses Ideals lässt sich als Linearkombination endlich vieler dieser Erzeuger schreiben, siehe Lemma 3.12). Mit dem Verfahren von Kronecker (Satz 4.13) können wir eine Erweiterung $E \supset K$ konstruieren, in der jedes Polynom f_i $(i = 1, \ldots, k)$ eine Nullstelle α_i hat (durch k-fache Anwendung dieses Verfahrens). Dann wenden wir den Einsetzungshomomorphismus (k-mal) auf das Polynom $\sum_{i=1}^{k} g_i \cdot f_i(x_{f_i})$ an, und ersetzen x_{f_i} durch α_i diese liefert $\sum_{i=1}^{k} g_i \cdot f_i(\alpha_i) = 0$, also $0 = 1$, dies ist ein Widerspruch. Also ist $\mathfrak{a} \subsetneq K[(x_f)_{f \in S}]$.
Nach Lemma 4.16, Teil 2., gibt es also ein maximales Ideal $\mathfrak{m} \supset \mathfrak{a}$, und dann ist die injektive Abbildung $K \hookrightarrow K[(x_f)_{f \in S}]/\mathfrak{m} =: L_1$ eine Körpererweiterung. Für alle $f = \sum_{i=0}^{n} b_i x^i \in S$ gilt dann

$$f([x_f]) = \sum_{i=0}^{n} b_i [x_f]^i = [\sum_{i=0}^{n} b_i x_f^i] = [f(x_f)] = 0$$

Damit hat jedes Polynom aus S, also jedes nicht-konstante Polynom aus $K[x]$, eine Nullstelle in L_1. Allerdings wissen wir nicht, ob L_1 algebraisch abgeschlossen ist, denn dazu müsste jedes Polynom aus $L_1[x]$ eine Nullstelle in L_1 haben. Daher wenden wir das obige Verfahren auf L_1 an, und erhalten eine Körpererweiterung $L_2 \supset L_1$. Induktiv bekommen wir eine Körperkette

$$L_0 := K \subset L_1 \subset L_2 \subset \ldots$$

und wir definieren $L := \bigcup_{i \geq 0} L_i$. Dann ist L ein Körper, genauer eine Körpererweiterung $L \supset K$. Jedes Polynom $g = c_m x^m + \ldots c_0 \in L[x]$ hat nur endlich viele von Null verschiedene Koeffizienten c_i, jeder dieser Koeffizienten c_i liegt in einem Körper $L_{j(i)}$, d.h., es gibt ein $n \in \mathbb{N}$ mit $g \in L_n[x]$. Dann hat g nach Konstruktion eine Nullstelle in L_{n+1}, und daher in L. Also ist L eine algebraisch abgeschlossene Körpererweiterung von K. □

Unter den algebraisch abgeschlossenen Erweiterungen eines Körpers K gibt es solche, welche in gewissem Sinne minimal sind.

Korollar 4.19. *Für einen Körper K existiert ein algebraisch abgeschlossener Erweiterungskörper $\overline{K} \supset K$, welcher algebraisch über K ist. $\overline{K}$ heisst ein algebraischer Abschluss von K.*

Beweis. Wir konstruieren wie in Satz 4.17 einen algebraisch abgeschlossenen Erweiterungskörper L von K. Dann setzen wir

$$\overline{K} := \{\alpha \in L \,|\, \alpha \text{ ist algebraisch über } K\}\,.$$

Wie schon in dem Beispiel vor Satz 4.13 gezeigt, ist dann $\overline{K}$ ein Körper, denn für $\alpha, \beta \in \overline{K}$ ist auch $K(\alpha, \beta) \subset \overline{K}$ und daher $\alpha + \beta, \alpha \cdot \beta \in \overline{K}$. Natürlich ist $\overline{K}$ algebraisch über K und es bleibt zu zeigen, dass er algebraisch abgeschlossen ist. Sei also $f \in \overline{K}[x]$ mit $\deg(f) > 0$. Dann hat f in L eine Nullstelle γ (denn L ist algebraisch abgeschlossen), aber γ ist natürlich algebraisch über $\overline{K}$ ist. Dann ist γ nach Korollar 4.12 (Transitivität der Algebraizität von Körpererweiterungen) auch algebraisch über K, und daher ist nach Definition $\gamma \in \overline{K}$. □

Die Notation $\overline{K}$ für einen algebraischen Abschluss von K suggeriert, dass dieser in gewisser Weise eindeutig ist. Dies ist tatsächlich der Fall, was wir als nächstes zeigen. Wir starten mit einem vorbereitenden Lemma, für welches wir eine Notation benötigen: Seien R und R' Ringe, und $\sigma : R \to R'$ ein Ringhomomorphismus, und sei $f = \sum_{i=0}^{n} a_i \cdot x^i \in R[x]$. Dann definieren wir $f^\sigma := \sum_{i=0}^{n} \sigma(a_i) \cdot x^i \in R'[x]$. Mit diesen Notationen haben wir das folgende Resultat.

Lemma 4.20. *Sei K ein Körper, $K' = K(\alpha)$ wobei α über K algebraisch ist. Sei $f = \mathrm{MinPol}_K(\alpha)$. Sei ein Körperhomomorphismus $\sigma : K \to L$ gegeben. Dann gilt:*

1. *Ist $\sigma' : K' \to L$ eine Fortsetzung von σ, d.h., σ' ist ein Körperhomomorphismus und es gilt $\sigma'_{|K} = \sigma$, dann ist $\sigma'(\alpha)$ eine Nullstelle von f^σ.*
2. *Für jede Nullstelle $\beta \in L$ von f^σ existiert genau eine Fortsetzung $\sigma' : K' \to L$ von σ welche $\sigma'(\alpha) = \beta$ erfüllt.*

Insbesondere gilt, dass die Anzahl möglicher Fortsetzungen $\sigma' : K' \to L$ von σ gleich der Anzahl der verschiedenen *Nullstellen von f^σ in L ist, d.h., wir haben*

$$|\{\text{Fortsetzungen } \sigma' : K' \to L \text{ von } \sigma\}| \leq \deg(f^\sigma).$$

Beweis. 1. Wir können f als Element von $K'[x]$ mit Nullstelle $\alpha \in K'$ auffassen. Dann ist $f^{\sigma'} = f^\sigma \in L[x]$ und es gilt

$$f^\sigma(\sigma'(\alpha)) = f^{\sigma'}(\sigma'(\alpha)) = \sum_{i=0}^{n} \sigma'(a_i)\,(\sigma'(\alpha))^i = \sigma'\left(\sum_{i=0}^{n} a_i\alpha^i\right) = \sigma'\left(f(\alpha)\right).$$

Da f das Minimalpolynom von α ist, gilt insbesondere $f(\alpha) = 0$, also $f^\sigma(\sigma'(\alpha)) = 0$.

2. Zuerst zeigen wir die Eindeutigkeit von σ': Wir wissen, dass $K' = K[\alpha]$ gilt, dass also die Elemente von K' Polynome in α mit Koeffizienten in K sind. Daher ist ein Körperhomomorphismus $K' \to L$ eindeutig durch seine Werte auf K und auf α bestimmt. Soll σ' eine Fortsetzung eines gegebenen Homomorphismus $\sigma : K \to L$ sein, ist er also eindeutig durch seinen Wert auf α bestimmt. Falls also solch eine Fortsetzung mit $\sigma'(\alpha) = \beta$ existiert, so ist sie eindeutig bestimmt.

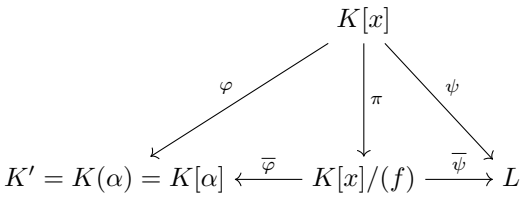
   Nun müssen wir die Existenz von σ' beweisen. Betrachte den Einsetzungshomomorphismus

$$\varphi : K[x] \longrightarrow K';\ g(x) \longmapsto g(\alpha),$$

   sowie den Homomorphismus

$$\psi : K[x] \longrightarrow L;\ g(x) \longmapsto g^\sigma(\beta)$$

   Wir haben $\ker(\varphi) = (f)$ nach Definition des Minimalpolynoms, und da β eine Nullstelle von f^σ ist, gilt $f \in \ker(\psi)$. Daher existiert nach dem Homomorphiesatz ein Homomorphismus $\overline{\psi} : K[x]/(f) \to L$, so dass $\psi = \overline{\psi} \circ \pi$, wobei $\pi : K[x] \to K[x]/(f)$ die kanonische Projektion ist. Wir haben also folgendes kommutative Diagramm



   wobei $\overline{\varphi}$ ein Isomorphismus ist. Also können wir $\sigma' : K' \to L$ einfach durch $\sigma' := \overline{\psi} \circ \overline{\varphi}^{-1}$ definieren. Es ist dann

$$\sigma'(\alpha) = \overline{\psi}(\pi(x)) = \psi(x) = \beta$$

   sowie

$$\sigma'(a) = \overline{\psi}(\pi(a)) = \psi(a) = \sigma(a)$$

   für alle $a \in K$, wie gefordert.

□

Jetzt betrachten wir die speziellere Situation, dass der Körper L aus dem letzten Lemma algebraisch abgeschlossen ist, dann können wir ein analoges Resultat für beliebige algebraische Erweiterungen $K' \supset K$ beweisen.

Satz 4.21. *Sei $K' \supset K$ eine algebraische Körpererweiterung, und $\sigma : K \to L$ ein Körperhomomorphismus, wobei L algebraisch abgeschlossen ist. Dann existiert eine Fortsetzung $\sigma' : K' \to L$.*
Falls K' auch algebraisch abgeschlossen ist und L algebraisch über $\sigma(K)$ ist, dann ist jede Fortsetzung σ' ein Körperisomorphismus.

Beweis. Hier benutzen wir das Zornsche Lemma (Lemma 4.16). Wir betrachten die Menge M aller Paare (F,τ), wobei $K \subset F \subset K'$, d.h., F ist ein Zwischenkörper der Körpererweiterung $K \subset K'$, und $\tau : F \hookrightarrow L$ eine Fortsetzung von σ auf F ist. Offensichtlich ist $(K,\sigma) \in M$, also $M \neq \emptyset$. Wir betrachten die Relation $(F_1,\tau_1) \leq (F_2,\tau_2) \iff F_1 \subset F_2,\ (\tau_2)_{|F_1} = \tau_1$, dann ist M bezüglich dieser Relation partiell geordnet. Sei $N \subset M$ total geordnet, dann besitzt N eine obere Schranke in M, welche einfach die Vereinigung der in N enthaltenen Körper ist, mit der darauf definierten Einbettung nach L. Also sagt das Zornsche Lemma 4.16, dass es in M ein maximales Element $(\widetilde{F},\widetilde{\tau})$ gibt.
Behauptung: Dann ist notwendig schon $\widetilde{F} = K'$. Beweis indirekt: Sei $\widetilde{F} \subsetneq K'$, dann existiert $\alpha \in K' \backslash \widetilde{F}$, aber dann ist $\widetilde{F}(\alpha)$ algebraisch über $\widetilde{F}$ (denn $\alpha \in K'$, und K' war sogar über K algebraisch). Sei $f \in \widetilde{F}[x]$ das Minimalpolynom von α, dann betrachten wir $f^{\widetilde{\tau}} \in L[x]$. Da L algebraisch abgeschlossen ist, gibt es auf jeden Fall eine Nullstelle von $f^{\widetilde{\tau}}$ in $L[x]$ und dann sagt Lemma 4.20, Punkt 2., dass es eine Fortsetzung $\widetilde{\tau}' : \widetilde{F}(\alpha) \hookrightarrow L$ von $\widetilde{\tau} : \widetilde{F} \hookrightarrow L$ geben muss, im Widerspruch zur Maximalität von $(\widetilde{F},\widetilde{\tau})$.
Also ist $\widetilde{F} = K'$ und daher definiert $\sigma' := \widetilde{\tau} : K' \hookrightarrow L$ die gewünschte Erweiterung von $\sigma : K \hookrightarrow L$.
Wir nehmen nun an, dass die Erweiterung K' algebraisch abgeschlossen ist, und dass wir eine Fortsetzung $\sigma' : K' \to L$ konstruiert haben. Dann überlegt man sich leicht, dass der Körper $\sigma'(K')$ auch algebraisch abgeschlossen ist, denn $\sigma' : K' \to L$ ist als Körperhomomorphismus injektiv, und daher ist K' zu $\sigma'(K')$ isomorph. Natürlich enthält $\sigma'(K')$ den Körper $\sigma(K)$, wenn also $L \supset \sigma(K)$ algebraisch ist, dann ist $L \supset \sigma'(K')$ erst recht eine algebraische Körperweiterung. Dann muss aber, da $\sigma'(K')$ algebraisch abgeschlossen ist, schon $L = \sigma'(K')$ gelten, also ist σ' surjektiv. Aber als Körperhomomorphismus ist σ' auch automatisch injektiv, und daher ein Isomorphismus □

Aus dem eben bewiesenen Resultat können wir jetzt die Eindeutigkeit (bis auf Isomorphie) des algebraischen Abschlusses folgern.

Korollar 4.22. *Sei K ein Körper und $\overline{K}_1$ sowie $\overline{K}_2$ zwei algebraische Abschlüsse von K. Dann existiert ein (nicht unbedingt eindeutig bestimmter) Körperisomorphismus $\varphi : \overline{K}_1 \to \overline{K}_2$, welcher die Identität auf K fortsetzt, d.h., so dass $\varphi_{|K} = \mathrm{id}_K$ gilt.*

Beweis. Wir wenden einfach den Satz 4.21 an, und zwar für $K' = \overline{K}_1$, $L = \overline{K}_2$ und $\sigma : K \hookrightarrow \overline{K}_2$, dann ist nach Definition $L = \overline{K}_2$ algebraisch über $K = \sigma(K)$ und $K' = \overline{K}_1$ ist algebraisch abgeschlossen, so dass der letzte Satz einen Isomorphismus φ von $K' = \overline{K}_1$ nach $L = \overline{K}_2$ liefert, welcher σ fortsetzt, d.h., welcher die Identität auf K ist. □

4.2 Normale und separable Erweiterungen

In diesem Abschnitt wollen wir zwei spezielle Arten von Körpererweiterungen studieren, welche im nächsten Kapitel von besonderer Bedeutung sind. Wir beginnen mit dem Begriff des Zerfällungskörper eines oder mehrerer Polynome, und zeigen unter Zuhilfenahme der Ergebnisse über algebraische Abschlüsse aus dem letzten Abschnitt die Existenz und Eindeutigkeit (bis auf Isomorphie) von Zerfällungskörpern.
Dann befassen wir uns mit dem Begriff der Separabilität. Zur Charakterisierung von separablen Erweiterungen benutzen wir eine algebraische Variante der Ableitung (von Polynomen).

Definition 4.23. *Sei K ein Körper und $S \subset K[x]$ eine Teilmenge mit $\deg(f) > 0$ für alle $f \in S$. Sei $L \supset K$ eine Körpererweiterung. Dann heißt L ein Zerfällungskörper der Familie von Polynomen S, falls die folgenden zwei Bedingungen erfüllt sind:*

1. *Alle $f \in S$ zerfallen über L in Linearfaktoren.*
2. *L wird als Körpererweiterung von den Nullstellen aller Polynome in S erzeugt.*

Es folgt direkt aus der Definition, dass ein Zerfällungskörper eine algebraische Körpererweiterung ist.
Für den Fall $S = \{f\}$ seien $a_1, \ldots, a_n$ die Nullstellen von f im algebraischen Abschluss $\overline{K}$, so ist $L = K(a_1, \ldots, a_n)$. Dies zeigt die Existenz eines Zerfällungskörpers für ein Polynom. Für beliebige Familien S

argumentiert man analog: In einem algebraischen Abschluss $\overline{K}$ von K zerfallen alle Polynome aus S in Linearfaktoren, und dann ist der von allen Nullstellen erzeugte Unterkörper von $\overline{K}$ ein Zerfällungskörper von S. Man überlegt sich leicht, dass für eine endliche Menge $S = \{f_1, \ldots, f_k\}$ eine Körpererweiterung $L \supset K$ genau dann ein Zerfällungskörper von S ist, wenn sie ein Zerfällungskörper des einzelnen Polynoms $f = f_1 \cdot \ldots \cdot f_k$ ist.
Wir zeigen jetzt, dass auch Zerfällungskörper im Wesentlichen eindeutig sind. Dazu zuerst die folgende Aussage.

Satz 4.24. *Sei wie oben K ein Körper und $S \subset K[x]$, $\deg(f) > 0\ \forall f \in S$. Seien L_1 und L_2 Zerfällungskörper von S. Sei $\sigma : L_1 \to \overline{L}_2$ ein K-Homomorphismus, d.h. ein Körperhomomorphismus, so dass $\sigma_{|K} = \mathrm{id}_K$ gilt. Wir schreiben dann auch $\sigma \in \mathrm{Hom}_K(L_1, \overline{L}_2)$. Dann ist $\mathrm{Im}(\sigma) = L_2$ und daher liefert σ einen Körperisomorphimus $L_1 \xrightarrow{\cong} L_2$.*

Beweis. Wir führen den Beweis zunächst in dem Spezialfall $S = \{f\}$ für ein nicht-konstantes Polynom $f \in K[x]$, welches wir ohne Beschränkung der Allgemeinheit als unitär annehmen können. f zerfällt sowohl in L_1 als auch in L_2 in Linearfaktoren, wenn $n := \deg(f)$ ist, kann man also schreiben

$$f = \prod_{i=1}^{n}(x - a_i) \in L_1[x] \quad \text{und} \quad f = \prod_{i=1}^{n}(x - b_i) \in L_2[x]$$

wobei $a_i \in L_1$ die Nullstellen von f über L_1 und $b_i \in L_2$ die Nullstellen von f über $L_2 \subset \overline{L}_2$ sind. Nach Definition ist dann $f^\sigma = \prod_{i=1}^{n}(x - \sigma(a_i)) \in \overline{L}_2[x]$, aber da $f \in K[x]$ und σ ein K-Homomorphismus ist, ist $f^\sigma = f$ und wir haben

$$f^\sigma = \prod_{i=1}^{n}(x - b_i)$$

Wir sehen, dass sich σ zu einer Bijektion

$$\sigma_{|\{a_1,\ldots,a_n\}} : \{a_1, \ldots, a_n\} \xrightarrow{\cong} \{b_1, \ldots, b_n\}$$

einschränkt. Nach Definition eines Zerfällungskörpers haben wir $L_2 = K(b_1, \ldots, b_n)$, also gilt

$$L_2 = K(b_1, \ldots, b_n) = K(\sigma(a_1), \ldots, \sigma(a_n)) = \sigma\left(K(a_1, \ldots, a_n)\right) = \sigma(L_1).$$

Dies beweist die Aussage im Fall $|S| = 1$.
Falls $S = \{f_1, \ldots, f_k\}$ endlich ist, dann sind, wie oben bemerkt, L_1 und L_2 auch Zerfällungskörper des Produktes $f = f_1 \cdot \ldots \cdot f_k$, und dann liefert der eben geführte Beweis, dass σ auch in diesem Fall ein Körperisomorphismus $L_1 \xrightarrow{\cong} L_2$ ist.
Falls S eine beliebige Familie von nicht-konstanten Polynomen in $K[x]$ ist, dann können wir S als Vereinigung aller endlichen Teilfamilien schreiben, und dann ist ein beliebiger Zerfällungskörper L von S die Vereinigung der Zerfällungskörper zu den endlichen Teilfamilien von S. Daher gilt die Behauptung auch in diesem Fall. □

Korollar 4.25. *Sei K ein Körper, dann sind je zwei Zerfällungskörper L_1 und L_2 einer Familie nicht-konstanter Polynome $S \subset K[x]$ isomorph.*

Beweis. Wegen Satz 4.21 erweitert sich die Inklusion $K \hookrightarrow \overline{L}_2$ zu einem Körperhomomorphismus $L_1 \to \overline{L}_2$. Dann liefert der letzte Satz (Satz 4.24), dass dieser Homomorphismus schon ein Körperisomorphismus $L_1 \xrightarrow{\cong} L_2$ ist. □

Wir kommen jetzt zur ersten speziellen Klasse von Körpererweiterungen, welche wir durch verschiedene Bedingungen charakterisieren können.

Definition-Lemma 4.26. *Sei $L \supset K$ eine algebraische Körpererweiterung. Dann sind die folgenden Bedingungen äquivalent.*

1. *Jeder K-Homomorphismus $g : L \to \overline{L}$ erfüllt $\mathrm{Im}(g) = L$, d.h., ist ein Automorphismus $g : L \xrightarrow{\cong} L$,*

2. *Alle irreduziblen Polynome in $K[x]$, welche eine Nullstelle in L besitzen, zerfallen über L in Linearfaktoren,*

3. *Es gibt eine Menge nicht-konstanter Polynome $S \subset K[x]$, so dass L Zerfällungskörper von S ist.*

Körpererweiterungen, welche die obengenannten äquivalenten Bedingungen erfüllen, heißen normal.

Beweis. **1. ⇒ 2.** Sei $f \in K[x]$ irreduzibel, und sei $a \in L$ eine Nullstelle von f. Betrachte einen algebraischen Abschluss $\overline{L}$ von L, und eine weitere Nullstelle $b \in \overline{L}$ von f. Dann existiert nach Lemma 4.20 ein K-Homomorphismus $\sigma : K(a) \to \overline{L}$ mit $\sigma(a) = b$ (setze für den Körper L im Lemma 4.20 den algebraischen Abschluß $\overline{L}$ ein). Da aber $\overline{L}$ algebraisch abgeschlossen ist, existiert nach Satz 4.21 eine Fortsetzung zu einem K-Homomorphismus $\sigma : L \to \overline{L}$. Nach Voraussetzung (Punkt 1.) gilt dann $\mathrm{Im}(\sigma) = L$, aber dann ist $b \in L$. Also zerfällt f schon über L in Linearfaktoren.

