Elemente der Algebra, Vorlesungsskript

Irene I. Bouw

Wintersemester 2014/2015

Inhaltsverzeichnis

1 Gruppen

Gruppen kommen „in der Natur“ als Symmetriegruppen vor. Die Gruppentheorie ist deshalb sowohl in der Mathematik als auch in den Naturwissenschaften ein wichtiges Werkzeug. Symmetriegruppen sind die wichtigsten Beispiele von Gruppen, die wir in diesem Kapitel betrachten werden.

1.1 Die Definition einer Gruppe

Definition 1.1.1 Eine *Gruppe* ist eine Menge G zusammen mit einer Verknüpfung

$$G \times G \to G, \qquad (a, b) \mapsto a * b,$$

welche die folgenden Eigenschaften besitzt:

(G1) Die Verknüpfung ist *assoziativ*, d.h. $(a * b) * c = a * (b * c)$, für alle $a, b, c \in G$.

(G2) Es existiert ein *neutrales Element*, d.h. ein Element $e \in G$ mit $e * a = a * e = a$ für alle $a \in G$.

(G3) Jedes Element $a \in G$ besitzt ein *inverses Element*, d.h. es existiert ein Element $b \in G$ mit $a * b = b * a = e$.

Eine Gruppe G heißt *abelsch* (oder *kommutativ*), falls $a * b = b * a$ für alle $a, b \in G$ gilt.

Bemerkung 1.1.2 (a) Die Definition einer Gruppe setzt voraus, dass die Verknüpfung $a * b$ zweier Gruppenelemente wieder ein Gruppenelement ist. Die Bedingung

(G0) Für alle $a, b \in G$ gilt $a * b \in G$ (*Abgeschlossenheit gegenüber der Verknüpfung*)

ist daher implizit in Definition 1.1.1 enthalten.

(b) Im Allgemeinen werden wir für Gruppen die *multiplikative Schreibweise* $(G, \cdot)$ benutzen. Wir schreiben $a \cdot b$ (oder kurz ab) für die Verknüpfung, $1 = 1_G$ für das neutrale Element und a^{-1} für das inverse Element zu a.

Für abelsche Gruppen $(G, +)$ benutzen wir manchmal auch die *additive Schreibweise*. Wir schreiben $a + b$ für die Verknüpfung, $-a$ für das inverse Element (genannt: *Negatives*) und $0 = 0_G$ für das neutrale Element (genannt: *Null*).

Beispiel 1.1.3 Wir geben einige Beispiele von Gruppen, die Ihnen aus der Vorlesung Lineare Algebra bekannt sind. Überzeugen Sie sich davon, dass dies Gruppen sind und bestimmen Sie das neutrale Element und das inverse Element zu $a \in G$.

(a) Die Mengen $\mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}$ mit Addition sind abelsche Gruppen.

(b) Sei K ein Körper. Die Menge $K^* := K \setminus \{0\}$ mit Multiplikation ist eine Gruppe.

(c) Sei K ein Körper. Die Menge $\mathrm{GL}_n(K)$ der invertierbaren $n \times n$ Matrizen mit Koeffizienten in K ist eine Gruppe unter Matrixmultiplikation. Die Abgeschlossenheit bezüglich der Multiplikation (G0) folgt aus

$$\det(AB) = \det(A)\det(B) \neq 0 \quad \text{für alle } A, B \in \mathrm{GL}_n(K).$$

Diese Gruppe ist nicht abelsch für $n \geq 2$.

(d) Die Menge $\mathrm{GL}_n(K)$ ist keine Gruppe bezüglich Addition.

Das folgende Lemma zeigt einige einfache Eigenschaften einer Gruppe.

Lemma 1.1.4 *Sei $(G, \cdot)$ eine Gruppe.*

(a) Falls $e' \cdot a = a$ für alle $a \in G$, so ist $e' = e$ das neutrale Element von G.

(b) Falls $b \in G$ die Gleichung $b \cdot a = e$ erfüllt, so ist $b = a^{-1}$ das Inverse von a.

(c) Das neutrale Element e ist eindeutig bestimmt. Jedes Element besitzt ein eindeutiges inverses Element.

(d) (Kürzungssatz) Seien $a, b, c \in G$. Falls $ab = ac$ oder $ba = ca$, so gilt $b = c$.

Beweis: Sei e' wie in (a) und sei e das neutrale Element von G. Wegen Gruppenaxiom (G2) gilt $e' = e' \cdot e$. Die Definition von e' impliziert, dass $e' \cdot e = e$. Also gilt $e' = e$. Teil (b) folgt, indem man die Gleichung $b \cdot a = e$ von rechts mit a^{-1} multipliziert. Teil (c) ist ein Spezialfall von (a) und (b). Für (d) multipliziert man beide Seiten der Gleichung von rechts mit a^{-1}. □

Beispiel 1.1.5 Der Beweis von Lemma 1.1.4.(d) benutzt Axiom (G3). Die Menge $M_{2,2}(\mathbb{R})$ der reellen 2×2 Matrizen mit Matrixmultiplikation als Verknüpfung ist keine Gruppe, da nicht jedes Element ein inverses Element besitzt. Lemma 1.1.4.(d) gilt nicht:

$$\begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} \begin{pmatrix} 1 & 0 \\ 2 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} \begin{pmatrix} 1 & 0 \\ 0 & 3 \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}, \quad \text{aber } \begin{pmatrix} 1 & 0 \\ 2 & 1 \end{pmatrix} \neq \begin{pmatrix} 1 & 0 \\ 0 & 3 \end{pmatrix}$$

Definition 1.1.6 Seien G und H Gruppen. Das *direkte Produkt* $G \times H$ ist die Menge

$$G \times H = \{(g, h) \mid g \in G, h \in H\}$$

von Elementen in G und H. Dies ist eine Gruppe mit Verknüpfung:

$$(g, h) \cdot (g', h') = (g \cdot_G g', h \cdot_H h').$$

Das neutrale Element ist (e_G, e_H). Das inverse Element von (g, h) ist (g^{-1}, h^{-1}).

Definition 1.1.7 Sei G eine Gruppe. Eine Teilmenge $H \subset G$ heißt *Untergruppe* von G, falls:

(U1) $e \in H$,

(U2) für alle $a, b \in H$ gilt $a \cdot b \in H$,

(U3) für alle $a \in H$ gilt $a^{-1} \in H$.

Bezeichnung: $H < G$.

Bemerkung 1.1.8 (a) Eine Untergruppe H von G ist mit der Verknüpfung von G eine Gruppe: Die Assoziativität von H folgt aus der Assoziativität von G. Dies braucht man also nicht mehr zu überprüfen.

(b) Die Untergruppenaxiome (U2) und (U3) kann man auch ersetzen durch:

(U2+3) Für alle $a, b \in H$ gilt $a \cdot b^{-1} \in H$.

Beispiel 1.1.9 (a) Sei T die Menge der invertierbaren, reellen, 2×2 oberen Dreiecksmatrizen:

$$T = \left\{ \begin{pmatrix} a & b \\ 0 & d \end{pmatrix} \mid a, b, d \in \mathbb{R},\, ad \neq 0 \right\}.$$

Dies ist eine Untergruppe von $\mathrm{GL}_2(\mathbb{R})$: Seien

$$A_i = \begin{pmatrix} a_i & b_i \\ 0 & d_i \end{pmatrix} \in T, \quad \text{für } i = 1, 2.$$

Es gilt

$$A_1 \cdot A_2 = \begin{pmatrix} a_1 a_2 & a_1 b_2 + b_1 d_2 \\ 0 & d_1 d_2 \end{pmatrix} \in T, \qquad A_1^{-1} = \frac{1}{a_1 d_1} \begin{pmatrix} d_1 & -b_1 \\ 0 & a_1 \end{pmatrix} \in T.$$

Außerdem ist die Einheitsmatrix ein Element von T.

(b) Der Einheitskreis $S := \{z \in \mathbb{C} \mid |z| = 1\}$ ist eine Untergruppe von $\mathbb{C}^*$.

(c) Sei K ein Körper. Die Gruppe $\mathrm{SL}_n(K)$ der invertierbaren Matrizen mit Determinante 1 ist eine Untergruppe von $\mathrm{GL}_n(K)$.

Satz 1.1.10 *Sei G eine Gruppe und S eine Teilmenge. Dann ist die Menge*

$$H = \langle S \rangle := \{a_1 \cdot a_2 \cdots a_n \mid n \in \mathbb{Z}_{\geq 0},\, \forall i : a_i \in S \text{ oder } a_i^{-1} \in S\} \subset G$$

die kleinste Untergruppe von G, die S als Teilmenge enthält. Für $n = 0$ setzt man das (leere) Produkt $a_1 \cdots a_n := e$.

Definition 1.1.11 Die Untergruppe $H = \langle S \rangle < G$ heißt die *von S erzeugte Untergruppe*. Die Teilmenge S heißt *Erzeugendensystem* von H.

Beweis des Satzes: Seien a, b Elemente von H. Dann gilt nach Definition

$$a = a_1 \cdots a_n, \quad b = b_1 \cdots b_m,$$

mit $n, m \geq 0$, $a_i \in S$ oder $a_i^{-1} \in S$ für alle i und $b_j \in S$ oder $b_j^{-1} \in S$ für alle j. Offenbar ist

$$a \cdot b^{-1} = a_1 \cdots a_n \cdot b_m^{-1} \cdots b_1^{-1}$$

wieder ein Element von H. Mit Bemerkung 1.1.8. (b) folgt, dass H eine Untergruppe von G ist, die S als Teilmenge enthält.

Ist nun $H' < G$ eine weitere Untergruppe, die S als Teilmenge enthält, so enthält H' auch jedes Element der Form $a_1 \cdots a_n$, wenn für alle i entweder a_i oder a_i^{-1} in S (und damit in H') liegen. Es gilt also $H \subset H'$. Damit ist alles gezeigt. □

Definition 1.1.12 Eine *zyklische Gruppe* ist eine Gruppe, die von einem Element erzeugt wird. Ein solches Element heißt *Erzeuger* der Gruppe.

Bemerkung 1.1.13 Jede zyklische Gruppe G ist auch abelsch. Sei nämlich g ein Erzeuger von G. Es gilt $g^i g^j = g^{i+j} = g^j g^i$.

Definition 1.1.14 Sei G eine Gruppe. Die *Ordnung* $|G|$ der Gruppe ist die Anzahl der Elemente von G. Eine Gruppe endlicher Ordnung heißt *endliche Gruppe*. Falls $g \in G$ ein Element ist, so heißt die Ordnung der Untergruppe $\langle g \rangle$, erzeugt von g, die *Ordnung* von g. Bezeichnung: $\mathrm{ord}(g)$.

Alternativ kann man die Ordnung eines Elements g einer Gruppe G auch definieren als die kleinste positive Zahl n mit $g^n = e_G$.

Beispiel 1.1.15 (a) Die Gruppe $(\mathbb{Z}, +)$ ist eine zyklische Gruppe. Erzeuger sind 1 oder -1. Die Ordnung der Gruppe ist unendlich.

(b) Sei $n \in \mathbb{N}$. Eine *n-te Einheitswurzel* ist eine komplexe Zahl $z \in \mathbb{C}$ mit $z^n = 1$. Die Menge aller n-ten Einheitswurzeln,

$$\mu_n := \{\, z \in \mathbb{C} \mid z^n = 1 \,\},$$

versehen mit der Multiplikation komplexer Zahlen, bildet eine kommutative Gruppe. (Warum?) Sie ist zyklisch, denn

$$\mu_n = \{\, e^{2\pi i k/n} \mid k \in \mathbb{Z} \,\} = \langle e^{2\pi i/n} \rangle.$$

Die Ordnung eines Elements $e^{2\pi i k/n}$ ist $n/\operatorname{ggT}(k, n)$. Insbesondere ist $\operatorname{ord}(e^{2\pi i k/n})$ genau dann n, wenn $\operatorname{ggT}(k, n) = 1$. Die Einheitswurzel der Ordnung n heißen *primitive n-te Einheitswurzel*.

(c) Sei

$$V := \left\{ \begin{pmatrix} \pm 1 & 0 \\ 0 & \pm 1 \end{pmatrix} \right\} \subset \mathrm{GL}_2(\mathbb{R}).$$

Man zeigt leicht, dass V eine Untergruppe von $\mathrm{GL}_2(\mathbb{R})$ mit 4 Elementen ist. Die Gruppe V heißt *Kleinsche Vierergruppe*. Jedes Element $A \in V$ ungleich der Einheitsmatrix E besitzt Ordnung 2, also ist V nicht zyklisch. Die Matrizen

$$A_1 = \begin{pmatrix} -1 & 0 \\ 0 & 1 \end{pmatrix}, \qquad A_2 = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$$

bilden einen Erzeugendensystem von V.

Das einfachste Beispiel einer Gruppe ist $(\mathbb{Z}, +)$. Theorem 1.1.16 bestimmt alle Untergruppen von $(\mathbb{Z}, +)$. (Dieser Beweis ist dem Beweis von [4, Lemma 1.1.9] sehr ähnlich.)

Der Beweis von Theorem 1.1.16 benutzt *Division mit Rest*: Seien $a, b \in \mathbb{Z}$ mit $b \neq 0$. Es existieren eindeutige Zahlen $q, r \in \mathbb{Z}$ mit $a = qb + r$ und $0 \leq r < |b|$. Die Zahl q heißt *Quotient* und r heißt *Rest*. Den Quotient q kann man als die größte ganze Zahl kleiner gleich a/b charakterisieren. Den Rest definiert man als $r := a - qb$. Mehr Details finden Sie in [4, Satz 1.1.5].

Theorem 1.1.16 *Für $b \in \mathbb{Z}$ definieren wir*

$$b\mathbb{Z} = \langle b \rangle = \{n \in \mathbb{Z} \mid n = bk \text{ für ein } k \in \mathbb{Z}\}.$$

Jede Untergruppe H von $\mathbb{Z}$ ist von der Form $H = b\mathbb{Z}$ für ein $b \in \mathbb{Z}_{\geq 0}$.

Beweis: Sei $H < (\mathbb{Z}, +)$ eine Untergruppe. Es gilt $0 \in H$ (Axiom (U1)). Falls 0 das einzige Element von H ist, gilt $H = 0\mathbb{Z} = \{0\}$.

Wir nehmen an, dass $H \neq \{0\}$ ist. Axiom (U3) impliziert, dass falls $a \in H$ mit $a \neq 0$ auch $-a \in H$. Daher enthält H mindestens eine positive Zahl. Sei b das kleinste positive Element von H.

Wir behaupten, dass $H = b\mathbb{Z}$. Die Inklusion $b\mathbb{Z} \subset H$ ist klar. Wir müssen also zeigen, dass jedes Element von H ein Vielfaches von b ist.

Sei $a \in H$ beliebig. Division mit Rest impliziert die Existenz von Zahlen q, r mit $a = qb + r$ und $0 \leq r < b$. Axiom (U2+3) impliziert, dass $r = a - qb \in H$ ist. Die Minimalität von b zusammen mit der Eigenschaft $0 \leq r < b$ impliziert, dass $r = 0$. Also ist $a = qb$ und es folgt, dass $H = b\mathbb{Z}$. □

Theorem 1.1.16 sagt also, dass jede Untergruppe von $\mathbb{Z}$ zyklisch ist. Dies impliziert folgende überraschende Tatsache. Seien $a, b \in \mathbb{Z}$ zwei verschiedene Elemente

ungleich 0. Die Untergruppe $\langle a, b\rangle = a\mathbb{Z} + b\mathbb{Z} = \{n \in \mathbb{Z} \mid n = ax + by, \text{ für } x, y \in \mathbb{Z}\}$ ist wieder zyklisch, also existiert ein $d \in \mathbb{Z}$ mit $a\mathbb{Z} + b\mathbb{Z} = d\mathbb{Z}$. Man kann sogar annehmen, dass $d > 0$ ist. Diese Zahl d nennt man den *größten gemeinsamen Teiler* von a und b. Bezeichnung: $d = \mathrm{ggT}(a, b)$. Zwei Zahlen mit $\mathrm{ggT}(a, b) = 1$ nennt man *teilerfremd*. Der größte gemeinsame Teiler hat die folgenden Eigenschaften (siehe auch [4, § 1.1]):

Korollar 1.1.17 *Seien $a, b \in \mathbb{Z}$ und sei $d = \mathrm{ggT}(a, b)$.*

(a) Es existieren $x, y \in \mathbb{Z}$ mit $d = ax + by$.

(b) d teilt sowohl a als auch b.

(c) Jeder gemeinsame Teiler von a und b teilt auch d.

Beweis: Teil (a) folgt aus $d \in a\mathbb{Z} + b\mathbb{Z}$. Teil (b) folgt aus $a, b \in d\mathbb{Z}$. Teil (c) folgt aus (a). □

Beispiel 1.1.18 Sei $a = 60$ und $b = 36$. Es gilt $d = \mathrm{ggT}(a, b) = 12$. Theorem 1.1.16 impliziert, dass $x, y \in \mathbb{Z}$ existieren mit $12 = 60x + 36y$. Man überprüft, dass $12 = 36 \cdot 2 - 60 \cdot 1$. Ein Algorithmus, der diese Zahlen berechnet, ist der erweiterte euklidische Algorithmus (siehe [4, § 1.1]).

1.2 Permutationen

Sei X eine endliche Menge. Eine *Permutation* von X ist eine Bijektion $\sigma : X \to X$. Die Menge $S(X)$ der Permutationen mit Komposition von Abbildungen als Verknüpfung ist eine Gruppe. Wir nennen $S(X)$ die *symmetrische Gruppe*. Die Identität

$$\mathrm{Id}_X : X \to X, \qquad x \mapsto x$$

ist das neutrale Element von $S(X)$. Das inverse Element von $\sigma \in S(X)$ ist die Umkehrfunktion. Diese existiert, da σ bijektiv ist.

Die Elemente von $S(X)$ heißen *Permutationen* der Menge X. Ist $X = \{1, 2, \ldots, n\}$, schreiben wir S_n statt $S(X)$. Diese Gruppe heißt die *symmetrische Gruppe* auf n Elemente.

Die Elemente von $\sigma \in S_n$ schreiben wir als Tabelle:

$$\begin{pmatrix} 1 & 2 & \cdots & n \\ \sigma(1) & \sigma(2) & \cdots & \sigma(n) \end{pmatrix}.$$

Die obere Zeile besteht aus den Elemente $1, 2 \ldots, n$ der Menge X. Die untere Zeile besteht aus den Bilder $\sigma(1), \sigma(2), \ldots \sigma(n)$. Beispielsweise sind die Elemente von S_3:

$$e = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix}, \quad a := \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}, \quad b := \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix},$$
$$c := \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix}, \quad d := \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}, \quad d^{-1} := \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}.$$

Die Menge S_3 hat also 6 Elemente.

Eine Permutation $\sigma \in S_n$ wird bestimmt durch den Vektor $(\sigma(1), \sigma(2), \ldots, \sigma(n))$. Jede Zahl aus der Menge $\{1, 2, \ldots, n\}$ kommt in diesem Vektor genau einmal vor. Dies zeigt folgendes Lemma:

Lemma 1.2.1 *Die Gruppe S_n besitzt genau $n!$ Elemente.*

Bemerkung 1.2.2 In dieser Vorlesung verknüpfen wir Permutationen $\sigma, \tau \in S_n$ wie Funktionen auf X: Also $\sigma \cdot \tau$ heißt: *zuerst* τ, *dann* σ ausführen. Wir folgen hiermit Armstrong [2]. Artin [1] macht dies anders!

Zum Beispiel ist

$$\begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix} \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}, \text{ und}$$
$$\begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix} \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix}.$$

Insbesondere ist die Gruppe S_n für $n \geq 3$ nicht abelsch.

Die Verknüpfung von S_3 ist in der folgenden *Verknüpfungstabelle* dargestellt:

$\sigma \cdot \tau$	e	a	b	c	d	d^{-1}
e	e	a	b	c	d	d^{-1}
a	a	e	d	d^{-1}	b	c
b	b	d^{-1}	e	d	c	a
c	c	d	d^{-1}	e	a	b
d	d	c	a	b	d^{-1}	e
d^{-1}	d^{-1}	b	c	a	e	d

Die oben eingeführte Schreibweise für Permutationen ist in der Praxis etwas zu umständlich. Daher führen wir eine kürzere Schreibweise ein.

Definition 1.2.3 Eine Permutation $\sigma \in S_n$ heißt *m-Zyklus*, wenn paarweise verschiedene Elemente $a_1, \ldots, a_m \in \{1, \ldots, n\}$ mit

$$\begin{cases} \sigma(a_j) = a_{j+1}, & \text{für } j = 1, \ldots, m-1, \\ \sigma(a_m) = a_1, & \\ \sigma(a) = a & \text{für } a \notin \{a_1, \ldots, a_m\} \end{cases}$$

existieren. Bezeichnung: $\sigma = (a_1\ a_2\ \cdots\ a_m)$.

Ein 2-Zyklus heißt auch *Transposition*.

Beispiel 1.2.4 Die symmetrische Gruppe S_3 enthält neben der Identität genau drei Transpositionen,

$$(1\ 2) = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}, \quad (2\ 3) = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}, \quad (1\ 3) = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix},$$

und zwei 3-Zyklen,

$$(1\ 2\ 3) = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}, \quad (1\ 3\ 2) = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}.$$

Bemerkung 1.2.5 (a) Sei $\sigma = (a_1\ a_2\ \cdots\ a_m)$. Das inverse Element ist $\sigma^{-1} = (a_m\ a_{m-1}\ \cdots\ a_1)$.

(b) Seien $\sigma = (a_1\ a_2\ \cdots\ a_m)$ und $\tau = (b_1\ b_2\ \cdots\ b_k)$ *disjunkte Zyklen*, d.h. es gilt

$$\{a_1, \ldots, a_m\} \cap \{b_1, \ldots, b_k\} = \emptyset.$$

Dann kommutieren beide Elemente:

$$\sigma \circ \tau = \tau \circ \sigma.$$

Das Beispiel aus Bemerkung 1.2.2 zeigt, dass dies im Allgemeinen nicht gilt, wenn die Zyklen nicht disjunkt sind.

Satz 1.2.6 *Sei $n \geq 2$. Jede Permutation $\sigma \in S_n$ lässt sich als Produkt disjunkter Zyklen schreiben.*

Beweis: Sei $\sigma \in S_n$. Wir definieren eine Äquivalenzrelation auf $X := \{1, 2, \ldots, n\}$ durch

$$x \sim_\sigma y \qquad :\Leftrightarrow \qquad \exists k \geq 0 : \; y = \sigma^k(x).$$

Man zeigt leicht, dass dies in der Tat ein Äquivalenzrelation ist. Es folgt, dass X die disjunkte Vereinigung der Äquivalenzklassen ist. Jede Äquivalenzrelation entspricht einem Zyklus. □

Beispiel 1.2.7 Als Beispiel betrachten wir

$$\sigma := \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 7 & 5 & 2 & 4 & 3 & 1 & 6 \end{pmatrix} \in S_7.$$

Die Äquivalenzklassen der Relation $\sim_\sigma$ sind

$$\{1, 7, 6\}, \qquad \{2, 5, 3\}, \qquad \{4\}.$$

Die Zyklenzerlegung ist daher

$$\sigma = (1\ 7\ 6)(2\ 5\ 3)(4).$$

Häufig lässt man in dieser Darstellung die 1-Zyklen weg und schreibt

$$\sigma = (1\ 7\ 6)(2\ 5\ 3).$$

Die Zyklenzerlegung ist nicht eindeutig. Beispielsweise gilt

$$(1\ 7\ 6) = (7\ 6\ 1) = (6\ 1\ 7).$$

In der Zyklenzerlegung sind alle vorkommenden Zyklen per Definition disjunkt. Also ist die Reihenfolge, in der die Zyklen vorkommen, egal (Bemerkung 1.2.5.(b)). Beispielsweise ist

$$\sigma = (1\ 7\ 6)(2\ 5\ 3) = (3\ 2\ 5)(6\ 1\ 7).$$

Das folgende Lemma ist eine gute Übung für das Verknüpfen von Permutationen; Wir überlassen es dem Leser/der Leserin.

Lemma 1.2.8 *(a) Die Ordnung eines k-Zyklus ist k.*

(b) Sei $\sigma = \prod_i \sigma_i$ das Produkt disjunkter Zyklen, wobei σ_i die Länge k_i besitzt. Die Ordnung von σ ist $\mathrm{kgV}(k_i)$.

Theorem 1.2.9 *Die Transpositionen in S_n erzeugen S_n.*

Beweis: Wir müssen zeigen, dass jedes Element von S_n ein Produkt von Transpositionen ist. Wir haben schon gesehen, dass jede Permutation $\sigma \in S_n$ das Produkt von disjunkten Zyklen ist. Das Theorem folgt daher aus der Formel

$$(a_1\ a_2\ \cdots\ a_k) = (a_1\ a_k)(a_1\ a_{k-1}) \cdots (a_1\ a_3)(a_1\ a_2). \tag{1.2.1}$$

□

Beispiel 1.2.10 Wir haben

$$(1\ 5\ 3)(2\ 4\ 6) = (1\ 3)(1\ 5)(2\ 6)(2\ 4).$$

Eine Permutation kann in vielen verschiedenen Weisen als Produkt von Transpositionen geschrieben werden. Zum Beispiel ist $(a\ b) = (1\ a)(1\ b)(1\ a)$. Die Anzahl der benötigten Permutationen ist immer entweder gerade oder ungerade. Um die beide Fälle zu unterscheiden, führen wir das Vorzeichen einer Permutation ein.

Dazu betrachten wir das Polynom

$$P(x_1, x_2, \ldots, x_n) = \prod_{1 \le i < j \le n} (x_i - x_j) \in \mathbb{Q}[x_1, \ldots, x_n].$$

Für $\sigma \in S_n$ definieren wir

$$\sigma(P) := \prod_{1 \le i < j \le n} (x_{\sigma(i)} - x_{\sigma(j)}).$$

Die Terme von $\sigma(P)$ sind bis auf das Vorzeichen genau die Gleichen wie die von P. Dies impliziert, dass $\sigma(P) = \pm P$.

Definition 1.2.11 Sei $\sigma \in S_n$. Das *Signum* $\operatorname{sgn}(\sigma) \in \{\pm 1\}$ ist definiert durch die Gleichung

$$\sigma(P) = \operatorname{sgn}(\sigma) P.$$

Eine Permutation $\sigma \in S_n$ heißt *gerade* (bzw. *ungerade*), wenn $\operatorname{sgn}(\sigma) = 1$ (bzw. $\operatorname{sgn}(\sigma) = -1$).

Zum Beispiel gilt für $\sigma = (1\ 3\ 2)$, dass

$$P = (x_1 - x_2)(x_1 - x_3)(x_2 - x_3) \qquad \sigma(P) = (x_3 - x_1)(x_3 - x_2)(x_1 - x_2) = P,$$

also ist σ eine gerade Permutation.

Lemma 1.2.12 *(a) Für $\sigma, \tau \in S_n$ gilt* $\operatorname{sgn}(\sigma\tau) = \operatorname{sgn}(\sigma)\operatorname{sgn}(\tau)$.

(b) Ist σ das Produkt von k Transpositionen, dann gilt $\operatorname{sgn}(\sigma) = (-1)^k$.

(c) Ist σ ein k-Zyklus, dann ist $\operatorname{sgn}(\sigma) = (-1)^{k+1}$. *Insbesondere ist ein k-Zyklus genau dann gerade, wenn k ungerade ist.*

Beweis: Es gilt

$$\begin{aligned}(\sigma \circ \tau)(P) &= \sigma(\tau(P)) = \sigma(\operatorname{sgn}(\tau)(P)) \\ &= \operatorname{sgn}(\tau)\sigma(P) = \operatorname{sgn}(\tau)\operatorname{sgn}(\sigma)(P).\end{aligned}$$

Teil (a) folgt.

Für eine Transposition τ gilt offensichtlich $\operatorname{sgn}(\tau) = -1$. Teil (b) folgt daher direkt aus (a). Teil (c) folgt aus (a), (b) und Theorem 1.2.9. □

Lemma 1.2.13 *Die Menge*

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

der geraden Permutationen ist eine Untergruppe von S_n. Die Untergruppe A_n heißt alternierende Gruppe.

