Einführung in die Algebra

und

Algebra I

Alfred Geroldinger

und

Franz Halter-Koch

Vorbemerkungen

Wir bezeichnen mit $\mathbb{N} = \{1, 2, 3, \dots\}$ die Menge der natürlichen Zahlen und setzen $\mathbb{N}_0 = \mathbb{N} \cup \{0\}$. Weiters bezeichnen wir mit $\mathbb{Z}$ ($\mathbb{Q}$, $\mathbb{R}$ bzw. $\mathbb{C}$) die Menge der ganzen (rationalen, reellen bzw. komplexen) Zahlen und erhalten

$$\mathbb{N} \subset \mathbb{N}_0 \subset \mathbb{Z} \subset \mathbb{Q} \subset \mathbb{R} \subset \mathbb{C}\,.$$

Für eine Menge X, bezeichne $|X| \in \mathbb{N}_0 \cup \{\infty\}$ die Anzahl der Elemente in X.

Für a, $b \in \mathbb{Z}$, setzen wir $[a, b] = \{x \in \mathbb{Z} \mid a \leq x \leq b\}$, insbesondere ist $[a, b] = \emptyset$ falls $a > b$.

Gesamtheiten von (mathematischen) Objekten, die keine Mengen zu sein brauchen, nennen wir *Klassen*.

Unter eine *Familie* $(X_i)_{i \in I}$ verstehen wir eine nichtleere Menge I (genannt *Indexmenge*), gemeinsam mit einer Abbildung $X\colon I \to \Omega$ in eine Klasse Ω, so dass $X(i) = X_i$ für alle $i \in I$.

Äquivalenzrelationen

Sei M eine nichtleere Menge. Eine *Relation* auf M ist eine Teilmenge $\sim$ von $M \times M$. Für a, $b \in M$ schreibt man $a \sim b$ an Stelle von $(a, b) \in \sim$.

Ein Relation $\sim$ auf M heißt *"Aquivalenzrelation*, wenn für alle $a, b, c \in M$ gilt:

- (*Reflexivität*) $a \sim a$.
- (*Symmetrie*) Aus $a \sim b$ folgt $b \sim a$.
- (*Transitivität*) Aus $a \sim b$ und $b \sim c$ folgt $a \sim c$.

Ist $\sim$ eine Äquivalenzrelation auf M und $a \in M$, so nennt man

$$[a]_\sim = [a] = \{c \in M \mid c \sim a\} \subset M$$

die (*Äquivalenz*)*klasse* von a, und jedes Element $c \in [a]$ heißt ein *Repräsentant* der Klasse $[a]$. Dann gilt für alle a, $b \in M$:

$$[a] = [b] \iff [a] \cap [b] \neq \emptyset \iff a \sim b\,.$$

Wir bezeichnen mit $M/\!\sim \;= \{[a] \mid a \in M\}$ die *Menge der Äquivalenzklassen* und nennen die Abbildung

$$\pi_\sim\colon M \to M/\!\sim, \quad \text{definiert durch} \quad \pi_\sim(a) = [a]\,,$$

die (*kanonische*) *Äquivalenzklassenabbildung*. Eine Teilmenge $\mathcal{P} \subset M$ heißt *Repräsentantensystem* für $\sim$, wenn es zu jedem $a \in M$ genau ein $a^* \in \mathcal{P}$ gibt mit $a \sim a^*$.

Die Äquivalenzrelation $\sim$ induziert eine Partition von M, nämlich

$$M = \biguplus_{g \in M/\sim} g\,.$$

Umgekehrt induziert jede Partition

$$M = \biguplus_{i \in I} M_i$$

von M eine Äquivalenzrelation auf M vermöge

$$a \sim b \iff \text{es gibt ein } i \in I \text{ mit } a, b \in M_i.$$

Ist dann $i \in I$ und $a \in M_i$, so folgt $[a]_\sim = M_i$.

Partielle Ordnungen und Totalordnungen

Sei wieder M eine nichtleere Menge. Eine Relation $\leq$ auf M heißt *partielle Ordnung* (auf M), wenn für alle a, b, $c \in M$ folgenden Eigenschaften erfüllt sind:

- (*Reflexivität*) $a \leq a$.
- (*Antisymmetrie*) Aus $a \leq b$ und $b \leq a$ folgt $a = b$.
- (*Transitivität*) Aus $a \leq b$ und $b \leq c$ folgt $a \leq c$.

Ist $\leq$ eine partielle Ordnung auf M, so heißt $(M, \leq)$ eine partiell geordnete Menge.

Sei nun $(M, \leq)$ eine partiell geordnete Menge und $\emptyset \neq N \subset M$. Ein Element $a \in M$ heißt

- *maximales* (bzw. *minimales*) *Element* von N, wenn $a \in N$ und für alle $x \in N$ gilt: Aus $a \leq x$ (bzw. $a \geq x$) folgt $a = x$.
- *größtes* (bzw. *kleinstes*) *Element* von N, wenn $a \in N$, und $x \leq a$ (bzw. $x \geq a$) für alle $x \in N$.
  N hat höchstens ein größtes Element, das mit $\max(N)$ bezeichnet wird, und höchstens ein kleinstes Element, das mit $\min(N)$ bezeichnet wird.
- *obere* (bzw. *untere*) *Schranke* von N, wenn $x \leq a$ (bzw. $x \leq a$) für alle $x \in N$.
- *Supremum* (bzw. *Infimum*) von N, wenn a ein kleinstes (bzw. größtes) Element in der Menge der oberen (bzw. unteren) Schranken von N ist.
  N hat höchstens ein Supremum, das mit $\sup(N) = \sup_{\leq}(N)$ bezeichnet wird und höchstens ein Infimum, das mit $\inf(N) = \inf_{\leq}(N)$ bezeichnet wird.

Eine Teilmenge A einer partiell geordneten Menge $(M, \leq)$ heißt (nach oben) *gerichtet*, wenn es zu je zwei Elementen x, $y \in A$ ein $z \in A$ gibt mit $z \geq x$ und $z \geq y$.

Eine *Totalordnung* auf M ist eine partielle Ordnung $\leq$, sodass für je zwei Elemente $a, b \in M$ entweder $a \leq b$ oder $b \leq a$. Man nennt dann $(M, \leq)$ *totalgeordnet*.

Seien $(M, \leq)$ und $(M', \leq')$ partiell geordnete Mengen. Ein *Ordnungsisomorphismus* $f\colon M \to M'$ ist eine bijektive Abbildung, so dass für alle a, $b \in M$ gilt: $a \leq b \iff f(a) \leq' f(b)$.

Zorn'sches Lemma. Sei M eine nichtleere partiell geordnete Menge. Wenn jede (bezüglich der induzierten Ordnung) totalgeordnete Teilmenge von M eine obere Schranke in M besitzt, dann besitzt M ein maximales Element.

Sei Ω eine Menge von Mengen. Dann ist $(\Omega, \subset)$ eine partiell geordnete Menge. Eine Teilmenge $\Sigma \subset \Omega$ heißt

- *gerichtet*, wenn sie bezüglich $\subset$ gerichtet ist.
- *Kette*, wenn sie bezüglich $\subset$ totalgeordnet ist.

Zorn'sches Lemma, konkrete Form. Sei Ω eine nichtleere Menge von Mengen. Gehört die Vereinigung jeder Kette in Ω wieder zu Ω, so besitzt Ω (bezüglich $\subset$) ein maximales Element.

Basiseigenschaften ganzer Zahlen

A. Algebraische Struktur

$\mathbb{Z}$ ist bezüglich der gewöhnlichen Addition und Multiplikation ganzer Zahlen ein kommutativer Ring.

B. Anordnung

$\mathbb{Z}$ ist in natürlicher Weise angeordnet:

$$\cdots < -2 < -1 < 0 < 1 < 2 < \ldots$$

Diese Anordnung lässt sich auf $\mathbb{Q}$ und dann auf $\mathbb{R}$ fortsetzen. $\mathbb{Q}$ und $\mathbb{R}$ sind angeordnete Körper (vgl. Analysis-Skriptum). Die Ordnung induziert Absolutbetrag: für $x \in \mathbb{R}$ sei

$$|x| = \begin{cases} x & x \geq 0 \\ -x & x < 0 \end{cases}$$

Es gelten die wohlbekannten Rechenregeln.

C. Induktionsprinzip

Es gelten die folgenden (im Rahmen einer axiomatischen Theorie äquivalenten) Aussagen:

C1 (Prinzip vom kleinsten Element)
Jede nichtleere Menge natürlicher Zahlen enthält ein kleinstes Element.

C2 Jede nach oben (bzw. unten) beschränkte nichtleere Menge ganzer Zahlen besitzt ein größtes (bzw. kleinstes) Element.

C3 (Prinzip der vollständigen Induktion) Sei B eine Menge natürlicher Zahlen, so dass gilt:
- Es gibt eine Zahl $b_0 \in B$ (Induktionsanfang)
- Ist $b \in B$, so ist $b+1 \in B$ (Induktionsschritt)

Dann ist $\{x \in \mathbb{N} \mid x \geq b_0\} \subset B$.

C4 (Prinzip der vollständigen Induktion, 2. Form) Sei B eine Menge natürlicher Zahlen, so dass für alle $b \in \mathbb{N}$ gilt:
- Ist $\{x \in \mathbb{N} \mid x < b\} \subset B$, so folgt $b \in B$.

Dann ist $B = \mathbb{N}$.

Wir verweisen noch auf einige einführende Lehrbücher in deutscher Sprache: [**?, ?, ?, ?, ?, ?**].

Contents

CHAPTER 1

Elementare Zahlentheorie

1.1. Fundamentalsatz der Arithmetik, ggT und kgV

Definition 1.1.1.

1. Seien $a, b \in \mathbb{Z}$. Man sagt, a *teilt* b und schreibt $a \mid b$, wenn es ein $c \in \mathbb{Z}$ gibt mit $b = ac$. Dann nennt man auch b ein *Vielfaches* von a und a einen *Teiler* von b.
2. Eine natürliche Zahl $p \in \mathbb{N}$ heißt *Primzahl*, wenn $p > 1$, und $\{a \in \mathbb{N} \mid a \mid p\} = \{1, p\}$. Wir bezeichnen mit $\mathbb{P}$ die Menge der Primzahlen.

Lemma 1.1.2 (Eigenschaften der Teilbarkeitsrelation)**.** *Seien $a, b, c \in Z$.*

1. $1 \mid a$, $a \mid a$, $a \mid 0$, *und* $0 \mid a \iff a = 0$.
2. $a \mid b \iff |a| \mid |b|$.
3. *Aus* $a \mid b$ *und* $a \mid c$ *folgt* $a \mid b \pm c$.
4. *Aus* $a \mid b$ *und* $b \mid c$ *folgt* $a \mid c$.
5. *Genau dann ist* $a \mid b$ *und* $b \mid a$, *wenn* $|a| = |b|$.
6. $(\mathbb{N}_0, \mid)$ *ist eine partiell geordnete Menge.*
7. *Sei* $|a| > 1$ *und* $p = \min\{q \in \mathbb{N} \mid q > 1$ *und* $q \mid a\}$. *Dann ist* $p \in \mathbb{P}$.

Beweis. Klar. □

Satz 1.1.3 (Hauptsatz der Arithmetik)**.** *Jedes $a \in \mathbb{N}$ besitzt eine (bis auf die Reihenfolge der Faktoren) eindeutige Darstellung $a = p_1 \cdot \ldots \cdot p_n$ mit $n \in \mathbb{N}_0$ und $p_1, \ldots, p_n \in \mathbb{P}$, und dann ist $\{p_1, \ldots, p_n\} = \{p \in \mathbb{P} \mid p \mid a\}$.*
Insbesondere besitzt jedes $a \in \mathbb{N}$ eine eindeutige Darstellung

$$a = p_1^{e_1} \cdot \ldots \cdot p_n^{e_n} \quad \text{mit} \quad n \in \mathbb{N}_0\,,\ e_1, \ldots, e_n \in \mathbb{N} \ \text{und}\ p_1, \ldots, p_n \in \mathbb{P}\,, \ \text{so dass}\ p_1 < p_2 < \ldots < p_n\,.$$

Beweis. Es genügt, die erste Aussage zu zeigen. Sei $a \in \mathbb{N}$, $a > 1$ und gelte die Behauptung für alle $c \in \mathbb{N}$ mit $c < a$. Nach Lemma 1.1.2 ist $p = \min\{b \in \mathbb{N} \mid b > 1\,,\ b \mid a\} \in \mathbb{P}$, und es sei $a = pb$ mit $b \in \mathbb{N}$. Ist $b = 1$, so sind wir fertig. Andernfalls besitzt b nach Voraussetzung eine eindeutige Darstellung der Form $b = p_2 \cdot \ldots \cdot p_n$ mit $p_2, \ldots, p_n \in \mathbb{P}$, und es ist $a = pp_2 \cdot \ldots \cdot p_n$. Sei nun $a = q_1 q_2 \cdot \ldots \cdot q_m$ eine weitere Darstellung von a als Produkt von Primzahlen. Ist $p \in \{q_1, \ldots, q_m\}$, etwa $p = q_1$, so folgt $b = q_2 \cdot \ldots \cdot q_m$, und nach Voraussetzung ist dann $n = m$ und (nach geeigneter Umnummerierung) $p_i = q_i$ für alle $i \in [2, n]$. Sei also $p \notin \{q_1, \ldots, q_m\}$. Dann ist $p < q_j$ für alle $j \in [1, m]$, und wir betrachten die Zahl $c = (q_1 - p)q_2 \cdot \ldots \cdot q_m = p(b - q_2 \cdot \ldots \cdot q_m) < a$. Nach Voraussetzung ist $q_1 - p = r_1 \cdot \ldots \cdot r_k$ mit $k \in \mathbb{N}_0$ und $r_1, \ldots, r_k \in \mathbb{P}$, und $c = r_1 \cdot \ldots \cdot r_k q_2 \cdot \ldots \cdot q_m$. Nun ist $p \mid c$, $p < q_j$ für alle $j \in [1, m]$ und $p \nmid q_1 - p$, also $p \notin \{r_1, \ldots, r_k, q_2, \ldots, q_m\}$, ein Widerspruch.

Sei nun $a = p_1 \cdot \ldots \cdot p_n$ mit $n \in \mathbb{N}$ und $p_1, \ldots, p_n \in \mathbb{P}$, und sei $p \in \mathbb{P}$ mit $p \,|\, a$. Dann ist $a = pb$, und $b = q_2 \cdot \ldots \cdot q_m$ mit $m \in \mathbb{N}$ und $q_2, \ldots, q_m \in \mathbb{P}$, also $a = pq_2 \cdot \ldots \cdot q_m$ und daher $p \in \{p_1, \ldots, p_n\}$ wegen der Eindeutigkeit der Darstellung. □

Definition 1.1.4 (Größter gemeinsamer Teiler und kleinstes gemeinsames Vielfaches)**.**
Sei $\emptyset \neq A \subset \mathbb{Z}$, und seien d, $e \in \mathbb{N}_0$.

1. d heißt *größter gemeinsamer Teiler* von A, $d = \mathrm{ggT}(A)$, wenn gilt:
   - Für alle $a \in A$ ist $d \,|\, a$.
   - Ist $g \in \mathbb{Z}$ und $g \,|\, a$ für alle $a \in A$, so folgt $g \,|\, d$.
2. e heißt *kleinstes gemeinsames Vielfaches* von A, $e = \mathrm{kgV}(A)$, wenn gilt:
   - Für alle $a \in A$ ist $a \,|\, e$.
   - Ist $g \in \mathbb{Z}$ und $a \,|\, g$ für alle $a \in A$, so folgt $e \,|\, g$.
3. $a, b \in \mathbb{Z}$ heißen *teilerfremd*, wenn $\mathrm{ggT}(a, b) = 1$. Man nennt dann auch a teilerfremd zu b oder b teilerfremd zu a.

Ist $A = \{a_1, \ldots, a_n\}$ mit $n \in \mathbb{N}$, so schreiben wir auch $\mathrm{ggT}(a_1, \ldots, a_n)$ an Stelle von $\mathrm{ggT}(A)$ und $\mathrm{kgV}(a_1, \ldots, a_n)$ an Stelle von $\mathrm{kgV}(A)$.

Bemerkungen 1.1.5. Sei $\emptyset \neq A \subset \mathbb{Z}$.

1. A besitzt höchstens einen größten gemeinsamen Teiler und höchstens ein kleinstes gemeinsames Vielfaches [Beweis: Sind d und d' größte gemeinsame Teiler von A, so folgt $d \,|\, d'$ und $d' \,|\, d$, also $d = d'$; ebenso argumentiert man für das kleinste gemeinsame Vielfache].
2. Ist $A' = \big\{|a| \;\big|\; a \in A\big\}$, so folgt $\mathrm{ggT}(A) = \mathrm{ggT}(A') = \inf_{|}(A')$ und $\mathrm{kgV}(A) = \mathrm{kgV}(A') = \sup_{|}(A')$.

Satz 1.1.6 (Hauptsatz über der Euklidischen Algorithmus)**.**

1. (Satz von der Division mit Rest) *Seien $a \in \mathbb{Z}$ und $b \in \mathbb{N}$. Dann gibt es eindeutig bestimmte Zahlen $q, r \in \mathbb{Z}$ mit $a = bq + r$ und $r \in [0, b-1]$. Ist $a \geq 0$, so ist auch $q \geq 0$.*
2. (Euklidischer Algorithmus) *Seien $a, b \in \mathbb{N}$, und seien die Folgen $(r_i)_{i \geq -1}$ und $(q_i)_{i \geq 0}$ in $\mathbb{N}_0$ rekursiv definiert durch $r_{-1} = a$, $r_0 = b$, und für $i \geq 0$ durch*
   $r_{i+1} = q_{i+1} = 0$, *falls* $r_i = 0$, *und*
   $r_{i-1} = q_i r_i + r_{i+1}$ *mit* $q_i, r_{i+1} \in \mathbb{N}_0$ *und* $r_{i+1} < r_i$ *(gemäß 1.).*
   Dann existiert ein $n \in \mathbb{N}_0$ mit $r_n > 0$, $r_{n+1} = 0$, und dann ist $\mathrm{ggT}(a, b) = r_n$.
3. (Algorithmus von Berlekamp) *Seien $a, b \in \mathbb{N}$, und seien $n \in \mathbb{N}$, $r_{-1}, \ldots, r_n, q_0, \ldots, q_n \in \mathbb{N}_0$ wie in 2. Die Folgen $(x_i)_{i \in [0,n]}$ und $(y_i)_{i \in [0,n]}$ in $\mathbb{Z}$ seien rekursiv definiert durch*
$$x_0 = 0\,, \quad y_0 = 1\,, \quad x_1 = 1\,, \quad y_1 = -q_0\,,$$
$$x_{i+1} = x_{i-1} - q_i x_i \quad \text{und} \quad y_{i+1} = y_{i-1} - q_i y_i \quad \text{für} \quad i \in [1, n-1]$$
   Dann folgt $r_i = ax_i + by_i$ für alle $i \in [0, n]$. Insbesondere ist $\mathrm{ggT}(a, b) = r_n = ax_n + by_n$.
4. (Kennzeichnung des ggT als Vielfachsumme) *Seien $a, b \in \mathbb{Z}$ und $d \in \mathbb{N}$. Dann gilt:*
$$d = \mathrm{ggT}(a, b) \iff \big[\, d \,|\, a\,,\ d \,|\, b\,, \quad \text{und es gibt} \quad x, y \in \mathbb{Z} \quad \text{mit} \quad d = ax + by \,\big].$$
5. *Seien $a, b \in \mathbb{Z}$ und $d \in \mathbb{N}$. Dann ist $\mathrm{ggT}(da, db) = d\,\mathrm{ggT}(a, b)$ und*
$$d = \mathrm{ggT}(a, b) \iff \Big[\, d \,|\, a\,,\ d \,|\, b\,,\ \mathrm{ggT}\Big(\frac{a}{d}, \frac{b}{d}\Big) = 1 \,\Big].$$

BEWEIS. 1. *Existenz.* Die Menge $T = \{x \in \mathbb{Z} \mid a - bx \geq 0\}$ ist nach oben beschränkt, und es sei $q = \max(T) \in \mathbb{Z}$ und $r = a - bq \in \mathbb{N}_0$. Wäre $r \geq b$, so folgte $a - b(q+1) = r - b \geq 0$ im Widerspruch zur Maximalität von T. Im Falle $a \geq 0$ ist $0 \in T$ und daher $q \geq 0$.

Eindeutigkeit. Seien $q, q', r, r' \in \mathbb{N}_0$ mit $a = bq + r = bq' + r'$ und $r, r' < b$. Dann folgt $b|q - q'| = |r - r'| < b$, also $q = q'$ und $r = r'$.

2. Wäre $r_n > 0$ für alle $n \in \mathbb{N}_0$, so folgte $r_0 > r_1 > r_2 > \ldots$, ein Widerspruch. Wir zeigen:

1) $r_n \mid a$ und $r_n \mid b$; **2)** Ist $g \in \mathbb{Z}$ mit $g \mid a$ und $g \mid b$, so folgt $g \mid r_n$.

1) Angenommen, das sei falsch, und es sei $i \in [0, n]$ maximal mit $r_n \nmid r_{i-1}$. Dann ist $r_n \mid r_i$, $r_n \mid r_{i+1}$ und wegen $r_{i-1} = q_i r_i + r_{i+1}$ folgt $r_n \mid r_{i-1}$, ein Widerspruch.

2) Angenommen, es gebe ein $g \in \mathbb{Z}$ mit $g \mid a$, $g \mid b$ und $g \nmid r_n$. Ist dann $i \in [1, n-1]$ minimal mit $g \nmid r_{i+1}$, so ist $g \mid r_i$, $g \mid r_{i-1}$, und wegen $r_{i+1} = r_{i-1} - q_i r_i$ folgt $g \mid r_{i+1}$, ein Widerspruch.

3. Induktion nach i. Für $i = 0$ und $i = 1$ rechnet man die Behauptung direkt nach.Sei also $i \geq 1$ und die Behauptung für $i - 1$ und i gezeigt. Dann folgt

$$r_{i+1} = r_{i-1} - q_i r_i = ax_{i-1} + by_{i-1} - q_i(ax_i + by_i) = a(x_{i-1} - q_i x_i) + b(y_{i-1} - q_i y_i) = ax_{i+1} + by_{i+1}\,.$$

4. Ist $a = 0$, so folgt $\operatorname{ggT}(0, b) = |b|$, und die Behauptung ist klar. Ist $b = 0$, so argumentiert man genauso. Sei also $a \neq 0$ und $b \neq 0$.

$\Rightarrow$: Ist $d = \operatorname{ggT}(a, b)$, so ist $d \mid a$, $d \mid b$, und $d = \operatorname{ggT}(|a|, |b|)$. Nach 3. gibt es $x', y' \in \mathbb{Z}$ mit $d = |a|x' + |b|y'$, und mit $x = \operatorname{sgn}(a)x'$ und $y = \operatorname{sgn}(b)y'$ folgt die Behauptung.

$\Leftarrow$: Ist $g \in \mathbb{Z}$ mit $g \mid a$ und $g \mid b$, so folgt auch $g \mid ax + by = d$.

5. Sei $c = \operatorname{ggT}(a, b)$. Nach 4. ist dann $c \mid a$, $c \mid b$, und es gibt $x, y \in \mathbb{Z}$ mit $c = ax + by$. Dann folgt $dc \mid da$, $dc \mid db$ und $dc = dax + day$. Also ist (wieder nach 4.) $dc = \operatorname{ggT}(da, db)$.

Ist $d \mid a$ und $d \mid b$, so folgt daher

$$\operatorname{ggT}(a, b) = d \operatorname{ggT}\Big(\frac{\mathrm{a}}{\mathrm{d}}, \frac{\mathrm{b}}{\mathrm{d}}\Big)\,.$$

□

Satz 1.1.7 (Satz von Euklid)**.** *Seien $n \in \mathbb{N}$ und $a, b, a_1, \ldots, a_n \in \mathbb{Z}$.*

1. *a und b besitzen einen größten gemeinsamen Teiler [d.h., es gibt ein $d \in \mathbb{N}_0$ mit $d = \operatorname{ggT}(a, b)$].*
2. *Sei $c \in \mathbb{Z}$ und $d = \operatorname{ggT}(a, c)$. Dann gilt: $c \mid ab \iff c \mid db$.*
   Insbesondere folgt: Ist $c \mid ab$ und c teilerfremd zu a, so folgt $c \mid b$.
3. *Ist $p \in \mathbb{P}$ und $p \mid a_1 \cdot \ldots \cdot a_n$, so gibt es ein $i \in [1, n]$ mit $p \mid a_i$.*
4. *Ist $\operatorname{ggT}(a_i, b) = 1$ für alle $i \in [1, n]$, so ist auch $\operatorname{ggT}(a_1 \cdot \ldots \cdot a_n, b) = 1$.*

BEWEIS. 1. Offensichtlich ist $\operatorname{ggT}(a, 0) = |a|$, $\operatorname{ggT}(0, b) = |b|$ und $\operatorname{ggT}(a, b) = \operatorname{ggT}(|a|, |b|)$. Daher können wir $a, b \in \mathbb{N}$ annehmen, und dafür folgt die Aussage aus dem Hauptsatz.

2. $\Leftarrow$: Offensichtlich.

$\Rightarrow$: Nach Satz 1.1.6.4 gibt es $x, y \in \mathbb{Z}$ mit $d = ax + cy$, und es gibt ein $z \in \mathbb{Z}$ mit $ab = cz$. Daher folgt $db = c(zx + by)$, also $c \mid db$.

3. Induktion nach n. Für $n = 1$ ist nichts zu zeigen.

$n \geq 2$, $n - 1 \to n$: Sei $a = a_1 \cdot \ldots \cdot a_{n-1}$ und $p \mid aa_n$. Ist $p \mid a$, so folgt $p \mid a_i$ für ein $i \in [1, n-1]$ nach Induktionsvoraussetzung. Ist $p \nmid a$, so ist $\operatorname{ggT}(a, p) = 1$ und daher $p \mid a_n$ nach 2.

4. Wir nehmen an, es sei $d = \operatorname{ggT}(a_1 \cdot \ldots \cdot a_n, b) > 1$ und $p \in \mathbb{P}$ mit $p \mid d$. Dann folgt $p \mid b$ und $p \mid a_1 \cdot \ldots \cdot a_n$, also $p \mid a_i$ für ein $i \in [1, n]$ nach 3., im Widerspruch zu $\operatorname{ggT}(a_i, b) = 1$. □

Satz 1.1.8 (Existenzsatz für ggT und kgV)**.** *Sei $\emptyset \neq A \subset \mathbb{N}$. Dann besitzt A einen größten gemeinsamen Teiler. Ist A endlich, so besitzt A auch ein kleinstes gemeinsames Vielfaches.*

BEWEIS. Sei zuerst A endlich und $V = \{g \in \mathbb{N} \mid \text{ für alle } a \in A \text{ ist } a \mid g\}$. Dann ist $V \neq \emptyset$, und es sei $e = \min(V)$. Dann ist $a \mid e$ für alle $a \in A$. Sei $g \in \mathbb{Z}$ und $a \mid g$ für alle $a \in A$, und sei $c = \mathrm{ggT}(e, g)$. Dann ist $c \leq e$ und $a \mid c$ für alle $a \in A$, also $e = c \mid g$ und daher $e = \mathrm{kgV}(A)$.

Sei nun A beliebig und $d = \max\{g \in \mathbb{Z} \mid \text{ für alle } a \in A \text{ ist } g \mid a\}$. Dann ist $d \mid a$ für alle $a \in A$. Sei $g \in \mathbb{Z}$ und $g \mid a$ für alle $a \in A$. Ist $c = \mathrm{kgV}(g, d)$, so folgt $c \geq d$ und $c \mid a$ für alle $a \in A$, also $c = d$, $g \mid d$ und daher $d = \mathrm{ggT}(A)$. □

Definition und Satz 1.1.9 (Satz von der reduzierten Bruchdarstellung)**.** *Jedes $r \in \mathbb{Q}$ hat eine eindeutige Darstellung*

$$r = \frac{p}{q} \quad \textit{mit} \quad p \in \mathbb{Z},\, q \in \mathbb{N} \quad \textit{und} \quad \mathrm{ggT}(p, q) = 1\,.$$

Man nennt p den *reduzierten Zähler* und q den *reduzierten Nenner* von r.

BEWEIS. Sei $r \in \mathbb{Q}$. Nach Definition von $\mathbb{Q}$ gibt es $p_1 \in \mathbb{Z}$ und $q_1 \in \mathbb{N}$ mit

$$r = \frac{p_1}{q_1}\,, \quad \text{und es sei} \quad d = \mathrm{ggT}(p_1, q_1)\,, \quad p = \frac{p_1}{d} \text{ und } q = \frac{q_1}{d}\,, \quad \text{also } r = \frac{p}{q} \text{ und } \mathrm{ggT}(p, q) = 1$$

(nach Satz 1.1.7.1). Es bleibt die Eindeutigkeit zu zeigen. Sei also

$$r = \frac{p}{q} = \frac{p'}{q'} \quad \text{mit} \quad p,\, p' \in \mathbb{Z}\,,\; q,\, q' \in \mathbb{N} \text{ und } \mathrm{ggT}(p, q) = \mathrm{ggT}(p', q') = 1\,.$$

Dann folgt $pq' = p'q$, also $q \mid pq'$ und $q' \mid p'q$. Aus Satz 1.1.7.2 folgt $q \mid q'$ und $q' \mid q$, also $q = q'$ und daher auch $p = p'$. □

Satz 1.1.10. *Sei $x \in \mathbb{Q}$, $n \in \mathbb{N}$ und*

$$x^n + a_{n-1}x^{n-1} + \ldots + a_1 x + a_0 = 0 \quad \textit{mit} \quad a_0, \ldots, a_{n-1} \in \mathbb{Z}\,.$$

Dann folgt $x \in \mathbb{Z}$. Insbesondere gilt: Aus $x^n \in \mathbb{Z}$ folgt $x \in \mathbb{Z}$.

BEWEIS. Nach Satz 1.1.9 gibt es $p \in \mathbb{Z}$ und $q \in \mathbb{N}$ mit $\mathrm{ggT}(p, q) = 1$ und

$$x = \frac{p}{q}\,, \quad \text{also} \quad p^n + qa_{n-1}p^{n-1} + \ldots + q^{n-1}a_1 p + q^n a_0 = 0\,, \quad \text{und daher} \quad q \mid p^n\,.$$

Nach Satz 1.1.7.4 ist aber $\mathrm{ggT}(q, p^n) = 1$, also $q = 1$ und $x \in \mathbb{Z}$. □

1.2. Primzahlen

Die Untersuchung der Primzahlen zählt zu den zentralen Themen der Zahlentheorie. Wir sprechen in der Folge einige naheliegende Fragen an, und orientieren uns dabei an dem Buch von P. Ribenboim [**?**]. Auf Beweise müssen wir weitgehend verzichten. Für jedes $n \in \mathbb{N}$ bezeichnen wir mit p_n die n-te Primzahl. Dann ist $p_1 = 2, p_2 = 3, p_3 = 5$ und so weiter.

Wieviele Primzahlen gibt es?

Der folgende Satz (und sein Beweis) gehen auf Euklid zurück (Euklid lebte um 300 v. Chr. in Alexandria; Werk: Elemente der Mathematik, 13 Bücher).

Satz 1.2.1. *Es gibt unendlich viele Primzahlen.*

BEWEIS. Wir führen den Beweis indirekt. Angenommen $\mathbb{P}$ wäre endlich, etwa $\mathbb{P} = \{p_1, \ldots, p_n\}$ mit $n \in \mathbb{N}$. Dann ist $a = p_1 \cdot \ldots \cdot p_n + 1 > 1$, und es sei $p \in \mathbb{P}$ mit $p \,|\, a$. Dann ist $p \in \{p_1, \ldots, p_n\}$, also $p \,|\, a - 1$ und daher $p \,|\, 1$, ein Widerspruch. □

Es ist unbekannt, ob es unendlich viele $n \in \mathbb{N}$ gibt, sodass $p_1 \cdot \ldots \cdot p_n + 1$ wieder prim ist.

Wie findet man Primzahlen ?

Der Beweis von Satz 1.2.1 liefert ein (prinzipielles) Verfahren um neue Primzahlen zu finden: ist $n \in \mathbb{N}$ und sind $u_1 < \ldots < u_n$ Primzahlen, so ist $u_1 \cdot \ldots \cdot u_n + 1$ durch ein $p \in \mathbb{P} \setminus \{u_1, \ldots, u_n\}$ teilbar.

Lemma 1.2.2. *Sei $a \in \mathbb{N}_{\geq 2} \setminus \mathbb{P}$. Dann gibt es ein $p \in \mathbb{P}$ mit $p \,|\, a$ und $p \leq \sqrt{a}$.*

BEWEIS. Sei $a \in \mathbb{N} \setminus (\mathbb{P} \cup \{1\})$. Nach Satz 1.1.3 gibt es ein $n \in \mathbb{N}_{\geq 2}$ und Primzahlen $u_1, \ldots, u_n$ mit $u_1 \leq \ldots \leq u_n$ und $a = u_1 \cdot \ldots \cdot u_n$. Dann ist $u_1 \leq u_2 \cdot \ldots \cdot u_n = u_1^{-1} a$ und daher $u_1^2 \leq a$. □

Bemerkung 1.2.3. [Sieb des Eratosthenes (3. Jh. v. Chr.)]
Der folgende Algorithmus zur Bestimmung aller Primzahlen unterhalb einer gegebenen Schranke $N \in \mathbb{N}$ heißt *Sieb des Eratosthenes* (dies ist Schulstoff vgl. [**?**]).

- Man schreibe alle Zahlen von 2 bis N auf.
- Man markiere die Zahl 2 und streiche alle Vielfachen von 2.
- Für alle $m \in \mathbb{N}$ mit $3 \leq m \leq \sqrt{N}$ führe man (in aufsteigender Reihenfolge) folgenden Schritt durch:

  Ist m nicht gestrichen, so markiere man m und streiche alle Vielfachen von m.

Die markierten und nicht gestrichenen Zahlen sind genau die Primzahlen $p \in [1, N]$.

Satz 1.2.4. *Sei $n \in \mathbb{N}_{\geq 2}$. Dann gilt: $n \in \mathbb{P} \iff n \mid \binom{n}{\nu}$ für alle $\nu \in [1, n-1]$.*

BEWEIS. Für $\nu \in [1, n-1]$ ist

$$\binom{n}{\nu} = \frac{n(n-1) \cdot \ldots \cdot (n-\nu+1)}{\nu!} \in \mathbb{N}\,, \quad \text{also} \quad \nu! \,|\, n(n-1) \cdot \ldots \cdot (n-\nu+1)\,.$$

Ist $n \in \mathbb{P}$, ist $\operatorname{ggT}(\nu!, n) = 1$ und daher $\nu! \,|\, (n-1) \cdot \ldots \cdot (n-\nu+1)$, also $n \,|\, \binom{n}{\nu}$.

Sei nun $n \notin \mathbb{P}$. Dann gibt es ein $\nu \in \mathbb{P}$ und $k \in \mathbb{N}$, so dass $\nu^k \,|\, n$ und $\nu^{k+1} \nmid n$. Dann ist $\nu \in [1, n-1]$, und wir nehmen an, es sei $n \,|\, \binom{n}{\nu}$. Dann folgt $\nu^k \,|\, \binom{n}{\nu}$ und daher $\nu^{k+1}(\nu-1)! \,|\, n(n-1)\cdot\ldots\cdot(n-\nu+1)$. Nach Satz 1.1.7 ist $\operatorname{ggT}(\nu^{k+1}, (n-1)(n-2)\cdot\ldots\cdot(n-\nu+1)) = 1$ und daher folgt $\nu^{k+1} \,|\, n$, ein Widerspruch. □

Gibt es eine Formel für Primzahlen?

Um auf diese häufig gestellte Frage eine präzise Antwort geben zu können, muss man sagen, was eine Formel sein soll. Natürlich ist etwa jedes (in einer beliebigen Programmiersprache verfasste) Programm zur Berechnung der Primzahlen nach dem Sieb des Eratosthenes eine Formel. Man wünscht sich aber „einfach zu berechnende Funktionen", welche die Primzahlen als Werte liefern.

Satz 1.2.5. *Sei $f\colon \mathbb{Z} \to \mathbb{Z}$ eine nichtkonstante Polynomfunktion. Dann gibt es unendlich viele $n \in \mathbb{Z}$ mit $|f(n)| \notin \mathbb{P}$.*

BEWEIS. Da f nicht konstant ist, folgt

$$\lim_{x \to \infty} |f(x)| = \infty\,.$$

Sei $a \in \mathbb{N}$ mit $|f(a)| > 1$ und $p \in \mathbb{P}$ mit $p \mid f(a)$. Wir zeigen: $p \mid f(a+kp)$ für alle $k \in \mathbb{Z}$. Da $|f(a+kp)| > p$ für fast alle $k \in \mathbb{N}$, folgt die Behauptung. Sei

$$f(x) = \sum_{i=0}^{n} c_i x^i \quad \text{mit} \quad n \in \mathbb{N} \ \text{ und } \ c_0, \ldots, c_n \in \mathbb{Z}\,.$$

Für $k \in \mathbb{Z}$ ist dann

$$f(a+kp) = f(a) + \sum_{i=1}^{n} c_i[(a+kp)^i - a^i] = f(a) + \sum_{i=1}^{n} c_i \sum_{\nu=1}^{i} \binom{i}{\nu} a^{i-\nu} k^\nu p^\nu \quad \text{durch } \ p \ \text{ teilbar.}$$

□

Bemerkungen 1.2.6.

1. Die Aussage von Satz 1.2.5 gilt auch für Polynomfunktionen mit komplexen Koeffizienten in mehreren Variablen (vgl. [**?**, Kapitel 3, III]). Andererseits gibt es eine ganzzahlige Polynomfunktion in 24 Variablen, deren sämtliche positiven Werte Primzahlen sind. Dies steht in engem Zusammenhang mit Hilbert's Zehntem Problem (vgl. [**?**, Kapitel 3, IV] und http://logic.pdmi.ras.ru/∼yumat/index.html, Personal Journal).

2. Kann eine nicht konstante Polynomfunktion mit ganzzahligen Koeffizienten unendlich viele Primzahlen darstellen? In diesem Zusammenhang gibt es eine Fülle von Vermutungen (Schinzel, Bouniakowski, Dickson). Ein zentrales Resultat ist die folgende qualitative Form des Dirichlet'schen Primzahlsatzes:

Sind a, $b \in \mathbb{N}$ und ist $\operatorname{ggT}(a,b) = 1$, so gibt es unendlich viele $n \in \mathbb{N}$, so dass $a + bn \in \mathbb{P}$.

3. Es gibt viele „Formeln", in denen die n-te Primzahl auftaucht. Diese sind aber nicht zur praktischen Berechnung geeignet.

Wie sind Primzahlen verteilt?

Definition 1.2.7. Für $x \in \mathbb{R}_{>0}$ sei

$$\pi(x) = |\{p \in \mathbb{P} \mid p \le x\}|$$

die Anzahl der Primzahlen mit $p \le x$.

Satz 1.2.8. *Zu jedem $N \in \mathbb{N}$ gibt es ein $n \in \mathbb{N}$ mit $p_{n+1} - p_n \ge N + 1$.*

Beweis. Sei $N \in \mathbb{N}$. Keine der N Zahlen

$$(N+1)! + 2,\ (N+1)! + 3,\ \ldots,\ (N+1)! + (N+1)$$

ist prim. Ist $p_n \in \mathbb{P}$ die größte Primzahl mit $p_n \le (N+1)! + 1$, so folgt $p_{n+1} \ge (N+1)! + (N+2)$ und daher $p_{n+1} - p_n \ge N + 1$. □

Bemerkungen 1.2.9.

1. Es ist unbekannt, ob ein $M \in \mathbb{N}$ existiert, so dass $p_{n+1} - p_n \le M$ für unendlich viele $n \in \mathbb{N}$. Man vermutet, dass bereits $M = 2$ diese Eigenschaft hat. Sind p und $p+2$ Primzahlen, so nennt man das Paar $(p, p+2)$ einen *Primzahlzwilling*, und man vermutet, dass es unendlich viele Primzahlzwillinge gibt. Allgemeiner ist die folgende *Primzahltupel-Vermutung*:

Sei $n \in \mathbb{N}$ und seien $a_1, \ldots, a_n \in \mathbb{N}$, so dass $\operatorname{ggT}\big(\{x(x+a_1)\cdot\ldots\cdot(x+a_n) \mid x \in \mathbb{N}\}\big) = 1$. Dann ist gibt es unendlich viele $x \in \mathbb{N}$, so dass $\{x, x+a_1, \ldots, x+a_n\} \subset \mathbb{P}$.

2. Für den Beweis der folgenden Sätze der Primzahltheorie verweisen wir auf [**?**, **?**, **?**]).

A. (*Ungleichungen von Tschebyscheff*: P.L. Tschebyscheff: 1821 - 1894)

(a) Es existieren $a_1, a_2 \in \mathbb{R}_{>0}$ mit

$$a_1 \frac{x}{\log x} < \pi(x) < a_2 \frac{x}{\log x}.$$

(b) Es existieren $a_1, a_2 \in \mathbb{R}_{>0}$ mit

$$a_1 n \log n < p_n < a_2 n \log n.$$

B. (*Bertrand'sches Postulat*; J. Bertrand: 1822 - 1900)
Für alle $a \in \mathbb{N}$ existiert ein $p \in \mathbb{P}$ mit $a < p \leq 2a$.

C. (*Primzahlsatz*; J. Hadamard (1865-1963) und Charles de la Vallée Poussin (1866-1962) konnten 1896 unabhängig voneinander den ersten Beweis geben)

$$\lim_{x\to\infty} \frac{\pi(x)}{\frac{x}{\log x}} = 1.$$

D. (*Dirichlet'scher Primzahlsatz*). Seien $a,\, b \in \mathbb{N}$ und $\mathrm{ggT}(a,b) = 1$. Dann ist

$$\lim_{x\to\infty} \frac{|\{a+kb \mid k \in \mathbb{N},\ k \leq x\}|}{\frac{x}{\log x}} = 1\,.$$

Folgende Implikationen sind einfach nachzuprüfen: $\mathrm{A\,(a)} \Rightarrow \mathrm{A\,(b)}$ und $\mathrm{C} \Rightarrow \mathrm{A}$.
Das entscheidende Hilfsmittel für 3. ist die *Riemann'sche Zetafunktion*

$$\zeta(s) = \sum_{n=1}^{\infty} \frac{1}{n^s} = \prod_{p\in\mathbb{P}} \frac{1}{1-p^{-s}} \qquad \text{für} \qquad \Re(s) > 1\,,$$

die mit Methoden der Komplexen Analysis studiert wird.

Fermat'sche und Mersenne'sche Primzahlen

Definition und Satz 1.2.10. *Seien $a, n \in \mathbb{N}$ mit $a \geq 2$.*

1. *Ist $a^n + 1 \in \mathbb{P}$, so ist a gerade und $n = 2^m$ mit $m \in \mathbb{N}_0$.*
2. *Ist $a^n - 1 \in \mathbb{P}$ und $n \geq 2$, so ist $a = 2$ und $n \in \mathbb{P}$.*

Für $n \in \mathbb{N}_0$ heißt $F_n = 2^{2^n} + 1$ die n-te *Fermat'sche Zahl*, und für $n \in \mathbb{N}$ heißt $M_n = 2^n - 1$ die n-te *Mersenne'sche Zahl*. Man nennt eine Primzahl eine *Mersenne'sche Primzahl* bzw. eine *Fermat'sche Primzahl*, wenn sie ein Mersenne'sche bzw. eine Fermat'sche Zahl ist.

Beweis. 1. Sei $a^n + 1$ prim. Wäre a ungerade, so wäre $a^n + 1$ gerade, was wegen $a^n + 1 \geq a + 1 \geq 3$ unmöglich ist. Also ist a gerade. Angenommen, $n > 1$ ist keine 2-Potenz. Dann ist $n = st$ mit $s, t \in \mathbb{N}$, so dass $t > 1$ ungerade ist. Damit folgt

$$1 + a^n = 1 - (-a^s)^t = (1 + a^s) \sum_{i=0}^{t-1} (-a^s)^i\,, \quad \text{und beide Faktoren sind in } \mathbb{N}_{>1}, \text{ ein Widerspruch}\,.$$

2. Sei $n \geq 2$ und $a^n - 1 \in \mathbb{P}$. Dann ist $a - 1 \,|\, a^n - 1$ und $a - 1 < a^n - 1$, also $a = 2$. Angenommen, $n \notin \mathbb{P}$, also $n = st$ mit $s > 1$ und $t > 1$. Dann folgt

$$2^n - 1 = \big((2^s)^t - 1\big) = (2^s - 1) \sum_{i=0}^{t-1} 2^{si}\,, \quad \text{und beide Faktoren sind in } \mathbb{N}_{>1}, \text{ ein Widerspruch}\,.$$

□

Bemerkungen 1.2.11. Es ist $F_0 = 3$, $F_1 = 5$, $F_2 = 17$, $F_3 = 257$ und $F_4 = 65537$. Dies sind alles Primzahlen, aber $F_5 = 2^{32} + 1$ ist durch 641 teilbar (wie Euler bemerkte). Bisher kennt man keine Primzahl F_n mit $n > 4$. Die Fermat'schen Primzahlen spielen bei der Konstruktion des regelmäßigen n-Ecks eine Rolle. In Korollar 8.4.6 werden wir zeigen:

Für $n \in \mathbb{N}_{\geq 3}$ ist das regelmäßige n-Eck genau dann mit Zirkel und Lineal konstruierbar, wenn $n = 2^e p_1 \cdot \ldots \cdot p_r$ mit $e, r \in \mathbb{N}_0$ und verschiedenen Fermat'schen Primzahlen $p_1, \ldots, p_r$.

Ist $n \in \mathbb{N}$ mit $M_n \in \mathbb{P}$ prim, so ist nach Satz 1.2.10 auch $n \in \mathbb{P}$, aber $M_{11} = 2047 = 23 \cdot 89$. Man vermutet, dass es unendlich viele Mersenne'sche Primzahlen gibt.

Das Aufsuchen Mersenne'scher Primzahlen und die Faktorisierung Fermat'scher Zahlen gehören zum Hochleistungssport der numerischen Zahlentheorie. Über den aktuellen Stand kann man sich auf den Seiten *www.mersenne.org* und *http://www.prothsearch.net/fermat.html* informieren.

Definition 1.2.12. Für $n \in \mathbb{N}$ sei

$$\sigma(n) = \sum_{\substack{d \in \mathbb{N} \\ d \mid n}} d \qquad \text{die Summe der positiven Teiler von } n\,.$$

Man nennt n *vollkommen*, wenn $\sigma(n) = 2n$.

Es ist unbekannt, ob es eine ungerade vollkommene Zahl gibt. Gerade vollkommenene Zahlen lassen sich wie folgt durch die Mersenne'schen Primzahlen charakterisieren.

Satz 1.2.13. *Für eine gerade Zahl $n \in \mathbb{N}$ sind folgende Bedingungen äquivalent:*

(a) *n ist vollkommen.*

(b) *$n = 2^{p-1} M_p$ mit $p \in \mathbb{P}$, so dass $M_p \in \mathbb{P}$.*

Beweis. (b) $\Rightarrow$ (a) (Euklid) Sei $p \in \mathbb{P}$ und $M_p = 2^p - 1 \in \mathbb{P}$. Dann ist

$$\sigma(2^{p-1} M_p) = \sum_{i=0}^{p-1} 2^i + \sum_{i=0}^{p-1} 2^i M_p = (2^p - 1)(1 + M_p) = 2^p M_p\,.$$

(a) $\Rightarrow$ (b) (Euler) Sei $n = 2^{k-1} m$ mit $k \geq 2$ und m ungerade. Dann ist

$$2n = 2^k m = \sigma(n) = \sum_{i=0}^{k-1} 2^i \sum_{\substack{d \in \mathbb{N} \\ d \mid m}} d = (2^k - 1)\sigma(m)$$

und daher $2^k \mid \sigma(m)$ nach Satz 1.1.7.2, also $\sigma(m) = 2^k l$ mit $l \in \mathbb{N}$ und $m = (2^k - 1)l$. Wäre $l > 1$, so wären 1, l und m verschiedene Teiler von m und daher $\sigma(m) \geq 1 + l + m = 1 + 2^k l > \sigma(m)$, ein Widerspruch. Also ist $l = 1$ und $n = 2^{k-1} m = 2^{k-1}(2^k - 1)$. Wegen $\sigma(m) = 2^k = 1 + m$ ist $m = 2^k - 1 \in \mathbb{P}$, und daher $k \in \mathbb{P}$ nach Satz 1.2.10. $\square$

CHAPTER 2

Elementare Gruppentheorie

2.1. Verknüpfungen

Definition 2.1.1. Sei H eine nichtleere Menge.

1. Eine *Verknüpfung* (oder *binäre Operation*) auf H ist eine Abbildung
$$*\colon \begin{cases} H \times H & \to \ H \\ (a,b) & \mapsto \ a*b \end{cases}$$
$a*b$ heißt *Verknüpfungsergebnis* von a und b.
2. Eine Verknüpfung $*$ auf H heißt
   - *assoziativ*, wenn $a*(b*c) = (a*b)*c$ für alle $a,b,c \in H$.
   - *kommutativ*, wenn $a*b = b*a$ für alle $a,b \in H$.
3. Sei $*$ eine Verknüpfung auf H. Ein Element $e \in H$ heißt *neutrales Element* (bzgl. $*$), falls $a*e = e*a = a$ für alle $a \in H$.
4. Sei $*$ eine Verknüpfung auf H. Ein Element $c \in H$ heißt *kürzbar*, wenn für alle $a, b \in H$ gilt:
$$c*a = c*b \ \Rightarrow \ a = b \quad \text{und} \quad a*c = b*c \ \Rightarrow \ a = b\,.$$
Wir bezeichnen mit $(H,*)^\bullet$ die Menge der kürzbaren Elemente von H.
5. Sei $*$ eine Verknüpfung auf H. Eine Teilmenge $U \subset H$ heißt *$*$-abgeschlossen*, wenn $a*b \in U$ für alle $a, b \in U$. Dann nennt man $*\,|\,U{\times}U\colon U{\times}U \to U$ die von $*$ auf U induzierte Verknüpfung.

Bemerkung 2.1.2. Sei H eine nichtleere Menge und $*$ eine Verknüpfung auf H. Dann gibt es in H höchstens ein neutrales Element bzgl. $*$. [Beweis: Sind e und e' neutrale Elemente von H, so folgt $e = e*e' = e'$.]

Definition 2.1.3.

1. Eine *Halbgruppe* $(H,*)$ ist eine nichtleere Menge H, gemeinsam mit einer assoziativen Verknüpfung $*$ auf H, so dass H ein neutrales Element bzgl. $*$ besitzt (dieses nennt man dann das neutrale Element von $(H,*)$).
2. Sei $(H,*)$ eine Halbgruppe mit neutralem Element e und $a \in H$.
   Ein Element $a' \in H$ heißt ein *Inverses von a* (bzgl. $*$), wenn $a*a' = a'*a = e$. Das Element a heißt *invertierbar* (bzgl. $*$ in H), wenn es ein Inverses besitzt.
   Die Menge $(H,*)^\times$ der invertierbaren Elemente von H heißt *Einheitengruppe von H*.
3. Eine *Gruppe* ist eine Halbgruppe, in der jedes Element invertierbar ist.
4. Eine Halbgruppe (bzw. Gruppe) heißt *kommutativ* oder *abelsch*, wenn ihre Verknüpfung kommutativ ist.
5. Ein *Monoid* ist eine kommutative Halbgruppe, in der jedes Element kürzbar ist.

Bemerkungen und Konventionen 2.1.4.

1. Die Definition der Halbgruppe und des Monoids ist in der Literatur nicht eindeutig. Häufig wird (anders als in diesem Skriptum) unter einer Halbgruppe bloß eine nichtleere Menge mit einer assoziativen Verknüpfung und unter einem Monoid eine Halbgruppe mit neutralem Element verstanden.

2. Sei H eine nichtleere Menge und $*$ eine Verknüpfung auf H. Ist aus dem Zusammenhang klar, um welche Verküpfung es sich handelt, so schreibt man kurz H an Stelle von $(H,*)$, $H^\bullet$ an Stelle von $(H,*)^\bullet$ und (im Falle der Existenz eines neutralen Elements bzgl. $*$) auch $H^\times$ an Stelle von $(H,*)^\times$. Insbesondere ist eine Halbgruppe H genau dann eine Gruppe, wenn $H = H^\times$, und eine kommutative Halbgrupe H ist genau dann ein Monoid, wenn $H = H^\bullet$.

3. Sei $*$ eine Verknüpfung auf eine nichtleeren Menge H. Für $a \in H$ und Teilmengen A, $B \subset H$ setzt man $a * B = \{a * b \mid b \in B\}$ und $A * B = \{a * b \mid a \in A, b \in B\}$.

Lemma 2.1.5. *Sei $H = (H,*)$ eine Halbgruppe mit neutralem Element e.*

1. *Jedes Element $a \in H$ besitzt höchstens ein Inverses. Bezeichnet man dieses mit a', so gilt:*
   (a) *$e \in H^\times$ und $e' = e$.*
   (b) *Ist $a \in H^\times$, so folgt $a' \in H^\times$ und $(a')' = a$.*
   (c) *Sind $a, b \in H^\times$, so ist auch $a * b \in H^\times$ und $(a * b)' = b' * a'$.*
2. *$H^\times = (H^\times, * \,|\, H^\times \times H^\times)$ ist eine Gruppe.*
3. *$H^\times \subset H^\bullet$. Insbesondere ist jede abelsche Gruppe ein Monoid.*
4. *Sind u, $v \in H^\bullet$, so ist auch $u * v \in H^\bullet$.*

Beweis. 1. Sei $a \in H$. Sind a' und $\widetilde{a}$ Inverse von a, so folgt

$$a' = a' * e = a' * (a * \widetilde{a}) = (a' * a) * \widetilde{a} = e * \widetilde{a} = \widetilde{a}\,.$$

1.(a) Wegen $e * e = e$ ist e das Inverse von e.

1.(b) Wegen $a * a' = a' * a = e$ ist a das Inverse von a'.

1.(c) Es ist $(a * b) * (b' * a') = \big((a * b) * b'\big) * a' = \big(a * (b * b')\big) * a' = \big(a * e\big) * a' = a * a' = e$, und in gleicher Weise folgt $(b' * a') * (a * b) = e$. Daher ist $b' * a'$ das Inverse von $a * b$.

2. Nach 1.(c) ist $H^\times$ $*$-abgeschlossen, und wegen 1.(a) und 1.(b) ist $H^\times$ mit der induzierten Verknüpfung eine Gruppe.

3. Sei $c \in H^\times$, und seien a, $b \in H$. Ist dann $c * a = c * b$, so folgt

$$a = e * a = (c' * c) * a = c' * (c * a) = c' * (c * b) = (c' * c) * b = e * b = b\,.$$

Ebenso zeigt man: Aus $a * c = b * c$ folgt $a = b$.

4. Seien u, $v \in H^\bullet$ und a, $b \in H$ mit $(u * v) * a = (u * v) * b$. Dann ist auch $u * (v * a) = u * (v * b)$, also $v * a = v * b$ und daher $a = b$. In gleicher Weise zeigt man: Aus $a * (u * v) = b * (u * v)$ folgt $a = b$. □

Beispiele und Konventionen 2.1.6.

1. Sei $G = \{e\}$ eine Menge mit einem Element. Dann gibt es genau eine Verknüpfung $*$ auf G, und bezüglich dieser ist $e * e = e$. $G = (G,*)$ ist eine Gruppe, die *triviale Gruppe* oder *Einsgruppe*.

2. Sei G eine der Mengen $\mathbb{N}_0$, $\mathbb{N}$, $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$. Dann sind die (gewöhnliche) Addition

$$+\colon \begin{cases} G \times G & \to & G \\ (a,b) & \mapsto & a+b \end{cases} \qquad \text{und die (gewöhnliche) Multiplikation} \qquad \cdot\colon \begin{cases} G \times G & \to & G \\ (a,b) & \mapsto & ab = a \cdot b \end{cases}$$

kommutative und assoziative Verknüpfungen auf G.

$(\mathbb{N}_0, +)$ ist ein (additives) Monoid mit neutralem Element 0 und Einheitengruppe $(\mathbb{N}_0,+)^\times = \{0\}$ (die triviale Gruppe). $(\mathbb{Z}, +)$ ist eine additive abelsche Gruppe mit neutralem Element 0.

$(\mathbb{N}_0,\cdot)$ ist eine (multiplikative) Halbgruppe, $(\mathbb{N},\cdot)$, $H=(4\mathbb{N}_0+1,\cdot)$ und $(\mathbb{Z},\cdot)$ sind (multiplikative) Monoide mit neutralem Element 1 und Einheitengruppen $(\mathbb{N},\cdot)^\times=H^\times=\{1\}$ und $(\mathbb{Z}^\bullet,\cdot)^\times=\{\pm 1\}$ (eine Gruppe mit 2 Elementen).

Wichtige Beispiele für Monoide sind die multiplikativen Monoide von Bereichen (siehe Lemma 3.1.6.4).

3. Wir erinnern an die Lineare Algebra. Ein *Körper* $(K,0_K,1_K,+_K,\cdot_K)$ ist eine Menge K, gemeinsam mit zwei ausgezeichneten Elementen $0_K\in K$ und $1_K\in K$ und zwei Verknüpfungen $+_K\colon K\times K\to K$ (Addition) und $\cdot_K\colon K\times K\to K$ (Multiplikation) derart, daß gilt:

(1) $(K,+_K)$ ist eine abelsche Gruppe mit neutralem Element 0_K.

(2) $(K,\cdot_K)$ ist eine abelsche Halbgruppe mit neutralem Element 1_K.

(3) $(K,\cdot_K)^\times=K\setminus\{0_K\}$.

(4) Es gilt das Distributivgesetz: Für alle $a,b,c\in K$ ist $(a+_K b)\cdot_K c=(a\cdot_K c)+_K(b\cdot_K c)$.

Entsprechend den Konventionen in 2.1.4.2 schreiben wir (falls Verwechslungen nicht zu befürchten sind) kurz K an Stelle von $(K,0_K,1_K,+_K,\cdot_K)$, $+$ an Stelle von $+_K$, $\cdot$ an Stelle von $\cdot_K$, 0 an Stelle von 0_K, 1 an Stelle von 1_K und $K^\times$ an Stelle von $(K,\cdot)^\times$. $\mathbb{Q}$, $\mathbb{R}$ und $\mathbb{C}$ sind Körper.

Man nennt $(K,+)$ die *Additionsgruppe* und $K^\times=(K^\times,\cdot)$ die *Multiplikationsgruppe* von K.

Ein K-*Vektorraum* V ist eine (additive) abelsche Gruppe $(V,+)$, gemeinsam mit einer K-linearen Struktur

$$\begin{cases} K\times V & \to\ V \\ (\lambda,v) & \mapsto\ \lambda v \end{cases}$$

derart, daß die Vektorraum-Axiome gelten (es kommt hier auf diese nicht im Einzelnen an). $(V,+)$ heißt *Vektorgruppe* oder *Additionsgruppe* von V.

Wichtige Beispiele für K-Vektorräume sind der Spalten- bzw. Zeilenraum K^n und der Raum $\mathsf{M}_{m,n}(K)$ der (m,n)-Matrizen über K (für $m,n\in\mathbb{N}$).

4. **Additive Konventionen**. Schreibt man die Verknüpfung auf einer nichtleeren Menge H als Addition, also $+\colon H\times H\to H$, $(a,b)\mapsto a+b$, so setzt man (stillschweigend) stets voraus, daß $+$ kommutativ und assoziativ ist. Man bezeichnet dann ein neutrales Element mit $0=0_H$ (und nennt es das *Nullelement* oder die *Null* von H). Man nennt dann $H=(H,+)$ eine *additive Halbgruppe* bzw. ein *additives Monoid* oder eine *additive* (*abelsche*) *Gruppe*. Das Inverse eines Elements $a\in H$ bezüglich $+$ bezeichnet man mit $-a$ (und nennt es das *Negative* von a). Für $a,b\in H$ definiert man $a-b=a+(-b)$ und nennt $a-b$ die *Differenz* von a und b (durch diese Einführung der Differenz erübrigt sich die in der didaktischen Literatur geführte Diskussion, wann das Minuszeichen ein Vorzeichen und wann es ein Rechenzeichen ist).

Ist $(H,+)$ eine additive Gruppe, so ist $-\colon H\times H\to H$ eine Verknüpfung auf H, welche im allgemeinen weder kommutativ noch assoziativ ist.

Beispiele für additive Gruppen sind $(\mathbb{Z},+)$ und die Additionsgruppen von Körpern und Vektorräumen.

5. **Multiplikative Konventionen**. Schreibt man die Verknüpfung auf einer nichtleeren Menge H also Multiplikation, also $\cdot\colon H\times H\to H$, $(a,b)\mapsto a\cdot b$, so setzt man (stillschweigend) stets voraus, daß $\cdot$ assoziativ ist. Man bezeichnet dann ein neutrales Element mit e oder auch mit $1=1_H$ (und nennt es das *Einselement* oder die *Eins* von H). Man nennt dann $H=(H,\cdot)$ eine *multiplikative Halbgruppe* bzw. ein *multiplikatives Monoid* oder eine *multiplikative Gruppe*. Für $a,b\in H$ schreibt man ab an Stelle von $a\cdot b$, und man bezeichnet das Inverse eines invertierbaren Elements $a\in H$ mit a^{-1}. Ist $\cdot$ kommutativ, so verwendet man auch die Bruchschreibweise: Für $a\in H^\times$, $b\in H$ setzt man

$$\frac{b}{a}\ =\ ba^{-1}\ =\ a^{-1}b\ \in H\,.$$

Beispiele für multiplikative Halbgruppen: Sei K ein Körper und $n\in\mathbb{N}$. Dann ist $(\mathsf{M}_n(K),\cdot)$ eine multiplikative Halbgruppe (die multiplikative Halbgruppe der n-reihigen quadratischen Matrizen über

K), die Einheitsmatrix ist das Einselement von $\mathsf{M}_n(K)$, und $\mathsf{GL}_n(K) = \mathsf{M}_n(K)^\times = \{A \in M_n(K) \mid \det(A) \neq 0\}$. Speziell ist $\mathsf{M}_1(K) = K$ und $\mathsf{GL}_1(K) = K^\times$.

$(\mathbb{N}_0, \cdot)$, $(\mathbb{N}, \cdot)$ und $(\mathbb{Z}, \cdot)$ sind multiplikative Halbgruppen.

6. **Komponentenweise Verknüpfung**. Sei $(H_i)_{i\in I}$ eine Familie nichtleerer Mengen. Für jedes $i \in I$ sei $*_i \colon H_i \times H_i \to H_i$ eine Verknüpfung auf H_i. Dann definiert man das Produkt

$$H = \prod_{i\in I} H_i = \{(a_i)_{i\in I} \mid a_i \in H_i\} \quad \text{und} \quad * \colon H \times H \to H \quad \text{durch} \quad (a_i)_{i\in I} * (b_i)_{i\in I} = (a_i *_i b_i)_{i\in I}\,.$$

Man nennt $*$ die von der Familie $(*_i)_{i\in I}$ induzierte *komponentenweise Verknüpfung* auf H und $(H, *)$ das (*äußere*) *direkte Produkt* der Familie $\big((H_i, *_i)\big)_{i\in I}$.

Die Verknüpfung $*$ ist genau dann assoziativ bzw. kommutativ, wenn alle $*_i$ assoziativ bzw. kommutativ sind. Eine Familie $e = (e_i)_{i\in I} \in H$ ist genau dann ein neutrales Element bzgl. $*$, wenn jedes e_i ein neutrales Element bzgl. $*_i$ ist. In diesem Falle ist eine Familie $a = (a_i)_{i\in I} \in H$ genau dann invertierbar in H, wenn alle a_i in H_i invertierbar sind. Ist dies der Fall und bezeichnet a_i' für jedes $i \in I$ das Inverse von a_i in H_i, so ist die Familie $a' = (a_i')_{i\in I}$ das Inverse von a in H. Eine Familie $a = (a_i)_{i\in I} \in H$ ist genau dann kürzbar, wenn alle a_i kürzbar sind.

Insbesondere gilt: Ist $(H_i)_{i\in I}$ eine Familie von Halbgruppen, so ist

$$H = \prod_{i\in I} H_i \quad \text{eine Halbgruppe,} \quad H^\times = \prod_{i\in I} H_i^\times\,, \quad H^\bullet = \prod_{i\in I} H_i^\bullet\,,$$

und H ist genau dann ein Monoid bzw. eine Gruppe, wenn alle H_i Monoide bzw. Gruppen sind. (Die Beweise aller dieser Aussagen sind einfache Übungsaufgaben.)

Im Spezialfall $I = [1, n]$ (mit $n \in \mathbb{N}$) schreibt man

$$\prod_{i\in I} H_i = \prod_{i=1}^{n} H_i = H_1 \times \ldots \times H_n\,, \quad (a_i)_{i\in I} = (a_1, \ldots, a_n)\,,$$

und dann ist $(a_1, \ldots, a_n) * (b_1, \ldots, b_n) = (a_1 *_1 b_1, \ldots, a_n *_n b_n)$.

Ist K ein Körper, so ist die Additionsgruppe $(K^n, +)$ das n-fache direkte Produkt von $(K, +)$ mit sich selbst: $K^n = K \times \cdots \times K$.

Ist $(H_i)_{i\in I}$ eine konstante Familie, also etwa $H_i = G$ für alle $i \in I$, so bezeichnet man ihr Produkt mit G^I, also

$$G^I = \prod_{i\in I} H_i\,.$$

7. **Wertweise Verknüpfung**. Seien X und H nichtleere Mengen und $\mathrm{Abb}(X, H)$ die Menge aller Abbildungen $f \colon X \to H$. Identifiziert man eine Abbildung $f \colon X \to H$ mit der Familie der Bilder $\big(f(x)\big)_{x\in X} \in H^X$, so folgt

$$\mathrm{Abb}(X, H) = H^X = \prod_{x\in X} H\,.$$

Ist $*$ eine Verknüpfung auf H, so nennt man die nach 6. von der konstanten Familie $(*)_{x\in X}$ auf $\mathrm{Abb}(X, H) = H^X$ induzierte komponentenweise Verknüpfung $\overline{*}$ die von $*$ induzierte *wertweise Verknüpfung* auf $\mathrm{Abb}(X, H)$. Für zwei Abbildungen $f, g \colon X \to H$ ist dann $f \overline{*} g \colon X \to H$ gegeben durch $(f \overline{*} g)(x) = f(x) * g(x)$. Die wertweise Verknüpfung $\overline{*}$ ist genau dann assoziativ bzw. kommutativ, wenn $*$ das ist.

Für $z \in H$ bezeichne $\mathsf{c}_z \colon X \to H$ die konstante Abbildung mit Wert z. Für alle $x, y \in H$ ist dann $\mathsf{c}_x \overline{*} \mathsf{c}_y = \mathsf{c}_{x*y}$. Ist $e \in H$ ein neutrales Element bzgl. $*$, so ist $\mathsf{c}_e \in \mathrm{Abb}(X, H)$ ein neutrales Element bzgl. $\overline{*}$. In diesem Falle ist eine Abbildung $f \in \mathrm{Abb}(X, H)$ genau dann invertierbar bzgl. $\overline{*}$, wenn für alle $x \in X$ das Element $f(x) \in H$ invertierbar bzgl. $*$ ist; bezeichnet $f(x)'$ das Inverse von $f(x)$ in H, so ist das Inverse f' von f in $\mathrm{Abb}(X, H)$ gegeben durch $f'(x) = f(x)'$ für alle $x \in X$.

Sind Verwechslungen nicht zu befürchten, so schreibt man wieder $*$ an Stelle von $\overline{*}$ und identifiziert die Elemente $z \in H$ mit den konstanten Abbildungen c_z.

Insbesondere gilt: Ist H eine Halbgruppe, so ist auch $\mathrm{Abb}(X,H)$ eine Halbgruppe mit Einheitengruppe $\mathrm{Abb}(X,H)^\times = \mathrm{Abb}(X,H^\times)$, und $\mathrm{Abb}(X,H)$ ist genau dann ein Monoid bzw. eine Gruppe, wenn H das ist.

Ist K ein Körper, so ist $\mathrm{Abb}(X,K)$ bezüglich der wertweisen Addition eine (abelsche) Gruppe und bezüglich der wertweisen Multiplikation eine kommutative Halbgruppe. Eine Abbildung $f \in \mathrm{Abb}(X,K)$ ist genau dann (multiplikativ) invertierbar, wenn $f(x) \neq 0$ für alle $x \in X$, und dann ist die Funktion $x \mapsto 1/f(x)$ das Inverse von f.

8. **Verknüpfungstabellen**. Sei $n \in \mathbb{N}$ und $H = \{a_1, \ldots, a_n\}$ eine Menge mit n Elementen. Eine Verknüpfung $*\colon H \times H \to H$ ist vollständig bestimmt durch die quadratische Matrix

$$(a_i * a_j)_{i,j\in[1,n]} \in \mathsf{M}_n(H)\,,$$

welche man als *Verknüpfungstabelle* notiert:

$*$	a_1	$\ldots$	a_j	$\ldots$	a_n
a_1	$a_1 * a_1$	$\ldots$	$a_1 * a_j$	$\ldots$	$a_1 * a_n$
$\vdots$	$\vdots$		$\vdots$		$\vdots$
a_i	$a_i * a_1$	$\ldots$	$a_i * a_j$	$\ldots$	$a_i * a_n$
$\vdots$	$\vdots$		$\vdots$		$\vdots$
a_n	$a_n * a_1$	$\ldots$	$a_n * a_j$	$\ldots$	$a_n * a_n$

Beispiel 1. Sei $H = \{e, a\}$ eine Menge mit zwei Elementen. Dann gibt es genau zwei Verknüpfungen auf H mit e als neutralem Element, welche wie folgt durch die Verknüpfungstabellen gegeben sind:

$*$	e	a
e	e	a
a	a	e

$\circledast$	e	a
e	e	a
a	a	a

$(G,*)$ ist eine abelsche Gruppe, $(G,\circledast)$ ist eine abelsche Halbgruppe mit $(G,\circledast)^\times = \{e\}$.

Beispiel 2. $\mathbb{F}_2 = \{\mathbf{0},\mathbf{1}\}$ sei Menge mit zwei Elementen. Dann gibt es gemäß Beispiel 1 auf $\mathbb{F}_2$ genau eine Verknüpfung $+$ mit neutralem Element $\mathbf{0}$, so dass $(\mathbb{F}_2,\mathbf{0})$ eine Gruppe ist, und es gibt genau eine Verknüpfung $\cdot$ mit neutralem Element $\mathbf{1}$, so dass $(\mathbb{F}_2,\cdot)$ keine Gruppe ist. Die Verknüpfungstabellen sind:

$+$	$\mathbf{0}$	$\mathbf{1}$
$\mathbf{0}$	$\mathbf{0}$	$\mathbf{1}$
$\mathbf{1}$	$\mathbf{1}$	$\mathbf{0}$

$\cdot$	$\mathbf{0}$	$\mathbf{1}$
$\mathbf{0}$	$\mathbf{0}$	$\mathbf{0}$
$\mathbf{1}$	$\mathbf{0}$	$\mathbf{1}$

Dann ist $\mathbb{F}_2 = (\mathbb{F}_2, \mathbf{0}, \mathbf{1}, +, \cdot)$ ein Körper. (Das Nachrechnen des Distributivgesetzes ist eine einfache Übungsaufgabe).

9. Sei X eine nichtleere Menge und $G = \mathrm{Abb}(X,X)$. Dann ist

$$\circ\colon \begin{cases} G\times G & \to & G \\ (f,g) & \mapsto & f \circ g \end{cases}$$

eine Verknüpfung auf G. $(G,\circ)$ ist eine Halbgruppe mit neutralem Element id_X. Genau dann ist $(G,\circ)$ abelsch, wenn $|X|=1$ (Beweis!). Genau dann ist $f\in G$ invertierbar bzgl. $\circ$, wenn f bijektiv ist, und dann ist die Umkehrfunktion $f^{-1}\in G$ das Inverse von f bzgl. $\circ$. Die Gruppe

$$\mathfrak{S}(X)=(G,\circ)^\times=\{f\in \mathrm{Abb}(X,X)\mid f \quad \text{bijektiv}\}$$

heißt *symmetrische Gruppe auf* X. Genau dann ist $\mathfrak{S}(X)$ abelsch, wenn $|X|\le 2$ (Beweis!).
Ist X endlich, $|X|=n\in\mathbb{N}$, so folgt

$$|\mathrm{Abb}(X,X)|=n^n \quad \text{und} \quad |\mathfrak{S}(X)|=n! \qquad (\text{Beweis durch Induktion nach } n).$$

Im Falle $X=[1,n]$ heißt $\mathfrak{S}_n=\mathfrak{S}\big([1,n]\big)$ die *symmetrische Gruppe auf* n *Ziffern*, die $\sigma\in\mathfrak{S}_n$ heißen *Permutationen* (*von* n *Ziffern*).

Definition 2.1.7 (**Verknüpfung mehrerer Elemente, Potenzen).** Sei H eine nichtleere Menge und $*$ eine Verknüpfung auf H. Für $n\in\mathbb{N}$ und $a_1,\dots,a_n\in H$ definiert man

$$\overset{n}{\underset{i=1}{*}} a_i\in H \quad \text{rekursiv durch} \qquad \overset{1}{\underset{i=1}{*}} a_i=a_1 \quad \text{und} \quad \overset{n}{\underset{i=1}{*}} a_i=\Big(\overset{n-1}{\underset{i=1}{*}} a_i\Big)*a_n\,.$$

Ist $e\in H$ ein neutrales Element bzgl. $*$, so definiert man

$$\overset{0}{\underset{i=1}{*}} a_i=e \quad (\text{leere Verknüpfung})\,.$$

Sind $p,q\in\mathbb{Z}$, $p\le q+1$ und $a_p,a_{p+1},\dots,a_q\in H$, so definiert man

$$\overset{q}{\underset{i=p}{*}} a_i \;=\; \overset{q-p+1}{\underset{i=1}{*}} a_{p-1+i}\,.$$

Schreibweisen:

$$\overset{n}{\underset{i=1}{*}} a_i \;=\; a_1*a_2*\cdots*a_n\,;$$

$$\overset{n}{\underset{i=1}{+}} a_i \;=\; \sum_{i=1}^n a_i \;=\; a_1+\cdots+a_n \quad \text{im Falle } *=+ \quad (\text{additive Konvention})\,;$$

$$\overset{n}{\underset{i=1}{\cdot}} a_i \;=\; \prod_{i=1}^n a_i \;=\; a_1\cdot\cdots\cdot a_n \quad \text{im Falle } *=\cdot \quad (\text{multiplikative Konvention})\,.$$

Für $a\in H$ und $n\in\mathbb{N}$ definiert man

$$a^n=a^{*n}=\overset{n}{\underset{i=1}{*}} a \quad \text{und} \quad (\text{falls } e\in H \text{ ein neutrales Element bzgl. } * \text{ ist}) \quad a^0=a^{*0}=e\,,$$

Ist H eine Halbgruppe, $a\in H^\times$, $a'\in H$ das Inverse von a und $n\in\mathbb{N}$, so definiert man

$$a^{-n}=a^{*(-n)}=a'^n\,.$$

Im Falle $*=\cdot$ ist $a^{-n}=(a^{-1})^n$ (und das ist mit der multiplikativen Konvention, das Inverse von a mit a^{-1} zu bezeichnen, kompatibel).
Im Falle $*=+$ schreibt man na an Stelle von a^{+n} und nennt na das n*-fache* von a.
Im Falle $H=\mathbb{Z}$ hat na für $n,a\in\mathbb{Z}$ zwei Bedeutungen: Es ist einerseits das n-fache von a und anderseits das Produkt aus n und a. Die beiden stimmen aber überein [Beweis: Zuerst für $n\in\mathbb{N}_0$ durch Induktion nach n und dann für $n=-k$ mit $k\in\mathbb{N}$ nach Definition].

Lemma 2.1.8 (Rechenregeln)**.** *Sei* $(H,*)$ *eine Halbgruppe.*

1. *Sind* $k,n\in\mathbb{N}_0$ *und* $a_1,\dots,a_{n+k}\in H$*, so ist*

$$\overset{n+k}{\underset{i=1}{*}} a_i \;=\; \Big(\overset{n}{\underset{i=1}{*}} a_i\Big)*\Big(\overset{n+k}{\underset{i=n+1}{*}} a_i\Big)$$

2. *Sei* $a \in H$.
   (a) $a^m * a^n = a^{m+n}$.
   (b) $(a^m)^n = a^{mn}$.
   (c) *Ist* $b \in H$ *und* $a * b = b * a$, *so folgt* $(a * b)^n = a^n * b^n$.

   (a), (b) *und* (c) *gelten für alle* $m, n \in \mathbb{N}_0$. *Ist* $a \in H^\times$, *so gelten* (a) *und* (b) *für alle* $m, n \in \mathbb{Z}$. *Ist* $a \in H^\times$ *und* $b \in H^\times$, *so gilt* (c) *für alle* $n \in \mathbb{Z}$.

3. (Allgemeines Kommutativgesetz) *Ist* $*$ *kommutativ und sind* $n \in \mathbb{N}$, $a_1, \ldots, a_n \in H$ *und* $\sigma \in \mathfrak{S}_n$, *so ist*

$$\mathop{*}_{i=1}^{n} a_i \;=\; \mathop{*}_{i=1}^{n} a_{\sigma(i)}\,.$$

BEWEIS. 1. Induktion nach k. Für $k = 0$ ist nichts zu zeigen.
$k \geq 0$, $k \to k+1$: Mit Hilfe des Assoziativgesetzes und der Induktionsvoraussetzung folgt

$$\begin{aligned}\mathop{*}_{i=1}^{n+k+1} a_i &= \left(\mathop{*}_{i=1}^{n+k} a_i\right) * a_{n+k+1} = \left[\left(\mathop{*}_{i=1}^{n} a_i\right) * \left(\mathop{*}_{i=n+1}^{n+k} a_i\right)\right] * a_{n+k+1} \\ &= \left(\mathop{*}_{i=1}^{n} a_i\right) * \left[\left(\mathop{*}_{i=n+1}^{n+k} a_i\right) * a_{n+k+1}\right] = \left(\mathop{*}_{i=1}^{n} a_i\right) * \left(\mathop{*}_{i=n+1}^{n+k+1} a_i\right).\end{aligned}$$

2.(a) FALL 1: $m, n \geq 0$. Die Behauptung folgt aus 1.

FALL 2: $m > 0$, $n = -1$. Wegen $m-1 \geq 0$ ist $a^m * a^{-1} = (a^{m-1} * a) * a^{-1} = a^{m-1} * (a * a^{-1}) = a^{m-1}$.

FALL 3: $m < 0$, $n = -1$. Sei $m = -k$ mit $k \in \mathbb{N}$. Dann ist $a^m * a^{-1} = (a^{-1})^k * a^{-1} = (a^{-1})^{k+1} = a^{m-1}$.

FALL 4: $m \in \mathbb{Z}$ beliebig, $n < 0$. Wir setzen $k = -n$ und führen den Beweis durch Induktion nach k. Für $k = 1$ siehe FALL 3 und FALL 4.
$k \geq 1$, $k \to k+1$: Nach Induktionsvoraussetzung, FALL 3 und FALL 4 ist

$$a^m * a^{-(k+1)} = a^m * (a^{-k} * a^{-1}) = (a^m * a^{-k}) * a^{-1} = a^{m-k} * a^{-1} = a^{m-k-1} = a^{m-(k+1)}\,.$$

FALL 5: $m < 0$, $n > 0$. Nach FALL 4 bei Vertauschung von m und n.

2.(c) FALL 1: $n \geq 0$. Wir zeigen $a * b^n = b^n * a$ und $(a * b)^n = a^n * b^n$ mittels Induktion nach n. Für $n = 0$ ist nichts zu zeigen.
$n \geq 0$, $n \to n+1$: Es ist

$$a * b^{n+1} = a * (b^n * b) = (a * b^n) * b = (b^n * a) * b = b^n * (a * b) = b^n * (b * a) = (b^n * b) * a = b^{n+1} * a\,,$$

und daher (unter Verwendung des Assoziativgesetzes und der Vertauschbarkeit von a und b)

$$\begin{aligned}(a * b)^{n+1} &= (a * b)^n * (a * b) = (a^n * b^n) * (a * b) = a^n * \big(b^n * (a * b)\big) = a^n * \big(b^n * (b * a)\big) \\ &= a^n * \big((b^n * b) * a\big) = a^n * (b^{n+1} * a) = a^n * (a * b^{n+1}) = (a^n * a) * b^{n+1} = a^{n+1} * b^{n+1}\,.\end{aligned}$$

FALL 2: $n = -k$ mit $k \in \mathbb{N}$. Nach FALL 1 folgt

$$(a * b)^{-k} = \big[(a * b)^{-1}\big]^k = \big[(b * a)^{-1}\big]^k = (a^{-1} * b^{-1})^k = (a^{-1})^k * (b^{-1})^k = a^{-k} * b^{-k}\,.$$

2.(b) FALL 1: $n \geq 0$. Induktion nach n (bei festem $m \in \mathbb{Z}$). Für $n = 0$ ist nichts zu zeigen.
$n \geq 0$, $n \to n+1$: Aus 2.(a) und der Induktionsvoraussetzung folgt

$$(a^m)^{n+1} = (a^m)^n * a^m = a^{mn} * a^m = a^{mn+m} = a^{m(n+1)}\,.$$

FALL 2: $n = -k$ mit $k \in \mathbb{N}$. Nach 2.(c) ist $a^m * a^{-m} = a^m * (a^{-1})^m = (a * a^{-1})^m = e$, also $a^{-m} = (a^m)^{-1}$, und daher nach FALL 1 $(a^m)^{-k} = \big[(a^m)^{-1}\big]^k = (a^{-m})^k = a^{-mk}$.

3. Induktion nach n. Für $n = 1$ ist nichts zu zeigen.

$n \geq 2$, $n-1 \to n$: Seien $k, l \in [1,n]$ mit $\sigma(l) = n$ und $\sigma(n) = k$. Im Falle $l = n$ ist auch $k = n$, also $\sigma(n) = n$ und $\sigma \,|\, [1, n-1] \in \mathfrak{S}_{n-1}$. Nach Induktionsvoraussetzung gilt daher

$$\overset{n}{\underset{i=1}{*}} a_{\sigma(i)} = \left(\overset{n-1}{\underset{i=1}{*}} a_{\sigma(i)}\right) * a_n = \left(\overset{n-1}{\underset{i=1}{*}} a_i\right) * a_n = \overset{n}{\underset{i=1}{*}} a_i \,.$$

Sei also nun $l < n$, und sei $\tau \in \mathfrak{S}_{n-1}$ definiert durch

$$\tau(i) = \begin{cases} \sigma(i)\,, & \text{falls} \quad i \neq l\,, \\ k\,, & \text{falls} \quad i = l\,. \end{cases}$$

Dann folgt mittels 1., des Assoziativgesetzes und der Induktionsvoraussetzung

$$\begin{aligned}
\overset{n}{\underset{i=1}{*}} a_{\sigma(i)} &= \left(\overset{n-1}{\underset{i=1}{*}} a_{\sigma(i)}\right) * a_k = \left[\left(\overset{l-1}{\underset{i=1}{*}} a_{\tau(i)}\right) * a_n\right] * \left[\left(\overset{n-1}{\underset{i=l+1}{*}} a_{\tau(i)}\right) * a_k\right] \\
&= \left(\overset{l-1}{\underset{i=1}{*}} a_{\tau(i)}\right) * \left[a_n * \left(a_k * \overset{n-1}{\underset{i=l+1}{*}} a_{\tau(i)}\right)\right] = \left(\overset{l-1}{\underset{i=1}{*}} a_{\tau(i)}\right) * \left[\left(a_k * \overset{n-1}{\underset{i=l+1}{*}} a_{\tau(i)}\right) * a_n\right] \\
&= \left(\overset{l-1}{\underset{i=1}{*}} a_{\tau(i)}\right) * \left[a_k * \left(\overset{n-1}{\underset{i=l+1}{*}} a_{\tau(i)} * a_n\right)\right] = \left(\overset{l-1}{\underset{i=1}{*}} a_{\tau(i)} * a_k\right) * \left(\overset{n-1}{\underset{i=l+1}{*}} a_{\tau(i)} * a_n\right) \\
&= \left[\left(\overset{l}{\underset{i=1}{*}} a_{\tau(i)}\right) * \left(\overset{n-1}{\underset{i=l+1}{*}} a_{\tau(i)}\right) * a_n\right] = \left(\overset{n-1}{\underset{i=1}{*}} a_{\tau(i)}\right) * a_n = \left(\overset{n-1}{\underset{i=1}{*}} a_i\right) * a_n = \overset{n}{\underset{i=1}{*}} a_i \,.
\end{aligned}$$

□

Bemerkungen 2.1.9.

1. Ist $*$ eine assoziative Verknüpfung auf einer nichtleeren Menge H, so ist, für alle $n \in \mathbb{N}$ und alle $a_1, \ldots, a_n \in H$, das Verknüpfungsergebnis $a_1 * \ldots * a_n$ unabhängig von der Beklammerung des Ausdrucks. Das ist die Aussage eines allgemeinen Assoziativgesetzes, welches auf einem präzisen Begriff der Beklammerung eines Ausdrucks beruht. Wir führen das in der vollen Allgemeinheit nicht durch und begnügen uns mit dem in Lemma 2.1.8.1 vorgestellten Spezialfall.

2. Ist $(H, *)$ eine kommutative Halbgruppe mit neutralem Element e und $E \subset H$ eine endliche Teilmenge, so definieren wir

$$\underset{a \in E}{*} a = e\,, \quad \text{falls} \quad E = \emptyset\,, \quad \text{und} \quad \underset{a \in E}{*} a = \overset{n}{\underset{i=1}{*}} a_{\sigma(i)}\,, \quad \text{falls} \quad n \in \mathbb{N} \ \text{ und } \ \sigma\colon [1,n] \to E \text{ bijektiv ist.}$$

Nach Lemma 2.1.8.3 ist diese Definition unabhängig von σ.

3. Sei $(H, *)$ eine abelsche Halbgruppe mit neutralem Element e und $(a_i)_{i \in I}$ eine Familie in H, so dass $a_i = e$ für fast alle $i \in I$. Dann setzen wir (in Verallgemeinerung von 2.)

$$\underset{i \in I}{*} a_i = \underset{i \in E}{*} a_i\,, \quad \text{wobei} \quad E = \{i \in I \mid a_i \neq e\}\,.$$

4. Wir formulieren Lemma 2.1.8.2 für eine additive abelsche Halbgruppe $H = (H, +)$. Für $a, b \in H$ und $m, n \in \mathbb{N}_0$ gilt:

$$\text{(a)} \quad ma + na = (m+n)a\,; \qquad \text{(b)} \quad n(ma) = (nm)a\,; \qquad \text{(c)} \quad n(a+b) = na + nb\,.$$

(a), (b) und (c) gelten für alle $m, n \in \mathbb{N}_0$ und im Falle $a, b \in H^\times$ für alle $m, n \in \mathbb{Z}$.

Satz 2.1.10. *Sei H eine endliche Halbgruppe mit $H = H^\bullet$. Dann ist H eine Gruppe. Insbesondere ist jedes endliche Monoid eine abelsche Gruppe.*

Beweis. Sei $H = H^\bullet$ und $a \in H$. Dann ist $\{a^n \mid n \in \mathbb{N}\}$ endlich, und daher gibt es $k, m \in \mathbb{N}$ mit $k < m$ und $a^k = a^m$. Damit folgt $e = a^{m-k} = aa^{m-k-1}$, also $a \in H^\times$. □

2.2. Untergruppen, Ordnung von Gruppenelementen

Definition 2.2.1. Sei $H = (H, *)$ eine Halbgruppe mit neutralem Element e.

1. Eine *Unterhalbgruppe* von H ist eine $*$-abgeschlossene Teilmenge $U \subset H$ mit $e \in U$ (dann ist U bzgl. der induzierten Verknüpfung eine Halbgruppe mit neutralem Element e). Ist $U \subset H$ eine Unterhalbgruppe, so nennt man U auch eine *Teilhalbgruppe* von H und H eine *Oberhalbgruppe* von U.
2. Eine Unterhalbgruppe $U \subset H$ heißt
   - *Untermonoid* oder *Teilmonoid*, wenn sie bzgl. der induzierten Verknüpfung ein Monoid ist.
   - *Untergruppe*, wenn sie bzgl. der induzierten Verknüpfung eine Gruppe ist. Dafür schreibt man $U < H$.

Wenn nicht ausdrücklich Anderes gesagt wird, schreiben wir ab jetzt alle Halbgruppen multiplikativ, verwenden die multiplikativen Konventionen aus 2.1.6.5 *und bezeichnen das Einselement einer Halbgruppe mit* e.

Satz 2.2.2 (Kennzeichnungssatz für Untergruppen)**.** *Sei G eine Gruppe und $U \subset G$. Dann sind äquivalent*:

(a) $U < G$.

(b) *U erfüllt die folgenden drei Bedingungen*:
   - $e \in U$.
   - *Für alle* $a, b \in U$ *ist* $ab \in U$.
   - *Für alle* $a \in U$ *ist* $a^{-1} \in U$.

(c) $U \neq \emptyset$, *und für alle* $a, b \in U$ *ist* $ab^{-1} \in U$.

Beweis. Die Äquivalenz von (a) und (b) gilt gemäß Definition, und offensichtlich gilt (b) $\Rightarrow$ (c).

(c) $\Rightarrow$ (b) Ist $a \in U$, so ist $e = aa^{-1} \in U$ und daher auch $a^{-1} = ea^{-1} \in U$. Sind $a, b \in U$, so ist nach dem eben Gezeigten $b^{-1} \in U$, und daher folgt auch $ab = a(b^{-1})^{-1} \in U$. □

Bemerkung 2.2.3. 1. Ist H eine Halbgruppe, so sind $\{e\}$ und $H^\times$ Untergruppen von H, und $H^\bullet$ ist eine Unterhalbgruppe von H. Ist H kommutativ, so ist $H^\bullet$ ein Teilmonoid von H. [Beweis: Mit Lemma 2.1.5.4].

2. Sei H eine Halbgruppe und $a \in H$. Dann ist $\{a^n \mid n \in \mathbb{N}_0\}$ eine Unterhalbgruppe von H. Ist $a \in H^\times$, so ist $\{a^n \mid n \in \mathbb{Z}\}$ eine Untergruppe von H. Ist insbesondere H eine abelsche Gruppe, so ist $\mathbb{Z}a = \{na \mid n \in \mathbb{Z}\}$ eine Untergruppe von H. [Beweis: Mit Lemma 2.1.8.2]

3. Sei $G = (G, +)$ eine additive abelsche Gruppe und $m \in \mathbb{N}$. Dann ist $mG = \{mg \mid g \in G\} < G$. [Beweis: Mit Satz 2.2.2(c)].

Korollar 2.2.4. *Sei G eine Gruppe.*

1. *Sei Σ eine Menge von Untergruppen von G,*
$$H = \bigcap_{U \in \Sigma} U \quad \text{und} \quad W = \bigcup_{U \in \Sigma} U\,.$$
Dann ist H eine Untergruppe von G. Ist Σ gerichtet, so ist auch W eine Untergruppe von G.
2. *Sei G abelsch, und seien $U_1, U_2 < G$. Dann ist U_1U_2 die kleinste Untergruppe von G, die $U_1 \cup U_2$ enthält. Insbesondere ist die Menge $\mathcal{U}(G)$ aller Untergruppen von G bezüglich der Verknüpfung $(U_1, U_2) \mapsto U_1U_2$ eine abelsche Halbgruppe mit neutralem Element $\{e\}$.*

BEWEIS. Wir verwenden die Charakterisierung aus Satz 2.2.2.

1. Für alle $U \in \Sigma$ ist $e \in U$ und daher $e \in H$, also insbesondere $H \neq \emptyset$. Sind $a, b \in H$, so folgt $a, b \in U$ und damit auch $ab^{-1} \in U$ für alle $U \in \Sigma$, also $ab^{-1} \in H$.

Sind $a, b \in W$, so gibt es $U_1, U_2 \in \Sigma$ mit $a \in U_1$ und $b \in U_2$. Ist Σ gerichtet, so gibt es ein $U \in \Sigma$ mit $U_1 \subset U$ und $U_2 \subset U$. Dann folgt $a, b \in U$ und damit auch $ab^{-1} \in U$, also $ab^{-1} \in W$.

2. Es genügt, zu zeigen, dass $U_1U_2 \subset G$ eine Untergruppe ist. Seien $a, b \in U_1U_2$, etwa $a = a_1a_2$ und $b = b_1b_2$ mit $a_1, b_1 \in U_1$ und $a_2, b_2 \in U_2$. Dann folgt $ab^{-1} = a_1b_1^{-1}a_2b_2^{-1} \in U_1U_2$. □

Satz 2.2.5 (Struktursatz für die Untergruppen von $\mathbb{Z}$).

1. *Für* $a, b \in \mathbb{Z}$ *gilt*: $a \mid b \iff b\mathbb{Z} \subset a\mathbb{Z}$. *Insbesondere*: $a\mathbb{Z} = b\mathbb{Z} \iff |a| = |b|$.
2. *Sei* $U < \mathbb{Z}$. *Dann gibt es genau ein* $d \in \mathbb{N}_0$ *mit* $U = d\mathbb{Z}$. *Ist* $U \neq \{0\}$, *so ist* $d = \min(U \cap \mathbb{N})$.
3. *Seien* $n \in \mathbb{N}$, $a_1, \ldots, a_n \in \mathbb{Z}$ *und* $d, e \in \mathbb{N}_0$. *Dann gilt*:
$$d = \mathrm{ggT}(a_1, \ldots, a_n) \iff d\mathbb{Z} = a_1\mathbb{Z} + \ldots + a_n\mathbb{Z}$$
und
$$e = \mathrm{kgV}(a_1, \ldots, a_n) \iff e\mathbb{Z} = a_1\mathbb{Z} \cap \ldots \cap a_n\mathbb{Z}\,.$$
4. *Seien* $r \in \mathbb{N}$ *und* $a_1, \ldots, a_r \in \mathbb{Z}$. *Dann sind äquivalent*:
   (a) $\mathrm{ggT}(a_1, \ldots, a_r) = 1$.
   (b) $a_1\mathbb{Z} + \ldots + a_r\mathbb{Z} = \mathbb{Z}$.
   (c) *Es gibt* $x_1, \ldots, x_r \in \mathbb{Z}$ *mit* $a_1x_1 + \ldots + a_rx_r = 1$.

BEWEIS. 1. Ist $a \mid b$, so ist $b = ac$ mit $c \in \mathbb{Z}$, und es folgt $b\mathbb{Z} = ac\mathbb{Z} \subset a\mathbb{Z}$. Ist umgekehrt $b\mathbb{Z} \subset a\mathbb{Z}$, so ist $b \in a\mathbb{Z}$, also $b = ac$ mit $c \in \mathbb{Z}$ und daher $a \mid b$. Damit folgt: $a\mathbb{Z} = b\mathbb{Z} \iff a \mid b$ und $b \mid a \iff |a| = |b|$.

2. Die Eindeutigkeit folgt aus 1., und im Falle $U = \{0\}$ ist nichts weiter zu zeigen. Sei also $U \neq \{0\}$. Für alle $a \in U$ ist auch $|a| \in U$ und daher $U \cap \mathbb{N} \neq \emptyset$. Ist $d = \min(U \cap \mathbb{N})$, so folgt $d\mathbb{Z} \subset U$. Für den Beweis der umgekehrten Inklusion sei $a \in U$. Nach Satz 1.1.6.1 ist dann $a = bd + r$ mit $b, r \in \mathbb{Z}$ und $r \in [0, d-1]$. Dann ist aber $r = a - bd \in U$ und daher $r = 0$, also $a = bd \in d\mathbb{Z}$.