2. ⇒ 3. Da L eine algebraische Körpererweiterung von K ist, existiert nach Satz 4.11 eine Menge $T = \{a_i\}_{i \in I}$ von algebraischen Elementen, so dass $L = K(T) = K\left((a_i)_{i \in I}\right)$ ist. Sei $f_i := \mathrm{MinPol}_K(a_i)$ für alle $i \in I$. Nach Definition ist a_i eine Nullstelle von f_i in L, und daher zerfallen nach Voraussetzung alle f_i über L in Linearfaktoren, dies aber bedeutet nichts anderes, als dass L der Zerfällungskörper der Menge $S := \{f_i\}_{i \in I}$ ist.

3. ⇒ 1. Sei L der Zerfällungskörper einer Menge $S \subset K[x]$ von nicht-konstanten Polynomen und sei $T \subset L$ die Menge aller Nullstellen von allen Elementen aus S. Sei weiterhin ein K-Homomorphismus $\sigma : L \to \overline{L}$ gegeben. Man zeigt genau wie im Beweis von Satz 4.24, dass sich dann σ zu einer Bijektion von T einschränkt, weil aber L per Definition von T erzeugt wird, d.h., weil $L = K(T)$ gilt, ist dann notwendig $\sigma(L) = L$, und daher ist σ ein Automorphismus von L.

□

Im Allgemeinen ist die Normalitätseigenschaft nicht transitiv bezüglich Zwischenkörpern: Zwar folgt bei Erweiterungen $E \supset K$ und $L \supset E$ aus der Normalität von $L \supset K$ natürlich die Normalität von $L \supset E$ (nämlich wegen Punkt 3. von Lemma 4.26), allerdings nicht unbedingt die Normalität von $E \supset K$. Auch umgekehrt folgt im Allgemeinen aus der Normalität von $L \supset E$ und von $E \supset K$ nicht, dass $L \supset K$ normal ist.
Als Beispiel betrachten wir den Fall $K = \mathbb{Q}$, $E = \mathbb{Q}(\sqrt[3]{2})$, dann ist $\mathrm{MinPol}_{\mathbb{Q}}(\sqrt[3]{2}) =: f = x^3 - 2$ irreduzibel in $\mathbb{Q}[x]$, also ist $[E : K] = 3$. Allerdings ist E nicht der Zerfällungskörper von f, denn über $\mathbb{C}$ ist $f = (x - \sqrt[3]{2})(x - \sqrt[3]{2} \cdot \zeta)(x - \sqrt[3]{2} \cdot \zeta^2)$, wobei $\zeta = e^{2\pi i/3}$ eine dritte Einheitswurzel ist. Da $\zeta \notin \mathbb{R}$, aber $E \subset \mathbb{R}$ gilt, ist wegen Punkt 2. von Lemma 4.26 die Erweiterung $E \supset K$ nicht normal. Man kann prüfen, dass die Erweiterung $L = \mathbb{Q}(\sqrt[3]{2}, \zeta)$ der Zerfällungskörper von f ist, also ist $L \supset K$ normal.
Für nicht-normale Erweiterungen $E \supset K$ möchte man daher ein in gewissem Sinne kleinsten Oberkörper L von E, so dass $L \supset K$ normal ist, konstruieren. Dies beschreibt der folgende Begriff.

Definition 4.27. *Sei $L \supset K$ eine algebraische Körpererweiterung. Dann heißt eine Erweiterung L' von L, so dass $L' \supset K$ normal ist, aber so, dass kein Zwischenkörper $\widetilde{L}$ von $L' \supset L$ mit $\widetilde{L} \supset K$ normal existiert, eine* normale Hülle *von $L \supset K$.*

Der folgende Satz liefert Konstruktionsmöglichkeiten der normalen Hülle.

Satz 4.28. *Sei eine algebraische Körpererweiterung $L \supset K$ gegeben. Dann gilt:*

1. *Es existiert eine bis auf Isomorphie eindeutig bestimmte normale Hülle L' von $L \supset K$.*

2. *Ist die Erweiterung $L \supset K$ endlich, so auch die Erweiterung $L' \supset K$.*

3. *Sei $M \supset L$ eine algebraische Erweiterung, so dass $M \supset K$ normal ist, dann kann man eine normale Hülle $\widetilde{L}$ von $L \supset K$ konstruieren als $\widetilde{L} = K(\widetilde{S})$ mit*

$$\widetilde{S} := \{\sigma(a) \,|\, a \in L, \sigma \in \mathrm{Hom}_K(L, M)\}$$

$\widetilde{L}$ heißt auch normale Hülle von L in M.

Beweis. 1. Da die Erweiterung $L \supset K$ algebraisch ist, folgt mit Satz 4.11, dass $L = K(S)$ für eine Teilmenge $S \subset L$ von über K algebraischen Elementen gilt. Sei $T := \{\mathrm{MinPol}_K(a) \,|\, a \in S\}$ dann definieren wir

$$S' := \bigcup_{f \in T} \{\text{Nullstellen von } (f)\} \subset \overline{L}$$

und setzen $L' := K(S')$. Dann ist die Erweiterung nach $L' \supset K$ nach Lemma 4.26 normal, und man sieht leicht, dass es die normale Hülle von $L \supset K$ sein muss (denn ein echter Zwischenkörper von $L' \supset L$ würde nicht alle Nullstellen aller Polynome aus T enthalten).

Da die normale Hülle nach Lemma 4.26 immer ein Zerfällungskörper einer Menge von Polynomen ist, folgt aus Korollar 4.25 die Eindeutigkeit bis auf Isomorphie.

2. Betrachte die Konstruktion einer normalen Hülle aus Punkt 1. War die Erweiterung $L \supset K$ endlich, dann wird L' von einer endlichen Menge von über K algebraischen Elemente erzeugt, ist als nach Satz 4.10 selbst endlich über K.

3. Wir betrachten die Konstruktion einer normalen Hülle $L' = K(S') \subset \overline{L} \cong \overline{M}$ aus Punkt 1. Sei $\sigma \in \mathrm{Hom}_K(L, M)$ und $a \in S$ (Erinnerung: $L = K(S)$), dann ist $\sigma(a)$ nach Lemma 4.20 eine Nullstelle von $\mathrm{MinPol}_K(a)$, also gilt $\sigma(a) \in L'$, für alle $a \in S$. Aber dies bedeutet, dass $\sigma(L) \subset L'$ ist, also $\widetilde{L} = K(\widetilde{S}) \subset L'$. Sei andererseits eine Nullstelle $b \in S'$ eines Minimalpolynoms $g = \mathrm{MinPol}_K(a)$ für $a \in L$ gegeben, dann existiert nach Lemma 4.20 ein $\sigma \in \mathrm{Hom}_K(K(b), L')$ mit $\sigma(a) = b$. Wegen Satz 4.21 kann man σ zu einem Homomorphismus $\sigma \in \mathrm{Hom}_K(M, \overline{M})$ fortsetzen, weil aber $M \supset K$ normal ist, gilt dann (siehe Lemma 4.26), dass $\mathrm{Im}(\sigma) = M$, dass also σ ein K-Automorphismus von M ist, insbesondere ist dann $b \in M$, also sogar $b \in K(\widetilde{S})$, und wir erhalten $L' \subset K(\widetilde{S}) = \widetilde{L}$.

□

Wir behandeln als nächstes die zweite spezielle Klasse von Körpererweiterungen, welche in der Galoistheorie eine große Rolle spielen werden. Hierzu benötigen wir zunächst eine algebraische Version der Ableitung.

Definition 4.29. *Sei K ein Körper, dann definieren wir folgendermaßen die Ableitungsabbildung*

$$D : K[x] \longrightarrow K[x]$$

$$f := \sum_{i=0}^{n} a_i \cdot x^i \longmapsto \sum_{i=1}^{n} i \cdot a_i \cdot x^{i-1},$$

hierbei soll $i \cdot a_i := \underbrace{a_i + \ldots + a_i}_{i-\text{mal}}$ für $i \in \{0, \ldots, n\}$ sein. Für $f \in K[x]$ setzen wir $f' := D(f)$.

Man prüft leicht nach, dass die Ableitungsabbildung D die folgenden Regeln für alle $f, g \in K[x]$ erfüllt:

$$\begin{aligned} D(f+g) &= D(f) + D(g) \\ D(f \cdot g) &= f \cdot D(g) + D(f) \cdot g \\ D(a) &= 0 \quad \forall a \in K, \end{aligned}$$

somit ist D kein Ringhomomorphismus, sondern ein Homomorphismus der abelschen Gruppe $(K[x], +)$, welcher die Leibniz-Regel *(die zweite obige Gleichung) erfüllt. Solche Abbildungen heißen auch K-*Derivationen *von $K[x]$.*

Wir können die Ableitung verwenden, um zu prüfen, ob ein Polynom mehrfache Nullstelle hat, wie die folgende Aussage zeigt.

Lemma 4.30. *Sei K ein Körper, $\overline{K}$ sein algebraischer Abschluss und $f \in K[x]\backslash\{0\}$. Dann sind die folgenden Aussagen äquivalent:*

1. *Ein Element $\alpha \in \overline{K}$ ist mehrfache Nullstelle von f, d.h. eine Nullstelle mit Multiplizität (auch Vielfachheit genannt) größer als 1.*
2. *Es gilt $f(\alpha) = f'(\alpha) = 0$.*
3. *Es ist $\mathrm{ggT}(f, f')(\alpha) = 0$.*

Falls zusätzlich f irreduzibel ist, dann hat f in $\overline{K}$ mehrfache Nullstellen genau dann, wenn $f' = 0$ gilt.

Beweis. **1. $\Leftrightarrow$ 2.** Sei $\alpha \in L$ eine Nullstelle von f der Vielfachheit r, dann kann man f, gesehen als Element von $\overline{K}[x]$ schreiben als

$$f(x) = (x - \alpha)^r \cdot g(x)$$

mit $g \in \overline{K}[x]$ und $g(\alpha) \neq 0$. Dann ist wegen der Leibniz-Regel

$$f'(x) = ((x - \alpha)^r)' \cdot g(x) + (x - \alpha)^r \cdot g'(x) = r(x - \alpha)^{r-1} \cdot g(x) + (x - \alpha)^r \cdot g'(x),$$

denn man sieht induktiv (wieder unter Verwendung der Leibniz- Regel) leicht, dass $((x - \alpha)^r)' = r(x - \alpha)^{r-1}$ ist. Falls also $r \geq 2$ ist, dann haben wir $f'(\alpha) = f(\alpha) = 0$. Wissen wir umgekehrt, dass $f(\alpha) = f'(\alpha) = 0$ ist, dann folgt, dass α Nullstelle von $r(x - \alpha)^{r-1} \cdot g(x)$ ist, da aber $g(\alpha) \neq 0$ gilt, muss dann notwendig $r > 1$ sein.

2. $\Leftrightarrow$ 3. Wir bezeichnen den größten gemeinsamen Teiler von f und f' in $K[x]$ mit $\mathrm{ggT}_{K[x]}(f, f')$ und analog den den größten gemeinsamen Teiler von f und f' in $\overline{K}[x]$ mit $\mathrm{ggT}_{\overline{K}[x]}(f, f')$ (die in der Formulierung des Lemmas benutzte Notation $\mathrm{ggT}(f, f')$ bedeutet dann genau $\mathrm{ggT}_{K[x]}(f, f')$).

Betrachte die Primfaktorzerlegung von f und f' in den faktoriellen Ringen $K[x]$ und $\overline{K}[x]$, dann folgt aus Satz 3.35, dass

$$\mathrm{ggT}_{K[x]}(f, f') = \mathrm{ggT}_{\overline{K}[x]}(f, f')$$

ist. Alternativ kann man auch mit Lemma 3.36 argumentieren: Schreibe $K[x]h$ bzw $\overline{K}[x]h'$ für das von Polynomen $h \in K[x]$ bzw. $h' \in \overline{K}[x]$ in den Ringen $K[x]$ bzw. $\overline{K}[x]$ erzeugte Hauptideal. Sei $d := \mathrm{ggT}_{K[x]}(f, f')$, dann ist

$$K[x]d = K[x]f + K[x]f',$$

aber dies impliziert die Gleichung

$$\overline{K}[x]d = \overline{K}[x]f + \overline{K}[x]f',$$

also ist $d = \mathrm{ggT}_{\overline{K}[x]}(f, f')$.

Die Primfaktorzerlegung von f und f' in $\overline{K}[x]$ besteht aber aus Linearfaktoren, also ist $f(\alpha) = f'(\alpha) = 0$ äquivalent dazu, dass $x - \alpha$ ein Teiler von $\mathrm{ggT}_{\overline{K}[x]}(f, f') = \mathrm{ggT}_{K[x]}(f, f')$ ist, und dies ist äquivalent zu $\mathrm{ggT}(f, f')(\alpha) = 0$.

Sei nun f irreduzibel in $K[x]$ und ohne Beschränkung der Allgemeinheit unitär. Sei $a \in \overline{K}$ eine mehrfache Nullstelle von f. Dann muss $f = \mathrm{MinPol}_K(a)$ gelten, aber wie wir eben gesehen haben, ist auch $f'(a) = 0$. Natürlich gilt $\deg(f') < \deg(f)$, also muss dann $f' = 0$ gelten, weil sonst die Minimalität von f verletzt wäre. Ist andererseits $f' = 0$, dann ist jede Nullstelle a von f automatisch eine doppelte Nullstelle. □

Die folgenden Beispiele illustrieren diese Kriterien für die Existenz von mehrfachen Nullstellen:

1. Sei $K = \mathbb{F}_p$, und $f = x^p - x \in K[x]$. Dann ist $f' = p \cdot x^{p-1} - 1 \stackrel{!}{=} -1$, und daher kann es keine mehrfachen Nullstellen von f geben. Man beachte, dass bei einem Polynom die Exponenten immer natürliche Zahlen sind, die Koeffizienten aber aus einem gewählten Ring (oder Körper) kommen, daher ist $x^p \in \mathbb{F}_p[x]$ nicht dass Nullpolynom, aber die Ableitung davon schon, dann durch das Anwenden des Ableitungsoperators „rutscht“ der Exponent in den Koeffizienten, und ist im Koeffizientenkörper $\mathbb{F}_p$ gleich Null.

2. Sei $K = Q(\mathbb{F}_p[t]) = \mathbb{F}_p(t)$ und $f = x^p - t \in K[x]$. Dann liefert das Eisensteinsche Irreduzibilitätskriterium (Satz 3.45), dass f irreduzibel in $K[x]$ ist, denn t ist prim in $\mathbb{F}_p[t]$, also nach dem Satz von Gauß (Satz 3.43) auch in $K = Q(\mathbb{F}_p[t])$, und dieses Primelement teilt den Absolutkoeffizienten von f, es teilt nicht den Leitkoeffizienten, und sein Quadrat teilt nicht den Absolutkoeffizienten von f. Außerdem ist $\mathrm{char}(K) = p$, so dass analog zum ersten Beispiel gilt $f' = p \cdot x^{p-1} = 0$ (denn die Ableitung von t ist Null, da t ein Element des Koeffizientenkörpers $K = Q(\mathbb{F}_p[t])$ ist). Also hat f mehrfache Nullstellen in $\overline{K}$.

3. Sei K ein Körper und $\mathrm{char}(K) = 0$, sei $f \in K[x]$ irreduzibel (insbesondere ist dann $\deg(f) > 0$). Dann ist $f' \neq 0$, also hat f dann keine mehrfachen Nullstellen im algebraischen Abschluss $\overline{K}$.

Polynome ohne doppelte Nullstellen haben eine besondere Bedeutung in der Körpertheorie, daher führen wir hierfür einen eigenen Begriff ein.

Definition 4.31. *Sei K ein Körper und $f \in K[x]$ ein Polynom mit $\deg(f) > 0$. Falls f in $\overline{K}$ keine mehrfachen Nullstellen hat, dann heißt f* separabel. *Nach dem letzten Lemma ist ein irreduzibles Polynom genau dann separabel, wenn seine Ableitung nicht verschwindet.*
Für eine algebraische Erweiterung $L \supset K$ heißt $\alpha \in L$ separabel genau dann, wenn es Nullstelle eines separablen Polynoms $f \in K[x]$ ist (und dies ist, wie man leicht sieht, äquivalent dazu, dass $\mathrm{MinPol}_K(\alpha)$ separabel ist). Die Erweiterung $L \supset K$ heißt separabel, falls alle $\alpha \in L$ separabel sind. Ein Körper K heißt perfekt, falls alle algebraischen Erweiterungen von K separabel sind.

Wie wir gerade gesehen haben, ist ein irreduzibles Polynom $f \in K[x]$ immer separabel, wenn $\mathrm{char}(K) = 0$ ist, also sind Körper der Charakteristik Null immer perfekt. Hingegen ist die Erweiterung $\mathbb{F}_p(t)[x]/(x^p - t) \supset \mathbb{F}_p(t)$ nicht separabel, also ist $\mathbb{F}_p(t)$ nicht perfekt. Um eine genauere Aussage für Polynome über Körpern der Charakteristik $p > 0$ zu erhalten, benötigen wir zunächst folgende Vorbereitung. Dazu machen wir zunächst eine Vorbemerkung, welche allgemeiner nicht nur für endliche Körper, sondern für beliebige Körper mit positiver Charakteristik gilt.

Definition-Lemma 4.32. *Sei K ein Körper mit $\mathrm{char}(K) = p > 0$. Dann gilt*

$$(a \pm b)^{p^r} = a^{p^r} \pm b^{p^r}$$

für alle $a, b \in K$, $r \in \mathbb{N}$.
Die Abbildung

$$\begin{array}{rccc} \sigma : & K & \longrightarrow & K \\ & a & \longmapsto & a^p \end{array}$$

ist ein Körperhomomorphismus, genannt der Frobenius-Homomorphismus *von K.*
Betrachte die Einschränkung $\sigma_{|\mathbb{F}_p}$ (Erinnerung: $\mathrm{char}(K) = p$ bedeutet, dass der Ringhomomorphismus $\mathbb{Z} \to K$ welcher $(\mathrm{char}(K))$ als Kern hat, einen injektiven Körperhomomorphismus $\mathbb{F}_p = \mathbb{Z}/\mathbb{Z}p \hookrightarrow K$ induziert). Dann ist $\sigma_{|\mathbb{F}_p} = \mathrm{id}_{\mathbb{F}_p}$.

Beweis. Die zweite Aussage folgt offenbar aus der ersten, denn die Eigenschaft $(a \cdot b)^p = a^p \cdot b^p$ ist offensichtlich. Man argumentiert per Induktion über r, und muss nur die Formel $(a \pm b)^p = a^p \pm b^p$ zeigen. Es gilt die binomische Formel

$$(a + b)^p = a^p + \sum_{i=1}^{p-1} \binom{p}{i} a^{p-i} b^i + b^p$$

und man sieht leicht, dass $p|\binom{p}{i}$ für alle $i \in \{1,\dots,p-1\}$ gilt, also ist $\sum_{i=1}^{p-1}\binom{p}{i}a^{p-i}b^i = 0$. Damit gilt $(a+b)^p = a^p + b^p$. Wenn wir nun b durch $-b$ ersetzen, erhalten wir

$$(a-b)^p = a^p + (-b)^p = \begin{cases} a^p + b^p & \text{falls } p \text{ gerade} \\ \\ a^p - b^p & \text{falls } p \text{ ungerade,} \end{cases}$$

aber der erste Fall kann nur für $p = 2$ eintreten, und dann ist $a^p + b^p = a^p - b^p$. Damit ist die Formel bewiesen.
Für die letzte Aussage betrachte $a \in \mathbb{F}_p \backslash \{0\} \subset K \backslash \{0\}$. Dann gilt

$$a^{p-1} = 1 \in \mathbb{F}_p$$

Dies ist eine Version des kleinen Satzes von Fermat (Satz 2.16), betrachtet man nämlich die Einheitengruppe $\mathbb{F}_p^*$, dann ist $\mathrm{ord}(\mathbb{F}_p^*) = p-1$, und damit folgt die gewünschte Aussage. Also erhalten wir $a^p = a \in \mathbb{F}_p$, und damit ist $\sigma_{|\mathbb{F}_p} = \mathrm{id}_{\mathbb{F}_p}$. □

Mit dieser Vorbereitung haben wir jetzt die folgende Aussage für Polynome über Körpern positiver Charakteristik.

Lemma 4.33. *Sei K ein Körper mit $\mathrm{char}(K) = p > 0$, und $f \in K[x]$ irreduzibel. Sei $r \in \mathbb{N}$ maximal so dass es ein $g \in K[x]$ gibt mit*

$$f(x) = g\left(x^{(p^r)}\right).$$

Dann haben alle Nullstellen von f die Multiplizität p^r, und g ist separabel und irreduzibel in $K[x]$. Die Nullstellen von f sind die p^r-ten Wurzeln der Nullstellen von g.

