Algebra, Vorlesungsskript

Prof. Dr. Irene I. Bouw

Wintersemester 2008

Inhaltsverzeichnis

1 Gruppen

1.1 Die Definition einer Gruppe

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

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

welche die folgende Eigenschaften besitzt:

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

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

(G3) Jedes Element $a \in G$ besitzt ein *Inverses*, d.h. es existiert ein Element $a^{-1} \in G$ mit $a \cdot a^{-1} = a^{-1} \cdot a = e$.

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

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

(G0) Für alle $a, b \in G$ gilt, dass $a \cdot b \in G$.

ist daher implizit in Definition 1.1.1 enthalten.

(b) Im Allgemeinen werden wir für Gruppen die multiplikative Schreibweise $a \cdot b$ (oder ab) benutzen. Für abelsche Gruppen benutzen wir machmal auch die additive Schreibweise und schreiben $a + b$ statt $a \cdot b$. Ebenso schreiben wir dann $-a$ für das Inverse und 0 für das neutrale Element.

Beispiel 1.1.3 Wir geben nun einige sehr wichtige Beispiele von Gruppen. Überzeugen Sie sich davon, dass dies Gruppen sind und bestimmen Sie das neutrale Element und das Inverse eines Elements $a \in G$.

(a) Die Mengen $\mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}$ mit Addition sind kommutative 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 Menge unter Matrixmultiplikation. Die Abgeschlossenheit bezüglich der Multiplikation folgt aus der Regel $\det(AB) = \det(A)\det(B) \neq 0$ für alle $A, B \in \mathrm{GL}_n(K)$.

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

(e) Die Menge O_n der orthogonale $n \times n$ Matrizen ist eine Gruppe. die *orthogonale Gruppe*.

(f) Sei $n \in \mathbb{N}$ eine natürliche Zahl. Die Menge $\{0, 1, 2, \ldots, n-1\}$ ist eine abelsche Gruppe unter *Addition modulo n*:

$$x +_n y = \begin{cases} x + y & \text{falls } 0 \leq x + y < n, \\ x + y - n & \text{sonst.} \end{cases}$$

Für mehr Details siehe [4, § 3.1] und Beispiel 1.7.5.

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.

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

Beweis: Sei e' wie in (a) und sei e das neutrale Element von G. Wegen Gruppenaxiom (2) gilt, dass $e' = e' \cdot e$. Die Definition von e' impliziert, dass $e' \cdot e = e$. Also gilt, dass $e' = e$. Teil (b) folgt, indem man die Gleichung $b \cdot a = e$ mit a^{-1} multipliziert. Teil (c) ist ein Spezialfall von (a) und (b). Für (d) multipliziert man beide Seiten der Gleichung mit a^{-1}. □

Lemma 1.1.4.(d) benutzt Axiom (G3). Die Menge $M(2 \times 2, \mathbb{R})$ der reellen 2×2 Matrizen mit Matrizenmultiplikation als Verknüpfung ist keine Gruppe, da nicht jedes Element ein Inverses besitzt. Lemma 1.1.4.(d) gilt nicht:

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

1.2 Diedergruppen

Wichtige Beispiele von Gruppen sind *Symmetriegruppen*. Ein großer Vorteil von Symmetriegruppen ist, dass man sich diese Gruppen konkret vorstellen kann. Um die abstrakte Theorie zu verstehen, ist es wichtig, genügend konkrete Beispiele zu kennen, an denen man überprüfen kann, ob man die abstrakte Theorie auch verstanden hat.

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 $P_k := (\cos(2(k-1)\pi/n), \sin(2(k-1)\pi/n))$ sind. Abbildung 1 zeigt ein Bild von Δ_8.

Die *Diedergruppe* D_n ist die Symmetriegruppe von Δ_n, d.h. die Menge der Drehungen und Spiegelungen der Ebene $\mathbb{R}^2$, die Δ_n nach sich selbst abbilden. Die Verknüpfung ist die Hinteneinanderausführung von Funktionen. Die

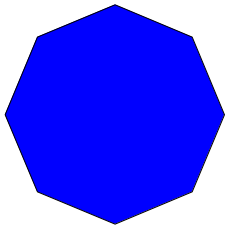


Abbildung 1: Das regelmäßiges 8-Eck

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 nun die Drehung um den Winkel $2k\pi/n$. Insbesondere ist $r^n = e$ die Drehung um 0 Grad, also das neutrale Element der Gruppe.

Betrachten wir nun die Spiegelsymmetrien von Δ_n. Falls n gerade ist, so gehen die Spiegelachsen entweder durch zwei gegenüberliegende Ecken oder durch die Mitte von zwei gegenüberliegende Kanten. Falls n ungerade ist, so gehen die Spiegelachsen durch eine Ecke und die Mitte der gegenüberliegenden Kante.

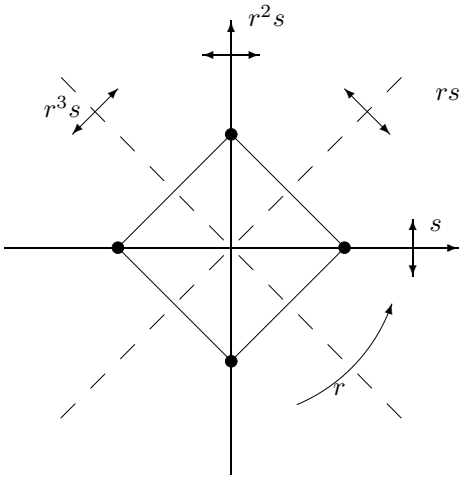


Abbildung 2: D_4 als Symmetriegruppe des regelmäßigen Vierecks

Sei s die Spiegelung an der x-Achse. Wegen unserer Wahl der Ecken ist dies eine Symmetrie von Δ_n für alle n. Da s eine Spiegelung ist, gilt $s^2 = e$. Mit Hilfe einer geometrischen Überlegung sieht man ein, dass $r^k s$ wieder eine Spiegelung ist. (Wie üblich bei Verknüpfungen von Funktionen, heißt $r^k s$ zuerst s, dann k-mal r anwenden.) Außerdem gilt die Relation $srs = r^{-1}$. Insbesondere ist D_n für $n \geq 3$ keine abelsche Gruppe. Alternativ kann man diese Relationen auch mit Hilfe der aus der Vorlesung *Lineare Algebra* bekannte Matrizen überprüfen:

Lemma 1.2.1 *(a) Die Diedergruppe D_n besteht aus $2n$ Elementen:*

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

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

(b) Es gilt

$$e := r^0, \quad r^n = e, \qquad s^2 = e, \qquad srs = r^{-1}.$$

1.3 Untergruppen

Definition 1.3.1 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, dass $a \cdot b \in H$,

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

Bemerkung 1.3.2 (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, dass $a \cdot b^{-1} \in H$.

Beispiel 1.3.3 (a) Sei T die Menge der invertierbaren, reellen, 2×2 oberen Dreiecksmatrizen:

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

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, dass

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

Außerdem ist die Einheitsmatrix ein Element von T.

(b) Sei $K := \{z \in \mathbb{C} \mid |z| = 1\}$ die Menge der komplexen Zahlen mit Betrag 1, also der Einheitskreis. Dies ist eine Untergruppe von $\mathbb{C}^*$.

(c) Sie K ein Körper. Die Gruppe $\mathrm{SL}_n(K)$ der invertierbaren Matrizen mit Determinante 1 ist eine Untergruppe von $\mathrm{GL}_2(K)$. Ebenso ist $\mathrm{SO}_n = \{A \in \mathrm{O}_n \mid \det(A) = 1\}$ eine Untergruppe von O_n.

(d) Sei $G = D_n$ die Diedergruppe und $H = \{e = r^0, r, r^2, \cdots, r^{n-1}\}$. Da $r^k \cdot r^\ell = r^{k+\ell}$, gilt, dass H eine Untergruppe von G ist.

Satz 1.3.4 *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 1.3.5 Die Untergruppe $H = \langle S \rangle \subset G$ heißt die *von S erzeugte Untergruppe*. Im Fall $G = \langle S \rangle$ heißt die Teilmenge S ein *Erzeugendensystem* von G.

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 1.3.2.(b) folgt, dass H eine Untergruppe von G ist, die S als Teilmenge enthält.

Ist nun $H' \subset G$ 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. □

Beispiel 1.3.6 (a) Die Diedergruppe D_n wird erzeugt von r und s.

(b) Sei K ein Körper und $G = \mathrm{GL}_n(K)$. Aus der lineare Algebra ist bekannt, dass die Menge S der Elementarmatrizen ein erzeugendes System von G bildet.

Definition 1.3.7 Eine *zyklische Gruppe* ist eine Gruppe, die von einem Element erzeugt wird. Ein solches Element heißt *Erzeuger* der Gruppe.

Bemerkung 1.3.8 Jede zyklische Gruppe ist auch abelsch, da $g^i g^j = g^{i+j} = g^j g^i$.

Definition 1.3.9 Sei G eine Gruppe mit endlich vielen Elementen. Die *Ordnung* $|G|$ der Gruppe ist die Anzahl der Elemente von G. Falls $g \in G$ ein Element ist, so heißt die Ordnung der Untergruppe $\langle g \rangle$ erzeugt von g die *Ordnung* von g.

Beispiel 1.3.10 (a) Die Gruppe $(\mathbb{Z}, +)$ ist eine zyklische Gruppe. Erzeugende Elemente sind 1 oder -1.

(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 $z := e^{2\pi i k/n}$ ist $n/\operatorname{ggT}(k, n)$. Dies ist die kleinste positive Zahl d, sodass $z^d = 1$.

Als weiteres Beispiel bestimmen wir alle Untergruppen von $(\mathbb{Z}, +)$. (Dieser Beweis ist sehr ähnlich am Beweis von [4, Lemma 2.1.9].)

Theorem 1.3.11 *Für $b \in \mathbb{Z}$ definieren wir*

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

(a) Für jedes $b \in \mathbb{Z}$ ist $b\mathbb{Z}$ eine Untergruppe von $\mathbb{Z}$.

(b) Jede Untergruppe H von $\mathbb{Z}$ ist von der Form $H = b\mathbb{Z}$, für ein $b \in \mathbb{Z}$.

Beweis: Teil (a) ist ein Spezialfall von Satz 1.3.4.
Sei $H \subset (\mathbb{Z}, +)$ eine Untergruppe. Es gilt $0 \in H$ (Axiom (U1)). Falls 0 das einzige Element von H ist, so gilt $H = 0\mathbb{Z} = \{0\}$.

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

Wir behaupten, dass $H = b\mathbb{Z}$, also, dass jedes Element von H ein Vielfaches von b ist. Nehmen wir an, dass es ein $a \in H$ gibt mit $b \nmid a$. Division mit Rest (siehe [4, Satz 2.1.5]) impliziert, dass Zahlen q, r existieren mit $a = qb + r$ und $0 \leq r < b$. Da $b \in H$ ist, so ist auch $k \cdot b = b + \cdots + b \in H$ für alle $k \in \mathbb{N}$. Ebenso ist $-kb = -(kb) \in H$. Also gilt, dass $qb \in H$ ist. Axiom (U2+3) impliziert nun, dass $r = a - qb \in H$ ist. Die Minimalität von b zusammen mit der Eigenschaft $0 \leq r < b$ impliziert nun, dass $r = 0$. Also ist $a = qb \in b\mathbb{Z}$. □

Theorem 1.3.11 sagt also, dass jede Untergruppe von $\mathbb{Z}$ zyklisch ist. Dies impliziert folgende überraschende Tatsache. Seien $a, b \in \mathbb{Z}$ zwei Elementen 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 $a\mathbb{Z} + b\mathbb{Z} = d\mathbb{Z}$. Sogar kann man annehmen, dass $d > 0$ ist. Diese Zahl d heißt der *größte gemeinsame Teiler* von a und b. Bezeichnung: $d = \operatorname{ggT}(a, b)$. Er hat die folgende Eigenschaften (siehe auch [4, § 2.1]):

Korollar 1.3.12 *Seien $a, b \in \mathbb{Z}$ und sei $d = \operatorname{ggT}(a, b)$.*

- *Es existieren $x, y \in \mathbb{Z}$ mit $d = ax + by$.*
- *d teilt sowohl a als auch b.*
- *Jeder gemeinsamer Teiler von a und b teilt auch d.*

Beispiel 1.3.13 Sei $a = 60$ und $b = 36$. Es gilt, dass $d = \mathrm{ggT}(a, b) = 12$. Theorem 1.3.11 impliziert, dass $x, y \in \mathbb{Z}$ existieren mit $12 = 60x + 36y$. Tatsächlich gilt, dass $12 = 36 \cdot 2 - 60 \cdot 1$. Für große Zahlen a und b ist es nicht einfach, die Zahlen d, x und y zu bestimmen. Ein Algorithmus, der diese Zahlen berechnet, ist der erweiterte euklidische Algorithmus (siehe [4, § 2.1]).

1.4 Permutationen

Sei X eine Menge. Sei $S(X)$ die Menge der bijektiven Abbildungen von X auf sich selbst. Wir behaupten, dass $S(X)$ mit der Komposition von Abbildungen als Verknüpfung eine Gruppe ist. Für $f, g \in S(X)$ schreiben wir die Verknüpfung als

$$g \circ f : X \to X, \qquad x \mapsto g(f(x)).$$

Falls $f, g \in S(X)$, so ist auch $g \circ f : X \to X$ eine Bijektion, also ist $S(X)$ abgeschlossen. Außerdem ist $\circ$ assoziativ. Die Identität

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

ist das neutrale Element. Da $f \in S(X)$ eine Bijektion ist, so existiert das Inverse f^{-1} von f, charakterisiert von der Eigenschaft

$$f(x) = y \quad \text{genau dann, wenn} \quad f^{-1}(y) = x.$$

Wir schließen, dass $S(X)$ eine Gruppe ist.

Die Elemente von $S(X)$ heißen *Permutationen* der Menge X. Falls $X = \{1, 2, \ldots, n\}$ ist, so heißt $S(X)$ die *symmetrische Gruppe* auf n Elemente. Wir schreiben für diese Gruppe S_n statt $S(X)$.

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 sind die Elementen $1, 2 \ldots, n$ der Menge X. Die untere Zeile sind die Bilder $\sigma(1), \sigma(2), \ldots \sigma(n)$. Zum Bespiel 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. Allgemeiner ist eine Permutation $\sigma \in S_n$ 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 1.4.1 *Die Gruppe S_n besitzt genau $n!$ Elementen.*

Bemerkung 1.4.2 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 dem Buch von Armstrong [2]. Andere Bücher, zum Beispiel Artin [1], machen 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 dargestellt in der folgenden *Verknüpfungstabelle*:

$\sigma \cdot \tau$	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: Die *Zyklenschreibweise*.

Als Beispiel nehmen wir die Permutation

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

Für $k = 1, 2, \ldots, 7$ betrachten wir die Folge

$$F(\sigma) := (k, \sigma(k), \sigma^2(k), \ldots).$$

Die Folge

$$F(1) = (1, \sigma(1), \sigma^2(1), \ldots) = (1, 7, 6, 1, 7, 6, 1, \ldots)$$

ist periodisch (mit Periodenlänge 3). Die Folgen

$$F(7) = (7, 6, 1, 7, 6, 1, \ldots), \qquad F(6) = (6, 1, 7, 6, 1, 7, \ldots)$$

haben dann dieselbe Eigenschaft und lassen sich aus $F(1)$ durch 'Verschieben' leicht ableiten. Offenbar wird die Teilmenge $\{1, 6, 7\}$ von σ in sich abgebildet; die Einschränkung von σ auf $\{1, 6, 7\}$ ist ein sogenannter 3-*Zyklus*, den wir folgendermaßen schreiben:

$$\sigma|_{\{1,6,7\}} = (1\ 7\ 6).$$

Man beachte, dass diese Schreibweise nicht eindeutig ist: es gilt

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

Durch Betrachten der Folgen $F(2)$ und $F(4)$ erhält man noch zwei weitere Zyklen, der Länge 3 und 1:

$$\sigma|_{\{2,3,5\}} = (2\ 5\ 3), \qquad \sigma|_{\{4\}} = (4).$$

Die *Zyklenschreibweise* der Permutation σ ist nun:

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

Es ist klar, dass σ hierdurch eindeutig bestimmt ist. Häufig lässt man in dieser Darstellung die 1-Zyklen weg und schreibt

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

Die zwei 3-Zyklen aus σ sind disjunkt, dies bedeutet, dass sie auf disjunkte Mengen von Indizes wirken. Daher kommutieren die beide Zyklen. Die Darstellung

$$(3\ 2\ 5)(6\ 1\ 7)$$

definiert die gleiche Permutation σ. Eine 2-Zyklus nennt man auch *Transposition.*

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

Lemma 1.4.3 *(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. So ist die Ordnung von σ gleich $\mathrm{kgV}(k_i)$.

Beispiel 1.4.4 Die symmetrische Gruppe S_3 enthält neben der Identität noch 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,

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

Theorem 1.4.5 *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

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

□

Beispiel 1.4.6 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 $(a\ b) = (1\ a)(1\ b)(1\ a)$. Aber die Anzahl der benötigte Permutationen ist immer entweder gerade oder ungerade. Dies überprüfen wir wie folgt. Wir betrachten das Polynom

$$P(x_1, x_2, \ldots, x_n) = \prod_{1 \le i < j \le n} (x_i - x_j)$$

in n Variablen. Für $\sigma \in S_n$ definieren wir

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

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

Definition 1.4.7 Sei $\sigma \in S_n$. Das *Signum* $\operatorname{sgn}(\sigma) \in \{\pm 1\}$ ist definiert durch die Gleichung $P(\sigma) = \operatorname{sgn}(\sigma)P$. Falls $\operatorname{sgn}(\sigma) = 1$, so heißt σ *gerade* , sonst *ungerade*.

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

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

also ist σ eine gerade Permutation.

Lemma 1.4.8 *(a) Für $\sigma, \tau \in S_n$ gilt* $\operatorname{sgn}(\sigma\tau) = \operatorname{sgn}(\sigma)\operatorname{sgn}(\tau)$.

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

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

Beweis: Teil (a) folgt direkt aus der Definition. Falls τ eine Transposition ist, so gilt offensichtlich $\operatorname{sgn}(\tau) = -1$. Teil (b) folgt daher direkt aus (a). Teil (c) folgt aus (a), (b) und Theorem 1.4.5. □

1.5 Gruppenhomomorphismen

Definition 1.5.1 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 1.5.2 (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

$$\varphi : \mathbb{R} \to \mathrm{O}_2, \qquad t \mapsto \begin{pmatrix} \cos(t) & -\sin(t) \\ \sin(t) & \cos(t) \end{pmatrix}$$

die einer reellen Zahl t die Drehmatrix um den Winkel t zuordnet, ist ein Gruppenhomomorphismus. Es gilt nämlich, dass

$$\varphi(t+s) = \begin{pmatrix} \cos(t+s) & -\sin(t+s) \\ \sin(t+s) & \cos(t+s) \end{pmatrix} = \varphi(t) \cdot \varphi(s).$$

(c) Sei $H \subset G$ eine Untergruppe. Die Inklusion $\iota : H \hookrightarrow G$ ist ein Gruppenhomomorphismus.

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

Die folgende Eigenschaften folgen unmittelbar aus der Definition.

Lemma 1.5.3 *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 heißt φ ein Gruppenisomorphismus *und die Gruppen G und H heißen* isomorph *(Bezeichnung: $G \simeq H$).*

Beweis: Teil (a) folgt aus $e_G = e_G \cdot e_G$. Teil (b) folgt aus $a \cdot_G a^{-1} = e_G$.
Wir beweisen (c). Sei 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 $\varphi(a \cdot_G b) = \varphi(a)\varphi(b) = x \cdot_H y$. Also gilt, dass

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

□

Beispiel 1.5.4 (a) Wir definieren einen Gruppenisomorphismus zwischen der Diedergruppe D_3 und der symmetrischen Gruppe S_3. Beide Gruppen haben 6 Elemente. Die Diedergruppe ist die Symmetriegruppe des gleichseitigen Dreiecks. Wie in § 1.2 nehmen wir als Ecken des Dreiecks

$$P_k \;=\; (\cos(2(k-1)\pi/3), \sin(2(k-1)\pi/3)), \qquad k = 1, 2, 3.$$

Wir definieren nun einen Gruppenhomomorphismus

$$\varphi : D_3 \to S_3, \qquad f \mapsto \sigma(f),$$

wobei $\sigma(f)$ die von f definierte Permutation der Ecken ist. Zum Beispiel sei $r \in D_3$ die Drehung um den Winkel $2\pi/3$, so ist die Permutation

$\sigma(r) = (1\ 2\ 3)$. Die Spiegelung s an der Gerade durch P_1 und die Mitte der Kante P_2P_3 definiert die Permutation $\sigma(s) = (2\ 3)$. Man überprüft, dass keine zwei Drehungen die gleiche Permutation der Ecken definieren. Dies zeigt, dass φ eine Bijektion ist.

(b) Seien $G = \langle g \rangle$ und $H = \langle h \rangle$ zwei zyklische Gruppen der Ordnung n. Wir definieren eine Abbildung

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

Dies ist offensichtlich ein Gruppenisomorphismus. Also sind G und H isomorph.

Definition 1.5.5 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.

Beispiel 1.5.6 Wir berechnen der Kern und das Bild der Gruppenhomomorphismen aus Beispiel 1.5.2:

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

(b) $\ker(\varphi) = 2\pi\mathbb{Z} = \{2\pi k \mid k \in \mathbb{Z}\}$, $\mathrm{im}(\varphi) = \mathrm{SO}_2$.

(c) $\ker(\iota) = \{e_H\}$ und $\mathrm{im}(\iota) = H$.

(d) $\ker(\psi_n) = \mu_n$, die Gruppe der n-ten Einheitswurzeln und $\mathrm{im}(\psi_n) = \mathbb{C}^*$.

Definition 1.5.7 Sei G eine Gruppe. Eine Untergruppe N von G heißt *Normalteiler*, falls

$$ghg^{-1} \in H \qquad \text{für alle } h \in N \text{ und } g \in G. \tag{2}$$

Das folgende Lemma folgt direkt aus Definition 1.5.7.

Lemma 1.5.8 *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 (2) trivial. □

Lemma 1.5.9 *Sei $\varphi : G \to H$ ein Gruppenhomomorphismus.*

(a) Der Kern von φ ist ein Normalteiler von G.

(b) Das Bild von φ ist eine Untergruppe von H.

Beweis: Man überprüft leicht, dass $\ker(\varphi)$ und $\mathrm{im}(\varphi)$ Untergruppen sind. 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 $ghg^{-1} \in \ker(\varphi)$. □

Lemma 1.4.8 impliziert, dass das Signum $\mathrm{sgn} : S_n \to \{\pm 1\}$ ein Gruppenhomomorphismus ist. Der Kern $A_n := \ker(\mathrm{sgn})$ ist also ein Normalteiler der symmetrischen Gruppe. Diese Gruppe A_n besteht aus den geraden Permutation und heißt die *alternierende Gruppe*.

Die Elemente der alternierenden Gruppe A_4 sind

$$\begin{array}{llll} e, & (1\,2)(3\,4), & (1\,3)(2\,4), & (1\,4)(2\,3), \\ (1\,2\,3), & (1\,2\,4), & (1\,3\,4), & (2\,3\,4), \\ (1\,3\,2), & (1\,4\,2), & (1\,4\,3), & (2\,4\,3). \end{array}$$

In Beispiel 2.1.6.(b) werden wir zeigen, dass A_4 die Symmetriegruppe des Tetraeders ist.

Insbesondere hat A_4 genau 12 Elemente, genau so viele wie die Diedergruppe D_6. Diese Gruppen sind aber nicht isomorph. Dies folgt aus folgendem Lemma, da D_6 ein Element der Ordnung 6 besitzt, A_4 aber nicht.

Lemma 1.5.10 *Sei $\varphi : G \to G'$ ein Gruppenisomorphismus. Die Elemente $g \in G$ und $\varphi(g) \in G'$ haben die gleiche Ordnung.*

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

Die folgende Aussage ist eine Folgerung von Theorem 1.3.11.

Korollar 1.5.11 *Sei G eine zyklische Gruppe. Jede Untergruppe von G ist auch zyklisch.*

Beweis: Sei g ein Erzeuger von G. Wir definieren einen Gruppenhomomorphismus

$$\varphi : \mathbb{Z} \to G, \qquad i \mapsto g^i.$$

Sei $H \subset G$ eine Untergruppe und $K = \{i \in \mathbb{Z} \mid \varphi(i) \in H\}$. Da G zyklisch ist, so ist jedes Element von G eine Potenz von g. Also ist $\varphi : K \to H$ surjektiv.

Es ist leicht einzusehen, dass K eine Untergruppe von $\mathbb{Z}$ ist. Theorem 1.3.11 impliziert, dass K zyklisch ist. Sei $d \in \mathbb{Z}$ ein Erzeuger von K. Da $\varphi : K \to H$ surjektiv ist, so ist $\varphi(d)$ ein Erzeuger von $H = \mathrm{im}(\varphi)$. □

1.6 Nebenklassen

Eine Äquivalenzrelation $\sim$ auf einer Menge S ist eine Relation zwischen bestimmten Elementen von S. Wir schreiben die Relation als $a \sim b$ und sagen, dass a und b äquivalent sind.