3. Sei $\mathcal{U}(\mathbb{Z})$ die Menge aller Untergruppen von $\mathbb{Z}$. Dann ist $(\mathcal{U}(\mathbb{Z}), \supset)$ eine partiell geordnete Menge. Für $a_1, \ldots, a_n \in \mathbb{Z}$ ist $\inf_{\supset}(a_1\mathbb{Z}, \ldots, a_n\mathbb{Z}) = a_1\mathbb{Z} + \ldots + a_n\mathbb{Z}$ und $\sup_{\supset}(a_1\mathbb{Z}, \ldots, a_n\mathbb{Z}) = a_1\mathbb{Z} \cap \ldots \cap a_n\mathbb{Z}$. Nach 1. und 2. ist die Abbildung $\phi\colon \mathbb{N}_0 \to \mathcal{U}(\mathbb{Z})$, definiert durch $\phi(d) = d\mathbb{Z}$, ein Ordnungsisomorphismus $(\mathbb{N}_0, \mid) \to (\mathcal{U}(\mathbb{Z}), \supset)$. Damit folgt:

$$d = \mathrm{ggT}(a_1, \ldots, a_n) \iff d = \mathrm{ggT}(|a_1|, \ldots, |a_n|) \iff d\mathbb{Z} = |a_1|\mathbb{Z} + \ldots + |a_n|\mathbb{Z} = a_1\mathbb{Z} + \ldots + a_n\mathbb{Z}\,.$$

Für kgV argumentiert man ebenso.

4. Klar nach 3. □

Definition 2.2.6. Sei G eine Gruppe, $X \subset G$ und $\Sigma = \{U < G \mid X \subset U\}$. Dann heißt
$$\langle X \rangle_{\mathbb{Z}} = \langle X \rangle = \bigcap_{U \in \Sigma} U < G$$
die von X erzeugte Untergruppe. Ist $X = \{a_1, \ldots, a_n\}$, so schreibt man auch $\langle a_1, \ldots, a_n \rangle$ an Stelle von $\langle \{a_1, \ldots, a_n\} \rangle$.

Satz 2.2.7 (Erzeugungssatz für Untergruppen)**.** *Sei G eine Gruppe, $X \subset G$ und $a \in G$.*

1. *$\langle X \rangle$ ist die kleinste X enthaltende Untergruppe von G (d.h., es ist $\langle X \rangle < G$, $X \subset \langle X \rangle$, und für jede Untergruppe $H < G$ mit $X \subset H$ ist $\langle X \rangle \subset H$).*

2. *$\langle X\rangle$ ist die Menge aller Potenzprodukte $a_1^{k_1}\cdot\ldots\cdot a_n^{k_n}$ $n\in\mathbb{N}$, $a_1,\ldots,a_n\in X$ und $k_1,\ldots,k_n\in\mathbb{Z}$. Insbesondere ist $\langle a\rangle=\{a^n\mid a\in\mathbb{Z}\}$.*

Beweis. 1. Nach Definition und Korollar 2.2.4.

2. Sei H die Menge aller Potenzprodukte $a_1^{k_1}\cdot\ldots\cdot a_n^{k_n}$ $n\in\mathbb{N}$, $a_1,\ldots,a_n\in X$ und $k_1,\ldots,k_n\in\mathbb{Z}$. Dann ist $e\in H$ (mit $n=1$ und $k_1=0$), und aus $x,y\in H$ folgt $x^{-1}\in H$ und $xy\in H$. Also ist $H<G$, und es ist $X\subset H$. Ist $U<G$ mit $X\subset U$, so enthält U auch alle Potenzprodukte von Elementen aus X, also ist $H\subset U$ und daher $H=\langle X\rangle$ nach 1. □

Definition 2.2.8. Sei G eine Gruppe und $a\in G$.

1. Man nennt $\langle a\rangle$ die *von a erzeugte zyklische Untergruppe* von G, und man definiert die *Ordnung* $\operatorname{ord}(a)$ von a durch
$$\operatorname{ord}(a)=\begin{cases}\infty\,, & \text{falls } a^n\neq e \text{ für alle } n\in\mathbb{N},\\ \min\{n\in\mathbb{N}\mid a^n=e\} & \text{sonst}\,.\end{cases}$$
Man sagt, a ist ein *Torsionselement*, wenn $\operatorname{ord}(a)<\infty$.
2. G heißt *zyklisch*, wenn ein Element $g\in G$ existiert mit $G=\langle g\rangle$. Man nennt dann g ein *erzeugendes Element* von G.
3. G heißt *Torsionsgruppe*, wenn jedes Element von G ein Torsionselement ist. G heißt *torsionsfrei*, wenn e das einzige Torsionselement von G ist. Ist G eine Torsionsgruppe, so nennt man
$$\exp(G)=\begin{cases}\operatorname{kgV}(\{\operatorname{ord}(g)\mid g\in G\})\,, & \text{falls } \sup\{\operatorname{ord}(g\in G)\mid g\in G\}<\infty\\ \infty & \text{sonst}\end{cases}$$
den *Exponenten* von G.
4. Man nennt $(G:1)=|G|\in\mathbb{N}\cup\{\infty\}$ die *Ordnung* von G.

Bemerkungen und Beispiele 2.2.9.

1. Sei G eine Gruppe und $g\in G$. Dann ist $\operatorname{ord}(g)=\operatorname{ord}(g^{-1})$, und im Falle $\operatorname{ord}(g)=\infty$ ist auch $\operatorname{ord}(g^n)=\infty$ für alle $n\in\mathbb{Z}\setminus\{0\}$.

2. Sei G eine abelsche Gruppe, $n\in\mathbb{N}$ und $a_1,\ldots,a_n\in G$. Dann ist
$$\langle a_1,\ldots,a_n\rangle=\{a_1^{k_1}\cdot\ldots\cdot a_n^{k_n}\mid k_1,\ldots,k_n\in\mathbb{Z}\}\,.$$
[Beweis: Nach 2.1.8.3]. Ist G eine additive abelsche Gruppe, so erhalten wir
$$\langle a_1,\ldots,a_n\rangle=\{k_1a_1+\ldots+k_na_n\mid k_1,\ldots,k_n\in\mathbb{Z}\}=\mathbb{Z}a_1+\ldots+\mathbb{Z}a_n<G\,.$$

3. Es ist $(\mathbb{Z},+)=\langle 1\rangle=\langle -1\rangle$, und für jedes $d\in\mathbb{Z}$ ist $\langle d\rangle=\mathbb{Z}d=d\mathbb{Z}=\{dk\mid k\in\mathbb{Z}\}$.

4. Sei K ein Körper und $n\in\mathbb{N}$. Man nennt
$$\mu_n(K)=\{z\in K^\times\mid z^n=1\}$$
die *Gruppe der n-ten Einheitswurzeln* von K und
$$\mu(K)=\bigcup_{m\in\mathbb{N}}\mu_m(K)=\{a\in K^\times\mid \operatorname{ord}(a)<\infty\}$$
die *Einheitswurzelgruppe* von K. $\mu_n(K)$ und $\mu(K)$ sind Untergruppen von $K^\times$. [Beweis: mit Satz 2.2.2]. Es ist $\mu(\mathbb{R})=\{\pm 1\}$.

Im Falle $K=\mathbb{C}$ weiß man aus der Analysis
$$\mu_n(\mathbb{C})=\{\mathsf{e}^{2\pi\mathrm{i}k/n}\mid k\in\mathbb{Z}\}=\langle\zeta_n\rangle\quad\text{mit}\quad\zeta_n=\mathsf{e}^{2\pi\mathrm{i}/n}\,.$$

Man nennt ζ_n eine (analytisch normierte) *primitive n-te Einheitswurzel*. Wir werden beweisen, dass die Gruppe $\mu_n(K)$ für jeden Körper K eine zyklische Gruppe ist. Die Einheitswurzeln von $\mathbb{C}$ spielen in der Theorie der algebraischen Gleichungen und bei der Konstruktion regelmäßiger Vielecke eine zentrale Rolle.

Satz 2.2.10. *Sei G eine Gruppe und $g \in G$.*

1. *Für alle $i, j \in \mathbb{N}_0$ mit $i < j < \operatorname{ord}(g)$ ist $g^i \neq g^j$, und es ist $|\langle g\rangle| = \operatorname{ord}(g) \in \mathbb{N} \cup \{\infty\}$.*
2. *Sei $\operatorname{ord}(g) = n \in \mathbb{N}$. Dann ist $\langle g\rangle = \{g^i \mid i \in [0, n-1]\}$, $\{k \in \mathbb{Z} \mid g^k = e\} = n\mathbb{Z}$, und für alle $k \in \mathbb{Z}$ ist*
$$\operatorname{ord}(g^k) = \frac{n}{\operatorname{ggT}(k,\, n)}\,.$$
Insbesondere folgt für alle $k, l \in \mathbb{Z}$: (a) $g^k = e \iff n \mid k$; (b) $g^k = g^l \iff n \mid k - l$.

Beweis. Seien $i, j \in \mathbb{N}_0$ mit $i < j < \operatorname{ord}(g)$. Dann ist $0 < j - i < \operatorname{ord}(g)$, also $g^{j-i} \neq e$ und daher $g^i \neq g^j$. Damit folgt $|\langle g\rangle| \geq \operatorname{ord}(g)$.

Sei nun $\operatorname{ord}(g) = n \in \mathbb{N}$. Ist $k \in \mathbb{Z}$, so gibt es $q, r \in \mathbb{Z}$ mit $k = qn + r$ und $r \in [0, n-1]$. Dann ist $g^k = (g^n)^q g^r = g^r \in \{g^i \mid i \in [0, n-1]\}$, und genau dann ist $g^k = e$, wenn $r = 0$, also $k \in n\mathbb{Z}$. Insbesondere folgt $|\langle g\rangle| = n$, und für $k, l \in \mathbb{Z}$ ist genau dann $g^k = g^l$, wenn $g^{k-l} = e$, also $n \mid k - l$.

Es bleibt die Formel für $\operatorname{ord}(g^k)$ zu beweisen. Sei also $k \in \mathbb{N}$ und $d = \operatorname{ggT}(k, n)$. Dann gilt nach Satz 1.1.7.2 für alle $m \in \mathbb{Z}$:
$$(g^k)^m = e \iff n \mid km \iff n \mid dm \iff \frac{n}{d} \,\Big|\, m\,, \quad \text{Daher ist } \operatorname{ord}(g^k) = \frac{n}{d}\,.$$

□

2.3. Normalteiler und Kongruenzen

Definition 2.3.1. Sei G eine Gruppe.

1. Sei $H < G$ und $a \in G$. Dann heißt
$$aH = \{ax \mid x \in H\} \subset G$$
die (*von a bestimmte*) *Linksnebenklasse von H in G* und
$$Ha = \{xa \mid x \in H\} \subset G$$
die (*von a bestimmte*) *Rechtsnebenklasse von H in G*. Wir bezeichnen mit G/H die Menge der Links- und mit $H\backslash G$ die Menge der Rechtsnebenklassen von H in G.
2. Eine Untergruppe $H < G$ heißt *Normalteiler*, $H \lhd G$, wenn $aH = Ha$ [bzw. $a^{-1}Ha = H$ oder $aHa^{-1} = H$ oder $a^{-1}Ha \subset H$] für alle $a \in G$ (dann ist $G/H = H\backslash G$).
Ist G abelsch, so ist jede Untergruppe von G ein Normalteiler.

Satz 2.3.2. *Sei G eine Gruppe, $H < G$ und seien $a, b \in G$.*

1. *Die folgenden Aussagen sind äquivalent*:
(a) $aH = bH$; (b) $aH \subset bH$; (c) $a \in bH$; (d) $b^{-1}a \in H$; (e) $aH \cap bH \neq \emptyset$.
Insbesondere ist
$$G = \biguplus_{A \in G/H} A\,.$$

2. *Die folgenden Aussagen sind äquivalent*:
   (a) $Ha = Hb$; (b) $Ha \subset Hb$; (c) $a \in Hb$; (d) $ab^{-1} \in H$; (e) $Ha \cap Hb \neq \emptyset$.
   Insbesondere ist
$$G = \biguplus_{A \in H\backslash G} A\,.$$
3. $a \in H \iff aH = H \iff Ha = H$.
4. $aH = bH \iff Ha^{-1} = Hb^{-1}$.
5. *Die Abbildungen*
$$\mu_a\colon \begin{cases} H & \to & aH \\ x & \mapsto & ax \end{cases} \qquad \textit{und} \qquad \mu'_a\colon \begin{cases} H & \to & Ha \\ x & \mapsto & xa \end{cases}$$
   sind bijektiv. Insbesondere ist $|aH| = |H| = |Ha|$.
6. *Die Abbildung* $\tau\colon G/H \to H\backslash G$, *definiert durch* $\tau(aH) = Ha^{-1}$, *ist bijektiv. Insbesondere ist* $|G/H| = |H\backslash G|$.
7. *Ist* $|G/H| \leq 2$, *so ist* $H \lhd G$.
8. *Ist* Ω *eine Menge von Normalteilern von* G,
$$M = \bigcap_{N \in \Omega} N \quad \textit{und} \quad W = \bigcup_{N \in \Omega} N\,.$$
   Dann ist M *ein Normalteiler von* G. *Ist* Ω *gerichtet, so ist auch* W *ein Normalteiler von* G.

Beweis. 1. (a) $\Rightarrow$ (b) Klar.

(b) $\Rightarrow$ (c) Es ist $a = ae \in aH \subset bH$.

(c) $\Rightarrow$ (d) Wegen $a \in bH$ ist $a = bx$ mit $x \in H$, und daher ist $b^{-1}a = b^{-1}(bx) = x \in H$.

(d) $\Rightarrow$ (e) Es ist $a = ae = b(b^{-1}a) \in aH \cap bH$.

(e) $\Rightarrow$ (a) Es genügt $aH \subset bH$ zu zeigen. Sei $z \in aH \cap bH$, also $z = au = bv$ mit $u, v \in H$. Ist nun $x \in aH$, so ist $x = ay$ mit $y \in H$, so ist $vu^{-1}y \in H$, und es folgt $x = ay = bvu^{-1}y \in bH$.

2. Analog.

3. Nach 1. und 2. mit $b = e$.

4. Nach 1. und 2. ist $[\,aH = bH \iff b^{-1}a \in H\,]$ und $[\,Ha^{-1} = Hb^{-1} \iff a^{-1}(b^{-1})^{-1} \in H\,]$, und da H eine Untergruppe ist, folgt $[\,b^{-1}a \in H \iff a^{-1}b = a^{-1}(b^{-1})^{-1} \in H\,]$.

5. $(z \mapsto a^{-1}z)$ ist die Umkehrabbildung von μ_a, und $(z \mapsto za^{-1})$ ist die von μ'_a.

6. Nach 4.

7. Im Falle $|G/H| = 1$ ist $G = H$ und nichts zu zeigen. Sei nun $|G/H| = 2$ und $a \in G \setminus H$. Dann ist $G = H \uplus aH = H \uplus Ha$ und daher $aH = Ha$.

8. Aus Korollar 2.2.4 folgt die Untergruppeneigenschaft. Sei $x \in M$ und $a \in G$. Für alle $N \in \Omega$ ist dann $x \in N$, also auch $a^{-1}xa \in N$, und daher folgt $a^{-1}xa \in M$. Also ist $M \lhd G$, und für W argumentiert man analog. □

Definition 2.3.3. Sei G eine Gruppe, $H < G$ und $(a_i)_{i\in I}$ eine Familie in G.

1. Die Partition
$$G = \biguplus_{A \in G/H} A$$
   nennt man *Linksnebenklassenzerlegung von* G *nach* H. Die Familie $(a_i)_{i\in I}$ (bzw. die Menge $\{a_i \mid i \in I\}$) heißt *Repräsentantensystem von* G/H (in G), wenn $G/H = \{a_iH \mid i \in I\}$ und $a_iH \neq a_jH$ für alle $i, j \in I$ mit $i \neq j$.

2. Die Partition
$$G = \biguplus_{A \in H\backslash G} A$$
nennt man *Rechtsnebenklassenzerlegung von* G *nach* H. Die Familie $(a_i)_{i\in I}$ (bzw. die Menge $\{a_i \mid i \in I\}$) heißt *Repräsentantensystem von* $H\backslash G$ (in G), wenn $H\backslash G = \{Ha_i \mid i \in I\}$ und $Ha_i \neq Ha_j$ für alle $i, j \in I$ mit $i \neq j$.

3. Man nennt $(G:H) = |G/H| = |H\backslash G| \in \mathbb{N} \cup \{\infty\}$ den *Index* von H in G.

Beispiele 2.3.4. Sei G eine Gruppe.

1. Sei $H = \{e\}$. Für $a \in G$ ist dann $aH = \{a\} = Ha$, also $\{e\} \lhd G$, und die Abbildung
$$G \to G/\{e\} = \{e\}\backslash G\,, \quad a \mapsto \{a\}\,,$$
ist bijektiv. Es ist also $(G:\{e\}) = (G:1) = |G|$.

2. Sei $H = G$. Dann ist $G/G = \{G\} = G \setminus G$ und $(G:G) = 1$.

3. Ist G abelsch und $H < G$, so ist $aH = Ha$ für alle $a \in G$, also $H \lhd G$ und $G/H = H \setminus G$. Ist G eine additive abelsche Gruppe, so schreibt man auch die Nebenklassen additiv. Für $a \in G$ ist dann
$$a + H = \{a + x \mid x \in H\} \in G/H = H \setminus G\,.$$

Definitionen und Bemerkungen 2.3.5 (Kongruenzen und Restklassen in $\mathbb{Z}$)**.** Sei $m \in \mathbb{N}$.

1. Ist $a \in \mathbb{Z}$, so nennt man die Nebenklasse $a + m\mathbb{Z} \in \mathbb{Z}/m\mathbb{Z}$ die *Restklasse von* a *modulo* m. An Stelle von $a + m\mathbb{Z}$ schreibt man häufig auch $[a]_m$ oder (wenn der Bezug zu m klar ist) einfach $[a]$ oder $\overline{a}$.

2. Zwei Zahlen $a, b \in \mathbb{Z}$ heißen *kongruent modulo* m, $a \equiv b \bmod m$, wenn $a + m\mathbb{Z} = b + m\mathbb{Z}$. Andernfalls heißen a und b *inkongruent modulo* m, und man schreibt $a \not\equiv b \bmod m$. An Stelle von $a \equiv b \bmod m$ schreibt man auch $a \equiv b \,(\mathrm{mod}\, m)$, $a \equiv b\ (m)$ oder $a \equiv_m b$.

3. Ist $a \in \mathbb{Z}$, so gibt es nach Satz 1.1.6.1 genau ein Paar $(q, r) \in \mathbb{Z}\times[0,\, m-1]$ mit $a = qm + r$. Man nennt dann q den *Quotienten* und r den *Rest* von a bei der *Division mit Rest* durch m. Für $a, b \in \mathbb{Z}$ sind (nach Definition) die folgenden Aussagen äquivalent:

(a) a und b lassen bei Division mit Rest durch m denselben Rest.

(b) $a - b \in m\mathbb{Z}$.

(c) $m \,|\, a - b$.

(d) $a \equiv b \bmod m$.

4. Kongruenz modulo m ist eine mit der Addition und Multiplikation kompatible Äquivalenzrelation auf $\mathbb{Z}$, d. h., für alle $a, b, c, d \in \mathbb{Z}$ gilt:

(a) $a \equiv a \bmod m$.

(b) Aus $a \equiv b \bmod m$ folgt $b \equiv a \bmod m$.

(c) Aus $a \equiv b \bmod m$ und $b \equiv c \bmod m$ folgt $a \equiv c \bmod m$.

(d) Aus $a \equiv b \bmod m$ und $c \equiv d \bmod m$ folgt $a \pm c \equiv b \pm d \bmod m$ und $ac \equiv bd \bmod m$.

[Beweis von (d): $(a \pm c) - (b \pm d) = (a - b) \pm (c - d)$ und $ac - bd = (a - b)c + b(c - d)$.]

5. Ein Repräsentantensystem von $\mathbb{Z}/m\mathbb{Z}$ in $\mathbb{Z}$ nennt man *Restsystem modulo* m. Nach 3. ist $[0,\, m-1]$ ein Restsystem modulo m (man nennt es das kleinste nicht-negative Restsystem modulo m). Eine Teilmenge $R \subset \mathbb{Z}$ ist genau dann ein Restssystem modulo m, wenn es Zahlen $k_0, \ldots, k_{m-1} \in \mathbb{Z}$ gibt, so dass $R = \{k_r m + r \mid r \in [0, m-1]\}$. Insbesondere ist $[1, m]$ ein Restsystem modulo m, und $(\mathbb{Z}:m\mathbb{Z}) = m$.

6. Für $a \in \mathbb{Z}$ ist $|a|\mathbb{Z} = a\mathbb{Z}$, und daher $(\mathbb{Z}:a\mathbb{Z}) = \infty$, falls $a = 0$, und $(\mathbb{Z}:a\mathbb{Z}) = |a|$, falls $a \neq 0$.

Satz 2.3.6. *Seien* $m \in \mathbb{N}$, $a, b \in \mathbb{Z}$ *und* $d = \mathrm{ggT}(a, m)$. *Dann sind äquivalent*:

(a) *Es gibt es ein* $x \in \mathbb{Z}$ *mit* $ax \equiv b \mod m$ (b) $d \mid b$.

Beweis. (a) $\Rightarrow$ (b) Sei $x \in \mathbb{Z}$ mit $ax \equiv b \bmod m$. Dann ist $ax - b = my$ mit $y \in \mathbb{Z}$, also $b = ax - my$ und daher $d \mid b$.

(b) $\Rightarrow$ (a) Seien $u, v, w \in \mathbb{Z}$ mit $d = au + mv$ und $b = dw$. Dann folgt $b = a(uw) + m(vw)$, also $b \equiv ax \mod m$ mit $x = uw$. □

Satz 2.3.7 (Satz von Lagrange). *Sei* G *eine Gruppe und seien* $K < H < G$ *Untergruppen. Dann ist*

$$(G:K) = (G:H)(H:K).$$

Beweis. Sei $\{a_i \mid i \in I\}$ ein Repräsentantensystem von G/H in G und $\{b_j \mid j \in J\}$ ein Repräsentantensystem von H/K in H. Dann ist

$$H = \biguplus_{j\in J} b_jK \quad \text{und} \quad G = \biguplus_{i\in H} a_iH\,, \quad \text{also} \quad G = \biguplus_{i\in I} a_i\Big(\biguplus_{j\in J} b_jK\Big) = \biguplus_{i\in I}\biguplus_{j\in J} a_ib_jK = \biguplus_{(i,j)\in I\times J} a_ib_jK\,.$$

Daher ist $\{a_ib_j \mid (i,j) \in I \times J\}$ ein Repräsentantensystem von G/K, und wir erhalten

$$(G:K) = |I \times J| = |I|\,|J| = (G:H)(H:K).$$

□

Satz 2.3.8. *Sei* G *eine Gruppe.*

1. *Für jede Untergruppe* $H < G$ *ist* $|G| = (G:H)\,|H|$.
2. *Ist* $|G| < \infty$ *und* $g \in G$, *so ist* $\mathrm{ord}(g)$ *ein Teiler von* $|G|$. *Insbesondere ist* $\exp(G)$ *ein Teiler von* $|G|$.
3. *Ist* $|G| \in \mathbb{P} \cup \{1\}$, *so ist* G *zyklisch, und für alle* $g \in G \setminus \{e\}$ *ist* $G = \langle g\rangle$.

Beweis. 1. Nach Satz 2.3.7 mit $K = \{e\}$ folgt $|G| = (G:\{e\}) = (G:H)(H:\{e\}) = (G:H)|H|$.

2. Ist $|G| < \infty$ und $g \in G$, so folgt $|G| = (G:\langle g\rangle)\,|\langle g\rangle| = (G:\langle g\rangle)\,\mathrm{ord}(g)$, und daher ist $\mathrm{ord}(g)$ ein Teiler von $|G|$. Auf Grund der Definition des kgV ist dann auch $\exp(G)$ in Teiler von $|G|$.

3. Ist $|G| = 1$, so ist $G = \{e\} = \langle e\rangle$ nach Definition. Sei also $|G| \in \mathbb{P}$ und $g \in G \setminus \{e\}$. Dann ist $|\langle g\rangle|$ ein Teiler von $|G|$, und wegen $|\langle g\rangle| > 1$ folgt $|\langle g\rangle| = |G|$, also $\langle g\rangle = G$. □

Bemerkung 2.3.9. Seien $a, b \in \mathbb{Z} \setminus \{0\}$. Dann ist $ab\mathbb{Z} \subset a\mathbb{Z} \subset \mathbb{Z}$, mit Satz 2.3.7 folgt

$$|ab| = (\mathbb{Z}:ab\mathbb{Z}) = (\mathbb{Z}:a\mathbb{Z})\,(a\mathbb{Z}:ab\mathbb{Z}) = |a|\,(a\mathbb{Z}:ab\mathbb{Z})\,, \quad \text{und daher} \quad (a\mathbb{Z}:ab\mathbb{Z}) = |b|\,.$$

2.4. Homomorphismen

Definition 2.4.1. Seien H und $\overline{H}$ nichtleere Mengen, $f\colon H \to \overline{H}$ eine Abbildung, $*$ eine Verknüpfung auf H und $\bar{*}$ eine Verknüpfung auf $\overline{H}$.

1. f heißt $(*, \bar{*})$-*Homomorphismus*, wenn $f(a * b) = f(a) \bar{*}\, f(b)$ für alle $a, b \in H$.
2. Sei $(H, *)$ eine Halbgruppe mit neutralem Element e und $(\overline{H}, \bar{*})$ eine Halbgruppe mit neutralem Element $\bar{e}$. Dann heißt f ein *Halbgruppenhomomorphismus*, wenn f ein $(*, \bar{*})$-Homomorphismus ist, und $f(e) = \bar{e}$.

   Sind $(H, *)$ und $(\overline{H}, \bar{*})$ Monoide (bzw. Gruppen) und ist f ein Halbgruppenhomomorphismus, so nennt man f auch einen *Monoidhomomorphismus* (bzw. einen *Gruppenhomomorphismus*). Besteht über die zu Grunde liegenden Strukturen Klarheit, so nennt man f auch kurz einen *Homomorphismus*.

3. Ein Homomorphismus f heißt
   - *Monomorphismus*, wenn f injektiv ist.
   - *Epimorphismus*, wenn f surjektiv ist.
   - *Isomorphismus*, wenn f bijektiv ist.
4. Ein Homomorphismus $f\colon H \to H$ heißt *Endomorphismus*, ein Isomorphismus $f\colon H \to H$ heißt *Automorphismus*. $\mathrm{End}(H) = \mathrm{End}(H,*)$ bezeichnet die Menge der Endomorphismen und $\mathrm{Aut}(H) = \mathrm{Aut}(H,*)$ die Menge der Automorphismen von $(H,*)$.

Lemma 2.4.2. *Seien H und $\overline{H}$ nichtleere Mengen, $*$ eine Verknüpfung auf H, $\bar{*}$ eine Verknüpfung auf $\overline{H}$ und $f\colon H \to \overline{H}$ ein $(*,\bar{*})$-Homomorphismus.*

1. *Ist $U \subset H$ $*$-abgeschlossen, so ist $f(U) \subset \overline{H}$ $\bar{*}$-abgeschlossen. Ist $\overline{U} \subset \overline{H}$ $\bar{*}$-abgeschlossen, so ist $f^{-1}(\overline{U}) \subset H$ $*$-abgeschlossen.*
2. *Sei $\widetilde{H}$ eine weitere nichtleere Menge, $\widetilde{*}$ eine Verknüpfung auf $\widetilde{H}$ und $\widetilde{f}\colon \overline{H} \to \widetilde{H}$ ein $(\bar{*},\widetilde{*})$-Homomorphismus. Dann ist $\widetilde{f}\circ f$ ein $(*,\widetilde{*})$-Homomorphismus.*
3. *Sei f surjektiv.*
   (a) *Ist $*$ assoziativ bzw. kommutativ, so ist auch $\bar{*}$ assoziativ bzw. kommutativ.*
   (b) *Ist $e \in H$ ein neutrales Element bzgl. $*$, so ist $f(e) \in \overline{H}$ ein neutrales Element bzgl. $\bar{*}$.*
4. *Sei f ein Isomorphismus. Dann ist $f^{-1}\colon \overline{H} \to H$ ein $(\bar{*},*)$-Isomorphismus.*
5. *$(\mathrm{End}(H,*),\circ)$ ist eine Halbgruppe mit neutralem Element id_H, und $\mathrm{End}(H,*)^\times = \mathrm{Aut}(H,*)$.*
6. *Sei $(H,*)$ und $(\overline{H},\bar{*})$ Halbgruppen.*
   (a) *Erfüllt $\bar{*}$ die Kürzungsregeln, so ist f ein Halbgruppenhomomorphismus (d.h., $f(e) = \bar{e}$).*
   (b) *Sei f ein Halbgruppenhomomorphismus und $a \in H^\times$. Dann ist $f(a) \in \overline{H}^\times$, und es ist $f(a)^{-1} = f(a^{-1})$. Insbesondere ist $f\,|\,H^\times\colon H^\times \to \overline{H}^\times$ ein Gruppenhomomorphismus.*
   (c) *Sei f ein Halbgruppenhomomorphismus, und seien $U \subset H$ und $\overline{U} \subset \overline{H}$ Unterhalbgruppen. Dann sind auch $f(U) \subset \overline{H}$ und $f^{-1}(\overline{U}) \subset H$ Unterhalbgruppen.*
   (d) *Sei f ein Halbgruppenhomomorphismus, und seien $U \subset H$ und $\overline{U} \subset \overline{H}$ Unterhalbgruppen, so dass $f(U) \subset \overline{U}$. Dann ist auch $f\,|\,U\colon U \to \overline{U}$ ein Halbgruppenhomomorphismus.*

Beweis. 1. Sei $U \subset H$ $*$-abgeschlossen und $\overline{a}, \overline{b} \in f(U)$. Dann gibt es $a, b \in U$ mit $\overline{a} = f(a)$ und $\overline{b} = f(b)$, es ist $a * b \in U$ und daher $\overline{a} \mathbin{\bar{*}} \overline{b} = f(a) \mathbin{\bar{*}} f(b) = f(a * b) \in f(U)$.

Sei nun $\overline{U} \subset \overline{H}$ $\bar{*}$-abgeschlossen und $a, b \in f^{-1}(\overline{U})$. Dann folgt $f(a) \in \overline{U}$, $f(b) \in \overline{U}$, also auch $f(a * b) = f(a) \mathbin{\bar{*}} f(b) \in \overline{U}$ und daher $a * b \in f^{-1}(\overline{U})$.

2. Für $a, b \in H$ ist $(\widetilde{f}\circ f)(a * b) = \widetilde{f}\big(f(a) \mathbin{\bar{*}} f(b)\big) = (\widetilde{f}\circ f)(a) \mathbin{\widetilde{*}} (\widetilde{f}\circ f)(b)$.

3.(a) Sei $*$ kommutativ, und seien $\overline{a}, \overline{b} \in \overline{H}$. Dann gibt es $a, b \in H$ mit $f(a) = \overline{a}$ und $f(b) = \overline{b}$, und es folgt $\overline{a} \mathbin{\bar{*}} \overline{b} = f(a) \mathbin{\bar{*}} f(b) = f(a * b) = f(b * a) = f(b) \mathbin{\bar{*}} f(a) = \overline{b} \mathbin{\bar{*}} \overline{a}$. Die Assoziativität beweist man analog.

3.(b) Sei $\overline{a} \in \overline{H}$. Dann ist $\overline{a} = f(a)$ mit $a \in H$, und $f(e) \mathbin{\bar{*}} \overline{a} = f(e) \mathbin{\bar{*}} f(a) = f(e * a) = f(a) = \overline{a}$. Daher ist $f(e)$ neutral bzgl. $\bar{*}$.

4. Seien $\overline{a}, \overline{b} \in \overline{H}$ und $a, b \in H$ mit $\overline{a} = f(a)$ und $\overline{b} = f(b)$. Dann ist $\overline{a} \mathbin{\bar{*}} \overline{b} = f(a) \mathbin{\bar{*}} f(b) = f(a * b)$ und daher $f^{-1}(\overline{a} \mathbin{\bar{*}} \overline{b}) = f^{-1}\big(f(a * b)\big) = a * b = f^{-1}(\overline{a}) * f^{-1}(\overline{b})$.

5. Nach 2. und 4.

6. Sei e bzw. $\bar{e}$ das neutrale Element von $(H,*)$ bzw. $(\overline{H},\bar{*})$.

6.(a) Aus $f(e) \mathbin{\bar{*}} f(e) = f(e * e) = f(e) = f(e) \mathbin{\bar{*}} \bar{e}$ folgt $f(e) = \bar{e}$, und daher ist f ein Halbgruppenhomomorphismus.

6.(b) Wegen $f(a^{-1}) \mathbin{\overline{*}} f(a) = f(a^{-1} * a) = f(e) = \overline{e} = f(a * a^{-1}) = f(a) \mathbin{\overline{*}} f(a^{-1})$ ist $f(a) \in \overline{H}^\times$ und $f(a)^{-1} = f(a^{-1})$.

6.(c) Nach 1. und wegen $f(e) = \overline{e}$.

6.(d) Offensichtlich. □

Definition 2.4.3. Sei $f\colon G \to \overline{G}$ ein Gruppenhomomorphismus, und sei $\overline{e}$ das neutrale Element von $\overline{G}$. Dann nennt man $\mathrm{Ker}(f) = f^{-1}(\{\overline{e}\}) \subset G$ den *Kern* von f.

Satz 2.4.4. *Sei $f\colon G \to \overline{G}$ ein Gruppenhomomorphismus, und sei e bzw. $\overline{e}$ das neutrale Element von G bzw. $\overline{G}$.*

1. *$f(e) = \overline{e}$, und für alle $a \in G$ ist $f(a^{-1}) = f(a)^{-1}$.*
2. *Ist $H < G$, so ist $f(H) < \overline{G}$.*
3. *Ist $H \lhd G$, so ist $f(H) \lhd f(G)$.*
4. *Ist $\overline{H} < \overline{G}$, so ist $f^{-1}(\overline{H}) < G$.*
5. *Ist $\overline{H} \lhd \overline{G}$, so ist $f^{-1}(\overline{H}) \lhd G$.*
6. *Für alle $a \in G$ ist $f^{-1}\big(\{f(a)\}\big) = a\,\mathrm{Ker}(f) = \mathrm{Ker}(f)\,a$. Insbesondere ist $\mathrm{Ker}(f) \lhd G$, und f ist genau dann ein Monomorphismus, wenn $\mathrm{Ker}(f) = \{e\}$.*
7. *Sei $X \subset G$ und $H = \langle X\rangle$ die von X erzeugte Untergruppe von G. Dann ist $\langle f(X)\rangle = f(H)$, und für jeden Gruppenhomomorphismus $g\colon G \to \overline{G}$ gilt: Aus $f \mid X = g \mid X$ folgt $f \mid H = g \mid H$.*
   Insbesondere gilt: Ist $G = \langle g\rangle$, so folgt $f(G) = \langle f(g)\rangle$.

Beweis. 1. Nach Lemma 2.4.2.6.

2. Sei $H < G$. Nach Lemma 2.4.2.6 ist $f(H) \subset \overline{G}$ eine Unterhalbgruppe, nach Lemma 2.4.2.6(b) folgt $f(H) = f(H^\times) \subset f(H)^\times \subset f(H)$. Also gilt Gleichheit und $f(H)$ ist eine Gruppe.

3. Sei $H \lhd G$. Nach 2. ist $f(H) < f(G) < \overline{G}$. Ist nun $\overline{a} \in f(G)$, so gibt es ein $a \in G$ mit $f(a) = \overline{a}$, und $\overline{a}f(H) = f(aH) = f(Ha) = f(H)\overline{a}$. Daher ist $f(H) \lhd f(G)$.

4. Sei $\overline{H} < \overline{G}$. Nach Lemma 2.4.2.6(c) ist $f^{-1}(\overline{H}) \subset G$ eine Unterhalbgruppe. Ist $a \in f^{-1}(\overline{H})$, also $f(a) \in \overline{H}$, so folgt mit 1. $f(a^{-1}) = f(a)^{-1} \in \overline{H}$ und $a^{-1} \in f^{-1}(\overline{H})$. Daher ist $f^{-1}(\overline{H}) < G$.

5. Sei $\overline{H} \lhd \overline{G}$. Nach 4. ist $f^{-1}(\overline{H}) < G$. Ist $a \in G$, so folgt

$$f\big(a^{-1}f^{-1}(\overline{H})a\big) = f(a^{-1})f\big(f^{-1}(\overline{H})\big)f(a) \subset f(a)^{-1}\overline{H}f(a) = \overline{H}\,, \quad \text{also} \quad f^{-1}(\overline{H}) \lhd G\,.$$

6. Sei $a \in G$. Ist $x \in f^{-1}\big(\{f(a)\}\big)$, so folgt $f(x) = f(a)$, also ist $f(xa^{-1}) = f(x)f(a)^{-1} = \overline{e}$ und $f(a^{-1}x) = f(a)^{-1}f(x) = \overline{e}$. Daher folgt $xa^{-1} \in \mathrm{Ker}(f)$ und $a^{-1}x \in \mathrm{Ker}(f)$, also $x \in \mathrm{Ker}(f)\,a$ und $x \in a\,\mathrm{Ker}(f)$. Ist umgekehrt $x \in a\,\mathrm{Ker}(f)$, also $x = au$ mit $u \in \mathrm{Ker}(f)$, so folgt $f(x) = f(a)f(u) = f(a)\overline{e} = f(a)$. Ist $x \in \mathrm{Ker}(f)\,a$, so folgt in gleicher Weise $f(x) = f(a)$.

7. Aus $X \subset H$ folgt $f(X) \subset f(H)$ und daher $\langle f(X)\rangle \subset f(H)$, da $f(H) < \overline{G}$. Sei nun $\overline{a} \in f(H)$, also $\overline{a} = f(a)$ mit $a \in H$. Nach Bemerkung 2.2.9.1 ist $a = a_1^{k_1} \cdot \ldots \cdot a_n^{k_n}$ mit $n \in \mathbb{N}$, $a_1, \ldots, a_n \in X$ und $k_1, \ldots, k_n \in \mathbb{Z}$, und wir erhalten $f(a) = f(a_1)^{k_1} \cdot \ldots \cdot f(a_n)^{k_n} \in \langle f(X)\rangle$.

Sei nun $g\colon G \to \overline{G}$ ein Gruppenhomomorphismus mit $f \mid X = g \mid X$ und $U = \{a \in G \mid f(a) = g(a)\}$. Dann ist $e \in U$, und für alle $a, b \in U$ ist auch $ab \in U$ und $a^{-1} \in U$. Daher ist $U < G$, und aus $X \subset U$ folgt $H \subset U$, also $f \mid H = g \mid H$. □

Bemerkungen und Beispiele 2.4.5.

1. Seien $(H, *)$ und $(\overline{H}, \overline{*})$ Halbgruppen, sei $\overline{e}$ das neutrale Element von $\overline{H}$ und $f = \mathsf{c}_{\overline{e}}\colon H \to \overline{H}$ die konstante Abbildung mit Wert $\overline{e}$. Dann ist f ein Homomorphismus und heißt *Einshomomorphismus*. Ist $\overline{H}$ eine additive Halbgruppe und $\overline{e} = 0$, so nennt man f einen *Nullhomomorphismus*. Ein Gruppenhomomorphismus $f\colon G \to \overline{G}$ ist genau dann der Einshomomorphismus, wenn $\mathrm{Ker}(f) = G$.

2. Sei $f\colon H \to \overline{H}$ ein Halbgruppenhomomorphismus. Dann ist $f\colon H \to f(H)$ ein Epimorphismus. Ist f ein Monomorphismus, so ist $f\colon H \to f(H)$ ein Isomorphismus.

3. Sei H eine Halbgruppe und $U \subset H$ eine Unterhalbgruppe. Dann ist die Einlagerungsabbildung $j\colon U \hookrightarrow H$, definiert durch $j(x) = x$ für alle $x \in U$, ein Halbgruppenmonomorphismus. Die identische Abbildung $\mathrm{id}_H\colon H \to H$ ist ein Isomorphismus.

4. Sei $(H_i)_{i\in I}$ eine Familie von Halbgruppen mit neutralen Elementen $e_i \in H_i$, und sei H ihr (äußeres) direktes Produkt. Für $j \in I$ seien die *Projektion* $p_j\colon H \to H_j$ und die *Einlagerung* $\varepsilon_j\colon H_j \to H$ definiert durch $p_j\big((a_i)_{i\in I}\big) = a_j$ und $\varepsilon_j(a_j) = (x_i)_{i\in I}$ mit $x_j = a_j$ und $x_i = e_i$ für alle $i \in I \setminus \{j\}$. Dann ist p_j ein Epimorphismus, ε_j ein Monomorphismus, $p_j \circ \varepsilon_j = \mathrm{id}_{H_j}$, und für $i \neq j$ ist $p_j \circ \varepsilon_i$ der Einshomomorphismus.

Sei $(H'_i)_{i\in I}$ eine weitere Familie von Halbgruppen, H' ihr direktes Produkt, und für jedes $i \in I$ sei $\varphi_i\colon H_i \to H'_i$ ein Homomorphismus. Dann ist auch $\varphi\colon H \to H'$, definiert durch $\varphi\big((a_i)_{i\in I}\big) = (\varphi_i(a_i))_{i\in I}$, ein Homomorphismus.

5. Sei K ein Körper, und seien V und W zwei K-Vektorräume. Dann ist jede K-lineare Abbildung $f\colon V \to W$ ein Homomorphismus der Additionsgruppen, und die Definition des Kernes von f stimmt mit der Definition aus der Linearen Algebra überein.

6. Sei K ein Körper und $n \in \mathbb{N}$. Dann ist die Determinantenabbildung $\det\colon \mathsf{GL}_n(K) \to K^\times$ ein Gruppenepimorphismus, und $\mathrm{Ker}(\det) = \mathsf{SL}_n(K) = \{A \in \mathsf{M}_n(K) \mid \det(A) = 1\} \lhd \mathsf{GL}_n(K)$.

7. Die Exponentialfunktion $\exp\colon \mathbb{R} \to \mathbb{R}_{>0}$ und die (natürliche) Logarithmusfunktion $\log\colon \mathbb{R}_{>0} \to \mathbb{R}$ sind zueinander inverse Isomorphismen der additiven Gruppe $(\mathbb{R}, +)$ und der multiplikativen Gruppe $(\mathbb{R}_{>0}, \cdot)$.

8. Sei $\boldsymbol{e}\colon \mathbb{R} \to \mathbb{C}^\times$ definiert durch $\boldsymbol{e}(x) = \mathrm{e}^{2\pi \mathrm{i} x}$. Dann ist $\boldsymbol{e}$ ein Gruppenhomomorphismus, $\mathrm{Ker}(\boldsymbol{e}) = \mathbb{Z}$, $\boldsymbol{e}(\mathbb{R}) = \big\{z \in \mathbb{C} \;\big|\; |z| = 1\big\}$ ist der komplexe Einheitskreis, und $\boldsymbol{e}(\mathbb{Q}) = \mu(\mathbb{C})$.

9. Sei $f\colon X \to Y$ eine bijektive Abbildung nichtleerer Mengen, und sei $f^*\colon \mathrm{Abb}(X, X) \to \mathrm{Abb}(Y, Y)$ definiert durch $f^*(\varphi) = f \circ \varphi \circ f^{-1}$. Dann ist f^* ein Halbgruppenisomorphismus, $(f^*)^{-1} = (f^{-1})^*$, und $f^* \,|\, \mathfrak{S}(X)\colon \mathfrak{S}(X) \to \mathfrak{S}(Y)$ ist ein Gruppenisomorphismus. Insbesondere folgt: Ist X endlich, $|X| = n \in \mathbb{N}$, so existiert ein Gruppenisomorphismus $\mathfrak{S}(X) \to \mathfrak{S}_n$.

Definitionen und Bemerkungen 2.4.6.

1. Man nennt zwei Halbgruppen H und H' *isomorph* und schreibt $H \cong H'$, wenn es einen Isomorphismus $f\colon H \to H'$ gibt. Man schreibt dafür auch $f\colon H \xrightarrow{\sim} H'$.

2. Isomorphie ist eine Äquivalenzrelation auf der Klasse der Halbgruppen (bzw. Gruppen), d. h., für Halbgruppen H, H', H'' gilt:

$$H \cong H; \quad \text{aus } H \cong H' \text{ folgt } H' \cong H; \quad \text{aus } H \cong H' \text{ und } H' \cong H'' \text{ folgt } H \cong H''.$$

[Beweis: $\mathrm{id}_H\colon H \to H$ ist ein Isomorphismus. Mit $f\colon H \to H'$ ist auch $f^{-1}\colon H' \to H$ ein Isomorphismus (siehe Lemma 2.4.2.4). Sind $f\colon H \to H'$ und $f'\colon H' \to H''$ Isomorphismen, so ist auch $f' \circ f\colon H \to H''$ ein Isomorphismus.]

3. **Isomorphieprinzip**. Isomorphe Strukturen haben dieselben (strukturspezifischen) Eigenschaften. In dieser allgemeinen (und unpräzisen) Formulierung ist das Isomorphieprinzip natürlich nicht beweisbar. Wir formulieren beispielhaft eine Reihe von Spezialfällen, welche dann, für sich genommen, trivial sind. Seien H und $\overline{H}$ nichtleere Mengen, $*$ eine Verknüpfung auf H, $\bar{*}$ eine Verknüpfung auf $\overline{H}$ und $f\colon H \to \overline{H}$ ein $(*, \bar{*})$-Isomorphismus.

(a) $*$ ist genau dann kommutativ (bzw. assoziativ), wenn $\bar{*}$ kommutativ (bzw. assoziativ) ist.

(b) $e \in H$ ist genau dann neutral bzgl. $*$, wenn $f(e) \in \overline{H}$ neutral bzgl. $\bar{*}$ ist.

(c) $(H, *)$ ist genau dann eine (abelsche) Gruppe, wenn $(\overline{H}, \bar{*})$ eine (abelsche) Gruppe ist.

(d) Seien $(H,*)$ und $(\overline{H},\bar{*})$ Gruppen. Dann definiert die Zuordnung $U \mapsto f(U)$ eine inklusionserhaltende Bijektion von der Menge der Untergruppen von H auf die Menge der Untergruppen von $\overline{H}$. Man sagt dann H und $\overline{H}$ haben dieselbe Untergruppenstruktur.

4. Häufig ist es sinnvoll, isomorphe Halbgruppen als gleich anzusehen. Ist $\phi\colon H \to \overline{H}$ ein Isomorphismus, so sagen wir, wir identifizieren H mit $\overline{H}$ vermöge ϕ und schreiben $H = \overline{H}$, wenn wir für alle $a \in H$ nicht mehr zwischen a und $\phi(a)$ unterscheiden.

5. Sei $(H_i)_{i\in I}$ eine Familie von Halbgruppen mit neutralen Elementen $e_i \in H_i$. Sei $\emptyset \neq J \subset I$, und für alle $i \in I \setminus J$ sei $H_i = \{e_i\}$. Dann ist die Abbildung

$$\phi\colon \prod_{i\in I} H_i \;\to\; \prod_{i\in J} H_i\,, \quad \text{definiert durch} \quad \phi\big((a_i)_{i\in I}\big) = \big((a_i)_{i\in J}\big)\,,$$

ein Isomorphismus, vermöge dessen wir die beiden Gruppen identifizieren. Insbesondere identifizieren wir jedes direkte Produkt $H\times\{e\}$ aus einer Halbgruppe H und einer trivialen Gruppe mit $H\colon\ H\times\{e\} = H$.

2.5. Kongruenzrelationen, Faktorstrukturen und Isomorphiesätze

Definition und Satz 2.5.1 (Kongruenzen und Faktorstrukturen)**.** *Sei H eine nichtleere Menge, $*$ eine Verknüpfung auf H, $\sim$ eine Äquivalenzrelation auf H, $H/\!\sim\ = \{[a]_\sim \mid a \in H\}$ die Menge der Äquivalenzklassen von H bezüglich $\sim$ und $\pi\colon H \to H/\!\sim$ die Äquivalenzklassenabbildung.*

Die Äquivalenzrelation $\sim$ heißt *Kongruenzrelation* (bezüglich $*$), wenn für alle $a, b, c \in H$ gilt:

Aus $a \sim b$ folgt $a * c \sim b * c$ und $c * a \sim c * b$.

Sei nun $\sim$ eine Kongruenzrelation bezüglich $*$. Dann existiert genau eine Verknüpfung $\widetilde{*}$ auf $H/\!\sim$, sodass $\pi\colon H \to H/\!\sim$ ein $(*,\widetilde{*})$-Epimorphismus ist. Insbesondere folgt:

1. *Für alle $a, b \in H$ ist $[a]_\sim \mathbin{\widetilde{*}} [b]_\sim = [a * b]_\sim$.*
2. *Ist $(H,*)$ kommutativ (eine Halbgruppe bzw. eine Gruppe), so gilt das auch für $(H/\!\sim,\widetilde{*})$.*

Man nennt $\widetilde{*}$ die von $*$ *induzierte Verknüpfung* auf $H/\!\sim$ und $(H/\!\sim,\widetilde{*})$ die *Faktorstruktur* (*Faktorhalbgruppe* bzw. *Faktorgruppe*) von $(H,*)$. Der Epimorphismus $\pi\colon H \to H/\!\sim$ heißt *kanonischer Epimorphismus.*

Beweis. Die Eindeutigkeit von $\widetilde{*}$ folgt auf Grund der Definition. Wir zeigen nun, dass für $a, b \in H$ die Kongruenzklasse $[a * b]_\sim$ nur von den Kongruenzklassen $[a]_\sim$ und $[b]_\sim$ abhängt. Dann definiert man $\widetilde{*}$ wie in 1., und 2. folgt mit Lemma 2.4.2.3.

Seien also $a, a', b, b' \in H$ mit $[a]_\sim = [a']_\sim$ und $[b]_\sim = [b']_\sim$. Dann ist $a \sim a'$ und $b \sim b'$, und wir erhalten $a * b \sim a' * b \sim a' * b'$, also auch $[a * b]_\sim = [a' * b']_\sim$. □

Definition 2.5.2. Sei H eine kommutative Halbgruppe.

1. $a, b \in H$ heißen *assoziiert*, $a \simeq b$, wenn $aH = bH$ $[\iff a \in bH$ und $b \in aH\,]$.
2. H heißt *reduziert* wenn für alle $a, b \in H$ gilt: Aus $a \simeq b$ folgt $a = b$.

Definition und Satz 2.5.3. *Sei H eine kommutative Halbgruppe.*

1. *$\simeq$ ist eine Kongruenzrelation auf H, und $H/\!\simeq$ ist eine reduzierte kommutative Halbgruppe.*
   Man nennt $H_{\mathrm{red}} = H/\!\simeq$ die zu H assoziierte reduzierte Halbgruppe.
2. *Seien $a, b \in H$, und sei $a \in H^\bullet$. Genau dann ist $a \simeq b$, wenn es ein $\varepsilon \in H^\times$ gibt mit $b = a\varepsilon$, und dann ist auch $b \in H^\bullet$. Insbesondere ist $[a]_\simeq = aH^\times$.*
3. *Sei H ein Monoid. Dann ist $[a]_\simeq = aH^\times$ für alle $a \in H$, und H ist genau dann reduziert, wenn $H^\times = \{1\}$.*

BEWEIS. 1. Offensichtlich ist $\simeq$ eine Äquivalenzrelation, und für alle a, b, $c \in H$ gilt: Aus $aH = bH$ folgt $caH = cbH$. Daher ist $\simeq$ eine Kongruenzrelation und $H/\simeq$ eine kommutative Halbgruppe. Es bleibt zu zeigen, dass $H/\simeq$ reduziert ist. Seien also a, $b \in H$ mit $[a]_\simeq \simeq [b]_\simeq$. Dann gibt es x, $y \in H$ mit $[a]_\simeq = [b]_\simeq [x]_\simeq$ und $[b]_\simeq = [a]_\simeq [y]_\simeq$, also $[a]_\simeq = [bx]_\simeq$ und $[b]_\simeq = [ay]_\simeq$. Damit folgt $a \simeq bx$ und $b \simeq ay$, also insbesondere $a \in bxH \subset bH$ und $b \in ayH \subset aH$. Folglich ist $a \simeq b$ und daher $[a]_\simeq = [b]_\simeq$.

2. Ist $b = a\varepsilon$ mit $\varepsilon \in H^\times$, so folgt $b \in aH$ und $a = b\varepsilon^{-1} \in bH$, also $a \simeq b$, und offensichtlich ist auch $b \in H^\bullet$. Ist $a \simeq b$, so gibt es x, $y \in H$ mit $a = bx$ und $b = ay$, es folgt $a = ayx$ und daher $xy = 1$, also x, $y \in H^\times$.

3. Klar nach 2. □

Bemerkungen 2.5.4.

1. Sei H eine kommutative Halbgruppe. Dann ist $[1]_\simeq = H^\times$, und genau dann ist H eine Gruppe, wenn $a \simeq b$ für alle a, $b \in H$.

2. Für $a \in \mathbb{Z}^\bullet = (\mathbb{Z}^\bullet, \cdot)$ ist $[a]_\simeq = \{\pm a\}$, und die Abbildung $\mathbb{Z}_{\mathrm{red}} \to \mathbb{N}$, $[a]_\simeq \mapsto |a|$, ist ein Isomorphismus.

Definition und Satz 2.5.5 (Kongruenzrelationen auf Gruppen)**.** *Sei G ein Gruppe.*

1. *Sei $N \lhd G$. Für a, $b \in G$ definiere man $a \equiv_N b$, wenn $aN = bN$. Dann ist $\equiv_N$ eine Kongruenzrelation auf G, für alle $a \in G$ ist $[a]_{\equiv_N} = aN$ und $G/\equiv_N = G/N$. Bezeichnet $\pi_N \colon G \to G/N$ den kanonischen Epimorphismus, so ist $\mathrm{Ker}(\pi_N) = N$.*
2. *Sei $\sim$ eine Kongruenzrelation auf G und $N = [e]_\sim$. Dann ist $N \lhd G$ und $\sim = \equiv_N$ wie in 1.*

Sei $N \lhd G$. Sind a, $b \in G$ mit $aN = bN$ (also $a \equiv_N b$), so nennt man a und b *kongruent modulo N*. Die Gruppe $G/N = G/\equiv_N$ heißt *Faktorgruppe von G modulo N*, und den kanonischen Epimorphismus $\pi_N \colon G \to G/N$ nennt man *Restklassenhomomorphismus modulo N*. Schreibt man die Verknüpfung auf G/N multiplikativ, so ist $(aN)(bN) = abN$ für alle a, $b \in N$. Ist $(G, +)$ eine additive Gruppe, so schreibt man auch G/N additiv, und dann ist $(a + N) + (b + N) = (a + b) + N$ für alle a, $b \in G$.

Im Falle $N = \{e\}$ ist $\pi_{\{e\}} \colon G \to G/\{e\}$ ein Isomorphismus. Wir identifizieren die beiden Gruppen auf Grund dieses Isomorphismus und schreiben $G = G/\{e\}$.

Sei $m \in \mathbb{N}$. Für a, $b \in \mathbb{Z}$ ist genau dann $a \equiv b \bmod m$ (siehe 2.3.5), wenn $a \equiv_{m\mathbb{Z}} b$. Die Restklassenabbildung $\mathbb{Z} \to \mathbb{Z}/m\mathbb{Z}$, $a \mapsto a + m\mathbb{Z}$, ist ein Gruppenepimorphismus, und nach Satz 2.4.4.7 ist $\mathbb{Z}/m\mathbb{Z} = \langle 1 + m\mathbb{Z} \rangle$ eine zyklische Gruppe mit m Elementen.

BEWEIS. 1. Es genügt, zu zeigen, dass $\equiv_N$ eine Kongruenzrelation auf G ist. Seien also a, b, $c \in G$ und $a \equiv_N b$. Dann ist $aN = bN$ und daher auch $Na = Nb$, und es folgt $caN = cbN$ und $Nac = Nbc$, also $ca \equiv_N cb$ und $ac \equiv_N bc$.

2. Sei $\pi \colon G \to G/\sim$ der kanonische Epimorphismus. Dann ist $\mathrm{Ker}(\pi) = [e]_\sim = N$, also $N \lhd G$, und für alle a, $b \in G$ ist genau dann $a \sim b$, wenn $\pi(a) = \pi(b)$, und das ist nach Satz 2.4.4.6 äquivalent mit $aN = bN$. □

Satz 2.5.6 (Kanonische Faktorisierung einer Abbildung; Homomorphiesatz)**.** *Sei $f \colon H \to \overline{H}$ eine Abbildung nichtleerer Mengen, sei die Relation $\sim_f$ auf H definiert durch*

$$a \sim_f b \iff f(a) = f(b)\,, \quad \text{und sei} \quad \pi_f \colon H \to H/\sim_f \quad \text{definiert durch} \quad \pi_f(a) = [a]_{\sim_f}\,.$$

1. *$\sim_f$ ist eine Äquivalenzrelation auf H, und für alle $a \in H$ ist $[a]_{\sim_f} = f^{-1}(\{f(a)\})$.*

2. *Sei* $j = (f(H) \hookrightarrow \overline{H})$ *die Inklusionsabbildung. Dann gibt es genau eine bijektive Abbildung* $f^*\colon H/\!\sim_f \;\to\; f(H)$*, so dass folgendes Diagramm kommutativ ist*:

$$\begin{array}{ccc} H & \xrightarrow{\;f\;} & \overline{H} \\ {\scriptstyle \pi_f}\big\downarrow & & \big\uparrow{\scriptstyle j} \\ H/\!\sim_f & \xrightarrow[\;f^*\;]{} & f(H) \end{array}$$

Es ist dann $f^*([a]_{\sim_f}) = f(a)$ *für alle* $a \in H$*. Insbesondere ist* $\overline{f} = j \circ f^*\colon H/\!\sim_f \;\to\; \overline{H}$ *die eindeutig bestimmte injektive Abbildung mit* $\overline{f}\big([a]_{\sim_f}\big) = f(a)$ *für alle* $a \in H$*.*

3. (Homomorphiesatz) *Sei* $*$ *eine Verknüpfung auf* H*,* $\bar{*}$ *eine Verknüpfung auf* $\overline{H}$*, und sei* f *ein* $(*, \bar{*})$*-Homomorphismus. Dann ist* $\sim_f$ *eine Kongruenzrelation bzgl.* $*$ *auf* H*. Bezüglich der von* $*$ *induzierten Verknüpfung auf* $H/\!\sim_f$ *ist dann* $\overline{f}$ *ein Monomorphismus und* f^* *ein Isomorphismus.*

Beweis. 1. Offensichtlich ist $\sim_f$ eine Äquivalenzrelation auf H, und für alle $a \in H$ ist

$$f^{-1}\big(\{f(a)\}\big) = \{x \in H \mid f(x) = f(a)\} = [a]_{\sim_f}\,.$$

2. Ist $a \in H$, so hängt $f(a)$ definitionsgemäß nur von der Äquivalenzklasse $[a]_{\sim_f}$ ab. Definiert man $f^*\colon H/\!\sim_f \;\to f(H)$ durch $f^*([a]_{\sim_f}) = f(a)$, so hat f^* die behaupteten Eigenschaften und ist offensichtlich die einzige Abbildung, die das Diagramm kommutativ macht.

3. Seien $a, b, c \in H$ und $a \sim_f b$. Dann folgt $f(a * c) = f(a) \bar{*} f(c) = f(b) \bar{*} f(c) = f(b * c)$ und daher $a * c \sim_f b * c$. In gleicher Weise folgt auch $c * a \sim_f c * b$, und daher ist $\sim_f$ eine Kongruenzrelation. Nach 2. genügt es nun, zu zeigen, dass f^* bzgl. der von $*$ induzierten Verknüpfung $\widetilde{*}$ auf $H/\!\sim_f$ ein Homomorphismus ist. Für $a, b \in H$ ist aber

$$f^*\big([a]_{\sim_f} \widetilde{*}\, [b]_{\sim_f}\big) = f^*\big([a * b]_{\sim_f}\big) = f(a * b) = f(a) \bar{*} f(b) = f^*\big([a]_{\sim_f}\big) \bar{*}\, f^*\big([b]_{\sim_f}\big)\,.$$

□

Satz 2.5.7 (Homomorphiesatz der Gruppentheorie)**.** *Sei* $f\colon G \to \overline{G}$ *ein Gruppenhomomorphismus,* $\pi\colon G \to G/\mathrm{Ker}(f)$ *der kanonische Restklassenhomomorphismus und* $j = (f(G) \hookrightarrow \overline{G})$ *die Injektionsabbildung. Dann gibt es genau einen Gruppenisomorphismus* $f^*\colon G/\mathrm{Ker}(f) \to f(G)$*, so dass folgendes Diagramm kommutativ ist*:

$$\begin{array}{ccc} G & \xrightarrow{\;f\;} & \overline{G} \\ {\scriptstyle \pi}\big\downarrow & & \big\uparrow{\scriptstyle j} \\ G/\mathrm{Ker}(f) & \xrightarrow[\;f^*\;]{} & f(G) \end{array}$$

Es ist dann $f^*\big(a\,\mathrm{Ker}(f)\big) = f(a)$ *für alle* $a \in G$*. Insbesondere ist* $\overline{f} = j \circ f^*\colon G/\mathrm{Ker}(f) \;\to\; \overline{G}$ *der eindeutig bestimmte Monomorphismus mit* $\overline{f}\big(a\,\mathrm{Ker}(f)\big) = f(a)$ *für alle* $a \in G$*.*

Beweis. Das ist ein Spezialfall von Satz 2.5.6. Für $a \in G$ ist nach Satz 2.4.4.6 und Satz 2.5.6 nämlich $[a]_{\sim_f} = f^{-1}\big(\{f(a)\}\big) = a\,\mathrm{Ker}(f) = [a]_{\equiv_{\mathrm{Ker}(f)}}$, also $\sim_f \;= \equiv_{\mathrm{Ker}(f)}$, und daher $G/\!\sim_f \;= G/\mathrm{Ker}(f)$. □

Satz 2.5.8 (1. Isomorphiesatz)**.** *Sei* G *eine Gruppe,* $U < G$ *und* $N \lhd G$*. Dann ist* $UN < G$*,* $U \cap N \lhd U$*, und die Abbildung*

$$\varphi\colon U/U \cap N \to UN/N\,, \quad \textit{definiert durch} \quad \varphi\big(u(U \cap N)\big) = uN \quad \textit{für alle} \quad u \in U\,,$$

ist ein Gruppenisomorphismus.

BEWEIS. Wir zeigen zunächst $UN < G$ mit Hilfe von Satz 2.2.2. Seien $z = xy$ und $z' = x'y' \in UN$ mit $x, x' \in U$ und $y, y' \in N$. Wegen $N \lhd G$ folgt $zz'^{-1} = xyy'^{-1}x'^{-1} = (xx'^{-1})(x'yy'^{-1}x'^{-1}) \in UN$. Wegen $N \lhd G$ ist insbesondere $N \lhd UN$. Sei $\pi\colon UN \to UN/N$ der kanonische Restklassenhomomorphismus und $f = \pi\,|\,U\colon U \to UN/N$. Für $u \in U$ und $x \in N$ ist $uxN = uN = f(u)$, und daher ist f surjektiv. Es ist $\mathrm{Ker}(f) = U \cap \mathrm{Ker}(\pi) = U \cap N \lhd U$, und daher induziert f nach Satz 2.5.7 einen Isomorphismus $\varphi\colon U/U \cap N \to f(U) = UN/N$ der gewünschten Eigenschaft. □

Korollar 2.5.9. *Für alle $a, b \in \mathbb{Z}$ ist $|ab| = \mathrm{ggT}(a,b)\ \mathrm{kgV}(a,b)$.*

BEWEIS. Sei $d = \mathrm{ggT}(a,b)$ und $e = \mathrm{kgV}(a,b)$. Ist $ab = 0$, so ist $e = 0$, und wir sind fertig. Sei also $ab \neq 0$. Nach Satz 2.2.5 und Satz 2.5.8 ist dann $d\mathbb{Z}/a\mathbb{Z} = a\mathbb{Z} + b\mathbb{Z}/a\mathbb{Z} \cong b\mathbb{Z}/a\mathbb{Z} \cap b\mathbb{Z} = b\mathbb{Z}/e\mathbb{Z}$, und mit Bemerkung 2.3.9 folgt

$$\frac{d}{|a|} = \frac{|b|}{e}, \quad \text{und daher} \quad |ab| = de\,.$$

□

Satz 2.5.10. *Sei $f\colon G \to \overline{G}$ ein Gruppenepimorphismus, Σ die Menge aller Untergruppen $U < G$ mit $\mathrm{Ker}(f) \subset U$ und $\overline{\Sigma}$ die Menge aller Untergruppen von $\overline{G}$. Dann sind*

$$\widetilde{f}\colon \begin{cases} \Sigma & \to & \overline{\Sigma} \\ U & \to & f(U) \end{cases} \qquad \text{und} \qquad \widetilde{f}^*\colon \begin{cases} \overline{\Sigma} & \to & \Sigma \\ \overline{U} & \to & f^{-1}(\overline{U}) \end{cases}$$

zueinander inverse inklusionserhaltende Bijektionen, und für alle $U, V \in \Sigma$ gilt:

1. *Ist $U \subset V$ und $\{\sigma_i \mid i \in I\} \subset V$ ein Repräsentantensystem von V/U, so ist $\{f(\sigma_i) \mid i \in I\} \subset f(V)$ ein Repräsentantensystem von $f(V)/f(U)$. Insbesondere ist $(V : U) = (f(V) : f(U))$, und die Abbildung*

   $$\widehat{f}\colon V/U \to f(V)/f(U)\,, \quad \text{definiert durch} \quad \widehat{f}(vU) = f(v)f(U) \quad \text{für alle} \quad v \in V\,,$$

   ist bijektiv.
2. *Genau dann ist $U \lhd V$, wenn $f(U) \lhd f(V)$, und dann ist die Abbildung $\widehat{f}$ aus 1. ein Isomorphismus.*

BEWEIS. Ist $\overline{U} \in \overline{\Sigma}$, so ist $f^{-1}(\overline{U}) < G$ nach Satz 2.4.4.4 und $f^{-1}(\overline{U}) \supset f^{-1}(\{\overline{e}\}) = \mathrm{Ker}(f)$, also folgt $f^{-1}(\overline{U}) \in \Sigma$, und wegen der Surjektivität von f ist $\widetilde{f} \circ \widetilde{f}^*(\overline{U}) = f(f^{-1}(\overline{U})) = \overline{U}$. Ist $U \in \Sigma$, so ist $f(U) \in \overline{\Sigma}$ nach Satz 2.4.4.2, und es folgt zunächst $\widetilde{f}^* \circ \widetilde{f}(U) = f^{-1}(f(U)) \supset U$. Zum Nachweis der umgekehrten Inklusion, sei $x \in f^{-1}(f(U))$, also $f(x) = f(u)$ mit $u \in U$. Dann ist $f(xu^{-1}) = f(x)f(u)^{-1} = \overline{e}$, also $xu^{-1} \in \mathrm{Ker}(f) \subset U$ und daher $x = xu^{-1}u \in U$.
Seien nun $U, V \in \Sigma$ mit $U \subset V$, und sei $\{\sigma_i \mid i \in I\} \subset V$ ein Repräsentantensystem von V/U. Dann ist

$$V = \biguplus_{i \in I} \sigma_i U\,, \quad \text{also} \quad f(V) = \bigcup_{i \in I} f(\sigma_i)f(U)\,,$$

und wir müssen die Disjunktheit der Zerlegung zu zeigen. Seien $i, j \in I$ mit $f(\sigma_i)f(U) \cap f(\sigma_j)f(U) \neq \emptyset$. Dann gibt es $x, y \in U$ mit $f(\sigma_i)f(x) = f(\sigma_j)f(y)$ und daher $(\sigma_j y)^{-1}(\sigma_i x) \in \mathrm{Ker}(f) \subset U$. Folglich ist $\sigma_i x \in \sigma_j yU$, also $\sigma_i U \cap \sigma_j U \neq \emptyset$ und daher $i = j$. Insbesondere ist $\widehat{f}$ eine bijektive Abbildung. Nach Satz 2.4.4.3 und 5 ist genau dann $U \lhd V$, wenn $f(U) \lhd f(V)$, und dann ist $\widehat{f}$ ein Homomorphismus (also ein Isomorphismus), denn für alle $v, w \in V$ ist

$$\widehat{f}\big((vU)(wU)\big) = \widehat{f}(vwU) = f(vw)f(U) = f(v)f(w)f(U) = \big(f(v)f(U)\big)\big(f(w)f(U)\big) = \widehat{f}(vU)\widehat{f}(wU)\,.$$

□

Korollar 2.5.11. *Sei G eine Gruppe und $N \lhd G$.*

1. $\{U/N \mid U < G\,,\ N \subset U\}$ *ist die Menge der Untergruppen von* G/N.
2. *Sei* $U < G$ *mit* $N \subset U$.
   (a) *Die Abbildung* $\phi\colon G/U \to (G/N)/(U/N)$, *definiert durch* $\phi(xU) = (xN)(U/N)$ *für alle* $x \in G$, *ist bijektiv.*
   (b) (2. Isomorphiesatz) *Genau dann ist* $U/N \lhd G/N$, *wenn* $U \lhd G$, *und dann ist die Abbildung* ϕ *aus* (a) *ein Isomorphismus.*

Beweis. Nach Satz 2.5.10, angewandt mit dem Restklassenhomomorphismus $f\colon G \to G/N = \overline{G}$ und $V = G$. □

Korollar 2.5.12 (Universelle Eigenschaft des Restklassenhomomorphismus). *Sei* G *eine Gruppe,* $N \lhd G$ *und* $f\colon G \to \overline{G}$ *ein Gruppenhomomorphismus mit* $N \subset \operatorname{Ker}(f)$. *Dann existiert genau ein Gruppenhomomorphismus* $\widehat{f}\colon G/N \to \overline{G}$, *so dass* $\widehat{f}(xN) = f(x)$ *für alle* $x \in G$. *Es ist dann* $\widehat{f}(G) = f(G)$ *und* $\operatorname{Ker}(\widehat{f}) = \operatorname{Ker}(f)/N$.

Beweis. Sei $U = \operatorname{Ker}(f)$. Nach Korollar 2.5.11 ist die Abbildung $\varphi\colon G/U \to (G/N)/(U/N)$, definiert durch $\varphi(xU) = (xN)(U/N)$, ein Isomorphismus, und nach Satz 2.5.7 ist die Abbildung $\overline{f}\colon G/U \to \overline{G}$, definiert durch $\overline{f}(xU) = f(x)$, ein Monomorphismus. Sei nun $\pi\colon G/N \to (G/N)/(U/N)$ der Restklassenhomomorphismus. Dann ist $\widehat{f} = \overline{f} \circ \varphi^{-1} \circ \pi\colon G/N \to \overline{G}$ ein Homomorphismus mit $\widehat{f}(xN) = f(x)$ für alle $x \in G$. Offensichtlich ist $\widehat{f}$ dadurch eindeutig bestimmt, es ist $\widehat{f}(G) = f(G)$, und da $\overline{f} \circ \varphi^{-1}$ injektiv ist, folgt $\operatorname{Ker}(\widehat{f}) = \operatorname{Ker}(\pi) = U/N$. □

Satz 2.5.13 (Struktursatz für zyklische Gruppen). *Sei* G *eine zyklische Gruppe und* $g \in G$ *mit* $G = \langle g \rangle$ (*also* $|G| = \operatorname{ord}(g)$).

1. *Ist* $|G| = \infty$, *so gibt es genau einen Isomorphismus* $\phi\colon \mathbb{Z} \to G$ *mit* $\phi(1) = g$, *und zu jedem* $d \in \mathbb{N}$ *gibt es genau eine Untergruppe* $U < G$ *mit* $(G\colon U) = d$, *nämlich* $U = \phi(d\mathbb{Z}) = \langle g^d \rangle$.
2. *Ist* $|G| = n \in \mathbb{N}$, *so gibt es genau einen Isomorphismus* $\phi\colon \mathbb{Z}/n\mathbb{Z} \to G$ *mit* $\phi(1 + n\mathbb{Z}) = g$, *und zu jedem* $d \in \mathbb{N}$ *mit* $d \mid n$ *gibt es genau eine Untergruppe* $U < G$ *mit* $(G\colon U) = d$, *nämlich* $U = \phi(d\mathbb{Z}/n\mathbb{Z}) = \langle g^d \rangle$, *und es ist*
$$|\langle g^d \rangle| = \frac{n}{d}\,.$$

Beweis. Die Eindeutigkeit von ϕ folgt in jedem Fall aus Satz 2.4.4.7. Definiert man $f\colon \mathbb{Z} \to G$ durch $f(n) = g^n$ für alle $n \in \mathbb{Z}$, so ist f surjektiv nach Definition und ein Homomorphismus nach Lemma 2.1.8.2. Nach Satz 2.2.10 ist $\operatorname{Ker}(f) = n\mathbb{Z}$ mit $n \in \mathbb{N}_0$.

Ist $n = 0$, so ist f ein Isomorphismus und daher $\{f(d\mathbb{Z}) \mid d \in \mathbb{N}_0\}$ die Menge der Untergruppen von G. Für $d \in \mathbb{N}$ ist $f(d\mathbb{Z}) = \langle g^d \rangle$ nach Satz 2.4.4.7, und $(G\colon \langle g^d \rangle) = (\mathbb{Z}\colon d\mathbb{Z}) = d$. Damit folgt 1.

Ist $n > 0$, so gibt es nach Satz 2.5.7 einen Isomorphismus $\phi\colon \mathbb{Z}/n\mathbb{Z} \to G$ mit $\phi(1 + n\mathbb{Z}) = g$. Nach Satz 2.5.10 induziert f ein bijektive Abbildung f^* von der Menge $\mathcal{U}$ der Untergruppen $U < \mathbb{Z}$ mit $n\mathbb{Z} \subset U$ auf die Menge aller Untergruppen von G vermöge $f^*(U) = U/n\mathbb{Z}$. Nach Satz 2.2.5 ist $\mathcal{U} = \left\{d\mathbb{Z} \;\middle|\; d \in \mathbb{N}\,,\ d \mid n\right\}$, und für $d \in \mathbb{N}$ mit $d \mid n$ ist $f(d\mathbb{Z}) = \langle g^d \rangle$, $(G\colon \langle g^d \rangle) = (\mathbb{Z}\colon d\mathbb{Z}) = d$, und nach Satz 2.3.7 folgt
$$|\langle g^d \rangle| = \frac{|G|}{(G\colon \langle g^d \rangle)} = \frac{n}{d}\,.$$

□

Korollar 2.5.14. *Sei* $G = \langle g \rangle$ *eine zyklische Gruppe, und sei* $|G| = 2m$ *mit* $m \in \mathbb{N}$. *Dann ist*
$$\prod_{h \in G} h = g^m\,, \quad \textit{und } g^m \textit{ ist das einzige Element der Ordnung 2 in } G\,.$$

BEWEIS. Es ist $m(2m-1) \equiv m \bmod 2m$ und daher

$$\prod_{h \in G} h = \prod_{i=0}^{2m-1} g^i = g^{m(2m-1)} = g^m \,.$$

Ist $k \in [1, 2m-1]$, so ist genau dann $\operatorname{ord}(g^k) = 2$, wenn $(g^k)^2 = g^{2k} = e$, also wenn $2m \mid 2k$, und das ist genau dann der Fall, wenn $k = m$. □

CHAPTER 3

Grundbegriffe der Ringtheorie

3.1. Ringe: Definitionen und Beispiele

Definition 3.1.1. Ein Ring $R = (R, 0_R, 1_R, +_R, \cdot_R)$ ist eine Menge R, gemeinsam mit zwei ausgezeichneten Elementen $0_R \in R$ und $1_R \in R$, und zwei Verknüpfungen $+_R$ und $\cdot_R$, so dass gilt:

(R1) $(R, +)$ ist eine (additive) abelsche Gruppe mit neutralem Element 0_R.

(R2) $(R, \cdot)$ ist eine (multiplikative) Halbgruppe mit neutralem Element 1_R.

(R3) Für alle $a, b, c \in R$ gelten die Distributivgesetze

$$a \cdot_R (b +_R c) = (a \cdot_R b) +_R (a \cdot_R c) \quad \text{und} \quad (b +_R c) \cdot_R a = (b \cdot_R a) +_R (c \cdot_R a)\,.$$

Man nennt $+_R$ die *Ringaddition*, $\cdot_R$ die Ringmultiplikation, 0_R die *Null* oder das *Nullelement* und 1_R die *Eins* oder das *Einselement* von R.

Ein Ring heißt *kommutativ*, wenn die Ringmultiplikation kommutativ ist.

Wenn Verwechslungen nicht zu befürchten sind, schreibt man kurz R oder $(R, +, \cdot)$ an Stelle von $(R, 0_R, 1_R, +_R, \cdot_R)$. Man schreibt 0 an Stelle von 0_R, 1 an Stelle von 1_R, $+$ an Stelle von $+_R$, für $a, b \in R$ setzt man $ab = a \cdot b = a \cdot_R b$, und man vereinbart die Konvention *Punkt- vor Strichrechnung*. Dann erhalten die Distributivgesetze die Form $a(b + c) = ab + ac$ und $(b + c)a = ba + ca$.

Man nennt $(R, +)$ die *Additionsgruppe* des Ringes R und verwendet für sie in in 2.1.6.4 formulierten additiven Konventionen. Insbesondere bezeichnet man das additive Inverse eines Elements $a \in R$ mit $-a$, für $a, b \in R$ definiert man $a - b = a + (-b)$, man verwendet das Summenzeichen und die Notation der Vielfachen na für $a \in R$ und $n \in \mathbb{Z}$.

Man nennt $(R, \cdot)$ die *multiplikative Halbgruppe* von R, ihre Einheitengruppe $R^\times = (R, \cdot)^\times$ die *Einheitengruppe* von R und $R^\bullet = (R, \cdot)^\bullet$ das Monoid der *regulären* (*kürzbaren*) *Elemente* von R. Man verwendet das Produktzeichen, die Notation von Potenzen, und (falls R kommutativ ist) die Notation von Brüchen mit Einheiten im Nenner: Für $b \in R$ und $a \in R^\times$ setzt man

$$\frac{b}{a} = a^{-1}b = ba^{-1}\,.$$

Es gelten dann die üblichen Regeln des Bruchrechnens.

Ist R kommutativ, so nennt man zwei Elemente $a, b \in R$ *assoziiert*, $a \simeq b$, wenn $aR = bR$ (siehe Definition 2.5.2).

Lemma 3.1.2 (Rechenregeln für Ringe)**.** *Sei R ein Ring, und seien $a, b \in R$.*

1. *Ist $ab = ba$, so gilt für alle $n \in \mathbb{N}_0$*

$$(a + b)^n = \sum_{i=0}^{n} \binom{n}{i} a^{n-i} b^i.$$

2. $a \cdot 0_R = 0_R \cdot a = 0_R$.

3. $a(-b) = (-a)b = -ab$ *und* $(-a)(-b) = ab$.
4. *Ist* $a \in R^\times$, *so ist* $-a \in R^\times$ *und* $(-a)^{-1} = -a^{-1}$.
5. *Für alle* $m \in \mathbb{Z}$ *ist* $(ma)b = a(mb) = m(ab)$.

BEWEIS. 1. Induktion nach n. Für $n = 0$ ist wegen $\binom{0}{0} = 1$ nichts zu zeigen.
$n \geq 0\,,\ n \to n+1$: Mit Hilfe der Eigenschaft des Binomialkoeffizienten

$$\binom{n+1}{l} = \binom{n}{l} + \binom{n}{l-1} \quad \text{für alle} \quad n, l \in \mathbb{N}$$

und der Induktionsvoraussetzung folgt

$$\begin{aligned}(a+b)^{n+1} = (a+b)^n(a+b) &= \Big[\sum_{i=0}^{n}\binom{n}{i}a^{n-i}b^i\Big](a+b) = \sum_{i=0}^{n}\binom{n}{i}a^{n+1-i}b^i + \sum_{i=0}^{n}\binom{n}{i}a^{n-i}b^{i+1}\\ &= a^{n+1} + \sum_{i=1}^{n}\binom{n}{i}a^{n+1-i}b^i + \sum_{i=1}^{n}\binom{n}{i-1}a^{n-(i-1)}b^i + b^{n+1}\\ &= a^{n+1} + \sum_{i=1}^{n}\Big[\binom{n}{i} + \binom{n}{i-1}\Big]a^{n+1-i}b^i + b^{n+1} = \sum_{i=0}^{n+1}\binom{n+1}{i}a^{n+1-i}b^i.\end{aligned}$$

2. Aus $a \cdot 0_R + a \cdot 0_R = a \cdot (0_R + 0_R) = a \cdot 0_R$ folgt $a \cdot 0_R = 0_R$. Ebenso zeigt man $0_R \cdot a = 0_R$.

3. Aus $ab + a(-b) = a[b + (-b)] = a \cdot 0_R = 0_R$ folgt $a(-b) = -ab$. Ebenso zeigt man $(-a)b = -ab$. Schließlich ist $(-a)(-b) = -[(-a)b] = -(-ab) = ab$.

4. Es ist $(-a)(-a^{-1}) = aa^{-1} = 1$ und $(-a^{-1})(-a) = a^{-1}a = 1$,. Daraus folgt $(-a) \in R^\times$ und $(-a)^{-1} = -a^{-1}$.

5. Wir zeigen $(ma)b = m(ab)$. Die zweite Gleichung erhält man dann genauso.

FALL 1: $m \in \mathbb{N}_0$. Wir führen den Beweis mittels Induktion nach m. Für $m = 0$ ist die Aussage klar.

$m \geq 0\,,\ m \to m+1$: Es ist $[(m+1)a]b = (ma + a)b = (ma)b + ab = m(ab) + ab = (m+1)(ab)$.

FALL 2: $m = -k$ mit $k \in \mathbb{N}$. Nach Definition der negativen Vielfachen und FALL 1 erhalten wir $(ma)b = [k(-a)]b = k[(-a)b] = k(-ab) = m(ab)$. □

Definition 3.1.3. Sei $R = (R, +, \cdot)$ ein Ring. Eine Teilmenge $R_0 \subset R$ heißt *Teilring* von R, wenn R_0 eine Untergruppe von $(R, +)$ und eine Unterhalbgruppe von $(R, \cdot)$ ist (dann ist R_0, versehen mit der induzierten Addition und Multiplikation, ein Ring). Ist R_0 ein Teilring von R, so sagt man auch, R ist ein *Oberring* von R_0 und nennt $R_0 \subset R$ eine *Ringerweiterung*.

Lemma 3.1.4 (Teilringkriterium)**.** *Sei R ein Ring und $R_0 \subset R$. Dann sind äquivalent*:

(a) R_0 *ist ein Teilring von* R.
(b) $1_R \in R_0$, *und für alle* $a, b \in R_0$ *ist* $a - b \in R_0$ *und* $ab \in R_0$.

BEWEIS. Nach Satz 2.2.2 ist R_0 genau dann eine Untergruppe von $(R, +)$, wenn $R_0 \neq \emptyset$ und $a - b \in R_0$ für alle $a, b \in R_0$. Nach Definition ist R_0 genau dann eine Unterhalbgruppe von $(R, \cdot)$, wenn $1_R \in R_0$ und $ab \in R_0$ für alle $a, b \in R_0$. □

Definition 3.1.5. Sei R ein Ring.

1. R heißt *Nullring*, wenn $|R| = 1$ (dann ist $R = \{0_R\} = \{1_R\}$ und $+_R = \cdot_R$).
2. $a \in R$ heißt *Nullteiler*, wenn es ein $x \in R \setminus \{0\}$ gibt, so dass $ax = 0$ oder $xa = 0$. Es bezeichne $n(R)$ die Menge der Nullteiler von R. Der Ring R heißt *nullteilerfrei*, wenn $n(R) = \{0_R\}$.

3. R heißt *Divisionsring*, wenn $R^\times = R \setminus \{0\}$.
4. Ein *Körper* ist ein kommutativer Divisionsring.
5. Ein *Integritätsbereich* oder *Bereich* ist ein nullteilerfreier kommutativer Ring.

Lemma 3.1.6. *Sei R ein Ring.*

1. *Es sind äquivalent*: (a) $|R| = 1$; (b) $0_R = 1_R$; (c) $0_R \notin n(R)$.
2. $R^\bullet = R \setminus n(R)$.
3. $R^\times \cap n(R) = \emptyset$.
4. *Ist R ein Bereich, so ist $1_R \neq 0_R$, $R^\bullet = R \setminus \{0\}$ ist ein Monoid, und jeder Teilring von R ist ein Bereich.*
5. *Jeder Körper ist ein Bereich, und jeder endliche nullteilerfreie Ring ist ein Divisionsring.*

Beweis. 1. (a) $\Rightarrow$ (b) und (a) $\Rightarrow$ (c) Klar.
(b) $\Rightarrow$ (a) Ist $a \in R$, so folgt $a = a \cdot 1_R = a \cdot 0_R = 0_R$.
(c) $\Rightarrow$ (a) Sei $|R| > 1$ und $a \in R \setminus \{0\}$. Dann ist $a \cdot 0 = 0$ und daher $0 \in n(R)$.

2. Sei $a \notin n(R)$, und seien b, $c \in R$ mit $ab = ac$. Dann ist $a(b-c) = 0$, also $b - c = 0$ und $b = c$. Ist $ba = ca$, so folgt in gleicher Weise $b = c$. Daher ist $a \in R^\bullet$.

Sei nun $a \in R^\bullet$. Ist $x \in R$ mit $ax = 0$, so ist $ax = a \cdot 0$ und daher $x = 0$. Ist $xa = 0$, so folgt in gleicher Weise $x = 0$. Daher ist $a \notin n(R)$.

3. Sei $a \in R^\times$ und $x \in R \setminus \{0\}$ mit $ax = 0$. Dann folgt $x = 1_R\, x = a^{-1}ax = a^{-1} \cdot 0 = 0$, ein Widerspruch.

4. Sei R ein Bereich. Dann ist $n(R) = \{0_R\}$, also $1_R \neq 0_R$ nach 1., und auf Grund der Definition ist $R^\bullet = R \setminus \{0\}$. Ist $R_0 \subset R$ ein Teilring, so ist $\{0_R, 1_R\} \subset R_0$, also $|R_0| \geq 2$ und daher (nach 1.) $\{0_R\} \subset n(R_0) \subset n(R) = \{0_R\}$, also $n(R_0) = \{0_R\}$.

5. Nach Lemma 2.1.5.3 und Satz 2.1.10. □

Bemerkungen und Beispiele 3.1.7.

1. $\mathbb{Z}$ ist ein Integritätsbereich, $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$ und $\mathbb{F}_2$ (siehe 2.1.6.8) sind Körper. $\mathbb{Z} \subset \mathbb{Q} \subset \mathbb{R} \subset \mathbb{C}$ sind Teilringe.

2. Ist R ein Ring und $n \in \mathbb{N}$, so ist $\mathsf{M}_n(R)$ ein Ring.

3. Sei G eine additive abelsche Gruppe. Sind $f, g \in \mathrm{End}(G)$, so ist $\mathrm{End}(G)$ bezüglich der wertweisen Addition eine additive abelsche Gruppe mit dem Nullhomomorphismus als Nullelement (siehe 2.1.6.7), $(\mathrm{End}(G), \circ)$ ist eine Halbgruppe mit neutralem Element id_G (nach Lemma 2.4.2.5), und $(\mathrm{End}(G), +, \circ)$ ist ein Ring (es sind noch die Distributivgesetze nachzurechnen).

4. Sei $\mathbb{H}$ die Menge aller Matrizen

$$\begin{pmatrix} a & b \\ -\overline{b} & \overline{a} \end{pmatrix} \in \mathsf{M}_2(\mathbb{C}) \quad \text{mit} \quad a, b \in \mathbb{C}\,.$$

$\mathbb{H} \subset \mathsf{M}_2(\mathbb{C})$ ist ein Teilring (nachrechnen mit Lemma 3.1.4), und $\mathbb{H}$ ist ein Divisionsring (nachrechnen!). Setzt man

$$\mathbf{1} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \quad \boldsymbol{i} = \begin{pmatrix} \mathsf{i} & 0 \\ 0 & -\mathsf{i} \end{pmatrix}, \quad \boldsymbol{j} = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}, \quad \boldsymbol{k} = \begin{pmatrix} 0 & -\mathsf{i} \\ -\mathsf{i} & 0 \end{pmatrix},$$

so ist $\mathbb{H}$ ein 4-dimensionaler $\mathbb{R}$-Vektorraum mit Basis $(\mathbf{1}, \boldsymbol{i}, \boldsymbol{j}, \boldsymbol{k})$, und $\mathsf{Q} = \{\pm\mathbf{1}, \pm\boldsymbol{i}, \pm\boldsymbol{j}, \pm\boldsymbol{k}\}$ ist eine (nicht-abelsche) Gruppe mit 8 Elementen. Man nennt $\mathbb{H}$ den *Quaternionenschiefkörper* und Q die *Quaternionengruppe*.

5. Sei R ein Oberring von $\mathbb{Z}$. Für $a \in R$, $m \in \mathbb{Z}$ hat dann ma zwei Bedeutungen, nämlich als Vielfaches und als Produkt. Diese beiden Bedeutungen stimmen aber überein (Beweis: zuerst für $m \in \mathbb{N}_0$ durch Induktion, dann für $m = -k$ mit $k \in \mathbb{N}$).

6. Sei R ein Nullring. Dann besitzt R keinen echten Oberring. [Beweis: Ist $S \supset R$ ein Oberring, so folgt $1_S = 1_R = 0_R = 0_S$ und daher ist $|S| = 1$, also $S = R$.]

7. Sei R ein Ring, Σ eine Menge von Teilringen von R,

$$T = \bigcap_{S \in \Sigma} S \quad \text{und} \quad V = \bigcup_{S \in \Sigma} S\,.$$

Dann ist T ein Teilring von R. Ist Σ gerichtet, so ist auch V ein Teilring von R. [Beweis: wie in Korollar 2.2.4].

Definition und Satz 3.1.8. *Sei $R \subset S$ eine Ringerweiterung kommutativer Ringe.*

1. *Sei $M \subset S$ und Ω die Menge aller Teilringe $T \subset S$ mit $R \cup M \subset T$. Dann ist*

$$R[M] = \bigcap_{T \in \Omega} T$$

der kleinste Teilring von S, der $R \cup M$ umfasst.

Man sagt, $R[M]$ entsteht durch *Ringadjunktion* von M an R. Ist $M = \{x_1, \ldots, x_n\}$, so schreibt man $R[x_1, \ldots, x_n]$ an Stelle von $R[M]$.

2. *Sei $M \subset S$ und $[M] = \{m_1 \cdot \ldots \cdot m_k \mid k \in \mathbb{N}_0\,,\ m_1, \ldots, m_k \in M\}$ die Menge aller Produkte von Elementen aus M. Dann ist $[M]$ die kleinste M umfassende multiplikative Unterhalbgruppe von S, und*

$$R[M] = \{c_1 x_1 + \ldots + c_n x_n \mid n \in \mathbb{N}_0,\ \ c_1, \ldots, c_n \in R\,,\ x_1, \ldots, x_n \in [M]\}\,.$$

3. *Sei $n \in \mathbb{N}$, und seien $x_1, \ldots, x_n \in S$. Sei $\boldsymbol{x} = (x_1, \ldots, x_n)$, und für $\boldsymbol{\nu} = (\nu_1, \ldots, \nu_n) \in \mathbb{N}_0^n$ sei $\boldsymbol{x}^{\boldsymbol{\nu}} = x_1^{\nu_1} \cdot \ldots \cdot x_n^{\nu_n}$. Dann ist*

$$R[x_1, \ldots, x_n] = \Big\{ \sum_{\boldsymbol{\nu} \in \mathbb{N}_0^n} c_{\boldsymbol{\nu}} \boldsymbol{x}^{\boldsymbol{\nu}} \;\Big|\; c_{\boldsymbol{\nu}} \in R\,,\ c_{\boldsymbol{\nu}} = 0 \ \textit{für fast alle}\ \ \boldsymbol{\nu} \in \mathbb{N}_0^n \Big\}\,.$$

An Stelle von

$$\sum_{\boldsymbol{\nu} \in \mathbb{N}_0^n} c_{\boldsymbol{\nu}} \boldsymbol{x}^{\boldsymbol{\nu}} \quad \text{schreibt man auch} \quad \sum_{\nu_1, \ldots, \nu_n \geq 0} c_{\nu_1, \ldots, \nu_n} x_1^{\nu_1} \cdot \ldots \cdot x_n^{\nu_n}\,.$$

4. *Sei $x \in S$. Dann ist*

$$R[x] = \Big\{ \sum_{j=0}^{m} c_j x^j \;\Big|\; m \in \mathbb{N}_0\,,\ c_0, \ldots, c_m \in R \Big\}\,.$$

Genügt x einer Gleichung der Form $x^d + a_{d-1}x^{d-1} + \ldots + a_1 x + a_0 = 0$ mit $d \in \mathbb{N}$ und $a_0, \ldots, a_{d-1} \in R$, so folgt

$$R[x] = \Big\{ \sum_{\nu=0}^{d-1} c_\nu x^\nu \;\Big|\; c_0, \ldots, c_d \in R \Big\}\,.$$

5. *Seien M_1, $M_2 \subset S$. Dann ist $R[M_1 \cup M_2] = R[M_1][M_2]$.*

Beweis. 1. Nach Bemerkung 3.1.7.7.

2. Offensichtlich ist $[M]$ die kleinste M umfassende multiplikative Unterhalbgruppe von M, und wegen $1 \in [M]$ ist

$$T = \{c_1 x_1 + \ldots + c_n x_n \mid n \in \mathbb{N}_0,\ \ c_1, \ldots, c_n \in R\,,\ m_1, \ldots, m_n \in [M]\}\,.$$

ein $R \cup M$ umfassender Teilring von S. Ist $R' \subset S$ ein Teilring mit $R \cup M \subset R'$, so ist auch $[M] \subset R'$ und daher $T \subset R'$. Daher ist T der kleinste $R \cup M$ umfassende Teilring von S, und es folgt $T = R[M]$.

3. und die erste Aussage in 4. sind offensichtlich. Sei nun $x \in S$, so dass $x^d + a_{d-1}x^{d-1} + \ldots + a_1x + a_0 = 0$ mit $d \in \mathbb{N}$ und $a_0, \ldots, a_{d-1} \in R$, und sei

$$T = \Big\{ \sum_{\nu=0}^{d-1} c_\nu x^\nu \;\Big|\; c_0, \ldots, c_d \in R \Big\} .$$

Dann ist $T \subset R[x]$ eine additive Untergruppe und $RT \subset T$. Wir zeigen mittels Induktion: Für alle $j \in \mathbb{N}_0$ ist $x^j \in T$ (dann folgt $R[x] \subset T$ und daher $R[x] = T$).
Für $j \leq d-1$ ist nichts zu zeigen. Sei $j \geq d$ und $\{x^\nu \mid \nu \in [0, j-1]\} \subset T$ (nach Induktionsvoraussetzung). Dann folgt

$$x^j = x^{j-d}x^d = x^{j-d}\Big(-\sum_{\nu=1}^{d} a_{d-\nu}x^{d-\nu}\Big) = \sum_{\nu=1}^{d}(-a_{d-\nu})x^{j-\nu} \;\in T .$$

5. Es ist $R \cup M_1 \subset R[M_1 \cup M_2]$. Daher ist $R[M_1] \subset R[M_1 \cup M_2]$, also auch $R[M_1] \cup M_2 \subset R[M_1 \cup M_2]$ und daher $R[M_1][M_2] \subset R[M_1 \cup M_2]$. Umgekehrt ist $R \cup M_1 \cup M_2 \subset R[M_1][M_2]$ und daher auch $R[M_1 \cup M_2] \subset R[M_1][M_2]$. □

Beispiel 3.1.9. Sei $R \subset S$ eine Ringerweiterung kommutativer Ringe, $x \in S$ und $x^2 \in R$. Dann ist $R[x] = \{a + bx \mid a, b \in R\}$.

3.2. Ringhomomorphismen, Ideale und Restklassenringe

Definition 3.2.1. Seien $R = (R, +, \cdot)$ und $R' = (R', +', \cdot')$ Ringe. Eine Abbildung $f\colon R \to R'$ heißt *Ringhomomorphismus*, wenn f ein Homomorphismus der additiven Gruppen und der multiplikativen Halbgruppen von R und R' ist, das heißt,

$$f(1_R) = 1_{R'}, \quad \text{und für alle } a, b \in R \text{ ist } \quad f(a+b) = f(a) +' f(b) \quad \text{und} \quad f(a \cdot b) = f(a) \cdot' f(b) .$$

Ein Ringhomomorphismus heißt *Ringepimorphismus* (*Ringmonomorphismus, Ringisomorphismus*), wenn er surjektiv (injektiv, bijektiv) ist. Ein Ringhomomorphismus $f\colon R \to R$ heißt *Ringendomorphismus*, und ein Ringisomorphismus $f\colon R \to R$ heißt *Ringautomorphismus*. Zwei Ringe R und $\overline{R}$ heißen *isomorph*, $R \cong \overline{R}$, wenn es einen Ringisomorphismus $f\colon R \xrightarrow{\sim} \overline{R}$ gibt.

