Skriptum zur Vorlesung

Algebra

Erstellt von Stephan Wagner
nach den Vorlesungsunterlagen von Sophie Frisch

WS 2005/06

Inhaltsverzeichnis

Teil I

Gruppentheorie, 1. Teil

Kapitel 1

Halbgruppen

Definition 1.1 Sei G eine Menge. Eine *innere Verknüpfung* auf G ist eine Funktion $\cdot : G \times G \to G$, $(g, h) \mapsto g \cdot h$. (Man schreibt also den Funktionswert von (g, h) unter $\cdot$ als $g \cdot h$.)

BEMERKUNG: Für $a \cdot b$ schreibt man auch kurz ab.

Definition 1.2 Sei $(G, \cdot)$ eine Menge mit innerer Verknüpfung, $e \in G$. Wenn $\forall g \in G \; e \cdot g = g$ (bzw. $\forall g \in G \; g \cdot e = g$) gilt, dann heißt e ein *linksneutrales* (bzw. *rechtsneutrales*) Element von $(G, \cdot)$. Ein sowohl links- als auch rechtsneutrales Element heißt *neutrales* Element.

Proposition 1.3 Sei $(G, \cdot)$ eine Menge mit einer innerer Verknüpfung, $e, f \in G$. Wenn e linksneutrales Element und f rechtsneutrales Element von $(G, \cdot)$ ist, dann folgt $e = f$.

Beweis: $e \overset{\text{f rechtsneutral}}{=} e \cdot f \overset{\text{e linksneutral}}{=} f$.

□

Korollar 1.4 Wenn $(G, \cdot)$ ein neutrales Element hat, dann ist dieses eindeutig bestimmt.

Definition 1.5 Eine nichtleere Menge G mit einer inneren Verknüpfung $\cdot$, für die

$$\forall a, b, c \in G \;\; (a \cdot b) \cdot c = a \cdot (b \cdot c) \qquad \text{„}\textit{Assoziativität} \text{ von } \cdot \text{“}$$

gilt, heißt *Halbgruppe*. Eine Halbgruppe, in der es ein neutrales Element gibt, heißt *Monoid*.

BEMERKUNG: Das neutrale Element eines Monoids ist eindeutig bestimmt.

BEISPIEL: $(\mathbb{N}, +)$, $(\mathbb{N}_0, +)$, $(\mathbb{N}, \cdot)$, $(\mathbb{N}_0, \cdot)$, $(\mathbb{R}^+, +)$, $(\mathbb{R}^+, \cdot)$ sind Halbgruppen (wobei $\mathbb{N} = \{1, 2, 3, \ldots\}$ (natürliche Zahlen), $\mathbb{N}_0 = \{0, 1, 2, \ldots\}$ (nichtnegative ganze Zahlen), $\mathbb{R}^+ = \{r \in \mathbb{R} \mid r > 0\}$ (positive reelle Zahlen)).

BEISPIEL: Die $n \times n$-Matrizen mit Eintragungen in $\mathbb{Z}$, $(M_n(\mathbb{Z}), \cdot)$, bilden mit der üblichen Matrizenmultiplikation

$$A = (a_{ij})_{1 \le i,j \le n},\ B = (b_{ij})_{1 \le i,j \le n} \Rightarrow A \cdot B = (c_{ij}) \text{ mit } c_{ij} = \sum_{k=1}^{n} a_{ik} b_{kj}$$

ein Monoid. Neutrales Element ist die Einheitsmatrix $I_n = (\delta_{ij})$. BEISPIEL:

$$H_n = (\{0, 1, 2, \ldots, n\}, *) \text{ mit } i * j := \min(i + j, n) = \begin{cases} i + j & i + j < n \\ n & i + j \ge n \end{cases}$$

ist ein Monoid.

BEISPIEL: $\widetilde{H}_n = (\{0, 1, 2, \ldots, n\}, \circ)$ mit $i \circ j := \min(i \cdot j, n)$ ist ein Monoid.

BEISPIEL: Die strikten oberen Dreiecksmatrizen

$$\{(a_{ij})_{1 \le i,j \le n} \mid a_{ij} \in \mathbb{Z},\ a_{ij} = 0 \text{ wenn } j \le i\} \subseteq M_n(\mathbb{Z})$$

bilden eine Halbgruppe ohne neutrales Element.

Definition 1.6 $(M, \cdot)$ sei ein Monoid, e das neutrale Element, $a \in M$;

- $b \in M$ heißt *Rechtsinverses* zu a, wenn $a \cdot b = e$.
- $c \in M$ heißt *Linksinverses* zu a, wenn $c \cdot a = e$.

Wenn $d \in M$ sowohl Links- als auch Rechtsinverses zu a ist, d.h.

$$d \cdot a = e = a \cdot d,$$

dann heißt d *Inverses* zu a. Ein Element, das ein Inverses hat, heißt *invertierbar*.

Proposition 1.7 Sei $(M, \cdot)$ ein Monoid, $a, b, c \in M$, e das neutrale Element. Wenn b Linksinverses zu a und c Rechtsinverses zu a ist, dann gilt $b = c$.

Beweis: Aufgrund der Assoziativität folgt aus $b \cdot a = e$, $a \cdot c = e$:

$$(b \cdot a) \cdot c = b \cdot (a \cdot c) \Rightarrow c = e \cdot c = (b \cdot a) \cdot c = b \cdot (a \cdot c) = b \cdot e = b$$

□

Korollar 1.8 Das Inverse eines Elements (wenn eines existiert) in einem Monoid ist eindeutig bestimmt.

Definition 1.9 Sei $(G, \cdot)$ eine Menge mit innerer Verknüpfung. Wenn

$$\forall\, a, b \in G\ a \cdot b = b \cdot a$$

gilt, dann heißt $(G, \cdot)$ *kommutativ*.

Definition 1.10 Eine Menge G heißt *endlich*,wenn $\exists n \in \mathbb{N}_0$, sodass G gleichmächtig zu $\{0, 1, \ldots, n-1\}$ ist.

Bemerkung: Die Mengen X, Y heißen gleichmächtig, wenn eine bijektive Funktion $f : X \to Y$ existiert.

Bemerkung: Ein wichtiges Monoid ist folgendermaßen gegeben:

X sei eine beliebige Menge, $X^X = \{f : X \to X \mid f \text{ Funktion}\}$, und $\circ$ sei die Hintereinanderausführung von Funktionen, d.h. $g \circ f(x) := g(f(x))$. $(X^X, \circ)$ ist ein Monoid, die identische Funktion id_X ($\mathrm{id}_X(a) = a$) das neutrale Element.

Definition 1.11 Seien X, Y Mengen, $f : X \to Y$ eine Funktion.

- Eine Funktion $g : Y \to X$ heißt *Linksinverse* von f, wenn $g \circ f = \mathrm{id}_X$.
- Eine Funktion $h : Y \to X$ heißt *Rechtsinverse* von f, wenn $f \circ h = \mathrm{id}_Y$.
- Eine Funktion $g : Y \to X$ heißt *Inverse* (*Umkehrfunktion*) von f, wenn $g \circ f = \mathrm{id}_X$ und $f \circ g = \mathrm{id}_Y$; man schreibt f^{-1} für die Inverse.

Bemerkung: Sind X, Y Mengen, $f : X \to Y$ eine Funktion; dann gilt

- f hat eine Linksinverse $\iff$ f injektiv
- f hat eine Rechtsinverse $\iff$ f surjektiv
- f hat eine Inverse (Umkehrfunktion) $\iff$ f bijektiv

Beweis: als Übung.

Definition 1.12 Ein Element a einer Menge mit innerer Verknüpfung $(G, \cdot)$ heißt *linkskürzbar*, wenn $\forall b, c \in G\ (a \cdot b = a \cdot c \Rightarrow b = c)$. Analog heißt a *rechtskürzbar*, wenn $\forall b, c \in G\ (b \cdot a = c \cdot a \Rightarrow b = c)$.

Definition 1.13 Eine Halbgruppe $(H, \cdot)$, in der $\forall a, b, c \in H$ gilt

$$a \cdot b = a \cdot c \Rightarrow b = c \quad \text{(Linkskürzungsregel)} \quad \text{und}$$

$$b \cdot a = c \cdot a \Rightarrow b = c \quad \text{(Rechtskürzungsregel)}$$

heißt *reguläre* Halbgruppe (oder Kürzungshalbgruppe). (Ein kommutatives reguläres Monoid wird auch *Gauß'sches Monoid* genannt.)

Definition 1.14 Sei $(G, \cdot)$ eine Menge mit innerer Verknüpfung, $a \in G$. Die Funktion $L_a : G \to G$ mit $L_a(x) = a \cdot x$ heißt *Linkstranslation* mit a, die Funktion $R_a : G \to G$ mit $R_a(x) = x \cdot a$ heißt *Rechtstranslation* mit a.

Bemerkung: $(G, \cdot)$ sei eine Menge mit innerer Verknüpfung. $a \in G$ ist genau dann linkskürzbar ($a \cdot b = a \cdot c \Rightarrow b = c$), wenn L_a injektiv ist ($L_a(b) = L_a(c) \Rightarrow b = c$); a ist genau dann rechtskürzbar, wenn R_a injektiv ist. Also erfüllt eine Halbgruppe H genau dann die Kürzungsregeln, wenn alle Links- und Rechtstranslationen L_a, R_a für alle $a \in H$ injektiv sind.

Proposition 1.15 (verallgemeinerte Assoziativität) $(H, \cdot)$ sei eine Halbgruppe, $a_1, \ldots, a_n \in H$ ($n \in \mathbb{N}$). Alle Produkte von $a_1, \ldots, a_n$ in dieser Reihenfolge bezeichnen dasselbe Element von H (unabhängig von der Klammerung).

Beweis: als Übung.

Definition 1.16 (Potenzen, Vielfache) Sei $(H, \cdot)$ eine Halbgruppe, $a \in H$, $n \in \mathbb{N}$. Man definiert

$$a^n := \underbrace{a \cdot a \cdot \ldots \cdot a}_{\text{n Stück a}}$$

als das Produkt von n Stück a, unabhängig von der Klammersetzung. Wenn $(H, \cdot)$ ein Monoid mit neutralem Element e ist, dann wird auch $a^0 := e$ definiert.
Sei $(H, +)$ eine Halbgruppe (additiv geschrieben), $a \in H$, $n \in \mathbb{N}$. Man definiert analog

$$na := \underbrace{a + a + \ldots + a}_{\text{n Stück a}}$$

Wenn $(H, +)$ ein Monoid mit neutralem Element e ist, dann wird $0a := e$ definiert.

Kapitel 2

Gruppen

Definition 2.1 Ein Monoid, in dem jedes Element ein Inverses hat, heißt *Gruppe*. Also ist eine Menge G mit einer Funktion $* : G \times G \to G$, $(g, h) \mapsto g * h$ eine Gruppe, wenn folgende Bedingungen erfüllt sind:

1. $G \neq \emptyset$
2. $\forall a, b, c \in G \; a * (b * c) = (a * b) * c$ (Assoziativität)
3. $\exists e \in G$, sodass
   (a) $\forall g \in G \; g * e = g = e * g$ (e ist neutrales Element)
   (b) $\forall g \in G \; \exists g' \in G$ mit $g * g' = e = g' * g$ (jedes $g \in G$ hat Inverses)

Eine kommutative Gruppe heißt *Abelsche Gruppe*.

Bemerkung: Das neutrale Element in einer Gruppe (bereits in einem Monoid) ist eindeutig; das Inverse zu g ist auch eindeutig, da schon in einem Monoid mit neutralem Element e gilt:

$$g' \cdot g = e \; \wedge \; g \cdot g'' = e \Rightarrow g' = g''$$

Notation: Ist $(G, \cdot)$ eine Gruppe (multiplikativ geschrieben), dann bezeichnen wir das Inverse von a mit a^{-1}.
Ist $(H, +)$ eine Gruppe (additiv geschrieben), dann bezeichnen wir das Inverse von a mit $-a$.

Beispiel: $(\mathbb{Z}, +)$, $(\mathbb{R}, +)$, $(\mathbb{R} \setminus \{0\}, \cdot)$, $(\mathbb{C} \setminus \{0\}, \cdot)$, $S^1 = (\{z \in \mathbb{C} \,|\, |z| = 1\}, \cdot)$ sind Gruppen.

Beispiel: $(\mathbb{Z}_n, +)$ $(n \in \mathbb{N})$ ist eine Gruppe.

Dabei sind die Elemente von $\mathbb{Z}_n$ die Äquivalenzklassen der Elemente von $\mathbb{Z}$ bezüglich der Äquivalenzrelation $a \sim b \Leftrightarrow n \,|\, a-b$. Die Klasse von a wird als $\overline{a}$ geschrieben:

$$\begin{aligned}\overline{a} &= \{b \in \mathbb{Z} \,|\, n \,|\, a-b\} = \{b \in \mathbb{Z} \,|\, \exists k \in \mathbb{Z}\ a-b = nk\} \\ &= \{b \in \mathbb{Z} \,|\, \exists k \in \mathbb{Z}\ b = a-nk\} = \{b \in \mathbb{Z} \,|\, \exists j \in \mathbb{Z}\ b = a+nj\} = a+n\mathbb{Z}\end{aligned}$$

$\sim$ ist Kongruenzrelation für $+$, d.h. $a \sim a', b \sim b' \Rightarrow a+b \sim a'+b'$:

$$a' = a+nk,\ b' = b+nj \Longrightarrow a'+b' = a+b+n(k+j);\ n \,|\, (a'+b') - (a+b)$$

Daher ist $\overline{a}+\overline{b} := \overline{a+b}$ wohldefiniert (die Klasse von $a+b$ hängt nur von der Klasse von a und der Klasse von b ab, nicht von der Wahl von a, b innerhalb ihrer Klassen).

Beispiel: $(\mathrm{GL}_n(\mathbb{R}), \cdot)$ mit $\mathrm{GL}_n(\mathbb{R}) = \{M \in M_n(\mathbb{R}) \,|\, \det M \neq 0\}$ ist eine nichtkommutative Gruppe. Ebenso sind

- $(\mathrm{SL}_n(\mathbb{R}), \cdot)$ mit $\mathrm{SL}_n(\mathbb{R}) = \{M \in M_n(\mathbb{R}) \,|\, \det M = 1\}$,
- $(\mathrm{GL}_n(\mathbb{Z}), \cdot)$ mit $\mathrm{GL}_n(\mathbb{Z}) = \{M \in M_n(\mathbb{Z}) \,|\, \det M = \pm 1\}$ und
- $(\mathrm{SL}_n(\mathbb{Z}), \cdot)$ mit $\mathrm{SL}_n(\mathbb{Z}) = \{M \in M_n(\mathbb{Z}) \,|\, \det M = 1\}$

nichtkommutative Gruppen (außer für $n = 1$).

Definition 2.2 (Potenzen,Vielfache) Wir erweitern die Definition von a^n mit $n \in \mathbb{N}_0$ für Monoide auf a^n mit $n \in \mathbb{Z}$ durch

$$a^{-m} := (a^{-1})^m = (a^{-1}) \cdot (a^{-1}) \cdot \ldots \cdot (a^{-1})$$

für $m \in \mathbb{N}$.
Wenn die Gruppenoperation als $+$ geschrieben wird, erweitern wir die Definition von na mit $n \in \mathbb{N}_0$ für Monoide auf na, $n \in \mathbb{Z}$, durch

$$(-m)a := (-a) + (-a) + \ldots + (-a)$$

Notation: Man verwendet die Abkürzung $a - b := a + (-b)$. Das neutrale Element eines additiv geschriebenen Monoids $(H, +)$ wird oft als 0 geschrieben.

Satz 2.3 (Rechenregeln für Potenzen und Vielfache) *Für $a \in (H, \cdot)$ und $n, m \in \mathbb{N}$ (falls H Halbgruppe) bzw. $n, m \in \mathbb{N}_0$ (falls H Monoid) bzw. $n, m \in \mathbb{Z}$ (falls H Gruppe) gilt $a^m \cdot a^n = a^{m+n}$ und $(a^m)^n = a^{m \cdot n}$.*

Falls $a \cdot b = b \cdot a$ gilt, dann auch $(a \cdot b)^n = a^n \cdot b^n$ für $n \in \mathbb{N}$ (bzw. $n \in \mathbb{N}_0$, falls H Monoid; $n \in \mathbb{Z}$, falls H Gruppe). Ist H kommutativ (d.h. $\forall a, b \in H\ a \cdot b = b \cdot a$), dann gilt $\forall a, b \in H\ (a \cdot b)^n = a^n \cdot b^n$.
Wenn die Operation von H als $+$ geschrieben wird, dann gilt $a + b = b + a \Rightarrow n(a + b) = na + nb$.

Satz 2.4 *Sei $(M, \cdot)$ ein Monoid, $M^* = \{a \in M \mid \exists a' \in M$ mit $a \cdot a' = e = a' \cdot a\}$ die Menge der invertierbaren Elemente. Dann ist $(M^*, \cdot)$ eine Gruppe.*

Beweis:

- Es ist $M^* \neq \emptyset$, da $e \in M^*$ $(e \cdot e = e \Rightarrow e = e^{-1})$.
- Damit $\cdot$ überhaupt wohldefinierte Verknüpfung auf M^* ist, muss M^* bezüglich $\cdot$ abgeschlossen sein, d.h. $a \in M^*$, $b \in M^* \Rightarrow a \cdot b \in M^*$ gelten:
  Seien a^{-1}, b^{-1} die Inversen. Dann gilt

  $$(a \cdot b) \cdot (b^{-1} \cdot a^{-1}) = a \cdot (b \cdot b^{-1}) \cdot a^{-1} = a \cdot e \cdot a^{-1} = a \cdot a^{-1} = e$$

  und analog auch $(b^{-1} \cdot a^{-1}) \cdot (a \cdot b) = e$. Also ist $a \cdot b \in M^*$, das Inverse ist $b^{-1} \cdot a^{-1}$. Daher ist die Einschränkung von $\cdot$ auf M^* definiert, d.h. $\cdot : M^* \times M^* \to M^*$.
- $(M^*, \cdot)$ ist eine Halbgruppe, da die Assoziativität schon in M gilt. Da $e \in M^*$ und $\forall a \in M^*\ a \cdot e = a = e \cdot a$ gilt, ist M^* ein Monoid mit neutralem Element e.
- Es bleibt zu zeigen, dass das Inverse von $a \in M^*$ in M^* liegt. Dies ist jedoch der Fall, denn a^{-1} hat auch ein Inverses, nämlich a. Also hat jedes $a \in M^*$ ein Inverses $a^{-1} \in M^*$.

□

Beispiel: Sei $(X^X, \circ)$ das Monoid der Funktionen $f : X \to X$ mit der Verknüpfung $(f \circ g)(x) = f(g(x))$. Dann sind die invertierbaren Elemente $\{f : X \to X \mid \exists g : X \to X\ g \circ f = \mathrm{id}_X = f \circ g\} = \{f : X \to X \mid f \text{ bijektiv}\}$. (Beweis als Übung)

$S_X = \{f : X \to X \mid f \text{ bijektiv}\}$ ist eine Gruppe bezüglich $\circ$. Besonders wichtig ist diese Gruppe für den Fall $X = \{1, 2, \ldots, n\}$. Man schreibt S_n für $S_{\{1,\ldots,n\}}$, die *symmetrische Gruppe* vom Grad n. S_n ist für $n > 2$ nicht kommutativ.

Charakterisierung der Gruppen innerhalb der Halbgruppen:

Proposition 2.5 Sei $G \neq \emptyset$ eine Menge, $\cdot : G \times G \to G$ eine Verknüpfung, sodass

1. $\forall a, b, c \in G \; a \cdot (b \cdot c) = (a \cdot b) \cdot c$
2. $\exists e \in G$, sodass $\forall a \in G \; a \cdot e = a$ (e ist rechtsneutrales Element)
3. $\forall a \in G \; \exists a' \in G \; a \cdot a' = e$ (jedes a hat ein Rechtsinverses)

Dann ist G eine Gruppe.

Beweis: als Übung.

Proposition 2.6 Sei $G \neq \emptyset$ eine Menge, $\cdot : G \times G \to G$ eine Verknüpfung, sodass

1. $\forall a, b, c \in G \; a \cdot (b \cdot c) = (a \cdot b) \cdot c$
2. $\forall a, b \in G \; \exists x \in G : \; a \cdot x = b$
3. $\forall a, b \in G \; \exists y \in G : \; y \cdot a = b$

Dann ist G eine Gruppe.

Beweis: als Übung.

Bemerkung: Eine Halbgruppe, in der alle Links- und Rechtstranslationen surjektiv sind, ist bereits eine Gruppe.

Bemerkung: Jede Gruppe erfüllt die Links- und Rechtskürzungsregeln, ist also eine reguläre Halbgruppe: aus $a \cdot b = a \cdot c$ folgt durch Multiplikation mit a^{-1} von links $e \cdot b = e \cdot c$, also $b = c$; ebenso folgt aus $b \cdot a = c \cdot a$ durch Multiplikation mit a^{-1} von rechts $b \cdot a = c \cdot a$.

Bemerkung: Die Links- und Rechtstranslationen $L_a : G \to G$, $R_a : G \to G$ mit $L_a(g) = a \cdot g$, $R_a(g) = g \cdot a$ sind bijektiv. Es gilt $L_a^{-1} = L_{a^{-1}}$ (d.h. $L_a \circ L_{a^{-1}} = \mathrm{id}_G = L_{a^{-1}} \circ L_a$), $R_a^{-1} = R_{a^{-1}}$.

Kapitel 3

Untergruppen

Definition 3.1 Sei $(G, \cdot)$ eine Menge mit innerer Verknüpfung, $H \subseteq G$. H heißt *abgeschlossen* bezüglich $\cdot$, wenn $\forall a, b \in G\ (a \in H \wedge b \in H \Rightarrow a \cdot b \in H)$. Ist H abgeschlossen bezüglich $\cdot$, so definiert die Einschränkung von $\cdot : G \times G \to G$ auf $H \times H$ eine Funktion $\cdot|_{H \times H} : H \times H \to H$, die wir einfach als $\cdot : H \times H \to H$ bezeichnen.

Definition 3.2 Sei $(G, \cdot)$ eine Gruppe, $H \subseteq G$, $H \neq \emptyset$. Wenn H abgeschlossen bezüglich $\cdot$ ist und $(H, \cdot)$ die Gruppenaxiome erfüllt, dann heißt H *Untergruppe* von G; man schreibt $(H, \cdot) \leq (G, \cdot)$ (bzw. $H \leq G$).

Beispiel: Jede Gruppe $(G, \cdot)$ hat die trivialen Untergruppen $\{e\}$ und G.

Beispiel: $\mathrm{SL}_n(\mathbb{R}) \leq \mathrm{GL}_n(\mathbb{R})$; $(\mathbb{Z}, +) \leq (\mathbb{R}, +)$; $(n\mathbb{Z}, +) \leq (\mathbb{Z}, +)$, wobei $n\mathbb{Z} = \{nk \mid k \in \mathbb{Z}\} = \{l \in \mathbb{Z} \mid n | l\}$

Satz 3.3 *Sei $(G, \cdot)$ eine Gruppe, e das neutrale Element von G, a^{-1} das Inverse (in G) von a, und sei $H \subseteq G$. Dann sind folgende Bedingungen äquivalent:*

1. $H \leq G$
2. $(e \in H) \wedge (\forall a, b \in H : a \cdot b \in H) \wedge (\forall a \in H : a^{-1} \in H)$
3. $(H \neq \emptyset) \wedge (\forall a, b \in H : a \cdot b^{-1} \in H)$

Beweis:

- (1. $\Rightarrow$ 2.): H hat ein neutrales Element e_H; in G gilt $e \cdot e_H = e_H$, in $H \subseteq G$ gilt $e_H \cdot e_H = e_H$, also $e \cdot e_H = e_H \cdot e_H$. Aufgrund der Kürzungsregel in G folgt $e = e_H$, also $e \in H$. $a \cdot b \in H$ $\forall a, b \in H$ gilt jedenfalls aufgrund der Definition von $H \leq G$.

Sei a' das Inverse in H zu $a \in H$. Es gilt $a \cdot a' = e$, $a \cdot a^{-1} = e$, also $a \cdot a' = a \cdot a^{-1}$. Aufgrund der Kürzungsregel folgt $a' = a^{-1}$, also $a^{-1} \in H$.

- (2. $\Rightarrow$ 3.): klar
- (3. $\Rightarrow$ 1.): $H \neq \emptyset$ ist erfüllt. Sei also $c \in H$. Dann muss $e = c \cdot c^{-1} \in H$ sein. Weiters gilt $e, c \in H \Rightarrow c^{-1} = e \cdot c^{-1} \in H$. Wenn $a, b \in H$, dann folgt $b^{-1} \in H$, also $a \cdot b = a \cdot (b^{-1})^{-1} \in H$, somit ist H bezüglich $\cdot$ abgeschlossen.
  H hat das neutrale Element e ($e \cdot a = a \cdot e = a$ gilt für alle $a \in G$, also auch für $a \in H$). Jedes $a \in H$ hat zudem ein Inverses a^{-1} in H (das Inverse von a in G, das aber in H liegt)

□

BEMERKUNG: $H \leq G \Rightarrow$ das neutrale Element von H ist das neutrale Element von G; das Inverse eines jeden Elements in H ist das Inverse in G.
Analoges gilt für Monoide nicht! (trotz Eindeutigkeit des neutralen Elements)

BEISPIEL: $(M_2(\mathbb{R}), \cdot)$ ist ein Monoid mit neutralem Element $I_2 = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$;
$X = \{\begin{pmatrix} a & 0 \\ 0 & 0 \end{pmatrix} \mid a \in \mathbb{R}\}$ ist bezüglich $\cdot$ abgeschlossen, $X \neq \emptyset$;
X ist ein Monoid (Teilmonoid) mit neutralem Element $\begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}$ ($\neq \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$!).

Proposition 3.4 Sei $(G, \cdot)$ eine Gruppe, $H \subseteq G$. Wenn H endlich ist, $H \neq \emptyset$ und bezüglich $\cdot$ abgeschlossen ist, dann folgt bereits $H \leq G$.

Beweis: als Übung.

BEISPIEL: $\mathbb{N}_0 \subseteq \mathbb{Z}$ ist eine unendliche, nichtleere Teilmenge, die bezüglich $+$ abgeschlossen ist, aber keine Gruppe!

BEMERKUNG: $H, K \leq G \Rightarrow H \cap K \leq G$, es gilt sogar:

Proposition 3.5 Sei $(G, \cdot)$ eine Gruppe, und für eine Indexmenge I gelte $H_i \leq G \ \forall i \in I$. Dann gilt $\bigcap_{i \in I} H_i \leq G$ (wobei für $I = \emptyset$ der leere Durchschnitt gleich ganz G sei, d.h. $\bigcap_{i \in \emptyset} H_i = G$).

Beweis: $\bigcap_{i\in I} H_i = \{g \in G \,|\, \forall i\ g \in H_i\}$; da $\forall i\ e \in H_i$, gilt $e \in \bigcap_{i\in I} H_i$, also insbesondere $\bigcap_{i\in I} H_i \neq \emptyset$. Außerdem gilt $a, b \in \bigcap_{i\in I} H_i \Rightarrow \forall i\ a, b \in H_i \Rightarrow \forall i\ a \cdot b^{-1} \in H_i \Rightarrow a \cdot b^{-1} \in \bigcap_{i\in I} H_i$. Nach Satz 3.3 ist daher $\bigcap_{i\in I} H_i$ eine Gruppe.

□

Definition 3.6 Sei G eine Gruppe, $X \subseteq G$. Die von X *erzeugte Untergruppe* von G ist definiert als

$$\langle X \rangle := \bigcap_{H\leq G, X\subseteq H} H$$

(Durchschnitt aller Untergruppen von G, die X enthalten).

Bemerkung: Da $X \subseteq G$, $G \leq G$, ist $\{H \leq G \,|\, X \subseteq H\} \neq \emptyset$; wegen vorhergehender Proposition ist $\langle X \rangle$ eine Gruppe, und $X \subseteq \langle X \rangle$; $\langle \emptyset \rangle = \bigcap_{H\leq G} H = \{e\}$, wobei e das neutrale Element der Gruppe ist.

Lemma 3.7 Sei G eine Gruppe, $X \subseteq G$. Sei $K \subseteq G$ eine Menge mit den Eigenschaften

1. K ist Untergruppe von G, die X enthält ($K \leq G$, $X \subseteq K$)
2. Jede Untergruppe von G, die X enthält, enthält auch K ($H \leq G \wedge X \subseteq H \Rightarrow K \subseteq H$)

Dann gilt $K = \langle X \rangle$.

Beweis: Sei K wie angegeben; aufgrund des ersten Punkts kommt K unter den $H \leq G$ mit $X \subseteq H$ vor, deren Durchschnitt $\langle X \rangle$ ist, also $\langle X \rangle \subseteq K$. Wegen des zweiten Punkts gilt $\forall H \leq G,\ X \subseteq H :\ K \subseteq H$, also $K \subseteq \bigcap_{H\leq G, X\subseteq H} H = \langle X \rangle$.

□

Proposition 3.8 Sei $(G, \cdot)$ eine Gruppe, $X \subseteq G$, dann gilt:

$$\langle X \rangle = \{g_1 \cdot \ldots \cdot g_n \,|\, n \in \mathbb{N}_0,\ \forall i \in \{1, \ldots, n\}\ (g_i \in X) \vee (g_i^{-1} \in X)\}$$

(für $n = 0$ sei das leere Produkt von Elementen das neutrale Element e)

Beweis: Sei K die rechts angegebene Menge. Wir zeigen, dass K beide Punkte des vorherigen Lemmas erfüllt:

1. $X \subseteq K$ ist klar; zu zeigen bleibt, dass K eine Untergruppe ist:
   $e \in K$, da das leere Produkt in K liegt, also ist $K \neq \emptyset$. Seien $a = g_1 \cdot \ldots \cdot g_n \in K$, $b = g'_1 \cdot \ldots \cdot g'_m \in K$ mit $(g_i \in X \vee g_i^{-1} \in X)$ und $(g'_i \in X \vee {g'_i}^{-1} \in X)$. Dann ist $a \cdot b^{-1} = g_1 \cdot \ldots \cdot g_n \cdot {g'_m}^{-1} \cdot \ldots \cdot {g'_1}^{-1}$ wieder ein Produkt von Elementen aus X und deren Inversen $\Rightarrow K \leq G$.

2. Sei $H \leq G$ mit $X \subseteq H$. $\Rightarrow \forall g \in X : \ g, g^{-1} \in H$; seien nun $g_1, \ldots, g_n$ beliebig mit $g_i \in X \vee g_i^{-1} \in X$. Dann folgt $g_i \in H$ $(i = 1, \ldots, n)$, und da H bezüglich $\cdot$ abgeschlossen ist, gilt $g_1 \cdot \ldots \cdot g_n \in H$, also $K \subseteq H$.

□

Kapitel 4

Nebenklassen

Definition 4.1 (Komplexprodukt) Sei $(G, \cdot)$ eine Gruppe, $A, B \subseteq G$. Wir definieren $AB := \{a \cdot b \,|\, a \in A, b \in B\}$; wenn $A = \{a\}$, schreiben wir aB für $\{a\}B$, also $aB := \{a \cdot b \,|\, b \in B\}$; analog $Ab := A\{b\} = \{a \cdot b \,|\, a \in A\}$.

Definition 4.2 Sei G eine Gruppe, $H \leq G$. Es werden zwei Relationen durch H auf G definiert:

$$a \,\rho_H\, b \;:\Longleftrightarrow\; ab^{-1} \in H \quad \text{und} \quad a \,\lambda_H\, b \;:\Longleftrightarrow\; a^{-1}b \in H$$

Proposition 4.3 $H \leq G \;\Rightarrow\; \rho_H, \lambda_H$ sind Äquivalenzrelationen auf G.

Beweis: für ρ_H:

- Reflexivität: $\forall a: \; aa^{-1} = e \in H$, also $\forall a : a \,\rho_H\, a$.
- Symmetrie: $a \,\rho_H\, b$ heißt $ab^{-1} \in H$, und damit auch $(ab^{-1})^{-1} \in H$, wobei $((ab^{-1})^{-1}) = (b^{-1})^{-1}a^{-1} = ba^{-1}$, also folgt $b \,\rho_H\, a$.
- Transitivität: es gelte $a \,\rho_H\, b$ und $b \,\rho_H\, c$, d.h. $ab^{-1}, bc^{-1} \in H$. Dann ist auch $(ab^{-1})(bc^{-1}) = ac^{-1} \in H$, also $a \,\rho_H\, c$.

Für λ_H läuft der Beweis analog ab.

□

Bemerkung: ρ_H ist eine Äquivalenzrelation, also bilden die Äquivalenzklassen $[a]_{\rho_H} = \{b \in G \,|\, a \,\rho_H\, b\}$ eine Partition von G, d.h. $\bigcup_{a \in G} [a]_{\rho_H} = G$ und $\forall a, b \in G : [a]_{\rho_H} \cap [b]_{\rho_H} = \emptyset \;\vee\; [a]_{\rho_H} = [b]_{\rho_H}$. Für $a, b \in G$ sind also die folgenden Bedingungen äquivalent:

1. $a \rho_H b$
2. $[a]_{\rho_H} = [b]_{\rho_H}$
3. $a \in [b]_{\rho_H}$
4. $b \in [a]_{\rho_H}$
5. $[a]_{\rho_H} \cap [b]_{\rho_H} \neq \emptyset$

Analoges gilt auch für λ_H (Beweis als Übung).

Proposition 4.4 Sei G eine Gruppe, $H \leq G$. Dann gilt für $a \in G$:

$$[a]_{\lambda_H} = aH = \{ah \,|\, h \in H\} \text{ und } [a]_{\rho_H} = Ha = \{ha \,|\, h \in H\}$$

Beweis: Sei $b \in [a]_{\lambda_H}$, d.h. $a \lambda_H b$, also $a^{-1}b = h \in H$, damit $b = ah$ und $b \in aH$; somit ist $[a]_{\lambda_H} \subseteq aH$ gezeigt.
Sei umgekehrt $b \in aH$, dann $\exists h \in H : \; b = ah$, also $a^{-1}b = h \in H$ und folglich $a \lambda_H b$. Somit ist auch $aH \subseteq [a]_{\lambda_H}$ gezeigt.

□

Analog folgt auch $[a]_{\rho_H} = Ha = \{ha \,|\, h \in H\}$ (Beweis als Übung).

Definition 4.5 Sei $H \leq G$, $a \in G$.
aH heißt *Linksnebenklasse* von a bezüglich H (bzw. eine Linksnebenklasse von H).
Ha heißt *Rechtsnebenklasse* von a bezüglich H (bzw. eine Rechtsnebenklasse von H).

Satz 4.6 *Sei G eine Gruppe, $H \leq G$, dann ist die Anzahl verschiedener Rechtsnebenklassen von H gleich der Anzahl verschiedener Linksnebenklassen von H.*

Beweis: Wir konstruieren eine bijektive Abbildung $f : \{aH \,|\, a \in G\} \to \{Hb \,|\, b \in G\}$, die definiert ist durch $f(aH) = Ha^{-1}$.

