Algebra I

Wintersemester 2003-2004

Prof. Dr. Helmut Maier

Inhaltsverzeichnis

1. Gruppentheorie

1.1. Gruppen

DEFINITION 1.1.1
Unter einer Verknüpfung (auch Operation) in einer Menge M versteht man eine Abbildung

$$v : M \times M \to C$$

in irgendeine Menge C. Für $(a, b) \in M \times M$ schreibt man statt $v(a, b)$ einfach ab (falls die Verknüpfung als Addition betrachtet wird, auch $a + b$).

DEFINITION 1.1.2
Eine nicht leere Menge G mit einer Verknüpfung

$$G \times G \to C \ , \ (g_1, g_2) \mapsto g_1 g_2 \ ,$$

wobei C irgendeine Menge ist, heißt Gruppe, wenn $\forall g_1, g_2, g_3 \in G$ gilt:

(i) $g_1 g_2 \in G$ (Abgeschlossenheit bzgl. der Verknüpfung)
(ii) $(g_1 g_2) g_3 = g_1 (g_2 g_3)$ (Assoziativgesetz)
(iii) Es existiert ein Einselement (neutrales Element) $1 \in G$ mit $1g = g1 = g \ \forall g \in G$.
(iv) Zu jedem $g \in G$ existiert ein Inverses $g^{-1} \in G$ mit $g^{-1} g = g g^{-1} = 1$.

Gelten nur die Eigenschaften (i) und (ii), so heißt G Halbgruppe. Gelten die Eigenschaften (i),(ii),(iii), so heißt G Monoid. $g \in G$ heißt Einheit des Monoids G, falls es ein Inverses $g^{-1} \in G$ besitzt. Die Menge der Einheiten von G wird mit G^* bezeichnet. Die Elementanzahl $|G|$ von G, die auch unendlich sein kann, heißt Ordnung von G.
Eine Gruppe (Halbgruppe, Monoid) heißt abelsch (auch kommutativ), wenn $\forall g_1, g_2 \in G$ gilt:

(v) $g_1 g_2 = g_2 g_1$ (Kommutativgesetz)

BEISPIEL 1.1.1
$(\mathbb{Z}, +)$ mit der Addition $+$ als Verknüpfung bildet eine kommutative Gruppe: neutrales Element (das im Fall einer als Addition geschriebenen Verknüpfung auch als Nullelement bezeichnet wird) ist 0: $a + 0 = 0 + a = a \ , \ \forall a \in \mathbb{Z}$. Jedes $a \in \mathbb{Z}$ besitzt als Inverses das Element $-a$: $(-a) + a = a + (-a) = 0$.

BEISPIEL 1.1.2
Die Menge $\mathbb{Z}$ bildet bzgl. der Multiplikation ein Monoid, jedoch keine Gruppe. Es existiert zwar ein Einselement (nämlich 1), jedoch existieren im allgemeinen keine inversen Elemente.

BEISPIEL 1.1.3
Die Menge $\mathbb{N}$ der natürlichen Zahlen bildet bzgl. der Addition eine kommutative Halbgruppe, bzgl. der Multiplikation ein kommutatives Monoid.

BEISPIEL 1.1.4
Es sei K ein Körper. Dann ist K eine Gruppe bzgl. der Addition, $K - \{0\}$ eine Gruppe bzgl. der Multiplikation.

BEISPIEL 1.1.5
Es sei M eine Menge $\neq \emptyset$. Eine Permutation von M ist eine bijektive Abbildung von M auf sich selbst. Die Menge $\mathfrak{S}(M)$ der Permutationen von M bildet bzgl. der Hintereinanderausführung eine Gruppe mit Einselement id_M ($\mathrm{id}_M(a) = a \ \forall a \in M$). $\mathfrak{S}(M)$ ist nicht abelsch, falls M mindestens 3 Elemente hat. Ist $M = \{1, \ldots, n\}$, so schreibt man statt $\mathfrak{S}(M)$ auch $\mathfrak{S}_n$. $\mathfrak{S}_n$ heißt die symmetrische Gruppe n-ten Grades, und es ist $|\mathfrak{S}_n| = n!$.

BEMERKUNG 1.1.1
Ist $\sigma \in \mathfrak{S}_n$, so schreibt man

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

Zur Nichtkommutativität: Es sei $n \geq 3$ und

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & \cdots & n \\ 2 & 3 & 1 & 4 & \cdots & n \end{pmatrix}, \ \tau = \begin{pmatrix} 1 & 2 & 3 & 4 & \cdots & n \\ 2 & 1 & 3 & 4 & \cdots & n \end{pmatrix}.$$

Dann ist

$$\sigma\tau = \begin{pmatrix} 1 & 2 & 3 & 4 & \cdots & n \\ 3 & 2 & 1 & 4 & \cdots & n \end{pmatrix}, \ \tau\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & \cdots & n \\ 1 & 3 & 2 & 4 & \cdots & n \end{pmatrix} \neq \sigma\tau.$$

Die Verknüpfung auf einer endlichen Gruppe kann auch mittels einer Verknüpfungstafel beschrieben werden:

BEISPIEL 1.1.6
Es ist $\mathfrak{S}_2 = \{\mathrm{id} = \begin{pmatrix} 1 & 2 \\ 1 & 2 \end{pmatrix}, \sigma = \begin{pmatrix} 1 & 2 \\ 2 & 1 \end{pmatrix}\}$. Wir haben die Verknüpfungstafel

$\circ$	id	σ
id	id	σ
σ	σ	id

Gruppen, die durch Namensänderung ihrer Elemente auseinander hervorgehen, werden als nicht wesentlich verschieden betrachtet. Es handelt sich um isomorphe Gruppen.

BEISPIEL 1.1.7
Die Gruppe $\mathfrak{S}^* = \{0', 1'\}$ mit der Verknüpfungstafel

$+$	$0'$	$1'$
$0'$	$0'$	$1'$
$1'$	$1'$	$0'$

unterscheidet sich von der obigen Gruppe $\mathfrak{S}_2$ nur durch die Namen ihrer Elemente. Die Namensänderung wird durch den Isomorphismus $\Phi : \mathfrak{S}_2 \to \mathfrak{S}^*$ mit $\Phi(\mathrm{id}) = 0'$, $\Phi(\sigma) = 1'$ vermittelt.

DEFINITION 1.1.3
Es seien G, H Gruppen. Eine Abbildung $\Phi : G \to H$ heißt Homomorphismus (von Gruppen), falls $\Phi(g_1 g_2) = \Phi(g_1)\Phi(g_2)$ für alle $g_1, g_2 \in G$ (Relationstreue) ist. Φ heißt Isomorphismus, falls Φ bijektiv ist. Wir schreiben $G \cong H$ (G ist isomorph zu H), falls ein Isomorphismus $\Phi : G \to H$ existiert.

Zentral in der Gruppentheorie ist die Betrachtung von Untergruppen U einer gegebenen Gruppe G.

DEFINITION 1.1.4
Eine Teilmenge U einer Gruppe G heißt Untergruppe von G ($U \leq G$), falls gilt:

(i) $g_1, g_2 \in U \ \Rightarrow \ g_1 g_2 \in U$
(ii) U ist bzgl. der auf G definierten Verknüpfung eine Gruppe.

Zum Nachweis, dass eine Teilmenge U einer Gruppe G eine Untergruppe bildet, empfiehlt es sich, nicht die Definition 1.1.4 direkt zu verwenden, sondern das folgende Untergruppenkriterium:

SATZ 1.1.1
Eine nicht leere Teilmenge U einer Gruppe G ist Untergruppe von G genau dann, wenn gilt:

$$g_1, g_2 \in U \;\Rightarrow\; g_1 g_2^{-1} \in U\,.$$

BEWEIS
Es ist klar, dass die Verknüpfung auf U das Assoziativgesetz erfüllt, da es auf G gilt. Da $U \neq \emptyset$ gibt es ein $g_1 \in U$. Daher ist $g_1 g_1^{-1} = 1 \in U$ (Existenz des Einselements). Mit $g_1 \in U$ ist dann auch $1 \cdot g_1^{-1} = g_1^{-1} \in U$ (Existenz des Inversen). Aus $g_1, g_2 \in U$ folgt schließlich $g_1 \cdot (g_2^{-1})^{-1} = g_1 g_2 \in U$ (Abgeschlossenheit). □

BEMERKUNG 1.1.2
Aus Satz 1.1.1 folgt unmittelbar, dass der Durchschnitt beliebig vieler Untergruppen von G wieder eine Untergruppe ist. Das Kriterium in Satz 1.1.1 lässt sich einfacher schreiben, wenn wir das so genannte Komplexprodukt einführen.

DEFINITION 1.1.5
Es seien S, T beliebige Teilmengen (Komplexe) einer Gruppe.

(a) Unter dem Komplexprodukt ST verstehen wir die Menge $ST := \{st \mid s \in S\,,\; t \in T\}$.
(b) Wir setzen $S^{-1} := \{s^{-1} \mid s \in S\}$.
(c) Ist $S = \{s\}$ eine einelementige Menge, so schreiben wir auch sT statt $\{s\}T$ (bzw. Ts statt $T\{s\}$).
(d) Komplexprodukte können rekursiv auch für mehr als zwei Komplexe gebildet werden.

Das Untergruppenkriterium von Satz 1.1.1 lässt sich mittels des Komplexprodukts auch so ausdrücken: Eine nicht leere Teilmenge U von G ist Untergruppe von G genau dann, wenn gilt: $UU^{-1} \subseteq U$.

DEFINITION 1.1.6
Es sei G eine Gruppe.

(a) $s, t \in G$ heißen konjugiert, falls es ein $g \in G$ gibt, so dass $t = gsg^{-1}$ gilt.
(b) Teilmengen $S, T \subseteq G$ heißen konjugiert (in G), falls es ein $g \in G$ gibt, so dass $T = gSg^{-1}$ gilt.

Man sieht leicht, dass die Konjugiertheit eine Äquivalenzrelation ist. Häufig ist es möglich, eine Untergruppe $U \leq G$ als die kleinste Untergruppe von G zu definieren, die eine gegebene Teilmenge $S \subseteq G$ enthält:

DEFINITION 1.1.7
Es sei $S \subseteq G$.

(a) Das Erzeugnis von S oder die von S erzeugte Untergruppe von S ist

$$\langle S \rangle := \bigcap_{\substack{U \leq G \\ S \subseteq U}} U\,.$$

(b) Falls $S = \{g\}$ für ein $g \in G$, dann $\langle g \rangle := \langle S \rangle$ und $|g| := |\langle g \rangle|$ heißt die Ordnung von g.
(c) Eine Gruppe, die von einem Element erzeugt wird, heißt zyklisch.

BEISPIEL 1.1.8
Es sei $G = \mathfrak{S}_3$ und $\sigma = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}$. Dann ist $\sigma^2 = \sigma^{-1} = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}$ und $\sigma^3 = \mathrm{id}$. Also ist $\langle \sigma \rangle = \{\mathrm{id}, \sigma, \sigma^2\}$ und $|\sigma| = 3$.

SATZ 1.1.2
Es sei G eine Gruppe, $S \subseteq G$. Dann ist

$$\langle S \rangle \;=\; \left\{ g_1 g_2 \cdots g_n \mid n \in \mathbb{N}_0 \;,\; g_i \in S \text{ oder } g_i^{-1} \in S \right\} \;=: X \;.$$

Das leere Produkt bezeichnet die 1.

BEWEIS
Das Untergruppenkriterium (Satz 1.1.1) zeigt, dass X eine Untergruppe von G ist, die S enthält. □

Durch vollständige Induktion zeigt man, dass in einer Gruppe die üblichen Potenzregeln gelten:

SATZ 1.1.3
Es sei G eine Gruppe, $g, h \in G$ und $n, m \in \mathbb{Z}$. Dann gilt:

$$\begin{array}{rcll} g^n g^m & = & g^{n+m} & \\ (g^n)^m & = & g^{nm} & \\ (gh)^n & = & g^n h^n & \text{falls } gh = hg \;. \end{array}$$

1.2. Operation von Gruppen, Bahnen

DEFINITION 1.2.1
Man sagt: Eine Gruppe G operiert auf einer Menge M (von links), wenn eine Abbildung

$$G \times M \to M \quad (g, m) \mapsto gm$$

gegeben ist, mit

(i) $(fg)m = f(gm)\ \forall f, g \in G, m \in M$
(ii) $1m = m\ \forall m \in M$ (1 das Einselement von G).

Analog werden Operationen von Rechts definiert.

Operationen von Gruppen kommen in vielen Gebieten der Mathematik vor. Sie sind jedoch auch in der Gruppentheorie von Bedeutung.

BEISPIEL 1.2.1
V sei ein Vektorraum über einem Körper K, $G = K - \{0\}$ ist eine Gruppe bzgl. der Multiplikation. G operiert auf V durch Skalarmultiplikation:

$$(\lambda, \vec{v}) \;=\; \lambda \vec{v} \;\; (\lambda \in G \;,\; \vec{v} \in V) \;.$$

DEFINITION 1.2.2
Es sei K ein Körper, $n \in \mathbb{N}$. Wir bezeichnen mit $\mathrm{GL}(n, K)$ die Gruppe aller nicht-singulären Matrizen aus $K^{(n,n)}$ bzgl. der Multiplikation. Mit $\mathrm{SL}(n, K)$ bezeichnen wir die Untergruppe aller Matrizen aus $\mathrm{GL}(n, K)$ mit Determinante 1.

BEISPIEL 1.2.2
Es sei K ein Körper, $V = K^n$ der Vektorraum aller n-Tupel über K (als Spaltenvektoren geschrieben). Die Gruppe $\mathrm{GL}(n, K)$ operiert auf V durch Matrixmultiplikation von links:

$$(A, \vec{v}) \;=\; A\vec{v} \;\; (A \in \mathrm{GL}(n, K) \;,\; \vec{v} \in K^n) \,.$$

BEISPIEL 1.2.3
Sei G Gruppe, $M = G$. Die Abbildung $G \times G \to G$ sei gegeben durch $(g, x) \mapsto gx$: G operiert auf sich selbst durch Linksmultiplikation.

DEFINITION 1.2.3
Die Gruppe G operiere von links auf der Menge M und es sei $m \in M$.

(a) $\mathrm{Stab}_G(m) := \{g \in G \mid gm = m\}$ heißt der Stabilisator von m in G.
(b) $Gm := \{gm \mid g \in G\}$ heißt die Bahn von m unter G.
(Bei Operationen von rechts definiert man analog $\mathrm{Stab}_G(m) := \{g \in G \mid mg = m\}$ und $mG = \{mg \mid g \in G\}$)
(c) Die Menge der Bahnen wird mit $G\backslash M$ bezeichnet (bei Operationen von rechts mit M/G).

BEISPIEL 1.2.4
Es sei K ein Körper, $V = K^n$ der Vektorraum aller n-Tupel über K. Die Gruppe $G = (K - \{0\}, \cdot)$ operiert auf V durch Skalarmultiplikation.

(a) Es sei $\vec{v} \neq \vec{0}$. Dann ist die Bahn von $\vec{v}$ gerade $G\vec{v} = \{\lambda\vec{v} \mid \lambda \in K - \{0\}\}$ der von $\vec{v}$ aufgespannte eindimensionale Untervektorraum (Gerade) ohne den Nullvektor. Es ist $\mathrm{Stab}_G(\vec{v}) = \{1\}$.
(b) Es sei $\vec{v} = \vec{0}$. Dann ist die Bahn $G\vec{v} = \{0\}$ und $\mathrm{Stab}_G(\vec{v}) = G$.

SATZ 1.2.1
Die Gruppe G operiere von links auf der Menge M.

(a) *Der Stabilisator $\mathrm{Stab}_G(m)$ ist eine Untergruppe von G.*
(b) *Die Menge aller Bahnen auf M unter G bildet eine Partition auf M, insbesondere sind zwei Bahnen entweder disjunkt oder gleich.*

BEWEIS
(a): Es ist $1 \in \mathrm{Stab}_G(m)$, insbesondere $\mathrm{Stab}_G(m) \neq \emptyset$. Sind $g, h \in \mathrm{Stab}_G(m)$, so ist $(gh^{-1})m = g(h^{-1}m) = gm = m$, denn aus $hm = m$ folgt $m = h^{-1}m$. Also ist $gh^{-1} \in \mathrm{Stab}_G(m)$, d. h. $\mathrm{Stab}_G(m)$ erfüllt das Untergruppenkriterium von Satz 1.1.1. (b): Aus $m = 1m \in Gm$ für alle $m \in M$ folgt

$$M \;=\; \bigcup_{m \in M} Gm \,.$$

Wir zeigen, dass die Bahnen Gm entweder gleich oder disjunkt sind. Dazu seien $x, y \in M$ und $Gx \cap Gy \neq \emptyset$. Dann existiert ein $n \in Gx \cap Gy$. Da $n \in Gx$ gibt es ein $g \in G$ mit $n = gx$. Es gilt $Gn = \{hn \mid h \in G\} = \{h(gx) \mid h \in G\} = \{(hg)x \mid h \in G\} = \{ix \mid i \in G\} = Gx$. Analog erhält man $Gn = Gy$, also ist $Gx = Gy$. □

DEFINITION 1.2.4
G operiere auf einer Menge M (von links oder von rechts). Eine Menge $R \subseteq M$ heißt ein Repräsentantensystem der Operation, falls es zu jeder Bahn B bzgl. der Operation genau ein $r \in R$ mit $r \in B$ gibt.

1.3. Nebenklassen

Wir kommen nun zu einem besonders wichtigen Spezialfall einer Gruppenoperation. Es sei U eine Untergruppe der Gruppe G. Dann operiert U auf G durch Multiplikation von links (oder rechts). Ist G kommutativ, so braucht zwischen links und rechts natürlich nicht unterschieden zu werden. In diesem Abschnitt werden wir die Bahnen bzgl. dieser Operation betrachten, die so genannten Nebenklassen von U. Eines der bekanntesten Beispiele entstammt der elementaren Zahlentheorie.

DEFINITION 1.3.1
Es sei $m \in \mathbb{N}$. Dann bedeute $(m\mathbb{Z}, +)$ die Untergruppe von $(\mathbb{Z}, +)$ der Vielfachen von m: $m\mathbb{Z} = \{k \cdot m \mid k \in \mathbb{Z}\}$.

BEISPIEL 1.3.1
Sei $m = 3$. Es ist $3\mathbb{Z} = \{\ldots, -6, -3, 0, 3, 6, \ldots\}$. Die Elemente $0, 1, 2$ gehören zu den Bahnen

$$\begin{array}{rcl} 0 + 3\mathbb{Z} & = & \{\ldots, -6, -3, 0, 3, 6, 9, \ldots\} \\ 1 + 3\mathbb{Z} & = & \{\ldots, -8, -5, -2, 1, 4, 7, \ldots\} \\ 2 + 3\mathbb{Z} & = & \{\ldots, -7, -4, -1, 2, 5, 8, \ldots\} \end{array}$$

DEFINITION 1.3.2
Es sei $m \in \mathbb{N}$. dann heißen die Bahnen bzgl. der Operation der Untergruppe $(m\mathbb{Z}, +)$ auf $(\mathbb{Z}, +)$ durch Addition die Restklassen mod m. Die Restklasse $a + m\mathbb{Z}$ wird auch mit $a \bmod m$ bezeichnet. Ein Repräsentantensystem der Operation wird auch als vollständiges Restsystem mod m bezeichnet. Nach Definition 1.2.3 wird die Menge der Restklassen mit $\mathbb{Z}/m\mathbb{Z}$ bezeichnet. $a, b \in \mathbb{Z}$ heißen kongruent modulo m ($a \equiv b \bmod m$) genau dann, wenn sie derselben Restklasse mod m angehören.

BEMERKUNG 1.3.1
Die Restklassen mod 3 sind nach dem obigen Beispiel

$$\begin{array}{rcccccccc} \bar{0} & = & 0 + 3\mathbb{Z} & = & 0 \bmod 3 & = & 3 \bmod 3 & = & \cdots \\ \bar{1} & = & 1 + 3\mathbb{Z} & = & 1 \bmod 3 & = & 4 \bmod 3 & = & \cdots \\ \bar{2} & = & 2 + 3\mathbb{Z} & = & 2 \bmod 3 & = & 5 \bmod 3 & = & \cdots \end{array}$$

und $\{0, 1, 2\}$ ist ein vollständiges Restsystem, ebenso $\{-1, 0, 1\}$ und $\{9, -8, 2\}$. Es ist $|\mathbb{Z}/3\mathbb{Z}| = 3$.

Zur Untersuchung des allgemeinen Falles benötigen wir die Division mit Rest.

SATZ 1.3.1 (Division mit Rest)
Zu $a, b \in \mathbb{Z}$ mit $b \neq 0$ gibt es genau ein Paar ganzer Zahlen q, r das die beiden Bedingungen $a = qb + r$ und $0 \leq r < |b|$ erfüllt.

BEWEIS
Es genügt, den Fall $b > 0$ zu betrachten. Da r durch q vermöge $r = a - qb$ festgelegt ist, bedeutet die Behauptung die Existenz einer einzigen Zahl $q \in \mathbb{Z}$, die $qb \leq a < qb + b$ erfüllt. Das ist gleichbedeutend mit der Bedingung $q \leq ab^{-1} < q+1$, welcher genau ein ganzes q genügt, nämlich $q = [ab^{-1}]$, wobei wie üblich $[x]$ für $x \in \mathbb{R}$ die größte ganze Zahl $\leq x$ ist. □

DEFINITION 1.3.3
Die in Satz 1.3.1 durch a und b definierte Zahl r heißt der Rest von a bzgl. der Division durch b.

SATZ 1.3.2
Es seien $m \in \mathbb{N}$ und $a, b \in \mathbb{Z}$.

(a) $a \equiv b \bmod m$ *genau dann, wenn a und b bzgl. der Division durch m gleiche Reste lassen.*
(b) *Es gibt genau m Restklassen mod m, nämlich*

$$\mathbb{Z}/m\mathbb{Z} = \{0 \bmod m, 1 \bmod m, \ldots, (m-1) \bmod m\} .$$

BEWEIS
(a): $\Rightarrow$: Es seien $a, b \equiv c \bmod m$,d. h. es gibt $k, k' \in \mathbb{Z}$ mit $a = km+c$ und $b = k'm+c$. Division mit Rest ergibt: $a = lm+r$ bzw. $b = l'm+r'$ mit $0 \leq r, r' \leq m-1$. Dann folgt: $b-a = (k'-k)m = (l'-l)m+r-r'$, also $r-r' = dm$ mit $d \in \mathbb{Z}$. Wegen $-m < r-r' < m$ folgt aber $d = 0$, also $r = r'$. $\Leftarrow$: Ist $a = km+r$ und $b = k'm+r$, so gehören a und b beide zur Restklasse $r \bmod m$. (b): Satz 1.3.1 zeigt, dass jedes $a \in \mathbb{Z}$ zu einer der Restklassen $0 \bmod m, 1 \bmod m, \ldots (m-1) \bmod m$ gehört. Nach a) sind diese Restklassen alle verschieden. □

BEISPIEL 1.3.2
Nach Satz 1.3.2 ist $\{0, \ldots, m-1\}$ ein vollständiges Restsystem mod m (kleinstes nicht-negatives Restsystem). Andere vollständige Restsysteme mod m sind:

$\{1, 2, \ldots, m\}$ (kleinstes positives Restsystem)

$\{0, \pm 1, \pm 2, \ldots, \frac{1}{2}(m-1)\}$ (absolut kleinstes Restsystem, n ungerade)

$\{0, \pm 1, \pm 2, \ldots, \frac{1}{2}m\}$ (absolut kleinstes Restsystem, n gerade)

Wir verallgemeinern den Begriff der Restklassen und der Kongruenz auf die allgemeine Situation, dass eine Gruppe G und eine Untergruppe $U \leq G$ gegeben sind.

DEFINITION 1.3.4
Es sei G eine Gruppe, $U \leq G$. Dann operiert U auf G durch Linksmultiplikation (bzw. Rechtsmultiplikation) auf G. Die Bahnen dieser Operation heißen Rechtsnebenklassen (bzw. Linksnebenklassen) von U in G. Zwei Elemente $g, h \in G$ heißen rechtskongruent modulo U (geschrieben $g \equiv_r h \bmod U$) bzw. linkskongruent modulo U (geschrieben $g \equiv_l h \bmod U$), wenn sie derselben Rechts- (bzw. Links-)nebenklasse modulo U angehören.

BEMERKUNG 1.3.2
Aus Definition 1.2.3 ergibt sich für die Menge der Rechts- (Links-)nebenklassen die Bezeichnung $U\backslash G$ bzw. G/U.

Man sieht sofort die Gültigkeit von

SATZ 1.3.3
Es sei G eine Gruppe und $g \in G$. Die Rechts- (bzw. Links-)nebenklasse von g ist gegeben durch Ug (bzw. gU) im Sinn von Definition 1.1.5. Es seien $g, h \in G$, dann gilt:

$$\begin{aligned} g \equiv_l h \bmod U &\Leftrightarrow h^{-1}g \in U \\ g \equiv_r h \bmod U &\Leftrightarrow hg^{-1} \in U \end{aligned}$$

Für endliche Gruppen G führt das Konzept der Nebenklassen zu einer wichtigen Beziehung zwischen der Ordnung der Gesamtgruppe G und der Ordnung einer Untergruppe U.

SATZ 1.3.4 (Lagrange)
Es sei G eine endliche Gruppe und $U \leq G$. Dann teilt die Ordnung der Gruppe U die Ordnung von G. Die Anzahl der Rechtsnebenklassen von U in G ist gleich der Anzahl der Linksnebenklassen, und es gilt $|U\backslash G| = |G/U| = |G| \,/\, |U|$.

BEWEIS
Nach Satz 1.2.1(b) bildet die Menge aller Rechts-(Links-)nebenklassen eine Partition von G: $G = U \,\dot\cup\, Ug_2 \,\dot\cup\, \cdots \,\dot\cup\, Ug_l$. Die Abbildung $U \to Ug$, $u \mapsto ug$ ist eine Bijektion. Also gilt $|U| = |Ug_i|$ für alle $i = 1, \ldots, l$ und damit $l \cdot |U| = |G|$, d. h. $|G| \,/\, |U| = |U\backslash G| = |G/U|$. □

DEFINITION 1.3.5
Es sei U Untergruppe einer Gruppe G. Die Anzahl der Links-(Rechts-)nebenklassen von U in G heißt der Index von U in G, und wird mit $(G : U)$ bezeichnet.

BEMERKUNG 1.3.3
Satz 1.3.4 lässt sich also auch formulieren als $|G| = (G : U) \cdot |U|$.

Wir schließen eine allgemeine Folgerung für die Operation einer Gruppe an.

SATZ 1.3.5 (Bahnensatz)
Die Gruppe G operiere (von links) auf der Menge M mit $m \in M$. Dann gibt es eine Bijektion φ zwischen den Elementen der Bahn von m und den Linksnebenklassen $G/\mathrm{Stab}_G(m)$, definiert durch

$$\varphi : \begin{cases} Gm & \to & G/\mathrm{Stab}_G(m) \\ gm & \mapsto & g\mathrm{Stab}_G(m) \end{cases} .$$

Insbesondere gilt

$$|Gm| \;=\; \frac{|G|}{|\mathrm{Stab}_G(m)|} .$$

BEWEIS
Es sei $G = \mathrm{Stab}_G(m) \,\dot\cup\, g_1\mathrm{Stab}_G(m) \,\dot\cup\, \cdots \,\dot\cup\, g_l\mathrm{Stab}_G(m)$ die Partition von G in die Linksnebenklassen von $\mathrm{Stab}_G(m)$ in G. Zu zeigen: φ ist wohldefiniert. Es seien $g, h \in G$. $gm = hm \Leftrightarrow h^{-1}gm = m \Leftrightarrow h^{-1}g \in \mathrm{Stab}_G(m) \Leftrightarrow g\mathrm{Stab}_G(m) = h\mathrm{Stab}_G(m)$. Das zeigt auch die Injektivität von φ. Die Surjektivität ist klar. □

1.4. Normalteiler, Faktorgruppen

Wir betrachten die Menge G/U der (Links-)Nebenklassen der Untergruppe U einer Gruppe G. In vielen Fällen wird die Menge G/U ebenfalls zu einer Gruppe, wenn die Nebenklassen mittels des Komplexprodukts multipliziert werden. Wir beginnen mit dem bekannten Beispiel $G = (\mathbb{Z}, +)$, $U = m\mathbb{Z}$ und illustrieren die Addition auf der Restklassenmenge $\mathbb{Z}/m\mathbb{Z}$ für den Fall $m = 3$ anhand einer „unendlichen Verknüpfungstafel". Hierbei gruppieren wir Elemente derselben Restklasse zusammen:

$+$	$\cdots$	-3	0	3	6	$\cdots$	$\cdots$	-2	1	4	7	$\cdots$
$\vdots$		$\vdots$	$\vdots$	$\vdots$	$\vdots$			$\vdots$	$\vdots$	$\vdots$	$\vdots$	
-3	$\cdots$	-6	-3	0	3	$\cdots$	$\cdots$	-5	-2	1	4	$\cdots$
0	$\cdots$	-3	0	3	6	$\cdots$	$\cdots$	-2	1	4	7	$\cdots$
3	$\cdots$	0	3	6	9	$\cdots$	$\cdots$	1	4	7	10	$\cdots$
6	$\cdots$	3	6	9	12	$\cdots$	$\cdots$	4	7	10	13	$\cdots$
$\vdots$		$\vdots$	$\vdots$	$\vdots$	$\vdots$			$\vdots$	$\vdots$	$\vdots$	$\vdots$	
$\vdots$		$\vdots$	$\vdots$	$\vdots$	$\vdots$			$\vdots$	$\vdots$	$\vdots$	$\vdots$	
-5	$\cdots$	-11	-8	-5	-2	$\cdots$	$\cdots$					
-2	$\cdots$	-8	-5	-2	1	$\cdots$	$\cdots$					
1	$\cdots$											

Die Gruppe $(\mathbb{Z}/m\mathbb{Z}, +)$ ist ein „Miniaturmodell" der ursprünglichen Gruppe $\mathbb{Z}$. Die Abbildung $\Phi : \mathbb{Z} \to \mathbb{Z}/m\mathbb{Z}$, $a \mapsto a \bmod m$ ist ein Homomorphismus der Gruppe $(\mathbb{Z}, +)$ auf die Gruppe $(\mathbb{Z}/m\mathbb{Z}, +)$.

Verknüpfungstafel für m=3:

$+$	$0 \bmod 3$	$1 \bmod 3$	$2 \bmod 3$
$0 \bmod 3$	$0 \bmod 3$	$1 \bmod 3$	$2 \bmod 3$
$1 \bmod 3$	$1 \bmod 3$	$2 \bmod 3$	$0 \bmod 3$
$2 \bmod 3$	$2 \bmod 3$	$0 \bmod 3$	$1 \bmod 3$

Entscheidend für das Funktionieren der Konstruktion ist die Tatsache, dass das Komplexprodukt zweier Nebenklassen wieder eine Nebenklasse ist. Dies ist sicher bei jeder abelschen Gruppe G und einer beliebigen Untergruppe $U \leq G$ der Fall:

(1) $(gU)(hU) = (gh)U$, da $UU = U$ und
(2) $Uh = hU$.

Allgemeiner gilt es, da es aus (1) und (2) folgt, in jedem Fall, in dem Rechtsnebenklassen und Linksnebenklassen zusammenfallen. Für jedes Paar (G, U) mit dieser Eigenschaft lässt sich die Menge G/U der Nebenklassen mittels des Komplexprodukts zu einer Gruppe machen, der so genannten Faktorgruppe G/U. Das Einselement von G/U ist die Nebenklasse $1U = U$ des Einselements von G, und das Inverse von gU ist $g^{-1}U$. Bei nicht abelschen Gruppen G kann es Paare (G, U) mit $U \leq G$ geben, in denen die Konstruktion der Faktorgruppe G/U möglich ist, und solche, in denen es nicht möglich ist.

Beispiel 1.4.1
Sei $G = \mathfrak{S}_3 = \{\mathrm{id}, \sigma, \sigma^2, \tau, \sigma\tau, \sigma^2\tau\}$ mit

$$\sigma = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix} \ , \ \tau = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix} .$$

Es gilt $\tau\sigma = \sigma^2\tau$ und $\tau\sigma^2 = \sigma\tau$. Wir betrachten die Untergruppe $U_1 = \{\mathrm{id}, \sigma, \sigma^2\}$:

	$\boxed{\text{id}\cdot U_1}$			$\boxed{\tau\cdot U_1}$		
$\circ$	id	σ	σ^2	τ	$\tau\sigma$	$\tau\sigma^2$
id	id	σ	σ^2	τ	$\tau\sigma$	$\tau\sigma^2$
σ	σ	σ^2	id	$\tau\sigma$	$\tau\sigma^2$	τ
σ^2	σ^2	id	σ	$\tau\sigma^2$	τ	$\tau\sigma$
τ	τ	$\tau\sigma^2$	$\tau\sigma$	id	σ^2	σ
$\tau\sigma$	$\tau\sigma$	τ	$\tau\sigma^2$	σ	id	σ^2
$\tau\sigma^2$	$\tau\sigma^2$	$\tau\sigma$	τ	σ^2	σ	id

$\xrightarrow[\phi]{}$

$\circ$	$\text{id}\cdot U_1$	$\tau\cdot U_1$
$\text{id}\cdot U_1$	$\text{id}\cdot U_1$	$\tau\cdot U_1$
$\tau\cdot U_1$	$\tau\cdot U_1$	$\text{id}\cdot U_1$

Wir haben die folgenden Eigenschaften:

(i) $g_1 \equiv_l g_2 \bmod U_1,\ h_1 \equiv_l h_2 \bmod U_1 \Rightarrow\ \ g_1h_1 \equiv_l g_2h_2 \bmod U_1$
(dasselbe gilt für die Rechtsnebenklassen)
(ii) Linksnebenklassen U_1 und $\tau U_1 = \{\tau, \tau\sigma, \tau\sigma^2\}$ entsprechen den Rechtsnebenklassen U_1 und $U_1\tau = \{\tau, \sigma\tau = \tau\sigma^2, \sigma^2\tau = \tau\sigma\}$.
(iii) Das Komplexprodukt zweier Nebenklassen ist wieder eine Nebenklasse.

Beispiel 1.4.2
Sei $G = \mathfrak{S}_3 = \{\text{id}, \sigma, \sigma^2, \tau, \sigma\tau, \sigma^2\tau\}$. Wir betrachten die Untergruppe $U_2 = \{\text{id}, \tau\}$:

Linksnebenklassen: $\quad U_2 = \{\text{id}, \tau\} \quad \sigma U_2 = \{\sigma, \sigma\tau\} \quad \sigma^2 U_2 = \{\sigma^2, \sigma^2\tau\}$

Rechtsnebenklassen: $\quad U_2 = \{\text{id}, \tau\} \quad U_2\sigma = \{\sigma, \sigma^2\tau\} \quad U_2\sigma^2 = \{\sigma^2, \sigma\tau\}$

	$\boxed{\text{id}\cdot U_2}$		$\boxed{\sigma\cdot U_2}$		$\boxed{\sigma^2\cdot U_2}$	
$\circ$	id	σ	σ^2	τ	$\tau\sigma$	$\tau\sigma^2$
id	id	σ	σ^2	τ	$\tau\sigma$	$\tau\sigma^2$
σ	σ	σ^2	id	$\tau\sigma$	$\tau\sigma^2$	τ
σ^2	σ^2	id	σ	$\tau\sigma^2$	τ	$\tau\sigma$
τ	τ	$\tau\sigma^2$	$\tau\sigma$	id	σ^2	σ
$\tau\sigma$	$\tau\sigma$	τ	$\tau\sigma^2$	σ	id	σ^2
$\tau\sigma^2$	$\tau\sigma^2$	$\tau\sigma$	τ	σ^2	σ	id

Wir sehen, dass keine der Eigenschaften, die in Beispiel 1.4.1 die Konstruktion einer Faktorgruppe ermöglicht haben, hier erfüllt ist.

Es stellt sich heraus, dass jede der drei Eigenschaften aus Beispiel 1.4.1 jeweils die beiden anderen impliziert. Wir legen eine dieser Eigenschaften der Definition des Normalteilers zugrunde.

Definition 1.4.1
Ein Normalteiler einer Gruppe G (geschrieben $N \trianglelefteq G$) ist eine Untergruppe N von G, für

die die Relation $\equiv_l \bmod N$ gleich der Relation $\equiv_r \bmod N$ ist. Man schreibt dann für beide Relationen einfach $\equiv \bmod N$.

SATZ 1.4.1
Es sei N eine Untergruppe der Gruppe G. Folgende Aussagen sind äquivalent:

(i) *N ist Normalteiler,*
(ii) *$gN = Ng$ für alle $g \in G$,*
(iii) *$gNg^{-1} = N$ für alle $g \in G$,*
(iv) *$gNg^{-1} \subseteq N$ für alle $g \in G$,*
(v) *$(gN)(hN) = (gh)N$ für alle $g, h \in G$,*
(vi) *$(Ng)(Nh) = N(gh)$ für alle $g, h \in G$,*
(vii) *Aus $g_1 \equiv_l g_2 \bmod N$ und $h_1 \equiv_l h_2 \bmod N$ folgt $g_1 h_1 \equiv_l g_2 h_2 \bmod N$,*
(viii) *Aus $g_1 \equiv_r g_2 \bmod N$ und $h_1 \equiv_r h_2 \bmod N$ folgt $g_1 h_1 \equiv_r g_2 h_2 \bmod N$.*

BEWEIS
(i) ist äquivalent zu (ii), da die Links- (bzw. Rechts-)nebenklassen die zu den Äquivalenzrelationen $\equiv_l$ (bzw. $\equiv_r$) gehörigen Äquivalenzklassen sind. Äquivalenzklassen zweier Äquivalenzrelationen stimmen genau dann überein, wenn die Äquivalenzrelationen übereinstimmen. (ii)⇒(iii): Mit $gN = Ng$ gilt auch $gNg^{-1} = (Ng)g^{-1} = N \cdot 1_G = N$. (iii)⇒(iv) ist trivial. (iv)⇒(i): Es gilt $g \equiv_l h \bmod N \Rightarrow h^{-1}g \in N \Rightarrow_{(iv)} gh^{-1} = g(h^{-1}g)g^{-1} \in gNg^{-1} \subseteq N \Rightarrow g \equiv_r h \bmod N$. Analog folgt aus $g \equiv_r h \bmod N$ auch $g \equiv_l h \bmod N$. Damit sind (i) bis (iv) als äquivalent nachgewiesen. (ii)⇒(v): Wegen $NN = N$ gilt $(gN)(hN) = g(Nh)N = g(hN)N = (gh)N$. (v)⇒(iv): Insbesondere ist $(gN)(g^{-1}N) = gg^{-1}N = N$. Annahme: $gNg^{-1} \not\subseteq N$. Dann ist $(gNg^{-1})N \not\subseteq N; \Rightarrow; (gN)(g^{-1}N) \not\subseteq N$, Widerspruch. Damit folgt die Äquivalenz von (i) bis (iv) mit (v), und analog mit (vi). (vii)⇒(iv): Es seien $g \in G$ und $n \in N$. Aus $n \equiv_l 1 \bmod N$ und $g^{-1} \equiv_l g^{-1} \bmod N$ folgt: $ng^{-1} \equiv_l g^{-1} \bmod N \Rightarrow gng^{-1} \in N \Rightarrow gNg^{-1} \subseteq N$, also (iv). (ii)⇒(vii): Aus $g_1 \equiv_l g_2 \bmod N$ und $h_1 \equiv_l h_2 \bmod N$ folgt $g_1 \in g_2 N$ und $h_1 \in h_2 N$. Also ist $g_1 h_1 \in g_2(Nh_2)N = g_2(h_2 N) = (g_2 h_2)N$. Damit folgt die Äquivalenz (i) bis (vi) mit (vii). Ebenso folgt die Äquivalenz von (i) bis (vi) mit (viii). □

DEFINITION 1.4.2
Zusätzlich zum Begriff des Homomorphismus definiert man:

(a) Ein surjektiver Homomorphismus heißt Epimorphismus
(b) Ein injektiver Homomorphismus heißt Monomorphismus
(c) Ein Isomorphismus einer Gruppe G auf sich selbst heißt Automorphismus.