Definition 1.6.1 Eine Äquivalenzrelation auf einer Menge S ist eine Relation, die folgende Eigenschaften erfüllt:
Reflexivität $a \sim a$ für alle $a \in S$,
Symmetrie Falls $a \sim b$, so auch $b \sim a$,
Transitivität Falls $a \sim b$ und $b \sim c$, so auch $a \sim c$.
Die Menge $S_a = \{b \in S \mid b \sim a\}$ heißt die *Äquivalenzklasse* von a.

Beispiel 1.6.2 (a) Sei $m > 1$ eine natürliche Zahl und $a, b \in \mathbb{Z}$. 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. Man überprüft, dass dies eine Äquivalenzrelation definiert. Die Äquivalenzklasse von a ist die Menge $a + m\mathbb{Z} = \{a + mk \mid k \in \mathbb{Z}\}$.

(b) Sei $S = \mathbb{C}^* = \mathbb{C} \setminus \{0\}$. Für $z, w \in \mathbb{C}^*$ definieren wir $z \sim w$ falls $|z| = |w|$. Dies definiert eine Äquivalenzrelation. Die Äquivalenzklassen sind Kreise $C_r = \{z \in \mathbb{C}^* \mid |z| = r\}$ mit Radius $r \in \mathbb{R}_{>0}$.

Lemma 1.6.3 *Sei $\sim$ eine Äquivalenzrelation auf S. Zwei Äquivalenzklassen sind entweder gleich oder disjunkt.*

Beweis: Seien C_a und C_b zwei Äquivalenzklassen. Da $a \in C_a$ und $b \in C_b$, sind die Äquivalenzklassen nichtleer.

Wir zeigen zuerst, dass, falls $b \sim a$, so auch $C_a = C_b$ gilt. Für jedes Element $c \in C_b$ gilt $c \sim b$. Aus der Transitivität folgt daher, dass $c \in C_a$. Also ist $C_b \subset C_a$. Das gleiche Argument zeigt auch, dass $C_a \subset C_b$. Also gilt $C_a = C_b$.

Wir nehmen nun an, dass $C_a \cap C_b$ nicht leer ist. Sei $d \in C_a \cap C_b$ ein Element aus der Schnittmenge. Also gilt $d \sim a$ und $d \sim b$. Das obige Argument zeigt, dass $C_a = C_d = C_b$. □

Seien G und G' Gruppen und sei $\varphi : G \to G'$ ein Gruppenhomomorphismus. Für Elemente $a, b \in G$, definieren wir $a \equiv b$ und sagen a ist *kongruent zu b*, falls $\varphi(a) = \varphi(b)$. Dies definiert eine Äquivalenzrelation. Die Äquivalenzklassen sind die Urbilder $\varphi^{-1}(h)$, für $h \in G'$. Beispiel 1.6.2 ist ein Spezialfall dieser Konstruktion; Der zugehörige Gruppenhomomorphismus ist

$$\mathbb{C}^* \to \mathbb{R}^*, \quad z \mapsto |z|.$$

Der nächste Satz beschreibt die Äquivalenzklassen etwas genauer.

Satz 1.6.4 *Sei $\varphi : G \to H$ ein Gruppenhomomorphismus und sei $N = \ker(\varphi)$. Es gilt, dass $\varphi(a) = \varphi(b)$ für $a, b \in G$ genau dann, wenn $b = an$ für ein $n \in N$. (Äquivalent: $a^{-1}b \in N$.)*

Beweis: Wir nehmen an, dass $\varphi(a) = \varphi(b)$. Da φ ein Gruppenhomomorphismus ist, gilt $e_H = \varphi(a)^{-1}\varphi(b) = \varphi(a^{-1}b)$. Also ist $a^{-1}b \in N$. Die andere Richtung beweist man analog. □

Ein wichtiger Spezialfall ist, wenn der Kern N eines Gruppenhomomorphismus $\varphi : G \to H$ trivial ist. Folgendes Korollar ist eine direkte Folgerung aus Satz 1.6.4.

Korollar 1.6.5 *Ein Gruppenhomomorphismus $\varphi : G \to H$ ist injektiv genau dann, wenn $\ker(\varphi) = \{e_G\}$ trivial ist.*

Für die Definition der Nebenklassen ist es nicht notwendig, dass N ein Normalteiler ist.

Definition 1.6.6 Sei $H \subset G$ eine Untergruppe. Eine Menge von der Form $aH = \{ah \mid h \in H\}$ heißt *Linksnebenklasse* von H in G. Ebenso heißt $Ha = \{ha \mid h \in H\}$ *Rechtsnebenklasse*. Die Anzahl der Linksnebenklassen von H in G heißt der *Index* von H in G und wird mit $[G : H]$ bezeichnet.

Sei H eine Untergruppe von G. Die Relation $a \equiv b$, falls $a^{-1}b \in H$ definiert eine Äquivalenzrelation. Im Spezialfall, dass $H = \ker(\varphi)$ der Kern eines Homomorphismus ist, haben wir dies in Satz 1.6.4 gesehen. Die Äquivalenklassen sind die Linksnebenklassen. Lemma 1.6.3 impliziert, dass G die disjunkte Vereinigung von Linksnebenklassen ist. Anders gesagt, falls zwei Linksnebenklassen aH und bH ein gemeinsames Element besitzen, so sind sie gleich.

Beispiel 1.6.7 (a) Eine Untergruppe H von G ist selber eine Linksnebenklasse, da $H = e \cdot H$.

(b) 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 $[G : H] = n$.

Die Rechstnebenklassen sind nicht notwendigerweise auch Linksnebenklassen. Zum Beispiel ist $Hr = \{r, sr = r^{n-1}s\}$ keine Linksnebenklasse, falls $n \geq 3$. In § 1.7 untersuchen wir dies genauer.

Satz 1.6.8 *Sei G eine Gruppe mit endlich vielen Elementen.*

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

(b) Es gilt

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

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

Beispiel 1.6.9 Wir betrachten die Untergruppe $A_n \subset S_n$. Da A_n der Kern von $\operatorname{sgn} : S_n \to \{\pm 1\}$ ist, so ist A_n ein Normalteiler. Satz 1.6.4 impliziert, dass es zwei Nebenklassen gibt: Die geraden Permutationen $A_n = 1 \cdot A_n$ und die ungeraden Permutationen $(1\ 2)A_n$. Satz 1.6.8 impliziert, dass $|A_n| = |S_n|/[S_n : A_n] = n!/2$ ist.

Diese einfache Bemerkung hat viele wichtige Folgerungen.

Satz 1.6.10 (Lagrange) *Sei G eine endliche Gruppe und H eine Untergruppe. Die Ordnung von H teilt die Ordnung von G.*

Insbesondere gilt Satz 1.6.10 für die Untergruppe erzeugt von einem Element $a \in G$. Wir schließen, dass die Ordnung eines Elements ein Teiler der Gruppenordnung ist.

Beispiel 1.6.11 Sei $m > 1$ eine natürliche Zahl. Wir definieren

$$(\mathbb{Z}/m\mathbb{Z})^* = \{0 < a < m \mid \operatorname{ggT}(a, m) = 1\}.$$

Wir behaupten, dass $((\mathbb{Z}/m\mathbb{Z})^*, \cdot)$ eine Gruppe ist. Die Abgeschlossenheit, Assoziativität und die Existenz des neutralen Elementes sind klar. Korollar 1.3.12 impliziert, dass für jedes $a \in \mathbb{Z}/m\mathbb{Z}^*$ Zahlen $x, y \in \mathbb{Z}$ existieren, sodass $1 = xa + ym$. Offensichtlich ist $\operatorname{ggT}(x, m) = 1$. Also ist $xa \equiv 1 \pmod m$. Daher besitzt $a \in (\mathbb{Z}/m\mathbb{Z})^*$ ein Inverses. Sei $\varphi(m)$ die Kardinalität der Gruppe $(\mathbb{Z}/m\mathbb{Z})^*$. Die Funktion φ heißt *eulersche phi-Funktion*.

Satz 1.6.10 impliziert, dass die Ordnung von $a \in (\mathbb{Z}/m\mathbb{Z})^*$ ein Teiler von $\varphi(m)$ ist. Insbesondere gilt, dass $a^{\varphi(m)} \equiv \pmod m$ für alle $a \in (\mathbb{Z}/m\mathbb{Z})^*$. Dieses Ergebnis ist in der Zahlentheorie bekannt als der Satz von Euler ([4, Satz 3.5.7]).

Korollar 1.6.12 *Sei p eine Primzahl und G eine Gruppe der Ordnung p, so ist G zyklisch.*

Beweis: Sei $a \in G$ ein Element ungleich das neutrale Element. Die Ordnung der Untergruppe $H = \langle a \rangle$ teilt $|G| = p$, ist aber nicht 1, da H nicht die triviale Gruppe ist. Also ist $|H| = |G| = p$ und $G = H = \langle a \rangle$. □

Korollar 1.6.13 *Sei G eine Gruppe der Ordnung 4, so ist G isomorph zu $\mathbb{Z}/4\mathbb{Z}$ oder $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} = \{(a, b) \mid a, b \in \mathbb{Z}/2\mathbb{Z}\}$. Die Gruppe $V := \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ heißt* kleinsche Vierergruppe.

Beweis: Sei G eine Gruppe der Ordnung 4 und sei $g \in G \setminus \{e\}$. Satz 1.6.10 impliziert, dass die Ordnung ein Teiler von 4 ist, also gilt $\mathrm{ord}(g) \in \{2, 4\}$. Falls G ein Element der Ordnung 4 besizt, so ist G zyklisch. Sonnst haben alle Elementen $g \in G \setminus \{e\}$ Ordnung 2.

Wir nehmen an, dass G nicht zyklisch ist und schreiben $G = \{e, a, b, c\}$. Die Elementen a, b, c haben Ordnung 2. Da $a^2 = b^2 = e$, so 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. Wir vergleichen die Verknüpfungstabelle von G mit der Verknüpfungstabelle von V.

G	e	a	b	c
e	e	a	b	c
a	a	e	c	b
b	b	c	e	a
c	c	b	a	e

V	$(0,0)$	$(1,0)$	$(0,1)$	$(1,1)$
$(0,0)$	$(0,0)$	$(1,0)$	$(0,1)$	$(1,1)$
$(1,0)$	$(1,0)$	$(0,0)$	$(1,1)$	$(0,1)$
$(0,1)$	$(0,1)$	$(1,1)$	$(0,0)$	$(1,0)$
$(1,1)$	$(1,1)$	$(0,1)$	$(1,0)$	$(0,0)$

Aus die Verknüpfungstabelle folgt direkt, dass $G \simeq V$ ist. □

Korollar 1.6.14 *Sei $\varphi : G \to G'$ ein Homomorphismus endlicher Gruppen. Es gilt, dass*

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

Beweis: Die Diskussion vor Satz 1.6.4 zeigt, dass $\mathrm{im}(\varphi)$ die Menge der Linksnebenklassen von $\ker(\varphi)$ in G ist, also gilt $|\mathrm{im}(\varphi)| = [G : \ker(\varphi)]$. Das Korollar folgt aus aus Satz 1.6.8. □

1.7 Faktorgruppen

In Beispiel 1.6.7.(c) haben wir gesehen, dass die Linksnebenklassen nicht immer auch Rechtsnebenklassen sind (und umgekehrt). Folgender Satz zeigt, dass dies der Fall ist genau dann, wenn die Untergruppe H ein Normalteiler ist.

Satz 1.7.1 *Eine Untergruppe H von G ist genau dann ein Normalteiler, wenn jede Linksnebenklasse auch ein Rechtsnebenklasse ist.*

Beweis: Wir nehmen zuerst an, dass $H \subset G$ 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 1.6.3 impliziert daher, dass Ha keine Linksnebenklasse ist. □

Falls A und B Teilmengen einer Gruppe G sind, so schreiben wir

$$AB = \{ab \mid a \in A, b \in B\} \subset G.$$

Lemma 1.7.2 *Sei $N \subset G$ ein Normalteiler einer Gruppe G. Das Produkt zweier Linksnebenklassen aN, bN ist wieder eine Linksnebenklasse. Es gilt*

$$(aN) \cdot (bN) = abN.$$

Beweis: Da N ein Normalteiler ist, gilt $aN = Na$ für alle $a \in G$ (Satz 1.7.1). Also gilt, dass

$$(aN)(bN) = a(Nb)N = a(bN)N = abN.$$

□

Wir schreiben G/N für die Menge der Nebenklassen von N in G. (Da die Linksnebenklassen und Rechtsnebenklassen gleich sind, reden wir hier von Nebenklassen.) Lemma 1.7.2 definiert eine Verknüpfung auf G/N. Folgendes Theorem sagt, dass die Menge der Nebenklassen mit dieser Verknüpfung tatsächlich eine Gruppe ist.

Theorem 1.7.3 *Sei $\bar{G} = G/N$ mit der Verknüpfung definiert in Lemma 1.7.2.*

(a) Die Menge $\bar{G}$ ist eine Gruppe. Diese Gruppe heißt die Faktorgruppe von G nach N.

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

Beweis: Die Assoziativität der Verknüpfung auf $\bar{G}$ folgt aus der Assoziativität der Verknüpfung auf G. Das neutrale Element ist $eN = N$. Das Inverse von aN ist $a^{-1}N$.

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

Folgendes Korollar folgt direkt aus Theorem 1.7.3.(b).

Korollar 1.7.4 *Jeder Normalteiler N von G ist der Kern eines Gruppenhomomorphismus.*

Beispiel 1.7.5 (a) Sei $G = \mathbb{Z}$ und $m \in \mathbb{N}$ eine natürliche Zahl. Die Untergruppe $m\mathbb{Z}$ von $\mathbb{Z}$ ist ein Normalteiler. Die Faktorgruppe bezeichnen wir mit $\mathbb{Z}/m\mathbb{Z}$. Da $\mathbb{Z}$ eine abelsche Gruppe ist, schreiben wir die Nebenklassen additiv als $a + m\mathbb{Z}$. Wir sehen, dass die Nebenklassen genau die Kongruenzklassen modulo m sind.

(b) Falls $H \subset G$ eine Untergruppe, aber kein Normalteiler ist, so ist die Menge G/H der Linksnebenklassen keine Gruppe. (Siehe den Beweis von Satz 1.7.1.) Wir überprüfen dies nochmal in einem konkreten Fall. In Beispiel 1.6.7.(b) haben wir gesehen, dass $H := \langle s \rangle \subset D_n$ für $n \geq 3$ kein Normalteiler ist. Die Linkenebenklassen sind $r^i H = \{r^i, r^i s\}$. Wir berechnen, dass

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

Die Elemente $\{r^2, r^2 s, s, rs\}$ formen keine Linksnebenklasse, sondern eine Vereinigung von Linksnebenklassen. Also ist die Multiplikation $(rH)(rH)$ nicht eindeutig definiert.

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

Satz 1.7.6 (Erster Isomorphiesatz) *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: Zuerst überprüfen wir, dass die Abbilding $\bar{\varphi}$ wohldefiniert ist. Seien $a, b \in G$ mit $aN = bN$. Es gilt $x := a^{-1}b \in N = \ker(\varphi)$. Also gilt $\varphi(b) = \varphi(ax) = \varphi(a)\varphi(x) = \varphi(a)$.

Satz 1.6.4 sagt, dass die Fasern $\varphi^{-1}(z)$ von φ genau die Nebenklassen sind, da φ surjektiv ist. Also ist $\bar{\varphi}$ eine Bijektion. Wir überprüfen, dass $\bar{\varphi}$ ein Gruppenhomomorphismus ist:

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

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

Beispiel 1.7.7 (a) Die Betragsfunktion $\mathbb{C}^* \to \mathbb{R}^*, z \mapsto |z|$ ist ein Gruppenhomomorphismus mit Kern $K := \{z \in \mathbb{C}^* \mid |z| = 1\}$ und Bild $\mathbb{R}_{>0} = \{r \in \mathbb{R} \mid r > 0\}$. Also ist die Betragsfunktion von $\mathbb{C}^* \to \mathbb{R}_{>0}$ surjektiv. Wir schließen, dass $\mathbb{C}^*/K \simeq \mathbb{R}_{>0}$.

(b) Aus Beispiel 1.5.6.(a) schließen wir, dass $K^* \simeq \mathrm{GL}_n(K)/\mathrm{SL}_2(K)$.

(c) Aus den Beispielen 1.5.2.(b) und 1.5.6.(b) schließen wir, dass $\mathrm{SO}_2 \simeq \mathbb{R}/2\pi\mathbb{Z}$ ist.

2 Gruppenwirkungen

2.1 Definitionen

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

Bemerkung 2.1.2 Sei τ eine Gruppenwirkung. Die Abbildung $\tau : G \to S(X)$ definiert eine Abbildung

$$\tau : G \times X \to X, \quad (g, x) \mapsto \tau_g(x)$$

mit $\tau_{g \cdot g'}(x) = \tau_g(\tau_{g'}(x))$ und $\tau_e(x) = x$ für alle $g, g' \in G$ und $x \in X$. Umgekehrt definiert jede Albbildung $\tau : G \times X \to X$ wie oben eine Gruppenwirkung. Dies liefert eine äquivalente Beschreibung von Gruppenwirkungen.

Machmal schreibt man auch $g \cdot x$ statt $\tau_g(x)$.

Beispiel 2.1.3 (a) Die Gruppe $\mathbb{Z}$ wirkt auf der reellen Gerade $\mathbb{R}$ als Translation. Wir definieren $\tau_m(x) = m + x$ für $m \in \mathbb{Z}$ und $x \in \mathbb{R}$. Dies definiert eine Gruppenwirkung, da $(m+n)+x = m+(n+x)$ 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 2.1.4 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 2.1.5 *(a) Sei $\tau : G \times X \to X$ eine Gruppenwirkung. Die Menge X ist eine disjunkte Vereinigung von Bahnen.*

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

Beweis: Für $x, y \in X$ definieren wir $x \sim_G y$, falls $y \in G(x)$ ist. Dies definiert eine Äquivalenzrelation. Daher folgt (a) aus Lemma 1.6.3. Teil (b) folgt aus der Definition. □

Beispiel 2.1.6 (a) Die Gruppe D_n wirkt transitiv auf der Menge X der Ecken des regelmäßiges n-Ecks.

(b) Sei $X = \{1, 2, 3, 4\}$ die Menge der Ecken des regelmäßigen Tetraeders. Sei G die Gruppe der Rotationssymmetrien von T.

Jede Drehung $g \in G$ bildet die Menge der die Ecken von T auf sich selbst ab. Zum Beispiel wirkt die Drehung r in Abbildung 3 auf X als $(2\ 3\ 4) \in S(X) = S_4$. Man überprüft, dass dies eine Gruppenwirkung $\rho : G \to S_4$ definiert.

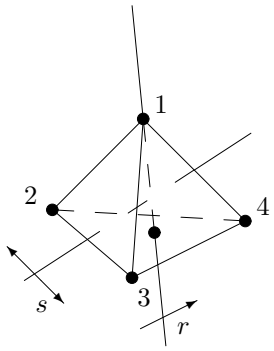


Abbildung 3: Die Rotationssymmetrien des Tetraeders

Die Gruppe G enthält einen Element e der Ordnung 1, 8 Elemente der Ordnung 3 (wie zum Beispiel r im Bild) und 3 Elemente der Ordnung 2 (wie zum Beispiel s im Bild). Also insgesamt enthält G genau 12 Elemente.

Es gilt, dass $G(1) = G(2) = G(3) = G(4) = \{1, 2, 3, 4\} = X$. Der Stabilisator der Ecke i besteht aus den Drehungen um die Achse durch i und die Mitte der gegenüberliegende Seitenfläche. Zum Beispiel ist $G_1 = \{e = r^0, r, r^2\}$.

Der Gruppenhomomorphismus $\rho : G \to S_4$ ist injektiv: Der Kern $\ker(\rho)$ besteht aus allen $g \in G$, sodass $g(i) = i$ für alle $i \in \{1, 2, 3, 4\}$. Man sieht leicht ein, dass $\ker(\rho) = \{e\}$. Das Bild $\rho(G) \subset S_4$ besteht genau aus den geraden Permutationen, wie man direkt nachrechnet. Wir schließen, dass $G \simeq A_4$ ist.

(c) Sei T und R wie in (b) und sei Y die Menge der Kanten von T. Wie in (a), wirkt R 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 gegenüberliegende Kante. Der Stabilisator der Kante 23 ist zum Beispiel $\{e, s\}$.

(d) Eine Gruppe wirkt in verschiedener Weise auf sich selbst:

$$G \times G \to G, \quad (g, x) \mapsto \tau_g(x) = gx \qquad \text{Linkstranslation},$$
$$G \times G \to G, \quad (g, x) \mapsto \kappa_g(x) = gxg^{-1} \qquad \text{Konjugation}.$$

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

Die Bahnen der Konjugation heißen *Konjugationsklassen*.

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

Beispiel 2.1.7 Wir machen jetzt noch ein etwas komplizierteres Beispiel. Sei $G = D_{12}$ die Symmetriegruppe des regelmäßigen 12-Ecks Δ_{12} mit Ecken $P_i = (\cos((i+1)\pi/6), \sin((i+1)\pi/6)$. Die Ecken P_1, P_5, P_9 formen ein regelmäßiges 3-Eck, siehe Abbildung 4.

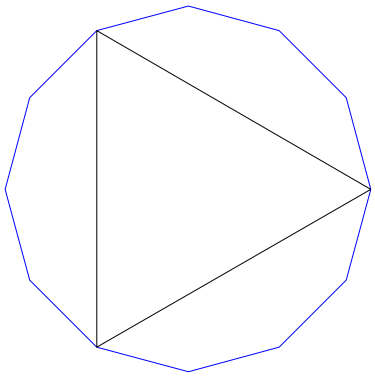


Abbildung 4: Das regelmäßige 12-Eck

Allgemeiner gilt dies auch für die Ecken P_i, P_{i+4}, P_{i+8}. Sei $X = \{1, 2, 3, 4\}$ die Menge der Dreiecken, wobei δ_i das Dreieck, dass P_i enthält, ist.

Die Gruppe D_{12} wirkt auf X. Dies definiert ein Gruppenhomomorphismus

$$\varphi : D_{12} \to S_4, \qquad g \mapsto \tau_g,$$

wobei $\tau_g \in S_4$ die von g definierte Permuation der Dreiecken ist. Seien $r \in D_{12}$ die Drehung um die Winkel $\pi/6$ und s die Spiegelung an der Gerade durch P_1 und P_7. Die Permutation τ_r vertauscht die 4 Dreiecken zyklisch: $\tau_r = (1\,2\,3\,4)$. Die Permutation τ_s lässt die Dreiecken δ_1 und δ_3 fest und vertauscht δ_2 und δ_4: $\tau_s = (2\,4)$. Man überprüft, dass

$$G(1) = \{1, 2, 3, 4\} = X, \qquad G_1 = \{e, r^4, r^8, s, r^4 s, r^8 s\}.$$

Der Stabilisator G_1 von δ_1 ist die Isomorphiegruppe des Dreiecks, also $G_1 \simeq D_3$.

Die Gruppe D_{12} wird erzeugt von r und s. Dies impliziert, dass $\tau_r = (1\,2\,3\,4)$ und $\tau_s = (2\,4)$ das Bild von φ erzeugen. Man rechnet nach, dass

$$\tau_r^4 = \tau_s^2 = 1, \qquad \tau_s \tau_r \tau_s = \tau_r^{-1}.$$

Aus Lemma 1.2.1 folgt, dass $\mathrm{im}(\varphi) \simeq D_4$ ist. Korollar 1.6.14 impliziert, dass $|\ker(\varphi)| = 3$. In der Tat überprüft man, dass $N := \ker(\varphi) = \{e, r^4, r^8\} = \langle r^4 \rangle$ ist. Insbesondere ist N ein Normalteiler von G (Lemma 1.5.9). Der erste Isomorphiesatz (Satz 1.7.6) impliziert, dass

$$D_{12}/N \simeq D_4.$$

Satz 2.1.8 (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. Dies definiert ein Gruppenhomomorphismus

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

Sei $g \in G \setminus \{e\}$. Es gilt, dass $\tau_g(e) = g \cdot e = g$. Also ist $g \notin \ker(\varphi)$. Wir schließen, dass φ injektiv ist. □

Lemma 2.1.9 *Sei $\tau : G \times X \to X$ eine Gruppenwirkung und sei $y \in G(x)$. Die Stabilisatoren G_y und G_x sind konjugiert als Untergruppen von G, d.h. es existiert ein $g \in G$, sodass $gG_xg^{-1} = G_y$.*

Beweis: Sei $y = g \cdot x$. Wir behaupten, dass $gG_xg^{-1} = G_y$ ist. Sei $h \in G_x$, also $h \cdot x = x$. Es gilt, dass $ghg^{-1} \cdot y = ghg^{-1}g \cdot x = gh \cdot x = g \cdot x = y$. Also ist $gG_xg^{-1} \subset G_y$. Ähnlich zeigt man, dass $g^{-1}G_yg \subset G_x$, oder äquivalent, dass $G_y \subset gG_xg^{-1}$ ist. Die Behauptung folgt. □

Satz 2.1.10 (Bahn-Stabilisator-Satz) *Sei $\tau : G \times X \to X$ eine Gruppenwirkung und sei $x \in X$. Die Abbildung $\varphi : g \cdot x \mapsto gG_x$ ist eine Bijektion von $G(x)$ auf die Menge der Linksnebenklassen von G_x in G.*

Beweis: Wir zeigen zuerst, dass die Abbildung φ wohldefiniert ist. Wir bemerken, dass $g_1 \cdot x = g_2 \cdot x$ genau dann, wenn $g_1^{-1}g_2 \in G_x$ ist. Also ist $\varphi(g_1 \cdot x) = g_1G_x = g_2G_x = \varphi(g_2 \cdot x)$. Somit ist φ wohldefiniert.