Beweis: Die Definition von sgn impliziert, dass $\operatorname{sgn}(e) = 1$, also ist $e \in A_n$. Lemma 1.2.12.(a) impliziert, dass A_n gegenüber der Verknüpfung abgeschlossen ist. Sei $\sigma \in A_n$ und σ^{-1} das inverse Element von $\sigma \in S_n$. Es gilt $1 = \operatorname{sgn}(e) = \operatorname{sgn}(\sigma \cdot \sigma^{-1}) = \operatorname{sgn}(\sigma) \cdot \operatorname{sgn}(\sigma^{-1})$. Also ist $\operatorname{sgn}(\sigma^{-1}) = \operatorname{sgn}(\sigma) = 1$. Wir schließen, dass A_n eine Untergruppe von S_n ist. □

1.3 Gruppenhomomorphismen

Definition 1.3.1 Es seien G und H Gruppen. Ein *Gruppenhomomorphismus* ist eine Abbildung $\varphi : G \to H$, sodass $\varphi(a \cdot_G b) = \varphi(a) \cdot_H \varphi(b)$ für alle $a, b \in G$ gilt.

Beispiel 1.3.2 (a) Sei K ein Körper. Die Determinante $\det : \mathrm{GL}_n(K) \to K^*$ ist ein Gruppenhomomorphismus, da $\det(AB) = \det(A)\det(B)$ ist.

(b) Die Abbildung $\psi_n : \mathbb{C}^* \to \mathbb{C}^*, \quad z \mapsto z^n$ ist ein Gruppenhomomorphismus.

(c) Die Abbildung $\mathrm{sgn} : S_n \to \{\pm 1\}$ ist ein Gruppenhomomorphismus.

(d) Die Abbildung $\exp : \mathbb{R} \to \mathbb{R}^*$ ist ein Gruppenhomomorphismus, da $\exp(x + y) = \exp(x)\exp(y)$ ist.

Die folgenden Eigenschaften folgen unmittelbar aus der Definition.

Lemma 1.3.3 *Sei $\varphi : G \to H$ ein Gruppenhomomorphismus.*

(a) $\varphi(e_G) = e_H$.

(b) $\varphi(a^{-1}) = \varphi(a)^{-1}$.

(c) Ist φ bijektiv, so ist die Umkehrabbildung $\varphi^{-1} : H \to G$ auch ein Gruppenhomomorphismus. In diesem Fall nennt man φ einen Gruppenisomorphismus *und die Gruppen G und H heißen* isomorph *(Bezeichnung: $G \simeq H$).*

Beweis: In G gilt $e_G = e_G \cdot_G e_G$, also auch

$$\varphi(e_G) = \varphi(e_G \cdot e_G) = \varphi(e_G) \cdot \varphi(e_G).$$

Bei der letzten Gleichheit haben wir Definition 1.3.1 benutzt. Teil (a) folgt, indem man beide Seiten mit dem inversen Element $\varphi(e_G)^{-1}$ von $\varphi(e_G)$ in H multipliziert.

Teil (b) folgt ähnlich aus $a \cdot_G a^{-1} = e_G$.

Wir beweisen (c). Seien dazu $x, y \in H$ beliebig. Da $\varphi : G \to H$ bijektiv ist, existieren eindeutige Elemente $a, b \in G$ mit $\varphi(a) = x$ und $\varphi(b) = y$. Da φ ein Gruppenhomomorphismus ist, gilt $\varphi(a \cdot_G b) = \varphi(a) \cdot_H \varphi(b) = x \cdot_H y$. Also gilt

$$\varphi^{-1}(x) \cdot_G \varphi^{-1}(y) = a \cdot_G b = \varphi^{-1}(x \cdot_H y).$$

□

Beispiel 1.3.4 Seien $G = \langle g \rangle$ und $H = \langle h \rangle$ zwei zyklische Gruppen der Ordnung n. Die Abbildung

$$\varphi : G \to H, \qquad g^i \mapsto h^i.$$

ist ein bijektiver Gruppenisomorphismus. Also sind G und H isomorph.

Definition 1.3.5 Sei $\varphi : G \to H$ ein Gruppenhomomorphismus. Der *Kern* von φ ist die Teilmenge $\ker(\varphi) = \{a \in G \mid \varphi(a) = e_H\}$ von G. Das *Bild* von φ ist die Teilmenge $\mathrm{im}(\varphi) = \{x \in H \mid \exists a \in G, x = \varphi(a)\}$ von H.

Man überprüft leicht, dass $\ker(\varphi) < G$ und $\mathrm{im}(\varphi) < H$ Untergruppen sind.

Beispiel 1.3.6 Wir berechnen den Kern und das Bild der Gruppenhomomorphismen aus Beispiel 1.3.2:

(a) $\ker(\det) = \mathrm{SL}_n(K) = \{A \in \mathrm{GL}_n(K) \mid \det(A) = 1\}$ und $\mathrm{im}(\det) = K^*$.

(b) $\ker(\psi_n) = \mu_n$, die Gruppe der n-ten Einheitswurzeln. Wir behaupten, dass ψ_n surjektiv ist, also $\mathrm{im}(\psi_n) = \mathbb{C}^*$. Sei dazu $w \in \mathbb{C}^*$. Wir schreiben $w = re^{i\alpha}$ in Polarkoordinaten und definieren $z = r^{1/n}e^{i\alpha/n}$. Nun gilt $\psi_n(z) = z^n = w$. Also ist ψ_n surjektiv.

(c) $\ker(\mathrm{sgn}) = A_n$ und $\mathrm{im}(\mathrm{sgn}) = \{\pm 1\}$.

(d) $\ker(\exp) = \{0\}$ und $\mathrm{im}(\exp) = \mathbb{R}_{>0}$.

Lemma 1.3.7 *Ein Gruppenhomomorphismus $\varphi : G \to H$ ist genau dann injektiv, wenn $\ker(\varphi) = \{e_G\}$ trivial ist.*

Beweis: Wir nehmen an, dass $\ker(\varphi) = \{e_G\}$. Sei $x, y \in G$ mit $\varphi(x) = \varphi(y)$. Es folgt, dass $\varphi(xy^{-1}) = \varphi(x)\varphi(y)^{-1} = e$, also ist $xy^{-1} \in \ker(\varphi)$. Wir schließen, dass $x = y$ und φ ist injektiv. Die Umkehrung folgt direkt aus den Definitionen. □

Es st im Allgemeinen nicht einfach zu überprüfen, ob zwei vorgegebeben Gruppen isomorph sind oder nicht. Sind zwei Gruppen G und H isomorph, dann haben Sie die gleiche Ordnung. Man sieht leicht, dass alle Gruppen mit zwei Elemente zyklisch und daher isomorph sind (Beispiel 1.3.4). Das gleiche gilt für Gruppen mit 3 Elemente. (Diese Aussagen sind ein Spezialfall von Korollar 1.5.10.) Die Anzahl der echt verschiedenen Gruppen wächst schnell: Es gibt genau 2 Gruppen der Ordnung 4, 5 Gruppen der Ordnung 12 und 15 Gruppen der Ordnung 24 (bis auf Isomorphie).

Das folgende Lemma kann benutzt werden, um zu überprüfen, ob zwei Gruppen isomorph sind. Das Lemma ist dem Beispiel 1.3.4 ähnlich.

Lemma 1.3.8 *Sei $\varphi : G \to G'$ ein Gruppenisomorphismus.*

(a) Die Gruppe G ist genau dann abelsch, wenn G' abelsch ist.

(b) Die Elemente $g \in G$ und $\varphi(g) \in G'$ haben die gleiche Ordnung.

Beweis: Wir zeigen (b), Teil (a) folgt ähnlich.

Sei $d := \mathrm{ord}(g)$ die Ordnung von g und $\delta = \mathrm{ord}(\varphi(g))$. Es gilt $e_H = \varphi(e_G) = \varphi(g^d) = \varphi(g)^d$, also gilt $\delta \mid d$. Das gleiche Argument auf die Umkehrabbildung angewendet, liefert $d \mid \delta$. Also ist $\delta = d$. □

Beispiel 1.3.9 (a) Die Matrix

$$A = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} \in \mathrm{GL}_2(\mathbb{R})$$

besitzt Ordnung 4. Die zyklische Gruppe $\langle A \rangle$ ist nicht isomorph zur Gruppe

$$V = \left\{ \begin{pmatrix} \pm 1 & 0 \\ 0 & \pm 1 \end{pmatrix} \right\} \subset \mathrm{GL}_2(\mathbb{R}).$$

In Beispiel 1.1.15.(c) haben wir nämlich gesehen, dass V kein Element der Ordnung 4 besitzt.

(b) Die Elemente der alternierenden Gruppe A_4 sind

e	$(1\,2)(3\,4)$	$(1\,3)(2\,4)$	$(1\,4)(2\,3)$,
$(1\,2\,3)$	$(1\,2\,4)$	$(1\,3\,4)$	$(2\,3\,4)$,
$(1\,3\,2)$	$(1\,4\,2)$	$(1\,4\,3)$	$(2\,4\,3)$.

Insbesondere hat A_4 genau 12 Elemente.

Wir betrachten die Gruppe

$$D := S_3 \times \{\pm 1\}.$$

Die Gruppe besitzt ebenfalls $|S_3| \cdot |\{\pm 1\}| = 6 \cdot 2 = 12$ Elemente. Beide Gruppen sind nichtabelsch, also können wir aus Lemma 1.3.8.(a) nicht schließen, ob beide Gruppen isomorph sind.

Das Element

$$((1\ 2\ 3), -1) \in D$$

besitzt Ordnung 6. Die Gruppe A_4 besitzt kein Element der Ordnung 6, also sind beide Gruppen nicht isomorph (Lemma 1.3.8.(b)).

1.4 Symmetriegruppen

In diesem Abschnitt behandeln wir Beispiele von Symmetriegruppen im 2- und 3-dimensionalen Raum.

Die *Symmetriegruppe* eines beschränkten Objekts $M \subset \mathbb{R}^n$ ist die Menge der Kongruenzabbildungen, die M auf sich selbst abbilden. Eine Symmetriegruppe ist immer eine Gruppe, da die Komposition von Kongruenzabbildungen wieder eine Kongruenzabbildung ist.

Der Schwerpunkt von M wird von allen Symmetrien von M fest gelassen. Liegt der Schwerpunkt eines Objektes im Ursprung $(0, \cdots, 0) \in \mathbb{R}^n$, sind die Kongruenzabbildungen linear und die Symmetriegruppe ist eine Untergruppe der *orthogonalen Gruppe*

$$O_n = \{A \in M_{n,n}(\mathbb{R}) \mid A^t = A^{-1}\}. \tag{1.4.1}$$

Ab jetzt werden wir dies immer annehmen. In dieser Vorlesung unterscheiden wir nicht zwischen der Matrix A und der von A definierten linearen Abbildung.

Die Definition (1.4.1) der orthogonalen Matrizen, zusammen mit der Multiplikativität der Determinanten, impliziert, dass $\det(A) = \pm 1$ für alle $A \in O_n$. Die *spezielle orthogonale Gruppe* ist definiert als

$$\mathrm{SO}_n = \{A \in O_n \mid \det(A) = 1\},$$

d.h. SO_n ist der Kern von $\det : O_n \to \{\pm\}$.

Der folgende Satz ist eine Klassifikation der orthogonalen Matrizen in Dimension 2 und der speziellen orthogonalen Matrizen in Dimension 3. Für einen Beweis verweisen wir auf [7, § 5.5].

Satz 1.4.1 *(a) Sei $A \in SO_2$. Dann ist A die Matrix einer Drehung, d.h. es existiert ein $\alpha \in [0, 2\pi)$ mit*

$$A = \rho_\alpha = \begin{pmatrix} \cos(\alpha) & -\sin(\alpha) \\ \sin(\alpha) & \cos(\alpha) \end{pmatrix}.$$

Hierbei ist α die Drehungswinkel.

(b) Sei $A \in O_2$ mit $\det(A) = -1$. Dann ist A die Matrix einer Spiegelung, d.h. es existiert ein $\alpha \in [0, 2\pi)$ mit

$$A = \sigma_\alpha = \begin{pmatrix} \cos(\alpha) & \sin(\alpha) \\ \sin(\alpha) & -\cos(\alpha) \end{pmatrix}.$$

Die Spiegelachse ist die Gerade durch den Ursprung, die mit der positiven x-Achse einen Winkel von $\alpha/2$ Grad macht.

(c) *Die Gruppe* SO_3 *besteht genau aus den Drehungen von* $\mathbb{R}^3$ *um eine Achse durch den Ursprung.*

Wir betrachten ein regelmäßiges n-Eck Δ_n in $\mathbb{R}^2$ mit Schwerpunkt im Ursprung $(0,0)$. Wir können zum Beispiel annehmen, dass die Ecken des n-Ecks $P_k := (\cos(2k\pi/n), \sin(2k\pi/n))$ $(k = 0, \ldots, n-1)$ sind. Abbildung 1.4.1 zeigt ein Bild von Δ_8.

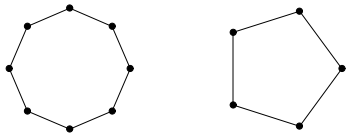


Abbildung 1.4.1: Δ_8 und Δ_5

Definition 1.4.2 Die *Diedergruppe* D_n ist die Symmetriegruppe von Δ_n, d.h.

$$D_n = \{A \in O_2 \mid A(\Delta_n) = \Delta_n\}.$$

Die Gruppe D_n enthält genau n Drehungen und n Spiegelungen. Sei $r : \mathbb{R}^2 \to \mathbb{R}^2$ die Drehung um den Winkel $2\pi/n$. Die Drehung r^k ist die Drehung um den Winkel $2k\pi/n$. Insbesondere ist $r^n = r^0 = e$ die Drehung um 2π Grad, also das neutrale Element der Gruppe.

Betrachten wir nun die Spiegelsymmetrien von Δ_n. Falls n gerade ist, gehen die Spiegelachsen entweder durch zwei gegenüberliegende Ecken oder durch die Mitte von zwei gegenüberliegenden Kanten. Falls n ungerade ist, gehen die Spiegelachsen durch eine Ecke und die Mitte der gegenüberliegenden Kante. Wir wählen s die Spiegelung an der x-Achse.

Lemma 1.4.3 (a) *Die Diedergruppe* D_n *besteht aus* $2n$ *Elementen:*

(i) n *Drehungen* $r^k := \begin{pmatrix} \cos(2k\pi/n) & -\sin(2k\pi/n) \\ \sin(2k\pi/n) & \cos(2k\pi/n) \end{pmatrix}$ *für* $k = 0, 1, \ldots, n-1$.

(ii) n *Spiegelungen* $r^k s := \begin{pmatrix} \cos(2k\pi/n) & \sin(2k\pi/n) \\ \sin(2k\pi/n) & -\cos(2k\pi/n) \end{pmatrix}$ *für* $k = 0, 1, \ldots, n-1$.

(b) *Es gilt*

$$r^n = e, \qquad s^2 = e, \qquad srs = r^{-1}.$$

(c) *Die Gruppe* D_n *ist erzeugt von* r *und* s. *Die Untergruppe* $H = \langle r \rangle$ *erzeugt von* r *ist eine zyklische Gruppe mit* n *Elementen.*

Beweis: Man zeigt leicht, dass die Drehungen und Spiegelungen aus Aussage (a) in der Tat Symmetrien von Δ_n sind. Wir zeigen, dass es keine weiteren Symmetrien gibt.

Jedes Element $A \in D_n$ bildet die Ecke $P_0 = (1,0)$ auf eine Ecke P_k ab. Ist A eine Drehung, dann folgt aus Satz 1.4.1.(a), dass A die Drehung um den Winkel $2k\pi/n$ ist. Ist A eine Spiegelung, dann folgt aus Satz 1.4.1.(b), dass A die Spiegelung $\sigma_{k\pi/n}$. ist. Dies zeigt Aussage (a).

Aussage (b) folgt durch direktes Nachrechnen. Aussage (c) folgt aus der Aussage, dass $r^k s$ die Spiegelung $\sigma_{k\pi/n}$ ist. Dies folgt ebenfalls aus direktem Nachrechnen. □

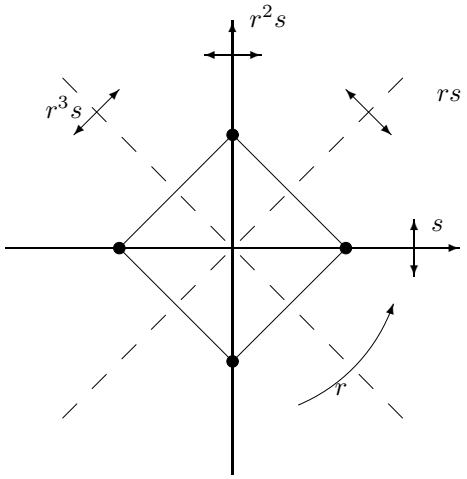


Abbildung 1.4.2: D_4 als Symmetriegruppe des regelmäßigen Vierecks

Bemerkung 1.4.4 Sei $X = \{P_0, P_1, \ldots, P_{n-1}\}$ die Menge der Ecken von Δ_n. Wir identifizieren X mit $\{1, 2, \ldots, n\}$ mit Hilfe der Bijektion $P_i \mapsto i + 1$.

Jede Symmetrie $A \in D_n$ definiert eine Permutation

$$\sigma_A := A|_X \in S(X) \simeq S_n.$$

Die Abbildung

$$\varphi : D_n \to S_n, \qquad \sigma \mapsto \sigma_A$$

ist ein injektiver Gruppenhomomorphismus. Das Bild $\varphi(D_n) \subset S_n$ ist eine Untergruppe von S_n, die zu D_n isomorph ist.

Für $n = 3$ definiert $\varphi : D_3 \to S_3$ einen Isomorphismus, da D_3 und S_3 beide 6 Elemente haben. Beispielsweise gilt für die Drehung r um den Winkel $2\pi/3$, dass $\varphi(r) = (1\ 2\ 3)$. Die Spiegelung s an der Geraden durch P_0 und die Mitte der Kante P_1P_2 definiert die Permutation $\varphi(s) = (2\ 3)$.

Im Rest des Abschnitts betrachten wir die Symmetriegruppen des Tetraeders und des Würfels. Wir beschränken uns dabei auf die orientierungserhaltenden Kongruenzabbildungen. Satz 1.4.1.(c) impliziert, dass alle diese Kongruenzabbildungen Drehungen sind. Die entsprechende Symmetriegruppen sind Untergruppen von SO_3.

Sei $T \subset \mathbb{R}^3$ das regelmäßiger Tetraeder mit Schwerpunkt im Ursprung und Ecken

$$\left\{ \begin{pmatrix} 1 \\ 1 \\ 1 \end{pmatrix}, \begin{pmatrix} 1 \\ -1 \\ -1 \end{pmatrix}, \begin{pmatrix} -1 \\ 1 \\ -1 \end{pmatrix}, \begin{pmatrix} -1 \\ -1 \\ 1 \end{pmatrix} \right\}.$$

Mit $W \subset \mathbb{R}^3$ bezeichnen wir den Würfel mit den 8 Ecken

$$\left\{ \begin{pmatrix} \pm 1 \\ \pm 1 \\ \pm 1 \end{pmatrix} \right\}.$$

Abbildung 1.4.3 zeigt T und W in einem Bild.

Definition 1.4.5 (a) Die *Tetraedergruppe* $\mathbb{T}$ ist die Menge der Drehungen, die T auf sich selbst abbilden:

$$\mathbb{T} := \{A \in \mathrm{SO}_3 \mid A(T) = T\}.$$

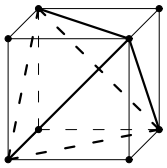


Abbildung 1.4.3: Tetraeder und Würfel

(b) Die *Würfelgruppe* $\mathbb{W}$ ist die Menge der Drehungen, die W auf sich selbst abbilden:

$$\mathbb{W} := \{A \in \mathrm{SO}_3 \mid A(W) = W\}.$$

Wir betrachten zuerst die Tetraedergruppe. Neben dem neutralen Element, enthält $\mathbb{T}$ Drehungen der Ordnung 2 und 3 (Abbildung 1.4.4).

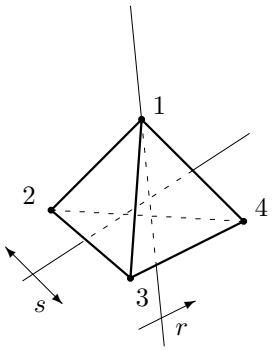


Abbildung 1.4.4: Die Rotationssymmetrien des Tetraeders

Die Achse einer Drehung der Ordnung 3 geht durch eine Ecke und die Mitte der gegenüberliegenden Kante. Insgesamt besitzt T 4 solcher Symmetrieachsen, also enthält $\mathbb{T}$ genau $(3-1)\cdot 4 = 8$ Drehungen der Ordnung 3. Die Achse einer Drehung der Ordnung 2 geht durch die Mitte zweier gegenüberliegender Kanten. Insgesamt enthält $\mathbb{T}$ also $6/2 = 3$ Drehungen der Ordnung 2. Zusammen mit dem neutralen Element haben wir

$$1 + 8 + 3 = 12$$

Elemente vin $\mathbb{T}$ gefunden. Im Beweis von Satz 1.4.6 zeigen wir, dass dies alle sind.

Satz 1.4.6 *Die Tetraedergruppe $\mathbb{T}$ ist isomorph zu A_4.*

Beweis: Wir nummerieren die Ecken des Tetraeders als $X := \{1, 2, 3, 4\}$, wie in Abbildung 1.4.4. Da $A \in \mathbb{T}$ Ecken des Tetraeders auf Ecken abbildet, erhalten wir einen Gruppenhomomorphismus

$$\varphi : \mathbb{T} \to S_4, \qquad A \mapsto A|_X.$$

Zum Beispiel gilt für r und s wie in Abbildung 1.4.4

$$\varphi(r) = (2\ 3\ 4), \qquad \varphi(s) = (1\ 4)(2\ 3).$$

Insbesondere sind $\varphi(r)$ und $\varphi(s)$ gerade. Ähnlich gilt dies auch für die andere Elemente von $\mathbb{T}$. Wir schließen, dass das Bild von φ in A_4 enthalten ist.

Wir zeigen, dass φ injektiv ist. Es reicht zu zeigen, dass $\ker(\varphi) = \{1\}$ (Lemma 1.3.7). Sei $\rho \in \mathbb{T}$ ein Element, dass alle Ecken von T festlässt. Die Richtungsvektoren von 3 der 4 Ecken bilden eine Basis von $\mathbb{R}^3$. Es folgt, dass jedes Element in $\mathbb{T}$ eindeutig durch die Bilder der Ecken bestimmt ist. Es folgt, dass $\rho = 1$ und φ ist injektiv. Es folgt, dass $\mathbb{T} \simeq \varphi(\mathbb{T}) < A_4$ eine Untergruppe von A_4 ist.

Wir haben schon gesehen, dass A_4 mindestens 12 Elemente besitzt,nämlich die Symmetrien, die wir vor der Formulierung des Satzes aufgelistet haben. Die Gruppe A_4 besitzt ebenfalls 12 Elemente, also ist φ auch surjektiv. Die Aussage des Satzes folgt. □

Bemerkung 1.4.7 (a) Ähnlich wie wir dies für den Tetraeder gemacht haben, kann man auch die Rotationssymmetrien des Würfels bestimmen.

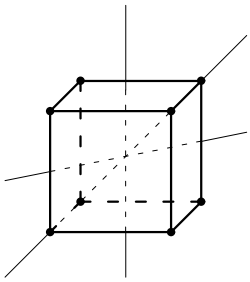


Abbildung 1.4.5: Die Rotationssymmetrien des Würfels

Wir geben nur die Aussagen. Der Würfel besitzt drei verschiedene Arten von Drehachsen:

(I) Drehachsen der Ordnung 4 durch die Mitten zweier gegenüberliegender Seitenflächen. Da W 6 Seitenflächen besitzt, gibt es $6/2 = 3$ solche Drehachsen. Insgesamt finden wir $3 \cdot (4-1) = 9$ nichttriviale Drehungen.

(II) Drehachsen der Ordnung 3 durch zwei gegenüberliegende Ecken. Da W 8 Ecken besitzt, gibt es $8/2 = 4$ solche Drehachsen, nämlich die Körperdiagonalen. Insgesamt finden wir $4 \cdot (3-1) = 8$ nichttriviale Drehungen.

(III) Drehachsen der Ordnung 2 durch die Mitten zweier gegenüberliegender Kanten. Da W 12 Kanten besitzt, gibt es $12/2 = 6$ solche Symmetrieachsen. Insgesamt finden wir $6 \cdot (2-1) = 6$ nichttriviale Drehungen.

Zusammen mit dem neutralen Element finden wir

$$|\mathbb{W}| = 1 + 9 + 8 + 6 = 24.$$

In Satz 2.1.8 werden wir zeigen, dass $\mathbb{W} \simeq S_4$ ist.

(b) Zu jedem Platonischen Körper P kann man einen *dualen Platonischen Körper* P^* assoziieren. Die Ecken des dualen Platonischen Körpers sind die Mitten der Seitenflächen. Zwei Ecken p_1, p_2 von P^* sind genau dann durch eine Kante verbunden, wenn die entsprechenden Seitenflächen von P angrenzend sind.

Der duale Körper des Würfels ist ein Oktaeder, siehe Abbildung 1.4.6. Der duale Körper des Tetraeders ist wieder ein Tetraeder. Es gibt genau zwei weitere Platonische Körper: Das Dodekaeder und das Ikosaeder. Diese sind ebenfalls zueinander dual.

Duale Platonische Körper haben die gleiche Symmetriegruppe. Die Symmetriegruppe des Oktaeders ist also ebenfalls $\mathbb{W}$.

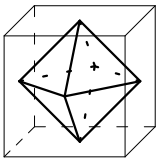


Abbildung 1.4.6: Würfel und Oktaeder

1.5 Nebenklassen

Sei G eine endliche Gruppe und $H < G$ eine Untergruppe. In diesem Abschnitt zeigen wir einen Zusammenhang zwischen der Ordnung von H und von G. Dazu definieren wir folgende Äquivalenzrelation.

Definition 1.5.1 Sei $H < G$ eine Untergruppe. Eine Teilmenge von G von der Form $aH = \{ah \mid h \in H\}$ heißt *Linksnebenklasse* von H in G. Die Menge aller Linksnebenklassen bezeichnen wir mit G/H. (In Worten: G modulo H.) Die Anzahl der Linksnebenklassen von H in G nennt man den *Index* von H in G und er wird mit $[G : H]$ bezeichnet.

Entsprechend heißt $Ha = \{ha \mid h \in H\}$ *Rechtsnebenklasse* und bezeichnet $H\backslash G$ die Menge der Rechntsnebenklassen.

Linksnebenklassen kann man interpretieren als Äquivalenzklassen einer Äquivalenzrelation.

Lemma 1.5.2 *Sei G eine Gruppe und $H < G$ eine Untergruppe.*

(a) Die Relation $\sim_H$ auf G definiert durch

$$a \sim_H b \qquad :\Leftrightarrow \qquad a^{-1}b \in H$$

ist eine Äquivalenzrelation.

(b) Die Äquivalenzklassen von $\sim_H$ sind die Linksnebenklassen.

(c) Die Gruppe G ist die disjunkte Vereinigung aller Linksnebenklassen von H.

Beweis: Der Beweis von (a) folgt durch direkter Verifikation. Wir überlassen es als Übungsaufgabe. Teil (b) folgt direkt aus der Definition der Äquivalenzrelation. Teil (c) folgt aus der Tatsache, dass zwei Aquivalenzklassen entweder gleich oder disjunkt sind. □

Wir betrachten den Spezialfall $G = \mathbb{Z}$ und $H = m\mathbb{Z}$ mit $m \in \mathbb{N}$. Die Relation $\sim_H$ aus Lemma 1.5.2.(a) ist in diesem Fall:

Definition 1.5.3 Sei m eine natürliche Zahl und seien a, b ganze Zahlen. Wir sagen, dass *a kongruent zu b modulo m* ist, falls $m \mid (b-a)$. Wir schreiben: $a \equiv b \pmod{m}$. Die Zahl m heißt der *Modul* der Kongruenz.

Die Linksnebenklassen $a + m\mathbb{Z} = \{b \in \mathbb{Z} \mid a \equiv b \pmod{m}\}$ heißen *Kongruenzklassen*.