- f ist wohldefiniert, d.h. $aH = bH \Rightarrow f(aH) = f(bH)$:
  Sei $aH = bH$. Dann folgt $a \lambda_H b \Rightarrow a^{-1}b \in H \Rightarrow a^{-1}(b^{-1})^{-1} \in H \Rightarrow a^{-1} \rho_H b^{-1} \Rightarrow Ha^{-1} = Hb^{-1} \Rightarrow f(aH) = f(bH)$. Also ist f wohldefiniert.
- f ist klarerweise surjektiv, denn $\forall a \in G : \; Ha = H(a^{-1})^{-1} = f(a^{-1}H)$.

- f ist injektiv: $Ha^{-1} = Hb^{-1} \Rightarrow a^{-1} \rho_H b^{-1} \Rightarrow a^{-1}(b^{-1})^{-1} \in H \Rightarrow a^{-1}b \in H \Rightarrow a \lambda_H b \Rightarrow aH = bH$.

□

Definition 4.7 Die Anzahl der verschiedenen Linksnebenklassen einer Untergruppe H in der Gruppe G heißt *Index* von H in G, geschrieben

$$[G : H] := |\{aH \mid a \in G\}|$$

Satz 4.8 (Satz von Lagrange)

$$H \leq G \Rightarrow |G| = [G : H] \cdot |H|$$

Beweis: $\forall a \in G \ |aH| = |H|$, denn $f : H \to aH$, $f(h) = ah$, ist bijektiv (Surjektivität: $g = f(a^{-1}g)$, Injektivität: Kürzungsregel). G ist die disjunkte Vereinigung von $[G : H]$ Linksnebenklassen. Wie festgestellt, haben diese alle die Ordnung $|H|$, also folgt $|G| = [G : H] \cdot |H|$.

□

Definition 4.9 Ein *Repräsentantensystem* der Linksnebenklassen von H in G ist eine Teilmenge von G, die aus jeder Linksnebenklasse von H genau ein Element enthält (d.h. $R \subseteq G$, sodass $\forall a \in G \ \exists! \, r \in R$ mit $a \lambda_H r$); analog für die Rechtsnebenklassen von H.

Bemerkung: Sei $H \leq G$, $K \subseteq H$. Dann gilt $K \leq H \Leftrightarrow K \leq G$. Somit ist die Untergruppenrelation transitiv: $K \leq H \wedge H \leq G \Rightarrow K \leq G$.

Satz 4.10 (allgemeine Form des Satzes von Lagrange) *Sei $(G, \cdot)$ eine Gruppe, $H \leq G$ und $K \leq H$ (also auch $K \leq G$). Dann gilt*

$$[G : K] = [G : H] \cdot [H : K]$$

Beweis: Sei R ein Repräsentantensystem der Linksnebenklassen von H in G, S ein Repräsentantensystem der Linksnebenklassen von K in H, also $|R| = [G : H]$, $|S| = [H : K]$. Wir zeigen:

1. $|RS| = |R \times S| = |R| \cdot |S|$
2. $RS = \{rs \mid r \in R, s \in S\}$ ist Repräsentantensystem der Linksnebenklassen von K in G.

Dann folgt $[G : K] = |RS| = |R| \cdot |S| = [G : H] \cdot [H : K]$.

1. $f : R \times S \to RS$ mit $f(r,s) = rs$ ist eine surjektive Funktion. Seien nun $r, r' \in R$ und $s, s' \in S$ mit $rs = r's'$. Dann folgt $ss'^{-1} = r^{-1}r'$. $ss'^{-1} \in H \Rightarrow r \,\lambda_H\, r'$, also $r = r'$ und somit $r^{-1}r' = e = ss'^{-1} \Rightarrow s = s'$. Folglich ist f auch injektiv und daher $|R \times S| = |R| \cdot |S|$.

2. Sei $g \in G$. Dann existieren $r \in R$, $h \in H$ mit $g = rh$. Für dieses h existieren $s \in S$, $k \in K$ mit $h = sk$. Also $\forall g \in G \;\exists r \in R, s \in S, k \in K : \; g = (rs)k$. Also enthält RS aus jeder Linksnebenklasse von K ein Element.
   Wenn nun $rs \,\lambda_K\, r's'$, d.h. $(rs)^{-1}(r's') \in K$, gilt, dann folgt $s^{-1}r^{-1}r's' = k \in K$, damit $r^{-1}r' = sks'^{-1} \in H$, also $r \,\lambda_H\, r' \Rightarrow r = r'$. Daher gilt auch $e = sks'^{-1}$, also $s^{-1}s' = k \in K \Rightarrow s \,\lambda_K\, s' \Rightarrow s = s'$, insbesondere somit $rs = r's'$. Also enthält RS aus jeder Linksnebenklasse von K in G genau ein Element und ist somit ein Repräsentantensystem.

□

BEMERKUNG: Für den Spezialfall $K = \{e\}$ folgt der Satz von Lagrange.

BEISPIEL: $H = n\mathbb{Z}$, $G = \mathbb{Z}$; dann ist $(H,+) \leq (G,+)$ und $a \,\rho_{n\mathbb{Z}}\, b \;\Leftrightarrow\; a - b \in n\mathbb{Z}$, d.h. wenn $n \mid a - b$.
$n \mid a - b \;\Leftrightarrow\; a, b$ haben denselben Rest bei Division durch n; zu jedem Rest r mit $0 \leq r < n$ ist also $\{a \in \mathbb{Z} \mid \exists k \in \mathbb{Z} : \; a = nk + r\} = r + n\mathbb{Z}$ eine Nebenklasse von $n\mathbb{Z}$, und das sind auch bereits alle Nebenklassen. Ein Repräsentantensystem wäre $0, 1, \ldots, (n-1)$ (Bemerkung: es ist untypisch, dass es ein solch „ausgezeichnetes“ Repräsentantensystem gibt).

BEISPIEL: $S_n = (\{\pi : \{1,\ldots,n\} \to \{1,\ldots,n\} \text{ bijektiv}\}, \circ)$; für $a \in \{1,\ldots,n\}$ ist $\mathrm{St}(a) = \{\pi \in S_n \mid \pi(a) = a\}$, der sogenannte Stabilisator von a unter S_n, eine Untergruppe von S_n, d.h. $\mathrm{St}(a) \leq S_n$. Für $\pi, \sigma \in S_n$ gilt dann

$$\pi \,\lambda_{\mathrm{St}(a)}\, \sigma \;\Leftrightarrow\; \pi^{-1}\sigma \in \mathrm{St}(a) \;\Leftrightarrow \pi^{-1}\sigma(a) = a \;\Leftrightarrow\; \sigma(a) = \pi(a)$$

D.h., jedes $b \in \{1,\ldots,n\}$ definiert eine Linksnebenklasse $\{\pi \in S_n \mid \pi(a) = b\} = K_b$; für jedes $\pi \in S_n$ mit $\pi(a) = b$ ist $\pi\,\mathrm{St}(a) = K_b$.
Analog gilt

$$\pi \,\rho_{\mathrm{St}(a)}\, \sigma \;\Leftrightarrow\; \pi\sigma^{-1} \in \mathrm{St}(a) \;\Leftrightarrow\; \pi\sigma^{-1}(a) = a \;\Leftrightarrow\; \sigma^{-1}(a) = \pi^{-1}(a)$$

D.h., jedes $b \in \{1,\ldots,n\}$ definiert eine Rechtsnebenklasse $\{\pi \in S_n \mid \pi^{-1}(a) = b\} = \{\pi \in S_n \mid \pi(b) = a\} = C_b$; für jedes $\sigma \in S_n$ mit $\pi(b) = a$ ist $\mathrm{St}(a)\pi = C_b$.

BEISPIEL: $\mathrm{SL}_n(K) \leq \mathrm{GL}_n(K)$ für einen Körper K. Für $A, B \in \mathrm{GL}_n(K)$ gilt:

$$A^{-1}B \in \mathrm{SL}_n(K) \;\Leftrightarrow\; \det(A^{-1}B) = 1 \;\Leftrightarrow\; \det(A)^{-1}\det(B) = 1 \;\Leftrightarrow\; \det(A) = \det(B)$$

Jedes $r \in K^*$ definiert eine Linksnebenklasse

$$K_r = \{A \in \mathrm{GL}_n(K) \mid \det(A) = r\}$$

Für jedes $A \in \mathrm{GL}_n(K)$ mit $\det(A) = r$ ist $A\ \mathrm{SL}_n(K) = K_r$. Es gilt aber auch

$$AB^{-1} \in \mathrm{SL}_n(K) \Leftrightarrow \det(AB^{-1}) = 1 \Leftrightarrow \det(A)\det(B)^{-1} = 1 \Leftrightarrow \det(A) = \det(B)$$

Also ist $\forall A \in \mathrm{GL}_n(K)\ A\ \mathrm{SL}_n(K) = \mathrm{SL}_n(K)\ A$ (!).

Kapitel 5

Normalteiler

Definition 5.1 Eine Untergruppe N von G heißt *Normalteiler*, wenn

$$\forall a \in G \; aN = Na$$

Man schreibt $N \trianglelefteq G$ für „N ist Normalteiler von G“.

Bemerkung: $aN = Na$ heißt $\{ah \,|\, h \in N\} = \{ka \,|\, k \in N\}$ (als Menge), aber nicht $\forall a \in G, h \in N \; ah = ha$;
$\{ah \,|\, h \in N\} = \{ka \,|\, k \in N\}$ heißt $\forall h \in N \exists k \in N$ mit $ah = ka$ und $\forall k \in N \exists h \in N$ mit $ka = ah$.

Bemerkung: Jede Gruppe hat die trivialen Normalteiler $\{e\}$ und G; in einer kommutativen Gruppe ist jede Untergruppe ein Normalteiler.

Proposition 5.2 Sei G eine Gruppe, $N \leq G$. Dann sind folgende Bedingungen äquivalent:

1. $\forall a \in G \; aNa^{-1} = N$
2. $\forall a \in G \; aN = Na$
3. $\forall a \in G \; aN \subseteq Na$
4. $\forall a \in G \; aNa^{-1} \subseteq N$

Beweis:

- (1. $\Rightarrow$ 2.): Durch Multiplikation von rechts mit a ergibt sich $aNa^{-1} = N \;\Rightarrow\; aN = Na$.
- (2. $\Rightarrow$ 3.): trivial

- (3. $\Rightarrow$ 4.): ergibt sich durch Multiplikation von rechts mit a^{-1} (wie im ersten Teil des Beweises)
- (4. $\Rightarrow$ 1.): Es gilt $\forall a \in G\ aNa^{-1} \subseteq N$ und – indem man a durch a^{-1} ersetzt – auch $\forall a \in G\ a^{-1}Na \subseteq N$. Durch Multiplikation von links mit a und von rechts mit a^{-1} ergibt sich daraus $\forall a \in G\ N \subseteq aNa^{-1}$. Zusammen folgt $\forall a \in G\ aNa^{-1} = N$.

□

Bemerkung: es gilt $(\forall a \in G\ aNa^{-1} \subseteq N) \iff (\forall a \in G\ aNa^{-1} = N)$, aber nicht $\forall a \in G\ (aNa^{-1} \subseteq N \iff aNa^{-1} = N)$!

Bemerkung: Sei $N \leq G$. Dann gelten folgende Äquivalenzen:

$$\begin{aligned} N \trianglelefteq G &\iff \forall a \in G\ aN = Na \\ &\iff \forall a \in G\ [a]_{\lambda_N} = [a]_{\rho_N} \\ &\iff (\forall a, b \in G\ a\,\lambda_N\,b \Leftrightarrow a\,\rho_N\,b) \\ &\iff \lambda_N = \rho_N \end{aligned}$$

Wenn $N \trianglelefteq G$, schreibt man oft $a \equiv b \bmod N$ („a kongruent b modulo N“) für $a\,\lambda_N\,b$ bzw. $a\,\rho_N\,b$.

Definition 5.3 Sei $(G, \cdot)$ eine Menge mit innerer Verknüpfung, $\equiv$ eine Äquivalenzrelation auf G. $\equiv$ heißt *Kongruenzrelation*, wenn $\forall a, a', b, b' \in G$ gilt:

$$a \equiv a' \wedge b \equiv b' \implies a \cdot b \equiv a' \cdot b'$$

Lemma 5.4 Sei $H \leq G$. Dann gilt $\forall a, a', b, b' \in G$

1. $a\,\lambda_H\,a' \Rightarrow ba\,\lambda_H\,ba'$
2. $b\,\rho_H\,b' \Rightarrow ba\,\rho_H\,b'a$

Beweis:

1. $a\,\lambda_H\,a' \Leftrightarrow \exists h \in H:\ a' = ah$; damit folgt $ba' = bah$, also $ba\,\lambda_H\,ba'$
2. $b\,\rho_H\,b' \Leftrightarrow \exists h \in H:\ b' = hb$; damit folgt $b'a = hba$, also $ba\,\lambda_H\,b'a$

□

Proposition 5.5 Sei $(G, \cdot)$ eine Gruppe, $N \trianglelefteq G$, dann ist $\equiv$, die Kongruenz mod N (definiert durch $a \equiv b \bmod N :\Leftrightarrow ab^{-1} \in N$), eine Kongruenzrelation.

Beweis: Sei $a \equiv a'$, $b \equiv b'$. Dann folgt $ab \overset{(*)}{\equiv} a'b \overset{(**)}{\equiv} a'b'$, wobei $(*)$ wegen $\equiv = \rho_N$ und $(**)$ wegen $\equiv = \lambda_N$ gilt. Aus der Transitivität von $\equiv$ folgt somit $ab \equiv a'b'$.

□

Kapitel 6

Faktorgruppen/Quotientengruppen

Definition 6.1 Sei $(G, \cdot)$ eine Gruppe, $N \trianglelefteq G$; G/N bezeichne die Menge der Nebenklassen von N in G:

$$G/N = \{aN \mid a \in G\} = \{Na \mid a \in G\}$$

Dann heißt G/N mit der Operation $(aN) \cdot (bN) := (ab)N$ *Faktorgruppe* oder *Quotientengruppe* von N in G.

Satz 6.2 $\cdot$ *ist auf diese Weise wohldefiniert, und* $(G/N, \cdot)$ *bildet tatsächlich eine Gruppe.*

Beweis: Die wesentliche Aussage ist jene, dass $\cdot$ auf diese Art wohldefiniert ist, d.h., wenn $aN = a'N$ und $bN = b'N$, dann muss $a'b'N = abN$ gelten.
Dies folgt direkt aus der Definition eines Normalteilers: seien $a' = ah$, $b' = bk$ mit $h, k \in N$. Dann gilt $a'b' = ahbk$; da $Nb = bN$ ist und $hb \in Nb$, muss ein $l \in N$ existieren, sodass $hb = bl$ ist. Damit folgt jedoch $a'b' = ahbk = ablk$, und da $lk \in N$ ist, ergibt sich $a'b' \in abN$, also $a'b'N = abN$.
Eine andere Möglichkeit zum Beweis läuft über Kongruenzrelationen: $aN = Na = [a]$ ist Kongruenzklasse von a bezüglich $\equiv$. $[a] \cdot [b] = [a \cdot b]$ ist daher wohldefiniert, weil $\equiv$ eine Kongruenzrelation ist. Die restlichen Gruppeneigenschaften folgen dann sofort aus jenen für G:

- Assoziativität: $([a][b])[c] = [ab][c] = [abc] = [a][bc] = [a]([b][c])$
- neutrales Element ist $[e]\,(= N)$: $[a][e] = [ae] = [a] = [ea] = [e][a]$
- Inverses von $[a]$ ist $[a^{-1}]$: $[a^{-1}][a] = [a^{-1}a] = [e] = [aa^{-1}] = [a][a^{-1}]$

□

BEMERKUNG: Das neutrale Element in G/N ist $[e]_N = eN = Ne = N$; für $a \in G$ gilt $aN = N \Leftrightarrow a \in N$:

$$[a] = N = [e] \iff a \equiv e \iff ae^{-1} = a \in N$$

BEMERKUNG: Ist $(G, +)$ eine additiv geschriebene Gruppe, dann wird die Gruppe $(G/N, +)$ definiert durch $(a + N) + (b + N) = (a + b) + N$, das neutrale Element ist $0 + N = N$, und es gilt $a + N = 0 + N \Leftrightarrow a \in N$.

BEISPIEL: $(\mathbb{Z}, +)$ ist eine kommutative Gruppe, daher ist jede Untergruppe ein Normalteiler; jede Untergruppe hat die Form $(n\mathbb{Z}, +)$ für ein $n \in \mathbb{N}_0$. Man schreibt die Faktorgruppe $(\mathbb{Z}/n\mathbb{Z}, +)$ auch als $(\mathbb{Z}_n, +)$. Die Addition von $(\mathbb{Z}_n, +)$ ist $(i+n\mathbb{Z})+(j+n\mathbb{Z}) = (i+j)+n\mathbb{Z}$, bzw., wenn man für fixes n die Nebenklasse $i+n\mathbb{Z}$ mit $\overline{i}$ abkürzt, $\overline{i}+\overline{j} = \overline{i+j}$. Ein Repräsentantensystem der Nebenklassen ist: $0, 1, \ldots, n-1$.

BEISPIEL: $\mathrm{GL}_n(K)/\mathrm{SL}_n(K) \simeq K^* = (K \setminus \{0\}, \cdot)$ für einen Körper K. Es gilt

$$A\ \mathrm{SL}_n(K) = \{B \in \mathrm{GL}_n(K) \mid \det(B) = \det(A)\} \text{ und } [A] \cdot [B] = [A \cdot B]$$

$[A]$ ist dabei jene Klasse, in der alle Matrizen Determinante $a = \det(A)$ haben, $[B]$ jene, in der alle Determinante $b = \det(B)$ haben, und $[A \cdot B]$ jene, in der alle Determinante $a \cdot b$ haben. Man kann daher jede Klasse mit dem Wert ihrer Determinante identifizieren, die Mutiplikation der Klassen entspricht der Multiplikation der entsprechenden Determinantenwerte.

Kapitel 7

Gruppenhomomorphismen

Definition 7.1 Seien $(G, \cdot)$ und $(H, *)$ Gruppen. Eine Funktion $f : G \to H$ heißt *Gruppenhomomorphismus*, wenn $\forall a, b \in G\ f(a \cdot b) = f(a) * f(b)$. Der *Kern* von f ist das Urbild des neutralen Elements e_H unter f:

$$\text{Ker } f := \{a \in G \mid f(a) = e_H\} = f^{-1}(e_H) \subseteq G$$

Das *Bild* von f bezeichnen wir mit Im f:

$$\text{Im } f := \{f(a) \mid a \in G\} = f(G) \subseteq H$$

Proposition 7.2 Seien G, H, K Gruppen und e_G, e_H die neutralen Elemente von G bzw. H. Dann gilt:

1. Wenn $f : G \to H$ Gruppenhomomorphismus, dann $f(e_G) = e_H$ und $\forall a \in G\ f(a^{-1}) = f(a)^{-1}$.
2. Sind $f : G \to H$, $g : H \to K$ Gruppenhomomorphismen, dann ist auch $g \circ f : G \to K$ ein Gruppenhomomorphismus.
3. Ist $f : G \to H$ ein bijektiver Gruppenhomomorphismus, dann ist auch die Inverse von f, $f^{-1} : H \to G$ ein Gruppenhomomorphismus.

Beweis:

1. als Übung.
2. $(g \circ f)(ab) = g(f(ab)) \overset{f \text{ ist Hom.}}{=} g(f(a)f(b)) \overset{g \text{ ist Hom.}}{=} g(f(a))(g(f(b)) = ((g \circ f)(a))((g \circ f)(b))$. Also ist auch $g \circ f$ ein Gruppenhomomorphismus.

3. Seien $a, b \in H$ und $\alpha, \beta \in G$ die eindeutig bestimmten Elemente mit $f(\alpha) = a$, $f(\beta) = b$. Es gilt $f(\alpha\beta) = f(\alpha)f(\beta)$, also $f^{-1}(f(\alpha)f(\beta)) = \alpha\beta = f^{-1}(a)f^{-1}(b)$. Insgesamt folgt daher

$$f^{-1}(ab) = f^{-1}(f(\alpha)f(\beta)) = f^{-1}(a)f^{-1}(b)$$

Also ist auch f^{-1} ein Gruppenhomomorphismus.

□

Bemerkung:

- Ad 1.: wenn G, H Monoide sind und $f : G \to H$ die Beziehung $f(ab) = f(a)f(b)$ erfüllt (d.h., f ist Monoidhomomorphismus), dann muss nicht $f(e_G) = f(e_H)$ gelten!
- Ad 3.: Ein injektiver Gruppenhomomorphismus muss keine Linksinverse haben, die auch Gruppenhomomorphismus ist! Ebenso muss ein surjektiver Gruppenhomomorphismus keine Rechtsinverse haben, die auch Gruppenhomomorphismus ist.

Definition 7.3 Sei $f : G \to H$ ein Gruppenhomomorphismus.

- Wenn f surjektiv ist, heißt f ein (Gruppen-)*Epimorphismus*.
- Wenn f injektiv ist, heißt f ein (Gruppen-)*Monomorphismus*.
- Wenn f bijektiv ist, heißt f ein (Gruppen-)*Isomorphismus*.
- Wenn $G = H$ ist, heißt f ein *Endomorphismus* von G.
- Wenn $G = H$ und f bijektiv ist, heißt f ein *Automorphismus* von G.

Definition 7.4 Zwei Gruppen A, B heißen *isomorph* (geschrieben $A \simeq B$), wenn es einen Isomorphismus $f : A \to B$ gibt.

Beispiel:

- $\det : \mathrm{GL}_n(K) \to (K^*, \cdot)$ ist ein Gruppenepimorphismus. Der Kern ist $\operatorname{Ker} \det = \mathrm{SL}_n(K)$.
- $\exp : (\mathbb{R}, +) \to (\mathbb{R}^+, \cdot)$ mit $\exp(a) = e^a$ ist ein Gruppenisomorphismus.
- $f : \mathrm{GL}_n(K) \to \mathrm{GL}_{n+m}(K)$ mit $f(A) = \begin{pmatrix} A & 0 \\ 0 & I_m \end{pmatrix}$ ist ein Gruppenmonomorphismus.

- $f : (\mathbb{Z}_n, +) \to S^1$ mit $f(\overline{k}) = e^{\frac{2k\pi i}{n}}$ ist ein Gruppenmonomorphismus.
- sgn : $S_n \to (\{1, -1\}, \cdot)$ (siehe Kapitel 12) ist ein Gruppenhomomorphismus.
- $f : \mathbb{Z}_s \to \mathbb{Z}_{2s}$ mit $f(\overline{x}) = \overline{2x}$ ist ein Gruppenmonomorphismus, der kein Linksinverses hat, das ebenfalls Gruppenhomomorphismus ist (Beweis als Übung).

Lemma 7.5 Sei $f : G \to H$ Gruppenhomomorphismus. Dann gilt

1. $K \leq G \;\Rightarrow\; f(K) \leq H$
2. $K \trianglelefteq G \;\Rightarrow\; f(K) \trianglelefteq f(G)$ (im Allgemeinen nicht $f(K) \trianglelefteq H$!)
3. $C \leq H \;\Rightarrow\; f^{-1}(C) \leq G$
4. $C \trianglelefteq H \;\Rightarrow\; f^{-1}(C) \trianglelefteq G$

Beweis: als Übung.

Korollar 7.6 $\operatorname{Ker} f \trianglelefteq G$ und $\operatorname{Im} f \leq H$.

Definition 7.7 Sei G eine Gruppe, $N \trianglelefteq G$. Dann heißt $\pi_N \colon G \to G/N$ mit $\pi_N(a) = aN$ die *kanonische Projektion* von G auf G/N.

Proposition 7.8 Die kanonische Projektion $\pi_N : G \to G/N$, $\pi_N(g) = gN$, ist ein Gruppenepimorphismus.

Beweis: Die Surjektivität von π_N ist klar. π_N ist ein Homomorphismus, weil die Multiplikation in G/N durch $\pi_N(ab) = (ab)N = (aN)(bN) = \pi_N(a)\pi_N(b)$ erklärt ist.

□

Lemma 7.9 Sei $f : G \to H$ ein Gruppenhomomorphismus, $a, b \in G$. Dann gilt $f(a) = f(b) \;\Leftrightarrow\; a \equiv b \mod \operatorname{Ker} f$.

Beweis:

$$f(a) = f(b) \;\Leftrightarrow\; e = f(a)f(b)^{-1} = f(ab^{-1}) \;\Leftrightarrow\; ab^{-1} \in \operatorname{Ker} f \;\Leftrightarrow\; a \equiv b \mod \operatorname{Ker} f$$

□

Korollar 7.10 Sei f Gruppenhomomorphismus. Dann gilt:

$$f \text{ injektiv} \iff \operatorname{Ker} f = \{e\}.$$

Satz 7.11 (Homomorphiesatz, 1. Isomorphiesatz) *Sei $f : G \to H$ ein Gruppenhomomorphismus. Dann gilt* $\operatorname{Ker} f \trianglelefteq G$, $\operatorname{Im} f \leq H$, *und*

$$\overline{f} \colon G/(\operatorname{Ker} f) \to \operatorname{Im} f,$$

definiert durch $\overline{f}(a \operatorname{Ker} f) = f(a)$, *ist ein Isomorphismus.*

Beweis: Die Wohldefiniertheit von $\overline{f}$ ist wegen des obigen Lemmas gegeben, ebenso die Injektivität. Die Surjektivität von $\overline{f}$ ist klar. Da außerdem

$$\overline{f}((a \operatorname{Ker} f)(b \operatorname{Ker} f)) = \overline{f}(ab \operatorname{Ker} f) = f(ab) = f(a)f(b) = \overline{f}(a \operatorname{Ker} f)\overline{f}(b \operatorname{Ker} f)$$

gilt, ist $\overline{f}$ ein Homomorphismus, insgesamt also ein Isomorphismus.

□

Beispiel: $\det : \mathrm{GL}_n(\mathbb{R}) \to \mathbb{R}^*$ ist ein Gruppenhomomorphismus. $\operatorname{Ker} \det = \mathrm{SL}_n(\mathbb{R}) = \{A \in \mathrm{GL}_n(\mathbb{R}) \mid \det A = 1\}$. $\overline{\det} : \mathrm{GL}_n(\mathbb{R})/\mathrm{SL}_n(\mathbb{R}) \to \mathbb{R}^*$ mit $\overline{\det}(A \mathrm{SL}_n(\mathbb{R})) = \det A$ ist ein Isomorphismus.

Beispiel: $\operatorname{sgn} : S_n \to (\{1, -1\}, \cdot)$ (siehe Kapitel 12) ist ein Gruppenhomomorphismus, $\operatorname{Ker} \operatorname{sgn} = A_n = \{\pi \in S_n \mid \operatorname{sgn} \pi = 1\}$, $\operatorname{Im} \operatorname{sgn} = \{1, -1\}$, $\overline{\operatorname{sgn}} : S_n/A_n \to \{1, -1\}$ mit $\overline{\operatorname{sgn}}(\pi A_n) = \operatorname{sgn} \pi$ ist ein Isomorphismus.

Bemerkung: G sei eine Gruppe, $N \trianglelefteq G$. Dann tritt N als Kern und G/N als Bild eines Gruppenhomomorphismus auf, nämlich $\pi_N : G \to G/N$, $\pi_N(a) = aN$ ($a \in \operatorname{Ker} \pi_N \Leftrightarrow aN = N \Leftrightarrow a \in N$).
Wenn umgekehrt $f : G \to H$ ein Gruppenhomomorphismus ist, dann gilt $\operatorname{Ker} f \trianglelefteq G$, $\operatorname{Im} f \simeq G/\operatorname{Ker} f$; also ist jedes homomorphe Bild von G isomorph zu einer Faktorgruppe. Bis auf Isomorphie sind daher Faktorgruppen und homomorphe Bilder dasselbe.

Beispiel: „Jede Faktorgruppe einer kommutativen Gruppe ist kommutativ“ ist gleichbedeutend mit „jedes homomorphe Bild einer kommutativen Gruppe ist kommutativ“.

Kapitel 8

Zyklische Gruppen

Definition 8.1 Eine Gruppe G heißt *zyklisch*, wenn $\exists a \in G : \ G = \langle a \rangle$. Dabei ist $\langle a \rangle = \langle \{a\} \rangle$ die von a erzeugte Untergruppe von G, definiert als $\langle a \rangle = \bigcap_{H \leq G, a \in H} H$; wir wissen, dass

$$\langle a \rangle = \{a^n \,|\, n \in \mathbb{Z}\} = \{\ldots, a^{-2}, a^{-1}, e, a, a^2, \ldots\}$$

gilt. Für additiv geschriebene Gruppen $(G, +)$ ist

$$\langle a \rangle = \{na \,|\, n \in \mathbb{Z}\} = \{\ldots, -2a, -a, e, a, 2a, \ldots\}$$

Beispiel: $(\mathbb{Z}, +)$ ist zyklisch, denn $\mathbb{Z} = \langle 1 \rangle = \langle -1 \rangle$.

Satz 8.2 *Für eine zyklische Gruppe G gilt:*

1. *Jeder Untergruppe von G ist zyklisch.*
2. *Jede Faktorgruppe (bzw. jedes homomorphe Bild) von G ist zyklisch.*

Beweis:

1. Sei $H \leq G = \langle a \rangle$. Wenn $H = \{e\}$, dann ist $H = \langle e \rangle$ zyklisch, ansonsten existiert ein $m \neq 0$ mit $a^m \in H$. Da aus $a^m \in H$ auch $a^{-m} = (a^m)^{-1} \in H$ folgt, gibt es sogar ein $m > 0$ mit $a^m \in H$.
   Sei $n = \min\{m \in \mathbb{N} \,|\, a^m \in H\}$ (dieser Wert existiert, da jede nichtleere Teilmenge von $\mathbb{N}$ ein Minimum hat), und sei $h \in H$ beliebig. Es gibt ein $m \in \mathbb{Z}$, sodass $h = a^m$ ist. Wir führen nun eine Division mit Rest durch: es gibt Werte q, r, sodass $m = qn + r$, $r, q \in \mathbb{Z}$, $0 \leq r < n$.
   Wegen $a^r = (a^{qn})^{-1} h \in H$ und der Minimalität von n muss $r = 0$ sein, also $h = a^{qn} \in \langle a^n \rangle$. Also ist $H \subseteq \langle a^n \rangle$, und wegen $a^n \in H$ gilt $\langle a^n \rangle \subseteq H$, insgesamt also $\langle a^n \rangle = H$.

2. Behauptung: ist $f : G \to K$ ein Homomorphismus und $H \leq G$ mit $H = \langle X \rangle$, dann gilt $f(H) = \langle f(X) \rangle$ (Beweis als Übung). Damit folgt dann für $G = \langle a \rangle$ sofort $\operatorname{Im} f = \langle f(a) \rangle$, also ist $\operatorname{Im} f$ zyklisch.

□

Korollar 8.3 Sei $H \leq G = \langle a \rangle$, dann ist $H = \{e\}$ oder $H = \langle a^n \rangle$ für $n = \min\{m \in \mathbb{N} \mid a^m \in H\}$.
Für eine additive Gruppe $H \leq (G, +)$, $G = \langle a \rangle$, folgt analog $H = \langle na \rangle$ für $n = \min\{m \in \mathbb{N} \mid ma \in H\}$.

Korollar 8.4 Jede Untergruppe von $\mathbb{Z} = \langle 1 \rangle$ hat die Form $(n\mathbb{Z}, +) = \langle n \rangle$ und $H \leq (\mathbb{Z}, +) \Rightarrow H = \{0\}$ oder $H = \langle n \rangle$ mit $n = \min\{n \in \mathbb{N} \mid n \in H\}$.

Bemerkung: $\langle n \rangle = \langle -n \rangle$; für $n, m \in \mathbb{N}$ mit $n \neq m$ gilt $\langle n \rangle \neq \langle m \rangle$. $\langle 0 \rangle = \{0\}$, $\langle 1 \rangle = \langle -1 \rangle = \mathbb{Z}$.

Bemerkung: Jede zyklische Gruppe ist kommutativ: $a^n a^m = a^{n+m} = a^{m+n} = a^m a^n$.

Satz 8.5 *Jede zyklische Gruppe ist entweder isomorph zu* $(\mathbb{Z}, +)$ *oder zu* $(\mathbb{Z}/n\mathbb{Z}, +)$ *für ein* $n \in \mathbb{N}$.

Beweis: Sei $G = \langle a \rangle = \{a^n \mid n \in \mathbb{Z}\}$. Definiere $f : \mathbb{Z} \to G$ durch $f(n) = a^n$. Dann ist f ein Homomorphismus, da $f(n+m) = a^{n+m} = a^n a^m = f(n)f(m)$. f ist surjektiv. Daher ist $G \simeq \mathbb{Z}/\operatorname{Ker} f$, also muss G isomorph zu $\mathbb{Z}/n\mathbb{Z}$ für ein $n \in \mathbb{N}_0$ sein (die Mengen $n\mathbb{Z}$ sind die einzigen Untergruppen von $\mathbb{Z}$). Für $n = 0$ ist $\mathbb{Z}/n\mathbb{Z} = \mathbb{Z}$.

□

Korollar 8.6 Ist G eine unendliche zyklische Gruppe, dann gilt $G \simeq (\mathbb{Z}, +)$. Ist G zyklisch mit $|G| = n$, dann gilt $G \simeq (\mathbb{Z}/n\mathbb{Z}, +) = (\mathbb{Z}_n, +)$.

Bemerkung: Der oben definierte Isomorphismus f hat den Kern $\operatorname{Ker} f = \{n \in \mathbb{Z} \mid a^n = e\}$. Es gilt

$$f \text{ injektiv} \Leftrightarrow \operatorname{Ker} f = \{0\} \Leftrightarrow G \simeq \mathbb{Z}$$

Wenn $\operatorname{Ker} f \neq \{0\}$ ist, dann ist $\operatorname{Ker} f = \langle n \rangle$, wobei $n = \min\{m \in \mathbb{N} \mid m \in \operatorname{Ker} f\} = \min\{m \in \mathbb{N} \mid a^m = e\}$, und $G = \langle a \rangle \simeq \mathbb{Z}/n\mathbb{Z}$.

Definition 8.7 Sei G eine Gruppe, $a \in G$. Die *Ordnung* von a ist definiert als $|a| = |\langle a \rangle|$ (die Ordnung der von a erzeugten Untergruppe). Man schreibt $|a| = \infty$, falls $\langle a \rangle$ unendlich ist.

Proposition 8.8 Sei G eine Gruppe und $a \in G$. Dann sind äquivalent:

1. (a) $|a| = \infty$
   (b) $\{m \in \mathbb{Z} \mid a^m = e\} = \{0\}$
   (c) $\langle a \rangle \simeq (\mathbb{Z}, +)$
2. (a) $|a| = n$
   (b) $\{m \in \mathbb{Z} \mid a^m = e\} = n\mathbb{Z}$
   (c) $\min\{m \in \mathbb{N} \mid a^m = e\} = n$
   (d) $\langle a \rangle \simeq (\mathbb{Z}_n, +)$

Beweis: $f : (\mathbb{Z}, +) \to \langle a \rangle$, definiert durch $f(n) = a^n$, ist ein Epimorphismus, daher ist $\langle a \rangle \simeq \mathbb{Z}/(\operatorname{Ker} f)$, wobei $\operatorname{Ker} f = \{m \in \mathbb{Z} \mid a^m = e\}$. Entweder ist $\operatorname{Ker} f = \{0\}$ (dann gelten alle Aussagen von 1.), oder es ist $\operatorname{Ker} f = \langle n \rangle$ für ein $n \in \mathbb{N}$ (dann gelten alle Aussagen von 2.) Da entsprechende Aussagen verschiedener Fälle einander widersprechen, müssen somit alle Bedingungen aus 1. bzw. alle Bedingungen aus 2. äquivalent sein.

