Algebra
Wintersemester 2022/23
Universität Regensburg

Marc Hoyois

10. Februar 2023

Inhaltsverzeichnis

Kapitel 1

Gruppentheorie

Die Definition einer Gruppe ist uns aus der Linearen Algebra schon bekannt. Der Begriff der Gruppe ist eigentlich einer der wichtigsten Begriffe in der ganzen Mathematik. Der Grund dafür ist, *jedes* mathematische Objekt X (z.B., eine Menge, eine Gruppe, ein Ring, ein Vektorraum, eine Kategorie, eine geometrische Figur, ein Zauberwürfel, usw.) besitzt eine *Automorphismengruppe* $\mathrm{Aut}(X)$, die man als „Gruppe der Symmetrien“ des Objekts X auffassen kann. Automorphismengruppen sind in den meisten Fällen nicht abelsch. Zum Beispiel:

- Die Automorphismengruppe der Menge $\{1, 2, \ldots, n\}$ ist die symmetrische Gruppe S_n mit $n!$ Elementen. Falls $n \geq 3$ ist sie nicht abelsch.
- Die Automorphismengruppe des K-Vektorraums K^n ist die allgemeine lineare Gruppe $\mathrm{GL}_n(K)$. Falls $n \geq 2$ ist sie nicht abelsch.
- Die Isometriegruppe eines regelmäßigen n-Ecks ($n \geq 3$) ist eine Gruppe D_n mit $2n$ Elementen (n Drehungen und n Spiegelungen), die nicht abelsch ist.

In der Vorlesung *Lineare Algebra* haben wir schon eine vollständige Klassifikation von endlichen *abelschen* Gruppen erhalten: Jede endliche abelsche Gruppe ist zu

$$\mathbb{Z}/p_1^{e_1}\mathbb{Z} \oplus \cdots \oplus \mathbb{Z}/p_s^{e_s}\mathbb{Z}$$

isomorph, wobei $p_1, \ldots, p_s$ Primzahlen sind und $e_1, \ldots, e_s \in \mathbb{N} \setminus \{0\}$. Die Struktur von nicht-abelschen Gruppen ist aber viel komplizierter, und es gibt nur eine teilweise Klassifikation von endlichen Gruppen. Diese Klassifikation ist aber ein riesiger Satz des 20. Jahrhunderts und ist nicht in Reichweite dieser Vorlesung. Wir werden jedoch so viel Gruppentheorie entwickeln, dass wir die Klassifikationsstrategie und später interessante Anwendungen der Galoistheorie verstehen können.

1.1 Die Kategorie der Gruppen

1.1.1 Gruppen und Gruppenhomomorphismen

Wir erinnern zunächst an die Definition einer Gruppe:

Definition 1.1.1 (Gruppe)**.** Eine *Gruppe* ist ein Paar $(G, \cdot)$, bestehend aus einer Menge G und einer Abbildung

$$\cdot : G \times G \to G, \quad (g, h) \mapsto g \cdot h$$

(die *Verknüpfung* der Gruppe), mit folgenden Eigenschaften:

(i) (Assoziativität) Die Verknüpfung ist *assoziativ*, d.h., für alle $g, h, k \in G$ gilt

$$g \cdot (h \cdot k) = (g \cdot h) \cdot k.$$

(ii) (neutrales Element) Es existiert ein *neutrales Element* bzgl. $\cdot$, d.h., ein Element $e \in G$ so dass

$$e \cdot g = g \quad \text{und} \quad g \cdot e = g$$

für alle $g \in G$.

(iii) (inverse Elemente) Jedes $g \in G$ besitzt ein *inverses Element*, d.h., ein Element $h \in G$ so dass

$$g \cdot h \quad \text{und} \quad h \cdot g$$

neutrale Elemente sind.

Proposition 1.1.2 (Eindeutigkeit von neutralen und inversen Elementen)**.** *Sei $(G, \cdot)$ eine Gruppe.*

(i) *Sind $e, e' \in G$ neutrale Elemente bzgl. $\cdot$, so gilt $e = e'$.*

(ii) *Sei $g \in G$. Sind $h, h' \in G$ inverse Elemente von g, so gilt $h = h'$.*

Beweis. Siehe Proposition LA.2.1.3. □

Notation 1.1.3. Wegen Proposition 1.1.2 darf man „*das* neutrale Element“ und „*das* inverse Element von g“ sagen, da die entsprechenden mathematischen Objekte eindeutig sind. Das neutrale Element einer Gruppe wird mit e oder 1 bezeichnet, und das inverse Element von einem Element g wird mit g^{-1} bezeichnet. Das Symbol $\cdot$ schreibt man normalerweise gar nicht, d.h., man schreibt eher gh statt $g \cdot h$.

Bemerkung 1.1.4. In einer Gruppe gilt $(gh)^{-1} = h^{-1}g^{-1}$ (Reihenfolge beachten!). Nach der Eindeutigkeit des inversen Element genügt es zu zeigen, dass $h^{-1}g^{-1}$ ein inverses Element von gh ist. Es gilt nämlich

$$(h^{-1}g^{-1})(gh) = h^{-1}((g^{-1}g)h) = h^{-1}(eh) = h^{-1}h = e,$$

und ebenso $(gh)(h^{-1}g^{-1}) = e$.

Notation 1.1.5. Wegen der Assoziativität der Verknupfung in einer Gruppe $(G, \cdot)$, darf man unmissverständlich $g \cdot h \cdot k$ schreiben: Es macht keinen Unterschied, ob wir die Klammern um $g \cdot h$ oder um $h \cdot k$ setzen. Für jede endliche Liste von Elementen $g_1, g_2, \ldots, g_n$ in G darf man allgemeiner das Produkt $g_1 \cdot g_2 \cdot \ldots \cdot g_n$ ohne Klammern schreiben. Man schreibt auch

$$\prod_{i=1}^{n} g_i := g_1 \cdot g_2 \cdot \ldots \cdot g_n.$$

Wenn $n = 0$ verstehen wir immer das „leere Produkt“ als das neutrale Element $e \in G$. Wenn alle Elemente g_i dasselbe Element g sind, schreibt man einfach g^n für das n-fache Produkt von g mit sich selbst. Man setzt auch $g^0 := e$ und $g^{-n} := (g^n)^{-1} = (g^{-1})^n$. So wird die Potenz g^n für alle ganzen Zahlen $n \in \mathbb{Z}$ definiert.

Proposition 1.1.6 (Eigenschaften der Potenzen)**.** *Sei $(G, \cdot)$ eine Gruppe und sei $g \in G$.*

(i) *Für alle $m, n \in \mathbb{Z}$ gilt $g^m \cdot g^n = g^{m+n}$.*

(ii) *Für alle $m, n \in \mathbb{Z}$ gilt $(g^n)^m = g^{mn}$.*

Beweis. Siehe Proposition LA.2.1.7. □

Bemerkung 1.1.7. Sei $(G, \cdot)$ eine Gruppe, $g, h \in G$ und $n \in \mathbb{Z}$. Im Allgemeinen gilt die Gleichheit $(gh)^n = g^n h^n$ nur für $n = 0$ und $n = 1$. Zum Beispiel ist $(gh)^2 = ghgh$ nicht unbedingt gleich $g^2h^2 = gghh$. Die Gleichheit $(gh)^n = g^n h^n$ gilt aber für alle $n \in \mathbb{Z}$, wenn die Gruppe abelsch ist (siehe Definition 1.1.14).

Beispiel 1.1.8 (allgemeine Automorphismengruppen)**.** Sei $\mathcal{C}$ eine Kategorie und $X \in \operatorname{Ob} \mathcal{C}$ ein Objekt. Dann ist die Menge $\operatorname{Aut}_{\mathcal{C}}(X)$ aller Automorphismen von X eine Gruppe bezüglich der Komposition. Diese Gruppe heißt die *Automorphismengruppe* von X (siehe Definition LA.A.1.13).

Bemerkung 1.1.9 (jede Gruppe ist eine Automorphismengruppe)**.** Sei G eine beliebige Gruppe. Dann kann man eine Kategorie $\mathcal{B}G$ bilden, mit einem einzigen Objekt $*$ und mit $\operatorname{Mor}_{\mathcal{B}G}(*, *) = G$, so dass die Kompositionsabbildung

$$\circ\colon \operatorname{Mor}_{\mathcal{B}G}(*, *) \times \operatorname{Mor}_{\mathcal{B}G}(*, *) \to \operatorname{Mor}_{\mathcal{B}G}(*, *)$$

genau die Verknüpfung der Gruppe G ist (siehe Beispiel LA.A.1.4). Für dieses Objekt $*$ gilt dann nach Konstruktion $\operatorname{Aut}_{\mathcal{B}G}(*) = G$.

Beispiel 1.1.10 (symmetrische Gruppen)**.** Sei X eine Menge. Die *symmetrische Gruppe* S_X von X ist die Automorphismengruppe von X in der Kategorie der Mengen. Anders gesagt ist S_X die Menge aller Permutationen (d.h., bijektiven Selbstabbildungen) von X, versehen mit der Komposition. Die Gruppe S_X ist nicht abelsch wenn $|X| \geq 3$ (Proposition LA.2.2.4). Im Spezialfall $X = \{1, \dots, n\}$ mit $n \in \mathbb{N}$ schreibt man S_n anstelle von S_X. Die Gruppe S_n hat genau $n!$ Elementen.

Beispiel 1.1.11 (allgemeine lineare Gruppen)**.** Sei R ein kommutativer Ring und $n \in \mathbb{N}$. Die *allgemeine lineare Gruppe* $\mathrm{GL}_n(R)$ besteht aus aller invertierbaren $n \times n$-Matrizen über R. Die Verknüpfung ist die gewöhnliche Matrixmultiplikation.

Zur Erinnerung kann man $n \times n$-Matrizen mit R-linearen Abbildungen $R^n \to R^n$ auf solche Weise identifizieren, dass die Matrixmultiplikation der Komposition von linearen Abbildungen entspricht. Unter dieser Identifikation ist dann die Gruppe $\mathrm{GL}_n(R)$ genau die Automorphismengruppe von R^n in der Kategorie der R-Moduln.

Beispiel 1.1.12 (Galoisgruppen)**.** Sei $K \subset L$ eine Körpererweiterung (d.h., K und L sind Körper und K ist ein Unterring von L). Die *Galoisgruppe* $\mathrm{Gal}(L \mid K)$ von L über K ist die Automorphismengruppe von L in der Kategorie der K-Algebren. Kongret gesagt besteht $\mathrm{Gal}(L \mid K)$ aus bijektiven Ringhomomorphismen $f\colon L \to L$ mit $f|_K = \mathrm{id}_K$, und die Verknüpfung auf $\mathrm{Gal}(L \mid K)$ ist die gewöhnliche Komposition.

Die *Galoistheorie* stellt eine enge Verbindung zwischen der Struktur einer Körpererweiterung und der Struktur ihrer Galoisgruppe her. Diese Theorie werden wir im Kapitel 3 ausführlich untersuchen. Wir werden zum Beispiel zeigen, dass wenn L eine endliche Erweiterung von K ist (d.h., wenn $\dim_K L < \infty$), dann ist die Galoisgruppe $\mathrm{Gal}(L \mid K)$ endlich und zwar

$$|\mathrm{Gal}(L \mid K)| \leq \dim_K L.$$

Zudem gilt die Gleichheit unter geeigneten Voraussetzungen.

Beispielsweise hat die Galoisgruppe $\mathrm{Gal}(\mathbb{C} \mid \mathbb{R})$ genau zwei Elemente, nämlich die Identität $\mathrm{id}_{\mathbb{C}}$ und die komplexe Konjugation $z \mapsto \bar{z}$. Denn sei $f\colon \mathbb{C} \to \mathbb{C}$ ein $\mathbb{R}$-Algebrenhomomorphismus. Insbesondere ist f eine $\mathbb{R}$-lineare Abbildung, und damit ist f durch $f(1)$ und $f(i)$ eindeutig bestimmt. Da f ein Ringhomomorphismus ist, gilt weiter $f(1) = 1$ und $f(i)^2 = f(i^2) = f(-1) = -1$, d.h., $f(i)$ muss eine Quadratwurzel von -1 sein. Es gibt also nur zwei Möglichkeiten: Entweder $f(i) = i$ und damit $f = \mathrm{id}_{\mathbb{C}}$, oder $f(i) = -i$ und damit $f(z) = \bar{z}$ für alle $z \in \mathbb{C}$.

Beispiel 1.1.13 (Isometriegruppen)**.** Sei (X, d) ein metrischer Raum. Die *Isometriegruppe* $\mathrm{Isom}(X, d)$ ist die Menge aller Isometrien $f\colon X \xrightarrow{\sim} X$ versehen mit der Komposition.

Definition 1.1.14 (abelsche Gruppe)**.** Eine Gruppe $(G, \cdot)$ heißt *abelsch*, falls ihre Verknüpfung *kommutativ* ist, d.h., für alle $g, h \in G$ gilt

$$g \cdot h = h \cdot g.$$

Notation 1.1.15. Bei abelschen Gruppen verwendet man häufig die *additive Notation* statt der *multiplikativen* Notation (Notation 1.1.3): d.h., man schreibt $+$ für die Verknüpfung, 0 für das neutrale Element und $-a$ für das Inverse von a. Man schreibt auch $a-b$ als Abkürzung von $a + (-b)$. Ist $a_1, a_2, \ldots, a_n$ eine Liste von Elementen, so schreibt man

$$\sum_{i=1}^{n} a_i := a_1 + a_2 + \cdots + a_n.$$

Wenn $n = 0$ verstehen wir die „leere Summe“ als das neutrale Element 0. Wenn alle a_i gleich a sind, schreibt man einfach $n \cdot a$ oder na für diese Summe. Man setzt auch $0 \cdot a := 0$ und $(-n) \cdot a := -(n \cdot a)$. So wird $n \cdot a$ für alle ganzen Zahlen $n \in \mathbb{Z}$ definiert.

Im Gegensatz zur multiplikativen Notation ist die Summe $\sum_{i=1}^{n} a_i$ *unabhängig* von der Reihenfolge der Elemente $a_1, \ldots, a_n$, wegen der Kommutativität der Verknüpfung. Das heißt: Für alle Permutationen $\sigma \in S_n$ gilt

$$\sum_{i=1}^{n} a_i = \sum_{i=1}^{n} a_{\sigma(i)}.$$

Bemerkung 1.1.16 (abelsche Gruppen sind $\mathbb{Z}$-Moduln)**.** Sei $(A, +)$ eine abelsche Gruppe. Mit der additiven Notation sagt Proposition 1.1.6, dass für alle $a \in A$ gilt:

(i) Für alle $m, n \in \mathbb{Z}$ gilt $ma + na = (m + n)a$.

(ii) Für alle $m, n \in \mathbb{Z}$ gilt $m(na) = (mn)a$.

Wegen der Kommutativität der Verknüpfung $+$ gilt hier weiter:

(iii) Für alle $a, b \in A$ und $n \in \mathbb{Z}$ gilt $n(a + b) = na + nb$.

Diese Formeln implizieren, dass die abelsche Gruppe A ein $\mathbb{Z}$-Modul ist, mit der Skalarmultiplikation $\mathbb{Z} \times A \to A$, $(n, a) \mapsto na$ (siehe LA.8.1.36).

Beispiel 1.1.17 (Gruppen aus Ringen)**.** Sei $(R, +, \cdot)$ ein Ring. Dann ist $(R, +)$ nach Definition eine abelsche Gruppe, die auch als *additive Gruppe* von R bezeichnet wird. Sei $R^\times \subset R$ die Teilmenge der Einheiten von R. Dann ist $(R^\times, \cdot)$ eine Gruppe, die als *Einheitengruppe* oder *multiplikative Gruppe* von R bezeichnet wird. Die Einheitengruppe $R^\times$ ist abelsch, wenn der Ring R kommutativ ist, aber im Allgemeinen nicht. Zum Beispiel:

(i) Ist K ein Körper, so sind $(K, +)$ und $(K \setminus \{0\}, \cdot)$ abelsche Gruppen.

(ii) Es gilt nach Definition $M_n(R)^\times = \mathrm{GL}_n(R)$.

Gruppen bilden eine Kategorie, in der die Morphismen die Gruppenhomomorphismen sind:

Definition 1.1.18 (Gruppenhomomorphismus)**.** Seien $(G, \cdot)$ und $(H, *)$ zwei Gruppen. Eine Abbildung $f\colon G \to H$ heißt *Gruppenhomomorphismus*, wenn für alle $g, g' \in G$ gilt:

$$f(g \cdot g') = f(g) * f(g').$$

Beispiel 1.1.19.

(i) Seien G und H beliebige Gruppen. Dann ist die konstante Abbildung

$$G \to H, \quad g \mapsto e,$$

ein Gruppenhomomorphismus. Sie heißt der *triviale* Gruppenhomomorphismus von G nach H.

(ii) Sei $n \in \mathbb{Z}$. Die Multiplikationsabbildung

$$\begin{aligned} \mathbb{Z} &\to \mathbb{Z}, \\ x &\mapsto nx, \end{aligned}$$

ist ein Gruppenhomomorphismus. Die sind eigentlich alle Gruppenhomomorphismen von $\mathbb{Z}$ nach $\mathbb{Z}$, denn ein Gruppenhomomorphismus $\mathbb{Z} \to \mathbb{Z}$ ist genau eine $\mathbb{Z}$-lineare Abbildung.

(iii) Ist allgemeiner A eine beliebige *abelsche* Gruppe, so ist die Abbildung

$$\begin{aligned} A &\to A, \\ a &\mapsto na, \end{aligned}$$

ein Gruppenhomomorphismus nach Bemerkung 1.1.16(iii). Für eine beliebige Gruppe G ist aber die Potenzabbildung

$$\begin{aligned} G &\to G, \\ g &\mapsto g^n, \end{aligned}$$

im Allgemeinen *kein* Gruppenhomomorphismus. Seien zum Beispiel $\tau = (1\ 2)$ und $\sigma = (1\ g2\ 3)$ in S_3. Dann gilt

$$(\tau \circ \sigma)^2 = (2\ 3)^2 = \mathrm{id} \quad \text{aber} \quad \tau^2 \circ \sigma^2 = (1\ 3\ 2).$$

(iv) Ist R ein *kommutativer* Ring und ist $n \in \mathbb{Z}$, so its nach (iii) die Potenzabbildung

$$\begin{aligned} R^\times &\to R^\times, \\ r &\mapsto r^n, \end{aligned}$$

ein Gruppenhomomorphismus (da $(R^\times, \cdot)$ eine abelsche Gruppe ist).

(v) Die Exponentialfunktion

$$\exp\colon \mathbb{C} \to \mathbb{C}^\times$$

ist ein Gruppenhomomorphismus von der additiven Gruppe $(\mathbb{C}, +)$ nach der multiplikativen Gruppe $(\mathbb{C}^\times, \cdot)$.

Die Matrixexponentialfunktion (siehe Bemerkung LA.9.2.36)

$$\exp\colon M_n(\mathbb{C}) \to \mathrm{GL}_n(\mathbb{C})$$

ist aber kein Gruppenhomomorphismus wenn $n \geq 2$. Die Gleichheit $\exp(A + B) = \exp(A)\exp(B)$ gilt, wenn A und B miteinander kommutieren, aber nicht im Allgemeinen.

Beispiel 1.1.20 (Vorzeichen und Determinante)**.** Das Vorzeichen und die Determinante sind zwei wichtige Beispiele von Gruppenhomomorphismen:

(i) Sei $n \in \mathbb{N}$. Das Vorzeichen/Signum einer Permutation definiert einen Gruppenhomomorphismus

$$\mathrm{sgn}\colon S_n \to \{\pm 1\}$$

(siehe Satz LA.5.3.5). Dabei ist $\{\pm 1\} = \mathbb{Z}^\times$ die Einheitengruppe vom Ring $\mathbb{Z}$. Zur Erinnerung gilt $\mathrm{sgn}(\sigma) = 1$ genau dann, wenn σ die Komposition einer geraden Anzahl von Transpositionen ist. Die Permutation σ heißt *gerade*, wenn $\mathrm{sgn}(\sigma) = 1$, und *ungerade*, wenn $\mathrm{sgn}(\sigma) = -1$.

(ii) Sei $n \in \mathbb{N}$ und sei R ein kommutativer Ring (z.B. ein Körper). Die Determinante $\det\colon M_n(R) \to R$ erfüllt $\det(I_n) = 1$ und $\det(AB) = \det(A)\det(B)$ für alle Matrizen $A, B \in M_n(R)$. Desewegen ist ihre Einschränkung

$$\det\colon \mathrm{GL}_n(R) \to R^\times$$

ein Gruppenhomomorphismus.

(iii) Die Beispiele (i) und (ii) hängen folgendermaße zusammen. Für jedes $\sigma \in S_n$ sei $P_\sigma \in \mathrm{GL}_n(R)$ die Permutationsmatrix mit $(P_\sigma)_{ij} = \delta_{i\sigma(j)}$. Die entsprechende lineare Abbildung $L_{P_\sigma}\colon R^n \to R^n$ bildet den Standardeinheitsvektor e_i auf $e_{\sigma(i)}$ ab. Die Abbildung

$$P\colon S_n \to \mathrm{GL}_n(R), \quad \sigma \mapsto P_\sigma,$$

ist dann ein Gruppenhomomorphismus (d.h., $P_{\sigma\circ\tau} = P_\sigma \cdot P_\tau$), und es gibt ein kommutatives Quadrat

$$\begin{array}{ccc} S_n & \xrightarrow{P} & \mathrm{GL}_n(R) \\ {\scriptstyle \mathrm{sgn}}\downarrow & & \downarrow{\scriptstyle \det} \\ \{\pm 1\} & \longrightarrow & R^\times. \end{array}$$

Falls $1 \neq 0$ in R (d.h., falls $R \neq \{0\}$), ist zudem die Abbildung P injektiv.

Proposition 1.1.21 (Rechnen mit Gruppenhomomorphismen)**.** *Sei $f\colon G \to H$ ein Gruppenhomomorphismus.*

(i) *Es gilt $f(e) = e$. (Dabei ist das erste e das neutrale Element von G und das zweite das von H.)*

(ii) *Für alle $g \in G$ gilt $f(g^{-1}) = f(g)^{-1}$, d.h., $f(g^{-1})$ ist das Inverse von $f(g)$ in H.*

(iii) *Für alle $g \in G$ und $n \in \mathbb{Z}$ gilt $f(g^n) = f(g)^n$.*

Beweis. Zu (i). Sei $h = f(e)$. Dann gilt

$$h = f(e) = f(e \cdot e) = f(e) \cdot f(e) = h \cdot h.$$

Multipliziert man von links mit h^{-1}, so erhalten wir

$$e = h^{-1} \cdot h = h^{-1} \cdot (h \cdot h) = (h^{-1} \cdot h) \cdot h = e \cdot h = h.$$

Zu (ii). Nach Definition des Inversen $f(g)^{-1}$ muss man zeigen, dass $f(g^{-1}) \cdot f(g) = e = f(g) \cdot f(g^{-1})$. Nach (i) gilt

$$f(g^{-1}) \cdot f(g) = f(g^{-1} \cdot g) = f(e) = e,$$

und ebenso $f(g) \cdot f(g^{-1}) = e$.

Zu (iii). Die Aussage ist trivial für $n = 1$. Für $n = 0$ ist die Aussage genau (i), und für $n = -1$ ist sie genau (ii). Nach Definition der Potenz g^n bleibt es zu zeigen, dass für $n \geq 2$ gilt $f(g^n) = f(g)^n$. Dies folgt aber unmittelbar aus der Definition von Gruppenhomomorphismus. □

Proposition 1.1.22 (Gruppenhomomorphismen und Komposition)**.** *Seien G, H, K Gruppen.*

(i) *Die Identität $\mathrm{id}_G\colon G \to G$ ist ein Gruppenhomomorphismus.*

(ii) *Sind $f\colon G \to H$ und $f'\colon H \to K$ Gruppenhomomorphismen, so ist $f' \circ f$ ein Gruppenhomomorphismus.*

Beweis. Beide Aussagen sind klar. □

Nach Proposition 1.1.22 bilden Gruppen und Gruppenhomomorphismen eine Kategorie $\mathcal{G}\mathrm{rp}$:

- $\mathrm{Ob}\,\mathcal{G}\mathrm{rp}$ ist die Klasse von Gruppen.
- Sind G und H Gruppen, so ist $\mathrm{Mor}_{\mathcal{G}\mathrm{rp}}(G,H)$ die Menge aller Gruppenhomomorphismen von G nach H.
- Die Komposition $\circ\colon \mathrm{Mor}_{\mathcal{G}\mathrm{rp}}(G,H)\times\mathrm{Mor}_{\mathcal{G}\mathrm{rp}}(H,K)\to\mathrm{Mor}_{\mathcal{G}\mathrm{rp}}(G,K)$ ist die gewöhnliche Komposition von Abbildungen.
- Die Identitätsmorphismus einer Gruppe G ist die Identitätsabbildung id_G.

Dementsprechend erhalten wir den Begriff von *Isomorphismus* zwischen Gruppen (Definition LA.A.1.7) und zusammenhängende Begriffe:

Definition 1.1.23 (Isomorphismus, Automorphismus, isomorph)**.** Ein Gruppenhomomorphismus $f\colon G\to H$ heißt *Gruppenisomorphismus* oder einfach *Isomorphismus*, wenn ein Gruppenhomomorphismus $g\colon H\to G$ existiert mit

$$g\circ f=\mathrm{id}_G\quad\text{und}\quad f\circ g=\mathrm{id}_H$$

Man schreibt $f\colon G\xrightarrow{\sim}H$, wenn f ein Isomorphismus ist. Wenn $G=H$ spricht man von einem *Automorphismus* von G.

Man sagt, dass zwei Gruppen G und H *isomorph* sind, und man schreibt $G\cong H$, wenn ein Isomorphismus von G nach H existiert. Nach Proposition LA.A.1.9 ist Isomorphie eine Äquivalenzrelation auf der Klasse der Gruppen.

Beispiel 1.1.24.

(i) Bis auf Isomorphie gibt es genau eine Gruppe mit 1 Element, die als *triviale Gruppe* bezeichnet wird. Da das einzige Element zwangsläufig das neutrale Element ist, schreibt man je nach Kontext $\{e\}$, $\{1\}$ oder $\{0\}$ für diese Gruppe.

(ii) Der Gruppenhomomorphismus $\mathbb{Z}\to\mathbb{Z}$, $x\mapsto nx$, aus Beispiel 1.1.19(i) ist genau dann ein Automorphismus, wenn $n=1$ oder $n=-1$. Die Gruppe $\mathbb{Z}$ hat also genau zwei Automorphismen.

(iii) Auf $\mathbb{R}$ eingeschränkt induziert die Exponentialfunktion $\exp\colon\mathbb{C}\to\mathbb{C}^\times$ ein Gruppenisomorphismus zwischen $(\mathbb{R},+)$ und $(\mathbb{R}_{>0},\cdot)$, mit Umkehrisomorphismus

$$\log\colon\mathbb{R}_{>0}\to\mathbb{R}.$$

Beispiel 1.1.25 (Konjugation)**.** Sei G eine Gruppe und sei $g\in G$. Die Abbildung

$$c_g\colon G\to G,\quad x\mapsto gxg^{-1},$$

heißt die *Konjugationsabbildung* bzgl. g. Man rechnet leicht nach, dass c_g ein Gruppenhomomorphismus ist, dass $c_e=\mathrm{id}_G$, und dass $c_{g\cdot h}=c_g\circ c_h$. Insbesondere ist $c_{g^{-1}}$ eine Umkehrabbildung zu c_g, und damit ist c_g ein Automorphismus der Gruppe G. Zwei Elemente $x,y\in G$ heißen *konjugiert*, wenn ein $g\in G$ mit $y=c_g(x)$ existiert.

Man bemerkt, dass eine Gruppe G genau dann abelsch ist, wenn für alle $g\in G$ gilt $c_g=\mathrm{id}_G$. Insbesondere sind konjugierte Elemente einer abelschen Gruppe gleich.

Die folgende Proposition kennen wir schon bei Vektorräumen und Moduln (Proposition LA.4.1.17) und bei Ringen (Proposition LA.8.1.25):

Proposition 1.1.26. *Sei $f\colon G \to H$ ein Gruppenhomomorphismus. Die folgenden Aussagen sind äquivalent:*

(i) *f ist ein Isomorphismus.*

(ii) *f ist bijektiv.*

Beweis. Die Implikation (i) $\Rightarrow$ (ii) ist klar. Um die Implikation (ii) $\Rightarrow$ (i) zu zeigen, muss man nachprüfen, dass die Umkehrabbildung f^{-1} von f ein Gruppenhomomorphismus ist. Seien $h, h' \in H$, $g = f^{-1}(h)$ und $g' = f^{-1}(h')$. Es gilt dann $f(g) = h$ und $f(g') = h'$, und somit $f(gg') = hh'$, da f ein Gruppenhomomorphismus ist. Anders gesagt gilt $f^{-1}(hh') = gg' = f^{-1}(h)f^{-1}(h')$, d.h., f^{-1} ist ein Gruppenhomomorphismus. □

Beispiel 1.1.27.

(i) Die Einheitengruppe $\mathbb{Z}^\times = \{\pm 1\}$ ist isomorph zu $\mathbb{Z}/2\mathbb{Z}$ durch den Isomorphismus

$$\mathbb{Z}/2\mathbb{Z} \to \mathbb{Z}^\times, \quad n + 2\mathbb{Z} \mapsto (-1)^n.$$

(ii) Die Einheitengruppe $\mathbb{Z}[i]^\times$ der Gaußschen Zahlen hat vier Elemente ± 1 und $\pm i$. Sie ist isomorph zu $\mathbb{Z}/4\mathbb{Z}$ durch den Isomorphismus

$$\mathbb{Z}/4\mathbb{Z} \to \mathbb{Z}[i]^\times, \quad n + 4\mathbb{Z} \mapsto i^n.$$

(iii) Sei p eine Primzahl. Wir werden später zeigen, dass die Einheitengruppe

$$\mathbb{F}_p^\times = \{[1], \ldots, [p-1]\}$$

zu $\mathbb{Z}/(p-1)\mathbb{Z}$ isomorph ist. Diese Aussage ist nicht offensichtlich. Zum Beispiel ist

$$\mathbb{Z}/4\mathbb{Z} \to \mathbb{F}_5^\times, \quad n + 4\mathbb{Z} \mapsto [3^n],$$

ein Gruppenisomorphismus, wie man leicht nachrechnen kann. Im Allgemeinen ist es aber schwierig, einen expliziten Isomorphismus zwischen $\mathbb{F}_p^\times$ und $\mathbb{Z}/(p-1)\mathbb{Z}$ zu finden.

Definition 1.1.28 (Kern, Bild)**.** Sei $f\colon G \to H$ ein Gruppenhomomorphismus.

- Der *Kern* von f ist die Teilmenge

$$\ker f = f^{-1}(\{e\}) = \{g \in G \mid f(g) = e\} \subset G.$$

- Das *Bild* von f ist die Teilmenge

$$\operatorname{im} f = f(G) = \{h \in H \mid \text{es gibt ein } g \in G \text{ mit } f(g) = h\} \subset H.$$

Proposition 1.1.29. *Sei $f\colon G \to H$ ein Gruppenhomomorphismus.*

(i) *f ist genau dann injektiv, wenn* $\ker f = \{e\}$.

(ii) *f ist genau dann surjektiv, wenn* $\operatorname{im} f = H$.

Beweis. Aussage (ii) ist genau die Definition der Surjektivität. Ist f injektiv, so hat e höchstens ein Urbild unter f. Es gilt aber $f(e) = e$ nach Proposition 1.1.21(i), und damit $\ker f = \{e\}$. Sei umgekehrt $\ker f = \{e\}$ und seien $x, y \in G$ mit $f(x) = f(y)$. Nach Proposition 1.1.21(i,ii) gilt

$$f(xy^{-1}) = f(x)f(y)^{-1} = e.$$

Damit liegt xy^{-1} im Kern von f. Nach Voraussetzung ist dann $xy^{-1} = e$. Multipliziert man von rechts mit y, so erhalten wir $x = y$. Also ist f injektiv. □

Proposition 1.1.30 (universelle Eigenschaft der Gruppe $\mathbb{Z}$)**.** *Sei G eine Gruppe und $g \in G$ ein Element. Dann gibt es* genau einen *Gruppenhomomorphismus $f\colon \mathbb{Z} \to G$ mit $f(1) = g$.*

Beweis. Ein solcher Gruppenhomomorphismus muss ein beliebiges $n \in \mathbb{Z}$ auf g^n abbilden, nach Proposition 1.1.21(iii). Also ist f eindeutig bestimmt. Zur Existenz muss man nachprüfen, dass die Abbildung $n \mapsto g^n$ ein Gruppenhomomorphismus von $\mathbb{Z}$ nach G ist. Dies ist genau der Inhalt von Proposition 1.1.6(i). □

Bemerkung 1.1.31. Proposition 1.1.30 sagt, dass die Gruppe $\mathbb{Z}$ den Vergissfunktor $\mathcal{G}\mathrm{rp} \to \mathcal{S}\mathrm{et}$ darstellt (siehe Definition LA.A.3.7).

1.1.2 Untergruppen

Definition 1.1.32 (Untergruppe)**.** Sei $(G, \cdot)$ eine Gruppe. Eine Teilmenge $H \subset G$ heißt *Untergruppe* von G, wenn sich die Abbildung $\cdot\colon G \times G \to G$ zu einer Abbildung $H \times H \to H$ so einschränkt, dass H mit dieser eingeschränkten Verknüpfung eine Gruppe ist. Man schreibt auch $H < G$, wenn H eine Untergruppe von G ist.

Proposition 1.1.33 (Kriterium für Untergruppen)**.** *Sei G eine Gruppe. Eine Teilmenge $H \subset G$ ist genau dann eine Untergruppe, wenn folgende drei Bedingungen erfüllt sind:*

(i) *H ist nicht leer.*

(ii) *Für alle $x, y \in H$ gilt $xy \in H$.*

(iii) *Für alle $x \in H$ gilt $x^{-1} \in H$.*

Außerdem gilt in diesem Fall $e \in H$.

Beweis. Sei H eine Untergruppe von G. Nach Definition sind die Bedingungen (i) und (ii) erfüllt. Weiter ist die Inklusionsabbildung $i\colon H \to G$ ein Gruppenhomomorphismus. Ist $x \in H$ und ist $y \in H$ das Inverse von x in H, so gilt $i(y) = i(x)^{-1}$ nach Proposition 1.1.21(ii). Also ist die Bedingung (iii) auch erfüllt.

Sei umgekehrt $H \subset G$ eine Teilmenge, die die Bedingungen (i)–(iii) erfüllt. Nach (ii) schränkt sich die Verknüpfung auf G zu einer Verknüpfung $\cdot\colon H \times H \to H$ ein. Diese Verknüpfung ist dann automatisch assoziativ. Nach (i) gibt es mindestens ein Element $x \in H$. Dann gilt auch $x^{-1} \in H$ nach (iii), und damit $e = xx^{-1} \in H$ nach (ii). Insbesondere ist e ein neutrales Element in H. Die Existenz von inversen Elementen in H folgt nun aus (iii). □

Bemerkung 1.1.34 (Transitivität von Untergruppen)**.** Sei G eine Gruppe, $H < G$ eine Untergruppe und $K \subset H$ eine weitere Teilmenge. Dann gilt $K < G$ genau dann, wenn $K < H$.

Beispiel 1.1.35 (generische Beispiele)**.**

(i) Sei G eine Gruppe. Dann sind G und $\{e\}$ stets Untergruppen von G. Die Untergruppe $\{e\}$ heißt die *triviale Untergruppe* von G.

(ii) Sei $f\colon G \to H$ ein Gruppenhomomorphismus. Dann ist $\ker f$ eine Untergruppe von G und $\operatorname{im} f$ eine Untergruppe von H. Dies kann man leicht mit dem Kriterium 1.1.33 nachrechnen.

Allgemeiner ist das Urbild unter f einer Untergruppe von H eine Untergruppe von G, und das Bild unter f einer Untergruppe von G eine Untergruppe von H.

(iii) Sei $H < G$ eine Untergruppe und sei $g \in G$. Dann ist

$$gHg^{-1} := \{ghg^{-1} \mid h \in H\} \subset G$$

wieder eine Untergruppe von G. Sie ist nämlich das Bild von H unter der Konjugationsabbildung c_g aus Beispiel 1.1.25. Eine Untergruppe von G der Form gHg^{-1} heißt *konjugierte Untergruppe* zu H.

Beispiel 1.1.36 (alternierende Gruppen)**.** Sei $n \in \mathbb{N}$. Die *alternierende Gruppe* $A_n \subset S_n$ ist nach Definition der Kern des Gruppenhomomorphismus $\operatorname{sgn}\colon S_n \to \{\pm 1\}$, d.h., die Menge aller geraden Permutationen von $\{1, \dots, n\}$ (siehe Beispiel 1.1.20).

Beispiel 1.1.37 (spezielle lineare Gruppen)**.** Sei R ein kommutativer Ring und $n \in \mathbb{N}$. Die *spezielle lineare Gruppe* $\mathrm{SL}_n(R) \subset \mathrm{GL}_n(R)$ ist der Kern des Gruppenhomomorphismus $\det\colon \mathrm{GL}_n(R) \to R^\times$, d.h., die Menge aller $n \times n$-Matrizen A mit $\det(A) = 1$.

Bemerkung 1.1.38. Sei R ein kommutativer Ring und $n \in \mathbb{N}$. Aus Beispiel 1.1.20(iii) folgt, dass sich der Gruppenhomomorphismus $S_n \to \mathrm{GL}_n(R)$, $\sigma \mapsto P_\sigma$, zu einem Gruppenhomomorphismus

$$A_n \to \mathrm{SL}_n(R), \quad \sigma \mapsto P_\sigma,$$

einschränkt.

Beispiel 1.1.39 (othogonale/unitäre Gruppen)**.** Sei $n \in \mathbb{N}$.

(i) Die orthogonale Gruppe

$$\mathrm{O}(n) = \{A \in \mathrm{GL}_n(\mathbb{R}) \mid A^{-1} = A^\intercal\}$$

ist eine Untergruppe von $\mathrm{GL}_n(\mathbb{R})$ (die Einheitsmatrix ist orthogonal, das Produkt zweier orthogonalen Matrizen ist orthogonal und das Inverse einer orthogonalen Matrix ist orthogonal). Die spezielle orthogonale Gruppe $\mathrm{SO}(n) = \mathrm{O}(n) \cap \mathrm{SL}_n(\mathbb{R})$ ist eine weitere Untergruppe davon.

(ii) Die unitäre Gruppe

$$\mathrm{U}(n) = \{A \in \mathrm{GL}_n(\mathbb{C}) \mid A^{-1} = A^\mathsf{H}\}$$

ist eine Untergruppe von $\mathrm{GL}_n(\mathbb{C})$. Die spezielle unitäre Gruppe $\mathrm{SU}(n) = \mathrm{U}(n) \cap \mathrm{SL}_n(\mathbb{C})$ ist eine weitere Untergruppe davon.

Beispiel 1.1.40 (Isometrien mit gegebenem Fixpunkt)**.** Sei (X, d) ein metrischer Raum und sei $x \in X$ ein Punkt. Dann ist die Menge

$$\mathrm{Isom}_x(X, d) = \{f \in \mathrm{Isom}(X, d) \mid f(x) = x\}$$

eine Untergruppe der Isometriegruppe $\mathrm{Isom}(X, d)$. Für den euklidischen Raum $\mathbb{R}^n$ gibt es einen Gruppenisomorphismus

$$\mathrm{O}(n) \xrightarrow{\sim} \mathrm{Isom}_0(\mathbb{R}^n), \quad A \mapsto L_A.$$

Das heißt, jede Isometrie von $\mathbb{R}^n$, die 0 auf 0 abbildet, ist linear (siehe Bemerkung LA.7.2.53).

Beispiel 1.1.41 (Diedergruppe)**.** Sei $n \geq 1$. Sei $\rho_n \in \mathrm{Isom}_0(\mathbb{R}^2)$ die Drehung um den Winkel $2\pi/n$, und sei $\sigma \in \mathrm{Isom}_0(\mathbb{R}^2)$ die Spiegelung $(x, y) \mapsto (x, -y)$. Dann ist

$$D_n = \{\mathrm{id}_{\mathbb{R}^2} = \rho_n^0, \rho_n, \dots, \rho_n^{n-1}, \sigma, \sigma\rho_n, \dots, \sigma\rho_n^{n-1}\}$$

eine Teilmenge von $\mathrm{Isom}_0(\mathbb{R}^2)$ mit $2n$ Elementen. Es gilt $\sigma^i \rho_n^j \in D_n$ für alle $i, j \in \mathbb{Z}$, denn $\sigma^2 = \rho_n^n = \mathrm{id}_{\mathbb{R}^2}$ (insbesondere: $\sigma^{-1} = \sigma$ und $\rho_n^{-1} = \rho_n^{n-1}$). Aus der Gleichheit

$$\rho_n \sigma = \sigma \rho_n^{-1}$$

folgt leicht, dass die Komposition zweier Elemente von D_n sowie das Inverse eines Elements von D_n wieder in D_n liegen. Deswegen ist D_n eine Untergruppe von $\mathrm{Isom}_0(\mathbb{R}^2)$, die als n-te *Diedergruppe* bezeichnet wird. Wenn $n \geq 3$ ist die Gruppe D_n nicht abelsch, denn $\rho_n \sigma = \sigma \rho_n^{-1} \neq \sigma \rho_n$.

Mann kann auch die Teilmenge D_n auf geometrische Weise charakterisieren: Sie besteht genau aus den linearen Isometrien von $\mathbb{R}^2$, die das reguläre n-Eck E_n mit Ecken $\rho_n^i(1, 0)$ auf sich selbst abbildet (falls $n \geq 3$ kann man sogar D_n mit der Isometriegruppe von E_n identifizieren).

Wie bei Vektorräumen kann mann eine Untergruppe aus einer beliebigen Teilmenge erzeugen. Dazu muss man zunächst bemerken, dass der Durchscnitt einer Familie von Untergruppen wieder eine Untergruppe ist:

Proposition 1.1.42 (Durchschnitt von Untergruppen)**.** *Sei G eine Gruppe und $(H_i)_{i\in I}$ eine Familie von Untergruppen von G. Dann ist $\bigcap_{i\in I} H_i$ wieder eine Untergruppe von G.*

Beweis. Dies folgt unmittelbar aus dem Kriterium 1.1.33. □

Definition 1.1.43 (erzeugte Untergruppe, Erzeugendensystem)**.** Sei G eine Gruppe und $S \subset G$ eine Teilmenge.

- Die *von S erzeugte Untergruppe* von G ist die Untergruppe

$$\langle S\rangle := \bigcap_{H\in\mathfrak{U}(S)} H \subset G,$$

  wobei $\mathfrak{U}(S)$ die Menge aller Untergruppen $H \subset G$ mit $S \subset H$ ist. Nach Proposition 1.1.42 ist $\langle S\rangle$ eine Untergruppe von G, und zwar die kleinste Untergruppe, die S enthält.

- Die Menge S heißt *Erzeugendensystem* von G, falls $\langle S\rangle = G$.

Bemerkung 1.1.44. Im Allgemeinen ist die Vereinigung einer Familie $(H_i)_{i\in I}$ von Untergruppen von G *keine* Untergruppe von G. Es gibt trotzdem eine kleinste Untergruppe von G, die alle Untergruppen H_i enthält, nämlich die von der Vereinigung erzeugte Untergruppe $\langle\bigcup_{i\in I} H_i\rangle$.

Proposition 1.1.45 (explizite Beschreibung erzeugter Untergruppen)**.** *Sei G eine Gruppe und $S \subset G$ eine Teilmenge. Dann gilt*

$$\langle S\rangle = \{s_1^{\varepsilon_1}\cdot\ldots\cdot s_n^{\varepsilon_n} \mid n\in\mathbb{N},\ s_i\in S,\ \varepsilon_i\in\{\pm 1\}\}.$$

(Dabei ist das leere Produkt gleich e, nach Notation 1.1.5.)

In der Gruppentheorie nennt man oft einen Ausdruck $s_1^{\varepsilon_1}\cdot\ldots\cdot s_n^{\varepsilon_n}$ wie in der obigen Proposition ein *Wort* in S. Die von S erzeugte Untergruppe besteht also aus allen Wörtern in S.

Beweis. Analog zum Beweis für erzeugte Untervektorräume (Proposition LA.3.2.18). Jedes Wort $s_1^{\varepsilon_1}\cdot\ldots\cdot s_n^{\varepsilon_n}$ liegt in jeder Untergruppe, die S enthält, also liegt in $\langle S\rangle$. Um die umgekehrte Inklusion zu beweisen, genügt es zu bemerken, dass die rechte Seite eine Untergruppe von G ist. Dies folgt leicht aus dem Kriterium 1.1.33 (zum Beispiel ist das Inverse von $s_1^{\varepsilon_1}\cdot\ldots\cdot s_n^{\varepsilon_n}$ gleich $s_n^{-\varepsilon_n}\cdot\ldots\cdot s_1^{-\varepsilon_1}$). □

Definition 1.1.46 (endlich erzeugt, zyklisch)**.** Eine Gruppe G heißt:

- *endlich erzeugt*, wenn sie ein endliches Erzeugendensystem besitzt.
- *zyklisch*, wenn sie ein einelementiges Erzeugendensystem besitzt.

Bemerkung 1.1.47. Sei A eine abelsche Gruppe. Dann gibt es keinen Unterschied zwischen Untergruppen von A und $\mathbb{Z}$-Untermoduln von A. Deswegen ist eine abelsche Gruppe genau dann endlich erzeugt bzw. zyklisch im Sinne der Definition 1.1.46, wenn sie als $\mathbb{Z}$-Modul endlich erzeugt bzw. zyklisch ist.

Beispiel 1.1.48.

(i) Jede endliche Gruppe G ist endlich erzeugt, da G selbst ein Erzeugendensystem von G ist.

(ii) Nach Konstruktion ist $\{\rho_n, \sigma\}$ ein Erzeugendensystem der Diedergruppe D_n.

(iii) Jede Permutation in S_n ist ein Produkt von Transpositionen (Lemma LA.5.3.4). Insbesondere ist die Teilmenge der Transpositionen ein Erzeugendensystem von S_n.

(iv) Die nicht-abelsche Gruppe $\mathrm{GL}_2(\mathbb{Z})$ ist endlich erzeugt, und zwar bilden die Matrizen

$$V_{12} = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \quad M_1(-1) = \begin{pmatrix} -1 & 0 \\ 0 & 1 \end{pmatrix}, \quad A_{12}(1) = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$$

ein Erzeugendensystem von $\mathrm{GL}_2(\mathbb{Z})$. Dies folgt aus der Theorie der Smith-Normalform: Da $\mathbb{Z}$ ein euklidischer Ring ist, ist jede Matrix in $\mathrm{GL}_n(\mathbb{Z})$ ein Produkt von Elementarmatrizen (Bemerkung LA.8.3.22). Falls $n = 2$ kann man leicht nachprüfen, dass jede Elementarmatrix als Wort in den obigen drei Matrizen geschrieben werden kann.

Beispiel 1.1.49 (zyklische Gruppen)**.**

(i) Die Gruppe $\mathbb{Z}$ ist zyklisch, von dem Element 1 (oder auch -1) erzeugt.

(ii) Sei $n \in \mathbb{N} \setminus \{0\}$. Dann ist die endliche Gruppe $\mathbb{Z}/n\mathbb{Z}$ zyklisch mit erzeugendem Element $1 + n\mathbb{Z}$.

Wir zeigen später, dass jede zyklische Gruppe zu entweder (i) oder (ii) isomorph ist (Korollar 1.1.79).

1.1.3 Nebenklassen und der Satz von Lagrange

Definition 1.1.50 (Nebenklasse, Quotient, Index)**.** Sei G eine Gruppe und $H < G$ eine Untergruppe.

- Sei $g \in G$. Die Teilmenge
$$gH = \{gh \mid h \in H\} \subset G$$
heißt die *Linksnebenklasse* von g bzgl. H.

  Man schreibt $G/H = \{gH \mid g \in G\}$ für die Menge aller Linksnebenklassen bzgl. H, die als *Quotient* von G nach H bezeichnet wird.

- Der *Index* $[G : H]$ von H in G ist die Mächtigkeit des Quotienten G/H:
$$[G : H] = |G/H|.$$

Beispiel 1.1.51. Für alle Gruppen G gelten $G/G = \{G\}$ und $G/\{e\} = \{\{g\} \mid g \in G\}$. Insbesondere:
$$[G : G] = 1 \quad \text{und} \quad [G : \{e\}] = |G|.$$

Bemerkung 1.1.52 (Nebenklassen als Äquivalenzklassen)**.** Sei G eine Gruppe und $H < G$ eine Untergruppe. Man definiert eine Relation $\sim_H$ auf G wie folgt:
$$g_1 \sim_H g_2 \iff g_2^{-1} g_1 \in H \iff g_1 \in g_2 H.$$
Man kann leicht nachrechnen, dass $\sim_H$ eine Äquivalenzrelation auf G ist. Nach Definition ist die Äquivalenklasse von g bzgl. $\sim_H$ genau die Linksnebenklasse gH von g. Damit ist die Quotientenmenge $G/\sim_H$ genau die Menge G/H der Linksnebenklassen. Dies zeigt, dass die Menge G/H eine *Partition* von G ist (Proposition LA.1.4.6), d.h., G ist die *disjunkte* Vereinigung ihrer Linksnebenklassen bzgl. H.

Beispiel 1.1.53 (Linksnebenklassen in abelschen Gruppen)**.** Sei A eine abelsche Gruppe und $B \subset A$ eine Untergruppe. Die Linksnebenklasse von $a \in A$ ist dann die Teilmenge $a + B \subset A$. Der Quotient A/B im Sinne der Definition 1.1.50 ist also der bekannte Quotient des $\mathbb{Z}$-Moduls A nach dem Untermodul B. Beispielsweise sind die Linksnebenklassen bzgl. $n\mathbb{Z}$ in $\mathbb{Z}$ die gewöhnlichen Restklassen modulo n.

Beispiel 1.1.54. Sei $H = \{\mathrm{id}, (1\ 2)\} < S_3$. Die Linksnebenklassen bzgl. H sind folgende:

$$\begin{aligned} \mathrm{id}\, H = (1\ 2)H &= \{\mathrm{id}, (1\ 2)\}, \\ (1\ 2\ 3)H = (1\ 3)H &= \{(1\ 2\ 3), (1\ 3)\}, \\ (1\ 3\ 2)H = (2\ 3)H &= \{(1\ 3\ 2), (2\ 3)\}. \end{aligned}$$

Damit ist der Index von H in S_3 gleich 3.

Satz 1.1.55 (Satz von Lagrange)**.** *Sei G eine Gruppe und seien $H < G$ und $K < H$ Untergruppen mit $[G : H] < \infty$ und $[H : K] < \infty$. Dann ist auch $[G : K]$ endlich und es gilt*

$$[G : K] = [G : H] \cdot [H : K].$$

Beweis. Wir betrachten die Quotientenabbildung

$$q \colon G \to G/H, \quad q(g) = gH,$$

und die Äquivalenzrelation $\sim_K$ auf G (Bemerkung 1.1.52). Aus $K \subset H$ folgt:

$$g_1 \sim_K g_2 \iff g_1 \in g_2 K \implies g_1 \in g_2 H \iff q(g_1) = q(g_2).$$

Nach der universellen Eigenschaft der Quotientenmenge (Satz LA.1.4.10) erhalten wir eine induzierte Abbildung

$$\bar{q} \colon G/K \to G/H, \quad \bar{q}(gK) = gH.$$

Damit können wir G/K als disjunkte Vereinigung der Urbilder unter $\bar{q}$ der Elemente von G/H darstellen:

$$G/K = \bigcup_{N \in G/H} \bar{q}^{-1}(\{N\}),$$

so dass

$$[G : K] = \sum_{N \in G/H} |\bar{q}^{-1}(\{N\})|.$$

Es genügt also zu zeigen, dass für jede Linksnebenklasse $N \in G/H$ gilt

$$|\bar{q}^{-1}(\{N\})| = [H : K].$$

Sei $g \in G$ mit $N = gH$. Wir betrachten nun die Abbildung

$$r_g \colon H \to \bar{q}^{-1}(\{gH\}), \quad r_g(h) = ghK.$$

Dies ist wohldefiniert, denn $\bar{q}(ghK) = ghH = gH$. Ist $h_1 \sim_K h_2$, so gilt $h_1 K = h_2 K$ und damit $gh_1 K = gh_2 K$. Nach der universellen Eigenschaft der Quotientenmenge erhalten wir eine induzierte Abbildung

$$\bar{r}_g \colon H/K \to \bar{q}^{-1}(\{gH\}), \quad \bar{r}_g(hK) = ghK.$$

Es bleibt zu zeigen, dass $\bar{r}_g$ bijektiv ist:

- *Injektivität.* Seien $hK, h'K \in H/K$ mit $\bar{r}_g(hK) = \bar{r}_g(h'K)$, d.h., $ghK = gh'K$. Multiplikation mit g^{-1} von links liefert $hK = h'K$, so dass $\bar{r}_g$ injektiv ist.
- *Surjektivität.* Sei $g'K \in \bar{q}^{-1}(\{gH\})$, d.h., $g'H = gH$. Dann ist $g^{-1}g'$ ein Element von H, und es gilt
$$\bar{r}_g(g^{-1}g'K) = gg^{-1}g'K = g'K,$$
so dass $\bar{r}_g$ surjektiv ist. □

Korollar 1.1.56 (Mächtigkeit von Untergruppen)**.** *Sei G eine endliche Gruppe und $H < G$ eine Untergruppe. Dann gilt $|G| = [G : H] \cdot |H|$. Insbesondere ist $|G|$ durch $|H|$ teilbar.*

Beweis. Dies folgt aus Satz 1.1.55 mit $K = \{e\}$. □

Korollar 1.1.57 (primmächtige Gruppen sind zyklisch)**.** *Sei G eine endliche Gruppe, deren Mächtigkeit $|G|$ eine Primzahl ist. Dann ist G zyklisch.*

Beweis. Aus dem Korollar 1.1.56 folgt, dass G und $\{e\}$ die einzigen Untergruppen von G sind. Insbesondere gilt $\langle g \rangle = G$ für alle $g \in G \setminus \{e\}$. □

Beispiel 1.1.58. Seien $p \neq q$ Primzahlen und sei G eine endliche Gruppe mit pq Elementen. Dann ist jede Untergruppe $H \lneq G$ zyklisch, denn: Nach dem Satz von Lagrange gilt $|H| \in \{1, p, q\}$, und aus Korollar 1.1.57 folgt dann, dass H zyklisch ist.

Bemerkung 1.1.59 (Links- und Rechtsnebenklassen)**.** Auf symmetrische Weise heißt

$$Hg = \{hg \mid h \in H\} \subset G$$

die *Rechtsnebenklasse* von g bzgl. H, und man schreibt $H\backslash G$ für die Menge aller Rechtsnebenklassen bzgl. H. Wenn G abelsch ist gilt natürlich $gH = Hg$ und $G/H = H\backslash G$, aber im Allgemeinen sind beide Gleichheiten falsch. Es gibt aber eine kanonische Bijektion

$$G/H \to H\backslash G, \quad gH \mapsto Hg^{-1},$$

so dass G/H und $H\backslash G$ gleichmächtig sind.

1.1.4 Normalteiler und Quotientengruppen

Bei Moduln über einem Ring kann man bekanntlich zu jedem Untermodul $N \subset M$ einen Quotientenmodul M/N definieren (Proposition LA.3.2.23). Es gibt eine kanonische lineare Abbildung

$$q \colon M \to M/N,$$

die surjektiv ist und deren Kern genau gleich N ist. Insbesondere gilt dies bei $\mathbb{Z}$-Moduln, d.h., abelschen Gruppen. Der Quotient M/N ist genau die Menge der Linksnebenklassen bzgl. N in M, und die Abbildung q bildet jedes Element $x \in M$ auf seine Linksnebenklasse $x + N$.

Eine natürliche Frage ist nun, ob diese Konstruktion bei beliebigen Gruppen sinnvoll bleibt. Das heißt: Ist G eine Gruppe und $H < G$ eine Untergruppe, gibt es auf der Menge G/H der Linksnebenklassen eine solche Gruppenstruktur, dass die Quotientenabbildung $q \colon G \to G/H$ ein Gruppenhomomorphismus wird? Die folgende Proposition gibt eine vollständige Antwort:

Proposition 1.1.60 (Existenz von Quotientengruppen)**.** *Sei G eine Gruppe, $H < G$ eine Untergruppe und $q \colon G \to G/H$ die Quotientenabbildung. Dann sind die folgenden Bedingungen äquivalent:*

(i) *Für jedes $g \in G$ und jedes $h \in H$ gilt $ghg^{-1} \in H$.*

(ii) *Für jedes $g \in G$ gilt $gH = Hg$.*

(iii) *Es gibt eine Verknüpfung*

$$\cdot \colon G/H \times G/H \to G/H,$$

so dass $(G/H, \cdot)$ eine Gruppe ist und q ein Gruppenhomomorphismus ist.

(iv) *Es gibt einen Gruppenhomomorphismus $f \colon G \to G'$ mit $H = \ker f$.*

Sind diese Bedingungen erfüllt, so ist die Verknüpfung in (iii) *eindeutig bestimmt.*

Definition 1.1.61 (Normalteiler, Quotientengruppe)**.** Sei G eine Gruppe. Eine Untergruppe $H < G$ heißt *Normalteiler* in G, oder eine *normale Untergruppe* von G, wenn die äquivalenten Bedingungen der Proposition 1.1.60 erfüllt sind. Man schreibt auch $H \lhd G$, wenn H ein Normalteiler in G ist. Die Gruppe G/H heißt dann die *Quotientengruppe* oder die *Faktorgruppe* von G nach H.

Beweis der Proposition 1.1.60. Wir zeigen (i) ⇒ (ii) ⇒ (iii) ⇒ (iv) ⇒ (i).

Zu (i) ⇒ (ii). Seien $g \in G$ und $h \in H$ beliebig. Nach (i) gilt $ghg^{-1} \in H$ und auch $g^{-1}hg = g^{-1}h(g^{-1})^{-1} \in H$. Daraus folgt

$$gh = \underbrace{ghg^{-1}}_{\in H} g \in Hg \quad \text{und} \quad hg = g\underbrace{g^{-1}hg}_{\in H} \in gH,$$

so dass beide Inklusionen $gH \subset Hg$ und $Hg \subset gH$ gelten.

Zu (ii) ⇒ (iii). Damit q ein Gruppenhomomorphismus ist, muss die Verknüpfung (xH, yH) auf xyH abbilden (sie ist insbesondere eindeutig bestimmt). Man muss also zunächst nachprüfen, dass die Abbildung

$$\begin{aligned} G/H \times G/H &\to G/H, \\ (xH, yH) &\mapsto xyH, \end{aligned}$$

wohldefiniert ist. Seien also $x, x'y, y' \in G$ mit $xH = x'H$ und $yH = y'H$. Zu zeigen ist, dass $xyH = x'y'H$. Nach (ii) gilt $yH = Hy$ und damit

$$xyH = xHy = x'Hy = x'yH = x'y'H,$$

wie gewünscht. Dass G/H mit dieser Verknüpfung eine Gruppe ist, folgt jetzt unmittelbar aus den entsprechenden Eigenschaften der Verknüpfung auf G.

Zu (iii) ⇒ (iv). Nach (iii) ist $q\colon G \to G/H$ ein Gruppenhomomorphismus, und nach Definition von q gilt $\ker q = H$.

Zu (iv) ⇒ (i). Seien $g \in G$ und $h \in H$ beliebig. Es gilt $f(h) = e$ und damit

$$f(ghg^{-1}) = f(g)f(h)f(g)^{-1} = f(g)f(g)^{-1} = e,$$

so dass $ghg^{-1} \in \ker f = H$. □

Beispiel 1.1.62 (generische Beispiele)**.** Sei G eine Gruppe.

(i) $\{e\}$ und G sind stets Normalteiler in G.

(ii) Nach Proposition 1.1.60(iv) ist der Kern eines Gruppenhomomorphismus $f\colon G \to H$ ein Normalteiler in G.

(iii) Ist G abelsch, so ist jede Untergruppe $H < G$ normal. Denn für alle $g \in G$ und $h \in H$ gilt $ghg^{-1} = h \in H$.

Beispiel 1.1.63.

(i) Die alternierende Gruppe A_n ist ein Normalteiler in S_n, denn sie ist nach Definition der Kern des Gruppenhomomorphismus $\operatorname{sgn}\colon S_n \to \{\pm 1\}$.

(ii) Ist R ein kommutativer Ring, so ist $\mathrm{SL}_n(R)$ ein Normalteiler in $\mathrm{GL}_n(R)$, nämlich der Kern des Gruppenhomomorphismus $\det\colon \mathrm{GL}_n(R) \to R^\times$.

(iii) Seien $\tau = (1\ 2)$ und $\sigma = (1\ 2\ 3)$ aus S_3. Da $\tau^2 = \mathrm{id}$ und $\sigma^3 = \mathrm{id}$ erzeugen τ und σ die Untergruppen $\langle\tau\rangle = \{\mathrm{id}, \tau\}$ und $\langle\sigma\rangle = \{\mathrm{id}, \sigma, \sigma^2\}$. Die Untergruppe $\langle\sigma\rangle$ ist ein Normalteiler von S_3, und zwar die alternierende Gruppe A_3. Die Untergruppe $\langle\tau\rangle$ ist *kein* Normalteiler von S_3, denn es gilt zum Beispiel

$$\sigma \circ \tau \circ \sigma^{-1} = (1\ 2\ 3)(1\ 2)(3\ 2\ 1) = (2\ 3) \notin \langle\tau\rangle.$$

(iv) Sei $D_n = \{\rho_n^i, \sigma\rho_n^i \,|\, 0 \leq i \leq n-1\}$ die n-te Diedergruppe (Beispiel 1.1.41). Die Drehung ρ_n erzeugt die zyklische Untergruppe $\langle\rho_n\rangle = \{\mathrm{id}, \rho_n, \ldots, \rho_n^{n-1}\}$. Aus der Gleichheit $\sigma\rho_n\sigma = \rho_n^{-1}$ folgt, dass $\langle\rho_n\rangle$ ein Normalteiler von D_n ist. Wenn $n \geq 3$ ist aber die Untergruppe $\langle\sigma\rangle = \{\mathrm{id}, \sigma\}$ kein Normalteiler von D_n, denn $\rho_n\sigma\rho_n^{-1} = \rho_n^2\sigma \notin \langle\sigma\rangle$.

Bemerkung 1.1.64. Im Gegensatz zu $<$ ist die Relation $\lhd$ *nicht* transitiv. Das heißt, aus $K \lhd H \lhd G$ folgt nicht unbedingt $K \lhd G$. Das einfachste Gegenbeispiel dazu ist folgendes: In der Diedergruppe D_4 ist die Unterguppe $\langle\sigma\rangle$ kein Normalteiler (Beispiel 1.1.63(iv)), aber es gilt $\langle\sigma\rangle \lhd \langle\sigma, \rho_4^2\rangle \lhd D_4$.

Bemerkung 1.1.65. Ist $N \lhd G$ ein Normalteiler, so gilt $gN = Ng$ für alle $g \in G$, d.h., es gibt keinen Unterschied zwischen Links- und Rechtsnebenklassen. Insbesondere gilt auch $G/N = N\backslash G$.

