Gregor Kemper

Algebra

Vorlesungsmanuskript*
Technische Universität München

29. März 2018

*Verbesserungsvorschläge und Meldungen von Fehlern bitte an: kemper@ma.tum.de.

Inhaltsverzeichnis

Gruppen

Der erste Teil der Vorlesung besteht aus einer Einführung in die Gruppentheorie.

1 Gruppen und Untergruppen

Definition 1.1. *Eine* **Gruppe** *ist eine Menge G zusammen mit einer Abbildung $G \times G \to G$, $(\sigma, \tau) \mapsto \sigma \cdot \tau$, so dass die folgenden Axiome gelten:*

$$\forall\ \sigma, \tau, \rho \in G: \quad (\sigma \cdot \tau) \cdot \rho = \sigma \cdot (\tau \cdot \rho), \tag{AG}$$

$$\exists\ \iota \in G: \quad \forall\ \sigma \in G: \quad \iota \cdot \sigma = \sigma, \tag{NE}$$

$$\forall\ \sigma \in G: \quad \exists\ \sigma' \in G: \quad \sigma' \cdot \sigma = \iota. \tag{IE}$$

(Hierbei ist (IE) *eigentlich eine weitere Eigenschaft von ι.)*

Eine Gruppe G heißt **abelsch** *(oder auch kommutativ), falls außerdem gilt:*

$$\forall\ \sigma, \tau \in G: \quad \sigma \cdot \tau = \tau \cdot \sigma. \tag{KG}$$

Sehr häufig werden wir bei Gruppen $\sigma\tau$ statt $\sigma \cdot \tau$ schreiben.

Die Elementanzahl $|G| \in \mathbb{N} \cup \{\infty\}$ heißt die **Ordnung** *der Gruppe G.*

Häufig werden folgende Abschwächungen des Gruppenbegriffs betrachtet:

Halbgruppe: Nur (AG) wird gefordert.
Monoid: Es wird (AG) gefordert und außerdem

$$\exists\ \iota \in G: \quad \forall\ \sigma \in G: \quad \iota \cdot \sigma = \sigma \cdot \iota = \sigma. \tag{NE'}$$

Bevor wir Beispiele von Gruppen anschauen, beweisen wir das folgende Resultat:

Satz 1.2 (elementare Eigenschaften von Gruppen)**.** *Für jede Gruppe G gelten:*

(a) Es gibt genau ein $\iota \in G$, das (NE) erfüllt. Dieses ι heißt das **neutrale Element** *von G.*
(b) Für jedes $\sigma \in G$ gibt es genau ein $\sigma' \in G$, das (IE) erfüllt. Dieses σ' heißt das **inverse Element** *zu σ und wird mit $\sigma' = \sigma^{-1}$ bezeichnet.*
(c) Für jedes $\sigma \in G$ gelten

$$\sigma\iota = \sigma \quad \textit{und} \quad \sigma\sigma^{-1} = \iota.$$

Beweis. Wir beginnen mit (c). Für $\sigma \in G$ gibt es wegen (IE) $\sigma' \in G$ mit $\sigma'\sigma = \iota$ und $\sigma'' \in G$ mit $\sigma''\sigma' = \iota$. Es folgt

$$\begin{aligned} \sigma\sigma' &\underset{\text{(NE)}}{=} \iota(\sigma\sigma') \underset{\text{(IE)}}{=} (\sigma''\sigma')(\sigma\sigma') \underset{\text{(AG)}}{=} \sigma''\left(\sigma'(\sigma\sigma')\right) \\ &\underset{\text{(AG)}}{=} \sigma''\left((\sigma'\sigma)\sigma'\right) \underset{\text{(IE)}}{=} \sigma''(\iota\sigma') \underset{\text{(NE)}}{=} \sigma''\sigma' \underset{\text{(IE)}}{=} \iota, \end{aligned} \tag{1.1}$$

und weiter

$$\sigma\iota \underset{\text{(IE)}}{=} \sigma(\sigma'\sigma) \underset{\text{(AG)}}{=} (\sigma\sigma')\sigma \underset{(1.1)}{=} \iota\sigma \underset{\text{(NE)}}{=} \sigma. \tag{1.2}$$

Damit ist (c) nachgewiesen. Zum Beweis von (a) sei $\widetilde{\iota} \in G$ ein weiteres Element, das (NE) erfüllt. Dann folgt

$$\widetilde{\iota} \underset{(1.2)}{=} \widetilde{\iota}\iota \underset{\text{(NE)}}{=} \iota,$$

was die behauptete Eindeutigkeit liefert. Zum Beweis von (b) sei $\widetilde{\sigma} \in G$ ein weiteres Element mit $\widetilde{\sigma}\sigma = \iota$. Dann folgt

$$\widetilde{\sigma} \underset{(1.2)}{=} \widetilde{\sigma}\iota \underset{(1.1)}{=} \widetilde{\sigma}(\sigma\sigma') \underset{\text{(AG)}}{=} (\widetilde{\sigma}\sigma)\sigma' = \iota\sigma' \underset{\text{(NE)}}{=} \sigma'.$$

Dies schließt den Beweis ab. □

Beispiel 1.3. (1) Die Mengen $\mathbb{Z}$, $\mathbb{Q}$ und $\mathbb{R}$ zusammen mit der gewöhnlichen Addition sind abelsche Gruppen.
(2) Die Menge $\mathbb{Z}$ zusammen mit der gewöhnlichen Multiplikation ist ein Monoid.
(3) Es sei V ein Vektorraum. Dann ist die allgemeine lineare Gruppe $\mathrm{GL}(V)$ mit $\varphi \cdot \psi := \varphi \circ \psi$ (Hintereinanderausführung) für $\varphi, \psi \in \mathrm{GL}(V)$ eine Gruppe. $\mathrm{GL}(V)$ ist nicht abelsch, falls $\dim(V) \geq 2$.
(4) Die Menge der Drehungen, die ein Quadrat in sich selbst überführen, ist mit der Hintereinanderausführung eine Gruppe. Sie hat 4 Elemente.
(5) Es seien $n \in \mathbb{N}_0$ eine natürliche Zahl und $\Omega := \{1, \ldots, n\}$. Dann ist

$$S_n := \{\sigma\colon \Omega \to \Omega \mid \sigma \text{ ist bijektiv}\}$$

mit der Hintereinanderausführung eine Gruppe. S_n heißt die **symmetrische Gruppe** und hat die Ordnung $|S_n| = n!$. S_n ist nur für $n \le 2$ abelsch. ◁

Für eine Gruppe G gelten die folgenden Rechenregeln:

- $\forall\ \sigma \in G: \quad (\sigma^{-1})^{-1} = \sigma$,
- $\forall\ \sigma, \tau \in G: \quad (\sigma\tau)^{-1} = \tau^{-1}\sigma^{-1}$.

Wir verwenden die folgenden Schreibweisen:

- Für $n \in \mathbb{N}_{>0}$: $\sigma^n = \underbrace{\sigma \cdots \sigma}_{n \text{ mal}}$, $\sigma^0 = \iota$ und $\sigma^{-n} = (\sigma^n)^{-1}$.
- Abelsche Gruppen schreiben wir manchmal *additiv*: Statt $\sigma \cdot \tau$ schreiben wir $\sigma + \tau$. In diesem Fall benutzen wir eher lateinische Buchstaben (statt griechische) für die Gruppenelemente, und wir schreiben 0 für das neutrale Element und $-a$ für das inverse Element von $a \in G$.

Definition 1.4. *Eine Teilmenge $H \subseteq G$ einer Gruppe heißt* **Untergruppe**, *falls $\iota \in H$, und für alle $\sigma, \tau \in H$ auch das Produkt $\sigma\tau$ und das Inverse σ^{-1} Elemente von H sind. Es folgt, dass H (zusammen mit der auf $H \times H$ eingeschränkten Abbildung $G \times G \to G$) eine Gruppe ist.*

Beispiel 1.5. (1) Für $n \in \mathbb{N}_0$ ist die Gruppe

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

wegen der Multiplikativität des Vorzeichens sgn eine Untergruppe. A_n heißt die **alternierende Gruppe**.

(2) Es sei V ein endlich-dimensionaler Vektorraum. Wegen des Determinantenmultiplikationssatzes ist die spezielle lineare Gruppe $\mathrm{SL}(V) \subseteq \mathrm{GL}(V)$ eine Untergruppe.

(3) Für jede Gruppe G sind $\{\iota\} \subseteq G$ und $G \subseteq G$ Untergruppen. Diese beiden bezeichnet man auch als die *trivialen Untergruppen*.

(4) Für die symmetrische Gruppe

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

finden wir folgende Untergruppen: die trivialen Untergruppen $\{\mathrm{id}\}$ und S_3, die alternierende Gruppe $A_3 = \{\mathrm{id}, (1,2,3), (3,2,1)\}$ und die Untergruppen $H_1 = \{\mathrm{id}, (1,2)\}$, $H_2 = \{\mathrm{id}, (1,3)\}$ und $H_3 = \{\mathrm{id}, (2,3)\}$. Es stellt sich heraus, dass dies alle Untergruppen sind. ◁

Proposition 1.6 (Schnitte von Untergruppen)**.** *Es seien G eine Gruppe und $\mathcal{U} \subseteq \mathfrak{P}(G)$ (die Potenzmenge) eine nicht-leere Menge bestehend aus Untergruppen von G. Dann ist auch der Schnitt*

$$\bigcap_{H \in \mathcal{U}} H \subseteq G$$

eine Untergruppe.

Beweis. Das neutrale Element $\iota \in G$ ist Element von jedem $H \in \mathcal{U}$, also auch vom Schnitt. Weiter liegen für zwei Elemente σ, τ aus dem Schnitt auch das Produkt $\sigma\tau$ und das Inverse σ^{-1} im Schnitt. Damit ist alles gezeigt. □

Proposition 1.6 ermöglicht die folgende Definition:

Definition 1.7. *Es seien G eine Gruppe und $M \subseteq G$ eine Teilmenge. Dann heißt*

$$\langle M \rangle := \bigcap_{\substack{H \in \mathfrak{P}(G), \\ H \text{ Untergruppe}, \\ M \subseteq H}} H$$

die von M **erzeugte Untergruppe** *von G (auch: das* **Erzeugnis** *von M). Dies ist die kleinste Untergruppe von G, die M als Teilmenge enthält. Es ist leicht zu sehen, dass $\langle M \rangle$ aus allen Produkten $\sigma_1\sigma_2 \cdots \sigma_k$ beliebiger Länge k aus Elementen σ_i von M oder Inversen von Elementen von M besteht. Falls $M = \{\sigma_1, \ldots, \sigma_n\}$ endlich ist, schreiben wir auch $\langle \sigma_1, \ldots, \sigma_n \rangle$ für $\langle M \rangle$.*

Falls es eine endliche Teilmenge $M \subseteq G$ gibt mit $G = \langle M \rangle$, so heißt G **endlich erzeugt**. *Insbesondere ist jede endliche Gruppe auch endlich erzeugt. Im Spezialfall $M = \{\sigma\}$ heißt*

$$\langle M \rangle = \langle \sigma \rangle = \left\{\sigma^i \mid i \in \mathbb{Z}\right\}$$

eine **zyklische Gruppe**. *Für $\sigma \in G$ heißt*

$$\operatorname{ord}(\sigma) := |\langle \sigma \rangle| \in \mathbb{N} \cup \{\infty\}$$

die **Ordnung** *von σ.*

Es ist leicht zu sehen, dass

$$\operatorname{ord}(\sigma) = \min\{i \in \mathbb{N}_{>0} \mid \sigma^i = \iota\} \tag{1.3}$$

gilt (mit der Konvention $\min \emptyset := \infty$). Falls $\operatorname{ord}(\sigma) = k < \infty$, so gilt nämlich

$$\langle \sigma \rangle = \{\iota, \sigma, \sigma^2, \ldots, \sigma^{k-1}\}.$$

Beispiel 1.8. (1) $\mathbb{Z}$ zusammen mit der gewöhnlichen Addition ist zyklisch: $\mathbb{Z} = \langle 1 \rangle$. Es gilt $\operatorname{ord}(1) = \infty$.

(2) $\mathbb{Q}$ zusammen mit der gewöhnlichen Addition ist nicht endlich erzeugt. (Frage: Wie lässt sich das begründen?)

(3) Die „Drehgruppe des Quadrats“ (siehe Beispiel 1.3(4)) ist zyklisch von der Ordnung 4.

(4) Es sei $n \in \mathbb{N}_{>0}$ eine positive natürliche Zahl. Wir schreiben

$$\mathbb{Z}/(n) = \{a + n\mathbb{Z} \mid a \in \mathbb{Z}\}$$

für den Ring der Restklassen modulo n. Zusammen mit der Addition bildet $\mathbb{Z}/(n)$ eine zyklische Gruppe der Ordnung n, die wir künftig mit Z_n bezeichnen. In diesem Zusammenhang wird $\mathbb{Z}$ zusammen mit der gewöhnlichen Addition oft als Z_∞ bezeichnet.

(5) Für die symmetrische Gruppe S_3 gilt:

$$S_3 = \langle (1,2), (1,3) \rangle = \langle (1,2), (1,2,3) \rangle.$$

Die Transpositionen $(1,2)$, $(1,3)$ und $(2,3)$ haben die Ordnung 2. ◁

Wir werden im Folgenden Begriffe aus der Arithmetik ganzer Zahlen „naiv" benutzen. Für ganze Zahlen $a, b \in \mathbb{Z}$ schreiben wir $a \mid b$, falls a ein Teiler von b ist. Wir werden später auch Primzahlen und die eindeutige Primzerlegung benutzen. Diese Begriffe und Aussagen werden in Abschnitt 13 in einem allgemeineren Rahmen eingeführt und bewiesen. Es entsteht keine Zirkularität unserer Argumente.

Proposition 1.9. *Es sei $\sigma \in G$ ein Gruppenelement von endlicher Ordnung k. Dann gilt für $i \in \mathbb{Z}$ die Äquivalenz*

$$\sigma^i = \iota \quad \Longleftrightarrow \quad k \mid i.$$

Beweis. Wir benutzen Division mit Rest: $i = d \cdot k + r$ mit $d, r \in \mathbb{Z}$ und $0 \le r < k$. Es folgt

$$\sigma^i = \sigma^{kd+r} = (\sigma^k)^d \sigma^r = \sigma^r,$$

also $\sigma^i = \iota$ genau dann, wenn $\sigma^r = \iota$, was wegen (1.3) gleichbedeutend ist mit $r = 0$, also mit $k \mid i$. □

Lemma 1.10 (Zerlegung in Nebenklassen)**.** *Es sei $H \subseteq G$ eine Untergruppe. Für $\sigma, \tau \in G$ schreiben wir $\sigma \sim \tau$, falls $\sigma^{-1}\tau \in H$.*

(a) Durch „$\sim$" wird eine Äquivalenzrelation auf G definiert.

(b) Die Äquivalenzklasse eines $\sigma \in G$ ist

$$[\sigma]_\sim = \sigma H := \{\sigma\rho \mid \rho \in H\}.$$

(c) Für jedes $\sigma \in G$ gilt:

$$|\sigma H| = |H|.$$

Beweis. (a) Wir weisen die Reflexivität, Symmetrie und Transitivität von „$\sim$" nach. Für $\sigma \in G$ gilt $\sigma^{-1}\sigma = \iota \in H$. Falls $\sigma \sim \tau$ mit $\sigma, \tau \in G$ gilt, so folgt

$$\tau^{-1}\sigma = \left(\sigma^{-1}\tau\right)^{-1} \in H,$$

also $\tau \sim \sigma$. Falls schließlich $\sigma \sim \tau$ und $\tau \sim \rho$ mit $\sigma, \tau, \rho \in G$ gelten, so folgt

$$\sigma^{-1}\rho = \sigma^{-1}\tau\tau^{-1}\rho \in H,$$

also $\sigma \sim \rho$.

(b) Für $\tau = \sigma\rho \in \sigma H$ gilt $\sigma^{-1}\tau = \rho \in H$, also $\sigma \sim \tau$. Umgekehrt folgt aus $\sigma \sim \tau$, dass τ ein Element von σH ist.

(c) Dies folgt daraus, dass $H \to \sigma H$, $\rho \mapsto \sigma\rho$ eine Bijektion ist. □

Anmerkung. Man nennt die Mengen σH aus Lemma 1.10(b) **Linksnebenklassen** von H. Entsprechend kann man *Rechtsnebenklassen* betrachten und das Lemma auf diese übertragen. ◁

Die Aufteilung von G in Nebenklassen gibt Anlass zu folgender Definition:

Definition 1.11. *Es sei $H \subseteq G$ eine Untergruppe. Dann heißt*

$$(G : H) := |\{\sigma H \mid \sigma \in G\}| \in \mathbb{N} \cup \{\infty\}$$

(also die Anzahl der Äquivalenzklassen bezüglich der in Lemma 1.10 definierten Äquivalenzrelation) der **Index** *von H (in G).*

Aus Lemma 1.10 folgt die Gleichung

$$\boxed{|G| = |H| \cdot (G : H),} \tag{1.4}$$

und hieraus unsere ersten wirklich interessanten Resultate:

Satz 1.12 (Satz von Lagrange). *Es seien G eine endliche Gruppe und $H \subseteq G$ eine Untergruppe. Dann ist $|H|$ ein Teiler von $|G|$.*

Korollar 1.13 (kleiner Satz von Fermat). *Für jedes Element $\sigma \in G$ einer endlichen Gruppe gilt:*

$$\sigma^{|G|} = \iota.$$

Beweis. Setze $H := \langle\sigma\rangle \subseteq G$. Wegen Satz 1.12 ist $|G|$ ein Vielfaches von $|H| = \operatorname{ord}(\sigma)$, und die Behauptung folgt aus Proposition 1.9. □

Korollar 1.14. *Es sei G eine Gruppe, so dass $|G|$ eine Primzahl ist. Dann ist G zyklisch.*

Beweis. Wegen $|G| > 1$ gibt es $\sigma \in G \setminus \{\iota\}$. Mit $H := \langle\sigma\rangle$ gilt dann $|H| > 1$, und $|H|$ teilt $|G|$. Nach Voraussetzung folgt $|H| = |G|$, also $H = G$. Damit ist G zyklisch. □

Beispiel 1.15. Wir können jetzt die Gruppen der Ordnung ≤ 5 bestimmen.

$|G| = 1$: $G = \{\iota\}$.

$|G| = 2$: G ist zyklisch. Unter Vorwegnahme des Isomorphiebegriffs (siehe Definition 2.9) können wir $G \cong Z_2$ schreiben (siehe Beispiel 1.8(4)). Es beeinträchtigt das Verständnis nicht, wenn diese vorweggenommene Schreibweise hier ignoriert wird.

$|G| = 3$: G ist zyklisch, also $G \cong Z_3$.

$|G| = 4$: Wir betrachten zunächst den Fall, dass G zyklisch ist. Dann kennen wir die Struktur von G (nämlich $G \cong Z_4$). Als zweiten Fall nehmen wir an, dass G *nicht* zyklisch ist. Dann gibt es kein Element der Ordnung 4. Da die Elementordnungen alle Teiler von 4 sind, muss also jedes Element außer ι die Ordnung 2 haben. Es gibt $\sigma \in G \setminus \{\iota\}$ und $\tau \in G \setminus \langle\sigma\rangle$. Man sieht sofort, dass die Elemente $\iota, \sigma, \tau, \sigma\tau$ paarweise verschieden sind, also

$$G = \{\iota, \sigma, \tau, \sigma\tau\}.$$

Außerdem bleibt für das Produkt $\tau\sigma$ nur die Möglichkeit $\tau\sigma = \sigma\tau$. Damit sind alle Produkte von Elementen in G bekannt. Es ist nicht schwer zu verifizieren, dass ein G mit diesem Produkt tatsächlich eine Gruppe bildet. Sie heißt die *Kleinsche Vierergruppe*.

$|G| = 5$: G ist zyklisch, also $G \cong Z_5$.

Nebenbei haben wir gesehen, dass alle Gruppen der Ordnung ≤ 5 abelsch sind. Es gibt aber eine nicht-abelsche Gruppe der Ordnung 6, nämlich die S_3. $\triangleleft$

2 Normalteiler und Homomorphismen

Definition 2.1. *Es sei G eine Gruppe.*

(a) Zwei Elemente $\sigma, \tau \in G$ heißen **konjugiert***, falls es $\rho \in G$ gibt mit*

$$\tau = \rho\sigma\rho^{-1}.$$

Für $\sigma \in G$ schreiben wir

$$[\sigma] := \{\rho\sigma\rho^{-1} \mid \rho \in G\} \subseteq G$$

und nennen diese Menge die **Konjugiertenklasse** *von σ.*

(b) Zwei Untergruppen $H_1, H_2 \subseteq G$ heißen **konjugiert***, falls es $\rho \in G$ gibt mit*

$$H_2 = \rho H_1 \rho^{-1} := \{\rho\sigma\rho^{-1} \mid \sigma \in H_1\}.$$

Eine Untergruppe $N \subseteq G$ heißt **Normalteiler** *von G, falls für alle $\rho \in G$ gilt: $\rho N \rho^{-1} = N$. (Dies ist gleichbedeutend mit $\rho N = N\rho$.) Die Schreibweise $N \trianglelefteq G$ bedeutet, dass N ein Normalteiler von G ist.*

(c) G heißt **einfach***, falls $G \neq \{\iota\}$ und G nur die Normalteiler $\{\iota\}$ und G (also die* trivialen *Normalteiler) hat.*

Beispiel 2.2. (1) Zwei Matrizen in $G = \mathrm{GL}_n(K)$ mit Einträgen in einem Körper sind genau dann konjugiert, wenn sie ähnlich sind.

(2) In Beispiel 1.5(4) haben wir die Untergruppen der S_3 aufgelistet. Man rechnet leicht nach, dass $\{\mathrm{id}\}$, A_3 und S_3 Normalteiler sind, die H_i aber nicht. Sie sind untereinander konjugiert.

(3) Für jede natürliche Zahl n gelten:

$$A_n \trianglelefteq S_n \quad \text{und} \quad \mathrm{SL}_n(K) \trianglelefteq \mathrm{GL}_n(K)$$

(K ein Körper).

(4) In einer abelschen Gruppe ist jede Untergruppe ein Normalteiler.

(5) Ist p eine Primzahl, so ist die zyklische Gruppe Z_p einfach. ◁

Normalteiler zeichnen sich dadurch aus, dass man die Menge ihrer Links- oder Rechtsnebenklassen in sinnvoller Weise mit einer Gruppenstruktur versehen kann. Diese wird im folgenden Satz definiert.

Satz 2.3 (Faktorgruppe)**.** *Es sei $N \trianglelefteq G$ ein Normalteiler einer Gruppe. Dann wird die Menge der (Links-)Nebenklassen von N zu einer Gruppe, indem man für $\sigma, \tau \in G$ definiert:*

$$(\sigma N) \cdot (\tau N) := \sigma\tau N.$$

Diese Gruppe heißt die **Faktorgruppe** *von G nach N (auch: modulo N) und wird mit G/N bezeichnet.*

Beweis. Der wesentliche Teil dieses Beweises ist der Nachweis der *Wohldefiniertheit* des Produkts: Wir müssen nachweisen, dass die Definition von $(\sigma N) \cdot (\tau N)$ nicht von der Wahl der Vertreter σ, τ der Nebenklassen abhängt. Es seien also σ', τ' weitere Vertreter, d.h. $\sigma' N = \sigma N$ und $\tau' N = \tau N$. Dann gibt es $\rho, \eta \in N$ mit $\sigma' = \sigma\rho$ und $\tau' = \tau\eta$. Es folgt

$$\sigma'\tau' N = \sigma\rho\tau\eta N = \sigma\tau \underbrace{\tau^{-1}\rho\tau}_{\in N} \eta N = \sigma\tau N.$$

Nachdem die Wohldefiniertheit geklärt ist, überträgt sich das Assoziativgesetz (AG) von G auf G/N. Ein neutrales Element wird durch $\iota N = N \in G/N$ gegeben, und das inverse Element zu σN ist $\sigma^{-1} N$. □

Ist $N \trianglelefteq G$ ein Normalteiler, so folgt aus (1.4):

$$|G| = |N| \cdot |G/N|. \tag{2.1}$$

Beispiel 2.4. (1) Wegen (2.1) gilt $|S_3/A_3| = 2$, also ist S_3/A_3 nach Beispiel 1.15 zyklisch.

(2) Es sei n eine natürliche Zahl. Die zyklische Gruppe Z_n ist die Faktorgruppe von Z_∞ nach der von n erzeugten Untergruppe. ◁

Definition 2.5. *Es sei G eine Gruppe.*

(a) Die Menge

$$Z(G) := \{\sigma \in G \mid \forall\ \tau \in G:\ \sigma\tau = \tau\sigma\}$$

heißt das **Zentrum** *von G.*

(b) Für $\sigma, \tau \in G$ heißt

$$[\sigma, \tau] := \sigma\tau\sigma^{-1}\tau^{-1}$$

der **Kommutator** *von σ und τ. Es gilt also $\sigma\tau = \tau\sigma$ („σ und τ* kommutieren*") genau dann, wenn $[\sigma, \tau] = \iota$.*

(c) Die von allen Kommutatoren erzeugte Untergruppe

$$G' := \langle [\sigma, \tau] \mid \sigma, \tau \in G \rangle$$

heißt die **Kommutatorgruppe** *von G.*

Bevor wir Beispiele betrachten, beweisen wir:

Proposition 2.6 (Eigenschaften von $Z(G)$ und G')**.** *Es sei G eine Gruppe. Dann gelten:*

(a) $Z(G) \trianglelefteq G$.
(b) $G' \trianglelefteq G$.
(c) Für jede Untergruppe $H \subseteq G$ gilt die Äquivalenz:

$$H \trianglelefteq G \quad \textit{und} \quad G/H \ \textit{ist abelsch} \quad \Longleftrightarrow \quad G' \subseteq H.$$

(Verkürzt ausgedrückt: Die Kommutatorgruppe ist der kleinste Normalteiler mit abelscher Faktorgruppe.)

Beweis. (a) ergibt sich durch direktes Nachrechnen.
(b) folgt aus (c).
(c) Zunächst seien $H \trianglelefteq G$ und G/H abelsch. Dann gilt für alle $\sigma, \tau \in G$:

$$\sigma\tau\sigma^{-1}\tau^{-1}H = (\sigma H)(\tau H)(\sigma H)^{-1}(\tau H)^{-1} = \iota H = H,$$

also $[\sigma, \tau] \in H$. Es folgt $G' \subseteq H$.
Nun sei umgekehrt $G' \subseteq H$. Dann gilt für alle $\sigma \in H$ und $\rho \in G$:

$$\rho\sigma\rho^{-1} = \rho\sigma\rho^{-1}\sigma^{-1}\sigma = [\rho, \sigma] \cdot \sigma \in H,$$

also $H \trianglelefteq G$. Weiter ist für $\sigma, \tau \in G$ der Kommutator $[\sigma, \tau]$ in H enthalten, also ist der Kommutator $[\sigma H, \tau H] \in G/H$ das neutrale Element. Dies bedeutet, dass σH und τH kommutieren. Also ist G/H abelsch. □

Beispiel 2.7. (1) Für $G = S_3$ ist $Z(G) = \{\mathrm{id}\}$ und $G' = A_3$. Die Kommutatorgruppe findet man unter den „Kandidaten" $\{\mathrm{id}\}$, A_3 und S_3 (siehe Beispiel 2.2(2)) am einfachsten durch Anwendung von Proposition 2.6(c).
(2) Ist G abelsch, so folgt $Z(G) = G$ und $G' = \{\iota\}$. ◁

Das folgende Resultat gibt Aufschluss über die Untergruppen einer Faktorgruppe.

Proposition 2.8 (Untergruppen einer Faktorgruppe)**.** *Es sei $N \trianglelefteq G$ ein Normalteiler einer Gruppe. Wir betrachten die Mengen*

$$\mathcal{A} := \{H \subseteq G \mid H \text{ Untergruppe und } N \subseteq H\}$$

und

$$\mathcal{B} := \{\mathfrak{H} \subseteq G/N \mid \mathfrak{H} \text{ Untergruppe}\}.$$

Dann liefert $\Phi\colon \mathcal{A} \to \mathcal{B},\ H \mapsto H/N$ eine Bijektion. Außerdem gelten:

(a) $\forall\ H_1, H_2 \in \mathcal{A}\colon H_1 \le H_2 \iff \Phi(H_1) \le \Phi(H_2)$.
(Man sagt auch, dass Φ inklusionserhaltend *ist.)*

(b) $\forall\ H_1, H_2 \in \mathcal{A}\colon H_1 \trianglelefteq H_2 \iff \Phi(H_1) \trianglelefteq \Phi(H_2)$.

Beweis. Die Abbildung

$$\Psi\colon \mathcal{B} \to \mathcal{A},\ \mathfrak{H} \mapsto \{\sigma \in G \mid \sigma N \in \mathfrak{H}\}$$

liefert die Umkehrabbildung von Φ (also $\Phi \circ \Psi = \mathrm{id}_{\mathcal{B}}$ und $\Psi \circ \Phi = \mathrm{id}_{\mathcal{A}}$). Dies rechnet man leicht nach. Ebenso einfach ist der Nachweis von (a) und der Implikation „$\Rightarrow$" in (b). Für den Nachweis von „$\Leftarrow$" in (b) sei $\Phi(H_1) \trianglelefteq \Phi(H_2)$. Nach (a) folgt $H_1 \subseteq H_2$, und für alle $\sigma \in H_1$ und $\rho \in H_2$ gilt

$$\rho\sigma\rho^{-1}N = (\rho N)(\sigma N)(\rho N)^{-1} \in \Phi(H_1),$$

also $\rho\sigma\rho^{-1} \in \Psi(\Phi(H_1)) = H_1$. Es folgt $H_1 \trianglelefteq H_2$. □

Definition 2.9. *Es seien G und H Gruppen. Eine Abbildung $\varphi\colon G \to H$ heißt ein* **Homomorphismus** *(von Gruppen), falls für alle $\sigma, \tau \in G$ gilt:*

$$\varphi(\sigma\tau) = \varphi(\sigma)\varphi(\tau).$$

Man sieht leicht, dass hieraus automatisch $\varphi(\iota_G) = \iota_H$ (mit der offensichtlichen Bezeichnung für die neutralen Elemente der beiden Gruppen) und $\varphi(\sigma^{-1}) = \varphi(\sigma)^{-1}$ folgen.

Für einen Homomorphismus $\varphi\colon G \to H$ heißt

$$\mathrm{Kern}(\varphi) := \{\sigma \in G \mid \varphi(\sigma) = \iota_H\}$$

der **Kern** *von φ.*

Ein **Isomorphismus** *ist ein bijektiver Homomorphismus. G und H heißen* **isomorph** *(in Zeichen: $G \cong H$), falls es einen Isomorphismus $G \to H$ gibt. Einen Isomorphismus $G \to G$ bezeichnen wir auch als* **Automorphismus**. *Die Menge*

$$\mathrm{Aut}(G) := \{\varphi\colon G \to G \mid \varphi \text{ ist ein Automorphismus}\}$$

heißt die **Automorphismengruppe** *von G.* Aut(G) *wird eine Gruppe mit der Hintereinanderausführung als Produkt.*

Ein Homomorphismus ist das gruppentheoretische Analogon zu einer linearen Abbildung. Anschaulich gesprochen bedeutet die Isomorphie zweier Gruppen, dass sie gruppentheoretisch nicht unterscheidbar sind.

Beispiel 2.10. (1) Die Determinante liefert einen Homomorphismus von der $\mathrm{GL}_n(K)$ in die multiplikative Gruppe von $K \setminus \{0\}$ (K ein Körper). Der Kern ist die $\mathrm{SL}_n(K)$.
(2) Das Vorzeichen liefert einen Homomorphismus $S_n \to \{1, -1\}$, dessen Kern die alternierende Gruppe A_n ist.
(3) Es gelten $A_3 \cong Z_3$ und $S_3/A_3 \cong Z_2$.
(4) Es sei $\tau \in G$ ein Gruppenelement. Dann ist

$$\varphi_\tau \colon G \to G,\ \sigma \mapsto \tau\sigma\tau^{-1}$$

ein Automorphismus von G. ◁

Wie in der linearen Algebra lässt sich die Injektivität am Kern ablesen:

Proposition 2.11 (Kern und Injektivität)**.** *Ein Homomorphismus $\varphi\colon G \to H$ von Gruppen ist genau dann injektiv, wenn* $\mathrm{Kern}(\varphi) \subseteq \{\iota_G\}$ *(und dann gilt* $\mathrm{Kern}(\varphi) = \{\iota_G\}$*, denn ι_G liegt immer im Kern).*

Beweis. Zunächst sei φ injektiv. Dann gilt für $\sigma \in \mathrm{Kern}(\varphi)$:

$$\varphi(\sigma) = \iota_H = \varphi(\iota_G),$$

also $\sigma = \iota$.

Umgekehrt sei $\mathrm{Kern}(\varphi) \subseteq \{\iota_G\}$. Für $\sigma, \tau \in G$ mit $\varphi(\sigma) = \varphi(\tau)$ folgt dann $\varphi(\sigma\tau^{-1}) = \iota_H$, also $\sigma\tau^{-1} \in \mathrm{Kern}(\varphi) \subseteq \{\iota_G\}$ und damit $\sigma = \tau$. Demnach ist φ injektiv. □

Aus (a) und (c) des folgenden Satzes geht hervor, dass die Normalteiler genau diejenigen Teilmengen einer Gruppe sind, die als Kerne von Homomorphismen auftreten.

Satz 2.12 (Eigenschaften von Kern und Bild)**.** *(a) Es sei $\varphi\colon G \to H$ ein Homomorphismus. Dann gilt* $\mathrm{Kern}(\varphi) \trianglelefteq G$.
(b) Es sei $\varphi\colon G \to H$ ein Homomorphismus. Dann ist $\mathrm{Bild}(\varphi) \subseteq H$ *eine Untergruppe.*
(c) Es sei $N \trianglelefteq G$ ein Normalteiler. Dann liefert $\varphi\colon G \to G/N$, $\sigma \mapsto \sigma N$ einen Homomorphismus mit $\mathrm{Kern}(\varphi) = N$.

Beweis. (a) Es ist klar, dass $\mathrm{Kern}(\varphi) \subseteq G$ eine Untergruppe ist. Zum Nachweis der Normalteilereigenschaft seien $\rho \in G$ und $\sigma \in \mathrm{Kern}(\varphi)$. Dann gilt

$$\varphi(\rho\sigma\rho^{-1}) = \varphi(\rho)\varphi(\sigma)\varphi(\rho)^{-1} = \varphi(\rho)\varphi(\rho)^{-1} = \iota_H,$$

also $\rho\sigma\rho^{-1} \in \mathrm{Kern}(\varphi)$.
(b) ist klar.

(c) Dass φ ein Homomorphismus ist, folgt direkt aus der Definition von G/N. Es gilt $\operatorname{Kern}(\varphi) = \iota N = N$. □

Der folgende Satz liefert ein wichtiges Werkzeug für den Nachweis, dass zwei Gruppen isomorph sind.

Satz 2.13 (Homomorphiesatz)**.** *Es sei $\varphi\colon G \to H$ ein Homomorphismus. Dann gilt*

$$G/\operatorname{Kern}(\varphi) \cong \operatorname{Bild}(\varphi).$$

Beweis. Wir schreiben $N := \operatorname{Kern}(\varphi)$ und betrachten die Abbildung

$$\Phi\colon G/N \to \operatorname{Bild}(\varphi),\ \sigma N \mapsto \varphi(\sigma).$$

Zunächst müssen wir uns vergewissern, dass Φ wohldefiniert ist, d.h., dass das Bild von σN nicht von der Wahl des Vertreters σ abhängt. Es sei also $\sigma' \in G$ ein weiterer Vertreter, also $\sigma' N = \sigma N$. Wir haben $\sigma' = \sigma\tau$ mit $\tau \in N$, also

$$\varphi(\sigma') = \varphi(\sigma)\varphi(\tau) = \varphi(\sigma).$$

Damit ist die Wohldefiniertheit gezeigt.

Es ist klar, dass Φ surjektiv und ein Homomorphismus ist. Zum Nachweis der Injektivität nehmen wir $\sigma \in G$ mit $\Phi(\sigma N) = \iota_H$. Dann gilt $\varphi(\sigma) = \iota_H$, also $\sigma \in N$. Also folgt die Injektivität von Φ aus Proposition 2.11. □

Beispiel 2.14. Für $n \geq 2$ ist die Vorzeichen-Abbildung $\operatorname{sgn}\colon S_n \to \{1, -1\}$ surjektiv. Nach Beispiel 2.10(2) ist $\operatorname{Kern}(\operatorname{sgn}) = A_n$, also liefert Satz 2.13

$$S_n/A_n \cong \{1, -1\} (\cong Z_2).$$

Insbesondere folgt mit (2.1):

$$|A_n| = \frac{n!}{2}.$$

◁

Wir schließen den Abschnitt mit zwei Anwendungen des Homomorphiesatzes ab.

Korollar 2.15. *Es seien $M, N \trianglelefteq G$ Normalteiler mit $N \subseteq M$. Dann gilt*

$$(G/N)\Big/(M/N) \cong G/M.$$

Beweis. Die Abbildung

$$\varphi\colon G/N \to G/M,\ \sigma N \mapsto \sigma M$$

ist wegen $N \subseteq M$ wohldefiniert. Es ist klar, dass φ surjektiv und ein Homomorphismus ist. Außerdem gilt $\operatorname{Kern}(\varphi) = M/N$. Nun folgt die Behauptung aus Satz 2.13. □

Korollar 2.16. *Es seien $N \trianglelefteq G$ ein Normalteiler und $H \subseteq G$ eine Untergruppe einer Gruppe. Dann gelten:*

(a) $HN := \{\sigma\tau \mid \sigma \in H,\ \tau \in N\} \subseteq G$ ist eine Untergruppe.
(b) $H \cap N \trianglelefteq H$ und $N \trianglelefteq HN$.
(c) $H/(H \cap N) \cong (HN)/N$.

Wir stellen den Beweis als Übungsaufgabe.

3 Kompositionsreihen

Das Ziel dieses Abschnitts ist es, die endlichen einfachen Gruppen als „Atome" der endlichen Gruppen herauszustellen.

Definition 3.1. *Es sei G eine Gruppe. Eine* **Normalreihe** *(der Länge r) von G ist eine endliche Folge von ineinander enthaltenen Untergruppen*

$$\{\iota\} = N_r \subsetneqq N_{r-1} \subsetneqq \cdots \subsetneqq N_1 \subsetneqq N_0 = G,$$

so dass für $i = 1, \ldots, r$ gilt: N_i ist ein Normalteiler in N_{i-1} (aber nicht notwendig $N_i \trianglelefteq G$). Wir schreiben eine Normalreihe als

$$\{\iota\} = N_r \triangleleft N_{r-1} \triangleleft \cdots \triangleleft N_1 \triangleleft N_0 = G, \qquad (\mathcal{N})$$

Ist

$$\{\iota\} = M_s \triangleleft M_{s-1} \triangleleft \cdots \triangleleft M_1 \triangleleft M_0 = H \qquad (\mathcal{M})$$

eine weitere Normalreihe (von einer Gruppe H), so heißen $(\mathcal{N})$ und $(\mathcal{M})$ **äquivalent***, falls $r = s$ und es eine Permutation $\pi \in S_r$ gibt, so dass*

$$N_{i-1}/N_i \cong M_{\pi(i)-1}/M_{\pi(i)} \quad \text{für} \quad i = 1, \ldots, r.$$

Eine Normalreihe $(\mathcal{N})$ heißt **Kompositionsreihe***, falls alle Faktorgruppen N_{i-1}/N_i einfache Gruppen sind. Dann heißen die N_{i-1}/N_i die* **Kompositionsfaktoren***.*

Beispiel 3.2. (1) Für die S_3 finden wir die Kompositionsreihe

$$\{\mathrm{id}\} \triangleleft A_3 \triangleleft S_3.$$

Die Kompositionsfaktoren sind isomorph zu Z_2 und Z_3.

(2) Wir schreiben $Z_6 = \{\overline{0}, \overline{1}, \ldots, \overline{5}\}$ und finden zwei Kompositionsreihen:

$$\{\overline{0}\} \triangleleft \langle \overline{2} \rangle \triangleleft Z_6$$

und

$$\{\overline{0}\} \triangleleft \langle \overline{3} \rangle \triangleleft Z_6.$$

Bei beiden sind die Kompositionsfaktoren isomorph zu Z_2 und Z_3, sie sind also äquivalent.

