

# Kurzskript Algebra

Immi Halupczok

29. Juni 2022

## Inhaltsverzeichnis

<b>Algebra</b>	<b>3</b>
<b>1 Gruppen</b>	<b>3</b>
1.1 Gruppen und Untergruppen . . . . .	3
1.2 Gruppenhomomorphismen . . . . .	5
1.3 Nebenklassen, Quotienten und der Isomorphiesatz . . . . .	6
1.4 Zyklische Gruppen und der chinesische Restsatz . . . . .	7
1.5 Endlich erzeugte abelsche Gruppen . . . . .	8
1.6 Die symmetrischen und alternierenden Gruppen . . . . .	9
1.7 Operationen von Gruppen auf Mengen . . . . .	10
1.8 $p$ -Gruppen und die Sylow-Sätze . . . . .	11
<b>2 Ringe</b>	<b>12</b>
2.1 Ringe und Unterringe . . . . .	12
2.2 Ringhomomorphismen und der Isomorphiesatz . . . . .	13
2.3 Mehr zu Idealen . . . . .	14
2.4 Nullteilerfreie Ringe . . . . .	15
2.5 Hauptidealringe und faktorielle Ringe . . . . .	15
2.6 Polynomringe . . . . .	16
<b>3 Körper</b>	<b>17</b>
3.1 Körpererweiterungen . . . . .	17
3.2 Adjunktion von Elementen . . . . .	18
3.3 Anwendung: Konstruktion mit Zirkel und Lineal . . . . .	19
3.4 Algebraische Körpererweiterungen . . . . .	20
3.5 Normale Körpererweiterungen . . . . .	21

3.6	Separable Körpererweiterungen . . . . .	22
3.7	Galois-Theorie . . . . .	22

# Algebra

**Konvention 0.0.1** (a) Wir fassen 0 als natürliche Zahl auf:  $\mathbb{N} = \{0, 1, 2, \dots\}$   
(b) Ist  $K$  ein Körper, so setzen wir  $K^\times := K \setminus \{0\}$

## 1 Gruppen

### 1.1 Gruppen und Untergruppen

**Definition 1.1.1** (a) Eine **Gruppe** ist eine Menge  $G$  mit einer Verknüpfung  $\circ: G \times G \rightarrow G$ , so dass folgendes gilt:  
(i)  $\circ$  ist **assoziativ**:  $\forall a, b, c \in G: a \circ (b \circ c) = (a \circ b) \circ c$   
(ii) Es existiert ein **neutrales Element**  $e \in G$ , d. h. es gilt:  $\forall a \in G: a \circ e = e \circ a = a$   
(iii) Jedes Element besitzt ein **Inverses**:  $\forall a \in G: \exists b \in G: a \circ b = b \circ a = e$ .  
(b) Man sagt auch: „ $(G, \circ)$  ist eine Gruppe“; und: „ $\circ$  ist eine Gruppenstruktur auf  $G$ “.  
(c) Eine Gruppe  $G$  heißt **abelsch** oder **kommutativ**, wenn außerdem gilt:  $\forall a, b \in G: a \circ b = b \circ a$ .

**Bemerkung 1.1.2** Das neutrale Element und die inversen Elemente sind eindeutig.

**Notation 1.1.3** Es gibt mehrere verschiedene typische Notationen für Gruppen; im Folgenden sind  $a, b$  Gruppenelemente und  $n \in \mathbb{N} \setminus \{0\}$ :

- (a) **Multiplikative Notation**: Verknüpfung:  $a \cdot b$  (oder  $ab$ ); neutrales Element:  $1$  oder  $e$ ; Inverses von  $a$ :  $a^{-1}$ . Wir definieren auch  $\frac{a}{b} := a \cdot b^{-1}$ ,  $a^0 := e$ ,  $a^n := \underbrace{a \cdots a}_{n \text{ mal}}$ ,  $a^{-n} := (a^{-1})^n$
- (b) **Additive Notation**: Verknüpfung:  $a + b$ ; neutrales Element:  $0$ ; Inverses von  $a$ :  $-a$ . Wir definieren auch  $a - b := a + (-b)$ ,  $0 \cdot a := 0$ ,  $n \cdot a := \underbrace{a + \cdots + a}_{n \text{ mal}}$ ,  $(-n) \cdot a := n \cdot (-a)$

Wenn nicht anders angegeben, verwenden wir (meistens) die multiplikative Notation.

Die additive Notation verwendet man nur bei abelschen Gruppen.

**Beispiel 1.1.4** (a)  $(\mathbb{Z}, +)$  ist eine abelsche Gruppe.  
(b) Ist  $K$  ein Körper, so sind  $(K, +)$  und  $(K^\times, \cdot)$  abelsche Gruppen.  
(c) Ist außerdem  $V$  ein  $K$ -Vektorraum, so ist  $(V, +)$  eine abelsche Gruppe.  
(d) Die Menge

$$\mathrm{GL}_n(K) := \{A \in K^{n \times n} \mid \det A \neq 0\}$$

der invertierbaren  $n \times n$ -Matrizen über  $K$  ist eine Gruppe mit Matrixmultiplikation als Verknüpfung. (GL = general linear group = **allgemeine lineare Gruppe**.)

Wenn wir in Zukunft eine der obigen Mengen ( $\mathbb{Z}$ ,  $K$ ,  $K^\times$ ,  $V$ ,  $GL_n(K)$ ) als Gruppe bezeichnen, dann ist immer die obige Verknüpfung gemeint.

**Beispiel 1.1.5** Ist  $M$  eine Menge, so definiert man die **symmetrische Gruppe** als

$$\text{Sym}(M) := \{f: M \rightarrow M \mid f \text{ ist bijektiv}\},$$

mit der Verkettung von Abbildungen als Verknüpfung. Das neutrale Element ist die Identitätsabbildung  $\text{id}_M$ ; das inverse Element zu  $f \in \text{Sym}(M)$  ist die inverse Abbildung. Elemente von  $\text{Sym}(M)$  nennt man auch **Permutationen** von  $M$ .

Wir setzen auch:  $S_n := \text{Sym}(\{1, \dots, n\})$ .

**Definition 1.1.6** Seien  $G$  und  $H$  Gruppen. Das (**direkte**) **Produkt** von  $G$  und  $H$  ist die Gruppe  $G \times H$  mit der komponentenweiser Verknüpfung:

$$(a, b) \cdot (a', b') := (aa', bb')$$

für  $a, a' \in G$ ,  $b, b' \in H$ .

**Lemma 1.1.7** Sei  $G$  eine Gruppe, und seien  $a, b \in G$ .

- (a) Wenn ein  $c \in G$  existiert mit  $ac = bc$  (oder  $ca = cb$ ), so gilt  $a = b$ .
- (b) Es gibt ein  $d \in G$  mit  $a = db$ .
- (c) Es gilt  $(ab)^{-1} = b^{-1}a^{-1}$ .
- (d) Für beliebige  $m, n \in \mathbb{Z}$  gilt:  $a^m \cdot a^n = a^{m+n}$ .
- (e) Gilt  $ab = e$ , so ist  $a$  das Inverse von  $b$  und  $b$  das Inverse von  $a$ .
- (f) Es gilt  $(a^{-1})^{-1} = a$ .

**Definition 1.1.8** Sei  $G$  eine Gruppe. Eine **Untergruppe** von  $G$  ist eine Teilmenge  $H \subseteq G$  mit folgenden Eigenschaften:

- (a)  $e \in H$
- (b) Sind  $a, b \in H$  Elemente von  $H$ , so sind auch  $a \cdot b$  und  $a^{-1}$  Elemente von  $H$ .

**Lemma 1.1.9** Sei  $(G, \circ)$  eine Gruppe und  $H \subseteq G$  eine Teilmenge. Folgende Bedingungen sind äquivalent:

- (a)  $H$  ist eine Untergruppe von  $G$ .
- (b) Die Einschränkung  $\circ|_{H \times H}$  definiert eine Gruppenstruktur auf  $H$ .
- (c)  $H$  ist nicht leer, und für alle  $a, b \in H$  gilt:  $a \cdot b^{-1} \in H$ .

**Beispiel 1.1.10** Ist  $G$  eine beliebige Gruppe, so sind  $G$  selbst und  $\{e\}$  Untergruppen von  $G$ . ( $\{e\}$  nennt man die **triviale Untergruppe**.)

**Satz 1.1.11** Die Untergruppen von  $\mathbb{Z}$  sind genau die Teilmengen der Form  $n\mathbb{Z} = \{nk \mid k \in \mathbb{Z}\}$ , für ein  $n \in \mathbb{N}$ . (Im Fall  $n = 0$  ist  $n\mathbb{Z} = \{0\}$ .)

**Lemma 1.1.12** Ist  $G$  eine Gruppe und  $A \subseteq G$  eine beliebige Teilmenge, so existiert unter allen Untergruppen von  $G$ , die  $A$  enthalten, eine kleinste.

Zur Erinnerung: Ist  $\mathcal{M}$  eine Menge von Mengen, so nennt man  $A \in \mathcal{M}$  die **kleinste Menge** von  $\mathcal{M}$ , wenn jede Menge  $B \in \mathcal{M}$  eine Obermenge von  $A$  ist. (Eine kleinste Menge muss nicht immer existieren, aber wenn sie existiert, ist sie eindeutig.)

**Definition 1.1.13** Sei  $G$  eine Gruppe.

- (a) Ist  $A \subseteq G$  eine beliebige Teilmenge, so nennt man die kleinste Untergruppe von  $G$ , die  $A$  enthält, die von  $A$  **erzeugte Untergruppe**. Notation für diese Untergruppe:  $\langle A \rangle$ . Sind  $a_i$  Elemente von  $G$ , für  $i \in I$ , so schreibt man statt  $\{a_i \mid i \in I\}$  auch  $\langle a_i \mid i \in I \rangle$ , und statt  $\langle a_i \mid i \in \{1, \dots, n\} \rangle$  schreibt man auch  $\langle a_1, \dots, a_n \rangle$ .
- (b) Gilt  $\langle A \rangle = G$ , so sagt man, die Elemente von  $A$  sind **Erzeuger** von  $G$ ; und:  $G$  wird von (den Elementen von)  $A$  **erzeugt**.
- (c) Wird  $G$  von einer endlichen Menge erzeugt, so nennt man  $G$  **endlich erzeugt**. Wird  $G$  von einer ein-elementigen Menge erzeugt, so nennt man  $G$  **zyklisch**.

**Beispiel 1.1.14** Ist  $G$  eine Gruppe und  $a \in G$ , so ist  $\langle a \rangle = \{a^n \mid n \in \mathbb{Z}\}$ .

**Satz 1.1.15** Ist  $G$  abelsch und sind  $a_1, \dots, a_n \in G$ , so ist

$$\langle a_1, \dots, a_n \rangle = \{a_1^{r_1} \cdots a_n^{r_n} \mid r_1, \dots, r_n \in \mathbb{Z}\}.$$

## 1.2 Gruppenhomomorphismen

**Definition 1.2.1** Seien  $G$  und  $H$  Gruppen.

- (a) Ein (**Gruppen-)****Homomorphismus** ist eine Abbildung  $f: G \rightarrow H$ , für die gilt:

$$\forall a, b \in G: f(ab) = f(a)f(b).$$

$\text{Hom}(G, H)$  bezeichnet die Menge aller Gruppenhomomorphismen von  $G$  nach  $H$ .