Proposition 1.1.66 (universelle Eigenschaft der Quotientengruppe)**.** *Sei G eine Gruppe, $N \lhd G$ ein Normalteiler, und $q\colon G \to G/N$ die Quotientenabbildung. Zu jeder Gruppe H und zu jedem Gruppenhomomorphismus $f\colon G \to H$ mit $N \subset \ker f$ gibt es* genau einem *Gruppenhomorphismus $\bar{f}\colon G/N \to H$ mit $\bar{f} \circ q = f$.*

Beweis. G/N ist nach Definition die Quotientenmenge $G/\!\sim_N$, wobei $g \sim_N h \iff h^{-1}g \in N$ (Bemerkung 1.1.52). Es gilt:

$$g \sim_N h \quad\Longrightarrow\quad f(h^{-1}g) \in f(N) = \{e\} \quad\Longrightarrow\quad f(g) = f(h).$$

Nach der universellen Eigenschaft der Quotientenmenge (Satz LA.1.4.10) gibt es genau eine Abbildung $\bar{f}\colon G/N \to H$ mit $\bar{f} \circ q = f$, und es bleibt zu zeigen, dass $\bar{f}$ ein Gruppenhomomorphismus ist. Dies folgt aber automatisch aus der Tatsache, dass q ein surjektiver Gruppenhomomorphismus ist: Sind $x, y \in G/N$ und sind $g, h \in G$ mit $q(g) = x$ und $q(h) = y$, so gilt

$$\bar{f}(xy) = \bar{f}(q(g)q(h)) = \bar{f}(q(gh)) = f(gh) = f(g)f(h) = \bar{f}(q(g))\bar{f}(q(h)) = \bar{f}(x)\bar{f}(y). \qquad \square$$

Korollar 1.1.67 (universelle Eigenschaft der Gruppe $\mathbb{Z}/n\mathbb{Z}$)**.** *Sei G eine Gruppe, $n \in \mathbb{N}$ und $g \in G$ ein Element mit $g^n = e$. Dann gibt es* genau einen *Gruppenhomorphismus $f\colon \mathbb{Z}/n\mathbb{Z} \to G$ mit $f([1]) = g$.*

Beweis. Nach der universellen Eigenschat von $\mathbb{Z}$ (Proposition 1.1.30) gibt es genau einen Gruppenhomomorphismus $h\colon \mathbb{Z} \to G$ mit $h(1) = g$. Aus $g^n = e$ folgt, dass $n \in \ker h$ und daher $\langle n\rangle = n\mathbb{Z} \subset \ker h$. Nach der universellen Eigenschaft der Quotientengruppe gibt es nun genau einen Gruppenhomomorphismus $f\colon \mathbb{Z}/n\mathbb{Z} \to G$ mit $f([1]) = g$. $\square$

Bemerkung 1.1.68. Korollar 1.1.67 sagt, dass die Gruppe $\mathbb{Z}/n\mathbb{Z}$ den Funktor

$$\mathcal{G}\mathrm{rp} \to \mathcal{S}\mathrm{et}, \quad G \mapsto \{g \in G \mid g^n = e\},$$

darstellt (siehe Definition LA.A.3.7).

Proposition 1.1.69 (Untergruppen einer Quotientengruppe)**.** *Sei G eine Gruppe, $N \lhd G$ ein Normalteiler und $q\colon G \to G/N$ die Quotientenabbildung. Dann gibt es eine Bijektion*

$$\{\textit{Untergruppen von } G, \textit{ die } N \textit{ enthalten}\} \xrightarrow{\sim} \{\textit{Untergruppen von } G/N\},$$
$$H \mapsto H/N.$$

Die Umkehrabbildung bildet eine Untergruppe K von G/N auf $q^{-1}(K)$ ab. Zudem ist H genau dann ein Normalteiler in G, wenn H/N ein Normalteiler in G/N ist.

Beweis. Man bemerkt zunächst, dass H/N eine Untegruppe von G/N ist, und dass $q^{-1}(K)$ eine Untergruppe von G ist, die N enthält. Da q surjektiv ist, gilt zudem $q^{-1}(K)/N = q(q^{-1}(K)) = K$. Sei umgekehrt H eine Untergruppe von G, die N enthält. Man muss dann zeigen, dass $H = q^{-1}(q(H))$ ist. Die Inklusion $\subset$ ist klar. Sei also $g \in q^{-1}(q(H))$, d.h., $q(g) \in q(H)$. Es gibt dann ein $h \in H$, so dass $gN = hN$, d.h., $g \in hN$. Aus $N \subset H$ folgt dann $g \in hH = H$, wie gewünscht.

Sei nun $K \lhd G/N$ ein Normalteiler. Dann ist K der Kern eines Gruppenhomomorphismus $f\colon G/N \to G'$. Sein Urbild $q^{-1}(K)$ ist dann der Kern des Gruppenhomomorphismus $f \circ q$, so dass $q^{-1}(K) \lhd G$. Sei umgekehrt H ein Normalteiler in G, der N enthält. Seien $hN \in H/N$ und $gN \in G/N$. Da q ein Gruppenhomomorphismus ist, gilt $(gN)(hN)(gN)^{-1} = (ghg^{-1})N \in H/N$, so dass H/N ein Normalteiler in G/N ist. □

Satz 1.1.70 (Homomorphiesatz für Gruppen)**.** *Sei $f\colon G \to H$ ein Gruppenhomomorphismus. Dann ist die von f induzierte Abbildung*

$$\begin{aligned} \bar{f}\colon G/\ker f &\to \operatorname{im} f, \\ [g] &\mapsto f(g), \end{aligned}$$

ein Gruppenisomorphismus.

Beweis. Die Abbildung $\bar{f}$ ist wohldefiniert und ein Gruppenhomomorphismus nach Proposition 1.1.66. Sie ist offensichtlich surjektiv, nach Definition von $\operatorname{im} f$. Wir berechnen nun den Kern von $\bar{f}$:

$$\ker \bar{f} = \{[g] \in G/\ker f \mid f(g) = e\} = \{[g] \in G/\ker f \mid g \in \ker f\} = \{[e]\}.$$

Nach Proposition 1.1.29 ist also $\bar{f}$ injektiv und damit bijektiv. Schließlich ist $\bar{f}$ ein Isomorphismus nach Proposition 1.1.26. □

Beispiel 1.1.71.

(i) Sei $n \geq 2$. Dann ist der Gruppenhomomorphismus $\operatorname{sgn}\colon S_n \to \{\pm 1\}$ surjektiv. Nach dem Homomorphiesatz induziert sgn einen Isomorphismus

$$S_n/A_n \xrightarrow{\sim} \{\pm 1\}, \quad [\sigma] \mapsto \operatorname{sgn}(\sigma).$$

(ii) Sei R ein kommutativer Ring und sei $n \geq 1$. Dann ist der Gruppenhomomorphismus $\det\colon \mathrm{GL}_n(R) \to R^\times$ surjektiv (die Matrix $\operatorname{diag}(r, 1, \ldots, 1)$ hat Determinante r). Der Homomorphiesatz liefert einen Isomorphismus

$$\mathrm{GL}_n(R)/\mathrm{SL}_n(R) \xrightarrow{\sim} R^\times, \quad [A] \mapsto \det(A).$$

Auf ähnliche Weise gibt es Isomorphismen $\mathrm{O}(n)/\mathrm{SO}(n) \xrightarrow{\sim} \{\pm 1\}$ und $\mathrm{U}(n)/\mathrm{SU}(n) \xrightarrow{\sim} U(1) \subset \mathbb{C}^\times$.

(iii) Die Determinante einer linearen Isometrie von $\mathbb{R}^n$ ist entweder 1 oder -1 (Korollar LA.7.2.46). Insbesondere ist die Einschränkung von $\det\colon \mathrm{Aut}_{\mathbb{R}}(\mathbb{R}^2) \to \mathbb{R}^\times$ auf D_n ein Gruppenhomomorphismus

$$\det\colon D_n \to \{\pm 1\}.$$

Er ist surjektiv, denn $\det(\sigma) = -1$. Der Kern ist genau die von ρ_n erzeugte Untergruppe $\langle \rho_n \rangle$, und wir erhalten einen Isomorphismus

$$D_n/\langle \rho_n \rangle \xrightarrow{\sim} \{\pm 1\}, \quad [\varphi] \mapsto \det(\varphi).$$

Satz 1.1.72 (Isomorphiesätze für Gruppen)**.** *Sei G eine Gruppe.*

(i) (erster Isomorphiesatz) *Sei $H < G$ eine Untergruppe und $N \lhd G$ ein Normalteiler. Dann ist $HN = \{h \cdot n \mid h \in H, n \in N\}$ eine Untergruppe von G und $H \cap N$ ein Normalteiler in H, und es gibt einen Gruppenisomorphismus*

$$H/(H \cap N) \xrightarrow{\sim} HN/N, \quad h(H \cap N) \mapsto hN.$$

(ii) (zweiter Isomorphiesatz) *Seien $H, N \lhd G$ Normalteiler in G mit $N \subset H$. Dann ist H/N ein Normalteiler in G/N, und es gibt einen Gruppenisomorphismus*

$$(G/N)/(H/N) \xrightarrow{\sim} G/H, \quad (gN)(H/N) \mapsto gH.$$

Beweis. Zu (i). Wir wenden zunächst das Kriterium 1.1.33 mit der Teilmenge HN an:

- HN ist nicht leer, denn $e \cdot e \in HN$.
- Seien $h, h' \in H$ und $n, n' \in N$. Dann gilt

$$(hn)(h'n') = hh' \underbrace{h'^{-1}nh'}_{\in N} n' \in HN.$$

  (Alternative Berechnung mit der Gleichheit $h'N = Nh'$: $hnh'n' \in hnh'N = hnNh' = hNh' = hh'N \subset HN$.)

- Seien $h \in H$ und $n \in N$. Dann gilt

$$(hn)^{-1} = n^{-1}h^{-1} = h^{-1} \underbrace{hn^{-1}h^{-1}}_{\in N} \in HN.$$

  (Alternative Berechnung: $(hn)^{-1} = n^{-1}h^{-1} \in Nh^{-1} = h^{-1}N \subset HN$.)

Also ist HN eine Untergruppe von G, wie behauptet. Da N ein Normalteiler in G ist, ist es auch insbesondere ein Normalteiler in HN. Jetzt betrachten wir den Gruppenhomomorphismus

$$f = q \circ i : H \overset{i}{\hookrightarrow} HN \overset{q}{\twoheadrightarrow} HN/N, \quad f(h) = hN,$$

wobei i die Inklusionsabbildung und q die Quotientenabbildung ist. Die Abbildung f ist surjektiv, denn $hnN = hN = f(h)$ für alle $h \in H$ und $n \in N$. Aus dem Homomorphiesatz 1.1.70 erhalten wir einen Isomorphismus

$$\bar{f} \colon H/\ker f \xrightarrow{\sim} HN/N.$$

Es gilt zudem $\ker f = \{h \in H \mid hN = N\} = \{h \in H \mid h \in N\} = H \cap N$ (insbesondere ist $H \cap N$ ein Normalteiler in H).

Zu (ii). Wir betrachten die Quotientenabbildung $q \colon G \twoheadrightarrow G/H$. Sie erfüllt $\ker q = H \supset N$. Nach der universellen Eigenschaft der Quotientengruppe erhalten wir einen induzierten Gruppenhomomorphismus

$$\bar{q} \colon G/N \twoheadrightarrow G/H, \quad gN \mapsto gH.$$

Der Kern von $\bar{q}$ ist nun

$$\ker \bar{q} = \{gN \mid gH = H\} = \{gN \mid g \in H\} = H/N.$$

Deswegen ist H/N ein Normalteiler in G/N, und der Homomorphiesatz liefert den gewünschten Isomorphismus. □

Bemerkung 1.1.73. Wenn $H, K < G$ beliebige Untergruppen sind, dann ist im Allgemeinen die Teilmenge $HK = \{hk \mid h \in H,\ k \in K\}$ keine Untergruppe von G.

Beispiel 1.1.74. Seien $n, m \in \mathbb{N}$.

(i) Es gilt $n\mathbb{Z} + m\mathbb{Z} = \mathrm{ggT}(n,m)\mathbb{Z}$ und $n\mathbb{Z} \cap m\mathbb{Z} = \mathrm{kgV}(n,m)\mathbb{Z}$. Nach dem ersten Isomorphiesatz gibt es einen Isomorphismus

$$n\mathbb{Z}/\,\mathrm{kgV}(n,m)\mathbb{Z} \xrightarrow{\sim} \mathrm{ggT}(n,m)\mathbb{Z}/m\mathbb{Z}.$$

Zum Beispiel: $4\mathbb{Z}/12\mathbb{Z} \xrightarrow{\sim} 2\mathbb{Z}/6\mathbb{Z}$.

(ii) Sei nun $n|m$, d.h., $m\mathbb{Z} \subset n\mathbb{Z}$. Nach dem zweiten Isomorphiesatz gibt es einen Isomorphismus

$$(\mathbb{Z}/m\mathbb{Z})/(n\mathbb{Z}/m\mathbb{Z}) \xrightarrow{\sim} \mathbb{Z}/n\mathbb{Z}.$$

Definition 1.1.75 (Ordnung)**.** Sei G eine Gruppe und sei $g \in G$. Die *Ordnung* von g ist

$$\mathrm{ord}(g) := \inf\{n \in \mathbb{N}_{>0} \mid g^n = e\} \in \mathbb{N}_{>0} \cup \{\infty\},$$

wobei $\inf \varnothing = \infty$.

Beispiel 1.1.76.

(i) Es gilt $\mathrm{ord}(g) = 1$ genau dann, wenn $g = e$.

(ii) In der Gruppe $\mathbb{Z}$ gilt $\mathrm{ord}(n) = \infty$ für alle $n \neq 0$.

(iii) In der Diedergruppe D_n gilt $\mathrm{ord}(\rho_n) = n$ und $\mathrm{ord}(\sigma) = 2$.

(iv) Ist $\sigma \in S_n$ ein Zyklus der Länge k, so gilt $\mathrm{ord}(\sigma) = k$.

Proposition 1.1.77. *Sei G eine Gruppe und sei $g \in G$.*

(i) *Ist* $\mathrm{ord}(g) = n < \infty$*, dann gibt es einen Gruppenisomorphismus*

$$\mathbb{Z}/n\mathbb{Z} \xrightarrow{\sim} \langle g \rangle, \quad [i] \mapsto g^i.$$

(ii) *Ist* $\mathrm{ord}(g) = \infty$*, dann gibt es einen Gruppenisomorphismus*

$$\mathbb{Z} \xrightarrow{\sim} \langle g \rangle, \quad [i] \mapsto g^i.$$

Insbesondere gilt $\mathrm{ord}(g) = |\langle g \rangle|$.

Beweis. Sei

$$n = \begin{cases} \mathrm{ord}(g), & \text{falls } \mathrm{ord}(g) < \infty, \\ 0, & \text{falls } \mathrm{ord}(g) = \infty, \end{cases}$$

damit $g^n = e$ gilt. Nach der universellen Eigenschaft von $\mathbb{Z}/n\mathbb{Z}$ (Korollar 1.1.67) gibt es einen Gruppenhomomorphismus

$$f\colon \mathbb{Z}/n\mathbb{Z} \to \langle g \rangle, \quad [i] \mapsto g^i.$$

Nach Proposition 1.1.45 ist

$$\langle g \rangle = \{g^i \mid i \in \mathbb{Z}\},$$

so dass f surjektiv ist. Nach Definition von $\mathrm{ord}(g)$ gilt $g^i \neq e$ für alle $1 \leq i < \mathrm{ord}(g)$. Damit ist der Kern von f trivial, und f ist ein Isomorphismus. □

Bemerkung 1.1.78. Die Mächtigkeit $|G|$ einer Gruppe G nennt man auch oft die *Ordnung* von G. Die Ordnung eines Elements $g \in G$ ist dann gleich der Ordnung der erzeugten Untergruppe $\langle g \rangle$.

Korollar 1.1.79 (Klassifikation der zyklischen Gruppen)**.** *Sei G eine zyklische Gruppe. Dann gibt es genau ein $n \in \mathbb{N}$ mit $G \cong \mathbb{Z}/n\mathbb{Z}$.*

Beweis. Sei $g \in G$ ein Element mit $G = \langle g \rangle$. Nach Proposition 1.1.77 gibt es ein $n \in \mathbb{N}$ mit $G \cong \mathbb{Z}/n\mathbb{Z}$. Das n ist eindeutig, denn wenn $n \neq m$ sind die Gruppen $\mathbb{Z}/n\mathbb{Z}$ und $\mathbb{Z}/m\mathbb{Z}$ nicht einmal gleichmächtig, insbesondere nicht isomorph. □

Notation 1.1.80 (zyklische Gruppen)**.** Man schreibt oft C_n für eine zyklische Gruppe mit n Elementen, wobei $n \in \mathbb{N}_{\geq 1} \cup \{\infty\}$. Nach Korollar 1.1.79 ist eine solche Gruppe eindeutig bis auf Isomorphie: Es gilt nämlich $C_\infty \cong \mathbb{Z}$ und $C_n \cong \mathbb{Z}/n\mathbb{Z}$ für $n \neq \infty$.

1.1.5 Erweiterungen und semidirekte Produkte

Definition 1.1.81 (Produkt von Gruppen)**.** Sei $(G_i)_{i \in I}$ eine Familie von Gruppen. Das *Produkt* der Familie ist die Gruppe

$$\prod_{i \in I} G_i = \{(g_i)_{i \in I} \mid \text{für alle } i \in I \text{ gilt } g_i \in G_i\},$$

mit der komponentenweisen Verknüpfung:

$$(g_i)_{i \in I} \cdot (h_i)_{i \in I} = (g_i \cdot h_i)_{i \in I}.$$

Die kanonischen Projektionen

$$\pi_e \colon \prod_{i \in I} G_i \to G_e, \quad (g_i)_{i \in I} \mapsto g_e,$$

sind dann Gruppenhomomorphismen für alle $e \in I$. Diese Konstruktion ist eigentlich ein Produkt im Sinne der Kategorientheorie (Definition LA.A.1.16):

Proposition 1.1.82 (universelle Eigenschaft des Produkts)**.** *Sei $(G_i)_{i \in I}$ eine Familie von Gruppen. Zu jeder Gruppe H und jeder Familie $(f_i \colon H \to G_i)_{i \in I}$ von Gruppenhomomorphismen gibt es* genau einen *Gruppenhomomorphismus $f \colon H \to \prod_{i \in I} G_i$, so dass $\pi_i \circ f = f_i$ für alle $i \in I$.*

Beweis. Ganz analog zum Fall der Vektorräume (Proposition LA.6.1.3(i)). □

Bemerkung 1.1.83. Das Produkt $\prod_{i \in I} G_i$ ist genau dann abelsch, wenn alle Gruppen G_i abelsch sind. In diesem Fall stimmt dieses Produkt mit dem Produkt von $\mathbb{Z}$-Moduln überein.

Bemerkung 1.1.84 (Summe von Gruppen)**.** Jede Familie $(G_i)_{i \in I}$ von Gruppen besitzt auch eine Summe/ein Koprodukt im Sinne der Kategorientheorie (Definition LA.A.1.16), die als *freies Produkt* der Familie bezeichnet wird. Diese Konstruktion ist aber nicht so einfach wie im Fall der Vektorräume (wobei die kategorische Summe die direkte Summe ist). Das freie Produkt zweier Gruppen G und H wird üblicherwise mit $G * H$ bezeichnet. Es ist stets unendlich, sofern G und H nicht trivial sind. Es gibt zum Beispiel einen berühmten Isomorphismus

$$\mathbb{Z}/2\mathbb{Z} * \mathbb{Z}/3\mathbb{Z} \xrightarrow{\sim} \mathrm{SL}_2(\mathbb{Z})/\{\pm I_2\}.$$

(Diese Gruppe heißt *Modulgruppe* und taucht in der Funktionentheorie im Zusammenhang mit Modulformen auf.) Insbesondere ist die Summe $\mathbb{Z}/2\mathbb{Z} * \mathbb{Z}/3\mathbb{Z}$ in der Kategorie der Gruppen nicht isomorph zu der Summe $\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/3\mathbb{Z} \cong \mathbb{Z}/6\mathbb{Z}$ in der Kategorie der *abelschen* Gruppen.

Folgendem Begriff haben wir schon im Zusammenhang mit Präsentationen von Moduln begegnet (siehe LA.8.3.1):

Definition 1.1.85 (exakte Sequenz)**.** Eine Sequenz von Gruppen und Gruppenhomomorphismen

$$G_0 \xrightarrow{f_1} G_1 \xrightarrow{f_2} \cdots \xrightarrow{f_n} G_n$$

heißt *exakt*, wenn für alle $i \in \{1, \ldots, n-1\}$ gilt $\operatorname{im} f_i = \ker f_{i+1}$. (Diese Definition lässt sich weiter auf unendliche Sequenzen verallgemeinern.)

Bemerkung 1.1.86 (Exaktheit und Injektivität/Surjektivität)**.** Sei $f\colon G \to H$ ein Gruppenhomomorphismus. Es gibt genau einen Gruppenhomomorphismus $\{e\} \to G$ (denn e muss auf e abgebildet werden) und auch genau einen Gruppenhomorphismus $H \to \{e\}$. Die Sequenz

$$\{e\} \to G \xrightarrow{f} H$$

ist genau dann exakt, wenn f injektiv ist, und die Sequenz

$$G \xrightarrow{f} H \to \{e\}$$

ist genau dann exakt, wenn f surjektiv ist.

Beispiel 1.1.87. Sei R ein Ring. Eine *Präsentation* eines R-Moduls M (Definition LA.8.3.1) ist eine exakte Sequenz von R-linearen Abbildungen der Form

$$R^{(J)} \to R^{(I)} \to M \to \{0\}.$$

Definition 1.1.88 (kurze exakte Sequence, Erweiterung)**.** Seien G, H und K Gruppen. Eine exakte Sequenz der Form

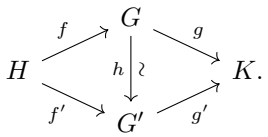
$$\{e\} \to H \xrightarrow{f} G \xrightarrow{g} K \to \{e\}$$

heißt *kurze exakte Sequenz* oder *Gruppenerweiterung*. Man sagt auch, dass die Gruppe G als Erweiterung der Gruppe K durch die Gruppe H dargestellt wird. Nach Bemerkung 1.1.86 ist eine kurze exakte Sequenz äquivalent zu einer exakten Sequenz $H \xrightarrow{f} G \xrightarrow{g} K$ mit f injektiv und g surjektiv.

Zwei Erweiterungen von K durch H

$$\{e\} \to H \xrightarrow{f} G \xrightarrow{g} K \to \{e\}$$
$$\{e\} \to H \xrightarrow{f'} G' \xrightarrow{g'} K \to \{e\}$$

heißen *isomorph*, wenn ein Isomorphismus $h\colon G \xrightarrow{\sim} G'$ mit $g' \circ h = g$ und $h \circ f = f'$ existiert:



Bemerkung 1.1.89. Sei

$$\{e\} \to H \xrightarrow{f} G \xrightarrow{g} K \to \{e\}.$$

eine kurze exakte Sequenz und sei $N = \operatorname{im} f = \ker g$. Da N der Kern eines Gruppenhomomorphismus ist, ist N ein Normalteiler in G. Da f injektiv ist, induziert es einen Isomorphismus $H \xrightarrow{\sim} N$. Da g surjektiv ist, induziert es nach dem Homomorphiesatz einen Isomorphismus $G/N \xrightarrow{\sim} K$. Bis auf Isomorphie hat also jede kurze exakte Sequenz die Form

$$N \overset{i}{\hookrightarrow} G \overset{q}{\twoheadrightarrow} G/N,$$

wobei i die Inklusionsabbildung eines Normalteilers ist und q die Quotientenabbildung ist.

Beispiel 1.1.90.

(i) Seien H, K zwei Gruppen. Dann ist das Produkt $H \times K$ eine Erweiterung von K durch H. Es gibt nämlich eine kurze exakte Sequenz

$$\{e\} \to H \xrightarrow{\iota_1} H \times K \xrightarrow{\pi_2} K \to \{e\},$$

wobei $\iota_1(h) = (h, e)$ und $\pi_2(h, k) = k$. Eine Erweiterung von K durch H heißt *trivial*, wenn sie zu dieser Erweiterung isomorph ist.

(ii) Für jedes $n \in \mathbb{N} \setminus \{0\}$ gibt es eine kurze exakte Sequenz von abelschen Gruppen

$$\{0\} \to \mathbb{Z} \xrightarrow{x \mapsto nx} \mathbb{Z} \xrightarrow{x \mapsto [x]} \mathbb{Z}/n\mathbb{Z} \to \{0\}.$$

Wenn $n \geq 2$ ist diese Erweiterung nicht trivial, denn $\mathbb{Z}$ ist nicht zu $\mathbb{Z} \oplus \mathbb{Z}/n\mathbb{Z}$ isomorph.

(iii) Nach Beispiel 1.1.71 haben wir die folgenden kurzen exakten Sequenzen (mit $n \geq 2$ für die erste und $n \geq 1$ für die anderen):

$$\{e\} \to A_n \to S_n \xrightarrow{\text{sgn}} \{\pm 1\} \to \{e\},$$
$$\{e\} \to \mathrm{SL}_n(R) \to \mathrm{GL}_n(R) \xrightarrow{\det} R^\times \to \{e\},$$
$$\{e\} \to \mathrm{SO}(n) \to \mathrm{O}(n) \xrightarrow{\det} \{\pm 1\} \to \{e\},$$
$$\{e\} \to \mathrm{SU}(n) \to \mathrm{U}(n) \xrightarrow{\det} \mathrm{U}(1) \to \{e\},$$
$$\{e\} \to \langle \rho_n \rangle \to D_n \xrightarrow{\det} \{\pm 1\} \to \{e\}.$$

Als Nächstes wollen wir das *semidirekte Produkt* von zwei Gruppen definieren, das eine weitere Quelle von nicht-trivialen Gruppenerweiterungen ist. Das prototypische Beispiel von diesem Begriff ist die Isometriegruppe $\mathrm{Isom}(\mathbb{R}^n)$ von $\mathbb{R}^n$ (mit der euklidischen Metrik). Diese Gruppe enthält zwei besondere Untergruppen, die Untergruppe $\mathrm{Isom}_0(\mathbb{R}^n) \cong \mathrm{O}(n)$ der *linearen* Isometrien und die Untergruppe V_n der Verschiebungen. Die letztere ist zu der Gruppe $(\mathbb{R}^n, +)$ isomorph durch

$$\mathbb{R}^n \xrightarrow{\sim} V_n, \quad v \mapsto T_v, \quad T_v(x) = x + v.$$

Jede Isometrie f von $\mathbb{R}^n$ lässt sich auf eindeutige Weise als Komposition einer linearen Isometrie mit einer Verschiebung zerlegen, nämlich

$$f = T_{f(0)} \circ f_0, \quad \text{wobei} \quad f_0 = T_{-f(0)} \circ f.$$

Anders gesagt ist die Abbildung

$$\alpha \colon \mathrm{Isom}(\mathbb{R}^n) \to \mathbb{R}^n \times \mathrm{O}(n), \quad f \mapsto (f(0), M(f_0)),$$

eine Bijektion. Sie ist aber *kein* Gruppenisomorphismus, denn für eine lineare Isometrie h und einen Vektor $v \in \mathbb{R}^n$ gilt

$$h \circ T_v = T_{h(v)} \circ h,$$

so dass die Komposition $\pi_1 \circ \alpha \colon \mathrm{Isom}(\mathbb{R}^n) \to \mathbb{R}^n$ kein Gruppenhomomorphismus ist. Man kann trotzdem die Bijektion α zu einem Gruppenisomorphismus befördern, indem man die Verknüpfung auf dem Produkt $\mathbb{R}^n \times \mathrm{O}(n)$ auf geeignete Weise anpasst: Anstatt der komponentenweisen Verknüpfung

$$(v, A)(w, B) = (v + w, AB)$$

braucht man die Verknüpfung

$$(v, A)(w, B) = (v + Aw, AB).$$

Diese neue Verknüpfung hängt nicht nur von den Verknüpfungen auf $\mathbb{R}^n$ und $\mathrm{O}(n)$ ab, sondern auch von der Abbildung $\varphi\colon \mathrm{O}(n) \to \mathrm{Aut}(\mathbb{R}^n)$, $A \mapsto (w \mapsto Aw)$. Die Produktmenge $\mathbb{R}^n \times \mathrm{O}(n)$ versehen mit dieser Verknüpfung heißt das *semidirekte Produkt* von $\mathbb{R}^n$ mit $\mathrm{O}(n)$ bzgl. φ und wird mit $\mathbb{R}^n \rtimes_\varphi \mathrm{O}(n)$ bezeichnet. Die Abbildung α ist dann ein Gruppenisomorphismus

$$\alpha\colon \mathrm{Isom}(\mathbb{R}^n) \xrightarrow{\sim} \mathbb{R}^n \rtimes_\varphi \mathrm{O}(n).$$

Jetzt kommen wir auf die allgemeine Definition:

Definition 1.1.91 (semidirektes Produkt)**.** Seien H, K Gruppen und sei $\varphi\colon K \to \mathrm{Aut}(H)$ ein Gruppenhomomorphismus (dabei ist $\mathrm{Aut}(H)$ die Gruppe der Gruppenautomorphismen von H). Das *semidirekte Produkt* $H \rtimes_\varphi K$ von H und K bzgl. φ ist die Menge $H \times K$ versehen mit der folgenden Verknüpfung:

$$\begin{aligned}(H \times K) \times (H \times K) &\to H \times K,\\ ((h,k),(h',k')) &\mapsto (h \cdot \varphi(k)(h'), k \cdot k').\end{aligned}$$

Bemerkung 1.1.92. Falls $\varphi\colon K \to \mathrm{Aut}(H)$ der triviale Gruppenhomomorphismus ist, d.h., $\varphi(k) = \mathrm{id}_H$ für alle $k \in K$, dann ist $H \rtimes_\varphi K$ einfach das Produkt $H \times K$ aus Definition 1.1.81.

Proposition 1.1.93 (Eigenschaften des semidirekten Produkts)**.** *Seien H, K Gruppen und sei $\varphi\colon K \to \mathrm{Aut}(H)$ ein Gruppenhomomorphismus.*

(i) *$H \rtimes_\varphi K$ ist eine Gruppe. Ihr neutrales Element ist (e,e) und das Inverse von (h,k) ist $(\varphi(k)^{-1}(h^{-1}), k^{-1})$.*

(ii) *Die Abbildungen*

$$\begin{aligned}\iota_1\colon H \to H \rtimes_\varphi K, &\quad h \mapsto (h,e),\\ \pi_2\colon H \rtimes_\varphi K \to K, &\quad (h,k) \mapsto k,\end{aligned}$$

sind Gruppenhomomorphismen, und es gibt eine kurze exakte Sequenz

$$\{e\} \to H \xrightarrow{\iota_1} H \rtimes_\varphi K \xrightarrow{\pi_2} K \to \{e\}.$$

Insbesondere ist $\iota_1(H)$ ein Normalteiler in $H \rtimes_\varphi K$.

(iii) *Die Abbildung*

$$\iota_2\colon K \to H \rtimes_\varphi K, \quad k \mapsto (e,k),$$

ist ein Gruppenhomomorphismus mit $\pi_2 \circ \iota_2 = \mathrm{id}_K$.

(iv) *Für alle $h \in H$ und $k \in K$ gilt*

$$c_{\iota_2(k)}(\iota_1(h)) = \iota_1(\varphi(k)(h)).$$

Das heißt, wenn wir H und K mit Untergruppen von $H \rtimes_\varphi K$ durch ι_1 und ι_2 identifizieren, dann ist $\varphi(k)$ die Einschränkung auf H der Konjugationsabbildung bzgl. k.

Beweis. Einfaches Nachrechnen. Wir beweisen als Beispiel die Assoziativität der Verknüpfung und (iv).

Zur Assoziativität. Seien $(h_1,k_1),(h_2,k_2),(h_3,k_3) \in H \rtimes_\varphi K$. Nach Definition gilt:

$$\begin{aligned}((h_1,k_1)(h_2,k_2))(h_3,k_3) &= (h_1\varphi(k_1)(h_2), k_1k_2)(h_3,k_3) = (h_1\varphi(k_1)(h_2)\varphi(k_1k_2)(h_3), k_1k_2k_3),\\ (h_1,k_1)((h_2,k_2)(h_3,k_3)) &= (h_1,k_1)(h_2\varphi(k_2)(h_3), k_2k_3) = (h_1\varphi(k_1)(h_2\varphi(k_2)(h_3)), k_1k_2k_3).\end{aligned}$$

Man muss also die folgende Gleichheit nachprüfen:

$$\varphi(k_1)(h_2)\varphi(k_1k_2)(h_3) = \varphi(k_1)(h_2\varphi(k_2)(h_3)).$$

Da $\varphi\colon K \to \mathrm{Aut}(H)$ ein Gruppenhomomorphismus ist, gilt

$$\varphi(k_1k_2) = \varphi(k_1) \circ \varphi(k_2). \tag{1.1.94}$$

Da $\varphi(k_1)\colon H \to H$ ein Gruppenhomomorphismus ist, gilt

$$\varphi(k_1)(h)\varphi(k_1)(h') = \varphi(k_1)(hh') \tag{1.1.95}$$

für alle $h, h' \in H$. Damit gilt

$$\varphi(k_1)(h_2)\varphi(k_1k_2)(h_3) \overset{(1.1.94)}{=} \varphi(k_1)(h_2)\varphi(k_1)(\varphi(k_2)(h_3)) \overset{(1.1.95)}{=} \varphi(k_1)(h_2\varphi(k_2)(h_3)),$$

wie gewünscht.

Zu (iv). Nach (iii) ist ι_2 ein Gruppenhomomorphismus, so dass $(e,k)^{-1} = (e,k^{-1})$. Dann gilt:

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

wie gewünscht. □

Bemerkung 1.1.96. Die Abbildung $\pi_1\colon H \rtimes_\varphi K \to K$, $(h,k) \mapsto h$, ist aber kein Gruppenhomomorphismus, wenn φ nicht trivial ist.

Die Eigenschaft (iii) in Proposition 1.1.93 charakterisiert die Gruppenerweiterungen, die aus semidirekten Produkten entstehen:

Proposition 1.1.97 (semidirekte Produkte aus Erweiterungen)**.** *Sei*

$$\{e\} \to H \xrightarrow{f} G \xrightarrow{g} K \to \{e\}$$

eine Gruppenerweiterung. Wenn ein Gruppenhomomorphismus $s\colon K \to G$ mit $g \circ s = \mathrm{id}_K$ existiert, dann gibt es einen Gruppenhomomorphismus $\varphi\colon K \to \mathrm{Aut}(H)$, so dass die gegebene Erweiterung zu der Erweiterung

$$\{e\} \to H \xrightarrow{\iota_1} H \rtimes_\varphi K \xrightarrow{\pi_2} K \to \{e\}$$

isomorph ist.

Ein Gruppenhomomorphismus $s\colon K \to G$ mit $g \circ s = \mathrm{id}$ heißt *Schnitt* oder *Spalt* von g, und eine kurze exakte Sequenz wie oben heißt *spaltend*, wenn ein Schnitt von g existiert.

Beweis. Ohne Einschränkung können wir annehmen, dass H der Kern von g ist, und dass f die Inklusionsabbildung ist. Die Abbildung $c\colon G \to \mathrm{Aut}(G)$, $g \mapsto c_g$, ist ein Gruppenhomomorphismus nach Beispiel 1.1.25. Wir setzen

$$\psi = c \circ s\colon K \to \mathrm{Aut}(G).$$

Das heißt, für jedes $k \in K$ ist $\psi(k) \in \mathrm{Aut}(G)$ die Konjugation bzgl. $s(k)$. Für alle $x \in G$ gilt dann

$$g(\psi(k)(x)) = g(s(k)xs(k)^{-1}) = kg(x)k^{-1}.$$

Ist nun $x \in H = \ker g$, so folgt $g(\psi(k)(x)) = e$, d.h., $\psi(k)(x) \in H$. Deswegen schränkt sich die Abbildung $\psi(k)\colon G \to G$ zu einer Abbildung $\varphi(k)\colon H \to H$. Zudem ist $\varphi(k)$ ein Automorphismus von H (mit Umkehrabbildung $\varphi(k^{-1})$) und die Abbildung $\varphi\colon K \to \mathrm{Aut}(H)$ ist ein Gruppenhomomorphismus. Man definiert

$$r\colon H \rtimes_\varphi K \to G, \quad (h,k) \mapsto h \cdot s(k),$$

so dass $r \circ \iota_1 = f$ und $g \circ r = \pi_2$. Die Berechnung

$$hs(k)h's(k') = hs(k)h's(k)^{-1}s(k)s(k') = h\varphi(k)(h')s(kk')$$

zeigt, dass r ein Gruppenhomomorphismus ist. Schließlich ist r bijektiv, mit Umkehrabbildung

$$G \to H \rtimes_\varphi K, \quad x \mapsto (x \cdot s(g(x))^{-1}, g(x)).$$ □

Beispiel 1.1.98 (symmetrische Gruppe als semidirektes Produkt)**.** Sei $n \geq 2$. Nach Beispiel 1.1.90(iii) gibt es eine kurze exakte Sequenz

$$\{e\} \to A_n \to S_n \xrightarrow{\text{sgn}} \{\pm 1\} \to \{e\}.$$

Es gibt zudem einen Gruppenhomomorphismus $s\colon \{\pm 1\} \to S_n$ mit $\text{sgn} \circ s = \text{id}$, zum Beispiel den mit $s(-1) = (1\ 2)$. Nach Proposition 1.1.97 erhalten wir einen Isomorphismus

$$S_n \cong A_n \rtimes_\varphi \{\pm 1\},$$

wobei $\varphi\colon \{\pm 1\} \to \text{Aut}(A_n)$ das Element -1 auf die Konjugation bzgl. $(1\ 2)$ abbildet.

Beispiel 1.1.99 (allgemeine lineare Gruppe als semidirektes Produkt)**.** Sei R ein kommutativer Ring und $n \geq 1$. Nach Beispiel 1.1.90(iii) gibt es eine kurze exakte Sequenz

$$\{e\} \to \text{SL}_n(R) \to \text{GL}_n(R) \xrightarrow{\det} R^\times \to \{e\}.$$

Es gibt zudem einen Schnitt $s\colon R^\times \to \text{GL}_n(R)$ von det, zum Beispiel $s(\lambda) = \text{diag}(\lambda, 1, \ldots, 1)$. Nach Proposition 1.1.97 erhalten wir einen Isomorphismus

$$\text{GL}_n(R) \cong \text{SL}_n(R) \rtimes_\varphi R^\times,$$

wobei $\varphi\colon R^\times \to \text{Aut}(\text{SL}_n(R))$ das Element λ auf die Konjugation bzgl. $\text{diag}(\lambda, 1, \ldots, 1)$ abbildet.

Beispiel 1.1.100 (Diedergruppe als semidirektes Produkt)**.** Nach Beispiel 1.1.90(iii) gibt es eine kurze exakte Sequenz

$$\{e\} \to \langle \rho_n \rangle \to D_n \xrightarrow{\det} \{\pm 1\} \to \{e\},$$

wobei $\langle \rho_n \rangle \cong \mathbb{Z}/n\mathbb{Z}$ und $\{\pm 1\} \cong \mathbb{Z}/2\mathbb{Z}$. Es gibt zudem einen Schnitt $s\colon \{\pm 1\} \to D_n$ von det, zum Beispiel mit $s(-1) = \sigma$. Nach Proposition 1.1.97 erhalten wir einen Isomorphismus

$$D_n \cong \langle \rho_n \rangle \rtimes_\varphi \{\pm 1\},$$

wobei $\varphi\colon \{\pm 1\} \to \text{Aut}(\langle \rho_n \rangle)$ das Element -1 auf den Automorphismus $\rho \mapsto \sigma\rho\sigma = \rho^{-1}$ abbildet.

1.2 Gruppenoperationen

1.2.1 Gruppenoperationen

Definition 1.2.1 (Gruppenoperation)**.** Sei G eine Gruppe und X eine Menge. Eine *Operation* von G auf X ist ein Gruppenhomomorphismus $\rho\colon G \to S_X$. Das Paar (X, ρ) heißt dann auch *G-Menge*.

Ist allgemeiner X ein Objekt einer Kategorie $\mathcal{C}$, so heißt ein Gruppenhomomorphismus $\rho\colon G \to \text{Aut}_\mathcal{C}(X)$ eine *Operation* von G auf dem Objekt X.

Konkret gesagt ordnet eine Operation von G auf X jedem Element $g \in G$ einen Automorphismus $\rho(g)\colon X \xrightarrow{\sim} X$, so dass für alle $g, h \in G$ gilt $\rho(g) \circ \rho(h) = \rho(g \cdot h)$.

Eine Gruppenoperation von G auf einer Menge X kann man auch als eine Veknüpfung $G \times X \to X$ verstehen. Dazu muss man sich an das *Exponentialgesetz* für Mengen erinnern: Sind X, Y, Z Mengen, so gibt es eine kanonische Bijektion

$$\begin{aligned} \text{Abb}(X, \text{Abb}(Y, Z)) &\xrightarrow{\sim} \text{Abb}(X \times Y, Z), \\ f &\mapsto ((x, y) \mapsto f(x)(y)), \\ (x \mapsto (y \mapsto g(x, y))) &\hookleftarrow g. \end{aligned}$$

Die folgende Proposition charakterisiert die Verknüpfungen $G \times X \to X$, die aus Gruppenoperationen entstehen (solche Verknüpfungen nennt man auch Gruppenoperationen):

Proposition 1.2.2 (Gruppenoperationen als Verknüpfungen)**.** *Sei G ein Gruppe und X eine Menge. Die Bijektion*

$$\mathrm{Abb}(G, \mathrm{Abb}(X, X)) \xrightarrow{\sim} \mathrm{Abb}(G \times X, X), \quad \rho \mapsto ((g, x) \mapsto \rho(g)(x)),$$

schränkt sich zu einer Bijektion zwischen folgenden Teilmengen ein:

- *Gruppenhomomorphismen $\rho\colon G \to S_X$, d.h., Gruppenoperationen von G auf X.*
- *Verknüpfungen $\cdot\colon G \times X \to X$ mit folgenden Eigenschaften:*
  - (i) *Für alle $x \in X$ gilt $e \cdot x = x$.*
  - (ii) *Für alle $g, h \in G$ und $x \in X$ gilt $g \cdot (h \cdot x) = (g \cdot h) \cdot x$.*

Beweis. Sei $\rho\colon G \to S_X$ ein Gruppenhomomorphismus und sei

$$\cdot\colon G \times X \to X, \quad (g, x) \mapsto \rho(g)(x),$$

die zugehörige Verknüpfung. Nach Definition gilt dann $\rho(g \cdot h) = \rho(g) \circ \rho(h)$ für alle $g, h \in X$, was genau die zweite Eigenschaft für $\cdot$ ist. Die erste Eigenschaft folgt daraus, dass ρ das neutrale Element $e \in G$ auf das neutrale Element $\mathrm{id}_X \in S_X$ abbildet.

Sei umgekehrt $\cdot\colon G \times X \to X$ eine Verknüpfung, die (i) und (ii) erfüllt, und sei

$$\rho\colon G \to \mathrm{Abb}(X, X), \quad g \mapsto (x \mapsto g \cdot x),$$

die zugehörige Abbildung. Nach (ii) gilt bereits $\rho(g \cdot h) = \rho(g) \circ \rho(h)$, und man muss noch zeigen, dass das Bild von ρ in $S_X \subset \mathrm{Abb}(X, X)$ enthalten ist. Nach (i) gilt zudem $\rho(e) = \mathrm{id}_X$, so dass

$$\rho(g) \circ \rho(g^{-1}) = \rho(g \cdot g^{-1}) = \rho(e) = \mathrm{id}_X,$$

und ebenso $\rho(g^{-1}) \circ \rho(g) = \mathrm{id}_X$. Also ist $\rho(g)$ bijektiv, mit Umkehrabbildung $\rho(g^{-1})$. □

Beispiel 1.2.3 (generische Beispiele)**.** Sei G eine Gruppe.

(i) Sei X eine beliebige Menge. Der triviale Gruppenhomomorphismus $G \to S_X$, $g \mapsto \mathrm{id}_X$, heißt die *triviale Operation* von G auf X. Die zugehörige Verknüpfung ist $G \times X \to X$, $(g, x) \mapsto x$.

(ii) Die Gruppe G operiert auf kanonische Weise auf sich selbst, durch ihre Verknüpfung $G \times G \to G$, $(g, h) \mapsto gh$. Diese Operation heißt *Linkstranslationsoperation* von G auf sich selbst.

(iii) Sei allgemeiner $H \subset G$ eine Untergruppe. Dann ist die Verknüpfung

$$G \times G/H \to G/H, \quad (g, g'H) \mapsto gg'H,$$

eine Gruppenoperation von G auf G/H. Sie heißt die *Linkstranslationsoperation* von G auf der Menge G/H der Linksnebenklassen bzgl. H.

(iv) Jede Gruppe G operiert auf sich selbst durch *Konjugation*, d.h., durch den Gruppenhomomorphismus $G \to \mathrm{Aut}(G)$, $g \mapsto c_g$ (siehe Beispiel 1.1.25). Im Gegensatz zu der Linkstranslationsoperation, die Konjugationsoperation ist sogar eine Operation in der Kategorie der Gruppen, da jedes c_g ein Gruppenautomorphismus ist.

(v) Ist $\rho\colon G \to S_X$ eine Gruppenoperation von G auf X und ist $H \subset G$ eine Untergruppe, so ist die Einschränkung $\rho|_H$ eine Gruppenoperation von H auf X. Ist allgemeiner $f\colon H \to G$ ein Gruppenhomomorphismus, so ist $\rho \circ f$ eine Operation von H auf X.

(vi) Nach (ii) und (v) induziert jeder Gruppenhomomorphismus $f\colon H \to G$ eine Operation von H auf G, nämlich $(h, g) \mapsto f(h) \cdot g$.

(vii) Nach der universellen Eigenschaft von $\mathbb{Z}$ (Proposition 1.1.30) definiert jede Permutation $f \in S_X$ eine Operation von $\mathbb{Z}$ auf X, mit zugehöriger Verknüpfung

$$\mathbb{Z} \times X \to X, \quad (n, x) \mapsto f^n(x).$$

Beispiel 1.2.4 (symmetrische Gruppen)**.** Sei X eine Menge. Die symmetrische Gruppe S_X operiert dann auf kanonische Weise auf X, durch die Identität $S_X \to S_X$. Die zugehörige Verknüpfung ist die Auswertungsabbildung

$$S_X \times X \to X, \quad (f, x) \mapsto f(x).$$

Insbesondere operiert S_n auf der Menge $\{1, \ldots, n\}$.

Beispiel 1.2.5 (lineare Gruppen)**.** Sei R ein kommutativer Ring und $n \in \mathbb{N}$. Dann gibt es eine kanonische Operation der Gruppe $\mathrm{GL}_n(R)$ auf der Menge R^n durch Matrixmultiplikation:

$$\mathrm{GL}_n(R) \times R^n \to R^n, \quad (A, x) \mapsto A \cdot x.$$

Dies ist sogar eine Operation in der Kategorie der R-Moduln, denn die Abbildung $R^n \to R^n$, $x \mapsto A \cdot x$, ist R-linear für alle $A \in \mathrm{GL}_n(R)$. Jede Untergruppe von $\mathrm{GL}_n(R)$, z.B. $\mathrm{SL}_n(R)$, operiert dann auch auf dem R-Modul R^n.

Bemerkung 1.2.6. Eine Operation einer Gruppe G in der Kategorie der K-Vektorräume heißt *lineare Darstellung* von G über K. Solche Operationen werden in der *Darstellungstheorie* untersucht, die viele Anwendungen in der Mathematik und in der Physik hat.

Beispiel 1.2.7 (orthogonale Gruppe)**.** Die orthogonale Gruppe $\mathrm{O}(n)$ ist eine Untergruppe von $\mathrm{GL}_n(\mathbb{R})$ und damit operiert auf dem $\mathbb{R}$-Vektorraum $\mathbb{R}^n$. Da jede Abbildung $x \mapsto A \cdot x$ mit $A \in \mathrm{O}(n)$ sogar eine lineare *Isometrie* von $\mathbb{R}^n$ ist, ist diese Operation auch eine Operation in der Kategorie der metrischen Räume oder der euklidischen Räume.

Beispiel 1.2.8 (Diedergruppe)**.** Sei $n \in \mathbb{N} \setminus \{0\}$ und sei

$$E_n = \{\rho_n^i(1, 0) \mid i \in \{0, \ldots, n-1\}\} \subset \mathbb{R}^2,$$

wobei ρ_n die Drehung um den Winkel $2\pi/n$ ist. Die Diedergruppe D_n besteht aus allen linearen Isometrien von $\mathbb{R}^2$, die E_n auf sich selbst abbilden. Die Verknüpfung

$$D_n \times E_n \to E_n, \quad (f, x) \mapsto f(x),$$

ist dann eine Operation von D_n auf der n-elementigen Menge E_n. Identifiziert man diese Menge mit $\{1, \ldots, n\}$, so erhält man einen Gruppenhomomorphismus

$$D_n \to S_n.$$

Falls $n \geq 3$ ist dieser Gruppenhomomorphismus injektiv. Wenn $n = 3$ ist er sogar bijektiv, d.h., ein Isomorphismus zwischen D_3 und S_3. Wenn $n = 4$ identifiziert er D_4 mit folgender Untergruppe von S_4:

$$\{\mathrm{id}, (1\ 2\ 3\ 4), (1\ 3)(2\ 4), (1\ 4\ 3\ 2), (2\ 4), (1\ 4)(2\ 3), (1\ 3), (1\ 2)(3\ 4)\}.$$

Beispiel 1.2.9 (Einheitengruppe)**.** Sei R ein Ring. Dann ist die eingeschränkte Multiplikation $R^\times \times R \to R$, $(x, y) \mapsto xy$, eine Operation der Einheitengruppe $R^\times$ auf der Menge R. Ist allgemeiner M ein R-Modul, so ist die eingeschränkte Skalarmultiplikation $R^\times \times M \to M$ eine Operation von $R^\times$ auf der Menge M.

Bemerkung 1.2.10 (Morphismen von G-Mengen)**.** Sei G eine feste Gruppe und seien X und Y zwei G-Mengen. Eine Abbildung $f\colon X \to Y$ heißt *G-äquivariant*, wenn für alle $g \in G$ und $x \in X$ gilt $f(g \cdot x) = g \cdot f(x)$. G-Mengen und G-äquivariante Abbildungen bilden dann eine Kategorie.

Bemerkung 1.2.11 (Gruppenoperationen als Funktoren)**.** Sei G eine Gruppe, $\mathcal{C}$ eine Kategorie und X ein Objekt von $\mathcal{C}$. Eine Operation von G auf X ist äquivalent zu einem Funktor $F\colon \mathcal{B}G \to \mathcal{C}$ mit $F(*) = X$ (siehe LA.A.2.11). Unter diesem Gesichtspunkt ist eine G-äquivariante Abbildung zwischen G-Mengen das Gleiche wie eine natürliche Transformation zwischen Funktoren $\mathcal{B}G \to \mathcal{S}\mathrm{et}$. Das heißt, die Kategorie von G-Mengen ist äquivalent zu der Kategorie von Funktoren $\mathrm{Fun}(\mathcal{B}G, \mathcal{S}\mathrm{et})$ (Definition LA.A.3.2).

Bemerkung 1.2.12 (Links- und Rechtsoperationen)**.** Eine Gruppenoperation wie in Definition 1.2.1 heißt manchmal *Linksoperation*. Eine *Rechtsoperation* von G auf X ist dann ein Gruppenhomomorphismus $G^{\mathrm{op}} \to S_X$, wobei G^{op} die Gruppe G mit der umgekehrten Verknüpfung ist: $(g, h) \mapsto h \cdot g$. Der Unterschied zwischen Links- und Rechtsoperationen ist ganz ähnlich wie der Unterschied zwischen Links- und Rechtsmoduln (Bemerkung LA.8.1.29). Eine Rechtsoperation entspricht einer Verknüpfung $X \times G \to X$, $(x, g) \mapsto x \cdot g$, wie in Proposition 1.2.2, aber das Axiom (ii) spiegelt sich: $(x \cdot h) \cdot g = x \cdot (h \cdot g)$.

Wir untersuchen jetzt einige elementare Eigenschaften von Gruppenoperationen:

Definition 1.2.13 (treue, freie, transitive Operation)**.** Eine Operation der Gruppe G auf der Menge X (oder eine G-Menge X) heißt:

- *treu*, wenn der Gruppenhomomorphismus $\rho\colon G \to S_X$ injektiv ist, d.h., wenn aus $g \cdot x = x$ für alle $x \in X$ folgt $g = e$.
- *frei*, wenn für alle $x \in X$ und $g \in G \setminus \{e\}$ gilt $g \cdot x \neq x$.
- *transitiv*, wenn X nicht leer ist und für alle $x, y \in X$ existiert ein $g \in G$ mit $g \cdot x = y$.

Beispiel 1.2.14 (Linkstranslationsoperation)**.** Sei G eine Gruppe und $H < G$ eine Untergruppe.

(i) Die Linkstranslationsoperation von G auf sich selbst (Beispiel 1.2.3(ii)) ist frei, denn: Aus $gh = h$ folgt $g = e$.

(ii) Die Linkstranslationsoperation von G auf G/H ist genau dann frei, wenn $H = \{e\}$. Denn es gilt $\rho(h)(H) = hH = H$ für alle $h \in H$. Sie kann aber treu sein, selbst wenn $H \neq \{e\}$. Zum Beispiel ist die Linkstranslationsoperation von S_3 auf der dreielementigen Menge $S_3/\langle(1\,2)\rangle$ treu, wie man leicht nachrechnen kann.

(iii) Die Linkstranslationsoperation von G auf G/H ist transitiv, denn G/H ist nicht leer und für alle $gH, g'H \in G/H$ gilt $(g'g^{-1})gH = g'H$.

Beispiel 1.2.15.

(i) Die kanonische Operation von S_X auf X (Beispiel 1.2.4) ist treu. Sie ist genau dann frei, wenn $|X| \leq 2$. Sie ist genau dann transitiv, wenn $X \neq \varnothing$.

(ii) Sei $n \geq 1$. Die Operation von D_n auf E_n aus Beispiel 1.2.8 ist transitiv und nicht frei. Sie ist aber treu, sofern $n \geq 3$, da der Gruppenhomomorphismus $D_n \to S_n$ injektiv ist.

(iii) Die Gruppe $(\mathbb{R}, +)$ operiert auf dem Einheitskreis $S^1 = \{z \in \mathbb{C} \mid |z| = 1\}$ durch

$$\mathbb{R} \times S^1 \to S^1, \quad (x, z) \mapsto e^{ix} z$$

(diese Operation ist die Komposition der Linkstranslationsoperation der Gruppe S^1 auf sich selbst mit dem Gruppenhomomorphismus $\mathbb{R} \to S^1$, $x \mapsto e^{ix}$). Diese Operation ist transitiv aber nicht treu: Der Kern von $\rho\colon \mathbb{R} \to S_{S^1}$ ist die Untergruppe $2\pi\mathbb{Z} \subset \mathbb{R}$.

(iv) Sei K ein Körper und $n \in \mathbb{N}_{\geq 1}$. Die Operation von $\mathrm{GL}_n(K)$ auf K^n ist nicht transitiv, denn für alle $A \in \mathrm{GL}_n(K)$ gilt $A \cdot 0 = 0$. Die eingeschränkte Operation

$$\mathrm{GL}_n(K) \times (K^n \setminus \{0\}) \to K^n \setminus \{0\}$$

ist aber transitiv, d.h.: Für alle $x, y \in K^n \setminus \{0\}$ gibt es ein $A \in \mathrm{GL}_n(K)$ mit $A \cdot x = y$.

(v) Sei $\alpha \in \mathbb{R}$ und sei $r_\alpha \colon S^1 \to S^1$ die Drehung um den Winkel α. Die induzierte Operation

$$\mathbb{Z} \times S^1 \to S^1, \quad (n, x) \mapsto r_\alpha^n(x),$$

ist genau dann frei, wenn α kein rationales Vielfaches von 2π ist.

Satz 1.2.16 (Satz von Cayley)**.** *Sei G eine Gruppe. Dann ist G zu einer Untergruppe der symmetrischen Gruppe S_G isomorph. Genauer ist die Abbildung*

$$\rho \colon G \to S_G, \quad g \mapsto (h \mapsto gh),$$

ein injektiver Gruppenhomomorphismus.

Beweis. Die Abbildung ρ ist die Linkstranslationsoperation von G auf sich selbst (Beispiel 1.2.3(ii)), also ist ρ ein Gruppenhomomorphismus. Es bleibt zu zeigen, dass ρ injektiv ist. Aber wenn $\rho(g) = \rho(g')$, dann gilt insbesondere

$$g = \rho(g)(e) = \rho(g')(e) = g'. \qquad \square$$

Korollar 1.2.17. *Sei G eine endliche Gruppe mit $|G| = n$. Dann ist G zu einer Untergruppe von S_n isomorph.*

1.2.2 Bahnen und Stabilisatoren

Definition 1.2.18 (Bahn, Bahnenraum)**.** Sei X eine G-Menge. Die *Bahn* (genauer die *G-Bahn*) oder der *Orbit* eines Elements $x \in X$ ist die Teilmenge

$$Gx := \{g \cdot x \mid g \in G\} \subset X.$$

Der *Bahnenraum* oder *Orbitraum* der G-Menge X ist die Menge

$$X/G := \{Gx \mid x \in X\}$$

aller Bahnen.

Bemerkung 1.2.19 (Bahnen als Äquivalenzklassen)**.** Sei X eine G-Menge. Man definiert eine Relation $\sim_G$ auf X durch

$$x \sim_G y \quad \Longleftrightarrow \quad \text{es gibt ein } g \in G \text{ mit } g \cdot x = y.$$

Dann ist $\sim_G$ eine Äquivalenrelation auf X, und die Äquivalenzklasse eines Elements $x \in X$ ist genau die G-Bahn Gx. Also gilt

$$X/G = X/{\sim_G},$$

d.h., der Bahnenraum der G-Menge X ist die Quotientenmenge von X modulo $\sim_G$. Insbesondere bilden die G-Bahnen von X eine *Partition* von X (Proposition LA.1.4.6).

Beispiel 1.2.20.

(i) Wir betrachten die Operation der Gruppe $\mathrm{O}(n)$ auf $\mathbb{R}^n$. Die Bahnen sind dann genau die $(n-1)$-Sphären

$$S_r^{n-1} := \{x \in \mathbb{R}^n \mid \|x\| = r\}$$

mit $r \in \mathbb{R}_{\geq 0}$, denn: Für alle $x \in \mathbb{R}^n$ und $A \in \mathrm{O}(n)$ gilt $\|Ax\| = \|x\|$, so dass x und Ax auf derselben Sphäre liegen. Umgekehrt gibt es zu je zwei Vektoren $x, y \in S_r^{n-1}$ eine orthogonale Matrix $A \in O(n)$ mit $A \cdot x = y$ (nach Korollar LA.7.2.34).

(ii) Sei $\alpha \in \mathbb{R}$ und sei
$$\mathbb{Z} \times S^1 \to S^1, \quad (n, x) \mapsto r_\alpha^n(x),$$
die Operation aus Beispiel 1.2.15(v). Die Bahn von $x \in S^1$ unter dieser Operation ist die Teilmenge $\{r_\alpha^n(x) \mid n \in \mathbb{Z}\} \subset S^1$. Sie ist endlich, wenn α ein rationales Vielfaches von 2π ist, sonst ist sie unendlich.

(iii) Sei G eine Gruppe. Die Bahn von $g \in G$ unter der Konjugationsoperation von G auf sich selbst heißt die *Konjugationsklasse* von g. Sie besteht aus allen zu g konjugierten Elementen hgh^{-1} mit $h \in G$.

Definition 1.2.21 (Stabilisator, Fixpunktmenge)**.** Sei X eine G-Menge.

- Der *Stabilisator* oder die *Standgruppe* eines Elements $x \in X$ ist die Teilmenge
$$G_x := \{g \in G \mid g \cdot x = x\} \subset G.$$
Nach dem Kriterium 1.1.33 ist G_x eine Untergruppe von G.

- Die *Fixpunktmenge* eines Elements $g \in G$ ist die Teilmenge
$$X^g := \{x \in X \mid g \cdot x = x\} \subset X.$$
Die gesamte Fixpunktmenge der Operation ist
$$X^G := \bigcap_{g \in G} X^g \subset X.$$

Beispiel 1.2.22.

(i) Wir betrachten die Operation der Diedergruppe D_n auf E_n wie im Beispiel 1.2.8. Der Stabilisator von $(1, 0) \in E_n$ ist dann die Untergruppe $\langle\sigma\rangle = \{\mathrm{id}, \sigma\}$ von D_n. Die Fixpunktmenge E_n^σ besteht nur aus dem Punkt $(1, 0)$, wenn n ungerade ist, und aus den zwei Punkten $(\pm 1, 0)$, wenn n gerade ist.

(ii) Sei X eine Menge. Der Stabilisator eines Elements $x \in X$ unter der Operation von S_X ist isomorph zu $S_{X\setminus\{x\}}$:
$$(S_X)_x \xrightarrow{\sim} S_{X\setminus\{x\}}, \quad f \mapsto f|_{X\setminus\{x\}}.$$

(iii) Sei (X, d) ein metrischer Raum und sei $x \in X$. Dann ist die Untergruppe $\mathrm{Isom}_x(X, d)$ aus Beispiel 1.1.40 genau der Stabilisator von x unter der Operation der Isometriegruppe $\mathrm{Isom}(X, d)$ auf X.

Bemerkung 1.2.23. Sie X eine G-Menge. Dann:

- X ist genau dann treu, wenn für alle $g \in G \setminus \{e\}$ gilt $X^g \neq X$.
- X ist genau dann frei, wenn für alle $x \in X$ gilt $G_x = \{e\}$.
- X ist genau dann transitiv, wenn der Bahnenraum X/G genau ein Element besitzt.

Bemerkung 1.2.24. Es gilt $X^g = X^{\langle g\rangle}$, d.h., jedes Element von X, das von g fixiert wird, wird auch von allen Potenzen von g fixiert.

Satz 1.2.25 (Bahnformel)**.** *Sei G eine Gruppe und X eine G-Menge. Für jedes $x \in X$ ist die Abbildung*
$$G/G_x \to Gx, \quad gG_x \mapsto gx,$$
wohldefiniert und bijektiv. Insbesondere gilt
$$[G : G_x] = |Gx|,$$
d.h., die Länge der Bahn von x ist gleich dem Index des Stabilisators von x.