□

BEMERKUNG: Ist $|a| = n$ endlich, dann gilt $a^m = e \;\Leftrightarrow\; n|m$.
Ist $|a| = \infty$, dann gilt $a^m = e \;\Leftrightarrow\; m = 0$.

Beweis: als Übung.

Korollar 8.9 Es gilt $a^k = e \;\Leftrightarrow |a| \Big| k$ (mit der Konvention, dass $\infty \mid 0$ und $\infty \nmid k$ für $k \neq 0$).

BEMERKUNG: Aus dem Satz von Lagrange ($H \leq G \;\Rightarrow\; |G| = [G : H] \cdot |H|$) folgt für endliche Gruppen G, dass $|H| \Big| |G|$, insbesondere $|a| \Big| |G|$, also $\forall a \in G$ $a^{|G|} = e$.

Lemma 8.10 Sei $a^k \in \langle a \rangle$ und $|a|$ endlich. Dann gilt $|a^k| = \frac{|a|}{\operatorname{ggT}(k,|a|)}$.

Beweis: $a^{km} = e \;\Leftrightarrow\; |a| \Big| km \;\Leftrightarrow\; \frac{|a|}{\operatorname{ggT}(k,|a|)} \Big| m$.

□

Definition 8.11 (Euler'sche φ-Funktion) Die *Euler'sche φ-Funktion* ist definiert durch $\varphi : \mathbb{N} \to \mathbb{N}$, $\varphi(n) = |\{1 \leq k \leq n \mid \operatorname{ggT}(k, n) = 1\}|$. Für Primzahlen p gilt $\varphi(p^m) = p^m - p^{m-1}$. Für relativ prime Zahlen m, n (d.h. $\operatorname{ggT}(m, n) = 1$) gilt $\varphi(nm) = \varphi(n)\varphi(m)$.

Korollar 8.12 Sei $n = md$. Dann hat die zyklische Gruppe der Ordnung n genau $\varphi(d)$ Elemente der Ordnung d.

Beweis: Sei $|\langle a\rangle| = n$. Dann ist $\langle a\rangle = \{e = a^n, a, a^2, \ldots, a^{n-1}\}$. Die Elemente mit Ordnung d sind genau jene a^k mit $1 \leq k \leq n$, für die $\mathrm{ggT}(k, n) = m$ gilt. Das sind wiederum genau jene a^k mit $k = ml$, $1 \leq l \leq d$ und $\mathrm{ggT}(l, d) = 1$. Davon gibt es genau $\varphi(d)$ Stück.

□

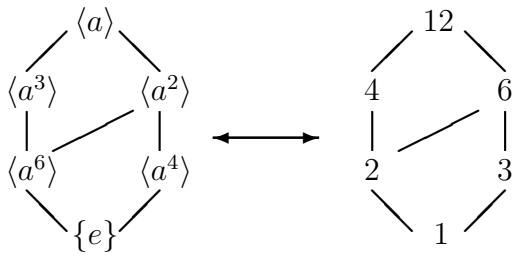
Korollar 8.13 Die zyklische Gruppe der Ordnung n hat für jeden Teiler $d \,|\, n$ genau eine Untergruppe der Ordnung d.

Beweis: Sei $n = md$ und $\langle a\rangle$ die zyklische Gruppe der Ordnung n. Jedenfalls ist $\langle a^m\rangle$ eine Untergruppe der Ordnung d. Sie enthält $\varphi(d)$ Erzeuger (also Elemente der Ordnung d). Die Gruppe $\langle a\rangle$ enthält jedoch nur $\varphi(d)$ Elemente der Ordnung d, also befinden sich alle in $\langle a^m\rangle$. Da jede Untergruppe von $\langle a\rangle$ zyklisch ist, muss somit $\langle a^m\rangle$ die einzige der Ordnung d sein.

□

Bemerkung: Der Untergruppenverband der zyklischen Gruppe der Ordnung n ist isomorph zum Teilerverband von n.

Beispiel: Betrachte die zyklische Gruppe der Ordnung 12 und ein Element a mit $|a| = 12$:



Kapitel 9

Isomorphiesätze

Proposition 9.1 (Einfache Tatsachen über Normalteiler) Sei G eine Gruppe. Es gelten folgende Beziehungen:

1. $H \leq G$, $N \trianglelefteq G \;\Rightarrow\; H \cap N \trianglelefteq H$
2. $H \leq G$, $K \trianglelefteq G$ mit $K \subseteq H \;\Rightarrow\; K \trianglelefteq H$.
3. $H \leq G$, $N \trianglelefteq G \;\Rightarrow\; HN = NH$; $HN \leq G$ und $N \trianglelefteq HN$

Beweis:

1. Zu zeigen ist, dass $\forall a \in H \cap N,\ h \in H$ gilt: $hah^{-1} \in H \cap N$. Wegen $a \in H \cap N \subseteq H,\ h \in H$ gilt jedoch $hah^{-1} \in H$, wegen $N \trianglelefteq G$ gilt $hah^{-1} \in N$. Insgesamt folgt also $hah^{-1} \in H \cap N$.
2. Aus $K \leq G$ und $K \subseteq H$ folgt sofort $K \leq H$. Da $\forall g \in G, k \in K$ $gkg^{-1} \in K$ ist, gilt insbesondere $\forall g \in H, k \in K$ $gkg^{-1} \in K$, also $K \trianglelefteq H$.
3. $\forall h \in H$ (sogar $\forall h \in G$) $hN = Nh$, d.h. $\forall h \in H, n \in N\ \exists m \in N :$ $hn = mh$. Ebenso gilt $\forall h \in H, m \in N\ \exists n \in N :\ mh = hn$. Daher ist $HN = \{hn \,|\, n \in N, h \in H\} \subseteq \{mh \,|\, m \in N, h \in H\} = NH$ und analog $NH \subseteq HN$, insgesamt also $HN = NH$.
   Es gilt $H, K \leq G \implies (HK \leq G \;\Leftrightarrow\; HK = KH)$ (Beweis als Übung). Damit folgt $HN \leq G$. Klarerweise ist $N = eN \leq HN$, und wegen $N \trianglelefteq G$ muss nach 2. auch $N \trianglelefteq HN$ sein.

□

Satz 9.2 (2. Isomorphiesatz) *Sei G eine Gruppe, $H \leq G$, $N \trianglelefteq G$. Dann gilt:*

$$H/(N \cap H) \simeq NH/N$$

BEMERKUNG: Die Motivation für diesen Satz ergibt sich daraus, dass man H/N bilden möchte, aber im Allgemeinen $N \not\subseteq H$ ist. Dies kann auf zwei Arten repariert werden: man kann N zu $N \cap H$ verkleinern oder H zu HN vergrößern. Der Satz zeigt, dass beide Varianten gleichwertig sind.

Beweis: $N \cap H \trianglelefteq H$ und $N \trianglelefteq NH$ sind erfüllt. Wir betrachten nun die Funktion $\varphi : H \to NH/N$, definiert durch $\varphi(h) = Nh$. φ ist dann ein Gruppenhomomorphismus: $\varphi(gh) = N(gh) = (Ng)(Nh) = \varphi(g)\varphi(h)$.
φ ist surjektiv, da $NH/N = \{Ng \,|\, g \in NH\} = \{Nnh \,|\, n \in N, h \in H\} = \{Nh \,|\, h \in H\} = \operatorname{Im}\varphi$ ist. Also ist $\overline{\varphi} : H/(\operatorname{Ker}\varphi) \to NH/N$ ein Isomorphismus (Nach Satz 7.11). Aus der Tatsache, dass $\operatorname{Ker}\varphi = \{h \in H \,|\, Nh = N\} = \{h \in H \,|\, h \in N\} = H \cap N$ ist, folgt die Behauptung.

□

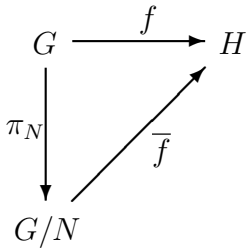
BEMERKUNG: $HN/N = \{gN \,|\, g \in HN\} = \{gN \,|\, g \in H\}$, da für $g = hn$, $h \in H, n \in N$ gilt: $gN = hnN = hN$; aber aus $gN \in HN/N = \{gN \,|\, g \in H\}$ folgt nicht, dass $g \in H$, sondern nur $g \in HN$!

BEMERKUNG: Wenn $N \trianglelefteq G$, $H \leq G$ mit $N \subseteq H$ gilt, dann ist $N \trianglelefteq H$ und $H/N = \{hN \,|\, h \in H\} \leq \{gN \,|\, g \in G\} = G/N$ (die Multiplikation in H/N ist gegeben durch $(hN)(h'N) = (hh')N$; dies ist lediglich die Einschränkung der Multiplikation in G/N auf H/N). Wenn zusätzlich $H \trianglelefteq G$ ist, dann gilt auch $H/N \trianglelefteq G/N$: aus $hN \in H/N$ und $gN \in G/N$ folgt nämlich:

$$(gN)(hN)(gN)^{-1} = (gN)(hN)(g^{-1}N) = (ghg^{-1})N \in H/N$$

da wegen $H \trianglelefteq G$ $ghg^{-1} \in H$ ist. Wir werden sehen, dass jede Untergruppe (jeder Normalteiler) von G/N die Form H/N mit $H \leq G$ (bzw. $H \trianglelefteq G$) hat.

Satz 9.3 *Sei $f : G \to H$ ein Gruppenhomomorphismus und $N \trianglelefteq G$ mit $N \subseteq \operatorname{Ker} f$. Dann existiert eine Funktion $\overline{f} : G/N \to H$, sodass $f = \overline{f} \circ \pi_N$, wobei $\pi_N : G \to G/N$ die kanonische Projektion ist. D.h., das folgende Diagramm kommutiert:*



Beweis: Die Funktion $\overline{f}$, die durch $\overline{f}(gN) = f(g)$ definiert ist, erfüllt die Bedingung:

- $\overline{f}$ ist wohldefiniert: $g' \in gN \Rightarrow g' = gn$ für ein $n \in N$, also $f(g') = f(gn) = f(g)f(n) = f(g)$, da wegen $N \subseteq \operatorname{Ker} f$ $f(n) = e$ ist.
- $\overline{f}$ ist ein Homomorphismus: $\overline{f}((gN)(g'N)) = \overline{f}(gg'N) = f(gg') = f(g)f(g') = \overline{f}(gN)\overline{f}(g'N)$
- $\forall a \in G$: $\overline{f}(\pi_N(a)) = \overline{f}(aN) = f(a)$, d.h. $\overline{f} \circ \pi_N = f$.

□

Lemma 9.4 Sei $f : G \to H$ ein Gruppenhomomorphismus, $a \in G$, $A \subseteq G$, $C \subseteq H$, dann gilt:

1. $f^{-1}(f(a)) = a \operatorname{Ker} f$
2. $f^{-1}(f(A)) = A \operatorname{Ker} f$
3. $f(f^{-1}(C)) = C \cap \operatorname{Im} f$

Beweis: als Übung.

Satz 9.5 (Korrespondenzsatz) *Seien G, H Gruppen, $f : G \to H$ ein Gruppenepimorphismus (also surjektiv), $K := \operatorname{Ker} f$. Wir definieren*

$$\mathcal{U}_K(G) := \{A \mid A \leq G, K \subseteq A\}$$

$$\mathcal{U}(H) := \{C \mid C \leq H\}$$

$$\mathcal{N}_K(G) := \{N \mid N \trianglelefteq G, K \subseteq N\}$$

$$\mathcal{N}(H) := \{M \mid M \trianglelefteq H\}$$

Es gilt:

1. - *$\varphi : \mathcal{U}_K(G) \to \mathcal{U}(H)$, definiert durch $\varphi(A) = f(A)$, ist eine bijektive Funktion.*
   - *$\psi : \mathcal{U}(H) \to \mathcal{U}_K(G)$, definiert durch $\psi(C) = f^{-1}(C)$, ist die Umkehrabbildung von φ.*
   - *$\varphi|_{\mathcal{N}_K(G)} : \mathcal{N}_K(G) \to \mathcal{N}(H)$ ist bijektiv mit der Umkehrabbildung $\psi|_{\mathcal{N}(H)} : \mathcal{N}(H) \to \mathcal{N}_K(G)$.*

2. $\forall A, B \in \mathcal{U}_K(G)$ (*Untergruppen mit* $K \subseteq A$, $K \subseteq B$) *gilt:*

$A \leq B \iff f(A) \leq f(B)$ *und, falls* $A \leq B$, *dann* $[B : A] = [f(B) : f(A)]$

$A \trianglelefteq B \iff f(A) \trianglelefteq f(B)$ *und, falls* $A \trianglelefteq B$, *dann* $B/A \simeq f(B)/f(A)$

Beweis:

1. $A \leq G \Rightarrow f(A) \leq H$, also definiert $\varphi(A) = f(A)$ eine Funktion $\varphi : \mathcal{U}_K(G) \to \mathcal{U}(H)$.
   $A \trianglelefteq G \Rightarrow f(A) \trianglelefteq \operatorname{Im} f = H$, da f surjektiv ist, also ist auch $\varphi|_{\mathcal{N}_K(G)} : \mathcal{N}_K(G) \to \mathcal{N}(H)$ eine Funktion.
   $C \leq H \Rightarrow f^{-1}(C) \leq G$, also ist auch $\psi : \mathcal{U}(H) \to \mathcal{U}_K(G)$ eine Funktion.
   $C \trianglelefteq H \Rightarrow f^{-1}(C) \trianglelefteq G$, also ist auch $\psi|_{\mathcal{N}(H)} : \mathcal{N}(H) \to \mathcal{N}_K(G)$ eine Funktion.
   Sei nun $A \in \mathcal{U}_K(G)$. Dann ist $\psi \circ \varphi(A) = f^{-1}f(A) = A \operatorname{Ker} f = A$, da $\operatorname{Ker} f \subseteq A$.
   Sei umgekehrt $C \in \mathcal{U}(H)$. Dann ist $\varphi \circ \psi(C) = ff^{-1}(C) = \operatorname{Im} f \cap C = C$, da f surjektiv ist.
   Also sind φ und ψ bijektiv und invers zueinander.

2. $A, B \leq G \Rightarrow f(A), f(B) \leq H$ ist bereits bekannt. Ist $A \subseteq B$, dann folgt $f(A) \subseteq f(B)$ und somit $f(A) \leq f(B)$.
   Ist umgekehrt $f(A) \leq f(B)$, dann folgt: $f(A) \subseteq f(B) \Rightarrow A = f^{-1}f(A) \subseteq f^{-1}f(B) = B$ (weil $K \subseteq A, B$).
   Sei nun $A \trianglelefteq B$. $f|_B : B \to f(B)$ ist ein Epimorphismus. Wendet man auf diesen 1. an, ergibt sich $f(A) \trianglelefteq f(B)$. Ist umgekehrt $f(A) \trianglelefteq f(B)$, dann folgt $(f|_B)^{-1}f|_B(A) = A \operatorname{Ker} f|_B = A \trianglelefteq B$.
   Es bleibt zu zeigen, dass $[B : A] = [f(B) : f(A)]$ ist, falls $A \leq B$: $g : \{bA \mid b \in B\} \to \{cf(A) \mid c \in f(B)\}$ mit $g(bA) = f(b)f(A)$ ist eine Bijektion:

   - g ist wohldefiniert: $bA = b'A \Rightarrow f(b)f(b')^{-1} = f(bb'^{-1}) \in f(A)$, da $bb'^{-1} \in A$, also ist $f(b)f(A) = f(b')f(A)$.
   - g ist surjektiv: trivial
   - g ist injektiv:

     $$\begin{aligned} g(bA) = g(b'A) &\Rightarrow f(b)f(b')^{-1} = f(bb'^{-1}) \in f(A) \\ &\Rightarrow bb'^{-1} \in f^{-1}(f(bb'^{-1})) \subseteq f^{-1}f(A) = A \\ &\Rightarrow bA = b'A \end{aligned}$$

Also folgt $[B : A] = [f(B) : f(A)]$. Ist zudem $A \trianglelefteq B$, dann ist g sogar ein Homomorphismus, denn dann gilt

$$\begin{aligned} g((bA)(b'A)) &= g(bb'A) = f(bb')f(A) = f(b)f(b')f(A) \\ &= f(b)f(A)f(b')f(A) = g(bA)g(b'A) \end{aligned}$$

Damit folgt dann $B/A \simeq f(B)/f(A)$.

□

Bilder und Urbilder unter der kanonischen Projektion:

BEMERKUNG: Sei $N \trianglelefteq G$ und $\pi_N : G \to G/N$, $\pi_N(a) = aN$, die kanonische Projektion. Dann gilt für eine Menge $A \subseteq G$:

$$\begin{aligned} \pi_N(A) &= \{aN \mid a \in A\} \\ &= \{\text{alle Nebenklassen von } N, \text{ die einen Repräsentanten in } A \text{ haben}\} \\ &= \{bN \mid b \in G, bN \cap A \neq \emptyset\} \\ &= AN/N \subseteq G/N \end{aligned}$$

Für eine Menge $C \subseteq G/N$, $C = \{bN \mid b \in B\}$, gilt umgekehrt:

$$\begin{aligned} \pi_N^{-1}(C) &= \{a \in G \mid aN \in C\} \\ &= \bigcup_{aN \in C} aN = \bigcup_{b \in B} bN \end{aligned}$$

Wenn $H \leq G$ mit $N \subseteq H$ gilt, dann ist $\pi_N(H) = HN/N = H/N$ ($N \subseteq H \Rightarrow HN = H$).

Satz 9.6 (3. Isomorphiesatz) *Sei G eine Gruppe, $N \trianglelefteq G$. Wir definieren weiters*

$$\mathcal{U}_N(G) = \{H \leq G \mid N \subseteq H\} \text{ und } \mathcal{U}(G/N) = \{K \mid K \leq G/N\}$$

Dann ist $\varphi : \mathcal{U}_N(G) \to \mathcal{U}(G/N)$ mit $\varphi(H) = H/N$ eine Bijektion mit der Umkehrabbildung $\psi : \mathcal{U}(G/N) \to \mathcal{U}_N(G)$ mit $\psi(K) = \pi_N^{-1}(K) = \bigcup_{aN \in K} aN$. Außerdem gilt für $H \in \mathcal{U}_N(G)$ die Äquivalenz $H \trianglelefteq G \Leftrightarrow H/N \trianglelefteq G/N$, und wenn $H \trianglelefteq G$, $H \in \mathcal{U}_N(G)$, dann gilt

$$G/H \simeq (G/N)/(H/N)$$

Beweis: Dies ist lediglich der Korrespondenzsatz, angewandt auf den Epimorphismus π_N.

BEMERKUNG: Aus dem Korrespondenzsatz folgt auch $[G : H] = [(G/N) : (H/N)]$, falls $H \leq G$ (nicht notwendigerweise ein Normalteiler) mit $N \subseteq H$ ist.

Kapitel 10

Untergruppen mit trivialem Durchschnitt

Definition 10.1 Seien $A, B \leq G$. Der Durchschnitt $A \cap B$ heißt *trivial*, wenn $A \cap B = \{e\}$.

Proposition 10.2 Sei G eine Gruppe, $H, K \leq G$. Wenn $H \cap K = \{e\}$, dann gilt $\forall g \in HK \ \exists!(h,k) \in H \times K$ mit $g = hk$.

Beweis: $hk = h'k' \ \Rightarrow \ h'^{-1}h = k'k^{-1} \in H \cap K$, daher ist $e = h'^{-1}h = k'k^{-1}$ und somit $h = h'$, $k = k'$.

□

Proposition 10.3 Seien $H, K \leq G$, $|H|$,$|K|$ endlich und $H \cap K = \{e\}$. Dann gilt $|HK| = |H||K|$.

Beweis: Da $\forall g \in HK \ \exists!(h,k) \in H \times K$ mit $g = hk$, ist $\varphi : H \times K \to HK$ mit $\varphi(h,k) = hk$ bijektiv. Also ist $|HK| = |H \times K| = |H||K|$.

□

Bemerkung: Sind $H, K \leq G$, dann gilt $|HK| = |H|[K : (H \cap K)]$; wenn $|H|, |K|$ endlich sind, dann ist $[K : (H \cap K)] = \frac{|K|}{|H \cap K|}$, also $|HK| = \frac{|H||K|}{|H \cap K|}$.

Beweis: als Übung.

Korollar 10.4 Ist G endlich, $H, K \leq G$ und $H \cap K = \{e\}$, $|H||K| = |G|$, dann ist $G = HK$.

Beweis: Aus $|H||K| = |G|$ folgt $|HK| = |G|$, zudem ist $HK \subseteq G$. Da G endlich ist, folgt daraus $HK = G$.

□

Proposition 10.5 Seien $H, K \trianglelefteq G$ Normalteiler mit $H \cap K = \{e\}$. Dann gilt $\forall h \in H, k \in K$: $hk = kh$.

Beweis: $hk(kh)^{-1} = (hkh^{-1})k^{-1} \in K$, weil aus $K \trianglelefteq G$ $hkh^{-1} \in K$ folgt. Ebenso gilt $hk(kh)^{-1} \in H$, also $hk(kh)^{-1} \in H \cap K = \{e\}$. Damit ergibt sich $hk(kh)^{-1} = e \;\Rightarrow\; hk = kh$

□

Bemerkung: Diese Tatsache gilt nur, falls H *und* K Normalteiler sind!

Proposition 10.6 Seien $H, K \leq G$, $|H|, |K|$ endlich und $\mathrm{ggT}(|H|, |K|) = 1$. Dann haben H und K trivialen Durchschnitt.

Beweis: Sei $a \in H \cap K$. Nach dem Satz von Lagrange gilt $|a| \Big| |H|$ und $|a| \Big| |K|$. Daher muss $|a| \Big| 1$ und somit $|a| = 1 \;\Rightarrow\; a = e$ gelten.

□

Bemerkung: Alles, was aus $H \cap K = \{e\}$ folgt, folgt damit auch aus $\mathrm{ggT}(|H|, |K|) = 1$.

Proposition 10.7 Seien $a, b \in G$, $|a|$,$|b|$ endlich, $\mathrm{ggT}(|a|, |b|) = 1$ und $ab = ba$. Dann folgt $|ab| = |a||b|$.
Allgemeiner gilt: falls $a, b \in G$, $\langle a \rangle \cap \langle b \rangle = \{e\}$ und $ab = ba$ gilt, dann folgt $|ab| = \mathrm{kgV}(|a|, |b|)$.

Beweis: als Übung.

Kapitel 11

Direktes Produkt zweier Gruppen

Definition 11.1 Seien H, K Gruppen. Die auf der Menge $H \times K = \{(h,k) \mid h \in H, k \in K\}$ durch $(h,k) \cdot (h',k') := (hh', kk')$ definierte Gruppe heißt (äußere) *direkte Summe* von H und K (geschrieben $H \oplus K$) oder (äußeres) *direktes Produkt* von H und K (geschrieben $H \times K$).

Bemerkung: $H \times K$ ist tatsächlich eine Gruppe:

- Assoziativität: klar.
- Neutrales Element: $e := (e_H, e_K)$ erfüllt die Bedingung.
- Inverses Element: $(h,k)^{-1} := (h^{-1}, k^{-1})$ erfüllt die Bedingung.

Proposition 11.2 $H \times (K \times G) \simeq (H \times K) \times G$

Beweis: $\varphi : H \times (K \times G) \to (H \times K) \times G$ mit $\varphi(h,(k,g)) = ((h,k),g)$ ist offensichtlich ein Isomorphismus.

□

Proposition 11.3 Seien H, K Gruppen.

1. $\varepsilon_H : H \to H \times K$ mit $\varepsilon_H(h) = (h,e)$ und $\varepsilon_K : K \to H \times K$ mit $\varepsilon_K(k) = (e,k)$ (die *Einbettungen*) sind Gruppenmonomorphismen; dabei ist $H \simeq \operatorname{Im} \varepsilon_H = \{(h,e) \mid h \in H\} = H \times \{e\} =: \widetilde{H}$ und $K \simeq \operatorname{Im} \varepsilon_K = \{(e,k) \mid k \in K\} = \{e\} \times K =: \widetilde{K}$.
2. $\widetilde{H}, \widetilde{K} \leq H \times K$ mit $\widetilde{H} \cap \widetilde{K} = \{(e_H, e_K)\} = \{e\}$ und $\widetilde{H}\widetilde{K} = H \times K$.

3. $p_H : H \times K \to H$ mit $p_H(h,k) = h$ und $p_K : H \times K \to K$ mit $p_K(h,k) = k$ (die *Projektionen*) sind Gruppenepimorphismen; Ker $p_H = \widetilde{K}$, Ker $p_K = \widetilde{H}$, also $\widetilde{K}, \widetilde{H} \trianglelefteq H \times K$.

Beweis: trivial.

Bemerkung: Für $\widetilde{h} = (h,e) \in \widetilde{H}$ und $\widetilde{k} = (e,k) \in \widetilde{K}$ folgt aus $\widetilde{H}, \widetilde{K} \trianglelefteq H \times K$, $\widetilde{H} \cap \widetilde{K} = \{e\}$, dass $\widetilde{h}\widetilde{k} = \widetilde{k}\widetilde{h}$; dies ergibt sich auch direkt aus $(h,e)(e,k) = (h,k) = (e,k)(h,e)$.

Satz 11.4 (Innere direkte Summe) *Wenn G eine Gruppe ist, $H \trianglelefteq G$, $K \trianglelefteq G$ mit $H \cap K = \{e\}$ und $HK = G$, dann gilt $G \simeq H \times K$, wobei $\varphi : H \times K \to G$ mit $\varphi(h,k) = hk$ der Isomorphismus ist.*

Beweis:

- φ ist Homomorphismus: $\varphi((h,k)(h',k')) = \varphi((hh',kk')) = hh'kk'$; da Normalteiler mit trivalem Durchschnitt elementweise kommutieren, gilt $h'k = kh'$, also $\varphi((h,k)(h',k')) = hh'kk' = hkh'k' = \varphi((h,k))\varphi((h',k'))$.
- φ ist surjektiv, da $G = HK$.
- φ ist injektiv: $\varphi(h,k) = \varphi(h',k') \;\Rightarrow\; hk = h'k' \;\Rightarrow\; h'^{-1}h = k'k^{-1} \in H \cap K = \{e\} \;\Rightarrow\; h = h', k = k'$.

□

Bemerkung: Wenn also $H \trianglelefteq G$, $K \trianglelefteq G$ mit $HK = G$, $H \cap K = \{e\}$ gilt, dann folgt $\forall g \in G\ \exists!(h,k) \in H \times K$ mit $g = hk$, und wenn $g = hk, g = h'k'$ mit $h, h' \in H$ und $k, k' \in K$, dann ist $gg' = hkh'k' = hh'kk'$, d.h., die H- und K-Anteile werden unabhängig multipliziert.

Bemerkung: Wenn $N \trianglelefteq G$ und $H \leq G$ (nicht notwendigerweise auch $H \trianglelefteq G$!) mit $NH = G$ und $H \cap N = \{e\}$ gilt, dann hat ebenso jedes Element $g \in G$ eine eindeutige Darstellung der Form $g = nh$ mit $h \in H, n \in N$, und es gilt: $nhn'h' = n(hn'h^{-1})hh'$ ($hn'h^{-1} \in N$, weil N Normalteiler ist).

Proposition 11.5 Sei G eine Gruppe, $a \in G$. Dann ist $\varphi_a : G \to G$ mit $\varphi_a(x) = axa^{-1}$ (*Konjugation* mit a) ein Automorphismus auf G.

Beweis:

- $\varphi_a(gh) = agha^{-1} = aga^{-1}aha^{-1} = \varphi_a(g)\varphi_a(h)$, also ist φ_a ein Homomorphismus.

- $\varphi_a \circ \varphi_{a^{-1}} = \mathrm{id}$ und $\varphi_{a^{-1}} \circ \varphi_a = \mathrm{id}$, also ist φ_a bijektiv.

□

Definition 11.6 Ein Automorphismus der Form φ_a für ein $a \in G$ heißt *innerer Automorphismus*.

Bemerkung: $\mathrm{Aut}(G) = \{\varphi : G \to G \,|\, \varphi \text{ ist Automorphismus}\}$ ist eine Gruppe bezüglich $\circ$. Das Bild von G unter der Abbildung $a \mapsto \varphi_a$, $\mathrm{Im}\, G = \{\varphi_a \,|\, a \in G\} \leq \mathrm{Aut}\, G$, ist eine Untergruppe.

Bemerkung: Ist $H \leq G$, dann gilt $H \trianglelefteq G \;\Leftrightarrow\; \forall a \in G\ \varphi_a(H) = H$.

Definition 11.7 Sei G eine Gruppe, $a, b \in G$. a heißt zu b *konjugiert*, wenn $\exists g \in G :\ a = gbg^{-1}$, man schreibt $a \sim_G b$. $\sim_G$ ist eine Äquivalenzrelation, die Äquivalenzklassen heißen *Konjugiertenklassen*.

Bemerkung: $H \leq G$ ist genau dann Normalteiler, wenn H Vereinigung ganzer Konjugiertenklassen ist.

Kapitel 12

Die symmetrische Gruppe

Definition 12.1 Sei $\underline{n} = \{1, \ldots, n\}$. Die Menge aller bijektiven Abbildungen von $\underline{n}$ auf sich (*Permutationen* von $\underline{n}$) bildet bezüglich der Verknüpfung $\circ$ eine Gruppe der Ordnung $n! = n(n-1)\ldots 1$, die *symmetrische Gruppe* vom Grad n, kurz S_n.

Definition 12.2 $\pi \in S_n$ heißt *r-Zyklus*, wenn es $a_1, \ldots, a_r$ (paarweise verschieden) in $\underline{n}$ gibt, sodass $\pi(a_1) = a_2$, $\pi(a_2) = a_3$, ..., $\pi(a_r) = a_1$ und $\pi(a) = a$ für alle anderen $a \in \underline{n}$ gilt. Wir schreiben in diesem Fall $\pi = (a_1 a_2 \ldots a_r)$. r heißt *Länge* des Zyklus.

Bemerkung: Man kann den Zyklus auch mit einem anderen a_i beginnen, z.B. $\pi = (a_2 a_3 \ldots a_r a_1)$, es gibt also r äquivalente Schreibweisen für jeden r-Zyklus.

Definition 12.3 Zwei Permutationen π, σ heißen *disjunkt*, wenn

$$\{i \mid \pi(i) \neq i\} \cap \{j \mid \sigma(j) \neq j\} = \emptyset$$

Lemma 12.4 Disjunkte Permutationen kommutieren, d.h. für disjunkte π, σ gilt $\pi\sigma = \sigma\pi$.

Beweis: Sei $A = \{i \mid \pi(i) \neq i\}$ und $B = \{j \mid \sigma(j) \neq j\}$. Dann ist $A \cap B = \emptyset$. Für $a \in A$ gilt auch $\pi(a) \in A$, da π bijektiv ist. Somit sind $a, \pi(a) \notin B$, und es folgt $\pi(\sigma(a)) = \pi(a) = \sigma(\pi(a))$ und analog für $b \in B$ $\pi(\sigma(b)) = \sigma(\pi(b))$. Für ein $c \in \underline{n} \setminus (A \cup B)$ gilt wiederum $\pi(\sigma(c)) = \pi(c) = c = \sigma(c) = \sigma(\pi(c)))$ Also ist $\pi\sigma = \sigma\pi$.

□

Satz 12.5 *Jede Permutation ist als Produkt disjunkter Zyklen darstellbar. Diese Darstellung ist eindeutig bis auf die Reihenfolge der Zyklen und die*

r verschiedenen Schreibweisen eines jeden r-Zyklus, wenn man festlegt, dass auch alle 1*-Zyklen* (*Fixpunkte*) *angeschrieben werden.*

Beweis: Sei $a \in \underline{n}$. Betrachte die Folge $a_0 = a$, $a_{i+1} = \pi(a_i)$. Da $\underline{n}$ endlich ist, muss es ein minimales $k \geq 0$ geben, sodass $a_k = a_j$ für ein $j < k$. Angenommen, es wäre $j \neq 0$. Dann folgt aus $\pi(a_{j-1}) = a_j = a_k = \pi(a_{k-1})$ wegen der Injektivität von π, dass $a_{j-1} = a_{k-1}$, im Widerspruch zur Minimalität von k. Also muss $j = 0$ sein.
Man schreibt nun den Zyklus $(a_0 \dots a_{k-1})$ an und iteriert diesen Vorgang mit einem $b_0 \in \underline{n} \setminus \{a_0, \dots, a_{k-1}\}$. Wegen der Injektivität von π ist der neue Zyklus disjunkt zum vorigen.
Der Vorgang bricht mit einer Menge von Zyklen ab, in der jedes $a \in \underline{n}$ genau einmal vorkommt. π ist das Produkt dieser Zyklen.

□

Bemerkung: Das Inverse wird in der Zyklendarstellung einfach gebildet, indem man alle Zyklen umkehrt, d.h. aus $(a_1 a_2 \dots a_r)$ wird $(a_r a_{r-1} \dots a_1)$.
Für disjunkte Permutationen gilt $\pi\sigma = \sigma\pi \;\Rightarrow\; (\pi\sigma)^{-1} = \sigma^{-1}\pi^{-1} = \pi^{-1}\sigma^{-1}$.

Definition 12.6 Der *Zyklentyp* einer Permutation $\pi \in S_n$ ist $[t_1, \dots, t_n]$ mit $t_i :=$ Anzahl der i-Zyklen in der Darstellung von π als Produkt disjunkter Zyklen.

Lemma 12.7 Zwei Permutationen π, σ sind genau dann konjugiert (d.h. $\exists \rho \in S_n : \sigma = \rho\pi\rho^{-1}$), wenn π, σ vom selben Zyklentyp sind.

Beweis: „⇒“: Sei $\sigma = \rho\pi\rho^{-1}$. Dann gilt für i, j mit $\pi(i) = j$: $\sigma(\rho(i)) = \rho(\pi(i)) = \rho(j)$. D.h., $\pi : i \mapsto j \;\Rightarrow\; \sigma : \rho(i) \mapsto \rho(j)$. Also führt Ersetzen von i durch $\rho(i)$ in der Zyklendarstellung von π zur Zyklendarstellung von σ. Somit haben π und σ denselben Zyklentyp.
„⇐“: Seien π, σ vom selben Zyklentyp. Man schreibt π, σ untereinander, sodass Zyklen gleicher Länge untereinander zu stehen kommen:

$$\begin{aligned} \pi &= (..)(...)(.)\dots \\ \sigma &= (..)(...)(.)\dots \end{aligned}$$

ρ sei jene Funktion, die jedes $a \in \underline{n}$ auf das darunterliegende abbildet. Dann ist ρ bijektiv; außerdem gilt $\pi : i \mapsto j \;\Leftrightarrow\; \sigma : \rho(i) \mapsto \rho(j)$, d.h. $\sigma(\rho(i)) = \rho(\pi(i))\ \forall i \in \underline{n}$ und somit $\sigma = \rho\pi\rho^{-1}$.

□

Beispiel: Sei $\pi = (34)(125)(6)$ und $\sigma = (56)(134)(2)$. Für $\rho = (1)(23546)$ gilt: $\sigma = \rho\pi\rho^{-1}$.

Korollar 12.8 Jede Konjugiertenklasse besteht genau aus allen Permutationen eines Zyklentyps.