(3) Die unendliche zyklische Gruppe Z_∞ (d.h. $\mathbb{Z}$ mit der Addition) hat *keine* Kompositionsreihe. Jede Untergruppe $\neq \{0\}$ hat nämlich die Form $m\mathbb{Z}$ mit $m \neq 0$, ist also isomorph zu Z_∞. $\triangleleft$

Das obige Beispiel hat uns gezeigt:

- Es gibt Gruppen, die mehrere verschiedene Kompositionsreihen haben (die im Beispiel allerdings äquivalent waren).
- Es gibt nicht-isomorphe Gruppen, die äquivalente Kompositionsreihen haben.
- Es gibt Gruppen, die gar keine Kompositionsreihe haben.

Satz 3.3. *Jede endliche Gruppe hat eine Kompositionsreihe.*

Beweis. Es sei G eine endliche Gruppe. Wir benutzen Induktion nach $|G|$. Im Falle $|G| = 1$ ist $\{\iota\} = N_0 = G$ eine Kompositionsreihe der Länge 0.

Falls $|G| > 1$, so gibt es einen echten Normalteiler (nämlich $\{\iota\}$). Wir können also unter allen echten Normalteilern von G einen auswählen, der maximale Ordnung hat. Wir nennen diesen Normalteiler N_1. Es liegt also kein weiterer Normalteiler zwischen N_1 und G. Nach Proposition 2.8 bedeutet dies, dass G/N_1 einfach ist. Nach Induktion hat N_1 eine Kompositionsreihe

$$\{\iota\} = N_r \triangleleft N_{r-1} \triangleleft \cdots \triangleleft N_2 \triangleleft N_1.$$

Durch Hinzufügen von $N_0 = G$ an der rechten Seite erhalten wir eine Kompositionsreihe von G. $\square$

Es folgt das wichtigste Resultat dieses Abschnitts. Es zeigt, dass unsere Beobachtung in Beispiel 3.2(2) kein Zufall war, und steht in Analogie zum Satz über die eindeutige Primzerlegung natürlicher Zahlen.

Satz 3.4 (Jordan-Hölder)**.** *Alle Kompositionsreihen einer endlichen Gruppe sind äquivalent.*

Beweis. Wir führen den Beweis durch Induktion nach $|G|$. Für $|G| = 1$ ist $\{\iota\} = N_0 = G$ die einzige Kompositionsreihe. Ab jetzt können wir also $|G| > 1$ voraussetzen, es gibt also keine Kompositionsreihe der Länge 0. Es seien

$$\{\iota\} = N_r \triangleleft N_{r-1} \triangleleft \cdots \triangleleft N_1 \triangleleft N_0 = G \qquad (\mathcal{N})$$

und

$$\{\iota\} = M_s \triangleleft M_{s-1} \triangleleft \cdots \triangleleft M_1 \triangleleft M_0 = G \qquad (\mathcal{M})$$

zwei Kompositionsreihen. Wir haben deren Äquivalenz zu zeigen. Wir betrachten zunächst den Fall $M_1 = N_1$. Dann bilden die bei N_1 bzw. M_1 abgeschnittenen Folgen ($\mathcal{N}$) und ($\mathcal{M}$) Kompositionsreihen für dieselbe Gruppe, und die Äquivalenz folgt per Induktion.

Es verbleibt der Fall $M_1 \neq N_1$. In diesem Fall ist N_1 echt in M_1N_1 enthalten. Wegen der Einfachheit von G/N_1 und wegen Proposition 2.8 ist N_1 maximal unter den echten Normalteilern von G. Wie man leicht nachrechnet, gilt $M_1N_1 \trianglelefteq G$, also folgt $M_1N_1 = G$. Mit $H := M_1 \cap N_1$ liefert Korollar 2.16:

$$M_1/H \cong G/N_1 \quad \text{und} \quad N_1/H \cong G/M_1. \tag{3.1}$$

Wir wählen nun noch eine Kompositionsreihe

$$\{\iota\} = L_t \lhd L_{t-1} \lhd \cdots \lhd L_1 \lhd L_0 = H$$

von H, deren Existenz von Satz 3.3 garantiert wird. Die Situation wird durch folgendes Diagramm veranschaulicht:

$$\begin{tikzcd}[arrows=-]
 & & G \arrow[dl] \arrow[dr] & & \\
 & M_1 \arrow[dl] \arrow[dr] & & N_1 \arrow[dl] \arrow[dr] & \\
M_2 \arrow[d] & & H \arrow[d] & & N_2 \arrow[d] \\
M_3 & & L_1 & & N_3 \\
\vdots & & \vdots & & \vdots \\
\{\iota\} & & \{\iota\} & & \{\iota\}
\end{tikzcd}$$

Aus (3.1) folgt, dass

$$\{\iota\} \lhd \cdots \lhd L_1 \lhd H \lhd M_1 \lhd G \tag{$\langle$}$$

und

$$\{\iota\} \lhd \cdots \lhd L_1 \lhd H \lhd N_1 \lhd G \tag{$\rangle$}$$

zwei äquivalente Kompositionsreihen von G sind. Ferner haben wir im obigen Diagramm zwei Kompositionsreihen von M_1, die nach Induktion äquivalent sind. Ebenso verhält es sich mit den beiden Kompositionsreihen von N_1. Also sind auch die Kompositionsreihen ($\mathcal{M}$) und ($\langle$) sowie ($\mathcal{N}$) und ($\rangle$) äquivalent. Da die Äquivalenz von Kompositionsreihen transitiv ist, folgt die behauptete Äquivalenz von ($\mathcal{M}$) und ($\mathcal{N}$). $\square$

Wir betrachten nun eine weitere Eigenschaft, die eine Gruppe haben kann, und bringen diese dann in Zusammenhang mit Kompositionsreihen.

Definition 3.5. *Es seien G eine Gruppe und G' die Kommutatorgruppe. Wir definieren $G^{(0)} := G$ und rekursiv $G^{(n+1)} := (G^{(n)})'$ für $n \in \mathbb{N}_0$. $G^{(n)}$ heißt die n-***te Kommutatorgruppe** *von G.*

G heißt **auflösbar**, *falls es ein $r \in \mathbb{N}$ gibt, so dass $G^{(r)} = \{\iota\}$.*

Beispiel 3.6. (1) Ist G abelsch, so folgt $G^{(1)} = G' = \{\iota\}$, also ist G auflösbar.

(2) Für $G = S_3$ gilt $G' = A_3$ (siehe Beispiel 2.7(1)). Da $A_3 \cong Z_3$ abelsch ist, gilt $G^{(2)} = A_3' = \{\iota\}$, also ist S_3 auflösbar.
(3) In Beispiel 3.10(1) (das auf Ergebnissen aus Abschnitt 4 aufbaut) werden wir sehen, dass die symmetrische Gruppe S_n für $n \geq 5$ nicht auflösbar ist. In Abschnitt 23 werden wir dann sehen, dass dies zur Folge hat, dass man die Nullstellen von Polynomen vom Grad ≥ 5 im Allgemeinen nicht durch verschachtelte Wurzelausdrücke darstellen kann. $\triangleleft$

Proposition 3.7 (Auflösbarkeit und Untergruppen)**.** *Es sei G eine Gruppe.*

(a) Ist G auflösbar und $H \subseteq G$ eine Untergruppe, so ist auch H auflösbar.
(b) Ist $N \trianglelefteq G$ ein Normalteiler, so gilt die Äquivalenz

$$G \text{ ist auflösbar} \iff N \text{ und } G/N \text{ sind auflösbar.}$$

Den Beweis stellen wir als Übungsaufgabe.

Wir werden jetzt die Auflösbarkeit einer endlichen Gruppe mit Hilfe der Kompositionsreihe charakterisieren. Wir benötigen zunächst ein Lemma.

Lemma 3.8 (auflösbare einfache Gruppen)**.** *Eine einfache Gruppe G ist genau dann auflösbar, wenn es eine Primzahl p gibt mit $G \cong Z_p$.*

Beweis. Als abelsche Gruppe ist Z_p auflösbar.

Es sei jetzt umgekehrt G auflösbar. Dann ist G' ein echter Normalteiler, also $G' = \{\iota\}$ wegen der Einfachheit von G. Damit ist G abelsch. Also sind $\{\iota\}$ und G die einzigen Untergruppen von G. Wir wählen ein $\sigma \in G \setminus \{\iota\}$. Es folgt $G = \langle\sigma\rangle$. Falls σ unendliche Ordnung hätte, wäre $\sigma \notin \langle\sigma^2\rangle$, also $\langle\sigma^2\rangle \neq G$, ein Widerspruch. Also $n := \operatorname{ord}(\sigma) < \infty$. Es sei p ein Primteiler von n. Dann gilt $\sigma^{n/p} \neq \iota$, also $G = \langle\sigma^{n/p}\rangle \cong Z_p$. $\square$

Satz 3.9 (Kompositionsreihen auflösbarer Gruppen)**.** *Für eine endliche Gruppe G sind äquivalent:*

(a) G ist auflösbar.
(b) Alle Kompositionsfaktoren von G sind zyklisch von Primzahlordnung.

Beweis. Wir betrachten eine Kompositionsreihe

$$\{\iota\} = N_r \triangleleft N_{r-1} \triangleleft \cdots \triangleleft N_1 \triangleleft N_0 = G. \qquad (\mathcal{N})$$

Zunächst sei G auflösbar. Alle N_i sind Untergruppen von G, also nach Proposition 3.7(a) auflösbar. Nach Proposition 3.7(b) sind auch die Faktorgruppen N_i/N_{i+1} auflösbar. Da sie einfach sind, sind sie wegen Lemma 3.8 zyklisch von Primzahlordnung.

Für die Rückrichtung benutzen wir Induktion nach $|G|$. Für $|G| = 1$ ist nichts zu zeigen. Es sei also $|G| > 1$, und alle Faktorgruppen N_i/N_{i+1} seien zyklisch von Primzahlordnung. Wenn man $(\mathcal{N})$ bei N_1 abschneidet, erhält man eine Kompositionsreihe von N_1. Per Induktion folgt, dass N_1 auflösbar ist. Außerdem ist G/N_1 zyklisch von Primzahlordnung, also wegen Lemma 3.8 auflösbar. Nun folgt mit Proposition 3.7(b) die Auflösbarkeit von G. □

Beispiel 3.10. (1) In Abschnitt 4 werden wir zeigen, dass für $n \geq 5$ die alternierende Gruppe A_n einfach ist. S_n hat also im Falle $n \geq 5$ die Kompositionsreihe

$$\{\mathrm{id}\} \lhd A_n \lhd S_n$$

mit Kompositionsfaktoren Z_2 und A_n. Insbesondere ist S_n nicht auflösbar.

(2) Hingegen ist S_n für $n \leq 4$ auflösbar. Für $n \leq 3$ wissen wir das schon (siehe Beispiel 3.6(2) für $n = 3$), und für $n = 4$ lässt sich leicht eine Kompositionsreihe mit den Faktoren vom Typ Z_p finden. ◁

4 Die symmetrische Gruppe

In diesem Abschnitt beschäftigen wir uns mit den symmetrischen und alternierenden Gruppen. Hauptziel ist es zu zeigen, dass die alternierenden Gruppen A_n für $n \geq 5$ einfach sind.

Eine Permutation $\sigma \in S_n$ schreiben wir als Produkt von elementfremden Zykeln, d.h.

$$\sigma = (a_{1,1}, a_{1,2}, \ldots, a_{1,r_1})(a_{2,1}, \ldots, a_{2,r_2}) \cdots (a_{s,1}, \ldots, a_{s,r_s}) \tag{4.1}$$

mit $a_{i,j} \in \{1, \ldots, n\}$, wobei $(a_{i,1}, a_{i,2}, \ldots, a_{i,r_i})$ für die Permutation steht, die $a_{i,j}$ auf $a_{i,j+1}$ abbildet ($1 \leq j < r_i$), a_{i,r_i} auf $a_{i,1}$ abbildet und alle $x \in \{1, \ldots, n\}$, die nicht unter den $a_{i,1}, \ldots, a_{i,r_i}$ vorkommen, festlässt. „Elementfremd“ bedeutet, dass die $a_{i,j}$ paarweise verschieden sind, so dass die Reihenfolge der Zykel in (4.1) keine Rolle spielt. Wir können sie so anordnen, dass $r_1 \leq r_2 \leq \cdots \leq r_s$ gilt. Dann heißt $(r_1, \ldots, r_s)$ der **Permutationstyp** (auch: Zykeltyp) von σ.

Beispiel 4.1. Wir schreiben die Permutation $\sigma \in S_5$ mit $\sigma(1) = 3$, $\sigma(2) = 5$, $\sigma(3) = 4$, $\sigma(4) = 1$ und $\sigma(5) = 2$ als Produkt von elementfremden Zykeln:

$$\sigma = (1, 3, 4)(2, 5).$$

Der Permutationstyp ist $(2, 3)$. ◁

Wir untersuchen jetzt, wie die Konjugation in der S_n wirkt.

Lemma 4.2 (Konjugation in S_n)**.** *Es seien $\sigma = (a_1, \ldots, a_r) \in S_n$ ein Zykel und $\rho \in S_n$. Dann gilt*

$$\rho\sigma\rho^{-1} = (\rho(a_1), \rho(a_2), \ldots, \rho(a_r))\,.$$

Beweis. Die Permutation $\rho\sigma\rho^{-1}$ bildet $\rho(a_i)$ auf $\rho(a_{i+1})$ ab $(1 \le i < r)$ und $\rho(a_r)$ auf $\rho(a_1)$. Da alle anderen Elemente von $\{1, \dots, n\}$ festbleiben, ergibt sich die Behauptung. □

Aus dem Lemma folgt, dass zwei Elemente der S_n genau dann konjugiert sind, wenn sie den gleichen Permutationstyp haben. Es folgt auch, dass $\sigma = (a_1, \dots, a_r)$ zu $(1, 2, \dots, r)$ konjugiert ist. Durch Zählen der Fehlstellen der letzteren Permutation ergibt sich $\mathrm{sgn}(\sigma) = (-1)^{r-1}$. Wegen der Mutiplikativität des Vorzeichens sehen wir auch, dass das Vorzeichen eines $\sigma \in S_n$ vom Permutationstyp $(r_1, \dots, r_s)$ sich zu

$$\mathrm{sgn}(\sigma) = \prod_{i=1}^{s} (-1)^{r_i - 1}$$

ergibt.

Wir erinnern uns, dass eine **Transposition** eine Permutation der Form (i, j) ist, also vom Permutationstyp (2).

Proposition 4.3. *Die Gruppe S_n wird von Transpositionen erzeugt.*

Beweis. Wir benutzen Induktion nach n. Für $n \le 1$ ist $|S_n| = 1$, also erzeugt durch die leere Menge. Wir setzen ab jetzt $n \ge 2$ voraus und betrachten zunächst den Fall $\sigma(n) = n$. Dann liefert die Einschränkung von σ auf $\{1, \dots, n-1\}$ ein Element von S_{n-1}, welches nach Induktion ein Produkt von Transpositionen ist. Also ist auch σ ein Produkt von Transpositionen.

Schließlich betrachten wir den Fall $\sigma(n) \ne n$. Wir setzen $k := \sigma(n)$ und bilden

$$\tau := (k, n) \circ \sigma.$$

Es folgt $\tau(n) = n$, also ist τ nach dem obigen Fall ein Produkt von Transpositionen, und $\sigma = (k, n) \circ \tau$ auch. □

Nun wenden wir uns der alternierenden Gruppe A_n zu.

Lemma 4.4. *Die alternierende Gruppe A_n wird von Dreierzykeln (d.h. von Elementen der Form (i, j, k) mit $i, j, k \in \{1, \dots, n\}$ paarweise verschieden) erzeugt.*

Beweis. Da die Transpositionen das Vorzeichen -1 haben, ergibt sich aus Proposition 4.3, dass A_n erzeugt wird von allen Elementen der Form $(i, j) \circ (k, l)$ mit $i, j, k, l \in \{1, \dots, n\}$, $i \ne j$ und $k \ne l$. Wir behaupten, dass jedes solche Element in der durch die Dreierzykeln erzeugten Untergruppe liegt.

1. Fall: i, j, k, l sind paarweise verschieden. Dann gilt

$$(i, j) \circ (k, l) = (k, i, l) \circ (i, j, k),$$

wie man leicht nachrechnet.

2. Fall: i, j, k, l sind nicht paarweise verschieden. Wir können $(i, j) \neq (k, l)$ voraussetzen, da bei Gleichheit das Produkt ohnehin in der durch die Dreierzykeln erzeugten Untergruppe liegt. Da wir außerdem i, j und k, l vertauschen können, dürfen wir $l = j$ aber $i \neq k$ annehmen. Es folgt

$$(i, j) \circ (k, l) = (i, j) \circ (k, j) = (i, j, k).$$

Damit ist alles gezeigt. □

Lemma 4.5. *Es sei $N \trianglelefteq A_n$ ein Normalteiler, der einen Dreierzykel enthält. Dann gilt $N = A_n$.*

Beweis. Wir haben $(i, j, k) \in N$. Wegen Lemma 4.4 genügt es zu zeigen, dass jeder Dreierzykel $(a, b, c) \in S_n$ in N liegt. Wir wählen zunächst $\rho \in S_n$ mit

$$\rho(i) = a, \quad \rho(j) = b \quad \text{und} \quad \rho(k) = c.$$

Falls $\operatorname{sgn}(\rho) = -1$, so ersetzen wir ρ durch $(a, c) \circ \rho$, so dass in jedem Fall $\rho \in A_n$ gilt. Aus Lemma 4.2 folgt

$$\rho \circ (i, j, k) \circ \rho^{-1} = (a, b, c) \quad \text{oder} \quad = (c, b, a).$$

Nach Voraussetzung liegt also (a, b, c) oder dessen Inverses (c, b, a) in N, also auch (a, b, c) selbst. □

Satz 4.6. *Für $n \geq 5$ ist die alternierende Gruppe A_n einfach.*

Beweis. Wir nehmen an, dass es einen Normalteiler $N \trianglelefteq A_n$ mit $\{\mathrm{id}\} \neq N \neq A_n$ gibt. Unter allen Elementen aus $N \setminus \{\mathrm{id}\}$ wählen wir ein σ, das eine maximale Anzahl von Elementen aus $\{1, \ldots, n\}$ fixiert. Wir unterscheiden drei Fälle. Dabei sind im Folgenden die a_i stets als paarweise verschiedene Elemente aus $\{1, \ldots, n\}$ zu verstehen.

1. Fall: Im Permutationstyp von σ kommt eine 3 vor. Dann gilt

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

so dass a_1, a_2, a_3 von $\sigma' \in S_n$ fixiert werden. Wegen Lemma 4.5 kann σ kein Dreierzykel sein, also gibt es a_4 und a_5 mit $\sigma(a_4) \neq a_4$ und $\sigma(a_5) \neq a_5$.

2. Fall: Im Permutationstyp von σ kommt keine 3, aber ein $r \geq 4$ vor. Dann gilt

$$\sigma = (a_1, a_2, \ldots, a_r) \circ \sigma',$$

so dass $a_1, \ldots, a_r$ von $\sigma' \in S_n$ fixiert werden. Im Fall $r = 4$ ist $\sigma = (a_1, a_2, a_3, a_4)$ unmöglich (da dieser Zykel das Vorzeichen -1 hat), also gibt es a_5 mit $\sigma(a_5) \neq a_5$.

3. Fall: Der Permutationstyp von σ ist $(2, 2, \ldots, 2)$. Wegen $\sigma \in A_n$ gilt dann

$$\sigma = (a_1, a_2)(a_3, a_4) \circ \sigma',$$

so dass $a_1, \dots, a_4$ von $\sigma' \in S_n$ fixiert werden. In diesem Fall können wir wegen $n \geq 5$ (was an dieser Stelle zum einzigen Mal verwendet wird) eine von $a_1, \dots, a_4$ verschiedene Zahl a_5 wählen.

In allen drei Fällen setzen wir

$$\rho := (a_3, a_4, a_5) \in A_n \quad \text{und} \quad \tau := \sigma^{-1}\rho^{-1}\sigma\rho \in N.$$

Wir werden nun zeigen, dass $\tau \neq \mathrm{id}$ und dass τ mehr Elemente fixiert als σ, was einen Widerspruch zur Annahme $\{\mathrm{id}\} \neq N \neq A_n$ liefert. Wir stellen fest:

$$\begin{array}{llll} \text{Fall 1, 2:} & \tau(a_1) = a_1, & \tau(a_2) = \sigma^{-1}(a_5) \neq a_2, & \\ \text{Fall 3:} & \tau(a_1) = a_1, & \tau(a_2) = a_2, & \tau(a_3) = \sigma^{-1}(a_5) \neq a_3. \end{array}$$

Zunächst folgt $\tau \neq \mathrm{id}$. Es sei nun $i \in \{1, \dots, n\}$ mit $\sigma(i) = i$. In den Fällen 1 und 2 folgt $i \notin \{a_1, a_2, a_3, a_4, a_5\}$, also auch $\tau(i) = i$. In diesen Fällen fixiert τ also jedes Element, das von σ fixiert wird, und zusätzlich a_1. Im Fall 3 folgt $i \notin \{a_1, a_2, a_3, a_4\}$. Bis auf die mögliche Ausnahme a_5 fixiert τ also jedes Element, das von σ fixiert wird, und zusätzlich a_1 und a_2. In jedem Fall fixiert τ also mehr Elemente als σ, was zu zeigen war. □

Beispiel 4.7. (1) Auch die A_3 ist einfach, denn $A_3 \cong Z_3$, was nach Beispiel 2.2(5) einfach ist.

(2) Die A_4 ist nicht einfach. Die Stelle im obigen Beweis, wo $n \geq 5$ verwendet wird, liefert eine Idee, wie ein nicht-trivialer Normalteiler zu finden sein könnte. In der Tat ist

$$N = \{\mathrm{id}, (1,2)(3,4), (1,3)(2,4), (1,4)(2,3)\} \trianglelefteq A_4$$

ein solcher. N ist isomorph zur Kleinschen Vierergruppe. ◁

Korollar 4.8. *Für $n \geq 5$ ist die symmetrische Gruppe S_n nicht auflösbar.*

5 Operationen von Gruppen

Definition 5.1. *Es seien G eine Gruppe und M eine Menge. Eine* **Operation** *von G auf M ist eine Abbildung $G \times M \to M$, $(\sigma, x) \mapsto \sigma(x)$, so dass folgende Bedingungen erfüllt sind:*

(a) Für alle $\sigma, \tau \in G$ und alle $x \in M$ gilt

$$(\sigma\tau)(x) = \sigma\left(\tau(x)\right).$$

(b) Für alle $x \in M$ gilt
$$\iota(x) = x.$$

Wir sagen, dass G auf M **operiert***, falls eine Operation von G auf M gegeben ist. Ab jetzt sei dies der Fall. Für $x \in M$ heißt*

$$G_x := \{\sigma \in G \mid \sigma(x) = x\} \subseteq G$$

die **Fixgruppe** *von x und*

$$G(x) := \{\sigma(x) \mid \sigma \in G\} \subseteq M$$

die **Bahn** *von x.*

Die Operation heißt **treu***, falls ι das einzige Gruppenelement ist, das alle $x \in M$ fixiert (anders ausgedrückt, falls $\bigcap_{x \in M} G_x = \{\iota\}$). Die Operation heißt* **transitiv***, falls es ein $x \in M$ gibt mit $G(x) = M$.*

Wir definieren noch die **symmetrische Gruppe** *auf M als*

$$S_M := \{\varphi\colon M \to M \mid \varphi \text{ ist bijektiv}\}.$$

Bevor wir Beispiele anschauen, beweisen wir ein erstes Resultat.

Proposition 5.2 (Operationen und Homomorphismen)**.** *Es seien G eine Gruppe und M eine Menge.*

(a) Zu einer Operation von G auf M gibt es einen Homomorphismus $\pi\colon G \to S_M$, $\sigma \mapsto \varphi_\sigma$, wobei φ_σ gegeben ist durch

$$\varphi_\sigma(x) = \sigma(x) \quad \text{für } \sigma \in G \text{ und } x \in M.$$

(b) Umgekehrt gibt es zu einem Homomorphismus $\pi\colon G \to S_M$ eine Operation von G auf M, gegeben durch

$$\sigma(x) = (\pi(\sigma))(x) \quad \text{für } \sigma \in G \text{ und } x \in M.$$

(c) Eine Operation von G auf M ist genau dann treu, wenn der zugehörige Homomorphismus $\pi\colon G \to S_M$ injektiv ist.

Beweis. (a) Die Abbildung $\varphi_\sigma\colon M \to M$ ist bijektiv, denn

$$\varphi_\sigma \circ \varphi_{\sigma^{-1}} = \varphi_{\sigma^{-1}} \circ \varphi_\sigma = \mathrm{id}_M.$$

Weiter ist π ein Homomorphismus, denn für $\sigma, \tau \in G$ und $x \in M$ gilt

$$\varphi_{\sigma\tau}(x) = (\sigma\tau)(x) = \sigma(\tau(x)) = (\varphi_\sigma \circ \varphi_\tau)(x).$$

Die Behauptungen (b) und (c) ergeben sich direkt aus den Definitionen. □

Beispiel 5.3. (1) Die orthogonale Gruppe $\mathrm{O}_2(\mathbb{R})$ operiert „in natürlicher Weise“ auf $\mathbb{R}^2$, d.h. durch $A(v) = A \cdot v$ für $A \in \mathrm{O}_2(\mathbb{R})$ und $v \in \mathbb{R}^2$. Die Operation ist treu. Die Bahnen sind die Kreise um den Nullpunkt. Für einen

Punkt $\neq 0$ besteht die Fixgruppe aus der Identität und der Spiegelung, die diesen Punkt fixiert.

(2) Es sei $G \subseteq \mathrm{SO}_3(\mathbb{R})$ die Gruppe derjenigen räumlichen Drehungen, die ein vorgegebenes Tetraeder (mit Schwerpunkt im Koordinatenursprung) in sich selbst überführen. (Man nennt G auch die *Symmetriegruppe* des Tetraeders.) G operiert in natürlicher Weise auf $\mathbb{R}^3$. Es gibt aber auch eine Operation auf der Menge der Eckpunkte des Tetraeders. Es ist klar, dass (auch) diese Operation treu ist. (Wir dürfen hier zum Zweck des Beispiels unsere geometrische Intuition einsetzen.) Nach Proposition 5.2 erhalten wir einen injektiven Homomorphismus $\pi\colon G \to S_4$. G enthält alle Drehungen um 120°, die einen Eckpunkt fixieren. Diese wirken als Dreierzykel auf den Eckpunkten. Wegen Lemma 4.4 folgt $A_4 \subseteq \pi(G)$, also $\pi(G) \in \{A_4, S_4\}$. Da es keine Drehung gibt, die zwei Ecken vertauscht und die beiden anderen fixiert (wieder dürfen wir unsere Intuition bemühen), gibt es in $\pi(G)$ keine Transposition, also $\pi(G) = A_4$. Wir erhalten $G \cong A_4$. ◁

Anmerkung. Einen Homomorphismus $G \to S_n$ von einer Gruppe G in eine symmetrische Gruppe nennt man auch eine *Permutationsdarstellung* von G. ◁

Gibt es zu jeder Gruppe G eine Menge M, auf der sie treu operiert? Die Antwort ist ja: Wir können $M = G$ nehmen mit der Operation gegeben durch $\sigma(\tau) = \sigma\tau$. Mit Proposition 5.2 erhalten wir folgendes Ergebnis, das die Bedeutung der symmetrischen Gruppen unterstreicht.

Satz 5.4. *Jede endliche Gruppe ist isomorph zu einer Untergruppe einer symmetrischen Gruppe S_n.*

Wir entwickeln nun die allgemeine Theorie der Gruppenoperationen weiter.

Satz 5.5. *Eine Gruppe G operiere auf einer Menge M. Für $x, y \in M$ schreiben wir $x \sim y$, falls es ein $\sigma \in G$ gibt mit $\sigma(x) = y$.*

(a) Durch „$\sim$“ wird eine Äquivalenzrelation auf M definiert.
(b) Die Äquivalenzklassen sind die Bahnen.
(c) Für $x \in M$ gilt:

$$|G(x)| = (G : G_x).$$

(In Worten: Die Bahnlänge ist der Index der Fixgruppe.)

Beweis. (a) Wir weisen die definierenden Eigenschaften einer Äquivalenzrelation nach. Wegen $\iota(x) = x$ gilt $x \sim x$ für alle $x \in M$. Gilt $x \sim y$ für $x, y \in M$, d.h. $\sigma(x) = y$ mit $\sigma \in G$, so folgt $\sigma^{-1}(y) = x$, also $y \sim x$. Gilt weiter $x \sim y$ und $y \sim z$ für $x, y, z \in M$, d.h. $\sigma(x) = y$ und $\tau(y) = z$ mit $\sigma, \tau \in G$, so folgt $(\tau\sigma)(x) = \tau(\sigma(x)) = z$, also $x \sim z$.

(b) ist klar.

(c) Wir betrachten die Menge $S := \{\sigma G_x \mid \sigma \in G\}$ der Linksnebenklassen. Die Abbildung

$$\Phi\colon S \to G(x),\ \sigma G_x \mapsto \sigma(x)$$

ist offenbar wohldefiniert (d.h. $\sigma(x)$ ist unabhängig von der Wahl des Vertreters σ) und surjektiv. Außerdem ist sie injektiv, denn aus $\sigma(x) = \tau(x)$ mit $\sigma, \tau \in G$ folgt $\tau^{-1}\sigma \in G_x$, also $\sigma G_x = \tau G_x$. Also ist Φ bijektiv, und es folgt $|G(x)| = |S| = (G : G_x)$. □

Aus Satz 5.5 ergibt sich direkt:

Korollar 5.6 (Bahnbilanzgleichung). *Eine Gruppe G operiere auf einer endlichen Menge M. Weiter seien $x_1, \ldots, x_r \in M$ Vertreter der Bahnen, d.h. M ist die disjunkte Vereinigung der Bahnen $G(x_i)$. Dann gilt*

$$|M| = \sum_{i=1}^{r} (G : G_{x_i}).$$

Das folgende Beispiel ist wichtig, und der Teil (1) wird für den Beweis der Sätze 5.9 und 6.2 benutzt.

Beispiel 5.7. Es sei G eine Gruppe.

(1) G operiert auf sich selbst (also $M = G$) durch Konjugation, d.h. $\sigma(\tau) = \sigma\tau\sigma^{-1}$ $(\sigma, \tau \in G)$. Für $\tau \in G$ ist $G(\tau) = [\tau]$ die Konjugiertenklasse von τ, und die Fixgruppe ist

$$G_\tau = \{\sigma \in G \mid \sigma\tau = \tau\sigma\} =: \mathcal{C}_G(\tau).$$

Die Gruppe $\mathcal{C}_G(\tau)$ heißt der **Zentralisator** von τ. Es gilt $\tau \in Z\left(\mathcal{C}_G(\tau)\right)$. Falls G endlich ist, können wir Vertreter $\tau_1, \ldots, \tau_n$ der Konjugiertenklassen wählen. Die Bahnbilanzgleichung sagt dann

$$|G| = \sum_{i=1}^{n} \left(G : \mathcal{C}_G(\tau_i)\right).$$

Wir können die τ_i so anordnen, dass $\tau_1, \ldots, \tau_r$ *nicht* im Zentrum $Z(G)$ liegen (hierbei ist $r = 0$ möglich) und $\tau_{r+1}, \ldots, \tau_n \in Z(G)$. Für jedes $\tau \in Z(G)$ gilt $[\tau] = \{\tau\}$, also ist τ selbst der einzige Vertreter der Konjugiertenklasse, und $(G : \mathcal{C}_G(\tau)) = 1$. Die obige Gleichung erhält nun die Gestalt

$$|G| = |Z(G)| + \sum_{i=1}^{r} \left(G : \mathcal{C}_G(\tau_i)\right), \tag{5.1}$$

wobei die Summanden in der rechten Summe alle > 1 sind.

(2) G operiert auch auf der Menge $M := \{H \subseteq G \mid H \text{ Untergruppe}\}$ aller Untergruppen durch Konjugation, d.h. $\sigma(H) = \sigma H \sigma^{-1}$ für $\sigma \in G$, $H \in M$. Für $H \in M$ ergibt sich die Fixgruppe

$$G_H = \left\{\sigma \in G \mid \sigma H \sigma^{-1} = H\right\} =: \mathcal{N}_G(H).$$

Die Gruppe $\mathcal{N}_G(H)$ heißt der **Normalisator** von H. Sie ist die größte Untergruppe von G, in der H ein Normalteiler ist. ◁

Wir können (5.1) benutzen, um eine interessante Eigenschaft sogenannter p-Gruppen zu beweisen. Diese definieren wir jetzt.

Definition 5.8. *Es sei p eine Primzahl. Eine Gruppe G heißt **p-Gruppe**, falls $|G| = p^k$ mit $k \in \mathbb{N}_0$.*

Der folgende Satz erscheint zunächst etwas unscheinbar, hat aber das wichtige Korollar 5.10 als Konsequenz.

Satz 5.9. *Es sei $G \neq \{\iota\}$ eine p-Gruppe. Dann gilt*

$$Z(G) \neq \{\iota\}.$$

Beweis. Dies folgt direkt aus (5.1), da $|G|$ und alle $(G : \mathcal{C}_G(\tau_i))$ durch p teilbar sind. □

Korollar 5.10. *Jede p-Gruppe ist auflösbar.*

Beweis. Es sei G eine p-Gruppe. Wir verwenden Induktion nach $|G|$. Für $|G| = 1$ ist nichts zu zeigen. Im Fall $|G| > 1$ liefert Satz 5.9, dass $|G/Z(G)| < |G|$. Also ist $G/Z(G)$ nach Induktion auflösbar. Außerdem ist $Z(G)$ als abelsche Gruppe ohnehin auflösbar. Also ergibt sich die Behauptung nach Proposition 3.7(b). □

Korollar 5.11. *Es seien p eine Primzahl und G eine Gruppe der Ordnung p^2. Dann ist G abelsch.*

Beweis. Wir nehmen an, dass G nicht abelsch ist. Dann hat $Z(G)$ die Ordnung p, also $|G/Z(G)| = p$. Wegen Korollar 1.14 ist $G/Z(G)$ also zyklisch. Wir stellen es als Übungsaufgabe nachzuweisen, dass jede Gruppe, deren Faktorgruppe nach dem Zentrum zyklisch ist, abelsch ist. Die Annahme ist also falsch. □

In Abschnitt 7 werden wir sehen, dass es genau zwei Isomorphietypen von abelschen Gruppen der Ordnung p^2 gibt (siehe Beispiel 7.6(2)).

6 Die Sylow-Sätze

Wir wissen, dass als Ordnungen von Untergruppen einer endlichen Gruppe nur Teiler der Gruppenordnung auftreten können (Satz 1.12). Es treten aber im Allgemeinen nicht alle Teiler der Gruppenordnung auf, beispielsweise hat die A_4 keine Untergruppe der Ordnung 6. Der folgende Satz besagt, dass

Primzahlpotenzen immer als Ordnungen von Untergruppen auftreten, wenn sie Teiler der Gruppenordnung sind. Wir beweisen zunächst ein Lemma.

Lemma 6.1. *G sei eine endliche, abelsche Gruppe, und p sei ein Primteiler der Ordnung $|G|$. Dann enthält G ein Element der Ordnung p.*

Beweis. Wir benutzen Induktion nach $|G|$. Ist G einfach, so folgt mit Lemma 3.8, dass $G \cong Z_p$, und es ist nichts mehr zu zeigen. Andernfalls gibt es einen Normalteiler $N \trianglelefteq G$ mit $\{\iota\} \neq N \neq G$. Falls p ein Teiler von $|N|$ ist, so liefert die Induktionsannahme ein Element der Ordnung p in N und damit in G. Andernfalls ist $|G/N|$ durch p teilbar, also liefert die Induktionsannahme ein Element $\sigma N \in G/N$ der Ordnung p. Setzen wir $k := \operatorname{ord}(\sigma)$, so folgt $(\sigma N)^k = \iota_{G/N}$, also $p \mid k$ wegen Proposition 1.9. Nun folgt $\operatorname{ord}\big(\sigma^{k/p}\big) = p$. □

Anmerkung. Aus dem folgenden Satz und Korollar 1.14 gehen hervor, dass in Lemma 6.1 die Voraussetzung, dass G abelsch ist, unnötig ist. (Dass das Lemma trotzdem im Beweis von Satz 6.2 benutzt wird, ist interessant.) Die Voraussetzung, dass p eine Primzahl ist, kann jedoch nicht weggelassen werden. Beispielsweise hat die Kleinsche Vierergruppe kein Element der Ordnung 4. ◁

Satz 6.2 (Untergruppen von Primpotenzordnung)**.** *Es seien G eine endliche Gruppe, p eine Primzahl und $k \in \mathbb{N}_0$, so dass p^k ein Teiler von $|G|$ ist. Dann gibt es eine Untergruppe $H \subseteq G$ mit $|H| = p^k$.*

Beweis. Wir benutzen Induktion nach $|G|$. Für $k = 0$ wird der Satz durch $H = \{\iota\}$ erfüllt, wir können also $k \geq 1$ annehmen. Nach (5.1) gilt

$$|G| = |Z(G)| + \sum_{i=1}^{r} \left(G : \mathcal{C}_G(\tau_i)\right), \tag{6.1}$$

wobei $r \geq 0$ und $\tau_i \in G \setminus Z(G)$. Wir unterscheiden zwei Fälle.

1. Fall: $|Z(G)|$ ist nicht durch p teilbar. Wegen (6.1) und $p \mid |G|$ muss es dann ein $i \in \{1, \ldots, r\}$ geben, so dass auch $\left(G : \mathcal{C}_G(\tau_i)\right)$ nicht durch p teilbar ist. Also ist $|\mathcal{C}_G(\tau_i)|$ durch p^k teilbar. Wegen $\tau_i \notin Z(G)$ ist $\mathcal{C}_G(\tau_i)$ eine echte Untergruppe von G, nach der Induktionsannahme hat $\mathcal{C}_G(\tau_i)$ also eine Untergruppe der Ordnung p^k.
2. Fall: $|Z(G)|$ ist durch p teilbar. Wegen Lemma 6.1 enthält $Z(G)$ dann ein Element σ der Ordnung p. Wegen $\sigma \in Z(G)$ ist $N := \langle\sigma\rangle \trianglelefteq G$ ein Normalteiler, und G/N hat die Ordnung $|G|/p$. Nach der Induktionsannahme hat G/N also eine Untergruppe $\mathfrak{H}$ der Ordnung p^{k-1}. Nach Proposition 2.8 existiert eine Untergruppe $H \subseteq G$ mit $\mathfrak{H} = H/N$. Also $|H| = |N| \cdot |\mathfrak{H}| = p^k$. □

Definition 6.3. *Es seien G eine endliche Gruppe und p eine Primzahl. Wir schreiben $|G| = p^k \cdot m$ mit $k, m \in \mathbb{N}_0$ und $p \nmid m$. Eine Untergruppe $P \subseteq G$ mit $|P| = p^k$ heißt eine* p**-Sylow-Gruppe** *von G.*

Es folgen nun die sogenannten Sylow-Sätze, die diesem Abschnitt seinen Namen geben, und die die Teile (a)–(c) des folgenden Satzes bilden.