SATZ 1.4.2
Es sei G eine Gruppe, N ein Normalteiler von G. Dann bildet die Menge G/N der Nebenklassen von N in G eine Gruppe mit dem Komplexprodukt als Verknüpfung. Die Abbildung $\Phi : G \to G/N$, $g \mapsto gN$ ist ein Epimorphismus von der Gruppe G auf die Gruppe G/N. (G/N ist also homomorphes Bild von G)

BEWEIS
Die Verknüpfung ist abgeschlossen wegen Eigenschaft (v) aus Satz 1.4.1. Das Assoziativgesetz von G überträgt sich auf G/N. Das neutrale Element ist $1_{N/G} = 1 \cdot N = N \in G/N$. Das Inverse von gN ist $g^{-1}N$. □

DEFINITION 1.4.3
Die Abbildung $\Phi : G \to G/N$ heißt auch kanonischer Epimorphismus.

Beispiele für Normalteiler

BEISPIEL 1.4.3
Eine Untergruppe einer abelschen Gruppe ist stets ein Normalteiler.

BEISPIEL 1.4.4
Jede Gruppe G hat die trivialen Normalteiler $\{1_G\}$ und G.

BEISPIEL 1.4.5
Es sei K ein Körper, $n \in \mathbb{N}$. Dann ist $\mathrm{SL}(n, K)$ ein Normalteiler von $\mathrm{GL}(n, K)$.

BEWEIS
Es sei $S \in \mathrm{SL}(n, K)$ und $G \in \mathrm{GL}(n, K)$. Dann ist $\det(GSG^{-1}) = \det(G)\det(S)\det(G)^{-1} = \det(S) = 1_K$ nach dem Determinantenmultiplikationssatz. Damit ist $G \cdot \mathrm{SL}(n, K) \cdot G^{-1} \subseteq \mathrm{SL}(n, K)$, und nach Eigenschaft (iv) von Satz 1.4.1 ist $\mathrm{SL}(n, K)$ ein Normalteiler von $\mathrm{GL}(n, K)$. □

BEISPIEL 1.4.6
Es sei G eine Gruppe und N eine Untergruppe von G mit Index $(G : N) = 2$. Dann sind die Linksnebenklassen von G unter N gleich den Rechtsnebenklassen. Nach Satz 1.4.1(ii) ist N ein Normalteiler.

DEFINITION 1.4.4
Es sei G eine Gruppe. Die Menge $Z(G)$ der Elemente von G, die mit allen Gruppenelementen vertauschbar sind, heißt das Zentrum von G. Also: $Z(G) = \{h \in G \mid \forall g \in G : \ gh = hg\}$.

SATZ 1.4.3
Das Zentrum einer Gruppe G ist ein Normalteiler von G.

BEWEIS
Es sei $h \in Z(G)$ und $g \in G$. Dann ist $ghg^{-1} = h \in Z(G)$. □

1.5. Homomorphie- und Isomorphiesätze

Wir haben gesehen, dass jede Faktorgruppe G/N ein homomorphes Bild der Gruppe G ist. Hier soll nun die Umkehrung gezeigt werden: Jedes homomorphe Bild einer Gruppe ist isomorph zu einer gewissen Faktorgruppe.

DEFINITION 1.5.1
Es sei $\Phi : G \to H$ ein Homomorphismus einer Gruppe G in eine Gruppe H mit Einselement 1_H. Unter dem Kern von Φ versteht man die Menge $\mathrm{Ker}(\Phi) = \{g \in G \mid \Phi(g) = 1_H\}$.

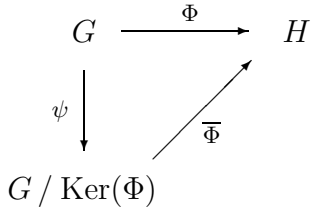
SATZ 1.5.1 (Homomorphiesatz)
Es seien G und H Gruppen mit Einselementen 1_G bzw. 1_H und $\Phi : G \to H$ ein Homomorphismus. Dann gilt:

(a) $\mathrm{Ker}(\Phi)$ *ist ein Normalteiler von G und $\Phi(G)$ ist eine Untergruppe von H, und es ist* $\Phi(1_G) = 1_H$.

(b) $G \,/\, \mathrm{Ker}(\Phi) \cong \Phi(G)$, *und zwar wird ein solcher Isomorphismus* $\overline{\Phi}$ *geliefert durch*

$$\overline{\Phi} = \begin{cases} G \,/\, \mathrm{Ker}(\Phi) & \to & \Phi(G) \\ g\mathrm{Ker}(\Phi) & \mapsto & \Phi(g) \end{cases}.$$

Ist ψ *der kanonische Epimorphismus von* G *auf* $G \,/\, \mathrm{Ker}(\Phi)$, *so ist* $\Phi = \overline{\Phi} \circ \psi$, *d. h. das Diagramm*



ist kommutativ.

(c) Φ *ist ein Monomorphismus genau dann, wenn* $\mathrm{Ker}(\Phi) = \{1_G\}$ *ist.*

BEWEIS
(a): $\forall g \in G$ gilt: $\Phi(g) = \Phi(1_G \cdot g) = \Phi(1_G)\Phi(g)$. Daher ist $\Phi(1_G) = 1_H$. Es seien $h_1, h_2 \in \Phi(G)$, beispielsweise $h_1 = \Phi(g_1)$ und $h_2 = \Phi(g_2)$. Dann ist $h_1 h_2^{-1} = \Phi(g_1 g_2^{-1})$, also $h_1 h_2^{-1} \in \Phi(G)$. Damit erfüllt $\Phi(G)$ das Untergruppenkriterium (Satz 1.1.1). Es sei $k \in \mathrm{Ker}(\Phi)$ und $g \in G$. Dann ist $\Phi(gkg^{-1}) = \Phi(g)\Phi(k)\Phi(g)^{-1} = \Phi(g) \cdot 1_H \cdot \Phi(g)^{-1} = 1_H$, also ist auch $gkg^{-1} \in \mathrm{Ker}(\Phi)$, d. h. $g\mathrm{Ker}(\Phi)g^{-1} \subseteq \mathrm{Ker}(\Phi)$. Nach Satz 1.4.1(iv) ist $\mathrm{Ker}(\Phi)$ ein Normalteiler von G. (b): Wir zeigen zunächst, dass die Abbildung $\overline{\Phi} : G \,/\, \mathrm{Ker}(\Phi) \to \Phi(G)$ wohldefiniert ist, d. h. nicht von dem Repräsentanten g der Nebenklasse $g\mathrm{Ker}(\Phi)$ abhängt: $g_1\mathrm{Ker}(\Phi) = g_2\mathrm{Ker}(\Phi)$ mit $g_1, g_2 \in G$ impliziert $g_1 = g_2 \cdot k$ für ein $k \in \mathrm{Ker}(\Phi)$, daraus folgt $\Phi(g_1) = \Phi(g_2)\Phi(k) = \Phi(g_2)$. Relationstreue: $\overline{\Phi}(g_1\mathrm{Ker}(\Phi)g_2\mathrm{Ker}(\Phi)) = \overline{\Phi}(g_1g_2\mathrm{Ker}(\Phi)) = \Phi(g_1g_2) = \Phi(g_1)\Phi(g_2) = \overline{\Phi}(g_1\mathrm{Ker}(\Phi))\overline{\Phi}(g_2\mathrm{Ker}(\Phi))$. Injektivität: $\overline{\Phi}(g_1\mathrm{Ker}(\Phi)) = \overline{\Phi}(g_2\mathrm{Ker}(\Phi)) \Rightarrow \Phi(g_1) = \Phi(g_2) \Rightarrow 1_H = \Phi(g_1)\Phi(g_2)^{-1} = \Phi(g_1g_2^{-1}) \Rightarrow g_1g_2^{-1} \in \mathrm{Ker}(\Phi) \Rightarrow g_1 \in g_2\mathrm{Ker}(\Phi) \Rightarrow g_1\mathrm{Ker}(\Phi) = g_2\mathrm{Ker}(\Phi)$. (c): ist Φ injektiv, so folgt $\{1_G\} = \Phi^{-1}(\{1_H\}) = \mathrm{Ker}(\Phi)$. Sei andererseits $\mathrm{Ker}(\Phi) = \{1_G\}$, dann gilt $\Phi(g_1) = \Phi(g_2) \Rightarrow g_1\mathrm{Ker}(\Phi) = g_2\mathrm{Ker}(\Phi) \Rightarrow g_1 = g_2$ nach (b). □

BEISPIEL 1.5.1
Es sei K ein Körper, $G = \mathrm{GL}(n, K)$ und $H = (K - \{0\}, \cdot)$. Nach dem Determinantenmultiplikationssatz ist $\Phi : G \to H$, $A \mapsto \det(A)$ ein Homomorphismus. Wegen

$$\Phi\left(\begin{pmatrix} \lambda & 0 & \cdots & 0 \\ 0 & 1 & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & 1 \end{pmatrix}\right) = \lambda$$

für $\lambda \in H$ ist $\Phi(G) = H$. Nach Satz 1.5.1 ist $K - \{0\} \cong \mathrm{GL}(n, K) \,/\, \mathrm{SL}(n, K)$, da $\mathrm{Ker}(\Phi) = \mathrm{SL}(n, K)$.

Als Anwendung bestimmen wir $|\mathrm{SL}(n, K)|$ für einen endlichen Körper K mit q Elementen. Zunächst bestimmen wir $|\mathrm{GL}(n, K)|$. Eine Matrix $A \in K^{(n,n)}$ gehört zu $\mathrm{GL}(n, K)$ genau dann, wenn ihre Zeilenvektoren linear unabhängig sind. Dies ergibt $q^n - 1$ Möglichkeiten für den ersten Zeilenvektor $\vec{z}_1$, der der einzigen Bedingung $\vec{z}_1 \neq \vec{0}$ genügen muss. Sind j Zeilenvektoren $\vec{z}_1, \ldots, \vec{z}_j$ schon gewählt, so darf $\vec{z}_{j+1}$ nicht in dem von $\vec{z}_1, \ldots, \vec{z}_j$ erzeugten Untervektorraum

V_j von K^n liegen. Es ist $V_j = \{\sum_{i=1}^{j} \lambda_i \vec{z}_i \mid \lambda_i \in K\}$, also $|V_j| = q^j$. Für die Wahl von $\vec{z}_{j+1}$ gibt es daher $q^n - q^j$ Möglichkeiten. Damit ist

$$\mathrm{GL}(n,K) = \prod_{j=0}^{n-1}(q^n - q^j)\,.$$

Aus $(K - \{0\},\ \cdot\ ) \cong \mathrm{GL}(n,K) \,/\, \mathrm{SL}(n,K)$ folgt

$$|\mathrm{SL}(n,K)| \;=\; \frac{1}{q-1}|\mathrm{GL}(n,K)| \;=\; q^{n-1}\prod_{j=0}^{n-2}(q^n - q^j)\,.$$

Als zweites Beispiel betrachten wir Automorphismengruppen. Dazu zunächst

DEFINITION 1.5.2
Es sei G eine Gruppe:

(a) Die Menge der Automorphismen von G bildet offenbar eine Gruppe bzgl. der Hintereinanderausführung, die Automorphismengruppe $\mathrm{Aut}(G)$.
(b) $\tau \in \mathrm{Aut}(G)$ heißt innerer Automorphismus von G, wenn τ von der Form $\tau : G \to G,\ h \mapsto ghg^{-1}$ für ein festes $g \in G$ ist. Die Menge der inneren Automorphismen bildet offenbar eine Untergruppe von $\mathrm{Aut}(G)$, die Gruppe der inneren Automorphismen $\mathrm{Inn}(G)$.

BEISPIEL 1.5.2
Es sei G eine Gruppe. Für $g \in G$ sei der innere Automorphismus τ_g definiert durch $\tau_g : G \to G,\ h \mapsto ghg^{-1}$. Die Abbildung $\Phi : G \to \mathrm{Inn}(G),\ g \mapsto \tau_g$ ist offenbar ein Epimorphismus. Wir bestimmen $\mathrm{Ker}(\Phi)$. Es gilt: $g \in \mathrm{Ker}(\Phi) \Leftrightarrow \tau_g = \mathrm{id} \Leftrightarrow \forall h \in G :\ ghg^{-1} = h \Leftrightarrow g \in Z(G)$. Nach Satz 1.5.1 ist also $\mathrm{Inn}(G) \cong G \,/\, Z(G)$.

SATZ 1.5.2 (1. Isomorphiesatz)
Es sei G eine Gruppe, $U \leq G$ eine Untergruppe und $N \trianglelefteq G$ ein Normalteiler. Dann ist

(a) $UN \leq G$.
(b) $N \trianglelefteq UN$.
(c) $(U \cap N) \trianglelefteq U$.

Die Abbildung

$$\overline{\Phi} \;=\; \begin{cases} U \,/\, (U \cap N) & \to & (UN) \,/\, N \\ u(U \cap N) & \mapsto & uN \end{cases}$$

ist ein Isomorphismus, insbesondere gilt $U \,/\, (U \cap N) \;\cong\; (UN) \,/\, N$.

BEWEIS
(a): $UN(UN)^{-1} = UNN^{-1}U^{-1} = UNU^{-1} = UN$. Also erfüllt UN das Untergruppenkriterium (Satz 1.1.1). (b): ist trivial. (c): Die Abbildung $\Phi : U \to G/N, u \mapsto uN$ ist ein Homomorphismus mit Bild $\Phi(U) = UN$ und Kern $\mathrm{Ker}(\Phi) = U \cap N$. Die Behauptung folgt aus Satz 1.5.1. □

SATZ 1.5.3 (2. Isomorphiesatz)
Es sei G eine Gruppe mit Normalteilern M und N. Es sei $N \subseteq M$, dann gilt:

(a) $(M/N) \trianglelefteq (G/N)$.

(b) *Die Abbildung*

$$\overline{\Phi} \;=\; \begin{cases} (G/N)\,/\,(M/N) & \to & G\,/\,M \\ (gN)(M/N) & \mapsto & gM \end{cases}$$

ist ein Isomorphismus, insbesondere gilt $(G/N)\,/\,(M/N) \;\cong\; G\,/\,M$.

BEWEIS
(a): ist trivial. (b): Wir betrachten die Abbildung $\Phi : (G/N) \to (G/M)$, $gN \mapsto gM$. Sie ist wohldefiniert, denn es gilt $g_1N = g_2N \Rightarrow g_2^{-1}g_1 \in N \Rightarrow g_2^{-1}g_1 \in M \Rightarrow g_1M = g_2M$. Φ ist ein Epimorphismus mit Kern $\mathrm{Ker}(\Phi) = M/N$. Das Resultat folgt aus dem Homomorphiesatz 1.5.1. □

SATZ 1.5.4
Es sei G eine Gruppe und N ein Normalteiler von G, weiter sei $\Phi : G \to G/N$, $g \mapsto gN$ der kanonische Epimorphismus. Dann gilt:

(a) *Für jede Untergruppe $U \leq G$ ist $\Phi(U) = (UN)/N$ eine Untergruppe von G/N.*
(b) *Für jede Untergruppe $\overline{U}$ von G/N ist $\Phi^{-1}(\overline{U})$ eine Untergruppe von G mit $N \trianglelefteq \Phi^{-1}(\overline{U})$, und es ist $\overline{U} = \Phi^{-1}(\overline{U})/N$.*
(c) *Die Zuordnungen aus (a) und (b) stiften eine Bijektion zwischen den Mengen*

$$\mathcal{U} \;=\; \{U \mid N \trianglelefteq U \leq G\} \;\text{ und }\; \overline{\mathcal{U}} \;=\; \{\overline{U} \mid \overline{U} \leq G/N\}\,.$$

(d) *Analoges gilt, wenn man an Stelle von Untergruppen Normalteiler betrachtet.*

BEWEIS
(a): ist klar. (b),(c): Ist $U \leq G$, so folgt $U = \Phi^{-1}(\Phi(U))$ und für Untergruppen $\overline{U}$ von G/N gilt: $\Phi(\Phi^{-1}(\overline{U})) = \overline{U}$. Also sind die Zuordnungen bijektiv. (d): Zu zeigen: Ist $M \leq G$ mit $N \trianglelefteq M$, so gilt $M \trianglelefteq G \;\Leftrightarrow\; \Phi(M) \trianglelefteq G/N$. Da $\Phi : G \to G/N$ surjektiv ist, gilt: $M \trianglelefteq G \Leftrightarrow \forall g \in G : \; gMg^{-1} = M \Leftrightarrow \forall g \in G : \; \Phi^{-1}(\Phi(gMg^{-1})) \subseteq \Phi^{-1}(\Phi(M)) \Leftrightarrow \forall g \in G : \; \Phi(gMg^{-1}) \subseteq \Phi(M) \Leftrightarrow \forall g \in G : \; \Phi(g)\Phi(M)\Phi(g)^{-1} \subseteq \Phi(M) \Leftrightarrow \forall \bar{g} \in G/N : \; \bar{g}\Phi(M)\bar{g}^{-1} \subseteq \Phi(M) \Leftrightarrow \Phi(M) \trianglelefteq G/N$. □

BEISPIEL 1.5.3
Sei $G = \mathbb{Z}$ und $N = 6\mathbb{Z}$. Die Menge $\mathcal{U}$ der Untergruppen von G mit $N \trianglelefteq U$ ist durch die Teiler von 6 gegeben:

$$\mathcal{U} \;=\; \{U_6 = 6\mathbb{Z} = N,\; U_3 = 3\mathbb{Z},\; U_2 = 2\mathbb{Z},\; U_1 = \mathbb{Z} = G\}\,.$$

Der kanonische Epimorphismus $\Phi : \mathbb{Z} \to 6\mathbb{Z}$, $a \mapsto a \bmod 6$ stellt folgende Zuordnung zwischen den Untergruppen $U \leq G$ der Menge $\mathcal{U}$ und den Untergruppen von G/N her:

$$\begin{array}{rcl} \Phi(U_6) &=& \{a \bmod 6 \mid a \in 6\mathbb{Z}\} \;=\; \{0 \bmod 6\} \\ \Phi(U_3) &=& \{a \bmod 6 \mid a \in 3\mathbb{Z}\} \;=\; \{0 \bmod 6,\; 3 \bmod 6\} \\ \Phi(U_2) &=& \{a \bmod 6 \mid a \in 2\mathbb{Z}\} \;=\; \{0 \bmod 6,\; 2 \bmod 6,\; 4 \bmod 6\} \\ \Phi(U_1) &=& \{a \bmod 6 \mid a \in 1\mathbb{Z}\} \;=\; \{0 \bmod 6, \cdots, 5 \bmod 6\} \;=\; G/N. \end{array}$$

1.6. Gruppen von Permutationen

Zunächst besprechen wir die Zyklendarstellung einer Permutation, die häufig der bisher benützten Darstellung vorzuziehen ist.

DEFINITION 1.6.1
Es sei $r \in \mathbb{N}$. Für r paarweise verschiedene $a_1, \ldots, a_r \in \{1, \ldots n\}$ bezeichne $(a_1\ a_2\ \cdots\ a_r)$ diejenige Permutation $\tau \in \mathfrak{S}_n$ mit $\tau(a_i) = a_{i+1}$ für $i = 1 \ldots r-1$ und $\tau(a_r) = a_1$, sowie $\tau(k) = k$ für alle $k \in \{1, \ldots, n\} - \{a_1, \ldots, a_r\}$. Man nennt $(a_1\ \cdots\ a_r)$ einen Zyklus der Länge r mit den Elementen $a_1, \ldots, a_r$. Ein Zyklus der Länge 2 heißt Transposition. Zwei Zyklen $(a_1\ \cdots\ a_r)$ und $(b_1\ \cdots\ b_s)$ heißen disjunkt, falls die Mengen $\{a_1, \ldots, a_r\}$ und $\{b_1, \ldots, b_s\}$ disjunkt sind.

SATZ 1.6.1
Sei $\sigma \in \mathfrak{S}_n$. Dann ist $\sigma = (a_1 \cdots a_r) \circ (b_1 \cdots b_s) \circ \cdots$, wobei

$$\{1, \ldots, n\} \ = \ \{a_1, \ldots, a_r\} \dot\cup \{b_1, \ldots, b_s\} \dot\cup \cdots$$

die Partition von $\{1, \ldots, n\}$ in Bahnen von $\langle\sigma\rangle$ ist, und die $a_i, b_i, \ldots$ geeignet nummeriert sind. Je zwei disjunkte Zyklen sind vertauschbar. Die Ordnung $|\langle\tau\rangle|$ eines Zyklus τ ist gleich seiner Länge.

BEWEIS
Wir führen den Beweis durch Induktion nach n. Für $n = 1$ ist $\mathrm{id} = (1)$. Es sei $\sigma \in \mathfrak{S}_n$ für $n \in \mathbb{N}$. Wir definieren die Folge (a_i) rekursiv durch $a_{i+1} = \sigma(a_i)$. Es sei $r = \min\{i \mid \sigma(a_i) = a_1\}$. Dann sind $a_1, \ldots, a_r$ alle paarweise verschieden, und wegen $a_i = \sigma^i(a_1)$ ist $\{a_1, \ldots, a_r\}$ eine Bahn von $\langle\sigma\rangle$ mit $|\langle\sigma\rangle| = r$. Nun sei $R = \{1, \ldots, n\} - \{a_1, \ldots, a_r\}$. Für die Restriktion $\sigma|_R$ gilt nach Induktionshypothese $\sigma|_R = (b_1\ \cdots\ b_s) \circ \cdots$, wobei $\{b_1, \ldots, b_s\} \dot\cup \cdots$ eine Partition von R in Bahnen von $\langle\sigma|_R\rangle$ ist. Damit ist dann $\sigma = (a_1\ \cdots\ a_r) \circ (b_1\ \cdots\ b_s) \circ \cdots$. □

DEFINITION 1.6.2
Die Darstellung einer Permutation σ nach Satz 1.6.1 heißt Zyklendarstellung von σ. Zyklen der Länge 1 können in der Darstellung weggelassen werden.

BEISPIEL 1.6.1
Die Permutation

$$\sigma \ = \ \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 \\ 3 & 7 & 2 & 4 & 6 & 5 & 9 & 10 & 1 & 8 \end{pmatrix}$$

hat die Zyklendarstellung $\sigma = (13279)(56)(8\ 10)$, oder (neben anderen Möglichkeiten) auch $\sigma = (65)(27913)(8\ 10)$. Der Zyklus (4) der Länge 1 wird weggelassen.

Eine Anwendung der Zyklendarstellung besteht in der Charakterisierung der Konjugiertenklassen von $\mathfrak{S}_n$.

DEFINITION 1.6.3
Für $\sigma \in \mathfrak{S}_n$ sei $z_i(\sigma)$ die Anzahl der Zyklen der Länge i in der Zyklendarstellung von σ. Dann heißt $(z_1(\sigma), \ldots, z_n(\sigma))$ der Zyklentyp von σ.

SATZ 1.6.2
Permutationen $\sigma, \tau \in \mathfrak{S}_n$ sind konjugiert genau dann, wenn sie vom gleichen Zyklentyp sind. Die Konjugiertenklassen der $\mathfrak{S}_n$ entsprechen also umkehrbar eindeutig den in $\mathfrak{S}_n$ möglichen Zyklentypen.

BEWEIS
Es seien $\sigma = (a_1 \cdots a_r) \in \mathfrak{S}_n$ ein Zyklus der Länge r und $\pi \in \mathfrak{S}_n$ beliebig. Dann ist Konjugation mit π äquivalent mit der Ersetzung von a_i durch $\pi(a_i)$:

$$(*): \ \pi\sigma\pi^{-1} \ = \ (\pi(a_1)\ \pi(a_2)\ \cdots\ \pi(a_r))$$

Dies zeigt, dass für $\sigma \in \mathfrak{S}_n$ die Permutationen σ und $\pi\sigma\pi^{-1}$ den gleichen Zyklentyp besitzen. Sind umgekehrt

$$\begin{array}{rcl} \sigma & = & (a_1^{(1)} \ \cdots \ a_{r_1}^{(1)}) \ \circ \ (a_1^{(2)} \ \cdots \ a_{r_2}^{(2)}) \ \circ \ \cdots \ \circ \ (a_1^{(s)} \ \cdots \ a_{r_s}^{(s)}) \\ \tau & = & (b_1^{(1)} \ \cdots \ b_{r_1}^{(1)}) \ \circ \ (b_1^{(2)} \ \cdots \ b_{r_2}^{(2)}) \ \circ \ \cdots \ \circ \ (b_1^{(s)} \ \cdots \ b_{r_s}^{(s)}) \end{array}$$

vom gleichen Zyklentyp, und ist $\pi \in \mathfrak{S}_n$ gegeben durch $\pi(a_i^{(j)}) = b_i^{(j)}$, so gilt $\tau = \pi\sigma\pi^{-1}$ wegen $(*)$. □

DEFINITION 1.6.4
Es sei $\sigma \in \mathfrak{S}_n$. Eine Inversion von σ ist eine zweielementige Teilmenge $\{a, b\} \subseteq \{1, \ldots n\}$ mit $a < b$ und $\sigma(a) > \sigma(b)$. Bezeichnet $I(\sigma)$ die Anzahl der Inversionen von σ, so heißt σ gerade, falls $I(\sigma)$ gerade ist, sonst ungerade. $\operatorname{sgn}(\sigma) = (-1)^{I(\sigma)}$ heißt das Vorzeichen (Signum) von σ. Die Menge der geraden Permutationen von $\mathfrak{S}_n$ heißt die alternierende Gruppe, und wird mit $\mathcal{A}_n$ bezeichnet.

SATZ 1.6.3
Jedes $\sigma \in \mathfrak{S}_n$ ist ein Produkt von Transpositionen. Ist σ gerade (bzw. ungerade), so ist in jeder Darstellung von σ als Produkt von Transpositionen die Anzahl der Faktoren gerade (bzw. ungerade). Sind $\sigma, \tau \in \mathfrak{S}_n$, so ist $\operatorname{sgn}(\sigma\tau) = \operatorname{sgn}(\sigma) \cdot \operatorname{sgn}(\tau)$.

Daraus ergibt sich:

SATZ 1.6.4
Es sei $n \geq 2$. Die Abbildung

$$\operatorname{sgn} \ = \ \begin{cases} \mathfrak{S}_n & \to & (\{1, -1\}, \ \cdot \ ) \\ \sigma & \mapsto & \operatorname{sgn}(\sigma) \end{cases}$$

ist ein Epimorphismus mit Kern $\operatorname{Ker}(\operatorname{sgn}) = \mathcal{A}_n$. *Die Menge $\mathcal{A}_n$ bildet einen Normalteiler von $\mathfrak{S}_n$ vom Index 2. Es ist* $\mathfrak{S}_n/\mathcal{A}_n \cong (\{1, -1\}, \ \cdot \ ) \cong (\mathbb{Z}/2\mathbb{Z}, +)$, *und* $|\mathcal{A}_n| = \frac{1}{2}n!$.

Für $n \geq 5$ besitzen die Gruppen $\mathcal{A}_n$ die bemerkenswerte Eigenschaft der Einfachheit.

DEFINITION 1.6.5
Eine Gruppe $G \neq \{1\}$ heißt einfach, falls G nur die trivialen Normalteiler $\{1\}$ und G besitzt.

SATZ 1.6.5
Für $n \geq 5$ ist $\mathcal{A}_n$ einfach.

Wir leiten Satz 1.6.5 aus drei Hilfssätzen her:

LEMMA 1.6.6
Es sei $n \geq 4$. Dann wird die Gruppe $\mathcal{A}_n$ von der Menge der Zyklen der Länge 3 (Dreierzyklen) erzeugt.

BEWEIS
Nach Satz 1.6.3 ist jedes $\sigma \in \mathcal{A}_n$ ein Produkt einer geraden Anzahl von Transpositionen. Die Faktoren fassen wir in Zweiergruppen zusammen. Es ist $(ab)(bc) = (abc)$, und $(ab)(cd) = (acb)(acd)$ für a, b, c, d paarweise verschieden. Jede Zweiergruppe von Transpositionen ist also ein Produkt von Dreierzyklen, und damit auch jedes $\sigma \in \mathcal{A}_n$. □

LEMMA 1.6.7
Es sei $n \geq 4$ und $N \trianglelefteq \mathcal{A}_n$ ein Normalteiler. Enthält N wenigstens einen Dreierzyklus, so ist $N = \mathcal{A}_n$.

BEWEIS
(Übungsaufgabe) □

LEMMA 1.6.8
Es sei $n \geq 5$ und $N \trianglelefteq \mathcal{A}_n$ ein Normalteiler mit $N \neq \{\mathrm{id}\}$. Dann enthält N einen Dreierzyklus.

BEWEIS
(Übungsaufgabe) □

1.7. Konstruktion von Gruppen

Die einfachsten Gruppen sind die zyklischen Gruppen, mit deren Betrachtung wir beginnen.

SATZ 1.7.1
Jede Untergruppe einer zyklischen Gruppe ist zyklisch.

BEWEIS
Es sei $G = \langle g \rangle$ und $\Phi : \mathbb{Z} \to G,\ n \mapsto g^n$, dann ist Φ ein Epimorphismus, und für jede Untergruppe $U \leq G$ ist $\Phi^{-1}(U)$ eine Untergruppe von $\mathbb{Z}$. Wegen $\Phi(\Phi^{-1}(U)) = U$ genügt es, die Behauptung für $G = (\mathbb{Z}, +)$ zu beweisen. Es sei nun $U \leq \mathbb{Z}$. Wir können $U \neq \{0\}$ annehmen. Es sei $g = \min\{k \in U \mid k \in \mathbb{N} \cap U\}$ und $n \in U$ beliebig. Nach Satz 1.3.1 (Division mit Rest) gibt es $q, r \in \mathbb{N}$ mit $0 \leq r < g$, so dass $n = qg + r$, also $r = n - qg \in U \Rightarrow r = 0$ (wegen $r < g$). Also $n \in U \Rightarrow n \in \langle g \rangle$, bzw. $\langle g \rangle = U$. □

SATZ 1.7.2 (Klassifikation der zyklischen Gruppen)
Sei $G = \langle g \rangle$ eine zyklische Gruppe.

(a) *Ist $|G| = \infty$, so ist $\Phi : \mathbb{Z} \to G,\ n \mapsto g^n$ ein Isomorphismus.*
(b) *Ist $|G| = m < \infty$, so ist $\overline{\Phi} : \mathbb{Z}/m\mathbb{Z} \to G,\ n \bmod m \mapsto g^n$ ein Isomorphismus.*

BEWEIS
Nach Satz 1.7.1 ist $\mathrm{Ker}(\Phi) = m\mathbb{Z}$ mit $m \in \mathbb{N}_0$. Nach Satz 1.5.1 (Homomorphiesatz) folgt, dass

$$\overline{\Phi} : \mathbb{Z}/\mathrm{Ker}(\Phi) \to G,\ n + \mathrm{Ker}(\Phi) \mapsto g^n$$

ein Isomorphismus ist. Es ist $\mathrm{Ker}(\Phi) = \{0\} \Leftrightarrow \Phi$ Isomorphismus $\Leftrightarrow G \cong (\mathbb{Z}, +) \Leftrightarrow |G| = \infty$. Ist $m \neq 0$, so ist $\overline{\Phi} : \mathbb{Z}/m\mathbb{Z} \to G,\ n \bmod m \mapsto g^n$ ein Isomorphismus. □

SATZ 1.7.3
Es sei G eine Gruppe, $g \in G$ und $n \in \mathbb{Z}$.

(a) *Ist $|\langle g \rangle| = \infty$, so ist $g^n = 1_G \Leftrightarrow n = 0$.*
(b) *Ist $|\langle g \rangle| < \infty$, so ist $g^n = 1_G \Leftrightarrow |\langle g \rangle|$ teilt n.*
(c) *Ist $|\langle g \rangle| < \infty$, so ist $g^{|G|} = 1_G$.*

BEWEIS
(a),(b): Es sei $\Phi : \mathbb{Z} \to \langle g \rangle,\ n \mapsto g^n$ wie in Satz 1.7.2. Nach diesem Satz ist $\mathrm{Ker}(\Phi) = \{0\}$ falls $|\langle G \rangle| = \infty$ ist und $\mathrm{Ker}(\Phi) = m\mathbb{Z}$ mit $m = |\langle g \rangle|$ sonst. Aus $g^n = 1_G \Leftrightarrow n \in \mathrm{Ker}(\Phi)$ folgt die Behauptung. (c): $\langle g \rangle$ ist Untergruppe von G, nach Satz 1.3.4 (Lagrange) teilt $|\langle g \rangle|$ die Gruppenordnung $|G|$, daher folgt die Behauptung mit Teil b). □

SATZ 1.7.4
Es sei G eine zyklische Gruppe und $|G| = n < \infty$. Dann gibt es zu jedem positiven Teiler m von n genau eine Untergruppe der Ordnung m. Ist $G = \langle g \rangle$ und $n = lm$, so gilt: $\langle g^l \rangle = \{x \in G \mid x^m = 1\}$ und $|\langle g^l \rangle| = m$.

BEWEIS
Es sei $U := \{x \in G \mid x^m = 1\}$. Dann ist $U \leq G$. Ist nun $H \leq G$ und $|H| = m$, so folgt nach Satz 1.7.3(c): $H \leq U$. Es bleibt noch $|U| = |H| = m$ zu zeigen. Nach Satz 1.7.1 ist $U = \langle h \rangle$ für $h \in G$. Nun ist $h^m = 1$, also $|U| \leq m$. Insbesondere $|\langle g^l \rangle| = m$. Somit ist $g^l \in U$ und $|U| = m$. □

DEFINITION 1.7.1
Eine natürliche Zahl $p > 1$ heißt Primzahl, falls p nur die positiven Teiler 1 und p besitzt.

SATZ 1.7.5
Es sei p eine Primzahl, und G eine Gruppe mit $|G| = p$. Dann ist $G \cong \mathbb{Z}/p\mathbb{Z}$, also zyklisch. G ist einfach.

BEWEIS
Es sei $g \in G - \{1\}$. Dann ist $|\langle g \rangle| \neq 1$. Also nach Satz 1.3.4 (Lagrange) $|\langle g \rangle| = p$ und somit $G = \langle g \rangle$. Nach Satz 1.7.2 ist $G \cong \mathbb{Z}/p\mathbb{Z}$. Ist U eine Untergruppe von G, so folgt ebenso: $|U| = 1$ oder p, also $U = \{1\}$ oder $U = G$, d. h. G ist einfach. □

Damit haben wir nach der Familie der $\mathcal{A}_n$ ($n \geq 5$) eine zweite unendliche Familie von endlichen einfachen Gruppen erhalten. Die Gruppen $\mathbb{Z}/p\mathbb{Z}$ sind die einzigen abelschen endlichen einfachen Gruppen.

SATZ 1.7.6
Die Gruppe G sei endlich, einfach und abelsch. Dann gibt es eine Primzahl p, so dass $G \cong \mathbb{Z}/p\mathbb{Z}$.

BEWEIS
Es sei $g \in G - \{1\}$. Dann ist $\langle g \rangle$ ein Normalteiler von G, da G abelsch ist. Wegen der Einfachheit von G folgt $\langle g \rangle = G$. Ist $|G|$ keine Primzahl, so besitzt G nach Satz 1.7.4 nicht triviale Normalteiler. Aus Satz 1.7.5 folgt die Behauptung. □

Das Problem der Bestimmung der endlichen einfachen Gruppen ist erst um etwa 1980 gelöst worden. Die Gesamtlänge aller Arbeiten, die zur Lösung des Problems führten, beträgt mehrere tausend Seiten. Die Gesamtheit der endlichen einfachen Gruppen besteht aus 18 unendlichen Familien (zwei davon sind die Familien $\mathbb{Z}/p\mathbb{Z}$ mit p Primzahl und $\mathcal{A}_n$ für $n \geq 5$), sowie 26 Einzelgängern, den so genannten sporadischen Gruppen. Die größte davon ist das Monster (friendly giant) M mit

$$|M| \;=\; 2^{46} \cdot 3^{20} \cdot 5^9 \cdot 7^6 \cdot 11^2 \cdot 13^3 \cdot 17 \cdot 19 \cdot 23 \cdot 29 \cdot 31 \cdot 41 \cdot 47 \cdot 59 \cdot 71 \;\sim\; 8 \cdot 10^{53}\,.$$

In einem Sinn, der in Abschnitt 1.9 präzisiert werden wird, sind die endlichen einfachen Gruppen die Bausteine aller endlichen Gruppen. Neben der Bestimmung der einfachen Gruppen ist daher ein anderes Hauptproblem die Konstruktion von komplizierteren Gruppen aus gegebenen Gruppen einfacherer Bauart. Diese Konstruktionsmethoden werden dann auch zu Hinweisen für die Analyse von Gruppen G führen, von denen zunächst nur unvollständige Information (wie z.B. die Ordnung $|G|$) vorliegt. Das wohl einfachste Konstruktionsprinzip ist das direkte Produkt.

DEFINITION 1.7.2
Es seien G_1, G_2 Gruppen. Dann wird $G_1 \times G_2$ durch komponentenweise Verknüpfung

$$(g_1, g_2)(h_1, h_2) \;=\; (g_1 h_1, g_2 h_2)$$

für alle $g_1, h_1 \in G_1$ und $g_2, h_2 \in G_2$ zu einer Gruppe, das (äußere) direkte Produkt von G_1 und G_2. Das direkte Produkt von mehr als zwei Gruppen kann rekursiv definiert werden.