Korollar 12.9 Eine Untergruppe von S_n ist genau dann ein Normalteiler, wenn sie eine Vereinigung von vollständigen Konjugiertenklassen ist, d.h. wenn sie zu jedem Element auch alle Permutationen desselben Zyklentyps enthält.

Definition 12.10 $\pi \in S_n$ heißt *Transposition*, wenn $\exists a, b \in \underline{n}$, $a \neq b$, sodass $\pi(a) = b$, $\pi(b) = a$ und $\forall j \in \underline{n} \setminus \{a, b\}$ $\pi(j) = j$, d.h. $\pi = (a\, b)$.

Lemma 12.11 Jedes $\pi \in S_n$ ist als Produkt von Transpositionen darstellbar.

Beweis: Es genügt zu zeigen, dass jeder Zyklus als Produkt von Transpositionen darstellbar ist. Dies ist jedoch der Fall:

$$(a_1 a_2 \dots a_r) = (a_1 a_r)(a_1 a_{r-1}) \dots (a_1 a_3)(a_1 a_2)$$

□

Definition 12.12 Für $\pi \in S_n$ ist

$$\operatorname{sgn} \pi := \prod_{\{i,j\}} \frac{\pi(i) - \pi(j)}{i - j}$$

wobei das Produkt über alle ungeordneten Paare $\{i, j\}$ läuft.

Bemerkung: sgn nimmt nur Werte ± 1 an! (alle ungeordneten Paare kommen sowohl im Zähler als auch im Nenner je einmal vor)

Lemma 12.13 Ist $\pi = (a\, b)$ eine Transposition, dann ist $\operatorname{sgn} \pi = -1$.

Beweis:

$$\begin{aligned}
\operatorname{sgn}(a\, b) &= \frac{\pi(a) - \pi(b)}{a - b} \cdot \prod_{j \notin \{a,b\}} \frac{\pi(a) - \pi(j)}{a - j} \frac{\pi(b) - \pi(j)}{b - j} \cdot \prod_{\substack{\{i,j\} \\ \{i,j\} \cap \{a,b\} = \emptyset}} \frac{\pi(i) - \pi(j)}{i - j} \\
&= \frac{b - a}{a - b} \cdot \prod_{j \notin \{a,b\}} \frac{b - j}{a - j} \frac{a - j}{b - j} \cdot \prod_{\substack{\{i,j\} \\ \{i,j\} \cap \{a,b\} = \emptyset}} \frac{i - j}{i - j} \\
&= (-1) \cdot 1 \cdot 1 = -1
\end{aligned}$$

□

Lemma 12.14 $\operatorname{sgn}(\pi\sigma) = (\operatorname{sgn}\pi)(\operatorname{sgn}\sigma)$

Beweis:

$$\begin{aligned}\operatorname{sgn}(\pi\sigma) &= \prod_{\{i,j\}} \frac{\pi(\sigma(i)) - \pi(\sigma(j))}{i-j} \\ &= \prod_{\{i,j\}} \frac{\pi(\sigma(i)) - \pi(\sigma(j))}{\sigma(i) - \sigma(j)} \prod_{\{i,j\}} \frac{\sigma(i) - \sigma(j)}{i-j} \\ &= \operatorname{sgn}(\pi)\operatorname{sgn}(\sigma)\end{aligned}$$

□

Korollar 12.15 Wenn π ein Produkt von m Transpositionen ist, dann ist $\operatorname{sgn}(\pi) = (-1)^m$; die Parität der Anzahl der Transpositionen in der Darstellung von π ist eindeutig.

Definition 12.16 $\pi \in S_n$ heißt *gerade*, wenn $\operatorname{sgn}\pi = 1$, *ungerade*, wenn $\operatorname{sgn}\pi = -1$.

Definition 12.17 $A_n := \{\pi \in S_n \mid \operatorname{sgn}\pi = 1\}$ heißt die *alternierende Gruppe* vom Grad n.

Bemerkung: Weil $\operatorname{sgn}(\pi\sigma) = (\operatorname{sgn}\pi)(\operatorname{sgn}\sigma)$, ist A_n abgeschlossen bezüglich $\cdot$. Da A_n endlich ist, muss daher A_n eine Untergruppe sein, d.h. $A_n \leq S_n$.

Lemma 12.18 $A_n \trianglelefteq S_n$

Beweis:

1. Variante: Da $\operatorname{sgn}\pi$ nur vom Zyklentyp abhängt, besteht A_n aus vollständigen Konjugiertenklassen.

2. Variante: $[S_n : A_n] = 2 \Rightarrow A_n$ ist Normalteiler (die einzigen Linksnebenklassen müssen A_n und $S_n \setminus A_n$ sein, dies sind jedoch auch die einzigen Rechtsnebenklassen).

3. Variante: Weil $\operatorname{sgn} : S_n \to (\{1,-1\},\cdot)$ ein Gruppenhomomorphismus ist und $A_n = \operatorname{Ker}\operatorname{sgn}$ ist, ist A_n ein Normalteiler.

□

BEMERKUNG:

Ad 1.: Da

$$(a_1 a_2 \dots a_r) = \underbrace{(a_1 a_r)(a_1 a_{r-1}) \dots (a_1 a_2)}_{r-1 \text{ Transpositionen}}$$

ist, gilt:

- Ein r-Zyklus mit $r \equiv 0 \mod 2$ ist eine ungerade Permutation.
- Ein r-Zyklus mit $r \equiv 1 \mod 2$ ist eine gerade Permutation.

D.h.: für π mit Zyklentyp $[t_1, \dots, t_n]$ ist $\operatorname{sgn} \pi = (-1)^{t_2 + t_4 + \cdots}$.

Kapitel 13

Direktes Produkt und direkte Summe von Gruppen

Definition 13.1 Sei I eine nichtleere Menge und für jedes $i \in I$ eine Gruppe G_i gegeben. Wir verallgemeinern das *direkte Produkt* von Gruppen durch die Definition

$$\prod_{i\in I} G_i = \{(g_i)_{i\in I} \,|\, g_i \in G_i \text{ für } i \in I\} = \{g : I \to \bigcup_{i\in I} G_i \,|\, g(i) \in G_i\}$$

D.h., ein Element von $\prod_{i\in I} G_i$ ist eine Zuordnung eines Elements $g(i) = g_i \in G_i$ zum Index i für jedes $i \in I$. Auf dieser Menge definieren wir die Multiplikation durch komponentenweise Multiplikation:

$$(g_i)_{i\in I} \cdot (h_i)_{i\in I} = (g_i h_i)_{i\in I}$$

Proposition 13.2 Sei G_i eine Gruppe für $i \in I$. Dann ist $\prod_{i\in I} G_i$ eine Gruppe mit dem neutralen Element $e = (e_i)_{i\in I}$ und dem Inversen $((g_i)_{i\in I})^{-1} = (g_i^{-1})_{i\in I}$. $\prod_{i\in I} G_i$ ist genau dann kommutativ, wenn alle G_i kommutativ sind.

Beweis: trivial.

Definition 13.3 Sei G_i eine Gruppe für $i \in I$, $\prod_{i\in I} G_i$ das direkte Produkt. Für $j \in I$ heißt

$$p_j : \prod_{i\in I} G_i \to G_j \text{ mit } p_j((g_i)_{i\in I}) = g_j$$

die *Projektion* auf den j-ten Faktor G_j und

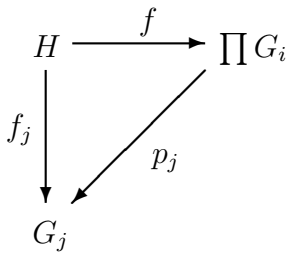
$$\varepsilon_j : G_j \to \prod_{i\in I} G_i \text{ mit } \varepsilon_j(g) = (g_i)_{i\in I}, \text{ wobei } g_i = \begin{cases} g & i = j \\ e_{G_i} & i \neq j \end{cases}$$

die *Einbettung* des j-ten Faktors G_j in $\prod_{i\in I} G_i$.

Proposition 13.4 p_j ist ein Gruppenepimorphismus, ε_j ist ein Gruppenmonomorphismus. $\widetilde{G}_j = \{(g_i)_{i\in I} \,|\, g_i = e_{G_i} \text{ für } i \neq j\} = \operatorname{Im}\varepsilon_j \simeq G_j$ ist ein Normalteiler von $\prod_{i\in I} G_i$.

Beweis: als Übung.

Satz 13.5 (Universelle Eigenschaft des direkten Produkts) *Für $i \in I$ sei G_i eine Gruppe, $P = \prod_{i\in I} G_i$, $p_j : P \to G_j$ die Projektion auf den j-ten Faktor. Dann gilt:*
Für alle Gruppen H und alle Mengen $\{f_i : H \to G_i \,|\, i \in I\}$ von Gruppenhomomorphismen gibt es genau einen Homomorphismus $f : H \to P$ mit $\forall j \in I\ p_j \circ f = f_j$, d.h. das folgende Diagramm kommutiert:



Beweis: $p_j(f(h)) = f_j(h)\ \forall j \ \Rightarrow\ f(h) = (f_i(h))_{i\in I}$, also kann es höchstens einen solchen Homomorphismus geben, nämlich $f : H \to P$ definiert durch $f(h) = (f_i(h))_{i\in I}$. Dann gilt tatsächlich für alle j: $p_j(f(h)) = p_j((f_i(h))_{i\in I}) = f_j(h)$. Es bleibt noch zu zeigen, dass f ein Homomorphismus ist:

$$f(hk) = (f_i(hk))_{i\in I} = (f_i(h)f_i(k))_{i\in I} = (f_i(h))_{i\in I}(f_i(k))_{i\in I} = f(h)f(k)$$

□

Definition 13.6 Sei $I \neq \emptyset$ eine Menge und für jedes $i \in I$ eine Gruppe G_i gegeben. Die *direkte Summe* der G_i, $\sum_{i\in I} G_i$ (oder $\bigoplus_{i\in I} G_i$), ist

$$\{(a_i)_{i\in I} \,|\, a_i \in G_i \text{ für } i \in I \wedge \text{ nur für endlich viele } i \in I \text{ ist } a_i \neq e_{G_i}\}$$

mit der komponentenweisen Multiplikation $(a_i)_{i\in I} \cdot (b_i)_{i\in I} = (a_i b_i)_{i\in I}$.
Sie kann als Untergruppe von $\prod_{i\in I} G_i$ aufgefasst werden:

$$\sum_{i\in I} G_i = \{(a_i)_{i\in I} \in \prod_{i\in I} G_i \,|\, \text{für höchstens endlich viele } i \in I \text{ ist } a_i \neq e_{G_i}\}$$

Bemerkung: $\sum_{i\in I} G_i \trianglelefteq \prod_{i\in I} G_i$.

Definition 13.7 Sei G_i eine Gruppe für $i \in I$, $\sum_{i\in I} G_i$ die direkte Summe. Für $j \in I$ heißt

$$p_j : \sum_{i\in I} G_i \to G_j \text{ mit } p_j((g_i)_{i\in I}) = g_j$$

die *Projektion* auf den j-ten Summanden G_j und

$$\varepsilon_j : G_j \to \sum_{i\in I} G_i \text{ mit } \varepsilon_j(g) = (g_i)_{i\in I}, \text{ wobei } g_i = \begin{cases} g & i = j \\ e_{G_i} & i \neq j \end{cases}$$

die *Einbettung* des j-ten Summanden G_j in $\sum_{i\in I} G_i$.

Proposition 13.8 p_j ist ein Gruppenepimorphismus, ε_j ist ein Gruppenmonomorphismus. $\widetilde{G}_j = \{(g_i)_{i\in I} \mid g_i = e_{G_i} \text{ für } i \neq j\} = \operatorname{Im} \varepsilon_j \simeq G_j$ ist ein Normalteiler von $\sum_{i\in I} G_i$. $\sum_{i\in I} G_i = \langle \bigcup_{j\in I} \widetilde{G}_j \rangle$ und $\forall j\ \widetilde{G_j} \cap \langle \bigcup_{j\in I, i\neq j} \widetilde{G}_j \rangle = \{e\}$.

Beweis: als Übung.

Satz 13.9 (Innere direkte Summe) *Sei $(G, +)$ eine Gruppe, $I \neq \emptyset$ eine Menge und für $i \in I$ sei $N_i \leq G$. Wenn die Bedingungen*

1. $\forall i \in I\ N_i \trianglelefteq G$
2. $\forall j \in I\ N_j \cap \langle \bigcup_{i\in I, i\neq j} N_i \rangle = \{0\}$
3. $G = \langle \bigcup_{i\in I} N_i \rangle$

gleichzeitig gelten, dann gilt

(a) Für $g_i \in N_i$, $g_j \in N_j$ mit $i \neq j$ ist $g_i + g_j = g_j + g_i$.

(b) Jedes $g \in G$ hat eine Darstellung $g = g_{i_1} + \ldots + g_{i_n}$ mit $g_{i_k} \in N_{i_k}$ und $i_k \neq i_j$ für $k \neq j$.

(c) Diese Darstellung ist bis auf die Reihenfolge und eventuell eingefügte Summanden $g_{i_j} = 0$ eindeutig.

Außerdem ist dann $\sum_{i\in I} N_i \simeq G$, wobei $\varphi : \sum_{i\in I} N_i \to G$ mit $\varphi((g_i)_{i\in I}) = g_{i_1} + \ldots + g_{i_n}$ (dabei ist $\{i_1, \ldots, i_n\} = \{i \in I \mid g_i \neq 0\} =: \operatorname{Supp} g$) der Isomorphismus ist.

Beweis:

(a) Nach 1. und 2. sind N_i und N_j Normalteiler mit trivialem Durchschnitt und kommutieren daher elementweise.

(b) Wegen 3. hat jedes $g \in G$ eine Darstellung der Form $g = g_{i_1} + \ldots + g_{i_n}$, wobei die i_k aber nicht notwendigerweise verschieden sein müssen. Wegen (a) kann man die g_{i_k} aber so vertauschen, dass alle g_{i_k} aus demselben N_i nebeneinanderstehen. Dann kann man sie zu einem Element zusammenfassen.

(c) Angenommen, es sei $g_{i_1} + \ldots + g_{i_k} = g'_{i_1} + \ldots + g'_{i_k}$ mit $g_{i_j}, g'_{i_j} \in N_{i_j}$, wobei die i_j paarweise verschieden seien (gegebenenfalls stellt man geeignet um und fügt Nullen ein, um links und rechts Elemente derselben Gruppen stehen zu haben). Dann folgt:

$$-g'_{i_1} + g_{i_1} = g'_{i_2} + \ldots + g'_{i_k} - g_{i_2} - \ldots - g_{i_k} \in N_{i_1} \cap \langle \bigcup_{i \in I, i \neq i_1} N_i \rangle$$

Wegen 2. muss daher $-g'_{i_1} + g_{i_1} = 0$, also $g'_{i_1} = g_{i_1}$, sein. Nun kann man auf beiden Seiten kürzen und erhält induktiv, dass $g'_{i_j} = g_{i_j}$ für alle j ist.

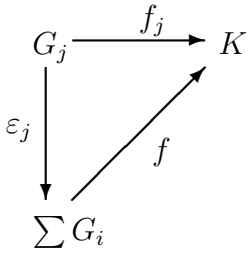
Sei nun φ wie oben definiert, wobei $\varphi(0) = 0$ gesetzt wird. Dann ist φ wegen (b) und (c) bijektiv. Es bleibt zu zeigen, dass φ ein Homomorphismus ist:
Zunächst sei bemerkt, dass für ein Element $(g_i)_{i \in I} \in \sum_{i \in I} N_i$ und eine beliebige endliche Menge $\{j_1, \ldots, j_m\}$, die $\operatorname{Supp} g$ enthält, auch $\varphi((g_i)_{i \in I}) = g_{j_1} + \ldots + g_{j_m}$ ist, da ja $g_{j_k} = 0$ für ein $j_k \notin \operatorname{Supp} g$ ist.
Seien nun $(g_i)_{i \in I}$, $(h_i)_{i \in I}$ zwei Elemente von $\sum_{i \in I} N_i$ und $K = \{k_1, \ldots, k_m\} =: (\operatorname{Supp} g) \cup (\operatorname{Supp} h)$. Dann ist jedenfalls für alle $i \in I \setminus K$ $g_i + h_i = 0$, d.h. $i \notin \operatorname{Supp}(g + h)$, also $\operatorname{Supp}(g + h) \subseteq K$. Es folgt:

$$\begin{aligned} \varphi((g_i)_{i \in I} + (h_i)_{i \in I}) &= \varphi((g_i + h_i)_{i \in I}) \\ &= (g_{k_1} + h_{k_1}) + \ldots + (g_{k_m} + h_{k_m}) \\ &\overset{(*)}{=} g_{k_1} + \ldots + g_{k_m} + h_{k_1} + \ldots + h_{k_m} \\ &= \varphi((g_i)_{i \in I}) + \varphi((h_i)_{i \in I}) \end{aligned}$$

Man beachte, dass g_{k_l} und h_{k_l} nicht kommutieren müssen, der Schritt $(*)$ ist also keineswegs trivial. Man kann dennoch leicht von der einen auf die Darstellung kommen: hinter jedem h_{k_l} stehen nur Elemente aus den Gruppen N_i mit $i > k_l$, daher kann man der Reihe nach alle h_{k_l} durch geeignete Vertauschungen nach hinten verschieben, bis alle g_{k_r} vor allen h_{k_l} stehen.

□

Satz 13.10 (Universelle Eigenschaft der direkten Summe) *Sei $I \neq \emptyset$ eine Menge und für $i \in I$ sei $(G_i, +)$ eine Gruppe. Dann gilt für alle kommutativen Gruppen $(K, +)$ und alle Mengen $\{f_i : G_i \to K \mid i \in I\}$ von Gruppenhomomorphismen, dass es genau einen Homomorphismus $f : \sum_{i \in I} G_i \to K$ mit $\forall j \in I$ $f \circ \varepsilon_j = f_j$ gibt, d.h. das folgende Diagramm kommutiert:*



Beweis: Sei $g = (g_i)_{i\in I}$ und $\{i_1, \ldots, i_n\}$ derart, dass $g_i = 0$ für alle $i \notin \{i_1, \ldots, i_n\}$ ist. Dann ist $g = \varepsilon_{i_1}(g_{i_1}) + \ldots + \varepsilon_{i_n}(g_{i_n})$, und es muss daher gelten:

$$f(g) = f(\varepsilon_{i_1}(g_{i_1})) + \ldots + f(\varepsilon_{i_n}(g_{i_n})) = f_{i_1}(g_{i_1}) + \ldots + f_{i_n}(g_{i_n})$$

Also gibt es höchstens einen solchen Homomorphismus, nämlich $f : \sum_{i\in I} G_i \to K$ mit $f((g_i)_{i\in I}) = f_{i_1}(g_{i_1}) + \ldots + f_{i_n}(g_{i_n})$ für $\{i_1, \ldots, i_n\} = \operatorname{Supp} g$ (und $f(0) = 0$). Weil K kommutativ ist, kommt es dabei nicht auf die Reihenfolge der Summanden an, f ist daher jedenfalls wohldefiniert. Es bleibt jedoch zu zeigen, dass f ein Homomorphismus ist:
Seien dazu $g = (g_i)_{i\in I}$ und $h = (h_i)_{i\in I}$ gegeben und $\{i_1, \ldots, i_n\} = (\operatorname{Supp} g) \cup (\operatorname{Supp} h)$.

$$\begin{aligned}
f((g_i)_{i\in I} + (h_i)_{i\in I}) &= f((g_i + h_i)_{i\in I}) \\
&= f_{i_1}(g_{i_1} + h_{i_1}) + \ldots + f_{i_n}(g_{i_n} + h_{i_n}) \\
&= f_{i_1}(g_{i_1}) + f_{i_1}(h_{i_1}) + \ldots + f_{i_n}(g_{i_n}) + f_{i_n}(h_{i_n}) \\
&\overset{K \text{ kommutativ}}{=} f_{i_1}(g_{i_1}) + \ldots + f_{i_n}(g_{i_n}) + f_{i_1}(h_{i_1}) + \ldots + f_{i_n}(h_{i_n}) \\
&= f((g_i)_{i\in I}) + f((h_i)_{i\in I})
\end{aligned}$$

□

Bemerkung: Wenn $H_i \leq G_i$ für $i \in I$, dann ist $\prod_{i\in I} H_i \simeq \{(a_i)_{i\in I} \in \prod_{i\in I} G_i \,|\, a_i \in H_i\} \leq \prod_{i\in I} G_i$.
Ebenso gilt $\sum_{i\in I} H_i \simeq \{(a_i)_{i\in I} \in \sum_{i\in I} G_i \,|\, a_i \in H_i\} \leq \sum_{i\in I} G_i$. Man schreibt daher $\prod_{i\in I} H_i \leq \prod_{i\in I} G_i$ und $\sum_{i\in I} H_i \leq \sum_{i\in I} G_i$.
Dies sind jedoch keineswegs alle Untergruppen von $\prod_{i\in I} G_i$ bzw. $\sum_{i\in I} G_i$, z.B. ist ja $\sum_{i\in I} G_i \leq \prod_{i\in I} G_i$ nicht von dieser Form. Auch $\{(g, g) \,|\, g \in G\} \leq G \times G$ ist nicht von dieser Form.

Satz 13.11 *Sei $I \neq \emptyset$ eine Menge und für jedes $i \in I$ seien Gruppen G_i, H_i und ein Homomorphismus $f_i : G_i \to H_i$ gegeben. Dann ist $f =: \prod_{i\in I} f_i : \prod_{i\in I} G_i \to \prod_{i\in I} H_i$, definiert durch $f((g_i)_{i\in I}) = (f_i(g_i))_{i\in I}$, ein Gruppenhomomorphismus mit*

$$f\left(\sum_{i\in I} G_i\right) \subseteq \sum_{i\in I} H_i$$

$$\operatorname{Ker} f = \{(g_i)_{i\in I} \mid g_i \in \operatorname{Ker} f_i \ \forall i\} = \prod_{i\in I} \operatorname{Ker} f_i$$

und

$$\operatorname{Im} f = \{(h_i)_{i\in I} \mid h_i \in \operatorname{Im} f_i \ \forall i\} = \prod_{i\in I} \operatorname{Im} f_i$$

Insbesondere ist f genau dann ein Epi- bzw. Monomorphismus, wenn alle f_i Epi- bzw. Monomorphismen sind. Weiters gilt auch für $\widetilde{f} = f|_{\sum G_i} : \sum_{i\in I} G_i \to \sum_{i\in I} H_i$:

$$\operatorname{Ker} \widetilde{f} = \sum_{i\in I} \operatorname{Ker} f_i \text{ und } \operatorname{Im} \widetilde{f} = \sum_{i\in I} \operatorname{Im} f_i$$

Beweis: als Übung.

Korollar 13.12 Wenn $N_i \trianglelefteq G_i$ für $i \in I$, dann ist $\prod_{i\in I} N_i \trianglelefteq \prod_{i\in I} G_i$, und es gilt

$$\left(\prod_{i\in I} G_i\right) / \left(\prod_{i\in I} N_i\right) \simeq \prod_{i\in I} (G_i/N_i) \text{ und } \left(\sum_{i\in I} G_i\right) / \left(\sum_{i\in I} N_i\right) \simeq \sum_{i\in I} (G_i/N_i)$$

Beweis: Man wende den vorherigen Satz auf $\pi_i : G_i \to G_i/N_i$ und den 1. Isomorphiesatz an.

Kapitel 14

Wirkung einer Gruppe auf eine Menge

Definition 14.1 Sei M eine Menge, $(G, \cdot)$ eine Gruppe. Eine *Wirkung* (von links) von G auf M ist eine Funktion $f : G \times M \to M$, $(g, x) \to gx$, sodass

1. $\forall x \in M \ \forall g, h \in G \ (g \cdot h)x = g(hx)$
2. $\forall x \in M \ ex = x$ (wobei e das neutrale Element von G ist)

Bemerkung: Wenn durch $f : G \times M \to M$ eine Wirkung auf M gegeben ist, dann definiert jedes $g \in G$ eine Funktion $\varphi_g : M \to M$ durch $\varphi_g(x) = gx$, und φ_g ist bijektiv ($\forall x \in M \ \varphi_g\varphi_{g^{-1}}(x) = g(g^{-1}x) = (gg^{-1})x = ex = x$, also gilt $\varphi_g \circ \varphi_{g^{-1}} = \mathrm{id}_M$). Die Abbildung $\varphi : G \to S_M = \{\pi : M \to M \mid \pi \text{ bijektiv}\}$ ist ein Gruppenhomomorphismus.
Wenn umgekehrt $\varphi : G \to S_M$ ein Gruppenhomomorphismus ist, dann definiert $f : G \times M \to M$ mit $f(g, x) = \varphi_g(x)$ eine Wirkung von G auf M.

Bemerkung: Bei Verwechslungsgefahr mit einem Produkt schreiben wir $\varphi_g(x)$ anstelle von gx.

Definition 14.2 Eine Wirkung heißt *treu*, wenn φ injektiv ist (d.h. wenn für ein $g \in G \ \forall x \in M \ gx = x$ gilt, dann muss $g = e$ sein).

Beispiel: $(G, \cdot)$ wirkt auf G durch Linkstranslation (sogenannte *Cayley-Darstellung*): $f : G \times G \to G$, $(g, x) \mapsto g \cdot x = L_g(x)$ (d.h. $\varphi_g = L_g$). Die Bedingungen für eine Wirkung sind offensichtlich erfüllt:

1. $(g \cdot h)x = (g \cdot h) \cdot x = g \cdot (h \cdot x) = g \cdot (hx) = g(hx)$
2. $ex = e \cdot x = x$

BEISPIEL: $(G, \cdot)$ wirkt auf G durch Konjugation: $f : G \times G \to G,\ (g, x) \mapsto g \cdot x \cdot g^{-1}$

1. $(g \cdot h)x = (g \cdot h) \cdot x \cdot (g \cdot h)^{-1} = g \cdot h \cdot x \cdot h^{-1} \cdot g^{-1} = g(h \cdot x \cdot h^{-1}) = g(hx)$
2. $ex = e \cdot x \cdot e^{-1} = e \cdot x \cdot e = x$

BEISPIEL: $(G, \cdot)$ wirkt auf der Menge der Linksnebenklassen von $H \leq G$ durch Linkstranslation: $(g, aH) \mapsto gaH$; auch $K \leq G$ wirkt auf den Linksnebenklassen von H in G durch Linkstranslation.

Definition 14.3 G wirke auf M; für $x \in M$ heißt

$$\overline{x} = \{y \in M \mid \exists g \in G :\ gx = y\} = \{gx \mid g \in G\}$$

die *Bahn* (*Orbit*) von x.

$$\mathrm{St}_G(x) = \{g \in G \mid gx = x\}$$

heißt *Stabilisator* von x.

BEMERKUNG:

1. Wenn G auf M wirkt, dann ist $x \sim y :\Leftrightarrow \exists g \in G : gx = y$ eine Äquivalenzrelation auf M:

   - Reflexivität: $ex = x$, also $x \sim x$.
   - Symmetrie: $gx = y \ \Rightarrow\ g^{-1}y = x$, also $x \sim y \ \Rightarrow\ y \sim x$.
   - Transitivität: $gx = y$, $hy = z \Rightarrow hgx = z$, also $x \sim y \wedge y \sim z \ \Rightarrow\ x \sim z$.

   Die Äquivalenzklasse von x bezüglich dieser Relation ist $\overline{x}$, die Bahn von x. Also bilden die Bahnen eine Partition von M.

2. $\mathrm{St}_G(x) \leq G$, denn es gilt:

   - $ex = x \ \Rightarrow e \in St_G(x)$
   - $g \in \mathrm{St}_G(x) \ \Rightarrow\ gx = x \ \Rightarrow g^{-1}x = x \ \Rightarrow g^{-1} \in \mathrm{St}_G(x)$
   - $g, h \in \mathrm{St}_G(x) \ \Rightarrow\ gx = x \wedge hx = x \ \Rightarrow\ ghx = gx = x \ \Rightarrow\ gh \in \mathrm{St}_G(x)$

BEISPIEL: $(G, \cdot)$ wirkt auf der Menge der Untergruppen von G durch Konjugation: $(g, H) \mapsto gHg^{-1}$. Die Bahn von H ist dann $\{gHg^{-1} \mid g \in G\}$, die Konjugiertenklasse von H.

Satz 14.4 *G wirke auf M. Es gilt:*

1. $|\overline{x}| = [G : \mathrm{St}_G(x)]$
2. $\mathrm{St}_G(gx) = g\,\mathrm{St}_G(x)g^{-1}$

Beweis:

1. $h\ \mathrm{St}_G(x) = g\ \mathrm{St}_G(x) \Leftrightarrow h^{-1}g \in \mathrm{St}_G(x) \Leftrightarrow h^{-1}gx = x \Leftrightarrow gx = hx$. Also hat jede Linksnebenklasse von $\mathrm{St}_G(x)$ die Form $g\ \mathrm{St}_G(x) = \{h \in G \,|\, hx = gx\} = \{h \in G \,|\, hx = y\}$ für $y = gx \in \overline{x}$. Da es auch zu jedem $y \in \overline{x}$ ein $g \in G$ mit $gx = y$ und daher eine Linksnebenklasse $g\ \mathrm{St}_G(x) = \{h \in G \,|\, hx = y\}$ gibt, definiert $y \mapsto \{g \in G \,|\, gx = y\}$ eine Bijektion $\overline{x} \to \{g\ \mathrm{St}_G(x) \,|\, g \in G\}$.
2. Sei $h \in \mathrm{St}_G(gx)$. Dann ist $ghg^{-1}(gx) = ghx = gx$, also $ghg^{-1} \in \mathrm{St}_G(gx)$. Damit folgt $g\,\mathrm{St}_G(x)g^{-1} \subseteq \mathrm{St}_G(gx)$.
   Sei umgekehrt $f \in \mathrm{St}_G(x)$. Dann ist $(g^{-1}fg)x = g^{-1}(f(gx)) = g^{-1}(gx) = ex = x$, also $g^{-1}fg \in \mathrm{St}_G(x)$ und damit $f \in g\,\mathrm{St}_G(x)g^{-1}$. Es folgt $\mathrm{St}_G(gx) \subseteq g\,\mathrm{St}_G(x)g^{-1}$.

□

Korollar 14.5 Die Stabilisatoren der Elemente eines Orbits bilden eine Konjugiertenklasse von Untergruppen von G.

Definition 14.6 Sei G eine Gruppe und $x \in G$. Der *Zentralisator* von x in G ist

$$Z_G(x) := \{g \in G \,|\, gx = xg\} = \{g \in G \,|\, gxg^{-1} = x\}$$

d.h. der Stabilisator von x unter der Wirkung von G auf sich durch Konjugation.
Für eine Untergruppe $H \leq G$ definiert man:

$$Z_H(x) := \{g \in H \,|\, gx = xg\} = \{g \in H \,|\, gxg^{-1} = x\}$$

(der Stabilisator von x unter der Wirkung von H auf G durch Konjugation)

Bemerkung: Die Konjugiertenklasse von x in G ist $\overline{x} = \{y \in G \,|\, \exists g \in G : gxg^{-1} = y\} = \{gxg^{-1} \,|\, g \in G\}$, d.h. die Bahn von x unter der Wirkung von G auf sich durch Konjugation. Wir wissen bereits, dass $|\overline{x}| = [G : Z_G(x)]$ gilt.

Definition 14.7 Sei G eine Gruppe. Dann heißt

$$Z(G) = \{g \in G \,|\, \forall x \in G \; gx = xg\} = \{g \in G \,|\, \forall x \in G \; gxg^{-1} = x\}$$

das *Zentrum* von G.

BEMERKUNG: $Z(G) \trianglelefteq G$. $Z(G)$ ist sogar eine sogenannte *charakteristische Untergruppe* , d.h. $\forall f \in \mathrm{Aut}(G) \; f(Z(G)) = Z(G)$.

BEMERKUNG: $x \in Z(G) \;\Leftrightarrow\; |\overline{x}| = 1$, weil $gxg^{-1} = x \;\Leftrightarrow\; gx = xg$.

Satz 14.8 (Klassengleichung) *Sei G eine endliche Gruppe, $x_1, \ldots, x_n$ ein Repräsentantensystem der Konjugiertenklassen. Dann gilt*

$$|G| = \sum_{i=1}^{n} [G : Z_G(x_i)]$$

Wenn $y_1, \ldots, y_m$ ein Repräsentantensystem der Konjugiertenklassen mit mehr als einem Element ist, dann gilt

$$|G| = |Z(G)| + \sum_{j=1}^{m} [G : Z_G(y_j)]$$

Beweis: G ist disjunkte Vereinigung von Konjugiertenklassen: $G = \bigcup\!\!\!\cdot_{i=1}^{n} \overline{x_i}$, also $|G| = \sum_{i=1}^{n} |\overline{x_i}| = \sum_{i=1}^{n} [G : Z_G(x_i)]$.
$Z(G) = \{x \in G \,|\, |\overline{x}| = 1\}$, also ist $G = Z(G) \cup \bigcup\!\!\!\cdot_{j=1}^{m} \overline{y_j}$ und somit $|G| = |Z(G)| + \sum_{j=1}^{m} [G : Z_G(y_j)]$.

□

Semidirektes Produkt von Gruppen:

BEMERKUNG: Aus Kapitel 11 wissen wir: wenn $N \trianglelefteq G$ und $H \leq G$ mit $NH = G$ und $H \cap N = \{e\}$ gilt, dann hat jedes Element $g \in G$ eine eindeutige Darstellung der Form $g = nh$ mit $h \in H, n \in N$, und es gilt: $nhn'h' = n(hn'h^{-1})hh' = n\varphi_h(n')hh'$. Dabei ist $\varphi_h \in \mathrm{Aut}(G)$ ein innerer Automorphismus, und weil N Normalteiler und somit $hNh^{-1} = N$ ist, ist auch $\varphi_h|_N \in \mathrm{Aut}(N)$.
Sei umgekehrt eine Funktion $\varphi : H \to \mathrm{Aut}(N)$, $\varphi(h) =: \varphi_h \in \mathrm{Aut}(N)$ gegeben, dann definiert die Operation $(n, h) \cdot (n', h') = (n\varphi_h(n'), hh')$ eine Gruppe auf der Menge $N \times H$, ein sogenanntes *semidirektes Produkt* von N und H, geschrieben $N \rtimes_\varphi H$.

Lemma 14.9 $N \rtimes_\varphi H$ ist tatsächlich eine Gruppe, $\widetilde{N} = \{(n,e) \in N \rtimes_\varphi H\} \trianglelefteq N \rtimes_\varphi H$, $\widetilde{H} = \{(e,h) \in N \rtimes_\varphi H\} \leq N \rtimes_\varphi H$, $\varepsilon_N : N \to \widetilde{N}$ mit $\varepsilon_N(n) = (n,e)$ und $\varepsilon_H : H \to \widetilde{H}$ mit $\varepsilon_H(h) = (e,h)$ sind Gruppenisomorphismen. Insbesondere also $N \simeq \widetilde{N}$, $H \simeq \widetilde{H}$ und $\widetilde{N} \cap \widetilde{H} = \{(e,e)\}$.

Beweis: als Übung.

Bemerkung: G ist genau dann semidirektes Produkt eines Normalteilers $N \trianglelefteq G$ mit einer Untergruppe $H \leq G$, wenn es ein Repräsentantensystem der Nebenklassen von N gibt, das eine Untergruppe von G bildet.