Beweis. Sei zunächst irgendein Polynom $h \in K[x]$ gegeben, mit $h = \sum_{i=0}^n c_i \cdot x^i$, dann ist $h' = \sum_{i=1}^n i \cdot c_i \cdot x^{i-1}$. Also haben wir $h' = 0$ genau dann, wenn für alle $i \in \{1,\dots,n\}$ mit $c_i \neq 0$ gilt, dass $p|i$ ist. Dies bedeutet aber nichts anderes, als dass es ein Polynom $\widetilde{h} \in K[x]$ mit $h(x) = \widetilde{h}(x^p)$ gibt.
Seien jetzt wie im Lemma $f, g \in K[x]$ mit $f(x) = g\left(x^{(p^r)}\right)$ gegeben, so dass r maximal mit dieser Eigenschaft ist. Dann kann also kein $\widetilde{g} \in K[x]$ mit $g(x) = g(x^p)$ existieren, d.h., es ist $g' \neq 0$. Offensichtlich ist g irreduzibel, weil auch f es ist. Deshalb ist also g separabel.
Wir wollen jetzt noch die Nullstellen von f bestimmen: Sei $\overline{K}$ ein algebraischer Abschluss, dann gilt

$$g = d \cdot \prod_{i=1}^n (x - a_i) \in \overline{K}[x]$$

mit $d, a_1, \dots, a_n \in \overline{K}$. Sei $b_i \in \overline{K}$ so dass $a_i = b_i^{(p^r)}$, dann gilt

$$f = d \cdot \prod_{i=1}^n \left(x^{(p^r)} - b_i^{(p^r)}\right) \overset{(*)}{=} d \cdot \prod_{i=1}^n (x - b_i)^{(p^r)},$$

also sind die Nullstellen von f genau die p^r-ten Wurzeln der Nullstellen von g und haben die Multiplizität p^r. Hierbei folgt die Gleichheit (*) aus den Formeln des letzten Lemmas (Lemma 4.32). □

Unser Ziel im verbleibenden Teil dieses Abschnittes ist der Satz vom primitiven Element (Satz 4.40), welcher besagt, dass endliche und separable Erweiterungen immer einfach sind, d.h., von einem Element erzeugt werden. Hierzu brauchen wir zunächst einen neuen Begriff.

Definition 4.34. *Sei $L \supset K$ eine algebraische Körpererweiterung und $\overline{K}$ ein algebraischer Abschluß von K. Dann setzen wir*

$$[L:K]_s := \left|\mathrm{Hom}_K\left(L, \overline{K}\right)\right|,$$

und nennen $[L:K]_s$ den Separabilitätsgrad von $L \supset K$, welcher wegen Korollar 4.22 nicht von der Wahl des algebraischen Abschlusses $\overline{K}$ abhängt.

Wir studieren den Separabilitätsgrad zunächst für einfache Erweiterungen.

Satz 4.35. *Sei K ein Körper, $L = K(\alpha)$ und $f = \mathrm{MinPol}_K(\alpha) \in K[x]$ das Minimalpolynom von α. Dann gilt:*

1. *Der Separabilitätsgrad $[L : K]_s$ ist gleich der Anzahl der* verschiedenen *Nullstellen von f in einem algebraischen Abschluss $\overline{K}$.*
2. *α ist separabel über K genau dann, wenn $[L : K]_s = [L : K]$ gilt.*
3. *Sei $\mathrm{char}(K) = p > 0$, und habe die Nullstelle α von f die Multiplizität p^r, dann ist*

$$[L : K] = p^r \cdot [L : K]_s$$

Beweis. 1. Wir verwenden Lemma 4.20, welches uns direkt liefert, dass die Anzahl der (verschiedenen) K-Homomorphismen von L nach $\overline{K}$ gleich der Anzahl der (verschiedenen) Nullstellen von f in $\overline{K}$ sind.

2. Sei $n := \deg(f)$. Angenommen, α ist separabel über K, dann hat f keine doppelten Nullstellen, also n verschiedene, und dann ist wegen Punkt 1. $[L : K]_s = n = [L : K]$. Haben wir andererseits, dass $[L : K]_s = [L : K]$ gilt (diese Zahl ist wegen $f = \mathrm{MinPol}_k(\alpha)$ gleich n), dann hat f wegen Punkt 1. n verschiedene Nullstellen und ist damit separabel (und daher ist nach Definition auch α separabel).

3. Wir haben in Lemma 4.33 gesehen, dass es ein maximales $r \in \mathbb{N}$ gibt, so dass $f(x) = g\left(x^{(p^r)}\right)$ für ein separables Polynom $g \in K[x]$ ist. Es gilt dann natürlich $[L : K] = \deg(f) = p^r \cdot \deg(g)$, aber weil g keine doppelten Nullstellen hat (und die Anzahl der verschiedenen Nullstellen von f gleich der Anzahl der Nullstellen von g ist), folgt aus Punkt 1., dass $[L : K]_s = \deg(g)$ ist.

□

Als nächstes zeigen wir einen Gradsatz für den Separabilitätsgrad.

Satz 4.36. *Seien $K \subset L \subset M$ algebraische Körpererweiterungen, dann gilt:*

$$[M : K]_s = [M : L]_s \cdot [L : K]_s$$

Beweis. Wie man sich leicht überlegt, ist ein algebraischer Abschluss $\overline{K}$ auch ein algebraischer Abschluss für L und M.
Sei

$$\mathrm{Hom}_K(L, \overline{K}) = \{\sigma_i \mid i \in I\}$$

$$\mathrm{Hom}_L(M, \overline{K}) = \{\tau_j \mid j \in J\}$$

mit gewissen Indexmengen I und J. In dieser Schreibweise sind also die Elemente σ_i paarweise verschieden, das gleiche gilt für die Elemente τ_j. Wir wissen aus Satz 4.21, dass sich jedes σ_i zu einem K-Automorphismus $\overline{\sigma}_i : \overline{K} \to \overline{K}$ fortsetzen lässt. Wir behaupten jetzt, dass

$$\mathrm{Hom}_K(M, \overline{K}) = \{\overline{\sigma}_i \circ \tau_j \mid i \in I, j \in J\} \tag{4.1}$$

gilt. Um dies zu zeigen, nehmen wir zunächst an, dass $\overline{\sigma}_i \circ \tau_j = \overline{\sigma}_{i'} \circ \tau_{j'}$ für gewisse $i \in I, i' \in I$ und $j, j' \in J$ sei. Dann können wir beide Seiten dieser Gleichung auf L einschränken, und da $(\tau_j)_{|L} = (\tau_{j'})_{|L} = \mathrm{id}_L$ gilt, folgt automatisch $\overline{\sigma}_i = \overline{\sigma}_{i'}$, d.h. $i = i'$. Dies impliziert $\tau_j = \tau_{j'}$, denn $\overline{\sigma}_i$ ist ein Isomorphismus, d.h., wir haben $j = j'$. Also ist die Schreibweise der rechten Seite von Gleichung (4.1) als Menge wohldefiniert, d.h., die Elemente, die dort stehen, sind paarweise verschieden. Wenn wir also Formel (4.1) beweisen können, dann folgt der gesuchte Gradsatz, denn $|I \times J| = |I| \cdot |J|$.
Die Inklusion $\supset$ in der Gleichung (4.1) ist klar, und wir haben die Inklusion $\subset$ zu zeigen: Sei $\tau \in \mathrm{Hom}_K(M, \overline{K})$ ein beliebiger K-Homomorphismus, dann ist die Einschränkung $\tau_{|L}$ ein Element in $\mathrm{Hom}_K(L, \overline{K})$, also $\tau_{|L} =$

σ_i für ein $i \in I$. Dies impliziert $\overline{\sigma}_i^{-1} \circ \tau_{|L} = \mathrm{id}_L$, aber natürlich ist $\overline{\sigma}_i^{-1} \circ \tau_{|L} = \left(\overline{\sigma}_i^{-1} \circ \tau\right)_{|L}$, also haben wir $\overline{\sigma}_i^{-1} \circ \tau \in \mathrm{Hom}_L(M, \overline{K})$. Dann gibt es also ein $j \in J$, so dass $\overline{\sigma}_i^{-1} \circ \tau = \tau_j$ ist, und dann erhalten wir

$$\tau = \overline{\sigma}_i \circ \tau_j,$$

wie gewünscht. □

Mit diesen Ergebnissen können wir zeigen, dass der Separabilitätsgrad benutzt werden kann, um festzustellen, ob eine Erweiterung separabel ist.

Satz 4.37. *Sei $L \supset K$ eine endliche Körpererweiterung, dann gilt:*

1. *Wenn L über K separabel ist, dann gilt $[L : K] = [L : K]_s$.*
2. *Falls $\mathrm{char}(K) = p > 0$ ist, gibt es ein $r \in \mathbb{N}$, so dass $[L : K] = p^r \cdot [L : K]_s$ gilt, insbesondere ist also $[L : K]_s$ ein Teiler von $[L : K]$ (und damit gilt stets, unabhängig von der Charakteristik von K, dass $[L : K]_s \leq [L : K]$ ist).*
3. *Wenn $[L : K] = [L : K]_s$ gilt, dann ist L separabel über K.*

Beweis. 1. Sei L über K separabel, d.h., alle $\alpha \in L$ sind Nullstellen separabler Polynome in K. Da L endlich über K ist, gilt insbesondere $L = K(a_1, \ldots, a_n)$ für gewisse Elemente $a_1, \ldots, a_n \in L$. Dann ist a_n auch separabel über $K(a_1, \ldots, a_{n-1})$, und es gilt wegen Satz 4.35, Punkt 2., dass $[K(a_1, \ldots, a_n) : K(a_1, \ldots, a_{n-1})]_s = [K(a_1, \ldots, a_n) : K(a_1, \ldots, a_{n-1})]$ ist. Aus den Gradsätzen (Satz 4.3 und Satz 4.36) folgt dann induktiv, dass $[L : K] = [L : K]_s$ gilt.

2. Wir wenden Satz 4.35, Punkt 3., induktiv auf die einfachen Erweiterungen $K(a_1, \ldots, a_{i+1}) \supset K(a_1, \ldots, a_i)$ an.

3. Falls $\mathrm{char}(K) = 0$ ist, dann ist K perfekt und jede Erweiterung separabel. Sei also $\mathrm{char}(K) = p > 0$. Sei $a \in L$ und $f = \mathrm{MinPol}_K(a) \in K[x]$. Wir haben zu zeigen, dass die Vielfachheit der Nullstelle a von f in einem algebraischen Abschluss $\overline{K}$ gleich Eins ist. Wie wir im Lemma 4.33 gesehen haben, gibt es ein maximales $r \in \mathbb{N}$, so dass diese Multiplizität gleich p^r ist. Dann gilt nach Satz 4.35, Punkt 3., dass

$$[K(a) : K] = p^r \cdot [K(a) : K]_s$$

ist. Dann haben wir

$$\begin{aligned} [L : K] &= [L : K(a)] \cdot [K(a) : K] \\ &\geq [L : K(a)]_s \cdot p^r [K(a) : K]_s \\ &= p^r \cdot [L : K]_s \end{aligned}$$

Hierbei folgt die erste Gleichung aus dem (gewöhnlichen) Gradsatz (Satz 4.3) und die letzte aus dem Gradsatz für den Separabilitätsgrad (Satz 4.36). Die Ungleichung folgt aus dem eben bewiesenen Punkt 2. Gilt also $[L : K] = [L : K]_s$, dann folgt $p^r = 1$, also ist die Multiplizität von a gleich Eins, d.h., f ist separabel.

□

Schließlich benötigen wir noch eine Aussage zur Transitivität der Separabilitätseigentschaft bei Zwischenkörpern.

Lemma 4.38. *Seien $K \subset L \subset M$ algebraische Körpererweiterungen, dann ist M separabel über K genau dann wenn, M über L und L über K separabel sind.*

Beweis. Falls $M \supset K$ separabel ist, dann auch die Erweiterungen $M \supset L$ und $L \supset K$, dies ergibt sich direkt aus der Definition der Separabilität (aus der Tatsache, dass jedes Element aus M Nullstelle eines separablen Polynoms aus $K[x]$ ist).
Seien also $M \supset L$ und $L \supset K$ separabel. Sei $a \in M$, dann wollen wir zeigen, dass a separabel über K ist. Sei $f = \mathrm{MinPol}_L(a) \in L[x]$, mit $f = a_n x^n + \ldots + a_0$. f ist ein separables Polynom, da die Erweiterung $M \supset L$ separabel ist. Wir betrachten den Zwischenkörper $L' := K(a_0, \ldots, a_n)$. Es ist dann auch die Erweiterung $L'(a) \supset L'$ separabel. Da $L' \subset L$ gilt und da $L \supset K$ separabel ist, muss auch $L' \supset K$ separabel sein. Dann erhalten wir

$$\begin{aligned} [L'(a) : K]_s &= [L'(a) : L']_s \cdot [L' : K]_s \qquad \text{wegen Satz 4.36} \\ &= [L'(a) : L'] \cdot [L' : K] \qquad \text{wegen Satz 4.37} \\ &= [L'(a) : K] \qquad \text{wegen Satz 4.3.} \end{aligned}$$

Aus Satz 4.36, angewendet auf die Erweiterung $L'(a) \supset K$ folgt dann, dass diese separabel ist, und daher ist das Element a separabel über K, wie gewünscht. □

Für den Satz vom primitiven Element, welcher das Ziel dieses Abschnitts ist, benötigen wir noch (mit den jetzt zur Verfügung stehenden Hilfsmitteln einfache) Aussage über endliche Körper.

Lemma 4.39. *Sei K ein Körper und $G < K^*$ eine* endliche *Untergruppe der Einheitengruppe von K. Dann ist G zyklisch, d.h., es gibt ein $\alpha \in \mathbb{N}_{>0}$ mit $G \cong \mathbb{Z}/\alpha\mathbb{Z}$. Insbesondere ist K^* zyklisch, falls K ein endlicher Körper ist.*

Beweis. Die Gruppe G ist nach Voraussetzung endlich und abelsch. Dann liefert uns Satz 3.54 (siehe auch die Bemerkung nach dem Beweis dieses Satzes), dass es einen Isomorphismus

$$G \cong \bigoplus_{i=1}^{n} \frac{\mathbb{Z}}{\alpha_i \mathbb{Z}}$$

von abelschen Gruppen gibt, so dass $\alpha_i | \alpha_{i+1}$ für alle $i \in \{1, \ldots, n-1\}$ gilt. Dann gilt für alle $a \in G$, dass die Ordnung $\mathrm{ord}(a)$ ein Teiler von α_n sein muss, mit anderen Worten, alle $a \in G$ erfüllen die Gleichung $a^{\alpha_n} - 1 = 0$. Noch einmal anders ausgedrückt bedeutet dies, dass alle $a \in G \subset K$ Nullstellen des Polynoms $x^{\alpha_n} - 1 \in K[x]$ sind. Es gilt aber natürlich $|G| = \sum_{i=1}^{n} \alpha_i$, aber das Polynom $x^{\alpha_n} - 1$ hat nur α_n viele Nullstellen, es muss daher $n = 1$ sein. Wir setzen $\alpha := \alpha_n$ und erhalten, dass $G \cong \mathbb{Z}/\alpha\mathbb{Z}$ zyklisch ist. □

Mit all diesen Vorbereitungen können wir jetzt den wichtigen Satz vom primitiven Element formulieren und beweisen.

Satz 4.40 (Satz vom primitiven Element)**.** *Sei $L \supset K$ eine endliche und separable Körpererweiterung. Dann existiert ein primitives Element, d.h., ein Element $a \in L$, so dass $L = K(a)$ ist.*

Beweis. Zuerst betrachten wir den Fall, dass K endlich ist. Da wir $[L : K] < \infty$ vorausgesetzt haben, ist dann auch L endlich, und wegen dem letzten Lemma (Lemma 4.39) ist dann L^* zyklisch, also erzeugt von einem Element α. Dann gilt natürlich $L = K(\alpha)$.
Sei nun also $|K| = \infty$. Da L endlich über K ist, wissen wir nach Satz 4.10, dass $L = K(a_1, \ldots, a_n)$ gilt. Per Induktion reicht es also, zu zeigen, dass für alle $a, b \in L$ die Erweiterung $K(a, b) \supset K$ ein primitives Element besitzt. Da $L \supset K$ separabel ist, ist auch die Erweiterung $K(a, b) \supset K$ separabel, es gilt also

$$[K(a, b) : K] = [K(a, b) : K]_s =: n$$

Sei $\mathrm{Hom}_K(K(a, b), \overline{K}) = \{\sigma_1, \ldots, \sigma_n\}$. Definiere das Polynom

$$P = \prod_{i \neq j} ((\sigma_i(a) - \sigma_j(a)) - (\sigma_i(b) - \sigma_j(b)) \cdot x) \in \overline{K}[x]$$

Wir zeigen zunächst, dass P nicht das Nullpolynom ist: Für Indizies $i, j \in \{1, \ldots, n\}$ mit $i \neq j$ gilt $\sigma_i \neq \sigma_j$, also muss $\sigma_i(a) \neq \sigma_j(a)$ oder $\sigma_i(b) \neq \sigma_j(b)$ sein, und der entsprechende Linearfaktor in P ist daher nicht gleich Null. Nun besitzt K unendlich viele Elemente, es gilt also ein $c \in K$ mit $P(c) \neq 0$. Für alle Paare von Indizes i, j mit $i \neq j$ gilt dann $((\sigma_i(a) - \sigma_j(a)) - (\sigma_i(b) - \sigma_j(b)) \cdot c) \neq 0$, d.h.

$$\sigma_i(a + c \cdot b) \neq \sigma_j(a + c \cdot b).$$

Sei $f = \mathrm{MinPol}_K(a + c \cdot b) \in K[x]$, so folgt aus Satz 4.35, dass die n paarweise verschiedenen Werte $\{\sigma_i(a + c \cdot b)\}_{i=1,\ldots,n}$ Nullstellen von f sind, also insbesondere, dass $\deg(f) \geq n$ ist. Damit erhalten wir die folgende Abschätzung:

$$[K(a,b) : K]_s = n \leq \deg(f) = [K(a + c \cdot b) : K] \leq [K(a,b) : K],$$

die letzte Abschätzung folgt dabei einfach aus $K(a + c \cdot b) \subset K(a,b)$. Weil die Erweiterung $K(a,b) \supset K$ aber separabel ist, gilt $[K(a,b) : K]_s = [K(a,b) : K]$, und daher erhalten wir $[K(a + c \cdot b) : K] = [K(a,b) : K]$, somit also $K(a + c \cdot b) = K(a,b)$, und wir haben damit das primitive Element $a + c \cdot b$ gefunden. □

4.3 Konstruktion endlicher Körper

Als Anwendung der bisher erreichten Resultate über Körpererweiterungen wollen wir hier alle endlichen Körper klassifizieren. Endliche Körper spielen in vielen Anwendungen der Algebra eine zentrale Rolle, z.B. in der Kryptologie und der Codierungstheorie.
Wir haben bereits in der Bemerkung nach Lemma 3.21 die endlichen Körper $\mathbb{F}_p$, deren zugrundeliegende abelsche Gruppe der Quotient $\mathbb{Z}/p\mathbb{Z}$ ist, kennengelernt. Der folgende Satz beschreibt alle anderen endlichen Körper.

Satz 4.41. *Sei $\mathbb{F}$ ein Körper mit $|\mathbb{F}| < \infty$, dann ist $\mathrm{char}(\mathbb{F}) = p > 0$, und es gibt ein $n \in \mathbb{N}$ mit $|\mathbb{F}| = q := p^n$. $\mathbb{F}$ ist Zerfällungskörper von $f = x^q - x \in \mathbb{F}_p[x]$ und daher ist die Erweiterung $\mathbb{F} \supset \mathbb{F}_p$ normal.*

Beweis. Falls $\mathrm{char}(\mathbb{F}) = 0$ ist, dann muss $\mathbb{Z}$ ein Unterring von $\mathbb{F}$ sein, und dann wäre $\mathbb{F}$ nicht endlich. Also ist $\mathrm{char}(\mathbb{F}) = p$, für eine Primzahl p, und es gibt eine Inklusion von Körpern $\mathbb{F}_p \hookrightarrow \mathbb{F}$. Dann kann man aber $\mathbb{F}$ als Körpererweiterung von $\mathbb{F}_p$ auffassen, und diese ist natürlich endlich, weil ja $\mathbb{F}$ selbst endlich ist. Also ist $[\mathbb{F} : \mathbb{F}_p] = n < \infty$, und $\mathbb{F}$ ist ein $\mathbb{F}_p$-Vektorraum der Dimension n, somit enthält $\mathbb{F}$ genau $q = p^n$-viele Elemente.
Es folgt, dass $\mathbb{F}^*$ genau $q - 1$ Elemente hat, daher ist die Ordnung jedes dieser Elemente ein Teiler von $q - 1$, mit anderen Worten, alle $a \in \mathbb{F}^*$ sind Nullstellen von $x^{q-1} - 1 \in \mathbb{F}_p[x]$. Daher sind alle Elemente aus $\mathbb{F}$ Nullstellen von $x^q - x \in \mathbb{F}_p[x]$ und es gibt auch keine weiteren Nullstellen. Daher zerfällt $x^q - x$ über $\mathbb{F}$ in Linearfaktoren, und damit ist $\mathbb{F}$ der Zerfällungskörper von f. □

Wir zeigen nun umgekehrt, dass für jede Potenz $q = p^n$ einer Primzahl p auch ein Körper mit q Elementen existiert.