BEISPIEL 1.7.1
Es sei $G_1 = G_2 = (\mathbb{R}, +)$. Dann ist $G_1 \times G_2 = (\mathbb{R}^2, +)$. Wir schreiben in diesem Fall auch $\mathbb{R}^2 = \mathbb{R} \oplus \mathbb{R}$ (direkte Summe).

Die Untergruppen

$$\begin{array}{rcccl} N_1 & = & G_1 \times \{1_{G_2}\} & = & \{(g_1, 1_{G_2}) \mid g_1 \in G_1\}\,, \\ N_2 & = & \{1_{G_1}\} \times G_2 & = & \{(1_{G_1}, g_2) \mid g_2 \in G_2\} \end{array}$$

sind offenbar zu G_1 bzw. G_2 isomorphe Normalteiler von $G_1 \times G_2$, deren Elemente kommutieren, und die nur die triviale Untergruppe $\{(1_{G_1}, 1_{G_2})\}$ als Durchschnitt besitzen. Es ist $N_1 N_2 = G_1 \times G_2$. Ist nun umgekehrt eine Gruppe G mit zwei Normalteilern gegeben, die dieselben Eigenschaften haben wie N_1 und N_2, so ist G zum äußeren direkten Produkt dieser Normalteiler isomorph.

SATZ 1.7.7
Es seien N_1, N_2 Normalteiler der Gruppe G mit $N_1 \cap N_2 = \{1\}$ und $N_1 N_2 = G$. Dann gilt:

(a) $n_1 \in N_1, n_2 \in N_2 \;\Rightarrow\; n_1 n_2 = n_2 n_1$.
(b) *Jedes $g \in G$ besitzt genau eine Darstellung der Form $g = n_1 n_2$ mit $n_1 \in N_1$ und $n_2 \in N$.*
(c) $G \cong N_1 \times N_2$.
(d) $G \,/\, N_1 \cong N_2$ *und* $G \,/\, N_2 \cong N_1$.

DEFINITION 1.7.3
G heißt das (innere) direkte Produkt von N_1 und N_2.

BEWEIS
(a): Es seien $n_1 \in N_1$ und $n_2 \in N_2$. Dann sind $n_1 n_2 n_1^{-1} \in N_2, n_2 n_1 n_2^{-1} \in N_1$, also

$$\begin{array}{rcccl} n_1 n_2 n_1^{-1} n_2^{-1} & = & (n_1 n_2 n_1^{-1}) n_2^{-1} & \in & N_2 \quad \text{und} \\ n_1 n_2 n_1^{-1} n_2^{-1} & = & n_1 (n_2 n_1^{-1} n_2^{-1}) & \in & N_1 \quad , \end{array}$$

also liegt $n_1 n_2 n_1^{-1} n_2^{-1}$ im Schnitt $N_1 \cap N_2 = \{1_G\}$. Also ist $n_1 n_2 n_1^{-1} n_2^{-1} = n_1 n_2 (n_2 n_1)^{-1} = 1$, und damit $n_1 n_2 = n_2 n_1$. (b),(c): Wegen $N_1 N_2 = G$ hat jedes $g \in G$ eine Darstellung der gegebenen Form mit $n_1 \in N_1$ und $n_2 \in N_2$. Diese Darstellung ist eindeutig: aus $g = n_1 n_2 = \tilde{n}_1 \tilde{n}_2$ folgt mit Teil a) auch $\tilde{n}_1 n_1^{-1} = \tilde{n}_2 n_2^{-1} \in N_1 \cap N_2 = \{1\}$, also $n_1 = \tilde{n}_1$ und $n_2 = \tilde{n}_2$. Die Abbildung $\Phi : G \to N_1 \times N_2,\ g = n_1 n_2 \mapsto (n_1, n_2)$ ist ein Isomorphismus. Die „Projektionen"

$$\begin{array}{rcl} \pi_1 : & G \to N_1 & , \quad g = n_1 n_2 \mapsto n_1 \\ \pi_2 : & G \to N_2 & , \quad g = n_1 n_2 \mapsto n_2 \end{array}$$

sind Epimorphismen mit den Kernen $\mathrm{Ker}(\pi_1) = N_2$ und $\mathrm{Ker}(\pi_2) = N_1$. Nach dem Homomorphiesatz (Satz 1.5.1) folgt (d). □

Die Konstruktion des direkten Produkts reicht aus, um alle endlich erzeugten abelschen Gruppen zu beschreiben.

SATZ 1.7.8 (Hauptsatz über endlich erzeugte abelsche Gruppen, Kurzform)
Jede endlich erzeugte abelsche Gruppe ist isomorph zu einem direkten Produkt von zyklischen Gruppen.

(ohne Beweis)

Schon für endliche nicht abelsche Gruppen benötigt man hingegen weitere Konstruktionen.

Wir untersuchen die Verallgemeinerung der Situation von Satz 1.7.7. Welche Aussage lässt sich über die Struktur der Gruppe G machen, wenn statt des Paares (N_1, N_2) von Normalteilern nur ein Paar (N, U) bestehend aus einem Normalteiler N und einer Untergruppe U gegeben sind mit $N \cap U = \{1\}$ und $NU = G$? So wie im ersten Fall G zum (äußeren) direkten Produkt $N_1 \times N_2$ isomorph ist, wird in diesem Fall G zum (äußeren) semidirekten Produkt von N und U isomorph sein. Um die Definition zu motivieren, machen wir zunächst folgende Beobachtung: Elemente $n \in N$ und $u \in U$ werden im allgemeinen nicht mehr kommutieren, d. h. es wird i.a. nicht mehr gelten $nu = un$ oder (äquivalent dazu) $unu^{-1} = n$. Statt dessen gilt jedoch wegen der Normalteilereigenschaft von N die schwächere Bedingung $uNu^{-1} = N$. Die Abbildung $\tau_u : n \mapsto unu^{-1}$ ist für jedes $u \in U$ ein Automorphismus von N, und die Abbildung $\Phi : U \to \mathrm{Aut}(N)$, $u \mapsto \tau_u$ ist ein Homomorphismus. Das Produkt zweier Elemente $n_1u_1, n_2u_2 \in NU$ mit $n_1, n_2 \in N$ und $u_1, u_2 \in U$ lässt sich dann berechnen als $(n_1u_1)(n_2u_2) = n_1(u_1n_2u_1^{-1})u_1u_2$ oder

$$(n_1u_1)(n_2u_2) \;=\; n_1\tau_{u_1}(n_2) \cdot u_1u_2$$

mit $n_1, \tau_{u_1}(n_2) \in N$ und $u_1, u_2 \in U$. Diese Beziehung geht in die Definition des semidirekten Produkts ein.

SATZ 1.7.9
Es seien G, H Gruppen, $\Phi : H \to \mathrm{Aut}(G)$, $h \mapsto \tau_h$ ein Homomorphismus von H in die Gruppe $\mathrm{Aut}(G)$ der Automorphismen von G. Dann wird $G \times H$ durch die Verknüpfung

$$\begin{array}{ccc} (G \times H) \times (G \times H) & \to & G \times H \\ ((g_1, h_1), (g_2, h_2)) & \mapsto & (g_1, h_1)(g_2, h_2) \end{array}$$

definiert durch

$$(g_1, h_1)(g_2, h_2) \;=\; (g_1 \cdot \tau_{h_1}(g_2), h_1h_2)$$

zu einer Gruppe (Bezeichnung: $G \times_\Phi H$).

BEWEIS
(Übungsaufgabe) □

DEFINITION 1.7.4
Voraussetzungen wie in Satz 1.7.9. Die Gruppe $G \times_\Phi H$ heißt das (äußere) semidirekte Produkt der Gruppen G und H.

SATZ 1.7.10
Es sei G eine Gruppe, N ein Normalteiler und U eine Untergruppe von G mit $N \cap U = \{1\}$ und $NU = G$. Für $u \in U$ sei der innere Automorphismus τ_u von N gegeben durch $\tau_u : N \to N$, $n \mapsto unu^{-1}$. Es sei $\Phi : U \to \mathrm{Aut}(G)$, $u \mapsto \tau_u$. Dann gilt:

(a) *Jedes $g \in G$ besitzt genau eine Darstellung der Form $g = nu$ mit $n \in N$ und $u \in U$.*
(b) *$G \cong N \times_\Phi U$.*
(c) *$G/N \cong U$.*

(d) *Die folgenden Aussagen sind äquivalent:*
(i) $U \trianglelefteq G$,
(ii) $\Phi(u) = \mathrm{id}_N \; \forall u \in U$,
(iii) G *ist inneres direktes Produkt von* N *und* U.

DEFINITION 1.7.5
G heißt (inneres) semidirektes Produkt von N und U.

BEWEIS
(a): Es seien $g = n_1u_1 = n_2u_2$, dann gilt $n_2^{-1}n_1 = u_2u_1^{-1} \in N \cap U = \{1\}$, also $n_1 = n_2$ und $u_1 = u_2$. (b): Die Abbildung $\psi : G \to N \times_\Phi U$, $g = nu \mapsto (n, u)$ ist ein Isomorphismus. Der Beweis besteht im Nachrechnen der Gleichung $(n_1u_1)(n_2u_2) = n_1\tau_{u_1}(n_2) \cdot u_1u_2$. (c): Die Abbildung $\Omega : G \to U$, $nu \mapsto u$ ist ein Epimorphismus mit Kern $\mathrm{Ker}(\Omega) = N$. Die Behauptung folgt aus dem Homomorphiesatz. (d): (i)$\Leftrightarrow$(iii) folgt nach Definition 1.7.3, (i)$\Rightarrow$(ii) mit Satz 1.7.7, und (ii)$\Rightarrow$(i) folgt wegen $\forall n \in N,\ u, v \in U : unu^{-1} = n \Rightarrow u = nun^{-1} \Rightarrow (nv)u(nv)^{-1} = vuv^{-1} \in U \Rightarrow U \trianglelefteq G$ da $G = NU$. □

Zum Schluss geben wir ein Beispiel, wie die Konstruktion des semidirekten Produkts benützt werden kann, um den Isomorphietyp einer Gruppe zu bestimmen, von der nur unvollständige Information vorliegt.

BEISPIEL 1.7.2
Folgende Aussagen sind äquivalent:

(i) G ist eine nicht abelsche Gruppe der Ordnung 12, und G besitzt einen Normalteiler N der Ordnung 4 und eine Untergruppe der Ordnung 3.
(ii) $G \cong \mathcal{A}_4$.

BEWEIS
(ii)$\Rightarrow$(i): $\mathcal{A}_4$ ist offenbar nicht abelsch, $V_4 = \{\mathrm{id}, (12)(34), (13)(24), (14)(23)\}$ ist ein Normalteiler der Ordnung 4, und $U_3 = \{\mathrm{id}, (123), (132)\}$ ist eine Untergruppe der Ordnung 3. (i)$\Rightarrow$(ii): Die möglichen Isomorphietypen für N bzw. U sind $N \cong \mathbb{Z}/4\mathbb{Z}$ oder $N = \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} =: V$ bzw. $U_3 \cong \mathbb{Z}/3\mathbb{Z}$. Nach Satz 1.7.10(b) ist $G \cong N \times_\Phi U$, wobei $\Phi : U \to \mathrm{Aut}(N)$, $u \mapsto \tau_u$ ist. Wegen $\Phi(U) \cong U/\mathrm{Ker}(\Phi)$ ergeben sich die Möglichkeiten $\Phi(U) = \{\mathrm{id}_N\}$ und $\Phi(U) \cong U \cong \mathbb{Z}/3\mathbb{Z}$. Annahme: $\Phi(U) = \{\mathrm{id}_N\}$. Es folgt $\tau_u = \mathrm{id}_N$ für alle $u \in U$. Nach Satz 1.7.10(d) ist damit G inneres direktes Produkt der abelschen Normalteiler N und U und damit selbst abelsch, ein Widerspruch. Also gilt $\Phi(U) \cong U \cong \mathbb{Z}/3\mathbb{Z}$. Annahme: $N \cong \mathbb{Z}/4\mathbb{Z}$. Wir untersuchen $\mathrm{Aut}(\mathbb{Z}/4\mathbb{Z}) \cong \mathrm{Aut}(N)$. Es sei $\tau \in \mathrm{Aut}(\mathbb{Z}/4\mathbb{Z}) - \{\mathrm{id}\}$. Da $|\langle\tau(g)\rangle| = |\langle g\rangle|$ für alle $g \in \mathbb{Z}/4\mathbb{Z}$ ist folgt $\tau(1 \bmod 4), \tau(3 \bmod 4) \in \{1 \bmod 4,\ 3 \bmod 4\}$. Also ist $\mathrm{Aut}(\mathbb{Z}/4\mathbb{Z}) = \{\mathrm{id}, \tau^*\}$ mit der Transposition $\tau^* = (1 \bmod 4 \ \ 3 \bmod 4)$, und damit $\mathrm{Aut}(\mathbb{Z}/4\mathbb{Z}) \cong \mathbb{Z}/2\mathbb{Z}$, im Widerspruch zu $\Phi(U) \cong U \cong \mathbb{Z}/3\mathbb{Z}$. Es verbleibt die Möglichkeit $N \cong V$. Es sei $N = \{1, a, b, ab\}$ mit $a, b \in G$, $U = \{1, \alpha, \alpha^2\}$ mit $\alpha \in G$. Wegen $\Phi(U) \cong \mathbb{Z}/3\mathbb{Z}$ gibt es genau ein $\beta \in \{\alpha, \alpha^2\}$, so dass die Konjugation $\tau_\beta : N \to N$, $n \mapsto \beta n\beta^{-1}$ auf $M = \{a, b, ab\}$ operiert wie der Dreierzyklus $(a\ b\ (ab))$. Mit dieser Festsetzung ist $U = \{1, \beta, \beta^2\}$ und $\beta a\beta^{-1} = b$, $\beta b\beta^{-1} = ab$ sowie $\beta(ab)\beta^{-1} = a$. Wir definieren die Isomorphismen $\psi_1 : N \to V_4$ und $\psi_2 : U \to U_3$ durch

$$\begin{aligned} \psi_1(1) &= \mathrm{id} \\ \psi_1(a) &= (12)(34) \\ \psi_1(b) &= (14)(23) \\ \psi_2(\beta) &= (123)\,. \end{aligned}$$

Dann rechnet man nach, dass $(*)$: $\psi_1(unu^{-1}) = \psi_2(u)\psi_1(n)\psi_2(u)^{-1}$ für alle $u \in U$ und $n \in N$ ist. Der Isomorphismus ψ : $G \to \mathcal{A}_4$ ist gegeben durch ψ : $g = nu \mapsto \psi_1(n)\psi_2(u)$. Es ist klar, dass ψ bijektiv ist. Die Relationstreue folgt mit $(*)$, es seien $n_1, n_2 \in N,\ u_1, u_2 \in U$:

$$\begin{aligned}
\psi(n_1u_1n_2u_2) &= \psi(n_1(u_1n_2u_1^{-1})u_1u_2) \\
&= \psi_1(n_1(u_1n_2u_1^{-1}))\psi_2(u_1u_2) \\
&= \psi_1(n_1)\psi_1(u_1n_2u_1^{-1})\psi_2(u_1)\psi_2(u_2) \\
&= \psi_1(n_1)\psi_2(u_1)\psi_1(n_2)\psi_2(u_1)^{-1}\psi_2(u_1)\psi_2(u_2) \\
&= \psi(n_1u_1)\psi(n_2u_2) \qquad .
\end{aligned}$$

□

1.8. Sylowsätze, weitere Gruppenoperationen in der Gruppentheorie

Das Studium von Operationen einer Gruppe G oder einer Untergruppe $U \leq G$ auf der Gruppe G selbst oder auf einer Menge M, die mit G verbunden ist, führt oft zu interessanten Tatsachen der Gruppentheorie. Ein erstes Beispiel haben wir im Satz von Lagrange kennen gelernt: die Tatsache, dass die Ordnung $|U|$ einer Untergruppe die Ordnung $|G|$ der Gesamtgruppe teilt, folgte durch Betrachtung der Operation von U auf G durch Links- (oder Rechts-)multiplikation. Außer durch Linksmultiplikation kann eine Untergruppe U auf einer Gruppe G auch durch Konjugation operieren. Diese beiden Arten von Operationen können außer auf der Menge $M = G$ auch noch auf anderen Mengen M geschehen, die mit G verbunden sind.

DEFINITION 1.8.1
Es sei M eine beliebige Menge und $k \in \mathbb{N}$. Unter $\mathrm{Pot}_k(M)$ verstehen wir die Menge der k-elementigen Teilmengen von M.

Ist G eine Gruppe und $K \in \mathrm{Pot}_k(G)$, so sind für $g \in G$ auch $gK \in \mathrm{Pot}_k(G)$ und $gKg^{-1} \in \mathrm{Pot}_k(G)$. Jede Untergruppe $U \leq G$ operiert also auf $\mathrm{Pot}_k(G)$ durch Linksmultiplikation $(g, K) \mapsto gK$ oder durch Konjugation $(g, K) \mapsto gKg^{-1}$. Von Interesse sind außerdem Operationen auf gewissen Teilmengen von $\mathrm{Pot}_k(G)$, wie beispielsweise Mengen von Nebenklassen oder Mengen von Untergruppen. Wir betrachten zunächst Operationen durch Konjugation.

DEFINITION 1.8.2 (Normalisator, Zentralisator)
Es sei G eine Gruppe, $K \subseteq G$ eine beliebige Teilmenge und h ein Element von G. Dann heißt

(a) $N_G(K) = \{g \in G \mid gKg^{-1} = K\}$ der Normalisator von K,
(b) $C_G(h) = \{g \in G \mid ghg^{-1} = h\}$ der Zentralisator von h.

Nach Definition 1.2.3 ist der Normalisator einer Teilmenge $K \in \mathrm{Pot}_k(G)$ gerade der Stabilisator der Operation

$$\begin{array}{ccc} G \times \mathrm{Pot}_k(G) & \to & \mathrm{Pot}_k(G) \\ (g, K) & \mapsto & gKg^{-1} \end{array} \quad .$$

Der Zentralisator erweist sich als Spezialfall des Normalisators für den Fall $k = 1$. Die Anwendung von Satz 1.2.1(a) und des Bahnensatzes 1.3.5 ergibt sofort:

SATZ 1.8.1
Es sei G eine Gruppe, $h \in G$ und $K \subseteq G$.

(a) *Der Zentralisator $C_G(h)$ und der Normalisator $N_G(K)$ sind Untergruppen von G.*

(b) *Ist $|G| < \infty$, so gilt für die Anzahl der Konjugierten von h*

$$|\{ghg^{-1} \mid g \in G\}| = \frac{|G|}{|C_G(h)|},$$

und für die Anzahl der zu K konjugierten Komplexe

$$|\{gKg^{-1} \mid g \in G\}| = \frac{|G|}{|N_G(K)|}.$$

BEMERKUNG 1.8.1
Ist $U \leq G$ eine Untergruppe von G, so ist stets $U \leq N_G(U)$. $N_G(U)$ ist die größte Untergruppe von G, in der U ein Normalteiler ist. U ist Normalteiler von G genau dann, wenn $N_G(U) = G$.

Wir kommen nun zu Operationen durch Linksmultiplikation. Einige davon führen zu interessanten Beziehungen zu Permutationsgruppen. Wir beginnen mit einem Satz, der sich mit beliebigen Operationen befasst.

SATZ 1.8.2
Es sei M eine beliebige Menge. Die Gruppe G operiere auf M (von Links). Für jedes $g \in G$ ist die Abbildung $l_g : M \to M$, $m \mapsto gm$ bijektiv ($l_{g^{-1}}$ ist das Inverse zu l_g). Die Abbildung $\Phi : G \mapsto \mathfrak{S}(M)$, $g \mapsto l_g$ ist ein Homomorphismus von G in $\mathfrak{S}(M)$.

BEWEIS
(Übungsaufgabe) □

DEFINITION 1.8.3
Der Homomorphismus Φ heißt die zur Gruppenoperation gehörende Permutationsdarstellung von G.

Wir untersuchen die zur Linksmultiplikation gehörende Permutationsdarstellung einer Gruppe G und finden, dass jede Gruppe isomorph zu einer Gruppe von Permutationen ist.

SATZ 1.8.3 (Cayley)
Jede Gruppe G ist isomorph zu einer Untergruppe von $\mathfrak{S}(G)$. Insbesondere ist eine endliche Gruppe der Ordnung n isomorph zu einer Untergruppe der $\mathfrak{S}_n$.

BEWEIS
Wir betrachten die zur Linksmultiplikation gehörende Permutationsdarstellung Φ mit $\Phi : G \to \mathfrak{S}(G)$, $g \mapsto l_g$ mit $l_g(h) = gh$ für $h \in G$. Φ ist nach Satz 1.8.2 ein Homomorphismus. $g \in \mathrm{Ker}(\Phi) \Leftrightarrow l_g = \mathrm{id}_g \Leftrightarrow g = 1_G$, also ist $\mathrm{Ker}(\Phi) = \{1\}$. Nach Satz 1.5.1 ist Φ ein Isomorphismus von G auf $\Phi(G) \leq \mathfrak{S}(G)$. □

Es sei nun U eine Untergruppe der Gruppe G. Dann operiert G auf der Menge G/U der Linksnebenklassen von U in G durch Linksmultiplikation:

$$\begin{array}{ccc} M = G/U & \to & G/U \\ (g, hU) & \mapsto & (gh)U \end{array}.$$

Auch zu dieser Operation gehört nach Satz 1.8.2 eine Permutationsdarstellung.

DEFINITION 1.8.4
Es sei G eine Gruppe und $U \leq G$. Unter dem Herz von U versteht man

$$H_G(U) := \bigcap_{g \in G} (gUg^{-1}) .$$

SATZ 1.8.4
Es sei G eine Gruppe mit Untergruppe U. Das Herz $H_G(U)$ ist ein Normalteiler von G. Ist $(G : U) = m$ endlich, so ist $(G : H_G(U))$ ein Teiler von $m!$. $H_G(U)$ ist der Kern der zur Linksmultiplikation der Linksnebenklassen von U gehörenden Permutationsdarstellung von G.

BEWEIS
Der zur besagten Operation gehörende Homomorphismus ist $\Phi : G \to \mathfrak{S}(G/U)$, $h \mapsto l_h$ mit $l_h(gU) = (hg)U$. Also gilt $h \in \mathrm{Ker}(\Phi) \Leftrightarrow l_h = \mathrm{id}_{G/U} \Leftrightarrow \forall g \in G : \ l_h(gU) = gU \Leftrightarrow \forall g \in G : \ (hg)U = gU \Leftrightarrow \forall g \in G : \ g^{-1}hgU = U \Leftrightarrow \forall g \in G : \ ghg^{-1} \in U \Leftrightarrow \forall g \in G : \ h \in gUg^{-1} \Leftrightarrow h \in H_G(U)$. Damit ist $\mathrm{Ker}(\Phi) = H_G(U)$. Die restlichen Behauptungen folgen aus dem Homomorphiesatz und dem Satz von Lagrange. □

Die vielleicht wichtigste Anwendung von Gruppenoperationen betrifft die Existenz von speziellen Untergruppen einer Gruppe, der so genannten Sylowgruppen. Zu ihrer Diskussion stellen wir den Fundamentalsatz der Arithmetik voran. Er wird später als Spezialfall eines allgemeinen Satzes über euklidische Ringe folgen, weshalb wir seinen Beweis hier nicht geben.

SATZ 1.8.5 (Fundamentalsatz der Arithmetik)
Jede Zahl $n \in \mathbb{N}$ hat eine bis die Reihenfolge der Faktoren eindeutige Zerlegung der Form $n = p_1 \cdot \cdots \cdot p_r$, wobei die p_j (nicht notwendig verschiedene) Primzahlen sind.

Fasst man gleiche Primzahlen zu Potenzen zusammen, so ergibt sich für jedes $n \in \mathbb{N}$ eine eindeutige Darstellung der Form

$$n = \prod_p p^{\alpha(p)} \quad (\alpha(p) \in \mathbb{N}_0) ,$$

wobei $\alpha(p) > 0$ nur für endlich viele Primzahlen gilt.

DEFINITION 1.8.5
Es seien $m, n \in \mathbb{Z}$. Für m teilt n schreiben wir auch $m|n$, für das Gegenteil $m \not| n$.

Wir können nach der Umkehrung des Satzes von Lagrange fragen: Es sei $|G| = n$. Gibt es zu jedem Teiler d von n eine Untergruppe $U \leq G$ mit $|U| = d$? Die Antwort ist im allgemeinen nein. Beschränken wir uns jedoch auf die Werte von d, welche Primzahlpotenzen sind, so kann die Existenz stets garantiert werden.

SATZ 1.8.6
Es sei G eine endliche Gruppe, p eine Primzahl und $p^k | n$ für $n = |G|$ und ein $k \in \mathbb{N}$. Es sei a die Anzahl der Untergruppen $U \leq G$ mit $|U| = p^k$. Dann gilt: $a \equiv 1 \bmod p$. Insbesondere ist $a \neq 0$.

BEWEIS
Es sei $m = |G|/p^k$ und $\mathbf{M} = \mathrm{Pot}_{p^k}(G)$. Dann gilt:

$$|\mathbf{M}| = \binom{|G|}{p^k} .$$

G operiert auf $\mathbf{M}$ durch Linksmultiplikation. Es sei $M \in \mathbf{M}$ und $S = \mathrm{Stab}_G(M) = \{g \in G \mid gM = M\}$. Aus

$$M \;=\; SM \;=\; \bigcup_{h \in M} Sh$$

folgt, dass M Vereinigung von vollen Rechtsnebenklassen von S in G ist. Deren Anzahl ist $|M|/|S|$. Also teilt $|S|$ die Anzahl der Elemente von M, welche p^k beträgt. Nach dem Bahnensatz 1.3.5 besitzt die Bahn von M gerade $|G|/|S| = mp^\alpha$ Elemente, wobei $\alpha = 0 \Leftrightarrow |S| = p^k$. Es seien $M_1, \ldots, M_l$ Vertreter der Bahnen mit Stabilisatoren $S_1, \ldots, S_l$ so angeordnet, dass $|S_1| = \cdots = |S_a| = p^k$ ist und $|S_i| < p^k$ für $i > a$. Dann gilt:

$$(*): \quad \binom{mp^k}{p^k} \;=\; |\mathbf{M}| \;=\; \sum_{i=1}^{l} |GM_i| \;=\; \sum_{i=1}^{l} \frac{|G|}{|S_i|} \;\equiv\; \sum_{i=1}^{a} \frac{|G|}{|S_i|} \;\equiv\; m \cdot a \mod p\,.$$

Dies gilt für jede Gruppe G mit $G = mp^k$, also insbesondere für die zyklische Gruppe $G = \mathbb{Z}/mp^k\mathbb{Z}$. In diesem Fall ist $a = 1$ nach Satz 1.7.4. Mit $(*)$ folgt:

$$\binom{mp^k}{p^k} \;\equiv\; m \cdot 1 \mod pm\,,$$

insgesamt also

$$\frac{ma - m}{pm} \in \mathbb{Z} \;\Rightarrow\; a \equiv 1 \bmod p\,.$$

□

DEFINITION 1.8.6
Es sei G eine endliche Gruppe, p eine Primzahl, $n \in \mathbb{N}$, und $|G| = np^\alpha$, wobei p kein Teiler von n ist. Eine Untergruppe $U \leq G$ mit $|U| = p^\alpha$ heißt p-Sylowgruppe von G. Die Menge der p-Sylowgruppen von G bezeichnen wir mit $\mathrm{Syl}_p(G)$.

SATZ 1.8.7 (Sylow)
Es sei G eine endliche Gruppe mit $|G| = np^\alpha$, $p \nmid n$. Dann gilt:

(a) $|\mathrm{Syl}_p(G)| \equiv 1 \bmod p$, *insbesondere existiert mindestens eine p-Sylowgruppe von G.*
(b) *Es sei $U \leq G$ mit $|U| = p^\beta$, dann gibt es $P \in \mathrm{Syl}_p(G)$ mit $U \leq P$.*
(c) *Alle p-Sylowgruppen von G sind konjugiert in G.*

Gibt es insbesondere nur eine einzige p-Sylowgruppe in G, so ist diese notwendig ein Normalteiler von G.

BEWEIS
(a): folgt unmittelbar aus Satz 1.8.6. (b): Es sei $Q \in \mathrm{Syl}_p(G)$. Dann operiert U auf G/Q durch Linksmultiplikation. Die Längen der Bahnen sind Teiler von $|U|$, also von der Form p^γ für ein $\gamma \leq \beta$. Die Summe der Bahnlängen ist $n = |G/Q|$. Da $p \nmid n$ vorausgesetzt ist, existiert mindestens eine Bahn der Länge $p^0 = 1$, d. h. es gibt ein $g \in G$, so dass $ugQ = gQ$ für alle $u \in U$ ist. Damit ist $U(gQg^{-1}) = gQg^{-1}$, also auch $U \leq P$ mit $P := gQg^{-1} \in \mathrm{Syl}_p(G)$. Damit folgt auch (c). □

BEMERKUNG 1.8.2
Satz 1.8.7 ermöglicht oft den Nachweis der Existenz von nicht trivialen Normalteilern von Gruppen, von denen lediglich die Ordnung bekannt ist, und ermöglicht so den Schluss, dass

Gruppen von gewisser Ordnung nicht einfach sein können. Aus Satz 1.8.1(b) folgt nämlich weiter für $P \in \mathrm{Syl}_p(G)$:

$$(*): \ |\mathrm{Syl}_p(G)| \ = \ \frac{|G|}{|N_G(P)|} \ \text{bzw.} \ |\mathrm{Syl}_p(G)| \mid \frac{|G|}{|P|} \, .$$

BEISPIEL 1.8.1
Es sei $|G| = p^\alpha n$ mit $n > 1$, p Primzahl und $p \nmid n$. Der einzige Teiler d von n mit $d \equiv 1 \bmod p$ sei $d = 1$. Dann gilt nach Satz 1.8.7: $|\mathrm{Syl}_p(G)| \equiv 1 \bmod p$, aber nach $(*)$ auch $|\mathrm{Syl}_p(G)| \mid n$. Also ist $|\mathrm{Syl}_p(G)| = 1$, und die einzige p-Sylowgruppe P ist ein Normalteiler von G. Beispielsweise hat eine Gruppe mit 45 Elementen einen Normalteiler der Ordnung 9.

BEISPIEL 1.8.2 (Isomorphietypen der Ordnung 12)
Jede Gruppe G mit $|G| = 12$ hat einen Normalteiler N_3 der Ordnung 3 oder einen Normalteiler N_4 der Ordnung 4: Angenommen G hat keinen Normalteiler der Ordnung 3, dann ist $|\mathrm{Syl}_3(G)| > 1$. Ist $P_3 \in \mathrm{Syl}_3(G)$, so folgt:

$$|\mathrm{Syl}_3(G)| \ = \ \frac{|G|}{|N_G(P_3)|} \ = \ 4 \, .$$

Die 4 zu P_3 konjugierten 3-Sylowgruppen enthalten zusammen 8 Elemente der Ordnung 3. Die restlichen 4 Elemente von G bilden dann die einzige 4-Sylowgruppe, die dann ein Normalteiler der Ordnung 4 von G ist.

Fall 1:
G hat sowohl einen Normalteiler N_3 als auch einen Normalteiler N_4. Dann ist G das innere direkte Produkt von N_3 und N_4, d. h. G ist abelsch. Die zwei möglichen Isomorphietypen $N_4 \cong \mathbb{Z}/4\mathbb{Z}$ und $N_4 \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ führen zu zwei möglichen Isomorphietypen für G:

(i) $G \cong \mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z} \cong \mathbb{Z}/12\mathbb{Z}$,
(ii) $G \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}$.

Fall 2:
G hat einen Normalteiler N_3 aber keinen Normalteiler N_4. Ist $P_4 \in \mathrm{Syl}_2(G)$, so ist G isomorph zum semidirekten Produkt $G \cong N_3 \times_\Phi P_4$ mit $\Phi : \ P_4 \to \mathrm{Aut}(N_3)$. Die zwei Möglichkeiten für P_4 führen zu den Isomorphietypen

(iii) $G \cong N_3 \times_\Phi \mathbb{Z}/4\mathbb{Z}$,
(iv) $G \cong N_3 \times_\Phi (\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z})$.

Unabhängig von der Wahl des Homomorphismus Φ ist der Isomorphietyp festgelegt: Ein Automorphismus von N_3 muss Elemente der Ordnung 2 wieder auf Elemente der Ordnung 2 abbilden, also gibt es nur die beiden Automorphismen id und τ, wobei τ die beiden Elemente der Ordnung 2 in N_3 vertauscht. Für $P_4 \cong \mathbb{Z}/4\mathbb{Z}$ ist Φ dann durch das Bild eines Erzeugers von P_4 festgelegt. Ist dessen Bild id, so liegt tatsächlich das innere direkte Produkt vor, im Widerspruch zur Annahme, dass U kein Normalteiler ist. Also bleibt nur τ als mögliches Bild, und Φ ist festgelegt. Im Fall $P_4 \cong (\mathbb{Z}/2\mathbb{Z}) \times (\mathbb{Z}/2\mathbb{Z})$ wird P_4 von den Elementen $(\bar{0}, \bar{1})$ und $(\bar{1}, \bar{0})$ erzeugt. Eines dieser Elemente muss durch Φ auf τ abgebildet werden, sonst wäre U ein Normalteiler. Wird auch das zweite Element auf τ abgebildet, so folgt wegen $\tau^2 = \mathrm{id}$, dass id das Bild von $(\bar{1}, \bar{1})$ ist. Ist id das Bild von $(\bar{1}, \bar{0})$, so ist umgekehrt τ das Bild von $(\bar{1}, \bar{1})$. In jedem Fall werden also genau zwei Elemente von P_4 auf τ und genau zwei Elemente auf id abgebildet. Tatsächlich handelt es sich bis auf Umbenennung der Elemente von P_4 also um den gleichen Homomorphismus Φ, und die zugehörigen semidirekten Produkte sind zueinander isomorph.

Fall 3:
G hat einen Normalteiler N_4 aber keinen Normalteiler N_3. Im letzten Abschnitt wurde gezeigt, dass dann

(v) $G \cong \mathcal{A}_4$

ist. Insgesamt gibt es also fünf Isomorphietypen von Gruppen der Ordnung 12.

Beispiel 1.8.3
Jede einfache Gruppe G der Ordnung 60 ist isomorph zu $\mathcal{A}_5$.

Lemma 1.8.8
G besitzt keine Untergruppe U mit $12 < |U| < 60$.

Beweis
Nach Satz 1.8.4 ist das Herz $H_G(U)$ ein Normalteiler von G mit $H_G(U) \trianglelefteq U$ und $(G : H_G(U)) \mid m!$, wobei $m = (G : U)$ ist. Aus $12 < |U| < 60$ folgt $1 < m \leq 4$, aber wegen $H_G(U) \neq \{1\}, G$ wäre G dann nicht einfach. □

Lemma 1.8.9
G besitzt eine Untergruppe U mit $|U| = 12$.

Beweis
Es sei $P_2 \in \mathrm{Syl}_2(G)$, also $|P_2| = 4$. Nach dem vorigen Lemma ist $|N_G(P_2)| = 4$ oder 12, also $|\mathrm{Syl}_2(G)| = |G|/|N_G(P_2)| = 5$ oder 15.
Fall 1: Es gibt 15 2-Sylowgruppen $P_2^{(1)}, \ldots, P_2^{(15)}$ mit $P_2^{(i)} \cap P_2^{(j)} = \{1\}$ für $i \neq j$. Diese 15 2-Sylowgruppen enthalten zusammen 45 Elemente der Ordnung $\neq 5$, damit enthält G höchstens $60 - 45 = 15$ Elemente der Ordnung 5. Es ist $|\mathrm{Syl}_5(G)| = 1$ oder 6. Wäre $|\mathrm{Syl}_5(G)| = 6$, so enthielten die 5-Sylowgruppen zusammen 24 Elemente der Ordnung 5, ein Widerspruch. Damit ist $|\mathrm{Syl}_5(G)| = 1$, und die einzige 5-Sylowgruppe ist ein Normalteiler von G im Widerspruch zur Einfachheit von G. Fall 1 ist also unmöglich.
Fall 2: Es gibt zwei 2-Sylowgruppen $P_2^{(i)}, P_2^{(j)}$ mit $|P_2^{(i)} \cap P_2^{(j)}| = 2$. Wegen $P_2^{(i)} \cap P_2^{(j)} \trianglelefteq P_2^{(i)}$ und $P_2^{(i)} \cap P_2^{(j)} \trianglelefteq P_2^{(j)}$ folgt $|N_G(P_2^{(i)} \cap P_2^{(j)})| \geq 12$, nach dem vorigen Lemma bleibt nur $|N_G(P_2^{(i)} \cap P_2^{(j)})| = 12$.
Fall 3: $|\mathrm{Syl}_2(G)| = 5 \Rightarrow |N_G(P_2)| = 12$.

□

Beweis von Beispiel 1.8.3:
Wir betrachten die Operation von G auf der Menge $\mathbf{M} = G/U$ der Linksnebenklassen von U in G. Die dazu gehörende Permutationsdarstellung $\Phi : G \to \mathfrak{S}(M)$, $g \mapsto l_g$ ist ein Homomorphismus von G in $\mathfrak{S}(M) \cong \mathfrak{S}_5$ mit $\Phi(G) \neq \{\mathrm{id}\}$. Also gibt es einen Homomorphismus $\psi : G \to \mathfrak{S}_n$ mit $\mathrm{Ker}(\psi) \trianglelefteq G$ und $\mathrm{Ker}(\psi) \neq G$. Wegen der Einfachheit von G ist $\mathrm{Ker}(\psi) = \{1\}$. Damit ist ψ ein Monomorphismus und $G \cong \psi(G) \trianglelefteq \mathfrak{S}_5$, woraus $\psi(G) = \mathcal{A}_5$ folgt (Übungsaufgabe). □

Die Sylowgruppen einer Gruppe sind so genannte p-Gruppen, deren Studium sich aus diesen und anderen Gründen lohnt.

Definition 1.8.7
Es sei p eine Primzahl. Eine Gruppe G mit $|G| = p^\alpha$ heißt p-Gruppe.

Satz 1.8.10
Jede p-Gruppe G besitzt ein nicht triviales Zentrum $Z(G)$, d. h. $Z(G) \neq \{1\}$.