Satz 6.4 (Sylow-Sätze)**.** *Es seien G eine endliche Gruppe und p eine Primzahl. Wir schreiben $|G| = p^k \cdot m$ mit $k, m \in \mathbb{N}_0$ und $p \nmid m$.*

(a) Es sei H eine p-Gruppe, die als Untergruppe in G enthalten ist. Dann gibt es eine p-Sylowgruppe $P \subseteq G$ mit $H \subseteq P$.
(b) Alle p-Sylow-Gruppen von G sind konjugiert, d.h. zu zwei p-Sylow-Gruppen $P, P' \subseteq G$ gibt es $\rho \in G$ mit $P' = \rho P \rho^{-1}$.
(c) Für die Anzahl n_p der p-Sylow-Gruppen gelten:

$$n_p \equiv 1 \mod p \quad \textit{(d.h. } p \textit{ teilt die Differenz } n_p - 1\textit{)} \quad \textit{und} \quad n_p \mid m.$$

Beweis. Aus Satz 6.2 folgt, dass es eine p-Sylow-Gruppe P gibt. Wir betrachten die Menge

$$M := \{\rho P \rho^{-1} \mid \rho \in G\}$$

der zu P konjugierten Untergruppen. G operiert transitiv auf M durch Konjugation, und die Fixgruppe von P ist $G_P = \mathcal{N}_G(P)$. Aus Korollar 5.6 folgt $|M| = (G : \mathcal{N}_G(P))$. Wegen $P \subseteq \mathcal{N}_G(P)$ ist p^k ein Teiler von $|\mathcal{N}_G(P)|$, also ist der Index $(G : \mathcal{N}_G(P))$ ein Teiler von m. Wir erhalten:

$$|M| \text{ teilt } m. \tag{6.2}$$

Nun sei H eine p-Gruppe, die als Untergruppe in G enthalten ist. Auch H operiert durch Konjugation auf M. Sind $Q_1, \ldots, Q_r \in M$ Vertreter der Bahnen dieser Operation, so liefert Korollar 5.6:

$$|M| = \sum_{i=1}^{r} (H : H_{Q_i})\,. \tag{6.3}$$

Da es sich bei allen $(H : H_{Q_i})$ um p-Potenzen handelt, muss es wegen (6.2) ein i geben mit $(H : H_{Q_i}) = 1$. Wir behaupten, dass hieraus $H \subseteq Q_i$ folgt. Wir haben $H_{Q_i} = H$. Das bedeutet, dass für alle $\rho \in H$ gilt: $\rho Q_i \rho^{-1} = Q_i$. Also gilt $H \subseteq \mathcal{N}_G(Q_i)$. Wir können nun Korollar 2.16 anwenden (wobei $\mathcal{N}_G(Q_i)$ die Rolle des dortigen G und Q_i die Rolle des dortigen N übernimmt) und erhalten

$$H/(H \cap Q_i) \cong (HQ_i)/Q_i.$$

Wegen $Q_i \in M$ ist Q_i zu P konjugiert, also $|Q_i| = |P| = p^k$, und damit ist der Index $(HQ_i : Q_i)$ nicht durch p teilbar. Aber $H/(H \cap Q_i)$ eine p-Gruppe. Aus dem obigen Isomorphismus folgt daher folgt $|H/(H \cap Q_i)| = 1$, also $H \cap Q_i = H$. Damit ist $H \subseteq Q_i$ bewiesen. Insbesondere folgt die Behauptung (a).

Ab jetzt betrachten wir den Spezialfall, dass H eine p-Sylow-Gruppe ist. Dann folgt aus $H \subseteq Q_i$ die Gleichheit, denn beide Gruppen haben dieselbe Elementanzahl. Nach der Definition von M ist H also konjugiert zu P, und es folgt (b).

Nachdem wir (b) bewiesen haben, folgt $|M| = n_p$. Die zweite Behauptung von (c) ergibt sich also aus (6.2).

Wir haben gesehen, dass aus $(H : H_{Q_i}) = 1$ für ein i die Gleichheit $H = Q_i$ ergibt. Dies kann also nur für ein i auftreten. Da alle $(H : H_{Q_i})$ Potenzen von p sind, folgt die erste Behauptung von (6.2) aus (6.3). □

Den Rest des Abschnitts widmen wir zwei Anwendungen der Sylow-Sätze. Zunächst bestimmen wir alle Gruppen, deren Ordnung das Produkt zweier verschiedener Primzahlen ist.

Es sei also G eine Gruppe mit $|G| = pq$, wobei p und q Primzahlen mit $p > q$ seien. Für die Anzahl n_p der p-Sylow-Gruppen liefert Satz 6.4(c) die Einschränkungen $n_p \equiv 1 \mod p$ und $n_p \mid q$. Es folgt $n_p = 1$, also gibt es genau eine Untergruppe $P \subseteq G$ mit $|P| = p$, die demnach Normalteiler ist. Wegen Korollar 1.14 folgt

$$P = \langle \sigma \rangle \cong Z_p.$$

Wir unterscheiden zwei Fälle.

1. Fall: G enthält ein Element der Ordnung pq. Dann ist G zyklisch, also

$$G \cong Z_{pq}.$$

2. Fall: G enthält kein Element der Ordnung pq. Es sei Q eine q-Sylow-Gruppe, also $Q = \langle \tau \rangle \cong Z_q$. Wir nehmen an, dass auch $n_q = 1$ gilt. Dann folgt $Q \trianglelefteq G$ und

$$\sigma\tau\sigma^{-1}\tau^{-1} \in P \cap Q = \{\iota\},$$

also $\sigma\tau = \tau\sigma$. Für $i \in \mathbb{Z}$ gilt also $(\sigma\tau)^i = \sigma^i\tau^i$, woraus $\operatorname{ord}(\sigma\tau) = pq$ folgt, im Widerspruch zum angenommenen Fall. Aus Satz 6.4(c) folgt nun $n_q = p$, also

$$p \equiv 1 \mod q.$$

Ist diese Bedingung verletzt, so kann der 2. Fall nicht auftreten. Wir behaupten

$$G = \left\{ \tau^i\sigma^j \mid i \in \{0, \dots, q-1\},\ j \in \{0, \dots, p-1\} \right\}.$$

Für den Nachweis genügt es zu zeigen, dass die $\tau^i\sigma^j$ in der obigen Menge paarweise verschieden sind. Es sei also $\tau^i\sigma^j = \tau^{i'}\sigma^{j'}$ mit $i, i' \in \{0, \dots, q-1\}$ und $j, j' \in \{0, \dots, p-1\}$. Es folgt

$$\tau^{i-i'} = \sigma^{j'-j} \in Q \cap P = \{\iota\},$$

also $i = i'$ und $j = j'$. Damit ist der Nachweis erbracht. Wir müssen noch wissen, wie das Produkt auf G funktioniert. Für $i_1, i_2, j_1, j_2 \in \mathbb{N}_0$ gilt

$$\tau^{i_1}\sigma^{j_1}\tau^{i_2}\sigma^{j_2} = \tau^{i_1+i_2}\tau^{-i_2}\sigma^{j_1}\tau^{i_2}\sigma^{j_2} = \tau^{i_1+i_2}\left(\tau^{-i_2}\sigma\tau^{i_2}\right)^{j_1}\sigma^{j_2}.$$

Hierbei ergibt sich $\tau^{-i_2}\sigma\tau^{i_2}$, indem man σ genau i_2 mal mit τ^{-1} konjugiert. Das Produkt ist also bekannt, wenn die Konjugation $\tau^{-1}\sigma\tau$ bekannt ist. Wegen $P \trianglelefteq G$ gibt es ein $k \in \{0, \dots, p-1\}$ mit

$$\tau^{-1}\sigma\tau = \sigma^k.$$

Für $i \in \mathbb{Z}$ folgt dann

$$\tau^{-i}\sigma\tau^i = \sigma^{k^i}.$$

Für $i = q$ ergibt dies wegen $\tau^q = \iota$, dass

$$k^q \equiv 1 \mod p \tag{6.4}$$

gelten muss. Hierbei ist $k = 1$ unmöglich, sonst hätte das Produkt $\tau\sigma$ die Ordnung pq. Wegen $\mathrm{ord}(\sigma) = p$ ist auch klar, dass es nur auf die Restklasse $k+p\mathbb{Z} \in \mathbb{Z}/(p) = \mathbb{F}_p$ von k modulo p ankommt. In Abschnitt 11 werden wir sehen, dass diejenigen Restklassen modulo p, die (6.4) erfüllen, eine (multiplikative) zyklische Gruppe der Ordnung q bilden (siehe die Bemerkung nach Beispiel 11.8). Wegen $k > 1$ wird diese also von $k + p\mathbb{Z}$ erzeugt. Wir können nun das kleinste $n \in \mathbb{N}$ mit $n > 1$ nehmen, so dass $n^q \equiv 1 \mod p$. Dann gilt $n \equiv k^s \mod p$ mit $s \in \{1, \dots, q-1\}$. Indem man τ durch τ^s ersetzt, erreicht man

$$\tau^{-1}\sigma\tau = \sigma^n.$$

Damit ist das Produkt von G vollständig aufgeklärt, und es folgt, dass alle nicht zyklischen Gruppen der Ordnung pq isomorph sind. Gibt es denn überhaupt nicht-zyklische Gruppen der Ordnung pq? Die Antwort lautet ja, was belegt wird durch das Beispiel

$$G = \left\{ \begin{pmatrix} 1 & a \\ 0 & b \end{pmatrix} \mid a, b \in \mathbb{F}_p,\ b^q = 1 \right\} \subseteq \mathrm{GL}_2(\mathbb{F}_p). \tag{6.5}$$

Hierbei steht $\mathbb{F}_p$ wie üblich für den Körper der Restklassen modulo p.

Wir fassen unser Ergebnis zusammen: Falls p nicht kongruent zu 1 modulo q ist, ist jede Gruppe G der Ordnung pq zyklisch, also $G \cong Z_{pq}$. Falls aber $p \equiv 1 \mod q$, so gibt es genau zwei Isomorphietypen von Gruppen der Ordnung pq: Die Z_{pq} und die Gruppe mit Elementen $\tau^i\sigma^j$ ($i \in \{0, \dots, q-1\}$, $j \in \{0, \dots, p-1\}$) und der Multiplikation

$$\tau^{i_1}\sigma^{j_1}\tau^{i_2}\sigma^{j_2} = \tau^{i_1+i_2}\sigma^{j_1 n^{i_2}+j_2}, \tag{6.6}$$

wobei die Exponenten modulo q bzw. p zu reduzieren sind und $n > 1$ minimal ist mit $n^q \equiv 1 \mod p$. Man kann diese Gruppe auch durch Erzeugende und Relationen definieren:

$$G = \left\langle \sigma, \tau \mid \sigma^p = \tau^q = \iota,\ \tau^{-1}\sigma\tau = \sigma^n \right\rangle.$$

Alternativ kann man den zweiten Isomorphietyp auch durch seinen in (6.5) gegebenen Repräsentanten beschreiben.

Beispiel 6.5. Wir betrachten zwei konkrete Beispiele.

(1) Jede Gruppe der Ordnung 15 ist zyklisch, denn 5 ist nicht kongruent zu 1 modulo 3.
(2) Es sei p eine ungerade Primzahl und $q = 2$. Dann ist $p \equiv 1 \mod q$, und das minimale $n > 1$ mit $n^q \equiv 1 \mod p$ ist $p - 1$. Es gibt also zwei Isomorphietypen von Gruppen der Ordnung $2p$, nämlich $G \cong Z_{2p}$ und

$$G \cong \left\{\tau^i\sigma^j | i \in \{0,1\},\ j \in \{0,\dots,p-1\}\right\} = \left\langle \sigma,\tau \mid \sigma^p = \tau^2 = \iota,\ \tau^{-1}\sigma\tau = \sigma^{-1}\right\rangle.$$

Man nennt diese Gruppe eine *Diedergruppe* und bezeichnet sie mit D_p. Es gibt auch Diedergruppen D_n der Ordnung $2n$ für n eine natürliche Zahl, die wie oben definiert sind. Die Gruppe aller orthogonaler Abbildungen, die ein regelmäßiges n-Eck in sich selbst überführt, ist isomorph zur Diedergruppe D_n. ◁

Als zweite Anwendung der Sylow-Sätze möchten wir nachweisen, dass alle Gruppen der Ordnung < 60 auflösbar sind. Für p-Gruppen haben wir das schon gezeigt (Korollar 5.10), und für Gruppen der Ordnung pq mit p und q Primzahlen folgt es aus dem Obigen. Wir behandeln die verbleibenden Gruppenordnungen im Folgenden. Dabei genügt es, jeweils die Existenz eines nicht-trivialen Normalteilers nachzuweisen.

$|G| = 12$: Wegen Satz 6.4(c) gilt $n_2 \equiv 1 \mod 2$ und $n_2 \mid 3$, also $n_2 \in \{1,3\}$. Im Fall $n_2 = 1$ liefert die 2-Sylow-Gruppe einen nicht-trivialen Normalteiler.
Wir betrachten den Fall $n_2 = 3$. G operiert durch Konjugation auf der Menge der 2-Sylow-Gruppen, was nach Proposition 5.2 einen Homomorphismus $G \to S_3$ liefert. $N \trianglelefteq G$ sei der Kern dieses Homomorphismus. Wäre $N = G$, so wäre die Operation nicht transitiv, was Satz 6.4(b) widersprechen würde. Wäre $N = \{\iota\}$, so wäre G isomorph zu einer Untergruppe der S_3, was wegen $|S_3| = 6 < 12 = |G|$ unmöglich ist. Also ist N ein nicht-trivialer Normalteiler.
$|G| = 18$: Wegen Satz 6.4(c) gilt $n_3 \equiv 1 \mod 3$ und $n_3 \mid 2$, also $n_3 = 1$. Die 3-Sylow-Gruppe liefert also einen nicht-trivialen Normalteiler.
$|G| = 20$: Wir haben $n_5 \equiv 1 \mod 5$ und $n_5 \mid 4$, also $n_5 = 1$.
$|G| = 24$: Wir haben $n_2 \in \{1,3\}$. Nun geht es weiter wie für $|G| = 12$.
$|G| = 28$: Wir haben $n_7 = 1$.
$|G| = 30$: Satz 6.4(c) liefert $n_5 \in \{1,6\}$. Der Fall $n_5 = 1$ ist klar, also nehmen wir $n_5 = 6$ an. Der Schnitt von zwei verschiedenen 5-Sylow-Gruppen ist $\{\iota\}$ (denn sie sind isomorph zu Z_5), also gibt es $6 \cdot 4 = 24$ Elemente der Ordnung 5. Andererseits haben wir $n_3 \in \{1,10\}$, und mit obigem Ar-

gument $2n_3$ Elemente der Ordnung 3. Wir erhalten $24 + 2n_3 \leq |G| = 30$, also $n_3 = 1$.

$|G| = 36$: Wir haben $n_3 \in \{1, 4\}$ und müssen den Fall $n_3 = 4$ betrachten. Die Operation von G auf der Menge der 3-Sylow-Gruppen liefert einen Homomorphismus $G \to S_4$. Wegen $|G| > 24 = |S_4|$ funktioniert dasselbe Argument wie für $|G| = 12$.

$|G| = 40$: $n_5 = 1$.

$|G| = 42$: $n_7 = 1$.

$|G| = 44$: $n_{11} = 1$.

$|G| = 45$: $n_5 = 1$.

$|G| = 48$: $n_2 \in \{1, 3\}$. Nun geht es weiter wie für $|G| = 12$.

$|G| = 50$: $n_5 = 1$.

$|G| = 52$: $n_{13} = 1$.

$|G| = 54$: $n_3 = 1$.

$|G| = 56$: $n_7 \in \{1, 8\}$. Ist $n_7 = 8$, so gibt es $8 \cdot 6 = 48$ Elemente der Ordnung 7. Es verbleiben 8 Elemente in G. Da eine 2-Sylow-Gruppe 8 Elemente hat, folgt $n_2 = 1$.

Es folgt, dass eine nicht-abelsche, einfache Gruppe mindestens 60 Elemente haben muss. Umgekehrt wissen wir von der A_5, dass sie einfach ist (Satz 4.6) und 60 Elemente hat. Es ist schwieriger zu zeigen, dass jede einfache Gruppe der Ordnung 60 isomorph zur A_5 ist.

7 Abelsche Gruppen

In diesem Abschnitt werden wir die Struktur der endlichen, abelschen Gruppen aufklären. Wir beginnen aber mit einem „Vorspann“ über direkte Produkte.

Definition 7.1. *G und H seien Gruppen (die nicht abelsch sein müssen). Das kartesische Produkt*

$$G \times H = \{(\sigma, \tau) \mid \sigma \in G,\ \tau \in H\}$$

wird zu einer Gruppe durch

$$(\sigma_1, \tau_1) \cdot (\sigma_2, \tau_2) := (\sigma_1\sigma_2, \tau_1\tau_2) \quad \textit{für} \quad \sigma_i \in G,\ \tau_i \in H.$$

$G \times H$ mit diesem Produkt heißt das **direkte Produkt** *von G und H.*

In derselben Weise wird auch das direkte Produkt $G_1 \times \cdots \times G_r$ mehrerer Gruppen G_i definiert.

Beispiel 7.2. (1) Es sei G die Kleinsche Vierergruppe. Man überzeugt sich leicht, dass $G \cong Z_2 \times Z_2$ gilt.

(2) Es sei $G = Z_2 \times Z_3$. Das Element $(1+2\mathbb{Z}, 1+3\mathbb{Z}) \in G$ hat die Ordnung 6, also gilt $G \cong Z_6$. ◁

Anmerkung 7.3. Es gibt noch weitere Möglichkeiten, das kartesische Produkt zweier Gruppen zu einer Gruppe zu machen. Eine Verallgemeinerung des direkten Produkts ist das *semidirekte Produkt*. Eine noch allgemeinere Konstruktion ist die sogenannte *Gruppenerweiterung*. Alle diese Konstruktionen haben gemeinsam, dass eine der beteiligten Gruppen als Normalteiler und die andere als Faktorgruppe nach diesem Normalteiler auftritt. ◁

Proposition 7.4 („inneres direktes Produkt"). *In einer Gruppe G seien $N, M \trianglelefteq G$ zwei Normalteiler mit $N \cap M = \{\iota\}$ und $NM = G$. Dann gilt*

$$G \cong N \times M,$$

wobei ein Isomorphismus durch

$$\Phi\colon N \times M \to G,\ (\sigma, \tau) \mapsto \sigma \cdot \tau$$

gegeben ist.

Beweis. Um zu zeigen, dass Φ ein Homomorphismus ist, nehmen wir $\sigma_1, \sigma_2 \in N$ und $\tau_1, \tau_2 \in M$. Es gilt

$$\begin{aligned}\Phi(\sigma_1, \tau_1) \cdot \Phi(\sigma_2, \tau_2) &= \sigma_1\tau_1\sigma_2\tau_2 = \sigma_1\sigma_2 \underbrace{\sigma_2^{-1}\tau_1\sigma_2\tau_1^{-1}}_{\in N \cap M = \{\iota\}} \tau_1\tau_2 = \sigma_1\sigma_2\tau_1\tau_2 \\ &= \Phi\left((\sigma_1, \tau_1) \cdot (\sigma_2, \tau_2)\right),\end{aligned}$$

also ist Φ ein Homomorphismus. Außerdem ist Φ injektiv, denn $\Phi(\sigma, \tau) = \iota$ (mit $\sigma \in N$, $\tau \in M$) impliziert

$$\sigma = \tau^{-1} \in N \cap M = \{\iota\},$$

also $(\sigma, \tau) = (\iota, \iota)$. Schließlich folgt die Surjektivität von Φ direkt aus der Voraussetzung $NM = G$. □

Der folgende Satz beschreibt die Struktur der endlichen erzeugten abelschen Gruppen. Da jede endliche Gruppe endlich erzeugt ist, sind die endlichen abelschen Gruppen inbegriffen. Der Satz ist das Hauptergebnis des Abschnitts.

Satz 7.5 (Hauptsatz über endlich erzeugte abelsche Gruppen). *Es sei G eine endlich erzeugte abelsche Gruppe. Dann gibt es s und $r \in \mathbb{N}_0$ und $d_1, \ldots, d_s \in \mathbb{N}_{>1}$ mit $d_i \mid d_{i+1}$ für $i \in \{1, \ldots, s-1\}$, so dass gilt:*

$$G \cong Z_{d_1} \times \cdots \times Z_{d_s} \times \underbrace{Z_\infty \times \cdots \times Z_\infty}_{r\ mal}. \tag{7.1}$$

Für $s = 0$ oder $r = 0$ ist das „leere" direkte Produkt als triviale Gruppe zu interpretieren, $r = 0$ tritt also genau dann auf, wenn G endlich ist.

Beweis. Wir haben $G = \langle \sigma_1, \ldots, \sigma_n \rangle$ und führen den Beweis durch Induktion nach n. Wir behaupten außerdem $r + s \leq n$. Zunächst betrachten wir den Fall, dass es keine Relationen zwischen den σ_i gibt. Damit meinen wir, dass aus $\prod_{i=1}^{n} \sigma_i^{e_i} = \iota$ mit $e_i \in \mathbb{Z}$ folgt, dass alle e_i Null sind. In diesem Fall folgt aus Proposition 7.4

$$G \cong \langle \sigma_1 \rangle \times \cdots \times \langle \sigma_n \rangle \cong Z_\infty \times \cdots \times Z_\infty.$$

Es bleibt der Fall, dass es Relationen $\prod_{i=1}^{n} \sigma_i^{e_i} = \iota$ gibt mit $e_i \in \mathbb{Z}$, nicht alle $e_i = 0$. Durch Umnummerieren und, falls nötig, Ersetzen der e_i durch $-e_i$ können wir $e_1 > 0$ erreichen. Nun wählen wir n Erzeuger $\sigma_1, \ldots, \sigma_n$ und eine Relation der σ_i, so dass $e_1 > 0$ *minimal* wird. Für keine alternative Wahl der Erzeuger gibt es also eine Relation mit kleinerem positiven e_1.

Wir behaupten, dass alle e_i Vielfache von e_1 sind. Für den Nachweis benutzen wir Division mit Rest: $e_i = qe_1 + r$ mit $q, r \in \mathbb{Z}$, $0 \leq r < e_1$. Mit $\tau_1 := \sigma_1 \sigma_i^q$ gelten dann $G = \langle \tau_1, \sigma_2, \ldots, \sigma_n \rangle$ und

$$\sigma_i^r \cdot \tau_1^{e_1} \cdot \prod_{\substack{j=2, \\ j \neq i}}^{n} \sigma_j^{e_j} = \iota$$

Die Annahme $r \neq 0$ würde also zu einem Widerspruch zur Minimalität von e_1 führen. Es folgt, wie behauptet, $e_1 \mid e_i$. Nun setzen wir $\tau := \sigma_1 \cdot \prod_{i=2}^{n} \sigma_i^{e_i/e_1}$. Dann gelten $G = \langle \tau, \sigma_2, \ldots, \sigma_n \rangle$ und $\tau^{e_1} = \iota$. Die Ordnung k von τ teilt also e_1. Da aber $\tau^k = \iota$ auch eine Relation ist, folgt $k = e_1$. Im Falle $e_1 = 1$ gilt $\tau = \iota$, also $G = \langle \sigma_2, \ldots, \sigma_n \rangle$, und der Satz folgt per Induktion. Wir könnnen also $e_1 > 1$ annehmen.

Die nächste Behauptung lautet

$$\langle \tau \rangle \cap \langle \sigma_2, \ldots, \sigma_n \rangle = \{\iota\}.$$

Jedes Element aus dem Schnitt kann man nämlich schreiben als τ^a und zugleich als $\prod_{i=2}^{n} \sigma_i^{a_i}$ mit $a, a_i \in \mathbb{Z}$. Wegen $\operatorname{ord}(\tau) = e_1$ könnnen wir $0 \leq a < e_1$ annehmen. Wir erhalten $\tau^a \cdot \prod_{i=2}^{n} \sigma_i^{-a_i} = \iota$, was im Falle $a > 0$ der Minimalität von e_1 widersprechen würde. Also $a = 0$ und $\tau^a = \iota$, womit die Behauptung bewiesen ist. Mit Proposition 7.4 und $d_1 := e_1$ folgt

$$G \cong \langle \tau \rangle \times \langle \sigma_2, \ldots, \sigma_n \rangle \cong Z_{d_1} \times \langle \sigma_2, \ldots, \sigma_n \rangle.$$

Die Induktionsannahme liefert

$$\langle \sigma_2, \ldots, \sigma_n \rangle \cong Z_{d_2} \times \cdots \times Z_{d_s} \times Z_\infty \times \cdots \times Z_\infty$$

mit $d_i \mid d_{i+1}$ für $1 < i < s$, und außerdem $r + s - 1 \leq n - 1$. Insgesamt folgt (7.1) mit $r + s \leq n$. Es ist nur noch $d_1 \mid d_2$ zu zeigen. Jedem Z_d (mit $d = d_i$ oder ∞) in (7.1) entspricht ein Erzeuger von τ_i von G. Wir können $r + s = n$ annehmen, denn sonst gäbe es weniger als n Erzeuger, und wir wären per Induktion fertig. Wir haben die Relation $\tau_1^{d_1}\tau_2^{d_2} = \iota$. Falls d_2 kein Vielfaches von $d_1 = e_1$ ist, so folgt aus obigem Argument, dass man (nach Ändern der Erzeuger) eine Relation mit einem kleineren positiven Exponenten als e_1 bekommt, im Widerspruch zur Minimalität von e_1. Damit ist alles gezeigt. □

Beispiel 7.6. (1) Es sei G eine abelsche Gruppe der Ordnung 8. Dann gibt es die Möglichkeiten $G \cong Z_8$, $G \cong Z_2 \times Z_4$ oder $G \cong Z_2 \times Z_2 \times Z_2$.
(2) Es sei G eine Gruppe der Ordnung p^2 mit p eine Primzahl. In Korollar 5.11 haben wir gesehen, dass G abelsch ist. Aus Satz 7.5 erhalten wir zwei Möglichkeiten: $G \cong Z_{p^2}$ oder $G \cong Z_p \times Z_p$.
(3) Die durch -1, 2 und 3 erzeugt Untergruppe von $\mathbb{Q} \setminus \{0\}$ (mit der gewöhnlichen Multiplikation) ist isomorph zu $Z_2 \times Z_\infty \times Z_\infty$.
(4) Die Gruppe $\mathbb{Q}$ zusammen mit der gewöhnlichen Addition ist nicht endlich erzeugt, der Hauptsatz ist also nicht anwendbar. Man kann aber zeigen, dass jede endlich erzeugt Untergruppe zyklisch ist. ◁

Anmerkung. Die Zahlen s, r und $d_1, \ldots, d_m$ in Satz 7.5 sind eindeutig bestimmt. Die d_i heißen die *Elementarteiler* von G, und r heißt der Rang. Den Beweis werden wir hier nicht führen. ◁

Wir schließen den Abschnitt mit einer Definition ab.

Definition 7.7. *Für eine endliche Gruppe G heißt*

$$\exp(G) := \operatorname{kgV}\{\operatorname{ord}(\sigma) \mid \sigma \in G\}$$

der **Exponent** *von G.*

Beispiel 7.8. (1) Die S_3 und die A_4 haben den Exponenten 6, die Kleinsche Vierergruppe hat den Exponenten 2 und die zyklische Gruppe Z_n hat den Exponenten n.
(2) Eine endliche abelsche Gruppe hat die Form $G \cong Z_{d_1} \times \cdots \times Z_{d_s}$ mit $d_i \mid d_{i+1}$, also $\exp(G) = d_s$. Es folgt, dass es ein Element $\sigma \in G$ gibt mit $\operatorname{ord}(\sigma) = \exp(G)$.
(3) Es sei $G \cong Z_6 \times Z_{10}$. Dies ist nicht die in Satz 7.5 angegebene Gestalt. Wir erhalten aber $\exp(G) = 30$. Somit bleibt als einzige Möglichkeit $G \cong Z_2 \times Z_{30}$. ◁

8 Einfache Gruppen

Aus Abschnitt 3 wissen wir, dass die endlichen Gruppen in gewisser Weise (die übrigens durch die Theorie der Gruppenerweiterungen beschrieben wird, siehe Anmerkung 7.3) aus den endlichen, einfachen Gruppen zusammengesetzt sind. Diese bilden also so etwas wie die „Atome“ der Gruppentheorie. Ziel dieses Abschnitts ist es, einen groben Überblick (ohne Beweise) über die Gesamtheit aller endlichen, einfachen Gruppen zu geben.

Wir haben bereits zwei Serien einfacher Gruppen kennengelernt: die zyklischen Gruppen Z_p mit p eine Primzahl (siehe Lemma 3.8) und die alternierenden Gruppen A_n mit $n \geq 5$ (siehe Satz 4.6). Wir werden nun einige weitere einfache Gruppen beschreiben.

Lineare Gruppen

Zu einem Körper K und $n \in \mathbb{N}_{>1}$ ist die spezielle lineare Gruppe $\mathrm{SL}_n(K)$ im Allgemeinen nicht einfach, denn

$$Z := \{a \cdot I_n \mid a \in K,\ a^n = 1\} \trianglelefteq \mathrm{SL}_n(K),$$

wobei I_n für die Einheitsmatrix steht. (Es stellt sich heraus, dass Z das Zentrum von $\mathrm{SL}_n(K)$ ist.) Für die *projektive spezielle lineare Gruppe*

$$\mathrm{PSL}_n(K) := \mathrm{SL}_n(K)/Z$$

gilt jedoch:

Satz 8.1. *Es seien $n > 1$ und $(n, |K|) \notin \{(2,2),(2,3)\}$. Dann ist $\mathrm{PSL}_n(K)$ einfach.*

Den Beweis lassen wir weg. Für $|K| = \infty$ ist auch $\mathrm{PSL}(n, K)$ unendlich. Endliche, einfache Gruppen ergeben sich also, wenn man für K einen endlichen Körper nimmt. Am Ende von Abschnitt 18 werden wir sehen, dass es (abgesehen von den Körpern $\mathbb{F}_p$ mit p eine Primzahl) zu jeder Primzahlpotenz $q = p^k$ einen Körper $\mathbb{F}_q$ mit q Elementen gibt. Für $n \in \mathbb{N}_{>1}$ und q eine Primzahlpotenz mit $(n, q) \notin \{(2,2),(2,3)\}$ erhalten wir also die endliche, einfache Gruppe $\mathrm{PSL}_n(\mathbb{F}_q)$.

Für niedrige n und q gibt es ein paar Isomorphien:

$$\mathrm{PSL}_2(\mathbb{F}_2) \cong S_3 \quad \text{und} \quad \mathrm{PSL}_2(\mathbb{F}_3) \cong A_4$$

(diese Gruppen sind also in der Tat nicht einfach), außerdem

$$\mathrm{PSL}_2(\mathbb{F}_4) \cong \mathrm{PSL}_2(\mathbb{F}_5) \cong A_5 \quad \text{und} \quad \mathrm{PSL}_2(\mathbb{F}_7) \cong \mathrm{PSL}_3(\mathbb{F}_2).$$

Weitere klassische Gruppen

Abgesehen von den linearen Gruppen gehören die orthogonalen, unitären und symplektischen Gruppen zu den sogenannten *klassischen Gruppen*. Auch aus diesen weiteren klassischen Gruppen entstehen einfache Gruppen. Da wir hier nur an endlichen Gruppen interessiert sind, setzen wir voraus, dass $K = \mathbb{F}_q$ ein endlicher Körper ist, und wir bilden $V = \mathbb{F}_q^n$ mit $n > 1$. Wir betrachten nun eine Funktion

$$f\colon V \times V \to \mathbb{F}_q,$$

die im zweiten Argument linear sei, und die außerdem *nicht ausgeartet* sei, d.h. aus $f(v,w) = 0$ für alle $w \in V$ folgt $v = 0$. Dann ist

$$G_f := \{A \in \mathrm{GL}_n(\mathbb{F}_q) \mid \ \forall\, v,w \in V: \ f(A \cdot v, A \cdot w) = f(v,w)\}$$

eine Untergruppe der $\mathrm{GL}_n(\mathbb{F}_q)$. Wir betrachten drei Spezialfälle, die die Möglichkeiten für f bei weitem nicht abdecken, die aber zu einfachen Gruppen führen.

1. Spezialfall: Die Funktion f ist *alternierend*, d.h. für alle $v,w \in V$ gelten $f(v,w) = -f(w,v)$ und $f(v,v) = 0$. Hieraus folgt automatisch, dass f bilinear ist. Es stellt sich heraus, dass es nur dann eine solche Bilinearform f gibt, wenn $n = \dim(V)$ gerade ist, und dass die Gruppe G_f dann bis auf Isomorphie unabhängig von der Wahl von f ist. G_f heißt *symplektische Gruppe* und wird (in etwas laxer Notation) mit $\mathrm{Sp}_n(\mathbb{F}_q)$ bezeichnet. Die *projektive symplektische Gruppe* ist die Faktorgruppe

$$\mathrm{PSp}_n(\mathbb{F}_q) := \mathrm{Sp}_n(\mathbb{F}_q)/\{I_n, -I_n\}$$

nach dem Zentrum.

Satz 8.2. *Es seien $n \in \mathbb{N}_{>1}$ gerade und q eine Primzahlpotenz. Bis auf einige Ausnahmen für kleine n und q ist $\mathrm{PSp}_n(\mathbb{F}_q)$ einfach.*

2. Spezialfall: Die Funktion f ist *hermitesch*. Dieser Fall ist nur möglich, wenn q eine Quadratzahl ist. Dann dient die Abbildung $\tau\colon \mathbb{F}_q \to \mathbb{F}_q,\ a \mapsto a^{\sqrt{q}}$ als Analogon zur komplexen Konjugation, und „hermitesch“ bedeutet, dass für alle $v,w \in V$ die Regel $f(v,w) = \tau(f(w,v))$ gilt. Dadurch wird f semilinear im ersten Argument. Wieder stellt sich heraus, dass die entsprechende Gruppe G_f bis auf Isomorphie unabhängig von der Wahl von f ist. Indem man G_f mit $\mathrm{SL}_n(\mathbb{F}_q)$ schneidet und dann das Zentrum herausfaktorisiert, erhält man die *projektive spezielle unitäre Gruppe* $\mathrm{PSU}_n(\mathbb{F}_q)$.

Satz 8.3. *Es seien $n \in \mathbb{N}_{>1}$ und q eine Primzahlpotenz, die eine Quadratzahl ist. Bis auf einige Ausnahmen für kleine n und q ist $PSU_n(\mathbb{F}_q)$ einfach.*

3. Spezialfall: Die Funktion f ist *symmetrisch*, d.h. für alle $v,w \in V$ gilt $f(v,w) = f(w,v)$. Damit ist f bilinear, und G_f heißt die (durch f gegebene) *orthogonale Gruppe*. Falls n ungerade ist, sind die orthogonalen Gruppen zu verschiedenen f isomorph, und wir schreiben sie als $\mathrm{GO}_n(\mathbb{F}_q)$. Für gerade n treten zwei Isomorphietypen auf, die wir als $\mathrm{GO}_n^{\pm}(\mathbb{F}_q)$ schreiben. Wir merken an, dass die Definition der orthogonalen Gruppen für gerade q modifiziert werden muss, indem man statt mit f mit einer quadratischen Form arbeitet. Die Kommutatorgruppe

$$\mathrm{GO}_n^{(\pm)}(\mathbb{F}_q)' =: \Omega_n^{(\pm)}(\mathbb{F}_q)$$

hat für ungerade q den Index 4, sonst 1 oder 2. $\Omega_n^{(\pm)}(\mathbb{F}_q)$ hat wiederum ein Zentrum der Ordnung 1 oder 2, und durch Faktorisieren nach diesem erhält man die Gruppen $\mathrm{P}\Omega_n^{(\pm)}(\mathbb{F}_q)$.

Satz 8.4. *Es sei $n \in \mathbb{N}_{>2}$ und q eine Primzahlpotenz. Bis auf einige Ausnahmen für kleine n und q ist $P\Omega_n^{(\pm)}(\mathbb{F}_q)$ einfach.*

Exzeptionelle Gruppen vom Lie-Typ

Die endlichen klassischen Gruppen bilden vier doppelt-parametrisierte Serien (lineare, symplektische, unitäre und orthogonale, jeweils parametrisiert durch n und q). Es gibt einige einfach-parametrisierte Serien endlicher, einfacher Gruppen. Diese werden bezeichnet mit

$$G_2(q),\ F_4(q),\ E_6(q),\ E_7(q),\ E_8(q) \tag{8.1}$$

sowie

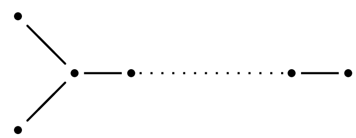
$${}^2E_6(q),\ {}^3D_4(q), {}^2B_2(2^{2m+1}),\ {}^2G_2(3^{2m+1}),\ {}^2F_4(2^{2m+1}) \quad \text{und} \quad {}^2F_4(2)'. \tag{8.2}$$

Überall steht q wieder für eine Primzahlpotenz. Im Gegensatz zu den klassischen Gruppen ist es uns hier nicht möglich, auch nur die Definition dieser Gruppen anzugeben. Ein paar Erläuterungen mögen trotzdem nützlich sein. Sowohl die klassischen Gruppen als auch die in (8.1) und (8.2) genannten Gruppen sind Gruppen vom *Lie-Typ*, die durch sogenannte *Dynkin-Diagramme* beschrieben werden können. Dynkin-Diagramme sind ganz bestimmte Graphen, von denen es vier unendliche Serien (A_n bis D_n) sowie fünf exzeptionelle Typen (G_2, F_4 und E_6 bis E_8) gibt. Beispielsweise hängt das Dynkin-Diagramm

$$A_n: \qquad \bullet\!-\!\!\!-\!\bullet\!-\!\!\!-\!\bullet \cdots\cdots\cdots \bullet\!-\!\!\!-\!\bullet$$

mit den Gruppen $\mathrm{PSL}_n(\mathbb{F}_q)$ zusammen, und das Diagramm

D_n:



mit den Gruppen $\mathrm{P}\Omega_{2n}^{+}(\mathbb{F}_q)$. Nun gibt es bei einigen Dynkin-Diagrammen *Graph-Automorphismen*. Diese führen zu sogenannten *getwisteten Gruppen vom Lie-Typ*. Beispielsweise kann man das Diagramm A_n an seinem Mittelpunkt spiegeln und erhält so einen nicht-trivialen Graph-Automorphismus, aus dem die Gruppen $\mathrm{PSU}_n(\mathbb{F}_q)$ hervorgehen. Die exzeptionellen Gruppen in (8.2) gehen alle aus Graph-Automorphismen hervor, während die in (8.1) ungetwistet sind.

Sporadische einfache Gruppen

Schließlich gibt es noch 26 einfache Gruppen, die sich nicht in die bisherige Systematik einordnen und die deshalb *sporadisch* genannt werden. Sie sind fast alle nach ihrem Entdecker benannt. Die Liste geht los mit M_{11} (Mathieu, Ordnung 7920), M_{12} (Mathieu, Ordnung 95040), J_1 (Janko, Ordnung 175560) und endet mit F_1 (Fischer-Griess, genannt „Monster“, Ordnung 808017424794512875886459904961710757005754368000000000).

Satz 8.5 (Klassifikation der endlichen, einfachen Gruppen)**.** *Jede endliche, einfache Gruppe ist isomorph zu (mindestens) einer Gruppe aus der folgenden Liste:*

- Z_p *mit* p *eine Primzahl;*
- A_n *mit* $n \geq 5$*;*
- *die einfachen, endlichen klassischen Gruppen;*
- *die exzeptionellen Gruppen vom Lie-Typ;*
- *die 26 sporadischen Gruppen.*

Dieser Satz ist das Resultat eines der umfangreichsten Projekte der Mathematikgeschichte, das sich von den 1920er bis in die 1980er Jahre hinzog. Der Beweis ist verteilt auf zahlreiche Fachartikel und dürfte etwa 15000 Druckseiten umfassen, allerdings sind nicht alle Teile publiziert. Inzwischen ist das „Revisionsprojekt“ weit gediehen, in dem der Beweis vereinfacht und lückenlos veröffentlicht werden soll. Fast alle Gruppentheoretiker haben festes Vertrauen in die Richtigkeit des Satzes.

Eine graphische Aufbereitung der Klassifikation als „Periodentafel“ findet man auf `https://irandrus.files.wordpress.com/2012/06/periodic-table-of-groups.pdf`.

Ringe

Im zweiten Teil der Vorlesung beschäftigen wir uns mit Ringen.

9 Ringe und Ideale

Definition 9.1. *Ein* **Ring** *ist eine Menge R zusammen mit zwei Abbildungen $R \times R \to R$, $(a,b) \mapsto a+b$ („Addition“) und $R \times R \to R$, $(a,b) \mapsto a \cdot b$ („Multiplikation“), so dass gelten:*

(a) Zusammen mit der Addition ist R eine abelsche Gruppe. (Wir benutzen additive Notation und schreiben 0 für das neutrale Element.)
(b) Zusammen mit der Multiplikation ist R ein Monoid. (Wir schreiben das neutrale Element als 1.)
(c) Für alle $a, b, c \in R$ gelten:

$$a \cdot (b+c) = a \cdot b + a \cdot c \quad \text{und} \quad (a+b) \cdot c = a \cdot c + b \cdot c.$$

Ein Ring R heißt **kommutativ***, falls für alle $a, b \in R$ gilt:*

$$a \cdot b = b \cdot a.$$

Anmerkung. (a) Manchmal wird nur gefordert, dass R zusammen mit der Multiplikation eine Halbgruppe ist. Für uns ist „Ring“ aber immer gleichbedeutend mit „Ring mit Eins“.
(b) Als weitere Abschwächung kann man nur fordern, dass R zusammen mit der Addition eine Halbgruppe ist. Man erhält dann den Begriff eines *Halbrings*. Ein typisches Beispiel ist der Halbring $\mathbb{N}$. ◁

Bevor wir Beispiele von Ringen anschauen, beweisen wir das folgende Resultat:

Satz 9.2 (elementare Eigenschaften von Ringen)**.** *Es sei R ein Ring.*

(a) Für alle $a \in R$ gilt:
$$0 \cdot a = a \cdot 0 = 0.$$
(b) Falls $0 = 1$ gilt, so folgt $R = \{0\}$. (R ist dann der sogenannte Nullring.*)*
(c) Für alle $a, b \in R$ gilt:
$$(-a) \cdot b = a \cdot (-b) = -(a \cdot b).$$
(d) Es gilt
$$(-1)^2 = 1.$$

Beweis. (a) Wir haben
$$0 \cdot a = 0 \cdot a + a - a = 0 \cdot a + 1 \cdot a - a = (0+1) \cdot a - a = 1 \cdot a - a = a - a = 0,$$
und ebenso folgt $a \cdot 0 = 0$.