Die Abbilding 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, dass $g' \cdot x = (gh) \cdot x = g \cdot x$, da $h \in G_x$ ist. □

Korollar 2.1.11 *Sei G eine endliche Gruppe, die auf einer Menge X wirkt. Es gilt*

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

Insbesondere ist die Kardinalität einer Bahn ein Teiler der Gruppenordnung.

Beweis: Satz 2.1.10 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 1.6.8.(b). □

Beispiel 2.1.12 (a) Sei X die Menge der Ecken des regelmäßigen Tetraeders. In Beispiel 2.1.6.(b) haben wir durch nachzählen bestimmt, dass G genau 12 Elemente bestimmt. Dies folgt auch aus Korollar 2.1.11, da $|G(1)| = 4$ und $|G_1| = 3$ (Beispiel 2.1.6.(b)).

(b) Sei $X = \{1, 2, 3, 4, 5, 6, 7, 8\}$ die Mengen der Ecken und G die Rotationssymmetriegruppe des regelmäßigen Würfels. Ähnlich wie im Beispiel 2.1.6.(b) überprüft man, dass die Wirkung transitiv ist, also dass der Bahn $G(1) = X$ ist. Sei r eine Drehung um $2\pi/3$ Grad um der Körperdiagonale durch 1. Der Stabilisator G_1 besteht aus $G_1 = \{e = r^0, r, r^2\}$. Wir schließen aus Korollor 2.1.11, dass $|G| = 8 \cdot 3 = 24$ ist. Man kann zeigen, dass $G \simeq S_4$ ist. (Übungsaufgabe. Tipp: betrachte die Wirkung von G auf die Menge der Körperdiagonale $Y = \{1, 2, 3, 4\}$ und argumentiere wie in Beispiel 2.1.6.(b).)

2.2 Das Theorem von Burnside

In diesem Abschnitt geben wir eine Anwendung von Gruppenwirkungen. Wir möchten zum Beispiel die Anzahl der Möglichkeiten zählen, um die Ecken des regelmäßigen Tetraeders T mit drei Farben anzumalen. Dieses Problem hat Anwendungen in der Chemie. Offensichtlich hat dieses Problem etwas mit der Symmetriegruppe des Tetraeders zu tun: Zwei Färbungen, die sich durch eine Drehung in einander überführen lassen, sind im Wesentlichen gleich.

Sei $E = \{1, 2, 3, 4\}$ die Menge der Ecken von T. Sei X die Menge der Färbungen der Ecken: Eine Färbung ordnet jeder Ecke eine der 3 Farben zu. Die Kardinalität von X ist also 3^4. Um die wirklich verschiedenen Färbungen zu bestimmen, betrachten wir die Wirkung der Rotationssymmetriegruppe R von T auf der Menge X der Färbungen. Die Anzahl der wirklich unterschiedlichen Färbungen ist die Anzahl der Bahnen dieser Wirkung. Das Theorem von Burnside liefert eine Methode, die Bahnen zu zählen.

Theorem 2.2.1 (Burnside) *Sei G eine endliche Gruppe, die auf einer Menge X wirkt. Für $g \in G$ definieren wir*

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

Die Anzahl der Bahnen ist

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

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

Wir zählen die Paare

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

Einerseits gilt

$$|S| = \sum_{g \in G} |X^g|. \tag{3}$$

Anderseits gilt

$$|S| = \sum_{x \in X} |G_x| = \sum_{i=1}^{k} \sum_{x \in X_i} |G_x|. \tag{4}$$

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

Lemma 2.1.9 sagt, dass Punkte in der gleichen Bahn konjugierte Stabilisatoren haben. Insbesondere gilt $|G_x| = |G_{x_i}|$ 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 den Bahn-Stabilisator-Satz (Korollar 2.1.11) folgt, dass $|G(x_i)| \cdot |G_{x_i}| = |G|$. Wir schließen aus (3) und (4), dass

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

Das Theorem folgt. □

Beispiel 2.2.2 (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 R die Rotationssymmetriegruppe des Tetraeders T. In R gibt es drei Typen von Elementen: (Siehe Abbildung 3):

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

Wir zählen für jedes Element $g \in R$ die Menge X^g der von g festgelassenen Färbungen. Diese Anzahl hängt nur vom Typ ab, wie man leicht einsieht. 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 gegenüberliegende Seitenfläche F. Falls $x \in X^g$ eine von g festgelassene Färbung ist, so 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 gegenüberliegenden Kanten K_1 und K_2. Die Drehung vertauscht die beide Ecken der Kante K_1 (bzw. K_2). Falls $x \in X^g$ eine von g festgelassene Färbung ist, so 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 verschiedene 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 Armbänder bestehend aus 5 Perlen an einem kreisförmigen Band. Wie viele Armbänder können wir mit roten, blauen und gelben Perlen machen? Die Symmetriegruppe hier ist die Diedergruppe D_5. Wir benutzen die Bezeichnung wie in § 1.2 und unterscheiden drei Fälle.

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

Die Drehungen $g = r, r^2, r^3, r^4$ 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 $g = s, rs, r^2s, r^3s, r^4s$ sind Spiegelungen an einer Achse durch eine Ecke P_k und die Mitte der gegenüberliegende Kante. Die Ecke P_k wird von der Spiegelung festgelassen. Die andere Ecke formen 2 Bahnen mit 2 Elementen. Also ist $|X^g| = 3^3$.

Die Anzahl der Armbänder ist daher

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

2.3 Der Satz von Cauchy

Der Satz von Lagrange (Satz 1.6.10) impliziert, dass die Ordnung eines Elements $g \in G$ einer endlichen Gruppe G ein Teiler der Grupenordnung ist. Die Umkehrung gilt nicht. Zum Beispiel besitzt S_4 kein Element der Ordnung 6 obwohl $6 \mid 24$. Der folgende Satz gibt eine partielle Umkehrung des Satzes von Lagrange.

Satz 2.3.1 *Sei G eine endliche Gruppe und p eine Primzahl mit $p \mid |G|$. So besitzt G ein Element der Ordnung p.*

Beweis: Sei G eine endliche Gruppe und p eine Primzahl mit $p \mid |G|$. Sei

$$X = \{(x_1, \ldots, x_p) \in G^p \mid x_1 \cdot x_2 \cdots x_p = e\}.$$

Wir suchen ein Element $x \in G \setminus \{e\}$ mit $x^p = e$, also ein Element $(x, x, \ldots x) \in X$.

Wir zählen die Kardinalität von X. Dazu bemerken wir, dass $(x_1, \ldots, x_p) \in G$ genau dann, wenn $x_p = (x_1x_2\cdots x_{p-1})^{-1}$. Also ist x_p von $x_1, \ldots, x_{p-1}$ bestimmt und sind $x_1, \ldots, x_{p-1}$ beliebig. Es folgt, dass $|X| = |G|^{p-1}$. Insbesondere gilt $p \mid |X|$.

Die Gruppe $\mathbb{Z}/p\mathbb{Z}$ wirkt auf X wie folgt: Für $i \in \mathbb{Z}/p\mathbb{Z}$ definieren wir

$$i \cdot (x_1, \ldots, x_p) = (x_{i+1}, x_{i+2}, \ldots, x_p, x_1, \cdots, x_i).$$

Man überprüft leicht, dass $i \cdot (x_1, \ldots, x_p) \in X$. Der Bahn–Stabilisator-Satz (Korollar 2.1.11) impliziert, dass jede Bahn dieser Wirkung entweder Länge p oder eins hat. Die Bahn eines Elements $(x_1, \ldots, x_p)$ hat genau dann Länge 1,

wenn alle x_i gleich sind, also wenn $x = x_1 = \cdots = x_p$ ein Element der Ordnung p ist.

Die Bahn von $(e, e, \ldots, e)$ hat auf jeden Fall nur ein Element. Da p ein Teiler von $|X|$ ist, existieren mindestens $p-1$ weitere Bahnen der Länge 1, also existieren Elemente der Ordnung p. □

Beispiel 2.3.2 Die Kardinalität der Gruppe S_4 ist 24. Die Gruppe S_4 enthält Elemente der Ordnung 2 und 3 (zum Beipiel (1 2) und (1 2 3)). Die Gruppe S_4 enthält keinen Element der Ordnung 6. Dies zeigt, dass Satz 2.3.1 nicht notwendigerweise gilt, wenn p keine Primzahl ist.

Korollar 2.3.3 *Jede Gruppe der Ordnung* 6 *ist isomorph zu* $\mathbb{Z}/6\mathbb{Z}$ *oder* D_3.

Beweis: Sei G eine Gruppe mit 6 Elementen. Der Satz von Cauchy (Satz 2.3.1) impliziert, dass G ein Element x der Ordnung 3 und ein Element y der Ordnung 2 besitzt. Sei $H = \langle x \rangle$ die Untergruppe erzeugt von x. Die Rechtsnebenklassen $H = \{e, x, x^2\}$ und $Hy = \{y, xy, x^2y\}$ sind disjunkt und besitzen zusammen 6 Elemente, also ist $G = H \amalg Hy$. Das Element yx ist verschieden von y und auch nicht in H. Wir schließen, dass entweder $yx = xy$ oder $yx = x^2y$ gilt. Falls $xy = yx$, so überprüft man, dass die Ordnung von xy gleich 6 ist, also ist G zyklisch. Sonst gilt $yx = x^2y$ oder äquivalent $yxy = x^{-1}$. Die Abbildung $\varphi : G \to D_3, x \mapsto r, y \mapsto s$ definiert nun einen Isomorphismus (vergleichen Sie mit Lemma 1.2.1.(c)). □

Sei p eine ungerade Primzahl und G eine Gruppe der Ordnung $2p$. Wie im Beweis von Korollar 2.3.3 zeigt man, dass G entweder zyklisch oder isomorph zur Diedergruppe D_p ist.

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 Modell ist der Ring $\mathbb{Z}$ der ganzen Zahlen. In Kapitel 1 haben wir $\mathbb{Z}$ als Gruppe mit Addition als Verknüpfung betrachtet und die Multiplikation ignoriert. Wenn wir $\mathbb{Z}$ als Ring auffassen, betrachten wir beide Verknüpfungen gleichzeitig.

3.1 Definitionen

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

(R1) $(R, +)$ ist eine abelsche Gruppe. Das neutrale Element von $(R, +)$ schreiben wir als 0.

(R2) Die Multiplikation ist assoziativ und besitzt ein neutrales Element 1.

(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 abgeschlossen bezüglich Addition, Subtraktion und Multiplikation ist und das 1-Element enthält.

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

Die meisten Ringe, die wir in der Vorlesung betrachten, sind kommutativ.

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

(b) Jeder Körper ist auch ein Ring.

(c) Sei R ein Ring. Die Menge $R[x] = \{f(x) = \sum_{i=0}^{n} a_i x^i \mid a_i \in R\}$ der Polynome mit Koeffizienten in R ist ein Ring.

(d) 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 gaußschen Zahlen*.

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

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

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

(g) 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 Ringes fordern wir nicht, dass jedes Element $a \in R$ ein multiplikatives Inverses besitzt. Die Elemente $a \in R$, welche in R ein multiplikatives Inverses b mit $ab = ba = 1$ besitzen, heißen *Einheiten*. Wir schreiben R^* für die Menge der Einheiten. Ein *Körper* ist ein kommutativer Ring K, sodass jedes Element $a \in K \setminus \{0\}$ eine Einheit ist.

Beispiel 3.1.3 (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 $\{0 < a < m \mid \mathrm{ggT}(a, m) = 1\}$ (Vergleichen Sie mit Beispiel 1.6.11).

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

(c) Der Ring $R = \mathbb{Z}/m\mathbb{Z}$ ist genau dann ein Körper, wenn $m = p$ eine Primzahl ist (Beispiel 1.6.11). Wir schreiben auch $\mathbb{F}_p := \mathbb{Z}/p\mathbb{Z}$ für der Körper mit p Elemente.

Definition 3.1.4 Ein Element $a \in R$ eines Ringes heißt *Nullteiler*, falls ein $b \in R \setminus \{0\}$ mit $ab = 0$ oder $ba = 0$ existiert. Ein kommutativer Ring $R \neq \{0\}$ nennen wir *Integritätsring*, falls 0 der einzige Nullteiler ist.

Beispiel 3.1.5 (a) Jeder Körper ist ein Integritätsring, da eine Einheit nie ein Nullteiler ist (außer wenn $R = \{0\}$).

(b) Falls R ein Integritätsring ist, so ist auch der Polynomring $R[x]$ ein Integritätsring.

(c) Sei K ein Körper und $R := K[\epsilon] = \{a + b\epsilon \mid a, b \in K, \epsilon^2 = 0\}$ der Ring der *duale Zahlen*. Das Element ϵ ist ein Nullteiler, also ist R kein Integritätsring.

3.2 Homomorphismen und Ideale

In dem Rest von Kapitel 3 nehmen wir an, dass alle Ringe kommutativ sind, wenn es nicht ausdrücklich anders gesagt wird. Einfachheitshalber, schließen wir außerdem $R = \{0\}$ aus.

In diesem Abschnitt definieren wir Ringhomomorphismen. Ähnlich wie für Gruppen (§ 1.5), sind dies Abbildungen zwischen Ringen, die verträglich sind mit Addition und Multiplikation.

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

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

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

Sei $\varphi : R \to R'$ ein Ringhomomorphismus. Es gilt, dass $\varphi(0_R) = \varphi(0_R + 0_R) = \varphi(0_R) + \varphi(0_R)$. Da $-\varphi(0_R) \in R'$ existiert, folgt, dass $\varphi(0_R) = 0_{R'}$. (Vergleichen Sie zu Lemma 1.5.3). Das gleiche Argument funktioniert nicht immer für 1_G, da nicht jedes Element von R' eine Einheit ist. Daher müssen wir in der Definition 3.2.1 fordern, dass $\varphi(1_R) = 1_{R'}$ 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 definiert einen Ringhomomorphismus:

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

da $(f + g)(\alpha) = f(\alpha) + g(\alpha)$ und $(fg)(\alpha) = f(\alpha)g(\alpha)$. Außerdem nimmt das Einspolynom 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 Homomorphismus. 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 $\varphi : \mathbb{Z} \to \mathbb{Z}/p\mathbb{Z} = \mathbb{F}_p, \quad a \mapsto a \pmod p =: [a]$ ist ein Homomorphismus. Sei $\alpha \in \mathbb{F}_p$. Satz 3.2.3 liefert einen Homomorphismus

$$\psi : \mathbb{Z}[x] \mapsto \mathbb{F}_p, \qquad f(x) = \sum_{i=0}^{n} a_i x^i \mapsto \sum_{i=0}^{n} [a]_i \alpha^i \in \mathbb{F}_p.$$

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 sehr ähnlich an der Definition des Kerns eines Gruppenhomomorphismus. 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 $R' \neq \{0\}$, so 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, aber u erfüllt 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, dass $a + b \in I$ ist.

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

Beweis: Seien $a, b \in I$ und $r \in R$. Es gilt, dass $\varphi(a + b) = \varphi(a) + \varphi(b) = 0 + 0 = 0$ und, dass $\varphi(ra) = \varphi(r)\varphi(a) = \varphi(r) \cdot 0 = 0$. Also sind $a + b, ra \in I$. □

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

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

(I1) $(I, +) \subset (R, +)$ eine Untergruppe ist,

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

Beispiel 3.2.8 (a) Der Kern eines Ringhomomorphismus ist ein Ideal.

(b) Sei $I \subset R$ 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 $I \neq (0)$. Also enthält I ein Element $a \neq 0$. Da K ein Körper ist, so existiert $a^{-1} \in K$. Aber nun ist auch $1 = a^{-1}a \in I$. Also ist $I = K$.

Sei $\alpha \in R$ ein Element. Die Menge $(a) = Ra = aR = \{ar \mid r \in R\}$ ist ein Ideal von R. (Hier benutzen wir die Annahme, dass R kommutativ ist!) Das Ideal (a) heißt, das *von a erzeugte Ideal*. Ein Ideal, das von einen Element erzeugt wird, heißt *Hauptideal*. Der folgende Satz zeigt, dass jedes Ideal von $\mathbb{Z}$ ein Hauptideal ist. Ringe mit dieser Eigenschaft heißen *Hauptidealringe*.

Satz 3.2.9 *Jedes Ideal I von $\mathbb{Z}$ ist ein Hauptideal.*

Beweis: Wir bestimmen die Ideale I von $\mathbb{Z}$. Da jedes Ideal I von $\mathbb{Z}$ auch eine Untergruppe bildet, folgt, dass $I = (m) = m\mathbb{Z}$, für ein $m \geq 0$ (Theorem 1.3.11). Beispiel 3.2.8.(b) zeigt, dass $I = (m)$ auch tatsächlich ein Ideal ist. □

Ein Ideal $I \subset R$ ist insbesondere eine Untergruppe von $(R, +)$. Da wir annehmen, dass R kommutativ ist, ist I auch ein Normalteiler der Gruppe $(R, +)$. Die Faktorgruppe $\bar{R} := R/I$ ist also wohldefiniert. In § 1.7 haben wir die Faktorgruppe definiert als die Menge der Linksnebenklassen $a + I = \{a + r \mid r \in I\}$. Die Addition auf $\bar{R}$ ist definiert als

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

Folgendes Theorem sagt, dass $\bar{I}$ sogar ein Ring ist. Ein Beispiel haben wir schon gesehen: Die Faktorgruppe $\mathbb{Z}/m\mathbb{Z}$ ist ein Ring (Beispiel 3.1.2.(a)).

Theorem 3.2.10 *Sei $I \subset R$ 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 Ringen**) Falls $\pi : R \to R'$ ein surjektiver Ringhomomorphismus mit Kern I ist, so ist $R' \simeq R/I$.*

Beweis: Wir müssen zuerst eine Multiplikation auf der Menge $\bar{R} = \{a + I\}$ der Linksnebenklassen von I in R definieren. Wir behaupten, dass

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

eine Multiplikation definiert. Die Menge $(a+I)(b+I)$ ist die Menge der Elemente $(a+x)(b+y) = ab+ay+bx+xy$ mit $x, y \in I$. Da I ein Ideal ist, ist $ay+bx+xy \in I$, also ist $(a + I)(b + I) \subset ab + I$. Die Menge $(a + I)(b + I)$ ist eine Vereinigung von Linksnebenklassen, da $(a + x)(b + y) + z \in (a + I)(b + I)$ für alle $z \in I$. Aber dies impliziert, dass $(a + I)(b + I) = ab + I$, da keine echte Teilmenge von $ab + I$ eine Linksnebenklasse ist.

Die Assoziativität der Multiplikation und die Distributivgesetze folgen aus der Assoziativität der Multiplikation und den Distributivgesetze von 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 ähnlich am Beweis von Satz 1.7.6. □

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

Beispiel 3.2.11 (a) In Beispiel 3.2.2 haben wir gesehen, dass

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

ein Ringhomomorphismus ist. Es gilt $I := \ker(\varphi) = \{f \in \mathbb{R}[x] \mid f(i) = 0\}$. Da $f \in \mathbb{R}[x]$, so folgt, dass $f(-i) = \overline{f(i)} = \bar{0} = 0$, wobei $^-$ die komplexe Konjugation ist. Polynomdivision impliziert, dass $(x^2 + 1) \mid f$. (Dies ist bekannt aus der Vorlesung *Lineare Algebra*, siehe auch § 3.3, insbesondere Korollar 3.3.3). Also ist $I = (x^2+1)$. Wir schließen, dass $\mathbb{C} \simeq \mathbb{R}[x]/(x^2+1)$.

(b) Sei p eine Primzahl und

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

wobei $[a_i] = a_i \pmod p$ ist. Dies ist ein surjektiver Ringhomomorphismus. Sei $f \in I := \ker(\varphi)$. Es gilt, dass $f(x) = \sum_{i=0}^{n} a_i x^i$, wobei $p \mid a_i$ 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 3.2.10.(b) folgt, dass $\mathbb{Z}[x]/p\mathbb{Z}[x] \simeq \mathbb{F}_p[x]$ ist.

Wir bestimmen nun wann ein Faktorring R/I ein Körper ist.

Definition 3.2.12 Sei R ein Ring. Ein Ideal $I \subset R$ heißt *maximal*, falls $I \neq R$ und die einzige Ideale die I enthalten I und R sind.

Beispiel 3.2.13 (a) Ein Ideal $m\mathbb{Z} \subset \mathbb{Z}$ mit $m > 0$ ist genau dann maximal, wenn m eine Primzahl ist.

(b) Ein Ring R ist ein Körper genau dann, wenn $I = (0)$ maximal ist. Nämlich, falls R ein Körper ist, so ist jedes Element $a \neq 0$ ein Einheit, also sind (0) und R die einzige Ideale von R. Umgekehrt, sei $(0) \subset R$ ein maximales Ideal. Für jedes $a \in R \setminus \{0\}$ gilt, dass $(a) = aR = R$. Insbesondere existiert ein $b \in R$, sodass $ab = 1$. Wir schließen, dass a eine Einheit ist. Es folgt, dass R ein Körper ist.

Satz 3.2.14 *Ein Ideal I eines Ringes R ist genau dann maximal, wenn der Faktorring $\bar{R} = R/I$ ein Körper ist.*

Beweis: Zuerst bemerken wir, dass $R/I = (0)$ genau dann, wenn $I = R$ ist. Da (0) kein Körper ist, stimmt die Aussage für $I = R$.

Wir dürfen also annehmen, dass $I \neq R$ ist. Wir bemerken nun, dass $I \subset R$ maximal ist genau dann, wenn $I + aR = R$ für alle $a \notin I$ gilt. (Sonst wäre $I \subsetneq I + aR \subsetneq R$.) Diese Bedingung ist äquivalent zu: Für alle $a \notin I$ existieren $r \in R$ und $x \in I$, sodass $x + ra = 1$ ist.

Wir nehmen an, dass I ein maximales Ideal ist und schreiben $\pi : R \to \bar{R} := R/I$ für die Abbildung aus Theorem 3.2.10.(b). Für alle $a \notin I$ existieren also $r \in R$ und $x \in I$, sodass $x + ra = 1$ ist. Dies impliziert, dass $\pi(ra) = \pi(r)\pi(a) = \pi(1) = 1$. Also ist $\pi(a) \in \bar{R}$ eine Einheit. Da jedes Element $0 \neq \pi(a) \in \bar{R}$ eine Einheit ist, ist $\bar{R}$ ein Körper. Die Umkehrung ist ähnlich. □

3.3 Polynomringe

Sei R ein Integritätsring. In diesem Abschnitt beschreiben wir den Polynomring $R[x]$ etwas genauer.

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

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

Seien $f(x), g(x) \in R[x]$ mit $g(x) \neq 0$. Wir sagen, dass $g(x)$ ein *Teiler* von $f(x)$ ist, falls ein Polynom $h(x) \in R[x]$ mit $f(x) = g(x)h(x)$ existiert.

Der folgende Satz ist ein Analogon der Division mit Rest für Polynome. Der Beweis ist ähnlich dem Beweis in [4, Satz 5.2.1], siehe auch [3, Satz 2.1.4]. Wir überlassen ihn dem Leser/der Leserin. Achtung: In loc.cit. werden Polynomringe über einen Körper betrachtet. Da alle Elemente von $K \setminus \{0\}$ Einheiten sind, kann man in diesem Fall die Bedingung an g ersetzen durch die Bedingung $g \neq 0$.

Satz 3.3.1 (Polynomdivision) *Sei R ein Ring und seien $f(x), g(x) \in R[x]$ Polynome mit $fg \neq 0$, sodass der führende Term von g eine Einheit in R ist. Es existieren eindeutige Polynome $q(x)$ und $r(x) \in R[x]$ mit*

$$f(x) = q(x)g(x) + r(x),$$

wobei $\mathrm{Grad}(r) < \mathrm{Grad}(g)$ *ist.*

Beispiel 3.3.2 Sei $f(x) = x^5 + x^2 - 4x - 2$ und $g(x) = 2x^4 + 2x^3 + 4x^2 + 6x + 2 \in \mathbb{Q}[x]$. Wir finden, dass $f = gq + r$ mit $q(x) = (x-1)/2$ und $r(x) = -x^3 - 2x - 1$.

Wir können f, g auch als Elemente von $\mathbb{Z}[x]$ auffassen. Da $1/2 \notin \mathbb{Z}$ ist, ist 2 keine Einheit in $\mathbb{Z}$. Also können wir Satz 3.3.1 nun nicht anwenden. In der Tat ist $q(x) \notin \mathbb{Z}[x]$.

Korollar 3.3.3 *Sei $f(x) \in R[x]$ ein Polynom. Es gilt, dass $a \in R$ eine Nullstelle von f ist genau dann, wenn ein Polynom $q(x) \in R[x]$ mit*

$$f(x) = q(x)(x - a)$$

existiert.

Beweis: Dies folgt unmittelbar aus Satz 3.3.1, da $x - a$ ein Teiler von $f(x)$ ist genau dann, wenn der Rest von f nach Division durch $x - a$ gleich 0 ist. Hier haben wir benutzt, dass $\mathrm{Grad}(x - a) = 1$ ist. □

Wir bestimmen nun die Ideale in $K[x]$, wo K ein Körper ist. Der Beweis von Theorem 3.3.4 ist ähnlich dem Beweis von Theorem 1.3.11. (Sehen Sie, wieso?) Theorem 3.3.4 sagt, dass $K[x]$ ein Hauptidealring ist.