Beweis. Sei $f_x\colon G \to Gx$ die Abbildung $g \mapsto gx$. Wenn $g_1 \sim_{G_x} g_2$, d.h., wenn $g_2^{-1}g_1 \in G_x$, dann gilt

$$g_2^{-1}g_1x = x \quad \text{und daher} \quad g_1x = g_2x.$$

Nach der universellen Eigenschaft der Quotientenmenge erhalten wir eine induzierte Abbildung

$$\bar{f}_x\colon G/G_x \to Gx, \quad gG_x \mapsto gx.$$

Nach Definition der Bahn ist $\bar{f}_x$ surjektiv. Zur Injektivität, seien $g_1G_x, g_2G_x \in G/G_x$ zwei Linksnebenklassen mit $g_1x = g_2x$. Dann gilt $g_2^{-1}g_1x = x$, d.h., $g_2^{-1}g_1$ liegt im Stabilisator G_x, so dass $g_1G_x = g_2G_x$. □

Beispiel 1.2.26. Die Operation von S_3 auf $\{1,2,3\}$ ist transitiv. Der Stabilisator von 3 ist die Untergruppe $H = \{\mathrm{id}, (1\ 2)\} < S_3$. Nach Satz 1.2.25 gibt es eine Bijektion

$$S_3/H \xrightarrow{\sim} \{1,2,3\}, \quad [\sigma] \mapsto \sigma(3).$$

Korollar 1.2.27 (Bahnengleichung)**.** *Sei G eine Gruppe und X eine G-Menge. Sei $R \subset X$ ein Repräsentantensystem der G-Bahnen von X (d.h., jede Bahn enthält genau ein Element von R). Dann gilt*

$$|X| = \sum_{x\in R}[G : G_x] = |X^G| + \sum_{x\in R\setminus X^G}[G : G_x].$$

Beweis. Nach Bemerkung 1.2.19 bilden die G-Bahnen von X eine Partition von X. Insbesondere ist X ist die disjunkte Vereinigung der Bahnen Gx, so dass

$$|X| = \sum_{x\in R}|Gx|.$$

Die erste Gleichung folgt nun aus Satz 1.2.25. Die zweite Gleichung folgt aus der weiteren Bemerkung, dass X^G die Vereinigung der einelementigen Bahnen ist. □

Die obigen Begriffe und Sätze kann man insbesondere auf die Konjugationsoperation einer Gruppe G auf sich selbst anwenden. Der Stabilisator eines Elements $g \in G$ heißt in diesem Fall der *Zentralisator* von g:

Definition 1.2.28 (Zentralisator, Zentrum)**.** Sei G eine Gruppe.

- Der *Zentralisator* eines Elements $g \in G$ ist die Untergruppe

$$Z_G(g) = \{h \in G \mid gh = hg\} \subset G.$$

- Das *Zentrum* von G ist die Untergruppe

$$Z(G) = \bigcap_{g\in G} Z_G(g) = \{h \in G \mid \text{für alle } g \in G \text{ gilt } gh = hg\} \subset G.$$

Bemerkung 1.2.29. Der Zentralisator von $g \in G$ ist gleichzeitig der Stabilisator von g sowie die Fixpunktmenge von g unter der Konjugationsoperation von G auf sich selbst. Das Zentrum von G ist daher die gesamte Fixpunktmenge der Konjugationsoperation. Das Zentrum ist außerdem der Kern des Gruppenhomomorphismus $c\colon G \to \mathrm{Aut}(G)$, $g \mapsto c_g$, und damit ist es ein Normalteiler in G.

Korollar 1.2.30 (Klassengleichung)**.** *Sei G eine Gruppe und $R \subset G$ ein Repräsentantensystem der Konjugationsklassen von G. Dann gilt*

$$|G| = \sum_{g\in R}[G : Z_G(g)] = |Z(G)| + \sum_{g\in R\setminus Z(G)}[G : Z_G(g)].$$

Beweis. Das ist der Sonderfall von Korollar 1.2.27 für die Konjugationsoperation von G auf sich selbst. □

1.2.3 Anwendung auf Permutationen

Als weitere Anwendung von Gruppenoperationen beweisen wir einen Struktursatz für Permutationen einer endlichen Menge. Zunächst erinnern wir an den Begriff von Zyklus:

Definition 1.2.31 (Zyklus, Träger)**.** Sei X eine Menge und sei $k \in \mathbb{N}_{\geq 1}$. Eine Permutation $\sigma \in S_X$ heißt *Zyklus der Länge k* oder *k-Zyklus*, wenn es paarweise verschiedene Elemente $x_1, \ldots, x_k \in X$ gibt, so dass $\sigma(x_i) = x_{i+1}$ für alle $i < k$, $\sigma(x_k) = x_1$, und $\sigma(y) = y$ für alle anderen Elemente $y \in X$. Man schreibt dann

$$\sigma = (x_1\ x_2\ \ldots\ x_k).$$

Wenn $k \geq 2$ ist die Menge $\{x_1, \ldots, x_k\}$ eindeutig durch σ bestimmt, und heißt der *Träger* des Zyklus σ.

Bemerkung 1.2.32. Sei X eine Menge und seien $\sigma, \tau \in S_X$ Zyklen der Länge ≥ 2 mit disjunkten Trägern. Dann gilt $\sigma \circ \tau = \tau \circ \sigma$.

Satz 1.2.33 (Zyklenzerlegung)**.** *Sei X eine endliche Menge und sei $\sigma \in S_X$. Dann gibt es ein $r \in \mathbb{N}$ und Zyklen $\sigma_1, \ldots, \sigma_r \in S_X$ der Länge ≥ 2 mit paarweise disjunkten Trägern, so dass*

$$\sigma = \sigma_1 \circ \ldots \circ \sigma_r.$$

Außerdem sind r und die Menge $\{\sigma_1, \ldots, \sigma_r\}$ eindeutig durch σ bestimmt.

Die Zerlegung $\sigma = \sigma_1 \circ \ldots \circ \sigma_r$ heißt die *Zyklenzerlegung* von σ.

Beweis. Zur Eindeutigkeit. Sei $\sigma = \sigma_1 \circ \ldots \circ \sigma_r$ eine solche Zerlegung und sei $X_i \subset X$ der Träger von σ_i. Wir betrachten die Operation der zyklischen Untergruppe $\langle\sigma\rangle$ auf X. Die Bahn eines Elements $x \in X$ ist entweder $\{x\}$ wenn $x \in X^\sigma$ oder X_i wenn $x \in X_i$. Die Teilmengen X_i sind also genau die $\langle\sigma\rangle$-Bahnen mit mindestens zwei Elementen, und r ist die Anzahl solcher Bahnen. Es gilt zudem $\sigma_i|_{X \setminus X_i} = \mathrm{id}$ und $\sigma_i|_{X_i} = \sigma|_{X_i}$, so dass die Zyklen σ_i eindeutig durch σ bestimmt sind.

Zur Existenz. Sei $\sigma \in S_X$. Seien $X_1, \ldots, X_r$ die Bahnen der Operation von $\langle\sigma\rangle$ auf X mit mindestens zwei Elementen, und definiere $\sigma_i \in S_X$ durch:

$$\sigma_i(x) = \begin{cases} \sigma(x), & \text{falls } x \in X_i, \\ x, & \text{andernfalls.} \end{cases}$$

Dann ist σ_i ein Zyklus mit Träger X_i, denn: Ist $x \in X_i$ beliebig, so gilt

$$X_i = \langle\sigma\rangle x = \{\sigma^i(x) \mid i \in \mathbb{Z}\} \quad \text{und somit} \quad \sigma_i = (x\ \sigma(x)\ \cdots\ \sigma^{|X_i|-1}(x)).$$

Nach Definition der σ_i gilt zudem $\sigma = \sigma_1 \circ \ldots \circ \sigma_r$, wie gewünscht. □

Definition 1.2.34 (Typ)**.** Sei X eine endliche Menge mit $|X| = n$ und sei $\sigma \in S_X$. Der *Typ* von σ ist das Tupel $(a_1, \ldots, a_n)$, wobei a_k die Anzahl der Bahnen der Länge k in X unter der Operation von $\langle\sigma\rangle$ ist. Anders gesagt ist $a_1 = |X^\sigma|$, und für $k \geq 2$ ist a_k die Anzahl der Zyklen der Länge k in der Zyklenzerlegung von σ.

Lemma 1.2.35. *Sei X eine Menge, $\sigma = (x_1\ \cdots\ x_k) \in S_X$ ein Zyklus und $\tau \in S_X$ eine beliebige Permutation. Dann gilt*

$$\tau \circ \sigma \circ \tau^{-1} = (\tau(x_1)\ \cdots\ \tau(x_k)).$$

Beweis. Direktes Vergleich von beiden Seiten. □

Proposition 1.2.36 (Konjugationsklassen in symmetrischen Gruppen)**.** *Sei X eine endliche Menge. Zwei Permutationen $\sigma, \sigma' \in S_X$ sind genau dann konjugiert, wenn sie denselben Typ haben.*

Beweis. Sei $\sigma' = \tau\sigma\tau^{-1}$ und sei $\sigma = \sigma_1 \dots \sigma_r$ die Zyklenzerlegung von σ. Da die Konjugationsabbildung c_τ ein Gruppenhomomorphismus ist, gilt

$$\sigma' = c_\tau(\sigma) = c_\tau(\sigma_1) \dots c_\tau(\sigma_r).$$

Nach Lemma 1.2.35 sind die Permutationen $c_\tau(\sigma_i)$ Zyklen mit paarweise disjunkten Trägern. Deswegen ist die obige Zerlegung die Zyklenzerlegung von σ'. Da die Zyklen σ_i und $c_\tau(\sigma_i)$ dieselbe Länge haben, haben σ und σ' denselben Typ.

Seien umgekehrt σ und σ' Permutationen desselben Typs. Man kann dann ihre Zyklenzerlegungen

$$\sigma = \sigma_1 \dots \sigma_r \quad \text{und} \quad \sigma' = \sigma'_1 \dots \sigma'_r$$

so anordnen, dass die Zyklen σ_i und σ'_i dieselbe Länge haben. Sei X_i bzw. X'_i der Träger von σ_i bzw. σ'_i. Dann gilt

$$X = X^\sigma \cup \bigcup_{i=1}^{r} X_i = X^{\sigma'} \cup \bigcup_{i=1}^{r} X'_i,$$

und beide Vereinigungen sind disjunkt. Man kann weiter für jedes i eine solche Bijektion $\tau_i \colon X_i \xrightarrow{\sim} X'_i$ auswählen, dass

$$\sigma_i = (x_1 \ \cdots \ x_k) \quad \Longrightarrow \quad \sigma'_i = (\tau_i(x_1) \ \cdots \ \tau_i(x_k)).$$

Da σ und σ' denselben Typ haben, sind auch die Fixpunktmengen X^σ und $X^{\sigma'}$ gleichmächtig, und wir wählen noch eine Bijektion $\rho \colon X^\sigma \xrightarrow{\sim} X^{\sigma'}$ aus. Zusammen bilden die Bijektionen τ_i und ρ eine Permutation $\tau \colon X \xrightarrow{\sim} X$, die nach Lemma 1.2.35 $\sigma' = \tau\sigma\tau^{-1}$ erfüllt. □

Bemerkung 1.2.37. Sei $|X| = n$. Ein Tupel $(a_1, \dots, a_n)$ ist genau dann der Typ einer Permutation $\sigma \in S_X$, wenn

$$n = \sum_{k=1}^{n} a_k k.$$

Die Anzahl der Konjugationsklassen in S_X ist deswegen die Anzahl der *Zahlpartitionen* von n, d.h., der Zerlegungen von n als Summe von positiven ganzen Zahlen.

Beispiel 1.2.38. In S_4 gibt es genau fünf Konjugationsklassen:

Typ	Zahlpartition	Konjugationsklasse
(4,0,0,0)	1+1+1+1	id
(2,1,0,0)	1+1+2	$(* \ *)$
(1,0,1,0)	1+3	$(* \ * \ *)$
(0,0,0,1)	4	$(* \ * \ * \ *)$
(0,2,0,0)	2+2	$(* \ *)(* \ *)$

Proposition 1.2.39 (Erzeugendensysteme symmetrischer Gruppen)**.** *Sei $n \in \mathbb{N}_{\geq 2}$. Die folgenden Teilmengen von S_n sind Erzeugendensysteme:*

(i) $\{(1\ 2), (2\ 3), \dots, (n-1\ n)\}$.

(ii) $\{(1\ 2), (1\ 2\ \cdots\ n)\}$.

Beweis. Zu (i). Transpositionen bilden ein Erzeugendensystem von S_n nach Lemma LA.5.3.4. Sei $(i\ j)$ eine beliebige Transposition mit $i < j$. Wir beweisen durch Induktion über $j - i$, dass $(i\ j)$ in der von (i) erzeugte Untergruppe liegt. Falls $j - i \geq 2$ gilt

$$(i\ j) = (i\ i+1) \circ (i+1\ j) \circ (i\ i+1)$$

nach Lemma 1.2.35, und man wendet die Induktionsvoraussetzung auf $(i+1\ j)$ an.

Zu (ii). Sei $\tau = (1\ 2\ \cdots\ n)$. Nach Lemma 1.2.35 gilt

$$\tau^i \circ (1\ 2) \circ \tau^{-i} = (i+1\ i+2)$$

für alle $i \in \{0, \ldots, n-2\}$. Nach (i) ist damit $\{(1\ 2), \tau\}$ ein Erzeugendensystem von S_n. □

Proposition 1.2.40 (Erzeugendensysteme alternierender Gruppen)**.** *Sei $n \in \mathbb{N}$. Dann bilden die 3-Zyklen ein Erzeugendensystem von A_n.*

Beweis. Jede gerade Permutation ist die Komposition einer geraden Anzahl von Transpositionen. Es genügt also zu zeigen, dass $\sigma = (i\ j)(k\ l)$ eine Komposition von 3-Zyklen ist. Wir betrachten zwei Fälle:

- Falls $\{i, j\} = \{k, l\}$, dann ist $\sigma = \mathrm{id}$.
- Sonst kann man annehmen, dass $j \neq k$. Dann gilt:

$$(i\ j)(k\ l) = (i\ j)(j\ k)(j\ k)(k\ l) = (i\ j\ k)(j\ k\ l). \qquad \square$$

1.3 Strukturätze für endliche Gruppen

Nach dem Hauptsatz über Moduln über Hauptidealringen (Satz LA.8.3.30(ii)) ist jede endliche *abelsche* Gruppe zu einem Produkt von zyklischen Gruppen

$$\prod_{i=1}^{r} C_{p_i^{n_i}}$$

isomorph, mit eindeutig bestimmten $r \in \mathbb{N}$, Primzahlen p_i und Potenzen $n_i \geq 1$. Ist p eine Primzahl und ist $n \geq 1$, so ist insbesondere die Gruppe C_{p^n} *unzerlegbar*, d.h., sie ist nicht isomorph zu einem Produkt von zwei nicht-trivialen Gruppen. Wenn $n \geq 2$ kann man aber C_{p^n} als *Erweiterung* zweier nicht-trivialen Gruppen darstellen: Es gibt eine kurze exakte Sequenz

$$\{e\} \to C_{p^{n-1}} \to C_{p^n} \to C_p \to \{e\}.$$

Genauer ist die Untergruppe $p\mathbb{Z}/p^n\mathbb{Z} < \mathbb{Z}/p^n\mathbb{Z}$ zu $\mathbb{Z}/p^{n-1}\mathbb{Z}$ isomorph nach dem Homomorphiesatz (angewendet auf den Gruppenhomomorphismus $\mathbb{Z} \twoheadrightarrow p\mathbb{Z}/p^n\mathbb{Z}$, der 1 auf $[p]$ abbildet), und die Quotientengruppe $(\mathbb{Z}/p^n\mathbb{Z})/(p\mathbb{Z}/p^n\mathbb{Z})$ ist zu $\mathbb{Z}/p\mathbb{Z}$ isomorph nach dem zweiten Isomorphiesatz.

Induktiv kann man also die Gruppe C_{p^n} aus der Gruppe C_p durch iterierte Erweiterungen erhalten. Da Produkte auch Erweiterungen sind (Beispiel 1.1.90(i)), ist schließlich jede endliche abelsche Gruppe A eine iterierte Erweiterung der zyklischen Gruppen C_p mit p prim. Genauer gibt es eine Folge von Untergruppen

$$\{e\} = A_n < \cdots < A_1 < A_0 = A$$

und Primzahlen $p_1, \ldots, p_n$, so dass jeder Quotient A_{i-1}/A_i zu C_{p_i} isomorph ist. Ungenauer kann man sagen, dass die zyklischen Gruppen C_p mit p prim alle endlichen abelschen Gruppen durch Erweiterungen „erzeugen“.

Im Abschnitt 1.3.1 verallgemeinern wir diese Aussage auf beliebige endliche Gruppen. Eine Gruppe heißt *einfach*, wenn sie nicht trivial ist und keine Erweiterung zweier nicht-trivialen Gruppen ist (die endlichen einfachen *abelschen* Gruppen sind also die Gruppen C_p mit p prim). Wir zeigen dann, dass die endlichen einfachen Gruppen alle endlichen Gruppen durch Erweiterungen „erzeugen“ (Proposition 1.3.8). Um endliche Gruppen zu klassifizieren, genügt es also

(i) endliche *einfache* Gruppen zu klassifizieren, und

(ii) Erweiterungen von endlichen Gruppen zu verstehen.

Der erste Schritt ist am Ende des 20. Jahrhunderts gelungen und ist eine der wichtigsten Errungenschaften der Gruppentheorie. Die Aussage selbst ist aber zu kompliziert, um sie hier zu erläutern. Das einfachste Beispiel einer nicht-abelschen einfachen Gruppe ist die alternierende Gruppe A_n mit $n \geq 5$ (Satz 1.3.10). Zur zweiten Schritt gibt es aber nur teilweise Resultate. Derzeit sind also endliche Gruppen nur „bis auf Erweiterungen“ klassifiziert.[1]

Im Abschnitt 1.3.2 untersuchen wir den Begriff der *Auflösbarkeit* von Gruppen. Auflösbare Gruppen sind Gruppen, die als iterierte Erweiterungen abelscher Gruppen dargestellt werden können. Diese Gruppen spielen eine wichtige Rolle für die Anwendung der Galoistheorie auf das Problem der Auflösbarkeit von Polynomgleichungen: Die Existenz von Wurzelausdrücken für die Lösungen von Polynomgleichungen vom Grad ≤ 4 hängt damit zusammen, dass die symmetrischen Gruppen S_n mit $n \leq 4$ auflösbar sind (Proposition 1.3.30).

Im Abschnitt 1.3.3 beweisen wir schließlich die wichtigen *Sylow-Sätze*. Die Sylow-Sätze sind allgemeine Struktursätze für endliche Gruppen, die manchmal stark genug sind, um alle Gruppen einer gegebenen Mächtigkeit bis auf Isomorphie zu bestimmen.

1.3.1 Einfache Gruppen

Definition 1.3.1 (Reihe, Normalreihe)**.** Sei G eine Gruppe. Eine Folge von Untergruppen

$$\cdots < G_2 < G_1 < G_0 = G$$

heißt auch eine *Reihe* von Untergruppen von G, und die Quotienten G_{i-1}/G_i heißen die *Faktoren* der Reihe.

Eine Reihe wie oben heißt *Normalreihe*, wenn jedes G_i ein Normalteiler in G_{i-1} ist. In diesem Fall sind die Faktoren G_{i-1}/G_i wieder Gruppen.

Bemerkung 1.3.2. Bei einer Normalreihe wird nicht vorausgesetzt, dass die Untergruppen G_i Normalteiler in G sind. Im Allgemeinen ist das nicht der Fall (siehe Bemerkung 1.1.64). Deswegen werden manchmal Normalreihen wie in Definition 1.3.1 *Subnormalreihen* genannt.

Bemerkung 1.3.3 (endliche Reihen)**.** Sei G eine Gruppe, sei $n \in \mathbb{N}$ und sei

$$\{e\} = G_n < \cdots < G_1 < G_0 = G$$

eine endliche Reihe von Untergruppen von G mit Faktoren $F_i = G_{i-1}/G_i$.

(i) Nach dem Satz von Lagrange gilt

$$|G| = \prod_{i=1}^{n} |F_i|.$$

(ii) Ist die Reihe eine Normalreihe, so gibt es für jedes $i \in \{1, \ldots, n\}$ eine kurze exakte Sequenz

$$\{e\} \to G_i \to G_{i-1} \to F_i \to \{e\}.$$

Die Gruppe G ist damit eine iterierte Erweiterung der Faktoren F_i.

Definition 1.3.4 (einfache Gruppe)**.** Eine Gruppe G heißt *einfach*, wenn sie nicht trivial ist und $\{e\}$ und G die einzigen Normalteiler in G sind.

Beispiel 1.3.5 (einfache abelsche Gruppen)**.** Sei p eine Primzahl. Nach dem Satz von Lagrange ist die zyklische Gruppe C_p einfach. Nach dem Struktursatz für endliche abelsche Gruppen ist umgekehrt jede einfache endliche abelsche Gruppe zu einem C_p isomorph.

[1] Im Dokument `https://www.mimuw.edu.pl/~zbimar/small_groups.pdf` werden alle Gruppen mit ≤ 100 Elementen aufgelistet. Die meisten sind Erweiterungen oder sogar semidirekte Produkte von bekannten Gruppen (wie C_n, S_n, A_n und D_n).

Definition 1.3.6 (Kompositionsreihe)**.** Sei G eine Gruppe. Eine *Kompositionsreihe* von G ist eine endliche Normalreihe

$$\{e\} = G_n \lhd \cdots \lhd G_1 \lhd G_0 = G,$$

deren Faktoren G_{i-1}/G_i einfach sind.

Lemma 1.3.7. *Sei $f\colon G \to H$ ein Gruppenhomomorphismus und sei $N \lhd H$ ein Normalteiler. Dann ist $f^{-1}(N)$ ein Normalteiler in G.*

Beweis. Seien $g \in G$ und $x \in f^{-1}(N)$. Dann gilt $f(gxg^{-1}) = f(g)f(x)f(g)^{-1} \in N$, da $f(x) \in N$ und N ein Normalteiler in H ist. Also gilt $gxg^{-1} \in f^{-1}(N)$, wie gewünscht. □

Proposition 1.3.8 (Existenz von Kompositionsreihen)**.** *Jede endliche Gruppe besitzt eine Kompositionsreihe.*

Beweis. Sei G eine endliche Gruppe. Wir beweisen die Aussage durch Induktion über $|G|$. Falls G trivial ist, ist die Folge $\{e\} = G_0 = G$ eine Kompositionsreihe von G. Sei dann $G \neq \{e\}$. Ist G einfach, so ist $\{e\} = G_1 \lhd G_0 = G$ eine Kompositionsreihe von G. Ansonsten gibt es nach Definition einen Normalteiler $N \lhd G$ mit $1 < |N| < |G|$. Nach dem Satz von Lagrange gilt dann $|G/N| = |G|/|N| < |G|$. Damit können wir die Induktionsvoraussetzung auf beide Gruppen N und G/N anwenden: Es gibt Kompositionsreihen

$$\{e\} = N_n \lhd \cdots \lhd N_1 \lhd N_0 = N \quad \text{und} \quad \{e\} = H_m \lhd \cdots \lhd H_1 \lhd H_0 = G/N.$$

Sei $H_i' = q^{-1}(H_i)$, wobei $q\colon G \twoheadrightarrow G/N$ die Quotientenabbildung ist. Dann ist H_i' eine Untergruppe von G. Nach Lemma 1.3.7 gilt zudem $H_i' \lhd H_{i-1}'$ für jedes $i \in \{1, \dots, m\}$.

Schließlich zeigen wir, dass die Normalreihe

$$\{e\} = N_n \lhd \cdots \lhd N_1 \lhd N_0 = N = H_m' \lhd \cdots \lhd H_1' \lhd H_0' = G$$

eine Kompositionsreihe von G ist. Man braucht nur zu zeigen, dass die Quotientengruppen H_{i-1}'/H_i' einfach sind. Nach dem zweiten Isomorphiesatz gilt aber

$$H_{i-1}'/H_i' \cong (H_{i-1}'/N)/(H_i'/N) = H_{i-1}/H_i,$$

und die Gruppe H_{i-1}/H_i ist einfach nach Voraussetzung. □

Lemma 1.3.9. *Sei $n \geq 5$. Je zwei 3-Zyklen in A_n sind zueinander konjugiert.*

Beweis. Seien $\sigma = (x_1\ x_2\ x_3)$ und $\sigma' = (x_1'\ x_2'\ x_3')$ zwei 3-Zyklen in A_n. Da $n \geq 5$ gibt es zwei weitere Elemente $u, v \in \{1, \dots, n\} \setminus \{x_1, x_2, x_3\}$. Sei $\tau \in S_n$ eine Permutation mit $\tau(x_i) = x_i'$. Falls τ ungerade ist, können wir τ durch $\tau \circ (u\ v)$ ersetzen, so dass $\tau \in A_n$. Nach Lemma 1.2.35 gilt dann $\tau\sigma\tau^{-1} = \sigma'$, wie gewünscht. □

Satz 1.3.10 (Einfachheit der alternierenden Gruppen)**.** *Sei $n \geq 5$. Dann ist die alternierende Gruppe A_n einfach.*

Beweis. Sei $N \lhd A_n$ ein Normalteiler mit $N \neq \{e\}$. Wir zeigen, dass dann bereits $N = A_n$ gilt. Nach Proposition 1.2.40 genügt es zu zeigen, dass N alle 3-Zyklen enthält. Nach Lemma 1.3.9 genügt es sogar zu zeigen, dass N *einen* 3-Zyklus enthält (da N unter Konjugation abgeschlossen ist).

Sei $\sigma \in N \setminus \{e\}$. Da N ein Normalteiler ist, gilt

$$c_\tau(\sigma)\sigma^{-1} \in N$$

für alle $\tau \in A_n$. Wir betrachten die Zyklenzerlegung $\sigma = \sigma_1 \dots \sigma_r$, wobei die Zyklen σ_i nach absteigender Länge angeordnet sind (Satz 1.2.33). Es gilt dann $c_\tau(\sigma) = c_\tau(\sigma_1) \dots c_\tau(\sigma_r)$, und jeder Zyklus $c_\tau(\sigma_i)$ lässt sich mit Lemma 1.2.35 berechnen. Wir zeigen nun durch Fallunterscheidung, dass N einen 3-Zyklus enthält:

(i) Falls $\sigma_1 = (x_1 \ \cdots \ x_k)$ mit $k \geq 4$, sei $\tau = (x_1 \ x_2 \ x_3)$. Dann ist $c_\tau(\sigma_i) = \sigma_i$ für alle $i \geq 2$ und damit

$$c_\tau(\sigma)\sigma^{-1} = c_\tau(\sigma_1)\sigma_1^{-1} = (x_2 \ x_3 \ x_1 \ x_4 \ \cdots \ x_r)(x_r \ \cdots \ x_4 \ x_3 \ x_2 \ x_1) = (x_1 \ x_2 \ x_4).$$

(ii) Falls $\sigma_1 = (x_1 \ x_2 \ x_3)$ und $\sigma_2 = (x_4 \ x_5 \ x_6)$, setzt man $\tau = (x_1 \ x_2 \ x_4)$. Dann gilt

$$\begin{aligned} c_\tau(\sigma)\sigma^{-1} &= c_\tau(\sigma_1\sigma_2)\sigma_2^{-1}\sigma_1^{-1} \\ &= (x_2 \ x_4 \ x_3)(x_1 \ x_5 \ x_6)(x_6 \ x_5 \ x_4)(x_3 \ x_2 \ x_1) \\ &= (x_1 \ x_2 \ x_5 \ x_3 \ x_4). \end{aligned}$$

Nach (i) enthält dann N einen 3-Zyklus.

(iii) Falls $\sigma_1 = (x_1 \ x_2 \ x_3)$ und die anderen σ_i Transpositionen sind, dann gilt $\sigma^2 = \sigma_1^2 = (x_1 \ x_3 \ x_2)$.

(iv) Die letzte Möglichkeit ist, dass alle σ_i Transpositionen sind. Dann ist r eine gerade Zahl ≥ 2. Sei $\sigma_1 = (x_1 \ x_2)$ und $\sigma_2 = (x_3 \ x_4)$. Falls $r = 2$, setzt man $\tau = (x_1 \ x_2 \ x_5)$ mit einem $x_5 \in \{1, \ldots, n\} \setminus \{x_1, x_2, x_3, x_4\}$. Es gilt dann

$$c_\tau(\sigma)\sigma^{-1} = (x_2 \ x_5)(x_3 \ x_4)(x_3 \ x_4)(x_1 \ x_2) = (x_1 \ x_5 \ x_2).$$

Falls $r \geq 4$ sei $\tau = (x_1 \ x_2 \ x_3)$. Dann gilt

$$c_\tau(\sigma)\sigma^{-1} = c_\tau(\sigma_1\sigma_2)\sigma_2^{-1}\sigma_1^{-1} = (x_2 \ x_3)(x_1 \ x_4)(x_3 \ x_4)(x_1 \ x_2) = (x_1 \ x_3)(x_2 \ x_4),$$

und damit können wir den vorherigen Fall $r = 2$ anwenden. □

Bemerkung 1.3.11. Die Gruppe $A_3 \cong C_3$ ist auch einfach. Die Gruppe A_4 ist aber nicht einfach: Die Untergruppe

$$V = \{\mathrm{id}, (1\,2)(3\,4), (1\,3)(2\,4), (1\,4)(2\,3)\} < A_4$$

ist ein Normalteiler in S_4 mit $S_4/V \cong S_3$ und $A_4/V \cong C_3$.

Beispiel 1.3.12. Sei $n \geq 5$ oder $n = 3$. Dann ist

$$\{e\} \lhd A_n \lhd S_n$$

eine Kompositionsreihe von S_n, mit Faktoren A_n und $S_n/A_n \cong C_2$. Die Gruppe S_4 hat eine Kompositionsreihe der Form

$$\{e\} \lhd C \lhd V \lhd A_4 \lhd S_4,$$

wobei $V \cong C_2 \times C_2$ die Untergruppe aus Bemerkung 1.3.11 ist und $C \cong C_2$. Die Faktoren dieser Reihe sind C_2, C_2, C_3 und C_2.

Bemerkung 1.3.13. Die nächste einfachste Familie in der Klassifikation der endlichen einfachen Gruppen ist die Familie der *projektiven speziellen linearen Gruppen* über endlichen Körpern:

$$\mathrm{PSL}_n(\mathbb{F}_q) = \mathrm{SL}_n(\mathbb{F}_q)/Z(\mathrm{SL}_n(\mathbb{F}_q)),$$

wobei $n \in \mathbb{N}_{\geq 2}$ und $q = p^r$ eine Primzahlpotenz ist. Das Zentrum $Z(\mathrm{SL}_n(\mathbb{F}_q))$ besteht aus den Skalarmatrizen λI_n mit $\lambda^n = 1$. Alle diesen Gruppen sind einfach, außer $\mathrm{PSL}_2(\mathbb{F}_2) \cong S_3$ und $\mathrm{PSL}_2(\mathbb{F}_3) \cong A_4$.

Der Satz von Jordan-Hölder ist eine Eindeutigkeitsaussage für Kompositionsreihen:

Satz 1.3.14 (Satz von Jordan-Hölder)**.** *Sei G eine Gruppe und seien*

$$\{e\} = G_r \lhd \cdots \lhd G_1 \lhd G_0 = G$$
$$\{e\} = G'_s \lhd \cdots \lhd G'_1 \lhd G'_0 = G$$

zwei Kompositionsreihen von G mit Faktoren $F_i = G_{i-1}/G_i$ und $F'_i = G'_{i-1}/G'_i$. Dann gibt es eine Bijektion $\sigma\colon \{1,\dots,r\} \to \{1,\dots,s\}$ und Isomorphismen $F_i \cong F'_{\sigma(i)}$ für alle $i \in \{1,\dots,r\}$.

**Beweis.* Wir verwenden Indukton über die Mächtigkeit von G. Falls $G = \{e\}$ ist die Aussage trivial. Falls $G_1 = G'_1$ können wir einfach die Induktionsvoraussetzung auf G_1 anwenden, und daraus das Gewünschte schließen.

Sei also $G_1 \neq G'_1$. Da G_1 und G'_1 Normalteiler in G sind, ist $G_1G'_1$ wieder ein Normalteiler in G (denn $gG_1G'_1 = G_1gG'_1 = G_1G'_1g$). Nach Definition einer Kompositionsreihe sind außerdem G_1 und G'_1 *maximale* Normalteiler in G, d.h., G selbst ist der einzige größere Normalteiler, denn: Ist $N \lhd G$ ein Normalteiler mit $G_1 \subsetneq N$, so ist N/G_1 ein nicht-trivialer Normalteiler in der einfachen Gruppe G/G_1, so dass $N/G_1 = G/G_1$ und damit $N = G$. Es muss also $G_1G'_1 = G$ gelten. Sei $H = G_1 \cap G'_1$. Nach dem ersten Isomorphiesatz gibt es dann Isomorphismen

$$G/G'_1 \cong G_1/H \quad \text{und} \quad G/G_1 \cong G'_1/H. \tag{1.3.15}$$

Insbesondere sind G_1/H und G'_1/H einfach.

Sei nun

$$\{0\} = H_t \lhd \cdots \lhd H_1 \lhd H_0 = H$$

eine Kompositionsreihe von H. Dann sind

$$\{e\} = G_r \lhd \cdots \lhd G_1 \quad \text{und} \quad \{e\} = H_t \lhd \cdots \lhd H_0 = H \lhd G_1$$

zwei Kompositionsreihen von G_1. Nach Induktionsvoraussetzung gilt $r - 1 = t + 1$ und die beiden Reihen haben dieselben Faktoren bis auf Isomorphie. Auf ähnliche Weise sind

$$\{e\} = G'_s \lhd \cdots \lhd G'_1, \quad \text{und} \quad \{e\} = H_t \lhd \cdots \lhd H_0 = H \lhd G'_1$$

zwei Kompositionsreihen von G'_1. Nach Induktionsvoraussetzung gilt $s - 1 = t + 1$ und die beiden Reihen haben dieselben Faktoren bis auf Isomorphie. Damit ist $r = s$, und zusammen mit (1.3.15) schließen wir, dass die gegebenen Reihen dieselben Faktoren bis auf Isomorphie haben. □

1.3.2 Auflösbare Gruppen

Definition 1.3.16 (auflösbare Gruppe)**.** Eine Gruppe G heißt *auflösbar*, wenn sie eine endliche Normalreihe

$$\{e\} = G_n \lhd \cdots \lhd G_1 \lhd G_0 = G$$

besitzt, deren Faktoren G_{i-1}/G_i abelsch sind.

Beispiel 1.3.17.

(i) Abelsche Gruppen sind auflösbar.

(ii) Die Gruppe S_3 ist auflösbar: Sie hat die Normalreihe $\{e\} \lhd A_3 \lhd S_3$, wobei $A_3 \cong C_3$ und $S_3/A_3 \cong C_2$ abelsch sind.

(iii) Die Gruppe S_4 ist auflösbar, da sie eine Normalreihe mit Faktoren C_2, C_2, C_3 und C_2 besitzt (siehe Beispiel 1.3.12).

(iv) Ein semidirektes Produkt $A \rtimes_\varphi B$ von abelschen Gruppen ist auflösbar: Es hat die Normalreihe $\{e\} \lhd A \times \{e\} \lhd A \rtimes_\varphi B$ mit Faktoren A und B. Zum Beispiel ist die Diedergruppe D_n auflösbar für alle $n \geq 1$ (nach Beispiel 1.1.100).

Bemerkung 1.3.18. Eine einfache Gruppe ist genau dann auflösbar, wenn sie abelsch ist. Denn eine einfache Gruppe besitzt keine nicht-triviale Normalreihe. Nach Satz 1.3.10 sind zum Beispiel die Gruppen A_n mit $n \geq 5$ nicht auflösbar.

Proposition 1.3.19 (Vererbungseigenschaften auflösbarer Gruppen)**.**

(i) *Jede Untergruppe einer auflösbaren Gruppe ist auflösbar.*

(ii) *Jede Quotientengruppe einer auflösbaren Gruppe ist auflösbar.*

(iii) *Jede Erweiterung einer auflösbaren Gruppe durch eine auflösbare Gruppe ist auflösbar, das heißt: Ist*

$$\{e\} \to H \xrightarrow{f} G \xrightarrow{g} K \to \{e\}$$

eine kurze exakte Sequenz und sind H und K auflösbar, so ist G auflösbar.

Beweis. Zu (i) *und* (ii). Sei G auflösbar und sei

$$\{e\} = G_n \lhd \cdots \lhd G_1 \lhd G_0 = G$$

eine Normalreihe mit abelschen Faktoren. Ist $H < G$, so ist

$$\{e\} = G_n \cap H \lhd \cdots \lhd G_1 \cap H \lhd G_0 \cap H = H$$

eine Normalreihe mit abelschen Faktoren, denn: Nach dem ersten Isomorphiesatz in G_{i-1} gilt

$$(G_{i-1} \cap H)/(G_i \cap H) = (G_{i-1} \cap H)/((G_{i-1} \cap H) \cap G_i) \cong (G_{i-1} \cap H)G_i/G_i < G_{i-1}/G_i,$$

und G_{i-1}/G_i ist abelsch. Ist $N \lhd G$, so ist

$$\{e\} = G_nN/N \lhd \cdots \lhd G_1N/N \lhd G_0N/N = G/N$$

eine Normalreihe mit abelschen Faktoren, denn:

$$\begin{aligned}
(G_{i-1}N/N)/(G_iN/N) &\cong G_{i-1}N/G_iN && \text{(2. Isomorphiesatz)} \\
&= G_{i-1}(G_iN)/G_iN \\
&\cong G_{i-1}/(G_{i-1} \cap G_iN) && \text{(1. Isomorphiesatz in } G_{i-1}N\text{)} \\
&\cong (G_{i-1}/G_i)/((G_{i-1} \cap G_iN)/G_i), && \text{(2. Isomorphiesatz)}
\end{aligned}$$

und G_{i-1}/G_i ist abelsch.

Zu (iii). Seien $\{e\} = H_n \lhd \cdots \lhd H_0 = H$ und $\{e\} = K_m \lhd \cdots \lhd K_0 = K$ Normalreihen von H und K. Dann ist

$$\{e\} = f(H_n) \lhd \cdots \lhd f(H_0) = g^{-1}(K_m) \lhd \cdots \lhd g^{-1}(K_0) = G$$

eine Normalreihe von G, deren Faktoren zu den Faktoren der beiden gegebenen Reihen isomorph sind:

$$f(H_{i-1})/f(H_i) \cong H_{i-1}/H_i \quad \text{und} \quad g^{-1}(K_{j-1})/g^{-1}(K_j) \cong K_{j-1}/K_j$$

(nach dem Homomorphiesatz). Damit ist G auflösbar, wenn H und K auflösbar sind. □

Definition 1.3.20 (Kommutator, Kommutatorgruppe, abgeleitete Gruppen, abgeleitete Reihe)**.** Sei G eine Gruppe.

- Seien $g, h \in G$. Der *Kommutator* von g und h ist das Element

$$[g, h] := ghg^{-1}h^{-1} \in G.$$

- Die *Kommutatorgruppe* oder *abgeleitete Gruppe* von G ist die von allen Kommutatoren erzeugte Untergruppe von G:

$$[G,G] := \langle \{[g,h] \mid g,h \in G\} \rangle < G.$$

- Sei $n \in \mathbb{N}$. Die *n-te abgeleitete Gruppe* $G^{(n)} < G$ wird rekursiv wie folgt definiert:

$$G^{(0)} := G, \quad G^{(n+1)} := [G^{(n)}, G^{(n)}].$$

- Die Reihe

$$\cdots < G^{(2)} < G^{(1)} < G^{(0)} = G$$

heißt die *abgeleitete Reihe* von G.

Bemerkung 1.3.21.

(i) Es gilt $[g,h] = e$ genau dann, wenn $gh = hg$. Deswegen ist eine Gruppe G genau dann abelsch, wenn $[G,G] = \{e\}$.

(ii) Das Inverse eines Kommutators $[g,h]$ ist der Kommtator $[h,g]$:

$$[g,h]^{-1} = (ghg^{-1}h^{-1})^{-1} = hgh^{-1}g^{-1} = [h,g].$$

Jedes Element der Kommutatorgruppe $[G,G]$ (d.h., jedes Wort in den Kommutatoren wie in Proposition 1.1.45) ist also ein Produkt von Kommutatoren. Im Allgemeinen bilden aber die Kommutatoren selbst keine Untergruppe von G.

(iii) Gruppenhomomorphismen erhalten Kommutatoren: Ist $f\colon G \to H$ ein Gruppenhomomorphismus, so gilt $f([g,h]) = [f(g), f(h)]$. Daraus folgt, dass $f([G,G]) \subset [H,H]$, d.h., f schränkt sich zu einem Gruppenhomomorphismus $f^{(1)}\colon [G,G] \to [H,H]$ ein. Es folgt induktiv daraus, dass sich f für alle $n \in \mathbb{N}$ zu einem Gruppenhomomorphismus

$$f^{(n)}\colon G^{(n)} \to H^{(n)}$$

einschränkt. Damit ist die Konstruktion $G \mapsto G^{(n)}$ ein Funktor (Definition LA.A.2.1).

Beispiel 1.3.22. Ist $n \in \mathbb{N}$, so gilt

$$[S_n, S_n] = A_n.$$

Jeder Kommutator in S_n ist gerade (sein Vorzeichen ist ein Kommutator in der abelschen Gruppe $\{\pm 1\}$), so dass $[S_n, S_n] \subset A_n$. Umgekehrt ist jeder 3-Zyklus $(x_1\ x_2\ x_3)$ ein Kommutator:

$$(x_1\ x_2\ x_3) = (x_1\ x_2) \circ (x_2\ x_3) = c_{(x_1\ x_3)}(x_2\ x_3) \circ (x_2\ x_3) = [(x_1\ x_3), (x_2\ x_3)],$$

so dass $A_n \subset [S_n, S_n]$ nach Proposition 1.2.40.

Proposition 1.3.23. *Sei G eine Gruppe. Die Kommutatorgruppe $[G,G]$ ist ein Normalteiler in G. Damit ist die abgeleitete Reihe von G eine Normalreihe.*

Beweis. Da $[G,G]$ von Kommutatoren erzeugt wird und $c_g\colon G \to G$ ein Gruppenhomomorphismus ist, genügt es zu zeigen, dass für alle $g,h,k \in G$ gilt $g[h,k]g^{-1} \in [G,G]$. Es gilt nämlich $c_g([h,k]) = [c_g(h), c_g(k)] \in [G,G]$. □

Bemerkung 1.3.24. Ist G eine nicht-abelsche einfache Gruppe, so folgt aus Proposition 1.3.23, dass $[G,G] = G$. Zum Beispiel gilt $[A_n, A_n] = A_n$ für alle $n \geq 5$ nach Satz 1.3.10. Eine Gruppe G mit $[G,G] = G$ heißt *perfekt*.

Definition 1.3.25 (Abelianisierung)**.** Sei G eine Gruppe. Die Quotientengruppe

$$G_{\mathrm{ab}} := G/[G,G]$$

heißt die *Abelianisierung* von G.

Beispiel 1.3.26. Für alle $n \geq 2$ induziert das Vorzeichen $\operatorname{sgn}\colon S_n \to \{\pm 1\}$ einen Isomorphismus $(S_n)_{\mathrm{ab}} \cong \{\pm 1\}$. Dies folgt aus Beispiel 1.3.22.

Proposition 1.3.27. *Sei G eine Gruppe.*

(i) *Die Abelianisierung G_{ab} ist abelsch.*

(ii) *Die Abelianisierung G_{ab} ist die größte abelsche Quotientengruppe von G, d.h.: Ist $N \lhd G$ ein solcher Normalteiler, dass G/N abelsch ist, so gilt $[G,G] \subset N$.*

(iii) (universelle Eigenschaft der Abelianisierung) *Sei $q\colon G \to G_{\mathrm{ab}}$ die Quotientenabbildung. Zu jeder* abelschen *Gruppe A und zu jedem Gruppenhomomorphismus $f\colon G \to A$ gibt es* genau einen *Gruppenhomomorphismus $\bar{f}\colon G_{\mathrm{ab}} \to A$ mit $\bar{f} \circ q = f$:*

$$\begin{array}{ccc} G & \xrightarrow{f} & A. \\ {\scriptstyle q}\downarrow & \nearrow_{\exists!\,\bar{f}} & \\ G_{\mathrm{ab}} & & \end{array}$$

Beweis. Zu (i) *und* (ii). Seien $N \lhd G$ und $g, h \in G$. Da die Quotientenabbildung $G \twoheadrightarrow G/N$ ein Gruppenhomomorphismus ist, gilt

$$[gN, hN] = [g,h]N.$$

Damit erhalten wir die Äquivalenzen

$$\begin{aligned} G/N \text{ ist abelsch} &\iff \text{für alle } gN, hN \in G/N \text{ gilt } [gN, hN] = N \\ &\iff \text{für alle } g, h \in G \text{ gilt } [g,h] \in N \\ &\iff [G,G] \subset N. \end{aligned}$$

Zu (iii). Nach der universellen Eigenschaft der Quotientengruppe (Proposition 1.1.66) genügt es zu zeigen, dass $[G,G] \subset \ker f$. Für alle $g, h \in G$ gilt $f([g,h]) = [f(g), f(h)] = e$, da A abelsch ist. Also enthält $\ker f$ alle Kommutatoren von G und damit die Kommutatorgruppe $[G,G]$. □

Korollar 1.3.28. *Sei G eine Gruppe. Alle Faktoren der abgeleiteten Reihe von G sind abelsch.*

Beweis. Der n-te Faktor $G^{(n-1)}/G^{(n)}$ ist nach Definition die Abelianisierung von $G^{(n-1)}$. □

Satz 1.3.29 (Charakterisierung der Auflösbarkeit)**.** *Sei G eine endliche Gruppe. Die folgenden Aussagen sind äquivalent:*

(i) *G ist auflösbar.*

(ii) *Es gibt ein $n \in \mathbb{N}$ mit $G^{(n)} = \{e\}$.*

(iii) *G besitzt eine Kompositionsreihe mit abelschen Faktoren.*

(iv) *G besitzt eine endliche Normalreihe mit zyklischen Faktoren.*

Beweis. Die Implikation (iii) ⇒ (iv) folgt daraus, dass einfache abelsche Gruppen zyklisch sind, und die Implikation (iv) ⇒ (i) folgt daraus, dass zyklische Gruppen abelsch sind. Die Implikation (ii) ⇒ (i) folgt aus Korollar 1.3.28. Es bleibt die Implikationen (i) ⇒ (ii) und (i) ⇒ (iii) zu zeigen.

Zu (i) ⇒ (ii). Sei $\{e\} = G_n \lhd \cdots \lhd G_0 = G$ eine Normalreihe mit abelschen Faktoren. Wir zeigen durch Induktion über i, dass $G^{(i)} \subset G_i$, damit $G^{(n)}$ trivial ist. Falls $i \geq 1$ gilt also $G^{(i-1)} \subset G_{i-1}$ nach Induktionsvoraussetzung. Mit dem ersten Isomorphiesatz in G_{i-1} erhalten wir

$$G^{(i-1)}/(G_i \cap G^{(i-1)}) \cong G^{(i-1)}G_i/G_i < G_{i-1}/G_i,$$

so dass die Quotientengruppe $G^{(i-1)}/(G_i \cap G^{(i-1)})$ abelsch ist. Aus Proposition 1.3.27(ii) folgt nun $G^{(i)} = [G^{(i-1)}, G^{(i-1)}] \subset G_i \cap G^{(i-1)} \subset G_i$, wie gewünscht.

Zu (i) ⇒ (iii). Sei $\{e\} = G_n \lhd \cdots \lhd G_1 \lhd G_0 = G$ eine Kompositionsreihe von G (die nach Proposition 1.3.8 existiert). Da G auflösbar ist, ist jeder Faktor G_{i-1}/G_i auflösbar nach Proposition 1.3.19(i,ii). Aber die Faktoren sind auch einfach und damit abelsch. □

Proposition 1.3.30 (Auflösbarkeit symmetrischer Gruppen)**.** *Sei $n \in \mathbb{N}$. Die symmetrische Gruppe S_n ist genau dann auflösbar, wenn $n \leq 4$.*

Beweis. Dass die Gruppen S_0, S_1, S_2, S_3 und S_4 auflösbar sind, folgt aus Beispiel 1.3.17. Ist $n \geq 5$, so ist A_n einfach nach Satz 1.3.10. Da A_n nicht abelsch ist, ist es nicht auflösbar. Da A_n eine Untergruppe von S_n ist, ist S_n auch nicht auflösbar nach Proposition 1.3.19. □

Bemerkung 1.3.31 (Satz von Feit-Thompson)**.** Der Satz von Feit-Thompson besagt, dass jede endliche Gruppe mit einer *ungeraden* Anzahl von Elementen auflösbar ist. Dies ist ein besonders schwieriger Satz. Eine unmittelbare Folgerung dieses Satzes ist, dass jede nicht-abelsche endliche einfache Gruppe eine gerade Anzahl von Elementen besitzt.

1.3.3 Die Sylow-Sätze

Definition 1.3.32 (p-Gruppe, p-Untergruppe, p-Sylowgruppe)**.** Sei G eine endliche Gruppe und sei p eine Primzahl.

- G heißt *p-Gruppe*, wenn $|G|$ eine Potenz von p ist.
- Eine Untergruppe $H < G$ heißt *p-Untergruppe*, wenn H eine p-Gruppe ist.
- Eine *p-Sylowgruppe* in G ist eine p-Untergruppe, deren Index nicht durch p teilbar ist.

Bemerkung 1.3.33. Ist k die Vielfachheit von p in $|G|$, so kann man schreiben $|G| = p^k m$ mit $\mathrm{ggT}(p, m) = 1$. Nach dem Satz von Lagrange (genauer nach Korollar 1.1.56) sind die folgenden Aussagen für eine Unterguppe $H < G$ äquivalent:

(i) H ist eine p-Sylowgruppe in G.

(ii) Es gilt $|H| = p^k$.

(iii) Es gilt $[G : H] = m$.

Beispiel 1.3.34.

(i) In S_3 ist A_3 die einzige 3-Sylowgruppe, und jede Transposition erzeugt eine 2-Sylowgruppe.

(ii) In A_4 ist die Untergruppe V aus Bemerkung 1.3.11 eine 2-Sylowgruppe, und jeder 3-Zyklus erzeugt eine 3-Sylowgruppe.

(iii) Die Diedergruppe D_{2^n} ist eine 2-Gruppe.

(iv) Ist p^n eine Primpotenz mit $p \neq 2$, so ist $\langle \rho_{p^n} \rangle$ eine p-Sylowgruppe und $\langle \sigma \rangle$ eine 2-Sylowgruppe in D_{p^n}.

Bemerkung 1.3.35 (p-Sylowgruppen in abelschen Gruppen)**.** Ist A eine endliche abelsche Gruppe, so folgt aus dem Klassifikationssatz, dass die p-Torsionsuntergruppe $T_pA < A$ eine p-Sylowgruppe ist, und zwar die einzige p-Sylowgruppe (siehe Notation LA.8.3.11).

Satz 1.3.36 (Auflösbarkeit der p-Gruppen)**.** *Sei p eine Primzahl und sei G eine endliche p-Gruppe. Dann gilt:*

(i) *Ist $G \neq \{e\}$, so ist das Zentrum $Z(G)$ von G nicht trivial.*

(ii) *G ist auflösbar.*

Beweis. Zu (i). Wir verwenden die Klassengleichung (Korollar 1.2.30):

$$|G| = |Z(G)| + \sum_{g \in R \setminus Z(G)} [G : Z_G(g)],$$

wobei $R \subset G$ ein Repräsentantensystem der Konjugationsklassen ist. Ist $g \in G \setminus Z(G)$, so gilt nach Definiton $Z_G(g) \neq G$. Nach dem Satz von Lagrange ist dann $[G : Z_G(g)] = |G|/|Z_G(g)|$ durch p teilbar. Damit muss auch $|Z(G)|$ durch p teilbar sein, und insbesondere $Z(G) \neq \{e\}$.

Zu (ii). Wir beweisen die Auflösbarkeit von G durch Induktion über $|G|$. Der Fall $G = \{e\}$ ist trivial. Sei also $G \neq \{e\}$. Zur Erinnerung ist das Zentrum $Z(G)$ ein Normalteiler in G (Bemerkung 1.2.29). Wir betrachten dann die Erweiterung

$$\{e\} \to Z(G) \to G \to G/Z(G) \to \{e\}.$$

Nach (i) und dem Satz von Lagrange ist $G/Z(G)$ eine p-Gruppe mit $|G/Z(G)| < |G|$. Nach Induktionsvoraussetzung ist damit $G/Z(G)$ auflösbar. Das Zentrum $Z(G)$ ist abelsch und insbesondere auflösbar. Nach Proposition 1.3.19(iii) schließen wir, dass G auflösbar ist. □

Der Satz von Lagrange sagt insbesondere, dass die Mächtigkeit einer Untergruppe einer endlichen Gruppe G stets ein Teiler von $|G|$ ist. Bei p-Gruppen gibt es eine Umkehrung dieser Aussage:

Korollar 1.3.37. *Sei p eine Primzahl, sei $k \in \mathbb{N}$ und sei G eine endliche Gruppe mit p^k Elementen. Für jedes $l \in \{0, \ldots, k\}$ besitzt dann G eine Untergruppe mit p^l Elementen.*

Beweis. Sei $\{0\} = G_r \lhd \cdots \lhd G_0 = G$ eine Kompositionsreihe von G. Da G auflösbar ist (Satz 1.3.36(ii)), ist jeder Faktor G_{i-1}/G_i abelsch und damit zu C_p isomorph. Daraus folgt induktiv, dass G_i genau p^{k-i} Elementen hat. □

Wie kompliziert können p-Gruppen sein? Gruppen mit p Elementen sind zyklisch (Korollar 1.1.57), und Gruppen mit p^3 Elementen sind nicht unbedingt abelsch (Beispiel: D_4). Wir bestimmen jetzt alle Gruppen mit p^2 Elementen.

Lemma 1.3.38. *Sei G eine Gruppe, so dass $G/Z(G)$ zyklisch ist. Dann ist G abelsch.*

Beweis. Es gilt $G/Z(G) = \langle [t] \rangle$ mit einem $t \in G$. Für jedes $g \in G$ gibt es dann ein $n \in \mathbb{Z}$, so dass $[g] = [t]^n$, d.h., $t^{-n}g \in Z(G)$. Seien $g, h \in G$ und seien $n, m \in \mathbb{Z}$ mit $t^{-n}g, t^{-m}h \in Z(G)$. Dann gilt $g = t^n(t^{-n}g)$ und $h = t^m(t^{-m}g)$, und die vier Elemente t^n, t^m, $t^{-n}g$ und $t^{-m}h$ kommutieren miteinander. Damit gilt $gh = hg$. □

Proposition 1.3.39 (Gruppen mit p^2 Elementen)**.** *Sei p eine Primzahl und sei G eine Gruppe mit p^2 Elementen. Dann ist G entweder zu C_{p^2} oder zu $C_p \times C_p$ isomorph.*

Beweis. Nach der Klassifikation von endlichen abelschen Gruppen genügt es zu zeigen, dass G abelsch ist. Nach Satz 1.3.36(i) ist $Z(G)$ nicht trivial. Die Quotientengruppe $G/Z(G)$ hat also 1 oder p Elementen, und damit ist zyklisch. Nach Lemma 1.3.38 ist G abelsch. □

Definition 1.3.40 (Normalisator)**.** Sei G eine Gruppe. Sie operiert durch Konjugation auf der Menge $\mathrm{Sub}(G)$ ihrer Untergruppen:

$$G \times \mathrm{Sub}(G) \to \mathrm{Sub}(G), \quad (g, H) \mapsto gHg^{-1}.$$

Der Stabilisator einer Untergruppe $H \in \mathrm{Sub}(G)$ unter dieser Operation heißt der *Normalisator* von H und wird mit $N_G(H)$ bezeichnet:

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

Bemerkung 1.3.41. Sei $H < G$ eine Untergruppe. Nach Definition ist H ein Normalteiler in seinem Normalisator $N_G(H)$. Zudem ist $N_G(H)$ die größte Untergruppe von G mit dieser Eigenschaft.

Lemma 1.3.42. *Sei G eine endliche Gruppe und $H < G$ eine Untergruppe. Die Anzahl der zu H konjugierten Untergruppen von G ist gleich dem Index $[G : N_G(H)]$ des Normalisators von H in G.*

Beweis. Dies ist ein Sonderfall der Bahnformel, indem wir die Operation von G durch Konjugation auf der Menge aller Untergruppen von G betrachten. Die Bahn von H ist genau die Menge der zu H konjugierten Untergruppen, und der Stabilisator von H ist nach Definition der Normalisator von H. □

Lemma 1.3.43. *Sei p eine Primzahl, sei $m \in \mathbb{N}$ mit $\mathrm{ggT}(p, m) = 1$, und sei $k \in \mathbb{N} \setminus \{0\}$. Dann ist $\binom{p^k m}{p^k}$ nicht durch p teilbar.*

Beweis. Im Allgemeinen gilt

$$\binom{n}{r} = \frac{n!}{r!(n-r)!} = \prod_{i=0}^{r-1} \frac{n-i}{r-i},$$

und damit

$$v_p\binom{n}{r} = \sum_{i=0}^{r-1} (v_p(n-i) - v_p(r-i)),$$

wobei v_p die Vielfachheit von p bezeichnet. Es genügt also zu zeigen, dass für alle $i \in \{0, \ldots, p^k - 1\}$ gilt $v_p(p^k m - i) = v_p(p^k - i)$. Falls $i = 0$ gilt $v_p(p^k m) = v_p(p^k) + v_p(m)$, und es gilt $v_p(m) = 0$ nach Voraussetzung. Falls $i > 0$, sei v die Vielfachheit von p in i und sei $j = i/p^v$. Für alle $n \in \mathbb{N}$ gilt dann

$$v_p(p^k n - i) = v + v_p(p^{k-v} n - j) = v,$$

denn $v < k$ und j ist nicht durch p teilbar. Insbesondere gilt $v_p(p^k m - i) = v = v_p(p^k - i)$. □

Satz 1.3.44 (Sylow-Sätze)**.** *Sei G eine endliche Gruppe und p eine Primzahl. Sei s_p die Anzahl der p-Sylowgruppen in G.*

(i) (1. Sylow-Satz) *Jede p-Untergruppe von G ist in einer p-Sylowgruppe enthalten. Insbesondere ist $s_p \geq 1$, d.h., es gibt eine p-Sylowgruppe in G.*

(ii) (2. Sylow-Satz) *Je zwei p-Sylowgruppen in G sind konjugiert zueinander. Damit gilt $s_p = [G : N_G(P)]$, wobei $P < G$ eine beliebige p-Sylowgruppe ist. Insbesondere teilt s_p die Mächtigkeit $|G|$.*

(iii) (3. Sylow-Satz) *Es gilt $s_p \equiv 1 \pmod{p}$.*

Beweis. Sei k die Vielfachheit von p in $|G|$, so dass $|G| = p^k m$ mit $\mathrm{ggT}(p, m) = 1$. Wir zeigen zunächst, dass eine p-Sylowgruppe überhaupt existiert. Dazu betrachten wir die Menge

$$\Omega = \{A \subset G \mid |A| = p^k\} \subset \mathcal{P}(G)$$

und die Linkstranslationsoperation von G auf Ω, das heißt:

$$G \times \Omega \to \Omega, \quad (g, A) \mapsto gA = \{ga \mid a \in A\}.$$

Die Bahnengleichung lautet

$$|\Omega| = \sum_{A \in R} [G : G_A],$$

wobei $R \subset \Omega$ ein Repräsentantensystem der Bahnen ist. Für jedes $A \in \Omega$ und jedes $a \in A$ gilt $G_A \cdot a \subset A$ nach Definition des Stabilisators, so dass $|G_A| \leq |A| = p^k$. Die Mächtigkeit von Ω ist der Binomialkoeffizient $\binom{p^k m}{p^k}$, der nicht durch p teilbar ist (Lemma 1.3.43). Damit gibt es mindestens ein $A \in \Omega$, so dass $[G : G_A]$ nicht durch p teilbar ist. Nach dem Satz von Lagrange gilt aber

$$p^k m = |G| = [G : G_A] \cdot |G_A|,$$

so dass $|G_A|$ durch p^k teilbar sein muss, und insbesondere $|G_A| \geq p^k$. Damit gilt $|G_A| = p^k$, d.h., G_A ist eine p-Sylowgruppe in G.

Zu (i) *und* (ii). Sei $H < G$ eine p-Untergruppe und sei $P < G$ eine p-Sylowgruppe. Wir zeigen dann, dass ein $g \in G$ mit $H \subset gPg^{-1}$ existiert. Dies zeigt (i), da gPg^{-1} auch eine p-Sylowgruppe ist, und es zeigt (ii), wenn man für H eine p-Sylowgruppe nimmt (die zweite Aussage in (ii) folgt dann aus Lemma 1.3.42). Wir betrachten die auf H eingeschränkte Linkstranslationsoperation

$$H \times G/P \to G/P, \quad (h, gP) \mapsto hgP.$$

Nach der Bahnengleichung gilt

$$m = [G : P] = |(G/P)^H| + \sum_{gP \in R \setminus (G/P)^H} [H : H_{gP}],$$

wobei $R \subset G/P$ ein Repräsentantensystem der H-Bahnen ist. Ist $gP \in G/P$ kein Fixpunkt der Operation, so gilt $H \neq H_{gP}$ nach Definition des Stabilisators, und damit ist $[H : H_{gP}]$ durch p teilbar (nach dem Satz von Lagrange). Da m nicht durch p teilbar ist, ist auch $|(G/P)^H|$ nicht durch p teilbar. Insbesondere ist $(G/P)^H \neq \varnothing$, d.h., es gibt ein $gP \in G/P$, so dass $hgP = gP$ und damit $g^{-1}hg \in P$ für alle $h \in H$. Dann gilt $H \subset gPg^{-1}$, wie gewünscht.

Zu (iii). Sei Σ die Menge aller p-Sylowgruppen in G und sei $P \in \Sigma$. Wir betrachten die auf P eingeschränkte Konjugationsoperation

$$P \times \Sigma \to \Sigma, \quad (g, Q) \mapsto gQg^{-1}.$$

Die Bahnengleichung lautet

$$s_p = |\Sigma| = |\Sigma^P| + \sum_{Q \in R \setminus \Sigma^P} [P : P_Q],$$

wobei $R \subset \Sigma$ ein Repräsentantensystem der Bahnen ist. Dabei ist Σ^P die Fixpunktmenge der Operation:

$$\Sigma^P = \{Q \in \Sigma \mid \text{für alle } g \in P \text{ gilt } gQg^{-1} = Q\} = \{Q \in \Sigma \mid P \subset N_G(Q)\}.$$

Ist $Q \in \Sigma$ kein Fixpunkt der Operation, so gilt $P_Q \neq P$ nach Definition des Stabilisators, und daher ist $[P : P_Q]$ durch p teilbar (nach dem Satz von Lagrange). Es gilt also

$$s_p \equiv |\Sigma^P| \pmod{p}.$$

Es bleibt zu zeigen, dass die Operation von P auf Σ genau einen Fixpunkt besitzt. Natürlich ist P selbst ein Fixpunkt, denn $P \subset N_G(P)$. Sei $Q \in \Sigma$ mit $P \subset N_G(Q)$. Dann sind beide P und Q p-Sylowgruppen in $N_G(Q)$. Nach (ii) gibt es ein $g \in N_G(Q)$ mit $P = gQg^{-1}$. Aber Q ist ein Normalteiler in $N_G(Q)$, und deswegen $P = Q$. □

Bemerkung 1.3.45 (normale p-Sylowgruppen)**.** Wenn G genau eine p-Sylowgruppe $P < G$ besitzt (d.h., wenn $s_p = 1$), dann ist P automatisch ein Normalteiler in G. Denn die zu P konjugierten Untergruppen von G sind auch p-Sylowgruppen und damit stimmen mit P überein. Der zweite Sylow-Satz impliziert eine Umkehrung: Wenn eine p-Sylowgruppe $P < G$ ein Normalteiler ist (d.h., wenn $N_G(P) = G$), dann ist P die einzige p-Sylowgruppe.