BEWEIS
Es sei $|G| = p^\alpha$ und $G = \{1\} \dot\cup U(h_1) \dot\cup \cdots \dot\cup U(h_l)$ die Partition von G in Konjugationsklassen $U(h_i) = \{gh_ig^{-1} \mid g \in G\}$. Es ist $h_i \in Z(G) \Leftrightarrow \forall g \in G : \ gh_ig^{-1} = h_i \Leftrightarrow U(h_i) = \{h_i\}$. Nach Satz 1.8.1 ist $|U(h_i)| = |G|/|C_G(h_i)|$, also $h_i \in Z(G) \Leftrightarrow |C_G(h_i)| = p^\alpha \Leftrightarrow p \nmid |U(h_i)| \Leftrightarrow |U(h_i)| = 1$. Nun ist $|G| = p^\alpha = 1 + |U(h_1)| + \cdots + |U(h_l)|$. Damit muss $p \nmid |U(h_i) \Leftrightarrow h \in Z(G)$ für mindestens ein $h_i \neq 1$ gelten, also $Z(G) \neq \{1\}$. □

1.9. Auflösbare Gruppen

Der Name auflösbar erklärt sich aus der Anwendung auf Fragen der Auflösbarkeit von algebraischen Gleichungen durch Radikale.

DEFINITION 1.9.1
Wir schreiben $N \lhd G$ (oder $G \rhd N$), falls N Normalteiler von G, aber $N \neq G$ ist.

DEFINITION 1.9.2
Sei G eine Gruppe:

(a) Unter einer Normalreihe von G versteht man eine Folge sukzessiver Normalteiler

$$(*) : \ G \ = \ N_0 \rhd \ N_1 \ \rhd \cdots \rhd \ N_k = \{1_G\} \, ,$$

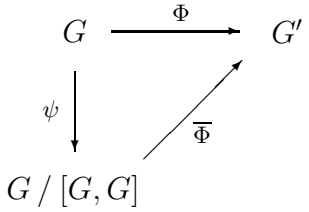
so dass $N_i \lhd N_{i-1}$ Normalteiler von N_{i-1} ist. Die Faktorgruppen N_{i-1}/N_i heißen Faktoren der Normalreihe.
(b) G heißt auflösbar, falls es eine Normalreihe von G der Form $(*)$ mit abelschen Faktoren N_{i-1}/N_i gibt.
(c) Eine Normalreihe der Form $(*)$ heißt Kompositionsreihe von G, wenn die Faktoren N_{i-1}/N_i einfach sind.

DEFINITION 1.9.3
Es sei G eine Gruppe:

(a) Für $g, h \in G$ heißt $[g, h] := ghg^{-1}h^{-1}$ der Kommutator von g und h.
(b) Die von allen Kommutatoren erzeugte Untergruppe $[G, G] := \langle \{[g, h] \mid g, h \in G\} \rangle$ heißt Kommutatorgruppe von G.

SATZ 1.9.1
Es sei G eine Gruppe, dann gilt:

(a) $[G, G] = \{[a_1, b_1] \ \cdot \ \cdots \ \cdot \ [a_r, b_r] \mid a_i, b_i \in G \ , \ r \in \mathbb{N}\}$.
(b) *$[G, G]$ ist Normalteiler von G.*
(c) *Es sei $N \trianglelefteq G$. Die Faktorgruppe G/N ist kommutativ genau dann, wenn $[G, G] \trianglelefteq N$ ist.*
(d) *(Universelle Abbildungseigenschaft) Es sei $\psi : \ G \to G/[G, G]$, $g \mapsto g[G, G]$ der kanonische Epimorphismus von G auf $G/[G, G]$. Für jeden Homomorphismus $\Phi : G \to G'$ von G in eine kommutative Gruppe G' existiert genau ein Homomorphismus $\overline{\Phi} : G/[G, G] \to G'$ mit $\Phi = \overline{\Phi} \circ \psi$, d. h. zu Φ gibt es stets $\overline{\Phi}$, so dass das Diagramm*



kommutiert.

BEWEIS
(a): Nach Satz 1.1.2 ist $[G,G] = \{g_1 \cdots g_l h_1 \cdots h_m \mid g_j = [a_j, b_j],\ h_j^{-1} = [c_j, d_j],\ a_j, b_j, c_j, d_j \in G\}$. Es ist $h_j = (c_j d_j c_j^{-1} d_j^{-1})^{-1} = [d_j, c_j]$. (b): Es sei $c \in [G,G]$ und $g \in G$. Dann ist $gcg^{-1} = gcg^{-1}c^{-1}c = [g,c]c \in [G,G]$. Damit $[G,G] \trianglelefteq G$. (c): G/N kommutativ$\Leftrightarrow \forall g,h \in G:\ N(gh) = N(hg) \Leftrightarrow \forall g,h \in G:\ N[g,h] = N \Leftrightarrow [G,G] \trianglelefteq N$. (d): Wir definieren $\overline{\Phi}$ durch

$$\overline{\Phi} := \begin{cases} G/[G,G] & \to & G \\ g[G,G] & \mapsto & \Phi(g) \end{cases}.$$

Die Abbildung $\overline{\Phi}$ ist wohldefiniert, denn wegen Teil a) gilt $g_1[G,G] = g_2[G,G] \Rightarrow g_2^{-1}g_1 \in [G,G] \Rightarrow g_2^{-1}g_1 = [a_1,b_1]\cdots[a_r,b_r]$ für $a_j, b_j \in G$. Daraus folgt nun

$$\Phi(g_2^{-1}g_1) \ = \ [\Phi(a_1),\Phi(b_1)]\cdots[\Phi(a_r),\Phi(b_r)] = 1_{G'}$$

da G' abelsch ist. Also ist $\Phi(g_1) = \Phi(g_2)$. Die übrigen Eigenschaften von $\overline{\Phi}$ sind klar. □

SATZ 1.9.2
Für eine Gruppe G sind folgende Aussagen äquivalent:

(i) *G ist auflösbar.*
(ii) *Es gibt ein $n \in \mathbb{N}$ mit $G^{(n)} = \{1\}$. Dabei ist $G^{(n)}$ rekursiv durch $G^{(0)} := G$ und $G^{(i+1)} := [G^{(i)}, G^{(i)}]$ definiert.*

BEWEIS
(i)⇒(ii): Es sei $G = G_0 \triangleright \cdots \triangleright G_n = \{1\}$ eine Normalreihe mit abelschen Faktoren. Wir zeigen durch Induktion nach i: $G^{(i)} \subseteq G_i$.
$\underline{i = 0}$: ist klar.
$\underline{(i-1) \ \to \ i}$: Da G_{i-1}/G_i abelsch ist, folgt nach Satz 1.9.1 und der Induktionshypothese $G_i \supseteq [G_{i-1}, G_{i-1}] \supseteq [G^{i-1}, G^{i-1}] = G^{(i)}$. (ii)⇒(i): Nach Satz 1.9.1 ist $G = G^{(0)} \triangleright G^{(1)} \triangleright \cdots \triangleright G^{(n)}$ eine Normalreihe mit abelschen Faktoren. □

SATZ 1.9.3
Es sei G eine auflösbare Gruppe, dann gilt:

(a) *Jede Untergruppe $U < G$ ist auflösbar.*
(b) *Ist $\Phi : G \to G'$ ein Epimorphismus, so ist auch G' auflösbar.*

BEWEIS
(a): folgt sofort nach Satz 1.9.2. (b): folgt wegen $\Phi(G)^{(i)} = \Phi(G^{(i)})$ aus Satz 1.9.2. □

SATZ 1.9.4
Es sei G eine Gruppe, N ein Normalteiler von G und $\Phi : G \to G/N$ der kanonische Epimorphismus:

(a) *Es seien*

$$(1): G/N = H_0 \triangleright H_1 \triangleright \cdots \triangleright H_k = \{N\}$$

eine Normalreihe von G/N und

$$(2): N = N_0 \triangleright N_1 \triangleright \cdots \triangleright N_l = \{1\}$$

eine Normalreihe von N und $G_i := \Phi^{-1}(H_i)$ für $1 \leq i \leq k$. Dann ist

$$(3): G = G_0 \triangleright G_1 \triangleright \cdots \triangleright G_k = N = N_0 \triangleright N_1 \triangleright \cdots \triangleright N_l = \{1\}$$

eine Normalreihe von G. Es ist $G_{i-1}/G_i \cong H_{i-1}/H_i$.

(b) *G ist auflösbar genau dann, wenn N und G/N auflösbar sind.*

BEWEIS
(a): Nach dem 2. Isomorphiesatz 1.5.3 sind die $G_i = \Phi^{-1}(H_i)$ Normalteiler von G mit $N \trianglelefteq G_i$, und es ist $H_{i-1}/H_i = (G_{i-1}/N) \,/\, (G_i/N) \cong G_{i-1}/G_i$. Daraus ergibt sich (a). (b): $\Rightarrow$ folgt nach Satz 1.9.3. $\Leftarrow$: Aus der Auflösbarkeit von G/N und N folgen die Existenz von Normalreihen der Form (1) und (2) mit abelsche Faktoren H_{i-1}/H_i und N_{i-1}/N_i. Wegen $G_{i-1}/G_i \cong H_{i-1}/H_i$ ist dann (3) eine Normalreihe von G mit abelschen Faktoren, d. h. G ist auflösbar. □

SATZ 1.9.5
Ein endliche Gruppe $G \neq \{1\}$ ist auflösbar genau dann, wenn sie eine Kompositionsreihe besitzt, deren Faktoren zyklische Gruppen von Primzahlordnung sind.

BEWEIS
$\Leftarrow$: folgt sofort aus der Definition der Auflösbarkeit. $\Rightarrow$: wir nehmen an die Aussage sei falsch. Es sei G ein „kleinster Verbrecher", d. h. $G \neq \{1\}$ sei eine Gruppe kleinster Ordnung, die zwar auflösbar ist, jedoch keine Normalreihe der beschriebenen Art besitzt. Annahme: G ist einfach. Dann ist $G \triangleright \{1\}$ die einzige Normalreihe von G. Also ist G abelsch, und damit nach Satz 1.7.6 von Primzahlordnung, Widerspruch. G ist also nicht einfach, d. h. es gibt $N \triangleleft G$ mit $\{1\} \triangleleft N \triangleleft G$. Dann sind nach Satz 1.9.4(a) G/N und N auflösbar, und da G der kleinste Verbrecher ist, besitzen G/N und N Kompositionsreihen, deren Faktoren zyklisch von Primzahlordnung sind. Nach Satz 1.9.4(a) lassen sich diese zu einer Kompositionsreihe von G zusammenfügen, Widerspruch. □

SATZ 1.9.6
Jede p-Gruppe ist auflösbar.

BEWEIS
Es sei G ein „kleinster Verbrecher", d. h. es sei $|G| = p^\alpha$ und G eine Gruppe kleinster Ordnung, die nicht auflösbar ist. Nach Satz 1.8.10 besitzt G ein Zentrum $Z(G) \neq \{1\}$. Es ist aber $|Z(G)| = p^\beta$ mit $1 \leq \beta \leq \alpha$. Da G der kleinste Verbrecher ist, ist $G/Z(G)$ auflösbar. Nach Satz 1.9.4 ist G auflösbar, Widerspruch. □

Ein tiefer Satz von Feit-Thompson (1963) sagt: Jede Gruppe ungerader Ordnung ist auflösbar. Nicht jede Gruppe besitzt eine Kompositionsreihe, jedoch jede endliche Gruppe.

Wir erwähnen ohne Beweis den wichtigen

SATZ 1.9.7 (Jordan-Hölder)
Es seien

$$G = G_0 \triangleright G_1 \triangleright \cdots \triangleright G_r = \{1\}$$
$$G = H_0 \triangleright H_1 \triangleright \cdots \triangleright H_s = \{1\}$$

zwei Kompositionsreihen einer Gruppe G. Dann ist $r = s$, und die Faktoren beider Kompositionsreihen sind bis auf die Reihenfolge isomorph, d. h. es existiert ein $\sigma \in \mathfrak{S}_r$ mit

$$G_i \,/\, G_{i+1} \;\cong\; H_{\sigma(i)} \,/\, H_{\sigma(i)+1} \;.$$

2. Ringtheorie

2.1. Ringe und Ideale

DEFINITION 2.1.1
Es sei R eine Menge, auf der die Verknüpfungen $+ : R \times R \to R$ (Addition) und $\cdot : R \times R \to R$ (Multiplikation) definiert sind. $(R, +, \cdot)$ heißt ein Ring, falls $(R, +)$ eine abelsche Gruppe und $(R, \cdot)$ eine Halbgruppe ist, und außerdem für alle $a, b, c \in R$ gilt:

$$\begin{array}{rcll} a \cdot (b + c) & = & a \cdot b + a \cdot c & \text{und} \\ (b + c) \cdot a & = & b \cdot a + c \cdot a & \text{(Distributivgesetze)} \end{array}$$

(Dabei wird die Regel „Punkt vor Strich" angewandt: $a \cdot b + c := (a \cdot b) + c$)
Das neutrale Element der Gruppe $(R, +)$ heißt Null des Rings R. Für $a \in R$ wird das Inverse bzgl. $+$ mit $-a$ bezeichnet („minus a"), und heißt auch das Negative von a. R heißt Ring mit Eins, falls ein (eindeutiges) Element $1 \in R$ existiert mit $1 \cdot a = a \cdot 1$ für alle $a \in R$. R heißt kommutativer Ring, falls für alle $a, b \in R$ gilt: $a \cdot b = b \cdot a$. R heißt entsprechend kommutativer Ring mit Eins, falls R Ring mit Eins und kommutativer Ring ist.

Aus den Distributivgesetzen folgt sofort:

SATZ 2.1.1
Es sei $(R, +, \cdot)$ ein Ring. Für alle $a, b \in R$ gilt:

(a) $a \cdot 0 = 0 \cdot a = 0$,
(b) $a \cdot (-b) = -(a \cdot b) = (-a) \cdot b$,
(c) $(-a) \cdot (-b) = a \cdot b$.

BEISPIEL 2.1.1
Es sei $R = \{0\}$. Setzt man $0 + 0 = 0$ und $0 \cdot 0 = 0$, so ist $(R, +, \cdot)$ ein kommutativer Ring mit Eins. Es ist $1_R = 0_R$. Dieser Ring heißt Nullring. Aus Satz 2.1.1 folgt sofort, dass für jeden Ring $(R, +, \cdot)$ mit Eins, für den $1_R = 0_R$ gilt, auch $R = \{0\}$ folgt.

DEFINITION 2.1.2
Es sei $(R, +, \cdot)$ ein Ring.

(a) $a \in R$ heißt linker bzw. rechter Nullteiler, wenn es $x \in R$ mit $x \neq 0_R$ und $a \cdot x = 0_R$ bzw. $x \cdot a = 0_R$ gibt. R heißt nullteilerfrei, wenn R außer 0_R keine Nullteiler besitzt.
(b) R heißt Integritätsring, wenn R ein kommutativer Ring mit Eins und nullteilerfrei ist, und wenn $1_R \neq 0_R$ gilt.
(c) Es sei R ein Ring mit Eins und $1_R \neq 0_R$. $a \in R$ heißt Einheit, falls es ein $b \in R$ gibt mit $a \cdot b = b \cdot a = 1_R$. Wie man leicht sieht, bildet die Menge aller Einheiten in R bzgl. der Multiplikation eine Gruppe, die Einheitengruppe von R, die mit R^* bezeichnet wird.
(d) R heißt Schiefkörper, wenn R ein Ring mit Eins ist, $1_R \neq 0_R$, und $R^* = R \backslash \{0_R\}$ gilt. Ist R zusätzlich ein kommutativer Ring, so heißt R ein Körper.

BEISPIEL 2.1.2
$(\mathbb{Z}, +, \cdot)$ ist ein Integritätsring. Die Einheitengruppe ist $\mathbb{Z}^* = \{1, -1\}$.

BEISPIEL 2.1.3
Es sei R ein Ring, $n \in \mathbb{N}$ und $R^{(n,n)}$ die Menge der Matrizen vom Typ (n, n) mit Elementen in

R. Dann ist auch $(R^{(n,n)}, +, \cdot)$ ein Ring. Ist R ein Ring mit Eins, so ist auch $(R^{(n,n)}, +, \cdot)$ ein Ring mit Eins. Die Eins ist dann die Einheitsmatrix

$$E_n = \begin{pmatrix} 1_R & 0_R & \cdots & 0_R \\ 0_R & 1_R & \cdots & 0_R \\ \vdots & \vdots & \ddots & \vdots \\ 0_R & 0_R & \cdots & 1_R \end{pmatrix} .$$

Andere Eigenschaften von R, wie beispielsweise Kommutativität oder Nullteilerfreiheit, übertragen sich im Allgemeinen nicht auf $R^{(n,n)}$.

Im Rest dieses Kapitels betrachten wir nur noch Ringe mit Eins. Die Existenz des Einselements wird im Folgenden stets vorausgesetzt, ohne dass es explizit festgestellt wird.

DEFINITION 2.1.3
Es seien $(R, +, \cdot)$ und $(S, \boxplus, \boxdot)$ Ringe.

(a) Eine Abbildung $\Phi : R \to S$ heißt (Ring-)homomorphismus, falls für alle $a, b \in R$ gilt:
  (i) $\Phi(a + b) = \Phi(a) \boxplus \Phi(b)$,
  (ii) $\Phi(a \cdot b) = \Phi(a) \boxdot \Phi(b)$,
  (iii) $\Phi(1_R) = 1_S$.
  Die Menge $\mathrm{Ker}(\Phi) = \{r \in R \mid \Phi(r) = 0_S\}$ wird der Kern von Φ genannt. Ein bijektiver, injektiver bzw. surjektiver (Ring-)homomorphismus heißt (Ring-)isomorphismus, (Ring-)monomorphismus bzw. (Ring-)epimorphismus.

(b) Es sei $(R, +, \cdot)$ ein Ring. Eine nicht leere Teilmenge T von R heißt Teilring von R, falls $(T, +) \leq (R, +)$, $1_R \in T$ und $t_1 \cdot t_2 \in T$ für alle $t_1, t_2 \in T$ gilt. R heißt Oberring von T (Bezeichnung: $T \leq R$).

(c) Eine Teilmenge $J \subseteq R$ heißt Ideal (bzw. zweiseitiges Ideal) von R, falls $(J, +) \leq (R, +)$ und $r \cdot a, a \cdot r \in J$ für alle $a \in J$ und $r \in R$ gilt. Schreibweise: $J \trianglelefteq R$.

(d) Es sei $M \subseteq R$. Das kleinste Ideal

$$\bigcap_{\substack{J \trianglelefteq R \\ M \subseteq J}} J$$

welches M enthält, heißt das von M erzeugte Ideal, und wird mit (M) bezeichnet. J heißt Hauptideal von R, falls $J = (\{m\})$ für ein $m \in R$ gilt. In diesem Fall schreiben wir auch $J = (m)$.

BEMERKUNG 2.1.1
Ist R kommutativ und $m \in R$, so hat das von m erzeugte Hauptideal offenbar die Form

$$(m) = \{mr \mid r \in R\} = mR = Rm .$$

Zwischen Ringhomomorphismen und Idealen besteht ein Zusammenhang, der dem zwischen Gruppenhomomorphismen und Normalteilern entspricht. Zunächst wird die Menge der Nebenklassen definiert, indem lediglich die Addition betrachtet wird.

DEFINITION 2.1.4
Es sei $(R, +, \cdot)$ ein Ring, J ein Ideal von R. Unter einer Restklasse von J in R versteht man eine Nebenklasse der Untergruppe $(J, +)$ von $(R, +)$ im Sinne von Definition 1.3.5. Die Menge aller Restklassen wird mit R / J bezeichnet: $R / J = \{x + J \mid x \in R\}$.

SATZ 2.1.2
Es sei $(R,+,\cdot)$ ein Ring, $J \trianglelefteq R$ ein Ideal und $\Phi : (R,+) \to (R/J,+)$ der kanonische Epimorphismus (der Gruppen bzgl $+$). Dann gibt es genau eine Verknüpfung „$\cdot$" (für die wir die selbe Bezeichnung verwenden, wie für die Multiplikation auf R) auf R/J, so dass $(R/J,+,\cdot)$ ein Ring und Φ ein Ringhomomorphismus ist, und zwar ist $\cdot$ definiert durch

$$\forall x,y \in R : \ (x+J) \ \cdot \ (y+J) \ = \ (x \cdot y) \ + \ J \, .$$

BEWEIS
Wir zeigen, dass das Produkt zweier Restklassen wohldefiniert ist. Es seien

(1) $x_1 + J = x_2 + J$, $y_1 + J = y_2 + J$. Zu zeigen:
(2) $(x_1 \cdot y_1) + J = (x_2 \cdot y_2) + J$.

(1)$\Rightarrow x_1 - x_2 \in J$, $y_1 - y_2 \in J \Rightarrow (x_1 - x_2) \cdot y_1 \in J \Rightarrow (x_1 \cdot y_1) + J = (x_2 \cdot y_1) + J$. Aber ebenso (1)$\Rightarrow x_2 \cdot (y_1 - y_2) \in J \Rightarrow (x_2 \cdot y_1) + J = (x_2 \cdot y_2) + J$, also (2). Die Rechenregeln (Assoziativgesetz und Distributivgesetze) folgen aus den entsprechenden Regeln in R. Die Restklasse $1 + J$ ist neutrales Element der Multiplikation in R/J. Damit ist $(R/J,+,\cdot)$ ein Ring mit Eins und Φ ein Ringhomomorphismus. Wegen $x \cdot y + J = \Phi(x \cdot y) = \Phi(x) \cdot \Phi(y) = (x+J) \cdot (y+J)$ ist $\cdot$ die einzige mögliche Multiplikation auf R/J mit den geforderten Eigenschaften. □

DEFINITION 2.1.5
Der Ring $(R/J,+,\cdot)$ von Satz 2.1.2 heißt Restklassenring von R modulo J.

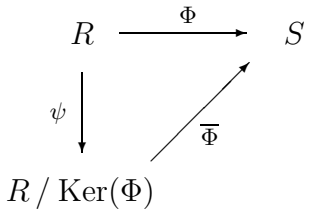
Wie im Homomorphiesatz der Gruppentheorie (Satz 1.5.1) betrachten wir nun die umgekehrte Situation. Es sei ein Ringhomomorphismus $\Phi : R \to S$ gegeben. Gesucht ist ein Restklassenring, der zu dem Bild $\Phi(R)$ isomorph ist.

SATZ 2.1.3 (Homomorphiesatz für Ringe)
Es seien R, S Ringe und $\Phi : R \to S$ ein Ringhomomorphismus:

(a) $\mathrm{Ker}(\Phi)$ *ist ein Ideal von R und $\Phi(R)$ ist ein Teilring von S,*
(b) *Die Abbildung*

$$\overline{\Phi} \ = \ \begin{cases} R \,/\, \mathrm{Ker}(\Phi) & \to \quad \Phi(R) \\ x + \mathrm{Ker}(\Phi) & \mapsto \quad \Phi(x) \end{cases}$$

ist ein Ringisomorphismus, also $R/\mathrm{Ker}(\Phi) \cong \Phi(R)$. Ist ψ der kanonische Epimorphismus von R auf $R/\mathrm{Ker}(\Phi)$, so ist $\Phi = \psi \circ \overline{\Phi}$, d. h. das Diagramm



ist kommutativ.
(c) Φ *ist ein Monomorphismus genau dann, wenn* $\mathrm{Ker}(\Phi) = \{0_R\}$ *ist.*

BEWEIS
Betrachtet man zunächst nur die Addition allein, so folgen die behaupteten Eigenschaften (beispielsweise $(\mathrm{Ker}(\Phi),+)$ Untergruppe von $(R,+)$) unmittelbar aus dem Homomorphiesatz für Gruppen. Man rechnet unmittelbar nach, dass auch die Eigenschaften, die die Multiplikation betreffen, erfüllt sind. □

DEFINITION 2.1.6
Es sei R ein kommutativer Ring mit Eins:

(a) Ein Ideal $\mathfrak{p} \trianglelefteq R$ heißt Primideal, wenn $\mathfrak{p} \neq R$ ist und folgende Eigenschaft erfüllt ist: für alle $a, b \in R$ mit $a \cdot b \in \mathfrak{p}$ gilt stets $a \in \mathfrak{p}$ oder $b \in \mathfrak{p}$.
(b) Ein Ideal $\mathfrak{m} \trianglelefteq R$ heißt maximales Ideal, wenn $\mathfrak{m} \neq R$ ist und folgendes gilt: für jedes Ideal J von R mit $\mathfrak{m} \subseteq J \neq R$ gilt $\mathfrak{m} = J$.

SATZ 2.1.4
Es sei R ein kommutativer Ring mit Eins:

(a) *Ein Ideal $\mathfrak{p}$ von R ist genau dann ein Primideal, wenn $R/\mathfrak{p}$ ein Integritätsring ist.*
(b) *Ein Ideal $\mathfrak{m}$ von R ist genau dann ein maximales Ideal, wenn $R/\mathfrak{m}$ ein Körper ist.*
(c) *Jedes maximale Ideal ist auch ein Primideal.*

BEWEIS
Hinrichtung von (a): Es sei $\mathfrak{p}$ ein Primideal, es ist zu zeigen, dass $R/\mathfrak{p}$ nullteilerfrei ist. Es seien $a, b \in R$ mit $(a + \mathfrak{p})(b + \mathfrak{p}) = 0_R + \mathfrak{p}$. Dann ist auch $(a \cdot b) + \mathfrak{p} = 0_R + \mathfrak{p}$, also $a \cdot b \in \mathfrak{p}$. Da $\mathfrak{p}$ prim ist folgt $a \in \mathfrak{p}$ oder $b \in \mathfrak{p}$, d. h. $a + \mathfrak{p} = 0_R + \mathfrak{p}$ oder $b + \mathfrak{p} = 0_R + \mathfrak{p}$. Rückrichtung: Sei $R/\mathfrak{p}$ ein Integritätsring. Wegen $R/\mathfrak{p} \neq \{0 + \mathfrak{p}\}$ ist $\mathfrak{p} \neq R$. Sind nun $a, b \in R$ mit $a \cdot b \in \mathfrak{p}$ gegeben, und gilt $0_R + \mathfrak{p} = (a \cdot b) + \mathfrak{p} = (a + \mathfrak{p}) \cdot (b + \mathfrak{p})$, dann ist $a + \mathfrak{p} = 0_R + \mathfrak{p}$ oder $b + \mathfrak{p} = 0_R + \mathfrak{p}$, also $a \in \mathfrak{p}$ oder $b \in \mathfrak{p}$. Hinrichtung von (b): Es sei $\mathfrak{m} \trianglelefteq R$ ein maximales Ideal, dann ist

$$a + \mathfrak{m} \ \in \ R / \mathfrak{m} \ - \ \{0_R + \mathfrak{m}\} \ \Leftrightarrow \ a \notin \mathfrak{m} \, .$$

Zu zeigen ist also: $a + \mathfrak{m}$ besitzt in diesem Fall ein multiplikatives Inverses. Wir betrachten das Ideal $J = (\{a\}, \mathfrak{m}) = aR + \mathfrak{m}$. Es ist $J \neq \mathfrak{m}$, da $a = 1_R \cdot a \in J$ aber $a \notin \mathfrak{m}$. Wegen der Maximalität von $\mathfrak{m}$ folgt $J = R$, insbesondere $1_R \in J$, d. h. es gibt $r \in R$ mit $a \cdot r + \mathfrak{m} = 1_R + \mathfrak{m}$, daraus folgt $1_R + \mathfrak{m} = a \cdot r + \mathfrak{m} = (a + \mathfrak{m}) \cdot (b + \mathfrak{m})$. Rückrichtung: Es sei $R/\mathfrak{m}$ ein Körper und $J \trianglelefteq R$ mit $\mathfrak{m} \subseteq J \subseteq R$ und $J \neq \mathfrak{m}$. Zu zeigen ist $J = R$. Es gibt $a \in J - \mathfrak{m}$, also $a + \mathfrak{m} \neq 0 + \mathfrak{m}$. Das multiplikative Inverse von $a + \mathfrak{m}$ sei $r + \mathfrak{m}$ mit $r \in R$, d. h. $(a + \mathfrak{m}) \cdot (r + \mathfrak{m}) = (a \cdot r) + \mathfrak{m} = 1_R + \mathfrak{m}$. Wegen $a \cdot r \in J$ ist $1_R \in J$, woraus $J = R$ folgt. □

SATZ 2.1.5
Für $p \in \mathbb{Z}$ mit $p \geq 1$ sind äquivalent:

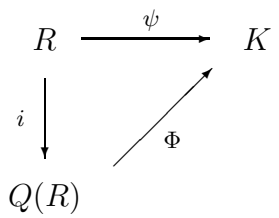
(i) *p ist Primzahl,*
(ii) *$(\mathbb{Z}/p\mathbb{Z}, +, \cdot)$ ist Integritätsring,*
(iii) *$(\mathbb{Z}/p\mathbb{Z}, +, \cdot)$ ist ein Körper.*

BEWEIS
Die Kette (iii)⇒(ii)⇒(i) ist klar. Es bleibt (i)⇒(iii) zu zeigen, d. h. dass $p\mathbb{Z}$ ein maximales Ideal von $\mathbb{Z}$ ist. Es sei $J \trianglelefteq \mathbb{Z}$ ein Ideal mit $p\mathbb{Z} \subseteq J \subseteq \mathbb{Z}$ und $J \neq \mathbb{Z}$. Da $(J, +)$ eine Untergruppe von $(\mathbb{Z}, +)$ ist, folgt mit Satz 1.7.1 $J = a\mathbb{Z}$ für ein $a \in \mathbb{Z}$. Also $p = ab$ mit $a, b \in \mathbb{Z}$. Wegen $a \neq \pm 1$ und p Primzahl folgt $a = \pm p$, also $J = p\mathbb{Z}$. □

2.2. Quotientenkörper

In diesem Abschnitt sei R stets ein Integritätsring. Sie wie der Integritätsring $(\mathbb{Z}, +, \cdot)$ ein Teilring des Körpers $(\mathbb{Q}, +, \cdot)$ der rationalen Zahlen ist, der aus den Quotienten ganzer Zahlen besteht, so kann jeder Integritätsring in einen Quotientenkörper eingebettet werden.

DEFINITION 2.2.1
Es sei R ein Integritätsring. Ein Paar $(Q(R), i)$, bestehend aus einem Körper $Q(R)$ und einem injektiven Ringhomomorphismus $i : R \to Q(R)$ heißt Quotientenkörper von R, wenn er folgende universelle Eigenschaft erfüllt: Für jeden Körper K und jeden injektiven Ringhomomorphismus $\psi : R \to K$ existiert genau ein Ringhomomorphismus $\Phi : Q(R) \to K$ mit $\psi = \Phi \circ i$, d. h. das Diagramm



kommutiert.

Da $Q(R)$ ein Körper ist, ist Φ injektiv. Aufgrund der Eindeutigkeitsaussage für Φ ist klar, dass das Paar $(Q(R), i)$ bis auf Isomorphie eindeutig bestimmt ist. Im Fall $R = \mathbb{Z}$ ist $Q(\mathbb{Z}) = \mathbb{Q}$ der Körper der rationalen Zahlen.

SATZ 2.2.1
Es sei R ein Integritätsring:

(a) *Auf* $M := \{(a, b) \mid a \in R,\ b \in R - \{0_R\}\ \}$ *erklärt man die Äquivalenzrelation*

$$(a, b) \sim (a', b') \ \Leftrightarrow\ a \cdot b' = a' \cdot b$$

(b) *Bezeichnet man mit* $\frac{a}{b}$ *die Äquivalenzklasse von* (a, b) *unter* $\sim$, *so ist*

$$Q(R) \ = \ \{\frac{a}{b} \mid a \in R,\ b \in R - \{0_R\}\}$$

eine Menge, wobei die Identität $\frac{a}{b} = \frac{a'}{b'} \Leftrightarrow ab' = a'b$ *erklärt ist. Auf* $Q(R)$ *erklärt man die Verknüpfungen*

$$\frac{a_1}{b_1} \ + \ \frac{a_2}{b_2} \ := \ \frac{a_1 b_2 + a_2 b_1}{b_1 b_2}$$

$$\frac{a_1}{b_1} \ \cdot \ \frac{a_2}{b_2} \ := \ \frac{a_1 a_2}{b_1 b_2} \quad .$$

Damit ist $(Q(R), +, \cdot)$ *ein Körper.*

(c) *Die Abbildung* $i : R \to Q(R)$, $r \mapsto \frac{r}{1}$ *ist ein injektiver Ringhomomorphismus.*

(d) $(Q(R), i)$ *ist der Quotientenkörper von* R.

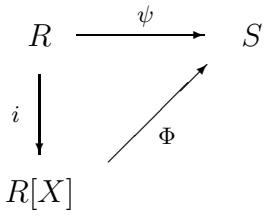
BEWEIS
Symmetrie und Reflexivität der Relation $\sim$ sind klar. Zur Transitivität: Es seien $(a_1, b_1) \sim (a_2, b_2)$ und $(a_2, b_2) \sim (a_3, b_3)$. Daraus folgt $a_1 \cdot b_2 = a_2 \cdot b_1$ und $a_2 \cdot b_3 = a_3 \cdot b_2$, also $a_1 b_2 b_3 = a_2 b_1 b_3 = b_1 a_3 b_2$ und damit $b_2(a_1 b_3) = b_2(a_3 b_1)$. Wegen der Nullteilerfreiheit von R kann der gemeinsame Faktor b_2 „gekürzt" werden: $(a_1, b_1) \sim (a_3, b_3)$. Wir zeigen, dass die Addition wohldefiniert ist: Es seien $\frac{a_1}{b_1} = \frac{\alpha_1}{\beta_1}$ und $\frac{a_2}{b_2} = \frac{\alpha_2}{\beta_2}$, also $a_1\beta_1 = \alpha_1 b_1$ und $a_2\beta_2 = \alpha_2 b_2$. Dann folgt $(a_1 b_2 + a_2 b_1)\beta_1\beta_2 = a_1\beta_1 b_2\beta_2 + a_2\beta_2 b_1\beta_1 = \alpha_1 b_1 b_2\beta_2 + a_2 b_2 b_1\beta_1 = (\alpha_1\beta_2 + \alpha_2\beta_1)b_1 b_2$. Es ist unmittelbar einsichtig, dass die Multiplikation wohldefiniert ist. Man rechnet leicht nach, dass $(Q(R), +, \cdot)$ ein Körper ist mit Nullelement $\frac{0}{1}$, dem Negativen $\frac{-a}{b}$ zu $\frac{a}{b}$, dem Einselement $\frac{1}{1}$ und dem Inversen $\frac{b}{a}$ zu $\frac{a}{b}$. Zu c): Die Abbildung i ist injektiv, denn aus $i(r) = \frac{r}{1} = \frac{0}{1}$ folgt $r \cdot 1_R = 1_R \cdot 0_R = 0_R$, also $r = 0_R$. Damit ist $\mathrm{Ker}(i) = \{0_R\}$. Zu d): Ist $\psi : R \to K$ ein injektiver

Ringhomomorphismus, so ist $\psi(R-\{0_R\}) \subseteq K$. Also ist $\Phi : Q(R) \to K$ mit $\Phi(\frac{a}{b}) := \psi(a)\psi(b)^{-1}$ wohldefiniert und offenbar ein Ringhomomorphismus. $\square$

2.3. Polynomringe

Im Folgenden sei R stets ein kommutativer Ring mit Eins und $\psi : R \to S$ ein Ringhomomorphismus.

DEFINITION 2.3.1
Ein Tripel $(R[X], X, i)$ bestehend aus einem kommutativen Ring $R[X]$, einem ausgezeichneten Element X und einem Ringhomomorphismus $i : R \to R[X]$, heißt Polynomring über R, wenn folgendes gilt: Für jeden Ringhomomorphismus $\psi : R \to S$ in einen kommutativen Ring S und für jedes $x \in S$ gibt es genau einen Ringhomomorphismus $\Phi : R[X] \to S$ mit $\psi = \Phi \circ i$ und $\Phi(X) = x$. Man hat ein kommutatives Diagramm



SATZ 2.3.1
Für jeden kommutativen Ring R mit Eins gilt:

(a) *Es gibt (bis auf Isomorphie) genau einen Polynomring $(R[X], X, i)$ in einer Unbestimmten X über R.*
(b) *Die Abbildung i ist injektiv. Man kann R mit $i(R)$ identifizieren und somit als Unterring von $R[X]$ auffassen. Für jedes $f \in R[X]$ mit $f \neq 0_{R[X]}$ gibt es eindeutig bestimmte $a_0, \ldots, a_n \in R$ mit $a_n \neq 0$, so dass*

$$f \;=\; a_n \cdot X^n + a_{n-1} \cdot X^{n-1} + \cdots + a_1 \cdot X^1 + a_0$$

gilt.

Die Zahl $n \in \mathbb{N}$ heißt Grad von f (Schreibweise: $\deg(f)$). Für $f = 0_{R[X]}$ schreiben wir $\deg(f) = -\infty$.

BEWEIS
Setze

$$R[X] \;:=\; \left\{ \sum_{i=0}^{\infty} a_i \cdot X^i \mid a_i \in R,\ \exists \text{ nur endlich viele } i \text{ mit } a_i \neq 0_R \right\} ,$$

wobei $\sum a_i X^i$ nur ein endlicher formaler Ausdruck mit Koeffizienten $a_i \in R$ ist. Formaler Ausdruck bedeutet, dass gilt

$$\sum_{i=0}^{\infty} a_i X^i \;=\; \sum_{i=0}^{\infty} b_i X^i \;\Leftrightarrow\; \forall i \in \mathbb{N}_0 :\; a_i = b_i \,.$$

In $R[X]$ erklärt man die Verknüpfungen

$$\begin{array}{rcl} (\sum_{i=0}^{\infty} a_i X^i) \;+\; (\sum_{i=0}^{\infty} b_i X^i) & := & (\sum_{i=0}^{\infty} (a_i + b_i) X^i) \\ (\sum_{i=0}^{\infty} a_i X^i) \;\cdot\; (\sum_{i=0}^{\infty} b_i X^i) & := & \left(\sum_{k=0}^{\infty} (\sum_{i+j=k} a_i b_j) X^k \right) \end{array}$$

Dadurch wird $1_{R[X]} = 1_R \cdot X^0$. Man definiert $i: R \to R[X]$, $r \mapsto r \cdot X^0$. Es ist i offenbar ein injektiver Ringhomomorphismus. Zum Nachweis der universellen Eigenschaft gebe man sich (ψ, x) vor, wobei $\psi: R \to S$ ein Ringhomomorphismus ist und $x \in S$ beliebig. Dann definiert man

$$\Phi: R[X] \to S, \ \Phi\left(\sum_{i=0}^{\infty} a_i X^i\right) := \sum_{i=0}^{\infty} \psi(a_i) x^i \ .$$

Durch Nachrechnen bestätigt man, dass Φ ein Ringhomomorphismus ist. Die Eindeutigkeit ist klar. □

Wir erweitern Definition 2.3.1 auf den Fall mehrerer Unbestimmter:

DEFINITION 2.3.2
Es sei R ein kommutativer Ring mit Eins und $n \in \mathbb{N}$. Unter einem Polynomring über R in n unabhängigen Unbestimmten $X_1, \ldots, X_n$ verstehen wir eine Folge der Länge n von Tripeln

$$\tau_k := (R[X_1, \ldots, X_{k-1}][X_k], X_k, i_k) \ , \ 1 \leq k \leq n \ .$$

Dabei soll τ_k ein Polynomring über $R[X_1, \ldots, X_{k-1}]$ in der Unbestimmten X_k im Sinne von Definition 2.3.1 sein.