(b) Ist $0 = 1$, so folgt für alle $a \in R$:
$$a = 1 \cdot a = 0 \cdot a \underset{(a)}{=} 0.$$

(c) Es gilt
$$(-a) \cdot b = (-a) \cdot b + a \cdot b - (a \cdot b) = (-a + a) \cdot b - (a \cdot b) = 0 \cdot b - (a \cdot b) \underset{(a)}{=} -(a \cdot b),$$
und ebenso folgt $a \cdot (-b) = -(a \cdot b)$.

(d) Wir haben
$$(-1)^2 \underset{(c)}{=} -(1 \cdot (-1)) = -(-1) = 1.$$
□

Beispiel 9.3. (1) $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$ und $\mathbb{C}$ sind kommutative Ringe.

(2) Es sei V ein Vektorraum. Dann ist
$$\mathrm{End}(V) := \{\varphi \colon V \to V \mid \varphi \text{ ist linear}\}$$
zusammen mit der (punktweisen) Addition und der Multiplikation gegeben durch Hintereinanderausführung ein Ring. Für $\dim(V) > 1$ ist $\mathrm{End}(V)$ nicht kommutativ.

(3) Ebenso bilden die $n \times n$-Matrizen mit Einträgen in einem Körper K einen Ring, der für $n > 1$ nicht kommutativ ist.

(4) Für $n \in \mathbb{Z}$ bildet die Menge $\mathbb{Z}/(n)$ der Restklassen modulo n einen kommutativen Ring, wobei Addition und Multiplikation vertreterweise definiert sind.

(5) Es seien S eine Menge und A ein (kommutativer) Ring. Dann wird
$$R = A^S := \{f \colon S \to A \mid f \text{ ist eine Abbildung}\}$$

mit

$$f \underset{+}{\cdot} g \colon S \to A,\ x \mapsto f(x) \underset{+}{\cdot} g(x)$$

(also punktweiser Addition und Multiplikation) ein (kommutativer) Ring. $\triangleleft$

Definition 9.4. *Es sei R ein Ring.*

(a) Ein Element $a \in R$ heißt eine **Einheit***, falls a* invertierbar *ist, d.h. es gibt ein $a' \in R$ mit*

$$a'a = aa' = 1.$$

Dieses a' ist dann eindeutig bestimmt, und wir schreiben $a' =: a^{-1}$. Die Menge

$$R^\times := \{a \in R \mid a \text{ ist Einheit}\}$$

heißt die **Einheitengruppe** *von R. ($R^\times$ ist zusammen mit der Multiplikation eine Gruppe.)*

(b) R heißt ein **Schiefkörper***, falls $R^\times = R \setminus \{0\}$ (dies impliziert $R \neq \{0\}$!), und ein* **Körper***, falls R zusätzlich kommutativ ist. (Der Körperbegriff ist wohlbekannt und wurde schon mehrfach verwendet.)*

(c) Ein Element $a \in R \setminus \{0\}$ heißt **Nullteiler***, falls es ein $b \in R \setminus \{0\}$ gibt mit $a \cdot b = 0$ oder $b \cdot a = 0$.*

(d) R heißt ein **Integritätsbereich***, falls R kommutativ ist, $R \neq \{0\}$, und R keine Nullteiler hat. Jeder Körper ist also ein Integritätsbereich.*

Beispiel 9.5. (1) $\mathbb{Z}$ ist ein Integritätsbereich, und $\mathbb{Z}^\times = \{1, -1\}$.

(2) Im Restklassenring $R = \mathbb{Z}/(6)$ gilt $\overline{2} \cdot \overline{3} = \overline{0}$, $\overline{2}$ und $\overline{3}$ sind also Nullteiler. $\triangleleft$

In der folgenden Definition geht es um Unterstrukturen eines Rings.

Definition 9.6. *Es sei R ein Ring.*

(a) Eine Teilmenge $S \subseteq R$ heißt ein **Unterring***, falls S ein Ring ist (mit der Addition und Multiplikation von R), und $1 \in S$.*

(b) Eine Teilmenge $I \subseteq R$ heißt ein **Linksideal** *(bzw.* **Rechtsideal***), falls $I \neq \emptyset$ und es gelten:*

(i) Für alle $a, b \in I$ ist auch $a + b \in I$.

(ii) Für $a \in I$ und $r \in R$ ist auch $ra \in I$ (bzw. $ar \in I$).

(c) Eine Teilmenge $I \subseteq R$ heißt **Ideal** *(auch:* beidseitiges Ideal*), falls I ein Links- und Rechtsideal ist. Wir benutzen die Schreibweise $I \trianglelefteq R$, um auszudrücken, dass I ein Ideal ist.*

Anmerkung. (a) Falls $I \subseteq R$ ein Links- oder Rechtsideal ist mit $1 \in I$, so folgt $I = R$. Schon hieran merkt man, dass die Begriffe „Ideal" und „Unterring" wenig miteinander zu tun haben.

(b) Jedes Links- oder Rechtsideal enthält das Element 0.

(c) Die Teilmengen $\{0\}$ und R sind immer Ideale. $\triangleleft$

Beispiel 9.7. (1) $\mathbb{Z} \subseteq \mathbb{Q}$ ist ein Unterring.

(2) Für $n \in \mathbb{Z}$ ist $(n) := \{n \cdot a \mid a \in \mathbb{Z}\} \subseteq \mathbb{Z}$ ein Ideal.

(3) Es seien S eine Menge, A ein Ring und $R = A^S$. Für eine Teilmenge $X \subseteq S$ ist

$$I_X := \{f \in R \mid f(x) = 0 \text{ für alle } x \in X\} \subseteq R$$

ein Ideal.

(4) Es seien V ein Vektorraum, $R = \operatorname{End}(V)$ und $W \subset V$ ein Unterraum. Dann ist

$$I := \{\varphi \in R \mid \varphi|_W = 0\} \subseteq R$$

ein Linksideal und

$$J := \{\varphi \in R \mid \varphi(V) \subseteq W\} \subseteq R$$

ein Rechtsideal.

(5) In einem Körper K sind $\{0\}$ und K die einzigen Ideale. ◁

Proposition 9.8 (Schnitte von Idealen)**.** *Es seien R ein Ring und $\mathcal{M} \subseteq \mathfrak{P}(R)$ (die Potenzmenge) eine nicht-leere Menge bestehend aus Idealen von R. Dann ist auch der Schnitt*

$$\bigcap_{I \in \mathcal{M}} I \subseteq R$$

ein Ideal.

Der Beweis verläuft ebenso wie der von Proposition 1.6. Die Proposition ermöglicht die Definition eines Erzeugnisses analog zu Definition 1.7: Für eine Teilmenge $M \subseteq R$ eines Rings ist

$$(M) := \bigcap_{\substack{I \trianglelefteq R \\ \text{mit } M \subseteq I}} I$$

das von M **erzeugte Ideal**. Falls $M = \{a_1, \dots, a_n\}$ endlich ist, schreiben wir auch $(a_1, \dots, a_n)$ für (M) (und nehmen in Kauf, dass diese Notation auch ein Element des n-fachen kartesischen Produkts von R bedeuten kann). Die ersten beiden Teile der folgenden Proposition klären auf, was das Erzeugnis (in den wichtigsten Spezialfällen) tatsächlich ist.

Proposition 9.9 (Idealerzeugnis)**.** *(a) Ist R kommutativ und $a_1, \dots, a_n \in R$, so gilt*

$$(a_1, \dots, a_n) = \{r_1 a_1 + \dots + r_n a_n \mid r_1, \dots, r_n \in R\}.$$

Insbesondere gilt für $a \in R$:

$$(a) = R \cdot a.$$

(b) *Sind $I, J \trianglelefteq R$ Ideale, so folgt*

$$(I \cup J) = \{a + b \mid a \in I,\ b \in J\} =: I + J.$$

(c) *Sind $I, J \trianglelefteq R$ Ideale, so ist auch*

$$I \cdot J := \left\{\sum_{i=1}^{n} a_i b_i \mid n \in \mathbb{N},\ a_i \in I,\ b_i \in J\right\}$$

ein Ideal. $I \cdot J$ heißt das **Idealprodukt***. Für $m \in \mathbb{N}$ schreiben wir I^m für das m-fache Idealprodukt von I.*

Für alle Teile der Proposition ist der Beweis einfach und wird weggelassen.

Beispiel 9.10. In $R = \mathbb{Z}$ gilt

$$(2) + (3) = (1) = \mathbb{Z}.$$

◁

Anmerkung. (a) Bei der Definition von Idealen ist die Analogie zu Untervektorräumen augenfällig, ebenso wie die Analogie zu Linearkombinationen bzw. Summenräumen in Proposition 9.9(a) bzw. (b).
(b) Die Menge aller Ideale bildet zusammen mit der Summe und dem Idealprodukt einen Halbring. ◁

Definition 9.11. *Es sei R ein kommutativer Ring.*

(a) *Ein Ideal von der Form $(a) = R \cdot a$ mit $a \in R$ heißt ein* **Hauptideal***.*
(b) *R heißt ein* **Hauptidealring***, falls R ein Integritätsbereich ist und alle Ideale Hauptideale sind.*

Beispiel 9.12. (1) Die Ideale $\{0\} = (0)$ und $R = (1)$ sind immer Hauptideale.
(2) Also ist jeder Körper ein Hauptidealring.
(3) $\mathbb{Z}[x]$ (der Ring aller Polynome mit Koeffizienten in $\mathbb{Z}$) ist *kein* Hauptidealring. Zur Begründung betrachten wir das Ideal

$$I = (2, x) = \{2g + xh \mid g, h \in \mathbb{Z}[x]\} = \{f \in \mathbb{Z}[x] \mid f(0) \text{ ist gerade}\}.$$

und nehmen an, dass $I = (f)$ mit $f \in I$ gilt. Wegen $2 \in (f)$ ist f konstant, also $f = 2m$ mit $m \in \mathbb{Z}$. Aber dann gilt $x \notin (f)$, ein Widerspruch. ◁

Satz 9.13. *$\mathbb{Z}$ ist ein Hauptidealring.*

Beweis. Es sei $I \trianglelefteq \mathbb{Z}$ ein Ideal mit $I \neq \{0\}$. Dann enthält I Elemente aus $\mathbb{N}_{>0}$, und wir können ein minimales $a \in \mathbb{N}_{>0}$ mit $a \in I$ wählen. Wir behaupten $I = (a)$. Es sei nämlich $b \in I$. Wir führen Division mit Rest aus und erhalten

$$b = qa + r$$

mit $q, r \in \mathbb{Z}$ und $0 \leq r < a$. Hieraus ergibt sich $r = b - qa \in I$, also $r = 0$ wegen der Minimalität von a. Wir erhalten $b = qa \in (a)$. □

10 Faktorringe und Homomorphismen

Ideale stehen in einer starken Analogie zu Normalteilern von Gruppen, da sich nach Idealen Faktorringe bilden lassen und da Ideale als Kerne von Homomorphismen auftreten. Um diese (und andere) Themen geht es in diesem Abschnitt.

Proposition 10.1. *Es seien R ein Ring und $I \trianglelefteq R$ ein Ideal. Für $a, b \in R$ schreiben wir $a \sim b$, falls $a - b \in I$.*

(a) Durch $\sim$ wird eine Äquivalenzrelation auf R gegeben.
(b) Für $a, a', b, b' \in R$ folgt aus $a \sim a'$ und $b \sim b'$, dass auch $a + b \sim a' + b'$ und $ab \sim a'b'$ gelten.

Beweis. (a) Dies folgt aus Lemma 1.10(a), da I eine Untergruppe der additiven Gruppe von R ist.
(b) Es gelten
$$a + b - (a' + b') = (a - a') + (b - b') \in I$$
und
$$ab - a'b' = ab - a'b + a'b - a'b' = (a - a')b + a'(b - b') \in I.$$
□

Proposition 10.1 ermöglicht es, der Menge
$$R/I := \{a + I \mid a \in R\}$$
der Äquivalenzklassen eine Ringstruktur zu geben, indem Addition und Multiplikation vertreterweise definiert werden. Der Ring R/I heißt **Faktorring** (auch: **Restklassenring**) von R modulo I. Seine Elemente heißen **Restklassen** modulo I.

Beispiel 10.2. (1) Es seien $n \in \mathbb{Z}$ und $(n) \subseteq \mathbb{Z}$ das von n erzeugte Ideal. Dann ist $\mathbb{Z}/(n)$ der (bekannte) Restklassenring modulo n. Falls $n = p$ eine Primzahl ist, ist $\mathbb{Z}/(p) = \mathbb{F}_p$ ein Körper mit p Elementen.
(2) Für jeden Ring R ist $R/(1) = \{0 + (1)\}$ der Nullring. ◁

Definition 10.3. *Es seien R ein kommutativer Ring und $I \trianglelefteq R$ ein Ideal.*

(a) I heißt **Primideal***, falls R/I ein Integritätsbereich ist.*
(b) I heißt **maximales Ideal***, falls R/I ein Körper ist.*

Insbesondere ist jedes maximale Ideal ein Primideal.

Beispiel 10.4. (1) Es sei $n \in \mathbb{N}_{>1}$ eine zusammengesetzte Zahl, also $n = mk$ mit $m, k \in \mathbb{N}_{>1}$. In $\mathbb{Z}/(n)$ gilt $\overline{m} \cdot \overline{k} = \overline{0}$, $(n) \subseteq \mathbb{Z}$ ist also kein Primideal.
(2) Ist p eine Primzahl, so ist $(p) \subseteq \mathbb{Z}$ ein maximales Ideal.
(3) $(0) \subseteq \mathbb{Z}$ ist ein Primideal, aber nicht maximal.

(4) $I := (x, 2) \subseteq \mathbb{Z}[x]$ ist ein maximales Ideal, denn $\mathbb{Z}[x]/I = \{0 + I, 1 + I\}$ ist ein Körper mit zwei Elementen. ◁

Der folgende Satz liefert eine Charakterisierung für Primideale und maximale Ideale.

Satz 10.5 (Primideale und maximale Ideale)**.** *Es seien R ein kommutativer Ring und $I \trianglelefteq R$ ein echtes Ideal, also $I \neq R$.*

(a) I ist genau dann ein Primideal, wenn für alle $a, b \in R$ mit $a \cdot b \in I$ auch a oder b ein Element von I ist.
(b) I ist genau dann ein maximales Ideal, wenn für jedes Ideal $J \trianglelefteq R$ mit $I \subsetneqq J$ gilt: $J = R$.

Beweis. Die Bedingung in (a) ist eine direkte Übersetzung der Bedingung, dass R/I nullteilerfrei ist. Im Beweis zu (b) schreiben wir $\overline{a} := a + I \in R/I$ für die Restklasse eines $a \in R$.

Zunächst sei I ein maximales Ideal, und es sei $J \trianglelefteq R$ ein Ideal mit $I \subsetneqq J$. Es gibt also $a \in J \setminus I$. Es gilt $\overline{a} \neq \overline{0}$, also gibt es nach Voraussetzung ein $b \in R$ mit $\overline{a} \cdot \overline{b} = 1$. Dies bedeutet $1 - ab \in I$, also auch $1 - ab \in J$. Wegen $a \in J$ folgt $1 \in J$, also $J = R$.

Nun habe I umgekehrt die Eigenschaft aus (b), und es sei $\overline{a} \in R/I$ mit $\overline{a} \neq \overline{0}$. Dann gilt $I \subsetneqq I + (a) \trianglelefteq R$, also nach Voraussetzung $I + (a) = R$. Insbesondere gilt $1 \in I + (a)$, also gibt es $b \in R$ und $c \in I$ mit $1 = c + ab$. Dies bedeutet $\overline{a} \cdot \overline{b} = \overline{1}$, also ist $\overline{a}$ invertierbar. Damit ist gezeigt, dass R/I ein Körper ist. □

Ist $I \trianglelefteq R$ ein Ideal, dann gibt es genau wie in der Gruppentheorie eine inklusionserhaltende Bijektion zwischen der Menge der Ideale $J \trianglelefteq R$ mit $I \subseteq J$ und der Menge der Ideale von R/I. Diese Bijektion ordnet jedem Ideal $J \trianglelefteq R$ mit $I \subseteq J$ das Ideal $\{a + I \mid a \in J\} \trianglelefteq R/I$ zu. Die Bijektion überträgt Primideale in Primideale und maximale Ideale in maximale Ideale.

Definition 10.6. *Es seien R und S Ringe. Eine Abbildung $\varphi\colon R \to S$ heißt ein* **Homomorphismus***, falls für alle $a, b \in R$ gelten:*

(a) $\varphi(a + b) = \varphi(a) + \varphi(b)$,
(b) $\varphi(a \cdot b) = \varphi(a) \cdot \varphi(b)$ und
(c) $\varphi(1_R) = 1_S$.

Für einen Homomorphismus $\varphi\colon R \to S$ heißt

$$\mathrm{Kern}(\varphi) := \{a \in R \mid \varphi(a) = 0\}$$

der **Kern** *von φ. Weiter heißt φ ein* **Isomorphismus***, falls φ bijektiv ist. Falls es einen Isomorphismus $\varphi\colon R \to S$ gibt, schreiben wir $R \cong S$.*

Beispiel 10.7. (1) Es seien A ein Ring, S eine Menge, $x \in S$ ein fest gewähltes Element und $R = A^S$. Dann ist

$$\varphi_x\colon R \to A,\ f \mapsto f(x)$$

ein Homomorphismus. Für eine Teilmenge $Y \subseteq S$ ist

$$\varphi_Y\colon R \to A^Y,\ f \mapsto f|_Y$$

(die Einschränkung auf Y) ein Homomorphismus.

(2) Für $n \in \mathbb{Z}$ ist die Abbildung

$$\varphi\colon \mathbb{Z} \to \mathbb{Z}/(n),\ a \mapsto a + (n)$$

ein Homomorphismus mit $\operatorname{Kern}(\varphi) = (n)$. In derselben Weise bekommt man zu jedem Ring R und jedem Ideal $I \trianglelefteq R$ einen Homomorphismus $R \to R/I$.

(3) Für jeden Ring R gilt $R/(0) \cong R$. ◁

Wie in der Gruppentheorie gelten für einen Homomorphismus $\varphi\colon R \to S$:

- $\operatorname{Kern}(\varphi) \trianglelefteq R$.
- Genau dann ist φ injektiv, wenn $\operatorname{Kern}(\varphi) \subseteq \{0\}$.
- Das Bild von φ ist eine Unterring von S.
- $R/\operatorname{Kern}(\varphi) \cong \operatorname{Bild}(\varphi)$ (Homomorphiesatz).

Beispiel 10.8. Es seien A ein Ring, $Y \subseteq S$ Mengen, $R = A^S$ und $I_Y := \{f \in R \mid f|_Y = 0\}$. Wegen des Homomorphismus φ_Y in Beispiel 10.7(1) folgt

$$R/I_Y \cong A^Y.$$

◁

Proposition 10.9. *Es sei R ein Ring. Dann gibt es genau einen Homomorphismus $\varphi_0\colon \mathbb{Z} \to R$.*

Beweis. Falls $\varphi_0\colon \mathbb{Z} \to R$ ein Homomorphismus ist, muss $\varphi_0(1_\mathbb{Z}) = 1_R$ gelten. Für $n \in \mathbb{N}_{>0}$ folgt

$$\varphi_0(n) = \varphi_0(\underbrace{1_\mathbb{Z} + \cdots + 1_\mathbb{Z}}_{n \text{ mal}}) = \underbrace{1_R + \cdots + 1_R}_{n \text{ mal}}$$

und

$$\varphi_0(-n) = -(\underbrace{1_R + \cdots + 1_R}_{n \text{ mal}}).$$

Da außerdem $\varphi_0(0_\mathbb{Z}) = 0_R$ gilt, ist φ_0 hierdurch eindeutig bestimmt. Umgekehrt ist das durch die obigen Gleichungen gegebene φ_0 ein Homomorphismus. □

Wegen Proposition 10.9 können wir folgende Definition machen.

Definition 10.10. *Es seien R ein Ring und $\varphi_0\colon \mathbb{Z} \to R$ der eindeutig bestimmte Homomorphismus. Da $\mathbb{Z}$ ein Hauptidealring ist (siehe Satz 9.13),* *gilt* $\mathrm{Kern}(\varphi_0) = (n)$ *mit* $n \in \mathbb{N}_0$. *Dieses* n *heißt die* **Charakteristik** *von* R, *geschrieben als* $n = \mathrm{char}(R)$.

Alternativ kann man die Charakteristik als das kleinste $n \in \mathbb{N}_{>0}$ *definieren, für das*

$$\underbrace{1_R + \cdots + 1_R}_{n \text{ mal}} = 0_R$$

gilt, wobei $\mathrm{char}(R) := 0$, *falls dies für kein* $n \in \mathbb{N}_{>0}$ *eintritt.*

Beispiel 10.11. (1) $\mathbb{Z}$ und $\mathbb{R}$ haben die Charakteristik 0.
(2) Für $n \in \mathbb{N}_0$ gilt $\mathrm{char}\,(\mathbb{Z}/(n)) = n$.
(3) Der Nullring $R = \{0\}$ hat $\mathrm{char}(R) = 1$. ◁

Proposition 10.12 (Charakteristik eines Integritätsbereichs)**.** *Ist* R *ein Integritätsbereich (zum Beispiel ein Körper), so ist* $\mathrm{char}(R)$ *eine Primzahl oder* 0.

Beweis. Wir setzen $n := \mathrm{char}(R)$. Der Homomorphiesatz liefert $\mathbb{Z}/(n) \cong \varphi_0(\mathbb{Z}) \subseteq R$, also ist $\mathbb{Z}/(n)$ ein Integritätsbereich. Damit ist (n) ein Primideal, also ist n nach Beispiel 10.4 eine Primzahl oder 0. □

Wir schließen den Paragraphen ab mit einem Resultat, das speziell für Ringe von Primzahlcharakteristik gilt.

Satz 10.13 (Der Frobenius-Homomorphismus)**.** *Es seien* R *kommutativ und* $p := \mathrm{char}(R)$ *eine Primzahl. Dann wird durch*

$$F\colon R \to R,\ a \mapsto a^p$$

ein Homomorphismus gegeben. F *heißt der* **Frobenius-Homomorphismus**.

Beweis. Es ist klar, dass $F(1) = 1$, und dass $F(a \cdot b) = F(a) \cdot F(b)$ für alle $a, b \in R$ gilt. Es sei $\varphi_0\colon \mathbb{Z} \to R$ der eindeutig bestimmte Homomorphismus. Für $a, b \in R$ gilt:

$$F(a+b) = (a+b)^p = \sum_{i=0}^{p} \varphi_0\left(\binom{p}{i}\right) \cdot a^i b^{p-i},$$

wobei $\binom{p}{i}$ den Binomialkoeffizienten bezeichnet. Für $0 < i < p$ ist $\binom{p}{i} = \frac{p!}{i!(p-i)!}$ ein Vielfaches von p, also gilt $\varphi_0\left(\binom{p}{i}\right) = 0$. Es folgt also $F(a+b) = a^p + b^p = F(a) + F(b)$. □

11 Polynomringe

In diesem Abschnitt steht R immer für einen *kommutativen* Ring.

Wir wollen Polynome mit Koeffizienten in R bilden. Nach dem naiven Polynombegriff sind Polynome Funktionen von einer bestimmten Form. Wenn wir das Polynom $f = x^3 - x$ als Polynom mit Koeffizienten in $\mathbb{F}_3$ anschauen, sehen wir, dass $f(0) = f(1) = f(-1) = 0$, also müsste f nach diesem Polynombegriff das Nullpolynom sein. Wir möchten aber auch Elemente aus größeren Ringen, beispielsweise dem Matrizenring $\mathbb{F}_3^{2\times 2}$, in Polynome einsetzen können. Mit obigem f gilt

$$f\left(\begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}\right) = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix},$$

also sollte f doch nicht als Nullpolynom angesehen werden. Ein anderer Polynombegriff ist also gefragt, und dieser wird in folgender Definition festgelegt. Die Idee ist, dass Polynome durch die Folge ihrer Koeffizienten bestimmt sind.

Definition 11.1. *Die Menge aller Abbildungen $\mathbb{N}_0 \to R$ (d.h. aller R-wertiger Folgen) wird mit $R[[x]]$ bezeichnet. Es seien $f\colon \mathbb{N}_0 \to R,\ i \mapsto a_i$ und $g\colon \mathbb{N}_0 \to R,\ i \mapsto b_i$ zwei Elemente von $R[[x]]$. Wir definieren*

$$f + g\colon \mathbb{N}_0 \to R,\ i \mapsto a_i + b_i \quad \textit{(koeffizientenweise Addition)}$$

und

$$f \cdot g\colon \mathbb{N}_0 \to R,\ i \mapsto \sum_{\substack{j,k\in\mathbb{N}_0 \\ \textit{mit } j+k=i}} a_j \cdot b_k. \quad \textit{(„Cauchy-Produkt“)}$$

Mit dieser Addition und Multiplikation heißt $R[[x]]$ der **formale Potenzreihenring** *über R. Die a_i heißen die* **Koeffizienten** *von f, und f heißt ein* **Polynom**, *falls höchstens endlich viele Koeffizienten ungleich 0 sind. In diesem Fall heißt*

$$\deg(f) := \max\{i \in \mathbb{N}_0 \mid a_i \neq 0\}$$

der **Grad** *von f, wobei $\deg(f) := -\infty$, falls alle a_i gleich 0 sind. Weiter heißt f* **konstant**, *falls $\deg(f) \le 0$, und* **normiert**, *falls $a_{\deg(f)} = 1$.*

Die Menge aller Polynome heißt der **Polynomring** *über R und wird mit $R[x]$ bezeichnet. Mit $x \in R[[x]]$ bezeichnen wir das spezielle Polynom, bei dem $1 \in \mathbb{N}_0$ auf $1 \in R$ und alle anderen $i \in \mathbb{N}_0$ auf $0 \in R$ abgebildet werden. Für $a \in R$ bezeichnen wir das Polynom mit $0 \mapsto a$ und $i \mapsto 0$ für $i > 0$ mit a. Dies führt zu keinen Verwechslungen, liefert aber für $n \ge \deg(f)$ die Beziehung*

$$f = a_0 + a_1 \cdot x + \cdots + a_n \cdot x^n = \sum_{i=0}^{n} a_i x^i.$$

Von nun an werden Polynome nur noch in dieser Form geschrieben, und formale Potenzreihen werden (symbolisch) als $\sum_{i=0}^{\infty} a_i x^i$ geschrieben.

Es ist leicht zu sehen, dass $R[[x]]$ ein kommutativer Ring ist (der Nachweis des Assoziativgesetzes der Multiplikation erfordert als einziges etwas Arbeit), und dass $R[x]$ ein Unterring ist. Die Abbildung $R \to R[x]$, die jedem $a \in R$ das konstante Polynom a zuordnet, ist ein injektiver Homomorphismus, der es uns ermöglicht, R als Unterring von $R[x]$ aufzufassen. Man sieht auch leicht, dass für einen Integritätsbereich R auch $R[[x]]$ und somit auch $R[x]$ Integritätsbereiche sind, und dass gelten:

$$R[x]^\times = R^\times \quad \text{und} \quad R[[x]]^\times = \left\{ \sum_{i=0}^{\infty} a_i x^i \mid a_0 \in R^\times \right\}.$$

Definition 11.2. *Es seien $f = \sum_{i=0}^{n} a_i x^i \in R[x]$ und S ein Ring, so dass $R \subseteq S$ ein Unterring ist. (S muss nicht kommutativ sein.) Für $\alpha \in S$ heißt*

$$f(\alpha) := \sum_{i=0}^{n} a_i \alpha^i \in S$$

die **Auswertung** *von f bei α, und α heißt eine* **Nullstelle** *von f, falls $f(\alpha) = 0$.*

Anmerkung. Falls (mit der Notation von Definition 11.2) R im Zentrum von S liegt, d.h. $r \cdot s = s \cdot r$ für alle $r \in R$ und $s \in S$, so liefert

$$R[x] \to S^S,\ f \mapsto f_S \quad \text{mit} \quad f_S \colon S \to S,\ \alpha \mapsto f(\alpha)$$

einen Homomorphismus. Dieser ordnet jedem Polynom seine *Polynomfunktion* zu. ◁

Zusätzlich zu Addition, Multiplikation und Auswerten liefert der folgende Satz eine weitere Operation, die mit Polynomen durchführbar ist.

Satz 11.3 (Division mit Rest)**.** *Es seien $f, g \in R[x]$, wobei $g = \sum_{i=0}^{n} a_i x^i$ mit $a_n \in R^\times$ und außerdem $R \neq \{0\}$. Dann gibt es Polynome $q, r \in R[x]$ mit*

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

Beweis. Wir schreiben $f = \sum_{i=0}^{m} b_i x^i$ mit $b_i \in R$ und benutzen Induktion nach m. Im Fall $m < n$ stimmt der Satz mit $q = 0$ und $r = f$. Falls $m \geq n$, bilden wir

$$\widetilde{f} := f - a_n^{-1} b_m x^{m-n} \cdot g.$$

Dann gilt $\widetilde{f} = \sum_{i=0}^{m-1} c_i x^i$ mit $c_i \in R$. Nach Induktion gibt es $\widetilde{q}, r \in R[x]$ mit

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

Es folgt

$$f = \widetilde{f} + a_n^{-1} b_m x^{m-n} \cdot g = \underbrace{\left(\widetilde{q} + a_n^{-1} b_m x^{m-n}\right)}_{=:q} \cdot g + r.$$

□

Satz 11.4. *Es seien R ein Integritätsbereich, $f \in R[x]$ und $n := \deg(f) \geq 0$. Dann hat f höchstens n Nullstellen (in R).*

Beweis. Wir benutzen Induktion nach n. Im Fall $n = 0$ ist $f \neq 0$ konstant, hat also keine Nullstellen. Wir können also $n > 0$ und die Existenz einer Nullstelle $\alpha \in R$ voraussetzen. Division mit Rest liefert

$$f = q \cdot (x - \alpha) + r$$

mit $q, r \in R[x]$ und $\deg(r) < 1$, also ist r konstant. Auswerten bei α liefert

$$0 = q(\alpha) \cdot (\alpha - \alpha) + r(\alpha) = r,$$

also

$$f = q \cdot (x - \alpha). \tag{11.1}$$

Falls $\beta \in R$ eine Nullstelle von f mit $\beta \neq \alpha$ ist, so folgt

$$0 = f(\beta) = q(\beta) \cdot (\beta - \alpha),$$

wegen der Nullteilerfreiheit von R also $q(\beta) = 0$. Aus (11.1) folgt $\deg(q) = n - 1$, also hat q nach Induktion höchstens $n - 1$ Nullstellen. Es folgt die Behauptung. □

Das folgende Beispiel zeigt, dass auf die Voraussetzung, dass R ein Integritätsbereich sei, nicht verzichtet werden kann.

Beispiel 11.5. Mit $R = \mathbb{Z}/(8)$ hat das Polynom $f = x^2 - 1$ die Nullstellen $\overline{1}$, $\overline{3}$, $\overline{5}$ und $\overline{7}$. ◁

Aus Satz 11.4 ziehen wir eine interessante Folgerung über Einheitengruppen $R^\times$.

Satz 11.6. *Es seien R ein Integritätsbereich und $G \subseteq R^\times$ eine endliche Untergruppe. Dann ist G zyklisch.*

Beweis. Mit $e := \exp(G)$ ist jedes $a \in G$ eine Nullstelle des Polynoms $x^e - 1 \in R[x]$, aus Satz 11.4 folgt also $|G| \leq e$. Da G abelsch ist, folgt aus Beispiel 7.8(2) die Existenz von $a \in G$ mit $\operatorname{ord}(a) = e$. Wir erhalten $G = \langle a \rangle$. □

Korollar 11.7 (Einheitengruppen in endlichen Körpern)**.** *Ist K ein endlicher Körper, so ist $K^\times$ zyklisch. Insbesondere gilt*

$$\mathbb{F}_p^\times \cong Z_{p-1}$$

In einem endlichen Körper K heißt ein $a \in K^\times$ eine **Primitivwurzel**, falls $K^\times = \langle a \rangle$.

Beispiel 11.8. (1) Es gilt $\mathbb{F}_7^\times \cong Z_6$. Wir suchen eine Primitivwurzel. Die Ordnung von $\overline{2} \in \mathbb{F}_7$ ist 3, und die Ordnung von $\overline{3}$ ist 6, da $\overline{3}^2 = \overline{2}$. Also ist $\overline{3}$ eine Primitivwurzel. Eine weitere ist $\overline{5}$.

(2) $\mathbb{Z}^\times = \{1, -1\} \cong Z_2$ ist zyklisch.

(3) Für $R = \mathbb{Z}/(8)$ gilt $R^\times = \{\overline{1}, \overline{3}, \overline{5}, \overline{7}\} \cong Z_2 \times Z_2$. $R^\times$ ist also nicht zyklisch.

(4) $\mathbb{Q}^\times$ ist nicht zyklisch. ◁

Wir können nun die Lücke schließen, die wir bei der Analyse der Gruppen der Ordnung pq in Abschnitt 6 gelassen haben. Dort wurde behauptet, dass die $\overline{k} \in \mathbb{F}_p$ mit $\overline{k}^q = \overline{1}$ eine zyklische Gruppe der Ordnung q bilden, wobei $p \equiv 1 \mod q$ vorausgesetzt wurde (siehe Seite 32). In der Tat folgt aus $\mathbb{F}_p^\times \cong Z_{p-1}$, dass für jeden Teiler $n \in \mathbb{N}$ von $p-1$ die Elemente $\overline{a} \in \mathbb{F}_p$ mit $\overline{a}^n = \overline{1}$ eine zyklische Gruppe der Ordnung n bilden.

Satz 11.9 (Interpolationspolynome)**.** *Es seien K ein Körper, $\alpha_0, \ldots, \alpha_n \in K$ paarweise verschieden und $\beta_0, \ldots, \beta_n \in K$ beliebig. Dann existiert genau ein Polynom $f \in K[x]$ mit $\deg(f) \le n$ und $f(\alpha_i) = \beta_i$ für $i = 0, \ldots, n$.*

Beweis. Für die Polynome

$$f_i := \prod_{j \in \{0,\ldots,n\} \setminus \{i\}} \frac{x - \alpha_j}{\alpha_i - \alpha_j} \quad (i \in \{0, \ldots, n\})$$

gelten $\deg(f_i) = n$ und

$$f_i(\alpha_j) = \delta_{i,j} := \begin{cases} 1 & \text{falls } i = j, \\ 0 & \text{sonst} \end{cases} \quad (i, j \in \{0, \ldots, n\}).$$

Also liefert $f := \sum_{i=0}^n \beta_i f_i$ das Gewünschte. Ist $g \in K[x]$ ein weiteres solches Polynom, so hat $f - g$ mindestens $n+1$ Nullstellen, also $f - g = 0$ wegen Satz 11.4. □

Bisher haben wir nur den *univariaten* Polynomring $R[x]$ betrachtet. Zum Abschluss des Abschnitts beschäftigen wir uns noch mit *multivariaten Polynomringen* $R[x_1, \ldots, x_n]$. Diese lassen sich rekursiv definieren als Polynomring über $R[x_1, \ldots, x_{n-1}]$:

$$R[x_1, \ldots, x_n] := (R[x_1, \ldots, x_{n-1}])\,[x_n].$$

Alternativ kann man sie definieren als einen Spezialfall von sogenannten *Monoidringen*, die wir nun einführen.

Definition 11.10. *Es sei G ein Monoid. Auf der Menge*

$$RG := \{f \colon G \to R \mid f(\sigma) \neq 0 \text{ für höchstens endlich viele } \sigma \in G\}$$

definieren wir eine Addition und Multiplikation, indem wir für $f, g \in RG$ setzen:

$$f+g\colon G\to R,\ \sigma\mapsto f(\sigma)+g(\sigma)$$

und

$$f\cdot g\colon G\to R,\ \sigma\mapsto \sum_{\substack{\tau,\rho\in G\\ \text{mit } \tau\cdot\rho=\sigma}} f(\tau)g(\rho).$$

(Man beachte, dass in der obigen Summe höchstens endlich viele Summanden $\neq 0$ sind.) RG heißt der **Monoidring** *von G (über R). Falls G eine Gruppe ist, heißt RG der Gruppenring.*

Man rechnet leicht nach, dass RG ein Ring ist. Er ist genau dann kommutativ, wenn G abelsch ist (oder wenn $R=\{0\}$). Vermöge der Einbettungen

$$R\to RG,\ a\mapsto f_a \quad \text{mit} \quad f_a\colon G\to R,\ \sigma\mapsto a\cdot\delta_{\sigma,\iota}=\begin{cases} a & \text{falls } \sigma=\iota,\\ 0 & \text{sonst}\end{cases}$$

und

$$G\to RG,\ \tau\mapsto f_\tau \quad \text{mit} \quad f_\tau\colon G\to R,\ \sigma\mapsto \delta_{\sigma,\tau}=\begin{cases} 1 & \text{falls } \sigma=\tau,\\ 0 & \text{sonst}\end{cases}$$

können wir R und G als Teilmengen von RG auffassen. Damit erhalten wir für $f\in RG$ die Darstellung

$$f=\sum_{\sigma\in G} a_\sigma\cdot\sigma,$$

wobei $a_\sigma=f(\sigma)\in R$.

Beispiel 11.11. (1) Für $G=\mathbb{N}_0$ (mit der natürlichen Addition) erhalten wir

$$RG=R[x].$$

(2) Für $G=\mathbb{N}_0\times\cdots\times\mathbb{N}_0$ (n-faches kartesisches Produkt mit komponentenweiser Addition) liefert RG die oben angekündigte alternative Definition des multivariaten Polynomrings. Mit der Schreibweise $x_i=(0,\dots,0,1,0,\dots,0)\in\mathbb{N}_0^n$ (mit der 1 in der i-ten Komponente) lässt sich jedes Element $f\in RG$ schreiben als

$$f=\sum_{i_1,\dots,i_n\in\mathbb{N}_0} a_{i_1,\dots,i_n}\cdot x_1^{i_1}\cdots x_n^{i_n}$$

mit $a_{i_1,\dots,i_n}\in R$, wobei höchstens endlich viele der $a_{i_1,\dots,i_n}$ ungleich 0 sind.

(3) Für $G=Z_\infty$ sei $x\in G$ ein Erzeuger. Dann lässt sich jedes $f\in RG$ schreiben als

$$f=\sum_{i=-N}^{N} a_i x^i$$

mit $N \in \mathbb{N}$ und $a_i \in R$. RG heißt der Ring der *Laurent-Polynome* und wird mit $R[x, x^{-1}]$ bezeichnet.

(4) Für $G = \langle\sigma\rangle \cong Z_2$ ist $RG = R \cdot \iota \oplus R \cdot \sigma$ mit $\sigma^2 = \iota$, also $RG \cong R[x]/(x^2-1)$. Die Gleichung $(\sigma-1)(\sigma+1) = 0$ zeigt, dass RG auch dann Nullteiler hat, wenn R ein Integritätsbereich ist. ◁

12 Quotientenkörper

In diesem Abschnitt wollen wir einen Ring zu einem Körper machen. Als Modell dient der Übergang von $\mathbb{Z}$ zu $\mathbb{Q}$. Wir haben $\mathbb{Q} = \{\frac{r}{s} \mid r, s \in \mathbb{Z},\ s \neq 0\}$, und für $\frac{r_1}{s_1}$ und $\frac{r_2}{s_2} \in \mathbb{Q}$ gilt:

$$\frac{r_1}{s_1} = \frac{r_2}{s_2} \quad \Longleftrightarrow \quad s_2 r_1 = s_1 r_2.$$

Dies motiviert die Einführung einer Relation, von der wir nachweisen, dass sie eine Äquivalenzrelation ist:

Lemma 12.1. *Es sei R ein Integritätsbereich. Für $(r_1, s_1), (r_2, s_2) \in R \times (R \setminus \{0\})$ schreiben wir*

$$(r_1, s_1) \sim (r_2, s_2), \quad \textit{falls} \quad s_2 r_1 = s_1 r_2.$$

Durch „$\sim$“ wird eine Äquivalenzrelation auf $R \times (R \setminus \{0\})$ definiert.