- (b) Das **Bild** von  $f$  ist  $\text{im } f := \{f(a) \mid a \in G\}$ ; der **Kern** von  $f$  ist  $\ker f := \{a \in G \mid f(a) = e\}$ .
- (c) Ein **Isomorphismus von Gruppen** ist ein bijektiver Gruppenhomomorphismus. Zwei Gruppen  $G$  und  $H$  heißen **isomorph** (Notation:  $G \cong H$ ), ein Isomorphismus  $G \rightarrow H$  existiert.
- (d) Ein **Endomorphismus** einer Gruppe  $G$  ist ein Homomorphismus von  $G$  nach  $G$ . Die Menge der Endomorphismen von  $G$  wird mit  $\text{End}(G)$  bezeichnet.
- (e) Ein **Automorphismus** einer Gruppe  $G$  ist ein Isomorphismus von  $G$  nach  $G$ . Die Menge der Automorphismen von  $G$  wird mit  $\text{Aut}(G)$  bezeichnet.

**Bemerkung 1.2.2** Ist  $f: G \rightarrow H$  ein Gruppenhomomorphismus, so gilt  $f(e) = e$ , und für  $a \in G$  gilt  $f(a^{-1}) = f(a)^{-1}$ .

**Bemerkung 1.2.3** Die Verknüpfung von zwei Gruppenhomomorphismen ist wieder ein Gruppenhomomorphismus, und das Inverse eines Gruppenisomorphismusses ist ein Gruppenisomorphismus. Insbesondere ist  $\text{Aut}(G)$  eine Untergruppe von  $\text{Sym}(G)$ .

**Beispiel 1.2.4** Ist  $G$  eine Gruppe und  $a \in G$ , so ist  $\mathbb{Z} \rightarrow G, n \mapsto a^n$  ein Gruppenhomomorphismus. Das Bild davon ist  $\langle a \rangle$ .

**Beispiel 1.2.5** Ist  $G$  eine Gruppe und  $a \in G$  ein fest gewähltes Element, so ist  $G \rightarrow G, x \mapsto axa^{-1}$  ein Automorphismus von  $G$ . (Diese Abbildung nennt man die **Konjugation** mit  $a$ .)

**Lemma 1.2.6** Ist  $f: G \rightarrow H$  ein Gruppenhomomorphismus (insbesondere seien  $G, H$  Gruppen) so ist  $\text{im } f$  eine Untergruppe von  $H$ . Allgemeiner gilt: Ist  $G' \subseteq G$  eine Untergruppe, so ist  $f(G')$  eine Untergruppe von  $H$ . Außerdem: Wird  $G'$  von  $A \subseteq G$  erzeugt, so wird  $f(G')$  von  $f(A)$  erzeugt.

**Definition 1.2.7** Ein **Normalteiler** (auch: **normale Untergruppe**) von  $G$  ist eine Untergruppe  $N \subseteq G$ , für die gilt: Für alle  $a \in N$  und alle  $b \in G$  gilt  $bab^{-1} \in N$ . Die Notation „ $N \triangleleft G$ “ bedeutet:  $N$  ist ein Normalteiler von  $G$ .

**Bemerkung 1.2.8** (a) Für beliebige Gruppen  $G$  sind sowohl  $G$  als auch  $\{e\}$  Normalteiler von  $G$ .  
 (b) Ist  $G$  abelsch, so ist jede Untergruppe von  $G$  bereits ein Normalteiler von  $G$ .

**Lemma 1.2.9** Sind  $G$  und  $H$  Gruppen und ist  $f: G \rightarrow H$  ein Gruppenhomomorphismus, so ist  $\ker f$  ein Normalteiler von  $G$ . Allgemeiner gilt: Ist  $H' \subseteq H$  eine Untergruppe bzw. ein Normalteiler von  $H$ , so ist  $f^{-1}(H')$  eine Untergruppe bzw. ein Normalteiler von  $G$ .

**Bemerkung 1.2.10** Eine Untergruppe  $H \subseteq G$  ist ein Normalteiler genau dann, wenn sie für jedes  $a \in G$  durch Konjugation mit  $a$  auf sich selbst abgebildet wird, d. h. wenn  $aHa^{-1} = H$  gilt für alle  $a \in G$ .

### 1.3 Nebenklassen, Quotienten und der Isomorphiesatz

**Definition 1.3.1** Sei  $G$  eine Gruppe und  $H \subseteq G$  eine Untergruppe.

- (a) Eine **Linksnebenklasse** von  $H$  ist eine Menge der Form  $aH := \{ah \mid h \in H\}$  für  $a \in G$ . Die Menge aller Linksnebenklassen von  $H$  wird mit  $G/H$  bezeichnet.
- (b) Eine **Rechtsnebenklasse** von  $H$  ist eine Menge der Form  $Ha := \{ha \mid h \in H\}$  für  $a \in G$ . Die Menge aller Rechtsnebenklassen von  $H$  wird mit  $H \backslash G$  bezeichnet.

**Lemma 1.3.2** Ist  $G$  eine Gruppe und  $N \triangleleft G$  ein Normalteiler und  $a \in G$ , so gilt  $aN = Na$ . Insbesondere sind Linksnebenklassen das gleiche wie Rechtsnebenklassen, und man spricht einfach von **Nebenklassen**.

Bemerkung: Wenn wir additive Notation verwenden, schreiben wir Nebenklassen als  $a + H = \{a + h \mid h \in H\}$ .

**Lemma 1.3.3** Sei  $G$  eine Gruppe und  $H \subseteq G$  eine Untergruppe.

- (a) Die Menge der Linksnebenklassen von  $H$  bildet eine Partition von  $G$ , d. h. jedes Element  $a \in G$  liegt in genau einer Linksnebenklasse, nämlich  $a \in aH$ .
- (b) Zwei Elemente  $a, b \in G$  liegen in der gleichen Linksnebenklasse von  $H$  genau dann, wenn  $a^{-1}b \in H$  gilt.
- (c) Jede Linksnebenklasse von  $H$  hat die gleiche Kardinalität wie  $H$  (d. h. für beliebige  $a \in G$  gilt:  $\#(aH) = \#H$ ).

Analoge Aussagen gelten für Rechtsnebenklassen.

**Definition 1.3.4** Sei  $G$  eine Gruppe.

- (a) Statt „Kardinalität von  $G$ “ sagt man auch **Ordnung** von  $G$ . (Als Notation verwendet man trotzdem  $\#G$ .)
- (b) Der **Index** einer Untergruppe  $H \subseteq G$  ist definiert durch  $(G : H) := \#(G/H) \in \mathbb{N} \cup \{\infty\}$ . (Manche Leute schreiben auch  $[G : H]$  für den Index von  $H$  in  $G$ .)

**Satz 1.3.5 (Satz von Lagrange)** Ist  $G$  eine Gruppe und  $H \subseteq G$  eine Untergruppe, so gilt  $\#G = \#H \cdot (G : H)$ .

**Bemerkung 1.3.6** Ist  $f: G \rightarrow H$  ein Gruppenhomomorphismus mit Kern  $N \triangleleft G$  und sind  $a, b \in G$ , so gilt  $f(a) = f(b)$  genau dann wenn  $aN = bN$ . Insbesondere ist  $f$  injektiv genau dann, wenn  $\ker f = \{e\}$  ist.

**Satz 1.3.7** Ist  $G$  eine Gruppe und  $N \triangleleft G$  ein Normalteiler, so wird durch  $(aN) \cdot (bN) := (ab)N$  (für  $a, b \in G$ ) eine Verknüpfung auf  $G/N$  definiert;  $G/N$  ist mit dieser Verknüpfung eine Gruppe, und die Abbildung  $G \rightarrow G/N, a \mapsto aN$  ist ein surjektiver Gruppenhomomorphismus mit Kern  $N$ .

**Definition 1.3.8** Die Gruppe  $G/N$  („ $G$  modulo  $N$ “) aus dem vorigen Satz wird **Quotientengruppe** (oder manchmal auch **Faktorgruppe**) genannt.

**Notation 1.3.9** Ist  $G$  eine Gruppe,  $N \triangleleft G$  und  $a \in G$ , so schreiben wir für die Nebenklasse  $aN \in G/N$  manchmal auch  $\bar{a}$ .

**Beispiel 1.3.10** Für  $n \geq 1$  ist  $\mathbb{Z}/n\mathbb{Z} = \{\bar{0}, \bar{1}, \dots, \overline{n-1}\}$ .

**Satz 1.3.11 (Isomorphiesatz)** Seien  $G$  und  $H$  Gruppen und  $f: G \rightarrow H$  ein Homomorphismus. Dann erhalten wir einen Isomorphismus  $\tilde{f}: G/\ker f \rightarrow \text{im } f$ , so dass für alle  $a \in G$  gilt:  $\tilde{f}(\bar{a}) = f(a)$ .

## 1.4 Zyklische Gruppen und der chinesische Restsatz

**Satz 1.4.1** Ist  $G$  eine zyklische Gruppe, so existiert ein  $n$ , so dass  $G$  isomorph zu  $\mathbb{Z}/n\mathbb{Z}$  ist. Genauer: Ist  $a \in G$  ein Erzeuger von  $G$ , so wird durch  $\bar{m} \mapsto a^m$  ein Isomorphismus von  $\mathbb{Z}/n\mathbb{Z}$  nach  $G$  definiert.

**Definition 1.4.2** Sei  $G$  eine Gruppe. Die **Ordnung**  $\text{ord}(a)$  eines Elements  $a$  von  $G$  ist die definiert als die Ordnung der von  $a$  erzeugten Gruppe  $\langle a \rangle$ . (Ist  $\langle a \rangle$  unendlich, so setzt man  $\text{ord}(a) := \infty$ .)

Die Ordnung eines Elements  $a$  ist 1 genau dann, wenn  $a$  das neutrale Element ist.

**Bemerkung 1.4.3** Sei  $G$  eine Gruppe und  $a \in G$ . Ist  $\text{ord}(a) \in \mathbb{N}$ , so gilt  $a^m = 1$  genau dann, wenn  $m$  ein Vielfaches von  $\text{ord}(a)$  ist. Insbesondere ist  $\text{ord}(a)$  die kleinste positive natürliche Zahl  $n$ , so dass  $a^n = e$  gilt. Ist  $\text{ord}(a) = \infty$ , so ist  $a^m \neq e$  für alle  $m$ .

**Satz 1.4.4** Ist  $G$  eine endliche Gruppe und  $a \in G$ , so ist  $a^{\#G} = e$ .

**Satz 1.4.5** Untergruppen zyklischer Gruppen sind zyklisch.

**Satz 1.4.6 (Chinesischer Restsatz, Gruppenversion)** Sind  $a_1, \dots, a_k \in \mathbb{N}_{\geq 1}$  paarweise teilerfremd und  $m = a_1 \cdot a_2 \cdot \dots \cdot a_k$ , so ist

$$\mathbb{Z}/m\mathbb{Z} \rightarrow \mathbb{Z}/a_1\mathbb{Z} \times \dots \times \mathbb{Z}/a_k\mathbb{Z}, n \mapsto (n + a_1\mathbb{Z}, \dots, n + a_k\mathbb{Z})$$

ein Isomorphismus von Gruppen.