Korollar 1.3.46. *Sei G eine endliche Gruppe, sei p eine Primzahl und sei $n \in \mathbb{N}$, so dass $|G|$ durch p^n teilbar ist. Dann besitzt G eine Untergruppe mit p^n Elementen.*

Beweis. Dies folgt aus Korollar 1.3.37, angewendet auf eine p-Sylowgruppe in G (die nach dem ersten Sylow-Satz existiert). □

Korollar 1.3.47 (Satz von Cauchy)**.** *Sei G eine endliche Gruppe und sei p ein Primteiler von $|G|$. Dann gibt es ein Element der Ordnung p in G.*

Beweis. Nach dem ersten Sylow-Satz gibt es eine nicht-triviale p-Untergruppe $P < G$. Sei $g \in P \setminus \{e\}$. Nach dem Satz von Lagrange gilt $\mathrm{ord}(g) = |\langle g \rangle| = p^k$ mit einem $k \geq 1$. Dann ist $g^{p^{k-1}} \in G$ ein Element der Ordnung p. □

Korollar 1.3.48. *Sei p eine Primzahl. Eine endliche Gruppe G ist genau dann eine p-Gruppe, wenn die Ordnung jedes Elements von G eine Potenz von p ist.*

Beweis. Dass die Ordnung jedes Elements einer endlichen p-Gruppe eine Potenz von p ist, folgt aus dem Satz von Lagrange. Sei umgekehrt G eine endliche Gruppe, in der die Ordnung jedes Elements eine Potenz von p ist. Sei q ein Primteiler von $|G|$. Nach Korollar 1.3.47 gibt es ein $g \in G$ mit $\mathrm{ord}(g) = q$. Also ist $q = p$ und G ist eine p-Gruppe. □

Bemerkung 1.3.49. Nach Korollar 1.3.48 lässt sich der Begriff der p-Gruppe vernünftig auf unendliche Gruppen verallgemeinern: Eine beliebige Gruppe G heißt *p-Gruppe*, wenn die Ordnung jedes Elements von G eine Potenz von p ist.

Beispiel 1.3.50 (Gruppen mit 12 Elementen)**.** Jede Gruppe G mit $|G| = 12$ ist auflösbar. Es gilt $12 = 2^2 \cdot 3$. Seien s_2 bzw. s_3 die Anzahlen der 2-Sylowgruppen bzw. der 3-Sylowgruppen in G. Nach den Sylow-Sätzen gilt

$$\begin{aligned} s_2 | 3 \quad &\text{und} \quad s_2 \equiv 1 \pmod 2, \\ s_3 | 4 \quad &\text{und} \quad s_3 \equiv 1 \pmod 3. \end{aligned}$$

Damit gilt $s_2 \in \{1, 3\}$ und $s_3 \in \{1, 4\}$. Falls $s_2 = 1$, dann ist die enzige 2-Sylowgruppe P ein Normalteiler in G, und G ist eine Erweiterung von G/P durch P. Da $|P| = 4$ und $|G/P| = 3$ sind P und G/P abelsch, und damit ist G auflösbar. Falls $s_3 = 1$, folgern wir auf ähnliche Weise, dass G auflösbar ist. Wir zeigen nun, dass entweder $s_2 = 1$ oder $s_3 = 1$ gelten muss. Angenommen ist $s_3 = 4$, d.h., es gibt vier verschiedene 3-Sylowgruppen P_1, P_2, P_3, P_4. Jedes P_i ist dann isomorph zu C_3, und damit gilt $P_i \cap P_j = \{e\}$ für alle $i \neq j$. Die Vereinigung der P_i enthält also 9 Elementen von G. Ist nun Q eine 2-Sylowgruppe, so gilt $Q \cap P_i = \{e\}$ nach dem Satz von Lagrange ($|Q \cap P_i|$ muss 4 und 3 teilen). Also muss $Q \setminus \{e\}$ genau aus den drei übrigen Elementen von G bestehen. Damit ist Q eindeutig bestimmt, so dass $s_2 = 1$.

Beispiel 1.3.51 (Gruppen mit 24 Elementen)**.** Ist G eine Gruppe mit $|G| = 24$, so ist G nicht einfach. Es gilt $24 = 2^3 \cdot 3$. Seien s_2 bzw. s_3 die Anzahlen der 2-Sylowgruppen bzw. der 3-Sylowgruppen in G. Nach den Sylow-Sätzen gilt

$$\begin{aligned} s_2 | 3 \quad &\text{und} \quad s_2 \equiv 1 \pmod 2, \\ s_3 | 8 \quad &\text{und} \quad s_3 \equiv 1 \pmod 3. \end{aligned}$$

Insbesondere gilt $s_2 \in \{1, 3\}$. Falls $s_2 = 1$, dann ist die einzige 2-Sylowgruppe ein Normalteiler und G ist nicht einfach. Sei also $s_2 = 3$, und sei Σ die 3-elementige Menge der 2-Sylowgruppen. Die Operation von G auf Σ durch Konjugation definiert einen Gruppenhomomorphismus

$$\rho\colon G \to S_\Sigma, \quad (g \mapsto (P \mapsto gPg^{-1})).$$

Sein Kern $N = \ker \rho$ ist damit ein Normalteiler von G. Wir zeigen nun, dass N weder $\{e\}$ noch G ist:

- $N \neq \{e\}$, denn $|G| = 24$ und $|S_\Sigma| = 3! = 6$.
- $N \neq G$, denn die Operation von G auf Σ ist transitiv nach dem zweiten Sylow-Satz.

Als weitere Anwendung der Sylow-Sätze können wir einen Sonderfall des Satzes von Feit-Thompson (Bemerkung 1.3.31) beweisen:

Proposition 1.3.52 (Gruppen mit pq Elementen)**.** *Seien p, q Primzahlen und sei G eine Gruppe mit pq Elementen. Dann ist G auflösbar. Ist $p < q$, so ist G sogar isomorph zu einem semidirekten Produkt $C_q \rtimes_\varphi C_p$.*

Beweis. Ist $p = q$, so ist G auflösbar und sogar abelsch nach Proposition 1.3.39. Sei also $p < q$ und sei s_q die Anzahl der q-Sylowgruppen in G. Da $s_q | pq$ gilt $s_q \in \{1, p, q, pq\}$, und aus $s_q \equiv 1 \pmod q$ und $p < q$ folgt $s_q = 1$. Es gibt damit nur eine q-Sylowgruppe $Q < G$, die ein Normalteiler sein muss (nach Bemerkung 1.3.45). Damit ist G eine Erweiterung der Gruppe $G/Q \cong C_p$ durch die Gruppe $Q \cong C_q$. Sei nun $P < G$ eine p-Sylowgruppe. Nach dem Satz von Lagrange gilt dann $P \cap Q = \{e\}$ und $PQ = G$. Nach dem ersten Isomorphiesatz ist die Abbildung $P \hookrightarrow G \twoheadrightarrow G/Q$ ein Isomorphismus, damit definiert die Inklusionsabbildung $P \hookrightarrow G$ einen Schnitt der Quotientenabbildung $G \twoheadrightarrow G/Q$. Aus Proposition 1.1.97 schließen wir, dass G zu einem semidirekten Produkt von C_q und C_p isomorph ist. □

Beispiel 1.3.53 (Gruppen mit 21 Elementen)**.** Nach Proposition 1.3.52 ist jede Gruppe G mit $|G| = 21$ ein semidirektes Produkt $C_7 \rtimes_\varphi C_3$. Man kann dann alle Gruppen mit 21 Elementen bestimmen, indem man alle möglichen Gruppenhomomorphismen $\varphi\colon C_3 \to \mathrm{Aut}(C_7)$ findet. Nach der universellen Eigenschaft von $\mathbb{Z}/3\mathbb{Z}$ (Korollar 1.1.67) ist ein solcher Gruppenhomomorphismus äquivalent zu einem Automorphismus α von $\mathbb{Z}/7\mathbb{Z}$ mit $\alpha^3 = \mathrm{id}$. Nach der universellen Eigenschaft von $\mathbb{Z}/7\mathbb{Z}$ ist jeder Endomorphismus von $\mathbb{Z}/7\mathbb{Z}$ Multiplikation mit einem $x \in \mathbb{Z}/7\mathbb{Z}$, und er ist genau dann ein Automorphismus, wenn $x \neq 0$ (da $\mathbb{F}_7$ ein Körper ist). Wir suchen also die Elemente $x \in \{1, \dots, 6\}$ mit $x^3 \equiv 1 \pmod 7$, und die sind genau 1, 2 und 4. Seien φ_1, φ_2 und φ_4 die entsprechenden Gruppenhomomorphismen $C_3 \to \mathrm{Aut}(C_7)$ und sei $G_i = C_7 \rtimes_{\varphi_i} C_3$. Da der Gruppenhomomorphismus φ_1 trivial ist, gilt $G_1 = C_7 \times C_3 \cong C_{21}$. Die Gruppenhomomorphismen φ_2 und φ_4 sind aber nicht trivial, so dass G_2 und G_4 nicht abelsch sind. Um die Klassifikation der 21-elementigen Gruppen abzuschließen, muss man noch bemerken, dass G_2 und G_4 isomorph sind. Dies folgt daraus, dass $\varphi_2 = \varphi_4 \circ \sigma$, wobei σ der einzige nicht-triviale Automorphismus von C_3 ist. Es gibt also bis auf Isomorphie genau zwei Gruppen mit 21 Elementen.

Beispiel 1.3.54 (Gruppen mit 33 Elementen)**.** Jede Gruppe G mit $|G| = 33$ ist zyklisch. Nach Proposition 1.3.52 ist G ein semidirektes Produkt $C_{11} \rtimes_\varphi C_3$. Die Behauptung ist dann, dass jeder Gruppenhomomorphismus $\varphi\colon C_3 \to \mathrm{Aut}(C_{11})$ trivial ist, so dass $C_{11} \rtimes_\varphi C_3 = C_{11} \times C_3 \cong C_{33}$. Wie im Beispiel 1.3.53 ist ein solcher Gruppenhomomorphismus durch ein Element $x \in \mathbb{F}_{11}^\times$ mit $x^3 = 1$ bestimmt. Die Gruppe $\mathbb{F}_{11}^\times$ hat aber 10 Elemente, und nach dem Satz von Lagrange ist das neutrale Element 1 das einzige solche Element.

Bemerkung 1.3.55 (Gruppen mit < 60 Elementen)**.** Durch eine aufwendige Einzelfallanalyse kann man mit den Sylow-Sätzen zeigen, dass alle Gruppen mit < 60 Elementen auflösbar sind. Das kleinste Beispiel einer nicht-auflösbaren Gruppe ist damit die einfache Gruppe A_5 mit 60 Elementen.

Kapitel 2

Kommutative Ringe

2.1 Die Kategorie der Ringe

2.1.1 Ringe und Ringhomomorphismen

Wir erinnern zunächst an ein paar grundlegende Definitionen (siehe auch LA.8.1.1).

Definition 2.1.1 (Ring, kommutativer Ring)**.** Ein *Ring* ist ein Tripel $(R, +, \cdot)$ bestehend aus einer Menge R und zwei Verknüpfungen

$$+ \colon R \times R \to R, \quad \cdot \colon R \times R \to R,$$

die als *Addition* und *Multiplikation* bezeichnet werden, mit folgenden Eigenschaften:

(i) $(R, +)$ ist eine abelsche Gruppe. Das neutrale Element bzgl. $+$ wird mit 0 bezeichnet.

(ii) Die Multiplikation ist assoziativ und besitzt ein neutrales Element 1, d.h., für alle $x, y, z \in R$ gilt:
$$x \cdot (y \cdot z) = (x \cdot y) \cdot z \quad \text{und} \quad 1 \cdot x = x = x \cdot 1.$$

(iii) Es gilt das Distributivgesetz, d.h., für alle $x, y, z \in R$ gilt:

$$x \cdot (y + z) = x \cdot y + x \cdot z \quad \text{und} \quad (x + y) \cdot z = x \cdot z + y \cdot z.$$

Der Ring $(R, +, \cdot)$ heißt *kommutativ*, wenn folgende zusätzliche Eigenschaft gilt:

(iv) Die Multiplikation ist kommutativ, d.h., für alle $x, y \in R$ gilt:

$$x \cdot y = y \cdot x.$$

Definition 2.1.2 (Einheit)**.** Sei R ein Ring. Ein Element $x \in R$ heißt *Einheit* von R, wenn es ein inverses Element bzgl. $\cdot$ besitzt, d.h., wenn ein $y \in R$ existiert mit $xy = 1 = yx$. Die Menge aller Einheiten von R wird mit $R^\times$ oder R^* bezeichnet.

Bemerkung 2.1.3 (Gruppen aus Ringen)**.** Ein Ring R hat zwei zugehörige Gruppen:

- Die *additive Gruppe* von R ist die abelsche Gruppe $(R, +)$.
- Die *Einheitengruppe* oder *multiplikative Gruppe* von R ist die Gruppe $(R^\times, \cdot)$. Sie ist abelsch, wenn R kommutativ ist.

Definition 2.1.4 (Nullteiler, Integritätsring)**.**

- Sei R ein Ring. Ein Element $x \in R$ heißt *Nullteiler*, wenn ein Element $y \in R \setminus \{0\}$ existiert, so dass $xy = 0$ oder $yx = 0$.

- Ein *Integritätsring* ist ein kommutativer Ring, in dem 0 der einzige Nullteiler ist.

Bemerkung 2.1.5. In einem Integritätsring gilt $0 \neq 1$. Denn 0 ist nach Definition *kein* Nullteiler im Nullring $\{0\}$.

Definition 2.1.6 (Shiefkörper, Körper)**.**

- Ein *Shiefkörper* oder *Divisionsring* ist ein Ring D mit $D^\times = D \setminus \{0\}$.
- Ein *Körper* ist ein kommutativer Schiefkörper, d.h., ein kommutativer Ring K mit $K^\times = K \setminus \{0\}$.

Bemerkung 2.1.7. Jeder Körper ist ein Integritätsring.

Definition 2.1.8 (Unterring)**.** Sei R ein Ring. Eine Teilmenge $S \subset R$ heißt *Unterring* von R, wenn $1 \in S$ und beide Verknüpfungen $+$ und $\cdot$ sich zu Verknüpfungen $S \times S \to S$ einschränken, so dass das Tripel $(S, +, \cdot)$ wieder ein Ring ist.

Proposition 2.1.9 (Kriterium für Unterringe)**.** *Sei R ein Ring. Eine Teilmenge $S \subset R$ ist genau dann ein Unterring, wenn folgende drei Bedingungen erfüllt sind:*

(i) $1 \in S$ *und* $-1 \in S$.

(ii) *Für alle* $r, s \in S$ *gilt* $r + s \in S$.

(iii) *Für alle* $r, s \in S$ *gilt* $r \cdot s \in S$.

Außerdem gilt in diesem Fall:

(iv) $0 \in S$.

(v) *Für alle* $r \in S$ *gilt* $-r \in S$.

Beweis. Siehe Proposition LA.8.1.8. □

Definition 2.1.10 (Ringhomomorphismus)**.** Seien R und S Ringe. Eine Abbildung $f\colon R \to S$ heißt *Ringhomomorphismus*, wenn folgende Eigenschaften erfüllt sind:

(i) Für alle $r, r' \in R$ gilt
$$f(r + r') = f(r) + f(r').$$

(ii) Für alle $r, r' \in R$ gilt
$$f(r \cdot r') = f(r) \cdot f(r').$$

(iii) Es gilt $f(1) = 1$.

Ein Ringhomomorphismus zwischen Körpern heißt auch *Körperhomomorphismus*.

Bemerkung 2.1.11 (die Kategorie der Ringe)**.** Die Identität auf einem Ring ist stets ein Ringhomomorphismus, und die Komposition zweier Ringhomomorphismen ist wieder ein Ringhomomorphismus. Damit bilden Ringe und Ringhomomorphismen eine Kategorie. Demnach sind die gewöhnlichen Begriffe von *Isomorphismus*, *Endomorphismus* und *Automorphismus* von Ringen definiert (Definitionen LA.A.1.7 und LA.A.1.13).

Bemerkung 2.1.12 (Gruppenhomomorhismen aus Ringhomomorphismen)**.** Ein Ringhomomorphismus $f\colon R \to S$ ist insbesondere ein Gruppenhomomorphismus zwischen den unterliegenden additiven Gruppen $(R, +)$ und $(S, +)$, und er schränkt sich zu einem Gruppenhomomorphismus zwischen den Einheitengruppen $(R^\times, \cdot)$ und $(S^\times, \cdot)$ ein. Aus Proposition 1.1.29 folgt, dass f genau dann injektiv ist, wenn $\ker f = \{0\}$.

Bemerkung 2.1.13 (Kern und Bild von Ringhomomorphismen)**.** Sei $f\colon R \to S$ ein Ringhomomorphismus. Das Bild $\operatorname{im} f$ von f ist stets ein Unterring von S, wie man leicht mit dem Kriterium 2.1.9 nachrechnen kann. Der Kern $\ker f$ von f ist aber kein Unterring von R (außer wenn $S = \{0\}$), denn er kann nur 1 enthalten, wenn $0 = f(1) = 1$ in S gilt. Stattdessen ist der Kern von f stets ein zweiseitiges Ideal in R (siehe Proposition 2.1.41).

Eine bemerkenswerte Eigenschaft von Körperhomomorphismen ist, dass sie automatisch injektiv sind:

Proposition 2.1.14. *Sei D ein Schiefkörper und sei R ein Ring mit $R \neq \{0\}$. Dann ist jeder Ringhomomorphismus $f\colon D \to R$ injektiv. Insbesondere ist jeder Körperhomomorphismus injektiv.*

Beweis. Da f Einheiten auf Einheiten abbildet, gilt

$$f(D \setminus \{0\}) = f(D^\times) \subset R^\times \subset R \setminus \{0\}.$$

Deswegen ist der Kern von f trivial, und somit ist f injektiv. □

Definition 2.1.15 (Produkt von Ringen)**.** Sei $(R_i)_{i\in I}$ eine Familie von Ringen. Das *Produkt* der Familie ist der Ring

$$\prod_{i\in I} R_i = \{(r_i)_{i\in I} \mid \text{für alle } i \in I \text{ gilt } r_i \in R_i\},$$

mit den komponentenweisen Verknüpfungen:

$$(r_i)_{i\in I} + (s_i)_{i\in I} = (r_i + s_i)_{i\in I},$$
$$(r_i)_{i\in I} \cdot (s_i)_{i\in I} = (r_i \cdot s_i)_{i\in I}.$$

Man beobachtet dabei, dass der Ring $\prod_{i\in I} R_i$ kommutativ ist, wenn alle Ringe R_i kommutativ sind.

Die kanonischen Projektionen

$$\pi_e\colon \prod_{i\in I} R_i \to R_e, \quad (r_i)_{i\in I} \mapsto r_e,$$

sind dann Ringhomomorphismen für alle $e \in I$. Das Produkt von Ringen hat die erwartete universelle Eigenschaft, d.h., es ist ein Produkt in der Kategorie der Ringe:

Proposition 2.1.16 (universelle Eigenschaft des Produkts)**.** *Sei $(R_i)_{i\in I}$ eine Familie von Ringen. Zu jedem Ring S und jeder Familie $(f_i\colon S \to R_i)_{i\in I}$ von Ringhomomorphismen gibt es* genau einen *Ringhomomorphismus $f\colon S \to \prod_{i\in I} R_i$, so dass $\pi_i \circ f = f_i$ für alle $i \in I$.*

Beweis. Ganz analog zum Fall der Vektorräume (Proposition LA.6.1.3(i)). □

Bemerkung 2.1.17. Seien R und S Ringe, in denen $0 \neq 1$. Dann ist das Produkt $R \times S$ nicht nullteilerfrei, denn es gilt

$$(1, 0) \cdot (0, 1) = (0, 0) = 0.$$

Insbesondere ist das Produkt zweier Körper kein Körper.

Bemerkung 2.1.18 (Summe von Ringen)**.** Eine Familie von Ringen $(R_i)_{i\in I}$ besitzt auch eine Summe/ein Koprodukt in der Kategorie der Ringe (Definition LA.A.1.16). Wie bei Gruppen (siehe Bemerkung 1.1.84) kann man aber diese Summe nicht einfach beschreiben, und sie ist fast nie ein kommutativer Ring, selbst wenn alle Ringe R_i kommutativ sind.

Summen existieren auch in der Kategorie der *kommutativen* Ringe, und sind einfacher: Man kann zeigen, dass die Summe zweier kommutativen Ringe R und S durch das Tensorprodukt $R \otimes_{\mathbb{Z}} S$ gegeben ist.

Proposition 2.1.19 (universelle Eigenschaft vom Ring $\mathbb{Z}$)**.** *Sei R ein Ring. Dann gibt es* genau einen *Ringhomomorphismus $\mathbb{Z} \to R$.*

Beweis. Nach der universellen Eigenschaft der additiven Gruppe $(\mathbb{Z}, +)$ (Proposition 1.1.30) gibt es genau einen Gruppenhomomorphismus $f\colon \mathbb{Z} \to R$ mit $f(1) = 1$. Es bleibt zu zeigen, dass für alle $n, m \in \mathbb{Z}$ gilt $f(n \cdot m) = f(n) \cdot f(m)$. Dies folgt unmittelbar aus dem Distributivgesetz und der Tatsache, dass jedes $n \in \mathbb{Z}$ gleich $\pm(1 + \cdots + 1)$ ist. □

Bemerkung 2.1.20 (Anfangsobjekte und Endobjekte)**.** Sei $\mathcal{C}$ eine Kategorie. Ein Object $X \in \operatorname{Ob}\mathcal{C}$ heißt *Anfangsobjekt* von $\mathcal{C}$, wenn für alle $Y \in \operatorname{Ob}\mathcal{C}$ die Menge $\operatorname{Mor}_{\mathcal{C}}(X, Y)$ genau ein Element hat, und es heißt *Endobjekt* von $\mathcal{C}$, wenn für alle $Y \in \operatorname{Ob}\mathcal{C}$ die Menge $\operatorname{Mor}_{\mathcal{C}}(Y, X)$ genau ein Element hat. Zum Beispiel:

(i) In der Kategorie der Mengen ist die leere Menge ein Anfangsobjekt und jede einelementige Menge ist ein Endobjekt.

(ii) In der Kategorie der Gruppen ist die triviale Gruppe gleichzeitig ein Anfangsobjekt und ein Endobjekt.

(iii) Proposition 2.1.19 besagt, dass $\mathbb{Z}$ ein Anfangsobjekt der Kategorie der Ringe ist. Der Nullring $\{0\}$ ist ein Endobjekt.

Diese Begriffe sind tatsächlich Sonderfälle der Begriffe der Summe und des Produkts: Ein Object ist genau dann ein Anfangsobjekt bzw. ein Endobjekt, wenn es die Summe bzw. das Produkt der *leeren* Familie von Objekten ist. Insbesondere sind Anfangsobjekte und Endobjekte eindeutig bis auf Isomorphie, wenn sie existieren (Proposition LA.A.1.18).

2.1.2 Polynome und Algebren

Wir erinnern nun an den Begriff des Polynoms über einem Ring (siehe dazu LA.6.3.1). Der Einfachheit halber betrachten wir hier nur Polynome über kommutativen Ringen, obwohl die untenstehende Definition auch für nicht-kommutative Ringe sinnvoll ist.

Definition 2.1.21 (Polynom, Polynomring)**.** Sei R ein kommutativer Ring und sei X ein Symbol, das als *Variable* oder *Unbestimmte* bezeichnet wird. Ein *Polynom* über R in der Variablen X ist ein Ausdruck der Gestalt

$$\sum_{i \in \mathbb{N}} a_i X^i \quad \text{mit} \quad (a_i)_{i \in \mathbb{N}} \in R^{(\mathbb{N})},$$

d.h., wobei nur endlich viele der Elemente $a_i \in R$ nicht null sind. Die Elemente a_i heißen die *Koeffizienten* des Polyoms und die Summanden $a_i X^i$ sind seine *Glieder*. Das Glied $a_0 X^0 = a_0$ heißt *Absolutglied*. Die Menge aller Polynome über R in der Variablen X wird mit $R[X]$ bezeichnet.

Addition und Multiplikation von Polynomen wird wie folgt definiert:

$$\left(\sum_{i \in \mathbb{N}} a_i X^i\right) + \left(\sum_{i \in \mathbb{N}} b_i X^i\right) = \sum_{i \in \mathbb{N}} (a_i + b_i) X^i,$$

$$\left(\sum_{i \in \mathbb{N}} a_i X^i\right) \cdot \left(\sum_{i \in \mathbb{N}} b_i X^i\right) = \sum_{i \in \mathbb{N}} \left(\sum_{j+k=i} a_j b_k\right) X^i.$$

Das Tripel $(R[X], +, \cdot)$ ist dann ein kommutativer Ring und heißt der *Polynomring* über R in der Variablen X.

Bemerkung 2.1.22 (Polynome in mehreren Variablen)**.** Sei R ein kommutativer Ring, I eine Menge und $(X_i)_{i\in I}$ eine Familie von Variablen mit Indexmenge I. Sei $\mathbb{N}^{(I)}$ die Menge aller Abbildungen $n\colon I \to \mathbb{N}$, die null außerhalb einer endlichen Teilmenge von I sind. Ein *Monom* in den Variablen $(X_i)_{i\in I}$ ist ein formaler Ausdruck der Gestalt

$$X^n := \prod_{i\in I} X_i^{n(i)} \quad \text{mit} \quad n \in \mathbb{N}^{(I)},$$

und ein *Polynom* über R in den Variablen $(X_i)_{i\in I}$ ist eine formale R-Linearkombination von Monomen:

$$\sum_{n\in\mathbb{N}^{(I)}} a_n X^n \quad \text{mit} \quad (a_n)_{n\in\mathbb{N}^{(I)}} \in R^{(\mathbb{N}^{(I)})}.$$

Solche Polynome bilden einen kommutativen Ring $R[X_i \mid i \in I]$. Falls $I = \{1,\dots,n\}$ kann man den Polynomring $R[X_1,\dots,X_n]$ mit dem iterierten Polynomring $R[X_1][X_2]\cdots[X_n]$ identifizieren. Zum Beispiel hat ein beliebiges Element von $R[X,Y] = R[X][Y]$ die Form

$$\sum_{i,j\in\mathbb{N}} a_{ij}X^iY^j = \sum_{j\in\mathbb{N}} \left(\sum_{i\in\mathbb{N}} a_{ij}X^i\right) Y^j,$$

wobei nur endlich viele der Koeffizienten $a_{ij} \in R$ nicht null sind.

Definition 2.1.23 (Grad, Leitkoeffizient, monisches Polynom)**.** Sei R ein kommutativer Ring. Der *Grad* eines Polynoms $f = \sum_{i\in\mathbb{N}} a_i X^i$ über R ist

$$\deg(f) := \sup\{i \in \mathbb{N} \mid a_i \neq 0\} \in \{-\infty\} \cup \mathbb{N},$$

wobei $\sup \varnothing = -\infty$. Das Nullpolynom ist also das einzige Polynom vom Grad $-\infty$, und ein Polynom $f \in R[X]$ vom Grad $d \geq 0$ kann wie folgt geschrieben werden, mit $a_d \neq 0$:

$$f = a_dX^d + a_{d-1}X^{d-1} + \cdots + a_1X + a_0.$$

Der Koeffizient $a_d \in R \setminus \{0\}$ heißt der *Leitkoeffizient* von f. Ein Polynom $f \in R[X]$ heißt *monisch* oder *normiert*, wenn $\deg(f) \geq 0$ und der Leitkoeffizient von f gleich 1 ist.

Proposition 2.1.24 (Eigenschaften des Grades)**.** *Sei R ein kommutativer Ring, seien $f, g \in R[X]$ Polynome und sei $r \in R$.*

(i) $\deg(f) = -\infty \iff p = 0$.

(ii) *Es gilt* $\deg(f \cdot g) \leq \deg(f) + \deg(g)$. *Die Gleichheit gilt, wenn f oder g null ist, oder wenn die Leitkoeffizienten von f und g keine Nullteiler sind.*

(iii) *Es gilt* $\deg(f + g) \leq \max\{\deg(f), \deg(g)\}$. *Die Gleichheit gilt, wenn* $\deg(f) \neq \deg(g)$.

(iv) *Es gilt* $\deg(r \cdot f) \leq \deg(f)$. *Die Gleichheit gilt, wenn r kein Nullteiler ist.*

Beweis. Dies folgt unmittelbar aus den Definitionen. □

Bemerkung 2.1.25. Aus Proposition 2.1.24(ii,iii) folgt, dass Polynome vom Grad ≤ 0 einen Unterring von $R[X]$ bilden. Dieser Unterring ist das Bild des injektiven Ringhomomorphismus

$$R \hookrightarrow R[X], \quad a \mapsto aX^0,$$

und kann damit mit dem Ring R identifiziert werden.

Korollar 2.1.26. *Ist R ein Integritätsring, so ist der Polynomring $R[X]$ ein Integritätsring.*

Beweis. Seien $f, g \in R[X] \setminus \{0\}$, so dass $\deg(f) \geq 0$ und $\deg(g) \geq 0$. Nach Proposition 2.1.24(ii) gilt dann $\deg(f \cdot g) = \deg(f) + \deg(g) \geq 0$, so dass $f \cdot g \neq 0$. □

Bemerkung 2.1.27 (der Grad als euklidische Gradfunktion)**.** Ist K ein Körper, so ist der Grad

$$\deg\colon K[X] \setminus \{0\} \to \mathbb{N}$$

eine euklidische Gradfunktion auf $K[X]$ (Definition LA.8.2.12), das heißt: Für alle Polynome $f, g \in K[X]$ mit $g \neq 0$ gibt es Polynome $q, r \in K[X]$ mit $f = qg + r$ und $\deg(r) < \deg(g)$ (die Polynome q und r sind sogar eindeutig bestimmt, siehe Satz LA.6.3.12). Bei allgemeineren kommutativen Ringen gilt dies aber nicht: Zum Beispiel ist der Grad keine euklidische Gradfunktion auf $\mathbb{Z}[X]$, da das Ideal $(2, X)$ in $\mathbb{Z}[X]$ kein Hauptideal ist, aber jeder Integritätsring mit einer euklidischen Gradfunktion ist ein Hauptidealring (Proposition LA.8.2.17).

Wir erinnern schließlich an den Begriff der Algebra (siehe dazu LA.8.1.3):

Definition 2.1.28 (Algebra, Algebrenhomomorphismus)**.** Sei R ein kommutativer Ring.

- Eine *R-Algebra* A ist ein R-Modul mit einer weiteren R-bilinearen Verknüpfung

  $$A \times A \to A, \quad (a, b) \mapsto a \cdot b,$$

  die assoziativ ist und ein neutrales Element $1 \in A$ besitzt. Sie heißt *kommutativ*, wenn diese Verknüpfung kommutativ ist.

- Seien A und A' zwei R-Algebren. Eine Abbildung $f\colon A \to A'$ heißt *R-Algebrenhomomorphismus*, wenn sie R-linear ist, wenn für alle $a, b \in A$ gilt $f(a \cdot b) = f(a) \cdot f(b)$, und wenn $f(1) = 1$.

Die R-Bilinearität der Multiplikation in einer R-Algebra A bedeutet, dass für alle $a, b, c \in A$ und alle $r \in R$ gilt:

$$\begin{aligned} (a + b) \cdot c = a \cdot c + b \cdot c \quad &\text{und} \quad a \cdot (b + c) = a \cdot b + a \cdot c, \\ ra \cdot b = r(a \cdot b) \quad &\text{und} \quad a \cdot rb = r(a \cdot b). \end{aligned}$$

Die ersten beiden Gleichungen sagen, dass die Multiplikation über die Addition distributiv ist, so dass das Tripel $(A, +, \cdot)$ ein Ring ist. Die letzten beiden Gleichungen drücken eine zusätzliche Kompatibilität zwischen der Multiplikation und der Skalarmultiplikation aus. Eine Abbildung zwischen R-Algebren ist genau dann ein R-Algebrenhomomorphismus, wenn sie gleichzeitig R-linear und ein Ringhomomorphismus ist.

Proposition 2.1.29 (kommutative Algebren sind Ringhomomorphismen)**.** *Seien R und A kommutative Ringe. Dann gibt es eine kanonische Bijektion zwischen:*

(i) *R-Algebren, deren unterliegender Ring gleich A ist.*

(ii) *Ringhomomorphismen $f\colon R \to A$.*

Beweis. Dies ist der Sonderfall von Proposition LA.8.1.50, in dem A kommutativ ist. Wenn eine Skalarmultiplikation von R auf A gegeben ist, definiert man f durch $f(r) = r1$, wobei $1 \in A$ das neutrale Element der Multiplikation ist. Ist umgekehrt der Ringhomomorphismus f gegeben, so definiert man eine Skalarmultiplikation von R auf A durch $ra := f(r) \cdot a$. □

Insbesondere hat der Polynomring $R[X]$ eine Struktur von R-Algebra durch den Ringhomomorphismus $R \hookrightarrow R[X]$, $r \mapsto rX^0$.

Proposition 2.1.30 (universelle Eigenschaft des Polynomringes)**.** *Sei R ein kommutativer Ring. Zu jeder R-Algebra A und jedem Element $a \in A$ gibt es* genau einen *R-Algebrenhomomorphismus $\varepsilon_a\colon R[X] \to A$ mit $\varepsilon_a(X) = a$.*

Beweis. Siehe Proposition LA.8.1.45. □

Die Abbildung ε_a heißt der *Einsetzungshomomorphismus* zu a. Man schreibt oft $f(a) \in A$ anstelle von $\varepsilon_a(f)$: Ist $f = \sum_{i\in\mathbb{N}} r_i X^i$, so gilt

$$f(a) = \sum_{i\in\mathbb{N}} r_i a^i \in A.$$

Bemerkung 2.1.31. Proposition 2.1.30 sagt, dass die R-Algebra $R[X]$ den Vergissfunktor $\mathcal{A}\mathrm{lg}_R \to \mathcal{S}\mathrm{et}$ darstellt (siehe Definition LA.A.3.7).

Bemerkung 2.1.32 (Polynome vs. Polynomfunktionen)**.** Jedes Polynom $f \in R[X]$ definiert eine Abbildung

$$f(-)\colon R \to R, \quad r \mapsto \varepsilon_r(f) = f(r).$$

Die Abbildung

$$R[X] \to \mathrm{Abb}(R, R), \quad f \mapsto f(-),$$

ist dann ein Ringhomomorphismus, wobei $\mathrm{Abb}(R, R)$ ein Ring bezüglich der punktweisen Verknüpfungen ist. Ihr Bild $\mathrm{Poly}(R, R) \subset \mathrm{Abb}(R, R)$ ist damit ein Unterring von $\mathrm{Abb}(R, R)$, dessen Elemente *Polynomfunktionen* auf R genannt werden. Im Allgemeinen ist der surjektive Ringhomomorphismus $R[X] \twoheadrightarrow \mathrm{Poly}(R, R)$ nicht injektiv: Ist zum Beispiel K ein endlicher Körper, so ist die Menge $\mathrm{Poly}(K, K)$ endlich, aber $K[X]$ ist unendlich. Man darf also *nicht* Polynome mit Polynomfunktionen identifizieren. Wenn K ein *unendlicher* Körper ist, ist aber die Abbildung $K[X] \to \mathrm{Poly}(K, K)$ bijektiv nach Korollar LA.6.3.18.

Definition 2.1.33 (Nullstelle)**.** Sei R ein kommutativer Ring und $f \in R[X]$. Ein Element $a \in R$ heißt *Nullstelle* von f, wenn $f(a) = 0$.

Proposition 2.1.34 (Charakterisierung der Nullstellen)**.** *Sei R ein kommutativer Ring, sei $f \in R[X]$ und sei $a \in R$. Dann sind die folgenden Aussagen äquivalent:*

(i) *a ist eine Nullstelle von f.*

(ii) *f ist durch das Polynom $X - a$ teilbar.*

Beweis. Die Aussage ist offensichtlich, wenn $a = 0$, denn: $f(0)$ ist das Absolutglied von f, und f ist genau dann durch X teilbar, wenn sei Absolutglied null ist. Wir führen den allgemeinen Fall auf diesen Sonderfall zurück. Der Einsetzungshomomorphismus

$$\varepsilon_{X+a}\colon R[X] \to R[X], \quad f \mapsto f(X + a),$$

ist ein R-Algebrenisomorphismus mit Umkehrabbildung ε_{X-a}, denn: Die Komposition $\varepsilon_{X+a} \circ \varepsilon_{X-a}$ bildet X auf X ab, und damit ist die Identität nach der universellen Eigenschaft der Polynomalgebra. Es gilt $f(a) = 0$ genau dann, wenn 0 eine Nullstelle von $\varepsilon_{X+a}(f)$ ist, d.h., wenn $\varepsilon_{X+a}(f)$ durch X teilbar ist. Da ε_{X-a} ein Ringisomorphismus ist, gilt das Letztere genau dann, wenn $\varepsilon_{X-a}(\varepsilon_{X+a}(f)) = f$ durch $\varepsilon_{X-a}(X) = X - a$ teilbar ist. □

2.1.3 Ideale und Restklassenringe

Definition 2.1.35 (Linksideal, Rechtsideal, zweiseitiges Ideal)**.** Sei R ein Ring. Eine Untergruppe I von $(R, +)$ heißt:

- *Linksideal* in R, wenn für alle $x \in I$ und alle $r \in R$ gilt $rx \in I$.
- *Rechtsideal* in R, wenn für alle $x \in I$ und alle $r \in R$ gilt $xr \in I$.
- *zweiseitiges Ideal* in R, wenn sie gleichzeitig ein Linksideal und ein Rechtsideal ist.

Wenn R kommutativ ist, sind natürlich alle drei Begriffe äquivalent, und man spricht einfach von einem *Ideal* in R.

Bemerkung 2.1.36 (Ideale als Untermoduln)**.** Ein Linksideal bzw. ein Rechtsideal in einem Ring R ist genau ein Linksuntermodul bzw. ein Rechtsuntermodul von R.

Definition 2.1.37 (erzeugtes Ideal, Hauptideal)**.** Sei R ein kommutativer Ring und sei $E \subset R$ eine Teilmenge. Das *von E erzeugte Ideal* in R ist der von E erzeugte Untermodul von R. Dieses Ideal wird mit (E) bezeichnet:

$$(E) := \mathrm{Span}_R(E) = \left\{ \sum_{i=1}^{n} r_i x_i \;\middle|\; n \in \mathbb{N},\ r_i \in E,\ x_i \in E \right\}.$$

Für Elemente $x_1, \ldots, x_n \in R$ schreibt man auch

$$(x_1, \ldots, x_n) := \mathrm{Span}_R\{x_1, \ldots, x_n\} = \left\{ \sum_{i=1}^{n} r_i x_i \;\middle|\; r_1, \ldots, r_n \in R \right\}.$$

Ein Ideal $I \subset R$ heißt *Hauptideal*, wenn ein $x \in R$ mit $I = (x)$ existiert.

Definition 2.1.38 (Hauptidealring)**.** Ein *Hauptidealring* ist ein Integritätsring, in dem jedes Ideal ein Hauptideal ist.

Bekannte Beispiele von Hauptidealringen sind (siehe Korollar LA.8.2.18):

- alle Körper K,
- der Ring $\mathbb{Z}$ der ganzen Zahlen,
- der Ring $\mathbb{Z}[i]$ der Gaußschen Zahlen,
- der Ring $\mathbb{Z}[\omega]$ der Eisenstein-Zahlen,
- der Polynomring $K[X]$ in einer Variablen über einem Körper K,
- der Ring der formalen Potenzreihen $K[[X]]$ über einem Körper K (Beispiel LA.8.2.20).

Beispiel 2.1.39.

(i) In einem beliebigen Ring sind $\{0\}$ und R stets zweiseitige Ideale. Das Ideal $\{0\}$ heißt das *Nullideal* und R heißt das *Einsideal*.

(ii) Für jedes $n \in \mathbb{N}$ ist die Teilmenge $n\mathbb{Z} \subset \mathbb{Z}$ ein Ideal in $\mathbb{Z}$, nämlich das von n erzeugte Ideal. Da $\mathbb{Z}$ ein Hauptidealring ist, gibt es in $\mathbb{Z}$ keine anderen Ideale.

(iii) Sei R ein kommutativer Ring und sei $a \in R$. Die Menge aller Polynome $f \in R[X]$ mit $f(a) = 0$ ist dann ein Ideal in $R[X]$. Nach Proposition 2.1.34 ist dieses Ideal gleich dem Hauptideal $(X - a)$.

Proposition 2.1.40 (Charakterisierung von Körpern über Ideale)**.** *Ein kommutativer Ring $R \neq \{0\}$ ist genau dann ein Körper, wenn $\{0\}$ und R die einzigen Ideale in R sind.*

Beweis. Sei R ein Körper und sei $I \neq \{0\}$ ein Ideal in R. Da I eine Einheit enthält, muss $I = R$ sein. Sei umgekehrt $R \neq \{0\}$ ein kommutativer Ring, der kein Körper ist. Es gibt dann ein Element $x \in R \setminus (\{0\} \cup R^\times)$. Das Ideal $(x) = \{rx \mid r \in R\}$ ist dann weder gleich $\{0\}$ noch gleich R, denn es enthält x aber nicht 1. □

Sei R ein Ring und $I \subset R$ eine Untergruppe. Wie bei Gruppen kann man sich fragen, unter welchen Bedingungen über I ist die Quotientengruppe R/I wieder ein Ring. Wir zeigen jetzt, dass das genau dann der Fall ist, wenn I ein zweiseitiges Ideal ist. Anders gesagt spielen die zweiseitigen Ideale in der Ringtheorie die gleiche Rolle wie die Normalteiler in der Gruppentheorie:

Proposition 2.1.41 (Existenz von Restklassenringen)**.** *Sei R ein Ring, $I \subset R$ eine Untergruppe, $R/I = \{r + I \mid r \in R\}$ die Quotientengruppe von R nach I und $q\colon R \to R/I$ die Quotientenabbildung. Dann sind die folgenden Bedingungen äquivalent:*

(i) *I ist ein zweiseitiges Ideal in R.*

(ii) *Es gibt eine Verknüpfung*
$$\cdot\colon R/I \times R/I \to R/I,$$
so dass $(R/I, +, \cdot)$ ein Ring ist und q ein Ringhomomorphismus ist.

(iii) *Es gibt einen Ringhomomorphismus $f\colon R \to S$ mit $I = \ker f$.*

Sind diese Bedingungen erfüllt, so ist die Verknüpfung in (ii) *eindeutig bestimmt.*

Definition 2.1.42 (Restklassenring)**.** Sei R ein Ring und $I \subset R$ ein zweiseitiges Ideal. Der Ring R/I aus Proposition 2.1.41 heißt der *Restklassenring*, *Quotientenring* oder *Faktorring* von R nach I. Die Elemente von R/I heißen die *Restklassen* von R modulo I. Man schreibt oft $[x]$ für die Restklasse $x + I$.

Beweis der Proposition 2.1.41. Zu (i) $\Rightarrow$ (ii). Damit q ein Ringhomomorphismus ist, muss die Verknüpfung $(r+I, s+I)$ auf $rs+I$ abbilden. Man muss also zunächst nachprüfen, dass die Verknüpfung
$$\begin{aligned} R/I \times R/I &\to R/I, \\ (r + I, s + I) &\mapsto rs + I, \end{aligned}$$
wohldefiniert ist. Seien also $r, r', s, s' \in R$ mit $r+I = r'+I$ und $s+I = s'+I$, d.h., $r-r' \in I$ und $s - s' \in I$. Dann gilt
$$rs - r's' = rs - r's + r's - r's' = (r - r')s + r'(s - s') \in I,$$
da I ein zweiseitiges Ideal ist. Dass die Gruppe R/I mit dieser Verknüpfung ein Ring ist, folgt jetzt unmittelbar aus den entsprechenden Eigenschaften der Multiplikation auf R. Es ist dann auch klar, dass q ein Ringhomomorphismus ist, und dass die obige Verknüpfung dadurch eindeutig bestimmt ist.

Zu (ii) $\Rightarrow$ (iii). Diese Implikation ist trivial, denn $I = \ker q$.

Zu (iii) $\Rightarrow$ (i). Sind $x \in \ker f$ und $r \in R$, so gilt
$$f(rx) = f(r)f(x) = f(r) \cdot 0 = 0 \quad \text{und} \quad f(xr) = f(x)f(r) = 0 \cdot f(r) = 0,$$
so dass $rx, xr \in \ker f$. Damit ist $\ker f$ ein zweiseitiges Ideal in R. □

Bemerkung 2.1.43. Wenn $I \subset R$ nur ein Linksideal ist, dann hat die Quotientengruppe R/I eine Struktur von R-Modul (durch das Multiplizieren von links). Dies ist analog zur Aussage, dass wenn $H < G$ eine Untergruppe ist, dann hat die Quotientenmenge G/H eine Struktur von G-Menge (durch die Linkstranslationsoperation).

Beispiel 2.1.44.

(i) Ist $n \in \mathbb{N} \setminus \{0\}$, so ist der Restklassenring $\mathbb{Z}/n\mathbb{Z}$ ein endlicher Ring mit n Elementen $[0], [1], \ldots, [n-1]$. Im Ring $\mathbb{Z}/12\mathbb{Z}$ gilt zum Beispiel
$$[9] + [5] = [2], \quad [3] - [8] = [7], \quad [3] \cdot [4] = [0], \quad [5] \cdot [5] = [1], \quad \text{usw.}$$

(ii) Sei R ein kommutativer Ring. Dann ist die Komposition der kanonischen Ringhomomorphismen
$$R \hookrightarrow R[X] \twoheadrightarrow R[X]/(X)$$
bijektiv und damit ein Ringisomorphismus. Insbesondere gilt $R[X, Y]/(X) \cong R[Y]$.

(iii) Sei $R = \mathbb{Z}[X]/(f)$ mit $f = X^3 - 2X^2 + 1$. Da f monisch ist, ist R ein freier $\mathbb{Z}$-Modul vom Rang 3 mit Basis $([1], [X], [X^2])$ (Lemma LA.9.2.5), das heißt:

$$\mathbb{Z}[X]/(f) = \{a_2[X]^2 + a_1[X] + a_0 \mid a_i \in \mathbb{Z}\}.$$

Es gilt zudem $[X]^3 = 2[X]^2 - 1$, $[X]^4 = [X][X]^3 = 2[X]^3 - [X] = 4[X]^2 - [X] - 2$, usw.

Beispiel 2.1.45 (diophantische Gleichungen)**.** Eine *diophantische Gleichung* ist eine Polynomgleichung in mehreren Variablen mit ganzzahligen Koeffizienten, die auch mit ganzen Zahlen gelöst werden soll. Das heißt, für ein gegebenes Polynom $f \in \mathbb{Z}[X_1, \ldots, X_r]$ suchen wir die r-Tupel $(x_1, \ldots, x_r) \in \mathbb{Z}^r$ mit $f(x_1, \ldots, x_r) = 0$. Im Allgemeinen sind solche Gleichungen wesentlich schwierig zu lösen: Man kann zum Beispiel zeigen, dass kein Algorithmus existiert, der für beliebiges f entscheiden kann, ob eine Lösung überhaupt existiert oder nicht. Die Aussage, dass die diophantische Gleichung $x^n + y^n - z^n = 0$ mit $n \geq 3$ keine ganzzahligen Lösungen besitzt (außer wenn x, y oder z null ist), ist der berühmte *große Satz von Fermat*, der erst 1994 bewiesen wurde.

Die endlichen Restklassenringe $\mathbb{Z}/n\mathbb{Z}$ sind aber manchmal hilfreich, um zu zeigen, dass *keine* ganzzahligen Lösungen existieren. Denn ist $(x_1, \ldots, x_r) \in \mathbb{Z}^r$ eine Lösung, so muss das Tupel der Restklassen $([x_1], \ldots, [x_r]) \in (\mathbb{Z}/n\mathbb{Z})^r$ eine Lösung der entsprechenden Gleichung im Ring $\mathbb{Z}/n\mathbb{Z}$ sein, und die Menge $(\mathbb{Z}/n\mathbb{Z})^r$ ist endlich. Seien zum Beispiel $x, y \in \mathbb{Z}$, die die Gleichung

$$x^2 + x + y^3 - y^2 = 27$$

erfüllen. Da die Quotientenabbildung $\mathbb{Z} \twoheadrightarrow \mathbb{Z}/2\mathbb{Z} = \mathbb{F}_2$ ein Ringhomomorphismus ist, gilt für die Restklassen $[x], [y] \in \mathbb{F}_2$ die Gleichung

$$[x]^2 + [x] + [y]^3 + [y]^2 = [1].$$

Aber für alle $z \in \mathbb{F}_2$ gelten $z^2 + z = 0$ und $z^3 + z^2 = 0$, so dass kein solches Paar $([x], [y])$ existiert. Die obige diophantische Gleichung hat damit keine ganzzahligen Lösungen.

Proposition 2.1.46 (universelle Eigenschaft des Restklassenringes)**.** *Sei R ein Ring, $I \subset R$ ein zweiseitiges Ideal und $q\colon R \to R/I$ die Quotientenabbildung. Zu jedem Ring S und zu jedem Ringhomomorphismus $f\colon R \to S$ mit $I \subset \ker f$ gibt es* genau einem *Ringhomomorphismus $\bar{f}\colon R/I \to S$ mit $\bar{f} \circ q = f$.*

Beweis. Nach der universellen Eigenschaft der Quotientengruppe (Proposition 1.1.66) gibt es genau einem Gruppenhomomorphismus $\bar{f}$ mit $\bar{f} \circ q = f$. Es bleibt zu zeigen, dass $\bar{f}$ ein Ringhomomorphismus ist. Es gilt aber $\bar{f}([1]) = f(1) = 1$ und

$$\bar{f}([x] \cdot [y]) = \bar{f}([x \cdot y]) = f(x \cdot y) = f(x) \cdot f(y) = \bar{f}([x]) \cdot \bar{f}([y]),$$

wie gewünscht. □

Beispiel 2.1.47 (Körper der Charakteristik p)**.** Sei K ein Körper der Charakteristik $p > 0$. Dann gibt es genau einem Ringhomomorphismus $\mathbb{F}_p \to K$ (der nach Proposition 2.1.14 injektiv ist), denn: Nach der universellen Eigenschaft von $\mathbb{Z}$ (Proposition 2.1.19) gibt es genau einen Ringhomomorphismus $\mathbb{Z} \to K$. Nach Definition der Charakteristik wird p und damit $p\mathbb{Z}$ auf Null abgebildet. Nach der universellen Eigenschaft des Restklassenringes gibt es also genau einen Ringhomomorphismus $\mathbb{Z}/p\mathbb{Z} = \mathbb{F}_p \to K$. Siehe auch Beispiel 2.1.69.

Beispiel 2.1.48 (Algebraische Geometrie)**.** Sei K ein Körper und seien $f_1, \ldots, f_k$ Polynome in n Variablen über K. Die gemeinsamen Nullstellen der Polynome $f_1, \ldots, f_k$ bilden eine Teilmenge $V(f_1, \ldots, f_k)$ von K^n:

$$V(f_1, \ldots, f_k) = \{(x_1, \ldots, x_n) \in K^n \mid \text{für alle } i \in \{1, \ldots, k\} \text{ gilt } f_i(x_1, \ldots, x_n) = 0\}.$$

Solche Teilmengen heißen *affine algebraische Varietäten* über K. Zum Beispiel ist $V(Y - X^2)$ eine Parabel in K^2, und $V(Y^2 - X^2, Z^2) \subset K^3$ ist die Vereinigung zweier Ursprungsgeraden.

Kombiniert man die universellen Eigenschaften des Polynomringes und des Restklassenringes, so erhalten wir eine Bijektion

$$\{K\text{-Algebrenhomomorphismen } K[X_1,\dots,X_n]/(f_1,\dots,f_k) \to K\} \xrightarrow{\sim} V(f_1,\dots,f_k),$$

indem wir einen Homomorphismus g auf das n-Tupel $(g([X_1]),\dots,g([X_n])) \in K^n$ abbilden. Diese Bijektion ist der Ausgangspunkt der Algebraischen Geometrie, die die „geometrischen“ Eigenschaften der Varietät $V(f_1,\dots,f_k)$ mit den „algebraischen“ Eigenschaften der K-Algebra $K[X_1,\dots,X_n]/(f_1,\dots,f_k)$ in engen Zusammenhang bringt.

Proposition 2.1.49 (Ideale im Restklassenring)**.** *Sei R ein Ring, $I \subset R$ ein zweiseitiges Ideal und $q\colon R \to R/I$ die Quotientenabbildung. Dann gibt es eine Bijektion*

$$\{\textit{Linksideale in } R, \textit{ die } I \textit{ enthalten}\} \xrightarrow{\sim} \{\textit{Linksideale in } R/I\},$$
$$J \mapsto J/I.$$

Die Umkehrabbildung bildet ein Linksideal K in R/I auf $q^{-1}(K)$ ab. Es gibt ähnliche Bijektionen mit Rechtsidealen und mit zweiseitigen Idealen.

Beweis. Man bemerkt zunächst, dass J/I ein Linksideal in R/I ist, und dass $q^{-1}(K)$ ein Linksideal in R ist, das I enthält. Damit sind die beiden Abbildungen wohldefiniert. Sie sind dann zueinander invers nach Proposition 1.1.69. □

Die folgende Aussage ist bekannt, aber wurde bisher nicht vollständig bewiesen:

Proposition 2.1.50. *Sei $n \in \mathbb{N}$. Der Restklassenring $\mathbb{Z}/n\mathbb{Z}$ ist genau dann ein Körper, wenn n eine Primzahl ist.*

Beweis. Wir verwenden die Charakterisierung von Körpern über Ideale (Proposition 2.1.40). Die Ideale von $\mathbb{Z}$, die $n\mathbb{Z}$ enthalten, sind genau die Ideale $r\mathbb{Z}$, wobei $r \in \mathbb{N}$ ein Teiler von n ist. Ist n keine Primzahl, so kann man $n = rs$ schreiben mit $r \notin \{1, n\}$. Dann ist $r\mathbb{Z}$ ein Ideal in $\mathbb{Z}$ mit $n\mathbb{Z} \subsetneq r\mathbb{Z} \subsetneq \mathbb{Z}$. Nach Proposition 2.1.49 hat also $\mathbb{Z}/n\mathbb{Z}$ mehr als zwei Ideale, und damit ist es kein Körper. Ist umgekehrt n eine Primzahl, so sind 1 und n die einzigen natürlichen Zahlen, die n teilen, d.h., $\mathbb{Z}$ und $n\mathbb{Z}$ sind die einzigen Ideale in $\mathbb{Z}$, die $n\mathbb{Z}$ enthalten. Nach Proposition 2.1.49 hat dann $\mathbb{Z}/n\mathbb{Z}$ genau zwei Ideale, und damit ist es ein Körper. □

Aus der universellen Eigenschaft des Restklassenringes lassen sich analog zum Fall der Gruppen einen Homomorphiesatz und Isomorphiesätze herleiten. Da die Beweise ganz ähnlich sind, lassen wir die Details weg:

Satz 2.1.51 (Homomorphiesatz für Ringe)**.** *Sei $f\colon R \to S$ ein Ringhomomorphismus. Dann ist die induzierte Abbildung*

$$\bar{f}\colon R/\ker f \to \operatorname{im} f,$$
$$[x] \mapsto f(x),$$

ein Ringisomorphismus.

Satz 2.1.52 (Isomorphiesätze für Ringe)**.** *Sei R ein Ring.*

(i) (erster Isomorphiesatz) *Sei $S \subset R$ ein Unterring und $I \subset R$ ein zweiseitiges Ideal. Dann ist $S + I = \{x + y \mid x \in S,\, y \in I\}$ ein Unterring von R und $S \cap I$ ein zweiseitiges Ideal in S, und es gibt einen Ringisomorphismus*

$$S/(S \cap I) \xrightarrow{\sim} (S + I)/I, \quad x + (S \cap I) \mapsto x + I.$$

(ii) (zweiter Isomorphiesatz) *Seien $I, J \subset R$ zweiseitige Ideale in R mit $I \subset J$. Dann ist J/I ein zweiseitiges Ideal in R/I, und es gibt einen Ringisomorphismus*

$$(R/I)/(J/I) \xrightarrow{\sim} R/J, \quad (x+I)+J/I \mapsto x+J.$$

Beispiel 2.1.53. Es gibt einen $\mathbb{R}$-Algebrenisomorphismus

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

der die Restklasse von X auf i abbildet. Denn nach der universellen Eigenschaft des Polynomringes gibt es einen $\mathbb{R}$-Algebrenhomomorphismus

$$\varphi\colon \mathbb{R}[X] \to \mathbb{C}, \quad X \mapsto i.$$

Er ist surjektiv, denn $a+bi = \varphi(a+bX)$. Nach dem Homomorphiesatz erhalten wir einen Ringisomorphismus

$$\mathbb{R}[X]/\ker\varphi \xrightarrow{\sim} \mathbb{C}.$$

Aus $i^2+1=0$ folgt $X^2+1 \in \ker\varphi$ und daher $(X^2+1) \subset \ker\varphi$. Das Polynom $X^2+1 \in \mathbb{R}[X]$ ist irreduzibel, da es keine Nullstellen in $\mathbb{R}$ besitzt (siehe Beispiel LA.8.2.10(ii)). Damit sind (X^2+1) und $(1) = \mathbb{R}[X]$ die einzigen Ideale, die (X^2+1) enthalten. Da $\ker\varphi \neq \mathbb{R}[X]$ gilt also $\ker\varphi = (X^2+1)$.

Bemerkung 2.1.54 (chinesischer Restsatz)**.** Sei R ein kommutativer Ring und seien $I_1, \ldots, I_n$ paarweise komaximale Ideale in R (Definition LA.8.2.46), d.h., für alle $i \neq j$ gilt $I_i + I_j = R$. Nach der universellen Eigenschaft des Produkts (Proposition 1.1.82) ist die Abbildung

$$\varphi\colon R \to \prod_{i=1}^{n} R/I_i, \quad \varphi(x) = (x+I_1, \ldots x+I_n),$$

ein Ringhomomorphismus. Nach dem chinesischen Restsatz (Satz LA.8.2.49) ist sie surjektiv mit Kern $\bigcap_{i=1}^n I_i$. Nach dem Homomorphiesatz erhalten wir einen Ringisomorphismus

$$\bar{\varphi}\colon R/\big(\textstyle\bigcap_{i=1}^n I_i\big) \xrightarrow{\sim} \displaystyle\prod_{i=1}^{n} R/I_i.$$

Sind zum Beispiel $n, m \in \mathbb{Z}$ teilerfremd, so ist die Abbildung

$$\mathbb{Z}/mn\mathbb{Z} \to \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}, \quad [x] \mapsto ([x],[x]),$$

einen Isomorphismus von Ringen.

2.1.4 Lokalisierung und Quotientenkörper

Lokalisierung ist eine andere wichtige Methode, um neue Ringe aus Ringen zu konstruieren. Ein bekanntes Beispiel davon ist die Konstruktion des Körpers $\mathbb{Q}$ aus dem Ring $\mathbb{Z}$: $\mathbb{Q}$ besteht aus „formalen Brüchen“ $\frac{a}{b}$ von ganzen Zahlen $a, b \in \mathbb{Z}$ mit $b \neq 0$, so dass alle ganzen Zahlen außer Null zu Einheiten in $\mathbb{Q}$ gemacht werden. Man kann diese Konstruktion mit einer beliebigen Integrtätsring R nachahmen, um einen Körper $Q(R)$ mit einem injektiven Ringhomomorphismus $R \hookrightarrow Q(R)$ zu erhalten. Der Körper $Q(R)$ heißt dann der *Quotientenkörper* von R (trotz des Namens ist $Q(R)$ kein Quotientenring von R im Sinne der Definition 2.1.42). Zum Beispiel ist $\mathbb{Q}(i)$ der Quotientenkörper von $\mathbb{Z}[i]$, und der Quotientenkörper des Polynomrings $K[X]$ ist der Körper $K(X)$ der sogenannten *rationalen Funktionen* über K, die Brüche zweier Polynome sind. Lokalisierung ist eine weitere Verallgemeinerung dieser Konstruktion, indem wir nicht alle Nicht-Null-Elemente sondern nur Elemente aus einer gegebenen Teilmenge $S \subset R$ zu Einheiten machen.

Definition 2.1.55 (multiplikativ abgeschlossene Teilmenge)**.** Sei R ein kommutativer Ring. Eine Teilmenge $S \subset R$ heißt *multiplikativ abgeschlossen* wenn die folgenden Bedingungen erfüllt sind:

(i) Es gilt $1 \in S$.

(ii) Für alle $s, t \in S$ gilt $st \in S$.

Beispiel 2.1.56. Sei R ein kommutativer Ring.

(i) Die Teilmenge der Einheiten $R^\times \subset R$ ist stets multiplikativ abgeschlossen.

(ii) Ist $f\colon R \to R'$ ein Ringhomomorphismus zwischen kommutativen Ringen und ist $S' \subset R'$ multiplikativ abgeschlossen, so ist $f^{-1}(S') \subset R$ wieder multiplikativ abgeschlossen. Insbesondere ist $f^{-1}(S^\times)$ eine multiplikativ abgeschlossene Teilmenge von R.

(iii) Die Teilmenge $R \setminus \{0\} \subset R$ ist genau dann multiplikativ abgeschlossen, wenn R ein Integritätsring ist.

(iv) Sei $s \in R$ ein beliebiges Element. Dann ist die Teilmenge $\{s^i \mid i \in \mathbb{N}\} \subset R$ multiplikativ abgeschlossen. Zum Beispiel bilden die Monome $\{X^i \mid i \in \mathbb{N}\}$ eine multiplikativ abgeschlossene Teilmenge von $R[X]$, und auch von $R[X, Y]$.

(v) Sei $p \in R \setminus \{0\}$. Die Teilmenge $R \setminus (p) \subset R$ der nicht durch p teilbaren Elemente von R ist genau dann multiplikativ abgeschlossen, wenn p ein *Primelement* von R ist (siehe Definition LA.8.2.6): 1 ist nicht durch p teilbar (d.h., p ist keine Einheit), und sind $s, t \in R$ nicht durch p teilbar, so ist st auch nicht durch p teilbar. Ist zum Beispiel $p \in \mathbb{N}$ eine Primzahl, so ist $\mathbb{Z} \setminus p\mathbb{Z} \subset \mathbb{Z}$ multiplikativ abgeschlossen (Primzahlen sind Primelemente von $\mathbb{Z}$ nach Proposition LA.8.2.9(ii)).

Proposition 2.1.57 (Lokalisierung)**.** *Sei R ein kommutativer Ring und $S \subset R$ eine multiplikativ abgeschlossene Teilmenge. Sei $\sim$ die folgende Relation auf der Produktmenge $R \times S$:*

$$(a, s) \sim (a', s') \quad \Longleftrightarrow \quad \text{es gibt ein } t \in S \text{ mit } t(as' - a's) = 0.$$

Dann:

(i) *$\sim$ ist eine Äquivalenzrelation auf $R \times S$. Man bezeichnet die Äquivalenzklasse von (a, s) mit dem Bruch $\frac{a}{s}$ und die Quotientenmenge $(R \times S)/\sim$ mit $S^{-1}R$:*

$$S^{-1}R := \left\{ \frac{a}{s} \;\middle|\; (a, s) \in R \times S \right\}.$$

(ii) *Die Verknüpfungen*

$$+\colon S^{-1}R \times S^{-1}R \to S^{-1}R, \qquad \left(\frac{a}{s}, \frac{b}{t}\right) \mapsto \frac{at + bs}{st},$$

$$\cdot\colon S^{-1}R \times S^{-1}R \to S^{-1}R, \qquad \left(\frac{a}{s}, \frac{b}{t}\right) \mapsto \frac{ab}{st},$$

sind wohldefiniert und das Tripel $(S^{-1}R, +, \cdot)$ ist ein kommutativer Ring.