Beweis. Die Reflexivität und Symmetrie von „$\sim$“ sind klar. Zum Beweis der Transitivität seien $(r_1, s_1), (r_2, s_2), (r_3, s_3) \in R \times (R \setminus \{0\})$ mit $s_2 r_1 = s_1 r_2$ und $s_3 r_2 = s_2 r_3$. Dann folgt

$$s_2 s_3 r_1 = s_3 s_2 r_1 = s_3 s_1 r_2 = s_1 s_3 r_2 = s_1 s_2 r_3 = s_2 s_1 r_3,$$

also $s_2 (s_3 r_1 - s_1 r_3) = 0$. Wegen $s_2 \neq 0$ und der Nullteilerfreiheit von R folgt $s_3 r_1 = s_1 r_3$, also $(r_1, s_1) \sim (r_3, s_3)$. □

Beispiel 12.2. Ohne die Voraussetzung, dass R ein Integritätsbereich ist, wäre Lemma 12.1 falsch. Beispielsweise gilt in $\mathbb{Z}/(4)$:

$$(\overline{1}, \overline{1}) \sim (\overline{2}, \overline{2}) \quad \text{und} \quad (\overline{2}, \overline{2}) \sim (\overline{0}, \overline{2}), \quad \text{aber } \textit{nicht} \quad (\overline{1}, \overline{1}) \sim (\overline{0}, \overline{2}).$$

◁

Auch die Addition und die Multiplikation in folgender Definition wird durch den Übergang von $\mathbb{Z}$ zu $\mathbb{Q}$ motiviert.

Definition 12.3. *Es sei R ein Integritätsbereich. Mit $\mathrm{Quot}(R)$ bezeichnen wir die Menge der Äquivalenzklassen bezüglich der Relation „$\sim$“ aus Lemma 12.1. Wir schreiben die Äquivalenzklassen als Brüche, d.h. für $r, s \in R$*

mit $s \neq 0$ *schreiben wir* $\frac{r}{s} := [(r,s)]_\sim$. *Für* $\frac{r_1}{s_1}, \frac{r_2}{s_2} \in \mathrm{Quot}(R)$ *definieren wir*

$$\frac{r_1}{s_1} + \frac{r_2}{s_2} := \frac{s_2 r_1 + s_1 r_2}{s_1 s_2} \quad \textit{und} \quad \frac{r_1}{s_1} \cdot \frac{r_2}{s_2} := \frac{r_1 r_2}{s_1 s_2}.$$

Versehen mit dieser Addition und Multiplikation heißt Quot(R) *der* **Quotientenkörper** *von* R.

Zu dieser Definition ist zunächst nachzuweisen, dass die Addition und die Multiplikation auf Quot(R) *wohldefiniert* sind, d.h. unabhängig von der Wahl der Klassenvertreter. Dies geschieht durch Rechnungen, die wir hier weglassen. Als nächstes kann man nachrechnen, dass Quot(R) ein kommutativer Ring ist. Das Nullelement ist $\frac{0}{1}$, und das Einselement ist $\frac{1}{1}$. Außerdem sieht man, dass es zu jedem $\frac{r}{s}$ mit $r \neq 0$ ein Inverses gibt, nämlich $\frac{s}{r}$. Damit ist Quot(R) in der Tat ein Körper.

Wir haben einen injektiven Homomorphismus

$$\varepsilon\colon R \to \mathrm{Quot}(R),\ r \mapsto \frac{r}{1},$$

der es uns erlaubt, R als Unterring von Quot(R) aufzufassen.

Beispiel 12.4. (1) $\mathrm{Quot}(\mathbb{Z}) = \mathbb{Q}$.

(2) Es sei K ein Körper. Dann heißt

$$\mathrm{Quot}\left(K[x]\right) = \left\{ \frac{f}{g} \mid f, g \in K[x],\ g \neq 0 \right\} =: K(x)$$

der **rationale Funktionenkörper** über K.

(3) Falls K ein Körper ist, gilt $\mathrm{Quot}(K) \cong K$. ◁

Anmerkung. Die Bildung des Quotientenkörpers ist ein Spezialfall des allgemeineren Prinzips der *Lokalisation*: Für einen kommutativen Ring R und ein (multiplikatives) Untermonoid $S \subseteq R$ wird $S^{-1}R$ so definiert, dass die Elemente aus S invertierbar werden. Genauer definiert man auf $R \times S$ eine Relation „$\sim$" durch

$$(r_1, s_1) \sim (r_2, s_2) \quad \Longleftrightarrow \quad \text{es gibt } s \in S \quad \textit{mit} \quad s s_2 r_1 = s s_1 r_2.$$

Nun kann man nachprüfen, dass „$\sim$" eine Äquivalenzrelation ist, und man kann der Faktormenge $S^{-1}R = (R \times S)/\sim$ wie in Definition 12.3 eine Ringstruktur geben.

Typische Beispiele für Untermonoide $S \subseteq R$ sind $S = \{a^i \mid i \in \mathbb{N}_0\}$ mit $a \in R$ und $S = R \setminus P$ mit $P \subseteq R$ ein Primideal. ◁

13 Teilbarkeit und Primzerlegung

Während des gesamten Abschnitts steht R für einen Integritätsbereich. Wir verallgemeinern einige für die Arithmetik von $\mathbb{Z}$ bekannte Begriffe.

Definition 13.1. *Es seien $a, b \in R$.*

(a) Die Sprechweise „a teilt b“ (Schreibweise: $a \mid b$) bedeutet, dass es $c \in R$ gibt mit $b = c \cdot a$.
(b) Falls $a \mid b$ und $b \mid a$, so heißen a und b **assoziiert** *(Schreibweise: $a \sim b$.) Hierzu gleichbedeutend sind die Bedingungen $b = c \cdot a$ mit $c \in R^\times$ und $(a) = (b)$. Assoziiertheit ist eine Äquivalenzrelation.*
(c) Wir nennen a **irreduzibel***, falls $a \neq 0$, $a \notin R^\times$, und für alle $b, c \in R$ mit $a = b \cdot c$ gilt: $b \sim a$ oder $c \sim a$.*
(d) Wir nennen a ein **Primelement***, falls $a \neq 0$, $a \notin R^\times$, und für alle $b, c \in R$ mit $a \mid (b \cdot c)$ gilt: $a \mid b$ oder $a \mid c$. Hierzu gleichbedeutend ist die Bedingung, dass das Hauptideal (a) ein Primideal ist. Es ist klar, dass jedes Primelement irreduzibel ist.*
(e) Wir sagen, dass R die Eigenschaft **F1** *hat, falls es für jedes $a \in R$ mit $a \neq 0$ und $a \notin R^\times$ irreduzible Elemente $p_1, \ldots, p_r \in R$ gibt mit $a = p_1 \cdots p_r$. (Achtung: dies ist nicht allgemein gängige Sprechweise!)*
(f) R heißt **faktoriell** *(auch:* Ring mit eindeutiger Primzerlegung*), falls R die Eigenschaft F1 hat und jedes irreduzible Element von R ein Primelement ist.*

Beispiel 13.2. Wir betrachten den formalen Potenzreihenring $R = K[[x]]$ über einem Körper K. Für $0 \neq f = \sum_{i=0}^{\infty} a_i x^i \in R$ schreiben wir $\operatorname{subdeg}(f) := \min\{i \in \mathbb{N}_0 \mid a_i \neq 0\}$. Weil f genau dann eine Einheit ist, wenn $a_0 \neq 0$ gilt, folgt

$$f \sim x^{\operatorname{subdeg}(f)}.$$

Mit $\operatorname{subdeg}(0) := \infty$ gelten also für $f, g \in R$:

$$f \mid g \quad \Longleftrightarrow \quad \operatorname{subdeg}(f) \leq \operatorname{subdeg}(g)$$

und

$$f \sim g \quad \Longleftrightarrow \quad \operatorname{subdeg}(f) = \operatorname{subdeg}(g).$$

Wegen $\operatorname{subdeg}(fg) = \operatorname{subdeg}(f) + \operatorname{subdeg}(g)$ gilt

$$f \text{ ist irreduzibel} \quad \Longleftrightarrow \quad \operatorname{subdeg}(f) = 1 \quad \Longleftrightarrow \quad f \text{ ist Primelement.}$$

Es folgt, dass R faktoriell ist. ◁

In Beispiel 13.4 werden wir einen nicht faktoriellen Ring kennenlernen. Die folgende Proposition liefert eine äquivalente Formulierung von Definition 13.1(f).

Proposition 13.3 (Charakterisierung von faktoriellen Ringen)**.** *R erfülle F1. Dann sind äquivalent:*

(a) *R ist faktoriell.*
(b) *Für irreduzible Elemente $p_1, \ldots, p_r, q_1, \ldots, q_s \in R$ mit*

$$p_1 \cdots p_r = q_1 \cdots q_s$$

gilt $r = s$, und es gibt eine Permutation $\pi \in S_r$, so dass für $i = 1, \ldots, r$ gilt:

$$q_i \sim p_{\pi(i)}.$$

Beweis. Wir setzen zunächst (a) voraus und benutzen Induktion nach r für den Nachweis von (b). Für $r = 1$ folgt aus der Irreduzibilität von p_1 sofort $s = 1$ und $p_1 = q_1$. Für $r \geq 2$ ist p_1 ein Teiler des Produkts $q_1 \cdots q_s$, wegen der Primelementeigenschaft von p_1 gibt es also ein i mit $p_1 \mid q_i$. Wegen der Irreduzibilität von q_i folgt

$$q_i = e \cdot p_1 \quad \text{mit} \quad e \in R^\times.$$

Wir können p_1 durch q_i und p_2 durch $e^{-1}p_2$ ersetzen. Wegen der Nullteilerfreiheit von R folgt

$$p_2 \cdots p_r = q_1 \cdots q_{i-1} q_{i+1} \cdots q_s.$$

Hieraus folgt (b) per Induktion.

Nun setzen wir (b) voraus und zeigen (a). Für $a, b, c, p \in R$ mit

$$c \cdot p = a \cdot b$$

mit p irreduzibel müssen wir $p \mid a$ oder $p \mid b$ zeigen. Dies folgt sofort, falls a, b oder c in $R^\times \cup \{0\}$ liegt. Andernfalls erhalten wir zwei Zerlegungen in irreduzible Faktoren:

$$(\text{Zerlegung von } a) \cdot (\text{Zerlegung von } b) = p \cdot (\text{Zerlegung von } c),$$

nach Voraussetzung ist p assoziiert zu einem irreduziblen Faktor von a oder b, also $p \mid a$ oder $p \mid b$. □

Beispiel 13.4. Wir betrachten den Ring

$$R = \mathbb{Z}[\sqrt{-5}] := \left\{a + b\sqrt{-5} \mid a, b \in \mathbb{Z}\right\} \subseteq \mathbb{C}.$$

Die sogenannte *Norm*, also die Abbildung

$$N\colon R \to \mathbb{Z},\ a + b\sqrt{-5} \mapsto (a + b\sqrt{-5}) \cdot (a - b\sqrt{-5}) = a^2 + 5b^2$$

ist multiplikativ. Dies benutzen wir, um zu zeigen, dass $2 \in R$ irreduzibel ist. Ist nämlich $2 = z_1 z_2$ mit $z_i \in R$, so folgt $4 = N(z_1) \cdot N(z_2)$, also $N(z_i) \in \{1, 2, 4\}$. Aber $N(z_i) = 2$ ist wegen der speziellen Gestalt der Norm unmöglich. Also hat eines der z_i Norm 1, und es folgt $z_i \in R^\times$. Der andere

Faktor ist also zu 2 assoziiert. Auf der anderen Seite ist 2 kein Primelement, denn 2 teilt $6 = (1+\sqrt{-5}) \cdot (1-\sqrt{-5})$, aber 2 teilt keinen der Faktoren. R ist also nicht faktoriell.

Man gewinnt aus der obigen Betrachtung auch ein sehr instruktives Beispiel für eine nicht eindeutige Zerlegung in irreduzible Elemente:

$$2 \cdot 3 = (1+\sqrt{-5}) \cdot (1-\sqrt{-5})$$

Ringe von dieser Art werden in der algebraischen Zahlentheorie betrachtet. $\triangleleft$

Unser nächstes Ziel ist es zu zeigen, dass jeder Hauptidealring faktoriell ist.

Lemma 13.5. *Es seien R ein Hauptidealring und $I_1, I_2, I_3, \ldots \trianglelefteq R$ eine Folge von Idealen mit $I_i \subseteq I_{i+1}$ für alle i. Dann gibt es ein $n \in \mathbb{N}$, so dass $I_i = I_n$ für $i \geq n$ gilt.*

Beweis. Wir zeigen zunächst, dass die Vereinigungsmenge $I := \bigcup_{i \in \mathbb{N}} I_i$ ein Ideal ist. Zu $a, b \in I$ gibt es $i, j \in \mathbb{N}$ mit $a \in I_i$ und $b \in I_j$. Mit $k := \max\{i, j\}$ folgt $a, b \in I_k$, also $a + b \in I_k$ und damit $a + b \in I$. Außerdem gilt für $r \in R$: $ra \in I_i \subseteq I$.

Da R ein Hauptidealring ist, gilt $I = (a)$ mit $a \in I$, also $a \in I_n$ für ein $n \in \mathbb{N}$. Für $i \geq n$ folgt

$$I_i \subseteq I = (a) \subseteq I_n \subseteq I_i,$$

also Gleichheit. $\square$

Ein Ring, der die Eigenschaft von Lemma 13.5 erfüllt, heißt ein *Noetherscher Ring*. Noethersche Ringe spielen in der kommutativen Algebra (d.h. der Theorie der kommutativen Ringe) eine wichtige Rolle.

Lemma 13.6. *Jeder Hauptidealring erfüllt die Eigenschaft F1.*

Beweis. Es sei R ein Hauptidealring. Aus Lemma 13.5 folgt, das jede nichtleere Menge von Idealen von R ein (bezüglich der Teilmengenrelation) maximales Element hat. Unter der Annahme, dass R die Eigenschaft F1 nicht erfüllt, ist die Menge

$$\mathcal{A} := \left\{(a) \mid 0 \neq a \in R \setminus R^\times, a \text{ ist nicht Produkt von irreduziblen Elementen}\right\}$$

nicht leer, hat also ein maximales Element (a). Wegen $(a) \in \mathcal{A}$ ist $0 \neq a \in R \setminus R^\times$, und a ist nicht irreduzibel, also $a = b \cdot c$ mit $b \not\sim a$ und $c \not\sim a$. Es folgt $(a) \subsetneqq (b)$ und $(a) \subsetneqq (c)$, also liegen (b) und (c) wegen der Maximalität von (a) nicht in $\mathcal{A}$. Folglich sind b und c und damit auch a Produkte von irreduziblen Elementen, im Widerspruch zu $(a) \in \mathcal{A}$. Damit ist der Beweis erbracht. $\square$

Satz 13.7. *Jeder Hauptidealring ist faktoriell.*

Beweis. Wir müssen zeigen, dass jedes irreduzible Element $p \in R$ eines Hauptidealrings ein Primelement ist. Wegen $p \notin R^\times$ ist $I := (p) \neq R$. Es sei $I \subsetneqq J \trianglelefteq R$. Dann gilt $J = (a)$ mit $a \mid p$ und $a \not\sim p$, also folgt $a \in R^\times$ aus der Irreduzibilität von p. Wir erhalten $J = R$. Dies zeigt, dass $I = (p)$ ein maximales Ideal ist, also auch ein Primideal. Es folgt die Behauptung. □

Wir definieren nun euklidische Ringe als Ringe, in denen es in folgendem Sinne eine Division mit Rest gibt.

Definition 13.8. *R heißt* **euklidisch***, falls es eine Funktion $\delta\colon R \to \mathbb{N}_0$ gibt, so dass für alle $a, b \in R$ mit $b \neq 0$ Elemente $q, r \in R$ existieren mit*

$$a = q \cdot b + r \quad \textit{und} \quad \delta(r) < \delta(b).$$

Beispiel 13.9. (1) $R = \mathbb{Z}$ mit $\delta(a) = |a|$ ist euklidisch.

(2) Es sei K ein Körper und $R = K[x]$ der Polynomring. Wegen Satz 11.3 ist R mit

$$\delta\colon R \to \mathbb{N}_0,\ f \mapsto \begin{cases} \deg(f) + 1 & \text{falls } f \neq 0, \\ 0 & \text{sonst} \end{cases}$$

ein euklidischer Ring.

(3) Jeder Körper K wird mit der Funktion

$$\delta\colon K \to \mathbb{N}_0,\ a \mapsto \begin{cases} 1 & \text{falls } a \neq 0, \\ 0 & \text{sonst} \end{cases}$$

ein euklidischer Ring. Für $a, b \in K$ mit $b \neq 0$ kann man $q = a/b$ und $r = 0$ nehmen.

(4) $R = \mathbb{Z}[i] := \{a + bi \mid a, b \in \mathbb{Z}\} \subseteq \mathbb{C}$ ist ein euklidischer Ring. Wir stellen dies als Übungsaufgabe. $\mathbb{Z}[i]$ heißt auch der Ring der *Gaußschen ganzen Zahlen.* ◁

Satz 13.10. *Jeder euklidische Ring ist ein Hauptidealring.*

Beweis. Es sei $I \trianglelefteq R$ ein Ideal in einem euklidischen Ring. Wir können $I \neq \{0\}$ annehmen, da $I = (0)$ ohnehin ein Hauptideal ist. Dann existiert ein $b \in I \setminus \{0\}$, so dass $\delta(b)$ minimal wird. Wir behaupten $I = (b)$. Für den Nachweis sei $a \in I$. Es gibt $q, r \in R$ mit

$$a = q \cdot b + r \quad \text{und} \quad \delta(r) < \delta(b).$$

Wegen $r = a - q \cdot b \in I$ folgt aus der Minimalität von $\delta(b)$, dass $r = 0$ gelten muss. Also $a = q \cdot b \in (b)$ wie behauptet. □

Korollar 13.11. *(a) $\mathbb{Z}$ ist faktoriell.*
(b) Jeder Polynomring $K[x]$ über einem Körper ist faktoriell.

Im ersten Teil der Vorlesung haben wir die eindeutige Primzerlegung in $\mathbb{Z}$ naiv benutzt. Dies ist hiermit gerechtfertigt.

Für den Rest des Abschnitts seien R ein faktorieller Ring und $K = \mathrm{Quot}(R)$ sein Quotientenkörper. Ist $p \in R$ ein Primelement, so ist auch jedes zu p assoziierte Element ein Primelement. Da Assoziiertheit eine Äquivalenzrelation ist, können wir ein Vertretersystem $\mathbb{P}_R$ der Assoziiertheitsklassen von Primelementen wählen. Dann hat jedes $a \in R \setminus \{0\}$ eine eindeutige Darstellung als

$$a = a_0 \cdot \prod_{p \in \mathbb{P}_R} p^{e_p}$$

mit $a_0 \in R^\times$ und $e_p \in \mathbb{N}_0$, wobei höchstens endlich viele e_p positiv sind.

Beispiel 13.12. (1) Für $R = \mathbb{Z}$ ist

$$\mathbb{P}_\mathbb{Z} := \{p \in \mathbb{N} \mid p \text{ ist Primzahl}\}$$

eine naheliegende Wahl.

(2) Für $R = k[x]$ (mit k ein Körper) ist

$$\mathbb{P}_{k[x]} := \{f \in k[x] \mid f \text{ ist irreduzibel und normiert}\}$$

eine naheliegende Wahl. ◁

Nachdem wir $\mathbb{P}_R$ gewählt haben, können wir einen eindeutigen größten gemeinsamen Teiler (ggT) definieren, indem wir für $a = a_0 \cdot \prod_{p \in \mathbb{P}_R} p^{e_p}$ und $b = b_0 \cdot \prod_{p \in \mathbb{P}_R} p^{f_p}$ definieren:

$$\mathrm{ggT}(a, b) := \prod_{p \in \mathbb{P}_R} p^{\min\{e_p, f_p\}}.$$

Weiter setzen wir $\mathrm{ggT}(a, 0) = \mathrm{ggT}(0, a) := \prod_{p \in \mathbb{P}_R} p^{e_p}$ und $\mathrm{ggT}(0, 0) := 0$. Falls $\mathrm{ggT}(a, b) = 1$, so heißen a und b **teilerfremd**. Für $a_1, \ldots, a_n \in R$ definieren wir rekursiv

$$\mathrm{ggT}(a_1, \ldots, a_n) = \mathrm{ggT}\left(a_1, \mathrm{ggT}(a_2, \ldots, a_n)\right).$$

Es ist klar, dass der ggT alle a_i teilt, aber umgekehrt ein Vielfaches von jedem gemeinsamen Teiler der a_i ist. Durch diese beiden Eigenschaften wird der ggT bis auf Assoziiertheit eindeutig bestimmt. Es dürfte klar sein, dass man auf ganz ähnliche Weise auch ein kleinstes gemeinsames Vielfaches (kgV) definieren kann.

Abgesehen davon, dass der ggT an sich interessant ist, werden wir ihn nun benutzen, um zu zeigen, dass mit R auch der Polynomring $R[x]$ faktoriell ist.

Definition 13.13. *Es sei $f = \sum_{i=0}^n a_i x^i \in R[x]$ ein Polynom.*

(a) Der **Inhalt** *von f ist*

$$c(f) := \mathrm{ggT}(a_0, \ldots, a_n).$$

(b) Wir nennen f **primitiv**, *falls $c(f) = 1$.*
(c) Falls $f \neq 0$, heißt

$$p(f) := \frac{f}{c(f)} \in R[x]$$

der **primitive Teil** *von f.*

Lemma 13.14 (Gaußsches Lemma)**.** *Sind $f, g \in R[x]$ primitiv, so auch $f \cdot g$.*

Beweis. Es genügt zu zeigen, dass kein $p \in \mathbb{P}_R$ ein Teiler von $c(f \cdot g)$ ist. Das ist gleichbedeutend mit $p \nmid (f \cdot g)$. Wir betrachten den Homomorphismus

$$\varphi\colon R[x] \to (R/(p))\,[x],\ \sum_{i=0}^{n} a_i x^i \mapsto \sum_{i=0}^{n} (a_i + (p))\, x^i.$$

Da f und g primitiv sind, sind $\varphi(f)$ und $\varphi(g)$ ungleich Null. Also ist auch

$$\varphi(f \cdot g) = \varphi(f) \cdot \varphi(g) \neq 0,$$

weil $(R/(p))\,[x]$ ein Integritätsbereich ist. Dies bedeutet aber $p \nmid (f \cdot g)$. □

Wir erinnern an die Bezeichnung $K = \mathrm{Quot}(R)$.

Definition 13.15. *Es sei $f \in K[x]$. Wir wählen ein $a \in R$, welches ein Produkt von Elementen aus $\mathbb{P}_R$ ist, so dass $a \cdot f \in R[x]$. (Man könnte a als einen gemeinsamen Nenner der Koeffizienten von f bezeichnen.) Dann ist*

$$c(f) := \frac{c(a \cdot f)}{a}$$

der **Inhalt** *von f.*

Die folgende Proposition garantiert unter anderem die Unabhängigkeit der obigen Definition von der Auswahl von a.

Proposition 13.16. *Es sei $f \in K[x]$.*

(a) Die Definition von $c(f)$ hängt nicht von der Wahl von a ab.
(b) Genau dann gilt $f \in R[x]$, wenn $c(f) \in R$.
(c) Falls $f \neq 0$, so ist

$$p(f) := \frac{f}{c(f)} \in R[x]$$

primitiv.
(d) Ist $g \in K[x]$ ein weiteres Polynom, so gilt

$$c(f \cdot g) = c(f) \cdot c(g).$$

Beweis. (a) Es sei $b \in R$ eine alternative Wahl für a. Dann gilt

$$a \cdot c(bf) = c(abf) = b \cdot c(af),$$

also
$$\frac{c(bf)}{b} = \frac{c(af)}{a},$$
was zu zeigen war.

(b) Falls $f \in R[x]$, kann man $a = 1$ wählen, also $c(f) \in R$. Ist umgekehrt $c(f) \in R$, so ist a ein Teiler von $c(a \cdot f)$. Also teilt a alle Koeffizienten von af und damit af selbst. Es folgt $f = \frac{af}{a} \in R[x]$.

(c) Aus
$$p(f) = \frac{f \cdot a}{c(af)}$$
folgt $p(f) \in R[x]$ primitiv.

(d) Wir können schreiben
$$f = c(f) \cdot p(f) \quad \text{und} \quad g = c(g) \cdot p(g),$$
also $fg = c(f)c(g) \cdot p(f)p(g)$ und
$$c(fg) = c(f)c(g) \cdot c\left(p(f)p(g)\right).$$
Da wegen (c) und Lemma 13.14 das Produkt $p(f)p(g)$ primitiv ist, folgt die Behauptung. □

Falls $a \in R$ ein irreduzibles Element ist, bleibt es im Allgemeinen nicht irreduzibel, wenn man es als Element eines größeren Rings betrachtet. Hieraus ergibt sich die Brisanz des folgenden Satzes.

Satz 13.17. *Ein primitives Polynom $f \in R[x]$ ist genau dann irreduzibel als Element von $K[x]$, wenn es als Element von $R[x]$ irreduzibel ist.*

Beweis. Zunächst sei f als Element von $K[x]$ irreduzibel. Dann ist f jedenfalls nicht konstant. Zum Nachweis der Irreduzibilität in $R[x]$ sei $f = g \cdot h$ mit $g, h \in R[x]$. Nach Voraussetzung liegt g oder h in $K[x]^\times = K^\times$, wir können also $h = a \in K$ annehmen, wegen $h \in R[x]$ also $a \in R$. Mit Proposition 13.16(d) erhalten wir
$$1 = c(f) = c(g) \cdot c(h) \sim a \cdot c(g),$$
also $a \in R^\times$, und es folgt $h \in R[x]^\times$. Damit ist f irreduzibel in $R[x]$.

Nun sei umgekehrt f irreduzibel in $R[x]$. Dann ist f nicht konstant, denn sonst läge es wegen der Primitivität in $R^\times$. Es sei $f = g \cdot h$ mit $g, h \in K[x]$. Wegen $c(g) \cdot c(h) = c(f) = 1$ folgt
$$p(g) \cdot p(h) = g \cdot h = f.$$
Weil die primitiven Teile in $R[x]$ liegen, folgt aus der Voraussetzung $p(g) \in R[x]^\times$ oder $p(h) \in R[x]^\times$. Also ist g oder h konstant, was zu zeigen war. □

Beispiel 13.18. Das Polynom $f = x^3 - x - 1 \in \mathbb{Z}[x]$ ist irreduzibel, denn sonst gäbe es einen Teiler von der Form $ax - b$ mit $a, b \in \mathbb{Z}$, und dann müssten a und b Einheiten sein. Aber $f(\pm 1) \neq 0$. Aus Satz 13.17 folgt, dass f auch in $\mathbb{Q}[x]$ irreduzibel ist. ◁

Wir können nun den angekündigten Satz beweisen, dass mit R auch $R[x]$ faktoriell ist.

Satz 13.19. *Ist R ein faktorieller Ring, so ist auch $R[x]$ faktoriell.*

Beweis. Wir zeigen zunächst, dass $R[x]$ die Eigenschaft F1 erfüllt. Nach Voraussetzung ist jedes konstante Polynom $\neq 0$ Produkt von Primelementen aus R. Für $f \in R[x] \setminus R$ gilt

$$c(f) = p_1 \cdots p_r$$

mit $p_i \in \mathbb{P}_R$ (wobei $r = 0$, falls $c(f) = 1$). Wegen Korollar 13.11(b) haben wir außerdem eine Zerlegung

$$p(f) = f_1 \cdots f_s$$

mit $f_i \in K[x]$ irreduzibel. Mit Proposition 13.16(d) erhalten wir $p(f) = p(f_1) \cdots p(f_s)$, also können wir voraussetzen, dass die f_i in $R[x]$ liegen und primitiv sind. Wegen Satz 13.17 sind die f_i auch in $R[x]$ irreduzibel. Insgesamt liefert

$$f = p_1 \cdots p_r \cdot f_1 \cdots f_s$$

eine Zerlegung als Produkt von irreduziblen Elementen.

Es bleibt zu zeigen, dass jedes irreduzible Polynom $f \in R[x]$ ein Primelement ist. Es gelte also $f \mid (gh)$ mit $g, h \in R[x]$. Wir betrachten zunächst den Fall, dass f konstant ist und machen das durch die Umbenennung $f =: p \in R$ sichtbar. Aus $p \mid (gh)$ folgt $p \mid c(gh) = c(g)c(h)$. Da R faktoriell ist, teilt p einen der beiden Inhalte, etwa $p \mid c(g)$. Hieraus folgt aber $p \mid g$.

Nun betrachten wir den verbleibenden Fall, dass f nicht konstant ist. Aus der Faktorisierung $f = c(f)p(f)$ folgt wegen der Irreduzibilität $c(f) = 1$. Weil $K[x]$ faktoriell ist, ist f ein Teiler von g oder h *in* $K[x]$, etwa $f \mid g$. Wir erhalten $g/f \in K[x]$. Wegen

$$c(g/f) = c(g)/c(f) = c(g) \in R$$

liefert Proposition 13.16(b), dass g/f in $R[x]$ liegt, also ist f auch in $R[X]$ ein Teiler von g. Damit ist gezeigt, dass f in beiden Fällen ein Primelement ist. □

Korollar 13.20. *(a) Der Polynomring $\mathbb{Z}[x]$ ist faktoriell.*

(b) Für einen Körper K ist der multivariate Polynomring $K[x_1, \ldots, x_n]$ faktoriell.

Wir haben uns folgende Hierarchie von Eigenschaften eines kommutativen Rings R erarbeitet:

$$R \text{ Körper} \implies R \text{ euklidisch} \implies R \text{ Hauptidealring}$$
$$\implies R \text{ faktoriell} \implies R \text{ Integritätsbereich.}$$

Zum Abschluss dieses Abschnittes besprechen wir das *Verfahren von Kronecker* zur Faktorisierung von Polynomen. Gegeben sei ein Polynom $f \in R[x]$ über einem Ring R von positivem Grad. Wir setzen voraus, dass R faktoriell ist und $|R^\times|$ endlich. Dies ist erfüllt für $R = \mathbb{Z}$ oder für Polynomringe über $\mathbb{Z}$. Wegen Satz 13.17 ist das Verfahren auch auf Polynome über $\mathrm{Quot}(R)$, also beispielsweise über $\mathbb{Q}$, anwendbar. Gesucht ist ein Polynom $g \in R[x]$ mit $g \mid f$ und $\deg(g) \le \lfloor \frac{1}{2} \deg(f) \rfloor =: s$.

Falls R endlich ist, gibt es höchstens $|R|^{s+1}$ Polynome vom Grad $\le s$, die man alle durchprobieren kann. Wir können also voraussetzen, dass R unendlich ist.

Wir wählen paarweise verschiedene „Stützstellen" $a_0, \dots, a_s \in R$. Falls g ein Teiler von f ist, so sind die $g(a_i)$ auch Teiler von $f(a_i)$. Außerdem ist g durch die Werte $g(a_i)$ nach Satz 11.9 eindeutig bestimmt. Wegen $|R^\times| < \infty$ sind die Mengen

$$T_i := \{b \in R \mid b \text{ teilt } f(a_i)\} \quad (i = 0, \dots, s)$$

endlich. Für jedes $(b_0, \dots, b_s) \in T_0 \times \cdots \times T_s$ können wir also nach Satz 11.9 das Interpolationspolynom $g_{b_0,\dots,b_s} \in K[x]$ mit $g_i(a_i) = b_i$ und $\deg(g) \le s$ bilden (wobei $K = \mathrm{Quot}(R)$). Dann testen wir, ob die Koeffizienten von $g_{b_0,\dots,b_s}$ in R liegen, ob $g_{b_0,\dots,b_s}$ eine Einheit oder Null ist, und schließlich, ob es ein Teiler von f ist.

Falls nach Durchlaufen von $T_0 \times \cdots \times T_s$ kein Teiler von f gefunden ist, ist die Irreduzibilität von f nachgewiesen.

Beispiel 13.21. Wir betrachten $f = x^5 + x^4 + 1 \in \mathbb{Z}[x]$ und wählen Stützstellen $-1, 0, 1$. Die Werte von f sind $1, 1, 3$, also

$$T_0 = T_1 = \{1, -1\} \quad \text{und} \quad T_2 = \{1, -1, 3, -3\}.$$

Allgemein hat das Interpolationspolynom die Form

$$g_{b_0,b_1,b_2} = \frac{b_0}{2}(x^2 - x) - b_1(x^2 - 1) + \frac{b_2}{2}(x^2 + x)$$

Wir können immer $b_0 = 1$ wählen, da wir andernfalls g durch $-g$ ersetzen können.

Für $(b_0, b_1, b_2) = (1, 1, 1)$ ergibt sich $g = 1$, eine Einheit. Für $(b_0, b_1, b_2) = (1, 1, -1)$ ergibt sich $g = -x^2 - x + 1$, welches kein Teiler von f ist. Für $(b_0, b_1, b_2) = (1, 1, 3)$ ergibt sich $g = x^2 + x + 1$. Der Test auf Teilbarkeit liefert

$$f = (x^2 + x + 1)(x^3 - x + 1),$$

womit eine Faktorisierung von f gefunden ist. ◁

14 Resultante und Diskriminante

In diesem Abschnitt ist K ein Körper.

Das folgende Lemma (und danach auch der Satz 14.3) geben Kriterien, wann zwei Polynome $f, g \in K[x]$ teilerfremd sind.

Lemma 14.1. *Zwei Polynome $f, g \in K[x] \setminus \{0\}$ sind genau dann* nicht *teilerfremd, wenn es $s, t \in K[x] \setminus \{0\}$ gibt mit $s \cdot f + t \cdot g = 0$ und $\deg(s) < \deg(g)$, $\deg(t) < \deg(f)$.*

Beweis. Wir schreiben $h = \mathrm{ggT}(f, g)$. Im Falle $h \neq 1$ wird die Bedingung durch $s := g/h$ und $t = -f/h$ erfüllt.

Umgekehrt seien $h = 1$ und $s, t \in K[x] \setminus \{0\}$ mit $s \cdot f + t \cdot g = 0$. Dann ist f ein Teiler von $t \cdot g$ und damit auch von t. Es folgt $\deg(t) \geq \deg(f)$. □

Wir können Lemma 14.1 auch folgendermaßen formulieren: Für $k \in \mathbb{N}_0$ betrachten wir den k-dimensionalen Vektorraum

$$P_k := \{h \in K[x] \mid \deg(h) < k\},$$

und mit $n := \deg(f)$, $m := \deg(g)$ bilden wir

$$\varphi_{f,g} \colon P_m \oplus P_n \to P_{n+m}, \ (s, t) \mapsto s \cdot f + t \cdot g.$$

Dann sagt Lemma 14.1:

$$\mathrm{ggT}(f, g) = 1 \quad \Longleftrightarrow \quad \varphi_{f,g} \text{ ist injektiv.} \tag{14.1}$$

Um eine Darstellungsmatrix von $\varphi_{f,g}$ zu bekommen, schreiben wir $f = \sum_{i=0}^{n} a_i x^i$, $g = \sum_{i=0}^{m} b_i x^i$ und wählen für P_k die (geordnete) Basis $x^{k-1}, x^{k-2}, \ldots, x, 1$. Dann lautet die gesuchte Darstellungsmatrix

$$S(f,g) = \begin{pmatrix} a_n & 0 & \cdots & 0 & b_m & & 0 \\ a_{n-1} & a_n & \ddots & \vdots & b_{m-1} & \ddots & \\ \vdots & a_{n-1} & \ddots & 0 & \vdots & \ddots & b_m \\ a_0 & \vdots & \ddots & a_n & b_1 & & b_{m-1} \\ 0 & a_0 & & a_{n-1} & b_0 & \ddots & \vdots \\ \vdots & \ddots & \ddots & \vdots & & \ddots & b_1 \\ 0 & \cdots & 0 & a_0 & 0 & & b_0 \end{pmatrix} \in K^{(n+m)\times(n+m)},$$

wobei der (linke) Block mit den a_i-Koeffizienten m Spalten umfasst und der (rechte) mit den b_i-Koeffizienten n Spalten. Man nennt $S(f, g)$ die *Sylvester-Matrix* von f und g.

Definition 14.2. *Es seien R ein kommutativer Ring und $f, g \in R[x] \setminus \{0\}$. Dann heißt*

$$\operatorname{res}(f, g) := \det\left(S(f, g)\right) \in R$$

die **Resultante** *von f und g. Falls $f \in R$ konstant ist, ergibt sich also $\operatorname{res}(f, g) = f^{\deg(g)}$ und entsprechend für g konstant. Weiter setzen wir $\operatorname{res}(f, 0) = \operatorname{res}(0, g) := 0$.*

Aus (14.1) ergibt sich:

Satz 14.3. *Zwei Polynome $f, g \in K[x]$ sind genau dann teilerfremd, wenn $\operatorname{res}(f, g) \neq 0$.*

Quantitativ gilt der folgende Satz:

Satz 14.4 (Produktdarstellung der Resultante)**.** *Es seien $f, g \in K[x]$ mit $f = \prod_{i=1}^{n}(x - \alpha_i)$, $\alpha_i \in K$. Dann gilt*

$$\operatorname{res}(f, g) = \prod_{i=1}^{n} g(\alpha_i).$$

Beweis. Da der Satz für g konstant direkt aus Definition 14.2 folgt, können wir voraussetzen, dass g nicht konstant ist. Wir bilden den rationalen Funktionenkörper $\widetilde{K} := K(A_1, \ldots, A_n, y)$ in $n+1$ Unbestimmten und setzen

$$\widetilde{f} := \prod_{i=1}^{n}(x - A_i) \in \widetilde{K}[x] \quad \text{und} \quad h := \operatorname{res}(\widetilde{f}, g - y) \in \widetilde{K}.$$

Die Resultante h wird gebildet mit der Matrix $S(\widetilde{f}, g - y)$, bei der gegenüber $S(\widetilde{f}, g)$ jeder Eintrag b_0 durch $b_0 - y$ ersetzt wird. Hieraus sehen wir, dass h ein Polynom (mit Koeffizienten in $K(A_1, \ldots, A_n)$) in der Unbestimmten y vom Grad n mit höchstem Koeffizienten $(-1)^n$ ist; letzteres weil $\widetilde{f}$ den höchsten Koeffizienten $a_n = 1$ hat. Weil für jedes $i \in \{1, \ldots, n\}$ die Polynome $\widetilde{f}$ und $g - g(A_i)$ die gemeinsame Nullstelle A_i haben, folgt aus Satz 14.3:

$$h\left(g(A_i)\right) = \operatorname{res}\left(\widetilde{f}, g - g(A_i)\right) = 0.$$

Weil g nicht konstant ist, sind die $g(A_i)$ paarweise verschieden. Weil h den Grad n und höchsten Koeffizienten $(-1)^n$ hat, erhalten wir

$$h = (-1)^n \prod_{i=1}^{n}\left(y - g(A_i)\right),$$

also

$$\operatorname{res}(\widetilde{f}, g) = h(0) = \prod_{i=1}^{n} g(A_i). \tag{14.2}$$

Auf beiden Seiten der Gleichung stehen Polynome in $K[A_1, \dots, A_n]$. Nun betrachten wir den Homomorphismus

$$\varphi\colon K[A_1, \dots, A_n, x] \to K[x],\ p \mapsto p(\alpha_1, \dots, \alpha_n, x).$$

und erhalten

$$\operatorname{res}(f, g) = \operatorname{res}\left(\varphi(\widetilde{f}), g\right) = \varphi\left(\operatorname{res}(\widetilde{f}, g)\right) \underset{(14.2)}{=} \varphi\left(\prod_{i=1}^{n} g(A_i)\right) = \prod_{i=1}^{n} g(\alpha_i).$$

□

Korollar 14.5. *Für* $f = \prod_{i=1}^{n}(x - \alpha_i)$ *und* $g = \prod_{j=1}^{m}(x - \beta_j) \in K[x]$ *gilt*

$$\operatorname{res}(f, g) = \prod_{i=1}^{n} \prod_{j=1}^{m} (\alpha_i - \beta_j).$$

Definition 14.6. *Es seien* R *ein kommutativer Ring und* $f = \sum_{i=0}^{n} a_i x^i \in R[x]$ *ein Polynom.*

(a) Die (formale) **Ableitung** *von* f *ist*

$$f' := \sum_{i=1}^{n} i \cdot a_i x^{i-1} \in R[x].$$

In dieser Formel ist i *zu interpretieren als* $\varphi_0(i)$ *mit* φ_0 *aus Proposition 10.9.*

(b) Falls $a_n \neq 0$, *heißt*

$$D(f) := (-1)^{\frac{n(n-1)}{2}} \operatorname{res}(f, f')$$

die **Diskriminante** *von* f.

