Skript
Einführung in die Algebra

SS 2003

Tim Römer

Fachbereich Mathematik/Informatik
Universität Osnabrück

Inhaltsverzeichnis

KAPITEL 1

Gruppentheorie

1. Gruppen und Monoide

Definition 1.1. Sei M eine Menge mit einer Verknüpfung (multiplikativ geschrieben)

$$\cdot : M \times M \longrightarrow M, \quad (a, b) \mapsto a \cdot b = ab.$$

(i) Die Verknüpfung heißt *assoziativ*, wenn $(ab)c = a(bc)$ für alle $a, b, c \in M$ gilt.
(ii) Die Verknüpfung heißt *kommutativ*, wenn $ab = ba$ für alle $a, b \in M$ gilt.
(iii) Ein Element $e \in M$ heißt *neutrales Element*, wenn $ea = ae = a$ für alle $a \in M$ gilt. Schreibt man die Verknüpfung multiplikativ, so bezeichnet man dieses Element auch als Einselement und schreibt 1. Ein Element $b \in M$ heißt dann *inverses Element* zu $a \in M$, wenn $ba = ab = e$ gilt. Man schreibt hierfür a^{-1}.

Bemerkung 1.2. Sei $a^0 = e$. Für $n \in \mathbb{N}, n > 0$ und $a \in M$ definiert man induktiv $a^n = a^{n-1}a$.

Seien $a_1, \ldots, a_n \in M$. Ist die Verknüpfung assoziativ, so kann man das Produkt $\prod_{i=1}^{n} a_i$ unabhängig von der Klammerung definieren (Übungsaufgabe). Als Konvention setzt man hierbei noch $\prod_{i=1}^{0} a_i = e$.

In 1.1 wurde die Verknüpfung multiplikativ geschrieben. Sie lässt sich auch additiv schreiben, also $a + b$ statt ab. Dann schreibt man auch $\sum a_i$ statt $\prod a_i$, $n \cdot a$ statt a^n, $-a$ statt a^{-1} für das inverse Element zu a und 0 (Nullelement) statt 1 für das neutrale Element.

Lemma 1.3. Sei M eine Menge mit einer Verknüpfung $\cdot : M \times M \longrightarrow M$.

(i) Es kann höchstens ein neutrales Element e bzgl. $\cdot$ geben.
(ii) Existiert ein neutrales Element, dann kann es zu einem Element $a \in M$ höchstens ein inverses Element $b \in M$ geben.

Beweis. Zu (i): Ist $e' \in M$ ein weiteres neutrales Element, dann folgt

$$e = ee' = e'$$

Zu (ii): Sei b' ein weiteres inverses Element zu a. Dann folgt

$$b' = b'e = b'ab = eb = b.$$

□

Definition 1.4. Sei G eine Menge zusammen mit einer Verknüpfung $\cdot : G \times G \longrightarrow G$.

(i) G heißt ein *Monoid*, wenn $\cdot$ assoziativ ist und G bzgl. $\cdot$ ein neutrales Element besitzt. Der Monoid heißt *kommutativ*, wenn $\cdot$ kommutativ ist.

(ii) G heißt eine *Gruppe*, wenn G ein Monoid ist und jedes Element von G ein inverses Element besitzt. Die Gruppe heißt *kommutativ* oder *abelsch*, wenn $\cdot$ kommutativ ist.

Man schreibt $(G, \cdot)$ oder G für den Monoid bzw. die Gruppe.

Bemerkung 1.5. Im Allgemeinen sind Gruppen und Monoide nicht kommutativ. Daher muss auf die Reihenfolge der Faktoren in einem Produkt geachtet werden. Zum Beispiel gilt $(ab)^{-1} = b^{-1}a^{-1}$ und $(a^{-1})^{-1} = a$ für $a, b \in G$.

In einer Gruppe gilt die Kürzungsregel, d.h. für $a \neq 0$ folgt aus $ab = ac$, dass $b = c$. Denn $b = a^{-1}(ab) = a^{-1}(ac) = c$.

Beispiele 1.6. Ein paar Beispiele:

(i) $(\mathbb{N}, \cdot)$, $(\mathbb{N}, +)$ und $(\mathbb{Z}, \cdot)$ sind kommutative Monoide, aber keine Gruppen.

(ii) $(\mathbb{Z}, +)$, $(\mathbb{Q}^*, \cdot)$, $(\mathbb{R}^*, \cdot)$ und $(\mathbb{C}^*, \cdot)$ sind abelsche Gruppen.

(iii) Aus der linearen Algebra ist folgende endliche Gruppe bekannt. Sei $m \in \mathbb{N}$, $m \neq 0$. Auf $\mathbb{Z}$ erklären wir die Äquivalenzrelation $z \sim z'$, wenn $z - z'$ durch m teilbar ist. Man schreibt dann $z \equiv z' \mod m$ und sagt, dass z *kongruent* z' modulo m ist. Die Äquivalenzklasse von z hat die Gestalt $\overline{z} = z + m\mathbb{Z}$ und wird auch Restklasse von z genannt. z heißt ein *Repräsentant* dieser Restklasse. Sei $\mathbb{Z}/m\mathbb{Z}$ die Menge aller Restklassen. Es gilt

$$\mathbb{Z}/m\mathbb{Z} = \{r + m\mathbb{Z} \colon r \in \{0, \dots, m-1\}\},$$

insbesondere ist $\mathbb{Z}/m\mathbb{Z}$ eine endliche Menge mit m Elementen. Auf $\mathbb{Z}/m\mathbb{Z}$ erklären wir eine Addition durch

$$\overline{z} + \overline{z'} = \overline{z + z'}.$$

Nun zeigt man, dass diese Verknüpfung wohldefiniert und eine Gruppenstruktur auf $\mathbb{Z}/m\mathbb{Z}$ definiert. Wir erhalten, dass $(\mathbb{Z}/m\mathbb{Z}, +)$ eine abelsche Gruppe ist (Übungsaufgabe: Beweise die Behauptungen).

(iv) $G = \{e, a\}, e =$ neutrales Element, $a^2 = aa = e$ ist eine abelsche Gruppe mit zwei Elementen.

(v) Eine Gruppe kann man durch eine Gruppentafel beschreiben:

$\cdot$	$\dots$	b	$\dots$
$\dots$			
a		$a \cdot b$	
$\dots$			

Sei $G = \{e, a, b, c\}$. Die Menge G mit

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

ist eine abelsche Gruppe.

G mit

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

ist auch eine abelsche Gruppe.

(vi) Sei $X \neq \emptyset$ ein Menge. Mit $S(X)$ bezeichnen wir die Menge aller bijektiven Abbildungen von X nach X. Die Menge $S(X)$ zusammen mit der Komposition von Abbildungen als Verknüpfung ist eine Gruppe. $S(X)$ heißt die *symmetrische Gruppe auf X*. Speziell:

$$S_n = S(\{1, \ldots, n\}).$$

Die Elemente von $S(X)$ heißen *Permutationen*. Falls $|X| \geq 3$, dann ist $S(X)$ nicht abelsch. Denn seien:

(a) $x_1, x_2, x_3 \in X$,

(b) $\varphi_1 \in S(X)$ mit $\varphi_1(x_1) = x_2,\ \varphi_1(x_2) = x_1,\ \varphi_1(x_3) = x_3,\ \varphi_1(x) = x$ sonst,

(c) $\varphi_2 \in S(X)$ mit $\varphi_2(x_1) = x_2,\ \varphi_2(x_2) = x_3,\ \varphi_2(x_3) = x_1,\ \varphi_2(x) = x$ sonst.

Dann gilt:

$$\varphi_1 \circ \varphi_2 \neq \varphi_2 \circ \varphi_1, \text{ etwa } \varphi_1 \circ \varphi_2(x_1) = x_1 \neq x_3 = \varphi_2 \circ \varphi_1(x_1).$$

Sei X endlich und $\varphi \in S(X)$, dann kann φ wie folgt beschrieben werden:
$\begin{pmatrix} x_1 & x_2 & \ldots \\ \varphi(x_1) & \varphi(x_2) & \ldots \end{pmatrix}$

Lemma 1.7. Sei G eine Menge mit einer assoziativen Verknüpfung $\cdot\colon G \times G \longrightarrow G$. Dann sind folgende Aussagen äquivalent:

(i) $(G, \cdot)$ ist eine Gruppe,

(ii) $(G, \cdot)$ hat ein links-neutrales Element (d.h. es gibt ein $e \in G$ mit $ea = a$ für alle $a \in G$) und zu jedem Element $a \in G$ existiert ein links-inverses Element (d.h. für alle $a \in G$ existiert ein b in G mit $ba = e$).

(iii) $(G, \cdot)$ hat ein rechts-neutrales Element (d.h. es gibt ein $e \in G$ mit $ae = a$ für alle $a \in G$) und zu jedem Element $a \in G$ existiert ein rechts-inverses Element (d.h. für alle $a \in G$ existiert ein b in G mit $ab = e$).

Beweis. Aus (i) folgt direkt (ii) und (iii).

Gelte die Aussage von (ii). Wir zeigen (i) und damit implizit (iii). Sei $a \in G$ beliebig und $b \in G$ links-invers zu a. Wir müssen zeigen, dass b rechts-invers und e rechts-neutral zu a ist. Zu b existiert ein weiteres links-inverses Element $c \in G$. Dann gilt

$$ab = e(ab) = (cb)(ab) = c(b(ab)) = c((ba)b) = c(eb) = cb = e.$$

Also ist b auch rechts-invers zu a. Ferner

$$ae = a(ba) = (ab)a = ea = a,$$

Somit ist e rechts-neutral zu a.

Analog folgen aus (iii) die Aussagen von (i) und (ii). □

Satz 1.8. Sei M ein Monoid. Dann ist

$$M^* = \{a \in M : a \text{ besitzt ein Inverses}\}$$

eine Gruppe.

Beweis. Da M ein Monoid ist und $e \in M^*$, bleibt zu zeigen, dass $ab \in M^*$ für alle $a, b \in M^*$ gilt.

Sei a' invers zu a und b' invers zu b, d.h. $aa' = a'a = bb' = b'b = e$, wobei e das neutrale Element von M ist. Dann gilt

$$(b'a')(ab) = b'(a'a)b = b'eb = b'b = e$$
$$(ab)(b'a') = a(bb')a' = aea' = aa' = e$$

Daher ist $b'a'$ invers zu ab und es folgt die Behauptung. □

Beispiele 1.9. Es gilt:

(i) $(\mathbb{N}, +)^* = \{0\}$, $(\mathbb{N}, \cdot)^* = \{1\}$, $(\mathbb{Z}, \cdot)^* = \{1, -1\}$.

(ii) Sei V ein Vektorraum und $\mathrm{End}(V)$ der Monoid der linearen Endomorphismen mit der Komposition $\circ$ als Verknüpfung. Dann gilt $\mathrm{End}(V)^* = \mathrm{GL}(V)$.

Definition 1.10. Sei G ein Monoid.

(i) Eine Teilmenge H von G ($H \subseteq G$) heißt *Untermonoid* von G, wenn:
   (a) $e \in H$,
   (b) Für alle $a, b \in H$ gilt $ab \in H$.

(ii) Ist G eine Gruppe, so nennt man $H \subseteq G$ eine *Untergruppe* von G, wenn gilt:
   (a) H ist ein Untermonoid,
   (b) Für alle $a \in H$ gilt $a^{-1} \in H$.

Beispiele 1.11. Betrachte:

(i) Sei G eine Gruppe (Monoid). Dann sind $\{e\}, G$ die trivialen Untergruppen (Untermonoide) von G.

(ii) Die Teilmenge $m\mathbb{Z}$, der durch m teilbaren ganzen Zahlen, ist eine Untergruppe von $\mathbb{Z}$.

Lemma 1.12. Sei G eine Gruppe. Eine nichtleere Teilmenge $H \subseteq G$ ist genau dann eine Untergruppe von G, wenn für alle $a, b \in H$ gilt:

$$ab^{-1} \in H.$$

Dies ist das sogenannte *Untergruppenkriterium*.

Beweis. Ist H eine Untergruppe von G, so folgt direkt aus der Definition, dass $ab^{-1} \in H$ für alle $a, b \in H$ gilt.

Gelte nun das Untergruppenkriterium für eine Menge $H \subseteq G$. Dann gilt:

(i) Sei $a \in H \neq \emptyset$ beliebig. Dann ist $e = aa^{-1} \in H$.

(ii) Sei $a \in H$ beliebig. Dann ist nach (i) $e \in H$ und es gilt $a^{-1} = ea^{-1} \in H$.

(iii) Sei $a, b \in H$. Dann folgt nach (ii), dass $b^{-1} \in H$ und somit $ab = a(b^{-1})^{-1} \in H$.

Mit Hilfe dieser Aussagen folgt, dass H eine Gruppe, speziell eine Untergruppe von G, ist. □

Satz 1.13. Sei $H \subseteq \mathbb{Z}$ eine Untergruppe. Dann existiert ein $m \in \mathbb{N}$ mit $H = m\mathbb{Z}$.

Beweis. Ist $H = \{0\}$, so können wir $m = 0$ wählen. Sei also $H \neq \{0\}$. Mit $z \in H$ ist auch $-z \in H$, also existieren positive Zahlen in H. Sei m die kleinste positive Zahl in H. Wir behaupten, dass $m\mathbb{Z} = H$. Es gilt immer $m\mathbb{Z} \subseteq H$. Sei nun $a \in H$. Dividiere a durch m mit Rest, d.h. es existieren zwei Zahlen $q, r \in \mathbb{Z}$ mit $0 \leq r < m$ und $a = qm + r$. Wegen $r = a - qm \in H$ und der Wahl von m (kleinste positive Zahl aus H) folgt $r = 0$, also $a = qm$. Somit gilt $m\mathbb{Z} = H$. □

Es gibt natürliche Operationen um aus bekannten Untergruppen bzw. Untermonoiden neue zu konstruieren.

Satz 1.14. Sei G eine Gruppe (ein Monoid) und $\{H_j\}_{j \in J}$ eine Familie von Untergruppen (Untermonoiden). Dann ist

$$\bigcap_{j \in J} H_j$$

eine Untergruppe (Untermonoid) von G.

Beweis. Trivial. □

2. Homomorphismen

Definition 2.1. Seien $(G, \cdot_G), (G', \cdot_{G'})$ Monoide mit neutralen Elementen e_G und $e_{G'}$. Eine Abbildung $\varphi\colon G \longrightarrow G'$ heißt *Monoidhomomorphismus*, wenn gilt:

(i) $\varphi(e_G) = e_{G'}$.
(ii) $\varphi(a \cdot_G b) = \varphi(a) \cdot_{G'} \varphi(b)$ für alle $a, b \in G$.

Sind G, G' Gruppen, so heißt φ auch *Gruppenhomomorphismus*.

Lemma 2.2. Seien G, G' Gruppen. Eine Abbildung $\varphi : G \longrightarrow G'$ ist genau dann ein Gruppenhomomorphismus, wenn $\varphi(ab) = \varphi(a)\varphi(b)$ für alle $a, b \in G$ gilt.

Beweis. Ist φ ein Gruppenhomomorphismus, so gilt per Definition $\varphi(ab) = \varphi(a)\varphi(b)$ für alle $a, b \in G$.

Gelte nun die Bedingung 2.1 (ii). Dann ist

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

Daraus folgt $\varphi(e_G) = e_{G'}$. □

Lemma 2.3. Seien G, G' Gruppen und $\varphi : G \longrightarrow G'$ ein Gruppenhomomorphismus. Dann gilt $\varphi(a^{-1}) = \varphi(a)^{-1}$ für alle $a \in G$.

Beweis. Sei $a \in G$. Dann gilt

$$e_{G'} = \varphi(e_G) = \varphi(aa^{-1}) = \varphi(a)\varphi(a^{-1}).$$

Daher folgt $\varphi(a^{-1}) = \varphi(a)^{-1}$. □

Bezeichnung 2.4. Ein Homomorphismus $\varphi\colon G \longrightarrow H$ von Gruppen oder Monoiden heißt

(i) *Monomorphismus*, wenn φ injektiv ist,
(ii) *Epimorphismus*, wenn φ surjektiv ist,
(iii) *Isomorphismus*, wenn φ bijektiv ist. Dann schreiben wir $G \cong H$.

Ein Homomorphismus $\varphi\colon G \longrightarrow G$ heißt *Endomorphismus*. Ein bijektiver Endomorphismus heißt ein *Automorphismus*.

Beispiele 2.5. Betrachte:

(i) Sei G ein Monoid und $a \in G$. Die Abbildung

$$\varphi\colon \mathbb{N} \longrightarrow G, \quad n \mapsto a^n$$

ist ein Monoidhomomorphismus, wenn man $\mathbb{N}$ mit der Addition als Verknüpfung als Monoid betrachtet. Ist G eine Gruppe, so folgt analog, dass

$$\varphi\colon \mathbb{Z} \longrightarrow G, \quad n \mapsto a^n$$

ein Gruppenhomomorphismus ist. Hierbei wird

$$a^n = \begin{cases} a \cdot \ldots \cdot a \text{ (n Faktoren)}, & \text{falls } n > 0 \\ e, & \text{falls } n = 0 \\ (a^{-1})^{-n}, & \text{falls } n < 0 \end{cases}$$

definiert.

(ii) Sei K ein Körper. Die Menge $\mathrm{M}(n \times n; K)$ aller $n \times n$-Matrizen mit der Matrizenmultiplikation als Verknüpfung ist ein Monoid. Die Menge $\mathrm{GL}(n; K) \subseteq \mathrm{M}(n \times n; K)$ der invertierbaren Matrizen ist eine Gruppe. Dann ist

$$\mathrm{Det}\colon \mathrm{M}(n \times n; K) \longrightarrow (K, \cdot) \text{ bzw. } \mathrm{Det}\colon \mathrm{GL}(n; K) \longrightarrow (K^*, \cdot)$$

ein Monoid- bzw. Gruppenhomomorphismus.

(iii) Sei G eine Gruppe oder ein Monoid. Dann ist die Identität $\mathrm{id}\colon G \longrightarrow G, a \mapsto a$ ein Homomorphismus.

(iv) Sei $\varphi\colon G \longrightarrow H$ ein Isomorphismus von Gruppen oder Monoiden. Dann ist auch die Umkehrabbildung $\varphi^{-1}\colon H \longrightarrow G$ ein Isomorphismus.

(v) Sind $\varphi\colon G \longrightarrow H$ und $\psi\colon H \longrightarrow L$ Homomorphismen von Gruppen oder Monoiden. Dann ist die Komposition $\psi \circ \varphi\colon G \longrightarrow L$ ein Homomorphismus.

(vi) Sei G eine abelsche Gruppe und $n \in \mathbb{N}$. Dann ist

$$\varphi\colon G \longrightarrow G, \quad a \mapsto a^n$$

ein Endomorphismus.

Satz 2.6. Seien M, N Monoide und $\varphi\colon M \longrightarrow N$ ein Monoidhomomorphismus. Dann ist die Einschränkung von φ auf M^* ein Gruppenhomomorphismus

$$\varphi^*\colon M^* \longrightarrow N^*.$$

Beweis. Da nach 1.8 M^* und N^* Gruppen sind, reicht es zu zeigen, dass für $a \in M^*$ gilt $\varphi(a) \in N^*$. Sei a^{-1} das inverse Element zur a. Dann ist (siehe 2.3)

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

Somit folgt aus 1.7, dass $\varphi(a) \in N^*$. □

Bezeichnung 2.7. Sei $\varphi\colon G \longrightarrow H$ ein Gruppen- oder Monoidhomomorphismus, $A \subseteq G$ und $B \subseteq H$. Dann heißt

(i) $\varphi(A) = \{b \in H\colon$ es gibt ein $a \in A$ mit $\varphi(a) = b\}$ das *Bild* von A unter φ.
(ii) $\mathrm{Im}(\varphi) = \varphi(G)$ das *Bild* von φ.
(iii) $\varphi^{-1}(B) = \{a \in G\colon\ \varphi(a) \in B\}$ das *Urbild* von B unter φ.
(iv) $\mathrm{Ker}(\varphi) = \varphi^{-1}(e_H) = \{a \in G\colon \varphi(a) = e_H\}$ der *Kern* von φ.

Satz 2.8. Es gilt:

(i) Seien $\varphi\colon G \longrightarrow H$ ein Monoidhomomorphismus und $A \subseteq G$, $B \subseteq H$ Untermonoide. Dann sind $\varphi(A) \subseteq H$ und $\varphi^{-1}(B) \subseteq G$ Untermonoide. Insbesondere sind $\mathrm{Im}(\varphi)$ und $\mathrm{Ker}(\varphi)$ Untermonoide.
(ii) Seien $\varphi\colon G \longrightarrow H$ ein Gruppenhomomorphismus und $A \subseteq G$, $B \subseteq H$ Untergruppen. Dann sind $\varphi(A) \subseteq H$ und $\varphi^{-1}(B) \subseteq G$ Untergruppen. Insbesondere sind $\mathrm{Im}(\varphi)$ und $\mathrm{Ker}(\varphi)$ Untergruppen.
(iii) Ein Gruppenhomomorphismus $\varphi\colon G \longrightarrow H$ ist genau dann injektiv, wenn $\mathrm{Ker}(\varphi) = \{e_G\}$.

Beweis. Übungsaufgabe (Beweise verlaufen analog zu den entsprechenden Beweisen in der L.A.). □

Satz 2.9. *(Cayley)* Jede Gruppe G ist isomorph zu einer Untergruppe von $S(G)$. Genauer gilt, dass

$$\varphi\colon G \longrightarrow S(G),\ a \mapsto \tau_a$$

mit

$$\tau_a\colon G \longrightarrow G,\ b \mapsto ab$$

ein Monomorphismus ist und daher gilt $G \cong \varphi(G) \subseteq S(G)$.

Beweis. Behauptung:

(i) $\tau_{e_G} = \mathrm{id}_G$.
(ii) Sei $a, b \in G$. Dann gilt $\tau_a \circ \tau_b = \tau_{ab}$.

Zu (i): Es gilt $\tau_{e_G}(b) = e_G b = b = \mathrm{id}_G(b)$ für alle $b \in G$, also $\tau_{e_G} = \mathrm{id}_G$.
Zu (ii) Sei $c \in G$. Dann ist

$$\tau_a \circ \tau_b(c) = \tau_a(bc) = abc = \tau_{ab}(c).$$

Für $a \in G$ folgt nun

$$\tau_a \circ \tau_{a^{-1}} = \tau_{aa^{-1}} = \tau_{e_G} = \mathrm{id}_G = \tau_{a^{-1}a} = \tau_{a^{-1}} \circ \tau_a,$$

d.h. $\tau_{a^{-1}}$ ist die Umkehrabbildung zu τ_a. Also ist τ_a eine bijektive Abbildung von G und daher $\tau_a \in S(G)$. Wegen (ii) ist dann φ ein Homomorphismus, denn

$$\varphi(ab) = \tau_{ab} = \tau_a \circ \tau_b = \varphi(a) \circ \varphi(b).$$

Schließlich ist φ injektiv, da

$$\varphi(a) = \mathrm{id}_G \Leftrightarrow \tau_a = \mathrm{id}_G \Leftrightarrow ab = b \ \forall b \in G \Leftrightarrow a = e_G$$

und daher $\mathrm{Ker}(\varphi) = \{e_G\}$. □

3. Zyklische Gruppen und Ordnung

Definition 3.1. Sei G eine Gruppe und $S \subset G$ eine Teilmenge. $\langle S \rangle$ sei die kleinste Untergruppe von G, die S enthält, d.h.

(i) $S \subseteq \langle S \rangle$,
(ii) Ist $H \subseteq G$ eine Untergruppe mit $S \subseteq H$, so folgt $\langle S \rangle \subseteq H$.

Gilt $G = \langle S \rangle$, so heißt S ein *Erzeugendensystem* von G. Ist $G = \langle a \rangle$, so heißt G *zyklisch*.

Satz 3.2. Sei G eine Gruppe und $S \subset G$ eine Teilmenge.

(i) $\langle S \rangle$ existiert. Genauer gilt

$$\langle S \rangle = \bigcap_{S \subseteq H \subseteq G,\ H \text{ Untergruppe}} H$$

(ii) $\langle \emptyset \rangle = \{e\}$.
(iii) Ist $S \neq \emptyset$, so ist

$$\langle S \rangle = \{a_1^{\varepsilon_1} \cdots a_r^{\varepsilon_r} \in G \colon a_1, \ldots, a_r \in S \text{ und } \varepsilon_1, \ldots, \varepsilon_r \in \{1, -1\}\}.$$

Ist insbesondere $S = \{a\}$, so folgt $\langle a \rangle = \{a^z \colon z \in \mathbb{Z}\}$.

Beweis. Zu (i): Sei $U = \bigcap_{S \subseteq H \subseteq G,\ H \text{ Untergruppe}} H$. Beachte, dass G eine Gruppe ist mit $S \subseteq G$. Daher ist $U \neq \emptyset$ eine Untergruppe von G mit $S \subseteq U$. Sei $U' \subseteq G$ eine weitere Untergruppe von G mit $S \subseteq U'$. Dann folgt per Definition von U, dass $U \subseteq U'$. Also ist $U = \langle S \rangle$.

Zu (ii): $\{e\}$ ist die kleinste Untergruppe von G, die $\emptyset$ als Teilmenge enthält. Die Behauptung folgt aus (i).

Zu (iii): Sei

$$U = \{a_1^{\varepsilon_1} \cdots a_r^{\varepsilon_r} \in G \colon a_1, \ldots, a_r \in S \text{ und } \varepsilon_1, \ldots, \varepsilon_r \in \{1, -1\}\}.$$

Dann ist U eine Untergruppe von G mit $S \subseteq U$ (nachrechnen). Sei nun H eine weitere Untergruppe von G mit $S \subseteq H$. Dann folgt, dass für $a_1, \ldots, a_r \in S$ und $\varepsilon_1, \ldots, \varepsilon_r \in \{1, -1\}$

$$a_1^{\varepsilon_1} \cdots a_r^{\varepsilon_r} \in H,$$

da H eine Gruppe ist. Also ist $U \subseteq H$ und daher $U = \langle S \rangle$. □

Beachte, dass der Beweis analog verlaufen ist zu dem entsprechenden Beweis für $\mathrm{Span}(A)$ für eine Teilmenge A in einem Vektorraum. Diese Art von Konstruktion lässt sich auf viele mathematische Objekte anwenden. Aus 3.2 (iii) folgt leicht:

Korollar 3.3. Jede zyklische Gruppe ist abelsch.

Beispiel 3.4. $(\mathbb{Z}, +)$ ist eine zyklische Gruppe mit Erzeuger 1.

Definition 3.5. Sei G eine Gruppe und $a \in G$. Wir bezeichnen mit der *Ordnung* $\operatorname{ord}(G)$ von G die Anzahl der Elemente von G und mit

$$\operatorname{ord}(a) = \begin{cases} \infty, & \text{falls } a^n \neq e \text{ für alle } n > 0, \\ \min\{0 \neq n \in \mathbb{N} \colon a^n = e\} & \text{sonst.} \end{cases}$$

die *Ordnung* von dem Element a.

Satz 3.6. Sei G eine Gruppe, $a \in G$ und $\varphi \colon (\mathbb{Z}, +) \longrightarrow G,\ z \mapsto a^z$.

(i) φ ist ein Gruppenhomomorphismus.
(ii) Sei $\operatorname{ord}(a) = \infty$. Dann sind die Potenzen a^z, $z \in \mathbb{Z}$ paarweise verschieden. Insbesondere ist die Abbildung
$$\mathbb{Z} \longrightarrow \langle a \rangle,\ z \mapsto \varphi(z)$$
ein Isomorphismus.
(iii) Sei $\operatorname{ord}(a) = n < \infty$. Für $z_1, z_2 \in \mathbb{Z}$ gilt $a^{z_1} = a^{z_2}$ genau dann, wenn $z_1 \equiv z_2 \mod n$. Insbesondere ist die Abbildung
$$\mathbb{Z}/n\mathbb{Z} \longrightarrow \langle a \rangle,\ \overline{z} \mapsto \varphi(z).$$
ein Isomorphismus.

Beweis. Zu (i): Seien $z_1, z_2 \in \mathbb{Z}$. Dann gilt

$$\varphi(z_1 + z_2) = a^{z_1 + z_2} = a^{z_1} a^{z_2} = \varphi(z_1)\varphi(z_2).$$

Daher ist φ ein Gruppenhomomorphismus. Beachte im Folgenden, dass $\operatorname{Im}(\varphi) = \langle a \rangle$. Sei $\operatorname{Ker}(\varphi) \subseteq \mathbb{Z}$. Dann ist $\operatorname{Ker}(\varphi)$ eine Untergruppe von $\mathbb{Z}$ und hat nach 1.13 die Gestalt $m\mathbb{Z}$ für ein $m \in \mathbb{N}$.

Zu (ii): Es muss $m = 0$ gelten, da $a^z \neq e$ für $z \in \mathbb{N}$ mit $z \neq 0$. Daher ist φ injektiv und die Potenzen a^z, $z \in \mathbb{Z}$ sind paarweise verschieden. Somit ist der Homomorphismus

$$\mathbb{Z} \longrightarrow \langle a \rangle,\ z \mapsto \varphi(z)$$

surjektiv und injektiv, also ein Isomorphismus.

Zu (iii): Es muss $\operatorname{ord}(a) = m$ gemäß der Definition von $\operatorname{ord}(a)$ gelten. Dann folgt

$$a^{z_1} = a^{z_2} \Leftrightarrow \varphi(z_1) = \varphi(z_2) \Leftrightarrow z_1 - z_2 \in \operatorname{Ker}(\varphi) = m\mathbb{Z} \Leftrightarrow z_1 \equiv z_2 \mod m.$$

Definiere nun

$$\overline{\varphi} \colon \mathbb{Z}/m\mathbb{Z} \longrightarrow \langle a \rangle,\ \overline{z} \mapsto \varphi(z) = a^z.$$

$\overline{\varphi}$ ist wegen dem bisher bewiesenen wohldefiniert und injektiv. Wegen φ ist die Abbildung ein Gruppenhomomorphismus und trivialerweise surjektiv. Daher ist $\overline{\varphi}$ ein Isomorphismus. □

Korollar 3.7. Sei G eine Gruppe und $a \in G$. Dann gilt:

$$\operatorname{ord}(\langle a \rangle) = \operatorname{ord}(a).$$

Ist G endlich, so folgt insbesondere, dass $\operatorname{ord}(a) < \infty$.

Beweis. Beachte, dass

$$\langle a\rangle = \{a^z \colon z \in \mathbb{Z}\}$$

eine zyklische Gruppe ist. Sei $\operatorname{ord}(a) = \infty$. Dann folgt aus 3.6 (ii), dass $\operatorname{ord}(\langle a\rangle) = \infty$. Sei nun $\operatorname{ord}(a) = m < \infty$. Wegen 3.6 (iii) ist

$$\langle a\rangle = \{a^0, a^1, \dots, a^{m-1}\}$$

und $a^i \neq a^j$ für $i \neq j$ und $i, j \in \{0, \dots, m-1\}$. Daher gilt auch in diesem Falle $\operatorname{ord}(\langle a\rangle) = m = \operatorname{ord}(a)$.

Ist G endlich, so ist auch $\langle a\rangle \subseteq G$ endlich. Daher folgt $\operatorname{ord}(a) < \infty$. □

Zyklische Gruppe lassen sich somit vollständig charakterisieren.

Satz 3.8. Sei G eine zyklische Gruppe. Dann gilt:

$$G \cong \begin{cases} \mathbb{Z}, & \text{falls } \operatorname{ord}(G) = \infty, \\ \mathbb{Z}/m\mathbb{Z}, & \text{falls } \operatorname{ord}(G) = m < \infty. \end{cases}$$

Insbesondere existiert zu jedem $m \in \mathbb{N}$ eine zyklische Gruppe der Ordnung m.

Beweis. Da G zyklisch ist, lässt G sich darstellen als $G = \langle a\rangle$ für ein $a \in G$. Aus 3.7 folgt $\operatorname{ord}(G) = \operatorname{ord}(a)$. Der Satz folgt aus 3.6. □

Beispiele 3.9. Jede endliche zyklische Gruppe ist (bis auf Isomorphie) vom Typ $\mathbb{Z}/m\mathbb{Z}$. Es gibt jedoch hierfür weitere „Modelle“:

(i) Betrachte die Permutationen

$$\zeta_k = \begin{pmatrix} 1 & 2 & \dots & k & k+1 & k+2 & \dots & m \\ m-k+1 & m-k+2 & \dots & m & 1 & 2 & \dots & m-k \end{pmatrix} \in S_m$$

für $k = 1, \dots, m$. Es gilt $\zeta_1^k = \zeta_k$ und daher ist

$$\langle \zeta_1\rangle = \{\zeta_k \colon k = 1, \dots, m\} \subseteq S_m$$

eine zyklische Untergruppe der Ordnung m.

(ii) Die Menge der Einheitswurzeln $\{z \in \mathbb{C} \colon z^m = 1\}$ ist eine Untergruppe von $(\mathbb{C}^*, \cdot)$, die von $\zeta = \cos(2\pi/m) + i\sin(2\pi/m)$ erzeugt wird.

Satz 3.10. Sei $G = \langle a\rangle$ eine zyklische Gruppe. Dann gilt:

(i) Ist $\varphi \colon G \longrightarrow G'$ ein Gruppenhomomorphismus für eine Gruppe G', so sind $\operatorname{Ker}(\varphi)$ und $\operatorname{Im}(\varphi)$ zyklische Gruppen.

(ii) Jede Untergruppe $H \subseteq G$ ist zyklisch. Genauer
   (a) Sei $\operatorname{ord}(G) = \infty$. Dann hat jede Untergruppe die Gestalt $\langle a^n\rangle$, $n \geq 0$ und diese Untergruppen sind paarweise verschieden.
   (b) Sei $\operatorname{ord}(G) = m < \infty$, so gibt es zu jedem Teiler d von m genau eine Untergruppe der Ordnung d. Diese wird von $a^{m/d}$ erzeugt. Es gibt keine weiteren Untergruppen.

Beweis. Zu (i): Sei $\varphi \colon G \longrightarrow G'$ ein Gruppenhomomorphismus. Sei $G = \langle a\rangle$ mit $a \in G$. Dann ist

$$\operatorname{Im}(\varphi) = \{\varphi(a)^z \colon z \in \mathbb{Z}\} = \langle \varphi(a)\rangle$$

eine zyklische Gruppe. $\mathrm{Ker}(\varphi) \subseteq G$ ist eine Untergruppe von G und somit bleibt (ii) zu zeigen.

Zu (ii): Sei $G = \langle a \rangle$ eine zyklische Gruppe und

$$\varphi\colon \mathbb{Z} \longrightarrow G, z \mapsto a^z$$

der Epimorphismus von 3.6. Sei $H \subseteq G$ eine Untergruppe. Dann ist $\varphi^{-1}(H)$ ist eine Untergruppe von $\mathbb{Z}$ und somit zyklisch nach 1.13, also $\varphi^{-1}(H) = n\mathbb{Z}$ für ein $n \in \mathbb{N}$. Da $\varphi(n) = a^n$, folgt

$$H = \varphi(\varphi^{-1}(H)) = \langle a^n \rangle$$

und H ist auch eine zyklische Gruppe. Ferner ist $\langle a^n \rangle$ für $n \in \mathbb{N}$ eine zyklische Untergruppe von G.

(a) In diesem Falle ist φ ein Isomorphismus (siehe 3.6 (ii)). Sind $H = \langle a^n \rangle$ und $H' = \langle a^{n'} \rangle$ zyklische Untergruppen von G mit $n, n' \in \mathbb{N}$ und $n \neq n'$. Wären $H = H'$, so würde

$$n\mathbb{Z} = \varphi^{-1}(H) = \varphi^{-1}(H') = n'\mathbb{Z}$$

folgen, da φ injektiv ist. Dies ist ein Widerspruch, also gilt $H \neq H'$.

(b) Sei d ein Teiler von m. Das Element $a^{m/d}$ hat Ordnung d, denn $(a^{m/d})^d = a^m = e$ und $(a^{m/d})^k = a^{km/d} \neq e$ für $k = 1, \ldots, d-1$, da $km/d \not\equiv 0 \mod m$. Somit ist $\langle a^{m/d} \rangle$ ein Untergruppe der Ordnung d.

Sei $H \subseteq G$ eine Untergruppe. Beachte, dass $\mathrm{ord}(H) \leq \mathrm{ord}(G) = m$. Dann ist $\varphi^{-1}(H) = n\mathbb{Z}$ für ein $n \in \mathbb{N}$. Es gilt

$$n\mathbb{Z} = \varphi^{-1}(H) \supseteq \mathrm{Ker}(\varphi) = m\mathbb{Z}$$

Somit ist $m \in n\mathbb{Z}$ und n muss ein Teiler von m sein, d.h. $m = dn$ für ein $d \in \mathbb{N}$. Da $H = \langle a^n \rangle$, folgt $\mathrm{ord}(H) = d$ mit $d|m$ und $n = m/d$.

Wir haben gezeigt, dass es höchstens so viele Untergruppen von G gibt, wie m Teiler hat. Zu jedem Teiler d von m gibt es aber auch eine Untergruppe der Ordnung d, also existiert zu jedem Teiler d genau eine Untergruppe mit d Elementen. □

4. Nebenklassen, Normalteiler und Faktorgruppen

Definition 4.1. Sei G eine Gruppe, $H \subseteq G$ eine Untergruppe und $a \in G$ beliebig.