(iii) *Die Abbildung*

$$j\colon R \to S^{-1}R, \quad a \mapsto \frac{a}{1},$$

ist ein Ringhomomorphismus, so dass $j(S) \subset (S^{-1}R)^\times$. Ist genauer $s \in S$, so ist der Bruch $\frac{1}{s} \in S^{-1}R$ das inverse Element zu $j(s)$.

Beweis. Zu (i). Die Relation $\sim$ ist reflexiv, denn $1 \in S$ und $1 \cdot (as - as) = 0$. Sie ist symmetrisch, denn aus $t(as' - a's) = 0$ folgt $t(a's - as') = -t(as' - a's) = 0$. Zur Transitivät seien $(a, s) \sim (a', s')$ und $(a', s') \sim (a'', s'')$. Es gibt dann t, t' in S mit

$$t(as' - a's) = 0 \quad \text{und} \quad t'(a's'' - a''s') = 0.$$

Multipliziert man die erste Gleichung mit $s''t'$ und die zweite mit st, so erhalten wir

$$s''t'tas = s''t'ta's \quad \text{und} \quad stt'a's'' = stt'a''s',$$

und daher $s''t'tas = stt'a''s'$, d.h., $s'tt'(as'' - a''s) = 0$. Da $s'tt' \in S$ gilt also $(a, s) \sim (a'', s'')$.

Zu (ii). Seien $(a, s) \sim (a', s')$ und $(b, t) \sim (b', t')$. Es gibt dann $u, v \in S$ mit $u(as' - a's) = 0$ und $v(bt' - b't) = 0$. Zu zeigen ist, dass

$$\frac{at + bs}{st} = \frac{a't' + b's'}{s't'} \quad \text{und} \quad \frac{ab}{st} = \frac{a'b'}{s't'}.$$

Dies folgt aus den Berechnungen:

$$\begin{aligned} uv((at + bs)s't' - (a't' + b's')st) &= u(as' - a's)vtt' + v(bt' - b't)uss' = 0, \\ uv(abs't' - a'b'st) &= uv(abs't' - a'bst' + a'bst' - a'b'st) \\ &= u(as' - a's)vbt' + v(bt' - b't)ua's = 0. \end{aligned}$$

Dass das Tripel $(S^{-1}R, +, \cdot)$ ein kommutativer Ring ist, kann man nun leicht nachrechnen. Das neutrale Element bzgl. $+$ ist $\frac{0}{1}$ und das neutrale Element bzgl. $\cdot$ ist $\frac{1}{1}$.

Zu (iii). Nach Definition der beiden Verknüpfungen gilt

$$\frac{a}{1} + \frac{a'}{1} = \frac{a + a'}{1} \quad \text{und} \quad \frac{a}{1} \cdot \frac{a'}{1} = \frac{aa'}{1}.$$

Zudem ist $j(1) = \frac{1}{1}$ das neutrale Element bzgl. $\cdot$ in $S^{-1}R$, so dass j ein Ringhomomorphismus ist. Ist $s \in S$, so gilt

$$\frac{s}{1} \cdot \frac{1}{s} = \frac{s}{s} = \frac{1}{1},$$

denn $1 \cdot (s \cdot 1 - 1 \cdot s) = 0$ und $1 \in S$. Also gilt $\frac{1}{s} = (\frac{s}{1})^{-1}$, wie behauptet. □

Bemerkung 2.1.58. Wenn die Elemente von S keine Nullteiler in R sind, z.B. wenn R ein Integritätsring ist und $S \subset R \setminus \{0\}$, dann vereinfacht sich die Äquivalenzrelation aus Proposition 2.1.57: Es gilt nämlich

$$(a, s) \sim (a', s') \quad \Longleftrightarrow \quad as' - a's = 0.$$

In diesem Fall gilt insbesondere $(a, 1) \sim (a', 1)$, nur wenn $a = a'$, so dass die Abbildung $j\colon R \to S^{-1}R$ injektiv ist. Im Allgemeinen würde aber diese vereinfachte Relation nicht transitiv sein, und j ist nicht unbedingt injektiv.

Definition 2.1.59 (Lokalisierung)**.** Sei R ein kommutativer Ring und $S \subset R$ eine multiplikativ abgeschlossene Teilmenge. Der Ring $S^{-1}R$ aus Proposition 2.1.57 heißt die *Lokalisierung* von R nach S. Man bezeichnet ihn auch mit $R[S^{-1}]$. Der Ringhomomorphismus $j\colon R \to S^{-1}R$, $r \mapsto \frac{r}{1}$, heißt der *kanonische* Ringhomomorphismus.

Bemerkung 2.1.60. Für einen Bruch $\frac{a}{s} \in S^{-1}R$ gilt

$$\frac{a}{s} = \frac{0}{1} \quad \Longleftrightarrow \quad \text{es gibt ein } t \in S \text{ mit } ta = 0.$$

Also wenn S keine Nullteiler enthält, dann ist ein Bruch $\frac{a}{s}$ genau dann null, wenn $a = 0$. Wenn aber S die Null enthält, dann ist jeder Bruch $\frac{a}{s}$ gleich Null, d.h., $S^{-1}R$ ist der Nullring.

Definition 2.1.61 (Quotientenkörper)**.** Sei R ein Integritätsring. Die Lokalisierung von R nach der multiplikativ abgeschlossenen Teilmenge $R \setminus \{0\}$ heißt der *Quotientenkörper* von R und wird mit $Q(R)$ oder $\mathrm{Quot}(R)$ bezeichnet.

Der Quotientenkörper ist eigentlich ein Körper, denn jeder Bruch $\frac{a}{b}$ mit $a, b \in R \setminus \{0\}$ hat ein multiplikatives Inverses, nämlich den Bruch $\frac{b}{a}$. Zudem ist der kanonische Ringhomomorphismus $j\colon R \to Q(R)$ injektiv (nach Bemerkung 2.1.58).

Bemerkung 2.1.62. Das Wort "Quotientenkörper" soll als "Körper der Quotienten" verstanden werden: Die Elemente von $Q(R)$ sind Quotienten von Elementen von R, aber $Q(R)$ selbst ist *kein* Quotientenring von R im Sinne der Definition 2.1.42.

Beispiel 2.1.63.

(i) Nach Konstruktion ist $\mathbb{Q}$ der Quotientenkörper von $\mathbb{Z}$.

(ii) Der Quotientkörper von $\mathbb{Z}[i]$ ist isomorph zum Körper $\mathbb{Q}(i)$ der rationalen komplexen Zahlen: $\mathbb{Q}(i) = \{a + bi \mid a, b \in \mathbb{Q}\} \subset \mathbb{C}$.

(iii) Sei K ein Körper. Der Quotientenkörper des Polynomrings $K[X]$ wird mit $K(X)$ bezeichnet: Er besteht aus Brüchen $\frac{f}{g}$ mit $f, g \in K[X]$ und $g \neq 0$. Die Elemente von $K(X)$ heißen *rationalen Funktionen* über K (die sind aber nicht wirklich Funktionen, siehe Bemerkung 2.1.32). Insbesondere ist $\mathbb{F}_p(X)$ ein unendlicher Körper der Charakteristik $p > 0$. Allgemeiner wird der Quotientenkörper von $K[X_1, \dots, X_n]$ mit $K(X_1, \dots, X_n)$ bezeichnet.

(iv) Sei R ein kommutativer Ring und sei $s \in R$. Die Lokalisierung von R nach der multiplikativ abgeschlossenen Teilmenge $\{1, s, s^2, \dots\}$ aus Beispiel 2.1.56(iv) bezeichnen wir mit $R[s^{-1}]$ oder $R[\frac{1}{s}]$. Ihre Elemente sind Brüche der Form $\frac{a}{s^i}$ mit $i \in \mathbb{N}$. Ist zum Beispiel $n \in \mathbb{N} \setminus \{0\}$, so kann man den Ring $\mathbb{Z}[\frac{1}{n}]$ mit einem Unterring von $\mathbb{Q}$ identifizieren.

Die Lokalisierung $R[X][X^{-1}] = R[X^{\pm 1}]$ ist der Ring der *Laurent-Polynome* über R, d.h., formale Summen $\sum_{i \in \mathbb{Z}} a_i X^i$ mit $a_i \in R$, wobei nur endlich viele der a_i nicht null sind.

(v) Sei p eine Primzahl, so dass die Teilmenge $\mathbb{Z} \setminus p\mathbb{Z} \subset \mathbb{Z}$ multiplikativ abgeschlossen ist (Beispiel 2.1.56(v)). Die Lokalisierung von $\mathbb{Z}$ nach $\mathbb{Z} \setminus p\mathbb{Z}$ wird mit $\mathbb{Z}_{(p)}$ bezeichnet: Sie besteht aus Brüchen $\frac{a}{b}$, wobei b nicht durch p teilbar ist. Man kann also den Ring $\mathbb{Z}_{(p)}$ mit einem Unterring von $\mathbb{Q}$ identifizieren. Dieser Ring erfüllt außerdem

$$\mathbb{Z}_{(p)}/(p) \cong \mathbb{F}_p \quad \text{und} \quad \mathbb{Z}_{(p)}[\tfrac{1}{p}] \cong \mathbb{Q}.$$

Bemerkung 2.1.64. Ist R ein *faktorieller* Ring, so kann jedes Element von $Q(R)$ als Bruch $\frac{r}{s}$ dargestellt werden, wobei r und s teilerfremd sind. Denn sind $a, b \in R$ beliebig mit $b \neq 0$ und ist $d = \mathrm{ggT}(a, b)$, so gibt es $r, s \in R$ mit $a = dr$ und $b = ds$. Dann sind r und s teilerfremd und es gilt $\frac{a}{b} = \frac{r}{s}$ in $Q(R)$.

Proposition 2.1.65. *Ein Ring R ist genau dann ein Integritätsring, wenn er ein Unterring eines Körpers ist.*

Beweis. Jeder Körper ist ein Integritätsring, und jeder Unterring eines Integritätsringes ist wieder ein Integritätsring. Ist umgekehrt R ein Integritätsring, so gibt es einen injektiven Ringhomomorphismus $R \hookrightarrow Q(R)$, und $Q(R)$ ist ein Körper (und man kann die Elemente von $Q(R)$ umbenennen, damit R wirklich ein Unterring von $Q(R)$ wird). □

Korollar 2.1.66 (Nullstellen von Polynomen in Integritätsringen)**.** *Sei R ein Integritätsring und sei $f \in R[X]$ ein Polynom vom Grad $d \geq 0$. Dann hat f höchstens d Nullstellen in R.*

Beweis. Sei K ein Körper, der R als Unterring enthält. Jede Nullstelle von f in R ist dann insbesondere eine Nullstelle von f in K. Nach Korollar LA.6.3.17 hat aber f höchstens d Nullstellen in K. □

Bemerkung 2.1.67. Korollar 2.1.66 gilt nicht in einem beliebigen kommutativen Ring. Sei zum Beispiel $R = K \times L$ mit Körpern K und L und sei $f = X^2 - 1$. Dann hat f vier verschiedene Nullstellen $(\pm 1, \pm 1)$.

Proposition 2.1.68 (universelle Eigenschaft der Lokalisierung)**.** *Sei R ein kommutativer Ring, $S \subset R$ eine multiplikativ abgeschlossene Teilmenge und $j\colon R \to S^{-1}R$ der kanonische Ringhomomorhismus. Zu jedem kommutativen Ring R' und jedem Ringhomomorphismus $f\colon R \to R'$ mit $f(S) \subset (R')^\times$ gibt es* genau einen *Ringhomomorphismus $\hat{f}\colon S^{-1}R \to R'$ mit $\hat{f} \circ j = f$.*

Beweis. Zur Eindeutigkeit. Für ein beliebiges Element $\frac{a}{s} \in S^{-1}R$ gilt

$$\hat{f}\left(\frac{a}{s}\right) = \hat{f}(j(s)^{-1}j(a)) = \hat{f}(j(s))^{-1}\hat{f}(j(a)) = f(s)^{-1}f(a),$$

so dass $\hat{f}$ eindeutig durch f bestimmt ist.

Zur Existenz. Man definiert zunächst die Abbildung

$$h\colon R \times S \to R', \quad (a, s) \mapsto f(s)^{-1}f(a).$$

Dies ist möglich, denn $f(s) \in (R')^\times$ für alle $s \in S$. Sei nun $(a, s) \sim (a', s')$, d.h., $t(as' - a's) = 0$ mit einem $t \in S$. Anwendung von f liefert

$$f(t)(f(a)f(s') - f(a')f(s)) = 0.$$

Da $f(t)$ eine Einheit in R' ist, folgt daraus, dass $f(a)f(s') = f(a')f(s)$. Multipliziert man beide Seiten mit $f(s)^{-1}f(s')^{-1}$, so erhält man $h(a, s) = h(a', s')$. Nach der universellen Eigenschaft der Quotientenmenge erhalten wir also eine Abbildung

$$\hat{f}\colon S^{-1}R \to R', \quad \frac{a}{s} \mapsto f(s)^{-1}f(a).$$

Es bleibt zu zeigen, dass $\hat{f}$ ein Ringhomomorphismus ist. Dies folgt aber unmittelbar aus den Definitionen der Verknüpfungen $+$ und $\cdot$ auf $S^{-1}R$. □

Beispiel 2.1.69 (Körper der Charakteristik 0)**.** Sei K ein Körper der Charakteristik 0 (z.B. $\mathbb{R}$ oder $\mathbb{C}$). Dann gibt es genau einen Ringhomomorphismus $\mathbb{Q} \to K$ (der nach Proposition 2.1.14 injektiv ist), denn: Nach der universellen Eigenschaft von $\mathbb{Z}$ (Proposition 2.1.19) gibt es genau einen Ringhomomorphismus $\mathbb{Z} \to K$. Nach Definition der Charakteristik wird jedes $n \in \mathbb{Z} \setminus \{0\}$ auf eine Einheit von K abgebildet. Nach der universellen Eigenschaft der Lokalisierung gibt es also genau einen Ringhomomorphismus $Q(\mathbb{Z}) = \mathbb{Q} \to K$. Siehe auch Beispiel 2.1.47.

Bemerkung 2.1.70 (universelle Eigenschaft des Quotientenkörpers)**.** Als Sonderfall der Proposition 2.1.68 erhalten wir eine universelle Eigenschaft für den Quotientenkörper. Sei R ein Integritätsring und K ein Körper. Jeder injektive Ringhomomorphismus $f\colon R \hookrightarrow K$ lässt sich dann eindeutig zu einem Körperhomomorphismus $\hat{f}\colon Q(R) \hookrightarrow K$ fortsetzen. Denn nach Injektivität gilt $f(R \setminus \{0\}) \subset K \setminus \{0\} = K^\times$.

2.2 Die Primeigenschaft

Wir erinnern zunächst an ein paar wichtige Definitionen und Resultate aus der Linearen Algebra (siehe dazu LA.8.2):

Definition 2.2.1 (teilbar, assoziiert)**.** Sei R ein kommutativer Ring und seien $x, y \in R$.

- Man sagt, dass y *durch* x *teilbar* ist oder dass x y *teilt*, und man schreibt $x|y$, wenn ein Element $t \in R$ mit $tx = y$ existiert, d.h., wenn $y \in (x)$. Man sagt dann auch, dass x ein *Teiler* von y ist und dass y ein *Vielfaches* von x ist.
- Man sagt, dass x und y *assoziiert* sind, wenn sie durcheinander teilbar sind, d.h., wenn $(x) = (y)$.

Proposition 2.2.2. *Sei R ein Integritätsring. Zwei Elemente $x, y \in R$ sind genau dann assoziiert, wenn eine Einheit $r \in R^\times$ existiert, so dass $rx = y$.*

Beweis. Siehe Proposition LA.8.2.4. □

Definition 2.2.3 (prim, irreduzibel)**.** Sei R ein kommutativer Ring und sei $x \in R$.

- x heißt *prim* oder ein *Primelement*, wenn $x \notin \{0\} \cup R^\times$ und für alle $r, s \in R$ gilt:
$$x|rs \implies (x|r \text{ oder } x|s).$$
- x heißt *irreduzibel*, wenn $x \notin \{0\} \cup R^\times$ und für alle $r, s \in R$ gilt:
$$x = rs \implies (r \in R^\times \text{ oder } s \in R^\times).$$

Proposition 2.2.4 (prim vs. irreduzibel)**.**

(i) *In einem Integritätsring ist jedes Primelement irreduzibel.*

(ii) *In einem faktoriellen Ring (z.B. in einem Hauptidealring) stimmen Primelemente und irreduzible Elemente überein.*

Beweis. Siehe Propositionen LA.8.2.9 und LA.8.2.27 □

Bemerkung 2.2.5. Die Umkehrung von Proposition 2.2.4(i) gilt im Allgemeinen nicht. Zum Beispiel: Im Integritätsring $\mathbb{Z}[\sqrt{-5}]$ kann man zeigen, dass 3 irreduzibel ist, aber 3 ist kein Primelement von $\mathbb{Z}[\sqrt{-5}]$, denn 3 teilt $9 = (2 + i\sqrt{5})(2 - i\sqrt{5})$, ohne einen der beiden Faktoren zu teilen. Insbesondere ist $\mathbb{Z}[\sqrt{-5}]$ kein faktorieller Ring.

Beispiel 2.2.6 (Assoziiertheit und Primelemente in $\mathbb{Z}$ und $K[T]$)**.**

(i) Die Einheiten vom Hauptidealring $\mathbb{Z}$ sind ± 1, so dass $\mathbb{N} \subset \mathbb{Z}$ ein Repräsentantensystem der Assoziiertheitsklassen ist (nach Proposition 2.2.2). Die Primzahlen sind nach Definition die positiven irreduziblen Elemente von $\mathbb{Z}$. Die irreduziblen Elemente von $\mathbb{Z}$ sind also $\pm$ die Primzahlen, und die sind auch genau die Primelemente von $\mathbb{Z}$ (nach Proposition 2.2.4(ii)).

(ii) Sei K ein Körper, so dass $K[T]$ ein Hauptidealring ist. Die Einheiten von $K[T]$ sind genau die Polynome vom Grad 0 (nach Proposition 2.1.24(ii)), d.h., $K[T]^\times = K^\times$. Jedes Polynom $f \neq 0$ ist damit zu genau einem monischen Polynom assoziiert, d.h., die Teilmenge
$$\{0\} \cup \{\text{monische Polynome}\} \subset K[T]$$
ist ein Repräsentantensystem der Assoziiertheitsklassen von $K[T]$. Ein Polynom f ist genau dann irreduzibel (und damit auch prim), wenn $\deg(f) \geq 1$ und wenn es sich nicht als Produkt zweier Polynome kleinsten Grades zerlegen lässt.

2.2.1 Primideale und maximale Ideale

Definition 2.2.7 (Primideal, maximales Ideal)**.** Sei R ein kommutativer Ring.

- Ein Ideal $\mathfrak{p} \subset R$ heißt *Primideal*, wenn $R \setminus \mathfrak{p}$ multiplikativ abgeschlossen ist, d.h.: Es gilt $\mathfrak{p} \neq R$ und aus $xy \in \mathfrak{p}$ folgt $x \in \mathfrak{p}$ oder $y \in \mathfrak{p}$.
- Ein Ideal $\mathfrak{m} \subset R$ heißt *maximales Ideal*, wenn $\mathfrak{m} \neq R$ und für alle Ideale $I \subsetneq R$ gilt: Ist $\mathfrak{m} \subset I$, so folgt $I = \mathfrak{m}$.

Bemerkung 2.2.8. Sei R ein kommutativer Ring.

(i) Ein Element $p \in R \setminus \{0\}$ ist genau dann ein Primelement, wenn das Hauptideal (p) ein Primideal ist. Man muss aber beachten, dass das Nullideal (0) ein Primideal sein darf, auch wenn 0 nach Definition kein Primelement ist.

(ii) Nach Definition ist ein kommutativer Ring R genau dann ein Integritätsring, wenn das Nullideal (0) ein Primideal ist.

(iii) Ein Ideal $\mathfrak{m} \subset R$ ist genau dann maximal, wenn es ein maximales Element der partiell geordneten Menge

$$(\{I \subset R \mid I \text{ Ideal in } R \text{ und } I \neq R\}, \subset)$$

ist (siehe Definition LA.1.4.15).

Beispiel 2.2.9.

(i) Ist K ein Körper, so hat K nur zwei Ideale, das Nullideal $(0) = \{0\}$ und das Einsideal $(1) = K$. Das Nullideal ist damit maximal. Es ist auch prim, da K nullteilerfrei ist. Das Einsideal ist nach Definition weder prim noch maximal. Nach Proposition 2.1.40 ist ein kommutativer Ring genau dann ein Körper, wenn sein Nullideal maximal ist.

(ii) Sei R ein Hauptidealring, der kein Körper ist. Dann sind die maximale Ideale von R genau die Hauptideale (p) mit $p \in R$ prim/irreduzibel. Denn jedes Ideal I mit $(x) \subset I$ hat die Form (y), wobei y ein Teiler von x ist. Falls x irreduzibel ist, dann muss y entweder eine Einheit oder zu x assoziiert sein, so dass $(y) = R$ oder $(y) = (x)$, und damit ist (x) maximal. Ist umgekehrt (x) maximal und ist $x = yz$, dann gilt $(x) \subset (y)$ und damit entweder $(y) = R$ oder $(y) = (x)$. Im ersten Fall ist y eine Einheit. Im zweiten Fall gibt es nach Proposition 2.2.2 eine Einheit $r \in R^\times$ mit $x = yr$. Da R ein Integritätsring ist, muss dann r gleich z sein, so dass z eine Einheit ist. Zudem ist $x \neq 0$, da R kein Körper ist. Also ist x irreduzibel.

(iii) Die Primideale in $\mathbb{Z}$ sind genau die Ideale (p) mit einer Primzahl p und das Nullideal (0). Dies folgt aus Bemerkung 2.2.8(i,ii) und der Tatsache, dass jedes Primelement in $\mathbb{Z}$ zu einer Primzahl assoziiert ist (Beispiel 2.2.6(i)).

Proposition 2.2.10 (Restklassenringe zu Primidealen/maximalen Idealen)**.** *Sei R ein kommutativer Ring und $I \subset R$ ein Ideal.*

(i) *I ist genau dann prim, wenn R/I ein Integritätsring ist.*

(ii) *I ist genau dann maximal, wenn R/I ein Körper ist.*

Beweis. Zu (i). Es gilt $1 \in I$ genau dann, wenn $1 \neq 0$ im Restklassenring R/I gilt. Seien $x, y \in R$. Dann gilt

$$xy \in I \quad \Longleftrightarrow \quad [x][y] = 0 \text{ in } R/I$$

und

$$x \in I \text{ oder } y \in I \quad \Longleftrightarrow \quad [x] = 0 \text{ oder } [y] = 0 \text{ in } R/I.$$

Daraus folgern wir die gewünschte Äquivalenz.

Zu (ii). Dies folgt aus der Kombination der Propositionen 2.1.49 und 2.1.40:

$$\begin{aligned} I \text{ ist maximal} &\iff \text{es gibt genau zwei Ideale } J \text{ in } R \text{ mit } I \subset J \\ &\iff \text{es gibt genau zwei Ideale in } R/I \\ &\iff R/I \text{ ist ein Körper.} \end{aligned}$$

□

Korollar 2.2.11 (maximale Ideale sind prim)**.** *Sei R ein kommutativer Ring und $\mathfrak{m}$ ein maximales Ideal in R. Dann ist $\mathfrak{m}$ ein Primideal.*

Beweis. Dies folgt aus Proposition 2.2.10, da jeder Körper ein Integritätsring ist. □

Beispiel 2.2.12 (der Körper $\mathbb{F}_p$)**.** Sei n eine natürliche Zahl. Nach Beispiel 2.2.9(ii) ist das Ideal $(n) \subset \mathbb{Z}$ genau dann maximal, wenn n eine Primzahl ist. Proposition 2.2.10(ii) impliziert dann die bekannte Aussage, dass $\mathbb{Z}/n\mathbb{Z}$ genau dann ein Körper ist, wenn n eine Primzahl ist.

Beispiel 2.2.13 (Endliche Körpererweiterungen aus irreduziblen Polynomen)**.** Sei K ein Körper und sei $f \in K[T]$. Nach Beispiel 2.2.9(ii) ist das Ideal $(f) \subset K[T]$ genau dann maximal, wenn f irreduzibel ist. Nach Proposition 2.2.10 ist also der Ring $K[T]/(f)$ genau dann ein Körper, wenn f irreduzibel ist. In diesem Fall gibt es außerdem einen kanonischen Körperhomomorphismus

$$K \hookrightarrow K[T] \twoheadrightarrow K[T]/(f),$$

der nach Proposition 2.1.14 automatisch injektiv ist. Man kann also K mit einem Teilkörper von $K[T]/(f)$ identifizieren, oder umgekehrt $K[T]/(f)$ als Körpererweiterung von K auffassen. Nach Lemma LA.9.2.5 ist zudem $K[T]/(f)$ ein endlich-dimensionaler K-Vektorraum: Seine Dimension ist genau der Grad d von f und die Familie $([1], [T], \ldots, [T^{d-1}])$ ist eine Basis.

Definition 2.2.14 (Restklassenkörper)**.** Sei R ein kommutativer Ring und $\mathfrak{p} \subset R$ ein Primideal. Der *Restklassenkörper* $\kappa(\mathfrak{p})$ von R bzgl. $\mathfrak{p}$ ist der Quotientenkörper des Integritätsringes $R/\mathfrak{p}$:

$$\kappa(\mathfrak{p}) = Q(R/\mathfrak{p}).$$

Bemerkung 2.2.15.

(i) Ist $\mathfrak{m} \subset R$ ein maximales Ideal, so ist der Restklassenring $R/\mathfrak{m}$ bereits ein Körper, so dass $\kappa(\mathfrak{m}) \cong R/\mathfrak{m}$.

(ii) Sei R ein Integritätsring, so dass (0) ein Primideal ist. Der Quotientenkörper $Q(R)$ ist dann nach Definition gleich dem Restklassenkörper $\kappa(0)$.

Beispiel 2.2.16 (Restklassenkörper von $\mathbb{Z}$)**.** Die Primideale in $\mathbb{Z}$ sind (0) und die maximalen Ideale (p), wobei p eine Primzahl ist. Die entsprechenden Restklassenkörper sind $\mathbb{Q}$ und die endlichen Körper $\mathbb{F}_p$.

Proposition 2.2.17 (Existenz maximaler Ideale)**.** *Sei R ein kommutativer Ring. Jedes Ideal $I \subsetneq R$ ist in einem maximalen Ideal enthalten. Insbesondere besitzt jeder kommutative Ring $R \neq \{0\}$ mindestens ein maximales Ideal.*

Beweis. Der Beweis ist eine Anwendung des Zornschen Lemmas (Satz LA.1.4.22). Wir betrachten nämlich die partiell geordnete Menge $(\mathfrak{X}, \subset)$, wobei

$$\mathfrak{X} = \{J \subset R \mid J \text{ ist ein Ideal in } R \text{ mit } I \subset J \subsetneq R\}.$$

Sei $\mathcal{K} \subset \mathfrak{X}$ eine Kette, d.h., eine solche Teilmenge, dass $(\mathcal{K}, \subset)$ total geordnet ist. Falls $\mathcal{K}$ leer ist, dann ist $I \in \mathfrak{X}$ eine obere Schranke von $\mathcal{K}$. Sonst ist die Vereinigung $J_\infty = \bigcup_{J \in \mathcal{K}} J$ wieder ein Ideal in R, denn: Sind $x, y \in J_\infty$, so gibt es $J_x, J_y \in \mathcal{K}$ mit $x \in J_x$ und $y \in J_y$. Da

$\mathcal{K}$ total geordnet ist, gilt $J_x \subset J_y$ oder $J_y \subset J_x$. Es gibt also ein $J \in \mathcal{K}$ mit $x, y \in J$. Dann sind 0, $-x$, $x+y$ und rx für alle $r \in R$ wieder Elemente von J und damit von J_∞. Zudem ist $J_\infty \neq R$, da $1 \notin J$ für alle $J \in \mathcal{K}$. Also ist J_∞ wieder ein Element von $\mathfrak{X}$ und damit eine obere Schranke der Kette $\mathcal{K}$. Das Zornsche Lemma sagt nun, dass $\mathfrak{X}$ ein maximales Element $\mathfrak{m}$ besitzt. Nach Definition ist dann $\mathfrak{m}$ ein maximales Ideal, das I enthält. □

2.2.2 Der Satz von Gauß

In diesem Abschnitt beweisen wir den *Satz von Gauß*: Ist R ein faktorieller Ring, so ist $R[X]$ wieder faktoriell. Wir erinnern zunächst an die Definition von faktoriellen Ringen und zusammenhängenden Begriffen (siehe auch LA.8.2.3).

Definition 2.2.18 (Primfaktorzerlegung, faktorieller Ring)**.**

- Sei R ein kommutativer Ring. Eine *Primfaktorzerlegung* eines Elements $r \in R \setminus \{0\}$ ist eine Darstellung
$$r = up_1 \dots p_n,$$
wobei $u \in R^\times$, $n \in \mathbb{N}$ und $p_1, \dots, p_n \in R$ Primelemente sind.
- Ein *faktorieller Ring* oder *ZPE-Ring* (für „Zerlegung in Primelemente“) ist ein Integritätsring, in dem jedes Nicht-Null-Element eine Primfaktorzerlegung besitzt.

Proposition 2.2.19 (Eindeutigkeit der Primfaktozerlegung)**.** *Sei R ein Integritätsring und sei $r \in R \setminus \{0\}$. Wenn r eine Primfaktorzerlegung besitzt, dann ist sie* im Wesentlichen eindeutig *im folgenden Sinne: Ist*

$$r = up_1 \dots p_n = vq_1 \dots q_m$$

mit Einheiten u, v und Primelementen p_i, q_j, so gibt es eine Bijektion $\sigma\colon \{1, \dots, n\} \to \{1, \dots, m\}$, so dass p_i und $q_{\sigma(i)}$ assoziiert sind für alle $i \in \{1, \dots, n\}$.

Beweis. Siehe Proposition LA.8.2.22. □

Proposition 2.2.20. *Jeder Hauptidealring ist faktoriell.*

Beweis. Siehe Proposition LA.8.2.24. □

Definition 2.2.21 (Vielfachheit)**.** Sei R ein faktorieller Ring, sei $r \in R$ und sei $p \in R$ ein Primelement. Die *Vielfachheit* von p in r ist

$$v_p(r) = \sup\{n \in \mathbb{N} \mid p^n \text{ teilt } r\} \in \mathbb{N} \cup \{+\infty\}.$$

(Sie kann nur $+\infty$ sein, wenn $r = 0$.) Man beachte dabei, dass $v_p(r)$ nur von der Assoziiertheitsklasse von p abhängt.

Jedes $r \in R \setminus \{0\}$ lässt sich dann als

$$r = u \cdot \prod_{p \in P} p^{v_p(r)}$$

darstellen, wobei $u \in R^\times$ und $P \subset R$ ein Repräsentantensystem der Assoziiertheitsklassen der Primelemente von R ist.

Proposition 2.2.22 (Teilbarkeitskriterium)**.** *Sei R ein faktorieller Ring und seien $r, s \in R$. Dann sind die folgenden Aussagen äquivalent:*

(i) *r teilt s.*

(ii) *Für alle Primelemente $p \in R$ gilt $v_p(r) \leq v_p(s)$.*

Beweis. Siehe Proposition LA.8.2.32. □

Um den Satz von Gauß zu beweisen, betrachten wir den Quotientenkörper $Q(R)$ des faktoriellen Ringes R. Die kanonische Einbettung $R \hookrightarrow Q(R)$ induziert eine Einbettung $R[X] \hookrightarrow Q(R)[X]$. Der Polynomring $Q(R)[X]$ ist ein Hauptidealring und damit faktoriell nach Proposition 2.2.20. Jedes $f \in R[X]$ besitzt also eine Primfaktorzerlegung in $Q(R)[X]$, und man möchte zeigen, dass man daraus eine Primfaktorzerlegung von f in $R[X]$ erhalten kann.

Als erster Schritt setzen wir die Abbildungen v_p aus Definition 2.2.21 auf dem Quotientenkörper und seinem Polynomring fort:

Definition 2.2.23 (Primbewertung)**.** Sei R ein faktorieller Ring und sei $p \in R$ ein Primelement.

- Ist $x = \frac{a}{b} \in Q(R)$ mit $a, b \in R$, $b \neq 0$, so definiert man

  $$v_p(x) = v_p(a) - v_p(b) \in \mathbb{Z} \cup \{+\infty\}.$$

  Dies ist woldefiniert, denn: Ist $\frac{a}{b} = \frac{c}{d}$, so gilt $ad = bc$ und damit $v_p(a) + v_p(d) = v_p(b) + v_p(c)$. Die so definierte Abbildung

  $$v_p \colon Q(R) \to \mathbb{Z} \cup \{+\infty\}$$

  heißt die *p-Bewertung* auf dem Körper $Q(R)$.

- Sei $f = \sum_{i \in \mathbb{N}} a_i X^i$ ein Polynom über $Q(R)$. Man definiert

  $$v_p(f) = \min\{v_p(a_i) \mid i \in \mathbb{N}\} \in \mathbb{Z} \cup \{+\infty\}.$$

Bemerkung 2.2.24. Sei R ein faktorieller Ring und $x \in Q(R)$. Aus dem Teilberkeitskriterium 2.2.22 folgt:

$$x \in R \quad \Longleftrightarrow \quad \text{für alle Primelemente } p \in R \text{ gilt } v_p(x) \geq 0.$$

Ist allgemeiner $f \in Q(R)[X]$, so gilt:

$$f \in R[X] \quad \Longleftrightarrow \quad \text{für alle Primelemente } p \in R \text{ gilt } v_p(f) \geq 0.$$

Bemerkung 2.2.25 (Bewertung)**.** Sei K ein Körper. Eine *Bewertung* auf K ist eine Abbildung $v \colon K \to \Gamma \cup \{+\infty\}$, wobei $(\Gamma, \leq)$ eine angeordnete abelsche Gruppe ist, mit folgenden Eigenschaften:

(i) Es gilt $v(x) = +\infty$ genau dann, wenn $x = 0$.

(ii) Für alle $x, y \in K$ gilt $v(xy) = v(x) + v(y)$.

(iii) Für alle $x, y \in K$ gilt $v(x + y) \geq \min\{v(x), v(y)\}$.

Im Fall $\Gamma = \mathbb{Z}$ spricht man von einer *diskreten Bewertung*. Die p-Bewertung auf $Q(R)$ aus Definition 2.2.23 ist eine diskrete Bewertung, wie man leicht nachrechnen kann.

Lemma 2.2.26. *Sei R ein kommutativer Ring und sei $\mathfrak{p} \subset R$ ein Primideal. Dann ist*

$$\mathfrak{p}[X] := \{f \in R[X] \mid \textit{alle Koeffizienten von } f \textit{ liegen in } \mathfrak{p}\}$$

ein Primideal im Polynomring $R[X]$.

Beweis. Die Quotientenabbildung $q\colon R \twoheadrightarrow R/\mathfrak{p}$ induziert einen surjektiven Ringhomomorphismus

$$\hat{q}\colon R[X] \twoheadrightarrow (R/\mathfrak{p})[X],$$

deren Kern genau $\mathfrak{p}[X]$ ist. Nach dem Homomorphiesatz 2.1.51 gibt es einen induzierten Isomorphismus $R[X]/\mathfrak{p}[X] \xrightarrow{\sim} (R/\mathfrak{p})[X]$. Nach Proposition 2.2.10(i) bleibt es zu zeigen, dass $(R/\mathfrak{p})[X]$ ein Integritätsring ist. Nach derselben Proposition ist aber $R/\mathfrak{p}$ ein Integritätsring, und nach Korollar 2.1.26 ist $(R/\mathfrak{p})[X]$ wieder ein Integritätsring. □

Proposition 2.2.27 (Lemma von Gauß)**.** *Sei R ein faktorieller Ring und sei $p \in R$ ein Primelement. Für alle $f, g \in Q(R)[X]$ gilt*

$$v_p(fg) = v_p(f) + v_p(g).$$

Beweis. Wir betrachten zunächst den Sonderfall $\deg f \leq 0$, das heißt, $f = a \in Q(R)$. Ist $g = \sum_{i\in\mathbb{N}} b_i X^i$, so gilt:

$$\begin{aligned} v_p(ag) &= \min\{v_p(ab_i) \mid i \in \mathbb{N}\} \\ &= \min\{v_p(a) + v_p(b_i) \mid i \in \mathbb{N}\} \\ &= v_p(a) + \min\{v_p(b_i) \mid i \in \mathbb{N}\} \\ &= v_p(a) + v_p(g). \end{aligned}$$

Um den allgemeinen Fall zu behandeln, brauchen wir die folgende Behauptung:

Behauptung. Sind $f, g \in R[X]$ mit $v_p(f) = v_p(g) = 0$, so gilt $v_p(fg) = 0$.

Die Teilmenge $\{f \in R[X] \mid v_p(f) \neq 0\}$ ist genau das Ideal $(p)[X]$ in $R[X]$, das nach Lemma 2.2.26 ein Primideal ist. Sein Komplement ist dann nach Definition multiplikativ abgeschlossen, was die Behauptung liefert.

Seien nun $f, g \in Q(R)[X] \setminus \{0\}$ beliebig. Man kann dann $c, d \in Q(R)^\times$ finden, so dass $cf, dg \in R[X]$ und $v_p(cf) = v_p(dg) = 0$ (man kann zum Beispiel mit dem Produkt aller Nenner multiplizieren, und danach durch die maximale Potenz von p dividieren). Nach der Behauptung gilt dann $v_p(cf \cdot dg) = 0$. Nach dem Sonderfall gilt aber $v_p(cf) = v_p(c) + v_p(f)$, $v_p(dg) = v_p(d) + v_p(g)$ und $v_p(cf \cdot dg) = v_p(cd) + v_p(fg)$. Insgesamt erhalten wir

$$v_p(fg) = -v_p(cd) = -v_p(c) - v_p(d) = v_p(f) + v_p(g).$$ □

Korollar 2.2.28. *Sei R ein faktorieller Ring und seien $f, g \in Q(R)[X]$ monische Polynome. Ist $fg \in R[X]$, so sind bereits $f, g \in R[X]$.*

Beweis. Sei $p \in R$ ein beliebiges Primelement. Aus $v_p(1) = 0$ folgt $v_p(f) \leq 0$ und $v_p(g) \leq 0$. Auf der anderen Seite gilt $v_p(fg) \geq 0$, da $fg \in R[X]$. Nach dem Lemma von Gauß ist das nur möglich, wenn $v_p(f) = v_p(g) = 0$. Nach Bemerkung 2.2.24 gilt insbesondere $f, g \in R[X]$. □

Definition 2.2.29 (primitives Polynom)**.** Sei R ein faktorieller Ring. Ein Polynom $f \in R[X]$ heißt *primitiv*, wenn für alle Primelemente $p \in R$ gilt $v_p(f) = 0$.

Beispiel 2.2.30.

(i) Monische Polynome sind primitiv, denn $v_p(1) = 0$.

(ii) Das Polynom

$$6X^2 + 15X + 10 \in \mathbb{Z}[X]$$

ist primitiv, denn $v_2(15) = 0$, $v_3(10) = 0$ und $v_p(6) = 0$ für alle anderen Primzahlen p.

(iii) Nach dem Lemma von Gauß ist das Produkt zweier primitiven Polynome wieder primitiv. Zum Beispiel ist

$$(6X^2 + 15X + 10)(2X + 3) = 12X^3 + 48X^2 + 65X + 30$$

primitiv in $\mathbb{Z}[X]$. Man beachte dabei, dass in einem solchen Produkt neue Primfaktoren in den Koeffizienten auftauchen können: 65 ist durch 13 teilbar.

Bemerkung 2.2.31. Sei R ein faktorieller Ring. Jedes Polynom $f \in Q(R)[X] \setminus \{0\}$ lässt sich dann als $f = u\bar{f}$ zerlegen, wobei $u \in Q(R)^\times$ und $\bar{f} \in R[X]$ primitiv ist. Man setzt nämlich

$$u = \prod_{p \in P} p^{v_p(f)} \quad \text{und} \quad \bar{f} = u^{-1} f,$$

wobei $P \subset R$ ein Repräsentantensystem der Assoziiertheitsklassen der Primelemente ist. Das Element $u \in Q(R)^\times$ ist bis auf Multiplikation mit einer Einheit von R eindeutig durch f bestimmt und heißt der *Inhalt* von f. Ist $f \in R[X] \setminus \{0\}$, so gilt $v_p(f) \geq 0$ für alle $p \in P$, und damit ist $u \in R$.

Wir können jetzt den Satz von Gauß genauer formulieren:

Satz 2.2.32 (Satz von Gauß)**.** *Sei R ein faktorieller Ring. Dann ist der Polynomring $R[X]$ faktoriell, und die Primelemente von $R[X]$ sind genau:*

(i) *die Primelemente von R, und*

(ii) *die primitiven Polynome, die irreduzibel in $Q(R)[X]$ sind.*

Beweis. Nach Lemma 2.2.26 ist jedes Primelement $p \in R$ auch ein Primelement von $R[X]$. Als nächstes zeigen wir, dass jedes primitive Polynom $f \in R[X]$, das in $Q(R)[X]$ irreduzibel ist, ein Primelement von $R[X]$ ist. Da f in $Q(R)[X]$ irreduzibel ist, gilt $\deg f \geq 1$. Insbesondere ist f weder null noch eine Einheit in $R[X]$. Seien $g, h \in R[X]$ mit $f | gh$. Da f ein Primelement in $Q(R)[X]$ ist (nach Proposition 2.2.4), gilt $f|g$ oder $f|h$ in $Q(R)[X]$. Ohne Einschränkung gilt der erste Fall, d.h., es gibt ein $k \in Q(R)[X]$ mit $fk = g$. Nach dem Lemma von Gauß gilt dann

$$v_p(k) = v_p(g) - v_p(f) = v_p(g) \geq 0,$$

da f primitiv ist. Also ist $k \in R[X]$ und damit ist g durch f in $R[X]$ teilbar.

Es bleibt zu zeigen, dass jedes $f \in R[X] \setminus \{0\}$ ein Produkt von Elementen der Form (i) oder (ii) ist. Da $Q(R)[X]$ ein faktorieller Ring ist, kann man schreiben

$$f = u f_1 \dots f_n,$$

wobei $u \in Q(R)[X]^\times = Q(R)^\times$ und $f_1, \dots, f_n$ Primelemente von $Q(R)[X]$ sind. Jedes f_i lässt sich weiter als $f_i = u_i \bar{f}_i$ schreiben, wobei $u_i \in Q(R)^\times$ und $\bar{f}_i \in R[X]$ primitiv ist (Bemerkung 2.2.31). Da f_i und $\bar{f}_i$ assoziiert sind, ist $\bar{f}_i$ auch ein Primelement von $Q(R)[X]$. In der obigen Primfaktorzerlegung von f kann man also annehmen, dass jedes f_i ein Polynom der Form (ii) ist. Für die Einheit $u \in Q(R)^\times$ gilt dann

$$v_p(u) = v_p(f) - v_p(f_1 \dots f_n) = v_p(f) - (v_p(f_1) + \dots + v_p(f_n)) = v_p(f) \geq 0$$

nach dem Lemma von Gauß, und somit $u \in R$. Da R faktoriell ist, ist nun u ein Produkt von Elementen der Form (i). □

2.2.3 Irreduzibilitätskriterien

Irreduzible Polynome über einem Körper K ermöglichen, Körpererweiterungen von K zu konstruieren (siehe Beispiel 2.2.13). Im Allgemeinen ist es aber schwierig zu bestimmen, ob ein gegebenes Polynom irreduzibel ist.

In diesem Abschnitt beweisen wir einige Irreduzibilitätskriterien für Polynome über einem Körper. Das einfachste solche Kriterium ist die bekannte Aussage, dass Polynome vom Grad 2 oder 3 genau dann irreduzibel sind, wenn sie keine Nullstellen haben: Dies folgt aus Proposition 2.1.34 und Eigenschaften des Grades (siehe Beispiel LA.8.2.10(ii)). Dieses Kriterium ist aber nur von begrenztem Wert: Es sagt nichts über Polynome vom Grad ≥ 4 und es ist auch nicht einfach zu entscheiden, ob ein Polynom Nullstellen hat oder nicht.

Die folgenden drei Kriterien kann man in der folgenden typischen Situation anwenden: f ist ein Polynom mit Koeffizienten in einem faktoriellen Ring R, und wir wollen bestimmen, ob f über dem Quotientenkörper $Q(R)$ irreduzibel ist (nach dem Satz von Gauß ist dann f auch in $R[X]$ irreduzibel, sofern es primitiv ist). Ein wichtiger Sonderfall ist $R = \mathbb{Z}$ und $Q(R) = \mathbb{Q}$.

Proposition 2.2.33 (Nullstellenkriterium)**.** *Sei R ein faktorieller Ring mit Quotientenkörper K und sei $f \neq 0$ ein Polynom über R. Ist $\frac{r}{s} \in K$ eine Nullstelle von f in K, wobei $r, s \in R$ teilerfremd sind, so muss r das Absolutglied von f und s den Leitkoeffizient von f teilen. Ist insbesondere f monisch, so sind alle Nullstellen von f in K bereits in R.*

Beweis. Sei $a \in K$ eine Nullstelle von f. Nach Proposition 2.1.34 gibt es ein Polynom $g \in K[X]$ mit $f = (X - a)g$. Sei $a = \frac{r}{s}$ mit $r, s \in R$ teilerfremd und sei $\bar{g} = s^{-1}g$. Dann haben wir die Zerlegung $f = (sX - r)\bar{g}$ in $K[X]$. Da r und s teilerfremd sind, ist $sX - r$ primitiv. Nach dem Lemma von Gauß gilt also

$$v_p(\bar{g}) = v_p(f) - v_p(sX - r) = v_p(f) \geq 0$$

für alle Primelemente $p \in R$, so dass $\bar{g} \in R[X]$. Aus der Zerlegung $f = (sX - r)\bar{g}$ in $R[X]$ folgt nun unmittelbar, dass das Absolutglied von f durch r teilbar ist, und dass der Leitkoeffizient von f durch s teilbar ist. □

Beispiel 2.2.34. Sei R ein faktorieller Ring mit nur endlich vielen Einheiten (z.B., $\mathbb{Z}$, $\mathbb{Z}[i]$ oder $\mathbb{F}_p[T]$). Ist $f \in R[X] \setminus \{0\}$, so gibt es nur endlich viele Brüche $\frac{r}{s}$ wie in der Proposition 2.2.33. Man kann also alle solche Brüche in f einsetzen und dadurch bestimmen, ob f Nullstellen in K besitzt. Wenn $\deg(f) \in \{2, 3\}$ kann man insbesondere entscheiden, ob f irreduzibel ist oder nicht. Zum Beispiel:

(i) Sei $f = X^3 + 4X - 2 \in \mathbb{Z}[X]$. Die einzigen möglichen Nullstellen von f in $\mathbb{Q}$ sind dann $\frac{r}{s}$ mit $r \in \{\pm 1, \pm 2\}$ und $s \in \{\pm 1\}$, d.h., ± 1 oder ± 2. Es gilt aber $f(1) = 3$, $f(-1) = -7$, $f(2) = 14$ und $f(-2) = -18$. Damit ist f irreduzibel in $\mathbb{Q}[X]$. Da f primitiv ist, ist es auch in $\mathbb{Z}[X]$ irreduzibel (nach Satz 2.2.32).

(ii) Sei $f = 3X^3 - 5X^2 - 1 \in \mathbb{Z}[X]$. Die einzigen möglichen Nullstellen von f in $\mathbb{Q}$ sind dann $\frac{r}{s}$ mit $r \in \{\pm 1\}$ und $s \in \{\pm 1, \pm 3\}$, d.h., ± 1 oder $\pm\frac{1}{3}$. Man sieht aber leicht, dass sie keine Nullstellen sind, so dass f irreduzibel in $\mathbb{Q}[X]$ ist. Da f primitiv ist, ist es auch in $\mathbb{Z}[X]$ irreduzibel.

(iii) Sei $f = X^5 - 3X^3 - 2X^2 + 3X - 6 \in \mathbb{Z}[X]$. Die Nullstellen von f in $\mathbb{Q}$ können nur ± 1, ± 2, ± 3 oder ± 6 sein. Es gilt $f(2) = 0$, so dass f in $\mathbb{Q}[X]$ und in $\mathbb{Z}[X]$ nicht irreduzibel ist.

(iv) Sei $f = TX^2 + X + T^2 \in \mathbb{F}_2[T][X]$. Die einzigen möglichen Nullstellen von f in $\mathbb{F}_2(T)$ sind dann $\frac{r}{s}$ mit $r \in \{1, T, T^2\}$ und $s \in \{1, T\}$, d.h., 1, T, T^2, und $\frac{1}{T}$. Es gilt aber $f(1) = T^2 + T + 1$, $f(T) = T^3 + T^2 + T$, $f(T^2) = T^5$ und $f(\frac{1}{T}) = \frac{T^5+T^2+1}{T^3}$. Damit ist f irreduzibel in $\mathbb{F}_2(T)[X]$. Da f primitiv ist, ist es auch in $\mathbb{F}_2[T][X] = \mathbb{F}_2[T, X]$ irreduzibel.

Proposition 2.2.35 (Reduktionskriterium)**.** *Sei R ein faktorieller Ring mit Quotientenkörper K und sei $f \in R[X]$ vom Grad ≥ 1. Sei $\mathfrak{p} \subset R$ ein Primideal mit folgenden Eigenschaften:*

(i) *Der Leitkoeffizient von f ist kein Element von $\mathfrak{p}$.*

(ii) *Das Bild von f in $\kappa(\mathfrak{p})[X]$ ist irreduzibel.*

Dann ist f in $K[X]$ irreduzibel.

Beweis. Sei $f = gh$ mit Polynomen $g, h \in K[X]$ vom Grad ≥ 1. Schreibt man $g = u\bar{g}$ und $h = v\bar{h}$ mit $u, v \in K^\times$ und $\bar{g}, \bar{h} \in R[X]$ primitiv, so gilt $uv \in R$ und damit erhalten wir eine Zerlegung $f = (uv\bar{g})\bar{h}$ in $R[X]$. Ohne Einschränkung kann man also annehmen, dass g, h Polynome über R sind. Sei $q\colon R[X] \twoheadrightarrow (R/\mathfrak{p})[X]$ die kanonische Abbildung. Nach (ii) ist $q(f)$ in $\kappa(\mathfrak{p})[X]$ irreduzibel. Da $q(f) = q(g)q(h)$ muss $q(g)$ oder $q(h)$ vom Grad 0 sein. Insbesondere liegt der Leitkoeffizient von g oder h, und somit der von f, im Ideal $\mathfrak{p}$, im Widerspruch zu (i). □

Beispiel 2.2.36.

(i) Sei $f = X^3 + bX + c \in \mathbb{Z}[X]$. Sind b und c ungerade, so ist f irreduzibel in $\mathbb{Q}[X]$ (und damit in $\mathbb{Z}[X]$, da f primitiv ist). Denn Reduktion modulo 2 liefert das Polynom $X^3 + X + 1$ in $\mathbb{F}_2[X]$, das keine Nullstellen hat und damit irreduzibel ist.

(ii) Sei $f = X^2+20X-12 \in \mathbb{Z}[X]$. Reduktion modulo 5 liefert das Polynom $X^2-2 \in \mathbb{F}_5[X]$, das keine Nullstellen hat und damit irreduzibel ist. Also ist f irreduzibel in $\mathbb{Q}[X]$ und in $\mathbb{Z}[X]$.

(iii) Sei $f = X^6Y^2 + Y^2 - X^2 + 1 \in \mathbb{R}[X, Y]$. Wir betrachten f als Polynom vom Grad 2 in der Variablen Y über dem Ring $\mathbb{R}[X]$:

$$f = (X^6 + 1)Y^2 + (-X^2 + 1) \in \mathbb{R}[X][Y].$$

Das Element $X \in \mathbb{R}[X]$ ist prim, und Reduktion modulo X liefert das Polynom $Y^2+1 \in (\mathbb{R}[X]/(X))[Y] \cong \mathbb{R}[Y]$, das irreduzibel ist. Zudem ist der Leitkoeffizient $X^6 + 1$ nicht durch X teilbar. Damit ist f irreduzibel in $\mathbb{R}(X)[Y]$. Das Polynom f ist auch primitiv über $\mathbb{R}[X]$, da die Primfaktoren $X \pm 1$ von $-X^2 + 1$ keine Faktoren von $X^6 + 1$ sind. Also ist f auch in $\mathbb{R}[X, Y]$ irreduzibel.

(iv) Sei $f = 3X+4X^2+XY-2 \in \mathbb{Z}[X, Y]$. Wir betrachten f als Polynom vom Grad 2 in der Variablen X über dem faktoriellen Ring $\mathbb{Z}[Y]$ mit Quotientenkörper $\mathbb{Q}(Y)$. Das Ideal $(3, Y) \subset \mathbb{Z}[Y]$ ist prim (sogar maximal, da $\mathbb{Z}[Y]/(3, Y) \cong \mathbb{F}_3$), und durch Reduktion modulo $(3, Y)$ erhalten wir das Polynom $X^2+1 \in \mathbb{F}_3[X]$, das keine Nullstellen hat und damit irreduzibel ist. Da der Leitkoeffizient 4 nicht in $(3, Y)$ liegt, ist f in $\mathbb{Q}(Y)[X]$ irreduzibel. Da der Koeffizient $Y+3$ von X nicht durch 2 teilbar ist, ist f auch primitiv über $\mathbb{Z}[Y]$, so dass f in $\mathbb{Z}[X, Y]$ irreduzibel ist.

Proposition 2.2.37 (Eisensteinsches Kriterium)**.** *Sei R ein faktorieller Ring mit Quotientenkörper K und sei $f \in R[X]$ vom Grad ≥ 1. Sei $\mathfrak{p} \subset R$ ein Primideal mit folgenden Eigenschaften:*

(i) *Der Leitkoeffizient von f ist kein Element von $\mathfrak{p}$.*

(ii) *Alle Koeffizienten von f außer dem Leitkoeffizient liegen in $\mathfrak{p}$.*

(iii) *Das Absolutglied von f ist kein Produkt zweier Elemente von $\mathfrak{p}$.*

Dann ist f in $K[X]$ irreduzibel.

Beweis. Sei $f = gh$ mit Polynomen $g, h \in K[X]$ vom Grad ≥ 1. Wie im Beweis des Reduktionskriteriums kann man annehmen, dass g, h Polynome über R sind. Sei $q\colon R[X] \twoheadrightarrow (R/\mathfrak{p})[X]$ die kanonische Abbildung, sei $d = \deg(f)$ und sei $a_d \in R$ der Leitkoeffizient von f. Dann gilt $q(f) = [a_d]X^d = q(g)q(h)$ mit $[a_d] \neq 0$ nach (i) und (ii). Nach Eindeutigkeit der Primfaktorzerlegung im faktoriellen Ring $\kappa(\mathfrak{p})[X]$ sind dann $q(g)$ und $q(h)$ Monome vom Grad ≥ 1. Insbesondere liegen die Absolutglieder von beiden g und h im Ideal $\mathfrak{p}$. Somit ist das Absolutglied von f das Produkt zweier Elemente von $\mathfrak{p}$, im Widerspruch zu (iii). □

Beispiel 2.2.38.

(i) Sei p eine Primzahl und $n \geq 1$. Dann ist das Polynom $X^n - p$ irreduzibel in $\mathbb{Q}[X]$. Dies folgt aus dem Eisensteinschen Kriterium mit dem Primideal (p).

(ii) Das Polynom $2X^{74}+3X^{41}-9X^7-12$ ist irreduzibel in $\mathbb{Q}[X]$ und in $\mathbb{Z}[X]$: Man wendet das Eisensteinsche Kriterium mit dem Primideal (3) an: 3 teilt jeden Koeffizient außer dem Leitkoeffizient, und 3^2 teilt nicht das Absolutglied.

(iii) Sei $f = 3Y^4+X^2Y^2+X^2+4 \in \mathbb{Z}[X,Y]$. Wie betrachten f als Polynom vom Grad 4 in der Variablen Y über $\mathbb{Z}[X]$. Sei $\mathfrak{p} = (2,X) \subset \mathbb{Z}[X]$. Es gilt $3 \notin \mathfrak{p}$ und $X^2, X^2+4 \in \mathfrak{p}$. Zudem ist das Polynom $X^2+4 \in \mathbb{Z}[X]$ irreduzibel und damit kein Produkt zweier Elemente von $\mathfrak{p}$. Nach dem Eisensteinschen Kriterium ist f irreduzibel in $\mathbb{Q}(X)[Y]$. Es ist auch primitiv, da X^2 nicht durch 3 teilbar ist, und somit auch in $\mathbb{Z}[X,Y]$ irreduzibel.

Definition 2.2.39 (Kreisteilungspolynome)**.** Sei $n \in \mathbb{N}_{\geq 1}$ und sei $\zeta_n = e^{2\pi i/n} \in \mathbb{C}$. Das Element ζ_n ist eine n-te Wurzel von 1 und ist insbesondere algebraisch über $\mathbb{Q}$. Das *n-te Kreisteilungspolynom* $\Phi_n \in \mathbb{Q}[X]$ ist das Minimalpolynom von ζ_n über $\mathbb{Q}$ (Definition LA.9.1.6), d.h., das einzige monische Polynom, so dass

$$(\Phi_n) = \{f \in \mathbb{Q}[X] \mid f(\zeta_n) = 0\} \subset \mathbb{Q}[X].$$

Nach Korollar 2.2.28 gilt $\Phi_n \in \mathbb{Z}[X]$, da Φ_n das monische Polynom $X^n - 1 \in \mathbb{Z}[X]$ teilt.

Bemerkung 2.2.40.

(i) Ist $n \geq 2$, so ist $\zeta_n \neq 1$ und damit ist Φ_n ein Teiler von

$$\frac{X^n-1}{X-1} = X^{n-1} + X^{n-2} + \cdots + X + 1 \in \mathbb{Z}[X].$$

(ii) Ist $n \geq 3$, so ist $\zeta_n \notin \mathbb{Q}$ und damit gilt $\deg(\Phi_n) \geq 2$.

Beispiel 2.2.41. Es gilt $\zeta_1 = 1$, $\zeta_2 = -1$, $\zeta_3 = \omega$ und $\zeta_4 = i$. Mithilfe von Bemerkung 2.2.40 berechnet man leicht:

$$\begin{aligned}\Phi_1 &= X - 1,\\ \Phi_2 &= X + 1,\\ \Phi_3 &= X^2 + X + 1,\\ \Phi_4 &= X^2 + 1.\end{aligned}$$

Im Allgemeinen gibt es keine einfache Formel für Φ_n, aber wir werden später zeigen, dass $\deg(\Phi_n) = \varphi(n)$ (siehe Definition 2.2.44).

Beispiel 2.2.42 (Kreisteilungspolynome primer Ordnung)**.** Sei p eine Primzahl und sei

$$f = \frac{X^p-1}{X-1} = X^{p-1} + X^{p-2} + \cdots + X + 1 \in \mathbb{Z}[X].$$

Wir behaupten, dass $\Phi_p = f$ ist. Nach Bemerkung 2.2.40(i) ist Φ_p ein Teiler von f vom Grad ≥ 1. Es genügt also zu zeigen, dass f in $\mathbb{Q}[X]$ irreduzibel ist. Man kann aber kein Kriterium unmittelbar darauf anwenden. Stattdessen betrachten wir den Ringisomorphismus

$$\varepsilon_{X+1} \colon \mathbb{Q}[X] \xrightarrow{\sim} \mathbb{Q}[X], \quad X \mapsto X+1,$$

mit Umkehrisomorphismus $X \mapsto X-1$. Ein Polynom $f \in \mathbb{Q}[X]$ ist genau dann irreduzibel, wenn $\varepsilon_{X+1}(f) = f(X+1)$ irreduzibel ist. Es gilt

$$f(X+1) = \frac{(X+1)^p-1}{X+1-1} = \frac{1}{X}\left(\sum_{i=0}^{p}\binom{p}{i}X^i - 1\right) = X^{p-1} + \sum_{i=2}^{p-1}\binom{p}{i}X^{i-1} + \binom{p}{1}.$$

Jeder Binomialkoeffizient $\binom{p}{i}$ mit $i \in \{1,\ldots,p-1\}$ ist durch p teilbar, und $\binom{p}{1} = p$ ist nicht durch p^2 teilbar. Nach dem Eisensteinschen Kriterium mit dem Primideal (p) ist also $f(X+1)$ und damit auch f in $\mathbb{Q}[X]$ irreduzibel.

2.2.4 Die Eulersche φ-Funktion und der kleine Satz von Fermat

In diesem Abschnitt untersuchen wir die Restklassenringe $\mathbb{Z}/n\mathbb{Z}$ und insbesondere ihre Einheiten. Wir verweisen auf LA.8.2.4 für die Definition und grundlegende Eigenschaften des größten gemeinesamen Teilers. In einem Hauptidealring ist insbesondere $\mathrm{ggT}(x, y)$ ein erzeugendes Element des Ideals (x, y) (Bemerkung LA.8.2.39).

Proposition 2.2.43 (Einheiten in $\mathbb{Z}/n\mathbb{Z}$)**.** *Seien $n \in \mathbb{N}$ und $x \in \mathbb{Z}$. Die Restklasse $[x] \in \mathbb{Z}/n\mathbb{Z}$ ist genau dann eine Einheit, wenn $\mathrm{ggT}(x, n) = 1$.*

Beweis. Die Restklasse $[x]$ ist genau dann eine Einheit, wenn $([x]) = \mathbb{Z}/n\mathbb{Z}$. Sei $q\colon \mathbb{Z} \twoheadrightarrow \mathbb{Z}/n\mathbb{Z}$ die Quotientenabbildung. Nach Proposition 2.1.49 gibt es eine Bijektion

$$\{\text{Ideale in } \mathbb{Z}, \text{ die } n\mathbb{Z} \text{ enthalten}\} \xrightarrow{\sim} \{\text{Ideale in } \mathbb{Z}/n\mathbb{Z}\},$$
$$I \mapsto q(I) = I/n\mathbb{Z},$$

mit Umkehrabbildung $J \mapsto q^{-1}(J)$. Das Urbild unter q des Ideals $([x])$ ist das Ideal $(x, n) = (\mathrm{ggT}(x, n))$ in $\mathbb{Z}$. Also ist $[x]$ genau dann eine Einheit, wenn $\mathrm{ggT}(x, n) = 1$. □

Definition 2.2.44 (Eulersche φ-Funktion)**.** Die *Eulersche φ-Funktion* ist die Abbildung

$$\varphi\colon \mathbb{N}_{\geq 1} \to \mathbb{N}_{\geq 1}, \quad \varphi(n) = |(\mathbb{Z}/n\mathbb{Z})^\times|.$$

Nach Proposition 2.2.43 gilt auch

$$\varphi(n) = |\{x \in \{0, \ldots, n-1\} \mid \mathrm{ggT}(x, n) = 1\}|.$$

Proposition 2.2.45 (Berechnung der Eulerschen φ-Funktion)**.**

(i) *Sei p eine Primzahl und $n \in \mathbb{N} \setminus \{0\}$. Dann gilt $\varphi(p^n) = p^{n-1}(p-1)$. Insbesondere gilt $\varphi(p) = p - 1$.*

(ii) *Es gilt $\varphi(1) = 1$ und sind $n, m \in \mathbb{N}_{\geq 1}$ teilerfremd, so gilt $\varphi(nm) = \varphi(n)\varphi(m)$.*

Beweis. Zu (i). Sei $x \in \{0, \ldots, p^n - 1\}$. Es gilt $\mathrm{ggT}(x, p^n) = 1$ genau dann, wenn x kein Vielfaches von p ist. Die Vielfachen von p zwischen 0 und $p^n - 1$ sind genau die Zahlen py mit $y \in \{0, \ldots, p^{n-1} - 1\}$. Es gibt also genau p^{n-1} von denen, so dass $\varphi(n) = p^n - p^{n-1} = p^{n-1}(p-1)$.