Satz 4.42. *Sei p eine Primzahl. Dann existiert für alle $n \in \mathbb{N}_{>0}$ ein Erweiterungskörper mit $q := p^n$-Elementen, genannt $\mathbb{F}_q$. Dieser ist bis auf Isomorphie eindeutig bestimmt, nämlich als der Zerfällungskörper von $f := x^q - x \in \mathbb{F}_p[x]$.*

Beweis. Wir haben schon in den Beispielen nach Lemma 4.30 gesehen, dass f separabel ist, d.h., dass es in einem algebraischen Abschluß $\overline{\mathbb{F}}_p$ keine mehrfachen Nullstellen hat. Nun sieht man leicht, dass die Menge aller Nullstellen von f einen Körper bildet: Falls a und b Nullstellen von f sind, dann ist nach Lemma 4.32

$$(a \pm b)^q = a^q \pm b^q = a \pm b$$

also sind $a + b$ und $a - b$ wieder Nullstellen von f. Natürlich sind auch ab sowie ab^{-1} Nullstellen von f, wie man durch Einsetzen sofort nachrechnet. Die Menge der Nullstellen von f in $\overline{\mathbb{F}}_p$ ist also ein Körper, und es

ist offensichtlich der Zerfällungskörper von f. Falls nun ein beliebiger endlicher Körper $\mathbb{F}$ gegeben ist (d.h., wie im letzten Satz erklärt wurde, eine Körpererweiterung $\mathbb{F} \supset \mathbb{F}_p$), dann ist nach dem letzten Satz $\mathbb{F}$ ein Zerfällungskörper von $x^q - x$ mit $q := p^{[\mathbb{F}:\mathbb{F}_p]}$, und dieser ist bis auf Isomorphie eindeutig (siehe Korollar 4.25), also haben wir $\mathbb{F} \cong \mathbb{F}_q$. □

Als Anwendung dieser Ergebnisse können wir Erweiterungen endlicher Körper klassifizieren und insbesondere zeigen, dass diese perfekt sind.

Korollar 4.43. *Sei p eine Primzahl und $\overline{\mathbb{F}}_p$ ein algebraischer Abschluss von $\mathbb{F}_p$. Sei $n \in \mathbb{N}$, dann existiert ein injektiver Körperhomomorphismus $\mathbb{F}_{p^n} \hookrightarrow \overline{\mathbb{F}}_p$, mit eindeutig bestimmtem (d.h. nicht von der Wahl des Homomorphismus abhängendem) Bild. Dieses bezeichnen wir auch mit $\mathbb{F}_{p^n}$. Dann gilt: $\mathbb{F}_{p^n} \subset \mathbb{F}_{p^m}$ genau dann, wenn $n|m$ gilt. Die einzigen endlichen Erweiterungen (bis auf Isomorphie) der Körper $\mathbb{F}_{p^n}$ sind die Körper $\mathbb{F}_{p^m}$ mit $n|m$.*

Beweis. Zum Beweis der ersten Aussage verwenden wir Satz 4.21, angewandt auf den kanonischen Homomorphismus $\mathbb{F}_p \hookrightarrow \overline{\mathbb{F}}_p$ und die Erweiterung $\mathbb{F}_{p^n} \supset \mathbb{F}_p$. Es folgt, dass es einen (injektiven) Körperhomomorphismus $\mathbb{F}_{p^n} \hookrightarrow \overline{\mathbb{F}}_p$ gibt. Die Erweiterung $\mathbb{F}_{p^n} \supset \mathbb{F}_p$ ist normal, daher ist das Bild dieses Homomorphismus eindeutig bestimmt (dies folgt aus Satz 4.24).
Sei jetzt $\mathbb{F}_{p^n} \subset \mathbb{F}_{p^m}$, und sei $r := [\mathbb{F}_{p^m} : \mathbb{F}_{p^n}]$, dann ist $p^m = |\mathbb{F}_{p^m}| = |\mathbb{F}_{p^n}|^r = p^{r \cdot n}$, also haben wir $n|m$. Sei andererseits $m = n \cdot r$, dann müssen wir $\mathbb{F}_{p^n} \subset \mathbb{F}_{p^m}$ zeigen. Sei $a \in \mathbb{F}_{p^n}$, dann gilt $a^{p^n} = a$ (zur Erinnerung: $\mathbb{F}_{p^n}$ besteht genau aus allen Nullstellen von $x^{p^n} - x \in \mathbb{F}_p[x]$). Dann kann man aber induktiv (Induktion über r) zeigen, dass auch $a^{p^{r \cdot n}} = a$ gilt, also ist a auch Nullstelle von $x^{p^m} - x = 0$, und daher gilt $a \in \mathbb{F}_{p^m}$.
Seien ganz allgemein $\mathbb{F}, \mathbb{F}'$ endliche Körper und $\mathbb{F}' \supset \mathbb{F}$ eine Erweiterung. Dann liefert uns wieder Satz 4.21, dass die Einbettung $\mathbb{F}_p \hookrightarrow \overline{\mathbb{F}}_p$ eine Fortsetzung $\mathbb{F} \hookrightarrow \overline{\mathbb{F}}_p$ und diese eine Fortsetzung $\mathbb{F}' \hookrightarrow \overline{\mathbb{F}}_p$ hat, d.h., modulo Isomorphie kann man jede Erweiterung $\mathbb{F} \subset \mathbb{F}'$ als Erweiterung von Unterkörpern von $\overline{\mathbb{F}}_p$ auffassen, und dann ist man wieder in der oben betrachteten Situation $\mathbb{F}_{p^m} \supset \mathbb{F}_{p^n}$ für $n|m$. □

Korollar 4.44. *Sei K endlich und $L \supset K$ eine algebraische Erweiterung, dann ist L normal und separabel. Insbesondere sind alle endlichen Körper perfekt.*

Beweis. Wir wissen aus Satz 4.42, dass $K \cong \mathbb{F}_q$ mit $q = p^n$ für eine Primzahl p ist. Wir betrachten zunächst den Fall, dass die Erweiterung $L \supset K$ endlich ist. Wegen dem letzten Korollar (Korollar 4.43) ist dann $L \cong \mathbb{F}_{q'}$ mit $q' = p^m$ und $n|m$. Nach Konstruktion in Satz 4.41 ist $\mathbb{F}_{q'}$ der Zerfällungskörper von $x^{q'} - x \in \mathbb{F}_p[x]$. Wir können aber natürlich $x^{q'} - x$ auch als Element von $\mathbb{F}_q[x]$ auffassen, und dann ist also $\mathbb{F}_{q'}$ ein Zerfällungskörper eines Polynoms aus $\mathbb{F}_q[x]$, insbesondere ist also die Erweiterung $L \supset K$ normal. Andererseits ist $x^{q'} - x$ separabel (seine Ableitung ist gleich 1 in $K[x]$), und daher ist $L \supset K$ auch separabel. Ist nun $L \supset K$ eine beliebige algebraische Erweiterung, dann kann man L als Vereinigung

$$L = \bigcup_{\substack{L' \subset L \\ L' \supset K \text{ endlich}}} L'$$

schreiben, und da alle Erweiterungen $L' \supset K$, wie oben gesehen, normal und separabel sind, müssen alle Elemente aus L separabel über K sein. Also ist $L \supset K$ separabel, und die Normalität folgt aus Lemma 4.26. □

Wir wollen zum Abschluss diesen Abschnittes noch die Automorphismen der Körper $\mathbb{F}_{p^m}$ genauer studieren. Ganz allgemein bezeichnen wir für eine Körpererweiterung $L \supset K$ mit

$$\mathrm{Aut}_K(L) := \left\{\sigma \in \mathrm{Aut}(L) \mid \sigma_{|K} = \mathrm{id}_K\right\}$$

die Gruppe (mit der Komposition als Verknüpfung) der K-Automorphismen von L, also der Körperautomorphismen von L, welche auf K die Identität sind. Wir werden im nächsten Kapitel Gruppen dieser Art noch intensiv studieren.

Seien wie oben $n, m \in \mathbb{N}$ mit $m = n \cdot r$, und $q = p^n$, $q' = p^m$, dann ist $\mathbb{F}_{q'} \supset \mathbb{F}_q$ eine endliche Körpererweiterung vom Grad r. Wir betrachten die Gruppe $\mathrm{Aut}_{\mathbb{F}_q}(\mathbb{F}_{q'})$. Wir wissen, dass $\mathbb{F}_{q'} \supset \mathbb{F}_q$ eine normale Körpererweiterung ist, also gilt nach Lemma 4.26

$$\mathrm{Aut}_{\mathbb{F}_q}(\mathbb{F}_{q'}) = \mathrm{Hom}_{\mathbb{F}_q}\left(\mathbb{F}_{q'}, \overline{\mathbb{F}}_q\right).$$

Andererseits ist $\mathbb{F}_{q'} \supset \mathbb{F}_q$ auch separabel, daher haben wir

$$\mathrm{ord}\left(\mathrm{Aut}_{\mathbb{F}_q}(\mathbb{F}_{q'})\right) = [\mathbb{F}_{q'} : \mathbb{F}_q]_s = [\mathbb{F}_{q'} : \mathbb{F}_q] = r$$

Sei wie oben $\sigma : \mathbb{F}_{q'} \to \mathbb{F}_{q'}; a \mapsto a^p$ der Frobeniushomomorphismus von $\mathbb{F}_{q'}$. Dann haben wir die folgende Aussage:

Satz 4.45. *Die Gruppe* $\mathrm{Aut}_{\mathbb{F}_q}(\mathbb{F}_{q'})$ *ist zyklisch, mit* $\mathrm{ord}\left(\mathrm{Aut}_{\mathbb{F}_q}(\mathbb{F}_{q'})\right) = r$ *und Erzeuger* σ^n *(genannt der relative Frobenius-Homomorphismus über* $\mathbb{F}_q$*).*
Insbesondere ist für den Fall $n = 1$ *(d.h.* $q = p$*) die Gruppe* $\mathrm{Aut}_{\mathbb{F}_p}(\mathbb{F}_{p^m})$ *zyklisch der Ordnung* m*, und wird vom (absoluten) Frobenius-Homomorphismus* $\sigma : \mathbb{F}_{p^m} \to \mathbb{F}_{p^m}$ *erzeugt.*

Beweis. Nach Definition ist σ^n ein Element von $\mathrm{Aut}_{\mathbb{F}_p}(\mathbb{F}_{q'})$. Darüber hinaus gilt aber für alle $a \in \mathbb{F}_q$, dass

$$\sigma^n(a) = \underbrace{\sigma(\sigma(\ldots\sigma(}_{n\text{-mal}}(a)\ldots) = \underbrace{(\ldots(}_{n\text{-mal}}a)^p)\ldots)^p = a^q \overset{a\in\mathbb{F}_q}{=} a$$

d.h., $\sigma^n_{|\mathbb{F}_q} = \mathrm{id}_{\mathbb{F}_q}$. Also gilt sogar $\sigma^n \in \mathrm{Aut}_{\mathbb{F}_q}(\mathbb{F}_{q'})$. Wir wollen jetzt zeigen, dass $\mathrm{ord}(\sigma^n) = r$ gilt, dann ist wegen $\mathrm{ord}\left(\mathrm{Aut}_{\mathbb{F}_q}(\mathbb{F}_{q'})\right) = r$ diese Gruppe zyklisch und σ^n ist ein Erzeuger.
Zunächst gilt für alle Elemente $a \in \mathbb{F}_{q'}$

$$\left(\sigma^n\right)^r(a) = \sigma^m(a) = a^{q'} = a,$$

d.h., es ist $(\sigma^n)^r = \mathrm{id}_{\mathbb{F}_{q'}}$. Wenn wir also $\mu := \mathrm{ord}(\sigma^n)$ setzen, dann gilt $\mu | r$. Aus $(\sigma^n)^\mu = \mathrm{id}_{\mathbb{F}_{q'}}$ folgt, dass für alle $a \in \mathbb{F}_{q'}$ die Gleichung $a^{p^{n\cdot\mu}} = a$ gilt. Also sind alle $a \in \mathbb{F}_{q'}$ Nullstellen des Polynoms $x^{p^{n\cdot\mu}} - x$. Dieses ist separabel, hat also $p^{n\cdot\mu}$ verschiedene Nullstellen. Daher ist die Anzahl der Elemente von $\mathbb{F}_{q'}$ kleiner oder gleich der Zahl $p^{n\cdot\mu}$, wir erhalten also $q' = p^m = p^{n\cdot r} \leq p^{n\cdot\mu}$, d.h. $r \leq \mu$. Damit muss also insgesamt $r = \mu$ gelten.

□

Kapitel 5

Galoistheorie

In diesem abschließenden Kapitel wollen wir die Krönung der klassischen Algebra, nämlich die Galoistheorie studieren. Wir werden den zentralen Begriff der Galoisgruppe kennenlernen, und den Hauptsatz der Galoistheorie beweisen, welcher eine Korrespondenz zwischen Untergruppen der Galoisgruppe und gewissen Zwischenkörpern einer Körpererweiterung herstellt. Als Anwendung werden wir das ganz am Anfang gestellte Problem der Auflösbarkeit algebraischer Gleichungen studieren. Desweiteren werden wir den schon mehrfach angekündigten Fundamentalsatz der Algebra mit galoistheoretischen Methoden beweisen.

5.1 Der Hauptsatz der Galoistheorie und der Fundamentalsatz der Algebra

Wir beginnen mit der Definition einer Galoiserweiterung und der Galoisgruppe. Letztere haben wir (unter anderem Namen) eigentlich schon im letzten Abschnitt diskutiert haben.

Definition 5.1. *Sei $K \subset L$ eine Körpererweiterung. Sie heißt eine* Galoiserweiterung *oder* galoissch*, falls sie normal und separabel ist. In diesem Fall nennen wir die Gruppe* $\mathrm{Aut}_K(L)$ *die Galoisgruppe der Erweiterung, geschrieben* $\mathrm{Gal}(L/K)$*.*

Nach der ausführlichen Diskussion von endlichen Körpern im letzten Kapitel können wir ein Beispiel für eine Galoiserweiterung sofort angeben: Sei p eine Primzahl, $n \in \mathbb{N}$ und $q = p^n$, dann ist jede algebraische Erweiterung $\mathbb{F} \supset \mathbb{F}_q$ normal und separabel und daher eine Galoiserweiterung. Ist $\mathbb{F}$ auch endlich, dann ist

$$\mathrm{Gal}(\mathbb{F}/\mathbb{F}_q) = \mathrm{Aut}_{\mathbb{F}_q}(\mathbb{F}) = \langle \sigma^n \rangle$$

zyklisch mit $\mathrm{ord}(\mathrm{Gal}(\mathbb{F}/\mathbb{F}_q)) = [\mathbb{F} : \mathbb{F}_q]$, der Erzeuger ist der relative Frobenius-Homomorphismus von $\mathbb{F}$ über $\mathbb{F}_q$.
Ein weiteres wichtiges Beispiel ist der Fall $L = K(a_1, \ldots, a_n)$, wobei L der Zerfällungskörper eines irreduziblen Polynoms $f \in K[x]$ mit den Nullstellen $a_1, \ldots, a_n$ sein soll. Dann folgt wie im Beweis von Satz 4.24, dass jedes $\sigma \in \mathrm{Gal}(L/K)$ sich zu einer Bijektion $\sigma_{|\{a_1,\ldots,a_n\}} : \{a_1, \ldots, a_n\} \to \{a_1, \ldots, a_n\}$ einschränkt, dies liefert eine Abbildung $\mathrm{Gal}(L/K) \to S_n$. L wird von $a_1, \ldots, a_n$ erzeugt wird, und jedes $\sigma \in \mathrm{Gal}(L/K)$ ist auf K die Identität, falls also σ auch auf der Menge $\{a_1, \ldots, a_n\}$ die Identität ist, dann gilt $\sigma = \mathrm{id}_L$. Also ist die Abbildung $\mathrm{Gal}(L/K) \to S_n$ injektiv. Für Zerfällungskörper eines einzelnen Polynoms können wir uns die Galoisgruppe also immer als eine Untergruppe der symmetrischen Gruppe vorstellen.
Ein zentraler Teil der Galoistheorie ist das Studium von Zwischenkörpern einer gegebenen Erweiterung. Hierzu haben wir die folgende erste Aussage.

Satz 5.2. *Sei $L \supset K$ eine Galoiserweiterung, und E ein Zwischenkörper, dann gilt:*

1. *Die Erweiterung $L \supset E$ ist ebenfalls Galoissch, und die Galoisgruppe* $\mathrm{Gal}(L/E)$ *ist eine Untergruppe von* $\mathrm{Gal}(L/K)$*.*

2. *Falls auch $E \supset K$ eine Galoiserweiterung ist, dann gilt für alle $\tau \in \mathrm{Gal}(L/K)$, dass die Einschränkung $\tau_{|E}$ ein K-Automorphismus von E ist, also ein Element von $\mathrm{Gal}(E/K)$. Die Abbildung*

$$\begin{array}{ccc} \mathrm{Gal}(L/K) & \longrightarrow & \mathrm{Gal}(E/K) \\ \tau & \longmapsto & \tau_{|E} \end{array}$$

ist ein surjektiver Gruppenhomomorphismus.

Beweis. 1. Wir haben zu zeigen, dass $L \supset E$ normal und separabel ist. Beide Eigenschaften haben wir schon gezeigt, nämlich die Normalität in Lemma 4.26 (und der Bemerkung danach), und die Separabilität in Lemma 4.38.

Ein Element in $\mathrm{Gal}(L/E)$ ist ein E-Automorphismus von L, aber dieser ist natürlich insbesondere die Identität auf K, d.h. in natürlicher Weise ein K-Automorphismus von L. Daher ist haben wir $\mathrm{Gal}(L/E) < \mathrm{Gal}(L/K)$.

2. Nach Voraussetzung ist die Erweiterung $E \supset K$ normal, also ist nach Lemma 4.26 jeder K-Homomorphismus $E \to \overline{E}$ ein K-Automorphismus von E. Insbesondere können wir für ein Element $\tau \in \mathrm{Gal}(L/K)$ die Einschränkung $\tau_{|E} : E \to L \subset \overline{E}$ betrachten, diese erfüllt also $\mathrm{Im}(\tau_{|E}) = E$, und ist also ein Element von $\mathrm{Gal}(E/K)$. Dies definiert eine Abbildung (welche natürlich ein Gruppenhomomorphismus ist) $\mathrm{Gal}(L/K) \to \mathrm{Gal}(E/K)$. Wir haben noch die Surjektivität zu prüfen. Sei also $\sigma \in \mathrm{Gal}(E/K)$ gegeben. Dann existiert nach Satz 4.21 eine Hochhebung $\sigma' : L \to \overline{E}$, welche ein K-Homomorphismus ist (also $\sigma' \in \mathrm{Hom}_K(L, \overline{E})$) da aber auch $L \supset K$ normal ist, folgt wieder $\sigma' \in \mathrm{Aut}_K(L)$. Natürlich ist nach Konstruktion $\sigma'_{|E} = \sigma$, also ist die oben definierte Abbildung $\mathrm{Gal}(L/K) \to \mathrm{Gal}(E/K); \tau \mapsto \tau_{|E}$ surjektiv.

□

Für endliche Galoiserweiterungen können wir die Ordnung der Galoisgruppe mit bereits bekannten Zahlen in Verbindung bringen.

Satz 5.3. *Sei $L \supset K$ eine endliche und normale Körpererweiterung, dann ist*

$$\mathrm{ord}\,(\mathrm{Aut}_K(L)) = [L : K]_s \leq [L : K]$$

Damit ist $\mathrm{ord}\,(\mathrm{Aut}_K(L)) = [L : K]$ *genau dann, wenn $L \supset K$ separabel ist, insbesondere gilt für Galoiserweiterungen $L \supset K$ immer die Gleichheit* $\mathrm{ord}(\mathrm{Gal}(L/K)) = [L : K]$.

Beweis. Für normale Erweiterungen $L \supset K$ gilt nach Lemma 4.26 $\mathrm{Aut}_K(L) = \mathrm{Hom}_K(L, \overline{L})$, aber die Ordnung letzterer Gruppe ist nach Definition genau der Separabilitätsgrad der Erweiterung $L \supset K$. Alle anderen Aussagen folgen dann aus Satz 4.37. □

Wir wollen jetzt den sogenannten Hauptsatz der Galoistheorie erarbeiten. Dazu benötigen wir zunächst das fundamentale Konzept des Fixkörpers einer Untergruppe der Galoisgruppe einer Erweiterung.

Definition 5.4. *Sei L ein Körper und $G < \mathrm{Aut}\,(L)$. Dann heißt die Menge*

$$L^G := \{a \in L \,|\, \sigma(a) = a \; \forall \sigma \in G\}$$

der Fixkörper *von G (man rechnet sofort nach, dass L^G tatsächlich ein Körper ist).*

Die erste Aussage über den Fixkörper einer gegebenen Gruppe ist die folgende. Man beachte, dass der Satz vom primitiven Element (4.40) im Beweis verwendet wird, daher gehen implizit viele der Konstruktionen des letzten Kapitels hier ein.

Satz 5.5. *Sei L ein Körper und $G < \mathrm{Aut}\,(L)$. Sei G endlich oder $L \supset L^G$ algebraisch. Dann ist $L \supset L^G$ eine Galoiserweiterung. Falls G endlich ist, dann ist auch $[L : L^G] < \infty$, es gilt* $\mathrm{Gal}(L/L^G) = G$ *und* $[L : L^G] = \mathrm{ord}(G)$.
Ist G unendlich, so ist auch $[L : L^G] = \infty$, und wir haben $G < \mathrm{Gal}(L/L^G)$.