Durch vollständige Induktion beweist man folgende Verallgemeinerung von Satz 2.3.1:

SATZ 2.3.2
Es gibt (bis auf Isomorphie) genau einen Polynomring über R in n unabhängigen Unbestimmten $X_1, \ldots, X_n$.

DEFINITION 2.3.3
Sei R ein kommutativer Ring mit Eins:

(a) Es sei $R \leq S$ und $x_1, \ldots, x_n \in S$. Unter $R[x_1, \ldots, x_n]$ versteht man den kleinsten Teilring von S, der die Menge $R \cup \{x_1, \ldots, x_n\}$ enthält:

$$R[x_1, \ldots, x_n] = \bigcap_{\substack{T \leq S \\ R \cup \{x_1, \ldots, x_n\} \subseteq T}} T$$

(b) Es sei $(R[X], X, i)$ der Polynomring über R in der Unbestimmten X. Das Element x heißt Unbestimmte über R, falls x Element eines kommutativen Oberrings S von R ist und der nach Satz 2.3.1 existierende Homomorphismus $\Phi: R[X] \to S$ mit $\Phi(X) = x$ ein Monomorphismus ist.

(c) $x_1, \ldots, x_n$ heißen unabhängige Unbestimmte über R, falls $x_1, \ldots, x_n$ Elemente eines kommutativen Oberrings S von R sind, x_1 Unbestimmte über R ist und für alle $2 \leq k \leq n$ gilt: x_k ist Unbestimmte über $R[x_1, \ldots, x_{k-1}]$.

Aus Satz 2.3.1 ergibt sich die Gültigkeit von

SATZ 2.3.3
Es sei S ein kommutativer Oberring von R und $x, x_1, \ldots, x_n \in S$. $(R[X], X, i)$ sei der Polynomring über R in der Unbestimmten X und $((R[X_1, \ldots, X_{k-1}][X_k], X_k, i_k))_{1 \leq k \leq n}$ sei der Polynomring über R in n unabhängigen Unbestimmten $X_1, \ldots, X_n$.

(a) *Folgende Aussagen sind äquivalent:*
  (i) *x ist Unbestimmte über R,*
  (ii) *$R[X] \cong R[x]$,*

(iii) *Aus* $\sum a_i x^i = 0$ *mit* $a_0, \ldots a_n \in R$ *und* $a_j = 0$ *für* $j > m$ *für ein* $m \in \mathbb{N}_0$ *folgt* $a_j = 0$ *für alle* $j \in \mathbb{N}_0$.

(b) *Folgende Aussagen sind äquivalent:*

(i) $x_1, \ldots, x_n$ *sind unabhängige Unbestimmte über* R,

(ii) $R[X_1, \ldots, X_n] \cong R[x_1, \ldots, x_n]$,

(iii) *Aus*

$$\sum_{(i_1 \ldots i_n) \in I} a_{i_1,\ldots,i_n} x_1^{i_1} x_2^{i_2} \cdots x_n^{i_n} \;=\; 0$$

mit $a_{i_1,\ldots,i_n} \in R$ *und* I *eine endliche Menge von* n*-Tupeln, folgt* $a_{j_1,\ldots,j_n} = 0$ *für alle* $j_1, \ldots, j_n \in \mathbb{N}_0$.

Für einen gegebenen kommutativen Ring R mit Eins bedeute künftig $R[X]$ bzw. $R[X_1, \ldots, X_n]$ stets den Polynomring über R in der Unbestimmten X bzw. in den n unabhängigen Unbestimmten $X_1, \ldots, X_n$.

DEFINITION 2.3.4
Es sei R ein Teilring von S. Ein Element $\alpha \in S$ heißt Nullstelle des Polynoms

$$f \;=\; \sum_{i=0}^{n} r_i X^i \;\in\; R[X]\,,$$

wenn

$$f(\alpha) \;=\; \sum_{i=0}^{n} r_i \alpha^i \;=\; 0_S$$

ist.

SATZ 2.3.4
Es sei R *ein Integritätsring. Dann besitzt jedes Polynom* $f \in R[X]$ *mit* $f \neq 0$ *höchstens* $\deg(f)$ *Nullstellen in* R.

BEWEIS
Vollständige Induktion nach $n := \deg(f)$. Ist $n = 0$, so ist $f \in R$ und $f \neq 0$, also ist f das konstante Polynom, welches keine Nullstelle besitzt. Es sei nun $n \geq 1$. Hat f keine Nullstelle, so gilt die Behauptung. Sonst gibt es $\alpha \in R$ mit $f(\alpha) = 0$. Durch „lange Division" erhält man ein $q \in R[X]$ mit $\deg(q) = n - 1$, so dass $f = q \cdot (X - \alpha) + r$ ist mit $r \in R$. Aus $f(\alpha) = 0$ folgt aber $r = 0$. Weil R Integritätsring ist, ist $\beta \in R$ genau dann Nullstelle von f, wenn β Nullstelle von q oder $\beta = \alpha$ ist. Nach Induktionsvoraussetzung hat q aber höchstens $n - 1$ Nullstellen, also hat f höchstens n Nullstellen. □

2.4. Teilbarkeitstheorie

In diesem Abschnitt sei R stets ein Integritätsring.

DEFINITION 2.4.1
Es seien $a, b, a' \in R$. a heißt Teiler von b (oder a teilt b), wenn es $r \in R$ gibt mit $b = r \cdot a$. Schreibweise: $a|b$. Ist a kein Teiler von b, so schreibt man $a \nmid b$. Die Elemente a und a' heißen assoziiert, wenn es eine Einheit $u \in R^*$ gibt mit $a' = ua$. Schreibweise: $a \sim a'$.

Folgende Teilbarkeitsregeln sind unmittelbar klar:

SATZ 2.4.1
Es sei R ein Integritätsring und $a, b, c, a', b_j \in R$, dann gilt:

$$\begin{array}{lccll}
\text{(a)} & a|b & \Leftrightarrow & (b) = bR \subseteq (a) = aR & \\
\text{(b)} & a \sim a' & \Leftrightarrow & (a) = (a') & \\
\text{(c)} & a|b\ ,\ b|c & \Rightarrow & a|c & \\
\text{(d)} & a|b_1, \ldots, a|b_n & \Rightarrow & a \mid \sum_{i=1}^{n} b_i r_i & \forall r_i \in R \\
\text{(e)} & a|1_R & \Leftrightarrow & a \in R^* & \\
\text{(f)} & a|a'\ ,\ a'|a & \Leftrightarrow & a \sim a' &
\end{array}$$

DEFINITION 2.4.2
Sei R ein Integritätsring.

(a) Ein Element $0 \neq a \in R - R^*$ heißt irreduzibel oder unzerlegbar, falls jede Faktorisierung von a in R trivial ist, d. h. falls $a = a_1 a_2$ gilt für $a_1, a_2 \in R$, so ist $a_1 \in R^*$ oder $a_2 \in R^*$.
(b) Ein Element $a \in R - R^*$ heißt prim oder Primelement, falls $a|b_1 b_2$ impliziert, dass $a|b_1$ oder $a|b_2$ gilt für alle $b_1, b_2 \in R$.

BEMERKUNG 2.4.1
Offenbar gilt: a prim $\Leftrightarrow$ $(a) = aR$ ist Primideal.

SATZ 2.4.2
Ist a prim, so ist a auch unzerlegbar.

BEWEIS
Es sei a zerlegbar, d. h. $a = a_1 a_2$ mit $a_1, a_2 \in R - R^*$. Annahme: $a|a_1$. Dann ist $a_1 = f \cdot a = f \cdot a_1 \cdot a_2$ mit $f \in R$. Daraus folgt aber der Widerspruch $f \cdot a_2 = 1$ bzw. $a_2 \in R^*$. Also $a \nmid a_1$. Ebenso folgt $a \nmid a_2$. Damit ist $a|a_1 a_2$ aber $a \nmid a_1$ und $a \nmid a_2$, also ist a nicht prim. □

BEMERKUNG 2.4.2
Die Umkehrung gilt im Allgemeinen nicht.

BEISPIEL 2.4.1
Es sei $R = \mathbb{Z}[\sqrt{-5}]$. Behauptung: 3 ist unzerlegbar. Es sei

$$\begin{array}{rcll}
3 & = & (a + b\sqrt{-5}) \cdot (c + d\sqrt{-5}) & a, b, c, d \in \mathbb{Z} \\
\Rightarrow \quad 3 & = & (a - b\sqrt{-5}) \cdot (c - d\sqrt{-5}) & \\
\Rightarrow \quad 9 & = & (a^2 + 5b^2)(c^2 + 5d^2) & \\
\Rightarrow & & b = 0 \text{ oder } d = 0 & \\
\text{sowie} & & a + b\sqrt{-5} \mid 1 \text{ oder } c + d\sqrt{-5} \mid 1 \quad . &
\end{array}$$

Nun ist aber $3 \cdot 2 = (1 + \sqrt{-5})(1 - \sqrt{-5})$. Damit gilt $3 \mid (1 + \sqrt{-5})(1 - \sqrt{-5})$ aber $3 \nmid 1 + \sqrt{-5}$ und $3 \nmid 1 - \sqrt{-5}$. Also ist 3 in $\mathbb{Z}[\sqrt{-5}]$ unzerlegbar, aber nicht prim.

DEFINITION 2.4.3
R heißt ein Ring mit eindeutiger Faktorisierung oder faktoriell (oder Gaußscher Bereich), falls jede Nichteinheit eine im Wesentlichen eindeutige Faktorisierung in unzerlegbare Elemente besitzt.

Das bedeutet: Falls $a = a_1 \cdots a_n = b_1 \cdots b_m$ Faktorisierungen von a in unzerlegbare Elemente von R sind, so folgt $m = n$, und nach Umnummerierung der b_j ist $a_j \sim b_j$ für $j = 1 \ldots n$.

SATZ 2.4.3
R ist faktoriell, falls

(i) *R keine unendlichen Teilerketten $a_1, a_2, \ldots$ mit $a_{j+1}|a_j$ und $a_j \not\sim a_{j+1}$ für alle $j \in \mathbb{N}$ enthält, und*
(ii) *jedes irreduzible Element in R prim ist.*

Die Umkehrung gilt trivialerweise.

BEWEIS
Es gelte (i): Wir zeigen zunächst, dass für jedes $a \in R - R^*$ eine Zerlegung in irreduzible Elemente existiert. Dazu konstruieren wir eine endliche Folge $b_0, \ldots, b_k$ von Teilern von a, so dass b_k irreduzibel ist. Sei $b_0 := a$ gesetzt. Falls b_0 unzerlegbar ist setzen wir $k = 0$ und sind fertig. Ansonsten existiert ein $b_1 \in R - R^*$ mit $b_1|a$ und $b_1 \not\sim a$. Sind $b_0, \ldots, b_{i-1}$ schon konstruiert, und ist keines davon irreduzibel, so existiert $b_i \in R - R^*$ mit $b_i|b_{i-1}$ und $b_i \not\sim b_{i-1}$. Wegen (i) erhalten wir auf diese Weise in endlich vielen Schritten ein irreduzibles $b_k|a$. Wir konstruieren als nächstes die Folge (a_j). Dazu setzen wir $a_1 = b_k$, und es gilt $a = a_1\tilde{a}_1$. Wir konstruieren in der selben Weise wie oben für $\tilde{a}_1$ ein irreduzibles a_2 mit $a_2|\tilde{a}_1$ und setzen $a = a_1a_2\tilde{a}_2$. Nach n Schritten ist $a = a_1 \cdots a_n \cdot \tilde{a}_n$, wobei alle a_i irreduzibel sind. Falls $\tilde{a}_n$ für alle n zerlegbar wäre, so wäre wieder die Folge $(\tilde{a}_i)$ eine unendliche Teilerkette im Widerspruch zu (i). Damit ist die Existenz der Faktorisierung gezeigt. Zur Eindeutigkeit: Es seien $a_1 \cdots a_n = b_1 \cdots b_m$ und alle $a_i, b_j \in R$ unzerlegbar. Wir führen den Beweis durch Induktion über das Minimum von m und n. a_1 teilt das Produkt $b_1 \cdots b_m$, und da a_1 nach (ii) prim ist, teilt a_1 eines der b_j. Ohne Einschränkung sei $j = 1$. Also gilt: a_1 teilt b_1 und b_1 ist unzerlegbar. Das heißt $a_1 \sim b_1$, und man kann ohne Einschränkung $a_1 = b_1$ annehmen. Es folgt $a_2 \cdots a_n = b_2 \cdots b_m$. Nach Induktionshypothese ist $m = n$ und (nach Umnummerierung) $a_i \sim b_i$. □

DEFINITION 2.4.4
Es sei R ein Integritätsring und $a, b \in R$ mit $a \neq 0$ oder $b \neq 0$. $c \in R$ heißt der größte gemeinsame Teiler von a und b (Schreibweise: $c = \mathrm{ggT}(a, b)$), falls:

(i) $c|a$ und $c|b$,
(ii) $d|a$ und $d|b$ impliziert $d|c$.

$x \in R$ heißt das kleinste gemeinsame Vielfache von a und b (Schreibweise: $x = \mathrm{kgV}(a, b)$), falls:

(i) $a|x$ und $b|x$,
(ii) $a|y$ und $b|y$ impliziert $x|y$.

Ist R faktoriell, so existieren ggT und kgV, und sind bis auf Einheiten eindeutig bestimmt.

DEFINITION 2.4.5
Sei R ein Integritätsring.

(a) R heißt Hauptidealring, falls jedes Ideal von R ein Hauptideal ist.
(b) Ein Euklidischer Ring ist ein Paar (R, δ), bestehend aus einem Integritätsring R und einer Abbildung $\delta : R - \{0_R\} \to \mathbb{N}_0$ mit der Eigenschaft: für alle $a, b \in R - \{0_R\}$ gibt es $q, r \in R$ mit $a = qb + r$ und $\delta(r) < \delta(b)$ oder $r = 0$. Die Abbildung δ heißt Höhenfunktion von R.

BEISPIEL 2.4.2
Folgende Ringe sind Euklidisch:

(1) $(\mathbb{Z}, \delta)$ mit $\delta(a) = |a|$.

(2) Der Polynomring $K[X]$ in einer Unbestimmten für einen Körper K mit $\delta(f) = \deg(f)$. Die Polynome q und r in der vorhergehenden Definition können durch die wohlbekannte „lange Division" gefunden werden.

SATZ 2.4.4
Es gilt:

(a) *Ein Euklidischer Ring ist immer ein Hauptidealring.*
(b) *Ein Hauptidealring ist immer faktoriell.*
(c) *In einem Hauptidealring ist jedes von $\{0\}$ verschiedene Primideal auch maximal.*

BEWEIS
(a): Es sei (R, δ) ein Euklidischer Ring und J ein Ideal von R. Wähle $a \in J - \{0_R\}$, so dass $\delta(a)$ minimal ist. Zu $b \in J$ gibt es $q \in R$, so dass $b = aq + r$ mit $\delta(r) < \delta(a)$ ist oder $r = 0_R$. Da $r \in J$ ist und $\delta(a)$ minimal gewählt war, folgt $r = 0_R$. Also ist $b = aq \in aR$. Da $b \in J$ beliebig war folgt $J = (a) = aR$. Zu (b): Nach Satz 2.4.3 genügt es zu zeigen:

(i) Es existieren keine unendlichen Teilerketten,
(ii) jedes irreduzible Element ist prim.

Zu (i): Angenommen es gäbe $a_1, a_2, \ldots$ mit $a_{i+1} | a_i$ und $a_i \not\sim a_{i+1}$ in R. Dann gilt: $a_1 R \subsetneq a_2 R \subsetneq \cdots$. Wir setzen

$$J := \bigcup_{j=1}^{\infty} a_j R \,,$$

dann ist $J \trianglelefteq R$ ein Ideal. Da R Hauptidealring ist, gibt es $a \in R$ mit $J = aR$. Dann gibt es auch ein i mit $a \in a_i R$, woraus $a_i R = a_{i+1} R = \cdots$ im Widerspruch zur Annahme folgt. Zu (ii): Es sei $a \in R - R^*$ irreduzibel. Es genügt zu zeigen, dass $aR \trianglelefteq R$ prim ist. Wir zeigen die stärkere Eigenschaft, dass aR maximal ist, womit auch (c) folgt. Es sei $aR \subseteq J \subsetneq R$. Es folgt: $J = dR$ für ein $d \in R - R^*$, und damit $a \in dR$, also $a = dd'$ mit $d' \in R$. Das bedeutet $d' \in R^*$, da a irreduzibel ist. Also $a \sim d$ und damit $J = aR$. □

SATZ 2.4.5 (Euklidischer Algorithmus)
Es sei (R, δ) ein Euklidischer Ring und $r_1, r_2 \in R$ mit $r_2 \neq 0_R$. Konstruiere $q_i, r_i \in R$ so dass gilt:

$$\begin{array}{lrcll} (*) & r_1 & = & q_1 r_2 + r_3 & \text{mit} \quad \delta(r_3) < \delta(r_2) \\ & r_2 & = & q_2 r_3 + r_4 & \text{mit} \quad \delta(r_4) < \delta(r_3) \\ & \vdots & & \vdots & \vdots \\ & r_{n-1} & = & q_{n-1} r_n + r_{n+1} & \text{mit} \quad \delta(r_{n+1}) < \delta(r_n) \\ & r_n & = & q_n r_{n+1} + r_{n+2} & \text{mit} \quad r_{n+2} = 0_R \end{array}$$

Das so erhaltene Element r_{n+1} ist der größte gemeinsame Teiler von r_1 und r_2, und indem man $(*)$ rückwärts durchläuft erhält man $a, b \in R$ mit $r_{n+1} = ar_1 + br_2$.

BEWEIS
Aus der letzten Gleichung von $(*)$ erhält man $r_{n+1} | r_n$, aus der Vorletzten $r_{n+1} | r_{n-1}$, usw.. Schließlich folgt aus der zweiten Gleichung $r_{n+1} | r_2$ und aus der Ersten $r_{n+1} | r_1$. Das heißt, dass r_{n+1} ein gemeinsamer Teiler von r_1 und r_2 ist. Es sei nun t ein beliebiger Teiler von r_1 und r_2. Dann folgt aus der ersten Gleichung $t | r_3$, usw. bis aus der letzten Gleichung $t | r_{n+1}$ folgt. Also ist r_{n+1} der größte gemeinsame Teiler. Zur Konstruktion von a und b: Aus der vorletzten Gleichung ergibt sich r_{n+1} als Linearkombination von r_{n-1} und r_n mit Koeffizienten aus R: $r_{n+1} = r_{n-1} - q_{n-1} r_n$. Ersetzt man mit Hilfe der vorigen Gleichung r_n, so erhält man

r_{n+1} als Linearkombination von r_{n-2} und r_{n-1}. So fortfahrend erhält man schließlich r_{n+1} als Linearkombination von r_1 und r_2 mit Koeffizienten a und b aus R. □

DEFINITION 2.4.6
R sei faktoriell. Das Polynom $f = a_0 + a_1X^1 + \cdots + a_{n-1}X^{n-1} + a_nX^n \in R[X]$ heißt primitiv, falls der größte gemeinsame Teiler von $a_0, \ldots, a_n$ gleich 1_R ist.

SATZ 2.4.6 (Gauß)
Das Produkt zweier primitiver Polynome ist wieder primitiv (in $R[X]$, wobei R ein faktorieller Ring ist).

BEWEIS
Es seien $f = a_0 + a_1X^1 + \cdots + a_nX^n$ und $g = b_0 + b_1X^1 + \cdots + b_mX^m$ mit $\mathrm{ggT}(a_0, \ldots, a_n) = 1$ und $\mathrm{ggT}(b_0, \ldots, b_m) = 1$, und $fg = c_0 + c_1X^1 + \cdots + c_{n+m}X^{n+m}$ das Produkt. Angenommen, fg sei nicht primitiv. Dann gibt es ein Primelement $p \in R$, das die c_i für $i = 0 \ldots n+m$ teilt. Definiere a_l :=letztes a_i mit $p \nmid a_i$ und b_k :=letztes b_j mit $p \nmid b_j$. Dann gilt:

$$c_{l+k} = \underbrace{a_0b_{l+k} + a_1b_{l+k-1} + \cdots}_{\uparrow\ p|b_j} + a_lb_k + \underbrace{a_{l+1}b_{k-1} + \cdots + a_{l+k}b_0}_{\uparrow\ p|a_i}$$

Da p ein Teiler von c_{l+k} ist, muss p auch a_lb_k teilen, also gilt $p|a_l$ oder $p|b_k$. Das ist aber ein Widerspruch zur Wahl von l und k. □

LEMMA 2.4.7
R sei faktoriell und K sei der Quotientenkörper von R. Ist $f \in R[X]$ irreduzibel, so ist f auch irreduzibel in $K[X]$.

BEWEIS
f ist irreduzibel in $R[X]$, also ist f primitiv. Angenommen, f zerfiele in $f = f_1f_2$ in $K[X]$ (also $f_1, f_2 \in K[X]$), so existierte ein $a \in R - \{0_R\}$ mit $af = \tilde{f}_1\tilde{f}_2$ mit $\tilde{f}_1, \tilde{f}_2 \in R[X]$ ($\tilde{f}_i$ ist also ein R-Vielfaches von f_i). Ohne Einschränkung seien die $\tilde{f}_i$ primitiv. Mit dem Gaußschen Lemma (Satz 2.4.6) folgt, dass auch $\tilde{f}_1\tilde{f}_2 \in R[X]$ primitiv ist. Damit folgt, dass a eine Einheit in R ist, und so $f = (a^{-1}\tilde{f}_1)\tilde{f}_2$ reduzibel in $R[X]$ ist. □

SATZ 2.4.8
Ist R faktoriell, so ist auch $R[X]$ faktoriell.

BEWEIS
Wir wenden Satz 2.4.3 an. (i): Es existieren keine unendlichen Teilerketten, da die Grade der Polynome beim Teilen bis auf Null verkleinert werden und auch in R keine unendlichen Teilerketten existieren, weil R faktoriell ist. (ii): Sei $q \in R[X]$ unzerlegbar. Es sei K der Quotientenkörper von R. Dann ist nach dem vorigen Lemma q auch in $K[X]$ unzerlegbar und prim, da $K[X]$ ein Hauptidealring ist. Also, falls $q|ab$ mit $a, b \in R[X]$ gilt, folgt: $q|a$ oder $q|b$ in $K[X]$. Da q primitiv ist, folgt $q|a$ in $R[X]$ oder $q|b$ in $R[X]$. □

SATZ 2.4.9 (Eisensteinkriterium)
R sei faktoriell mit Quotientenkörper K und $f = a_0 + a_1X^1 + \cdots + a_nX^n \in R[X]$ mit $a_n \neq 0$ für $n > 1$. Es sei weiter $p \in R$ prim, so dass $p \nmid a_n$ und $p|a_i$ für $i = n-1 \ldots 0$ und $p^2 \nmid a_0$. Dann ist f irreduzibel in $K[X]$.

BEWEIS
Ohne Einschränkung sei f primitiv. Angenommen, f sei nicht irreduzibel, ließe sich also darstellen als $f = gh$ mit $g = b_0 + \cdots + b_d X^d \in R[X]$ und $h = c_0 + \cdots + c_m X^m \in R[X]$ (mit $b_d, c_m \neq 0$). Nun gilt $p | a_0 = b_0 c_0$ aber $p^2 \nmid b_0 c_0$. Daraus folgt ohne Einschränkung $p | c_0$ aber $p \nmid b_0$. Da p nicht $c_m b_d = a_n$ teilt, teilt p auch nicht c_m. Wähle nun r minimal mit p teilt nicht c_r. Dann ist $r > 0$ und $a_r = b_0 c_r + b_1 c_{r-1} + \cdots$. Da p weder b_0 noch c_r teilt, teilt es auch nicht das Produkt $b_0 c_r$. Andererseits gilt $p | c_{r-i}$ für $i = 1 \ldots r$, da $p | c_i$ für $i < r$. Das ist aber ein Widerspruch zu $p | a_r$. □

2.5. Der Chinesische Restesatz

DEFINITION 2.5.1
Es seien $(R_1, +_1, \cdot_1), \ldots, (R_n, +_n, \cdot_n)$ Ringe. Unter dem direkten Produkt der Ringe $R_1, \ldots, R_n$ (Schreibweise $R_1 \times R_2 \times \cdots \times R_n$ oder auch $\prod_{i=1}^{n} R_j$) versteht man den Ring, dessen Elemente die Elemente des kartesischen Produkts $R_1 \times \cdots \times R_n$ von Mengen sind, und für den Addition und Multiplikation komponentenweise definiert sind:

$$\begin{array}{rcl} (r_1, \ldots, r_n) & + & (s_1, \ldots, s_n) := (r_1 +_1 s_1, \ldots, r_n +_n s_n) \\ (r_1, \ldots, r_n) & \cdot & (s_1, \ldots, s_n) := (r_1 \cdot_1 s_1, \ldots, r_n \cdot_n s_n) \end{array} .$$

Das Einselement von $\prod R_j$ ist offenbar $(1_{R_1}, \ldots, 1_{R_n})$.

DEFINITION 2.5.2
Es sei R ein Ring und $\mathfrak{a}, \mathfrak{b} \trianglelefteq R$ Ideale.

(a) Unter der Summe von $\mathfrak{a}$ und $\mathfrak{b}$ versteht man

$$\mathfrak{a} + \mathfrak{b} := \{a + b \mid a \in \mathfrak{a}\ ,\ b \in \mathfrak{b}\} .$$

(b) Unter dem Durchschnitt von $\mathfrak{a}$ und $\mathfrak{b}$ versteht man

$$\mathfrak{a} \cap \mathfrak{b} := \{x \mid x \in \mathfrak{a}\ ,\ x \in \mathfrak{b}\} .$$

(c) Unter dem Produkt von $\mathfrak{a}$ und $\mathfrak{b}$ versteht man

$$\mathfrak{a} \cdot \mathfrak{b} := \left\{ \sum a_i b_i \mid a_i \in \mathfrak{a}\ ,\ b_i \in \mathfrak{b} \right\} .$$

Offenbar sind die in (a), (b) und (c) definierten Objekte ebenfalls Ideale, und es gilt $\mathfrak{a} \cdot \mathfrak{b} \subseteq \mathfrak{a} \cap \mathfrak{b}$. Summen, Durchschnitte und Produkte können rekursiv auch für mehr als zwei Ideale definiert werden.

DEFINITION 2.5.3
Es sei R ein Ring. Ideale $\mathfrak{a}, \mathfrak{b} \trianglelefteq R$ heißen komaximal, falls $\mathfrak{a} + \mathfrak{b} = R$ gilt.

SATZ 2.5.1 (Chinesischer Restsatz)
Es sei R ein kommutativer Ring (mit Eins). Es seien $\mathfrak{a}_1, \ldots, \mathfrak{a}_n \trianglelefteq R$ paarweise komaximale Ideale von R, d. h. $\mathfrak{a}_i + \mathfrak{a}_j = R$ für alle $i \neq j$. Dann gilt:

(a) $\mathfrak{a}_1 \cap \cdots \cap \mathfrak{a}_n = \mathfrak{a}_1 \cdot \cdots \cdot \mathfrak{a}_n$.

(b) *Es gibt eine Menge* $\{e_1, \ldots, e_n\} \subseteq R$ *mit*

$$(*)\ e_j \in \mathfrak{a}_i \text{ falls } i \neq j \text{ und } e_j \equiv 1_R \bmod \mathfrak{a}_j$$

Für $(r_1, \ldots, r_n) \in R^n$ *ist das System der Kongruenzen*

$$(1)\ r \equiv r_1 \bmod \mathfrak{a}_1\ ,\ r \equiv r_2 \bmod \mathfrak{a}_2\ ,\ \cdots\ ,\ r \equiv r_n \bmod \mathfrak{a}_n$$

äquivalent zu der einzigen Kongruenz

$$(2)\ r \equiv r_1 e_1 + \cdots + r_n e_n \bmod \prod_{i=1}^{n} \mathfrak{a}_i\ .$$

(c) *Die Abbildung*

$$\Phi = \begin{cases} R / \prod_{i=1}^n \mathfrak{a}_i & \to \quad \prod_{i=1}^n (R / \mathfrak{a}_i) \\ r + \prod_{i=1}^n \mathfrak{a}_i & \mapsto \quad (r + \mathfrak{a}_1, \ldots, r + \mathfrak{a}_n) \end{cases}$$

ist ein Isomorphismus von Ringen, insbesondere ist

$$R \Big/ \prod_{i=1}^{n} \mathfrak{a}_i \ \cong\ R / \mathfrak{a}_1 \ \times \cdots \times\ R / \mathfrak{a}_n\ .$$

BEWEIS
(a): Die Inklusion $\mathfrak{a}_1 \cdots \mathfrak{a}_n \subseteq \mathfrak{a}_1 \cap \cdots \cap \mathfrak{a}_n$ ist klar. Wir zeigen die Umkehrung durch Induktion nach n. Im Fall $n = 2$ gibt es eine Relation $1_R = a_1 + a_2$ mit $a_i \in \mathfrak{a}_i$. Dann gilt für $a \in \mathfrak{a}_1 \cap \mathfrak{a}_2$ aber auch $a = a \cdot 1_R = a \cdot a_1 + a \cdot a_2 \in \mathfrak{a}_1 \cdot \mathfrak{a}_2$. Im Fall $n \geq 2$ hat man nach Induktionsvoraussetzung: $(\mathfrak{a}_1 \cdots \mathfrak{a}_{n-1})\mathfrak{a}_n = (\mathfrak{a}_1 \cdots \mathfrak{a}_{n-1}) \cap \mathfrak{a}_n = \mathfrak{a}_1 \cap \cdots \cap \mathfrak{a}_n$ wenn $R = \mathfrak{a}_1 \cdots \mathfrak{a}_{n-1} + \mathfrak{a}_n$ gilt. Nun hat man stets Relationen $1_R = a_i + b_i$ mit $a_i \in \mathfrak{a}_i$ und $b_i \in \mathfrak{a}_n$ für $i = 1 \ldots (n-1)$. Dann folgt durch Ausmultiplizieren

$$1_R \ =\ \prod_{i=1}^{n-1}(a_i + b_i) \ =\ \prod_{i=1}^{n-1} a_i + \sum_{i=1}^{n-1} b_i c_i \ \in\ \mathfrak{a}_1 \cdots \mathfrak{a}_{n-1} + \mathfrak{a}_n\ .$$

(b): Nach Voraussetzung gibt es für alle i, j mit $i \neq j$ Elemente $a_{ij} \in \mathfrak{a}_i$ und $b_{ij} \in \mathfrak{b}_j$ mit $1_R = a_{ij} + b_{ij}$. Wir setzen

$$e_j \ :=\ \prod_{\substack{i=1 \\ i \neq j}}^{n} a_{ij} \ \in \mathfrak{a}_i \ \ \forall i \text{ mit } i \neq j\ .$$

Es gilt

$$e_j \ =\ \prod_{i=1}^{n}(1 - b_{ij}) \ \equiv\ 1_R \bmod \mathfrak{a}_j\ .$$

Aus (*) folgt mit (a) sofort die Äquivalenz der Kongruenzsysteme (1) und (2). (c): Für $(r_1, \ldots, r_n) \in R^n$ sei r durch (2) gegeben. Dann ist $(r + \mathfrak{a}_1, \ldots, r + \mathfrak{a}_n) = (r_1 + \mathfrak{a}_1, \ldots, r_n + \mathfrak{a}_n)$ und r ist eindeutig bestimmt modulo $\prod_{i=1}^n \mathfrak{a}_i$. Damit ist die Bijektivität von Φ gezeigt. □

Wir wenden uns nun dem Spezialfall $R = \mathbb{Z}$ zu.

DEFINITION 2.5.4
$a, b \in \mathbb{Z}$ heißen teilerfremd, falls $\mathrm{ggT}(a, b) = 1$ ist.

Da $\mathbb{Z}$ ein Hauptidealring ist, ist jedes Ideal $\mathfrak{a}_i \neq \{0\}$ von der Form $\mathfrak{a}_i = (m_i) = m_i\mathbb{Z}$ für $m_i \in \mathbb{N}$. Nach Satz 2.4.5 sind $\mathfrak{a}_i$ und $\mathfrak{a}_j$ komaximal genau dann, wenn m_i und m_j teilerfremd sind. Für $R = \mathbb{Z}$ lautet also der Chinesische Restsatz folgendermaßen:

SATZ 2.5.2
Es seien $m_1, \ldots, m_n$ paarweise teilerfremde natürliche Zahlen und $M = m_1 \cdots m_n$. Dann gibt es für $1 \leq j \leq n$ Zahlen $l_j \in \mathbb{Z}$ mit

$$\begin{array}{rcll} l_j & \equiv & 0 & \mod m_i \qquad (\forall i \neq j) \\ l_j & \equiv & 1 & \mod m_j \quad . \end{array}$$

Für ein beliebiges n-Tupel $(r_1, \ldots, r_n) \in \mathbb{Z}^n$ ist das System der Kongruenzen

$$(1) \quad r \equiv r_1 \bmod m_1 \ , \ \cdots \ , \ r \equiv r_n \bmod m_n$$

äquivalent zu der einzigen Kongruenz

$$(2) \quad r \equiv r_1 l_1 + \cdots + r_n l_n \mod M \ .$$

Die Abbildung

$$\Phi \ = \ \begin{cases} \mathbb{Z} \,/\, M\mathbb{Z} & \to \quad \prod_{i=1}^{n} (\mathbb{Z} \,/\, m_i\mathbb{Z}) \\ r + M\mathbb{Z} & \mapsto \quad (r + m_1\mathbb{Z}, \ldots, r + m_n\mathbb{Z}) \end{cases}$$

ist ein Isomorphismus von Ringen, insbesondere ist

$$\mathbb{Z} \,/\, M\mathbb{Z} \ \cong \ \mathbb{Z} \,/\, m_1\mathbb{Z} \ \times \ \cdots \ \times \ \mathbb{Z} \,/\, m_n\mathbb{Z} \ .$$

BEISPIEL 2.5.1
Sei $M = m_1 \cdot m_2$ mit $m_1 = 5$ und $m_2 = 3$. Nach Satz 2.5.2 ist

$$\mathbb{Z} \,/\, 15\mathbb{Z} \ \cong \ (\mathbb{Z} \,/\, 5\mathbb{Z}) \ \times \ (\mathbb{Z} \,/\, 3\mathbb{Z}) \ .$$

Die Tafel, die Φ beschreibt, erhält man, indem für alle Restklassen $r + 15\mathbb{Z}$ das zugehörige Paar $(r_1 + 5\mathbb{Z}, r_2 + 3\mathbb{Z})$ berechnet wird. Beispielsweise $r = 7$:

$$\begin{array}{rcll} r & \equiv & 2 & \mod 5 \\ r & \equiv & 1 & \mod 3 \quad , \end{array}$$

also $\Phi(7 + 15\mathbb{Z}) = (2 + 5\mathbb{Z}, 1 + 3\mathbb{Z})$.

	0	1	2	3	4	mod5
0	0	6	12	3	9	
1	10	1	7	13	4	
2	5	11	2	8	14	
mod3					↖	
						mod15

Die Idee des Chinesischen Restsatzes liegt der so genannten „modularen Arithmetik" zugrunde, die Anwendung in der Informatik gefunden hat: Zunächst wird jede Restklasse $r + M\mathbb{Z}$ durch ihr Bild $\Phi(r + M\mathbb{Z}) = (r_1 + m_1\mathbb{Z}, \ldots, r_n + m_n\mathbb{Z})$ ersetzt. Danach werden die Rechenschritte komponentenweise ausgeführt.

BEISPIEL 2.5.2
Berechne $(7 + 15\mathbb{Z}) \cdot (8 + 15\mathbb{Z})$: Es ist

$$\begin{array}{rcl} \Phi(7 + 15\mathbb{Z}) & = & (2 + 5\mathbb{Z}, 1 + 3\mathbb{Z}) \\ \Phi(8 + 15\mathbb{Z}) & = & (3 + 5\mathbb{Z}, 2 + 3\mathbb{Z}) \quad . \end{array}$$

Komponentenweise Rechnung ergibt $(2 + 5\mathbb{Z}, 1 + 3\mathbb{Z}) \cdot (3 + 5\mathbb{Z}, 2 + 3\mathbb{Z}) = (1 + 5\mathbb{Z}, 2 + 3\mathbb{Z}) = \Phi(11 + 15\mathbb{Z})$. Also ist $(7 + 15\mathbb{Z}) \cdot (8 + 15\mathbb{Z}) = (11 + 15\mathbb{Z})$.

Zur algorithmischen Bestimmung der Zahlen l_j kann der Euklidische Algorithmus verwendet werden.

BEISPIEL 2.5.3
Man finde die Lösungsmenge des Systems

$$\begin{aligned} r &\equiv 2 \mod 15 \\ r &\equiv 3 \mod 23 \\ r &\equiv 5 \mod 37 \end{aligned}$$

Lösung: Es sei $m_1 = 15$, $m_2 = 23$ und $m_3 = 37$. Dann ist $M = 12765 = m_1 m_2 m_3$. Nach Satz 2.5.2 besteht die Lösungsmenge aus einer Restklasse modulo M. Wir bestimmen die Konstanten l_j: Dazu sei

$$M_j := \prod_{\substack{i=1 \\ i \neq j}}^{n} m_i \quad (1 \leq i \leq 3)$$

gesetzt. Aus $l_j \equiv 0 \bmod m_i$ für alle $i \neq j$ und $l_j \equiv 1 \bmod m_j$ folgt $l_j = M_j x_j$ für $x_j \in \mathbb{Z}$. Es sind also x_j zu bestimmen, so dass $M_j x_j \equiv 1 \bmod m_j$ gilt.