Wir schreiben $\mathbb{Z}/m\mathbb{Z}$ für die Menge der Kongruenzklassen modulo m. Ist der Modul m aus dem Kontext klar, schreiben wir auch $[a]$ für die Kongruenzklasse $a + m\mathbb{Z}$, manchmal auch einfach a. Division mit Rest zeigt, dass jede Kongruenzklasse einen eindeutigen Repräsentanten in $\{0, \ldots, m-1\}$ besitzt. Wir schreiben also

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

Die Addition und Multiplikation auf $\mathbb{Z}$ induzieren eine Addition und Multiplikation auf $\mathbb{Z}/m\mathbb{Z}$. Die Menge $\mathbb{Z}/m\mathbb{Z}$ zusammen mit den beiden Strukturen $+$ und $\cdot$ ist ein Ring, siehe Abschnitt 3.1 für die Definition.

Lemma 1.5.4 *(a) Addition und Multiplikation modulo m definieren abelsche, assoziative Verknüpfungen auf $\mathbb{Z}/m\mathbb{Z}$.*

(b) Die Menge $\mathbb{Z}/m\mathbb{Z}$ mit Addition modulo m ist eine zyklische Gruppe mit m Elementen.

Beweis: Wir definieren

$$(a + m\mathbb{Z}) + (b + m\mathbb{Z}) = (a + b) + m\mathbb{Z}, \qquad (a + m\mathbb{Z}) \cdot (b + m\mathbb{Z}) = (a \cdot b) + m\mathbb{Z}.$$

Diese Verknüpfungen sind wohldefiniert, d.h. unabhängig von der Wahl des Repräsentanten a, b. (Überprüfen Sie dies!) Diese Verknüpfungen sind abelsch und assoziativ, da Addition und Multiplikation in $\mathbb{Z}$ abelsch und assoziativ sind.

Das neutrale Element von $(\mathbb{Z}/m\mathbb{Z}, +)$ ist $0+m\mathbb{Z}$. Das inverse Element von $a+m\mathbb{Z}$ ist $(m-a) + m\mathbb{Z}$. Also ist $(\mathbb{Z}/m\mathbb{Z}, +)$ eine Gruppe. Das Element $1 + m\mathbb{Z}$ ist ein Erzeuger, also ist $\mathbb{Z}/m\mathbb{Z}$ zyklisch. □

Satz 1.5.5 *Sei G eine Gruppe mit endlich vielen Elementen und $H < G$ eine Untergruppe.*

(a) Die Anzahl der Elemente einer Linksnebenklasse aH hängt nicht von a ab, also $|aH| = |H|$.

(b) (Indexformel) Es gilt

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

Beweis: Die Abbildung $\psi : H \to aH, \quad h \mapsto ah$ ist eine Bijektion: Die Umkehrabbildung ist gegeben durch $x = ah \mapsto a^{-1}x = h$. Dies beweist (a). Teil (b) folgt aus (a). □

Beispiel 1.5.6 Die Untergruppe $A_n < S_n$ besitzt genau zwei Nebenklassen, nämlich

$$A_n = \{\sigma \in S_n \mid \operatorname{sgn}(\sigma) = 1\},$$
$$S_n \setminus A_n = \{\sigma \in S_n \mid \operatorname{sgn}(\sigma) = -1\}.$$

Die Menge der ungeraden Permutationen ist die Linksnebenklasse $(1\ 2)A_n$. Sind nämlich $\sigma, \tau \in S_n \setminus A_n$ ungerade Permutationen, dann ist

$$\operatorname{sgn}(\sigma^{-1}\tau) = \operatorname{sgn}(\sigma)^{-1} \operatorname{sgn}(\tau) = (-1)^2 = 1.$$

Also ist $\sigma^{-1}\tau \in A_n$. Es folgt, dass die ungeraden Permutationen eine Linksnebenklasse formen.

Der surjektive Gruppenhomomorphismus $\operatorname{sgn} : S_n \to \{\pm 1\}$ induziert eine Bijektion

$$\operatorname{sgn} : S_n/A_n \to \{\pm 1\}.$$

Dies ist ein Spezialfall der Konstruktion der Faktorgruppe in Abschnitt 1.6.

Satz 1.5.5 besitzt viele wichtige Konsequenzen.

Satz 1.5.7 (Lagrange) *Sei G eine endliche Gruppe.*

(a) Sei $H < G$ eine Untergruppe. Die Ordnung von H teilt die Ordnung von G.

(b) Die Ordnung von $g \in G$ teilt die Ordnung von G.

Beweis: Teil (a) folgt direkt aus Satz 1.5.5. Teil (b) folgt aus (a) angewandt auf die Untergruppe $H = \langle g \rangle$. □

Lemma 1.5.8 *Die Menge $\mathbb{Z}/m\mathbb{Z}^* = \{[a] \in \mathbb{Z}/m\mathbb{Z} \mid \operatorname{ggT}(a, m) = 1\}$ ist eine Gruppe mit Multiplikation modulo m als Verknüpfung.*

Beweis: Die Abgeschlossenheit, Assoziativität und die Existenz des neutralen Elementes sind klar. Korollar 1.1.17 impliziert, dass für jedes $a \in \mathbb{Z}$ mit $\operatorname{ggT}(a, m) = 1$ Zahlen $x, y \in \mathbb{Z}$ existieren, sodass $1 = xa + ym$. Offensichtlich ist $\operatorname{ggT}(x, m) = 1$. Also ist $xa \equiv 1 \pmod{m}$ und $x + m\mathbb{Z}$ ist das inverse Element von a. Daher besitzt jedes Element $a \in (\mathbb{Z}/m\mathbb{Z})^*$ ein inverses Element von $a + m\mathbb{Z}$. □

Sei $\varphi(m)$ die Kardinalität der Gruppe $(\mathbb{Z}/m\mathbb{Z})^*$. Die Funktion φ heißt *Eulersche phi-Funktion*. Folgendes Korollar ist in der Elementaren Zahlentheorie bekannt als der Satz von Euler und ist ein Spezialfall von Satz 1.5.7.(b).

Korollar 1.5.9 (Satz von Euler) *Sei $m \in \mathbb{N}$ und $a \in \mathbb{Z}$ mit $\operatorname{ggT}(a, m) = 1$. So gilt*

$$a^{\varphi(m)} \equiv 1 \pmod{m}.$$

Beweis: Dies folgt aus $\varphi(m) = |\mathbb{Z}/m\mathbb{Z}^*|$. □

Korollar 1.5.10 *Sei p eine Primzahl. Jede Gruppe der Ordnung p ist zyklisch.*

Beweis: Sei G eine Gruppe mit p Elementen und $a \in G$ ein Element mit $a \neq e$. Satz 1.5.7.(b) impliziert, dass $\operatorname{ord}(a) = p = |G|$, da p eine Primzahl ist. Es folgt, dass $\langle a \rangle = G$ und G ist zyklisch. □

Das folgende Korollar bestimmt die Gruppe der Ordnung 4. Die Kleinsche Vierergruppe wurde in Beispiel 1.1.15.(c) eingeführt.

Korollar 1.5.11 *Jede Gruppe G der Ordnung 4 ist isomorph zu $\mathbb{Z}/4\mathbb{Z}$ oder zur Kleinschen Vierergruppe V.*

Beweis: Sei G eine Gruppe der Ordnung 4 und sei $g \in G \setminus \{e\}$. Satz 1.5.7 impliziert, dass die Ordnung ein Teiler von 4 ist, also gilt $\operatorname{ord}(g) \in \{2, 4\}$. Falls G ein Element der Ordnung 4 besitzt, ist G zyklisch. Sonst haben alle Elemente $g \in G \setminus \{e\}$ Ordnung 2.

Wir nehmen an, dass G nicht zyklisch ist und schreiben $G = \{e, a, b, c\}$. Die Elemente a, b, c haben Ordnung 2. Da $a^2 = b^2 = e$, impliziert Lemma 1.1.4.(d), dass

$a \cdot b \neq e, a, b$. Wir schließen, dass $a \cdot b = c$. Ebenso folgt, dass $b \cdot a = c$. Dies bestimmt die Verknüpfungstabelle von G:

$\cdot$	e	a	b	c
e	e	a	b	c
a	a	e	c	b
b	b	c	e	a
c	c	b	a	e.

Die Verknüpfungstabelle ist bis auf die Wahl der Namen der Elemente eindeutig. Ein konkreter Isomorphismus $\varphi : V \to G$ ist zum Beispiel gegeben durch

$$\varphi(A_1) = a, \quad \varphi(A_2) = b,$$

wobei A_1, A_2 die Erzeuger von V aus Beispiel 1.1.15.(c) sind. □

Beispiel 1.5.12 Die Gruppe $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} = \{(0,0), (1,0), (0,1), (1,1)\}$ besitzt 4 Elemente und erfüllt $2 \cdot (x, y) = (0, 0)$ für alls $(x, y) \in \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$.

Die Gruppe $\mathbb{Z}/8\mathbb{Z}^* = \{[1], [3], [5], [7]\}$ besitzt ebenfalls 4 Elemente und es gilt, dass $[a]^2 = [1]$ für alle $[a] \in \mathbb{Z}/8\mathbb{Z}^*$.

Also gilt $V \simeq \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \simeq \mathbb{Z}/8\mathbb{Z}^* \simeq V$.

1.6 Faktorgruppen

Lemma 1.5.4 zeigt, dass die Menge $\mathbb{Z}/m\mathbb{Z}$ der Linksnebenklassen von $m\mathbb{Z} \subset \mathbb{Z}$ eine Gruppe ist. Im Allgemeinen ist die Menge der Linksnebenklassen keine Gruppe. Theorem 1.6.4 bestimmt wann dies der Fall ist.

Definition 1.6.1 Sei G eine Gruppe. Eine Untergruppe N von G heißt *Normalteiler*, falls

$$ghg^{-1} \in N \qquad \text{für alle } h \in N \text{ und } g \in G. \tag{1.6.1}$$

Bezeichnung: $N \lhd G$.

Beispiel 1.6.2 Die Untergruppe $m\mathbb{Z} < \mathbb{Z}$ ist ein Normalteiler.

Satz 1.6.3 *Eine Untergruppe H von G ist genau dann ein Normalteiler, wenn jede Linksnebenklasse auch eine Rechtsnebenklasse ist.*

Beweis: Wir nehmen zuerst an, dass $H \lhd G$ ein Normalteiler ist. Also gilt für $h \in H$ und $a \in G$, dass $aha^{-1} \in H$ ist. Wir schließen, dass

$$ah = (aha^{-1})a \in Ha.$$

Also ist $aH \subset Ha$. Ähnlich gilt auch, dass $Ha \subset aH$. Also ist $aH = Ha$.

Für die andere Implikation nehmen wir an, dass H kein Normalteiler ist. Also existieren Elemente $a \in G$ und $h \in H$ mit $h' := aha^{-1} \notin H$. Das Element ah ist in aH, aber $ah = h'a \notin Ha$. Das Element $a = a \cdot e = e \cdot a$ ist sowohl in aH als auch in Ha. Also sind aH und Ha nicht disjunkt. Lemma 1.5.2.(c) impliziert daher, dass Ha keine Linksnebenklasse ist. □

Theorem 1.6.4 *Sei $N \lhd G$ ein Normalteiler.*

(a) Die Menge $\bar{G} := G/N$ der Linksnebenklassen ist eine Gruppe mit Verknüpfung:

$$aN \cdot bN = abN.$$

Diese Gruppe heißt die Faktorgruppe von G nach N.

(b) *Falls G eine endliche Gruppe ist, gilt $|\bar{G}| = |G|/|N|$.*

(c) *Die Abbildung $\pi : G \to \bar{G} = G/N$, $a \mapsto aN$ ist ein surjektiver Gruppenhomomorphismus mit Kern N.*

Beweis: Sei N ein Normalteiler von G. Wir definieren

$$aN \cdot bN = \{x \in G \mid x = ahbh' \text{ für } h, h' \in N\}.$$

Wir behaupten, dass $aN \cdot bN$ wieder eine Linksnebenklasse ist, nämlich

$$aN \cdot bN = abN.$$

Sobald wir dies gezeigt haben, folgt, dass die Verknüpfung auf $\bar{G}$ wohldefiniert ist, d.h. das Produkt $aN \cdot bN$ hängt nicht von der Wahl der Repräsentanten a, b ab.

Sei $x \in aN \cdot bN$. Es gilt $x = ahbh'$ mit $h, h' \in N$. Wir können dies auch als $x = ab(b^{-1}hb)h'$ schreiben. Da $N \lhd G$, ist $bhb^{-1} \in N$ und daher ist auch $bhb^{-1}h' \in N$. Also ist $x \in abN$. Wir schließen, dass $aN \cdot bN \subset abN$.

Umgekehrt, sei $y = abh \in abN$ für ein $h \in N$. Es gilt $y = abh = (a \cdot e)(b \cdot h) \in aN \cdot bN$. Also ist $abN \subset aN \cdot bN$ und damit gilt $aN \cdot bN = abN$.

Die Assoziativität der Verknüpfung auf $\bar{G}$ folgt aus der Assoziativität der Verknüpfung auf G. Das neutrale Element ist $eN = N$. Das inverse Element von aN ist $a^{-1}N$. Dies beweist (a). Teil (b) folgt direkt aus Satz 1.5.5.(b).

Wir beweisen nun (c). Sei π wie in (c). Die Tatsache, dass π einen Gruppenhomomorphismus definiert, folgt direkt aus der Definition der Verknüpfung auf $\bar{G}$. Die Surjektivität von π folgt direkt aus der Definition von π. Da $eN = N$ das neutrale Element von $\bar{G}$ ist, folgt $\ker(\varphi) = \{g \in G \mid gN = N\} = N$. Nun ist alles gezeigt. □

Beispiel 1.6.5 (a) Falls $H < G$ eine Untergruppe, aber kein Normalteiler ist, so ist die Menge G/H der Linksnebenklassen keine Gruppe. Wir überprüfen dies in einem konkreten Fall.

Sei $G = D_n$ und $H = \langle s \rangle = \{e, s\}$ die Untergruppe erzeugt von einer Spiegelung. Die Linksnebenklassen sind:

$$H = \{e, s\}, \quad rH = \{r, rs\}, \quad \cdots, \quad r^{n-1}H = \{r^{n-1}, r^{n-1}s\}.$$

Also ist $[G : H] = n$. (Dies folgt auch aus Satz 1.5.5.(b).)

Falls $n \geq 3$ ist, ist

$$rsr^{-1} = r^2 s \notin H.$$

Dies impliziert, dass H für $n \geq 3$ kein Normalteiler von D_n ist. (Alternativ könnte man auch überprüfen, dass $Hr = \{r, sr = r^{n-1}s\}$ keine Linksnebenklasse ist.) (Was passiert für $n = 2$?)

Wir berechnen, dass

$$r \cdot r = r^2, \quad r \cdot rs = r^2 s, \quad rs \cdot r = s, \quad rs \cdot rs = e.$$

Also ist $rH \cdot rH = \{r^2, r^2 s, s, rs\}$; dies ist keine Linksnebenklasse, sondern eine Vereinigung von Linksnebenklassen. Also ist die Multiplikation $(rH)(rH)$ nicht wohl definiert.

(b) Sei $n = 2m$ eine gerade Zahl und $H = \langle r^2 \rangle$ die Untergruppe von D_n erzeugt von r^2. Die Ordnung von r^2 ist $n/2 = m$, also ist $[D_n : H] = 4$.

Wir überprüfen, dass $H \lhd D_n$ ein Normalteiler ist. Es reicht die Bedingung aus Definition 1.6.1 für die Erzeuger r, s von D_n und r^2 von H zu überprüfen. Mit Hilfe der Relation $srs = r^{-1}$ berechnen wir:

$$rr^2r^{-1} = r^2 \in H, \qquad sr^2s = r^{-2} \in H.$$

Also ist $H \lhd D_n$ ein Normalteiler.

Die Faktorgruppe D_n/H ist eine Gruppe mit 4 Elementen, also ist D_n/H entweder zyklisch oder isomorph zur Kleinschen Vierergruppe V (Korollar 1.5.11). Wir berechnen die Ordnung der Elemente der Faktorgruppe.

Die Linksnebenklassen sind:

$$H, \quad rH, \quad sH, \quad rsH.$$

Lemma 1.5.2 impliziert, dass $xH = yH$ genau dann, wenn $x^{-1}y \in H$ ist. Man überprüft damit, dass die 4 Linksnebenklassen in der Tat verschieden sind.

Wir berechnen:

$$(rH)^2 = r^2H = H, \ (sH)^2 = s^2H = H, \ (rsH)^2 = rsrsH = rr^{-1}H = H.$$

Die Faktorgruppe D_n/H besitzt also kein Element der Ordnung 4 und ist daher isomorph zur Kleinschen Vierergruppe.

Wir geben einige Kriterien, um zu überprüfen, ob eine Untergruppe $H < G$ ein Normalteiler ist.

Lemma 1.6.6 *Falls G eine abelsche Gruppe ist, ist jede Untergruppe ein Normalteiler.*

Beweis: Falls G abelsch ist, gilt $ghg^{-1} = h$ für alle $h, g \in G$. Also ist die Bedingung (1.6.1) aus Definition 1.6.1 trivial. □

Den Beweis von Lemma 1.2.13 kann man als Spezialfall des folgenden Lemmas auffassen. Die Untergruppe A_n ist also sogar ein Normalteiler von S_n.

Lemma 1.6.7 *Sei $\varphi : G \to H$ ein Gruppenhomomorphismus. Der Kern von φ ist ein Normalteiler von G.*

Beweis: Sei $\varphi : G \to H$ ein Gruppenhomomorphismus. Seien $h \in \ker(\varphi)$ und $g \in G$ beliebige Elemente. Es gilt

$$\varphi(ghg^{-1}) = \varphi(g)\varphi(h)\varphi(g)^{-1} = \varphi(g)\varphi(g)^{-1} = e_H.$$

Also ist $ghg^{-1} \in \ker(\varphi)$. □

Theorem 1.6.4.(b) zeigt, dass die Umkehrung von Lemma 1.6.7 auch gilt: Jeder Normalteiler ist der Kern eines Gruppenhomomorphismus.

Lemma 1.6.8 *Jede Untergruppe H einer Untergruppe G mit $[G : H] = 2$ ist ein Normalteiler. Die Faktorgruppe G/H ist isomorph zu $\mathbb{Z}/2\mathbb{Z}$.*

Beweis: Wir zeigen, dass $xH = Hx$ für alle $x \in G$. Das Lemma folgt dann aus Satz 1.6.3. Falls $x \in H$, gilt $xH = Hx = H$. Sei $x \in G \setminus H$. Es existieren genau $[G : H] = 2$ Linksnebenklassen. Die Linksnebenklassen H und xH sind disjunkt und $G = H \cup xH$, also ist $xH = G \setminus H$. Das gleiche Argument zeigt, dass $Hx = G \setminus H$. Also ist $xH = Hx$ und $H \lhd G$ is ein Normalteiler.

Die Faktorgruppe G/H besitzt 2 Elemente, also ist $G/H \simeq \mathbb{Z}/2\mathbb{Z}$ (Korollar 1.5.10). □

Beispiel 1.6.9 Die Untergruppen $A_n < S_n$ und $\langle r \rangle < D_n$ haben Index 2 und sind daher Normalteiler. Es gilt $S_n/A_n \simeq D_n/\langle r \rangle \simeq \mathbb{Z}/2\mathbb{Z}$.

Folgender Satz ist manchmal die einfachste Methode, die Faktorgruppe zu beschreiben.

Satz 1.6.10 (Erster Isomorphiesatz für Gruppen) *Sei $\varphi : G \to G'$ ein surjektiver Gruppenhomomorphismus und sei $N = \ker(\varphi)$. Die Abbildung*

$$\bar{\varphi} : \bar{G} := G/N \to G', \qquad aN \mapsto \varphi(a)$$

ist ein Isomorphismus.

Beweis: Lemma 1.6.7 zeigt, dass $N \lhd G$ ein Normalteiler ist. Insbesondere ist $\bar{G}$ eine Gruppe.

Zuerst überprüfen wir, dass die Abbildung $\bar{\varphi}$ wohldefiniert ist. Seien $a, b \in G$ mit $aN = bN$. Es gilt $x := a^{-1}b \in N = \ker(\varphi)$. Also gilt $\varphi(b) = \varphi(ax) = \varphi(a)\varphi(x) = \varphi(a)$.

Sei $\varphi(a) = \bar{a} \in G'$. Wir überprüfen, dass $\varphi^{-1}(\bar{a}) = aN$, also, dass jede Linksnebenklasse das Urbild eines Elements $\bar{a} \in G'$ ist. Sei $x \in \varphi^{-1}(\bar{a})$. Es gilt $\bar{a} = \varphi(a) = \varphi(x)$. Dies impliziert, dass $\varphi(a^{-1}x) = e_{G'}$, also ist $a^{-1}x \in N$. Also gilt $x \in aN$. Die Inklusion $aN \subset \varphi^{-1}(\bar{a})$ haben wir schon gezeigt.

Die Surjektivität von $\bar{\varphi}$ folgt aus der Surjektivität von φ. Da $\ker(\varphi) = N$, folgt, dass $\ker(\bar{\varphi}) = N = e_{\bar{G}}$. Also ist $\bar{\varphi}$ injektiv (Lemma 1.3.7).

Wir überprüfen, dass $\bar{\varphi}$ ein Gruppenhomomorphismus ist:

$$\bar{\varphi}((aN)(bN)) = \bar{\varphi}(abN) = \varphi(ab) = \varphi(a)\varphi(b) = \bar{\varphi}(aN)\bar{\varphi}(bN).$$

Also ist $\bar{\varphi}$ ein Isomorphismus. □

Korollar 1.6.11 *Sei $\varphi : G \to G'$ ein Homomorphismus endlicher Gruppen. Es gilt*

$$|G| = |\ker(\varphi)| \cdot |\operatorname{im}(\varphi)|.$$

Beweis: Sei $N := \ker(\varphi)$. Der Homomorphismus $\varphi : G \to \operatorname{im}(\varphi)$ ist surjektiv. Also folgt aus Satz 1.6.10 und Satz 1.5.5, dass

$$|\operatorname{im}(\varphi)| = |G/N| = [G : N] = \frac{|G|}{|N|}.$$

Das Korollar folgt. □

Beispiel 1.6.12 (a) Aus den Beispielen 1.3.2.(a) und 1.3.6.(a) schließen wir, dass $K^* \simeq \mathrm{GL}_n(K)/\mathrm{SL}_n(K)$.

(b) Wir haben gesehen, dass $A_n = \ker(\mathrm{sgn})$ ist. Außerdem ist $\mathrm{sgn} : S_n \to \{\pm 1\}$ surjektiv. Dies zeigt nochmals, dass $S_n/A_n \simeq \{\pm 1\} \simeq \mathbb{Z}/2\mathbb{Z}$.

(c) Sei $S^1 = \{z \in \mathbb{C} \mid |z| = 1\}$ der Einheitskreis. Dies ist eine Gruppe mit Multiplikation als Verknüpfung (Beispiel 1.1.9.(b)). Die Abbildung

$$\mathbb{R} \to S^1, \qquad x \mapsto e^{2\pi i x}$$

ist ein surjektiver Gruppenhomomorphismus mit $\ker = \mathbb{Z}$. Wir schließen, dass $\mathbb{R}/\mathbb{Z} \simeq S^1$ ist.

(d) Wir betrachten $G = S_4$ und $H = \{e, (1\ 2)(3\ 4), (1\ 3)(2\ 4), (1\ 4)(2\ 3)\}$. Dann ist H eine Untergruppe von G isomorph zur Kleinschen Vierergruppe (Übungsaufgabe). Wir werden einen surjektiven Gruppenhomomorphismus

$$\varphi : S_4 \to S_3$$

mit $\ker(\varphi) = H$ konstruieren.

Wir betrachten die Menge der Partitionen von $X = \{1, 2, 3, 4\}$ in genau zwei Blöcke der Kardinalität 2, d.h. $M = \{p_1, p_2, p_3\}$ mit

$$\begin{aligned} p_1 &= \{\{1, 2\}, \{3, 4\}\}, \\ p_2 &= \{\{1, 3\}, \{2, 4\}\}, \\ p_3 &= \{\{1, 4\}, \{2, 3\}\}. \end{aligned}$$

Die Elemente p_i von M entsprechen genau den Zyklen der nicht-trivialen Permutationen in H.

Jede Permutation $\sigma \in S_4$ induziert eine Permutation von M. Beispielsweise finden wir für $\sigma = (1\ 2\ 3\ 4)$:

$$\begin{aligned} \sigma(p_1) &= \{\{2, 3\}, \{4, 1\}\} = p_3, \\ \sigma(p_2) &= \{\{2, 4\}, \{3, 1\}\} = p_2, \\ \sigma(p_3) &= \{\{2, 1\}, \{3, 4\}\} = p_1. \end{aligned}$$

Dies enspricht der Permutation $(1\ 3) \in S(M) \simeq S_3$.

Ebenso finden wir für $\tau = (1\ 2\ 3)$:

$$\begin{aligned} \tau(p_1) &= \{\{2, 3\}, \{1, 4\}\} = p_3, \\ \tau(p_2) &= \{\{2, 1\}, \{3, 4\}\} = p_1, \\ \tau(p_3) &= \{\{2, 4\}, \{3, 1\}\} = p_2. \end{aligned}$$

Dies entspricht der Permutation $(1\ 3\ 2) \in S(M) \simeq S_3$.

Wir erhalten einen Gruppenhomomorphismus

$$\varphi : S_4 \to S(M) \simeq S_3, \qquad \sigma \mapsto (p_i \mapsto \sigma(p_i)).$$

Dieser Gruppenhomomorphismus ist surjektiv, da S_3 von $\varphi(\sigma) = (1\ 3)$ und $\varphi(\tau) = (1\ 3\ 2)$ erzeugt wird. Ähnlich überprüft man, dass $H \subset \ker(\varphi)$.

Korollar 1.6.11 impliziert, dass

$$|\ker(\varphi)| = \frac{|S_4|}{|S_3|} = \frac{24}{6} = 4 = |H|.$$

Wir schließen, dass $H = \ker(\varphi)$ ist. Der erste Isomorphiesatz (Satz 1.6.10) zeigt, dass

$$S_4/H \simeq S_3.$$

2 Gruppenwirkungen

Als Motivation für die Definitionen in Abschnitt 2.1 betrachten wir folgendes Problem.

Wir haben Perlen in drei verschiedenen Farben (z.B. gelb, rot und blau). Wie viele echt verschiedene Möglichkeiten gibt es, 5 solcher Perlen auf einer geschlossenen Schnur aufzureihen?

Nummeriert man die einzelnen Positionen als $1, 2, 3, 4, 5$ haben wir 3 Möglichkeiten eine Perle für jede Position zu wählen. Insgesamt finden wir also $5^3 = 125$ Möglichkeiten. Diese Möglichkeiten sind nicht alle verschieden, da wir die Symmetrien nicht berücksichtigt haben.

Zwei Perlenketten sind genau dann gleich, wenn man sie durch Drehungen und Spiegelungen in Einander überführen kann. Beispielsweise sind alle Perlenketten bestehend aus 4 roten und einer gelben Perle gleich. Mit Hilfe von Theorem 2.3.1 werden wir diese und ähnliche Fragen beantworten.

2.1 Definitionen

Definition 2.1.1 Sei G eine Gruppe und X eine nicht leere Menge. Eine *Gruppenwirkung* τ von G auf X ist ein Gruppenhomomorphismus $G \to S(X)$.

Eine Gruppenwirkung $\tau : G \to S(X)$ ordnet jedes Gruppenelement $g \in G$ einer Permutation $\tau(g)$ der Elemente von X zu.

Beispiel 2.1.2 Sei $G = D_n$ und X die Menge der Ecken des regelmäßigen n-Ecks Δ_n (§ 1.4). Wir nummerieren die Ecken als $X = \{1, 2, 3 \ldots, n\}$. Jedes Element $g \in D_n$ permutiert die Ecken von Δ_n. Dies definiert eine Permutation $\tau(g) \in S(X) \simeq S_n$. Die Abbildung τ ist offensichtlich ein Gruppenhomomorphismus. Für die Gruppenwirkung aus dem Beispiel von Abbildung 2.1.1 sehen wir beispielsweise, dass $(1\ 2)(3\ 4) = \tau(rs) = \tau(r)\tau(s) = (1\ 2\ 3\ 4)(2\ 4)$.

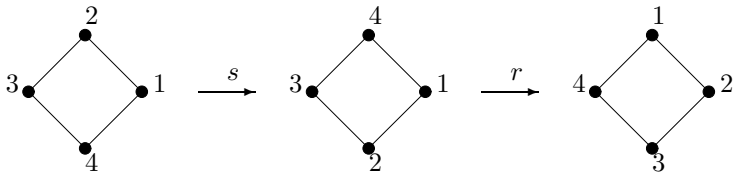


Abbildung 2.1.1: D_4 definiert eine Gruppenwirkung

Das folgende Lemma gibt eine alternative Definition einer Gruppenwirkung.