Beweis. Zunächst zeigen wir, dass $L \supset L^G$ separabel ist. Wir müssen für jedes $a \in L$ ein separables Polynom $f \in L^G[x]$ mit $f(a) = 0$ finden. Wir betrachten die Menge $M := \{\sigma(a) \,|\, \sigma \in G\}$. Wir zeigen zunächst die folgende Hilfsaussage: In beiden Fällen (G endlich bzw. $L \supset L^G$ algebraisch) existieren $\sigma_1, \ldots, \sigma_r \in G$, so dass $M = \{\sigma_1(a), \ldots, \sigma_r(a)\}$ ist. Im Fall $\mathrm{ord}(G) < \infty$ ist dies offensichtlich. Falls $\mathrm{ord}(G) = \infty$, aber $L \supset L^G$ algebraisch ist, argumentiert man wie folgt: Für jedes $\sigma \in G$ ist nach Definition $\sigma_{|L^G} = \mathrm{id}_{L^G}$, insbesondere ist für $h \in L^G[x]$ dann $h^\sigma = h$. Daher liefert uns Lemma 4.20, dass $\sigma(a)$ Nullstelle von $\mathrm{MinPol}_{L^G}(a)$ ist. Sei $r = \deg(\mathrm{MinPol}_{L^G}(a))$, dann muss es also $\sigma_1, \ldots, \sigma_r \in G$ geben, so dass $M = \{\sigma_1(a), \ldots, \sigma_r(a)\}$ gilt. Damit ist die Hilfsaussage bewiesen.
Da $\mathrm{id} \in G$ und $\mathrm{id}(a) = a$ ist, haben wir insbesondere $a \in \{\sigma_1(a), \ldots, \sigma_r(a)\}$. Somit ist a Nullstelle von

$$f := \prod_{i=1}^{r}(x - \sigma_i(a)) \in L[x].$$

Da aber für alle $\sigma \in G$ die Einschränkung $\sigma_{|M}$ eine Bijektion der Menge $M = \{\sigma_1(a), \ldots, \sigma_r(a)\}$ auf sich selbst ist, folgt, dass für alle $\sigma \in G$

$$f^\sigma = \prod_{i=1}^{r}(x - \sigma \circ \sigma_i(a)) = f$$

ist. Daher ist f ein Element von $L^G[x]$. Natürlich ist f separabel, dies zeigt, dass a separabel über L^G ist. Die Körpererweiterung $L \supset L^G$ muss aber auch normal sein, denn man kann alle Polynome (in $L^G[x]$) der Form $\prod_{i=1}^{r}(x - \sigma_i(a))$ für alle $a \in L$ und wie oben konstruierte $\sigma_1, \ldots, \sigma_r$ (abhängig von a) betrachten, und dann ist L der Zerfällungskörper aller dieser Polynome, wie man leicht sieht (per Definition zerfallen diese Polynome über L in Linearfaktoren, und falls der Zerfällungskörper aller solcher Polynome kleiner als L wäre, dann konstruiert man für ein $a \in L$, welches nicht im Zerfällungskörper liegt, wieder ein Polynom wie oben, dies führt zum Widerspruch). Damit haben wir gezeigt, dass $L \supset L^G$ eine Galoiserweiterung ist.
Wir nehmen nun an, dass G endlich ist und setzten $n := \mathrm{ord}(G)$. Wir wollen zeigen, dass die Erweiterung $L \supset L^G$ dann auch endlich ist. Sei zunächst E ein Zwischenkörper dieser Erweiterung, also $L^G \subset E \subset L$, und zwar so dass $E \supset L^G$ endlich ist. Natürlich ist $E \supset L^G$ auch separabel (weil jedes Element von L separabel über L^G ist, wie gerade gezeigt). Damit wissen wir nach dem Satz vom primitiven Element (Satz 4.40), dass $E = L^G(a)$ für ein $a \in E$ gilt. Dann haben wir $[E : L^G] = \deg(\mathrm{MinPol}_{L^G}(a))$. Dieses Minimalpolynom ist aber in jedem Fall ein Teiler des oben konstruierten Polynoms f, also ist $[E : L^G] \leq \mathrm{ord}(G) = n$. Somit ist für alle Zwischenkörper E von $L^G \subset L$, welche endlich über L^G sind, der Grad $[E : L^G]$ nach oben beschränkt (nämlich durch die Ordnung der Gruppe G). Sei daher E so ein Zwischenkörper, so dass $[E : L^G]$ maximal ist. Dann muss für alle $a \in L$ $[E(a) : L^G] \leq [E : L^G]$ gelten (weil natürlich auch $[E(a) : L^G]$ endlich ist), aber dies bedeutet $E(a) = E$. Da dies für alle $a \in L$ erfüllt ist, folgt $L = E$, und dies liefert die Endlichkeit von L über L^G. Außerdem folgt aus diesem Argument, dass $[L : L^G] \leq n$ gilt. Wir wissen aber, dass G alle Elemente aus L^G fixiert, d.h. es gilt $G < \mathrm{Gal}(L/L^G)$. Damit folgt

$$n = \mathrm{ord}(G) \leq \mathrm{ord}\left(\mathrm{Gal}(L/L^G)\right) = [L : L^G] \leq n$$

und dies beweist die gewünschte Gleichung $n = [L : L^G]$ sowie $G = \mathrm{Gal}(L/L^G)$.
Falls G nicht endlich ist, gilt natürlich immer noch $G < \mathrm{Gal}(L/L^G)$, aber eine Galoiserweiterung, deren Galoisgruppe nicht endlich ist, kann keine endliche Erweiterung sein (man kann z.B. zeigen, dass es endliche Zwischenkörper beliebig hohen Grades gibt). □

Wir zeigen jetzt, dass man eine beliebige normale Erweiterung immerin zwei Teile zerlegen kann, von denen eine Galoissch, also separabel ist. Für den anderen Teil führen wir einen neuen Begriff ein.

Definition 5.6. *Sei $L \supset K$ eine algebraische Erweiterung, dann heißt diese* rein inseparabel, *falls $[L : K]_s = 1$ gilt.*

Damit haben wir folgendes Ergebnis.

Satz 5.7. *Sei $L \supset K$ eine normale Erweiterung, und setzte $G := \mathrm{Aut}_K(L)$. Dann gilt:*

1. *$L \supset L^G$ ist eine Galoiserweiterung mit $\mathrm{Gal}(L/L^G) = G$.*
2. *$L^G \supset K$ ist rein inseparabel.*
3. *Ist $L \supset K$ separabel, d.h., galoissch, dann ist $L^G = K$.*

Beweis. 1. Wir benutzen den letzten Satz (Satz 5.5), für den Spezialfall $G = \mathrm{Aut}_K(L)$. Wir haben gesehen, dass immer $G < \mathrm{Aut}_{L^G}(L)$ gilt. Andererseits ist wegen $K \subset L^G$ natürlich $\mathrm{Aut}_{L^G}(L) \subset \mathrm{Aut}_K(L)$, dies liefert die Gleichheit $G = \mathrm{Aut}_K(L) \stackrel{!}{=} \mathrm{Gal}(L/L^G)$, unabhängig davon, ob diese Gruppe endlich oder unendlich ist.

2. Zur Erinnerung: Der Separabilitätsgrad $[L^G : K]_s$ ist definiert als die Anzahl der Elemente der Gruppe $\mathrm{Hom}_K(L^G, \overline{K})$, und wir haben zu zeigen, dass diese Gruppe nur ein Element enthält, dass also die Identität auf L^G der einzige K-Homomorphismus von L^G nach $\overline{K}$ ist. Sei $\sigma \in \mathrm{Hom}_K(L^G, \overline{K})$ gegeben, dann folgt aus Satz 4.21, dass es eine Fortsetzung $\sigma' : L \to \overline{K}$ von σ gibt, aber wegen der Normalität von $L \supset K$ ist dann $\mathrm{Im}(\sigma') = L$, und wir haben $\sigma' \in \mathrm{Aut}_K(L)$. Wir wir eben im Punkt 1. gesehen haben, ist aber $\mathrm{Aut}_K(L) = \mathrm{Aut}_{L^G}(L)$, und damit muss $\sigma'_{|L^G} = \sigma = \mathrm{id}_{L^G}$ sein.

3. Falls $L \supset K$ Galoissch und damit separabel ist, dann sind alle Elemente aus L separabel über K, dann ist aber auch $L^G \supset K$ separabel. Wegen Punkt 2. haben wir dann
$$1 = [L^G : K]_s = [L^G : K]$$
und dies bedeutet, dass $K = L^G$ ist.

□

Wir kommen nun zur zentralen Aussage dieses Kapitels, welche einen Höhepunkt der gesamten Vorlesung darstellt. Wir beschränken uns aus Zeitgründen auf endliche Galoiserweiterungen, eine analoge Aussage existiert für den unendliche Fall, ist aber etwas komplizierter, weil man dann die Topologie der entsprechenden Galoisgruppe mit berücksichtigen muss.

Satz 5.8 (Hauptsatz der Galoistheorie)**.** *Sei $L \supset K$ eine endliche Galoiserweiterung und $G := \mathrm{Gal}(L/K)$. Wir definieren Abbildungen*

$$\{\text{Untergruppen von } G\} \underset{\Psi}{\overset{\Phi}{\rightleftarrows}} \{\text{Zwischenkörper von } L \supset K\}$$

$$H \longmapsto^{\Phi} L^H$$

$$\mathrm{Gal}(L/E) \longmapsto^{\Psi} E.$$

Dann sind Φ und Ψ bijektiv und invers zu einander.
Für eine Untergruppe $H < G$ ist der Fixkörper L^H genau dann eine normale (und damit Galoissche) Erweiterung von K, wenn H ein Normalteiler in G ist. In diesem Fall ist H der Kern des surjektiven Gruppenhomomorphismus

$$\begin{aligned} \varphi : G &\longrightarrow \mathrm{Gal}(L^H/K) \\ \tau &\longmapsto \tau_{|L^H} \end{aligned}$$

und dieser induziert einen Isomorphismus $\mathrm{Gal}(L^H/K) \cong G/H$.

Beweis. Da wir $\mathrm{ord}(G) < \infty$ vorausgesetzt haben, ist auch jede Untergruppe $H < G$ endlich, also gilt nach Satz 5.7, dass $L \supset L^H$ eine Galoiserweiterung ist und dass $\mathrm{Gal}(L/L^H) = H$ gilt, dies bedeutet nichts anderes als $\Psi(\Phi(H)) = H$.
Andererseits ist für jeden Zwischenkörper E (also $K \subset E \subset L$) die Erweiterung $L \supset E$ eine Galoiserweiterung (Satz 5.2), und wir haben $H := \mathrm{Gal}(L/E) < G$. Da $L \supset K$ Galoissch ist, folgt aus Punkt 3. von Satz 5.7, dass $L^H = E$ ist, also gilt auch $\Phi(\Psi(E)) = E$.
Sei nun für gegebenes $H < G$ der Fixkörper L^H eine normale Erweiterung von K. Dann ist natürlich $L^H \supset K$ eine Galoiserweiterung, und wir wissen aus Satz 5.2, dass φ ein surjektiver Gruppenhomomorphismus ist. Offensichtlich besteht sein Kern aus denjenigen K-Automorphismen von L, welche nach Einschränkung auf L^H die Identität sind, also genau aus $\mathrm{Aut}_{L^H}(L) = \mathrm{Gal}(L/L^H) = \Psi(\Phi(H)) = H$.
Sei andererseits H ein Normalteiler in G. Wir wollen zeigen, dass die Erweiterung $L^H \supset K$ normal ist, und wir verwenden dazu das Kriterium aus Lemma 4.26: Sei $\overline{L}$ ein algebraischer Abschluss von L (und dann ist es auch einer von K und L^G). Sei $\sigma \in \mathrm{Hom}_K(L^H, \overline{L})$, dann müssen wir zeigen, dass $\mathrm{Im}(\sigma) = L^H$ gilt. Zunächst wissen wir aus Lemma 4.21, dass sich σ zu einem K-Homomorphismus $\sigma' : L \to \overline{L}$ fortsetzen lässt. Da aber $L \supset K$ Galoissch und damit normal ist, gilt $\mathrm{Im}(\sigma') = L$, also $\sigma' \in \mathrm{Aut}_K(L) = G$. Sei $a \in L^H$ und $b := \sigma'(a) = \sigma(a) \in L$. Wir benutzen jetzt die Eigenschaft $H \lhd G$, genauer, wir verwenden, dass für jedes $\tau \in H$ ein $\widetilde{\tau} \in H$ mit $\tau \circ \sigma' = \sigma' \circ \widetilde{\tau}$ existiert. Also ist

$$\tau(b) = \tau \circ \sigma'(a) = \sigma' \circ \widetilde{\tau}(a) \overset{a \in L^H}{=} \sigma'(a) = b.$$

Dies zeigt, dass $b = \sigma(a) \in L^H$ liegt, wir erhalten also $\sigma(L^H) \subset L_H$. Sei $\sigma^{-1} : \sigma(L_H) \to L_H$ die Umkehrabbildung, dann lässt sich diese wieder wegen Satz 4.21 zu einem K-Homomorphismus $(\sigma^{-1})' : L_H \to \overline{L}$ fortsetzen, aber dann wenden wir das obige Argument auf das Element $(\sigma^{-1})' \in \mathrm{Hom}_K(L^H, \overline{L})$ an, und erhalten $(\sigma^{-1})'(L^H) \subset L^H$. Dies liefert $(\sigma^{-1})'(L^H) = L^H$, und daher ist σ ein Element von $\mathrm{Aut}_K(L^H)$. □

Als Konsequenz erhalten wir die folgende Aussage über die Anzahl der Zwischenkörper einer gegebenen Erweiterung.

Korollar 5.9. *Sei $L \supset K$ eine endliche separable Erweiterung, dann existieren nur endlich viele Zwischenkörper E mit $K \subset E \subset L$. Insbesondere gilt dies also für endliche Galoiserweiterungen $L \supset K$.*

Beweis. Wir betrachten die in 4.28 konstruierte normale Hülle $M \supset K$, für die L ein Zwischenkörper ist. Offensichtlich reicht es, die Aussage für die Erweiterung $M \supset K$ zu beweisen. Wir wissen aus Punkt 2. von Satz 4.28, dass $[M : K] < \infty$ gilt. Wir wollen zeigen, dass auch die Erweiterung $M \supset K$ separabel ist: Sei $L = K(a_1, \ldots, a_n)$, dann haben wir (in Punkt 3. von Satz 4.28) gesehen, dass

$$M = K\left(\{\sigma_j(a_i) \,|\, i = 1, \ldots, n;\, j = 1, \ldots, m\}\right)$$

ist, wobei $\mathrm{Hom}_K(L, \overline{K}) = \{\sigma_1, \ldots, \sigma_m\}$ gilt. Nun ist aber (mit einem schon häufig benutzen Argument, welches auf Satz 4.21 zurückgeht) $\mathrm{MinPol}_K(a_i) = \mathrm{MinPol}_K(\sigma_j(a_i))$, für alle $i \in \{1, \ldots, n\}$ und alle $j \in \{1, \ldots, m\}$. Da a_i separabel über K ist, müssen auch alle $\sigma_j(a_i)$ separabel sein. Also ist auch M separabel und deshalb eine endliche Galoiserweiterung von K. Dann sagt der eben bewiesene Hauptsatz (Satz 5.8), dass die Zwischenkörper von $M \supset K$ bijektiv den Untergruppen von $\mathrm{Gal}(M/K)$ entsprechen, und da letztere Gruppe endlich ist, hat sie natürlich nur endlich viele verschiedene Untergruppen. □

Für spätere Anwendungen brauchen wir den Begriff des Kompositums zweier Unterkörper und eine Aussage über die zugehörige Galoisgruppe.

Definition-Lemma 5.10. *Sei L ein Körper und seien $E, E' \subset L$ Unterkörper, dann definieren wir das Kompositum EE' als den kleinsten Teilkörper (bezüglich der Inklusion) von L, welche E und E' enthält. Man sieht leicht, dass dann*

$$EE' = E\left(\{a \,|\, a \in E'\}\right) = E'\left(\{b \,|\, b \in E\}\right)$$

gilt.
Falls K ein weiterer Körper und $L \supset K$ eine endliche Galoiserweiterung mit den Zwischenkörpern E und E' mit $H := \mathrm{Gal}(L/E)$ und $H' := \mathrm{Gal}(L/E')$ ist, dann gilt:

1. *$E \subset E'$ genau dann, wenn $H' \subset H$.*
2. *$EE' = L^{H \cap H'}$.*
3. *$E \cap E' = L^{\langle H, H' \rangle}$, hierbei bezeichnet $\langle H, H' \rangle$ die von H, H' in $\mathrm{Gal}(L/K)$ erzeugte Untergruppe.*

Beweis. 1. Die Richtung „$\Rightarrow$“ ist offensichtlich: Falls $E \subset E'$, dann ist ein E'-Automorphismus von L, also ein Automorphismus von L, welcher auf E' die Identität ist, natürlich insbesondere auf E die Identität, also ein Element von $\mathrm{Aut}_E(L) = \mathrm{Gal}(L/E)$.

Sei andererseits $H' \subset H$ gegeben, dann gilt nach Definition $L^H \subset L^{H'}$, und der Hauptsatz der Galoistheorie (Satz 5.8) sagt, dass $E = L^H$ und $E' = L^{H'}$ ist, also haben wir $E \subset E'$.

2. Die Inklusion $EE' \subset L^{H \cap H'}$ ist klar: Die Gruppe $H \cap H'$ besteht aus Automorphismen von L, welche sowohl E als auch E' festhalten. Da EE' von E' über E erzeugt wird (oder andersherum), liegen seine Elemente natürlich im Fixkörper zu $H \cap H'$.

   Andererseits können wir Punkt 1. auf die Unterkörper $E \subset EE'$ und $E' \subset EE'$ anwenden, und erhalten $\mathrm{Gal}(L/EE') \subset \mathrm{Gal}(L/E)$ und $\mathrm{Gal}(L/EE') \subset \mathrm{Gal}(L/E')$, also $\mathrm{Gal}(L/EE') \subset \mathrm{Gal}(L/E) \cap \mathrm{Gal}(L/E') = H \cap H'$. Aus dieser Inklusion bekommen wir, wieder mit Punkt 1., dass $L^{H \cap H'} \subset EE'$ gilt.

3. Dies folgt unter Benutzung des Hauptsatzes aus der Gleichheit $L^{\langle H, H' \rangle} = L^H \cap L^{H'}$.

□

Wir betrachten noch spezielle Galoiserweiterungen, bei denen die Galoisgruppen besonders einfach zu verstehen sind.

Definition-Lemma 5.11. *Sei $L \supset K$ eine Galoiserweiterung, dann heißt diese abelsch bzw. zyklisch, falls $\mathrm{Gal}(L/K)$ abelsch bzw. zyklisch ist.*
Ist $[L : K] < \infty$ und ist $L \supset K$ abelsch bzw. zyklisch, so ist auch für jeden Zwischenkörper E von $L \supset K$ die Erweiterung $E \supset K$ eine Galoiserweiterung, und die Gruppe $\mathrm{Gal}(E/K)$ ist ebenfalls abelsch bzw. zyklisch.

Beweis. Wir haben im Hauptsatz (Satz 5.8) gesehen, dass $E \supset K$ Galoissch ist genau dann, wenn $\mathrm{Gal}(L/E)$ ein Normalteiler in $\mathrm{Gal}(L/K)$ ist. Wenn aber $\mathrm{Gal}(L/K)$ zyklisch ist, dann ist sie auch abelsch, also ist in beiden Fällen (abelsch oder zyklisch) die Untergruppe $\mathrm{Gal}(L/E)$ ein Normalteiler. Desweiteren haben wir $\mathrm{Gal}(E/K) \cong \mathrm{Gal}(L/K)/\mathrm{Gal}(L/E)$, also ist $\mathrm{Gal}(E/K)$ zyklisch bzw. abelsch, wenn $\mathrm{Gal}(L/E)$ zyklisch bzw. abelsch ist. □

Der folgende Satz gibt präzise Informationen über die zu einem Kompositum von Unterkörpern gehörenden Galoisgruppen.

Satz 5.12. *Sei die Körpererweiterung $L \supset K$ gegeben und seien E, E' Zwischenkörper. Seien $E \supset K$ und $E' \supset K$ endlich und Galoissch. Dann haben wir:*

1. *Die Erweiterung $EE' \supset K$ ist auch endlich und Galoissch und die Abbildung*

$$\begin{aligned} \varphi : \mathrm{Gal}(EE'/E) &\longrightarrow \mathrm{Gal}(E'/E \cap E') \\ \sigma &\longmapsto \sigma_{|E'} \end{aligned}$$

   ist ein Gruppenisomorphismus.

2. *Der Gruppenhomomorphismus*

$$\begin{aligned} \psi : \mathrm{Gal}(EE'/K) &\longrightarrow \mathrm{Gal}(E/K) \times \mathrm{Gal}(E'/K) \\ \sigma &\longmapsto \left(\sigma_{|E}, \sigma_{|E'}\right) \end{aligned}$$

ist injektiv. Er ist bijektiv, falls $E \cap E' = K$ gilt.

Beweis. 1. Es gilt $EE' = K(E, E')$, daher sind Endlichkeit und Separabilität von EE' über K evidente Konsequenzen der Tatsache, dass $E \supset K$ und $E' \supset K$ endlich und separabel sind. Wenn man Mengen Polynome in $K[x]$ wählt, so dass sich E bzw. E' als ihre Zerfällungskörper konstruieren lassen, dann ist EE' Zerfällungskörper der Vereinigung dieser Mengen von Polynomen, also ist die Erweiterung $EE' \supset K$ auch normal und daher Galoissch.