Zu (ii). $\mathbb{Z}/1\mathbb{Z}$ ist der Nullring, der genau eine Einheit enthält. Sind n, m teilerfremd, so gibt es einen Ringisomorphismus

$$\mathbb{Z}/nm\mathbb{Z} \xrightarrow{\sim} \mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z}$$

nach dem chinesischen Restsatz (Bemerkung 2.1.54). Ein Paar (x, y) in einem Produktring $R \times S$ ist genau dann eine Einheit, wenn beide x und y Einheiten sind. Wir erhalten somit einen Gruppenisomorphismus

$$(\mathbb{Z}/nm\mathbb{Z})^\times \xrightarrow{\sim} (\mathbb{Z}/n\mathbb{Z})^\times \times (\mathbb{Z}/m\mathbb{Z})^\times,$$

so dass $\varphi(nm) = \varphi(n)\varphi(m)$. □

Proposition 2.2.46. *Seien $n \in \mathbb{N}_{\geq 1}$ und $x \in \mathbb{Z}$ mit $\mathrm{ggT}(x, n) = 1$. Dann gilt $x^{\varphi(n)} \equiv 1 \pmod{n}$.*

Beweis. Nach Proposition 2.2.43 gilt $[x] \in (\mathbb{Z}/n\mathbb{Z})^\times$. Nach dem Satz von Lagrange ist die Ordnung von $[x]$ in der Gruppe $(\mathbb{Z}/n\mathbb{Z})^\times$ ein Teiler der Mächtigkeit $|(\mathbb{Z}/n\mathbb{Z})^\times| = \varphi(n)$. Insbesondere gilt $[x]^{\varphi(n)} = [1]$ in $\mathbb{Z}/n\mathbb{Z}$, d.h., $x^{\varphi(n)} \equiv 1 \pmod{n}$. □

Als Sonderfall dieser Proposition erhalten wir den *kleinen Satz von Fermat* (der nichts mit dem großen Satz von Fermat zu tun hat):

Korollar 2.2.47 (kleiner Satz von Fermat)**.** *Sei p eine Primzahl und sei $x \in \mathbb{Z}$ mit* $\mathrm{ggT}(x,p) = 1$*. Dann gilt $x^{p-1} \equiv 1 \pmod{p}$. Für beliebiges $x \in \mathbb{Z}$ gilt $x^p \equiv x \pmod{p}$.*

Beweis. Nach Proposition 2.2.45(i) ist $\varphi(p) = p-1$. Die erste Aussage folgt nun aus Proposition 2.2.46. Die zweite Aussage folgt aus der esrten, wenn x kein Vielfaches von p ist, und sonst ist trivial. □

Bemerkung 2.2.48. Der kleine Satz von Fermat impliziert, dass alle Elemente von $\mathbb{F}_p$ Nullstellen von $X^p - X$ sind. Aus Proposition 2.1.34 erhalten wir die Zerlegung

$$X^p - X = \prod_{a \in \mathbb{F}_p} (X - a)$$

im Polynomring $\mathbb{F}_p[X]$.

Beispiel 2.2.49. Es gilt $84 = 2^2 \cdot 3 \cdot 7$. Mit der Proposition 2.2.45 berechnen wir

$$\varphi(84) = \varphi(2^2)\varphi(3)\varphi(7) = 2(2-1)(3-1)(7-1) = 24.$$

Für alle $x \in \mathbb{Z}$, die nicht durch 2, 3 oder 7 teilbar sind, gilt dann $x^{24} \equiv 1 \pmod{84}$ nach Proposition 2.2.46.

Bemerkung 2.2.50. Der kleine Satz von Fermat hat eine wichtige Anwendung in der realen Welt: Er ist die Grundlage des *RSA-Kryptosystems*, das heutzutage für fast alle elektronischen Transaktionen und digitalen Zertifikate verwendet wird.

2.2.5 Die Einheitengruppe eines Körpers

Lemma 2.2.51. *Sei $n \in \mathbb{N}_{\geq 1}$. Dann gilt*

$$\{x \in \mathbb{Z}/n\mathbb{Z} \mid \langle x \rangle = \mathbb{Z}/n\mathbb{Z}\} = (\mathbb{Z}/n\mathbb{Z})^\times.$$

Insbesondere ist die Anzahl der erzeugenden Elemente von C_n gleich $\varphi(n)$.

Beweis. Ist $\langle x \rangle = \mathbb{Z}/n\mathbb{Z}$, so gibt es ein $m \in \mathbb{Z}$ mit $mx = 1$. Die Restklasse von m ist dann ein multiplikatives Inverses zu x im Ring $\mathbb{Z}/n\mathbb{Z}$. Sei umgekehrt $x \in \mathbb{Z}/n\mathbb{Z}$ eine Einheit. Dann gibt es ein $m \in \mathbb{Z}$ mit $mx = 1$, so dass $1 \in \langle x \rangle$. Da 1 ein erzeugendes Element von $\mathbb{Z}/n\mathbb{Z}$ ist, folgt daraus $\langle x \rangle = \mathbb{Z}/n\mathbb{Z}$. □

Lemma 2.2.52. *Für alle $n \in \mathbb{N}_{\geq 1}$ gilt*

$$n = \sum_{d \in \mathbb{N},\, d|n} \varphi(d).$$

Beweis. Sei $E_d \subset \mathbb{Z}/n\mathbb{Z}$ die Teilmenge der Elemente der Ordnung d. Nach dem Satz von Lagrange ist E_d leer, wenn d kein Teiler von n ist. Für jeden Teiler $d|n$ besitzt $\mathbb{Z}/n\mathbb{Z}$ genau eine Untergruppe H_d mit d Elementen, nämlich $\frac{n}{d}\mathbb{Z}/n\mathbb{Z}$ (nach Proposition 1.1.69). Damit ist E_d die Menge der erzeugenden Elemente von H_d. Da $H_d \cong \mathbb{Z}/d\mathbb{Z}$ zyklisch ist, gilt $|E_d| = \varphi(d)$ nach Lemma 2.2.51. Schließlich ist $\mathbb{Z}/n\mathbb{Z}$ die disjunkte Vereinung der Teilmengen E_d mit $d|n$, was die gewünschte Formel liefert. □

Satz 2.2.53. *Sei R ein Integritätsring und sei $G < R^\times$ eine* endliche *Untergruppe seiner Einheitengruppe. Dann ist G zyklisch.*

Beweis. Sei $n = |G|$. Für alle $d|n$, sei $G[d] = \{x \in G \mid x^d = 1\}$. Jedes $x \in G[d]$ ist dann eine Nullstelle von $X^d - 1$ in R. Nach Korollar 2.1.66 gilt insbesondere $|G[d]| \leq d$. Sei $E_d \subset G[d]$ die Teilmenge der Elemente der Ordnung d, so dass G die disjunkte Vereinigung der Mengen E_d mit $d|n$ ist. Die Gruppe G ist genau dann zyklisch, wenn $E_n \neq \varnothing$.

Behauptung. Ist E_d nicht leer, so gilt $|E_d| = \varphi(d)$.

Denn sei $x \in E_d$. Es gilt dann $\langle x \rangle \subset G[d]$ und damit $\langle x \rangle = G[d]$, da $\langle x \rangle$ bereits d Elemente hat. Also ist $G[d]$ eine zyklische Untergruppe von G mit d Elementen, und E_d ist genau die Teilmenge ihrer erzeugenden Elemente. Die Behauptung folgt nun aus Lemma 2.2.51.

Nach der Behauptung gilt $|E_d| \in \{0, \varphi(d)\}$ für jedes $d|n$. Damit erhalten wir

$$n = |G| = \sum_{d|n} |E_d| \leq \sum_{d|n} \varphi(d) = n,$$

nach Lemma 2.2.52. Daraus folgt $|E_d| = \varphi(d)$ für alle $d|n$. Insbesondere gilt $|E_n| = \varphi(n) > 0$, so dass G zyklisch ist. □

Korollar 2.2.54. *Sei K ein endlicher Körper. Dann ist $K^\times$ eine zyklische Gruppe.*

Beispiel 2.2.55. Insbesondere ist $\mathbb{F}_p^\times$ eine zyklische Gruppe mit $p-1$ Elementen. Erzeugende Elemente von $\mathbb{F}_p^\times$ heißen *Primitivwurzeln* modulo p. Zum Beispiel ist 2 eine Primitivwurzel modulo 5, denn $2^2 = 4$, $2^3 = 8 \equiv 3 \pmod 5$ und $2^4 \equiv 2 \cdot 3 \equiv 1 \pmod 5$. Modulo 7 ist 2 keine Primitivwurzel, denn $2^3 \equiv 1 \pmod 7$, aber man kann leicht nachrechnen, dass 3 eine Primitivwurzel modulo 7 ist. Obwohl Primitivwurzeln stets existieren, ist keine effiziente Methode zur Bestimmung einer Primitivwurzel bekannt. Aus diesem Grund werden Primitivwurzeln in der Kryptographie häufig verwendet, beispielsweise in dem allgegenwärtigen Diffie-Hellman-Schlüsselaustausch.

Lemma 2.2.56. *Sei R ein Integritätsring und sei $G < R^\times$ eine endliche Untergruppe. Dann gilt*

$$\prod_{a \in G} a = \begin{cases} -1, & \text{falls } -1 \in G, \\ 1, & \text{sonst.} \end{cases}$$

Beweis. Falls $a \neq a^{-1}$ kann man das Paar $aa^{-1} = 1$ aus dem Produkt streichen. Es bleibt übrig die Elemente $a \in G$ mit $a = a^{-1}$, d.h., $a^2 = 1$. Da R ein Integritätsring ist, hat das Polynom $X^2 - 1 = (X+1)(X-1)$ höchstens zwei Nullstellen in R, und zwar genau zwei ± 1, wenn $1 \neq -1$, und genau eine sonst. In beiden Fällen erhalten wir das Gewünschte. □

Proposition 2.2.57 (Satz von Wilson)**.** *Sei $n \in \mathbb{N}_{\geq 2}$. Die folgenden Aussagen sind äquivalent:*

(i) *n ist eine Primzahl.*

(ii) *Es gilt $(n-1)! \equiv -1 \pmod n$.*

Beweis. Zu (ii) $\Rightarrow$ (i). Wir beweisen die Kontraposition. Sei $n = rs$ mit $r, s \geq 2$. Aus $r \leq n-1$ folgt, dass $(n-1)!$ ein Vielfaches von r ist. Da $r \geq 2$ ist also $(n-1)! + 1$ nicht durch r teilbar, und insbesondere nicht durch n teilbar.

Zu (i) $\Rightarrow$ (ii). Sei p eine Primzahl. Im Körper $\mathbb{Z}/p\mathbb{Z} = \mathbb{F}_p$ gilt dann $[(p-1)!] = \prod_{a \in \mathbb{F}_p^\times} a = -1$ nach Lemma 2.2.56. □

Bemerkung 2.2.58 (alternativer Beweis des Satzes von Wilson)**.** Sei p eine Primzahl. Die p-Sylowgruppen der symmetrischen Gruppe S_p haben p Elemente und damit die Form $\langle \sigma \rangle$ mit $\operatorname{ord}(\sigma) = p$. Die Elemente von S_p der Ordnung p sind genau die Zyklen der Länge p, und es gibt $p!/p = (p-1)!$ von denen. Die Anzahl der p-Sylowgruppen in S_p ist dann $(p-1)!/(p-1) = (p-2)!$, denn jede p-Sylowgruppe wird von jedem seiner $p-1$ nichttrivialen Elemente erzeugt. Nach dem dritten Sylow-Satz gilt $(p-2)! \equiv 1 \pmod p$, und daher $(p-1)! \equiv p - 1 \equiv -1 \pmod p$.

Kapitel 3

Galoistheorie

3.1 Körper und Körpererweiterungen

3.1.1 Körpererweiterungen

Definition 3.1.1 (Teilkörper, Körpererweiterung, Zwischenkörper)**.** Sei K ein Körper.

- Ein *Teilkörper* von K ist ein Unterring von K (Definition 2.1.8), der auch ein Körper ist.
- Eine *Körpererweiterung* von K ist ein Körper L, der K als Teilkörper enthält. Man schreibt in diesem Fall $L \mid K$ oder L/K (gelesen „L über K“).
- Sei $L \mid K$ eine Körpererweiterung. Ein *Zwischenkörper* von $L \mid K$ ist ein Teilkörper $M \subset L$ mit $K \subset M$.

Manchmal bezeichnen wir auch einen beliebigen Körperhomomorphismus $\varphi\colon K \to L$ als „Körpererweiterung“. Der Grund dafür ist, dass φ automatisch injektiv ist (Proposition 2.1.14), so dass K durch φ zum Teilkörper $\varphi(K)$ von L isomorph ist; alternativ dazu kann man die Elemente von L umbenennen, so dass φ die Inklusionsabbildung wird.

Notation 3.1.2. Eine Körpererweiterung $L \mid K$ wird oft mit einem senkrechten Strich

$$\begin{array}{c} L \\ | \\ K \end{array}$$

bezeichnet. Auf diese Weise kann man kompliziertere Situationen anschaulich darstellen. Zum Beispiel sagt der Diamant

$$\begin{array}{ccc} & \mathbb{C} & \\ \diagup & & \diagdown \\ \mathbb{Q}(i) & & \mathbb{R} \\ \diagdown & & \diagup \\ & \mathbb{Q}, & \end{array}$$

dass $\mathbb{Q}(i)$ und $\mathbb{R}$ Zwischenkörper von $\mathbb{C} \mid \mathbb{Q}$ sind.

Definition 3.1.3 (Grad einer Körpererweiterung)**.** Sei $L \mid K$ eine Körpererweiterung. Insbesondere hat L eine Struktur von K-Vektorraum (siehe Beispiel LA.3.2.4). Der *Grad* von L über K ist die Dimension von L als K-Vektorraum und wird mit $[L : K]$ bezeichnet:

$$[L : K] = \dim_K L.$$

Die Körpererweiterung $L \mid K$ heißt *endlich*, wenn $[L : K] < \infty$, und *unendlich*, wenn $[L : K] = \infty$.

Beispiel 3.1.4.

(i) Jeder Körper K ist eine Körpererweiterung von sich selbst, und zwar die einzige Körpererweiterung von K vom Grad 1.

(ii) $\mathbb{C} \mid \mathbb{R}$, $\mathbb{Q}(i) \mid \mathbb{Q}$ und $\mathbb{F}_4 \mid \mathbb{F}_2$ sind Körpererweiterungen vom Grad 2.

(iii) Ist f ein irreduzibles Polynom über K, so ist $K[X]/(f)$ eine endliche Körpererweiterung von K vom Grad $\deg(f)$ (siehe Beispiel 2.2.13).

(iv) Der Körper $K(X) = Q(K[X])$ der rationalen Funktionen über K ist eine unendliche Körpererweiterung von K.

Beispiel 3.1.5 (Primkörper)**.** Jeder Körper K enthält einen *kleinsten* Teilkörper K_0, d.h., einen Teilkörper, der in allen Teilkörpern von K enthalten ist. Dies folgt aus Beispiel 2.1.47, wenn K die Primcharakteristik p hat, und aus Beispiel 2.1.69, wenn K die Charakteristik 0 hat: Im ersten Fall ist K_0 zu $\mathbb{F}_p$ isomorph, und in zweiten Fall ist es zu $\mathbb{Q}$ isomorph. Der Körper K_0 heißt der *Primkörper* von K.

Bemerkung 3.1.6 (additive Gruppe endlicher Körper)**.** Sei K ein endlicher Körper der Charakteristik p. Dann ist K ein endlich-dimensionaler Vektorraum über seinem Primkörper $K_0 \cong \mathbb{F}_p$, und damit ist seine additive Gruppe $(K, +)$ zu $\mathbb{F}_p^n$ isomorph. Insbesondere ist die Mächtigkeit von K eine Potenz von p.

Proposition 3.1.7 (Multiplikativität des Grades)**.** *Sei $L \mid K$ eine Körpererweiterung und sei M ein Zwischenkörper von $L \mid K$. Dann gilt*

$$[L : K] = [L : M] \cdot [M : K].$$

Beweis. Sei $(x_i)_{i \in I}$ eine Basis von M über K und $(y_j)_{j \in J}$ eine Basis von L über M. Dann ist die Familie $(x_i y_j)_{(i,j) \in I \times J}$ eine Basis von L über K:

- Sie ist linear unabhängig, denn: Sei $\sum_{i,j} \lambda_{ij} x_i y_j = 0$ mit $\lambda_{ij} \in K$. Da die Familie $(y_j)_{j \in J}$ M-linear unabhängig ist, folgt daraus, dass für alle $j \in J$ gilt $\sum_i \lambda_{ij} x_i = 0$. Aus der K-linearen Unabhängigkeit der Familie $(x_i)_{i \in I}$ schließen wir, dass jedes λ_{ij} null sein muss.
- Sie ist erzeugend, denn: Sei $a \in L$ beliebig. Es gibt eine Familie $(\mu_j)_{j \in J} \in M^{(J)}$ mit $a = \sum_{j \in J} \mu_j y_j$. Jedes μ_j ist wiederum eine Summe $\sum_{i \in I} \lambda_{ij} x_i$ mit einer Familie $(\lambda_{ij})_{i \in I} \in K^{(I)}$ (die die Nullfamilie ist, wenn $\mu_j = 0$). Insgesamt sind nur endlich viele der λ_{ij} nicht null, und es gilt $a = \sum_{i,j} \lambda_{ij} x_i y_j$.

Damit gilt $[L : K] = |I \times J| = |I| \cdot |J| = [L : M] \cdot [M : K]$. □

Definition 3.1.8 (Morphismen von Körpererweiterungen)**.** Sei K ein Körper und seien $L \mid K$ und $M \mid K$ Körpererweiterungen. Ein *Morphismus von Körpererweiterungen* von $L \mid K$ nach $M \mid K$ ist ein Körperhomomorphismus $\varphi \colon L \to M$ mit $\varphi|_K = \mathrm{id}_K$.

Bemerkung 3.1.9 (die Kategorie der Körpererweiterungen)**.** Sei K ein Körper. Körpererweiterungen von K und ihre Morphismen bilden eine Kategorie. Dementsprechend werden die Begriffe von *Isomorphismen*, *Endomorphismen* und *Automorphismen* von Körpererweiterungen wie gewöhnlich definiert.

Die Tatsache, dass Körperhomomorphismen injektiv sind, impliziert, dass die Kategorie der Körpererweiterungen von K *äquivalent* zur Kommakategorie der Körper unter K ist (siehe Beispiel LA.A.1.15 und Definition LA.A.3.12), die weiter zu einer vollen Unterkategorie der Kategorie der K-Algebren äquivalent ist (siehe Beispiel LA.A.3.18).

Definition 3.1.10 (Galoisgruppe)**.** Sei $L \mid K$ eine Körpererweiterung. Die *Galoisgruppe* von L über K ist die Automorphismengruppe von $L \mid K$ in der Kategorie der Körpererweiterungen von K, das heißt:

$$\mathrm{Gal}(L \mid K) = (\{\varphi\colon L \to L \mid \varphi \text{ ist ein Ringisomorphismus mit } \varphi|_K = \mathrm{id}_K\}, \circ).$$

Beispiel 3.1.11. Die Galoisgruppe $\mathrm{Gal}(\mathbb{C} \mid \mathbb{R})$ haben wir schon im Beispiel 1.1.12 berechnet: Sie ist die zweielementige Gruppe $\{\mathrm{id}_{\mathbb{C}}, z \mapsto \bar{z}\}$. Eine ähnliches Argument zeigt, dass $\mathrm{Gal}(\mathbb{Q}(i) \mid \mathbb{Q}) = \{\mathrm{id}_{\mathbb{Q}(i)}, z \mapsto \bar{z}\}$.

Wie bei Untergruppen (Proposition 1.1.42) und bei Unterringen (Bemerkung LA.8.1.11) ist ein Durchschnitt von Teilkörpern eines Körpers K wieder ein Teilkörper von K. Dies ermöglicht die folgende Definition:

Definition 3.1.12 (erzeugter Teilkörper/Zwischenkörper, endlich erzeugte Körpererweiterung, Kompositum)**.**

- Sei L ein Körper und $S \subset L$ eine Teilmenge. Der *von S erzeugte Teilkörper* von L ist der kleinste Teilkörper von L, der S enthält, d.h., der Durchschnitt aller Teilkörper von L, die S enthalten.
- Sei $L \mid K$ eine Körpererweiterung und sei $S \subset L$ eine Teilmenge. Der *von S erzeugte Zwischenkörper* von $L \mid K$ ist der kleinste Zwischenkörper von $L \mid K$, der S enthält, d.h., der von $S \cup K$ erzeugte Teilkörper von L. Man bezeichnet ihn mit $K(S)$. Falls $S = \{a_1, \ldots, a_n\}$ schreibt man auch $K(a_1, \ldots, a_n)$ statt $K(S)$.
- Eine Körpererweiterung $L \mid K$ heißt *endlich erzeugt*, wenn eine endliche Teilmenge $S \subset L$ mit $L = K(S)$ existiert.
- Seien M und N Teilkörper von L. Das *Kompositum* von M und N in L ist der von $M \cup N$ erzeugte Teilkörper von L. Man bezeichnet ihn mit MN.

Bei den Bezeichnungen $K(S)$ und MN man muss beachten, dass diese Konstruktionen nicht nur von K und S bzw. von M und N abhängen, sondern auch vom umgebenden Körper L.

Beispiel 3.1.13.

(i) Der Primkörper eines Körpers K ist der von $\varnothing$ erzeugte Teilkörper von K.

(ii) Jeder Körper K kann als Körpererweiterung seines Primkörpers K_0 aufgefasst werden. Ist $S \subset K$ eine Teilmenge, so ist der von S erzeugte Teilkörper von K gleich dem von S erzeugten Zwischenkörper von $K \mid K_0$.

(iii) Der Körper $\mathbb{Q}(i)$ der rationalen komplexen Zahlen ist der von i erzeugte Teilkörper von $\mathbb{C}$.

(iv) Der kleinste Teilkörper von $K(X) = Q(K[X])$, der K und X enthält, ist $K(X)$ selbst. Die Notation $K(X)$ ist damit kompatibel mit der Notation für den von X erzeugten Zwischenkörper von $K(X) \mid K$.

Bemerkung 3.1.14. Eine endliche Körpererweiterung $L \mid K$ ist endlich erzeugt, denn: Ist $(a_1, \ldots, a_d)$ eine Basis von L über K, so gilt $L = K(a_1, \ldots, a_d)$. Die Umkehrung gilt aber nicht: Zum Beispiel ist $K(X) \mid K$ eine unendliche aber endlich erzeugte Körpererweiterung.

Definition 3.1.15 (einfache Körpererweiterung, primitives Element)**.** Eine Körpererweiterung $L \mid K$ heißt *einfach* oder *monogen*, wenn ein Element $a \in L$ mit $L = K(a)$ existiert. Ein solches Element $a \in L$ heißt dann *primitives Element* von $L \mid K$.

Beispiel 3.1.16. $\mathbb{C}$ ist eine einfache Körpererweiterung von $\mathbb{R}$, denn $\mathbb{C} = \mathbb{R}(i)$. Jedes Element $a \in \mathbb{C} \setminus \mathbb{R}$ ist ein pimitives Element von $\mathbb{C} \mid \mathbb{R}$, denn aus $\mathbb{R} \subsetneqq \mathbb{R}(a) \subset \mathbb{C}$ und Dimensionsgründen folgt $\mathbb{R}(a) = \mathbb{C}$.

3.1.2 Algebraizität

Wir erinnern zunächst an ein paar Definitionen aus der Linearen Algebra (siehe dazu LA.9.1).

Definition 3.1.17 (algebraisch, transzendent)**.** Sei K ein Körper und A eine K-Algebra. Ein Element $a \in A$ heißt *algebraisch* über K, wenn ein Polynom $f \in K[X] \setminus \{0\}$ existiert mit $f(a) = 0$, d.h., wenn der Einsetzungshomomorphismus $\varepsilon_a \colon K[X] \to A$ nicht injektiv ist. Sonst heißt a *transzendent* über K.

Proposition 3.1.18 (Charakterisierung der Algebraizität)**.** *Sei K ein Körper, A eine K-Algebra und $a \in A$. Dann sind die folgenden Aussagen äquivalent:*

(i) *a ist algebraisch über K.*

(ii) $\ker \varepsilon_a \neq \{0\}$.

(iii) $\dim_K \ker \varepsilon_a = \infty$.

(iv) $\dim_K \operatorname{im} \varepsilon_a < \infty$.

Beweis. Siehe Proposition LA.9.1.2. □

Korollar 3.1.19. *Sei K ein Körper und A eine K-Algebra, so dass $\dim_K A < \infty$. Dann sind alle Elemente von A algebraisch über K.*

Beweis. Dies folgt aus Proposition 3.1.18 (iv) $\Rightarrow$ (i). □

Beispiel 3.1.20.

(i) In der K-Algebra $K[X]$ sind alle Polynome p vom Grad ≥ 1 transzendent uber K. Denn der Einsetzungshomomorphismus $\varepsilon_p \colon K[X] \to K[X]$ bildet ein Polynom vom Grad d auf ein Polynom vom Grad $d \cdot \deg(p)$ ab.

(ii) Da $\dim_K M_n(K) = n^2 < \infty$ sind alle quadratischen Matrizen über K algebraisch über K.

(iii) Da $\dim_{\mathbb{R}} \mathbb{C} = 2 < \infty$ ist jede komplexe Zahl algebraisch über $\mathbb{R}$.

(iv) Die komplexe Zahl $i \in \mathbb{C}$ ist algebraisch über $\mathbb{Q}$, denn $i^2 + 1 = 0$, d.h., $X^2 + 1 \in \ker \varepsilon_i$.

(v) Die reelle Zahl $a = \sqrt{2} + \sqrt{3}$ ist algebraisch über $\mathbb{Q}$. Denn

$$a^2 = 5 + 2\sqrt{6} \quad \Longrightarrow \quad (a^2 - 5)^2 = 24 \quad \Longrightarrow \quad a^4 - 10a^2 + 1 = 0.$$

(vi) Die Elemente $\alpha, \beta \in \mathbb{F}_4$ sind algebraisch über $\mathbb{F}_2$, da $\dim_{\mathbb{F}_2} \mathbb{F}_4 = 2 < \infty$. Expliziter gilt $\alpha^3 - 1 = \beta^3 - 1 = 0$ (siehe Bemerkung LA.2.4.11).

Bemerkung 3.1.21 (algebraische und transzendente Zahlen)**.** Komplexe Zahlen, die algebraisch über $\mathbb{Q}$ sind, heißen *algebraische Zahlen*. Man bezeichnet mit $\bar{\mathbb{Q}} \subset \mathbb{C}$ die Menge aller algebraischen Zahlen (die ein Teilkörper von $\mathbb{C}$ ist, siehe Korollar 3.1.43). Elemente von $\mathbb{C} \setminus \bar{\mathbb{Q}}$ heißen *transzendente Zahlen*. Es folgt aus Satz LA.1.3.36, dass $\bar{\mathbb{Q}}$ abzählbar ist, da jedes Polynom über $\mathbb{Q}$ nur endlich viele Koeffizienten aus $\mathbb{Q}$ enthält und nur endlich viele Nullstellen in $\mathbb{C}$ hat. Da $\mathbb{C}$ selbst überabzählbar ist, ist auch die Menge $\mathbb{C} \setminus \bar{\mathbb{Q}}$ überabzählbar. In diesem Sinne sind die meisten komplexen Zahlen transzendent. Es ist jedoch nicht einfach zu entscheiden, ob eine gegebene Zahl transzendent ist oder nicht. Die Zahlen π und e sind bekanntlich transzendent, aber es ist zum Beispiel nicht bekannt, ob $\pi + e$ transzendent ist.

Nach Beispiel 2.2.6(ii) ist $K[X]$ ein Hauptidealring, in dem jedes Nicht-Null-Element zu genau einem monischen Polynom assoziiert ist, d.h., es gibt eine Bijektion

$$\begin{aligned} \{0\} \cup \{\text{monische Polynome in } K[X]\} &\xrightarrow{\sim} \{\text{Ideale in } K[X]\}, \\ f &\mapsto (f). \end{aligned}$$

Definition 3.1.22 (Minimalpolynom)**.** Sei K ein Körper, A eine K-Algebra und $a \in A$. Sei $\varepsilon_a \colon K[X] \to A$ der Einsetzungshomomorphismus mit $\varepsilon_a(X) = a$. Das *Minimalpolynom* von a über K ist das eindeutige Polynom $m_a \in K[X]$, das entweder null oder monisch ist, so dass

$$\ker \varepsilon_a = (m_a).$$

Bemerkung 3.1.23 (Bestimmung des Minimalpolynoms)**.** Sei $L \mid K$ eine Körpererweiterung und sei $a \in L$.

(i) Ist $f \in K[X]$ ein irreduzibles monisches Polynom mit $f(a) = 0$, so ist f bereits das Minimalpolynom von a über K, denn das Ideal (f) in $K[X]$ ist maximal und erfüllt $(f) \subset \ker \varepsilon_a \subsetneq K[X]$. Dabei sind die Irreduzibilitätskriterien aus Abschnitt 2.2.3 hilfreich.

(ii) Wenn $[L : K] < \infty$ und eine Basis von L über K bekannt ist, kann man das Minimalpolynom m_a mit folgendem Rezept bestimmen. Mithilfe der Linearen Algebra kann man das kleinste d bestimmen, so dass die Familie $(1, a, \dots, a^{d-1})$ K-linear unabhängig ist, und dadurch findet man Skalare $\lambda_0, \dots, \lambda_{d-1} \in K$ mit

$$a^d = \sum_{i=0}^{d-1} \lambda_i a^i.$$

Dann ist $m_a = X^d - \sum_{i=0}^{d-1} \lambda_i X^i$. Denn nach Konstruktion gilt $f(a) \neq 0$ für alle Polynome $f \neq 0$ vom Grad $< d$.

Satz 3.1.24 (explizite Beschreibung einfacher Körpererweiterungen)**.** *Sei $L \mid K$ eine Körpererweiterung, sei $a \in L$, sei $K(a)$ der von a erzeugte Zwischenkörper von $L \mid K$, und sei*

$$\varepsilon_a \colon K[X] \to L, \quad f \mapsto f(a),$$

der Einsetzungshomomorphismus zu a.

(i) *Ist a algebraisch über K, so ist sein Minimalpolynom $m_a \in K[X]$ irreduzibel, und ε_a induziert einen K-Algebrenisomorphismus $\bar{\varepsilon}_a \colon K[X]/(m_a) \xrightarrow{\sim} K(a)$. Insbesondere gilt $[K(a) : K] = \deg(m_a)$, und $(1, a, \dots, a^{\deg(m_a)-1})$ ist eine Basis von $K(a)$ über K.*

(ii) *Ist a transzendent über K, so induziert ε_a einen K-Algebrenisomorphismus $\hat{\varepsilon}_a \colon K(X) \xrightarrow{\sim} K(a)$.*

Beweis. Nach dem Homomorphiesatz induziert ε_a einen Isomorphismus

$$K[X]/\ker \varepsilon_a \xrightarrow{\sim} \operatorname{im} \varepsilon_a.$$

Da $\operatorname{im} \varepsilon_a$ ein Unterring vom Körper L ist, ist er ein Integritätsring. Nach Proposition 2.2.10(i) ist $\ker \varepsilon_a = (m_a)$ ein Primideal im Hauptidealring $K[X]$.

Zu (i). Nach Definition gilt in diesem Fall $m_a \neq 0$. Damit ist m_a ein Primelement von $K[X]$, d.h., irreduzibel, und das Ideal (m_a) ist ein maximales Ideal (nach Beispiel 2.2.9(ii)). Nach Proposition 2.2.10(ii) ist dann $\operatorname{im} \varepsilon_a$ ein Körper. Aus $K \subset \operatorname{im} \varepsilon_a \subset K(a)$ und der Definition von $K(a)$ folgt, dass $\operatorname{im} \varepsilon_a = K(a)$. Die zusätzliche Aussage folgt daraus, dass $(1, [X], \dots, [X]^{\deg(m_a)-1})$ eine Basis von $K[X]/(m_a)$ über K ist (siehe Beispiel 2.2.13).

Zu (ii). In diesem Fall gilt $m_a = 0$. Nach der universellen Eigenschaft des Quotientenkörpers (Bemerkung 2.1.70) induziert ε_a einen Körperhomomorphismus $\hat{\varepsilon}_a \colon K(X) \hookrightarrow K(a)$. Das Bild von $\hat{\varepsilon}_a$ ist dann ein Teilkörper von L, der K und a enthält. Da $K(a)$ der kleinste solche Teilkörper von L ist, ist $\hat{\varepsilon}_a$ bijektiv. □

Bemerkung 3.1.25. In beiden Fällen des Satzes 3.1.24 ist der Zwischenkörper $K(a)$ zum Restklassenkörper $\kappa(m_a)$ isomorph (Definition 2.2.14).

Beispiel 3.1.26. Wir betrachten die Körpererweiterung $\mathbb{C} \mid \mathbb{Q}$.

(i) Das Minimalpolynom von $\sqrt{2}$ über $\mathbb{Q}$ ist $X^2 - 2$. Es gibt damit einen Isomorphismus

$$\mathbb{Q}[X]/(X^2 - 2) \xrightarrow{\sim} \mathbb{Q}(\sqrt{2}),$$

der $[X]$ auf $\sqrt{2}$ abbildet. Zudem ist $(1, \sqrt{2})$ eine Basis von $\mathbb{Q}(\sqrt{2})$ über $\mathbb{Q}$, so dass

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

(ii) Das Minimalpolynom von $\sqrt[3]{2}$ über $\mathbb{Q}$ ist $X^3 - 2$ (da dieses Polynom irreduzibel ist, z.B. nach dem Eisensteinschen Kriterium). Es gibt damit einen Isomorphismus

$$\mathbb{Q}[X]/(X^3 - 2) \xrightarrow{\sim} \mathbb{Q}(\sqrt[3]{2}),$$

der $[X]$ auf $\sqrt[3]{2}$ abbildet. Zudem ist $(1, \sqrt[3]{2}, (\sqrt[3]{2})^2)$ eine Basis von $\mathbb{Q}(\sqrt[3]{2})$ über $\mathbb{Q}$, so dass

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

(iii) Das Minimalpolynom von $\omega = e^{2\pi i/3}$ über $\mathbb{Q}$ ist das Kreisteilungspolynom $\Phi_3 = X^2 + X + 1$ (Beispiel 2.2.41). Es gibt damit einen Isomorphismus

$$\mathbb{Q}[X]/(X^2 + X + 1) \xrightarrow{\sim} \mathbb{Q}(\omega),$$

der $[X]$ auf ω abbildet. Zudem ist $(1, \omega)$ eine Basis von $\mathbb{Q}(\omega)$ über $\mathbb{Q}$, so dass

$$\mathbb{Q}(\omega) = \{a + b\omega \mid a, b \in \mathbb{Q}\}.$$

(iv) Da π transzendent über $\mathbb{Q}$ ist, gibt es einen Isomorphismus $\mathbb{Q}(X) \xrightarrow{\sim} \mathbb{Q}(\pi)$, der X auf π abbildet.

Beispiel 3.1.27 (Einheitswurzeln und Kreisteilungskörper)**.** Sei K ein Körper und $n \in \mathbb{N}_{\geq 1}$. Ein element $\zeta \in K$ mit $\zeta^n = 1$ heißt n-te *Einheitswurzel*. Man bezeichnet mit $\mu_n(K)$ die Menge aller n-ten Einheitswurzeln in K, die eine Untergruppe der multiplikativen Gruppe $K^\times$ ist. Nach Korollar 2.1.66 gilt zudem $|\mu_n(K)| \leq n$, und nach Satz 2.2.53 ist $\mu_n(K)$ eine zyklische Gruppe. Eine n-te Einheitswurzel ζ heißt *primitiv*, wenn $\zeta^m \neq 1$ für alle $m \in \{1, \ldots, n-1\}$. Primitive n-te Einheitswurzeln existieren genau dann, wenn $|\mu_n(K)| = n$, in welchem Fall sie genau die erzeugenden Elemente der zyklischen Gruppe $\mu_n(K)$ sind. Insbesondere gibt es dann genau $\varphi(n)$ primitive Einheitswurzeln nach Lemma 2.2.51. Die primitiven $(p-1)$-ten Einheitswurzeln in $\mathbb{F}_p$ sind genau die Primitivwurzeln modulo p aus Beispiel 2.2.55.

Im Körper $\mathbb{C}$ ist $\zeta_n = e^{2\pi i/n}$ eine primitive n-te Einheitswurzel. Das Minimalpolynom von ζ_n über $\mathbb{Q}$ ist nach Definition das Kreisteilungspolynom $\Phi_n \in \mathbb{Z}[X]$ (Definition 2.2.39). Es gibt also einen Isomorphismus

$$\mathbb{Q}[X]/(\Phi_n) \xrightarrow{\sim} \mathbb{Q}(\zeta_n).$$

Der Körper $\mathbb{Q}(\zeta_n)$ heißt der n-te *Kreisteilungskörper* und spielt eine wichtige Rolle in der Zahlentheorie.

Korollar 3.1.28 (universelle Eigenschaft einfacher algebraischer Körpererweiterungen)**.** *Sei $L \mid K$ eine Körpererweiterung und sei $a \in L$ algebraisch über K mit Minimalpolynom $m_a \in K[X]$. Zu jeder K-Algebra A und jedem Element $b \in A$ mit $m_a(b) = 0$ gibt es* genau einen *K-Algebrenhomomorphismus $\varphi\colon K(a) \to A$ mit $\varphi(a) = b$.*

Beweis. Nach Satz 3.1.24(i) gilt $K(a) \cong K[X]/(m_a)$. Die Aussage folgt nun aus den universellen Eigenschaften der Polynomalgebra (Proposition 2.1.30) und des Restklassenringes (Proposition 2.1.46). □

Definition 3.1.29 (algebraisch konjugiert)**.** Sei $L \mid K$ eine Körpererweiterung. Zwei Elemente $a, b \in L$ heißen *algebraisch konjugiert* über K, wenn sie dasselbe Minimalpolynom über K haben.

Beispiel 3.1.30.

(i) Die komplexen Zahlen i und $-i$ sind algebraisch konjugiert über $\mathbb{Q}$ und über $\mathbb{R}$, aber nicht über $\mathbb{C}$. Die Elemente $\alpha, \beta \in \mathbb{F}_4$ sind algebraisch konjugiert über $\mathbb{F}_2$.

(ii) Die komplexen Zahlen $\sqrt[3]{2}$ und $\omega\sqrt[3]{2}$ sind algebraisch konjugiert über $\mathbb{Q}$. Sie sind aber nicht algebraisch konjugiert über $\mathbb{Q}(\sqrt[3]{2})$.

(iii) Das Minimalpolynom von $\sqrt{2}+\sqrt{3}$ über $\mathbb{Q}$ ist X^4-10X^2+1 (siehe Beispiel 3.1.20(iv)), da dieses Polynom irreduzibel ist. Die algebraisch konjugierten Elemente zu $\sqrt{2}+\sqrt{3}$ über $\mathbb{Q}$ sind deswegen die vier Nullstellen von $X^4 - 10X^2 + 1$, nämlich $\pm\sqrt{2} \pm \sqrt{3}$.

(iv) Im Körper $K(X)$ sind X und $X + 1$ algebraisch konjugiert über K, denn beide sind transzendent über K.

Proposition 3.1.31 (Konjugationsprinzip)**.** *Sei $L \mid K$ eine Körpererweiterung und seien $a, b \in L$. Dann sind die folgenden Aussagen äquivalent:*

(i) *a und b sind algebraisch konjugiert über K.*

(ii) *Es gibt einen Isomorphismus $\sigma\colon K(a) \xrightarrow{\sim} K(b)$ von Körpererweiterungen von K mit $\sigma(a) = b$.*

Außerdem ist der Morphismus σ in (ii) *eindeutig durch a und b bestimmt.*

Beweis. Zu (ii) $\Rightarrow$ (i). Ist $b = \sigma(a)$, so folgt $f(b) = \sigma(f(a))$ für alle $f \in K[X]$. Ist a transzendent über K, so ist auch b transzendent über K, da σ injektiv ist. Sonst ist m_a irreduzibel, und damit ist m_a auch das Minimalpolynom von b.

Zu (i) $\Rightarrow$ (ii). Wir betrachten zwei Fälle:

- *a ist algebraisch über K*, d.h., $m_a \neq 0$. Es gilt $m_a(b) = m_b(b) = 0$. Nach Korollar 3.1.28 gibt es genau einen Morphismus von Körpererweiterungen von K

$$\sigma\colon K(a) \to K(b) \quad \text{mit} \quad \sigma(a) = b.$$

  Nach Satz 3.1.24(i) sind beide Grade $[K(a) : K]$ und $[K(b) : K]$ gleich dem Grad von m_a. Da σ ein Körperhomomorphismus ist, ist es injektiv und damit auch bijektiv nach Korollar LA.4.1.39.

- *a ist transzendent über K.* Dann ist b auch transzendent über K. Nach Satz 3.1.24(ii) gibt es Isomorphismen $\hat{\varepsilon}_a\colon K(X) \cong K(a)$ und $\hat{\varepsilon}_b\colon K(X) \cong K(b)$. Dann hat $\sigma = \hat{\varepsilon}_b \circ \hat{\varepsilon}_a^{-1}$ die gewünschte Eigenschaft. Die Eindeutigkeit von σ folgt aus den universellen Eigenschaften der Polynomalgebra (Proposition 2.1.30) und der Lokalisierung (Proposition 2.1.68). □

Konstruktion 3.1.32 (die Galoisoperation auf den Nullstellen)**.** Sei $L \mid K$ eine Körpererweiterung, sei $f \in K[X]$ und sei $N_L(f) \subset L$ die Nullstellenmenge von f in L. Ist $a \in N_L(f)$ und ist $\sigma \in \mathrm{Gal}(L \mid K)$, so gilt $f(\sigma(a)) = \sigma(f(a)) = 0$ (da σ die Koeffizienten von f erhält), so dass $\sigma(a) \in N_L(f)$. Damit erhalten wir eine Verknüpfung

$$\mathrm{Gal}(L \mid K) \times N_L(f) \to N_L(f), \quad (\sigma, a) \mapsto \sigma(a),$$

die eine Gruppenoperation der Galoisgruppe von $L \mid K$ auf der Menge $N_L(f)$ definiert.

Beispiel 3.1.33. Die Nullstellenmenge von $X^3 - 1$ in $\mathbb{C}$ ist $\{1, \omega, \omega^2\}$. Die Operation von $\mathrm{Gal}(\mathbb{C} \mid \mathbb{R}) = \{\mathrm{id}_{\mathbb{C}}, z \mapsto \bar{z}\}$ darauf hat die zwei Bahnen $\{1\}$ und $\{\omega, \omega^2\}$.

Korollar 3.1.34. *Sei $L \mid K$ eine Körpererweiterung und sei $a \in L$ algebraisch über K mit Minimalpolynom $m_a \in K[X]$.*

(i) *Für alle $b \in N_{K(a)}(m_a)$ gelten $m_b = m_a$ und $K(b) = K(a)$.*

(ii) *Die Operation der Galoisgruppe $\mathrm{Gal}(K(a) \mid K)$ auf $N_{K(a)}(m_a)$ ist frei und transitiv.*

(iii) *Es gilt $|\mathrm{Gal}(K(a) \mid K)| = |N_{K(a)}(m_a)| \leq \deg(m_a) = [K(a) : K]$.*

Beweis. Zu (i). Da $m_a(b) = 0$ und m_a irreduzibel ist, ist m_a auch das Minimalpolynom von b. Nach Voraussetzung gilt $b \in K(a)$ und somit $K(b) \subset K(a)$. Nach Satz 3.1.24(i) gilt $[K(b) : K] = \deg(m_a) = [K(a) : K] < \infty$. Aus Proposition LA.3.3.35 folgt nun $K(b) = K(a)$.

Zu (ii). Dies folgt aus (i) mit dem Konjugationsprinzip (Proposition 3.1.31): Für alle $b, c \in N_{K(a)}(m_a)$ gibt es genau einen Isomorphismus $\sigma\colon K(a) = K(b) \xrightarrow{\sim} K(c) = K(a)$ von Körpererweiterungen von K mit $\sigma(b) = c$. Die Existenz bzw. die Eindeutigkeit von σ bedeutet, dass die Operation transitiv bzw. frei ist.

Zu (iii). Die Abbildung

$$\mathrm{Gal}(K(a) \mid K) \to N_{K(a)}(m_a), \quad \sigma \mapsto \sigma(a),$$

ist injektiv (da die Operation frei ist) und surjektiv (da die Operation transitiv ist). Die Ungleichung $|N_{K(a)}(m_a)| \leq \deg(m_a)$ folgt aus Korollar 2.1.66. □

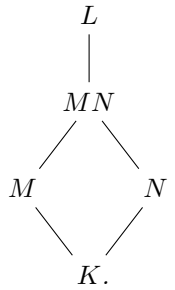
Beispiel 3.1.35. Die Ungleichung $|\mathrm{Gal}(K(a) \mid K)| < [K(a) : K]$ im Korollar 3.1.34(iii) ist möglich. Sei zum Beispiel $K = \mathbb{Q}$, $L = \mathbb{C}$ und $a = \sqrt[3]{2}$. Das Minimalpolynom von $\sqrt[3]{2}$ über $\mathbb{Q}$ ist $X^3 - 2$, so dass $[\mathbb{Q}(\sqrt[3]{2}) : \mathbb{Q}] = 3$. Die Nullstellen von $X^3 - 2$ in $\mathbb{C}$ sind $\sqrt[3]{2}$, $\omega\sqrt[3]{2}$ und $\omega^2\sqrt[3]{2}$. Nur die erste von denen liegt im Körper $\mathbb{Q}(\sqrt[3]{2}) \subset \mathbb{R}$, so dass $|\mathrm{Gal}(\mathbb{Q}(\sqrt[3]{2}) \mid \mathbb{Q})| = 1$.

Beispiel 3.1.36. Wir bestimmen die Galoisgruppe $\mathrm{Gal}(\mathbb{Q}(\omega) \mid \mathbb{Q})$. Nach Beispiel 3.1.26(iii) gilt $[\mathbb{Q}(\omega) : \mathbb{Q}] = 2$, so dass $\mathrm{Gal}(\mathbb{Q}(\omega) \mid \mathbb{Q})$ höchstens zwei Elemente hat. Da $\bar{\omega} = \omega^2 \in \mathbb{Q}(\omega)$ schränkt sich die komplexe Konjugation $z \mapsto \bar{z}$ zu einem Automorphismus von $\mathbb{Q}(\omega)|\mathbb{Q}$, der nicht die Identität ist. Also gilt

$$\mathrm{Gal}(\mathbb{Q}(\omega) \mid \mathbb{Q}) = \{\mathrm{id}_{\mathbb{Q}(\omega)}, z \mapsto \bar{z}\}.$$

Alternativ dazu kann man Korollar 3.1.34(ii) direkt anwenden: Die Gruppe $\mathrm{Gal}(\mathbb{Q}(\omega) \mid \mathbb{Q})$ muss frei und transitiv auf der Nullstellenmenge $\{\omega, \omega^2\}$ von $\Phi_3 = X^2 + X + 1$ in $\mathbb{Q}(\omega)$ operieren, und damit hat genau zwei Elemente, die Identität sowie einen Automorphismus, der ω und ω^2 vertauscht.

Proposition 3.1.37 (Grade von Komposita)**.** *Sei $L \mid K$ eine Körpererweiterung und seien M und N Zwischenkörper von $L \mid K$ mit Kompositum MN:*



(i) *Ist $[M : K]$ endlich, so ist auch $[MN : N]$ endlich und zwar*

$$[MN : N] \leq [M : K].$$

Insbesondere gilt $[MN : K] \leq [M : K] \cdot [N : K]$.

(ii) *Sind* $[M : K]$ *und* $[N : K]$ *endlich und teilerfremd, so gilt*

$$[MN : K] = [M : K] \cdot [N : K].$$

Beweis. Zu (i). Die zweite Aussage folgt aus der ersten mit Proposition 3.1.7. Sei $d = [M : K]$ und sei $(a_1, \ldots, a_d)$ eine Basis von M über K. Sei $M_i = K(a_1, \ldots, a_i) \subset M$, so dass $M_0 = K$ und $M_d = M$. Wir zeigen

$$[M_iN : N] \leq [M_i : K]$$

durch Induktion über i. Der Fall $i = 0$ ist trivial. Nach Proposition 3.1.7 gilt

$$[M_iN : N] = [M_iN : M_{i-1}N] \cdot [M_{i-1}N : N] \quad \text{und} \quad [M_i : K] = [M_i : M_{i-1}] \cdot [M_{i-1} : K].$$

Nach Induktionsvoraussetzung genügt es zu zeigen:

$$[M_iN : M_{i-1}N] \leq [M_i : M_{i-1}].$$

Es gilt nach Definition $M_i = M_{i-1}(a_i)$ und $M_iN = M_{i-1}N(a_i)$. Sei $m \in M_{i-1}[X]$ das Minimalpolynom von a_i über M_{i-1} und sei $n \in M_{i-1}N[X]$ das Minimalpolynom von a_i über $M_{i-1}N$. Nach Satz 3.1.24(i) gilt $[M_i : M_{i-1}] = \deg(m)$ und $[M_iN : M_{i-1}N] = \deg(n)$. Da $m(a_i) = 0$ muss m in $M_{i-1}N[X]$ durch n teilbar sein. Insbesondere gilt $\deg(n) \leq \deg(m)$, wie gewünscht.

Zu (ii). Nach (i) ist $[MN : K]$ endlich, und nach Proposition 3.1.7 ist $[MN : K]$ durch $\mathrm{kgV}([M : K], [M : N])$ teilbar. Da $[M : K]$ und $[N : K]$ teilerfremd sind, ist ihr kgV gleich ihrem Produkt, so dass $[MN : K] \geq [M : K] \cdot [N : K]$. Zusammen mit (i) erhalten wir die Gleichheit. □

Beispiel 3.1.38. In der Situation der Proposition 3.1.37 ist es möglich, dass

$$[MN : K] < [M : K] \cdot [N : K]$$

gilt, selbst wenn $M \cap N = K$. Seien zum Beispiel $K = \mathbb{Q}$, $L = \mathbb{C}$, $M = \mathbb{Q}(\sqrt[3]{2})$ und $N = \mathbb{Q}(\omega\sqrt[3]{2})$. Beide $\sqrt[3]{2}$ und $\omega\sqrt[3]{2}$ sind Nullstellen des irreduziblen Polynoms $X^3 - 2 \in \mathbb{Q}[X]$, so dass beide Erweiterungen $M \mid \mathbb{Q}$ und $N \mid \mathbb{Q}$ den Grad 3 haben. Nach Proposition 3.1.7 ist dann $[M \cap N : \mathbb{Q}]$ ein Teiler von 3, also entweder 3 (d.h., $M = N$) oder 1 (d.h., $M \cap N = \mathbb{Q}$). Es gilt aber $M \neq N$, denn $M \subset \mathbb{R}$ und $\omega\sqrt[3]{2} \in \mathbb{C} \setminus \mathbb{R}$, und damit ist $M \cap N = \mathbb{Q}$. Das Kompositum MN ist der Körper

$$MN = \mathbb{Q}(\sqrt[3]{2})(\omega\sqrt[3]{2}) = \mathbb{Q}(\sqrt[3]{2})(\omega) \subset \mathbb{C}.$$

Das Minimalpolynom $\Phi_3 = X^2 + X + 1$ von ω über $\mathbb{Q}$ ist auch das Minimalpolynom von ω über $\mathbb{Q}(\sqrt[3]{2})$ (da sein Grad bereits minimal ist), so dass

$$[MN : \mathbb{Q}] = [MN : \mathbb{Q}(\sqrt[3]{2})] \cdot [\mathbb{Q}(\sqrt[3]{2}) : \mathbb{Q}] = 2 \cdot 3 = 6 < 9 = [M : \mathbb{Q}] \cdot [N : \mathbb{Q}].$$

Definition 3.1.39 (algebraische Körpererweiterung)**.** Eine Körpererweiterung $L \mid K$ heißt *algebraisch*, wenn jedes Element von L algebraisch über K ist.

Bemerkung 3.1.40. Nach Korollar 3.1.19 sind endliche Körpererweiterungen algebraisch.

Proposition 3.1.41 (Vererbung der Algebraizität)**.** *Sei $L \mid K$ eine Körpererweiterung und M ein Zwischenkörper von $L \mid K$.*

(i) *Sind beide $L \mid M$ und $M \mid K$ algebraisch, so ist auch $L \mid K$ algebraisch.*

(ii) *Ist umgekehrt $L \mid K$ algebraisch, so sind beide $L \mid M$ und $M \mid K$ algebraisch.*

Beweis. Zu (i). Sei $a \in L$ und sei $f = \sum_{i=0}^{d} a_i X^i \in M[X]$ mit $f(a) = 0$. Da die Koeffizienten a_i von f algebraisch über K sind, ist die Körpererweiterung $K(a_0, \ldots, a_d) \mid K$ endlich (nach Satz 3.1.24(i) und Proposition 3.1.7). Zudem ist a algebraisch über $K(a_0, \ldots, a_d)$, so dass $K(a_0, \ldots, a_d, a) \mid K$ endlich ist. Nach Korollar 3.1.19 ist a algebraisch über K.

Zu (ii). Dies folgt unmittelbar aus den Definitionen. □

Proposition 3.1.42. *Sei $L \mid K$ eine Körpererweiterung und sei $S \subset L$ eine Teilmenge bestehend aus über K algebraischen Elementen. Dann ist die Körpererweiterung $K(S) \mid K$ algebraisch.*

Beweis. Sei $a \in K(S)$. Es gibt dann eine endliche Teilmenge $T = \{x_1, \ldots, x_n\}$ mit $a \in K(T)$ (denn die Vereinigung der Teilkörper $K(T)$ über alle endlichen Teilmengen $T \subset S$ ist wieder ein Teilkörper von L, und damit gleich $K(S)$). Nach Satz 3.1.24(i) ist jede Erweiterung $K(x_1, \ldots, x_i) \mid K(x_1, \ldots, x_{i-1})$ endlich, und aus Proposition 3.1.7 folgt, dass $K(T) \mid K$ endlich ist. Nach Korollar 3.1.19 ist dann die Erweiterung $K(T) \mid K$ algebraisch und insbesondere ist a algebraisch über K. □

Korollar 3.1.43. *Sei $L \mid K$ eine Körpererweiterung. Dann ist die Teilmenge $A \subset L$ aller über K algebraischen Elemente ein Zwischenkörper von $L \mid K$. Insbesondere sind Summen, Differenzen, Produkte und Inverse von über K algebraischen Elementen wieder algebraisch über K.*

Beweis. Nach Proposition 3.1.42 ist $K(A) \mid K$ eine algebraische Körpererweiterung, so dass $K(A) \subset A$ und damit $K(A) = A$. □

Beispiel 3.1.44. Nach Korollar 3.1.43 bilden die algebraischen komplexen Zahlen einen Teilkörper $\bar{\mathbb{Q}} \subset \mathbb{C}$. Zudem ist der Körper $\bar{\mathbb{Q}}$ algebraisch abgeschlossen, denn: Jedes Polynom $f \in \bar{\mathbb{Q}}[X]$ vom Grad ≥ 1 besitzt eine Nullstelle $a \in \mathbb{C}$, die algebraisch über $\bar{\mathbb{Q}}$ ist. Nach Proposition 3.1.42 ist die Körpererweiterung $\bar{\mathbb{Q}}(a) \mid \bar{\mathbb{Q}}$ algebraisch, und nach Proposition 3.1.41(i) ist dann $\bar{\mathbb{Q}}(a) \mid \mathbb{Q}$ algebraisch. Insbesondere ist a algebraisch über $\mathbb{Q}$, d.h., es gilt $a \in \bar{\mathbb{Q}}$.

3.1.3 Zerfällungskörper und algebraische Abschlüsse

Definition 3.1.45 (Zerfällungskörper)**.** Sei K ein Körper und sei $f \in K[X]$ monisch vom Grad d. Ein *Zerfällungskörper* von f über K ist eine Körpererweiterung $L \mid K$ mit folgenden Eigenschaften:

- f zerfällt in seine Linearfaktoren in $L[X]$:

$$f = \prod_{i=1}^{d} (X - a_i).$$

- Es gilt $L = K(a_1, \ldots, a_d)$.

Beispiel 3.1.46.

(i) Falls $f \in K[X]$ bereits in seine Linearfaktoren zerfällt, dann ist K selbst ein Zerfällungskörper von f.

(ii) $\mathbb{C}$ ist ein Zerfällungskörper von $X^2 + 1 \in \mathbb{R}[X]$. Da $\mathbb{C}$ algebraisch abgeschlossen ist, ist es sogar ein Zerfällungskörper von jedem Polynom $f \in \mathbb{R}[X]$, das nicht in seine Linearfaktoren über $\mathbb{R}$ zerfällt.

(iii) $\mathbb{Q}(\omega)$ ist ein Zerfällungskörper von $X^3 - 1 \in \mathbb{Q}[X]$. Denn die drei Nullstellen $1, \omega, \omega^2$ von $X^3 - 1$ in $\mathbb{C}$ liegen bereits in $\mathbb{Q}(\omega)$, so dass $X^3 + 1 = (X - 1)(X - \omega)(X - \omega^2)$.

Satz 3.1.47 (Existenz und Eindeutigkeit von Zerfällungskörpern)**.** *Sei K ein Körper und sei $f \in K[X]$ monisch.*

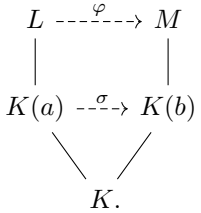
(i) *Ein Zerfällungskörper von f existiert.*

(ii) *Seien $L \mid K$ und $M \mid K$ Zerfällungskörper von f. Dann sind die Körpererweiterungen $L \mid K$ und $M \mid K$ isomorph.*

Beweis. Wir beweisen beide Aussagen durch Induktion über $\deg(f)$.

Zu (i). Falls f bereits in $K[X]$ in seine Linearfaktoren zerfällt (z.B., falls $\deg(f) \leq 1$), so ist K selbst ein Zerfällungskörper von f. Man kann also annehmen, dass ein irreduzibles Polynom g vom Grad ≥ 2 in der Primfaktorzerlegung von f in $K[X]$ vorkommt. Sei $K' = K[X]/(g)$ und sei a die Restklasse von X in K'. Dann ist K' eine Körpererweiterung von K, in der a eine Nullstelle von g und somit von f ist. Damit gibt es ein $f' \in K'[X]$ mit $f = (X-a)f'$. Es gilt insbesondere $\deg(f') = \deg(f) - 1$. Nach Induktionsvoraussetzung gibt es einen Zerfällungskörper $L \mid K'$ von f'. Im Körper L gilt also $f' = \prod_{i=1}^{d-1}(X - a_i)$ und somit $f = (X-a) \cdot \prod_{i=1}^{d-1}(X - a_i)$. Der Zwischenkörper $K(a, a_1, \ldots, a_{d-1}) \subset L$ ist damit ein Zerfällungskörper von f.

Zu (ii). Falls $\deg f \leq 1$ gilt $L = M = K$ und die Aussage ist trivial. Sei sonst $a \in L$ eine Nullstelle von f und sei $m_a \in K[X]$ ihr Minimalpolynom über K, so dass $m_a | f$. Insbesondere zerfällt m_a in seine Linearfaktoren in $M[X]$ und somit gibt es eine Nullstelle $b \in M$ von m_a. Nach Korollar 3.1.28 gibt es einen K-Algebrenhomomorphismus $\sigma\colon K(a) \hookrightarrow K(b)$ mit $\sigma(a) = b$ (der aus Dimensionsgründen ein Isomorphismus ist). Wir werden nun σ zu einem K-Algebrenisomorphismus $\varphi\colon L \xrightarrow{\sim} M$ fortsetzen:



Sei $g \in K(a)[X]$ das Polynom mit $f = (X-a)g$, und sei $g^\sigma \in K(b)[X]$ das Polynom, das man aus g durch Anwendung von σ auf die Koeffizienten erhält, so dass $f = (X-b)g^\sigma$ in $K(b)[X]$ gilt. Dann ist $L \mid K(a)$ ein Zerfällungskörper von g und $M \mid K(b)$ ein Zerfällungskörper von g^σ. Betrachtet man nun M als Körpererweiterung von $K(a)$ durch den Körperhomomorphismus $K(a) \xrightarrow{\sigma} K(b) \hookrightarrow M$, so ist $M \mid K(a)$ ein Zerfällungskörper von g. Da $\deg(g) = \deg(f) - 1$ gibt es nach Induktionsvoraussetzung einen $K(a)$-Algebrenisomorphismus $\varphi\colon L \xrightarrow{\sim} M$. Insbesondere ist φ einen K-Algebrenisomorphismus, wie gewünscht. □

Definition 3.1.48 (Galoisgruppe eines Polynoms)**.** Sei K ein Körper, sei $f \in K[X]$ monisch und sei $L \mid K$ ein Zerfällungskörper von f. Die Galoisgruppe $\mathrm{Gal}(L \mid K)$ heißt auch die *Galoisgruppe von f über K* und wird mit $\mathrm{Gal}(f \mid K)$ oder $\mathrm{Gal}(f)$ bezeichnet. Nach Satz 3.1.47(ii) ist diese Gruppe eindeutig bis auf Isomorphie durch f bestimmt.

Bemerkung 3.1.49. Nach Konstruktion 3.1.32 operiert die Galoisgruppe von f auf der Nullstellenmenge von f im Zerfällungskörper L: Ist $f = \prod_{i=1}^{d}(X - a_i)$ in L, so gibt es eine kanonische Gruppenoperation

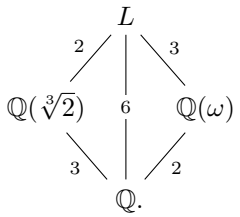
$$\begin{aligned} \mathrm{Gal}(f \mid K) \times \{a_1, \ldots, a_d\} &\to \{a_1, \ldots, a_d\}, \\ (\sigma, a) &\mapsto \sigma(a). \end{aligned}$$

Da $L = K(a_1, \ldots, a_d)$ ist jedes $\sigma \in \mathrm{Gal}(f \mid K)$ eindeutig durch die Werte $\sigma(a_1), \ldots, \sigma(a_d)$ bestimmt, d.h., diese Operation ist *treu* und identifiziert $\mathrm{Gal}(f \mid K)$ mit einer Untergruppe der symmetrischen Gruppe $S_{\{a_1,\ldots,a_d\}}$. Im Allgemeinen ist diese Operation weder frei noch transitiv.