(i) Die Menge $aH = \{ab\colon b \in H\}$ heißt eine *Linksnebenklasse von H* in G.
(ii) Die Menge $Ha = \{ba\colon b \in H\}$ heißt eine *Rechtsnebenklasse von H* in G.
(iii) Mit G/H bezeichnen wir die Menge der Linksnebenklassen von H in G.
(iv) Mit $H \setminus G$ bezeichnen wir die Menge der Rechtsnebenklassen von H in G.

Im Folgenden betrachten wir nur Linksnebenklassen. Alle Aussagen gelten jedoch analog für Rechtsnebenklassen.

Lemma 4.2. Sei G eine Gruppe und $H \subseteq G$ eine Untergruppe. Seien aH und bH Linksnebenklassen von H in G. Dann sind folgende Aussagen äquivalent:

(i) $aH = bH$,
(ii) $aH \cap bH \neq \emptyset$,
(iii) $a \in bH$,
(iv) $b^{-1}a \in H$.

Beweis. Gilt (i), so folgt direkt (ii), da $H \neq \emptyset$.

Sei nun (ii) gegeben. Dann existiert ein $c \in aH \cap bH$ und $c = ah_1 = bh_2$ für $h_1, h_2 \in H$. Dann ist $a = bh_2h_1^{-1} \in bH$ und daher gilt (iii).

Aus (iii) folgt ähnlich (iv). Gelte (iv), etwa $b^{-1}a = h \in H$. Dann ist $a = bh \in bH$ und es folgt $aH \subseteq bH$. Mit $b^{-1}a \in H$ ist auch das inverse Element $(b^{-1}a)^{-1} = a^{-1}b \in H$. Es folgt analog $bH \subseteq aH$ und somit $aH = bH$. □

Satz 4.3. Sei G eine Gruppe und $H \subseteq G$ eine Untergruppe von G. Dann gilt:

(i) Für jedes $a \in G$ ist die Abbildung $\mu_a \colon H \longrightarrow aH,\ b \mapsto ab$ bijektiv. Insbesondere sind je zwei Linksnebenklassen gleichmächtig.
(ii) Verschiedene Linksnebenklassen sind paarweise disjunkt.
(iii) G ist die disjunkte Vereinigung der Linksnebenklassen von H in G.

Beweis. Zu (i): μ_a ist trivialerweise surjektiv. Seien $b, b' \in H$ mit $\mu_a(b) = \mu_a(b')$. Dann folgt aus $ab = ab'$ nach kürzen, dass $b = b'$. Also ist μ_a injektiv und somit bijektiv. (ii) folgt aus 4.2.

Zu (iii): Jedes $a \in G$ ist Element der Linksnebenklasse $L = aH$. Daher folgt, dass $G = \cup_{L \in G/H} L$. Wegen (ii) ist diese Vereinigung disjunkt. □

Definition 4.4. Sei G eine Gruppe und $H \subseteq G$ eine Untergruppe von G. Der *Index* $[G : H]$ von H in G ist definiert als die Anzahl der Linksnebenklassen von H in G.

Satz 4.5. *(Lagrange)* Sei G eine endliche Gruppe und H eine Untergruppe von G. Dann gilt:

$$\mathrm{ord}(G) = [G : H]\mathrm{ord}(H).$$

Beweis. Seien $a_1, \ldots, a_r$ so gewählt, dass $G/H = \{a_1H, \ldots, a_rH\}$ und $a_iH \neq a_jH$. Es folgt

$$G = \bigcup_{i=1}^{r} a_iH.$$

Wegen 4.3 (ii) ist diese Vereinigung disjunkt und somit $\mathrm{ord}(G) = \sum_{i=1}^{r} |a_iH|$. Nach 4.3 (i) gilt $|H| = |a_iH| = |a_jH|$. Daher

$$\mathrm{ord}(G) = \sum_{i=1}^{r} |a_iH| = r|H| = [G : H]\mathrm{ord}(H).$$

□

Beispiel 4.6. Mit Hilfe der bisherigen Resultate kann man bereits in einigen Fällen sämtliche Untergruppen einer Gruppe bestimmen. Sei $G = S_3$. Diese besteht aus den Elementen

$$\mathrm{id} = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix},\ a_1 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix},\ a_2 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix},$$

$$b_1 = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix},\ b_2 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix},\ b_3 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}.$$

Man sieht sofort, dass folgendes gilt:

$$\mathrm{ord}(\mathrm{id}) = 1,\ \mathrm{ord}(a_1) = \mathrm{ord}(a_2) = 3,\ \mathrm{ord}(b_1) = \mathrm{ord}(b_2) = \mathrm{ord}(b_3) = 2$$

und

$$\langle a_i \rangle = \{\mathrm{id}, a_1, a_2\},\ i = 1, 2,$$
$$\langle b_j \rangle = \{\mathrm{id}, b_j\},\ j = 1, 2, 3.$$

Sei $H \subseteq G$ eine beliebige Untergruppe mit $H \neq \{e\}, G$. Aus dem Satz von Lagrange 4.5 folgt $\mathrm{ord}(H) = 2$ oder $\mathrm{ord}(H) = 3$. Gilt $\mathrm{ord}(H) = 2$, so muss H ein Element der Ordnung 2 enthalten. Daraus folgt, dass $H = \langle b_i \rangle$ für ein i. Ist $\mathrm{ord}(H) = 3$, so folgt analog, dass $H = \langle a_j \rangle$ für ein j.

Es gilt

$$a_1\langle b_1 \rangle = \{a_1, b_2\} \neq \{a_1, b_3\} = \langle b_1 \rangle a_1.$$

Dies zeigt, dass im Allgemeinen Links- und Rechtsnebenklassen nicht übereinstimmen müssen.

Gruppen von Primzahlordnung lassen mit Hilfe des Satzes von Lagrange vollständig charakterisieren.

Korollar 4.7. Sei G eine Gruppe und $\mathrm{ord}(G)$ eine Primzahl. Dann ist G zyklisch und besitzt keine echten Untergruppen, d.h. $\{e\}$ und G sind die einzigen Untergruppen von G.

Beweis. Sei $\mathrm{ord}(G) = p$ eine Primzahl und $H \subseteq G$ eine Untergruppe. Da $\mathrm{ord}(H) | p$, muss $\mathrm{ord}(H) = 1$ oder $\mathrm{ord}(H) = p$ gelten. Dies bedeutet $H = \{e\}$ oder $H = G$. Wähle nun ein $a \in G$ mit $a \neq e$. Da $\{e\} \neq \langle a \rangle \subseteq G$ eine Untergruppe ist, gilt $G = \langle a \rangle$. □

Beispiel 4.8. Dies ist ein erneuter Beweis, dass für eine Primzahl p die Gruppe $\mathbb{Z}/p\mathbb{Z}$ keine echten Untergruppen besitzt (siehe 3.10). Somit ist auch bewiesen, dass es neben den zyklischen Gruppen bis auf Isomorphie keine weiteren Gruppe von Primzahlordnung gibt.

Im Falle von Elementordnungen in endlichen Gruppen liefert der Satz von Lagrange:

Satz 4.9. Sei G eine endliche Gruppe und $a \in G$. Dann gilt:

(i) $\mathrm{ord}(a) | \mathrm{ord}(G)$,
(ii) (kleiner Fermatsche Satz) $a^{\mathrm{ord}(G)} = e$.

Beweis. Beachte, dass wegen 3.7 $\mathrm{ord}(a) < \infty$ gilt. Wegen $\mathrm{ord}(\langle a \rangle) = \mathrm{ord}(a)$ folgt (i) aus 4.5. Es gilt

$$a^{\mathrm{ord}(G)} = (a^{\mathrm{ord}(a)})^{\mathrm{ord}(G)/\mathrm{ord}(a)} = e$$

und dies beweist (ii). □

Im Folgenden soll das Problem studiert werden, für welche Untergruppen $H \subseteq G$ man eine Gruppenstruktur auf G/H definieren kann. Wir werden die Frage beantworten können, welche Untergruppen einer Gruppe Kern eines Gruppenhomomorphismus sein können.

Satz 4.10. Sei $\varphi\colon G \longrightarrow G'$ ein Gruppenhomomorphismus und $H = \mathrm{Ker}(\varphi)$. Dann gilt für alle $a \in G$:

$$aH = Ha.$$

Die zugehörigen Links- und Rechtsnebenklassen stimmen also überein.

Beweis. Sei $b \in H$, d. h. $\varphi(b) = e$. Dann gilt

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

Also $aba^{-1} \in H$. Nun folgt

$$ab = aba^{-1}a \in Ha.$$

Somit $aH \subseteq Ha$. Analog zeigt man $Ha \subseteq aH$ und daher folgt

$$aH = Ha.$$

□

Definition 4.11. Sei G eine Gruppe. Eine Untergruppe $H \subseteq G$ heißt *Normalteiler*, wenn $aH = Ha$ für alle $a \in G$ gilt. Wir schreiben hierfür $H \triangleleft G$.

Beispiel 4.12. Betrachte:

(i) G und $\{e\}$ sind die trivialen Normalteiler einer Gruppe G.
(ii) Ist G eine abelsche Gruppe, dann ist jede Untergruppe $H \subseteq G$ ein Normalteiler.
(iii) Wir haben gesehen, dass jeder Kern eines Gruppenhomomorphismus ein Normalteiler ist. Daher die alternierende Gruppe A_n ein Normalteiler in S_n, da sie Kern der Signum Abbildung $\operatorname{sign}\colon S_n \longrightarrow \{\pm 1\}$ ist.
(iv) Jede Untergruppe H einer Gruppe G mit Index $[G : H] = 2$ ist ein Normalteiler (Übungsaufgabe).

Bemerkung 4.13. Sei G eine Gruppe und $X, Y \subseteq G$ Mengen. Wir definieren das Produkt

$$XY = \{ab\colon a \in X, b \in Y\}.$$

Ist $X = \{a\}$, so schreiben wir hierfür auch aY (analog für Y). Diese Verknüpfung ist assoziativ und es gelten Rechenregeln wie

(i) $aa^{-1}Y = Y = Yaa^{-1}$,
(ii) ...

Lemma 4.14. Sei G eine Gruppe und $H \subseteq G$ eine Untergruppe. Dann sind folgende Aussagen äquivalent:

(i) $H \triangleleft G$,
(ii) $aHa^{-1} = H$ für alle $a \in G$.
(iii) $aHa^{-1} \subseteq H$ für alle $a \in G$,

Beweis. Sei stets $a \in G$ beliebig. (ii) folgt aus (i) wegen

$$aHa^{-1} = Haa^{-1} = H.$$

Analog folgt (i) aus (ii) durch

$$aH = aHa^{-1}a = Ha.$$

Gilt (ii), so auch (iii). Die umgekehrte Folgerung gilt wegen

$$H = aa^{-1}Haa^{-1} \subseteq aHa^{-1} \subseteq H.$$

Also $H = aHa^{-1}$. □

Ähnlich wie Untergruppen verhalten sich Normalteiler unter Gruppenhomomorphismen.

Satz 4.15. Seien G, G' Gruppen und $\varphi\colon G \longrightarrow G'$ ein Gruppenhomomorphismus. Dann gilt:

(i) Ist $H' \triangleleft G'$, so ist $\varphi^{-1}(H') \triangleleft G$.
(ii) Ist $H \triangleleft G$ und φ surjektiv, so ist $\varphi(H) \triangleleft G'$.

Beweis. Wir zeigen:

(i) Beachte, dass $\varphi^{-1}(H')$ eine Untergruppe ist. Sei $a \in G$ und $b \in \varphi^{-1}(H')$ beliebig. Es ist $\varphi(aba^{-1}) = \varphi(a)\varphi(b)\varphi(a)^{-1} \in H'$, da H' ein Normalteiler ist. Es folgt, dass $a\varphi^{-1}(H')a^{-1} \subseteq \varphi^{-1}(H')$ und daher $a\varphi^{-1}(H')a^{-1} = \varphi^{-1}(H')$. Also ist $\varphi^{-1}(H')$ ein Normalteiler von G.
(ii) Seien $a' \in G'$ und $b' \in \varphi(H)$ mit $b' = \varphi(b)$. Die Abbildung φ ist surjektiv und es folgt, dass ein $a \in G$ existiert mit $\varphi(a) = a'$. Dann ist $a'b'(a')^{-1} = \varphi(a)\varphi(b)\varphi(a)^{-1} = \varphi(aba^{-1}) \in \varphi(H)$, da H ein Normalteiler ist und daher $aba^{-1} \in H$ gilt. Es folgt, dass $a'\varphi(H)(a')^{-1} \subseteq \varphi(H)$ und somit $a'\varphi(H)(a')^{-1} = \varphi(H)$. Daraus folgt die Behauptung.

□

Konstruktion 4.16. Sei G eine Gruppe und $H \triangleleft G$. Wir erklären auf G/H eine Gruppenstruktur. Seien $aH, bH \in G/H$, dann definieren wir $aH \cdot bH = abH$. Dieses Produkt ist wohldefiniert. Sei $a_1H = a_2H$ und $b_1H = b_2H$. Dann gilt nach 4.2 $a_1^{-1}a_2, b_1^{-1}b_2 \in H$ und somit

$$(a_1b_1)^{-1}a_2b_2 = b_1^{-1}a_1^{-1}a_2b_2 = (b_1^{-1}(a_1^{-1}a_2)b_1)(b_1^{-1}b_2) \in H.$$

Also gilt $a_1b_1H = a_2b_2H$. G/H ist zusammen mit dieser Abbildung eine Gruppe ($eH = H$ ist das neutrale Element; $a^{-1}H$ ist das inverse Element zu aH).

Satz 4.17. Sei G eine Gruppe und $H \triangleleft G$. Dann gilt:

(i) G/H ist zusammen mit der Verknüpfung

$$G/H \times G/H \longrightarrow G/H,\ aH \times bH \mapsto abH$$

eine Gruppe. Sie heißt die *Faktorgruppe* (von G modulo H).
(ii) Die Abbildung

$$\varepsilon\colon G \longrightarrow G/H,\ a \mapsto aH$$

ist ein Epimorphismus und heißt der *kanonische Epimorphismus*. Es gilt $\mathrm{Ker}(\varepsilon) = H$.

Beweis. Zu (i): Übungsaufgabe.

Zu (ii): Seien $a, b \in G$. Dann gilt

$$\varepsilon(ab) = abH = aHbH = \varepsilon(a)\varepsilon(b).$$

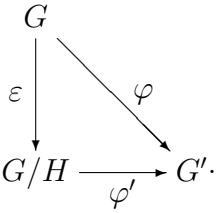
Daher ist ε ein Gruppenhomomorphismus, der trivialerweise surjektiv ist. Sei $a \in H$. Dann ist $\varepsilon(a) = aH = H$, also $a \in \mathrm{Ker}(\varepsilon)$. Ist umgekehrt $a \in \mathrm{Ker}(\varepsilon)$, dann folgt aus $eH = H = \varepsilon(aH) = aH$, dass $a = e^{-1}a \in H$. Somit $H = \mathrm{Ker}(\varepsilon)$. □

Beispiel 4.18. Beachte, dass die Elemente der Gruppe G/H Mengen (gerade die Linksnebenklassen) sind. Wir kennen jedoch schon bereits ein Beispiel: Die Faktorgruppen $(\mathbb{Z}/m\mathbb{Z}, +)$ für $m \in \mathbb{N}$.

Korollar 4.19. Sei G eine Gruppe und $H \subseteq G$ eine Untergruppe. Genau dann ist $H \triangleleft G$, wenn $H = \mathrm{Ker}(\varphi)$ für einen geeigneten Gruppenhomomorphismus.

Beweis. Ist $H = \mathrm{Ker}(\varphi)$, so haben wir schon gesehen, dass $H \triangleleft G$. Wenn umgekehrt $H \triangleleft G$ gilt, so ist $H = \mathrm{Ker}(\varepsilon)$, wobei ε der kanonische Epimorphismus von $G \longrightarrow G/H$ ist. □

Satz 4.20. *(Die universelle Eigenschaft der Faktorgruppe)* Seien G, G' Gruppen, $H \triangleleft G$ und $\varphi\colon G \longrightarrow G'$ ein Gruppenhomomorphismus mit $H \subseteq \mathrm{Ker}(\varphi)$. Dann gibt es genau einen Gruppenhomomorphismus $\varphi'\colon G/H \longrightarrow G'$ mit $\varphi = \varphi' \circ \varepsilon$, d.h. folgendes Diagramm ist kommutativ:



Es gilt $\mathrm{Ker}(\varphi') = \mathrm{Ker}(\varphi)/H = \varepsilon(\mathrm{Ker}(\varphi))$ und $\mathrm{Im}(\varphi') = \mathrm{Im}(\varphi)$.

Beweis. Eindeutigkeit von φ': Sei $aH \in G/H$ für ein $a \in G$. Dann ist

$$\varphi'(aH) = \varphi' \circ \varepsilon(a) = \varphi(a).$$

und somit folgt die Behauptung

Existenz von φ': Sei $aH \in G/H$ für ein $a \in G$. Wir definieren $\varphi'(aH) = \varphi(a)$. Als erstes ist zu zeigen, dass φ' wohldefiniert ist. Sei $aH = bH$ für $a, b \in G$, d.h. $a^{-1}b \in H$. Da $H \subseteq \mathrm{Ker}(\varphi)$, folgt $e_{G'} = \varphi(a^{-1}b) = \varphi(a)^{-1}\varphi(b)$. Daher $\varphi(a) = \varphi(b)$.

φ' ist ein Gruppenhomomorphismus: Seien $aH, bH \in G/H$ für $a, b \in G$. Dann gilt

$$\varphi'(aHbH) = \varphi'(abH) = \varphi(ab) = \varphi(a)\varphi(b) = \varphi'(aH)\varphi'(bH).$$

Sei $aH \in \mathrm{Ker}(\varphi')$. Dann gilt $e_{G'} = \varphi'(aH) = \varphi(a)$ und es folgt $a \in \mathrm{Ker}(\varphi)$. Daher ist $\mathrm{Ker}(\varphi') \subseteq \mathrm{Ker}(\varphi)/H$. Sei umgekehrt $a \in \mathrm{Ker}(\varphi)$. Es folgt, dass $\varphi'(aH) = \varphi(a) = e$ und somit $\mathrm{Ker}(\varphi') \supseteq \mathrm{Ker}(\varphi)/H$. Insgesamt folgt die Behauptung. □

Man kann sich leicht überlegen, dass die Faktorgruppe durch die universelle Eigenschaft eindeutig bestimmt ist.

Korollar 4.21. *(Homomorphiesatz)* Seien G, G' Gruppen und $\varphi\colon G \longrightarrow G'$ ein Gruppenhomomorphismus. Dann ist die induzierte Abbildung

$$\varphi'\colon G/\mathrm{Ker}(\varphi) \longrightarrow \mathrm{Im}(\varphi)$$

ein Isomorphismus.

Mit Hilfe dieses Resultats, lassen sich ähnliche Aussagen zum Satz von Lagrange beweisen.

Satz 4.22. Seien G, G' endliche Gruppen und $\varphi\colon G \longrightarrow G'$ ein Gruppenhomomorphismus.

(i) Für jede Untergruppe $H \subseteq G$ gilt

$$\operatorname{ord}(H) = \operatorname{ord}(\varphi(H))\operatorname{ord}(H \cap \operatorname{Ker}(\varphi)).$$

(ii) Sei φ surjektiv. Dann gilt für jede Untergruppe $H' \subseteq G'$

$$\operatorname{ord}(\varphi^{-1}(H')) = \operatorname{ord}(H')\operatorname{ord}(\operatorname{Ker}(\varphi)).$$

Beweis. Zu (i): Definiere

$$\varphi_0 = \varphi_{|H} \colon H \longrightarrow \varphi(H).$$

φ_0 ist ein Epimorphismus mit $\operatorname{Ker}(\varphi_0) = H \cap \operatorname{Ker}(\varphi)$. Nach dem Homomorphiesatz ist

$$\varphi(H) \cong H/\operatorname{Ker}(\varphi_0).$$

Aus dem Satz von Lagrange folgt:

$$\operatorname{ord}(\varphi(H)) = \operatorname{ord}(H/\operatorname{Ker}(\varphi_0)) = [H : \operatorname{Ker}(\varphi_0)]$$

$$= \operatorname{ord}(H)/\operatorname{ord}(\operatorname{Ker}(\varphi_0)) = \operatorname{ord}(H)/\operatorname{ord}(H \cap \operatorname{Ker}(\varphi))$$

Zu (ii): Definiere $H = \varphi^{-1}(H')$. Da φ surjektiv, folgt $H' = \varphi(H)$. Ferner ist $\operatorname{Ker}(\varphi) \subseteq H$. Also ist (ii) ein Spezialfall von (i). □

5. Produkte

Satz 5.1. Seien G, H Gruppen (Monoide), dann ist $G \times H = \{(a, b) \colon a \in G,\ b \in H\}$ mit der Verknüpfung

$$(a_1, b_1) \cdot (a_2, b_2) = (a_1 a_2, b_1 b_2)$$

eine Gruppe (Monoid).

Beweis. Übungsaufgabe. □

Beispiel 5.2. Betrachte $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$. Neben $\mathbb{Z}/4\mathbb{Z}$ ist dies die einzige Gruppe (bis auf Isomorphie) mit vier Elementen.

Satz 5.3. Seien G, H Gruppen. Dann gilt

(i) Die Abbildungen

$$\iota_G \colon G \longrightarrow G \times H,\ a \mapsto (a, e_H),$$

$$\iota_H \colon H \longrightarrow G \times H,\ b \mapsto (e_G, b)$$

sind Monomorphismen. G, H können daher als Untergruppen von $G \times H$ aufgefasst werden.

(ii) $G \times \{e_H\}, \{e_G\} \times H \lhd G \times H$.

(iii) Die Abbildungen

$$\pi_G \colon G \times H \longrightarrow G,\ (a, b) \mapsto a$$

$$\pi_H \colon G \times H \longrightarrow H,\ (a, b) \mapsto b$$

sind Epimorphismen. Es gilt $\operatorname{Ker}(\pi_G) = \{e_G\} \times H$, $\operatorname{Ker}(\pi_H) = G \times \{e_H\}$ und

$$(G \times H)/H \cong G,\ (G \times H)/G \cong H.$$

Beweis. Wir beweisen die Aussagen für G. Die Aussagen für H folgen dann analog.

Zu (i): Für $a, b \in G$ ist

$$\iota_G(ab) = (ab, e_H) = (a, e_H)(b, e_H) = \iota_G(a)\iota_G(b).$$

und $\iota_G(a) = e$ genau dann, wenn $a = e_G$ gilt. Dies zeigt die Behauptung.

Zu (ii): Seien $a, b \in G$ und $c \in H$. Dann gilt

$$(b, c)(a, e_H)(b^{-1}, c^{-1}) = (bab^{-1}, ce_Hc^{-1}) = (bab^{-1}, e_H) \in \iota_G(G) \cong G.$$

Daher folgt $G \times \{e_H\} \lhd G \times H$.

Zu (iii): Man sieht leicht, dass π_G ein Epimorphismus mit $\mathrm{Ker}(\pi_G) = \{e_G\} \times H$ ist. Aus dem Homomorphiesatz folgt dann

$$(G \times H)/H \cong (G \times H)/\{e_G\} \times H \cong G.$$

□

Definition 5.4. Eine Gruppe G heißt *inneres Produkt* zweier Untergruppen H_1, H_2, wenn die Abbildung

$$\varphi\colon H_1 \times H_2 \longrightarrow G,\ (a, b) \mapsto ab$$

ein Isomorphismus ist. Man schreibt dann $G = H_1 \times H_2$.

Lemma 5.5. Sei G eine Gruppe, $H_1, H_2 \subseteq G$ Untergruppen und

$$\varphi\colon H_1 \times H_2 \longrightarrow G,\ (a, b) \mapsto ab.$$

Dann gilt:

(i) φ ist genau dann ein Gruppenhomomorphismus, wenn $ab = ba$ für alle $a \in H_1$ und $b \in H_2$.

(ii) Gilt

$$H_1 \lhd G,\ H_2 \lhd G \text{ und } H_1 \cap H_2 = \{e\},$$

dann ist φ ein Monomorphismus.

Beweis. Zu (i): Seien $a_1, a_2 \in H_1$ und $b_1, b_2 \in H_2$ beliebig. Dann ist

$$\varphi((a_1, b_1) \cdot (a_2, b_2)) = \varphi((a_1a_2, b_1b_2)) = a_1a_2b_1b_2$$

und

$$\varphi((a_1, b_1))\varphi((a_2, b_2)) = a_1b_1a_2b_2.$$

φ ist genau dann ein Homomorphismus, wenn

$$a_1a_2b_1b_2 = a_1b_1a_2b_2.$$

Gilt nun $a_2b_1 = b_1a_2$, so ist φ ein Homomorphismus. Ist umgekehrt φ ein Homomorphismus, so folgt $a_2b_1 = b_1a_2$, indem wir $a_1 = b_2 = e$ setzen.

Zu (ii): Sei $a \in H_1$ und $b \in H_2$. Da $H_1 \lhd G$, folgt $b^{-1}ab \in H_1$ und es gilt

$$a^{-1}b^{-1}ab \in a^{-1}H_1 = H_1.$$

Analog ist $a^{-1}b^{-1}a \in H_2$, da $H_2 \lhd G$, und

$$a^{-1}b^{-1}ab \in H_2b = H_2.$$

Insgesamt erhalten wir $a^{-1}b^{-1}ab \in H_1 \cap H_2 = \{e\}$. Also $a^{-1}b^{-1}ab = e$ und daraus folgt $ab = ba$. Nach (i) ist φ daher ein Homomorphismus.

Sei nun $(a, b) \in \mathrm{Ker}(\varphi)$, d.h.

$$e = \varphi((a, b)) = ab.$$

Somit $a = b^{-1} \in H_1 \cap H_2 = \{e\}$ und daher $a = b^{-1} = e$. Dann gilt aber auch $b = e$ und es folgt, dass $\mathrm{Ker}(\varphi) = \{e, e\}$. Also ist φ injektiv. □

Satz 5.6. Sei G eine Gruppe und $H_1, H_2 \subseteq G$ Untergruppen. Dann sind folgende Aussagen äquivalent:

(i) $G \cong H_1 \times H_2$.
(ii) $G = H_1H_2,\ H_1 \triangleleft G,\ H_2 \triangleleft G$ und $H_1 \cap H_2 = \{e\}$.

Beweis. (i) ⇒ (ii): Beachte, dass $\varphi(H_1 \times \{e\}) = H_1$ und $\varphi(\{e\} \times H_2) = H_2$. Aus 5.3 folgt, dass

$$H_1 \times \{e\},\ \{e\} \times H_2$$

Normalteiler in $H_1 \times H_2$ sind. Da φ ein Isomorphismus ist, sind $\varphi(H_1 \times \{e\}) = H_1$ und $\varphi(\{e\} \times H_2) = H_2$ Normalteiler in G (siehe 4.15). Es gilt

$$H_1 \times \{e\} \cdot \{e\} \times H_2 = \{(a, e) \cdot (e, b) = (a, b) \colon a \in H_1,\ b \in H_2\} = H_1 \times H_2,$$

$$H_1 \times \{e\} \cap \{e\} \times H_2 = \{e, e\}.$$

Daraus folgt

$$G = \varphi(H_1 \times H_2) = \varphi(H_1 \times \{e\} \cdot \{e\} \times H_2) = \varphi(H_1 \times \{e\}) \cdot \varphi(\{e\} \times H_2) = H_1 \cdot H_2$$

und

$$H_1 \cap H_2 = \varphi(H_1 \times \{e\}) \cap \varphi(\{e\} \times H_2) = \varphi(H_1 \times \{e\} \cap \{e\} \times H_2) = \varphi(\{e, e\}) = \{e\}.$$

(ii) ⇒ (i): Wegen 5.5 ist φ ein Monomorphismus. Es gilt außerdem $G = H_1H_2$, d.h. für alle $a \in G$ existieren $b \in H_2, c \in H_2$ mit

$$a = bc = \varphi((b, c)).$$

Also ist φ auch surjektiv. □

Beispiel 5.7. Wir zeigen, dass

$$\mathbb{Z}/6\mathbb{Z} \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}.$$

$G = \mathbb{Z}/6\mathbb{Z}$ ist abelsch, also sind die Untergruppen

$$\langle \overline{2} \rangle \text{ und } \langle \overline{3} \rangle$$

Normalteiler von G. Es ist

$$\langle \overline{2} \rangle = \{\overline{0}, \overline{2}, \overline{4}\} \cong \mathbb{Z}/3\mathbb{Z},\ \langle \overline{3} \rangle = \{\overline{0}, \overline{3}\} \cong \mathbb{Z}/2\mathbb{Z}.$$

Ferner ist

$$\langle \overline{2} \rangle \cap \langle \overline{3} \rangle = \{\overline{0}\}$$

und

$$\langle \overline{2} \rangle + \langle \overline{3} \rangle = \{\overline{0}, \overline{1}, \ldots, \overline{5}\} = \mathbb{Z}/6\mathbb{Z}.$$

Die Behauptung folgt nun aus 5.6.

6. Operationen von Gruppen, p-Sylowuntergruppen

Definition 6.1. Sei G eine Gruppe und X eine Menge. Eine *Operation* von G auf X ist eine Abbildung

$$G \times X \longrightarrow X, \quad (a, x) \mapsto a(x) = ax,$$

mit:

(i) Ist e das neutrale Element von G, so gilt $e(x) = x$ für alle $x \in X$.
(ii) Für alle $a, b \in G$ und $x \in X$ gilt $(ab)(x) = a(b(x))$.

Man sagt G *operiert auf* X.

Beispiele 6.2. Es gilt:

(i) Sei G eine Gruppe, dann operiert G auf sich selber durch

$$G \times G \longrightarrow G, \quad (a, b) \mapsto ab.$$

(ii) Für jede Menge X operiert $S(X)$ auf X durch

$$S(X) \times X \longrightarrow X, \ (\sigma, a) \mapsto \sigma(a).$$

Satz 6.3. Sei G eine Gruppe und X eine Menge.

(i) Wenn G auf X operiert, dann gibt es genau einen Gruppenhomomorphismus $\varphi : G \longrightarrow S(X)$ mit $\varphi(a)(x) = a(x)$ für alle $a \in G$ und $x \in X$.
(ii) Ist umgekehrt $\varphi : G \longrightarrow S(X)$ ein Gruppenhomomorphismus, dann ist die Abbildung

$$G \times X \longrightarrow X, \quad (a, x) \mapsto \varphi(a)(x)$$

eine Operation.

Somit entsprechen Operationen von G auf X umkehrbar eindeutig den Gruppenhomomorphismen $G \longrightarrow S(X)$.

Beweis. Zu (i): Es ist zu zeigen, dass φ eine Abbildung von G nach $S(X)$ ist. Als erstes zeigen wir, dass $\varphi(a) \in S(X)$ für $a \in G$ ist.

$\varphi(a)$ ist injektiv: Seien $x_1, x_2 \in X$ mit $\varphi(a)(x_1) = \varphi(a)(x_2)$, d.h. $a(x_1) = a(x_2)$. Dann ist

$$x_1 = e(x_1) = (a^{-1}a)(x_1) = a^{-1}(a(x_1)) = a^{-1}(a(x_2)) = (a^{-1}a)(x_2) = e(x_2) = x_2.$$

Somit folgt die Behauptung.

$\varphi(a)$ ist surjektiv: Sei $y \in X$. Dann ist

$$\varphi(a)(a^{-1}(y)) = a(a^{-1}(y)) = (aa^{-1})(y) = e(y) = y.$$

Es folgt, dass $\varphi(a)$ eine bijektive Abbildung ist. Als nächstes muss gezeigt werden, dass φ ein Gruppenhomomorphismus ist. Seien $a, b \in G$. Es ist zu zeigen, dass $\varphi(ab) = \varphi(a)\varphi(b)$. Sei $x \in X$ beliebig, dann gilt

$$\varphi(ab)(x) = (ab)(x) = a(b(x)) = a(\varphi(b)(x)) = \varphi(a)(\varphi(b)(x)) = (\varphi(a)\varphi(b))(x).$$

Wegen der Definition ist φ eindeutig bestimmt.

Zu (ii): Sei e das neutrale Element von G. Dann folgt für $x \in X$

$$e(x) = \varphi(e)(x) = x, \text{da } \varphi(e) \text{ das neutrale Element von } S(X) \text{ ist.}$$

Seien $a, b \in G$ und $x \in X$, dann gilt

$$(ab)(x) = \varphi(ab)(x) = (\varphi(a)\varphi(b))(x) = \varphi(a)(\varphi(b)(x)) = a(b(x)).$$

□

Definition 6.4. Sei G eine Gruppe, die auf einer Menge X operiert.

(i) Zwei Elemente $x, y \in X$ heißen *G-äquivalent* ($x \sim y$), wenn ein $a \in G$ existiert mit $a(x) = y$.
(ii) Die Äquivalenzklassen ($Gx = \{a(x) \colon a \in G\}$) bzgl. $\sim$ heißen *Bahnen* von G in X.

Beispiele 6.5. Betrachte:

(i) Die multiplikative Gruppe der komplexen Zahlen vom Betrag 1 operiert auf der Gaußschen Zahlenebene ($\mathbb{C}$). Die Bahnen sind die konzentrischen Kreise mit Mittelpunkt 0.
(ii) Sei G eine Gruppe und $H \subseteq G$ eine Untergruppe. Durch Rechts- bzw. Linksmultiplikation wird eine Operation von H auf G erklärt:

$$R \colon H \times G \longrightarrow G, (a, b) \mapsto ba^{-1},$$

$$L \colon H \times G \longrightarrow G, (a, b) \mapsto ab.$$

Die Bahnen bzgl. der Rechts- bzw. Linksmultiplikation sind die Links- bzw. Rechtsnebenklassen von H.

Lemma 6.6. Sei G eine Gruppe, die auf einer Menge X operiert. Dann ist X die disjunkte Vereinigung der Bahnen von G.

Beweis. Da $X = \cup_{x \in X} Gx$ gilt, ist zu zeigen, dass für $x, y \in X$ aus $Gx \cap Gy \neq \emptyset$ schon $Gx = Gy$ folgt. Sei $z \in Gx \cap Gy$, etwa $z = a(x) = b(y)$ für $a, b \in G$. Es folgt $x = (a^{-1}b)(y)$ und somit $Gx \subseteq Gy$. Analog gilt $Gy \subseteq Gx$ und daher $Gx = Gy$. □

Definition 6.7. Sei G eine Gruppe, die auf einer Menge X operiert.

(i) Ein Element $x \in X$ heißt *Vertreter* der Bahn Gx.
(ii) Ein *Vertretersystem* einer Familie $(B_i)_{i \in I}$ paarweise disjunkter Bahnen ist eine Familie $(x_i)_{i \in I}$ mit $x_i \in B_i (B_i = Gx_i)$. Das Vertretersystem heißt *vollständig*, wenn $X = \cup_{i \in I} B_i$ gilt.

Definition 6.8. Sei G eine Gruppe, die auf einer Menge X operiert und $x \in X$. Die Untergruppe $G_x = \{a \in G \colon a(x) = x\}$ von G heißt die *Standgruppe* von x. Ist $G_x = G$, so heißt x ein *Fixpunkt* der Operation.

Lemma 6.9. Sei G eine Gruppe, die auf einer Menge X operiert und $x \in X$. Dann gilt $|Gx| = [G : G_x]$.

Beweis. Wir definieren eine bijektive Abbildung

$$\alpha \colon G/G_x \longrightarrow Gx, \ aG_x \mapsto a(x).$$

Wir zeigen:

(1) α ist wohldefiniert: Sei $aG_x = bG_x$ und daher $b^{-1}a \in G_x$. Es folgt

$$b(x) = b(b^{-1}a(x)) = (bb^{-1}a)(x) = a(x)$$

und daher $\alpha(bG_x) = \alpha(aG_x)$.

(2) α ist surjektiv: Sei $y \in Gx$ beliebig und $y = a(x)$ für ein $a \in G$. Dann ist $\alpha(aG_x) = y$.

(3) α ist injektiv: Seien $a, b \in G$ mit $\alpha(aG_x) = \alpha(bG_x)$, d.h. $a(x) = b(x)$. Es folgt $x = b^{-1}a(x)$ und somit $b^{-1}a \in G_x$. Dies ist äquivalent zu

$$aG_x = bG_x$$

und daraus folgt die Behauptung.

□

Satz 6.10. *(Bahnengleichung)* Sei G eine Gruppe, die auf einer endlichen nichtleeren Menge X operiert und $x_1, \ldots, x_n$ ein vollständiges Vertretersystem der Bahnen von G. Dann gilt:

$$|X| = \sum_{i=1}^{n} [G : G_{x_i}].$$

G ist hierbei nicht notwendigerweise endlich.