Die Injektivität von φ ist einfach: Alle $\sigma \in \mathrm{Gal}(EE'/E)$ erfüllen $\sigma_{|E} = \mathrm{id}_E$, aber falls $\varphi(\sigma) = \mathrm{id}_{E'}$, dann gilt auch $\varphi_{|E'} = \mathrm{id}_{E'}$ und aus $EE' = E(E')$ folgt dann $\varphi = \mathrm{id}_{EE'}$.

Sei $H := \mathrm{Im}(\varphi) < \mathrm{Gal}(E'/E \cap E')$. Wir wollen $(E')^H = E \cap E'$ zeigen. Da wir aus dem Hauptsatz (Satz 5.8) wissen, dass $H = \mathrm{Gal}(E'/(E')^H)$ gilt, folgt dann $H = \mathrm{Gal}(E'/E \cap E')$, und damit ist φ surjektiv. Wir zeigen zuerst, dass $E \cap E' \subset (E')^H$ gilt: Sei $a \in E \cap E'$, und $\tau \in H$. Dies bedeutet, dass es ein $\sigma \in \mathrm{Gal}(EE'/E)$ gibt mit $\varphi(\sigma) = \tau$, also $\sigma_{|E'} = \tau$. Da aber $a \in E$ gilt und $\sigma_{|E} = \mathrm{id}_E$ ist, folgt $\tau(a) = a$, und damit ist $a \in (E')^H$.

Sei andererseits $a \in (E')^H$ gegeben, und sei $\sigma \in \mathrm{Gal}(EE'/E)$ beliebig. Dann gilt

$$\sigma(a) = \sigma_{|E'}(a) = \varphi(\sigma)(a) \overset{a \in (E')^H}{=} a.$$

Also ist a ein Element aus $(EE')^{\mathrm{Gal}(EE'/E)}$, aber dieser Zwischenkörper ist wieder wegen dem Hauptsatz gleich E. Insbesondere erhalten wir also $a \in E \cap E'$, und damit ist die gewünschte Gleichheit $(E')^H = E \cap E'$ bewiesen.

2. Falls $\sigma \in \mathrm{Gal}(EE'/K)$ ist, so dass $\sigma_{|E} = \mathrm{id}_E$ und $\sigma_{|E'} = \mathrm{id}_{E'}$ gilt, dann ist natürlich wie oben auch $\sigma = \mathrm{id}_{EE'}$, also ist ψ injektiv. Falls darüber hinaus $E \cap E' = K$ ist, können wir Punkt 1. auf die Erweiterungen $EE' \supset E$ und $EE' \supset E'$ anwenden: Seien $\sigma \in \mathrm{Gal}(E/K)$ und $\sigma' \in \mathrm{Gal}(E'/K)$ gegeben, dann existieren also Fortsetzungen $\widetilde{\sigma} \in \mathrm{Gal}(EE'/E') \subset \mathrm{Gal}(EE'/K)$ und $\widetilde{\sigma}' \in \mathrm{Gal}(EE'/E) \subset \mathrm{Gal}(EE'/K)$ mit $\widetilde{\sigma}_{|E} = \sigma$ und $\widetilde{\sigma}'_{|E'} = \sigma'$. Die Verknüpfung $\widetilde{\sigma} \circ \widetilde{\sigma}'$ ist wieder ein Element von $\mathrm{Gal}(EE'/K)$ und es gilt:

$$(\widetilde{\sigma} \circ \widetilde{\sigma}')_{|E} = \widetilde{\sigma}_{|E} \circ \widetilde{\sigma}'_{|E} = \sigma \circ \mathrm{id}_E = \sigma \in \mathrm{Gal}(E/K)$$

$$(\widetilde{\sigma} \circ \widetilde{\sigma}')_{|E'} = \widetilde{\sigma}_{|E'} \circ \widetilde{\sigma}'_{|E'} = \mathrm{id}_{E'} \circ \sigma' = \sigma' \in \mathrm{Gal}(E'/K),$$

also ist $\widetilde{\sigma} \circ \widetilde{\sigma}'$ ein Urbild von $(\sigma, \sigma') \in \mathrm{Gal}(E/K) \times \mathrm{Gal}(E'/K)$ unter ψ.

□

Nach all diesen Vorbereitungen wollen wir nun die ersten Anwendungen der Galoistheorie erarbeiten. Um das Studium der von Galoisgruppen von gegebenen Erweiterungen effektiv durchführen zu können, benutzen wir die Sylowsätze (Satz 2.29) zur Struktur endlicher Gruppen aus Kapitel 2. Zur Erinnerung hier noch einmal der Inhalt dieses Satzes.

Sei G eine endliche Gruppe mit $\mathrm{ord}(G) = n$ und p eine Primzahl. Schreibe $n = p^k \cdot m$, mit $m \in \mathbb{N}$ und $\mathrm{ggT}(m, p) = 1$.

1. *Für jede p-Untergruppe $H < G$ (d.h., $\mathrm{ord}(H) = p^l$ für ein $l \in \{1, \ldots, k\}$) existiert eine p-Sylowgruppe $S \subset G$ (d.h. $\mathrm{ord}(S) = p^k$) mit $H \subset S$.*

2. *Für jede p-Sylowgruppe S von G gilt: Alle zu S konjugierten Untergruppen sind p-Sylowgruppen. Umgekehrt sind alle p-Sylowgruppen konjugiert.*

3. Sei s_p die Anzahl der p-Sylowgruppen von G, dann gilt

$$s_p | m \qquad \text{und} \qquad s \equiv 1 \mod (p)$$

Insbesondere ist also $s_p > 0$, d.h. aus 3. folgt insbesondere die Existenz einer p-Sylowgruppe $S < G$.

Zur Anwendung dieses Satzes in der Galoistheorie hier zunächst einfaches Beispiel, welches wir zum Teil schon nach dem Beweis von Lemma 4.26 diskutiert hatten:
Sei $K = \mathbb{Q}$, und $f = x^3 - 2 \in \mathbb{Q}[x]$, sei L der Zerfällungskörper von f. Die Nullstellen von f in $\mathbb{C}$ sind $\sqrt[3]{2}$, $\zeta\sqrt[3]{2}$ und $\zeta^2\sqrt[3]{2}$, wobei $\zeta = e^{2\pi i/3}$ ist. Dann rechnet man leicht nach, dass $L = \mathbb{Q}(\sqrt[3]{2}, \zeta\sqrt[3]{2}, \zeta^2\sqrt[3]{2}) \stackrel{!}{=} L(\sqrt[3]{2}, \zeta)$ gilt. Da f irreduzibel in $\mathbb{Q}[x]$ ist (Eisenstein), gilt $f = \mathrm{MinPol}_{\mathbb{Q}}(\sqrt[3]{2})$, und wir haben $\mathrm{MinPol}_{\mathbb{Q}}(\zeta) = \frac{x^3-1}{x-1} = x^2+x+1$. Es gilt also $[\mathbb{Q}(\sqrt[3]{2}) : \mathbb{Q}] = 3$ und $[\mathbb{Q}(\zeta) : \mathbb{Q}] = 2$. Da das Polynom x^2+x+1 auch in $\mathbb{Q}(\sqrt[3]{2})$ irreduzibel ist, gilt auch $[\mathbb{Q}(\sqrt[3]{2}, \zeta) : \mathbb{Q}(\sqrt[3]{2})] = 2$, und damit wegen dem Gradsatz (Satz 4.3) $[L : \mathbb{Q}] = 6$. f ist separabel, also ist der Zerfällungskörper L eine Galoiserweiterung von $\mathbb{Q}$, und wir haben $\mathrm{ord}\,(\mathrm{Gal}(L/\mathbb{Q})) = 6$. Damit wissen wir, dass diese Gruppe entweder zyklisch, also isomorph zu $\mathbb{Z}/6\mathbb{Z}$ oder isomorph zu S_3 ist. Es gibt verschiedene Möglichkeiten, festzustellen, welche der beiden Gruppen es ist: Am einfachsten argumentiert man mit der Bemerkung nach Definition 5.1, welche uns sagt, dass die Galoisgruppe in jedem Fall eine Untergruppe von S_3 ist, daher kann sie hier nur isomorph zu S_3 sein. Eine etwas kompliziertere, aber auch interessantere Möglichkeit nutzt die Sylowsätze, auf die folgende Art und Weise: Die Gruppen $\mathrm{Gal}(L/\mathbb{Q}(\sqrt[3]{2}))$ und $\mathrm{Gal}(L/\mathbb{Q}(\zeta))$ sind Untergruppen von $\mathrm{Gal}(L/\mathbb{Q})$. Wir wissen, dass $\mathbb{Q}(\zeta) \supset \mathbb{Q}$ normal ist, denn $\mathbb{Q}(\zeta)$ enthält auch ζ^2, ist also der Zerfällungskörper von $x^2 + x + 1$ über $\mathbb{Q}$. Daher ist $\mathrm{Gal}(L/\mathbb{Q}(\zeta))$ ein Normalteiler der Ordnung 3 (vom Index 2) in $\mathrm{Gal}(L/\mathbb{Q})$. Hingegen ist $\mathbb{Q}(\sqrt[3]{2}) \supset \mathbb{Q}$ nicht normal, denn $\mathbb{Q}(\sqrt[3]{2})$ ist nicht der Zerfällungskörper des Minimalpolynoms f von $\sqrt[3]{2}$. Also ist $\mathrm{Gal}(L/\mathbb{Q}(\sqrt[3]{2}))$ eine Untergruppe der Ordnung 2 (vom Index 3) in $\mathrm{Gal}(L/\mathbb{Q})$. Da alle 3-Sylowgruppen in $\mathrm{Gal}(L/\mathbb{Q})$ konjugiert sind, folgt $s_3 = 1$, hingegen muss $s_2 > 1$ gelten (sonst wäre $\mathrm{Gal}(L/\mathbb{Q}(\sqrt[3]{2}))$ ein Normalteiler). Der dritte Sylowsatz sagt, dass $s_2|6$ und $s_2 \equiv 1 \mod (2)$ gilt, die impliziert $s_2 = 3$. Also gibt es genau eine Unterguppe der Ordnung 3 und genau 3 Untergruppen der Ordnung 2 in $\mathrm{Gal}(L/\mathbb{Q})$ und wegen dem Satz von Langrange keine weiteren. Natürlich kann man diese Aussagen (also die Bestimmung der Untergruppen von S_3) auch direkt ohne Verwendung der Sylowsätze zeigen.
Wir können leicht zu diesen Untergruppen zugehörigen Zwischenkörper bestimmen, nach dem Hauptsatz gilt $L^{\mathrm{Gal}(L/\mathbb{Q}(\zeta))} = \mathbb{Q}(\zeta)$, $L^{\mathrm{Gal}(L/\mathbb{Q}(\sqrt[3]{2}))} = \mathbb{Q}(\sqrt[3]{2})$. Seien U_1 und U_2 die zu $\mathrm{Gal}(L/\mathbb{Q}(\sqrt[3]{2}))$ konjugierten Untergruppen von $\mathrm{Gal}(L/\mathbb{Q})$, dann ist $L^{U_1} = \mathbb{Q}(\zeta \cdot \sqrt[3]{2})$ und $L^{U_2} = \mathbb{Q}(\zeta^2 \cdot \sqrt[3]{2})$ (die letzen beiden Aussagen folgen aus der Tatsache, dass U_1 und U_2 Untergruppen von $\mathrm{Bij}(\sqrt[3]{2}, \zeta \cdot \sqrt[3]{2}, \zeta^2 \cdot \sqrt[3]{2}) = S_3$ der Ordnung 2 sind, welche $\sqrt[3]{2}$ nicht in sich selbst überführen).
Die erste bedeutende Anwendung der Galoistheorie zusammen mit den Sylowsätzen ist der folgenden Fundamentalsatz der Algebra. Es sei erwähnt, dass es noch viele andere, weniger algebraische Beweise gibt, die allerdings mehr Hilfsmittel aus der Analysis benutzen.

Satz 5.13 (Fundamentalsatz der Algebra)**.** *Der Körper $\mathbb{C}$ ist algebraisch abgeschlossen.*

Beweis. Ein rein algebraischer Beweis des Fundamentalsatzes der Algebra kann nicht existieren, weil die Definition von $\mathbb{C}$ auf (einer) der analytischen Konstruktion(en) von $\mathbb{R}$ aufbaut. Im folgenden geben wir einen galoistheoretischen Beweis, welcher nur die folgenden Aussagen aus der Analysis benutzt:

1. Jedes Polynom aus $\mathbb{R}[x]$, dessen Grad ungerade ist, hat mindestens eine Nullstelle in $\mathbb{R}$ (dies kann man mit dem Zwischenwertsatz leicht beweisen).

2. Jedes Element $a \in \mathbb{R}_{\geq 0}$ besitzt eine Quadratwurzel in $\mathbb{R}$.

Als erstes beweisen wir folgende Aussage: Es gibt keine Erweiterungen von $\mathbb{C}$ vom Grad 2. Eine solche Erweiterung wäre von einem Element erzeugt, welches ein Minimalpolynom $f = x^2 + u \cdot x + v \in \mathbb{C}[x]$ vom Grad 2 hätte. Es ist dann $f = (x + \frac{u}{2})^2 + w$, mit $w := v - \frac{u^2}{4}$. Schreibe $w = r + i \cdot s$, mit $r, s \in \mathbb{R}$, dann ist $|w| = \sqrt{r^2 + s^2} \geq \pm r$. Also gibt es wegen der oben angenommenen Aussage 2. reelle Zahlen a, b, so dass

$$a^2 = \frac{|w| - r}{2} \quad \text{und} \quad b^2 = \frac{|w| + r}{2}$$

gilt. Dann haben wir $a^2 - b^2 = -r$ und $2|a \cdot b| = 2\sqrt{\frac{|w|^2 - r^2}{4}} = |s|$. Bei der Wahl der Quadratwurzeln a und b können wir die Vorzeichen frei festsetzen, dies machen wir so, dass $2ab = -s$ gilt. Dann haben wir

$$(a + ib)^2 + w = a^2 + 2iab - b^2 + w = -r + i \cdot (-s) + w = 0,$$

und damit ist $a + ib - \frac{u}{2} \in \mathbb{C}$ eine Nullstelle des Polynoms f, d.h., dieses kann nicht irreduzibel in $\mathbb{C}[x]$ sein. Um zu zeigen, dass $\mathbb{C}$ algebraisch abgeschlossen ist, benutzen wir nun Lemma 4.15. Sei also $L \supset \mathbb{C}$ eine Erweiterung mit $1 < [L : \mathbb{C}] < \infty$. In dem wir gegebenenfalls zu einem Zerfällungskörper übergehen, können wir annehmen, dass die Erweiterung $L \supset \mathbb{R}$ normal und damit eine Galoiserweiterung ist (separabel ist sie sowieso, da $\mathrm{char}(\mathbb{C}) = \mathrm{char}(\mathbb{R}) = 0$ gilt). Aus dem Gradsatz folgt, dass $2 \mid [L : \mathbb{R}]$ gilt, genauer, $[L : \mathbb{R}] = 2^k \cdot m$, wobei m ungerade sein soll. Wir benötigen jetzt wieder die Sylowsätze, welche wir auf die Gruppe $G := \mathrm{Gal}(L/\mathbb{R}) = \mathrm{Aut}_{\mathbb{R}}(L)$ anwenden. G enthält eine 2-Sylowuntergruppe $H < G$ der Ordnung 2^k. Dann ist nach Satz 5.5 die Erweiterung $L \supset L^H$ eine Galoiserweiterung, also $[L : L^H] = 2^k$, also wegen des Gradsatzes (Satz 4.3) $[L^H : \mathbb{R}] = m$. Nach dem Satz vom primitiven Element (Satz 4.40) existiert ein $a \in L^H$ mit $L^H = \mathbb{R}(a)$. Das Minimalpolynom $f := \mathrm{MinPol}_{\mathbb{R}}(a) \in \mathbb{R}[x]$ hat Grad m (eine ungerade Zahl), also hat f nach Punkt 1. der obigen Annahme eine Nullstelle in $\mathbb{R}$. Wegen der Irreduzibilität von f muss dann $\deg(f) = m \stackrel{!}{=} 1$ gelten. Damit ist also $\mathrm{ord}(\mathrm{Gal}(L/\mathbb{R})) = [L : \mathbb{R}] = 2^k$, und dies impliziert (wieder wegen des Gradsatzes), dass $[L : \mathbb{C}] = 2^{k-1}$ ist, also $\mathrm{ord}\,(\mathrm{Gal}(L/\mathbb{C})) = 2^{k-1}$. Jetzt muss aber $k > 1$ gelten (wegen $[L : \mathbb{C}] > 1$) und aus Korollar 2.26 folgt, dass eine Untergruppe H' in $\mathrm{Gal}(L/\mathbb{C})$ der Ordnung 2^{k-2} existiert, aber dann ist wieder $L \supset L^{H'}$ Galoisch mit $[L : L^{H'}] = 2^{k-2}$, also $[L^{H'} : \mathbb{C}] = 2$. Dies ist ein Widerspruch zu der oben bewiesenen Aussage, dass es keine Körpererweiterungen von $\mathbb{C}$ der Ordnung 2 gibt. □

5.2 Einheitswurzeln und auflösbare Erweiterungen

Wir wollen hier die Galoistheorie anwenden, um die ganz am Anfang (in Kapitel 1) erwähnte Frage der Auflösbarkeit von algebraischen Gleichungen zu lösen. Als Vorbereitung behandeln bzw. wiederholen wir kurz einige Tatsachen über Einheitswurzeln, welche beim Beweis des entscheidenden Satzes zur Auflösbarkeit von Gleichungen (Satz 5.24) benötigt werden. Wir starten mit einigen Definitionen

Definition 5.14. *Sei K ein Körper.*

1. *Die Nullstellen des Polynoms $x^n - 1$ in $\overline{K}$ heißen n-te Einheitwurzeln. Man sieht leicht, dass sie eine endliche Untergruppe (der Ordnung n) von $\overline{K}^*$ bilden, manchmal U_n oder auch μ_n genannt. Nach Lemma 4.39 ist U_n dann zyklisch.*

   Man beachte, dass für $\mathrm{char}(K) \nmid n$ *das Polynom $x^n - 1$ separabel ist, aber nicht für* $\mathrm{char}(K) \mid n$. *In diesem Fall ist $x^n - 1 = (x^m - 1)^{p^r}$ mit $n = m \cdot p^r$ und* $\mathrm{ggT}(m, p) = 1$ *und es gilt $U_n = U_m$.*

2. *Sei* $\mathrm{char}(K) \nmid n$. *Dann heißt jeder Erzeuger von U_n eine* primitive *n-te Einheitswurzel.*

Das vielleicht wichtigste Beispiel ist der Fall $K = \mathbb{C}$, hier ist

$$U_n = \left\{ e^{\frac{2\pi i k}{n}} \mid k = 0, \ldots, n-1 \right\}$$

Der folgende Satz beschreibt die primitiven Einheitswurzeln genauer.

Satz 5.15. *Sei* $\mathrm{char}(K) \nmid n$. *Sei ζ eine primitive n-te Einheitswurzel. Dann gilt für alle $k \in \mathbb{N}$, dass ζ^k eine primitive n-te Einheitswurzel ist genau dann, wenn* $\mathrm{ggT}(k, n) = 1$ *ist.*

Beweis. Da ζ primitiv ist, gilt $\mathbb{Z}/n\mathbb{Z} \cong \langle \zeta \rangle = U_n$, dieser Isomorphismus wird durch $k \mapsto \zeta^k$ realisiert. Wir wissen, dass die Restklasse $\overline{k} \in \mathbb{Z}/n\mathbb{Z}$ genau dann ein Erzeuger von $\mathbb{Z}/n\mathbb{Z}$ ist, wenn $\mathrm{ggT}(k, n) = 1$ gilt, dies zeigt die Behauptung. □

Wir studieren zunächst Erweiterungen von $\mathbb{Q}$ durch primitive Einheitswurzeln.

Satz 5.16. *Sei $\zeta \in \overline{\mathbb{Q}}$ eine primitive n-te Einheitswurzel. Dann ist die Erweiterung $\mathbb{Q}(\zeta) \supset \mathbb{Q}$ Galoissch und es gilt $[\mathbb{Q}(\zeta) : \mathbb{Q}] = \varphi(n)$. Hierbei bezeichnet $\varphi(n) := \operatorname{ord}((\mathbb{Z}/n\mathbb{Z})^*)$ die in Korollar 3.25 eingeführte Eulersche φ-Funktion.*
Sei

$$\Phi_n(x) := \prod_{a \text{ mit } 0<a\leq n, \operatorname{ggT}(a,n)=1} \left(x - e^{2\pi i \frac{a}{n}}\right) \in \mathbb{Z}[x]$$

das bereits in den Übungen verwendete n-te Kreisteilungspolynom. Dann gilt

$$x^n - 1 = \prod_{d|n} \Phi_d(x)$$

sowie $\Phi_n(x) \in \mathbb{Z}[x]$. Außerdem ist $\operatorname{MinPol}_{\mathbb{Q}}(\zeta) = \Phi_n$, und damit ist Φ_n irreduzibel in $\mathbb{Q}[x]$ und wegen des Satzes von Gauß (Satz 3.43) auch irreduzibel in $\mathbb{Z}[x]$.