Bemerkung: Sind H und K kommutativ, so gilt

$$G \text{ kommutativ } \Leftrightarrow \varphi \text{ trivial } (\forall h \in H\ \varphi_h = \mathrm{id}_K) \Leftrightarrow G \simeq N \times K$$

Beispiel: *Diëdergruppe* D_n = Symmetriegruppe des regelmäßigen n-Ecks:

Das regelmäßige n-Eck wird durch Spiegelungen an n Symmetrieachsen und Drehungen um Vielfache von $\frac{2\pi}{n}$ auf sich abgebildet. Diese werden von einer fixen Spiegelung β und der Drehung um $\frac{2\pi}{n}$ (o.B.d.A. im Uhrzeigersinn), α, erzeugt. Die Diëdergruppe besteht somit aus den Elementen

$$D_n = \{e, \alpha, \ldots, \alpha^{n-1}, \beta, \alpha\beta, \ldots, \alpha^{n-1}\beta\}$$

Sei C_n die zyklische Gruppe der Ordnung n, multiplikativ geschrieben, erzeugt von α, also $C_n = \langle\alpha\rangle$ mit $|\alpha| = n$. Sei weiters C_2 die zyklische Gruppe der Ordnung 2, die von β erzeugt wird. Dann gilt: $C_n \trianglelefteq D_n$, $C_2 \leq D_n$ und $C_n \cap C_2 = \emptyset$. Weiters wirkt C_2 auf C_n durch $\varphi_e(g) = g$ und $\varphi_\beta(g) = g^{-1}$. Da die Abbildung $g \mapsto g^{-1}$ für die kommutative Gruppe C_n ein Automorphismus ist (siehe unten), sind alle Bedingungen für ein semidirektes Produkt erfüllt, also gilt $D_n = C_n \rtimes_\varphi C_2$.
Die Multiplikation in D_n ist durch folgende Rechenregeln gegeben:

$$\alpha^n = e;\ \beta^2 = e;\ \beta\alpha^k = \alpha^{-k}\beta;\ \alpha^k\alpha^l = \alpha^{k+l};\ \alpha^k\beta\alpha^l\beta = \alpha^{k-l}; \alpha^k\beta\alpha^l = \alpha^{k-l}\beta$$

Bemerkung: Für eine Gruppe G ist die Abbildung $g \mapsto g^{-1}$ genau dann ein Isomorphismus, wenn G kommutativ ist, denn: $(ab)^{-1} = a^{-1}b^{-1} \Leftrightarrow ab = (b^{-1})^{-1}(a^{-1})^{-1} = ba$.

Kapitel 15

Sylowsätze

Definition 15.1 Sei p eine Primzahl. Eine Gruppe $(G, \cdot)$ heißt *endliche p-Gruppe*, wenn $\exists n \in \mathbb{N}_0$ mit $|G| = p^n$.

Bemerkung: Eine Gruppe heißt allgemein *p-Gruppe* (für eine Primzahl p), wenn $\forall x \in G\ \exists m \in \mathbb{N}_0$, sodass $|x| = p^m$; eine endliche Gruppe G ist genau dann p-Gruppe, wenn $\exists n \in \mathbb{N}_0$ mit $|G| = p^n$.

Lemma 15.2 Eine endliche p-Gruppe wirke auf eine endliche Menge M; sei $M_0 := \{x \in M \,|\, \forall g \in G\ gx = x\}$, dann gilt $|M_0| \equiv |M| \mod p$.

Beweis: M ist disjunkte Vereinigung von Bahnen, $M_0 = \{x \in M \,|\, |\overline{x}| = 1\}$. Sei $y_1, \ldots, y_m$ ein Repräsentantensystem der Bahnen mit mehr als einem Element. Dann gilt $M = M_0 \cup \bigdot_{i=1}^{m} \overline{y_i}$ und somit $|M| = |M_0| + \sum_{i=1}^{m} |\overline{y_i}| = |M_0| + \sum_{i=1}^{m} [G : \mathrm{St}_G(y_i)]$. Wegen $|G| = p^n$ und $1 < [G : \mathrm{St}_G(y_i)] \,\Big|\, |G| = p^n$ gibt es zu jedem i ein $n_i > 0$, sodass $[G : \mathrm{St}_G(y_i)] = p^{n_i}$ und somit $[G : \mathrm{St}_G(y_i)] \equiv 0 \mod p$. Daraus folgt die Behauptung.

□

Satz 15.3 (Satz von Cauchy) *Sei G eine endliche Gruppe und p eine Primzahl mit $p \,\Big|\, |G|$. Dann $\exists g \in G$ mit $|g| = p$.*

Beweis: Sei $M = \{(g_1, \ldots, g_p) \in G \times \ldots \times G \,|\, g_1 g_2 \ldots g_p = e\}$. $\mathbb{Z}_p$ wirke auf M durch zyklische Vertauschung, d.h. $\overline{1}(g_1, \ldots, g_p) = (g_2, \ldots, g_p, g_1)$, $\overline{k}(g_1, \ldots, g_p) = (g_{k+1 \bmod p}, \ldots, g_{k+p \bmod p})$.

$\varphi_{\overline{k}}$ ist wohldefiniert, d.h. es hängt nicht von k, sondern von $\overline{k}$ ab. Es bleibt zu überprüfen, dass $(g_1, \ldots, g_p) \in M \Rightarrow \varphi_{\overline{k}}(g_1, \ldots, g_p) \in M$ gilt:

$$\begin{aligned} g_1 g_2 \ldots g_p = e &\implies (g_1 \ldots g_k)(g_{k+1} \ldots g_p) = e \\ &\implies (g_1 \ldots g_k)^{-1} = (g_{k+1} \ldots g_p) \\ &\implies (g_{k+1} \ldots g_p)(g_1 \ldots g_k) = e \end{aligned}$$

Es handelt sich auch tatsächlich um eine Wirkung:

$$\overline{0}(g_1, \ldots, g_p) = (g_1, \ldots, g_p)$$

und

$$\begin{aligned} (\overline{k+l})(g_1, \ldots, g_p) &= (g_{k+l+1 \mod p}, \ldots, g_{k+l+p \mod p}) \\ &= \overline{k}(g_{l+1 \mod p}, \ldots, g_{l+p \mod p}) \\ &= \overline{k}(\overline{l}(g_1, \ldots, g_p)) \end{aligned}$$

Dann ist

$$\begin{aligned} M_0 &= \{(g_1, \ldots, g_p) \in M \,|\, (g_{k+1 \mod p}, \ldots, g_{k+p \mod p}) = (g_1, \ldots, g_p)\ \forall k\} \\ &= \{(g_1, \ldots, g_p) \in G \times \ldots \times G \,|\, g_1 g_2 \ldots g_p = e \text{ und } g_1 = \ldots = g_p\} \\ &= \{(g, \ldots, g) \,|\, g^p = e\} \end{aligned}$$

Folglich gilt $|M_0| = |\{g \in G \,|\, g^p = e\}|$; $|M_0| \geq 1$, da $e^p = e$ und somit $(e, \ldots, e) \in M_0$.
$|M| = |G|^{p-1}$, da jedes $(p-1)$-tupel $(g_1, \ldots, g_{p-1})$ ein eindeutig bestimmtes $x \in G$ mit $(g_1, \ldots, g_{p-1}, x) \in M$ definiert, nämlich $x = (g_1 \ldots g_{p-1})^{-1}$.
p ist prim, daher $p - 1 \geq 1$. Somit folgt aus $p \,\Big|\, |G|$ $p \,\Big|\, |G|^{p-1}$ und daher $|M_0| \equiv |M| \equiv 0 \mod p$.
Wegen $p \,\Big|\, |M_0|$ und $|M_0| \geq 1$ gilt $|M_0| = np$ für ein $n > 0$, also $\exists g \neq e$ mit $g^p = e$. Für dieses g folgt dann $|g| = p$.

□

Definition 15.4 Sei $H \leq G$. Der *Normalisator* von H in G ist

$$N_G(H) := \{g \in G \,|\, g^{-1} H g = H\}$$

$N_G(H)$ ist der Stabilisator von H unter der Wirkung von G durch Konjugation auf der Menge der Untergruppen von G; daher ist $N_G(H) \leq G$.

BEMERKUNG: $H \subseteq N_G(H)$ (für $h \in H$ gilt $h^{-1}Hh \subseteq H$ und $hHh^{-1} \subseteq H \Rightarrow H \subseteq h^{-1}Hh$, somit ist $h^{-1}Hh = H$ für alle $h \in H$).
Also gilt $H \trianglelefteq N_G(H)$ nach Definition von $N_G(H)$. $N_G(H)$ ist die größte Untergruppe K von G mit $H \trianglelefteq K$.

BEMERKUNG: $|\{g^{-1}Hg \,|\, g \in G\}| = [G : N_G(H)]$ (Mächtigkeit einer Bahn = Index des Normalisators).

Lemma 15.5 Sei $H \leq G$, $|H| = p^k$ für eine Primzahl p. Dann gilt $[G : H] \equiv [N_G(H) : H] \bmod p$.

Beweis: H wirke auf $M = \{gH \,|\, g \in G\}$, den Linksnebenklassen von H, durch Linkstranslation: $(h, gH) \mapsto hgH$.
Es gilt:

$$\begin{aligned} xH \in M_0 &\iff \forall h \in H\ hxH = xH \ \Leftrightarrow\ \forall h \in H\ x^{-1}hxH = H \\ &\iff \forall h \in H\ x^{-1}hx \in H \ \Leftrightarrow\ x^{-1}Hx \subseteq H \\ &\overset{(*)}{\iff} x^{-1}Hx = H \ \Leftrightarrow\ x \in N_G(H) \end{aligned}$$

wobei die Äquivalenz $(*)$ gilt, weil die Abbildung $g \mapsto x^{-1}gx$ ein Automorphismus auf G und daher bijektiv und H endlich ist. Deswegen muss $|x^{-1}Hx| = |H|$ gelten.
Somit ist $M_0 = \{xH \,|\, x \in N_G(H)\} \Rightarrow |M_0| = [N_G(H) : H]$. Mit Lemma 15.2 folgt die Behauptung.

□

Satz 15.6 (1. Sylowsatz) *Sei G eine endliche Gruppe, p eine Primzahl, $n \geq 0$ maximal mit $p^n \,\big|\, |G|$. Dann gilt $\forall k$ mit $0 \leq k < n$: $\exists H \leq G$ mit $|H| = p^k$ und $\forall H \leq G$ mit $|H| = p^k$ $\exists K \leq G$ mit $|K| = p^{k+1}$ und $H \trianglelefteq K$.*

Korollar 15.7 Ist n maximal mit $p^n \,\big|\, |G|$, dann existiert eine Untergruppe $K \leq G$ mit $|K| = p^n$.

Beweis: durch Induktion nach k. Für $k = 0$ erfüllt $H = \{e\}$ die Bedingung $|H| = p^0 = 1$. Nach dem Satz von Cauchy gibt es ein $g \in G$ mit $|g| = p$. $K = \langle g \rangle$ ist dann eine Gruppe mit $|K| = p$ und $H = \{e\} \trianglelefteq K$.
Induktionsschritt: Nach Induktionsvoraussetzung existiert ein $H \leq G$ mit $|H| = p^k$ (das K aus der Induktionsvoraussetzung). $|G| = [G : H]|H|$, und da $p^n \,\big|\, |G|$, $|H| = p^k$ gilt, muss $p \,|\, [G : H]$ gelten. Nach obigem Lemma folgt $p \,|\, [N_G(H) : H]$.

Nach dem Satz von Cauchy hat daher $N_G(H)/H$ eine Untergruppe der Ordnung p (diese sei $\{g_1H, \ldots, g_pH\}$). Das Urbild dieser Untergruppe unter dem Homomorphismus $\pi : N_G(H) \to N_G(H)/H$ ist $g_1H \cup \ldots \cup g_pH =: K$ mit $|K| = p|H| = p^{k+1}$. Es muss $H \trianglelefteq K$ sein, da $K \subseteq N_G(H)$.

□

Definition 15.8 Sei G eine endliche Gruppe, p eine Primzahl und n maximal mit $p^n \Big| |G|$; eine Untergruppe $H \leq G$ mit $|H| = p^n$ heißt *p-Sylowgruppe* von G.

Satz 15.9 (2. Sylowsatz) *Sei G eine endliche Gruppe, $S \leq G$ eine p-Sylowgruppe und $H \leq G$ mit $|H| = p^k$ für ein $k \in \mathbb{N}_0$. Dann gibt es ein $g \in G$, sodass $H \leq gSg^{-1}$ ist.*

Korollar 15.10 Je zwei p-Sylowgruppen von G sind zueinander konjugiert; daher bilden die p-Sylowgruppen von G eine Konjugiertenklasse von Untergruppen.

Beweis: Sei $M = \{gS \,|\, g \in G\}$. H wirke auf M durch Linkstranslation: $\varphi_h(gS) = hgS$. Weil n maximal mit $p^n \Big| |G|$ ist, gilt

$$p \nmid \frac{|G|}{p^n} = \frac{|G|}{|S|} = [G : S] = |M|$$

Nach Lemma 15.2 gilt daher auch $p \nmid |M_0|$ für

$$\begin{aligned} M_0 &= \{gS \,|\, \forall h \in H \; hgS = gS\} = \{gS \,|\, \forall h \in H \; g^{-1}hgS = S\} \\ &= \{gS \,|\, \forall h \in H \; g^{-1}hg \in S\} = \{gS \,|\, g^{-1}Hg \subseteq S\} \\ &= \{gS \,|\, H \subseteq gSg^{-1}\} \end{aligned}$$

Wegen $p \nmid |M_0|$ muss $M_0 \neq \emptyset$ sein, also gibt es ein $g \in G$ mit $gS \in M_0$. Für dieses g gilt dann $H \subseteq gSg^{-1}$.

□

Bemerkung: Da $|gSg^{-1}| = |S|$ ist, ist jede Konjugierte einer Sylowgruppe wieder eine Sylowgruppe. Nach dem zweiten Sylowsatz sind daher je zwei Sylowgruppen konjugiert. Wenn also S eine beliebige p-Sylowgruppe ist, dann ist $\{gSg^{-1} \,|\, g \in G\}$ die Menge aller p-Sylowgruppen von G.

Bemerkung: Es gibt genau dann eine p-Sylowgruppe S mit $S \trianglelefteq G$, wenn es genau eine p-Sylowgruppe gibt (beides ist äquivalent zu $|\{gSg^{-1} \,|\, g \in G\}| = 1$).

Satz 15.11 (3. Sylowsatz) *Sei p eine Primzahl und G eine endliche Gruppe. Sei n_p die Anzahl der p-Sylowgruppen von G. Dann gilt:*

1. $n_p \Big| |G|$
2. $n_p \equiv 1 \bmod p$

Beweis: Wenn $p \nmid |G|$, dann ist die einzige p-Sylowgruppe in G $\{e\}$, also ist $n_p = 1$, und der Satz ist erfüllt. Sei nun p ein Teiler von $|G|$ und S eine p-Sylowgruppe. Dann ist $n_p = |\{gSg^{-1} \,|\, g \in G\}| = [G : N_G(S)] \Big| |G|$ ($|\overline{S}| = [G : \mathrm{St}_G(S)]$ für die Wirkung von G auf die Untergruppen von G durch Konjugation). Somit ist der erste Punkt erfüllt.
Eine fixe Sylowgruppe S wirkt auf der Menge M der p-Sylowgruppen von G durch Konjugation: für $x \in S$, $T \in M$ sei $\varphi_x(T) = x^{-1}Tx$ (was wieder in M liegt). Weil $S \neq \emptyset$ eine endliche p-Gruppe ist, die auf M wirkt, gilt $|M| \equiv |M_0| \bmod p$, wobei $M_0 = \{T \leq G \,|\, |T| = |S| \wedge \forall x \in S\ x^{-1}Tx = T\} = \{T \leq G \,|\, |T| = |S| \wedge S \subseteq N_G(T)\}$ ist.
Sei nun $T \in M_0$. Dann sind S, T Untergruppen von $N_G(T)$. Weil $T \leq N_G(T) \leq G$ gilt, $|T| = p^n$ ist und n maximal mit $p^n \Big| |G|$ ist, muss n auch maximal mit $p^n \Big| |N_G(T)|$ sein. Nach dem zweiten Sylowsatz sind S, T daher in $N_G(T)$ konjugiert, d.h. $\exists g \in N_G(T)$ mit $g^{-1}Tg = S$. Also ist $S = g^{-1}Tg = T$ (weil $g \in N_G(T)$). Folglich besteht M_0 nur aus einem Element, nämlich S. Es folgt $1 = |M_0| \equiv |M| \bmod p$.

□

Beispiel: Jede Gruppe der Ordnung 12 hat einen nichttrivialen Normalteiler:
$n_2 \equiv 1 \bmod 2$ und $n_2 \,|\, 12 \ \Rightarrow\ n_2 \in \{1, 3\}$.
$n_3 \equiv 1 \bmod 3$ und $n_3 \,|\, 12 \ \Rightarrow\ n_3 \in \{1, 4\}$.
Angenommen, es gäbe keinen Normalteiler der Ordnung 3, d.h. $n_3 = 4$. Jede 3-Sylowgruppe hat dann die Form $\{e, a, a^{-1}\}$, und verschiedene 3-Sylowgruppen haben trivialen Durchschnitt, weil a, a^{-1} bereits Erzeuger von $\{e, a, a^{-1}\}$ sind. Die 4 3-Sylowgruppen enthalten also 8 Elemente der Ordnung 3. Es bleiben nur noch e und drei weitere Elemente übrig. Diese müssen die einzig mögliche 2-Sylowgruppe bilden, und diese ist dann auch Normalteiler.

Beispiel: Seien p, q Primzahlen mit $p > q$. Wenn $|G| = p^n q$ für ein $n \in \mathbb{N}$ ist, dann ist die p-Sylowgruppe ein Normalteiler von G:
$c_p \equiv 1 \bmod p$ und $c_p \Big| |G| = p^n q \ \Rightarrow\ c_p \,|\, q$. Da $p > q$ ist, ist auch $mp + 1 > q$ für alle $m \geq 1$, also jedenfalls nicht $mp + 1 \,|\, q$. Daher muss $c_p = 1$ sein.

Teil II

Ringtheorie

Kapitel 16

Definitionen und Beispiele

Definition 16.1 Eine Menge $R \neq \emptyset$ zusammen mit zwei inneren Operationen $+ : R \times R \to R$ (genannt Addition) und $\cdot : R \times R \to R$ (genannt Multiplikation) heißt *Ring*, wenn gilt:

- $(R, +)$ ist eine kommutative Gruppe (das neutrale Element bezüglich $+$ wird mit 0 bzw. 0_R bezeichnet)
- $(R, \cdot)$ ist eine Halbgruppe
- $\forall a, b, c \in R : \ a \cdot (b + c) = a \cdot b + a \cdot c \wedge (a + b) \cdot c = a \cdot c + b \cdot c$ („*Distributivität*“)

Man schreibt: $(R, +, \cdot)$ ist Ring (oder: R ist Ring).

Definition 16.2

- $(R, +, \cdot)$ heißt *Ring mit Eins*, wenn $(R, \cdot)$ ein Monoid ist; das neutrale Element bezüglich $\cdot$ wird mit 1 (bzw. 1_R) bezeichnet.
- R heißt *kommutativer Ring*, wenn $(R, \cdot)$ kommutativ ist.
- Ein Ring heißt *endlicher Ring*, wenn $\exists n \in \mathbb{N}$ mit $|R| = n$.

Definition 16.3 Für $(R, +)$ und $(R, \cdot)$ werden die für Gruppen und Monoide eingeführten Schreibweisen verwendet:

- Das Inverse von a bezüglich $+$ wird als $-a$ geschrieben; $a - b := a + (-b)$
  Das Inverse von a bezüglich $\cdot$ wird als a^{-1} geschrieben;

- *Vielfache*: für $a \in R, n \in \mathbb{Z}$ definiert man

$$na := \begin{cases} a + \ldots + a & n > 0 \\ 0 & n = 0 \\ (-a) + \ldots + (-a) & n < 0 \end{cases}$$

- *Potenzen*: $a^n := a \cdot \ldots \cdot a$ für $n \in \mathbb{N}$; falls R Ring mit Eins ist, $a^0 := 1$; falls R Ring mit Eins ist und a ein Inverses a^{-1} hat, $a^{-n} := a^{-1} \cdot \ldots \cdot a^{-1}$

BEISPIEL: $(\mathbb{Z}, +, \cdot)$, $(\mathbb{Q}, +, \cdot)$, $(\mathbb{Z}_n, +, \cdot)$ ($\mathbb{Z}_n = \{\overline{k} = k + n\mathbb{Z} \,|\, k \in \mathbb{Z}\}$, $\overline{k} + \overline{l} = \overline{k + l}$ und $\overline{k} \cdot \overline{l} = \overline{k \cdot l}$) sind kommutative Ringe mit Eins.

BEISPIEL: $(2\mathbb{Z}, +, \cdot)$ ist ein kommutativer Ring ohne 1.

BEISPIEL: für einen Körper K (z.B. $K = \mathbb{Q}$ oder $K = \mathbb{R}$) bilden die Matrizen $M_n(K)$ mit der üblichen Matrizenaddition und -multiplikation einen Ring; für $n > 1$ ist er nichtkommutativ.
Unter den Matrizenringen gibt es auch endliche nichtkommutative Ringe: $M_n(\mathbb{Z}_p)$ (für eine Primzahl p) ist ein endlicher nichtkommutativer Ring.

BEISPIEL: Sei $(G, +)$ eine kommutative Gruppe; $\mathrm{End}(G) = \{\varphi : G \to G \,|\, \varphi(g + h) = \varphi(g) + \varphi(h)\}$ (die Menge der Endomorphismen von G) bildet mit den Operationen $+$, definiert durch $(\varphi + \psi)(g) = \varphi(g) + \psi(g)$ $\forall g \in G$, sowie $\circ$, definiert durch $(\varphi \circ \psi)(g) = \varphi(\psi(g))$ $\forall g \in G$, einen Ring mit Eins.

Satz 16.4 (Rechenregeln für Ringe) *Wenn $(R, +, \cdot)$ ein Ring ist, dann gilt:*

1. $\forall a \in R: \; a \cdot 0_R = 0_R \cdot a = 0_R$ (*Bemerkung: dies ist eine andere Aussage als die Definition des* 0*-ten Vielfachen von a durch $0a := 0_R$!*)
2. $\forall a, b, c \in R: \; a \cdot (b - c) = a \cdot b - a \cdot c$; $\forall a, b, c \in R: \; (a - b) \cdot c = a \cdot c - b \cdot c$
3. $(-a) \cdot b = a \cdot (-b) = -(a \cdot b)$; $(-a) \cdot (-b) = a \cdot b$
4. $(-a)^n = (-1)^n a = \begin{cases} a^n & n \text{ gerade} \\ -a^n & n \text{ ungerade} \end{cases}$ (*hierbei ist $(-1)^n$ in $\mathbb{Z}$ zu verstehen*)
5. *für $n, m \in \mathbb{Z}$, $a, b \in R$:* $(na) \cdot (mb) = (m \cdot n)(a \cdot b)$
6. *wenn R ein Einselement 1_R hat, dann ist* $\forall n \in \mathbb{Z}$, $a \in R$: $na = (n1_R) \cdot a = a \cdot (n1_R)$

7. *verallgemeinerte Distributivität:*

$$\left(\sum_{i=1}^{n} a_i\right)\left(\sum_{j=1}^{m} b_j\right) = \sum_{i=1}^{n}\sum_{j=1}^{m} a_i b_j \left(= \sum_{j=1}^{m}\sum_{i=1}^{n} a_i b_j\right)$$

$$\begin{aligned}(a_1 + \ldots + a_n) \cdot (b_1 + \ldots + b_m) &= (a_1 \cdot b_1 + \ldots a_1 \cdot b_m) + \ldots + (a_n \cdot b_1 + \ldots a_n \cdot b_m) \\ &= (a_1 \cdot b_1 + \ldots a_n \cdot b_1) + \ldots + (a_1 \cdot b_m + \ldots a_n \cdot b_m)\end{aligned}$$

Beweis:

1. $(a \cdot 0_R) = a \cdot (0_R + 0_R) = a \cdot 0_R + a \cdot 0_R$; durch Addition von $-(a \cdot 0_R)$ erhält man $0_R = a \cdot 0_R$. Analog folgt $0_R = 0_R \cdot a$.
Rest: als Übung.

□

Kapitel 17

Spezielle Elemente eines Ringes

Definition 17.1 Sei $(R, +, \cdot)$ ein Ring.

- $a \in R$ heißt *nilpotent*, wenn $\exists n \in \mathbb{N}$ mit $a^n = 0$.
- $b \in R$ heißt *Linksnullteiler*, wenn $\exists c \in R \setminus \{0\}$ mit $b \cdot c = 0$.
- $b \in R$ heißt *Rechtsnullteiler*, wenn $\exists c \in R \setminus \{0\}$ mit $c \cdot b = 0$.
- $b \in R$ heißt *Nullteiler*, wenn b Links- oder Rechtsnullteiler ist.

Bemerkung: 0 ist Nullteiler, sofern $R \neq \{0\}$.

Bemerkung: $a^n = 0$, d.h. a ist Nullteiler in einem Ring, ist nicht zu verwechseln mit $a^n = e$, d.h. a hat endliche Ordnung in einer Gruppe!

Bemerkung: In einem kommutativen Ring sind die Begriffe Linksnullteiler, Rechtsnullteiler und Nullteiler äquivalent (da $b \cdot c = c \cdot b$). Auch im Folgenden sind alle Eigenschaften, die links und rechts definiert werden, für kommutative Ringe äquivalent.

Proposition 17.2 Sei $R \neq \{0\}$. Dann gilt: a nilpotent $\Rightarrow$ a Nullteiler (Rechts- und Linksnullteiler).

Beweis: Sei $n \in \mathbb{N}$ minimal, sodass $a^n = 0$. Wenn $n = 1$, dann ist $a = 0$, also wegen $R \neq \{0\}$ ein Nullteiler. Wenn $n > 1$, dann gilt $0 = a^n = a \cdot a^{n-1} = a^{n-1} \cdot a$ und $a^{n-1} \neq 0$.

□

Beispiel: In $\mathbb{Z}_6$ sind $\overline{2}$ und $\overline{3}$ Nullteiler, denn $\overline{2} \cdot \overline{3} = \overline{3} \cdot \overline{2} = \overline{6} = \overline{0}$, aber $\overline{2}$ und $\overline{3}$ sind nicht nilpotent: $\overline{2}^n = \overline{2^n} = \overline{0}$ würde gelten, wenn $6|2^n$; dies ist jedoch unmöglich.

Definition 17.3 Sei $(R, +, \cdot)$ ein Ring mit Eins.

- $a \in R$ heißt *rechtsinvertierbar* (*Rechtseinheit*), wenn

$$\exists a_r \in R \text{ mit } a \cdot a_r = 1_R$$

- $a \in R$ heißt *linksinvertierbar* (*Linkseinheit*), wenn

$$\exists a_l \in R \text{ mit } a_l \cdot a = 1_R$$

a_r heißt dann Rechtsinverses von a, a_l Linksinverses.
a heißt *invertierbar* oder *Einheit*, wenn a links- und rechtsinvertierbar ist. In diesem Falle gibt es ein eindeutiges $a^{-1} \in R$, sodass $a \cdot a^{-1} = a^{-1} \cdot a = 1_R$ (siehe das entsprechende Resultat für Monoide).

Definition 17.4 Sei R ein Ring mit Eins. Dann ist

$$E(R) = R^* := \{a \in R \,|\, a \text{ invertierbar}\}$$

eine Gruppe, die *Einheitengruppe* von R (wir wissen bereits: die invertierbaren Elemente eines Monoids bilden eine Gruppe).

Beispiel: Sei K ein Körper, z.B. $K = \mathbb{R}$, V ein K-Vektorraum. Die Menge der Endomorphismen auf V,

$$\mathrm{End}_K(V) := \{L : V \to V \,|\, L(x+y) = L(x)+L(y), L(kx) = kL(x)\ \forall x, y \in V,\ k \in K\}$$

bildet einen Ring bezüglich der Operationen $+$, $\circ$.
In $\mathrm{End}_K(V)$ gilt:

1. L rechtsinvertierbar $\iff$ L surjektiv
2. L linksinvertierbar $\iff$ L injektiv

Beweis:

1. ($\Leftarrow$) Sei L surjektiv, B eine Basis von V. Für jedes $b \in B$ wähle $b' \in L^{-1}(b)$ $(\neq \emptyset)$; setze $\widetilde{L}(b) = b'$ für $b \in B$ ($\exists!$ lineare Abbildung $\widetilde{L} : V \to V$, die das erfüllt). Dann gilt $\forall b \in B$ $(L \circ \widetilde{L})(b) = L(b') = b$, also ist $L \circ \widetilde{L}$ eine lineare Abbildung, die auf einer Basis B $L \circ \widetilde{L} = \mathrm{id}$ erfüllt. Somit gilt $L \circ \widetilde{L} = \mathrm{id}$.
($\Rightarrow$) Wir wissen bereits: L hat (als Funktion) eine Rechtsinverse $\Rightarrow$ L ist surjektiv.

2. ($\Leftarrow$) Sei L injektiv, B eine Basis von V. Dann ist $B' = \{L(b) = b' \mid b \in B\}$ eine linear unabhängige Menge:
   Seien $b'_1 = L(b_1), \ldots, b'_n = L(b_n) \in B'$ und $c_1 b'_1 + \ldots + c_n b'_n = 0$. Dann folgt:

   $$0 = c_1 b'_1 + \ldots + c_n b'_n = c_1 L(b_1) + \ldots + c_n L(b_n) = L(c_1 b_1 + \ldots + c_n b_n)$$

   Da L injektiv ist, muss daher $c_1 b_1 + \ldots + c_n b_n = 0$ sein, also $c_i = 0 \; \forall i$, da B eine Basis ist. Folglich ist B' linear unabhängig.
   Nun kann man B' zu einer Basis C ergänzen und eine Funktion $\widetilde{L} : V \to V$ auf der Basis C definieren: für $b' \in B'$ sei $\widetilde{L}(b') = b$, wobei b das eindeutig bestimmte Element von B mit $L(b) = b'$ sei; für $c \in C \setminus B$ sei $\widetilde{L}(c)$ beliebig, z.B. $\widetilde{L}(c) = 0$. Dann folgt für $b \in B$ $\widetilde{L}(L(b)) = \widetilde{L}(b') = b$, also muss $\widetilde{L} \circ L = \mathrm{id}$ sein.
   ($\Rightarrow$) Wir wissen bereits: L hat (als Funktion) eine Linksinverse $\Rightarrow L$ ist injektiv.

□

Beispiel: Sei $(G, +)$ eine kommutative Gruppe, $f \in \mathrm{End}(G)$. Dann gilt: f linksinvertierbar in $(\mathrm{End}(G), +, \circ) \Rightarrow f$ ist injektiv. Die Umkehrung gilt jedoch nicht:
Wähle z.B. $G = (\mathbb{Z}, +)$, $f \in \mathrm{End}(\mathbb{Z})$ als $f(x) = 2x$. Dann ist f injektiv, hat aber keine Linksinverse: aus $g(f(x)) = x$ würde etwa für $x = 1$ folgen, dass $g(f(1)) = g(2) = g(1 + 1) = g(1) + g(1) = 1$ ist, was in den ganzen Zahlen unmöglich ist.

Definition 17.5 Sei $(R, +, \cdot)$ ein Ring.

- $a \in R$ heißt *linkskürzbar*, wenn $\forall b, c \in R \; ab = ac \Rightarrow b = c$.
- $a \in R$ heißt *rechtskürzbar*, wenn $\forall b, c \in R \; ba = ca \Rightarrow b = c$.

Proposition 17.6 Sei $(R, +, \cdot)$ ein Ring, $a \in R$. Dann gilt:

- (1) a linkskürzbar $\iff a$ kein Linksnullteiler
- (1') a rechtskürzbar $\iff a$ kein Rechtsnullteiler

Wenn R weiters ein Ring mit Eins ist, gilt:

- (2) a linksinvertierbar $\Longrightarrow a$ linkskürzbar
- (2') a rechtsinvertierbar $\Longrightarrow a$ rechtskürzbar

Beweis: (1), (1') als Übung.
(2) Sei a_l das Linksinverse von a, d.h. $a_l a = 1$; multipliziert man nun $ab = ac$ von links mit a_l, dann folgt $a_l ab = 1b = b = c = 1c = a_l ac$. (2') folgt analog.

□

Proposition 17.7 Sei $(R, +, \cdot)$ ein Ring, und für ein $a \in R$ sei $L_a : R \to R$ definiert durch $L_a(x) = a \cdot x$, $R_a : R \to R$ durch $R_a(x) = x \cdot a$. Dann gilt:

- (1) a rechtskürzbar $\iff$ R_a injektiv
- (1') a linkskürzbar $\iff$ L_a injektiv

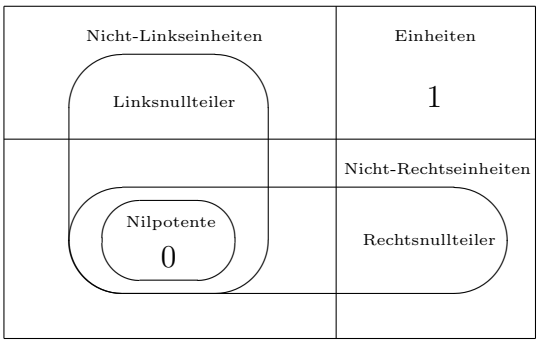
Wenn R weiters ein Ring mit Eins ist, gilt:

- (2) a Linkseinheit $\iff$ R_a surjektiv
- (2') a Rechtseinheit $\iff$ L_a surjektiv

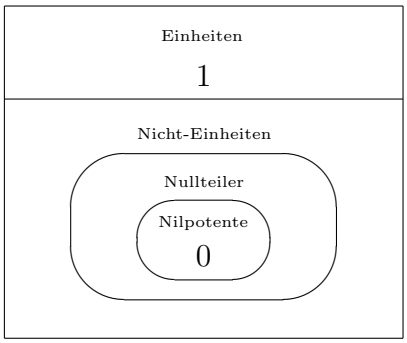
Beweis: (1), (1') als Übung.
(2) ($\Rightarrow$) $\exists a_l : \ a_l a = 1$; für $b \in R$ folgt damit $b = b1 = ba_l a = R_a(ba_l)$, also ist R_a surjektiv.
($\Leftarrow$) $\exists a' \in R$ mit $R_a(a') = 1$, d.h. $a'a = 1$. Damit ist a' Linksinverses von a.
(2') folgt analog.

□

Ring mit 1



Kommutativer Ring mit 1



Satz 17.8 *Sei R ein endlicher Ring mit Eins und $a \in R$. Dann gilt:*

1. *a ist Links- oder Rechtseinheit $\Longrightarrow$ a ist Einheit*
2. *a ist nicht Einheit $\Longrightarrow$ a ist Rechts- und Linksnullteiler.*

Beweis:

1. Sei a Linkseinheit. Dann ist a linkskürzbar, also L_a injektiv. Weil R endlich ist, muss L_a auch surjektiv sein. Damit ist a jedoch auch Rechtseinheit. Analog folgt, dass a Linkseinheit sein muss, wenn a Rechtseinheit ist.
2. Sei a keine Einheit, o.B.d.A. keine Linkseinheit. Dann ist R_a nicht surjektiv, und weil R endlich ist, ist R_a auch nicht injektiv. Daher ist a Rechtsnullteiler, also keine Rechtseinheit. Dann ist L_a nicht surjektiv und (weil R endlich ist) auch nicht injektiv. Damit muss a auch Linksnullteiler sein.