## 1.5 Endlich erzeugte abelsche Gruppen

In diesem Abschnitt sind alle Gruppen abelsch, und wir verwenden die additive Notation.

**Satz 1.5.1** Sei  $G$  eine abelsche Gruppe und sei  $m \in \mathbb{N}$ .

- (a) Sind  $a_1, \dots, a_m \in G$ , so ist  $f: \mathbb{Z}^m \rightarrow G, (r_1, \dots, r_m) \mapsto r_1 a_1 + \dots + r_m a_m$  ein Gruppenhomomorphismus mit Bild  $\text{im } f = \langle a_1, \dots, a_m \rangle$ .
- (b) Jeder Gruppenhomomorphismus  $f: \mathbb{Z}^m \rightarrow G$  hat die Form wie in (a), für gewisse  $a_i \in G$ , d. h. (a) definiert eine Bijektion  $G^m \rightarrow \text{Hom}(\mathbb{Z}^m, G)$ .

**Bemerkung 1.5.2** Wenn  $G = \mathbb{Z}^n$  ist und wir Elemente von  $\mathbb{Z}^m$  und  $\mathbb{Z}^n$  als Spaltenvektoren auffassen, dann ist  $f(v) = Av$ , wobei  $A := (a_1 \mid \dots \mid a_m) \in \mathbb{Z}^{m \times n}$  die Matrix mit Spalten  $a_i$  ist.

**Satz 1.5.3** Sei  $G$  eine abelsche Gruppe und  $H$  eine Untergruppe. Lässt sich  $G$  von  $n$  Elementen erzeugen (d. h. existieren  $a_1, \dots, a_n \in G$  mit  $\langle a_1, \dots, a_n \rangle = G$ ), so auch  $H$ .

Notation: Sind  $a, b \in \mathbb{Z}$ , so schreiben wir  $a \mid b$ , wenn  $a$  ein **Teiler** von  $b$  ist, also wenn ein  $c \in \mathbb{Z}$  existiert, so dass  $a \cdot c = b$  gilt. Wir sagen auch „ $a$  teilt  $b$ “. Man beachte, dass nach dieser Definition  $a \mid 0$  gilt für jede ganze Zahl  $a$ .

**Satz 1.5.4 (Elementarteilersatz)** Zu jeder Matrix  $A \in \mathbb{Z}^{m \times n}$  gibt es invertierbare Matrizen  $S \in \mathbb{Z}^{m \times m}$  und  $T \in \mathbb{Z}^{n \times n}$  so dass  $S^{-1}$  und  $T^{-1}$  auch ganzzahlige Einträge haben und so dass  $SAT$  die Form

$$SAT = \begin{pmatrix} d_1 & 0 & \dots & 0 & \dots & 0 \\ 0 & \ddots & \ddots & \vdots & & \vdots \\ \vdots & \ddots & d_k & 0 & \dots & 0 \\ 0 & \dots & 0 & 0 & \dots & 0 \\ \vdots & & \vdots & \vdots & & \vdots \\ 0 & \dots & 0 & 0 & \dots & 0 \end{pmatrix},$$



hat für gewisse  $d_1, \dots, d_k \in \mathbb{N}_{\geq 1}$  mit  $d_1 \mid d_2 \mid \dots \mid d_k$ .

Die  $d_1, \dots, d_k$  durch  $A$  eindeutig bestimmt.

**Satz 1.5.5 (Beschreibung der Untergruppen von  $\mathbb{Z}^m$ )** Ist  $H \subseteq \mathbb{Z}^m$  eine Untergruppe, so gibt es einen Automorphismus  $f: \mathbb{Z}^m \rightarrow \mathbb{Z}^m$  so dass  $f(H) = d_1\mathbb{Z} \times \dots \times d_m\mathbb{Z}$  ist, für gewisse  $d_i \in \mathbb{N}$  mit  $d_1 \mid d_2 \mid \dots \mid d_m$ .

**Satz 1.5.6 (Klassifikation der endlich erzeugten abelschen Gruppen)**  
Sei  $G$  eine endlich erzeugte abelsche Gruppe.

(a)  $G$  ist isomorph zu einer Gruppe der Form

$$\mathbb{Z}/d_1\mathbb{Z} \times \dots \times \mathbb{Z}/d_k\mathbb{Z},$$

für gewisse  $d_1, \dots, d_k \in \mathbb{N}$ . (Hierbei ist auch  $d_i = 0$  erlaubt, so dass  $\mathbb{Z}/d_i\mathbb{Z} \cong \mathbb{Z}$  ist.)

(b) Man kann zusätzlich fordern, dass  $d_1 \mid \dots \mid d_k$  gilt, und wenn man diese zusätzliche Forderung stellt, sind  $d_1, \dots, d_k$  durch  $G$  schon eindeutig festgelegt.

## 1.6 Die symmetrischen und alternierenden Gruppen

**Definition 1.6.1** (a) Ein Element  $\sigma \in S_n$  heißt **Zyklus** (der Länge  $k \geq 2$ ), wenn es paarweise verschiedene  $x_1, \dots, x_k \in \{1, \dots, n\}$  gibt, so dass gilt:  $\sigma(x_i) = x_{i+1}$  für  $1 \leq i < k$ ;  $\sigma(x_k) = x_1$ ;  $\sigma(y) = y$  falls  $y \notin \{x_1, \dots, x_k\}$ . Die Menge  $\{x_1, \dots, x_k\}$  nennt man den **Träger** von  $\sigma$ . Notation für einen solchen Zyklus:  $(x_1, x_2, \dots, x_k)$ .

(b) Zykel der Länge 2 nennt man auch **Transpositionen**.

**Lemma 1.6.2** Sind  $\sigma, \sigma' \in S_n$  Zykel mit disjunkten Trägern, so gilt  $\sigma\sigma' = \sigma'\sigma$ .

**Satz 1.6.3** Jedes Element  $\sigma \in S_n$  lässt sich als Produkt  $\sigma_1 \cdots \sigma_m$  von Zykeln  $\sigma_j$  schreiben, die paarweise disjunkte Träger haben. Diese Schreibweise ist eindeutig bis auf Reihenfolge. (Man nennt dies die **Zykelzerlegung** von  $\sigma$ .)

**Satz 1.6.4**  $S_n$  wird von den Transposition erzeugt (d. h. jedes Element von  $S_n$  lässt sich als Produkt von Transpositionen schreiben).

**Lemma 1.6.5** Ist  $\sigma = (x_1, \dots, x_k)$  ein Zyklus und  $\tau \in S_n$  beliebig, so ist  $\tau\sigma\tau^{-1} = (\tau(x_1), \dots, \tau(x_k))$ .

Insbesondere: Ist  $N \triangleleft S_n$  ein Normalteiler, der einen Zyklus der Länge  $k$  enthält, so enthält  $N$  alle Zyklen der Länge  $k$ .

**Definition 1.6.6** Sei  $\sigma \in S_n$ .

(a) Die zugehörige **Permutationsmatrix** ist diejenige Matrix  $A_\sigma \in \mathbb{Z}^{n \times n}$ , die  $e_i \in \mathbb{Z}^n$  abbildet auf  $e_{\sigma(i)}$  für  $i = 1, \dots, n$ .

(b) Das **Signum** von  $\sigma$  ist definiert als  $\text{sgn}(\sigma) := \det(A_\sigma)$ .

Ist  $A_\sigma = (a_{ij})_{ij}$ , so ist also  $a_{\sigma(i),i} = 1$  für alle  $i$ , und alle restlichen Einträge sind 0.

**Lemma 1.6.7** Die Signum-Abbildung ist ein Gruppenhomomorphismus von  $S_n$  nach  $\{\pm 1\}$ . Lässt sich  $\sigma \in S_n$  als Produkt von  $k$  Transpositionen schreiben, so ist  $\text{sgn}(\sigma) = (-1)^k$ .

**Definition 1.6.8** Die **alternierende Gruppe**  $A_n \subseteq S_n$  ist der Kern von  $\text{sgn}: S_n \rightarrow \{\pm 1\}$ .

**Beispiel 1.6.9** Die Gruppen  $A_1$  und  $A_2$  sind trivial.  $A_3 \cong \mathbb{Z}/3\mathbb{Z}$ .

**Definition 1.6.10** Eine Gruppe  $G$  heißt **einfach**, wenn  $G$  und  $\{e\}$  ihre einzigen Normalteiler sind.

**Satz 1.6.11** (a) Die **kleinsche Vierergruppe**  $\{\text{id}, (1, 2)(3, 4), (1, 3)(2, 4), (1, 4)(2, 3)\}$  ist ein Normalteiler von  $A_4$ .  
 (b) Für  $n \geq 5$  ist  $A_n$  einfach.

## 1.7 Operationen von Gruppen auf Mengen

**Definition 1.7.1** Sei  $G$  eine Gruppe und  $X$  eine Menge. Eine **Gruppenwirkung** (auch: **Gruppenoperation**) von  $G$  auf  $X$  ist eine Abbildung  $\lambda: G \times X \rightarrow X$ ,  $(g, x) \mapsto \lambda(g, x) =: \lambda_g(x)$ , so dass für alle  $g, h \in G$  und  $x \in X$  gilt:

- (a)  $\lambda_e(x) = x$
- (b)  $\lambda_{gh}(x) = \lambda_g(\lambda_h(x))$

Ist die Gruppenwirkung implizit festgelegt, so schreibt man statt  $\lambda_g(x)$  auch  $gx$ .

**Bemerkung 1.7.2** Es existiert eine Bijektion

$$\{\text{Gruppenwirkungen von } G \text{ auf } X\} \xrightarrow{1:1} \text{Hom}(G, \text{Sym}(X))$$

gegeben durch  $\lambda \mapsto (g \mapsto \lambda_g)$ . Die Umkehrabbildung ist  $f \mapsto ((g, x) \mapsto f(g)(x))$ .

**Beispiel 1.7.3** Jede Gruppe  $G$  operiert auf mehrere Weisen auf sich selbst:

- (a) durch links-Multiplikation:  $\lambda: G \rightarrow \text{Sym}(G), a \mapsto (b \mapsto ab)$ .
- (b) durch rechts-Multiplikation:  $\lambda: G \rightarrow \text{Sym}(G), a \mapsto (b \mapsto ba^{-1})$ .
- (c) durch Konjugation:  $\lambda: G \rightarrow \text{Sym}(G), a \mapsto (b \mapsto aba^{-1})$ .

**Satz 1.7.4 (Satz von Cayley)** Jede Gruppe ist isomorph zu einer Untergruppe von  $\text{Sym}(X)$ , für eine geeignete Menge  $X$ .

**Lemma 1.7.5** Operiert  $G$  auf  $X$ , so gilt für  $a \in G$  und  $x, y \in X$ : Wenn  $ax = y$  ist, ist  $a^{-1}y = x$ .