Beweis. Aus 6.6 folgt $X = \dot{\bigcup}_{i=1}^{n} Gx_i$ und daher gilt

$$|X| = \sum_{i=1}^{n} |Gx_i|.$$

Wegen 6.9 gilt $|Gx_i| = [G : G_{x_i}]$. Dann folgt

$$|X| = \sum_{i=1}^{n} |Gx_i| = \sum_{i=1}^{n} [G : G_{x_i}].$$

□

Beispiel 6.11. Dieser Satz enthält eine wichtige Methode zum Abzählen der Elemente von X. Als Beispiel wollen wir erneut den Satz von Lagrange beweisen. Sei G eine endliche Gruppe und $H \subseteq G$ eine Untergruppe. G wird die Rolle von X und H die Rolle von G in der Bahnengleichung übernehmen. H operiert auf G durch

$$H \times G \longrightarrow G, (a, b) \mapsto ba^{-1}.$$

Wir haben gesehen, dass die Bahnen gerade die Linksnebenklassen bH sind. Ein vollständiges Vertretersystem aller Bahnen wird gerade durch

$$G/H = \{b_1 H, \ldots, b_t H\}$$

gegeben. Die Standgruppen H_b sind trivial, da für $a \in H$ mit $ba^{-1} = b$ folgt, dass $a = e$. Dann ist $[H : H_b] = |H|$. Insgesamt erhalten wir

$$\mathrm{ord}(G) = |G| = |G/H||H| = [G : H]\mathrm{ord}(H).$$

Definition 6.12. Sei G eine Gruppe. Die Operation

$$G \times G \longrightarrow G, (a, x) \mapsto axa^{-1}$$

heißt *Konjugation*. Sei $x \in G$. Die Bahnen Gx der Konjugation heißt *Konjugationsklasse* von x. Die Standgruppe heißt *Zentralisator* von x und wird mit Z_x bezeichnet. Zwei Elemente $x, y \in G$ sind *konjugiert*, wenn ein $a \in G$ existiert mit $x = aya^{-1}$. Die Untergruppe

$$Z_G = \{a \in G \colon axa^{-1} = x \text{ für alle } x \in G\} = \{a \in G \colon ax = xa \text{ für alle } x \in G\}$$

heißt das *Zentrum* von G.

Bemerkung 6.13. Z_G besteht aus den Elementen von G, die mit allen Elementen von G kommutieren. Die Gruppe G ist abelsch $\Leftrightarrow G = Z_G$. Es ist

$$G_x = Z_x = \{a \in G \colon axa^{-1} = x\} = \{a \in G \colon ax = xa\}.$$

Satz 6.14. *(Klassengleichung)* Sei G eine endliche Gruppe mit Zentrum Z_G und $x_1, \ldots, x_n$ ein Vertretersystem der Bahnen in $G \setminus Z_G$ unter der Konjugation. Dann gilt:

$$\operatorname{ord}(G) = \operatorname{ord}(Z_G) + \sum_{i=1}^{n} [G : Z_{x_i}].$$

Beweis. Es gilt

$$x \in Z_G \Leftrightarrow Z_x = G \Leftrightarrow [G : Z_x] = 1 \Leftrightarrow Gx = \{x\}.$$

Sei $x_1, \ldots, x_n, y_1, \ldots, y_m$ ein vollständiges Vertretersystem der Bahnen von G unter der Konjugation mit $x_1, \ldots, x_n \in G \setminus Z_G$ und $y_1, \ldots, y_m \in Z_G$. Dann gilt nach 6.10

$$\operatorname{ord}(G) = \sum_{j=1}^{m} [G : Z_{y_j}] + \sum_{i=1}^{n} [G : Z_{x_i}] = \operatorname{ord}(Z_G) + \sum_{i=1}^{n} [G : Z_{x_i}].$$

□

Korollar 6.15. Sei p eine Primzahl und G eine Gruppe der Ordnung p^n für ein $n > 0$. Dann ist $Z_G \neq \{e\}$.

Beweis. Ist $G = Z_G$, so ist nichts zu zeigen. Sei nun $G \neq Z_G$ und $x \in G \setminus Z_G$. Da $1 < [G : Z_x]$, ist Z_x eine echte Untergruppe von G. Es folgt $[G : Z_x] | \operatorname{ord}(G) = p^n$ und daher $[G : Z_x] = p^m$ für ein $1 < m < n$. Sei nun $x_1, \ldots, x_r$ ein Vertretersystem der Bahnen in $G \setminus Z_G$ unter der Konjugation. Dann existieren Zahlen $1 < m_i < n$ mit $[G : Z_{x_i}] = p^{m_i}$. Somit

$$p^n = \operatorname{ord}(G) = \operatorname{ord}(Z_G) + \sum_{i=1}^{r} [G : Z_{x_i}] = \operatorname{ord}(Z_G) + \sum_{i=1}^{r} p^{m_i}.$$

Es folgt $p | \operatorname{ord}(Z_G)$ und daher $Z_G \neq \{e\}$. □

Zum Abschluss dieses Abschnitts wollen wir erste Existenzaussagen über Elemente bzw. Untergruppen bestimmter Ordnung beweisen.

Satz 6.16. *(Cauchy)* Sei G eine endliche abelsche Gruppe mit $p | \operatorname{ord}(G)$. Dann gibt es ein Element $a \in G$ mit $\operatorname{ord}(a) = p$.

Beweis. Wir beweisen den Satz durch eine Induktion nach $\mathrm{ord}(G)$. Ist $\mathrm{ord}(G) = p$, so folgt aus 4.7, dass $G = \langle a \rangle$ zyklisch ist mit $\mathrm{ord}(a) = p$.

Sei nun $\mathrm{ord}(G) > p$. Wähle $a \in G$ mit $a \neq e$. Gilt $p | \mathrm{ord}(a)$, so enthält $\langle a \rangle$ wegen 3.10 ein Element der Ordnung p. Wir dürfen also $p \nmid \mathrm{ord}(a)$ annehmen. Aus

$$\mathrm{ord}(G) = \mathrm{ord}(\langle a \rangle)[G : \langle a \rangle]$$

folgt dann $p | [G : \langle a \rangle]$. Nun ist G abelsch, also $\langle a \rangle \triangleleft G$. Daher ist $G/\langle a \rangle$ eine Gruppe mit

$$\mathrm{ord}(G/\langle a \rangle) = [G : \langle a \rangle] < \mathrm{ord}(G).$$

Nach der Induktionsannahme existiert ein $b \in G$ mit $\mathrm{ord}(\overline{b}) = p$ in $G/\langle a \rangle$. Sei $m = \mathrm{ord}(b)$. Da $\overline{b}^m = \overline{b^m} = \overline{e}$, folgt, dass $p = \mathrm{ord}(\overline{b})$ die Zahl m teilt. Daher ist $\langle b \rangle \subseteq G$ eine zyklische Gruppe, deren Ordnung von p geteilt wird. Wieder nach 3.10 existiert dann ein Element der Ordnung p in G. □

Nicht zu jedem Teiler d einer Gruppenordnung existiert eine Untergruppe der Ordnung d. Hat der Teiler eine spezielle Gestalt, so ist dies jedoch der Fall.

Satz 6.17. Sei G eine endliche Gruppe, p eine Primzahl mit $p^m | \mathrm{ord}(G)$. Dann existiert eine Untergruppe der Ordnung p^m in G.

Beweis. Der Beweis erfolgt durch eine Induktion nach $\mathrm{ord}(G)$. Der Fall $m = 0$ ist trivial (wähle $\{\mathrm{e}\}$), sei also $m > 0$. Die kleinste in Frage kommende Ordnung von G ist p. Dann ist G selbst die gesuchte Untergruppe. Sei nun $\mathrm{ord}(G) > p$. Wir betrachten zwei Fälle

(i) $p | \mathrm{ord}(Z_G)$,
(ii) $p \nmid \mathrm{ord}(Z_G)$.

(i) Aus 6.16 folgt, dass ein Element $a \in Z_G$ existiert mit $\mathrm{ord}(a) = p$. Da $Z_G \triangleleft G$, ist auch $\langle a \rangle \triangleleft G$. Ferner gilt

$$\mathrm{ord}(G/\langle a \rangle) = [G : \langle a \rangle] = \frac{\mathrm{ord}(G)}{\mathrm{ord}\langle a \rangle} < \mathrm{ord}(G)$$

und $p^{m-1} | \mathrm{ord}(G/\langle a \rangle)$. Nach der Induktionsvoraussetzung existiert eine Untergruppe $\overline{H} \subseteq G/\langle a \rangle$ mit $\mathrm{ord}(\overline{H}) = p^{m-1}$. Sei $\varepsilon \colon G \longrightarrow G/\langle a \rangle$ der kanonische Epimorphismus und $H = \varepsilon^{-1}(\overline{H})$. Aus 4.22 folgt, dass

$$\mathrm{ord}(H) = \mathrm{ord}(\overline{H})\mathrm{ord}(\mathrm{Ker}(\varepsilon)) = p^m.$$

(ii) Betrachte die Konjugation auf G ($G \times G \longrightarrow G, (a, x) \mapsto axa^{-1}$). Sei $x_1, \ldots, x_n$ ein Vertretersystem der Bahnen (Konjugationsklassen) in $G \setminus Z_G$. Dann gilt die Klassengleichung 6.14

$$\mathrm{ord}(G) = \mathrm{ord}(Z_G) + \sum_{i=1}^{n} [G : Z_{x_i}]$$

und $1 < \mathrm{ord}(Z_{x_i}) < \mathrm{ord}(G)$. Da $p | \mathrm{ord}(G)$ und $p \nmid \mathrm{ord}(Z_G)$, existiert ein i mit $p \nmid [G : Z_{x_i}]$. Aus

$$\mathrm{ord}(G) = [G : Z_{x_i}]\mathrm{ord}(Z_{x_i})$$

folgt, dass $p^m | \text{ord}(Z_{x_i})$. Die Induktionsvoraussetzung auf Z_{x_i} angewendet liefert die Behauptung. □

Definition 6.18. Sei G eine endliche Gruppe mit $\text{ord}(G) = p^n m$ und $p \nmid m$. Eine Untergruppe $H \subseteq G$ heißt eine *p-Sylowuntergruppe* von G, wenn $\text{ord}(H) = p^n$ gilt.

Aus 6.17 folgt, dass stets eine p-Sylowuntergruppe existiert. Der Satz 6.17 ist Teil der so genannten Sylow-Sätze, die sich mit den p-Sylowuntergruppen beschäftigen. Durch diese Sätze können einige wichtige strukturelle Aussagen über Gruppen gemacht werden.

7. Permutationsgruppen

Sei stets $n \in \mathbb{N}$. In diesem Abschnitt untersuchen wir die Gruppe S_n. Wir lassen das Zeichen $\circ$ bei der Komposition von Permutationen meist aus. Man zeigt leicht, dass S_n eine Gruppe mit $\text{ord}(S_n) = n!$ ist. In diesem Abschnitt werden wir die Struktur dieser Gruppe genauer studieren.

Definition 7.1. Für $r \in \mathbb{N}$, $r \geq 2$ heißt ein $\sigma \in S_n$ ein *r-Zyklus*, wenn es natürliche Zahlen $j_1, \ldots, j_r$ gibt mit $\sigma(j_i) = j_{i+1}$ für $i = 1, \ldots, r-1$, $\sigma(j_r) = j_1$ und $\sigma(k) = k$ für $k \in \{1, \ldots, n\} \setminus \{j_1, \ldots, j_r\}$. Ein solcher Zyklus wird

$$(j_1, \ldots, j_r)$$

geschrieben. 2-Zyklen heißen auch *Transpositionen*.

Bemerkung 7.2. Es gilt:

(i) Eine Transposition (i, j) vertauscht i und j und lässt alle anderen Zahlen aus $\{1, \ldots, n\}$ fest. Es ist $(i, j)^{-1} = (i, j)$ und $(i, j)^2 = id$.
(ii) Sei $\sigma = (j_1, \ldots, j_r)$ ein r-Zyklus. Dann gilt

$$\text{ord}(\sigma) = r \text{ und } \sigma^{-1} = (j_r, \ldots, j_1).$$

Für ein $\tau \in S_n$ rechnet man nach, dass

$$\tau\sigma\tau^{-1} = (\tau(j_1), \ldots, \tau(j_r))$$

gilt.

Definition 7.3. Zwei Permutationen $\sigma, \tau \in S_n$ heißen *disjunkt*, wenn alle Zahlen, die bei σ bzw. τ bewegt werden, bei τ bzw. σ fest bleiben.

Bemerkung 7.4. Es ist:

(i) Z.B. sind $(1, 2)$ und $(3, 4)$ disjunkt, aber $(1, 2)$ und $(2, 3)$ nicht.
(ii) Sind $\sigma, \tau \in S_n$ disjunkt, so gilt $\sigma\tau = \tau\sigma$.

Satz 7.5. Jede Permutation $\sigma \in S_n$ lässt sich eindeutig (bis auf Reihenfolge der Faktoren) als Produkt paarweise disjunkter Zyklen zerlegen. Diese Zerlegung heißt die *Zyklenzerlegung* von σ.

Beweis. Sei $H = \langle \sigma \rangle \subseteq S_n$. Dann operiert H auf $\{1, \ldots, n\}$.

Existenz der Zerlegung: Seien $B_1, \dots, B_l$ die Bahnen der Operation von H mit $|B_i| > 1$ für $i = 1, \dots, l$. Definiere

$$\sigma_i(x) = \begin{cases} \sigma(x) \in B_i & \text{für } x \in B_i, \\ x & \text{für } x \notin B_i. \end{cases}$$

Dann gilt $\sigma_i \in S_n$. Da die Bahnen paarweise disjunkt sind folgt, dass auch die σ_i paarweise disjunkt sind. Ferner gilt per Definition

$$\sigma = \sigma_1 \cdots \sigma_l.$$

Nun muss noch gezeigt werden, dass die σ_i Zyklen sind. Sei $|B_i| = r_i$ und $m > 0$ die kleinste Zahl mit $\sigma^m(x) = x$ für ein $x \in B_i$. Dann sind

$$x = \sigma^0(x), \sigma(x), \dots, \sigma^{m-1}(x)$$

paarweise verschieden und für jedes $n \in \mathbb{Z}$ ist $\sigma^n(x) = \sigma^j(x)$ für ein $j \in \{0, \dots, m-1\}$. Daher gilt

$$B_i = \{x, \sigma(x), \dots, \sigma^{m-1}(x)\}$$

und $m = r_i$. Ferner ist σ_i der r_i-Zyklus

$$(x, \sigma(x), \dots, \sigma^{r_i-1}(x)).$$

Eindeutigkeit: Sei

$$\sigma = \sigma'_1 \cdots \sigma'_k.$$

eine weitere Zerlegungen von σ in ein Produkt paarweise disjunkter Zyklen. Wir beweisen die Aussage durch eine Induktion nach $m = \min\{l, k\}$. Ist $m = 0$, so ist $\sigma = \mathrm{id}_{S_n}$ und die Behauptung ist trivial. Sei nun $m > 0$. Wähle $x \in \{1, \dots, n\}$ mit $\sigma(x) \neq x$. Dann muss $x \in B_i$ für ein i gelten. Ferner existiert ein eindeutiges $j \in \{1, \dots, k\}$ mit $\sigma'_j(x) \neq x$. Ist

$$\sigma'_j = (j'_1, \dots, j'_{r'_j}),$$

dann muss $\{j'_1, \dots, j'_{r'_j}\}$ die Bahn von x sein, da alle anderen σ'_l das Element x festhalten. Also $B_i = \{j'_1, \dots, j'_{r'_j}\}$. Dies bedeutet aber $\sigma'_j = \sigma_i$. Betrachte

$$\begin{aligned} \sigma\sigma_i^{-1} &= \sigma_1 \cdots \sigma_{i-1}\sigma_{i+1} \cdots \sigma_l \\ &= \sigma'_1 \cdots \sigma'_{j-1}\sigma'_{j+1} \cdots \sigma'_k. \end{aligned}$$

Nach der Induktionsannahme hat $\sigma\sigma_i^{-1}$ eine eindeutige Zyklenzerlegung und es folgt nach einer eventuellen Umnummerierung $l = k$ und $\sigma_j = \sigma'_j$ für $j = 1, \dots, l$. □

Beispiel 7.6. Sei

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

Dann hat σ die Zyklenzerlegung

$$(1, 4, 2, 7)(3, 5)(6).$$

Man schreibt dann $\sigma = (1, 4, 2, 7)(3, 5)(6)$. Beachte, dass $(6) = \mathrm{id}$, daher lässt man oft die 1-Zyklen weg und

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

Es gilt $\sigma = \pi_1\pi_2$ mit $\pi_1 = (1, 4, 2, 7)$ und $\pi_2 = (3, 5)$.

Satz 7.7. S_n wird von $A = \{(k, k+1) \colon k = 1, \ldots, n-1\}$ erzeugt, d.h. jedes $\sigma \in S_n$ ist Produkt von Transpositionen vom Typ $(k, k+1)$.

Beweis. Wegen 7.5 reicht es, die Behauptung für Zyklen zu beweisen. Sei $(j_1, \ldots, j_r) \in S_n$ ein beliebiger Zyklus. Dann gilt

$$(j_1, \ldots, j_r) = (j_1, j_2)(j_2, j_3) \cdots (j_{r-1}, j_r).$$

Also müssen wir die Behauptung für einen Zyklus vom Typ (i, j) beweisen. Sei o.E. $i < j$. Wir beweisen dies durch eine Induktion nach $j - i$. Für $j - i = 1$ ist nichts zu zeigen. Sei $j - i > 1$. Es gilt

$$(i, j) = (i, j-1)(j-1, j)(i, j-1).$$

$(j-1, j)$ ist vom gewünschten Typ. Nach der Induktionsannahme ist $(i, j-1)$ ebenfalls Produkt von Transpositionen aus A und somit auch (i, j). □

Die folgende Abbildung ist aus der linearen Algebra bekannt.

Definition 7.8. Sei $\sigma \in S_n$. Die Abbildung

$$\operatorname{sign}(\sigma) = \prod_{1 \le j < i \le n} \frac{\sigma(i) - \sigma(j)}{i - j} \in \{1, -1\}$$

heißt das *Signum* von σ. Ist $j < i$, aber $\sigma(j) > \sigma(i)$, so heißt (j, i) ein *Fehlstand* von σ. Ist $\operatorname{sign}(\sigma) = 1$ bzw. $\operatorname{sign}(\sigma) = -1$, dann heißt σ eine *gerade* bzw. *ungerade* Permutation.

Beispiel 7.9. Sei $\tau = (i, j) \in S_n$ eine Transposition, dann gilt $\operatorname{sign}(\tau) = -1$.

Satz 7.10. Sei $\sigma, \tau \in S_n$ beliebig. Dann gilt $\operatorname{sign}(\sigma\tau) = \operatorname{sign}(\sigma) \cdot \operatorname{sign}(\tau)$.

Beweis. Es gilt

$$\begin{aligned}\operatorname{sign}(\sigma\tau) &= \prod_{j<i} \frac{\sigma(\tau(i)) - \sigma(\tau(j))}{i - j} = \prod_{j<i} \frac{\sigma(\tau(i)) - \sigma(\tau(j))}{\tau(i) - \tau(j)} \prod_{j<i} \frac{\tau(i) - \tau(j)}{i - j} \\ &= \prod_{j<i} \frac{\sigma(\tau(i)) - \sigma(\tau(j))}{\tau(i) - \tau(j)} \cdot \operatorname{sign}(\tau) = \operatorname{sign}(\sigma) \cdot \operatorname{sign}(\tau).\end{aligned}$$

□

Korollar 7.11. Es gilt:

(i) Ist $\sigma \in S_n$ Produkt von m Transpositionen, dann

$$\operatorname{sign}(\sigma) = (-1)^m.$$

(ii) Ist σ ein r-Zyklus, dann ist $\operatorname{sign}(\sigma) = (-1)^{r-1}$.

Beweis. Zu (i): Dies ist nun trivial.

Zu (ii): Ist $\sigma = (j_1, \ldots, j_r) \in S_n$, dann gilt

$$(j_1, \ldots, j_r) = (j_1, j_2)(j_2, j_3) \cdots (j_{r-1}, j_r).$$

Die Behauptung folgt nun aus (i). □

Korollar 7.12. Die Abbildung

$$\operatorname{sign}\colon S_n \longrightarrow \{1,-1\}, \quad \sigma \mapsto \operatorname{sign}(\sigma)$$

ist ein Gruppenhomomorphismus.

Definition 7.13. Die Menge

$$A_n = \{\sigma \in S_n \colon \operatorname{sign}(\sigma) = 1\}$$

der geraden Permutationen heißt die *alternierende Gruppe* n-ten Grades.

Bemerkung 7.14. Es gilt:

(i) A_n ist ein Normalteiler von S_n, da A_n der Kern eines Gruppenhomomorphismus ist.
(ii) Für $n > 1$ gilt $S_n/A_n \cong \{1,-1\}$. Daher folgt

$$[S_n : A_n] = 2, \quad \operatorname{ord}(A_n) = \frac{1}{2}n!.$$

Ein wesentliches Ziel der Gruppentheorie ist es, die Struktur von endlichen Gruppen aus möglichst wenigen einfachen Gruppen aufzubauen.

Definition 7.15. Eine Gruppe G heißt *einfach*, wenn G und $\{e\}$ die einzigen Normalteiler von G sind.

Einer der schwierigsten Sätze in der Mathematik ist der Klassifikationssatz für die endlichen einfachen Gruppen. Zum Abschluss dieses Abschnitts zeigen wir folgendes:

Satz 7.16. Für $n \neq 4$ ist A_n einfach.

Lemma 7.17. Seien $a, b \in \{1,\dots,n\}$ verschiedene Zahlen. Für $n \geq 3$ wird A_n von den Dreierzyklen (a,b,k) mit $k \in \{1,\dots,n\}$, $k \neq a,b$ erzeugt.

Beweis. Sei $\sigma \in A_n$. Dann ist σ gerade und daher Produkt von Elementen der Form $(i,j)(k,l)$ und $(i,j)(i,k)$ mit paarweise verschiedenen $i,j,k,l \in \{1,\dots,n\}$ (sofern dies möglich ist). Es ist

$$(i,j)(k,l) = (i,k,j)(i,k,l) \text{ und } (i,j)(i,k) = (i,k,j).$$

Damit ist bereits gezeigt, dass A_n von Dreierzyklen erzeugt wird.

A_3 wird von $(1,2,3)$ erzeugt, daher gilt die Aussage für $n = 3$. Sei nun $n > 3$. Ein beliebiger Dreierzyklus enthält von den Zahlen a, b keine, eine oder beide. Für Dreierzyklen, die nicht von der Form (a,b,k) sind, gelten folgende Formeln:

$$(a,u,b) = (a,b,u)^2,$$

$$(a,u,v) = (a,b,v)(a,b,u)^2, \ (b,u,v) = (a,b,v)^2(a,b,u),$$

$$(u,v,x) = (a,b,u)^2(a,b,x)(a,b,v)^2(a,b,u).$$

Dies beweist die Behauptung. □

Lemma 7.18. Ist $n \geq 3$ und $H \triangleleft A_n$, welcher einen Dreierzyklus enthält, dann ist $H = A_n$.

Beweis. Sei $(a,b,c) \in H$. Für $k \neq a,b,c$ gilt

$$(a,b,k) = (a,b)(c,k)(a,b,c)^2(c,k)(a,b) = [(a,b)(c,k)](a,b,c)^2[(a,b)(c,k)]^{-1} \in H,$$

da H ein Normalteiler ist. Nach 7.17 erzeugen diese Element A_n und somit $A_n = H$. □

Beweis. 7.16 Es ist $|A_1| = |A_2| = 1$ und $|A_3| = 3$. Daher sind A_1, A_2, A_3 einfach. Sei nun $n > 4$ und $\{\mathrm{id}\} \neq H \triangleleft A_n$. Wir müssen zeigen, dass $H = A_n$ gilt. Da die Elemente von A_n die geraden Permutationen sind, werden bei jedem $\mathrm{id} \neq \sigma \in A_n$ mindestens 3 Zahlen bewegt. Wir unterscheiden folgende Fälle

(i) H enthält ein Dreierzyklus.
(ii) Es existiert ein $\sigma \in H$, welches genau 4 Zahlen permutiert und keine Permutation, die weniger als 4 Zahlen permutiert.
(iii) Alle $\sigma \in H$ permutieren mehr als 4 Zahlen.

(i) Aus 7.18 folgt, dass $H = A_n$.

(ii) σ muss von der Form $(a,b)(c,d)$ mit paarweise verschiedenen Zahlen a,b,c,d sein. Sei $e \in \{1,\dots,n\} \setminus \{a,b,c,d\}$. Dies ist wegen $n \geq 5$ möglich. Definiere

$$\tau = (c,d,e)$$

Es ist

$$\sigma' = (a,b)(d,e) = \tau\sigma\tau^{-1} \in H,$$

da H ein Normalteiler ist. Nun folgt

$$\sigma\sigma' = (c,d,e) \in H$$

und dies ist ein Widerspruch zur Voraussetzung in (ii). Dieser Fall kann also nicht auftreten.

(iii) Jede Permutation aus H bewegt nun mehr als 4 Zahlen. Wähle ein $\sigma \in H$, welches am wenigsten Zahlen permutiert (dies muss nicht eindeutig sein). Wir müssen wieder eine Fallunterscheidung machen. Bei der Zyklenzerlegung schreiben wir den längsten Zyklus zuerst:

(a) $\sigma = (a,b,c,d,\dots)\dots$,
(b) $\sigma = (a,b,c)(d,e,\dots)\dots$,
(c) $\sigma = (a,b)(c,d)(e,f)\dots$.

Mit $\tau = (b,c,d)$ erhält man für $\sigma' = \tau\sigma\tau^{-1} \in H$ in den drei Fällen

(a) $\sigma' = (a,c,d,b,\dots)\dots$,
(b) $\sigma' = (a,c,d)(b,e,\dots)\dots$,
(c) $\sigma' = (a,c)(d,b)(e,f)\dots$.

Es ist $\sigma' \neq \sigma$ und

$$(\sigma')^{-1}\sigma = \tau\sigma^{-1}\tau^{-1}\sigma \in H$$

hält in den Fällen (a), (c) alle Zahlen aus $\{1,\dots,n\} \setminus \{a,b,c,d\}$ und im Fall (b) alle Zahlen aus $\{1,\dots,n\} \setminus \{a,b,c,d,e\}$ fest. Im Fall (b) muss σ aber mehr als 5 Zahlen bewegt haben, da σ gerade ist. Das heißt, in jedem Fall haben wir eine Permutation in H gefunden, die weniger Zahlen permutiert als σ. Dies ist ein Widerspruch zur Wahl von σ und daher kann der Fall (iii) nicht auftreten.

Insgesamt haben wir damit den Satz bewiesen. □

KAPITEL 2

Ringtheorie

1. Ringe

$\mathbb{Z}$ ist mit $+$ und $\cdot$ ein vertrautes mathematisches Objekt; ein Ring, wie wir sehen werden. In $\mathbb{Z}$ sind Begriffe wie Teiler oder Primzahl bekannt. Ein Ziel dieses Kapitels ist es, allgemein Ringe einzuführen und die gewohnten Rechenregeln sinnvoll zu verallgemeinern.

Definition 1.1. Ein *Ring* ist eine Menge R zusammen mit zwei Verknüpfungen $+\colon R \longrightarrow R$ (Addition) und $\cdot\colon R \longrightarrow R$ (Multiplikation), so dass folgende Bedingungen erfüllt sind:

(i) $(R, +)$ ist eine abelsche Gruppe mit neutralem Element 0.
(ii) $(R, \cdot)$ ist ein Monoid mit neutralem Element 1.
(iii) Es gelten die Distributivgesetze, d.h. für alle $a, b, c \in R$ gilt $a(b+c) = ab+ac$ und $(b + c)a = ba + ca$.

Der Ring heißt *kommutativ*, wenn für alle $a, b \in R$ gilt $ab = ba$. Man schreibt $(R, +, \cdot)$ oder R für den Ring.

Bemerkung 1.2. Beachte:

(i) In der Algebra werden auch Ringe ohne 1 betrachtet. Im Teil (ii) der Definition wird die Existenz des Einselements dann nicht gefordert. Wir verzichten auf diesen Teil der Theorie.
(ii) In einem Ring kann auch $1 = 0$ gelten. Dies ist genau dann der Fall, wenn $R = \{0\}$ gilt. Wir betrachten im Folgenden nur Ringe mit $1 \neq 0$.
(iii) Zur Vermeidung von Klammern vereinbart man, dass die Multiplikation stärker in einem Ring bindet als die Addition (z.B. bedeutet dann $ab+cd = (ab) + (cd)$).
(iv) Vorsicht, es gilt nicht in jedem Ring die Kürzungsregel.

Folgende Beweise verlaufen vollkommen analog zu den entsprechenden Beweisen für Körper aus der linearen Algebra.

Lemma 1.3. Sei R ein Ring und $a, b \in R$. Es gelten die Rechenregeln:

(i) $0a = a0 = 0$,
(ii) $a(-b) = -ab = (-a)b$,
(iii) $(-a)(-b) = ab$.

Definition 1.4. Sei R ein Ring.

(i) Ein Element $a \in R$ heißt *Einheit*, wenn ein $b \in R$ existiert mit $ab = ba = 1$.
(ii) Die Menge der Einheiten R^* von R bildet hinsichtlich der Multiplikation eine Gruppe. Sie heißt die *Einheitengruppe* von R.

(iii) Gilt $R^* = R \setminus \{0\}$, so heißt R ein *Schiefkörper*. Ist R ein kommutativer Schiefkörper, so heißt R ein *Körper*.

Beispiele 1.5. Betrachte:

(i) $(\mathbb{Z}, +, \cdot)$ ist ein Ring mit $\mathbb{Z}^* = \{-1, 1\}$.

(ii) Für $m \in \mathbb{N}$ haben wir schon gesehen, dass $(\mathbb{Z}/m\mathbb{Z}, +)$ eine abelsche Gruppe ist. Auf $\mathbb{Z}/m\mathbb{Z}$ lässt sich auch ein Produkt definieren durch

$$\cdot\colon \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z} \longrightarrow \mathbb{Z}/m\mathbb{Z},\ (\overline{r}, \overline{s}) \mapsto \overline{rs}.$$

Nun muss wieder gezeigt werden, dass diese Verknüpfung wohldefiniert ist und $(\mathbb{Z}/m\mathbb{Z}, +, \cdot)$ tatsächlich ein Ring ist (Übungsaufgabe).

(iii) Die Menge aller $n \times n$-Matrizen $\mathrm{M}(n \times n; K)$ mit Koeffizienten in einem Körper K zusammen mit der Matrizenaddition und Matrizenmultiplikation ist ein Ring R. Dieser ist für $n \geq 2$ nicht kommutativ. Es gilt

$$R^* = \{A \in \mathrm{M}(n \times n; K)\colon \det(A) \neq 0\} = \mathrm{GL}(n; K).$$

(iv) Ist K ein Körper, so ist der Polynomring $K[X]$ ein Ring. Diesen werden wir in einem späteren Kapitel noch gründlich diskutieren.

Definition 1.6.

(i) Ein Element a in einem Ring R heißt *Nullteiler*, wenn ein $0 \neq b \in R$ existiert mit $ab = 0$ oder $ba = 0$. Der Ring R heißt *nullteilerfrei*, wenn R keine Nullteiler außer 0 besitzt.

(ii) Ein kommutativer, nullteilerfreier Ring $R \neq 0$ heißt ein *Integritätsbereich* (oder Integritätsring).

Beispiele 1.7. Betrachte:

(i) $\mathbb{Z}$ ist ein Integritätsbereich.

(ii) In dem Ring $\mathrm{M}(n \times n; K)$ existieren von 0 verschiedene Nullteiler (Überlegen Sie sich ein Beispiel).

Satz 1.8. Ein kommutativer Ring R ist genau dann ein Integritätsbereich, wenn in ihm die Kürzungsregel:

$$ab = ac,\ a \neq 0 \Rightarrow b = c$$

gilt.

Beweis. Sei R ein Integritätsbereich. Dann gilt

$$ab = ac \Leftrightarrow a(b - c) = 0 \Rightarrow b - c = 0 \Leftrightarrow b = c.$$

Ist R kein Integritätsbereich, so existieren $0 \neq a, b \in R$ mit $ab = 0$. Dann ist die Kürzungsregel wegen $ab = 0 = a0$ und $b \neq 0$ verletzt. □

Satz 1.9. Sei R ein Integritätsbereich mit endlich vielen Elementen. Dann ist R ein Körper.

Beweis. Sei $0 \neq a \in R$ beliebig. Die Abbildung $\varphi_a\colon R \longrightarrow R, b \mapsto ab$ ist injektiv, da R ein Integritätsbereich ist. Da $|R| < \infty$ folgt, dass φ_a bijektiv ist. Somit $1 \in \mathrm{Im}(\varphi_a)$, d.h. es existiert ein $b \in R$ mit $1 = ba$. Dies zeigt die Behauptung. □

Definition 1.10. Eine Teilmenge S eines Rings R heißt ein *Unterring* von R, wenn

(i) $1_R \in S$.
(ii) S mit den induzierten Verknüpfungen von R ein Ring ist.

Das Paar $S \subseteq R$ heißt dann eine *Ringerweiterung*.

Bemerkung 1.11. Eine Menge S ist genau dann ein Unterring von einem Ring R, wenn $1_R \in S$ und für alle $a, b \in R$ gilt $a - b, ab \in S$. Z. B. ist $\mathbb{Z}$ der einzige nicht triviale Unterring von $\mathbb{Z}$. Jeder Körper K ist Unterring des Polynomrings $K[X]$.

Satz 1.12. Seien $R_1, \ldots, R_n$ Ringe. Dann ist $R = R_1 \times \cdots \times R_n$ mit komponentenweiser Addition und Multiplikation ein Ring, d.h.

$$(a_1, \ldots, a_n) + (b_1, \ldots, b_n) = (a_1 + b_1, \ldots, a_n + b_n),$$

$$(a_1, \ldots, a_n) \cdot (b_1, \ldots, b_n) = (a_1 b_1, \ldots, a_n b_n).$$

Es gilt $1_R = (1_{R_1}, \ldots, 1_{R_n})$, $0_R = (0_{R_1}, \ldots, 0_{R_n})$ und $R^* = R_1^* \times \cdots \times R_n^*$. Wir nennen R das *direkte Produkt* der Ringe $R_1, \ldots, R_n$.

Beweis. Dies ist leicht zu zeigen und der Beweis ist dem Leser überlassen. □

Beachte, dass für $n \geq 2$ R kein Integritätsbereich ist, da z.B.

$$(0, 1, 0, \ldots)(1, 0, 0, \ldots) = (0, 0, 0, \ldots).$$

gilt.

Definition 1.13. Sei R ein Ring. Für ein Element $a \in R$ bezeichnen wir mit $\mathrm{ord}_+(a)$ die Ordnung des Elements a in der Gruppe $(R, +)$. Sei nun R ein Integritätsbereich. Die Zahl

$$\mathrm{char}(R) = \begin{cases} 0, & \text{falls } \mathrm{ord}_+(a) = \infty \text{ für alle } 0 \neq a \in R, \\ \min\{\mathrm{ord}_+(a) \colon 0 \neq a \in R\} & \text{sonst.} \end{cases}$$

heißt die *Charakteristik* von R.

Satz 1.14. Die Charakteristik eines Integritätsbereichs R ist entweder 0 oder eine Primzahl. Ist $\mathrm{char}(R) > 0$, dann gilt $\mathrm{char}(R) = \mathrm{ord}_+(1_R)$ und $\mathrm{char}(R)a = 0$ für alle $a \in R$.

Beweis. Beachte, dass $\mathrm{char}(R) \neq 1$ ist. Sei $\mathrm{char}(R) = p > 0$. Dann existiert ein $0 \neq a \in R$ mit $pa = 0$. Angenommen, dass $p = mn$ mit $0 \neq n, m \in \mathbb{N}$. Dann gilt

$$0 = pa = (mn)a = m(na).$$

Ist $n \neq 1$, so folgt aus der Definition der Charakteristik, dass $m = 1$ und $n = p$ gilt. Daher ist p eine Primzahl. Es ist

$$0 = pa = p(1_R \cdot_R a) = (p1_R) \cdot_R a.$$

Da R ein Integritätsbereich und $a \neq 0$ ist, gilt $p1_R = 0$. Daher ist $\mathrm{char}(R) = \mathrm{ord}_+(1_R)$. Dann gilt auch $pb = p(1_R \cdot_R b) = (p1_R) \cdot_R b = 0$ für alle $b \in R$. □

Beispiel 1.15. Die Ringe $\mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}$ sind alles Integritätsbereiche der Charakteristik 0.

Da ein Integritätsbereich mit Charakteristik 0 immer unendlich viele Elemente hat, ist jeder endliche Körper ein Integritätsbereich mit Primzahlcharakteristik. Zum

Beispiel ist der aus der L.A. bekannte Körper $\mathbb{F}_2$ mit zwei Elementen von diesem Typ.

Definition 1.16. Seien R und S Ringe. Eine Abbildung $\varphi\colon R \longrightarrow S$ heißt ein *Ringhomomorphismus*, wenn für alle $a, b \in R$ gilt

$$\varphi(a+b) = \varphi(a) + \varphi(b), \quad \varphi(ab) = \varphi(a)\varphi(b) \text{ und } \varphi(1_R) = 1_S.$$

Ein Ringhomomorphismus φ heißt

(i) *Monomorphismus*, wenn φ injektiv ist,
(ii) *Epimorphismus*, wenn φ surjektiv ist, und
(iii) *Isomorphismus*, wenn φ bijektiv ist.

Die Ringe R, S sind *isomorph*, wenn φ ein Isomorphismus ist. Man schreibt dann $R \cong S$.

Bemerkung 1.17. Ein Ringhomomorphismus ist ein Gruppenhomomorphismus bzgl. der Addition und ein Monoidhomomorphismus bzgl. der Multiplikation.