Bemerkungen 3.2.2.

1. Ist $f\colon R \to \overline{R}$ ein Ringhomomorphismus, so ist $f(R^\times) \subset \overline{R}^\times$, und $f \,|\, R^\times\colon R^\times \to \overline{R}^\times$ ist ein Gruppenhomomorphismus.

2. Sei $R_0 \subset R$ ein Teilring. Dann ist die Einlagerung $R_0 \hookrightarrow R$ ein Ringmonomorphismus. Insbesondere ist $\mathrm{id}_R\colon R \xrightarrow{\sim} R$ ein Ringisomorphismus.

3. Sind $f\colon R \to \overline{R}$ und $\overline{f}\colon \overline{R} \to \overline{\overline{R}}$ Ringhomomorphismen, so ist auch $\overline{f} \circ f\colon R \to \overline{\overline{R}}$ ein Ringhomomorphismus.

4. Sind $f\colon R \to \overline{R}$ und $\overline{f}\colon \overline{R} \to \overline{\overline{R}}$ Ringisomorphismen, so sind auch $\overline{f} \circ f\colon R \to \overline{\overline{R}}$ und $f^{-1}\colon \overline{R} \xrightarrow{\sim} R$ Ringisomorphismen. Insbesondere ist Isomorphie eine Äquivalenzrelation auf der Klasse der Ringe und die in 2.4.6 für Halbgruppen und Gruppen gemachten Bemerkungen gelten sinngemäß auch für Ringe.

5. Sei $f\colon R \to \overline{R}$ ein Ringhomomorphismus. Dann ist $f(R) \subset \overline{R}$ ein Teilring, und $f\colon R \to f(R)$ ist ein Ringepimorphismus. Ist $\overline{R_0} \subset \overline{R}$ ein Teilring, so ist auch $f^{-1}(\overline{R_0}) \subset R$ ein Teilring.Ist $f\colon R \to \overline{R}$ ein Ringmonomorphismus, so ist $f\colon R \xrightarrow{\sim} f(R)$ ein Ringisomorphismus.

6. Seien R und $\overline{R}$ Ringe. Der Nullhomomorphismus $\mathsf{c}_0 \colon R \to \overline{R}$ der Additionsgruppen ist genau dann ein Ringhomomorphismus, wenn $\overline{R} = \{0_{\overline{R}}\}$ [Beweis: Ist $\overline{R} = \{0_{\overline{R}}\}$, so ist c_0 ein Ringhomomorphismus. Ist umgekehrt c_0 ein Ringhomomorphismus, so ist $1_{\overline{R}} = \mathsf{c}_0(1_R) = 0_{\overline{R}}$ und daher $\overline{R} = \{0_{\overline{R}}\}$].

7. Sei $R \subset S$ eine Ringerweiterung kommutativer Ringe und $M \subset S$. Sind $f, g \colon S \to T$ Ringhomomorphismen mit $f \mid R \cup M = g \mid R \cup M$, so folgt $f \mid R[M] = g \mid R[M]$, und $f(R[M]) = f(R)[f(M)]$.

Beispiele 3.2.3.

1. Sei $(R_i)_{i \in I}$ eine Familie von Ringen mit Nullelementen $0_i \in R_i$ und Einselementen $1_i \in R_i$, und sei

$$R = \prod_{i \in I} R_i$$

das direkte Produkt. Dann ist R mit der komponentenweisen Addition und Multiplikation ein Ring mit Nullelement $(0_i)_{i \in I}$, Einselement $(1_i)_{i \in I}$ und Einheitengruppe

$$R^\times = \prod_{i \in I} R_i^\times \, .$$

Die Projektionen $p_j \colon R \to R_j$ sind Ringepimorphismen, und die Einlagerungen $\varepsilon_j \colon R_j \to R$ sind Ringmonomorphismen.

2. Sei R ein Ring, X eine nichtleere Menge und $\mathrm{Abb}(X, R)$ die Menge aller Abbildungen $f \colon X \to R$. Für $z \in R$ sei $\mathsf{c}_z \in \mathrm{Abb}(X, R)$ die konstante Abbildung mit Wert z. Nach 2.1.6.7 ist $\mathrm{Abb}(X, R)$ bezüglich der wertweisen Addition eine abelsche Gruppe mit neutralem Element c_0 und bezüglich der wertweisen Multiplikation eien Halbgruppe mit neutralem Element c_1. Ferner gelten die Distributivgesetze (nachrechnen!), und daher ist $\mathrm{Abb}(X, R)$ ein Ring. Die Abbildung

$$\mathsf{c} \colon \begin{cases} R & \to \ \mathrm{Abb}(X, R) \\ a & \mapsto \quad \mathsf{c}_a \end{cases}$$

ist ein Ringmonomorphismus; genau dann ist c ein Isomorphismus, wenn $|X| = 1$. Für jedes $z \in X$ ist die *Auswertungsabbildung*

$$\eta_z \colon \begin{cases} \mathrm{Abb}(X, R) & \to \quad R \\ f & \mapsto \ f(z) \end{cases}$$

ein Ringepimorphismus, und es ist $\eta_z \circ \mathsf{c} = \mathrm{id}_R$ (nachrechnen!).

Definition 3.2.4. Sei $R = (R, +, \cdot)$ ein Ring.

1. Eine Teilmenge $I \subset R$ heißt *Ideal* von R, $I \lhd R$, wenn gilt:
   (a) I ist eine Untergruppe von $(R, +)$.
   (b) $RI = \{xa \mid x \in R,\ a \in I\} \subset I$ und $IR = \{ax \mid x \in R,\ a \in I\} \subset I$.
2. Sei $I \lhd R$. Zwei Elemente $a, b \in R$ heißen *kongruent modulo* I, wenn $a - b \in I$. Man schreibt dann $a \equiv_I b$ oder $a \equiv b \bmod I$ und bezeichnet mit R/I die additive Faktorgruppe von R modulo I (diese Definition ist mit 2.5.5 konsistent).
3. Eine Äquivalenzrelation $\sim$ auf R heißt *Kongruenzrelation*, wenn $\sim$ eine Kongruenzrelation bezüglich $+$ und bezüglich $\cdot$ ist [d. h., für alle $a, b, c \in R$ gilt: Aus $a \sim b$ folgt $a + c \sim b + c$ und $ac \sim bc$].

Bemerkungen 3.2.5.

1. Jede additive Untergruppe von $\mathbb{Z}$ ist ein Ideal von $\mathbb{Z}$. Nach Satz 2.2.5 ist daher $\{m\mathbb{Z} \mid m \in \mathbb{N}_0\}$ die Menge aller Ideale von $\mathbb{Z}$.

Sind $m \in \mathbb{N}$ und $a, b \in \mathbb{Z}$, so ist genau dann $a \equiv b \bmod m\mathbb{Z}$, wenn $a \equiv b \bmod m$.

2. Ist R ein Ring, so sind das *Nullideal* $\{0_R\}$ und das *Einsideal* R Ideale von R. Für alle $a, b \in R$ ist $a \equiv b \bmod R$, und genau dann ist $a \equiv b \bmod \{0_R\}$, wenn $a = b$.

3. Sei R ein Ring und $I \lhd R$. Dann sind äquivalent: (a) $I = R$; (b) $1 \in I$; (c) $I \cap R^\times \neq \emptyset$.

[Beweis: (a) $\Rightarrow$ (b) $\Rightarrow$ (c) Klar. (c) $\Rightarrow$ (a) Sei $u \in I \cap R^\times$ und $a \in R$. Dann ist $a = uu^{-1}a \in IR = I$.]

4. Sei R ein Ring, Σ eine Menge von Idealen von R,

$$J = \bigcap_{I \in \Sigma} I \quad \text{und} \quad K = \bigcup_{I \in \Sigma} I\,.$$

Dann ist J ein Ideal von R. Ist Σ gerichtet, so ist auch K ein Ideal von R. [Beweis: Wie für Gruppen, siehe Korollar 2.2.4 und Satz 2.3.2.8].

5. Sei R ein kommutativer Ring, und sei $a \in R$. Dann ist $aR \lhd R$, und nach 3. ist genau dann $aR = R$, wenn $a \in R^\times$. Sind $a, b \in R$, so ist nach Definition genau dann $aR = bR$, wenn $a \simeq b$. Ist R ein Bereich, so gilt: $aR = bR \iff b = a\varepsilon$ mit $\varepsilon \in R^\times \iff aR^\times = bR^\times$.

Definition und Satz 3.2.6. *Sei R ein Ring.*

1. *Ist $I \lhd R$, so ist $\equiv_I$ eine Kongruenzrelation auf R.*
2. *Ist $\sim$ eine Kongruenzrelation auf R, so ist $I = [0]_\sim \lhd R$, und $\sim\, = \equiv_I$.*
3. *Sei $I \lhd R$. Dann ist $R/I = R/\equiv_I$ mit den von $+$ und $\cdot$ induzierten Verknüpfungen ein Ring, und der Restklassenhomomorphismus $\pi\colon R \to R/I$ ist ein Ringepimorphismus.*

   Man nennt R/I den *Restklassenring* oder *Faktorring* von R modulo I, man nennt die von $+$ und $\cdot$ auf R/I induzierten Verknüpfungen die *Restklassenaddition* und die *Restklassenmultiplikation* und bezeichnet sie wieder mit $+$ und $\cdot$. Für alle $a, b, c \in R$ ist dann

   $$(a + I) + (b + I) = (a + b) + I \quad \text{und} \quad aI \cdot bI = abI\,,$$

   und es gilt:

   $$(a + I) + (b + I) = c + I \iff a + b \equiv c \mod I \quad \text{und} \quad aI \cdot bI = cI \iff ab \equiv c \mod I\,.$$

   Offensichtlich ist $R/R = \{R\}$ ein Nullring, und $\pi\colon R \to R/\{0_R\}$ ein Ringisomorphismus (wir identifizieren: $R = R/\{0_R\}$).

Beweis. 1. Sei $I \lhd R$. Nach Satz 2.5.5 ist $\equiv_I$ eine Kongruenzrelation bezüglich $+$, und wir müssen zeigen, dass $\equiv_I$ auch eine Kongruenz bezüglich $\cdot$ ist. Seien $a, b, c \in R$ und $a \equiv_I b$. Dann ist $a - b \in I$, und daher folgt $ac - bc = (a - b)c \in I$ und $ca - cb = c(a - b) \in I$, also $ac \equiv_I bc$ und $ca \equiv_I cb$.

2. Sei $\sim$ eine Kongruenzrelation auf R und $I = [0]_\sim$. Nach Satz 2.5.5 ist $I \subset R$ eine additive Untergruppe und $\sim\, = \equiv_I$. Sei nun $a \in I$ und $x \in R$. Zu zeigen bleibt, dass $ax \in I$ und $xa \in I$. Es ist $a \sim 0$ und daher auch $ax \sim 0 \cdot x = 0$ und $xa \sim x \cdot 0 = 0$, also $ax \in I$ und $xa \in I$.

3. Nach 2.5.1 genügt es, die Distributivgesetze nachzurechnen. Für $a, b, c \in R$ ist

$$\begin{aligned}(a + I) \cdot [(b + I) + (c + I)] &= (a + I) \cdot [(b + c) + I] = a(b + c) + I = (ab + ac) + I \\ &= (ab + I) + (ac + I) = (a + I) \cdot (b + I) + (a + I) \cdot (c + I)\,.\end{aligned}$$

□

Beispiel 3.2.7 (C.F. Gauß 1801, Hauptsatz über Kongruenzen)**.** Sei $m \in \mathbb{N}$.

1. Die Kongruenz modulo m (im Sinne von 2.3.5) ist eine Kongruenzrelation auf $\mathbb{Z}$, d. h., für alle a, a', b, $b' \in \mathbb{Z}$ gilt: Aus $a \equiv a' \bmod m$ und $b \equiv b' \bmod m$ folgt $a+b \equiv a'+b' \bmod m$ und $ab \equiv a'b' \bmod m$.
2. $\mathbb{Z}/m\mathbb{Z} = \{r + m\mathbb{Z} \mid r \in \mathbb{Z}\} = \{r + m\mathbb{Z} \mid r \in [0, m-1]\}$ ist bezüglich der Restklassenaddition und der Restklassenmultiplikation ein kommutativer Ring mit m Elementen, dem Nullelement $m\mathbb{Z} = 0 + m\mathbb{Z}$ und dem Einselement $1 + m\mathbb{Z}$.

Satz 3.2.8 (Struktur des Restklassenringes modulo m)**.** *Sei $m \in \mathbb{N}$.*

1. $n(\mathbb{Z}/m\mathbb{Z}) = \{a + m\mathbb{Z} \mid a \in [1, m]\,,\ \mathrm{ggT}(a, m) > 1\}$.
2. $(\mathbb{Z}/m\mathbb{Z})^\times = \{a + m\mathbb{Z} \mid a \in [1, m]\,,\ \mathrm{ggT}(a, m) = 1\}$.
3. *Es sind äquivalent*: (a) $\mathbb{Z}/m\mathbb{Z}$ *ist ein Körper;* (b) $\mathbb{Z}/m\mathbb{Z}$ *ist ein Bereich;* (c) $m \in \mathbb{P}$.

Beweis. 1. und 2. Wegen $n(\mathbb{Z}/m\mathbb{Z}) \cap (\mathbb{Z}/m\mathbb{Z})^\times = \emptyset$, genügt es, für beide Fälle die Inklusion $\supset$ zu zeigen. Sei also $a \in [1, m]$ und $d = \mathrm{ggT}(a, m)$.
Ist $d > 1$, so folgt $m = dm'$ und $a = da'$ mit $m' \in [1, m-1]$ und $a' \in [1, m-1]$, es ist $m' + m\mathbb{Z} \neq 0 + m\mathbb{Z}$ und $(a + m\mathbb{Z})(m' + m\mathbb{Z}) = am' + m\mathbb{Z} = ma' + m\mathbb{Z} = 0 + m\mathbb{Z}$, also $a + m\mathbb{Z} \in n(\mathbb{Z}/m\mathbb{Z})$.
Ist $d = 1$, so gibt es $x, y \in \mathbb{Z}$ mit $ax + my = 1$ und daher $(a + m\mathbb{Z})(x + m\mathbb{Z}) = 1 + m\mathbb{Z}$, also $a + m\mathbb{Z} \in (\mathbb{Z}/m\mathbb{Z})^\times$.

3. Nach 1. und 2. gilt: $n(\mathbb{Z}/m\mathbb{Z}) = \{0\} \iff m \in \mathbb{P} \iff (\mathbb{Z}/m\mathbb{Z})^\times = \mathbb{Z}/m\mathbb{Z} \setminus \{0 + m\mathbb{Z}\}$. Definitionsgemäß folgt daraus die Behauptung. □

Satz 3.2.9. *Sei $f\colon R \to \overline{R}$ ein Ringhomomorphismus.*

1. *Sei $I \lhd R$ und $\overline{I} \lhd \overline{R}$. Dann ist $f(I) \lhd f(R)$ und $f^{-1}(\overline{I}) \lhd R$. Insbesondere ist* $\mathrm{Ker}(f) \lhd R$.
2. (Universelle Eigenschaft des Restklassenhomomorphismus) *Ist $I \lhd R$ und $I \subset \mathrm{Ker}(f)$, so existiert genau ein Ringhomomorphismus $\widehat{f}\colon R/I \to \overline{R}$ mit $\widehat{f}(a + I) = f(a)$ für alle $a \in R$. Es ist $\widehat{f}(R/I) = f(R)$ und $\mathrm{Ker}(\widehat{f}) = \mathrm{Ker}(f)/I \lhd R/I$.*
3. (Homomorphiesatz für Ringe) *Es gibt genau einen Ringmonomorphismus $\overline{f}\colon R/\mathrm{Ker}(f) \to \overline{R}$, so dass $\overline{f}(a + \mathrm{Ker}(f)) = f(a)$ für alle $a \in R$. Ist f surjektiv, so ist $\overline{f}$ ein Ringisomorphismus.*
4. *Sei f surjektiv, Σ die Menge aller Ideale $I \lhd R$ mit $\mathrm{Ker}(f) \subset I$ und $\overline{\Sigma}$ die Menge aller Ideale von $\overline{R}$. Dann sind*

$$\widetilde{f}\colon \begin{cases} \Sigma & \to & \overline{\Sigma} \\ I & \mapsto & f(I) \end{cases} \quad \text{und} \quad \widetilde{f}^*\colon \begin{cases} \overline{\Sigma} & \to & \Sigma \\ \overline{I} & \mapsto & f^{-1}(\overline{I}) \end{cases}$$

zueinander inverse inklusionserhaltende Bijektionen, und die Abbildung

$$\widehat{f}\colon R/I \to \overline{R}/f(I)\,, \quad \text{definiert durch} \quad \widehat{f}(a + I) = f(a) + f(I) \quad \text{für alle} \quad a \in R\,,$$

ist ein Ringisomorphismus.

Beweis. 1. Nach Satz 2.4.4 sind $f(I) \subset f(R)$ und $f^{-1}(\overline{I}) \subset R$ additive Untergruppen. Ist $\overline{a} \in f(I)$ und $\overline{x} \in f(R)$, so gibt es Elemente $a \in I$ und $x \in R$, so dass $f(a) = \overline{a}$ und $f(x) = \overline{x}$. Dann ist $xa \in I$ und $ax \in I$, also folgt $\overline{x}\,\overline{a} = f(x)f(a) = f(xa) \in f(I)$ und $\overline{a}\,\overline{x} = f(a)f(x) = f(ax) \in f(I)$.
Ist $a \in f^{-1}(\overline{I})$ und $x \in R$, so folgt $f(xa) = f(x)f(a) \in \overline{I}$ und $f(ax) = f(a)f(x) \in \overline{I}$, also auch $xa \in f^{-1}(\overline{I})$ und $ax \in f^{-1}(\overline{I})$. Daher ist $f^{-1}(\overline{I}) \lhd R$.

2. Nach Korollar 2.5.12 existiert genau ein (additiver) Gruppenhomomorphismus $\widehat{f}\colon R/I \to \overline{R}$ mit den angegebenen Eigenschaften. Wegen $\widehat{f}(1 + I) = f(1) = 1$ und

$$\widehat{f}\big((a + I)(b + I)\big) = \widehat{f}(ab + I) = f(ab) = f(a)f(b) = \widehat{f}(a + I)\widehat{f}(b + I)$$

für alle $a, b \in R$ ist $\widehat{f}$ ein Ringhomomorphismus.

3. Nach 2. mit $I = \mathrm{Ker}(f)$.

4. Nach 1. und Satz 2.5.10 genügt es, zu zeigen, dass $\widehat{f}$ ein Ringhomomorphismus ist. Das zeigt dieselbe Rechnung wie im Beweis von 2. □

Korollar 3.2.10. *Sei R ein Ring und $I \lhd R$. Dann ist $\{J/I \mid J \lhd R,\ I \subset J\}$ die Menge aller Ideale von R/I, und für jedes Ideal $J \lhd R$ mit $I \subset J$ ist die Abbildung*

$$\widehat{f}\colon R/J \to (R/I)/(J/I), \quad \text{definiert durch} \quad f(a+J) = (a+I) + J/I \quad \text{für alle} \quad a \in R,$$

ein Ringisomorphismus.

Beweis. Nach Satz 3.2.9.4, angewandt auf den Restklassenepimorphismus $f\colon R \to R/I$. □

3.3. Quotientenbildung

Jede Unterhalbgruppe einer kommutativen Gruppe ist ein Monoid, und jeder Teilring eines Körpers ist ein Bereich. Wir werden nun umgekehrt zeigen, dass man jedes Monoid in eine Gruppe und jeden Bereich in einen Körper (in kanonischer Weise) einbetten kann. Dazu sind eine Reihe elementarer mengentheoretischer Vorbereitungen nötig, welche auch bei anderen Konstruktionen der Algebra Verwendung finden.

Lemma 3.3.1 (Strukturübertragungsprinzip)**.** *Sei $(\overline{H}, \overline{*})$ eine Halbgruppe, H eine nichtleere Menge und $f\colon H \to \overline{H}$ eine bijektive Abbildung. Dann gibt es genau eine Verknüpfung $*$ auf H, sodass f ein $(*, \overline{*})$-Isomorphismus ist.*

Beweis. Offensichtlich hat die Verknüpfung $*$ auf H, definiert durch

$$x * y = f^{-1}\big(f(x) \overline{*} f(y)\big) \quad \text{für alle} \quad x, y \in H,$$

die gewünschte Eigenschaft. □

Lemma 3.3.2 (Existenz elementfremder Exemplare)**.** *Sind B, C nichtleere Mengen, so existiert eine Menge B^* mit $B^* \cap C = \emptyset$ und eine Bijektion $f\colon B^* \to B$.*

Beweis. Für jedes Element $b \in B$ wähle man ein Objekt e_b, so dass $(b, e_b) \notin C$ (die Existenz einer solchen Familie von Objekten kann im Rahmen einer axiomatischen Mengenlehre bewiesen werden und erscheint im Rahmen der von uns praktizierten naiven Mengenlehre plausibel). Setzt man dann $B^* = \{(b, e_b) \mid b \in B\}$ und definiert $f\colon B^* \to B$ durch $f(b, e_b) = b$ für alle $b \in B$, so folgt die Behauptung. □

Lemma 3.3.3 (Austauschprinzip)**.** *Sei $\overline{H}$ eine Halbgruppe (eine Gruppe, ein Monoid, ein Ring, ...), sei H eine nichtleere Menge, Ω eine Menge mit $\Omega \cap H = \emptyset$ und $f\colon H \to \overline{H}$ eine injektive Abbildung.*

Dann existieren eine Halbgruppe (eine Gruppe, ein Monoid, ein Ring, ...) $\widetilde{H}$ und ein Isomorphismus $\widetilde{f}\colon \widetilde{H} \to \overline{H}$, so dass $H \subset \widetilde{H}$, $\widetilde{H} \cap \Omega = \emptyset$ und $\widetilde{f} \mid H = f$. Ist H eine Halbgruppe (eine Gruppe, ein Monoid, ein Ring, ...) und f ein Monomorphismus, so ist $H \subset \widetilde{H}$ eine Unterhalbgruppe (eine Untergruppe, ein Teilmonoid, ein Teilring, ...).

Beweis. Wir führen den Beweis für Halbgruppen. Die für Gruppen, Ringe usw. nötigen Modifikationen und Zusätze sind offensichtlich.

Sei $\overline{H} = (\overline{H}, \overline{*})$; nach Lemma 3.3.2 gibt es eine Menge A mit $A \cap (H \cup \Omega) = \emptyset$ und eine bijektive Abbildung $f_0\colon A \to \overline{H} \setminus f(H)$. Wir setzen $\widetilde{H} = H \cup A$ (dann ist $\Omega \cap \widetilde{H} = \emptyset$) und definieren $\widetilde{f}\colon \widetilde{H} \to \overline{H}$ durch $\widetilde{f} \mid H = f$ und $\widetilde{f} \mid A = f_0$. Dann ist $\widetilde{f}$ bijektiv, und nach Lemma 3.3.1 gibt es eine Verknüpfung $\widetilde{*}$ auf $\widetilde{H}$, so daß $\widetilde{f}$ ein Isomorphismus ist. Mit $(\overline{H}, \overline{*})$ ist dann auch $(\widetilde{H}, \widetilde{*})$ eine Halbgruppe.

Sei nun $(H,*)$ eine Halbgruppe und f ein Monomorphismus. Dann haben wir $\widetilde{*}\,|\,H\times H = *$ zu zeigen. Für $a,b\in H$ gilt $\widetilde{f}(a\,\widetilde{*}\,b) = \widetilde{f}(a)\,\overline{*}\,\widetilde{f}(b) = f(a)\,\overline{*}\,f(b) = f(a*b) = \widetilde{f}(a*b)$ auf Grund der Definition von $\widetilde{*}$ und daher $a\,\widetilde{*}\,b = a*b$, da $\widetilde{f}$ bijektiv ist. □

Bemerkung 3.3.4. Sei $f\colon H\to\overline{H}$ ein Monomorphismus von Halbgruppen (Gruppen, Monoiden, Ringen, ...), $\widetilde{H}\supset H$ eine Oberhalbgruppe (Obergruppe, Obermonoid, Oberring, ...) und $\widetilde{f}\colon\widetilde{H}\to\overline{H}$ ein Isomorphimus mit $\widetilde{f}\,|\,H = f$ gemäß Lemma 3.3.3. Identifiziert man nun $\widetilde{H}$ mit $\overline{H}$ vermöge f (gemäß 2.4.6.4), so wird H mit $f(H)$ identifiziert und zum Teilmonoid von $\overline{H}$ (dabei setzt man, meist stillschweigend, voraus, dass $H\cap\big(\overline{H}\setminus f(H)\big)=\emptyset$). Man sagt dann auch, man *bettet H vermöge f in $\overline{H}$ ein.*

Definition und Satz 3.3.5. *Sei $H=(H,*)$ eine kommutative Halbgruppe.*

1. *Es gibt eine kommutative Oberhalbgruppe $H_1=(H_1,*_1)$ von $(H,*)$, so dass $H^\bullet\subset H_1^\times$ und $H_1=\{t^{-1}*_1 a\mid t\in H^\bullet,\ a\in H\}$.*

   Man nennt H_1 eine (*totale*) *Quotientenhalbgruppe* von H.

   Ist Ω eine Menge mit $H\cap\Omega=\emptyset$, so kann man auch H_1 so konstruieren, dass $H_1\cap\Omega=\emptyset$.
2. *Sei H_1 eine Quotientenhalbgruppe von H und $\varphi\colon H\to K$ ein Halbgruppenhomomorphismus, so dass $\varphi(H^\bullet)\subset K^\times$. Dann gibt es genau einen Halbgruppenhomomorphismus $\varphi_1\colon H_1\to K$ mit $\varphi_1\,|\,H=\varphi$.*
3. *Seien H_1 und H_2 Quotientenhalbgruppen von H. Dann gibt es genau einen Halbgruppenisomorphismus $\phi\colon H_1\to H_2$ mit $\phi\,|\,H=\mathrm{id}_H$.*

   Redeweise: Die (totale) Quotientenhalbgruppe von H ist bis auf eindeutige Isomorphie eindeutig bestimmt. Man spricht daher von *der* Quotientenhalbgruppe von H, bezeichnet diese mit $\mathsf{q}(H)$ und schreibt (falls Verwechslungen nicht zu befürchten sind) die Verknüpfungen auf H und auf $\mathsf{q}(H)$ wieder als Multiplikation.
4. *Es ist $\mathsf{q}(H)^\times=\mathsf{q}(H)^\bullet=\{t^{-1}a\mid t,\,a\in H^\bullet\}$. Ist H ein Monoid, so ist $\mathsf{q}(H)$ eine Gruppe.*

   Ist H ein Monoid, so nennt man $\mathsf{q}(H)$ die *Quotientengruppe* von H.

Beweis. Wir werden für die Konstruktion im Beweis von 1. alle Verknüpfungen verschieden bezeichnen, in den übrigen Teilen des Beweises aber wieder einfach multiplikative Notation für alle auftretenden Halbgruppen benutzen.

1. Sei $1\in H$ das neutrale Element von H und Ω eine Menge mit $H\cap\Omega=\emptyset$. Wir definieren eine Relation $\sim$ auf $H\times H^\bullet$ durch

$$(a,t)\sim(a',t')\,,\quad\text{falls}\quad a*t'=a'*t\,.$$

Dann ist $\sim$ eine Äquivalenzrelation [Symmetrie und Reflexivität sind offensichtlich, und die Transitivität rechnet man wie folgt nach: Seien (a,t), (a',t'), $(a'',t'')\in H\times H^\bullet$, $(a,t)\sim(a',t')$ und $(a',t')\sim(a'',t'')$. Dann ist $a*t'=a'*t$, $a'*t''=a''*t'$, und unter Benutzung der Kommutativität von $*$ folgt

$$a*t''*t'=a*t'*t''=a'*t*t''=a'*t''*t=a''*t'*t=a''*t*t'\,.$$

Wegen $t'\in H^\bullet$ ist dann $a*t''=a''*t$, also $(a,t)\sim(a'',t'')$, was zu zeigen war.]

Sei $H'=H\times H^\bullet/\!\sim$ die Menge aller Äquivalenzklassen von $H\times H^\bullet$ unter $\sim$. Für $(a,t)\in H\times H^\bullet$ sei $(a/t)\in H'$ die Äquivalenzklasse von (a,t). Nach Definition ist dann $(a*s/t*s)=(a/t)$ für alle $a\in H$ und $s,\,t\in H^\bullet$. Wir definieren eine Verknüpfung $*'$ auf H'

$$(a/t)*'(b/s)=(a*b/t*s)\quad\text{für alle}\quad a,\,b\in H\quad\text{und}\quad s,\,t\in H^\bullet\,.$$

Diese Definition ist unabhängig von der Wahl der Repräsentanten [denn aus $(a/t)=(a_1/t_1)$ und $(b/s)=(b_1/s_1)$ folgt $a*t_1=a_1*t$ und $b*s_1=b_1*s$, also unter Benutzung der Kommutativität

von $*$ auch $a*b*s_1*t_1 = a_1*b_1*s*t$ und daher $(a*b/s*t) = (a_1*b_1/s_1*t_1)\,]$. Es ist nun leicht (wenn auch lang und langweilig) nachzurechnen, dass $*'$ kommutativ und assoziativ ist, und dass $(1/1)$ ein neutrales Element bezüglich $*'$ ist. Daher ist $(H', *')$ eine kommutative Halbgruppe.

Wir definieren $f\colon H \to H'$ durch $f(a) = (a/1)$. Für alle $a, b \in H$ ist dann

$$f(a*b) = (a*b/1) = (a/1) *' (b/1) = f(a) *' f(b)\,, \quad \text{und aus } \; f(a) = f(b) \; \text{ folgt } \; a = b\,.$$

Daher ist f ein Halbgruppenmonomorphismus. Nach Lemma 3.3.3 gibt es eine Halbgruppe $(H_1, *_1)$ und einen Isomorphismus $f_1\colon H_1 \to H'$, so dass $H_1 \cap \Omega = \emptyset$, $H \subset H_1$ ist eine Unterhalbgruppe, und $f_1 \,|\, H = f$.

Als Nächstes zeigen wir $H^\bullet \subset H_1^\times$. Für $t \in H^\bullet$ sei $t_1 = f_1^{-1}(1/t) \in H_1$. Dann folgt

$$f_1(t *_1 t_1) = (t/1) *' (1/t) = (t/t) = (1/1) = f(1) = f_1(1)\,, \quad \text{also} \quad t *_1 t_1 = 1 \quad \text{und daher} \quad t \in H_1^\times\,.$$

Für $t \in H^\bullet \subset H_1^\times$ und $a \in H$ ist $t^{-1} *_1 a \in H_1$, und es bleibt zu zeigen, dass jedes Element von H_1 von dieser Form ist. Sei also $x \in H_1$ und $f_1(x) = (a/t)$ mit $a \in H$ und $t \in H^\bullet$. Dann folgt

$$f_1(x) = (a/1) *' (1/t) = f(a) *' f(t)^{-1} = f_1(a) *' f_1(t)^{-1} = f_1(a *_1 t^{-1}) \quad \text{und daher} \quad x = a *_1 t^{-1}\,.$$

2. Es ist $H_1 = \{t^{-1}a \mid t \in H^\bullet\,,\ a \in H\}$.

EXISTENZ: Wir definieren $\varphi_1\colon H_1 \to K$ durch $\varphi_1(t^{-1}a) = \varphi(t)^{-1}\varphi(a)$ für alle $t \in H^\bullet$ und $a \in H$, und dafür müssen wir zeigen: Sind $t, t_1 \in H^\bullet$ und $a, a_1 \in H$ mit $t^{-1}a = t_1^{-1}a_1$, so folgt $\varphi(t)^{-1}\varphi(a) = \varphi(t_1)^{-1}\varphi(a_1)$. Aber aus $t^{-1}a = t_1^{-1}a_1$ folgt $t_1 a = t a_1$, also $\varphi(t_1)\varphi(a) = \varphi(t)\varphi(a_1)$ und daher $\varphi(t)^{-1}\varphi(a) = \varphi(t_1)^{-1}\varphi(a_1)$.

Ist $a \in H$, so ist $a = 1^{-1}a$ und daher $\varphi_1(a) = \varphi(1)^{-1}\varphi(a) = \varphi(a)$. Daher ist $\varphi_1 \,|\, H = \varphi$.

Sind $t, s \in H^\bullet$ und $a, b \in H$, so folgt

$$\varphi_1\big((t^{-1}a)(s^{-1}b)\big) = \varphi_1\big((ts)^{-1}(ab)\big) = \varphi(ts)^{-1}\varphi(ab) = \varphi(t)^{-1}\varphi(a)\varphi(s)^{-1}\varphi(b) = \varphi_1(t^{-1}a)\varphi_1(s^{-1}b)\,,$$

und daher ist φ_1 ein Halbgruppenhomomorphismus.

EINDEUTIGKEIT: Seien $\varphi_1, \varphi_1'\colon H_1 \to K$ Halbgruppenhomomorphismen mit $\varphi_1 \,|H = \varphi_1' \,|H = \varphi$. Für $t \in H^\bullet$ und $a \in H$ ist dann $\varphi_1(t^{-1}a) = \varphi_1(t)^{-1}\varphi_1(a) = \varphi(t)^{-1}\varphi(a) = \varphi_1'(t)^{-1}\varphi_1'(a) = \varphi_1'(t^{-1}a)$ und daher $\varphi_1 = \varphi_1'$.

3. Nach 2. gibt es genau einen Halbgruppenhomomorphismus $\phi\colon H_1 \to H_2$ mit $\phi \,|\, H = \mathrm{id}_H$, und wir müssen zeigen, dass ϕ ein Isomorphismus ist. Es gibt aber auch einen Halbgruppenhomomorphismus $\psi\colon H_2 \to H_1$ mit $\psi \,|\, H = \mathrm{id}_H$. Dann sind $\psi\circ\phi\colon H_1 \to H_1$ und id_{H_1} Halbgruppenhomomorphismen mit $\psi\circ\phi \,|\, H = \mathrm{id}_{H_1} \,|\, H = \mathrm{id}_H$. Nach der Eindeutigkeitsaussage in 2. folgt $\psi\circ\phi = \mathrm{id}_{H_1}$, und in gleicher Weise folgert man $\phi\circ\psi = \mathrm{id}_{H_2}$. Daher ist ϕ ein Isomorphismus.

4. Offensichtlich ist $\{t^{-1}a \mid t, a \in H^\bullet\} \subset \mathfrak{q}(H)^\times \subset \mathfrak{q}(H)^\bullet$. Sei nun $t \in H^\bullet$, $a \in H$ und $t^{-1}a \in \mathfrak{q}(H)^\bullet$. Wir zeigen $a \in H^\bullet$. Seien $b, c \in H$ mit $ab = ac$. Dann folgt $t^{-1}ab = t^{-1}ac$ und daher $b = c$. Ist H ein Monoid, so ist $H^\bullet = H$ und daher $\mathfrak{q}(H)^\times = \mathfrak{q}(H)$, also $\mathfrak{q}(H)$ eine Gruppe. □

Definition und Satz 3.3.6. *Sei R ein kommutativer Ring.*

1. *Es gibt einen kommutativen Oberring $R_1 \supset R$, so dass $R^\bullet \subset R_1^\times$ und $R_1 = \{t^{-1}a \mid t \in R^\bullet\,,\ a \in R\}$.*

   Man nennt R_1 einen (*totalen*) *Quotientenring* von R.

   Ist Ω eine Menge mit $R \cap \Omega = \emptyset$, so kann man auch R_1 so konstruieren, dass $R_1 \cap \Omega = \emptyset$.

2. *Sei R_1 ein totaler Quotientenring von R und $\varphi\colon R \to K$ ein Ringhomomorphismus, so dass $\varphi(R^\bullet) \subset K^\times$. Dann gibt es genau einen Ringhomomorphismus $\varphi_1\colon R_1 \to K$ mit $\varphi_1 \,|\, R = \varphi$.*

3. *Seien R_1 und R_2 totale Quotientenringe von R. Dann gibt es genau einen Ringisomorphismus $\phi\colon R_1 \to R_2$ mit $\phi \mid R = \mathrm{id}_R$.*

   Redeweise: Der totale Quotientenring von R ist bis auf eindeutige Isomorphie eindeutig bestimmt. Man spricht daher von *dem* totalen Quotientenring von R und bezeichnet diesen mit $\mathfrak{q}(R)$.

4. *Es ist $\mathfrak{q}(R)^\times = \mathfrak{q}(R)^\bullet = \{t^{-1}a \mid t, a \in R^\bullet\}$. Ist R ein Bereich, so ist $\mathfrak{q}(R)$ ein Körper.*

   Ist R ein Bereich, so nennt man $\mathfrak{q}(R) = \{t^{-1}a \mid t, a \in R,\ t \neq 0\}$ den *Quotientenkörper* von R.

5. *Sei R ein Bereich, K ein Körper und $\varphi\colon R \to K$ ein Ringmonomorphismus. Dann gibt es genau einen Körpermonomorphismus $\varphi_1\colon \mathfrak{q}(R) \to K$ mit $\varphi_1 \mid R = \varphi$.*

BEWEIS. 1. Sei R_1 die multiplikative Quotientenhalbgruppe von R. Dann ist (nach 3.3.5) $R^\bullet \subset R_1^\times$ und $R_1 = \{t^{-1}a \mid t \in R^\bullet,\ a \in R\}$. Wir definieren eine Addition $+'$ auf R_1 durch

$$t^{-1}a +' s^{-1}b = (ts)^{-1}(sa + tb) \quad \text{für alle } t, s \in R^\bullet \text{ und } a, b \in R.$$

Diese Definition ist unabhängig von den gewählten Darstellungen von $t^{-1}a$ und $s^{-1}b$ [denn: Aus $t^{-1}a = t_1^{-1}a_1$ und $s^{-1}b = s_1^{-1}b_1$ folgt $t_1a = ta_1$ und $s_1b = sb_1$, also

$$t_1s_1(sa + tb) = t_1s_1sa + t_1s_1tb = tss_1a_1 + t_1stb_1 = ts(s_1a_1 + t_1b_1)$$

und daher $(ts)^{-1}(sa + tb) = (t_1s_1)^{-1}(s_1a_1 + t_1b_1)$].

Für alle $a \in R$ und $s, t \in R^\bullet$ ist $(st)^{-1}(sa) = t^{-1}a$, und daher gilt: Sind $x, y, z \in R_1$, so gibt es $a, b, c \in R$ und $t \in R^\bullet$ mit $x = t^{-1}a$, $y = t^{-1}b$ und $z = t^{-1}c$. Mit diesen Darstellungen ist es nun leicht, nachzurechnen, dass $+'$ assoziativ und kommutativ ist und gemeinsam mit der Multiplikation auf R_1 das Distributivgesetz erfüllt. Für $a, b \in R$ ist $a +' b = a + b$, und wir schreiben daher im Folgenden wieder $+$ an Stelle von $+'$. Daher ist R_1 ein kommutativer Oberring von R.

2. R_1 ist eine multiplikative Quotientenhalbgruppe von R, und daher gibt es nach 3.3.5 genau einen Homomorphismus multiplikativer Halbgruppen $\varphi_1\colon R_1 \to K$ mit $\varphi_1 \mid R = \varphi$. Seien nun $x, y \in R_1$ und $a, b \in R$, $t \in R^\bullet$ mit $x = t^{-1}a$ und $y = t^{-1}b$. Dann ist $x + y = t^{-1}(a + b)$ und

$$\begin{aligned}\varphi_1(x + y) &= \varphi_1(t)^{-1}\varphi_1(a + b) = \varphi(t)^{-1}\varphi(a + b) = \varphi(t)^{-1}[\varphi(a) + \varphi(b)] \\ &= \varphi_1(t)^{-1}[\varphi_1(a) + \varphi_1(b)] = \varphi_1(t^{-1}a) + \varphi_1(t^{-1}b) = \varphi_1(x) + \varphi_1(y),\end{aligned}$$

also φ_1 ein Ringhomomorphismus.

3. Der Beweis von 3.3.5.3 überträgt sich (fast) wörtlich.

4. Nach 3.3.5.4 ist $\mathfrak{q}(R)^\times = \mathfrak{q}(R)^\bullet = \{t^{-1}a \mid t, a \in R^\bullet\}$. Ist R ein Bereich, so ist $R^\bullet = R \setminus \{0\}$ und daher $\mathfrak{q}(R)^\times = \mathfrak{q}(R) \setminus \{0\}$, also $\mathfrak{q}(R)$ ein Körper.

5. Nach 2., denn genau dann ist $\varphi(R^\bullet) \subset K^\times$, wenn $\mathrm{Ker}(\varphi) = \{0\}$, also φ ein Monomorphismus ist. □

Bemerkungen 3.3.7. 1. Sei G ein abelsche Gruppe und $H \subset G$ eine Unterhalbgruppe. Dann ist H ein Monoid und $\{a^{-1}b \mid a, b \in H\} \subset G$ ist eine Quotientengruppe von H. In diesem Falle können wir also $\mathfrak{q}(H) \subset G$ annehmen und auf die abstrakte Konstruktion der Quotientengruppe in 3.3.5 verzichten.

2. Sei K ein Körper und $R \subset K$ ein Teilring. Dann ist R ein Bereich und $\{a^{-1}b \mid a \in R^\bullet,\ b \in R\} \subset K$ ist ein Quotientenkörper von R. In diesem Falle können wir also $\mathfrak{q}(R) \subset K$ annehmen und auf die abstrakte Konstruktion des Quotientenkörpers in 3.3.6 verzichten.

3. $\mathbb{Q}$ ist ein Quotientenkörper von $\mathbb{Z}$, $(\mathbb{Q}_{>0}, \cdot)$ ist eine Quotientengruppe von $(\mathbb{N}, \cdot)$, $(\mathbb{Z}, +)$ ist eine Quotientengruppe von $(\mathbb{N}_0, +)$.

4. Ist H eine kommutative Halbgruppe mit $H^\bullet = H^\times$, so ist $H = \mathfrak{q}(H)$. Insbesondere ist $\mathfrak{q}(G) = G$ für jede Gruppe G und $\mathfrak{q}(R) = R$ für jeden Körper R. Nach Satz 3.2.8 ist $\mathfrak{q}(\mathbb{Z}/m\mathbb{Z}) = \mathbb{Z}/m\mathbb{Z}$ für alle $m \in \mathbb{N}$.

5. Sei H eine kommutative Halbgruppe oder ein kommutativer Ring, $n \in \mathbb{N}$ und $x_1, \ldots, x_n \in \mathsf{q}(H)$. Dann gibt es ein $a \in H^\bullet$, so dass $ax_i \in H$ für alle $i \in [1,n]$. Man nennt jedes solche $a \in H^\bullet$ einen *gemeinsamen Nenner* von $x_1, \ldots, x_n$.

Satz 3.3.8. *Sei $H = (H, +)$ ein additives Monoid und $G = \mathsf{q}(H)$. Dann sind äquivalent*:

(a) *G ist torsionsfrei.*

(b) *Es gibt eine Teilmenge $P \subset G \setminus \{0\}$, so dass $P+P \subset P$, $P \cap (-P) = \emptyset$ und $P \cup (-P) = G \setminus \{0\}$.*

(c) *Es gibt eine Totalordnung $\leq$ auf H, so dass für alle $a, b, c \in H$ gilt: Aus $a \leq b$ folgt $a+c \leq b+c$.*

Beweis. (a) $\Rightarrow$ (b) Sei $\Omega = \{P \subset G \setminus \{0\} \mid P+P \subset P \text{ und } P \cap (-P) = \emptyset\}$. Dann ist $\emptyset \in \Omega$ und die Vereinigungsmenge jeder Kette in Ω liegt in Ω. Nach dem Zorn'schen Lemma besitzt Ω ein bezüglich $\subset$ maximales Element P, und wir nehmen an, es sei $P \cup (-P) \subsetneq G \setminus \{0\}$. Sei $x \in G \setminus \{0\} \setminus [P \cup (-P)]$ und $P_1 = \{p + nx \mid p \in P,\ n \in \mathbb{N}_0\}$. Wegen $P_1 + P_1 \subset P_1$ und der Maximalität von P gibt es dann $p, p' \in P$ und $n, n' \in \mathbb{N}_0$, so dass $p + nx = -(p' + n'x)$ und daher $(n+n')x = -(p+p') \in (-P)$. Sei nun $P_2 = \{q - mx \mid p \in P,\ m \in \mathbb{N}_0\}$. Wegen $P_2 + P_2 \subset P_2$ und der Maximalität von P gibt es dann $q, q' \in P$ und $m, m' \in \mathbb{N}_0$, so dass $q - mx = -(q' - m'x)$ und daher $(m+m')x = q + q' \in P$. Es folgt $(n+n')(m+m')x \in P \cap (-P)$, ein Widerspruch.

(b) $\Rightarrow$ (c) Für $x, y \in H$ definieren wir $x \leq y$, falls $y - x \in P \cup \{0\}$. Dann ist die Reflexiviät dieser Relation trivial, die Antisymmetrie folgt wegen $P \cap (-P) = \emptyset$ und die Transitivität wegen $P + P \subset P$. Wegen $G = P \cup (-P) \cup \{0\}$ ist $\leq$ eine Totalordnung auf H. Sind $a, b, c \in H$ mit $a \leq b$, so folgt $b - a = (b+c) - (a+c) \in P$ und daher auch $a + c \leq b + c$.

(c) $\Rightarrow$ (a) Sei $x = s - t \in G \setminus \{0\}$ mit $s, t \in H$. Wegen $\operatorname{ord}(x) = \operatorname{ord}(-x)$ können wir $s < t$ annehmen. Dann ist aber auch $ns < nt$ (und daher $nx \neq 0$) für alle $n \in \mathbb{N}$. □

3.4. Arithmetik der Ideale; noethersche Bereiche und Hauptidealbereiche

Definition und Satz 3.4.1. *Sei R ein Ring.*

1. *Sei $X \subset R$. Dann ist*

$$ {}_R\langle X\rangle_R \;=\; \bigcap_{\substack{I \lhd R \\ X \subset I}} I \;=\; \Big\{ \sum_{i=1}^{n} a_i x_i b_i \;\Big|\; n \in \mathbb{N},\ x_1, \ldots, x_n \in X,\ a_1, \ldots, a_n, b_1, \ldots, b_n \in R \Big\} $$

das kleinste X enthaltende Ideal von R.

${}_R\langle X\rangle_R$ heißt das *von X erzeugte (zweiseitige) Ideal* von R. Ist R kommutativ, so schreibt man ${}_R\langle X\rangle$ an Stelle von ${}_R\langle X\rangle_R$. Es ist dann

$$ {}_R\langle X\rangle \;=\; \Big\{ \sum_{i=1}^{n} a_i x_i \;\Big|\; n \in \mathbb{N},\ x_1, \ldots, x_n \in X,\ a_1, \ldots, a_n \in R \Big\}. $$

Ist insbesondere $X = \{x_1, \ldots, x_n\}$ (mit $n \in \mathbb{N}_0$), so schreibt man ${}_R\langle x_1, \ldots, x_n\rangle$ an Stelle von ${}_R\langle X\rangle$.

2. *Sei R kommutativ, $n \in \mathbb{N}$ und $x_1, \ldots, x_n \in R$. Dann ist*

$$ {}_R\langle x_1, \ldots, x_n\rangle \;=\; \{a_1x_1 + \ldots + a_nx_n \mid a_1, \ldots, a_n \in R\} = Rx_1 + \ldots + Rx_n = \sum_{i=1}^{n} Rx_i. $$

Ein Ideal $I \lhd R$ heißt

- *endlich erzeugt*, wenn $I = {}_R\langle X\rangle$ mit einer endlichen Menge X;

- *Hauptideal*, wenn $I = {}_R\langle a\rangle = Ra = aR$ mit $a \in R$ (siehe Bemerkung 3.2.5.5). Es ist $\{0_R\} = {}_R\langle 0_R\rangle$ und $R = {}_R\langle 1_R\rangle = {}_R\langle \varepsilon\rangle$ für alle $\varepsilon \in R^\times$.

Der Ring R heißt

- *noethersch*, wenn jedes Ideal von R endlich erzeugt ist;
- *Hauptidealring*, wenn jedes Ideal von R ein Hauptideal ist;
- *Hauptidealbereich*, wenn R ein Bereich und ein Hauptidealring ist.

3. *$\mathbb{Z}$ ist ein Hauptidealbereich.*
4. *Die folgenden Aussagen sind äquivalent*:
   (a) *R ist noethersch;*
   (b) *Jede aufsteigende Folge von Idealen wird stationär* [*explizit*: *Ist $(I_n)_{n\geq 0}$ eine Folge von Idealen und $I_n \subset I_{n+1}$ für alle $n \geq 0$, so gibt es ein $m \in \mathbb{N}_0$, so dass $I_n = I_{n+1}$ für alle $n \geq m$*];
   (c) *In jeder nichtleeren Menge von Idealen von R gibt es ein maximales Element* (*bezüglich $\subset$*).

Beweis. 1. Nach Definition und Bemerkung 3.2.5.4 sind

$$I = \bigcap_{\substack{I \lhd R \\ X \subset I}} I \quad \text{und} \quad J = \Big\{ \sum_{i=1}^{n} a_i x_i b_i \;\Big|\; n \in \mathbb{N},\ x_1, \ldots, x_n \in X,\ a_1, \ldots, a_n, b_1, \ldots, b_n \in R \Big\}$$

Ideale von R, es ist $X \subset I$ und $X \subset J$, und für jedes Ideal $K \lhd R$ mit $X \subset K$ ist $I \subset K$ und $J \subset K$. Daher ist $I = J$ das kleinste X umfassende Ideal von R. Die Vereinfachungen im kommutativen Fall sind klar.

2. Nach Definition ist

$$I = \{a_1 x_1 + \ldots + a_n x_n \mid a_1, \ldots, a_n \in R\} = Rx_1 + \ldots + Rx_n = \sum_{i=1}^{n} Rx_i$$

ein Ideal mit $\{x_1, \ldots, x_n\} \subset I$, und für jedes Ideal $K \lhd R$ mit $\{x_1, \ldots, x_n\} \subset K$ ist $I \subset K$. Daher folgt $I = {}_R\langle x_1, \ldots, x_n\rangle$ nach 1.

3. Nach Bemerkung 3.2.5.1 ist $\{m\mathbb{Z} \mid m \in \mathbb{N}_0\}$ die Menge aller Ideale von $\mathbb{Z}$.

4. (a) $\Rightarrow$ (b) Sei $(I_n)_{n\geq 0}$ eine Folge von Idealen mit $I_n \subset I_{n+1}$ für alle $n \geq 0$, und sei

$$I = \bigcup_{n\geq 0} I_n .$$

Nach Bemerkung 3.2.5.4 ist $I \lhd R$, also $I = {}_R\langle a_1, \ldots, a_k\rangle$ (mit $k \in \mathbb{N}$ und $a_1, \ldots, a_k \in I$). Für $i \in [1, k]$ sei $m_i \in \mathbb{N}_0$ mit $a_i \in I_{m_i}$, und es sei $m = \max\{m_1, \ldots, m_k\}$. Dann folgt $\{a_1, \ldots, a_k\} \subset I_m$, also $I \subset I_m$ und daher $I_n = I_m$ für alle $n \geq m$.

(b) $\Rightarrow$ (c) Durch Widerspruch. Sei Ω eine nichtleere Menge von Idealen ohne maximales Element und $I_0 \in \Omega$ beliebig. Dann gibt es zu jedem $I \in \Omega$ ein $I' \in \Omega$ mit $I \subsetneq I'$, und wir definieren die Folge $(I_n)_{n\geq 0}$ in Ω rekursiv durch $I_{n+1} = I'_n$ für alle $n \geq 0$. Diese Folge widerspricht (b).

(c) $\Rightarrow$ (a) Durch Widerspruch. Angenommen, es sei $I \lhd R$ nicht endlich erzeugt. Dann gibt es eine Folge $(a_n)_{n\geq 0}$ in I, so dass ${}_R\langle a_0, \ldots, a_n\rangle \subsetneq {}_R\langle a_0, \ldots, a_{n+1}\rangle$ für alle $n \geq 0$. Dann hat die Menge $\{{}_R\langle a_0, \ldots, a_n\rangle \mid n \in \mathbb{N}_0\}$ kein maximales Element, im Widerspruch zu (c). □

Satz 3.4.2. *Sei R ein kommutativer Ring.*

1. *Genau dann ist R ein Körper, wenn $\{0_R\}$ und R die einzigen Ideale von R sind. Insbesondere ist jeder Körper ein Hauptidealbereich.*
2. *Sei R ein Körper und $f\colon R \to \overline{R}$ ein Ringhomomorphismus. Dann ist entweder $\overline{R} = \{0_{\overline{R}}\}$ oder f ein Monomorphismus.*

BEWEIS. 1. Sei R ein Körper und $\{0\} \subsetneq I \lhd R$. Dann ist $I \cap R^\times \neq \emptyset$ und daher $I = R$ nach Bemerkung 3.2.5.3.

Ist R kein Körper und $a \in R \setminus (R^\times \cup \{0\})$, so ist $aR \lhd R$, $aR \neq \{0_R\}$ und $aR \cap R^\times = \emptyset$ (denn aus $ax \in R^\times$ folgt $a \in R^\times$), also $aR \neq R$.

2. Nach 1., da $\operatorname{Ker}(f) \lhd R$. □

Bemerkung 3.4.3. Satz 3.4.2 ist falsch, falls R nicht kommutativ ist. Ist R ein Körper und $n \in \mathbb{N}$, so hat der Matrixring $\mathsf{M}_n(R)$ nur die Ideale $\{0\}$ und $\mathsf{M}_n(R)$ [Beweis: Sei $I \lhd \mathsf{M}_n(R)$, $0 \neq A = (a_{i,j})_{i,j\in[1,n]} \in I$ und seien $k, l \in [1,n]$ mit $a_{k,l} \neq 0$. Für $i, j \in [1,n]$ sei $E_{i,j}$ die Matrix mit einer Eins an der Stelle (i,j) und Null an allen übrigen Stellen. Dann ist $E_{i,j} = a_{k,l}^{-1} E_{i,k} A E_{l,j} \in I$. Also folgt $E_{i,j} \in I$ für alle $i, j \in [1,n]$ und daher $I = \mathsf{M}_n(R)$.]

Definition 3.4.4. Sei R ein Bereich. Eine Abbildung $\nu\colon R^\bullet \to \mathbb{N}_0$ heißt *euklidische Normfunktion*, wenn für alle $a, b \in R^\bullet$ gilt:

Es gibt $q, r \in R$, so dass $a = bq + r$, und entweder $r \in R^\bullet$, $\nu(r) < \nu(b)$ oder $r = 0$.

R heißt *euklidischer Bereich*, wenn es eine euklidische Normfunktion $\nu\colon R^\bullet \to \mathbb{N}_0$ gibt.

Nach Satz 1.1.6 ist die Betragsfunktion $|\cdot|\colon \mathbb{Z}^\bullet \to \mathbb{N}_0$ eine euklidische Normfunktion, also $\mathbb{Z}$ ein euklidischer Bereich.

Satz 3.4.5. *Sei R ein Bereich, $\nu\colon R^\bullet \to \mathbb{N}_0$ eine euklidische Normfunktion, $I \lhd R$ und $b \in I\setminus\{0\}$, so dass $\nu(b) = \min\big(\{\nu(x) \mid x \in I,\ x \neq 0\}\big)$. Dann ist $I = bR$.*

Insbesondere ist jeder euklidische Bereich ein Hauptidealbereich.

BEWEIS. Nach Definition ist $bR \subset I$. Ist $a \in I$, so gibt es $q, r \in R$ mit $a = bq + r$ und entweder $r \in R^\bullet$, $\nu(r) < \nu(b)$, oder $r = 0$. Wegen $r = a - bq \in I$ folgt aber $r = 0$ wegen der minimalen Wahl von b und daher $a \in bR$. □

Satz 3.4.6. *Sei $d \in \mathbb{Z}$ kein Quadrat, $\sqrt{d} \in \mathbb{C}$, $K = \mathbb{Q}[\sqrt{d}] \subset \mathbb{C}$ und $R = \mathbb{Z}[\sqrt{d}] \subset K$.*

1. *$(1, \sqrt{d})$ ist linear unabhängig über $\mathbb{Q}$, jedes $\alpha \in K$ hat eine eindeutige Darstellung in der Form $\alpha = a + b\sqrt{d}$ mit $a, b \in \mathbb{Q}$, und genau dann ist $\alpha \in R$, wenn $a, b \in \mathbb{Z}$.*

   Ist $\alpha = a+b\sqrt{d} \in K$ mit $a, b \in \mathbb{Q}$, so definieren wir $\overline{\alpha} = a-b\sqrt{d}$ und $\mathcal{N}(\alpha) = |\alpha\overline{\alpha}| = |a^2-b^2d|$.
2. *$K = \mathsf{q}(R)$, $R \cap \mathbb{Q} = \mathbb{Z}$, $(\alpha \mapsto \overline{\alpha})$ ist ein Automorphismus von K, und für alle $\alpha, \beta \in K$ gilt:*

   $$\mathcal{N}(\alpha\beta) = \mathcal{N}(\alpha)\mathcal{N}(\beta), \quad \mathcal{N}(\alpha) = 0 \iff \alpha = 0 \quad \text{und} \quad R^\times = \{\alpha \in R \mid \mathcal{N}(\alpha) = 1\}.$$

   Insbesondere ist $\mathcal{N} \mid R^\bullet\colon R^\bullet \to \mathbb{N}$ ein Homomorphismus, so dass $\mathcal{N}(\alpha) > 1$ für alle $\alpha \in R^\bullet\setminus R^\times$.
3. *Ist $d \in \{-2, -1, 2, 3\}$, so ist $\mathcal{N} \mid R^\bullet\colon R^\bullet \to \mathbb{N}$ eine euklidische Normfunktion (also R ein Hauptidealbereich).*

BEWEIS. 1. Nach Beispiel 3.1.9 ist $R = \{a + b\sqrt{d} \mid a, b \in \mathbb{Z}\}$ und $K = \{a + b\sqrt{d} \mid a, b \in \mathbb{Q}\}$. Nach Satz 1.1.10 ist $\sqrt{d} \notin \mathbb{Q}$. Daher ist $(1, \sqrt{d})$ linear unabhängig über $\mathbb{Q}$, und daraus folgt die Eindeutigkeit.

2. Wegen der linearen Unabhängigkeit von $(1, \sqrt{d})$ ist $R \cap \mathbb{Q} = \mathbb{Z}$. Seien $\alpha, \beta \in K$, $\alpha = a + a'\sqrt{d}$ und $\beta = b + b'\sqrt{d}$ mit $a, a', b, b' \in \mathbb{Q}$. Dann folgt

$$\overline{\alpha} + \overline{\beta} = (a + b) - (a' + b')\sqrt{d} = \overline{\alpha + \beta}, \quad \overline{\alpha}\overline{\beta} = (ab + a'b'd) - (ab' + a'b)\sqrt{d} = \overline{\alpha\beta} \quad \text{und} \quad \overline{\overline{\alpha}} = \alpha.$$

Daher ist $(\alpha \mapsto \overline{\alpha})$ ein Ringautomorphismus, und für $\alpha \in R$ ist $\overline{\alpha} \in R$ und $\mathcal{N}(\alpha) \in \mathbb{N}_0$. Für $\alpha, \beta \in K$ folgt $\mathcal{N}(\alpha\beta) = |\alpha\beta\overline{\alpha\beta}| = |\alpha\overline{\alpha}\beta\overline{\beta}| = \mathcal{N}(\alpha)\mathcal{N}(\beta)$, und genau dann ist $\mathcal{N}(\alpha) = 0$, wenn $\alpha = 0$. Daher ist $\mathcal{N} \mid R^\bullet\colon R^\bullet \to \mathbb{N}$ ein Halbgruppenhomomorphismus, und es ist $\mathcal{N}(R^\times) \subset \mathbb{N}^\times = \{1\}$. Ist umgekehrt $\mathcal{N}(\alpha) = 1$, so folgt $\pm\alpha\overline{\alpha} = 1$, und daher ist $\alpha \in R^\times$.

Nach Definition ist jedes $\xi \in K$ von der Form $\xi = q^{-1}\alpha$ mit $q \in \mathbb{N}$ und $\alpha \in R$, also $K \subset \mathsf{q}(R) \subset \mathbb{C}$. Ist $\xi \neq 0$, so folgt $\xi^{-1} = \pm\mathcal{N}(\xi)^{-1}\overline{\xi} \in K$. Daher ist K ein Körper und $\mathsf{q}(R) = K$.

3. Sei nun $d \in \{-2, -1, 2, 3\}$, und seien $\alpha, \beta \in R$. Dann ist $\beta^{-1}\alpha = a + b\sqrt{d}$ mit $a, b \in \mathbb{Q}$, und es gibt $x, y \in \mathbb{Z}$ mit

$$|a - x| \leq \frac{1}{2} \quad \text{und} \quad |b - y| \leq \frac{1}{2}\,.$$

Dann ist $q = x + y\sqrt{d} \in R$, und es folgt

$$\mathcal{N}(\beta^{-1}\alpha - q) = \mathcal{N}\Big(\frac{\alpha - \beta q}{\beta}\Big) = |(a-x)^2 - (b-y)^2 d| \leq \frac{3}{4} < 1\,, \quad \text{also} \quad \mathcal{N}(\alpha - \beta q) < \mathcal{N}(\beta)\,.$$

□

Bemerkung 3.4.7. Ist $d \in \mathbb{Z}$ und $d < -2$, so ist der Bereich $\mathbb{Z}[\sqrt{d}]$ kein Hauptidealbereich (siehe Beispiel 5.2.12). Nach einer Vermutung von Gauß gibt es unendlich viele $d \in \mathbb{N}$, so dass $\mathbb{Z}[\sqrt{d}]$ ein Hauptidealbereich ist, und man vermutet, dass diese Bereiche dann auch euklidisch sind.

Definition 3.4.8. Sei R ein Ring, und seien $I, J \lhd R$. Abweichend von der in 2.1.4.3 gemachten Konvention definieren wir das *Produkt* von I und J durch

$$I \cdot J = IJ = \{a_1b_1 + \ldots + a_nb_n \mid n \in \mathbb{N}\,,\ a_1, \ldots, a_n \in I\,,\ b_1, \ldots, b_n \in J\,\}\,.$$

Satz 3.4.9. *Sei R ein Ring.*

1. *Seien I und J Ideale von R. Dann sind auch $I + J$, $I \cap J$ und IJ Ideale von R, es ist $IJ \subset I \cap J$, $I + J = {}_R\langle I \cup J\rangle_R$ und $IJ = {}_R\langle\{ab \mid a \in I\,,\ b \in J\,\}\rangle_R$.*
2. *Sei $\mathcal{I}(R)$ die Menge aller Ideale von R. Dann ist $(\mathcal{I}(R), +)$ eine kommutative Halbgruppe mit neutralem Element $\{0\}$. $(\mathcal{I}(R), \cap)$ und $(\mathcal{I}(R), \cdot)$ sind Halbgruppen mit neutralem Element R. $(\mathcal{I}(R), \cap)$ ist kommutativ. Ist R kommutativ, so ist auch $(\mathcal{I}(R), \cdot)$ kommutativ.*
3. *Für alle $I, J, K \lhd R$ ist $K(I + J) = KI + KJ$ und $(I + J)K = IK + JK$.*
4. *Sei R kommutativ. Dann ist die Menge $\mathcal{H}(R)$ aller Hauptideale von R eine Unterhalbgruppe von $(\mathcal{I}(R), \cdot)$. Die Abbildung*

$$\partial\colon R \to \mathcal{H}(R)\,, \quad \textit{definiert durch} \quad \partial(a) = aR \quad \textit{für alle} \quad a \in R\,,$$

ist ein Epimorphismus multiplikativer Halbgruppen und induziert einen Isomorphismus

$$\partial^*\colon (R, \cdot)_{\mathrm{red}} \xrightarrow{\sim} \mathcal{H}(R)\,, \quad \textit{gegeben durch} \quad \partial^*([a]_\simeq) = aR \quad \textit{für alle} \quad a \in R\,.$$

Beweis. 1. Nach Bemerkung 3.2.5.4 ist $I \cap J$ ein Ideal, und nach Korollar 2.2.4 ist $I + J$ eine additive Untergruppe. Sei nun $x \in R$ und $a \in I + J$, also $a = b + c$ mit $b \in I$ und $c \in J$. Dann ist $xb \in I$, $xc \in J$ und daher $xa = xb + xc \in I + J$. Ebenso zeigt man $ax \in I + J$. Offensichtlich ist $I + J$ das kleinste $I \cup J$ enthaltende Ideal, und daher ist $I + J = {}_R\langle I \cup J\rangle$.

Es ist $0 \in IJ$, und nach Konstruktion ist für alle $x, y \in IJ$ auch $x - y \in IJ$. Nach Korollar 2.2.4 ist daher IJ eine additive Untergruppe von R. Sei nun $x \in R$ und $a \in IJ$, etwa $a = a_1b_1 + \ldots + a_nb_n$ mit $n \in \mathbb{N}$, $a_1, \ldots, a_n \in I$ und $b_1, \ldots, b_n \in J$. Für alle $i \in [1, n]$ ist dann $xa_i \in I$ und $b_ix \in J$. Daher folgt $xa = xa_1b_1 + \ldots + xa_nb_n \in IJ$ und $ax = a_1b_1x + \ldots + a_nb_nx \in IJ$. Also ist $IJ \lhd R$, und nach Konstruktion ist IJ das kleinste Ideal von R, das alle Produkte ab mit $a \in I$ und $b \in J$ enthält. Ist $a \in I$ und $b \in J$, so ist $ab \in I \cap J$, und daher folgt $IJ \subset I \cap J$.

2. und 3. Die behaupteten Rechenregeln für Ideale sind leicht elementweise nachzurechnen.

4. Für alle $a, b \in R$ ist $abR = (aR)(bR)$. Daher ist ∂ ein Epimorphismus. Nach Definition ist $\sim_\partial\, = \simeq$, und die Behauptung folgt aus Satz 2.5.6.3. □

3.5. Halbgruppenringe und Polynomringe

Bemerkung und Definition 3.5.1. Sei $R \neq \{0\}$ ein kommutativer Ring und $H = (H,+)$ eine additive kommutative Halbgruppe mit neutralem Element $0 = 0_H$. Für eine Abbildung $f\colon H \to R$ nennt man $\operatorname{supp}(f) = \{h \in H \mid f(h) \neq 0_R\}$ den *Träger* von f. Dann ist

$$R[H] = \{f\colon H \to R \mid \operatorname{supp}(f) \text{ ist endlich}\} < \operatorname{Abb}(H,R)$$

eine Untergruppe der additiven Gruppe aller Abbildungen von H nach R bzgl. der wertweisen Addition (siehe Beispiel 2.1.6.7; das Nullelement von $R[H]$ ist die konstante Abbildung c_0 mit Wert 0_R). Für $f, g \in R[H]$ und $z \in H$ ist dann die Menge

$$\{(x,y) \in H \times H \mid z = x + y\,,\ f(x)g(y) \neq 0\} \subset \operatorname{supp}(f) \times \operatorname{supp}(g)$$

endlich, und wir definieren

$$fg = f \cdot g\colon H \to R \quad \text{durch} \quad (f \cdot g)(z) = \sum_{\substack{(x,y) \in H \times H \\ x+y=z}} f(x)g(y) \quad \text{für alle } z \in H\,.$$

Für $h \in H$ definieren wir $X^h \in R[H]$ durch

$$X^h(z) = \begin{cases} 1_R\,, & \text{falls} \quad h = z\,, \\ 0_R\,, & \text{falls} \quad h \neq z\,, \end{cases}$$

und für $a \in R$ definieren wir $\theta(a) \in R[H]$ durch

$$\theta(a)(z) = \begin{cases} a\,, & \text{falls} \quad z = 0_H\,, \\ 0_R\,, & \text{falls} \quad z \neq 0_H\,. \end{cases}$$

Definition und Satz 3.5.2. *Sei $R \neq \{0\}$ ein kommutativer Ring und $H = (H,+)$ eine additive kommutative Halbgruppe.*

1. *$(R[H], +, \cdot)$ ist ein kommutativer Ring mit Einselement X^0, die Abbildung $\theta\colon R \to R[H]$ ist ein Ringmonomorphismus, und die Abbildung $X\colon H \to R[H]\,,\ h \mapsto X^h$ ist ein Halbgruppenmonomorphismus.*

   Wir betten nun R vermöge θ in $R[H]$ ein (vgl. Bemerkung 3.3.4), d.h., wir identifizieren R mit $\theta(R)$, und dadurch wird $R \subset R[H]$ zum Teilring. Der Oberring $R[H] \supset R$ heißt *Halbgruppenring* von H über R.

   Für alle $a \in R$, $f \in R[H]$ und $z \in H$ ist dann $(af)(z) = (\theta(a) \cdot f)(z) = af(z)$.

2. *Jedes $f \in R[H]$ hat eine eindeutige Darstellung der Form*

$$f = \sum_{h \in H} a_h X^h \quad \textit{mit} \quad a_h \in R \ \textit{ und } \ a_h = 0 \ \textit{ für fast alle } \ h \in H\,.$$

   Insbesondere gilt: $R[H] = R\big[\{X^h \mid h \in H\}\big]$ (gemäß 3.1.8). Ist R ein Körper, so ist $R[H]$ ein R-Vektorraum mit Basis $\{X^h \mid h \in H\}$.

3. *Sei*

$$f = \sum_{h \in H} a_h X^h \ \textit{ und } \ g = \sum_{h \in H} b_h X^h \in R[H]\,.$$

   Dann folgt

$$f + g = \sum_{h \in H} (a_h + b_h) X^h \quad \textit{und} \quad fg = \sum_{h \in H} \Big(\sum_{\substack{(x,y) \in H \times H \\ x+y=h}} a_x b_y \Big) X^h\,.$$

4. *Genau dann ist $R[H]$ ein Bereich, wenn die beiden folgenden Bedingungen erfüllt sind:*

- *R ist ein Bereich.*
- *H ist ein Monoid, und $\mathsf{q}(H)$ ist torsionsfrei.*

5. *Ist $R[H]$ ein Bereich und H reduziert, so ist $R[H]^\times = R^\times$.*

BEWEIS. 1. Definitionsgemäß ist $R[H]$ eine additive abelsche Gruppe. Offensichtlich ist $\cdot$ kommutativ, und für alle $f \in R[H]$ ist $X^0 f = f$.

Seien nun f, g, $h \in R[H]$. Dann gilt für alle $z \in H$

$$[(f\cdot g)\cdot h](z) = \sum_{\substack{(x,y)\in H\times H\\ x+y=z}} (f\cdot g)(x)h(y) = \sum_{\substack{(x,y)\in H\times H\\ x+y=z}} \Big(\sum_{\substack{(u,v)\in H\times H\\ u+v=x}} f(u)g(v)\Big)h(y) = \sum_{\substack{(u,v,y)\in H\times H\times H\\ u+v+y=z}} f(u)g(v)h(y)$$

und

$$[f\cdot(g\cdot h)](z) = \sum_{\substack{(u,x)\in H\times H\\ u+x=z}} f(u)(g\cdot h)(x) = \sum_{\substack{(u,x)\in H\times H\\ u+x=z}} f(u)\Big(\sum_{\substack{(v,y)\in H\times H\\ v+y=x}} g(v)h(y)\Big) = \sum_{\substack{(u,v,y)\in H\times H\times H\\ u+v+y=z}} f(u)g(v)h(y)\,.$$

In gleicher Weise ist das Distributivgesetz nachzurechnen.

Die Abbildung $h \mapsto X^h$ ist nach Definition injektiv, und für alle h, g, $z \in H$ ist

$$(X^g\cdot X^h)(z) = \sum_{\substack{(x,y)\in H\times H\\ x+y=z}} X^g(x)X^h(y) = \begin{cases} X^g(g)X^h(h)\,, & \text{falls} \quad z = g+h\,,\\ 0\,, & \text{falls} \quad z \neq g+h\,,\end{cases} \quad \text{also} \quad X^g\cdot X^h = X^{g+h}\,.$$

Die Abbildung θ ist ebenfalls nach Definition injektiv, es ist $\theta(1) = X^0$, und für alle a, $b \in R$ und $z \in H$ ist

$$[\theta(a)+\theta(b)](z) = \theta(a)(z)+\theta(b)(z) = \begin{cases} a+b\,, & \text{falls} \quad z = 0\,,\\ 0\,, & \text{falls} \quad z \neq 0\,,\end{cases} \quad \text{also} \quad \theta(a)+\theta(b) = \theta(a+b)$$

und

$$[\theta(a)\cdot\theta(b)](z) = \theta(a)(z)\theta(b)(z) = \begin{cases} ab\,, & \text{falls} \quad z = 0\,,\\ 0\,, & \text{falls} \quad z \neq 0\,,\end{cases} \quad \text{also} \quad \theta(a)\cdot\theta(b) = \theta(ab)\,.$$

2. Sei $f \in R[H]$. Für alle $z \in H$ ist

$$\Big(\sum_{h\in H} f(h)X^h\Big)(z) = \sum_{h\in H} f(h)X^h(z) = f(z) \quad \text{und daher} \quad \sum_{h\in H} f(h)X^h = f\,.$$

Wir müssen die Eindeutigkeit dieser Darstellung nachweisen. Sei dazu

$$f = \sum_{h\in H} a_h X^h \quad \text{mit} \quad a_h \in R \ \text{ und } \ a_h = 0 \ \text{ für fast alle } \ h \in H\,.$$

Für alle $z \in H$ ist dann

$$f(z) = \Big(\sum_{h\in H} a_h X^h\Big)(z) = \sum_{h\in H} a_h X^h(z) = a_z\,.$$

3. Nach 2. und den Rechenregeln für Ringe.

4. und 5. Sei zuerst $R[H]$ ein Bereich. Dann ist auch R (als Teilring von $R[H]$) ein Bereich, und da $h \mapsto X^h$ ein Monomorphismus ist, ist H ein Monoid. Angenommen, $\mathsf{q}(H)$ sei nicht torsionsfrei. Dann gibt es $s, t \in H$ mit $s \neq t$ und ein $\operatorname{ord}(s-t) = n \in \mathbb{N}$. Dann ist $ns = nt$ und

$$0 = X^{ns} - X^{nt} = (X^s - X^t)\Big(\sum_{i=0}^{n-1} X^{(n-i-1)s+it}\Big)\,.$$

und für alle i, $j \in [0, n-1]$ mit $i \neq j$ ist $(n-i-1)s+it \neq (n-j-1)s+jt$, also $X^s - X^t \in n(R[H]) \setminus \{0\}$.

Sei nun R ein Bereich, H ein Monoid und $\mathsf{q}(H)$ torsionsfrei. Dann gibt es nach Satz 3.3.8 eine mit der Addition verträgliche Totalordnung $\leq$ auf H. Seien $f, g \in R[H] \setminus \{0\}$, sei $x_0 = \min_{\leq}(\mathrm{supp}(f))$ und $y_0 = \min_{\leq}(\mathrm{supp}(g))$. Dann ist $(f \cdot g)(x_0 + y_0) = f(x_0)g(y_0) \neq 0$ und daher $f \cdot g \neq 0$.

Ist $f \cdot g = 1$, also $(f \cdot g)(0) = 1$ und $(f \cdot g)(z) = 0$ für alle $z \in H \setminus \{0\}$, so folgt $x_0 + y_0 = 0$, also $x_0 = y_0 = 0$ wegen $H^\times = \{0\}$, und $(f \cdot g)(0) = f(0)g(0) = 1$. Ist $x_1 = \max_{\leq}(\mathrm{supp}(f))$ und $y_1 = \max_{\leq}(\mathrm{supp}(g))$, so folgt auch $(f \cdot g)(x_1 + y_1) = f(x_1)g(y_1) \neq 0$ und daher $x_1 = 0$ und $y_1 = 0$, also $f = f(0) \in R^\times$ und $g = g(0) \in R^\times$. □

Satz 3.5.3 (Universelle Eigenschaft des Halbgruppenringes)**.** *Seien $R \neq \{0\}$ ein kommutativer Ring, H eine additive kommutative Halbgruppe, $\varphi\colon R \to \overline{R}$ ein Ringhomomorphismus und $\sigma\colon H \to (\overline{R}, \cdot)$ ein Halbgruppenhomomorphismus. Dann existiert genau ein Ringhomomorphismus $\Phi\colon R[H] \to \overline{R}$ mit $\Phi \mid R = \varphi$ und $\Phi(X^h) = \sigma(h)$ für alle $h \in H$.*

Beweis. EINDEUTIGKKEIT: Sei $\Phi\colon R[H] \to \overline{R}$ ein Ringhomomorphismus mit $\Phi \mid R = \varphi$ und $\Phi(X^h) = \sigma(h)$ für alle $h \in H$. Für $f \in R[H]$ gilt dann:

$$(*)\quad \text{Aus}\quad f = \sum_{h \in H} a_h X^h \in R[H] \quad \text{folgt}\quad \Phi(f) = \sum_{h \in H} \Phi(a_h X^h) = \sum_{h \in H} \Phi(a_h)\Phi(X^h) = \sum_{h \in H} \varphi(a_h)\sigma(h)\,.$$

Daher ist Φ durch φ und σ eindeutig bestimmt.

EXISTENZ: Man definiere eine Abbildung Φ mittels $(*)$ (man beachte die Eindeutigkeit der Darstellung von $f \in R[H]$ gemäß Satz 3.5.2.2). Dann sind die behaupteten Eigenschaften leicht nachzurechnen . □

Definitionen und Bemerkungen 3.5.4. Sei $R \neq \{0\}$ ein kommutativer Ring.

1. Sei $H = (\mathbb{N}_0, +)$. Dann ist (nach 3.1.8)

$$R[\mathbb{N}_0] = \Big\{ \sum_{n \in \mathbb{N}_0} a_n X^n \;\Big|\; a_n \in R\,,\ a_n = 0 \text{ für fast alle } n \in \mathbb{N}_0 \Big\} = R[X]\,.$$

In diesem Fall nennt man $X \in R[H]$ eine *Unbestimmte* über R und nennt den Ring $R[X]$ den *Polynomring* in der Unbestimmten X über R.

2. Sei $n \in \mathbb{N}$, $H = (\mathbb{N}_0^n, +)$, und seien $\boldsymbol{e}_1, \ldots, \boldsymbol{e}_n \in \mathbb{N}_0^n$ die Einheitsvektoren, und für $i \in [1, n]$ sei $X_i = X^{\boldsymbol{e}_i} \in R[H]$. Ist dann $\boldsymbol{\nu} = (\nu_1, \ldots, \nu_n) = \nu_1 \boldsymbol{e}_1 + \ldots + \nu_n \boldsymbol{e}_n \in \mathbb{N}_0^n$, so folgt $X^{\boldsymbol{\nu}} = X_1^{\nu_1} \cdot \ldots \cdot X_n^{\nu_n}$ und daher

$$R[\mathbb{N}_0^n] = R[X_1, \ldots, X_n]\,.$$

Man nennt $R[X_1, \ldots, X_n]$ den *Polynomring* in den Unbestimmten $(X_1, \ldots, X_n)$ über R und die $f \in R[X_1, \ldots, X_n]$ *Polynome* in den Unbestimmten $(X_1, \ldots, X_n)$.

Für $\boldsymbol{\nu} = (\nu_1, \ldots, \nu_n) \in \mathbb{N}_0^n$ sei $\boldsymbol{X}^{\boldsymbol{\nu}} = X_1^{\nu_1} \cdot \ldots \cdot X_n^{\nu_n}$. Dann hat nach Satz 3.5.2.2 jedes $f \in R[X_1, \ldots, X_n]$ eine eindeutige Darstellung

$$f = \sum_{\boldsymbol{\nu} \in \mathbb{N}_0^n} c_{\boldsymbol{\nu}} \boldsymbol{X}^{\boldsymbol{\nu}} \qquad \text{mit } c_{\boldsymbol{\nu}} \in R \text{ und } c_{\boldsymbol{\nu}} = 0 \text{ für fast alle } \boldsymbol{\nu} \in \mathbb{N}_0^n\,.$$

Satz 3.5.5. *Sei $n \in \mathbb{N}$, $\{0\} \neq R \subset S = R[T_1, \ldots, T_n]$ eine Ringerweiterung kommutativer Ringe, sei $\boldsymbol{T}^{\boldsymbol{\nu}} = T_1^{\nu_1} \cdot \ldots \cdot T_n^{\nu_n}$ für alle $\boldsymbol{\nu} = (\nu_1, \ldots, \nu_n) \in \mathbb{N}_0^n$, und sei $R[\mathbb{N}_0^n] = R[X_1, \ldots, X_n]$ wie in 3.5.4. Dann sind äquivalent:*

(a) *Es gibt (genau einen) Ringisomorphismus $\Phi\colon R[\mathbb{N}_0^n] = R[X_1, \ldots, X_n] \to R[T_1, \ldots, T_n]$ mit $\Phi \mid R = \mathrm{id}_R$ und $\Phi(X_i) = T_i$ für alle $i \in \{1, \ldots, n\}$.*

(b) *Jedes* $F \in R[T_1, \dots, T_n]$ *hat eine eindeutige Darstellung in der Form*

$$F = \sum_{\boldsymbol{\nu} \in \mathbb{N}_0^n} c_{\boldsymbol{\nu}} \boldsymbol{T}^{\boldsymbol{\nu}} \qquad \textit{mit } c_{\boldsymbol{\nu}} \in R \textit{ und } c_{\boldsymbol{\nu}} = 0 \textit{ für fast alle } \boldsymbol{\nu} \in \mathbb{N}_0^n .$$

(c) *Ist*

$$\sum_{\boldsymbol{\nu} \in \mathbb{N}_0^n} c_{\boldsymbol{\nu}} \boldsymbol{T}^{\boldsymbol{\nu}} = 0 \qquad \textit{mit } c_{\boldsymbol{\nu}} \in R \textit{ und } c_{\boldsymbol{\nu}} = 0 \textit{ für fast alle } \boldsymbol{\nu} \in \mathbb{N}_0^n ,$$

so folgt $c_{\boldsymbol{\nu}} = 0$ *für alle* $\boldsymbol{\nu} \in \mathbb{N}_0^n$.

(d) *Zu jedem Ringhomomorphismus* $\psi\colon R \to \overline{R}$ *und jedem* $(z_1, \dots, z_n) \in \overline{R}^n$ *gibt es (genau einen) Ringhomomorphismus* $\Psi\colon R[T_1, \dots, T_n] \to \overline{R}$ *mit* $\Psi \,|\, R = \psi$ *und* $\Psi(T_i) = z_i$ *für alle* $i \in [1, n]$.

Sind diese Bedingungen erfüllt, so ist insbesondere $\boldsymbol{T}^{\boldsymbol{\nu}} \neq \boldsymbol{T}^{\boldsymbol{\mu}}$ *für alle* $\boldsymbol{\nu}, \boldsymbol{\mu} \in \mathbb{N}_0^n$ *mit* $\boldsymbol{\nu} \neq \boldsymbol{\mu}$ *und* $R \cap \{\boldsymbol{T}^{\boldsymbol{\nu}} \mid \nu \in \mathbb{N}_0^n\} = \emptyset$.

Beweis. Die Eindeutigkeitsaussagen in (a) und (d) folgen aus Bemerkung 3.2.2.7.

Sei $\sigma\colon \mathbb{N}_0^n \to R[T_1, \dots, T_n]$ definiert durch $\sigma(\boldsymbol{\nu}) = \boldsymbol{T}^{\boldsymbol{\nu}}$. Dann ist σ ein Halbgruppenhomomorphismus, und nach Satz 3.5.3 gibt es genau einen Ringhomomorphismus $\Phi\colon R[X_1, \dots, X_n] \to R[T_1, \dots, T_n]$ mit $\Phi \,|\, R = \mathrm{id}_R$ und $\Phi(X^{\boldsymbol{\nu}}) = \sigma(\boldsymbol{\nu}) = T^{\boldsymbol{\nu}}$, also $\Phi(X_i) = T_i$ für alle $i \in [1, n]$, und daher ist Φ ein Epimorphismus.

(a) $\Rightarrow$ (b) Nach Bemerkung 3.5.4.2.

(b) $\Rightarrow$ (c) Mit $F = 0$.

(c) $\Rightarrow$ (a) Wegen

$$\Phi\Big(\sum_{\boldsymbol{\nu} \in \mathbb{N}_0^n} c_{\boldsymbol{\nu}} X^{\boldsymbol{\nu}}\Big) = \sum_{\boldsymbol{\nu} \in \mathbb{N}_0^n} c_{\boldsymbol{\nu}} T^{\boldsymbol{\nu}}$$

folgt $\mathrm{Ker}(\Phi) = \{0\}$, und daher ist Φ ein Isomorphismus.

(a) $\Rightarrow$ (d) Sei $\psi\colon R \to \overline{R}$ ein Ringhomomorphismus, $(z_1, \dots, z_n) \in \overline{R}^n$, und sei $\sigma'\colon \mathbb{N}_0^n \to \overline{R}$ definiert durch $\sigma'(\nu_1, \dots, \nu_n) = z_1^{\nu_1} \cdot \ldots \cdot z_n^{\nu_n}$. Dann ist σ' ein Homomorphismus multiplikativer Halbgruppen, und nach Satz 3.5.3 gibt es genau einen Ringhomomorphismus $\lambda\colon R[X_1, \dots, X_n] \to \overline{R}$ mit $\lambda \,|\, R = \psi$ und $\lambda(X^{\boldsymbol{\nu}}) = \sigma'(\boldsymbol{\nu})$ für alle $\boldsymbol{\nu} \in \mathbb{N}_0^n$, also $\lambda(X_i) = z_i$ für alle $i \in [1, n]$. Nach Voraussetzung ist Φ ein Isomorphismus, und $\Psi = \lambda \circ \Phi^{-1}$ hat die gewünschte Eigenschaft.

(d) $\Rightarrow$ (a) Nach (d) gibt es genau einen Ringhomomorphismus $\Psi\colon R[T_1, \dots, T_n] \to R[X_1, \dots, X_n]$ mit $\Psi \,|\, R = \mathrm{id}_R$ und $\Psi(T_i) = X_i$ für alle $i \in [1, n]$. Dann ist $\Psi \circ \Phi = \mathrm{id}_{R[X_1, \dots, X_n]}$ nach Bemerkung 3.2.2.7 und daher Φ ein Isomorphismus.

Seien die Bedingungen des Satzes erfüllt und $\boldsymbol{\nu} \in \mathbb{N}_0^n$ mit $c = \boldsymbol{T}^{\boldsymbol{\nu}} \in R$. Dann folgt $c\boldsymbol{T}^{\boldsymbol{0}} = 1_R \boldsymbol{T}^{\boldsymbol{\nu}}$ im Widerspruch zu (b). Sind $\boldsymbol{\nu}, \boldsymbol{\mu} \in \mathbb{N}_0^n$ mit $\boldsymbol{T}^{\boldsymbol{\nu}} = \boldsymbol{T}^{\boldsymbol{\mu}}$, so folgt mit (b) $\boldsymbol{\nu} = \boldsymbol{\mu}$. □

Definitionen und Bemerkungen 3.5.6. Sei $\{0\} \neq R \subset \overline{R}$ eine Ringerweiterung kommutativer Ringe, und seien $n \in \mathbb{N}$ und $(T_1, \dots, T_n) \in \overline{R}^n$, so dass die Bedingungen von Satz 3.5.5 erfüllt sind. Dann nennt man das n-tupel $(T_1, \dots, T_n)$ (bzw. die Elemente $T_1, \dots, T_n$) *algebraisch unabhängig* über R (andernfalls *algebraisch abhängig*).

Sei nun $(T_1, \dots, T_n)$ algebraisch unabhängig über R. Dann nennt man (allgemeiner als in 3.5.4) den Ring $R[T_1, \dots, T_n]$ einen *Polynomring* (in den Unbestimmten $T_1, \dots, T_n$) über R. Dann hat jedes $f \in R[T_1, \dots, T_n]$ eine eindeutige Darstellung

$$f = \sum_{\nu_1, \dots, \nu_n \geq 0} c_{\nu_1, \dots, \nu_n} T_1^{\nu_1} \cdot \ldots \cdot T_n^{\nu_n} \text{ mit } c_{\nu_1, \dots, \nu_n} \in R,\ c_{\nu_1, \dots, \nu_n} = 0 \text{ für fast alle } (\nu_1, \dots, \nu_n) \in \mathbb{N}_0^n .$$

Die Elemente $c_{\nu_1, \dots, \nu_n} \in R$ heißen die *Koeffizienten* von f, und man sagt auch, f ist ein *Polynom* in n Unbestimmten mit Koeffizienten in R.

Ist $S \supset R$ ein kommutativer Oberring und $(z_1, \dots, z_n) \in S^n$, so gibt es nach Satz 3.5.5 genau einen Ringhomomorphismus

$$\Psi = \Psi^{(T_1,\dots,T_n)}_{(z_1,\dots,z_n)} \colon R[T_1, \dots, T_n] \to S \quad \text{mit} \quad \Psi \,|\, R = \mathrm{id}_R \quad \text{und} \quad \Psi(T_i) = z_i \quad \text{für alle } i \in [1, n] \,.$$

Man nennt Ψ den *Einsetzungshomomorphismus* und schreibt (wenn bezüglich der Unbestimmten $T_1, \dots, T_n$ keine Verwechslungen zu befürchten sind) $f(z_1, \dots, z_n)$ an Stelle von $\Psi^{(T_1,\dots,T_n)}_{(z_1,\dots,z_n)}(f)$. Ist

$$f = \sum_{\nu_1,\dots,\nu_n \geq 0} c_{\nu_1,\dots,\nu_n} T_1^{\nu_1} \cdot \ldots \cdot T_n^{\nu_n} \,, \quad \text{so folgt} \quad f(z_1, \dots, z_n) = \sum_{\nu_1,\dots,\nu_n \geq 0} c_{\nu_1,\dots,\nu_n} z_1^{\nu_1} \cdot \ldots \cdot z_n^{\nu_n} \,.$$

Man nennt $f(z_1, \dots, z_n)$ den *Wert* von f an der Stelle $\boldsymbol{z} = (z_1, \dots, z_n)$, und man nennt $\boldsymbol{z} \in S^n$ eine *Nullstelle* von f, wenn $f(\boldsymbol{z}) = 0$. f heißt *nullstellenfrei* in S^n, wenn $f(\boldsymbol{z}) \neq 0$ für alle $\boldsymbol{z} \in S^n$.

Für alle $f, g \in R[T_1, \dots, T_n]$ und $\boldsymbol{z} \in S^n$ ist dann $(f + g)(\boldsymbol{z}) = f(\boldsymbol{z}) + g(\boldsymbol{z})$ und $(fg)(\boldsymbol{z}) = f(\boldsymbol{z})g(\boldsymbol{z})$. Ist insbesondere $f \in R$, so ist $f(\boldsymbol{z}) = f$.

Ist insbesondere $S = R[T_1, \dots, T_n]$, so ist $f = f(T_1, \dots, T_n)$ für alle $f \in R[T_1, \dots, T_n]$ (was diese häufig unreflektiert gebrauchte Schreibweise rechtfertigt). Sind $g_1, \dots, g_n \in R[T_1, \dots, T_n]$, so ist auch $f(g_1, \dots, g_n) \in R[T_1, \dots, T_n]$ (Einsetzen von Polynomen in Polynome).

Für $f \in R[X_1, \dots, X_n]$ heißt die Abbildung

$$f_S \colon S^n \to S \,, \quad \text{definiert durch} \quad f_S(\boldsymbol{z}) = f(\boldsymbol{z}) \,,$$

die durch f auf S^n definierte *Polynomfunktion*. Die Abbildung

$$\theta \colon R[X_1, \dots, X_n] \to \mathrm{Abb}(S^n, S) \,, \quad \text{definiert durch} \quad \theta(f) = f_S \,,$$

ist ein Ringhomomorphismus, der im Allgemeinen weder injektiv noch surjektiv ist.

[Beweis: Für $f, g \in R[X_1, \dots, X_n]$ und $\boldsymbol{z} \in S^n$ ist

$$(f + g)_S(\boldsymbol{z}) = (f + g)(\boldsymbol{z}) = f(\boldsymbol{z}) + g(\boldsymbol{z}) = f_S(\boldsymbol{z}) + g_S(\boldsymbol{z}) = (f_S + g_S)(\boldsymbol{z}) \,,$$

und in gleicher Weise für $\cdot$ an Stelle von $+$. Im Falle $R = S = \mathbb{R}$ ist θ nicht surjektiv (nicht jede Abbildung ist eine Polynomfunktion), und im Falle $R = S = \mathbb{F}_2$ mit $n = 1$ ist θ nicht injektiv (für alle $k \in \mathbb{N}$ ist $\theta(X^k) = \mathrm{id}_{\mathbb{F}_2}$)].

Konvention. Im Folgenden werden wir die Symbole X und $X_1, \dots, X_n$ nicht mehr für die Bedeutungen von Definition 3.5.1 reservieren und unter einem Polynomring $R[X]$ bzw. $R[X_1, \dots, X_n]$ einen beliebigen Polynomring im Sinne dieser Definition in der Unbestimmten X bzw. in den Unbestimmten $X_1, \dots, X_n$ verstehen.

Satz 3.5.7 (Existenzsatz für Polynomringe). *Sei $(R_\lambda \neq \{0\})_{\lambda \in \Lambda}$ eine Familie kommutativer Ringe und $n \in \mathbb{N}$. Dann gibt es eine Menge $X = \{X_1, \dots, X_n\}$ mit $|X| = n$, und es gibt für jedes $\lambda \in \Lambda$ einen Oberring $R'_\lambda \supset R_\lambda$, so dass $R'_\lambda = R_\lambda[X_1, \dots, X_n]$ ein Polynomring in $X_1, \dots, X_n$ über R_λ ist. Ist Ω eine Menge mit $\Omega \cap R_\lambda = \emptyset$ für alle $\lambda \in \Lambda$, so kann man die Polynomringe R'_λ so wählen, dass $R'_\lambda \cap \Omega = \emptyset$ für alle $\lambda \in \Lambda$.*

Beweis. Für $\lambda \in \Lambda$ sei $\overline{R}_\lambda = R_\lambda[X'_{\lambda,1}, \dots, X'_{\lambda,n}]$ ein Polynomring über R_λ gemäß 3.5.4.2., und sei X eine Menge mit $|X| = n$ und $X \cap (\Omega \cup R_\lambda) = \emptyset$ für alle $\lambda \in \Lambda$ (siehe Lemma 3.3.2). Für $\lambda \in \Lambda$ sei die Abbildung $\varphi_\lambda \colon R_\lambda \cup X \to \overline{R}_\lambda$ definiert durch $\varphi_\lambda \,|\, R_\lambda = \mathrm{id}_{R_\lambda}$ und $\varphi_\lambda(X_i) = X'_{\lambda,i}$ für alle $i \in [1, n]$. Dann ist φ_λ injektiv, und nach Lemma 3.3.3 gibt es einen Oberring $R'_\lambda \supset R_\lambda$ mit $X \subset R'_\lambda$, $R'_\lambda \cap \Omega = \emptyset$, und es gibt einen Ringisomorphismus $\varphi'_\lambda \colon R'_\lambda \to \overline{R}_\lambda$, so dass $\varphi'_\lambda \,|\, R_\lambda \cup X = \varphi_\lambda$. Dann ist $R'_\lambda = R_\lambda[X_1, \dots, X_n]$ ein Polynomring in $X_1, \dots, X_n$ über R_λ. □

Satz 3.5.8 (Iterationssatz für Polynomringe). *Sei $\{0\} \neq R \subset \overline{R}$ eine Ringerweiterung kommutativer Ringe, $n \in \mathbb{N}$, $k \in [1, n-1]$ und $(X_1, \dots, X_n) \in R^n$. Dann sind äquivalent:*

(a) $R[X_1, \dots, X_n]$ *ist ein Polynomring in* $X_1, \dots, X_n$ *über* R.

(b) $R[X_1, \dots, X_k]$ *ist ein Polynomring in* $X_1, \dots, X_k$ *über* R, *und* $R[X_1, \dots, X_n]$ *ist ein Polynomring in* $(X_{k+1}, \dots, X_n)$ *über* $R[X_1, \dots, X_k]$.