□

Beispiel: Sei $(G,+) = \prod_{n\in\mathbb{N}}(\mathbb{Z},+)$ und $R = \mathrm{End}(G)$. Definiere die Funktionen $f, g, h \in R$ durch

$$\begin{aligned} f((a_1,a_2,a_3,\ldots)) &= (a_2,a_4,a_6,\ldots) \\ g((a_1,a_2,a_3,\ldots)) &= (a_1,0,a_2,0,a_3,\ldots) \\ h((a_1,a_2,a_3,\ldots)) &= (0,a_1,0,a_2,0,\ldots) \end{aligned}$$

Dann gilt $f \circ g = 0$, also ist f Linksnullteiler (und g Rechtsnullteiler). Andererseits ist f jedoch rechtsinvertierbar, denn $f \circ h = \mathrm{id}$ (und g ist linksinvertierbar, denn für $k : (a_1,a_2,a_3,\ldots) \mapsto (a_1,a_3,a_5,\ldots)$ gilt $k \circ g = \mathrm{id}$).

Kapitel 18

Ideale

Definition 18.1 Sei R ein Ring und $S \subseteq R$. Wenn $(S, +)$ eine Untergruppe von $(R, +)$ ist und S bezüglich $\cdot$ abgeschlossen ist (d.h. $a, b \in S \Rightarrow ab \in S$), dann heißt S *Unterring* von S, geschrieben $S \leq R$.

Definition 18.2 Sei R ein Ring, $I \subseteq R$. Wenn $(I, +)$ eine Untergruppe von $(R, +)$ ist und $\forall i \in I, r \in R\ ir \in I$, dann heißt I *Rechtsideal* von R. Wenn $(I, +)$ eine Untergruppe von $(R, +)$ ist und $\forall i \in I, r \in R\ ri \in I$, dann heißt I *Linksideal* von R. Wenn I Links- und Rechtsideal ist, dann heißt I *Ideal* von R, geschrieben $I \trianglelefteq R$.

Bemerkung: Eine Untergruppe $(I, +) \leq (R, +)$ ist

- Unterring, wenn $a, b \in I \Rightarrow ab \in I$ (schwächste Bedingung)
- Linksideal, wenn $r \in R, b \in I \Rightarrow rb \in I$
- Rechtsideal, wenn $a \in I, r \in R \Rightarrow ar \in I$
- Ideal, wenn $r \in R, i \in I \Rightarrow ri \in I$ und $ir \in I$ (stärkste Bedingung)

Daher ist jedes Links- oder Rechtsideal Unterring, aber nicht umgekehrt. In einem kommutativen Ring ist jedes Linksideal auch Rechtsideal und umgekehrt. Jeder Ring hat die trivialen Ideale $\{0\}$ und R.

Bemerkung: Sei $I \subseteq R$. Wenn $I \neq \emptyset$, $a, b \in I \Rightarrow a - b \in I$ und $r \in R, i \in I \Rightarrow ri, ir \in I$ gilt, dann ist I ein Ideal.

Beispiel: Als Ideale von $(\mathbb{Z}, +, \cdot)$ kommen nur Untergruppen von $(\mathbb{Z}, +)$ in Frage, diese sind von der Form $\{0\}$ oder $n\mathbb{Z}$ für ein $n \in \mathbb{N}$. $n\mathbb{Z}$ ist auch ein Ideal: wenn $r \in \mathbb{Z}$ und $i = nl \in n\mathbb{Z}$ ist, dann ist $ri = ir = nrl \in n\mathbb{Z}$. Also sind die Ideale von $\mathbb{Z}$ $\{0\}$ und $n\mathbb{Z}$ $(n \in \mathbb{N})$.

BEISPIEL: $\mathbb{Z} \leq \mathbb{Q}$ ist ein Unterring, aber weder Links- noch Rechtsideal: $1 \in \mathbb{Z}, \frac{1}{2} \in \mathbb{Q}$, aber $1 \cdot \frac{1}{2} = \frac{1}{2} \notin \mathbb{Z}$.

BEISPIEL: Sei K ein Körper und $M_n(K)$ der Matrizenring über diesem Körper. Dann ist jedes Linksideal von der Form $\mathcal{L}_A := \{MA \mid M \in M_n(K)\}$ für eine Matrix $A \in M_n(K)$.
Ebenso ist jedes Rechtsideal von der Form $\mathcal{R}_B := \{BM \mid M \in M_n(K)\}$ für eine Matrix $B \in M_n(K)$.
Daher hat $M_n(K)$ nur die trivialen Ideale $\{0\}$ und $M_n(K)$ (Beweise als Übung).

Lemma 18.3 Sei R ein Ring und für $i \in I$ sei A_i ein Unterring (Rechtsideal/Linksideal/Ideal). Dann ist $\bigcap_{i \in I} A_i$ ein Unterring (Rechtsideal/Linksideal/Ideal).

Beweis: Wir wissen bereits, dass $(A_i, +) \leq (R, +) \Rightarrow (\bigcap_{i \in I} A_i, +) \leq (R, +)$. Wenn jedes A_i Unterring ist, also $\forall i \in I \ (r, s \in A_i \Rightarrow rs \in A_i)$ gilt, und $r, s \in \bigcap_{i \in I} A_i$ sind, dann ist $\forall i \in I \ r, s \in A_i$, also $\forall i \in I \ rs \in A_i$ und somit $rs \in \bigcap_{i \in I} A_i$. Daher ist A_i ein Unterring. Für Rechtsideal/Linksideale/Ideale läuft der Beweis analog.

□

Definition 18.4 Sei R ein Ring und $X \subseteq R$. Das von X *erzeugte Ideal* ist

$$(X) := \bigcap_{I \trianglelefteq R, X \subseteq I} I$$

Der von X *erzeugte Unterring* ist

$$[X] := \bigcap_{S \leq R, X \subseteq S} S$$

Weiters ist das von X erzeugte Linksideal $\bigcap_{I \text{ Linksideal}, X \subseteq I} I$, das von X erzeugte Rechtsideal $\bigcap_{I \text{ Rechtsideal}, X \subseteq I} I$.
Statt $(\{a\})$ schreibt man (a), statt $(\{a_1, \ldots, a_n\})$ schreibt man $(a_1, \ldots, a_n)$.
Ein Ideal der Form (a) für ein $a \in R$ heißt *Hauptideal* von R.

Satz 18.5 (Hauptideale) *Sei $(R, +, \cdot)$ ein Ring, $a \in R$. Dann gilt:*

1. $(a) = \{na + ra + as + \sum_{i=1}^{m} r_i a s_i \mid n \in \mathbb{Z}, r, s, r_i, s_i \in R, m \in \mathbb{N}_0\}$
2. *Für einen Ring mit Eins:* $(a) = \{\sum_{i=1}^{m} r_i a s_i \mid r_i, s_i \in R, m \in \mathbb{N}_0\}$
3. *Für einen kommutativen Ring:* $(a) = \{na + ra \mid n \in \mathbb{Z}, r \in R\}$

4. Für einen kommutativen Ring mit Eins: $(a) = \{ra \,|\, r \in R\}$

Beweis:

Ad 1.: Sei $M = \{na + ra + as + \sum_{i=1}^{m} r_i a s_i \,|\, n \in \mathbb{Z}, r, s, r_i, s_i \in R, m \in \mathbb{N}_0\}$. Dann gilt:

i. Für alle Ideale $I \trianglelefteq R$ mit $a \in I$ gilt $M \subseteq I$, denn: $(I, +) \leq (R, +) \Rightarrow na \in I$; I ist bezüglich Multiplikation von links und rechts abgeschlossen $\Rightarrow$ $ra, as, r_i a s_i \in I$; I ist bezüglich $+$ abgeschlossen $\Rightarrow$ jedes Element der Form $na + ra + as + \sum_{i=1}^{m} r_i a s_i$ muss in I enthalten sein, also $M \subseteq I$.

ii. M ist ein Ideal von M und $a \in M$:
Zweiteres ist unmittelbar klar, da $a = 1_{\mathbb{Z}} a + 0_R a + a 0_R + 0_R a 0_R \in M$. Damit ist außerdem $M \neq \emptyset$.
Es seien $na + ra + as + \sum_{i=1}^{m} r_i a s_i$ und $n'a + r'a + as' + \sum_{i=1}^{m'} r'_i a s'_i$ zwei Elemente aus M. Dann ist ihre Differenz

$$(n - n')a + (r - r')a + a(s - s') + \sum_{i=1}^{m+m'} r''_i a s''_i \in M$$

Seien weiters $b = na + ra + as + \sum_{i=1}^{m} r_i a s_i \in M$ und $r' \in R$. Dann ist ihr Produkt

$$\begin{aligned} r'b &= r'(na + ra + as + \sum_{i=1}^{m} r_i a s_i) \\ &= r'(na) + r'ra + ras + \sum_{i=1}^{m} r' r_i a s_i \\ &= (nr' + r'r)a + \sum_{i=1}^{m'} r'_i a s'_i \in M \end{aligned}$$

Analog ist auch $br' \in M$.

Wegen ii. kommt M unter den Idealen, die a enthalten, vor. Daher ist $(a) = \bigcap_{I \trianglelefteq R, a \in I} I \subseteq M$. Wegen i. wiederum muss $M \subseteq \bigcap_{I \trianglelefteq R, a \in I} I = (a)$ sein, also folgt $M = (a)$.

Ad 2.-4.: Die entsprechenden Mengen sind jedenfalls nach 1. in (a) enthalten. Sie umfassen jedoch aufgrund der zusätzlichen Bedingungen auch ganz (a):

- Ad 2.: R hat ein Einselement $\Rightarrow na = (n1_R)a1_R$, $ra = ra1_R$, $as = 1_R as$
- Ad 3.: R ist kommutativ $\Rightarrow as = sa$, $\sum_{i=1}^{m} r_i a s_i = (\sum_{i=1}^{m} r_i s_i)a$

- Ad 4.: R ist kommutativer Ring mit Einselement $\Rightarrow na = (n1_R)a$, $as = sa$, $\sum_{i=1}^{m} r_i a s_i = (\sum_{i=1}^{m} r_i s_i)a$

Daher ist $na + ra + as + \sum_{i=1}^{m} r_i a s_i$ jeweils von der angegebenen Form.

□

Definition 18.6 Sei R ein Ring und $A, B \subseteq R$. Dann definiert man:

$$AB := \{a_1 b_1 + \ldots + a_n b_n \,|\, n \in \mathbb{N}, a_i \in A, b_i \in B\}$$

$$A + B := \{a + b \,|\, a \in A, b \in B\}$$

Durch diese Definition ist AB bezüglich $+$ abgeschlossen.

BEMERKUNG: Statt $\{a\}B$ für ein $a \in R$ schreibt man aB, analog $Ab = A\{b\}$. Wegen der Distributivität gilt $aR = \{ar_1 + \ldots + ar_n \,|\, r_i \in R\} = \{ar \,|\, r \in R\}$ und analog $Ra = \{ra \,|\, r \in R\}$. In diesem Sinne ist dann für einen Ring mit Eins $(a) = RaR$ und für einen kommutativen Ring mit Eins $(a) = aR = Ra$.

Satz 18.7 *Seien $A_1, \ldots, A_n, A, B, C$ Ideale (Linksideale/Rechtsideale). Dann sind auch $A_1 + \ldots + A_n$ und AB Ideale (Linksideale/Rechtsideale), und es gilt:*

1. $A + (B + C) = (A + B) + C$
2. $A(BC) = (AB)C$
3. $A(B + C) = AB + AC$, $(A + B)C = AC + BC$
4. $(A_1 + \ldots + A_n)B = A_1B + \ldots + A_nB$, $B(A_1 + \ldots + A_n) = BA_1 + \ldots + BA_n$
5. *Wenn R ein Ring mit Eins ist, dann gilt für alle Linksideale I von R $RI = I$ und für alle Rechtsideale J von R $JR = J$.*

Beweis: als Übung.

Kapitel 19

Homomorphismen

Definition 19.1 Seien R, S Ringe. Eine Funktion $R \to S$ heißt *Ringhomomorphismus*, wenn $\forall a, b \in R\ f(a+b) = f(a) + f(b)$ und $f(ab) = f(a)f(b)$.

Definition 19.2 Der *Kern* eines Ringhomomorphismus $f : R \to S$ ist definiert als

$$\operatorname{Ker} f := \{a \in R \,|\, f(a) = 0_S\} = f^{-1}(0_S)$$

Das *Bild* von f wiederum ist

$$\operatorname{Im} f := \{f(a) \,|\, a \in R\}$$

Definition 19.3 Ein surjektiver Ringhomomorphismus heißt – wie für Gruppen – *Epimorphismus*, ein injektiver *Monomorphismus*, ein bijektiver *Isomorphismus*, einer, der R auf sich abbildet, *Endomorphismus*, und ein bijektiver Endomorphismus heißt *Automorphismus*.

Satz 19.4 *Sei $(R, +, \cdot)$ ein Ring und $I \trianglelefteq R$. Für $a \in R$ sei $a+I := \{a+i \,|\, i \in I\} = \{b \in R \,|\, b - a \in I\}$ (die Nebenklasse von a bezüglich $(I, +) \leq (R, +)$) und $R/I := \{a + I \,|\, a \in R\}$.*
Dann bildet R/I mit der Addition $(a + I) + (b + I) = (a + b) + I$ und der Multiplikation $(a + I) \cdot (b + I) = (a \cdot b) + I$ einen Ring.
Wenn R kommutativ ist, dann auch R/I; wenn R ein Ring mit einem Einselement 1_R ist, dann ist $1_R + I$ das Einselement von R/I. Weiters ist $\pi : R \to R/I$ mit $\pi(a) = a + I$ ein Ringepimorphismus (die kanonische Projektion) mit $\operatorname{Ker} \pi = I$.

Beweis: Wir wissen bereits, dass $(R/I, +)$ eine kommutative Gruppe ist. Zu zeigen ist zunächst, dass $(R/I, \cdot)$ eine Halbgruppe ist und das Distributivgesetz erfüllt ist:

- $\cdot$ ist wohldefiniert: sei $a+I=a'+I$, $b+I=b'+I$, d.h. $a-a'=i\in I$ und $b-b'=j\in I$. Dann ist $a'b'-ab=(a+i)(b+j)-ab=ab+aj+ib+ij-ab=aj+ib+ij\in I$, also $a'b'+I=ab+I$.
- Die Assoziativität von $\cdot$ und die Distributivität ergeben sich aus den entsprechenden Bedingungen für R. Ebenso ist R/I kommutativ, wenn R kommutativ ist. Falls R ein Einselement hat, ist $(a+I)(1+I)=a1+I=a+I=1a+I=(1+I)(a+I)$, also muss $1+I$ Einselement in R/I sein.

Es ist bereits bekannt, dass $\pi: R\to R/I$ ein Gruppenepimorphismus bezüglich $+$ ist, wobei $\operatorname{Ker}\pi=I$. Weil zudem $\pi(ab)=ab+I=(a+I)(b+I)=\pi(a)\pi(b)$ gilt, ist π auch Ringhomomorphismus.

Satz 19.5 (Homomorphiesatz, 1. Isomorphiesatz) *Sei $f: R\to S$ ein Ringhomomorphismus. Dann ist* $\operatorname{Ker} f$ *ein Ideal von R,* $\operatorname{Im} f$ *ein Unterring von S und $\overline{f}: R/(\operatorname{Ker} f)\to \operatorname{Im} f$ mit $\overline{f}(a+\operatorname{Ker} f)=f(a)$ ein Ringisomorphismus.*

Beweis: $\operatorname{Ker} f\leq (R,+)$, weil f ein Gruppenhomomorphismus bezüglich $+$ ist. Sei nun $k\in\operatorname{Ker} f$ und $a\in R$. Dann gilt:

$$f(ak)=f(a)f(k)=f(a)\cdot 0=0\ \Rightarrow ak\in\operatorname{Ker} f$$

$$f(ka)=f(k)f(a)=0\cdot f(a)=0\ \Rightarrow ka\in\operatorname{Ker} f$$

Daher ist $\operatorname{Ker} f$ ein Ideal von R.
$\operatorname{Im} f$ ist eine Untergruppe von $(S,+)$ und abgeschlossen bezüglich $\cdot$, da für $a=f(\alpha), b=f(\beta)\in\operatorname{Im} f$ $ab=f(\alpha\beta)\in\operatorname{Im} f$ ist. Daher ist $\operatorname{Im} f$ tatsächlich Unterring.
Nun betrachten wir die Funktion $\overline{f}: R/K\to\operatorname{Im} f$, wobei $K=\operatorname{Ker} f$ sei:

- $\overline{f}$ ist wohldefiniert: $a'\in a+K\ \Rightarrow\ a'=a+k$ für ein $k\in K\ \Rightarrow\ f(a')=f(a)+f(k)=f(a)+0=f(a)$
- $\overline{f}$ ist offensichtlich surjektiv, und zudem auch injektiv: $\overline{f}(a+K)=\overline{f}(b+K)\ \Rightarrow f(a)=f(b)\ \Rightarrow f(a-b)=0\ \Rightarrow a-b\in K\ \Rightarrow\ a+K=b+K$
- $\overline{f}$ ist Ringhomomorphismus:

$$\overline{f}((a+K)+(b+K))=\overline{f}(a+b+K)=f(a+b)=f(a)+f(b)=\overline{f}(a+K)+\overline{f}(b+K)$$

$$\overline{f}((a+K)(b+K))=\overline{f}(ab+K)=f(ab)=f(a)f(b)=\overline{f}(a+K)\overline{f}(b+K)$$

□

BEISPIEL: $n\mathbb{Z} \trianglelefteq \mathbb{Z}$; $\pi : \mathbb{Z} \to \mathbb{Z}/(n\mathbb{Z}) = \mathbb{Z}_n$ mit $\pi(m) = \overline{m} = m + \mathbb{Z}$ ist auch Ringepimorphismus.

BEMERKUNG: Sei S Unterring von R und $I \trianglelefteq R$. Dann ist $S \cap I \trianglelefteq S$ (die Einschränkung von I auf S).

Satz 19.6 (2. Isomorphiesatz) *Sei R ein Ring, S ein Unterring von R und I ein Ideal von R. Dann gilt*

$$S/(S \cap I) \simeq (I + S)/I$$

wobei $\varphi : S/(S \cap I) \to (I + S)/I$ mit $\varphi(s + S \cap I) = s + I$ der Isomorphismus ist.

Beweis: Wir wissen bereits, dass φ ein Gruppenisomorphismus bezüglich $+$ ist. Wegen $\varphi((s+S\cap I)(t+S\cap I)) = \varphi(st+S\cap I) = st+I = (s+I)(t+I) = \varphi(s + S \cap I)\varphi(t + S \cap I)$ ist φ jedoch auch Ringisomorphismus.

□

Proposition 19.7 Sei $f : R \to S$ ein Ringhomomorphismus. Dann gilt:

- $R' \leq R \;\Rightarrow\; f(R') \leq S$
- $S' \leq S \;\Rightarrow\; f^{-1}(S') \leq R$
- $R' \trianglelefteq R \;\Rightarrow\; f(R') \trianglelefteq f(R)$ (im Allgemeinen aber nicht $f(R') \trianglelefteq S$!)
- $S' \trianglelefteq S \;\Rightarrow\; f^{-1}(S') \trianglelefteq R$

Beweis: als Übung.

Lemma 19.8 Sei $f : R \to S$ ein Ringhomomorphismus. Dann gilt:

$$X \subseteq R \implies f^{-1}(f(X)) = X + \operatorname{Ker} f$$

$$Y \subseteq S \implies f(f^{-1}(Y)) = Y \cap \operatorname{Im} f$$

Beweis: Dies gilt bereits, weil f ein Gruppenhomomorphismus bezüglich $+$ ist (Lemma 9.4).

Definition 19.9 Für $I \trianglelefteq R$ ist $[R : I] = |R/I| = |\{a + I \,|\, a \in R\}|$ der *Index* von I (d.h. der Index der Untergruppe $(I, +)$ von $(R, +)$).

Satz 19.10 (Korrespondenzsatz) *Seien R, S Ringe, $f : R \to S$ ein Ringepimorphismus (also surjektiv) und $K := \operatorname{Ker} f$. Seien weiters*

$$\mathcal{R}_K(R) := \{A \mid A \leq R, K \subseteq A\}$$

$$\mathcal{R}(S) := \{B \mid B \leq S\}$$

$$\mathcal{I}_K(R) := \{I \mid I \trianglelefteq R, K \subseteq I\}$$

$$\mathcal{I}(S) := \{J \mid J \trianglelefteq S\}$$

Dann gilt:

1. *$\varphi : \mathcal{R}_K(R) \to \mathcal{R}(S)$ mit $\varphi(A) = f(A)$ ist eine Bijektion mit der Inversen $\psi : \mathcal{R}(S) \to \mathcal{R}_K(R)$ mit $\psi(B) = f^{-1}(B)$ und $\varphi|_{\mathcal{I}_K(R)} : \mathcal{I}_K(R) \to \mathcal{I}(S)$ ist eine Bijektion mit der Inversen $\psi|_{\mathcal{I}(S)} : \mathcal{I}(S) \to \mathcal{I}_K(R)$.*

2. *$\forall A, C \in \mathcal{R}_K(R) : A \trianglelefteq C \;\Leftrightarrow\; f(A) \trianglelefteq f(C)$, und falls $A \trianglelefteq C$ ist, dann $C/A \simeq f(C)/f(A)$.*

Beweis:

1. $A \leq R \;\Rightarrow f(A) \leq S$; $B \leq S \;\Rightarrow f^{-1}(B) \leq R$ mit $K = f^{-1}(0) \subseteq f^{-1}(B)$, da $0 \in B$. Also sind φ und ψ Funktionen.
   Sei nun $A \in \mathcal{R}_K(R)$: dann ist

   $$\psi(\varphi(A)) = f^{-1}(f(A)) = A + \operatorname{Ker} f = A \text{ (da } \operatorname{Ker} f \subseteq A)$$

   Sei andererseits $B \in \mathcal{R}(S)$: dann ist

   $$\varphi(\psi(B)) = f(f^{-1}(B)) = B \cap \operatorname{Im} f = B \text{ (da } f \text{ surjektiv ist)}$$

   Daher sind φ und ψ invers zueinander und somit bijektiv.
   $I \in \mathcal{I}_K(R) \;\Rightarrow\; f(I) \trianglelefteq \operatorname{Im} f = S$; $J \in \mathcal{I}(S) \;\Rightarrow\; f^{-1}(J) \trianglelefteq R$, also sind $\varphi|_{\mathcal{I}_K(R)}$ und $\psi|_{\mathcal{I}(S)}$ Funktionen. Sie sind invers zueinander, weil φ und ψ es sind.

2. Für $A \trianglelefteq C$ sei $g = f|_C : C \to f(C)$. Dann ist g ein Ringepimorphismus, und man kann 1. anwenden. Es folgt $A \trianglelefteq C \;\Rightarrow\; f(A) \trianglelefteq f(C)$.
   Sei dann $h : C/A \to f(C)/f(A)$ durch $h(c+A) = f(c)+f(A)$ gegeben.

   - h ist wohldefiniert: seien $c, c' \in C$ mit $c+A = c'+A \;\Leftrightarrow\; c-c' \in A$. Dann ist $f(c) - f(c') = f(c-c') \in f(A)$ und daher $f(c)+f(A) = f(c')+f(A)$.

- h ist ein Ringhomomorphismus:

$$\begin{aligned} h((c+A)+(d+A)) &= h((c+d)+A) \\ &= f(c+d)+f(A) \\ &= f(c)+f(d)+f(A) \\ &= (f(c)+f(A))+(f(d)+f(A)) \\ &= h(c+A)+h(d+A) \end{aligned}$$

und

$$\begin{aligned} h((c+A)\cdot(d+A)) &= h(cd+A) \\ &= f(cd)+f(A) \\ &= f(c)f(d)+f(A) \\ &= (f(c)+f(A))(f(d)+f(A)) \\ &= h(c+A)\cdot h(d+A) \end{aligned}$$

- h ist injektiv: $c+A \in \operatorname{Ker} h \Rightarrow f(c)+f(A)=f(A)$, d.h. $f(c) \in f(A)$. Es muss also ein $a \in A$ geben, sodass $f(c)=f(a)$ ist. Es folgt $f(a-c)=0$, also $c-a \in \operatorname{Ker} f \subseteq A$ und somit wegen $a \in A$ auch $c \in A$. Also besteht der Kern von h nur aus dem neutralen Element $0+A$.
- h ist klarerweise surjektiv.

Also ist h ein Ringisomorphismus, und es gilt $C/A \simeq f(C)/f(A)$.
Seien umgekehrt A, C beliebige Unterringe von R und $f(A) \trianglelefteq f(C)$. Dann ist $f(A) \subseteq f(C)$, also $A = A + \operatorname{Ker} f = f^{-1}(f(A)) \subseteq C + \operatorname{Ker} f = C$ und folglich $A \leq C$. Wendet man nun wiederum 1. auf den Ringepimorphismus $g : C \to f(C)$ an, ergibt sich aus $f(A) = g(A) \trianglelefteq g(C) = f(C)$ sofort $A \trianglelefteq C$.

□

Satz 19.11 (3. Isomorphiesatz) *Sei R ein Ring und I ein Ideal von R. Definiere*

$$\mathcal{R}_I(R) := \{S \leq R \mid I \subseteq S\}$$
$$\mathcal{I}_I(R) := \{J \trianglelefteq R \mid I \subseteq J\}$$
$$\mathcal{R}(R/I) := \{S' \leq R/I\}$$
$$\mathcal{I}(R/I) := \{J' \trianglelefteq R/I\}$$

Dann ist $\varphi : \mathcal{R}_I(R) \to \mathcal{R}(R/I)$ *mit* $\varphi(S) = S/I = \{s + I \,|\, s \in S\}$ *eine Bijektion, und für* $J \leq R$ *mit* $I \subseteq J$ *gilt* $J \trianglelefteq R \Leftrightarrow J/I \trianglelefteq R/I$.
Außerdem gilt für $I \trianglelefteq R$, $J \trianglelefteq R$ *mit* $I \subseteq J$*:*

$$R/J \simeq (R/I)/(J/I)$$

Beweis: Dies ist lediglich der Korrespondenzsatz, angewandt auf den Ringepimorphismus $\pi : R \to R/I$ mit $\pi(r) = r + I$. Für $S \leq R$ mit $I \subseteq S$ ist $\pi(S) = \{s + I \,|\, s \in S\} = S/I$.

Korollar 19.12 Jedes Ideal von R/I hat die Form J/I für ein $J \trianglelefteq R$, $I \subseteq J$.

Kapitel 20

Charakteristik

Definition 20.1 Sei R ein Ring. Wenn $\{n \in \mathbb{N} \mid \forall r \in R\ nr = 0\} = \emptyset$, dann definiere $\chi(R) := 0$, andernfalls

$$\chi(R) := \min\{n \in \mathbb{N} \mid \forall r \in R\ nr = 0\}$$

$\chi(R)$ heißt *Charakteristik* von R.

Beispiel: $\chi(\mathbb{Z}) = 0$, $\chi(\mathbb{Z}_n) = n$, $\chi(M_n(\mathbb{Q})) = 0$, $\chi(M_n(\mathbb{Z}_p)) = p$

Proposition 20.2 Wenn R ein Ring mit Eins ist, dann ist $\chi(R) = 0$, falls $\{n \in \mathbb{N} \mid n1_R = 0_R\} = \emptyset$, andernfalls ist $\chi(R) = \min\{n \in \mathbb{N} \mid n1_R = 0_R\}$.

Beweis: als Übung.

Definition 20.3 Ein Ring R heißt *nullteilerfrei*, wenn R außer 0 keine Nullteiler enthält, d.h. wenn $\forall a, b \in R$ gilt: $ab = 0 \ \Rightarrow\ a = 0 \vee b = 0$.

Bemerkung: R ist nullteilerfrei $\Rightarrow$ jedes $a \neq 0$ ist links- und rechtskürzbar: $ab = ac \ \Rightarrow a(b - c) = 0 \ \Rightarrow a = 0 \vee b = c$

Proposition 20.4 Wenn R ein nullteilerfreier Ring ist, dann ist $\chi(R) = 0$ oder $\chi(R) = p$ eine Primzahl.

Beweis: Angenommen, $\chi(R)$ wäre weder 0 noch eine Primzahl. Dann ist $\chi(R) = nm$ für $n, m \in \mathbb{N}$, $n, m > 1$.
Weil $\chi(R) \neq 0$ ist, ist $\chi(R) = \min\{k \in \mathbb{N} \mid \forall r \in R\ kr = 0\}$. Wegen $m > 1$ ist $n < nm = \chi(R) = \min\{k \in \mathbb{N} \mid \forall r \in R\ kr = 0\}$, daher gibt es ein $r \in R$, sodass $nr \neq 0$ ist, und ebenso ein $s \in R$, sodass $ms \neq 0$ ist. Es gilt jedoch $(nr)(ms) = (nm)(rs) = \chi(R)(rs) = 0$, also müsste R Nullteiler haben, ein Widerspruch.

□

Definition 20.5 Sei R ein Ring mit Eins. Der von 1 erzeugte Unterring von R heißt *Primring* von R, $\Pi_R := \bigcap_{S \leq R, 1 \in S} S$.

Satz 20.6 *Sei R ein Ring mit Eins. Dann gilt*

1. $\Pi_R = \{n1_R \,|\, n \in \mathbb{Z}\}$
2. *Wenn $\chi(R) = 0$, dann ist $\Pi_R \simeq \mathbb{Z}$, wenn $\chi(R) = n \in \mathbb{N}$, dann ist $\Pi_R \simeq \mathbb{Z}_n$.*

Beweis:

1. $\{n1_R \,|\, n \in \mathbb{Z}\} = \bigcap_{(H,+) \leq (R,+), 1 \in H} H \subseteq \bigcap_{S \leq R, 1 \in S} S = \Pi_R$ (da jeder Unterring von R auch Untergruppe bezüglich + ist).
   Zudem ist $G = \{n1_R \,|\, n \in \mathbb{Z}\}$ ein Ring, denn G ist bezüglich $\cdot$ abgeschlossen: $(n1_R)(m1_R) = (nm)(1_R 1_R) = (nm)1_R \in G$ (dass G bezüglich + eine Gruppe bildet, ist bereits bekannt). Daher ist G ein Unterring von R mit $1 \in G$, also $\Pi_R = \bigcap_{S \leq R, 1 \in S} \subseteq G$ und insgesamt folglich $\Pi_R = G$.

2. $\varphi : \mathbb{Z} \to R$, definiert durch $\varphi(n) = n1_R$, ist ein Ringhomomorphismus, denn $\varphi(n+m) = (n+m)1_R = n1_R + m1_R = \varphi(n) + \varphi(m)$ und $\varphi(nm) = nm1_R = (n1_R)(m1_R) = \varphi(n)\varphi(m)$. $\operatorname{Im}\varphi = \{n1_R \,|\, n \in \mathbb{Z}\} = \Pi_R$ und $\operatorname{Ker}\varphi = \{n \in \mathbb{Z} \,|\, n1_R = 0\}$.
   Ist $\chi(R) = 0$, dann existiert kein $n \in \mathbb{N}$ mit $n1_R = 0$. In diesem Fall ist $\operatorname{Ker}\varphi = \{0\}$ und somit $\Pi_R = \operatorname{Im}\varphi \simeq \mathbb{Z}/\{0\} = \mathbb{Z}$.
   Ist andererseits $\chi(R) = m \in \mathbb{N}$, dann ist $\operatorname{Ker}\varphi = m\mathbb{Z}$ und somit $\Pi_R = \operatorname{Im}\varphi \simeq \mathbb{Z}/(m\mathbb{Z}) = \mathbb{Z}_m$.

□

Definition 20.7 (Binomialkoeffizienten) Für $n \in \mathbb{N}_0$, $k \in \mathbb{Z}$ sei

$$\binom{n}{k} := \text{ Anzahl aller } k\text{-elementigen Teilmengen einer } n\text{-elementigen Menge}$$

Bemerkung: $\binom{0}{0} = 1$, denn $\emptyset$ hat genau eine 0-elementige Teilmenge; $\binom{n}{k} = 0$ für $k < 0$ und für $k > n$.

Proposition 20.8 Für $n \in \mathbb{N}$, $k \in \mathbb{Z}$ gilt

1. $\binom{n}{k} = \frac{n!}{k!(n-k)!}$
2. $\binom{n+1}{k} = \binom{n}{k-1} + \binom{n}{k}$

3. $\binom{n}{0} = \binom{n}{n} = 1$, $\binom{n}{k} = \binom{n}{n-k}$

4. Ist p eine Primzahl und $0 < k < p$, dann gilt $p \mid \binom{p}{k}$.

Beweis:

1. Man kann eine beliebige k-elementige Teilmenge einer n-elementigen Menge $\{a_1, \ldots, a_n\}$ auswählen, indem man die Elemente in einer beliebigen Reihenfolge anschreibt (dafür gibt es $n!$ Möglichkeiten) und die ersten k auswählt. Dabei kommt dieselbe Menge je $k!(n-k)!$ Mal vor, denn jede Reihenfolge der ersten k (dafür gibt es $k!$ Möglichkeiten) und der letzten $n-k$ (dafür gibt es $(n-k)!$ Möglichkeiten) Elemente führt zu denselben k ausgewählten Elementen. Also gibt es $\frac{n!}{k!(n-k)!}$ k-elementige Teilmengen einer n-elementigen Menge.

2. als Übung

3. Offensichtlich gibt es je genau eine Teilmenge der Mächtigkeit 0 bzw. n. Weiters ist durch $T \mapsto M/T$ eine Bijektion zwischen den k-elementigen und den $(n-k)$-elementigen Teilmengen von M (mit $|M| = n$) gegeben.

4. Es ist

$$\binom{p}{k} = \frac{p(p-1)\cdot\ldots\cdot 1}{k(k-1)\cdot\ldots\cdot 1\cdot(n-k)(n-k-1)\cdot\ldots\cdot 1}$$

   Da p den Zähler, aber nicht den Nenner teilt, muss $p \mid \binom{n}{k}$ gelten.

□

Satz 20.9 (Binomischer Lehrsatz) *Sei R ein Ring und $a, b \in R$ mit $ab = ba$. Für $n \in \mathbb{N}$ sei $a^0 b^n := b^n$ und $a^n b^0 := a^n$ (auch wenn R kein Einselement hat). Dann gilt für $n \in \mathbb{N}$:*

$$(a+b)^n = \sum_{k=0}^{n} \binom{n}{k} a^k b^{n-k}$$

Beweis: Entwickelt man $(a+b)^n = (a+b)\ldots(a+b)$ mit dem Distributivgesetz, so erhält man wegen $ab = ba$ nur Summanden der Form $a^k b^{n-k}$ (da es n Faktoren gibt, erhält man beim Ausmultiplizieren wiederum nur Glieder mit n Faktoren).

Dabei kommt ein Faktor $a^k b^{n-k}$ sooft vor, wie es Möglichkeiten gibt, jene k Faktoren auszuwählen, aus denen ein a stammt (bzw. $n-k$ Faktoren, aus denen ein b stammt). Dafür gibt es nach der vorhergehenden Definition genau $\binom{n}{k}$ Möglichkeiten, womit die Behauptung folgt.