Beispiele 1.18. Betrachte:

(i) Die Identität $\mathrm{id}_R\colon R \longrightarrow R,\ a \mapsto a$ ist ein Ringhomomorphismus.
(ii) Die Komposition von Ringhomomorphismen ist wieder ein Ringhomomorphismus.
(iii) Die Umkehrabbildung eines Isomorphismus ist wieder ein Isomorphismus.
(iv) Sei V ein n-dimensionaler K-Vektorraum über einem Körper K mit Basis $v_1, \ldots, v_n$. Die Menge der Endomorphismen $\mathrm{End}(V)$ zusammen mit der Addition $+$ von Endomorphismen und der Verknüpfung $\circ$ von Endomorphismen ist ein Ring (Nullelement ist die Nullabbildung, Einselement die Identität). Wie wir schon gesehen haben, ist auch $(M(n \times n; K), +, \cdot)$ ein Ring. Jedem Endomorphismus wird nun seine Matrix bzgl. der Basis $v_1, \ldots, v_n$ zugeordnet. Diese Abbildung ist mit der Multiplikation und Addition verträglich und stellt sich als ein Isomorphismus $\mathrm{End}(V) \longrightarrow M(n \times n; K)$ heraus.

Definition 1.19. Seien R, S Ringe und $\varphi\colon R \longrightarrow S$ ein Ringhomomorphismus.

(i) Die Menge $\mathrm{Ker}(\varphi) = \{a \in R\colon \varphi(a) = 0\}$ heißt der *Kern* von φ.
(ii) Die Menge $\mathrm{Im}(\varphi) = \{\varphi(a) \in S\colon a \in R\}$ heißt das *Bild* von φ.

Bemerkung 1.20. Es gilt:

(i) $\mathrm{Im}(\varphi)$ ist ein Unterring von S.
(ii) $\mathrm{Ker}(\varphi)$ ist i.A. kein Unterring von R, da i.A. $1 \notin \mathrm{Ker}(\varphi)$.
(iii) φ ist genau dann injektiv, wenn $\mathrm{Ker}(\varphi) = \{0\}$.
(iv) φ induziert einen Gruppenhomomorphismus $R^* \longrightarrow S^*$ zwischen den Einheitengruppen von R und S.

Zwar ist $\mathrm{Ker}(\varphi)$ kein Unterring, aber $(\mathrm{Ker}(\varphi), +)$ ist eine Untergruppe von $(R, +)$. Man überlegt sich leicht, dass für $a \in \mathrm{Ker}(\varphi)$ und $b \in R$ gilt $ba, ab \in \mathrm{Ker}(\varphi)$, denn

$$\varphi(ab) = \varphi(a)\varphi(b) = 0 = \varphi(b)\varphi(a) = \varphi(ba).$$

Diese beiden Eigenschaften charakterisieren Ideale in einem Ring, die eine ähnlich wichtige Bedeutung wie Normalteiler in Gruppen haben.

Definition 1.21. Sei R ein Ring. Eine Teilmenge $I \subseteq R$ heißt ein (zweiseitiges) *Ideal*, wenn:

(i) $(I, +)$ ist eine Untergruppe von $(R, +)$.
(ii) Für alle $a \in R$ und $b \in I$ gilt $ab, ba \in I$.

Beispiele 1.22. Sei R ein Ring.

(i) $\{0\}$ und R sind die trivialen Ideale von R.
(ii) R ist genau dann ein Körper, wenn $\{0\}$ und R die einzigen Ideale von R sind.
(iii) Sei S ein weiterer Ring und $\varphi\colon R \longrightarrow S$ ein Ringhomomorphismus. Dann ist $\mathrm{Ker}(\varphi)$ ein Ideal von R. Ist insbesondere R ein Körper, so ist φ injektiv.
(iv) Seien R, S wie in (iii). Für ein Ideal $I \subseteq R$ ist i.A. $\varphi(I)$ kein Ideal. Dies gilt nur, wenn φ surjektiv ist. Ist jedoch $J \subseteq S$ ein Ideal, so gilt immer, dass $\varphi^{-1}(J)$ ein Ideal in R ist.
(v) Genau die Mengen $n\mathbb{Z}$ sind die Ideale von $\mathbb{Z}$.
(vi) In einem kommutativen Ring lässt sich die Bedingung (ii) der Definition abschwächen zu: $(*)$ Für alle $a \in R$ und $b \in I$ gilt $ab \in I$.

Im Allgemeinen ist dies jedoch eine schwächere Bedingung. Zum Beispiel genügt die Menge

$$J = \{(a_{ij}) \in \mathrm{M}(2 \times 2; \mathbb{R})\colon a_{12} = a_{22} = 0\}$$

$(*)$, ist aber kein Ideal in $\mathrm{M}(2 \times 2; \mathbb{R})$.

Lemma und Definition 1.23. Sei R ein Ring und $(J_i)_{i \in I}$ eine Familie von Idealen von R. Dann gilt:

(i) Der *Durchschnitt* $\bigcap_{i \in I} J_i$ ist ein Ideal von R.
(ii) Die *Summe* $\sum_{i \in I} J_i = \{\sum_{i \in I} a_i\colon a_i \in J_i,\ \text{fast alle } a_i = 0\}$ ist ein Ideal von R. (Fast alle heißt hier: alle bis auf endlich viele.)

Definition 1.24. Sei R ein Ring und $M \subseteq R$ eine Teilmenge. Das kleinste Ideal $I(M)$ von R, welches M enthält, heißt das von M erzeugte Ideal:

$$I(M) = \bigcap_{M \subseteq J \subseteq R \text{ Ideal}} J.$$

M heißt dann ein *Erzeugendensystem* von dem Ideal $I(M)$. Wird $I(M)$ von $a_1, \ldots, a_n \in R$ erzeugt, so schreibt man $I(M) = (a_1, \ldots, a_n)$. Ist $M = \{a\}$ einelementig, so heißt $I(M)$ ein *Hauptideal*.

Lemma 1.25. Sei R ein Ring und $M \subseteq R$. Dann gilt

$$I(M) = \{\sum_{i=1}^{n} r_i a_i s_i\colon r_i, s_i \in R,\ a_i \in M,\ n \in \mathbb{N}\}.$$

Ist R kommutativ, so ist

$$I(M) = \{\sum_{i=1}^{n} r_i a_i\colon r_i \in R,\ a_i \in M,\ n \in \mathbb{N}\}.$$

Ist $M = \{a_1, \ldots, a_n\}$ endlich und R kommutativ, so verwenden wir auch die Schreibweise

$$I(M) = (a_1, \ldots, a_n) = Ra_1 + \cdots + Ra_n.$$

Definition 1.26. Sei R ein Ring und $J_1, \ldots, J_n$ Ideale von R. Dann ist

$$J_1 \cdots J_n = (a_1 \cdots a_n \colon a_i \in J_i)$$

das *Produkt* der Ideale $J_1, \ldots, J_n$.

Beispiel 1.27. Sei $R = \mathbb{Z}$, $I_1 = 4\mathbb{Z}$ und $I_2 = 6\mathbb{Z}$. Dann gilt

$$I_1 + I_2 = 2\mathbb{Z} = I(2),\ I_1 \cap I_2 = 12\mathbb{Z} = I(12),\ I_1 \cdot I_2 = 24\mathbb{Z} = I(24).$$

Lemma 1.28. Sei R ein Ring und I, J Ideale von R. Dann gilt $I \cdot J \subseteq I \cap J$.

Beweis. Sei $a \in I, b \in J$. Dann ist $ab \in I \cap J$. Dann folgt aus der Definition des Produkts, dass $I \cdot J \subseteq I \cap J$. □

Bemerkung 1.29. In 1.28 gilt im Allgemeinen keine Gleichheit. Siehe 1.27.

Definition 1.30. Ein Integritätsbereich R heißt ein *Hauptidealbereich* (Hauptidealring), wenn jedes Ideal I von R ein Hauptideal ist, d.h. $I = (a)$ für ein $a \in R$.

Satz 1.31. Der Ring $\mathbb{Z}$ ist ein Hauptidealring.

Beweis. Sei $I \subseteq \mathbb{Z}$ ein Ideal. Dann ist $(I, +)$ eine Untergruppe von $(\mathbb{Z}, +)$, also hat I nach Kapitel 1, 1.13 die Gestalt $n\mathbb{Z} = (n)$ für ein $n \in \mathbb{Z}$. Die zeigt die Behauptung. □

2. Restklassenringe

Motivation 2.1. Wir betrachten in $\mathbb{N}$ das Problem, wann eine Zahl durch 3 teilbar ist. Sei $x \in \mathbb{N}$. Dann lässt sich x in der Dezimalschreibweise durch

$$x = \sum_{i=0}^{n} a_i 10^i,\ 0 \leq a_i < 10$$

darstellen. Nun ist

$$a_i 10^i = a_i(3 \cdot 3 + 1)^i = a_i + 3(\ldots).$$

Das heißt x ist genau dann durch 3 teilbar, wenn $\sum_{i=0}^{n} a_i$ durch 3 teilbar ist. Dies ist gerade die Quersumme von x und das Kriterium wird oft in der Schule schon behandelt. Das Prinzip ist, dass alle offensichtlichen Vielfachen von 3 vernachlässigt werden können. Nun kann man sich überlegen, dass die obige Rechnung zu folgenden Überlegungen äquivalent ist:

(i) Eine Zahl $x \in \mathbb{N}$ ist genau dann durch 3 teilbar, wenn $x \equiv 0 \mod 3\mathbb{Z}$.
(ii) $x = \sum_{i=0}^{n} a_i 10^i \equiv \sum_{i=0}^{n} a_i \mod 3\mathbb{Z}$, da $10 \equiv 1 \mod 3\mathbb{Z}$. Beachte, dass diese Rechnung in $\mathbb{Z}/3\mathbb{Z}$ durchgeführt wird.
(iii) Somit ist x genau dann durch 3 teilbar, wenn $\sum_{i=0}^{n} a_i$ durch 3 teilbar ist.

Übungsaufgabe: Überlegen Sie sich ein Kriterium, wann eine Zahl $x \in \mathbb{N}$ durch 11 teilbar ist.

Dieses Beispiel zeigt, dass es sinnvoll ist in dem Ring $\mathbb{Z}/m\mathbb{Z}$ zu rechnen. Beachte, dass $\mathbb{Z}$ ein Ring und $3\mathbb{Z}$ ein Ideal in $\mathbb{Z}$ ist. Wir werden nun allgemein einen Ring R und ein Ideal $I \subseteq R$ betrachten um einen Ring R/I zu definieren.

Konstruktion 2.2. Sei R ein Ring und $I \subseteq R$ ein Ideal. Definiere (analog zu den Faktorgruppen!)

$$R/I = \{a + I \colon a \in R\}.$$

Beachte, dass die $a + I$ gerade Linksnebenklassen von der Untergruppe $(I, +)$ in $(R, +)$ sind (R ist dadurch die disjunkte Vereinigung der Linksnebenklassen $a + I$). Da I ein Normalteiler von R ist, ist R/I eine (additive) Gruppe. Wir erklären nun auch ein Produkt auf R/I. Seien $a_1 + I, a_2 + I \in R/I$. Setze $(a_1 + I)(a_2 + I) = a_1a_2 + I$. Diese Definition ist unabhängig von der Wahl der Repräsentanten. Seien etwa $a_1 + I = b_1 + I$ und $a_2 + I = b_2 + I$, d.h. $a_1 - b_1 = c_1 \in I$ und $a_2 - b_2 = c_2 \in I$. Dann gilt

$$b_1b_2 = (a_1 - c_1)(a_2 - c_2) = a_1a_2 + (c_1c_2 - a_1c_2 - a_2c_1) \in a_1a_2 + I.$$

Daraus folgt, dass $a_1a_2 + I = b_1b_2 + I$. Man sieht nun leicht, dass R/I ein Ring ist. Dieser Ring heißt der *Restklassenring* (Faktorring) von R modulo I. Ein Element $\overline{a} = a + I$ heißt die *Restklasse* von a modulo I. Für $a + I = b + I$ schreibt man auch $a \equiv b \mod I$.

Satz 2.3. Sei R ein Ring und $I \subseteq R$ ein Ideal. Dann gilt:

(i) R/I ist mit den in 2.2 definierten Verknüpfungen ein Ring. Dieser ist kommutativ, wenn R kommutativ ist.

(ii) Die Abbildung $\varepsilon \colon R \longrightarrow R/I,\ a \mapsto \overline{a}$ ist ein surjektiver Ringhomomorphismus und $\mathrm{Ker}(\varepsilon) = I$. ε heißt der *kanonische Epimorphismus*.

(iii) Jedes Ideal ist Kern eines Ringhomomorphismus und jeder Kern eines Ringhomomorphismus ist ein Ideal.

(iv) (Die universelle Eigenschaft des Restklassenrings) Sei S ein weiterer Ring und $\varphi \colon R \longrightarrow S$ ein Ringhomomorphismus mit $I \subseteq \mathrm{Ker}(\varphi)$. Dann existiert genau ein Ringhomomorphismus $\varphi' \colon R/I \longrightarrow S$ mit $\varphi = \varphi' \circ \varepsilon$. Es gilt $\mathrm{Im}(\varphi') = \mathrm{Im}(\varphi)$ und $\mathrm{Ker}(\varphi') = \mathrm{Ker}(\varphi)/I \subseteq R/I$.

Beweis. Der Beweis verläuft analog zu dem entsprechenden Beweis in der Gruppentheorie (Die universelle Eigenschaft der Faktorgruppe) und ist dem Leser überlassen. □

Bemerkung 2.4. Nun sehen wir, dass der bereits bekannte Ring $\mathbb{Z}/m\mathbb{Z}$ für ein $m \in \mathbb{N}$ von dem konstruierten Typ ist. $\mathbb{Z}/m\mathbb{Z}$ hat die m Elemente $\overline{0}, \ldots, \overline{m-1}$. Man kann jedoch auch andere Repräsentanten wählen. Zum Beispiel ist es sinnvoll, wenn man $\overline{m-1}$ mit einem anderen Element aus $\mathbb{Z}/m\mathbb{Z}$ multipliziert, statt dessen mit $\overline{-1} = \overline{m-1}$ zu rechnen. Das Ergebnis ist natürlich dasselbe, jedoch ist der Rechenaufwand wesentlich geringer. Man kann sich auch wieder überlegen, dass der Restklassenring durch die universelle Eigenschaft eindeutig bestimmt ist.

Wir wollen den Ring $\mathbb{Z}/m\mathbb{Z}$ näher untersuchen.

Satz 2.5. Sei $m \in \mathbb{N}, m \geq 2$. Folgende Aussagen sind äquivalent:

(i) $\mathbb{Z}/m\mathbb{Z}$ ist ein Integritätsbereich.

(ii) $\mathbb{Z}/m\mathbb{Z}$ ist ein Körper.
(iii) m ist eine Primzahl.

Beweis. Da $\mathbb{Z}/m\mathbb{Z}$ endlich ist, sind die Aussagen (i) und (ii) wegen 1.9 äquivalent.

Sei $\varepsilon\colon \mathbb{Z} \longrightarrow \mathbb{Z}/m\mathbb{Z}$ der kanonische Epimorphismus.

(i) $\Rightarrow$ (iii): Ist m keine Primzahl, so lässt sich $m = ab$ mit $a, b \in \mathbb{N}$ und $1 < a, b < m$ schreiben. Dann gilt

$$0 = \varepsilon(m) = \varepsilon(ab) = \varepsilon(a)\varepsilon(b).$$

Aber $\varepsilon(a) \neq 0 \neq \varepsilon(b)$. Dies ist ein Widerspruch, da nach Voraussetzung $\mathbb{Z}/m\mathbb{Z}$ ein Integritätsbereich ist. Somit ist m eine Primzahl.

(iii) $\Rightarrow$ (i): Sei nun m eine Primzahl. Angenommen $\overline{a}\overline{b} = 0$. Dann gilt

$$0 = \overline{a}\overline{b} = \overline{ab} = \varepsilon(ab).$$

Daher $ab \in \mathrm{Ker}(\varepsilon) = m\mathbb{Z}$. Da m eine Primzahl ist folgt $m|a$ oder $m|b$. Dies bedeutet aber gerade $\overline{a} = 0$ oder $\overline{b} = 0$. Daher ist $\mathbb{Z}/m\mathbb{Z}$ ein Integritätsbereich. □

Die Aussagen dieses Satzes werden wir in einem späteren Kapitel verallgemeinern.

Bezeichnung 2.6. Sei p eine Primzahl. Dann wird der Körper $\mathbb{Z}/p\mathbb{Z}$ auch mit $\mathbb{F}_p$ bezeichnet.

Satz 2.7. *(Homomorphiesatz)* Seien R, S Ringe und $\varphi\colon R \longrightarrow S$ ein Epimorphismus. Dann gilt $R/\mathrm{Ker}(\varphi) \simeq S$.

Beweis. Wähle $I = \mathrm{Ker}(\varphi)$ in 2.3 (iv). Dann ist die induzierte Abbildung $R/\mathrm{Ker}(\varphi) \longrightarrow S$ ein Isomorphismus. □

Satz 2.8. Seien R, S Ringe, $\varphi\colon R \longrightarrow S$ ein Epimorphismus. Die Abbildung

$$\{J \subseteq S\colon J \text{ ist ein Ideal}\} \longrightarrow \{I \subseteq R\colon I \text{ ist ein Ideal und } \mathrm{Ker}(\varphi) \subseteq I\},\ J \mapsto \varphi^{-1}(J)$$

ist bijektiv. Insbesondere ist jedes Ideal in $S \cong R/\mathrm{Ker}(\varphi)$ von der Form $I/\mathrm{Ker}(\varphi)$ für ein Ideal $\mathrm{Ker}(\varphi) \subseteq I \subseteq R$.

Beweis. Sei $J \subseteq S$ ein Ideal, dann gilt immer, dass $\varphi^{-1}(J) \subseteq R$ ein Ideal ist. Nun ist

$$\varphi(\mathrm{Ker}(\varphi)) = \{0\} \in J,$$

d.h. $\mathrm{Ker}(\varphi) \subseteq \varphi^{-1}(J)$. Ist umgekehrt $I \subseteq R$ ein Ideal, dann ist $\varphi(I)$ ein Ideal von S, da φ surjektiv ist. Die Behauptung folgt nun aus:

(i) $\varphi(\varphi^{-1}(J)) = J$ für ein Ideal $J \subseteq S$.
(ii) $\varphi^{-1}(\varphi(I)) = I$ für ein Ideal $I \subseteq R$ mit $\mathrm{Ker}(\varphi) \subseteq I$.

Zu (i): Es gilt immer $\varphi(\varphi^{-1}(J)) \subseteq J$. Sei $a \in J$. Da φ surjektiv ist, existiert ein $b \in R$ mit $\varphi(b) = a$. Da $b \in \varphi^{-1}(J)$ folgt (i).

Zu (ii): Es gilt $I \subseteq \varphi^{-1}(\varphi(I))$. Sei nun $a \in \varphi^{-1}(\varphi(I))$, d.h. $\varphi(a) \in \varphi(I)$. Sei $b \in I$ mit $\varphi(a) = \varphi(b)$. Dann gilt $\varphi(a - b) = 0$, also $a - b \in \mathrm{Ker}(\varphi) \subseteq I$. Daher existiert ein $c \in I$ mit $a - b = c$. Dann ist aber $a = b + c \in I$ und dies war zu zeigen. □

Beispiel 2.9. Betrachte den Ring $\mathbb{Z}/(6)$. Man überlege sich, dass die einzig möglichen Ideale $(0)/(6)$, $(1)/(6)$, $(2)/(6)$ und $(3)/(6)$ sind.

Definition 2.10. Sei R ein kommutativer Ring und $I, J \subseteq R$ Ideale. I und J heißen *teilerfremd (koprim)*, wenn $I + J = R$ gilt.

Bemerkung 2.11. Für zwei Zahlen $m, n \in \mathbb{Z}$ gilt $(m) + (n) = \mathbb{Z}$ genau dann, wenn n und m teilerfremd sind.

In der Zahlentheorie wird meist folgender Satz bewiesen:

Satz 2.12. *(Chinesischer Restsatz)* Sei R ein kommutativer Ring und $I_1, \ldots, I_n$ paarweise teilerfremde Ideale von R. Dann ist die Abbildung

$$\varphi\colon R \longrightarrow R/I_1 \times \cdots \times R/I_n, \quad a \mapsto (a + I_1, \ldots, a + I_n)$$

ein Epimorphismus mit $\mathrm{Ker}(\varphi) = \bigcap_{i=1}^{n} I_i$. Insbesondere gilt

$$R/(\bigcap_{i=1}^{n} I_i) \simeq R/I_1 \times \cdots \times R/I_n.$$

Beweis. Man sieht leicht, dass φ ein Ringhomomorphismus ist und dass $\mathrm{Ker}(\varphi) = \bigcap_{i=1}^{n} I_i$ gilt. Es bleibt zu zeigen, dass φ surjektiv ist.

Behauptung: Für $i = 1, \ldots, n$ existieren Elemente x_i mit $x_i \equiv 1 \mod I_i$ und $x_i \equiv 0 \mod I_j$ für $j \neq i$. Ist dann $(a_1 + I_1, \ldots, a_n + I_n) \in R/I_1 \times \cdots \times R/I_n$ beliebig gewählt, dann gilt

$$\varphi(a_1 x_1 + \cdots + a_n x_n) = (a_1 x_1 + I_1, \ldots, a_n x_n + I_n) = (a_1 + I_1, \ldots, a_n + I_n)$$

und somit ist φ surjektiv. Es bleibt die Behauptung zu zeigen. Sei im Folgenden $i \in \{1, \ldots, n\}$ fest gewählt. Für $j \neq i$ gilt nach Voraussetzung $I_i + I_j = R$, also existiert ein $a_j \in I_i$ und $b_j \in I_j$ mit $a_j + b_j = 1$. Dann gilt

$$1 = \prod_{j \neq i} (a_j + b_j) = c_i + x_i \text{ mit } c_i \in I_i \text{ und } x_i \in \prod_{j \neq i} I_j.$$

Es gilt $1 - x_i = c_i \in I_i$, $x_i \in I_j$ für $j \neq i$. Also $x_i \equiv 1 \mod I_i$ und $x_i \equiv 0 \mod I_j$ für $j \neq i$. □

Der Durchschnitt von teilerfremden Idealen lässt sich sehr einfach bestimmen.

Satz 2.13. Sei R ein kommutativer Ring und $I_1, \ldots, I_n$ paarweise teilerfremde Ideale von R. Dann gilt:

(i) Für $i = 1, \ldots, n$ ist das Ideal I_i teilerfremd zu $\prod_{j \neq i} I_j$.

(ii)
$$\bigcap_{i=1}^{n} I_i = \prod_{i=1}^{n} I_i.$$

Beweis. (i) Im Beweis von 2.12 wurde gezeigt, dass ein $c_i \in I_i$ und ein $x_i \in \prod_{j \neq i} I_j$ existiert mit $1 = c_i + x_i$. Daraus folgt $R = I_i + \prod_{j \neq i} I_j$.

(ii) Wir beweisen dies durch eine Induktion nach n. Sei $n = 2$. Es gilt immer

$$I_1 I_2 \subseteq I_1 \cap I_2.$$

Ferner gilt

$$(I_1 + I_2) I_1 \cap I_2 \subseteq I_1 I_2,$$

denn für $a \in I_1, b \in I_2, c \in I_1 \cap I_2$ ist $(a+b)c \in I_1 I_2$, da $ac, bc \in I_1 I_2$. Da aber $I_1 + I_2 = R$ gilt, folgt $I_1 \cap I_2 \subseteq I_1 I_2$, also $I_1 I_2 = I_1 \cap I_2$.

Sei nun $n \geq 2$. Definiere $J = \prod_{i=2}^{n} I_i$. Wegen (i) sind I_1 und J teilerfremd. Daher gilt nach der Induktionsannahme und analog zum Fall $n = 2$

$$\bigcap_{i=1}^{n} I_i = I_1 \cap J = I_1 J = \prod_{i=1}^{n} I_i.$$

□

Korollar 2.14. Seien $b_1, \ldots, b_n \in \mathbb{Z}$ paarweise teilerfremde Zahlen. Dann ist das simultane Kongruenzsystem $x \equiv a_i \mod (b_i)$ für $i = 1, \ldots, n$ und beliebige Zahlen $a_1, \ldots, a_n \in \mathbb{Z}$ lösbar. Die Lösung ist eindeutig modulo $b_1 \cdots b_n$.

Beweis. Die Behauptung folgt aus 2.12 und 2.13. □

Bemerkung 2.15. Der Beweis von 2.12 zeigt auch, wie eine Lösung in 2.14 gewonnen werden kann. Seien $I_1, \ldots, I_n$ die Ideale. Definiere $J_i = \bigcap_{j=1, j\neq i}^{n} I_j$. Um das x zu finden, muss man gerade

$$1 = c_i + x_i$$

mit $c_i \in I_i$ und $x_i \in J_i$ darstellen können. Wir werden hierfür zu einem späteren Zeitpunkt eine Methode (den euklidischen Algorithmus) entwickeln, um eine solche Darstellung zu gewinnen.

3. Integritätsbereiche und Körper

Da der Durchschnitt von Teilkörpern eines Integritätsbereichs wieder ein Teilkörper ist, macht folgende Definition Sinn:

Definition 3.1. Sei R ein Integritätsbereich, der wenigstens einen Teilkörper enthält. Dann heißt der Durchschnitt aller Teilkörper von R der *Primkörper von R.*

Bemerkung 3.2. Wenn ein Primkörper existiert, dann ist dies der kleinste Teilkörper von R. Insbesondere ist er in jedem anderen Teilkörper enthalten. Jeder Körper besitzt einen Primkörper. Z.B. ist $\mathbb{Q}$ der Primkörper von $\mathbb{R}$ und $\mathbb{C}$. Der Ring $\mathbb{Z}$ besitzt keine Teilkörper, also auch keinen Primkörper.

Also besitzen Integritätsbereiche der Charakteristik 0 i.A. keinen Primkörper. In Charakteristik p sieht diese Situation anders aus.

Satz 3.3. Sei R ein Integritätsbereich der Charakteristik $p > 0$. Dann hat R einen Primkörper und dieser ist isomorph zu $\mathbb{F}_p$.

Beweis. Definiere die Abbildung

$$\Phi \colon \mathbb{F}_p = \mathbb{Z}/p\mathbb{Z} \longrightarrow R,\ \overline{z} \mapsto z \cdot 1_R.$$

Diese ist wohldefiniert, da $p = \mathrm{char}(R) = \mathrm{ord}(1_R)$ (siehe 1.14). Nun verifiziert man, dass Φ ein Ringhomomorphismus ist. Da $\mathbb{F}_p$ ein Körper ist, muss Φ injektiv sein. Somit ist $\mathbb{F}_p$ Teilkörper von R. Dies ist aber auch der kleinste Teilkörper, den R enthalten kann und stimmt daher mit dem Primkörper überein. □

Korollar 3.4. Sei K ein endlicher Körper. Dann gilt:

(i) $\mathrm{char}(K) = p > 0$.
(ii) Die Anzahl der Elemente von K ist eine Potenz von p.

Beweis. (i) Ein Körper der Charakteristik 0 hat immer unendlich viele Elemente, daher muss K eine endliche Charakteristik haben.

(ii) Sei $\mathbb{F}_p$ der Primkörper von K. Dieser existiert wegen 3.3. K ist in natürlicher Weise ein endlich dimensionaler $\mathbb{F}_p$-Vektorraum und daher isomorph zu $\mathbb{F}_p^n$ für ein $n \in \mathbb{N}$. Dann ist die Anzahl der Elemente von K gleich p^n. □

Sei ein Integritätsbereich R Unterring eines Körpers K. Der Durchschnitt aller Teilkörper von K, die R umfassen, ist wieder ein R umfassender Teilkörper von K.

Definition 3.5. Sei ein Integritätsbereich R Unterring eines Körpers K. Dann heißt der Durchschnitt aller R umfassenden Teilkörper von K der *Körper der Brüche* oder *Quotientenkörper* von R in K.

Bemerkung 3.6. Es seien R und K wie in der Definition und Q der Quotientenkörper von R in K. Dann gilt

$$Q = \{ab^{-1} \colon a, b \in R,\ b \neq 0\},$$

wie leicht zu sehen ist. (Die rechte Menge ist ein Körper, der Q enthält. Ferner ist dieser Körper der kleinste Körper mit dieser Eigenschaft.) Zum Beispiel ist $\mathbb{Q}$ der Quotientenkörper von $\mathbb{Z}$ in $\mathbb{Q}$ (oder $\mathbb{R}$ bzw. $\mathbb{C}$).

Man kann jeden Integritätsbereich als Unterring eines Körpers auffassen, wie folgende Konstruktion und nachfolgender Satz zeigt.

Konstruktion 3.7. Sei R ein Integritätsbereich, $T = R \backslash \{0\}$. Wir definieren auf der Menge der Paare $\{(a, b) \colon a \in R, b \in T\}$ eine Äquivalenzrelation: $(a_1, b_1) \sim (a_2, b_2) \Leftrightarrow a_1 b_2 = a_2 b_1$. Die Äquivalenzklasse (a, b) wird mit $\frac{a}{b}$ bezeichnet. Die Menge der Äquivalenzklassen bezeichnen wir mit $Q(R)$. Definiere Addition und Multiplikation auf $Q(R)$ wie folgt:

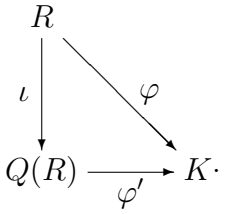
$$\frac{a_1}{b_1} \cdot \frac{a_2}{b_2} = \frac{a_1 a_2}{b_1 b_2} \text{ und } \frac{a_1}{b_1} + \frac{a_2}{b_2} = \frac{a_1 b_2 + a_2 b_1}{b_1 b_2}.$$

Die Definitionen sind unabhängig von der Wahl der Repräsentanten und $(Q(R), +, \cdot)$ ist ein Körper mit $\frac{1}{1}$ als Einselement, $\frac{0}{1}$ als Nullelement, ... (Übungsaufgabe: Beweisen Sie die Behauptungen.)

Satz 3.8. Sei R ein Integritätsbereich. Dann gilt:

(i) $(Q(R), +, \cdot)$ ist ein Körper.
(ii) Die Abbildung $\iota \colon R \longrightarrow Q(R), a \mapsto \frac{a}{1}$ ist ein Monomorphismus und wird die kanonische Einbettung genannt.
(iii) (Universelle Eigenschaft des Quotientenkörpers) Sei $\varphi \colon R \longrightarrow K$ ein Ringhomomorphismus in einen Körper K. Dann gibt es genau einen Körperhomomorphismus $\varphi' \colon Q(R) \longrightarrow K$ mit $\varphi = \varphi' \circ \iota$, d.h. folgendes Diagramm

ist kommutativ:



Beweis. (i) siehe Konstruktion des Quotientenkörpers.

(ii) Trivial.

(iii) Eindeutigkeit: Sei $\frac{a}{b} \in Q(R)$ beliebig. Dann gilt

$$\varphi'(\frac{a}{b}) = \varphi'(\frac{a}{1} \cdot \frac{1}{b}) = \varphi'(\frac{a}{1} \cdot (\frac{b}{1})^{-1}) = \varphi'(\frac{a}{1}) \cdot \varphi'(\frac{b}{1})^{-1}$$
$$= \varphi'(\iota(a)) \cdot \varphi'(\iota(b))^{-1} = \varphi(a) \cdot \varphi(b)^{-1}.$$

Existenz: Zeige, dass die Abbildung φ' mit $\varphi'(\frac{a}{b}) = \varphi(a) \cdot \varphi(b)^{-1}$ die gewünschten Eigenschaften hat. □

Bemerkung 3.9. Identifiziert man R mit seinem Bild in $Q(R)$, so ist R Unterring eines Körpers. Wegen 3.6 ist $Q(R)$ der Quotientenkörper von R in $Q(R)$. Wegen 3.8 kann man von dem Quotienkörper von R sprechen: Ist R Unterring eines weiteren Körpers K und Q der Quotientenkörper von R in K, dann induziert $\iota\colon R \longrightarrow Q$ einen Isomorphismus $Q(R) \longrightarrow Q$.

In Ringen der Charakteristik $p > 0$ konnten wir den Primkörper charakterisieren. Dies ist nun auch für Ringe der Charakteristik 0 möglich, sofern ein Primkörper existiert.

Satz 3.10. Sei R ein Integritätsbereich mit $\mathrm{char}(R) = 0$, der wenigstens einen Teilkörper enthält. Dann ist der Primkörper von R isomorph zu dem Körper $\mathbb{Q}$.

Beweis. Definiere den Ringhomomorphismus

$$\varphi\colon \mathbb{Z} \longrightarrow R,\ z \mapsto z \cdot 1_R.$$

Dieser ist wegen $\mathrm{char}(R) = 0$ injektiv und $\mathrm{Im}(\varphi)$ ist in jedem Teilkörper von R enthalten. Sei Q der Primkörper von R. Dann induziert φ einen Monomorphismus

$$\varphi\colon \mathbb{Z} \longrightarrow Q.$$

Wegen 3.8 (iii) existiert eine eindeutige Fortsetzung

$$\varphi'\colon \mathbb{Q} \longrightarrow Q.$$

Diese ist injektiv, da $\mathbb{Q}$ ein Körper ist. Das heißt $\mathrm{Im}(\varphi') \subseteq Q$. Wegen der Definition eines Primkörpers muss φ' surjektiv sein, da sonst ein kleinerer Teilkörper $\mathrm{Im}(\varphi') \subsetneq R$ existieren würde. Daher folgt $\mathbb{Q} \cong Q$. □

Sei R ein kommutativer Ring, S ein Integritätsbereich oder Körper und $\varphi\colon R \longrightarrow S$ ein Epimorphismus. Wir untersuchen die Fragen, welche Struktur das Ideal $\mathrm{Ker}(\varphi)$ in solch einer Situation hat. Man sieht leicht, dass folgende Eigenschaft erfüllt sein muss: Ist $a, b \in R$ und $ab \in \mathrm{Ker}(\varphi)$, dann gilt $a \in \mathrm{Ker}(\varphi)$ oder $b \in \mathrm{Ker}(\varphi)$.

Definition 3.11. Sei R ein kommutativer Ring. Ein Ideal $P \subseteq R$ heißt *Primideal*, wenn $P \neq R$ und wenn für alle $a, b \in R$ mit $ab \in P$ folgt, dass $a \in P$ oder $b \in P$ gilt.

Satz 3.12. Sei R ein kommutativer Ring und $P \subseteq R$ ein Ideal. Folgende Aussagen sind äquivalent:

(i) P ist ein Primideal,
(ii) R/P ist ein Integritätsbereich.

Beweis. (i) $\Rightarrow$ (ii): Seien $P \neq a + P, b + P \in R/P$. Also gilt $a \notin P$ und $b \notin P$. Da P ein Primideal ist, folgt $ab \notin P$, also $ab + P \neq P$.

(ii) $\Rightarrow$ (i): Seien $a, b \in R$ mit $ab \in P$. Es folgt, dass $P = ab + P = (a + P)(b + P)$. Da R/P ein Integritätsbereich ist, gilt $a + P = P$ oder $b + P = P$. Dies ist äquivalent zu $a \in P$ oder $b \in P$. □

Die folgende Aussage kann man auch leicht direkt beweisen.

Korollar 3.13. Sei $n \in \mathbb{Z}, n > 1$. Dann ist (n) genau dann ein Primideal, wenn n eine Primzahl ist. Ferner ist (0) ein Primideal.

Beweis. Dies folgt aus 2.5 und 3.12. □

Definition 3.14. Sei R ein kommutativer Ring. Ein Ideal $M \subseteq R$ heißt ein *maximales Ideal*, wenn $M \neq R$ und für alle Ideale $I \subseteq R$ mit $M \subseteq I$ folgt, dass $I = M$ oder $I = R$ gilt.

Satz 3.15. Sei R ein kommutativer Ring und $M \subseteq R$ ein Ideal. Folgende Aussagen sind äquivalent:

(i) M ist ein maximales Ideal,
(ii) R/M ist ein Körper.

Beweis. (i) $\Rightarrow$ (ii): Sei M ein maximales Ideal. Sei $0 \neq a + M \in R/M$ beliebig mit $a \notin M$. Betrachte das Ideal $M \subseteq J = M + (a)$. Es gilt $J \neq M$ und daher $J = R$. Dann ist $1 \in J$, d. h. es existiert ein $b \in R$ und ein $c \in M$ mit $1 = ba + c$. Somit ist $(b + M)(a + M) = ba + M = 1 + M$. Also ist $b + M$ das inverse Element zu $a + M$ und R/M ist ein Körper.

(ii) $\Rightarrow$ (i): Sei $M \subseteq J \subseteq R$ ein Ideal mit $M \neq J$. Sei $a \in J \setminus M$. Dann ist $a + M \neq M$ in R/M. Da R/M ein Körper ist, existiert ein $b \in R$ mit $(b + M)(a + M) = ba + M = 1 + M$. Es folgt, dass $1 - ba \in M$, also $1 \in (a) + M \subseteq J$. Somit $J = R$ und M ist ein maximales Ideal. □

Korollar 3.16. Maximale Ideale sind Primideale.

Beweis. Sei M ein maximales Ideal in einem kommutativen Ring R. Nach 3.15 ist R/M ein Körper, also insbesondere ein Integritätsbereich. Aus 3.12 folgt, dass M ein Primideal ist. □

Beispiel 3.17. Maximale Ideale in $\mathbb{Z}$ sind die Ideale (p) mit p Primzahl. Das Ideal (0) ist das einzige Primideal in $\mathbb{Z}$, das nicht maximal ist.