**Bemerkung 1.7.6** Ist  $\lambda$  eine Operation einer Gruppe  $G$  auf einer Menge  $X$  und ist  $H$  eine Untergruppe von  $G$ , so definiert  $\lambda$  auch eine Operation von  $H$  auf  $X$ .

**Definition 1.7.7** Sei  $G$  eine Gruppe, die auf einer Menge  $X$  operiert und seien  $a \in G$  und  $x \in X$ .

- (a) Die **Bahn** von  $x$  ist die Menge  $Gx := \{ax \mid a \in G\} \subseteq X$ .
- (b) Gilt  $Gx = X$ , so sagt man, „ $G$  operiert **transitiv** auf  $X$ “.
- (c) Man sagt,  $a$  **stabilisiert**  $x$  oder  $a$  **hält**  $x$  **fest**, wenn  $ax = x$  gilt.
- (d) Der **Stabilisator** von  $x$  ist  $\text{Stab}_G(x) := \{a \in G \mid ax = x\}$ .

**Satz 1.7.8** Sei  $G$  eine Gruppe, die auf einer Menge  $X$  operiert. Dann gilt:

- (a) Für jedes  $x \in X$  ist  $\text{Stab}_G(x)$  eine Untergruppe von  $G$ .
- (b) Die Menge  $\{Gx \mid x \in X\}$  aller Bahnen bilden eine Partition von  $X$ .
- (c) Für alle  $x \in X$  gilt:  $\#(Gx) = (G : \text{Stab}_G(x))$ .

**Korollar 1.7.9 (Bahnenformel)** Ist  $G$  eine endliche Gruppe, die auf einer endlichen Menge  $X$  operiert, und sind  $Gx_1, \dots, Gx_k$  die Bahnen dieser Operation (mit  $Gx_i \neq Gx_j$  für  $i \neq j$ ), so gilt

$$\#X = \sum_{i=1}^k \#(Gx_i) = \sum_{i=1}^k (G : \text{Stab}_G x_i) = \sum_{i=1}^k \frac{\#G}{\#\text{Stab}_G x_i}$$

## 1.8 $p$ -Gruppen und die Sylow-Sätze

**Definition 1.8.1** Sei  $p$  eine Primzahl. Eine  $p$ -Gruppe ist eine endliche Gruppe  $G$ , deren Ordnung eine Potenz von  $p$  ist.

**Lemma 1.8.2** Ist  $G$  eine nicht-triviale  $p$ -Gruppe, so ist  $Z(G)$  nicht-trivial.

**Satz 1.8.3** Gruppen der Ordnung  $p^2$  für Primzahlen  $p$  sind abelsch.

**Korollar 1.8.4** Bis auf Isomorphie sind alle Gruppen der Ordnung  $p^2$  (für  $p$  prim) der Form  $\mathbb{Z}/p^2\mathbb{Z}$  und  $(\mathbb{Z}/p\mathbb{Z})^2$ .

**Definition 1.8.5** Sei  $p$  eine Primzahl und  $G$  eine endliche Gruppe. Wir schreiben die Ordnung von  $G$  als  $\#G = m \cdot p^\ell$  für  $\ell, m \in \mathbb{N}$  mit  $p \nmid m$ .

- (a) Eine  **$p$ -Untergruppe** von  $G$  ist eine Untergruppe, die eine  $p$ -Gruppe ist (also der Ordnung  $p^k$  für ein  $k \leq \ell$ ).
- (b) Eine **Sylow- $p$ -Untergruppe** von  $G$  ist eine Untergruppe der Ordnung genau  $p^\ell$ .

**Satz 1.8.6 (Sylow-Sätze)** Sei  $G$  endlich und sei  $p$  eine Primzahl. Wir schreiben  $\#G = m \cdot p^\ell$  für  $\ell, m \in \mathbb{N}$  mit  $p \nmid m$ . Dann gilt:

- (a) Jede  $p$ -Untergruppe von  $G$  ist in einer Sylow- $p$ -Untergruppe enthalten.
- (b) Alle Sylow- $p$ -Untergruppen von  $G$  sind konjugiert, d. h. sind  $H, H' \subseteq G$  Sylow- $p$ -Untergruppen, so gibt es ein  $a \in G$  mit  $aHa^{-1} = H'$ .
- (c) Ist  $s_p$  die Anzahl der Sylow- $p$ -Untergruppen von  $G$ , so gilt  $s_p \equiv 1 \pmod{p}$  und  $s_p \mid m$ .

Zur Erinnerung:  $a \equiv b \pmod{m}$  (für  $a, b \in \mathbb{Z}$ ,  $m \in \mathbb{N}_{\geq 1}$ ) bedeutet:  $m \mid a - b$ ; oder, äquivalent:  $a$  und  $b$  haben das selbe Bild in  $\mathbb{Z}/m\mathbb{Z}$ .

**Korollar 1.8.7 (Satz von Cauchy)** *Ist  $G$  eine endliche Gruppe und  $p$  eine Primzahl mit  $p \mid |G|$ , so existiert in  $G$  ein Element der Ordnung  $p$ .*

**Korollar 1.8.8** *Sei  $G$  eine endliche Gruppe und  $p$  eine Primzahl. Eine Sylow- $p$ -Untergruppe von  $G$  ist ein Normalteiler von  $G$  genau dann, wenn  $P$  die einzige Sylow- $p$ -Untergruppe von  $G$  ist.*

## 2 Ringe

### 2.1 Ringe und Unterringe

**Definition 2.1.1** *Ein **kommutativer Ring mit eins** ist eine (additiv geschriebene) abelsche Gruppe  $R$  zusammen mit einer weiteren Verknüpfung  $\cdot : R \times R \rightarrow R$  mit folgenden Eigenschaften:*

- (a)  $\cdot$  ist assoziativ und kommutativ;
- (b) es gibt ein bezüglich  $\cdot$  neutrales Element (das mit 1 bezeichnet wird);
- (c) Distributivität gilt (d. h. für alle  $a, b, c \in R$  gilt:  $a \cdot (b + c) = a \cdot b + a \cdot c$ ).

Im Folgenden ist, wenn nicht anders angegeben, mit „Ring“ immer ein kommutativer Ring mit eins gemeint.

Wie bei Gruppen schreiben wir, für  $a \in R$  und  $n \in \mathbb{N}$ :

$$n \cdot a := \underbrace{a + a + \dots + a}_n, \quad (-n) \cdot a := -(n \cdot a), \quad a^0 = 1, \quad a^n := \underbrace{a \cdot a \cdot \dots \cdot a}_n$$

**Bemerkung 2.1.2** *In jedem Ring  $R$  gilt:*

- (a) Das neutrale Element bezüglich  $\cdot$  ist eindeutig.
- (b)  $0 \cdot a = 0$
- (c)  $(-1) \cdot a = -a$

**Beispiel 2.1.3** *Ist  $R$  ein Ring, so ist auch  $R[X] = \{\sum_{i=0}^n a_i X^i \mid n \in \mathbb{N}, a_i \in R\}$  ein Ring.*

Erinnerung:  $R[X]$  nennt man den **Polynomring** über  $R$ . Die Elemente von  $R[X]$  nennt man **Polynome**. Ist  $f = \sum_{i=0}^n a_i X^i$  mit  $a_n \neq 0$ , so ist  $n$  der **Grad** von  $f$ . Ist  $a_n = 1$ , so nennt man  $f$  **normiert**. Elemente der Form  $aX^k$  (für  $a \in R$ ,  $k \in \mathbb{N}$ ) nennt man **Monome**.

Analog definiert man auch Polynome in mehreren Variablen. Der Ring der Polynome in den Variablen  $X_1, \dots, X_k$  wird mit  $R[X_1, \dots, X_k]$  bezeichnet. Es gilt:  $R[X_1, \dots, X_k] = R[X_1][X_2] \dots [X_k]$

**Definition 2.1.4** *Das (**direkte**) **Produkt** von zwei Ringen  $R$  und  $S$  ist die Gruppe  $R \times S$  mit komponentenweiser Multiplikation:*

$$(a, b) \cdot (a', b') := (a \cdot a', b \cdot b')$$

für  $a, a' \in R$ ,  $b, b' \in S$ .

**Definition 2.1.5** Sei  $R$  ein Ring. Ein **Unterring** von  $R$  ist eine Teilmenge  $S \subseteq R$ , so dass  $S$  ein Ring ist (mit der auf  $S$  eingeschränkten Addition von Multiplikation von  $R$ ) und  $1 \in S$  gilt.

## 2.2 Ringhomomorphismen und der Isomorphiesatz

**Definition 2.2.1** Seien  $R$  und  $S$  Ringe. Ein **Ringhomomorphismus** ist ein Gruppenhomomorphismus  $f: R \rightarrow S$ , so dass gilt:  $f(a \cdot b) = f(a) \cdot f(b)$  für alle  $a, b \in R$ ;  $f(1) = 1$ .  $\text{Hom}(R, S)$  bezeichnet die Menge aller Ringhomomorphismen von  $R$  nach  $S$ .

Ein **Isomorphismus von Ringen** ist ein bijektiver Ringhomomorphismus.

Zwei Ringe  $R$  und  $S$  heißen **isomorph** (Notation:  $R \cong S$ ), wenn es einen Ringisomorphismus  $R \rightarrow S$  gibt.

Ein **Endomorphismus** eines Rings  $R$  ist ein Homomorphismus von  $R$  nach  $R$ . Die Menge der Endomorphismen von  $R$  wird mit  $\text{End}(R)$  bezeichnet.

Ein **Automorphismus** eines Rings  $R$  ist ein Isomorphismus von  $R$  nach  $R$ . Die Menge der Automorphismen von  $R$  wird mit  $\text{Aut}(R)$  bezeichnet.

**Bemerkung 2.2.2** Die Verknüpfung von zwei Ringhomomorphismen ist wieder ein Ringhomomorphismus. Das Inverse eines Ring-Isomorphismus ist wieder ein Ring-Isomorphismus.

**Beispiel 2.2.3** Ist  $R$  ein beliebiger Ring, so gibt es genau einen Ringhomomorphismus  $\mathbb{Z} \rightarrow R$ . Er bildet  $n \in \mathbb{Z}$  auf  $n \cdot 1 \in R$  ab.

**Beispiel 2.2.4** Ist  $R$  ein Ring und  $a \in R$ , so ist die Abbildung  $R[X] \rightarrow R$ ,  $f \mapsto f(a)$  ein Ringhomomorphismus. (Man nennt dies die **Evaluationsabbildung** an  $a$ .) Jeder Ringhomomorphismus von  $R[X]$  nach  $R$ , der auf  $R$  die Identität ist, ist von dieser Form.

**Definition 2.2.5** Sei  $R$  ein Ring. Ein **Ideal** von  $R$  ist eine additive Untergruppe  $\mathfrak{a} \subseteq R$ , so dass außerdem für alle  $r \in R$  und  $a \in \mathfrak{a}$  gilt:  $ra \in \mathfrak{a}$ . Die Notation „ $\mathfrak{a} \triangleleft R$ “ bedeutet:  $\mathfrak{a}$  ist ein Ideal von  $R$ .