BEWEIS. Nach Satz 3.1.8.5 ist $R[X_1, \dots, X_n] = R[X_1, \dots, X_k][X_{k+1}, \dots, X_n]$.

(a) $\Rightarrow$ (b) Sind $X_1, \dots, X_n$ algebraisch unabhängig über R, so sind auch $X_1, \dots, X_k$ algebraisch unabhängig über R, und es ist die algebraische Unabhängigkeit von $(X_{k+1}, \dots, X_n)$ über $R[X_1, \dots, X_k]$ zu zeigen. Wir weisen die Bedingung von Satz 3.5.5(d) nach. Sei also $\psi\colon R[X_1, \dots, X_k] \to \overline{R}$ ein Ringhomomorphismus und $(z_{k+1}, \dots, z_n) \in \overline{R}^{n-k}$. Für $i \in [1, k]$ sei $z_i = \psi(X_i) \in \overline{R}$. Dann gibt es genau einen Ringhomomorphismus $\Psi\colon R[X_1, \dots, X_n] \to \overline{R}$ mit $\Psi \mid R = \psi \mid R$ und $\Psi(X_i) = z_i$ für alle $i \in [1, n]$, und für diesen ist $\Psi \mid R[X_1, \dots, X_k] = \psi$.

(b) $\Rightarrow$ (a) Wir weisen wieder die Bedingung von Satz 3.5.5(d) nach. Sei $\psi\colon R \to \overline{R}$ ein Ringhomomorphismus, und sei $(z_1, \dots, z_n) \in \overline{R}^n$. Wegen der algebraischen Unabhängigkeit von $(X_1, \dots, X_k)$ gibt es einen Ringhomomorphismus $\psi_1\colon R[X_1, \dots, X_k] \to \overline{R}$, so dass $\psi_1 \mid R = \psi$ und $\psi_1(X_i) = z_i$ für alle $i \in [1, k]$, und wegen der algebraischen Unabhängigkeit von $(X_{k+1}, \dots, X_n)$ über $R[X_1, \dots, X_k]$ gibt es einen Ringhomomorphismus $\Psi\colon R[X_1, \dots, X_n] \to \overline{R}$, so dass $\Psi \mid R[X_1, \dots, X_k] = \psi_1$ und $\Psi(X_i) = z_i$ für alle $i \in [k+1, n]$. Dann ist $\Psi \mid R = \psi$ und $\Psi(X_i) = z_i$ für alle $i \in [1, n]$. □

Satz 3.5.9. *Sei* R *ein Bereich,* $n \in \mathbb{N}$ *und* $R[X_1, \dots, X_n]$ *ein Polynomring. Dann ist* $R[X_1, \dots, X_n]$ *ein Bereich, und* $R[X_1, \dots, X_n]^\times = R^\times$. *Insbesondere ist* $R[X_1, \dots, X_n]$ *kein Körper.*

BEWEIS. Nach Definition gibt es einen Isomorphismus $\Phi\colon R[\mathbb{N}_0^n] \to R[X_1, \dots, X_n]$ mit $\Phi \mid R = \mathrm{id}_R$, und daher genügt es, die Behauptung für $R[\mathbb{N}_0^n]$ zu zeigen. $(\mathbb{N}_0^n, +)$ ist ein reduziertes Monoid, und $\mathsf{q}(\mathbb{N}_0^n) = \mathbb{Z}^n$ ist torsionsfrei. Daher folgen die Behauptungen aus Satz 3.5.2.4. und 5. □

Definition 3.5.10. Sei K ein Körper, $n \in \mathbb{N}$ und $K[X_1, \dots, X_n]$ ein Polynomring. Der Quotientenkörper $K(X_1, \dots, X_n) = \mathsf{q}(K[X_1, \dots, X_n])$ heißt *rationaler Funktionenkörper* (in den Unbestimmten $X_1, \dots, X_n$) über K.

Korollar 3.5.11. *Sei* R *ein Bereich,* $K = \mathsf{q}(R)$, $n \in \mathbb{N}$ *und* $R[X_1, \dots, X_n]$ *ein Polynomring. Dann ist* $K(X_1, \dots, X_n) = \mathsf{q}(R[X_1, \dots, X_n])$.

BEWEIS. Nach Definition und Bemerkung 3.3.7.2 ist $\mathsf{q}(R[X_1, \dots, X_n]) \subset K(X_1, \dots, X_n)$. Sei also $h = g^{-1}f \in K(X_1, \dots, X_n)$ mit $f, g \in K[X_1, \dots, X_n]$, $g \neq 0$. Sei $a \in R^\bullet$ ein gemeinsamer Nenner der von 0 verschiedenen Koeffizienten von f und g. Dann folgt $af, ag \in R[X_1, \dots, X_n]$, $ag \neq 0$ und $h = (ag)^{-1}(af) \in \mathsf{q}(R[X_1, \dots, X_n])$. □

Bemerkung und Definition 3.5.12. Sei $\varphi\colon R \to \overline{R}$ ein Homomorphismus kommutativer Ringe, sei $R \neq \{0\}$, $\overline{R} \neq \{0\}$, $n \in \mathbb{N}$ und seien $R[X_1, \dots, X_n]$ und $\overline{R}[X_1, \dots, X_n]$ Polynomringe (gemäß Satz 3.5.7). Dann gibt es nach Satz 3.5.5(d) genau einen Ringhomomorphismus

$$\varphi_1\colon R[X_1, \dots, X_n] \to \overline{R}[X_1, \dots, X_n] \quad \text{mit} \quad \varphi_1 \mid R = \varphi \quad \text{und} \quad \varphi_1(X_i) = X_i \ \text{ für alle } \ i \in [1, n]\,.$$

Man nennt φ_1 die *kanonische Fortsetzung von* φ *auf die Polynomringe.*

Ist φ injektiv (bzw. surjektiv), so ist auch φ_1 injektiv (bzw. surjektiv).

Satz 3.5.13. *Sei* R *ein kommutativer Ring,* $I \lhd R$, $I \neq R$, $\pi\colon R \to R/I$ *der Restklassenhomomorphismus,* $n \in \mathbb{N}$, *und* $\pi_1\colon R[X_1, \dots, X_n] \to (R/I)[X_1, \dots, X_n]$ *die kanonische Fortsetzung von* π *auf die Polynomringe. Dann ist*

$$\mathrm{Ker}(\pi_1) = IR[X_1, \dots, X_n] = \Big\{ \sum_{\boldsymbol{\nu} \in \mathbb{N}_0^n} c_{\boldsymbol{\nu}} \boldsymbol{X}^{\boldsymbol{\nu}} \;\Big|\; c_{\boldsymbol{\nu}} \in I\,,\ c_{\boldsymbol{\nu}} = 0 \ \textit{für fast alle}\ \boldsymbol{\nu} \in \mathbb{N}_0^n \Big\}$$

(*mit* $\boldsymbol{X}^{\boldsymbol{\nu}} = X_1^{\nu_1} \cdot \ldots \cdot X_n^{\nu_n}$ *für* $\boldsymbol{\nu} = (\nu_1, \ldots, \nu_n) \in \mathbb{N}_0^n$). *Insbesondere induziert* π_1 *einen Isomorphismus*

$$R[X_1, \ldots, X_n]/IR[X_1, \ldots, X_n] \xrightarrow{\sim} (R/I)[X_1, \ldots, X_n] .$$

BEWEIS. π_1 ist ein Epimorphismus und induziert nach Satz 3.2.9.3 einen Isomorphismus

$$R[X_1, \ldots, X_n]/\mathrm{Ker}(\pi_1) \xrightarrow{\sim} (R/I)[X_1, \ldots, X_n] .$$

Ist

$$f = \sum_{\boldsymbol{\nu} \in \mathbb{N}_0^n} c_{\boldsymbol{\nu}} \boldsymbol{X}^{\boldsymbol{\nu}} \quad \text{mit} \quad c_{\boldsymbol{\nu}} \in R, \ c_{\boldsymbol{\nu}} = 0 \ \text{ für fast alle } \boldsymbol{\nu} \in \mathbb{N}_0^n, \ \text{ so folgt } \quad \pi_1(f) = \sum_{\boldsymbol{\nu} \in \mathbb{N}_0^n} (c_{\boldsymbol{\nu}} + I) \boldsymbol{X}^{\boldsymbol{\nu}} .$$

Also ist genau dann $f \in \mathrm{Ker}(\pi_1)$, wenn $c_{\boldsymbol{\nu}} \in I$ für alle $\boldsymbol{\nu} \in \mathbb{N}_0^n$. □

3.6. Polynome in einer Unbestimmten

Definition 3.6.1. Sei $R \neq \{0\}$ ein kommutativer Ring, $R[X]$ ein Polynomring und

$$f = \sum_{\nu \geq 0} a_\nu X^\nu \in R[X] .$$

1. Es sei $\mathrm{gr}(f) = \max\{\nu \in \mathbb{N}_0 \mid a_\nu \neq 0\}$, falls $f \neq 0$, und $\mathrm{gr}(0) = -\infty$.
   Dann heißt $\mathrm{gr}(f) \in \mathbb{N}_0 \cup \{-\infty\}$ der *Grad von* f. Ist $\mathrm{gr}(f) = n \in \mathbb{N}_0$, so heißt a_n der *höchste Koeffizient* oder *Leitkoeffizient* von f. Das Polynom f heißt
   - *normiert*, wenn $f \neq 0$ und 1 der höchste Koeffizient von f ist.
   - *konstant*, wenn $f \in R$ (äquivalent: $\mathrm{gr}(f) \leq 0$).

   Für jedes $n \geq \mathrm{gr}(f)$ können wir dann f auch in der Form

   $$f = \sum_{\nu=0}^{n} a_\nu X^\nu \quad \text{mit} \quad a_0, \ldots, a_n \in R$$

   schreiben, und dann gilt: $\mathrm{gr}(f) = n \iff a_n \neq 0$.
2. Das Polynom
   $$f' = \sum_{\nu \geq 1} \nu a_\nu X^{\nu-1} \in R[X]$$
   heißt *Ableitung* von f.

Lemma 3.6.2. *Sei* $R \neq \{0\}$ *ein kommutativer Ring,* $R[X]$ *ein Polynomring, und seien* $f, g \in R[X]$.

1. *Es ist* $\mathrm{gr}(f+g) \leq \max\{\mathrm{gr}(f), \mathrm{gr}(g)\}$, $\mathrm{gr}(fg) \leq \mathrm{gr}(f) + \mathrm{gr}(g)$, *und im Falle* $\mathrm{gr}(f) \neq \mathrm{gr}(g)$ *ist* $\mathrm{gr}(f+g) = \max\{\mathrm{gr}(f), \mathrm{gr}(g)\}$.
2. *Sei* $f \neq 0$, $g \neq 0$, $a \in R$ *der höchste Koeffizient von* f *und* $b \in R$ *der höchste Koeffizient von* g. *Ist* $ab = 0$, *so ist* $\mathrm{gr}(fg) < \mathrm{gr}(f) + \mathrm{gr}(g)$. *Ist* $ab \neq 0$, *so ist* $\mathrm{gr}(fg) = \mathrm{gr}(f) + \mathrm{gr}(g)$, *und* ab *ist der höchste Koeffizient von* fg. *Ist insbesondere* $a \in R^\bullet$, *so ist* $f \in R[X]^\bullet$.
3. *Sind zwei der drei Polynome* f, g, fg *normiert, so ist auch das dritte normiert, und es ist* $\mathrm{gr}(fg) = \mathrm{gr}(f) + \mathrm{gr}(g)$.

BEWEIS. Klar. □

Lemma 3.6.3. *Sei* $R \neq \{0\}$ *ein kommutativer Ring,* $R[X]$ *ein Polynomring,* $f, g \in R[X]$, $c \in R$ *und* $k \in \mathbb{N}$.

1. $(f+g)' = f' + g'$, $(fg)' = f'g + fg'$ *und* $(cf)' = cf'$.

2. $(g^k)' = kg^{k-1}g'$.
3. $f(g)' = f'(g)g'$.

BEWEIS. 1. Offensichtlich ist $(f+g)' = f' + g'$ und $(cf)' = cf'$, und für $n \in \mathbb{N}$ gilt:

$$g = \sum_{\nu\geq 0} b_\nu X^\nu \quad \text{folgt} \quad (X^n g)' = \Big(\sum_{\nu\geq 0} b_\nu X^{n+\nu}\Big)' = \sum_{\nu\geq 0} b_\nu (n+\nu) X^{n+\nu-1}$$
$$= nX^{n-1}\sum_{\nu\geq 0} b_\nu X^\nu + X^n \sum_{\nu\geq 1} \nu b_\nu X^{\nu-1} = (X^n)'g + X^n g' .$$

Damit folgt $(cX^n g)' = (cX^n)'g + cX^n g'$, und das gilt auch für $n = 0$. Ist nun

$$f = \sum_{\nu\geq 0} a_\nu X^\nu , \quad \text{so folgt} \quad (fg)' = \Big(\sum_{\nu\geq 0} a_\nu X^\nu g\Big)' = \sum_{\nu\geq 0} (a_\nu X^\nu)'g + \sum_{\nu\geq 0} a_\nu X^\nu g' = f'g + fg' .$$

2. Induktion nach k mittels 1. (Übung).
3. Aus
$$f = \sum_{\nu\geq 0} a_\nu X^\nu \quad \text{folgt} \quad f(g)' = \sum_{\nu\geq 0} a_\nu (g^\nu)' = \sum_{\nu\geq 1} a_\nu \nu g^{\nu-1} g' = f'(g)g' .$$

□

Satz 3.6.4 (Division mit Rest)**.** *Sei $R \neq \{0\}$ ein kommutativer Ring und $R[X]$ ein Polynomring. Seien $f, g \in R[X]$, $g \neq 0$, und sei der höchste Koeffizient von g in $R^\times$. Dann existieren eindeutig bestimmte $q, r \in R[X]$ mit*

$$f = gq + r \quad \textit{und} \quad \operatorname{gr}(r) < \operatorname{gr}(g).$$

BEWEIS. EINDEUTIGKEIT: Seien $q_1, r_1, q_2, r_2 \in R[X]$, so dass $f = q_1 g + r_1 = q_2 g + r_2$, $\operatorname{gr}(r_1) < \operatorname{gr}(g)$ und $\operatorname{gr}(r_2) < \operatorname{gr}(g)$. Wäre $q_1 \neq q_2$, so folgte

$$\operatorname{gr}\big(g(q_1 - q_2)\big) = \operatorname{gr}(g) + \operatorname{gr}(q_1 - q_2) \geq \operatorname{gr}(g) > \max\{\operatorname{gr}(r_1), \operatorname{gr}(r_2)\} \geq \operatorname{gr}(r_2 - r_1) = \operatorname{gr}\big(g(q_1 - q_2)\big) ,$$

ein Widerspruch. Also ist $q_1 = q_2$ und daher auch $r_1 = r_2$.

EXISTENZ: Induktion nach $\operatorname{gr}(f)$. Ist $\operatorname{gr}(f) < \operatorname{gr}(g)$, so setzen wir $q = 0$ und $r = f$.
Sei nun $\operatorname{gr}(f) = n \geq \operatorname{gr}(g)$ und die Behauptung für alle $f_0 \in R[X]$ mit $\operatorname{gr}(f_0) < n$ gezeigt. Sei $f = aX^n + f_1$ mit $a \in R \setminus \{0\}$, $f_1 \in R[X]$, $\operatorname{gr}(f_1) < n$, und sei $g = uX^m + g_1$ mit $0 \leq m = \operatorname{gr}(g) \leq n$, $u \in R^\times$, $g_1 \in R[X]$ mit $\operatorname{gr}(g_1) < m$. Dann ist

$$f_0 = f - u^{-1}aX^{n-m}g = f_1 - u^{-1}aX^{n-m}g_1 \in R[X] \quad \text{und} \quad \operatorname{gr}(f_0) < n .$$

Nach Induktionsvoraussetzung existieren $q_0, r \in R[X]$ mit $f_0 = gq_0 + r$ und $\operatorname{gr}(r) < \operatorname{gr}(g)$. Dann ist

$$f = f_0 + u^{-1}aX^{n-m}g = g(q_0 + u^{-1}aX^{n-m}) + r ,$$

und mit $q = q_0 + u^{-1}aX^{n-m}$ folgt die Behauptung. □

Definition und Satz 3.6.5. *Sei $R \neq \{0\}$ ein kommutativer Ring, $R[X]$ ein Polynomring, $f \in R[X]$ und $\alpha \in R$.*

1. *Genau dann ist $f(\alpha) = 0$, wenn es ein $g \in R[X]$ gibt, so dass $f = (X - \alpha)g$.*
2. *Sei $f \neq 0$. Dann gibt es genau ein $k \in \mathbb{N}_0$, so dass $f = (X-\alpha)^k g$ mit einem Polynom $g \in R[X]$, so dass $g(\alpha) \neq 0$.*
   Man nennt $k = \operatorname{ord}(f, \alpha)$ die *Ordnung* von f an der Stelle α. Im Falle $k \geq 1$ heißt k die *Vielfachheit* der Nullstelle α von f und man nennt dann α eine *k-fache Nullstelle* von f. Im Falle $k = 1$ heißt α eine *einfache Nullstelle* von f, im Falle $k \geq 2$ heißt α eine *mehrfache Nullstelle* von f.
3. *Sei $f \neq 0$. Genau dann ist α eine mehrfache Nullstelle von f, wenn $f(\alpha) = f'(\alpha) = 0$.*

BEWEIS. 1. Ist $f = (X-\alpha)g$ mit $g \in R[X]$, so folgt $f(\alpha) = (\alpha-\alpha)g(\alpha) = 0$.

Sei nun $f(\alpha) = 0$. Nach Satz 3.6.4 existieren Polynome q, $r \in R[X]$, so dass $f = (X-\alpha)q + r$ und $\operatorname{gr}(r) < \operatorname{gr}(X-\alpha) = 1$, also $r \in R$. Aus $0 = f(\alpha) = (\alpha-\alpha)q(\alpha) + r = r$ folgt $r = 0$.

2. EXISTENZ: Sei $T = \{n \in \mathbb{N}_0 \mid f = (X-\alpha)^n g \text{ mit einem Polynom } g \in R[X]\}$. Ist $n \in T$, so folgt $\operatorname{gr}(f) \geq n$ und daher existiert $k = \max(T) \in \mathbb{N}_0$. Sei $g \in R[X]$ mit $f = (X-\alpha)^k g$. Aus 1. und der Maximalität von k folgt dann $g(\alpha) \neq 0$.

EINDEUTIGKEIT: Sei $f = (X-\alpha)^m g = (X-\alpha)^n h$ mit $m, n \in \mathbb{N}_0$, $m \leq n$ und $g, h \in R[X]$. Wegen $X - \alpha \in R^\bullet$ folgt daraus $g = (X-\alpha)^{n-m} h$, und wegen $g(\alpha) \neq 0$ folgt $m = n$.

3. Sei $\operatorname{ord}(f,\alpha) = k \geq 1$ und $f = (X-\alpha)^k g$ mit $g \in R[X]$ und $g(\alpha) \neq 0$. Dann ist $f' = k(X-\alpha)^{k-1} g + (X-\alpha)^k g'$, also $f'(\alpha) = 0$, falls $k \geq 2$, und $f'(\alpha) = g(\alpha) \neq 0$, falls $k = 1$. □

Satz 3.6.6. *Sei K ein Körper, $n \in \mathbb{N}$ und $K[X]$ ein Polynomring. Dann ist*

$$\operatorname{gr} | K[X]^\bullet \colon K[X]^\bullet \to \mathbb{N}_0 \quad \textit{eine euklidische Normfunktion.}$$

Insbesondere ist $K[X]$ ein Hauptidealbereich, und für jedes Ideal $\{0\} \neq I \lhd K[X]$ gilt:

1. *Ist $f \in I \setminus \{0\}$, so dass $\operatorname{gr}(f) = \min\big(\{\operatorname{gr}(g) \mid g \in I\,,\ g \neq 0\}\big)$, so ist $I = fK[X]$.*
2. *Es gibt genau ein normiertes Polynom $f \in K[X]$, so dass $I = fK[X]$.*

BEWEIS. Nach Satz 3.6.4 ist $\operatorname{gr} | K[X]^\bullet$ eine euklidische Normfunktion, und nach Satz 3.4.5 ist $K[X]$ ein Hauptidealring, und es gilt 1.

2. Sei $\{0\} \neq I \lhd K[X]$. Nach 1. ist $I = f_1 K[X]$ mit $f_1 \in K[X]^\bullet$. Sei $a \in K^\times$ der höchste Koeffizient von f_1. Dann ist $f = a^{-1} f_1 \in K[X]$ normiert und $f \simeq f_1$, also $fK[X] = f_1 K[X]$. Sind f_1, $f_2 \in K[X]$ normierte Polynome mit $f_1 K[X] = f_2 K[X]$, so folgt $f_2 = f_1 u$ mit $u \in K[X]^\times = K^\times$. Nach Lemma 3.6.2.3 ist u normiert, also $u = 1$. □

Satz 3.6.7. *Sei R ein Bereich, $R[X]$ ein Polynomring und $f \in R[X]^\bullet$. Dann hat f eine (bis auf die Reihenfolge der Faktoren) eindeutige Darstellung der Form*

$$(*) \qquad f = \prod_{i=1}^{r} (X-\alpha_i)^{k_i} g$$

mit $r \in \mathbb{N}_0$, verschiedenen $\alpha_1, \ldots, \alpha_r \in R$, $k_1, \ldots, k_r \in \mathbb{N}$ und einem in R nullstellenfreiem $g \in R[X]$. Für alle $i \in [1,r]$ ist $k_i = \operatorname{ord}(f, \alpha_i)$, und

$$|\{\alpha \in R \mid f(\alpha) = 0\}| \leq \sum_{i=1}^{r} \operatorname{ord}(f,\alpha_i) \leq n\,.$$

BEWEIS. EXISTENZ: Induktion nach $\operatorname{gr}(f)$. Ist f in R nullstellenfrei, so setzen wir $r = 0$ und $g = f$. Sei nun $\alpha \in R$ mit $f(\alpha) = 0$. Nach Satz 3.6.5 ist $f = (X-\alpha) f_1$ mit $f_1 \in R[X]^\bullet$, und $\operatorname{gr}(f) = 1 + \operatorname{gr}(f_1) > \operatorname{gr}(f_1)$. Nach Induktionsvoraussetzung hat f_1 eine Darstellung der gewünschten Form, und daher hat auch f eine solche Darstellung.

EINDEUTIGKEIT: Habe f die Darstellung $(*)$. Wir zeigen: $\{\alpha_1, \ldots, \alpha_r\} = \{\alpha \in R \mid f(\alpha) = 0\}$, und für alle $i \in [1,r]$ ist $k_i = \operatorname{ord}(f, \alpha_i)$.

Für $i \in [1,r]$ $f(\alpha_i) = 0$ und

$$f = (X-\alpha_i)^{k_i} f_i \quad \text{mit} \quad f_i = \prod_{\substack{j=1 \\ j \neq i}}^{r} (X-\alpha_j) g\,, \quad \text{und} \quad f_i(\alpha_i) = \prod_{\substack{j=1 \\ j \neq i}}^{r} (\alpha_i - \alpha_j) g(\alpha_i) \neq 0\,,$$

also $\operatorname{ord}(f,\alpha_i)=k_i$. Für $\alpha\in R$ ist $g(\alpha)\neq 0$ und daher

$$f(\alpha)=\prod_{i=1}^{r}(\alpha-\alpha_i)^{k_i}g(\alpha)=0 \iff \alpha\in\{\alpha_1,\dots,\alpha_r\}\,.$$

□

Bemerkung 3.6.8. Ist R kein Bereich, so braucht Satz 3.6.7 nicht zu gelten. Sei dazu $R=\mathbb{Z}/8\mathbb{Z}$. Dann hat das Polynom

$$f=X^2-\overline{1}=(X-\overline{1})(X-\overline{7})=(X-\overline{3})(X-\overline{5})\in R[X]$$

die Nullstellen $\overline{1},\overline{3},\overline{5}$ und $\overline{7}$ (mit $\overline{k}=k+8\mathbb{Z}$) .

Korollar 3.6.9. *Sei R ein unendlicher Bereich, $n\in\mathbb{N}$ und $R[X_1,\dots,X_n]$ ein Polynomring. Für $f\in R[X_1,\dots,X_n]$ sei $f_R\colon R^n\to R$, $\boldsymbol{z}\mapsto f(\boldsymbol{z})$, die durch f definierte Polynomfunktion auf R^n. Dann ist die Abbildung*

$$\theta\colon R[X_1,\dots,X_n]\to \operatorname{Abb}(R^n,R)\,,\ \textit{definiert durch}\quad \theta(f)=f_R\,,$$

ein Ringmonomorphismus.

Beweis. Nach 3.5.6 ist θ ein Ringhomomorphismus. Wir müssen zeigen: Ist $f\in R[X_1,\dots,X_n]$ und $f(\boldsymbol{z})=0$ für alle $\boldsymbol{z}\in R^n$, so ist $f=0$. Wir führen den Beweis durch Induktion nach n.

$n=1$: Ist $f\in R[X]^\bullet$, so ist $|\{z\in R\mid f(z)=0\}|\le \operatorname{gr}(f)$ nach Satz 3.6.7, und wegen $|R|=\infty$ folgt die Behauptung.

$n\ge 2$, $n-1\mapsto n$: Sei $f\in R[X_1,\dots,X_n]$ und $f(\boldsymbol{z})=0$ für alle $\boldsymbol{z}\in R^n$. Wegen $R[X_1,\dots,X_n]=R[X_1,\dots,X_{n-1}][X_n]$ hat f eine Darstellung in der Form

$$f=\sum_{\nu\ge 0}f_\nu X_n^\nu \quad\text{mit}\quad f_\nu\in R[X_1,\dots,X_{n-1}] \text{ und } f_\nu=0 \text{ für fast alle } \nu\ge 0\,.$$

Für $\boldsymbol{z}'=(z_1,\dots,z_{n-1})\in R^{n-1}$ sei

$$f_{\boldsymbol{z}'}=\sum_{\nu\ge 0}f_\nu(\boldsymbol{z}')X_n^\nu\in R[X_n]\,,\quad \text{also}\quad f_{\boldsymbol{z}'}(z)=f(z_1,\dots,z_n,z)=0\quad\text{für alle}\quad z\in R$$

und daher $f_{\boldsymbol{z}'}=0$, also $f_\nu(\boldsymbol{z}')=0$ für alle $\nu\ge 0$.

Für jedes $\nu\ge 0$ ist nun $f_\nu(\boldsymbol{z}')=0$ für alle $\boldsymbol{z}'\in R^{n-1}$, also $f_\nu=0$ nach Induktionsvoraussetzung, und daher $f=0$. □

3.7. Primideale und maximale Ideale

Definition 3.7.1. Sei R ein kommutativer Ring. Ein Ideal $Q\lhd R$ heißt

- *Primideal* oder *primes Ideal*, wenn $Q\neq R$ und für alle $a,b\in R$ gilt: Aus $ab\in Q$ folgt $a\in Q$ oder $b\in Q$ ($\iff$ $1\notin Q$, und $R\setminus Q$ ist multiplikativ abgeschlossen).
- *maximales Ideal*, wenn $Q\neq R$, und es gibt kein Ideal $I\lhd R$ mit $Q\subsetneq I\subsetneq R$.

Satz 3.7.2. *Sei R ein kommutativer Ring und $Q\lhd R$ ein Ideal.*

1. *Genau dann ist Q ein maximales Ideal, wenn R/Q ein Körper ist.*
2. *Genau dann ist Q ein Primideal, wenn R/Q ein Bereich ist.*

   Insbesondere ist jedes maximale Ideal ein Primideal, und R ist genau dann ein Bereich, wenn $\{0\}$ ein Primideal ist.

3. *Ist R ein Hauptidealbereich, so ist jedes von $\{0\}$ verschiedene Primideal ein maximales Ideal.*

BEWEIS. 1. Nach Korollar 3.2.10 ist Q genau dann ein maximales Ideal von R, wenn $Q/Q = \{0_{R/Q}\}$ und R/Q die einzigen Ideale von R/Q sind. Dies ist nach Satz 3.4.2 genau dann der Fall, wenn R/Q ein Körper ist.

2. Sei $a \in R$. Genau dann ist $a+Q \in n(R/Q)$, wenn es ein $b \in R$ gibt, so dass $b+Q \neq 0+Q$ (das heißt, $b \notin Q$) und $(a+Q)(b+Q) = 0+Q$ (das heißt, $ab \in Q$). Daher ist R/Q genau dann nullteilerfrei (also ein Bereich), wenn $Q \neq R$ und für alle $a, b \in R$ gilt: Aus $ab \in Q$ und $b \notin Q$ folgt $a \in Q$. Nach Definition ist das aber genau dann der Fall, wenn Q ein Primideal ist.

3. Sei R ein Hauptidealbereich, $\{0\} \neq P \lhd R$ ein Primideal von R und $Q \lhd R$ mit $P \subsetneq Q$. Wir zeigen $Q = R$. Sei $P = aR$ und $Q = bR$ mit $a, b \in R^\bullet$. Dann ist $b \notin aR$ und $a = bu$ mit $u \in R$. Damit folgt $u \in aR$, also $u = ax$ mit $x \in R$. Es ist dann $a = bax$, also $bx = 1$, $b \in R^\times$ und $Q = bR = R$. □

Satz 3.7.3 (Krull'scher Existenzsatz)**.** *Sei R ein kommutativer Ring, $I \lhd R$ ein Ideal, $T \subset R$ eine multiplikativ abgeschlossene Teilmenge, so dass $I \cap T = \emptyset$, und $\Omega = \{J \lhd R \mid I \subset J \text{ und } J \cap T = \emptyset\}$.*

1. *Ω besitzt ein (bzgl. $\subset$) maximales Element .*
2. *Jedes maximale Element von Ω ist ein Primideal.*

   Insbesondere gilt: Es gibt ein Primideal $P \lhd R$ mit $I \subset P$ und $P \cap T = \emptyset$.

BEWEIS. 1. Es ist $I \in \Omega$, und die Vereinigung jeder Kette in Ω gehört zu Ω (siehe Bemerkung 3.2.5.4). Nach dem Zorn'schen Lemma besitzt Ω ein maximales Element.

2. Durch Widerspruch. Wir nehmen an, es gibt ein maximales Element $P \in \Omega$, das kein Primideal ist. Dann gibt es $a, b \in R \setminus P$ mit $ab \in P$. Dann folgt $P + aR \notin \Omega$ und $P + bR \notin \Omega$, also $(P + aR) \cap T \neq \emptyset$ und $(P + bR) \cap T \neq \emptyset$. Seien $p_1, p_2 \in P$ und $c_1, c_2 \in R$ mit $p_1 + c_1 a \in T$ und $p_2 + c_2 b \in T$. Dann folgt $(p_1 + c_1 a)(p_2 + c_2 b) = p_1(p_2 + c_2 b) + p_2 c_1 a + c_1 c_2 ab \in P \cap T$, ein Widerspruch. □

Korollar 3.7.4. *Sei R ein kommutativer Ring. Dann gibt es zu jedem Ideal $I \lhd R$ mit $I \neq R$ ein maximales Ideal $M \lhd R$ mit $I \subset M$.*
Insbesondere gibt es zu jedem $a \in R \setminus R^\times$ ein maximales Ideal $M \lhd R$ mit $a \in M$.

BEWEIS. Sei $I \lhd R$, $I \neq R$. Dann folgt die Existenz eines maximalen Ideals $M \lhd R$ mit $I \subset M$ aus Satz 3.7.3 (mit $T = \{1\}$). Ist $a \in R \setminus R^\times$, so ist $aR \neq R$, und daher gibt es ein maximales Ideal $M \lhd R$ mit $aR \subset M$, also $a \in M$. □

Satz 3.7.5. *Sei $R \neq \{0\}$ ein kommutativer Ring, $n \in \mathbb{N}$ und $R[X_1, \ldots, X_n]$ ein Polynomring.*

1. *Sei entweder $n \geq 2$ oder R kein Körper. Dann gibt es in $R[X_1, \ldots, X_n]$ ein nicht maximales Primideal.*
2. *$R[X_1, \ldots, X_n]$ ist genau dann ein Hauptidealbereich, wenn $n = 1$ und R ein Körper ist.*

BEWEIS. 1. Sei zuerst $n = 1$ und R kein Körper. Nach Korollar 3.7.4 gibt es ein maximales Ideal $M \lhd R$. Sei $\pi\colon R \to R/M$ der Restklassenhomomorphismus und (mit $X = X_1$) $\pi_1\colon R[X] \to (R/M)[X]$ die kanonische Fortsetzung auf die Polynomringe. Da R kein Körper ist, ist $M \neq \{0\}$, und daher folgt $\mathrm{Ker}(\pi_1) = MR[X] \neq \{0\}$. Nun ist aber $R[X]/MR[X] \cong (R/M)[X]$, und $(R/M)[X]$ ist ein Bereich, aber kein Körper. Daher ist $MR[X]$ ein nicht maximales von $\{0\}$ verschiedenes Primideal.
Ist $n \geq 2$, so ist $R[X_1, \ldots, X_n] = R[X_1, \ldots, X_{n-1}][X_n]$, und $R[X_1, \ldots, X_{n-1}]$ ist kein Körper. Daher folgt die Behauptung aus dem Obigen.

2. Ist R ein Körper und $n = 1$, so ist der Polynomring $R[X]$ ein Hauptidealbereich nach Satz 3.6.6. Ist $n \geq 2$ oder R kein Körper, so ist $R[X_1, \ldots, X_n]$ kein Hauptidealbereich nach 1., und Satz 3.7.2.3. □

Beispiel 3.7.6. Sei $R \subset \mathbb{R}$ ein Teilkörper. Dann ist $\mathrm{F}(R) = \mathrm{Abb}(\mathbb{N}_0, R)$ (versehen mit wertweiser Addition und Multiplikation) der Ring aller Folgen in R. Es bezeichne

- $\mathrm{BF}(R)$ die Menge der beschränkten Folgen in R,
- $\mathrm{KF}(R)$ die Menge der konvergenten Folgen in R,
- $\mathrm{CF}(R)$ die Menge der Cauchyfolgen in R,
- $\mathrm{NF}(R)$ die Menge der Nullfolgen in R.

Im Folgenden geben wir eine ringtheoretischen Formulierungen der Rechenregeln für konvergente Folgen und Grenzwerte.

Identifiziert man die Elemente von R mit den konstanten Folgen, so ist

$$R \subset \mathrm{KF}(R) \subset \mathrm{CF}(R) \subset \mathrm{BF}(R) \subset \mathrm{F}(R)$$

eine Kette von Teilringen. Es ist $\mathrm{NF}(R) \subset \mathrm{KF}(R)$, und $\mathrm{NF}(R)$ ist ein Ideal von $\mathrm{BF}(R)$, also auch von $\mathrm{KF}(R)$ und von $\mathrm{CF}(R)$. Die Grenzwertabbildung $\lim\colon \mathrm{KF}(R) \to R$ ist ein Ringepimorphismus, und es ist $\mathrm{Ker}(\lim) = \mathrm{NF}(R)$. Daher induziert $\lim$ einen Isomorphismus $\mathrm{KF}(R)/\mathrm{NF}(R) \xrightarrow{\sim} R$, und $\mathrm{NF}(R)$ ist ein maximales Ideal von $\mathrm{KF}(R)$.

Wir benutzen nun, dass $R \subset \mathbb{R}$ dicht ist und jede Cauchyfolge in $\mathbb{R}$ konvergiert. Nach Definition ist $\mathrm{NF}(R) = \mathrm{NF}(\mathbb{R}) \cap \mathrm{F}(R) \subset \mathrm{KF}(R)$, und $\mathrm{CF}(R) = \mathrm{CF}(\mathbb{R}) \cap \mathrm{F}(R) = \mathrm{KF}(\mathbb{R}) \cap \mathrm{F}(R)$. Jedes Element von $\mathbb{R}$ ist Limes einer Folge $a \in \mathrm{KF}(R) \cap \mathrm{F}(R) = \mathrm{CF}(R)$, und daher ist $\lim | \mathrm{CF}(R)\colon \mathrm{CF}(R) \to \mathbb{R}$ ein Epimorphismus mit Kern $\mathrm{NF}(R)$, induziert also einen Isomorphismus $\mathrm{CF}(R)/\mathrm{NF}(R) \xrightarrow{\sim} \mathbb{R}$. Man kann nun umgekehrt diesen Isomorphismus zur algebraischen Konstruktion der reellen Zahlen aus den rationationen Zahlen verwenden.

CHAPTER 4

Direkte Produkte, prime Restklassen und Zifferndarstellungen

4.1. Endliche direkte Produkte

Satz 4.1.1. *Sei* $r \in \mathbb{N}$, *seien* $G_1, \ldots, G_r$ *Gruppen und* $G = G_1 \times \ldots \times G_r$ *ihr direktes Produkt.*

1. *Sei* $j \in [1, r]$ *und* $e_j \in G_j$ *das neutrale Element von* G_j. *Dann hat die Projektion* $p_j \colon G \to G_j$ *den Kern* $\mathrm{Ker}(p_j) = G_1 \times \ldots \times G_{j-1} \times \{e_j\} \times G_{j+1} \times \ldots \times G_r \lhd G$.
2. *Für jedes* $j \in [1, r]$ *sei* $N_j \lhd G_j$, *und es sei* $N = N_1 \times \ldots \times N_r$. *Dann ist* $N \lhd G$, *und*

$$\phi \colon G/N \to G_1/N_1 \times \ldots \times G_r/N_r\,, \quad \text{definiert durch} \quad (a_1, \ldots, a_r)N \mapsto (a_1N_1, \ldots, a_rN_r)$$

für alle $(a_1, \ldots, a_r) \in G$, *ist ein Isomorphismus.*

Beweis. 1. Nach Definition.

2. Definiere $\varphi \colon G \to G_1/N_1 \times \ldots \times G_r/N_r$ durch $\varphi(a_1, \ldots, a_r) = (a_1N_1, \ldots, a_rN_r)$. Dann ist φ ein Epimorphismus, $\mathrm{Ker}(\varphi) = N_1 \times \ldots \times N_r \lhd G$, und die Behauptung folgt aus Satz 2.5.7. □

Definition und Satz 4.1.2 (Innere direkte Produkte)**.** *Sei* G *eine Gruppe,* $r \in \mathbb{N}$, *und für jedes* $j \in [1, r]$ *sei* $G_j \lhd G$. *Dann ist*

$$G_1 \cdot \ldots \cdot G_r = \{\, a_1 \cdot \ldots \cdot a_r \mid (a_1, \ldots, a_r) \in G_1 \times \ldots \times G_r \,\} \lhd G$$

und man nennt $G_1 \cdot \ldots \cdot G_r$ das *Produkt* der Normalteiler $G_1, \ldots, G_r$.

Die folgenden Aussagen sind äquivalent:

(a) *Die Abbildung*

$$\varphi \colon G_1 \times \ldots \times G_r \to G_1 \cdot \ldots \cdot G_r\,, \quad \text{definiert durch} \quad \varphi(a_1, \ldots, a_r) = a_1 \cdot \ldots \cdot a_r\,,$$

ist ein Gruppenisomorphismus.

(b) *Jedes* $a \in G_1 \cdot \ldots \cdot G_r$ *hat eine eindeutige Darstellung als Produkt* $a = a_1 \cdot \ldots \cdot a_r$ *mit* $(a_1, \ldots, a_r) \in G_1 \times \ldots \times G_r$.

(c) *Für jedes* $j \in [1, r]$ *ist* $G_j \cap (G_1 \cdot \ldots \cdot G_{j-1} \cdot G_{j+1} \cdot \ldots \cdot G_r) = \{e\}$.

Sind diese Bedingungen erfüllt, so sagt man, das Produkt aus $G_1, \ldots, G_r$ ist *direkt*. Ist $G = G_1 \cdot \ldots \cdot G_r$, so nennt man G das (*innere*) *direkte Produkt* von $G_1, \ldots, G_r$ und schreibt $G = G_1 \cdot \ldots \cdot G_r$ (dir).

Ist G eine additive geschriebene abelsche Gruppe, so wird das innere direkte Produkt von aus $G_1, \ldots, G_r$ auch als *direkte Summe* bezeichnet, und man schreibt

$$\bigoplus_{i=1}^{r} G_i = G_1 \oplus \ldots \oplus G_r \qquad \text{an Stelle von} \qquad G_1 + \ldots + G_r \text{ (dir)}\,.$$

BEWEIS. Wir zeigen zuerst durch Induktion nach r, dass $G_1 \cdot \ldots \cdot G_r \lhd G$. Für $r = 1$ ist nichts zu zeigen.

$r \geq 2\,,\ r-1 \to r$ Sei $G' = G_1 \cdot \ldots \cdot G_{r-1}$, also $G' \lhd G$ nach Induktionsvoraussetzung. Nach Satz 2.5.8 ist $G'G_r < G$, und für $x \in G$ ist $xG'G_r = G'xG_r = G'G_rx$, also ist $G'G_r = G_1 \cdot \ldots \cdot G_r \lhd G$.

(a) $\Rightarrow$ (b) Das folgt aus der Bijektivität von φ.

(b) $\Rightarrow$ (c) Sei $j \in [1,r]$ und $a_j \in G_j \cap (G_1 \cdot \ldots \cdot G_{j-1} \cdot G_{j+1} \cdot \ldots \cdot G_r)$. Dann ist

$$a_j = e \cdot \ldots \cdot e\, a_j\, e \cdot \ldots \cdot e \;=\; a_1 \cdot \ldots \cdot a_{j-1}\, e\, a_{j+1} \cdot \ldots \cdot a_r \quad \text{mit} \quad a_i \in G_i \ \text{ für alle } \ i \in [1,r] \setminus \{j\}\,,$$

und daher folgt $a_j = e$ wegen der Eindeutigkeit der Produktdarstellung.

(c) $\Rightarrow$ (a) Nach Definition ist φ eine surjektive Abbildung. Um φ als Gruppenhomomorphismus nachzuweisen, müssen wir zeigen:

Für alle $(a_1,\ldots,a_r), (b_1,\ldots,b_r) \in G_1 \times \ldots \times G_r$ ist $a_1b_1 \cdot \ldots \cdot a_rb_r = (a_1 \cdot \ldots \cdot a_r)(b_1 \cdot \ldots \cdot b_r)$.

Wir beweisen das mittels Induktion nach r. Für $r = 1$ ist nichts zu zeigen.

$r \geq 2\,,\ r-1 \to r$: Seien $(a_1,\ldots,a_r), (b_1,\ldots,b_r) \in G_1 \times \ldots \times G_r$, $G' = G_1 \cdot \ldots \cdot G_{r-1} \lhd G$ und $b' = b_1 \cdot \ldots \cdot b_{r-1} \in G'$. Nach Induktionsvoraussetzung ist $a_1b_1 \cdot \ldots \cdot a_rb_r = a_1 \cdot \ldots \cdot a_r(a_r^{-1}b'a_rb'^{-1})b_1 \cdot \ldots \cdot b_r$. Wegen $a_r^{-1}b'a_r \in a_r^{-1}G'a_r = G'$ ist auch $a_r^{-1}b'a_rb'^{-1} \in G'$, und wegen $b'a_rb'^{-1} \in b'G_rb'^{-1} = G_r$ ist auch $a_r^{-1}b'a_rb'^{-1} \in G_r$. Nach Voraussetzung ist $G' \cap G_r = \{e\}$, also $a_r^{-1}b'a_rb'^{-1} = e$ und daher $a_1b_1 \cdot \ldots \cdot a_rb_r = (a_1 \cdot \ldots \cdot a_r)(b_1 \cdot \ldots \cdot b_r)$.

Für den Nachweis der Injektivität von φ sei $(a_1,\ldots,a_r) \in \mathrm{Ker}(\varphi)$ und $j \in [1,r]$. Aus $a_1 \cdot \ldots \cdot a_r = e$ folgt dann $a_j = (a_1 \cdot \ldots \cdot a_{j-1})^{-1}(a_{j+1} \cdot \ldots \cdot a_r)^{-1} \in G_j \cap (G_1 \cdot \ldots \cdot G_{j-1} \cdot G_{j+1} \cdot \ldots \cdot G_r) = \{e\}$. □

Korollar 4.1.3. *Sei $r \in \mathbb{N}$, für jedes $j \in [1,r]$ sei G_j eine Gruppe mit neutralem Element e_j, und es sei $G'_j = \{e_1\} \times \ldots \times \{e_{j-1}\} \times G_j \times \{e_{j+1}\} \times \ldots \times \{e_r\}$. Für alle $j \in [1,r]$ ist dann $G_j \cong G'_j$, $G'_j \lhd G_1 \times \ldots \times G_r$, und $G_1 \times \ldots \times G_r = G'_1 \cdot \ldots \cdot G'_r$ (dir).*

BEWEIS. Für $j \in [1,r]$ ist offensichtlich $G'_j \cong G_j$, und nach Satz 4.1.1.2 ist $G'_j \lhd G_1 \times \ldots \times G_r$. Für $(a_1,\ldots,a_r) \in G_1 \times \ldots \times G_r$ ist

$$(a_1,\ldots,a_r) \;=\; \prod_{i=1}^{r} (e_1,\ldots,e_{i-1},a_i,e_{i+1},\ldots,e_r) \;\in\; G'_1 \cdot \ldots \cdot G'_r\,,$$

und diese Darstellung ist eindeutig. Daher ist $G_1 \times \ldots \times G_r = G'_1 \cdot \ldots \cdot G'_r$ (dir) nach Satz 4.1.2. □

Satz 4.1.4. *Sei $n \in \mathbb{N}$, seien $R_1,\ldots,R_n$ Ringe und $R = R_1 \times \ldots \times R_n$ ihr direktes Produkt.*

1. *Für $j \in [1,n]$ hat die Projektion $p_j\colon R \to R_j$ den Kern*
$$\mathrm{Ker}(p_j) \;=\; R_1 \times \ldots \times R_{j-1} \times \{0_{R_j}\} \times R_{j+1} \times \ldots \times R_n \;\lhd R\,.$$
2. *Für jedes $j \in [1,n]$ sei $I_j \lhd R_j$, und es sei $I = I_1 \times \ldots \times I_n$. Dann ist $I \lhd R$, und*
$$\phi\colon R/I \;\to\; R_1/I_1 \times \ldots \times R_n/I_n\,, \quad \text{definiert durch} \quad (a_1,\ldots,a_n) + I \mapsto (a_1+I_1,\ldots,a_n+I_n)$$
für alle $(a_1,\ldots,a_n) \in R$, ist ein Isomorphismus.

BEWEIS. Wie Satz 4.1.1. □

Satz 4.1.5. *Sei R ein kommutativer Ring, $r \in \mathbb{N}$, seien $I_1,\ldots,I_r$ Ideale von R und $I = I_1 \cdot \ldots \cdot I_r$.*

1. *Sei $J \lhd R$, und sei $I_i + J = R$ für alle $i \in [1,r]$. Dann ist auch $I + J = R$.*
2. *Sei $I_i + I_j = R$ für alle $i, j \in [1,r]$ mit $i \neq j$. Dann ist $I = I_1 \cap \ldots \cap I_r$, und die Abbildung*
$$\phi\colon R/I \;\to\; R/I_1 \times \ldots \times R/I_r\,, \quad \text{definiert durch } \ \phi(a+I) = (a+I_1,\ldots,a+I_r) \ \text{ für alle } \ a \in R\,,$$
ist ein Ringisomorphismus.

BEWEIS. 1. Für $i \in [1,r]$ sei $a_i \in I_i$ und $b_i \in J$ mit $a_i + b_i = 1$. Dann folgt

$$1 = \prod_{i=1}^{r}(a_i + b_i) = a_1 \cdot \ldots \cdot a_r + b \quad \text{mit} \quad b \in J\,,$$

und daher folgt $I + J = R$.

2. Wir zeigen zuerst die Gleichheit $I_1 \cdot \ldots \cdot I_r = I_1 \cap \ldots \cap I_r$ durch Induktion nach r. Für $r = 1$ ist nichts zu zeigen.

$r \geq 2\,,\ r-1 \to r$: Nach Satz 3.4.9.1 ist $I_1 \cdot \ldots \cdot I_r \subset I_1 \cap \ldots \cap I_r$, nach Induktionsvoraussetzung ist $I_1 \cap \ldots \cap I_r = I_1 \cdot \ldots \cdot I_{r-1} \cap I_r$, und nach 1. ist $I_1 \cdot \ldots \cdot I_{r-1} + I_r = R$ und daher $1 = b + c$ mit $b \in I_1 \cdot \ldots \cdot I_{r-1}$ und $c \in I_r$. Ist nun $a \in I_1 \cap \ldots \cap I_r$, so folgt $a = ab + ac \in I_1 \cdot \ldots \cdot I_r$.

Sei nun $f\colon R \to R/I_1 \times \ldots \times R/I_r$ definiert durch $f(a) = (a + I_1, \ldots, a + I_r)$ für alle $a \in R$. Dann ist f ein Ringhomomorphismus, $\mathrm{Ker}(f) = I_1 \cap \ldots \cap I_r = I$, und nach Satz 3.2.9.3 induziert f einen Ringmonomorphismus $\phi\colon R/I \to R/I_1 \times \ldots \times R/I_r$ mit $\phi(a + I) = (a + I_1, \ldots, a + I_r)$ für alle $a \in R$. Wir müssen zeigen, dass ϕ surjektiv ist. Seien dazu $a_1, \ldots, a_r \in R$. Für alle $i \in [1,r]$ ist $I_1 \cdot \ldots \cdot I_{i-1} \cdot I_{i+1} \cdot \ldots \cdot I_r + I_i = R$, also $1 = d_i + e_i$ mit $d_i \in I_1 \cdot \ldots \cdot I_{i-1} \cdot I_{i+1} \cdot \ldots \cdot I_r$, $e_i \in I_i$, und wir setzen $a = a_1 d_1 + \ldots + a_r d_r \in R$. Dann ist $a_i d_i + I_i = a_i - a_i e_i + I_i = a_i + I_i$ und $a_i d_i \in I_j$ für alle $i, j \in [1,r]$ mit $i \neq j$. Daraus folgt $a + I_i = a_i + I_i$ für alle $i \in [1,r]$, also $\phi(a + I) = (a_1 + I_1, \ldots, a_r + I_r)$. □

Korollar 4.1.6 (Chinesischer Restsatz)**.** *Seien $r, m_1, \ldots, m_r \in \mathbb{N}$, $m = m_1 \cdot \ldots \cdot m_r$, und sei $\mathrm{ggT}(m_i, m_j) = 1$ für alle $i, j \in [1,r]$ mit $i \neq j$. Dann ist $m = \mathrm{kgV}(m_1, \ldots, m_r)$, und es gilt:*

1. *Die Abbildung*

$$\phi\colon \mathbb{Z}/m\mathbb{Z} \to \mathbb{Z}/m_1\mathbb{Z} \times \ldots \times \mathbb{Z}/m_r\mathbb{Z}\,, \quad \textit{definiert durch} \quad \phi(a + m\mathbb{Z}) = (a + m_1\mathbb{Z}, \ldots, a + m_r\mathbb{Z})\,,$$

   ist ein Ringisomorphismus.

2. *Seien $a_1, \ldots, a_r \in \mathbb{Z}$. Dann gibt es ein $a \in \mathbb{Z}$, so dass $a \equiv a_i \bmod m_i$ für alle $i \in [1,r]$, und die Restklasse $a + m\mathbb{Z}$ ist durch $a_1, \ldots, a_r$ eindeutig bestimmt. Insbesondere gilt: Sind $a, b \in \mathbb{Z}$ und ist $a \equiv b \bmod m_i$ für alle $i \in [1,r]$, so folgt $a \equiv b \bmod m$.*

BEWEIS. Nach Satz 2.2.5 ist genau dann $\mathrm{ggT}(m_i, m_j) = 1$, wenn $m_i\mathbb{Z} + m_j\mathbb{Z} = \mathbb{Z}$; und genau dann ist $m = \mathrm{kgV}(m_1, \ldots, m_r)$, wenn $m\mathbb{Z} = m_1\mathbb{Z} \cap \ldots \cap m_r\mathbb{Z}$. Für $a, b \in \mathbb{Z}$ und $d \in \mathbb{N}$ ist außerdem genau dann $a \equiv b \bmod d$, wenn $a + d\mathbb{Z} = b + d\mathbb{Z}$. Daher folgen die Behauptungen aus Satz 4.1.5. □

4.2. Struktur endlicher abelscher Gruppen

Definition 4.2.1. Sei G eine Gruppe, $p \in \mathbb{P}$ und $G_p = \{g \in G \mid \mathrm{ord}(g) \text{ ist eine } p\text{-Potenz}\}$.

1. G heißt *p-Gruppe*, wenn die $G = G_p$.
2. Eine Untergruppe $H < G$ heißt *p-Sylow-Gruppe* von G, wenn H eine maximale p-Untergruppe von H ist [explizit: H ist eine p-Gruppe und für jede p-Gruppe H' mit $H \subset H' \subset G$ ist $H = H'$].

Lemma 4.2.2. *Sei G eine abelsche Gruppe, $r \in \mathbb{N}$, seien $g_1, \ldots, g_r \in G$ und $g = g_1 \cdot \ldots \cdot g_r$. Für $i \in [1,r]$ sei $m_i = \mathrm{ord}(g_i) \in \mathbb{N}$, und es sei $m = \mathrm{kgV}(m_1, \ldots, m_r)$. Dann ist $\mathrm{ord}(g) \mid m$. Ist $\mathrm{ggT}(m_i, m_j) = 1$ für alle $i, j \in [1,r]$ mit $i \neq j$, so ist $\mathrm{ord}(g) = m = m_1 \cdot \ldots \cdot m_r$.*

BEWEIS. Offensichtlich ist $g^m = e$, also $\mathrm{ord}(g) \mid m$. Sei nun $\mathrm{ggT}(m_i, m_j) = 1$ für alle $i, j \in [1,r]$ mit $i \neq j$. Wir müssen zeigen: Ist $n \in \mathbb{N}$ mit $g^n = e$, so folgt $m_i \mid n$ für alle $i \in [1,r]$ (denn dann ist auch $m \mid n$).

Sei $n \in \mathbb{N}$ mit $g^n = e$ und $i \in [1,r]$. Nach Korollar 4.1.6 ist $m = m_1 \cdot \ldots \cdot m_r$, und es gibt ein $l \in \mathbb{N}$ mit $l \equiv 1 \bmod m_i$ und $l \equiv 0 \bmod m_j$ für alle $j \in [1,r] \setminus \{i\}$. Mit Satz 2.2.10.2 folgt

$$e = g^{nl} = g_i^{nl} = g_i^n, \quad \text{also } m_i \mid n.$$

□

Satz 4.2.3. *Sei G eine abelsche Torsionsgruppe.*

1. *Für jedes $p \in \mathbb{P}$ ist G_p die einzige p-Sylow-Gruppe von G.*
2. *Sei $\exp(G) = n = p_1^{d_1} \cdot \ldots \cdot p_r^{d_r} \in \mathbb{N}$ mit n, r, $d_1, \ldots, d_r \in \mathbb{N}$ und verschiedenen Primzahlen $p_1, \ldots, p_r \in \mathbb{P}$. Dann gilt:*
   (a) $G = G_{p_1} \cdot \ldots \cdot G_{p_r}$ (dir), *und für alle $i \in [1,r]$ gibt es ein $g_i \in G_{p_i}$ mit $\operatorname{ord}(g_i) = p_i^{d_i}$.*
   (b) *Es gibt ein $g \in G$ mit $\operatorname{ord}(g) = n$ (und daher $\operatorname{ord}(g^d) = n/d$ für jedes $d \in \mathbb{N}$ mit $d \mid n$).*
   (c) *Ist $g \in G$ mit $\operatorname{ord}(g) = n$, so gibt es eine Untergruppe $H < G$, so dass $G = H\langle g\rangle$ (dir).*

Beweis. 1. Sei $p \in \mathbb{P}$. Es genügt, zu zeigen, dass G_p eine Untergruppe von G ist. Seien a, $b \in G_p$. Dann ist $\operatorname{ord}(ab^{-1})$ eine p-Potenz nach Lemma 4.2.2, also $ab^{-1} \in G_p$. Nach Satz 2.2.2 folgt $G_p < G$.

2.(a) Für $i \in [1,r]$ sei $q_i = p_1^{d_1} \cdot \ldots \cdot p_{i-1}^{d_{i-1}} p_{i+1}^{d_{i+1}} \cdot \ldots \cdot p_r^{d_r}$. Dann ist $\operatorname{ggT}(q_1, \ldots, q_r) = 1$, und nach Satz 2.2.5.4 gibt es $k_1, \ldots, k_r \in \mathbb{Z}$ mit $k_1 q_1 + \ldots + k_r q_r = 1$. Für $g \in G$ ist dann $g = g^{k_1 q_1} \cdot \ldots \cdot g^{k_r q_r}$, und für alle $i \in [1,r]$ ist $(g^{k_i q_i})^{p^{d_i}} = e$, also $g^{k_i q_i} \in G_{p_i}$, und es folgt $G = G_{p_1} \cdot \ldots \cdot G_{p_r}$.

Ist nun $i \in [1,r]$ und $g \in G_{p_i} \cap G_{p_1} \cdot \ldots \cdot G_{p_{i-1}} \cdot G_{p_{i+1}} \cdot \ldots \cdot G_{p_r}$, so ist einerseits $\operatorname{ord}(g)$ eine p_i-Potenz, aber anderseits nach Lemma 4.2.2 ein Teiler einer Potenz von $p_1 \cdot \ldots \cdot p_{i-1} p_{i+1} \cdot \ldots \cdot p_r$. Daher ist $\operatorname{ord}(g) = 1$, also $g = e$, und das Produkt der G_{p_i} ist direkt nach Satz 4.1.2.

Nach Definition ist $\exp(G_{p_i}) = \operatorname{kgV}\big(\{\operatorname{ord}(g) \mid g \in G_{p_i}\}\big) = p_i^{d_i'}$ mit $d_i' \in [0, d_i]$, und daher gibt es ein $g_i \in G_{p_i}$ mit $\operatorname{ord}(g_i) = p_i^{d_i'}$. Ist nun $g' \in G$, $g' = g_1' \cdot \ldots \cdot g_r'$ mit $g_i' \in G_{p_i}$ für alle $i \in [1,r]$, so folgt $\operatorname{ord}(g') = \operatorname{ord}(g_1') \cdot \ldots \cdot \operatorname{ord}(g_r') \mid p_1^{d_1'} \cdot \ldots \cdot p_r^{d_r'}$ und daher $\exp(G) \mid p_1^{d_1'} \cdot \ldots \cdot p_r^{d_r'}$, also $d_i' = d_i$ für alle $i \in [1,r]$.

2.(b) Ist $g_i \in G_{p_i}$ mit $\operatorname{ord}(g_i) = p^{d_i}$, so folgt $\operatorname{ord}(g_1 \cdot \ldots \cdot g_r) = n$.

2.(c) Sei $g \in G$ mit $\operatorname{ord}(g) = n$, und sei Ω die Menge aller Untergruppen $U < G$ mit $U \cap \langle g\rangle = \{e\}$. Dann ist $\Omega \neq \emptyset$, und die Vereinigung jeder Kette in Ω gehört zu Ω. Daher besitzt Ω ein maximales Element $H < G$. Wegen $H \cap \langle g\rangle = \{e\}$ genügt es nun, $G = H\langle g\rangle$ zu zeigen.

Wir nehmen an, es sei $H\langle g\rangle \subsetneq G$, und es sei $x \in G \setminus H\langle g\rangle$ ein Element minimaler Ordnung. Ist $p \in \mathbb{P}$ mit $p \mid \operatorname{ord}(x)$, so ist $\operatorname{ord}(x^p) < \operatorname{ord}(x)$ und daher $x^p \in H\langle g\rangle$. Sei $x^p = hg^l$ mit $h \in H$ und $l \in \mathbb{N}$, und sei $\operatorname{ord}(g) = n = p^\nu m$ mit ν, $m \in \mathbb{N}$ und $p \nmid m$. Dann folgt $e = x^n = h^{p^{\nu-1}m} g^{p^{\nu-1}lm}$ und daher $l = pj$ mit $j \in \mathbb{N}$. Es ist $(xg^{-j})^p = h \in H$, und wegen $x \notin H\langle g\rangle$ ist $xg^{-j} \notin H$. Aus der Maximalität von H folgt nun $\langle H \cup \{xg^{-j}\}\rangle \cap \langle g\rangle \neq \{e\}$. Daher besteht eine Relation $h_1 (xg^{-j})^u = g^k \neq e$ mit $h_1 \in H$ und u, $k \in \mathbb{N}$, und wir erhalten $x^u = h_1^{-1} g^{ju+k} \in H\langle g\rangle$. Wäre nun $p \mid u$, etwa $u = pv$ mit $v \in \mathbb{N}$, so folgte $(xg^{-j})^u = h^v \in H$ und daher $g^k \in H$, ein Widerspruch. Daher ist $p \nmid u$, also $\operatorname{ggT}(p,u) = 1$, und es gibt s, $t \in \mathbb{N}$ mit $ps + ut = 1$. Damit folgt $x = (x^u)^t (x^p)^s \in H\langle g\rangle$, ein Widerspruch! □

Satz 4.2.4 (Hauptsatz über endliche abelsche Gruppen)**.** *Sei G eine endliche abelsche Gruppe und $|G| > 1$.*

1. *Es existieren genau ein $r \in \mathbb{N}$ und eineutig bestimmte $d_1, \ldots, d_r \in \mathbb{N}$ mit $1 < d_1 \mid d_2 \mid \ldots \mid d_r$, so dass $G \cong \mathbb{Z}/d_1\mathbb{Z} \times \ldots \times \mathbb{Z}/d_r\mathbb{Z}$.*

   Insbesondere existieren $g_1, \ldots, g_r \in G$, so dass $G = \langle g_1\rangle \cdot \ldots \cdot \langle g_r\rangle$ (dir) und $\operatorname{ord}(g_i) = d_i$ für alle $i \in [1,r]$, $d_r = \exp(G)$, und G ist genau dann zyklisch, wenn $\exp(G) = |G|$.

2. *Es existiert genau ein* $s \in \mathbb{N}$*, eindeutig bestimmte Primzahlen* $p_1, \ldots, p_s$ *und für jedes* $j \in [1,s]$ *eindeutig bestimmte Zahlen* $r_j, n_{j,1}, \ldots, n_{j,r_j} \in \mathbb{N}$*, so dass*

$$G \cong \prod_{j=1}^{s} G_{p_j}\,, \quad \text{und} \quad G_{p_j} \cong \prod_{\nu=1}^{r_j} \mathbb{Z}/p_j^{n_{j,\nu}}\mathbb{Z} \quad \text{für alle} \quad j \in [1,s]\,.$$

BEWEIS. Induktion nach $|G|$. Sei die Behauptung für alle Gruppen G' mit $|G'| < |G|$ gezeigt.

1. EXISTENZ: Nach Satz 4.2.3.2 gibt es ein Element $g \in G$ mit $\mathrm{ord}(g) = d = \exp(G)$ und eine Untergruppe $H < G$, so dass $G = H\langle g\rangle$ (dir). Dann ist $|H| < |G|$, und im Falle $|H| = 1$ sind wir fertig. Ist $|H| > 1$, so gibt es nach Induktionsvoraussetzung ein $r \in \mathbb{N}_{\geq 2}$, $d_1, \ldots, d_{r-1} \in \mathbb{N}$ mit $1 < d_1 \,|\, d_2 \,|\, \ldots \,|\, d_{r-1}$ und $g_1, \ldots, g_{r-1} \in G$, so dass $\mathrm{ord}(g_i) = d_i$ für alle $i \in [1, r-1]$ und $H = \langle g_1\rangle \cdot \ldots \cdot \langle g_{r-1}\rangle$ (dir). Dann folgt $d_{r-1} \,|\, d$ und $G = \langle g_1\rangle \cdot \ldots \cdot \langle g_{r-1}\rangle \cdot \langle g_r\rangle$.

2. EINDEUTIGKEIT: Für eine Primzahl $p \in \mathbb{P}$ sei $G^p = \{g^p \mid g \in G\}$. Dann ist $G^p < G$, und für alle $g \in G$ mit $\mathrm{ord}(g) = d \in \mathbb{N}$ ist

$$(\langle g\rangle : \langle g^p\rangle) = \frac{\mathrm{ord}(g)}{\mathrm{ord}(g^p)} = \mathrm{ggT}(d,p) = \begin{cases} p\,, & \text{falls} \quad p \,|\, d\,, \\ 1\,, & \text{falls} \quad p \nmid d\,. \end{cases}$$

Seien nun $r, s, d_1, \ldots, d_r, d'_1, \ldots, d'_s \in \mathbb{N}$ und $g_1, \ldots, g_r, g'_1, \ldots, g'_s \in G$, so dass $1 < d_1 \,|\, d_2 \,|\, \ldots \,|\, d_r$, $1 < d'_1 \,|\, d'_2 \,|\, \ldots \,|\, d'_s$, $G = \langle g_1\rangle \cdot \ldots \cdot \langle g_r\rangle$ (dir), $G = \langle g'_1\rangle \cdot \ldots \cdot \langle g'_s\rangle$ (dir), $\mathrm{ord}(g_i) = d_i$ für alle $i \in [1,r]$ und $\mathrm{ord}(g'_j) = d'_j$ für alle $j \in [1,s]$. Damit folgt $|G| = d_1 \cdot \ldots \cdot d_r = d'_1 \cdot \ldots \cdot d'_s$. Für $p \in \mathbb{P}$ ist

$$G^p = \langle g_1^p\rangle \cdot \ldots \cdot \langle g_r^p\rangle \text{ (dir)} \quad \text{und} \quad G^p = \langle g_1'^p\rangle \cdot \ldots \cdot \langle g_s'^p\rangle \text{ (dir)}$$

und daher

$$|G^p| = \prod_{i=1}^{r} \frac{d_i}{\mathrm{ggT}(p,d_i)} = \prod_{j=1}^{s} \frac{d'_j}{\mathrm{ggT}(p,d'_j)}\,, \quad \text{also} \quad \big|\{i \in [1,r] \;\big|\; p \,|\, d_i\}\big| = \big|\{j \in [1,s] \;\big|\; p \,|\, d'_j\}\big| \leq \min\{r,s\}\,.$$

Ist $p \,|\, d_1$, so folgt $r = \big|\{i \in [1,r] \;\big|\; p \,|\, d_i\}\big| \leq s$. Ist $p \,|\, d'_1$, so folgt $s = \big|\{j \in [1,s] \;\big|\; p \,|\, d'_j\}\big| \leq r$. Also ist $r = s$, und für $p \in P$ ist genau dann $p \,|\, d_1$, wenn $p \,|\, d'_1$.

Sei nun $p \in \mathbb{P}$ mit $p \,|\, d_1$, und seien $\rho, \sigma \in [0,r]$, so dass $d_i = d'_j = p$ für alle $i \in [1,\rho]$ und $j \in [1,\sigma]$, $d_i \neq p$ für alle $i \in [\rho+1, r]$ und $d'_j \neq p$ für alle $j \in [\sigma+1, r]$. Dann ist

$$G^p = \langle g_{\rho+1}^p\rangle \cdot \ldots \cdot \langle g_r^p\rangle \text{ (dir)} \quad \text{und} \quad G^p = \langle g_{\sigma+1}'^p\rangle \cdot \ldots \cdot \langle g_r'^p\rangle \text{ (dir)}\,,$$

$1 < \mathrm{ord}(g_{\rho+1}^p) \,|\, \ldots \,|\, \mathrm{ord}(g_r^p)$ und $1 < \mathrm{ord}(g_{\sigma+1}'^p) \,|\, \ldots \,|\, \mathrm{ord}(g_s'^p)$. Nach Induktionsvoraussetzung folgt $\rho = \sigma$, also $d_i = d'_i = p$ für alle $i \in [1,\rho]$, und

$$\frac{d_i}{p} = \mathrm{ord}(g_i^p) = \mathrm{ord}(g_i'^p) = \frac{d'_i}{p} \quad \text{für alle} \quad i \in [\rho+1, r]\ ,$$

also $d_i = d'_i$ für alle $i \in [1,r]$.

2. Nach 1. und Satz 4.2.3.2(a). □

Satz 4.2.5. *Sei* K *ein Körper und* $G < K^\times$ *eine endliche Untergruppe. Dann ist* G *zyklisch.*

BEWEIS. Sei $d = \exp(G)$. Dann ist jedes $a \in G$ eine Nullstelle des Polynoms $X^d - 1$. Aus Satz 3.6.7 folgt $|G| \leq d$, und daher ist G zyklisch nach Satz 4.2.4. □

4.3. Prime Restklassen

Lemma 4.3.1. *Seien* $m, n \in \mathbb{N}$.

1. *Seien* $a, b \in \mathbb{Z}$ *und* $a \equiv b \bmod m$. *Dann ist* $\operatorname{ggT}(a,m) = \operatorname{ggT}(b,m)$.
2. $(\mathbb{Z}/m\mathbb{Z})^\times = \{k+m\mathbb{Z} \mid k \in \mathbb{Z},\ \operatorname{ggT}(k,m)=1\}$, *und es gibt genau einen (im Folgenden kanonisch genannten) Epimorphismus*

$$\omega\colon (\mathbb{Z}/mn\mathbb{Z})^\times \to (\mathbb{Z}/m\mathbb{Z})^\times \quad \text{mit} \quad \omega(a+mn\mathbb{Z}) = a+m\mathbb{Z} \quad \text{für alle } a\in\mathbb{Z} \text{ mit } \operatorname{ggT}(a,mn)=1\,.$$

Es ist $\operatorname{Ker}(\omega) = \{a+mn\mathbb{Z} \mid a\in\mathbb{Z},\ \operatorname{ggT}(a,mn)=1,\ a\equiv 1 \bmod m\}$.

Beweis. 1. Mit Satz 1.1.6.4. Seien $a, b \in \mathbb{Z}$ mit $a \equiv b \bmod m$ und $d = \operatorname{ggT}(a,m)$. Dann ist $d \mid a$, $d \mid m$ und $d = ax + my$ mit $x, y \in \mathbb{Z}$. Ist $a = b + mk$ mit $k \in \mathbb{Z}$, so folgt $d \mid b$ und $d = bx + m(y + kx)$, also $d = \operatorname{ggT}(b,m)$.

2. Nach Satz 3.2.8.2 ist $(\mathbb{Z}/m\mathbb{Z})^\times = \{k + m\mathbb{Z} \mid k \in [1,m],\ \operatorname{ggT}(k,m) = 1\}$. Zu jedem $k \in \mathbb{Z}$ gibt es genau ein $k_0 \in [1,m]$ mit $k \equiv k_0 \bmod m$, es ist dann $k + m\mathbb{Z} = k_0 + m\mathbb{Z}$, und nach 1. ist $\operatorname{ggT}(k,m) = \operatorname{ggT}(k_0,m)$. Daher folgt $(\mathbb{Z}/m\mathbb{Z})^\times = \{k + m\mathbb{Z} \mid k \in \mathbb{Z},\ \operatorname{ggT}(k,m) = 1\}$.

Für den Restklassenepimorphismus $\rho\colon \mathbb{Z} \to \mathbb{Z}/m\mathbb{Z}$ ist $mn\mathbb{Z} \subset \operatorname{Ker}(\rho)$. Daher induziert ρ nach Satz 3.2.9.2 einen Ringepimorphismus $\mathbb{Z}/mn\mathbb{Z} \to \mathbb{Z}/m\mathbb{Z}$ und daher einen Gruppenhomomorphismus $\omega\colon (\mathbb{Z}/mn\mathbb{Z})^\times \to (\mathbb{Z}/m\mathbb{Z})^\times$, so dass $\omega(a + mn\mathbb{Z}) = a + m\mathbb{Z}$ für alle $a \in \mathbb{Z}$ mit $\operatorname{ggT}(a,mn) = 1$.

Offensichtlich ist $\operatorname{Ker}(\omega) = \{a + mn\mathbb{Z} \mid a \in \mathbb{Z},\ \operatorname{ggT}(a,mn) = 1,\ a \equiv 1 \bmod m\}$, und es bleibt die Surjektivität von ω zu zeigen. Sei dazu $k_0 + m\mathbb{Z} \in (\mathbb{Z}/m\mathbb{Z})^\times$ mit $k_0 \in [1,m]$ und $\operatorname{ggT}(k_0,m) = 1$. Sei $\{p_1,\ldots,p_s\} = \{p \in \mathbb{P} \mid p \mid n,\ p \nmid m\}$ und $q = p_1 \cdot \ldots \cdot p_s$. Dann ist $\operatorname{ggT}(q,m) = 1$, und nach Satz 2.3.6 gibt es ein $r \in \mathbb{Z}$ mit $mr \equiv 1 - k_0 \bmod q$. Sei nun $k = k_0 + mr$. Dann ist $k + m\mathbb{Z} = k_0 + m\mathbb{Z}$, und wir zeigen $\operatorname{ggT}(k,mn) = 1$. Dazu genügt es, zu zeigen: Ist $p \in \mathbb{P}$ und $p \mid mn$, so ist $p \nmid k$. Sei $p \in \mathbb{P}$ und $p \mid mn$, also $p \mid m$ oder $p \mid n$. Ist $p \mid m$, so ist $p \nmid k_0$ und daher $p \nmid k$. Ist $p \mid n$ und $p \nmid m$, so ist $p \mid q \mid k_0 + mr - 1 = k - 1$ und daher $p \nmid k$. □

Definition 4.3.2. Sei $m \in \mathbb{N}$.

1. Die Gruppe $(\mathbb{Z}/m\mathbb{Z})^\times$ heißt *prime Restklassengruppe* modulo m.
2. Sei $a \in \mathbb{Z}$ und $\operatorname{ggT}(a,m) = 1$. Dann heißt $\operatorname{ord}_m(a) = \operatorname{ord}_{(\mathbb{Z}/m\mathbb{Z})^\times}(a + m\mathbb{Z})$ die *Ordnung* von a modulo m.
3. Die Funktion $\varphi\colon \mathbb{N} \to \mathbb{N}$, definiert durch $\varphi(m) = |(\mathbb{Z}/m\mathbb{Z})^\times|$, heißt *Euler'sche Phi-Funktion*.

Satz 4.3.3. *Sei* $m \in \mathbb{N}$.

1. *Es ist* $\varphi(m) = |\{k \in [1,m] \mid \operatorname{ggT}(k,m) = 1\}|$, *und*

$$m = \sum_{1 \le d \mid m} \varphi(d)\,.$$

2. *Für* $p \in \mathbb{P}$ *und* $e \in \mathbb{N}$ *ist* $\varphi(p^e) = p^{e-1}(p-1)$.
3. *Sei* $m = p_1^{e_1} \cdot \ldots \cdot p_r^{e_r} \in \mathbb{N}$ *mit* $r \in \mathbb{N}_0$, *verschiedenen Primzahlen* $p_1,\ldots,p_r$ *und* $e_1,\ldots,e_r \in \mathbb{N}$. *Dann ist die Abbildung*

$$\psi\colon (\mathbb{Z}/m\mathbb{Z})^\times \to (\mathbb{Z}/p_1^{e_1}\mathbb{Z})^\times \times \ldots \times (\mathbb{Z}/p_r^{e_r}\mathbb{Z})^\times\,,$$

definiert durch $\psi(a + m\mathbb{Z}) = (a + p_1^{e_1}\mathbb{Z}, \ldots, a + p_r^{e_r}\mathbb{Z})$ *für alle* $a \in \mathbb{Z}$ *mit* $\operatorname{ggT}(a,m) = 1$, *ein Isomorphismus, und*

$$\varphi(m) = \prod_{i=1}^{r} \varphi(p_i^{e_i}) = \prod_{i=1}^{r} p_i^{e_i-1}(p_i - 1)\,.$$

4. *Für alle* $m_1, m_2 \in \mathbb{N}$ *mit* $\operatorname{ggT}(m_1, m_2) = 1$ *ist* $(\mathbb{Z}/m_1m_2\mathbb{Z})^\times \cong (\mathbb{Z}/m_1\mathbb{Z})^\times \times (\mathbb{Z}/m_2\mathbb{Z})^\times$ *und* $\varphi(m_1m_2) = \varphi(m_1)\varphi(m_2)$.

BEWEIS. 1. Nach Satz 3.2.8.2 ist $(\mathbb{Z}/m\mathbb{Z})^\times = \{k + m\mathbb{Z} \mid k \in [1, m] \ \operatorname{ggT}(k, m) = 1\}$ und daher $\varphi(m) = |\{k \in [1, m] \mid \operatorname{ggT}(k, m) = 1\}|$.

Sei nun $m = dd'$ mit $d, d' \in \mathbb{N}$, und sei $l \in [1, d]$ mit $\operatorname{ggT}(l, d) = 1$. Dann ist $ld' \in [1, m]$ und $\operatorname{ggT}(ld', m) = \operatorname{ggT}(ld', dd') = d'$. Ist umgekehrt $k \in [1, m]$ mit $\operatorname{ggT}(k, m) = d'$, so folgt $k = ld'$ mit $l \in [1, d]$ und $\operatorname{ggT}(l, d) = 1$. Daher ist

$$\{l \in [1, d] \mid \operatorname{ggT}(l, d) = 1\} \ \to \ \{k \in [1, m] \mid \operatorname{ggT}(k, m) = d'\}, \quad l \mapsto ld',$$

eine bijektive Abbildung, und es folgt

$$m = \sum_{1 \le d' \mid m} \big|\{k \in [1, m] \mid \operatorname{ggT}(k, m) = d'\}\big| = \sum_{1 \le d \mid m} \big|\{l \in [1, d] \mid \operatorname{ggT}(l, d) = 1\}\big| = \sum_{1 \le d \mid m} \varphi(d).$$

2. Es ist

$$\big|\{k \in [1, p^e] \mid \operatorname{ggT}(k, p^e) = 1\}\big| = \big|\{k \in [1, p^e] \mid p \nmid k\}\big| = p^e - \big|\{pj \mid j \in [1, p^{e-1}]\}\big| = p^e - p^{e-1}$$

und daher $\varphi(p^e) = p^e - p^{e-1} = p^{e-1}(p-1)$ nach 1.

3. Sind $R, R_1, \ldots, R_r$ Ringe und ist $\phi\colon R \to R_1 \times \ldots \times R_r$ ein Ringisomorphismus, so ist $\phi \mid R^\times\colon R^\times \to (R_1 \times \ldots \times R_r)^\times = R_1^\times \times \ldots \times R_r^\times$ ein Gruppenisomorphismus. Daher folgt die Behauptung aus Korollar 4.1.6.

4. Klar nach 3. □

Satz 4.3.4 (Fermat - Euler)**.**

1. *Sei* $m \in \mathbb{N}$, $a \in \mathbb{Z}$ *und* $\operatorname{ggT}(a, m) = 1$. *Dann ist* $\operatorname{ord}_m(a) \mid \varphi(m)$, *und für* $n \in \mathbb{Z}$ *ist genau dann* $a^n \equiv 1 \bmod m$, *wenn* $\operatorname{ord}_m(a) \mid n$.
2. (Kleiner Satz von Fermat) *Sei* $p \in \mathbb{P}$. *Dann ist*
$$a^{p-1} \equiv 1 \mod p \ \textit{für alle} \ a \in \mathbb{Z} \ \textit{mit} \ p \nmid a, \quad \textit{und} \quad a^p \equiv a \mod p \ \textit{für alle} \ a \in \mathbb{Z}.$$
3. (Satz von Euler) *Für* $m \in \mathbb{N}$ *und alle* $a \in \mathbb{Z}$ *mit* $\operatorname{ggT}(a, m) = 1$ *ist* $a^{\varphi(m)} \equiv 1 \bmod m$.

BEWEIS. Nach Satz 4.3.3 genügt es, 1. zu zeigen. Nach Definition ist genau dann $a^n \equiv 1 \bmod m$, wenn $(a + m\mathbb{Z})^n = 1 + m\mathbb{Z} \in (\mathbb{Z}/m\mathbb{Z})^\times$, und nach Satz 2.2.10.2 ist das äquivalent mit $\operatorname{ord}_m(a) \mid n$. Nach Satz 2.3.8.2 folgt $\operatorname{ord}_m(a) \mid \varphi(m)$. □

Lemma 4.3.5. *Sei* $a \in \mathbb{Z}$ *und* $e \in \mathbb{N}$.

1. *Ist* $e \ge 2$, *so folgt* $(1+p)^{p^{e-2}} \equiv 1 + p^{e-1} \bmod p^e$. *Insbesondere ist* $\operatorname{ord}_{p^e}(1+p) = p^{e-1}$.
2. *Ist* $e \ge 3$ *und* $2 \nmid a$, *so folgt* $a^{2^{e-2}} \equiv 1 \bmod 2^e$, *und es ist* $\operatorname{ord}_{2^e}(5) = 2^{e-2}$. *Insbesondere folgt*:
$$(\mathbb{Z}/2^e\mathbb{Z})^\times = \langle 5 + 2^e\mathbb{Z}\rangle \, \langle -1 + 2^e\mathbb{Z}\rangle \ (\text{dir}) \quad \textit{und} \quad (\mathbb{Z}/2^e\mathbb{Z})^\times \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2^{e-2}\mathbb{Z}.$$

BEWEIS. 1. Es genügt, die Kongruenz zu zeigen. Wir verwenden Induktion nach e. Für $e = 2$ ist nichts zu zeigen.

$e \ge 2$, $e \to e+1$: Sei $(1+p)^{p^{e-2}} = 1 + p^{e-1} + kp^e = 1 + p^{e-1}(1+kp)$ mit $k \in \mathbb{Z}$. Dann folgt

$$(1+p)^{p^{e-1}} = [1+p^{e-1}(1+kp)]^p = 1 + p^e(1+kp) + \frac{p-1}{2}p^{1+2(e-1)}(1+kp)^2 + \sum_{j=3}^{p}\binom{p}{j}p^{j(e-1)}(1+kp)^j.$$

Wegen $e \ge 2$ ist $1 + 2(e-1) \ge e+1$ und für $j \ge 3$ ist $j(e-1) \ge 3e - 3 \ge e+1$. Daher folgt $(1+p)^{p^{e-1}} \equiv 1 + p^e \bmod p^{e+1}$.

2. Induktion nach e. Für $e = 3$ folgt die Behauptung wegen $1^2 \equiv 3^2 \equiv 5^2 \equiv 7^2 \equiv 1 \bmod 8$.

$e \geq 3$, $e \to e+1$: Sei $a^{2^{e-2}} \equiv 1 \bmod 2^e$ und $5^{2^{e-3}} \not\equiv 1 \bmod 2^e$, also $a^{2^{e-2}} = 1 + 2^e k$ und $5^{2^{e-3}} = 1 + 2^{e-1} + 2^e l$ mit $k, l \in \mathbb{Z}$. Dann folgt $a^{2^{e-1}} = [1 + 2^e k]^2 = 1 + 2^{e+1}k + 2^{2e}k^2 \equiv 1 \bmod 2^{e+1}$ und $5^{2^{e-2}} = [1 + 2^{e-1}(2l+1)]^2 = 1 + 2^e(2l+1) + 2^{2e-2}(2l+1)^2 \equiv 1 + 2^e \bmod 2^{e+1}$, da $2e - 2 \geq e + 1$.

Wegen $5^k \equiv 1 \bmod 4$ für alle $k \in \mathbb{N}$ ist $\langle 5 + 2^e\mathbb{Z}\rangle \cap \langle -1 + 2^e\mathbb{Z}\rangle = \{1 + 2^e\mathbb{Z}\}$, und daher ist das Produkt direkt. Damit folgt $|\langle 5 + 2^e\mathbb{Z}\rangle \langle -1 + 2^e\mathbb{Z}\rangle| = \operatorname{ord}_{2^e}(5) \operatorname{ord}_{2^e}(-1) = 2^{e-1} = \varphi(2^e)$, und wir erhalten $(\mathbb{Z}/2^e\mathbb{Z})^\times = \langle 5 + 2^e\mathbb{Z}\rangle \langle -1 + 2^e\mathbb{Z}\rangle$. □

Satz 4.3.6. *Für $m \in \mathbb{N}$ gilt*: $(\mathbb{Z}/m\mathbb{Z})^\times$ *ist zyklisch* $\iff$ $m \in \{1, 2, 4, p^e, 2p^e \mid 2 \neq p \in \mathbb{P},\ e \in \mathbb{N}\}$.

Beweis. Wegen $\varphi(1) = \varphi(2) = 1$ und $\varphi(4) = 2$ ist $(\mathbb{Z}/m\mathbb{Z})^\times$ für $m \in \{1, 2, 4\}$ zyklisch nach Satz 2.3.8.3. Ist $p \in \mathbb{P}$, so ist $\mathbb{Z}/p\mathbb{Z}$ ein Körper nach Satz 3.2.8.3 und daher $(\mathbb{Z}/p\mathbb{Z})^\times$ zyklisch nach Satz 4.2.5.

Sei nun $p \in \mathbb{P} \setminus \{2\}$, $n \in \mathbb{N}$ und $w \in \mathbb{Z}$ mit $(\mathbb{Z}/p\mathbb{Z})^\times = \langle w + p\mathbb{Z}\rangle$. Sei (gemäß Lemma 4.3.1.2) $\omega\colon (\mathbb{Z}/p^e\mathbb{Z})^\times \to (\mathbb{Z}/p\mathbb{Z})^\times$ der kanonische Epimorphismus. Dann ist $\omega(w^{p^{e-1}} + p^e\mathbb{Z}) = w^{p^{e-1}} + p\mathbb{Z} = w + p\mathbb{Z}$ nach Satz 4.3.4.2, und wegen $w^{p^{e-1}(p-1)} \equiv 1 \bmod p^e$ folgt $\operatorname{ord}_{p^e}(w^{p^{e-1}}) = p - 1$. Nach Lemma 4.3.5.1 ist $\operatorname{ord}_{p^e}(1 + p) = p^{e-1}$, und mit Lemma 4.2.2 folgt

$$\operatorname{ord}_{p^e}\big(w^{p^{e-1}}(1+p)\big) = p^{e-1}(p-1) = \varphi(p^e)\ ;$$

und daher ist $(\mathbb{Z}/p^e\mathbb{Z})^\times$ zyklisch. Sei nun (wieder gemäß Lemma 4.3.1.2) $\omega_2\colon (\mathbb{Z}/2p^e\mathbb{Z})^\times \to (\mathbb{Z}/p^e\mathbb{Z})^\times$ der kanonische Epimorphismus. Wegen $\varphi(2p^e) = \varphi(p^e)$ ist ω_2 ein Isomorphismus, und daher ist auch $(\mathbb{Z}/2p^e\mathbb{Z})^\times$ zyklisch.

Ist entweder $m = 8$ oder $m = 4p$ mit $p \in \mathbb{P} \setminus \{2\}$ oder $m = pq$ mit $p, q \in \mathbb{P} \setminus \{2\}$ und $p \neq q$, so besitzt die Gruppe $(\mathbb{Z}/m\mathbb{Z})^\times$ zwei verschiedene Elemente der Ordnung 2 und ist daher nach Korollar 2.5.14 nicht zyklisch. In $(\mathbb{Z}/8\mathbb{Z})^\times$ sind $3 + 8\mathbb{Z}$ und $5 + 8\mathbb{Z}$ Elemente der Ordnung 2. Ist $p \in \mathbb{P} \setminus \{2\}$, so ist $(\mathbb{Z}/4p\mathbb{Z})^\times \cong (\mathbb{Z}/4\mathbb{Z})^\times \times (\mathbb{Z}/p\mathbb{Z})^\times$, und in diesem direkten Produkt sind $(1 + 4\mathbb{Z}, -1 + p\mathbb{Z})$ und $(-1 + 4\mathbb{Z}, 1 + p\mathbb{Z})$ Elemente der Ordnung 2. Sind $p, q \in \mathbb{P} \setminus \{2\}$ mit $p \neq q$, so ist $(\mathbb{Z}/pq\mathbb{Z})^\times \cong (\mathbb{Z}/p\mathbb{Z})^\times \times (\mathbb{Z}/q\mathbb{Z})^\times$, und man argumentiert wie eben.

Sei schließlich $m \in \mathbb{N} \setminus \{1, 2, 4, p^e, 2p^e \mid 2 \neq p \in \mathbb{P},\ e \in \mathbb{N}\}$. Dann gibt es ein $d \in \mathbb{N}$ mit $d \mid m$ und $d \in \{8, 4p, pq \mid p, q \in \mathbb{P} \setminus \{2\},\ p \neq q\}$. Nach Lemma 4.3.1 gibt es einen Epimorphismus $(\mathbb{Z}/m\mathbb{Z})^\times \to (\mathbb{Z}/d\mathbb{Z})^\times$, und da $(\mathbb{Z}/d\mathbb{Z})^\times$ nicht zyklisch ist, kann auch $(\mathbb{Z}/m\mathbb{Z})^\times$ nicht zyklisch sein. □

Satz 4.3.7. *Sei $m \in \mathbb{N}$, $m > 2$, und sei $(\mathbb{Z}/m\mathbb{Z})^\times$ zyklisch. Dann ist*

$$\prod_{\substack{j=1 \\ \operatorname{ggT}(j,m)=1}}^{m-1} j \equiv -1 \bmod m\,, \quad \textit{und genau dann gibt es ein } x \in \mathbb{Z} \textit{ mit } x^2 \equiv -1 \bmod m\textit{, wenn } 4 \mid \varphi(m)\,.$$

Insbesondere gilt: *Ist $p \in \mathbb{P}$, so folgt $(p-1)! \equiv -1 \bmod p$* (Satz von Wilson).

Beweis. Nach Korollar 2.5.14 ist

$$\sigma = \prod_{\substack{j=1 \\ \operatorname{ggT}(j,m)=1}}^{m-1} (j + m\mathbb{Z}) \in (\mathbb{Z}/m\mathbb{Z})^\times \text{ das einzige Element der Ordnung 2, und daher ist } \sigma = -1 + m\mathbb{Z}\,.$$

Sei nun $(\mathbb{Z}/m\mathbb{Z})^\times = \langle\omega\rangle$ und $\varphi(m) = 4k$ mit $k \in \mathbb{N}$. Ist dann $\omega^{2k} = \sigma$, und ist $x \in \mathbb{Z}$ mit $\omega^k = x + m\mathbb{Z}$, so folgt $x^2 \equiv -1 \bmod m$. Ist umgekehrt $x \in \mathbb{Z}$ mit $x^2 \equiv -1 \bmod m$, so folgt $4 = \operatorname{ord}_m(x) \mid \varphi(m)$. □

Satz 4.3.8. *Sei $m \in \mathbb{N}$, $m = p_1^{e_1} \cdot \ldots \cdot p_r^{e_r}$ mit $r \in \mathbb{N}_0$, $e_1, \ldots, e_r \in \mathbb{N}$ und verschiedenen Primzahlen $p_1, \ldots, p_r$. Dann sind äquivalent*:

(a) *Es gibt $a, b \in \mathbb{Z}$ mit $m = a^2 + b^2$.*

(b) *Für alle $i \in [1, r]$ gilt*: *Ist $p_i \equiv -1 \bmod 4$, so ist $2 \mid e_i$.*

BEWEIS. (a) $\Rightarrow$ (b) Sei $i \in [1,r]$, $p_i \equiv -1 \bmod 4$, sei $\nu \in \mathbb{N}_0$ maximal, so dass $p_i^\nu \mid a$ und $p_i^\nu \mid b$, sei $a = p_i^\nu a_0$, $b = p_i^\nu b_0$, und sei (ohne Einschränkung) $p_i \nmid a_0$. Dann ist $m = p_i^{2\nu} m_0$ mit $m_0 = a_0^2 + b_0^2$, und es genügt, $p_i \nmid m_0$ zu zeigen (denn dann ist $e_i = 2\nu$). Wir nehmen im Gegenteil an, es sei $p_i \mid m_0$. Wegen $p_i \nmid a_0$ gibt es nach Satz 2.3.6 ein $x \in \mathbb{Z}$ mit $a_0 x \equiv b_0 \bmod p_i$. Dann folgt

$$m_0 \equiv a_0^2(1+x^2) \equiv 0 \mod p_i\,, \quad \text{also} \quad x^2 \equiv -1 \mod p_i$$

und folglich $4 \mid \varphi(p_i) = p_i - 1$ nach Satz 4.3.7, ein Widerspruch.

(b) $\Rightarrow$ (a) Wir betrachten die quadratische Ordnung $R = \mathbb{Z}[\sqrt{-1}]$ (siehe Satz 3.4.6). Für $a, b \in \mathbb{Z}$ ist $a^2 + b^2 = \mathcal{N}(a + b\sqrt{-1})$, und für alle $\alpha, \beta \in R$ ist $\mathcal{N}(\alpha\beta) = \mathcal{N}(\alpha)\mathcal{N}(\beta)$. Nach Voraussetzung ist $m = m_0^2 p_1 \cdot \ldots \cdot p_s$ mit $m_0 \in \mathbb{N}$, $s \in \mathbb{N}_0$ und Primzahlen $p_1, \ldots, p_s$, so dass $p_i \equiv 1 \bmod 4$ für alle $i \in [1,s]$. Es ist $m_0^2 = \mathcal{N}(m_0)$, und daher genügt es, $p_i \in \mathcal{N}(R)$ für alle $i \in [1,s]$ zu zeigen, denn dann ist auch $m \in \mathcal{N}(R)$, also eine Summe von zwei Quadratzahlen. Wegen $2 = \mathcal{N}(1+\sqrt{-1})$ genügt es, zu zeigen:

Ist $p \in \mathbb{P}$ und $p \equiv 1 \bmod 4$, so ist $p \in \mathcal{N}(R)$.

Sei $p \in \mathbb{P}$ und $p \equiv 1 \bmod 4$. Nach Satz 4.3.7 gibt es ein $x \in \mathbb{Z}$ mit $x^2 \equiv -1 \bmod p$, und es sei $P = {}_R\langle p, x + \sqrt{-1}\rangle$. Wegen $p^{-1}(x+\sqrt{-1}) \notin R$ ist $P \supsetneq pR$. Wir nehmen nun an, es sei $P = R$. Dann gibt es $\alpha, \beta \in R$, so dass $1 = p\alpha + (x+\sqrt{-1})\beta$, und es folgt

$$x - \sqrt{-1} = p\alpha(x - \sqrt{-1}) + (x^2+1)\beta \in pR\,, \quad \text{ein Widerspruch}\,.$$

Nach Satz 3.4.6 ist nun $P = \omega R$ mit $\omega \in R^\bullet \setminus R^\times$, und es ist $p = \omega\omega_1$ mit $\omega_1 \in R^\bullet \setminus R^\times$. Damit folgt $p^2 = \mathcal{N}(p) = \mathcal{N}(\omega)\mathcal{N}(\omega_1)$, und wegen $1 < \mathcal{N}(\omega) \le p$ folgt $\mathcal{N}(\omega) = p$. □

4.4. g-adische Zifferndarstellungen

In diesem Abschnitt sei $g \in \mathbb{N}_{\ge 2}$.

Bemerkung 4.4.1. Sei $d \in \mathbb{Z}$. Für $n \ge d$ ist

$$\sum_{i=d}^{n} g^{-i} = g^{-d} \sum_{j=0}^{n-d} (g^{-1})^j = g^{-d}\,\frac{(g^{-1})^{n-d+1} - 1}{g^{-1} - 1} = \frac{g^{-d+1} - g^{-n}}{g-1}\,,$$

und daher ist

$$\Big(\sum_{i=d}^{n} g^{-i}\Big)_{n \ge d} \quad \text{eine monoton wachsende Folge mit Limes} \quad \frac{g^{-d+1}}{g-1}\,.$$

Ist $(a_i)_{i \ge d}$ eine Folge in $[0, g-1]$, so folgt

$$\sum_{i=d}^{n} a_i g^{-i} \le (g-1) \sum_{i=d}^{n} g^{-i} \le g^{-d+1} \quad \text{für alle} \quad n \ge d\,.$$

Daher ist

$$\Big(\sum_{i=d}^{n} a_i g^{-i}\Big)_{n \ge d} \quad \text{monoton wachsend und beschränkt, also konvergent.}$$

Definition 4.4.2. Sei $z \in \mathbb{R}_{>0}$, $d \in \mathbb{Z}$ und $(a_i)_{i\geq d}$ eine Folge in $[0, g-1]$. Dann heißt $-d$ der *g-adische Exponent* und $(a_i)_{i\geq d}$ die *g-adische Ziffernfolge* von z, wenn gilt:

$$z = \sum_{i=d}^{\infty} a_i g^{-i}, \quad a_d \neq 0, \quad \text{und zu jedem } l \geq d \text{ gibt es ein } i \geq l \text{ mit } a_i \neq g-1.$$

Man schreibt dann

$$z = (a_d a_{d+1} \ldots a_0, a_1 a_2 \ldots)_g, \text{ falls } d \leq 0, \quad \text{und} \quad z = (0, \underbrace{0 \ldots 0}_{d-1} a_d d_{d+1} \ldots)_g, \text{ falls } d > 0.$$

Satz 4.4.3 (Kennzeichnungssatz für die g-adische Ziffernentwicklung)**.** *Sei $z \in \mathbb{R}_{>0}$, $d \in \mathbb{Z}$ und $(a_i)_{i\geq d}$ eine Folge in $[0, g-1]$. Dann sind äquivalent*:

(a) *$-d$ ist der g-adische Exponent und $(a_i)_{i\geq d}$ ist die g-adische Ziffernfolge von z.*

(b) *$a_d \neq 0$, und für alle $n \geq d$ ist*

$$\sum_{i=d}^{n} a_i g^{-i} \leq z < \sum_{i=d}^{n} a_i g^{-i} + g^{-n}.$$

Beweis. (a) $\Rightarrow$ (b) Es ist

$\left(\sum_{i=d}^{n} a_i g^{-i}\right)_{n\geq d}$ monoton wachsend mit Grenzwert z und daher $\sum_{i=d}^{n} a_i g^{-i} \leq z$ für alle $n \geq d$.