Fall j=1:

$$\begin{aligned} 23 \cdot 37 x_1 &\equiv 1 \mod 15 \\ -4 x_1 &\equiv 1 \mod 15 \end{aligned}$$

Zur Lösung der letzten Kongruenz genügt es, die Gleichung $-4x_1 + 15y_1 = 1$ mittels des Euklidischen Algorithmus (oder durch Erraten, was bei kleinen Koeffizienten einfach ist) zu lösen. Man findet

$$\begin{aligned} 15 &= 3 \cdot 4 + 3 \\ 4 &= 3 + 1 \end{aligned}$$

Also $1 = 4 - 3 = 4 - (15 - 3 \cdot 4) = 4 \cdot 4 - 15$ und $x_1 = -4$ bzw. $l_1 = -4 \cdot 23 \cdot 37$.

Fall j=2:

$$\begin{aligned} 15 \cdot 37 x_2 &\equiv 1 \mod 23 \\ 3 x_2 &\equiv 1 \mod 23 \end{aligned}$$

$\Rightarrow x_2 = 8$ bzw. $l_2 = 8 \cdot 15 \cdot 37$.

Fall j=3:

$$15 \cdot 23 x_3 \equiv 1 \mod 37$$

$$\begin{aligned} 15 \cdot 23 = 345 &= 10 \cdot 37 - 25 \\ 37 &= 25 + 12 \\ 25 &= 2 \cdot 12 + 1 \end{aligned}$$

$\Rightarrow 1 = 25 - 2 \cdot 12 = 25 - 2 \cdot (37 - 25) = 3 \cdot 25 - 2 \cdot 37 = 3 \cdot (10 \cdot 37 - 345) - 2 \cdot 37 = -3 \cdot 345 + 28 \cdot 37$

$\Rightarrow x_3 = -3$ bzw. $l_3 = -3 \cdot 15 \cdot 23$. Nach Satz 2.5.2 ist das System der Kongruenzen äquivalent zu der einzigen Kongruenz

$$r \equiv 2l_1 + 3l_2 + 5l_3 = 1337 \mod 12765\,.$$

Wir betrachten nun die Einheitengruppe eines direkten Produkts von Ringen. Man sieht unmittelbar die Gültigkeit von

SATZ 2.5.3
Es sei $R = R_1 \times \cdots \times R_n$. Dann ist die Einheitengruppe gegeben durch das direkte Produkt

$$R^* \;=\; R_1^* \times \cdots \times R_n^*$$

von Gruppen.

SATZ 2.5.4
Es sei $m \in \mathbb{N}$ und $a \in \mathbb{Z}$. Es gilt:

$$a + m\mathbb{Z} \;\in\; (\mathbb{Z}\,/\,m\mathbb{Z})^* \;\Leftrightarrow\; \mathrm{ggT}(a,m) \;=\; 1\,.$$

BEWEIS
$a + m\mathbb{Z} \in (\mathbb{Z}/m\mathbb{Z})^* \;\Leftrightarrow\; \exists x \in \mathbb{Z} :\; ax + m\mathbb{Z} = 1 + m\mathbb{Z} \;\Leftrightarrow\; \exists x, y \in \mathbb{Z} :\; ax + my = 1$. Nach Satz 2.4.5 ist dies äquivalent zu $\mathrm{ggT}(a,m) = 1$. □

DEFINITION 2.5.5
Es sei $m \in \mathbb{N}$. Die Restklasse $a + m\mathbb{Z} \in (\mathbb{Z}/m\mathbb{Z})$ heißt teilerfremde Restklasse modulo m genau dann, wenn $a + m\mathbb{Z} \in (\mathbb{Z}/m\mathbb{Z})^*$ ist.

DEFINITION 2.5.6
Die Eulersche φ-Funktion ist die Funktion

$$\varphi \;=\; \begin{cases} \mathbb{N} & \to & \mathbb{N} \\ m & \mapsto & |(\mathbb{Z}\,/\,m\mathbb{Z})^*| \end{cases}\,.$$

BEMERKUNG 2.5.1
Man sieht sofort, dass äquivalente Beschreibungen für φ sind:

(a) $\varphi(m)$ ist die Anzahl der zu m teilerfremden Restklassen.
(b) $\varphi(m) = |\{1 \le a \le m \mid \mathrm{ggT}(a,m) = 1\}|$.

BEISPIEL 2.5.4
Von den Zahlen $\{a \mid 1 \le a \le 10\}$ sind $a = 1, 3, 7, 9$ teilerfremd zu 10, also $\varphi(10) = 4$.

Wir wollen eine Formel herleiten, die es erlaubt, die Eulersche φ-Funktion schnell zu berechnen.

SATZ 2.5.5
Es sei $m = m_1 \cdots m_r$ mit paarweise teilerfremden $m_i \in \mathbb{N}$. Dann gilt

$$(\mathbb{Z}\,/\,m\mathbb{Z})^* \;\cong\; (\mathbb{Z}\,/\,m_1\mathbb{Z})^* \;\times\; \cdots \;\times\; (\mathbb{Z}\,/\,m_r\mathbb{Z})^*$$

und $\varphi(m) = \varphi(m_1) \cdots \varphi(m_r)$.

BEWEIS
Das folgt aus den Sätzen 2.5.2 und 2.5.4. □

SATZ 2.5.6
Für $m \in \mathbb{N}$ gilt

$$\varphi(m) \;=\; m \cdot \prod_{p \mid m} \left(1 - \frac{1}{p}\right)\,,$$

wobei sich das Produkt über alle Primzahlen erstreckt, die m teilen. Ist insbesondere $m = p^\alpha$ mit $\alpha \in \mathbb{N}$ und einer Primzahl p, so ist $\varphi(m) = p^\alpha - p^{\alpha-1} = p^\alpha(1 - \frac{1}{p})$.

BEWEIS
Von den Repräsentanten $1, \ldots, p^\alpha$ von $\mathbb{Z}/p^\alpha\mathbb{Z}$ sind genau die Vielfachen von p, also $p, 2p, 3p, \ldots, p^\alpha$ nicht teilerfremd zu p. Also gilt

$$(*): \ \varphi(p^\alpha) \ = \ p^\alpha - p^{\alpha-1} \ = \ p^\alpha \left(1 - \frac{1}{p}\right) .$$

Hat $m \in \mathbb{N}$ die Primfaktorzerlegung $m = p_1^{\alpha_1} \cdots p_r^{\alpha_r}$ mit $\alpha_j > 0$, so folgt mit Satz 2.5.5 und $(*)$ die Formel

$$\varphi(m) \ = \ \varphi(p_1^{\alpha_1}) \cdots \varphi(p_r^{\alpha_r}) \ = \ \prod_{i=1}^{r} p_i^{\alpha_i} \left(1 - \frac{1}{p_i}\right) \ = \ m \cdot \prod_{p|m} \left(1 - \frac{1}{p}\right) .$$

□

BEISPIEL 2.5.5
Bestimme $\varphi(360)$. Es ist $360 = 2^3 \cdot 3^2 \cdot 5$. Also $\varphi(360) = 360 \cdot (1 - \frac{1}{2})(1 - \frac{1}{3})(1 - \frac{1}{5}) = 96$.

Die folgenden zahlentheoretischen Aussagen - Folgerungen aus allgemeinen gruppentheoretischen Aussagen - waren schon lange vor der Entwicklung der Gruppentheorie bekannt:

SATZ 2.5.7
Es gilt:

(a) *(Euler 18. Jahrhundert) Es sei $a \in \mathbb{Z}$ und $n \in \mathbb{N}$ mit $\mathrm{ggT}(a, n) = 1$. Dann ist $a^{\varphi(n)} \equiv 1 \bmod n$.*
(b) *(„Kleiner Satz" von Fermat 17. Jahrhundert) Es sei p eine Primzahl und $a \in \mathbb{Z}$ mit $p \nmid a$. Dann ist $a^{p-1} \equiv 1 \bmod p$.*

BEWEIS
Wegen $\varphi(p) = p - 1$ für Primzahlen p ist (b) ein Spezialfall von (a). (a) ist andererseits der Spezialfall $G = (\mathbb{Z}/n\mathbb{Z})^*$ von Satz 1.7.3(c). □

Die Eulersche φ-Funktion ist auch in der Theorie der endlichen zyklischen Gruppen von Bedeutung.

SATZ 2.5.8
Es sei G eine endliche zyklische Gruppe, $G = \langle g \rangle$ und $|G| = |\langle g \rangle| = n$. Es sei $h = g^r$ mit $0 \leq r \leq n - 1$, dann gilt:

(a) *$G = \langle h \rangle = \langle g^r \rangle$ genau dann, wenn $\mathrm{ggT}(r, n) = 1$ ist. Die Anzahl der Erzeugenden von G ist $\varphi(n)$.*
(b) *Es gilt die Gleichung*

$$\sum_{d|n} \varphi(d) \ = \ n .$$

BEWEIS
(a): Es sei $l = \mathrm{ggT}(r, n)$ und $n = l \cdot m$, $r = l \cdot q$ mit $\mathrm{ggT}(q, m) = 1$. Nach Satz 1.7.3(b) ist $h^t = 1_G \ \Leftrightarrow \ g^{lqt} = 1_G \ \Leftrightarrow \ n | lqt \ \Leftrightarrow \ m | t$. Es folgt $|\langle h \rangle| = m$. Also $\langle h \rangle = G \ \Leftrightarrow \ m = n \ \Leftrightarrow \ l = 1$.
(b): Für $d|n$ sei $B_d = \{x \in G \mid |\langle x \rangle| = d\}$ und $F(d) = |B_d|$. Da

$$G \ = \ \dot{\bigcup}_{d|n} B_d$$

eine Partition von G darstellt, folgt die Gleichung

$$(*): \sum_{d|n} F(d) \;=\; |G| \;=\; n\,.$$

Es sei $U_d = \{x \in G \mid x^d = 1_G\}$. Nach Satz 1.7.4 ist U_d zyklisch und $|U_d| = d$. Andererseits ist $B_d \subseteq U_d$. Nach (a) ist $F(d) = |B_d| = \varphi(d)$, womit aus $(*)$ die Behauptung folgt. □

SATZ 2.5.9
Es sei G eine endliche abelsche Gruppe. G ist zyklisch genau dann, wenn für alle $d \in \mathbb{N}$ die Gleichung

$$(*)\;\; x^d \;=\; 1_G$$

höchstens d Lösungen $x \in G$ besitzt.

BEWEIS
Hinrichtung: Es sei $G = \langle g\rangle$ mit $|\langle g\rangle| = n$. Wegen $x^n = 1_G$ für alle $x \in G$ folgt aus $x^d = 1_G$ stets $d|n$. Es sei $n = l \cdot d$. Nach Satz 1.7.4 ist $\{x \in G \mid x^d = 1_G\} = \langle g^l\rangle$ mit Ordnung $|\langle g^l\rangle| = d$. Die Gleichung $(*)$ hat also genau d Lösungen. Rückrichtung: Wie im Beweis des vorigen Satzes sei $F(d) = |\{x \in G \mid |\langle x\rangle| = d\}$. Es gilt

$$(1)\;\; \sum_{d|n} F(d) \;=\; n\,.$$

Es ist zu zeigen, dass $F(n) > 0$ ist. Wir zeigen zunächst, dass

$$(2)\;\; F(d) \;\leq\; \varphi(d)$$

für jedes $d|n$ gilt. Fall a): $F(d) = 0$. Dann ist (2) natürlich erfüllt. Fall b): $F(d) > 0$. Dann gibt es ein $g \in G$ mit $|\langle g\rangle| = d$. Wegen $(*)$ ist $\{x \in G \mid x^d = 1_G\} = \langle g\rangle$. Es gilt $|\langle x\rangle| = d \;\Rightarrow\; x \in \langle g\rangle$. Nach Satz 2.5.8 ist $F(d) = \varphi(d)$. Gäbe es ein $d|n$ mit $F(d) < \varphi(d)$, so folgte aus (2) und Satz 2.5.8(b) der Widerspruch

$$|G| \;=\; \sum_{d|n} F(d) \;<\; \sum_{d|n} \varphi(d) \;=\; |G|\,.$$

□

Aus Satz 2.5.9 ergibt sich als Folgerung eine Aussage über die Struktur der Einheitengruppe von endlichen Integritätsringen.

BEMERKUNG 2.5.2
Man kann zeigen, dass ein endlicher Integritätsring stets ein Körper ist.

SATZ 2.5.10
Es sei R ein endlicher Integritätsring. Dann ist die Einheitengruppe R^* zyklisch. Ist insbesondere $(K, +, \cdot)$ ein endlicher Körper, so ist $K^* = K - \{0_K\}$ zyklisch. Insbesondere ist für eine Primzahl p die Gruppe $(\mathbb{Z}/p\mathbb{Z})^*$ zyklisch.

BEWEIS
Nach Satz 2.3.3 hat für jedes $d \in \mathbb{N}$ das Polynom $f = X^d - 1_R$ höchstens d Nullstellen in R. Nach Satz 2.5.9 ist R^* zyklisch. □

DEFINITION 2.5.7
Es sei $n \in \mathbb{N}$. Ein $r \in \mathbb{Z}$ mit $\mathrm{ggT}(r, n) = 1$ heißt Primitivwurzel modulo n, falls $\langle r \bmod n\rangle = (\mathbb{Z}/n\mathbb{Z})^*$ ist.

Beispiel 2.5.6
Es sei $n = 7$. Es ist $3^1 \equiv 3 \bmod 7$, $3^2 \equiv 2 \bmod 7$, $3^3 \equiv 6 \bmod 7$, $3^4 \equiv 4 \bmod 7$, $3^5 \equiv 5 \bmod 7$ und $3^6 \equiv 1 \bmod 7$. Also ist $\langle 3 \bmod 7 \rangle = (\mathbb{Z}/7\mathbb{Z})^*$, und 3 ist Primitivwurzel modulo 7.

Nach Satz 2.5.10 gibt es zu jeder Primzahl p eine Primitivwurzel modulo p. Wir geben ohne Beweis den folgenden Satz an:

Satz 2.5.11
Es sei $n \in \mathbb{N}$. Dann ist $(\mathbb{Z}/n\mathbb{Z})^*$ zyklisch (d. h. es gibt eine Primitivwurzel modulo n) genau dann, wenn $n = 1, 2, 4$ ist, $n = p^\alpha$ oder $n = 2p^\alpha$ für eine ungerade Primzahl p und ein $\alpha \in \mathbb{N}$. Für $k \geq 3$ ist $(\mathbb{Z}/2^k\mathbb{Z})^*$ das innere direkte Produkt der zyklischen Untergruppen $\langle 5 \bmod 2^k \rangle$ und $\langle (-1) \bmod 2^k \rangle$.

3. Körpertheorie

3.1. Charakteristik und Primkörper

DEFINITION 3.1.1
Es sei L ein Körper.

(a) Unter einem Unterkörper K von L versteht man einen Teilring von L, der ein Körper ist.
(b) Es sei K ein Körper. Unter einer Körpererweiterung von K versteht man ein Paar (L, K), wobei L ein Körper ist, der K als Unterkörper hat (Schreibweise: L/K). Dann heißt L Oberkörper von K.

BEISPIEL 3.1.1
$\mathbb{R}/\mathbb{Q}$, $\mathbb{C}/\mathbb{Q}$ und $\mathbb{C}/\mathbb{R}$ sind Körpererweiterungen.

DEFINITION 3.1.2
Es seien K_1, K_2 Körper. Ein $\Phi : K_1 \to K_2$ heißt (Körper-)isomorphismus, falls es ein Ringisomorphismus ist. In diesem Fall heißen K_1 und K_2 isomorph ($K_1 \cong K_2$).

SATZ 3.1.1
Es sei K ein Körper. Es gibt genau einen Ringhomomorphismus $\Phi : \mathbb{Z} \to K$ mit $\Phi(1) = 1_K$. Es gibt $p \in \mathbb{Z}$ mit $\mathrm{Ker}(\Phi) = p\mathbb{Z}$. Man unterscheidet zwei Fälle:

(1) *Ist $p > 0$, so ist p eine Primzahl. Dann ist $\Phi(\mathbb{Z})$ der kleinste Unterkörper von K. Er ist isomorph zum Körper $\mathbb{F}_p := \mathbb{Z}/p\mathbb{Z}$.*
(2) *Ist $p = 0$, so ist Φ injektiv. Dann gibt es genau einen Ringhomomorphismus $\psi : \mathbb{Q} \to K$ mit $\psi|_{\mathbb{Z}} = \Phi$. Dann ist $\psi(\mathbb{Q})$ der kleinste Unterkörper von K. Dieser ist isomorph zu $\mathbb{F}_0 := \mathbb{Q}$.*

DEFINITION 3.1.3
Die Zahl p aus Satz 3.1.1 heißt Charakteristik von K (Schreibweise: $p = \mathrm{char}(K)$). Man nennt $\mathbb{F}_p$ den Primkörper der Charakteristik p. Der kleinste Unterkörper von K (d. h. der Durchschnitt aller Unterkörper von K) heißt Primkörper von K.

SATZ 3.1.1
Offenbar ist $\Phi : \mathbb{Z} \to K$, $n \mapsto n \cdot 1_K$ ein Ringhomomorphismus. Weil $\tilde{\Phi}(1) = 1_K$ für jeden Ringhomomorphismus $\tilde{\Phi} : \mathbb{Z} \to K$ gilt, ist Φ eindeutig bestimmt. Da K Integritätsring ist, ist auch $\Phi(\mathbb{Z}) \subseteq K$ Integritätsring. Wegen $\Phi(\mathbb{Z}) \cong \mathbb{Z}/\mathrm{Ker}(\Phi)$ ist nach Satz 2.1.4 $\mathrm{Ker}(\Phi)$ ein Primideal von $\mathbb{Z}$. Nach Satz 2.1.5 folgt: $\mathrm{Ker}(\Phi) = \{0\}$ oder $\mathrm{Ker}(\Phi) = p\mathbb{Z}$ mit p Primzahl. Da jeder Unterkörper von K das Einselement 1_K enthalten muss, muss er auch $\Phi(\mathbb{Z})$ enthalten. Daraus folgt die Behauptung im 1. Fall. Es sei $p = 0$. Dann ist Φ injektiv. Da $\mathbb{Q}$ ein Quotientenkörper von $\mathbb{Z}$ ist, gibt es nach Satz 2.2.1 genau einen Homomorphismus $\phi : \mathbb{Q} \to K$, der Φ fortsetzt. □

DEFINITION 3.1.4
Es sei L/K eine Körpererweiterung und M eine Teilmenge von L. Dann setzt man

- $[M]$:= der kleinste Teilring von L, der M umfasst,
- (M) := der kleinste Unterkörper von L, der M umfasst,
- $K[M] := [K \cup M]$,
- $K(M) := (K \cup M)$.

Ist $M = \{\alpha_1, \ldots, \alpha_n\}$, so schreibt man $K(\alpha_1, \ldots, \alpha_n)$ für $K(M)$. Eine Körpererweiterung L/K heißt einfach bzw. endlich erzeugt, falls $L = K(\alpha)$ bzw. $L = K(\alpha_1, \ldots, \alpha_n)$ ist für $\alpha, \alpha_1, \ldots, \alpha_n \in L$. Sind K_1, K_2 Unterkörper von L, so heißt $K_1(K_2) = K_2(K_1)$ das Kompositum von K_1 und K_2 (Schreibweise: K_1K_2).

3.2. Körpererweiterungen

DEFINITION 3.2.1
Es sei L eine Erweiterung eines Körpers K. Unter dem Grad von L über K (Schreibweise $[L : K]$) versteht man die Dimension von L als Vektorraum über K. L heißt unendliche Erweiterung von K, falls $[L : K] = \infty$ ist. L heißt endliche Erweiterung von K, falls $[L : K] = n < \infty$ ist.

SATZ 3.2.1 (Gradsatz)
Es seien L, K, M Körper und L/K und M/L Körpererweiterungen (Schreibweise: $M/L/K$).

(a) *Es ist $[M : K] < \infty$ genau dann, wenn $[M : L] < \infty$ und $[L : K] < \infty$ ist.*
(b) *In diesem Fall ist $[M : K] = [M : L] \cdot [L : K]$.*
(c) *Ist $\{x_1, \ldots, x_m\}$ eine Basis des Vektorraums L über K und $\{y_1, \ldots, y_n\}$ eine Basis von M über L, so ist $\{x_i \cdot y_j \mid 1 \leq i \leq m\ ,\ 1 \leq j \leq n\}$ eine Basis von M über K.*

BEWEIS
Wir beweisen c), daraus folgt offenbar a) und b). Wir zeigen zunächst, dass $B = \{x_iy_j \mid 1 \leq i \leq m\ ,\ 1 \leq j \leq n\}$ ein Erzeugendensystem des Vektorraums M über K ist. Es sei $\gamma \in M$. Da $\{y_1, \ldots, y_n\}$ eine Basis des Vektorraums M über dem Körper L ist, gibt es $\beta_1, \ldots, \beta_n \in L$ mit $\gamma = \beta_1y_1 + \cdots + \beta_ny_n$. Da andererseits $\{x_1, \ldots, x_m\}$ Basis von L über K ist gibt es α_{ij} für $1 \leq i \leq m$ und $1 \leq j \leq n$, so dass $\beta_j = \alpha_{1j}x_1 + \cdots + \alpha_{mj}x_m$ für $1 \leq j \leq n$ ist. Es folgt

$$\gamma \ = \ \sum_{j=1}^{n} \sum_{i=1}^{m} \alpha_{ij} x_i y_j \ .$$

Es bleibt, die lineare Unabhängigkeit der x_iy_j über K zu zeigen. Angenommen

$$\sum_{j=1}^{n} \sum_{i=1}^{m} \alpha_{ij} x_i y_j \ = \ 0$$

für Koeffizienten $\alpha_{ij} \in K$, dann folgt

$$\sum_{j=1}^{n} \left(\sum_{i=1}^{m} \alpha_{ij} x_i \right) y_j \ = \ 0 \, ,$$

und damit für jedes j auch

$$\sum_{i=1}^{m} \alpha_{ij} x_i \ = \ 0 \, ,$$

da die y_i linear unabhängig über L sind. Aus der linearen Unabhängigkeit der x_i über K folgt damit dann $\alpha_{ij} = 0$ für alle $1 \leq i \leq m$ und $1 \leq j \leq n$. □

Wir untersuchen nun einfache Körpererweiterungen auf Endlichkeit.

DEFINITION 3.2.2
Es sei L/K eine Körpererweiterung. Ein $\alpha \in L$ heißt algebraisch über K, falls es ein Polynom $f \in K[X] - \{0\}$ gibt mit $f(\alpha) = 0$. Ein $\alpha \in L$ heißt transzendent über K, falls es nicht algebraisch über K ist. Die Erweiterung L/K heißt algebraisch über K, falls alle $\alpha \in L$ algebraisch über K sind. Nicht algebraische Erweiterungen heißen transzendent. Eine komplexe Zahl $z \in \mathbb{C}$ heißt algebraisch (bzw. transzendent), falls z algebraisch (bzw. transzendent) über $\mathbb{Q}$ ist.

BEMERKUNG 3.2.1
Es sei $\alpha \in L$.

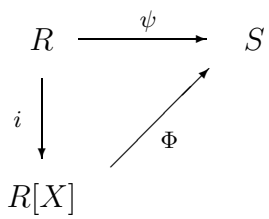
(a) Offenbar ist α transzendent über K genau dann, wenn α eine Unbestimmte über K ist.
(b) Man kann zeigen, dass wichtige Konstanten der Analysis (beispielsweise e und π) transzendent sind.

DEFINITION 3.2.3
Unter einem normierten Polynom $f \in K[X]$ versteht man ein Polynom mit höchstem Koeffizienten 1_K: $f = X^n + a_{n-1}X^{n-1} + \cdots + a_1X + a_0$.

SATZ 3.2.2
Es sei X eine Unbestimmte über K und L/K eine Körpererweiterung von K mit $\alpha \in L$. Der Ringhomomorphismus Φ sei gegeben durch $\Phi : K[X] \to K[\alpha]$, $f \mapsto f(\alpha)$.

(a) *α ist transzendent über K genau dann, wenn $\mathrm{Ker}(\Phi) = \{0\}$ ist. In diesem Fall ist $K[\alpha] \cong K[X]$, und $K[\alpha]$ ist kein Körper. $K(\alpha)$ ist der Quotientenkörper von $K[\alpha]$.*
(b) *Es sei α algebraisch über K. Dann ist $\mathrm{Ker}(\Phi) = (g)$ für ein eindeutig bestimmtes normiertes und irreduzibles Polynom $g \in K[X]$. Für $h \in K[x]$ gilt: $h(\alpha) = 0 \Leftrightarrow g|h$, und g ist durch diese Eigenschaft eindeutig bestimmt: es ist das Polynom kleinsten Grades aus $K[X] - \{0\}$ mit der Nullstelle α. Es gilt: $K(\alpha) = K[\alpha] \cong K[X]/(g)$ und $K(\alpha) = \{\beta \mid \beta = a_0 + a_1\alpha + \cdots + a_{n-1}\alpha^{n-1}\ ,\ a_i \in K\ ,\ 0 \leq i \leq n-1\}$, wobei jedes $\beta \in K(\alpha)$ genau eine Darstellung der Form $\beta = a_0 + a_1\alpha + \cdots + a_{n-1}\alpha^{n-1}$ mit Koeffizienten aus K besitzt. Es ist $[K(\alpha) : K] = \deg(g) = n$.*
(c) *Folgende Aussagen sind äquivalent:*
  (i) *α ist algebraisch über K,*
  (ii) *$K(\alpha)/K$ ist eine endliche Erweiterung,*
  (iii) *$K(\alpha)/K$ ist eine algebraische Erweiterung.*

BEWEIS
Zu a) und b): Wir verwenden die Definition 2.3.1 des Polynomrings. Danach besteht ein Polynomring aus einem kommutativen Ring $R[X]$ und einem Ringhomomorphismus $i : R \to R[X]$, so dass für jeden Ringhomomorphismus $\psi : R \to S$ in einen kommutativen Ring S und $x \in S$ es genau einen Ringhomomorphismus $\Phi : R[X] \to S$ mit $\psi = \Phi \circ i$ und $\Phi(X) = x$ gibt, d. h. wir haben das kommutative Diagramm



von Ringen. Wir setzen nun $R = K$, $i = \mathrm{id}_K$, $S = L$, $x = \alpha$ und $\psi = \mathrm{id}_K$. Es gibt genau einen Ringhomomorphismus $\Phi: K[X] \to K[\alpha]$, für den wegen der Relationstreue $\Phi(f(X)) = f(\alpha)$ für alle $f \in K[X]$ gelten muss. Nach Satz 2.3.3 ist Φ ein Isomorphismus genau dann, wenn α eine Unbestimmte über K, d. h. transzendent über K ist. Da $K[X]$ kein Körper ist, ist auch $K[\alpha]$ keiner. Der kleinste Körper, der $K[\alpha]$ enthält, ist sein Quotientenkörper. Ist α algebraisch über K, so ist $\mathrm{Ker}(\Phi)$ ein Ideal $\neq \{0\}$. Da $K[X]$ ein Euklidischer Ring ist, ist $\mathrm{Ker}(\Phi) = (g)$ mit $g \in K[X] - \{0\}$. Nach dem Homomorphiesatz für Ringe (Satz 2.1.3) ist dann $K[X]/(g) \cong K[\alpha]$. Da $K[\alpha]$ ein Integritätsring ist, ist (g) nach Satz 2.1.4 ein Primideal. Nach Satz 2.4.2 ist g irreduzibel. Nach Satz 2.4.4(c) ist (g) maximal. Damit ist nach Satz 2.1.4(b) der Faktorring $K[x]/(g)$ und somit auch $K[\alpha]$ ein Körper. Also $K(\alpha) = K[\alpha]$. Es sei $h \in K[X]$, dann gilt $h(\alpha) = 0 \Leftrightarrow h \in \mathrm{Ker}(\Phi) = (g) \Leftrightarrow g|h$. Es sei $f \in K[X]$ und $f(X) = g(X)q(X) + r(X)$ mit $\deg(r) < \deg(g) = n$. Dann ist $f(\alpha) = g(\alpha)q(\alpha) + r(\alpha) = r(\alpha)$, und damit $K[\alpha] = \{r(\alpha) \mid r \in K[X]\ ,\ \deg(r) \leq n-1\} = \{a_0 + a_1\alpha + \cdots + a_{n-1}\alpha^{n-1} \mid a_i \in K\}$. Es ist $a_0 + a_1\alpha + \cdots + a_{n-1}\alpha^{n-1} = 0 \Leftrightarrow \forall i: \ a_i = 0$. Damit ist $\{1, \alpha, \cdots, \alpha^{n-1}\}$ eine Basis des Vektorraums $K(\alpha)$ über K, und die Darstellung jedes $\beta \in K(\alpha)$ in der angegebenen Form ist eindeutig. Es folgt $[K(\alpha) : K] = n$. Zu c): Die Aussage (i)⇒(ii) ist schon in b) enthalten. (ii)⇒(iii): Es sei $\beta \in K(\alpha)$ mit $[K(\alpha) : K] = n$. Dann sind die $n+1$ Elemente $1, \beta, \ldots, \beta^n$ des Vektorraums $K(\alpha)$ über K linear abhängig, d. h. es gibt ein $g = b_0 + b_1X + \cdots + b_nX^n \in K[X]$ mit $g(\beta) = b_0 + b_1\beta + \cdots + b_n\beta^n = 0$. Das heißt, dass β algebraisch über K ist. (iii)⇒(i): Insbesondere ist α algebraisch über K, und nach Teil b) ist $K(\alpha)/K$ endlich. □

DEFINITION 3.2.4
Es sei α algebraisch über dem Körper K. Das Polynom g des Satzes 3.2.2 heißt Minimalpolynom von α über K (Schreibweise: $m_K(\alpha, X)$). Der Grad $\deg(m_K(\alpha, X))$ des Minimalpolynoms heißt auch Grad von α über K (Schreibweise: $\deg_K(\alpha)$). Nach Satz 3.2.2 ist $\deg_K(\alpha) = [K(\alpha) : K]$. Offenbar ist $\deg_K(\alpha) = 1 \Leftrightarrow m_K(\alpha, X) = X - \alpha \Leftrightarrow \alpha \in K$.

BEISPIEL 3.2.1
Es sei $K = \mathbb{Q}$ und $L = \mathbb{R}$. Nach dem Zwischenwertsatz der Analysis hat das Polynom $g(X) = X^3 - 2$ in $L = \mathbb{R}$ genau eine Nullstelle, nämlich $\alpha = \sqrt[3]{2}$. Nach dem Eisensteinkriterium (Satz 2.4.9) ist g irreduzibel. Daher ist $m_{\mathbb{Q}}(\sqrt[3]{2}, X) = X^3 - 2$. Nach Satz 3.2.3 ist

$$\mathbb{Q}(\sqrt[3]{2}) \ = \ \left\{a_0 + a_1\sqrt[3]{2} + a_2(\sqrt[3]{2})^2 \mid a_0, a_1, a_2 \in \mathbb{Q}\right\}$$

und $[\mathbb{Q}(\sqrt[3]{2}) : \mathbb{Q}] = 3$. Es sei $\gamma = 4 - 2\sqrt[3]{2} + (\sqrt[3]{2})^2 \in \mathbb{Q}(\sqrt[3]{2})$. Wir wollen γ^{-1} als Polynom höchstens zweiten Grades in $\sqrt[3]{2}$ schreiben.

Lösung: Wir setzen $g(X) = m_{\mathbb{Q}}(\sqrt[3]{2}, X) = X^3 - 2$ und $f(X) = X^2 - 2X + 4$, also $\gamma = f(\sqrt[3]{2})$. Mittels des Euklidischen Algorithmus bestimmen wir $s, t \in \mathbb{Q}[X]$ so dass $f \cdot s + g \cdot t = 1$ ist in $\mathbb{Q}[X]$:

$$\begin{array}{rrcl} & X^3 - 2 & = & (X+2)(X^2 - 2X + 4) - 10 \\ \Rightarrow & 10 & = & (X+2)(X^2 - 2X + 4) - (X^3 - 2) \\ \Rightarrow & 1 & = & (\frac{1}{10}X + \frac{1}{5})(X^2 - 2X + 4) - \frac{1}{10}(X^3 - 2) \\ \Rightarrow & 1 & = & (\frac{1}{5} + \frac{1}{10}\sqrt[3]{2})(4 - 2\sqrt[3]{2} + (\sqrt[3]{2})^2) \end{array}$$

und damit $\gamma^{-1} = \frac{1}{5} + \frac{1}{10}\sqrt[3]{2}$.

Wir wenden uns nun Körpererweiterungen zu, die nicht notwendig einfach sind.

SATZ 3.2.3
Es sei L/K eine Körpererweiterung. Folgende Eigenschaften sind äquivalent:

(i) *L/K ist endlich,*
(ii) *L/K ist algebraisch und $L = K(\alpha_1, \ldots, \alpha_n)$,*
(iii) *$L = K(\alpha_1, \ldots, \alpha_n)$ ist endlich erzeugt, wobei α_i jeweils algebraisch über $K(\alpha_1, \ldots, \alpha_{i-1})$ ist für $i = 1 \ldots n$.*

BEWEIS
(i)⇒(ii): Es sei $\alpha \in L$. Wegen $K \subseteq K(\alpha) \subseteq L$ ist $K(\alpha)/K$ nach Satz 3.2.1 endlich. Nach Satz 3.2.2(c) ist α algebraisch über K. Also ist L/K algebraisch. Wir konstruieren nun eine beliebige (endliche oder unendliche) Folge (α_i) mit $\alpha_i \in L$, so dass $\alpha_1 \notin K$ und $\alpha_i \notin K(\alpha_1, \ldots, \alpha_{i-1})$ ist. Nach dem Gradsatz (Satz 3.2.1) ist dann

$$\begin{aligned}[K(\alpha_1, \ldots, \alpha_i) : K] \;=\; & [K(\alpha_1, \ldots, \alpha_i \;\;) : K(\alpha_1, \ldots, \alpha_{i-1})] \;\cdot \\ & [K(\alpha_1, \ldots, \alpha_{i-1}) : K(\alpha_1, \ldots, \alpha_{i-2})] \;\cdot \\ & \vdots \\ & [K(\alpha_1) : K] \;\geq\; 2^i.\end{aligned}$$

Da L/K endlich ist, muss nach endlich vielen Schritten $K(\alpha_1, \ldots, \alpha_n) = L$ gelten. (ii)⇒(iii): Da L/K algebraisch ist, ist α_i algebraisch über K und damit auch über $K(\alpha_1, \ldots, \alpha_{i-1})$. (iii)⇒(i): Nach dem Gradsatz und Satz 3.2.2(c) ist

$$[L : K] \;=\; [L : K(\alpha_1, \ldots, \alpha_{n-1})] \cdots [K(\alpha_1) : K] \;<\; \infty\,.$$

□

SATZ 3.2.4
Es seien $M/L/K$ Körpererweiterungen. Ist M algebraisch über L und L algebraisch über K, so ist auch M algebraisch über K.

BEWEIS
Es sei $\beta \in M$, dann ist β algebraisch über L, d. h. es gibt ein $f \in L[X] - \{0\}$ mit $f(X) = \alpha_n X^n + \alpha_{n-1} X^{n-1} + \cdots + \alpha_0$ $(\alpha_i \in L)$ und $f(\beta) = 0$. Damit ist β auch algebraisch über $K(\alpha_0, \ldots, \alpha_n)$, insbesondere ist $[K(\alpha_0, \ldots, \alpha_n, \beta) : K(\alpha_0, \ldots, \alpha_n)] < \infty$. Nach Satz 3.2.3(a) ist $[K(\alpha_0, \ldots, \alpha_n) : K] < \infty$, nach dem Gradsatz (Satz 3.2.1) ist also $[K(\alpha_0, \ldots, \alpha_n, \beta) : K] < \infty$, also auch $[K(\beta) : K] < \infty$, und β ist algebraisch über K. □

3.3. Fortsetzung von Körperisomorphismen und Automorphismengruppen

DEFINITION 3.3.1
Es seien L_1, L_2 Erweiterungen eines Körpers K. Ein Isomorphismus $\sigma : L_1 \to L_2$ heißt K-Isomorphismus, falls $\sigma(z) = z$ für alle $z \in K$ ist. Falls ein solcher K-Isomorphismus existiert, heißen L_1 und L_2 auch K-isomorph. Ist $L_1 = L_2$, so heißt σ auch K-Automorphismus von L.

Wir untersuchen zunächst die Frage, wann zwei einfache endliche Erweiterungen eines gegebenen Körpers K zueinander K-isomorph sind.

DEFINITION 3.3.2
Es sei K ein Körper, α und β Elemente einer Erweiterung von K. α und β heißen konjugiert über K, wenn beide Elemente algebraisch über K sind, und das gleiche Minimalpolynom über K besitzen. β heißt auch Konjugierte von α.

Beispiel 3.3.1
Es sei $\alpha = \sqrt[4]{2}$ und $K = \mathbb{Q}$. Nach dem Eisensteinkriterium (Satz 2.4.9) ist $X^4 - 2$ in $\mathbb{Q}[X]$ irreduzibel und hat die Nullstelle α. Damit ist $m_{\mathbb{Q}}(\alpha, X) = X^4 - 2$. Im Körper $\mathbb{C}$ der komplexen Zahlen gilt dann:

$$m_{\mathbb{Q}}(\alpha, X) = \left(X - \sqrt[4]{2}\right) \cdot \left(X + \sqrt[4]{2}\right) \cdot \left(X - i\sqrt[4]{2}\right) \cdot \left(X + i\sqrt[4]{2}\right) .$$

Damit sind die Elemente $\alpha_1 = \sqrt[4]{2}$, $\alpha_2 = -\sqrt[4]{2}$, $\alpha_3 = i \cdot \sqrt[4]{2}$ und $\alpha_4 = -i \cdot \sqrt[4]{2}$ Konjugierte über $\mathbb{Q}$. Diese vier Elemente sind alle Konjugierten von α in $\mathbb{C}$, da $m_{\mathbb{Q}}(\alpha, X)$ keine anderen Nullstellen besitzt. Die Elemente α_1 und α_2 sind auch konjugiert über $\mathbb{Q}(\sqrt{2})$, da

$$m_{\mathbb{Q}(\sqrt{2})}(\alpha_1, X) \;=\; m_{\mathbb{Q}(\sqrt{2})}(\alpha_2, X) \;=\; X^2 - \sqrt{2}$$

ist. Ebenso sind α_3 und α_4 konjugiert über $\mathbb{Q}(\sqrt{2})$, da

$$m_{\mathbb{Q}(\sqrt{2})}(\alpha_3, X) \;=\; m_{\mathbb{Q}(\sqrt{2})}(\alpha_4, X) \;=\; X^2 + \sqrt{2}$$

gilt. Hingegen sind α_1 oder α_2 zu keinem der Elemente α_3 oder α_4 konjugiert über $\mathbb{Q}(\sqrt{2})$.