□

Proposition 20.10 Sei R ein kommutativer Ring, sodass $\chi(R) = p$ eine Primzahl ist. Dann ist $\varphi : R \to R$, gegeben durch $\varphi(x) = x^p$, ein Ringhomomorphismus (der *Frobenius-Homomorphismus*).

Beweis:

- $\varphi(xy) = (xy)^p = x^p y^p = \varphi(x)\varphi(y)$ gilt aufgrund der Kommutativität von R.
- Es ist

$$\begin{aligned}
\varphi(x+y) &= (x+y)^p \\
&= \sum_{k=0}^{p} \binom{p}{k} x^k y^{p-k} \\
&= \binom{p}{0} x^0 y^p + \ldots + \binom{p}{p} x^p y^0 \\
&= \binom{p}{0} x^0 y^p + \binom{p}{p} x^p y^0 = y^p + x^p \\
&= \varphi(x) + \varphi(y)
\end{aligned}$$

  weil wegen $p \mid \binom{p}{k}$ für $0 < k < p$ und $\chi(R) = p$ alle übrigen Summanden $\binom{p}{k} x^k y^{p-k} = m(p(x^k y^{p-k})) = m0 = 0$ wegfallen.

□

Korollar 20.11 Sei R ein kommutativer Ring mit $\chi(R) = p$ für eine Primzahl p. Dann gilt $\forall a, b \in R, n \in \mathbb{N}$: $(a+b)^{p^n} = a^{p^n} + b^{p^n}$

Beweis: $\varphi : R \to R$ mit $\varphi(x) = x^p$ ist ein Homomorphismus, daher auch $\varphi \circ \ldots \circ \varphi = \varphi^n$, und es ist $\varphi^n(x) = (((x^p)^p)\ldots)^p = x^{p^n}$. Also muss $(a+b)^{p^n} = \varphi^n(a+b) = \varphi^n(a) + \varphi^n(b) = a^{p^n} + b^{p^n}$ sein.

□

Kapitel 21

Adjunktion der Eins

Satz 21.1 (Adjunktion der Eins) *Sei R ein Ring.*

1. *Dann gibt es einen Ring S mit Einselement, sodass $\chi(S) = 0$ und $R \leq S$ ist, nämlich $S = \mathbb{Z} \times R$ mit der Addition $(k, r)+(k', r') = (k+k', r+r')$ und der Multiplikation $(k, r) \cdot (k', r') = (kk', kr' + k'r + rr')$.*

2. *Wenn $\chi(R) = n \in \mathbb{N}$ ist und m ein Vielfaches von n, dann gibt es einen Ring S mit Einselement, sodass $\chi(S) = m$ und $R \leq S$ ist, nämlich $S = \mathbb{Z}_m \times R$ mit der Addition $(\overline{k}, r) + (\overline{k'}, r') = (\overline{k + k'}, r + r')$ und der Multiplikation $(\overline{k}, r) \cdot (\overline{k'}, r') = (\overline{kk'}, kr' + k'r + rr')$.*

Beweis:

1.
   - S ist eine kommutative Gruppe, denn $(S, +) = (\mathbb{Z}, +) \oplus (R, +)$.
   - $\cdot$ ist assoziativ:

$$\begin{aligned}(k_1, r_1)((k_2, r_2)(k_3, r_3)) &= (k_1, r_1)(k_2k_3, k_2r_3 + k_3r_2 + r_2r_3) \\ &= (k_1k_2k_3, k_1k_2r_3 + k_1k_3r_2 + k_1r_2r_3 + \\ &\quad k_2k_3r_1 + k_2r_1r_3 + k_3r_1r_2 + r_1r_2r_3) \\ &= (k_1k_2, k_1r_2 + k_2r_1 + r_1r_2)(k_3, r_3) \\ &= ((k_1, r_1)(k_2, r_2))(k_3, r_3)\end{aligned}$$

   - Das Distributivitätsgesetz ergibt sich ebenso durch direktes Nachrechnen.
   - $(1, 0)$ ist Einselement: $(1, 0)(k, r) = (k, 1r + k0 + 0r) = (k, r)$ und $(k, r)(1, 0) = (k, k0 + 1r + r0) = (k, r)$.
   - R ist ein Unterring vermöge der Einbettung $\varphi : R \to S$ mit $\varphi(r) = (0, r)$: es gilt $\varphi(r + s) = (0, r + s) = (0, r) + (0, s) = \varphi(r) + \varphi(s)$ und $\varphi(rs) = (0, rs) = (0, 0r + 0s + rs) = (0, r)(0, s) = \varphi(r)\varphi(s)$. φ ist daher ein Ringhomomorphismus und offensichtlich injektiv.

- $\chi(S) = 0$, denn aus $n(k,r) = (0,0)$ folgt für $k = 1$ sofort $n = 0$. Also kann es kein $n \in \mathbb{N}$ geben, sodass $n(k,r) = (0,0)$ für alle Elemente von S gilt.

2.
- Die Multiplikation ist wohldefiniert: seien k, k' Repräsentanten von $\overline{k}$, d.h. $\overline{k} = \overline{k'}$ Dann gilt $m|k - k'$ und somit

$$\begin{aligned}(\overline{k},r)(\overline{l},s) &= (\overline{kl}, ks + lr + rs)\\ &= (\overline{k'l}, k's + (k-k')s + lr + rs)\\ &= (\overline{k'l}, k's + lr + rs)\\ &= (\overline{k'}, r)(\overline{l}, s)\end{aligned}$$

  weil wegen $\chi(R) = n \,|\, m \,|\, (k - k')\ (k - k')s = 0$ sein muss.

- $m(\overline{k}, r) = (m\overline{k}, mr) = (0,0)$ für alle Elemente $(\overline{k}, r)$ von S, weil wegen $\overline{k} \in \mathbb{Z}_m$ $m\overline{k} = 0$ und wegen $\chi(R) = n \,|\, m$ $mr = 0$ sein muss. Andererseits ist für alle $l \in \mathbb{N}$ mit $l < m$ $l(\overline{1}, 0) = (\overline{l}, 0) \neq (0,0)$, weswegen

$$m = \min\{l \in \mathbb{N} \,|\, \forall s \in S\ ls = 0\} = \chi(S)$$

  sein muss.

- Der Rest läuft analog zu 1. ab.

□

Bemerkung: Auch wenn R nullteilerfrei ist, kann S nichttriviale Nullteiler haben. Man betrachte als Beispiel etwa die Adjunktion der Eins an $R = 2\mathbb{Z}$: Dann ist $S = \mathbb{Z}\times 2\mathbb{Z}$, und es gilt die Multiplikation $(k, 2n)(l, 2m) = (kl, 2km + 2ln + 4nm)$. Daher ist

$$(0,2)(-2,2) = (0 \cdot (-2), 0 \cdot 2 + 2 \cdot (-2) + 2 \cdot 2) = (0,0)$$

Also hat S die nichttrivialen Nullteiler $(0,2)$ und $(-2,2)$.

Kapitel 22

Primideale, maximale Ideale

Definition 22.1 Sei R ein Ring und $P \trianglelefteq R$. P heißt *Primideal*, wenn $P \neq R$ und $\forall A, B \trianglelefteq R$ gilt: $AB \subseteq P \;\Rightarrow\; A \subseteq P \vee B \subseteq P$.

Lemma 22.2 Sei R ein Ring und $a, b \in R$. Dann gilt $(ab) \subseteq (a)(b)$. Wenn R kommutativ ist, gilt sogar $(ab) = (a)(b)$.

Beweis: als Übung.

Satz 22.3 *Sei R ein Ring, $P \trianglelefteq R$ und $P \neq R$. Wenn P die Eigenschaft hat, dass $\forall a, b \in R$ $(ab \in P \;\Rightarrow\; a \in P \vee b \in P)$ gilt, dann ist P ein Primideal. Wenn R kommutativ ist und $P \trianglelefteq R$, dann ist P genau dann Primideal, wenn diese Bedingung erfüllt ist.*

Beweis: P habe die oben genannte Eigenschaft. Seien dann $A, B \trianglelefteq R$ Ideale mit $AB \subseteq P$. Angenommen, $A \nsubseteq P$. Dann wähle ein $a_0 \in A$, das nicht in P liegt. Für alle $b \in B$ muss dann gelten:

$$a_0 b \in AB \subseteq P \;\Rightarrow\; a_0 \in P \vee b \in P \;\Rightarrow\; b \in P$$

Also ist $B \subseteq P$. Analog folgt $B \nsubseteq P \;\Rightarrow\; A \subseteq P$.
Sei jetzt P ein Primideal in einem kommutativen Ring. Wenn $ab \in P$ ist, dann muss $(a)(b) = (ab) \subseteq P$ und somit $(a) \subseteq P$ oder $(b) \subseteq P$ sein. Daraus folgt jedoch insbesondere $a \in P \vee b \in P$.

□

Bemerkung: Für nichtkommutative Ringe gilt nicht $(ab) \subseteq P \;\Rightarrow\; (a)(b) \subseteq P$, weil im Allgemeinen $(ab) \subsetneq (a)(b)$ ist.

Definition 22.4 Ein Ring $R \neq \{0\}$ heißt *Integritätsbereich*, wenn R kommutativer Ring mit Eins und nullteilerfrei ist.

BEISPIEL: $(\mathbb{Z}, +, \cdot)$ ist Integritätsbereich.

Lemma 22.5 Sei R ein Ring und $I \trianglelefteq R$ ein Ideal. Dann gilt:

$$R/I \neq \{0\} \text{ und nullteilerfrei } \iff I \neq R \text{ und } \forall a, b \in R\,(ab \in I \Rightarrow a \in I \vee b \in I)$$

Beweis: $R/I \neq \{0\} \Leftrightarrow R \neq I$ gilt offensichtlich.
Da $a + I = 0_{R/I} = I \Leftrightarrow a \in I$ gilt, ist die Bedingung $ab \in I \Rightarrow a \in I \vee b \in I$ äquivalent zu $ab + I = 0_{R/I} \Rightarrow a + I = 0_{R/I} \vee b + I = 0_{R/I}$. Dies ist jedoch genau die Bedingung, dass R/I keine nichttrivialen Nullteiler hat.

□

Satz 22.6 *Sei R ein kommutativer Ring mit Eins und $P \trianglelefteq R$. Dann gilt*

$$P \textit{ ist Primideal} \iff R/P \textit{ ist Integritätsbereich}$$

Beweis: Sei P zunächst ein Primideal. Dann folgt $P \neq R \Rightarrow R/P \neq \{0\}$. Weil R kommutativ ist, gilt $\forall a, b \in R\ (ab \in P \Rightarrow a \in P \vee b \in P)$, nach dem vorigen Lemma ist damit R/P nullteilerfrei. Da R kommutativer Ring mit Eins ist, muss dies außerdem auch auf R/P zutreffen. Also ist R/P Integritätsbereich.
Sei umgekehrt R/P ein Integritätsbereich. Dann folgt $R/P \neq \{0\} \Rightarrow P \neq R$. Aus dem vorigen Lemma folgt wiederum aus der Tatsache, dass R/P nullteilerfrei ist, dass $(ab \in P \Rightarrow a \in P \vee b \in P)$ gelten muss, daher ist P ein Primideal.

□

Definition 22.7 Sei R ein Ring, $M \trianglelefteq R$. M heißt *maximales Ideal*, wenn $M \neq R$ ist und für alle $I \trianglelefteq R$ mit $M \subsetneqq I \subseteq R$ bereits $I = R$ gelten muss.

Definition 22.8 Ein Ring R heißt *einfach*, wenn

$$I \trianglelefteq R \Rightarrow (I = \{0\} \vee I = R)$$

Proposition 22.9 Sei R ein Ring und $M \trianglelefteq R$. Dann gilt:

$$M \text{ ist maximales Ideal} \iff R/M \neq \{0\} \text{ und } R/M \text{ ist einfach}$$

Beweis: Aus $M \neq R$ folgt $R/M \neq \{0\}$ und umgekehrt.
Sei nun zunächst M ein maximales Ideal. Nach dem 3. Isomorphiesatz hat jedes Ideal von R/M die Form J/M für ein Ideal $J \trianglelefteq R$ mit $M \subseteq J$. Wenn $J = M$, dann ist $J/M = M/M = \{0\}$, wenn $J \neq M$, dann ist $M \subsetneqq J \subseteq R$,

also muss $J = R$ und somit $J/M = R/M$ sein. Daher ist R/M einfach.
Sei umgekehrt R/M einfach. Dies ist äquivalent dazu, dass $|\{J \trianglelefteq R/M\}| = 2$ ist. Nach dem 3. Isomorphiesatz gilt $|\{I \trianglelefteq R \,|\, M \subseteq I\}| = |\{J \trianglelefteq R/M\}|$, also $|\{I \trianglelefteq R \,|\, M \subseteq I\}| = 2$. Daher kann $M \subseteq I \subseteq R$ nur für die Ideale $I = M$ und $I = R$ gelten. Damit ist M jedoch maximal.

□

Definition 22.10 Ein Ring $R \neq \{0\}$ mit Eins, in dem jedes Element außer 0 invertierbar ist (d.h. $E(R) = R \setminus \{0\}$), heißt *Schiefkörper*.
Ein kommutativer Ring $R \neq \{0\}$ mit Eins, in dem jedes Element außer 0 invertierbar ist, heißt *Körper*.

Bemerkung: Sei R ein Ring.

- $R \neq \{0\}$ und R ist nullteilerfrei $\iff (R \setminus \{0\}, \cdot)$ ist Halbgruppe
- R ist Schiefkörper $\iff (R \setminus \{0\}, \cdot)$ ist Gruppe
- R ist Körper $\iff (R \setminus \{0\}, \cdot)$ ist kommutative Gruppe

Bemerkung: Jeder Schiefkörper ist nullteilerfrei, jeder Körper ist Integritätsbereich (ein Element, das invertierbar ist, kann kein Nullteiler sein).

Beispiel: $\mathbb{Q}, \mathbb{R}, \mathbb{C}, \mathbb{Z}_p$ (wobei p Primzahl ist) sind Körper.

Beispiel: Seien i, j, k beliebige Symbole. Definiere eine Menge

$$\mathbb{H} := \{a + bi + cj + dk \,|\, a, b, c, d \in \mathbb{Q}\}$$

Die Addition auf dieser Menge sei durch $(a+bi+cj+dk)+(a'+b'i+c'j+d'k) = (a + a') + (b + b')i + (c + c')j + (d + d')k$ erklärt, die Multiplikation durch $i^2 = j^2 = k^2 = -1$, $ij = k$, $jk = i$, $ki = j$, $ji = -k$, $kj = -i$, $ik = -j$ (wobei $-i = (-1)i$ sei). Zudem soll das Distributivgesetz gelten.
Dann bildet $(\mathbb{H}, +, \cdot)$ einen nichtkommutativen Schiefkörper, die sogenannten rationalen *Quaternionen* (analog definiert man auch die reellen Quaternionen).

Bemerkung: $\{1, -1, i, -i, j, -j, k, -k\}$ bildet bezüglich der oben definierten Multiplikation (mit der zusätzlichen Bedingung $(-x)y = x(-y) = -(xy)$) eine Gruppe, die sogenannte *Quaternionengruppe* Q_8. Hierbei sind $i, -i, \ldots$ nur Symbole, die mit einer Addition nichts mehr zu tun haben! (also ist $-$ nur ein Zusatz zum Namen)

Lemma 22.11 Sei R ein kommutativer Ring mit Eins. Dann gilt:

$$R \text{ ist einfach und } \neq \{0\} \iff R \text{ ist Körper}$$

Beweis: In einem kommutativen Ring mit Eins gilt $\forall a \in R\ (a) = Ra = aR$. Sei nun $R \neq \{0\}$ einfach und $a \neq 0$ ein Element von R. Dann ist $aR = (a) \trianglelefteq R$, und weil $a \neq 0$ in (a) enthalten ist, muss $(a) \neq \{0\}$ sein. Da R einfach ist, kann somit nur $(a) = aR = R$ gelten, und daher gibt es ein $b \in R$ mit $ab = 1$ (weil R kommutativ ist, auch $ba = 1$). Also ist a invertierbar. Da somit jedes Element von $R \setminus \{0\}$ invertierbar ist, ist R ein Körper.
Sei umgekehrt R ein Körper und $I \trianglelefteq R$, $I \neq \{0\}$, ein Ideal. Dann gibt es ein $a \in I$, $a \neq 0$, das invertierbar ist. Damit ist jedoch $a^{-1}a = 1 \in I$ und damit auch $r = 1r \in I$ für jedes $r \in R$. Also muss $I = R$ sein, und folglich ist R einfach.

□

Satz 22.12 *Sei R ein kommutativer Ring mit Eins und $M \trianglelefteq R$. Dann gilt:*

$$M \textit{ ist maximales Ideal} \iff R/M \textit{ ist Körper}$$

Beweis: Ist M maximal, dann ist $R/M \neq \{0\}$ und einfach. Daher muss R/M ein Körper sein.
Ist umgekehrt R/M ein Körper, dann ist R/M einfach und $R/M \neq \{0\}$. Daraus folgt, dass M maximales Ideal ist.

Beispiel: Für eine Primzahl p ist wegen $p\mathbb{Z} \subseteq n\mathbb{Z} \Leftrightarrow n|p\ p\mathbb{Z}$ ein maximales Ideal von $\mathbb{Z}$, also ist $\mathbb{Z}_p = \mathbb{Z}/p\mathbb{Z}$ ein Körper.

Bemerkung: Man kann dies auf nichtkommutative Ringe verallgemeinern: ist R ein Ring mit Eins, dann gilt:

$$R \text{ rechts- und linkseinfach} \iff R \text{ ist Schiefkörper}$$

(dabei bedeutet „rechtseinfach“, dass es keine Rechtsideale außer R und $\{0\}$ gibt, „linkseinfach“, dass es keine Linksideale außer R und $\{0\}$ gibt)
Wenn R ein Ring mit Eins ist und $M \trianglelefteq R$, dann gilt:

M ist maximal unter den Links- und Rechtsidealen $\iff R/M$ ist Schiefkörper

(d.h. für jedes Rechts- oder Linksideal J mit $M \subsetneq J \subseteq R$ gilt bereits $J = R$)
Wenn R ein Ring mit Eins und M ein maximales Ideal ist, dann muss R/M nicht notwendigerweise Schiefkörper sein!

Halbgeordnete Mengen:

Definition 22.13 Sei X eine Menge und $\leq \subseteq X \times X$ eine Relation (man schreibt $x \leq y$ für $(x, y) \in \leq$). $\leq$ heißt *Ordnungsrelation* (und $(X, \leq)$ heißt *geordnete Menge*), wenn gilt:

1. $\forall x \in X \; x \leq x$
2. $\forall x, y, z \in X \; (x \leq y \wedge y \leq z) \; \Rightarrow \; x \leq z$
3. $\forall x, y \in X \; (x \leq y \wedge y \leq x \; \Rightarrow \; x = y)$

Definition 22.14 Sei $(X, \leq)$ eine geordnete Menge, $Y \subseteq X$.

- $s \in X$ heißt *obere Schranke* von Y, wenn $\forall y \in Y \; y \leq s$
- $y_0 \in Y$ heißt *maximales Element* von Y, wenn $\forall y \in Y \; (y_0 \leq y \; \Rightarrow y = y_0)$

Bemerkung: Eine obere Schranke von Y muss nicht unbedingt in Y liegen, ein maximales Element schon. Ein maximales Element y_0 ist im Allgemeinen keine obere Schranke (weil erlaubt ist, dass es in Y Elemente gibt, die mit y_0 nicht vergleichbar sind).

Definition 22.15 Eine geordnete Menge $(Y, \leq)$ heißt *totalgeordnet*, wenn $\forall x, y \in Y : (x \leq y \vee y \leq x)$.
Eine Teilmenge Y einer geordneten Menge $(X, \leq)$ heißt *Kette*, wenn Y bezüglich $\leq$ totalgeordnet ist, d.h. $\forall x, y \in Y \; (x \leq y \vee y \leq x)$.

Lemma 22.16 (Lemma von Zorn) Sei $(X, \leq)$ eine halbgeordnete Menge, $X \neq \emptyset$. Wenn jede Kette $Y \subseteq X$ eine obere Schranke in X hat, dann hat X ein maximales Element.

Bemerkung: Sei R ein Ring mit Eins und $I \trianglelefteq R$. Dann gilt $(I = R \; \Leftrightarrow \; 1 \in I)$.

Satz 22.17 *Sei R ein Ring mit Eins und $I \trianglelefteq R$. Wenn $I \neq R$, dann existiert ein maximales Ideal $M \trianglelefteq R$ mit $I \subseteq M$.*

Beweis: Sei $X = \{J \trianglelefteq R \,|\, I \subseteq J \subsetneq R\}$. Dann ist $X \neq \emptyset$, weil $I \in X$. X ist eine geordnete Menge durch $J \leq J' :\Leftrightarrow J \subseteq J'$. Jede Kette in X hat eine obere Schranke in X:
Sei $Y = \{J_\lambda \,|\, \lambda \in \Lambda\} \subseteq X$ eine Kette. Wenn $\Lambda = \emptyset$, dann ist jedes $x \in X$ eine obere Schranke. Sei andernfalls $J = \bigcup_{\lambda \in \Lambda} J_\lambda$. Dann gilt $\forall y = J_\mu \in Y$: $y \subseteq J$, also wäre J eine obere Schranke. Es bleibt jedoch zu zeigen, dass $J \in X$ ist:

- $0 \in J$, weil $0 \in J_\lambda$ für ein $\lambda \in \Lambda$. Daher ist $J \neq \emptyset$.
  Seien nun $a, b \in J$. Dann gibt es $\lambda, \mu \in \Lambda$ mit $a \in J_\lambda$ und $b \in J_\mu$. Weil Y eine Kette ist, muss $J_\lambda \subseteq J_\mu$ oder $J_\mu \subseteq J_\lambda$ gelten, o.B.d.A ersteres. Dann folgt $a, b \in J_\mu$, also $a - b \in J_\mu$ und folglich auch $a - b \in J$.
  Seien schließlich $a \in J$ und $r \in R$. Dann gibt es ein $\lambda \in \Lambda$ mit $a \in J_\lambda$. Weil J_λ ein Ideal ist, sind damit $ar, ra \in J_\lambda$ und somit auch $ar, ra \in J$. Folglich ist J ein Ideal.

- $I \subseteq J$ ist klar, weil für ein beliebiges $\lambda \in \Lambda$ $I \subseteq J_\lambda$ gilt.

- Da $\forall \lambda \in \Lambda$ $J_\lambda \neq R$ und folglich $1 \notin J_\lambda$ ist, muss $1 \notin J$ sein, und somit ist $J \neq R$.

Also ist J eine obere Schranke von Y, und man darf das Lemma von Zorn anwenden. Daher hat X ein maximales Element $M \in X$, d.h. $M \trianglelefteq R$, $I \subseteq M \subsetneq R$ und $\forall J \trianglelefteq R$ mit $I \subseteq J \subsetneq R$: wenn $M \subseteq J$, dann $J = M$. Also ist M ein maximales Ideal mit $I \subseteq M$.

□

Satz 22.18 *R sei ein Ring mit Eins und $M \trianglelefteq R$. Wenn M ein maximales Ideal ist, dann ist M auch ein Primideal.*

Beweis: Sei M ein maximales Ideal, $A, B \trianglelefteq R$ und $AB \subseteq M$. Angenommen, $A \nsubseteq M$. Dann ist $A + M$ ein Ideal mit $M \subsetneq A + M$, also $A + M = R$, da M maximal ist. R ist ein Ring mit Eins, also folgt $B \trianglelefteq R \Rightarrow RB = B$. Damit ist $B = RB = (A + M)B = AB + MB \subseteq AB + M \subseteq M$ (da $AB \subseteq M$). Hiermit ist gezeigt, dass $B \subseteq M$.

□

Bemerkung: Die Umkehrung gilt nicht, z.B. ist $(0) \subseteq \mathbb{Z}$ ein Primideal, aber nicht maximal.

Bemerkung: Für kommutative Ringe R folgt dieser Satz auch folgendermaßen:

M maximales Ideal $\Rightarrow$ R/M Körper $\Rightarrow$ R/M Integritätsbereich $\Rightarrow$ M Primideal

Bemerkung: Ist R ein kommutativer Ring mit Eins und P ein Primideal mit endlichem Index $[R : P]$, dann ist R/P ein endlicher Integritätsbereich und somit ein Körper (jeder endliche Integritätsbereich ist ein Körper – Beweis als Übung). Somit ist P dann ein maximales Ideal.

Kapitel 23

Direktes Produkt und direkte Summe von Ringen

Satz 23.1 *Sei* $\{R_i \mid i \in I\}$ *eine nichtleere Menge von Ringen. Dann ist* $(\prod_{i\in I} R_i, +, \cdot)$*, wobei* $(\prod_{i\in I} R_i, +)$ *das direkte Produkt der Abelschen Gruppen* $(R_i, +)$ *und* $(r_i)_{i\in I} \cdot (s_i)_{i\in I} = (r_i s_i)_{i\in I}$ *(komponentenweise Multiplikation) ist, ein Ring, das direkte Produkt der Ringe.*

- $\prod_{i\in I} R_i$ *ist genau dann kommutativ, wenn* $\forall i \in I$ R_i *kommutativ ist.*
- $\prod_{i\in I} R_i$ *hat genau dann ein Einselement, wenn* $\forall i \in I$ R_i *ein Einselement hat (dann ist* $1 = (1_{R_i})_{i\in I}$*).*
- $p_j : \prod_{i\in I} R_i \to R_j$ *mit* $p_j((r_i)_{i\in I}) = r_j$ *ist Ringepimorphismus (die Projektion in den* j*-ten Faktor).*
- $\varepsilon_j : R_j \to \prod_{i\in I} R_i$ *mit* $\varepsilon_j(r) = (r_i)_{i\in I}$*, wobei* $r_i = \begin{cases} r & i = j \\ 0 & sonst \end{cases}$ *ist, ist Ringmonomorphismus (die Einbettung des* j*-ten Faktors).*

Beweis: Die Assoziativität und die Distributivität übertragen sich von den einzelnen R_i, da $+$ und $\cdot$ komponentenweise definiert sind, ebenso die Kommutativität. Ist jedoch ein R_j nicht kommutativ, dann ist $\widetilde{R}_j = \operatorname{Im} \varepsilon_j \leq \prod_{i\in I} R_i$, also ist $\widetilde{R}_j \simeq R_j$ ein nichtkommutativer Unterring von $\prod_{i\in I} R_i$, und damit ist auch $\prod_{i\in I} R_i$ nichtkommutativ.
Wenn jedes R_i ein Ring mit Einselement 1_{R_i} ist, dann ist $1 = (1_{R_i})_{i\in I}$ Einselement in $\prod_{i\in I} R_i$. Wenn umgekehrt $(r_i)_{i\in I}$ Einselement in $\prod_{i\in I} R_i$ ist, dann muss r_i Einselement in R_i sein.
Es ist bereits bekannt, dass p_j Gruppenepimorphismus bezüglich $+$ ist. Weil

zudem $p_j((r_i)_{i\in I}(s_i)_{i\in I}) = p_j((r_is_i)_{i\in I}) = r_js_j = p_j((r_i)_{i\in I})p_j((s_i)_{i\in I})$ gilt, ist p_j auch Ringhomomorphismus.
Ebenso ist bekannt, dass ε_j Gruppenmonomorphismus ist. Weil zudem $\varepsilon_j(rs) = (t_i)_{i\in I} = (r_i)_{i\in I}(s_i)_{i\in I} = \varepsilon_j(r)\varepsilon_j(s)$ mit $t_i = \begin{cases} rs & i = j \\ 0 & \text{sonst} \end{cases} = r_is_i, r_i = \begin{cases} r & i = j \\ 0 & \text{sonst} \end{cases}$ und $s_i = \begin{cases} s & i = j \\ 0 & \text{sonst} \end{cases}$ gilt, ist ε_j auch Ringhomomorphismus.

□

Proposition 23.2 Sei für $i \in I$ R_i ein Ring und $J_i \trianglelefteq R_i$ ein Ideal. Dann ist $\prod_{i\in I} J_i = \{(r_i)_{i\in I} \,|\, r_i \in J_i \ \forall i\}$ ein Ideal in $\prod_{i\in I} R_i$; insbesondere ist $\operatorname{Im}\varepsilon_j = \{(r_i)_{i\in I} \,|\, r_i = 0 \text{ für } i \neq j\}$ ein Ideal von $\prod_{i\in I} R_i$.

Beweis: Es ist klar, dass es sich um Unterringe handelt. Da die Multiplikation komponentenweise definiert ist, gilt zudem für $(r_i)_{i\in I} \in \prod_{i\in I} R_i$ und $(j_i)_{i\in I} \in \prod_{i\in I} J_i$: $(r_i)_{i\in I}(j_i)_{i\in I} = (r_ij_i)_{i\in I} \in \prod_{i\in I} J_i$, also ist $\prod_{i\in I} J_i$ ein Ideal.
Insbesondere ist $\operatorname{Im}\varepsilon_j = \prod_{i\in I} J_i$ mit $J_i = \{0\}$ für $i \neq j$ und $J_j = R_j$ ein Ideal.

□

Proposition 23.3 Wenn $R_1, \ldots, R_n$ Ringe mit Eins sind, dann ist jedes Ideal $J \trianglelefteq \prod_{i=1}^n R_i$ von der Form $J = \prod_{i=1}^n J_i$ für Ideale $J_i \trianglelefteq R_i$. Dabei ist

$$J_i = \{r_i \in R_i \,|\, \exists r_1, \ldots, r_{i-1}, r_{i+1}, \ldots, r_n \text{ sodass } (r_1, \ldots, r_n) \in J\}$$

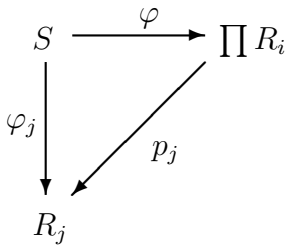
Beweis: als Übung.

Bemerkung: Wenn $R = \prod_{i\in I} R_i$ und I unendlich ist, dann muß nicht jedes Ideal diese Form haben.

Bemerkung: Die direkte Summe von unendlich vielen Ringen ist nicht so wichtig wie etwa die direkte Summe von Gruppen; z.B. hat die direkte Summe von unendlich vielen Ringen mit Eins kein Einselement!
Es gilt aber

$$\sum_{i\in I} R_i = \{(r_i)_{i\in I} \,|\, \text{nur endlich viele } r_i \text{ sind } \neq 0\} \trianglelefteq \prod_{i\in I} R_i$$

Satz 23.4 (Universelle Eigenschaft des direkten Produkts) *Für $i \in I$ sei R_i ein Ring. Dann gilt für alle Ringe S und alle Mengen $\{\varphi_i : S \to R_i \,|\, i \in I\}$ von Ringhomomorphismen, dass es genau einen Ringhomomorphismus $\varphi : S \to \prod_{i\in I} R_i$ gibt, sodass $\forall j \in I$ $p_j \circ \varphi = \varphi_j$, d.h. das folgende Diagramm kommutiert:*



Beweis: Wir wissen bereits, dass es genau einen Gruppenhomomorphismus bezüglich + gibt, der die Bedingung erfüllt, nämlich $\varphi(s) = (\varphi_i(s))_{i\in I}$. Dieser ist jedoch auch Ringhomomorphismus, denn es gilt

$$\begin{aligned}\varphi(rs) &= (\varphi_i(rs))_{i\in I}\\ &= (\varphi_i(r)\varphi_i(s))_{i\in I}\\ &= (\varphi_i(r))_{i\in I}(\varphi_i(s))_{i\in I}\\ &= \varphi(r)\varphi(s)\end{aligned}$$

□

Satz 23.5 (Innere direkte Summe) *Sei R ein Ring und $A_1, \ldots, A_n$ Ideale von R, sodass $A_1 + \ldots + A_n = R$ und $\forall k \in \{1, \ldots, n\}$ $A_k \cap (A_1 + \ldots + A_{k-1} + A_{k+1} + \ldots + A_n) = \{0\}$.*
Dann ist $R \simeq \sum_{i=1}^n A_i$, wobei $\varphi : \sum_{i=1}^n A_i \to R$, definiert durch $\varphi((a_1, \ldots, a_n)) = a_1 + \ldots + a_n$, der Isomorphismus ist.

Beweis: Die A_i sind Normalteiler von $(R, +)$, die R erzeugen sodass

$$A_k \cap \langle \bigcup_{i\neq k} A_i \rangle = A_k \cap (A_1 + \ldots + A_{k-1} + A_{k+1} + \ldots + A_n) = \{0\}$$

ist, also gilt $(R, +) \simeq \sum_{i=1}^n (A_i, +)$. φ ist ein Gruppenisomorphismus, es bleibt nur noch zu zeigen, dass φ auch Ringhomomorphismus ist:
Für $a_i \in A_i$, $a_j \in A_j$ mit $i \neq j$ gilt $a_i a_j = 0$, da $a_i a_j \in A_i \cap A_j = \{0\}$ ist, daher:

$$\begin{aligned}\varphi((a_1, \ldots, a_n))\varphi((b_1, \ldots, b_n)) &= (a_1 + \ldots + a_n)(b_1 + \ldots + b_n)\\ &= a_1 b_1 + \ldots + a_n b_n\\ &= \varphi((a_1 b_1, \ldots, a_n b_n))\\ &= \varphi((a_1, \ldots, a_n)(b_1, \ldots, b_n))\end{aligned}$$

□

Kapitel 24

Chinesischer Restsatz

Definition 24.1 Sei R ein Ring, $I, J \trianglelefteq R$. I, J heißen *relativ prim*, wenn $I + J = R$.

Bemerkung: Diese Definition stimmt mit jener für $n, m \in \mathbb{Z}$ überein, denn es gilt $\mathrm{ggT}(n, m) = 1 \Leftrightarrow n\mathbb{Z} + m\mathbb{Z} = \mathbb{Z}$ (allgemein ist $m\mathbb{Z} + n\mathbb{Z} = d\mathbb{Z}$, wobei $d = \mathrm{ggT}(n, m)$).

Bemerkung: Sei R ein Ring, $I, J \trianglelefteq R$. Dann ist $IJ \subseteq I \cap J$:

$$IJ = \{i_1 j_1 + \ldots + i_n j_n \,|\, i_k \in I, j_k \in J, n \in \mathbb{N}\}$$

Weil I, J Ideale sind, ist jedoch $i_k j_k \in I$ und $i_k j_k \in J$, also $i_k j_k \in I \cap J$ und somit $i_1 j_1 + \ldots + i_n j_n \in I \cap J$.
Im allgemeinen ist jedoch $IJ \neq I \cap J$, etwa für $I = J = 2\mathbb{Z} \trianglelefteq \mathbb{Z}$: hier ist $IJ = 4\mathbb{Z}$ und $I \cap J = 2\mathbb{Z}$.

Proposition 24.2 Sei R ein kommutativer Ring mit Eins, $I, J \trianglelefteq R$ mit $I + J = R$. Dann gilt $IJ = I \cap J$.

Beweis: Es genügt zu zeigen, dass $I \cap J \subseteq IJ$ ist. Weil R ein Ring mit Eins ist, gilt zunächst $\forall A \trianglelefteq R\ AR = A$, also

$$I \cap J = (I \cap J)R = (I \cap J)(I + J) = (I \cap J)I + (I \cap J)J \subseteq JI + IJ = IJ + IJ = IJ$$

weil wegen der Kommutativität $IJ = JI$ gilt.