4. Teilbarkeitstheorie

Ziel dieses Abschnitts ist es, die bekannte Teilbarkeitstheorie der ganzen Zahlen sinnvoll zu verallgemeinern und die Aussagen für eine größere Klasse von Ringen bereitzustellen.

Definition 4.1. Sei R ein Integritätsbereich und $a, b \in R$. Das Element a heißt ein *Teiler* von b, wenn ein $c \in R$ existiert mit $b = ac$. Man schreibt hierfür $a|b$. Das Element a heißt *assoziiert* zu b, wenn $a|b$ und $b|a$ gilt. Dies wird mit $a \sim b$ bezeichnet. (Bemerkung: $\sim$ ist eine Äquivalenzrelation.)

Bezeichnung 4.2. 1 (bzw. jede Einheit) und a sind die *trivialen Teiler* von einem Element $a \in R$. Ein Element a ist ein *echter Teiler* von b, wenn $a|b$ und $a \notin R^*, a \not\sim b$ gilt.

Lemma 4.3. Sei R ein Integritätsbereich und $a, b, c, d \in R$. Dann gelten folgende Rechenregeln:

(i) $a|b$ und $b|c \Rightarrow a|c$.
(ii) $a|b$ und $a|c \Rightarrow a|b \pm c$.
(iii) $a|b$ und $a|b + c \Rightarrow a|c$.
(iv) $a|b$ und $c|d \Rightarrow ac|bd$.
(v) $a|b \Leftrightarrow (a) \supseteq (b)$.
(vi) $a \sim b \Leftrightarrow (a) = (b) \Leftrightarrow a = bc$ mit $c \in R^*$.

Beweis. Diese Regeln rechnet man leicht nach. Z.B. (v): Es gilt $a|b$ genau dann, wenn ein $c \in R$ mit $ac = b$ existiert. Dies ist äquivalent zu $(a) \supseteq (b)$. Oder (vi): $(a) = (b) \Leftrightarrow a \sim b$ folgt direkt aus (v). Sei $a = bc$ für ein $c \in R$ nach Voraussetzung. Es existiert aber auch ein $d \in R$, so dass $ad = b$, denn $a|b$. Es folgt, dass $a = bc = adc$ und nach 1.8 ist dann $1 = dc$, also sind $c, d \in R^*$. □

Definition 4.4. Sei R ein Integritätsbereich. Ein Element $0 \neq a \in R \setminus R^*$ heißt *irreduzibel* (oder unzerlegbar), wenn für $b, c \in R$ mit $a = bc$ stets $b \in R^*$ oder $c \in R^*$ gilt.

Eine Zahl ist somit genau dann unzerlegbar, wenn sie keine echten Teiler besitzt.

Beispiel 4.5. In Körpern sind alle Elemente ungleich 0 assoziiert. Es gibt keine unzerlegbaren Elemente.

In $\mathbb{Z}$ sind zwei Zahlen m, n genau dann assoziiert, wenn $m = \pm n$ gilt. Eine Zahl ist genau dann unzerlegbar, wenn ihr Betrag eine Primzahl ist.

Satz 4.6. Sei R ein Hauptidealbereich. Für ein $0 \neq a \in R$ sind folgende Aussagen äquivalent:

(i) a ist irreduzibel,
(ii) (a) ist ein maximales Ideal.

Beweis. (i) $\Rightarrow$ (ii): Sei $(a) \subseteq (b) \subseteq R$ ein Ideal mit $b \in R$. Da $a \in (b)$ existiert ein $c \in R$ mit $a = bc$. Nun folgt wegen der Irreduzibilität von a, dass $b \in R^*$ oder $c \in R^*$. Dies ist äquivalent zu $(b) = R$ oder $(a) = (b)$. Daher ist (a) ein maximales Ideal.

(ii) $\Rightarrow$ (i): Sei $a = bc$ mit $b, c \in R$. Nun gilt $(a) \subseteq (b) \subseteq R$. Da (a) ein maximales Ideal ist, folgt $(a) = (b)$ oder $(b) = R$. Gilt $(b) = R$, dann ist $b \in R^*$, da dann $1 \in (b)$. Sonst ist $(a) = (b)$, und es gilt nach 4.3 (vi) $c \in R^*$. Damit ist a irreduzibel. □

Definition 4.7. Sei R ein Integritätsbereich. Eine Folge von Elementen $(a_n)_{n\in\mathbb{N}}$ mit $a_n \in R \setminus \{0\}$ heißt *Teilerkette*, wenn für alle $n \in \mathbb{N}$ $a_{n+1}|a_n$ gilt. Man sagt, in R gilt der *Teilerkettensatz*, wenn jede Teilerkette $(a_n)_{n\in\mathbb{N}}$ stationär wird, d.h. es gibt ein $n_0 \in \mathbb{N}$ mit $a_n \sim a_{n+1}$ für $n \geq n_0$.

Beispiel 4.8. In $\mathbb{Z}$ gilt der Teilerkettensatz. Sei $(a_n)_{n\in\mathbb{N}}$ eine Teilerkette in $\mathbb{Z}$. Die Menge $\{|a_n| \colon n \in \mathbb{N}\}$ besitzt ein kleinstes Element $|a_{n_0}|$. Da $|a_{n+1}| \leq |a_n|$ für alle $n \in \mathbb{N}$ gilt, folgt $a_n \sim a_{n+1}$ für $n \geq n_0$.

Satz 4.9. In R gelte der Teilerkettensatz. Dann lässt sich jedes Element $0 \neq a \in R \setminus R^*$ als Produkt $a = b_1 \cdots b_n$ mit endlich vielen irreduziblen Elementen $b_1, \ldots, b_n$ darstellen (das Produkt ist nicht notwendigerweise eindeutig).

Beweis. Sei $0 \neq a \in R \setminus R^*$ ein beliebiges Element. Angenommen a lässt sich nicht als Produkt von endlich vielen irreduziblen Elementen schreiben. Wir definieren induktiv ein Kette von Elementen $(a_n)_{n\in\mathbb{N}}$ mit $a_{n+1}|a_n$, $a_n \not\sim a_{n+1}$ und a_n lässt sich für alle $n \in \mathbb{N}$ nicht als Produkt von endlich vielen irreduziblen Elementen schreiben. Dies ist ein Widerspruch zur Voraussetzung, dass in R der Teilerkettensatz gilt.

Für $n = 0$ setze $a_0 = a$. Sei $n \geq 0$ und die Kette $a_0, \ldots, a_n$ bereits konstruiert. a_n kann nicht irreduzibel sein, also existieren $0 \neq b, c \in R \setminus R^*$ mit $a_n = bc$. Wegen der Wahl von a_n können b und c sich nicht beide als Produkt von endlich vielen irreduziblen Elementen schreiben lassen. Lässt sich etwa b nicht so schreiben, dann setze $a_{n+1} = b$. Die so konstruierte Folge $(a_n)_{n\in\mathbb{N}}$ würde also nicht stationär werden. Dies zeigt die Behauptung. □

Satz 4.10. Sei R ein Hauptidealbereich. Dann gilt in R der Teilerkettensatz.

Beweis. Sei $(a_n)_{n\in\mathbb{N}}$ eine Teilerkette in R. Da $a_{n+1}|a_n$ für alle $n \in \mathbb{N}$ gilt, folgt

$$(a_0) \subseteq (a_1) \subseteq \ldots \subseteq (a_n) \subseteq \ldots$$

Sei $I = \bigcup_{n\in\mathbb{N}}(a_n)$. Dann ist I ein Ideal, insbesondere ein Hauptideal. Also existiert ein $b \in R$ mit $I = (b)$. Sei n_0 so gewählt, dass $b \in (a_{n_0})$ gilt. Dann ist $(a_n) = (a_{n+1})$ für $n \geq n_0$ und somit $a_n \sim a_{n+1}$ für $n \geq n_0$. □

Nun führen wir den Begriff eines Primelements ein.

Definition 4.11. Sei R ein Integritätsbereich und $0 \neq p \in R \setminus R^*$. Das Element p heißt ein *Primelement*, wenn für alle $a, b \in R$ mit $p|ab$ folgt, dass $p|a$ oder $p|b$ gilt.

Lemma 4.12. Sei R ein Integritätsbereich und $0 \neq p \in R \setminus R^*$. Dann gilt:

(i) p ist genau dann ein Primelement, wenn (p) ein Primideal ist.
(ii) Ist p ein Primelement, so ist p irreduzibel.

Beweis. Zu (i): Dies folgt direkt aus den Definitionen von Primelement und Primideal.

Zu (ii): Sei p ein Primelement und $p = ab$ für $a, b \in R$. Da $p|ab$ gilt, folgt $p|a$ oder $p|b$. Gelte etwa $p|a$, dann existiert ein $c \in R$ mit $pc = a$. Somit folgt aus $p = ab = pcb$, dass $1 = cb$ gilt. Also ist $b \in R^*$. Damit ist p irreduzibel. □

Bemerkung 4.13. Sei R ein Integritätsbereich. Dann gelten folgende Regeln:

(i) Seien $p, q \in R$, p ein Primelement und $p \sim q$, dann ist q ist ein Primelement.
(ii) Sind $p, q \in R$ Primelemente mit $p|q$, dann gilt $p \sim q$.
(iii) Ist $p \in R$ ein Primelement mit $p|a_1 \cdots a_n$, dann gilt $p|a_i$ für ein $i \in \{1, \ldots, n\}$.

In Hauptidealbereichen (wie z.B. $\mathbb{Z}$) sind die Begriffe Primelement und irreduzibles Element äquivalent:

Satz 4.14. Sei R ein Hauptidealbereich, $0 \neq p \in R \setminus R^*$. Dann sind folgende Aussagen äquivalent:

(i) p ist ein Primelement,
(ii) p ist irreduzibel,
(iii) (p) ist ein maximales Ideal.

Beweis. In 4.12 und 4.6 wurde bereits (i) ⇒ (ii) und (ii) ⇔ (iii) bewiesen. Es bleibt zu zeigen, dass (iii) ⇒ (i) gilt. Ist (p) ein maximales Ideal, so ist (p) ein Primideal nach 3.16. Aus 4.12 (i) folgt die Behauptung. □

Lemma 4.15. Sei R ein Integritätsbereich und $0 \neq a \in R$. Seien $a = p_1 \cdots p_m = q_1 \cdots q_n$ zwei Darstellungen von a als Produkt von Primelementen. Dann gilt:

(i) $m = n$.
(ii) Nach einer geeigneten Umnummerierung gilt $p_i \sim q_i$.

Die Darstellung von Primelementen ist also im Wesentlichen eindeutig.

Beweis. Wir beweisen den Satz durch eine Induktion nach $l = \min\{m, n\}$. O.E. ist $l = m$.

Für $l = 1$ folgt wegen $p_1|q_1 \cdots q_n$, dass $p_1|q_i$ für ein $i \in \{1, \ldots, n\}$ und somit nach 4.13 $p_1 \sim q_i$, etwa $q_i = \varepsilon p_1$ für ein $\varepsilon \in R^*$. Außerdem gilt nach Kürzen durch p_1, dass $1 = \varepsilon q_1 \cdots q_{i-1} q_{i+1} \cdots q_n$. Also gilt $n = 1$ und damit die Behauptung.

Sei nun $l > 1$. Es gilt $p_m|q_1 \cdots q_n$ und daher wieder $p_m|q_i$ für ein $i \in \{1, \ldots, n\}$. Sei o.E. $i = n$ und daher $p_m \sim q_n$, etwa $q_m = \varepsilon p_n$ für ein $\varepsilon \in R^*$. Nach Kürzen gilt $p_1 \cdots p_{m-1} = \varepsilon q_1 \cdots q_{n-1}$ mit $\min\{m-1, n-1\} < l$. Nach der Induktionsannahme gilt $m - 1 = n - 1$, also $m = n$. Nach einer geeigneten Nummerierung gilt $p_i \sim q_i$ für $i = 1, \ldots, n-1$. □

Definition 4.16. Sei R ein Integritätsbereich. R heißt *faktoriell*, wenn sich jedes Element $0 \neq a \in R \setminus R^*$ als endliches Produkt von Primelementen schreiben lässt. (Diese Darstellung ist wegen 4.15 im Wesentlichen eindeutig.)

Bemerkung 4.17. Sei R ein faktorieller Ring, $0 \neq a \in R$ und $\mathcal{P}$ ein Vertretersystem der Primelemente von R. Dann besitzt a die eindeutige Darstellung

$$a = \varepsilon \prod_{p \in \mathcal{P}} p^{v_p(a)}$$

mit $\varepsilon \in R^*$, $v_p(a) \in \mathbb{N}$ und fast allen $v_p(a) = 0$.

Korollar 4.18. Sei R ein Hauptidealbereich, dann ist R faktoriell.

Beweis. Dies folgt aus 4.9, 4.10, 4.14 und 4.15. □

Beispiel 4.19. In faktoriellen Ringen sind die Primelemente genau die irreduziblen Elemente. Das die Unterscheidung zwischen Primelementen und irreduziblen Elementen notwendig ist, zeigt folgendes Beispiel.

$$D = \{a + bi\sqrt{5} \colon a, b \in \mathbb{Z}\} \subseteq \mathbb{C}$$

ist ein Unterring, wie man leicht nachrechnet. Insbesondere ist D ein Integritätsbereich. Definiere

$$N(a + bi\sqrt{5}) = |a + bi\sqrt{5}|^2 = a^2 + b^2 5.$$

Dann gilt offenbar

$$N(xy) = N(x)N(y) \text{ für } x, y \in D.$$

Daher ist $N \colon D \longrightarrow (\mathbb{Z}, \cdot)$ ein Monoidhomomorphismus. Dann ist $x \in D^*$ äquivalent zu $N(x) = 1 \Leftrightarrow x = \pm 1$. Es folgt auch, dass $N(a) < N(b)$ für einen echten Teiler a von b gilt. Man überlegt sich leicht, dass jedes Element von D sich als Produkt von irreduziblen Elementen darstellen lässt, da in D der Teilerkettensatz gilt (analog zu 4.8). Aber nicht jedes irreduzible Element ist ein Primelement. Betrachte $2 \in D$. Aus $2 = xy$ folgt $4 = N(x)N(y)$. Es kann nie $N(x) = 2$ bzw. $N(y) = 2$ gelten. Also ist $N(x) = 1, N(y) = 4$ oder $N(x) = 4, N(y) = 1$. Daher muss x oder y eine Einheit sein und somit ist 2 irreduzibel. Nun ist

$$(1 + i\sqrt{5})(1 - i\sqrt{5}) = 1 + 5 = 2 \cdot 3,$$

also teilt 2 die linke Seite. Aber 2 teilt nicht $(1 \pm i\sqrt{5})$. Aus

$$(1 \pm i\sqrt{5}) = 2 \cdot x \text{ mit } x \in D$$

folgt $6 = 4N(x)$, was nicht sein kann. Also ist 2 kein Primelement. Insbesondere kann D nicht faktoriell sein.

Definition 4.20. Ein Integritätsbereich R zusammen mit einer Abbildung $\delta \colon R \backslash \{0\} \longrightarrow \mathbb{N}$ heißt ein *euklidischer Ring*, wenn für alle Elemente $a, b \in R$ mit $b \neq 0$ Elemente $q, r \in R$ existieren mit

(i) $a = qb + r$,
(ii) $r = 0$ oder $\delta(r) < \delta(b)$.

Die Abbildung δ wird mit *Grad- oder Normabbildung* von R bezeichnet.

Beispiel 4.21. Betrachte:

(i) $\mathbb{Z}$ bildet zusammen mit der Betragsfunktion $|\cdot|$ einen euklidischen Ring.
(ii) Jeder Körper ist aus trivialen Gründen ein euklidischer Ring.
(iii) Wir werden in einem späteren Abschnitt sehen, dass der Polynomring $K[X]$ über einem Körper K ein euklidischer Ring ist.

(iv) Der Unterring

$$G = \mathbb{Z} + i\mathbb{Z} = \{a + bi \colon a, b \in \mathbb{Z}\} \subseteq \mathbb{C}$$

der komplexen Zahlen ist ein euklidischer Ring (Übungsaufgabe). Dieser Ring heißt der *Ring der ganzen Gaußschen Zahlen*.

Satz 4.22. Sei R ein euklidischer Ring. Dann ist R ein Hauptidealbereich. Insbesondere gilt:

$$\begin{aligned} &R \text{ ist ein Körper} \\ \Rightarrow\ &R \text{ ist ein euklidischer Ring} \\ \Rightarrow\ &R \text{ ist ein Hauptidealbereich} \\ \Rightarrow\ &R \text{ ist ein faktorieller Ring} \\ \Rightarrow\ &R \text{ ist ein Integritätsbereich.} \end{aligned}$$

Beweis. Sei σ die Gradabbildung und $I \subseteq R$ ein beliebiges Ideal. Ist $I = (0)$, so ist I ein Hauptideal. Sei also $I \neq (0)$. Definiere $m = \min\{\delta(a) \colon a \in I, a \neq 0\}$ und $0 \neq a \in I$ mit $\delta(a) = m$. Behauptung: $I = (a)$. Es gilt immer $(a) \subseteq I$. Sei nun $0 \neq b \in I$. Dann existieren $q, r \in R$ mit $b = qa + r$ und $r = 0$ oder $0 \leq \delta(r) < \delta(a)$. Da $r = b - qa \in I$ folgt wegen der Wahl von a, dass $r = 0$ und $b = qa \in (a)$ gilt. □

Die Umkehrungen in dem Satz sind alle falsch. $\mathbb{Z}$ ist ein euklidischer Ring, aber kein Körper. Es gibt Hauptidealbereiche, die nicht euklidisch sind (wird in dieser Vorlesung nicht behandelt). Wir werden später beweisen, dass $\mathbb{Z}[X]$ faktoriell, aber kein Hauptidealbereich ist. Schließlich ist $\mathbb{Z}[\sqrt{-5}]$ ein Integritätsbereich, der kein faktorieller Ring ist (s.o.).

Definition 4.23. Sei R ein Integritätsbereich. Seien $a_1, \ldots, a_n \in R$.

(i) $d \in R$ heißt *größter gemeinsamer Teiler* von $a_1, \ldots, a_n$, wenn gilt:
   (a) $d | a_i$ für $i = 1, \ldots, n$.
   (b) Ist $e \in R$ mit $e | a_i$ für $i = 1, \ldots, n$, so gilt $e | d$.

   Wir schreiben dann $\mathrm{ggT}(a_1, \ldots, a_n)$ für d.

(ii) $v \in R$ heißt *kleinstes gemeinsames Vielfaches* von $a_1, \ldots, a_n$, wenn gilt:
   (a) $a_i | v$ für $i = 1, \ldots, n$.
   (b) Ist $u \in R$ mit $a_i | u$ für $i = 1, \ldots, n$, so gilt $v | u$.

   Wir schreiben dann $\mathrm{kgV}(a_1, \ldots, a_n)$ für v.

Bemerkung 4.24. $\mathrm{ggT}(a_1, \ldots, a_n)$ und $\mathrm{kgV}(a_1, \ldots, a_n)$ sind bis auf Assoziiertheit eindeutig (Übungsaufgabe). a, b heißen *teilerfremd*, wenn $\mathrm{ggT}(a, b) = 1$ gilt.

Satz 4.25. Sei R ein faktorieller Ring, $a_1, \ldots, a_n \in R \setminus \{0\}$, $\mathcal{P}$ ein Vertretersystem der Primelemente von R und

$$a_i = e_i \prod_{p \in \mathcal{P}} p^{v_p(a_i)} \text{ für } i = 1, \ldots, n$$

die Primfaktorzerlegungen von $a_1, \ldots, a_n$. Dann existieren ggT und kgV und es gilt

$$\mathrm{ggT}(a_1, \ldots, a_n) = \prod_{p \in \mathcal{P}} p^{\min(v_p(a_1), \ldots, v_p(a_n))},$$

$$\mathrm{kgV}(a_1, \ldots, a_n) = \prod_{p \in \mathcal{P}} p^{\max(v_p(a_1), \ldots, v_p(a_n))}.$$

Beweis. Man beachte, dass für

$$\prod_{p \in \mathcal{P}} p^{v_p(a)} | \prod_{p \in \mathcal{P}} p^{v_p(b)}$$

$v_p(a) \leq v_p(b)$ für alle $p \in \mathcal{P}$ gelten muss. Nun folgt die Behauptung. □

Satz 4.26. Sei R ein Hauptidealbereich und $a_1, \ldots, a_n \in R$. Ist d der ggT von $a_1, \ldots, a_n$, so gilt $(d) = (a_1, \ldots, a_n)$. Insbesondere sind $a, b \in R$ genau dann teilerfremd, wenn $R = (a, b)$ gilt.

Beweis. Da $d | a_i$ gilt, folgt $(d) \supseteq (a_i)$ für alle i. Daher $(d) \supseteq (a_1, \ldots, a_n)$. Nun ist R ein Hauptidealbereich, also gilt $(a_1, \ldots, a_n) = (c)$ für ein $c \in R$. Dann ist aber auch c ein Teiler aller a_i. Aus der Definition des ggT folgt, dass $c | d$. Dann ist

$$(c) = (a_1, \ldots, a_n) \subseteq (d) \subseteq (c),$$

also $(d) = (a_1, \ldots, a_n)$. □

Der Satz besagt insbesondere, dass der ggT d sich darstellen lässt als $d = r_1 a_1 + \ldots + r_n a_n$ für $r_i \in R$. In euklidischen Ringen existiert ein einfacher Algorithmus, den ggT zu berechnen und um letztere Darstellung zu gewinnen.

Satz 4.27. *(Euklidischer Algorithmus)* Sei R ein euklidischer Ring mit Gradabbildung δ. Für Elemente $a, b \in R \setminus \{0\}$ betrachte man die Folge $z_0, z_1, \ldots \in R$, die induktiv gegeben ist durch:

$$\begin{aligned} z_0 &= a \\ z_1 &= b \\ z_{i+1} &= \begin{cases} \text{der Rest der Division von } z_{i-1} \text{ durch } z_i, \text{ falls } z_i \neq 0, \\ 0 \text{ sonst.} \end{cases} \end{aligned}$$

Dann gibt es einen kleinsten Index $n \in \mathbb{N}$ mit $z_{n+1} = 0$. Für dieses n gilt $z_n = \mathrm{ggT}(a, b)$.

Beweis. Nach der Definition der Folge $(z_i)_{i \in \mathbb{N}}$ hat man für $i > 0$ und unter der Voraussetzung $z_i \neq 0$ eine Gleichung der Form

$$z_{i-1} = q_i z_i + z_{i+1} \text{ mit } \delta(z_{i+1}) < \delta(z_i) \text{ oder } z_{i+1} = 0.$$

Die Folge $\delta(z_i)$ ist für $i > 0$ und $z_i \neq 0$ streng monoton fallend. Daher hat die Menge $\mathcal{N} = \{\delta(z_i) \colon z_i \neq 0\}$ ein Minimum und es kann nur endlich viele $z_i \neq 0$ geben. Sei n minimal mit $z_{n+1} = 0$.

Behauptung: z_n teilt z_i für $0 \leq i < n$. Wir beweisen die Behauptung durch eine Induktion nach $n - i$. Für $n - 1$ folgt dies aus der Gleichung $z_{n-1} = q_n z_n$. Sei die Aussage für $n - i$ gezeigt. Aus der Gleichung

$$z_{n-i-1} = q_{n-i} z_{n-i} + z_{n-i+1}$$

folgt aus der Induktionsannahme $z_n|z_{n-i+1}$ und $z_n|z_{n-i}$, dass $z_n|z_{n-i-1}$. Insbesondere gilt $z_n|z_0 = a$ und $z_n|z_1 = b$.

Sei $c \in R$ mit $c|a$ und $c|b$. Wir zeigen durch eine Induktion nach i, dass $c|z_i$ gilt. Insbesondere $c|z_n$ und es folgt $z_n = \mathrm{ggT}(a, b)$. Für $i = 0$ und $i = 1$ gilt $c|z_i$ nach Voraussetzung. Sei nun $i > 1$. Wegen der Gleichung

$$z_{i-1} = q_i z_i + z_{i+1}$$

und der Induktionsannahme gilt $c|z_{i+1}$. □

Bemerkung 4.28. Mit dem $\mathrm{ggT}(a, b)$ hat man in der Situation von 4.27 auch den $\mathrm{kgV}(a, b)$ bestimmt, da

$$ab = \mathrm{ggT}(a, b)\mathrm{kgV}(a, b)$$

gilt.

Beispiel 4.29. Durch den Beweis des Satzes 4.27 lässt sich eine explizite Darstellung des ggT's durch a und b gewinnen. Man muss lediglich die Gleichungen "rückwärts" auflösen. Wir berechnen als Beispiel $\mathrm{ggT}(705, 423)$ in $\mathbb{Z}$. Es gilt:

$$\begin{aligned} z_0 = \quad 705 &= \quad 1 \cdot 423 + 282 \\ z_1 = \quad 423 &= \quad 1 \cdot 282 + 141 \\ z_2 = \quad 282 &= \quad 2 \cdot 141 + 0 \end{aligned}$$

Dann ist

$$\begin{aligned} \mathrm{ggT}(705, 423) &= 141 \\ &= 1 \cdot 423 - 1 \cdot 282 \\ &= 1 \cdot 423 - 1 \cdot (1 \cdot 705 - 1 \cdot 423) \\ &= 2 \cdot 423 - 1 \cdot 705 \end{aligned}$$

Als Anwendung des euklidischen Algorithmus können wir Einheiten in Restklassenringen bestimmen. Zunächst beweisen wir ein Kriterium, wann eine Zahl ein multiplikatives Inverses besitzt.

Satz 4.30. Sei R ein Hauptidealbereich und $a, u \in R$. Genau dann ist $\overline{a} \in R/(u)$ eine Einheit, wenn a und u teilerfremd sind.

Beweis. Seien a, u teilerfremd. Dann existieren $b, v \in R$ mit $1 = ba + uv$. Dann gilt aber $\overline{b}\overline{a} = \overline{1}$ in $R/(u)$.

Sei umgekehrt $\overline{a}$ eine Einheit in $R/(u)$. Dann existiert ein $b \in R$ mit $\overline{b}\overline{a} = \overline{1}$. Daher existiert ein $v \in R$ mit

$$1 - ba = uv \Leftrightarrow 1 = ba + uv.$$

Somit ist $\mathrm{ggT}(a, u) = 1$ und a, u sind teilerfremd. □

In euklidischen Ringen können wir dieses Kriterium mittels des euklidischen Algorithmus testen, da wir einfach

$$\mathrm{ggT}(a, b) = x \cdot a + y \cdot b$$

bestimmen müssen. Insbesondere ist nun $\overline{m} \in \mathbb{Z}/(n)$ genau dann eine Einheit, wenn $\mathrm{ggT}(m, n) = 1$ gilt.

Eine weitere Anwendung ist die Bestimmung aller Lösungen in einem System simultaner Kongruenzen (siehe chinesischer Restsatz). Dort mussten wir gerade Darstellungen der Form $1 = xm + yn$ für teilerfremde Zahlen $m, n \in \mathbb{Z}$ finden.

5. Polynomringe

Alle Ringe in diesem Abschnitt sind **kommutativ**. In der linearen Algebra wurde schon der Polynomring $K[X]$ über einem Körper K betrachtet. Seine Elemente haben die Form

$$a_0 + a_1 X + \cdots + a_n X^n$$

mit $a_i \in K$ und den üblichen Rechenregeln. Zwei Polynome sind genau dann gleich, wenn ihre Koeffizienten übereinstimmen. Es ist aber nicht offensichtlich, dass solch ein Ring überhaupt existiert. Wir werden uns daher zunächst mit der Frage der Existenz des Polynomrings beschäftigen, bevor wir seine Eigenschaften studieren. Hierbei werden wir auch direkt den Koeffizientenkörper durch einen beliebigen kommutativen Ring R ersetzen. Die Idee der folgenden Konstruktion ist es, den Polynomring über seine Koeffizienten zu definieren.

Konstruktion 5.1. Sei

$$R^{\mathbb{N}} \text{ die Menge aller Folgen } (a_n) = (a_0, a_1, \ldots),\ a_n \in R.$$

Definiere auf $R^{\mathbb{N}}$ die Addition

$$(a_n) + (b_n) = (a_n + b_n),$$

d.h. zwei Folgen werden komponentenweise addiert. Dann ist $(R^{\mathbb{N}}, +)$ eine abelsche Gruppe mit Nullelement $0 = (0)$. Definiere die Multiplikation

$$(a_n) \cdot (b_n) = (c_n)$$

mit

$$c_n = \sum_{i=0}^{n} a_i b_{n-i}.$$

Die Multiplikation ist kommutativ, da

$$\sum_{i=0}^{n} a_i b_{n-i} = \sum_{i=0}^{n} b_{n-i} a_i = \sum_{i=0}^{n} b_i a_{n-i}.$$

Sie ist assoziativ, denn

$$((a_n)(b_n))(c_n) = (\sum_{j=0}^{n} a_j b_{n-j})(c_n) = (\sum_{i=0}^{n}(\sum_{j=0}^{i} a_j b_{i-j}) c_{n-i}),$$

$$\sum_{i=0}^{n}(\sum_{j=0}^{i} a_j b_{i-j}) c_{n-i} = \sum_{j=0}^{n} a_j (\sum_{i=j}^{n} b_{i-j} c_{n-i}) = \sum_{j=0}^{n} a_j (\sum_{i=0}^{n-j} b_i c_{n-i-j})$$

und

$$(\sum_{j=0}^{n} a_j (\sum_{i=0}^{n-j} b_i c_{n-i-j})) = (a_n)((b_n)(c_n)).$$

Das neutrale Element der Multiplikation ist $(1, 0, 0, \ldots)$ und man rechnet leicht die Distributivgesetze nach.

Satz 5.2. $R^{\mathbb{N}}$ ist mit der in 5.1 definierten Addition und Multiplikation ein kommutativer Ring. Die Abbildung

$$R \longrightarrow R^{\mathbb{N}},\ a \mapsto (a, 0, 0, \ldots)$$

ist ein Monomorphismus. Insbesondere kann R als Unterring von $R^{\mathbb{N}}$ aufgefasst werden und man schreibt für das Element $(a, 0, 0, \ldots)$ auch einfach a.

Beweis. Nur der Monomorphismus bleibt zu zeigen und dies folgt leicht. □

Der Ring $R^{\mathbb{N}}$ ist noch nicht der gesuchte Polynomring. Zum Beispiel enthält er das Element

$$(1, 1, 1, \ldots)$$

mit unendlich vielen Folgengliedern ungleich Null. Wenn diese Folgenglieder den Koeffizienten eines Polynoms entsprechen sollen, dann dürfen nur endlich viele ungleich Null sein. Daher definieren wir:

Definition 5.3. Sei

$$R^{(\mathbb{N})} = \{(a_n) \colon a_n = 0 \text{ für fast alle } n\}.$$

(Fast alle heißt hier: alle bis auf endlich viele.)

Satz 5.4. $R^{(\mathbb{N})}$ ist ein Unterring von $R^{\mathbb{N}}$ und R ein Unterring von $R^{(\mathbb{N})}$.

Bemerkung 5.5. Sei

$$X = (0, 1, 0, 0, \ldots) \in R^{(\mathbb{N})}.$$

Dann gilt:

$$X^2 = (0, 0, 1, 0, 0, \ldots),\ X^3 = (0, 0, 0, 1, 0, 0, \ldots), \ldots$$

Jedes Element $(a_n) \in R^{(\mathbb{N})}$ hat dann eine eindeutige Darstellung als

$$(a_n) = \sum_n a_n X^n,$$

wobei die Summe wohldefiniert ist, da nur endlich viele a_n ungleich 0 sind. Somit sind zwei Polynome genau dann gleich, wenn ihre Koeffizienten übereinstimmen. Es ist üblich, diese Darstellung auch für Elemente von $R^{\mathbb{N}}$ zu übernehmen.

Definition 5.6. Wir definieren:

(i) Der Ring $R^{(\mathbb{N})}$ heißt der *Polynomring über R* in der *Unbestimmten X*. Seine Elemente heißen *Polynome* über R in X. Man schreibt für $R^{(\mathbb{N})}$ auch $R[X]$. In der Darstellung $\sum_n a_n X^n$ eines Polynoms heißen die Elemente a_n die *Koeffizienten* des Polynoms.

(ii) Der Ring $R^{\mathbb{N}}$ heißt der Ring der *formalen Potenzreihen über R* in der *Unbestimmten X*. Seine Elemente heißen *formale Potenzreihen* über R in X. Man schreibt für $R^{\mathbb{N}}$ auch $R[|X|]$.

Bemerkung 5.7. Die Konstruktion eines Polynomrings kann man iterieren. Z.B. kann man so den Polynomring $(R[X])[Y]$ in zwei Unbestimmten erhalten. Eine andere Möglichkeit ist es, $\mathbb{N}$ sinnvoll durch $\mathbb{N}^n$ zu ersetzen. Dies spielt in dieser Vorlesung jedoch keine Rolle. Im Folgenden untersuchen wir den Ring $R[X]$.

Beachte, dass für zwei Polynome $f = \sum_n a_n X^n$ und $g = \sum_n b_n X^n$ nun wie gewohnt gerechnet werden kann, d.h.

$$f + g = \sum_n (a_n + b_n) X^n,$$

$$f \cdot g = \sum_n (\sum_{i=0}^{n} a_i b_{n-i}) X^n.$$

Definition 5.8. Sei R ein Ring und $f = \sum_{n\in\mathbb{N}} a_n X^n \in R[X]$. Ist $f \neq 0$, dann heißt die Zahl $\operatorname{grad}(f) = \max\{n\colon a_n \neq 0\}$ der *Grad* von f. Das Element $a_{\operatorname{grad}(f)} = \operatorname{Leit}(f)$ heißt der *Leitkoeffizient* von f. f heißt *normiert*, wenn $\operatorname{Leit}(f) = 1$. Für das *Nullpolynom* 0 definiert man $\operatorname{grad}(0) = -\infty$.

Bemerkung 5.9. Seien $f, g \in R[X]$, $\operatorname{grad}(f) = m$, $\operatorname{grad}(g) = n$, $a_m = \operatorname{Leit}(f)$ und $b_n = \operatorname{Leit}(g)$. Dann gilt:

(i) $\operatorname{grad}(f+g) \leq \max\{\operatorname{grad}(f), \operatorname{grad}(g)\}$. Es gilt Gleichheit genau dann, wenn
  (a) $\operatorname{grad}(f) \neq \operatorname{grad}(g)$,
  (b) oder $f = g = 0$,
  (c) oder $\operatorname{grad}(f) = \operatorname{grad}(g)$ und $a_n + b_n \neq 0$.

(ii) $\operatorname{grad}(fg) \leq \operatorname{grad}(f) + \operatorname{grad}(g)$. Es gilt Gleichheit genau dann, wenn
  (a) $f = 0$ oder $g = 0$,
  (b) oder $f \neq 0$, $g \neq 0$ und $a_m b_n \neq 0$ (z.B. in einem Integritätsbereich).

Satz 5.10. Sei R ein Ring. Dann ist $R[X]$ genau dann ein Integritätsbereich, wenn R ein Integritätsbereich ist. In diesem Falle ist $(R[X])^* = R^*$.

Beweis. Ist R ein Integritätsbereich und $0 \neq f, g \in R[X]$. Dann gilt nach 5.9, dass $\operatorname{grad}(fg) = \operatorname{grad}(f) + \operatorname{grad}(g) \neq -\infty$ und daher $fg \neq 0$. Also ist $R[X]$ ein Integritätsbereich. Ist umgekehrt $R[X]$ ein Integritätsring, so ist dies auch R als ein Unterring von $R[X]$.

Man beachte, dass für ein $0 \neq f \in R[X]$ genau dann $\operatorname{grad}(f) = 0$ gilt, wenn $f \in R$. Es gilt immer $R^* \subseteq (R[X])^*$. Sei nun $f \in (R[X])^*$. Dann ist $f \neq 0$ und es existiert ein $0 \neq g \in R[X]$ mit $1 = fg$. Also $0 = \operatorname{grad}(1) = \operatorname{grad}(fg) = \operatorname{grad}(f) + \operatorname{grad}(g)$. Somit ist $\operatorname{grad}(f) = \operatorname{grad}(g) = 0$ und daher $f, g \in R$, speziell $f, g \in R^*$. □

Beispiel 5.11. Ist R kein Integritätsbereich, so ist der Satz falsch. Betrachte $f = 2X + 1 \in \mathbb{Z}/4\mathbb{Z}[X]$. Dann gilt $f^2 = 1$.

Satz 5.12. *(Division mit Rest)* Sei R ein Ring, $f, g \in R[X]$, $g \neq 0$ und $\operatorname{Leit}(g) \in R^*$. Dann existieren eindeutig bestimmte Polynome $q, r \in R[X]$ mit

(i) $f = qg + r$,
(ii) $\operatorname{grad}(r) < \operatorname{grad}(g)$.

Beweis. Existenz: Ist $f = 0$, so setze $q = r = 0$. Sei nun $f \neq 0$. Wir beweisen den Satz durch eine Induktion nach $\operatorname{grad}(f)$.

Sei $\operatorname{grad}(f) = 0$. Ist $\operatorname{grad}(g) = 0$, so gilt $g \in R^*$. Dann können wir $q = g^{-1}f$ und $r = 0$ wählen und erhalten $f = qg$. Ist $\operatorname{grad}(g) > 0$, dann sind $q = 0$ und $r = f$ die gesuchten Elemente mit $f = 0g + r$.