Beispiel 14.7. Für $f = x^2 + ax + b \in R[x]$ (wobei wir $\operatorname{char}(R) \neq 2$ voraussetzen) gilt $f' = 2x + a$, also

$$D(f) = -\det \begin{pmatrix} 1 & 2 & 0 \\ a & a & 2 \\ b & 0 & a \end{pmatrix} = a^2 - 4b.$$

◁

Proposition 14.8. *Für zwei Polynome* $f, g \in R[x]$ *über einem kommutativen Ring gelten:*

(a) $(f + g)' = f' + g'$ *und*
(b) $(f \cdot g)' = f \cdot g' + g \cdot f'$ *(„Leibniz-Regel“).*

Beweis. Der Teil (a) ist klar. Für den Nachweis von (b) schreiben wir $f = \sum_{i=0}^{n} a_i x^i$ und $g = \sum_{j=0}^{n} b_j x^j$ mit $n \geq \max\{\deg(f), \deg(g)\}$. Es gelten

$$(f \cdot g)' = \sum_{i,j=0}^{n} (i+j) a_i b_j x^{i+j-1}$$

und andererseits

$$f \cdot g' = \sum_{i,j=0}^{n} j a_i b_j x^{i+j-1} \quad \text{und} \quad g \cdot f' = \sum_{i,j=0}^{n} i a_i b_j x^{i+j-1}.$$

Hieraus ergibt sich (b). □

Satz 14.9. *Es sei* $f = \prod_{i=1}^{n} (x - \alpha_i) \in K[x]$. *Dann gilt*

$$D(f) = \prod_{1 \leq i < j \leq n} (\alpha_i - \alpha_j)^2.$$

Insbesondere hat f *genau dann mehrfache Nullstellen, wenn* $D(f) = 0$.

Beweis. Durch mehrfache Anwendung von Proposition 14.8(b) ergibt sich

$$f' = \sum_{i=1}^{n} \prod_{j \in \{1,\dots,n\} \setminus \{i\}} (x - \alpha_j),$$

nach Satz 14.4 also

$$D(f) = (-1)^{\frac{n(n-1)}{2}} \prod_{i=1}^{n} f'(\alpha_i) = (-1)^{\frac{n(n-1)}{2}} \prod_{i \neq j} (\alpha_i - \alpha_j) = \prod_{1 \leq i < j \leq n} (\alpha_i - \alpha_j)^2.$$

□

Beispiel 14.10. Ein quadratisches Polynom $f = x^2 + ax + b$ hat also genau dann eine doppelte Nullstelle, wenn $a^2 - 4b = 0$ gilt. Sind α, β die Nullstellen, so gilt $(\alpha - \beta)^2 = a^2 - 4b$. Außerdem sieht man direkt die Beziehung $\alpha + \beta = -a$. Es ergibt sich die bekannte Formel

$$\{\alpha, \beta\} = \left\{ \frac{-a \pm \sqrt{a^2 - 4b}}{2} \right\}.$$

◁

15 Der Chinesische Restsatz

In diesem Abschnitt beschäftigen wir uns mit sogenannten *Kongruenzsystemen* wie $x \equiv 2 \mod 6$, $x \equiv -1 \mod 5$ oder $x \equiv 2 \mod 6$, $x \equiv -1 \mod 4$. Die Lösbarkeit aller solcher Systeme (mit $\mod 5$ und $\mod 6$) ist gleichbedeutend mit der Surjektivität der Abbildung

$$\mathbb{Z} \to \mathbb{Z}/(6) \times \mathbb{Z}/(5),\ x \mapsto (x + (6), x + (5)) .$$

Es ist praktisch, die Zielmenge dieser Abbildung mit einer Ringstruktur zu versehen.

Definition 15.1. *Es seien $R_1, \dots, R_n$ Ringe. Das kartesische Produkt $S := R_1 \times \cdots \times R_n$ wird mit komponentenweiser Addition und Multiplikation, also*

$$(a_1, \dots, a_n) \stackrel{+}{\cdot} (b_1, \dots, b_n) := \left(a_1 \stackrel{+}{\cdot} b_1, \dots, a_n \stackrel{+}{\cdot} b_n\right),$$

zu einem Ring. S heißt die **direkte Summe** *von $R_1, \dots, R_n$ und wird mit $R_1 \oplus \cdots \oplus R_n$ bezeichnet.*

Das Einselement der direkten Summe ist $(1_{R_1}, \dots, 1_{R_n})$. Es ist klar, dass für die Einheitengruppe gilt:

$$(R_1 \oplus \cdots \oplus R_n)^\times = R_1^\times \times \cdots \times R_n^\times$$

(direktes Produkt der Einheitengruppen). Sind R ein kommutativer Ring und $a_1, \dots, a_n \in R$, so erhalten wir einen Homomorphismus

$$\varphi\colon R \to R/(a_1) \oplus \cdots \oplus R/(a_n),\ r \mapsto (r + (a_1), \dots, r + (a_n)) . \qquad (15.1)$$

Unter gewissen Voraussetzungen werden wir dessen Surjektivität beweisen.

Lemma 15.2. *Es seien R ein Hauptidealring, $a_1, \dots, a_n \in R$ und $d \in R$ ein ggT der a_i (wobei allgemein ein ggT definiert ist als ein gemeinsamer Teiler, der Vielfaches jedes anderen gemeinsamen Teilers ist). Dann gilt*

$$(a_1, \dots, a_n) = (d).$$

Beweis. Da d ein gemeinsamer Teiler ist, folgt

$$I := (a_1, \dots, a_n) \subseteq (d).$$

Nach Voraussetzung gilt $I = (c)$ mit $c \in R$, c ist also ein gemeinsamer Teiler der a_i. Es folgt $c \mid d$, also

$$(d) \subseteq (c) = I.$$

Insgesamt folgt $I = (d)$, wie behauptet. □

Falls also $a_1, \dots, a_n \in R$ teilerfremde Elemente in einem Hauptidealring sind (d.h. 1 ist ein ggT der a_i), so gibt es $e_1, \dots, e_n \in R$ mit

$$e_1 a_1 + \cdots + e_n a_n = 1. \tag{15.2}$$

Wie folgendes Beispiel zeigt, gilt dies im Allgemeinen in faktoriellen Ringen nicht.

Beispiel 15.3. Im Polynomring $R = K[x, y]$ über einem Körper sind x und y teilerfremd, aber es gibt keine $e_1, e_2 \in R$ mit $e_1 x + e_2 y = 1$. ◁

Satz 15.4 (Chinesischer Restsatz)**.** *Es seien R ein Hauptidealring und $a_1, \dots, a_n \in R$ paarweise teilerfremd (d.h. für $i \neq j$ sei 1 ein ggT von a_i und a_j). Dann ist der in (15.1) definierte Homomorphismus φ surjektiv. Mit $a := a_1 \cdots a_n$ gilt*

$$\mathrm{Kern}(\varphi) = (a).$$

Beweis. Die $b_i := a/a_i$ $(i = 1, \dots, n)$ sind teilerfremd, denn für jedes Primelement p, das sämtliche b_i teilt, gibt es ein j mit $p \mid a_j$, aber dann folgt nach Voraussetzung $p \nmid b_j$. Wegen Lemma 15.2 gibt es also $e_1, \dots, e_n \in R$ mit $\sum_{i=1}^n e_i b_i = 1$. Es folgt

$$e_i b_i = 1 - \sum_{j \in \{1,\dots,n\} \setminus \{i\}} e_j b_j \equiv 1 \mod a_i \quad \text{und} \quad e_i b_i \equiv 0 \mod a_j \quad \text{für } j \neq i.$$

Es sei nun $(r_1 + (a_1), \dots, r_n + (a_n)) \in R/(a_1) \oplus \cdots \oplus R/(a_n)$ beliebig. Mit

$$r := r_1 e_1 b_1 + \cdots + r_n e_n b_n$$

gilt dann $\varphi(r) = (r_1 + (a_1), \dots, r_n + (a_n))$. Also ist φ surjektiv.

Aus $\varphi(r) = 0$ für $r \in R$ folgt $a_i \mid r$ für alle i, also $a \mid r$ wegen der Teilerfremdheit der a_i. Da umgekehrt a im Kern von φ liegt, folgt $\mathrm{Kern}(\varphi) = (a)$. □

Korollar 15.5. *Mit den Voraussetzungen und der Notation von Satz 15.4 gilt*

$$R/(a) \cong R/(a_1) \oplus \cdots \oplus R/(a_n).$$

Es folgt also auch

$$(R/(a))^\times \cong (R/(a_1))^\times \times \cdots \times (R/(a_n))^\times. \tag{15.3}$$

Der Beweis zu Satz 15.4 liefert eine Methode, wie man Lösungen von Kongruenzgleichungssystemen bestimmen kann. Wir demonstrieren dies an einem Beispiel

Beispiel 15.6. Es seien $R = \mathbb{Z}$, $a_1 = 4$, $a_2 = 5$ und $a_3 = 7$. Mit der Notation des Beweises ist also $b_1 = 35$, $b_2 = 28$ und $b_3 = 20$. Wir benötigen nun $e_1, e_2, e_3 \in \mathbb{Z}$ mit $e_1 b_1 + e_2 b_2 + e_3 b_3 = 1$. Wir beginnen, indem wir 1 als

Linearkombination von a_1 und a_2 schreiben, was ganz einfach ist: $1 = 5 - 4$. Es folgt

$$7 = 35 - 28 = b_1 - b_2.$$

Wenn wir nun 1 als Linearkombination von 7 und $b_3 = 20$ schreiben können, haben wir unser Ziel erreicht. Division mit Rest ergibt

$$20 = 3 \cdot 7 - 1,$$

also

$$1 = 3 \cdot 7 - 20 = 3(b_1 - b_2) - b_3 = 3b_1 - 3b_2 - b_3 = 105 - 84 - 20.$$

Mit dieser „Zerlegung der Eins“ kann man nun Kongruenzsysteme lösen. Für $x_1, x_2, x_3 \in \mathbb{Z}$ liefert nämlich

$$x = 105x_1 - 84x_2 - 20x_3$$

eine Lösung von

$$x \equiv x_1 \mod 4, \quad x \equiv x_2 \mod 5, \quad x \equiv x_3 \mod 7.$$

Mit etwas Glück ging die Rechnung hier ziemlich schnell. Im Allgemeinen muss man mehrere Divisionen mit Rest durchführen, was auf den *Euklidischen Algorithmus* führt. $\triangleleft$

Wir schließen den Abschnitt mit der Einführung der sogenannten Eulerschen φ-Funktion ab.

Definition 15.7. *Die* **Eulersche φ-Funktion** *ist definiert als*

$$\varphi\colon \mathbb{N}_{>0} \to \mathbb{N},\ n \mapsto \left|\left(\mathbb{Z}/(n)\right)^\times\right|.$$

Beispiel 15.8. $\varphi(1) = 1$, $\varphi(2) = 1$, $\varphi(3) = 2$, $\varphi(4) = 2$, $\varphi(5) = 4$, $\varphi(6) = 2$, ... $\triangleleft$

Wir entwickeln nun eine Formel, mit der man $\varphi(n)$ berechnen kann, sofern eine Primzerlegung von n bekannt ist.

Proposition 15.9. *Für $n \in \mathbb{N}_{>0}$ gilt:*

$$\varphi(n) = \left|\left\{i \in \mathbb{N} \mid 1 \le i \le n,\ \mathrm{ggT}(i,n) = 1\right\}\right|.$$

Beweis. Die Proposition folgt aus folgender Behauptung: Für $i \in \mathbb{N}$ mit $1 \le i \le n$ gilt die Äquivalenz

$$\bar{i} \in \left(\mathbb{Z}/(n)\right)^\times \quad \Longleftrightarrow \quad \mathrm{ggT}(i,n) = 1.$$

Zum Nachweis der Äquivalenz nehmen wir zunächst $\overline{i} \in \left(\mathbb{Z}/(n)\right)^{\times}$ an, es gibt also $j \in \mathbb{Z}$ mit $\overline{i} \cdot \overline{j} = \overline{1}$. Dies bedeutet $ij + xn = 1$ mit $x \in \mathbb{Z}$, also teilt jeder gemeinsame Teiler von i und n auch 1, und es folgt $\mathrm{ggT}(i, n) = 1$.

Umgekehrt setzen wir $\mathrm{ggT}(i, n) = 1$ voraus. Wegen (15.2) folgt $xi + yn = 1$ mit $x, y \in \mathbb{Z}$, also $\overline{i} \cdot \overline{x} = \overline{1} \in \mathbb{Z}/(n)$. Dies bedeutet $\overline{i} \in \left(\mathbb{Z}/(n)\right)^{\times}$. □

Für eine Primzahl und $e \in \mathbb{N}_{>0}$ gilt also:

$$\varphi(p^e) = (p - 1)p^{e-1}.$$

Hieraus und aus (15.3) folgt die angekündigte Formel zum Berechnen der φ-Funktion.

Satz 15.10. *Es sei $n = \prod_{i=1}^{r} p_i^{e_i}$, wobei die p_i paarweise verschiedene Primzahlen und die $e_i \in \mathbb{N}_{>0}$ sind. Dann gilt*

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

Körper

16 Körpererweiterungen

Definition 16.1. *Es sei L ein Körper. Eine Teilmenge $K \subseteq L$ heißt ein* **Teilkörper** *(gleichbedeutend:* **Unterkörper***), falls K ein Unterring von L und außerdem ein Körper ist. L heißt dann eine* **Körpererweiterung** *von K. Wir bezeichnen Körpererweiterungen mit $K \leq L$ oder L/K und sagen auch, dass L über K liegt.*

Beispiel 16.2. $\mathbb{Q} \leq \operatorname{Quot}\left(\mathbb{Z}[\sqrt{5}]\right) \leq \mathbb{R} \leq \mathbb{C} \leq \mathbb{C}(x)$ (rationaler Funktionenkörper über $\mathbb{C}$). ◁

Proposition 16.3. *Es seien L/K eine Körpererweiterung und $\mathcal{M}$ eine nichtleere Menge von Zwischenkörpern (d.h. $K \leq M \leq L$ für alle $M \in \mathcal{M}$). Dann ist auch der Schnitt*

$$\bigcap_{M \in \mathcal{M}} M$$

eine Körpererweiterung von K.

Beweis. Dies ist offensichtlich. □

Hiermit können wir die von einer Teilmenge erzeugte Körpererweiterung definieren.

Definition 16.4. *Es seien L/K eine Körpererweiterung und $S \subseteq L$ eine Teilmenge. Dann heißt*

$$K(S) := \bigcap_{\substack{K \leq M \leq L \\ \text{mit } S \subseteq M}} M$$

die von S **erzeugte Körpererweiterung** *von K. Falls $S = \{\alpha_1, \ldots, \alpha_n\}$ endlich ist, schreiben wir auch $K(S) = K(\alpha_1, \ldots, \alpha_n)$. L/K heißt* **endlich erzeugt***, falls $L = K(S)$ mit $S \subseteq L$ endlich.*

Es stellt sich die Frage, wie man die von einer Menge S erzeugte Körpererweiterung explizit beschreiben kann. Wir beantworten dies für S endlich.

Proposition 16.5 (endlich erzeugte Körpererweiterungen)**.** *Es seien L/K eine Körpererweiterung und $\alpha_1, \ldots, \alpha_n \in L$. Dann gilt*

$$K(\alpha_1, \ldots, \alpha_n) = \left\{ \frac{f(\alpha_1, \ldots, \alpha_n)}{g(\alpha_1, \ldots, \alpha_n)} \,\middle|\, f, g \in K[x_1, \ldots, x_n],\ g(\alpha_1, \ldots, \alpha_n) \neq 0 \right\},$$

wobei $K[x_1, \ldots, x_n]$ für den Polynomring in n Unbestimmten steht.

Beweis. Wir schreiben L' für die rechte Seite der obigen Gleichung und $\mathcal{M} := \{M \mid K \leq M \leq L,\ \alpha_1, \ldots, \alpha_n \in M\}$. Es ist klar, dass $L' \in \mathcal{M}$. Es sei andererseits $M \in \mathcal{M}$. Dann folgt $L' \subseteq M$. Insgesamt erhalten wir $L' = \bigcap_{M \in \mathcal{M}} M$, was zu zeigen war. □

Beispiel 16.6. (1) $\mathbb{C} = \mathbb{R}(i)$.

(2) Es seien K ein Körper und $L = \operatorname{Quot}(K[x])$ der rationale Funktionenkörper. Dann ist $L = K(x)$ die von x erzeugte Körpererweiterung.

◁

Definition 16.7. *Es sei L/K eine Körpererweiterung.*

(a) Ein Element $\alpha \in L$ heißt **algebraisch** *über K, falls es ein Polynom $f \in K[x] \setminus \{0\}$ gibt mit $f(\alpha) = 0$. Andernfalls heißt α* **transzendent** *über K.*

(b) Die Körpererweiterung L/K heißt **algebraisch***, falls alle $\alpha \in L$ algebraisch über K sind. Andernfalls heißt L/K transzendent.*

Beispiel 16.8. (1) Über $\mathbb{Q}$ ist $\sqrt{2} \in \mathbb{R}$ als Nullstelle von $x^2 - 2$ algebraisch.

(2) $\mathbb{C}/\mathbb{R}$ ist algebraisch, denn ein $z \in \mathbb{C}$ ist Nullstelle von

$$x^2 - 2\operatorname{Re}(z) \cdot x + |z|^2 \in \mathbb{R}[x].$$

(3) Jedes $\alpha \in K$ ist algebraisch über K, denn es ist Nullstelle von $x - \alpha \in K[x]$.

(4) Im rationalen Funktionenkörper $K(x)$ ist das Element x transzendent über K, und ebenso jede nicht-konstante rationale Funktion.

(5) $\mathbb{R}$ ist transzendent über $\mathbb{Q}$. Falls man über hinreichende Kenntnisse in Kardinalzahlarithmetik verfügt, kann man dies aus der Überabzählbarkeit von $\mathbb{R}$ folgern. Schwieriger ist es zu zeigen, dass spezielle reelle Zahlen, beispielsweise π und e, transzendent über $\mathbb{Q}$ sind. ◁

Der folgende Satz beschreibt sogenannte *einfache Körpererweiterungen*, d.h. Körpererweiterungen vom Typ $K(\alpha)$.

Satz 16.9 (einfache Körpererweiterungen)**.** *Es seien L/K eine Körpererweiterung und $\alpha \in L$.*

(a) Falls α transzendent über K ist, so gilt $K(\alpha) \cong K(x)$ (der rationale Funktionenkörper).

(b) *Falls α algebraisch über K ist, gibt es genau ein normiertes Polynom $g \in K[x]$ von minimalem Grad mit $g(\alpha) = 0$. Außerdem ist g irreduzibel, und die Abbildung*

$$K[x]/(g) \to K(\alpha),\ f + (g) \mapsto f(\alpha)$$

ist ein Isomorphismus.

Beweis. Wir betrachten den Homomorphismus

$$\varphi\colon K[x] \to L,\ f \mapsto f(\alpha).$$

Genau dann ist α transzendent über K, wenn φ injektiv ist. Falls dies erfüllt ist, lässt sich φ fortsetzen zu

$$\varphi'\colon K(x) \to L,\ f/g \mapsto f(\alpha)/g(\alpha).$$

Auch φ' ist injektiv, und wegen Proposition 16.5 gilt $\text{Bild}(\varphi') = K(\alpha)$. Es folgt also (a).

Nun sei α algebraisch über K. Die Menge aller $g \in K[x]$ mit $g(\alpha) = 0$ ist nichts anderes als $\text{Kern}(\varphi)$. Weil $K[x]$ ein Hauptidealring ist, wird das Ideal $\text{Kern}(\varphi) \neq \{0\}$ von einem eindeutig bestimmten normierten Element minimalen Grades erzeugt, also $\text{Kern}(\varphi) = (g)$. Hieraus folgt die Eindeutigkeit von g. Wegen des Homomorphiesatzes folgt die Wohldefiniertheit und Injektivität der Abbildung $K[x]/(g) \to L,\ f + (g) \mapsto f(\alpha)$. Somit gilt

$$K[x]/(g) \cong \text{Bild}(\varphi) \subseteq L,$$

also ist $K[x]/(g)$ ein Integritätsbereich. Es folgt die Irreduzibilität von g. Da $K[x]$ ein Hauptidealring ist, folgt hieraus, dass (g) ein maximales Ideal ist, also ist $\text{Bild}(\varphi) \leq L$ ein Teilkörper. Wegen $\alpha \in \text{Bild}(\varphi)$ folgt $K(\alpha) \subseteq \text{Bild}(\varphi)$. Andererseits ist $\text{Bild}(\varphi) = \{f(\alpha) \mid f \in K[x]\}$ wegen Proposition 16.5 in $K(\alpha)$ enthalten, also

$$K(\alpha) = \text{Bild}(\varphi) \cong K[x]/(g).$$

Dies schließt den Beweis ab. □

Definition 16.10. *Das Polynom g aus Satz 16.9(b) heißt das* **Minimalpolynom** *von α über K. Es wird mit $g =: \text{irr}(\alpha, K)$ bezeichnet.*

Falls L/K eine Körpererweiterung ist, ist L ein K-Vektorraum (mit Addition und Multiplikation gegeben durch die Körperstruktur von L), denn die Vektorraum-Axiome sind erfüllt. Diese Beobachtung motiviert die folgende Definition.

Definition 16.11. *Es sei L/K eine Körpererweiterung. Dann heißt*

$$[L : K] := \dim_K(L) \in \mathbb{N} \cup \{\infty\}$$

der **Grad** *der Körpererweiterung. Die Körpererweiterung heißt* **endlich**, *falls* $[L : K] < \infty$.

Beispiel 16.12. (1) $[\mathbb{C} : \mathbb{R}] = 2$.
(2) Für jeden Körper K gilt: $[K : K] = 1$.
(3) Für den rationalen Funktionenkörper $K(x)$ gilt: $[K(x) : K] = \infty$. ◁

Proposition 16.13 (Grad einer einfachen Körpererweiterung)**.** *Es seien L/K eine Körpererweiterung und $\alpha \in L$ algebraisch über K. Mit $g := \operatorname{irr}(\alpha, K)$ und $n := \deg(g)$ gilt dann*

$$[K(\alpha) : K] = n,$$

und die Elemente $1 = \alpha^0, \alpha, \ldots, \alpha^{n-1}$ bilden eine Basis von $K(\alpha)$ als K-Vektorraum.

Beweis. Wegen des Isomorphismus von Satz 16.9(b) ist zu zeigen, dass die Elemente $1 + (g), x + (g), \ldots, x^{n-1} + (g)$ eine Basis von $K[x]/(g)$ als K-Vektorraum bilden.

Zum Nachweis der linearen Unabhängigkeit sei also $\sum_{i=0}^{n-1} a_i(x^i + (g)) = 0 + (g)$. Dann ist g ein Teiler von $f := \sum_{i=0}^{n-1} a_i x^i$, und wegen $\deg(g) = n$ folgt $f = 0$, also $a_0 = \ldots = a_{n-1} = 0$.

Zum Nachweis der Erzeugereigenschaft sei $f \in K[x]$ beliebig. Division mit Rest liefert

$$f = qg + r$$

mit $q, r \in K[x]$, $\deg(r) < n$, also $r = \sum_{i=0}^{n-1} a_i x^i$ mit $a_i \in K$. Es folgt

$$f + (g) = \sum_{i=0}^{n-1} a_i(x^i + (g)).$$

Dies schließt den Beweis ab. □

Proposition 16.14 (Multiplikativität des Grades)**.** *Es seien L/K und M/L Körpererweiterungen. Dann gilt*

$$[M : K] = [M : L] \cdot [L : K].$$

Insbesondere ist M/K genau dann endlich, wenn M/L und L/K endlich sind.

Beweis. Falls $[L : K] = \infty$, so ist auch M unendlich-dimensional als K-Vektorraum, also $[M : K] = \infty$. Falls $[M : L] = \infty$, so hat M kein endliches Erzeugendensystem als L-Vektorraum, also auch nicht als K-Vektorraum, und es folgt $[M : K] = \infty$.

Es bleibt der Fall zu behandeln, dass M/L und L/K endlich sind. Mit $m := [M : L]$ gibt es eine L-lineare, bijektive Abbildung $M \to L^m$. Da diese auch K-linear ist, ist M als K-Vektorraum isomorph zur direkten Summe

$L \oplus \cdots \oplus L$ von m Exemplaren von L. Mit $n := [L : K]$ gilt $L \cong K^n$, also $M \cong K^{mn}$ (Isomorphien als K-Vektorräume). Es folgt $[M : K] = mn$. □

Der folgende Satz charakterisiert endliche Körpererweiterungen und enthält außerdem die Aussage, dass algebraisch erzeugte Körpererweiterungen algebraisch sind.

Satz 16.15 (endliche und endlich erzeugte Körpererweiterungen)**.** *Für eine Körpererweiterung L/K sind folgende Aussagen äquivalent:*

(a) L/K ist endlich.
(b) L/K ist endlich erzeugt und algebraisch.
(c) Es gibt algebraische Elemente $\alpha_1, \ldots, \alpha_m \in L$ mit $L = K(\alpha_1, \ldots, \alpha_m)$.

Beweis. Wir setzen zunächst (a) voraus und zeigen, dass hieraus (b) folgt. Da jedes Erzeugendensystem von L als K-Vektorraum auch ein Erzeugendensystem als Körpererweiterung ist, folgt, dass L/K endlich erzeugt ist. Es sei nun $\alpha \in L$. Mit $n := [L : K]$ sind dann $1, \alpha, \ldots, \alpha^n$ linear abhängig. Dies liefert $f \in K[x] \setminus \{0\}$ mit $f(\alpha) = 0$. Also ist L/K algebraisch.

Es ist klar, dass die Bedingung (c) aus (b) folgt.

Nun setzen wir (c) voraus und beweisen (a) durch Induktion nach m. Mit $L' := K(\alpha_1, \ldots, \alpha_{m-1})$ gilt $L = L'(\alpha_m)$. Das Element α_m ist algebraisch über K, also auch über L', Proposition 16.13 liefert also

$$[L : L'] < \infty.$$

Da nach Induktion auch $[L' : K] < \infty$ gilt, folgt $[L : K] < \infty$ wegen Proposition 16.14. □

Korollar 16.16. *Es seien L/K eine Körpererweiterung und $\alpha, \beta \in L$ algebraisch. Dann sind auch $\alpha + \beta$, $\alpha - \beta$, $\alpha \cdot \beta$ und α/β (falls $\beta \neq 0$) algebraisch.*

Beweis. Dies folgt durch Anwendung von Satz 16.15 auf $L' := K(\alpha, \beta)$. □

Korollar 16.17 (Türme von algebraischen Erweiterungen)**.** *Es seien L/K und M/L Körpererweiterungen. Genau dann ist M/K algebraisch, wenn L/K und M/L algebraisch sind.*

Beweis. Falls M/K algebraisch ist, ist klar, dass dies auch für L/K und M/L gilt.

Umgekehrt seien L/K und M/L algebraisch, und es sei $\alpha \in M$ beliebig. Dann gibt es $g = \sum_{i=0}^{n} c_i x^i \in L[x] \setminus \{0\}$ mit $g(\alpha) = 0$. Also ist α algebraisch über $L' := K(c_0, \ldots, c_n) \leq L$. Die Körpererweiterung L'/K ist algebraisch und endlich erzeugt, nach Satz 16.15 also endlich. Aus den Propositionen 16.13 und 16.14 folgt, dass $L'(\alpha)/K$ endlich ist. Wegen Satz 16.15 ist $L'(\alpha)/K$ also auch algebraisch. Damit ist gezeigt, dass α algebraisch über K ist. □

17 Transzendenzbasen

In diesem Abschnitt werden wir die Darstellung sehr knapp halten und die Beweise weglassen. Die Ergebnisse werden in keinem anderen Teil der Vorlesung verwendet.

Definition 17.1. *Es sei L/K eine Körpererweiterung.*

(a) Elemente $\alpha_1, \ldots, \alpha_n \in L$ heißen **algebraisch unabhängig***, falls für jedes multivariate Polynom $f \in K[x_1, \ldots, x_n] \setminus \{0\}$ gilt: $f(\alpha_1, \ldots, \alpha_n) \neq 0$. Eine Teilmenge $S \subseteq L$ heißt* **algebraisch unabhängig***, falls jede endliche Teilmenge von S algebraisch unabhängig ist.*
(b) Die Erweiterung L/K heißt **rein transzendent***, falls $L = K(S)$ mit $S \subseteq L$ algebraisch unabhängig. Falls $S = \{\alpha_1, \ldots, \alpha_n\}$ endlich ist, bedeutet dies, dass L isomorph ist zum rationalen Funktionenkörper $K(x_1, \ldots, x_n)$ in n Unbestimmten.*
(c) Eine Teilmenge $B \subseteq L$ heißt eine **Transzendenzbasis** *von L/K, falls B algebraisch unabhängig ist und $L/K(B)$ algebraisch ist.*

Man beachte die Analogie von (a) und (c) mit den Begriffen *linear unabhängig* und *Basis* aus der linearen Algebra.

Beispiel 17.2. (1) Es sei $L = K(x_1, \ldots, x_n)$ der rationale Funktionenkörper in n Unbestimmten. Dann ist jede Teilmenge von $\{x_1, \ldots, x_n\}$ algebraisch unabhängig, ebenso jede Teilmenge von $\{x_1^2, \ldots, x_n^2\}$. Aber $\{x_1, x_2, x_1^2 x_2\}$ ist algebraisch abhängig.
(2) Falls L/K algebraisch ist, so ist $\emptyset$ eine Transzendenzbasis.
(3) Für den rationalen Funktionenkörper $L = K(x)$ ist $\{x\}$ eine Transzendenzbasis und ebenso $\{x^2\}$. ◁

Auch der folgende Satz steht in starker Analogie zu Sätzen aus der linearen Algebra.

Satz 17.3 (Existenz von Transzendenzbasen)**.** *Es sei L/K eine Körpererweiterung.*

(a) Ist $S \subseteq L$ eine algebraisch unabhängige Teilmenge (beispielsweise $S = \emptyset$), so gibt es eine Transzendenzbasis $B \subseteq L$ mit $S \subseteq B$.
(b) Falls L/K eine endliche Transzendenzbasis hat, so sind alle Transzendenzbasen endlich und haben gleich viele Elemente.

Wie angekündigt lassen wir den Beweis weg. Aus Teil (a) folgt, dass jede endlich erzeugte Körpererweiterung isomorph ist zu einer algebraischen Erweiterung eines rationalen Funktionenkörpers. Der Teil (b) gibt Anlass zu folgender Definition:

Definition 17.4. *Der* **Transzendenzgrad** *einer Körpererweiterung L/K ist die Elementanzahl einer Transzendenzbasis. Er wird mit $\mathrm{trdeg}(L/K)$ bezeichnet und ist eine Zahl aus $\mathbb{N}_0$ oder ∞.*

Beispiel 17.5. (1) Für den rationalen Funktionenkörper $K(x_1, \dots, x_n)$ gilt: $\operatorname{trdeg}(K(x_1, \dots, x_n)/K) = n$.
(2) Eine Körpererweiterung L/K ist genau dann algebraisch, wenn $\operatorname{trdeg}(L/K) = 0$ gilt.
(3) Der Transzendenzgrad von $\mathbb{R}/\mathbb{Q}$ ist unendlich. Falls man über hinreichende Kenntnisse in Kardinalzahlarithmetik vefügt, kann man dies aus der Überabzählbarkeit von $\mathbb{R}$ folgern. $\triangleleft$

18 Zerfällungskörper

In diesem Abschnitt werden wir uns mit der Frage beschäftigen, ob ein gegebenes (nicht-konstantes) Polynom $f \in K[x]$ in einem geeigneten Erweiterungskörper von K eine Nullstelle hat, oder sogar in Linearfaktoren zerfällt.

Satz 18.1 (Körpererweiterungen mit Nullstellen)**.** *Es sei $f \in K[x]$ ein nicht-konstantes Polynom über einem Körper. Dann gibt es eine Körpererweiterung L/K, so dass f in L eine Nullstelle hat.*

Beweis. Es sei $g \in K[x]$ ein irreduzibler Faktor von f. Weil $K[x]$ ein Hauptidealring ist, folgt, dass $(g) \trianglelefteq K[x]$ ein maximales Ideal ist, also ist $L := K[x]/(g)$ ein Körper. Via der Abbildung $K \to L,\ a \mapsto a + (g)$ können wir K also als Teilkörper von L auffassen. Für $\alpha := x + (g) \in L$ gilt $g(\alpha) = 0$, also auch $f(\alpha) = 0$. $\square$

Die folgende Eindeutigkeitsaussage benötigen wir in einer recht allgemeinen (und damit etwas umständlichen) Form.

Proposition 18.2 (Fortsetzung von Automorphismen)**.** *Es seien $f \in K[x]$ ein irreduzibles Polynom über einem Körper K, L/K eine Körpererweiterung und $\alpha \in L$ eine Nullstelle von f. Außerdem seien K' ein Körper, $\varphi\colon K \to K'$ ein Isomorphismus, L'/K' eine Körpererweiterung und $\alpha' \in L'$ eine Nullstelle des Polynoms $\varphi(f) \in K'[x]$, das durch Anwenden von φ auf die Koeffizienten von f entsteht. Dann gibt es einen Isomorphismus*

$$\psi\colon K(\alpha) \to K'(\alpha')$$

mit $\psi|_K = \varphi$ und $\psi(\alpha) = \alpha'$.

Beweis. Es sei $g \in K[x]$ das Minimalpolynom von α. Aus $f(\alpha) = 0$ folgt $g \mid f$, also nach Voraussetzung $f \sim g$. Es ist klar, dass $\varphi(f)$ auch irreduzibel ist, also ist $g' := \varphi(g)$ das Minimalpolynom von α'. Durch

$$K[x]/(g) \to K'[x]/(g'),\ h + (g) \mapsto \varphi(h) + (g')$$

wird ein Isomorphismus gegeben, der φ fortsetzt. Wenn man ihn mit den Isomorphismen $K(\alpha) \to K[x]/(g)$ und $K'[x]/(g') \to K'(\alpha')$ aus Satz 16.9(b) verbindet, erhält man den gewünschten Isomorphismus $K(\alpha) \to K'(\alpha')$. □

Der Spezialfall $K = K'$ und $\varphi = \mathrm{id}_K$ liefert, dass für zwei Körpererweiterungen L/K und L'/K mit Nullstellen $\alpha \in L$ und $\alpha' \in L'$ von f die Erweiterungen $K(\alpha)$ und $K(\alpha')$ im Sinne der folgenden Definition isomorph sind.

Definition 18.3. *Es seien L_1/K und L_2/K zwei Körpererweiterungen. Ein* K**-Homomorphismus** *ist ein Ringhomomorphismus $\varphi\colon L_1 \to L_2$ mit $\varphi|_K = \mathrm{id}_K$ (d.h. $\varphi(a) = a$ für alle $a \in K$). Falls φ zusätzlich bijektiv ist, so heißt φ ein* K**-Isomorphismus**, *und gilt zudem noch $L_1 = L_2$, so heißt φ ein* K**-Automorphismus**. *Falls es einen K-Isomorphismus $L_1 \to L_2$ gibt, so heißen die Körpererweiterungen* **isomorph**.

Beispiel 18.4. Das Polynom $f = x^4 - 2 \in \mathbb{Q}[x]$ ist irreduzibel, wie man beispielsweise mit dem Eisenstein-Kriterium sieht. In $\mathbb{C}$ haben wir die Nullstellen $\pm\sqrt[4]{2}$ und $\pm i \cdot \sqrt[4]{2}$. Gemäß Proposition 18.2 (angewandt auf $\varphi = \mathrm{id}_{\mathbb{Q}}$) sind $\mathbb{Q}(\sqrt[4]{2})/\mathbb{Q}$ und $\mathbb{Q}(i\sqrt[4]{2})/\mathbb{Q}$ isomorph. ◁

Definition 18.5. *Es seien $f \in K[x]$ ein Polynom über einem Körper K mit $f \neq 0$ und L/K eine Körpererweiterung. L heißt ein* **Zerfällungskörper** *von f (über K), falls es $\alpha_1, \ldots, \alpha_n, c \in L$ gibt, so dass*

$$f = c \cdot \prod_{i=1}^{n} (x - \alpha_i)$$

und außerdem

$$L = K(\alpha_1, \ldots, \alpha_n).$$

Satz 18.6 (Existenz und Eindeutigkeit von Zerfällungskörpern)**.** *Es sei $f \in K[x] \setminus \{0\}$ ein Polynom über einem Körper K. Dann gelten:*

(a) Es gibt einen Zerfällungskörper von f über K.
(b) Zwei Zerfällungskörper von f über K sind (als Körpererweiterungen von K) isomorph.

Beweis. (a) Wir benutzen Induktion nach $\deg(f) =: n$. Für $n = 0$ ist K ein Zerfällungskörper. Ist $n > 0$, so hat f nach Satz 18.1 eine Nullstelle α_1 in einer Körpererweiterung von K. Wir setzen $K' := K(\alpha_1)$. Dann gelten

$$g := \frac{f}{x - \alpha_1} \in K'[x]$$

und $\deg(g) = n - 1$. Nach Induktion hat g also einen Zerfällungskörper $L = K'(\alpha_2, \ldots, \alpha_n)$ über K'. Es folgt $f = c \cdot \prod_{i=1}^{n}(x - \alpha_i)$ mit $c \in L$ und $L = K'(\alpha_2, \ldots, \alpha_n) = K(\alpha_1, \ldots, \alpha_n)$, also ist L ein Zerfällungskörper von f über K.

(b) Es seien L_1 und L_2 zwei Zerfällungskörper von f. Weiter sei L'/K eine Körpererweiterung maximalen Grades mit $L' \leq L_1$, so dass ein K-Homomorphismus $\varphi\colon L' \to L_2$ existiert. (Da L_1/K wegen Satz 16.15 endlich ist, haben alle Zwischenkörper höchstens den Grad $[L_1 : K]$, daher existiert so ein L'.) Es sei $\alpha \in L_1$ eine Nullstelle von f. Das Minimalpolynom $g := \operatorname{irr}(\alpha, L')$ von α über L' teilt f, also teilt $\varphi(g)$ auch $\varphi(f) = f$. Da L_2 ein Zerfällungskörper von f ist, folgt, dass L_2 eine Nullstelle von $\varphi(g)$ enthält. Nun liefert Proposition 18.2 eine Fortsetzung

$$\psi\colon L'(\alpha) \to L_2$$

von φ. Aus der Maximalität von $[L' : K]$ folgt $L'(\alpha) = L'$, also $\alpha \in L'$. Wir haben gezeigt, dass L' alle Nullstellen von f in L_1 enthält. Da L_1 ein Zerfällungskörper von f ist, folgt $L' = L_1$. Also gibt es einen K-Homomorphismus $\varphi\colon L_1 \to L_2$. Aus $f = c \cdot \prod_{i=1}^n (x - \alpha_i)$ mit $c, \alpha_i \in L_1$ folgt

$$\varphi(c) \cdot \prod_{i=1}^n (x - \varphi(\alpha_i)) = \varphi(f) = f,$$

also sind die $\varphi(\alpha_i)$ die Nullstellen von f in L_2. Da sie alle im Bild von φ liegen, und da sie L_2 erzeugen, folgt die Surjektivität von φ. Also ist φ ein K-Isomorphismus. □

Den Teil (b) des Satzes hätten wir auch in derselben Allgemeinheit wie Proposition 18.2 formulieren und beweisen können.