Satz 3.3.1
Es sei K ein Körper und α, β algebraisch über K. Falls α und β das gleiche Minimalpolynom über K besitzen, sind $K(\alpha)$ und $K(\beta)$ K-isomorph. Ein K-Isomorphismus wird dann durch die Zuordnung

$$\sum_{j=0}^{n-1} b_j \alpha^j \;\mapsto\; \sum_{j=0}^{n-1} b_j \beta^j$$

für $n = \deg(\alpha) = \deg(\beta)$ mit $b_j \in K$ hergestellt.

In Hinblick auf weitere Anwendungen beweisen wir eine Verallgemeinerung (Satz 3.3.2).

Definition 3.3.3
Es seien L bzw. $\overline{L}$ Erweiterungen von K bzw. $\overline{K}$. Es sei σ ein Isomorphismus von K auf $\overline{K}$ und τ ein Isomorphismus von L auf $\overline{L}$. Wir sagen: τ setzt σ fort, bzw. τ ist Fortsetzung von σ, falls $\tau(z) = \sigma(z)$ für alle $z \in K$ gilt, wenn also σ gerade die Einschränkung $\tau|_K$ von τ ist.

Satz 3.3.2
Es sei α algebraisch über K und $g(X) = m_K(\alpha, X) = a_0 + a_1 X + \cdots + a_{n-1} X^{n-1} + X^n$. Ferner sei $\overline{L}$ eine Erweiterung eines Körpers $\overline{K}$ und ein Isomorphismus $\sigma : K \to \overline{K}$ gegeben, sowie $g^{(\sigma)}(Y) = \sigma(a_0) + \sigma(a_1)Y + \cdots + \sigma(a_{n-1})Y^{n-1} + Y^n \in K[Y]$ mit einer Unbestimmten Y über $\overline{K}$ gesetzt.

(a) *Genau dann gibt es einen Isomorphismus $\tau : K(\alpha) \to K'$ in einen Unterkörper $K' \leq \overline{L}$ der σ fortsetzt, wenn $g^{(\sigma)}$ mindestens eine Nullstelle in $\overline{L}$ besitzt.*
(b) *Sind $\beta_1, \ldots, \beta_r$ die verschiedenen Nullstellen von $g^{(\sigma)}$ in $\overline{L}$, so gibt es genau r derartige Fortsetzungen von σ. Dies sind die surjektiven Abbildungen $\tau_k : K(\alpha) \to \overline{K}(\beta_k)$ für $k = 1, \ldots, r$ definiert durch*

$$\tau_k \left(\sum_{j=0}^{n-1} b_j \alpha^j \right) \;=\; \sum_{j=0}^{n-1} \sigma(b_j) \beta_k^j$$

mit $n = [K(\alpha) : K]$.

Kurz ausgedrückt: Die Fortsetzungen $\tau_1, \ldots, \tau_r$ von σ sind den Nullstellen $\beta_1, \ldots, \beta_r$ von $g^{(\sigma)}(Y)$ in $\overline{L}$ eindeutig zugeordnet. Die Abbildung τ_k ist eindeutig bestimmt durch die Forderung

$$\tau_k(\alpha) \;=\; \beta_k \,,$$

und es ist $[K(\alpha) : K] = [\overline{K}(\beta_k) : \overline{K}]$ für $k = 1 \ldots r$.

BEMERKUNG 3.3.1
Satz 3.3.1 ergibt sich als Spezialfall von Satz 3.3.2, wenn $K = \overline{K}$ und $\sigma = \mathrm{id}_K$ gesetzt wird.

BEWEIS
Zu a): Es sei $\tau :\; K(\alpha) \to K'$ ein Isomorphismus, der σ fortsetzt. Dann gilt

$$0 \;=\; \tau(g(\alpha)) \;=\; \sum_{j=0}^{n} \tau(a_j) \cdot \tau(\alpha)^j \;=\; \sum_{j=0}^{n} \sigma(a_j) \cdot \tau(\alpha)^j \;=\; g^{(\sigma)}(\tau(\alpha)) \,,$$

also ist $\tau(\alpha)$ eine Nullstelle von $g^{(\sigma)}$ in $\overline{L}$. Durch die Kenntnis von $\beta = \tau(\alpha)$ ist τ vollständig bestimmt, denn für ein beliebiges $b \in K(\alpha)$ gilt:

$$b \;=\; \sum_{j=0}^{n-1} b_j \alpha^j \;\;\Rightarrow\;\; \tau(b) \;=\; \sum_{j=0}^{n-1} \tau(b_j)\tau(\alpha^j) \;=\; \sum_{j=0}^{n-1} \sigma(b_j)\beta^j \,.$$

Zu b): Umgekehrt sei β irgend eine Nullstelle von $g^{(\sigma)}(Y)$ in $\overline{L}$. Für ein beliebiges $b \in K(\alpha)$, etwa $b = \sum b_j \alpha^j$ mit $b_j \in K$, setzen wir

$$\tau(b) \;:=\; \sum_{j=0}^{n-1} \sigma(b_j)\alpha^j \,.$$

Es bleibt nachzuweisen, dass τ ein Isomorphismus von $K(\alpha)$ auf $\overline{K}(\beta)$ ist, der σ fortsetzt. Dazu beachtet man zunächst, dass $g^{(\sigma)}(Y) = m_{\overline{K}}(\beta, Y)$ ist. Wie man leicht nachrechnet, ist die Abbildung

$$\omega :\; \sum b_j X^j \;\mapsto\; \sum \sigma(b_j) Y^j$$

ein Isomorphismus $K[X] \to \overline{K}[Y]$ mit $\omega(g) = g^{(\sigma)}$. Aus der Irreduzibilität von g in $K[X]$ folgt die Irreduzibilität von $g^{(\sigma)}$ in $\overline{K}[Y]$. Es sei

$$h :\; \sum b_j X^j \;+ (g) \;\mapsto\; \sum \sigma(b_j) Y^j \;+ (g^{(\sigma)}) \,.$$

Offenbar ist h ein Epimorphismus $h :\; K[x] \,/\, (g) \;\to\; \overline{K}[Y] \,/\, (g^{(\sigma)})$. Wir wollen zeigen, dass h auch injektiv, und damit ein Isomorphismus ist. Dazu bestimmen wir $\mathrm{Ker}(h)$. Es sei $h(\sum b_j X^j + (g)) = 0_{\overline{K}[Y]} + (g^{(\sigma)}) = (g^{(\sigma)})$. Dann gilt $g^{(\sigma)} \mid \sum \sigma(b_j) Y^j$, also ist $\sum \sigma(b_j) Y^j = g^{(\sigma)} \cdot h^{(\sigma)}$ für ein $h^{(\sigma)} = \sum \sigma(d_j) Y^j = \omega(h)$ mit $h = \sum d_j X^j$. Anwendung von ω^{-1} ergibt dann $\sum b_j X^j = g \cdot h$, also $\sum b_j X^j + (g) = 0_{K[X]} + (g)$. Daraus folgt $\mathrm{Ker}(h) = \{0_{K[X]/(g)}\}$. Nach Satz 3.2.2 sind die Abbildungen

$$\begin{array}{rccccccc} \psi_1 : & K[\alpha] & \to & K[X] \,/\, (g) & , & \sum b_j \alpha^j & \mapsto & \sum b_j X^j \;+\; (g) \\ \psi_2 : & \overline{K}[\beta] & \to & \overline{K}[Y] \,/\, (g^{(\sigma)}) & , & \sum \sigma(b_j)\beta^j & \mapsto & \sum \sigma(b_j) Y^j \;+\; (g^{(\sigma)}) \end{array}$$

Isomorphismen. Daher ist auch $\tau = \psi_2^{-1} \circ h \circ \psi_1$ ein Isomorphismus, und besitzt die gewünschten Eigenschaften. □

BEISPIEL 3.3.2
Es sei $K = \overline{K} = \mathbb{Q}$ und $\overline{L} = \mathbb{C}$ mit $\sigma = \mathrm{id}_{\mathbb{Q}}$ und $\alpha = \sqrt{2}$. Es liegt also der Spezialfall Satz 3.3.1 vor. Nach dem Eisensteinkriterium ist das Polynom $q(X) = X^2 - 2$ irreduzibel. Das Element $\alpha = \sqrt{2}$ hat daher das Minimalpolynom $q(X) = X^2 - 2$. Wegen $\sigma = \mathrm{id}_{\mathbb{Q}}$ ist $g^{(\sigma)} = Y^2 - 2$ mit den Nullstellen $\beta_1 = \sqrt{2}$ und $\beta_2 = -\sqrt{2}$ in $\overline{L} = \mathbb{C}$. Die Fortsetzungen τ_j $(j = 1, 2)$ von $\sigma = \mathrm{id}$ sind also bestimmt durch den Wert $\tau_j(\alpha) \in \{\beta_1, \beta_2\}$.

Fall j=1:
Die Festlegung $\tau_1 : \sqrt{2} \mapsto \sqrt{2}$ ergibt $\tau_1(b_0 + b_1\sqrt{2}) = b_0 + b_1\sqrt{2}$ für alle $b_0, b_1 \in \mathbb{Q}$, also $\tau_1 = \mathrm{id}_{\mathbb{Q}(\sqrt{2})}$.

Fall j=2:
Die Festlegung $\tau_2 : \sqrt{2} \mapsto -\sqrt{2}$ ergibt $\tau_2(b_0 + b_1\sqrt{2}) = b_0 - b_1\sqrt{2}$.

BEISPIEL 3.3.3
Es sei $K = \overline{K} = \mathbb{Q}(\sqrt{2})$ mit $\sigma_1 = \mathrm{id}_K = \tau_1$ und $\sigma_2 = \tau_2$ aus dem vorigen Beispiel. Dazu sei $\alpha_1 = \sqrt[4]{2}$ und $\alpha_2 = i \cdot \sqrt[4]{2}$. Nach Beispiel 1.3.1 ist $m_{\mathbb{Q}}(\alpha_1, X) = m_{\mathbb{Q}}(\alpha_2, X) = X^4 - 2$. Also ist $\deg(\alpha_1) = \deg(\alpha_2) = 4$. Damit sind $\alpha_1, \alpha_2 \notin K$ wegen $[K : \mathbb{Q}] = 2$. Es ist

$$\begin{array}{rcccl} m_K(\alpha_1, X) & = & X^2 - \sqrt{2} & = & g_1(X) \\ m_K(\alpha_2, X) & = & X^2 + \sqrt{2} & = & g_2(X) \quad . \end{array}$$

Die Fortsetzungen von σ_1:
Die Fortsetzungen von σ_1 sind nach Satz 3.3.2 eindeutig durch die Nullstellen $\beta_{1,1} = \sqrt[4]{2}$ und $\beta_{1,2} = -\sqrt[4]{2}$ von $g_1^{(\sigma_1)} = Y^2 - \sqrt{2}$ bestimmt. Wir haben die Fortsetzungen

$$\begin{array}{rcccl} \sigma_{1,1} : & \sqrt[4]{2} & \mapsto & \sqrt[4]{2} & \text{, d. h. } \sigma_{1,1} = \mathrm{id}_{\mathbb{Q}(\sqrt[4]{2})} \\ \sigma_{1,2} : & \sqrt[4]{2} & \mapsto & -\sqrt[4]{2} & \text{, d. h.} \end{array}$$

$$\sigma_{1,2} : \; b_0 + b_1\sqrt[4]{2} + b_2\sqrt[2]{2} + b_3(\sqrt[4]{2})^3 \mapsto b_0 - b_1\sqrt[4]{2} + b_2\sqrt[2]{2} - b_3(\sqrt[4]{2})^3 \; .$$

Die Fortsetzungen von σ_2:
Die Fortsetzungen von σ_2 sind durch die Nullstellen von $g^{(\sigma_2)}(Y) = Y^2 - \sigma_2(\sqrt{2}) = Y^2 + \sqrt{2}$ gegeben: $\beta_{2,1} = i \cdot \sqrt[4]{2}$ und $\beta_{2,2} = -i \cdot \sqrt[4]{2}$.

$$\sigma_{2,1} : \; \sqrt[4]{2} \mapsto i \cdot \sqrt[4]{2} \quad \text{, d. h.}$$

$$\sigma_{2,1} : \; b_0 + b_1\sqrt[4]{2} + b_2\sqrt[2]{2} + b_3(\sqrt[4]{2})^3 \mapsto b_0 + b_1(i \cdot \sqrt[4]{2}) - b_2\sqrt[2]{2} + b_3(i \cdot \sqrt[4]{2})^3 \; .$$

$$\sigma_{2,2} : \; \sqrt[4]{2} \mapsto -i \cdot \sqrt[4]{2} \quad \text{, d. h.}$$

$$\sigma_{2,1} : \; b_0 + b_1\sqrt[4]{2} + b_2\sqrt[2]{2} + b_3(\sqrt[4]{2})^3 \mapsto b_0 - b_1(i \cdot \sqrt[4]{2}) - b_2\sqrt[2]{2} + b_3 \cdot i \cdot (\sqrt[4]{2})^3 \; .$$

Das heißt, dass σ_2 keine Fortsetzung zu Isomorphismen $\mathbb{Q}(\sqrt[4]{2}) \to \mathbb{Q}(\sqrt[4]{2})$ besitzt, da $g^{(\sigma_2)}$ keine Nullstellen in $\mathbb{Q}(\sqrt[4]{2})$ hat.

BEISPIEL 3.3.4
Man finde sämtliche $\mathbb{Q}$-Automorphismen von $L = \mathbb{Q}(\sqrt[4]{2}, i)$.

Lösung:
L ist eine Erweiterung des im vorigen Beispiel betrachteten Körpers $\mathbb{Q}(\sqrt[4]{2})$. Nach Satz 3.3.2 findet man sämtliche Automorphismen von L als Fortsetzungen der im vorigen Beispiel betrachteten Isomorphismen von $\mathbb{Q}(\sqrt[4]{2})$, deren Bilder in L liegen.

Die Fortsetzungen der Isomorphismen $\sigma_{1,1}$ und $\sigma_{1,2}$:
Wir wenden Satz 3.3.2 mit $K = \overline{K} = \mathbb{Q}(\sqrt[4]{2})$ an. Das Polynom $q(X) = X^2 + 1$ ist irreduzibel in $K[X]$, da es in K keine Nullstelle besitzt. Also ist $m_K(i, X) = X^2 + 1 = (X + i)(X - i)$ und somit $[L : \mathbb{Q}] = 8$. Es ist $g^{(\sigma_{1,1})}(Y) = g^{(\sigma_{1,2})} = Y^2 + 1$. Die Fortsetzungen $\sigma_{1,1,1}$ und $\sigma_{1,1,2}$ von $\sigma_{1,1}$ bzw. $\sigma_{1,2,1}$ und $\sigma_{1,2,2}$ von $\sigma_{1,2}$ sind durch die Nullstellen i und $-i$ von $g^{(\sigma_{1,2})}(Y)$ bestimmt:

$$\begin{array}{rrcrcrl} \sigma_{1,1,1}: & \sqrt[4]{2} & \mapsto & \sqrt[4]{2} & , & i \mapsto & i \\ \sigma_{1,1,2}: & \sqrt[4]{2} & \mapsto & \sqrt[4]{2} & , & i \mapsto & -i \\ \sigma_{1,2,1}: & \sqrt[4]{2} & \mapsto & -\sqrt[4]{2} & , & i \mapsto & i \\ \sigma_{1,2,2}: & \sqrt[4]{2} & \mapsto & -\sqrt[4]{2} & , & i \mapsto & -i \quad . \end{array}$$

Insbesondere ist $\sigma_{1,1,1} = \mathrm{id}_L$.

Die Fortsetzungen der Isomorphismen $\sigma_{2,1}$ und $\sigma_{2,2}$:
Wir wenden Satz 3.3.2 mit $K = \mathbb{Q}(\sqrt[4]{2})$ und $\overline{K} = \mathbb{Q}(i \cdot \sqrt[4]{2})$ an. Wäre $i \in \overline{K}$, so wäre $L = \overline{K}$ im Widerspruch zu $[L : \mathbb{Q}] = 8$ und $[\overline{K} : \mathbb{Q}] = 4$. Damit besitzt g auch in $\overline{K}$ keine Nullstelle und ist irreduzibel in $\overline{K}[X]$. Wiederum sind die Fortsetzungen von $\sigma_{2,1}$ und $\sigma_{2,2}$ durch die Nullstellen von $g^{(\sigma_{2,1})} = g^{(\sigma_{2,2})} = Y^2 + 1$ bestimmt:

$$\begin{array}{rrcrcrl} \sigma_{2,1,1}: & \sqrt[4]{2} & \mapsto & i \cdot \sqrt[4]{2} & , & i \mapsto & i \\ \sigma_{2,1,2}: & \sqrt[4]{2} & \mapsto & i \cdot \sqrt[4]{2} & , & i \mapsto & -i \\ \sigma_{2,2,1}: & \sqrt[4]{2} & \mapsto & -i \cdot \sqrt[4]{2} & , & i \mapsto & i \\ \sigma_{2,2,2}: & \sqrt[4]{2} & \mapsto & -i \cdot \sqrt[4]{2} & , & i \mapsto & -i \quad . \end{array}$$

Damit sind alle Fortsetzungen von $\mathrm{id}_{\mathbb{Q}}$ Automorphismen von L, es gibt also insgesamt 8 Automorphismen von $L = \mathbb{Q}(\sqrt[4]{2}, i)$.

Satz 3.3.2 gibt eine Methode, die schon in den obigen Beispielen illustriert wurde, um alle K-isomorphen Bilder einer endlichen Erweiterung $K(\alpha_1, \ldots, \alpha_n)$ von K in einer Erweiterung L von K zu finden. Durch wiederholte Anwendung von Satz 3.3.1 findet man zunächst alle Fortsetzungen von id_K zu K-Isomorphismen von $K(\alpha_1)$, dann alle Fortsetzungen dieser Isomorphismen zu K-Isomorphismen von $K(\alpha_1, \alpha_2)$ usw. Auf diese Weise gelingt es, insbesondere auch sämtliche K-Automorphismen einer endlichen Erweiterung von K zu finden. Diese sind unter den Körperisomorphismen von besonderem Interesse, da ihre Menge eine Gruppe bzgl. der Hintereinanderausführung $\circ$ bildet. In den folgenden Definitionen wird zunächst nicht vorausgesetzt, dass die betrachteten Körpererweiterungen endlich sind.

Definition 3.3.4
Es sei L/K eine Körpererweiterung.

(a) Die Gruppe aller K-Automorphismen von L heißt Galoisgruppe von L/K (Schreibweise: $G(L/K)$),
(b) Ein Körper Z mit $K \subseteq Z \subseteq L$ heißt Zwischenkörper von L/K (Schreibweise: $L/Z/K$),
(c) Ist U eine Untergruppe von $G(L/K)$, so heißt

$$L^U := \{z \in L \mid \forall \sigma \in U \; \sigma(z) = z\}$$

der Fixkörper zu U in L.

Die Galoistheorie (nach E. Galois) befasst sich mit der Beziehung zwischen den Untergruppen von $G(L/K)$ und den Zwischenkörpern von L/K. Es gibt zwei Zuordnungen. Die Erste ist die Zuordnung $Z \mapsto G(L/Z)$, die jedem Zwischenkörper die Untergruppe der Z-Automorphismen

von L zuordnet. Die Zweite ist die Zuordnung $U \mapsto L^U$, die einer Untergruppe von $G(L/K)$ den zugehörigen Fixkörper in L zuordnet. In wichtigen Fällen, den so genannten galoisschen Erweiterungen, sind diese beiden Zuordnungen bijektiv und invers zueinander, also

$$G(L/L^U) = U \text{ und } L^{G(L/Z)} = Z$$

für alle Untergruppen $U \leq G(L/K)$ und Zwischenkörper $L/Z/K$. Wir geben die Ergebnisse in diesem Abschnitt an, müssen ihre Beweise aber auf später verschieben.

DEFINITION 3.3.5
Eine Körpererweiterung L/K heißt galoissch, wenn $K = L^G$ für eine endliche Untergruppe G von $G(L/K)$ ist.

SATZ 3.3.3 (Hauptsatz der Galoistheorie - Kurzform)
Es sei L/K eine galoissche Erweiterung, d. h. $K = L^G$ für eine endliche Untergruppe $G \leq G(L/K)$. Dann gilt:

(a) *$G = G(L/K)$ und $[L : K] = |G(L/K)|$, insbesondere ist L/K eine endliche Körpererweiterung.*
(b) *Die Abbildungen*

$$\{Z \mid L/Z/K \text{ Zwischenk.}\} \rightleftarrows \{U \mid U \leq G(L/K) \text{ Untergruppe}\}$$
$$\begin{array}{ccc} Z & \leftarrow & G(L/Z) \\ L^U & \rightarrow & U \end{array}$$

sind bijektiv und invers zueinander.
(c) *Für jeden Zwischenkörper $L/Z/K$ gilt:*
  (i) *L/Z ist galoissch,*
  (ii) *Z/K galoissch $\Leftrightarrow G(L/Z) \trianglelefteq G(L/K)$ ist Normalteiler.*

Wir beweisen zunächst nur den folgenden einfachen

SATZ 3.3.4
Es sei L/K eine Körpererweiterung und $U \leq G(L/K)$, sowie V eine zu U konjugierte Untergruppe, d. h. $V = \tau U \tau^{-1}$ mit einem $\tau \in G(L/K)$. Dann ist $L^V = \tau(L^U)$. Ist insbesondere U ein Normalteiler von $G(L/K)$, so ist $\tau(L^U) = L^U$ für alle $\tau \in G(L/K)$.

BEWEIS
Es sei $z \in L^U$ und $\sigma \in U$. Dann ist $\tau\sigma\tau^{-1}(\tau(z)) = \tau\sigma(z) = \tau(z)$ wegen $z \in L^U$. Also $\tau(z) \in L^V$ und damit $\tau(L^U) \subseteq L^V$. Wegen $U = \tau^{-1}V\tau$ folgt $\tau^{-1}L^V \subseteq L^U$ und damit $L^V \subseteq \tau(L^U)$. Insgesamt folgt die Behauptung. □

BEISPIEL 3.3.5
Sei $K = \mathbb{Q}$ und $L = \mathbb{Q}(\sqrt{2}, \sqrt{3})$. Bestimme die Struktur von $G(L/K)$, ihre Untergruppen und deren Fixkörper.

Lösung:
Die Fortsetzungen von $\mathrm{id}_\mathbb{Q}$ auf $\mathbb{Q}(\sqrt{2})$ sind schon in Beispiel 1.3.2 beschrieben worden. Sie sind bestimmt durch

$$\begin{array}{rcrcl} \mathrm{id}_{\mathbb{Q}(\sqrt{2})} & = & \sigma_0 : & \sqrt{2} & \mapsto & \sqrt{2} \\ & & \sigma_1 : & \sqrt{2} & \mapsto & -\sqrt{2} \end{array}$$

Annahme: $\sqrt{3} \in \mathbb{Q}(\sqrt{2})$. Dann ist $\sqrt{3} = b_0 + b_1\sqrt{2}$ für $b_1, b_2 \in \mathbb{Q}$. Wegen $\sigma_1(\sqrt{3})^2 = \sigma_1((\sqrt{3})^2) = \sigma_1(3) = 3$ folgt $b_0 - b_1\sqrt{2} \in \{\sqrt{3}, -\sqrt{3}\}$. Damit ist $b_0 = \sqrt{3}$ oder $b_1 = \sqrt{3/2}$, was wegen

$\sqrt{3}, \sqrt{3/2} \notin \mathbb{Q}$ unmöglich ist. Also $\sqrt{3} \notin \mathbb{Q}(\sqrt{2})$. Somit ist $m_{\mathbb{Q}(\sqrt{2})}(\sqrt{3}, X) = X^2 - 3 = (X - \sqrt{3})(X + \sqrt{3})$. Nach Satz 3.3.2 sind die Fortsetzungen von σ_0 und σ_1 gegeben durch

$$\begin{array}{lrcrcrcl} \sigma_{0,0}: & \sqrt{2} & \mapsto & \sqrt{2} & , & \sqrt{3} & \mapsto & \sqrt{3} \\ \sigma_{0,1}: & \sqrt{2} & \mapsto & \sqrt{2} & , & \sqrt{3} & \mapsto & -\sqrt{3} \\ \sigma_{1,0}: & \sqrt{2} & \mapsto & -\sqrt{2} & , & \sqrt{3} & \mapsto & \sqrt{3} \\ \sigma_{1,1}: & \sqrt{2} & \mapsto & -\sqrt{2} & , & \sqrt{3} & \mapsto & -\sqrt{3} \quad . \end{array}$$

Also gilt $\sigma_{k,l}: \sqrt{2} \mapsto (-1)^k\sqrt{2}$, $\sqrt{3} \mapsto (-1)^l\sqrt{3}$ für $k, l \in \{0, 1\}$. Die Komposition zweier Automorphismen wird berechnet, indem ihre Wirkung auf die Elemente $\sqrt{2}$ und $\sqrt{3}$ untersucht wird:

$$\begin{array}{rcccccl} (\sigma_{k_1,l_1} \circ \sigma_{k_2,l_2})(\sqrt{2}) & = & \sigma_{k_1,l_1}(\sigma_{k_2,l_2}(\sqrt{2})) & = & \sigma_{k_1,l_1}((-1)^{k_2}\sqrt{2}) & = & \\ & = & \sigma_{k_1,l_1}((-1)^{k_2})\sigma_{k_1,l_1}(\sqrt{2}) & = & (-1)^{k_2}\sigma_{k_1,l_1}(\sqrt{2}) & = & (-1)^{k_1+k_2} \cdot \sqrt{2} \quad , \\ \\ (\sigma_{k_1,l_1} \circ \sigma_{k_2,l_2})(\sqrt{3}) & = & \sigma_{k_1,l_1}(\sigma_{k_2,l_2}(\sqrt{3})) & = & \sigma_{k_1,l_1}((-1)^{l_2}\sqrt{3}) & = & \\ & = & \sigma_{k_1,l_1}((-1)^{l_2})\sigma_{k_1,l_1}(\sqrt{3}) & = & (-1)^{l_2}\sigma_{k_1,l_1}(\sqrt{3}) & = & (-1)^{l_1+l_2} \cdot \sqrt{3} \quad . \end{array}$$

Damit gilt $\sigma_{k_1,l_1} \circ \sigma_{k_2,l_2} = \sigma_{k_3,l_3}$, wobei (k_3, l_3) bestimmt ist durch $k_3 \equiv k_1 + k_2 \bmod 2$ und $l_3 \equiv l_1 + l_2 \bmod 2$. Diese Beziehungen legen nahe, die Beschreibung zu vereinfachen, indem man zur Indizierung der Automorphismen Restklassen mod 2 verwendet. Für $(r, s) \in (\mathbb{Z}/2\mathbb{Z}) \times (\mathbb{Z}/2\mathbb{Z})$ setzen wir $\sigma_{r,s}: \sqrt{2} \mapsto (-1)^k\sqrt{2}\,,\ \sqrt{3} \mapsto (-1)^l\sqrt{3}$ für beliebige $k \in r$ und $l \in s$. Wir erhalten die Beziehung $\sigma_{r_1,s_1} \circ \sigma_{r_2,s_2} = \sigma_{r_1+r_2,s_1+s_2}$. Die Untergruppen von $G(L/K)$ sind dann

$$\begin{array}{rcccccl} \langle \sigma_{\bar{0},\bar{0}} \rangle & = & \{\sigma_{\bar{0},\bar{0}}\} = \{\mathrm{id}_L\} & , & \langle \sigma_{\bar{0},\bar{1}} \rangle & = & \{\sigma_{\bar{0},\bar{0}}, \sigma_{\bar{0},\bar{1}}\} \quad , \\ \\ \langle \sigma_{\bar{1},\bar{0}} \rangle & = & \{\sigma_{\bar{0},\bar{0}}, \sigma_{\bar{1},\bar{0}}\} & , & \langle \sigma_{\bar{1},\bar{1}} \rangle & = & \{\sigma_{\bar{0},\bar{0}}, \sigma_{\bar{1},\bar{1}}\} \end{array}$$

und $G(L/K)$ selbst (hierbei ist $\bar{k}$ als die Restklasse $k \bmod 2$ zu verstehen). Nach den Sätzen 3.2.1 und 3.2.2 ist

$$\begin{array}{rcl} L & = & \{b_0 + b_1\sqrt{2} + b_2\sqrt{3} + b_3\sqrt{6} \mid b_i \in \mathbb{Q}\}\,, \\ L^{\langle \sigma_{\bar{0},\bar{1}} \rangle} & = & \{z \in L \mid \sigma_{\bar{0},\bar{0}}(z) = z\ ,\ \sigma_{\bar{0},\bar{1}}(z) = z\}\,. \end{array}$$

Es ist $\sigma_{\bar{0},\bar{0}}(z) = z$ für alle $z \in L$. Andererseits ist $\sigma_{\bar{0},\bar{1}}(b_0 + b_1\sqrt{2} + b_2\sqrt{3} + b_3\sqrt{6}) = b_0 + b_1\sqrt{2} - b_2\sqrt{3} - b_3\sqrt{6}$, und damit gilt $\sigma_{\bar{0},\bar{1}}(z) = z \Leftrightarrow z = b_0 + b_2\sqrt{2} \Leftrightarrow z \in \mathbb{Q}(\sqrt{2})$, d. h. $L^{\langle \sigma_{\bar{0},\bar{1}} \rangle} = \mathbb{Q}(\sqrt{2})$. Weiter folgt:

$$\begin{array}{lcl} \sigma_{\bar{1},\bar{0}}: & b_0 + b_1\sqrt{2} + b_2\sqrt{3} + b_3\sqrt{6} & \mapsto \quad b_0 - b_1\sqrt{2} + b_2\sqrt{3} - b_3\sqrt{6} \\ \sigma_{\bar{1},\bar{1}}: & b_0 + b_1\sqrt{2} + b_2\sqrt{3} + b_3\sqrt{6} & \mapsto \quad b_0 - b_1\sqrt{2} - b_2\sqrt{3} + b_3\sqrt{6} \quad , \end{array}$$

also gilt analog

$$\begin{array}{rcl} \sigma_{\bar{1},\bar{0}}(z) = z & \Leftrightarrow & z \in \mathbb{Q}(\sqrt{3}) \quad , \\ \sigma_{\bar{1},\bar{1}}(z) = z & \Leftrightarrow & z \in \mathbb{Q}(\sqrt{6}) \quad . \end{array}$$

Insgesamt ergeben sich die zu den Untergruppen von $G(L/K)$ gehörenden Fixkörper mit

$$\begin{array}{rcccccl} L^{\langle \sigma_{\bar{0},\bar{0}} \rangle} & = & L & , & L^{\langle \sigma_{\bar{0},\bar{1}} \rangle} & = & \mathbb{Q}(\sqrt{2}) \quad , \\ L^{\langle \sigma_{\bar{1},\bar{0}} \rangle} & = & \mathbb{Q}(\sqrt{3}) & , & L^{\langle \sigma_{\bar{1},\bar{1}} \rangle} & = & \mathbb{Q}(\sqrt{6}) \quad , \\ L^{G(L/K)} & = & K = \mathbb{Q} \quad . & & & & \end{array}$$

Damit ist die Körpererweiterung L/K nach Definition 3.3.5 galoissch. Die Zuordnungen zwischen Untergruppen von $G(L/K)$ und den Zwischenkörpern $L/Z/K$ lassen sich durch die folgenden Diagramme illustrieren:

$$
\begin{array}{ccccc}
\{\mathrm{id}\} & & & & L \\
\| & & & & \| \\
\langle \sigma_{\bar{0},\bar{0}} \rangle & & & & \mathbb{Q}(\sqrt{2},\sqrt{3}) \\
/ \quad | \quad \backslash & & U \longrightarrow L^U & & / \quad | \quad \backslash \\
\langle \sigma_{\bar{0},\bar{1}} \rangle \quad \langle \sigma_{\bar{1},\bar{0}} \rangle \quad \langle \sigma_{\bar{1},\bar{1}} \rangle & & & & \mathbb{Q}(\sqrt{2}) \quad \mathbb{Q}(\sqrt{3}) \quad \mathbb{Q}(\sqrt{6}) \\
\backslash \quad | \quad / & & G(L/Z) \longleftarrow Z & & \backslash \quad | \quad / \\
G(L/K) & & & & \mathbb{Q} \\
\| & & & & \| \\
G & & & & K
\end{array}
$$

Nach dem Hauptsatz der Galoistheorie (Satz 3.3.3) enthält das rechte Diagramm sämtliche Zwischenkörper von L/K. Man beachte, dass die Enthaltenseinsbeziehungen in den beiden Diagrammen entgegengesetzt sind.

BEISPIEL 3.3.6
Es sei $K = \mathbb{Q}$ und $L = \mathbb{Q}(\sqrt{2+\sqrt{2}})$. Wir könnten zunächst alle Konjugierten von $\alpha = \sqrt{2+\sqrt{2}}$ durch Anwendung des Spezialfalls Satz 3.3.1 bestimmen. Eine andere Methode ist jedoch etwas übersichtlicher. Wir schreiben $L = K(\alpha_1, \alpha_2)$ mit $\alpha_1 = \sqrt{2}$ und $\alpha_2 = \sqrt{2+\sqrt{2}}$. Die Isomorphismen von $K(\alpha_1) = \mathbb{Q}(\sqrt{2})$ sind $\sigma_0 = \mathrm{id}_{\mathbb{Q}(\sqrt{2})}$ und $\sigma_1 : \sqrt{2} \mapsto -\sqrt{2}$.

Fortsetzungen von σ_0:
Falls das Polynom $g(X) = X^2 - (2+\sqrt{2})$ irreduzibel in $\mathbb{Q}(\sqrt{2})[X]$ ist, so ist $m_{\mathbb{Q}(\sqrt{2})}(\alpha_2, X) = g(X)$. Wir werden die Irreduzibilität von g später beweisen. Die Nullstellen von $g^{(\sigma_0)}(Y) = Y^2 - (2+\sqrt{2})$ in L sind $\beta_{0,0} = \sqrt{2+\sqrt{2}}$ und $\beta_{0,1} = -\sqrt{2+\sqrt{2}}$. Damit lassen sich die Fortsetzungen von σ_0 beschreiben durch

$$
\begin{array}{rcl}
\mathrm{id}_L & = & \sigma_{0,0} : \sqrt{2} \mapsto \sqrt{2} \;,\; \sqrt{2+\sqrt{2}} \mapsto \sqrt{2+\sqrt{2}} \;, \\
 & & \sigma_{0,1} : \sqrt{2} \mapsto \sqrt{2} \;,\; \sqrt{2+\sqrt{2}} \mapsto -\sqrt{2+\sqrt{2}} \;.
\end{array}
$$

Fortsetzungen von σ_1:
Es ist $g^{(\sigma_1)}(Y) = Y^2 - \sigma_1(2+\sqrt{2}) = Y^2 - (2-\sqrt{2})$ mit den Nullstellen $\beta_{1,0} = \sqrt{2-\sqrt{2}} = \sqrt{2} \cdot \beta_{0,0}^{-1} \in L$ und $\beta_{1,1} = -\sqrt{2-\sqrt{2}} = -\beta_{1,0} \in L$. Damit lassen sich die zugehörigen Fortsetzungen beschreiben durch

$$
\begin{array}{rcl}
\sigma_{1,0} : \sqrt{2} \mapsto -\sqrt{2} \;,\; \sqrt{2+\sqrt{2}} \mapsto \sqrt{2-\sqrt{2}} \;, \\
\sigma_{1,1} : \sqrt{2} \mapsto -\sqrt{2} \;,\; \sqrt{2+\sqrt{2}} \mapsto -\sqrt{2-\sqrt{2}} \;.
\end{array}
$$

Es ist zu vermuten, dass $\beta_{0,0}, \beta_{0,1}, \beta_{1,0}$ und $\beta_{1,1}$ die Konjugierten von $\alpha_2 = \sqrt{2+\sqrt{2}}$ über $\mathbb{Q}$ sind. Wir zeigen dies, indem wir das Polynom $h(X) = (X-\beta_{0,0})(X-\beta_{0,1})(X-\beta_{1,0})(X-\beta_{1,1})$ berechnen. Es ist $h(X) = (X^2-(2+\sqrt{2}))(X^2-(2-\sqrt{2})) = X^4-4X^2+2$, das nach dem Eisensteinkriterium irreduzibel in $\mathbb{Q}[X]$ ist. Damit ist h das Minimalpolynom von $\beta_{0,0}, \beta_{0,1}, \beta_{1,0}, \beta_{1,1}$ über $\mathbb{Q}$, die somit alle den Grad 4 über $\mathbb{Q}$ besitzen und daher nicht in $\mathbb{Q}(\sqrt{2})$ liegen können. Damit ist g auch das Minimalpolynom von $\beta_{0,0}$ und $\beta_{0,1}$ sowie $g^{(\sigma_1)}$ von $\beta_{1,0}$ und $\beta_{1,1}$ über $\mathbb{Q}(\sqrt{2})$. Also ist $G(L/K) = \{\sigma_{0,0}, \sigma_{0,1}, \sigma_{1,0}, \sigma_{1,1}\}$. Wir bestimmen die Gruppenstruktur von $G(L/K)$, indem wir geeignete Potenzen der Elemente $\sigma_{r,s}$ berechnen.

Bestimmung von $\sigma_{0,1}^2$:

Es ist $\sigma_{0,1}^2(\sqrt{2}) = \sigma_{0,1}(\sigma_{0,1}(\sqrt{2})) = \sqrt{2}$. Andererseits ist $\sigma_{0,1}^2(\sqrt{2+\sqrt{2}}) = \sigma_{0,1}(\sigma_{0,1}(\sqrt{2+\sqrt{2}})) = \sigma_{0,1}(-\sqrt{2+\sqrt{2}}) = \sigma_{0,1}(-1)\sigma_{0,1}(\sqrt{2+\sqrt{2}}) = \sqrt{2+\sqrt{2}}$. Also ist $\sigma_{0,1}^2 = \sigma_{0,0} = \mathrm{id}_L$ und $\langle\sigma_{0,1}\rangle = \{\sigma_{0,0}, \sigma_{0,1}\}$.

Bestimmung von $\sigma_{1,0}^2$:

Es ist $\sigma_{1,0}^2(\sqrt{2}) = \sigma_{1,0}(\sigma_{1,0}(\sqrt{2})) = \sigma_{1,0}(-\sqrt{2}) = \sigma_{1,0}(-1)\sigma_{1,0}(\sqrt{2}) = \sqrt{2}$. Andererseits ist $\sigma_{1,0}^2(\sqrt{2+\sqrt{2}}) = \sigma_{1,0}(\sigma_{1,0}(\sqrt{2+\sqrt{2}}) = \sigma_{1,0}(\sqrt{2-\sqrt{2}})$. Es gilt $\sqrt{2+\sqrt{2}} \cdot \sqrt{2-\sqrt{2}} = \sqrt{2}$, also ist $\sqrt{2-\sqrt{2}} = \sqrt{2}(\sqrt{2+\sqrt{2}})^{-1}$, und damit $\sigma_{1,0}(\sqrt{2-\sqrt{2}}) = \sigma_{1,0}(\sqrt{2})(\sigma_{1,0}(\sqrt{2+\sqrt{2}}))^{-1} = -\sqrt{2}(\sqrt{2-\sqrt{2}})^{-1} = -\sqrt{2+\sqrt{2}}$. Damit ist $\sigma_{1,0}^2 = \sigma_{0,1}$, also $|\langle\sigma_{1,0}\rangle| = 4$.