Wäre $n \geq d$ mit

$$z - \sum_{i=d}^{n} a_i g^{-i} \geq g^{-n}, \text{ so folgte } \sum_{i=n+1}^{\infty} a_i g^{-i} \geq g^{-n} = \sum_{i=n+1}^{\infty} (g-1) g^{-i}, \text{ also } \sum_{i=n+1}^{\infty} (g-1-a_i) g^{-i} \leq 0.$$

Wegen $g-1-a_i \geq 0$ folgte daraus aber $a_i = g-1$ für alle $i \geq n+1$, ein Widerspruch.

(b) $\Rightarrow$ (a) Für alle $n \geq d$ ist

$$\sum_{i=d}^{n} a_i g^{-i} \leq z < \sum_{i=d}^{n} a_i g^{-i} + g^{-n},$$

und für $n \to \infty$ erhalten wir

$$\sum_{i=d}^{\infty} a_i g^{-i} \leq z \leq \sum_{i=d}^{\infty} a_i g^{-i} + \lim_{n\to\infty} g^{-n}, \quad \text{also} \quad z = \sum_{i=d}^{\infty} a_i g^{-i}.$$

Wir nehmen nun an, es sei $l \geq d$ und $a_i = g-1$ für alle $i \geq l$. Dann ist

$$z = \sum_{i=d}^{\infty} a_i g^{-i} = \sum_{i=d}^{l} a_i g^{-i} + \sum_{i=l+1}^{\infty} (g-1) g^{-i} = \sum_{i=d}^{l} a_i g^{-i} + g^{-l} > z, \quad \text{ein Widerspruch.}$$

□

Satz 4.4.4 (Existenz- und Eindeutigkeit der g-adischen Ziffernentwicklung)**.** *Sei $z \in \mathbb{R}_{>0}$. Dann gibt es genau ein $d \in \mathbb{Z}$ und genau eine Folge $(a_i)_{i\geq d}$ in $[0, g-1]$ so dass $-d$ ist der g-adische Exponent und $(a_i)_{i\geq d}$ die g-adische Ziffernfolge von z ist.*

Beweis. EXISTENZ: $\mathbb{R}_{>0}$ ist die disjunkte Vereinigung der Intervalle $[g^{-d}, g^{-d+1})$. Daher gibt es ein $d \in \mathbb{Z}$ mit $g^{-d} \leq z < g^{-d+1}$. Wir konstruieren rekursiv eine Folge $(a_i)_{i\geq d}$ in $[0, g-1]$ mit Eigenschaft (b) aus Satz 4.4.3.

Ist $n = d$, so ist $g^{-d} \leq z < g^{-d+1}$, und wegen $g^{-d} < 2g^{-d} < \ldots < (g-1)g^{-d} < g \cdot g^{-d}$ existiert ein $a_d \in [1, g-1]$ mit $a_d g^{-d} \leq z < a_d g^{-d} + g^{-d}$.

Sei nun $n \geq d$ und seien $a_d, a_{d+1}, \ldots, a_n \in [0, g-1]$ mit

$$\sum_{i=d}^{n} a_i g^{-i} \leq z < \sum_{i=d}^{n} a_i g^{-i} + g^{-n}\,, \quad \text{also} \quad 0 \leq z' = z - \sum_{i=d}^{n} a_i g^{-i} < g^{-n}\,.$$

Wegen $0 < g^{-(n+1)} < 2g^{-(n+1)} < \ldots < (g-1)g^{-(n+1)} < g \cdot g^{-(n+1)}$ existiert ein $a_{n+1} \in [0, g-1]$ mit $a_{n+1} g^{-(n+1)} \leq z' < (a_{n+1}+1)g^{-(n+1)}$, und wir erhalten

$$\sum_{i=d}^{n+1} a_i g^{-i} \leq z < \sum_{i=d}^{n+1} a_i g^{-i} + g^{-(n+1)}\,.$$

EINDEUTIGKEIT: Seien $-d$, $-d'$ zwei g-adische Exponenten und $(a_i)_{i\geq d}$, $(a'_i)_{i\geq d'}$ zwei g-adische Ziffernfolgen. Dann ist $g^{-d} \leq a_d g^{-d} \leq z < a_d g^{-d} + g^{-d} \leq g^{-d+1}$ und in gleicher Weise $g^{-d'} \leq z < g^{-d'+1}$. Daher folgt $d = d'$. Wir nehmen nun an, es sei $T = \{n \geq d \mid a_n \neq a'_n\} \neq \emptyset$, $m = \min T$ und $a_m < a'_m$. Dann ist $m \geq d$, $a_n = a'_n$ für alle $n \in [d, m-1]$, und wir erhalten

$$\sum_{i=d}^{m} a_i g^{-i} \leq z < \sum_{i=d}^{m} a_i g^{-i} + g^{-m} \leq \sum_{i=d}^{m-1} a'_i g^{-i} + a'_m g^{-m} \leq z\,, \quad \text{ein Widerspruch.}$$

□

Korollar 4.4.5. *Sei $z \in \mathbb{R}_{>0}$, $d \in \mathbb{Z}$, $-d$ der g-adische Exponent und $(a_i)_{i\geq d}$ die g-adische Ziffernfolge von z. Genau dann ist $z \in \mathbb{N}$, wenn $d \leq 0$ und $a_i = 0$ für alle $i \geq 1$.*

BEWEIS. Ist $d \leq 0$ und $a_i = 0$ für alle $i \geq 1$, so ist

$$z = \sum_{i=d}^{\infty} a_i g^{-i} = \sum_{i=d}^{0} a_i g^{-i} \in \mathbb{N}\,.$$

Sei nun $z \in \mathbb{N}$. Dann ist $g^0 = 1 \leq z < g^{-d+1}$, und daher $-d+1 > 0$, also $d \leq 0$. Wir nehmen an, es sei $a_i \neq 0$ für ein $i \geq 1$. Ist nun $l \geq 1$ mit $a_l \neq g-1$, so folgt

$$0 < \sum_{i=1}^{\infty} a_i g^{-i} = z - \sum_{i=d}^{0} a_i g^{-i} \in \mathbb{N} \text{ und } 0 < \sum_{i=1}^{\infty} a_i g^{-i} \leq \sum_{i=1}^{\infty} (g-1)g^{-i} - g^{-l} < 1\,, \text{ ein Widerspruch.}$$

□

Korollar 4.4.6. *Sei $z \in \mathbb{R}_{\geq 0}$. Dann gibt es genau ein $a_0 \in \mathbb{N}_0$ und genau eine Folge $(a_i)_{i\geq 1}$ in $[0, g-1]$, so dass*

$$z = a_0 + \sum_{i=1}^{\infty} a_i g^{-i}\,, \quad \textit{und zu jedem } l \geq 1 \textit{ existiert ein } i \geq l \textit{ mit } a_i \neq g-1\,.$$

Weiters gilt:

1. $a_0 = \lfloor z \rfloor$.
2. $z \in \mathbb{N}_0 \iff a_i = 0$ *für alle* $i \geq 1$.
3. $z = 0 \iff a_i = 0$ *für alle* $i \geq 0$.
4. *Ist* $z \notin \mathbb{N}_0$ *und* $d = \min\{i \geq 1 \mid a_i \neq 0\}$, *so ist* $-d$ *der g-adische Exponent und* $(a_i)_{i\geq d}$ *die g-adische Ziffernfolge von* $z - \lfloor z \rfloor$.

Man schreibt dann $z = (a_0, a_1 a_2 \ldots)_g$ und nennt $(a_i)_{i\geq 1}$ die *g-adische Nachkommafolge* von z.

BEWEIS. Ist $z \in \mathbb{N}_0$, so setzen wir $a_0 = z$ und $a_i = 0$ für alle $i \geq 1$. Sei nun $z \notin \mathbb{N}_0$. Dann ist $0 < z - [z] < 1$, es sei $-d$ der g-adische Exponent und $(a_i)_{i \geq d}$ die g-adische Ziffernfolge von $z - [z]$. Dann ist $g^{-d} \leq z - [z] < 1 = g^0$, also $d \geq 1$, und wir setzen $a_i = 0$ für alle $i \in [1, d-1]$. Dann hat $(a_i)_{i \geq 1}$ die gewünschten Eigenschaften. Insbesondere gelten 1. bis 4., und aus 4. und der Eindeutigkeitsaussage in Satz 4.4.4 folgt die Eindeutigkeit der Folge $(a_i)_{i \geq 0}$. □

Korollar 4.4.7 (g-adischer Ziffernalgorithmus)**.** *Sei $z \in \mathbb{R}_{\geq 0}$. Die Folgen $(a_n)_{n \geq 0}$ und $(z_n)_{n \geq 0}$ seien rekursiv definiert durch*

$$a_0 = \lfloor z \rfloor\,, \quad z_0 = z - \lfloor z \rfloor \qquad \text{und} \qquad a_n = \lfloor g z_{n-1} \rfloor\,, \quad z_n = g z_{n-1} - a_n \ \text{ für alle } \ n \geq 1\,.$$

Dann ist $(a_n)_{n \geq 1}$ die g-adische Nachkommafolge von z.

BEWEIS. Für alle $n \geq 0$ ist $0 \leq z_n < 1$, und daher ist $a_n = \lfloor g z_{n-1} \rfloor \in [0, g-1]$ für alle $n \geq 1$. Also genügt es nach Korollar 4.4.6, die beiden folgenden Behauptungen nachzuweisen.

B1. $z = a_0 + \sum_{i \geq 1} a_i g^{-i}\,,$ **B2.** Zu jedem $l \geq 1$ existiert ein $i \geq l$ mit $a_i \neq g - 1$.

Beweis von **B1**. Wir zeigen (mittels Induktion nach n), dass

$$z = a_0 + \sum_{i=1}^{n} a_i g^{-i} + g^{-n} z_n \quad \text{für alle } \ n \geq 0\,.$$

Für $n \to \infty$ folgt dann die Behauptung.

$n = 0$: $z = a_0 + z_0$.

$n \geq 0\,,\ n \to n+1$. Aus $z_{n+1} = g z_n - a_{n+1}$ folgt $g^{-n} z_n = a_{n+1} g^{-(n+1)} + g^{-(n+1)} z_{n+1}$, und wir erhalten

$$z = a_0 + \sum_{i=1}^{n} a_i g^{-i} + g^{-n} z_n = a_0 + \sum_{i=1}^{n+1} a_i g^{-i} + g^{-(n+1)} z_{n+1}\,.$$

Beweis von **B2**. Wir nehmen an, es existiert ein $l \geq 1$ mit $a_i = g - 1$ für alle $i \geq l$. Dann folgt

$$z = a_0 + \sum_{i=1}^{\infty} a_i g^{-i} = a_0 + \sum_{i=1}^{l} a_i g^{-i} + g^{-l} z_l \ \text{ und daher } \ z_l = g^l \sum_{i=l+1}^{\infty} (g-1) g^{-i} = 1\,, \ \text{ ein Widerspruch.}$$

□

Definition 4.4.8. Eine Folge $(a_n)_{n \geq 1}$ (in einer Menge X) heißt *schließlich periodisch*, wenn es $k, l \in \mathbb{N}$ gibt, so dass $a_{i+l} = a_i$ für alle $i \geq k$.

Sei $(a_n)_{n \geq 1}$ eine schließlich periodische Folge. Dann heißt

$$k_0 = \min\{k \in \mathbb{N}_0 \mid \text{es gibt ein } l \in \mathbb{N}\,, \text{ so dass } \ a_{i+l} = a_i \ \text{ für alle } i \geq k+1\,\}$$

die *Vorperiodenlänge* von $(a_n)_{n \geq 1}$. Ist $k_0 \geq 1$, so heißt $(a_1, \ldots, a_{k_0})$ die *Vorperiode* von $(a_n)_{n \geq 1}$. Ist $k_0 = 0$, so heißt $(a_n)_{n \geq 1}$ *rein-periodisch*. Ist $k_0 \in \mathbb{N}_0$ die Vorperiodenlänge von $(a_n)_{n \geq 1}$, so heißt

$$l_0 = \min\{l \in \mathbb{N} \mid \text{ für alle } \ i \geq k_0 + 1 \text{ ist } a_{i+l} = a_i\}$$

die *Periodenlänge* von $(a_n)_{n \geq 1}$ und $(a_{k_0+1}, \ldots, a_{k_0+l_0})$ die *primitive Periode* von $(a_n)_{n \geq 1}$.

Proposition 4.4.9. *Sei $z \in \mathbb{R}_{\geq 0}$ und $(a_i)_{i \geq 1}$ die g-adische Nachkommafolge von z. Dann sind äquivalent*:

(a) $z \in \mathbb{Q}$.

(b) $(a_i)_{i \geq 1}$ *ist schließlich periodisch.*

BEWEIS. (b) $\Rightarrow$ (a) Seien $k, l \in \mathbb{N}$ und $a_{i+l} = a_i$ für alle $i \geq k$. Dann ist $a_{i+jl} = a_i$ für alle $i \geq k$ und alle $j \in \mathbb{N}_0$, und wir erhalten

$$z = \lfloor z \rfloor + \sum_{i=1}^{\infty} a_i g^{-i} = \lfloor z \rfloor + \sum_{i=1}^{k-1} a_i g^{-i} + \sum_{r=0}^{l-1} \sum_{j=0}^{\infty} a_{k+jl+r} g^{-(k+jl+r)} ,$$

und wegen

$$\sum_{j=0}^{\infty} a_{k+jl+r} g^{-(k+jl+r)} \;=\; a_{k+r} g^{-(k+r)} \sum_{j=0}^{\infty} \left(g^{-l}\right)^j \;=\; a_{k+r} g^{-(k+r)} \frac{1}{1-g^{-l}} \;\in \mathbb{Q} \quad \text{ist auch} \quad z \in \mathbb{Q} .$$

(a) $\Rightarrow$ (b) Sei $(z_n)_{n\geq 0}$ rekursiv definiert durch $z_0 = z - \lfloor z \rfloor$ und $z_n = g z_{n-1} - \lfloor g z_{n-1} \rfloor$ für $n \geq 1$. Nach Korollar 4.4.7 ist $a_n = \lfloor g z_{n-1} \rfloor$ für alle $n \in \mathbb{N}$. Es sei nun $z = \frac{s}{q}$ mit $s \in \mathbb{N}_0$ und $q \in \mathbb{N}$, und es sei $(s_n)_{n\geq 0}$ rekursiv definiert durch

$$s_0 = q z_0 \quad \text{und} \quad g s_{n-1} = q k_n + s_n \text{ mit } k_n,\, s_n \in \mathbb{N}_0 \text{ und } 0 \leq s_n < q \quad \text{für } n \geq 1 .$$

Offensichtlich ist $s_0 = q z_0 = qz - q\lfloor z \rfloor = s - q\lfloor z \rfloor \in \mathbb{Z}$, $0 \leq s_0 < q$, und es existieren $k, l \in \mathbb{N}$ mit $s_{k-1+l} = s_{k-1}$. Wir zeigen nun die beiden folgenden Behauptungen.

B1. Für alle $n \geq 0$ ist $z_n = \dfrac{s_n}{q}$. **B2.** Für alle $i \geq k$ ist $a_{i+l} = a_i$ und $z_{i+l} = z_i$.

Nach **B2** ist dann $(a_i)_{i\geq 1}$ schließlich periodisch.

Beweis von **B1**. Induktion nach n. Für $n = 0$ ist die Aussage klar.

$n \geq 1$, $n - 1 \to n$: Es ist

$$z_{n-1} = \frac{s_{n-1}}{q}, \text{ also } g z_{n-1} = \frac{g s_{n-1}}{q} = k_n + \frac{s_n}{q} \text{ und daher } z_n = g z_{n-1} - \lfloor g z_{n-1} \rfloor = g z_{n-1} - k_n = \frac{s_n}{q} .$$

Beweis von **B2**. Induktion nach i.

$i = k$: Nach **B1** ist $z_{k-1+l} = z_{k-1}$ und daher

$$a_{k+l} = \lfloor g z_{k+l-1} \rfloor = \lfloor g z_{k-1} \rfloor = a_k \quad \text{und} \quad z_{k+l} = g z_{k+l-1} - a_{k+l} = g z_{k-1} - a_k = z_k .$$

$i \geq k$, $i \to i+1$: Es ist

$$a_{i+l+1} = \lfloor g z_{i+l} \rfloor = \lfloor g z_i \rfloor = a_{i+1} \quad \text{und} \quad z_{i+l+1} = g z_{i+l} - a_{i+l+1} = g z_i - a_{i+1} = z_{i+1} .$$

□

Definition 4.4.10. Sei $z \in \mathbb{Q}_{\geq 0}$, $a_0 = \lfloor z \rfloor$ und $(a_n)_{n\geq 1}$ die g-adische Nachkommafolge von z. Sei k_0 die Vorperiodenlänge und l_0 die Periodenlänge von $(a_n)_{n\geq 1}$. Dann schreibt man

$$z = (a_0, a_1 \ldots a_{k_0} \overline{a_{k_0+1} \ldots a_{k_0+l_0}})_g .$$

Man sagt, die g-adische Ziffernentwicklung von z *bricht ab*, wenn $l_0 = 1$ und $a_{k_0+1} = 0$ (d. h., $(a_n)_{n\geq 1}$ ist schließlich periodisch ist mit primitiver Periode (0)) . In diesem Falle schreibt man

$$z = (a_0, a_1 \ldots a_{k_0}\ \overline{0})_g = (a_0, a_1 \ldots a_{k_0})_g .$$

Satz 4.4.11. *Sei $z \in \mathbb{Q}_{\geq 0}$, $(a_n)_{n\geq 1}$ die g-adische Nachkommafolge von z, $k_0 \in \mathbb{N}_0$ die Vorperiodenlänge und $l_0 \in \mathbb{N}$ die Periodenlänge von $(a_n)_{n\geq 1}$. Dann gilt*:

1. $k_0 = \min\{k \in \mathbb{N}_0 \mid$ *der reduzierte Nenner von zg^k ist teilerfremd zu g* $\}$.
2. *Sei q der reduzierte Nenner von zg^{k_0}. Dann ist $l_0 = \mathrm{ord}_q(g)$.*
3. *Sei $t \in \mathbb{N}$ der reduzierte Nenner von z. Dann gilt*:

$$\textit{Die } g\textit{-adische Entwicklung von } z \textit{ bricht ab} \iff t \mid g^N \textit{ für ein } N \in \mathbb{N} .$$

BEWEIS. Sei $a_0 = \lfloor z \rfloor$ und $z = (a_0, a_1 \dots a_{k_0}\ \overline{a_{k_0+1} \dots a_{k_0+l_0}})_g$. Dann ist

$$z = a_0 + \sum_{i=1}^{k_0} a_i g^{-i} + \sum_{i=1}^{l_0} \sum_{n=0}^{\infty} a_{k_0+i+nl_0} g^{-(k_0+i+nl_0)} = \sum_{i=0}^{k_0} a_i g^{-i} + \sum_{i=1}^{l_0} a_{k_0+i} g^{-k_0-i} \sum_{n=0}^{\infty} (g^{-l_0})^n$$
$$= \sum_{i=0}^{k_0} a_i g^{-i} + \frac{g^{l_0}}{g^{l_0}-1} \sum_{i=1}^{l_0} a_{k_0+i} g^{-k_0-i}$$

1. Sei $k \in \mathbb{N}_0$, v der reduzierte Nenner und u der reduzierte Zähler von zg^k. Dann müssen wir zeigen:

$$\mathrm{ggT}(v, g) = 1 \iff k \geq k_0 .$$

Ist $k \geq k_0$, so folgt

$$zg^k = \sum_{i=0}^{k_0} a_i g^{k-i} + \frac{1}{g^{l_0}-1} \sum_{i=1}^{l_0} a_{k_0+i} g^{(k-k_0)+(l_0-i)} = \frac{u}{v} ,$$

also $v \,|\, u(g^{l_0}-1)$. Wegen $\mathrm{ggT}(u, v) = 1$ folgt $v \mid g^{l_0}-1$ und daher $\mathrm{ggT}(v, g) = 1$.

Ist $k < k_0$, so folgt

$$zg^k = \frac{zg^{k_0}}{g^{k_0-k}} = \frac{1}{(g^{l_0}-1)(g^{k_0-k})} \Big[(g^{l_0}-1) \sum_{i=0}^{k_0} a_i g^{k_0-i} + \sum_{i=1}^{l_0} a_{k_0+i} g^{l_0-i} \Big] = \frac{C}{(g^{l_0}-1)g^{k_0-k}} = \frac{u}{v}$$

mit $C \in \mathbb{Z}$, $C \equiv -a_{k_0} + a_{k_0+l_0} \mod g$. Daher ist $g \,|\, Cv$. Wäre $\mathrm{ggT}(v, g) = 1$, so folgte $g \,|\, C$ und daher $a_{k_0} = a_{k_0+l_0}$ im Widerspruch zur Minimalität von k_0.

2. Sei q der reduzierte Nenner und r der reduzierte Zähler von zg^{k_0}, und sei $m = \mathrm{ord}_q(g)$. Wegen

$$zg^{k_0} = \sum_{i=0}^{k_0} a_i g^{k_0-i} + \frac{1}{g^{l_0}-1} \sum_{i=1}^{l_0} a_{k_0+i} g^{l_0-i} = \frac{r}{q}$$

folgt $q \,|\, g^{l_0}-1$, also $g^{l_0} \equiv 1 \mod q$ und daher $m \,|\, l_0$. Es genügt nun, zu zeigen:

Für alle $i, i' \in [0, l_0-1]$ mit $i \equiv i' \bmod m$ ist $a_{k_0+1+i} = a_{k_0+1+i'}$.

Aufgrund der Minimalität von l_0 folgt dann $l_0 \leq m$ und daher $l_0 = m$.

Sei $l_0 = ms$ und $g^m - 1 = qe$ mit $s, e \in \mathbb{N}$. Dann ist

$$g^{l_0}-1 = (g^m-1) \sum_{j=0}^{s-1} (g^m)^j = qe \sum_{j=0}^{s-1} g^{jm} \quad \text{und} \quad q(g^{l_0}-1) \sum_{i=0}^{k_0} a_i g^{k_0-i} + q \sum_{i=1}^{l_0} a_{k_0+i} g^{l_0-i} = (g^{l_0}-1)r .$$

Also erhalten wir

$$g^{l_0}-1 \;\Big|\; q \sum_{i=1}^{l_0} a_{k_0+i} g^{l_0-i} \quad \text{und daher} \quad \sum_{j=0}^{s-1} g^{jm} \;\Big|\; \sum_{i=1}^{l_0} a_{k_0+i} g^{l_0-i} .$$

Sei $b \in \mathbb{N}$ mit

$$\sum_{i=1}^{l_0} a_{k_0+i} g^{l_0-i} = b \sum_{j=0}^{s-1} g^{jm} = b \, \frac{g^{ms}-1}{g^m-1} , \quad \text{also} \quad b \, \frac{g^{ms}-1}{g^m-1} \leq (g-1) \frac{g^{l_0}-1}{g-1} = g^{ms}-1 .$$

Daher ist $b \leq g^m - 1$, und nach Korollar 4.4.5 hat b eine Darstellung

$$b = \sum_{\mu=0}^{m-1} b_\mu g^\mu \quad \text{mit} \quad b_0, \dots, b_{m-1} \in [0, g-1] .$$

Insgesamt erhalten wir

$$\sum_{i=1}^{l_0} a_{k_0+i} g^{l_0-i} = \sum_{\mu=0}^{m-1} \sum_{j=0}^{s-1} b_\mu g^{jm+\mu} .$$

Seien nun $i,\ i' \in [0, l_0-1]$ mit $i \equiv i' \bmod m$. Dann folgt $l_0-(i+1) \in [0, l_0-1],\ l_0-(i'+1) \in [0, l_0-1]$, und es existieren eindeutig bestimmte $\mu,\ \mu' \in [0, m-1]$ und $j,\ j' \in [0, s-1]$, so dass

$$l_0-(i+1) = jm+\mu \quad \text{und} \quad l_0-(i'+1) = j'm+\mu' , \quad \text{und es ist} \quad \mu \equiv \mu' \mod m , \quad \text{also} \quad \mu = \mu' .$$

Aus der Eindeutigkeit der g-adischen Darstellung folgt

$$a_{k_0+i+1} = b_\mu \quad \text{und} \quad a_{k_0+i'+1} = b_{\mu'} , \quad \text{also} \quad a_{k_0+i+1} = a_{k_0+i'+1} .$$

3. Sei $r \in \mathbb{N}$ der reduzierte Zähler von z. Wir nehmen zuerst an, die g-adische Entwicklung bricht ab. Dann ist $l_0 = 1,\ a_{k_0+1} = 0$, und

$$z = a_0 + \sum_{i=1}^{k_0} a_i g^{-i} = \frac{r}{t} , \quad \text{und daher} \quad t \,|\, g^{k_0} .$$

Sei nun $m \in \mathbb{N}$ mit $t \,|\, g^m,\ g^m = tb$ mit $b \in \mathbb{N}$. Nach Korollar 4.4.5 ist

$$rb = \sum_{j=0}^{s} b_j g^j \quad \text{mit} \quad s \in \mathbb{N} \ \text{ und } \ b_0, \ldots, b_s \in [0, g-1] \quad \text{und daher} \quad z = \frac{rb}{g^m} = \sum_{j=0}^{s} b_j g^{j-m} .$$

Das ist aber eine abbrechende Ziffernentwicklung von z. □

Beispiel 4.4.12. Bestimmung der Vorperiodenlänge und der Periodenlänge von $z = \frac{517}{740}$ mit Hilfe von Satz 4.4.11: siehe Proseminar.

CHAPTER 5

Abstrakte Teilbarkeitslehre und faktorielle Bereiche

5.1. Teilbarkeit, ggT und kgV in multiplikativen Halbgruppen

Wir formulieren die Begriffe und Sätze der elementaren Teilbarkeitslehre für (multiplikative) Monoide. Die wichtigsten Beispiele für Monoide sind das Monoid $(\mathbb{N}, \cdot)$ und die multiplikativen Monoide $R^\bullet$ von Bereichen (siehe Lemma 3.1.6.4). Für die Teilbarkeitslehre in Bereichen ist es manchmal sinnvoll, die multiplikative Halbgruppe $(R, \cdot)$ an Stelle des Monoids $R^\bullet$ zu betrachten, und eine Reihe einfacher Aussagen bleiben für kommutative multiplikative Halbgruppen richtig. Wir entwickeln die Theorie in dieser Allgemeinheit, soweit das ohne Schwierigkeiten möglich ist.

Im Folgenden betrachten wir jede kommutative multiplikative Halbgruppe H als Unterhalbgruppe ihrer Quotientenhalbgruppe $\mathsf{q}(H)$ (siehe 3.3.5). Für jedes $a \in H^\bullet$ ist dann $a^{-1} \in \mathsf{q}(H)$.

Definition 5.1.1. Sei H eine kommutative (multiplikative) Halbgruppe.

1. Seien $a, b \in H$. Man sagt, a *teilt* b (in H) und schreibt $a \,|\, b$ oder $a \,|_H b$, wenn ein $c \in H$ existiert mit $b = ac$ [$\iff b \in aH$]. Man nennt dann a einen *Teiler* von b und b ein *Vielfaches* von a, und man sagt auch, b ist durch a teilbar.
2. Sei $A \subset H$.
   (a) Ein Element $d \in H$ heißt *größter gemeinsamer Teiler* von A, wenn gilt:
   - Für alle $a \in A$ ist $d \,|\, a$.
   - Ist $g \in H$ und $g \,|\, a$ für alle $a \in A$, so folgt $g \,|\, d$.

   Wir bezeichnen mit $\mathrm{GGT}(A) = \mathrm{GGT}_H(A)$ die Menge der größten gemeinsamen Teiler von A in H. Ist $A = \{a_1, \ldots, a_n\}$, so schreiben wir $\mathrm{GGT}(a_1, \ldots, a_n)$ an Stelle von $\mathrm{GGT}(A)$. Ist $\mathrm{GGT}(a_1, \ldots, a_n) = H^\times$, so nennt man $a_1, \ldots, a_n$ *teilerfremd*.

   (b) Ein Element $e \in H$ heißt *kleinstes gemeinsames Vielfaches* von A, wenn gilt:
   - Für alle $a \in A$ ist $a \,|\, e$.
   - Ist $g \in H$ und $a \,|\, g$ für alle $a \in A$, so folgt $e \,|\, g$.

   Wir bezeichnen mit $\mathrm{KGV}(A) = \mathrm{KGV}_H(A)$ die Menge der kleinsten gemeinsamen Vielfachen von A in H. Ist $A = \{a_1, \ldots, a_n\}$, so schreiben wir $\mathrm{KGV}(a_1, \ldots, a_n)$ an Stelle von $\mathrm{KGV}(A)$.

Lemma 5.1.2 (Elementare Eigenschaften der Teilbarkeit)**.** *Sei H eine kommutative Halbgruppe, und seien $a, b, c, d \in H$.*

1. *Für alle $\varepsilon \in H^\times$ ist $\varepsilon \,|\, a$ und $a\varepsilon \,|\, a$.*
2. *Aus $a \,|\, b$ und $c \,|\, d$ folgt $ac \,|\, bd$.*
3. *Aus $a \,|\, b$ folgt $ac \,|\, bc$. Ist $c \in H^\bullet$ und $ac \,|\, bc$, so folgt $a \,|\, b$.*
4. *Aus $a \,|\, b$ und $b \,|\, c$ folgt $a \,|\, c$.*

5. *Ist* $a \in H^\bullet$*, so ist genau dann* $a \mid b$*, wenn* $a^{-1}b \in H$*.*
6. *Genau dann ist* $a \simeq b$*, wenn* $a \mid b$ *und* $b \mid a$*.*
7. $a \in H^\times \iff a \mid 1 \iff a \simeq 1$*.*
8. *Sei* $a \simeq b$ *und* $c \simeq d$*. Dann gilt:* $a \mid c \iff b \mid d$*. Insbesondere folgt:* $a \mid_H b \iff [a]_\simeq \mid_{H/\simeq} [b]_\simeq$*.*

BEWEIS. 1. Für $\varepsilon \in H^\times$ ist $a = \varepsilon(\varepsilon^{-1}a) = \varepsilon^{-1}(\varepsilon a)$.

2. Sei $a \mid b$ und $c \mid d$, also $b = ax$ und $d = cy$ mit $x, y \in H$. Dann ist $bd = (ax)(cy) = (ac)(xy)$ und daher $ac \mid bd$.

3. Sei $a \mid b$, also $b = ax$ mit $x \in H$. Dann ist $bc = acx$ und daher $ac \mid bc$. Sei umgekehrt $ac \mid bc$, also $bc = acx$ mit $x \in H$. Ist c kürzbar, so folgt $b = xa$ und daher $a \mid b$.

4. Sei $a \mid b$ und $b \mid c$, also $b = ax$ und $c = by$ mit $x, y \in H$. Dann ist $c = axy$ und daher $a \mid c$.

5., 6., 7. und 8. Nach Definition. □

Satz 5.1.3 (Elementare Eigenschaften von GGT und KGV)**.** *Sei* H *eine kommutative Halbgruppe, und seien* $A, B \subset H$*.*

1. *Sei* $d \in \mathrm{GGT}(A)$*. Dann ist* $\mathrm{GGT}(A) = [d]_\simeq$*. Ist* $\alpha\colon H \to H$ *eine Abbildung mit* $\alpha(a) \simeq a$ *für alle* $a \in H$*, so folgt* $\mathrm{GGT}(\alpha(A)) = \mathrm{GGT}(A)$*. Dasselbe gilt für* KGV *an Stelle von* GGT*.*
2. *Sei* $a \in \mathrm{GGT}(A)$ *und* $b \in \mathrm{GGT}(B)$*. Dann ist* $\mathrm{GGT}(A \cup B) = \mathrm{GGT}(a, b)$*. Insbesondere folgt: Ist* $\mathrm{GGT}(a, b) \neq \emptyset$ *für alle* $a, b \in H$*, so ist* $\mathrm{GGT}(E) \neq \emptyset$ *für jede endliche nichtleere Teilmenge* $E \subset H$*. Dasselbe gilt für* KGV *an Stelle von* GGT*.*
3. *Für* $e \in H$ *gilt:*
$$e \in \mathrm{KGV}(A) \iff eH = \bigcap_{a \in A} aH\,.$$
4. *Ist* $b \in H^\bullet$ *und* $\mathrm{GGT}(bA) \neq \emptyset$*, so folgt* $\mathrm{GGT}(bA) = b\,\mathrm{GGT}(A)$*.*
5. *Sei* $\mathrm{GGT}(A) \neq \emptyset$ *und* $d \in H^\bullet$*. Genau dann ist* $d \in \mathrm{GGT}(A)$*, wenn* $d \mid a$ *für alle* $a \in A$ *und* $\mathrm{GGT}(d^{-1}A) = H^\times$*.*

BEWEIS. 1. Aus Symmetriegründen genügt es, zu zeigen: Ist $d \in \mathrm{GGT}(A)$, $d' \simeq d$ und $\alpha\colon H \to H$ eine Abbildung mit $\alpha(a) \simeq a$ für alle $a \in H$, so ist $d' \in \mathrm{GGT}(\alpha(A))$.

Sei also $d \in \mathrm{GGT}(A)$, $d' \simeq d$ und $\alpha\colon H \to H$ eine Abbildung mit $\alpha(a) \simeq a$ für alle $a \in H$. Für alle $a \in A$ ist $d \mid a$, $a \mid \alpha(a)$, und wegen $d' \mid d$ folgt $d' \mid \alpha(a)$. Sei nun $g \in H$ und $g \mid \alpha(a)$ für alle $a \in A$. Für alle $a \in A$ ist dann $\alpha(a) \mid a$, also $g \mid a$, es folgt $g \mid d$ und wegen $d \mid d'$ auch $g \mid d'$.

Die Beweise für KGV sind analog.

2. $\subset$: Sei $d \in \mathrm{GGT}(A \cup B)$. Dann ist $d \mid x$ für alle $x \in A$, also $d \mid a$, und $d \mid y$ für alle $y \in B$, also $d \mid b$. Sei nun $g \in H$, $g \mid a$ und $g \mid b$. Dann folgt $g \mid z$ für alle $z \in A \cup B$ und daher $g \mid d$. Folglich ist $d \in \mathrm{GGT}(a, b)$.

$\supset$: Sei $d \in \mathrm{GGT}(a, b)$. Dann ist $d \mid a$, also $d \mid x$ für alle $x \in A$, und $d \mid b$, also $d \mid y$ für alle $y \in B$. Also ist $d \mid z$ für alle $z \in A \cup B$. Sei nun $g \in H$ und $g \mid z$ für alle $z \in A \cup B$. Dann folgt $g \mid a$ und $g \mid b$, also auch $g \mid d$. Folglich ist $d \in \mathrm{GGT}(A \cup B)$.

Ist $\mathrm{GGT}(a, b) \neq \emptyset$ für alle $a, b \in H$, so folgt $\mathrm{GGT}(E) \neq \emptyset$ für jede nichtleere endliche Teilmenge von H durch Induktion nach $|E|$.

Die Beweise für KGV sind analog.

3. $\Rightarrow$: Sei $e \in \mathrm{KGV}(A)$. Dann gilt für alle $x \in H$:
$$x \in \bigcap_{a \in A} aH \iff a \mid x \text{ für alle } a \in A \iff e \mid x \iff x \in eH\,.$$
$\Leftarrow$: Für alle $a \in A$ ist $e \in aH$, also $a \mid e$. Sei nun $g \in H$ und $a \mid g$ (also $g \in aH$) für alle $a \in A$. Dann folgt $g \in eH$, also $e \mid g$.

4. Sei $b \in H^\bullet$ und $d \in \mathrm{GGT}(bA)$. Dann is $d \,|\, ba$ für alle $a \in A$, und wegen $b \,|\, ba$ für alle $a \in A$ folgt $b \,|\, d$, also $d = bc$ mit $c \in H$.

$\subset$: Wir zeigen $c \in \mathrm{GGT}(A)$ (dann folgt $d = bc \in b\,\mathrm{GGT}(A)$). Für alle $a \in A$ ist $bc \,|\, ba$, also $c \,|\, a$. Sei $g \in H$ und $g \,|\, a$ für alle $a \in A$. Dann ist $gb \,|\, ba$ für alle $a \in A$, also $gb \,|\, d = bc$ und daher $g \,|\, c$.

$\supset$: Sei $e \in \mathrm{GGT}(A)$. Dann ist $e \,|\, a$, also $be \,|\, ba$ für alle $a \in A$ und daher $be \,|\, d = bc$, also auch $e \,|\, c$. Für alle $a \in A$ ist $d = bc \,|\, ba$, also $c \,|\, a$, und daher folgt $c \,|\, e$. Es folgt $e \simeq c$ und $be \in [bc]_\simeq = [d]_\simeq = \mathrm{GGT}(bA)$.

5. Sei $d \in \mathrm{GGT}(A)$. Dann ist $d \,|\, a$ für alle $a \in A$, und aus 4. folgt

$$dH^\times = \mathrm{GGT}(A) = \mathrm{GGT}(d(d^{-1}A) = d\,\mathrm{GGT}(d^{-1}A)\,, \quad \text{also} \quad H^\times = \mathrm{GGT}(d^{-1}A)\,.$$

Sei nun $d \,|\, a$ für alle $a \in A$ und $\mathrm{GGT}(d^{-1}A) = H^\times$. Dann folgt (wieder mit 4. wegen $\mathrm{GGT}(A) \neq \emptyset$) $\mathrm{GGT}(A) = \mathrm{GGT}(d(d^{-1}A)) = d\,\mathrm{GGT}(d^{-1}A) = dH^\times$. □

Definitionen und Bemerkungen 5.1.4.

1. Sei H eine reduzierte kommutative Halbgruppe. Dann ist H bezüglich der Teilbarkeitsrelation $|$ eine partiell geordnete Menge. Für jede Teilmenge $A \subset H$ ist dann $|\mathrm{GGT}(A)| \leq 1$ und $|\mathrm{KGV}(A)| \leq 1$. In diesem Falle schreiben wir $\mathrm{ggT}(A) = d$ an Stelle von $\mathrm{GGT}(A) = \{d\}$ und $\mathrm{kgV}(A) = e$ an Stelle von $\mathrm{KGV}(A) = \{e\}$. Es ist dann $\mathrm{ggT}(A) = \inf_{|}(A)$ und $\mathrm{KGV}(A) = \sup_{|}(A)$.

Für $H = \mathbb{N}$ sind das die Bezeichnungen in der Einleitung. Für $A \subset \mathbb{Z}$ gilt mit den Bezeichnungen der Einleitung $\mathrm{GGT}(A) = \{\pm\,\mathrm{ggT}(A)\}$ und $\mathrm{KGV}(A) = \{\pm\,\mathrm{kgV}(A)\}$.

2. Ein Monoid H heißt GGT-*Monoid*, wenn $\mathrm{GGT}(a, b) \neq \emptyset$ für alle $a, b \in H$ (nach Lemma 5.1.3 ist dann $\mathrm{GGT}(E) \neq \emptyset$ für jede nichtleere endliche Menge $E \subset H$).

3. Sei R ein Bereich. Dann ist $(R, \cdot)$ eine kommutative multiplikative Halbgrupe, und $R^\bullet$ ist ein Monoid. Für $a, b \in R$ gilt:

$$a \,|_R b \iff Rb \subset Ra \iff a \,|_{R^\bullet} b \text{ oder } b = 0\,. \text{ Insbesondere: } 0 \,|\, a \iff a = 0\,.$$

Damit folgt:

- $\mathrm{GGT}_R(\emptyset) = \{0\}$, $\mathrm{GGT}_{R^\bullet}(\emptyset) = \emptyset$, und $\mathrm{KGV}_R(\emptyset) = \mathrm{KGV}_{R^\bullet}(\emptyset) = R^\times$;
- für jede Teilmenge $A \subset R$ ist $\mathrm{GGT}_R(A \cup \{0\}) = \mathrm{GGT}_R(A)$ und $\mathrm{KGV}_R(A \cup \{0\}) = \{0\}$;
- für jede Teilmenge $\emptyset \neq A \subset R^\bullet$ ist $\mathrm{GGT}_{R^\bullet}(A) = \mathrm{GGT}_R(A)$ und $\mathrm{KGV}_{R^\bullet}(A) = \mathrm{KGV}_R(A)$.

4. Alle im Folgenden für Monoide definierten Begriffe der Teilbarkeitslehre werden für Bereiche übernommen, indem man sie auf das multiplikative Monoid des Bereiches anwendet (beispielsweise ist ein Bereich R genau dann ein GGT-Bereich, wenn $R^\bullet$ ein GGT-Monoid ist). Auf Grund von 3. spielt die Null für die Teilbarkeitslehre eine triviale Rolle..

5. Sei R ein Bereich, und seien a, b, $d \in R$. Genau dann ist $d \in \mathrm{GGT}_R(a, b)$, wenn dR das kleinste $\{a, b\}$ umfassende Hauptideal ist. Insbesondere ist jeder Hauptidealbereich ein GGT-Bereich.

6. Sei $R = \mathbb{Z}[\sqrt{-5}]$, $a = 6$ und $b = 2(1 + \sqrt{-5})$. Dann ist $\mathrm{GGT}(a, b) = \emptyset$: siehe Proseminar.

Satz 5.1.5. *Sei H ein* GGT-*Monoid, und seien a, b, c, $b_1, \ldots, b_n \in H$.*

1. *Sei $a \,|\, bc$. Dann ist $a = b'c'$ mit b', $c' \in H$, so dass $b' \,|\, b$ und $c' \,|\, c$.*
   Insbesondere gilt: Ist $\mathrm{GGT}(a, b) = H^\times$, so folgt $a \,|\, c$.
2. *Ist $\mathrm{GGT}(a, b_j) = H^\times$ für alle $j \in [1, n]$, so folgt $\mathrm{GGT}(a, b_1 \cdot \ldots \cdot b_n) = H^\times$.*
3. *Ist $\mathrm{GGT}(a, b) = H^\times$, so folgt $\mathrm{GGT}(a^k, b^l) = H^\times$ für alle $k, l \in \mathbb{N}$.*
4. (Reduzierte Bruchdarstellung) *Jedes $x \in \mathfrak{q}(H)$ hat eine Darstellung $x = a^{-1}b$ mit teilerfremden a, $b \in H$. Dabei sind $[a]_\simeq$ und $[b]_\simeq$ durch x eindeutig bestimmt.*

BEWEIS. 1. Sei $b' \in \mathrm{GGT}(a,b)$, und sei $c' \in H$ mit $a = b'c'$. Dann ist $b'c \in \mathrm{GGT}(ac,bc)$ und daher $b'\mathrm{GGT}(c',c) = \mathrm{GGT}(a,b'c) = \mathrm{GGT}(a,\, ac,\, bc) = aH^\times = b'c'H^\times$. Also ist $\mathrm{GGT}(c',c) = c'H^\times$ und somit $c' \mid c$. Ist insbesondere $b' \in H^\times$, so folgt $a \simeq c'$ und daher $a \mid c$.

2. folgt aus 1. mittels Induktion nach n, und 3. folgt durch zweimalige Anwendung von 2.

4. Sei $x \in \mathfrak{q}(H)$, $x = a_1^{-1}b_1$ mit $a_1, b_1 \in H$, und sei $d \in \mathrm{GGT}(a_1,b_1)$. Dann folgt $a = d^{-1}a_1 \in H$, $b = d^{-1}b_1 \in H$, $x = a^{-1}b$ und $\mathrm{GGT}(a,b) = H^\times$ nach Satz 5.1.3.5. Seien nun auch $a', b' \in H$ mit $x = a'^{-1}b'$ und $\mathrm{GGT}(a',b') = H^\times$. Dann folgt $ab' = a'b$, und mit 1. erhalten wir $a \mid a'$, $a' \mid a$, $b \mid b'$ und $b' \mid b$, also $a \simeq a'$ und $b \simeq b'$. □

Satz 5.1.6. *Sei H ein Monoid, und seien $a, b \in H$.*

1. *Ist $e \in \mathrm{KGV}(a,b)$, so folgt $e^{-1}ab \in \mathrm{GGT}(a,b)$.*
2. *Sei H ein* GGT*-Monoid. Dann ist $\mathrm{KGV}(a,b) \neq \emptyset$, und $\mathrm{GGT}(a,b)\,\mathrm{KGV}(a,b) = abH^\times$.*

BEWEIS. 1. Sei $e \in \mathrm{KGV}(a,b)$. Dann ist $a = (e^{-1}ab)(b^{-1}e)$ und $b = (e^{-1}ab)(a^{-1}e)$, also $e^{-1}ab \mid a$ und $e^{-1}ab \mid b$. Sei nun $g \in H$ mit $g \mid a$ und $g \mid b$. Dann ist $a \mid g^{-1}ab$ und $b \mid g^{-1}ab$, also auch $e \mid g^{-1}ab$, und es folgt $g \mid e^{-1}ab$. Daher ist $e^{-1}ab \in \mathrm{GGT}(a,b)$.

2. Sei $d \in \mathrm{GGT}(a,b)$. Es genügt nun, $d^{-1}ab \in \mathrm{KGV}(a,b)$ zu zeigen. Wegen $d^{-1}ab = a(d^{-1}b) = b(d^{-1}a)$ folgt $a \mid d^{-1}ab$ und $b \mid d^{-1}ab$. Sei $g \in H$ mit $a \mid g$ und $b \mid g$. Dann folgt $d^{-1}a \mid d^{-1}g = (d^{-1}b)(b^{-1}g)$. Nach Satz 5.1.3.5 ist $\mathrm{GGT}(d^{-1}a, d^{-1}b) = H^\times$, und aus Satz 5.1.5.1 folgt $d^{-1}a \mid b^{-1}g$, also $abd^{-1} \mid g$. □

5.2. Atomische und faktorielle Monoide und Bereiche

Definition 5.2.1. Sei H ein Monoid.

1. Ein Element $p \in H \setminus H^\times$ heißt
   - *unzerlegbar* (*irreduzibel,* ein *Atom*), wenn für alle $a, b \in H$ gilt:
     Aus $p = ab$ folgt $a \in H^\times$ oder $b \in H^\times$.
   - *prim* (ein *Primelement*), wenn für alle $a, b \in H$ gilt:
     Aus $p \mid ab$ folgt $p \mid a$ oder $p \mid b$.
2. Das Monoid H heißt
   - *atomisch*, wenn es zu jedem $a \in H$ ein $n \in \mathbb{N}_0$ und Atome $p_1, \ldots, p_n \in H$ gibt mit $a \simeq p_1 \cdot \ldots \cdot p_n$.
   - *faktoriell*, wenn es zu jedem $a \in H$ ein $n \in \mathbb{N}_0$ und Primelemente $p_1, \ldots, p_n \in H$ gibt mit $a \simeq p_1 \cdot \ldots \cdot p_n$.

   Ist R ein Bereich, so nennen wir (gemäß den Bemerkungen 5.1.4) ein Element $p \in R$ ein Atom bzw. ein Primelement, wenn p ein Atom bzw. ein Primelement von $R^\bullet$ ist, und wir nennen den Bereich R atomisch bzw. faktoriell, wenn das Monoid $R^\bullet$ atomisch bzw. faktoriell ist.

Satz 5.2.2. *Sei H ein Monoid.*

1. *Jedes Primelement von H ist ein Atom. Ist H ein* GGT*-Monoid, so ist jedes Atom von H prim. Insbesondere ist jedes atomische* GGT*-Monoid faktoriell.*
2. *Seien $m, n \in \mathbb{N}_0$ und $p_1, \ldots, p_m, q_1, \ldots, q_n \in H$ Primelemente mit $p_1 \cdot \ldots \cdot p_m \simeq q_1 \cdot \ldots \cdot q_n$. Dann ist $m = n$, und im Falle $m > 0$ existiert eine Permutation $\rho \in \mathfrak{S}_m$, so dass $q_{\rho(i)} \simeq p_i$ für alle $i \in [1,m]$.*

   Sprechweise: Die Darstellung eines Elementes von H als Produkt von Primelementen ist eindeutig bis auf die Reihenfolge und bis auf Assoziierte.

BEWEIS. 1. Sei $p \in H$ ein Primelement, und seien $a, b \in H$ mit $p = ab$. Dann folgt $p \,|\, ab$, also $p \,|\, a$ oder $p \,|\, b$, und wir können ohne Einschränkung $p \,|\, a$ annehmen. Dann existiert ein $c \in H$ mit $a = pc$, und es folgt $p = ab = pcb$, also $1 = cb$ und somit $b \in H^\times$.

Sei nun H ein GGT-Monoid, sei $p \in H$ ein Atom, und seien $a, b \in H$ mit $p \,|\, ab$. Nach Satz 5.1.5.1 ist dann $p = a'b'$ mit $a', b' \in H$, so dass $a' \,|\, a$ und $b' \,|\, b$. Da p ein Atom ist, folgt $a' \in H^\times$ oder $b' \in H^\times$. Ist $a' \in H^\times$, so folgt $p \simeq b'$ und daher $p \,|\, b$. Ist $b' \in H^\times$, so folgt in gleicher Weise $p \,|\, a$.

2. Induktion nach m. Im Falle $m = 0$ folgt $q_1 \cdot \ldots \cdot q_n \simeq 1$, also $n = 0$.

$m \geq 1\,,\ m-1 \to m\colon$ Es ist $p_1 \,|\, q_1 \cdot \ldots \cdot q_n$, und daher existiert ein $j \in [1, n]$ mit $p_1 \,|\, q_j$, also $q_j = p_1 e$ mit $e \in H$. Nach 1. ist q_j irreduzibel, und wegen $p_1 \notin H^\times$ folgt $e \in H^\times$ und somit $p_1 \simeq q_j$, also $p_2 \cdot \ldots \cdot p_m \simeq q_1 \cdot \ldots \cdot q_{j-1} q_{j+1} \cdot \ldots \cdot q_n$. Nach Induktionsvoraussetzung folgt $m = n$, im Falle $m = 1$ ist nichts mehr zu zeigen, und im Falle $m \geq 2$ gibt es eine bijektive Abbildung $\rho'\colon [2, m] \to [1, m] \setminus \{j\}$, so dass $q_{\rho'(i)} \simeq p_i$ für alle $i \in [2, m]$. Definiert man $\rho \in \mathfrak{S}_m$ durch $\rho(1) = j$ und $\rho \,|\, [2, m] = \rho'$, so folgt die Behauptung. □

Bemerkungen 5.2.3. Sei H ein Monoid, und seien $p, p' \in H$.

1. Ist $p \simeq p'$, so ist p' genau dann ein Atom (bzw. prim), wenn p ein Atom (bzw. prim) ist [das folgt unmittelbar aus der Definition und Lemma 5.1.2.8].

Insbesondere gilt:

- p ist genau dann ein Atom (bzw. prim), wenn $[p]_\simeq \in H/\simeq$ ein Atom (bzw. prim) ist.
- H ist genau dann atomisch (bzw. faktoriell), wenn $H/\simeq$ atomisch (bzw. faktoriell) ist.

2. Genau dann ist H faktoriell (bzw. atomisch), wenn jedes $a \in H \setminus H^\times$ eine Darstellung als Produkt endlich vieler Primelemente (bzw. Atome) besitzt. [das folgt mittels 1.]

3. Ist $p \in H$ prim, $n \in \mathbb{N}$, und sind $a_1, \ldots, a_n \in H$ mit $p \,|\, a_1 \cdot \ldots \cdot a_n$, so existiert ein $i \in [1, n]$ mit $p \,|\, a_i$. [Beweis durch Induktion nach n].

Satz 5.2.4. *Sei R ein Bereich und $p \in R^\bullet$*

1. *Genau dann ist p ein Primelement, wenn pR ein Primideal ist.*
2. *Genau dann ist p ein Atom, wenn pR (bzgl. $\subset$) maximal in der Menge aller Hauptideale von R ist.*

BEWEIS. Offensichtlich auf Grund der Definitionen. □

Satz 5.2.5. *Jeder noethersche Bereich ist atomisch, und jeder Hauptidealbereich ist faktoriell.*

BEWEIS. Wir nehmen an, R sei ein nicht atomischer noetherscher Bereich. Dann ist

$$\Omega = \{aR \mid a \in R^\bullet \setminus R^\times \text{ ist nicht Produkt von Atomen}\}$$

eine nichtleere Menge von Idealen und besitzt daher ein maximales Element aR. Wegen $aR \in \Omega$ ist a kein Atom, also $a = bc$ mit $b, c \in R^\bullet \setminus R^\times$. Dann ist aber $aR \subsetneq bR$ und $aR \subsetneq cR$, also $bR \notin \Omega$ und $cR \notin \Omega$. Daher sind b und c beide Produkte endlich vieler Atome, und folglich gilt das auch für a, im Widerspruch zu $aR \in \Omega$.

Ist R ein Hauptidealbereich, so ist R ein noetherscher GGT-Bereich und daher faktoriell nach 1. und Satz 5.2.2.1. □

Satz 5.2.6. *Sei H ein Monoid und $\varphi\colon H \to \mathbb{N}$ ein Homomorphismus, so dass $\varphi(a) > 1$ für alle $a \in H \setminus H^\times$. Dann ist H atomisch. Insbesondere ist jedes Untermonoid von $\mathbb{N}$ atomisch.*

BEWEIS. Durch Widerspruch. Sei Ω die Menge aller $a \in H \setminus H^\times$, welche nicht Produkt von Atomen sind, sei $n = \min(\varphi(\Omega))$, und $a \in \Omega$ mit $n = \varphi(a)$. Dann ist a kein Atom und daher $a = bc$ mit $b, c \in H \setminus H^\times$, also $\varphi(b) > 1$, $\varphi(c) > 1$ und $n = \varphi(a) = \varphi(b)\varphi(c)$. Wegen der Minimalität von n sind b und c beide Produkte von Atomen, und daher ist auch a ein Produkt von Atomen. Widerspruch!

Ist $H \subset \mathbb{N}$ eine Unterhalbgruppe, so hat die Inklusionsabbildung $\varphi = (H \hookrightarrow N)$ die geforderte Eigenschaft. □

Bemerkungen 5.2.7. 1. Nach Satz 1.1.3 ist $\mathbb{N}$ ein faktorielles Monoid. Wegen $(\mathbb{Z}, \cdot)_{\mathrm{red}} \cong \mathbb{N}$ ist daher auch $(\mathbb{Z}, \cdot)$ ein faktorielles Monoid, also $\mathbb{Z}$ ein faktorieller Bereich. Da $\mathbb{Z}$ ein Hauptidealbereich ist, folgt das auch aus Satz 5.2.5.

2. Das Monoid $H = 1 + 4\mathbb{N}_0 \subset \mathbb{N}$ ist ein Untermonoid von $\mathbb{N}$ und daher atomisch nach Satz 5.2.6. Die Zahlen 9, 21 und 49 sind offensichtlich Atome von H, aber wegen $441 = 21 \cdot 21 = 9 \cdot 49$ sind diese Zahlen keine Primelemente von H. Außerdem sind die angegebenen Zerlegungen von 441 die einzigen Zerlegungen in Atome. Daher besitzt 449 keine Darstellung als Produkt von Primelementen, und H ist nicht faktoriell.

Satz 5.2.8. *Sei H ein Monoid. Dann sind äquivalent*:

(a) *H ist faktoriell.*

(b) *Zu jedem $a \in H$ gibt es ein $n \in \mathbb{N}_0$ und Primelemente $p_1, \ldots, p_n \in H$, so dass $a \simeq p_1 \cdot \ldots \cdot p_n$, und diese Darstellung ist eindeutig bis auf die Reihenfolge und bis auf Assoziierte.*

(c) *Zu jedem $a \in H$ gibt es ein $n \in \mathbb{N}_0$ und Atome $p_1, \ldots, p_n \in H$, so dass $a \simeq p_1 \cdot \ldots \cdot p_n$, und diese Darstellung ist eindeutig bis auf die Reihenfolge und bis auf Assoziierte.*

(d) *H ist atomisch, und jedes Atom ist prim.*

BEWEIS. (a) ⇒ (b) ⇒ (c) Nach Satz 5.2.2.

(c) ⇒ (d) Wir müssen zeigen, dass jedes Atom von H prim ist. Sei $p \in H$ ein Atom, und seien $a, b \in H$ mit $p \mid ab$, also $ab = pc$ mit $c \in H$. Seien $n, m, k \in \mathbb{N}_0$ und $p_1, \ldots, p_n, q_1, \ldots, q_m, r_1, \ldots, r_k$ Atome mit $a \simeq p_1 \cdot \ldots \cdot p_n$, $b \simeq q_1 \cdot \ldots \cdot q_m$ und $c \simeq r_1 \cdot \ldots \cdot r_k$. Dann ist

$$ab \simeq p_1 \cdot \ldots \cdot p_n q_1 \cdot \ldots \cdot q_m \simeq p r_1 \cdot \ldots \cdot r_k \,,$$

und wegen der Eindeutigkeit der Darstellung existiert ein $\varepsilon \in R^\times$ mit $p\epsilon \in \{p_1, \ldots, p_n, q_1, \ldots, q_m\}$, also $p \mid a$ oder $p \mid b$.

(d) ⇒ (a) Nach Definition. □

Bemerkung und Definition 5.2.9. Die Eindeutigkeitsaussage in Satz 5.2.8(b) gestattet eine Neuformulierung unter Verwendung der Schreibweise aus Bemerkung 2.1.9.3. wie folgt.

Sei H ein faktorielles Monoid. Eine Menge $\mathcal{P} \subset H$ heißt *Repräsentantensystem der Primelemente* von H, wenn es zu jedem Primelement $p \in H$ genau ein $p_0 \in \mathcal{P}$ gibt mit $p \simeq p_0$. Dann hat jedes $a \in H$ eine eindeutige Darstellung in der Form

$$a = \varepsilon \prod_{p \in \mathcal{P}} p^{k_p} \quad \text{mit} \quad \varepsilon \in H^\times \quad \text{und einer Familie} \quad (k_p)_{p \in \mathcal{P}} \quad \text{in} \quad \mathbb{N}_0, \text{ so dass} \quad k_p = 0 \quad \text{für fast alle} \quad p \in \mathcal{P} \,.$$

Ist R ein faktorieller Bereich (also $R^\bullet$ ein faktorielles Monoid), so verstehen wir (wie üblich) unter einem Repräsentantensystem der Primelemente von R ein Repräsentantensystem der Primelemente von $R^\bullet$. Offensichtlich ist $\mathbb{P}$ ein Repräsentantensystem der Primelemente von $\mathbb{Z}$.

Definition und Satz 5.2.10. *Sei H ein faktorielles Monoid und $\mathcal{P} \subset H$ ein Repräsentantensystem der Primelemente von H. Dann hat jedes $a \in \mathsf{q}(H)$ eine eindeutige Darstellung in der Form*

$$a = \varepsilon \prod_{p \in \mathcal{P}} p^{k_p} \quad \textit{mit} \quad \varepsilon \in H^\times \quad \textit{und einer Familie} \quad (k_p)_{p \in \mathcal{P}} \quad \textit{in} \quad \mathbb{Z}, \textit{ so dass} \quad k_p = 0 \quad \textit{für fast alle} \quad p \in \mathcal{P},$$

und genau dann ist $a \in H$, wenn $\mathsf{v}_p(a) \geq 0$ für alle $p \in \mathcal{P}$.

Man nennt $\mathsf{v}_p(a) = k_p \in \mathbb{Z}$ den *p-adischen Exponenten* von a.

Für alle $p \in \mathcal{P}$ ist $\mathsf{v}_p \colon \mathsf{q}(H) \to \mathbb{Z}$ ein Gruppenhomomorphismus.

Beweis. Nach 5.2.9 genügt es, die Eindeutigkeit zu zeigen. Sei also

$$\varepsilon \prod_{p \in \mathcal{P}} p^{k_p} = \varepsilon' \prod_{p \in \mathcal{P}} p^{k'_p} \quad \text{mit} \quad \varepsilon, \varepsilon' \in H^\times, \ k_p, k'_p \in \mathbb{Z} \ \text{ und } \ k_p = k'_p = 0 \ \text{ für fast alle } \ p \in \mathcal{P}.$$

Dann folgt

$$\varepsilon \prod_{\substack{p \in \mathcal{P} \\ k_p > k'_p}} p^{k_p - k'_p} = \varepsilon' \prod_{\substack{p \in \mathcal{P} \\ k_p < k'_p}} p^{k'_p - k_p} \ \in H,$$

und aufgrund der Eindeutigkeitsaussage in 5.2.9 sind beide Produkte leer. □

Satz 5.2.11. *Sei H ein faktorielles Monoid und $\mathcal{P}$ ein Repräsentantensystem der Primelemente.*

1. *Seien $a, b \in H$.*
   (a) $a \mid b \iff \mathsf{v}_p(a) \leq \mathsf{v}_p(b)$ *für alle $p \in \mathcal{P}$.*
   (b) *Für $q \in \mathcal{P}$ gilt:* $q \mid a \iff \mathsf{v}_q(a) > 0$.
2. *Sei $\emptyset \neq A \subset H$. Dann ist*

$$d = \prod_{p \in \mathcal{P}} p^{\min\{\mathsf{v}_p(a) \mid a \in A\}} \ \in \ \mathrm{GGT}(A).$$

   Insbesondere ist H ein GGT-*Monoid.*

Beweis. 1.(a) $\Rightarrow$: Sei $c \in H$ mit $b = ac$. Dann existieren $\varepsilon_a, \varepsilon_b, \varepsilon_c \in H^\times$ mit

$$\varepsilon_b \prod_{p \in \mathcal{P}} p^{\mathsf{v}_p(b)} = b = ac = \varepsilon_a \prod_{p \in \mathcal{P}} p^{\mathsf{v}_p(a)} \varepsilon_c \prod_{p \in \mathcal{P}} p^{\mathsf{v}_p(c)} = \varepsilon_a \varepsilon_c \prod_{p \in \mathcal{P}} p^{\mathsf{v}_p(a) + \mathsf{v}_p(c)}.$$

Wegen der Eindeutigkeit der Darstellung erhalten wir $\mathsf{v}_p(b) = \mathsf{v}_p(a) + \mathsf{v}_p(c) \geq \mathsf{v}_p(a)$ für alle $p \in \mathcal{P}$.

$\Leftarrow$: Für $p \in \mathcal{P}$ sei $k_p = \mathsf{v}_p(b) - \mathsf{v}_p(a) \in \mathbb{N}_0$. Dann ist $k_p = 0$ für fast alle $p \in P$, also

$$c = \varepsilon_b \varepsilon_a^{-1} \prod_{p \in \mathcal{P}} p^{k_p} \in H, \quad \text{und} \quad b = ac.$$

1.(b) Für $p, q \in \mathcal{P}$ ist $\mathsf{v}_p(q) = 1$, falls $p = q$, und $\mathsf{v}_p(q) = 0$ sonst. Daher folgt die Aussage aus 1.(a).

2. Für $p \in \mathcal{P}$ ist $\mathsf{v}_p(d) = \min\{\mathsf{v}_p(a) \mid a \in A\} \leq \mathsf{v}_p(c)$ für alle $c \in A$. Daher folgt $d \mid a$ für alle $a \in A$. Sei nun $g \in H$ und $g \mid a$ für alle $a \in A$. Für alle $p \in \mathcal{P}$ und alle $c \in A$ ist dann $\mathsf{v}_p(g) \leq \mathsf{v}_p(c)$, also auch $\mathsf{v}_p(g) \leq \mathsf{v}_p(d)$ und daher $g \mid d$. □

Beispiel 5.2.12. Sei $d \in \mathbb{Z}$ kein Quadrat, $\sqrt{d} \in \mathbb{C}$ und $R_d = \mathbb{Z}[\sqrt{d}] = \{a + b\sqrt{d} \mid a, b \in \mathbb{Z}\} \subset \mathbb{C}$ (siehe Satz 3.4.6).

1. Nach 3.4.6 ist $\mathcal{N} \mid R^\bullet \colon R^\bullet \to \mathbb{N}$ ein Homomorphismus, so dass $\mathcal{N}(\alpha) > 1$ für alle $\alpha \in R^\bullet \setminus R^\times$. Also ist R_d atomisch nach Satz 5.2.6.

2. Ist $d \in \{-2, -1, 2, 3\}$, so ist R_d ein Hauptidealbereich und daher faktoriell.

3. Sei $d < -2$. Dann ist $2 \in R_d$ ein Atom, aber kein Primelement. Daher ist R_d nicht faktoriell und auch kein Hauptidealbereich.

[Beweis: Sei $d = -m$ mit $m \in \mathbb{N}_{\geq 3}$. Ist m gerade, so ist $2 \mid (\sqrt{-m})^2$, aber $2 \nmid \sqrt{-m}$. Ist m ungerade, so ist 2 ein Teiler von $1 + m = (1 + \sqrt{-m})(1 - \sqrt{-m})$, aber $2 \nmid 1 + \sqrt{-m}$ und $2 \nmid 1 - \sqrt{-m}$. Daher ist 2 kein Primelement von R.

Wir nehmen nun an, 2 sei kein Atom von R. Dann gibt es ein $\alpha \in R^\bullet \setminus R^\times$ mit $\alpha \mid 2$ und $\alpha \not\simeq 2$. Dann ist $1 < \mathcal{N}(\alpha) < \mathcal{N}(2) = 4$ und $\mathcal{N}(\alpha) \mid_{\mathbb{N}} \mathcal{N}(2)$, also $\mathcal{N}(\alpha) = 2$. Ist $\alpha = a + b\sqrt{-m}$, so folgt $\mathcal{N}(\alpha) = a^2 + b^2 m = 2$, was wegen $m > 2$ unmöglich ist.]

5.3. Polynomringe über faktoriellen Ringen

In diesem Abschnitt sei $n \in \mathbb{N}$, für einen Bereich R seien $R[X]$ bzw. $R[X_1, \ldots, X_n]$ Polynomringe in einer bzw. n Unbestimmten und $\boldsymbol{X} = (X_1, \ldots, X_n)$.

Definition 5.3.1. Sei R ein Bereich. Ein Polynom $f \in R[\boldsymbol{X}]$ heißt *irreduzibel* (über R), wenn $f \notin R$ und für alle $f_1, f_2 \in R[\boldsymbol{X}]$ gilt: Aus $f = f_1 f_2$ folgt $f_1 \in R$ oder $f_2 \in R$.

Bemerkungen 5.3.2. Sei R ein Bereich.

1. Ist $f \in R[\boldsymbol{X}] \setminus R$ ein Atom von $R[\boldsymbol{X}]$, so ist f irreduzibel über R [Beweis: Es ist $R[\boldsymbol{X}]^\times = R^\times$ (Satz 3.5.2)]. Das Polynom $2X \in \mathbb{Z}[X]$ ist irreduzibel, aber kein Atom.

2. Sei $f \in R[X]$ und $c \in R$. Genau dann ist f irreduzibel über R, wenn das Polynom $f_1 = f(X + c)$ irreduzibel über R ist.

3. Sei $f \in R[X]$. Ist $\operatorname{gr}(f) = 1$, so ist f irreduzibel über R. Ist $\operatorname{gr}(f) \in \{2, 3\}$, so ist f genau dann irreduzibel über R, wenn $f(z) \neq 0$ für alle $z \in R$ [Beweis: Satz 3.6.5].

Satz 5.3.3. *Sei K ein Körper. Dann ist $K[X]$ faktoriell, jedes irreduzible Polynom ist ein Primelement von $K[X]$, und*

$$\mathcal{P} = \{f \in K[X] \mid f \text{ ist irreduzibel und normiert}\}$$

ist ein Repräsentantensystem der Primelemente von $K[X]$.

Beweis. Nach Satz 3.7.5 ist $K[X]$ ein Hauptidealbereich und daher faktoriell nach Satz 5.2.5. Nach Satz 3.5.2 ist $K[X]^\times = K^\times$, und daher ist ein Polynom $f \in K[X]$ genau dann irreduzibel über K, wenn f ein Atom (also ein Primelement) von $K[X]$ ist. Da es zu jedem $f \in K[X]^\bullet$ genau ein normiertes $f_0 \in K[X]$ mit $f \simeq f_0$ gibt, folgt die Behauptung. □

Satz 5.3.4 (Eisenstein'sches Irreduzibilitätskriterium)**.** *Sei R ein Bereich, $P \lhd R$ ein Primideal, $d \in \mathbb{N}$ und*

$$f = \sum_{\nu=0}^{d} a_\nu X^\nu \in R[X] \setminus R \quad \textit{mit} \quad a_\nu \in P \ \textit{für alle} \ \nu \in [0, d-1]\,, \ a_d \notin P \ \textit{und} \ a_0 \notin P^2\,.$$

Dann ist f irreduzibel über R.

Beweis. Sei $K = \mathfrak{q}(R/P)$ und $\pi\colon R[X] \to (R/P)[X] \hookrightarrow K[X]$ die kanonische Fortsetzung des Restklassenhomomorphismus $R \to R/P$ auf die Polynomringe. Sei $f = gh$ mit $g, h \in R[X]$, sei $k = \operatorname{gr}(f)$, $l = \operatorname{gr}(g)$, $a \in R$ der höchste Koeffizient von g und $b \in R$ der höchste Koeffizient von h. Dann ist $ab = a_d \notin P$, also $\pi(a)$ der höchste Koeffizient und k der Grad von $\pi(g)$, und $\pi(b)$ der höchste Koeffizient und l der Grad von $\pi(h)$. Es ist $\pi(f) = \pi(a_d)X^d = \pi(g)\pi(h)$, und da $K[X]$ faktoriell ist, folgt $\pi(g) = \pi(a)X^k$ und $\pi(h) = \pi(b)X^l$. Wir nehmen nun an, es sei $k > 0$ und $l > 0$. Dann folgt $g(0) \in P$, $h(0) \in P$, und $a_0 = f(0) = g(0)h(0) \in P^2$, ein Widerspruch. □

Beispiele 5.3.5.

1. Sei R ein Bereich, $p \in R$ ein Primelement, $d \in \mathbb{N}$ und $f = a_d X^d + a_{d-1} X^{d-1} + \ldots + a_0 \in R[X]$, so dass $p \,|\, a_\nu$ für alle $\nu \in [0, d-1]$, $p \nmid a_d$ und $p^2 \nmid a_0$. Dann ist f irreduzibel über R. [Beweis: Satz 5.3.4 mit $P = pR$].

2. Sei $p \in \mathbb{P}$, $a \in \mathbb{Z}$ mit $\mathsf{v}_p(a) = 1$ und $n \in \mathbb{N}$. Dann ist $f = X^n - a$ irreduzibel über $\mathbb{Z}$.

3. Sei K ein Körper. Dann ist T ein Primelement von $R = K[T]$, und daher ist für alle $n \in \mathbb{N}$ das Polynom $f = X^n - T \in R[X]$ irreduzibel über R.

4. Sei $p \in \mathbb{P}$ ungerade und

$$\Phi_p = \frac{X^p - 1}{X - 1} = X^{p-1} + X^{p-2} + \ldots + 1 \in \mathbb{Z}[X]\,.$$

Dann ist

$$\Psi = \Phi_p(X+1) = \frac{(X+1)^p - 1}{X} = \sum_{j=0}^{p-1} \binom{p}{j+1} X^j \in \mathbb{Z}[X]\,,$$

Ψ ist normiert, für alle $j \in [0, p-2]$ ist $p \,|\, \binom{p}{j+1}$ nach Satz 1.2.4, und $p^2 \nmid \Psi(0) = p$. Nach 1. ist Ψ irreduzibel über $\mathbb{Z}$, und nach Bemerkung 5.3.2.2 ist daher auch Φ_p irreduzibel über $\mathbb{Z}$.

Satz 5.3.6. *Sei R ein Bereich und $p \in R^\bullet$. Genau dann ist p ein Primelement von R, wenn p ein Primelement von $R[\boldsymbol{X}]$ ist.*

Beweis. Nach Satz 3.5.13 ist $R[\boldsymbol{X}]/pR[\boldsymbol{X}] \cong (R/pR)[\boldsymbol{X}]$, und daher gilt:

$$\begin{aligned} p \text{ ist ein Primelement von } R[\boldsymbol{X}] &\iff R[\boldsymbol{X}]/pR[\boldsymbol{X}] \text{ ist ein Bereich} \iff (R/pR)[\boldsymbol{X}] \text{ ist ein Bereich} \\ &\iff R/pR \text{ ist ein Bereich} \iff p \text{ ist ein Primelement von } R. \end{aligned}$$

□

Definition 5.3.7. Sei R ein Bereich, $K = \mathsf{q}(R)$ und

$$f = \sum_{\boldsymbol{\nu} \in \mathbb{N}_0^n} a_{\boldsymbol{\nu}} \boldsymbol{X}^{\boldsymbol{\nu}} \in K[\boldsymbol{X}]^\bullet \quad \text{mit} \quad \boldsymbol{X}^{\boldsymbol{\nu}} = X_1^{\nu_1} \cdot \ldots \cdot X_n^{\nu_n} \quad \text{für} \quad \boldsymbol{\nu} = (\nu_1, \ldots, \nu_n) \in \mathbb{N}_0^n\,.$$

Ein Element $d \in K^\times$ heißt *Inhalt* von f, wenn $d^{-1} a_\nu \in R$ für alle $\nu \in \mathbb{N}_0$, und

$$\mathrm{GGT}\big(\{d^{-1} a_\nu \mid \nu \in \mathbb{N}_0\,,\ a_\nu \neq 0\}\big) = R^\times\,.$$

Wir bezeichnen mit $\mathrm{cont}(f)$ die Menge aller Inhalte von f. Das Polynom f heißt *primitiv*, wenn $\mathrm{cont}(f) = R^\times$.

Satz 5.3.8. *Sei R ein faktorieller Bereich, $\mathcal{P}$ ein Repräsentantensystem der Primelemente von R, $K = \mathsf{q}(R)$, $f \in K[\boldsymbol{X}]^\bullet$ und $A \subset K^\times$ die Menge der von Null verschiedenen Koeffizienten von f. Für $p \in \mathcal{P}$ bezeichne $\pi_p \colon R[\boldsymbol{X}] \to (R/pR)[\boldsymbol{X}]$ die kanonische Fortsetzung des Restklassenhomomorphismus auf die Polynomringe.*

1. *Es ist*
$$\mathrm{cont}(f) = dR^\times \quad \textit{mit} \quad d = \prod_{p \in \mathcal{P}} p^{\min\{\mathsf{v}_p(a) \mid a \in A\}}\,.$$
Insbesondere ist genau dann $f \in R[\boldsymbol{X}]$, wenn $\mathrm{cont}(f) \subset R$, und dann ist $\mathrm{cont}(f) = \mathrm{GGT}(A)$.
2. *Sei $a \in K^\times$. Dann ist $\mathrm{cont}(af) = a\,\mathrm{cont}(f)$, und genau dann ist $a \in \mathrm{cont}(f)$, wenn $a^{-1} f$ primitiv ist.*
3. *Genau dann ist f primitiv, wenn $f \in R[\boldsymbol{X}]$ und $\pi_p(f) \neq 0$ für alle $p \in \mathcal{P}$.*

BEWEIS. 1. Sei $d \in K^\times$. Genau dann ist $d^{-1}a \in R$ für alle $a \in A$, wenn $\mathsf{v}_p(d^{-1}a) = -\mathsf{v}_p(d) + \mathsf{v}_p(a) \geq 0$ für alle $p \in \mathcal{P}$ und alle $a \in A$. Ist das der Fall, so ist genau dann $\mathrm{GGT}(d^{-1}A) = R^\times$, wenn $0 = \min\{-\mathsf{v}_p(d) + \mathsf{v}_p(a) \mid a \in A\}$ für alle $p \in \mathcal{P}$. Daher ist genau dann $d \in \mathrm{cont}(f)$, wenn $\mathsf{v}_p(d) = \min\{\mathsf{v}_p(a) \mid a \in A\}$.

2. Nach 1., denn aA ist die Menge der von Null verschiedenen Koeffizienten von af.

3. Sei $f \in R[\boldsymbol{X}]$. Für $p \in \mathcal{P}$ ist genau dann $\pi_p(f) = 0$, wenn $p \,|\, a$ für alle $a \in A$. Genau dann ist f primitiv, wenn es kein $p \in \mathcal{P}$ gibt, das alle $a \in A$ teilt, und das ist genau dann der Fall, wenn $\pi_p(f) \neq 0$ für alle $p \in \mathcal{P}$. Die übrigen Behauptungen sind aufgrund der Definition klar. □

Satz 5.3.9 (Gauß'sches Lemma)**.** *Sei R ein faktorieller Bereich, $K = \mathsf{q}(R)$ und $f, g \in K[\boldsymbol{X}]^\bullet$.*

1. $\mathrm{cont}(fg) = \mathrm{cont}(f)\,\mathrm{cont}(g)$.

   Insbesondere gilt: Sind f und g primitiv, so ist auch fg primitiv.
2. *Sei einer der Koeffizienten von f und einer der Koeffizienten von g in $R^\times$, und sei $fg \in R[\boldsymbol{X}]$. Dann folgt $f \in R[\boldsymbol{X}]$ und $g \in R[\boldsymbol{X}]$.*

BEWEIS. Sei $c \in \mathrm{cont}(f)$, $d \in \mathrm{cont}(g)$, $f_0 = c^{-1}f$ und $g_0 = d^{-1}g$. Dann sind $f_0, g_0 \in R[\boldsymbol{X}]$ primitiv. Sei $\mathcal{P}$ ein Repräsentantensystem der Primelemente von R. Für $p \in \mathcal{P}$ sei $\pi_p \colon R[\boldsymbol{X}] \to (R/pR)[\boldsymbol{X}]$ die kanonische Fortsetzung des Restklassenhomomorphismus auf die Polynomringe..

1. Für alle $p \in \mathcal{P}$ ist $\pi_p(f_0g_0) = \pi_p(f_0)\pi_p(g_0) \neq 0$ nach Satz 5.3.8. Daher ist f_0g_0 primitiv, und wegen $fg = cdf_0g_0$ ist $\mathrm{cont}(fg) = \mathrm{cont}\big(cd(f_0g_0)\big) = cdR^\times = \mathrm{cont}(f)\mathrm{cont}(g)$.

2. Nach Voraussetzung ist $c^{-1} \in R$, $d^{-1} \in R$ und $cd \in R$. Daher folgt $c = d^{-1}cd \in R$ und $d = c^{-1}cd \in R$, also $f, g \in R[\boldsymbol{X}]$. □

Satz 5.3.10 (Satz von Gauß)**.** *Sei R ein faktorieller Bereich und $K = \mathsf{q}(R)$.*

1. *Ein Polynom $f \in R[X]$ ist genau dann irreduzibel über R, wenn f irreduzibel über K ist.*
2. *Ein Polynom $q \in R[X]$ ist genau dann ein Primelement in $R[X]$, wenn eine der beiden folgenden Bedingungen erfüllt ist:*
   - *$q \in R$ ist ein Primelement von R.*
   - *q ist primitiv, und q ist irreduzibel über K.*
3. *$R[\boldsymbol{X}]$ ist faktoriell.*

BEWEIS. 1. Sei $f \in R[X] \setminus R$. Ist f irreduzibel über K, so ist f auch irreduzibel über R. Sei nun f reduzibel über K, $f = gh$ mit $g, h \in K[X] \setminus K$. Sei $c \in \mathrm{cont}(g)$ und $d \in \mathrm{cont}(h)$. Dann ist $c^{-1}g \in R[X]$, $d^{-1}h \in R[X]$ und $cd \in \mathrm{cont}(f) \subset R$. Wegen $f = [(cd)(c^{-1}g)](d^{-1}h)$ ist f reduzibel über R.

2. FALL 1: $q \in R$. Nach Satz 5.3.6

FALL 2 : $q \notin R$. Ist $q \in R[X]$ nicht primitiv, so ist $q = cq_0$ mit $c \in R^\bullet \setminus R^\times$ und $q_0 \in R[X] \setminus R$, also q kein Atom und daher kein Primelement in $R[X]$. Ist q reduzibel über K, so ist nach 1. q auch reduzibel über R und daher ebenfalls kein Primelement.

Sei nun q primitiv und irreduzibel über K, und seien $f, g \in R[X]$ mit $q \,|_{R[X]} fg$. Dann ist $q \,|_{K[X]} fg$, und nach Satz 5.3.3 ist $q \,|_{K[X]} f$ oder $q \,|_{K[X]} g$. Sei $q \,|_{K[X]} f$ und $h \in K[X]$ mit $f = qh$. Wegen $\mathrm{cont}(q) = R^\times$ folgt $\mathrm{cont}(h) = \mathrm{cont}(f) \subset R$ und daher $h \in R[X]$, also $q \,|_{R[X]} f$.

3. Es ist $R[\boldsymbol{X}] = R[X_1, \ldots, X_n] = R[X_1, \ldots, X_{n-1}][X_n]$. Daher genügt es, die Behauptung für $n = 1$ zu zeigen. Der allgemeine Fall folgt dann durch Induktion nach n.

Wir zeigen, dass jedes $f \in R[X]^\bullet \setminus R[X]^\times = R[X]^\bullet \setminus R^\times$ ein Produkt von Primelementen von $R[X]$ ist.

Sei also $f \in R[X]^\bullet \setminus R^\times$. Ist $f \in R$, so ist f ein Produkt von Primelementen von R und daher ein Produkt von Primelementen von $R[X]$. Sei also $f \in R[X] \setminus R$. Dann ist $f = f_1 \cdot \ldots \cdot f_r$ mit irreduziblen Polynomen $f_1, \ldots, f_r \in K[X]$. Für $i \in [1, r]$ sei $c_i \in \mathrm{cont}(f_i)$, und dann ist $q_i = c_i^{-1} f_i \in R[X]$ primitiv. Dann sind $q_1, \ldots, q_r$ Primelemente von $R[X]$ nach 2., und $f = c_1 \cdot \ldots \cdot c_r q_1 \cdot \ldots \cdot q_r$. Weil

$c_1 \cdot \ldots \cdot c_r \in \mathrm{cont}(c_1 \cdot \ldots \cdot c_r q_1 \cdot \ldots \cdot q_r) = \mathrm{cont}(f) \subset R$ ein Produkt von Primelementen von R ist, ist somit auch f ein Produkt von Primelementen von $R[X]$. □

Korollar 5.3.11. *Sei R ein faktorieller Bereich, $K = \mathsf{q}(R)$ und $K(\boldsymbol{X})$ ein rationaler Funktionenkörper. Dann hat jedes $h \in K(\boldsymbol{X})$ eine Darstellung $h = g^{-1}f$ mit zueinander teilerfremden $f, g \in R[\boldsymbol{X}]$. Dabei sind f und g bis auf Faktoren in $R^\times$ eindeutig bestimmt.*

Beweis. Nach Korollar 3.5.11 ist $K(\boldsymbol{X}) = \mathsf{q}(R[\boldsymbol{X}])$, und daher folgt die Behauptung aus Satz 5.1.5.4. □

Bemerkung 5.3.12. In der Schulmathematik nennt man die $f \in \mathbb{Z}[\boldsymbol{X}] = \mathbb{Z}[X_1, \ldots, X_n]$ *ganzzahlige Terme*, die $f \in \mathbb{Q}[\boldsymbol{X}]$ *rationalzahlige Terme* und die $h \in \mathbb{Q}(\boldsymbol{X})$ *Bruchterme* in den Unbestimmten $X_1, \ldots, X_n$. Nach Korollar 5.3.11 besitzt jedes $h \in \mathbb{Q}(\boldsymbol{X})$ eine Bruchdarstellung

$$j = \frac{f}{g} \quad \text{mit teilerfremden} \quad f, g \in \mathbb{Z}[\boldsymbol{X}]\,.$$

Dabei sind f und g wegen $\mathbb{Z}^\times = \{\pm 1\}$ bis auf das Vorzeichen eindeutig bestimmt.

CHAPTER 6

Körpertheorie

Konvention. Sei $R \neq \{0\}$ ein kommutativer Ring. Dann bezeichnen wir mit $R[X]$ bzw. $R[X_1, \ldots, X_n]$ stets Polynomringe über R. Ist $R \subset R'$ ein Teilring, so nehmen wir immer auch an, dass $R[X] \subset R'[X]$ bzw. $R[X_1, \ldots, X_n] \subset R'[X_1, \ldots, X_n]$.

6.1. Primringe und Primkörper

Definition und Satz 6.1.1. *Sei R ein Ring und $R_0 = \{m1_R \mid m \in \mathbb{Z}\} \subset R$.*

1. *R_0 ist der kleinste Teilring von R.*
2. *Es gibt genau einen Ringhomomorphismus $f\colon \mathbb{Z} \to R$. Dieser ist gegeben durch $f(m) = m1_R$ für alle $m \in \mathbb{Z}$, und es ist $f(\mathbb{Z}) = R_0$. Ist $\operatorname{Ker}(f) = n\mathbb{Z}$ mit $n \in \mathbb{N}_0$, so induziert f einen Ringisomorphismus $f^*\colon \mathbb{Z}/n\mathbb{Z} \to R_0$.*

   Insbesondere ist $R_0 \cong \mathbb{Z}/n\mathbb{Z}$, falls $n \in \mathbb{N}$, und $R_0 \cong \mathbb{Z}$, falls $n = 0$. Ist R ein Bereich, so ist $n \in \mathbb{P} \cup \{0\}$.

Der Ring R_0 heißt *Primring* und $n = \operatorname{char}(R)$ die *Charakteristik* von R. Ist $\operatorname{char}(R) = p \in \mathbb{P}$, so nennt man die Abbildung $\varphi\colon R \to R$, definiert durch $\varphi(x) = x^p$, die *Frobeniusabbildung* von R.

Beweis. Sei $f\colon \mathbb{Z} \to R$ definiert durch $f(m) = m1_R$. Dann ist $f(1) = 1_R$, und für alle $m, n \in \mathbb{Z}$ ist $(m+n)1_R = m1_R + n1_R$ und $(mn)1_R = (m1_R)(n1_R)$. Daher ist f ein Ringhomomorphismus und $R_0 = f(\mathbb{Z}) \subset R$ ein Teilring. Ist $\varphi\colon \mathbb{Z} \to R$ ein Ringhomomorphismus, so folgt $\varphi(m) = m\varphi(1) = m1_R$ für alle $m \in \mathbb{Z}$ und daher $\varphi = f$. Für jeden Teilring $R' \subset R$ ist $1_R \in R'$ und daher $R_0 \subset R'$. Folglich ist R_0 der kleinste Teilring von R.

Ist $\operatorname{Ker}(f) = n\mathbb{Z}$ mit $n \in \mathbb{N}_0$, so induziert f nach Satz 3.2.9.3 einen Ringisomorphismus $f^*\colon \mathbb{Z}/n\mathbb{Z} \xrightarrow{\sim} R_0$. Ist R ein Bereich, so ist auch $R_0 \cong \mathbb{Z}/n\mathbb{Z}$ ein Bereich und daher $n \in \mathbb{P} \cup \{0\}$ nach Satz 3.2.8. □

Bemerkung 6.1.2. Sei R ein Ring. Dann ist $\operatorname{ord}_{(R,+)}(1_R) = \infty$, falls $\operatorname{char}(R) = 0$, und es ist $\operatorname{ord}_{(R,+)}(1_R) = \operatorname{char}(R)$, falls $\operatorname{char}(R) > 0$. Insbesondere ist genau dann $\operatorname{char}(R) = 1$, wenn $R = \{0\}$.

Definition und Satz 6.1.3. *Sei K ein Körper, R_0 sein Primring und*

$$K_0 = \left\{ \frac{m1_K}{n1_K} \;\middle|\; m, n \in \mathbb{Z}\,,\ n1_K \neq 0_K \right\}.$$

1. *K_0 ist ein Quotientenkörper von R_0 und der kleinste Teilkörper von K.*
2. *Im Falle $\operatorname{char}(K) = p \in \mathbb{P}$ ist $K_0 = R_0 \cong \mathbb{Z}/p\mathbb{Z}$.*
3. *Im Falle $\operatorname{char}(K) = 0$ gibt es genau einen Körpermonomorphismus $f\colon \mathbb{Q} \to K$. Dieser ist gegeben durch*

$$f\Big(\frac{m}{n}\Big) = \frac{m1_K}{n1_K} \quad \text{für alle} \quad m, n \in \mathbb{Z} \quad \text{mit} \quad n \neq 0\,, \quad \text{und es ist} \quad f(\mathbb{Q}) = K_0\,.$$

Der Körper K_0 heißt *Primkörper* von K. Für $x \in K$ und $m \in \mathbb{Z}$ mit $m1_K \in K^\times$ definieren wir

$$\frac{x}{m} = \frac{1}{m}\, x = \frac{x}{m1_K}\,.$$

Ist $p \in \mathbb{P}$, so nennt man $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$ den *Primkörper* oder das *Galoisfeld* mit p Elementen.

BEWEIS. 1. Nach Bemerkung 3.3.7.2 ist K_0 ein Quotientenkörper von R_0, und es ist der kleinste R_0 umfassende Teilkörper von K. Ist $K' \subset K$ ein Teilkörper, so ist $R_0 \subset K'$ (nach Satz 6.1.1) und daher auch $K_0 \subset K'$. Daher ist K_0 der kleinste Teilkörper von K.

2. Im Falle $\mathrm{char}(K) = p \in \mathbb{P}$ ist $R_0 \cong \mathbb{Z}/p\mathbb{Z}$ ein Körper und daher $R_0 = K_0$.

3. Ist $\mathrm{char}(K) = 0$, so gibt es nach Satz 6.1.1 einen Ringisomorphismus $f_0 \colon \mathbb{Z} \xrightarrow{\sim} R_0$, und dieser besitzt nach Satz 3.3.6.5 eine Fortsetzung zu einem Monomorphismus $f \colon \mathbb{Q} \to K$. Wegen $f(1) = 1_K$ folgt

$$f\Big(\frac{m}{n}\Big) = \frac{f(m)}{f(n)} = \frac{m1_K}{n1_K} \quad \text{für alle } m\,, n \in \mathbb{Z} \text{ mit } n \neq 0\,.$$

Daher ist f eindeutig bestimmt, und $f(\mathbb{Q}) = K_0$. □

Satz 6.1.4. *Sei R ein kommutativer Ring, $\mathrm{char}(R) = p \in \mathbb{P}$, $R_0 \cong \mathbb{F}_p$ der Primring von R und $n \in \mathbb{N}$.*

1. *Für alle $x, y \in R$ und $n \in \mathbb{N}$ ist*

   $$(x+y)^{p^n} = x^{p^n} + y^{p^n}\,, \quad \text{und} \quad A_n = \{x \in R \mid x^{p^n} = x\} \quad \text{ist ein Teilring von } R.$$

   Insbesondere ist die Frobeniusabbildung $\varphi \colon R \to R$ ein Ringhomomorphismus. Ist R ein Bereich, so ist φ ein Monomorphismus.
2. *Die Abbildung $\wp \colon R \to R$, definiert durch $\wp(x) = x^p - x$, ist ein Endomorphismus der Additionsgruppe von R mit $R_0 \subset \mathrm{Ker}(\wp)$. Ist R ein Bereich, so ist $R_0 = \mathrm{Ker}(\wp)$.*

BEWEIS. 1. Nach Satz 1.2.4 ist

$$p \,\Big|\, \binom{p}{\nu} \quad \text{und daher} \quad \binom{p}{\nu} x = 0 \quad \text{für alle } \nu \in [1, p-1] \text{ und } x \in R\,.$$

Für $x, y \in R$ folgt

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

und damit $(x+y)^{p^n} = x^{p^n} + y^{p^n}$ (mittels Induktion nach n). Es ist $1 \in A_n$, und für alle $x, y \in A_n$ folgt $x - y \in A_n$ und $xy \in A_n$. Daher ist $A_n \subset R$ ein Teilring nach Lemma 3.1.4. Für alle $x, y \in R$ ist $\varphi(x+y) = (x+y)^p = x^p + y^p = \varphi(x) + \varphi(y)$ und $\varphi(xy) = (xy)^p = x^p y^p = \varphi(x)\varphi(y)$, also ist φ ein Ringhomomorphismus. Ist R ein Bereich, so ist $\mathrm{Ker}(\varphi) = \{x \in R \mid x^p = 0\} = \{0\}$ und daher φ ein Monomorphismus.

2. Für $x, y \in R$ ist $\wp(x+y) = (x+y)^p - (x+y) = x^p + y^p - x - y = \wp(x) + \wp(y)$, also $\wp \colon R \to R$ ein Endomorphismus. Es ist $R_0 \cong \mathbb{F}_p$, und nach Satz 4.2.5 ist $\mathbb{F}_p^\times$ eine zyklische Gruppe mit $|\mathbb{F}_p^\times| = p - 1$. Daher ist $x^{p-1} = 1$ für alle $x \in \mathbb{F}_p^\times$ und $x^p = x$ (also $\wp(x) = 0$) für alle $x \in \mathbb{F}_p$. Ist R ein Bereich, so hat das Polynom $X^p - X \in R[X]$ nach Satz 3.6.7 in R höchstens p Nullstellen, und daher ist $\mathrm{Ker}(\wp) = R_0$. □

Satz 6.1.5. *Sei R ein Bereich und $f \in R[X]$.*

1. *Ist $\mathrm{char}(R) = 0$, so ist genau dann $f' = 0$, wenn $f \in R$.*
2. *Ist $\mathrm{char}(R) = p \in \mathbb{P}$, so ist genau dann $f' = 0$, wenn es ein Polynom $g \in R[X]$ gibt, so dass $f = g(X^p)$.*

BEWEIS. Sei $f \in R[X]$, also

$$f = \sum_{\nu \geq 0} a_\nu X^\nu \quad \text{mit} \quad a_\nu \in R\,,\ a_\nu = 0 \ \text{ für fast alle } \ \nu \in \mathbb{N}_0\,, \quad \text{und} \quad f' = \sum_{\nu \geq 1} \nu a_\nu X^{\nu-1}\,.$$

Genau dann ist $f' = 0$, wenn $\nu a_\nu = (\nu 1_R) a_\nu = 0$ für alle $\nu \in \mathbb{N}_0$. Im Falle $\mathrm{char}(R) = 0$ ist das genau dann der Fall, wenn $a_\nu = 0$ für alle $\nu \geq 1$, also $f = a_0 \in R$. Im Falle $\mathrm{char}(R) = p \in \mathbb{P}$ ist das genau dann der Fall, wenn $a_\nu = 0$ für alle $\nu \in \mathbb{N}_0$ mit $p \nmid \nu$, wenn also

$$f = g(X^p) \quad \text{mit} \quad g = \sum_{\nu \geq 0} a_{p\nu} X^\nu\,.$$

□

6.2. Körpererweiterungen

Definition 6.2.1.

1. Sei R ein Ring und $K \subset R$ ein Teilkörper. Dann ist
$$K \times R\,, \quad (a,x) \mapsto ax$$
eine K-lineare Struktur auf R und damit R ein K-Vektorraum. Die Dimension
$$[R\!:\!K] = \dim_K(R) \in \mathbb{N} \cup \{\infty\}$$
heißt *Grad* von R über K. Unter einer *K-Basis* von R versteht man eine (geordnete) K-Vektorraumbasis von R.
2. Unter einer *Körpererweiterung* L/K versteht man ein Paar von Körpern $K \subset L$, wobei K ein Teilkörper von L ist. Man nennt dann L einen *Erweiterungskörper* von K und $[L\!:\!K]$ den *Grad* der Körpererweiterung L/K. Unter einem *Zwischenkörper* von L/K versteht man einen Teilkörper $M \subset L$ mit $K \subset M$ (kurz: $K \subset M \subset L$ seien Körper).
3. Eine Körpererweiterung L/K heißt *endlich*, wenn $[L\!:\!K] < \infty$.