**Bemerkung 2.2.6** Für beliebige Ringe  $R$  sind sowohl  $R$  als auch  $\{0\}$  Ideale von  $R$ .

**Bemerkung 2.2.7** Ist  $R$  ein Ring und  $\mathfrak{a} \triangleleft R$  ein Ideal mit  $1 \in \mathfrak{a}$ , so ist bereits  $\mathfrak{a} = R$ .

**Beispiel 2.2.8** Ist  $R$  ein Ring und  $a \in R$  beliebig, so ist  $aR = \{ar \mid r \in R\}$  ein Ideal von  $R$ .

**Beispiel 2.2.9** Die Ideale von  $\mathbb{Z}$  sind genau die Untergruppen von  $\mathbb{Z}$ , also die Teilmengen der Form  $n\mathbb{Z}$  für  $n \in \mathbb{N}$ .

**Lemma 2.2.10** Ist  $f: R \rightarrow S$  ein Ringhomomorphismus, so ist  $\text{im } f$  ein Unterring von  $S$  und  $\ker f$  ein Ideal von  $R$ . Allgemeiner gilt:

- (a) Ist  $R' \subseteq R$  ein Unterring, so ist  $f(R')$  ein Unterring von  $S$ .
- (b) Ist  $\mathfrak{a}$  ein Ideal von  $S$ , so ist  $f^{-1}(\mathfrak{a})$  ein Ideal von  $R$ .

**Satz 2.2.11** Ist  $R$  ein Ring und  $\mathfrak{a} \triangleleft R$  ein Ideal, so induziert die Multiplikation von  $R$  eine Verknüpfung auf der Quotientengruppe  $R/\mathfrak{a}$ :  $(a + \mathfrak{a}) \cdot (b + \mathfrak{a}) := ab + \mathfrak{a}$  für  $a, b \in R$ . Mit dieser Verknüpfung als Multiplikation wird  $R/\mathfrak{a}$  zu einem Ring.

**Definition 2.2.12** Der Ring  $R/\mathfrak{a}$  („ $R$  modulo  $\mathfrak{a}$ “) aus dem vorigen Satz wird **Quotientenring** genannt (oder manchmal auch **Faktorring** oder **Restklassenring**). Ist klar, welches Ideal  $\mathfrak{a}$  gemeint ist, so schreiben wir statt  $a + \mathfrak{a}$  oft  $\bar{a}$  (für  $a \in R$ ).

**Beispiel 2.2.13** Ist  $K$  ein Körper und  $f \in K[X]$  ein Polynom vom Grad  $n \geq 1$ , so ist  $K[X]/fK[X]$  ein  $K$ -Vektorraum mit Basis  $\bar{1}, \bar{X}, \dots, \bar{X}^{n-1}$ .

**Satz 2.2.14 (Isomorphiesatz)** Seien  $R$  und  $S$  Ringe und  $f: R \rightarrow S$  ein Homomorphismus. Dann ist der induzierte Gruppenisomorphismus  $\tilde{f}: R/\ker f \rightarrow \text{im } f$  (aus dem Isomorphiesatz für Gruppen; Satz 1.3.11) bereits ein Ringisomorphismus.

## 2.3 Mehr zu Idealen

**Lemma 2.3.1** Sei  $R$  ein Ring. Eine nicht-leere Teilmenge  $\mathfrak{a} \subseteq R$  ist ein Ideal genau dann, wenn für alle  $a, b \in \mathfrak{a}$  und alle  $r \in R$  gilt:  $ar + b \in \mathfrak{a}$ .

**Lemma 2.3.2** Ist  $R$  ein Ring und  $A \subseteq R$  eine beliebige Teilmenge, so existiert unter allen Idealen von  $R$ , die  $A$  enthalten, ein kleinstes. Dieses kleinste Ideal, das  $A$  enthält besteht genau aus endlichen Summen der Form  $\sum_{i=1}^k r_i a_i$  für  $r_i \in R$  und  $a_i \in A$ .

**Definition 2.3.3** Das kleinste Ideal, das das im obigen Lemma  $A$  enthält, nennt man das von  $A$  **erzeugte** Ideal. Ist  $A = \{a_1, \dots, a_n\}$ , so schreibt man für das von  $A$  erzeugte Ideal  $(a_1, \dots, a_n)$ . Ideale, die von einem Element erzeugt werden, nennt man **Hauptideale**.

**Definition 2.3.4** Sei  $R$  ein Ring. Eine **Einheit** von  $R$  ist ein Element  $a \in R$ , so dass ein  $b \in R$  existiert mit  $ab = 1$ . Die Menge der Einheiten von  $R$  wird mit  $R^\times$  bezeichnet.

**Beispiel 2.3.5** Die Einheiten eines Körpers  $K$  sind  $K^\times = K \setminus \{0\}$ .

**Bemerkung 2.3.6** Für  $a \in R$  gilt:  $a$  ist eine Einheit genau dann, wenn  $(a) = R$  ist.

**Lemma 2.3.7** Die Menge  $R^\times$  der Einheiten eines Rings  $R$  bildet mit  $\cdot$  eine Gruppe.

**Definition 2.3.8** Sei  $R$  ein Ring. Ein Ideal  $\mathfrak{a} \subsetneq R$  heißt **maximal**, wenn es kein Ideal  $\mathfrak{b} \subsetneq R$  gibt mit  $\mathfrak{a} \subsetneq \mathfrak{b}$ .

**Satz 2.3.9** Ein Ideal  $\mathfrak{a}$  in einem Ring  $R$  ist maximal genau dann, wenn  $R/\mathfrak{a}$  ein Körper ist.

**Satz 2.3.10** Sei  $R$  ein Ring und  $\mathfrak{a} \subsetneq R$  ein beliebiges Ideal. Dann existiert ein maximales Ideal  $\mathfrak{a}_0 \supseteq \mathfrak{a}$ .

## 2.4 Nullteilerfreie Ringe

**Definition 2.4.1** Ein Ring  $R \neq \{0\}$  heißt **nullteilerfrei** (auch: **integer**, **Integritätsbereich**) wenn für alle  $a, b \in R \setminus \{0\}$  gilt:  $a \cdot b \neq 0$ .

**Bemerkung 2.4.2** Ist  $R$  ein nullteilerfreier Ring und sind  $a, b \in R$  und  $c \in R \setminus \{0\}$  mit  $ac = bc$ , so gilt  $a = b$ .

**Satz 2.4.3** Sei  $R$  ein nullteilerfreier Ring. Dann existiert ein Körper  $K$  und ein injektiver Ringhomomorphismus  $f: R \rightarrow K$  so dass jedes Element von  $K$  sich schreiben lässt als  $\frac{f(a)}{f(b)}$  für geeignete  $a \in R, b \in R \setminus \{0\}$ .

**Definition 2.4.4** Der Körper  $K$  aus Satz 2.4.3 wird **Brückekörper** (auch: **Quotientenkörper**) von  $R$  genannt und mit  $\text{Frac}(R)$  bezeichnet. Wir fassen in Zukunft Nullteilerfreie Ringe  $R$  immer als Teilmenge von  $\text{Frac}(R)$  auf.

**Beispiel 2.4.5** Ist  $K$  ein Körper, so schreibt man den Brückekörper eines Polynomrings über  $K$  mit runden Klammern:  $K(X_1, \dots, X_n) := \text{Frac}(K[X_1, \dots, X_n])$ .

**Satz 2.4.6** Der Brückekörper eines nullteilerfreien Rings  $R$  hat die folgende universelle Eigenschaft: Ist  $f': R \rightarrow K'$  ein injektiver Ringhomomorphismus in einen Körper  $K'$ , so gibt es genau eine Fortsetzung von  $f'$  zu einem Ringhomomorphismus  $g: \text{Frac}(R) \rightarrow K'$ .

**Satz 2.4.7** Ist  $R$  ein nullteilerfreier Ring, so gilt für Polynome  $f, g \in R[X] \setminus \{0\}$ :  $\deg(fg) = \deg f + \deg g$ . Insbesondere:

- (a)  $(R[X])^\times = R^\times$
- (b)  $R[X]$  ist auch nullteilerfrei.

## 2.5 Hauptidealringe und faktorielle Ringe

**Definition 2.5.1** Sei  $R$  ein nullteilerfreier Ring.

- (a) Für  $a, b \in R$  sagt man „ $a$  teilt  $b$ “, wenn ein  $c \in R$  existiert mit  $ac = b$ . Man sagt auch  $a$  ist ein **Teiler** von  $b$  oder  $b$  ist ein **Vielfaches** von  $a$ .
- (b) Ein Element  $a \in R$  heißt **irreduzibel** (in  $R$ ) wenn  $a$  keine Einheit ist und aus  $b \cdot c = a$  (für  $b, c \in R$ ) folgt, dass  $b$  oder  $c$  eine Einheit ist.
- (c) Zwei Elemente  $a, b \in R \setminus \{0\}$  heißen **assoziiert** zueinander, wenn  $\frac{a}{b} \in R^\times$  ist.
- (d) Zwei Elemente  $a, b \in R$  heißen **teilerfremd** zueinander, wenn aus  $c \mid a$  und  $c \mid b$  folgt, dass  $c$  eine Einheit ist (für  $c \in R$ ).

**Bemerkung 2.5.2** Sei  $R$  ein nullteilerfreier Ring und seien  $a, b \in R$  irreduzibel. Dann sind  $a$  und  $b$  entweder teilerfremd oder assoziiert zueinander.

**Definition 2.5.3** Ein nullteilerfreier Ring  $R$  heißt **Hauptidealring**, wenn jedes Ideal ein Hauptideal ist.

**Lemma 2.5.4** Sei  $R$  ein Hauptidealring und  $a \in R$ . Das Hauptideal  $(a)$  ist maximal genau dann, wenn  $a$  irreduzibel ist.

**Lemma 2.5.5** Sei  $R$  ein Hauptidealring und seien  $a, b, b' \in R \setminus \{0\}$ .

- (a)  $a$  und  $b$  sind teilerfremd genau dann, wenn  $(a, b) = R$  ist.
- (b) Ist  $a$  teilerfremd zu  $b$  und zu  $b'$ , so ist  $a$  auch teilerfremd zu  $bb'$ .

**Beispiel 2.5.6** Ist  $K$  ein Körper, so ist  $K[X]$  ein Hauptidealring.

**Definition 2.5.7** Sei  $R$  ein nullteilerfreier Ring. Ein Repräsentantensystem der irreduziblen Elemente von  $R$  ist eine Menge  $P \subseteq R$  von irreduziblen Elementen, so dass für jedes irreduzible Element  $p \in R$  genau ein  $p' \in P$  existiert, dass zu  $p$  assoziiert ist.

**Definition 2.5.8** Ein nullteilerfreier Ring  $R$  heißt **faktoriell** wenn eindeutige Primfaktorzerlegungen existieren, d. h. wenn für ein (oder jedes) Repräsentantensystem der irreduziblen Elemente  $P \subseteq R$  folgendes gilt: Jedes Element  $a \in R \setminus \{0\}$  lässt sich auf eindeutige (bis auf Reihenfolge) Weise schreiben als  $a = e \cdot p_1 \cdot p_2 \cdots p_k$ , für  $e \in R^\times$  und  $p_i \in P$ . (Dies nennt man eine **Primfaktorzerlegung** von  $a$ .)