Lemma 2.1.3 *(a) Eine Gruppenwirkung $\tau : G \to S(X)$ definiert eine Abbildung*

$$\rho : G \times X \to X, \quad (g, x) \mapsto \rho_g(x)$$

mit $\rho_{g\cdot g'}(x) = \rho_g(\rho_{g'}(x))$ und $\rho_e(x) = x$ für alle $g, g' \in G$ und $x \in X$.

(b) Jede Abbildung $\rho : G \times X \to X$ mit $\rho_{g\cdot g'}(x) = \rho_g(\rho_{g'}(x))$ und $\rho_e(x) = x$ für alle $g, g' \in G$ und $x \in X$ definiert eine Gruppenwirkung.

Beweis: Wir definieren $\rho_g(x) := \tau(g)(x)$, d.h. $\rho_g(x)$ ist das Bild von x unter der Permutation $\tau(g) \in S(X)$. Die Eigenschaften aus (a) gelten, da τ ein Gruppenhomomorphismus ist.

Umgekehrt, für ρ wie in (b), definieren wir $\tau(g)$ als die Abbildung, die x dem Element $\rho_g(x)$ zuordnet. Die Eigenschaft $\rho_{g\cdot g'}(x) = \rho_g(\rho_{g'}(x))$ impliziert, dass τ ein Gruppenhomomorphismus ist.

Wir müssen zeigen, dass $\tau(g)$ für alle $g \in G$ bijektiv ist, d.h. $\tau(g) \in S(X)$. Hierzu zeigen wir, dass $\tau(g^{-1})$ die Umkehrabbildung von $\tau(g)$ ist. Es gilt

$$\tau(g) \circ \tau(g^{-1})(x) = \rho_g(\rho_{g^{-1}}(x)) = \rho_{g\cdot g^{-1}}(x) = \rho_e(x) = x.$$

Die letzte Gleichheit folgt aus Eigenschaft (b). □

Statt $\tau(g)(x) = \rho_g(x)$ schreiben wir meistens $g \cdot x$.

Beispiel 2.1.4 (a) Die Gruppe $\mathbb{Z}$ wirkt auf der reellen Gerade $\mathbb{R}$ als Translation. Wir definieren $\tau_m(x) = x + m$ für $m \in \mathbb{Z}$ und $x \in \mathbb{R}$. Dies definiert eine Gruppenwirkung, da $x + (m + n) = (x + n) + m$ für alle $m, n \in \mathbb{Z}$ und $x \in \mathbb{R}$.

(b) Sei K ein Körper. Eine Matrix $A \in \mathrm{GL}_n(K)$ wirkt auf K^n als Matrixmultiplikation: $\tau_A(x) = A \cdot x$.

Definition 2.1.5 Sei $\tau : G \times X \to X$ eine Gruppenwirkung. Für $x \in X$ heißt

$$G(x) = \{y \in X \mid y = g \cdot x\} \subset X$$

die *Bahn* von x. Eine Gruppenwirkung mit nur einer Bahn heißt *transitiv*.

Die Menge

$$G_x = \{g \in G \mid g \cdot x = x\} \subset G$$

heißt *Stabilisator* von x.

Lemma 2.1.6 *Sei $\rho : G \times X \to X$ eine Gruppenwirkung.*

(a) Die Menge X ist eine disjunkte Vereinigung von Bahnen.

(b) Der Stabilisator G_x ist eine Untergruppe von G.

(c) Sei $y = g \cdot x \in G_x$. Dann gilt $gG_xg^{-1} = G_y$. Insbesondere gilt $|G_x| = |G_y|$.

Beweis: Für $x, y \in X$ definieren wir eine Äquivalenzrelation

$$x \sim_G y \qquad :\Leftrightarrow \qquad y \in G(x).$$

Die Bahnen der Gruppenwirkung sind die Äquivalenzklassen von $\sim_G$. Zwei verschiedene Bahnen sind daher disjunkt. Teil (b) folgt aus der Definition des Stabilisators.

Sei $y = g \cdot x$ wie in (c). Für $h \in G_x$ gilt $h \cdot x = x$, also $ghg^{-1} \cdot y = ghg^{-1}g \cdot x = gh \cdot x = g \cdot x = y$. Es folgt, dass $gG_xg^{-1} \subset G_y$. Ähnlich zeigt man, dass $g^{-1}G_yg \subset G_x$, oder äquivalent, dass $G_y \subset gG_xg^{-1}$ ist. Die erste Aussage von (c) folgt. Die zweite Aussage von (c) folgt ebenfalls, da

$$G_x \to G_y, \qquad h \mapsto ghg^{-1}$$

eine Bijektion ist. □

Beispiel 2.1.7 (a) Die Gruppe D_n wirkt transitiv auf der Menge X der Ecken des regelmäßigen n-Ecks.

(b) Der Gruppenhomomorphismus $\varphi : \mathbb{T} \to S_4$ aus dem Beweis von Satz 1.4.6 entspricht der Gruppenwirkung von $\mathbb{T}$ auf der Menge $\{1, 2, 3, 4\}$ der Ecken des regelmäßigen Tetraeders T.

Sei $Y = \{12, 13, 14, 23, 24, 34\}$ die Menge der Kanten von T, d.h. 12 ist die Kante durch die Ecken 1 und 2 usw. Die Tetraedergruppe $\mathbb{T}$ wirkt auf Y. Man sieht leicht ein, dass die Kanten eine Bahn formen. Der Stabilisator einer Kante besteht aus zwei Elementen: Dem neutralen Element e und der Drehung um den Winkel π um die Gerade durch die Mitte der Kante und der gegenüberliegenden Kante. Der Stabilisator der Kante 23 ist zum Beispiel $\{e, s\}$, wobei s wie in Abbbildung 1.4.4 ist.

Satz 2.1.8 *Die Würfelgruppe $\mathbb{W}$ ist isomorph zu S_4.*

Beweis: Sei $X = \{1, 2, 3, 4\}$ die Menge der Körperdiagonalen des Würfels W. Die Würfelgruppe $\mathbb{W}$ wirkt auf X, also erhalten wir einen Gruppenhomomorphismus

$$\varphi : \mathbb{W} \to S(X) \simeq S_4.$$

In Bemerkung 1.4.7 haben wir alle 24 Elemente von $\mathbb{W}$ aufgelistet. Mit einem Fallunterscheidung zeigt man, dass das einzige Element von $\mathbb{W}$, dass alle Diagonalen festhält das neutrale Element ist. Also ist $\ker(\varphi) = \{1\}$ und φ ist injektiv. Da $|\mathbb{W}| = |S_4| = 24$ ist φ ebenfalls surjektiv. □

Satz 2.1.9 (Bahn-Stabilisator-Satz) *Sei $\rho : G \times X \to X$ eine Gruppenwirkung und $x \in X$. Die Abbildung*

$$\varphi : G(x) \to G/G_x, \qquad g \cdot x \mapsto gG_x$$

ist eine Bijektion der Bahn $G(x)$ auf der Menge der Linksnebenklassen von G_x in G.

Beweis: Wir zeigen zuerst, dass die Abbildung φ wohldefiniert ist. Wir wählen $g_1, g_2 \in G$ mit $g_1 \cdot x = g_2 \cdot x$. Dies ist äquivalent zu $g_1^{-1} g_2 \in G_x$. Also ist $\varphi(g_1 \cdot x) = g_1 G_x = g_2 G_x = \varphi(g_2 \cdot x)$. Somit ist φ wohldefiniert.

Die Abbildung φ ist offensichtlich surjektiv. Wir zeigen, dass sie auch injektiv ist. Dazu nehmen wir an, dass $gG_x = g'G_x$ für $g, g' \in G$ gilt. Dies bedeutet, dass $h := g^{-1}g' \in G_x$ ist. Also gilt $g' \cdot x = (gh) \cdot x = g \cdot x$, da $h \in G_x$ ist. □

Korollar 2.1.10 *Sei G eine endliche Gruppe, die auf einer Menge X wirkt. Für $x \in X$ gilt*

$$|G(x)| \cdot |G_x| = |G|.$$

Insbesondere ist die Kardinalität einer Bahn ein Teiler der Gruppenordnung.

Beweis: Satz 2.1.9 sagt, dass die Kardinalität der Bahn die Anzahl der Linksnebenklassen, also der Index $[G : G_x]$ von G_x in G, ist. Die Aussage folgt daher aus Satz 1.5.5.(b). □

Beispiel 2.1.11 (a) Sei $X = \{1, 2, 3, 4, 5, 6, 7, 8\}$ die Menge der Ecken und $\mathbb{W}$ die Rotationssymmetriegruppe des regelmäßigen Würfels. Ähnlich wie im Beispiel 2.1.7.(b) überprüft man, dass $\mathbb{W}$ transitiv auf X wirkt, also dass die Bahn $\mathbb{W}(1) = X$ ist.

Die Würfelgruppe ist isomorph zu S_4 (Satz 2.1.8). Korollar 2.1.10 zeigt, dass der Stabilisator $24/8 = 3$ Elemente besitzt. Die Drehung r um $2\pi/3$ Grad um die Körperdiagonale durch die Ecke 1 lässt die Ecke 1 fest. Wir schließen, dass $\mathbb{W}_1 = \{e = r^0, r, r^2\}$.

(b) Der Ikosaeder ist ein platonischer Körper mit 20 gleichseitigen Dreiecken als Seitenflächen. Der Ikosaeder besitzt 12 Ecken, 30 Kanten und 20 Seitenflächen.

Die Rotationssymmetriegruppe $\mathbb{I}$ des Ikosaeders wirkt transitiv auf der Menge $X := \{1, 2, 3, \ldots, 12\}$ der Ecken. Die Stabilisatorgruppe $\mathbb{I}_1$ einer Ecke wird erzeugt von der Drehung r um die Achse durch die Ecke und der gegenüberliegenden Ecke. Die Ordnung von r ist 5, da in der Ecke 1 genau 5 Kanten zusammen kommen. Wir schließen, dass $|\mathbb{I}| = |\mathbb{I}(1)| \cdot |\mathbb{I}_1| = 12 \cdot 5 = 60$. Man kann zeigen, dass $\mathbb{I} \simeq A_5$ ist (siehe zum Beispiel [6, § 1.5.5]).

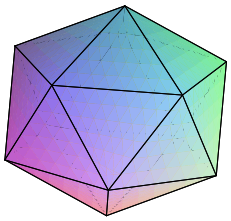


Abbildung 2.1.2: Der Ikosaeder

2.2 Wirkungen einer Gruppe auf sich selbst

Eine Gruppe wirkt in unterschiedlicher Weise auf sich selbst.

Definition 2.2.1 *Linkstranslation* ist eine Gruppenwirkung von G auf sich selbst, definiert als

$$G \times G \to G, \quad (g, x) \mapsto \tau_g(x) = gx$$

Die Rechtstranslation $G \times G \to G, \quad (g, x) \mapsto \rho_g(x) = xg$ ist nur dann eine Gruppenwirkung, wenn G abelsch ist. Es gilt nämlich, dass $\rho_{gg'}(x) = xgg'$ und $\rho_g(\rho_{g'}(x)) = xg'g$.

Satz 2.2.2 (Cayley) *Jede endliche Gruppe der Ordnung d ist eine Untergruppe von S_d.*

Beweis: Eine endliche Gruppe G der Ordnung d wirkt auf sich selbst mittels Linkstranslation. Wir erhalten einen Gruppenhomomorphismus

$$\varphi : G \to S(G), \qquad g \mapsto \tau_g.$$

Für $g \in G \setminus \{e\}$ gilt $\tau_g(e) = g \cdot e = g$. Also ist $g \notin \ker(\varphi)$. Wir schließen, dass φ injektiv ist. Also ist $\mathrm{im}(\varphi) \simeq G$ (Satz 1.6.10). Das Bild $\mathrm{im}(\varphi)$ ist eine Untergruppe von $S(G) \simeq S_d$. □

Definition 2.2.3 Die *Konjugation* einer Gruppe G ist eine Gruppenwirkung von G auf sich selbst, definiert als

$$G \times G \to G, \quad (g, x) \mapsto \kappa_g(x) = gxg^{-1}.$$

Die Bahnen der Konjugation heißen *Konjugationsklassen*.

Wir bestimmen die Konjugationsklassen in S_n. Der *Zyklentyp* einer Permutation ist die Liste der Längen der Zyklen in der disjunkten Zyklendarstellung. Beispielsweise besitzt $(1\ 2)(3\ 4)$ Zyklentyp 2-2.

Lemma 2.2.4 *(a) Sei $\sigma \in S_n$ beliebig und $\tau = (a_1\ \cdots\ a_k) \in S_n$ ein k-Zyklus. Es gilt*

$$\sigma(a_1\ \cdots\ a_k)\sigma^{-1} = (\sigma(a_1)\ \sigma(a_2)\ \cdots\ \sigma(a_k)).$$

(b) Zwei Permutationen τ_1, τ_2 in S_n sind genau dann konjugiert, wenn sie den gleichen Zyklentyp besitzen.

Beweis: Teil (a) überprüfen wir durch direktes Nachrechnen:

$$\sigma\tau\sigma^{-1}(\sigma(a_i)) = \sigma\tau(a_i) = \sigma(a_{i+1}).$$

Teil (a) impliziert, dass konjugierte Elemente immer den gleichen Zyklentyp besitzen. Wir zeigen die Umkehrung und betrachten dazu zuerst den Fall, dass $\tau_1 = (a_1 \ \cdots \ a_k)$ und $\tau_2 = (b_1 \ \cdots \ b_k)$ beide k-Zyklen sind. Sei σ eine Permutation mit $\sigma(a_i) = b_i$ für $i = 1, \ldots, k$. Ein solches σ existiert immer, aber ist nicht notwendigerweise eindeutig. Teil (a) impliziert, dass $\sigma\tau_1\sigma^{-1} = \tau_2$.

Der allgemeine Fall folgt aus $\sigma\tau_1\tau_2\sigma^{-1} = \sigma\tau_1\sigma^{-1}\sigma\tau_2\sigma^{-1}$ und der Tatsache, dass sich jede Permutation als Produkt disjunkter Zyklen schreiben lässt. □

Beispiel 2.2.5 (a) Sei $\tau_1 = (1\ 2\ 3) \in S_4$ und $\tau_2 = (1\ 3\ 4) \in S_4$. Lemma 2.2.4.(b) impliziert, dass τ_1 und τ_2 konjugiert sind. Wir suchen ein Element $\sigma \in S_4$ mit $\sigma\tau_1\sigma^{-1} = \tau_2$. Wir wählen z.B.

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

Da σ eine Permutation ist, gilt $\sigma(4) = 2$, also $\sigma = (1)(2\ 3\ 4)$. Da $\tau_2 = (1\ 3\ 4) = (3\ 4\ 1)$, hätten wir aber auch

$$\sigma(1) = 3, \quad \sigma(2) = 4, \quad \sigma(3) = 1, \quad \sigma(4) = 2,$$

d.h. $\sigma = (1\ 3)(2\ 4)$, wählen können. Insbesondere ist σ nicht eindeutig bestimmt, wie schon im Beweis von Lemma 2.2.4 bemerkt wurde.

(b) Sei $\tau \in S_n =: G$ ein n-Zyklus. Lemma 2.2.4.(b) impliziert, dass die Konjugationsklasse $G(\tau)$ von τ aus allen n-Zyklen besteht. Also ist $|G(\tau)| = n!/n = (n-1)!$. Korollar 2.1.10 impliziert, dass $|G_1| = n!/(n-1)! = n$. Da offensichtlich $\tau \in G(\tau)$, folgt, dass $G(\tau) = \langle\tau\rangle$.

(c) Sei K ein Körper. Die Gruppe $\mathrm{GL}_n(K)$ wirkt auf $M_{n,n}(K)$ durch Konjugation: Für $A \in \mathrm{GL}_n(K)$ und $M \in M_{n,n}(K)$ definieren wir $\tau_A(M) = AMA^{-1}$. Zwei Matrizen M_1, M_2, die in der gleichen Bahn bezüglich dieser Wirkung sind, heißen *ähnlich*.

(d) Sei $H := \{e, (1\ 2)(3\ 4), (1\ 3)(2\ 4), (1\ 4)(2\ 3)\} < S_4$ wie im Beispiel 1.6.12.(d). Die Untergruppe H enthält alle Permutationen vom Zyklentyp 2-2. Lemma 2.2.4.(b) impliziert daher, dass $H \lhd S_4$ ein Normalteiler ist. Im Beispiel 1.6.12.(d) haben wir dies gezeigt, indem wir einen Gruppenhomomorphismus mit Kern H konstruiert haben.

2.3 Das Theorem von Burnside

In diesem Abschnitt kommen wir zurück auf der Motivationsfrage.

Theorem 2.3.1 (Burnside) *Sei G eine endliche Gruppe, die auf einer endlichen Menge X wirkt. Für $g \in G$ definieren wir*

$$X^g = \{x \in X \mid g \cdot x = x\}$$

die Menge der Fixpunkte *von g.*

Die Anzahl der Bahnen ist

$$\frac{1}{|G|} \sum_{g \in G} |X^g|.$$

Beweis: Seien $X_1, \ldots, X_k$ die verschiedenen Bahnen der Gruppenwirkung. Wir suchen eine Formel für k.

Wir zählen die Paare

$$S := \{(g, x) \in G \times X \mid g \cdot x = x\}.$$

Einerseits gilt

$$|S| = \sum_{g \in G} |X^g|. \tag{2.3.1}$$

Anderseits gilt

$$|S| = \sum_{x \in X} |G_x| = \sum_{i=1}^{k} \sum_{x \in X_i} |G_x|. \tag{2.3.2}$$

Wir wählen einen Punkt $x_i \in X_i$ für jedes i.

Lemma 2.1.6.(c) sagt, dass $|G_x| = |G_{x_i}|$ für alle $x \in X_i$. Also gilt

$$\sum_{x \in X_i} |G_x| = |X_i| \cdot |G_{x_i}| = |G(x_i)| \cdot |G_{x_i}|.$$

Aus dem Bahn-Stabilisator-Satz (Korollar 2.1.10) folgt, dass $|G(x_i)| \cdot |G_{x_i}| = |G|$. Wir schließen aus (2.3.1) und (2.3.2), dass

$$|S| = \sum_{g \in G} |X^g| = \sum_{i=1}^{k} |G| = k|G|.$$

Das Theorem folgt. □

Beispiel 2.3.2 (a) Wir malen die Ecken des Tetraeders T mit 3 verschiedenen Farben an. Sei X die Menge der Färbungen. Diese Menge hat 3^4 Elemente. Sei $\mathbb{T} \simeq A_4$ die Symmetriegruppe des Tetraeders T. In $\mathbb{T}$ gibt es folgende Elementen: (Siehe Abbildung 1.4.4):

* das neutrale Element e,
* 8 Drehungen der Ordnung 3,
* 3 Drehungen der Ordnung 2.

Wir zählen für jedes Element $g \in \mathbb{T}$ die Menge X^g der von g fest gelassenen Färbungen. Das neutrale Element lässt alle Färbungen fest: $|X^e| = |X| = 3^4$.

Sei g eine Drehung der Ordnung 3, also ist g eine Drehung um eine Achse durch eine Ecke P und die Mitte der gegenüberliegenden Seitenfläche F. Falls $x \in X^g$ eine von g festgelassene Färbung ist, haben die Ecken der Seitenfläche F alle die gleiche Farbe. Die Ecke P darf eine andere Farbe haben. Wir schließen, dass $|X^g| = 3^2$ ist.

Sei g eine Drehung der Ordnung 2, also ist g eine Drehung um eine Achse durch die Mitten zweier gegenüberliegender Kanten K_1 und K_2. Die Drehung vertauscht die beiden Ecken der Kante K_1 (bzw. K_2). Falls $x \in X^g$ eine von g fest gelassene Färbung ist, haben die Ecken der Kante K_1 die gleiche Farbe und ebenso die Ecken der Kante K_2. Also ist $|X^g| = 3^2$.

Die Anzahl der wirklich verschiedenen Färbungen ist also

$$\frac{1}{|G|} \sum_{g \in G} |X^g| = \frac{1}{12}(1 \cdot 3^4 + 8 \cdot 3^2 + 3 \cdot 3^2) = 15.$$

(b) Wir betrachten Ketten bestehend aus 5 Perlen an einem kreisförmigen Band. Wie viele echt verschiedene Ketten können wir mit roten, blauen und gelben Perlen machen? Die Symmetriegruppe ist die Diedergruppe D_5. Wir benutzen die Bezeichnung aus § 1.4 und unterscheiden drei Fälle.

Das neutrale Element lässt alle Färbungen fest, also $|X^e| = 3^5$.

Die Drehungen $g \in \{r, r^2, r^3, r^4\}$ vertauschen die 5 Perlen zyklisch. Bei der von einer Drehung festgelassenen Färbung haben also alle Perlen die gleiche Farbe. Also ist $|X^g| = 3$.

Die Spiegelungen $g \in \{s, rs, r^2s, r^3s, r^4s\}$ sind Spiegelungen an einer Achse durch eine Ecke P_k und die Mitte der gegenüberliegenden Kante. Die Ecke P_k wird von der Spiegelung fest gelassen. Die andere Ecke formen 2 Bahnen mit 2 Elementen. Also ist $|X^g| = 3^3$.

Die Anzahl der Ketten ist daher

$$\frac{1}{|D_5|} \sum_{g \in G} |X^g| = \frac{1}{10}(1 \cdot 3^5 + 4 \cdot 3 + 5 \cdot 3^3) = 39.$$

2.4 Die endlichen Rotationsgruppen

In diesem Abschnitt bestimmen wir alle endlichen Symmetriegruppen in $\mathbb{R}^2$ und $\mathbb{R}^3$. (Siehe auch [2, § 19] und [1, §§ 5.3+5.9].)

Wir betrachten zunächst die endlichen Symmetriegruppen der Ebene. Satz 1.4.1 beschreibt die lineare Kongruenzabbildungen der Ebene: Dies sind Drehungen und Spiegelungen. Wir bemerken, dass die Spiegelungen der Ebene Einschränkungen von Drehungen des Raums sind.

Satz 2.4.1 *Sei $G < O_2$ eine endliche Untergruppe. Dann ist G entweder zyklisch oder isomorph zur Diedergruppe D_n.*

Beweis: Fall I: $G < SO_2$.
Satz 1.4.1.(a) impliziert, dass jedes Element $r \in G$ eine Drehung

$$r = \rho_\alpha = \begin{pmatrix} \cos(\alpha) & -\sin(\alpha) \\ \sin(\alpha) & \cos(\alpha) \end{pmatrix}$$

für $\alpha \in [0, 2\pi)$ ist. Wir nehmen oBdA an, dass $G \neq \{1\}$ ist und wählen $r \in G \setminus \{1\}$ mit α minimal.

Behauptung: Die Gruppe G ist zyklisch mit Erzeuger r.
Sei $g \in G \setminus \{1\}$ ein beliebiges Element. Dann ist $g = \rho_\beta$ für ein $\beta \in (0, 2\pi)$. Wir schreiben

$$\beta = k\alpha + \gamma, \qquad \text{mit } k \in \mathbb{Z} \text{ und } 0 \leq \gamma < \alpha.$$

Es folgt, dass

$$\rho_\gamma = \rho_{\beta - k\alpha} = g \cdot r^{-k} \in G.$$

Die Wahl von α impliziert, dass $\gamma = 0$. Es folgt, dass $g = r^k \in \langle r \rangle$ und G ist zyklisch mit Erzeuger r.

Fall II: $G \subsetneq \mathrm{SO}_2$.
Wir definieren $H := G \cap \mathrm{SO}_2$. Satz 1.4.1 impliziert, dass $H < G$ die Untergruppe der Drehungen ist. Fall I impliziert, dass $H \simeq \mathbb{Z}/n\mathbb{Z}$ eine zyklische Gruppe ist. Wir wählen einen Erzeuger r.

Das Komplement $G \setminus H$ besteht genau aus den Spiegelungen, dies sind die Matrizen mit Determinante -1 (Satz 1.4.1.(b)). Das Produkt zweier Spiegelungen

$s, s' \in G \setminus H$ erfüllt $\det(s \cdot s') = \det(s)\det(s') = 1$, also ist $ss' \in H$. Es folgt, dass

$$G = H \sqcup sH \qquad \text{für } s \in G \setminus H.$$

Als Spiegelung besitzt s Ordnung 2 und es gilt die Relation $srs = r^{-1}$. Diese Relation kann man beispielsweise mit Hilfe der Matrixdarstellung aus Satz 1.4.1 nachrechnen. Wir schließen, dass

$$G = \langle r, s \rangle \subset O_2$$

isomorph zur Diedergruppe D_n der Ordnung $2n$ ist. (Vergleichen Sie zu Lemma 1.4.3). □

Das folgende Theorem sagt, dass eine endliche Rotationsgruppe entweder zyklisch, eine Diedergruppe oder eine Symmetriegruppe eines Platonischen Körpers ist. In Satz 2.4.1 haben wir gesehen, dass die zyklischen Gruppen und die Diedergruppen Untergruppen von O_2 sind. Spiegelungen der Ebene kann man als Drehungen um der z-Achse in $\mathbb{R}^3$ auffassen. Es folgt, dass die zyklische Gruppen und die Diedergruppen ebenfalls Untergruppen von SO_3 sind.

Wir haben schon gesehen, dass die Tetraedergruppe $\mathbb{T}$ isomorph zu A_4 ist (Satz 1.4.6). Die Würfelgruppe $\mathbb{W}$ ist isomorph zu S_4 (Satz 2.1.8). Das Oktaeder ist der duale Platonische Körper des Würfels und besitzt deswegen auch $\mathbb{W}$ als Symmetriegruppe (Bemerkung 1.4.7.(b)). Es gibt nur zwei weitere Platonische Körper: Das Ikosaeder und das Dodekaeder. Diese sind ebenfalls dual zu Einander und besitzen Symmetriegruppe $\mathbb{I} \simeq A_5$ (Beispiel 2.1.11.(b)).

Theorem 2.4.2 *Sei $G < \mathrm{SO}_3$ eine endliche Untergruppe. Dann ist G isomorph zu einer der folgenden Gruppen:*

- *Die zyklische Gruppe $\mathbb{Z}/n\mathbb{Z}$.*
- *Die Diedergruppe D_n.*
- *Die Tetraedergruppe $\mathbb{T}$.*
- *Die Würfelgruppe $\mathbb{W}$.*
- *Die Ikosaedergruppe $\mathbb{I}$.*

Bevor wir Theorem 2.4.2 beweisen, brauchen wir einige Vorbereitungen.
Sei $G < \mathrm{SO}_3$ eine endliche Untergruppe. Die Gruppe G wirkt auf der 2-Sphäre

$$S^2 := \{x \in \mathbb{R}^3 \mid \|x\| = 1\},$$

da $g \in G$ längentreu ist. Jede nichttriviale Drehung $g \in \mathrm{SO}_3 \setminus \{I\}$ besitzt eine Drehachse $L_g \subset \mathbb{R}^3$. Dies ist eine Gerade durch den Ursprung und schneidet S^2 in genau zwei Punkten $x_g, -x_g$. Wir nennen diese Punkte die *Pole* von g. Es sind genau die Punkte $x \in S^2$ mit $g(x) = x$. Wir schreiben

$$X = X_G := \{x \in S^2 \mid \exists g \in G \setminus \{1\} \text{ mit } g(x) = x\}$$

für die Menge der Polen.

Lemma 2.4.3 *Die Gruppe G wirkt auf der Menge X_G der Pole.*

Beweis: Sei $x \in X$ ein Pol und $g \in G$ eine Drehung mit $g(x) = x$, d.h. x ist ein Pol zu g. Für $h \in G$ gilt

$$(hgh^{-1})(h(x)) = hg(x) = h(x).$$

Also ist $h(x) \in X$ ein Pol zu $hgh^{-1} \in G$. $\square$

Der Beweis von Theorem 2.4.2 beruht auf dem Studium der Bahnen der Wirkung von G auf X. Wir betrachten dies zunächst in einem Beispiel.

Beispiel 2.4.4 Sei $G = \mathbb{T}$ die Tetraedergruppe. Um die Pole mit Hilfe von Koordinaten einfacher angeben zu können, betrachten wir X als Teilmenge der Sphäre mit Radius $\sqrt{3} = \|(1,1,1)\|$.