Theorem 3.3.4 *Sei K ein Körper. Jedes Ideal $I \subset K[x]$ ist ein Hauptideal.*

Beweis: Sei $I \subset K[x]$ ein Ideal. Das 0-Ideal ist ein Hauptideal, also dürfen wir annehmen, dass $I \neq (0)$ ist. Sei $0 \neq g \in I$ ein Polynom minimalen Grades. Wir behaupten, dass $I = (g)$ ist. Sei dazu $f \in I$ beliebig. Polynomdivision liefert Polynome $q, r \in K[x]$ mit $f = qg + r$ und $\mathrm{Grad}(r) < \mathrm{Grad}(g)$. Da $f, g \in I$ sind, folgt, dass $r = f - qg \in I$ ist. Da g ein Polynom minimalen Grades ist, folgt, dass $r = 0$. Also ist $f = qg \in (g)$. □

Beispiel 3.3.5 Nicht jeder Ring ist ein Hauptidealring. Sei $p \in \mathbb{Z}$ eine Primzahl. Das Ideal $I = (p, x) \subset \mathbb{Z}[x]$ erzeugt von p und x ist kein Hauptideal.

Folgendes Korollar ist ähnlich wie Korollar 1.3.12. Mehr Details finden Sie in [4, § 5.2].

Korollar 3.3.6 *Sei K ein Körper und $f, g \in K[x]$ nicht beide Null. Es existiert ein eindeutiges normiertes Polynom $d = \mathrm{ggT}(f, g)$, 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 Polynome r und s mit $rf + sg = d$.

Sei nun K ein Körper und $I \subset K[x]$ ein Ideal mit $I \neq (1) = K[x]$. Theorem 3.3.4 impliziert, dass ein Polynom $f \in K[x]$ mit $I = (f)$ existiert.

Definition 3.3.7 Sei R ein Integritätsring. Ein Element $a \in R$ heißt *irreduzibel*, falls a keine Einheit ist und für alle $b, c \in R$ mit $a = bc$ gilt, dass entweder $b \in R^*$ oder $c \in R^*$ ist.

Wir betrachten nun den Spezialfall, dass $R = K[x]$ mit K ein Körper ist. Ein nicht-konstantes Polynom $f \in K[x]$ ist genau dann irreduzibel, wenn die einzigen echten Teiler $g(x)$ von $f(x)$ die konstanten Polynome sind. Hier benutzen wir, dass $K[x]^* = K^*$ gilt.

Der folgende Satz beschreibt den Faktorring $K[x]/I$ etwas genauer. Teil (b) des Satzes sagt, dass $K[x]/(f)$ genau dann ein Körper ist, wenn $f(x)$ ein *irreduzibles* Polynom ist.

Satz 3.3.8 *(a) Sei K ein Körper und $I = (f) \subset K[x]$ ein nichttriviales Ideal (d.h. $I \neq (0), K[x]$)). Sei $n := \mathrm{Grad}(f)$. Die Menge*

$$K[\alpha] := \{\sum_{i=0}^{n-1} a_i \alpha^i \mid a_i \in K,\ f(\alpha) = 0\}$$

ist ein Ring. Außerdem gilt $K[x]/I \simeq R$.

(b) Ein Ideal $I = (f) \subset K[x]$ ist genau dann maximal, wenn f ein nichtkonstantes, irreduzibles Polynom ist. Insbesondere ist $K[\alpha] = K[x]/(f)$ genau dann einen Körper, wenn f irredizibel ist.

Beweis: Wir überprüfen zuerst, dass R ein Ring ist. Es ist offensichtlich, dass R mit Addition eine abelsche Gruppe ist. Es ist sogar ein K-Vektorraum. Wir schreiben $f(x) = \sum_{i=0}^{n} c_i x^i$ mit $c_n \neq 0$. In R gilt daher die Relation

$$\alpha^n = -\sum_{i=0}^{n-1} \frac{c_i}{c_n} \alpha^i.$$

Dies definiert die Multiplikation auf R.

Satz 3.2.3 impliziert, dass ein eindeutiger Ringhomomorphismus $\varphi : K[x] \to R$ existiert mit $\varphi(x) = \alpha$ und $\varphi(a) = a$ für alle $a \in K$. Offensichtlich gilt, dass $\ker(\varphi) = I$. Außerdem ist φ surjektiv. Der erste Isomorphiesatz (Theorem 3.2.10.(b)) impliziert, dass $K[x]/I \simeq R$ ist.

Teil (b) folgt direkt aus der Definition und Satz 3.2.14. □

Beispiel 3.3.9 Sei $f(x) = x^2 + x + 1 \in \mathbb{Q}[x]$. Satz 3.3.8 impliziert, dass

$$R := \mathbb{Q}[x]/(f) = \{a_0 + a_1\alpha \mid a_i \in \mathbb{Q},\ \alpha^2 = -\alpha - 1\}.$$

Insbesondere gilt, dass $\alpha^3 = \alpha(-\alpha - 1) = -\alpha^2 - \alpha = 1 \in R$. Die Ordnung von α in der multiplikativen Gruppe $(R^*, \times)$ ist daher 3. Alternativ kann man R auch beschreiben als Unterring von $\mathbb{C}$: Sei $\mathbb{Q}[\zeta_3]$ der kleinste Unterring von $\mathbb{C}$, der die primitive dritte Einheitswurzel $\zeta_3 := e^{2\pi i/3}$ enthält. Es gilt, dass

$$R := \mathbb{Q}[x]/(f) \simeq \mathbb{Q}[\zeta_3].$$

Das Polynom $f(x) = x^2+x+1$ faktorisiert in $\mathbb{C}[x]$ als $f(x) = (x-\zeta_3)(x-\zeta_3^2)$. Da $\zeta_3, \zeta_3^2 \notin \mathbb{Q}$, schließen wir, dass $f(x) \in \mathbb{Q}[x]$ irreduzibel ist. Wir schließen, dass $\mathbb{Q}[\zeta_3]$ ein Körper ist (Satz 3.3.8.(b) und Satz 3.2.14).

In der Tat sehen wir, dass für $0 \neq a + b\zeta_3 \in \mathbb{Q}[\zeta_3]$ gilt, dass

$$\frac{1}{a+b\zeta_3} = \frac{a+b\zeta_3^2}{(a+b\zeta_3)(a+b\zeta_3^2)} = \frac{a+b\zeta_3^2}{a^2-ab+b^2} = \frac{a-b-b\zeta_3}{a^2-ab+b^2} \in \mathbb{Q}[\zeta_3].$$

Hier haben wir die Relation $1 + \zeta_3 + \zeta_3^2 = 0$ mehrmals benutzt.

3.4 Faktorisieren von Polynomen

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

Lemma 3.4.1 *Sei K ein Körper.*

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

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

Beweis: Teil (a) ist klar. Sei f ein Polynom zweiten oder dritten Grades. Wir nehmen an, dass f reduzibel ist. Also lässt sich f schreiben als $f(x) = g(x)h(x)$ mit $1 \leq \mathrm{Grad}(g) < \mathrm{Grad}(f)$. Es folgt, dass entweder g oder h ein Polynom ersten Grades ist. □

Die Methode von Lemma 3.4.1 kann man erweitern für Polynome größeren Grades. 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 finden durch ausprobieren: 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 einer Faktor 2 kann man nun überprüfen durch Koeffizientenvergleich.

Das Durchprobieren von Faktoren ist nur geeignet für Polynome kleinen Grades, daher ist es wünschenswert, allgemeine Kriterien zu haben. Dies ist das Ziel dieses Abschnittes.

Satz 3.4.2 (Gauß) *Sei $f \in \mathbb{Z}[x]$ ein irreduzibles Polynom über $\mathbb{Z}$. So 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. Dies bedeutet, dass $g, h \in \mathbb{Q}[x]$ Polynome von Grad größer gleich 1 sind. Es existiert ein $n \in \mathbb{Z}$, sodass

$$nf = g'h'$$

eine Zerlegung in $\mathbb{Z}[x]$ ist, zum Beispiel können wir für n das Produkt der Nenner der Koeffizienten von g und h nehmen. Wir schreiben $g' = \sum_{i=0}^{s} g_i x^i$ und $h' = \sum_{j=0}^{t} h_j x^j$, wobei $g_i, h_j \in \mathbb{Z}$ sind.

Sei p ein Primfaktor von n. Wir behaupten, dass p alle Koeffizienten von g oder alle Koeffizienten von h teilt. Nehmen wir an, dies würde nicht gelten. Sei i und j minimal, sodass $p \nmid g_i$ und $p \nmid h_j$. Da $p \mid n$, so teilt p der Koeffizient c_{i+j} von x^{i+j} in $g'h'$. Es gilt, dass

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

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

Wir schließen, dass p entweder alle Koeffizienten von g' oder alle Koeffizienten von h' teilt. OBdA dürfen wir also annehmen, dass p alle Koeffizienten von g teilt. Wir schreiben $n = pn_1$ und $g' = pg''$. Wir können nun den Faktor p kürzen, und erhalten

$$n_1 f = g''h'.$$

Dieses Verfahren wiederholend mit allen Primfaktoren von n, finden wir letzendlich eine Faktorisierung

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

mit $\bar{g}, \bar{h} \in \mathbb{Z}[x]$. Da außerdem gilt, dass $\bar{g} = \alpha g$ und $\bar{h} = \beta h$ für $\alpha, \beta \in \mathbb{Z}$, ist dies eine nicht-triviale Zerlegung von f über $\mathbb{Z}$. Dies widerspricht der Irreduzibilität von f über $\mathbb{Z}$. Wir schließen, dass f auch irreduzibel über $\mathbb{Q}$ ist. □

Beispiel 3.4.3 Wir benutzen die Idee des Satzes von Gauss (Satz 3.4.2) 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 $\mathrm{ggT}(b, c) = 1$. Satz 3.4.2 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.

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

Theorem 3.4.4 (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

1. $p \nmid a_n$,
2. $p \mid a_i, \qquad i = 0, \dots a_{n-1}$,
3. $p^2 \nmid a_0$.

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 3.4.2). 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 (1). Sei $1 \leq i \leq s$ minimal, sodass $p \nmid g_i$. Es gilt, dass

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

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 3.4.5 Sei

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

Das Polynom f ist irreduzibel über $\mathbb{Q}$ genau dann, wenn $9f = 2x^5 + 15x^4 + 9x^3 + 3$ irreduzibel über $\mathbb{Z}$ ist. Das folgt aus dem Eisenstein-Kriterium (Theorem 3.4.4) angewendet mit $p = 3$.

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

Lemma 3.4.6 *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, so 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 $f \in \mathbb{Q}[x]$ besitzt. Falls $f \in \mathbb{Q}[x]$ reduzibel ist, so existieren nicht-konstante Polynome $g, h \in \mathbb{Z}[x]$ mit $f = gh$ (Satz 3.4.2). Da $\text{Grad}(f) = \text{Grad}(\bar{f})$ und $\bar{f} = \bar{g}\bar{h}$, folgt, dass $\text{Grad}(g) = \text{Grad}(\bar{g})$ und $\text{Grad}(h) = \text{Grad}(\bar{h})$. 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 Korollar 3.3.3 liefert, dass ein Polynom $g \in K[x]$ existiert, sodass

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

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, so 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 3.4.7 *Sei $\alpha \in K$ eine Nullstelle von $f(x) \in K[x]$. Die Nullstelle α ist eine mehrfache Nullstelle von f genau dann, 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, dass

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

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

Satz 3.4.8 *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. Korollar 3.3.3 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 Körpererweiterungen

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

Eine *Teil-* oder *Zwischenerweiterung* von L/K ist ein Teilkörper M von L, der K enthält. Notation: $L/M/K$.

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

(b) Sei K ein beliebiger Körper und $K[t]$ der Polynomring über K in einer Unbestimmten t. Da $K[t]$ ein Integritätsring ist (Beispiel 3.1.5), existiert ein kleinster Körper L, der den Ring $K[t]$ enthält, der sogenannte *Quotientenkörper* von $K[t]$, siehe zum Beispiel [3, p. 61f]. Wir schreiben

$$L = K(t)$$

und nennen $K(t)$ den *Körper der rationalen Funktionen* über K.

Konkret sind die Elemente von $K(t)$ Brüche, deren Zähler und Nenner Polynome in t mit Koeffizienten in K sind,

$$f = \frac{g}{h} \in K(t), \qquad g, h \in K[t],\ h \neq 0.$$

Das Rechnen mit Elementen aus $K(t)$ erfolgt nach den üblichen Regeln des Bruchrechnens. Beispiel:

$$\Big(\frac{t-1}{t+1}\Big)^{-1} - 1 = \frac{2}{t-1}.$$

(c) Sei K ein Körper und $f \in K[x]$ ein irreduzibles Polynom. Wir haben gesehen, dass $L := K[x]/(f)$ ein Körper ist. Offensichtlich ist L eine Körpererweiterung von K.

Definition 4.1.3 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.

Beispiel 4.1.4 (a) Wir haben $\mathbb{R}(i) = \mathbb{C}$.

(b) Der Körper $\mathbb{Q}(\zeta_3)$ ist der Teilkörper von $\mathbb{C}/\mathbb{Q}$ entstanden durch Adjunktion von $\zeta_3 \in \mathbb{C}$ (siehe auch Beispiel 3.3.9).

(c) Sei $\alpha \in \mathbb{R}$ die (eindeutig bestimmte) reelle dritte Wurzel aus 2 und sei $L := \mathbb{Q}(\alpha)$. Wir überlassen es dem Leser/der Leserin zu überprüfen, dass

$$L = \{a_0 + a_1\alpha + a_2\alpha^2 \mid a_i \in \mathbb{Q}\}$$

ist.

4.2 Algebraische und transzendente Zahlen

Definition 4.2.1 Sei L/K eine Körpererweiterung. Ein Element $\alpha \in L$ heißt *algebraisch* über K, wenn ein von Null verschiedenes Polynom $f \in K[x]$ mit $f(\alpha) = 0$ 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. Sie heißt *rein transzendent*, wenn jedes Element $\alpha \in L \backslash K$ transzendent über K ist.

Beispiel 4.2.2 (a) Die reelle Zahl $\sqrt{2} \in \mathbb{R}$ ist algebraisch über $\mathbb{Q}$, da sie Nullstelle des Polynoms $x^2 - 2$ ist.

(b) Die reellen Zahlen $e = 2,71828\cdots$ und $\pi = 3,141592\cdots$ sind transzendent über $\mathbb{Q}$ (siehe [6, Kapitel 6]).

(c) Die komplexe Zahl $2\pi i \in \mathbb{C}$ ist transzendent über $\mathbb{Q}$ (das folgt aus (b)), aber algebraisch über $\mathbb{R}$.

(d) Aus den vorhergehenden Beispielen folgt: Die Körpererweiterung $\mathbb{R}/\mathbb{Q}$ ist weder algebraisch noch rein transzendent. Dagegen ist $\mathbb{C}/\mathbb{R}$ eine algebraische Erweiterung.

(e) Sei K ein beliebiger Körper und t eine Unbestimmte. Dann ist $K(t)/K$ eine rein transzendente Körpererweiterung (Übungsaufgabe).

Satz 4.2.3 *Sei L/K eine Körpererweiterung und $\alpha \in L$ ein Element aus L, welches algebraisch über K ist. Es existiert ein eindeutiges Polynom $f \in K[x]$, für das gilt:*

(a) f ist normiert und irreduzibel,

(b) $f(\alpha) = 0$.

Beweis: Die Menge

$$I := \{\, g \in K[x] \mid g(\alpha) = 0 \,\}$$

ist ein Ideal. Theorem 3.3.4 impliziert, dass I ein Hauptideal ist. Sei $f \in K[x]$ mit $I = (f)$. Wir dürfen annehmen, dass f normiert ist. Der Beweis von Theorem 3.3.4 zeigt, dass f das eindeutige normierte Polynom minimalen Grades in I ist.

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, so 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. □

Definition 4.2.4 Das Polynom f aus Satz 4.2.3 heißt das *Minimalpolynom* von α bezüglich des Körpers K. Notation: $f = \min_K(\alpha)$.

Das folgende Lemma gibt eine alternative Interpretation des Minimalpolynoms.

Lemma 4.2.5 *(a) Sei L/K eine Körpererweiterung und $\alpha \in L$ algebraisch über K. Sei $f = \min_K(\alpha)$ das Minimalpolynom von α über K. Die Abbildung*

$$K[x]/(f) \xrightarrow{\sim} K(\alpha)$$

ist ein Isomorphismus.

(b) Sei $f \in K[x]$ ein irreduzibles Polynom und sei $L = K[x]/(f)$. Das Polynom f besitzt in L mindestens eine Nullstelle.

Beweis: Sei $\varphi : K[x] \to K(\alpha)$, $g \mapsto g(\alpha)$ die natürliche Abbildung. Dies ist ein Ringhomomorphismus (Satz 3.2.3). Offensichtlich ist φ surjektiv. Satz 4.2.3 impliziert, dass $\ker(\varphi) = (f)$. Daher folgt die Aussage (a) aus Theorem 3.2.10.(b).

Teil (b) folgt direkt aus Satz 3.3.8. □

Mit Hilfe von Satz 3.3.8, gibt Lemma 4.2.5.(a) eine konkrete Beschreibung vom Körper $K(\alpha)$. Lemma 4.2.5.(b) sagt, dass jedes irreduzibles Polynom das Minimalpolynom eines Elements α in einem Erweiterungskörper ist.

Ist L/K eine Körpererweiterung, so können wir L als einen 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 4.2.6 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 $[L : K] < \infty$, d.h. wenn L als K-Vektorraum endlich erzeugt ist.

Beispiel 4.2.7 (a) Der Körper $\mathbb{C}$ ist eine endliche Körpererweiterung von $\mathbb{R}$. Es gilt:

$$[\mathbb{C} : \mathbb{R}] = 2,$$

da $(1, i)$ eine $\mathbb{R}$-Basis von $\mathbb{C}$ bildet.

(b) Sei ζ_3 eine primitiver 3te Einheitswurzel und $K = \mathbb{Q}(\zeta_3)$. Die Körpererweiterung $K/\mathbb{Q}$ hat Grad $[K : \mathbb{Q}] = 2$, da $(1, \zeta_3)$ eine $\mathbb{Q}$-Basis von K bildet (Beispiel 3.3.9).

Satz 4.2.8 *Sei $L = K(\alpha)$.*

(a) *Falls α transzendent über K ist, so ist $[K(\alpha) : K] = \infty$.*

(b) *Falls α algebraisch über K ist, so ist $[K(\alpha) : K] = \mathrm{Grad}(\min_K(\alpha))$.*

Beweis: Falls α transzendent über K ist, so sind $1, \alpha, \alpha^2, \ldots$ linear unabhängig über K. Dies impliziert (a).

Sei α algebraisch über K und sei $n = \mathrm{Grad}(\min_K(\alpha))$. Aus Lemma 4.2.5 und Satz 3.3.8.(a) folgt, dass $(1, \alpha, \ldots, \alpha^{n-1})$ eine Basis von $K(\alpha)$ als K-Vektorraum ist. Wir schließen, dass $[K(\alpha) : K] = n$ bildet. □

Beispiel 4.2.9 (a) Sei $d \in \mathbb{Z} \setminus \{0, \pm 1\}$ und sei $\alpha \in \mathbb{C}$ eine Quadratwurzel aus d, d.h. $\alpha^2 = d$. Das Minimalpolynom von α über $\mathbb{Q}$ ist $\min_{\mathbb{Q}}(\alpha) = x^2 - d$, da $\alpha \notin \mathbb{Q}$ ist. Wir schließen, dass $[\mathbb{Q}(\alpha) : \mathbb{Q}] = 2$. Satz 4.2.8 impliziert zusätzlich, dass $(1, \alpha)$ eine Basis von $\mathbb{Q}(\alpha)$ als $\mathbb{Q}$-Vektorraum bildet.

(b) Sei $\zeta_8 \in \mathbb{C}$ eine primitive 8te Einheitswurzel, z.B. $\zeta_8 = \cos(\pi/4) + i \sin(\pi/4)$. Wir bestimmen das Minimalpolynom $\min_{\mathbb{Q}}(\zeta_8)$. Offensichtlich ist $\min_{\mathbb{Q}}(\zeta_8)$ ein Teiler von $x^8 - 1 = (x^4 - 1)(x^4 + 1)$. Wir bemerken, dass $\zeta_8^4 = -1$ (am Einfachsten sieht man dies ein mit Hilfe von Polarkoordinaten). Also ist ζ_8 eine Nullstelle von $f(x) := x^4 + 1$. Wir behaupten, dass $\min_{\mathbb{Q}}(\zeta_8) = x^4 + 1$. Es reicht zu zeigen, dass $f(x)$ irreduzibel über $\mathbb{Q}$ ist.

Nehmen wir an $f(x)$ wäre reduzibel über $\mathbb{Q}$. Offensichtlich besitzt f keine Nullstellen in $\mathbb{Q}$, also keine linearen Faktoren (Lemma 3.4.1). Das Polynom f ist also in $\mathbb{Q}[x]$ das Produkt $f = f_1 \cdot f_2$ zweier Polynome 2ten Grades. Ohne Einschränkung dürfen wir annehmen, dass $f_i(x) = x^2 + a_i x + b_i$ normiert ist. Ausmultiplizieren liefert nun einen Widerspruch. Also ist $f(x)$ irreduzibel über $\mathbb{Q}$. Wir schließen, dass $[\mathbb{Q}(\zeta_8) : \mathbb{Q}] = 4$. Die Elemente $1, \zeta_8, \zeta_8^2, \zeta_8^3$ formen eine Basis von $\mathbb{Q}(\zeta_3)$ als $\mathbb{Q}$-Vektorraum. Konkret bedeutet dies, dass

$$\mathbb{Q}(\zeta_8) = \{a_0 + a_1\zeta_8 + a_2\zeta_8^2 + a_3\zeta_8^3 \mid a_i \in \mathbb{Q}\},$$

wobei $\zeta_8^4 = -1$ ist. Ein alternativer Beweis finden Sie in § 4.4.

Theorem 4.2.10 *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, also können

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. □

Bemerke, dass es im Beweis von Theorem 4.2.10 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.

Beispiel 4.2.11 Wir berechnen $[\mathbb{Q}(\sqrt{2}, i) : \mathbb{Q}]$, wobei $i^2 = -1$ ist. Theorem 4.2.10 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 4.2.9.(a) impliziert, dass $[\mathbb{Q}(\sqrt{2}) : \mathbb{Q}] = 2$. Außerdem folgt, dass $\min_{\mathbb{Q}(\sqrt{2})}(i)$ ein Teiler von $\min_{\mathbb{Q}}(i) = x^2 + 1$ ist. Es gilt, dass $\min_{\mathbb{Q}(\sqrt{2})}(i) = \min_{\mathbb{Q}}(i) = x^2 + 1$ genau dann, 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 3.4.1). Diese Bedingung ist erfüllt, da $\mathbb{Q}(i) \neq \mathbb{Q}(\sqrt{2})$ als Unterkörper von $\mathbb{C}$ ist. Wir schließen, dass $[\mathbb{Q}(\sqrt{2}, i) : \mathbb{Q}(\sqrt{2})] = 2$, und daher, dass $[\mathbb{Q}(\sqrt{2}, i) : \mathbb{Q}] = 2 \cdot 2 = 4$ ist. Der Beweis von Theorem 4.2.10 liefert uns außerdem, 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 4.2.9.(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. Da $[\mathbb{Q}(\zeta_8) : \mathbb{Q}] = [\mathbb{Q}(\sqrt{2}, i) : \mathbb{Q}] = 4$, schließen wir, dass $\mathbb{Q}(\sqrt{2}, i) = \mathbb{Q}(\zeta_8)$ ist.

4.3 Konstruktion mit Zirkel und Lineal

Plato (427 - 347 v. Chr.) behauptete, dass Gerade und Kreis die einzigen "perfekten" geometrischen Figuren sind. In der klassischen griechischen Geometrie führte dies dazu, dass man sich interessierte für Konstruktionen, 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: `http://www-history.mcs.st-and.ac.uk/Indexes/Greeks.html`

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 folgende 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 Abbilding 5).

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.

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 6):

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.

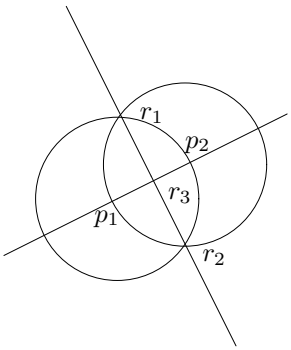


Abbildung 5: Konstruktion des Mittelpunktes

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.

Wir erklären nun, 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 Notation. 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.