**Satz 2.5.9** Hauptidealringe sind faktoriell.

**Bemerkung 2.5.10** Ist  $R$  faktoriell, so lassen sich Teilbarkeit und Teilerfremdheit an den Primfaktorzerlegungen ablesen.

**Lemma 2.5.11** Ist  $R$  faktoriell und  $p \in R$  irreduzibel, so ist  $R/(p)$  nullteilerfrei.

## 2.6 Polynomringe

**Satz 2.6.1 (Satz von Gauß)** Ist  $R$  ein faktorieller Ring, so ist auch  $R[X]$  faktoriell.

**Korollar 2.6.2** (a)  $\mathbb{Z}[X_1, \dots, X_n]$  ist faktoriell.

(b) Ist  $K$  ein Körper, so ist  $K[X_1, \dots, X_n]$  faktoriell.

In diesem gesamten Abschnitt sei  $R$  ein faktorieller Ring und  $K = \text{Frac}(R)$ .

**Definition 2.6.3** Ein Polynom  $f \in R[X]$  heißt **primitiv**, wenn kein  $a \in R \setminus R^\times$  existiert, das alle Koeffizienten von  $f$  teilt.



**Bemerkung 2.6.4** Zu jedem  $f \in K[X]$  existiert ein  $a \in K^\times$ , so dass  $f \in R[X]$  ist und primitiv ist.

**Lemma 2.6.5** Sind  $f \in K[X]$  und  $a \in K^\times$  so, dass sowohl  $f$  als auch  $af$  primitive Polynome in  $R[X]$  sind, so ist  $a \in R^\times$ .

**Lemma 2.6.6** Seien  $f, g \in K[X]$  primitiv. Dann ist auch  $f \cdot g$  primitiv.

**Satz 2.6.7** Die irreduziblen Elemente von  $R[X]$  sind genau die irreduziblen Elemente von  $R$  und die nicht-konstanten primitiven Polynome in  $R[X]$ , die irreduzibel in  $K[X]$  sind.

Bemerkung: Wir haben insbesondere gesehen: Lässt sich ein Polynom  $f \in R[X]$  als Produkt  $f = g \cdot h$  schreiben, für  $g, h \in K[X]$ , so erhalten wir auch  $f = \tilde{g} \cdot \tilde{h}$  für  $\tilde{g} = g \cdot a, \tilde{h} = h \cdot a^{-1} \in R[X]$ , für ein geeignetes  $a \in K$ .

**Satz 2.6.8 (Eisensteinsches Irreduzibilitätskriterium)** Ist  $f = \sum a_i X^i \in R[X]$  ein Polynom vom Grad  $n \geq 1$ , und gibt es ein irreduzibles Element  $p \in R$  mit  $p \mid a_i$  für  $i < n$ ,  $p^2 \nmid a_0$  und  $p \nmid a_n$ , so ist  $f$  irreduzibel in  $K[X]$ .

## 3 Körper

### 3.1 Körpererweiterungen

**Definition 3.1.1** Sei  $K$  ein Körper. Der Kern des Ringhomomorphismus  $\mathbb{Z} \rightarrow K$  (aus Beispiel 2.2.3) hat die Form  $n\mathbb{Z}$ , für ein  $n \in \mathbb{N}$ . Dieses  $n$  nennt man die **Charakteristik** von  $K$ , und man schreibt  $\text{char } K$  dafür.

**Satz 3.1.2** Die Charakteristik eines Körpers ist entweder 0 oder eine Primzahl.

**Bemerkung 3.1.3** Sind  $K$  und  $L$  Körper und ist  $f: K \rightarrow L$  ein Ringhomomorphismus, so ist  $f$  automatisch injektiv.

**Definition 3.1.4** (a) Einen Ringhomomorphismus  $f: L_1 \rightarrow L_2$  zwischen Körpern  $L_1$  und  $L_2$  nennt man auch **Körperhomomorphismus**. Enthalten  $L_1$  und  $L_2$  einen gemeinsamen Unterkörper  $K$ , und ist die Einschränkung  $f|_K$  die Identität auf  $K$ , so sagt man auch,  $f$  ist ein **Körperhomomorphismus über  $K$** .  
 (b) Analog definiert man **Körperisomorphismus** (über  $K$ ) und **Körperautomorphismus** (über  $K$ ). Die Menge der Automorphismen eines Körpers  $L$  über einem Unterkörper  $K \subseteq L$  wird mit  $\text{Aut}(L/K)$  bezeichnet.

**Definition 3.1.5** Sei  $L$  ein Körper. Ein **Unterkörper** ist eine Teilmenge  $K \subseteq L$ , so dass  $K$  auch wieder ein Körper ist. Man nennt  $L$  dann einen **Oberkörper** von  $K$ , und man schreibt auch „ $L/K$  ist eine **Körpererweiterung**“ um zu sagen, dass  $L$  ein Körper ist und  $K$  ein Unterkörper von  $L$ .

**Satz 3.1.6** Ist  $K$  ein Körper und  $A$  eine Teilmenge von  $K$ , so existiert unter allen Unterkörpern von  $K$ , die  $A$  enthalten, ein kleinster.

**Definition 3.1.7** Sei  $K$  ein Körper.

- (a) Den kleinsten Unterkörper eines Körpers  $K$  nennt man den **Primkörper** von  $K$
- (b) Ist  $K_0$  ein Unterkörper von  $K$  und sind  $a_1, \dots, a_n \in K$ , so wird der kleinste Unterkörper von  $K$ , der  $K_0 \cup \{a_1, \dots, a_n\}$  enthält, mit  $K_0(a_1, \dots, a_n)$  bezeichnet. Man nennt dies den von den  $a_i$  **erzeugten Unterkörper** über  $K_0$ .

**Satz 3.1.8** Der Primkörper eines Körpers  $K$  ist isomorph zu  $\mathbb{Q}$  falls  $\text{char } K = 0$  ist und isomorph zu  $\mathbb{F}_p$  falls  $\text{char } K = p$  ist für eine Primzahl  $p$ .

**Bemerkung 3.1.9** Ist  $L/K$  eine Körpererweiterung, so ist  $L$  ein  $K$ -Vektorraum.

**Definition 3.1.10** Der **Grad** einer Körpererweiterung  $L/K$  ist  $[L : K] := \dim_K L$ , d. h. die Dimension von  $L$  als  $K$ -Vektorraum aufgefasst. ( $[L : K]$  kann auch  $\infty$  sein.) Eine **endliche Körpererweiterung** ist eine Körpererweiterung von endlichem Grad.

**Satz 3.1.11** Sind  $K \subseteq L \subseteq M$  Körper, so gilt  $[M : K] = [M : L] \cdot [L : K]$ . Insbesondere ist  $[M : K]$  endlich genau dann, wenn sowohl  $[M : L]$  als auch  $[L : K]$  endlich sind.

## 3.2 Adjunktion von Elementen

**Satz 3.2.1** Sei  $L/K$  eine Körpererweiterung und sei  $a \in L$ . Die Menge  $\mathfrak{a} := \{f \in K[X] \mid f(a) = 0\}$  ist ein Hauptideal in  $K[X]$ . Außerdem gilt:

- (a) Ist  $\mathfrak{a} = \{0\}$ , so ist  $K(a) \cong K(X)$  und  $[K(a) : K] = \infty$ .
- (b) Ist  $\mathfrak{a} \neq \{0\}$ , so ist  $K(a) \cong K[X]/\mathfrak{a}$ , und  $\mathfrak{a} = (f_0)$  für ein irreduzibles normiertes Polynom  $f_0$ . Außerdem gilt  $\deg f_0 = [K(a) : K]$ .

**Bemerkung 3.2.2** Im Fall (b) aus dem obigen Satz gilt:

- (a)  $f_0$  ist das eindeutige normierte Polynom minimalen Grades, das  $a$  als Nullstelle hat. Außerdem ist es auch das eindeutige irreduzible normierte Polynom, das  $a$  als Nullstelle hat.
- (b) Jedes Element von  $K(a)$  eindeutig schreiben als  $\sum_{i=0}^{n-1} b_i a^i$ , für gewisse  $b_i \in K$ .

**Definition 3.2.3** Sei  $L/K$  eine Körpererweiterung und sei  $a \in L$ .

- (a) Im Fall (a) aus Satz 3.2.1 nennt man  $a$  **transzendent** über  $K$ .
- (b) Im Fall (b) aus Satz 3.2.1 nennt man  $a$  **algebraisch** über  $K$ . Das Polynom  $f_0$  aus Satz 3.2.1 nennt man das **Minimalpolynom** von  $a$  (über  $K$ ). Notation dafür:  $\text{MiPo}_{a/K}$ . Den Grad  $\deg \text{MiPo}_{a/K} = [K(a) : K]$  nennt man auch den **Grad** von  $a$  über  $K$ .

Sagt man nur „transzendent“ oder „algebraisch“ (ohne  $K$  zu erwähnen), so meint man transzendent bzw. algebraisch über dem Primkörper von  $K$ .

**Bemerkung 3.2.4** Fast alle komplexen Zahlen sind transzendent: Es gibt überabzählbar viele komplexe Zahlen aber nur abzählbar viele algebraische Zahlen. Insbesondere gibt es überabzählbar transzendente komplexe Zahlen.

**Satz 3.2.5**  $e$  und  $\pi$  sind transzendent. (Ohne Beweis; ein Beweis steht z. B. im Algebra-Buch von Lang.)

**Definition 3.2.6** Sei  $n \in \mathbb{N}$ ,  $n \geq 1$ . Eine  $n$ -te **Einheitswurzel** ist eine komplexe Zahl  $z$ , so dass  $z^n = 1$  ist. Eine **primitive  $n$ -te Einheitswurzel** ist eine  $n$ -te Einheitswurzel, die keine  $k$ -te Einheitswurzel für  $k < n$  ist.

**Bemerkung 3.2.7**  $\zeta_n := e^{2\pi i/n}$  ist eine primitive  $n$ -te Einheitswurzel. Allgemeiner ist auch  $\zeta_n^m$  eine primitive  $n$ -te Einheitswurzel, wenn  $m$  und  $n$  teilerfremd sind.

**Beispiel 3.2.8** Ist  $p$  prim, so ist  $[\mathbb{Q}(\zeta_p) : \mathbb{Q}] = p - 1$ .

**Satz 3.2.9** Seien  $K, L_1, L_2, M$  Körper mit  $K \subseteq L_1 \subseteq M$  und  $K \subseteq L_2 \subseteq M$ , und so, dass  $M$  von  $L_1$  und  $L_2$  erzeugt wird. Dann gilt  $[L_1 : K] \geq [M : L_2]$ .