Sei nun $\operatorname{grad}(f) > 0$. Im Falle $\operatorname{grad}(f) < \operatorname{grad}(g)$, kann wieder $q = 0$ und $r = f$ gewählt werden. Betrachte also $\operatorname{grad}(f) \geq \operatorname{grad}(g)$. Sei $m = \operatorname{grad}(f)$, $n = \operatorname{grad}(g)$, $a_m = \operatorname{Leit}(f)$ und $b_n = \operatorname{Leit}(g)$. Definiere

$$q_1 = b_n^{-1} a_m X^{m-n} \text{ und } f_1 = f - q_1 g.$$

Dann ist $\operatorname{grad}(f_1) < \operatorname{grad}(f)$. Nach der Induktionsannahme existieren $q_2, r \in R[X]$ mit $f - q_1 g = f_1 = q_2 g + r$ und $\operatorname{grad}(r) < \operatorname{grad}(g)$. Somit gilt

$$f = (q_1 + q_2)g + r.$$

Wähle nun $q = q_1 + q_2$.

Eindeutigkeit: Sei

$$f = q_1 g + r_1 = q_2 g + r_2 \text{ mit } \operatorname{grad}(r_1), \operatorname{grad}(r_2) < \operatorname{grad}(g),$$

also $(q_1 - q_2)g = r_2 - r_1$. Es gilt $\operatorname{grad}(r_2 - r_1) \leq \max\{\operatorname{grad}(r_1), \operatorname{grad}(r_2)\} < \operatorname{grad}(g)$. Auf der anderen Seite ist $\operatorname{grad}((q_1 - q_2)g) = \operatorname{grad}(q_1 - q_2) + \operatorname{grad}(g)$, da $\operatorname{Leit}(g) \in R^*$ und somit

$$\operatorname{grad}(g) + \operatorname{grad}(q_1 - q_2) = \operatorname{grad}(r_2 - r_1) < \operatorname{grad}(g).$$

Dies ist nur für $q_1 = q_2$ und $r_1 = r_2$ möglich. Dies zeigt die Eindeutigkeit. □

Korollar 5.13. Sei K ein Körper. Dann ist $K[X]$ zusammen mit der Abbildung grad ein euklidischer Ring. Insbesondere ist $K[X]$ ein Hauptidealbereich und faktoriell.

Beispiel 5.14. Die Bestimmung von q und r bei der Division mit Rest ist gerade die aus der Schule bekannte Polynomdivision. Zum Beispiel:

$$\begin{array}{rll} (X^4 + X^2 & +X + 1) & : (X^2 - 1) = X^2 + 2 (= q) \\ -(X^4 - X^2) & & \\ 2X^2 & +X + 1 & \\ -\,(2X^2 & -\,2) & \\ & X + 3 (= r) & \end{array}$$

Satz 5.15. *(Die universelle Eigenschaft des Polynomrings)* Seien R und S Ringe, $\varphi\colon R \longrightarrow S$ ein Ringhomomorphismus und $z \in S$. Dann gibt es einen eindeutig bestimmten Ringhomomorphismus $\Phi\colon R[X] \longrightarrow S$ mit

(i) $\Phi_{|R} = \varphi$,
(ii) $\Phi(X) = z$.

Beweis. Eindeutigkeit: Existiert Φ und ist

$$f = \sum_n a_n X^n \in R[X],$$

so gilt

$$\Phi(f) = \sum_n \Phi(a_n)\Phi(X)^n = \sum_n \varphi(a_n) z^n.$$

Existenz: Definiere

$$\Phi(f) = \sum_n \varphi(a_n) z^n.$$

Es gilt

$$\Phi(1) = \varphi(1) = 1,$$

da φ ein Ringhomorphismus ist. Sei $f = \sum_n a_n X^n$ und $g = \sum_n b_n X^n$. Dann gilt

$$\Phi(f+g) = \sum_n \varphi(a_n + b_n) z^n = \sum_n (\varphi(a_n) + \varphi(b_n)) z^n$$

$$= \sum_n \varphi(a_n) z^n + \sum_n \varphi(b_n) z^n = \Phi(f) + \Phi(g)$$

und

$$\Phi(f \cdot g) = \sum_n \varphi(\sum_{i=0}^{n} a_i b_{n-i}) z^n = \sum_n (\sum_{i=0}^{n} \varphi(a_i)\varphi(b_{n-i})) z^n$$

$$= (\sum_i \varphi(a_i) z^i)(\sum_j \varphi(b_j) z^j) = \Phi(f) \cdot \Phi(g).$$

□

Beispiele 5.16. Betrachte:

(i) Sei R ein Unterring eines Rings S, $\varphi\colon R \longrightarrow S$ die Inklusion und $b \in S$. Das Bild von $R[X]$ unter Φ bezeichnet man dann mit $R[b]$. Für $f \in R[X]$ heißt $f(b) := \Phi(f)$ der *Wert* von f an der Stelle b. Man sagt auch, dass $R[b]$ aus R durch *Adjunktion* des Elements b und $f(b)$ durch *Substitution* des Elements b entsteht.

Insbesondere ist damit erklärt, was der Wert $f(b)$ eines Polynoms $f \in R[X]$ an der Stelle $b \in R$ ist. Gilt $f(b) = 0$, dann heißt b eine *Nullstelle* von f (in R). Somit ist b genau dann eine Nullstelle von f, wenn f im Kern des Einsetzungshomomorphismus

$$R[X] \longrightarrow R, \quad f \mapsto f(b)$$

ist.

Die Abbildung

$$\varphi\colon R[X] \longrightarrow \mathrm{Abb}(R,R),\ f \mapsto \varphi_f \text{ mit } \varphi_f(b) = f(b)$$

ist ein Ringhomomorphismus (Vorsicht: φ_f ist i.A. kein Ringhomomorphismus von R). Jedes Polynom induziert somit eine polynomiale Abbildung. Diese ist i.A. nicht injektiv. Ist zum Beispiel $R = \mathbb{F}_2$, so ist $\varphi_{2X+1} = \varphi_1$.

(ii) Sei $\varphi\colon R \longrightarrow S$ ein Ringhomomorphismus. Es gibt genau einen Ringhomomorphismus

$$\Phi\colon R[X] \longrightarrow S[X],\ \sum_n a_n X^n \mapsto \sum_n \varphi(a_n) X^n.$$

Man kann zeigen, dass dieser injektiv ist, wenn φ injektiv ist. Ist also insbesondere R ein Unterring von S, so kann $R[X]$ als Unterring von $S[X]$ aufgefasst werden.

Satz 5.17. Sei R ein Ring, $I \subseteq R$ ein Ideal und $\tilde{I}$ das von I in $R[X]$ erzeugte Ideal. Dann gilt:

(i) $\tilde{I} \cap R = I$.
(ii) $R[X]/\tilde{I} \cong (R/I)[X]$.
(iii) $\tilde{I}$ ist genau dann ein Primideal in $R[X]$, wenn I ein Primideal in R ist.

Beweis. Zunächst überlege man sich, dass $\tilde{I}$ gerade die Menge der Polynome aus $R[X]$ ist, deren Koeffizienten zu I gehören. Dann folgt direkt $\tilde{I} \cap R = I$.

Sei $\varphi\colon R \longrightarrow R/I$ der kanonische Epimorphismus. Nach 5.15 existiert ein Epimorphismus $\Phi\colon R[X] \longrightarrow (R/I)[X]$ mit $\Phi(X) = X$ und $\Phi_{|R} = \varphi$. Genau dann ist $\Phi(f) = 0$, wenn die Koeffizienten zu I gehören. Somit $\mathrm{Ker}(\Phi) = \tilde{I}$. Aus dem Homomorphiesatz folgt (ii). Schließlich folgt (iii) aus folgenden Äquivalenzen:

$$I \text{ Primideal } \Leftrightarrow R/I \text{ Integritätsbereich}$$

$$\Leftrightarrow (R/I)[X] \cong R[X]/\tilde{I} \text{ Integritätsbereich} \Leftrightarrow \tilde{I} \text{ Primideal.}$$

□

Satz 5.18. Sei R ein Ring und $0 \neq f \in R[X]$. Dann ist $b \in R$ genau dann eine Nullstelle von f, wenn $(X - b)|f$ in $R[X]$.

Beweis. Gilt $(X-b)|f$, so ist $f = (X-b)g$. Also $f(b) = (b-b)g = 0$. Sei nun b eine Nullstelle von f. Teile f mit Division mit Rest durch $X - b$. Dann existieren $q, r \in R[X]$ mit $f = q \cdot (X-b) + r$ und $\mathrm{grad}(r) \leq 0$. Es gilt $0 = f(b) = q(b) \cdot 0 + r(b) = r(b)$ und daher $r = 0$, da $0 \neq r \in R$ ein Widerspruch geben würde. Also gilt $(X-b)|f$. □

Satz 5.19. Sei R ein Integritätsbereich und $0 \neq f \in R[X]$ ein Polynom vom Grad n. Dann besitzt f höchstens n Nullstellen in R.

Beweis. Wir beweisen die Aussage durch eine Induktion nach $\mathrm{grad}(f)$. Ist $\mathrm{grad}(f) = 0$, so ist $f \in R$ und f kann keine Nullstellen besitzen. Sei nun $\mathrm{grad}(f) > 0$. Falls f keine Nullstelle besitzt, ist nichts zu zeigen. Sei also b eine Nullstelle von f. Nach 5.18 gilt $f = (X - b)g$ für ein $g \in R[X]$ mit $\mathrm{grad}(g) = \mathrm{grad}(f) - 1$. Nach der Induktionsannahme hat g höchstens $n - 1$ Nullstellen in R. Da b' genau dann eine Nullstelle von f ist, wenn b' eine Nullstelle von $(X-b)$ oder von g ist, hat f höchstens $n - 1 + 1 = n$ Nullstellen. □

Korollar 5.20. Sei R ein Integritätsbereich und $0 \neq f \in R[X]$ ein Polynom vom Grad n. Dann ist f durch seine Werte auf $n + 1$ verschiedenen Elementen von R eindeutig bestimmt.

Beweis. Seien $f, g \in R[X]$ vom Grad $\leq n$, die auf $n + 1$ verschiedenen Elementen von R übereinstimmen. Das Polynom $f - g$ hat den Grad $\leq n$ und mindestens $n+1$ Nullstellen. Daher muss es das Nullpolynom sein und es folgt $f = g$. □

6. Faktorielle Polynomringe: Der Satz von Gauß

In diesem Abschnitt ist R stets ein kommutativer Ring. Es ist leicht Primelemente und irreduzible Elemente von R in $R[X]$ zu verstehen.

Satz 6.1. Sei R ein Integritätsbereich und $a \in R$.

(i) Genau dann ist a ein Primelement in R, wenn a ein Primelement in $R[X]$ ist.
(ii) Genau dann ist a irreduzibel in R, wenn a irreduzibel in $R[X]$ ist.
(iii) Ist der Ring $R[X]$ faktoriell, dann ist auch R faktoriell.

Beweis. (i): Die Aussage ist äquivalent zu aR ist genau dann ein Primideal in R, wenn $aR[X]$ ein Primideal in $R[X]$ ist. Dies wurde in 5.17 bewiesen.
(ii): Dies folgt aus Gradgründen, da jeder Teiler von a den Grad 0 haben muss.
(iii): Dies folgt aus (i) und aus Gradgründen. □

Ziel dieses Abschnitts ist es, die Umkehrung von (iii) zu beweisen, also:

Satz 6.2. *(Gauß)* Sei R ein faktorieller Ring, dann ist auch der Polynomring $R[X]$ faktoriell.

Lemma 6.3. Sei R ein faktorieller Ring, $\mathcal{P}$ ein Repräsentantensystem der Primelemente von R. Dann besitzt jedes Element $0 \neq x = \frac{a}{b} \in Q(R)$ eine eindeutige Darstellung

$$x = \varepsilon \prod_{p \in \mathcal{P}} p^{v_p(x)}$$

mit $\varepsilon \in R^*$, $v_p(x) \in \mathbb{Z}$ und fast alle $v_p(x) = 0$. Insbesondere ist $x \in R$ genau dann, wenn alle $v_p(x) \in \mathbb{N}$.

Beweis. Existenz: Sei

$$a = \varepsilon_a \prod_{p \in \mathcal{P}} p^{v_p(a)} \text{ und } b = \varepsilon_b \prod_{p \in \mathcal{P}} p^{v_p(b)}$$

mit $\varepsilon_a, \varepsilon_b \in R^*$, $v_p(a), v_p(b) \in \mathbb{N}$ und fast alle $v_p(a) = 0$ bzw. $v_p(b) = 0$. Dann ist

$$x = \varepsilon_a \varepsilon_b^{-1} \prod_{p \in \mathcal{P}} p^{v_p(a) - v_p(b)}.$$

O.E. kann angenommen werden, dass immer $v_p(a) = 0$ oder $v_p(b) = 0$ gilt.

Eindeutigkeit: Sei

$$x = \varepsilon' \prod_{p \in \mathcal{P}} p^{v'_p(x)}$$

eine weitere Darstellung. Definiere

$$c = \prod_{p \in \mathcal{P}, v'_p(x) \geq 0} p^{v'_p(x)} \text{ und } d = \prod_{p \in \mathcal{P}, v'_p(x) < 0} p^{-v'_p(x)}.$$

Dann ist $x = \frac{c}{d}$, also $ad = cb$. Wegen der Wahl von a, b, c, d und der Eindeutigkeit der Primfaktorzerlegung in R folgt nun $a = c$ und $b = d$ und damit die Behauptung. □

Definition 6.4. Sei R ein faktorieller Ring, $\mathcal{P}$ ein Repräsentantensystem der Primelemente von R und $0 \neq f = \sum a_n X^n \in Q(R)[X]$. Dann definieren wir:

(i) $v_p(f) = \min\{v_p(a_n)\colon a_n \neq 0\}$.
(ii) $I(f) = \prod_{p\in\mathcal{P}} p^{v_p(f)}$ heißt der *Inhalt* von f. Dieser Ausdruck ist definiert, aber abhängig von $\mathcal{P}$.
(iii) f heißt *primitiv*, wenn $I(f) \in R^*$ (d.h. $f \in R[X]$ und der ggT der Koeffizienten ist 1).

Beispiel 6.5. Für normierte Polynome $f \in R[X]$ gilt, dass f primitiv ist.

Ist $g = 2X^2 + 6 \in \mathbb{Z}[X]$, dann ist $v_2(g) = 1, v_3(g) = 0$ und $v_p(g) = 0$ für alle Primzahlen $p \neq 2, 3$.

Lemma 6.6. Sei R ein faktorieller Ring und $\mathcal{P}$ ein Repräsentantensystem der Primelemente von R.

(i) Sei $a \in Q(R)$ und $f \in Q(R)[X]$. Dann ist $I(af) = I(a)I(f) = \varepsilon a I(f)$ für ein $\varepsilon \in R^*$. Ist $a = \prod_{p\in\mathcal{P}} p^{v_p(a)}$, so kann $\varepsilon = 1$ gewählt werden.
(ii) Sei $0 \neq f \in Q(R)[X]$. Dann gibt es ein $g \in R[X]$, $I(g) = 1$ und $f = I(f)g$.
(iii) Sei $f \in R[X]$ irreduzibel und $\operatorname{grad}(f) > 0$. Dann ist f primitiv.
(iv) Sei $f \in R[X]$ primitiv und in $Q(R)[X]$ irreduzibel. Dann ist f in $R[X]$ irreduzibel.

Beweis. Zu (i): Sei $f = \sum_{n\in\mathbb{N}} a_n X^n$. Dann ist $v_p(af) = \min\{v_p(aa_n)\colon a_n \neq 0\} = v_p(a) + v_p(f)$. Somit ist

$$I(af) = \prod_{p\in\mathcal{P}} p^{v_p(af)} = \prod_{p\in\mathcal{P}} p^{v_p(a)} \prod_{p\in\mathcal{P}} p^{v_p(f)} = \varepsilon a I(f)$$

für ein $\varepsilon \in R^*$. Ist $a = \prod_{p\in\mathcal{P}} p^{v_p(a)}$, so kann $\varepsilon = 1$ gewählt werden.

Zu (ii): Sei $g = I(f)^{-1}f$. Dann ist $f = I(f)g$. Ferner $I(g) = I(f)^{-1}I(f) = 1 \in R^*$ und somit ist $g \in R[X]$ und primitiv.

Sei $f = \sum_{n\in\mathbb{N}} a_n X^n$. Es ist $v_p(I(f)^{-1}a_n) \geq 0$ für alle $p \in \mathcal{P}$, also ist $g \in R[X]$.

Zu (iii): Nach (ii) ist $f = I(f)g$ und $g \in R[X]$ primitiv. Außerdem $\operatorname{grad}(g) = \operatorname{grad}(f) > 0$. Da f irreduzibel ist, muss $I(f) \in (R[X])^*$ gelten. Dann ist $I(f) \in R^*$ und somit f primitiv.

Zu (iv): Sei $f = gh$ mit $g, h \in R[X]$. Da f irreduzibel über $Q(R)[X]$ ist, muss $g \in Q(R) \setminus \{0\}$ oder $h \in Q(R) \setminus \{0\}$ gelten. Sei etwa $g \in Q(R) \setminus \{0\}$. Dann ist $\varepsilon g I(h) = I(gh) = I(f) \in R^*$. Da $I(h) \in R$ gilt, folgt $g \in R^*$. Dies war zu zeigen. □

Beispiel 6.7. Sei $f(X) = 2X$, also $I(f) = 2$. Dann ist f in $\mathbb{Q}[X]$ irreduzibel, aber nicht in $\mathbb{Z}[X]$, da hier 2 keine Einheit ist.

Lemma 6.8. *(Gauß)* Sei R ein faktorieller Ring und $\mathcal{P}$ ein Repräsentantensystem der Primelemente von R. Seien $0 \neq f, g \in Q(R)[X]$. Dann gilt:

$$I(fg) = I(f)I(g).$$

Beweis. Sei $f = I(f)f_1$ und $g = I(g)g_1$ mit $f_1, g_1 \in R[X]$ primitiv und $I(f_1) = I(g_1) = 1$. Dann ist

$$fg = I(f)I(g)f_1g_1$$

und damit

$$I(fg) = I(f)I(g)I(f_1g_1)$$

Es genügt zu zeigen, dass $I(f_1 g_1) = 1$ gilt. Wir können also o. E. annehmen, dass $f, g \in R[X]$ und $I(f) = I(g) = 1$ gilt.

Dann ist zu zeigen, dass für alle $p \in \mathcal{P}$ gilt $v_p(fg) = 0$. Sei $p \in \mathcal{P}$ fest gewählt, $\operatorname{grad}(f) = m$, $\operatorname{grad}(g) = n$

$$f = \sum_{i=0}^{m} a_i X^i, g = \sum_{j=0}^{n} b_j X^j, fg = \sum_{k=0}^{m+n} c_k X^k.$$

Es ist z. z., dass ein $k \in \{0, \ldots, m+n\}$ existiert mit $v_p(c_k) = 0$, d.h $p \nmid c_k$. Da $I(f) = 1$, existiert ein maximales $r \in \{0, \ldots, n\}$ mit p teilt nicht a_r. Wähle analog $s \in \{0, \ldots, m\}$ maximal mit p teilt nicht b_s. Dann ist

$$c_{r+s} = \sum_{i+j=r+s} a_i b_j = a_r b_s + \sum_{i>0} a_{r+i} b_{s-i} + \sum_{i>0} a_{r-i} b_{s+i}.$$

Für $i > 0$ gilt $p | a_{r+i} b_{s-i}$, da $p | a_{r+i}$. Für $i < 0$ gilt $p | a_{r-i} b_{s+i}$, da $p | b_{s+i}$. Da aber p nicht $a_r b_s$ teilt (p ist ein Primelement), folgt, dass p nicht c_{r+s} teilt. Dies zeigt die Behauptung. □

Korollar 6.9. Sei R ein faktorieller Ring. Seien $0 \neq f \in R[X]$ mit $\operatorname{grad}(f) > 0$. Dann sind folgende Aussagen äquivalent:

(i) f ist irreduzibel in $R[X]$,
(ii) f ist irreduzibel in $Q(R)[X]$ und f ist primitiv.

Beweis. (ii) ⇒ (i): Dies wurde in 6.6 gezeigt.

(i) ⇒ (ii): Nach 6.6 ist f primitiv. Insbesondere gilt $I(f) \in R^*$. Sei nun $f = gh$ mit $g, h \in Q(R)[X]$. Dann folgt $I(f) = I(g)I(h)$. Somit ist

$$I(f)^{-1} f = I(g)^{-1} g I(h)^{-1} h.$$

Da $I(f)^{-1} f$ irreduzibel in $R[X]$ und $I(g)^{-1} g, I(h)^{-1} h \in R[X]$ gilt, folgt o.E., dass $I(g)^{-1} g \in (R[X])^* = R^*$, also $g \in (Q(R)[X])^* = Q(R) \setminus \{0\}$.

□

Korollar 6.10. Sei R ein faktorieller Ring. Seien $0 \neq f, g \in R[X]$, f primitiv, $h \in Q(R)[X]$ und $g = fh$. Dann gilt $h \in R[X]$. D. h. teilt f ein Element g in $Q(R)[X]$, dann teilt f das Element g in $R[X]$.

Beweis. Es ist $I(g) = I(f)I(h)$. Da f primitiv ist, gilt $I(f) \in R^*$. Also $I(h) = I(f)^{-1} I(g) \in R$ und daher $h \in R[X]$. □

Beweis. (Beweis des Satzes von Gauß) Sei R ein faktorieller Ring, $0 \neq f \in R[X] \setminus R^*$. Der Ring $Q(R)[X]$ ist ein euklidischer Ring, also faktoriell. Somit existieren $f_1, \ldots, f_n \in Q(R)[X]$ irreduzibel mit $f = f_1 \cdots f_n$. Sei $c = \prod_{i=1}^{n} I(f_i)$ und $\tilde{f}_i = I(f_i)^{-1} f_i$. Dann folgt

$$I(\tilde{f}_i) = 1, \quad \tilde{f}_i \in R[X], \quad f = c \prod_{i=1}^{n} \tilde{f}_i \text{ mit } c = I(f) \in R.$$

Also ist c ist ein Produkt von Primelementen von R, die auch Primelemente von $R[X]$ sind (siehe 6.1).

$\tilde{f}_i$ ist primitiv und irreduzibel in $Q(R)[X]$. Nach 6.9 sind $\tilde{f}_i$ irreduzibel in $R[X]$. Es bleibt folgende Behauptung zu zeigen: Ist $f \in R[X]$ irreduzibel und primitiv, dann ist f ein Primelement.

Sei $g, h \in R[X]$ mit $f|gh$ in $R[X]$. Insbesondere gilt $f|gh$ in $Q(R)[X]$. Da f irreduzibel in $Q(R)[X]$ ist folgt, dass f ein Primelement in $Q(R)[X]$ ist. Somit $f|g$ oder $f|h$ in $Q(R)[X]$. Da f primitiv ist, folgt aus 6.10, dass $f|g$ oder $f|h$ in $R[X]$. Also ist f ein Primelement in $R[X]$. □

Beispiel 6.11. Betrachte:

(i) Sei K ein Körper. Dann ist $K[X]$ faktoriell. Dies war schon bekannt aus der Tatsache, dass $K[X]$ ein Hauptidealbereich ist.
(ii) $\mathbb{Z}[X]$ ist faktoriell, aber kein Hauptidealbereich.

7. Irreduzibilitätskriterien

Auch in diesem Abschnitt sei R stets ein kommutativer Ring. Wir werden Kriterien entwickeln, wann Polynome z.B. über $\mathbb{Q}[X]$ bzw. $\mathbb{Z}[X]$ irreduzibel sind.

Beispiel 7.1. Sei $f = X^3 + aX^2 + bX + c \in \mathbb{Z}[X]$. Dann ist f genau dann irreduzibel in $\mathbb{Q}[X]$, wenn f keine Nullstelle in $\mathbb{Z}$ hat:

Beweis. Es gilt:

$$f \text{ irreduzibel in } \mathbb{Q}[X] \Leftrightarrow f \text{ irreduzibel in } \mathbb{Z}[X], \text{ da } f \text{ primitiv}$$

Ferner ist f reduzibel in $\mathbb{Z}[X]$ genau dann, wenn es $g, h \in \mathbb{Z}[X]$ gibt, $f = gh$, mit $\operatorname{grad}(g) = 1$ und $\operatorname{grad}(h) = 2$, also f wegen g eine Nullstelle in $\mathbb{Z}$ hat. □

Problem: Welche Polynome sind irreduzibel in $R[X]$ (bzw. in $Q(R)[X]$)? Teilt man durch den Inhalt, so kann o.E. angenommen werden, dass die Polynome primitiv sind.

Satz 7.2. *(Eisensteinsches Irreduzibilitätskriterium)* Sei R ein faktorieller Ring, $0 \neq f = \sum_{i=0}^{n} a_i X^i \in R[X]$ primitiv, $\operatorname{grad}(f) = n > 0$. Weiter sei $p \in R$ ein Primelement mit $p \nmid a_n$, $p|a_i$ für $i = 0, \ldots, n-1$, $p^2 \nmid a_0$. Dann ist f irreduzibel in $R[X]$ und somit auch in $Q(R)[X]$.

Beweis. Angenommen $f = gh$ mit $g = \sum_{i=0}^{n_g} b_i X^i$, $h = \sum_{i=0}^{n_h} c_i X^i$, $\operatorname{grad}(g) = n_g$ und $\operatorname{grad}(h) = n_h$. O.E. gilt $n_g, n_h > 0$, da f primitiv ist. (Wäre etwa $n_g = 0$, so würde aus $I(g)I(h) = I(f) \in R^*$ folgen, dass $g \in R^*$).

Da $p|a_0 = b_0 c_0$, folgt $p|b_0$ oder $p|c_0$. Sei o.E. $p|c_0$. Dann kann nicht $p|b_0$ gelten, da sonst $p^2|a_0$ ein Widerspruch wäre. Da $p \nmid a_n = b_{n_g} c_{n_h}$ folgt, dass $p \nmid b_{n_g}$ und $p \nmid c_{n_h}$.

Sei nun $r = \min\{j : p \nmid c_j\}$. Es gilt $0 < r \leq n_h < n = n_h + n_g$. Betrachte

$$a_r = b_0 c_r + \sum_{i=1}^{r} b_i c_{r-i}.$$

Es gilt $p \nmid b_0 c_r$ und $p|b_i c_{r-i}$ für $i = 1, \ldots r$ wegen der Wahl von r. Somit gilt $p \nmid a_r$. Dies ist ein Widerspruch zur Voraussetzung, da $0 < r < n$. □

Beispiel 7.3. Sei p eine Primzahl, dann ist $X^n - p$ irreduzibel in $\mathbb{Z}[X]$.

Lemma 7.4. Sei R ein Integritätsbereich. Dann gilt:

(i) Sei $\varphi\colon R \longrightarrow R$ ein Automorphismus und $a \in R$. Dann ist a irreduzibel genau dann, wenn $\varphi(a)$ irreduzibel ist.

(ii) Sei $a \in R$ und $\varepsilon \in R^*$. Dann ist die Abbildung $\varphi\colon R[X] \longrightarrow R[X], f(X) \mapsto f(\varepsilon X + a)$ ein Automorphismus. Insbesondere ist $f(X)$ irreduzibel genau dann, wenn $f(\varepsilon X + a)$ irreduzibel ist.

Beweis. Zu (i): Trivial.

Zu (ii): Man sieht leicht, dass φ ein Homomorphismus ist. Die Abbildung

$$\psi\colon R[X] \longrightarrow R[X], \quad f(X) \mapsto f(\varepsilon^{-1}(X - a))$$

ist die Umkehrabbildung zu φ. Somit ist φ ein Automorphismus. □

Beispiel 7.5. Behauptung: Sei p eine Primzahl, dann ist $f(X) = \sum_{i=0}^{p-1} X^i$ irreduzibel in $\mathbb{Z}[X]$.

Die Behauptung ist äquivalent zu: $f(X+1) = \sum_{i=0}^{p-1}(X+1)^i$ ist irreduzibel in $\mathbb{Z}[X]$. Es gilt $(X-1)f(X) = X^p - 1$. Also ist $Xf(X+1) = (X+1)^p - 1$ und somit

$$f(X+1) = \frac{(X+1)^p - 1}{X} = \frac{\sum_{i=1}^{p} \binom{p}{i} X^i}{X} = \sum_{i=0}^{p-1} \binom{p}{i+1} X^i.$$

Nun sieht man, dass $f(X+1)$ irreduzibel nach dem Eisensteinkriterium ist.

Satz 7.6. *(Reduktionsmethode)* Sei R faktoriell, $0 \neq f = \sum_{i=0}^{n} a_i X^i$ primitiv, $\operatorname{grad}(f) = n$, $P \subset R$ ein Primideal, $a_n \notin P$, $\overline{R} = R/P$ und $\overline{f} = \sum_{i=0}^{n} \overline{a_i} X^i \in \overline{R}[X]$ mit $\overline{a_i} = a_i + P$. Wenn $\overline{f}$ irreduzibel in $\overline{R}[X]$ ist, so folgt, dass f irreduzibel in $Q(R)[X]$ und $R[X]$ ist.

Beweis. Es genügt zu zeigen, dass f irreduzibel in $R[X]$ ist.

Angenommen: $f = gh$ mit $g, h \in R[X]$, $\operatorname{grad}(g) > 0$ und $\operatorname{grad}(h) > 0$. (Es kann wieder $\operatorname{grad}(g) = 0$ bzw. $\operatorname{grad}(h) = 0$ ausgeschlossen werden, da f primitiv ist.) Der kanonische Epimorphismus $\varepsilon\colon R \longrightarrow \overline{R}$ induziert einen Epimorphismus

$$\overline{\varepsilon}\colon R[X] \longrightarrow \overline{R}[X], \quad \sum b_i X^i \mapsto \sum \overline{b_i} X^i.$$

Da nach Voraussetzung $\overline{a_n} \neq 0$ gilt folgt, dass $\operatorname{grad}(\overline{f}) = \operatorname{grad}(f) \geq 1$. Es ist $\operatorname{grad}(\overline{g}) \leq \operatorname{grad}(g)$ und $\operatorname{grad}(\overline{h}) \leq \operatorname{grad}(h)$. Da

$$\operatorname{grad}(f) = \operatorname{grad}(g) + \operatorname{grad}(h) \geq \operatorname{grad}(\overline{g}) + \operatorname{grad}(\overline{h}) = \operatorname{grad}(\overline{f}) = \operatorname{grad}(f),$$

folgt $\operatorname{grad}(\overline{g}) = \operatorname{grad}(g)$ und $\operatorname{grad}(\overline{h}) = \operatorname{grad}(h)$. Dann ist $\overline{f} = \overline{g}\overline{h}$ reduzibel ein Widerspruch zur Voraussetzung. □

Beispiel 7.7. Problem: Ist $f = X^4 + 3X + 1$ irreduzibel in $\mathbb{Q}[X]$ bzw. $\mathbb{Z}[X]$?

Betrachte Reduktion mod 2, also $\overline{f} = X^4 + X + 1$ in $\mathbb{F}_2[X]$.

X und $X + 1$ sind die einzig möglichen Linearfaktoren in $\mathbb{F}_2[X]$. Da $\overline{f}(0) = \overline{f}(1) = 1$, besitzt f keine Linearfaktoren.

X^2, $X^2 + X$, $X^2 + 1$ und $X^2 + X + 1$ sind die einzigen möglichen quadratischen Polynome. Keines von diesen teilt $\overline{f}$ (ausrechnen).

Also ist $\overline{f}$ irreduzibel in $\mathbb{F}_2[X]$ und somit f irreduzibel in $\mathbb{Z}[X]$.

8. *Zahlbereichserweiterungen

Dieser Abschnitt ist eine Ergänzung zu dem Kapitel Ringtheorie. Zahlbereichserweiterungen von $(\mathbb{N}, +)$ nach $(\mathbb{Z}, +)$ oder $(\mathbb{Z}, +, \cdot)$ nach $(\mathbb{Q}, +, \cdot)$ sind aus der Schule bekannt. In der Vorlesung und in den Übungen wurden eine Reihe von Resultaten bzgl. dieser Erweiterungen bewiesen. In diesem Abschnitt werden diese Resultate zusammengefasst um sie einheitlich darzustellen.

Zuerst betrachten wir die Erweiterung von $(\mathbb{N}, +)$ nach $(\mathbb{Z}, +)$. Diese ist ein Spezialfall folgender Konstruktion:

Konstruktion 8.1 (Gruppenkomplettierung)**.** Sei $(M, \cdot)$ ein kommutativer Monoid. Definiere $G(M) = M \times M/\sim$, wobei $\sim$ folgende Relation ist:

$$(a_1, b_1) \sim (a_2, b_2) \Leftrightarrow \text{ Es gibt ein } c \in M \text{ mit } a_1 b_2 c = a_2 b_1 c.$$

Man überlegt sich leicht, dass $\sim$ eine Äquivalenzrelation ist. Wir bezeichnen die Äquivalenzklasse von (a, b) mit $[a, b]$. Definiere auf $G(M)$ die Verknüpfung

$$[a_1, b_1] \cdot [a_2, b_2] = [a_1 \cdot a_2, b_1 \cdot b_2].$$

Bemerkung 8.2. Diese Konstruktion wird auch in der Schule für die Einführung von $(\mathbb{Z}, +)$ benutzt. Hier wird $\mathbb{Z}$ über ein Haben-Soll-Modell eingeführt: Das Gesamtguthaben wird aus einem Paar (a, b) natürlicher Zahlen als Differenz $a - b$ errechnet. Diese Paare entsprechen den Elementen von $\mathbb{Z}$, wobei zwei Paare (a_1, b_1) und (a_2, b_2) miteinander identifiziert werden, wenn $a_1 - b_1 = a_2 - b_2$ gilt. (Man überlege sich, warum dies äquivalent zu 8.1 ist.)

Nun gilt:

Satz 8.3. Sei $(M, \cdot)$ ein kommutativer Monoid. Dann gilt:

(i) $(G(M), \cdot)$ ist eine kommutative Gruppe mit neutralem Element $[e, e]$. Die Gruppe $G(M)$ heißt die *Gruppenkomplettierung* von M.
(ii) Die Abbildung $\iota_M \colon M \longrightarrow G(M),\ a \mapsto [a, e]$ ist ein Monoidhomomorphismus.

Beweis. Siehe 7. Übung. □

Bemerkung 8.4. ι_M ist injektiv, wenn in M die "Kürzungsregel" gilt. (Dies ist z.B. in $\mathbb{N}$ der Fall.)

Die Konstruktion $G(M)$ erfüllt natürlich eine universelle Eigenschaft:

Satz 8.5 (Universelle Eigenschaft der Gruppenkomplettierung)**.** Sei M ein kommutativer Monoid.

(i) Sei G eine Gruppe und $\varphi \colon M \longrightarrow G$ ein Monoidhomomorphismus. Zeigen Sie, dass genau ein Gruppenhomomorphismus $\overline{\varphi} \colon G(M) \longrightarrow G$ existiert mit $\varphi = \overline{\varphi} \circ \iota_M$.
(ii) $G(M)$ ist durch die universelle Eigenschaft eindeutig bestimmt. Das heißt, ist H eine weitere Gruppe, für die ein Gruppenhomomorphismus $j_M \colon M \longrightarrow H$ existiert, so dass für alle Gruppenhomomorphismen $\varphi \colon M \longrightarrow G$ genau ein Gruppenhomomorphismus $\overline{\varphi} \colon H \longrightarrow G$ mit $\varphi = \overline{\varphi} \circ j_M$ existiert, dann ist H isomorph zu $G(M)$.

Beweis. Siehe 7. Übung. □

Bemerkung 8.6. Man sieht nun leicht, dass $G((\mathbb{N},+)) \cong (\mathbb{Z},+)$. Da $\iota_{\mathbb{N}}$ injektiv ist, kann $\mathbb{N}$ mit seinem Bild in $G((\mathbb{N},+))$ identifiziert werden und die Gruppenkompletierung entspricht in diesem Falle also wirklich der natürlichen Zahlbereichserweiterung von $(\mathbb{N},+)$ nach $(\mathbb{Z},+)$.

Nun wenden wir uns der Erweiterung von $(\mathbb{Z},+,\cdot)$ nach $(\mathbb{Q},+,\cdot)$ zu. Der direkte Weg wurde in 3.8 behandelt. Dort wurde der Quotientenkörper eines Integritätsbereichs eingeführt. Dieser ist Spezialfall folgender allgemeineren Konstruktion:

Konstruktion 8.7. Eine Teilmenge S eines kommutativen Rings R heißt *multiplikativ abgeschlossen*, wenn $1 \in S$ und für alle $a,b \in S$ auch $ab \in S$ gilt. ($(S,\cdot)$ ist also ein Untermonoid von $(R,\cdot)$.) Sei nun S eine multiplikativ abgeschlossene Menge von R. Wir definieren auf der Menge $\{(a,b)\colon a \in R,\ b \in S\}$ die Äquivalenzrelation:

$$(a_1,b_1) \sim (a_2,b_2) \Leftrightarrow \text{ Es gibt ein } s \in S \text{ mit } a_1b_2s = a_2b_1s.$$

Die Äquivalenzklasse von (a,b) wird mit $\frac{a}{b}$ und die Menge der Äquivalenzklassen mit R_S bezeichnet. Definiere eine Addition und Multiplikation auf R_S wie folgt:

$$\frac{a_1}{b_1}\cdot\frac{a_2}{b_2} = \frac{a_1a_2}{b_1b_2} \text{ und } \frac{a_1}{b_1} + \frac{a_2}{b_2} = \frac{a_1b_2 + a_2b_1}{b_1b_2}.$$

Nun zeigt man wieder, dass die Relation wirklich eine Äquivalenzrelation und die Verknüpfungen wohldefiniert sind.