Die Menge X der Pole besteht aus 3 Bahnen:

- Die Menge
$$X_1 = \left\{ \begin{pmatrix} 1 \\ 1 \\ 1 \end{pmatrix}, \begin{pmatrix} 1 \\ -1 \\ -1 \end{pmatrix}, \begin{pmatrix} -1 \\ 1 \\ -1 \end{pmatrix}, \begin{pmatrix} -1 \\ -1 \\ 1 \end{pmatrix} \right\}$$
der Ecken von T. Es gilt $|X_1| = 4$.

- Die Menge
$$X_2 = \{-x \mid x \in X_1\} = \left\{ \begin{pmatrix} -1 \\ -1 \\ -1 \end{pmatrix}, \begin{pmatrix} -1 \\ 1 \\ 1 \end{pmatrix}, \begin{pmatrix} 1 \\ -1 \\ 1 \end{pmatrix}, \begin{pmatrix} 1 \\ 1 \\ -1 \end{pmatrix} \right\}.$$
Dies sind die 2ten Pole der Drehungen der Ordnung 3.

- Die Menge
$$X_3 = \left\{ \begin{pmatrix} \pm\sqrt{3} \\ 0 \\ 0 \end{pmatrix}, \begin{pmatrix} 0 \\ \pm\sqrt{3} \\ 0 \end{pmatrix}, \begin{pmatrix} 0 \\ 0 \\ \pm\sqrt{3} \end{pmatrix} \right\}$$
der Polen der Drehungen der Ordnung 2. Es gilt $|X_3| = 6$.

Bemerke, dass $X_1 \cup X_2$ die Ecken des Würfels W sind. Die Menge X_3 besteht aus den Ecken eines Oktaeders.

Wir skizzieren den Beweis von Theorem 2.4.2

Beweisskizze: Sei $N := |G|$ die Kardinalität von G. Wir schreiben $X_1, \ldots, X_m$ für die verschiedenen Bahnen der Wirkung und wählen $x_i \in X$ mit $X_i = G(x_i)$. Setze $n_i = |X_i|$ und $k_i = |G_{x_i}|$. Aus dem Bahn-Stabilisator-Satz (Korollar 2.1.10) und der Tatsache, dass x_i ein Pol ist, folgt, dass

$$k_i := N/n_i, \qquad 2 \leq k_i \leq N. \tag{2.4.1}$$

Jedes nichtriviale Element $g \in G$ besitzt genau zwei Pole, also gilt

$$|X^g| = \begin{cases} |X| = \sum_{i=1}^m n_i & \text{falls } g = 1, \\ 2 & \text{falls } g \neq 1. \end{cases} \tag{2.4.2}$$

Der Satz von Burnside (Theorem 2.3.1) impliziert daher, dass

$$\begin{aligned} m = \frac{1}{N} \sum_{g \in G} |X^g| &\overset{(2.4.2)}{=} \frac{1}{N} \left(\sum_{i=1}^m n_i + 2(N-1) \right) \\ &= \sum_{i=1}^m \frac{n_i}{N} + 2 - \frac{2}{N} \overset{(2.4.1)}{=} \sum_{i=1}^m \frac{1}{k_i} + 2 - \frac{2}{N}. \end{aligned}$$

Wir können diese Gleichung zu

$$2 - \frac{2}{N} = \sum_{i=1}^{m} \left(1 - \frac{1}{k_i}\right) \tag{2.4.3}$$

umschreiben.

Wir haben angenommen, dass G nichttrivial ist, also ist $N \geq 2$. Die linke Seite von (2.4.3) erfüllt daher $1 \leq 2 - 2/N \leq 2$. Die Zahlen $k_i = |G_{x_i}|$ sind größer gleich 2 (Gleichung (2.4.1)). Jeder Term der rechten Seite von (2.4.3) ist daher größer gleich $1/2$. Es folgt, dass $m \in \{2, 3\}$ ist.

Fall I: $m = 2$. In diesem Fall lässt sich (2.4.3) zu

$$\frac{2}{N} = \frac{1}{k_1} + \frac{1}{k_2}$$

vereinfachen. Wir wissen, dass $2 \leq k_1, k_2 \leq N$ ist (Gleichung (2.4.1)). Es folgt sofort, dass $k_1 = k_2 = N$. Also ist $n_1 = n_2 = N/N = 1$ und $X = \{x, -x\}$ besteht aus genau zwei Polen. Alle Elemente $g \in G \setminus \{1\}$ besitzen also eine gemeinsame Drehachse, nämlich die Gerade L durch die Pole $x, -x$.

Wir schränken G auf das orthogonale Komplement $L^\perp \simeq \mathbb{R}^2$ von L ein und erhalten eine Einbettung

$$G \hookrightarrow \mathrm{SO}_2(\mathbb{R}), \qquad g \mapsto g|_{\mathbb{R}^2}.$$

Fall I aus dem Beweis von Satz 2.4.1 impliziert, dass G als endliche Untergruppe von SO_2 zyklisch ist.

Fall II: $m = 3$. In diesem Fall lässt sich (2.4.3) zu

$$1 + \frac{2}{N} = \frac{1}{k_1} + \frac{1}{k_2} + \frac{1}{k_3} \tag{2.4.4}$$

vereinfachen. OBdA dürfen wir annehmen, dass $2 \leq k_1 \leq k_2 \leq k_3 \leq N$ ist.

Behauptung: Die Gleichung (2.4.4) besitzt genau die folgenden Lösungen:

N	k_1	k_2	k_3	Bedingung
$2n$	2	2	n	$n \geq 2$
12	2	3	3	
24	2	3	4	
60	2	3	5	

(2.4.5)

Der Beweis der Behauptung folgt aus einer kombinatorischen Überlegung, siehe beispielsweise [1, § 5.9].

Um das Theorem zu beweisen, müssen wir die Gruppen G in jedem der Fällen aus (2.4.5) bestimmen. Im Fall $(k_1, k_2, k_3) = (2, 2, n)$ ist G isomorph zur Diedergruppe D_n. Im Fall $(k_1, k_2, k_3) = (2, 3, 3)$ ist G isomorph zur Tetraedergruppe $\mathbb{T}$. Im Fall $(k_1, k_2, k_3) = (2, 3, 4)$ ist G isomorph zur Würfelgruppe $\mathbb{W}$. Im Fall $(k_1, k_2, k_3) = (2, 3, 5)$ ist G isomorph zur Ikosaedergruppe $\mathbb{I}$.

Wir zeigen dies exemplarisch im Fall $N = 24$ und $(k_1, k_2, k_3) = (2, 3, 4)$. Für die anderen Fälle verweisen wir auf [1, § 5.9] oder [2, § 19].

Wir wählen $z = x_3 \in X_3$. Es gilt $|X_3| = n_3 = N/k_3 = 24/4 = 6$. Wähle $u \in X_3 \setminus \{\pm z\}$. Fall I zeigt, dass die Gruppe $G_z = \langle g \rangle \simeq \mathbb{Z}/4\mathbb{Z}$ zyklisch ist. Lemma 2.4.3 impliziert, dass $g(u) \in X_3$ ist. Da die Drehung g nur die zwei Pole $\pm z$ besitzt, gilt

$$X_3 = \{z, -z, u, g(u), g^2(u), g^3(u)\}.$$

Die Drehung $g \in \mathrm{SO}_3$ ist längentreu, also ist

$$\|u - g(u)\| = \|g(u) - g^2(u)\| = \|g^2(u) - g^3(u)\| = \|g^3(u) - u\|.$$

Da $g \in \mathrm{SO}_3$ ebenfalls winkeltreu ist, folgt, dass $\{u, g(u), g^2(u), g^3(u)\} \subset S^2$ die Ecken eines Quadrats sind. Das Quadrat liegt in der Ebene $L_g^\perp$ orthogonal zur Drehachse L_g von g. Es folgt, dass X_3 die Ecken eines Oktaeders bilden. Wir schließen, dass G eine Untergruppe der Symmetriegruppe $\mathbb{W}$ des Oktaeders ist. Die Gruppen $\mathbb{W}$ und G haben beide 24 Elemente und sind daher isomorph. □

3 Ringtheorie

In diesem Kapitel geben wir eine kurze Einführung in die Ringtheorie. Ein Ring ist eine Menge mit 2 Verknüpfungen: Addition und Multiplikation. Das einfachste Beispiel eines Rings ist $\mathbb{Z}$. In Kapitel 1 haben wir $\mathbb{Z}$ als Gruppe mit Addition als Verknüpfung betrachtet und die Multiplikation ignoriert.

3.1 Definitionen

Definition 3.1.1 Ein *Ring* ist eine Menge R mit zwei Verknüpfungen $+$ (Addition) und $\cdot$ (Multiplikation), welche die folgenden Eigenschaften besitzen:

(R1) $(R, +)$ ist eine abelsche Gruppe. Das neutrale Element $0 = 0_R$ heißt *Nullelement*.

(R2) Die Multiplikation ist assoziativ und besitzt ein neutrales Element 1, das *Einselement*.

(R3) Es gelten die Distributivgesetze:

$$(a + b)c = ac + bc, \qquad \text{und} \qquad c(a + b) = ca + cb,$$

für alle $a, b, c \in R$.

Ein *Unterring* von R ist eine Teilmenge $S \subset R$, welche bezüglich Addition, Subtraktion und Multiplikation abgeschlossen ist und das 1-Element enthält.

Ein Ring heißt *kommutativ*, falls die Multiplikation kommutativ ist.

Beispiel 3.1.2 (a) Die Menge $\mathbb{Z}/m\mathbb{Z}$ ist ein Ring mit den Verknüpfungen Addition und Multiplikation modulo m.

(b) Sei $\mathbb{Z}[i] = \{a + bi \mid a, b \in \mathbb{Z}\} \subset \mathbb{C}$ die Menge der komplexen Zahlen mit ganzen Koeffizienten. Diese Menge ist ein Unterring von $\mathbb{C}$ und heißt *Ring der ganzen Gaußschen Zahlen*.

(c) Sei K ein Körper. Die Menge $M_{n,n}(K)$ der $n \times n$-Matrizen mit Koeffizienten in K ist ein Ring mit Matrixaddition und Matrixmultiplikation.

(d) Die Menge $\mathcal{C}(\mathbb{R})$ der stetigen Funktionen $f : \mathbb{R} \to \mathbb{R}$ mit

$$(f + g)(x) = f(x) + g(x), \qquad (f \cdot g)(x) = f(x) \cdot g(x), \qquad \text{für } f, g \in \mathcal{C}(\mathbb{R})$$

ist ein Ring.

(e) Der Nullring $R = \{0\}$ besteht aus einem einzigen Element $0 = 1$. Dies ist der einzige Ring mit $0 = 1$ (Überprüfen Sie dies!)

In der Definition eines Rings fordern wir nicht, dass jedes Element $a \in R$ ein multiplikatives Inverses besitzt.

Definition 3.1.3 (a) Ein Element $a \in R$ heißt *Einheit*, wenn a in R ein multiplikatives Inverses besitzt, d.h. es existiert ein $b \in R$ mit $ab = ba = 1$. Wir schreiben R^* für die Menge der Einheiten.

(b) Ein Element $a \in R$ eines Ringes heißt *Nullteiler*, falls ein $b \in R \setminus \{0\}$ mit $ab = 0$ oder $ba = 0$ existiert. Einen kommutativen Ring $R \neq \{0\}$ nennen wir *Integritätsring*, falls 0 der einzige Nullteiler ist.

(a) Sei R ein Integritätsring. Ein Element b heißt *Teiler* von a, wenn ein $c \in R$ mit $a = b \cdot c$ existiert. (Bezeichnung $b \mid a$.)

Definition 3.1.4 Ein *Körper* ist ein kommutativer Ring K, indem jedes Element $x \neq 0$ ein multiplikatives Inverses besitzt, d.h. $K^* = K \setminus \{0\}$.

Beispiel 3.1.5 (a) Die Menge $\mathbb{Z}/m\mathbb{Z}^* \subset \mathbb{Z}/m\mathbb{Z}$ der Einheiten in $\mathbb{Z}/m\mathbb{Z}$ besteht aus allen $\{0 < a < m \mid \mathrm{ggT}(a, m) = 1\}$ (Lemma 1.5.8). Es folgt, dass $\mathbb{Z}/m\mathbb{Z}$ genau dann ein Körper ist, wenn $m = p$ eine Primzahl ist. Wir schreiben auch $\mathbb{F}_p := \mathbb{Z}/p\mathbb{Z}$ für den Körper mit p Elementen.

(b) Sei K ein Körper. Die Einheiten in $M_{n,n}(K)$ sind die invertierbaren Matrizen $\mathrm{GL}_n(K)$.

Ist $n \geq 2$, dann besitzt $M_{n,n}(K)$ nichttriviale Nullteiler. Beispielsweise ist

$$\begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix} \cdot \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix} \cdot = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix} \in M(2 \times 2, \mathbb{R}) . \cdot$$

Beispiel 3.1.6 (Polynomringe) Neben $\mathbb{Z}$ sind die für uns wichtigsten Beispiele eines Ringes die Polynomringe. Als Abschluß des Abschnittes führen wir einige Begriffe für Polynomringe ein. Sei R ein Ring. Der Polynomring

$$R[x] = \{f(x) = \sum_{i=0}^{n} a_i x^i \mid a_i \in R\}$$

ist ein Ring mit Addition und Multiplikation von Polynomen als Verknüpfung.

Sei $f(x) = \sum_{i=0}^{n} a_i x^i \in R[x]$ ein Polynom mit *Koeffizienten* a_i in R. Das *Nullpolynom* $f = 0$ ist das Polynom, dessen Koeffizienten alle Null sind. Für $f \neq 0$ definieren wir den *Grad* von f als die größte Zahl n, sodass $a_n \neq 0$ ist (Bezeichnung: $\mathrm{Grad}(f)$). Den Grad des Nullpolynoms definieren wir als $-\infty$.

Wir nehmen nun an, dass R ein Integritätsring ist. Dann ist $R[x]$ ebenfalls ein Integritätsring. In diesem Fall gilt $\mathrm{Grad}(fg) = \mathrm{Grad}(f)\,\mathrm{Grad}(g)$. Hieraus folgt, dass

$$(R[x])^* = R^*[x]. \tag{3.1.1}$$

Falls $f(x) = \sum_{i=0}^{n} a_i x^i$ mit $a_n \neq 0$ ist, heißt $a_n x^n$ der *führende Term* von f. Ein Polynom vom Grad n heißt *normiert*, falls der führende Term x^n ist.

3.2 Ringhomomorphismen und Ideale

Im Rest von Kapitel 3 nehmen wir an, dass alle Ringe kommutativ sind. Einfachheitshalber schließen wir außerdem $R = \{0\}$ aus.

In diesem Abschnitt definieren wir Ringhomomorphismen. Ähnlich wie für Gruppen (§ 1.3), sind dies Abbildungen zwischen Ringen, die mit Addition und Multiplikation verträglich sind.

Definition 3.2.1 Eine Abbildung $\varphi : R \to R'$ zwischen Ringen heißt *Ringhomomorphismus*, falls für alle $a, b \in R$ gilt

- $\varphi(a+b) = \varphi(a) + \varphi(b)$,
- $\varphi(ab) = \varphi(a)\varphi(b)$,
- $\varphi(1_R) = 1_{R'}$.

Ein Ringhomomorphismus $\varphi : R \to R'$ heißt *Isomorphismus*, falls φ zusätzlich bijektiv ist. In diesem Fall nennt man R und R' *isomorph*. Wir bezeichnen dies als $R \simeq R'$.

Sei $\varphi : R \to R'$ ein Ringhomomorphismus. Es gilt $\varphi(0_R) = \varphi(0_R + 0_R) = \varphi(0_R) + \varphi(0_R)$. Da $-\varphi(0_R) \in R'$ existiert, folgt, dass $\varphi(0_R) = 0_{R'}$. (Vergleichen Sie zu Lemma 1.3.3). Das gleiche Argument funktioniert nicht immer für 1_R, da nicht jedes Element von R' eine Einheit ist. Daher müssen wir in Definition 3.2.1 explizit fordern, dass $\varphi(1_R) = 1_{R'}$ ist.

Ähnlich wie im Beweis von Lemma 1.3.3.(c) zeigt man, dass die Umkehrabbildung eines Ringisomorphismus auch ein Ringhomomorphismus ist.

Beispiel 3.2.2 Sei K ein Körper und $\alpha \in K$ ein Element. Die Evaluation eines Polynoms $f \in K[x]$ an der Stelle α

$$\varphi : K[x] \to K, \qquad f \mapsto f(\alpha)$$

definiert einen Ringhomomorphismus, da $(f+g)(\alpha) = f(\alpha) + g(\alpha)$ und $(fg)(\alpha) = f(\alpha)g(\alpha)$. Außerdem nimmt das Eins-Polynom an jeder Stelle den Wert 1 an.

Ebenso definiert

$$\varphi : \mathbb{R}[x] \to \mathbb{C}, \qquad f \mapsto f(i)$$

einen Ringhomomorphismus.

Folgender Satz ist eine Verallgemeinerung von Beispiel 3.2.2.

Satz 3.2.3 *Sei $\varphi : R \to R'$ ein Ringhomomorphismus und $\alpha \in R'$ ein Element. Es existiert ein eindeutiger Ringhomomorphismus $\psi : R[x] \to R'$ mit $\psi(x) = \alpha$ und $\psi(r) = \varphi(r)$, für $r \in R$.*

Beweis: Die Abbildung ψ definiert als $f(x) = \sum_{i=0}^{n} a_i x^i \mapsto \sum_{i=0}^{n} \varphi(a_i)\alpha^i$ ist ein Ringhomomorphismus. Also existiert ψ.

Man sieht leicht ein, dass jede Abbildung, die die Bedingungen des Satzes erfüllt, $f(x) = \sum_{i=0}^{n} a_i x^i$ auf $\sum_{i=0}^{n} \varphi(a_i)\alpha^i$ abbildet. Also ist ψ eindeutig. □

Beispiel 3.2.4 Die Abbildung $\varphi : \mathbb{Z} \to \mathbb{Z}/m\mathbb{Z}, \quad a \mapsto a \pmod m =: [a]$ ist ein Ringhomomorphismus. Sei $\alpha \in \mathbb{Z}/m\mathbb{Z}$. Satz 3.2.3 liefert einen Ringhomomorphismus

$$\psi : \mathbb{Z}[x] \to \mathbb{Z}/m\mathbb{Z}, \qquad f(x) = \sum_{i=0}^{n} a_i x^i \mapsto \sum_{i=0}^{n} [a_i]\alpha^i \in \mathbb{Z}/m\mathbb{Z}.$$

Definition 3.2.5 Sei $\varphi : R \to R'$ ein Ringhomomorphismus. Der *Kern* von φ ist definiert als

$$\ker(\varphi) = \{r \in R \mid \varphi(r) = 0_{R'}\}.$$

Die Definition des Kerns eines Ringhomomorphismus ist der Definition des Kerns eines Gruppenhomomorphismus sehr ähnlich. Der Unterschied ist, dass ein Ring sowohl ein 0-Element als auch ein 1-Element besitzt. Da $\varphi(1_R) = 1_{R'}$, ist $1_R \notin \ker(\varphi)$, außer wenn $R' = \{0\}$ der 0-Ring ist. Falls $R' \neq \{0\}$, ist $\ker(\varphi)$ also kein Unterring von R. Folgendes Lemma überprüft einige der Eigenschaften von $\ker(\varphi)$. Der Kern ist abgeschlossen gegenüber Addition und Multiplikation, erfüllt aber noch die stärkere Bedingung (b).

Lemma 3.2.6 *Sei $\varphi : R \to R'$ ein Ringhomomorphismus und sei $I = \ker(\varphi)$.*

(a) Für alle $a, b \in I$ gilt $a + b \in I$.

(b) Für $a \in I$ und $r \in R$ gilt $ra \in I$.

Beweis: Seien $a, b \in I$ und $r \in R$. Es gilt

$$\varphi(a + b) = \varphi(a) + \varphi(b) = 0 + 0 = 0,$$
$$\varphi(ra) = \varphi(r)\varphi(a) = \varphi(r) \cdot 0 = 0.$$

Also sind $a + b$ und ra in I enthalten. □

Da $\ker(\varphi)$ im Allgemeinen kein Unterring von R ist, führen wir einen neuen Namen für Teilmengen von R ein, die die Bedingungen von Lemma 3.2.6 erfüllen.

Definition 3.2.7 Eine Teilmenge I eines Rings R heißt *Ideal*, falls:

(I1) $(I, +) < (R, +)$ ist eine Untergruppe.

(I2) Für alle $a \in I$ und $r \in R$ gilt $ra \in I$.

Beispiel 3.2.8 (a) Lemma 3.2.6 sagt, dass der Kern eines Ringhomomorphismus ein Ideal ist.

(b) Sei $I < R$ ein Ideal mit $1 \in I$. Da $r \cdot 1 = r \in I$ für alle $r \in R$, folgt, dass $I = R$ ist.

(c) Sei K ein Körper. Die einzigen Ideale von K sind (0) und $(1) = K$. Sei nämlich $I \subset K$ ein Ideal mit $I \neq (0)$. Dann enthält I ein Element $a \neq 0$. Da K ein Körper ist, existiert $a^{-1} \in K$. Aber nun ist auch $1 = a^{-1}a \in I$. Aus (b) folgt daher, dass $I = K$ ist.

Ein Ideal $I < R$ ist insbesondere eine Untergruppe der abelschen Gruppe $(R, +)$. Sogar ist $I \lhd (R, +)$ ein Normalteiler (Lemma 1.6.6) und die Faktorgruppe

$$\bar{R} := R/I = \{a + I \mid a \in R\}$$

ist definiert. Die Addition auf $\bar{R}$ wurde in Theorem 1.6.4 als

$$(a + I) + (b + I) = (a + b) + I$$

definiert. Das folgende Theorem zeigt, dass $\bar{R}$ sogar ein Ring ist. Ein Beispiel dieser Konstruktion haben wir schon gesehen: Die Faktorgruppe $\mathbb{Z}/m\mathbb{Z}$ ist ein Ring (Beispiel 3.1.2.(a)).

Theorem 3.2.9 *Sei $I < R$ ein Ideal.*

(a) Die Faktorgruppe $\bar{R} = R/I$ besitzt eine Ringstruktur.

(b) *Die Abbildung*

$$\pi : R \to \bar{R}, \qquad a \mapsto a + I$$

ist ein surjektiver Ringhomomorphismus mit Kern I.

(c) *(***Erster Isomorphiesatz für Ringe***) Falls $\pi : R \to R'$ ein surjektiver Ringhomomorphismus mit Kern I ist, so ist $R' \simeq R/I$.*

Beweis: Wir definieren die Multiplikation auf $\bar{R} = \{a + I\}$ als

$$(a + I)(b + I) = (ab + I).$$

Wir zeigen die Wohldefiniertheit dieser Multiplikation.

Die Menge $P := (a + I)(b + I)$ ist die Menge der Elemente

$$P = \{(a + x)(b + y) = ab + ay + bx + xy \mid x, y \in I\}.$$

Da I ein Ideal ist, ist $ay + bx + xy \in I$, also ist $P = (a + I)(b + I) \subset ab + I$. Im Allgemeinen ist P aber selbst keine Linksnebenklasse. Zwei Linksnebenklassen sind entweder disjunkt oder gleich. Daher ist $ab + I$ die einzige Linksnebenklasse, die P enthält. Dies zeigt, dass die Multiplikation wohldefiniert ist.

Die Assoziativität der Multiplikation und die Distributivgesetze folgen aus der Assoziativität der Multiplikation und den Distributivgesetzen für R. Das 1-Element ist die Linksnebenklasse $1 + I$. Wir schließen, dass $\bar{R}$ ein Ring ist.

Teil (b) folgt direkt aus der Definition von $\bar{R}$.

Der Beweis von (c) ist dem Beweis von Satz 1.6.10 ähnlich. □

Wie für Gruppen, ist der erste Isomorphiesatz oft die einfachste Methode, den Faktorring zu bestimmen.

Beispiel 3.2.10 (a) In Beispiel 3.2.2 haben wir gesehen, dass

$$\varphi : \mathbb{R}[x] \to \mathbb{C}, \qquad f(x) \mapsto f(i)$$

ein surjektiver Ringhomomorphismus ist. Es gilt

$$I := \ker(\varphi) = \{f \in \mathbb{R}[x] \mid f(i) = 0\}.$$

Für $f \in \mathbb{R}[x]$ gilt $f(-i) = \overline{f(i)} = \bar{0} = 0$, wobei $^-$ die komplexe Konjugation ist. Polynomdivision impliziert, dass $(x^2 + 1) \mid f$. (Siehe auch Satz 4.1.8.(b)). Also ist $I = (x^2 + 1)$. Wir schließen, dass $\mathbb{C} \simeq \mathbb{R}[x]/(x^2 + 1)$ ist.

(b) Sei p eine Primzahl. Die Abbildung

$$\varphi : \mathbb{Z}[x] \to \mathbb{F}_p[x], \quad f(x) = \sum_{i=0}^{n} a_i x^i \mapsto \sum_{i=0}^{n} [a_i] x^i,$$

ist ein surjektiver Ringhomomorphismus. Hierbei ist $[a_i] = a_i \pmod p$.

Sei $f \in I := \ker(\varphi)$. Es gilt $f(x) = \sum_{i=0}^{n} a_i x^i$ mit $p \mid a_i$ für alle i. Also ist $f \in (p) = p\mathbb{Z}[x]$. Umgekehrt ist jedes Element $f \in p\mathbb{Z}[x]$ im Kern. Wir schließen, dass $I = p\mathbb{Z}[x]$ ist. Aus Theorem 3.2.9.(b) folgt, dass $\mathbb{Z}[x]/p\mathbb{Z}[x] \simeq \mathbb{F}_p[x]$ ist.

3.3 Hauptideal- und Euklidische Ringe

Sei $S = \{a_1, \ldots, a_n\} \subset R$ eine Menge von Elementen. Die Menge

$$(a_1, \ldots, a_n) := \{r_1 a_1 + \cdots + r_n a_n \mid r_i \in R\}$$

ist ein Ideal. Das Ideal $(a_1, \ldots, a_n)$ heißt das *von S erzeugte Ideal.*

Definition 3.3.1 Ein Ideal $I = (a) = aR = Ra$, dass von einem Element erzeugt wird, heißt *Hauptideal*. Ein *Hauptidealring* ist ein Ring, in dem jedes Ideal ein Hauptideal ist.

Der folgende Satz zeigt, dass $\mathbb{Z}$ ein Hauptidealring ist.

Satz 3.3.2 *Jedes Ideal I von $\mathbb{Z}$ ist ein Hauptideal.*

Beweis: Wir bestimmen die Ideale I von $\mathbb{Z}$. Jedes Ideal I von $\mathbb{Z}$ ist insbesondere auch eine Untergruppe. Es folgt, dass $I = (m) = m\mathbb{Z}$, für ein $m \geq 0$ (Theorem 1.1.16). Die Menge $I = (m)$ ist ein Ideal, nämlich, dass Ideal erzeugt von m. Es folgt, dass alle Ideale von $\mathbb{Z}$ von dieser Form sind. □

Satz 3.3.2 beruht auf der Division mit Rest in $\mathbb{Z}$: Dies ist der wesentliche Schritt im Beweis von Theorem 1.1.16. Euklidische Ringe sind Ringe, in denen eine Division mit Rest ähnlich wie in $\mathbb{Z}$ existiert.

Definition 3.3.3 Ein *Euklidischer Ring* ist ein Paar (R, δ), wobei R ein Integritätsring ist und

$$N : R \setminus \{0\} \to \mathbb{Z}_{>0}$$

eine Abbildung, sodass folgende Eigenschaft erfüllt ist: Für alle $a, b \in R$ mit $b \neq 0$ existieren $q, r \in R$ mit

$$a = qb + r, \quad \text{mit } N(r) < N(b) \text{ oder } r = 0.$$

In diesem Fall nennen wir q den *Quotienten* und r den *Rest* der Division von a durch b.

Beispiel 3.3.4 (a) Der Ring $\mathbb{Z}$ mit der Abbildung $N(a) = |a|$ ist ein Euklidischer Ring. Dies entspricht der Division mit Rest. Für $R = \mathbb{Z}$ fordern wir sogar die stärkere Bedingung $0 \leq r < |b|$. Unter dieser stärkeren Bedingung sind q und r eindeutig.