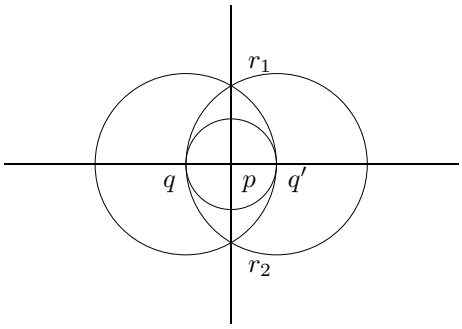
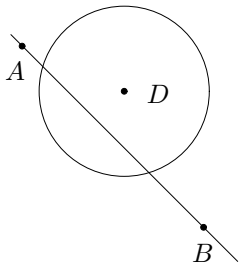


Abbildung 6: Konstruktion einer senkrechten Gerade

Wir gehen davon aus, dass der Kreis C und die Gerade L konstruiert sind mit Hilfe von Punkte aus K_{i-1}. Sei $D = (d_1, d_2)$ das Zentrum und w der Radius des Kreises C. Die Annahme, dass C und L mit Hilfe von Punkte 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:

$$\begin{aligned} L: &\quad y = a_2 + \frac{b_2 - a_2}{b_1 - a_1}(x - a_1), \\ C: &\quad (x - c_1)^2 + (y - c_2)^2 = w^2. \end{aligned} \tag{5}$$

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 (5) 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 4.2.10 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 $[K_{i-1}(x_i, y_i) : K_{i-1}(x_i)]$ ein Teiler von $[K_{i-1}(y_i) : K_{i-1}]$ 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 4.2.10. □

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 $M_0 = \{P, Q\}$, wobei P der Mittelpunkt des Kreises und Q 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 $M_0 = \{(0, 0), (1, 0)\}$ und $K_0 = \mathbb{Q}$ ist. Die Quadratur des Kreises bedeutet, ein Quadrat Q zu konstruieren mit gleichem Flächeninhalt wie der Kreis C, also mit Fläche π. Dies bedeutet, dass wir den Punkt $p := (\sqrt{\pi}, 0)$ konstruieren müssen.

Satz 4.3.3 impliziert, dass, falls p 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 $[\mathbb{Q}(\pi) : \mathbb{Q}(\sqrt{\pi})] = 2$, so 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 4.2.2). 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 $K_0 = \mathbb{Q}$. 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 4.1.4.(c) impliziert aber, dass $[\mathbb{Q}(\sqrt[3]{2}) : \mathbb{Q}] = 3$ ist. Also ist die Würfelverdopplung unmöglich. □

Das folgende Lemma ist nützlich, um zu zeigen, dass ein bestimmter Punkt konstruiert werden kann. Wir nehmen als Ausgangsmenge $M_0 = \{p := (0,0), q := (1,0)\}$. Mit Hilfe der Konstruktion von Beispiel 4.3.1.(b) können wir die Koordinatenachsen einzeichnen. Man überlegt sich, dass ein Punkt $p = (a,b)$ genau dann konstruiert werden kann, wenn die Punkte $(a,0)$ und $(0,b)$ konstruiert werden können. Um dies zu beweisen, muss man zeigen, dass gegeben eine Gerade L und einen Punkt $p \notin L$, so kann man eine Gerade durch P parallel an L konstruieren. Für Details verweisen wir auf [1, § 13.4].

Eine Zahl $a \in \mathbb{R}$ heißt *konstruierbar*, wenn der Betrag $|a|$ der Abstand zwischen zwei konstruierbaren Punkten ist. Die obige Bemerkung sagt daher, dass $p = (a,b)$ genau dann konstruierbar ist, wenn sowohl a also auch b konstruierbare Zahlen sind.

Lemma 4.3.6 *Sei $a \in \mathbb{R}$ eine positive konstruierbare Zahl. So ist auch die Zahl $\sqrt{a}$ konstruierbar.*

Beweis: Wir nehmen wieder als Ausgangsmenge $M_0 = \{p_0 := (0,0), p_1 := (1,0)\}$. Sei $a \in \mathbb{R}$ eine konstruierbare Zahl. Die Definition einer konstruierbaren Zahl impliziert, dass $q := (-a,0)$ konstruierbar ist. Wir machen die folgenden Konstruktionen (siehe Abbildung 7):

1. Sei r_1 der Mittelpunkt zwischen q und p_1 (Beispiel 4.3.1.(a)).
2. Sei C der Kreis mit Mittelpunkt r_1 und Radius $d(r_1, p_1)$.
3. Sei L die Gerade durch p_0 senkrecht zur Gerade durch p_0 und p_1 (Beispiel 4.3.1.(b)).
4. Sei r_2 der Schnittpunkt von C und L.

Der Kreis C erfüllt die Gleichung:

$$\left(x + \frac{a-1}{2}\right)^2 + y^2 = \left(\frac{1+a}{2}\right)^2.$$

Da $r_2 = (0,\gamma)$ auf C liegt, folgt, dass

$$\gamma^2 = \left(\frac{1+a}{2}\right)^2 - \left(\frac{a-1}{2}\right)^2 = a.$$

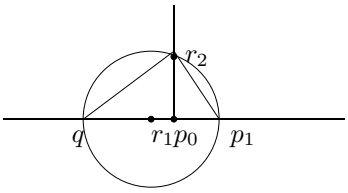


Abbildung 7: Konstruktion einer Quadratwurzel

Also ist $\gamma = d(p_0, r_2) = \sqrt{a}$. Hieraus folgt, dass $\sqrt{a}$ eine konstruierbare Zahl ist.

Alternativ kann man auch mit Hilfe des Satzes von Pythagoras zeigen, dass das Dreieck q, r_2, p_1 rechtwinklig ist. Hieraus folgert man, dass die Dreiecke q, r_2, p_0 und p_0, r_2, p_1 kongruent sind. Das Verhältnis ist $\sqrt{a}$. □

4.4 Die Kreisteilungkörper

Als Beispiel einer Körpererweiterung betrachten wir in diesem Abschnitt die sogenannten *Kreisteilungskörper*.

Sei $\mu_n \subset \mathbb{C}^*$ die Untergruppe der n-ten Einheitswurzeln. Wir haben gesehen, dass μ_n mit Multiplikation als Verknüpfung eine zyklische Gruppe ist (Beispiel 1.3.10.(b)). Die komplexe Zahl $\zeta_n := \cos(2\pi/n) + i\sin(2\pi/n)$ ist ein Erzeuger dieser Gruppe. Die Ordnung von $\zeta_n^i \in \mu_n$ ist genau dann n, wenn $\mathrm{ggT}(i, n) = 1$ ist. Die Elemente von μ_n der Ordnung n sind die *primitiven Einheitswurzel*. Die Anzahl der primitiven n-ten Einheitswurzel ist

$$\varphi(n) = |(\mathbb{Z}/n\mathbb{Z})^*| = |\{0 < i < n \mid \mathrm{ggT}(i, n) = 1\}|,$$

wobei φ die eulersche φ-Funktion ist, siehe Beispiel 1.6.11.

Die Körper $K_n := \mathbb{Q}(\zeta_n)$ heißen *Kreisteilungskörper*. Wir bestimmen das Minimalpolynom von ζ_n über $\mathbb{Q}$. Dazu definieren wir das n-te *Kreisteilungspolynom*

$$\Phi_n(x) = \prod_{i \in (\mathbb{Z}/n\mathbb{Z})^\times} (x - \zeta_n^i).$$

Wir werden zeigen, dass $\Phi_n = \min_{\mathbb{Q}}(\zeta_n)$ ist. Zunächst ist $\Phi_n(x)$ ein Polynom mit Koeffizienten in $\mathbb{C}$. Das folgende Lemma zeigt, dass $\Phi_n(x) \in \mathbb{Z}[x]$ ist.

Lemma 4.4.1 *(a) Es gilt:* $x^n - 1 = \prod_{d|n} \Phi_d$.

(b) Für alle $n \geq 1$ *ist* $\Phi_n(x)$ *ein normiertes Polynom mit ganzzahligen Koeffizienten.*

Beweis: Wir bemerken zuerst, dass

$$x^n - 1 = \prod_{i=0}^{n-1} (x - \zeta_n^i) \in \mathbb{C}[x].$$

Falls $d \mid n$, so gilt, dass jede d-te Einheitswurzel auch ein n-te Einheitswurzel ist. Insbesondere gilt $\zeta_d = \zeta_n^{n/d}$. Teil (a) folgt hieraus.

Die Formel (a) impliziert, dass man Φ_n recursiv berechnen kann, indem man $x^n - 1$ durch alle Φ_d mit $d \mid n$ und $d < n$ teilt.

Die Polynome $x^n - 1$ und $\Phi_1(x) = x - 1$ sind normiert und besitzen ganzzahlige Koeffizienten. Division mit Rest in $\mathbb{Z}[x]$ impliziert daher, dass $(x^n - 1)/(x - 1)$ auch normiert ist und ganze Koeffizienten besitzt (Satz 3.3.1). Mit Induktion folgt, dass alle Φ_n diese Eigenschaften besitzen. □

Beispiel 4.4.2 (a) Sei p eine Primzahl. Lemma 4.4.1.(a) impliziert, dass

$$\Phi_p(x) = \frac{x^p - 1}{x - 1} = x^{p-1} + x^{p-2} + \cdots + 1.$$

(b) Für $n \leq 10$ zusammengesetzt finden wir mit dem rekursiven Verfahren aus dem Beweis von Lemma 4.4.1:

n	Φ_n
4	$x^2 + 1$
6	$x^2 - x + 1$
8	$x^4 + 1$
9	$x^6 + x^3 + 1$
10	$x^4 - x^3 + x^2 - x + 1$

Folgendes Lemma benötigen wir im Beweis von Satz 4.4.4.

Lemma 4.4.3 *Sei p eine Primzahl.*

(a) Für $i = 1, \ldots, p-1$ gilt, dass $p \mid \binom{p}{i}$.

(b) Sei $k = \mathbb{F}_p$. Für alle $\alpha, \beta \in k$ gilt, dass

$$(\alpha + \beta)^p = \alpha^p + \beta^p.$$

Allgemeiner gilt Lemma 4.4.3.(b) für alle Körper der Charakteristik p. Dies sind Körper in dem $p = 0$ gilt (siehe § 4.5).

Beweis: Teil (a) folgt unmittelbar aus der Definition des Bimonialkoeffizientes. Teil (b) folgt aus (a) und der binomischer Lehrsatz. □

Satz 4.4.4 *Das Kreisteilungspolynom Φ_n ist irreduzibel über $\mathbb{Q}$. Insbesondere ist Φ_n das Minimalpolynom von ζ_n über $\mathbb{Q}$.*

Beweis: Wir geben zuerst ein Beweis für den Fall, dass $n = p$ eine Primzahl ist. Es gilt, dass $\Phi_p(x) = \sum_{i=0}^{p-1} x^i$ (Beispiel 4.4.2.(a)). Wir definieren $f(x) := \Phi_p(x + 1)$. Aus der Identität $\Phi_p(x) = (x^p - 1)/(x - 1)$ folgt

$$f(x) = \frac{(x+1)^p - 1}{x} = \sum_{i=1}^{p} \binom{p}{i} x^{i-1}.$$

Die Binomialkoeffizienten $\binom{p}{i}$ sind durch p teilbar für $i = 1, \ldots, p-1$ (Lemma 4.4.3.(a)). Außerdem gilt $p^2 \nmid \binom{p}{1} = p$. Aus dem Eisenstein-Kriterium (Theorem 3.4.4) folgt daher, dass f und also auch Φ_p irreduzibel ist.

Wir geben nun einen zweiten Beweis, das für alle n funktioniert. Der Beweis geht zurück auf Dedekind. Sei $f = \min_{\mathbb{Q}}(\zeta_n)$. Da $\Phi_n(\zeta_n) = 0$ ist, ist f ein Teiler von Φ_n. Um zu zeigen, dass $\Phi_n = f$, reicht es zu zeigen, dass $f(\zeta_n^i) = 0$ für alle i mit $\mathrm{ggT}(i, n) = 1$. Da jedes solches i sich schreiben lässt als Produkt von Primzahlen, reicht es, dies für Primzahlen p mit $\mathrm{ggT}(i, p) = 1$ zu zeigen.

Wir schreiben $\Phi_n = f \cdot g$ mit $f, g \in \mathbb{Z}[x]$ (Satz 3.3.1). Da Φ_n und f normiert sind, ist g auch normiert. Sei p eine Primzahl teilerfremd zu n. Wir nehmen an, dass $f(\zeta_n^p) \neq 0$. Es gilt also, dass $g(\zeta_n^p) = 0$. Es folgt, dass ζ_n eine Nullstelle von $g(x^p)$ ist. Da $f = \min_{\mathbb{Q}}(\zeta_n)$ ist, folgt, dass $f(x)$ ein Teiler von $g(x^p)$ ist.

Es gilt, dass $g(x^p) \equiv g(x)^p \pmod{p}$. Dies ist eine Verallgemeinerung von Lemma 4.4.3.(b). Wir überlassen dies dem Leser/der Leserin als Übungsaufgabe.

Wir schreiben $\bar{\Phi}_n, \bar{f}, \bar{g}$ für die Reduktion von Φ_n, f, g modulo p. Da $f(x) \mid g(x^p)$, so folgt, dass

$$\bar{f}(x) \mid \bar{g}(x^p) \equiv [\bar{g}(x)]^p \pmod{p}.$$

Also folgt, dass $\bar{f}^2$ ein Teiler von $\bar{\Phi}_n$ ist. Insbesondere besitzt $\bar{\Phi}_n$ doppelte Nullstellen. Wir erinnern uns, dass $\bar{\Phi}_n$ ein Teiler von $x^n - 1$ ist. Die formale Ableitung von $(x^n - 1) \in \mathbb{F}_p[x]$ ist $[n]x^{n-1} \in \mathbb{F}_p[x]$. Da $p \nmid n$, so besitzen $x^n - 1$ und seine formale Ableitung keine gemeinsame Nullstellen in $\mathbb{F}_p$. Dies widerspricht Lemma 3.4.7. Wir schließen, dass $f(\zeta_n^p) = 0$. Hieraus folgt, dass $f = \Phi_n$, also, dass Φ_n irreduzibel ist. □

4.5 Endliche Körper

Für jeden Ring R definiert

$$\psi : \mathbb{Z} \to R, \qquad n \mapsto n \cdot 1 \tag{6}$$

einen Ringhomomorphismus, wobei für $n > 0$ positiv $n \cdot 1 = 1 + \cdots + 1$ (n-mal) und $(-n) \cdot 1 = -(n \cdot 1)$ ist. Satz 3.2.9 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 $\mathrm{Char}(R) = m \neq 0$, so ist m die kleinste positive Zahl, sodass $m \cdot 1 = 0$ in R gilt. Falls $R \neq \{0\}$, ist $1 \neq 0$ in R. In diesem Fall ist $\mathrm{Char}(R) \neq 1$.

Lemma 4.5.1 *Die Charakteristik* $\mathrm{Char}(K)$ *eines Körpers* K *ist entweder* 0 *oder eine Primzahl.*

Beweis: Sei $\psi : \mathbb{Z} \to K$ wie in (6) 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 (siehe auch Beispiel 3.1.5.(a)). Das Lemma folgt. □

Sei K ein Körper der Charakteristik 0. Die Abbildung $\psi : \mathbb{Z} \to K$ ist also injektiv. Hieraus folgt, dass $\mathbb{Q}$ ein Teilkörper von K ist. Falls K ein Körper der Charakteristik $p > 0$ ist, so folgt aus dem ersten Isomorphiesatz (Theorem 3.2.10.(c)), dass $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$ ein Teilkörper von K ist.

Der kleinste Teilkörper eines Körpers K heißt *Primkörper*. Die obige Bemerkung sagt, dass $\mathrm{Char}(K) = 0$ genau dann, wenn $\mathbb{Q}$ der Primkörper von K ist. Ebenso gilt, dass $\mathrm{Char}(K) = p$ genau dann, wenn $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$ der Primkörper von K ist.

In diesem Abschnitt bestimmen wir alle Körper mit endlich vielen Elementen. Solche Körper nennen wir *endliche Körper*.

Lemma 4.5.2 *Sei F ein endlicher Körper. Insbesondere ist $\mathrm{Char}(F) = p > 0$. 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 endlichen Grad. Sei $n = [F : \mathbb{F}_p]$ die Grad der Körpererweiterung. Dies bedeutet, dass die Kardinalität einer Basis $(\alpha_1 = 1, \alpha_2, \ldots, \alpha_n)$ von F als $\mathbb{F}_p$-Vektorraum n ist. Jedes Element x von F lässt sich also 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 4.5.4). Außerdem zeigen wir, dass zwei endliche Körper mit gleichen Kardinalität isomorph sind (Theorem 4.5.10). Dieser Körper mit q Elementen werden wir häufig mit $\mathbb{F}_q$ bezeichnen.

Beispiel 4.5.3 Wir konstruieren einen Körper $\mathbb{F}_4$ mit 4 Elementen. Man überprüft, dass genau ein irreduzibles Polynom $f(x) \in \mathbb{F}_2[x]$ von Grad 2 existiert: Nämlich $f(x) = x^2 + x + 1$. 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.

Theorem 4.5.4 *Sei $q = p^n$ eine Primzahlpotenz.*

(a) Es existiert ein Körper k mit q Elementen.

(b) Die Elemente von k sind Nullstellen des Polynoms $f_q(x) := x^q - x$. Dieses Polynom zerfällt in Linearfaktoren über k.

Beweis: Wir beweisen zuerst (b). Sei k ein Körper mit q Elementen. Die multiplikative Gruppe $k^\times = k \setminus \{0\}$ enthält $q-1$ Elemente. Die Ordnung eines Elementes $\alpha \in k^\times$ ist also ein Teiler von $q-1$ (Satz 1.6.10). Insbesondere ist α eine Nullstelle von $x^{q-1}-1$, also auch von $f_q = x^q - x$. Das Element $0 \in k$ ist auch eine Nullstelle dieses Polynoms. Das Polynom f_q besitzt also q verschiedene Nullstellen in k. Wir schließen, dass f_q über k in Linearfaktoren zerfällt:

$$f_q(x) = \prod_{\alpha \in k} (x - \alpha).$$

Wir beweisen nun die Existenz eines Körpers k mit q Elementen. Teil (b) impliziert, dass die Elemente von k genau die Nullstellen von f_q sind.

Wir behaupten, dass eine Körpererweiterung L von $\mathbb{F}_p$, in dem f_q in Linearfaktoren zerfällt, existiert. Sei $g_1 \in \mathbb{F}_p[x]$ ein irreduzibler Faktor von f_q von Grad echt größer als 1. In der Körpererweiterung $L_1 := \mathbb{F}_p[x]/(g_1)$ besitzt g_1 eine Nullstelle. Mit Induktion folgt nun die Existenz eine Körpererweiterung, in der f_q in Linearfaktoren zerfällt. (Siehe auch § 5.3 oder [4, Satz 5.4.4].)

Wir behaupten, dass g keine mehrfache Nullstellen in L besitzt. Da $q = p^n \equiv 0 \in \mathbb{F}_p$ gilt, dass $g'(x) = qx^{q-1} - 1 \equiv -1 \in \mathbb{F}_p[x]$. Also gilt, dass $\mathrm{ggT}(g, g') = 1$ ist. Lemma 3.4.7 impliziert, dass g keine mehrfache Nullstellen besitzt. Insbesondere besitzt g genau q Nullstellen in L.

Sei $F \subset L$ die Menge der Nullstellen von g. Wir behaupten, dass F ein Körper ist. Die Definition der Menge F impliziert, dass $\alpha \in F$ genau dann, wenn $\alpha^q = \alpha$ ist. Seien nun $\alpha, \beta \in F$. Es 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 4.4.3.(b), 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 4.5.5 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`:

$$x^q - x = x(x-1)(x+1)(x^2+1)(x^2-x-1)(x^2+x-1).$$

Um den Körper mit 9 Elementen darzustellen, wählen wir einen der irreduziblen Faktoren von g von Grad 2, zum Beispiel $h(x) = x^2 + 1$. 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. Also ist $\alpha \in \mathbb{F}_9$ eine Nullstelle des Polynoms $x^2 + 1$.

Der Beweis von Theorem 4.5.4 impliziert, dass $x^q - x$ über $\mathbb{F}_9$ in Linearfaktoren zerfällt. Wir rechnen dies nach. Wir suchen dazu die Nullstellen von x^2+1, x^2-x-1 und x^2+x-1 in $\mathbb{F}_9$:

$$x^2+1 = (x+\alpha)(x-\alpha), \qquad x^2-x-1 = (x+\alpha+1)(x-\alpha+1),$$
$$x^2+x-1 = (x-\alpha-1)(x+\alpha-1).$$

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 (§ 4.4).

Satz 4.5.6 *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 $H \subset K^\times$ eine Untergruppe der Ordnung n. Die Ordnung eines Elements $\alpha \in H$ ist ein Teiler von n (Satz 1.6.10), also ist α eine Nullstelle des Polynoms $x^n - 1$. Satz 3.4.8 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 4.5.6:

Korollar 4.5.7 *Sei k ein Körper mit $q = p^n$ Elementen. Die Gruppe k^* ist zyklisch.*

Bemerkung 4.5.8 Sei $k = \mathbb{F}_q$ ein Körper mit $q = p^n$ Elemente. Es existiert ein Element $\alpha \in k$ der Ordnung $q-1$ (Korollar 4.5.7). Dies bedeutet, dass jedes Element in k^* eine Potenz von α ist: $k^* = \{\alpha, \alpha^2, \ldots, \alpha^{q-1} = 1\}$.

Falls $q = p$ eine Primzahl ist, heißt ein Element α der Ordnung $p-1$ eine *Primitivwurzel* modulo p. Korollar 4.5.7 sagt uns nicht, wie man eine Primitivwurzel effizient findet. Eine Möglichkeit eine Primitivwurzel zu bestimmen, ist die Ordnung von Elemente in $\mathbb{Z}/p\mathbb{Z}^*$ zu berechnen bis wir einen Element der Ordnung $p-1$ gefunden haben. Falls p groß ist, ist dies nicht sehr effizient. Siehe auch [4, § 6.1].

Beispiel 4.5.9 (a) Sei $\alpha \in \mathbb{F}_9$ ein Element mit $\alpha^2 = -1$ (siehe Beispiel 4.5.5). Da $\alpha^4 = 1$ ist, folgt, dass $\mathrm{ord}(\alpha) = 4$ ist. Ein Element der Ordnung 8 in $\mathbb{F}_9^\times$ ist zum Beispiel $\beta := \alpha - 1$. Wir haben gesehen, dass β eine Nullstelle von $x^2 - x - 1$ ist.

(b) Sei $\alpha \in \mathbb{F}_4^\times$ eine Nullstelle von $x^2 + x + 1$ (Beispiel 4.5.3). Die Ordnung von α ist 3.

Theorem 4.5.10 *Sei $q = p^n$ eine Primzahlpotenz und seien k, k' zwei Körper mit q Elementen. Die Körper k und k' sind isomorph.*

Beweis: Seien k, k' zwei Körper mit q Elemente und sei α ein Erzeuger der zyklischen Gruppe k^*. Der Körper $\mathbb{F}_p(\alpha)$ enthält auf jeden Fall die q Elemente $0, \alpha, \alpha^2, \ldots, \alpha^{q-1}$. Also gilt $k = \mathbb{F}_p(\alpha)$.

Sei $f(x) = \min_{\mathbb{F}_p}(\alpha)$, also $k = \mathbb{F}_p[x]/(f)$. Da α auch eine Nullstelle des Polynoms $f_q(x) = x^q - x$ ist, folgt aus Satz 4.2.3, dass $f \mid f_q$.

Das Polynom $f_q(x)$ zerfält auch in k' in Linearfaktoren (Theorem 4.5.4.(b)). Insbesondere besitzt f eine Nullstelle $\alpha' \in k'$. Es folgt, dass $k \simeq \mathbb{F}_p[x]/(f) \simeq \mathbb{F}_p(\alpha') \subset k'$. Da k und k' die gleiche Kardinalität haben, folgt $k' \simeq k$. □

5 Galois-Theorie

5.1 Einführung

Die Galois-Theorie ist entstanden aus der Frage nach der Lösbarkeit von Polynomgleichungen

$$f(x) = a_n x^n + a_{n-1} x^{n-1} + \cdots + a_0 = 0, \qquad a_i \in \mathbb{Z}$$

mit Hilfe von Radikalen. Grob gesagt, ist $f(x) = 0$ auflösbar mir Hilfe von Radikalen, wenn man die Nullstellen der Gleichung mit Hilfe der Operationen Addition, Multiplikation und ziehen k-ter Wurzeln aus den Koeffizienten a_i berechnen kann. Die bekannte *Mitternachtsformel* sagt, dass die Nullstellen eines Polynoms $ax^2 + bx + c = 0$ von Grad 2 gegeben sind durch

$$x = \frac{-b}{2a} \pm \frac{1}{2a}\sqrt{b^2 - 4ac}.$$

Also sind Gleichungen zweiter Ordnung mit Hilfe von Radikalen auflösbar. Im Prinzip wussten babylonische Mathematiker schon 400 v.Chr. wie man quadratische Gleichungen löst, obwohl der Begriff einer *Gleichung* noch nicht bekannt war.