### 3.3 Anwendung: Konstruktion mit Zirkel und Lineal

**Definition 3.3.1** Sei  $M \subseteq \mathbb{R}^2$  eine Menge von Punkten. Die folgenden Punkte  $a \in \mathbb{R}^2$  nennt man **mit Zirkel und Lineal aus  $M$  konstruierbar**:

- $a$  ist der Schnittpunkt von zwei (verschiedenen) Geraden  $g_1, g_2$ , die jeweils durch (mindestens) zwei Punkte aus  $M$  gehen.
- $a$  ist ein Schnittpunkt einer Geraden, die durch (mindestens) zwei Punkte aus  $M$  geht, und eines Kreises, dessen Mittelpunkt in  $M$  liegt und auf dem (mindestens) ein Punkt aus  $M$  liegt.
- $a$  ist ein Schnittpunkt von zwei Kreisen, deren Mittelpunkte in  $M$  liegen und auf denen jeweils (mindestens) ein Punkt aus  $M$  liegt.
- $a$  lässt sich durch wiederholtes Anwenden von (a)–(c) konstruieren, d. h. es existieren  $a_1, \dots, a_n = a$ , so dass  $a_i$  sich mit (a)–(c) aus  $M \cup \{a_1, \dots, a_{i-1}\}$  erhalten lässt (für jedes  $i$ ).

**Definition 3.3.2** Eine komplexe Zahl  $a$  heißt **konstruierbar**, wenn  $a_1, \dots, a_n \in \mathbb{C}$  existieren mit  $a = a_n$  und  $a_i^2 \in \mathbb{Q}(a_1, \dots, a_{i-1})$  für  $i = 1, \dots, n$ .

**Satz 3.3.3** Wenn wir auf die übliche Weise  $\mathbb{C}$  mit  $\mathbb{R}^2$  identifizieren, gilt: Die aus  $0 = (0, 0)$  und  $1 = (1, 0)$  mit Zirkel und Lineal konstruierbaren Punkte in  $\mathbb{R}^2$  sind genau die konstruierbaren komplexen Zahlen.

**Lemma 3.3.4** Ist  $a \in \mathbb{C}$  konstruierbar, so ist  $[\mathbb{Q}(a) : \mathbb{Q}]$  eine Zweierpotenz.

**Beispiel 3.3.5**  $\sqrt[3]{2}$  ist nicht konstruierbar.

**Korollar 3.3.6** Die folgenden Dinge lassen sich nicht mit Zirkel und Lineal machen:

- (a) Würfelverdopplung
- (b) die Quadratur des Kreises
- (c) Winkeldrittung

Bei (a), (b) ist gemeint: Aus Punkten  $a, b \in \mathbb{R}^2$  lassen sich keine Punkte  $a', b' \in \mathbb{R}$  mit Zirkel und Lineal konstruieren, so dass

- (a) der Würfel mit Kantenlänge  $|a' - b'|$  das doppelte Volumen des Würfels mit Kantenlänge  $|a - b|$  hat;
- (b) das Quadrat mit Kantenlänge  $|a' - b'|$  die gleiche Fläche hat wie der Kreis mit Radius  $|a - b|$ .

**Korollar 3.3.7** Das regelmäßige  $n$ -Eck kann nicht mit Zirkel und Lineal konstruiert werden wenn

- (a)  $n$  einen Primfaktor  $p \geq 3$  hat, so dass  $p - 1$  keine Zweierpotenz ist.
- (b)  $n$  einen beliebigen Primfaktor  $p \geq 3$  mehrfach hat.

Bemerkung: Wir werden später zeigen, dass alle anderen  $n$ -Ecke konstruierbar sind.

## 3.4 Algebraische Körpererweiterungen

**Definition 3.4.1** Eine Körpererweiterung  $L/K$  heißt **algebraisch**, wenn alle  $a \in L$  algebraisch über  $K$  sind.

**Bemerkung 3.4.2** Sei  $L/K$  eine Körpererweiterung und seien  $a_i \in L$  für  $i \in I$ . Dann ist  $K((a_i)_{i \in I})$  eine algebraische Körpererweiterung genau dann, wenn alle  $a_i$  algebraisch über  $K$  sind.

**Bemerkung 3.4.3** Ist  $L/K$  eine beliebige Körpererweiterung, so ist die Menge  $\{a \in L \mid a \text{ ist algebraisch über } K\}$  ein Unterkörper von  $L$ .

**Satz 3.4.4** Ist  $L/K$  algebraisch und  $M/L$  algebraisch, so ist auch  $M/K$  algebraisch.

**Satz 3.4.5** Für einen Körper  $K$  sind äquivalent:

- (a) Jedes nicht-konstante Polynom in  $K[X]$  hat (mindestens) eine Nullstelle in  $K$ .
- (b) Jedes Polynom in  $K[X]$  zerfällt in Linearfaktoren.
- (c) Jedes irreduzible Polynom in  $K[X]$  hat Grad 1.
- (d) Die einzige algebraische Körpererweiterung von  $K$  ist  $K$  selbst.

**Definition 3.4.6** Ein Körper  $K$ , der die Bedingungen aus Satz 3.4.5 erfüllt, heißt **algebraisch abgeschlossen**.

**Satz 3.4.7** Zu jedem Körper  $K$  gibt es eine algebraische Erweiterung  $L \supseteq K$ , die algebraisch abgeschlossen ist. Außerdem ist  $L$  eindeutig bis auf Isomorphismus

über  $K$ , d. h. ist  $L' \supseteq K$  eine weitere algebraisch abgeschlossene algebraische Erweiterung von  $K$ , so existiert ein Isomorphismus  $\phi: L \rightarrow L'$ , der auf  $K$  die Identität ist.

**Definition 3.4.8** Den Körper  $L$  aus Satz 3.4.7 nennt man den **algebraischen Abschluss** von  $K$ ; Notation für den algebraischen Abschluss:  $K^{\text{alg}}$ .

**Bemerkung 3.4.9** Ist  $L/K$  algebraisch, so existiert eine Einbettung  $\phi: L \rightarrow K^{\text{alg}}$ , die auf  $K$  die Identität ist. Anders ausgedrückt: Wir können  $L$  als Unterkörper von  $K^{\text{alg}}$  auffassen.

**Lemma 3.4.10** Ist  $L \supseteq K$  eine algebraische Erweiterung (die wir als Unterkörper von  $K^{\text{alg}}$  auffassen), so lässt sich jede Einbettung  $\phi: L \rightarrow K^{\text{alg}}$ , die auf  $K$  die Identität ist, zu einem Automorphismus von  $K^{\text{alg}}$  fortsetzen.

### 3.5 Normale Körpererweiterungen

Erinnerung an Definition 3.1.4: Ist  $L/K$  eine Körpererweiterung, so bezeichnet  $\text{Aut}(L/K)$  die Menge der Automorphismen von  $L$  über  $K$ , d. h. der Automorphismen von  $L$ , die auf  $K$  die Identität sind.

**Bemerkung 3.5.1** Ist  $K \subseteq L \subseteq M$ , so ist  $\text{Aut}(M/L)$  eine Untergruppe von  $\text{Aut}(M/K)$ .

**Satz 3.5.2** Sei  $K$  ein Körper und seien  $a_1, a_2 \in K^{\text{alg}}$ . Dann liegen  $a_1$  und  $a_2$  genau dann in der gleichen Bahn unter der Operation von  $\text{Aut}(K^{\text{alg}}/K)$  auf  $K^{\text{alg}}$ , wenn sie das selbe Minimalpolynom über  $K$  haben.

**Definition 3.5.3** Sei  $K$  ein Körper. Der **Zerfällungskörper** (über  $K$ ) eines Polynoms  $f \in K[X] \setminus \{0\}$  ist der kleinste Unterkörper  $L \subseteq K^{\text{alg}}$ , der  $K$  enthält und so dass  $f$  in  $L[X]$  in Linearfaktoren zerfällt.

**Satz 3.5.4** Ist  $f \in K[X]$  und sind  $a_1, \dots, a_n \in K^{\text{alg}}$  die Nullstellen von  $f$ , so ist  $L := K(a_1, \dots, a_n)$  der Zerfällungskörper von  $f$ . Es gilt  $[L : K] \leq n!$ .

**Bemerkung 3.5.5** Ist  $L/K$  eine Körpererweiterung und sind  $a_1, \dots, a_n$  die Nullstellen in  $L$  eines Polynoms  $f \in K[X]$ , so erhält man einen Gruppenhomomorphismus  $\text{Aut}(L/K) \rightarrow \text{Sym}(\{a_1, \dots, a_n\})$ ,  $\sigma \mapsto \sigma|_{\{a_1, \dots, a_n\}}$ .

**Satz 3.5.6** Die folgenden Bedingungen an eine endliche Körpererweiterung  $L/K$  sind äquivalent:

- (a)  $L$  ist Zerfällungskörper eines Polynoms  $f \in K[X] \setminus \{0\}$ .
- (b) Für alle  $a \in L$  zerfällt  $\text{MiPo}_{a/K}$  in  $L[X]$  in Linearfaktoren.
- (c) Jeder Automorphismus  $\sigma \in \text{Aut}(K^{\text{alg}}/K)$  bildet  $L$  auf sich selbst ab.

**Definition 3.5.7** Wenn die Bedingungen aus Satz 3.5.6 gelten, nennt man die Körpererweiterung  $L/K$  **normal**. Man sagt auch: „ $L$  ist **normal** über  $K$ “. (Ist  $L/K$  unendlich, so sind nur noch (b) und (c) äquivalent, und man verwendet dies als Definition von normal.)

**Bemerkung 3.5.8** Teil (c) von Satz 3.6.5 besagt insbesondere, dass wir einen (surjektiven) Gruppenhomomorphismus  $\text{Aut}(K^{\text{alg}}/K) \rightarrow \text{Aut}(L/K), \sigma \mapsto \sigma|_L$  haben, falls  $L/K$  normal ist. Der Kern davon ist  $\text{Aut}(K^{\text{alg}}/L)$ .

**Bemerkung 3.5.9** Sind  $K \subseteq L \subseteq M$  Körper und ist  $M/K$  normal, so ist auch  $M/L$  normal.

### 3.6 Separable Körpererweiterungen

**Satz 3.6.1** Ist  $K$  ein Körper der Charakteristik 0 und  $f \in K[X]$  irreduzibel, so hat  $f$  in  $K^{\text{alg}}$  keine mehrfachen Nullstellen (d. h. alle Linearfaktoren von  $f$  in  $K^{\text{alg}}[X]$  sind verschieden).

**Definition 3.6.2** Sei  $L/K$  eine algebraische Körpererweiterung.

- (a) Ein Element  $a \in L$  heißt **separabel** über  $K$  wenn sein Minimalpolynom  $\text{MiPo}_{a/K}$  keine mehrfachen Nullstellen in  $K^{\text{alg}}$  hat.
- (b) Die Körpererweiterung  $L/K$  heißt **separabel**, wenn alle Elemente von  $L$  separabel über  $K$  sind.

**Bemerkung 3.6.3** Nach Satz 3.6.1 ist eine algebraische Körpererweiterung  $L/K$  immer separabel, wenn  $\text{char } K = 0$  ist.

**Bemerkung 3.6.4** Sind  $K \subseteq L \subseteq M$  Körper, so gilt:  $M/K$  ist separabel genau dann, wenn  $L/K$  und  $M/L$  separabel sind.