Beweis. Wir zeigen zuerst die Aussagen über das Kreisteilungspolynom. Bemerke, dass die Abbildung

$$\begin{array}{rcl} \psi : \{d \in \mathbb{N} \mid d|n\} & \longrightarrow & \{d \in \mathbb{N} \mid d|n\} \\ d & \longmapsto & \frac{n}{d} \end{array}$$

bijektiv ist. Dann folgt

$$\begin{aligned} x^n - 1 &= \prod_{1\leq a\leq n} \left(x - e^{2\pi i \frac{a}{n}}\right) \\ &= \prod_{d|n} \prod_{\operatorname{ggT}(a,n)=d} \left(x - e^{2\pi i \frac{a}{n}}\right) \\ &= \prod_{d|n} \prod_{\operatorname{ggT}(a,n)=d} \left(x - e^{2\pi i \frac{a/d}{n/d}}\right) \\ &= \prod_{d|n} \prod_{\operatorname{ggT}(b,n/d)=1} \left(x - e^{2\pi i \frac{b}{n/d}}\right) \\ &\overset{\psi}{=} \prod_{d|n} \Phi_d(x) \end{aligned}$$

Jetzt zeigt man per Induktion über n, dass $\Phi_n(x) \in \mathbb{Z}[x]$ gilt: Für $n = 1$ ist $\Phi_1(x) = x - 1 \in \mathbb{Z}[x]$. Außerdem hat man wegen dem eben Bewiesenen für $n \in \mathbb{N}_{>0}$ beliebig, dass

$$x^n - 1 = \Phi_n(x) \cdot \prod_{d|n, d\neq n} \Phi_d(x)$$

gilt. Jetzt benutzen wir die folgende Tatsache: Ist R ein Integritätsring und sind $f(x), g(x) \in R[x]\backslash\{0\}$ und ist $g(x)$ unitär, so gibt es eindeutige $q(x), r(x) \in R[x]$ mit $\deg r(x) < \deg g(x)$ und $f(x) = q(x) \cdot g(x) + r(x)$. Man beachte: Im Allgemeinen ist $R[x]$ kein euklidischer Ring, aber Polynomdivision funktioniert trotzdem, wenn man voraussetzt, dass $g(x)$ unitär ist. Angewandt auf $f(x) = x^n - 1 \in \mathbb{Z}[x]$ und $g(x) = \prod_{d|n, d\neq n} \Phi_d(x) \in \mathbb{Z}[x]$ (letzteres folgt aus der Induktionshypothese) erhalten wir $\Phi_n(x) \in \mathbb{Z}[x]$, wie gewünscht. Die Irreduzibilität von $\Phi_n(x)$ wird weiter unten aus $\operatorname{MinPol}_{\mathbb{Q}}(\zeta) = \Phi_n$ folgen.
Klar ist: $x^n - 1 \in \mathbb{Q}[x]$ ist separabel, und $\mathbb{Q}(\zeta)$ ist ein Zerfällungskörper dieses Polynoms. Daher ist $\mathbb{Q}(\zeta) \supset \mathbb{Q}$ eine Galoiserweiterung. Sei nun $f := \operatorname{MinPol}_{\mathbb{Q}}(\zeta)$. Für alle $\sigma \in \operatorname{Gal}(\mathbb{Q}(\zeta)/\mathbb{Q})$ induziert σ einen Gruppenautomorphismus von U_n, insbesondere ist $\sigma(\zeta)$ wieder primitiv. Andererseits gibt es zu jeder Nullstelle η von f nach Lemma 4.20 ein Element $\sigma \in \operatorname{Gal}(\mathbb{Q}(\zeta)/\mathbb{Q})$ mit $\sigma(\zeta) = \eta$, und daher ist auch η eine primitive n-te

Einheitswurzel. Dies zeigt $[\mathbb{Q}(\zeta):\mathbb{Q}] = \deg(f) \leq \varphi(n)$. Natürlich ist f ein Teiler von x^n-1, also $x^n-1 = f\cdot h$. Da f als Minimalpolynom nach Definition unitär ist, gilt dies auch für h. Aus Korollar 3.42 (aus dem Umfeld des Satzes von Gauß) folgt dann, dass $f, h \in \mathbb{Z}[x]$ gilt. Sei nun p ein Primzahl und $\mathrm{ggT}(p,n) = 1$. Dann ist nach dem letzten Satz (Satz 5.15) auch ζ^p primitiv. Angenommen, es gelte $f(\zeta^p) \neq 0$. Dann ist $h(\zeta^p) = 0$, dies bedeutet, dass ζ Nullstelle von $h(x^p)$ ist, also haben wir $h(x^p) = f(x)\cdot g(x)$, wobei g wieder unitär sein muss, und erneut ist wegen Korollar 3.42 $g \in \mathbb{Z}[x]$. Wir betrachten den Reduktionshomomorphismus

$$\begin{array}{rcl} \mathbb{Z}[x] & \longrightarrow & \mathbb{F}_p[x] \\ q(x) = \sum_{i=0}^m a_i x^i & \longmapsto & \overline{q}(x) = \sum_{i=0}^m \overline{a}_i x^i. \end{array}$$

Dann gilt $\overline{h}^p \overset{(*)}{=} \overline{h(x^p)} = \overline{f}\cdot\overline{g}$, wobei die Gleichung $(*)$ wieder aus der in $\mathbb{F}_p$ gültigen Formel $(a+b)^p = a^p + b^p$ folgt. Damit gilt $\mathrm{ggT}_{\mathbb{F}_p[x]}(\overline{f},\overline{h}) \neq 1$. Damit hat $\overline{f}\cdot\overline{h} = x^n - 1 \in \mathbb{F}_p[x]$ mehrfache Nullstellen in $\overline{\mathbb{F}}_p$. Aber wegen $p \nmid n$ ist $x^n - 1 \in \mathbb{F}_p[x]$ separabel, dies ist ein Widerspruch, und wir haben $f(\zeta^p) = 0$ gezeigt.
Falls ζ' eine beliebige primitive n-te Einheitswurzel ist, dann gilt $\zeta' = \zeta^m$ mit $\mathrm{ggT}(n,m) = 1$. Dann betrachten wir die Primfaktorzerlegung von m, und ζ' entsteht aus ζ durch wiederholtes Potenzieren mit den Primfaktoren von m. Damit folgt mit dem obigen Argument, dass $f(\zeta') = 0$ gilt, also sind alle primitiven n-ten Einheitswurzel Nullstellen von f. Daher ist $\varphi(n) \leq \deg(f)$. Wir erhalten also $\varphi(n) = \deg(f)$ und damit auch $\Phi_n = f$, welches als Minimalpolynom von ζ natürlich irreduzibel in $\mathbb{Q}[x]$ und damit auch in $\mathbb{Z}[x]$ ist. □

Im folgenden wollen wir nun die Galoisgruppen von Körpern, die durch Adjunktion von Einheitswurzeln entstehen, studieren.

Satz 5.17. *Sei K ein Körper, $\zeta \in U_n \subset \overline{K}$ eine primitive n-te Einheitswurzel, und es sei $\mathrm{char}(K) \nmid n$. Dann gilt*

1. *$K(\zeta) \subset K$ ist eine endliche abelsche Galoiserweiterung mit $[K(\zeta):K] \leq \varphi(n)$.*
2. *Für alle $\sigma \in \mathrm{Gal}(K(\zeta)/K)$ existiert ein $r(\sigma) \in \mathbb{N}$, so dass $\sigma(\zeta) = \zeta^{r(\sigma)}$ gilt. Die Restklasse $\overline{r(\sigma)}$ in $\mathbb{Z}/n\mathbb{Z}$ ist ein Element von $(\mathbb{Z}/n\mathbb{Z})^*$, und wir erhalten einen wohldefinierten Gruppenhomomorphismus*

$$\begin{array}{rcl} \psi : \mathrm{Gal}(K(\zeta)/K) & \longrightarrow & (\mathbb{Z}/n\mathbb{Z})^* \\ \sigma & \longmapsto & \overline{r(\sigma)} \end{array},$$

welcher nicht von der Wahl von ζ in U_n abhängt. ψ ist injektiv, und im Fall $K = \mathbb{Q}$ sogar bijektiv.

Ist also $\zeta \in \overline{\mathbb{Q}}$ eine primitive n-te Einheitswurzel, so ist $\mathbb{Q}(\zeta) \supset \mathbb{Q}$ eine abelsche Galoiserweiterung mit $\mathrm{Gal}(\mathbb{Q}(\zeta)/\mathbb{Q}) \cong (\mathbb{Z}/n\mathbb{Z})^*$.

Beweis. 1. Der Körper $K(\zeta)$ ist der Zerfällungskörper des separablen Polynoms $x^n - 1 \in K[x]$, daher ist $K(\zeta) \supset K$ eine Galoiserweiterung. Also ist $[K(\zeta):K] = \mathrm{ord}\,(\mathrm{Gal}(K(\zeta)/K))$, und aus dem noch zu zeigenden Punkt 2. folgt, dass $\mathrm{Gal}(K(\zeta)/K) < (\mathbb{Z}/n\mathbb{Z})^*$ gilt, daher ist $K(\zeta) \supset K$ abelsch und wir haben $[K(\zeta):K] \leq \varphi(n)$.

2. Für alle $\sigma \in \mathrm{Gal}(K(\zeta)/K)$ ist $\sigma(\zeta)$ wieder eine primitive n-te Einheitswurzel, also gilt (nach Satz 5.15) $\overline{r(\sigma)} \in (\mathbb{Z}/n\mathbb{Z})^*$. Ist andererseits ζ' eine weitere primitive n-te Einheitswurzel, so gilt ebenfalls nach Satz 5.15, dass $\zeta' = \zeta^l$ mit $\overline{l} \in (\mathbb{Z}/n\mathbb{Z})^*$. Dann ist

$$\sigma(\zeta') = \sigma(\zeta)^l = \zeta^{r(\sigma)\cdot l} = (\zeta')^{r(\sigma)}$$

also ist $\overline{r(\sigma)} \in \mathbb{Z}/n\mathbb{Z}$ unabhängig von der Wahl von ζ.

Natürlich ist die Abbildung ψ ein Gruppenhomomorphismus, und es gilt

$$\psi(\sigma) = \psi(\tau) \iff \overline{r(\sigma)} = \overline{r(\tau)} \iff \sigma(\zeta) = \tau(\zeta) \iff \sigma = \tau,$$

also ist ψ injektiv.

Sei nun $K = \mathbb{Q}$, dann ist nach Satz 5.16 $\operatorname{ord}(\mathrm{Gal}(\mathbb{Q}(\zeta)/\mathbb{Q})) = \varphi(n)$, und die Eulersche φ-Funktion ist nach Korollar 3.25 genau die Ordnung von $(\mathbb{Z}/n\mathbb{Z})^*$, also ist φ in diesem Fall ein Gruppenisomorphismus.

□

Den folgenden Satz werden wir aus Zeitgründen nicht beweisen.

Satz 5.18. *Sei $L \supset K$ Galoissch und zyklisch, mit $[L : K] = n$.*

1. *Sei $\mathrm{char}(K) \nmid n$, und enthalte K eine primitive n-te Einheitswurzel ζ, dann gibt es einen Erzeuger $\sigma \in \mathrm{Gal}(L/K)$ und ein Element $a \in L^*$, so dass $\sigma(a) = \zeta \cdot a$ gilt.*
2. *Sei $n = \mathrm{char}(K) = p > 0$, dann gibt es einen Erzeuger $\sigma \in \mathrm{Gal}(L/K)$ und ein Element $a \in L^*$ mit $\sigma(a) - a = 1$.*

Wir erhalten die folgenden Konsequenzen, welche wir gleich zum Studium der Auflösbarkeit von Gleichungen brauchen.

Korollar 5.19. *Sei $L \supset K$ eine endliche Erweiterung, und $\zeta \in K$ eine primitive n-te Einheitswurzel. Dann gilt:*

1. *Ist $L \supset K$ Galoissch und zyklisch mit $[L : K] = n$ und so dass $\mathrm{char}(K) \nmid n$ gilt, so existiert $a \in L$ mit $L = K(a)$ und ein $c \in K$ mit $\mathrm{MinPol}_K(a) = x^n - c \in K[x]$ (genauer, es ist $c := a^n \in K$ und $\mathrm{MinPol}_K(a) = x^n - a^n$).*
2. *Falls umgekehrt $L = K(a)$ gilt und a Nullstelle von $x^n - c \in K[x]$ ist, so dass wieder $\mathrm{char}(K) \nmid n$ gilt, dann ist $L \supset K$ zyklisch, $d := [L : K]$ ist eine Teiler von n und es gilt $\mathrm{MinPol}_K(a) = x^d - a^d$.*

Beweis. 1. Nach dem letzten (Satz 5.18) existiert ein Erzeuger σ von $\mathrm{Gal}(L/K)$ und ein $a \in L^*$ mit $\sigma(a) = \zeta \cdot a$. Dann sind die n Elemente $\zeta \cdot a, \zeta^2 \cdot a, \ldots, \zeta^n \cdot a = a$ verschieden, und daher ist $[K(a) : K] \geq n$. Weil aber natürlich $K(a) \subset L$ gilt, erhalten wir $L = K(a)$. Andererseits ist $\zeta^n = 1$, daraus folgt $a^n = \zeta^n \cdot a^n = \sigma(a)^n = \sigma(a^n)$. Da σ ein Erzeuger von $\mathrm{Gal}(L/K)$ ist, folgt, dass für alle $\tau \in \mathrm{Gal}(L/K)$ gilt, dass $\tau(a^n) = a^n$ ist, und dies impliziert wegen $L^{\mathrm{Gal}(L/K)} = K$, dass $a^n \in K$ gilt. Also ist $x^n - a^n \in K[x]$, und a ist natürlich Nullstelle diese Polynoms. Wegen $\deg(x^n - a^n) = n$ ist $x^n - a^n = \mathrm{MinPol}_K(a)$.

2. Sei $a \neq 0$ (sonst ist $L = K$), dann sind die Nullstellen von $x^n - c$ gegeben durch $a, \zeta \cdot a, \ldots, \zeta^{n-1} \cdot a$. $L = K(a)$ ist damit ein Zerfällungskörper von $x^n - c$, und für $\mathrm{char}(K) \nmid n$ ist $x^n - c$ separabel, also ist $L \supset K$ eine Galoiserweiterung. Sei $\tau \in \mathrm{Gal}(L/K)$ beliebig, dann ist $\tau(a)$ auch eine Nullstelle von $x^n - c$, also gilt $\tau(a)^n = c = a^n$. Daher ist $\frac{\tau(a)}{a} \in U_n$, und wir können die Abbildung

$$\begin{array}{ccc} \mathrm{Gal}(L/K) & \longrightarrow & U_n \\ \tau & \longmapsto & \frac{\tau(a)}{a} \end{array}$$

definieren. Es ist klar, dass diese injektiv ist (wenn $\tau(a)/a = \epsilon(a)/a$ gilt, ist $\tau(a) = \epsilon(a)$ und da $L = K(a)$ und τ, ϵ die Identität auf K sind, folgt daraus $\tau = \epsilon$). Die Abbildung ist aber auch ein Gruppenhomomorphismus: für alle $\tau, \epsilon \in \mathrm{Gal}(L/K)$ gilt

$$\frac{\tau \circ \epsilon(a)}{a} = \frac{\tau\epsilon((a))}{\tau(a)} \frac{\tau(a)}{a} = \tau\left(\frac{\epsilon(a)}{a}\right) \frac{\tau(a)}{a} \overset{\frac{\epsilon(a)}{a} \in K}{=} \frac{\epsilon(a)}{a} \frac{\tau(a)}{a}.$$

Damit wissen wir, dass $\mathrm{Gal}(L/K)$ als Untergruppe von U_n aufgefasst werden kann, und deshalb zyklisch ist, mit $\operatorname{ord}(\mathrm{Gal}(L/K)) = d$ für ein $d | n$. Sei σ ein Erzeuger von $\mathrm{Gal}(L/K)$, dann ist $\sigma(a)/a$ schon eine d-te Einheitswurzel, und wir haben

$$\sigma(a^d) = \sigma(a)^d = \left(\frac{\sigma(a)}{a}\right)^d a^d = a^d,$$

also ist mit dem gleichen Argument wie oben $a^d \in K$ und wir erhalten $x^d - a^d = \mathrm{MinPol}_K(a)$.

□

Das nächste Korollar ist eine zur eben behandelten Aussage analoges Resultat, aber für den Fall, dass der Grad des Minimalpolynoms gleich der Charakteristik des Grundkörpers ist.

Korollar 5.20. *Sei $L \supset K$ eine Erweiterung und $\mathrm{char}(K) = p > 0$.*

1. *Falls $L \supset K$ zyklisch und $[L : K] = p$ ist, dann existiert $a \in L$ mit $L = K(a)$ und $\mathrm{MinPol}_K(a) = x^p - x - c$ für ein $c \in K$.*
2. *Ist umgekehrt $L = K(a)$, wobei a eine Nullstelle von $x^p - x - c \in K[x]$ ist, dann ist $L \supset K$ zyklisch. Entweder zerfällt $x^p - x - c$ schon über K vollständig in Linearfaktoren, oder es ist in $K[x]$ irreduzibel. In letztem Fall ist $[L : K] = p$.*

Beweis. 1. Wegen Satz 5.18, Punkt 2., gibt es einen Erzeuger σ von $\mathrm{Gal}(L/K)$ sowie ein Element $a \in L$, so dass $\sigma(a) - a = 1$ gilt. Induktiv können wir dann folgern, dass $\sigma^k(a) - a = k$ gilt. Daher sind die p Elemente $a, \sigma(a), \sigma^2(a), \ldots, \sigma^{p-1}(a)$ alle verschieden, und wir haben $[K(a) : K] \geq p$, dies zeigt $L = K(a)$. Außerdem gilt

$$\begin{aligned} \sigma(a^p - a) &= \sigma(a)^p - \sigma(a) \\ &= (a+1)^p - (a+1) \\ &= a^p - a \end{aligned}$$

daher ist wieder $c := a^p - a$ ein Element von K. a ist Nullstelle von $x^p - x - c \in K[x]$, und wegen $\deg(x^p - x - c) = [L : K]$ ist $\mathrm{MinPol}_K(a) = x^p - x - c$.

2. Sei $L = K(a)$ und a eine Nullstelle von $f := x^p - x - c \in K[x]$. Dann ist wegen $(a+1)^p = a^p + 1$ auch $a + 1$ Nullstelle von f, und somit sind die Elemente

$$a, a+1, \ldots, a+p-1$$

die p verschiedenen Nullstellen von f. Falls eine dieser Nullstellen in K liegt, dann auch alle, d.h., f zerfällt dann schon in K in Linearfaktoren. Klar ist damit auch (wegen Lemma 4.26), dass L in jedem Fall der Zerfällungskörper von f ist, insbesondere ist $L \supset K$ eine Galoiserweiterung. Falls $L = K$ gilt, ist dies natürlich eine zyklische Erweiterung, d.h., wir können uns im folgenden auf den Fall, dass f keine Nullstelle in K hat, beschränken. Wir müssen zeigen, dass f dann schon irreduzibel in $K[x]$ ist. Sei also $f = g \cdot h$, wobei g und h nicht-konstant und unitär sind. Es gilt

$$f = \prod_{i=0}^{p-1} (x - a - i) \in L[x]$$

und das Polynom g ist ein Produkt gewisser dieser Faktoren. Sei $d := \deg(g) < p$, also $g = x^d + b_{d-1}x^{d-1} + \ldots + b_0$. Dann gilt $b_{d-1} = -d \cdot a + j$, wobei j ein Element in K ist, was aber sogar im Bild des Homomorphismus $\mathbb{Z} \hookrightarrow K$ (dem sogenannten Primkörper von K) liegt. Dieses Bild ist isomorph zu $\mathbb{F}_p$. Es ist also $b_{d-1} = -d \cdot a + j \in K$, aber $p \nmid d$, also muss $a \in K$ gelten, und damit hat f eine Nullstelle in K, was wir ausgeschlossen hatten. Somit muss also f irreduzibel sein, wenn es keine Nullstellen in K hat. Sei jetzt $\sigma \in \mathrm{Gal}(L/K)$ mit $\sigma(a) = a + 1$ (solch ein Element aus $\mathrm{Gal}(L/K)$ existiert nach Lemma 4.20), dann ist $\mathrm{ord}(\sigma) \geq p$ (weil eben die Elemente $\{a, a+1, \ldots, a+(p-1)\}$ verschieden sind), da aber $\mathrm{ord}(\mathrm{Gal}(L/K)) = [L : K] = \deg(f) = p$ gilt, ist dann $\mathrm{Gal}(L/K)$ ist zyklisch mit Erzeuger σ und Ordnung p.

□

Wir beginnen nun mit dem eingangs angekündigtem Studium der Auflösbarkeit von Gleichungen. Diese charakterisieren wir in körpertheoretische Art und Weise.

Definition 5.21. *Sei $L \supset K$ eine endliche Körpererweiterung. Sie heißt*

1. durch Radikale auflösbar*, falls es eine Erweiterung $E \supset L$ gibt, so dass eine Körperkette*

$$K = E_0 \subset E_1 \subset \ldots \subset E_m = E$$

existiert, so dass für alle $i \in \{0, \ldots, m-1\}$ gilt: $E_{i+1} = E_i(a)$, wobei a eines der folgenden Elemente ist:

   1. *Eine Einheitswurzel,*

   2. *Eine Nullstelle des Polynoms $x^n - c \in E_i[x]$ mit $\mathrm{char}(K) \nmid n$,*

   3. *Eine Nullstelle des Polynoms $x^p - x - c \in E_i[x]$ mit $\mathrm{char}(K) = p > 0$.*

2. auflösbar*, falls es eine Erweiterung $E \supset L$ gibt, so dass $E \supset K$ eine Galoiserweiterung und so dass $G := \mathrm{Gal}(E/K)$ eine auflösbare Gruppe im Sinne von Definition 2.41 ist (zur Erinnerung: dies bedeutet, dass es eine Normalreihe $G = G_0 \supset G_1 \supset \ldots \supset G_n = \{1\}$ mit abelschen Quotienten G_{i-1}/G_i gibt).*

Man bemerke, dass sowohl durch Radikale auflösbare als auch auflösbare Erweiterungen stets separabel sind. Ist $L \supset K$ durch Radikale auflösbar und $\mathrm{char}(K) = 0$, so existiert für alle $a \in L$ eine Formel, welche a aus Elementen von K durch Anwenden der Grundrechenarten und durch iteriertes Wurzelziehen berechnet.
Sei $f \in K[x]$ ein nicht-konstantes separables Polynom und L ein Zerfällungskörper von f. Dann heißt f auflösbar bzw. durch Radikale auflösbar, falls $L \supset K$ auflösbar bzw. durch Radikale auflösbar ist.