Der Beweis, dass kubische Gleichungen mit Hilfe von Radikale auflösbar sind, ist von Scipione dal Ferro um 1515. Wahrscheinlich konnte er nur Gleichungen von der Form $x^3 + ax = b$ mit $a, b > 0$ auflösen. Man kann aber zeigen, dass

man den allgemeinen Fall auf diesen Spezialfall zurückführen kann. Die Formel für die (eindeutige reelle) Nullstelle lautet in dem Spezialfall:

$$x = \sqrt[3]{\frac{b}{2} + \sqrt{\left(\frac{b}{2}\right)^2 + \left(\frac{a}{3}\right)^3}} + \sqrt[3]{\frac{b}{2} - \sqrt{\left(\frac{b}{2}\right)^2 + \left(\frac{a}{3}\right)^3}}.$$

In 1540 gelangte Ludovico Ferrarri den Beweis der Lösbarkeit von Gleichungen von Grad 4. Für die faszinierende Geschichte, siehe [3, Einführung] und
`www-history.mcs.st-and.ac.uk/HistTopics/Quadratic_etc_equations.html`

Der erste Mathematiker, der behauptete, dass man die "allgemeine" Gleichung 5-ten Grades nicht mit Hilfe von Radikale auflösen kann, war Paolo Ruffini (1799). Sein Beweis, der einige Lücken enthält, beruht auf der Theorie der Permutationsgruppen (§ 1.4). Eine allgemeine Definition einer Gruppe gab es zu dieser Zeit noch nicht. Der erste vollständige Beweis ist von Niels Abel (1824). Die Charakterisierung alle Gleichungen deren Nullstellen mit Hilfe von Radikalen auflösbar sind, gelang letztendlich Evariste Galois in 1831. Seine Ergebnisse wurde in 1846, erst lange nach Galois' Tod, von Liouville publiziert. Mehr über das kurze aber ungewöhnliche Leben von Galois lesen Sie auf der MacTutor-Webseite
`http://www-history.mcs.st-andrews.ac.uk/Biographies/Galois.html`
Galois' Ergebnisse zu verstehen ist das Ziel dieses Kapitels.

Wir skizzieren nun kurz die Idee der Galois-Theorie. Sei K ein Körper, zum Beispiel $K = \mathbb{Q}$. Sei $f(x) \in K[x]$ ein Polynom von Grad n. Einfachheitshalber nehmen wir an, dass f irreduzibel über K ist. In der Galois-Theorie studiert man die Menge aller Nullstellen von $f(x) = 0$ in einem Körper der groß genug ist (z.B. $\mathbb{C}$) und die Symmetrien zwischen diesen Nullstellen.

Als Beispiel betrachten wir $f(x) = x^2 + 1 \in \mathbb{R}[x]$. Das Polynom zerfällt in Linearfaktoren über $\mathbb{C} \simeq \mathbb{R}[x]/(x^2 + 1)$. Es gilt: $x^2 + 1 = (x - i)(x + i)$. Die Nullstellen $\pm i$ spielen die gleiche Rolle: Man kann sie nicht auseinander halten. Die komplexe Konjugation $\iota : z = a + bi \mapsto a - bi$ vertauscht die beiden Nullstellen und lässt die reellen Zahlen fest (Beispiel 5.2.3).

Sei nun wieder $f(x) \in K[x]$ ein beliebiges Polynom. Einfachheitshalber nehmen wir in der Einleitung an, dass $\mathrm{Char}(K) = 0$. Wir werden sehen, dass eine kleinste Körpererweiterung L/K existiert, sodass $f \in L[x]$ in Linearfaktoren zerfällt. Dieser Körper heißt *Zerfällungskörper*. Um zu bestimmen ob die Gleichung $f(x) = 0$ durch Radikale auflösbar ist, brauchen wir ein "Maß" für die Komplexität der Körpererweiterung L/K. Hierzu benutzen wir die Gruppen-Theorie.

Die *Galois-Gruppe* $\mathrm{Gal}(L/K)$ der Erweiterung L/K ist die Menge der Körperisomorphismen $L \to L$, welche eingeschränkt auf K trivial sind. Die Elemente von $\mathrm{Gal}(L/K)$ vertauschen die Nullstellen des Polynoms f, also kann man $\mathrm{Gal}(L/K)$ als Symmetriegruppe der Nullstellen betrachten. Ziel der Galois-Theorie ist es nun, eine Beziehung zwischen den Eigenschaften der Körpererweiterung L/K und die Eigenschaften der Galois-Gruppe $\mathrm{Gal}(L/K)$ herzustellen. Genauer stellt der Hauptsatz der Galois-Theorie eine Beziehung her

zwischen Teilerweiterungen von L/K und Untergruppen von $\mathrm{Gal}(L/K)$. Hieraus kann man zum Beispiel ableiten, ob eine Gleichung $f(x) = 0$ mittels Radikalen auflösbar ist oder nicht.

Teilen dieses Kapitels sind übernommen aus [7]

5.2 Körpererweiterungen und Automorphismen

Definition 5.2.1 Sei L/K eine Körpererweiterung. Ein *K-Automorphismus* von L ist ein Körperisomorphismus $\alpha : L \to L$ mit $\alpha(c) = c$ für alle $c \in K$. Die Menge aller K-Automorphismen von L bezeichnen wir mit $\mathrm{Aut}_K(L)$.

Lemma 5.2.2 *Für jede Körpererweiterung L/K ist $\mathrm{Aut}_K(L)$ eine Gruppe.*

Beweis: Seien $\alpha, \beta \in \mathrm{Aut}_K(L)$. Offensichtlich sind $\alpha \circ \beta$ und β^{-1} wieder K-Isomorphismen von L. Die Komposition von Funktionen ist immer assoziativ, also ist $\mathrm{Aut}_K(L)$ eine Gruppe. □

Beispiel 5.2.3 (a) Wir betrachten die Körpererweiterung $\mathbb{C}/\mathbb{R}$. Die komplexe Konjugation $\iota : \mathbb{C} \to \mathbb{C}$, $z = a + bi \mapsto a - bi$ ist ein $\mathbb{R}$-Automorphismus von $\mathbb{C}$. Wir behaupten, dass $\mathrm{Aut}_{\mathbb{R}}(\mathbb{C}) = \{\mathrm{Id}, \iota\}$. Sei dazu $\alpha \in \mathrm{Aut}_{\mathbb{R}}(\mathbb{C})$ beliebig, und sei $j := \alpha(i)$. Da $i^2 = -1 \in \mathbb{R}$, gilt $j^2 = \alpha(i)^2 = \alpha(i^2) = \alpha(-1) = -1$. Wir schließen, dass $j = \pm i$.

Jeder $\mathbb{R}$-Automorphismus von $\mathbb{C}$ ist insbesondere auch ein $\mathbb{R}$-lineare Abbildung von $\mathbb{C} \to \mathbb{C}$. Also ist $\alpha \in \mathrm{Aut}_{\mathbb{R}}(\mathbb{C})$ bestimmt durch die Bilder einer Basis von $\mathbb{C}$ als $\mathbb{R}$-Vektorraum, zum Beispiel $\{1, i\}$. Da $1 \in \mathbb{R}$, gilt $\alpha(1) = 1$. Also wird α bestimmt durch $\alpha(i)$. Dies impliziert, dass $\mathrm{Aut}_{\mathbb{R}}(\mathbb{C}) = \{\mathrm{Id}, \iota\}$ ist.

(b) Sei $\alpha = \sqrt[3]{2} \in \mathbb{R}$ eine reelle 3-te Wurzel aus 2 und $K = \mathbb{Q}(\alpha) \subset \mathbb{Q}$. Sei $g \in \mathrm{Aut}_{\mathbb{Q}}(K)$. Es gilt, dass

$$g(\alpha)^3 = g(\alpha^3) = g(2) = 2.$$

Aber α ist die einzige reelle Lösung der Gleichung $x^3 = 2$, also auch die einzige Lösung dieser Gleichung in K. Wir schließen, dass $g(\alpha) = \alpha$ und daher, dass $g = \mathrm{Id}$.

Das folgende Lemma ist eine Verallgemeinerung von Beispiel 5.2.3.

Lemma 5.2.4 *Sei $f \in K[x]$ und $\varphi \in \mathrm{Aut}_K(L)$. Falls $\alpha \in L$ eine Nullstelle von f ist, so ist auch $\varphi(\alpha)$ eine Nullstelle von f.*

Beweis: Sei $f(x) = \sum_{i=0}^{n} a_i x^i \in K[x]$ und sei $\alpha \in L$ eine Nullstelle von f. Für $\varphi \in \mathrm{Aut}_K(L)$ gilt, dass $f(\varphi(\alpha)) = \sum_{i=0}^{n} a_i \varphi(\alpha)^i = \varphi(f(\alpha))$, da $a_i \in K$ ist. Wir schließen, dass $\varphi(\alpha)$ auch eine Nullstelle von f ist. □

Satz 5.2.5 *Sei $\mathbb{Q}(\zeta_n)$ der n-te Kreisteilungskörper. Es gilt, dass*

$$\mathrm{Aut}_{\mathbb{Q}}(\mathbb{Q}(\zeta_n)) \simeq (\mathbb{Z}/n\mathbb{Z})^*.$$

Beweis: Sei $\varphi \in \mathrm{Aut}_{\mathbb{Q}}(\mathbb{Q}(\zeta_n))$. Sei m ein Teiler von n. Lemma 5.2.4 impliziert, dass φ die m-te Einheitswurzeln permutiert. Mit Induktion folgt, dass $\varphi(\zeta_n)$ auch eine primitive n-te Einheitswurzel ist. Wir schreiben $\varphi(\zeta_n) = \zeta_n^i$ mit $\mathrm{ggT}(i, n) = 1$. Dies definiert eine Abbildung

$$\Phi : \mathrm{Aut}_{\mathbb{Q}}(\mathbb{Q}(\zeta_n)) \to (\mathbb{Z}/n\mathbb{Z})^*, \quad \varphi \mapsto i.$$

Da φ ein Körperisomorphismus ist, ist φ eindeutig bestimmt ist durch das Bild von ζ_n. Dies impliziert, dass die Abbildung Φ bijektiv ist.

Wir überprüfen, dass Φ ein Gruppenhomomorphismus ist. Sei $\varphi_i \in \mathrm{Aut}_{\mathbb{Q}}(\mathbb{Q}(\zeta_n))$ bestimmt durch $\varphi_i(\zeta_n) = \zeta_n^i$. Es gilt, dass

$$\varphi_i \circ \varphi_j(\zeta_n) = \varphi_i(\zeta_n^j) = \varphi_i(\zeta_n)^j = \zeta_n^{ij}.$$

Dies impliziert, dass $\Phi(\varphi_i \circ \varphi_j) = ij = \Phi(\varphi_i)\Phi(\varphi_j)$. Also ist Φ ein Gruppenhomomorphismus. □

Der Hauptsatz der Galois-Theorie (Theorem 5.7.1) gibt für *bestimmte Körpererweiterung* L/K eine Korrespondenz zwischen

(1) Teilerweiterungen von L/K,

(2) Untergruppen von $\mathrm{Aut}_K(L)$.

Als erste Schritt im Verständniss dieser Korrespondenz erklären wir, wie man zu einer Untergruppe $H \subset \mathrm{Aut}_K(L)$ eine Teilerweiterung M von L/K assoziieren kann.

Lemma 5.2.6 *Sei L/K eine endliche Körpererweiterung und $H \subset \mathrm{Aut}_K(L)$ eine Untergruppe. Die Menge*

$$M := L^H = \{x \in L \mid \varphi(x) = x \text{ für alle } \varphi \in H\}.$$

ist eine Teilerweiterung von L/K.

Der Körper M heißt Fixkörper von H.

Beweis: Seien $x, y \in M$ und $\varphi \in H$. Es gilt $\varphi(x + y) = \varphi(x) + \varphi(y) = x + y$, also ist M abgeschlossen gegenüber die Addition. Ähnlich überprüft man, dass M auch abgeschlossen gegenüber den anderen Körperoperationen ist. Wir schließen, dass M ein Körper ist. Da $H \subset \mathrm{Aut}_K(L)$ ist, folgt, dass $K \subset M$ ist. □

Beispiel 5.2.7 Sei $\zeta = \zeta_8$ eine primitive 8-te Einheitswurzel. Wir haben gesehen, dass $\mathrm{Aut}_{\mathbb{Q}}(\mathbb{Q}(\zeta_8)) \simeq (\mathbb{Z}/8\mathbb{Z})^* = \{[1], [3], [5], [7]\}$ ist (Satz 5.2.5).

Man überprüft, dass alle Elemente $g \in (\mathbb{Z}/8\mathbb{Z})^* \setminus \{1\}$ Ordnung 2 haben. Also ist $(\mathbb{Z}/8\mathbb{Z})^* \simeq \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ (Korollar 1.6.13). Wir berechnen die Fixkörper der Untergruppen von $(\mathbb{Z}/8\mathbb{Z})^*$ der Ordnung 2.

Sei $H_1 = \langle [7] \rangle \subset (\mathbb{Z}/8\mathbb{Z})^*$. Dies ist eine Untergruppe mit zwei Elementen. Wir haben gesehen, dass man jedes Element $x \in \mathbb{Q}(\zeta_8)$ als

$$x = a_0 + a_1\zeta_8 + a_2\zeta_8^2 + a_3\zeta_8^3, \qquad a_i \in \mathbb{Q}$$

darstellen kann (Beispiel 4.2.9.(b)). Das Element $[7] \in H_1$ korrespondiert zum Körperisomorphismus bestimmt von $\varphi_7(\zeta_8) = \zeta_8^7$ (siehe den Beweis von Satz 5.2.5). Ein Element $x = \sum_{i=0}^3 a_i\zeta_8^i \in \mathbb{Q}(\zeta_8)$ wird genau dann von φ_7 fixiert, wenn

$$x = \varphi_7(x) = \sum_{i=0}^{3} a_i\zeta_8^i = a_0 - a_1\zeta_8^3 - a_2\zeta_8^2 - a_3\zeta_8.$$

Hier haben wir benutzt, dass $\zeta_8^4 = -1$ ist (Beispiel 4.2.9.(b)). Wir schließen, dass $\varphi_7(x) = x$ genau dann gilt, wenn $a_1 = -a_3$ und $a_2 = 0$ ist. Da $-\zeta_*^3 = \zeta_8^7 = \zeta_8^{-1}$, impliziert dies, dass

$$\mathbb{Q}(\zeta_8)^{H_1} = \mathbb{Q}(\zeta_8 + \zeta_8^{-1}).$$

Sei $H_2 = \langle [3] \rangle \subset (\mathbb{Z}/8\mathbb{Z})^*$ und sei $\varphi_3(\zeta_8) = \zeta_8^3$ der zu [3] gehörige Automorphismus von $\mathbb{Q}(\zeta_8)$. Wie oben überprüft man, dass $x = a_0 + a_1\zeta_8 + a_2\zeta_8^2 + a_3\zeta_8^3$ genau dann von φ_3 festgelassen wird, wenn $a_1 = a_3$ und $a_2 = 0$. Wir schließen, dass

$$\mathbb{Q}(\zeta_8)^{H_2} = \mathbb{Q}(\zeta_8 + \zeta_8^3).$$

Sei $H_3 = \langle [5] \rangle \subset (\mathbb{Z}/8\mathbb{Z})^*$. Ähnlich überprüft man, dass

$$\mathbb{Q}(\zeta_8)^{H_3} = \mathbb{Q}(\zeta_8 + \zeta_8^5).$$

5.3 Der Zerfällungskörper eines Polynoms

Definition 5.3.1 Sei L eine Körperweiterung und $f \in K[x]$ ein Polynom. Wir sagen, dass L ein *Zerfällungskörper* von f über K ist, falls folgende Bedingungen erfüllt sind:

(a) $f \in L[x]$ zerfällt in Linearfaktoren, d.h. es existieren $c, \alpha_1, \ldots, \alpha_n \in L$, sodass $f(x) = c\prod_{i=1}^n (x - \alpha_i)$,

(b) falls $L/M/K$ eine Teilerweiterung ist, sodass f schon über M in Linearfaktoren zerfällt, gilt $M = L$. Mit anderen Wörter: L ist die kleinste Körpererweiterung von K, in der f in Linearfaktoren zerfällt.

Die Bedingung (b) ist äquivalent zu:

(b') $L = K(\alpha_1, \ldots, \alpha_n)$, wobei $\alpha_i \in L$ die Nullstellen von f sind.

Satz 5.3.2 (Kronecker) *Sei K ein Körper und $f \in K[x]$ ein Polynom. Es existiert ein Zerfällungskörper L von f über K.*

Beweis: Wir beweisen den Satz mit vollständigem Induktion nach dem Grad von f. Falls $\text{Grad}(f) = 1$, so zerfällt f über K in Linearfaktoren, also gibt es in diesem Fall nichts zu zeigen.

Wir nehmen an, wir die Existenz des Zerfällungskörper für alle Polynome von Grad $< n = \text{Grad}(f)$ gezeigt haben. Falls alle irreduzible Faktoren von f über K Grad 1 haben, zerfällt f über K in Linearfaktoren. Wir durfen also annehmen, dass f über K mindestens einen irreduziblen Faktor f_1 von Grad > 1 besitzt. In der Körpererweiterung $K_1 := K[x]/(f_1)$ besitzt f mindestens eine Nullstelle α_1 (Lemma 4.2.5.(b)). Daher gilt in in $K_1[x]$, dass $f(x) = (x - \alpha_1)g(x)$ ist, wobei $\text{Grad}(g) = n - 1$ ist. Laut Induktionshypothese existiert ein Zerfällungskörper L von g über K_1. Aber L ist auch der Zerfällungskörper von f über K. □

Aus dem Beweis von Satz 5.3.2 wird nicht klar, ob der Zerfällungskörper von der Wahl der Nullstelle α_1 abhängt. Wir werden sehen, dass dies nicht der Fall ist: Zwei Zerfällungskörper von f sind isomorph über K (Korollar 5.3.5).

Jeder Körperisomorphismus $\varphi : K \to \tilde{K}$ induziert einen Ringisomorphismus

$$\varphi : K[x] \to \tilde{K}[x], \quad f(x) = \sum_{i=0}^{n} a_i x^i \mapsto \tilde{f} = \sum_{i=0}^{n} \varphi(a_i) x^i. \tag{7}$$

Also ist $\tilde{f}$ genau dann irreduzibel, wenn f irreduzibel ist.

Lemma 5.3.3 *Sei $\varphi : K \to \tilde{K}$ ein Körperisomorphismus. Wir benutzen die obigen Bezeichnungen. Sei $f \in K[x]$ irreduzibel. Sei α eine Nullstelle von f in einer Körpererweiterung L von K und sei $\tilde{\alpha}$ eine Nullstelle von $\tilde{f}$ in einer Körpererweiterung $\tilde{L}$ von $\tilde{K}$. Es existiert ein eindeutiger Isomorphismus*

$$\psi : K(\alpha) \to \tilde{K}(\tilde{\alpha}),$$

sodass $\psi(\alpha) = \tilde{\alpha}$ und $\psi(a) = \varphi(a)$ für alle $a \in K$.

Beweis: Wir wissen, dass $K(\alpha) \simeq K[x]/(f)$ und $\tilde{K}(\tilde{\alpha}) \simeq \tilde{K}[x]/(\tilde{f})$ (Lemma 4.2.5.(a)). Der Ringisomorphismus $\varphi : K[x] \to \tilde{K}[x]$ bildet das Ideal (f) auf das Ideal $(\tilde{f})$ ab. Daher induziert $\varphi : K[x] \to \tilde{K}[x]$ einen Isomorphismus $\psi : K[x]/(f) \to \tilde{K}[x]/(\tilde{f})$ der Faktorringe. Offensichtlich gilt, dass $\psi(\alpha) = \tilde{\alpha}$, also $\psi(\sum_i a_i \alpha^i) \mapsto \sum_i \varphi(a_i)\tilde{\alpha}^i$. Das Lemma folgt. □

Satz 5.3.4 *Sei $\varphi : K \to \tilde{K}$ ein Körperisomorphismus. Sei $f(x) \in K[x]$ ein Polynom von $\text{Grad}\, f \geq 1$ und sei $\tilde{f} \in \tilde{K}[x]$ das zugehörige Polynom mit Koeffizienten in $\tilde{K}$. Seien L und $\tilde{L}$ Zerfällungskörper für f und $\tilde{f}$. Es existiert ein Isomorphismus $\psi : L \to \tilde{L}$, sodass $\psi(\alpha) = \tilde{\alpha}$ und $\psi(a) = \varphi(a)$ für alle $a \in K$.*

Falls wir $K = \tilde{K}$ und $\varphi = \text{Id}$ im obigen Satz nehmen, erhalten wir folgendes wichtige Korollar:

Korollar 5.3.5 *Alle Zerfällungskörper von $f \in K[x]$ sind isomorph über K.*

Beweis des Satzes: Dies folgt mit Induktion, wie im Beweis von Satz 5.3.2.

Falls f über K in Linearfaktoren zerfällt, so zerfällt $\tilde{f}$ in Linearfaktoren über $\tilde{K}$. In diesem Fall gilt $L = K$, $\tilde{L} = \tilde{K}$ und $\psi = \varphi$.

Wir nehmen also an, dass f über K nicht in Linearfaktoren zerfällt. Sei g ein nichtkonstanter irreduzible Faktor von f und sei $\tilde{g}$ der zugehörige Faktor von $\tilde{f}$. In $K[x]/(g)$ besitzt g eine Nullstelle α und $K(\alpha) \simeq K[x]/(g)$. Ebenso besitzt $\tilde{g}$ eine Nullstelle $\tilde{\alpha} \in \tilde{K}[x]/(\tilde{g})$ und $\tilde{K}(\tilde{\alpha}) \simeq \tilde{K}[x]/(\tilde{g})$.

Nach Lemma 5.3.3 existiert ein Körperisomorphsmus $\psi : K(\alpha) \to \tilde{K}(\tilde{\alpha})$ mit $\psi(\alpha) = \tilde{\alpha}$ und $\psi(a) = \varphi(a)$ für alle $a \in K$. Der Körper L ist auch der Zerfällungskörper von $h(x) = f(x)/(x - \alpha)$ über dem größeren Körper $K(\alpha)$. (Vergleichen Sie zum Beweis von Satz 5.3.2.) Daher folgt der Satz mit Induktion nach dem Grad von f. □

Beispiel 5.3.6 (a) Sei $f(x) = (x^2 - 3)(x^3 + 1) \in \mathbb{Q}[x]$. In $\mathbb{C}[x]$ zerfällt f in Linearfaktoren:

$$f(x) = (x - \sqrt{3})(x + \sqrt{3})(x + 1)(x + \zeta_3)(x + \zeta_3^2),$$

wobei $\zeta_3 = \cos(2\pi i/3) + i \sin(2\pi i/3) = (-1 + i\sqrt{3})/2 \in \mathbb{C}$ eine primitive 3-te Einheitswurzel ist. Wir schließen, dass f in $L = \mathbb{Q}(\sqrt{3}, \zeta_3) = \mathbb{Q}(\sqrt{3}, i)$ in Linearfaktoren zerfällt. Da dies die kleinste Teilerweiterung von $\mathbb{C}/\mathbb{Q}$ mit dieser Eigenschaft ist, ist L der Zerfällungskörper von f über $\mathbb{Q}$.

(b) Sei nun $k = \mathbb{F}_2$ und f wie in (a). Wir schreiben

$$f(x) \equiv (x - 1)^3(x^2 + x + 1) \in \mathbb{F}_2[x].$$

Das Polynom $x^2 + x + 1$ ist irreduzibel über $\mathbb{F}_2$, zerfällt aber in Linearfaktoren über $\mathbb{F}_{2^2}$ (Beispiel 4.5.3). Also ist $\mathbb{F}_{2^2}$ der Zerfällungskörper von f über $\mathbb{F}_2$.

(c) Das Zerfällungskörper des n-ten Kreisteilungspolynoms Φ_n über $\mathbb{Q}$ ist $\mathbb{Q}(\zeta_n)$, siehe § 4.4.

(d) Sei $f(x) = x^3 - 2 \in \mathbb{Q}[x]$. In $\mathbb{C}[x]$ zerfällt f in Linearfaktoren als

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

wobei ζ_3 eine primitive 3-te Einheitswurzel ist. Wir schreiben $\alpha_1 = \sqrt[3]{2}, \alpha_2 = \zeta_3 \sqrt[3]{2}, \alpha_3 = \zeta_3^2 \sqrt[3]{2}$ für die Nullstellen von f. Wir bemerken, dass

$$\alpha_3 = \alpha_2^2/\alpha_1, \qquad \zeta_3 = \frac{\alpha_2}{\alpha_1}.$$

Also ist $L := \mathbb{Q}(\alpha_1, \alpha_2) = \mathbb{Q}(\sqrt[3]{2}, \zeta_3)$ der Zerfällungskörper von f über $\mathbb{Q}$. Da $L \neq \mathbb{Q}(\sqrt[3]{2})$ (Beispiel 5.2.3), folgt

$$[L : \mathbb{Q}] = [\mathbb{Q}(\sqrt[3]{2}, \zeta_3) : \mathbb{Q}(\sqrt[3]{2})][\mathbb{Q}(\sqrt[3]{2}) : \mathbb{Q}] = 2 \cdot 3 = 6.$$

Definition 5.3.7 Die *Galois-Gruppe* eines Polynoms $f \in K[x]$ ist die Automorphismengruppe

$$G(f) := \mathrm{Aut}_K(L)$$

des Zerfällungskörpers L von f über K.

Satz 5.3.8 *Sei $f \in K[x]$ ein (normiertes) Polynom, L ein Zerfällungskörper von f über K und*

$$X_f := \{\alpha_1, \ldots, \alpha_n\} \subset L$$

die Menge der Nullstellen von f.

(a) Die Galois-Gruppe $G(f) = \mathrm{Aut}_K(L)$ wirkt auf der Menge X_f.

(b) Die Galois-Gruppe $G(f)$ ist isomorph zu einer Untergruppe von S_n.

Beweis: Sei $f(x) \in K[x]$ ein Polynom und $\alpha \in X_f$ eine Nullstelle von f und $\sigma : L \xrightarrow{\sim} L$ ein K-Automorphismus von L. Lemma 5.2.4 impliziert, dass $\sigma(\alpha)$ wieder eine Nullstelle von f ist. Dies beweist (a).