Satz 8.8. Sei R ein kommutativer Ring und $S \subseteq R$ eine multiplikativ abgeschlossene Menge von R, dann gilt:

(i) R_S ist ein kommutativer Ring. Dieser Ring heißt der *Quotientenring* von R bzgl. S.
(ii) Die Abbildung $\iota_R\colon R \longrightarrow R_S,\ a \mapsto \frac{a}{1}$ ist ein Ringhomomorphismus. Dieser ist genau dann injektiv, wenn S keine Nullteiler enthält.
(iii) Ist R ein Integritätsbereich und $S = R \setminus \{0\}$, dann ist R_S gleich der Quotientenkörper von R.

Beweis. Siehe 8. Übung. □

Satz 8.9 (Universelle Eigenschaft des Quotientenrings)**.** Sei R ein kommutativer Ring und $S \subseteq R$ eine multiplikativ abgeschlossene Menge von R. Dann gilt:

(i) Zu jedem Ringhomomorphismus $\varphi\colon R \longrightarrow R'$ mit $\varphi(S) \subseteq (R')^*$ existiert genau ein Ringhomomorphismus $\overline{\varphi}\colon R_S \longrightarrow R'$ mit $\varphi = \overline{\varphi} \circ \iota_R$
(ii) R_S ist durch die universelle Eigenschaft eindeutig bestimmt. Das heißt, ist T ein weiterer Ring, für den
   (a) ein Ringhomomorphismus $j_R\colon R \longrightarrow T$ existiert, so dass $j_R(S) \subseteq T^*$ und
   (b) für alle Ringhomomorphismen $\varphi\colon R \longrightarrow R'$ mit $\varphi(S) \subseteq (R')^*$ existiert genau ein Ringhomomorphismus $\overline{\varphi}\colon T \longrightarrow R'$ mit $\varphi = \overline{\varphi} \circ j_R$,

   dann ist T isomorph zu R_S.

Beweis. Siehe 9. Übung. □

Die Konstruktion von R_S ist ein sehr nützliches Hilfsmittel in der kommutativen Algebra und algebraischen Geometrie.

Beispiele 8.10. Sei R ein kommutativer Ring.

(i) Sei a ein Nichtnullteiler von R. Dann ist $S = \{a^n : n \in \mathbb{N}\}$ eine multiplikativ abgeschlossene Menge von R. Der Ring R_S wird dann auch mit R_a bezeichnet und es gilt $R_a = \{\frac{b}{a^n} : b \in R,\ n \in \mathbb{N}\}$.

(ii) Sei $P \subset R$ ein Primideal. Die Menge Menge $S = \{a \in R \setminus P\}$ ist multiplikativ abgeschlossen. Der Ring R_S wird dann auch mit R_P bezeichnet. Der Ring R_P hat die Eigenschaft, dass er genau ein maximales Ideal besitzt. Dieses Ideal ist gerade das von P erzeugte Ideal in R_P. (Beachte, dass alle Elemente $a \notin P$ invertierbar in R_P sind.) Ringe mit nur einem maximalen Ideal werden *lokale Ringe* genannt. R_P heißt die *Lokalisierung von R an der Stelle P*.

KAPITEL 3

Körpertheorie

1. Algebraische Körpererweiterungen

Betrachte den Körper $\mathbb{C}$. Nach dem Fundamentalsatz der Algebra besitzt jedes nicht konstante Polynom $f \in \mathbb{C}[X]$ eine Nullstelle. Dies gilt dann erst recht für Polynome aus $\mathbb{Q}[X]$, $\mathbb{R}[X]$ bzw. für $K[X]$, wenn $K \subseteq \mathbb{C}$ ein beliebiger Unterkörper von $\mathbb{C}$ ist.

Ist nun K ein beliebiger Körper und $f \in K[X]$ nicht konstant, so ist nicht offensichtlich, dass ein Körper $K \subseteq L$ existiert, so dass f dort eine Nullstelle besitzt. Ziel ist es, einen solchen Körper zu finden. Zunächst erklären wir den Begriff eines Homomorphismus.

Definition 1.1. Seien K, L Körper. Eine Abbildung $\varphi\colon K \longrightarrow L$ heißt ein *Körperhomomorphismus* (Homomorphismus), wenn φ ein Ringhomomorphismus ist.

Lemma 1.2. Sei $\varphi\colon K \longrightarrow L$ ein Homomorphismus von Körpern. Dann ist φ injektiv. Insbesondere kann K als Unterkörper von L aufgefasst werden.

Beweis. $\mathrm{Ker}(\varphi)$ ist ein Ideal, dass wegen $\varphi(1) = 1$ nicht K ist. Da K nur die Ideale $\{0\}$ und K besitzt, muss $\mathrm{Ker}(\varphi) = \{0\}$ gelten. Daher ist φ injektiv. □

Definition 1.3. Sei L ein Körper und K ein Teilkörper. Dann heißt das Paar $K \subseteq L$ eine *Körpererweiterung*. Man schreibt hierfür L/K.

Nun können wir Nullstellen für beliebige nicht konstante Polynome $f \in K[X]$ in einem geeigneten Erweiterungskörper finden.

Satz 1.4. Sei K ein Körper und $0 \neq f \in K[X]$ mit $\mathrm{grad}(f) > 0$ (d.h. f ist nicht konstant). Dann gibt es eine Körpererweiterung L/K und ein $a \in L$ mit $f(a) = 0$. Ist f irreduzibel, so kann $L = K[X]/(f)$ gewählt werden.

Beweis. Ist f nicht irreduzibel, so wähle einen irreduziblen Faktor von f.

Also kann o.E. angenommen werden, dass f irreduzibel ist. Dann ist (f) ein maximales Ideal, da $K[X]$ ein Hauptidealbereich ist, und $L = K[X]/(f)$ ein Körper. Man bilde die Komposition von Abbildungen

$$K \hookrightarrow K[X] \xrightarrow{\varepsilon} K[X]/(f) = L,$$

wobei ε der kanonische Epimorphismus ist. Die resultierende Abbildung $K \longrightarrow L$ ist injektiv und wir können L als Erweiterungskörper von K auffassen, indem wir K mit seinem Bild in L identifizieren. Sei nun $a = \varepsilon(X)$. Ist $f = \sum_{i=0}^{n} b_i X^i \in K[X]$, dann gilt

$$f(a) = \sum_{i=0}^{n} b_i a^i = \varepsilon(\sum_{i=0}^{n} b_i X^i) = \varepsilon(f) = 0.$$

D.h. a ist Nullstelle von f in L. □

Nun hat f auf jeden Fall eine Nullstelle in dem Körper L. Indem das Verfahren auf die Teiler von f angewendet wird, erhält man:

Korollar 1.5. Sei K ein Körper und $0 \neq f \in K[X]$ mit $\operatorname{grad}(f) > 0$. Dann gibt es eine Körpererweiterung L/K, so dass f in L $\operatorname{grad}(f)$ viele Nullstellen besitzt. Insbesondere zerfällt f in $L[X]$ in Linearfaktoren, d.h. es gibt $a_1, \ldots, a_{\operatorname{grad}(f)} \in L$ mit

$$f = (X - a_1) \cdots (X - a_{\operatorname{grad}(f)}).$$

Bemerkung 1.6. Sei $f \in K[X]$ irreduzibel. In 1.4 wurde der Körper L als $K[X]/f$ und $a = \varepsilon(X)$ mit

$$\varepsilon : K[X] \longrightarrow L,\ X \mapsto \overline{X} = a$$

gewählt. Beachte, dass für ein $g \in K[X]$ gilt $\varepsilon(g(X)) = g(a)$. Die Struktur von L wird durch f bestimmt. Ist o.E. f normiert und $f = X^n + a_{n-1}X^{n-1} + \cdots + a_1X + a_0$, dann gilt gerade

$$(*) \quad a^n = -(a_{n-1}a^{n-1} + \cdots + a_1a + a_0).$$

Die Elemente von L lassen sich wie folgt beschreiben: Sei $g \in K[X]$. Dividiere g durch f mit Rest und erhalte $g = qf + r$ mit $\operatorname{grad}(r) < \operatorname{grad}(f)$. Dann ist $\varepsilon(g) = \varepsilon(r) \in L$. Sind andererseits $r, s \in K[X]$ mit $\operatorname{grad}(r), \operatorname{grad}(s) < \operatorname{grad}(f)$ und $s \neq r$, so ist $\varepsilon(r) \neq \varepsilon(s)$. Elemente von L lassen sich also eindeutig durch Polynome vom Grad kleiner als $\operatorname{grad}(f)$ beschreiben, indem man das Element a "einsetzt". Die Abbildung

$$K^n \longrightarrow L,\ (b_{n-1}, \ldots, b_0) \mapsto b_{n-1}a^{n-1} + \cdots + b_0$$

ist bijektiv und K-linear. Damit ist L als K-Vektorraum beschrieben. In L wird nun auf folgende Weise multipliziert. Hat man zwei Elemente $b_{n-1}a^{n-1} + \cdots + b_0$ und $c_{n-1}a^{n-1} + \cdots + c_0$, dann wird die Multiplikation wie gewohnt ausgeführt und dann die Potenzen a^m mit $m \geq n$ durch $(*)$ sukzessive ersetzt.

Inverse Elemente lassen sich auch durch f bestimmen. Sei $0 \neq b_{n-1}a^{n-1} + \cdots + b_0 \in L$. Betrachte $g = b_{n-1}X^{n-1} + \cdots + b_1X + b_0 \in K[X]$. Da f irreduzibel ist, sind f und g teilerfremd. Daher existieren $u, v \in K[X]$ mit

$$1 = uf + vg.$$

Die Restklasse $\varepsilon(v) \in L$ ist dann das inverse Element zu $b_{n-1}a^{n-1} + \cdots + b_0 = \varepsilon(g)$.

Nun betrachten wir die umgekehrte Situation. Ist eine Körpererweiterung L/K vorgegeben und a in L. Dann stellt sich die Frage, wann a Nullstelle eines Elements $f \in K[X]$ ist.

Definition 1.7. Sei L/K eine Körpererweiterung. Ein Element $a \in L$ heißt *algebraisch* über K, wenn ein $0 \neq f \in K[X]$ existiert mit $f(a) = 0$. Falls a nicht algebraisch ist, so heißt a *transzendent* über K. Die Körpererweiterung L/K heißt *algebraisch*, wenn jedes Element $a \in L$ algebraisch über K ist.

Beispiel 1.8. Sei L/K eine Körpererweiterung.

(i) Alle Elemente $a \in K$ sind algebraisch über K, da für $f(X) = X - a$ gilt $f(a) = 0$.

(ii) Ist $K = \mathbb{Q}$ und $L = \mathbb{C}$, so ist $\sqrt{2}$ algebraisch und e transzendent über K.

(iii) Die Körpererweiterung $\mathbb{C}/\mathbb{R}$ ist algebraisch. Jede Komplexe Zahl $a + bi$, $a, b \in \mathbb{R}$ ist Nullstelle von $X^2 - 2aX + a^2 + b^2 \in \mathbb{R}[X]$.

(iv) $\mathbb{R}/\mathbb{Q}$ ist nicht algebraisch. Wir wissen, dass $\mathbb{R}$ nicht abzählbar ist. Hingegen ist die Menge

$$\mathbb{A} = \{z \in \mathbb{C} \colon f(z) = 0 \text{ für ein } f \in \mathbb{Q}[X], f \neq 0\}$$

der *algebraischen Zahlen* abzählbar: $\mathbb{Q}$ ist abzählbar. Daher auch $\mathbb{Q}^{n+1}$. Letztere Menge lässt sich bijektiv auf die Menge aller Polynome vom Grad $\leq n$ abbilden, indem man $(a_0, \ldots, a_n) \in \mathbb{Q}^{n+1}$ das Polynom $a_0 + \cdots + a_n X^n$ zuordnet. Als abzählbare Vereinigung abzählbarer Mengen ist daher $\mathbb{Q}[X]$ abzählbar. Jedes Polynom $0 \neq f \in \mathbb{Q}[X]$ hat nur endlich viele Nullstellen. Daher ist $\mathbb{A}$ als Vereinigung abzählbarer vieler endlicher Mengen selber abzählbar.

Satz 1.9. Sei L/K eine Körpererweiterung und $M \subseteq L$.

(i) Es existiert ein kleinster Teilkörper $L' \subseteq L$ mit
   (a) $K \subseteq L'$,
   (b) $M \subseteq L'$.
   Dieser wird mit $K(M)$ bezeichnet.

(ii) Es existiert ein kleinster Ring $R \subseteq L$ mit
   (a) $K \subseteq R$,
   (b) $M \subseteq R$.
   Dieser wird mit $K[M]$ bezeichnet.

Ist $M = \{a_1, \ldots, a_n\}$ so schreiben wir auch $K(a_1, \ldots, a_n)$ bzw. $K[a_1, \ldots, a_n]$.

Beweis. Definiere

$$L' = \bigcap_{M, K \subseteq U \subseteq L \text{ Körper}} U$$

und

$$R = \bigcap_{M, K \subseteq U \subseteq L \text{ Ring}} U.$$

Dann erfüllen L' und U die Behauptungen. □

Bemerkung 1.10. Speziell in der Situation $M = \{a\}$ gilt

$$K[a] = \{b_0 + b_1 a + \cdots + b_n a^n \colon n \in \mathbb{N},\ b_i \in K\}$$

und $K(a)$ ist der Quotientenkörper von $K[a]$ in L. Diese Objekte sind uns schon bekannt.

Nun können wir algebraische Elemente auf verschiedene Weisen charakterisieren.

Satz 1.11. Sei L/K eine Körpererweiterung, $a \in L$ und $\varphi \colon K[X] \longrightarrow L,\ g \mapsto g(a)$ der Einsetzungshomomorphismus. Dann sind folgende Aussagen äquivalent:

(i) a ist algebraisch über K.
(ii) φ ist nicht injektiv.
(iii) $K[a]$ ist ein Körper.
(iv) $K[a] = K(a)$.

(v) $\mathrm{Ker}(\varphi)$ wird von einem irreduziblen normierten Polynom $f_a \in K[X]$ erzeugt und dieses ist das eindeutig bestimmte normierte Polynom kleinsten Grades mit $f(a) = 0$.

Beweis. Das Bild von φ ist auf jeden Fall als Unterring von L ein Integritätsbereich. Daher ist $\mathrm{Ker}(\varphi)$ immer ein Primideal.

(i) $\Leftrightarrow$ (ii): Ergibt sich aus der Definition eines algebraischen Elements.

(ii)$\Leftrightarrow$ (iii): Genau dann ist φ nicht injektiv, wenn $\mathrm{Ker}(\varphi) \neq \{0\}$. Also $\mathrm{Ker}(\varphi) = (f)$ und f ein Primelement. Da $K[X]$ ein Hauptidealbereich ist, ist f irreduzibel und daher $\mathrm{Ker}(\varphi)$ ein maximales Ideal. Daher ist $K[a] \cong K[X]/\mathrm{Ker}(\varphi)$ ein Körper.

(ii) $\Leftrightarrow$ (v): Dies ist mit bewiesen worden bewiesen, wenn man noch fordert, dass f normiert ist. Eindeutigkeit: Ist g ein Polynom mit $g(a) = 0$, dann ist $g \in \mathrm{Ker}(\varphi)$ und daher gilt $g = fq$ für ein $q \in K[X]$. Also ist $\mathrm{grad}(g) \geq \mathrm{grad}(f)$ und $f|g$. Gilt $\mathrm{grad}(g) = \mathrm{grad}(f)$, so ist $q \in K$. Ist g auch normiert, so muss $q = 1$ und daher $f = g$ gelten.

(iii)$\Leftrightarrow$ (iv): Dies folgt aus 1.9. □

Definition 1.12. Sei L/K eine Körpererweiterung und $a \in L$ algebraisch über K. Das Polynom f_a aus 1.11 heißt das *Minimalpolynom* von a über K.

Beispiel 1.13. Betrachte:

(i) $X^2 + 1$ ist das Minimalpolynom von $i \in \mathbb{C}$ über $\mathbb{R}$.
(ii) $X^2 - 2$ ist das Minimalpolynom von $\sqrt{2} \in \mathbb{R}$ über $\mathbb{Q}$.
(iii) Ist $f \in K[X]$ irreduzibel, $L = K[X]/(f)$, dann ist f das Minimalpolynom von der Restklasse von X in L (siehe 1.4).

Sei L/K eine Körpererweiterung. Dann definieren die Addition und die Multiplikation eine K-Vektorraumstruktur auf L.

Definition 1.14. Sei L/K eine Körpererweiterung. Die K-Vektorraumdimension $\dim_K(L) = [L\colon K]$ heißt der *Grad* von L über K. Die Körpererweiterung heißt *endlich* oder *unendlich*, je nachdem ob $[L\colon K]$ endlich oder unendlich ist.

Beispiel 1.15. Betrachte:

(i) Es gilt $L = K$ genau dann, wenn $[L\colon K] = 1$.
(ii) Es ist $[\mathbb{C} : \mathbb{R}] = 2$. Eine Basis ist durch $1, i$ gegeben.

Satz 1.16. Sei L/K eine Körpererweiterung, $a \in L$ algebraisch über K und das Minimalpolynom f_a besitze den Grad n. Die Substitution $X \mapsto a$ induziert einen Isomorphismus $K[X]/(f_a) \cong K[a] = K(a)$. Die Potenzen $1, a, \ldots, a^{n-1}$ bilden eine K-Basis von $K(a)$. Insbesondere ist $K(a)/K$ eine endliche Körpererweiterung mit $[K(a) : K] = n$.

Beweis. Dies folgt aus dem Beweis in 1.11. Es gilt $K(a) = K + Ka + \cdots + Ka^{n-1}$. Wir zeigen nur noch, dass $1, a, \ldots, a^{n-1}$ linear unabhängig über K sind (siehe auch 1.6). Wären $1, a, \ldots, a^{n-1}$ linear abhängig, so würden $b_i \in K$ existieren mit

$$\sum_{i=0}^{n-1} b_i a^i = 0.$$

Definiere $g = \sum_{i=0}^{n-1} b_i X^i \in K[X]$. Dann gilt $g(a) = 0$ und $\operatorname{grad}(g) < n = \operatorname{grad}(f_a)$. Dies ist ein Widerspruch, da f_a das Minimalpolynom von a ist. □

Beispiel 1.17. Betrachte die Körpererweiterung $\mathbb{R}/\mathbb{Q}$. Sei p eine Primzahl und $0 \neq n \in \mathbb{N}$. Dann ist nach dem Eisensteinschen Kriterium das Polynom $f = X^n - p$ irreduzibel und somit das Minimalpolynom von $\sqrt[n]{p}$. Daher ist $\sqrt[n]{p}$ algebraisch mit $[\mathbb{Q}(\sqrt[n]{p})\colon \mathbb{Q}] = n$. Insbesondere kann $\mathbb{R}/\mathbb{Q}$ nicht endlich sein.

Satz 1.18. Seien L/K und M/L Körpererweiterungen. Dann gilt die Gradformel:

$$[M\colon K] = [M\colon L][L\colon K].$$

Beweis. Sei $[M\colon L] < \infty$ und $[L\colon K] < \infty$. Wähle eine L-Vektorraumbasis $v_1, \ldots, v_r$ von M und eine K-Vektorraumbasis $w_1, \ldots, w_s$ von L. Wir behaupten, dass $v_i w_j$, $i = 1, \ldots, r$, $j = 1, \ldots, s$ eine K-Vektorraumbasis von M ist. Daraus folgt dann die Gradformel.

Sei $x \in M$. Dann existieren $l_i \in L$ mit $x = \sum_{i=1}^{r} l_i v_i$. Für jedes l_i gibt es $a_{ij} \in K$ mit $l_i = \sum_{j=1}^{s} a_{ij} w_j$. Dann folgt

$$x = \sum_{i=1}^{r} \sum_{j=1}^{s} a_{ij} w_j v_i$$

und somit sind die Elemente $v_i w_j$ ein K-Vektorraumerzeugendensystem von M/K.

Seien $b_{ij} \in K$ mit

$$0 = \sum_{i=1}^{r} \sum_{j=1}^{s} b_{ij} v_i w_j = \sum_{i=1}^{r} (\sum_{j=1}^{s} b_{ij} w_j) v_i.$$

Da die v_i linear unabhängig über L sind, folgt für $i = 1, \ldots, r$

$$\sum_{j=1}^{s} b_{ij} w_j = 0.$$

Da die w_j linear unabhängig über K sind, folgt für $i = 1, \ldots, r$ und $j = 1, \ldots, s$, dass $b_{ij} = 0$ gilt. Also sind die Elemente $v_i w_j$ linear unabhängig und sie bilden somit eine K-Basis von M.

Wir haben darüber hinaus gezeigt, dass mit $[M\colon L] \geq m$ und $[L\colon K] \geq n$ folgt, dass $[M\colon K] \geq mn$. Ist also $[M\colon L] = \infty$ oder $[L\colon K] = \infty$, dann ist auch $[M\colon K] = \infty$. □

Korollar 1.19. Seien L/K, M/L Körpererweiterungen und $[M\colon K]$ endlich. Dann ist $[L\colon K]$ endlich und $[L\colon K] | [M\colon K]$.

Korollar 1.20. Seien L/K, M/L Körpererweiterungen und $[M\colon K]$ eine Primzahl. Dann ist $L = M$ oder $L = K$.

Beispiel 1.21. Es ist $[\mathbb{Q}(\sqrt{3})\colon \mathbb{Q}] = 2$. Also besitzt $\mathbb{Q}(\sqrt{3})/\mathbb{Q}$ keine Zwischenkörper.

Definition 1.22. Sei L/K eine Körpererweiterung.

(i) L/K heißt *endlich erzeugt*, wenn $a_1, \ldots, a_n \in L$ existieren mit

$$L = K(a_1, \ldots, a_n).$$

(ii) L/K heißt eine *einfache Körpererweiterung*, wenn ein $a \in L$ existiert mit $L = K(a)$.

Bemerkung 1.23. Es gilt immer:

$$K(a_1, \ldots, a_n) = Q(K[a_1, \ldots, a_n]).$$

Satz 1.24. Sei L/K eine Körpererweiterung. Dann sind folgende Aussagen äquivalent:

(i) $[L\colon K] < \infty$ (d.h. L/K ist endlich),
(ii) L/K ist algebraisch und L/K ist endlich erzeugt.

Beweis. (i)⇒(ii): Ist L/K endlich, so existieren $a_1, \ldots, a_n \in L$ mit

$$L = Ka_1 + \cdots + Ka_n.$$

Es folgt direkt, dass $L = K(a_1, \ldots, a_n)$ endlich erzeugt ist.

Ist nun $a \in L$ beliebig, dann gilt nach der Gradformel $[K(a)\colon K] < \infty$. Dann ist a algebraisch über K nach 1.11.

(ii)⇒(i): Seien $a_1, \ldots, a_n \in L$ mit $L = K(a_1, \ldots, a_n)$. Für alle i ist

$$K(a_1, \ldots, a_i)/K(a_1, \ldots, a_{i-1})$$

einfach und algebraisch, da a_i bereits algebraisch über K ist. Daher gilt

$$[K(a_1, \ldots, a_i)\colon K(a_1, \ldots, a_{i-1})] = n_i < \infty.$$

Nun beweist man durch eine einfache Induktion

$$[L\colon K] = \prod_i n_i < \infty.$$

Daher ist L/K endlich. □

Korollar 1.25. Jede endliche Körpererweiterung ist algebraisch.

Bemerkung 1.26. Aus einer endlich erzeugten Körpererweiterungen L/K folgt nicht, dass L/K endlich ist. Betrachte etwa $\mathbb{Q}(e)/\mathbb{Q}$. Es gibt algebraische Körpererweiterungen, die nicht endlich sind.

Satz 1.27. Sei L/K eine Körpererweiterung. Definiere

$$\overline{K} = \{a \in L\colon a \text{ algebraisch über } K\}.$$

Dann ist $\overline{K}$ ein Körper. Dieser heißt der *algebraische Abschluss* von K in L.

Beweis. Seien $a, b \in \overline{K}$ und $b \neq 0$. Behauptung: $a - b, ab^{-1} \in \overline{K}$. Daraus folgt dann, dass $\overline{K}$ ein Körper ist.

Es gilt $a - b, ab^{-1} \in K(a, b)$. Wir zeigen, dass $K(a, b)/K$ algebraisch ist. Daraus folgt die Behauptung. Es genügt zu zeigen, dass $[K(a, b) : K] < \infty$ gilt.

Da a algebraisch über K ist, gilt $[K(a) : K] < \infty$. Sei $g \in K[X]$ das Minimalpolynom von b über K. Es gilt $g(b) = 0$. Ferner ist $g \in K(a)[X]$. Also ist b algebraisch über $K(a)$. Sei $f \in K(a)[X]$ das Minimalpolynom von b über $K(a)$. Wir wissen, dass $f|g$ in $K(a)[X]$. Daher gilt

$$[K(a, b) : K(a)] \leq [K(b) : K] < \infty$$

Nach der Gradformel folgt

$$[K(a,b):K] = [K(a,b):K(a)][K(a):K] < \infty.$$

□

Beispiel 1.28. Sei etwa

$$\overline{\mathbb{Q}} = \{a \in \mathbb{C} \colon a \text{ algebraisch über } \mathbb{Q}\}.$$

Es ist $\overline{\mathbb{Q}}/\mathbb{Q}$ algebraisch. Aber $[\overline{\mathbb{Q}} \colon \mathbb{Q}] = \infty$, da etwa für eine Primzahl p und $0 \neq n \in \mathbb{N}$ immer $\sqrt[n]{p} \in \overline{\mathbb{Q}}$ mit $[\mathbb{Q}(\sqrt[n]{p}) \colon \mathbb{Q}] = n$ gilt.

Die Eigenschaft "Algebraisch" ist transitiv.

Satz 1.29. Seien M/L und L/K Körpererweiterungen. Dann sind folgende Aussagen äquivalent:

(i) M/K ist algebraisch,
(ii) M/L und L/K sind algebraisch.

Beweis. Ist M/K ist algebraisch, so folgt direkt, dass M/L und L/K algebraisch sind.

Seien nun M/L und L/K algebraisch. Wähle $a \in M$ beliebig. Da a algebraisch über L ist, existiert ein Polynom $0 \neq f = \sum_{i=0}^{n} a_i X^i \in L[X]$ mit $f(a) = 0$. Dann ist a bereits über dem Körper $K(a_0, \ldots, a_n)$ algebraisch. Daraus folgt

$$[K(a_0, \ldots, a_n, a) : K(a_0, \ldots, a_n)] < \infty.$$

Da L/K algebraisch ist, sind die Elemente a_i algebraisch über K. Eine Induktion nach n zeigt

$$[K(a_0, \ldots, a_n) : K] < \infty.$$

Nach der Gradformel gilt nun

$$[K(a_0, \ldots, a_n, a) : K] = [K(a_0, \ldots, a_n, a) : K(a_0, \ldots, a_n)][K(a_0, \ldots, a_n) : K] < \infty,$$

also ist $K(a_0, \ldots, a_n, a)$ algebraisch über K. Dies bedeutet speziell, dass a algebraisch über K ist. □

2. Zerfällungskörper und endliche Körper

Ist K ein Körper und $f \in K[X]$ ein nicht konstantes Polynom, so existiert wegen 1.4 ein Körper L/K, über dem f in Linearfaktoren zerfällt: Zerfällt f nicht in $K[X]$, so erweitern wir K durch Adjunktion von Nullstellen von f. Dieses Verfahren muss höchstens $\operatorname{grad}(f)$ mal angewendet werden, um den Körper L zu finden. Sind $a_1, \ldots, a_n$ die verschiedenen Nullstellen von f, so zerfällt f schon über $K(a_1, \ldots, a_n)$. Jeder K umfassende Teilkörper von L, über dem f in Linearfaktoren zerfällt, muss $K(a_1, \ldots, a_n)$ enthalten. Somit ist dies der kleinste K umfassende Teilkörper von L, über dem f in Linearfaktoren zerfällt. Dies motiviert folgende Definition:

Definition 2.1. Sei K ein Körper und $f \in K[X]$ mit $\operatorname{grad}(f) > 0$. Ein Erweiterungskörper L von K heißt *Zerfällungskörper* von f (über K), wenn folgendes gilt:

(i) f zerfällt über L vollständig in Linearfaktoren.

(ii) Die Körpererweiterung L/K wird von den Nullstellen von f erzeugt.

Zerfällungskörper sind daher endliche Körpererweiterungen über dem Grundkörper.

Beispiel 2.2.

(i) Sei $f = X^3 - 1 = (X-1)(X^2+X+1) \in \mathbb{Q}[X]$. Dann hat f die Nullstellen 1, $a = (1 + i3\sqrt{2})/2$ und $b = a^2$. Damit ist $b \in \mathbb{Q}[a]$ und f zerfällt über $\mathbb{Q}[a]$ in Linearfaktoren.

Diesem Beispiel liegt folgende Überlegung zugrunde: Ist $g \in K[X]$ ein Polynom mit $\operatorname{grad}(g) = 2$ und ist c eine Nullstelle von g, dann muss g über $K[c]$ in Linearfaktoren zerfallen.

(ii) Sei $g = X^3 - 2$. Dieses Polynom ist irreduzibel über $\mathbb{Q}$ (z.B. Eisensteinkriterium anwenden). $\sqrt[3]{2}$ ist eine Nullstelle von g. Definiere $K = \mathbb{Q}[\sqrt[3]{2}]$. Dann gilt $[K : \mathbb{Q}] = 3$. Aber K ist nicht der Zerfällungskörper von g, da $K \subseteq \mathbb{R}$ und g die nicht reellen Nullstellen $c = \sqrt[3]{2}a$ und $d = \sqrt[3]{2}b$ besitzt (a und b wie in (i)). Sei $g = (X - \sqrt[3]{2})h$. Dann hat $h \in K[X]$ den Grad 2 und wenn wir $L = K[a]$ setzen, so zerfällt g über L in Linearfaktoren. Es ist $[L : K] = 2$ und daher $[L : \mathbb{Q}] = 6$.

Zerfällungskörper existieren immer, wie wir uns schon überlegt haben. Nun stellt sich die Frage, ob ein Zerfällungskörper eindeutig bestimmt ist.

Definition 2.3. Seien L/K, L'/K Körpererweiterungen und $\varphi\colon L \longrightarrow L'$ ein Körperhomomorphismus. φ heißt ein *K-Homomorphismus*, wenn φ eine Fortsetzung der Identität von K ist, d. h. $\varphi_{|K} = \mathrm{id}_K$.

Bemerkung 2.4. Ein K-Homomorphismus ist also ein Ringhomomorphismus $\varphi\colon L \longrightarrow L'$, der gleichzeitig eine K-lineare Abbildung im Sinne der linearen Algebra ist.

Satz 2.5. Sei $f \in K[X]$ ein irreduzibles Polynom über K. Seien a, b Nullstellen von f in Erweiterungskörpern von K. Dann gibt es genau einen Körperisomorphismus $\varphi\colon K(a) \longrightarrow K(b)$ mit

(i) $\varphi_{|K} = \mathrm{id}_K$,
(ii) $\varphi(a) = b$.

Beweis. Sei $\varepsilon\colon K[X] \longrightarrow K(a), h(X) \mapsto h(a)$ der Einsetzungshomomorphismus. Da a algebraisch über K ist, folgt $K(a) = K[a]$ und daher ist ε surjektiv. Da $K[X]$ ein Hauptidealbereich ist, folgt $\operatorname{Ker}(\varepsilon) = (f)$, da f irreduzibel ist. Nach dem Isomorphiesatz induziert ε einen Isomorphismus

$$\varphi_1\colon K[X]/(f) \longrightarrow K(a), \quad h(X) + (f(X)) \mapsto h(a).$$

Analog gibt es einen Isomorphismus

$$\varphi_2\colon K[X]/(f) \longrightarrow K(b), \quad h(X) + (f(X)) \mapsto h(b).$$

Definiere den Isomorphismus

$$\varphi = \varphi_2 \circ \varphi_1^{-1}\colon K(a) \longrightarrow K(b).$$

Da

$$\varphi_{1|K} = \mathrm{id}_K, \quad \varphi_{2|K} = \mathrm{id}_K$$

gilt, folgt $\varphi_{|K} = \mathrm{id}_K$. Ferner ist

$$\varphi(a) = \varphi_2 \circ \varphi_1^{-1}(a) = \varphi_2(X + (f)) = b.$$

Sei λ ein weiterer solcher Isomorphismus. Ist $z \in K(a) = K[a], z = \sum c_i a^i$ mit $c_i \in K$, dann folgt

$$\lambda(z) = \lambda(\sum c_i a^i) = \sum \lambda(c_i)\lambda(a)^i = \sum c_i (b)^i = \varphi(z).$$

□

Satz 2.6. Seien $f \in K[X]$, $\mathrm{grad}(f) > 0$ und L, L' Zerfällungskörper von f über K. Dann existiert ein K-Isomorphismus $\varphi\colon L \longrightarrow L'$. Ferner:

(i) Jeder K-Isomorphismus $\varphi\colon L \longrightarrow L'$ bildet die Nullstellen von f auf die Nullstellen von f ab.

(ii) Sei g ein irreduzibler Faktor von f in $K[X]$, a eine Nullstelle von g in L und b eine Nullstelle von g in L'. Dann gibt es eine Fortsetzung $\varphi\colon L \longrightarrow L'$ mit $\varphi(a) = b$.

Beweis. Wir beweisen die Aussage durch eine Induktion nach $[L : K] < \infty$. Ist $[L : K] = 1$, so folgt $L = K = L'$ und man setzt $\varphi = \mathrm{id}_K$.

Sei nun $[L : K] > 1$. Es gibt einen irreduzibler Faktor g von f in $K[X]$ mit $\mathrm{grad}(g) \geq 2$. Sei a eine Nullstelle von g in L und b eine Nullstelle von g in L'. Nach 2.5 existiert ein K-Isomorphismus $\varphi\colon K(a) \longrightarrow K(b)$ mit $\varphi(a) = b$. Wir können $K(a)$ und $K(b)$ mittels φ identifizieren und annehmen, dass $\tilde{K} = K(a) \subseteq L$ und $a = b$ gilt.

Nun ist L auch ein Zerfällungskörper von f über $\tilde{K}$ und L' ein Zerfällungskörper von f über $\tilde{K}$ (fasse f als Polynom in $\tilde{K}[X]$ auf).

Es ist $[L : \tilde{K}] < [L : K]$ und nach der Induktionsannahme erhalten wir einen K-Isomorphismus $L \cong L'$

Zu (i): Sei $\varphi\colon L \longrightarrow L'$ ein K-Isomorphismus und a eine Nullstelle von f. Dann gilt

$$0 = \varphi(0) = \varphi(f(a)) = f(\varphi(a)).$$

Also ist $\varphi(a)$ eine Nullstelle von f.

Zu (ii): Dies wurde im Induktionsschritt mit bewiesen. □

Man kann mittels dieses Satzes von dem Zerfällungskörper reden. Aber der Isomorphismus ist nicht eindeutig bestimmt. Der Beweis gibt sogar eine Möglichkeit vor, eine beliebe Nullstelle von f auf eine andere Nullstelle abzubilden, sofern sie Nullstellen desselben irreduziblen Faktors sind.

Beispiel 2.7. Sei $f = (X^2 - 2)(X^2 + 1) \in \mathbb{Q}[X]$. Dann ist $\mathbb{Q}(i, \sqrt{2})$ ein Zerfällungskörper von f. Da $X^2 + 1$ auch irreduzibel über $\mathbb{Q}(\sqrt{2})$ ist, existiert ein $\mathbb{Q}(\sqrt{2})$-Isomorphismus

$$\varphi_1\colon \mathbb{Q}(i, \sqrt{2}) \longrightarrow \mathbb{Q}(i, \sqrt{2})$$

mit $\varphi_1(i) = -i$. Ferner gilt $\varphi_1(\sqrt{2}) = \sqrt{2}$. φ_1 ist auch ein $\mathbb{Q}$-Isomorphismus. Analog lässt sich ein $\mathbb{Q}$-Isomorphismus φ_2 konstruieren mit $\varphi_2(\sqrt{2}) = -\sqrt{2}$ und $\varphi_2(i) = i$. Durch Komposition von φ_1 und φ_2 erhält man schließlich noch einen

$\mathbb{Q}$-Isomorphismus φ_3 konstruieren mit $\varphi_3(\sqrt{2}) = -\sqrt{2}$ und $\varphi_3(i) = -i$. Neben der Identität sind dies alle $\mathbb{Q}$-Automorphismen von $\mathbb{Q}(i, \sqrt{2})$, da jeder $\mathbb{Q}$-Isomorphismus durch die Werte von i und $\sqrt{2}$ eindeutig bestimmt ist. Die genauere Untersuchung von Automorphismen von Körpern ist Gegenstand der Galoistheorie.