**Satz 3.6.5** Die folgenden Bedingungen an eine endliche Körpererweiterung  $L/K$  sind äquivalent:

- (a)  $L/K$  ist separabel.
- (b)  $L = K(a_1, \dots, a_n)$  für Elemente  $a_1, \dots, a_n$ , die separabel über  $K$  sind.
- (c) Es gibt genau  $[L : K]$  viele Einbettungen von  $L$  nach  $K^{\text{alg}}$ , die auf  $K$  die Identität sind.

### 3.7 Galois-Theorie

**Definition 3.7.1** Eine Körpererweiterung  $L/K$  heißt **galoissch**, wenn sie normal und separabel ist. Man sagt auch: „ $L/K$  ist eine **Galois-Erweiterung**.“ Ist  $L/K$  galoissch, so nennt man  $\text{Aut}(L/K)$  auch die **Galois-Gruppe** von  $L/K$  (und oft schreibt man  $\text{Gal}(L/K)$  dafür).

**Satz 3.7.2** Ist  $L/K$  eine endliche galoissche Körpererweiterung, so ist  $\# \text{Aut}(L/K) = [L : K]$ .

**Definition 3.7.3** Ein **Zwischenkörper** einer Körpererweiterung  $L/K$  ist ein Körper  $F$  mit  $K \subseteq F \subseteq L$ .

**Satz 3.7.4** Ist  $L/K$  eine Körpererweiterung und  $H \subseteq \text{Aut}(L/K)$  eine Untergruppe, so ist die Menge  $F := \{a \in L \mid \forall \sigma \in H: \sigma(a) = a\}$  ein Zwischenkörper von  $L/K$ .

**Definition 3.7.5** Den Körper  $F$  aus Satz 3.7.4 nennt man den **Fixkörper** von  $H$ ; Notation dafür:  $\text{Fix}(H)$ .

**Satz 3.7.6 (Hauptsatz der Galois-Theorie)** Sei  $L/K$  eine endliche galoissche Körpererweiterung mit Galoisgruppe  $G = \text{Aut}(L/K)$ . Dann hat man eine Bijektion zwischen der Menge der Untergruppen von  $G$  und der Menge der Zwischenkörper von  $L/K$ , die gegeben ist durch  $H \mapsto \text{Fix}(H)$ . Die Umkehrabbildung ist  $F \mapsto \text{Aut}(L/F)$ .

**Definition 3.7.7** Die Bijektion aus Satz 3.7.6 heißt **Galois-Korrespondenz**.

**Satz 3.7.8** Sei  $L/K$  eine endliche Galoiserweiterung mit Galois-Gruppe  $G = \text{Aut}(L/K)$ , seien  $H, H' \subseteq G$  Untergruppen und seien  $F = \text{Fix}(H)$ ,  $F' = \text{Fix}(H')$ . Dann gilt:

- (a) Die Galois-Korrespondenz ist „inklusionsumkehrend“, d. h.  $H \subseteq H' \iff F \supseteq F'$ .
- (b)  $[L : F] = \#H$  und  $[F : K] = (G : H)$
- (c) Die Körpererweiterung  $F/K$  ist normal genau dann, wenn  $H$  ein Normalteiler von  $G$  ist. Ist dies der Fall, so hat man eine surjektive Einschränkungabbildung  $\text{Aut}(L/K) \rightarrow \text{Aut}(F/K)$ , deren Kern  $H$  ist. Insbesondere ist dann also  $\text{Aut}(F/K) \cong G/H$ .

**Beispiel 3.7.9** Sei  $p$  prim,  $\zeta_p := e^{2\pi i/p}$  und  $L := \mathbb{Q}(\zeta_p)$ . Dann ist  $[L : \mathbb{Q}]$  galoissch, und wir haben einen Isomorphismus  $\mathbb{F}_p^\times \rightarrow \text{Aut}(L/\mathbb{Q})$ , der gegeben ist durch  $k \mapsto (\zeta_p \mapsto \zeta_p^k)$ .

**Beispiel 3.7.10** Sei  $p$  prim, sei  $K$  ein Körper mit  $\zeta_p \in K$ , sei  $b \in K$  so, dass  $f(X) := X^p - b$  keine Nullstelle in  $K$  hat, und sei  $L$  der Zerfällungskörper von  $f$ . Dann ist  $\text{Aut}(L/K)$  isomorph zu  $\mathbb{Z}/p\mathbb{Z}$ .

**Satz 3.7.11 (Satz vom primitiven Element)** Ist  $L/K$  eine endliche separable Körpererweiterung, so existiert ein  $a \in L$ , so dass  $L = K(a)$  gilt.

**Satz 3.7.12** Seien  $K \subseteq L'$  Körper, seien  $L, K'$  Zwischenkörper von  $L'/K$  so, dass  $L'$  von  $L$  und  $K'$  erzeugt wird. Wir nehmen an, dass  $L/K$  endlich und galoissch ist. Dann ist auch  $L'/K'$  endlich und galoissch, und wir haben einen injektiven Gruppenhomomorphismus  $\text{Aut}(L'/K') \rightarrow \text{Aut}(L/K)$ ,  $\sigma \mapsto \sigma|_L$ . Insbesondere ist  $[L' : K']$  ein Teiler von  $[L : K]$ .

**Beispiel 3.7.13** Sei  $K \subseteq \mathbb{Q}^{\text{alg}}$  ein Körper und sei  $p$  prim. Dann ist  $K(\zeta_p)/K$  galoissch, und die Galois-Gruppe  $\text{Aut}(K(\zeta_p)/K)$  ist isomorph zu einer Untergruppe von  $\mathbb{F}_p^\times$ .

## Index

- $K(X)$ , 15
- $K^{\text{alg}}$ , 21
- $R^\times$ , 14
- $S_n$ , 4
- Aut, 5, 13
- End, 5, 13
- Gal, 22
- Hom
  - von Gruppen, 5
  - von Ringen, 13
- MiPo, 18
- $SL_n$ , 3
- $\text{Sym}(M)$ , 4
- $\cong$ , 5, 13
- im, 5
- ker, 5
- $\langle A \rangle$ , 5
- $\triangleleft$ , 6, 13
- $n$ -te Einheitswurzel, 19
- $p$ -Untergruppe, 11
  
- Abbildung
  - Evaluations-, 13
- abelsch, 3
- Additive Notation, 3
- algebraisch abgeschlossen, 20
- algebraische Körpererweiterung, 20
- algebraischer Abschluss, 21
- algebraisches Element, 18
- allgemeine lineare Gruppe, 3
- alternierende Gruppe, 10
- assoziativ, 3
- Assoziativität, 12
- assoziiert, 15
- Automorphismus
  - von Gruppen, 5
  - von Körpern, 17
  - von Ringen, 13
  
- Bahn, 11
- Bahnenformel, 11
- Bild, 5
- Brückekörper, 15
  
- Charakteristik, 17
- Chinesischer Restsatz, 8
  
- direktes Produkt
  - von Gruppen, 4
  - von Ringen, 12
- Distributivität, 12
  
- einfach, 10
- Einheit, 14
- Eisensteinsches Irreduzibilitätskriterium, 17
- Elementarteilersatz, 8
- endlich erzeugt, 5
- endliche Körpererweiterung, 18
- Endomorphismus
  - von Gruppen, 5
  - von Ringen, 13
- erzeugen, 5
- Erzeuger, 5
- erzeugte Untergruppe, 5
- erzeugter Unterkörper, 18
- erzeugtes Ideal, 14
- Evaluationsabbildung, 13
  
- Faktorgruppe, 7
- faktoriell, 16
- Faktorring, 14
- festhalten, 11
- Fixkörper, 23
  
- Galois-Erweiterung, 22
- Galois-Gruppe, 22
- Galois-Korrespondenz, 23
- galoissch, 22
- Grad, 12
  - einer Körpererweiterung, 18
  - eines algebraischen Elements, 18
- Gruppe, 3
  - Galois-Gruppe, 22
- Gruppenautomorphismus, 5
- Gruppenendomorphismus, 5
- Gruppenhomomorphismus, 5
- Gruppenisomorphismus, 5
- Gruppenoperation, 10
- Gruppenwirkung, 10
  
- Hauptideale, 14
- Hauptidealring, 16
- Hauptsatz der Galois-Theorie, 23
- Homomorphismus
  - Gruppenhomomorphismus, 5



Ringhomomorphismus, 13  
 von Körpern, 17

Ideal, 13  
 maximales, 14

Index, 7

integer, 15

Integritätsbereich, 15

Inverses, 3

irreduzibel, 15

Irreduzibilitätskriterium  
 von Eisenstein, 17

isomorph, 5, 13

Isomorphiesatz, 7, 14  
 für Gruppen, 7  
 für Ringe, 14

Isomorphismus  
 von Gruppen, 5  
 von Körpern, 17  
 von Ringen, 13

Kern, 5

kleinsche Vierergruppe, 10

kleinste Menge, 5

kommutativ, 3

kommutativer Ring, 12

Konjugation, 6

konstruierbar, 19  
 mit Zirkel und lineal, 19

Körperautomorphismus, 17

Körpererweiterung, 17  
 normale, 21

Körperhomomorphismus, 17

Körperisomorphismus, 17

Linksnebenklasse, 6

maximales Ideal, 14

mit Zirkel und Lineal konstruierbar, 19

modulo, 7, 14

Monom, 12

Multiplikative Notation, 3

Nebenklassen, 6

normale Körpererweiterung, 21

normale Untergruppe, 6

Normalteiler, 6

normiert, 12

nullteilerfrei, 15

Oberkörper, 17

Ordnung, 7

Permutation, 4

Permutationsmatrix, 9

Polynom, 12

Polynomring, 12

Primfaktorzerlegung, 16

primitiv, 16

primitive  $n$ -te Einheitswurzel, 19

primitives Element, 23

Primkörper, 18

Produkt  
 direktes  
 von Gruppen, 4  
 von Ringen, 12

Quotientengruppe, 7

Quotientenkörper, 15

Quotientenring, 14

Rechtsnebenklasse, 6

Restklassenring, 14

Ring, 12

Ringautomorphismus, 13

Ringendomorphismus, 13

Ringhomomorphismus, 13

Ringisomorphismus, 13

Satz  
 Chinesischer Restsatz  
 für Gruppen, 8

Eisensteinsches Irreduzibilitätskriterium, 17

Elementarteilersatz, 8

Hauptsatz der Galois-Theorie, 23

Isomorphiesatz  
 für Gruppen, 7  
 für Ringe, 14

Klassifikation der endlich erzeugten abelschen Gruppen, 9

von Cauchy, 12

Satz vom primitiven Element, 23

Satz von Cayley, 10

Satz von Gauß, 16

Satz von Lagrange, 7

separabel, 22

Signum, 9

Stabilisator, 11

stabilisieren, 11

Sylow- $p$ -Untergruppe, 11

Sylow-Sätze, 11  
symmetrische Gruppe, 4

teilen, 8, 15  
Teiler, 8, 15  
teilerfremd, 15  
transitiv, 11  
Transposition, 9  
transzendentes Element, 18  
triviale Untergruppe, 4  
Träger, 9

Untergruppe, 4  
Unterkörper, 17  
Unterring, 13

Vielfaches, 15

Zerfallungskörper, 21  
Zwischenkörper, 22  
Zykelzerlegung, 9  
zyklisch, 5  
Zyklus, 9