Es folgt $G(L/K) = \{\sigma_{1,0}^0, \sigma_{1,0}^1, \sigma_{1,0}^2, \sigma_{1,0}^3\} = \langle\sigma_{1,0}\rangle \cong \mathbb{Z}/4\mathbb{Z}$. Darin liegen die Untergruppen $\langle\sigma_{1,0}^0\rangle = \{\mathrm{id}_L\}$, $\langle\sigma_{1,0}^2\rangle = \{\sigma_{0,0}, \sigma_{0,1}\}$ und $G(L/K)$ selbst. Wir bestimmen die Fixkörper dieser Untergruppen: Nach den Sätzen 3.2.1 und 3.2.2 ist $L = \{b_0 + b_1\sqrt{2} + b_2\sqrt{2+\sqrt{2}} + b_3\sqrt{2}\sqrt{2-\sqrt{2}} \mid b_i \in \mathbb{Q}\}$ und damit $\sigma_{1,0}^2(z) = b_0 + b_1\sqrt{2} - b_2\sqrt{2+\sqrt{2}} - b_3\sqrt{2}\sqrt{2+\sqrt{2}}$. Also $\sigma_{0,1}^2(z) = z \Leftrightarrow z \in \mathbb{Q}(\sqrt{2})$, bzw. $L^{\langle\sigma_{1,0}^2\rangle} = \mathbb{Q}(\sqrt{2})$. Weiter gilt $z \in \mathbb{Q}(\sqrt{2}),\ \sigma_{1,0}(z) = z \Leftrightarrow z \in \mathbb{Q}$. Also ist $L^{G(L/K)} = K = \mathbb{Q}$, und nach Definition 3.3.5 ist L/K galoissch. Natürlich ist $L^{\langle\sigma_{0,0}\rangle} = L$. Wir erhalten das folgende Diagramm für Untergruppen und Zwischenkörper:

$$
\begin{array}{ccccc}
\{\mathrm{id}\} & & & & L \\
\| & & & & \| \\
\langle\sigma_{\bar{0},\bar{0}}\rangle & & & & \mathbb{Q}(\sqrt{2+\sqrt{2}}) \\
| & & U & \longrightarrow & L^U \quad | \\
\left\langle\sigma_{\bar{1},\bar{0}}^2\right\rangle & & & & \mathbb{Q}(\sqrt{2}) \\
| & & G(L/Z) & \longleftarrow & Z \quad | \\
G(L/K) & & & & \mathbb{Q} \\
\| & & & & \| \\
G & & & & K
\end{array}
$$

Wiederum enthält das rechte Diagramm sämtliche Zwischenkörper von L/K.

BEISPIEL 3.3.7
Es sei $K = \mathbb{Q}$ und $L = \mathbb{Q}(\sqrt[8]{3}, i)$. Wir finden zunächst die Isomorphismen von $\mathbb{Q}(\sqrt[8]{3})$ mit Bildern in L. Es ist $g_1(X) = m_{\mathbb{Q}}(\sqrt[8]{3}, X) = X^8 - 3$ nach dem Eisensteinkriterium irreduzibel. Von den acht Nullstellen, die g_1 in $\mathbb{C}$ besitzt, liegen nur 4 in L, nämlich $\beta_0 = \sqrt[8]{3}$, $\beta_1 = i \cdot \sqrt[8]{3}$, $\beta_2 = -\sqrt[8]{3}$ und $\beta_3 = -i \cdot \sqrt[8]{3}$. Also ist

$$\{\beta_0, \beta_1, \beta_2, \beta_3\} \;=\; \{\sqrt[8]{3} \cdot i^k \mid k \in \mathbb{Z}\}$$

(Übungsaufgabe). Im Gegensatz zu den Beispielen 3.3.5 und 3.3.6 zerfällt also das Minimalpolynom $m_{\mathbb{Q}}(\sqrt[8]{3}, X)$ nicht vollständig in Linearfaktoren. Wir werden in den nächsten Abschnitten sehen, dass schon aus dieser Tatsache folgt, dass die Erweiterung L/K nicht galoissch sein kann. Nach Satz 3.3.2 haben wir vier Isomorphismen, die wir in Analogie zu Beispiel 3.3.5 mittels Restklassen indizieren wollen, diesmal mit Elementen aus $\mathbb{Z}/4\mathbb{Z}$, da der Wert von $\beta = \sqrt[8]{3} \cdot i^k$ nur von der Restklasse von k modulo 4 abhängt. Wir haben also die vier Isomorphismen

$$\sigma_s : \; \sqrt[8]{3} \mapsto \sqrt[8]{3} \cdot i^k \;\; (s \in \mathbb{Z}/4\mathbb{Z} \;,\; k \in s)$$

von L. $\sigma_{\bar{0}}$ und $\sigma_{\bar{2}}$ sind Isomorphismen mit Bild $\mathbb{Q}(\sqrt[8]{3})$, während $\sigma_{\bar{1}}$ und $\sigma_{\bar{3}}$ das Bild $L = \mathbb{Q}(\sqrt[8]{3}, i)$ besitzen. Das Element i ist Nullstelle von $g_2(X) = X^2 + 1$, und offenbar ist $i \notin \mathbb{Q}(\sqrt[8]{3})$ wegen $i \notin \mathbb{R}$. Also ist $m_{\mathbb{Q}(\sqrt[8]{3})}(i, X) = X^2 + 1$. Damit ist nach dem Gradsatz

$$[\mathbb{Q}(\sqrt[8]{3}, i) : \mathbb{Q}] \;=\; [\mathbb{Q}(\sqrt[8]{3}, i) : \mathbb{Q}(\sqrt[8]{3})] \cdot [\mathbb{Q}(\sqrt[8]{3}) : \mathbb{Q}] \;=\; 16\,.$$

Wäre $i \in \mathbb{Q}(i \cdot \sqrt[8]{3})$, so wäre $\mathbb{Q}(i \cdot \sqrt[8]{3}) = \mathbb{Q}(\sqrt[8]{3}, i)$, also $[\mathbb{Q}(i \cdot \sqrt[8]{3}) : \mathbb{Q}] = 16$, während nach Satz 3.3.2 $[\mathbb{Q}(i \cdot \sqrt[8]{3}) : \mathbb{Q}] = 8$ ist. Also ist $g_2(X) = X^2 + 1$ auch das Minimalpolynom von i über $\mathbb{Q}(\sqrt[8]{3})$. Jeder der vier Isomorphismen σ_s hat damit zwei Fortsetzungen

$$\sigma_{r,s} : \; \sqrt[8]{3} \mapsto \sqrt[8]{3} \cdot i^k \;,\; i \mapsto i^l \qquad r \in (\mathbb{Z}/4\mathbb{Z})^*,\; s \in \mathbb{Z}/4\mathbb{Z},\; l \in r,\; k \in s\,.$$

Wir berechnen die Struktur der Automorphismengruppe $G(L/K)$. Es seien $l_j \in r_j$ und $k_j \in s_j$. Dann ist $(\sigma_{r_1,s_1} \circ \sigma_{r_2,s_2})(\sqrt[8]{3}) = \sigma_{r_1,s_1}(\sqrt[8]{3} \cdot i^{k_2}) = \sigma_{r_1,s_1}(\sqrt[8]{3})\sigma_{r_1,s_1}(i^{k_2}) = \sqrt[8]{3} \cdot i^{(l_1 k_2 + k_1)}$. Andererseits ist $(\sigma_{r_1,s_1} \circ \sigma_{r_2,s_2})(i) = \sigma_{r_1,s_1}(i^{l_2}) = i^{(l_1 l_2)}$. Also gilt

$$(*) : \;\; \sigma_{r_1,s_1} \circ \sigma_{r_2,s_2} \;=\; \sigma_{r_1 r_2, r_1 s_2 + s_1}\,.$$

Die Beschreibung lässt sich vereinfachen, wenn wir Matrizen einführen: $\sigma_{r_1,s_1} \circ \sigma_{r_2,s_2} = \sigma_{r_3,s_3}$, wobei das Paar (r_3, s_3) bestimmt ist durch

$$\begin{pmatrix} r_1 & s_1 \\ \bar{0} & \bar{1} \end{pmatrix} \cdot \begin{pmatrix} r_2 & s_2 \\ \bar{0} & \bar{1} \end{pmatrix} \;=\; \begin{pmatrix} r_3 & s_3 \\ \bar{0} & \bar{1} \end{pmatrix}\,.$$

Die Gruppe $G(L/K)$ ist somit isomorph zur Matrizengruppe

$$M_4 \;=\; \left\{ \begin{pmatrix} r & s \\ \bar{0} & \bar{1} \end{pmatrix} \mid r \in (\mathbb{Z}\,/\,4\mathbb{Z})^* \;,\; s \in \mathbb{Z}\,/\,4\mathbb{Z} \right\}$$

bzgl. der Matrizenmultiplikation. Diese Gruppe besitzt den zyklischen Normalteiler

$$N_4 \;=\; \left\{ \begin{pmatrix} \bar{1} & s \\ \bar{0} & \bar{1} \end{pmatrix} \mid s \in \mathbb{Z}\,/\,4\mathbb{Z} \right\}$$

der Ordnung 4, sowie eine Untergruppe der Ordnung 2

$$U_2 \;=\; \left\{ \begin{pmatrix} \bar{1} & \bar{0} \\ \bar{0} & \bar{1} \end{pmatrix} \;,\; \begin{pmatrix} -\bar{1} & \bar{0} \\ \bar{0} & \bar{1} \end{pmatrix} \;,\; \right\}\,.$$

Die Gruppe M_4 ist nicht abelsch. Nach Satz 1.7.10 ist M_4 das innere semidirekte Produkt von N_4 und U_2:

$$M_4 \cong (\mathbb{Z}\,/\,4\mathbb{Z}) \times_\Phi (\mathbb{Z}\,/\,2\mathbb{Z})$$

mit einem Homomorphismus $\Phi : \mathbb{Z}/4\mathbb{Z} \to \mathrm{Aut}(\mathbb{Z}/4\mathbb{Z})$. Da es genau einen von der Identität verschiedenen Automorphismus von N_4 gibt, ist Φ eindeutig bestimmt. Wie man leicht nachrechnet, ist auch die Symmetriegruppe des Quadrats, die Diedergruppe D_4, von diesem Isomorphietyp. Also folgt $G(L/K) \cong D_4$. Wir wollen den „Verband" der Untergruppen von $G(L/K)$ bestimmen. Der Normalteiler $\langle\sigma_{\bar{1},\bar{1}}\rangle$ der Ordnung 4 besitzt die zyklischen Untergruppen $\langle\sigma_{\bar{1},\bar{0}}\rangle$, $\langle\sigma_{\bar{1},\bar{2}}\rangle$ bzw. $\langle\sigma_{\bar{1},\bar{1}}\rangle$ der Ordnungen 1, 2 bzw. 4. Das Zentrum von $G(L/K)$ ist $Z(G(L/K)) = \{\sigma_{\bar{1},\bar{0}}, \sigma_{\bar{1},\bar{2}}\}$. Die Konjugierten von $\sigma_{-\bar{1},\bar{0}}$ erzeugen jeweils Untergruppen der Ordnung 2: $\langle\sigma_{-\bar{1},\bar{0}}\rangle$, $\langle\sigma_{-\bar{1},\bar{2}}\rangle$, $\langle\sigma_{-\bar{1},\bar{1}}\rangle$ und $\langle\sigma_{-\bar{1},-\bar{1}}\rangle$. Ist $M_t = \{\sigma_{-\bar{1},t}, \sigma_{\bar{1},t}\}$ mit $t \in \{\bar{1},\bar{3}\}$, so ist $\langle M_t\rangle = G(L/K)$. Für $t = \bar{2}$ ist hingegen $|\langle M_t\rangle| = 4$. Man rechnet leicht nach, dass

$$L^{G(L/K)} = \mathbb{Q}(\sqrt{3}) \neq K$$

gilt. Somit ist L/K nicht galoissch, vgl. auch die zugehörigen Übungsaufgaben.

3.4. Zerfällungskörper und normale Erweiterungen

Wir wollen im Folgenden ein Kriterium dafür erhalten, dass eine Körpererweiterung galoissch ist. Es lautet: Eine Körpererweiterung L/K ist galoissch genau dann, wenn sie endlich, normal und separabel ist. Die Bedeutung des ersten Begriffs ist schon bekannt. In diesem und dem nächsten Abschnitt sollen die beiden anderen eingeführt werden. Eng mit dem Konzept der Normalität ist das des Zerfällungskörpers verbunden:

DEFINITION 3.4.1
Es sei K ein Körper und $f \in K[X]$ mit $\deg(f) \geq 1$. Eine algebraische Erweiterung L von K heißt Zerfällungskörper von f über K, wenn $L = K(\alpha_1, \ldots, \alpha_n)$ und $f = c\cdot(X-\alpha_1)\cdots(X-\alpha_n)$ mit $c \in K$ gilt.

BEMERKUNG 3.4.1
Man beachte, dass f nicht irreduzibel zu sein braucht.

BEISPIEL 3.4.1
Die Körper aus den Beispielen 3.3.5 und 3.3.6 sind Zerfällungskörper von Polynomen über $\mathbb{Q}$. $L_1 = \mathbb{Q}(\sqrt{2},\sqrt{3})$ ist Zerfällungskörper von $f_1(X) = (X^2-2)(X^2-3)$ über $\mathbb{Q}$, denn es ist $f_1(X) = (X-\sqrt{2})(X-(-\sqrt{2}))(X-\sqrt{3})(X-(-\sqrt{3}))$ in $L_1[X]$, und $L_1 = \mathbb{Q}(\sqrt{2},-\sqrt{2},\sqrt{3},-\sqrt{3})$. Der Körper $L_2 = \mathbb{Q}(\sqrt{2+\sqrt{2}})$ ist Zerfällungskörper von $f_2(X) = X^4 - 4X^2 + 2$ über $\mathbb{Q}$, denn mit $\beta_{0,0} = \sqrt{2+\sqrt{2}}$ gilt $f_2(X) = (X-\beta_{0,0})(X-(-\beta_{0,0}))(X-\sqrt{2}\beta_{0,0}^{-1})(X-(-\sqrt{2}\beta_{0,0}^{-1}))$ und $L_2 = \mathbb{Q}(\beta_{0,0}, -\beta_{0,0}, \sqrt{2}\beta_{0,0}^{-1}, -\sqrt{2}\beta_{0,0}^{-1})$.

BEISPIEL 3.4.2
Der Körper $\mathbb{C}$ ist Zerfällungskörper von X^2+1 über $\mathbb{R}$, da $X^2+1 = (X-i)(X-(-i))$ und $\mathbb{C} = \mathbb{R}(i,-i)$ ist.

Folgender Satz ist trivial:

SATZ 3.4.1
Es sei K ein Körper und $f \in K[X]$, sowie M ein Zerfällungskörper von f über K und Z ein Zwischenkörper (d. h. $M/Z/K$). Dann ist M auch ein Zerfällungskörper von f über Z.

Wir werden im Folgenden eine Aussage über Existenz und Eindeutigkeit von Zerfällungskörpern beweisen. In Beispiel 3.4.1 wurden die Zerfällungskörper L_1 und L_2 als Unterkörper von vorgegebenen großen Oberkörpern ($\mathbb{R}$ oder $\mathbb{C}$) erhalten, die mit Hilfsmitteln der Analysis (Cauchyfolgen) aus dem Körper $\mathbb{Q}$ konstruiert werden können. Im Folgenden werden diese Zerfällungskörper mit rein algebraischen Hilfsmitteln konstruiert werden. In einem ersten Schritt konstruieren wir zu einem vorgegebenen Körper K und Polynom $f \in K[X]$ eine Körpererweiterung L/K, in der f mindestens eine Nullstelle besitzt.

SATZ 3.4.2
Es sei $g \in K[X]$ normiert und irreduzibel. Dann existiert eine einfache algebraische Erweiterung L/K mit $\alpha \in L$ und $m_K(\alpha, X) = g(X)$.

BEWEIS
Satz 3.2.2 b) legt es nahe, den Restklassenring $\overline{L} = K[X]/(g)$ zu betrachten. Nach Satz 2.4.4 c) ist (g) maximales Ideal, damit ist $\overline{L}$ nach Satz 2.1.4 b) ein Körper. Wir setzen $\alpha = X + (g) \in \overline{L}$. Der Körper $\overline{L}$ enthält den zu K isomorphen Unterkörper $\overline{K} := \{z + (g) \mid z \in K\}$. Es sei $L = (\overline{L} - \overline{K}) \cup K$ und

$$\Phi := \begin{cases} z + (g) & \mapsto \quad z \quad \text{falls} \quad z + (g) \in \overline{K} \\ z & \mapsto \quad z \quad \text{falls} \quad z \in \overline{L} - \overline{K} \end{cases}$$

Wir definieren Addition und Multiplikation auf L durch

$$\Phi(z_1) + \Phi(z_2) \;=\; \Phi(z_1 + z_2)\;,\;\; \Phi(z_1) \cdot \Phi(z_2) \;=\; \Phi(z_1 \cdot z_2)\,.$$

Dann ist $g(\alpha) = 0$, und L ist von der gewünschten Art. □

Der folgende Satz macht Aussagen über Existenz und Eindeutigkeit von Zerfällungskörpern.

SATZ 3.4.3
Es sei K ein Körper und $f \in K[X]$. Dann gibt es einen Zerfällungskörper L von f über K. Es sei $f(X) = c \cdot (X - \alpha_1) \cdots (X - \alpha_n)$ mit $c \in K$ und $\alpha_1, \ldots, \alpha_n \in L$. Ist $\overline{L}$ irgend ein Zerfällungskörper von f über K, so gibt es einen K-Isomorphismus $\sigma : L \to \overline{L}$, so dass $f(X) = c \cdot (X - \sigma(\alpha_1)) \cdots (X - \sigma(\alpha_n))$ in $\overline{L}[X]$ ist. Insbesondere sind Zerfällungskörper von f über K stets K-isomorph.

BEWEIS
Existenz:
Wir beweisen die Existenz eines Zerfällungskörpers L von f über K durch Induktion nach dem Grad $n = \deg(f)$.

$n = 1$:
$f(X) = a_1 X + a_0$ mit $a_1 \neq 0$, also $f(X) = a_1 \cdot (X - (-a_0 a_1^{-1})$, d. h. K ist schon selbst Zerfällungskörper.

$n - 1 \to n$:
Es sei $f \in K[X]$ mit $\deg(f) = n$. Dann gibt es nach Satz 3.4.2 eine Körpererweiterung $K(\alpha_1)$ mit $m_K(\alpha_1, X) = f(X)$. Es ist $f(X) = c \cdot (X - \alpha_1) \cdot h(X)$ mit $c \in K$ für ein $h \in K(\alpha_1)[X]$ normiert und irreduzibel, sowie $\deg(h) = n - 1$. Nach Induktionshypothese gibt es eine algebraische Erweiterung $L = K(\alpha_1, \ldots, \alpha_n)$ von $K(\alpha_1)$, so dass $h(X) = (X - \alpha_2) \cdots (X - \alpha_n)$ in $L[X]$ gilt. Also ist L Zerfällungskörper von f über K.

Eindeutigkeit: Die Eindeutigkeit bis auf K-Isomorphie ist ein Spezialfall des folgenden allgemeinen Satzes. □

SATZ 3.4.4
Es seien K und $\overline{K}$ Körper, X und Y Unbestimmte über K bzw. $\overline{K}$, und $\sigma : K \to \overline{K}$ ein Körperisomorphismus. Für $f(X) = a_n X^n + \cdots + a_0 \in K[X]$ sei $f^{(\sigma)}(Y) = \sigma(a_n)Y^n + \cdots + \sigma(a_0)$ gesetzt. Es sei L ein Zerfällungskörper von f über K mit $f(X) = c \cdot (X - \alpha_1) \cdots (X - \alpha_n)$, $c \in K$, $\alpha_1, \ldots, \alpha_n \in L$. Ferner sei $\overline{L}$ ein Zerfällungskörper von $f^{(\sigma)}$ über $\overline{K}$. Dann gibt es einen Isomorphismus $\tau : L \to \overline{L}$, der σ fortsetzt, mit $f^{(\sigma)} = \sigma(c) \cdot (Y - \tau(\alpha_1)) \cdots (Y - \tau(\alpha_m))$.

BEWEIS
Wir beweisen die Behauptung durch Induktion nach $n = \deg(f)$:

$n = 1$:
Es gilt $f(X) = c \cdot (X - \alpha_1)$ mit $c, \alpha \in K$ und $f^{(\sigma)}(Y) = \sigma(c) \cdot (Y - \tau(\alpha_1))$. Die Behauptung gilt dann wegen $L = K$, $\overline{L} = \overline{K}$, wenn $\tau = \sigma$ gesetzt wird.

$n - 1 \to n$:
Die Behauptung sei schon für alle Grade $\leq n - 1$ gezeigt. Es sei $n = \deg(f)$ und es gelte $f(X) = c \cdot g_1(X) \cdots g_l(X)$ mit $c \in K$ und irreduziblen normierten $g_j \in K[X]$ für $1 \leq j \leq l$. Es sei α eine Nullstelle in L von $g_1(X)$. Damit gilt in $K(\alpha)[X]$:

$$f(X) \;=\; c \cdot (X - \alpha)h(X) \cdot g_2(X) \cdots g_l(X) \;=\; (X - \alpha) \cdot k(X)$$

für ein $k \in K(\alpha)[X]$. Es sei β eine Nullstelle von $g_1^{(\sigma)}(Y)$ in $\overline{K}$. Dann gibt es nach Satz 3.3.2 einen Isomorphismus $\psi : K(\alpha) \to \overline{K}(\beta)$ mit $\psi(\alpha) = \beta$, der σ fortsetzt. Es gilt

$$f^{(\sigma)}(Y) \;=\; \sigma(c) \cdot (Y - \beta)h^{(\psi)}(Y) \cdot g_2^{(\psi)}(Y) \cdots g_l^{(\psi)}(Y) \;=\; (Y - \beta) \cdot k^{(\psi)}(Y)\,.$$

Nun ist L Zerfällungskörper von k über $K(\alpha)$ und $\overline{L}$ Zerfällungskörper von $k^{(\psi)}$ über $\overline{K}$. Nach Induktionshypothese (mit $\deg(k) = n - 1$) kann ψ zu einem Isomorphismus τ von L nach $\overline{L}$ fortgesetzt werden, so dass die gewünschten Eigenschaften gelten. □

DEFINITION 3.4.2
Es sei f ein nicht konstantes Polynom aus $K[X]$.

(a) Man hat alle Nullstellen von f zu K adjungiert, wenn man einen Zerfällungskörper von f über K betrachtet.
(b) Man hat eine Nullstelle von f zu K adjungiert, wenn man eine einfache Erweiterung $K(\alpha)$ von K mit $f(\alpha) = 0$ betrachtet.
(c) Ist α algebraisch über K, so heißt $\alpha_1, \ldots, \alpha_n$ ein volles System von Konjugierten zu α über K, wenn $\alpha_1 = \alpha$ ist und es eine Erweiterung L/K mit $\alpha_1, \ldots, \alpha_n \in L$ und $m_K(\alpha, X) = (X - \alpha_1) \cdots (X - \alpha_n)$ gibt.

DEFINITION 3.4.3
Ein Körper L heißt normal über K (oder eine normale Erweiterung von K), wenn L eine algebraische Erweiterung von K ist, und jedes irreduzible Polynom aus $K[X]$, das in L mindestens eine Nullstelle besitzt, in lauter Linearfaktoren aus $L[X]$ zerfällt.

BEISPIEL 3.4.3
Die Erweiterung $L = \mathbb{Q}(\sqrt[4]{2})$ ist nicht normal über $\mathbb{Q}$, denn $f(x) = X^4 - 2$ ist irreduzibel in $\mathbb{Q}[X]$, hat in $\mathbb{Q}(\sqrt[4]{2})$ eine Nullstelle $\alpha = \sqrt[4]{2}$, zerfällt jedoch nicht in Linearfaktoren aus $L[X]$, da die Nullstelle $\sqrt[4]{2} \cdot i \in \mathbb{C}$ nicht in L liegt.

Der folgende Satz sagt aus, dass endliche normale Erweiterungen und Zerfällungskörper ein und dasselbe sind:

SATZ 3.4.5
Genau dann ist ein Körper L eine normale und endliche Erweiterung von K, wenn L ein Zerfällungskörper eines Polynoms aus $K[X]$ über K ist.

BEWEIS
$\Rightarrow$: Es sei L eine normale und endliche Erweiterung von K. Dann ist $L = K(\alpha_1, \ldots, \alpha_n)$ für endlich viele $\alpha_1, \ldots, \alpha_n \in L$. Es sei $f(X) = m_K(\alpha_1, X) \cdots m_K(\alpha_n, X)$. Da jeder Faktor $m_K(\alpha_j, X)$ in Linearfaktoren aus $L[X]$ zerfällt, ist L ein Zerfällungskörper von f über K. $\Leftarrow$: Es sei L Zerfällungskörper eines Polynoms $f \in K[X]$ über K, etwa mit Zerfall

$$f(X) \;=\; c \cdot (X - \alpha_1) \cdots (X - \alpha_n)$$

in Linearfaktoren in $L[X]$, und $L = K(\alpha_1, \ldots, \alpha_n)$. Es sei $g \in L[X]$ normiert und irreduzibel mit $g(\beta) = 0$ für ein $\beta \in L$. Es ist zu zeigen, dass g in $L[X]$ in Linearfaktoren zerfällt. Dazu sei Z ein Zerfällungskörper von g über L. Ist $\overline{\beta}$ irgend eine Nullstelle von g in Z, so bleibt $\overline{\beta} \in L$ zu zeigen. Wegen $g(X) = m_K(\beta, X) = m_K(\overline{\beta}, X)$ gibt es nach Satz 3.3.1 einen K-Isomorphismus $\sigma : K(\beta) \to K(\overline{\beta})$ mit $\sigma(\beta) = \overline{\beta}$. Da $L = L(\beta)$ ein Zerfällungskörper von f auch über $K(\beta)$ und $L(\overline{\beta})$ ein Zerfällungskörper von f über $K(\overline{\beta})$ ist, existiert nach Satz 3.4.4 ein Isomorphismus $\tau : L \to L(\overline{\beta})$, der σ fortsetzt. Wegen $0 = \tau(f(\alpha_j)) = f(\tau(\alpha_j))$ bilden die Elemente $\tau(\alpha_1), \ldots, \tau(\alpha_n)$ eine Permutation von $\alpha_1, \ldots, \alpha_n$. Für $\beta \in K(\alpha_1, \ldots, \alpha_n)$ gilt dann

$$\beta \;=\; p(\alpha_1, \ldots, \alpha_n)$$

mit $p \in K[X_1, \ldots, X_n]$. Daraus folgt

$$\overline{\beta} \;=\; p(\tau(\alpha_1), \ldots, \tau(\alpha_n)) \;\in\; K(\alpha_1, \ldots, \alpha_n) \;=\; L\,.$$

□

SATZ 3.4.6
Ist ein Körper L normal über K, so ist L normal über Z für jeden Zwischenkörper $L/Z/K$.

BEWEIS
Es sei g ein irreduzibles und normiertes Polynom aus $Z[X]$ und $g(\alpha) = 0$ für ein $\alpha \in L$. Es gilt $g(X) = m_Z(\alpha, X) \;\Rightarrow\; g(X) \mid m_K(\alpha, X)$ (Teilbarkeitsrelation in $Z[X]$). Da $m_K(\alpha, X)$ in $L[X]$ in Linearfakoren zerfällt, gilt das auch für den Teiler $g(X)$. □

3.5. Separabilität

DEFINITION 3.5.1
Es sei L/K eine Körpererweiterung. $\alpha \in L$ heißt r-fache Nullstelle eines Polynoms $f \in K[X]$ ($r \in \mathbb{N}_0$), falls $(X - \alpha)^r \mid f(X)$ und $(X - \alpha)^{r+1} \nmid f(X)$ in $L[X]$ gilt.

DEFINITION 3.5.2
Es sei f ein nicht konstantes Polynom aus $K[X]$ und L ein Zerfällungskörper von f über K.

(a) f heißt separabel, wenn f nur einfache Nullstellen in L besitzt. Andernfalls heißt f inseparabel.
(b) Die Anzahl der verschiedenen Nullstellen von f in L wird der reduzierte Grad von f genannt.

Ein wichtiges Kriterium für die Separabilität eines Polynoms f kann mittels dessen Ableitung f' gewonnen werden.

DEFINITION 3.5.3
Es sei

$$f(X) \;=\; \sum_{j=0}^{n} a_j X^j \;\in\; K[X]$$

beliebig. Unter der Ableitung f' von f versteht man das Polynom

$$f'(X) \;=\; \sum_{j=1}^{n} j \cdot a_j X^{j-1} \;\in\; K[X]\,,$$

wobei j innerhalb der Summe als Abkürzung für $\Phi(j)$ mit dem Ringhomomorphismus $\Phi : \mathbb{Z} \to K$ aus Satz 3.1.1 zu verstehen ist. Man beweist leicht die Gültigkeit der Produktregel:

$$(fg)' \;=\; f'g + fg'\,.$$

SATZ 3.5.1
Es sei f ein nicht konstantes Polynom aus $K[X]$. f ist separabel genau dann, wenn f und f' in $K[X]$ teilerfremd sind.

BEWEIS
$\Rightarrow$: Es sei α eine mehrfache Nullstelle von f in L. Dann gilt: $f(X) = (X-\alpha)^2 \cdot g(X)$ für ein $g \in L[X]$. Nach der Produktregel ist

$$f'(X) \;=\; 2(X-\alpha)\cdot g(X) + (X-\alpha)^2 \cdot g'(X)\,,$$

also gilt $(X-\alpha) \mid f(X)$ und $(X-\alpha) \mid f'(X)$ in $L[X]$. Wären f und f' teilerfremd in $K[X]$, so folgte $(X-\alpha) \mid 1$ in $L[X]$, ein Widerspruch. $\Leftarrow$: Es sei $f(X) = c \cdot (X-\alpha_1)\cdots(X-\alpha_n)$ mit $c \in K$, $\alpha_j \in L$ und alle a_j paarweise verschieden. Angenommen f und f' sind nicht teilerfremd in $K[X]$. Da $L[X]$ faktoriell ist folgt: $g|f$ und $g|f'$ für ein irreduzibles $g \in L[X]$. Weiter folgt $g \mid (X-\alpha_j)$ für genau ein j, ein Widerspruch, da $(X-\alpha_j) \nmid f'$. □

SATZ 3.5.2
Es sei f ein irreduzibles Polynom in $K[X]$ mit $\mathrm{char}(K) = 0$. *Dann ist f separabel.*

BEWEIS
Nach Satz 3.5.2 ist f inseparabel genau dann, wenn f und f' einen nicht konstanten ggT in $K[X]$ besitzen. Wegen der Irreduzibilität von f folgt: $f|f'$ oder $f'(X) = 0$. Ist $f(X) = a_0 + a_1X + \cdots + a_nX^n$ mit $a_n \neq 0$ und $n \geq 1$, so ist $f'(X) = a_1 + 2a_2X + \cdots + n \cdot a_nX^{n-1} \neq 0$, da wegen $\mathrm{char}(K) = 0$ auch $n \neq 0$ gilt für $n \geq 1$. □

BEMERKUNG 3.5.1
Für Körper K mit Primzahlcharakteristik p können irreduzible Polynome inseparabel sein.

DEFINITION 3.5.4
Sei K ein Körper:

(a) Ein über K algebraisches Element α heißt separabel bzw. inseparabel über K, falls $m_K(\alpha, X)$ separabel bzw. inseparabel ist. Der reduzierte Grad von $m_K(\alpha, X)$ wird der reduzierte Grad von α über K genannt.
(b) Eine algebraische Erweiterung L/K heißt separabel (oder separable Erweiterung von K), falls alle $\alpha \in L$ über K separabel sind. Andernfalls heißt L inseparabel über K.

SATZ 3.5.3
Es ist stets K separabel über K. Ist L separabel über K, so ist L separabel über jedem Zwischenkörper $L/Z/K$.

BEWEIS
Ist $\alpha \in K$, so ist $m_K(\alpha, X) = X - \alpha$ offensichtlich separabel. Für $\alpha \in L$ gilt: $m_Z(\alpha, X) \mid m_K(\alpha, X)$ in $Z[X]$. Aus der Separabilität von $m_K(\alpha, X)$ folgt daher die Separabilität von $m_Z(\alpha, X)$. $\square$

Der folgende Satz ist für die Beziehung der Begriffe Normalität und Separabilität zur Galoistheorie von entscheidender Bedeutung:

SATZ 3.5.4
Es sei L/K endlich, $L = K(\alpha_1, \ldots, \alpha_r)$ und m_j der reduzierte Grad von α_j über $K(\alpha_1, \ldots, \alpha_{j-1})$ für $j = 1 \ldots r$. Dann gilt $|G(L/K)| \leq m_1 \cdots m_r$. In dieser Ungleichung steht das Gleichheitszeichen, wenn L über K normal ist. Insbesondere ist stets $|G(L/K)| \leq [L : K]$.

BEWEIS
Schritt 1:
Wir beweisen durch Induktion nach j folgende Behauptung, aus welcher für $j = r$ die erste Behauptung des Satzes folgt: Die Anzahl n_j der K-Isomorphismen von $K(\alpha_1, \ldots, \alpha_j)$ erfüllt $n_j \leq m_1 \cdots m_j$. Der Induktionsanfang $j = 0$ ist klar. Es sei $j > 0$ und die Behauptung für $j - 1$ schon gezeigt, d. h. es gibt n_{j-1} verschiedene K-Isomorphismen $\sigma_1, \ldots, \sigma_{n_{j-1}}$ von $L' = K(\alpha_1, \ldots, \alpha_{j-1})$ in L, wobei $n_{j-1} \leq m_1 \cdots m_{j-1}$ ist. Die K-Isomorphismen von $K(\alpha_1, \ldots, \alpha_j)$ werden nach Satz 3.3.2 aus den Fortsetzungen der σ_i erhalten. Es sei σ eines der σ_i, sowie $g(X) = m_{L'}(\alpha_j, X) = \sum a_k X^k$. und $g^{(\sigma)}(Y) = \sum \sigma(a_k) Y^k$. Nach Satz 3.3.2 sind die Fortsetzungen von σ durch die verschiedenen Nullstellen $\beta_1, \ldots, \beta_m$ von $g^{(\sigma)}(Y)$ in L über $\sigma(\alpha_j) = \beta_l$ charakterisiert. Es gibt also genau m' Fortsetzungen von σ, wobei $m' \leq \overline{m}_j$ ist für den reduzierte Grad $\overline{m}_j$ von $g^{(\sigma)}$. Da nach Satz 3.4.4 σ zu einem Isomorphismus eines Zerfällungskörpers von g über L' und einem Zerfällungskörper von $g^{(\sigma)}$ über $\sigma(L')$ fortgesetzt werden kann, gilt $\overline{m}_j = m_j$. Also folgt $n_j \leq n_{j-1} m_j \leq m_1 \cdots m_j$.

Schritt 2:
Es sei nun zusätzlich vorausgesetzt, dass L normal über K ist. Der Beweis für das Gleichheitszeichen wird wieder durch Induktion über j geführt. Die Induktionshypothese ist somit, dass es genau $m_1 \cdots m_{j-1}$ verschiedene K-Isomorphismen σ von $L' = K(\alpha_1, \ldots, \alpha_{j-1})$ gibt. Es ist zu zeigen, dass es zu jedem σ genau m_j Fortsetzungen zu einem Isomorphismus auf $K(\alpha_1, \ldots, \alpha_j)$ gibt. Dazu genügt es zu zeigen, dass $g^{(\sigma)}(Y)$ in $L[Y]$ vollständig in Linearfaktoren zerfällt. Wegen $g^{(\sigma)}(Y) = m_{L'}(\alpha_j, Y)$ gilt: $h(X) = m_K(\alpha_j, X) = b_0 + b_1 X + \cdots + b_{m-1} X^{m-1} + b_m X^m = g(X) \cdot q(X)$, mit $b_i \in K$ und $g, q \in K(\alpha_1, \ldots, \alpha_{j-1})[X]$. Dann ist $h(X) = \sigma(b_0) + \cdots + \sigma(b_{m-1}) X^{m-1} + X^m = g^{(\sigma)}(X) \cdot q^{(\sigma)}(X)$. Da aber L normal über K ist, zerfällt auch h wegen $h(\alpha_j) = 0$ vollständig in Linearfaktoren in $L[X]$, somit auch $g^{(\sigma)}$. Schließlich ist

$$\begin{aligned} [L : K] &= [K(\alpha_1) : K] \cdot [K(\alpha_1, \alpha_2) : K(\alpha_1)] \cdots [K(\alpha_1, \ldots, \alpha_r) : K(\alpha_1, \ldots, \alpha_{r-1})] \\ &\geq m_1 \cdots m_r \\ &\geq |G(L/K)| \end{aligned}$$

woraus die letzte Behauptung des Satzes folgt. $\square$

SATZ 3.5.5
Es sei L/K endlich, normal und separabel. Dann ist $|G(L/K)| = [L : K]$.

BEWEIS
Im Beweis des vorigen Satzes fallen Grade und reduzierte Grade zusammen, also gilt stets

$$[K(\alpha_1, \ldots, \alpha_j) : K(\alpha_1, \ldots, \alpha_{j-1}] \; = \; m_j$$

und damit $[L : K] = |G(L/K)|$. □

3.6. Charakterisierung von galoisschen Erweiterungen

SATZ 3.6.1
Eine Erweiterung L/K ist galoissch genau dann, wenn sie endlich,normal, und separabel ist.

Wir geben den Beweis nur für eine Richtung:

Es sei L/K endlich, normal und separabel. Es sei $Z = L^{G(L/K)}$ der zur vollen Automorphismengruppe $G(L/K)$ gehörende Fixkörper. Nach den Sätzen 3.2.1, 3.4.6 und 3.5.3 ist auch L/Z eine Erweiterung, die endlich, normal und separabel ist. Nach Satz 3.5.5 gilt:

$$[L : K] \; = \; |G(L/K)| \; = \; |G(L/Z)| \; = \; [L : Z] \, .$$

Also ist $Z = L^{G(L/K)} = K$.