Als nächstes Ziel wollen wir alle endlichen Körper bestimmen. Wir wissen schon, dass ein endlicher Körper eine Primzahl p als Charakteristik und p^n viele Elemente (für ein $n \in \mathbb{N}$) hat (siehe Kapitel 2, 3.4). Zunächst zeigen wir, dass endliche Körper eindeutig bestimmt sind.

Satz 2.8. Sei L ein endlicher Körper, $\operatorname{char}(L) = p$ und $|L| = p^n$ für ein $n \in \mathbb{N}$. Dann ist L Zerfällungskörper des Polynoms $X^{p^n} - X$ über dem Primkörper $\mathbb{F}_p$ von L. Insbesondere ist jeder Körper mit p^n bis auf Isomorphie eindeutig bestimmt.

Beweis. Die Einheitengruppe L^* von L hat $p^n - 1$ viele Elemente. Nach Kapitel 1, 4.9 (kleiner Fermatscher Satz) gilt $a^{p^n-1} = 1$ für alle $a \in L^*$. Also

$$a^{p^n} - a = 0 \text{ für alle } a \in L.$$

Damit sind alle Elemente von L Nullstellen des Polynoms $X^{p^n} - X \in \mathbb{F}_p[X]$. Der Grad dieses Polynoms ist p^n und somit zerfällt es über L in Linearfaktoren. L ist somit der Zerfällungskörper des Polynoms $X^{p^n} - X \in \mathbb{F}_p[X]$. □

Als nächstes zeigen wir, dass stets ein Körper mit p^n vielen Elementen existiert. Im Folgenden sei R immer ein kommutativer Ring (mit 1).

Definition 2.9. Sei $f = \sum_{i=0}^{n} a_i X^i \in R[X]$. Das Polynom

$$f' = \begin{cases} 0, & \text{falls } f \text{ konstant ist,} \\ \sum_{i=1}^{n} i a_i X^{i-1} & \text{sonst.} \end{cases}$$

heißt die (formale) *Ableitung* von f.

Man rechnet wie aus der Analysis gewohnt:

Satz 2.10. Seien $f, g \in R[X]$, $a \in R$ und $n \in \mathbb{N}$, $n > 0$. Dann gilt:

(i) $(f + g)' = f' + g'$.
(ii) $(af)' = af'$.
(iii) $(fg)' = f'g + fg'$.
(iv) $(f^n)' = nf^{n-1}f'$.

Beweis. Einfaches Nachrechnen. □

Satz 2.11. Sei $f \in R[X]$, $f \neq 0$, $a \in R$. Genau dann ist a eine einfache Nullstelle von f, wenn $f(a) = 0$ und $f'(a) \neq 0$ gilt.

Beweis. Sei $f(a) = 0$. Dann ist $f = (X - a)g$, $g \in R[X]$ (siehe Kapitel 2, 5.18). Hat f in a eine einfache Nullstelle, dann ist $g(a) \neq 0$. Wegen

$$f' = g + (X - a)g'$$

ist dann $f'(a) = g(a) \neq 0$. Ist a eine mehrfache Nullstelle von f, so gilt $f = (X-a)^2 h$ für ein $h \in R[X]$ und

$$f' = 2(X - a)h + (X - a)^2 h,$$

also $f'(a) = 0$. □

Satz 2.12. Sei p eine Primzahl und n eine positive ganze Zahl. Dann ist der Zerfällungskörper des Polynoms $f = X^{p^n} - X$ über $\mathbb{F}_p$ bis auf Isomorphie der einzige Körper mit p^n vielen Elementen.

Beweis. Beachte, dass in $\mathbb{F}_p[X]$ folgendes gilt:

$$(X^{p^n})' = p^n X^{p^n-1} = 0.$$

Daher ist $f' = -1$ und f hat im Zerfällungskörper L über $\mathbb{F}_p$ nur einfache Nullstellen.

Sei nun $N(f)$ die Menge der Nullstellen von f. Der Frobenius-Endomorphismus

$$F\colon L \longrightarrow L,\ x \mapsto x^p$$

ist ein Automorphismus von L (7. Übung). Sei $G = F^n$. Dann ist auch G ein Automorphismus von L. Nun ist

$$N(f) = \{x \in L\colon G(x) = x\}$$

und daher ein Teilkörper von L. Wegen der Definition des Zerfällungskörpers muss $N(f) = L$ gelten. Ferner ist $|L| = p^n$. □

3. Konstruktionen mit Zirkel und Lineal

Als Anwendung der bisher entwickelten Körpertheorie werden wir folgende klassischen Konstruktionsprobleme mit Zirkel und Lineal behandeln:

(i) Quadratur des Kreises,
(ii) Würfelverdoppelung,
(iii) Winkeldreiteilung,
(iv) Konstruktion des regulären n-Ecks.

Wir wollen dies zunächst präzisieren. Wir betrachten die Konstruktionsprobleme in der euklidischen Ebene $\mathbb{E}$, die wir mit $\mathbb{C}$ identifizieren wollen. Sei $M \subseteq \mathbb{C}$ und

(i) $G(M)$ die Menge aller Geraden g, die zwei verschiedene Punkte von M enthalten.
(ii) $K(M)$ die Menge aller Kreise, deren Mittelpunkt ein Element von M und deren Radius gleich dem Abstand zweier verschiedener Punkte von M ist.

Wir nehmen an, dass wir jede Gerade aus $G(M)$ und jeden Kreis aus $K(M)$ konstruieren können.

Bemerkung 3.1. Eine Gerade g soll durch zwei ihrer Punkte gegeben sein, da für $z_0, z_1 \in M$

$$g = g(z_0, z_1) = \{z_0 + r(z_1 - z_0)\colon r \in \mathbb{R}\}.$$

Analog ist ein Kreis k stets durch einen Mittelpunkt und den Radius gegeben, welcher als Abstand zweier Punkte aufgefasst werden kann, da

$$k = k(z_0, z_1, z_2) = \{z \in \mathbb{C}\colon |z - z_0| = |z_1 - z_2|\}.$$

Durch folgende *elementare Konstruktionsschritte* lassen sich neue Punkte gewinnen, die nicht in der gegebenen Menge M liegen müssen:

(i) Schnittpunkt zweier verschiedener Geraden aus $G(M)$.

(ii) Schnittpunkte einer Geraden aus $G(M)$ und eines Kreises aus $K(M)$.
(iii) Schnittpunkte zweier verschiedener Kreise aus $K(M)$.

Definition 3.2. Sei $M \subseteq \mathbb{C}$. Dann ist $\mathrm{Kon}(M)$ die Menge der Punkte $z \in \mathbb{C}$ mit der Eigenschaft, dass eine Kette $M = M_0 \subseteq M_1 \subseteq \cdots \subseteq M_r$ existiert, so dass $z \in M_r$ und M_i entsteht aus M_{i-1} durch Hinzunahme der Punkte, die aus M_{i-1} durch einen elementaren Konstruktionsschritt gewonnen werden. $\mathrm{Kon}(M)$ heißt die aus M durch *Zirkel und Lineal konstruierbaren Punkte*.

Besteht M nur aus einem Punkt, so sind $G(M)$ und $K(M)$ leer und es lassen sich keine neuen Punkte konstruieren. Daher soll M immer mindestens zwei Punkte besitzen und wir wollen stets annehmen, dass $0, 1 \in M$.

Aus der Schule sind folgende Resultate bekannt:

Satz 3.3.

(i) Sind zwei Punkte aus M konstruierbar, dann ist auch der Mittelpunkt der Verbindungsstrecke konstruierbar.
(ii) Ist ein Punkt z_0 und eine Gerade g aus M mit $z_0 \notin g$ konstruierbar, dann ist auch die Senkrechte zu g durch z_0 konstruierbar.
(iii) Ist ein Punkt z_0 und eine Gerade g aus M mit $z_0 \in g$ konstruierbar, dann ist auch die Senkrechte zu g durch z_0 konstruierbar.
(iv) Ist eine Gerade g und ein Punkt z_0 außerhalb g aus M konstruierbar, dann ist auch die parallele Gerade zu g durch z_0 konstruierbar.

Beweis. (i) Seien $z_0, z_1 \in \mathrm{Kon}(M)$. Da der Fall $z_0 = z_1$ trivial ist, wählen wir $z_0 \neq z_1$. Die Kreise um z_0 und z_1 mit dem Abstand $|z_0 - z_1|$ als Radius schneiden sich in zwei verschiedenen Punkten. Deren Verbindungsgerade (ist die Mittelsenkrechte und) schneidet die Gerade durch z_0 und z_1 im gesuchten Mittelpunkt.

(ii) Sei $z_1 \neq z_0$ ein aus M konstruierbarer Punkt von g und r der Abstand von z_1 und z_0. Ein Kreis um z_0 mit Radius $|z_0 - z_1|$ schneidet die Gerade g in den Punkten z_1 und z_1'. Ist $z_1 = z_1'$, so ist die Verbindungsgerade von z_0 und z_1 die gesuchte Senkrechte. Ist $z_1 \neq z_1'$ so bestimmen die Kreise um z_1 und z_1' mit Abstand $|z_1 - z_1'|$ die Senkrechte auf g durch z_0.

(iii) Sei $z_0 \neq z_1 \in g$ ein weiterer Punkt aus $\mathrm{Kon}(M)$. Die Gerade g schneidet den Kreis k mit Mittelpunkt z_0 und Radius $|z_0 - z_1|$ in zwei Punkten z_1, z_1'. Die Kreise um z_1 und z_1' mit Abstand $|z_1 - z_1'|$ bestimmen dann die Senkrechte auf g durch z_0.

(iv) Sei $z_1 \in g$ konstruierbar. Mittels (iii) können wir die Senkrechte g' auf g durch z_1 konstruieren, mit (ii) bzw. (iii) dann auch die Senkrechte g'' auf g' durch z_0. g'' ist dann die gesuchte parallele Gerade von g. □

Nun beweisen wir einige weitere nützliche Aussagen.

Proposition 3.4. Es gilt:

(i) $\mathrm{Kon}(\mathrm{Kon}(M)) = \mathrm{Kon}(M)$.
(ii) Mit $0 \neq z \in \mathrm{Kon}(M)$ ist auch $|z| \in \mathrm{Kon}(M)$
(iii) Mit $0 \neq z \in \mathrm{Kon}(M)$ ist auch $\frac{z}{|z|} \in \mathrm{Kon}(M)$
(iv) Sei $z = a + bi$. Dann ist $z \in \mathrm{Kon}(M)$ genau dann, wenn $a, b \in \mathrm{Kon}(M)$.

Beweis. (i) Dies folgt direkt aus der Definition, da sich ein konstruierbarer Punkt aus endlich vielen elementaren Konstruktionsschritten gewinnen lässt.

(ii) Der Punkt $|z|$ ist der Schnittpunkt der Geraden $g(0,1)$ mit dem Kreis $k(0,0,z)$.

(iii) $\frac{z}{|z|}$ ist als Schnittpunkt von $g(0,z)$ und $k(0,0,1)$ konstruierbar.

(iv) Da $0,1 \in M$, ist die 'x-Achse' $g(0,1)$ und nach 3.3 auch die 'y-Achse' $g(0,i)$ konstruierbar. Ist nun $z = a + bi \in \mathrm{Kon}(M)$, so wiederum nach 3.3 auch a, b. Sind umgekehrt a, b konstruierbar, dann ist auch ib konstruierbar, da der Kreis um Null mit Radius b die Gerade $g(0,i)$ in ib schneidet. Nun ist $a + bi$ aber als Schnittpunkt der Lote durch a und ib auf die Geraden $g(0,1)$ und $g(0,i)$ konstruierbar. □

Folgender Satz liefert den Zugang, wie Konstruktionsprobleme mittels der Körpertheorie angegangen werden können.

Satz 3.5. Sei $M \subseteq \mathbb{C}$ mit $0,1 \in M$. Dann ist $\mathrm{Kon}(M)$ ein Zwischenkörper von $\mathbb{C}/\mathbb{Q}(M \cup \overline{M})$ mit $\overline{M} = \{\overline{z} \in M : z \in M\}$.

Beweis. Wir zeigen:

(i) $z_1, z_2 \in \mathrm{Kon}(M) \Rightarrow z_1 + z_2 \in \mathrm{Kon}(M)$.
(ii) $z \in \mathrm{Kon}(M) \Rightarrow -z \in \mathrm{Kon}(M)$.
(iii) $z_1, z_2 \in \mathrm{Kon}(M) \Rightarrow z_1 \cdot z_2 \in \mathrm{Kon}(M)$.
(iv) $z \in \mathrm{Kon}(M), z \neq 0 \Rightarrow z^{-1} \in \mathrm{Kon}(M)$.
(v) $z \in \mathrm{Kon}(M) \Rightarrow \overline{z} \in \mathrm{Kon}(M)$.

Aus (i)-(iv) folgt, dass $\mathrm{Kon}(M)$ ein Körper ist. Dieser muss $\mathbb{Q}$ enthalten: Aus $1 \in \mathrm{Kon}(M)$ folgt $n \in \mathrm{Kon}(M)$ für alle $n \in \mathbb{N}$. Dann ist aber auch $-n \in \mathrm{Kon}(M)$ und schließlich $\frac{p}{q} \in \mathrm{Kon}(M)$ für alle $p, q \in \mathbb{Z}$. Durch (v) wird bewiesen, dass $\mathbb{Q}(M \cup \overline{M}) \subseteq \mathrm{Kon}(M)$. (Die folgenden Beweise sollte man sich durch Skizzen verdeutlichen.)

Zu (i): Die Kreise $k(z_1, 0, z_2)$ und $k(z_2, 0, z_1)$ schneiden sich in $z_1 + z_2$. (Dies entspricht der Vektoraddition.) Daher ist $z_1 + z_2 \in \mathrm{Kon}(M)$.

Zu (ii): Die Gerade $g(0,z)$ und der Kreis $k(0,0,z)$ schneiden sich in $-z$. Daher ist $-z \in \mathrm{Kon}(M)$.

Zu (iii): Da $z_1 = 0$ oder $z_2 = 0$ trivial ist, wähle $z_1 \neq 0$ und $z_2 \neq 0$. Es ist $z_1 z_2 = z_1 \frac{z_2}{|z_2|} |z_2|$. Daher reicht es, die beiden Fälle $|z_2| = 1$ und $z_2 \in \mathbb{R}^+$ zu betrachten.

Sei $|z_2| = 1$. Die Gerade $g(0, z_1)$ und der Kreis $k(0,0,1)$ schneiden sich in dem Punkt $\frac{z_1}{|z_1|}$. Der Kreis $k(\frac{z_1}{|z_1|}, 1, z_2)$ und der Kreis $k(0,0,1)$ schneiden sich in $\frac{z_1}{|z_1|} z_2$. Schließlich schneiden sich die Gerade $g(0, \frac{z_1}{|z_1|} z_2)$ und der Kreis $k(0,0,z_1)$ in dem Punkt $z_1 z_2$.

Sei nun $z_2 \in \mathbb{R}^+$. Wir unterscheiden wieder zwei Fälle. Der erste Fall ist $z_1 \in \mathbb{R}^+$. Mit Hilfe von 3.3 (iii) lässt sich die Figur eines Strahlensatzes konstruieren: Betrachte die Punkte $1, z_2$ auf der Geraden $g(1, z_2)$. Dann wird (die Länge) z_1 auf der senkrechten Geraden zu $g(1, z_2)$ durch 1 abgetragen und man erhält einen Punkt z_3. Als nächstes wird eine Gerade durch 0 und z_3 gezogen. Schließlich wird eine senkrechte Gerade zu $g(1, z_2)$ durch z_2 abgetragen um einen weiteren Punkt z_4 zu

erhalten. Man erhält dann direkt, dass $z_1 z_2 \in \mathrm{Kon}(M)$ gilt, da dies die Länge der Strecke zwischen z_2 und z_4 ist.

Ist z_1 beliebig, dann ist $|z_1|$ und somit nach dem bisher bewiesenen $|z_1|z_2$ konstruierbar. Aber $z_1 z_2$ ist der Schnittpunkt des Kreises $k(0, 0, |z_1|z_2)$ mit der Geraden $g(0, z_1)$, also auch konstruierbar.

Zu (iv): Es ist $z^{-1} = (\frac{z}{|z|})^{-1}|z|^{-1}$. Da mit z auch $\frac{z}{|z|}$ und $|z|$ konstruierbar sind, reicht es wieder die Fälle $|z| = 1$ und $z \in \mathbb{R}^+$ zu betrachten.

Sei $|z| = 1$. Der Kreis $k(0, 0, 1)$ und der Kreis $k(1, 1, z)$ schneiden sich in z^{-1} und dies zeigt die Behauptung.

Sei $z \in \mathbb{R}^+$. Dies behandelt man wieder mit einer geeigneten Anwendung des Strahlensatzes: Betrachte die Gerade durch $1, z$. Dann wird (die Länge) 1 auf der senkrechten Gerade zu $g(1, z)$ durch den Punkt z abgetragen und eine Gerade durch 0 und dem neu konstruierten Punkt gezogen. Schließlich wird eine senkrechte Gerade zu $g(1, z_2)$ durch 1 abgetragen, um einen weiteren Punkt z' zu erhalten. Die Länge der Strecke zwischen 1 und z' ist z^{-1} und daher gilt $z^{-1} \in \mathrm{Kon}(M)$.

Zu (v): Konstruiere die Senkrechte g zu $g(0, 1)$ durch z. Der zweite Schnittpunkt des Kreises $k(1, 1, z)$ mit g ist $\overline{z}$. (Dies ist eine Spiegelung von z an $g(1, 0)$). □

Satz 3.6. Sei $M \subseteq \mathbb{C}$ mit $0, 1 \in M$. Dann sind folgende Aussagen äquivalent:

(i) $z \in \mathrm{Kon}(M)$.

(ii) Es existiert eine Körperkette $\mathbb{Q}(M \cup \overline{M}) = L_0 \subseteq L_1 \subseteq \cdots \subseteq L_m \subseteq \mathbb{C}$ mit $z \in L_m$ und $[L_i : L_{i-1}] \leq 2$ für $i = 1, \ldots, m$.

Zunächst geben wir einige Folgerungen und Beispiele, bevor der Satz bewiesen wird.

Korollar 3.7. Sei $M \subseteq \mathbb{C}$ mit $0, 1 \in M$, $z \in \mathrm{Kon}(M)$ und f das Minimalpolynom von z über $\mathbb{Q}(M \cup \overline{M})$. Dann ist

$$\mathrm{grad}(f) = [\mathbb{Q}(M \cup \overline{M})(z) : \mathbb{Q}(M \cup \overline{M})]$$

eine Potenz von 2.

Beweis. Sei

$$\mathbb{Q}(M \cup \overline{M}) = L_0 \subseteq L_1 \subseteq \cdots \subseteq L_m \subseteq \mathbb{C}$$

die Körperkette aus 3.6. Dann ist $[L_m : \mathbb{Q}(M \cup \overline{M})]$ nach der Gradformel (1.18) eine Potenz von 2. Da

$$\mathbb{Q}(M \cup \overline{M}) \subseteq \mathbb{Q}(M \cup \overline{M})(z) \subseteq L_m,$$

folgt die Behauptung indem man erneut die Gradformel anwendet. □

Beispiele 3.8. Durch die bisherigen Ergebnisse lässt sich bereits die Unlösbarkeit einiger klassischer Konstruktionsprobleme beweisen.

(i) (Quadratur des Kreises) Die Quadratur des Kreises ist nicht möglich, d.h. es ist nicht möglich zu einem gegebenen Kreis (mit Mittelpunkt und Radius) ein flächengleiches Quadrat mit Zirkel und Lineal zu konstruieren: Wir nehmen an, dass der Kreis den Mittelpunkt 0 und den Radius 1 hat. Sein Flächeninhalt ist dann π. Ein flächengleiches Quadrat hat die Kantenlänge $\sqrt{\pi}$. Sei $M = \{0, 1\}$. Dann gilt $\mathbb{Q}(M \cup \overline{M}) = \mathbb{Q}$. Es ist zu entscheiden, ob

$\sqrt{\pi} \in \mathrm{Kon}(M)$ gilt. Nach 3.6 ist $\mathrm{Kon}(M)/\mathbb{Q}$ algebraisch. Aber $\sqrt{\pi}$ ist transzendent über $\mathbb{Q}$. Also ist die Quadratur des Kreises nicht möglich.

(ii) (Delische Problem der Würfelverdoppelung) Es ist nicht möglich zu einem gegebenen Würfel einen Würfel mit dem doppelten Volumen mit Zirkel und Lineal zu konstruieren: Der vorgegebene Würfel besitze die Kantenlänge 1. Sei wieder $M = \{0, 1\}$. Ein Würfel mit doppelten Volumen hat die Kantenlänge $\sqrt[3]{2}$. Das Minimalpolynom von $\sqrt[3]{2}$ ist $X^3 - 2$ und hat den Grad 3. Also ist die Würfelverdoppelung nach 3.7 nicht möglich.

(iii) (Dreiteilung eines Winkels) Im Allgemeinen ist es nicht möglich einen vorgegebenen Winkel mit Zirkel und Lineal in drei gleiche Teile zu zerlegen: Ein Winkel ist durch einen Punkt $z \in \mathbb{C}$ mit $|z| = 1$ gegeben. Wir zeigen, dass es z. B. nicht möglich ist, den 60°-Winkel dreizuteilen. Sei $M = \{0, 1\}$. Der 60°-Winkel ist aus M als Schnittpunkt des Einheitskreises $k(0, 0, 1)$ und $k(1, 0, 1)$ elementar konstruierbar. Wäre der 20°-Winkel konstruierbar, so müsste der Punkt $\cos(20°) + i \sin(20°)$ in $\mathrm{Kon}(M)$ liegen. Dann gilt aber auch $c = 2\cos(20°) \in \mathrm{Kon}(M)$. Wir zeigen, dass c das Minimalpolynom $f = X^3 - 3X - 1 \in \mathbb{Q}[X]$ hat. Dies ist dann ein Widerspruch. f ist irreduzibel wegen der Reduktionsmethode nach der Primzahl 2. Es gilt

$$c^3 - 3c - 1 = 8\cos^3(20°) - 6\cos(20°) - 1$$

$$= 2(4\cos^3(20°) - 3\cos(20°)) - 1 = 2\cos(60°) - 1 = 0,$$

da $4\cos^3(20°) - 3\cos(20°) = \cos(3x)$ (Additionstheoreme verwenden) und $2\cos(60°) - 1 = 0$. Dies zeigt die Behauptung.

Ein weiteres Beispiel, welches wir behandeln können, ist die Frage, wann ein reguläres n-Eck konstruierbar ist. Hierbei handelt es sich für $n \geq 3$ um die n-Teilung des Winkels von 360°. Zum Beispiel ist dies möglich, wenn $n = 2^m$ gilt, da jeder Winkel mit Zirkel und Lineal halbiert werden kann. Ein reguläres 3-Eck ist konstruierbar, da, wie wir wissen, das 6-Eck konstruierbar ist. Folgender Satz zeigt, dass zwar ein reguläres 5-Eck, aber kein 7-Eck konstruierbar ist. Hierfür benötigen wir einen neuen Begriff:

Definition 3.9. Für $m \in \mathbb{Z}$ heißt $F_m = 2^{2^m} + 1$ die m-te *Fermat'sche Zahl*. Ist F_m prim, so heißt F_m eine *Fermat'sche Primzahl*.

Es ist leicht zu sehen, dass eine Zahl der Form $2^k + 1$ nur dann eine Primzahl sein kann, wenn $k = 0$ oder $k = 2^m$ gilt. $F_0 = 3$, $F_1 = 5$, $F_2 = 17$, $F_3 = 257$, $F_4 = 65537$ sind Fermat'sche Primzahlen. $F_5 = 641 \cdot 6700417$ jedoch nicht. Bis heute sind keine weiteren Fermat'en Primzahlen gefunden worden. Insbesondere ist nicht bekannt, ob unendlich viele Primzahlen dieser Art existieren.

Satz 3.10. Die Primfaktorzerlegung von $n \in \mathbb{N}$ enthalte eine Primzahl $p \geq 3$, die keine Fermatsche Primzahl ist. Dann ist das reguläre n-Eck nicht konstruierbar.

Beweis. Angenommen das reguläre n-Eck ist konstruierbar. Dann ist der Punkt $\cos(\alpha) + i\sin(\alpha)$ mit $\alpha = \frac{360°}{n}$ aus M konstruierbar. Dann ist auch der Punkt $\zeta_p = \cos(\beta) + i\sin(\beta)$ mit $\beta = \frac{360°}{p}$ aus M konstruierbar. Sei L der Zerfällungskörper des Polynoms $f = X^p - 1$ über $\mathbb{Q}$. Die Potenzen von ζ_p sind Nullstellen von f und das

sind die p-verschiedenen komplexen p-ten Einheitswurzeln $\cos(k\beta) + i\sin(k\beta)$ für $k = 1, \ldots, p$. Daher gilt $L = \mathbb{Q}(\zeta_p)$. Nun ist

$$f = (X-1)(X^{p-1} + X^{p-2} + \cdots + 1)$$

und $X^{p-1} + X^{p-2} + \cdots + 1$ ist, wie wir wissen, irreduzibel über $\mathbb{Q}$. Daher ist $[L : \mathbb{Q}] = p - 1$. Nach Voraussetzung ist $p - 1$ aber keine Potenz von 2, im Widerspruch zu 3.7. □

Die Bedingung des Satzes ist nur hinreichend, aber nicht notwendig. Zum Beispiel ist das reguläre $9 = F_3 \cdot F_3$-Eck nicht konstruierbar. Sonst wäre der Punkt $\cos(40°) + i\sin(40°)$ und damit auch $\cos(20°) + i\sin(20°)$ konstruierbar. Dies ist aber nicht möglich, wie wir in 3.8 gesehen haben. Ein notwendiges und hinreichendes Kriterium ist folgender Satz, den wir mit unseren Mittel nicht beweisen können.

Satz 3.11 (Gauß)**.** Das reguläre n-Eck ist genau dann mit Zirkel und Lineal konstruierbar, wenn $n = 2^s \cdot p_1 \cdots p_s$ mit paarweise verschiedenen Fermat'schen Primzahlen p_i.

Die Konstruktion des regulären 17-Ecks war ein erster mathematischer Triumph von Gauß.

Bevor wir 3.6 beweisen, stellen wir einige Hilfsmittel zusammen. Für eine komplexe Zahl $0 \neq z \in \mathbb{C}$ bezeichnen wir mit $\pm\sqrt{z}$ die *Quadratwurzeln* von z (dies sind die zwei Nullstellen des Polynoms $X^2 - z$).

Satz 3.12. Sei $M \subseteq \mathbb{C}$ mit $0, 1 \in M$ und $0 \neq z \in \mathrm{Kon}(M)$. Dann ist auch $\sqrt{z} \in \mathrm{Kon}(M)$.

Beweis. Mit z ist $|z|$ und $\frac{z}{|z|}$ ein Element von $\mathrm{Kon}(M)$. Ferner ist $\sqrt{z} = \sqrt{\frac{z}{|z|}} \cdot \sqrt{|z|}$. Daher reicht es, die Fälle $|z| = 1$ und $z \in \mathbb{R}^+$ zu betrachten.

Sei $|z| = 1$. Dann sind $\pm\frac{1+z}{|1+z|}$ die Quadratwurzeln von z (ausrechnen). Diese Zahlen sind konstruierbar. Daher $\sqrt{z} \in \mathrm{Kon}(M)$.

Sei $z \in \mathbb{R}^+$. Es ist z oder $\frac{1}{z}$ größer oder gleich 1. Ist eine der beiden Wurzeln konstruierbar, dann auch die andere, da $\mathrm{Kon}(M)$ ein Körper ist. Also können wir o.E. annehmen, dass $z > 1$ ($z = 1$ ist trivial). Beachte, dass $\frac{z}{2} \in \mathrm{Kon}(M)$.

Der Kreis $k(\frac{z}{2}, 0, \frac{z}{2})$ schneidet die senkrechte Gerade zu der Geraden $g(0, z)$ im Punkt 1 in einem Punkt $z' = 1 + iy$. Daher ist $z' \in \mathrm{Kon}(M)$ und $|z'| = \sqrt{1 + y^2}$. Nun liegt z' auf dem obigen Kreis und es gilt

$$(\frac{z}{2})^2 = (1 - \frac{z}{2})^2 + y^2 = 1 - z + (\frac{z}{2})^2 + y^2.$$

Daher $z = 1 + y^2$ und $\sqrt{z} = |z'| \in \mathrm{Kon}(M)$. □

Lemma 3.13. Sei $M \subseteq \mathbb{C}$ mit $0, 1 \in M$. Dann gilt $\mathbb{Q}(M \cup \overline{M}) = \overline{\mathbb{Q}(M \cup \overline{M})}$.

Beweis. Sei $L = \mathbb{Q}(M \cup \overline{M})$. Dann ist $\overline{L} = \{z \in \mathbb{C} \colon \overline{z} \in L\}$ wieder ein Körper mit $\mathbb{Q}, M, \overline{M} \subseteq \overline{L}$. Daher $L \subseteq \overline{L}$. Nun gilt $\overline{L} \subseteq \overline{\overline{L}} = L$ und somit folgt die Behauptung. □

Lemma 3.14. Sei $L \subseteq \mathbb{C}$ ein Teilkörper mit $L = \overline{L}$. Dann gilt:

(i) Der Schnittpunkt zweier verschiedener Geraden aus $G(L)$ ist in L enthalten.
(ii) Die Schnittpunkte einer Geraden aus $G(L)$ mit einem Kreis aus $K(L)$ sind in $L(\sqrt{w})$ für ein $w \in L$ enthalten.
(iii) Die Schnittpunkte zweier verschiedener Geraden aus $K(L)$ sind in $L(\sqrt{w})$ für ein $w \in L$ enthalten.

Beweis. Zu (i): Sei z Schnittpunkt zweier verschiedener Geraden. Beachte, dass mit $q, q' \in L$ auch $q - q' \in L$ gilt. Daher existieren

$$z_0 = x_0 + iy_0, \quad z_1 = x_1 + iy_1, \quad w_0 = x_0' + iy_0', \quad w_1' = x_1' + iy_1' \in L.$$

und $r, s \in \mathbb{R}$ mit

$$z = z_0 + rz_1 = z_0' + sz_1'.$$

Zerlegt man dies in Realteil und Imaginärteil, so erhält man ein lineares Gleichungssystem in r und s

$$\begin{aligned} x_0 + rx_1 &= x_0' + sx_1' \\ iy_0 + riy_1 &= iy_0' + siy_1', \end{aligned}$$

in dem wegen $L = \overline{L}$ die Koeffizienten $x_0, x_1, x_0', x_1', iy_0, iy_1, iy_0', iy_1'$ alle Elemente von L sind. Dieses Gleichungssystem ist lösbar, also muss die Lösung auch in L liegen.

Zu (ii): Die Gerade sei durch $\{z_0 + rz_1 \colon r \in \mathbb{R}\}$ mit $z_0 = x_0 + iy_0, z_1 = x_1 + iy_1 \in L$ gegeben und der Kreis durch $k(w_0, w_1, w_2)$ mit $w_0 = x_0' + iy_0', w_1, w_2 \in L$. Beachte, dass $l^2 = |w_1 - w_2|^2$ auch ein Element von L ist. Sei z ein Schnittpunkt der Geraden und des Kreises. Dann ist $z = z_0 + rz_1$ für ein $r \in \mathbb{R}$. Es gilt die Kreisbedingung

$$(rx_1 + x_0 - x_0')^2 - (r(iy_1) + (iy_0) - (iy_0'))^2 = l^2.$$

Dies ist eine lineare oder quadratische Gleichung in r und auch hier sind wieder alle Koeffizienten Elemente von L. Im ersten Fall folgt $r \in L$ und daher $z \in L$. Man kann $w = 1$ setzen. Im zweiten Fall gilt eine Gleichung der Form

$$r^2 + pr + q = 0 \text{ mit } p, q \in L.$$

Dann ist

$$r = -\frac{p}{2} \pm \sqrt{\frac{p^2}{4} - q}.$$

Mit $w = \frac{p^2}{4} - q$ folgt, dass alle Schnittpunkte der Geraden und des Kreises in $L(\sqrt{w})$ enthalten sind.

Zu (iii): Mit $z = x + iy$ und analog zur Bezeichnung in (i) und (ii) erfülle z zwei Kreisgleichungen der Form

$$\begin{aligned} (x - x_0)^2 - (iy - iy_0)^2 &= r_0^2 \\ (x - x_0')^2 - (iy - iy_0')^2 &= (r_0')^2 \end{aligned}$$

mit $x_0, x_0', iy_0, iy_0', r_0^2, (r_0')^2 \in L$. Durch eine Differenzbildung erhält man

$$ax + b(iy) = c \text{ mit } a, b, c \in L \text{ und } (a, b) \neq (0, 0),$$

da dies nach Voraussetzung verschiedene Kreise sind, die sich schneiden. Die letzte Gleichung beschreibt eine Gerade aus $G(L)$ und z ist ein Schnittpunkt dieser Geraden mit den Kreisen. Aus (ii) folgt dann die Behauptung. □

Lemma 3.15. Sei L/K eine Körpererweiterung mit $[L : K] = 2$. Dann existiert ein $a \in L$ mit $a^2 \in K$ und $L = K(a)$.

Beweis. Es existiert ein $b \in L \setminus K$ mit $L = K(b)$. Ist $f \in K[X]$ das Minimalpolynom von b, so gilt $\operatorname{grad}(f) = 2$. Daher ist $f = X^2 + pX + q$ mit $p, q \in K$. Dann ist aber $b = -\frac{p}{2} + \sqrt{\frac{p^2}{4} - q}$ oder $b = -\frac{p}{2} - \sqrt{\frac{p^2}{4} - q}$. Sei $a = \sqrt{\frac{p^2}{4} - q}$. Dann ist $K(a) = K(b)$ und $a^2 \in K$. □

Beweis. (von 3.6) (i) ⇒ (ii): Sei $z \in \operatorname{Kon}(M)$. Dann existiert eine Kette

$$M = M_0 \subseteq \cdots \subseteq M_m$$

von Teilmengen von $\mathbb{C}$ und M_i entsteht aus M_{i-1} durch Hinzunahme der Elemente, die aus einem elementaren Konstruktionsschritt gewonnen werden können. Wir beweisen durch eine Induktion nach i, dass eine Körperkette

$$L_0 = \mathbb{Q}(M_0 \cup \overline{M_0}) \subseteq L_1 \subseteq \cdots \subseteq L_{2i+1} \subseteq L_{2i+2}$$

existiert mit $[L_{2j+2} : L_{2j+1}] \leq 2$, $[L_{2j+1} : L_{2j}] \leq 2$ und $L_{2j+2} = \overline{L_{2j+2}}$ für $j = 0, \ldots, i$, so dass $M_i \subseteq L_{2i+2}$ gilt. Sei nun die Aussage für $i - 1$ bewiesen. Sind z_0 und z_1 diejenigen Elemente mit $M_i = M_{i-1} \cup \{z_0, z_1\}$ (im Falle eines Elements einfach $z_0 = z_1$ setzen), so folgt aus 3.14, dass immer ein $w \in L_{2i}$ existiert mit $z_0, z_1 \in L_{2i}(\sqrt{w})$. Beachte, dass auch $\overline{w} \in \overline{L_{2i}} = L_{2i}$. Definiere $L_{2i+1} = L_{2i}(\sqrt{w})$ und $L_{2i+2} = L_{2i}(\sqrt{w}, \sqrt{\overline{w}})$. Dann gilt

$$[L_{2i+2} : L_{2i+1}] \leq 2, \quad [L_{2i+2} : L_{2i+1}] \leq 2, \quad \overline{L_{2i+2}} = L_{2i+2}.$$

Ferner $M_i \subseteq L_{2i+2}$. Für $i = m$ erhält man schließlich (ii).

(ii) ⇒ (i): Sei

$$\mathbb{Q}(M \cup \overline{M}) = L_0 \subseteq L_1 \subseteq \cdots \subseteq L_m \subseteq \mathbb{C}$$

die Körperkette mit $z \in L_m$ und $[L_i : L_{i-1}] \leq 2$ für $i = 2, \ldots, m$. Nach 3.15 existieren Elemente $a_i \in L_i$ mit $L_i = L_{i-1}(a_i)$ und $a_i^2 \in L_{i-1}$. Wir beweisen durch eine Induktion nach i, dass L_i ein Teilkörper von $\operatorname{Kon}(M)$ ist. Nach 3.5 ist L_0 ein Teilkörper von $\operatorname{Kon}(M)$. Sei nun nach der Induktionsannahme L_{i-1} ein Teilkörper von $\operatorname{Kon}(M)$. Da $L_i = L_{i-1}(a_i)$ und $a_i^2 \in \operatorname{Kon}(M)$, so folgt, dass $L_i \subseteq \operatorname{Kon}(M)$, da nach 3.12 auch $a_i \in \operatorname{Kon}(M)$ gilt. □

Literaturverzeichnis

[1] M. Artin, Algebra, Birkhäuser, Basel, 1993.
[2] S. Bosch, Algebra, Algebra, Springer, Berlin Heidelberg, 2001.
[3] W. Bruns, Einführung in die Algebra, Vorlesungsskript, Osnabrück.
[4] E. Kunz, Algebra, Algebra, Vieweg, Braunschweig Wiesbaden, 1994.
[5] G. Scheja und U. Storch, Lehrbuch der Algebra 1 und 2, Teubner, Stuttgart, 1980.
[6] B. L. van der Waerden, Algebra I und II, Springer, Berlin, 1967.
[7] R. Vogt, Einführung in die Algebra, Vorlesungsskript, Osnabrück.