Man überprüft leicht, dass

$$\tau : \mathrm{Aut}_K(L) \times X_f \to X_f, \qquad (\sigma, \alpha) \mapsto \sigma(\alpha)$$

eine Gruppenwirkung definiert. Sei $\rho : \mathrm{Aut}_K(L) \to S(X_f)$ der zugehörige Gruppenhomomorphismus. Teil (b) folgt aus der Behauptung, dass ρ injectiv ist. Wir müssen also zeigen, dass $\ker(\rho) = \{1\}$ ist (Korollar 1.6.5).

Nach Definition des Zerfällungskörpers wird L/K von den Elementen aus X_f erzeugt (Definition 5.3.1.(b')). Ein K-Automorphismus $\sigma : L \xrightarrow{\sim} L$, der jedes Element aus X_f festlässt, ist deshalb die Identität auf L, also das neutrale Element von $G(f)$. Die beweist (b). □

Injektive Gruppenwirkungen $\rho : G \to S(X)$ heißen *treu*.

Beispiel 5.3.9 (a) Sei $f(x) = x^3 - 2 \in \mathbb{Q}[x]$ und sei L der Zerfällungskörper von f über $\mathbb{Q}$ (Beispiel 5.3.6.(c)). Wir nummerieren die Nullstellen von f wie in diesem Beispiel.

Satz 5.3.8 impliziert, dass die Galois-Gruppe $G(f)$ von f eine Untergruppe der symmetrischen Gruppe S_3 ist: Jedes Element $\varphi \in G(f) = \mathrm{Aut}_{\mathbb{Q}}(L)$ definiert eine Permutation der Nullstellen $\alpha_i \in L$ von f. Wir behaupten, dass $G(f) \simeq S_3$ ist.

Da $\alpha_2 = \zeta_3 \sqrt[3]{2} \notin \mathbb{Q}(\sqrt[3]{2})$ ist, sind die Nullstellen α_1 und α_2 *algebraisch unabhängig*. Dies bedeutet, dass keine nicht-triviale Beziehungen zwischen α_1 und α_2 existieren. Die 3-te Nullstelle erfüllt aber $\alpha_3 = \alpha_2^2/\alpha_1$ und ist also algebraisch abhängig von α_1 und α_2.

Ähnlich sieht man, dass jede zwei Nullstellen algebraisch unabhängig sind. Wir schließen, dass für jedes Paar $\beta_1 \neq \beta_2 \in X_f = \{\alpha_1, \alpha_2, \alpha_3\}$ genau ein

$\mathbb{Q}$-Automorphismus $\varphi \in G(f)$ mit $\varphi(\alpha_1) = \beta_1$ und $\varphi(\alpha_2) = \beta_2$ existiert. Also ist $G(f) \simeq S_3$. Folgende Tabelle listet die Elemente von $G(f)$ auf:

	α_1	α_2	α_3	$\zeta_3 = \frac{\alpha_2}{\alpha_1}$	ζ_3^2	Elt. in S_3
Id	α_1	α_2	α_3	ζ_3	ζ_3^2	e
φ_1	α_2	α_1	α_3	ζ_3^2	ζ_3	$(1\,2)$
φ_2	α_2	α_3	α_1	ζ_3	ζ_3^2	$(1\,2\,3)$
φ_2^2	α_3	α_1	α^3	ζ_3	ζ_3^2	$(1\,3\,2)$
$\varphi_1 \circ \varphi_2$	α_1	α_3	α_2	ζ_3^2	ζ_3	$(2\,3)$
$\varphi_1 \circ \varphi_2^2$	α_3	α_2	α_1	ζ_3^2	ζ_3	$(1\,3)$.

(b) Sei $\Phi_n \in \mathbb{Q}[x]$ das n-te Kreisteilungspolynom. Wir haben gesehen, dass $G(\Phi_n) \simeq (\mathbb{Z}/n\mathbb{Z})^*$ (Satz 5.2.5). In diesem Fall ist $G(f)$ also nicht die volle symmetrische Gruppe.

5.4 Normale und separable Erweiterungen

In nächsten Abschnitt definieren wir Galois-Erweiterungen L/K als Erweiterungen für die die Gruppe $\mathrm{Aut}_K(L)$ der K-Automorphismen von L "groß genug" ist. Solche Erweiterungen werden von den Bedingungen Normalität und Separabilität charakterisiert. In diesem Abschnitt definieren wir diese Begriffe.

Definition 5.4.1 Eine Körpererweiterung L/K heißt *normal*, falls jedes irreduzible Polynom $f \in K[x]$, das in L eine Nullstelle besitzt, in L in Linearfaktoren zerfällt.

Beispiel 5.4.2 (a) Die Erweiterung $\mathbb{C}/\mathbb{R}$ ist normal, da jedes Polynom $f \in \mathbb{R}[x]$ in $\mathbb{C}$ in Linearfaktoren zerfällt.

(b) Wir behaupten, dass die Erweiterung $\mathbb{Q}(\sqrt[3]{2})/\mathbb{Q}$ nicht normal ist. Wir betrachten dazu $f(x) = \min_{\mathbb{Q}}(\sqrt[3]{2}) = x^3 - 2$ (Beispiel 4.1.4.(c)), wobei $\sqrt[3]{2}$ die eindeutig bestimmte reelle Nullstelle von f ist. Da f ein Minimalpolynom über $\mathbb{Q}$ ist, ist f auf jedem Fall irreduzibel über $\mathbb{Q}$. In $K := \mathbb{Q}(\sqrt[3]{2})$ besitzt f die Nullstelle $\sqrt[3]{2}$. Die andere Nullstellen von f in $\mathbb{C}$ sind nicht reell, also nicht enthalten in K, da K ein Teilkörper von $\mathbb{R}$ ist (Beispiel 5.2.3.(b)). Die Nichtnormalität der Erweiterung hat zur Folge, dass die Gruppe $\mathrm{Aut}_{\mathbb{Q}}(K)$ trivial ist. Der Zerfällungkörper L von f über $\mathbb{Q}$ ist aber normal (Satz 5.4.3).

Definition 5.4.1 ist relativ unpraktisch, da man die Normalitätsbedingung für jedem Polynom überprüfen muss. Folgender Satz gibt ein einfaches Kriterium für Normalität: Der Satz sagt, dass eine Erweiterung genau dann normal ist, wenn es ein Zerfällungskörper ist. Dies bedeutet, dass man nur ein Polynom zu überprüfen braucht.

Satz 5.4.3 *Eine endliche Körpererweiterung L/K ist genau dann normal, wenn L der Zerfällungskörper eines Polynoms $f \in K[x]$ ist.*

Beweisskizze: Wir skizzieren nur dem Beweis. Sei L/K eine endliche Körpererweiterung, d.h., dass der Grad $[L : K]$ der Körpererweiterung endlich ist. Insbesondere ist L/K eine algebraische Erweiterung. Wir nehmen an, dass L/K eine normale Körpererweiterung ist. Wir schreiben $L = K(\alpha_1, \ldots, \alpha_s)$, wobei die α_i algebraisch über K sind. Sei $m_i = \min_K(\alpha_i)$ und $f = m_1 \cdots m_s$. Die irreduziblen Polynome m_i besitzen eine Nullstelle $\alpha_i \in L$. Da L/K normal ist, folgt also, dass die m_i über L in Linearfaktoren zerfällen. Dies gilt also auch für f. Da L über K von $\alpha_1, \ldots, \alpha_s$ erzeugt wird, ist L der Zerfällungskörper von f.

Wir skizzieren die andere Richtung. Sei L/K der Zerfällungskörper von $f \in K[x]$ und sei $g \in K[x]$ ein Polynom, das in L mindestens eine Nullstelle α besitzt. Wir müssen zeigen, dass g über L in Linearfaktoren zerfällt. Sei dazu $M \supset L$ der Zerfällungskörper von fg.

Behauptung: Seien $\theta_1, \theta_2 \in M$ zwei beliebige Nullstellen von g. Es gilt $[L(\theta_1) : L] = [L(\theta_2) : L]$.

Der Beweis der Behauptung überlassen wir dem Leser/der Leserin als Übungsaufgabe. Die wichtigste Schritte im Beweis sind:

(1) Es existiert ein K-Isomorphismus $K(\theta_1) \xrightarrow{\sim} K(\theta_2)$.

(2) Für $j = 1, 2$ gilt, dass

$$[L(\theta_j) : L][L : K] = [L(\theta_j) : K] = [L(\theta_j) : K(\theta_j)][K(\theta_j) : K].$$

Siehe auch [6, Theorem 8.4].

Wir zeigen nun, dass die Behauptung impliziert, dass L/K normal ist. Wir haben angenommen, dass g in L eine Nullstelle α besitzt. Wir nehmen $\theta_1 = \alpha$ und θ_2 eine beliebige andere Nullstelle von g. Da $\alpha \in L$ ist, ist $[L(\alpha) : L] = 1$. Wir schließen, dass $[L(\theta_2) : L] = [L(\alpha) : L] = 1$. Also ist $\theta_2 \in L$. □

Definition 5.4.4 Sei K ein Körper. Ein irreduzibles Polynom $f \in K[x]$ heißt *separabel* über K, falls f keine mehrfache Nullstelle besitzt in seinem Zerfällungskörper.

Ein irreduzibles Polynom $f \in K[x]$ heißt *inseparabel* über K, falls f nicht separabel über K ist. Ein reduzibles Polynom $f \in K[x]$ heißt *separabel*, falls alle irreduzible Faktoren separabel sind.

Sei L/K eine Körpererweiterung. Ein algebraisches Element $\alpha \in L$ heißt *separabel* über K, falls das Minimalpolynom $\min_K(\alpha)$ separabel ist.

Eine algebraische Körpererweiterung L/K heißt *separabel*, falls jedes Element $\alpha \in L$ separabel über K ist.

Beispiel 5.4.5 (a) Das n-te Kreisteilungspolynom $\Phi_n \in \mathbb{Q}[x]$ ist irreduzibel über $\mathbb{Q}$ (Satz 4.4.4). Der Zerfällungskörper von Φ_n über $\mathbb{Q}$ ist $\mathbb{Q}(\zeta_n)$. Insbesondere ist $\mathbb{Q}(\zeta_n)/\mathbb{Q}$ normal (Satz 5.4.3). Das Polynom Φ_n besitzt keine mehrfache Nullstellen über $\mathbb{Q}(\zeta_n)$ (§ 4.4), also ist Φ_n separabel über $\mathbb{Q}$. (Dies folgt alternativ auch aus Satz 5.4.6.)

(b) Wir geben ein Beispiel eines inseparablen Polynoms. Sei $K = \mathbb{F}_p(t)$ (Beispiel 4.1.2.(b)). Dies ist eine rein transzendente Erweiterung von $\mathbb{F}_p$. Wir betrachten $f(x) = x^p - t \in K[x]$. Sei L/K der Zerfällungskörper von f. Das Polynom f besitzt also mindestens eine Nullstelle $\alpha \in L$. Diese Nullstelle erfüllt $f(\alpha) = \alpha^p - t = 0$, also ist α eine p-te Wurzel aus t. Offensichtlich ist $\alpha \notin K$.

In $L[x]$ zerfällt f als

$$f(x) = x^p - t = x^p - \alpha^p = (x - \alpha)^p, \tag{8}$$

Lemma 4.4.3. Hier benutzen wir, dass K ein Körper der Charakteristik p ist. Also ist α eine mehrfache Nullstelle von f mit Vielfachheit p.

Als letzter Schritt im Beweis der Inseparabilität von f müssen wir überprüfen, dass f irreduzibel über K ist. Nehmen wir an, es gäbe eine Zerlegung $f = gh$ mit $g, h \in K[x]$ Polynome kleineren Grades. OBdA dürfen wir annehmen, dass g und h normiert sind. Wir schließen aus (8), dass

$$g(x) = (x - \alpha)^m = x^m - \binom{m}{1}\alpha x^{m-1} + \cdots + (-1)^m \alpha^m \in K[x]$$

gilt. Dies bedeutet, dass alle Koeffizienten von g (insbesondere $-m\alpha$) Elemente von K sind. Da $0 < m < p$ ist, folgt, dass $m \in \mathbb{F}_p^\times$ ist, also folgt, dass $\alpha \in K$ ist. Dies ist ein Widerspruch. (Alternativ folgt die Irreduzibilität auch aus einer Verallgemeinerung des Eisenstein-Kriteriums (Theorem 3.4.4) nach $K[x]$. Siehe zum Beispiel [3, Satz 2.8.1].)

Da f nur eine Nullstelle in seinem Zerfällungskörper L besitzt, ist die Galois-Gruppe $G(f) = \mathrm{Aut}_K(L) = \{1\}$ trivial (Satz 5.3.8.(b)).

(c) Sei $q = p^n$ eine Primzahlpotenz. Theorem 4.5.4 impliziert, dass $\mathbb{F}_q$ der Zerfällungskörper von $f_q := x^q - x \in \mathbb{F}_p[x]$ ist. Außerdem haben wir gezeigt, dass f_q in $\mathbb{F}_q$ genau q verschiedene Nullstellen besitzt. Falls $g \in \mathbb{F}_p[x]$ ein irreduzibles Polynom ist, so teilt $g \mid f_q$, für q groß genug. Da f_q nur einfache Nullstellen besitzt, schließen wir, dass $g \in \mathbb{F}_p[x]$ separabel ist. Es folgt, dass die Erweiterung $\mathbb{F}_q/\mathbb{F}_p$ separabel ist.

Satz 5.4.6 *Sei K ein Körper der Charakteristik 0. Jedes Polynom $f \in K[x]$ ist separabel.*

Beweis: Wir müssen zeigen, dass alle irreduziblen Polynome separabel sind (Definition 5.4.4). Sei K ein Körper der Charakteristik 0 und sei $f(x) = \sum_{i=0}^n a_i x^i \in K[x]$ ein irreduzibles Polynom. Das Polynom f ist genau dann inseparabel, wenn f und seine formale Ableitung f' eine gemeinsame Nullstelle besitzen (Lemma 3.4.7).

Da $\mathrm{Char}(K) = 0$ ist, ist f' ein Polynom von Grad $n - 1$. Falls f und f' eine gemeinsame Nullstelle haben, ist $g := \mathrm{ggT}(f, f')$ ein Polynom von Grad ≥ 1. Das Polynom g ist daher ein Teiler des irreduziblen Polynoms f. Da g auch ein Teiler von f' ist, ist g ein echter Teiler von f, aber dies ist unmöglich. □

Das folgende Lemma gibt eine Charakterisierung von separable Polynome. Der Beweis ist eine Verallgemeinerung vom Beweis von Satz 5.4.6, siehe zum Beispiel [6, Prop. 8.6].

Lemma 5.4.7 *Sei $f \in K[x]$ ein nichtkonstantes, irreduzibles Polynom. Dann ist f genau dann inseparabel, wenn die formale Ableitung von f verschwindet: $f' = 0$.*

Beispiel 5.4.8 Sei $f(x) = x^p - t \in K[x]$ wie in Beispiel 5.4.5.(b). Die formale Ableitung von f nach x ist $f'(x) = \partial f/\partial x = px^{p-1} = 0 \in K[x]$. Die Inseparabilität von f folgt also auch aus Lemma 5.4.7.

Folgender sehr praktischer Satz sagt, dass jede endliche separable Körpererweiterung von einem Element erzeugt wird. In Beweisen reicht es also, nur solche Erweiterungen zu betrachten.

Satz 5.4.9 (vom primitiven Element) *Ist L/K eine endliche und separable Körpererweiterung, so gibt es ein Element $\alpha \in L$ mit $L = K(\alpha)$.*

Das Element α heißt ein primitives Element *von L/K.*

Beweis: Ist K ein endlicher Körper, so ist L auch endlich, und man kann für α z.B. einen zyklischen Erzeuger von $L^\times$ wählen. Wir dürfen also annehmen, dass der Körper K unendlich viele Elemente besitzt.

Da L/K endlich ist, können wir Erzeuger $\epsilon_1, \ldots, \epsilon_r$ von L über K wählen: Es gilt $L = K(\epsilon_1, \ldots, \epsilon_r)$. Wir müssen zeigen, dass wir schon mit einem Erzeuger (also $r = 1$) auskommen. Um dies zu zeigen, genügt es, den Fall $r = 2$ zu betrachten, da wir dann induktiv die Anzahl der Erzeuger der Zwischenerweiterungen $K(\alpha_1, \ldots, \alpha_i)$ auf eins reduzieren können.

Der Einfachheit halber schreiben wir $\alpha := \epsilon_1$ und $\beta := \epsilon_2$. Nach Annahme ist $L = K(\alpha, \beta)/K$ eine endliche separable Erweiterung. Seien $f := \min_K(\alpha)$ und $g := \min_K(\beta)$ die Minimalpolynome von α und β. Sei M/L eine Erweiterung, sodass sowohl f als auch g in M in Linearfaktoren zerfällt. (Zum Beispiel kann man für M der Zerfällungskörper von fg über L nehmen.) Über M zerfallen f und g in Linearfaktoren:

$$f = \prod_{i=1}^{n} (x - \alpha_i), \qquad g = \prod_{j=1}^{m} (x - \beta_j),$$

mit $\alpha_i, \beta_j \in \bar{K}$. Wir dürfen annehmen, dass $\alpha = \alpha_1$ und $\beta = \beta_1$. Die Separabilität von L/K hat zur Folge, dass die m Elemente $\beta = \beta_1, \ldots, \beta_m$ paarweise verschieden sind.

Da der Körper K nach Annahme unendlich viele Elemente besitzt, gibt es ein $c \in K$ mit

$$\gamma := \alpha + c\beta \neq \alpha_i + c\beta_j, \quad \text{für } i = 1, \ldots, n,\ j = 2, \ldots, m. \tag{9}$$

(Es sind nur die endlich vielen Elemente $c = -(\alpha - \alpha_i)/(\beta - \beta_j)$ zu vermeiden.) Wir wollen zeigen, dass $L = K(\gamma)$ gilt. Dazu betrachten wir den Zwischenkörper $M := K(\gamma)$ und das Polynom

$$h := f(\gamma - cx) = \prod_{i=1}^{n} \big(\gamma - (\alpha_i + cx)\big) \in M[x].$$

Nach Wahl von c und γ gilt

$$h(\beta) = 0, \quad h(\beta_j) = \prod_{i=1}^{n} (\gamma - (\alpha_i + c\beta_j)) \neq 0, \quad \text{für } j > 1.$$

Es folgt:

$$\mathrm{ggT}(h, g) = x - \beta.$$

Da der ggT von h und g in dem Polynomring $M[x]$ berechnet werden kann (Satz 3.3.1), folgt $\beta \in M$. Dann gilt aber auch $\alpha = \gamma - c\beta \in M$ und insgesamt $L = K(\alpha, \beta) = M = K(\gamma)$. Dies beweist den Satz. □

Beispiel 5.4.10 Sei $L = \mathbb{Q}(\sqrt[3]{2}, \zeta_3)$ der Zerfällungskörper von $f(x) = x^3 - 2 \in \mathbb{Q}[x]$ (Beispiel 5.3.6.(c)). Wir finden ein primitives Element von L über $\mathbb{Q}$. Wir benutzen die Bezeichnung aus dem Beweis von Satz 5.4.9.

Sei $\alpha = \sqrt[3]{2}$ und $\beta = \zeta_3$, also gilt $\min_{\mathbb{Q}}(\alpha) = x^3 - 2 = \prod_{i=0}^{2}(x - \zeta_3^i \alpha)$ und $\min_{\mathbb{Q}}(\beta) = x^2 + x + 1 = \prod_{j=1}^{2}(x - \zeta_3^i)$. Wir suchen ein Element $c \in \mathbb{Q}$, das die Bedingung (9) erfüllt. Man überprüft, dass $c = 1$ die Bedingung erfüllt. Also ist $\gamma = \alpha + \beta$ ein Erzeuger von L über $\mathbb{Q}$.

In der Tat sind die Elemente

$$1, \gamma = \alpha + \beta, \gamma^2, \ldots, \gamma^5$$

linear unabhängig über $\mathbb{Q}$. Hier aus folgt auch, dass $[\mathbb{Q}(\gamma) : \mathbb{Q}] = [L : \mathbb{Q}] = 6$, also, dass $L = \mathbb{Q}(\gamma)$ ist.

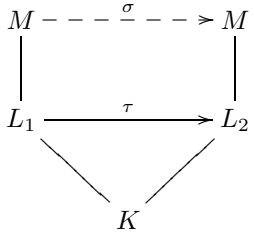
5.5 Fortsetzen von Körperisomorphismen

Folgender Satz ist eine Verallgemeinerung von Satz 5.3.4. Er erlaubt uns, Körperautomorphismen mit vorgegebenen Eigenschaften zu konstruieren.

Satz 5.5.1 *Sei M/K eine endliche normale Erweiterung und $M/L_i/K$, $i = 1, 2$ zwei Zwischenerweiterungen. Sei $\tau : L_1 \xrightarrow{\sim} L_2$ ein K-Isomorphismus. Dann gilt:*

(a) Es existiert eine Fortsetzung von τ zu einem K-Automorphismus $\sigma : M \xrightarrow{\sim} M$.

(b) Ist M/L_1 separabel, so gibt es in (a) genau $[M : L_1]$ verschiedene Fortsetzungen σ von τ.



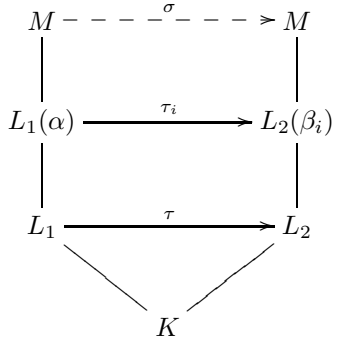
Beweis: Satz 5.4.3 sagt, dass M der Zerfällungskörper eines Polynoms $f \in K[x]$ ist. Also ist M der Zerfällungskörper von f über L_i für $i = 1$ und $i = 2$. Der Isomorphismus $\tau : L_1 \xrightarrow{\sim} L_2$ ist die Identität auf K, also ist $\tau(f) = f$ (wobei $\tau(f)$ definiert ist wie in (7)). Aus Satz 5.3.4 folgt die Existenz einer Fortsetzung $\sigma : M \to M$ von $\tau : L_1 \to L_2$. Da $\tau(a) = a$ für alle $a \in K$, ist $\sigma \in \mathrm{Aut}_K(M)$.

Der Beweis von (b) folgt mit Induktion, ähnlich wie im Beweis von Satz 5.3.4. Zusätzlich müssen wir über die Anzahl der Fortsetzungen buchführen.

Sei $f \in K[x]$ wieder wie oben. Wir nehmen an, dass f separabel über L_1 ist. Dies bedeutet, dass alle irreduziblen Faktoren von f über L_1 separabel sind.

Falls der Grad $[M : L_1] = 1$ ist, so ist (b) automatisch erfüllt, da $M = L_1$ ist. Also nehmen wir an, dass $n := [M : L_1] > 1$ ist. Sei $g \in L_1[x]$ ein nichtkonstanter irreduzibler Faktor von f über L_1. Da M ein Zerfällungskörper von f ist, zerfällt auch g in M in Linearfaktoren. Außerdem ist g separabel über L_1. Also besitzt g genau $m = \mathrm{Grad}(g)$ paarweise verschiedene Nullstellen $\alpha := \alpha_1, \ldots, \alpha_m$ in M.

Nach Teil (a) existiert eine Forsetzung $\sigma : M \to M$ von $\tau : L_1 \to L_2$. Sei $\beta_i := \sigma(\alpha_i) \in M$. Die β_i sind Nullstellen von $\tau(f) = f$. Da σ eine Bijektion ist, sind die β_i auch paarweise verschieden. Nach Lemma 5.3.3 existieren m paarweise verschiedene Fortsetzungen $\tau_i : L_1(\alpha) \xrightarrow{\sim} L_2(\beta_i)\,(i = 1, \ldots, m)$:



Der Grad $d := [M : L_1(\alpha)]$ der Körpererweiterung $M/L_1(\alpha)$ erfüllt

$$n := [M : L_1] = [M : L_1(\alpha)][L_1(\alpha) : L_1] = dm.$$

Insbesondere ist $d < n$. Außerdem ist $M/L_1(\alpha)$ ebenfalls separabel. Aus der Induktionshypothese schließen wir die Existenz von d paarweise verschiedenen Fortsetzungen von $\tau_i : L_1(\alpha) \xrightarrow{\sim} L_2(\beta_i)$ für jedes $i = 1, \ldots, m$. Insgesamt erhalten wir so mit genau $n = d \cdot m$ Fortsetzungen. □

Korollar 5.5.2 *Sei $f \in K[x]$ ein separables Polynom und L/K ein Zerfällungskörper von f. Es gilt*

$$|G(f)| = [L : K].$$

Beweis: Die Behauptung folgt unmittelbar aus Teil (b) von Satz 5.5.1 (mit $L_1 = L_2 = K$ und $\tau = \mathrm{Id}$). □

Beispiel 5.5.3 (a) Sei $\Phi_n \in \mathbb{Q}[x]$ das n-te Kreisteilungspolynom. Wir haben gesehen, dass $L = \mathbb{Q}(\zeta_n)$ ein Zerfällungskörper von Φ_n über $\mathbb{Q}$ ist. Die Galois-Gruppe $G(\Phi_n)$ ist isomorph zu $(\mathbb{Z}/n\mathbb{Z})^*$. In der Tat ist $|G(\Phi_n)| = [L : \mathbb{Q}] = \varphi(n)$ (siehe § 4.4 und Satz 5.2.5).