(b) Sei K ein Körper und $R = K[x]$ der Polynomring. Wir definieren $N(f) = \deg(f)$. Die Division mit Rest aus Definition 3.3.3 ist die Polynomdivision. Als Beispiel betrachten wir $f(x) = x^5 + x^2 - 4x - 2$ und $g(x) = 2x^4 + 2x^3 + 4x^2 + 6x + 2 \in \mathbb{Q}[x]$. Wir stellen fest, dass $f = gq + r$ mit $q(x) = (x-1)/2$ und $r(x) = -x^3 - 2x - 1$.

(c) Wir betrachten den Ring $\mathbb{Z}[i]$ der ganzen Gaußschen Zahlen (Beispiel 3.1.2.(b)) mit

$$N : \mathbb{Z}[i] \to \mathbb{Z}_{\geq 0}, \qquad z = a + bi \mapsto (a + bi)(a - bi) = a^2 + b^2.$$

Wir bemerken, dass $N(z) = |z|^2$, wobei $|z|$ der komplexe Betrag ist. Es folgt, dass $N(zw) = N(z)N(w)$. Wir nennen die Funktion N *Norm*.

Wir zeigen, dass $(\mathbb{Z}[i], N)$ ein Euklidischer Ring ist. (Siehe auch [4, § 7.3, Satz 7.3.4].) Sei dazu $\alpha, \beta \in \mathbb{Z}[i]$ mit $\beta \neq 0$. Wir betrachten die komplexe Zahl $z := \alpha/\beta$ und schreiben

$$z = \alpha/\beta = x + yi, \qquad x, y \in \mathbb{Q}.$$

Sei $q = m + ni$ die ganze Gaußsche Zahl mit $N(z - q)$ minimal. Diese Zahl muss nicht eindeutig sein. Es gilt, dass $|x - m| \leq 1/2$ und $|y - n| \leq 1/2$. Also gilt

$$N(z - q) = (x - m)^2 + (y - n)^2 \leq \left(\frac{1}{2}\right)^2 + \left(\frac{1}{2}\right)^2 = \frac{1}{2} < 1.$$

Setze $r = (z-q)\beta$. Aus der Definition von z folgt, dass $r = \alpha - q\beta \in \mathbb{Z}[i]$ ist. Außerdem gilt, dass

$$N(r) = N(z-q)N(\beta) < N(\beta).$$

Dies zeigt, dass $\mathbb{Z}[i]$ ein Euklidischer Ring ist.

Der folgende Satz ist eine direkte Verallgemeinerung vom Beweis von Theorem 3.3.2.

Satz 3.3.5 *Jeder Euklidische Ring ist ein Hauptidealring.*

Beweis: Sei (R, N) ein Euklidischer Ring und $I \subsetneq R$ ein Ideal. Das $I = (0)$ ist ein Hauptideal, also reicht es die Ideale $I \neq (0)$ zu betrachten.

Sei

$$n = \min\{N(a) \mid a \in I \setminus \{0\}\}.$$

Wir wählen $b \in I$ mit $N(b) = n$. Es gilt $(b) \subset I$. Wir behaupten, dass $I = (b)$.

Sei $a \in I$. Da R Euklidisch ist, existieren $q, r \in R$ mit $a = qb + r$ und $r = 0$ oder $N(r) < N(b)$. Es ist $r = a - qb \in I$. Die Wahl von b impliziert also, dass $r = 0$ und, dass $a \in (b)$. □

Korollar 3.3.6 *Sei K ein Körper. Dann ist der Polynomring $K[x]$ ein Hauptidealring. Ein Ideal $(0) \neq I < K[x]$ ist erzeugt vom (eindeutig bestimmten) normierten Polynom kleinsten Grades.*

Beweis: Der Ring $K[x]$ ist Euklidisch (Beispiel 3.3.4.(b)) mit Norm $N(f) = \mathrm{Grad}(f)$, also ein Hauptidealring (Satz 3.3.5). Die zweite Aussage folgt aus dem Beweis von Satz 3.3.5. □

Folgendes Korollar ist dem Korollar 1.1.17 ähnlich.

Korollar 3.3.7 *Sei R ein Hauptidealring und $f, g \in R$ nicht beide Null. Es existiert ein $d \in R \setminus \{0\}$, der* größte gemeinsame Teiler*, mit folgenden Eigenschaften:*

(a) d erzeugt das Ideal $I = (f, g)$,

(b) d ist ein Teiler von f und g,

(c) Jeder Teiler von f und g teilt auch d.

(d) Es existieren $r, s \in R$ mit $rf + sg = d$.

Beweis: Sei $I = (f, g)$. Da R ein Hauptidealring ist, existiert ein Erzeuger d von I, d.h. $I = (f, g) = (d)$. Dies zeigt Teil (a). Die Existenz von $r, s \in R$ wie in Teil (d) folgt aus $d \in (f, g)$.

Aus $f, g \in (f, g) = (d)$ folgt, dass d ein gemeinsamer Teiler von f und g ist. Sei e ein weiterer gemeinsamer Teiler von f und g. Dann existieren $a, b \in R$ mit $f = ae$ und $g = be$. Also gilt $d = rf + sg = e(ra + sb)$. Wir schließen, dass $e \mid d$. Dies zeigt Teil (b) und Teil (c). □

Beispiel 3.3.8 (a) Seien $f(x) = x^5 + x^2 - 4x - 2$ und $g(x) = 2x^4 + 2x^3 + 2x^2 + 6x + 2 \in \mathbb{Q}[x]$. Das Ideal $I = (x^5 + x^2 - 4x - 2, 2x^4 + 2x^3 + 4x^2 + 6x + 2) \subset \mathbb{Q}[x]$ ist ein Hauptideal mit Erzeuger $d := \mathrm{ggT}(f, g) = x^3 + 2x + 1$. (Überprüfen Sie dies!) Die Polynome r und s aus Korrolar 3.3.7.(d) sind

$$r = -1, \qquad s = -\frac{1}{2} + \frac{1}{2}x.$$

(b) Nicht jeder Ring ist ein Hauptidealring. Das Ideal $I = (2, x) < \mathbb{Z}[x]$ erzeugt von 2 und x ist kein Hauptideal. Wir zeigen dies, indem wir überprüfen, dass Korolar 3.3.7 in diesem Fall nicht gilt.

Wir nehmen an, dass $I = (2, x) = (d)$ ein Hauptideal ist. Dann ist $d \in \mathbb{Z}[x]$ ein gemeinsamer Teiler von 2 und x, also ist $d = \pm 1$ und es folgt, dass $I = (d) = (1) = \mathbb{Z}[x]$. Insbesondere ist $1 \in I$. Wie in Korollar 3.3.7 existieren Polynome $s, r \in \mathbb{Z}[x]$ mit $1 = s \cdot 2 + r \cdot x$. Dies ist aber unmöglich, wie man beispielsweise sieht in dem man die Gleichung modulo 2 reduziert. Es folgt, dass I kein Hauptideal ist.

(c) Das Ideal $J = (x^5 + x^2 - 4x - 2, 2x^4 + 2x^3 + 4x^2 + 6x + 2)$ aus (a), aufgefasst als Ideal in $\mathbb{Z}[x]$, ist **nicht** erzeugt von $d = x^3 + 2x + 1$. Es gilt zwar $d \mid f$ und $d \mid g$, aber es existieren keine Polynome $r, s \in \mathbb{Z}[x]$ mit $r \cdot f + s \cdot g = d$. Dies bedeutet, dass $d \notin J \subset \mathbb{Z}[x]$. Das Ideal $J < \mathbb{Z}[x]$ ist also auch kein Hauptideal.

3.4 Faktorisieren in Ringen

Der Fundamentalsatz der Arithmetik ([4, Theorem 1.2.4]) sagt, dass jede natürliche Zahl $n \geq 2$ als Produkt von Primzahlen geschrieben werden kann, wobei diese Zerlegung eindeutig bis auf Reihenfolge ist. In diesem Abschnitt zeigen wir eine ähnliche Aussage in Hauptidealringen. Der folgende Begriff verallgemeinert den Begriff Primzahl in $\mathbb{Z}$.

Definition 3.4.1 Sei R ein Integritätsring und $a, b, c \in R$. Ein Element $a \in R \setminus \{0\}$ heißt *irreduzibel*, wenn a keine Einheit ist und wenn für $a = b \cdot c$ gilt, dass b oder c eine Einheit ist. Sonst heißt a *reduzibel*.

Beispiel 3.4.2 (a) Die irreduziblen Elemente in $\mathbb{Z}$ sind

$$\{\pm p \mid p \text{ eine Primzahl}\}.$$

(b) Sei K ein Körper. Ein Polynom $f \in K[x]$ ist genau dann irreduzibel, wenn man f nicht als $f = g \cdot h$ mit $g, h \in K[x]$ Polynome von Grad $1 \leq g, h < \deg(f)$ schreiben kann. Hier benutzen wir, dass die Einheiten in $K[x]$ genau die Polynome $g \neq 0$ vom Grad 0 sind (Gleichung 3.1.1). In Abschnitt 3.5 betrachten wir Kriterien zur Überprüfung der Irreduzibilität eines Polynoms.

(c) Wir betrachten den Ring $\mathbb{Z}[i]$ der ganzen Gaußschen Zahlen. Im Beispiel 3.3.4.(c) haben wir gezeigt, dass $\mathbb{Z}[i]$ ein Euklidischer Ring ist. Sei $z = a \cdot bi \in \mathbb{Z}[i]^*$ eine Einheit. Im Beispiel 3.3.4.(c) haben wir gesehen, dass die Norm $N(a + bi) = a^2 + b^2 = |a + bi|^2$ multiplikativ ist. Es folgt, dass

$$N(z) \cdot N(z^{-1}) = N(1) = 1$$

und $N(z) = 1$. Wir schließen, dass $\mathbb{Z}[i]^* = \{\pm 1, \pm i\}$.

Ist $w \mid z$ ein Teiler in den Gaußschen Zahlen, dann ist $N(w)$ ein Teiler von $N(z)$ in $\mathbb{Z}$. Hieraus folgt, dass $z = 1 + i$ und $w = 1 + 2i$ irreduzibel in $\mathbb{Z}[i]$ sind: Die Norm dieser Elemente ist eine Primzahl in $\mathbb{Z}$.

Definition 3.4.3 Ein Integritätsring R heißt *faktoriell*, wenn folgende zwei Bedingungen erfüllt sind.

(a) Jedes $a \in R \setminus \{0\}$, das keine Einheit ist, lässt sich als

$$a = p_1 \cdots p_k$$

mit p_i irreduzibel schreiben.

(b) Sind

$$a = p_1 \cdots p_k = q_1 \cdots q_m$$

zwei Zerlegungen wie in (a), dann ist $m = k$ und nach eventuellem Umnummerieren gilt $p_i = \varepsilon_i q_i$ mit $\varepsilon_i \in R^*$ eine Einheit.

Der Fundamentalsatz der Arithmetik ist die Aussage, dass $\mathbb{Z}$ ein faktorieller Ring ist. Der wesentliche Schritt im Beweis der Eindeutigkeit der Zerlegung einer natürlichen Zahl als Produkt von Primzahlen ist die folgende Eigenschaft von irreduziblen Elementen. Für $R = \mathbb{Z}$ ist dies [4, Lemma 1.2.3]. In beliebigen Integritätsringen nennt man Elemente, die die Eigenschaft aus Lemma 3.4.4 erfüllen, Primelemente.

Lemma 3.4.4 *Sei R ein Hauptidealring und $f \in R$ irreduzibel. Falls $f \mid gh$ dann gilt $f \mid g$ oder $f \mid h$.*

Beweis: Wir nehmen an, dass $f \mid gh$, aber $f \nmid g$. Wir müssen zeigen, dass $f \mid h$. Im Hauptidealring R existiert $\mathrm{ggT}(f, g)$ (Korollar 3.3.7). Da f irreduzibel ist, ist $\mathrm{ggT}(f, g)$ entweder eine Einheit oder εf für eine Einheit ε. Wir haben angenommen, dass $f \nmid g$, also tritt der letzte Fall nicht auf. Wir schließen, dass $\mathrm{ggT}(f, g)$ eine Einheit ist.

Korollar 3.3.7 impliziert die Existenz von $r, s \in R$ mit $\mathrm{ggT}(f, g) = rf + sg$. Wir ergänzen die Gleichung mit h und erhalten $h\,\mathrm{ggT}(f, g) = rfh = sgh = rfh + sf$. Da $\mathrm{ggT}(f, g)$ eine Einheit ist, können wir diese Gleichung durch $\mathrm{ggT}(f, g)$ teilen und erhalten:

$$h = \mathrm{ggT}(f, g)^{-1}(rfh + sf).$$

Die rechte Seite ist von f teilbar, also gilt $f \mid h$. □

Satz 3.4.5 *Jeder nullteilerfreie Hauptidealring ist faktoriel.*

Beweis: Sei R ein nullteilerfreier Hauptidealring und $a \in R \setminus \{0\}$ keine Einheit.

Schritt I: Existenz einer Zerlegung von a in irreduziblen Elementen.

Ist a irreduzibel, gibt es nichts zu zeigen. Ansonsten existiert eine Zerlegung $a = a_1 \cdot b_1$ mit Nichteinheiten $a_1, b_1 \in R$. Wir wenden das Verfahren rekursiv auf a_1 und b_1 an.

Die Frage ist, ob dieses Verfahren immer nach endlich vielen Schritten abbricht. Angenommen, dies sei nicht der Fall. Dann existiert eine unendliche Folge $a = a_0, a_1, a_2 \ldots$ von Elementen, sodass a_{n+1} ein echter Teiler von a_n ist, d.h.

$$a_{n+1} \mid a_n \qquad a_n \nmid a_{n+1}.$$

Wir definieren

$$I := \cup_{n \geq 0}(a_n).$$

Man überlegt sich leicht, dass I ein Ideal von R ist. Da R nach Voraussetzung ein Hauptidealring ist, existiert ein Element $c \in R$ mit $I = (c)$. Das Ideal I enthält a_n, also gilt $c \mid a_n$ für alle n. Andererseits liegt c in einem der Ideale (a_n), also existiert ein m mit $a_m \mid c$. Da $c \mid a_{m+1}$ ist, folgt, dass

$$a_m \mid a_{m+1}.$$

Dies ist ein Widerspruch zur Annahme. Dies zeigt die Existenz einer Zerlegung wie in Definition 3.4.3.

Schritt II: Eindeutigkeit der Zerlegung.

Seien

$$a = p_1 \cdots p_k = q_1 \cdots q_m$$

zwei Zerlegungen mit p_i, q_i irreduzibel. Wir dürfen oBdA annehmen, dass $k \leq m$ ist. Wir zeigen die Aussage mit Induktion nach k.

Induktionsanfang: Für $k = 1$ gilt $a = p_1 = q_1 \cdots q_m$. Da p_1 irreduzibel ist, folgt $m = 1$ und $q_1 = p_1$.

Induktionsschritt: Da $p_1 \mid a$, folgt aus Lemma 3.4.4, dass p_1 einer der q_j teilt. Nach Umnummerieren der q_j dürfen wir annehmen, dass $p_1 \mid q_1$. Die Elemente p_1, q_1 sind irreduzibel, also ist $q_1 = \varepsilon p_1$ für eine Einheit ε. Wir kürzen p_1 auf beiden Seiten und erhalten:

$$p_2 \cdots p_k = \varepsilon q_2 \cdots q_m = q_2' \cdots q_m, \qquad \text{mit } q_2' = \varepsilon q_2.$$

Dies ist eine Zerlegung mit $k-1$ Termen auf der linken Seite. Die Aussage des Satzes folgt daher mit Induktion. □

Beispiel 3.4.6 (a) Wir haben gezeigt, dass Euklidische Ringe Hauptidealringe sind (Satz 3.3.5) und also auch faktoriell. Insbesondere sind $\mathbb{Z}$, $K[x]$ und $\mathbb{Z}[i]$ faktorielle Ringen. Weitere Beispiele findet man in [5, § 3.6]).

(b) Der Ring $\mathbb{Z}[\sqrt{-5}] = \{a + b\sqrt{-5} \mid a, b \in \mathbb{Z}\}$ ist nicht faktoriell. Genau wie für $R = \mathbb{Z}[i]$ definiert man einen Norm durch

$$N : \mathbb{Z}[\sqrt{-5}] \to \mathbb{Z}_{\geq 0}, \qquad z = a + b\sqrt{-5} \mapsto (a + b\sqrt{-5})(a - b\sqrt{-5}) = a^2 + 5b^2.$$

Es gilt $N(zw) = |zw|^2 = |z|^2|w|^2 = N(z)N(w)$. Ist also $w \mid z$ ein Teiler, dann gilt $N(w) \mid N(z)$. Hieraus folgt wie in Beispiel 3.3.4.(c), dass die Einheiten Norm 1 besitzen. Die einzigen Elemente mit $N(w) = 1$ sind $w = \pm 1$, also ist $\mathbb{Z}[\sqrt{-5}]^* = \{\pm 1\}$.

Wir betrachten die zwei Faktorisierungen

$$6 = 2 \cdot 3 = (1 + \sqrt{-5})(1 - \sqrt{-5}). \tag{3.4.1}$$

Wir behaupten, dass $2 \in R$ irreduzibel ist. Es gilt $N(2) = 4$. Ist $2 = wz$, dann gibt es folgende 2 Fälle:

(i) $N(w) = 1$ und $N(z) = 4$ oder umgekehrt,

(ii) $N(w) = N(z) = 2$.

Man zeigt leicht, dass kein z mit $N(z) = 2$ existiert, also tritt Fall (ii) nicht auf. Die Elemente mit Norm 1 sind Einheiten, also ist 2 irreduzibel ist. Ähnlich kann man auch zeigen, dass $3, 1 \pm \sqrt{-5}$ irreduzibel sind.

Wir haben $N(2) = 4 \neq N(1 + \sqrt{-5}) = N(1 - \sqrt{-5}) = 6$, also unterscheidet sich 2 nicht um eine Einheit von $1 \pm \sqrt{-6}$. Die beiden Zerlegungen in (3.4.1) sind echt verschieden. Wir schließen, dass $\mathbb{Z}[\sqrt{-5}]$ nicht faktoriel ist.

Aus $N(2) = 4 \nmid N(1 + \sqrt{-5}) = N(1 - \sqrt{-5}) = 6$ folgt auch, dass 2 kein Teiler von $(1 \pm \sqrt{-5})$ ist. Lemma 3.4.4 impliziert ebenfalls, dass $\mathbb{Z}[\sqrt{-5}]$ kein Hauptidealring und daher auch nicht faktoriell ist.

Ähnlich wie in Beispiel 3.3.8.(b) kann man schließen, dass das Ideal

$$\wp = (2, 1 + \sqrt{-5})$$

kein Hauptideal ist.

3.5 Faktorisieren von Polynomen

In diesem Abschnitt besprechen wir Methoden, ein Polynom in irreduzible Faktoren zu zerlegen. Insbesondere interessiert uns hier der Fall von Polynomen $f \in \mathbb{Q}[x]$ mit Koeffizienten in $\mathbb{Q}$.

Lemma 3.5.1 *Sei K ein Körper.*

(a) Jedes Polynom $f \in K[x]$ von Grad 1 ist irreduzibel.

(b) Ein Element $\alpha \in K$ ist genau dann eine Nullstelle von $f \in K[x]$, wenn $(x-\alpha) \mid f$.

(c) Sei $f \in K[x]$ ein Polynom zweiten oder dritten Grades. Dann ist f genau dann reduzibel, wenn f eine Nullstelle in K besitzt.

Beweis: Teil (a) ist klar. Sei $\alpha \in K$. Division mit Rest liefert

$$f(x) = q(x)(x-\alpha) + r(x), \qquad \mathrm{Grad}(r) < \mathrm{Grad}(x-\alpha) = 1.$$

Der Rest $r \in K$ ist folglich eine Konstante. Das Polynom $x - \alpha$ ist genau dann ein Teiler von f, wenn der $r = 0$, also, wenn $f(\alpha) = 0$. Dies zeigt (b).

Sei f ein Polynom zweiten oder dritten Grades. Ist f reduzibel, lässt sich f schreiben als $f(x) = g(x)h(x)$ mit $1 \leq \mathrm{Grad}(g) \leq \mathrm{Grad}(h) < \mathrm{Grad}(f) \leq 3$. Aus $\mathrm{Grad}(f) = \mathrm{Grad}(g) + \mathrm{Grad}(h)$ folgt, dass $\mathrm{Grad}(g) = 1$. Es gilt, dass $g(x) = c(x-\alpha)$ und α ist eine Nullstelle von f. Die Umkehrung folgt aus (b). □

Ist f ein Polynom mit $\mathrm{Grad}(f) \geq 4$ ohne Nullstellen in K, dann folgt nicht, dass f irreduzibel ist: Ein Polynom $f \in K[x]$ vierten Grades ist irreduzibel, wenn f keine Nullstellen in K und keine Faktoren von Grad 2 besitzt. Die Faktoren von Grad 2 kann man durch Ausprobieren finden: Sei $f(x) = \sum_{i=0}^{4} a_i x^i \in K[x]$. Wir nehmen an, dass $f = g \cdot h$ mit $g(x) = \sum_{i=0}^{2} b_i x^i$ und $h(x) = \sum_{i=0}^{2} c_i x^i$. OBdA kann man annehmen, dass $a_4 = b_2 = c_2 = 1$ ist. Die Existenz eines Faktors 2ten Grades kann man nun, wie im folgenden Beispiel durch Koeffizientenvergleich überprüfen.

Beispiel 3.5.2 Wir betrachten, dass Polynom $x^4+1 \in \mathbb{Q}[x]$. Sei $\zeta_8 = e^{i\pi/4} = (\sqrt{2} + \sqrt{2}i)/2 \in \mathbb{C}$ eine primitive 8te Einheitswurzel. Die Nullstellen von f in $\mathbb{C}$ sind ζ_8^{2j+1} für $j = 1, 3, 5, 7$. (Am einfachsten sieht man dies mit Hilfe von Polarkoordinaten.) Insbesondere besitzt f keine Nullstellen in $\mathbb{Q}$.

Wir nehmen an, dass f das Produkt zweier Polynome von Grad 2 ist:

$$x^4 + 1 = (x^2 + ax + b)(x^2 + cx + d), \qquad a, b, c, d \in \mathbb{Q}.$$

Koeffizientenvergleich ergibt:

$$a + c = 0, \quad ac + b + d = 0, \quad ad + bc = 0, \quad bd = 1.$$

Einsetzen der ersten und letzten Gleichung in die beiden Anderen, ergibt:

$$b^2 - a^2 b + 1 = 0, \qquad a(1 - b^2) = 0.$$

Die zweite Gleichung impliziert, dass $a = 0$ oder $b = \pm 1$. Ist $a = 0$, dann ist $b^2 + 1 = 0$. Aber diese Gleichung besitzt keine Lösung $b \in \mathbb{Q}$. Ist $b = \pm 1$, dann ist $a^2 = \pm 2$. Diese Gleichung besitzt ebenfalls keine Lösung $a \in \mathbb{Q}$. Wir schließen, dass $f \in \mathbb{Q}[x]$ irreduzibel ist.

Satz 3.5.3 (Gauß) *Sei $f \in \mathbb{Z}[x]$ ein irreduzibles Polynom über $\mathbb{Z}$. Dann ist f auch irreduzibel über $\mathbb{Q}$.*

Beweis: Sei $f \in \mathbb{Z}[x]$ ein irreduzibles Polynom über $\mathbb{Z}$. Wir nehmen an, dass eine nicht-triviale Zerlegung $f = g \cdot h$ über $\mathbb{Q}$ existiert, d.h. $g, h \in \mathbb{Q}[x]$ sind nicht-konstante Polynome.

Es existiert ein $n = a \cdot b \in \mathbb{Z}$ und eine Zerlegung

$$nf = g^{(1)} \cdot h^{(1)}$$

mit $g^{(1)} = a \cdot g, h^{(1)} = b \cdot h \in \mathbb{Z}[x]$. Wähle für n beispielsweise das Produkt der Nenner der Koeffizienten von g und h. Schreibe $g^{(1)} = \sum_{i=0}^{s} g_i x^i$ und $h^{(1)} = \sum_{j=0}^{t} h_j x^j$.

Sei p ein Primfaktor von n. Wir behaupten, dass p entweder alle Koeffizienten von $g^{(1)}$ oder alle Koeffizienten von $h^{(1)}$ teilt. Nehmen wir an, dies würde nicht gelten. Seien i und j minimal mit $p \nmid g_i$ und $p \nmid h_j$. Da $p \mid n$, teilt p den Koeffizienten c_{i+j} von x^{i+j} in $g^{(1)}h^{(1)}$. Es gilt

$$c_{i+j} = \sum_{k=0}^{i+j} h_k g_{i+j-k}.$$

Die Wahl von i und j impliziert, dass p jeden Term der Summe außer $h_j g_i$ teilt. Dies liefert einen Widerspruch, da p außerdem c_{i+j} teilt.

OBdA dürfen wir annehmen, dass p alle Koeffizienten von $g^{(1)}$ teilt. Schreibe $n = pn_1$ und $g^{(1)} = pg^{(2)}$. Nach Kürzung des Faktors p, erhalten wir

$$n_1 f = g^{(2)} h^{(1)}.$$

Wiederholtes Anwenden des Arguments liefert eine Faktorisierung

$$f = \bar{g}\bar{h}$$

mit $\bar{g}, \bar{h} \in \mathbb{Z}[x]$ und $\bar{g} = \alpha g$ und $\bar{h} = \beta h$ für $\alpha, \beta \in \mathbb{Z}$, ist dies eine nicht-triviale Zerlegung von f über $\mathbb{Z}$. Dies widerspricht die Irreduzibilität von f über $\mathbb{Z}$. □

Beispiel 3.5.4 Wir benutzen die Idee des Satzes von Gauß (Satz 3.5.3) um Nullstellen von $f \in \mathbb{Q}[x]$ zu finden. Nach Multiplikation mit einer geeigneten ganzen Zahl, dürfen wir annehmen, dass $f(x) = \sum_{i=0}^{n} a_i x^i \in \mathbb{Z}[x]$ ganze Koeffizienten besitzt. Außerdem dürfen wir oBdA annehmen, dass $a_n \neq 0$ und $a_0 \neq 0$ sind. Sei $\alpha = b/c \in \mathbb{Q}$ eine Nullstelle von f mit $\mathrm{ggT}(b, c) = 1$. Lemma 3.5.1.(b), zusammen mit Satz 3.5.3, impliziert, dass

$$f = (cx - b)g, \qquad \text{mit } g \in \mathbb{Z}[x].$$

Koeffizientenvergleich liefert, dass $b \mid a_0$ und $c \mid a_n$. Zusätzlich darf man annehmen, dass c positiv ist. Diese Bedingungen liefern eine (endliche) Liste von möglichen Nullstellen. Einsetzen dieser möglichen Nullstellen in f, liefert alle Nullstellen.

Sei zum Beispiel $f = 2x^3 + x^2 - x + 3$. Für b kommen nur die Werte $\pm 1, \pm 3$ in Frage. Für c kommen nur die Werte $1, 2$ in Frage. Ausprobieren aller 8 Möglichkeiten liefert, dass $\alpha = -3/2$ die einzige rationale Nullstelle von f ist.

Theorem 3.5.5 (Eisenstein-Kriterium) *Sei*

$$f(x) = \sum_{i=0}^{n} a_i x^i \in \mathbb{Z}[x].$$

Sei $p \in \mathbb{Z}$ eine Primzahl, sodass

(a) $p \nmid a_n$,

(b) $p \mid a_i, \qquad i = 0, \ldots n-1,$

(c) $p^2 \nmid a_0$.

So ist f irreduzibel über $\mathbb{Q}$.

Beweis: Sei f wie in der Aussage des Theorems. Es reicht zu zeigen, dass f irreduzibel über $\mathbb{Z}$ ist (Satz 3.5.3). Wir nehmen an, dass $f = g \cdot h$ mit $g = \sum_{i=0}^{s} g_i x^i \in \mathbb{Z}[x]$ und $h = \sum_{j=0}^{t} h_j x^j \in \mathbb{Z}[x]$ Polynome kleineren Grades. Es gilt $a_0 = g_0 h_0$. Da $p \mid a_0$ und $p^2 \nmid a_0$, schließen wir, dass entweder $p \mid g_0$ oder $p \mid h_0$. OBdA dürfen wir annehmen, dass $p \mid g_0$ und $p \nmid h_0$.