Beispiel 3.1.50. Wir bestimmen die Galoisgruppe des Polynoms $X^3 - 2$ über $\mathbb{Q}$. Dieses Polynom hat die Nullstellenmenge $N = \{\sqrt[3]{2}, \omega\sqrt[3]{2}, \omega^2\sqrt[3]{2}\}$ in $\mathbb{C}$, so dass $L := \mathbb{Q}(N) \subset \mathbb{C}$ ein Zerfällungskörper von $X^3 - 2$ ist. Der Körper L enthält die dritte Einheitswurzel ω, denn:

$$\omega = \frac{1}{2}\big(\sqrt[3]{2} \cdot (\omega^2\sqrt[3]{2})^2\big) \in L.$$

Also gilt $L = \mathbb{Q}(\omega, \sqrt[3]{2})$. Nach Beispiel 3.1.26(ii,iii) gelten $[\mathbb{Q}(\sqrt[3]{2}) : \mathbb{Q}] = 3$ und $[\mathbb{Q}(\omega) : \mathbb{Q}] = 2$. Nach Proposition 3.1.37(ii) hat das Kompositum $L = \mathbb{Q}(\sqrt[3]{2})\mathbb{Q}(\omega)$ den Grad 6 über $\mathbb{Q}$ (siehe auch Beispiel 3.1.38):



Behauptung. Jeder Automorphismus $\sigma \in \mathrm{Gal}(L \mid K)$ lässt sich zu einem Automorphismus von $\mathbb{Q}(\omega) \mid \mathbb{Q}$ einschränken.

Denn $\sigma(\omega)$ muss wieder eine dritte Wurzel von 1 sein, d.h., $\sigma(\omega) \in \{1, \omega, \omega^2\} \subset \mathbb{Q}(\omega)$, so dass $\sigma(\mathbb{Q}(\omega)) \subset \mathbb{Q}(\omega)$. Dies gilt auch für den Umkehrmorphismus σ^{-1}, was die Behauptung liefert. Damit gibt es einen wohldefinierten Gruppenhomomorphismus

$$r\colon \mathrm{Gal}(L \mid \mathbb{Q}) \to \mathrm{Gal}(\mathbb{Q}(\omega) \mid \mathbb{Q}), \quad \sigma \mapsto \sigma|_{\mathbb{Q}(\omega)}.$$

Der Kern von r ist nach Definition $\mathrm{Gal}(L \mid \mathbb{Q}(\omega)) < \mathrm{Gal}(L \mid \mathbb{Q})$. Nach Beispiel 3.1.36 hat $\mathrm{Gal}(\mathbb{Q}(\omega) \mid \mathbb{Q})$ nur zwei Elemente, die Identität und die komplexe Konjugation. Die komplexe Konjugation $z \mapsto \bar{z}$ definiert auch einen Automorphismus von $L \mid \mathbb{Q}$, so dass r surjektiv ist. Damit erhalten wir eine (spaltende) Gruppenerweiterung

$$\{e\} \to \mathrm{Gal}(L \mid \mathbb{Q}(\omega)) \to \mathrm{Gal}(L \mid \mathbb{Q}) \xrightarrow{r} \mathrm{Gal}(\mathbb{Q}(\omega) \mid \mathbb{Q}) \to \{e\}.$$

Auf der anderen Seite kann man $\mathrm{Gal}(L \mid \mathbb{Q})$ mit einer Untergruppe von $S_N \cong S_3$ identifizieren (Bemerkung 3.1.49). Nach dem Satz von Lagrange ist $|\mathrm{Gal}(L \mid \mathbb{Q})|$ ein Teiler von $|S_3| = 6$ sowie ein Vielfaches von $|\mathrm{Gal}(\mathbb{Q}(\omega) \mid \mathbb{Q})| = 2$. Es gibt also nur zwei Möglichkeiten: Entweder $\mathrm{Gal}(L \mid \mathbb{Q}) \cong C_2$ (und r ist ein Isomorphismus), oder $\mathrm{Gal}(L \mid \mathbb{Q}) \cong S_3$. Um die erste Möglichkeit auszuschließen, berechnen wir $\mathrm{Gal}(L \mid \mathbb{Q}(\omega))$. Das Polynom $X^3 - 2$ ist das Minimalpolynom von $\sqrt[3]{2}$ über $\mathbb{Q}(\omega)$, da sein Grad gleich $[L : \mathbb{Q}(\omega)] = 3$ ist. Da dieses Polynom drei Nullstellen in L hat, hat die Galoisgruppe $\mathrm{Gal}(L \mid \mathbb{Q}(\omega))$ genau drei Elemente nach Korollar 3.1.34(ii). Es gilt genauer $\mathrm{Gal}(L \mid \mathbb{Q}(\omega)) = \{\mathrm{id}, \sigma, \sigma^2\}$, wobei σ die Nullstellenmenge N auf zyklische Weise permutiert: $\sigma(\omega^i\sqrt[3]{2}) = \omega^{i+1}\sqrt[3]{2}$. Also gilt $\mathrm{Gal}(L \mid \mathbb{Q}) \cong S_3$, d.h., jede Permutation der Nullstellenmenge N lässt sich zu einem Automorphismus von $L \mid \mathbb{Q}$ fortsetzen. Die folgende Tabelle fasst diese Berechnung zusammen (dabei ist c die komplexe Konugation):

$\mathrm{Gal}(X^3 - 2 \mid \mathbb{Q})$	Wert auf ω	Wert auf $\sqrt[3]{2}$
id	ω	$\sqrt[3]{2}$
σ	ω	$\omega\sqrt[3]{2}$
σ^2	ω	$\omega^2\sqrt[3]{2}$
c	ω^2	$\sqrt[3]{2}$
$c \circ \sigma$	ω^2	$\omega^2\sqrt[3]{2}$
$c \circ \sigma^2$	ω^2	$\omega\sqrt[3]{2}$

Definition 3.1.51 (algebraisch abgeschlossen, algebraischer Abschluss)**.** Sei K ein Körper.

- K heißt *algebraisch abgeschlossen*, wenn jedes Polynom $f \in K[X]$ vom Grad ≥ 1 eine Nullstelle in K besitzt (und somit nach Proposition 2.1.34 in seine Linearfaktoren zerfällt).
- Ein *algebraischer Abschluss* von K ist eine algebraische Körpererweiterung $L \mid K$, wobei L algebraisch abgeschlossen ist.

Beispiel 3.1.52.

(i) $\mathbb{C}$ ist bekanntlich algebraisch abgeschlossen und damit ein algebraischer Abschluss von $\mathbb{R}$.

(ii) $\bar{\mathbb{Q}}$ ist ein algebraischer Abschluss von $\mathbb{Q}$ (siehe Beispiel 3.1.44).

(iii) Sei K ein endlicher Körper. Dann ist K nicht algebraisch abgeschlossen, denn das Polynom
$$f = \prod_{a \in K} (X - a) + 1$$
hat keine Nullstellen in K.

(iv) Sei K ein beliebiger Körper. Dann ist der Körper $K(T)$ der rationalen Funktionen über K nicht algebraisch abgeschlossen. Zum Beispiel hat das Polynom $X^2 - T \in K(T)[X]$ keine Nullstellen in $K(T)$ (nach dem Eisensteinschen Kriterium).

Proposition 3.1.53. *Sei $\sigma\colon K \to M$ ein Körperhomomorphismus, wobei M algebraisch abgeschlossen ist, und sei $L \mid K$ eine beliebige algebraische Körpererweiterung. Dann gibt es einen Körperhomomorphismus $\hat{\sigma}\colon L \to M$ mit $\hat{\sigma}|_K = \sigma$:*

$$\begin{array}{ccc} K & \xrightarrow{\sigma} & M. \\ \big\downarrow & \nearrow_{\exists \hat{\sigma}} & \\ L & & \end{array}$$

Beweis. Wir verwenden das Zornsche Lemma (Satz LA.1.4.22). Dazu betrachten wir die Menge
$$\mathfrak{X} = \left\{ (Z, \varphi) \;\middle|\; \begin{array}{c} Z \text{ ist ein Zwischenkörper von } L \mid K \text{ und } \varphi\colon Z \to M \\ \text{ist ein Körperhomomorphismus mit } \varphi|_K = \sigma \end{array} \right\}$$
mit der partiellen Ordnung
$$(Z, \varphi) \prec (Z', \varphi') \quad \Longleftrightarrow \quad Z \subset Z' \text{ und } \varphi = \varphi'|_Z.$$
Die Menge $\mathfrak{X}$ enthält das Paar (K, σ). Sei nun $\mathcal{K} \subset \mathfrak{X}$ eine Kette. Ist $\mathcal{K}$ leer, so ist (K, σ) eine obere Schranke von $\mathcal{K}$. Sonst definiert man
$$Z_\infty = \bigcup_{(Z,\varphi) \in \mathcal{K}} Z \subset L \quad \text{und} \quad \varphi_\infty\colon Z_\infty \to L,$$
so dass für alle $(Z, \varphi) \in \mathcal{K}$ gilt $\varphi_\infty|_Z = \varphi$. Da $\mathcal{K}$ eine Kette ist, ist Z_∞ wieder ein Zwischenkörper von $L \mid K$ (vgl. Proposition 2.2.17), und es gilt $(Z_\infty, \varphi_\infty) \in \mathfrak{X}$. Also ist $(Z_\infty, \varphi_\infty)$ eine obere Schranke von $\mathcal{K}$.

Nach dem Zornschen Lemma besitzt $\mathfrak{X}$ ein maximales Element $(Z_{\max}, \varphi_{\max})$. Es bleibt zu zeigen, dass $Z_{\max} = L$. Sei also $a \in L$ beliebig und sei $m_a \in Z_{\max}[X]$ sein Minimalpolynom über $Z_{\max}$. Nach Voraussetzung ist a algebraisch über K und insbesondere über $Z_{\max}$, so dass $\deg(m_a) \geq 1$. Wir betrachten M als $Z_{\max}$-Algebra durch den Körperhomomorphismus $\varphi_{\max}\colon Z_{\max} \hookrightarrow M$. Da M algebraisch abgeschlossen ist, hat m_a eine Nullstelle $b \in M$. Nach Korollar 3.1.28 gibt es einen $Z_{\max}$-Algebrenhomomorphismus $\varphi'\colon Z_{\max}(a) \to M$ mit $\varphi'(a) = b$, der insbesondere eine Fortsetzung von $\varphi_{\max}$ auf $Z_{\max}(a)$ ist. Also gilt $(Z_{\max}, \varphi_{\max}) \prec (Z_{\max}(a), \varphi')$. Aus der Maximalität von $(Z_{\max}, \varphi_{\max})$ folgt nun, dass $Z_{\max}(a) = Z_{\max}$, d.h., $a \in Z_{\max}$. □

Lemma 3.1.54. *Sei $L \mid K$ eine algebraische Körpererweiterung. Dann ist jeder Endomorphismus von $L \mid K$ ein Isomorphismus.*

Beweis. Sei $\sigma\colon L \to L$ ein Körperhomomorphismus mit $\sigma|_K = \mathrm{id}_K$. Nach Proposition 2.1.14 ist σ injektiv, und es bleibt zu zeigen, dass σ surjektiv ist. Sei $a \in L$ mit Minimalpolynom $m_a \in K[X]$. Da $L \mid K$ algebraisch ist, ist a algebraisch über K, so dass m_a irreduzibel ist (Satz 3.1.24(i)). Der Morphismus σ schränkt sich zu einer injektiven Abbildung

$$\sigma'\colon N_L(m_a) \hookrightarrow N_L(m_a)$$

ein. Da die Nullstellenmenge $N_L(m_a)$ endlich ist, muss σ' bijektiv sein. Insbesondere liegt a im Bild von σ. □

Satz 3.1.55 (Existenz und Eindeutigkeit algebraischer Abschlüsse)**.** *Sei K ein Körper.*

(i) *Ein algebraischer Abschluss von K existiert.*

(ii) *Seien $L \mid K$ und $M \mid K$ algebraische Abschlüsse von K. Dann sind die Körpererweiterungen $L \mid K$ und $M \mid K$ isomorph.*

Beweis. Zu (i). Sei $K[X]_{\geq 1} \subset K[X]$ die Teilmenge der Polynome vom Grad ≥ 1. Wir bilden zunächst eine algebraische Körpererweiterung $C(K)|K$ mit folgender Eigenschaft: Jedes Polynom $f \in K[X]_{\geq 1}$ hat eine Nullstelle in $C(K)$. Dazu betrachten wir den Polynomring in mehreren Variablen $R = K[X_f \mid f \in K[X]_{\geq 1}]$ (siehe Bemerkung 2.1.22) und das Ideal

$$I = (\{f(X_f) \mid f \in K[X]_{\geq 1}\}) \subset R.$$

Behauptung. Es gilt $I \neq R$.

Angenommen, es wäre $I = R$, d.h., $1 \in I$. Dann gäbe es eine endliche Teilmenge $E \subset K[X]_{\geq 1}$ und eine Familie $(g_f)_{f\in E} \in R^E$ mit

$$1 = \sum_{f\in E} g_f f(X_f).$$

Man kann aber eine Körpererweiterung $K' \mid K$ bilden, in der jedes $f \in E$ eine Nullstelle a_f besitzt (zum Beispiel durch endlich viele Anwendungen von Satz 3.1.47(i)). Sei $\varepsilon\colon R \to K'$ der Einsetzungshomomorphismus mit

$$\varepsilon(X_f) = \begin{cases} a_f, & \text{falls } f \in E, \\ 0, & \text{sonst.} \end{cases}$$

Wendet man ε auf die obige Gleichheit an, so erreichen wir den Widerspruch

$$1 = \sum_{f\in E} \varepsilon(g_f) f(a_f) = 0.$$

Nach der Behauptung und Proposition 2.2.17 gibt es ein maximales Ideal $\mathfrak{m} \subset R$ mit $I \subset \mathfrak{m}$. Dann ist $C(K) := R/\mathfrak{m}$ eine Körpererweiterung von K mit der gewünschten Eigenschaft: Die Restklasse $[X_f] \in C(K)$ ist eine Nullstelle von f. Zudem gilt nach Konstruktion $C(K) = K(\{[X_f] \mid f \in K[X]_{\geq 1}\})$, so dass die Erweiterung $C(K) \mid K$ algebraisch ist (nach Proposition 3.1.42).

Jetzt iterieren wir diese Konstruktion, um einen Turm von Körpererweiterungen zu erhalten:

$$K \subset C(K) \subset C^2(K) \subset C^3(K) \subset \cdots.$$

Sei $L = \bigcup_{n\in\mathbb{N}} C^n(K)$. Man definiert auf naheliegende Weise die Verknüpfungen $+$ und $\cdot$ auf L und rechnet leicht nach, dass L wieder ein Körper ist. Nach Proposition 3.1.41(i) ist jede Erweiterung $C^n(K) \mid K$ algebraisch, so dass jedes Element von L algebraisch über K ist.

Schließlich ist L algebraisch abgeschlossen, denn: Jedes Polynom $f \in L[X]$ vom Grad ≥ 1 hat nur endlich viele Nicht-Null-Koeffizienten, die damit in einen Teilkörper $C^n(K) \subset L$ liegen. Dann hat f eine Nullstelle in $C^{n+1}(K) \subset L$.

Zu (ii). Nach Proposition 3.1.53 existieren Körperhomomorphismen $\sigma\colon L \to M$ und $\tau\colon M \to L$ mit $\sigma|_K = \mathrm{id}_K$ und $\tau|_K = \mathrm{id}_K$. Nach Lemma 3.1.54 sind beide Kompositionen $\sigma \circ \tau$ und $\tau \circ \sigma$ Isomorphismen. Daraus folgt, dass σ surjektiv sowie injektiv ist. □

Bemerkung 3.1.56. Obwohl je zwei algebraische Abschlüsse von K zueinander isomorph sind, gibt es im Allgemeinen *mehrere* Isomorphismen zwischen denen und keine kanonische Wahl davon.

3.1.4 Klassifikation der endlichen Körper

Definition 3.1.57 (Ableitung von Polynomen)**.** Sei R ein kommutativer Ring und sei $f = \sum_{i\in\mathbb{N}} a_i X^i$ ein Polynom über R. Die *Ableitung* Df von f is das Polynom

$$Df = \sum_{i\in\mathbb{N}_{\geq 1}} i a_i X^{i-1} \in R[X].$$

Bemerkung 3.1.58. Die Ableitungsabbildung $D\colon R[X] \to R[X]$ ist R-linear aber kein Ringhomomorphismus. Stattdessen erfüllt D die *Leibniz-Regel*

$$D(fg) = D(f)g + fD(g),$$

wie man leicht nachrechnen kann.

Zur Erinnerung ist $a \in R$ genau dann eine Nullstelle von $f \in R[X]$, wenn f durch $X - a$ teilbar ist (Proposition 2.1.34).

Definition 3.1.59 (mehrfache Nullstelle)**.** Sei R ein kommutativer Ring und $f \in R[X]$ ein Polynom. Ein Element $a \in R$ heißt *mehrfache Nullstelle* von f, wenn f durch $(X - a)^2$ teilbar ist.

Proposition 3.1.60 (Ableitungskriterium für mehrfache Nullstellen)**.** *Sei R ein kommutativer Ring, $f \in R[X]$ ein Polynom und $a \in R$ eine Nullstelle von f. Dann sind die folgenden Aussagen äquivalent:*

(i) *a ist eine mehrfache Nullstelle von f.*

(ii) *a ist eine Nullstelle von Df.*

Beweis. Zu (i) ⇒ (ii). Sei $a \in R$ eine mehrfache Nullstelle von f, so dass $f = (X-a)^2 g$ mit einem $g \in R[X]$. Mit der Leibniz-Regel (Bemerkung 3.1.58) erhalten wir

$$Df = 2(X - a)g + (X - a)^2 Dg.$$

Insbesondere ist a eine Nullstelle von Df.

Zu (ii) ⇒ (i). Sei $a \in R$ mit $f(a) = 0$ und $(Df)(a) = 0$. Es gibt dann ein $g \in R[X]$ mit $f = (X - a)g$. Aus der Leibniz-Regel folgt

$$Df = g + (X - a)Dg.$$

Da beide Df und $(X-a)Dg$ durch $X-a$ teilbar sind, ist auch g durch $X-a$ teilbar. Damit ist f durch $(X - a)^2$ teilbar. □

Definition 3.1.61 (Frobenius-Endomorphismus)**.** Sei p eine Primzahl und sei A eine kommutative $\mathbb{F}_p$-Algebra (z.B., ein Körper der Primcharakteristik p). Die Abbildung

$$\varphi\colon A \to A, \quad x \mapsto x^p,$$

heißt der *Frobenius-Endomorphismus* von A. Nach dem binomischen Lehrsatz ist φ ein Ringhomomorphismus.

Wir wissen bereits, dass die Mächtigkeit eines endlichen Körpers K der Charakteristik p eine Potenz von p sein muss, da K ein $\mathbb{F}_p$-Vektorraum ist (Bemerkung 3.1.6).

Satz 3.1.62 (Klassifikation der endlichen Körper)**.** *Sei p eine Primzahl und sei $n \in \mathbb{N}_{\geq 1}$. Dann gibt es bis auf Isomorphie genau einen Körper mit p^n Elementen. Dieser Körper ist ein Zerfällungskörper des Polynoms $X^{p^n} - X$ über seinem Primkörper.*

Beweis. Zur Eindeutigkeit. Sei K ein endlicher Körper mit p^n Elementen. Sein Primkörper ist dann zu $\mathbb{F}_p$ isomorph. Ohne Einschränkung (indem man K durch einen isomorphen Körper ersetzt) kann man annehmen, dass K eine Körpererweiterung von $\mathbb{F}_p$ ist. Die Einheitengruppe $K^\times$ hat $p^n - 1$ Elementen. Nach dem Satz von Lagrange gilt dann $x^{p^n-1} = 1$ für alle $x \in K^\times$, und damit $x^{p^n} = x$ für alle $x \in K$. Also sind alle Elemente von K Nullstellen des Polynoms $X^{p^n} - X$. Da dieses Polynom höchstens p^n Nullstellen hat (Korollar 2.1.66) ist $K \mid \mathbb{F}_p$ ein Zerfällungskörper von $X^{p^n} - X$. Nach Satz 3.1.47(ii) ist K eindeutig bis auf Isomorphie dadurch bestimmt.

Zur Existenz. Sei $K \mid \mathbb{F}_p$ ein Zerfällungskörper von $X^{p^n} - X$ (Satz 3.1.47(i)). Man muss zeigen, dass $|K| = p^n$. Sei $N \subset K$ die Nullstellenmenge von $X^{p^n} - X$:

$$N = \{x \in K \mid x^{p^n} = x\} = \{x \in K \mid \varphi^n(x) = x\},$$

wobei $\varphi\colon K \to K$ der Frobenius-Endomorphismus ist. Da φ^n ein Körperhomomorphismus ist, kann man leicht nachprüfen, dass N ein Teilkörper von K ist. Nach Definition eines Zerfällungskörpers gilt dann $N = K$. Aus Korollar 2.1.66 folgt nun $|K| = |N| \leq p^n$. Es bleibt zu zeigen, dass das Polynom $X^{p^n} - X$ keine mehrfachen Nullstellen in K besitzt. Dies folgt aus dem Ableitungskriterium 3.1.60, denn die Ableitung

$$D(X^{p^n} - X) = p^n X^{p^n-1} - 1 = -1$$

hat keine Nullstellen. □

Proposition 3.1.63 (Erweiterungen zwischen endlichen Körpern und ihre Galoisgruppen)**.** *Sei p eine Primzahl, sei $n \in \mathbb{N}_{\geq 1}$ und sei K ein endlicher Körper mit p^n Elementen.*

(i) *Für jedes $d \in \mathbb{N}_{\geq 1}$ gibt es bis auf Isomorphie genau eine Körpererweiterung $L \mid K$ vom Grad d. Zudem gibt es einen Gruppenisomorphismus*

$$\begin{aligned} \mathbb{Z}/d\mathbb{Z} &\xrightarrow{\sim} \mathrm{Gal}(L \mid K), \\ [k] &\mapsto \varphi^{nk}. \end{aligned}$$

(ii) *Für jeden Teiler m von n ist die Nullstellenmenge $N_K(X^{p^m} - X)$ ein Teilkörper von K mit p^m Elementen. Dies definiert eine Bijektion*

$$\begin{aligned} \{\textit{Teiler von } n\} &\xrightarrow{\sim} \{\textit{Teilkörper von } K\}, \\ m &\mapsto N_K(X^{p^m} - X). \end{aligned}$$

Beweis. Zu (i). Sei $r = nd$. Jede Körpererweiterung $L \mid K$ vom Grad d hat $(p^n)^d = p^r$ Elemente und ist nach Satz 3.1.62 ein Zerfällungskörper von $X^{p^r} - X$ über seinem Primkörper, und insbesondere über K. Nach Satz 3.1.47(ii) ist eine solche Erweiterung eindeutig bis auf Isomorphie bestimmt. Zur Existenz sei nun $L \mid K$ ein Zerfällungskörper von $X^{p^r} - X$. Jedes Element $x \in K$ erfüllt $x^{p^n} = x$ nach dem Satz von Lagrange (angewendet auf die Gruppe $K^\times$) und damit auch $x^{p^r} = x^{(p^n)^d} = x$. Also ist L ein Zerfällungskörper von $X^{p^r} - X$ über seinem Primkörper. Nach Satz 3.1.62 hat dann L genau p^r Elemente, so dass $[L : K] = d$.

Da $L^\times$ zyklisch ist (Korollar 2.2.54) ist die Erweiterung $L \mid K$ einfach, d.h., es gibt ein $a \in L$ mit $L = K(a)$. Aus Korollar 3.1.34(iii) folgt

$$|\mathrm{Gal}(L \mid K)| \leq [L : K] = d.$$

Der iterierte Frobenius-Endomorphismus $\varphi^n\colon L \to L$ ist injektiv und damit bijektiv, und seine Einschränkung auf K ist gleich der Identität (da $x^{p^n} = x$ für alle $x \in K$). Also gilt $\varphi^n \in \mathrm{Gal}(L \mid K)$. Es bleibt zu zeigen, dass die Ordnung von φ^n mindestens d ist. Die Gleichheit $(\varphi^n)^k = \mathrm{id}$ bedeutet, dass jedes Element von L eine Nullstelle von $X^{p^{nk}} - X$ ist. Nach Korollar 2.1.66 ist dies nur möglich, wenn

$$p^r = |L| \leq \deg(X^{p^{nk}} - X) = p^{nk},$$

d.h., wenn $d \leq k$.

Zu (ii). Ist K' ein Teilkörper von K, so gilt $|K'| = p^m$ mit einem $m \leq n$. Zudem ist K ein K'-Vektorraum, so dass $|K|$ eine Potenz von $|K'|$ sein muss, d.h., m muss ein Teiler von n sein. Sei nun m ein Teiler von n. Nach Satz 3.1.62 ist K ein Zerfällungskörper von $X^{p^n} - X$ über seinem Primkörper. Ein Teilkörper K' von K mit p^m Elementen muss ebenso von den Nullstellen von $X^{p^m} - X$ in K erzeugt wird, und ist dadurch eindeutig bestimmt. Zudem muss jedes Element von K' eine Nullstelle von $X^{p^m} - X$ sein (nach dem Satz von Lagrange), und somit besteht K' genau aus diesen Nullstellen. Um die Existenz eines solchen Teilkörpers zu beweisen, sei L' ein Körper mit p^m Elementen. Nach (i) gibt es eine Körpererweiterung $L \mid L'$ vom Grad $d = n/m$, so dass $|L| = p^n$. Nach der Eindeutigkeitsaussage im Satz 3.1.62 gibt es einen Körperisomorphismus $\sigma\colon L \xrightarrow{\sim} K$, so dass $\sigma(L')$ ein Teilkörper von K mit p^m Elementen ist. □

Notation 3.1.64. Sei q eine Primpotenz (d.h., $q = p^n$ mit einer Primzahl p und einem $n \in \mathbb{N}_{\geq 1}$). Man bezeichnet mit $\mathbb{F}_q$ einen endlichen Körper mit q Elementen.

Bemerkung 3.1.65 (algebraischer Abschluss endlicher Körper)**.** Sei p eine Primzahl. Nach Proposition 3.1.63(i) kann man einen Turm von endlichen Körpern

$$\mathbb{F}_p \subset \mathbb{F}_{p^{2!}} \subset \mathbb{F}_{p^{3!}} \subset \cdots$$

konstruieren. Die Vereinigung

$$\bar{\mathbb{F}}_p = \bigcup_{n \geq 1} \mathbb{F}_{p^{n!}}$$

ist dann eine unendliche algebraische Körpererweiterung von $\mathbb{F}_p$. Aus dieser Proposition folgt außerdem:

(i) Für jedes $n \in \mathbb{N}_{\geq 1}$ enthält $\bar{\mathbb{F}}_p$ genau einen Teilkörper mit p^n Elementen, der aus den Nullstellen von $X^{p^n} - X$ besteht.

(ii) $\bar{\mathbb{F}}_p$ ist algebraisch abgeschlossen und somit ein algebraischer Abschluss von $\mathbb{F}_p$.

3.2 Galoiserweiterungen

Sei $L|K$ eine endliche Körpererweiterung. Wenn $L \mid K$ einfach ist, haben wir im Korollar 3.1.34(iii) gezeigt, dass

$$|\mathrm{Gal}(L \mid K)| \leq [L : K].$$

Dies gilt eigentlich für beliebige endliche Körpererweiterungen (siehe Korollar 3.2.29). Manchmal gilt die Gleichheit (Beispiel 3.1.36) und manchmal nicht (Beispiel 3.1.35).

Der Einfachheit halber betrachten wir nun den einfachen Fall $L = K(a)$. Nach Korollar 3.1.34(iii) ist die Mächtigkeit der Galoisgruppe gleich der Anzahl der Nullstellen von m_a in L, während der Grad von L über K gleich dem Grad von m_a ist. Im Allgemeinen gibt es zwei Situationen, in denen die Anzahl der Nullstellen eines Polynoms f kleiner als sein Grad ist:

(i) f zerfällt nicht in seine Linearfaktoren;

(ii) f hat mehrfache Nullstellen.

In diesem Abschnitt untersuchen wir geeignete Bedingungen, die diese Probleme bei Minimalpolynomen ausschließen (dabei kann das zweite Problem nur in der positiven Charakteristik vorkommen). Dies führt zu den wichtigen Begriffen von *normalen* und *separablen* Körpererweiterungen. Eine algebraische Körpererweiterung, die gleichzeitig normal und separabel ist, heißt *Galoiserweiterung*. Bei einer endlichen Galoiserweiterung $L \mid K$ gilt dann $|\mathrm{Gal}(L \mid K)| = [L : K]$. Der Hauptsatz der Galoistheorie beschreibt eine Bijektion zwischen der Menge aller Untergruppen von $\mathrm{Gal}(L \mid K)$ und der Menge aller Zwischenkörper von $L \mid K$. Dadurch kann man die Struktur von Körpererweiterungen (oder konkreter gesagt, von Nullstellenmengen von Polynomen in einer Variablen) mithilfe der Gruppentheorie verstehen.

3.2.1 Normale Körpererweiterungen

Proposition 3.2.1 (Charakterisierung der Normalität)**.** *Sei $L \mid K$ eine algebraische Körpererweiterung. Die folgenden Aussagen sind äquivalent:*

(i) *Das Minimalpolynom über K von jedem $a \in L$ zerfällt in seine Linearfaktoren in $L[X]$.*

(ii) *Es gibt eine Teilmenge $S \subset L$ mit $L = K(S)$, so dass das Minimalpolynom über K von jedem $a \in S$ in seine Linearfaktoren in $L[X]$ zerfällt.*

(iii) *Für jede Körpererweiterung $M \mid L$ und jeden K-Algebrenhomomorphismus $\sigma\colon L \to M$ gilt $\sigma(L) \subset L$.*

(iv) *Die Aussage* (iii) *gilt für ein M, das algebraisch abgeschlossen ist.*

Beweis. Die Implikationen (i) $\Rightarrow$ (ii) und (iii) $\Rightarrow$ (iv) sind klar.

Zu (ii) $\Rightarrow$ (iii). Für jedes $a \in S$ ist $\sigma(a)$ eine Nullstelle von $m_a \in K[X]$. Da m_a über L in seine Linearfaktoren zerfällt, liegen alle Nullstellen von m_a in M bereits in L. Insbesondere gilt $\sigma(S) \subset L$ und daher $\sigma(L) = \sigma(K(S)) \subset L$.

Zu (iv) $\Rightarrow$ (i). Sei $a \in L$ mit Minimalpolynom $m_a \in K[X]$. Da M algebraisch abgeschlossen ist, zerfällt m_a in seine Linearfaktoren in $M[X]$. Es genügt also zu zeigen, dass alle Nullstellen von m_a in M bereits in L liegen. Sei $b \in M$ eine Nullstelle von m_a. Nach Korollar 3.1.28 gibt es einen K-Algebrenhomomorphismus $\tau\colon K(a) \to M$ mit $\tau(a) = b$. Nach Proposition 3.1.53 kann man τ zu einem K-Algebrenhomomorphismus $\sigma\colon L \to M$ fortsetzen. Nach Voraussetzung gilt dann $\sigma(L) \subset L$. Insbesondere gilt $b = \sigma(a) \in L$, wie gewünscht. □

Definition 3.2.2 (normale Körpererweiterung)**.** Eine algebraische Körpererweiterung $L \mid K$ heißt *normal*, wenn die äquivalenten Bedingungen der Proposition 3.2.1 erfüllt sind.

Beispiel 3.2.3. Sei $a \in \mathbb{C}$ algebraisch über $\mathbb{Q}$. Die Körpererweiterung $\mathbb{Q}(a) \mid \mathbb{Q}$ ist genau dann normal, wenn alle zu a konjugierten Elemente von $\mathbb{C}$ (d.h., alle Nullstellen von m_a) bereits in $\mathbb{Q}(a)$ liegen. Zum Beispiel:

(i) $\mathbb{Q}(\sqrt{2}) \mid \mathbb{Q}$ und $\mathbb{Q}(\omega) \mid \mathbb{Q}$ sind normal, denn $\pm\sqrt{2} \in \mathbb{Q}(\sqrt{2})$ und $\omega, \omega^2 \in \mathbb{Q}(\omega)$.

(ii) Allgemeiner ist jede Körpererweiterung vom Grad 2 normal (denn jedes monische Polynom zweiten Grades, das eine Nullstelle besitzt, zerfällt in seine Linearfaktoren).

(iii) $\mathbb{Q}(\sqrt[3]{2}) \mid \mathbb{Q}$ ist *nicht* normal, denn $\omega\sqrt[3]{2} \notin \mathbb{Q}(\sqrt[3]{2})$.

(iv) $\mathbb{Q}(\sqrt{2}+\sqrt{3}) \mid \mathbb{Q}$ ist normal, denn $\pm\sqrt{2} \pm \sqrt{3} \in \mathbb{Q}(\sqrt{2}+\sqrt{3})$ (siehe Beispiel 3.1.30(iii)).

Beispiel 3.2.4. Ist $L \mid K$ ein Zerfällungskörper von einem monischen Polynom $f \in K[X]$, so ist $L \mid K$ normal. Denn es gilt $L = K(a_1, \ldots, a_d)$, wobei $f = \prod_{i=1}^{d}(X - a_i)$ in $L[X]$, und jedes Minimalpolynom m_{a_i} teilt f und damit zerfällt in seine Linearfaktoren in $L[X]$. Zum Beispiel:

(i) $\mathbb{Q}(\sqrt[3]{2}, \omega) \mid \mathbb{Q}$ ist ein Zerfällungskörper von $X^3 - 2$ (Beispiel 3.1.50) und somit normal.

(ii) Jede Erweiterung $L \mid K$ zwischen endlichen Körpern ist normal, denn L ist ein Zerfällungskörper über seinem Primkörper und insbesondere auch über K (Satz 3.1.62).

Bemerkung 3.2.5. Sind $L \mid K$ und $M \mid L$ normale Körpererweiterungen, so ist $M \mid K$ *nicht unbedingt* normal. Zum Beispiel sind beide Erweiterungen $\mathbb{Q}(\sqrt{2}) \mid \mathbb{Q}$ und $\mathbb{Q}(\sqrt[4]{2}) \mid \mathbb{Q}(\sqrt{2})$ normal (da sie den Grad 2 haben, siehe Beispiel 3.2.3(ii)), aber $\mathbb{Q}(\sqrt[4]{2}) \mid \mathbb{Q}$ ist nicht normal (da die Nullstelle $i\sqrt[4]{2}$ von $X^4 - 2$ nicht in $\mathbb{Q}(\sqrt[4]{2})$ liegt). Durch die Galoistheorie hängt diese Bemerkung mit Bemerkung 1.1.64 zusammen.

Proposition 3.2.6. *Sei $L \mid K$ eine normale Körpererweiterung und sei M ein Zwischenkörper von $L \mid K$. Jeder Morphismus von $M \mid K$ nach $L \mid K$ lässt sich zu einem Automorphismus von $L \mid K$ fortsetzen.*

Beweis. Sei $\sigma\colon M \to L$ ein K-Algebrenhomomorphismus und sei $\bar{L}$ ein algebraischer Abschluss von L. Nach Proposition 3.1.53 gibt es eine Fortsetzung $\hat{\sigma}\colon L \to \bar{L}$ von σ. Da $L \mid K$ normal ist, gilt $\hat{\sigma}(L) \subset L$. Also ist $\hat{\sigma}$ ein Endomorphismus von $L \mid K$ mit $\hat{\sigma}|_M = \sigma$. Nach Lemma 3.1.54 ist $\hat{\sigma}$ automatisch ein Automorphismus. □

Bemerkung 3.2.7 (normale Hülle)**.** Jede algebraische Körpererweiterung $L \mid K$ besitzt eine *normale Hülle* $M \mid L$, d.h., eine minimale Erweiterung von L, die eine normale Erweiterung von K ist: Man wählt zum Beispiel einen algebraischen Abschluss $\bar{K} \mid K$ und setzt $M = K(S) \subset \bar{K}$, wobei $S \subset \bar{K}$ die Menge aller Nullstellen aller Minimalpolynome über K von Elementen von L. Eine normale Hülle von $L \mid K$ ist eindeutig bis auf Isomorphie bestimmt (nach der Eindeutigkeit algebraischer Abschlüsse und Proposition 3.1.53). Zum Beispiel ist $\mathbb{Q}(\sqrt[3]{2}, \omega)$ eine normale Hülle von $\mathbb{Q}(\sqrt[3]{2})$.

3.2.2 Separable Körpererweiterungen

Proposition 3.2.8 (Charakterisierung der Separabilität)**.** *Sei K ein Körper und $f \in K[X]$ ein Polynom über K. Die folgenden Aussagen sind äquivalent:*

(i) *Für jede Körpererweiterung $L \mid K$ hat f keine mehrfachen Nullstellen in L.*

(ii) *Die Aussage* (i) *gilt für ein L, über dem f in seine Linearfaktoren zerfällt.*

(iii) *Es gilt* $\mathrm{ggT}(f, Df) = 1$ *in* $K[X]$.

Beweis. Die Implikation (i) ⇒ (ii) ist offensichtlich.

Zu (ii) ⇒ (iii). Nach dem Ableitungskriterium für mehrfache Nullstellen (Proposition 3.1.60) haben f und Df keine gemeinsame Nullstelle in L. Da f in $L[X]$ in seine Linearfaktoren zerfällt, haben f und Df keine gemeinsamen Teiler vom Grad ≥ 1. Damit sind f und Df teilerfremd in $L[X]$, und insbesondere auch in $K[X]$.

Zu (iii) ⇒ (i). Nach dem Lemma von Bézout (Bemerkung LA.8.2.45) gibt es Polynome $u, v \in K[X]$ mit $uf + vDf = 1$. Also erzeugen f und Df das Einsideal in $L[X]$ für alle Körpererweiterungen $L \mid K$, d.h., es gilt auch $\mathrm{ggT}(f, Df) = 1$ in $L[X]$. Inbesondere haben f und Df keine gemeinsamen Nullstellen in L. Aus dem Ableitungskriterium 3.1.60 folgt, dass f keine mehrfachen Nullstellen in L besitzt. □

Definition 3.2.9 (separables Polynom)**.** Sei K ein Körper. Ein Polynom $f \in K[X]$ heißt *separabel*, wenn die äquivalenten Bedingungen der Proposition 3.2.8 erfüllt sind.

Beispiel 3.2.10. Sei p eine Primzahl.

(i) Das Polynom $X^{p^n} - X$ über $\mathbb{F}_p$ ist separabel, da es p^n verschiedene Nullstellen in $\mathbb{F}_{p^n}$ besitzt.

(ii) Das Polynom $X^p - T$ über $\mathbb{F}_p(T)$ ist *nicht* separabel: Ist a eine p-te Wurzel von T in einer Körpererweiterung von $\mathbb{F}_p(T)$, so gilt $X^p - T = X^p - a^p = (X-a)^p$, da der Frobenius-Endomorphismus $x \mapsto x^p$ ein Ringhomomorphismus ist.

Bemerkung 3.2.11.

(i) Ist $f \in K[X]$ separabel, so ist jeder Teiler von f separabel.

(ii) Sei $L \mid K$ eine Körpererweiterung und sei $f \in K[X]$. Aus Proposition 3.2.8(i,ii) folgt unmittelbar, dass f genau dann in $K[X]$ separabel ist, wenn es in $L[X]$ separabel ist. In diesem Sinne ist die Separabilität eines Polynoms unabhängig von dem Grundkörper.

Proposition 3.2.12. *Sei K ein Körper und sei $f \in K[X]$ irreduzibel.*

(i) *Ist* $\mathrm{char}(K) = 0$*, so ist f separabel.*

(ii) *Sei* $\mathrm{char}(K) = p > 0$ *und sei $n \in \mathbb{N}$ die größte Zahl, so dass $f = g(X^{p^n})$ mit einem $g \in K[X]$. Dann ist g irreduzibel und separabel, und f ist genau dann separabel, wenn $n = 0$.*

Beweis. Da f irreduzibel ist, gilt $\mathrm{ggT}(f, Df) \neq 1$ genau dann, wenn $f | Df$. Da $\deg(Df) < \deg(f)$ ist dies aber nur möglich, wenn $Df = 0$. Im Fall $\mathrm{char}(K) = 0$ gilt $\deg(Df) = \deg(f) - 1 \geq 0$ und damit $Df \neq 0$. Also ist f separabel.

Falls $\mathrm{char}(K) = p > 0$ gilt $D(X^i) = 0$ genau dann, wenn i ein Vielfaches von p ist. Also ist Df genau dann gleich Null, wenn f ein Polynom in X^p ist, d.h., wenn $n \geq 1$. Nach Maximalität von n gilt dann $Dg \neq 0$. Zudem ist g auch irreduzibel (sonst wäre f selbst reduzibel), so dass g separabel ist. □

Definition 3.2.13 (separables Element, separable Körpererweiterung)**.** Sei K ein Körper und $L \mid K$ eine algebraische Körpererweiterung.

- Ein Element $a \in L$ heißt *separabel* über K, wenn sein Minimalpolynom $m_a \in K[X]$ separabel ist.
- $L \mid K$ heißt *separabel*, wenn jedes Element von L separabel über K ist.

Korollar 3.2.14. *Sei $L \mid K$ eine algebraische Körpererweiterung und sei $a \in L$.*

(i) *Ist* $\mathrm{char}(K) = 0$*, so ist a separabel uber K. Insbesondere ist $L \mid K$ separabel.*

(ii) *Ist* $\mathrm{char}(K) = p > 0$*, so gibt es ein $n \in \mathbb{N}$, so dass a^{p^n} separabel über K ist.*

Beweis. Das Minimalpolynom $m_a \in K[X]$ ist irreduzibel nach Satz 3.1.24(i). Beide Aussagen folgen nun aus Proposition 3.2.12. Im Fall $\mathrm{char}(K) = p > 0$ gibt es ein separables irreduzibles Polynom $g \in K[X]$ mit $m_a = g(X^{p^n})$. Dann ist g das Minimalpolynom von a^{p^n} über K, so dass a^{p^n} separabel über K ist. □

Beispiel 3.2.15. Sei K ein endlicher Körper und sei $L \mid K$ eine algebraische Körpererweiterung. Dann ist $L \mid K$ separabel, denn: Ist $a \in L$, so ist $K(a)$ ein endlicher Körper und damit ein Zerfällungskörper von $X^{p^n} - X$ über K. Das Minimalpolynom von a ist dann ein Teiler von $X^{p^n} - X$ und damit separabel (Beispiel 3.2.10(i)).

Definition 3.2.16 (Separabilitätsgrad)**.** Sei $L \mid K$ eine endliche Körpererweiterung und sei $\bar{K}$ ein algebraischer Abschluss von K. Der *Separabilitätsgrad* $[L : K]_s$ von L über K ist die Mächtigkeit der Menge aller K-Algebrenhomomorphismen $L \to \bar{K}$. Nach Satz 3.1.55(ii) ist diese Mächtigkeit unabhängig von der Wahl von $\bar{K}$.

Proposition 3.2.17 (Multiplikativität des Separabilitätsgrades)**.** *Sei $L \mid K$ eine endliche Körpererweiterung und sei M ein Zwischenkörper von $L \mid K$. Dann gilt*

$$[L : K]_s = [L : M]_s \cdot [M : K]_s.$$

Beweis. Sei $\sigma\colon M \to \bar{K}$ ein K-Algebrenhomomorphismus. Es genügt zu zeigen, dass es genau $[L : M]_s$ Fortsetzungen von σ auf L gibt. Da σ injektiv ist, kann man ohne Einschränkung annehmen, dass M ein Teilkörper von $\bar{K}$ ist, und dass σ die Inklusionsabbildung ist. Dann ist $\bar{K}$ ein algebraischer Abschluss von M und die gewünschte Aussage ist genau die Definition von $[L : M]_s$. □

Lemma 3.2.18. *Sei $L \mid K$ eine algebraische Körpererweiterung und sei $a \in L$. Dann gilt $[K(a) : K]_s \leq [K(a) : K]$, und die Gleichheit gilt genau dann, wenn a separabel über K ist.*

Beweis. Sei $\bar{K}$ ein algebraischer Abschluss von K. Nach Korollar 3.1.28 gibt es eine Bijektion

$$\begin{aligned}\{K\text{-Algebrenhomomorphismen } K(a) \to \bar{K}\} &\xrightarrow{\sim} N_{\bar{K}}(m_a),\\ \sigma &\mapsto \sigma(a),\end{aligned}$$

so dass $[K(a) : K]_s = |N_{\bar{K}}(m_a)|$. Auf der anderen Seite gilt

$$|N_{\bar{K}}(m_a)| \leq \deg(m_a) = [K(a) : K]$$

nach Korollar 2.1.66 und Satz 3.1.24(i). Nach Definition ist a genau dann separabel über K, wenn die Nullstellenmenge $N_{\bar{K}}(m_a)$ genau $\deg(m_a)$ Elemente hat. □

Proposition 3.2.19. *Sei $L \mid K$ eine endliche Körpererweiterung. Dann gilt*

$$[L : K]_s \leq [L : K],$$

und die Gleichheit gilt genau dann, wenn $L \mid K$ separabel ist.

Beweis. Sei $(a_1, \ldots, a_d)$ eine Familie von Elementen von L mit $L = K(a_1, \ldots, a_d)$. Aus Lemma 3.2.18 folgt induktiv mit der Multiplikativität des Grades (Proposition 3.1.7) und des Separabilitätsgrades (Proposition 3.2.17), dass $[L : K]_s \leq [L : K]$, und dass die Gleichheit genau dann gilt, wenn jedes a_i über $K(a_1, \ldots, a_{i-1})$ separabel ist. Man beachte, dass das Minimalpolynom von a_i über $K(a_1, \ldots, a_{i-1})$ ein Teiler des Minimalpolynoms von a_i über K ist. Ist jedes a_i separabel über K, so folgt es daraus, dass $[L : K]_s = [L : K]$. Ist umgekehrt $[L : K]_s = [L : K]$, so ist insbesondere a_1 separabel über K. Aber $a_1 \in L$ war beliebig, so dass L separabel über K ist. □

Korollar 3.2.20. *Sei $L \mid K$ eine algebraische Körpererweiterung und sei $S \subset L$ eine Teilmenge bestehend aus über K separablen Elementen. Dann ist die Körpererweiterung $K(S) \mid K$ separabel.*

Beweis. Jedes $a \in K(S)$ liegt in $K(T)$ für eine endliche Teilmenge $T = \{x_1, \ldots, x_n\}$ von S. Wie im Beweis der Proposition 3.2.19 gilt dann $[K(T) : K]_s = [K(T) : K]$, und nach dieser Proposition ist dann $K(T) \mid K$ separabel. Insbesondere ist a separabel über K. □

Proposition 3.2.21 (Separabilitätsgrad vs. Grad)**.** *Sei $L \mid K$ eine algebraische Körpererweiterung. Dann ist die Teilmenge $S \subset L$ aller über K separablen Elemente ein Zwischenkörper von $L \mid K$. Ist $L \mid K$ endlich, so gilt außerdem*

$$[L : K]_s = [S : K].$$

Insbesondere ist $[L : K]_s$ ein Teiler von $[L : K]$.

Beweis. Nach Korollar 3.2.20 ist $K(S) \mid K$ eine separable Körpererweiterung, so dass $K(S) \subset S$ und damit $K(S) = S$. Ist $L \mid K$ endlich, so gilt $[S : K]_s = [S : K]$ nach Proposition 3.2.19. Nach der Multiplikativität des Separabilitätsgrades bleibt es zu zeigen, dass $[L : S]_s = 1$. Dazu verwenden wir das Korollar 3.2.14: Ist $\mathrm{char}(K) = 0$, so ist $L = S$ und es gilt $[L : L]_s = 1$ nach Definition. Ist $\mathrm{char}(K) = p > 0$, so ist jedes Element von L eine p^n-te Wurzel von einem Element von S. In einem algebraischen Abschluss $\bar{S}$ von S hat aber

jedes $a \in S$ *genau eine* p^n-te Wurzel b, denn die p^n-ten Wurzeln von a sind die Nullstellen von $X^{p^n} - a = (X-b)^{p^n}$ (da $\varphi^n \colon \bar{S} \to \bar{S}$ ein Ringhomomorphismus ist). Nach Proposition 3.1.53 gibt es mindestens ein S-Algebrenhomomorphismus $\sigma \colon L \to \bar{S}$. Das Bild unter σ einer p^n-ten Wurzel von $a \in S$ muss die p^n-te Wurzel von a in $\bar{S}$ sein, so dass σ eindeutig bestimmt ist. Damit gilt $[L : S]_s = 1$. Die letzte Aussage folgt aus der Multiplikativität des Grades: $[L : K] = [L : S] \cdot [S : K]$. □

Satz 3.2.22 (Satz vom primitiven Element)**.** *Sei $L \mid K$ eine endliche separable Körpererweiterung. Dann ist $L \mid K$ einfach, d.h., es gibt ein $a \in L$ mit $L = K(a)$.*

Beweis. Falls K endlich ist, dann ist auch L endlich. Nach Korollar 2.2.54 ist die Einheitengruppe $L^\times$ zyklisch. Ist $L^\times = \langle a \rangle$, so gilt $L = K(a)$, wie gewünscht.

Sei nun K unendlich. Da $L \mid K$ endlich ist, gibt es Elemente $a_1, \ldots, a_n \in L$ mit $L = K(a_1, \ldots, a_n)$. Durch Induktion über n genügt es, der Fall $n = 2$ zu betrachten. Sei also $L = K(a, b)$ und sei $d = [L : K]_s$. Ist $\bar{K}$ ein algebraischer Abschluss von K, so gibt es nach Definition von $[L : K]_s$ genau d K-Algebrenhomomorphismus

$$\sigma_1, \ldots, \sigma_d \colon L \to \bar{K}.$$

Behauptung. Es gibt ein $c \in L$, so dass die Elemente $\sigma_1(c), \ldots, \sigma_d(c)$ paarweise verschieden sind.

Ist $m_c \in K[X]$ das Minimalpolynom eines solchen c über K, so gilt $m_c(\sigma_i(c)) = \sigma_i(m_c(c)) = 0$ für alle i, so dass m_a mindestens d Nullstellen in $\bar{K}$ besitzt. Damit gilt $[K(c) : K] = \deg(m_c) \geq d$. Ist nun $x \in L$ beliebig, so gilt

$$\begin{aligned}
d &= [L : K]_s && \text{(nach Definition)} \\
&\geq [K(c, x) : K]_s && \text{(nach Proposition 3.2.17)} \\
&= [K(c, x) : K(c)]_s \cdot [K(c) : K]_s && \text{(nach Proposition 3.2.17)} \\
&= [K(c, x) : K(c)] \cdot [K(c) : K] && \text{(nach Lemma 3.2.18)} \\
&\geq [K(c, x) : K(c)] \cdot d.
\end{aligned}$$

Damit gilt $[K(c, x) : K(c)] = 1$, d.h., $x \in K(c)$ und damit $L = K(c)$, wie gewünscht.

Es bleibt also die Behauptung zu beweisen. Dazu betrachten wir ein Element c der Form

$$c = \lambda a + b \in L \quad \text{mit} \quad \lambda \in K.$$

Für solches c gilt $\sigma_i(c) = \sigma_j(c)$ genau dann, wenn

$$\lambda(\sigma_i(a) - \sigma_j(a)) + (\sigma_i(b) - \sigma_j(b)) = 0.$$

Sei also

$$f = \prod_{1 \leq i < j \leq d} \big((\sigma_i(a) - \sigma_j(a))X + (\sigma_i(b) - \sigma_j(b))\big) \in \bar{K}[X].$$

Für alle $i < j$ gilt $\sigma_i \neq \sigma_j$ und somit $\sigma_i(a) \neq \sigma_j(a)$ oder $\sigma_i(b) \neq \sigma_j(b)$ (da $L = K(a, b)$). Also ist f nicht das Nullpolynom. Damit hat f endlich viele Nullstellen in $\bar{K}$. Da K unendlich ist, gibt es ein $\lambda \in K$ mit $f(\lambda) \neq 0$. Für dieses λ and für $c = \lambda a + b$ gilt dann die Behauptung nach Konstruktion. □

3.2.3 Der Hauptsatz der Galoistheorie

Definition 3.2.23 (Galoiserweiterung)**.** Eine *Galoiserweiterung* ist eine algebraische Körpererweiterung, die normal und separabel ist.

Beispiel 3.2.24.

(i) Ist K ein Körper der Charakteristik 0, so ist eine algebraische Körpererweiterung $L \mid K$ genau dann galoissch, wenn sie normal ist (nach Korollar 3.2.14(i)). Zum Beispiel ist jeder Zerfällungskörper eines Polynoms über K eine Galoiserweiterung von K.

(ii) Jede Erweiterung zwischen endlichen Körpern ist eine Galoiserweiterung (siehe Beispiele 3.2.4(ii) und 3.2.15).

(iii) Ist K entweder endlich oder der Charakteristik 0, so ist ein algebraischer Abschluss $\bar{K} \mid K$ eine Galoiserweiterung.

(iv) Die Erweiterung $\mathbb{Q}(\sqrt[3]{2}) \mid \mathbb{Q}$ ist keine Galoiserweiterung, da sie nicht normal ist (Beispiel 3.2.3(iii)).

(v) Ist p eine Primzahl, so ist die Erweiterung $\mathbb{F}_p(T)(\sqrt[p]{T}) \mid \mathbb{F}_p(T)$ keine Galoiserweiterung, da sie nicht separabel ist (Beispiel 3.2.10(ii)).

Bemerkung 3.2.25.

(i) Sei $L \mid K$ eine Galoiserweiterung und sei M ein Zwischenkörper von $L \mid K$. Dann ist $L \mid M$ auch eine Galoiserweiterung. Denn das Minimalpolynom über M eines Elements von L teilt sein Minimalpolynom über K, und damit zerfällt in paarweise verschiedene Linearfaktoren in $L[X]$.

(ii) Sei $L \mid K$ eine Körpererweiterung und sei $S \subset L$ eine Teilmenge. Dann ist $K(S) \mid K$ genau dann eine Galoiserweiterung, wenn für jedes $a \in S$ das Minimalpolynom von a über K in paarweise verschiedene Linearfaktoren in $K(S)[X]$ zerfällt. Dies folgt aus Proposition 3.2.1(ii) und Korollar 3.2.20.

Proposition 3.2.26 (Grad endlicher Galoiswerweiterungen)**.** *Sei K ein Körper und sei $L \mid K$ eine endliche Galoiserweiterung. Dann gilt*

$$[L : K] = [L : K]_s = |\mathrm{Gal}(L \mid K)|.$$

Beweis. Die erste Gleichheit folgt aus Proposition 3.2.19. Nach dem Satz vom primitiven Element (Satz 3.2.22) gibt es ein $a \in L$ mit $L = K(a)$. Da $L \mid K$ normal und separabel ist, ist der Grad von m_a gleich der Anzahl seiner Nullstellen in L. Die zweite Gleichheit folgt nun aus Korollar 3.1.34(iii). □

Satz 3.2.27 (Trick von Artin)**.** *Sei $L \mid K$ eine Körpererweiterung und sei $G < \mathrm{Gal}(L \mid K)$ eine* endliche *Untergruppe. Sei*

$$L^G = \{x \in L \mid \textit{für alle } \sigma \in G \textit{ gilt } \sigma(x) = x\}$$

die Fixpunktmenge der Operation von G auf L. Dann gilt:

(i) *L^G ist ein Zwischenkörper von $L \mid K$.*

(ii) *$L \mid L^G$ ist eine Galoiserweiterung.*

(iii) *Es gilt $\mathrm{Gal}(L \mid L^G) = G$ und $[L : L^G] = |G|$.*

Beweis. Die erste Aussage folgt unmittelbar aus den Definitionen. Sei $a \in L$, sei $B \subset L$ die Bahn von a unter der Operation von G und sei

$$f = \prod_{b \in B} (X - b) \in L[X].$$

Für jedes $\sigma \in G$ gilt $\sigma(B) = B$, so dass $f = \prod_{b \in B}(X - \sigma(b))$. Dies zeigt, dass die Fortsetzung von σ auf $L[X]$ das Polynom f auf sich selbst abbildet, so dass die Koeffizienten von f im Fixkörper L^G liegen, d.h., $f \in L^G[X]$. Da $f(a) = 0$ ist a algebraisch über L^G und sein Minimalpolynom m_a teilt f. Insbesondere zerfällt m_a in seine Linearfaktoren in $L[X]$, und es hat keine mehrfachen Nullstellen. Also ist $L \mid L^G$ normal und separabel. Zudem erhalten wir die Ungleichung

$$[L^G(a) : L^G] \leq |B| \leq |G|.$$

Ist nun $(a_1, \ldots, a_n)$ eine L^G-linear unabhängige Familie in L, so folgt induktiv aus Proposition 3.1.37, dass $[L^G(a_1, \ldots, a_n) : L^G] < \infty$. Nach dem Satz vom primitiven Element (Satz 3.2.22) gibt es dann ein $a \in L$ mit $L^G(a_1, \ldots, a_n) = L^G(a)$, so dass

$$n \leq [L^G(a_1, \ldots, a_n) : L^G] = [L^G(a) : L^G] \leq |G|.$$

Daraus folgt, dass $[L : L^G] \leq |G|$. Auf der anderen Seite gilt $G \subset \mathrm{Gal}(L \mid L^G)$ nach Definition von L^G. Nach Proposition 3.2.26 erhalten wir

$$|G| \leq |\mathrm{Gal}(L \mid L^G)| = [L : L^G] \leq |G|,$$

was die Aussage (iii) liefert. □

Korollar 3.2.28 (Fixkörper der Galoisgruppe)**.** *Sei $L \mid K$ eine endliche Galoiserweiterung. Dann gilt*

$$L^{\mathrm{Gal}(L|K)} = K.$$

Beweis. Nach Proposition 3.2.26 gilt $[L : K] = |\mathrm{Gal}(L \mid K)|$. Insbesondere ist die Galoisgruppe $\mathrm{Gal}(L \mid K)$ endlich. Nach Satz 3.2.27(iii) gilt auch $[L : L^{\mathrm{Gal}(L|K)}] = |\mathrm{Gal}(L \mid K)|$. Nach der Multiplikativität des Grades erhalten wir

$$[L^{\mathrm{Gal}(L|K)} : K] = 1,$$

d.h., $L^{\mathrm{Gal}(L|K)} = K$. □

Korollar 3.2.29 (Grad vs. Mächtigkeit der Galoisgruppe)**.** *Sei $L \mid K$ eine endliche Körpererweiterung. Dann ist der Grad $[L : K]$ durch die Mächtigkeit von $\mathrm{Gal}(L \mid K)$ teilbar, und sie sind genau dann gleich, wenn $L \mid K$ eine Galoiserweiterung ist.*

Beweis. Die Galoisgruppe $\mathrm{Gal}(L \mid K)$ ist endlich, denn: Es gibt über K algebraische Elemente $a_1, \ldots, a_n \in L$ mit $L = K(a_1, \ldots, a_n)$. Nach Korollar 3.1.28 ist ein K-Algebrenhomomorphismus $\sigma\colon L \to L$ eindeutig durch die Werte $\sigma(a_1), \ldots, \sigma(a_n)$ bestimmt, und jedes $\sigma(a_i)$ muss eine der endlich vielen Nullstellen von m_{a_i} sein. Nach Satz 3.2.27 ist $L \mid L^{\mathrm{Gal}(L|K)}$ eine Galoiserweiterung mit $[L : L^{\mathrm{Gal}(L|K)}] = |\mathrm{Gal}(L \mid K)|$, und nach der Multiplikativität des Grades gilt

$$[L : K] = |\mathrm{Gal}(L \mid K)| \cdot [L^{\mathrm{Gal}(L|K)} : K].$$

Also gilt $[L : K] = |\mathrm{Gal}(L \mid K)|$ genau dann, wenn $L^{\mathrm{Gal}(L|K)} = K$. □

Korollar 3.2.30 (endliche Gruppen als Galoisgruppen)**.** *Sei G eine endliche Gruppe und sei K_0 ein Körper. Dann gibt es eine Körpererweiterung $K \mid K_0$ und eine endliche Galoiserweiterung $L \mid K$ mit $\mathrm{Gal}(L \mid K) \cong G$.*

Beweis. Sei $n = |G|$. Nach dem Satz von Cayley (Satz 1.2.16) ist G zu einer Untergruppe der symmetrischen Gruppe S_n isomorph. Sei $L = K_0(X_1, \ldots, X_n)$ der Quotientenkörper vom Polynomring $K_0[X_1, \ldots, X_n]$. Die Gruppe S_n operiert auf der K_0-Algebra L durch Permutation der n Variablen $X_1, \ldots, X_n$. Diese Operation ist treu und identifiziert S_n und damit G mit Untergruppen von $\mathrm{Gal}(L \mid K_0)$. Sei $K = L^G$. Nach Satz 3.2.27 hat dann $L \mid K$ die gewünschte Eigenschaft. □

Bemerkung 3.2.31 (inverses Galoisproblem)**.** Das *inverse Galoisproblem* fragt danach, welche endlichen Gruppen als Galoisgruppen von Körpererweiterungen von $\mathbb{Q}$ auftauchen können. Es ist bis heute noch nicht gelöst.

Satz 3.2.32 (Hauptsatz der Galoistheorie)**.** *Sei $L \mid K$ eine endliche Galoiserweiterung.*

(i) *Es gibt eine inklusionsumkehrende Bijektion*

$$\begin{aligned} \{\textit{Zwischenkörper von } L \mid K\} &\xrightarrow{\sim} \{\textit{Untergruppen von } \mathrm{Gal}(L \mid K)\}, \\ M &\mapsto \mathrm{Gal}(L \mid M), \\ L^H &\hookleftarrow H. \end{aligned}$$

Außerdem ist der Grad von $M \mid K$ gleich dem Index von $\mathrm{Gal}(L \mid M)$ in $\mathrm{Gal}(L \mid K)$:

$$[M : K] = [\mathrm{Gal}(L \mid K) : \mathrm{Gal}(L \mid M)].$$

(ii) *Ein Zwischenkörper M von $L \mid K$ ist genau dann eine normale Erweiterung von K, wenn $\mathrm{Gal}(L \mid M)$ ein Normalteiler in $\mathrm{Gal}(L \mid K)$ ist. In diesem Fall gibt es eine kurze exakte Sequenz*

$$\{e\} \to \mathrm{Gal}(L \mid M) \to \mathrm{Gal}(L \mid K) \to \mathrm{Gal}(M \mid K) \to \{e\},$$
$$\sigma \mapsto \sigma|_M.$$

Beweis. Zu (i). Wir zeigen zunächst, dass die gegebenen Abbildungen wohldefiniert sind. Die Gruppe $\mathrm{Gal}(L \mid M)$ ist eine Untergruppe von $\mathrm{Gal}(L \mid K)$ nach Definition. Zudem gilt $\mathrm{Gal}(L \mid N) \subset \mathrm{Gal}(L \mid M)$, wenn $M \subset N$, so dass die Abbildung inklusionsumkehrend ist. Auf der anderen Seite ist die Fixpunktmenge L^H ein Zwischenkörper von $L \mid K$ (da jedes $\sigma \in H$ ein Körperautomorphismus von L mit $\sigma|_K = \mathrm{id}_K$ ist). Also sind beide Abbildungen wohldefiniert.

Nach Proposition 3.2.26 ist die Gruppe $\mathrm{Gal}(L \mid K)$ endlich. Nach Satz 3.2.27 gilt dann $\mathrm{Gal}(L \mid L^H) = H$, d.h., die Komposition

$$H \mapsto L^H \mapsto \mathrm{Gal}(L \mid L^H)$$

ist die Identität. Ist M ein Zwischenkörper von $L \mid K$, so ist die Erweiterung $L \mid M$ galoissch nach Bemerkung 3.2.25(i). Nach Korollar 3.2.28 gilt dann $M = L^{\mathrm{Gal}(L|M)}$, d.h., die Komposition

$$M \mapsto \mathrm{Gal}(L \mid M) \mapsto L^{\mathrm{Gal}(L|M)}$$

ist die Identität.