Bemerkungen 6.2.2.

1. Sei L/K eine Körpererweiterung. Genau dann ist $[L\!:\!K] = 1$, wenn $L = K$ (und dann ist (1) eine K-Basis von K).

2. Ist L/K eine Körpererweiterung, $n = [L\!:\!K] \in \mathbb{N}$, und $(u_1, \ldots, u_n)$ eine K-Basis von L, so ist für jedes $x \in L^\times$ auch $(xu_1, \ldots, xu_n)$ eine K-Basis von L.

3. Es ist $[\mathbb{C}\!:\!\mathbb{R}] = 2$ und $(1, i)$ eine $\mathbb{R}$-Basis von $\mathbb{C}$.

3. Sei K ein Körper und $n \in \mathbb{N}$. Dann ist die Menge $\{X_1^{\nu_1} \cdot \ldots \cdot X_n^{\nu_n} \mid (\nu_1, \ldots, \nu_n \in \mathbb{N}_0^n\}$ eine K-Basis von $K[X_1, \ldots, X_n]$ und daher $[K[X_1, \ldots, X_n]\!:\!K] = \infty$.

Satz 6.2.3. *Seien $K \subset L \subset N$ Körper. Dann ist*

$$[N\!:\!K] = [N\!:\!L][L\!:\!K]\,.$$

Insbesondere ist N/K genau dann endlich, wenn N/L und L/K beide endlich sind, und dann gilt: Ist $(u_1, \ldots, u_m)$ eine K-Basis von L und $(v_1, \ldots, v_n)$ eine L-Basis von N, so ist $\{u_i v_j \mid i \in [1,m], j \in [1,n]\}$ eine K-Basis von N.

BEWEIS. Sei zunächst N/K endlich. Da $L \subset N$ ein K-Untervektorraum ist, ist auch L/K endlich. Jede K-Basis von N ist ein Erzeugendensystem von N als L-Vektorraum, und daher ist auch N/L endlich. Sei nun $(u_1, \ldots, u_n)$ eine K-Basis von L und $(v_1, \ldots, v_m)$ eine L-Basis von N. Wir zeigen:

1. $\{u_i v_j \mid i \in [1,n]\,,\ j \in [1,m]\}$ ist ein Erzeugendensystem von N als K-Vektorraum.

2. $\{u_i v_j \mid i \in [1,n]\,,\ j \in [1,m]\}$ ist linear unabhängig über K.

1. Sei $z \in N$. Dann ist $z = b_1 v_1 + \ldots + b_m v_m$ mit $b_1, \ldots, b_m \in L$, und jedes b_j hat eine Darstellung $b_j = a_{j1}u_1 + \ldots + a_{jn}u_n$ mit $a_{j\nu} \in K$, also folgt

$$z = \sum_{j=1}^{m}\sum_{i=1}^{n} a_{ji} u_i v_j\,.$$

2. Sei

$$0 = \sum_{j=1}^{m}\sum_{i=1}^{n} a_{j,i} u_i v_j \quad \text{mit} \quad a_{j,i} \in K\,, \quad \text{also} \quad 0 = \sum_{j=1}^{m} b_j v_j \quad \text{mit} \quad b_j = \sum_{i=1}^{n} a_{j,i} u_i \in L\,.$$

Wegen der linearen Unabhängigkeit von $(v_1, \ldots, v_m)$ über L folgt $b_j = 0$ für alle $j \in [1,m]$, und wegen der linearen Unabhängigkeit von $(u_1, \ldots, u_n)$ über K folgt $a_{ji} = 0$ für alle $i \in [1,n]$ und $j \in [1,m]$. □

Definition 6.2.4. Sei L/K eine Körpererweiterung.

1. Für eine Teilmenge $M \subset L$ definiert man
$$K(M) = \{z \in L \mid z = x^{-1}y \ \text{ mit } \ x,\, y \in K[M]\,,\ x \neq 0\} \subset L$$
und sagt, $K(M)$ entsteht durch *Körperadjunktion* von M an K. Ist $M = \{z_1, \ldots, z_n\}$, so schreibt man $K(z_1, \ldots, z_n)$ an Stelle von $K(M)$.
2. Seien $K_1, \ldots, K_n$ Zwischenkörper von L/K. Dann heißt $K_1 \cdot \ldots \cdot K_n = K(K_1 \cup \ldots \cup K_n)$ das *Kompositum* von $K_1, \ldots, K_n$.
3. Die Körpererweiterung L/K heißt
   - *einfach*, wenn es ein $\alpha \in L$ gibt mit $L = K(\alpha)$;
   - *endlich erzeugt*, wenn es ein $n \in \mathbb{N}$ und $\alpha_1, \ldots, \alpha_n \in L$ gibt mit $L = K(\alpha_1, \ldots, \alpha_n)$.

Lemma 6.2.5. *Sei L/K eine Körpererweiterung und $M \subset L$ eine Teilmenge.*

1. *$K(M)$ ist der kleinste $K \cup M$ umfassende Teilkörper von L und ein Quotientenkörper von $K[M]$.*
2. *Ist $M = M_1 \cup M_2$, so ist $K(M) = K(M_1)(M_2)$.*
3. *Sei $M = M_1 \cup \ldots \cup M_n$ und $K_i = K(M_i)$ für alle $i \in [1,n]$. Dann ist $K(M) = K_1 \cdot \ldots \cdot K_n$ der kleinste $K_1 \cup \ldots \cup K_n$ umfassende Teilkörper von L.*
4. *Sind $\varphi, \varphi' \colon K(M) \to R$ Ringhomomorphismen mit $\varphi \,|\, K \cup M = \varphi' \,|\, K \cup M$, so folgt $\varphi = \varphi'$.*

Beweis. 1. Nach Bemerkung 3.3.7.2 ist $K(M)$ ein Quotientenkörper von $K[M]$. Ist $L' \subset L$ ein Teilkörper mit $K \cup M \subset L'$, so ist $K[M] \subset L'$ nach Satz 3.1.8 und daher auch $K(M) \subset L'$.

2. Aus $K \cup M = K \cup M_1 \cup M_2 \subset K(M_1)(M_2)$ folgt $K(M) \subset K(M_1)(M_2)$. Wegen $K \cup M_1 \subset K(M)$ ist $K(M_1) \subset K(M)$, also $K(M_1) \cup M_2 \subset K(M)$ und daher $K(M_1)(M_2) \subset K(M)$.

3. Für einen Teilkörper $K' \subset L$ und $i \in [1,n]$ ist genau dann $K_i \subset K'$, wenn $K \cup M_i \subset K'$. Folglich ist genau dann $K_1 \cup \ldots \cup K_n \subset K'$, wenn $K \cup M \subset K'$. Daher ist $K(M) = K_1 \cdot \ldots \cdot K_n$ der kleinste $K_1 \cup \ldots \cup K_n$ umfassende Teilkörper von L.

4. Aus $\varphi \,|\, K \cup M = \varphi' \,|\, K \cup M$ folgt $\varphi \,|\, K[M] = \varphi' \,|\, K[M]$ nach Bemerkung 3.2.2.7, und daraus folgt $\varphi \,|\, K(M) = \varphi' \,|\, K(M)$ nach Satz 3.3.6.5. □

Bemerkung 6.2.6. Sei K ein Körper. In Definition 3.5.10 hatten wir den rationalen Funktionenkörper $K(X_1, \ldots, X_n)$ in den Unbestimmten $X_1, \ldots, X_n$ über K definiert. Die Bezeichnung ist mit der von Definition 6.2.5 konsistent.

6.3. Algebraische Körpererweiterungen

Definition 6.3.1. Sei L/K eine Körpererweiterung.

1. Ein Element $\alpha \in L$ heißt *algebraisch* über K, es ein $f \in K[X]^\bullet$ gibt mit $f(\alpha) = 0$. Andernfalls heißt α *transzendent* über K.
2. Die Körpererweiterung L/K heißt *algebraisch*, wenn jedes $\alpha \in L$ algebraisch über K ist. Man sagt dann auch, L ist *algebraisch* über K.
3. Eine komplexe Zahl $\alpha \in \mathbb{C}$ heißt *algebraisch,* (*eine algebraische Zahl*), wenn α algebraisch über $\mathbb{Q}$ ist. Andernfalls heißt α *transzendent*.

   $\overline{\mathbb{Q}}$ bezeichne die Menge aller algebraischen Zahlen.

Bemerkung 6.3.2. Sei K ein Körper und $f \in K[X]$ irreduzibel. Dann ist $fK[X]$ ein maximales Ideal von $K[X]$ und $K[X]/fK[X]$ ein Körper. [Beweis: Nach Satz 5.3.3 ist f ein Primelement von $K[X]$, also $fK[X] \lhd K[X]$ ein Primideal nach Satz 5.2.3. Da $K[X]$ ein Hauptidealbereich ist, ist $fK[X]$ ein maximales Ideal, also $K[X]/fK[X]$ ein Körper (Satz 3.7.2).]

Definition und Satz 6.3.3. *Sei L/K eine Körpererweiterung, $K[X]$ ein Polynomring, $\alpha \in L$ und $\Phi = \Phi_\alpha^X \colon K[X] \to L$ der Einsetzungshomomorphismus, definiert durch $\Phi_\alpha^X(g) = g(\alpha)$ für alle $g \in K[X]$.*

1. *Genau dann ist α algebraisch über K, wenn* $\operatorname{Ker}(\Phi_\alpha^X) \neq \{0\}$.
2. *Sei α algebraisch über K.*
   (a) *Sei $f \in K[X]^\bullet$ mit $f(\alpha) = 0$. Dann gilt:*

$$\begin{aligned} \operatorname{Ker}(\Phi_\alpha^X) = fK[X] &\iff \operatorname{gr}(f) = \min\big(\{\operatorname{gr}(g) \mid g \in K[X]^\bullet,\ g(\alpha) = 0\}\big) \\ &\iff f \text{ ist irreduzibel über } K. \end{aligned}$$

   (b) *Sei $f \in K[X]$ mit* $\operatorname{Ker}(\Phi_\alpha^X) = fK[X]$ *und* $d = \operatorname{gr}(f)$. *Dann induziert Φ_α^X einen Isomorphismus*

$$\overline{\Phi} \colon K[X]/fK[X] \xrightarrow{\sim} K[\alpha], \quad \text{gegeben durch } \overline{\Phi}(g + fK[X]) = g(\alpha).$$

   Insbesondere ist $K[\alpha]$ ein Körper, $K[\alpha] = K(\alpha)$, $[K(\alpha):K] = d$, *und* $(1, \alpha, \ldots, \alpha^{d-1})$ *ist eine K-Basis von $K(\alpha)$.*

   (c) *Es gibt genau ein normiertes über K irreduzibles Polynom $f \in K[X]$ mit $f(\alpha) = 0$. Für dieses ist* $\operatorname{gr}(f) = [K(\alpha):K]$, *und* $\{g \in K[X] \mid g(\alpha) = 0\} = fK[X]$.

   Das (eindeutig bestimmte) normierte irreduzible Polynom $f \in K[X]$ mit $f(\alpha) = 0$ heißt *Minimalpolynom* von α über K, und $d = \operatorname{gr}_K(\alpha) = \operatorname{gr}(f) = [K(\alpha):K]$ heißt *Grad* von α über K.

Beweis. Sei $I = \operatorname{Ker}(\Phi_\alpha^X) = \{g \in K[X] \mid g(\alpha) = 0\} \lhd K[X]$. Wegen $\Phi_\alpha^X \neq 0$ ist $I \neq K[X]$.

1. Nach Definition.

2. (a) Nach Satz 3.6.6 ist genau dann $I = fK[X]$, wenn $\operatorname{gr}(f) = \min\big(\{\operatorname{gr}(g) \mid g \in I,\ g \neq 0\}\big)$.

Sei nun $\operatorname{gr}(f) = \min\big(\{\operatorname{gr}(g) \mid g \in I,\ g \neq 0\}\big)$, und sei $f = f_1 f_2$ mit $f_1, f_2 \in K[X]$. Dann ist $0 = f(\alpha) = f_1(\alpha) f_2(\alpha)$, und es sei $f_1(\alpha) = 0$. Wegen $\operatorname{gr}(f) = \operatorname{gr}(f_1) + \operatorname{gr}(f_2)$ folgt $\operatorname{gr}(f_1) \leq \operatorname{gr}(f)$, also $\operatorname{gr}(f_1) = \operatorname{gr}(f)$ und $\operatorname{gr}(f_2) = 0$, also $f_2 \in K$. Daher ist f irreduzibel.

Sei nun $f \in I$ irreduzibel und $f_0 \in I$ mit $I = f_0 K[X]$ ($K[X]$ ist ein Hauptidealbereich, siehe Satz 3.6.6). Dann ist $f_0 \notin K$ und $f = f_0 g$ mit $g \in K[X]$, also $g \in K^\times$ und daher auch $I = fK[X]$.

2. (b) Nach Satz 3.2.9.3 induziert Φ_α^X einen Isomorphismus $\overline{\Phi} \colon K[X]/fK[X] \xrightarrow{\sim} K[\alpha]$ wie behauptet. Nach (a) ist f irreduzibel, und nach Bemerkung 6.3.2 ist $K[X]/fK[X]$ ein Körper. Daher ist auch $K[\alpha]$ ein Körper, und es folgt $K[\alpha] = K(\alpha)$.

Sei nun $d = \mathrm{gr}(f)$. Wir zeigen, dass $(1, \alpha, \dots, \alpha^{d-1})$ ein linear unabhängiges K-Erzeugendensystem von $K[\alpha]$ ist. Sei $x \in K(\alpha) = K[\alpha]$ und $g \in K[X]$ mit $x = g(\alpha)$. Dann existieren Polynome q, $r \in K[X]$ mit $g = qf + r$ und $\mathrm{gr}(r) < d$, und es sei $r = a_0 + a_1 X + \dots a_{d-1} X^{d-1}$ mit $a_0, \dots, a_{d-1} \in K$. Dann ist $x = g(\alpha) = r(\alpha) = a_0 + a_1\alpha + \dots a_{d-1}\alpha^{d-1} \in K + K\alpha + \dots, K\alpha^{d-1}$, und daher ist $\{1, \dots, \alpha^{n-1}\}$ ein K-Erzeugendensystem. Zum Nachweis der K-linearen Unabhängigkeit seien $a_0, \dots, a_{d-1} \in K$ mit $a_0 + a_1\alpha + \dots a_{d-1}\alpha^{d-1} = 0$. Dann ist $g = a_0 + a_1 X + \dots a_{d-1} X^{d-1} \in K[X]$, $g(\alpha) = 0$, und wegen $\mathrm{gr}(g) \le d - 1 < \mathrm{gr}(f)$ folgt $g = 0$, also $a_0 = \dots = a_{d-1} = 0$.

2. (c) Nach Satz 3.6.6 gibt es genau ein normiertes Polynom $f \in K[X]$ mit $I = fK[X]$. Nach 2.(a) ist f irreduzibel, und nach 2.(b) ist $\mathrm{gr}(f) = [K(\alpha) : K]$. □

Bemerkungen und Beispiele 6.3.4. 1. Sei L/K Körpererweiterung. Dann ist

$$K = \{\alpha \in L \mid \alpha \text{ ist algebraisch über } K, \text{ und } \mathrm{gr}_K(\alpha) = 1\},$$

und für $\alpha \in K$ ist $X - \alpha \in K[X]$ das Minimalpolynom von α über K.

2. Sei L/K Körpererweiterung, $\alpha \in L$ und $f \in K[X] \setminus K$ mit $f(\alpha) = 0$. Dann ist $\mathrm{gr}_K(\alpha) \le \mathrm{gr}(f)$, und Gleichheit gilt genau dann, wenn f über K irreduzibel ist.

[Beweis: Sei $h \in K[X]$ das Minimalpolynom von α über K. Nach Satz 6.3.2 ist dann $f = gh$ mit $g \in K[X]$, und $\mathrm{gr}(f) = \mathrm{gr}(g) + \mathrm{gr}(h) \ge \mathrm{gr}(h) = \mathrm{gr}_K(\alpha)$, mit Gleichheit genau dann, wenn $g \in K^\times$, und das ist äquivalent zur Irreduzibilität von f über K.]

3. Sei L/K eine Körpererweiterung, $[L : K] = p \in \mathbb{P}$, und sei M ein Zwischenkörper von L/K. Dann ist $M \in \{K, L\}$, und für alle $\alpha \in L \setminus K$ ist $L = K(\alpha)$. [Beweis: Nach Satz 6.2.3 ist $[L:K] = [L:M]\,[M:K]$, also entweder $[L:M] = 1$ und $L = M$ oder $[M:K] = 1$ und $M = K$.]

4. Eine Körpererweiterung L/K heißt *quadratisch*, wenn $[L:K] = 2$. Ist L/K eine quadratische Körpererweiterung und $\mathrm{char}(K) \ne 2$, so gibt es ein $\alpha \in L$ und ein $d \in K^\times \setminus K^{\times 2}$ mit $L = K(\alpha)$ und $\alpha^2 = d$ (man schreibt dann $L = K(\sqrt{d})$). Die Nebenklasse $dK^{\times 2} \in K^\times/K^{\times 2}$ ist durch L eindeutig bestimmt. [Beweis: Sei $\beta \in L \setminus K$. Dann ist $L = K(\beta)$ und $\mathrm{gr}_K(\beta) = 2$. Sei $f = X^2 + pX + q \in K[X]$ das Minimalpolynom von β über K. Dann ist

$$\beta^2 = -\frac{p}{2} + \alpha \quad \text{mit} \quad d = \alpha^2 = \left(\frac{p}{2}\right)^2 - q \in K, \quad \text{also} \quad L = K(\alpha) \text{ und } (1, \alpha) \text{ eine } K\text{-Basis von } L.$$

Wäre $d = c^2$ mit $c \in K$, so folgte

$$f = \left(X + \frac{p}{2} + c\right)\left(X + \frac{p}{2} - c\right),$$

was der Irreduzibilität von f widerspricht. Daher ist $d \in K^\times \setminus K^{\times 2}$. Es bleibt zu zeigen:

> Sind L_1/K und L_2/K quadratische Erweiterungen, $L_1 = K(\alpha_1)$, $L_2 = K(\alpha_2)$, $\alpha_1^2 = d_1 \in K$ und $\alpha_2^2 = d_2 \in K$, so ist genau dann $L_1 = L_2$, wenn $d_1 K^{\times 2} = d_2 K^{\times 2}$.

Ist $L_1 = L_2$, so ist $\alpha_1 = a + b\alpha_2$ mit $a, b \in K$ und daher $d_1 = \alpha_1^2 = a^2 + b^2 d_2 + 2ab\alpha_2 \in K$. Wegen der linearen Unabhängigkeit von $(1, \alpha_2)$ ist $ab = 0$, und wegen $\alpha_1 \notin K$ ist $b \ne 0$. Es folgt $a = 0$ und $d_1 = b^2 d_2$, also $d_1 K^{\times 2} = d_2 K^{\times 2}$. Ist umgekehrt $d_1 K^{\times 2} = d_2 K^{\times 2}$, so ist $d_1 = b^2 d_2$ mit $b \in K^\times$, also $\alpha_1 = \pm b\alpha_2$ und daher $L_2 = K(\alpha_2) = L(\alpha_1) = L_1$.

5. Seien $n \in \mathbb{N}$, $a \in \mathbb{Q}^\times$, $p \in \mathbb{P}$ und $\mathrm{ggT}(n, \mathsf{v}_p(a)) = 1$. Dann ist $f = X^n - a \in \mathbb{Q}[X]$ irreduzibel über $\mathbb{Q}$. Ist $\alpha \in \mathbb{C}$ mit $\alpha^n = a$, so folgt $[\mathbb{Q}(\alpha) : \mathbb{Q}] = n$. [Beweis: Wegen $f(\alpha) = 0$ ist $[\mathbb{Q}(\alpha) : \mathbb{Q}] = \mathrm{gr}_{\mathbb{Q}}(\alpha) \le \mathrm{gr}(f) = n$. Sei nun $a = p^r b^{-1} c$ mit $r = \mathsf{v}_p(a)$, $b \in \mathbb{N}$ und $c \in \mathbb{Z}$ mit $p \nmid bc$. Wegen $\mathrm{ggT}(r, n) = 1$ gibt es nach Satz 2.3.6 ein $s \in \mathbb{Z}$ mit $rs \equiv 1 \bmod n$. Wir können $s \in \mathbb{N}$ annehmen, setzen $rs = 1 - nt$ mit $t \in \mathbb{Z}$ und $a_1 = a^s (p^t b^s)^n = p^{rs+nt} c^s b^{s(n-1)} = p(cb^{n-1})^s \in \mathbb{Z}$. Dann ist $\mathsf{v}_p(a_1) = 1$, also $f_1 = X^n - a_1$ irreduzibel über $\mathbb{Z}$ nach Satz 5.3.4 und daher irreduzibel über $\mathbb{Q}$ nach Satz 5.3.10.1. Ist nun $\alpha \in \mathbb{C}$ mit $\alpha^n = a$ und $\alpha_1 = \alpha^s p^t b^s \in \mathbb{Q}(\alpha)$, so folgt $f_1(\alpha_1) = 0$ und daher

$$n = \mathrm{gr}_{\mathbb{Q}}(\alpha_1) = [\mathbb{Q}(\alpha_1) : \mathbb{Q}] \le [\mathbb{Q}(\alpha) : \mathbb{Q}] =\le n.$$

Also ist $\mathrm{gr}_{\mathbb{Q}}(\alpha) = [\mathbb{Q}(\alpha):\mathbb{Q}] = n$ und daher f irreduzibel über $\mathbb{Q}$ nach 2.]

6. Sei $q \in \mathbb{Q}$, $n \in \mathbb{N}$ und $\alpha \in \mathbb{C}$ mit $\alpha^n = q$. Dann ist α Nullstelle des Polynoms $X^n - q \in \mathbb{Q}[X]$, also α algebraisch und $\mathrm{gr}_{\mathbb{Q}}(\alpha) \le n$. Ist $q = 1$ und $\alpha = \mathsf{e}^{2\pi \mathsf{i}/n}$ eine primitive n-te Einheitswurzel, so ist $\mathrm{gr}_{\mathbb{Q}}(\alpha) = \varphi(n)$ (Euler'sche Phi-Funktion, siehe 8.3).

7. Sei $\alpha \in \mathbb{C}^\times$. Nach dem Satz von Hermite-Lindemann ist entweder α oder e^α transzendent. Insbesondere ist e transzendent (Satz von Hermite), und da $\mathsf{e}^{\mathsf{i}\pi} = -1$ nicht transzendent ist, ist $\mathsf{i}\pi$ und daher auch π transzendent.

Nach dem Satz von Gelfond-Schneider ist für jedes $\beta \in \mathbb{C} \setminus \mathbb{Q}$ eine der Zahlen e^α, β oder $\mathsf{e}^{\alpha\beta}$ transzendent. Ist insbesondere $\beta \in \mathbb{C} \setminus \mathbb{Q}$ algebraisch, $b \in \mathbb{Q}_{>0}$ und $\alpha = \log b$, so ist $\mathsf{e}^\alpha = b$ und daher $\mathsf{e}^{\alpha\beta} = b^\beta$ transzendent.

Satz 6.3.5. *Sei L/K eine Körpererweiterung.*

1. *Sei $n \in \mathbb{N}$. Sind $\alpha_1, \ldots, \alpha_n \in L$ algebraisch über K, so ist $K(\alpha_1, \ldots, \alpha_n) = K[\alpha_1, \ldots, \alpha_n]$, und $[K(\alpha_1, \ldots, \alpha_n):K] < \infty$.*
2. *Die folgenden Aussagen sind äquivalent:*
   (a) *L/K ist endlich.*
   (b) *L/K ist algebraisch und endlich erzeugt.*
   (c) *Es gibt ein $n \in \mathbb{N}$ und über K algebraische $\alpha_1, \ldots, \alpha_n \in L$ mit $L = K(\alpha_1, \ldots, \alpha_n)$.*

Beweis. 1. Induktion nach n. Seien $\alpha_1, \ldots, \alpha_n \in L$ algebraisch über K.

$n = 1$: Satz 6.3.3.2(b).

$n \ge 2$, $n-1 \to n$: Sei $K' = K(\alpha_1, \ldots, \alpha_{n-1})$. Dann ist α_n auch algebraisch über K', und mit Satz 6.3.3.2(b) folgt $K'(\alpha_n) = K'[\alpha_n]$ und $[K'(\alpha_n) : K'] < \infty$. Nach Induktionsvoraussetzung ist $K' = K[\alpha_1, \ldots, \alpha_{n-1}]$ und $[K':K] < \infty$. Damit folgt

$$K(\alpha_1, \ldots, \alpha_n) = K'(\alpha_n) = K'[\alpha_n] = K[\alpha_1, \ldots, \alpha_{n-1}][\alpha_n] = K[\alpha_1, \ldots, \alpha_n]$$

und $[K(\alpha_1, \ldots, \alpha_n):K] = [K'(\alpha_n):K']\,[K':K] < \infty$ nach Satz 6.2.3.

2. (a) $\Rightarrow$ (b) Sei $[L:K] = n \in \mathbb{N}$ und $(u_1, \ldots, u_n)$ eine K-Basis von L. Dann ist $L = K(u_1, \ldots, u_n)$, also L/K endlich erzeugt, und wir müssen zeigen, dass jedes $\alpha \in L$ algebraisch über K ist.

Sei $\alpha \in L$. Dann ist $(1, \alpha, \alpha^2, \ldots, \alpha^n)$ linear abhängig über K. Daher gibt es $a_0, \ldots, a_n \in K$ mit $(a_0, \ldots, a_n) \ne (0, \ldots, 0)$ und $a_0 + a_1\alpha + \ldots + a_n\alpha^n = 0$. Dann ist $f = a_0 + a_1X + \ldots + a_nX^n \in K[X]^\bullet$ und $f(\alpha) = 0$, also α algebraisch über K.

(b) $\Rightarrow$ (c) Nach Definition.

(c) $\Rightarrow$ (a) Nach 1. □

Korollar 6.3.6. *Sei L/K eine Körpererweiterung. Dann sind äquivalent:*

(a) *L/K ist algebraisch.*

(b) *L wird über K von algebraischen Elementen erzeugt (d.h., $K = K(M)$ mit einer Menge über K algebraischer Elemente $M \subset L$).*

Beweis.

(a) $\Rightarrow$ (b) Es ist $L = K(L)$.

(b) $\Rightarrow$ (a) Sei $L = K(M)$ mit einer Menge über K algebraischer Elemente $M \subset L$, und sei $x \in L$. Nach Definition von $K(M)$ existieren endlich viele Elemente $\alpha_1, \ldots, \alpha_n \in M$ mit $x \in K(\alpha_1, \ldots, \alpha_n)$. Nach Satz 6.3.5.2 ist $K(\alpha_1, \ldots, \alpha_n)/K$ algebraisch und daher insbesondere x algebraisch über K. □

Satz 6.3.7. *Seien $K \subset L \subset M$ Körper. Genau dann ist M/K algebraisch, wenn M/L und L/K algebraisch sind.*

BEWEIS. Ist M/K algebraisch, so sind definitionsgemäß auch M/L und L/K algebraisch. Seien nun M/L und L/K algebraisch, und sei $\alpha \in M$. Sei $f = X^n + c_{n-1}X^{n-1} + \ldots + c_1X + c_0 \in L[X]$ das Minimalpolynom von α über L. Dann ist α algebraisch über $K(c_0, \ldots, c_{n-1})$, und nach Satz 6.3.3.2(b) ist $[K(c_0, \ldots, c_{n-1})(\alpha) : K(c_0, \ldots, c_{n-1})] < \infty$. Da $c_0, \ldots, c_{n-1}$ über K algebraisch sind, folgt $[K(c_0, \ldots, c_{n-1}) : K] < \infty$ nach Satz 6.3.4, und es ist

$$[K(c_0, \ldots, c_{n-1})(\alpha) : K] = [K(c_0, \ldots, c_{n-1})(\alpha) : K(c_0, \ldots, c_{n-1})]\,[K(c_0, \ldots, c_{n-1}) : K] < \infty\,.$$

Daher ist $K(c_0, \ldots, c_{n-1})(\alpha)/K$ algebraisch und insbesondere α algebraisch über K. □

Bemerkung 6.3.8. Eine algebraische Körpererweiterung brauchen nicht endlich zu sein. Für $n \in \mathbb{N}$ ist $[\mathbb{Q}(\sqrt[n]{2}) : \mathbb{Q}] = n$. Ist $M = \{\sqrt[n]{2} \mid n \in \mathbb{N}\} \subset \mathbb{R}$, so ist $\mathbb{Q}(M)/\mathbb{Q}$ algebraisch, aber nicht endlich.

6.4. Stammkörper, Zerfällungskörper und algebraischer Abschluss

Definition und Satz 6.4.1. *Seien L/K und L'/K Körpererweiterungen.*

1. *Sei $\varphi : L \to L'$ ein Körpermonomorphismus. Genau dann ist φ ein K-Vektorraum-Homomorphismus, wenn $\varphi \mid K = \mathrm{id}_K$.*

   Ein Körpermonomorphismus $\varphi : L \to L'$ mit $\varphi \mid K = \mathrm{id}_K$ heißt *K-Homomorphismus*. Ein bijektiver K-Homomorphismus heißt *K-Isomorphismus*. Wir bezeichnen mit $\mathrm{Hom}_K(L, L')$ die Menge aller K-Homomorphismen $\varphi : L \to L'$ und mit $\mathrm{Gal}(L/K)$ die Menge aller K-Isomorphismen $\varphi : L \to L$.

   $\mathrm{Gal}(L/K) \subset \mathfrak{S}(L)$ *ist eine Untergruppe.* $\mathrm{Gal}(L/K)$ heißt *Galoisgruppe* von L/K.
2. *Sei $\varphi : L \to L'$ ein Körpermonomorphismus und $\varphi_1 : L[X] \to L'[X]$ seine Fortsetzung auf die Polynomringe. Ist $f \in L[X]$ und $\alpha \in L$, so folgt $\varphi(f(\alpha)) = \varphi_1(f)(\varphi(\alpha))$.*

   Ist insbesondere $\varphi \in \mathrm{Hom}_K(L, L')$ und $f \in K[X]$, so folgt $\varphi(f(\alpha)) = f(\varphi(\alpha))$.
3. *Ist L/K algebraisch, so ist $\mathrm{Hom}_K(L, L) = \mathrm{Gal}(L/K)$.*

BEWEIS. 1. Sei zuerst $\varphi \mid K = \mathrm{id}_K$. Für $a \in K$ und $x \in L$ ist dann $\varphi(ax) = \varphi(a)\varphi(x) = a\varphi(x)$, und daher ist φ ein K-Vektorraum-Homomorphismus. Ist φ ein K-Vektorraum-Homomorphismus und $a \in K$, so folgt $\varphi(a) = \varphi(a\,1_L) = a\varphi(1_L) = a\,1_{L'} = a$, also ist $\varphi \mid K = \mathrm{id}_K$.
Sind $\varphi, \psi : L \to L$ K-Isomorphismen, so sind auch $\psi \circ \varphi : L \to L$ und $\varphi^{-1} : L \to L$ K-Isomorphismen. Daner ist $\mathrm{Gal}(L/K) < \mathfrak{S}(L)$.

2. Aus

$$f = \sum_{\nu=0}^{n} a_\nu X^\nu \quad \text{folgt} \quad \varphi_1(f) = \sum_{\nu=0}^{n} \varphi(a_\nu) X^\nu$$

und daher

$$\varphi(f(\alpha)) = \varphi\Big(\sum_{\nu=0}^{n} a_\nu \alpha^\nu\Big) = \sum_{\nu=0}^{n} \varphi(a_\nu)\varphi(\alpha)^\nu = \varphi_1(f)(\varphi(\alpha))\,.$$

Ist insbesondere $\varphi \in \mathrm{Hom}_K(L, L')$ und $f \in K[X]$, so folgt $\varphi(a_\nu) = a_\nu$ für alle $\nu \in [0, n]$ und $\varphi_1(f) = f$.

3. Sei L/K algebraisch und $\varphi \in \mathrm{Hom}_K(L, L)$. Wir müssen die Surjektivität von φ zeigen. Sei $a \in L$, $f \in K[X]$ das Minimalpolynom von a über K und $E = \{x \in L \mid f(x) = 0\}$. Nach 2. ist $f(E) \subset E$, also $f(E) = E$, da f injektiv und E endlich ist. Wegen $a \in E$ folgt $a \in f(E) \subset f(L)$. □

Satz 6.4.2. *Sei K ein Körper und $f \in K[X] \setminus K$. Dann existiert ein Oberkörper $L \supset K$ und ein $\alpha \in L$ mit $f(\alpha) = 0$.*

BEWEIS. Sei $f_0 \in K[X]$ irreduzibel mit $f_0 \mid f$, also $f = f_0 g$ mit $g \in K[X]$. Nach Bemerkung 6.3.2 ist $L' = K[X]/f_0K[X]$ ein Körper, und es sei $\pi\colon K[X] \to L'$ der Restklassenepimorphismus. Dann ist $\operatorname{Ker}(\pi \mid K) = f_0K[X] \cap K = \{0\}$, also $\pi \mid K$ ein Monomorphismus. Nach dem Austauschprinzip (Lemma 3.3.3) gibt es einen Oberkörper $L \supset K$ und einen Isomorphismus $\varphi\colon L \to L'$ mit $\varphi \mid K = \pi \mid K$. Sei $\alpha \in L$ mit $\varphi(\alpha) = \pi(X) \in L'$. Ist nun

$$f_0 = \sum_{\nu=0}^{n} a_\nu X^\nu\,, \quad \text{so folgt} \quad \varphi(f_0(\alpha)) = \varphi\Big(\sum_{\nu=0}^{n} a_\nu \alpha^\nu\Big) = \sum_{\nu=0}^{n} \pi(a_\nu)\pi(X)^\nu = \pi(f_0) = 0$$

und daher $f_0(\alpha) = 0$, also auch $f(\alpha) = 0$. □

Satz 6.4.3. *Sei K ein Körper und $f \in K[X]$ irreduzibel. Sei $\varphi\colon K \to K'$ ein Körperisomorphismus, $\varphi_1\colon K[X] \to K'[X]$ seine Fortsetzung auf die Polynomringe und $f_1 = \varphi_1(f)$. Seien L/K und L'/K' Körpererweiterungen, $\alpha \in L$ mit $f(\alpha) = 0$ und $\alpha' \in L'$ mit $f_1(\alpha') = 0$. Dann existiert genau ein Körperisomorphismus $\overline{\varphi}\colon K(\alpha) \to K'(\alpha')$ mit $\overline{\varphi} \mid K = \varphi$ und $\overline{\varphi}(\alpha) = \alpha'$.*

BEWEIS. Die Eindeutigkeit folgt aus Lemma 6.2.5.3. Für den Existenzbeiweis können wir annehmen, dass f normiert ist (sonst betrachten wir an Stelle von f das normierte Polynom $a^{-1}f$, wobei $a \in K^\times$ der höchste Koeffizient von f ist). φ_1 ist ein Isomorphismus, also ist auch $f_1 \in K'[X]$ normiert und irreduzibel. Insbesondere ist f das Minimalpolynom von α über K und f_1 das Minimalpolynom von α' über K'. Nach Satz 6.3.3.2(b) gibt es Isomorphismen $\overline{\Phi}\colon K[X]/fK[X] \xrightarrow{\sim} K(\alpha)$ und $\overline{\Phi}'\colon K'[X]/f_1K'[X] \xrightarrow{\sim} K'(\alpha')$ mit $\overline{\Phi}(X + fK[X]) = \alpha$ und $\overline{\Phi}'(X + f_1K'[X]) = \alpha'$. Der Isomorphismus φ_1 induziert einen Ringisomorphismus $\varphi_1^*\colon K[X]/fK[X] \xrightarrow{\sim} K'[X]/f_1K'[X]$, so dass $\varphi_1^*(g + fK[X]) = \varphi_1(g) + f_1K'[X]$ für alle $g \in K[X]$. Daher ist $\overline{\varphi} = \overline{\Phi}^{-1} \circ \varphi_1^* \circ \overline{\Phi}'\colon K(\alpha) \to K'(\alpha')$ der gewünschte Isomorphismus. Das folgende kommutative Diagramm veranschaulicht die durchgeführte Konstruktion:

$$\begin{array}{ccc} K[X]/fK[X] & \xrightarrow{\overline{\Phi}} & K(\alpha) \\ {\scriptstyle \varphi_1^*}\downarrow & & \downarrow{\scriptstyle \overline{\varphi}} \\ K'[X]/f_1K'[X] & \xrightarrow{\overline{\Phi}'} & K'(\alpha') \end{array}$$

□

Definition 6.4.4. Sei K ein Körper und $f \in K[X]$ irreduzibel. Ein Oberkörper $L \supset K$ heißt *Stammkörper* von f (über K), wenn es ein $\alpha \in L$ gibt mit $f(\alpha) = 0$ und $L = K(\alpha)$.

Satz 6.4.5 (Existenz und Eindeutigkeit des Stammkörpers, Satz von Kronecker)**.** *Sei K ein Körper und $f \in K[X]$ irreduzibel. Dann besitzt f über K einen Stammkörper, und dieser ist bis auf K-Isomorphie eindeutig bestimmt.*

Genauer gilt:

Sind $L = K(\alpha)$ und $L' = K(\alpha')$ Oberkörper von K und ist $f(\alpha) = f(\alpha') = 0$, so existiert genau ein K-Isomorphismus $\Phi\colon L \to L'$ mit $\Phi(\alpha) = \alpha'$.

BEWEIS. Nach Satz 6.4.2 gibt es einen Oberkörper $L' \supset K$ und ein $\alpha \in L'$ mit $f(\alpha) = 0$. Dann ist $L = K(\alpha) \subset L'$ ein Stammkörper von f. Die Eindeutigkeit folgt aus Satz 6.4.3 mit $K = K'$ und $\varphi = \mathrm{id}_K$. □

Korollar und Definition 6.4.6. *Sei L/K eine Körpererweiterung, und seien $\alpha, \alpha' \in L$. Dann sind die folgenden Aussagen äquivalent*:

(a) *α und α' besitzen dasselbe Minimalpolynom über K.*

(b) *Es gibt ein (über K) irreduzibles Polynom $f \in K[X]$ mit $f(\alpha) = f(\alpha') = 0$.*

(c) *Es gibt einen K-Isomorphismus* $\Phi\colon K(\alpha) \to K(\alpha')$ *mit* $\Phi(\alpha) = \alpha'$.

(d) *Es gibt einen K-Monomorphismus* $\varphi\colon K(\alpha) \to L$ *mit* $\varphi(\alpha) = \alpha'$.

Sind diese Eigenschaften erfüllt, so heißen α und α' *konjugiert* (über K).

BEWEIS. (a) $\Rightarrow$ (b) Das Minimalpolynom ist irreduzibel.

(b) $\Rightarrow$ (c) Nach Satz 6.4.5, da $K(\alpha)$ und $K(\alpha')$ Stammkörper von f über K sind.

(c) $\Rightarrow$ (d) Sei $j = (K(\alpha') \hookrightarrow L$ und $\varphi = j \circ \Phi$.

(d) $\Rightarrow$ (a) Ist $f \in K[X]$ das Minimalpolynom von α über K, so ist $0 = \varphi(f(\alpha)) = f(\varphi(\alpha)) = f(\alpha')$, und daher ist f auch das Minimalpolynom von α' über K. □

Definition 6.4.7. Sei K ein Körper und $f \in K[X] \setminus K$. Ein Erweiterungskörper $L \supset K$ heißt *Zerfällungskörper von f (über K)*, wenn ein $c \in K^\times$ und $\alpha_1, \ldots, \alpha_n \in L$ existieren mit

$$f = c \prod_{\nu=1}^{n} (X - \alpha_\nu) \quad \text{und} \quad L = K(\alpha_1, \ldots, \alpha_n).$$

Man sagt dann auch, f *zerfällt über L in Linearfaktoren.*

Bemerkung 6.4.8. Sei K ein Körper, $f \in K[X]$ und $\operatorname{gr}(f) = 1$. Dann ist $f = aX + b$ mit $a \in K^\times$ und $b \in K$, also $f = a(X - \alpha)$ mit $\alpha = a^{-1}b \in K$. Daher ist K ein Zerfällungskörper von f über K.

Satz 6.4.9. *Sei $\varphi\colon K \to K'$ ein Körperisomorphismus und $\varphi_1\colon K[X] \to K'[X]$ seine Fortsetzung auf die Polynomringe. Sei $f \in K[X] \setminus K$, $f_1 = \varphi_1(f) \in K'[X]$, L ein Zerfällungskörper von f über K und L' ein Zerfällungskörper von f_1 über K'. Dann existiert ein Körperisomorphismus $\overline{\varphi}\colon L \to L'$ mit $\overline{\varphi} \mid K = \varphi$.*

BEWEIS. Induktion nach $n = \operatorname{gr}(f)$.

$n = 1$: In diesem Falle ist $L = K$, $L' = K'$ und $\overline{\varphi} = \varphi$.

$n \geq 2$, $n - 1 \to n$: Seien $c \in K^\times$, $c' = \varphi(c) \in K'^\times$, $\alpha_1, \ldots, \alpha_n \in L$ und $\alpha'_1, \ldots, \alpha'_n \in L'$ mit

$$f = c \prod_{\nu=1}^{n} (X - \alpha_\nu) \in L[X], \quad f_1 = c' \prod_{\nu=1}^{n} (X - \alpha'_\nu) \in L'[X], \quad L = K(\alpha_1, \ldots, \alpha_n) \text{ und } L' = K'(\alpha'_1, \ldots, \alpha'_n).$$

Sei $h \in K[X]$ das Minimalpolynom von α_1 über K und $h_1 = \varphi_1(h) \in K'[X]$. Nach Satz 6.3.3 ist dann $h \mid f$, also auch $h_1 \mid f_1$, mit h ist auch das Polynom h_1 normiert und irreduzibel, und es gibt ein $\nu \in [1, n]$ mit $h_1(\alpha'_\nu) = 0$. Wir können (nach eventueller Umnummerierung von $\alpha'_1, \ldots, \alpha'_n$) $h_1(\alpha'_1) = 0$ annehmen. Nach Satz 6.4.3 gibt es einen Isomorphismus $\varphi'\colon K(\alpha_1) \to K'(\alpha'_1)$ mit $\varphi' \mid K = \varphi$ und $\varphi'(\alpha_1) = \alpha'_1$. Sei $\varphi'_1\colon K(\alpha_1)[X] \to K'(\alpha'_1)[X]$ die Fortsetzung von φ' auf die Polynomringe. Wegen $f(\alpha_1) = 0$ gibt es ein Polynom $g \in K(\alpha_1)[X]$ mit $f = (X - \alpha_1)g$, und es sei $g_1 = \varphi'_1(g) \in K'(\alpha'_1)[X]$. Dann folgt $f_1 = (X - \alpha'_1)g_1$, und es ist

$$g = c \prod_{\nu=2}^{n} (X - \alpha_\nu) \in L[X] \quad \text{und} \quad g_1 = c' \prod_{\nu=2}^{n} (X - \alpha'_\nu) \in L'[X].$$

Wegen $L = K(\alpha_1)(\alpha_2, \ldots, \alpha_n)$ und $L' = K'(\alpha'_1)(\alpha'_2, \ldots, \alpha'_n)$ ist L ein Zerfällungskörper von g über $K(\alpha_1)$ und L' ein Zerfällungskörper von g_1 über $K'(\alpha'_1)$. Nach Induktionsvoraussetzung gibt es einen Isomorphismus $\overline{\varphi}\colon L \to L'$ mit $\overline{\varphi} \mid K(\alpha_1) = \varphi'$, und für diesen ist $\overline{\varphi} \mid K = \varphi$. □

Satz 6.4.10 (Existenz und Eindeutigkeit des Zerfällungskörpers)**.** *Sei K ein Körper, $f \in K[X]$ und $n = \operatorname{gr}(f) \in \mathbb{N}$. Dann besitzt f einen Zerfällungskörper über K, und dieser ist bis auf K-Isomorphie eindeutig bestimmt. Ist L ein Zerfällungskörper von f über K, so folgt $[L\colon K] \leq n!$.*

BEWEIS. EXISTENZ: Induktion nach n.

$n = 1$: In diesem Falle ist K ein Zerfällungskörper von f über K.

$n \geq 2$, $n-1 \to n$: Nach Satz 6.4.2 gibt es einen Oberkörper $M \supset K$ und ein $\alpha \in L$ mit $f(\alpha) = 0$. Dann ist $K(\alpha) \subset M$, es gibt ein $g \in K(\alpha)[X]$ mit $f = (X-\alpha)g$, es ist $\operatorname{gr}(g) = n-1$, und nach Bemerkung 6.3.4.2 ist $[K(\alpha):K] = \operatorname{gr}_K(\alpha) \leq n$. Nach Induktionsvoraussetzung besitzt g einen Zerfällungskörper L über $K(\alpha)$ mit $[L:K(\alpha)] \leq (n-1)!$. Ist nun $g = c(X-\alpha_2)\cdot\ldots\cdot(X-\alpha_n)$ mit $c \in K(\alpha)^\times$, $\alpha_2, \ldots, \alpha_n \in L$ und $L = K(\alpha)(\alpha_2, \ldots, \alpha_n)$, so folgt $f = c(X-\alpha_1)(X-\alpha_2)\cdot\ldots\cdot(X-\alpha_n)$, also $c \in K^\times$, L ist Zerfällungskörper von f über K, und $[L:K] = \big[L:K(\alpha)\big]\big[K(\alpha):K\big] \leq n(n-1)! = n!$

EINDEUTIGKEIT: Nach Satz 6.4.9 mit $K = K_1$ und $\varphi = \mathrm{id}_K$. □

Beispiel 6.4.11. Wir bestimmen den Zerfällungskörper von X^3-2 über $\mathbb{Q}$. In $\mathbb{C}[X]$ ist

$$X^3-2 = (X-\sqrt[3]{2})(X-\rho\sqrt[3]{2})(X-\rho^2\sqrt[3]{2}) \quad \text{mit} \quad \sqrt[3]{2} \in \mathbb{R}_{>0} \quad \text{und} \quad \rho = \mathsf{e}^{\frac{2\pi i}{3}} = \frac{-1+\sqrt{-3}}{2} \in \mathbb{Q}(\sqrt{-3}),$$

und daher ist

$$L = \mathbb{Q}(\sqrt[3]{2}, \rho\sqrt[3]{2}, \rho^2\sqrt[3]{2}) = \mathbb{Q}(\sqrt[3]{2}, \rho) = \mathbb{Q}(\sqrt[3]{2}, \sqrt{-3})$$

ein Zerfällungskörper von X^3-2 über $\mathbb{Q}$. Nach Beispiel 5.3.5.2 und Satz 5.3.10.1 ist X^3-2 irreduzibel über $\mathbb{Q}$ und daher das Minimalpolynom der drei Zahlen $\sqrt[3]{2}$, $\rho\sqrt[3]{2}$, $\rho^2\sqrt[3]{2}$ über $\mathbb{Q}$. Die Körper

$$K_1 = \mathbb{Q}(\sqrt[3]{2}), \quad K_2 = \mathbb{Q}(\rho\sqrt[3]{2}) \quad \text{und} \quad K_3 = \mathbb{Q}(\rho^2\sqrt[3]{2})$$

sind Stammkörper von X^3-2 über $\mathbb{Q}$, es ist $[K_i:\mathbb{Q}] = 3$ für alle $i \in [1,3]$, $K_1 \subset \mathbb{R}$, $K_2 \not\subset \mathbb{R}$, $K_3 \not\subset \mathbb{R}$, $\sqrt[3]{2} = \big(\rho\sqrt[3]{2}\big)^2\big(\rho^2\sqrt[3]{2}\big)^{-1} \in K_2K_3$, $\rho\sqrt[3]{2} = \big(\rho^2\sqrt[3]{2}\big)^2\big(\sqrt[3]{2}\big)^{-1} \in K_3K_1$ und $\rho^2\sqrt[3]{2} = \big(\rho\sqrt[3]{2}\big)^2\big(\sqrt[3]{2}\big)^{-1}$. Daher ist $K_1 \subset K_2K_3$, $K_2 \subset K_3K_1$ und $K_3 \subset K_2K_1$, die Körper K_1, K_2 und K_3 sind verschieden, und $L = K_1K_2K_3 = K_1K_2 = K_1K_3 = K_2K_3$.

Wir betrachen nun den Körper $k = \mathbb{Q}(\sqrt{-3}) \subset L$. $\sqrt{-3}$ ist Nullstelle des Polynoms $X^2+3 \in \mathbb{Q}[X]$. Wegen $L = \mathbb{Q}(\sqrt[3]{2}, \sqrt{-3}) = K_1k = K_1(\sqrt{-3}) \supsetneq K_1$ ist X^2+3 irreduzibel über K_1, also $[L:K_1] = 2$ und $[L:\mathbb{Q}] = [L:K_1]\,[K_1:\mathbb{Q}] = 6$.

Definition und Satz 6.4.12. *Sei K ein Körper.*

1. *Die folgenden Aussagen sind äquivalent:*
   (a) *Jedes $f \in K[X] \setminus K$ besitzt in K eine Nullstelle.*
   (b) *Jedes $f \in K[X] \setminus K$ zerfällt über K in Linearfaktoren.*
   (c) *Es gibt keine endliche Körpererweiterung L/K mit $L \neq K$.*

   Sind diese Bedingungen erfüllt, so heißt K *algebraisch abgeschlossen*.
2. *Sei $L \supset K$ ein Oberkörper und $\overline{K} = \{\alpha \in L \mid \alpha$ ist algebraisch über $K\}$. Dann ist $\overline{K}$ ein Körper. Ist L algebraisch abgeschlossen, so auch $\overline{K}$.*

   $\overline{K}$ heißt *algebraischer Abschluss* von K in L.
3. Ein Oberkörper $L \supset K$ heißt *algebraische Hülle* von K, wenn L algebraisch abgeschlossen und L/K algebraisch ist.

   Jeder Körper besitzt eine (bis auf K-Isomorphie eindeutig bestimmte) algebraische Hülle.

BEWEIS. 1. (a) ⇒ (b) Nach Satz 3.6.7.

(b) ⇒ (c) Sei L/K eine endliche Körpererweiterung und $\alpha \in L$. Nach Satz 6.3.5 ist L/K algebraisch. Sei $f \in K[X]$ das Minimalpolynom von α über K. Da f über K in Linearfaktoren zerfällt, folgt $\alpha \in K$.

(c) ⇒ (a) Sei $f \in K[X] \setminus K$. Nach Satz 6.4.2 gibt es einen Oberkörper $L \supset K$ und ein $\alpha \in L$ mit $f(\alpha) = 0$. Dann ist $K(\alpha)/K$ endlich, also $K(\alpha) = K$ und daher $\alpha \in K$.

2. Wir müsen zeigen: Sind $\alpha, \beta \in \overline{K}$, so sind auch $\alpha-\beta$, $\alpha\beta$ und (im Falle $\alpha \neq 0$) $\alpha^{-1} \in \overline{K}$. Aber das folgt aus Satz 6.3.5.2, denn für alle $\alpha, \beta \in \overline{K}$ ist $K(\alpha, \beta)/K$ algebraisch.

Sei nun L algebraisch abgeschlossen und $f \in K[X] \setminus K$. Dann hat f eine Nullstelle $\alpha \in L$, und $\overline{K}(\alpha)/\overline{K}$ ist algebraisch. Da $\overline{K}/K$ eine algebraische Körpererweiterung ist, ist nach Satz 6.3.7 auch $\overline{K}(\alpha)/K$ algebraisch, also α algebraisch über K und daher $\alpha \in \overline{K}$.

3. Für den Beweis verweisen wir auf [**?**, § 3.4]. □

In Korollar 8.3.2 zeigen wir, dass $\mathbb{C}$ und $\overline{\mathbb{Q}} = \{\alpha \in \mathbb{C} \mid \alpha \text{ ist algebraisch über } \mathbb{Q}\}$ algebraisch abgeschlossene Körper sind.

6.5. Normale Körpererweiterungen

Definition 6.5.1. Eine Körpererweiterung L/K heißt *normal*, wenn L/K algebraisch ist und für jedes über K irreduzible Polynom $f \in K[X]$ gilt: Besitzt f in L eine Nullstelle, so zerfällt f über L in Linearfaktoren.

Satz 6.5.2. *Sei L/K eine endliche Körpererweiterung. Dann sind die folgenden Aussagen äquivalent:*

(a) *L/K ist normal.*

(b) *L ist Zerfällungskörper eines Polynoms $f \in K[X] \setminus K$ über K.*

(c) *Für jeden Oberkörper $N \supset L$ und jedes $\varphi \in \mathrm{Hom}_K(L, N)$ ist $\varphi(L) \subset L$.*

(d) *Für jeden Oberkörper $N \supset L$ und je zwei Elemente $\alpha \in L$ und $\beta \in N$ gilt: Sind α und β konjugiert über K, so ist $\beta \in L$, und es existiert ein $\sigma \in \mathrm{Gal}(L/K) = \mathrm{Hom}_K(L, L)$ mit $\sigma(\alpha) = \beta$.*

Beweis.

(a) ⇒ (b) Nach Satz 6.3.5.2 gibt es ein $n \in \mathbb{N}$ und über K algebraische Elemente $\alpha_1, \ldots, \alpha_n \in L$ mit $L = K(\alpha_1, \ldots, \alpha_n)$. Für $i \in [1, n]$ sei $f_i \in K[X]$ das Minimalpolynom von α_i über K, und es sei $f = f_1 \cdot \ldots \cdot f_n \in K[X]$. Alle f_i und daher auch f zerfallen über L in Linearfaktoren, und L entsteht durch Adjunktion der Nullstellen von f an K. Daher ist L ein Zerfällungskörper von f über K.

(b) ⇒ (c) Sei $f \in K[X] \setminus K$ und L ein Zerfällungskörper von f über K, also

$$f = c \prod_{\nu=1}^{n} (X - \alpha_\nu) \quad \text{mit} \quad c \in K^\times,\ \alpha_1, \ldots, \alpha_n \in L \quad \text{und} \quad L = K(\alpha_1, \ldots, \alpha_n)\,.$$

Sei $N \supset L$ ein Oberkörper und $\varphi \in \mathrm{Hom}_K(L, N)$. Für alle $\nu \in [1, n]$ ist dann $0 = \varphi(f(\alpha_\nu)) = f(\varphi(\alpha_\nu))$, also $\varphi(\alpha_\nu) \in \{\alpha_1, \ldots, \alpha_n\}$ und daher $\varphi(L) = K(\varphi(\alpha_1), \ldots, \varphi(\alpha_n)) \subset K(\alpha_1, \ldots, \alpha_n) = L$.

(c) ⇒ (d) Sei $N \supset L$ ein Oberkörper, $\alpha_1 = \alpha \in L$, $\beta \in N$, und seien α, β konjugiert über K. Seien $n \in \mathbb{N}$ und $\alpha_2, \ldots, \alpha_n \in L$ mit $L = K(\alpha_1, \ldots, \alpha_n$. Für $\nu \in [1, n]$ sei $f_\nu \in K[X]$ das Minimalpolynom von α_ν über K, und es sei $f = f_1 \cdot \ldots \cdot f_n \in K[X]$. Nach Korollar 6.4.6 ist dann $f_1(\beta) = 0$. Sei L' ein Zerfällungskörper von f über $L(\beta)$ und $M \subset L'$ die Menge der Nullstellen von f in L'. Dann ist $\{\alpha_1, \ldots, \alpha_n, \beta\} \subset M$ und

$$L' = L(\beta)(M) = K(\alpha_1, \ldots, \alpha_n, \beta)(M) = K(\alpha)(M) = K(\beta)(M)\,.$$

Also ist L' auch ein Zerfällungskörper von f über $K(\alpha)$ und von f über $K(\beta)$. Nach Korollar 6.4.6 existiert ein K-Isomorphismus $\varphi\colon K(\alpha) \to K(\beta)$ mit $\varphi(\alpha) = \varphi(\beta)$. Ist $\varphi_1\colon K(\alpha)[X] \to K(\beta)[X]$ die Fortsetzung von φ auf die Polynomringe, so ist $\varphi_1 \,|\, K[X] = \mathrm{id}$ und daher $\varphi_1(f) = f$. Nach Satz 6.4.9 existiert ein Körperisomorphismus $\psi\colon L' \xrightarrow{\sim} L'$ mit $\psi \,|\, K(\alpha) = \varphi$. Dann ist $\psi \,|\, K = \varphi \,|\, K = \mathrm{id}_K$ und $\psi \,|\, L \in \mathrm{Hom}_K(L, L')$. Nach (c) ist $\psi(L) \subset L$, also $\sigma = (\psi \,|\, L\colon L \to L) \in \mathrm{Hom}_K(L, L) = \mathrm{Gal}(L/K)$ und $\beta = \varphi(\alpha) = \psi(\alpha) = \sigma(\alpha) \in L$.

(d) ⇒ (a) Sei $f \in K[X]$ irreduzibel über K, $\alpha \in L$ mit $f(\alpha) = 0$ und N ein Zerfällungskörper von f über L. Dann ist $f = c(X - \alpha_1) \cdot \ldots \cdot (X - \alpha_n)$ mit $c \in K^\times$, $\alpha_1, \ldots, \alpha_n \in N$, und es ist

$N = L(\alpha_1, \ldots, \alpha_n)$. Für alle $\nu \in [2, n]$ sind α und α_ν konjugiert über K, also $\alpha_\nu \in L$, und daher zerfällt f über L in Linearfaktoren. □

Korollar 6.5.3. *Sei L/K eine endliche normale Körpererweiterung, und seien $\alpha, \beta \in L$. Genau dann sind α und β konjugiert über K, wenn ein $\varphi \in \mathrm{Gal}(L/K)$ existiert mit $\varphi(\alpha) = \beta$.*

Beweis. Ist $\varphi \in \mathrm{Gal}(L/K)$ mit $\varphi(\alpha) = \beta$, so ist $\varphi \,|\, K(\alpha)\colon K(\alpha) \to K(\beta)$ ein K-Isomorphismus und die Behauptung folgt aus Korollar 6.4.6. Die Umkehrung folgt aus Satz 6.5.2.(d). □

Korollar 6.5.4. *Sei L/K eine endliche Körpererweiterung.*

1. *Sei L/K normal und $K \subset M \subset L$ ein Zwischenkörper. Dann ist auch L/M normal.*
2. *Es gibt einen Oberkörper $N \supset L$, so dass N/K endlich und normal ist.*

Beweis. 1. Nach Satz 6.5.2 ist L Zerfällungskörper eines Polynoms $f \in K[X] \setminus K$ über K. Dann ist aber L auch Zerfällungskörper von f über M und daher L/M normal (wieder nach Satz 6.5.2).

2. Sei $L = K(\alpha_1, \ldots, \alpha_n)$. Für $i \in [1, n]$ sei $f_i \in K[X]$ das Minimalpolynom von α_i über K, es sei $f = f_1 \cdot \ldots \cdot f_n \in K[X]$ und N ein Zerfällungskörper von f über L. Dann ist N auch ein Zerfällungskörper von f über K, und daher ist N/K endlich und normal. □

Beispiele 6.5.5.

1. Jede quadratische Körpererweiterung ist normal. [Beweis: Sei L/K eine quadratische Körpererweiterung, $\alpha \in L \setminus K$ und $f \in K[X]$ das Minimalpolynom von α über K. Dann ist

$$1 < \mathrm{gr}(f) = \mathrm{gr}_K(\alpha) = [K(\alpha)\colon K] \le [L\colon K] = 2\,, \quad \text{also} \quad L = K[\alpha] \quad \text{und} \quad \mathrm{gr}(f) = \mathrm{gr}_K(\alpha) = 2\,.$$

Wegen $f(\alpha) = 0$ ist $f = (X - \alpha)g$ mit einem normierten Polynom $g \in L[X]$, und wegen $\mathrm{gr}(g) = 1$ ist $g = X - \beta$ mit $\beta \in L$. Daher ist $L = K(\alpha, \beta)$ ein Zerfällungskörper von f über K, also L/K normal nach Satz 6.5.2.

2. Seien $K \subset M \subset L$ Körper und seien M/K und L/M normal. Dann braucht L/K nicht normal zu sein. [Beispiel: Sei $K = \mathbb{Q}$, $M = \mathbb{Q}(\sqrt{2})$ und $L = \mathbb{Q}(\sqrt[4]{2}\,)$. Dann ist L ein Stammkörper des über $\mathbb{Q}$ irreduziblen Polynoms $f = X^4 - 2$, es ist $[L\colon M] = [M\colon \mathbb{Q}] = 2$, und daher sind nach 1. die Körpererweiterungen L/M und $M/\mathbb{Q}$ normal. Es ist $L \subset \mathbb{R}$, aber f hat die Nullstelle $\mathrm{i}\sqrt[4]{2} \in \mathbb{C} \setminus \mathbb{R}$. Daher zerfällt f über L nicht in Linearfaktoren, und $L/\mathbb{Q}$ ist nicht normal.

6.6. Separabilität und Fortsetzung von Homomorphismen

Definition 6.6.1. Sei K ein Körper.

1. Ein Polynom $f \in K[X] \setminus K$ heißt *separabel*, wenn f in keinem Oberkörper $L \supset K$ mehrfache Nullstellen besitzt.
2. K heißt *vollkommen*, wenn jedes über K irreduzible Polynom $f \in K[X]$ separabel ist.

Satz 6.6.2. *Sei K ein Körper, $f \in K[X]$ und $L \supset K$ ein Zerfällungskörper von f. Dann sind die folgenden Aussagen äquivalent:*

(a) *f ist separabel.*

(b) *f hat in L keine mehrfachen Nullstellen.*

(c) *f und f' sind teilerfremd in $K[X]$.*

Ist f irreduzibel über K, so ist ferner äquivalent:

(d) *$f' \neq 0$.*

BEWEIS. (a) $\Rightarrow$ (b) Nach Definition.

(b) $\Rightarrow$ (c) Durch Widerspruch. Sei $g \in K[X] \setminus K$ mit $g \mid f$ und $g \mid f'$. Mit f zerällt auch g über L in Linearfaktoren, und daher gibt es ein $\alpha \in L$ mit $g(\alpha) = 0$. Es ist dann aber auch $f(\alpha) = f'(\alpha) = 0$ und daher nach Satz 3.6.5.3 α eine mehrfache Nullstelle von f, ein Widerspruch.

(c) $\Rightarrow$ (a) Durch Widerspruch. Sei $L \supset K$ ein Oberkörper und $\alpha \in L$ eine mehrfache Nullstelle von f. Dann ist α algebraisch über K, und es sei $g \in K[X$ das Minimalpolynom von α über K. Wegen $f(\alpha) = f'(\alpha) = 0$ folgt $g \mid f$ und $g \mid f'$ nach Satz 6.3.3.2(c).

(c) $\Rightarrow$ (d) Ist $f' = 0$, so ist f ein gemeinsamer Teiler von f und f', also f und f' nicht teilerfremd.

(d) $\Rightarrow$ (c) Sei f irreduzibel über K, $f' \neq 0$ und $g \in K[X]$ ein gemeinsamer Teiler von f und f'. Dann ist $\operatorname{gr}(g) \leq \operatorname{gr}(f') < \operatorname{gr}(f)$, und wegen der Irreduzibilität von f folgt $g \in K$. Daher sind f und f' teilerfremd. □

Satz 6.6.3. *Sei K ein Körper.*

1. *Ist $\operatorname{char}(K) = 0$, so ist K vollkommen.*
2. *Ist $\operatorname{char}(K) = p \in \mathbb{P}$, so ist K genau dann vollkommen, wenn $K = \{x^p \mid x \in K\}$.*
3. *Ist K endlich oder algebraisch abgeschlossen, so ist K vollkommen.*

BEWEIS. 1. Sei $f \in K[X] \setminus K$ irreduzibel. Nach Satz 6.1.5 ist $f' \neq 0$ und daher f separabel nach Satz 6.6.2.

2. Sei zuerst $K = \{x^p \mid x \in K\}$. Wir zeigen: Ist $f \in K[X] \setminus K$ mit $f' = 0$, so ist f nicht irreduzibel über K. Sei $f \in K[X] \setminus K$ mit $f' = 0$. Nach Satz 6.1.5 ist dann $f = g(X^p)$ mit $g \in K[X]$, etwa $g = a_0 + a_1 X + \ldots + a_n X^n$ mit $n \in \mathbb{N}$ und $a_\nu \in K$, also $a_\nu = c_\nu^p$ mit $c_\nu \in K$ für alle $\nu \in [1, n]$. Nach Satz 6.1.4 ist dann

$$f = c_0^p + c_1^p X^p + \ldots + c_n^p X^{np} = (c_0 + c_1 X + \ldots + c_n X^n)^p \in K[X]$$

nicht irreduzibel.

Sein nun $K \neq \{x^p \mid x \in K\}$ und $a \in K \setminus \{x^p \mid x \in K\}$. Dann hat das Polynom $f = X^p - a$ keine Nullstelle in K. Sei $L \supset K$ ein Stammkörper von f. Ist $\alpha \in L$ mit $f(\alpha) = 0$, so ist $\alpha^p = a$ und daher $f = (X - \alpha)^p \in L[X]$. Sei $g \in K[X]$ das Minimalpolynom von α über K. Dann ist $g \mid f$, und daher folgt $g = (X - \alpha)^m \in L[X]$ mit $m \geq 2$. Insbesondere ist α eine mehrfache Nullstelle des irreduziblen Polynoms g und daher K nicht vollkommen.

3. Ist K endlich, $\operatorname{char}(K) = p \in \mathbb{P}$, so ist die Abbildung $\varphi\colon K \to K$, definiert durch $\varphi(x) = x^p$, injektiv, also bijektiv und daher $K = \{x^p \mid x \in K\}$. Ist K algebraisch abgeschlossen und $f \in K[X] \setminus K$ irreduzibel, so ist $f = cX + d$ mit $c \in K^\times$ und $d \in K$, also $f' = c \neq 0$ und daher f separabel. □

Beispiel 6.6.4. Sei K Körper mit $\operatorname{char}(K) = p \in \mathbb{P}$ und $K(T)$ ein rationaler Funktionenkörper in T über K. Nach Beispiel 5.3.5.3 ist das Polynom $f = X^p - T \in K[T][X]$ irreduzibel über $K[T]$, und da $K[T]$ faktoriell ist, auch über $K(T)$ (siehe Satz 5.3.10.1). Wegen $f' = pX^{p-1} = 0$ ist f inseparabel über $K(T)$ und daher $K(T)$ nicht vollkommen.

Definition 6.6.5. Sei L/K eine algebraische Körpererweiterung.

1. $\alpha \in L$ heißt *separabel* über K, wenn das Minimalpolynom von α über K separabel ist.
2. L/K heißt *separabel*, wenn jedes $\alpha \in L$ separabel über K ist. Andernfalls heißt L/K *inseparabel*.
3. L/K heißt *galoissch*, wenn L/K normal und separabel ist.

Bemerkungen 6.6.6. Sei L/K eine Körpererweiterung.

1. Sei $\alpha \in L$ und $f \in K[X] \setminus K$ ein separables Polynom mit $f(\alpha) = 0$. Dann ist α separabel über K. [Beweis: Ist $g \in K[X]$ das Minimalpolynom von α über K, so ist $g \mid f$, und mit f hat auch g in jedem Oberkörper von K nur einfache Nullstellen, ist also separabel.]

2. Ist K vollkommen, so ist jede algebraische Körpererweiterung separabel.

3. Ist L/K endlich und inseparabel, so ist $\operatorname{char}(K) = p \in \mathbb{P}$ und $p \mid [L:K]$. [Beweis: Sei $\alpha \in L$ nicht separabel über K und $f \in K[X]$ das Minimalpolynom von α über K. Dann ist f irreduzibel und nach separabel, also $f' = 0$ und daher $f = g(X^p)$ mit einem Polynom $g \in K[X]$. Damit folgt $p \operatorname{gr}(g) = \operatorname{gr}(f) = [K(\alpha):K] \mid [L:K]$.]

Satz 6.6.7 (Fortsetzungssatz für Homomorphismen)**.** *Sei $\varphi\colon K \to K'$ ein Körperisomorphismus und $\varphi_1\colon K[X] \to K'[X]$ seine Fortsetzung auf die Polynomringe. Seien L/K und L'/K' Körpererweiterungen, $[L:K] < \infty$, und sei Ω die Menge aller Körpermonomorphismen $\psi\colon L \to L'$ mit $\psi \mid K = \varphi$.*

1. *Ist $L = K(\alpha)$ und f das Minimalpolynom von α über K, so ist $|\Omega|$ die Anzahl der Nullstellen von $\varphi_1(f)$ in L'.*
2. *Es ist $|\Omega| \le [L:K]$, und Gleichheit gilt genau dann, wenn die beiden folgenden Bedingungen erfüllt sind:*
   - *L/K ist separabel.*
   - *Für jedes über K irreduzible Polynom $f \in K[X]$ gilt: Hat f eine Nullstelle in L, so zerfällt $\varphi_1(f)$ über L' in Linearfaktoren.*

Beweis. 1. Sei $\Sigma = \{\alpha' \in L' \mid \varphi_1(f)(\alpha') = 0\}$. Ist $\psi \in \Omega$, so ist $\varphi_1(f)(\psi(\alpha)) = \psi(f(\alpha)) = 0$ nach Satz 6.4.1.2 und daher $\psi(\alpha) \in \Sigma$. Also bleibt zu zeigen, dass es zu jedem $\alpha' \in \Sigma$ genau ein $\psi \in \Omega$ gibt, so dass $\psi(\alpha) = \alpha'$.

Sei $\alpha' \in \Sigma$. Nach Satz 6.4.3 existiert genau ein Isomorphismus $\psi\colon K(\alpha) \to K'(\alpha')$ mit $\psi \mid K = \varphi$ und $\psi(\alpha) = \alpha'$, und es ist $\big(\psi\colon K(\alpha) \to K'(\alpha') \hookrightarrow L\big) \in \Omega$.

2. Induktion nach $[L:K]$. Ist $[L:K] = 1$, so ist $L = K$ und $\Omega = \{\varphi\}$. Sei also $[L:K] > 1$ und die Behauptung für alle Körpererweiterungen kleineren Grades gezeigt. Sei $\alpha \in L \setminus K$, $f \in K[X]$ das Minimalpolynom von α über K und Ω' die Menge aller Körpermonomorphismen $\varphi'\colon K(\alpha) \to L'$ mit $\varphi' \mid K = \varphi$. Nach 1. ist dann

$$|\Omega'| = |\{\alpha' \in L' \mid \varphi_1(f)(\alpha') = 0\}| \le \operatorname{gr}(\varphi_1(f)) = \operatorname{gr}(f) = [K(\alpha):K]\,.$$

Wegen $K \subsetneq K(\alpha) \subset L$ ist $[L:K(\alpha)] < [L:K]$, und mit der Induktionsvoraussetzung folgt

$$|\Omega| = \sum_{\varphi' \in \Omega'} \big|\{\psi\colon L \to L' \mid \psi \mid K(\alpha) = \varphi'\}\big| \;\le\; \sum_{\varphi' \in \Omega'} [L:K(\alpha)] \le [K(\alpha):K]\,[L:K(\alpha)] = [L:K]\,.$$

Ist L/K inseparabel, so wählen wir in obiger Konstruktion $\alpha \in L \setminus K$ so, dass α nicht separabel über K ist. Dann ist f nicht separabel, und da φ_1 ein Isomorphismus ist, ist auch $\varphi_1(f)$ nicht separabel. Daher ist $|\Omega'| < \operatorname{gr}(\varphi_1(f)) = [K(\alpha):K]$ und folglich auch $|\Omega| < [L:K]$.

Sei nun $f \in K[X]$ ein über K irreduzibles Polynom mit einer Nullstelle in $\alpha \in L$, so dass $\varphi_1(f)$ über L' nicht in Linearfaktoren zerfällt. Dann ist $\operatorname{gr}(f) > 1$, also $\alpha \in L \setminus K$, und wir machen obige Konstruktion mit diesem α. Dann ist wieder $|\Omega'| < \operatorname{gr}(\varphi_1(f)) = [K(\alpha):K]$ und folglich $|\Omega| < [L:K]$.

Seien schließlich die beiden Bedingungen in 2. erfüllt, und sei $\alpha \in L \setminus K$. Dann ist α separabel über K, und für das Minimalpolynom $f \in K[X]$ von α über K gilt: $\varphi_1(f)$ zerfällt über L' in Linearfaktoren. Da f separabel ist, ist auch $\varphi_1(f)$ separabel, und daher zerfällt $\varphi_1(f)$ über L' in verschiedene Linearfaktoren. In obiger Konstruktion ist also $|\Omega'| = [K(\alpha):K]$, und es genügt, zu zeigen: Für jedes $\varphi' \in \Omega'$ ist

$$(*) \qquad \big|\{\psi\colon L \to L' \mid \psi \text{ ist ein Körpermonomorphismus mit } \psi \mid K(\alpha) = \varphi'\}\big| = [L:K(\alpha)]\,.$$

Sei $\varphi' \in \Omega'$, also $\varphi' \colon K(\alpha) \to L'$ ein Körpermonomorphismus mit $\varphi' \,|\, K = \varphi$. Wir beweisen $(*)$ mit Hilfe der Induktionsvoraussetzung für die Körpererweiterung $L/K(\alpha)$. Sei $\varphi_1' \colon K(\alpha)[X] \to L'[X]$ die Fortsetzung von φ_1 auf die Polynomringe. Dann müssen wir zeigen:

> $L/K(\alpha)$ ist separabel, und für jedes über $K(\alpha)$ irreduzible Polynom $F \in K(\alpha)[X]$ mit einer Nullstelle in L zerfällt das Polynom $\varphi_1'(F)$ über L' in Linearfaktoren.

Sei $\beta \in L$, $h \in K(\alpha)[X]$ das Minimalpolynom von β über $K(\alpha)$ und $H \in K[X]$ das Minimalpolynom von β über K. Dann ist h ein Teiler von H in $K(\alpha)[X]$. Weil β separael über K ist, ist H separabel, daher ist auch h separabel und somit β separabel über $K(\alpha)$. Daher ist $L/K(\alpha)$ separabel.

Sei $F \in K(\alpha)[X]$ irreduzibel über $K(\alpha)$, $\beta \in L$ eine Nullstelle von F und $f \in K[X]$ das Minimalpolynom von β über K. Dann ist F ein Teiler von f in $K(\alpha)[X]$ und daher $\psi_1'(F)$ ein Teiler von $\varphi_1'(f)$. Das Polynom $\varphi_1(f) = \varphi_1'(f)$ zerfällt über L' in Linearfaktoren, und daher zerfällt auch das Polynom $\varphi_1'(F)$ über L' in Linearfaktoren. □

Korollar 6.6.8. *Sei L/K eine endliche Körpererweiterung.*

1. *Für jede Körpererweiterung L'/K ist $|\mathrm{Hom}_K(L, L')| \leq [L\colon K]$, und Gleichheit gilt genau dann, wenn die beiden folgenden Bedingungen erfüllt sind:*
   - *L/K ist separabel.*
   - *Für jedes über K irreduzible Polynom $f \in K[X]$ gilt: Hat f eine Nullstelle in L, so zerfällt f über L' in Linearfaktoren.*
2. *Sei $L' \supset L$ ein Oberkörper und L'/K normal. Dann ist $|\mathrm{Hom}_K(L, L')| \leq [L\colon K]$, und Gleichheit gilt genau dann, wenn L/K separabel ist.*
3. *Es ist $|\mathrm{Gal}(L/K)| \leq [L\colon K]$, und Gleichheit gilt genau dann, wenn L/K galoissch ist.*

Beweis. 1. Nach Satz 6.6.7 mit $\varphi = \mathrm{id}_K$.

2. Ist $f \in K[X]$ irreduzibel über K und besitzt eine Nullstelle in L, so zerfällt f über L' in Linearfaktoren, da L'/K normal ist. Daher folgt die Behauptung aus 1.

3. Nach 2. mit $L = L'$. □

Satz 6.6.9. *Seien $K \subset M \subset L$ Körper und $[L\colon K] < \infty$.*

1. *Sei $\alpha \in L$ separabel über M, $L = M(\alpha)$ und M/K separabel. Dann ist auch L/K separabel.*
2. *Sei M/K separabel, $n \in \mathbb{N}$, und sei $L = M(\alpha_1, \ldots, \alpha_n)$ mit über M separablen Elementen $\alpha_1, \ldots, \alpha_n \in L$. Dann ist L/K separabel.*
   Insbesondere gilt: Ist $L = K(\alpha_1, \ldots, \alpha_n)$ mit über K separablen Elementen $\alpha_1, \ldots, \alpha_n \in L$, so ist L/K separabel.
3. *Genau dann ist L/K separabel, wenn L/M und M/K separabel sind.*
4. *Ist L/K galoissch, so ist auch L/M galoissch.*

Beweis. 1. Sei $N \supset L$ ein Oberkörper, so dass N/K endlich und normal ist (nach Korollar 6.5.4.2). Nach Korollar 6.6.8.2 ist dann $|\mathrm{Hom}_K(M, N)| = [M\colon K]$. Für $\varphi \in \mathrm{Hom}_K(M, N)$ sei $\varphi_1 \colon M[X] \to N[X]$ die Fortsetzung von φ auf die Polynomringe und $\Omega_\varphi = \big\{\psi \in \mathrm{Hom}_K(L, N) \;\big|\; \psi \,|\, M = \varphi\big\}$. Sei $f \in M[X]$ das Minimalpolynom von α über M. Mit f ist auch $\varphi_1(f) \in \varphi(M)[X]$ irreduzibel und separabel, und nach Korollar 6.5.4.1 ist $N/\varphi(M)$ normal. Sei $F \in K[X]$ das Minimalpolynom von α über K. Dann ist f ein Teiler von F in $M[X]$, also ist auch $\varphi_1(f)$ ein Teiler von $\varphi_1(F) = F$ in $\varphi(M)[X]$. Da F über N in Linearfaktoren zerfällt, zerfällt auch $\varphi_1(f)$ über N in Linearfaktoren. Nach Satz 6.6.7.1 ist $|\Omega_\varphi|$ die Anzahl der Nullstellen von $\varphi_1(f)$ in N, also $|\Omega_\varphi| = \mathrm{gr}(\varphi_1(f)) = \mathrm{gr}(f) = [L\colon M]$, da $\varphi_1(f)$ separabel ist. Damit erhalten wir

$$|\mathrm{Hom}_K(L, N)| = \sum_{\varphi \in \mathrm{Hom}_K(M,N)} |\Omega_\varphi| \;=\; [M\colon K]\,[L\colon M] = [L\colon K]\,,$$

und daher ist L/K nach Korollar 6.6.9.2 separabel.

2. Nach 1. mittels Induktion nach n.

3. Sei L/K separabel. Dann ist nach Definition auch M/K separabel. Für $\alpha \in L$ sei $f \in M[X]$ das Minimalpolynom von α über M und $F \in K[X]$ das Minimalpolynom von α über K. Dann ist F separabel und f ein Teiler von F in $M[X]$, also auch f separabel und daher α separabel über M. Daher ist auch L/M separabel.
Seien nun L/M und M/K separabel. Dann ist $L = M(\alpha_1, \ldots, \alpha_n)$ mit über M separablen Elementen $\alpha_1, \ldots, \alpha_n \in L$, und nach 2. ist L/K separabel.

4. Nach 3. und Korollar 6.5.4. □

Satz 6.6.10 (Satz vom primitiven Element)**.** *Sei L/K eine endliche separable Körpererweiterung. Dann existiert ein $\alpha \in L$ mit $L = K(\alpha)$.*

Beweis. FALL 1: $|K| < \infty$. Wegen $[L:K] < \infty$ ist dann auch $|L| < \infty$ und daher (nach Satz 4.2.5) $L^\times$ eine zyklische Gruppe. Ist $L^\times = \langle\alpha\rangle$, so folgt $L = K(\alpha)$.

FALL 2: $|K| = \infty$. Sei $m \in \mathbb{N}$ minimal, so dass $L = K(\alpha_1, \ldots, \alpha_m)$ mit $\alpha_1, \ldots, \alpha_m \in L$, sei (entgegen der Behauptung) $m \geq 2$, $M = K(\alpha_1, \alpha_2)$ und $[M:K] = n$. Wir zeigen die Existenz eines $\alpha \in M$ mit $M = K(\alpha)$. Dann folgt $L = K(\alpha, \alpha_3, \ldots, \alpha_m)$ im Widerspruch zur Minimalität von m.
Sei $N \supset M$ ein Oberkörper, so dass M/K endlich und normal ist. Da M/K separabel ist, folgt $|\mathrm{Hom}_K(M,N)| = [M:K] = n$ nach Korollar 6.6.8.2. Sei $\mathrm{Hom}_K(M,N) = \{\varphi_1, \ldots, \varphi_n\}$ und

$$F = \prod_{1 \leq i < j \leq n} \Big([\,\varphi_i(\alpha_2) - \varphi_j(\alpha_2)\,]X + [\,\varphi_i(\alpha_1) - \varphi_j(\alpha_1)\,] \Big) \in N[X]\,.$$

Für $i, j \in [1,n]$ mit $i \neq j$ ist $\varphi_i \neq \varphi_j$ und daher $(\varphi_i(\alpha_1), \varphi_i(\alpha_2)) \neq (\varphi_j(\alpha_1), \varphi_j(\alpha_2))$. Damit folgt $F \neq 0$, und da K unendlich ist, existiert ein $c \in K$ mit $F(c) \neq 0$. Für alle $i, j \in [1,n]$ mit $i \neq j$ folgt wegen $c = \varphi_i(c) = \varphi_j(c)$

$$[\,\varphi_i(\alpha_2) - \varphi_j(\alpha_2)\,]c \neq \varphi_i(\alpha_1) - \varphi_j(\alpha_1)\,, \quad \text{also} \quad \varphi_i(\alpha_2 c - \alpha_1) \neq \varphi_j(\alpha_2 c - \alpha_1)\,.$$

Sei $\alpha = \alpha_2 c + \alpha_1 \in M$. Dann folgt $\varphi_i \,|\, K(\alpha) \neq \varphi_j \,|\, K(\alpha)$ für alle $i, j \in [1,n]$ mit $i \neq j$, also (nach Korollar 6.6.8.2) $n \geq [K(\alpha:K)] \geq |\mathrm{Hom}_K(K(\alpha), N)| \geq n$. Daher ist $[K(\alpha):K] = n$, und es folgt $K(\alpha) = L$. □

Satz 6.6.11. *Sei L/K eine endliche Körpererweiterung. Dann sind die folgenden Aussagen äquivalent:*

(a) *L/K ist galoissch.*

(b) *L ist Zerfällungskörper eines separablen über K irreduziblen Polynoms $f \in K[X]$ über K mit $\mathrm{gr}(f) = [L:K]$.*

(c) *L ist Zerfällungskörper eines separablen Polynoms über K.*

Beweis. (a) ⇒ (b) Nach Satz 6.6.10 existiert ein $\alpha \in L$ mit $L = K(\alpha)$. Sei $f \in K[X]$ das Minimalpolynom von α über K. Dann ist f separabel und über K irreduzibel, L ist Zerfällungkörper von f über K, und $\mathrm{gr}(f) = \mathrm{gr}(\alpha) = [L:K]$.

(b) ⇒ (c) Klar.

(c) ⇒ (a) Sei $f \in K[X] \setminus K$ separabel und L Zerfällungskörper von f. Dann ist L/K normal nach Satz 6.5.2, und $L = K(\alpha_1, \ldots, \alpha_n)$, wobei $\alpha_1, \ldots, \alpha_n$ die Nullstellen von f über L sind. Dann sind $\alpha_1, \ldots, \alpha_n$ separabel über K, und daher ist L/K separabel nach Satz 6.6.9. □

Definition und Satz 6.6.12. *Sei L/K eine endliche Körpererweiterung. Dann existiert ein bis auf L-Isomorphie eindeutig bestimmter Oberkörper $N \supset L$ mit folgenden Eigenschaften:*

(a) *N/K ist endlich und normal.*

(b) *Ist $L \subset M \subset N$ ein Zwischenkörper und M/K normal, so folgt $M = N$.*

Ist L/K separabel, so ist auch N/K separabel, also galoissch.

Ein Oberkörper $N \supset L$ mit den Eigenschaften (a) und (b) heißt *normale Hülle* von L/K. Ist L/K separabel, so heißt N eine *galoissche Hülle* von L/K.

BEWEIS. Sei $L = K(\alpha_1, \ldots, \alpha_n)$ mit $n \in \mathbb{N}$ und $\alpha_1, \ldots, \alpha_n \in L$, und sei $N \supset L$ ein Oberkörper, so dass N/K endlich und normal ist (siehe Korollar 6.5.4.2). Für $i \in [1, n]$ sei $f_i \in K[X]$ das Minimalpolynom von α_i über K, und es sei

$$f_i = \prod_{\nu=1}^{n_i} (X - \alpha_{i,\nu}) \text{ mit } \alpha_i = \alpha_{i,1}, \ldots, \alpha_{i,n_i}, \quad A = \{\alpha_{i,\nu} \mid i \in [1,n],\ \nu \in [1, n_i]\} \text{ und } f = f_1 \cdot \ldots \cdot f_n .$$

Genau hat N die Minimaleigenschaft (b), wenn $N = K(A) = L(A)$, wenn also N ein Zerfällungskörper von f über L ist. Daher folgen Existenz und Eindeutigkeit der normalen Hülle aus Satz 6.4.10. Ist L/K separabel, so sind alle f_i und daher alle $\alpha_{i,\nu}$ separabel über K, und daher ist nach Satz 6.6.9.2 auch N/K separabel. □

6.7. Endliche Körper

Satz 6.7.1. *Sei K ein endlicher Körper, $\operatorname{char}(K) = p \in \mathbb{P}$, F der Primkörper von K, $[K:F] = n$ und $\varphi\colon K \to K$ die Frobeniusabbildung von K* (siehe Definition 6.1.1).

1. *$|K| = p^n$ und $a^{p^n} = a$ für alle $a \in K$.*
2. *K ist Zerfällungskörper von $f = X^{p^n} - X \in F[X]$ über F, und die Erweiterung K/F ist galoissch.*
3. *$\operatorname{Gal}(K/F) = \langle\varphi\rangle$, und $\operatorname{ord}(\varphi) = n$.*

BEWEIS. 1. Wegen $n = [K:F] = \dim_F(K)$ ist K als F-Vektorraum isomorph zu F^n, und daher ist $|K| = |F^n| = p^n$. Wegen $|K^\times| = p^n - 1$ und $\operatorname{ord}(a) \,|\, p^n - 1$ folgt $a^{p^n - 1} = 1$ für alle $a \in K^\times$ und daher $a^{p^n} = a$ für alle $a \in K$.

2. Nach 1. ist jedes $a \in K$ Nullstelle von $f = X^{p^n} - X$, und wegen $|K| = p^n$ folgt

$$f = \prod_{a \in K} (X - a) .$$

Daher ist K Zerfällungskörper von f über F, und f hat keine mehrfachen Nullstellen, ist also separabel. Nach Satz 6.6.11 ist K/F galoissch.

3. Nach Satz 6.1.4 ist $\varphi\colon K \to K$ ein Körpermonomorphismus, und nach 1. ist $\varphi \,|\, F = \mathrm{id}_F$. Daher ist $\varphi \in \operatorname{Hom}_F(K, K) = \operatorname{Gal}(K/F)$, und es sei $d = \operatorname{ord}(\varphi)$. Nach Korollar 6.6.8 ist $d \le |\operatorname{Gal}(K/F)| = n$ und $\varphi^d = \mathrm{id}_K$. Für alle $a \in K$ ist $a = \varphi^d(a) = a^{p^d}$ und daher a Nullstelle des Polynoms $X^{p^d} - X$. Also folgt $p^n \le p^d$ und daher $d = n$. □

Korollar 6.7.2.

1. *Ist K ein endlicher Körper, so ist $|K|$ eine Primzahlpotenz.*
2. *Ist $p \in \mathbb{P}$ und $n \in \mathbb{N}$, so gibt es (bis auf Isomorphie) genau einen Körper K mit $|K| = p^n$.*

BEWEIS. 1. Klar.

2. Sei $p \in \mathbb{P}$ und $n \in \mathbb{N}$.

EINDEUTIGKEIT: Seien K, K' Körper mit Primkörpern F, F', und sei $|K| = |K'| = p^n$. Dann ist $\operatorname{char}(K) = \operatorname{char}(K') = p$, also ist $F \cong F'$, es sei $\varphi\colon F \to F'$ ein Isomorphismus und $\varphi_1\colon F[X] \to F'[X]$ seine Fortsetzung auf die Polynomringe. Dann ist $\varphi_1(X^{p^n} - X) = X^{p^n} - X$ (einmal in $F[X]$ und einmal in $F'[X]$ betrachtet). K Nach Satz 6.7.1 ist K ein Zerfällungskörper von $X^{p^n} - X$ über F und

K' ein Zerfällungskörper von $X^{p^n} - X$ über F'. Nach Satz 6.4.9 gibt es daher einen Isomorphismus $\overline{\varphi}\colon K \to K'$ mit $\overline{\varphi} \mid F = \varphi$.

EXISTENZ: Sei $f = X^{p^n} - X \in \mathbb{F}_p[X]$. Dann ist $f' = -1$ und daher f separabel nach Satz 6.6.2. Sei K ein Zerfällungskörper von f über $\mathbb{F}_p$ und $A = \{x \in K \mid f(x) = 0\} = \{x \in K \mid x^{p^n} = x\}$. Dann ist $|A| = p^n$, nach Satz 6.1.4 ist $A \subset K$ ein Teilring, also ein endlicher Bereich und daher ein Körper nach Lemma 3.1.6. □

CHAPTER 7

Fortsetzung der Gruppentheorie

7.1. Konjugierte Elemente und Untergruppen

Definition 7.1.1. Sei G eine Gruppe.

Zur Erinnerung (Definition 2.4.1 und Lemma 2.4.2): Die Menge $\mathrm{End}(G)$ aller Homomorphismen $\tau\colon G \to G$ ist bezüglich der Verknüpfung $\circ$ eine Halbgruppe, die *Endomorphismenhalbgruppe* von G. Ihre Einheitengruppe $\mathrm{Aut}(G) = \mathrm{End}(G)^\times < \mathfrak{S}(G)$ besteht aus allen Isomorphismen $\tau\colon G \to G$ und heißt *Automorphismengruppe* von G.

1. Sei $g \in G$. Die Abbildung
$$\kappa_g\colon G \to G\,, \quad \text{definiert durch} \quad \kappa_g(a) = gag^{-1} \quad \text{für alle} \quad a \in G,$$
heißt *Konjugation* mit g [ist G abelsch, so ist $\kappa_h = \mathrm{id}_G$ für alle $h \in G$].
2. Zwei Elemente $a, b \in G$ heißen *konjugiert*, $a \sim b$, wenn es ein $g \in G$ gibt mit $b = \kappa_g(a) = gag^{-1}$.
3. Zwei Untergruppen $U, V < G$ heißen *konjugiert*, $U \sim V$, wenn es ein $g \in G$ gibt mit $V = \kappa_g(U) = gUg^{-1}$.

Satz 7.1.2. *Sei G eine Gruppe.*

1. *Für jedes $g \in G$ ist die $\kappa_g \in \mathrm{Aut}(G)$, und die Abbildung*
$$\kappa\colon G \to \mathrm{Aut}(G)\,, \quad \textit{definiert durch} \quad \kappa(g) = \kappa_g \quad \textit{für alle} \quad g \in G\,,$$
ist ein Gruppenhomomorphismus, und $\mathrm{Ker}(\kappa) = \mathsf{Z}(G) \lhd G$.
2. *Konjugiertsein ist eine Äquivalenzrelation auf G und auf der Menge der Untergruppen von G. Ist $H < G$ und $g \in G$, so ist $\kappa_g(H) = gHg^{-1} < G$, und aus*
$$G = \biguplus_{i\in I} g_i H \quad \textit{folgt} \quad G = \biguplus_{i\in I} (g_i g^{-1})(gHg^{-1})\,.$$
Insbesondere ist $(G\colon H) = (G\colon gHg^{-1})$, und genau dann ist $H \lhd G$, wenn $H = \kappa_g(H)$ für alle $g \in G$.

Beweis. 1. Sei $g \in G$. Für alle $a, b \in G$ ist $\kappa_g(ab) = gabg^{-1} = (gag^{-1})(gbg)^{-1} = \kappa_g(a)\kappa_g(b)$, und daher ist $\kappa_g \in \mathrm{End}(G)$.

Seien nun $g, h \in G$. Für alle $a \in G$ ist
$$\kappa_{gh}(a) = ghah)(gh)^{-1} = ghah^{-1}g^{-1} = \kappa_g(hah^{-1}) = (\kappa_g \circ \kappa_h)(a)$$
und daher $\kappa(gh) = \kappa(g) \circ \kappa_h$. Daher ist $\kappa\colon G \to \mathrm{End}(G)$ ein Homomorphismus, also $\kappa(G) \subset \mathrm{Aut}(G)$ und $\kappa\colon G \to \mathrm{Aut}(G)$ ein Homomorphismus. Für $g \in G$ gilt:

$$g \in \mathrm{Ker}(\kappa) \iff \kappa_g = \mathrm{id}_G \iff \text{für alle } x \in G \text{ ist } gxg^{-1} = x\,, \text{ also } gx = xg \iff g \in \mathsf{Z}(G)\,.$$

Daher ist $\mathrm{Ker}(\kappa) = \mathsf{Z}(G)$.

2. Ist $H < G$, so folgt $\kappa_g(H) = \{\kappa_g(h) \mid h \in H\} = \{ghg^{-1} \mid h \in H\} = gHg^{-1} < G$, und aus

$$G = \biguplus_{i\in I} g_i H \qquad \text{folgt} \qquad G = Gg^{-1} = \biguplus_{i\in I} g_i H g^{-1} = \biguplus_{i\in I} (g_i g^{-1})(gHg^{-1})\,.$$

Nach Definition ist genau dann $H \lhd G$, wenn $H = gHg^{-1} = \kappa_g(H)$ für alle $g \in G$.
Seien a, b, $c \in G$. Ist $e \in G$ das Einselement, so ist $\kappa_e(a) = a$ und daher $a \sim a$. Ist $a \sim b$ und $g \in G$ mit $\kappa_g(a) = b$, so folgt $a = \kappa_{g^{-1}}(b)$ und daher $b \sim a$. Sei schließlich $a \sim b$ und $b \sim c$, etwa $b = \kappa_g(a)$ und $c = \kappa_h(b)$. Dann folgt $c = \kappa_h \circ \kappa_g(a) = \kappa_{hg}(a)$, also $a \sim c$. Daher ist $\sim$ eine Äquivalenzrelation auf G, und in gleicher Weise zeigt man, dass $\sim$ eine Äquivalenzrelation auf der Menge der Untergruppen vo G ist. □

7.2. Permutationsgruppen

Im ganzen Abschnitt sei $n \in \mathbb{N}$ und $\mathfrak{S}_n = \mathfrak{S}([1,n])$ die *symmetrische Gruppe* auf n Ziffern (siehe Beispiel 2.1.6.9). Die Elemente von $\mathfrak{S}_n$ nennt man *Permutationen*, die Untergruppn von $\mathfrak{S}_n$ nennt man *Permutationsgruppen* auf n Ziffern, und für σ, $\tau \in \mathfrak{S}_n$ sei $\sigma\tau = \sigma \circ \tau$.

Definition 7.2.1.

1. Sei $\sigma \in \mathfrak{S}_n$. Die Menge $|\sigma| = \{i \in [1,n] \mid \sigma(i) \neq i\}$ heißt *Trägermenge* von σ.
2. Seien $r \in \mathbb{N}$ und $i_1, \dots, i_r \in [1,n]$ paarweise verschieden. Dann sei $\sigma = (i_1, \dots, i_r) \in \mathfrak{S}_n$ definiert durch
$$\sigma(i) = \begin{cases} i\,, & \text{falls} \quad i \notin \{i_1, \dots, i_r\}\,, \\ i_{\rho+1}\,, & \text{falls} \quad i = i_\rho \text{ mit } \rho \in [1, r-1]\,, \\ i_1\,, & \text{falls} \quad i = i_r\,, \end{cases}$$
und man nennt σ einen *r-Zykel*. Ein *Zykel* ist ein r-Zykel für ein $r \in \mathbb{N}$. Ein *nicht-trivialer Zykel* ist ein r-Zykel für ein $r > 1$. Eine *Transposition* ist ein 2-Zykel.