Falls p alle Koeffizienten g_i von g teilt, so wäre p ein Teiler von a_n, aber dies widerspricht (a). Sei $1 \leq i \leq s$ minimal, sodass $p \nmid g_i$. Es gilt

$$a_i = \sum_{k=0}^{i} g_k h_{i-k}.$$

Da $s = \mathrm{Grad}(g) < \mathrm{Grad}(f) = n$ ist, folgt, dass $i < n$ ist. Insbesondere ist p ein Teiler von a_i. Die Primzahl p teilt alle Termen der rechten Seite außer $g_i h_0$. Dies liefert einen Widerspruch, da $p \nmid g_i$ und $p \nmid h_0$. Wir schließen, dass f irreduzibel über $\mathbb{Z}$ ist. □

Beispiel 3.5.6 (a) Das Polynom $x^n - 2 \in \mathbb{Q}[x]$ ist irreduzibel für alle $n \geq 2$. Dies folgt aus dem Eisenstein-Kriterium (Theorem 3.5.5) angewendet mit $p = 2$.

Für $n = 3$ kann man auch benutzen, dass

$$f(x) = (x - \sqrt[3]{2})(x - \zeta_3 \sqrt[3]{2})(x - \zeta_3^2 \sqrt[3]{2}) \in \mathbb{C}[x],$$

wobei $\zeta_3 := e^{2\pi i/3}$ eine primitive 3te Einheitswurzel und $\sqrt[3]{2}$ die reelle 3te Wurzel aus 2 ist. (Dies sieht man am Einfachsten mit Hilfe von Polarkoordinaten.)

Die Nullstellen von f in $\mathbb{C}$ sind nicht in $\mathbb{Q}$. Der Beweis hiervon ist im Wesentlichen ein Spezialfall vom Beweis von Theorem 3.5.5. Die Irreduzibilität von f folgt also ebenfalls aus Lemma 3.5.1.(c), da $\mathrm{Grad}(f) = 3$ und die Nullstellen von f nicht in $\mathbb{Q}$ sind.

(b) Sei

$$f(x) = \frac{2}{9}x^5 + \frac{5}{3}x^4 + x^3 + \frac{1}{3} \in \mathbb{Q}[x].$$

Das Eisenstein-Kriterium (Theorem 3.5.5) angewendet mit $p = 3$ zeigt, dass $9f = 2x^5 + 15x^4 + 9x^3 + 3$ irreduzibel über $\mathbb{Z}$ ist. Der Satz von Gauß (Satz 3.5.3) zeigt, dass f ist irreduzibel über $\mathbb{Q}$ ist.

Eine weitere Möglichkeit ein Polynom $f \in \mathbb{Z}[x]$ auf Irreduzibilität zu überprüfen, ist f modulo p zu reduzieren:

Lemma 3.5.7 *Sei $f(x) = \sum_{i=0}^{n} a_i x^i \in \mathbb{Z}[x]$ und p eine Primzahl mit $p \nmid a_n$. Falls die Reduktion $\bar{f} \in \mathbb{F}_p[x]$ von f modulo p irreduzibel ist, ist f irreduzibel in $\mathbb{Q}[x]$.*

Beweis: Die Annahme $p \nmid a_n$ impliziert, dass $\bar{f} \in \mathbb{F}_p[x]$ den gleichen Grad wie $f \in \mathbb{Z}[x]$ besitzt. Falls $f \in \mathbb{Q}[x]$ reduzibel ist, existieren nicht-konstante Polynome $g, h \in \mathbb{Z}[x]$ mit $f = gh$ (Satz 3.5.3). Da $\mathrm{Grad}(f) = \mathrm{Grad}(\bar{f})$ und $\bar{f} = \bar{g}\bar{h}$, folgt, dass $\mathrm{Grad}(g) = \mathrm{Grad}(\bar{g})$ und $\mathrm{Grad}(h) = \mathrm{Grad}(\bar{h})$. Wir schließen, dass $\bar{f} \in \mathbb{F}_p[x]$ auch reduzibel ist. □

Sei $f \in K[x]$ ein Polynom und $\alpha \in K$ eine Nullstelle von f. Wiederholtes Anwenden von Lemma 3.5.1.(b) liefert, dass

$$f(x) = (x-\alpha)^m g(x), \qquad \text{mit } g(\alpha) \neq 0$$

für ein Polynom $g(x) \in K[x]$. Wir nennen m die *Vielfachheit* der Nullstelle α. Falls $m > 1$, so heißt α eine *mehrfache Nullstelle* von f.

Sei $f(x) = \sum_{i=0}^{n} a_i x^i$. Wir definieren die *formale Ableitung* von f als

$$f'(x) := \sum_{i=1}^{n} i a_i x^{i-1}.$$

Falls $K = \mathbb{R}$ ist, ist die formale Ableitung einfach die Ableitung von f nach x. Die formale Ableitung erfüllt die gleichen Rechenregeln wie die Ableitung. Zum Beispiel gilt $(f+g)' = f' + g'$ und $(f \cdot g)' = f'g + fg'$. Das folgende Lemma zeigt, dass die formale Ableitung ähnliche Eigenschaften wie die Ableitung besitzt.

Lemma 3.5.8 *Sei $\alpha \in K$ eine Nullstelle von $f(x) \in K[x]$. Die Nullstelle α ist genau dann eine mehrfache Nullstelle von f, wenn $f'(\alpha) = 0$ ist.*

Beweis: Sei $\alpha \in K$ eine Nullstelle von f mit Vielfachheit $m > 1$. Wir schreiben $f(x) = (x-\alpha)^m g(x)$ mit $g(\alpha) \neq 0$. Es gilt

$$f'(x) = m(x-\alpha)^{m-1} g(x) + (x-\alpha)^m g'(x).$$

Da $m > 1$ ist, gilt also, dass $f'(\alpha) = 0$. Die Umkehrung beweist man ähnlich. □

Satz 3.5.9 *Sei K ein Körper und sei $f \in K[x]$ ein Polynom von Grad n. Das Polynom f besitzt höchstens n Nullstellen in K gezählt mit Vielfachheit.*

Beweis: Seien $\alpha_1, \ldots, \alpha_r \in K$ die Nullstellen von f, wobei die Nullstelle α_i die Vielfachheit n_i besitzt. Lemma 3.5.1.(b) impliziert, dass

$$f(x) = g(x) \prod_{i=1}^{r} (x-\alpha_i)^{n_i}$$

ist, wobei $g(\alpha_i) \neq 0$ für $i = 1, \ldots, r$ ist. Also ist $\sum_{i=1}^{r} n_i \leq \text{Grad}(f) = n$. □

4 Körper

4.1 Algebraische und transzendente Körpererweiterungen

Definition 4.1.1 Sei K ein Körper. Eine *Körpererweiterung* von K ist ein Körper L, der K als Teilkörper enthält. Bezeichnung: L/K.

Beispiel 4.1.2 Der Körper der reellen Zahlen $\mathbb{R}$ ist eine Körpererweiterung des Körpers der rationalen Zahlen $\mathbb{Q}$, kurz: $\mathbb{R}/\mathbb{Q}$. Ebenso: $\mathbb{C}/\mathbb{R}$, $\mathbb{C}/\mathbb{Q}$.

Ist L/K eine Körpererweiterung, so können wir L als K-Vektorraum auffassen: Die Vektoraddition ist die übliche Addition in L, und die skalare Multiplikation ist die Einschränkung der Multiplikation $\cdot : L \times L \to L$ auf die Teilmenge $K \times L$. Man „vergisst“ einfach, dass man auch zwei beliebige Elemente aus L miteinander multiplizieren kann.

Definition 4.1.3 Der *Grad* einer Körpererweiterung L/K ist die Dimension von L als K-Vektorraum:

$$[L : K] := \dim_K L \in \{1, 2, 3, \ldots, \infty\}.$$

Die Erweiterung L/K heißt *endlich*, wenn $[L : K] < \infty$.

Beispiel 4.1.4 Der Körper $\mathbb{C}$ ist eine 2-dimensionale Körpererweiterung von $\mathbb{R}$, da $(1, i)$ eine $\mathbb{R}$-Basis von $\mathbb{C}$ bildet.

Definition 4.1.5 Sei L/K eine Körpererweiterung. Ein Element $\alpha \in L$ heißt *algebraisch* über K, wenn ein Polynom $f \in K[x]$ mit $f \neq 0$ und $f(\alpha) = 0$ existiert. Ein Element $\alpha \in L$, das nicht algebraisch über K ist, heißt *transzendent* über K. Eine Körpererweiterung L/K heißt *algebraisch*, wenn jedes Element $\alpha \in L$ algebraisch über K ist. Sonst heißt L/K transzendent.

Bemerkung 4.1.6 Sei L/K eine Körpererweiterung und $\alpha \in L$ transzendent über K. Dann sind $1, \alpha, \alpha^2, \ldots$ linear unabhängig über K. Es folgt, dass $[L : K] = \infty$. Eine endliche Erweiterung ist also immer algebraisch. Die Umkehrung gilt nicht: Es existieren algebraische Erweiterungen L/K mit $[L : K] = \infty$.

Beispiel 4.1.7 (a) Die reelle Zahl $\sqrt{2} \in \mathbb{R}$ ist algebraisch über $\mathbb{Q}$, da sie eine Nullstelle des Polynoms $x^2 - 2 \in \mathbb{Q}[x]$ ist.

(b) Die reellen Zahlen $e = 2,71828\cdots$ und $\pi = 3,141592\cdots$ sind transzendent über $\mathbb{Q}$ (siehe [8, Kapitel 6]).

(c) Die komplexe Zahl $2\pi i \in \mathbb{C}$ ist transzendent über $\mathbb{Q}$ (das folgt aus (b)), aber algebraisch über $\mathbb{R}$. Insbesondere ist $[\mathbb{R} : \mathbb{Q}] = \infty$.

(d) Die Körpererweiterung $\mathbb{C}/\mathbb{R}$ ist eine algebraische Erweiterung: Jede komplexe Zahl $z = a + bi$ ist die Nullstelle des Polynoms

$$f(x) = (x - z)(x - \bar{z}) = x^2 - 2ax + a^2 + b^2 \in \mathbb{R}[x].$$

Dies folgt auch aus der Tatsache, dass $[\mathbb{C} : \mathbb{R}] = 2$ (Bemerkung 4.1.6).

Satz 4.1.8 *Sei L/K eine Körpererweiterung und $\alpha \in L$ ein Element aus L, welches algebraisch über K ist.*

(a) Es existiert ein eindeutiges Polynom $f \in K[x]$, für das gilt:

(i) f ist normiert und irreduzibel,

(ii) $f(\alpha) = 0$.

(b) Jedes Polynom $g \in K[x]$ mit $g(\alpha) = 0$ wird von f aus (a) geteilt.

Beweis: Die Menge

$$I := \{\, g \in K[x] \mid g(\alpha) = 0 \,\}$$

ist ein Ideal. Der Ring $K[x]$ ist ein Hauptidealring (Korollar 3.3.6), also ist I ein Hauptideal ist. Korollar 3.3.6 sagt, dass I vom normierten Polynom minimalen Grades in I erzeugt wird.

Wir müssen zeigen, dass f irreduzibel ist. Sei $f = g \cdot h$ mit $g, h \in K[x]$. Nach Einsetzen von α erhalten wir

$$0 = f(\alpha) = g(\alpha) \cdot h(\alpha).$$

Da K ein Körper und somit insbesondere nullteilerfrei ist, ist entweder $g(\alpha) = 0$ oder $h(\alpha) = 0$. Wir nehmen an, dass $g(\alpha) = 0$ ist. Da $f \in I$ ein Element minimalen Grades und $g \neq 0$ ist, folgt, dass $\mathrm{Grad}(g) \geq \mathrm{Grad}(f)$. Wir schließen, dass $g(x) = cf(x)$ und $h(x) = 1/c$ für ein $c \in K^*$. Also ist f irreduzibel. Dies zeigt (a). Aussage (b) folgt ebenfalls. □

Definition 4.1.9 Das Polynom f aus Satz 4.1.8 heißt das *Minimalpolynom* von α bezüglich des Körpers K. Bezeichnung: $f = \min_K(\alpha)$.

Beispiel 4.1.10 (a) Sei $d \in \mathbb{Z}\backslash\{0\}$ ein Nichtquadrat und sei $\alpha \in \mathbb{C}$ eine Quadratwurzel aus d, d.h. $\alpha^2 = d$. Das Minimalpolynom von α über $\mathbb{Q}$ ist $f := \min_{\mathbb{Q}}(\alpha) = x^2 - d$: Das Polynom f ist irreduzibel, weil $\mathrm{Grad}(f) = 2$ und die Nullstellen $\pm\alpha \notin \mathbb{Q}$ sind (Lemma 3.5.1.(b)).

(b) Beispiel 3.5.2 zeigt, dass $\min_{\mathbb{Q}}(\zeta_8) = x^4 + 1$.

Theorem 4.1.11 *Seien $F \subset K \subset L$ Körper. Es gilt*

$$[L : F] = [L : K][K : F].$$

Beweis: Dies ist ein bekannter Satz aus der Linearen Algebra, siehe zum Beispiel [1, Theorem 3.4]. Wir wiederholen den Beweis.

Sei dazu $\mathbb{B}_1 = (y_j)_{j\in J}$ eine Basis von L als K-Vektorraum und $\mathbb{B}_2 = (x_i)_{i\in I}$ eine Basis von K als F-Vektorraum. Wir behaupten, dass $\mathbb{B}_3 = (x_i y_j)_{i\in I, j\in J}$ eine Basis von L als F-Vektorraum ist.

Sei $\alpha \in L$. Da $\mathbb{B}_1$ eine Basis von L als K-Vektorraum ist, können wir α eindeutig als Linearkombination $\alpha = \sum_{j\in J} c_j y_j$ mit $c_j \in K$ darstellen, wobei höchstens endlich viele $c_j \neq 0$ sind. Die c_j sind Elemente aus K. Sie können also eindeutig als Linearkombination $c_j = \sum_{i\in I} d_{i,j} x_i$ mit $d_{i,j} \in F$ dargestellt werden. Wir schließen, dass $\alpha = \sum_{i,j} d_{i,j} x_i y_j$. Also ist $\mathbb{B}_3$ ein Erzeugendensystem von L über F.

Wir nehmen an, dass $d_{i,j} \in F$ mit $S := \sum_{i,j} d_{i,j} x_i y_j = 0$ existieren, wobei höchstens endlich viele der $d_{i,j}$ ungleich Null sind. Wir schreiben die Summe um als $S = \sum_j (\sum_i d_{i,j} x_i) y_j$, wobei $\sum_i d_{i,j} x_i \in K$ ist. Da $\mathbb{B}_1 = (y_j)_{j\in J}$ eine Basis von L als K-Vektorraum ist, folgt, dass $\sum_i d_{i,j} x_i = 0$ für alle i. Da $\mathbb{B}_2 = (x_i)_{i\in I}$ ein Basis von K als F-Vektorraum ist, folgt, dass $d_{i,j} = 0$ für alle i und j. Wir schließen, dass die Vektoren $(x_i y_j)_{i\in I, j\in J}$ linear unabhängig sind, also ist $\mathbb{B}_3$ eine Basis von L als F-Vektorraum. □

Man beachte, dass es im Beweis von Theorem 4.1.11 nicht nötig ist anzunehmen, dass L/F eine endliche Körpererweiterung ist. Der Satz sagt, dass $[L : F] = \infty$ genau dann, wenn $[L : K] = \infty$ oder $[K : F] = \infty$ ist. Der Beweis funktioniert auch in diesem Fall.

4.2 Konstruktion von algebraischen Körpererweiterungen

In diesem Abschnitt diskutieren wir eine allgemeine Methode um algebraische Körpererweiterungen zu konstruieren. Diese Methode beruht auf folgendem Satz:

Satz 4.2.1 *Sei K ein Körper und $f \in K[x]$ ein normiertes, irreduzibles Polynom.*

(a) Der Quotientenring $L := K[x]/(f)$ ist eine endliche Körpererweiterung von K. Dieser Körper heißt Stammkörper *von f.*

(b) Sei $\alpha := x + (f) \in L$. Dann gilt $f(\alpha) = 0$ und $f = \min_K(\alpha)$ ist das Minimalpolynom von α über K.

(c) *Es gilt* $[L : K] = \mathrm{Grad}(f) =: n$. *Eine Basis von* L *als* K*-Vektorraum ist* $1, \alpha, \ldots, \alpha^{n-1}$.

Beweis: Der Quotientenring L enthält K als Teilring. Wir zeigen, dass L ein Körper ist. Dazu reicht es zu zeigen, dass jedes Element $g + (f) \in L \setminus \{0\}$ ein multiplikatives Inverses besitzt. Alle andere Körperaxiome sind automatisch erfüllt.

Wir bemerken, dass genau dann $g + (f) = 0 + (f) \in L$, wenn $g \in (f)$, also wenn $f \mid g$. Sei also $g \in K[x]$ mit $f \nmid g$. Das Polynom f ist nach Annahme irreduzibel, also ist $\mathrm{ggT}(f, g) = 1$. Korollar 3.3.7 impliziert, dass Polynome $r, s \in K[x]$ mit $rf + sg = 1$ existieren. In L gilt daher

$$sg + (f) = 1 + (f)$$

und $s + (f)$ ist das Inverses von $g + (f)$. Es folgt, dass L ein Körper ist. Dies zeigt (a).

Das Element $\alpha := x + (f)$ erfüllt

$$f(\alpha) = f(x) + (f) = 0 + (f) \in L = K(x)/(f).$$

Wir haben angenommen, dass $f \in K[x]$ normiert und irreduzibel ist, also ist f das Minimalpolynom von α. Dies zeigt (b).

Sei $g + (f) \in L$ ein beliebiges Element. Division mit Rest liefert $q, r \in K[x]$ mit $g = qf + r$ und $\mathrm{Grad}(r) < \mathrm{Grad}(f) = n$. Wir schreiben $r(x) = \sum_{i=0}^{n-1} c_i x^i$ mit $c_i \in K$. Es gilt

$$g(x) + (f) = r(x) + (f) = \sum_{i=0}^{n-1} c_i (x + (f)) = \sum_{i=0}^{n-1} c_i \alpha^{n-1}.$$

Es folgt, dass $(1, \alpha, \ldots, \alpha^{n-1})$ ein Erzeugendensystem von L als K-Vektorraum ist.

Die Zahl $n = \mathrm{Grad}(\min_K(\alpha))$ ist minimal mit der Eigenschaft, dass $(1, \alpha, \alpha^2, \ldots, \alpha^n)$ linear abhängig über K ist. Insbesondere ist $(1, \alpha, \ldots, \alpha^{n-1})$ eine Basis von L als K-Vektorraum. Dies zeigt (c). □

Bemerkung 4.2.2 (a) Satz 4.2.1.(b) sagt, dass jedes irreduzible Polynom das Minimalpolynom eines Elements α in einem Erweiterungskörper ist.

(b) Es gilt auch eine stärkere Version von Satz 4.2.1: Der Ring $L := K[x]/(f)$ ist genau dann ein Körper, wenn $f \in K[x]$ irreduzibel ist. Dies beruht auf der Beobachtung, dass $g + (f) \in L$ genau dann eine Einheit ist, wenn $\mathrm{ggT}(f, g) = 1$. Diese Aussage zeigt man ähnlich wie Satz 4.2.1. Eine ähnliche Aussage für $\mathbb{Z}/m\mathbb{Z}$ haben wir in Beispiel 3.1.5.(b) gesehen.

Definition 4.2.3 Sei L/K eine Körpererweiterung und $S \subset L$ eine beliebige Teilmenge. Der Körper $K(S)$ ist der kleinste Teilkörper von L/K, der S enthält. Wir nennen $M := K(S)$ die Körpererweiterung von K *erzeugt* von S. Alternativ sagen wir auch, dass M aus K entsteht durch *Adjunktion* der Elemente von S.

Lemma 4.2.4 *Sei* L/K *eine Körpererweiterung und* $\alpha \in L$ *algebraisch über* K *mit Minimalpolynom* $f = \min_K(\alpha)$. *Die Abbildung*

$$K[x]/(f) \xrightarrow{\sim} K(\alpha), \qquad g + (f) \mapsto g(\alpha)$$

ist ein Isomorphismus.

Beweis: Die Abbildung

$$\varphi : K[x] \to K(\alpha), \qquad g \mapsto g(\alpha)$$

ist ein Ringhomomorphismus (Satz 3.2.3). Offensichtlich ist φ surjektiv. Satz 4.1.8 impliziert, dass $\ker(\varphi) = (f)$. Daher folgt die Aussage aus Theorem 3.2.9.(b). $\square$

Bemerkung 4.2.5 Mit Hilfe von Satz 4.2.1.(c), gibt Lemma 4.2.4 eine konkrete Beschreibung der Elemente von $K(\alpha)$:

$$K(\alpha) = \{\sum_{i=0}^{n-1} c_i \alpha^i \mid c_i \in K,\ f(\alpha) = 0\}.$$

Hierbei ist $n = \mathrm{Grad}(\min_K(\alpha))$.

Beispiel 4.2.6 (a) Sei $\zeta_3 := e^{2\pi i/3}$ eine primitive 3te Einheitswurzel. Dann ist $f(x) := \min_{\mathbb{Q}}(\zeta_3) = (x^3 - 1)/(x - 1) = x^2 + x + 1$. Also ist

$$R := \mathbb{Q}[x]/(f) \simeq \mathbb{Q}(\zeta_3).$$

Wir berechnen das multiplikative Inverse von $0 \neq a + b\zeta_3 \in \mathbb{Q}(\zeta_3)$ und finden

$$\frac{1}{a + b\zeta_3} = \frac{a + b\zeta_3^2}{(a + b\zeta_3)(a + b\zeta_3^2)} = \frac{a + b\zeta_3^2}{a^2 - ab + b^2} = \frac{a - b - b\zeta_3}{a^2 - ab + b^2} \in \mathbb{Q}(\zeta_3).$$

Hier haben wir die Relation $1 + \zeta_3 + \zeta_3^2 = 0$ mehrmals benutzt.

(b) Wir berechnen $[\mathbb{Q}(\sqrt{2}, i) : \mathbb{Q}]$, wobei $i^2 = -1$ ist. Theorem 4.1.11 sagt, dass

$$[\mathbb{Q}(\sqrt{2}, i) : \mathbb{Q}] = [\mathbb{Q}(\sqrt{2}, i) : \mathbb{Q}(\sqrt{2})][\mathbb{Q}(\sqrt{2}) : \mathbb{Q}]$$

ist. Beispiel 4.1.10.(a) impliziert, dass $[\mathbb{Q}(\sqrt{2}) : \mathbb{Q}] = 2$. Außerdem folgt, dass

$$\min_{\mathbb{Q}(\sqrt{2})}(i) \mid \min_{\mathbb{Q}}(i) = x^2 + 1.$$

Das Polynom $x^2 + 1$ ist genau dann das Minimalpolynom von i über $\mathbb{Q}(\sqrt{2})$, wenn $x^2 + 1$ irreduzibel über $\mathbb{Q}(\sqrt{2})$ ist, also genau dann, wenn $x^2 + 1$ keine Nullstellen in $\mathbb{Q}(\sqrt{2})$ besitzt (Lemma 3.5.1). Diese Bedingung ist erfüllt, da

$$\pm i \notin \mathbb{Q}(\sqrt{2}) \subset \mathbb{R}.$$

Wir schließen, dass $[\mathbb{Q}(\sqrt{2}, i) : \mathbb{Q}(\sqrt{2})] = 2$, und daher, dass

$$[\mathbb{Q}(\sqrt{2}, i) : \mathbb{Q}] = 2 \cdot 2 = 4.$$

Der Beweis von Theorem 4.1.11 liefert uns, dass $(1, \sqrt{2}, i, \sqrt{2}i = \sqrt{-2})$ eine Basis von $\mathbb{Q}(\sqrt{2}, i)$ als $\mathbb{Q}$-Vektorraum ist.

Wir behaupten, dass $\mathbb{Q}(\sqrt{2}, i) = \mathbb{Q}(\zeta_8)$ ist, wobei $\zeta_8 \in \mathbb{C}$ wie in Beispiel 4.1.10.(b) eine primitive 8te Einheitswurzel ist. Sei z.B.

$$\zeta_8 = \cos(\pi/4) + i\sin(\pi/4) = \frac{\sqrt{2}}{2} + \frac{\sqrt{2}}{2}i \in \mathbb{Q}(\sqrt{2}, i).$$

Es folgt, dass $\mathbb{Q}(\zeta_8) \subset \mathbb{Q}(\sqrt{2}, i)$ ist.

Beispiel 4.1.10.(b) impliziert, dass $[\mathbb{Q}(\zeta_8) : \mathbb{Q}] = \mathrm{Grad}(\min_{\mathbb{Q}}(\zeta_8)) = 4 = [\mathbb{Q}(\sqrt{2}, i) : \mathbb{Q}] = 4$. Wir schliessen, dass $\mathbb{Q}(\sqrt{2}, i) = \mathbb{Q}(\zeta_8)$ ist.

Korollar 4.2.7 (Kronecker) *Sei K ein Körper und $f \in K[x]$. Es existiert eine Körpererweiterung L/K, in der f in Linearfaktoren zerfälllt, d.h. es existieren $c, \alpha_i \in L$ mit*

$$f(x) = c \prod_{i=1}^{n} (x - \alpha_i) \in L[x].$$

Beweis: Wir schreiben

$$f = \prod_i f_i \in K[x]$$

als Produkt von irreduziblen Polynomen in $K[x]$. Das Polynom f zerfällt genau dann in Linearfaktoren in $K[x]$, wenn alle Faktoren f_i Grad 1 besitzen. Ist dies nicht der Fall, existiert mindestens ein Faktor f_i mit $\mathrm{Grad}(f_i) \geq 2$. Im Stammkörper $M := K[x]/(f_i)$ von f_i besitzt f also mindestens eine Nullstelle mehr als in K (Satz 4.2.1.(b)).

Wir betrachten nun die Zerlegung von f in irreduzible Faktoren in $M[x]$ und argumentieren wie im vorherigen Schritt. Das Polynom f besitzt in jeder Körpererweiterung L/K höchstens $n := \mathrm{Grad}(f)$ Nullstellen (Satz 1.5.7), also terminiert das Verfahren nach endlich vielen Schritten. Die Aussage folgt mit Induktion. □

Beispiel 4.2.8 Sei $\alpha := \sqrt[3]{2} \in \mathbb{R}$ die reelle 3te Wurzel aus 2. Offensichtlich ist α eine Nullstelle von $f(x) := \min_{\mathbb{Q}}(\alpha) = x^3 - 2$. Die Irreduzibilität von f folgt aus dem Eisenstein-Kriterium (Beispiel 3.5.6.(a)).

Sei $L = \mathbb{Q}(\sqrt[3]{2}) \simeq \mathbb{Q}[x]/(x^2 - 2)$ der Stammkörper von f. In L besitzt f die Nullstelle α, aber keine weitere Nullstellen. Es gilt nämlich

$$f(x) = (x - \alpha)(x - \zeta_3\alpha)(x - \zeta_3^2\alpha) \in \mathbb{C}[x],$$

wobei $\zeta_3 = e^{2\pi i/3}$ eine primitive 3te Einheitswurzel ist. Der Körper $\mathbb{Q}(\sqrt[3]{2})$ ist ein Teilkörper von $\mathbb{R}$, aber $\zeta_3\alpha, \zeta_3^2\alpha \notin \mathbb{R}$. Mit Hilfe der Relation $\zeta_3 + \zeta_3^2 = -1$ finden wir

$$f(x) = (x - \alpha)(x^2 + \alpha x + \alpha^2) =: (x - \alpha)g \in L[x].$$

Über $M := L(\alpha, \zeta_3) \simeq L(\alpha, \zeta_3\alpha) \simeq L[x]/(g)$ zerfällt f in Linearfaktoren.

Wir bemerken, dass $[L : \mathbb{Q}] = \mathrm{Grad}(f) = 3$ und $[M : L] = \mathrm{Grad}(g) = 2$. Also ist $[M : K] = 3 \cdot 2 = 6$ (Theorem 4.1.11).