Beispiel 18.7. Wir betrachten das Polynom $f = x^4 - 2$ über $K = \mathbb{Q}$. Über $\mathbb{C}$ zerfällt f in Linearfaktoren:

$$f = \left(x - \sqrt[4]{2}\right)\left(x + \sqrt[4]{2}\right)\left(x - i\sqrt[4]{2}\right)\left(x + i\sqrt[4]{2}\right).$$

Ein Zerfällungskörper ist also

$$L := \mathbb{Q}\left(\sqrt[4]{2}, i\sqrt[4]{2}\right) = \mathbb{Q}\left(\sqrt[4]{2}, i\right) \subseteq \mathbb{C}.$$

Wir können auch den Grad von L bestimmen:

$$[L : \mathbb{Q}] = \left[L : \mathbb{Q}\left(\sqrt[4]{2}\right)\right] \cdot \left[\mathbb{Q}\left(\sqrt[4]{2}\right) : \mathbb{Q}\right] = 2 \cdot 4 = 8.$$

Im Allgemeinen ist es keine einfache Aufgabe, den Grad eines Zerfällungskörpers zu bestimmen. ◁

Wir sind nun so weit, dass wir die wichtige und interessante Frage beantworten können, welche endlichen Körper es gibt.

Satz 18.8 (endliche Körper)**.** *(a) Zu jeder Primzahlpotenz $q := p^n$ (mit p einer Primzahl und $n \in \mathbb{N}_{>0}$) gibt es einen Körper mit q Elementen.*

(b) Es sei K ein endlicher Körper. Dann gilt $|K| = p^n$ mit p einer Primzahl und $n \in \mathbb{N}_{>0}$, und K ist ein Zerfällungskörper des Polynoms $x^{p^n} - x$ über $\mathbb{F}_p$.

Beweis. Wir beginnen mit (b). Wegen Proposition 10.12 ist $\operatorname{char}(K)$ eine Primzahl p, denn $\operatorname{char}(K) = 0$ würde der Endlichkeit von K widersprechen. Es folgt $\mathbb{F}_p \subseteq K$, K ist also eine Erweiterung von $\mathbb{F}_p$. Wegen $|K| < \infty$ ist $n := [K : \mathbb{F}_p] < \infty$. Es folgt $|K| = |\mathbb{F}_p^n| = p^n =: q$. Die Einheitengruppe $K^\times$ hat die Ordnung $q-1$, Korollar 1.13 liefert also $a^{q-1} = 1$ für alle $a \in K \setminus \{0\}$. Alle $a \in K$ sind also Nullstellen des Polynoms $f := x^q - x \in \mathbb{F}_p[x]$. Es folgt, dass K ein Zerfällungskörper von f über $\mathbb{F}_p$ ist.

Nun zeigen wir (a). Wegen Satz 18.6(a) gibt es einen Zerfällungskörper L von $f := x^q - x \in \mathbb{F}_p[x]$ über $\mathbb{F}_p$. Wir setzen

$$K := \{a \in L \mid a^q = a\} \subseteq L.$$

Es ist klar, dass 0 und 1 in K liegen, und dass mit $a, b \in K$ auch das Produkt $a \cdot b$ und (falls $a \neq 0$) a^{-1} in K liegen. Wegen Satz 10.13 gilt auch $a + b \in K$. Somit ist K ein Körper. Die Diskriminante von f ist

$$D(f) = (-1)^{\frac{q(q-1)}{2}} \operatorname{res}(f, -1) \neq 0,$$

also hat f nach Satz 14.9 keine mehrfachen Nullstellen. Hieraus folgt $|K| = q$, also ist K ein Körper mit q Elementen. □

Mit Satz 18.6(b) folgt, dass es für jede Primzahlpotenz einen bis auf Isomorphie eindeutig bestimmten Körper mit q Elementen gibt. Wir bezeichnen diesen Körper mit $\mathbb{F}_q$. In diesem Zusammenhang sei an Korollar 11.7 erinnert, nach dem $\mathbb{F}_q^\times$ zyklisch von der Ordnung $q-1$ ist. Um Missverständnissen vorzubeugen, sei betont, dass es sich bei dem Körper $\mathbb{F}_q$ *nicht* um den Restklassenring $\mathbb{Z}/(q)$ handelt, es sei denn, q ist eine Primzahl.

19 Algebraischer Abschluss

Definition 19.1. *Es sei K ein Körper.*

(a) K heißt **algebraisch abgeschlossen***, falls jedes nicht-konstante Polynom $f \in K[x]$ eine Nullstelle in K hat.*
(b) Eine algebraische Körpererweiterung $\overline{K}/K$ heißt ein **algebraischer Abschluss** *von K, falls $\overline{K}$ algebraisch abgeschlossen ist.*

Es ist klar, dass jedes nicht-konstante Polynom über einem algebraisch abgeschlossenen Körper in Linearfaktoren zerfällt. Wegen Satz 18.1 ist ein Körper genau dann algebraisch abgeschlossen, wenn er keine echte algebraische Körpererweiterung hat.

Beispiel 19.2. Es ist bekannt, dass $\mathbb{C}$ algebraisch abgeschlossen ist. Wir werden den Nachweis in Abschnitt 24 führen. $\mathbb{C}$ ist ein algebraischer Abschluss von $\mathbb{R}$. Es folgt auch, dass

$$\overline{\mathbb{Q}} := \{z \in \mathbb{C} \mid z \text{ ist algebraisch über } \mathbb{Q}\}$$

ein algebraischer Abschluss von $\mathbb{Q}$ ist. ◁

Satz 19.3. *Jeder Körper besitzt einen algebraischen Abschluss.*

Beweis. Wir bilden das kartesische Produkt

$$\Omega := (K[x] \setminus \{0\}) \times \mathbb{N}_{>0}$$

und die injektive Abbildung

$$\varphi\colon K \to \Omega,\ c \mapsto (x - c, 1).$$

Wir schreiben $K_0 := \operatorname{Bild}(\varphi)$ und definieren die Abbildungen

$$+_0, \cdot_0\colon K_0 \times K_0 \to K_0,\ (\varphi(a), \varphi(b)) \mapsto \varphi(a + b) \text{ bzw. } \varphi(a \cdot b),$$

wodurch K_0 ein zu K isomorpher Körper wird. Nun betrachten wir die Menge $\mathcal{M}$ aller Tripel $(L, +, \cdot)$ mit:

(1) $L \subseteq \Omega$ und $+, \cdot\colon L \times L \to L$.
(2) Zusammen mit $+$ und $\cdot$ ist L ein Körper.
(3) $K_0 \subseteq L$, $+|_{K_0 \times K_0} = +_0$ und $\cdot|_{K_0 \times K_0} = \cdot_0$ (d.h. K_0 ist Unterkörper von L).
(4) Jedes $\alpha = (f, i) \in L$ ist eine Nullstelle des Polynoms $\varphi(f) \in K_0[x]$, das aus f durch Anwendung von φ auf die Koeffizienten entsteht.

Es ist leicht zu sehen, dass $(K_0, +_0, \cdot_0) \in \mathcal{M}$ gilt. $\mathcal{M}$ ist durch die Teilkörperrelation angeordnet. Um das Zornsche Lemma anwenden zu können, betrachten wir eine Kette $\emptyset \neq \mathcal{K} \subseteq \mathcal{M}$. Die Additionen und Multiplikationen der $(L, +, \cdot) \in \mathcal{K}$ haben gemeinsame Fortsetzungen auf die Vereinigung

$$N := \bigcup_{(L,+,\cdot) \in \mathcal{K}} L,$$

und es ist klar, dass N zusammen mit diesen Fortsetzungen ein Element von $\mathcal{M}$ bildet. $\mathcal{K}$ hat also eine obere Schranke in $\mathcal{M}$, und somit ist das Zornsche Lemma anwendbar. Dies liefert ein maximales Element $(\overline{K}, +, \cdot)$ von $\mathcal{M}$. Wegen (4) ist $\overline{K}/K_0$ algebraisch. Es sei $L/\overline{K}$ eine algebraische Erweiterung. Es ist zu zeigen, dass $L = \overline{K}$ gilt. Wir konstruieren eine injektive Abbildung $\psi\colon L \to \Omega$ wie folgt: Für ein normiertes, irreduzibles Polynom $f \in K[x]$ seien $\alpha_1, \ldots, \alpha_r \in L$ die Nullstellen von $\varphi(f)$ in L, und zwar so angeordnet, dass $\alpha_1, \ldots, \alpha_s \in L \setminus \overline{K}$ und $\alpha_{s+1}, \ldots, \alpha_r \in \overline{K}$. (Hierbei sind $r = 0$ oder $s = 0$

möglich.) Weiter seien $n_1, \dots, n_s \in \mathbb{N}_{>0}$ die minimalen (verschiedenen) Zahlen mit $(f, n_i) \notin \overline{K}$. (Man beachte, dass es wegen (4) für jedes $f \in K[x]$ höchstens endlich viele $i \in \mathbb{N}$ gibt mit $(f, i) \in \overline{K}$.) Für $i = 1, \dots, s$ definieren wir $\psi(\alpha_i) = (f, n_i)$, und für $i = s+1, \dots, r$ setzen wir $\psi(\alpha_i) = \alpha_i$. Da jedes über K_0 algebraische Element von L genau ein Minimalpolynom hat, ist ψ eine injektive Abbildung von der Menge der über K_0 algebraischen Elemente von L in Ω. Wegen Korollar 16.17 ist ψ also auf ganz L definiert. Außerdem gilt nach Konstruktion $\psi|_{\overline{K}} = \mathrm{id}_{\overline{K}}$. Indem wir die Addition und die Multiplikation von L mittels ψ auf $\psi(L)$ übertragen, erhalten wir $(\psi(L), +, \cdot) \in \mathcal{M}$ mit $\overline{K}$ als Unterkörper. Wegen der Maximalität von $(\overline{K}, +, \cdot)$ folgt $\psi(L) = \overline{K}$, also $L = \overline{K}$. Dies schließt den Beweis ab. □

Der folgende Satz zeigt, dass sich jede algebraische Erweiterung von K in einen gegebenen algebraischen Abschluss einbetten lässt.

Satz 19.4 (Einbettungen in einen algebraischen Abschluss)**.** *Es seien K ein Körper, $\overline{K}$ ein algebraischer Abschluss, L/K eine algebraische Körpererweiterung, L_1 ein Zwischenkörper (d.h. $K \le L_1 \le L$) und $\varphi_1\colon L_1 \to \overline{K}$ ein Homomorphismus. Dann gibt es einen Homomorphismus $\varphi\colon L \to \overline{K}$ mit $\varphi|_{L_1} = \varphi_1$.*

Beweis. Wir betrachten die Menge

$$\mathcal{M} := \left\{(L', \psi) \mid L_1 \le L' \le L,\ \psi\colon L' \to \overline{K} \text{ Homomorphismus},\ \psi|_{L_1} = \varphi_1\right\}.$$

Es gilt $(L_1, \varphi_1) \in \mathcal{M}$. Wir definieren auf $\mathcal{M}$ eine Ordnungsrelation durch

$$(L', \psi) \le (L'', \eta) \quad \Longleftrightarrow \quad L' \le L'' \quad \text{und} \quad \eta|_{L'} = \psi.$$

Ist $\emptyset \ne \mathcal{K} \subseteq \mathcal{M}$ eine Kette, so ist $N := \bigcup_{(L', \psi) \in \mathcal{K}} L'$ ein Zwischenkörper, und die Abbildungen ψ mit $(L', \psi) \in \mathcal{K}$ haben eine gemeinsame Fortsetzung η auf N. Wir erhalten also (N, η) als obere Schranke von $\mathcal{K}$ in $\mathcal{M}$. Somit liefert das Zornsche Lemma ein maximales Element $(L', \varphi) \in \mathcal{M}$. Der Beweis ist abgeschlossen, wenn wir $L' = L$ zeigen können.

Es sei $\alpha \in L$ beliebig und $f := \mathrm{irr}(\alpha, L')$. Da $\overline{K}$ algebraisch abgeschlossen ist, enthält es eine Nullstelle β von $\varphi(f)$. Nach Proposition 18.2 gibt es einen Homomorphismus $\Phi\colon L'(\alpha) \to \overline{K}$ mit $\Phi|_{L'} = \varphi$, also $(L'(\alpha), \Phi) \in \mathcal{M}$. Aus der Maximalität von (L', φ) folgt $L'(\alpha) = L'$, also $\alpha \in L'$. Wir erhalten $L' = L$, wie behauptet. □

Nun erhalten wir auch eine Eindeutigkeitsaussage für algebraische Abschlüsse.

Korollar 19.5 (Eindeutigkeit des algebraischen Abschlusses)**.** *Es seien K ein Körper und $\overline{K}$ und $\widetilde{K}$ zwei algebraische Abschlüsse. Dann gilt $\overline{K} \cong \widetilde{K}$ (K-Isomorphie).*

Beweis. Satz 19.4 (angewandt auf den Spezialfall $L_1 = K$ und $\varphi_1 = \mathrm{id}$) liefert einen K-Homomorphismus $\varphi\colon \overline{K} \to \widetilde{K}$. Jeder Homomorphismus von Körpern ist injektiv, also auch φ. $\widetilde{K}$ is algebraisch über K, also auch über $\varphi(\overline{K})$. Da $\varphi(\overline{K}) \cong \overline{K}$ algebraisch abgeschlossen ist, folgt $\widetilde{K} = \varphi(\overline{K})$. Also ist φ auch surjektiv. □

Korollar 19.5 rechtfertigt es, immer die Schreibweise $\overline{K}$ für einen algebraischen Abschluss eines Körpers K zu benutzen und bisweilen von *dem* algebraischen Abschluss zu sprechen.

20 Normale und separable Körpererweiterungen

Definition 20.1. *Eine algebraische Körpererweiterung L/K heißt* **normal***, falls für jedes $\alpha \in L$ das Minimalpolynom $f = \mathrm{irr}(\alpha, K)$ über L in Linearfaktoren zerfällt, d.h. alle Nullstellen von f in L liegen.*

Beispiel 20.2. (1) $\mathbb{Q}\left(\sqrt[4]{2}\right)/\mathbb{Q}$ ist nicht normal, denn für das Minimalpolynom $x^4 - 2$ „fehlen“ die Nullstellen $\pm i\sqrt[4]{2}$.
(2) Für jeden Körper K sind K/K und $\overline{K}/K$ normal. ◁

Satz 20.3 (Charakterisierung von Normalität)**.** *Für eine endliche Körpererweiterung L/K sind folgende Aussagen äquivalent:*

(a) L/K ist normal.
(b) L ist Zerfällungskörper eines Polynoms $f \in K[x]$ über K.
(c) Sind $\varphi_1, \varphi_2\colon L \to \overline{K}$ zwei K-Homomorphismen in einen algebraischen Abschluss von K, so gilt $\mathrm{Bild}(\varphi_1) = \mathrm{Bild}(\varphi_2)$.

Beweis. Wir setzen zunächst (a) voraus und zeigen (b). Nach Satz 16.15 gibt es algebraische Elemente $\alpha_1, \ldots, \alpha_n \in L$ mit $L = K(\alpha_1, \ldots, \alpha_n)$. Wegen der Normalität von L zerfallen alle $f_i := \mathrm{irr}(\alpha_i, K)$ über L in Linearfaktoren. Also ist L der Zerfällungskörper von $f := \prod_{i=1}^n f_i$.

Nun setzen wir (b) voraus. Es gilt also $L = K(\alpha_1, \ldots, \alpha_n)$ mit $f := \prod_{i=1}^n (x - \alpha_i) \in K[x]$. Andererseits gibt es $\beta_1, \ldots, \beta_n \in \overline{K}$ mit $f = \prod_{i=1}^n (x - \beta_i)$. (Man beachte, dass wir hier nicht $L \subseteq \overline{K}$ voraussetzen können. L und $\overline{K}$ haben gewissermaßen nichts miteinander zu tun.) Ist nun $\varphi\colon L \to \overline{K}$ ein K-Homomorphismus, so folgt

$$\prod_{i=1}^n (x - \varphi(\alpha_i)) = \varphi(f) = f = \prod_{i=1}^n (x - \beta_i),$$

also $\{\varphi(\alpha_1), \ldots, \varphi(\alpha_n)\} = \{\beta_1, \ldots, \beta_n\}$. Es folgt

$$\mathrm{Bild}(\varphi) = K\left(\varphi(\alpha_1), \ldots, \varphi(\alpha_n)\right) = K(\beta_1, \ldots, \beta_n),$$

was unabhängig von der Wahl von φ ist. Die Aussage (c) gilt also.

Schließlich setzen wir (c) voraus. Um (a) nachzuweisen, betrachten wir ein beliebiges $\alpha \in L$ und setzen $f := \operatorname{irr}(\alpha, K)$. Wir haben $\beta_1, \ldots, \beta_n \in \overline{K}$ mit $f = \prod_{i=1}^n (x - \beta_i)$. Proposition 18.2 liefert zu jedem i einen K-Homomorphismus $\varphi_i\colon K(\alpha) \to \overline{K}$ mit $\varphi_i(\alpha) = \beta_i$. Satz 19.4 liefert einen Homomorphismus $\psi_i\colon L \to \overline{K}$, der φ_i fortsetzt. Wegen (c) gilt

$$\beta_i = \psi_i(\alpha) \in \operatorname{Bild}(\psi_i) = \operatorname{Bild}(\psi_1),$$

wir haben also $\alpha_i := \psi_1^{-1}(\beta_i) \in L$, und es gilt

$$f = \psi_1^{-1}(f) = \psi_1^{-1}\left(\prod_{i=1}^n (x - \beta_i)\right) = \prod_{i=1}^n \left(x - \psi_1^{-1}(\beta_i)\right) = \prod_{i=1}^n (x - \alpha_i).$$

Damit haben wir gezeigt, dass L/K normal ist. □

Beispiel 20.4. (1) $\mathbb{Q}\left(\sqrt[4]{2}, i\right)/\mathbb{Q}$ ist normal.
(2) $\mathbb{Q}(i)/\mathbb{Q}$ ist normal.
(3) Für p eine Primzahl und q eine p-Potenz ist $\mathbb{F}_q/\mathbb{F}_p$ normal. ◁

Zum Thema Normalität beweisen wir noch die folgende Proposition.

Proposition 20.5. *Es seien L/K und M/L Körpererweiterungen. Falls M/K normal ist, so auch M/L.*

Beweis. Es sei $\alpha \in M$. Dann gilt $f := \operatorname{irr}(\alpha, K) = \prod_{i=1}^n (x - \alpha_i)$ mit $\alpha_i \in M$. Das Minimalpolynom $g := \operatorname{irr}(\alpha, L)$ ist (in $L[x]$) ein Teiler von f, also ist g das Produkt einiger der $(x - \alpha_i)$ und zerfällt damit über M in Linearfaktoren. Dies war zu zeigen. □

Als zweite Eigenschaft, die Körpererweiterungen haben können, behandeln wir in diesem Abschnitt die Separabilität. Wir führen den Begriff zunächst für Polynome ein.

Definition 20.6. *Es sei K ein Körper.*

(a) Ein Polynom $f \in K[x] \setminus \{0\}$ heißt **separabel***, falls es in $\overline{K}$ keine mehrfachen Nullstellen hat.*
(b) K heißt **vollkommen***, falls jedes irreduzible Polynom in $K[x]$ separabel ist.*

Nach Satz 14.9 ist ein nicht-konstantes Polynom genau dann separabel, wenn seine Diskriminante $\neq 0$ ist.

Proposition 20.7 (irreduzible separable Polynome)**.** *Es sei $f \in K[x]$ ein irreduzibles Polynom über einem Körper K.*

(a) Im Falle $\operatorname{char}(K) = 0$ ist f separabel.
(b) Im Falle $\operatorname{char}(K) = p > 0$ gilt folgende Äquivalenz:

$$f \text{ ist nicht separabel} \iff f' = 0 \iff f = g(x^p) \text{ mit } g \in K[x].$$

Beweis. Ist $f' \neq 0$, so folgt wegen der Irreduzibilität von f, dass f und f' teilerfremd sind, also $D(f) \neq 0$ wegen Satz 14.3. Ist umgekehrt $f' = 0$, so folgt $D(f) = 0$. Also ist f genau dann separabel, wenn $f' \neq 0$. Hieraus folgt (a), und wir haben die erste Äquivalenz von (b). Wir schreiben $f = \sum_{i=0}^{n} a_i x^i$, also $f' = \sum_{i=1}^{n} i a_i x^{i-1}$. Im Fall (b) gilt also $f' = 0$ genau dann, wenn $a_i = 0$ für alle i mit $p \nmid i$ gilt. Dies ist gleichbedeutend mit $f = g(x^p)$ mit $g \in K[x]$. □

Beispiel 20.8. Es sei $K = \mathbb{F}_p(t)$ der rationale Funktionenkörper über $\mathbb{F}_p$. Das Polynom $f = x^p - t$ ist nach dem Eisenstein-Kriterium irreduzibel in $\mathbb{F}_p[t,x]$, wegen Satz 13.17 also auch in $K[x]$. Wegen $f' = 0$ ist es aber nicht separabel. Tatsächlich ist $\sqrt[p]{t}$ eine p-fache Nullstelle: $f = (x - \sqrt[p]{t})^p$. Es folgt, dass K nicht vollkommen ist. ◁

Satz 20.9 (vollkommene Körper)**.** *Es sei K ein Körper.*

(a) Falls $\operatorname{char}(K) = 0$, so ist K vollkommen.
(b) Falls K ein endlicher Körper ist, so ist K vollkommen.

Beweis. Der Teil (a) ergibt sich direkt aus Proposition 20.7(a).

Für den Nachweis von (b) sei $f \in K[x]$ ein Polynom, so dass $f = g(x^p)$ mit $g \in K[x]$ gilt. Der Frobenius-Homomorphismus $F\colon K \to K$, $a \mapsto a^p$ ist (als Homomorphismus von Körpern) injektiv, wegen $|K| < \infty$ also auch surjektiv. Daher gibt es ein Polynom $h = \sum_{i=0}^{n} a_i x^i$, so dass $g = \sum_{i=0}^{n} a_i^p x^i$. Es folgt

$$f = \sum_{i=0}^{n} a_i^p x^{pi} = h^p,$$

wobei die letzte Gleichheit aus Satz 10.13 folgt. Also ist f nicht irreduzibel. Aus Proposition 20.7(b) folgt, dass K vollkommen ist. □

Nun kommen wir zu separablen Körpererweiterungen.

Definition 20.10. *Es sei L/K eine algebraische Körpererweiterung.*

(a) Ein Element $\alpha \in L$ heißt **separabel** *(über K), falls das Minimalpolynom $\operatorname{irr}(\alpha, K) \in K[x]$ separabel ist.*
(b) L/K heißt **separabel***, falls alle $\alpha \in L$ über K separabel sind.*

Es ist klar, dass jede algebraische Erweiterung über einem vollkommenen Körper (z.B. einem Körper der Charakteristik 0) separabel ist.

Wir können nun einen wichtigen Satz über separable Körpererweiterungen beweisen.

Satz 20.11 (Satz vom primitiven Element)**.** *Es sei L/K eine endliche Körpererweiterung, die von über K separablen Elementen erzeugt wird. Dann gibt es ein über K separables Element $\gamma \in L$ mit*

$$L = K(\gamma).$$

Anmerkung. Wir werden später sehen, dass eine durch endlich viele separable Elemente erzeugte Körpererweiterung separabel ist (siehe Anmerkung 21.4). Mit diesem Wissen können wir den Satz auch ohne Verlust an Aussagekraft so formulieren: *Jede endliche separable Körpererweiterung wird von einem einzigen Element erzeugt.* Insbesondere gilt dies also für jede endliche Erweiterung eines Körpers der Charakteristik 0. $\triangleleft$

Beweis von Satz 20.11. Wir behandeln zunächst den Fall, das K ein endlicher Körper ist. Dann gilt dies auch für L, also $L \cong \mathbb{F}_q$ mit q einer Primzahlpotenz. Ist $\gamma \in L$ eine Primitivwurzel (d.h. $L^\times = \langle\gamma\rangle$), so folgt $L = K(\gamma)$. Weiter ist γ eine Nullstelle von $f = x^q - x$, also ist $g := \operatorname{irr}(\gamma, K)$ ein Teiler von f. Wegen $D(f) \neq 0$ ist f und damit auch g separabel.

Nachdem dieser Fall abgehandelt ist, können wir $|K| = \infty$ annehmen. Aus der Endlichkeit von L/K folgt, dass L/K durch endlich viele separable Elemente erzeugt wird. Eine Induktion nach deren Anzahl reduziert die Behauptung auf den Fall $L = K(\alpha, \beta)$ mit $\alpha, \beta \in L$ separabel. Wir setzen $f := \operatorname{irr}(\alpha, K)$ und $g := \operatorname{irr}(\beta, K)$. In einem algebraischen Abschluss $\overline{L}$ von L gibt es $\alpha_1, \dots, \alpha_n$ und $\beta_1, \dots, \beta_m$ mit

$$f = \prod_{i=1}^{n}(x - \alpha_i) \quad \text{und} \quad g = \prod_{j=1}^{m}(x - \beta_j),$$

wobei wir $\alpha_1 = \alpha$ und $\beta_1 = \beta$ voraussetzen können. Wegen $|K| = \infty$ existiert $\lambda \in K$, so dass

$$\lambda \notin \left\{ \frac{\alpha_{i'} - \alpha_i}{\beta_{j'} - \beta_j} \mid 1 \le i, i' \le n,\ 1 \le j < j' \le m \right\}. \tag{20.1}$$

(man beachte, dass die β_j ebenso wie die α_i paarweise verschieden sind.) Es folgt, dass die Elemente

$$\gamma_{i,j} := \alpha_i + \lambda\beta_j \in \overline{L} \quad (i = 1, \dots, n,\ j = 1, \dots, m)$$

paarweise verschieden sind. Wir setzen

$$\gamma := \gamma_{1,1} = \alpha + \lambda\beta \in L \quad \text{und} \quad L' := K(\gamma)$$

und behaupten $L' = L$. Der Nachweis ist trickreich. Wir betrachten das Polynom

$$h := f(\gamma - \lambda x) \in L'[x]$$

Für $j \in \{1, \dots, m\}$ gilt

$$h(\beta_j) = f\left(\alpha_1 + \lambda(\beta_1 - \beta_j)\right) = \prod_{i=1}^{n}\left(\alpha_1 - \alpha_i + \lambda(\beta_1 - \beta_j)\right),$$

also $h(\beta_1) = 0$ und $h(\beta_j) \neq 0$ für $j > 1$ wegen (20.1). Die Polynome g und h haben also $\beta_1 = \beta$ als (einzige) gemeinsame Nullstelle. Deshalb sind beide Polynome Vielfache des Minimalpolynoms $s := \operatorname{irr}(\beta, L')$ über L'. Falls der Grad von s größer als 1 wäre, so hätten g und h weitere gemeinsame Nullstellen. Es folgt $s = x - \beta$, wegen $s \in L'[x]$ also $\beta \in L'$. Nun folgt auch $\alpha = \gamma - \lambda\beta \in L'$ und damit $L' = L$, wie behauptet.

Es bleibt zu zeigen, dass γ separabel über K ist. Da die $\gamma_{i,j}$ paarweise verschieden sind genügt es zu zeigen, dass

$$\prod_{i=1}^{n} \prod_{j=1}^{m} (x - \gamma_{i,j}) \in K[x]. \tag{20.2}$$

Auch der Nachweis hierfür ist trickreich. Im bivariaten Polynomring $K[x, y]$ bilden wir

$$\widetilde{f} := (-1)^n f(x - y) \in K[x, y] \quad \text{und} \quad \widetilde{g} := \lambda^m g(\lambda^{-1} y) \in K[y]$$

(Man beachte $\lambda \neq 0$ wegen (20.1)). Es gelten

$$\widetilde{f} = \prod_{i=1}^{n} (y - (x - \alpha_i)) \quad \text{und} \quad \widetilde{g} = \prod_{j=1}^{m} (y - \lambda\beta_j),$$

und nach Korollar 14.5 ergibt sich für die Resultante bezüglich y als Hauptvariablen

$$\operatorname{res}_y\left(\widetilde{f}, \widetilde{g}\right) = \prod_{i=1}^{n} \prod_{j=1}^{m} (x - \alpha_i - \lambda\beta_j) = \prod_{i=1}^{n} \prod_{j=1}^{m} (x - \gamma_{i,j}).$$

Wegen $\operatorname{res}_y(\widetilde{f}, \widetilde{g}) \in K[x]$ folgt (20.2). Damit ist der Beweis vollständig. □

Anmerkung. Aus dem Beweis sieht man, dass man γ als eine (geeignete) K-Linearkombination der gegebenen Erzeuger wählen kann, und dass die „meisten" Linearkombinationen dabei zum Erfolg führen. ◁

Beispiel 20.12. (1) $\mathbb{Q}\left(\sqrt{2}, \sqrt{3}\right) = \mathbb{Q}\left(\sqrt{2} + \sqrt{3}\right)$.

(2) Um einzusehen, dass die Separabilitätsvoraussetzung in Satz 20.11 nicht überflüssig ist, betrachten wir den bivariaten rationalen Funktionenkörper $L := \mathbb{F}_p(x, y)$ als Erweiterung von $K := \mathbb{F}_p(x^p, y^p)$. Es gilt

$$[L : K] = [L : \mathbb{F}_p(x^p, y)] \cdot [\mathbb{F}_p(x^p, y) : K] = p^2.$$

Für jedes $g = g(x, y) \in L$ gilt aber wegen Satz 10.13 und wegen $a^p = a$ für alle $a \in \mathbb{F}_p$:

$$g^p = g(x^p, y^p) \in K,$$

also

$$[K(g) : K] \leq p.$$

Es folgt $K(g) \subsetneqq L$, also wird L nicht durch ein einziges Element erzeugt. $\triangleleft$

21 Galoistheorie

Der Abschnitt über Galoistheorie bildet den Kulminationspunkt der in dieser Vorlesung behandelten Körpertheorie.

Definition 21.1. *Ist L/K eine Körpererweiterung, so heißt*

$$\operatorname{Aut}(L/K) := \{\varphi\colon L \to L \mid \varphi \text{ ist ein } K\text{-Isomorphismus}\}$$

die **Automorphismengruppe** *von L/K. $\operatorname{Aut}(L/K)$ wird mit der Hintereinanderausführung als Produkt zu einer Gruppe.*

Für eine Untergruppe $H \subseteq \operatorname{Aut}(L/K)$ ist

$$L^H := \{\alpha \in L \mid \sigma(\alpha) = \alpha \text{ für alle } \sigma \in H\}$$

der **Fixkörper** *von H. Es ist klar, dass L^H ein Zwischenkörper zwischen K und L ist.*

Beispiel 21.2. Wir betrachten $L = \mathbb{Q}(\sqrt{2})$ als Erweiterung von $K = \mathbb{Q}$. Durch

$$\sigma\colon L \to L,\ a + b\sqrt{2} \mapsto a - b\sqrt{2}$$

(für $a, b \in \mathbb{Q}$) wird ein Automorphismus in $\operatorname{Aut}(L/K)$ gegeben. Für jeden Automorphismus $\varphi \in \operatorname{Aut}(L/K)$ muss gelten: $\varphi(\sqrt{2})^2 = \varphi\left(\sqrt{2}^2\right) = \varphi(2) = 2$, also $\varphi(\sqrt{2}) = \pm\sqrt{2}$. Außerdem ist φ durch das Bild $\varphi(\sqrt{2})$ eindeutig bestimmt. Wir erhalten

$$\operatorname{Aut}(L/K) = \{\sigma, \mathrm{id}_L\} \cong Z_2.$$

Mit $G := \operatorname{Aut}(L/K)$ gilt $L^G = K$.

Ebenso sieht man

$$H := \operatorname{Aut}\left(\mathbb{Q}(\sqrt[4]{2})/\mathbb{Q}\right) = \{\tau, \mathrm{id}\} \cong Z_2$$

mit $\tau(\sqrt[4]{2}) = -\sqrt[4]{2}$, und es gilt $\mathbb{Q}(\sqrt[4]{2})^H = \mathbb{Q}(\sqrt{2})$. $\triangleleft$

Satz 21.3. *Für eine endliche Körpererweiterung L/K sind folgende vier Aussagen äquivalent:*

(a) L/K ist normal und separabel.
(b) L ist der Zerfällungskörper eines separablen Polynoms über K.
(c) $|Aut(L/K)| = [L : K]$.
(d) Es gibt eine endliche Untergruppe $H \subseteq \operatorname{Aut}(L/K)$ mit $K = L^H$.

Falls eine Untergruppe $H \subseteq \mathrm{Aut}(L/K)$ *die Bedingung* (d) *erfüllt, so folgt* $H = \mathrm{Aut}(L/K)$.

Beweis. Wir beginnen mit der Implikation „(d) $\Rightarrow$ (a)“. Wir setzen also die Existenz von $H \subseteq \mathrm{Aut}(L/K)$ mit $L^H = K$ voraus und müssen zeigen, dass für jedes $\alpha \in L$ das Minimalpolynom $g := \mathrm{irr}(\alpha, K)$ separabel ist und über L in Linearfaktoren zerfällt. Wegen $|H| < \infty$ ist die Menge $S := \{\sigma(\alpha) \mid \sigma \in H\} \subseteq L$ endlich. Wir können also

$$f := \prod_{\beta \in S} (x - \beta)$$

bilden. Es gilt $f(\alpha) = 0$ (weil $\mathrm{id}_L \in H$) und $f \in L^H[x] = K[x]$, also ist f ein Vielfaches von g. Da f separabel ist und über L in Linearfaktoren zerfällt, folgt dies auch für g.

Nun beweisen wir die Implikation „(a) $\Rightarrow$ (b)“. Wegen der Endlichkeit von L/K gilt $L = K(\alpha_1, \ldots, \alpha_n)$. Wegen (a) sind die Minimalpolynome $g_i := \mathrm{irr}(\alpha_i, K)$ separabel und zerfallen über L in Linearfaktoren. Also ist auch deren kleinstes gemeinsames Vielfache $f = \mathrm{kgV}(g_1, \ldots, g_n)$ separabel, und L ist ein Zerfällungskörper von f über K.

Wir betrachten noch die folgende zusätzliche Bedingung:

(b’) $L = K(\alpha)$, so dass $\mathrm{irr}(\alpha, K)$ separabel ist und über L in Linearfaktoren zerfällt.

Nun zeigen wir die Implikation „(b) $\Rightarrow$ (b’)“. Wir setzen also $L = K(\alpha_1, \ldots, \alpha_n)$ voraus, so dass $f := \prod_{i=1}^n (x - \alpha_i)$ in $K[x]$ liegt und separabel ist. Die α_i sind dann separabel, und Satz 20.11 liefert $L = K(\alpha)$ mit α separabel. Da L/K nach Satz 20.3 normal ist, zerfällt $\mathrm{irr}(\alpha, K)$ über L in Linearfaktoren.

Als nächstes zeigen wir die Implikation „(b’) $\Rightarrow$ (c)“. Wir haben also

$$g := \mathrm{irr}(\alpha, K) = \prod_{i=1}^n (x - \alpha_i) \tag{21.1}$$

mit $\alpha_i \in L$ paarweise verschieden und $\alpha_1 = \alpha$. Aus Proposition 16.13 folgt $n = [L : K]$. Für jedes $\sigma \in \mathrm{Aut}(L/K) =: G$ gilt

$$g\left(\sigma(\alpha)\right) = \sigma\left(g(\alpha)\right) = \sigma(0) = 0,$$

wegen (21.1) folgt also $\sigma(\alpha) \in \{\alpha_1, \ldots, \alpha_n\}$. Dies liefert eine Abbildung

$$\Phi\colon G \to \{\alpha_1, \ldots, \alpha_n\},\ \sigma \mapsto \sigma(\alpha).$$

Wegen $L = K(\alpha)$ ist Φ injektiv. Zum Nachweis der Surjektivität nehmen wir $i \in \{1, \ldots, n\}$. Wegen $g(\alpha_i) = 0$ liefert Proposition 18.2 einen K-Homomorphismus $\sigma\colon L \to K(\alpha_i)$ mit $\sigma(\alpha) = \alpha_i$. Wegen $[K(\alpha_i) : K] =$

$\deg(g) = n = [L : K]$ ist σ ein Automorphismus, also $\sigma \in G$ und $\Phi(\sigma) = \alpha_i$. Damit ist Φ bijektiv, und es folgt $|G| = n = [L : K]$.

Wir schließen den Beweis der Äquivalenz durch den Nachweis der Implikation „(c) $\Rightarrow$ (d)" ab. Wir setzen $H := \mathrm{Aut}(L/K)$ und $K' := L^H$. Es folgt $H \subseteq \mathrm{Aut}(L/K')$, also gilt (d) für L/K'. Nach dem bisher Bewiesenen gilt also auch (c) für L/K', also

$$[L : K'] = |\operatorname{Aut}(L/K')| \geq |H| = [L : K] = [L : K'] \cdot [K' : K],$$

wobei die vorletzte Gleichheit wegen der Annahme (c) gilt und die letzte wegen Proposition 16.14. Es folgt $K' = K$, also gilt (d).

Für den Beweis der Zusatzaussage nehmen wir eine Untergruppe $H \subseteq \mathrm{Aut}(L/K)$ mit $L^H = K$. Insbesondere gelten (a)–(d) und (b'). Wir haben also $\alpha \in L$ mit $L = K(\alpha)$. Mit $g := \mathrm{irr}(\alpha, K)$ und $f := \prod_{\sigma \in H} (x - \sigma(\alpha))$ folgt $f \in L^H[x] = K[x]$, also ist g ein Teiler von f. Wir erhalten

$$|H| = \deg(f) \geq \deg(g) = [L : K] \underset{(c)}{=} |\operatorname{Aut}(L/K)|,$$

und es folgt $H = \mathrm{Aut}(L/K)$. Dies schließt den Beweis ab. $\square$

Anmerkung 21.4. Wir können nun auch schließen, dass eine (in folgendem Sinne) separabel erzeugte Körpererweiterung separabel ist. Es sei nämlich $L = K(\alpha_1, \ldots, \alpha_n)/K$ eine Körpererweiterung mit $\alpha_1, \ldots, \alpha_n$ separabel. Dann ist auch das Polynom $f := \mathrm{kgV}\left(\mathrm{irr}(\alpha_1, K), \ldots, \mathrm{irr}(\alpha_n, K)\right) \in K[x]$ separabel. Wegen Satz 21.3 ist ein Zerfällungskörper N von f separabel. Wegen $L \subseteq N$ (bei geeigneter Wahl von N) ist L/K also auch separabel. $\triangleleft$

Definition 21.5. *Eine endliche Körpererweiterung L/K, die die Bedingungen aus Satz 21.3 erfüllt, heißt* **galoissch**. *Falls L/K galoissch ist, so heißt*

$$\mathrm{Gal}(L/K) := \mathrm{Aut}(L/K)$$

die **Galoisgruppe** *von L/K.*

Beispiel 21.6. (1) L sei der Zerfällungskörper von $f := x^3 - 2$ über $K = \mathbb{Q}$, also $L = \mathbb{Q}(\alpha_1, \alpha_2, \alpha_3)$ mit $x^3 - 2 = (x - \alpha_1)(x - \alpha_2)(x - \alpha_3)$. Als Zerfällungskörper ist L/K galoissch. Wir möchten die Galoisgruppe bestimmen. Jedes $\sigma \in G := \mathrm{Gal}(L/K)$ permutiert die α_i, denn

$$\sigma(\alpha_i)^3 = \sigma(\alpha_i^3) = \sigma(2) = 2.$$

Dies liefert eine Permutationsdarstellung $G \to S_3$. Wegen $L = \mathbb{Q}(\alpha_1, \alpha_2, \alpha_3)$ ist diese injektiv. Es gilt

$$[L : \mathbb{Q}] = [L : \mathbb{Q}(\alpha_1)] \cdot [\mathbb{Q}(\alpha_1) : \mathbb{Q}] = [L : \mathbb{Q}(\alpha_1)] \cdot 3 > 3,$$

weil man α_1 reell wählen kann, aber die anderen α_i dann nicht reell sind. Also folgt $|G| > 3$. Da G zu einer Untergruppe der S_3 isomorph ist, folgt $G \cong S_3$.

(2) $L := \mathbb{Q}(\sqrt[4]{2})$ ist nicht galoissch über $K := \mathbb{Q}$. Dies haben wir in Beispiel 21.2 gesehen. Dort haben wir auch gesehen, dass $H := \mathrm{Aut}(L/K) \cong Z_2$ ist, und
$$L^H = \mathbb{Q}(\sqrt{2}) \neq \mathbb{Q}.$$

$\triangleleft$

Satz 21.7 (Hauptsatz der Galoistheorie)**.** *Es seien N/K eine galoissche Körpererweiterung und $G = \mathrm{Gal}(N/K)$. Wir setzen*
$$\mathcal{A} := \{H \subseteq G \mid H \ \textit{Untergruppe}\}$$
und
$$\mathcal{B} := \{L \leq N \mid K \leq L\}$$
(die Menge der Zwischenkörper). Dann gelten

(a) Die Abbildung
$$\Phi\colon \mathcal{A} \to \mathcal{B},\ H \mapsto N^H$$
ist eine Bijektion mit Umkehrabbildung
$$\Psi\colon \mathcal{B} \to \mathcal{A},\ L \mapsto \mathrm{Gal}(N/L).$$

(b) Für $H_1, H_2 \in \mathcal{A}$ gilt die Äquivalenz
$$H_1 \subseteq H_2 \quad \Longleftrightarrow \quad \Phi(H_1) \supseteq \Phi(H_2),$$
d.h. Φ und Ψ sind inklusionsumkehrend.