Bemerkungen 7.2.2. Sei $r \in [1,n]$, und seien $i_1, \dots, i_r \in [1,n]$ paarweise verschieden.

1. Für alle $\rho \in [1,r]$ ist $(i_1, \dots, i_r) = (i_\rho, i_{\rho+1}, \dots, i_r, i_1, \dots, i_{\rho-1})$.
2. Für $\sigma \in \mathfrak{S}_n$ gilt:
$$\sigma \text{ ist ein 1-Zykel} \iff \big||\sigma|\big| \leq 1 \iff \sigma = \mathrm{id}_{[1,n]} = (1) \iff \sigma = (k) \text{ für ein } k \in [1,n].$$
3. Für alle $\sigma \in \mathfrak{S}_n$ ist $\sigma(|\sigma|) = |\sigma| = |\sigma^{-1}|$.
4. Seien σ, $\tau \in \mathfrak{S}_n$ mit $|\sigma| \cap |\tau| = \emptyset$. Dann folgt $\sigma\tau = \tau\sigma$ und $|\sigma\tau| = |\sigma| \cup |\tau|$.
5. Sei $r \geq 2$ und $\sigma = (i_1, \dots, i_r)$ ein r-Zykel. Dann ist $|\sigma| = \{i_1, \dots, i_r\}$, $\sigma^{-1} = (i_r, i_{r-1}, \dots, i_1)$, $\mathrm{ord}(\sigma) = \big||\sigma|\big| = r$ und $\tau\sigma\tau^{-1} = (\tau(i_1), \dots, \tau(i_r))$ für alle $\tau \in \mathfrak{S}_n$.

Lemma 7.2.3. *Sei $\sigma \in \mathfrak{S}_n$, $k_1 \in |\sigma|$ und $k_i = \sigma^{i-1}(k_1)$ für alle $i \in \mathbb{N}$. Sei $r \in \mathbb{N}$ minimal mit $k_{r+1} \in \{k_1, \dots, k_r\}$. Dann ist $r \geq 2$, $k_{r+1} = k_1$, es sei $\tau = (k_1, \dots, k_r)$ und $\sigma' = \sigma\tau^{-1}$. Dann folgt $|\tau| \subset |\sigma|$ und $|\sigma'| = |\sigma| \setminus |\tau|$. Ist σ ein Zykel, so ist $\sigma = \tau$.*

Beweis. Wegen $k_1 \in |\sigma|$ ist $r \geq 2$. Wäre $k_{r+1} = k_i$ mit $i > 1$, so folgte $k_{r+1} = \sigma(k_r) = k_i = \sigma(k_{i-1})$ und daher $k_r = k_{i-1}$ im Widerspruch zur minimalen Wahl von r. Daher ist $k_{r+1} = k_1$ und $\tau = (k_1, \dots, k_r)$ ein Zykel mit $|\tau| \subset |\sigma|$. Es ist $\sigma' = \sigma\,(k_r, k_{r-1}, \dots, k_1)$ und daher

$$\sigma'(k) = \begin{cases} \sigma(k)\,, & \text{falls} \quad k \notin \{k_1, \dots, k_r\}\,, \\ \sigma(k_r) = k_1\,, & \text{falls} \quad k = k_1\,, \\ \sigma(k_{i-1}) = k_i\,, & \text{falls} \quad k = k_i \text{ für } i \in [2,r]\,. \end{cases}$$

Damit folgt $|\sigma'| = |\sigma| \setminus \{k_1, \dots, k_r\} = |\sigma| \setminus |\tau|$. Ist σ ein Zykel, so hat σ nach Bemerkung 7.2.2.1 eine Darstellug $\sigma = (k_1, \dots)$, und daher ist dann $\sigma = (k_1, \dots, k_r)$. □

Satz 7.2.4 (Existenz- und Eindeutigkeitssatz der Zykeldarstellung)**.** *Sei $\sigma \in \mathfrak{S}_n$.*

1. *σ besitzt eine (bis auf die Reihenfolge der Faktoren) eindeutige Darstellung*

$$\sigma = \sigma_1 \cdot \ldots \cdot \sigma_m$$

mit $m \in \mathbb{N}_0$ und nicht-trivialen Zykeln $\sigma_1, \dots, \sigma_m \in \mathfrak{S}_n$, so dass $|\sigma_i| \cap |\sigma_j| = \emptyset$ für alle $i, j \in [1, m]$ mit $i \neq j$.

2. *σ besitzt eine (nicht notwendigerweise eindeutige) Darstellung als Produkt von Transpositionen. Insbesondere ist $\mathfrak{S}_n = \langle (i, j) \mid i, j \in [1, n],\ i \neq j \,\}\rangle$.*

Beweis. 2. folgt aus 1. und Bemerkung 7.2.2.5.

1. Induktion nach $\operatorname{ord}(\sigma)$. Im Falle $\operatorname{ord}(\sigma) = 1$ ist $\sigma = (1)$ und die Behauptung folgt mit $m = 0$. Sei $\operatorname{ord}(\sigma) \geq 2$, gelte die Behauptung für alle $\sigma' \in \mathfrak{S}_n$ mit $\operatorname{ord}(\sigma') < \operatorname{ord}(\sigma)$.

EXISTENZ: Nach Lemma 7.2.3 gibt es einen nicht-trivialen Zykel $\tau \in \mathfrak{S}_n$ mit $|\tau| \subset |\sigma|$ und $|\sigma\tau^{-1}| = |\sigma| \setminus |\tau|$, also $\operatorname{ord}(\sigma\tau^{-1}) < \operatorname{ord}(\sigma)$. Nach Induktionsvoraussetzung $\sigma\tau^{-1} = \sigma_1 \cdot \ldots \cdot \sigma_m$ mit $m \in \mathbb{N}_0$ und nicht-trivialen Zykeln $\sigma_1, \dots, \sigma_m \in \mathfrak{S}_n$, so dass $|\sigma_i| \cap |\sigma_j| = \emptyset$ für alle $i, j \in [1, m]$ mit $i \neq j$. Daher ist $\sigma = \sigma_1 \cdot \ldots \cdot \sigma_m\tau$, und wegen $|\sigma\tau^{-1}| = |\sigma_1| \cup \ldots \cup |\sigma_m|$ und $|\sigma\tau^{-1}| \cap |\tau| = \emptyset$ folgt $|\sigma_j| \cap |\tau| = \emptyset$ für alle $j \in [1, m]$.

EINDEUTIGKEIT: Sei $\sigma = \sigma_1 \cdot \ldots \cdot \sigma_m = \sigma'_1 \cdot \ldots \cdot \sigma'_l$ mit $l, m \in \mathbb{N}$ und nicht-trivialen Zykeln $\sigma_1, \dots, \sigma_m, \sigma'_1, \dots, \sigma'_l \in \mathfrak{S}_n$, so dass $|\sigma_i| \cap |\sigma_j| = \emptyset$ für alle $i, j \in [1, m]$ mit $i \neq j$, und $|\sigma'_\nu| \cap |\sigma'_\mu| = \emptyset$ für alle $\nu, \mu \in [1, l]$ mit $\nu \neq \mu$. Dann ist $|\sigma| = |\sigma_1| \cup \ldots \cup |\sigma_m| = |\sigma'_1| \cup \ldots \cup |\sigma'_l|$, und es sei (nach geeigneter Umnummerierung) $|\sigma_1| \cap |\sigma'_1| \neq \emptyset$. Für alle $k \in |\sigma_1| \cap |\sigma'_1|$ ist dann $\sigma(k) = \sigma_1(k) = \sigma'_1(k)$. Sei $k_1 \in |\sigma_1| \cap |\sigma'_1|$ und $k_i = \sigma^{i-1}(k_1)$ für alle $i \in [1, n]$. Nach Lemma 7.2.3 gibt es ein $r \in \mathbb{N}_{\geq 2}$, so dass $\sigma_1 = \sigma'_1 = (k_1, \dots, k_r)$. Dann ist aber $\sigma_2 \cdot \ldots \cdot \sigma_m = \sigma'_2 \cdot \ldots \cdot \sigma'_l$, und nach Induktionsvoraussetzung ist $\{\sigma_2, \dots, \sigma_m\} = \{\sigma'_2, \dots, \sigma'_l\}$. □

Korollar 7.2.5. $\mathfrak{S}_n = \langle \{(1, k) \mid k \in [2, n] \,\}\rangle = \langle \{(i, i+1) \mid i \in [1, n-1] \,\}\rangle = \langle \{(1, 2),\ (1, 2, \dots, n)\}\rangle$.

Beweis. Sei $U = \langle \{(1, k) \mid k \in [2, n] \,\}\rangle$, $V = \langle \{(i, i+1) \mid i \in [1, n-1]\}\rangle$, $W = \langle \{(1, 2),\ (1, 2, \dots, n)\}\rangle$. Für alle $k, l \in [1, n]$ mit $k \neq l$ ist $(k, l) = (1, k)(1, l)(1, k) \in U$ und daher $U = \mathfrak{S}_n$ nach Satz 7.2.4.2.

Für alle $k \in [2, n]$ ist $(1, k) = (k-1, k)(k-2, k-1) \cdot \ldots \cdot (2, 3)(1, 2,)(2, 3) \cdot \ldots \cdot (k-1, k) \in V$, also folgt $U \subset V$ und daher $V = \mathfrak{S}_n$.

Sei $\sigma = (1, 2, \dots, n)$ und $\tau = (1, 2)$. Für alle $k \in [2, n]$ ist dann $\sigma^{k-1}\tau\sigma^{-(k-1)} = (k, k+1) \in W$, also folgt $V \subset W$ und daher auch $W = \mathfrak{S}_n$.

□

Definition und Satz 7.2.6. *Für $\sigma \in \mathfrak{S}_n$ sei*

$$\operatorname{sgn}(\sigma) = \prod_{1 \leq i < j \leq n} \frac{\sigma(j) - \sigma(i)}{j - i}\,.$$

1. *Für alle $\sigma \in \mathfrak{S}_n$ ist $\operatorname{sgn}(\sigma) \in \{\pm 1\}$, und für jede Transposition $\tau \in \mathfrak{S}_n$ ist $\operatorname{sgn}(\tau) = -1$.*

   $\operatorname{sgn}(\sigma)$ heißt *Vorzeichen* oder *Signum* von σ. Eine Permutation σ heißt *gerade*, wenn $\operatorname{sgn}(\sigma) = 1$, und *ungerade*, wenn $\operatorname{sgn}(\sigma) = -1$.

2. *Die Abbildung $\operatorname{sgn}\colon \mathfrak{S}_n \to \{\pm 1\}$ ist ein Gruppenhomomorphismus,*

$$\mathfrak{A}_n = \operatorname{Ker}(\operatorname{sgn}) = \{\sigma \in \mathfrak{S}_n \mid \operatorname{sgn}(\sigma) = 1\} \lhd \mathfrak{S}_n\,, \quad \text{und im Falle } n \geq 2 \text{ ist } \quad (\mathfrak{S}_n : \mathfrak{A}_n) = 2\,.$$

   Die Gruppe $\mathfrak{A}_n$ heißt *alternierende Gruppe* auf n Ziffern.

BEWEIS. Sei Z_n die Menge aller 2-elementigen Teilmengen von $[1,n]$. Für $\sigma \in \mathfrak{S}_n$ ist dann

$$Z_n = \big\{\{\sigma(i),\,\sigma(j)\} \bigm| \{i,j\} \in Z_n\big\} \quad \text{und} \quad \Big|\prod_{1\le i<j\le n} \sigma(j)-\sigma(i)\Big| = \Big|\prod_{\{i,j\}\in Z_n} (j-i)\Big| = \prod_{1\le i<j\le n} (j-i)\,.$$

Daher folgt $\operatorname{sgn}(\sigma) \in \{\pm 1\}$ und

$$\operatorname{sgn}(\sigma) = \prod_{\{i,j\}\in Z_n} \frac{\sigma(j)-\sigma(i)}{j-i} = (-1)^{|F(\sigma)|} \quad \text{mit} \quad F(\sigma) = \big\{(i,j) \in Z_n \mid i<j \text{ und } \sigma(i)>\sigma(j)\big\}\,.$$

Für eine Transposition $\tau = (k,l) \in \mathfrak{S}_n$ mit $1 \le k < l \le n$ ist

$F(\sigma) = \{(k,j) \mid j \in [k{+}1, l]\} \cup \{(i,l) \mid i \in [k{+}1, l{-}1]\}$, also $|F(\sigma)| = 2(l{-}k){-}1$ und $\operatorname{sgn}(\tau) = -1$.

Für $\sigma,\, \tau \in \mathfrak{S}_n$ ist

$$\operatorname{sgn}(\sigma\tau) = \prod_{\{i,j\}\in Z_n\}} \frac{\sigma\tau(j)-\sigma\tau(i)}{j-i} = \prod_{\{i,j\}\in Z_n\}} \frac{\sigma\tau(j)-\sigma\tau(i)}{\tau(j)-\tau(i)} \prod_{\{i,j\}\in Z_n\}} \frac{\tau(j)-\tau(i)}{j-i} = \operatorname{sgn}(\sigma)\operatorname{sgn}(\tau)\,,$$

und daher ist $\operatorname{sgn}\colon \mathfrak{S}_n \to \{\pm 1\}$ ein Homomorphismus. Ist $n \ge 2$, so ist sgn ein Epimorphismus und induziert einen Isomorphismus $\mathfrak{S}_n/\mathfrak{A}_n \xrightarrow{\sim} \{\pm 1\}$. Insbesondere ist $\mathfrak{A}_n \lhd \mathfrak{S}_n$ und $(\mathfrak{S}_n : \mathfrak{A}_n) = 2$. □

Definition und Satz 7.2.7. *Sei $n \ge 2$.*

Für $i \in [1,n]$ sei

$$F_i = F_i^{(n)} = \{\sigma \in \mathfrak{S}_n \mid \sigma(i) = i\}\,.$$

Dann ist $F_i < \mathfrak{S}_n$ eine maximale echte Untergruppe (das heißt, es gibt keine Untergruppe $H < \mathfrak{S}_n$ mit $F_i \subsetneq H \subsetneq \mathfrak{S}_n$), und die Abbildung $\rho\colon F_n \to \mathfrak{S}([1,n] \setminus \{i\})$, definiert durch $\rho(\sigma) = \sigma\,|\,[1,n] \setminus \{i\}$, ist ein Isomorphismus. Insbesondere ist $F_i \cong \mathfrak{S}_{n-1}$.

Seien $\sigma_1, \ldots, \sigma_n \in \mathfrak{S}_n$, so dass $\sigma_i(1) = i$ für alle $i \in [1,n]$. Dann folgt

$$\mathfrak{S}_n = \biguplus_{i=1}^{n} \sigma_i F_1\,, \quad \text{für alle } i \in [2,n] \text{ ist } \quad F_i = \sigma_i F_1 \sigma_i^{-1}\,, \quad \text{und} \quad |\mathfrak{S}_n| = n!\,.$$

Insbesondere sind $F_1, \ldots, F_n$ zueinander konjugierte Untergruppen mit $(\mathfrak{S}_n : F_i) = n$.

Für $i \in [1,n]$ heißt F_i die *Fixgruppe* oder *Isotropiegruppe* der Ziffer i in $\mathfrak{S}_n$.

BEWEIS. Sei $i \in [1,n]$. Offensichtlich ist $F_i < \mathfrak{S}_n$ eine Untergruppe und $\rho\colon F_i \to \mathfrak{S}([1,n] \setminus \{i\})$ ist ein Isomorphismus. Ist X eine beliebige Menge mit $|X| = m \in \mathbb{N}$ und $f\colon [1,m] \to X$ eine bijektive Abbildung, so ist $f^*\colon \mathfrak{S}(X) \to \mathfrak{S}_m$, definiert durch $f^*(\varphi) = f \circ \varphi \circ f^{-1}$, ein Isomorphismus (Beispiel 2.4.5.9). Insbesondere ist daher $F_i \cong \mathfrak{S}_{n-1}$.

Es ist $\sigma_i F_1 = F_i \sigma_i = \{\sigma \in \mathfrak{S}_n \mid \sigma(1) = i\}$, denn für $\sigma \in \mathfrak{S}_n$ gilt

$$\begin{aligned} \sigma(1) = i &\iff \sigma\sigma_i^{-1}(i) = i \iff \sigma\sigma_i^{-1} \in F_i \iff \sigma \in F_i\sigma_i \\ &\iff \sigma_i^{-1}\sigma(1) = 1 \iff \sigma_i^{-1}\sigma \in F_1 \iff \sigma \in \sigma_i F_1 \end{aligned}$$

Daher folgt

$$\mathfrak{S}_n = \biguplus_{i=1}^{n} \sigma_i F_1 \quad \text{und} \quad F_i = \sigma_i F_1 \sigma_i^{-1} \quad \text{für alle } i \in [2,n]\,.$$

Insbesondere ist $|\mathfrak{S}_n| = n\,|F_1| = n\,|\mathfrak{S}_{n-1}|$, und mittels Induktion nach n folgt $|\mathfrak{S}_n| = n!$.

Es bleibt zu zeigen, dass F_i eine maximale Untergruppe ist. Ist κ_i die Konjugation mit σ_i, so ist $\kappa_i\colon \mathfrak{S}_n \to \mathfrak{S}_n$ ein Isomorphismus mit $\kappa_i(F_1) = F_i$, und daher genügt es, zu zeigen, dass $F_1 < \mathfrak{S}_n$ eine maximale Untergruppe ist.

Sei $F_1 \subsetneq H < \mathfrak{S}_n$, $\tau \in H \setminus F_1$ und $\tau(1) = k \in [2,n]$. Für $i \in [1,n]$ sei

$$\sigma_i' = \begin{cases} (1)\,, & \text{falls} \quad i = 1\,, \\ (\tau)\,, & \text{falls} \quad i = k\,, \\ (k,i)\tau\,, & \text{falls} \quad i \in [2,n] \setminus \{k\}\,, \end{cases} \qquad \text{also} \quad \sigma_i'(1) = i\,, \quad \text{und daher folgt} \quad \mathfrak{S}_n = \biguplus_{i=1}^{n} \sigma_i' F_1\,.$$

Für alle $i \in [1,n]$ ist $\sigma_i' \in H$, und daher folgt $H = \mathfrak{S}_n$. □

Beispiel 7.2.8 (Untergruppen der $\mathfrak{S}_3$)**.** Es ist $|\mathfrak{S}_3| = 3! = 6$ und

$$\mathfrak{S}_3 = \{(1),\,(1,2),\,(1,3),\,(2,3),\,(1,2,3),\,(1,3,2)\}\,.$$

Ist $H < \mathfrak{S}_3$ und $H \neq \{(1)\}, \mathfrak{S}_3$, so folgt $|H| \in \{2,3\}$, und daher ist H zyklisch nach Satz 2.3.8. Folglich besitzt $\mathfrak{S}_3$ vier nicht-triviale Untergruppen, nämlich den Normalteiler

$$\mathfrak{A}_3 = \langle (1,2,3) \rangle = \langle (1,3,2) \rangle = \{(1),(1,2,3),(1,3,2)\} \quad \text{mit} \quad |\mathfrak{A}_3| = 3\,,$$

und 3 Untergruppen der Ordnung 2, nämlich die zueinander konjugierten Isotropiegruppen $F_1 = \langle (2,3) \rangle$, $F_2 = \langle (1,3) \rangle$ und $F_3 = \langle (2,3) \rangle$.

Beispiel 7.2.9 (Untergruppen der $\mathfrak{S}_4$)**.**

$\mathfrak{S}_4$

$\mathfrak{A}_4$

D'' D D'

F_1 F_2 F_3 F_4

• • • C'' C C' $\mathfrak{V}_4$

A_1 A_2 A_3 A_4

F_{34} F_{12} F_{24} F_{13} F_{23} F_{14} $\langle (1,2)(3,4) \rangle$ $\langle (1,3)(2,4) \rangle$ $\langle (1,4)(2,4) \rangle$

Es ist $|\mathfrak{S}_4| = 4! = 24$, und wir schreiben zunächst die Elemente der $\mathfrak{S}_4$ in ihrer Zykeldarstellung auf.

Ordnung 1: (1).

Ordnung 2: $(1,2)$; $(1,3)$; $(1,4)$; $(2,3)$; $(2,4)$; $(3,4)$; $(1,2)(3,4)$; $(1,3)(2,4)$; $(1,4)(2,3)$.

Ordnung 3: $(1,2,3)$; $(1,3,2)$; $(1,2,4)$; $(1,4,2)$; $(1,3,4)$; $(1,4,3)$; $(2,3,4)$; $(2,4,3)$.

Ordnung 4: $(1,2,3,4)$; $(1,2,4,3)$; $(1,3,2,4)$; $(1,3,4,2)$; $(1,4,2,3)$; $(1,4,3,2)$.

Für $i \in \{1,2,3,4\}$ sei F_i die Isotropiegruppe der Ziffer i in $\mathfrak{S}_4$. Es ist $|F_i| = 6$, F_1, F_2, F_3, F_4 sind maximale zueinander konjugierte und zu $\mathfrak{S}_3$ isomorphe Untergruppen. Sei $A_i = F_i \cap \mathfrak{A}_4$ die Menge der geraden Permutationen in F_i. Dann ist $|A_i| = 3$, $A_i \lhd F_i$, und bei der Isomorphie zwischen F_i und $\mathfrak{S}_3$ entspricht A_i die Gruppe $\mathfrak{A}_3$. Sei $\rho_1 = (1)$; für $i \in \{2,3,4\}$ sei $j \in \{2,3,4\} \setminus \{i\}$ und $\rho_i = (1,i,j) \in \mathfrak{A}_4$. Wegen $\rho_i(1) = i$ folgt $F_i = \rho_i F_1 \rho_i^{-1}$, und daher ist auch $A_i = \rho_i A_1 \rho_i^{-1}$. Folglich sind auch A_1, A_2, A_3, A_4 konjugierte Untergruppen von $\mathfrak{A}_4$ (und nicht nur von $\mathfrak{S}_4$). Insbesondere sind

die Gruppen A_i keine Normalteiler von $\mathfrak{A}_4$. Setzt man $\{1,2,3,4\} = \{i,j,k,l\}$, so folgt $F_i \cap F_j = \langle (k,l)\rangle$, und wir setzen $F_{ij} = F_i \cap F_j$. Die 6 Untergruppen F_{ij} für $1 \le i < j \le 4$ sind zueinander konjugierte Untergruppen von $\mathfrak{S}_4$, in jedem F_i liegen 3 von ihnen und sind bereits dort konjugiert, siehe Beispiel 7.2.8).

Als Nächstes betrachten wir

$$\mathfrak{V}_4 = \{(1);\ (1,2)(3,4);\ (1,3)(2,4);\ (1,4)(2,3)\}\,.$$

Setzt man $\sigma = (1,2)(3,4)$ und $\tau = (1,3)(2,4)$, so folgt $\sigma^2 = \tau^2 = (1)$, $\sigma\tau = \tau\sigma = (1,4)(2,3)$, und daher ist $\mathfrak{V}_4 = \langle \sigma,\tau\rangle < \mathfrak{A}_4$ eine Untergruppe; sie heißt *Klein'sche Vierergruppe*. $\mathfrak{V}_4$ ist abelsch, aber nicht zyklisch, und $|\mathfrak{V}_4| = 4$. Ist $\{1,2,3,4\} = \{i,j,k,l\}$, so gilt für alle $\rho \in \mathfrak{S}_4$

$$\rho\,(i,j)(k,l)\,\rho^{-1} = \big(\rho(i),\rho(j)\big)\big(\rho(k),\rho(l)\big)\,, \quad \text{also} \quad \rho\mathfrak{V}_4\rho^{-1} = \mathfrak{V}_4 \quad \text{und} \quad \mathfrak{V}_4 \lhd \mathfrak{S}_4\,.$$

Mit $\rho = (2,3,4) \in \mathfrak{A}_4$ folgt $\rho\sigma\rho^{-1} = \tau$ und $\rho\tau\rho^{-1} = \sigma\tau$. Daher sind $\langle\sigma\rangle$, $\langle\tau\rangle$ und $\langle\sigma\tau\rangle$ konjugierte Untergruppen in $\mathfrak{A}_4$, aber sie sind Normalteiler in der abelschen Gruppe $\mathfrak{V}_4$.

Wir behaupten nun, dass die genannten Untergruppen alle Untergruppen von $\mathfrak{A}_4$ sind (insbesondere besitzt $\mathfrak{A}_4$ keine Untergruppe der Ordnung 6). Dazu müssen wir zeigen:

a) Sind $\sigma,\tau \in \mathfrak{A}_4$ zwei 3-Zykeln mit $\sigma \notin \{\tau,\tau^{-1}\}$, so folgt $\mathfrak{A}_4 = \langle\sigma,\tau\rangle$.

b) Ist $\sigma \in \mathfrak{A}_4$ ein 3-Zykel und τ das Produkt zweier elementfremder Transpositionen, so folgt $\mathfrak{A}_4 = \langle\sigma,\tau\rangle$.

Beweis von **a)** Seien σ,τ zwei 3-Zykeln mit $\sigma \ne \tau$ und $\sigma \ne \tau^{-1}$. Dann ist $\big||\sigma| \cap |\tau|\big| = 2$, und wir können (nach eventueller Umnummerierung der Ziffern) annehmen, dass $\sigma = (1,2,3)$ und $\tau = (1,2,4)$. Dann ist $\sigma\tau = (1,3)(2,4)$ und $\tau\sigma = (1,4)(2,3)$, also $\mathfrak{V}_4 \subsetneq \langle\sigma,\tau\rangle \subset \mathfrak{A}_4$. Wegen $(\mathfrak{A}_4 : \mathfrak{V}_4) = 3$ folgt $\langle\sigma,\tau\rangle = \mathfrak{A}_4$ nach Satz 2.3.8.

Beweis von **b)** Wie eben können wir (nach eventueller Umnummerierung der Ziffern) annehmen, dass $\sigma = (1,2,3)$. Nun ist aber $\sigma(1,2)(3,4) = (1,3,4)$, $\sigma(1,3)(2,4) = (2,3,4)$ und $\sigma(1,4)(2,3) = (1,4,2)$, und daher enthält dann $\langle\sigma,\tau\rangle$ einen 3-Zykel $\sigma' \notin \{\sigma,\sigma^{-1}\}$. Nach **a)** folgt $\mathfrak{A}_4 = \langle\sigma,\tau\rangle$.

Als Nächstes studieren wir die drei Untergruppen

$$D = \langle (1,2,3,4);\ (2,4)\rangle = \{(1);\ (1,2,3,4);\ (1,3)(2,4);\ (1,4,3,2);\ (2,4);\ (1,2)(3,4)\ \ (1,3);\ (1,4)(2,3)\}\,,$$

$$D' = \langle (1,2,4,3);\ (2,3)\rangle = \{(1);\ (1,2,4,3);\ (1,4)(2,3);\ (1,3,4,2);\ (2,3);\ (1,2)(3,4)\ \ (1,4);\ (1,3)(2,4)\}\,,$$

$$D'' = \langle (1,3,2,4);\ (3,4)\rangle = \{(1);\ (1,3,2,4);\ (1,2)(3,4);\ (1,4,2,3);\ (3,4);\ (1,3)(2,4)\ \ (1,2);\ (1,4)(2,3)\}\,.$$

Jede dieser 3 Untergruppen der Ordnung 8 enthält $\mathfrak{V}_4$. Wegen $(3,4)\,D\,(3,4) = D'$ und $(2,3)\,D\,(2,3) = D''$ sind D, D', D'' konjugierte Untergruppen von $\mathfrak{S}_4$, sie sind also isomorph und haben dieselbe Untergruppenstruktur. Wir beschreiben die Untergruppenstruktur von D. Sei dazu $\sigma = (1,2,3,4)$ und $\tau = (2,4)$. Dann ist

$$\sigma^4 = \tau^2 = (1)\,, \quad \sigma\tau = \tau\sigma^{-1} \quad \text{und} \quad D = \{(1),\,\sigma,\,\sigma^2,\,\sigma^3,\,\tau,\,\sigma\tau,\,\sigma^2\tau,\,\sigma^3\tau\}\,.$$

Die 5 Elemente der Ordnung 2, nämlich σ^2, τ, $\sigma^2\tau$, $\sigma\tau$, $\sigma^3\tau$ erzeugen Untergruppen der Ordnung 2. Wegen $\sigma(\sigma^2\tau)\sigma^{-1} = \tau$ sind $\langle\tau\rangle$ und $\langle\sigma^2\tau\rangle$ konjugierte Untergruppen von D, und wegen $\sigma(\sigma\tau)\sigma^{-1} = \sigma^3\tau$ sind auch $\langle\sigma\tau\rangle$ und $\langle\sigma^3\tau\rangle$ konjugierte Untergruppen von D. Die Untergruppe $\langle\sigma^2\rangle$ ist ein Normalteiler von D (es ist $\rho\sigma^2\rho^{-1} = \sigma^2$ für alle $\rho \in D$). D besitzt drei Untergruppen der Ordnung 4: die zyklische Gruppe $C = \langle\sigma\rangle$ und die beiden nicht-zyklischen Gruppen $\langle\sigma^2,\tau\rangle$ und $\mathfrak{V}_4 = \langle\sigma^2,\sigma\tau\rangle$ (diese sind nach Satz 2.3.2.7 Normalteiler in D). Die zu C konjugierten Untergruppen von D' und D'' bezeichnen wir mit C' und C''.

Wir behaupten, nun bereits alle Untergruppen von $\mathfrak{S}_4$ beschrieben zu haben. Für den Beweis sei $H < \mathfrak{S}_4$ und $H \not\subset \mathfrak{A}_4$. Wir haben die folgenden 8 Fälle zu diskutieren.

1) H enthält zwei 4-Zykeln σ,τ mit $\sigma \notin \{\tau,\tau^{-1}\}$. Wegen $\langle\sigma,\tau\rangle = \langle\sigma^{-1},\tau\rangle = \langle\sigma,\tau^{-1}\rangle = \langle\sigma^{-1},\tau^{-1}\rangle$ genügt es, die beiden Fälle $\sigma = (1,2,3,4)$, $\tau = (1,2,4,3)$ und $\sigma = (1,2,3,4)$, $\tau = (1,3,2,4)$ zu betrachten. Im ersten Falle ist $\sigma\tau = (1,3,2)$ und $\tau\sigma = (1,4,2)$, also enthält H zwei 3-Zykeln ρ_1, ρ_2

mit $\rho_2 \notin \{\rho_1, \rho_1^{-1}\}$. Nach dem oben in **a)** Gezeigten ist $\mathfrak{A}_4 \subset H$. Wegen $(1,2,3,4) \notin \mathfrak{A}_4$ folgt $\mathfrak{A}_4 \subsetneq H$ und daher $H = \mathfrak{S}_4$. Im zweiten Falle ist $\sigma\tau = (1,4,2)$ und $\tau\sigma = (1,4,3)$, und man argumentiert wie eben.

2) H enthält einen 4-Zykel σ und einen 3-Zykel τ. Nach eventueller Umnummerierung der Ziffern können wir annehmen, dass $\sigma = (1,2,3,4)$ und $\tau(1) = 1$. Dann ist $\rho = \tau\sigma\tau^{-1} = (1, \tau(2), \tau(3), \tau(4)) \in H$, wegen $\tau(2) \neq 2$ ist $\rho \neq \sigma$, und wegen $\tau(3) \neq 3$ ist $\rho \neq \sigma^{-1}$. Daher ist $\rho \in H$ ein 4-Zykel mit $\rho \notin \{\sigma, \sigma^{-1}\}$, und nach **1)** ist $H = \mathfrak{S}_4$.

3) H enthält einen 4-Zykel σ und eine Transposition τ. Wegen $\langle\sigma, \tau\rangle = \langle\sigma^{-1}, \tau\rangle$ können wir (nach eventueller Umnummerierung der Ziffern) annehmen, daß $\sigma = (1,2,3,4)$ und entweder $\tau = (1,2)$ oder $\tau = (1,3)$. Im ersten Falle ist $(1,2,3,4)\,(1,2) = (1,3,4) \in H$, also $H = \mathfrak{S}_4$ nach **2)**. Im zweiten Falle ist $D \subset H$, und wegen $(\mathfrak{S}_4 : D) = 3$ folgt $H = D$ oder $H = \mathfrak{S}_4$.

4) H enthält einen 4-Zykel σ und ein Produkt von zwei elementfremden Transpositionen τ, so dass $\tau \neq \sigma^2$. Wegen $\langle\sigma, \tau\rangle = \langle\sigma^{-1}, \tau\rangle$ können wir (nach eventueller Umnummerierung der Ziffern) annehmen, daß $\sigma = (1,2,3,4)$ und $\tau = (1,2)\,(3,4)$. Dann ist aber $D \subset H$, und wie in **3)** folgt $H \in \{D, \mathfrak{S}_4\}$.

5) H enthält einen 3-Zykel σ und eine Transposition τ. Wegen $\langle\sigma, \tau\rangle = \langle\sigma^{-1}, \tau\rangle$ können wir (nach eventueller Umnummerierung der Ziffern) annehmen, dass $\sigma = (1,2,3)$, und entweder $\tau = (1,2)$ oder $\tau = (1,4)$. Im ersten Falle ist $\langle\sigma, \tau\rangle = F_4 \subset H$ und daher $H \in \{F_4, \mathfrak{S}_4\}$ nach Satz 7.2.7. Im zweiten Falle ist $\sigma\tau = (1,4,2,3)$, also $H = \mathfrak{S}_4$ nach **2)**.

6) H enthält zwei elementfremde Transpositionen. Nach eventureller Umnummerierung der Ziffern können wir annehmen, dass $\sigma = (1,3)$ und $\tau = (2,4)$. Dann ist $\langle\sigma, \tau\rangle \subset D$, und wir haben mögliche weitere Elemente von $H \setminus \langle\sigma, \tau\rangle$ zu diskutieren. Enthält H eine dritte Transposition ρ, so können wir $\rho = (1,2)$ annehmen. Dann folgt $\rho\tau\rho = (1,4) \in H$ und daher $H = \mathfrak{S}_4$ nach Korollar 7.2.5. Enthält H das Produkt zweier elementfremder Transpositionen ρ, so dass $\rho \neq \sigma\tau$, so folgt $\langle\rho, \sigma, \tau\rangle = D \subset H$ und daher $H \in \{\mathfrak{S}_4, D\}$. Enthält H einen 3-Zykel oder einen 4-Zykel, so folgt $H \in \{D, F_4, \mathfrak{S}_4\}$ nach **3)** und **5)**.

7) H enthält zwei Transpositionen σ, τ mit $|\sigma| \cap |\tau| \neq \emptyset$. Wir können (nach eventueller Umnummerierung der Ziffern) $\sigma = (1,2)$ und $\tau = (1,3)$ annehmen. Dann ist $F_4 = \langle\sigma, \tau\rangle \supset H$, also $H \in \{F_4, \mathfrak{S}_4\}$ nach Satz 7.2.7.

8) H enthält das Produkt zweier elementfremder Transpositionen σ, aber nur eine Transposition τ. Nach eventueller Umnummerierung der Ziffern können wir $\sigma = (1,2)(3,4)$ und $\tau = (1,3)$ annehmen. Wegen $\sigma\tau = (1,4,3,2)$ folgt $H \in \{D, \mathfrak{S}_4\}$ nach **3)**.

Satz 7.2.10. *Sei $n \geq 3$.*

1. $\mathfrak{A}_n = \langle\{\sigma \in \mathfrak{S}_n \mid \sigma \textit{ ist ein 3-Zykel}\}\rangle$.
2. *Ist $N < \mathfrak{S}_n$ und $(\mathfrak{S}_n : N) = 2$, so folgt $N = \mathfrak{A}_n$.*
3. (Satz von Abel) *Ist $n \geq 5$, so sind $\{(1)\}$ und $\mathfrak{A}_n$ die einzigen Normalteiler von $\mathfrak{A}_n$.*

BEWEIS. 1. Sei $N = \langle\{\sigma \in \mathfrak{S}_n \mid \sigma \text{ ist ein 3-Zykel}\}\rangle$. Jedes $\sigma \in \mathfrak{A}_n$ ist Produkt einer geraden Anzahl von Transpositionen. Daher genügt es, zu zeigen, daß das Produkt von je zwei Transpositionen in N liegt. Seien also $\tau, \tau' \in \mathfrak{S}_n$ Transpositionen. Im Falle $\tau = \tau'$ ist $\tau\tau' = (1) \in N$. Im Falle $|\tau| \cap |\tau'| = \emptyset$ sei $\tau = (i,j)$ und $\tau' = (k,l)$ mit $|\{i,j,k,l\}| = 4$. Dann folgt $\tau\tau' = (i,k,l)(i,j,l) \in N$. Im Falle $|\tau| \cap |\tau'| \neq \emptyset$ und $\tau \neq \tau'$ sei $\tau = (i,j)$ und $\tau' = (i,k)$ mit $j \neq k$. Dann folgt $\tau\tau' = (i,k,j) \in N$.

2. Sei $N < \mathfrak{S}_n$, so dass $(\mathfrak{S}_n : N) = 2$. Wir zeigen, dass N alle 3-Zykeln enthält. Sei also $\sigma \in \mathfrak{S}_n$ ein 3-Zykel. Wegen $|\mathfrak{S}_n / N| = 2$ ist $|\{N, \sigma N, \sigma^2 N\}| \leq 2$, also $\sigma N = N$ oder $\sigma N = \sigma^2 N$ und daher $\sigma \in N$.

3. Sei $n \geq 5$ und $N \lhd \mathfrak{A}_n$ mit $|N| > 1$. Wir zeigen zuerst, dass N einen 3-Zykel enthält. Sei dazu $\sigma \in N \setminus \{(1)\}$. Wegen $N \subset \mathfrak{A}_n$ ist σ keine Transposition und daher $|\sigma| \geq 4$. Sei $\sigma = \sigma_1 \cdot \ldots \cdot \sigma_r$ mit

nicht-trivialen Zykeln $\sigma_1, \dots, \sigma_r \in \mathfrak{S}_n$, so dass $|\sigma_i| \cap |\sigma_j| = \emptyset$ für alle $i, j \in [1,r]$ mit $i \neq j$ und $\big||\sigma_1|\big| \geq \dots \geq \big||\sigma_r|\big| \geq 2$.

FALL 1: $\big||\sigma_1|\big| = k \geq 4$. Dann ist $\sigma = (i_1, \dots, i_k)\sigma'$ mit $\sigma' \in \mathfrak{S}_n$ und $|\sigma'| \cap \{i_1, \dots, i_k\} = \emptyset$. Mit $\lambda = (i_1, i_2, i_3) \in \mathfrak{A}_n$ folgt $\sigma^{-1}(\delta\sigma\delta^{-1}) = (i_1, i_3, i_k) \in N$.

FALL 2: $r \geq 2$ und $\big||\sigma_1|\big| = 3 > \big||\sigma_2|\big|$. Dann ist $\sigma^2 = \sigma_1^2 \in N$ ein 3-Zykel.

FALL 3: $r \geq 2$ uns $\big||\sigma_1|\big| = \big||\sigma_2|\big| = 3$. Dann ist $\sigma = (i_1, i_2, i_3)(i_4, i_5, i_6)\,\sigma'$ mit $\sigma' \in \mathfrak{S}_n$, $|\sigma'| \cap \{i_1, \dots, i_6\} = \emptyset$ und $|\{i_1, \dots, i_6\}| = 6$. Mit $\delta = (i_1, i_2, i_4) \in \mathfrak{A}_n$ folgt

$$\widetilde{\sigma} = \sigma^{-1}(\delta\sigma\delta^{-1}) = (i_1, i_4, i_2, i_6, i_3) \in N\,,$$

und nach FALL 1, angewandt auf $\widetilde{\sigma}$ an Stelle von σ, enthält N einen 3-Zykel.

FALL 4: $r = 2$ und $\big||\sigma_1|\big| = \big||\sigma_2|\big| = 2$. Dann ist $\sigma = (i_1, i_2)(i_3, i_4)$. Mit $i_5 \in [1,n] \setminus \{i_1, \dots, i_4\}$ und $\delta = (i_1, i_2, i_5)$ folgt $\sigma^{-1}(\delta\sigma\delta^{-1}) = (i_1, i_2, i_5) \in N$.

FALL 5: $r \geq 3$ und $\big||\sigma_1|\big| = \big||\sigma_2|\big| = \big||\sigma_3|\big| = 2$. Dann ist $\sigma = (i_1, i_2)(i_3, i_4)(i_5, i_6)\,\sigma'$ mit $\sigma' \in \mathfrak{S}_n$, $|\{i_1, \dots, i_6\}| = 6$ und $|\sigma'| \cap \{i_1, \dots, i_6\} = \emptyset$. Mit $\delta = (i_1, i_2, i_5) \in \mathfrak{A}_n$ folgt

$$\widetilde{\sigma} = \sigma^{-1}(\delta\sigma\delta^{-1}) = (i_1, i_5)(i_2, i_6)\,,$$

und nach FALL 4, angewandt auf $\widetilde{\sigma}$ an Stelle von σ, enthält N einen 3-Zykel.

Sei nun $(i,j,k) \in N$ ein 3-Zykel. Nach 1. genügt es, zu zeigen, dass N alle 3-Zykeln enthält. Sei also (i',j',k') ein weiterer 3-Zykel. Dann gibt es ein $\tau \in \mathfrak{S}_n$ mit $\tau(i) = i'$, $\tau(j) = j'$ und $\tau(k) = k'$. Wegen $n \geq 5$ existieren $l_1, l_2 \in [1,n] \setminus \{i', j', k'\}$ mit $l_1 \neq l_2$, und es sei

$$\rho = \begin{cases} \tau & \text{falls} \quad \tau \in \mathfrak{A}_n\,, \\ (l_1, l_2) \circ \tau\,, & \text{falls} \quad \tau \notin \mathfrak{A}_n\,. \end{cases}$$

Dann ist $\rho \in \mathfrak{A}_n$, $\rho(i) = i'$, $\rho(j) = j'$, $\rho(k) = k'$ und $\rho\,(i,j,k)\,\rho^{-1} = (i',j',k') \in N$. □

Satz 7.2.11 (Satz von Cayley)**.** *Sei G eine Gruppe. Für $x \in G$ sei $\tau_x \colon G \to G$ definiert durch $\tau_x(g) = xg$ für alle $g \in G$. Dann ist $\tau_x \in \mathfrak{S}(G)$, und die Abbildung*

$$\tau \colon G \to \mathfrak{S}(G)\,, \quad \textit{definiert durch} \quad \tau(x) = \tau_x\,,$$

ist ein Gruppenmonomorphismus. Insbesondere ist G isomorph zu einer Untergruppe von $\mathfrak{S}(G)$ (und im Falle $|G| = n$ zu einer Permutationsgruppe auf n Ziffern).

Beweis. Für $x \in G$ ist $\tau_x \circ \tau_{x^{-1}} = \mathrm{id}_G$, also $\tau_x \in \mathfrak{S}(G)$. Für alle $x, y \in G$ ist

$$\tau_{xy}(g) = xyg = x\tau_y(g) = \tau_x\tau_y(g) \quad \text{für alle} \quad g \in G\,, \quad \text{also} \quad \tau_{xy} = \tau_x\tau_y\,.$$

Daher ist τ ein Homomorphismus. Ist $x \in \mathrm{Ker}(\tau)$, so folgt $\tau_x = id_G$, also $g = xg$ für alle $g \in G$ und daher $x = e$. □

7.3. Operationen einer Gruppe auf einer Menge

Definition 7.3.1. Sei G eine Gruppe und M eine nichtleere Menge.

1. Eine *Operation von G auf M* ist eine Abbildung

$$* \colon G \times M \to M\,, \quad (g,m) \mapsto g * m = gm\,,$$

so dass für alle $g, g' \in G$ und alle $m \in M$ die beiden folgenden Bedingungen gelten:

- $1_G m = m$.
- $(gg')m = g(g'm)$.

2. Sei $G\times M \to M$ eine Operation von G auf M. Für $m \in M$ sei

$$G_m = \{g \in G \mid gm = m\} < G \quad \text{und} \quad Gm = \{gm \mid g \in G\} \subset M\,.$$

Die Untergruppe $G_m < G$ heißt *Isotropiegruppe* oder *Fixgruppe* oder *Stabilisator* von m in G, die Menge Gm heißt *Bahn* oder *Orbit* von m unter G.

$G\backslash M = \{Gm \mid m \in N\}$ heißt *Bahnenraum* der Operation $G\times M \to M$. Eine Familie $(m_i)_{i\in I}$ in M heißt *Repräsentantensystem* des Bahnenraumes, wenn $G\backslash M = \{Gm_i \mid i \in I\}$ und $Gm_i \neq Gm_j$ für alle $i, j \in I$ mit $i \neq j$.

Bemerkungen und Beispiele 7.3.2.

1. Sei G eine Gruppe, $M \neq \emptyset$ eine Menge und $*\colon G\times M \to M$ eine Operation von G auf M. Für alle $g \in G$ und $m, m' \in M$ ist dan $g(g^{-1}m) = m$, und aus $gm = m'$ folgt $m = g^{-1}m'$. Die Abbildung

$$\rho\colon G \to \mathfrak{S}(M)\,, \quad \text{definiert durch} \quad \rho(g)(m) = g * m \ \text{ für alle } \ g \in G \ \text{ und } \ m \in M\,,$$

ist ein Gruppenhomomorphismus.

2. Sei K ein Körper und V ein K-Vektorraum. Dann ist die skalare Multiplikation $K\times V \to V$, $(\lambda, v) \mapsto \lambda v$, eine Operation der Additionsgruppe von K auf der Additionsgruppe von V.

3. Sei M eine Gruppe und $G < M$ eine Untergruppe. Die Operation $*\colon G\times M \to M$ von G auf M sei definiert durch $g * m = gm$ für alle $g \in G$ und $m \in M$. Für $m \in M$ ist dann $G_m = \{e\}$ und Gm ist die durch m bestimmte Rechtsnebenklasse von G in M. Der Bahnenraum $G\backslash M$ ist gerade der Rechtsnebenklassenraum (Konsistenz der Bezeichnungen!).

4. Sei $M \neq \emptyset$ eine Menge und $G \subset \mathfrak{S}(M)$ eine Untergruppe. Dann operiert G auf M (in natürlicher Weise) vermöge $(f, m) \mapsto f(m)$. Ist insbesondere $n \in \mathbb{N}$, so operiert $\mathfrak{S}_n$ auf $[1, n]$. Für alle $i \in [1, n]$ ist $[1, n]$ die Bahn und F_i die Isotropiegruppe von i (siehe Satz 7.2.7).

Satz 7.3.3. *Sei G eine Gruppe, M eine nichtleere Menge und $*\colon G\times M \to M$ eine Operation von G auf M.*

1. *Für alle $m_1, m_2 \in M$ ist entweder $Gm_1 = Gm_2$ oder $Gm_1 \cap Gm_2 = \emptyset$.*
2. *Für alle $m \in M$ ist $|Gm| = (G\colon G_m)$.*
3. (Bahnengleichung) *Sei $(m_i)_{i\in I}$ ein Repräsentantensystem des Bahnenraumes. Dann ist*

$$|M| = \sum_{i\in I} (G\colon G_{m_i}).$$

Beweis. 1.Seien $m_1, m_2 \in M$ und $m \in Gm_1 \cap Gm_2$. Dann ist $m = gm_1$ für ein $g \in G$ und daher $Gm = G(gm_1) = (Gg)m_1 = Gm_1$. Analog folgt $Gm = Gm_2$.

2. Sei $m \in M$ und $(g_j)_{j\in J}$ ein Repräsentantensystem von G/G_m. Dann folgt

$$Gm = \bigcup_{j\in J} g_j G_m m = \{g_j m \mid j \in J\}\,,$$

und daher genügt es, zu zeigen: Sind $j, k \in J$ mit $g_j m = g_k m$, so folgt $j = k$. Seien $j, k \in J$ mit $g_j m = g_k m$. Dann folgt $g_k^{-1} g_j m = m$, also $g_k^{-1} g_j \in G_m$ und daher $g_j G_m = g_k G_m$, also $j = k$.

3. Wegen

$$M = \biguplus_{i\in I} Gm_i \quad \text{folgt} \quad |M| = \sum_{i\in I} |Gm_i| = \sum_{i\in I} (G\colon G_{m_i}) \qquad (\text{nach } 2.)\,.$$

□

7.4. Zentralisatoren, Normalisatoren und Sylow'sche Sätze

Definition 7.4.1. Sei G eine Gruppe. Für $x \in G$ heißt

- $\mathsf{k}(x) = \{g \in G \mid g \sim x\} = \{hxh^{-1} \mid h \in G\}$ die *Konjugiertheitsklasse* von x,
- $\mathsf{C}(x) = \{g \in G \mid gxg^{-1} = x\} = \{g \in G \mid gx = xg\}$ der *Zentralisator* von x, und

$$\mathsf{Z}(G) = \{g \in G \mid gx = xg \text{ für alle } x \in G\} = \bigcap_{a \in G} \mathsf{C}(a) \quad \text{heißt } \textit{Zentrum} \text{ von } G.$$

Eine Familie $(x_i)_{i \in I}$ in G heißt *Repräsentantensystem der nicht-trivialen Konjugiertenklassen*, wenn $|\mathsf{k}(x_i)| > 1$ für alle $i \in I$, und $\mathsf{k}(x_i) \cap \mathsf{k}(x_j) = \emptyset$ für alle $i, j \in I$ mit $i \neq j$.

Zur Erinnerung (Definition 4.2.1):
Sei p eine Primzahl. Dann heißt $G_p = \{g \in G \mid \operatorname{ord}(g) \text{ ist eine } p\text{-Potenz}\}$ die *p-Komponente* von G, und G heißt *p-Gruppe*, wenn $G = G_p$. Eine Untergruppe $H < G$ heißt *p-Sylowgruppe* von G, wenn H eine maximale p-Untergruppe von G ist (das heißt, H ist eine p-Gruppe und es gibt keine p-Gruppe $H' < G$ mit $H \subsetneq H'$). Mit $\operatorname{Syl}_p(G)$ bezeichnen wir die Menge der p-Sylowgruppen von G.

Satz 7.4.2. *Sei G eine endliche Gruppe.*

1. *Für $x \in G$ ist $\mathsf{C}(x) < G$ und $|\mathsf{k}(x)| = (G : \mathsf{C}(x))$.*
2. *Für $x \in G$ gilt: $x \in \mathsf{Z}(G) \iff \mathsf{C}(x) = G \iff |\mathsf{k}(x)| = 1$.*
3. (Klassengleichung) *Sei $(x_1, \ldots, x_m)$ ein Repräsentantensystem der nicht-trivialen Konjugiertenklassen von G. Dann ist*

$$|G| = |\mathsf{Z}(G)| + \sum_{j=1}^{m} (G : \mathsf{C}(x_j)) .$$

4. (Satz von Cauchy) *Sei $p \in \mathbb{P}$ und $p \mid |G|$. Dann gibt es ein $a \in G$ mit $\operatorname{ord}(a) = p$ (und daher auch eine Untergruppe $U < G$ mit $|U| = p$).*
5. *Sei p eine Primzahl. Genau dann ist G eine p-Gruppe, wenn $|G|$ eine p-Potenz ist. Ist G eine p-Gruppe und $|G| > 1$, so ist auch $|\mathsf{Z}(G)| > 1$.*

Beweis. Sei $*\colon G \times G \to G$ definiert durch $g * x = gxg^{-1}$ für alle $g, x \in G$. Dann ist $*$ eine Operation von G auf G (G operiert auf sich selbst durch Konjugation). Für $x \in G$ ist dabei $G_x = \{g \in G \mid gxg^{-1} = x\} = \mathsf{C}(x)$ die Isotropiegruppe von x und $G * x = \{gxg^{-1} \mid g \in G\} = \mathsf{k}(x)$ die Bahn von x. Daher ist $\mathsf{C}(x) < G$, und nach Satz 7.3.3.2 folgt $|\mathsf{k}(x)| = (G : \mathsf{C}(x))$. Damit folgt 1.

2. Nach Definition ist genau dann $x \in \mathsf{Z}(G)$, wenn $\mathsf{C}(x) = G$, und das ist nach 1. äquivalent zu $|\mathsf{k}(x)| = 1$.

3. Ist $\mathsf{Z}(G) = \{z_1, \ldots, z_k\}$, so ist $(z_1, \ldots, z_k, x_1, \ldots, x_m)$ ein Repräsentantensystem des Bahnenraumes der Operation $*$, und die Behauptung folgt aus Satz 7.3.3.3.

4. Induktion nach $|G|$. Ist G abelsch, so folgt die Behauptung aus Satz 4.2.3.2(b). Sei nun G beliebig und gelte die Behauptung für alle Gruppen G' mit $|G'| < |G|$. Im Falle $p \mid \mathsf{Z}(G)$ gibt es ein $a \in \mathsf{Z}(G)$ mit $\operatorname{ord}(a) = p$, da $\mathsf{Z}(G)$ abelsch ist. Sei also $p \nmid |\mathsf{Z}(G)|$. Nach 3. ist dann $p \nmid (G : \mathsf{C}(x))$ für ein $x \in G$ mit $|\mathsf{k}(x)| = (G : \mathsf{C}(x)) > 1$. Wegen $|G| = (G : \mathsf{C}(x))\,|\mathsf{C}(x)|$ folgt $p \mid |\mathsf{C}(x)|$ und $|\mathsf{C}(x)| < |G|$. Nach Induktionsvoraussetzung enthält $\mathsf{C}(x)$ ein Element der Ordnung p.

5. Ist $|G|$ eine p-Potenz, so ist für alle $a \in G$ auch $\operatorname{ord}(a)$ eine p-Potenz nach Satz 2.3.8.2 und daher G eine p-Gruppe. Ist $|G|$ keine p-Potenz, so gibt es ein $q \in \mathbb{P}$ mit $q \mid |G|$, und nach 4. gibt es ein Element $a \in G$ mit $\operatorname{ord}(a) = q$. Daher ist dann G keine p-Gruppe.

Sei nun G eine p-Gruppe und $|G| > 1$. In der Klassengleichung (siehe 3.) ist für alle $j \in [1, m]$ (nach 1.) $(G : \mathsf{C}(x_j)) > 1$, und wegen $(G : \mathsf{C}(x_j)) \mid |G|$ folgt $p \mid (G : \mathsf{C}(x_j))$ und daher auch $p \mid |\mathsf{Z}(G)|$. □

Definition 7.4.3. Sei G eine Gruppe und $H < G$ eine Untergruppe. Dann heißt

$$\mathsf{N}_G(H) = \{g \in G \mid gHg^{-1} = H\}$$

der *Normalisator* von H in G.

Satz 7.4.4. *Sei G eine endliche Gruppe und $H < G$ eine Untergruppe.*

1. *$\mathsf{N}_G(H)$ ist die größte Untergruppe von G mit $H \lhd \mathsf{N}_G(H)$, und $(G:\mathsf{N}_G(H))$ ist die Anzahl der zu H konjugierten Untergruppen von G.*
2. *Sei p eine Primzahl, $n \in \mathbb{N}$ und $|H| = p^n$. Dann ist*

$$(G:H) \equiv (\mathsf{N}_G(H):H) \mod p\,,$$

und für jede Untergruppe $U < G$ mit $p \nmid (G:U)$ gibt es ein $x \in G$ mit $H \subset xUx^{-1}$.

Beweis. 1. Sei Σ die Menge aller Untergruppen von G, und sei $*\colon G \times \Sigma \to \Sigma$ definiert durch $g*U = gUg^{-1}$. Dann ist $*$ eine Operation von G auf Σ. Für $H \in \Sigma$ ist dann $\mathsf{N}_G(H)$ die Isotropiegruppe von H, und $G*H = \{gHg^{-1} \mid g \in G\}$ ist die Menge der zu H konjugierten Untergruppen von G. Daher ist $\mathsf{N}_G(H) < G$, und nach Definition ist $\mathsf{N}_G(H)$ die größte Untergruppe von G, in der H ein Normalteiler ist. Nach Satz 7.3.3.2 ist $(G:\mathsf{N}_G(H))$ die Anzahl der zu H konjugierten Untergruppen von G.

2. Sei $U < G$ und $*\colon H \times G/U \to G/U$ definiert durch $g * xU = gxU$. Dann ist $*$ eine Operation von H auf G/U. Seien $x_1, \ldots, x_m \in G$, so dass $(x_1U, \ldots, x_mU)$ ein Repräsentantensystem des Bahnenraumes von $*$ ist. Für $j \in [1,m]$ sei $H_{x_jU} \subset H$ die Isotropiegruppe von x_jU. Nach Satz 7.3.3.3 und wegen $|H| = p^n$ ist dann

$$|G/U| = \sum_{j=1}^{m} (H:H_{x_jU}) \;\equiv\; \big|\{j \in [1,m] \mid H_{x_jU} = H\} \mod p\,.$$

Ist nun $p \nmid (G:U)$, so gibt es ein $j \in [1,m]$ mit $H_{x_jU} = H$. Für alle $g \in H$ ist dann $gx_j \in x_jU$ und daher $H \subset x_jUx_j^{-1}$. Damit ist 4. gezeigt.

Für den Beweis von 3. sei nun $H = U$. Sei $s \in [0,m]$, so daß $H_{x_jH} = H$ für alle $j \in [1,s]$ und $H_{x_jH} \neq H$ für alle $j \in [s+1,m]$. Dann folgt $(G:H) \equiv s \mod p$, und daher genügt es, zu zeigen, daß $(x_1, \ldots, x_s)$ ein Repräsentantensystem von $\mathsf{N}_G(H)/H$ ist.

Für $j \in [1,s]$ ist $Hx_j \subset Hx_jH = x_jH$, also $H \subset x_jHx_j^{-1}$. Daraus folgt $x_jHx_j^{-1} = H$, also $x_j \in \mathsf{N}_G(H)$. Ist $x \in \mathsf{N}_G(H)$, so folgt $xH = gx_jH$ für ein $g \in H$ und $j \in [1,m]$, also $x = gx_jh$ mit $h \in H$. Daher ist $x_j = g^{-1}xh^{-1} \in \mathsf{N}_G(H)$ und $x = x_j(x_j^{-1}gx_jh) \in x_jH$. Nach Definition ist $x_iH \neq x_jH$ für alle $i, j \in [1,m]$ mit $i \neq j$. □

Satz 7.4.5. *Sei G eine endliche Gruppe, $p \in \mathbb{P}$, $n \in \mathbb{N}$, $p^n \,\big|\, |G|$ und $i \in [1,n]$.*

1. *Sei $i < n$ und $H < G$ mit $|H| = p^i$. Dann gibt es eine Untergruppe $H' < G$ mit $H \lhd H'$ und $|H'| = p^{i+1}$. Ist insbesondere $|G| = p^n$ und $H = p^{n-1}$, so folgt $H \lhd G$.*
2. *Es gibt eine Untergruppe $H < G$ mit $|H| = p^i$.*

Beweis. 1. Wegen $p^n \,\big|\, |G| = (G:H)\,|H|$ und $i < n$ folgt $p \,|\, (G:H)$, also

$$(\mathsf{N}_G(H):H) \equiv (G:H) \equiv 0 \mod p$$

nach Satz 7.4.4.2. Wegen $H \lhd \mathsf{N}_G(H)$ und $p \,\big|\, |\mathsf{N}_G(H)/H|$ gibt es nach Satz 7.4.2.4 eine Untergruppe $U' < \mathsf{N}_G(H)/H$ mit $|U'| = p$. Nach Korollar 2.5.11 ist $U' = H'/H$ mit $H < H' < \mathsf{N}_G(H)$. Dann ist $H \lhd H'$, $(H':H) = |U'| = p$ und $H' = (H':H)\,|H| = p^{i+1}$.

2. Induktion nach i.

$i = 1$: Nach Satz 7.4.2.4.

$i \geq 1$, $i \to i+1$: Nach 1. □

Satz 7.4.6 (Sylow'sche Sätze)**.** *Sei G eine endliche Gruppe, $|G| = p^n m$ mit $p \in \mathbb{P}$, $m, n \in \mathbb{N}$ und $p \nmid m$.*

1. $\mathrm{Syl}_p(G) = \{H < G \mid |H| = p^n\} = \{H < G \mid (G:H) = m\} \neq \emptyset$.
2. *Sei $H \in \mathrm{Syl}_p(G)$. Dann ist $\mathrm{Syl}_p(G)$ die Menge der zu H konjugierten Untergruppen von G.*
3. $|\mathrm{Syl}_p(G)| \equiv 1 \bmod p$, *und* $|\mathrm{Syl}_p(G)| \mid |G|$.

Beweis. 1. Sei $H < G$. Wegen $|G| = (G:H)\,|H|$ ist genau dann $|H| = p^n$, wenn $(G:H) = m$. Ist $H < G$ mit $|H| = p^n$, so ist H eine maximale p-Untergruppe von G, also $H \in \mathrm{Syl}_p(G)$, und daher ist $\mathrm{Syl}_p(G) \neq \emptyset$ nach Satz 7.4.5.2 (mit $i = n$). Ist $H < G$ und $|H| = p^i$ mit $i < n$, so ist $H \notin \mathrm{Syl}_p(G)$ nach Satz 7.4.5.1.

2. Sei $U < G$. Ist U zu H konjugiert, so ist $|U| = p^n$ und daher $U \in \mathrm{Syl}_p(G)$ nach 1. Ist umgekehrt $U \in \mathrm{Syl}_p(G)$, so ist $p \nmid (G:U)$, und nach Satz 7.4.4.2 gibt es ein $x \in G$ mit $H \subset xUx^{-1}$. Wegen $|xUx^{-1}| = |U| = p^n = |H|$ folgt $H = xUx^{-1}$.

3. Sei $H \in \mathrm{Syl}_p(G)$. Nach 2. ist $|\mathrm{Syl}_p(G)|$ die Anzahl der zu H konjugierten Untergruppen von G. Aus Satz 7.4.4 folgt $|\mathrm{Syl}_p(G)| = (G:\mathsf{N}_G(H) \mid |G|$ und

$$(G:H) = (G:\mathsf{N}_G(H))\,(\mathsf{N}_G(H):H) \equiv (\mathsf{N}_G(H):H) \mod p\,, \quad \text{also} \quad p \mid (\mathsf{N}_G(H):H)\big[(G:\mathsf{N}_G(H)) - 1\big]\,.$$

Wegen $p \nmid (G:H)$ ist auch $p \nmid (\mathsf{N}_G(H):H)$, und daher folgt $p \mid \big[(G:\mathsf{N}_G(H)) - 1\big]$, also $|\mathrm{Syl}_p(G) \equiv 1 \bmod p$. □

7.5. Auflösbare Gruppen

Definition 7.5.1. Eine Gruppe G heißt *auflösbar*, wenn es ein $k \in \mathbb{N}$ und eine absteigende Folge

$$G = G_0 > G_1 > \ldots > G_k = \{e\}$$

von Untergruppen gibt, so dass für alle $i \in [1,k]$ gilt: $G_i \lhd G_{i-1}$ und G_{i-1}/G_i ist abelsch.

Jede solche Folge von Untergruppen nennt man eine *Auflösung* von G.

Satz 7.5.2. *Sei G eine endliche Gruppe.*

1. *Ist G abelsch, so ist G auflösbar.*
2. *Ist G auflösbar und $H < G$, so ist H auflösbar.*
3. *Ist G auflösbar und $f: G \to G'$ ein Gruppenepimorphismus, so ist auch G' auflösbar.*
4. *Ist $N \lhd G$, so ist G genau dann auflösbar, wenn N und G/N auflösbar sind.*
5. *Ist $|G| = p^n$ mit $p \in \mathbb{P}$ und $n \in \mathbb{N}$, so ist G auflösbar.*

Beweis. 1. Die Folge $G > \{e\}$ hat die gewünschte Eigenschaft.

2. Sei $G = G_0 > G_1 > \ldots > G_k = \{e\}$ eine Auflösung von G. Nach Satz 2.5.8 gilt für alle $i \in [1,k]$: $G_i \cap H = G_i \cap (G_{i-1} \cap H) \lhd G_{i-1} \cap H$,

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

und da G_{i-1}/G_i abelsch ist, ist auch $G_{i-1} \cap H/G_i \cap H$ abelsch. Daher ist

$$H = G_0 \cap H > G_1 \cap H > G_1 \cap H > \ldots > G_k \cap H = \{e\} \quad \text{eine Auflösung von } H.$$

3. Sei $G = G_0 > G_1 > \ldots > G_k = \{e\}$ eine Auflösung von G. Nach Satz 2.5.10 gilt für alle $i \in [1,k]$: $f(G_i) \lhd f(G_{i-1})$, und $f(G_{i-1})/f(G_i) \cong G_{i-1}/G_i$ ist abelsch. Daher ist

$$G' = f(G_0) > f(G_1) > \ldots > f(G_k) = \{e'\} \quad \text{eine Auflösung von } G'.$$

4. Ist G auflösbar, so folgt aus 2. und 3., dass auch N und G/N auflösbar sind.

Seien nun N und G/N auflösbar, sei $N = N_0 > N_1 > \ldots > N_k = \{e\}$ eine Auflösung von N und $G/N = \Gamma_0 > \Gamma_1 > \ldots > \Gamma_m = \{e'\}$ eine Auflösung von G/N. Nach Korollar 2.5.11 gibt es eine Folge von Untergruppen $G = G_0 > G_1 > \ldots > G_m = N$, so dass für alle $j \in [1,m]$ gilt: $\Gamma_j = G_j/N$, wegen $\Gamma_j \lhd \Gamma_{j-1}$ ist auch $G_j \lhd G_{j-1}$, und $\Gamma_{j-1}/\Gamma_j = (G_{j-1}/N)/(G_j/N) \cong G_{j-1}/G_j$ ist abelsch. Daher ist

$$G = G_0 > G_1 > \ldots > G_m = N = N_0 > N_1 > \ldots > N_k = \{e\} \quad \text{eine Auflösung von } G.$$

5. Induktion nach n.

$n = 1$: Dann ist G abelsch und daher auflösbar.

$n \geq 2$, $n-1 \to n$: Sei $|G| = p^n$. Nach Satz 7.4.5 gibt es einen Normalteiler $H \lhd G$ mit $|H| = p^{n-1}$. Dann sind H und G/H auflösbar, und nach 4. ist auch G auflösbar. □

Korollar 7.5.3. *$\mathfrak{S}_3$ und $\mathfrak{S}_4$ sind auflösbar. Für $n \geq 5$ sind $\mathfrak{A}_n$ und $\mathfrak{S}_n$ nicht auflösbar.*

Beweis. $\mathfrak{S}_3 > \mathfrak{A}_3 > \{(1)\}$ ist eine Auflösung von $\mathfrak{S}_3$, und $\mathfrak{S}_4 > \mathfrak{A}_4 > \mathcal{V}_4 > \{(1)\}$ ist eine Auflösung von $\mathfrak{S}_4$.

Sei nun $n \geq 5$. Nach Satz 7.2.10.2 sind $\{(1)\}$ und $\mathfrak{A}_n$ die einzigen Normalteiler von $\mathfrak{A}_n$, und wegen $(1,2,3)(1,2,4) \neq (1,2,4)(1,2,3)$ ist $\mathfrak{A}_n$ nicht abelsch. Daher ist $\mathfrak{A}_n$ nicht auflösbar, und nach Satz 7.5.2.2 ist auch $\mathfrak{S}_n$ nicht auflösbar. □

Satz 7.5.4. *Sei G eine endliche Gruppe.*

1. *Sei G auflösbar. Dann existiert ein $m \in \mathbb{N}_0$ und eine Folge von Untergruppen*
$$G = G_0 > G_1 > \ldots > G_m = \{e\},$$
so dass für alle $i \in [1,m]$ gilt: $G_i \lhd G_{i-1}$ und $(G_{i-1}:G_i) \in \mathbb{P}$.
2. *Sei $U < G$, $m \in \mathbb{N}$ und $G = G_0 > G_1 > \ldots > G_m = U$ eine Folge von Untergruppen, so dass für alle $i \in [1,m]$ gilt: $G_i \lhd G_{i-1}$, und G_{i-1}/G_i ist abelsch. Ist dann*
$$\bigcap_{\sigma \in G} \sigma U \sigma^{-1} = \{e\},$$
so ist G auflösbar, und jeder Primteiler von $|G|$ teilt $(G:U)$.

Beweis. 1. Induktion nach $|G|$. Im Falle $|G| = 1$ ist nichts zu zeigen. Sei also $|G| > 1$ und gelte die Behauptung für alle Gruppen G' mit $|G'| < |G|$. Da G auflösbar ist, gibt es einen Normalteiler $N \lhd G$, so dass $|N| < |G|$ und G/N abelsch ist. Sei $p \in \mathbb{P}$ mit $p \mid |G/N|$. Nach Satz 4.2.3 gibt es ein $g \in G/N$ und eine Untergruppe $\Gamma < G/N$, so dass $\mathrm{ord}(g) = p$ und $G/N = \Gamma\langle g\rangle$ (dir), also insbesondere $(G/N:\Gamma) = p$. Nach Korollar 2.5.11 gibt es einen Normalteiler $G_1 \lhd G$ mit $N \subset G_1$ und $G_1/N = \Gamma$, und es ist $G/G_1 \cong (G/N)/(G_1/N) = (G/N)/\Gamma$, also $(G:G_1) = p$. Nach Satz 7.5.2.2 ist G_1 auflösbar, und nach Induktionsvoraussetzung gibt es eine Folge von Untergruppen $G_1 > \ldots > G_m = \{e\}$, so dass für alle $i \in [2,m]$ gilt: $G_i \lhd G_{i-1}$ und $(G_{i-1}:G_i) \in \mathbb{P}$.

2. Induktion nach $|U|$. Im Falle $|U| = 1$ ist nichts zu zeigen. Sei also $|U| > 1$ und die Behauptung für alle Untergruppen $U' < G$ mit $|U'| < |U|$ gezeigt. Nach Voraussetzung gibt es ein $\tau \in G$, so dass $U_1 = U \cap \tau U \tau^{-1} \subsetneq U$, und es sei $\kappa = \kappa_\tau \colon G \to G$ die Konjugation mit τ, definiert durch $\kappa(x) = \tau x \tau^{-1}$. Dann ist auch
$$\bigcap_{\sigma \in G} \sigma U_1 \sigma^{-1} = \{e\},$$
und wir erhalten die Untergruppenfolge
$$G = \kappa(G_0) > \kappa(G_1) > \cdots > \kappa(G_m) = U = G_0 \cap U > G_1 \cap U > \cdots > G_m \cap U = U_1.$$
Für alle $j \in [1,m]$ ist $\kappa(G_j) \lhd \kappa(G_{j-1})$, und $\kappa(G_{j-1})/\kappa(G_j) \cong G_{j-1}/G_j$ ist abelsch. Nach Satz 2.5.8 gilt für alle $j \in [1,m]$: $G_j \cap U = G_j \cap (G_{j-1} \cap U) \lhd G_{j-1} \cap U$,
$$G_{j-1} \cap U / G_j \cap U = G_{j-1} \cap U / G_j \cap (G_{j-1} \cap U) \cong (G_{j-1} \cap U) G_j / G_j < G_{j-1}/G_j,$$

und da G_{j-1}/G_j abelsch ist, ist auch $G_{j-1} \cap U/G_j \cap U$ abelsch. Nach Induktionsvoraussetzung is G auflösbar, und jeder Primteiler p von G teilt $(G:U_1) = (G:U)(U:U_1)$. Ist $p \,|\, (U:U_1)$, so teilt p auch $(G_{j-1} \cap U : G_j \cap U)$ und daher $(G_{j-1}:G_j)$ für ein $j \in [1,m]$, und es folgt $p \,|\, (G:U)$. □

CHAPTER 8

Galoistheorie

Wir erinnern an einige Begriffe und Tatsachen aus Kapitel 6, die wir nun häufig beötigen.

Sei L/K eine Körpererweiterung.

L/K heißt *galoissch*, wenn L/K normal und separabel ist (Definition 6.6.5). Ist L/K galoissch und $K \subset M \subset L$ ein Zwischenkörper, so ist auch L/M galoissch (Satz 6.6.9.4).

Für einen Oberkörper $L' \supset K$ bezeichnet $\mathrm{Hom}_K(L, L')$ die Menge der K-Homomorphismen $\varphi\colon L \to L'$. Ist L/K endlich, so ist $|\mathrm{Hom}_K(L, L')| \leq [L\colon K]$, mit Gleichheit, falls L/K separabel und L'/K normal ist (Korollar 6.6.8).

Es sei $\mathrm{Gal}(L/K) \subset \mathfrak{S}(L)$ die Menge aller K-Isomorphismen $\varphi\colon L \to L$. $\mathrm{Gal}(L/K$ heißt *Galoisgruppe* von L/K. Ist L/K algebraisch, so ist $\mathrm{Gal}(L/K) = \mathrm{Hom}_K(L, L)$ (Satz 6.4.1). Ist L/K endlich, so ist $|\mathrm{Gal}(L/K)| \leq [L\colon K]$, mit Gleichheit genau dann, wenn L/K galoissch ist (Korollar 6.6.8.3).

8.1. Hauptsatz der Galoistheorie

Definitionen und Bemerkungen 8.1.1.

1. Für einen Körper L bezeichne $\mathrm{Aut}(L) = \{\varphi\colon L \to L \mid \varphi \text{ ist ein Isomorphismus}\}$ die Menge der Automorphismen von L.

   Ist L/K eine Körpererweiterung und $K_0 \subset K$ der Primkörper von K, so folgt

   $$\mathrm{Gal}(L/K) < \mathrm{Aut}(L) = \mathrm{Gal}(L/K_0) < \mathfrak{S}(L)\,.$$

   [Beweis: Nach Definition sind $\mathrm{Gal}(K/K_0) \subset \mathrm{Aut}(K) \subset \mathfrak{S}(L)$ Untergruppen. Ist $\varphi \in \mathrm{Aut}(L)$, so folgt $\varphi(m1_K) = m\varphi(1_K) = m1_K$ für alle $m \in \mathbb{Z}$. Ist $R_0 = \{m1_K \mid m \in \mathbb{Z}\}$ der Primring von K, so ist K_0 ein Quotientenkörper von R_0 und daher $\varphi \,|\, K_0 = \mathrm{id}_{K_0}$, also $\varphi \in \mathrm{Gal}(K/K_0)$].

2. Für eine Untergruppe $H < \mathrm{Aut}(L)$ heißt

   $$L^H = \{\alpha \in L \mid \sigma(\alpha) = \alpha \text{ für alle } \sigma \in H\} \quad \text{der } \textit{Fixkörper} \text{ von } H.$$

   Offensichtlich ist L^H ein Teilkörper von L und $L^H < \mathrm{Gal}(L/L^H)$.

   Ist L/K eine Körpererweiterung und $K \subset M \subset L$ ein Zwischenkörper, so folgt

   $$\mathrm{Gal}(L/M) < \mathrm{Gal}(L/K) \quad \text{und} \quad L^{\mathrm{Gal}(L/M)} \supset M\,.$$

3. Zwei Zwischenkörper M, M' von L/K heißen *konjugiert* über K, wenn ein $\sigma \in \mathrm{Gal}(L/K)$ existiert mit $\sigma(M) = M'$.

   Ist $G = \mathrm{Gal}(L/K)$, $K \subset L \subset M$ ein Zwischenkörper, $H = \mathrm{Gal}(L/M)$ und $\sigma \in G$, so folgt

   $\mathrm{Gal}(L/\sigma M) = \sigma H \sigma^{-1}$ (konjugierte Zwischenkörper gehören zu konjugierten Untergruppen).

   [Beweis: Für $\tau \in G$ gilt: $\tau \in \mathrm{Gal}(L/\sigma M) \iff \tau|\sigma M = \mathrm{id}_{\sigma M} \iff \tau\sigma x = \sigma x$ für alle $x \in M$ $\iff \sigma^{-1}\tau\sigma x = x$ für alle $x \in M \iff \sigma^{-1}\tau\sigma \in H \iff \tau \in \sigma H \sigma^{-1}$].

Satz 8.1.2 (Lineare Unabhängigkeit von Charakteren)**.** *Sei H ein (multiplikatives) Monoid, K ein Körper, und seien $\sigma_1, \ldots, \sigma_n \colon H \to K^\times$ paarweise verschiedene Monoidhomomorphismen. Dann sind $\sigma_1, \ldots, \sigma_n$ K-linear unabhängige Elemente des K-Vektorraumes $\mathrm{Abb}(H, K)$.*

Beweis. Induktion nach n.
$n = 1$: $\sigma_1 \neq 0$ ist linear unabhängig.
$n \geq 2$, $n-1 \to n$: Seien $\lambda_1, \ldots, \lambda_n \in K$ mit

$$\sum_{i=1}^{n} \lambda_i \sigma_i = 0 \colon H \to K^\times, \quad \text{also} \quad \sum_{i=1}^{n} \lambda_i \sigma_i(x) = 0 \quad \text{für alle } x \in H.$$

Sei $y \in H$ mit $\sigma_1(y) \neq \sigma_n(y)$. Dann folgt für alle $x \in H$

$$0 = \sum_{i=1}^{n} \lambda_i \sigma_i(xy) = \sum_{i=1}^{n} \lambda_i \sigma_i(x)\sigma_i(y) \quad \text{und} \quad 0 = \sum_{i=1}^{n} \lambda_i \sigma_i(x)\sigma_n(y),$$

also auch

$$0 = \sum_{i=1}^{n-1} \lambda_i \left[\, \sigma_i(y) - \sigma_n(y) \,\right] \sigma_i(x), \quad \text{und daher} \quad 0 = \sum_{i=1}^{n-1} \lambda_i \left[\, \sigma_i(y) - \sigma_n(y) \,\right] \sigma_i.$$

Nach Induktionsvoraussetzung folgt $\lambda_i \left[\, \sigma_i(y) - \sigma_n(y) \,\right] = 0$ für alle $i \in [1, n-1]$. Also ist $\lambda_1 = 0$ und daher $\lambda_2\sigma_2 + \ldots + \lambda_n\sigma_n = 0$. Nach Induktionsvoraussetzung folgt nund auch $\lambda_2 = \ldots = \lambda_n = 0$. □

Satz 8.1.3 (Satz von Artin)**.** *Sei L ein Körper und $G < \mathrm{Aut}(L)$ eine endliche Untergruppe. Dann ist L/L^G eine endliche galoissche Körpererweiterung, es ist $[L\colon L^G] = |G|$ und $\mathrm{Gal}(L/L^G) = G$.*

Beweis. Sei $K = L^G$, $|G| = n$ und $G = \{\sigma_1, \ldots, \sigma_n\}$.
Es genügt, $[L : K] \leq n$ zu zeigen. Denn nach Definition ist $G \subset \mathrm{Gal}(L/K)$, und nach Korollar 6.6.8.3 folgt dann $n = |G| \leq |\mathrm{Gal}(L/L)| \leq [L\colon K] \leq n$, also $\mathrm{Gal}(L/K) = G$ und $[L\colon K] = n$.
Die Abbildung $S = \sigma_1 + \ldots + \sigma_n \colon L \to L$ ist K-linear (da $\sigma_1, \ldots, \sigma_n$ das sind). Nach Satz 8.1.2 ist $S \neq 0$, und für alle $x \in L$ und $\tau \in G$ ist $\tau S(x) = \tau\sigma_1(x) + \ldots + \tau\sigma_n = S(x)$, also $S(x) \in L^G = K$, da $\{\tau\sigma_1, \ldots, \tau\sigma_n\} = \{\sigma_1, \ldots, \sigma_n\}$. Damit folgt $S(L) = K$. Wir zeigen nun, dass je $n+1$ Elemente von L über K linear abhängig sind.
Seien $y_1, \ldots, y_{n+1} \in L$. Da jedes homogene Gleichungssystem aus $n+1$ Gleichungen in n Unbekannten eine nicht-triviale Lösung besitzt, gibt es $(a_1, \ldots, a_{n+1}) \in L^{n+1}$, so dass $(a_1, \ldots, a_{n+1}) \neq (0, \ldots, 0)$ und

$$\sum_{\nu=1}^{n+1} \sigma_i^{-1}(y_\nu)\, a_\nu = 0 \quad \text{für alle } i \in [1, n].$$

Es sei (nach eventueller Umnummerierung von $\sigma_1, \ldots, \sigma_n$) $a_1 \neq 0$. Wegen $S(a_1 L) = S(L) = K$ existiert ein $z \in L$ mit $S(a_1 z) \neq 0$. Somit erhalten wir

$$0 = \sum_{i=1}^{n} \sigma_i \Big(\sum_{\nu=1}^{n+1} \sigma_i^{-1}(y_\nu) a_\nu z \Big) = \sum_{\nu=1}^{n+1} \sum_{i=1}^{n} \sigma_i(a_\nu z) y_\nu = \sum_{\nu=1}^{n+1} S(a_\nu z) y_\nu,$$

also die lineare Abhängigkeit von $y_1, \ldots, y_{n+1}$. □

Korollar 8.1.4. *Sei L/K eine endliche Körpererweiterung und $G = \mathrm{Gal}(L/K)$.Dann sind die folgenden Aussagen äquivalent*:

(a) *L/K ist galoissch;* (b) $[L\colon K] = |G|$; (c) $K = L^G$.

Beweis. Die Äquivalenz von (a) und (b) folgt nach Korollar 6.6.8.3. Wegen $K \subset L^G \subset L$ ist (mit Satz 8.1.3) $[L\colon K] = [L\colon L^G]\,[L^G\colon K] = |G|\,[L^G\colon K]$, und es folgt die Äquivalenz von (b) und (c). □

Satz 8.1.5 (Hauptsatz der Galoistheorie)**.** *Sei L/K eine endliche galoissche Körpererweiterung, $G = \mathrm{Gal}(L/K)$, $\mathcal{Z}(L/K)$ die Menge der Zwischenkörper von L/K und $\mathcal{U}(G)$ die Menge der Untergruppen von G. Dann sind die Abbildungen*

$$\begin{cases} \mathcal{Z}(L/K) & \to & \mathcal{U}(G) \\ M & \mapsto & \mathrm{Gal}(L/M) \end{cases} \quad \textit{und} \quad \begin{cases} \mathcal{U}(G) & \to & \mathcal{Z}(L/K) \\ H & \mapsto & L^H \end{cases}$$

zueinander inverse, inklusionsumkehrende Bijektionen.
Insbesondere gilt für alle Zwischenkörper M, M' von L/K mit $H = \mathrm{Gal}(L/M)$ und $H' = \mathrm{Gal}(L/M')$:

1. $M \subset M' \iff H \supset H'$.
2. $MM' = L^{H\cap H'}$ *und* $H \cap H' = \mathrm{Gal}(L/MM')$.
3. $M \cap M' = L^{\langle H,H'\rangle}$ *und* $\langle H, H'\rangle = \mathrm{Gal}(L/M \cap M')$.

Beweis. Ist $M \in \mathcal{Z}(L/K)$ und $H = \mathrm{Gal}(L/M)$, so ist L/M galoissch nach Satz 6.6.9.4, und $M = L^H$ nach Korollar 8.1.4. Ist $H < G$ eine Untergruppe und $M = L^H$, so folgt $\mathrm{Gal}(L/L^H) = H$ nach Satz 8.1.3. Daher sind die angegebenen Abbildungen zueinander inverse Bijektionen, und offensichtlich sind sie inklusionsumkehrend. Damit folgen dann auch 1., 2. und 3., denn MM' ist der kleinste M und M' umfassende und $M \cap M'$ ist der größte in M und M' enthaltene Zwischenkörper von L/K. Anderseits ist $H \cap H'$ die größte in H und H' enthaltene und $\langle H, H'\rangle$ ist die kleinste H und H' umfassende Untergruppe von G. □

Korollar 8.1.6. *Sei L/K eine endliche galoissche Körpererweiterung, $G = \mathrm{Gal}(L/K)$, M ein Zwischenkörper von L/K und $H = \mathrm{Gal}(L/M) < G$.*

1. $[M\!:\!K] = (G\!:\!H)$*, und die Abbildung*

$$\rho\colon \mathsf{N}_G(H) \to \mathrm{Gal}(M/K), \quad \textit{definiert durch} \quad \rho(\sigma) = \sigma\,|\,M \quad \textit{für alle} \quad \sigma \in G,$$

   ist ein Gruppenepimorphismus mit $\mathrm{Ker}(\rho) = H$.
2. *Genau dann ist M/K galoissch, wenn $H \lhd G$, und dann ist*

$$G/H \to \mathrm{Gal}(M/K), \quad \sigma H \mapsto \sigma\,|\,M \quad \textit{ein Isomorphismus}.$$

Beweis. 1. Nach Korollar 8.1.4 ist $[L\!:\!K] = |G|$ und $[L\!:\!M] = |H|$, und daher folgt

$$[M\!:\!K] = \frac{[L\!:\!K]}{[L\!:\!M]} = \frac{|G|}{|H|} = (G\!:\!H).$$

Nach Satz 8.1.5 ist genau dann $\sigma M = M$, wenn $H = \mathrm{Gal}(L/\sigma M)$, und nach Bemerkung 8.1.1.3 ist $\mathrm{Gal}(L/\sigma M) = \sigma H \sigma^{-1}$. Daher ist genau dann $\sigma M = M$ wenn $\sigma \in \mathsf{N}_G(H)$.

Für $\sigma \in \mathsf{N}_G(H)$ ist also $\sigma\,|\,M \in \mathrm{Gal}(M/K)$, und daher ist ρ ein Gruppenhomomorphismus mit $\mathrm{Ker}(\rho) = H$. Sei $\varphi\colon M \to M \hookrightarrow L$. Ist $\varphi \in \mathrm{Gal}(M/K)$, so gibt es nach Satz 6.6.7 einen Körpermonomorphismus $\sigma\colon L \to L$ mit $\sigma\,|\,M = \varphi$, und nach Satz 6.4.1.3 ist $\sigma \in \mathrm{Gal}(L/K)$. Daher ist ρ surjektiv.

2. Nach 1. ist $[M : K] = (G : H)$, und der Epimorphismus ρ induziert einen Isomorphismus $\rho^*\colon \mathsf{N}_G(H)/H \xrightarrow{\sim} \mathrm{Gal}(M/K)$, gegeben durch $\rho^*(\sigma H) = \sigma\,|\,M$. Daher gilt:

$$\begin{aligned} M/K \text{ ist galoissch} &\iff [M\!:\!K] = |\mathrm{Gal}(M/K)| \iff (G\!:\!H) = (\mathsf{N}_G(H)\!:\!H) \\ &\iff G = \mathsf{N}_G(H) \iff H \lhd G. \end{aligned}$$

□

Korollar 8.1.7. *Sei L/K eine endliche separable Körpererweiterung.*

1. *L/K besitzt nur endlich viele Zwischenkörper.*

2. *Sei $N \supset L$ ein Oberkörper, N/K endlich galoissch, $G = \mathrm{Gal}(N/K)$, $H = \mathrm{Gal}(N/L)$,*

$$H' = \bigcap_{\sigma\in G} \sigma H \sigma^{-1} \quad \textit{und} \quad N' = \prod_{\sigma\in G} \sigma(L) \subset N\,.$$

Dann ist N' eine galoissche Hülle von L/K.

Beweis. 1. Nach Satz 8.1.5 besitzt N/K (also erst recht L/K) nur endlich viele Zwischenkörper.

2. Nach Satz 8.1.5 ist

$$\mathrm{Gal}(N/N') = \bigcap_{\sigma\in G} \mathrm{Gal}(N/\sigma L) = \bigcap_{\sigma\in G} \sigma H \sigma^{-1} = H' \lhd G$$

und daher N'/K galoissch nach Korollar 8.1.6.2. Ist $L \subset M \subset N'$ ein Zwischenkörper und M/K galoissch, so ist $\mathrm{Gal}(N/M) \lhd G$ und $H' \subset \mathrm{Gal}(N/M) \subset H$, also

$$\mathrm{Gal}(N/M) = \bigcap_{\sigma\in G} \sigma \mathrm{Gal}(N/M)\sigma^{-1} \subset \bigcap_{\sigma\in G} \sigma H \sigma^{-1} = H' \quad \text{und daher} \quad M = N'.$$

□

Korollar 8.1.8 (Verschiebungssatz der Galoistheorie)**.** *Sei L/K eine endliche Körpererweiterung, und seien M, M' Zwischenkörper von L/K.*

1. *Ist M/K galoissch, so ist auch MM'/M' galoissch, und die Abbildung*

$$\rho\,:\ \mathrm{Gal}(MM'/M') \to \mathrm{Gal}(M/M\cap M')\,, \quad \textit{definiert durch} \quad \rho(\sigma) = \sigma\,|\,M\,,$$

ist ein Gruppenisomorphismus.

2. *Sind M/K und M'/K galoissch, so ist auch MM'/K galoisch, und die Abbildung*

$$\pi\,:\ \mathrm{Gal}(MM'/K) \to \mathrm{Gal}(M/K)\times\mathrm{Gal}(M'/K)\,, \quad \textit{definiert durch} \quad \pi(\sigma) = (\sigma\,|\,M, \sigma\,|\,M')\,,$$

ist ein Gruppenmonomorphismus. Ist $K = M\cap M'$, so ist π ein Isomorphismus.

Beweis. 1. Nach Satz 6.6.11 ist M Zerfällungskörper eines separablen Polynoms $f \in K[X]$. Dann ist MM' Zerfällungskörper von f über M', also MM'/M' galoissch, und offensichlich ist ρ ein Gruppenhomomorphismus. Ist $\sigma \in \mathrm{Ker}(\rho)$, so ist $\sigma\,|\,M' = \mathrm{id}_{M'}$ und $\sigma\,|\,M = \mathrm{id}_M$, also wegen $MM' = M'(M)$ bereits $\sigma = \mathrm{id}_{MM'}$. Daher ist ρ injektiv.

Für den Nachweis der Surjektivität von ρ sei $H = \rho(\mathrm{Gal}(MM'/M')) < \mathrm{Gal}(M/M\cap M')$. Dann ist

$$M^H = M \cap (MM')^{\mathrm{Gal}(MM'/M')} = M\cap M'\,, \quad \text{also} \quad H = \mathrm{Gal}(M/M\cap M') \quad \text{nach Satz 8.1.5.}$$

2. Seien f, $g \in K[X]$, so dass M ein Zerfällungskörper von f über K und M' ein Zerfällungskörper von g über K ist. Dann ist MM' ein Zerfällungskörper von fg über K, und daher ist MM'/K normal. Nach 1. ist MM'/M separabel, und dan M/K separabel ist, ist nach Satz 6.6.9.3 auch MM'/K separabel, also galoissch. Offensichtlich ist π ein Gruppenhomomorphismus. Ist $\sigma \in \mathrm{Ker}(\pi)$, so ist $\sigma\,|\,M = \mathrm{id}_M$ und $\sigma\,|\,M' = \mathrm{id}_{M'}$, also $\sigma = \mathrm{id}_{MM'}$ und somit σ injektiv.

Sei nun $K = M\cap M'$ und $(\tau,\tau') \in \mathrm{Gal}(M/K)\times\mathrm{Gal}(M'/K)$. Nach 1. sind die Abbildungen

$$\rho\colon \begin{cases} \mathrm{Gal}(MM'/M') & \xrightarrow{\sim} & \mathrm{Gal}(M/K) \\ \sigma & \mapsto & \sigma\,|\,M \end{cases} \quad \text{und} \quad \rho'\colon \begin{cases} \mathrm{Gal}(MM'/M) & \xrightarrow{\sim} & \mathrm{Gal}(M'/K) \\ \sigma & \mapsto & \sigma\,|\,M' \end{cases}$$

Isomorphismen. Daher existieren $\tau_1 \in \mathrm{Gal}(MM'/M')$ mit $\tau_1|M = \tau$ und $\tau_2 \in \mathrm{Gal}(MM'/M)$ mit $\tau_2|M' = \tau'$. Damit folgt $\pi(\tau_1,\tau_2) = (\tau,\tau')$. □

8.2. Fundamentalsatz der Algebra

Satz 8.2.1. *Sei R ein Körper mit $\mathrm{char}(R) = 0$ und C/R eine endliche Körpererweiterung mit folgenden Eigenschaften:*

- *Jedes normierte Polynom ungeraden Grades $f \in R[X]$ hat eine Nullstelle in R.*
- *Zu jedem $\alpha \in C$ existiert ein $\beta \in C$ mit $\beta^2 = \alpha$.*

Dann ist C algebraisch abgeschlossen.

Beweis. Nach Satz 6.4.12 ist zu zeigen: Ist K/C eine endliche Körpererweiterung, so ist $K = C$. Sei K/C eine endliche Körpererweiterung. Nach Satz 6.6.3 und Bemerkung 6.6.6 ist K/R separabel, und es sei N eine galoissche Hülle von K/R (siehe Satz 6.6.12). Sei $G = \mathrm{Gal}(N/R)$, $H \in \mathrm{Syl}_2(G)$ und $M = N^H$. Nach Satz 7.4.6.1 und Korollar 8.1.6.1 ist $2 \nmid (G:H) = [M:R]$. Ist $\alpha \in M$ und $f \in R[X]$ das Minimalpolynom von α über R, so ist $\mathrm{gr}(f) = \mathrm{gr}_R(\alpha) = [R(\alpha):R] \mid [M:R]$, also $\mathrm{gr}(f)$ ungerade, und daher besitzt f eine Nullstelle in R. Da f über R irreduzibel ist, folgt $\mathrm{gr}(f) = 1$ und daher $\alpha \in R$.

Es ist also $M = R$, $G = H$ und daher $|G| = 2^m$ mit $m \in \mathbb{N}$. Sei $U = \mathrm{Gal}(N|C) < G$ und $|U| = 2^c$. Ist $c = 0$, so folgt $N = C$ und daher $K = C$. Sei also $c \geq 1$. Nach Satz 7.4.5 gibt es eine Untergruppe $V < U$ mit $|V| = 2^{c-1}$, und es ist $[N^V : C] = 2$. Nach Beispiel 6.3.4.4 ist $N^V = C(\beta)$ mit $\beta^2 = \alpha \in C$. Nach Voraussetzung existiert ein $\beta' \in C$ mit $\beta'^2 = \alpha$, es ist dann $\beta = \pm\beta' \in C$ und daher $N^V = C$, ein Widerspruch. □

Korollar 8.2.2. *$\mathbb{C}$ und $\overline{\mathbb{Q}}$ sind algebraisch abgeschlossene Körper.*

Beweis. Nach Satz 6.4.12.2 genügt es, zu zeigen, dass $\mathbb{C}$ algebraisch abgeschlossen ist, und dazu zeigen wir, dass die Körpererweiterung $\mathbb{C}/\mathbb{R}$ die Bedingungen von Satz 8.2.1 erfüllt.

Ist $f \in \mathbb{R}[X]$ normiert und $\mathrm{gr}(f)$ ungerade, so hat f nach dem Zwischenwertsatz für stetige Funktionen eine Nullstelle in $\mathbb{R}$.

Ist $\alpha = a + \mathrm{i}b \in \mathbb{C}$ mit $a, b \in \mathbb{R}$, so folgt

$$\alpha = \beta^2 \quad \text{mit} \quad \beta = \frac{1}{\sqrt{2}}\Big(\sqrt{\sqrt{a^2+b^2}+a} \; + i\varepsilon\sqrt{\sqrt{a^2+b^2}-a}\Big), \quad \text{wobei} \quad \varepsilon = \begin{cases} 1\,, & \text{falls} \quad b \geq 0\,, \\ -1\,, & \text{falls} \quad b < 0\,. \end{cases}$$

□

8.3. Einheitswurzelkörper

Wir erinnern an einige Eigenschaften der Euler'sche Phi-Funktion (Satz 4.3.3). Für $n \in \mathbb{N}$ ist

$$(\mathbb{Z}/n\mathbb{Z})^\times = \{a + n\mathbb{Z} \mid a \in [0, n-1],\ \mathrm{ggT}(a,n) = 1\} \quad \text{und} \quad \varphi(n) = |(\mathbb{Z}/n\mathbb{Z})^\times|\,.$$

Für $p \in \mathbb{P}$ und $k \in \mathbb{N}$ ist $\varphi(p^k) = p^{k-1}(p-1)$.

Definition 8.3.1. Sei K ein Körper und $n \in \mathbb{N}$. Ein Element $\zeta \in K$ heißt *n-te Einheitswurzel*, wenn $\zeta^n = 1$. Eine n-te Einheitswurzel $\zeta \in K$ heißt *primitiv*, wenn $\mathrm{ord}_{K^\times}(\zeta) = n$. Es bezeichne $\mu_n(K) \subset K^\times$ die Gruppe der n-ten Einheitswurzeln in K und $\mu_n^*(K) \subset \mu_n(K)$ die Menge der primitiven n-ten Einheitswurzeln in K.