4.3 Konstruktion mit Zirkel und Lineal

Für Plato (427 - 347 v. Chr.) waren Gerade und Kreis die einzigen „perfekten“ geometrische Figuren. In der klassischen griechischen Geometrie führte dies dazu, dass man sich für Konstruktionen interessierte, die nur mit einem Zirkel und einem (unmarkierten) Lineal ausgeführt werden können. Damit sind erstaunlich viele Konstruktionen möglich. Drei Konstruktionen konnten die Griechen nicht ausführen: Die Würfelverdopplung, die Winkeldreiteilung und die Quadratur des Kreises. Ziel dieses Abschnitts ist es zu verstehen, warum diese Konstruktionen unmöglich sind. Mehr Details zur Geschichte finden Sie auf der MacTutor-Webseite.

Zuerst geben wir eine mathematische Formulierung des Problems. Gegeben ist eine Menge $M_0 \subset \mathbb{R}^2$ von Punkten im 2-dimensionalen euklidischen Raum ausgestattet mit der Standardnorm $||(x_1, x_2)^t|| = \sqrt{x_1^2 + x_2^2}$. Wir betrachten die folgenden zwei Konstruktionen:

K1 (Lineal): Male eine Gerade durch zwei Punkte $p, q \in M_0$,

K2 (Zirkel): Male einen Kreis mit Mittelpunkt $p \in M_0$ und Radius $d(q_1, q_2)$, den Abstand zweier Punkte $q_1, q_2 \in M_0$.

Ein Punkt $p \in \mathbb{R}^2$ heißt *konstruierbar in einem Schritt aus* M_0, falls p der Schnittpunkt von Geraden oder Kreisen aus Konstruktion (K1) oder (K2) ist. Ein Punkt $p \in \mathbb{R}^2$ heißt *konstruierbar aus* M_0, falls es eine Kette von Punkten $p_1, p_2, \cdots, p_r \in \mathbb{R}^2$ gibt, sodass p_{i+1} konstruierbar in einem Schritt aus $M_i := M_0 \cup \{p_1, p_2, \ldots, p_{i-1}\}$ ist. Die Menge der konstruierbaren Punkte bezeichnen wir mit $\mathrm{KON}(M_0) \subset \mathbb{R}^2$.

Beispiel 4.3.1 (a) Seien $p_1, p_2 \in \mathbb{R}^2$ und $M_0 = \{p_1, p_2\}$. Wir konstruieren den Mittelpunkt der Strecke p_1p_2 (siehe Abbildung 4.3.1).

1. Sei L_1 die Gerade durch p_1 und p_2.
2. Sei C_1 der Kreis mit Mittelpunkt p_1 und Radius $d(p_1, p_2)$.
3. Sei C_2 der Kreis mit Mittelpunkt p_2 und Radius $d(p_1, p_2)$. Die zwei Schnittpunkte der Kreise C_1 und C_2 nennen wir r_1, r_2.
4. Sei L_2 die Gerade durch r_1 und r_2. Der Schnittpunkt r_3 von L_1 mit L_2 ist der gesuchte Punkt.

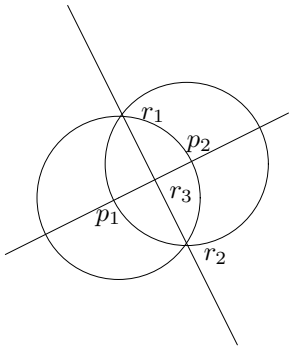


Abbildung 4.3.1: Konstruktion des Mittelpunktes

Die zugehörigen Mengen der konstruierbaren Punkte sind

$$M_0 = \{p_1, p_2\} \subset M_1 = \{p_1, p_2, r_1\} \subset$$
$$\subset M_2 = \{p_1, p_2, r_1, r_2\} \subset M_3 = \{p_1, p_2, r_1, r_2, r_3\}.$$

(b) Seien p, q zwei Punkte und sei L die Gerade durch p und q. Wir konstruieren eine Gerade L' durch p senkrecht zu L (aus den Punkten $M_0 = \{p, q\}$.) Wir konstruieren dazu die folgenden Geraden und Kreise (siehe Abbildung 4.3.2):

1. Sei C_1 der Kreis mit Mittelpunkt p und Radius $d(p, q)$. Den zweiten Schnittpunkt von C_1 mit L nennen wir q'.
2. Sei C_2 (bzw. C_3) der Kreis mit Mittelpunkt q (bzw. q') und Radius $d(q, q')$. Die Schnittpunkte von C_2 und C_3 nennen wir r_1, r_2.
3. Die gesuchte Gerade L' ist die Gerade durch r_1 und r_2.

Alternativ kann man diese Konstruktion auch auf der Konstruktion aus (a) zurückführen: Man konstruiere zuerst q' wie im Schritt 1. Mit Hilfe von Konstruktion (a) konstruiere man nun den Mittelpunkt der Strecke qq'. Die Gerade L_1 aus (a) ist die gesuchte Gerade.

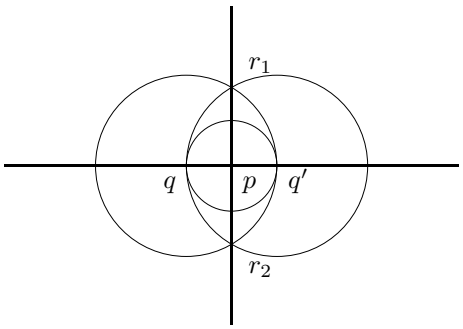


Abbildung 4.3.2: Konstruktion einer senkrechten Gerade

Wir erklären, wie man das Problem der Beschreibung der konstruierbaren Punkte algebraisch formulieren kann. Sei dazu $M_0 \subset \mathbb{R}^2$ vorgegeben. Sei $p \in \mathrm{KON}(M)$ ein konstruierbarer Punkt und $p_1, p_2, \ldots, p_r = p$ die zugehörige Kette der konstruierbaren Punkte, wie oben. Wir schreiben $p_i = (x_i, y_i)$. Sei K_0 der Zwischenkörper von $\mathbb{R}/\mathbb{Q}$ erzeugt von allen x- und y-Koordinaten der Punkte in M_0. Wir definieren induktiv einen Körper

$$K_i = K_{i-1}(x_i, y_i)$$

durch Adjunktion der Koordinaten von p_i. Wir erhalten also eine Kette

$$\mathbb{Q} \subset K_0 \subset K_1 \subset \cdots \subset K_r \subset \mathbb{R}$$

von Zwischenkörpern von $\mathbb{R}/\mathbb{Q}$.

Lemma 4.3.2 *Wir benutzen die obige Bezeichnung. Die Koordinaten $x_i, y_i \in K_i$ sind Nullstellen eines quadratischen Polynoms mit Koeffizienten in K_{i-1}. Insbesondere gilt* $\mathrm{Grad}(\min_{K_{i-1}}(x_i)) \leq 2$ *und* $\mathrm{Grad}(\min_{K_{i-1}}(y_i)) \leq 2$.

Beweis: Wir müssen drei Fälle unterscheiden: r_i ist konstruiert als Schnittpunkt zweier Kreise, zweier Geraden oder als Schnittpunkt eines Kreises mit einer Gerade. Wir betrachten nur den Fall, dass r_i als Schnittpunkt eines Kreises C mit einer Gerade L konstruiert ist. Die anderen zwei Fälle sind ähnlich.

Wir gehen davon aus, dass der Kreis C und die Gerade L mit Hilfe von Punkten aus K_{i-1} konstruiert sind. Sei $D = (d_1, d_2)$ das Zentrum und w der Radius des Kreises C. Die Annahme, dass C und L mit Hilfe von Punkten mit Koordinaten aus K_{i-1} konstruiert sind, impliziert, dass L die Gerade durch zwei Punkte $A = (a_1, a_2), B = (b_1, b_2)$ mit Koordinaten in K_{i-1} und dass $d_1, d_2 \in K_{i-1}$ sind. Da w der Abstand zweier Punkte mit Koordinaten in K_{i-1} ist, folgt aus dem Satz von Pythagoras, dass $w^2 \in K_{i-1}$ ist.

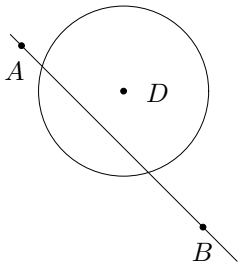
Die Gleichungen für L und C sind:

$$\begin{aligned} L: &\quad y = a_2 + \frac{b_2 - a_2}{b_1 - a_1}(x - a_1), \\ C: &\quad (x - c_1)^2 + (y - c_2)^2 = w^2. \end{aligned} \tag{4.3.1}$$

Einsetzen liefert:

$$(x - c_1)^2 + \left[\frac{b_2 - a_2}{b_1 - a_1}(x - a_1) + a_2 - c_2\right]^2 = w^2.$$

Dies ist eine quadratische Gleichung mit Koeffizienten in K_{i-1} für die x-Koordinate der Schnittpunkte. Sehr ähnlich kann man (4.3.1) auch nach y auflösen. Dies liefert



nach Einsetzen eine quadratische Gleichung mit Koeffizienten in K_{i-1} für die y-Koordinate der Schnittpunkte. □

Satz 4.3.3 *Sei $M_0 \subset \mathbb{R}^2$ eine Menge und $\mathbb{Q} \subset K_0 \subset \mathbb{R}$ der Zwischenkörper erzeugt von den x- und y-Koordinaten der Punkte aus M_0. Sei $p = (x, y) \in \mathbb{R}^2$ ein konstruierbarer Punkt, so ist der Grad*

$$[K_0(x, y) : K_0]$$

eine 2-er-Potenz.

Beweis: Sei $p = (x, y) \in \mathbb{R}^2$ ein konstruierbarer Punkt und

$$\mathbb{Q} \subset K_0 \subset K_1 \subset \cdots K_r \subset \mathbb{R}$$

die entsprechende Kette von Zwischenkörpern von $\mathbb{R}/\mathbb{Q}$ wie oben. Per Definition ist $K_i = K_{i-1}(x_i, y_i)$, wobei $p_i = (x_i, y_i)$ der i-te Punkt in der Konstruktionskette ist. Lemma 4.3.2 impliziert, dass $[K_{i-1}(x_i) : K_{i-1}] \in \{1, 2\}$ und $[K_{i-1}(y_i) : K_{i-1}] \in \{1, 2\}$. Theorem 4.1.11 impliziert, dass

$$[K_i : K_{i-1}] = [K_{i-1}(x_i, y_i) : K_{i-1}(x_i)][K_{i-1}(x_i) : K_{i-1}].$$

Da $[K_{i-1}(x_i, y_i) : K_{i-1}(x_i)]$ kleiner gleich $[K_{i-1}(y_i) : K_{i-1}]$ ist, folgt, dass $[K_i : K_{i-1}]$ ein Teiler von 4 ist. Der Satz folgt nun aus der Definition der K_i und Theorem 4.1.11. □

Theorem 4.3.4 *Die Quadratur des Kreises ist mit Zirkel und Lineal unmöglich.*

Als Teil der Fragestellung muss man eigentlich auch die Ausgangsmenge M_0 vorgeben. Wir nehmen hier als Ausgangmenge $M_0 = \{p_0, p_1\}$, wobei p_0 der Mittelpunkt des Kreises und p_1 ein Punkt auf dem Kreis ist.

Beweis: Gegeben ist ein Kreis C. Ohne Einschränkung dürfen wir annehmen, dass C Mittelpunkt $(0, 0)$ und Radius 1 hat. Ohne Einschränkung dürfen wir also annehmen, dass $M_0 = \{p_0 = (0, 0), p_1 = (1, 0)\}$ und $K_0 = \mathbb{Q}$ ist. Die Aufgabe ist ein Quadrat Q mit gleichem Flächeninhalt wie der Kreis C, also mit Fläche π, zu konstruieren. Dies bedeutet, dass wir den Punkt $q := (\sqrt{\pi}, 0)$ konstruieren müssen.

Satz 4.3.3 impliziert, dass, falls q konstruierbar wäre, $[\mathbb{Q}(\sqrt{\pi}) : \mathbb{Q}]$ eine 2-er-Potenz wäre, insbesondere wäre $\mathbb{Q}(\sqrt{\pi})/\mathbb{Q}$ eine algebraische Erweiterung. Da $[\mathbb{Q}(\sqrt{\pi}) : \mathbb{Q}(\pi)] = 2$, ist $\mathbb{Q}(\sqrt{\pi})/\mathbb{Q}$ genau dann eine algebraische Erweiterung, wenn $\mathbb{Q}(\pi)/\mathbb{Q}$ algebraisch ist. Aber π ist transzendent über $\mathbb{Q}$ (Beispiel 4.1.7). Wir schließen, dass die Quadratur des Kreises unmöglich ist. □

Theorem 4.3.5 *Es ist nicht möglich, mit Zirkel und Lineal das Volumen eines Würfels zu verdopplen.*

Beweis: Gegeben ist nun ein regelmäßiger Würfel W. Ohne Einschränkung dürfen wir annehmen, dass $(0,0,0)$ und $(1,0,0)$ Ecken des Würfels sind. Wir nehmen also $K_0 = \mathbb{Q}$. Die Verdopplung des Würfels ist nun äquivalent zur Aussage, dass $(\sqrt[3]{2}, 0, 0)$ ein konstruierbarer Punkt ist. Satz 4.3.3 impliziert, dass, wenn $(\sqrt[3]{2}, 0, 0)$ konstruierbar ist, $[\mathbb{Q}(\sqrt[3]{2}) : \mathbb{Q}]$ eine 2-er-Potenz ist. Beispiel 4.2.8 impliziert aber, dass $[\mathbb{Q}(\sqrt[3]{2}) : \mathbb{Q}] = 3$ ist. Also ist die Würfelverdopplung unmöglich. □

4.4 Endliche Körper

Für jeden Ring R definiert

$$\psi : \mathbb{Z} \to R, \qquad n \mapsto n \cdot 1 \tag{4.4.1}$$

einen Ringhomomorphismus, wobei für $n > 0$ positiv $n \cdot 1 = 1 + \cdots + 1$ (n-mal) und $(-n) \cdot 1 = -(n \cdot 1)$ ist. Satz 3.3.2 impliziert, dass ein $m \geq 0$ existiert, sodass $\ker(\psi) = m\mathbb{Z}$. Diese Zahl m heißt *Charakteristik* von R. (Bezeichnung: $\mathrm{Char}(R)$.) Falls $\mathrm{Char}(R) = m \neq 0$, ist m die kleinste positive Zahl, sodass $m \cdot 1 = 0$ in R gilt.

Lemma 4.4.1 *Die Charakteristik eines Körpers K ist entweder 0 oder eine Primzahl.*

Beweis: Sei $\psi : \mathbb{Z} \to K$ wie in (4.4.1) und sei $I := \ker(\psi) = m\mathbb{Z}$. Falls m eine zusammengesetzte Zahl ist, existieren $a, b \in \mathbb{N} \setminus \{1, m\}$ mit $m = ab$. Also gilt $0 = \psi(m) = \psi(ab) = \psi(a)\psi(b) = (a \cdot 1)(b \cdot 1)$. Aus der Minimalität von m folgt, dass $(a \cdot 1) \neq 0$ und $(b \cdot 1) \neq 0$. Also ist $a \cdot 1 \in K$ ein Nullteiler. Dies liefert einen Widerspruch zu den Körperaxiomen (Definition 3.1.4). Das Lemma folgt. □

Der kleinste Teilkörper eines Körpers K heißt *Primkörper*.

Sei K ein Körper der Charakteristik 0. Dann ist die Abbildung $\psi : \mathbb{Z} \to K$ injektiv. Hieraus folgt, dass $\mathbb{Q}$ ein Teilkörper von K ist.

Falls K ein Körper der Charakteristik $p > 0$ ist, folgt aus dem ersten Isomorphiesatz (Theorem 3.2.9.(c)), dass $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$ ein Teilkörper von K ist. In diesem Fall ist der Primkörper von K also $\mathbb{F}_p$.

In diesem Abschnitt bestimmen wir alle Körper mit endlich vielen Elementen. Solche Körper nennen wir *endliche Körper*. Ein endlicher Körper enthält nie $\mathbb{Q}$ als Teilkörper. Wir schließen, dass $\mathrm{Char}(K) = p > 0$ eine Primzahl ist.

Lemma 4.4.2 *Sei F ein endlicher Körper und $p = \mathrm{Char}(F)$. Die Anzahl der Elemente von F ist $q = p^n$.*

Beweis: Ein endlicher Körper F der Charakteristik $p > 0$ enthält $\mathbb{F}_p$ als Primkörper. Insbesondere ist F eine Körpererweiterung von $\mathbb{F}_p$ von endlichem Grad $n = [F : \mathbb{F}_p]$. Sei $(\alpha_1 = 1, \alpha_2, \ldots, \alpha_n)$ eine Basis von F als $\mathbb{F}_p$-Vektorraum. Jedes Element $x \in F$ lässt sich eindeutig als

$$x = \sum_{i=1}^{n} c_i \alpha_i, \qquad c_i \in \mathbb{F}_p$$

schreiben. Die Anzahl der Elemente von F ist daher $q = p^n$. □

Wir werden zeigen, dass für jede Primzahlpotenz $q = p^n$ ein Körper mit q Elementen existiert (Theorem 4.4.5). Außerdem zeigen wir, dass zwei endliche Körper mit gleicher Kardinalität isomorph sind (Theorem 4.4.11). Der Körper mit q Elementen werden wir mit $\mathbb{F}_q$ bezeichnen.

Beispiel 4.4.3 Wir konstruieren einen Körper $\mathbb{F}_4$ mit 4 Elementen. Das Polynom $f(x) = x^2 + x + 1 \in \mathbb{F}_2[x]$ ist ein irreduzibles Polynom $f(x) \in \mathbb{F}_2[x]$ von Grad 2. (Es ist sogar das Einzige.) Also ist

$$\mathbb{F}_4 := \mathbb{F}_2[x]/(x^2 + x + 1)$$

ein Körper mit 4 Elementen. Sei $\alpha \in \mathbb{F}_4$ die Restklasse von x. Die Elemente $(1, \alpha)$ formen eine Basis von $\mathbb{F}_4$ als $\mathbb{F}_2$-Vektorraum. Es gilt

$$\mathbb{F}_4 = \{0, 1, \alpha, 1 + \alpha\}.$$

Man sollte den Körper $\mathbb{F}_4$ nicht mit dem Ring $\mathbb{Z}/4\mathbb{Z}$ verwechseln.

Wir beweisen zunächst ein einfaches Lemma. Die Aussage ist als „freshman's dream“ bekannt.

Lemma 4.4.4 *Sei F ein Körper der Charakteristik $p > 0$. Dann gilt*

$$(\alpha + \beta)^p = \alpha^p + \beta^p, \qquad \text{für alle } \alpha, \beta \in F.$$

Beweis: Sei $1 \leq i \leq p - 1$. Dann ist

$$\binom{p}{i} = \frac{p!}{i!(p-1)!} = 0 \in \mathbb{F}_p \subset F.$$

Hier haben wir benutzt, dass p den Zähler aber nicht den Nenner des Bruchs teilt. Die Aussage des Lemmas folgt aus der binomischen Formel. □

Theorem 4.4.5 *Sei $q = p^n$ eine Primzahlpotenz.*

(a) Es existiert ein Körper F mit q Elementen.

(b) Die Elemente von F sind Nullstellen des Polynoms $f_q(x) := x^q - x$. Dieses Polynom zerfällt in Linearfaktoren über F.

Beweis: Wir beweisen zuerst (b). Sei F ein Körper mit q Elementen. Die multiplikative Gruppe $F^* = F \setminus \{0\}$ enthält $q - 1$ Elemente. Die Ordnung eines Elements $\alpha \in F^*$ ist also ein Teiler von $q - 1$ (Satz 1.5.7). Insbesondere ist α eine Nullstelle von $x^{q-1} - 1$, also auch von $f_q = x^q - x$. Das Element $0 \in F$ ist ebenfalls eine Nullstelle dieses Polynoms. Das Polynom f_q besitzt also q verschiedene Nullstellen in F. Wir schließen, dass f_q über F als

$$f_q(x) = \prod_{\alpha \in F} (x - \alpha)$$

in Linearfaktoren zerfällt.

Wir beweisen die Existenz eines Körpers F mit q Elementen. Teil (b) impliziert, dass die Elemente von F genau die Nullstellen von f_q sind.

Sei L/F eine Körpererweiterung in dem f in Linearfaktoren zerfällt. Eine solche Körpererweiterung existiert nach Korollar 4.2.7. Da $q = p^n \equiv 0 \in \mathbb{F}_p$, gilt

$$f_q'(x) = qx^{q-1} - 1 \equiv -1 \in \mathbb{F}_p[x].$$

Also ist $\mathrm{ggT}(f_q, f_q') = 1$. Lemma 3.5.8 impliziert, dass f_q keine mehrfache Nullstellen besitzt. Wir schließen, dass f_q genau q Nullstellen in L besitzt.

Sei $F \subset L$ die Menge der Nullstellen von f_q. Wir behaupten, dass F ein Körper ist. Die Definition von F impliziert, dass

$$F = \{\alpha \in L \mid \alpha^q = \alpha\}.$$

Sind $\alpha, \beta \in F$, dann gilt

$$(\alpha\beta)^q = \alpha^q\beta^q, \quad (-\alpha)^q = -\alpha, \quad (1/\alpha)^q = 1/\alpha^q.$$

Außerdem folgt mit Induktion aus Lemma 4.4.4, dass

$$(\alpha + \beta)^q = (\alpha^p + \beta^p)^{p^{n-1}} = \cdots = \alpha^q + \beta^q \in L.$$

Insbesondere ist $\alpha + \beta \in F$. Wir schließen, dass F ein Körper ist. □

Beispiel 4.4.6 Sei $q = 3^2 = 9$. Wir faktorisieren das Polynom $x^q - x$ in irreduzible Faktoren in $\mathbb{F}_3[x]$, zum Beispiel mit Hilfe des Maple-Kommandos `Factor(`$x^q - x$`) mod 3`:

$$f_9(x) = x^9 - x = x(x-1)(x+1)(x^2+1)(x^2-x-1)(x^2+x-1) \in \mathbb{F}_3[x].$$

Wir wählen einen der irreduziblen Faktoren von f_9 von Grad 2, zum Beispiel $g(x) = x^2 + 1$. Wir können $\mathbb{F}_9$ nun darstellen als

$$\mathbb{F}_9 = \mathbb{F}_3[x]/(x^2+1) = \{a_0 + a_1\alpha \mid a_j \in \mathbb{F}_3\},$$

wobei α die Relation $\alpha^2 = -1$ erfüllt.

Der Beweis von Theorem 4.4.5 impliziert, dass $x^q - x$ über $\mathbb{F}_9$ in Linearfaktoren zerfällt. Wir finden als Zerlegung von x^2+1, x^2-x-1 und x^2+x-1 in irreduziblen Faktoren in $\mathbb{F}_9[x]$:

$$x^2 + 1 = (x+\alpha)(x-\alpha), \qquad x^2 - x - 1 = (x+\alpha+1)(x-\alpha+1),$$
$$x^2 + x - 1 = (x-\alpha-1)(x+\alpha-1).$$

Ein Element α eines Körpers K heißt *n-te Einheitswurzel*, falls $\alpha^n = 1$ ist. Im Körper $\mathbb{C}$ der komplexen Zahlen formen die n-ten Einheitswurzeln die Gruppe μ_n (Beispiel 1.1.15.(b)).

Satz 4.4.7 *Sei K ein Körper und H eine endliche Untergruppe von K^* mit n Elementen. Die Gruppe H ist zyklisch und besteht genau aus den n-ten Einheitswurzeln in K.*

Beweis: Sei $H \subset K^*$ eine Untergruppe der Ordnung n. Die Ordnung eines Elements $\alpha \in H$ ist ein Teiler von n (Satz 1.5.7), also ist α eine Nullstelle des Polynoms $x^n - 1$. Satz 3.5.9 impliziert, dass $x^n - 1$ höchstens n Nullstellen in K besitzt, also besitzt dieses Polynom keine weiteren Nullstellen in K. Wir schließen, dass die Elemente von H genau die n-ten Einheitswurzeln in K sind.

Der Beweis, dass die Gruppe zyklisch ist, ist komplizierter. Sei $a \in H$ ein Element maximaler Ordnung m, und sei $H_m \subset H$ die Untergruppe, bestehend aus allen Elemente deren Ordnung ein Teiler von m ist. Die Elemente von H_m sind also genau die m-te Einheitswurzeln in K. Insbesondere besitzt H_m genau m Elemente. Da $a \in H_m$ ein Element der Ordnung m ist, schließen wir, dass $H_m = \langle a \rangle$ zyklisch ist.

Wir behaupten, dass $H = H_m$ ist. Falls nicht, existiert ein Element $b \in H \setminus H_m$ der Ordnung $\ell < m$. Da H abelsch ist, sieht man leicht ein, dass ab ein Element der Ordnung $\mathrm{kgV}(\ell, m)$ ist. Aus der Annahme $b \notin H_m$ folgt, dass $\ell \nmid m$, also, dass $\mathrm{kgV}(\ell, m) > m$ ist. Dies liefert einen Widerspruch zur Wahl von a. Wir schließen, dass $H = H_m$ ist. Insbesondere ist H zyklisch. □

Das folgende Korollar ist ein Spezialfall von Satz 4.4.7:

Korollar 4.4.8 *Sei F ein Körper mit $q = p^n$ Elementen. Die Gruppe F^* ist zyklisch.*

Bemerkung 4.4.9 Sei $F = \mathbb{F}_q$ ein Körper mit $q = p^n$ Elementen. Es existiert ein Element $\alpha \in F$ der Ordnung $q - 1$ (Korollar 4.4.8). Dies bedeutet, dass jedes Element in F^* eine Potenz von α ist: Es gilt $F^* = \{\alpha, \alpha^2, \ldots, \alpha^{q-1} = 1\}$.

Falls $q = p$ eine Primzahl ist, heißt ein Element α der Ordnung $p - 1$ eine *Primitivwurzel* modulo p. Korollar 4.4.8 sagt uns nicht, wie man eine Primitivwurzel effizient findet.

Beispiel 4.4.10 (a) Sei $\alpha \in \mathbb{F}_9$ ein Element mit $\alpha^2 = -1$ (siehe Beispiel 4.4.6). Es gilt $\mathrm{ord}(\alpha) = 4$. Ein Element der Ordnung 8 in $\mathbb{F}_9^*$ ist zum Beispiel $\beta := \alpha - 1$. Wir haben gesehen, dass β eine Nullstelle von $x^2 - x - 1$ ist.

(b) Sei $\alpha \in \mathbb{F}_4^*$ eine Nullstelle von $x^2 + x + 1$ (Beispiel 4.4.3). Die Ordnung von α ist 3 und α ist ein Erzeuger von $\mathbb{F}_4^*$.

Theorem 4.4.11 *Sei $q = p^n$ eine Primzahlpotenz und seien F, F' zwei Körper mit q Elementen. Die Körper F und F' sind isomorph.*

Beweis: Seien F, F' zwei Körper mit q Elementen und sei α ein Erzeuger der zyklischen Gruppe F^*. Der Körper $\mathbb{F}_p(\alpha)$ enthält auf jeden Fall die q Elemente $0, \alpha, \alpha^2, \ldots, \alpha^{q-1}$. Also gilt $F = \mathbb{F}_p(\alpha)$.

Sei $f(x) = \min_{\mathbb{F}_p}(\alpha)$, also $F \simeq \mathbb{F}_p[x]/(f)$. Da α auch eine Nullstelle des Polynoms $f_q(x) = x^q - x$ ist, folgt aus Satz 4.1.8, dass $f \mid f_q$.

Das Polynom $f_q(x)$ zerfällt auch in F' in Linearfaktoren (Theorem 4.4.5.(b)). Insbesondere besitzt f eine Nullstelle $\alpha' \in F'$. Es folgt, dass $F \simeq \mathbb{F}_p[x]/(f) \simeq \mathbb{F}_p(\alpha') \subset F'$. Da F und F' die gleiche Kardinalität haben, folgt $F' \simeq F$. □

Literatur

[1] M. Artin, *Algebra*. Birkäuser, 1993.

[2] M.A. Armstrong, *Groups and symmetry*. Undergraduate texts in mathematics. Springer-Verlag, 1988.

[3] S. Bosch, *Algebra*. Springer-Verlag, 2006.

[4] I.I. Bouw, *Elementare Zahlentheorie*, Vorlesungsskript, SS 2010.

[5] I.I. Bouw, *Algebra (Master)*, Vorlesungskript, WS 2013/2014.

[6] G. Fischer, *Lehrbuch der Algebra*. Vieweg, 2008.

[7] G. Fischer, *Lineare Algebra*, 15. Auflage. Vieweg, 2005.

[8] I. Stewart, *Galois theory*. Chapmann & Hall, 2004.