Das Ziel dieses Abschnitts ist es, zu zeigen, dass die Begriffe *auflösbar* und *auflösbar durch Radikale* äquivalent sind. Dazu zeigen wir zunächst einige einfache Eigenschaften dieser beiden Begriffe.

Lemma 5.22. *1. Falls die Erweiterung $L \supset K$ Galoissch ist, dann ist sie auflösbar genau dann, wenn $\mathrm{Gal}(L/K)$ auflösbar ist.*

2. Sei $[L : K] < \infty$, und $F \supset K$ eine beliebige Erweiterung (welche L nicht unbedingt enthält). Wir können L durch einen K-Homomorphismus in einen algebraischen Abschluss $\overline{F}$ einbetten (genauer, wir können die Einbettung $K \hookrightarrow \overline{F}$ mit Satz 4.21 zu einem K-Homomorphismus $L \hookrightarrow \overline{F}$ ausdehenen). Dann sei FL das Kompositum von F und L in $\overline{F}$. Dann gilt: ist $L \supset K$ auflösbar (insbesondere ist dann nach Punkt 1. $\mathrm{Gal}(L/K)$ auflösbar, falls $L \supset K$ Galoissch ist) bzw. durch Radikale auflösbar, so ist auch FL/F auflösbar bzw. durch Radikale auflösbar.

Beweis. 1. Sei $L \supset K$ auflösbar, d.h., es gibt eine Erweiterung $M \supset L$, so dass $M \supset K$ Galoissch mit auflösbarer Galoisgruppe $\mathrm{Gal}(M/K)$ ist. Da die Erweiterung $L \supset K$ selbst Galoissch sein soll, ist sie insbesondere normal, und nach dem Hauptsatz der Galoistheorie ist dann $\mathrm{Gal}(M/L)$ ein Normalteiler in $\mathrm{Gal}(M/K)$ und wir haben $\mathrm{Gal}(L/K) \cong \mathrm{Gal}(M/K)/\mathrm{Gal}(M/L)$. Wir wissen (Satz 2.45), dass eine Untergruppe einer auflösbaren Gruppe stets auflösbar ist, und dass für einen Normalteiler $U \lhd G$ in einer Gruppe G gilt: G ist auflösbar genau dann, wenn U und G/U auflösbar sind. Ist also $\mathrm{Gal}(M/K)$ auflösbar, dann auch $\mathrm{Gal}(L/K)$. Ist andererseits $\mathrm{Gal}(L/K)$ auflösbar, dann ist nach Definition $L \supset K$ auflösbar, weil wir als Erweiterungskörper E von L, so dass $\mathrm{Gal}(E/K)$ auflösbar ist, einfach $E := L$ nehmen können.

2. Wenn $L \supset K$ auflösbar ist, dann existiert eine endliche Galoiserweiterung $E \supset K$ mit $L \subset E$, so dass $\mathrm{Gal}(E/K)$ eine auflösbare Gruppe ist. Die Einbettung $L \hookrightarrow \overline{F}$ lässt sich auf E fortsetzen. Da E endlich und separabel über K ist, gilt nach dem Satz vom primitiven Element (Satz 4.40), dass $E = K(a)$ für ein $a \in \overline{F}$ ist. Da E auch normal ist, ist es also der Zerfällungskörper von $\mathrm{MinPol}_K(a)$. Dann können wir $EF = F(a)$ als Zerfällungskörper von $\mathrm{MinPol}_K(a)$, gesehen als Element von $F[x]$ konstruieren. Da $\mathrm{MinPol}_K(a)$ natürlich separabel ist (egal, ob als Element von $K[x]$ oder $F[x]$), ist $EF \supset F$ separabel und daher Galoissch (und natürlich endlich). Wir zeigen jetzt, dass es einen injektiven Gruppenhomomorphismus $\mathrm{Gal}(EF/F) \hookrightarrow \mathrm{Gal}(E/K)$ gibt, d.h., wir können $\mathrm{Gal}(EF/F)$ als Untergruppe von $\mathrm{Gal}(E/K)$ auffassen, und daher folgt aus der Auflösbarkeit von $\mathrm{Gal}(E/K)$ die von

$\mathrm{Gal}(EF/F)$, und dies bedeutet wegen $EF \supset FL$ nichts anderes, als dass $FL \supset F$ auflösbar im Sinne von Definition 5.21, 2. ist.

Sei also $\sigma \in \mathrm{Gal}(EF/F)$ gegeben, dann gilt natürlich $\sigma_{|K} = \mathrm{id}_K$ (wegen $K \subset F$), also ist die Einschränkung $\sigma_{|E}$ ein Element von $\mathrm{Hom}_K(E, \overline{F})$. Da aber $E \supset K$ normal ist, gilt $\sigma_{|E} \in \mathrm{Aut}_K(E) = \mathrm{Gal}(E/K)$. Dies liefert eine Gruppenhomomorphismus $\mathrm{Gal}(EF/F) \to \mathrm{Gal}(E/K)$. Wir haben noch zu zeigen, dass dieser injektiv ist. Sei $\sigma_{|E} = \mathrm{id}_E$, dann folgt aus $EF = E(F)$ (und der Tatsache, dass immer $\sigma_{|F} = \mathrm{id}_F$ ist, wegen $\sigma \in \mathrm{Gal}(EF/F)$), dass $\sigma = \mathrm{id}_{EF}$ ist. Dies beweist die Injektivität.

Sei andererseits $L \supset K$ durch Radikale auflösbar, d.h., es existiert eine Kette

$$K = E_0 \subset E_1 \subset \ldots \subset E_m = E$$

so dass E_{i+1} aus E_i durch Adjunktion eines Elementes der 3 Typen aus Definition 5.21 hervorgeht, dann ist

$$F = E_0F \subset E_1F \subset \ldots \subset E_mF = EF$$

eine entsprechende Kette von $EF \supset F$, dies zeigt, dass $LF \supset F$ durch Radikale auflösbar ist, falls $L \supset K$ durch Radikale auflösbar ist.

□

Um den uns eigentlich interessierenden Satz zu zeigen, brauchen wir noch folgende Hilfsaussage.

Lemma 5.23. *Seien $K \subset L \subset M$ endliche Körpererweiterungen, dann ist $M \supset K$ genau dann auflösbar bzw. durch Radikale auflösbar, wenn $M \supset L$ sowie $L \supset K$ auflösbar bzw. durch Radikale auflösbar sind.*

Beweis. Sei $M \supset K$ auflösbar, mit Erweiterungskörper $M' \supset M \supset K$, so dass $M' \supset K$ Galoissch und $\mathrm{Gal}(M'/K)$ auflösbar ist. Natürlich können wir M' auch als Erweiterungskörper von L auffassen, und dann ist nach Definition auch $L \supset K$ auflösbar. Andererseits ist $\mathrm{Gal}(M'/L)$ eine Untergruppe von $\mathrm{Gal}(M'/K)$, also auch auflösbar, und dies bedeutet (wieder nach Definition 5.21), dass auch $M \supset L$ auflösbar ist.
Wir nehmen nun an, dass $M \supset L$ und $L \supset K$ auflösbar sind. Wir wählen Erweiterungen $L' \supset L$ und $M' \supset M$, so dass $L' \supset K$ und $M' \supset L$ Galoiserweiterungen und die Gruppen $\mathrm{Gal}(L'/K)$ und $\mathrm{Gal}(M'/L)$ auflösbar sind. Dann ist nach dem letzten Lemma (Lemma 5.22) auch $L'M' \supset L'$ Galoissch und die Gruppe $\mathrm{Gal}(L'M'/L')$ ist auflösbar. Wir können also statt der Körperkette $K \subset L \subset M$ auch die Körperkette $K \subset L' \subset L'M'$ betrachten. Mit anderen Worten, wir können ohne Beschränkung der Allgemeinheit annehmen, dass schon die Erweiterungen $L \supset K$ und $M \supset L$ Galoissch mit auflösbaren Galoisgruppen $\mathrm{Gal}(L/K)$ und $\mathrm{Gal}(M/L)$ sind.
Da also $L \supset K$ und $M \supset L$ Galoissch und daher separabel sind, ist auch $M \supset K$ separabel (Lemma 4.38). Hingegen braucht $M \supset K$ nicht normal zu sein, in diesem Fall gehen wir zu einer normalen Hülle $M' \supset K$ über, von der wir schon einmal (Beweis von Korollar 5.9) gezeigt haben, dass sie auch separabel, also Galoissch über K ist. Es sei daran erinnert, wie M' konstruiert werden kann: M' ist das Kompositum aller Körper $\sigma(M)$, wobei σ die Menge aller K-Homomorphismen $\sigma : M \to \overline{M}$ durchläuft (dies folgt aus Satz 4.28). Klar ist auch, dass für jedes $\sigma \in \mathrm{Hom}_K(M, \overline{M})$ gilt, dass $\sigma(L) = L$ ist (Normalität von $L \supset K$), und daher ist die Erweiterung $\sigma(M) \supset L$ isomorph zu $M \supset L$, insbesondere ist $\mathrm{Gal}(M/L) \cong \mathrm{Gal}(\sigma(M)/L)$.
Wir wollen jetzt zeigen, dass $\mathrm{Gal}(M'/K)$ auflösbar ist. Dies lässt sich auf die Auflösbarkeit von $\mathrm{Gal}(M'/L)$ reduzieren, denn wir haben die surjektive Abbildung

$$\mathrm{Gal}(M'/K) \to \mathrm{Gal}(L/K)$$

deren Kern genau $\mathrm{Gal}(M'/L)$ ist. Die Auflösbarkeit von $\mathrm{Gal}(L/K)$ ist gegeben, daher ist noch die von $\mathrm{Gal}(M'/L)$ zu zeigen. Da M' das Kompositum von $\sigma(M)$ für alle $\sigma \in Hom_K(M, \overline{M})$ ist, folgt aus Lemma 5.12, dass

$$\begin{array}{ccc} \mathrm{Gal}(M'/L) & \longrightarrow & \prod_{\sigma \in \mathrm{Hom}_K(M,\overline{M})} \mathrm{Gal}(\sigma(M)/L) \\ \tau & \longmapsto & \left(\tau_{|\sigma(M)}\right)_\sigma \end{array}$$

ein injektiver Gruppenhomomorphismus ist. Wir haben also nur die Auflösbarkeit der rechten Seite zu zeigen. Jeder Faktor dieser Gruppe ist auflösbar (denn isomorph zu $\mathrm{Gal}(M/L)$), daher ist auch das Produkt auflösbar (Dies ist eine einfache Übung, z.B. kann man mit Induktion über die Anzahl der Faktoren argumentieren).
Wir müssen jetzt noch die Transitivität der Eigenschaft „durch Radikale auflösbar“ zeigen. Sei zunächst vorausgesetzt, dass $M \supset K$ durch Radikale auflösbar ist. Dann gilt die (wieder nach der Definition des Begriffes „auflösbar durch Radikale“) auch für die Erweiterung $L \supset K$. Weil $M \supset K$ durch Radikale auflösbar ist, hat man also eine Kette $K = E_0 \subset E_1 \subset \ldots \subset E_n = M'$ für eine Oberkörper M' von M, wobei jeder Körper E_{i+1} aus E_i durch Adjunktion eines Elementes der Typen 1. bis 3. aus Definition 5.21 entsteht. Dann kann man das Kompositum dieser Kette mit L betrachten, dies liefert eine entsprechende Kette für die Erweiterung $M'L \supset L$. $M'L$ ist ein Oberkörper von M, und daher ist $M \supset L$ auch durch Radikale auflösbar.
Seien nun $M \supset L$ und $L \supset K$ durch Radikale auflösbar. Es gibt dann Erweiterungen $L' \supset L$ und $M' \supset M$, so dass $L' \supset K$ und $M' \supset L$ durch Körperketten wie in Definition 5.21 ausgeschöpft werden können. Man bilde das Kompositum $L'M$ in $\overline{M}$ und dann sagt Lemma 5.22, dass $L'M \supset L'$ durch Radikale auflösbar ist. Durch das Zusammenfügen der Körperketten von $L'M \supset L'$ und $L' \supset K$ erhält man eine solche Kette für $L'M \supset K$, und $L'M$ ist ein Oberkörper von M, also ist auch $M \supset K$ durch Radikale auflösbar. □

Der wichtigste Satz dieses Abschnittes ist der folgende, welcher ein präzises Kriterium für die Lösbarkeit algebraischer Gleichungen impliziert.

Satz 5.24. *Eine endlich Körpererweiterung $L \supset K$ ist genau dann auflösbar, wenn sie durch Radikale auflösbar ist.*

Beweis. Sei zunächst $L \supset K$ auflösbar. Wie schon zuvor nehmen wir durch Vergrößern von L an, dass $L \supset K$ selbst Galoissch mit auflösbarer Galoisgruppe $\mathrm{Gal}(L/K)$ ist. Wir definieren

$$m := \prod_{\substack{p \text{ Primzahl} \\ p \nmid \mathrm{char}(K) \\ p \mid [L:K]}} p$$

Sei ζ_m eine primitive m-te Einheitswurzel und $F = K(\zeta_m)$. Wir gehen jetzt wie in Lemma 5.22 vor, d.h., wir betrachten das Kompositum FL in einem algebraischen Abschluss von L. Dann haben wir $K \subset F \subset FL$, und die Erweiterung $F \supset K$ ist nach Definition durch Radikale auflösbar. Es genügt also nach Lemma 5.23, zu zeigen, dass $FL \supset F$ durch Radikale auflösbar ist (denn dann wissen wir, dass $FL \supset K$ durch Radikale auflösbar ist, und weil FL ein Oberkörper von L ist, ist dann $L \supset K$ nach Definition durch Radikale auflösbar). Wir wissen aus Lemma 5.22, dass die Auflösbarkeit von $L \supset K$ die Auflösbarkeit von $FL \supset F$ impliziert. Nun ist aber die $FL \supset F$ selbst eine Galoiserweiterung: Nach Voraussetzung ist $L \supset K$ eine Galoiserweiterung, und ebenso ist $F \supset K$ nach Satz 5.17, 1. eine Galoiserweiterung. Dann ist nach Satz 5.12, 1. auch $FL \supset K$ eine Galoiserweiterung, und damit nach Satz 5.2, 1. auch $FL \supset F$. Dann folgt aber nach Lemma 5.22, dass die Gruppe $\mathrm{Gal}(FL/F)$ auflösbar ist, es gibt also eine Normalreihe

$$\mathrm{Gal}(FL/F) = G_0 \supset \ldots \supset G_n = \{1\}$$

mit abelschen Quotienten. Dann folgt aus Satz 2.45, dass man diese Normalreihe verfeinern kann, so dass die Quotienten G_i/G_{i+1} zyklisch von Primzahlordnung sind. Nach dem Hauptsatz der Galoistheorie entspricht dieser Normalreihe eine Kette von Unterkörpern

$$F = F_0 \subset F_1 \subset \ldots \subset F_n = FL$$

mit $F_i = (FL)^{G_i}$ und so, dass F_{i+1}/F_i ein Galoiserweiterung mit zyklischer Galoisgruppe $\mathrm{Gal}(F_{i+1}/F_i) \cong G_i/G_{i+1}$ der Ordnung p_i für eine Primzahl p_i ist. Also ist p_i ein Teiler von $[FL : F]$, aber wir hatten in Lemma 5.12 gezeigt, dass $\mathrm{Gal}(FL/F) \cong \mathrm{Gal}(L/F \cap L)$ gilt, und natürlich ist $\mathrm{Gal}(L/F \cap L) < \mathrm{Gal}(L/K)$.

Daher ist p_i auch ein Teiler von $\text{ord}(\text{Gal}(L/K)) = [L : K]$, und deshalb gilt $p_i | m$, falls $p \neq \text{char}(K)$ ist. Daher ist eine gewisse Potenz von ζ_m eine primitive p_i-te Einheitswurzel, und diese ist also (wegen $\zeta_m \in F$) in F enthalten. Also ist diese primitive p_i-te Einheitswurzel auch in F_i enthalten, und nach Korollar 5.19 gilt dann $F_{i+1} = F_i(c_i)$, wobei c_i eine Nullstelle von $x^{p_i} - a \in F_i[x]$ ist. Im Fall $\text{char}(K) = p_i$ folgt aus Korollar 5.20, dass c_i Nullstelle von $x^{p_i} - x - a \in F_i[x]$ ist. Also ist $FL \supset F$ in jedem Fall durch Radikale auflösbar. Sei jetzt umgekehrt vorausgesetzt, dass $L \supset K$ durch Radikale auflösbar ist. Dann können wir wegen Lemma 5.22 und Lemma 5.23 annehmen, dass es eine Körperkette

$$K = K_0 \subset K_1 \subset \ldots \subset K_m = L$$

gibt, so dass die Erweiterungen $K_{i+1} \supset K_i$ vom Typ 1., 2., oder 3. wie in Definition 5.21 sind. Nach Lemma 5.23 müssen wir nur zeigen, dass jede einzelne Erweiterung $K_{i+1} \supset K_i$ auflösbar ist. Sei $K_{i+1} \supset K_i$ vom Typ 1., d.h., K_{i+1} entsteht aus K_i durch Adjunktion einer Einheitswurzel. Dann handelt es sich nach Satz 5.17 um eine abelsche Galoiserweiterung, also ist $\text{Gal}(K_{i+1}/K_i)$ auflösbar.
Analog ist (wegen Korollar 5.20) die Erweiterung $K_{i+1} \supset K_i$ im Fall des Typs 3., falls also $K_{i+1} = K_i(c_i)$, wobei c_i Nullstelle von $x^{p_i} - x - a$ ist und $\text{char}(K_i) = p_i$ gilt, zyklisch und Galoissch, und daher ist $\text{Gal}(K_{i+1}/K_i)$ auch in diesem Fall auflösbar.
Sei nun $K_{i+1} = K_i(c_i)$, wobei c_i Nullstelle von $x^n - a$ ist und so, dass $\text{char}(K) \nmid n$ gilt. Definiere wieder $F = K_i(\zeta_n)$, für eine primitive n-te Einheitswurzel ζ_n. Wir betten F in einen algebraischen Abschluss von K_i ein und betrachten die Erweiterungen

$$K_i \subset F \subset FK_i = F(c).$$

Nach Satz 5.17 ist F/K_i abelsch und also auflösbar. Nach Korollar 5.19 ist $F(c)/F$ galoisch und zyklisch und auch auflösbar. Daher ist nach Lemma 5.23 auch die Erweiterung $F(c) = FK_{i+1} \supset K_i$ auflösbar, und daher auch die Erweiterung $K_{i+1} \supset K_i$ (weil gilt $\text{Gal}(K_{i+1}/K_i) < \text{Gal}(FK_{i+1}/K_i)$). □

Als Konsequenz können wir Gleichungen finden, welche nicht durch Radikale auflösbar sind.

Korollar 5.25. *Sei $K \subset \mathbb{R}$ ein Körper, $n \geq 5$ eine Primzahl und $f = a_n x^n + \ldots + a_0 \in K[x]$ irreduzibel mit $f = \prod_{i=1}^{n}(x - \alpha_i)$, $\alpha_1, \ldots, \alpha_n \in \mathbb{C}$. Nach Lemma 4.30 sind alle Nullstellen $\alpha_1, ..., \alpha_n$ verschieden. Die Nullstellen seien so, daß gilt:*

$$\alpha_3, ..., \alpha_n \in \mathbb{R} \quad \text{und} \quad \alpha_1, \alpha_2 \in \mathbb{C} - \mathbb{R}, \quad \text{also} \quad \overline{\alpha_1} = \alpha_2.$$

Sei L ein Zerfällungskörper von f. Dann ist $L \supset K$ nicht durch Radikale auflösbar. Es gibt daher keine Formel, welche die Nullstellen $\alpha_1, \ldots, \alpha_n$ durch Anwenden der Grundrechenoperationen und iteriertes Wurzelziehen aus den Koeffizienten $a_0, \ldots, a_n$ bestimmt.

Beweis. Es ist $L \cong K(\alpha_1, \ldots, \alpha_n)$, und nach Aufgabe 4 auf Übungsblatt 13 gilt $\text{Gal}(L/K) \cong S_n$. Daher ist nach Korollar 2.47 die Gruppe $\text{Gal}(L/K)$ nicht auflösbar. Somit kann $L \supset K$ nach dem letzten Satz (Satz 5.24) auch nicht durch Radikale auflösbar sein. □

Literaturverzeichnis

[1] Siegfried Bosch, *Algebra*, Springer, 7.Auflage (2008).

[2] Annette Werner, *Algebra*, Vorlesungsskript, Johannes-Goethe-Universität Frankfurt, verfügbar unter `http://www.uni-frankfurt.de/fb/fb12/mathematik/ag/personen/werner/skripte/algebra.pdf`

[3] Claus Hertling, *Algebra*, Vorlesungsskript, Universität Mannheim