(c) Für $H \in \mathcal{A}$ gelten
$$[N : N^H] = |H| \quad \textit{und} \quad [N^H : K] = (G : H).$$

(d) Für $H \in \mathcal{A}$ gilt die Äquivalenz
$$N^H/K \ \textit{ist galoissch} \quad \Longleftrightarrow \quad H \trianglelefteq G \ \textit{(Normalteiler)}.$$
Falls diese Bedingungen erfüllt sind, gilt
$$\mathrm{Gal}(N^H/K) \cong G/H.$$

Beweis. (a) Es sei $H \in \mathcal{A}$. Dann trifft Satz 21.3(d) auf N/N^H zu, also gilt $H = \mathrm{Gal}(N/N^H)$. Dies bedeutet $\Psi \circ \Phi = \mathrm{id}_{\mathcal{A}}$. Es sei nun $L \in \mathcal{B}$. Da N/K normal und separabel ist, folgt dies auch für N/L (wegen Proposition 20.5 und Definition 20.10). Wegen Satz 21.3 folgt $L = N^{\mathrm{Gal}(N/L)}$. Dies bedeutet $\Phi \circ \Psi = \mathrm{id}_{\mathcal{B}}$.

(b) Dies folgt unmittelbar aus der Definition von Φ und Ψ.

(c) Wegen $H = \mathrm{Gal}(N/N^H)$ liefert Satz 21.3(c) die Gleichung $|H| = [N : N^H]$. Hieraus folgt

$$(G : H) = \frac{|G|}{|H|} = \frac{[N : K]}{[N : N^H]} = [N^H : K].$$

(d) Zur Vorbereitung bemerken wir, dass für alle $\sigma \in G$ die Gleichung

$$\sigma\left(N^H\right) = N^{\sigma H \sigma^{-1}} \tag{21.2}$$

gilt, denn für alle $\alpha \in N$ haben wir die folgende Äquivalenz:

$$\begin{aligned}\alpha \in \sigma\left(N^H\right) &\iff \sigma^{-1}(\alpha) \in N^H \\ &\iff \forall\, \tau \in H:\ \sigma\tau\sigma^{-1}(\alpha) = \alpha \iff \alpha \in N^{\sigma H \sigma^{-1}}.\end{aligned}$$

Wir nehmen nun an, dass $L := N^H$ galoissch über K ist. Wegen Satz 19.4 gibt es einen K-Homomorphismus $\varphi\colon N \to \overline{K}$ in einen algebraischen Abschluss von K. Für jedes $\sigma \in G$ ist $\varphi \circ \sigma|_L\colon L \to \overline{K}$ ein K-Homomorphismus, wegen Satz 20.3 folgt also $\varphi(\sigma(L)) = \varphi(L)$. Wegen der Injektivität von φ erhalten wir $\sigma(L) = L$, also $\sigma^{-1} H \sigma = H$ wegen (21.2) und (a).
Umgekehrt sei $H \trianglelefteq G$ ein Normalteiler. Wegen (21.2) bildet jedes $\sigma \in G$ dann den Körper $L := N^H$ in sich selbst ab, und wir erhalten einen Homomorphismus

$$\mathrm{res}\colon G \to \mathrm{Aut}(L/K),\ \sigma \mapsto \sigma|_L.$$

Dessen Kern ist $\mathrm{Gal}(N/L) = H$, also gilt $G/H \cong \mathrm{Bild}(\mathrm{res}) =: \widetilde{G}$. Wir haben

$$K \subseteq L^{\widetilde{G}} \subseteq N^G = K,$$

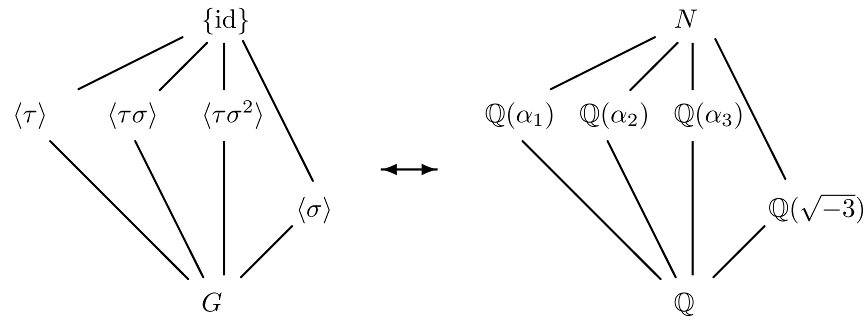
also ist L/K galoissch mit Galoisgruppe $\mathrm{Gal}(L/K) = \widetilde{G} \cong G/H$. □

Beispiel 21.8. In Beispiel 21.6(1) haben wir die Galoisgruppe des Zerfällungskörpers $N := \mathbb{Q}(\alpha_1, \alpha_2, \alpha_3)$ von $f = x^3 - 2 = \prod_{i=1}^{3}(x - \alpha_i)$ über $K = \mathbb{Q}$ bestimmt. Das Ergebnis war $G := \mathrm{Gal}(N/K) \cong S_3$, d.h. jede Permutation der α_i lässt sich genau zu einem Element von G fortsetzen. Insbesondere haben wir Elemente $\sigma, \tau \in G$ mit

$$\sigma\colon \alpha_1 \mapsto \alpha_2 \mapsto \alpha_3 \mapsto \alpha_1 \quad \text{und} \quad \tau\colon \alpha_1 \mapsto \alpha_1,\ \alpha_2 \leftrightarrow \alpha_3,$$

und $G = \langle \sigma, \tau \rangle$. In Beispiel 1.5(4) haben wir die Untergruppen der S_3 bestimmt. Diese stellen wir in einem Diagramm dar, das die Untergruppenbeziehungen beschreibt. Nach Satz 21.7 erhalten wir ein entsprechendes Diagramm der Zwischenkörper. Weil unsere Bijektionen inklusionsumkehrend sind, stellen wir das Untergruppendiagramm auf den Kopf, also mit der trivialen Gruppe nach oben, so dass im Körperdiagramm der größte Körper

(N) oben steht. Wir erhalten folgende Diagramme:



Im rechten Diagramm stehen die Fixkörper, wobei $\mathbb{Q}(\sqrt{-3})$ als Fixkörper von $\langle\sigma\rangle$ erklärungsbedürftig ist. Aus $\alpha_1\alpha_2\alpha_3 = 2$ folgt $\alpha_1\alpha_3 = \frac{2}{\alpha_2} = \alpha_2^2$, also $\frac{\alpha_1}{\alpha_2} = \frac{\alpha_2}{\alpha_3} =: \omega$. Es folgt $\sigma(\omega) = \omega$, also $\omega \in N^{\langle\sigma\rangle}$. Für ω gilt $0 = \omega^3 - 1 = (\omega - 1)(\omega^2 + \omega + 1)$, also $\omega^2 + \omega + 1 = 0$, denn $\omega \neq 1$. Es folgt $\omega = \frac{-1\pm\sqrt{-3}}{2}$, also $\mathbb{Q}(\omega) = \mathbb{Q}(\sqrt{-3})$. Wir erhalten $\mathbb{Q}(\sqrt{-3}) \subseteq N^{\langle\sigma\rangle}$, und wegen

$$[N^{\langle\sigma\rangle} : K] = (G : \langle\sigma\rangle) = 2$$

folgt Gleichheit.

Im Untergruppendiagramm ist $\langle\sigma\rangle$ der einzige nicht-triviale Normalteiler, und entsprechend ist $\mathbb{Q}(\sqrt{-3})$ der einzige über $\mathbb{Q}$ galoissche echte Zwischenkörper. Es gilt $\mathrm{Gal}\big(\mathbb{Q}(\sqrt{-3})/\mathbb{Q}\big) \cong G/\langle\sigma\rangle \cong Z_2$. Die anderen Zwischenkörper sind *konjugiert*, d.h. sie werden durch Automorphismen von N/K ineinander übergeführt, ebenso wie die entsprechenden Untergruppen konjugiert sind. $\triangleleft$

Beispiel 21.9. Es seien p eine Primzahl und $q = p^n$ mit $n \in \mathbb{N}_{>0}$ eine Potenz. Wir wissen, dass $\mathbb{F}_q$ der Zerfällungskörper von $x^q - x$ über $\mathbb{F}_p$ ist, und dass $\mathbb{F}_q/\mathbb{F}_p$ separabel ist. Also ist $\mathbb{F}_q/\mathbb{F}_p$ galoissch. Um die Galoisgruppe zu bestimmen, erinnern wir uns an den Frobenius-Homomorphismus

$$F\colon \mathbb{F}_q \to \mathbb{F}_q,\ \alpha \mapsto \alpha^p$$

(siehe Satz 10.13). F ist injektiv, also auch surjektiv (wegen $|\mathbb{F}_q| < \infty$), und $F|_{\mathbb{F}_p} = \mathrm{id}$. Also $F \in \mathrm{Gal}(\mathbb{F}_q/\mathbb{F}_p)$. Was ist die Ordnung von F? Falls $F^i = \mathrm{id}$, so folgt $\alpha^{p^i} = \alpha$ für alle $\alpha \in \mathbb{F}_q$. Das kleinste positive i, für das dies zutrifft, ist $i = n$. Es folgt $\mathrm{ord}(F) = n$, also

$$|\langle F\rangle| = n = [\mathbb{F}_q : \mathbb{F}_p] = |\,\mathrm{Gal}(\mathbb{F}_q/\mathbb{F}_p)|.$$

Es folgt

$$\mathrm{Gal}(\mathbb{F}_q/\mathbb{F}_p) = \langle F\rangle \cong Z_n.$$

Es folgt nun auch, dass die Galoisgruppe $\mathrm{Gal}(\mathbb{F}_q/L)$ für einen Zwischenkörper L (als Untergruppe von $\mathrm{Gal}(\mathbb{F}_q/\mathbb{F}_p)$) zyklisch ist. Wir ziehen das Fazit, dass Erweiterungen von endlichen Körpern galoissch sind mit zyklischer Galoisgruppe. ◁

Zum Schluss erwähnen wir noch, dass man auch zu Polynomen eine Galoisgruppe definieren kann. Es sei nämlich $f \in K[x]$ ein separables Polynom über einem Körper und $\alpha_1, \dots, \alpha_n$ die Nullstellen von f in einem Zerfällungskörper N. Für $\sigma \in G := \mathrm{Gal}(N/K)$ und $i \in \{1, \dots, n\}$ gilt

$$f(\sigma(\alpha_i)) = \sigma(f(\alpha_i)) = \sigma(0) = 0,$$

also $\sigma(\alpha_i) = \alpha_j$ mit $j \in \{1, \dots, n\}$. Dies liefert eine Permutationsdarstellung

$$\pi\colon G \to S_n \quad \text{mit} \quad \sigma(\alpha_i) = \alpha_{\pi(\sigma)(i)} \text{ für } \sigma \in G,\ i \in \{1, \dots, n\}.$$

Wegen $N = K(\alpha_1, \dots, \alpha_n)$ ist π injektiv, also $\mathrm{Bild}(\pi) \cong G$. Wir nennen

$$\mathrm{Gal}(f) := \mathrm{Bild}(\pi) \subseteq S_n$$

die **Galoisgruppe** von f. Die Galoisgruppe eines Polynoms ist also ein Permutationsgruppe.

Beispiel 21.10. (1) Für $f = x^3 - 2 \in \mathbb{Q}[x]$ gilt wegen Beispiel 21.6(1)

$$\mathrm{Gal}(f) = S_3.$$

(2) In Beispiel 18.7 wurde der Zerfällungskörper N des Polynoms $f = x^4 - 2 \in \mathbb{Q}[x]$ bestimmt und der Grad $[N : \mathbb{Q}] = 8$ berechnet. $\mathrm{Gal}(f)$ ist also eine Untergruppe der Ordnung 8 von S_4. Bis auf Isomorphie gibt es nur eine solche Untergruppe, nämlich die Diedergruppe D_4. Es folgt $\mathrm{Gal}(f) \cong D_4$. ◁

Anmerkung 21.11. Die „meisten" (in einem zu spezifizierenden Sinne) Polynome über $\mathbb{Q}$ haben die Galoisgruppe S_n. ◁

22 Kreisteilungskörper

Definition 22.1. *Es seien K ein Körper und $n \in \mathbb{N}_{>0}$ eine natürliche Zahl. Der Zerfällungskörper des Polynoms $x^n - 1 \in K[x]$ über K heißt der n-te* **Kreisteilungskörper** *und wird mit $K^{(n)}$ bezeichnet. Wir setzen*

$$W_n := \{\zeta \in K^{(n)} \mid \zeta^n = 1\}$$

und bezeichnen die Elemente von W_n als n-te **Einheitswurzeln***. Man beachte, dass W_n wegen Satz 11.6 eine zyklische Gruppe ist. Eine n-te Einheitswurzel $\zeta \in W_n$ heißt* **primitiv***, falls $W_n = \langle \zeta \rangle$. Das Polynom*

$$\Phi_n := \prod_{\substack{\zeta \in W_n \\ primitiv}} (x - \zeta)$$

heißt das n-te **Kreisteilungspolynom** *über K.*

Beispiel 22.2. In $K = \mathbb{C}$ gibt es die vierten Einheitswurzeln ± 1 und $\pm i$. Davon sind $\pm i$ primitiv. Wir erhalten $\Phi_4 = (x-i)(x+i) = x^2 + 1$. ◁

Lemma 22.3. *Es seien K ein Körper der Charakteristik p (mit $p = 0$ oder Primzahl) und $n \in \mathbb{N}_{>0}$ eine natürliche Zahl.*

(a) Falls n kein Vielfaches von p ist, so ist $f := x^n - 1 \in K[x]$ separabel.
(b) Es sei $n = p^r \cdot m$ mit $r, m \in \mathbb{N}_{>0}$. Dann gilt

$$x^n - 1 = (x^m - 1)^{p^r},$$

f ist also nicht seprabel.

Beweis. (a) Wegen $f' = nx^{n-1}$ sind f und f' teilerfremd, also ist f separabel.
(b) Dies ergibt sich durch r-fache Anwendung des Frobenius-Homomorphismus auf $(x^m - 1)$. □

Satz 22.4. *Es seien K ein Körper der Charakteristik p und $n \in \mathbb{N}_{>0}$ eine natürliche Zahl. Falls $p \mid n$, schreiben wir $n = p^r \cdot m$ mit $r, m \in \mathbb{N}_{>0}$ und $p \nmid m$, und andernfalls $m := n$.*

(a) $K^{(n)}/K$ ist galoissch.
(b) Für das n-te Kreisteilungspolynom gilt: $\Phi_n \in K[x]$.
(c) Es gelten $|W_n| = m$ und $\deg(\Phi_n) = \varphi(m)$ (die Eulersche φ-Funktion).
(d) $\operatorname{Gal}\left(K^{(n)}/K\right)$ ist isomorph zu einer Untergruppe von $(\mathbb{Z}/(m))^{\times}$.

Beweis. (a) Wegen Lemma 22.3 ist $K^{(n)}$ der Zerfällungskörper des separablen Polynoms $x^m - 1$.
(b) Jedes $\sigma \in G := \operatorname{Gal}\left(K^{(n)}/K\right)$ permutiert die primitiven Einheitswurzeln. Es folgt

$$\Phi_n \in \left(K^{(n)}\right)^G [x] = K[x].$$

(c) Aus Lemma 22.3 folgt $|W_n| = |W_m| = m$. Da W_n wegen Satz 11.6 zyklisch ist, gibt es $\varphi(m)$ Elemente, die W_n erzeugen, also $\deg(\Phi_n) = \varphi(m)$.
(d) $G := \operatorname{Gal}\left(K^{(n)}/K\right)$ operiert treu auf W_n, wobei jedes $\sigma \in G$ als Gruppen-Homomorphismus auf W_n wirkt. Dies liefert einen injektiven Homomorphismus

$$G \to \operatorname{Aut}(W_n) \cong \operatorname{Aut}(Z_m) \cong (\mathbb{Z}/(m))^{\times},$$

wie behauptet. □

Beispiel 22.5. Wir haben $\Phi_1 = x - 1$, $\Phi_2 = x + 1$, $\Phi_3 = x^2 + x + 1$, $\Phi_4 = x^2 + 1$, $\Phi_5 = x^4 + x^3 + x^2 + x + 1$, $\Phi_6 = x^2 - x + 1$, $\Phi_8 = x^4 + 1$, … ◁

Anmerkung. Über $K = \mathbb{Q}$ sind sämtliche Kreisteilungspolynome irreduzibel, es gilt also $\operatorname{Gal}\left(\mathbb{Q}^{(n)}/\mathbb{Q}\right) \cong (\mathbb{Z}/(n))^\times$. Wir werden dies nicht beweisen und auch nicht benutzen. ◁

23 Auflösbare Polynome

Der Einfachheit halber seien alle Körper in diesem Abschnitt von der Charakteristik 0.

Eine der Motivationen für die Entwicklung der Galoistheorie war der Versuch, Formeln für die Nullstellen von Polynomen zu finden. Wir wissen, dass x^2+ax+b die Nullstelle $\frac{-a+\sqrt{a^2-4b}}{2}$ hat. Weiter hat das Polynom x^3+ax+b (gemäß der berühmten *Cardanischen Formeln*) die Nullstelle

$$\frac{1}{6}\left(\left(-108b+12\sqrt{12a^3+81b^2}\right)^{1/3}+\left(-108b-12\sqrt{12a^3+81b^2}\right)^{1/3}\right).$$

Es stellt sich die Frage, ob ähnliche Formeln auch für Polynome von höheren Graden existieren. Diese Frage wird durch die folgende Definition präzisiert:

Definition 23.1. *(a) Eine Körpererweiterung L/K heißt eine* **Radikalerweiterung***, falls es Zwischenkörper*

$$K = L_0 \leq L_1 \leq \cdots \leq L_r = L$$

*gibt, so dass für alle $i = 1, \ldots, r$ gelten: $L_i = L_{i-1}(\alpha_i)$ mit $\alpha_i^{n_i} \in L_{i-1}$ für ein $n_i \in \mathbb{N}_{>0}$. Genauer heißt L/K eine n-***Radikalerweiterung** *($n \in \mathbb{N}_{>0}$), falls n ein Vielfaches aller n_i ist.*

(b) Ein Polynom $f \in K[x]$ heißt **auflösbar***, falls es eine Radikalerweiterung L/K gibt, so dass f eine Nullstelle in L hat.*

Die oben genannten Formeln besagen also, dass alle Polynome vom Grad ≤ 3 auflösbar sind.

Ziel des Abschnitts ist es, einen Zusammenhang zwischen auflösbaren Polynomen und auflösbaren Gruppen herzustellen. Hierfür benötigen wir drei Lemmata.

Lemma 23.2. *Es seien L/K eine Körpererweiterung und $n \in \mathbb{N}_{>0}$ eine natürliche Zahl. Wir setzen $K^{(n)} = K$ voraus, d.h. K enthalte n verschiedene n-te Einheitswurzeln.*

(a) Falls $L = K(\alpha)$ mit $\alpha^n \in K$, so ist L/K galoissch, und $\operatorname{Gal}(L/K)$ ist isomorph zu einer Untergruppe von Z_n.

(b) Ist L/K galoissch mit $\operatorname{Gal}(L/K) \cong Z_n$ und n eine Primzahl, so gibt es $\lambda \in L$ mit $L = K(\lambda)$ und $\lambda^n \in K$.

Beweis. (a) Mit $W_n := \{\zeta \in K \mid \zeta^n = 1\} \cong Z_n$ ist L der Zerfällungskörper von $x^n - \alpha^n = \prod_{\zeta\in W_n}(x-\zeta\alpha)$ über K, also ist L/K galoissch. Wir können $\alpha \neq 0$ voraussetzen und erhalten eine Abbildung

$$\varphi\colon G := \mathrm{Gal}(L/K) \to W_n,\ \sigma \mapsto \frac{\sigma(\alpha)}{\alpha}.$$

Wegen $L = K(\alpha)$ ist φ injektiv, und wegen $W_n \subseteq K$ gilt für $\sigma, \tau \in G$:

$$\varphi(\sigma\tau) = \frac{\sigma(\tau(\alpha))}{\alpha} = \sigma\left(\frac{\tau(\alpha)}{\alpha}\right) \cdot \frac{\sigma(\alpha)}{\alpha} = \frac{\tau(\alpha)}{\alpha} \cdot \frac{\sigma(\alpha)}{\alpha} = \varphi(\sigma)\varphi(\tau).$$

Also ist φ ein Homomorphismus.

(b) Wir wählen einen Erzeuger σ von $G := \mathrm{Gal}(L/K)$, einen Erzeuger ζ von W_n, und ein $\alpha \in L \setminus K$. Für die sogenannten *Lagrangeschen Resolventen*

$$\lambda_i := \sum_{j=0}^{n-1} \zeta^{ij} \sigma^j(\alpha) \in L \quad (i = 0, \ldots, n-1)$$

gilt $\sigma(\lambda_i) = \zeta^{-i}\lambda_i$, also $\lambda_i^n \in L^G = K$. Aus $\det\left(\zeta^{ij}\right)_{i,j=0,\ldots,n-1} \neq 0$ (Vandermondesche Determinante) folgt, dass sich α als K-Linearkombination der λ_i schreiben lässt. (Explizit: $\alpha = \frac{1}{n}\sum_{i=0}^{n-1} \lambda_i$.) Insbesondere gibt es also ein i mit $\lambda_i \notin K$. Da n ein Primzahl ist und $[L : K] = n$, folgt $L = K(\lambda_i)$. □

Wir erhalten nun den folgenden Zusammenhang zwischen Radikalerweiterungen und auflösbaren Gruppen.

Lemma 23.3. *Es seien N/K eine galoissche Körpererweiterung und $G = \mathrm{Gal}(N/K)$.*

(a) Falls N/K eine n-Radikalerweiterung ist und $K^{(n)} = K$, so ist G auflösbar.

(b) Falls G auflösbar ist und $K^{(|G|)} = K$, so ist N/K eine Radikalerweiterung.

Beweis. Gemäß dem Hauptsatz der Galoistheorie (Satz 21.7) entsprechen sich Normalreihen

$$\{\iota\} = G_r \triangleleft G_{r-1} \triangleleft \cdots \triangleleft G_1 \triangleleft G_0 = G$$

von G und Ketten von Körpererweiterungen

$$N = L_r \geq L_{r-1} \geq \cdots \geq L_1 \geq L_0 = K$$

mit L_i/L_{i-1} galoissch $(i = 1, \ldots, r)$, und es gilt $\mathrm{Gal}\left(L_i/L_{i-1}\right) \cong G_{i-1}/G_i$.

Ist nun N/K eine n-Radikalerweiterung, so liefert Lemma 23.2(a) eine Kette von galoisschen Körpererweiterungen mit zyklischen Galoisgruppen. Wir bekommen also eine Normalreihe von G mit zyklischen Faktorgruppen, und aus Proposition 3.7(b) folgt, dass G auflösbar ist.

Ist umgekehrt G auflösbar, so liefert Satz 3.9 eine Normalreihe von G mit zyklischen Faktorgruppen von Primzahlordnung. Lemma 23.2(b) beschreibt also die entsprechenden Körpererweiterungen L_i/L_{i-1}, und es ergibt sich, dass N/K eine Radikalerweiterung ist. □

Lemma 23.4. *Es sei L/K eine Radikalerweiterung. Dann gibt es eine galoissche Radikalerweiterung N/K mit $L \subseteq N$.*

Beweis. Wegen $\text{char}(K) = 0$ ist Satz 20.11 anwendbar und liefert $L = K(\alpha)$. Es seien $\alpha_1 = \alpha, \alpha_2, \ldots, \alpha_n$ die Nullstellen von $f := \text{irr}(\alpha, K)$ in einem Zerfällungskörper N von f. Wegen Proposition 18.2 ist jedes $K(\alpha_i)/K$ isomorph zu L/K und damit eine Radikalerweiterung. Also ist auch $K(\alpha_1, \ldots, \alpha_i)/K(\alpha_1, \ldots, \alpha_{i-1})$ eine Radikalerweiterung. Es folgt, dass $N = K(\alpha_1, \ldots, \alpha_n)$ ebenso eine Radikalerweiterung ist, und $L \subseteq N$ wegen $\alpha = \alpha_1 \in N$. □

Satz 23.5. *Für ein irreduzibles Polynom $f \in K[x]$ über einem Körper der Charakteristik 0 sind folgende Aussagen äquivalent:*

(a) Das Polynom f ist auflösbar.
(b) Die Galoisgruppe $\text{Gal}(f)$ ist auflösbar.

Beweis. Wir setzen zunächst voraus, dass f auflösbar ist, also gibt es eine Radikalerweiterung N/K, so dass f ein Nullstelle $\alpha \in N$ hat. Wegen Lemma 23.4 können wir annehmen, dass N/K galoissch ist. Es sei N/K eine n-Radikalerweiterung. Es ist klar, dass auch $N^{(n)}/K$ galoissch ist und dass $N^{(n)}/K^{(n)}$ eine n-Radikalerweiterung ist. Nach Lemma 23.3 ist $\text{Gal}\left(N^{(n)}/K^{(n)}\right)$ also auflösbar. Weiter ist $K^{(n)}/K$ nach Satz 22.4 galoissch mit abelscher Galoisgruppe. $\text{Gal}\left(N^{(n)}/K\right)$ hat also einen auflösbaren Normalteiler mit abelscher Faktorgruppe, ist nach Proposition 3.7(b) also selbst auflösbar. Da f irreduzibel ist und in $N^{(n)}$ eine Nullstelle hat, folgt aus der Normalität von $N^{(n)}/K$, dass $N^{(n)}$ einen Zerfällungskörper L von f über K enthält. $\text{Gal}(f) \cong \text{Gal}(L/K)$ ist nun als Faktorgruppe von $\text{Gal}\left(N^{(n)}/K\right)$ auflösbar.

Nun setzen wir voraus, dass $\text{Gal}(f)$ auflösbar ist, für einen Zerfällungskörper L von f über K ist also $G := \text{Gal}(L/K)$ auflösbar. Mit $n := |G|$ ist auch $L^{(n)}/K^{(n)}$ galoissch, und mit $\widetilde{G} := \text{Gal}\left(L^{(n)}/K^{(n)}\right)$ haben wir einen Homomorphismus

$$\varphi\colon \widetilde{G} \to G,\ \sigma \mapsto \sigma|_L.$$

Dieser ist injektiv, denn für $\sigma \in \text{Kern}(\varphi)$ gilt $\sigma|_L = \text{id}$ und $\sigma|_{K^{(n)}} = \text{id}$, also $\sigma = \text{id}$. $\widetilde{G}$ ist also isomorph zu einer Untergruppe der auflösbaren Gruppe G und damit nach Proposition 3.7(a) selbst auflösbar. Weil n ein Vielfaches von $|\widetilde{G}|$ ist, liefert Lemma 23.3, dass $L^{(n)}/K^{(n)}$ eine Radikalerweiterung ist. Da $K^{(n)}/K$ ohnehin eine Radikalerweiterung ist, gilt dasselbe für $L^{(n)}/K$. Da f eine Nullstelle in $L^{(n)}$ hat, ist f auflösbar. □

Korollar 23.6. *Alle Polynome vom Grad* ≤ 4 *über einem Körper der Charakteristik* 0 *sind auflösbar.*

Beweis. Ist $f \in K[x]$ ein Polynom vom Grad n, so ist $G := \mathrm{Gal}(f)$ eine Untergruppe der S_n. Für $n \leq 4$ ist die S_n auflösbar (siehe Beispiel 4.7), also auch G. □

Im Gegensatz hierzu ist die S_n für $n \geq 5$ nicht auflösbar (siehe Korollar 4.8). Wir können also bei Polynomen vom Grad ≥ 5 keine Auflösbarkeit erwarten, und wegen Anmerkung 21.11 sind sogar die „meisten“ Polynome über $\mathbb{Q}$ von Grad ≥ 5 nicht auflösbar.

Beispiel 23.7. Wir betrachten das Polynom $f = x^5 - 4x + 2 \in \mathbb{Q}[x]$. Kurvendiskussion liefert, dass f genau drei reelle Nullstellen hat. Die verbleibenden zwei komplexen Nullstellen werden also durch die komplexe Konjugation permutiert. Dies liefert eine Transposition $\tau \in G := \mathrm{Gal}(f)$. Nach dem Eisensteinkriterium ist f irreduzibel, also gilt $[\mathbb{Q}(\alpha) : \mathbb{Q}] = 5$ für jede Nullstelle α von f. Für einen Zerfällungskörper L von f folgt $5 \mid [L : \mathbb{Q}]$, also teilt 5 auch $|G|$. Rechnungen in der S_5 (die wir hier nicht wiedergeben) zeigen, dass die einzige Untergruppe, die eine Transposition enthält und deren Ordnung durch 5 teilbar ist, die S_5 selbst ist. Also $\mathrm{Gal}(f) = S_5$. Es folgt, dass f nicht auflösbar ist. ◁

Schon aus dem obigen Beispiel folgt, dass es keine Formel gibt, die die Nullstellen eines Polynoms von Grad 5 durch verschachtelte Wurzeln und die Grundrechenarten ausdrückt. Ebensowenig geht das für Polynome vom Grad > 5.

24 Bonusmaterial: Der Fundamentalsatz der Algebra

In diesem Abschnitt geben wir einen weitgehend algebraischen Beweis des folgenden Satzes:

Satz 24.1 (Fundamentalsatz der Algebra)**.** *Der Körper* $\mathbb{C}$ *ist algebraisch abgeschlossen.*

Wir benötigen zwei Lemmata.

Lemma 24.2. *Es sei* $L/\mathbb{R}$ *eine endliche Körpererweiterung mit* $[L : \mathbb{R}]$ *ungerade. Dann ist* $L = \mathbb{R}$.

Beweis. Es sei $\alpha \in L$ und $f := \mathrm{irr}(\alpha, \mathbb{R})$. Dann ist $\deg(f) = [\mathbb{R}(\alpha) : \mathbb{R}]$ ein Teiler von $[L : \mathbb{R}]$, also ungerade. Es folgt, dass f positive und negative Werte annimmt, nach dem Zwischenwertsatz hat f also eine Nullstelle $c \in \mathbb{R}$. Wegen der Irreduzibilität von f folgt $f = x - c$, also $\alpha = c \in \mathbb{R}$. Wir erhalten $L = \mathbb{R}$. □

Lemma 24.3. $\mathbb{C}$ *hat keine Körpererweiterung vom Grad* 2.

Beweis. Wir nehmen an, dass es eine Körpererweiterung $L/\mathbb{C}$ gibt mit $[L : \mathbb{C}] = 2$. Es folgt $L = \mathbb{C}(\alpha)$, so dass $f := \operatorname{irr}(\alpha, \mathbb{C})$ den Grad 2 hat. Mit $z := D(f) \in \mathbb{C}$ (die Diskriminante) folgt $L = \mathbb{C}(\sqrt{z})$. Wir schreiben $z = x + iy$ mit $x, y \in \mathbb{R}$. Wir bilden $r := \sqrt{x^2 + y^2} \in \mathbb{R}_{\geq 0}$ (wobei die Existenz von Quadratwurzeln nicht-negativer reeller Zahlen durch den Zwischenwertsatz garantiert wird). Es gilt

$$\begin{aligned}\left(\sqrt{\frac{r+x}{2}} + i\operatorname{sgn}(y)\sqrt{\frac{r-x}{2}}\right)^2 &= \frac{r+x}{2} + 2i\operatorname{sgn}(y)\sqrt{\frac{r+x}{2}}\sqrt{\frac{r-x}{2}} - \frac{r-x}{2} \\ &= x + 2i\operatorname{sgn}(y)\sqrt{\frac{r^2-x^2}{4}} = x + i\operatorname{sgn}(y)\sqrt{y^2} \\ &= z,\end{aligned}$$

also $\sqrt{z} \in \mathbb{C}$. Es folgt $L = \mathbb{C}$. □

Beweis von Satz 24.1. Es sei α ein Element einer algebraischen Erweiterung von $\mathbb{C}$, und es sei N ein Zerfällungskörper von $f := \operatorname{irr}(\alpha, \mathbb{R})$ über $\mathbb{C}$ mit $\alpha \in N$. Als Zerfällungskörper von $(x^2 + 1) \cdot f$ ist N auch galoissch über $\mathbb{R}$. Es sei $P \subseteq G := \operatorname{Gal}(N/\mathbb{R})$ eine 2-Sylow-Gruppe der Galoisgruppe. Dann ist $[N^P : \mathbb{R}] = (G : P)$ ungerade, also $N^P = \mathbb{R}$ wegen Lemma 24.2. Es folgt $P = G$, also ist G eine 2-Gruppe. Dasselbe gilt für $H := \operatorname{Gal}(N/\mathbb{C})$. Unter der Annahme $H \neq \{\mathrm{id}\}$ hätte H wegen Satz 6.2 eine Untergruppe $H_1 \subseteq H$ vom Index 2, also $[N^{H_1} : \mathbb{C}] = 2$, im Widerspruch zu Lemma 24.3. Es folgt $H = \{\mathrm{id}\}$, also $N = \mathbb{C}$. Dies liefert $\alpha \in \mathbb{C}$, also hat $\mathbb{C}$ keine echte algebraische Erweiterung und ist damit algebraisch abgeschlossen. □

25 Bonusmaterial: Konstruktion mit Zirkel und Lineal

In diesem Abschnitt wenden wir Körpertheorie auf geometrische Konstruktionsaufgaben aus der Antike an. Hierbei starten wir mit einer Punktmenge $S \subseteq \mathbb{R}^2$ in der euklidischen Ebene und gewinnen durch folgende Konstruktionsschritte neue Punkte:

(1) **Schnitt zweier Geraden**: Für Punkte $A, B, C, D \in S$ mit $A \neq B$, $C \neq D$ bilde den Schnittpunkt der Geraden $\overline{AB}$ und $\overline{CD}$, falls diese nicht parallel sind.

(2) **Schnitt eines Kreises und einer Geraden**: Für Punkte $A, B, C, D, E \in S$ mit $A \neq B$ bilde die Schnittpunkte der Geraden $\overline{AB}$ mit dem Kreis um C, dessen Radius der Abstand von D und E ist. **Anmerkung**: Man kann zeigen, dass man dieselbe Menge an konstruierbaren Punkten erhält, wenn man bei diesem Schritt die Einschränkung $C = D$ macht, also kein „Abtragen" von Längen mit dem Zirkel zulässt. Dasselbe gilt für (3).

(3) **Schnitt zweier Kreise** Bilde die Schnittpunkte zweier (verschiedener) Kreise wie in (2).

In diesem Abschnitt untersuchen wir die Konstuierbarkeit von Punkten mit Methoden der Körpertheorie. Dazu bilden wir die durch alle Koordinaten x, y von Punkten $P = (x, y) \in S$ erzeugte Körpererweiterung $K \subseteq \mathbb{R}$ von $\mathbb{Q}$.

Lemma 25.1. *Der Punkt $P = (x, y)$ sei in einem Schritt aus der Punktmenge $S \subseteq \mathbb{R}^2$ konstruierbar. Mit K wie oben gilt dann*

$$[K(x, y) : K] \leq 2.$$

Beweis. Wir unterscheiden drei Fälle entsprechend der drei möglichen Konstruktionsschritte.

(1) Die Gerade durch zwei Punkte (a, b) und (c, d) in S ist gegeben durch die Gleichung

$$(d - b)x + (a - c)y = ad - bc,$$

deren Koeffizienten in K liegen. Der Schnittpunkt $P = (x, y)$ zweier nicht paralleler Geraden ist also die eindeutige Lösung eines LGS mit Koeffizienten in K, also $x, y \in K$.

(2) Der Kreis um $(a, b) \in S$ mit dem Abstand von $(a_1, b_1) \in S$ und $(a_2, b_2) \in S$ als Radius ist gegeben durch

$$(x - a)^2 + (y - b)^2 = (a_1 - a_2)^2 + (b_1 - b_2)^2.$$

Die Schnittpunkte mit einer durch $cx + dy = e$ (wobei $c, d, e \in K$ und ohne Einschränkung $c \neq 0$) gegebenen Gerade sind Lösungen einer quadratischen Gleichung für y, also $[K(y) : K] \leq 2$ und $x \in K(y)$.

(3) Zwei Kreise sind gegeben durch Gleichungen

$$(x - a_1)^2 + (y - b_1)^2 = r_1^2$$

und

$$(x - a_2)^2 + (y - b_2)^2 = r_2^2$$

mit $a_i, b_i, r_i \in K$. Subtraktion liefert eine lineare Gleichung, die auf den zweiten Fall reduziert. □

Satz 25.2. *Der Punkt $P = (x, y)$ sei aus der Punktmenge $S \subseteq \mathbb{R}^2$ mit endlich vielen Schritten konstruierbar. Dann liegen x und y in einer 2-Radikalerweiterung $L \subseteq \mathbb{R}$ von K.*

Beweis. Dies folgt aus Lemma 25.1 durch Induktion nach der Anzahl der Konstruktionsschritte. □

Anmerkung. Enthält S mindestens zwei Punkte, so kann man diese durch Drehen, Skalieren und Verschieben auf die Punkte $(0, 0)$ und $(1, 0)$ transportieren. Falls nun $(0, 0), (1, 0) \in S$, dann gilt die Umkehrung von Satz 25.2. Der

Beweis läuft mit einigen geometrischen Konstuktionen. Er ist nicht schwer, würde aber den Umfang dieses Abschnitts erheblich erweitern. ◁

Mit Hilfe von Satz 25.2 kann man die Unlösbarkeit einiger klassischer Konstruktionsaufgaben beweisen. Wir behandeln drei davon.

Delisches Problem Gegeben sei die Kantenlänge a eines Würfels. Konstruiere die Kantenlänge eines Würfels mit dem doppelten Volumen („Würfelverdoppelung"). Für $a = 1$ müsste also $(\sqrt[3]{2}, 0)$ konstruierbar sein. Wegen $[\mathbb{Q}(\sqrt[3]{2}) : \mathbb{Q}] = 3$ liegt $\mathbb{Q}(\sqrt[3]{2})$ aber in keiner 2-Radikalerweiterung von $\mathbb{Q}$, also ist dies unmöglich.

Dreiteilung des Winkels Gegeben seien Punkte A,B und C, und $\measuredangle(A, B, C)$ bezeichne den Winkel zwischen den Vektoren $\overrightarrow{AB}$ und $\overrightarrow{AC}$. Konstruiere einen Punkt D mit

$$\measuredangle(A, B, D) = \frac{1}{3}\measuredangle(A, B, C).$$

Man kann leicht sehen, dass aus $S = \{A = (0, 0), B = (1, 0)\}$ ein gleichseitiges Dreieck ABC konstruierbar ist. Es müsste also ein Punkt D mit $\measuredangle(A, B, D) = 20°$ konstruierbar sein, und Schnitt mit dem Einheitskreis liefert einen Punkt mit $x = \cos(20°)$. Die Additionstheoreme ergeben für $\alpha \in \mathbb{R}$ allgemein $\cos(3\alpha) = 4\cos(\alpha)^3 - 3\cos(\alpha)$. Für $\alpha = 20°$ folgt $4x^3 - 3x = 1/2$. Substitution von x durch $x/2$ liefert $x^3 - 3x - 1 = 0$. Das Polynom ist irreduzibel, also $[\mathbb{Q}(x) : \mathbb{Q}] = 3$. Wieder liegt x also in keiner 2-Radikalerweiterung von $\mathbb{Q}$, die Winkeldreiteilung (auch „Trisektion" genannt) ist also unmöglich.

Quadratur des Kreises Gegeben eine Strecke der Länge r, konstruiere ein Quadrat mit dem gleichen Flächeninhalt wie der Kreis mit Radius r. Für $r = 1$ würde eine Lösung bedeuten, dass $\sqrt{\pi}$ in einer 2-Radikalerweiterung von $\mathbb{Q}$ liegt. Nach dem (schwierigen) *Satz von Lindemann* ist π aber transzendent über $\mathbb{Q}$. Also ist die Quadratur des Kreises unmöglich.

Notation

Index