(b) Sei L der Zerfällungskörper von $f(x) = x^3 - 2$ über $\mathbb{Q}$ (Beispiel 5.3.6.(c)). Wir haben gesehen, dass $G(f) \simeq S_3$ (Beispiel 5.3.9.(a)). Also ist $[L : \mathbb{Q}] = |G(f)| = 6$.

5.6 Galois-Erweiterungen

In § 5.3 haben wir die Galois-Gruppe $G(f)$ eines Polynoms $f \in K[x]$ definiert. Falls f separabel ist, ist die Kardinalität der Galois-Gruppe genau der Grad der Körpererweiterung des Zerfällungskörpers von f über K. Allgemeiner nennt man Erweiterungen mit dieser Eigenschaft *galoisch*. Falls man statt Polynome Galois-Erweiterungen studiert, erhält man eine bessere Theorie.

Definition 5.6.1 Eine endliche Körpererweiterung heißt *galoisch*, wenn gilt:

$$|\operatorname{Aut}_K(L)| = [L : K].$$

In diesem Fall nennt man die Gruppe der K-Automorphismen von L die *Galois-Gruppe* von L/K. Die übliche Schreibweise ist:

$$\operatorname{Gal}(L/K) := \operatorname{Aut}_K(L).$$

Nach Korollar 5.5.2 ist der Zerfällungskörper eines separablen Polynoms eine Galois-Erweiterung. Wir zeigen, dass umgekehrt jede Galois-Erweiterung Zerfällungskörper eines separablen Polynoms ist (Korollar 5.6.4).

Satz 5.6.2 *Eine Körpererweiterung L/K, die endlich, normal und separabel ist, ist eine Galois-Erweiterung.*

Beweis: Ist L/K endlich und normal, so folgt aus Satz 5.4.3, dass L/K der Zerfällungskörper eines Polynoms $f \in K[x]$ ist. Aus der Separabilität von L/K folgt aber auch die Separabilität von f. Das Korollar 5.5.2 zeigt nun, dass L/K galoisch ist. □

Der folgende Satz ist im gewissen Sinne der Hauptsatz der Galoistheorie – auch wenn man üblicherweise eine etwas andere Aussage so bezeichnet, nämlich den Theorem 5.7.1 des folgenden Abschnittes.

Satz 5.6.3 *Sei L ein Körper und $G \subset \mathrm{Aut}(L)$ eine* endliche *Untergruppe der Automorphismengruppe* $\mathrm{Aut}(L)$ *von L. Sei $K = L^G$ der* Fixkörper *von G. Es gilt:*

(a) L/K ist endlich, normal, separabel und galoisch,

(b) $G = \mathrm{Gal}(L/K)$.

Beweis: Es ist klar, dass K ein Teilkörper von L ist und dass

$$G \subset \mathrm{Aut}_K(L).$$

Behauptung 1: Sei $\alpha \in L$. Es gilt:

(a) α ist algebraisch und separabel über K.

(b) Das Minimalpolynom $g := \min_K(\alpha)$ zerfällt über L in Linearfaktoren.

(c) Der Körpergrad $[K(\alpha) : K] = \deg(f)$ ist ein Teiler von $|G|$.

Insbesondere ist L/K algebraisch, normal und separabel.

Zum Beweis dieser Behauptung betrachten wir die Wirkung von G auf den Elementen von L. Sei

$$G(\alpha) = \{\alpha := \alpha_1, \ldots, \alpha_n\}$$

die Bahn von α. Der Bahn–Stabilizatorsatz (Satz 2.1.10) sagt, dass $n := |G(\alpha)|$ ein Teiler von $|G|$ ist.

Sei

$$f(x) := \prod_{i=1}^{n} (x - \alpha_i) = x^n + a_{n-1}x^{n-1} + \cdots + a_0.$$

Dies ist nach Konstruktion ein separables Polynom, dessen Nullstellen genau die Elemente von $G(\alpha)$ sind. Zum Beweis der Behauptung 1 reicht es zu zeigen, dass f das Minimalpolynom von α über K ist.

A priori liegen die Koeffizienten a_i von f in dem Körper L. Tatsächlich liegen sie in dem Fixkörper $K = L^G$. Ist nämlich $\sigma \in G$, so gilt

$$\begin{aligned}\sigma(f) &:= x^n + \sigma(a_{n-1})x^{n-1} + \cdots + \sigma(a_0) \\ &= \prod_{i=1}^{n} (x - \sigma(\alpha_i)) = \prod_{i=1}^{n} (x - \alpha_i) = f.\end{aligned}$$

(Wir haben hier ausgenutzt, dass $\sigma \in G$ die Elemente von $G(\alpha)$ permutiert.) Koeffizientenvergleich zeigt nun, dass $\sigma(a_i) = a_i$ für $i = 0, \ldots, n-1$. Da dies für alle $\sigma \in G$ gilt, folgt $a_i \in L^G = K$, wie behauptet.

Sei $g := \min_K(\alpha)$ das Minimalpolynom von α über K. Nach Definition der Bahn $G(\alpha)$ gibt es für alle $i = 1, \ldots, n$ ein Element $\sigma \in G \subset \mathrm{Aut}_K(L)$ mit $\alpha_i = \sigma(\alpha)$. Aus $g(\alpha) = 0$ folgt deshalb $g(\alpha_i) = 0$ für alle i (Lemma 5.2.4). Da die α_i paarweise verschieden sind, folgt $f \mid g$ und, wegen der Irreduzibilität

von g, sogar $f = g$. Insbesondere zerfällt g in Linearfaktoren in L. Nun ist die Behauptung 1 vollständig bewiesen.

Behauptung 2: Es gilt die Ungleichung $[L : K] \leq |G|$. Insbesondere ist L/K endlich.

Angenommen, wir haben $[L : K] > |G|$. Da L/K als algebraische Erweiterung die Vereinigung aller endlichen Zwischenerweiterungen ist, gäbe es dann eine endliche Zwischenerweiterung L'/K mit $[L' : K] > |G|$. Da L/K nach Behauptung 1 separabel ist, wäre L'/K ebenfalls separabel. Aus dem Satz vom primitiven Element (Satz 5.4.9) folgt $L' = K(\gamma)$, für ein $\gamma \in L$. Die Behauptung 1.(c) sagt aber, dass dann $[L' : K] \leq |G|$. Dies ist ein Widerspruch zur Annahme und beweist die Behauptung 2.

Aus den Behauptungen 1 und 2 folgt, dass L/K endlich, normal und separabel ist. Nach Satz 5.6.2 ist L/K also eine Galois-Erweiterung. Teil (a) des Satzes ist somit bewiesen, und wir erhalten die Ungleichung

$$|G| \leq |\operatorname{Aut}_K(L)| = [L : K].$$

Zusammen mit der Ungleichung aus Behauptung 2 folgt daraus $G = \operatorname{Aut}_K(L)$. Jetzt ist alles gezeigt. □

Korollar 5.6.4 *Sei L/K eine Galois-Erweiterung und $G := \operatorname{Gal}(L/K)$ ihre Galois-Gruppe. Dann ist $K = L^G$ der Fixkörper von G.*

Beweis: Sei $K' := L^G$ der Fixkörper von G. Nach Definition gilt $K \subset K'$ und nach Satz 5.6.3:

$$[L : K'] = |G| = [L : K].$$

Also folgt $K' = K$. □

Korollar 5.6.5 *Eine endliche Körpererweiterung L/K ist genau dann galoisch, wenn sie normal und separabel ist. Insbesondere ist jede Galois-Erweiterung Zerfällungskörper eines separablen Polynoms.*

Beweis: Eine Richtung ist genau die Aussage von Satz 5.6.2. Die andere Richtung folgt sofort aus Satz 5.6.3. □

Korollar 5.6.6 *Sei L/K eine endliche Körpererweiterung und M ein Zwischenkörper von L/K. Wenn L/K galoisch ist, so ist auch L/M galoisch.*

Beweis: Dieses Korollar überlassen wir dem Leser/der Leserin als Übungsaufgabe. □

5.7 Der Hauptsatz der Galois-Theorie

Sei L/K eine Galois-Erweiterung mit Galois-Gruppe $G = \mathrm{Gal}(L/K)$. Sei $H \subset G$ eine beliebige Untergruppe und $M := L^H$ der Fixkörper von H. Nach Korollar 5.6.6 ist die Erweiterung L/M wieder eine Galois-Erweiterung, mit Galois-Gruppe $H = \mathrm{Gal}(L/M)$. Nach Konstruktion gilt $K \subset M \subset L$, d.h. M ist ein Zwischenkörper von L/K. Wir erhalten somit eine Abbildung

$$H \subset G \quad \mapsto \quad M := L^H$$

von der Menge aller Untergruppen von G auf die Menge aller Zwischenkörper von L/K. Der Hauptsatz der Galois-Theorie sagt, dass diese Abbildung eine Bijektion ist.

Der Hauptsatz ermöglicht uns, die Struktur der Körpererweiterung L/K anhand der Struktur ihrer Galois-Gruppe G zu studieren. Zum Studium von Körpererweiterungen kann man also auch Methoden der Gruppentheorie benutzen.

Theorem 5.7.1 (Hauptsatz der Galois-Theorie) *Es sei L/K eine endliche Galois-Erweiterung mit Galois-Gruppe $G := \mathrm{Gal}(L/K)$. Wir bezeichnen mit*

$$\mathcal{G} := \{\, H \subset G \,\}$$

die Menge aller Untergruppen von G und mit

$$\mathcal{F} := \{\, M \mid K \subset M \subset L \,\}$$

die Menge aller Zwischenkörper von L/K.

(a) Die Abbildung

$$\mathcal{G} \to \mathcal{F}, \qquad H \mapsto L^H,$$

die einer Untergruppe $H \subset G$ den Fixkörper L^H zuordnet, ist bijektiv. Die Umkehrabbildung ist

$$\mathcal{F} \to \mathcal{G}, \qquad M \mapsto \mathrm{Aut}_M(L) \subset G.$$

(b) Die Bijektionen aus (a) sind inklusionsumkehrend. Genauer: für $H_1, H_2 \in \mathcal{G}$ gilt:

$$H_1 \subset H_2 \quad \Leftrightarrow \quad L^{H_1} \supset L^{H_2},$$

und für $M_1, M_2 \in \mathcal{F}$ gilt:

$$M_1 \subset M_2 \quad \Leftrightarrow \quad \mathrm{Aut}_{M_1}(L) \supset \mathrm{Aut}_{M_2}(L)$$

(c) Für alle $H \in G$ gilt

$$[L : L^H] = |H|, \qquad [L^H : K] = [G : H].$$

Beweis: Der Hauptsatz folgt fast unmittelbar aus dem Satz 5.6.3 und seinen Korollaren.

Ist $H \subset G$ eine Untergruppe und $M := L^H$ der Fixkörper von H, so folgt aus Satz 5.6.3 die Gleichheit $H = \mathrm{Aut}_M(L)$. Dies ist äquivalent zu der Aussage, dass die Hintereinanderausführung der zwei Abbildungen in (a),

$$\mathcal{G} \to \mathcal{F} \to \mathcal{G}, \qquad H \mapsto \mathrm{Aut}_{L^H}(L),$$

die Identität auf der Menge $\mathcal{G}$ ist.

Sei andersherum M ein Zwischenkörper von L/K. Nach Korollar 5.6.6 ist L/M eine Galois-Erweiterung. Die Galois-Gruppe $H := \mathrm{Gal}(L/M)$ ist nach Definition eine Untergruppe von G, und es gilt $M = L^H$ nach Korollar 5.6.4. Dies ist äquivalent zu der Aussage, dass die Hintereinanderausführung

$$\mathcal{F} \to \mathcal{G} \to \mathcal{F}, \qquad M \mapsto L^{\mathrm{Aut}(L/M)}$$

die Identität auf der Menge $\mathcal{F}$ ist. Damit ist (a) bewiesen.

Zum Beweis von (b) bemerke man, dass die Implikationen

$$H_1 \subset H_2 \quad \Rightarrow \quad L^{H_1} \supset L^{H_2}$$

und

$$M_1 \subset M_2 \quad \Rightarrow \quad \mathrm{Aut}_{M_1}(L) \supset \mathrm{Aut}_{M_2}(L)$$

trivial sind. Aufgrund von (a) folgt aber aus der ersten Implikation die Umkehrung der zweiten und aus der zweiten Implikation die Umkehrung der ersten. Nun ist auch (b) bewiesen. Die Aussage (c) ist offensichtlich. □

5.8 Die Galois-Gruppe eines kubischen Polynoms

Es sei $K = \mathbb{Q}$ und $f = x^3 + ax^2 + bx + c \in K[x]$ ein normiertes, kubisches Polynom über K. (Allgemeiner gilt dies für beliebige Körper der Charakteristik ungleich 2.) Wir nehmen an, dass f keine mehrfachen Nullstellen hat. Über einem geeignet gewählten Zerfällungskörper L zerfällt f in paarweise verschiedene Linearfaktoren:

$$f = x^3 + ax^2 + bx + c = (x - \alpha_1)(x - \alpha_2)(x - \alpha_3),$$

mit $\alpha_i \in L$, $\alpha_i \neq \alpha_j$ für $i \neq j$. Durch Ausmultiplizieren sieht man, dass die drei Nullstellen α_i Lösungen des Gleichungssystems

$$\begin{aligned} \alpha_1 + \alpha_2 + \alpha_3 &= -a \\ \alpha_1\alpha_2 + \alpha_1\alpha_3 + \alpha_2\alpha_3 &= b \\ \alpha_1\alpha_2\alpha_3 &= -c \end{aligned}$$

sind. Es ist kein Zufall, dass dieses Gleichungssystem *symmetrisch* ist bezüglich Permutationen der drei Unbekannten; schließlich bestimmt das Polynom f nur die Menge $X_f = \{\alpha_1, \alpha_2, \alpha_3\}$ seiner Nullstellen, nicht aber die von uns willkürlich

gewählte Nummerierung seiner Elemente. Die Frage ist, welche Permutationen von X_f als K-Automorphismen des Zerfällungskörpers $L := K(\alpha_1, \alpha_2, \alpha_3)$ realisiert werden können.

Es sei $G := \mathrm{Aut}_K(L)$ die Galois-Gruppe von f. Nach Satz 5.3.8 können wir G auffassen als Untergruppe von S_3. Ist $\sigma \in G$ und $\pi := \phi(\sigma)$, so gilt nach Definition:

$$\sigma(\alpha_i) = \alpha_{\pi(i)}, \qquad i = 1, 2, 3.$$

Wir wollen nun durch eine Fallunterscheidung zeigen, dass die Bahnen der G-Wirkung auf X_f den irreduziblen Faktoren von f entsprechen.

Fall 1: $X_f \subset K$, d.h. f zerfällt bereits über K in Linearfaktoren.

In diesem Fall gilt $L = K$ und somit $G = \{1\}$. Mehr gibt es hier nicht zu sagen.

Fall 2: f besitzt genau eine Nullstelle in K.

Durch geeignete Wahl der Nummerierung dürfen wir annehmen, dass $\alpha_1 \in K$ und $\alpha_2, \alpha_3 \notin K$. Die Zerlegung von f in irreduzible Faktoren über K ist dann

$$f = (x - \alpha_1)g, \qquad g = x^2 + px + q = (x - \alpha_2)(x - \alpha_3),$$

mit

$$p = -\alpha_2 - \alpha_3 \in K, \quad q = \alpha_2\alpha_3 \in K.$$

Der Zerfällungskörper L/K von f ist der Zerfällungsörper $L = K(\alpha_2) = K(\alpha_3)$ von g, und es gilt $[L : K] = 2$. Die Mitternachtsformel liefert ein Formel für die Nullstellen von g:

$$\alpha_2 = -\frac{p}{2} + \sqrt{\left(\frac{p}{2}\right)^2 - q}, \quad \alpha_3 = -\frac{p}{2} - \sqrt{\left(\frac{p}{2}\right)^2 - q}.$$

Das einzige nichttriviale Element von G ist der K-Automorphismus $\sigma : L \xrightarrow{\sim} L$, der α_2 und α_3 vertauscht. Das Bild von ϕ ist also die von der Transposition $(2\,3)$ erzeugte Untergruppe von S_3:

$$\phi(G) = \langle\, (2\,3) \,\rangle \subset S_3.$$

Fall 3: f ist irreduzibel über K.

Für $i = 1, 2, 3$ sei $L_i := K(\alpha_i) \subset L$ der von α_i erzeugte Körper von f. Es gilt $[L_i : K] = 3$, und für jedes Paar $i, j \in \{1, 2, 3\}$ existiert ein eindeutiger K-Isomorphismus $\tau_{i,j} : L_i \xrightarrow{\sim} L_j$ mit $\tau_{i,j}(\alpha_i) = \alpha_j$. Nach dem Gradsatz (Theorem 4.2.10) gilt $[L : K] = 3 \cdot [L : L_i]$.

Fall 3 (a): $[L : K] = 3$.

Dieser Fall tritt genau dann ein, wenn z.B. der Körper $L_1 = K(\alpha_1)$ bereits ein Zerfällungskörper von f ist, d.h. wenn sich die anderen beiden Nullstellen α_2, α_3 als rationale Ausdrücke in α_1 schreiben lassen. Es gilt dann sogar $L = L_1 = L_2 = L_3$. Da L/K galoisch ist, folgt $|\,\mathrm{Gal}(L/K)| = [L : K] = 3$. Da 3

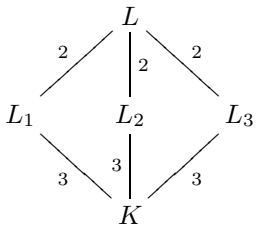
eine Primzahl ist, folgt also, dass $G \simeq \mathbb{Z}/3\mathbb{Z}$ (Korollar 1.6.12). Die zugehörige Untergruppe von S_3 ist $G = A_3$.

Fall 3 (b): $[L : K] > 3$.

Das Polynom f zerfällt in diesem Fall nicht über $L_1 = K(\alpha_1)$ in Linearfaktoren. Die Zerlegung in irreduzible Faktoren über L_1 ist

$$f = (x - \alpha_1)g, \qquad g = x^2 + px + q = (x - \alpha_2)(x - \alpha_3),$$

mit $p, q \in L_1$ und g irreduzibel über L_1. Es folgt, dass L/L_1 ein Zerfällungskörper von g und insbesondere $[L : L_1] = 2$ ist. Mit dem Gradsatz (Theorem 4.2.10) erhält man nun $[L : K] = 6$ und $[L_i : K] = 3$, $[L : L_i] = 2$ für $i = 1, 2, 3$.



Wir schließen, dass $\mathrm{Gal}(L/K)$ eine Untergruppe von S_3 ist mit $|\mathrm{Gal}(L/K)| = [L : K] = 6 = |S_3|$, also, dass $\mathrm{Gal}(L/K) \simeq S_3$ ist.

Wir wollen nun den Hauptsatz der Galois-Theorie (Theorem 5.7.1) im Fall 3.b explizit machen.

Sei $K = \mathbb{Q}$ und

$$f = x^3 + a\,x^2 + b\,x + c \in \mathbb{Q}[x]$$

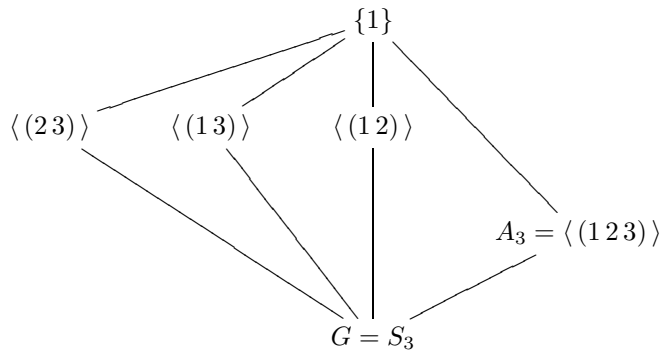
ein normiertes, irreduzibles kubisches Polynom. Wir nehmen an, dass f maximaler Galois-Gruppe $G(f) \simeq S_3$ besitzt, also, dass wir in dem Fall 3b sind.

Sei $L = K(\alpha_1, \alpha_2, \alpha_3)$ der Zerfällungskörper von f, wobei $\alpha_1, \alpha_2, \alpha_3 \in L$ die paarweise verschiedenen Nullstellen von f sind. Sei schließlich $G = \mathrm{Gal}(L/K)$ die Galois-Gruppe von f.

Zur Vereinfachung der Notation wollen wir im Folgenden die Galois-Gruppe G mit der symmetrischen Gruppe S_3 identifizieren: Wir fassen also Elemente von G gleichzeitig als K-Automorphismen von L und als Permutationen auf. Die Menge $\mathcal{G}$ aller Untergruppen von G besteht aus den folgenden 6 Elementen:

- der trivialen Untergruppe $\{1\}$,
- den drei Untergruppen der Ordnung 2, jeweils erzeugt von einer Transposition,
- der alternierenden Gruppe A_3, erzeugt von einem 3-Zyklus,
- der vollen symmetrischen Gruppe S_3.

Auf dieser Menge bildet die Inklusion eine natürliche Ordnungsrelation, die man am besten durch das folgende Diagram veranschaulicht:



Nach dem Hauptsatz der Galois-Theorie entsprechen die Untergruppen $H \subset G$ eins zu eins den Zwischenkörpern von L/K, vermöge der Abbildung $H \mapsto L^H$. Es ist klar, dass der Fixkörper der trivialen Untergruppe der Körper L ist. Nach Korollar 5.6.4 ist der Fixkörper der vollen Gruppe G der Körper K.

Nun sei $H = \langle (2\,3) \rangle$. Das einzige nichttriviale Element $\sigma \in H$ ist ein K-Automorphismus von L mit

$$\sigma(\alpha_1) = \alpha_1, \quad \sigma(\alpha_2) = \alpha_3, \quad \sigma(\alpha_3) = \alpha_2.$$

Offenbar ist der Körper $L_1 := K(\alpha_1)$ in dem Fixkörper L^H enhalten. Wegen

$$[L_1 : K] = 3 = [G : H] = [L^H : K]$$

(Theorem 5.7.1.(c)) folgt daraus sogar $L^H = L_1$. Mit demselben Argument zeigt man

$$L_2 := K(\alpha_2) = L^{\langle (1\,3) \rangle}, \qquad L_3 := K(\alpha_3) = L^{\langle (1\,2) \rangle}.$$

Schließlich wollen wir den Fixkörper $M := L^{A_3}$ der alternierenden Gruppe bestimmen. Dazu setzen wir

$$\delta := (\alpha_1 - \alpha_2)(\alpha_1 - \alpha_3)(\alpha_2 - \alpha_3) \in L.$$

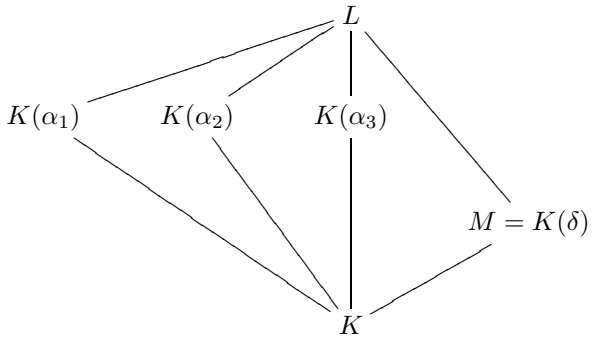
Für alle $\sigma \in G$ gilt dann

$$\sigma(\delta) = \operatorname{sgn}(\sigma) \cdot \delta,$$

wobei $\operatorname{sgn}(\sigma) = \pm 1$ das Vorzeichen von σ, aufgefaßt als Permutation, bezeichnet. Insbesondere gilt $\sigma(\delta) = \delta$ genau dann, wenn $\sigma \in A_3$. Aus dieser Äquivalenz folgt $\delta \in M \backslash K$, also $M = K(\delta)$.

Wir haben nun sämtliche Zwischenkörper von L/K bestimmt. Unter Berück-

sichtigung der bestehenden Inklusionen erhält man das folgende Diagramm:



Interessant ist, dass der Zwischenkörper $M = K(\delta)$ nur auf eher indirekte Weise von dem Polynom f abhängt. Der Zusammenhang wird etwas deutlicher, wenn man bedenkt, dass

$$D := \delta^2 = (\alpha_1 - \alpha_2)^2(\alpha_1 - \alpha_3)^2(\alpha_2 - \alpha_3)^2$$

invariant unter allen Elementen von G ist und deshalb im Grundkörper $K = L^G$ liegt. Man überlegt sich leicht, dass D nur von f, nicht aber von der Wahl des Zerfällungskörpers L und der Nummerierung der Nullstellen $\alpha_i \in L$ abhängt. Das Element $D = D(f) \in K$ heißt die *Diskriminante* des kubischen Polynoms f. Man kann zeigen, dass

$$D(f) = a^2b^2 - 4b^3 - 4a^3c - 27c^2 + 18abc,$$

für $f = x^3 + ax^2 + bx + c \in K[x]$. Den Zwischenkörper $M = K(\sqrt{D})$ kann man also sehr wohl an dem Polynom f direkt ablesen.

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 2008.

[5] G. Fischer, *Lehrbuch der Algebra*. Vieweg, 2008.

[6] I. Stewart, *Galois theory*. Chapmann & Hall, 2004.

[7] S. Wewers, *Galois-Theorie*. Vorlesungsskript, Universität Hannover, WS 2008/2009.