Lemma 8.3.2. *Sei K ein Körper und $n \in \mathbb{N}$.*

1. *$\mu_n(K)$ ist eine zyklische Untergruppe von $K^\times$, und $|\mu_n(K)| \;\big|\; n$.*
2. *Das Polynom $X^n - 1 \in K[X]$ ist genau dann separabel, wenn $\mathrm{char}(K) \nmid n$.*
3. *Die folgenden Aussagen sind äquivalent:*
   (a) $|\mu_n(K)| = n$.

(b) $\mu_n^*(K) \neq \emptyset$.
(c) $|\mu_n^*(K)| = \varphi(n)$.
(d) $X^n - 1$ *zerfällt über* K *in Linearfaktoren, und* $\operatorname{char}(K) \nmid n$.
Sind diese Bedingungen erfüllt, so folgt $\mu_n(K) = \langle\zeta\rangle$ *für alle* $\zeta \in \mu_n^*(K)$.

BEWEIS. 1. $\mu_n(K)$ ist die Menge der Nullstellen von $X^n - 1$ in K, also endlich. Daher ist $\mu_n(K)$ eine endliche Untergruppe von $K^\times$, also zyklisch nach Satz 4.2.5. Ist $\mu_n(K) = \langle\zeta\rangle$, so ist $\zeta^n = 1$ und daher $|\mu_n(K)| = \operatorname{ord}(\zeta) \mid n$.

2. Sei $f = X^n - 1$. Dann ist $f' = nX^{n-1}$. Ist $\operatorname{char}(K) \mid n$, so folgt $f' = 0$. Ist $\operatorname{char}(K) \nmid n$, so sind f und f' teilerfremd in $K[X]$. Daher ist nach Satz 6.6.2 f genau dann separabel, wenn $\operatorname{char}(K) \nmid n$.

3. (a) $\Leftrightarrow$ (b) $\Leftrightarrow$ (c) Nach 1. ist $\mu_n(K) = \langle\zeta\rangle$, und genau dann ist $|\mu_n(K)| = n$, wenn $\operatorname{ord}(\zeta) = n$, also wenn $\zeta \in \mu_n^*(K)$. Ist $\operatorname{ord}(\zeta) = n$, so folgt $\mu_n^*(K) = \{\zeta^k \mid k \in [1,n]\,,\ \operatorname{ggT}(k,n) = 1\}$ nach Satz 2.2.10, also $|\mu_n^*(K)| = \varphi(n)$.
(a) $\Leftrightarrow$ (d) Nach 1. und 2. □

Definition 8.3.3. Sei K ein Körper, $n \in \mathbb{N}$, $\operatorname{char}(K) \nmid n$ und L ein Zerfällungskörper von $X^n - 1$ über K. Dann heißt

$$\Phi_n^K = \Phi_n = \prod_{\zeta \in \mu_n^*(L)} (X - \zeta) \in L[X]$$

das *n-te Kreisteilungspolynom* über K und L ein *n-ter Kreis(teilungs)körper* oder *Einheitswurzelkörper* über K.

Bemerkungen 8.3.4.

1. Sei $n \in \mathbb{N}$. Dann ist $\mathbb{Q}(\mathsf{e}^{2\pi\mathrm{i}/n})$ ein n-ter Kreisteilungskörper über $\mathbb{Q}$.

2. Sei $\operatorname{char}(K) = p \in \mathbb{P}$ und $n = p^k m$ mit $k \in \mathbb{N}$ und $p \nmid m$. Dann ist $\mu_n(K) = \mu_m(K)$ [Beweis: Nach Definition ist $\mu_m(K) \subset \mu_n(K)$. Ist $\zeta \in \mu_n(K)$, so folgt $0 = \zeta^n - 1 = (\zeta^m)^{p^k} - 1 = (\zeta^m - 1)^{p^k}$, also $\zeta^m = 1$ und daher $\zeta \in \mu_m(K)$.]

3. Die folgende Beobachtung geht auf E. Kummer (1810 – 1893) zurück. Sei $p \in \mathbb{P}$ ungerade und $K = \mathbb{Q}(\zeta)$ mit $\zeta = \mathsf{e}^{2\pi\mathrm{i}/p}$. Dann ist

$$X^p - 1 = \prod_{i=0}^{p-1} (X - \zeta^i) \in K[X]\,,$$

und der Einsetzungshomomorphismus $X \mapsto\!= -\frac{x}{y}$ mit $x, y \in \mathbb{Q}^\times$ liefert die Identität

$$(-x)^p - y^p = \prod_{i=0}^{p-1} (-x - y^{\zeta^i})\,, \quad \text{also} \quad x^p + y^p = \prod_{i=0}^{p-1} (x + \zeta^i y)\,.$$

Damit kann man zeigen: Ist der Bereich $\mathbb{Z}[\zeta]$ faktoriell (was allerdings für unendlich viele Primzahlen nicht der Fall ist), so hat die Gleichung $x^p + y^p = z^p$ keine Lösung $(x, y, z) \in \mathbb{N}^3$.

Satz 8.3.5. *Sei* K *ein Körper,* $n \in \mathbb{N}$, $\operatorname{char}(K) \nmid n$, L *ein Zerfällungskörper von* $X^n - 1$ *über* K, $\Phi_n \in L[X]$ *das n-te Kreisteilungspolynom über* K *und* F *der Primring von* K.

1. *Es ist* $\Phi_n^K \in F[X]$, *das Polynom* Φ_n^K *ist normiert und separabel,* $\operatorname{gr}(\Phi_n^K) = \varphi(n)$, *und*

$$X^n - 1 = \prod_{1 \leq d \mid n} \Phi_d^K\,.$$

Ist $f\colon \mathbb{Z} \to F$ *der Ringhomomorphismus gemäß* 6.1.1 *und* $f_1\colon \mathbb{Z}[X] \to F[X]$ *seine Fortsetzung auf die Polynomringe, so ist* $f_1(\Phi_n^{\mathbb{Q}}) = \Phi_n^K$.

2. $\Phi_n^{\mathbb{Q}} \in \mathbb{Z}[X]$ *ist irreduzibel über* $\mathbb{Q}$.

BEWEIS. 1. Nach Definition ist Φ_n^K normiert, $\operatorname{gr}(\Phi_n^K) = \varphi(n)$, und wegen $\Phi_n^K \mid X^n - 1$ ist Φ_n^K separabel nach Lemma 8.3.2.2. Nach Lemma 8.3.2.3 ist $|\mu_n(L)| = n$, und wegen

$$\mu_n(L) = \biguplus_{1 \le d \mid n} \mu_d^*(L) \qquad \text{folgt} \qquad X^n - 1 = \prod_{\zeta \in \mu_n(L)} (X - \zeta) = \prod_{1 \le d \mid n} \prod_{\zeta \in \mu_d^*(L)} (X - \zeta) = \prod_{1 \le d \mid n} \Phi_d^K \,.$$

Im Falle $K = \mathbb{Q}$ folgt daraus bereits $\Phi_n^{\mathbb{Q}} \in \mathbb{Z}[X]$ nach dem Gauß'schen Lemma (Satz 5.3.9).

2. Sei $\Phi_n = \Phi_n^{\mathbb{Q}}$, $\zeta \in \mu_n^*(K)$ und $f \in \mathbb{Q}[X]$ das Minimalpolynom von ζ über $\mathbb{Q}$. Dann ist $f \mid \Phi_n \mid X^n - 1$, und wir zeigen:

A. Für alle $k \in \mathbb{N}$ mit $\operatorname{ggT}(k, n) = 1$ ist $f(\zeta^k) = 0$.

Dann ist $\varphi(n) \le \operatorname{gr}(f) \le \operatorname{gr}(\Phi_n) = \varphi(n)$, also $\Phi_n = f$ irreduzibel über $\mathbb{Q}$.

Wir beweisen **A** durch Widerspruch und nehmen an, es sei $k \in \mathbb{N}$ minimal mit $\operatorname{ggT}(k, n) = 1$ und $f(\zeta^k) \ne 0$. Sei $p \in \mathbb{P}$ mit $p \mid k$ und $\xi = \zeta^{k/p}$. Dann ist $\operatorname{ggT}(\frac{k}{p}, n) = 1$, also $\xi \in \mu_n^*(K)$, $f(\xi) = 0$ und $f(\xi^p) \ne 0$. Ist $X^n - 1 = fg$ mit $g \in \mathbb{Q}[X]$, so ist g normiert, und mit dem Gauß'schen Lemma folgt $g \in \mathbb{Z}[X]$. Wegen $g(\xi^p) = 0$ ist ξ Nullstelle des Polyoms $g(X^p)$. Da f das Minimalpolynom von ξ ist, folgt $g(X^p) = f(X)h(X)$ mit $h \in \mathbb{Q}[X]$, also (wieder nach dem Gauß'schen Lemma) $h \in \mathbb{Z}[X]$. Sei

$$\overline{\ }\colon \mathbb{Z}[X] \to \mathbb{Z}/p\mathbb{Z}[X] = \mathbb{F}_p[X]\,, \quad f \mapsto \overline{f}\,,$$

die Fortsetzung des Restklassenhomomorphismus auf die Polynomringe. Dann ist $\overline{g}(X^p) = \overline{f}\,\overline{h}$, und

$$\text{aus} \quad g = \sum_{\nu \ge 0} b_\nu X^\nu \quad \text{folgt} \quad \overline{g}(X^p) = \sum_{\nu \ge 0} \overline{b}_\nu X^{\nu p} = \sum_{\nu \ge 0} \overline{b}_\nu^p X^{\nu p} = \Big(\sum_{\nu \ge 0} \overline{b}_\nu X^\nu\Big)^p = \overline{g}^p\,, \quad \text{also} \quad \overline{g}^p = \overline{f}\,\overline{h}\,.$$

Sei nun $E \supset \mathbb{F}_p$ ein Oberkörper und $\beta \in E$ mit $\overline{f}(\beta) = 0$. Dann folgt $\overline{g}(\beta) = 0$, und daher ist β mehrfache Nullstelle von $X^n - \overline{1} = \overline{f}\,\overline{g}$. Wegen $p \nmid n$ ist aber $X^n - \overline{1} \in \mathbb{F}_p[X]$ separabel, ein Widerspruch . □

Satz 8.3.6. *Sei K ein Körper, $n \in \mathbb{N}$, $\operatorname{char}(K) \nmid n$, und sei L ein n-ter Kreiskörper über K.*

1. *Für alle $\zeta \in \mu_n^*(L)$ ist $L = K(\zeta)$, es ist $[L\colon K] \mid \varphi(n)$, und im Falle $K = \mathbb{Q}$ ist $[L\colon K] = \varphi(n)$.*
2. *L/K ist endlich galoissch, und es gibt genau einen Gruppenmonomorphismus*

$$\theta\colon \operatorname{Gal}(L/K) \to (\mathbb{Z}/n\mathbb{Z})^\times$$

so dass für alle $\sigma \in \operatorname{Gal}(L/K)$, $\zeta \in \mu_n(L)$ und $k \in \mathbb{Z}$ gilt: $\sigma(\zeta) = \zeta^k \iff \theta(\sigma) = k + n\mathbb{Z}$.

Im Falle $K = \mathbb{Q}$ ist θ ein Isomorphismus.

BEWEIS. 1. Nach Definition ist $L = K(\mu_n^*(L))$. Ist $\zeta \in \mu_n^*(L)$, so ist $\mu_n^*(L) \subset \langle\zeta\rangle$, und daher ist auch $L = K(\zeta)$. Ist $f \in K[X]$ das Minimalpolynom von ζ über K, so ist $f \mid \Phi_n^K$ und daher $[L\colon K] = \operatorname{gr}(f) \le \operatorname{gr}\Phi_n^K$, mit Gleichheit im Falle $K = \mathbb{Q}$ nach Satz 8.3.5.

2. L ist Zerfällungskörper des separablen Polynoms Φ_n^K über K, und daher ist L/K galoissch nach Satz 6.6.11.

Sei $\zeta \in \mu_n^*(L)$ mit $L = K(\zeta)$ und $\sigma \in \operatorname{Gal}(L/K)$. Dann ist $\sigma(\zeta) \in \mu_n^*(L)$, also $\sigma(\zeta) = \zeta^k$ mit $k \in \mathbb{Z}$ und $\operatorname{ggT}(k, n) = 1$. Für $k' \in \mathbb{Z}$ ist genau dann $\zeta^k = \zeta^{k'}$, wenn $k + n\mathbb{Z} = k' + n\mathbb{Z}$. Daher ist die Restklasse $k + n\mathbb{Z}$ durch σ eindeutig bestimmt, und für alle $\zeta_1 \in \mu_n(L)$ so ist $\sigma(\zeta_1) = \zeta_1^k$ (denn ist $\zeta_1 \in \mu_n(L)$, so ist $\zeta_1 = \zeta^l$ mit $l \in \mathbb{N}$, und $\sigma(\zeta_1) = \sigma(\zeta)^l = \zeta^{kl} = \zeta_1^l$). Folglich existiert eine Abbildung

$$\theta\colon \operatorname{Gal}(L/K) \to (\mathbb{Z}/n\mathbb{Z})^\times\,,$$

so dass für alle $\sigma \in \operatorname{Gal}(L/K)$, $\zeta \in \mu_n(L)$ und $k \in \mathbb{Z}$ gilt: $\sigma(\zeta) = \zeta^k \iff \theta(\sigma) = k + n\mathbb{Z}$.

θ ist ein Homomorhpismus ist: Seien $\sigma, \tau \in \mathrm{Gal}(L/K)$, $\theta(\sigma) = k+n\mathbb{Z}$ und $\theta(\tau) = l+n\mathbb{Z}$. Für $\zeta \in \mu_n(L)$ ist dann $\sigma\tau(\zeta) = \sigma(\zeta^l) = \sigma(\zeta)^l = \zeta^{kl}$, und daher folgt $\theta(\sigma\tau) = kl + n\mathbb{Z} = \theta(\sigma)\theta(\tau)$. Ist $\sigma \in \mathrm{Ker}(\theta)$, also $\theta(\sigma) = 1 + n\mathbb{Z}$, so folgt $\sigma(\zeta) = \zeta$ und daher $\sigma = \mathrm{id}_{K(\zeta)} = \mathrm{id}_L$. Also ist θ ein Monomorphismus. □

Beispiel 8.3.7.

1. Es ist $\Phi_1 = X - 1$, $\Phi_2 = X + 1$, $\Phi_3 = X^2 + X + 1$, $\Phi_4 = X^2 + 1$, $\Phi_5 = X^4 + X^3 + X^2 + X + 1$, $\Phi_6 = X^2 - X + 1, \ldots$

1. Für $p \in \mathbb{P}$ ist $X^p - 1 = \Phi_1\Phi_p$ und daher

$$\Phi_p = \frac{X^p - 1}{X - 1} = X^{p-1} + \ldots + X + 1\,.$$

3. Φ_{105} ist das erste Kreisteilungspolynom mit einem von ± 1 verschiedenen Koeffizienten.

8.4. Konstruktionen mit Zirkel und Lineal

Problem: Welche geometrischen Konstruktionen sind mit Zirkel und Lineal durchführbar?

Definition 8.4.1. Für eine Teilmenge $S \subset \mathbb{C}$ sei $\overline{S} = \{\overline{z} \in \mathbb{C} \mid z \in S\}$. Sei $S \subset \mathbb{C}$.

1. Für $z_1, z_2 \in \mathbb{C}$ mit $z_1 \neq z_2$ sei $z_1 \vee z_2 = z_1 + \mathbb{R}(z_2 - z_1)$ die Verbindungsgerade von z_1 und z_2.
2. Für $z_0 \in \mathbb{C}$ und $r \in \mathbb{R}_{>0}$ sei $\mathsf{k}_r(z_0) = \left\{z \in \mathbb{C} \;\middle|\; |z - z_0| = r\right\}$ die Kreislinie mit Mittelpunkt z_0 und Radius r.
3. Eine Teilmenge $g \subset \mathbb{C}$ heißt *Gerade über S*, wenn $z_1, z_2 \in S$ existieren mit $g = z_1 \vee z_2$.
4. Eine Teilmenge $k \subset \mathbb{C}$ heißt *Kreis über S*, wenn $z_0, z_1, z_2 \in S$ existieren mit $z_1 \neq z_2$ und $k = \mathsf{k}_{|z_1 - z_2|}(z_0)$.
5. Ein Punkt $z \in \mathbb{C}$ heißt *direkt aus S konstruierbar*, wenn eine der folgenden vier Bedingungen erfüllt ist:
   (a) $z \in S$.
   (b) Es gibt zwei Gerade g_1, g_2 über S mit $g_1 \cap g_2 = \{z\}$.
   (c) Es gibt eine Gerade g über S und einen Kreis k über S mit $z \in g \cap k$.
   (d) Es gibt zwei Kreise k_1, k_2 über S mit $k_1 \neq k_2$ und $z \in k_1 \cap k_2$.
6. Die Folge $(S_n)_{n\geq 0}$ von Teilmengen von $\mathbb{C}$ sei rekursiv definiert durch $S_0 = S$, und für $n \geq 0$ sei $S_{n+1} \supset S_n$ die Menge der aus S_n direkt konstruierbaren Punkte. Dann heißt

$$C(S) = \bigcup_{n\geq 0} S_n \subset \mathbb{C}$$

die *Menge der aus S konstruierbaren Punkte.*

Die Menge $C = C(\{0,1\})$ heißt die *Menge der (absolut) konstruierbaren Punkte.*

Satz 8.4.2. *Sei $\{0,1\} \subset S \subset \mathbb{C}$.*

1. *$C(C(S)) = C(S)$.*
2. *$C(S) \subset \mathbb{C}$ ist ein Teilkörper.*
3. *Ist $z \in C(S)$, so sind $\Re(z)$, $\Im(z)$, $\overline{z}$, $|z| \in C(S)$, und ist $w \in \mathbb{C}$ mit $w^2 = z$, so ist auch $w \in C(S)$.*

BEWEIS. 1. Sei $(S'_n)_{n\geq 0}$ rekursiv definiert durch $S'_0 = C(S)$, und für $n \geq 0$ sei S'_{n+1} die Menge der direkt aus S'_n konstruierbaren Punkte. Dann folgt

$$C(C(S)) = \bigcup_{n\geq 0} S'_n \supset C(S)\,,$$

und es genügt, zu zeigen: Für alle $n \in \mathbb{N}_0$ ist $S'_n \subset C(S)$.

Induktion nach n. Für $n = 0$ ist nichts zu zeigen. Sei $n \geq 0$, $S'_n \subset C(S)$ und $z \in S'_{n+1}$. Dann ist z direkt aus $C(S)$ konstruierbar, und daher gibt es eine endliche Menge $E \subset C(S)$, so daß z direkt aus E konstruierbar ist. Dann gibt es ein $k \in \mathbb{N}_0$ mit $E \subset S_k$, und es folgt $z \in S_{k+1} \subset C(S)$.

2. und 3. Wir führen den Beweis in 8 Konstruktionsschritten.

1. *Sei g eine Gerade über $C(S)$, $z \in C(S)$ und l das Lot von z auf g. Dann ist auch l eine Gerade über $C(S)$.*

Beweis. FALL 1: $z \in g$. Dann gibt es einen Punkt $z_1 \in g \cap C(S)$ mit $z_1 \neq z$, $k = \mathsf{k}_{|z-z_1|}(z)$ ist ein Kreis über $C(S)$, und es gibt einen Punkt $z_2 \in k \cap g \setminus \{z_1\} \subset C(C(S)) = C(S)$. Daher sind $k_1 = \mathsf{k}_{|z_1-z_2|}(z_1)$ und $k_2 = \mathsf{k}_{|z_1-z_2|}(z_2)$ Kreise über $C(S)$. Ist nun $w \in k_1 \cap k_2 \subset C(S)$, so ist $l = w \vee z$ eine Gerade über $C(S)$.

FALL 2: $z \notin g$. Sei $z_1 \in g \cap C(S)$, also $\mathsf{k}_{|z-z_1|}(z) \cap g = \{z_1, z_2\} \subset C(S)$. Ist $z_1 = z_2$, so ist $l = z \vee z_1$ eine Gerade über $C(S)$. Ist $z_1 \neq z_2$, so ist $\mathsf{k}_{|z-z_1|}(z_1) \cap \mathsf{k}_{|z-z_1|}(z_2) = \{z, w\}$ mit $w \neq z$, also $w \in C(S)$, und $l = z \vee w$ ist eine Gerade über $C(S)$. □

2. *$\mathbb{R}$ und $\mathsf{i}\,\mathbb{R}$ sind Geraden über $C(S)$.*

Beweis. Wegen $\mathbb{R} = 0 \vee 1$ ist $\mathbb{R}$ eine Gerade über $C(S)$, und $\mathsf{i}\mathbb{R}$ ist das Lot von 0 auf $\mathbb{R}$, also eine Gerade über $C(S)$ nach **1.** □

3. *Sei $z = x + iy$ mit $x, y \in \mathbb{R}$. Genau dann ist $z \in C(S)$, wenn $x, y \in C(S)$.*

Beweis. Sei $z \in C(S)$, l_1 das Lot von z auf $\mathbb{R}$ und l_2 das Lot von z auf $\mathsf{i}\mathbb{R}$. Nach **1.** und **2.** sind l_1 und l_2 Geraden über $C(S)$, und es folgt $\{x\} = \mathbb{R} \cap l_1$ und $\{\mathsf{i}y\} = \mathsf{i}\,\mathbb{R} \cap l_2$, und daher folgt $x, \mathsf{i}y \in C(C(S)) = C(S)$. Im Falle $y = 0$ sind wir fertig, im Falle $y \neq 0$ ist $\mathsf{k}_{|\mathsf{i}y|}(0)$ ein Kreis über $C(S)$ und $y \in \mathbb{R} \cap \mathsf{k}_{|\mathsf{i}y|}(0)$, also ebenfalls $y \in C(S)$.

Seien nun $x, y \in C(S)$. Im Falle $y = 0$ ist $z = x \in C(S)$. Im Falle $y \neq 0$ ist $\mathsf{k}_{|y|}(0)$ ein Kreis über $C(S)$ und $\mathsf{i}y \in \mathsf{k}_{|y|}(0) \cap \mathsf{i}\,\mathbb{R}$, also nach **2.** $\mathsf{i}y \in C(S)$. Ist l_1 das Lot von x auf $\mathbb{R}$ und l_2 das Lot von $\mathsf{i}y$ auf $\mathsf{i}\mathbb{R}$, so sind l_1 und l_2 Geraden über $C(S)$ (nach **1.** und **2.**), und $l_1 \cap l_2 = \{z\} \subset C(S)$. □

4. *Für alle $x, y \in C(S) \cap \mathbb{R}$ ist $x \pm y \in C(S)$, $xy \in C(S)$, und im Falle $x \neq 0$ ist auch $x^{-1} \in C(S)$.*

Beweis. Wir können $y \neq 0$ annehmen. Dann ist $x \pm y \in \mathsf{k}_{|y|}(x) \cap \mathbb{R} \subset C(C(S)) = C(S)$. Insbesondere folgt (mit $x = 0$) für alle $w \in \mathbb{R}$: $w \in C(S) \iff |w| \in C(S)$.

Daher bleibt zu zeigen: Für alle $x, y \in \mathbb{R}_{>0}$ ist $xy \in C(S)$ und $x^{-1} \in C(S)$. Seien $x, y \in \mathbb{R}_{>0}$. Sei l_1 das Lot von 1 auf $\mathbb{R}$ und $\mathfrak{l}$ das Lot von x auf $\mathbb{R}$. Sei $z \in l_1 \cap \mathsf{k}_y(1)$, $g = 0 \vee z$ und $\{w\} = g \cap l$. Dann ist nach dem Strahlensatz $xy = |w - x|$ und $xy \in \mathsf{k}_{|w-x|}(0) \cap \mathbb{R} \subset C(S)$.

Sei $g = \mathsf{i} \vee x$ und h das Lot von i auf g. Nach **3.** ist $\mathsf{i} \in C(S)$, und daher sind g und h Geraden über $C(S)$. Nach dem Höhensatz für rechtwinkelige Dreiecke folgt $h \cap \mathbb{R} = \{-x^{-1}\} \subset C(S)$, und daher ist $x^{-1} \in C(S)$. □

5. *$C(S)$ ist ein Körper.*

Beweis. Nach **4.** ist $C(S) \cap \mathbb{R}$ ein Körper. Sind $z_1, z_2 \in \mathbb{C}$ mit $z_\nu = x_\nu + \mathsf{i}y_\nu$ für $\nu \in \{1, 2\}$, so folgt

$$z_1 \pm z_2 = (x_1 \pm x_2) + \mathsf{i}(y_1 \pm y_2)\,,\quad z_1 z_2 = (x_1 y_1 - x_2 y_2) + \mathsf{i}(x_1 y_2 + x_2 y_1) \text{ und } z_1^{-1} = \frac{x_1 - \mathsf{i}y_1}{x_1^2 + y_1^2}\,,\text{ falls } z_1 \neq 0\,.$$

6. *Ist $z \in C(S)$, so folgt $|z| \in C(S)$ und $\overline{z} \in C(S)$.*

Beweis. Wir können $z = x + \mathrm{i}y \neq 0$ annehmen. Dann ist $|z| \in \mathbb{R} \cap \mathsf{k}_{|z|}(0) \subset C(S)$, und mit **3.** und **4.** folgt $y \in C(S)$, $-y \in C(S)$ und $\overline{z} = x - \mathrm{i}y \in C(S)$. □

7. *Für alle* $r \in C(S) \cap \mathbb{R}_{>0}$ *ist* $\sqrt{r} \in C(S)$.

Beweis. Nach **5.** ist $z = \frac{1}{2}(r-1) \in C(S)$ und daher $k = \mathsf{k}_{\frac{1}{2}(r+1)}(z)$ ein Kreis über $C(S)$. Ist $w \in k \cap \mathrm{i}\mathbb{R}$, so ist das Dreieck $(-1, r, w)$ nach dem Satz vom Thaleskreis rechtwinkelig bei w, und nach dem Höhensatz und **6.** folgt $|w| = \sqrt{r} \in C(S)$. □

8. *Ist* $z \in C(S)$ *und* $w \in \mathbb{C}$ *mit* $w^2 = z$*, so folgt* $w \in C(S)$.

Beweis. Sei $z = r\mathsf{e}^{\mathrm{i}\varphi} \in \mathbb{C}^\times$ und $w \in \mathbb{C}$ mit $w^2 = z$. Dann ist $r = |z| \in C(S) \cap \mathbb{R}_{>0}$, $\sqrt{r} \in C(S)$ und $\mathsf{e}^{i\varphi} = |z|^{-1} z \in C(S)$ nach **5.**, **6.** und **7.**, und es genügt, $\mathsf{e}^{\mathrm{i}\varphi/2} \in C(S)$ zu zeigen, denn dann ist $w = \pm\sqrt{r}\,\mathsf{e}^{\mathrm{i}\varphi/2} \in C(S)$. Sei dazu $z \in \mathsf{k}_2(\mathsf{e}^{\mathrm{i}\varphi}) \cap \mathsf{k}_2(1) \subset C(S)$ und $g = 0 \vee z$. Dann ist g eine Gerade über $C(S)$ und $\mathsf{e}^{\mathrm{i}\varphi/2} \in \mathsf{k}_1(0) \cap g$, also $\mathsf{e}^{\mathrm{i}\varphi/2} \in C(S)$. □ □

Satz 8.4.3 (Konstruktion mit Zirkel und Lineal)**.** *Sei* $\{0,1\} \subset S \subset \mathbb{C}$.

1. *Für* $z \in \mathbb{C}$ *sind folgende Aussagen äquivalent*:
   (a) $z \in C(S)$.
   (b) *Es existiert eine Folge von Körpern* $\mathbb{Q}(S \cup \overline{S}) = L_0 \subset L_1 \subset \ldots \subset L_n \subset \mathbb{C}$*, so dass* $z \in L_n$ *und* $[L_i : L_{i-1}] = 2$ *für alle* $i \in [1, n]$.
   (c) *Es existiert eine endliche galoissche Köpererweiterung* $N/\mathbb{Q}(S \cup \overline{S})$ *von 2-Potenzgrad mit* $z \in N$.
2. *Sei* $C = C(\{0,1\})$*. Dann ist* $C \subset \overline{\mathbb{Q}}$*, und für jedes* $z \in C$ *ist* $[\mathbb{Q}(z) : \mathbb{Q}]$ *eine 2-Potenz.*

Beweis. 1. (a) ⇒ (b) Wir zeigen die folgenden beiden Behauptungen:

A. Sei $S \subset \mathbb{C}$ und $z \in C(S)$. Dann gibt es eine endliche Folge $(z_1, \ldots, z_m)$ in $\mathbb{C}$ mit $z_m = z$, so dass für alle $j \in [1, m]$ gilt: z_j ist direkt aus $S \cup \{z_1, \ldots, z_{j-1}\}$ konstruierbar.

B. Sei $L \subset \mathbb{C}$ ein Teilkörper mit $\mathsf{i} \in L$ und $L = \overline{L}$, und sei $z \in \mathbb{C}$ direkt aus L konstruierbar. Dann ist $[L(z, \overline{z}) : L] \leq 2$.

Seien **A** und **B** gezeigt und sei $(z_1, \ldots, z_m)$ wie in **A**. Sei $L_0 = \mathbb{Q}(S \cup \overline{S})$, $L_1 = L_0(\mathrm{i})$, und für $j \in [1, m]$ sei $L_{j+1} = L_0(\mathrm{i}, z_1, \ldots, z_j, \overline{z}_1, \ldots, \overline{z}_j)$. Dann ist $z \in L_{m+1}$ und $L_0 \subset L_1 \subset \ldots \subset L_{m+1}$. Da i Nullstelle von $X^2 + 1$ ist, folgt $[L_1 : L_0] \leq 2$. Für $j \in [1, m]$ ist $L_{j+1} = L_j(z_j, \overline{z}_j)$, und wegen $S \cup \{z_1, \ldots, z_{j-1}\} \subset L_j$ ist z_j direkt aus L_j konstruierbar. Daher folgt $[L_{j+1} : L_j] \leq 2$ nach **B**.

Beweis von **A**. Sei $(S_n)_{n \geq 0}$ wie in Definition 8.4.1.6 und $z \in C(S)$. Dann gibt es ein $n \in \mathbb{N}_0$ mit $z \in S_n$, und wir beweisen die Behauptung durch Induktion nach n. Im Falle $n = 0$ folgt die Behauptung mit $m = 1$ und $z_1 = z$.

$n \geq 2$, $n-1 \to n$: Sei $z \in S_n$, und seien $y_1, \ldots, y_k \in S_{n-1}$, so dass z direkt aus $\{y_1, \ldots, y_k\}$ konstruierbar ist. Nach Induktionsvoraussetzung gibt es zu jedem $\nu \in [1, k]$ eine endliche Folge $(z_{\nu,1} \ldots, z_{\nu,m_\nu})$ in $\mathbb{C}$, so dass $z_{\nu,m_\nu} = y_\nu$ und für alle $\rho \in [1, m_\nu]$ gilt: $z_{\nu,\rho}$ ist direkt aus $S \cup \{z_{\nu,1}, \ldots, z_{\nu,\rho-1}\}$ konstruierbar. Daher hat die Folge $(z_1, \ldots, z_m) = (z_{1,1}, \ldots, z_{1,m_1}, z_{2,1}, \ldots, z_{2,m_2}, \ldots, z_{k,1}, \ldots, z_{k,m_k})$ die verlangte Eigenschaft. □

Beweis von **B**. Wegen $L = \overline{L}$ und $\mathsf{i} \in L$ gilt für alle $z \in \mathbb{C}$: $z \in L \iff \Re(z) \in L$ und $\Im(z) \in L$.
Ist $z = x + \mathrm{i}y$ mit $x, y \in \mathbb{R}$, so ist genau dann $z \in L$, wenn $x, y \in L$.

Sei z direkt aus L konstruierbar.

FALL 1: Es gibt Geraden g_1, g_2 über L mit $\{z\} = g_1 \cap g_2$. Sei $g_\nu = z_\nu + \mathbb{R}(w_\nu - z_\nu)$ mit z_ν, $w_\nu \in L$ und $z_\nu \neq w_\nu$. Dann gibt es eindeutig bestimmte t_1, $t_2 \in \mathbb{R}$, so dass $z = z_\nu + t_\nu(w_\nu - z_\nu)$ für $\nu \in \{1, 2\}$, und (t_1, t_2) ist die eindeutig bestimmte Lösung des linearen Gleichungssystems

$$t_1\Re(w_1 - z_1) - t_2\Re(w_2 - z_2) = \Re(z_2 - z_1) \quad \text{und} \quad t_1\Im(w_1 - z_1) - t_2\Im(w_2 - z_2) = \Im(z_2 - z_1)\,.$$

Löst man dieses Gleichungssystem mit der Cramer'schen Regel, so folgt $t_1, t_2 \in L$, also auch $z \in L$ und damit $\overline{z} \in \overline{L} = L$. Daher ist in diesem Falle $L(z, \overline{z}) = L$.

FALL 2: Es gibt eine Gerade g und einen Kreis k über L mit $z \in g \cap k$. Sei $g = z_0 + \mathbb{R}(z_1 - z_0)$ und $k = \mathsf{k}_{|z_3 - z_4|}(z_2)$ mit $z_\nu \in L$ für alle $\nu \in [1,4]$, $z_1 \neq z_0$ und $z_3 \neq z_4$. Dann ist $z = z_0 + t(z_1 - z_0) \in L(t)$ und $\overline{z} \in L(t)$ mit $t \in \mathbb{R}$, so dass $|z_0 + t(z_1 - z_0) - z_2|^2 = |z_3 - z_2|^2$. Daher ist t Nullstelle eines Polynoms $g \in L[X]$ mit $\mathrm{gr}(g) \leq 2$, und es folgt $[L(z, \overline{z}) : L] \leq [L(t) : L] \leq 2$.

FALL 3: Es gibt zwei Kreise k_1, k_2 über L mit $k_1 \neq k_2$ und $z \in k_1 \cap k_2$. Für $\nu \in \{1, 2\}$ sei $k_\nu = \mathsf{k}_{|z'_\nu - z''_\nu|}(z_\nu)$ mit $z_\nu, z'_\nu, z''_\nu \in L$. Dann ist auch $r_\nu = |z'_\nu - z''_\nu|^2 = (z'_\nu - z''_\nu)(\overline{z'_\nu} - \overline{z''_\nu}) \in L$. Setzt man $z_\nu = x_\nu + iy_\nu$ und $z = x + iy$ mit $x, x_\nu, y, y_\nu \in \mathbb{R}$, so folgt $x_\nu, y_\nu \in L$, $(x_1, y_1) \neq (x_2, y_2)$ und

$$(\dagger) \qquad (x - x_\nu)^2 + (y - y_\nu)^2 = r_\nu \quad \text{für} \quad \nu \in \{1, 2\}.$$

Subtrahiert man diese beiden Gleichungen von einander, so folgt

$$x(x_2 - x_1) + y(y_2 - y_1) = r_1 - r_2 - x_1^2 - y_1^2 + x_2^2 + y_2^2 \in L.$$

Ist $x_2 - x_1 \neq 0$, so folgt $x = ay + b$ mit $a, b \in L$, also $x \in L(y)$, und Einsetzen in $(\dagger)$ liefert eine Gleichung der Form $g(y) = 0$ mit $g \in L[X]$ und $\mathrm{gr}(g) \leq 2$. Damit folgt $[L(y) : L] \leq 2$ und wegen $L(z, \overline{z}) = L(x, y) = L(y)$ die Behauptung. Im Falle $y_2 - y_1 \neq 0$ schließt man analog. □

1. (b) $\Rightarrow$ (c) Sei $\mathbb{Q}(S \cup \overline{S}) = L_0 \subset L_1 \subset \ldots \subset L_n \subset \mathbb{C}$ eine Folge von Körpern, so dass $z \in L_n$ und $[L_i : L_{i-1}] = 2$ für alle $i \in [1, n]$. Dann ist $[L_n : L_0] = 2^n$, und L_n / L_0 ist separabel (da $\mathrm{char}(\mathbb{Q}) = 0$). Sei N eine galoissche Hülle von L_n / L_0, $G = \mathrm{Gal}(N / L_0)$ und $G_j = \mathrm{Gal}(N / L_j)$ für alle $j \in [0, n]$. Dann folgt $G = G_0 \supset G_1 \supset \ldots \supset G_n$,

$$(G_{j-1} : G_j) = \frac{|G_{j-1}|}{|G_j|} = \frac{[N : L_{j-1}]}{[N : L_j]} = [L_j : L_{j-1}] = 2 \quad \text{für alle } j \in [1, n], \text{ und } \bigcap_{\sigma \in G} \sigma G_n \sigma^{-1} = \{\mathrm{id}_N\}$$

nach Korollar 8.1.7. Nach Satz 2.3.2.7 ist insbesondere $G_j \lhd G_{j-1}$ für alle $j \in [1, n]$, und aus Satz 7.5.4.2 folgt: G ist auflösbar, und jeder Primteiler von $|G|$ teilt $(G : G_n) = 2^n$. Daher ist $[N : L_0] = |G|$ eine 2-Potenz.

1. (c) $\Rightarrow$ (a) Sei $L_0 = \mathbb{Q}(S \cup \overline{S})$, N / L_0 endlich galoissch, $G = \mathrm{Gal}(N / L_0)$, $|G| = [N : L_0] = 2^r$ mit $r \in \mathbb{N}_0$ und $z \in N$. Dann ist $[L_0(z) : L_0] = 2^s$ mit $s \in [0, r]$, und wir führen den Beweis durch Induktion nach s.

$s = 0$: Dann ist $z \in L_0 \subset C(S)$.

$s \in [1, r]$, $s - 1 \to s$: Sei $H = \mathrm{Gal}(N / L_0(z))$. Dann ist $|H| = [N : L_0(z)] = 2^{r-s}$, nach Satz 7.4.5.1 gibt es eine Untergruppe $H' < G$ mit $H \subset H'$ und $|H'| = 2^{r-s+1}$, und es sei $L = N^H$. Dann ist $L_0 \subset L \subset L_0(z)$ und $[L_0(z) : L] = (H' : H) = 2$. Nach Beispiel 6.3.4.4 ist $L_0(z) = L(y)$ mit $y \in L$, so dass $y^2 = x \in L_0$. Nach Induktionsvoraussetzung ist $x \in C(S)$, und nach Satz 8.4.2.3 ist auch $y \in C(S)$, also $z \in L_0(z) = L_(y) \subset C(S)$.

2. Ist $z \in C$, so ist $\mathbb{Q}(z) / \mathbb{Q}$ eine endliche Körpererweiterung von 2-Potenzgrad nach 1.(b) und daher insbesondere $z \in \overline{\mathbb{Q}}$. □

Korollar 8.4.4 (Delisches Problem der Würfelverdoppelung). *Es ist* $\sqrt[3]{2} \notin C$. Es ist nicht möglich, aus der Seite eines gegebenen Würfels die Seite eines Würfels mit doppeltem Volumen zu konstruieren.

BEWEIS. Es ist $[\mathbb{Q}(\sqrt[3]{2}) : \mathbb{Q}] = 3$ und daher $\sqrt[3]{2} \notin C$ nach Satz 8.4.3.2. □

Korollar 8.4.5 (Quadratur des Kreises). *Es ist* $\sqrt{\pi} \notin C$. Es ist nicht möglich, aus dem Radius eines gegebenen Kreises die Seite eines Quadrates mit gleichem Flächeninhalt zu konstruieren.

BEWEIS. Nach dem Satz von Lindemann ist $\pi \notin \overline{\mathbb{Q}}$ und daher auch $\sqrt{\pi} \notin \overline{\mathbb{Q}}$. Nach Satz 8.4.3.2 ist daher auch $\sqrt{\pi} \notin C$. □

Korollar 8.4.6 (Konstruktion des regelmäßigen n-Ecks)**.** *Sei $n \in \mathbb{N}_{\geq 3}$. Dann sind die folgenden Aussagen äquivalent*:

(a) $\zeta_n = \mathrm{e}^{2\pi \mathrm{i}/n} \in C$ (das regelmäßige n-Eck ist mit Zirkel und Lineal konstruierbar).

(b) $\varphi(n)$ *ist eine* 2*-Potenz.*

(c) $n = 2^a p_1 \cdot \ldots p_r$ *mit* $a, r \in \mathbb{N}_0$ *und verschiedenen Fermat'sche Primzahlen* $p_1, \ldots, p_r$.

Beweis. (a) $\Leftrightarrow$ (b) Nach Satz 8.3.6 ist $\mathbb{Q}(\zeta_n)/Q$ endlich galoissch vom Grade $\varphi(n)$. Daher folgt die Behauptung aus Satz 8.4.3.

(b) $\Leftrightarrow$ (c) Sei $n = 2^a p_1^{e_1} \cdot \ldots \cdot p_r^{e_r}$ mit $a, r \in \mathbb{N}_0$, $e_1, \ldots, e_r \in \mathbb{N}$ und verschiedenen ungeraden Primzahlen $p_1, \ldots, p_r$. Dann ist

$$\varphi(n) = 2^{a-1} \prod_{i=1}^{r} p^{e_i - 1}(p_i - 1)\,,$$

also genau dann $\varphi(n)$ eine 2-Potenz, wenn $e_i = 1$ und $p_i = 2^{k_i} + 1$ mit $k_i \in \mathbb{N}$ für alle $i \in [1, r]$. Aber $p_i = 2^{k_i} + 1$ ist höchstens dann eine Primzahl, wenn k_i eine 2-Potenz und p_i eine Fermat'sche Primzahl ist (siehe Satz 1.1.10.1. □

Beispiel 8.4.7. Das regelmäßige n-Eck ist für $n \in \{7, 9, 11, 13, \ldots\}$ nicht konstruierbar und für $n \in \{3, 4, 5, 6, 8, 10, 12, \ldots 257, 65537 \ldots\}$ konstruierbar.

Korollar 8.4.8 (Winkeldreiteilung)**.** *Es existieren $\alpha \in [0, \pi)$ mit $\cos \frac{\alpha}{3} \notin C(\{0, 1, \cos \alpha\})$.* Es gibt kein Konstruktionsverfahren zur Dreiteilung eines beliebigen Winkels.

Beweis. Sei $\alpha = \frac{\pi}{3}$. Dann ist $\cos \alpha = \frac{1}{2}$ und daher $\mathbb{C}(\{0, 1, \cos \alpha\}) = \mathbb{Q}$. Nach Korollar 8.4.6 ist $\mathrm{e}^{\mathrm{i}\pi/9} \notin C$. Wäre aber $\cos \frac{\pi}{9} \in C$, so folgte auch

$$\mathrm{e}^{\mathrm{i}\pi/9} = \cos \frac{\pi}{9} + \mathrm{i}\sqrt{1 - \cos^2 \frac{\pi}{9}} \in C\,, \quad \text{ein Widerspruch.}$$

□

8.5. Auflösbarkeit algebraischer Gleichungen durch Radikale

Definition 8.5.1. Eine Körpererweiterung L/K heißt *zyklisch* [*abelsch, auflösbar*], wenn L/K endlich galoissch und $\mathrm{Gal}(L/K)$ zyklisch [abelsch, auflösbar] ist.

Lemma 8.5.2. *Seien N/K und N'/K Körpererweiterungen, $\mathrm{Hom}_K(N, N') \neq \emptyset$, N/K sei endlich galoissch, und N'/K sei zyklisch* [*abelsch, auflösbar*]*. Dann ist auch N/K zyklisch* [*abelsch, auflösbar*].

Beweis. Sei $\varphi \in \mathrm{Hom}_K(N, N')$. Dann ist $\varphi(N) \subset N'$ ein Teilkörper, $\varphi\colon N \to \varphi(N)$ ist ein K-Isomorphismus, und

$$\varphi^*\colon \mathrm{Gal}(\varphi(N)/K) \to \mathrm{Gal}(N/K) \quad \text{definiert durch} \quad \varphi^*(\sigma) = \varphi^{-1} \circ \sigma \circ \varphi\,.$$

ist ein Gruppenisomorphismus. Daher ist $[\varphi(N) : K] = [N : K] = |\mathrm{Gal}(N/K)| = |\mathrm{Gal}(\varphi(N)/K)|$, also $\varphi(N)/K$ galoissch, und nach Korollar 8.1.6 ist $\mathrm{Gal}(\varphi(N)/K)$ isomorph zu einer Faktorgruppe von $G' = \mathrm{Gal}(N'/K)$. Also ist auch $\mathrm{Gal}(N/K)$ isomorph zu einer Faktorgruppe von G' und daher mit G' zyklisch [abelsch, auflösbar]. □

Satz 8.5.3. *Sei K ein Körper, $n \in \mathbb{N}$ und $\zeta \in \mu_n^*(K)$.*

1. *Sei $a \in K^\times$, L ein Zerfällungskörper von $X^n - a$ über K und $\alpha \in L$ mit $\alpha^n = a$. Dann ist L/K zyklisch, $[L:K] \mid n$, $L = K(\alpha)$, und die Abbildung*

$$\theta\colon \mathrm{Gal}(L/K) \to \mu_n(K), \quad \textit{definiert durch} \quad \theta(\sigma) = \frac{\sigma(\alpha)}{\alpha},$$

ist ein (von α unabhängiger) Gruppenmonomorphismus.

2. *Sei L/K zyklisch und $[L:K] \mid n$. Dann existiert ein $\alpha \in L^\times$ mit $L = K(\alpha)$ und $\alpha^n \in K$.*

Beweis. Wegen $\mu_n^*(K) \neq \emptyset$ ist $\mathrm{char}(K) \nmid n$ nach Lemma 8.3.2.3.

1. Es ist

$$X^n - a = \prod_{\nu=0}^{n-1} (X - \zeta^\nu \alpha),$$

und wegen $\zeta \in \mu_n^*(K) \subset K$ zerfällt $X^n - a$ über $K(\alpha)$ in verschiedene Linearfaktoren. Daher ist $K(\alpha) = L$ und $X^n - a$ separabel, also L/K galoissch nach Satz 6.6.11. Ist $\sigma \in \mathrm{Gal}(L/K)$, so folgt

$$\Big(\frac{\sigma(\alpha)}{\alpha}\Big)^n = \frac{\sigma(\alpha^n)}{\alpha^n} = \frac{\sigma(a)}{a} = 1 \quad \text{und} \quad \frac{\sigma(\zeta^\nu \alpha)}{\zeta^\nu \alpha} = \frac{\zeta^\nu \sigma(\alpha)}{\zeta^\nu \alpha} = \frac{\sigma(\alpha)}{\alpha} \quad \text{für alle } \nu \in [0, n-1].$$

Daher ist

$$\theta(\sigma) = \frac{\sigma(\alpha)}{\alpha} \in \mu_n(K) \quad \text{und unabhängig von } \alpha.$$

Sind $\sigma, \tau \in \mathrm{Gal}(L/K)$, so ist $\tau(\alpha) = \theta(\tau)\alpha$ und

$$\theta(\sigma\tau) = \frac{\sigma\tau(\alpha)}{\alpha} = \frac{\sigma(\tau(\alpha))}{\tau(\alpha)} \frac{\tau(\alpha)}{\alpha} = \frac{\sigma(\theta(\tau)\alpha)}{\theta(\tau)\alpha} \frac{\tau(\alpha)}{\alpha} = \frac{\theta(\tau)\sigma(\alpha)}{\theta(\tau)\alpha} \frac{\tau(\alpha)}{\alpha} = \frac{\sigma(\alpha)}{\alpha} \frac{\tau(\alpha)}{\alpha} = \theta(\sigma)\theta(\tau).$$

Daher ist θ ein Gruppenhomomorphismus. Ist $\sigma \in \mathrm{Ker}(\theta)$, so ist $\sigma(\alpha) = \alpha$, also $\sigma = \mathrm{id}_L$. Folglich ist θ ein Monomorphismus und $\mathrm{Gal}(L/K)$ isomorph zu einer Untergruppe von $\mu_n(K)$. Daher ist $\mathrm{Gal}(L/K)$ zyklisch, und $[L:K] = |\mathrm{Gal}(L/K)| \mid n$.

2. Sei $\mathrm{Gal}(L/K) = \langle\sigma\rangle$, und sei zuerst $[L:K] = n$. Nach Satz 8.1.2 ist

$$\Big(\sum_{\nu=0}^{n-1} \zeta^{-\nu}\sigma^\nu : L \to L\Big) \neq 0, \quad \text{und daher gibt es ein } \beta \in L, \text{ so dass } \quad \alpha = \sum_{\nu=0}^{n-1} \zeta^{-\nu}\sigma^\nu(\beta) \neq 0.$$

Wegen

$$\sigma(\alpha) = \sum_{\nu=0}^{n-1} \zeta^{-\nu}\sigma^{\nu+1}(\beta) = \zeta \sum_{\nu=1}^{n} \zeta^{-\nu}\sigma^\nu(\beta) = \zeta \sum_{\nu=0}^{n-1} \zeta^{-\nu}\sigma^\nu(\beta) = \zeta\,\alpha$$

folgt $\sigma(\alpha^n) = \sigma(\alpha)^n = \alpha^n$, also auch $\sigma^\nu(\alpha^n) = \alpha^n$ für alle $\nu \in [0, n-1]$, und daher $\tau(\alpha^n) = \alpha^n$ für alle $\tau \in \mathrm{Gal}(L/K)$. Es folgt $\alpha^n \in K$, $K \subset K(\alpha) \subset L$ und $\mathrm{Gal}(L/K(\alpha)) < \langle\sigma\rangle$. Ist $d \in \mathbb{N}_0$ mit $\sigma^d \in \mathrm{Gal}(L/K(\alpha))$, so folgt $\alpha = \sigma^d(\alpha) = \zeta^d\alpha$, also $\zeta^d = 1$ und daher $n \mid d$ und $\sigma^d = \mathrm{id}_L$. Daher ist $\mathrm{Gal}(L/K(\alpha)) = \{\mathrm{id}_L\}$ und $L = K(\alpha)$.

Sei nun $[L:K] = m|n$. Wegen $\zeta^{n/m} \in \mu_m^*(L)$ folgt $L = K(\alpha_1)$ mit $\alpha_1 \in L$ und $\alpha_1^m \in K$. Dann ist aber auch $\alpha_1^n = (\alpha_1^m)^{n/m} \in K$. □

Definition 8.5.4. Sei K ein Körper und $\mathrm{char}(K) = 0$.

1. Eine Körpererweiterung L/K heißt *durch Radikale auflösbar*, wenn es eine Folge von Körpern $K = K_0 \subset K_1 \subset \ldots \subset K_m$ gibt, so dass $L \subset K_m$, und für alle $j \in [1, m]$ gilt:

   Es existieren $\alpha_j \in K_j$ und $n_j \in \mathbb{N}$ mit $K_j = K_{j-1}(\alpha_j)$ und $\alpha_j^{n_j} \in K_{j-1}$.

2. Ein Polynom $f \in K[X] \setminus K$ heißt über K (*durch Radikale*) *auflösbar*, wenn es eine durch Radikale auflösbare Körpererweiterung L/K gibt, so dass f über L in Linearfaktoren zerfällt.

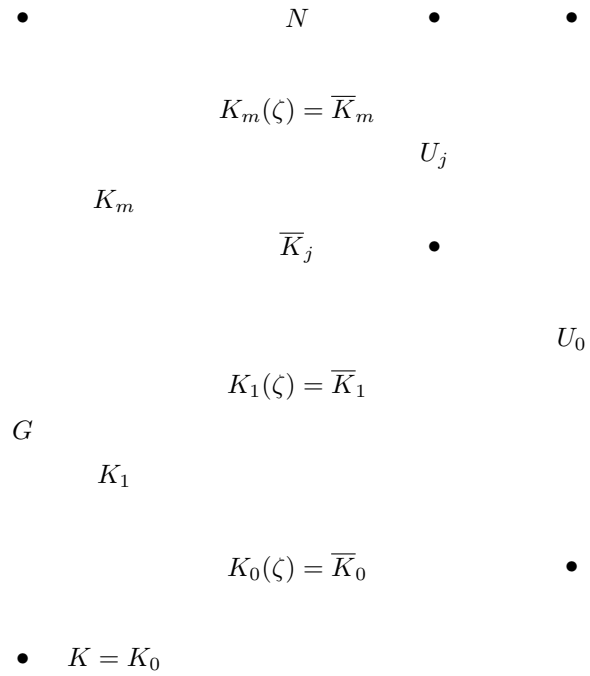
Satz 8.5.5. *Sei K ein Körper und* $\mathrm{char}(K) = 0$.

1. *Für eine Körpererweiterung* L/K *sind die folgenden Aussagen äquivalent*:
   (a) L/K *ist durch Radikale auflösbar.*
   (b) *Es gibt einen Oberkörper* $N \supset L$*, so dass* N/K *auflösbar ist.*
   (c) *Ist* N *eine galoissche Hülle von* L/K*, so ist* N/K *auflösbar.*
2. *Sei* $f \in K[X] \setminus K$ *und* L *ein Zerfällungskörper von* f *über* K*. Genau dann ist* f *durch Radikale auflösbar, wenn* L/K *auflösbar ist.*

BEWEIS. 1. (a) $\Rightarrow$ (b) Sei $K = K_0 \subset K_1 \subset \ldots \subset K_m$ eine Folge von Körpern, so dass $L \subset K_m$ und für alle $j \in [1,m]$ gilt: Es existieren $\alpha_j \in K_j$ und $n_j \in \mathbb{N}$ mit $\mathrm{char}(K) \nmid n_j$, $K_j = K_{j-1}(\alpha_j)$ und $\alpha_j^{n_j} \in K_{j-1}$. Sei $n = n_1 \cdot \ldots \cdot n_m \in \mathbb{N}$, $\overline{K}_m$ ein Zerfällungskörper von $X^n - 1$ über K_m, $\zeta \in \mu_n^*(\overline{K}_m)$, und für alle $j \in [0, m-1]$ sei $\overline{K}_j = K_j(\zeta)$. Für alle $j \in [1,m]$ ist dann $\overline{K}_j = K_{j-1}(\alpha_j, \zeta) = \overline{K}_{j-1}(\alpha_j)$, $\alpha_j^{n_j} \in \overline{K}_{j-1}$, und es ist $K = K_0 \subset \overline{K}_0 \subset \overline{K}_1 \subset \ldots \subset \overline{K}_m = K_m(\zeta)$. Sei $N \supset \overline{K}_m$ eine galoissche Hülle von $\overline{K}_m/K$, $G = \mathrm{Gal}(N/K)$ und $U_j = \mathrm{Gal}(N/\overline{K}_j)$ für alle $j \in [0,m]$. Dann ist

$$G = U_0 \supset U_1 \supset \ldots \supset U_m \qquad \text{und} \qquad \bigcap_{\sigma \in G} \sigma U_m \sigma^{-1} = \{\mathrm{id}_N\} \quad \text{nach Korollar 8.1.7.}$$

Für $j \in [1,m]$ ist $\overline{K}_j/\overline{K}_{j-1}$ zyklisch (nach Satz 8.5.3), also $U_j \lhd U_{j-1}$ und $U_{j-1}/U_j \cong \mathrm{Gal}(\overline{K}_j/\overline{K}_{j-1})$ zyklisch. Nach Satz 8.3.6 ist $\overline{K}_0/K_0$ abelsch, daher ist $U_0 \lhd G$, und $G/U_0 \cong \mathrm{Gal}(\overline{K}_0/K)$ abelsch. Nach Satz 7.5.4.2 ist G und damit N/K auflösbar.



2. (b) $\Rightarrow$ (c) Sei $N' \supset L$ ein Oberkörper, so dass N'/K auflösbar ist, und sei N eine galoissche Hülle von L/K. Nach Korollar 8.1.7 gibt es einen Zwischenkörper N_1 von N'/L, so dass N_1 eine galoissche Hülle von L/K ist. Nach Satz 6.6.12 gibt es einen L-Isomorphismus $\varphi\colon N \to N_1$. Dieser ist auch ein K-Isomorphismus, also ist $\mathrm{Hom}_K(N, N') \neq \emptyset$, und nach Lemma 8.5.2 ist N/K auflösbar.

2. (c) $\Rightarrow$ (a) Sei N eine galoissche Hülle von L/K, $G = \mathrm{Gal}(N/K)$ auflösbar und $|G| = n$. Nach Satz 7.5.4.1 besitzt G eine Auflösung $G = G_0 > G_1 > \ldots > G_m = \{\mathrm{id}_N\}$, so dass $G_j \lhd G_{j-1}$ und G_{j-1}/G_j primzyklisch ist für alle $j \in [1,m]$. Sei $\overline{N}$ ein Zerfällungskörper von $X^n - 1$ über N, $\zeta \in \mu_n^*(\overline{N})$, und für $j \in [0,m]$ sei $K_j = N^{G_j}$ und $\overline{K}_j = K_j(\zeta)$, also ist $\overline{K}_j = K_j \overline{K}_{j-1}$, und insbesondere $\overline{N} = \overline{K}_m$.

Wegen $G_j \lhd G_{j-1}$ ist K_j/K_{j-1} galoissch und $\mathrm{Gal}(K_j/K_{j-1} \cong G_{j-1}/G_j$ ist zyklisch. Aus Korollar 8.1.8 folgt, dass auch $\overline{K}_j/\overline{K}_{j-1}$ galoissch ist, und $\mathrm{Gal}(\overline{K}_j/\overline{K}_{j-1}) \cong \mathrm{Gal}(K_j/K_j \cap \overline{K}_{j-1}) < \mathrm{Gal}(K_j/K_{j-1})$. Daher ist auch $\mathrm{Gal}(K_j/K_{j-1}$ zyklisch, $[\overline{K}_j : \overline{K}_{j-1}] \,\big|\, |G| = n$, und wegen $\mu_n^*(\overline{K}_{j-1}) \neq \emptyset$ folgt mit Satz 8.5.2, dass $\overline{K}_j = \overline{K}_{j-1}(\alpha_j)$ mit $\alpha_j \in K_j$, so dass $\alpha_j^n \in \overline{K}_{j-1}$. Es ist auch $\overline{K}_0 = K_0(\zeta) = K(\zeta)$ und $\zeta^n = 1 \in K$ ist $\overline{N}/K$, und wegen $L \subset \overline{N}$ ist L/K duch Radikale auflösbar.

$$\overline{K}_m = K_m(\zeta) = \overline{N}$$

- $N = K_m$

G_j $\overline{K}_j = K_j(\zeta)$

- $K_j = N^{G_j}$

$\overline{K}_{j-1} = K_{j-1}(\zeta)$

G

$K_{j-1} = N^{G_{j-1}}$

$K_0(\zeta)$

- $K = K_0$

3. Ist L/K durch Radikale auflösbar, so ist nach Definition f auflösbar. Sei nun f auflösbar und L'/K eine durch Radikale auflösbare Körpererweiterung, so dass f über L' in Linearfaktoren zerfällt. Nach 1. gibt es einen Oberkörper $N \supset L'$, so dass N/K auflösbar ist. Seien $\alpha_1, \ldots, \alpha_n \in N$ die Nullstellen von f. Dann ist $L_1 = K(\alpha_1, \ldots, \alpha_n)$ ein Zerfällungskörper von f über K, und nach Satz 6.4.10 gibt es einen K-Isomorphismus $\varphi\colon L \to L_1$. Daher ist $\mathrm{Hom}_K(L, N) \neq \emptyset$, und nach Lemma 8.1.2 ist L/K auflösbar. □

Definition und Satz 8.5.6. *Sei K ein Körper, $f \in K[X] \setminus K$ separabel, N ein Zerfällungskörper von f über K, $G = \mathrm{Gal}(N/K)$ und*

$$f = a \prod_{\nu=1}^{n} (X - \alpha_\nu) \quad \textit{mit} \quad a \in K^\times \quad \textit{und} \quad \boldsymbol{\alpha} = (\alpha_1, \ldots, \alpha_n) \in N^n \,.$$

Dann gibt es einen (eindeutig bestimmten) Gruppenmonomorphismus

$$\theta = \theta_{\boldsymbol{\alpha}}\colon G \to \mathfrak{S}_n \,, \quad \textit{so dass} \quad \sigma(\alpha_\nu) = \alpha_{\theta(\sigma)(\nu)} \quad \textit{für alle} \quad \sigma \in G \quad \textit{und} \quad \nu \in [1, n] \,,$$

und das Bild $\theta(G) < \mathfrak{S}_n$ ist bis auf Konjugierte eindeutig durch f bestimmt.

Insbesondere ist G isomorph zu einer Untergruppe von $\mathfrak{S}_n$, $|G| = [L : K] \,|\, n!$, und f ist genau dann auflösbar, wenn G auflösbar ist .

Man nennt G die *Galoisgruppe* des Polynoms f und $\mathrm{Gal}(f, \boldsymbol{\alpha}) = \theta_{\boldsymbol{\alpha}}(G)$ eine Realisierung der Galoisgruppe von f über K als Permutationsgruppe.

Beweis. Es ist $N = K(\alpha_1, \ldots, \alpha_n)$, und daher ist für $\sigma, \tau \in G$ genau dann $\sigma(\alpha_\nu) = \tau(\alpha_\nu)$ für alle $\nu \in [1, n]$, wenn $\sigma = \tau$. Für $\nu \in [1, n]$ und $\sigma \in G$ ist $0 = \sigma(f(\alpha_\nu)) = f(\sigma(\alpha_\nu))$ und daher $\sigma(\alpha_\nu) \in \{\alpha_1, \ldots, \alpha_n\}$. Folglich gibt es eine eindeutig bestimmte injektive Abbildung $\theta\colon G \to \mathfrak{S}_n$, so

dass $\sigma(\alpha_\nu) = \alpha_{\theta(\sigma)(\nu)}$ für alle $\sigma \in G$ und $\nu \in [1,n]$. Diese ist ein Gruppenmonomorphismus, denn für alle $\sigma, \tau \in G$ und $\nu \in [1,n]$ ist $\alpha_{\theta(\sigma\tau)(\nu)} = \sigma\tau(\alpha_\nu) = \sigma(\alpha_{\theta(\tau)(\nu)}) = \alpha_{\theta(\sigma)\theta(\tau)(\nu)}$.
Sei nun N' ein weiterer Zerfällungskörper von f über K, $G' = \mathrm{Gal}(N'/K)$ und $\boldsymbol{\alpha}' = (\alpha'_1, \ldots, \alpha'_n) \in N'^n$ ein Nullstellenvektor von f. Nach Satz 6.4.10 gibt es einen K-Isomorphismus $\varphi\colon N \to N'$. Dieser induziert einen Gruppenisomorphismus $\varphi^*\colon G \to G'$ vermöge $\varphi^*(\sigma) = \varphi\circ\sigma\circ\varphi^{-1}$, und eine bijektive Abbildung $\varphi\,|\,\{\alpha_1, \ldots, \alpha_n\}\colon \{\alpha_1, \ldots, \alpha_n\} \to \{\alpha'_1, \ldots, \alpha'_n\}$. Sei $\rho \in \mathfrak{S}_n$ mit $\varphi(\alpha_\nu) = \alpha'_{\rho(\nu)}$ für alle $\nu \in [1,n]$. Für alle $\sigma \in G$ und $\nu \in [1,n]$ ist dann

$$\begin{aligned}\alpha'_{\theta'(\varphi\circ\sigma\circ\varphi^{-1})(\nu)} &= \varphi\circ\sigma\circ\varphi^{-1}(\alpha'_\nu) = \varphi\circ\sigma\circ\varphi^{-1}(\varphi(\alpha_{\rho^{-1}(\nu)})) = \varphi\circ\sigma(\alpha_{\rho^{-1}(\nu)}) = \varphi(\alpha_{\theta(\sigma)\circ\rho^{-1}(\nu)})\\ &= \alpha'_{\rho\circ\theta(\sigma)\circ\rho^{-1}(\nu)}\,, \quad \text{also} \quad \theta'(\varphi\circ\sigma\circ\varphi^{-1}) = \rho\circ\theta(\sigma)\circ\rho^{-1}\,.\end{aligned}$$

Die restlichen Aussagen sind nun offensichtlich. □

Korollar 8.5.7. *Sei K ein Körper, $\mathrm{char}(K) = 0$ und $f \in K[X] \setminus K$.*

1. *Ist $\mathrm{gr}(f) \le 4$, so ist f über K auflösbar.*
2. *Sei $\mathrm{gr}(f) \ge 5$ und G die Galoisgruppe von f über K. Ist $G \cong \mathfrak{A}_n$ oder $G \cong \mathfrak{S}_n$, so ist f über K nicht auflösbar.*

Beweis. Nach Satz 8.5.6 und Korollar 7.5.3. □

Definition 8.5.8. Sei $n \in \mathbb{N}$. Eine Untergruppe $U < \mathfrak{S}_n$ heißt *transitiv*, wenn für alle $i, j \in [1,n]$ ein $\tau \in U$ existiert, so dass $\tau(i) = j$.

Beispiel 8.5.9. Sei $K = \mathbb{Q}$ und $f = X^5 - 4X + 2 \in \mathbb{Q}[X]$. Die Kurvendiskussion der von f induzierten Polynomfunktion $f_\mathbb{R}\colon \mathbb{R} \to \mathbb{R}$ zeigt:

$$f_\mathbb{R} \text{ hat lokale Extrema in } \pm\sqrt[4]{0.8} \text{ mit } f(\sqrt[4]{0.8}) < 0 \text{ und } f(-\sqrt[4]{0.8}) > 0\,.$$

Daher hat f in $\mathbb{C}$ ein Paar konjugiert-komplexer Nullstellen (α_1, α_2) (mit $\overline{\alpha}_1 = \alpha_2 \ne \alpha_1$) und drei reelle Nullstellen $\alpha_3, \alpha_4, \alpha_5 \in \mathbb{R}$. Sei $L = \mathbb{Q}(\alpha_1, \alpha_2, \alpha_3, \alpha_4, \alpha_5) \subset \mathbb{C}$ ein Zerfällungskörper von f über $\mathbb{Q}$, $G = \mathrm{Gal}(L/\mathbb{Q})$, $\boldsymbol{\alpha} = (\alpha_1, \ldots, \alpha_5) \in L^5$ und $\theta = \theta_{\boldsymbol{\alpha}}\colon G \to \mathfrak{S}_5$ der Monomorphismus aus Satz 8.5.6. Wegen $[\mathbb{Q}(\alpha_1):\mathbb{Q}] = 5\,|\,[L:\mathbb{Q}] = |G|$ gibt es nach Satz 7.4.2.4 ein $\sigma \in G$ mit $\mathrm{ord}(\sigma) = 5$, und dann ist $\theta(\sigma) \in \theta(G)$ ein 5-Zykel. Sei $\iota\colon \mathbb{C} \to \mathbb{C}$ die komplexe Konjugation, definiert durch $\iota(z) = \overline{z}$. Dann ist $\tau = \iota\,|\,L \in G$, $\tau(\alpha_1) = \alpha_2$, $\tau(\alpha_2) = \alpha_1$, und $\tau(\alpha_\nu) = \alpha_\nu$ für $\nu \in \{3,4,5\}$. Daher folgt $\theta(\tau) = (12) \in \theta(G)$. Sei $\theta(\sigma) = (1, k_2, k_3, k_4, k_5)$ und $2 = k_\nu$. Dann ist $\theta(\sigma)^{\nu-1} = (1, 2, k_3, k_4, k_5)$, wir können nach geeigneter Umnummerierung der Nullstellen $(k_3, k_4, k_5) = (3,4,5)$ annehmen und erhalten $\mathfrak{S}_5 = \langle (1,2)\,,\ (1,2,3,4,5)\rangle \subset \theta(G)$ nach Korollar 7.2.5, also $\theta(G) = \mathfrak{S}_5$. Daraus folgt:

Das Polynom $X^5 - 4X + 2$ ist über $\mathbb{Q}$ nicht auflösbar.

Mit etwas mehr Mühe zeigt man ([**?**, § 6.1, Satz 10]):
Ist $f \in \mathbb{Q}[X]$ irreduzibel und auflösbar und $\mathrm{gr}(f) \in \mathbb{P}$, so erhält man einen Zerfällungskörper von f über $\mathbb{Q}$ durch Akjunktion zweier beliebiger Nullstellen von f. Ist daher $\mathrm{gr}(f) \ge 5$ und besitzt f mindestens zwei reelle Nullstellen, so sind alle Nullstellen von f reell.

Satz 8.5.10. *Sei K ein Körper, $f \in K[X] \setminus K$ separabel, $n = \mathrm{gr}(f)$ und $\Gamma < \mathfrak{S}_n$ eine Realisierung der Galoisgruppe von f über K als Permutationsgruppe. Genau dann ist f irreduzibel über K, wenn Γ transitiv ist.*

Beweis. Sei N ein Zerfällungskörper von f über K, $G = \mathrm{Gal}(N/K)$, $\boldsymbol{\alpha} = (\alpha_1, \ldots, \alpha_n) \in N^n$ ein Nullstellenvektor von f und $\Gamma = \theta_{\boldsymbol{\alpha}}(G)$ (siehe Satz 8.5.6).

Sei zuerst f irreduzibel über K, und seien $i, j \in [1,n]$. Dann sind α_i und α_j konjugiert über K, und nach Korollar 6.5.3 gibt es ein $\sigma \in G$ mit $\sigma(\alpha_i) = \alpha_j$. Dann ist aber $\theta(\sigma)(i) = j$.

Sei nun Γ transitiv, sei $f = af_1 \cdot \dots \cdot f_r$ mit $a \in K^\times$ und normierten über K irreduziblen Polynomen $f_1, \dots, f_r \in K[X]$, und sei $r \geq 2$. Dann gibt es $i, j \in [1,n]$ mit $f_1(\alpha_i) = f_2(\alpha_j) = 0$, und es gibt ein $\sigma \in G$ mit $\theta(\sigma)(i) = j$. Dann ist aber $\sigma(\alpha_i) = \alpha_j$, also sind α_i und α_j konjugiert über K (nach Korollar 6.5.3), und es folgt $f_1 = f_2$ im Widerspruch zur Separabilität von f. □

Satz 8.5.11 (Die allgemeine Gleichung)**.** *Sei F ein Körper, $n \in \mathbb{N}$, $K = F(S_1, \dots, S_n)$ ein rationaler Funktionenkörper in den Unbestimmten $S_1, \dots, S_n$ über K und*

$$p = X^n + S_1 X^{n-1} + \dots + S_{n-1}X + S_n \in K[X]\,.$$

1. *p ist separabel und irreduzibel über K.*
2. *Die Galoisgruppe von p über F ist isomorph zu $\mathfrak{S}_n$.*
3. *Ist $n \geq 5$ und $\mathrm{char}(K) = 0$, so ist p über F nicht auflösbar.*

Beweis. Sei $F[X_1, \dots, X_n]$ ein Polynmomring in $(X_1, \dots, X_n)$ über F, und seien die elementarsymmetrischen Funktionen $\sigma_1, \dots, \sigma_n \in F[X_1, \dots, X_n]$ definiert durch

$$\sigma_i = \sum_{1 \leq \nu_1 < \dots < \nu_i \leq n} X_{\nu_1} \cdot \dots \cdot X_{\nu_i}\,,$$

also $\sigma_1 = X_1 + \dots + X_n$, $\sigma_2 = X_1X_2 + X_1X_3 + \dots + X_{n-1}X_n$, …, $\sigma_n = X_1 \cdot \dots \cdot X_n$.

Sei $E = F(T_1, \dots, T_n)$ ein rationaler Funktionenkörper in den (von $S_1, \dots, S_n$ verschiedenen) Unbestimmten $T_1, \dots, T_n$ über F. Für $\pi \in \mathfrak{S}_n$ sei $\pi^*\colon F[T_1, \dots, T_n] \to F[T_1, \dots, T_n]$ der eindeutig bestimmte Ringhomomorphismus mit $\pi^* \mid F = \mathrm{id}_F$ und $\pi^*(T_i) = T_{\pi(i)}$. Dann ist π^* ein Isomorphismus und besitzt eine eindeutige Fortsetzung zu einem Automorphismus $\widetilde{\pi} \in \mathrm{Aut}(E)$. Sei $G = \{\widetilde{\pi} \mid \pi \in \mathfrak{S}_n\} < \mathrm{Aut}(G)$. Nach Satz 8.1.3 ist E/E^G eine endlich galoissche Körpererweiterung, $\mathrm{Gal}(E/E^G) = G \cong \mathfrak{S}_n$, für alle $i \in [1,n]$ ist $s_i = (-1)^i\sigma_i(T_1, \dots, T_n) \in E^G$, und daher folgt $F(s_1, \dots, s_n) \subset E^G$. Es ist

$$P = \prod_{i=1}^{n}(X - T_i) = X^n + s_1X^{n-1} + \dots + s_{n-1}X + s_n \in F(s_1, \dots, s_n)[X]\,,$$

P ist separabel, und E ist ein Zerfällungskörper von P über $F(s_1, \dots, s_n)$. Daher folgt

$$n! = [E\colon E^G] \leq [E\colon F(s_1, \dots, s_n)] \leq n!\,, \quad \text{also} \quad E^G = F(s_1, \dots, s_n)\,,$$

und wegen $[E\colon E^G] = |G| = n!$ ist P irreduzibel.

Sei nun L ein Zerfällungskörper von p über K, und seien $t_1, \dots t_n \in L$ mit

$$p = \prod_{i=1}^{n}(X - t_i)\,, \quad \text{also} \quad S_i = (-1)^i\sigma_i(t_1, \dots, t_n) \quad \text{für alle } i \in [1,n] \quad \text{und} \quad L = K(t_1, \dots, t_n)\,.$$

Wegen $S_i \in F[t_1, \dots, t_n]$ folgt $L = F(t_1, \dots, t_n)$. Sei nun $\Phi\colon F[T_1, \dots, T_n] \to F[t_1, \dots, t_n]$ der eindeutig bestimmte Ringhomomorphismus mit $\Phi \mid F = \mathrm{id}_F$ und $\Phi(T_i) = t_i$ für alle $i \in [1,n]$. Dann ist Φ surjektiv, und für alle $i \in [1,n]$ ist $\Phi(s_i) = S_i$. Ist $g \in \mathrm{Ker}(\Phi)$, so folgt

$$\Phi\big(g(s_1, \dots, s_n)\big) = g\big(\Phi(s_1), \dots, \Phi(s_n)\big) = g(S_1, \dots, S_n) = 0 \quad \text{und daher} \quad g = 0\,.$$

Also ist Φ ein Isomorphismus und hat eine eindeutige Fortsetzung zu einem Isomorphismus $\widetilde{\Phi}\colon E \to L$. Wegen $\widetilde{\Phi} \mid F = \mathrm{id}_F$ und $\widetilde{\Phi}(s_i) = S_i$ ist $\phi = \widetilde{\Phi} \mid E^G\colon E^G \xrightarrow{\sim} K$ ein Isomorphismus. Ist $\phi_1\colon E^G[X] \to K[X]$ die Fortsetzung auf die Polynomringe, so folgt $\phi_1(P) = p$, also ist p irreduzibel und separabel, und $\widetilde{\Phi}$ induziert einen Gruppenisomorphismus $\mathrm{Gal}(E/E^G) \xrightarrow{\sim} \mathrm{Gal}(L/K)$. Daher ist auch die Galoisgruppe von p isomorph zu $\mathfrak{S}_n$.

Damit sind 1. und 2. bewiesen, und 3. folgt mit Korollar 8.5.7. □

8.6. Galoistheorie der Polynome 2., 3. und 4. Grades

Definition 8.6.1. Sei K ein Körper, $f \in K[X] \setminus K$ ein normiertes Polynom, $n = \mathrm{gr}(f)$, N ein Zerfällungskörper von f über K,

$$f = \prod_{\nu=1}^{n}(X-\alpha_\nu) \quad \text{mit} \quad a \in K^\times \quad \text{und} \quad \alpha_1,\ldots,\alpha_n \in N\,, \quad \text{uns sei} \quad \mathsf{d}(f) = \prod_{1\le\nu<\mu\le n}(\alpha_\nu-\alpha_\nu)^2\,.$$

Dann heißt $\mathsf{d}(f)$ die *Diskriminante* von f.

Satz 8.6.2. *Sei K ein Körper, $f \in K[X]\setminus K$ normiert und separabel, $\mathrm{gr}(f) = n \in \mathbb{N}$, N ein Zerfällungskörper von f über K und*

$$f = \prod_{\nu=1}^{n}(X-\alpha_\nu) \quad \textit{mit} \quad a \in K^\times \quad \textit{und} \quad \boldsymbol{\alpha} = (\alpha_1,\ldots,\alpha_n) \in N^n\,.$$

1. $\mathsf{d}(f) \in K^\times$.
2. *Im Falle* $\mathrm{char}(K) \neq 2$ *ist genau dann ist* $\mathsf{d}(f) \in K^2$, *wenn* $\mathrm{Gal}(f,\boldsymbol{\alpha}) \subset \mathfrak{A}_n$.

Beweis. Sei $\theta = \theta_{\boldsymbol{\alpha}}\colon G \xrightarrow{\sim} \mathrm{Gal}(f,\boldsymbol{\alpha}) < \mathfrak{S}_n$ und

$$\Delta = \prod_{1\le\nu\le\mu\le n}(\alpha_\mu-\alpha_\nu) = \det\begin{pmatrix} 1 & 1 & \ldots & 1 \\ \alpha_1 & \alpha_2 & \ldots & \alpha_n \\ \vdots & \vdots & & \vdots \\ \alpha_1^{n-1} & \alpha_2^{n-1} & \ldots & \alpha_n^{n-1} \end{pmatrix} \in N^\times\,.$$

Ist $\sigma \in G$, so folgt

$$\sigma(\Delta) = \det\bigl(\sigma(\alpha_\nu)^j\bigr)_{\substack{\nu=1,\ldots,n\\ j=0,\ldots,n-1}} = \det\bigl(\alpha^j_{\theta(\sigma)(\nu)}\bigr)_{\substack{\nu=1,\ldots,n\\ j=0,\ldots,n-1}} = \mathrm{sgn}(\theta(\sigma))\Delta\,,$$

also $\sigma(\Delta^2) = \Delta^2$, und $\sigma(\Delta) = \Delta$ genau dann, wenn $\theta(\sigma) \in \mathfrak{A}_n$. Wegen $\mathsf{d}(f) = \Delta^2$ ist $\sigma(\mathsf{d}(f)) = \mathsf{d}(f)$ für alle $\sigma \in G$, also $\mathsf{d}(f) \in K^\times$. Genau dann ist $\mathsf{d}(f) \in K^2$, wenn $\Delta \in K$, und das ist genau dann der Fall, wenn $\mathrm{Gal}(f,\boldsymbol{\alpha}) \subset \mathfrak{A}_n$. □

Bemerkung 8.6.3. Sei K ein Körper, $n \in \mathbb{N}$, $\mathrm{char}(K) \nmid n$, $f = X^n + a_{n-1}X^{n-1} + \ldots + a_0 \in K[X]$, N ein Zerfällungskörper von f über K,

$$f = \prod_{\nu=1}^{n}(X-\alpha_\nu) \quad \text{mit} \quad \boldsymbol{\alpha} = (\alpha_1,\ldots,\alpha_n) \in N^n\,, \quad G = \mathrm{Gal}(N/K) \ \text{ und } \ \theta = \theta_{\boldsymbol{\alpha}}\colon G \to \mathfrak{S}_n\,.$$

Für $\nu \in [1,n]$ sei

$$\beta_\nu = \alpha_\nu - \frac{a_{n-1}}{n}\,, \quad g = \prod_{\nu=1}^{n}(X-\beta_\nu) \quad \text{und} \quad \boldsymbol{\beta} = (\beta_1,\ldots,\beta_n)\,.$$

Dann folgt $g = X^n + b_{n-2}X^{n-2} + \ldots + b_0 \in K[X]$, N ist auch ein Zerfällungskörper von g über K, $\theta_{\boldsymbol{\alpha}} = \theta_{\boldsymbol{\beta}}$ und $\mathrm{Gal}(f,\boldsymbol{\alpha}) = \mathrm{Gal}(g,\boldsymbol{\beta})$.
Daher werden wir im folgenden stets $a_{n-1} = 0$ annehmen.

Polynome 2. Grades. Sei K ein Körper, $\mathrm{char}(K) \neq 2$, $p \in K$ und $f = X^2 + p \in K[X]$. Sei N ein Zerfällungskörper von f über K, $f = (X-\alpha_1)(X-\alpha_2)$ mit $\boldsymbol{\alpha} = (\alpha_1,\alpha_2) \in N^2$. Dann ist

$$\alpha_1+\alpha_2 = 0\,, \quad \alpha_1\alpha_2 = -\alpha_1^2 = p\,, \quad \alpha_1 = \sqrt{-p} \quad \text{und} \quad \mathsf{d}(f) = (\alpha_2-\alpha_1)^2 = (\alpha_1+\alpha_2)^2 - 4\alpha_1\alpha_2 = -4p\,.$$

Ist $-p \in K^2$, so folgt $N = K$ und $\mathrm{Gal}(f,\boldsymbol{\alpha}) = \mathfrak{A}_2 = \{(1)\}$, Ist $-p \notin K^2$, so folgt $[N:K] = 2$ und $\mathrm{Gal}(f,\boldsymbol{\alpha}) = \mathfrak{S}_2$.

Polynome 3. Grades. Sei K ein Körper, $\mathrm{char}(K) \notin \{2,3\}$ und $f = X^3 + pX + q \in K[X]$. Sei N ein Zerfällungskörper von f über K und

$$f = (X-\alpha_1)(X-\alpha_2)(X-\alpha_3) \quad \text{mit} \quad \boldsymbol{\alpha} = (\alpha_1,\alpha_2,\alpha_3) \in N^3\,.$$

Ist f nicht irreduzibel über K, so zerfällt f entweder in 3 Faktoren 1. Grades (dann ist $N = K$) oder in eine Faktor 1. Grades und eine Faktor 2. Grades (dann ist $[N:K] = 2$). Sei also im Folgenden f irreduzibel über K, $G = \mathrm{Gal}(N/K)$ und $\theta = \theta_{\boldsymbol{\alpha}} \colon G \xrightarrow{\sim} \Gamma = \mathrm{Gal}(f,\boldsymbol{\alpha}) \subset \mathfrak{S}_3$. Dann ist Γ transitiv und daher $\Gamma \in \{\mathfrak{S}_3, \mathfrak{A}_3\}$ nach Beispiel 7.2.8.

Es ist

$$\alpha_1+\alpha_2+\alpha_3 = 0\,, \quad \alpha_1\alpha_2+\alpha_1\alpha_3+\alpha_2\alpha_3 = p\,, \quad \alpha_1\alpha_2\alpha_3 = -q\,,$$

und

$$\mathsf{d}(f) = \det\begin{pmatrix} 1 & 1 & 1 \\ \alpha_1 & \alpha_2 & \alpha_3 \\ \alpha_1^2 & \alpha_2^2 & \alpha_3^2 \end{pmatrix}^2 = \det\begin{pmatrix} 1 & 1 & 1 \\ \alpha_1 & \alpha_2 & \alpha_3 \\ \alpha_1^2 & \alpha_2^2 & \alpha_3^2 \end{pmatrix}\begin{pmatrix} 1 & \alpha_1 & \alpha_1^2 \\ 1 & \alpha_2 & \alpha_2^2 \\ 1 & \alpha_3 & \alpha_3^2 \end{pmatrix} = \det\begin{pmatrix} s_0 & s_1 & s_2 \\ s_1 & s_2 & s_3 \\ s_2 & s_3 & s_4 \end{pmatrix}$$

mit $s_\nu = \alpha_1^\nu + \alpha_2^\nu + \alpha_3^\nu$ für $\nu \in [1,4]$. Wegen $s_1 = 0$ folgt

$$0 = s_1^2 = \alpha_1^2+\alpha_2^2+\alpha_3^2+2(\alpha_1\alpha_2+\alpha_1\alpha_3+\alpha_2\alpha_3) = s_2+2p \quad \text{und daher} \quad s_2 = -2p\,,$$

ferner

$$\begin{aligned} 0 = s_1^3 &= \alpha_1^3+\alpha_2^3+\alpha_3^3+3(\alpha_1^2\alpha_2+\alpha_1^2\alpha_3+\alpha_1\alpha_2^2+\alpha_2^2\alpha_3+\alpha_1\alpha_3^2+\alpha_2\alpha_3^2)+6\alpha_1\alpha_2\alpha_3 \\ &= s_3+3[(\alpha_1^2+\alpha_2^2+\alpha_3^2)(\alpha_1+\alpha_2+\alpha_3)-s_3]-6q = -2s_3-6q \quad \text{und daher} \quad s_3 = -3q\,, \end{aligned}$$

und schließlich

$$\begin{aligned} s_4 = {} & (\alpha_1^3+\alpha_2^3+\alpha_3^3)(\alpha_1+\alpha_2+\alpha_3)-(\alpha_1^2+\alpha_2^2+\alpha_3^2)(\alpha_1\alpha_2+\alpha_1\alpha_3+\alpha_2\alpha_3) \\ & +(\alpha_1+\alpha_2+\alpha_3)\alpha_1\alpha_2\alpha_3 = -s_2p = 2p^2\,. \end{aligned}$$

Damit folgt

$$\mathsf{d}(f) = \det\begin{pmatrix} 3 & 0 & -2p \\ 0 & -2p & -3q \\ -2p & -3q & 2p^2 \end{pmatrix} = -4p^3-27q^2\,,$$

also $\Gamma = \mathfrak{A}_3$, falls $-4p^3-27q^2 \in K^2$, und $\Gamma = \mathfrak{S}_3$ sonst.

Sei $L_0 = K(\sqrt{\mathsf{d}(f)}) \subset N$. Dann ist N auch Zerfällungskörper von f über L_0. Wegen $[L:K] \in \{3,6\}$ ist $[N:L_0] = 3$, f ist irreduzibel über L_0 und N/L_0 ist zyklisch. Sei $\overline{N}$ ein Zerfällungskörper von X^3-1 über N. Dann ist

$$\mu_3(\overline{N}) = \{1,\zeta,\zeta^2\} \quad \text{mit} \quad \zeta = \frac{-1+\sqrt{-3}}{2}\,.$$

Setzt man $\overline{L}_0 = L_0(\zeta)$, so folgt $\mathrm{Gal}(\overline{N}/\overline{L}_0) \cong \mathrm{Gal}(N/L_0)$ nach Korollar 8.1.8, und wir suchen eine Erzeugung von $\overline{N}/\overline{L}$ gemaäß Satz 8.5.3. Sei $\sigma \in \mathrm{Gal}(\overline{N}/\overline{L}_0)$ mit $\theta(\sigma \,|\, N) = (123) \in \mathfrak{A}_3 \subset \Gamma$. Dann ist $\sigma(\alpha_1) = \alpha_2$, $\sigma(\alpha_2) = \alpha_3$ und $\sigma(\alpha_3) = \alpha_1$. Wir machen nun den Ansatz

$$\begin{aligned} u &= (1+\zeta\sigma+\zeta^2\sigma^2)(\alpha_1) = \alpha_1+\zeta\alpha_2+\zeta^2\alpha_3 \in N\,, \\ v &= (1+\zeta^2\sigma+\zeta\sigma^2)(\alpha_1) = \alpha_1+\zeta^2\alpha_2+\zeta\alpha_3 \in N\,, \end{aligned}$$

und erhalten

$$\begin{aligned} u^3 &= \alpha_1^3+\alpha_2^3+\alpha_3^3+6\alpha_1\alpha_2\alpha_3+3\zeta\alpha_1^2\alpha_2+3\zeta^2\alpha_1^2\alpha_3+3\zeta^2\alpha_1\alpha_2^2+3\zeta\alpha_1\alpha_3^2+3\zeta^2\alpha_2\alpha_3^2+3\zeta\alpha_2^2\alpha_3 \in \overline{L}_0\,, \\ v^3 &= \alpha_1^3+\alpha_2^3+\alpha_3^3+6\alpha_1\alpha_2\alpha_3+3\zeta^2\alpha_1^2\alpha_2+3\zeta\alpha_1^2\alpha_3+3\zeta\alpha_1\alpha_2^2+3\zeta^2\alpha_1\alpha_3^2+3\zeta\alpha_2\alpha_3^2+3\zeta^2\alpha_2^2\alpha_3 \in \overline{L}_0\,, \end{aligned}$$

also wegen $1+\zeta+\zeta^2 = 0$

$$u^3+v^3 = -27q\,, \quad uv = -3p \quad \text{und} \quad (X-u^3)(X-v^3) = X^2+27qX-27p^3\,.$$

Durch Auflösen der quadratischen Gleichung folgt

$$u^3, v^3 = -\frac{27q}{2} \pm \sqrt{\frac{729q^2}{4} + 27p^3} = 27\left(-\frac{q}{2} \pm \sqrt{\frac{-\mathsf{d}(f)}{108}}\right).$$

Wegen

$$u+v = 2\alpha_1 + (\zeta+\zeta^2)\alpha_2 + (\zeta+\zeta^2)\alpha_3 + (\alpha_1+\alpha_2+\alpha_3) = 3\alpha_1\,, \quad u+\zeta v = 3\alpha_2 \quad \text{und} \quad u+\zeta^2 v = 3\alpha_3$$

folgt

$$\alpha_1 = \frac{1}{3}(u+v)\,,\ \alpha_2 = \frac{1}{3}(u+\zeta v)\,,\ \alpha_3 = \frac{1}{3}(u+\zeta^2 v)\,.$$

Man schreibt die Lösungsformel auch als

$$\alpha_1 = \sqrt[3]{-\frac{q}{2} + \sqrt{\frac{-\mathsf{d}(f)}{108}}} + \sqrt[3]{-\frac{q}{2} - \sqrt{\frac{-\mathsf{d}(f)}{108}}}\,,$$

hat dabei aber zu beachten, dass die dritten Wurzeln nicht unabhängig von einander gewählt werden dürfen, es ist

$$\sqrt[3]{-\frac{q}{2} + \sqrt{\frac{-\mathsf{d}(f)}{108}}} \cdot \sqrt[3]{-\frac{q}{2} - \sqrt{\frac{-\mathsf{d}(f)}{108}}} = uv = -3p\,.$$

Im Spezialfall $K=\mathbb{Q}$ ist $D>0$, falls $\{\alpha_1,\alpha_2,\alpha_3\}\subset\mathbb{R}$, und $D<0$ sonst. Im Falle $\{\alpha_1,\alpha_2,\alpha_3\}\subset\mathbb{R}$ kommt in der Lösungsformel die imaginäre Zahl

$$\sqrt{\frac{-\mathsf{d}(f)}{108}} = \frac{1}{18}\sqrt{-3\mathsf{d}(f)} \in \overline{N}$$

vor.

Polynome 4. Grades. Sei K ein Körper, $\mathrm{char}(K)\notin\{2,3\}$, und sei

$$f = X^4 + bX^2 + cX + d \in K[X]$$

irreduzibel über K. Sei N ein Zerfällungskörper von f über K,

$$f = \prod_{\nu=1}^{4}(X-\alpha_\nu) \quad \text{mit} \quad \boldsymbol{\alpha} = (\alpha_1,\alpha_2,\alpha_3,\alpha_4) \in N^4$$

$G = \mathrm{Gal}(N/K)$ und $\theta = \theta_{\boldsymbol{\alpha}}\colon G \xrightarrow{\sim} \Gamma = \mathrm{Gal}(f,\boldsymbol{\alpha}) < \mathfrak{S}_4$. Dann ist Γ transitiv nach Satz 8.5.10. Nach Beispiel 7.2.9 ist (nach geeigneter Umnummerierung der Nullstellen) $\Gamma \in \{C,\ D_4,\ \mathfrak{V}_4,\ \mathfrak{A}_4,\ \mathfrak{S}_4\}$. Es ist

$$\begin{aligned}
\alpha_1+\alpha_2+\alpha_3+\alpha_4 &= 0\,,\\
\alpha_1\alpha_2+\alpha_1\alpha_3+\alpha_1\alpha_4+\alpha_2\alpha_3+\alpha_2\alpha_4+\alpha_3\alpha_4 &= b\,,\\
\alpha_1\alpha_2\alpha_3+\alpha_1\alpha_2\alpha_4+\alpha_1\alpha_3\alpha_4+\alpha_2\alpha_3\alpha_4 &= -c\,,\\
\alpha_1\alpha_2\alpha_3\alpha_4 &= d\,,
\end{aligned}$$

und wir setzen

$$\beta_1 = \alpha_1\alpha_2+\alpha_3\alpha_4\,, \quad \beta_2 = \alpha_1\alpha_3+\alpha_2\alpha_4\,, \quad \beta_3 = \alpha_1\alpha_4+\alpha_2\alpha_3\,, \quad \text{und} \quad \overline{K} = K(\beta_1,\beta_2,\beta_3)\subset N\,.$$

Dann folgt

$$\beta_1-\beta_2 = (\alpha_1-\alpha_4)(\alpha_2-\alpha_3)\neq 0\,, \quad \beta_1-\beta_3 = (\alpha_1-\alpha_3)(\alpha_2-\alpha_4)\neq 0\,, \quad \beta_2-\beta_3 = (\alpha_1-\alpha_2)(\alpha_3-\alpha_4)\neq 0\,,$$

und wir zeigen $\mathrm{Gal}(N/\overline{K}) = \theta^{-1}(\mathfrak{V}_4)$.

Offensichtlich ist $\theta^{-1}(\mathfrak{V}_4)\subset\mathrm{Gal}(N/\overline{K})$, also $\Gamma\cap\mathfrak{V}_4\subset\theta(\mathrm{Gal}(N/\overline{K}))$, und wir nehmen an, die Inklusion sei echt. Wegen

$$\Gamma\cap\mathfrak{V}_4 = \begin{cases} \langle(1,3)(2,4)\rangle\,, & \text{falls} \quad \Gamma = C\,,\\ \mathfrak{V}_4 & \text{sonst} \end{cases} \qquad \text{folgt} \quad (1,2,3,4)\in\Gamma \quad \text{oder} \quad (1,2,3)\in\Gamma.$$

Ist $\sigma \in G$ mit $\theta(\sigma) = (1,2,3,4)$, so folgt $\sigma(\beta_1) = \alpha_2\alpha_3 + \alpha_4\alpha_1 = \beta_3 \neq \beta_1$. Ist $\sigma \in G$ mit $\theta(\sigma) = (1,2,3)$, so folgt $\sigma(\beta_1) = \alpha_2\alpha_3 + \alpha_1\alpha_4 = \beta_3 \neq \beta_1$. Also ist in beiden Fällen $\sigma \notin \mathrm{Gal}(N/\overline{K})$.

Man erhält nun durch einfache Rechnung

$$g = (X - \beta_1)(X - \beta_2)(X - \beta_3) = X^3 - bX^2 + 4dX + (4bd - c^2),$$

also $g \in K[X]$ und $\mathsf{d}(g) = \mathsf{d}(f)$. Man nennt g eine *kubische Resolvente* von f. $\beta_1, \beta_2, \beta_3$ sind durch Radikale ausdrückbar, und es verbleibt die Aufgabe, $\alpha_1, \alpha_2, \alpha_3, \alpha_4$ aus $\beta_1, \beta_2, \beta_3$ auszurechnen. Setzt man

$$\gamma_1 = \alpha_1 + \alpha_2 - \alpha_3 - \alpha_4, \quad \gamma_2 = \alpha_1 - \alpha_2 + \alpha_3 - \alpha_4 \text{ und } \gamma_3 = \alpha_1 - \alpha_2 - \alpha_3 + \alpha_4,$$

so folgen wegen $\alpha_1 + \alpha_2 + \alpha_3 + \alpha_4 = 0$ die Gleichungen

$$\alpha_1 = \frac{1}{4}(\gamma_1 + \gamma_2 + \gamma_3), \quad \alpha_2 = \frac{1}{4}(\gamma_1 - \gamma_2 - \gamma_3), \quad \alpha_3 = \frac{1}{4}(-\gamma_1 + \gamma_2 - \gamma_3), \quad \alpha_4 = \frac{1}{4}(-\gamma_1 - \gamma_2 + \gamma_3),$$

und

$$\gamma_1^2 = -4(\beta_2 + \beta_3), \quad \gamma_2^2 = -4(\beta_1 + \beta_3), \quad \gamma_3^2 = -4(\beta_1 + \beta_2) \text{ und } \gamma_1\gamma_2\gamma_3 = -8c.$$

Die letzte Gleichung ist wieder eine Normierungsbedingung für die drei Quadratwurzeln, mittels derer man $\alpha_1, \alpha_2, \alpha_3, \alpha_4$ aus $\beta_1, \beta_2, \beta_3$ berechnet.

Bibliography