Nach der Multiplikativität des Grades, Proposition 3.2.26 und dem Satz von Lagrange gilt

$$[M : K] = \frac{[L : K]}{[L : M]} = \frac{|\mathrm{Gal}(L \mid K)|}{|\mathrm{Gal}(L \mid M)|} = [\mathrm{Gal}(L \mid K) : \mathrm{Gal}(L \mid M)].$$

Zu (ii). Sei $M \mid K$ normal und sei $\sigma \in \mathrm{Gal}(L \mid K)$. Nach Proposition 3.2.1(iii) gilt dann $\sigma(M) \subset M$. Damit ist die Abbildung

$$r\colon \mathrm{Gal}(L \mid K) \to \mathrm{Gal}(M \mid K), \quad \sigma \mapsto \sigma|_M$$

wohldefiniert, und sie ist offensichtlich ein Gruppenhomomorphismus. Nach Proposition 3.2.6 ist r surjektiv. Der Kern von r ist nach Definition die Untergruppe $\mathrm{Gal}(L \mid M)$, die damit ein Normalteiler in $\mathrm{Gal}(L \mid K)$ ist.

Sei umgekehrt $\mathrm{Gal}(L \mid M) \lhd \mathrm{Gal}(L \mid K)$. Sei $a \in M$ mit Minimalpolynom $m_a \in K[X]$. Da $L \mid K$ normal ist, zerfällt m_a in seine Linearfaktoren in $L[X]$. Es genügt also zu zeigen, dass alle Nullstellen von m_a in L bereits in M liegen. Sei $b \in L$ eine Nullstelle von m_a. Nach Korollar 3.1.28 gibt es einen K-Algebrenhomomorphismus $\sigma_0\colon K(a) \to L$ mit $\sigma_0(a) = b$. Nach Proposition 3.2.6 ist σ_0 die Einschränkung eines $\sigma \in \mathrm{Gal}(L \mid K)$. Sei $\tau \in \mathrm{Gal}(L \mid M)$ beliebig und sei $\tau' = \sigma^{-1} \circ \tau \circ \sigma$. Nach Normalität gilt $\tau' \in \mathrm{Gal}(L \mid M)$ und damit

$$\tau(b) = (\tau \circ \sigma)(a) = (\sigma \circ \tau')(a) = \sigma(a) = b.$$

Also liegt b im Fixkörper $L^{\mathrm{Gal}(L|M)} = M$, wie gewünscht. □

Beispiel 3.2.33. Sei $L = \mathbb{Q}(\sqrt[3]{2}, \omega)$. Die Körpererweiterung $L \mid \mathbb{Q}$ ist normal (Beispiel 3.2.4(i)) und damit galoissch (Korollar 3.2.14(i)). Ihre Galoisgruppe haben wir im Beispiel 3.1.50 berechnet:

$$\mathrm{Gal}(L \mid \mathbb{Q}) = \{\mathrm{id}, \sigma, \sigma^2, c, c \circ \sigma, c \circ \sigma^2\} \cong S_3.$$

Dabei ist c die komplexe Konjugation, und $\sigma \in \mathrm{Gal}(L \mid \mathbb{Q}(\omega))$ bildet $\sqrt[3]{2}$ auf $\omega\sqrt[3]{2}$ ab. Man erhält einen expliziten Isomorphismus $\mathrm{Gal}(L \mid \mathbb{Q}) \xrightarrow{\sim} S_3$ wie folgt:

$$\begin{aligned}\sigma &\mapsto (1\ 2\ 3),\\ \sigma^2 &\mapsto (1\ 3\ 2),\\ c &\mapsto (1\ 2),\\ c\circ\sigma &\mapsto (2\ 3),\\ c\circ\sigma^2 &\mapsto (1\ 3).\end{aligned}$$

Die Untergruppen von $\mathrm{Gal}(L \mid \mathbb{Q})$ außer $\{\mathrm{id}_L\}$ und $\mathrm{Gal}(L \mid \mathbb{Q})$ sind die vier zyklischen Untergruppen

$$H_1 = \langle c\rangle, \quad H_2 = \langle c\circ\sigma\rangle, \quad H_3 = \langle c\circ\sigma^2\rangle, \quad K = \langle\sigma\rangle,$$

mit $|H_i| = 2$ und $|K| = 3$. Die entsprechenden Fixkörper sind

$$L^{H_1} = \mathbb{Q}(\sqrt[3]{2}), \quad L^{H_2} = \mathbb{Q}(\omega\sqrt[3]{2}), \quad L^{H_3} = \mathbb{Q}(\omega^2\sqrt[3]{2}), \quad L^K = \mathbb{Q}(\omega).$$

Zum Beispiel: Es gilt $(c\circ\sigma)(\omega\sqrt[3]{2}) = c(\omega^2\sqrt[3]{2}) = \omega\sqrt[3]{2}$, so dass $\omega\sqrt[3]{2} \in L^{H_2}$, und der Grad $[\mathbb{Q}(\omega\sqrt[3]{2}) : \mathbb{Q}]$ ist bereits gleich dem Index von H_2 in $\mathrm{Gal}(L \mid \mathbb{Q})$. Die Untergruppen H_i sind keine Normalteiler in $\mathrm{Gal}(L \mid \mathbb{Q})$, und die entsprechenden Körpererweiterungen $L^{H_i} \mid \mathbb{Q}$ sind tatsächlich nicht normal. Der Normalteiler $K \lhd \mathrm{Gal}(L \mid \mathbb{Q})$ entspricht der normalen Erweiterung $\mathbb{Q}(\omega) \mid \mathbb{Q}$, und es gibt eine kurze exakte Sequenz

$$\{e\} \to K = \mathrm{Gal}(L \mid \mathbb{Q}(\omega)) \to \mathrm{Gal}(L \mid \mathbb{Q}) \to \mathrm{Gal}(\mathbb{Q}(\omega) \mid \mathbb{Q}) \to \{e\}$$

(die wir bereits in unserer Berechnung von $\mathrm{Gal}(L \mid \mathbb{Q})$ verwendet haben).

3.2.4 Kreisteilungskörper

Wir bestimmen die Galoisgruppen der Kreisteilungskörper $\mathbb{Q}(\zeta_n) \mid \mathbb{Q}$ (siehe Beispiel 3.1.27).

Satz 3.2.34 (Kreisteilungskörper)**.** *Sei $n \in \mathbb{N}_{\geq 1}$ und sei $\zeta_n = e^{2\pi i/n} \in \mathbb{C}$.*

(i) *Das Minimalpolynom Φ_n von ζ_n über $\mathbb{Q}$ ist*

$$\Phi_n = \prod_{[i]\in(\mathbb{Z}/n\mathbb{Z})^\times} (X - \zeta_n^i).$$

Insbesondere gilt $\deg(\Phi_n) = \varphi(n)$ und damit $[\mathbb{Q}(\zeta_n) : \mathbb{Q}] = \varphi(n)$.

(ii) *Die Körpererweiterung $\mathbb{Q}(\zeta_n) \mid \mathbb{Q}$ is galoissch und es gibt einen Gruppenisomorphismus*

$$\begin{aligned}(\mathbb{Z}/n\mathbb{Z})^\times &\xrightarrow{\sim} \mathrm{Gal}(\mathbb{Q}(\zeta_n) \mid \mathbb{Q}),\\ [i] &\mapsto (\zeta_n \mapsto \zeta_n^i).\end{aligned}$$

Beweis. Zu (i). Da $\mathrm{char}(\mathbb{Q}) = 0$ ist das Minimalpolynom Φ_n separabel (Proposition 3.2.12(i)). Es genügt also zu zeigen, dass die Nullstellen von Φ_n in $\mathbb{C}$ genau die Potenzen ζ_n^i mit $[i] \in (\mathbb{Z}/n\mathbb{Z})^\times$ sind. Nach Lemma 2.2.51 sind diese Potenzen genau die *primitiven* n-ten Einheitswurzeln in $\mathbb{C}$, d.h., die Elemente von $\mu_n(\mathbb{C})$ der Ordnung n. Sei $a \in N_{\mathbb{C}}(\Phi_n)$. Nach Korollar 3.1.34 ist die Operation von $\mathrm{Gal}(\mathbb{Q}(\zeta_n) \mid \mathbb{Q})$ auf der Nullstellenmenge $N_{\mathbb{C}}(\Phi_n)$ transitiv. Es gibt damit ein $\sigma \in \mathrm{Gal}(\mathbb{Q}(\zeta_n) \mid \mathbb{Q})$ mit $\sigma(\zeta_n) = a$. Da σ ein Körperisomorphismus ist, ist a auch eine primitive n-te Einheitswurzel.

Sei umgekehrt $i \geq 1$ mit $\mathrm{ggT}(n, i) = 1$. Wir beweisen die folgende Aussage durch Induktion über i: Für jede Nullstelle ζ von Φ_n (z.B. ζ_n) ist ζ^i wieder eine Nullstelle von Φ_n. Der Fall $i = 1$ ist trivial. Sei sonst p ein Primteiler von i. Nach Induktionsvoraussetzung ist $\zeta^{i/p}$ eine Nullstelle von Φ_n. Indem wir ζ durch $\zeta^{i/p}$ ersetzen, bleibt es zu zeigen, dass

$\Phi_n(\zeta^p) = 0$. Angenommen, es wäre $\Phi_n(\zeta^p) \neq 0$. Nach Korollar 2.2.28 gibt es ein $f \in \mathbb{Z}[X]$ mit $T^n - 1 = \Phi_n \cdot f$. Da ζ und damit ζ^p Nullstellen von $T^n - 1$ sind, muss dann ζ^p eine Nullstelle von f sein. Also ist ζ eine Nullstelle von $f(X^p)$, so dass $\Phi_n | f(X^p)$. Wieder nach Korollar 2.2.28 gibt es ein $g \in \mathbb{Z}[X]$ mit $f(X^p) = \Phi_n \cdot g$. Wir wenden nun die Reduktionsabbildung $\pi\colon \mathbb{Z}[X] \to \mathbb{F}_p[X]$ an. Da der Frobenius-Endomorphismus $\varphi\colon \mathbb{F}_p[X] \to \mathbb{F}_p[X]$ ein Ringhomomorphismus ist, gilt $h^p = h(X^p)$ für alle $h \in \mathbb{F}_p[X]$, so dass

$$\pi(f)^p = \pi(f(X^p)) = \pi(\Phi_n)\pi(g).$$

Damit haben $\pi(f)$ und $\pi(\Phi_n)$ einen gemeinsamen Primteiler in $\mathbb{F}_p[X]$, so dass das Polynom $X^n - 1 = \pi(\Phi_n)\pi(f)$ über $\mathbb{F}_p$ *nicht* separabel ist. Dies steht aber im Widerspruch zum Ableitungskriterium 3.1.60, denn die einzige Nullstelle von $D(X^n - 1) = nX^{n-1}$ ist 0 (da n nicht durch p teilbar ist)

Zu (ii). Da $\Phi_n | X^n - 1$ sind alle Nullstellen von Φ_n in $\mathbb{C}$ n-te Einheitswurzeln und damit liegen bereits in $\mathbb{Q}(\zeta_n)$. Also ist die Körpererweiterung $\mathbb{Q}(\zeta_n) \mid \mathbb{Q}$ normal und damit galoissch (Korollar 3.2.14(i)). Nach Korollar 3.1.34 operiert die Galoisgruppe $\mathrm{Gal}(\mathbb{Q}(\zeta_n) \mid \mathbb{Q})$ frei und transitiv auf der Nullstellenmenge $N_{\mathbb{C}}(\Phi_n)$, die nach (i) genau aus den Potenzen ζ_n^i mit $[i] \in (\mathbb{Z}/n\mathbb{Z})^\times$ besteht. Zu jedem $[i] \in (\mathbb{Z}/n\mathbb{Z})^\times$ gibt es also genau ein $\sigma_i \in \mathrm{Gal}(\mathbb{Q}(\zeta_n) \mid \mathbb{Q})$ mit $\sigma_i(\zeta_n) = \zeta_n^i$. Damit erhalten wir eine wohldefinierte Bjektion

$$(\mathbb{Z}/n\mathbb{Z})^\times \xrightarrow{\sim} \mathrm{Gal}(\mathbb{Q}(\zeta_n) \mid \mathbb{Q}), \quad [i] \mapsto \sigma_i.$$

Für $[i], [j] \in (\mathbb{Z}/n\mathbb{Z})^\times$ gilt dann

$$(\sigma_j \circ \sigma_i)(\zeta_n) = \sigma_j(\zeta_n^i) = \sigma_j(\zeta_n)^i = \zeta_n^{ji},$$

so dass $\sigma_j \circ \sigma_i = \sigma_{ji}$. Damit ist die obige Bijektion ein Gruppenisomorphismus. □

Bemerkung 3.2.35. Die Einheitengruppe $(\mathbb{Z}/n\mathbb{Z})^\times$ ist abelsch aber nicht unbedingt zyklisch. Zum Beispiel gilt

$$(\mathbb{Z}/15\mathbb{Z})^\times \cong (\mathbb{Z}/3\mathbb{Z})^\times \times (\mathbb{Z}/5\mathbb{Z})^\times \cong C_2 \times C_4 \ncong C_8.$$

Sei im Allgemeinen $n = p_1^{e_1} \dots p_r^{e_r}$ die Primfaktorzerlegung eines $n \in \mathbb{N} \setminus \{0\}$, wobei die Primzahlen p_i paarweise verschieden sind. Nach dem chinesischen Restsatz gilt dann

$$(\mathbb{Z}/n\mathbb{Z})^\times \cong \prod_{i=1}^{r} (\mathbb{Z}/p_i^{e_i}\mathbb{Z})^\times.$$

Es ist möglich, die Gruppen $(\mathbb{Z}/p^e\mathbb{Z})^\times$ bis auf Isomorphie zu bestimmen:

$$(\mathbb{Z}/p^e\mathbb{Z})^\times \cong \begin{cases} C_{(p-1)p^{e-1}}, & \text{falls } p \text{ ungerade oder } e \leq 2, \\ C_2 \times C_{2^{e-2}}, & \text{falls } p = 2 \text{ und } e \geq 3. \end{cases}$$

Beispiel 3.2.36. Sind $L \mid K$ und $L' \mid K$ isomorphe Körpererweiterungen, so sind die Galoisgruppen $\mathrm{Gal}(L \mid K)$ und $\mathrm{Gal}(L' \mid K)$ isomorph. Die Umkehrung gilt aber nicht, selbst wenn $L \mid K$ und $L' \mid K$ endliche Galoiserweiterungen sind. Zum Beispiel:

(i) Für die Körper $\mathbb{Q}(\sqrt[3]{2}, \omega)$ und $\mathbb{Q}(\zeta_7)$ gelten

$$\mathrm{Gal}((\sqrt[3]{2}, \omega) \mid \mathbb{Q}) \cong S_3 \quad \text{und} \quad \mathrm{Gal}(\mathbb{Q}(\zeta_7) \mid \mathbb{Q}) \cong (\mathbb{Z}/7\mathbb{Z})^\times \cong C_6.$$

(nach Beispiel 3.1.50 und Satz 3.2.34(ii)). Also sind die Körper $\mathbb{Q}(\sqrt[3]{2}, \omega)$ und $\mathbb{Q}(\zeta_7)$ nicht isomorph, obwohl beide den Grad 6 über $\mathbb{Q}$ haben.

(ii) Ist $L \mid \mathbb{Q}$ eine Körpererweiterung vom Grad 2, so ist $L \mid \mathbb{Q}$ galoissch (Beispiel 3.2.3(ii)) und damit gilt $\mathrm{Gal}(L \mid \mathbb{Q}) \cong C_2$. Aber die Körper $\mathbb{Q}(\sqrt{2})$ und $\mathbb{Q}(i)$ sind nicht isomorph ($X^2 + 1$ hat Nullstellen in $\mathbb{Q}(i)$ aber nicht in $\mathbb{Q}(\sqrt{2})$).

Beispiel 3.2.37. Wir konstruieren eine Galoiserweiterung $L \mid \mathbb{Q}$ mit $\mathrm{Gal}(L \mid \mathbb{Q}) \cong C_3$. Nach Satz 3.2.34 ist $\mathbb{Q}(\zeta_7) \mid \mathbb{Q}$ eine Galoiserweiterung mit Galoisgruppe C_6. Sei $H \lhd \mathrm{Gal}(\mathbb{Q}(\zeta_7) \mid \mathbb{Q})$ die Untergruppe vom Index 3. Nach dem Hauptsatz der Galoistheorie ist $L = \mathbb{Q}(\zeta_7)^H$ eine Galoiserweiterung von $\mathbb{Q}$ mit

$$\mathrm{Gal}(L \mid \mathbb{Q}) \cong \mathrm{Gal}(\mathbb{Q}(\zeta_7) \mid \mathbb{Q})/H \cong C_3.$$

Genauer ist die komplexe Konjugation c ein Element von $\mathrm{Gal}(\mathbb{Q}(\zeta_7) \mid \mathbb{Q})$ der Ordnung 2, so dass $H = \langle c \rangle$. Also gilt $L = \{x \in \mathbb{Q}(\zeta_7) \mid \bar{x} = x\} = \mathbb{Q}(\zeta_7) \cap \mathbb{R}$.

Bemerkung 3.2.38 (abelsche Körpererweiterungen von $\mathbb{Q}$)**.** Mit dem Hauptsatz der Galoistheorie, der Klassifikation der endlichen abelschen Gruppen und Bemerkung 3.2.35 kann man leicht beweisen: Zu jeder endlichen abelschen Gruppe A gibt es eine endliche Galoiserweiterung $L \mid \mathbb{Q}$ mit $\mathrm{Gal}(L \mid \mathbb{Q}) \cong A$. Man konstruiert nämlich L als Teilkörper von einem Kreisteilungskörper wie im Beispiel 3.2.37.

Sei umgekehrt $L \mid \mathbb{Q}$ eine endliche Galoiserweiterung mit abelscher Galoisgruppe. Der *Satz von Kronecker-Weber* sagt, dass L ein Teilkörper eines Kreisteilungskörpers $\mathbb{Q}(\zeta_n)$ ist.

3.3 Anwendungen der Galoistheorie

3.3.1 Auflösbarkeit durch Radikale

Wir untersuchen nun die Existenz von Wurzelausdrücken für die Nullstellen eines Polynoms. Zunächst formulieren wir genauer, was mit einem „Wurzelausdruck“ gemeint ist:

Definition 3.3.1 (Wurzelerweiterung, auflösbar durch Radikale)**.** Sei K ein Körper.

- Eine Körpererweiterung $L \mid K$ heißt *Wurzelerweiterung*, wenn es ein $a \in L$ und ein $n \geq 1$ gibt, so dass $L = K(a)$ und $a^n \in K$.
- Eine Körpererweiterung $L \mid K$ heißt *durch Radikale auflösbar*, wenn L ein Teilkörper einer iterierten Wurzelerweiterung von K ist, d.h.: Es gibt eine Körpererweiterung $M \mid L$ und Teilkörper
$$K = M_0 \subset M_1 \subset \cdots \subset M_r = M,$$
so dass jede Erweiterung $M_i \mid M_{i-1}$ eine Wurzelerweiterung ist.
- Ein monisches Polynom $f \in K[X]$ heißt *durch Radikale auflösbar* über K, wenn der Zerfällungskörper von f über K durch Radikale auflösbar ist.

Beispiel 3.3.2 (Mitternachtsformel)**.** Sei K ein Körper mit $\mathrm{char}(K) \neq 2$ und seien $b, c \in K$. Nach der Mitternachtsformel ist das Polynom

$$f = X^2 + bX + c \in K[X]$$

durch Radikale auflösbar: Falls f keine Nullstellen in K besitzt, dann zerfällt f in seine Linearfaktoren in der Wurzelerweiterung $K(\sqrt{\Delta}) := K[T]/(T^2 - \Delta)$, wobei $\Delta = b^2 - 4c$.

Beispiel 3.3.3. Nach Korollar 2.2.54 ist jede Erweiterung $L \mid K$ zwischen endlichen Körpern eine Wurzelerweiterung: Es gilt $L = K(a)$ mit $a^{|L|-1} = 1 \in K$.

Ein besonders wichtiges Beispiel von Wurzeln sind *Einheitswurzeln*. Zur Erinnerung bezeichnen wir mit $\mu_n(K)$ die Untergruppe von $K^\times$ bestehend aus den n-ten Einheitswurzeln (siehe Beispiel 3.1.27). Eine *primitive* n-te Einheitswurzel in K ist ein Element von $\mu_n(K)$ der Ordnung n.

Proposition 3.3.4 (Existenz von primitiven Einheitswurzeln)**.** *Sei K ein Körper und sei $n \geq 1$, das nicht durch $\mathrm{char}(K)$ teilbar ist. Ist $L \mid K$ ein Zerfällungskörper von $X^n - 1$, so gilt $\mu_n(L) \cong C_n$. Insbesondere gibt es eine primitive n-te Einheitswurzel in L.*

Beweis. Wir verwenden das Ableitungskriterium 3.1.60: Da $n \neq 0$ in K ist 0 die einzige Nullstelle der Ableitung $D(X^n - 1) = nX^{n-1}$. Also hat $X^n - 1$ keine mehrfachen Nullstellen in L, so dass $|\mu_n(L)| = n$. Die Gruppe $\mu_n(L)$ ist zudem zyklisch nach Satz 2.2.53. □

Bemerkung 3.3.5 (Einheitswurzeln in der positiven Charakteristik)**.** Sei K ein Körper der Charakteristik $p > 0$ und sei $n = p^k m$ mit $\mathrm{ggT}(p, m) = 1$. Eine n-te Einheitswurzel in K ist dann das Gleiche wie eine m-te Einheitswurzel, denn 1 ist die einzige p^k-te Einheitswurzel (es gilt $X^{p^k} - 1 = (X - 1)^{p^k}$ in $K[X]$). Ist $L \mid K$ ein Zerfällungskörper von $X^n - 1$, so gilt in diesem Fall $\mu_n(L) = \mu_m(L) \cong C_m$.

Proposition 3.3.6 (Hinzufügen von Einheitswurzeln)**.** *Sei $L \mid K$ eine Galoiserweiterung und sei ζ eine Einheitswurzel in einer Körpererweiterung M von L.*

(i) *$L(\zeta) \mid K$ ist eine Galoiserweiterung. Insbesondere ist $L(\zeta) \mid L$ eine Galoiserweiterung.*

(ii) *Die Galoisgruppe $\mathrm{Gal}(L(\zeta) \mid L)$ ist abelsch.*

Beweis. Sei $n \geq 1$ minimal mit $\zeta^n = 1$. Dann gibt es n paarweise verschiedene Potenzen von ζ, die Nullstellen von $X^n - 1$ sind. Insbesondere zerfällt das Minimalpolynom von ζ über K in paarweise verschieden Linearfaktoren in $L(\zeta)$. Nach Bemerkung 3.2.25(ii) ist $L(\zeta) \mid K$ eine Galoiserweiterung. Jedes $\sigma \in \mathrm{Gal}(L(\zeta) \mid L)$ muss ζ auf eine primitive n-te Einheitswurzel abbilden, d.h., auf eine Potenz ζ^i mit $[i] \in (\mathbb{Z}/n\mathbb{Z})^\times$ (Lemma 2.2.51). Die so definierte Abbildung

$$\mathrm{Gal}(L(\zeta) \mid L) \to (\mathbb{Z}/n\mathbb{Z})^\times, \quad \sigma \mapsto [i],$$

ist dann ein injektiv, und sie ist ein Gruppenhomomorphismus: Ist $\sigma(\zeta) = \zeta^i$ und $\tau(\zeta) = \zeta^j$, so gilt

$$(\sigma \circ \tau)(\zeta) = \sigma(\zeta^j) = \sigma(\zeta)^j = \zeta^{ij}.$$

Damit ist $\mathrm{Gal}(L(\zeta) \mid L)$ abelsch. □

Proposition 3.3.7 (Charakterisierung von Wurzelerweiterungen)**.** *Sei $n \geq 1$, sei K ein Körper, der eine primitive n-te Einheitswurzel ζ enthält, und sei $L \mid K$ eine Körpererweiterung vom Grad n. Die folgenden Aussagen sind äquivalent:*

(i) *Es gibt $a \in L$ mit $L = K(a)$ und $a^n \in K$.*

(ii) *$L \mid K$ ist eine Galoiserweiterung mit zyklischer Galoisgruppe.*

Beweis. Zu (i) $\Rightarrow$ (ii). Die Elemente $a, \zeta a, \ldots, \zeta^{n-1}a$ sind paarweise verschiedene Nullstellen von $X^n - a^n$ in L, so dass $L \mid K$ eine Galoiserweiterung ist. Die Galoisgruppe $\mathrm{Gal}(L \mid K)$ operiert auf der Menge $\{a, \zeta a, \ldots, \zeta^{n-1}a\}$, und jedes $\sigma \in \mathrm{Gal}(L \mid K)$ ist durch seinen Wert $\sigma(a) = \zeta_\sigma a$ eindeutig bestimmt. Die Abbildung

$$\mathrm{Gal}(L \mid K) \to \mu_n(K) \cong C_n, \quad \sigma \mapsto \zeta_\sigma,$$

ist damit injektiv, und sie ist ein Gruppenhomomorphismus, denn:

$$(\sigma \circ \tau)(a) = \sigma(\zeta_\tau a) = \zeta_\tau \sigma(a) = \zeta_\tau \zeta_\sigma a.$$

Nach Proposition 3.2.26 gilt aber $|\mathrm{Gal}(L \mid K)| = n$, so dass $\mathrm{Gal}(L \mid K) \cong C_n$.

Zu (ii) $\Rightarrow$ (i). Sei $\mathrm{Gal}(L \mid K) = \langle \sigma \rangle$. Wir betrachten σ als K-linearen Endomorphismus von L. Sei $E \subset K$ die Menge der Eigenwerte von σ. Da $\sigma^n = \mathrm{id}_L$ aber $\sigma^m \neq \mathrm{id}_L$ für alle $0 < m < n$ ist das Minimalpolynom von σ ein Teiler von $X^n - 1$ aber kein Teiler von $X^m - 1$ für $0 < m < n$. Die Eigenwerte von σ sind insbesondere n-te Einheitswurzeln in K. Da σ ein Körperhomomorphismus ist, ist E sogar eine Untergruppe von $\mu_n(K)$: Ist $\sigma(a) = \omega a$ und $\sigma(a') = \omega' a'$ mit $a, a' \in L \setminus \{0\}$ und $\omega, \omega' \in K$, so ist aa' bzw. a^{-1} ein Eigenvektor von σ zum Eigenwert $\omega\omega'$ bzw. ω^{-1}. Es gilt also $E = \mu_m(K)$ mit einem $m|n$, und nach der Minimalität von n muss $m = n$ sein. Es gibt damit einen Eigenwert $\omega \in K$ von σ, der

eine *primitive* n-te Einheitswurzel ist. Sei $a \in L \setminus \{0\}$ ein zugehöriger Eigenvektor, so dass $\sigma(a) = \omega a$. Dann gilt $a^n \in K$, denn $\sigma(a^n) = a^n$ und $K = L^{\mathrm{Gal}(L|K)}$. Nach dem ersten Teil ist dann $K(a) \mid K$ eine Galoiserweiterung. Nach Konstruktion sind die Potenzen $\sigma^i(a)$ mit $i \in \{0, \dots, n-1\}$ paarweise verschieden, so dass die Galoisgruppe $\mathrm{Gal}(K(a) \mid K)$ mindestens n Elemente hat und somit $[K(a) : K] \geq n$. Es gilt aber $[L : K] = n$ nach Voraussetzung, so dass $L = K(a)$. □

Bemerkung 3.3.8. Proposition 3.3.7 gilt im Allgemeinen nicht, wenn K keine primitive n-te Einheitswurzel enthält. Zum Beispiel ist $\mathbb{Q}(\sqrt[3]{2}) \mid \mathbb{Q}$ nicht normal und ist $\mathbb{F}_p(T)(\sqrt[p]{T}) \mid \mathbb{F}_p(T)$ nicht separabel.

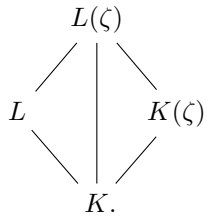
Lemma 3.3.9. *Sei $L \mid K$ eine endliche Galoiserweiterung und sei ζ eine Einheitswurzel in einer Körpererweiterung M von L.*

(i) *Ist $L(\zeta) \mid K(\zeta)$ durch Radikale auflösbar, so ist $L \mid K$ durch Radikale auflösbar.*

(ii) *Ist $\mathrm{Gal}(L(\zeta) \mid K(\zeta))$ auflösbar, so ist $\mathrm{Gal}(L \mid K)$ auflösbar.*

Beweis. Zu (i). Dies folgt unmittelbar daraus, dass $K(\zeta) \mid K$ eine Wurzelerweiterung ist.

Zu (ii). Nach Proposition 3.3.6(i) und Bemerkung 3.2.25(i) sind die folgenden fünf Erweiterungen endliche Galoiserweiterungen:



Nach Satz 3.2.32(ii) erhalten wir kurze exakte Sequenzen

$$\mathrm{Gal}(L(\zeta) \mid L) \hookrightarrow \mathrm{Gal}(L(\zeta) \mid K) \twoheadrightarrow \mathrm{Gal}(L \mid K),$$
$$\mathrm{Gal}(L(\zeta) \mid K(\zeta)) \hookrightarrow \mathrm{Gal}(L(\zeta) \mid K) \twoheadrightarrow \mathrm{Gal}(K(\zeta) \mid K).$$

Nach Proposition 3.3.6(ii) sind die Galoisgruppen $\mathrm{Gal}(L(\zeta) \mid L)$ und $\mathrm{Gal}(K(\zeta) \mid K)$ abelsch und insbesondere auflösbar. Aus Proposition 1.3.19 folgen nun die Äquivalenzen:

$$\mathrm{Gal}(L \mid K) \text{ auflösbar} \iff \mathrm{Gal}(L(\zeta) \mid K) \text{ auflösbar} \iff \mathrm{Gal}(L(\zeta) \mid K(\zeta)) \text{ auflösbar.} \quad \square$$

Lemma 3.3.10 (normale Hülle von Wurzelerweiterungen)**.** *Sei $L \mid K$ eine normale Körpererweiterung, sei $c \in L$ und sei $\bar{L}$ ein algebraischer Abschluss von L. Dann gibt es eine endliche Teilmenge $E \subset L$ mit $c \in E$, so dass für alle $n \geq 1$ die Erweiterung $L(\sqrt[n]{E}) \mid K$ normal ist, wobei $\sqrt[n]{E} = \{x \in \bar{L} \mid x^n \in E\}$.*

Beweis. Sei $E \subset L$ die Nullstellenmenge des Minimalpolynoms m_c von c über K. Sei $a \in \sqrt[n]{E}$ und sei $b \in \bar{L}$ eine Nullstelle seines Minimalpolynoms m_a über K. Da $L \mid K$ normal ist, genügt es zu zeigen, dass b bereits in $L(\sqrt[n]{E})$ liegt. Da $m_c(a^n) = 0$ gilt $m_a | m_c(X^n)$. Damit gilt auch $m_c(b^n) = 0$, d.h., es gilt $b^n \in E$ und damit $b \in \sqrt[n]{E}$, wie gewünscht. □

Der Einfachheit halber formulieren wir den folgenden Satz nur im Fall der Charakteristik 0. In der positiven Charakteristik gibt es eine ähnliche aber kompliziertere Aussage.

Satz 3.3.11 (Charakterisierung der Auflösbarkeit durch Radikale)**.** *Sei K ein Körper der Charakteristik 0.*

(i) *Eine endliche Galoiserweiterung $L \mid K$ ist genau dann durch Radikale auflösbar, wenn ihre Galoisgruppe $\mathrm{Gal}(L \mid K)$ auflösbar ist.*

(ii) *Ein monisches Polynom $f \in K[X]$ ist genau dann durch Radikale auflösbar, wenn seine Galoisgruppe* $\mathrm{Gal}(f \mid K)$ *auflösbar ist.*

Beweis. (ii) folgt aus (i), angewendet mit einem Zerfällungskörper von f.

Sei $L \mid K$ durch Radikale auflösbar. Es gibt nach Definition einen Turm von Wurzelerweiterungen

$$K = M_0 \subset M_1 \subset \cdots \subset M_r = M$$

mit $L \subset M$. Sei $a_i \in M_i$ mit $M_i = M_{i-1}(a_i)$ und $a_i^{n_i} \in M_{i-1}$. Nach Lemma 3.3.10 kann man ohne Einschränkung annehmen, indem wir weitere Wurzeln von Elementen von M hinzufügen, dass M eine normale Körpererweiterung von K ist. Nach Satz 3.2.32(ii) ist dann $\mathrm{Gal}(L \mid K)$ eine Quotientengruppe von $\mathrm{Gal}(M \mid K)$. Es genügt also zu zeigen, dass $\mathrm{Gal}(M \mid K)$ auflösbar ist. Nach Lemma 3.3.9(ii) und Proposition 3.3.4 können wir annehmen, dass K primitive n_i-te Einheitswurzeln für alle i enthält. Wir gehen nun durch Induktion über r vor. Nach Proposition 3.3.7 ist $M_1 \mid K$ normal mit zyklischer Galoisgruppe, und nach Satz 3.2.32(ii) ist $\mathrm{Gal}(M \mid K)$ eine Gruppenerweiterung von $\mathrm{Gal}(M_1 \mid K)$ durch $\mathrm{Gal}(M \mid M_1)$. Nach Induktionsvoraussetzung ist $\mathrm{Gal}(M \mid M_1)$ auflösbar, so dass $\mathrm{Gal}(M \mid K)$ auflösbar ist.

Sei umgekehrt $G = \mathrm{Gal}(L \mid K)$ auflösbar. Wir beweisen die Aussage durch Induktion über den Grad $d = [L : K] = |G|$. Wenn $d = 1$ ist $L = K$, und $K \mid K$ ist durch Radikale auflösbar. Sei also $d \geq 2$. Sei ζ eine primitive d-te Einheitswurzel in einer Körpererweiterung von L (Proposition 3.3.4). Nach Proposition 3.3.6(i) ist dann $L(\zeta) \mid K(\zeta)$ eine Galoiserweiterung. Da $L \mid K$ normal ist, gibt es einen wohldefinierten Gruppenhomomorphismus

$$\mathrm{Gal}(L(\zeta) \mid K(\zeta)) \to \mathrm{Gal}(L \mid K), \quad \sigma \mapsto \sigma|_L,$$

der offensichtlich injektiv ist (da $\sigma(\zeta) = \zeta$). Insbesondere ist $\mathrm{Gal}(L(\zeta) \mid K(\zeta))$ auch auflösbar, und d ist durch $e = [L(\zeta) : K(\zeta)]$ teilbar, so dass K auch eine primitive e-te Einheitswurzel enthält. Indem wir nun K durch $K(\zeta)$ ersetzen, können wir nach Lemma 3.3.9(i) annehmen, dass K selbst eine primitive d-te Einheitswurzel enthält. Nach Satz 1.3.29 besitzt G einen Normalteiler $H \lhd G$ mit $G/H \cong C_n$ und $n \geq 2$. Nach Satz 3.2.32 ist dann $L^H \mid K$ eine Galoiserweiterung mit Galoisgruppe

$$\mathrm{Gal}(L^H \mid K) \cong \frac{\mathrm{Gal}(L \mid K)}{\mathrm{Gal}(L \mid L^H)} = G/N \cong C_n.$$

Nach Proposition 3.3.7 ist damit $L^H \mid K$ eine Wurzelerweiterung. Auf der anderen Seite ist $L \mid L^H$ eine Galoiserweiterung mit Galoisgruppe H (Satz 3.2.27). Nach Induktionsvoraussetzung ist dann $L \mid L^H$ durch Radikale auflösbar, und somit ist $L \mid K$ durch Radikale auflösbar. □

Beispiel 3.3.12. Für alle $n \geq 1$ gibt es einen Wurzelausdruck für $\cos(2\pi/n)$ über $\mathbb{Q}$, denn $\cos(2\pi/n) = \zeta_n + \zeta_n^{-1} \in \mathbb{Q}(\zeta_n)$ und $\mathbb{Q}(\zeta_n) \mid \mathbb{Q}$ ist eine Galoiserweiterung mit abelscher Galoisgruppe.

Beispiel 3.3.13. Sei $f = X^5 - 4X^2 + 2 \in \mathbb{Q}[X]$. Wir zeigen im Folgenden, dass $\mathrm{Gal}(f) \cong S_5$. Da S_5 nicht auflösbar ist (Proposition 1.3.30), ist f nicht durch Radikale auflösbar, d.h., die Nullstellen von f lassen sich nicht mit rationalen Zahlen und den Symbolen $+$, $\cdot$ und $\sqrt[n]{}$ ausdrücken. Nach Bemerkung 3.1.49 operiert die Galoisgruppe $\mathrm{Gal}(f)$ treu auf der Nullstellenmenge $N = N_{\mathbb{C}}(f)$. Nach dem Einsensteinschen Kriterium ist f irreduzibel und damit separabel, so dass $|N| = 5$. Man kann also $\mathrm{Gal}(f)$ mit einer Untergruppe von $S_N \cong S_5$ identifizieren, und es bleibt zu zeigen, dass $\mathrm{Gal}(f)$ eine Transposition sowie einen 5-Zyklus enthält (Proposition 1.2.39).

- *Existenz einer Transposition.* Das Polynom f hat genau drei reelle Nullstellen (nach Analysis). Die komplexe Konjugation definiert damit einen Automorphismus von $\mathbb{Q}(N)$, die die zwei nicht-reellen Nullstellen vertauscht.

- *Existenz eines* 5*-Zyklus.* Die 5-Zyklen in S_5 sind genau die Elemente der Ordnung 5. Da f irreduzibel ist, ist $|\mathrm{Gal}(f)| = [\mathbb{Q}(N) : \mathbb{Q}]$ durch $\deg(f) = 5$ teilbar. Nach dem Satz von Cauchy (Korollar 1.3.47) besitzt dann $\mathrm{Gal}(f)$ ein Element der Ordnung 5.

Dieses Argument zeigt übrigens: Ist p eine Primzahl und ist $f \in \mathbb{Q}[X]$ irreduzibel vom Grad p mit $< p$ reellen Nullstellen, so gilt $\mathrm{Gal}(f) \cong S_p$. Falls $p \geq 5$ ist dann f nicht durch Radikale auflösbar.

Beispiel 3.3.14 (Polynome vom Grad ≤ 4)**.** Jedes monische Polynom f vom Grad ≤ 4 über einem Körper K der Charakteristik 0 ist durch Radikale auflösbar. Denn die Galoisgruppe $\mathrm{Gal}(f \mid K)$ ist isomorph zu einer Untergruppe von S_4 (Bemerkung 3.1.49), und S_4 ist auflösbar (Proposition 1.3.17). Explizite Wurzelausdrücke für die Nullstellen von Polynomen vom Grad 3 und 4 sind bekannt, aber sie sind ziemlich kompliziert.

Bemerkung 3.3.15 (Satz von Abel-Ruffini)**.** Der *Satz von Abel-Ruffini* besagt, dass die Galoisgruppe des *allgemeinen* monischen Polynoms vom Grad n zu S_n isomorph ist. Dabei ist das „allgemeine monische Polynom vom Grad n“ das Polynom

$$X^n + T_1 X^{n-1} + \cdots + T_{n-1} X + T_n$$

über dem Körper von rationalen Funktionen $\mathbb{Q}(T_1, \ldots, T_n)$. Dies impliziert im geeigneten Sinne, dass die *meisten* Polynome vom Grad n über $\mathbb{Q}$ die Galoisgruppe S_n haben (und damit nicht durch Radikale auflösbar sind, wenn $n \geq 5$). Es gilt zum Beispiel

$$\mathrm{Gal}(X^n - X - 1 \mid \mathbb{Q}) \cong S_n$$

für alle $n \in \mathbb{N}$.

3.3.2 Konstruierbarkeit mit Zirkel und Lineal

Sei M eine Teilmenge von $\mathbb{R}^2$. In diesem Abschnitt untersuchen wir die folgende Frage: Welche Punkte kann man aus M mit Zirkel und Lineal konstruieren? Mit dem Lineal kann man die Gerade $G(x, y)$ durch zwei gegebene Punkte $x \neq y$ ziehen, und mit dem Zirkel kann man den Kreis $K(x, r)$ mit einem gegebenen Mittelpunkt x und einem gegebenen Radius r ziehen (dabei ist ein Radius r gegeben, wenn r gleich dem Abstand zwischen zwei gegebenen Punkten ist).

Wir betrachten genauer die folgenden Mengen:

- $G(M)$ ist die Menge der Geraden in $\mathbb{R}^2$, die zwei verschiedene Punkte aus M enthalten.
- $K(M)$ ist die Menge der Kreise in $\mathbb{R}^2$, deren Mittelpunkt in M liegt und deren Radius gleich dem Abstand zwischen zwei verschiedenen Punkten aus M ist.
- $\mathrm{ZL}^1(M)$ ist die Menge aller Punkte aus $\mathbb{R}^2$, die Schnittpunkte von zwei verschiedenen Geraden aus $G(M)$, von zwei verschiedenen Kreisen aus $K(M)$ oder von einer Geraden aus $G(M)$ und einem Kreis aus $K(M)$ sind.

Man definiert dann induktiv

$$\mathrm{ZL}^0(M) = M \quad \text{und} \quad \mathrm{ZL}^{n+1}(M) = \mathrm{ZL}^1(\mathrm{ZL}^n(M)).$$

Definition 3.3.16 (konstruierbar mit Zirkel und Lineal)**.** Sei $M \subset \mathbb{R}^2$ eine Teilmenge. Ein Punkt $x \in \mathbb{R}^2$ ist *aus M mit Zirkel und Lineal konstruierbar*, wenn es ein $n \in \mathbb{N}$ mit $x \in \mathrm{ZL}^n(M)$ gibt. Wir bezeichnen mit

$$\mathrm{ZL}(M) = \bigcup_{n \in \mathbb{N}} \mathrm{ZL}^n(M) \subset \mathbb{R}^2$$

die Teilmenge aller aus M mit Zirkel und Lineal konstruierbaren Punkte.

Ein Punkt aus $\mathbb{R}^2$ heißt *mit Zirkel und Lineal konstruierbar* oder einfach *konstruierbar*, wenn er aus $\{(0, 0), (1, 0)\}$ mit Zirkel und Lineal konstruierbar ist.

Bemerkung 3.3.17.

(i) Falls $|M| \geq 2$ gilt $M \subset \mathrm{ZL}^1(M)$ und somit $\mathrm{ZL}^n(M) \subset \mathrm{ZL}^{n+1}(M)$. Daraus folgt $\mathrm{ZL}^1(\mathrm{ZL}(M)) = \mathrm{ZL}(M)$.

(ii) Eine Konstruktion mit Zirkel und Lineal kann nur endlich viele Punkte verwenden. Damit gelten

$$\mathrm{ZL}^1(M) = \bigcup_{\substack{E \subset M \\ \text{endlich}}} \mathrm{ZL}^1(E) \quad \text{und} \quad \mathrm{ZL}(M) = \bigcup_{\substack{E \subset M \\ \text{endlich}}} \mathrm{ZL}(E).$$

Um die Menge $\mathrm{ZL}(M)$ zu verstehen, ist es hilfreich, die Ebene $\mathbb{R}^2$ mit dem Körper $\mathbb{C}$ zu identifizieren.

Proposition 3.3.18 (der Körper der konstruierbaren Punkte)**.** *Sei $M \subset \mathbb{C}$ eine Teilmenge mit $0, 1 \in M$. Dann ist* $\mathrm{ZL}(M)$ *ein Zwischenkörper von $\mathbb{C} \mid \mathbb{Q}$, der außerdem* quadratisch abgeschlossen *ist, d.h.: Jedes $a \in \mathbb{C}$ mit $a^2 \in \mathrm{ZL}(M)$ liegt bereits in* $\mathrm{ZL}(M)$*.*

Beweis. Nach Voraussetzung gilt $0, 1 \in \mathrm{ZL}(M)$. Seien $x, y \in \mathrm{ZL}(M) \setminus \{0\}$. Ist $x \neq y$, so ist die Summe $x+y$ ein Schnittpunkt der Kreise $K(x, |y|)$ und $K(y, |x|)$, so dass $x+y \in \mathrm{ZL}(M)$. Dies gilt auch wenn $x = y$, denn $2x$ ist ein Schnittpunkt des Kreises $K(x, |x|)$ und der Geraden $G(0, x)$. Zudem ist $-x$ ein Schnittpunkt von $K(0, |x|)$ und $G(0, x)$, so dass $-x \in \mathrm{ZL}(M)$. Also ist $\mathrm{ZL}(M)$ eine Untergruppe von $(\mathbb{C}, +)$.

Im Folgenden bezeichnen wir einfach als „konstruierbar“ die Elemente von $\mathrm{ZL}(M)$. Sei nun $z = re^{i\varphi} \in \mathbb{C}$ mit $r \in \mathbb{R}_{\geq 0}$ und $\varphi \in \mathbb{R}$. Es ist klar, dass z genau dann konstruierbar ist, wenn beide r und $e^{i\varphi}$ konstruierbar sind. Es bleibt also die folgenden vier Aussagen zu beweisen:

(i) Sind $x, y \in \mathbb{R}^\times$ konstruierbar, so sind xy und x^{-1} konstruierbar.

(ii) Sind $e^{i\varphi}$ und $e^{i\psi}$ konstruierbar, so sind $e^{i(\varphi+\psi)}$ und $e^{-i\varphi}$ konstruierbar.

(iii) Ist $x \in \mathbb{R}_{>0}$ konstruierbar, so ist $\sqrt{x}$ konstruierbar.

(iv) Ist $e^{i\varphi}$ konstruierbar, so ist $e^{i\varphi/2}$ konstruierbar.

Wir bemerken zunächst, dass i aus $\{0, 1\}$ mit Zirkel und Lineal konstruierbar ist: Man konstruiert nämlich hintereinander $e^{i\pi/3}$, $i\sqrt{3}$ und i.

Zu (i). Sei G die Gerade durch x und i, und sei G' die zu G parallele Gerade durch yi. Dann gilt $G' \cap \mathbb{R} = \{xy\}$ und damit ist xy konstruierbar. Ist G'' die zu G parallele Gerade durch 1, so gilt $G'' \cap \mathbb{R}i = \{x^{-1}i\}$, so dass $x^{-1}i$ und damit x^{-1} konstruierbar sind.

Zu (ii). Der Punkt $e^{i(\varphi+\psi)}$ ist ein Schnittpunkt von $K(0, 1)$ und $K(e^{i\varphi}, |e^{i\psi} - 1|)$. Der Punkt $e^{-i\varphi}$ ist ein Schnittpunkt von $K(0, 1)$ und $K(1, |e^{i\varphi} - 1|)$.

Zu (iii). Sei K der Kreis durch -1 und x mit Mittelpunkt $(x-1)/2$. Die reelle Zahl $y \in \mathbb{R}_{>0}$ mit $K \cap \mathbb{R}i = \{\pm yi\}$ ist dann konstruierbar. Nach dem Satz von Thales sind $-1, yi, x$ die Ecken eines rechtwinkligen Dreiecks. Nach dem Satz von Pythagoras gilt dann

$$(x+1)^2 = |yi+1|^2 + |yi-x|^2 = (y^2+1) + (y^2+x^2) \implies x = y^2.$$

Zu (iv). Falls $e^{i\varphi} = -1$ haben wir schon bemerkt, dass i und $-i$ konstruierbar sind. Sonst liegt der Punkt $e^{i\varphi/2}$ auf dem Einheitskreis und auf der Ursprungsgerade durch $e^{i\varphi} + 1$. □

Für eine Teilmenge $M \subset \mathbb{C}$ schreiben wir $\bar{M} = \{\bar{z} \mid z \in M\} \subset \mathbb{C}$.

Satz 3.3.19 (Charakterisierung der Konstruierbarkeit mit Zirkel und Lineal)**.** *Sei $M \subset \mathbb{C}$ eine Teilmenge mit $0, 1 \in M$. Die folgenden Aussagen sind äquivalent für $z \in \mathbb{C}$:*

(i) *Es gilt $z \in \mathrm{ZL}(M)$, d.h., z ist aus M mit Zirkel und Lineal konstruierbar.*

(ii) *Es gibt eine Galoiserweiterung* $L \mid \mathbb{Q}(M \cup \bar{M})$ *mit* $z \in L$*, so dass* $[L : \mathbb{Q}(M \cup \bar{M})]$ *eine Zweierpotenz ist.*

(iii) *Es gibt einen Turm von Körpererweiterungen*

$$\mathbb{Q}(M \cup \bar{M}) = L_0 \subset L_1 \subset \cdots \subset L_r \subset \mathbb{C}$$

mit $z \in L_r$ *und* $[L_i : L_{i-1}] = 2$ *für alle* i*.*

Beweis. Nach Proposition 3.3.18 ist $\mathrm{ZL}(M)$ ein Teilkörper von $\mathbb{C}$. Zudem gilt $M \cup \bar{M} \subset \mathrm{ZL}(M)$ (man kann $\bar{z}$ aus $\{0, 1, z\}$ mit Zirkel und Lineal konstruieren), so dass $\mathbb{Q}(M \cup \bar{M}) \subset \mathrm{ZL}(M)$. Ohne Einschränkung ist also M ein Teilkörper von $\mathbb{C}$ mit $\bar{M} = M$ (d.h., M ist unter komplexer Konjugation abgeschlossen).

Zu (ii) $\Rightarrow$ (iii). Die Galoisgruppe $\mathrm{Gal}(L \mid M)$ ist eine 2-Gruppe. Nach Satz 1.3.36 ist $\mathrm{Gal}(L \mid M)$ auflösbar. Nach Satz 1.3.29 besitzt $\mathrm{Gal}(L \mid M)$ eine Kompositionsreihe

$$\{\mathrm{id}\} = G_r \lhd \cdots \lhd G_1 \lhd G_0 = \mathrm{Gal}(L \mid M),$$

so dass die Faktoren G_{i-1}/G_i einfache abelsche 2-Gruppen sind, und damit zu C_2 isomorph. Durch den Hauptsatz der Galoistheorie erhalten wir einen Turm von Körpererweiterungen

$$M = L^{G_0} \subset L^{G_1} \subset \cdots \subset L^{G_r} = L$$

mit $[L^{G_i} : L^{G_{i-1}}] = 2$.

Zu (iii) $\Rightarrow$ (i,ii). Nach Proposition 3.3.7 gibt es Elemente $a_i \in L_i$ mit $L_i = L_{i-1}(a_i)$ und $a_i^2 \in L_{i-1}$. Wir zeigen $L_i \subset \mathrm{ZL}(M)$ durch Induktion über i. Es gilt $L_0 = M \subset \mathrm{ZL}(M)$. Nach Proposition 3.3.18 ist der Körper $\mathrm{ZL}(M)$ quadratisch abgeschlossen. Ist $L_{i-1} \subset \mathrm{ZL}(M)$, so folgt $a_i \in \mathrm{ZL}(M)$ und damit $L_i \subset \mathrm{ZL}(M)$. Dies zeigt (i). Nach Lemma 3.3.10 können wir weitere Quadratwurzeln zu L_r hinzufügen, um eine normale Körpererweiterung L von M zu erhalten. Nach der Multiplikativität des Grades ist dann $L \mid M$ eine Galoiserweiterung wie in (ii).

Zu (i) $\Rightarrow$ (iii). Wir konstruieren genauer einen solchen Turm von Körpererweiterungen mit $L_i = L_{i-1}(a_i)$ und $a_i^2 \in L_{i-1} \cap \mathbb{R}$. Als erster Schritt können wir i hinzufügen und damit annehmen, dass $i \in M$. Durch Induktion genügt es die folgende Aussage zu beweisen: Ist M ein Zwischenkörper von $\mathbb{C} \mid \mathbb{Q}(i)$ mit $\bar{M} = M$ und ist $z \in \mathrm{ZL}^1(M)$, so gibt es ein $a \in M \cap \mathbb{R}_{>0}$ mit $z \in M(\sqrt{a})$. Nach Definition ist z ein Schnittpunkt von zwei verschiedenen Geraden aus $G(M)$, von zwei verschiedenen Kreisen aus $K(M)$ oder von einer Geraden aus $G(M)$ und einem Kreis aus $K(M)$. Man kann leicht nachprüfen, dass Schnittpunkte des ersten Typs bereits in M liegen. Bei zwei Kreisen in $K(M)$ liegt die Gerade durch die zwei Schnittpunkte (oder die Tangente zum einzelnen Schnittpunkt) in $G(M)$. Es bleibt also Schnittpunkte des letzten Typs zu betrachten. Solche Schnittpunkte erhält man, indem man eine geeignete reelle Polynomgleichung vom Grad ≤ 2 auflöst, deren Koeffizienten aus den Real- und Imaginärteilen von Elementen von M durch Körperoperationen gebildet werden. Die Voraussetzungen $i \in M$ und $\bar{M} = M$ implizieren aber, dass die Real- und Imaginärteile von Elementen von M wieder in M liegen. Mit der Mitternachtsformel findet man dann ein $a \in M \cap \mathbb{R}_{>0}$ mit $z \in M(\sqrt{a})$, wie gewünscht. □

Korollar 3.3.20. *Sei* $a \in \bar{\mathbb{Q}}$ *eine algebraische Zahl, so dass* $[\mathbb{Q}(a) : \mathbb{Q}]$ *keine Zweierpotenz ist. Dann ist* a *nicht mit Zirkel und Lineal konstruierbar.*

Beweis. Dies folgt aus Satz 3.3.19(ii) und der Multiplikativität des Grades. □

Bemerkung 3.3.21. Die Umkehrung von Korollar 3.3.20 gilt nicht. Sei $f \in \mathbb{Q}[X]$ ein irreduzibles monisches Polynom vom Grad 4 mit Galoisgruppe S_4 (z.B. $f = X^4 - X - 1$), und sei $a \in \mathbb{C}$ eine Nullstelle von f, so dass $[\mathbb{Q}(a) : \mathbb{Q}] = 4$. Sei $M \subset \mathbb{C}$ der Zerfällungskörper von f. Ist $L \mid \mathbb{Q}$ eine endliche Galoiserweiterung mit $L \subset \mathbb{C}$ und $a \in L$, so ist auch $L \cap M$ eine Galoiserweiterung von $\mathbb{Q}$, die $\mathbb{Q}(a)$ enthält. Nach Satz 3.2.32(ii) ist damit $\mathrm{Gal}(L \cap M \mid \mathbb{Q})$

eine Quotientengruppe von S_4 mit ≥ 4 Elementen. Da S_4 keinen Normalteiler mit 3 oder 6 Elementen enthält, ist $[L \cap M : \mathbb{Q}]$ und damit auch $[L : \mathbb{Q}]$ durch 3 teilbar. Insbesondere kann $[L : \mathbb{Q}]$ keine Zweierpotenz sein, so dass a nicht konstruierbar ist.

Beispiel 3.3.22 (Würfelverdopplung)**.** Die Seitenlänge $\sqrt[3]{2}$ eines Würfels mit Volumen 2 ist nicht mit Zirkel und Lineal konstruierbar, denn $[\mathbb{Q}(\sqrt[3]{2}) : \mathbb{Q}] = 3$ keine Zweierpotenz ist.

Beispiel 3.3.23 (Quadratur des Kreises)**.** Ein Quadrat, dessen Flächeninhalt gleim dem des Einheitskreises ist, ist nicht mit Zirkel und Lineal konstruierbar. Denn seine Seitenlänge $\sqrt{\pi}$ ist nicht einmal algebraisch über $\mathbb{Q}$.

Beispiel 3.3.24 (reguläre Polygone)**.** Sei $n \geq 1$ und sei $\zeta_n = e^{2\pi i/n} \in \mathbb{C}$. Die Potenzen von ζ_n sind genau die Ecken eines regulären n-Ecks im Einheitskreis. Nach Satz 3.2.34 ist $\mathbb{Q}(\zeta_n) \mid \mathbb{Q}$ eine Galoiserweiterung vom Grad $\varphi(n)$. Damit ist ein reguläres n-Eck *genau dann* mit Zirkel und Lineal konstruierbar, wenn $\varphi(n)$ eine Zweierpotenz ist. Zum Beispiel ist ein reguläres Neuneck nicht mit Zirkel und Lineal konstruierbar, denn $\varphi(9) = 6$.

Primzahlen der Gestalt $2^k + 1$ heißen *Fermatsche Primzahlen.* Die sind also genau die Primzahlen p, so dass ein reguläres p-Eck mit Zirkel und Lineal konstruierbar ist. Es gibt nur fünf bekannte Fermatsche Primzahlen: 3, 5, 17, 257 und 65537; es wird vermutet, dass keine weiteren existieren. Nach Proposition 2.2.45 ist ein reguläres n-Eck genau dann mit Zirkel und Lineal konstruierbar, wenn $n = 2^k p_1 \dots p_r$, wobei $k \in \mathbb{N}$ und $p_1, \dots, p_r$ paarweise verschiedene Fermatsche Primzahlen sind.

Beispiel 3.3.25 (Winkeldreiteilung)**.** Man kann bekanntlich einen beliebigen Winkel mit Zirkel und Lineal in zwei gleich große Winkel unterteilen. Es ist aber nicht möglich, einen beliebigen Winkel mit Zirkel und Lineal in drei gleich große Winkel zu unterteilen. Zum Beispiel ist der Winkel $\pi/3$ konstruierbar (d.h., ζ_6 ist konstruierbar), aber der Winkel $\pi/9$ ist nicht konstruierbar (denn $\varphi(18) = 6$ keine Zweierpotenz ist).

3.3.3 Der Fundamentalsatz der Algebra

Satz 3.3.26 (Fundamentalsatz der Algebra)**.** *Der Körper $\mathbb{C}$ ist algebraisch abgeschlossen.*

Es gibt viele Beweise von diesem Satz. Trotz des Namens gehört der Fundamentalsatz der Algebra eher zur Analysis, denn er hat mit der analytischen Vollständigkeit der reellen Zahlen zu tun. Man kann zum Beispiel den Fundamentalsatz mit der Funktionentheorie einfach beweisen.

In diesem Abschnitt beweisen wir den Fundamentalsatz mithilfe der Galoistheorie und der folgenden zwei analytischen Eigenschaften von $\mathbb{R}$:

- *Nullstellen von Polynomen ungeraden Grades.* Ist $f \in \mathbb{R}[X]$ und ist $\deg f$ ungerade, so hat f eine Nullstelle in $\mathbb{R}$.
- *Quadratwurzeln positiver Zahlen.* Ist $c \in \mathbb{R}_{\geq 0}$, so gibt es ein $x \in \mathbb{R}$ mit $x^2 = c$.

Lemma 3.3.27. *Jedes Polynom zweiten Grades über $\mathbb{C}$ hat eine Nullstelle.*

Beweis. Nach der Mitternachtsformel genügt es zu zeigen, dass jedes $c \in \mathbb{C}$ eine Quadratwurzel besitzt. Ist $c = re^{i\varphi}$ mit $r \in \mathbb{R}_{\geq 0}$, so ist $\sqrt{r}e^{i\varphi/2}$ eine Quadratwurzel von c. □

Beweis von Satz 3.3.26. Nach der Existenz von Zerfällungskörpern genügt es zu zeigen, dass jede endliche Körpererweiterung L von $\mathbb{C}$ gleich $\mathbb{C}$ ist. Da $[\mathbb{C} : \mathbb{R}] = 2$ ist die Erweiterung $L \mid \mathbb{R}$ auch endlich, so dass $L = \mathbb{R}(S)$ für eine endliche Teilmenge $S \subset L$. Sei $\bar{L}$ ein algebraischer Abschluss von L. Indem man alle Nullstellen in $\bar{L}$ der Minimalpolynome über $\mathbb{R}$ der Elemente von S hinzufügt, kann man ohne Einschränkung annehmen, dass $L \mid \mathbb{R}$ normal ist. Da $\mathrm{char}(\mathbb{R}) = 0$ ist dann $L \mid \mathbb{R}$ eine endliche Galoiserweiterung.

Sei $[L:\mathbb{R}] = |\mathrm{Gal}(L \mid \mathbb{R})| = 2^k m$ mit $m \in \mathbb{N}$ ungerade. Nach dem ersten Sylow-Satz gibt es eine 2-Sylowgruppe $H < \mathrm{Gal}(L \mid \mathbb{R})$. Nach Satz 3.2.27(iii) gilt dann $[L:L^H] = |H| = 2^k$ und damit

$$[L^H:\mathbb{R}] = \frac{[L:\mathbb{R}]}{[L:L^H]} = \frac{2^k m}{2^k} = m.$$

Nach dem Satz vom primitiven Element (Satz 3.2.22) gibt es ein $a \in L^H$ mit $L^H = \mathbb{R}(a)$. Das Minimalpolynom m_a von a über $\mathbb{R}$ hat damit den Grad $[\mathbb{R}(a):\mathbb{R}] = m$, der ungerade ist. Also hat m_a eine Nullstelle in $\mathbb{R}$. Da m_a irreduzibel ist, ist dies nur möglich, wenn $\deg(m_a) = 1$, d.h., es gilt $m = 1$ und damit $[L:\mathbb{R}] = 2^k$. Da $[\mathbb{C}:\mathbb{R}] = 2$ ist $[L:\mathbb{C}]$ auch eine Zweierpotenz.

Also ist die Galoisgruppe $\mathrm{Gal}(L \mid \mathbb{C})$ eine 2-Gruppe. Wir zeigen schließlich, dass diese Gruppe trivial sein muss. Falls sie *nicht* trivial ist, dann gibt es nach Korollar 1.3.37 eine Untergruppe $H < \mathrm{Gal}(L \mid \mathbb{C})$ vom Index 2. Nach dem Hauptsatz der Galoistheorie ist dann L^H eine Körpererweiterung von $\mathbb{C}$ vom Grad 2. Das Minimalpolynom über $\mathbb{C}$ von einem $a \in L^H \setminus \mathbb{C}$ ist dann ein irreduzibles Polynom zweiten Grades, im Widerspruch zum Lemma 3.3.27. Also ist $\mathrm{Gal}(L \mid \mathbb{C})$ trivial, so dass $L = \mathbb{C}$. □

Bemerkung 3.3.28 (reell abgeschlossene Körper)**.** Ein Körper K heißt *formal reell*, wenn -1 keine Summe von Quadraten in K ist. Ein solcher Körper hat unbedingt die Charakteristik 0 (in der positiven Charakteristik ist -1 stets eine Summe von Einsen). Ein formal reeller Körper K heißt *reell abgeschlossen*, wenn außerdem:

- Jedes Polynom ungeraden Grades über K hat eine Nullstelle in K.
- Für jedes $a \in K$ hat a oder $-a$ eine Quadratwurzel in K.

Die sind genau die zwei Eigenschaften von $\mathbb{R}$, die wir im obigen Beweis des Fundamentalsatzes der Algebra verwendet haben. Ein anderes Beispiel ist der Körper $\bar{\mathbb{Q}} \cap \mathbb{R}$ der reellen algebraischen Zahlen. Es stellt sich heraus, dass ein Körper K genau dann reell abgeschlossen ist, wenn -1 keine Quadratwurzel in K besitzt und $K(\sqrt{-1}) = K[X]/(X^2+1)$ algebraisch abgeschlossen ist.

Der *Satz von Artin-Schreier* sagt ferner, dass ein Körper K genau dann reell abgeschlossen ist, wenn $1 < [\bar{K}:K] < \infty$ gilt, wobei $\bar{K}$ ein algebraischer Abschluss von K ist. Anders gesagt ist die Erweiterung $\bar{K} \mid K$ stets unendlich, außer wenn K bereits algebraisch abgeschlossen ist (in dem Fall $[\bar{K}:K] = 1$) oder wenn K reell abgeschlossen ist (in dem Fall $[\bar{K}:K] = 2$).

Index