□

Bemerkung: Diese Proposition verallgemeinert die Tatsache, dass für relativ prime $n, m \in \mathbb{Z}$ $nm = \mathrm{kgV}(n, m)$ gilt, denn allgemein ist $(n\mathbb{Z})(m\mathbb{Z}) = nm\mathbb{Z}$ und $(n\mathbb{Z}) \cap (m\mathbb{Z}) = (\mathrm{kgV}(n, m))\mathbb{Z}$.

BEMERKUNG: Ist M ein maximales Ideal und $J \not\subseteq M$ ein beliebiges Ideal, dann sind M, J relativ prim, denn wegen $M \subsetneq J + M$ muss $J + M = R$ sein.

Definition 24.3 Sei $I \trianglelefteq R$ ein Ideal, $a, b \in R$. Dann definieren wir die Kongruenz modulo I als $a \equiv b \bmod I \Leftrightarrow a - b \in I$, d.h. $a \equiv b \bmod I \Leftrightarrow a + I = b + I$.
Man schreibt manchmal $\overline{a}$ für $a + I$. Es gelten die Rechenregeln $\overline{a} + \overline{b} = \overline{a + b}$ und $\overline{a} \cdot \overline{b} = \overline{a \cdot b}$. Die Schreibweise $a + I$ ist jedoch zu bevorzugen, da hervorgeht, um welches Ideal es sich handelt.

Lemma 24.4 Sei R ein Ring mit Eins, $A_1, \ldots, A_n \trianglelefteq R$ mit $A_i + A_j = R$ für $i \neq j$. Dann gilt für $k = 1, \ldots, n$: $A_k + A_1 \ldots A_{k-1} A_{k+1} \ldots A_n = R$. Insbesondere gilt dann auch $A_k + \bigcap_{i \neq k} A_i = R$.

Beweis: Gegeben A_k, sei $\{B_1, \ldots, B_{n-1}\} = \{A_i \mid i \neq k\}$. Wir zeigen durch Induktion nach j, dass $R = A_k + B_1 \ldots B_j$ für alle $1 \leq j \leq n - 1$ gilt:

- $j = 1$: $R = A_k + B_1$ gilt nach Voraussetzung.
- Es gelte $R = A_k + B_1 \ldots B_{j-1}$. Es folgt

$$\begin{aligned} R &= (A_k + B_1 \ldots B_{j-1})R \\ &= (A_k + B_1 \ldots B_{j-1})(A_k + B_j) \\ &= A_k^2 + A_k B_j + B_1 \ldots B_{j-1} A_k + B_1 \ldots B_j \\ &\subseteq A_k + B_1 \ldots B_j \end{aligned}$$

  Also muss auch $R = A_k + B_1 \ldots B_j$ gelten.

□

Satz 24.5 (Chinesischer Restsatz) *Sei R ein Ring mit Eins, $A_1, \ldots, A_n$ Ideale von R, und für $i \neq j$ sei $A_i + A_j = R$. Dann gibt es für alle $b_1, \ldots, b_n \in R$ ein $b \in R$, sodass $b \equiv b_i \bmod A_i$ für $i = 1, \ldots, n$. Dieses b ist eindeutig modulo $\bigcap_{i=1}^{n} A_i$.*

Beweis: Nach dem vorherigen Lemma ist $A_i + \bigcap_{j \neq i} A_j = R$; für jedes i sei $c_i \in A_i$, $d_i \in \bigcap_{j \neq i} A_j$, sodass $c_i + d_i = b_i$. Setze $b := d_1 + \ldots + d_n$. Dann gilt für alle i $d_i \equiv b_i \bmod A_i$ (da $c_i = b_i - d_i \in A_i$) und $d_i \equiv 0 \bmod A_j$ für alle $j \neq i$ (da $d_i \in A_j$). Daher ist

$$\begin{aligned} b &= d_1 + \ldots + d_n \\ &= d_1 + \ldots + d_{i-1} + d_i + d_{i+1} + \ldots + d_n \\ &\equiv 0 + \ldots + 0 + b_i + 0 + \ldots + 0 \equiv b_i \mod A_i \end{aligned}$$

Die Eindeutigkeit modulo $\bigcap_{i=1}^{n} A_i$ ergibt sich folgendermaßen: wenn b, b' gegeben sind, sodass $b \equiv b_i \equiv b' \bmod A_i$ ist, dann gilt $\forall i\ b - b' \in A_i$, d.h. $b - b' \in \bigcap_{i=1}^{n} A_i$ und somit $b \equiv b' \bmod \bigcap_{i=1}^{n} A_i$.

□

Korollar 24.6 (Chinesischer Restsatz für $\mathbb{Z}$) Seien $m_1, \ldots, m_n \in \mathbb{Z}$, sodass für $i \neq j$ $\mathrm{ggT}(m_i, m_j) = 1$ ist. Dann gibt es für alle $b_1, \ldots, b_n \in \mathbb{Z}$ ein $b \in \mathbb{Z}$, sodass $\forall i\ b \equiv b_i \bmod m_i$ (und dieses b ist eindeutig modulo $m_1 \ldots m_n$).

Beweis: Es gilt $m_i\mathbb{Z} + m_j\mathbb{Z} = \mathrm{ggT}(m_i, m_j)\mathbb{Z} = \mathbb{Z}$, also kann man den chinesischen Restsatz anwenden. Es gibt daher ein eindeutiges $b \bmod \bigcap_{i=1}^{n} m_i\mathbb{Z} = m_1 \ldots m_n\mathbb{Z}$ (allgemein ist $\bigcap_{i=1}^{n} m_i\mathbb{Z} = \mathrm{kgV}(m_1, \ldots, m_n)\mathbb{Z}$), das $b \equiv b_i \bmod m_i\mathbb{Z}$, also $b \equiv b_i \bmod m_i$, für alle i erfüllt.

□

Lemma 24.7 Sei R ein kommutativer Ring mit Eins, $A_1, \ldots, A_n \trianglelefteq R$ mit $A_i + A_j = R$ für $i \neq j$. Dann gilt $A_1 \cap \ldots \cap A_n = A_1 \cdot \ldots \cdot A_n$.

Beweis: durch Induktion nach n:

- Für $n = 1$ ist die Aussage trivial.
- Es gelte bereits $A_1 \cap \ldots \cap A_{n-1} = A_1 \cdot \ldots \cdot A_{n-1}$. Dann folgt:

  $A_1 \cap \ldots \cap A_n = (A_1 \cap \ldots \cap A_{n-1}) \cap A_n = (A_1 \cdot \ldots \cdot A_{n-1}) \cap A_n = (A_1 \cdot \ldots \cdot A_{n-1}) \cdot A_n$

  da nach Lemma 24.4 $A_1 \cdot \ldots \cdot A_{n-1} + A_n = R$ und nach Proposition 24.2 $I + J = R \ \Rightarrow\ I \cap J = I \cdot J$ gilt.

□

Korollar 24.8 Seien R ein Ring mit Eins und $A_1, \ldots, A_n$ Ideale von R. Dann ist $\varphi : R/(A_1 \cap \ldots \cap A_n) \to R/A_1 \times \ldots \times R/A_n$ mit $\varphi(r + A_1 \cap \ldots \cap A_n) = (r + A_1, \ldots, r + A_n)$ ein Ringmonomorphismus. Wenn zusätzlich für $i \neq j$ $A_i + A_j = R$ gilt, dann ist φ auch surjektiv, also ein Isomorphismus.

Beweis: als Übung.

Korollar 24.9 Seien R ein kommutativer Ring mit Eins und $A_1, \ldots, A_n$ Ideale von R, sodass für $i \neq j$ $A_i + A_j = R$ gelte. Dann folgt

$$[R : (A_1 \cdot \ldots \cdot A_n)] = [R : A_1] \cdot \ldots \cdot [R : A_n]$$

BEMERKUNG: Einfacher Beweis des chinesischen Restsatzes für $\mathbb{Z}$:

Es mögen die Voraussetzungen von Korollar 24.6 gelten.
$\varphi : \mathbb{Z}/(m_1 \cdot \ldots \cdot m_n)\mathbb{Z} \to (\mathbb{Z}/m_1\mathbb{Z}) \times \ldots \times (\mathbb{Z}/m_n\mathbb{Z})$, gegeben durch $\varphi(k + m_1 \ldots m_n\mathbb{Z}) = (k + m_1\mathbb{Z}, \ldots, k + m_n\mathbb{Z})$, ist wohldefiniert und ein Ringhomomorphismus.
φ ist injektiv, denn aus $\varphi(k+m_1 \ldots m_n\mathbb{Z}) = \varphi(l+m_1 \ldots m_n\mathbb{Z})$ folgt $k+m_i\mathbb{Z} = l+m_i\mathbb{Z}$ für alle i, damit $m_i|k-l$ für alle i und schließlich $\mathrm{kgV}(m_1, \ldots, m_n)|k-l$. Da die m_i paarweise relativ prim sind, ist $\mathrm{kgV}(m_1, \ldots, m_n) = m_1 \ldots m_n$, also $m_1 \ldots m_n|k - l$ und damit $k + m_1 \ldots m_n\mathbb{Z} = l + m_1 \ldots m_n\mathbb{Z}$.
Weil zudem $|\mathbb{Z}/(m_1 \cdot \ldots \cdot m_n)\mathbb{Z}| = m_1 \cdot \ldots \cdot m_n = |\mathbb{Z}/m_1\mathbb{Z}| \cdot \ldots \cdot |\mathbb{Z}/m_n\mathbb{Z}| = |(\mathbb{Z}/m_1\mathbb{Z}) \times \ldots \times (\mathbb{Z}/m_n\mathbb{Z})|$ ist, also Grund- und Zielmenge von φ gleichmächtige endliche Mengen sind, muss φ auch bijektiv sein.
Also gibt es genau ein b modulo $m_1 \cdot \ldots \cdot m_n$, sodass $\varphi(b + m_1 \ldots m_n\mathbb{Z}) = (b_1 + m_1\mathbb{Z}, \ldots, b_n + m_n\mathbb{Z})$ und damit $b \equiv b_i \mod m_i$ für alle i ist.

□

Kapitel 25

Das Nilradikal

Lemma 25.1 Sei R ein kommutativer Ring, dann ist

$$\mathrm{Nil}(R) := \{r \in R \,|\, \exists n \in \mathbb{N} \text{ mit } r^n = 0\}$$

(die Menge der nilpotenten Elemente von R) ein Ideal von R, genannt das *Nilradikal* von R.

Beweis: als Übung.

Definition 25.2 Sei $S \neq \emptyset$ eine Teilmenge eines Ringes R. S heißt *multiplikativ abgeschlossen*, wenn $a, b \in S \;\Rightarrow\; ab \in S$ gilt.

Lemma 25.3 Sei R ein kommutativer Ring mit Eins und $S \subseteq R$ multiplikativ abgeschlossen, $0 \notin S$. Dann gibt es ein Primideal $P \trianglelefteq R$ mit $P \cap S = \emptyset$.

Beweis: Sei $X = \{I \trianglelefteq R \,|\, I \cap S = \emptyset\}$. $X \neq \emptyset$, da $\{0\} \in X$. X werde durch $\subseteq$ geordnet. Dann kann man das Zorn'sche Lemma auf X anwenden:
Wenn $Y = \{I_\lambda \,|\, \lambda \in \Lambda\} \subseteq X$ eine Kette ist, dann ist $J = \bigcup_{\lambda\in\Lambda} I_\lambda$ ein Ideal (Beweis wie in Satz 22.17), und da für alle λ $I_\lambda \cap S = \emptyset$ ist, muss $J \cap S = \emptyset$ sein, also $J \in X$. Zudem ist J offensichtlich eine obere Schranke von Y.
Also enthält X ein maximales Element P mit $P \cap S = \emptyset$. Wir zeigen nun, dass es sich um ein Primideal handelt:
$P \neq R$, da $P \cap S = \emptyset$ und $S \neq \emptyset$. Seien nun $a, b \in R$ mit $ab \in P$:
Angenommen, $a \notin P$ und $b \notin P$. Dann gilt $P \subsetneq (a) + P$ und $P \subsetneq (b) + P$. Wegen der Maximalität von P in X ist daher $((a) + P) \cap S \neq \emptyset$ und $((b) + P) \cap S \neq \emptyset$. Seien $s \in ((a) + P) \cap S$ und $t \in ((b) + P) \cap S$. Weil S multiplikativ abgeschlossen ist, muss daher $st \in S$ sein, und damit $st \in ((a) + P)((b) + P) = (ab) + (a)P + (b)P + P^2 \subseteq P$, weil für kommutative Ringe mit Eins $(a)(b) = (ab)$ gilt. Also folgt $st \in S \cap P$ und somit $S \cap P \neq \emptyset$, ein Widerspruch.

Folglich erfüllt P die Bedingungen eines Primideals, und wegen $P \in X$ gilt $P \cap S = \emptyset$.

□

Satz 25.4 *Ist R ein kommutativer Ring mit Eins, dann ist*

$$\mathrm{Nil}(R) = \bigcap_{P \text{ Primideal von } R} P$$

Beweis: Sei $a \in \mathrm{Nil}(R)$, $n \in \mathbb{N}$ mit $a^n = 0$. Sei weiters P ein Primideal. Dann ist $a \cdot a^{n-1} = a^n = 0 \in P$, also $a \in P$ oder $a^{n-1} \in P$. Im ersten Fall folgt sofort $a \in P$, andernfalls gilt $a^{n-1} \in P \Rightarrow a \in P \vee a^{n-2} \in P$, etc. Also muss $a \in P$ sein, und daher gilt $a \in \bigcap_{P \text{ Primideal von } R} P$.
Sei umgekehrt $a \notin \mathrm{Nil}(R)$. Dann ist $S = \{a^n \mid n \in \mathbb{N}\}$ multiplikativ abgeschlossen. Da a nicht nilpotent ist, enthält S nicht 0. Also gibt es ein Primideal P, sodass $P \cap S = \emptyset$ ist, d.h. insbesondere $a \notin P$. Damit folgt $a \notin \bigcap_{P \text{ Primideal von } R} P$.

□

Bemerkung: Sei R ein kommutativer Ring mit Eins und I ein Ideal. Sei $\sqrt{I} := \{a \in R \mid \exists n \in \mathbb{N}\ a^n \in I\}$, dann heißt $\sqrt{I}$ das *Radikal* von I. Insbesondere ist $\mathrm{Nil}(R) = \sqrt{\{0\}}$. Es gilt $\sqrt{I} = \bigcap_{P \text{ Primideal von } R, I \subseteq P} P$, wie sich mit Hilfe des folgenden Lemmas zeigen lässt:

Lemma 25.5 Sei R ein kommutativer Ring mit Eins, $I \trianglelefteq R$, $I \neq R$, und S eine multiplikativ abgeschlossene Teilmenge von R mit $S \cap I = \emptyset$. Dann gibt es ein Primideal P mit $I \subseteq P$, sodass $S \cap P = \emptyset$.

Beweis: mit Hilfe des Zorn'schen Lemmas, angewandt auf $X = \{J \trianglelefteq R \mid I \subseteq J, J \cap S = \emptyset\}$.

Lemma 25.6 Ist R ein kommutativer Ring mit Eins, $a \in \mathrm{Nil}(R)$, b eine Einheit, dann ist auch $a \pm b$ eine Einheit.

Beweis: als Übung, folgt aus $a^n - b^n = (a - b) \sum_{k=0}^{n-1} a^k b^{n-1-k}$.

Kapitel 26

Der Polynomring

Definition 26.1 Der *Polynomring in einer Unbestimmten* über R ist definiert durch die additive Gruppe $\sum_{i=0}^{\infty}(R,+)$ und die Multiplikation

$$(a_n)_{n=0}^{\infty} \cdot (b_n)_{n=0}^{\infty} = (c_n)_{n=0}^{\infty} \text{ mit } c_n = \sum_{k=0}^{n} a_k b_{n-k} = \sum_{k+l=n} a_k b_l \text{ (Faltung)}$$

Bemerkung: Wir identifizieren hierbei ein Polynom $a_0 + \ldots + a_n x^n$ mit der Folge seiner Koeffizienten. Nur endlich viele sind dabei $\neq 0$.

Proposition 26.2 Sei R ein Ring. Der Polynomring in einer Unbestimmten über R ist ein Ring. Er ist kommutativ, wenn R kommutativ ist. Wenn R ein Ring mit Eins ist, dann ist $(1,0,0,\ldots)$ Einselement. Außerdem ist $r \mapsto (r,0,0,\ldots)$ ein Ringmonomorphismus (die Einbettung von R in den Polynomring).

Beweis:

- Es ist bereits bekannt, dass der Polynomring bezüglich + eine kommutative Gruppe ist.
- Die Assoziativität lässt sich leicht nachrechnen: sei dazu

  $((a_n)_{n=0}^{\infty}(b_n)_{n=0}^{\infty})(c_n)_{n=0}^{\infty} = (d_n)_{n=0}^{\infty}$ und $(a_n)_{n=0}^{\infty}((b_n)_{n=0}^{\infty}(c_n)_{n=0}^{\infty}) = (d'_n)_{n=0}^{\infty}$

$$\begin{aligned} d_n &= \sum_{k+m=n} \left(\sum_{i+j=k} a_i b_j \right) c_m \\ &= \sum_{i+j+m=n} a_i b_j c_m \\ &= \sum_{i+l=n} a_i \left(\sum_{j+m=l} b_j c_m \right) \\ &= d'n \end{aligned}$$

- Ebenso lässt sich die Distributivität nachprüfen.
- Wenn R kommutativ ist, dann gilt $\sum_{k+l=n} a_k b_l = \sum_{l+k=n} b_l a_k$, also $(a_n)_{n=0}^{\infty}(b_n)_{n=0}^{\infty} = (b_n)_{n=0}^{\infty}(a_n)_{n=0}^{\infty}$
- Sei $\varepsilon = (\varepsilon_n)_{n=0}^{\infty}$ mit $\varepsilon_0 = 1$ und $\varepsilon_n = 0$ für $n > 0$. Dann ist ε Einselement: $\sum_{k+l=n} \varepsilon_k a_l = a_n$, weil $\varepsilon_0 a_n = a_n$ und $\varepsilon_k a_l = 0$ für alle $k > 0$ ist, daher muss $(\varepsilon_n)_{n=0}^{\infty}(a_n)_{n=0}^{\infty} = (a_n)_{n=0}^{\infty}$ sein, analog auch $(a_n)_{n=0}^{\infty}(\varepsilon_n)_{n=0}^{\infty} = (a_n)_{n=0}^{\infty}$.
- Die Einbettung $r \mapsto (r_n)_{n=0}^{\infty} = (r, 0, 0, \ldots)$ ist bekanntermaßen ein Gruppenmonomorphismus. Es gilt jedoch auch $(r, 0, 0, \ldots)(s, 0, 0, \ldots) = (rs, 0, 0, \ldots)$, denn da für $k \neq 0$ oder $l \neq 0$ $r_k s_l = 0$ ist, kann $\sum_{k+l=n} r_k s_l \neq 0$ nur gelten, falls $k + l = n = 0$. Zudem ist $\sum_{k+l=0} r_k s_l = r_0 s_0 = rs$, also $(r, 0, 0, \ldots)(s, 0, 0, \ldots) = (rs, 0, 0, \ldots)$.

□

Bemerkung: Man schreibt für ein $r \in R$ $r := (r, 0, 0, \ldots)$ und, falls R ein Einselement hat, $x := (0, 1, 0, \ldots)$. Es gilt in diesem Fall:

- $x^n = (0, 0, \ldots, 0, 1, 0, \ldots)$ („1“ steht an der n-ten Stelle)
- $r \cdot (a_n)_{n=0}^{\infty} = (ra_n)_{n=0}^{\infty}$ und $(a_n)_{n=0}^{\infty} \cdot r = (a_n r)_{n=0}^{\infty}$
- $rx^n = x^n r = (0, 0, \ldots, 0, r, 0, \ldots)$ („r“ steht an der n-ten Stelle)

Jedes Element im Polynomring hat dann eine eindeutige Darstellung der Form $(a_n)_{n=0}^{\infty} = \sum_{n=0}^{N} r_n x^n$. Sei nämlich N so, dass $a_n = 0$ für $n > N$ ist, dann gilt

$$(a_n)_{n=0}^{\infty} = (a_0, \ldots, a_n, 0, 0, \ldots) = a_0 1 + a_2 x + \ldots + a_n x^n$$

Die $r_i = a_i$ sind eindeutig bestimmt, bis auf Hinzufügen von beliebig vielen $a_i = 0$ für $i > N$.

In Hinkunft sei R ein kommutativer Ring mit Eins, und wir schreiben $a_0 + \ldots + a_n x^n$ für $(a_0, \ldots, a_n, \ldots)$ sowie $R[x]$ für den Polynomring in einer Unbestimmten über R (bzw. $R[y]$, wenn man $(0, 1, 0, \ldots) = y$ setzt).

Definition 26.3 (Grad eines Polynoms) Sei $f = (a_n)_{n=0}^{\infty} = \sum a_n x^n \in R[x]$.

- Wenn $f = 0$, d.h. $\forall n\ a_n = 0$, dann sei $\deg f := -\infty$.
- Wenn $f \neq 0$, dann sei $\deg f := \max\{n \in \mathbb{N} \mid a_n \neq 0\}$.

Wenn $f \neq 0$ und $m = \max\{n \in \mathbb{N} \mid a_n \neq 0\}$, dann heißt a_m der *Leitkoeffizient* von f (das Nullpolynom hat keinen Leitkoeffizienten).

BEMERKUNG: Da wir $r \in R$ mit $(r, 0, 0, \ldots) = r + 0x + 0x^2 + \ldots$ identifizieren, d.h. $R \simeq \{(r, 0, 0, \ldots) \mid r \in R\} \leq R[x]$, gilt für $f = (a_n)_{n=0}^{\infty} \in R[x]$:

$$\begin{aligned} f = (a_n)_{n=0}^{\infty} \in R &\iff \forall n > 0\ a_n = 0 \\ &\iff \deg f = 0 \vee \deg f = -\infty \\ &\iff \deg f \leq 0 \end{aligned}$$

Ein Polynom mit $\deg f = 0 \vee \deg f = -\infty$ heißt *konstantes* Polynom.

Satz 26.4 (Einsetzhomomorphismus) *Seien R, S kommutative Ringe mit Eins und $\varphi : R \to S$ ein Ringhomomorphismus mit $\varphi(1) = 1$. Sei weiters $s \in S$. Dann existiert genau ein Ringhomomorphismus $\overline{\varphi} : R[x] \to S$ mit $\overline{\varphi}|_R = \varphi$ und $\overline{\varphi}(x) = s$, nämlich $\overline{\varphi}(a_0 + a_1 x + \ldots + a_n x^n) = \varphi(a_0) + \varphi(a_1)s + \ldots + \varphi(a_n)s^n$.*

Beweis: Wenn ein solches $\overline{\varphi}$ existiert, dann muss

$$\begin{aligned} \overline{\varphi}(a_0 + a_1 x + \ldots + a_n x^n) &= \overline{\varphi}(a_0) + \overline{\varphi}(a_1)\overline{\varphi}(x) + \ldots + \overline{\varphi}(a_n)\overline{\varphi}(x)^n \\ &= \varphi(a_0) + \varphi(a_1)s + \ldots + \varphi(a_n)s^n \end{aligned}$$

gelten. Wenn $\overline{\varphi}$ so definiert ist, ist $\overline{\varphi}|_R = \varphi$ klar. Es bleibt zu zeigen, dass es sich um einen Ringhomomorphismus handelt:
Sei dazu $f = a_0 + \ldots + a_n x^n$ und $g = b_0 + \ldots + b_n x^n$ und $fg = \sum c_k x^k$. Dann

gilt:

$$\begin{aligned}
\overline{\varphi}(fg) &= \overline{\varphi}\Big(\sum_{k\geq 0} c_k x^k\Big) \\
&= \sum_{k\geq 0} \varphi(c_k) s^k \\
&= \sum_{k\geq 0} \Big(\sum_{i+j=k} \varphi(a_i)\varphi(b_j)\Big) s^k \\
&= \sum_{k\geq 0} \sum_{i+j=k} \varphi(a_i) s^i \varphi(b_j) s^j \text{ (wegen der Kommutativität!)} \\
&= \Big(\sum_{i\geq 0} \varphi(a_i) s^i\Big)\Big(\sum_{j\geq 0} \varphi(b_j) s^j\Big) \\
&= \overline{\varphi}(f)\overline{\varphi}(g)
\end{aligned}$$

Offensichtlich gilt auch

$$\begin{aligned}
\overline{\varphi}(f+g) &= \sum_{i\geq 0} \varphi(a_i + b_i) s^i \\
&= \sum_{i\geq 0} (\varphi(a_i) + \varphi(b_i)) s^i \\
&= \sum_{i\geq 0} \varphi(a_i) s^i + \sum_{i\geq 0} \varphi(b_i) s^i \\
&= \overline{\varphi}(f) + \overline{\varphi}(g)
\end{aligned}$$

Also ist $\overline{\varphi}$ tatsächlich Ringhomomorphismus.

□

Bemerkung: Damit $\overline{\varphi}$ Ringhomomorphismus ist, muss zumindest für das fixe s gelten, dass $\forall r \in R\ \varphi(r)s = s\varphi(r)$ ist.

Korollar 26.5 Sei R ein kommutativer Ring mit Eins und $c \in R$. Dann ist $\varphi_c : R[x] \to R$ mit $\varphi_c(a_0 + a_1 x + \ldots + a_n x^n) = a_0 + a_1 c + \ldots + a_n c^n$ ein Ringhomomorphismus, d.h. jedes Polynom $f \in R[x]$ definiert durch Einsetzen eine Funktion $f : R \to R$, $c \mapsto f(c)$.

Bemerkung: Dies ist gerade der Einsetzhomomorphismus für $S = R$, $\varphi = \mathrm{id}_R$. Wenn wir $f(c) := a_0 + a_1 c + \ldots + a_n c^n$ definieren, dann heißt das für $f, g \in R[x]$: $(f+g)(c) = f(c) + g(c)$ und $(fg)(c) = f(c)g(c)$ (weil φ_c ein Ringhomomorphismus ist). Man kann also in ein Produkt oder eine Summe

einsetzen, indem man in die einzelnen Faktoren/Summanden einsetzt und dann multipliziert/addiert.

BEISPIEL: Sei $\mathbb{H}$ der Schiefkörper der rationalen Quaternionen, $f(x) = x+i \in \mathbb{H}[x]$ und $g(x) = x - i \in \mathbb{H}[x]$. Dann gilt $fg = (x + i)(x - i) = x^2 + 1$. Setzt man jedoch $j \in \mathbb{H}$ ein, ergibt sich $f(j)g(j) = (j+i)(j-i) = j^2-ji+ij-i^2 = -1+k+k+1 = 2k$, aber $(fg)(j) = j^2+1 = 0$. D.h., j ist Nullstelle von fg, aber weder von f noch von g, obwohl $\mathbb{H}$ keine Nullteiler hat. Dieses Beispiel zeigt, dass die Kommutativität eine wichtige Voraussetzung ist.

Proposition 26.6 Sei R ein Ring, $f, g \in R[x]$. Dann gilt:

1. $\deg(f + g) \leq \max(\deg f, \deg g)$
2. $\deg(f) \neq \deg(g) \;\Rightarrow\; \deg(f + g) = \max(\deg f, \deg g)$
3. $\deg(fg) \leq \deg(f) + \deg(g)$
4. Wenn f oder g einen Leitkoeffizienten hat, der kein Nullteiler ist, dann gilt sogar $\deg(fg) = \deg(f) + \deg(g)$.

Beweis: als Übung.

BEMERKUNG: Es gilt daher, wenn $f \neq 0$ und der Leitkoeffizient von g kein Nullteiler ist, dass $\deg(fg) = \deg(f) + \deg(g) \geq \deg(g)$.

Korollar 26.7 Sei R ein Integritätsbereich und $f, g \in R[x]$. Dann gilt $\deg(fg) = \deg(f) + \deg(g)$.

Kapitel 27

Einheiten in $R[x]$

Proposition 27.1 Sei R ein Integritätsbereich und $f \in R[x]$. f ist genau dann Einheit in $R[x]$, wenn $f = r \in R$ ein konstantes Polynom ist, sodass r eine Einheit in R ist.

Beweis: Wenn in R gilt, dass $rs = 1$ ist, dann gilt dies auch in $R[x]$, d.h. das Inverse von r in R ist auch Inverses in $R[x]$.
Ist umgekehrt $fg = 1$ in $R[x]$, dann muss zunächst $f, g \neq 0$ gelten, da andernfalls $fg = 0$ wäre. Damit gilt $\deg(f) \geq 0$ und $\deg(g) \geq 0$, und daher wegen $\deg(f) + \deg(g) = \deg(fg) = \deg(1) = 0$ auch $\deg(f) = \deg(g) = 0$, d.h. f, g sind Konstante mit $fg = 1$, also Einheiten in R.

□

Lemma 27.2 Sei $I \trianglelefteq R$. Dann folgt $I[x] \trianglelefteq R[x]$ und $R[x]/I[x] \simeq R/I[x]$, wobei $\varphi : R[x]/I[x] \to R/I[x]$ mit

$$\varphi(a_0 + a_1x + \ldots + a^nx^n + I[x]) = (a_0 + I) + (a_1 + I)x + \ldots + (a_n + I)x^n$$

der Isomorphismus ist.

Beweis: als Übung.

Satz 27.3 *Sei R ein kommutativer Ring mit Eins, $f = a_0 + \ldots + a_nx^n \in R[x]$. Dann ist f genau dann Einheit in $R[x]$, wenn a_0 Einheit in R ist und $\forall i > 0$ $a_i \in \mathrm{Nil}(R)$.*

Beweis: („⇐“) Ist a_0 Einheit in R, dann auch in $R[x]$. Ist a_i nilpotent in R, dann auch a_ix^i in $R[x]$: $a_i^n = 0 \;\Rightarrow\; (a_ix^i)^n = a_i^nx^{in} = 0x^{in} = 0$. Aus Lemma 25.6 folgt, dass $f = a_0 + a_1x + \ldots + a_nx^n$ eine Einheit sein muss.
(„⇒“) Ist f Einheit in $R[x]$, dann ist $f + I[x]$ in jedem Faktorring $R[x]/I[x] = R/I[x]$ auch Einheit.

Insbesondere ist für alle Primideale P $\overline{f} = \overline{a_0} + \overline{a_1}x + \ldots + \overline{a_n}x^n$ (mit $\overline{a_i} = a_i + P$) eine Einheit in $R/P[x]$. Weil P Primideal ist, ist R/P ein Integritätsbereich, und daher sind nur konstante Polynome in R/P Einheiten, also $\overline{a_i} = \overline{0}$ für $i > 0$.
Damit folgt für alle Koeffizienten a_i von f mit $i > 0$, dass $a_i \in P$ für alle Primideale P, daher $\forall i > 0$ $a_i \in \mathrm{Nil}(R)$, weil $\mathrm{Nil}(R)$ der Durchschnitt aller Primideale von R ist.
Schließlich folgt aus $fg = 1$ (wobei $f = \sum a_i x^i$ und $g = \sum b_i x^i$) insbesondere $\sum_{k+l=0} a_k b_l = a_0 b_0 = 1$, also ist a_0 Einheit in R.

□

Kapitel 28

Polynomring in mehreren Unbestimmten

BEMERKUNG: Die Multiplikation von Monomen entspricht der Addition der Exponenten: $x_1^{k_1} \cdot \ldots \cdot x_n^{k_n} \cdot x_1^{l_1} \cdot \ldots \cdot x_n^{l_n} = x_1^{k_1+l_1} \cdot \ldots \cdot x_n^{k_n+l_n}$
$(\mathbb{N}_0, +)$ ist ein Monoid, $\mathbb{N}_0^n = \{(k_1, \ldots, k_n) \mid k_i \in \mathbb{N}_0\}$ ist ein Monoid bezüglich der Addition $(k_1, \ldots, k_n) + (l_1, \ldots, l_n)$; wir schreiben im Folgenden statt $(k_1, \ldots, k_n)$ $x_1^{k_1} \cdot \ldots \cdot x_n^{k_n}$ und erhalten so ein zu $(\mathbb{N}_0^n, +)$ isomorphes Monoid mit der Monoidoperation $x_1^{k_1} \cdot \ldots \cdot x_n^{k_n} \cdot x_1^{l_1} \cdot \ldots \cdot x_n^{l_n} = x_1^{k_1+l_1} \cdot \ldots \cdot x_n^{k_n+l_n}$.
$(\mathbb{N}_0^n, +)$ hat die wichtige Eigenschaft, dass für alle $(k_1, \ldots, k_n) \in \mathbb{N}_0^n$ höchstens endlich viele Paare $(l_1, \ldots, l_n)$, $(m_1, \ldots, m_n)$ existieren, sodass $(l_1, \ldots, l_n) + (m_1, \ldots, m_n) = (k_1, \ldots, k_n)$ ist.

Proposition 28.1 (Monoidring) Sei R ein Ring und $(H, *)$ ein Monoid mit der Eigenschaft, dass für alle $h \in H$ nur endlich viele $k, l \in H$ existieren, sodass $k * l = h$ ist.
Dann ist $R(H)$ mit der Addition $(R(H), +) = \sum_{h \in H}(R, +)$ und der Multiplikation $(r_h)_{h \in H} \cdot (s_h)_{h \in H} = (t_h)_{h \in H}$ mit $t_h = \sum_{k,l \in H, k*l=h} r_k s_l$ ein Ring.
Wenn R ein Einselement hat, dann auch $R(H)$. Wenn R und H kommutativ sind, dann auch $R(H)$. R ist in $R(H)$ eingebettet via $r \mapsto (r_h)_{h \in H}$ mit

$$r_h = \begin{cases} r & h = e \text{ (neutrales Element von } H) \\ 0 & \text{sonst} \end{cases}$$

Beweis: als Übung.

Notation: man schreibt $\sum_{h \in H} r_h h$ für $(r_h)_{h \in H}$. Wenn $h_1, \ldots, h_n$ die (endlich vielen) Elemente von H sind, für die $r_h \neq 0$ ist, dann schreibt man $r_1 h_1 + \ldots + r_n h_n$.

BEMERKUNG: Die Multiplikation von solchen formalen R-Linearkombinationen

von Elementen aus H ergibt sich durch Ausdistribuieren, Multiplikation von Elementen in H und Zusammenfassen der Koeffizienten:

$$(r_1h_1+\ldots+r_nh_n)(s_1g_1+\ldots+s_mg_m) = r_1s_1(h_1*g_1)+r_2s_1(h_2*g_1)+\ldots+r_ns_m(h_n*g_m)$$

BEMERKUNG: $R[x]$ ist der Monoidring $R(\mathbb{N}_0)$, wobei $k \in \mathbb{N}_0$ als x^k geschrieben wird.

Definition 28.2 Sei R ein Ring. Der *Polynomring in mehreren Unbestimmten* $R[x_1, \ldots, x_n]$ ist der Monoidring $R(\mathbb{N}_0^n)$, wobei das Element $(k_1, \ldots, k_n)$ als $x_1^{k_1} \ldots x_n^{k_n}$ geschrieben wird.

Satz 28.3 *Seien R,S Ringe mit Eins, $\varphi : R \to S$ ein Ringhomomorphismus mit $\varphi(1) = 1$ und $s_1, \ldots, s_n \in S$, sodass $s_is_j = s_js_i$ $\forall i, j$ und $\forall i$ $\forall r \in R$ $s_i\varphi(r) = \varphi(r)s_i$. Dann gibt es genau einen Ringhomomorphismus $\overline{\varphi} : R[x_1, \ldots, x_n] \to S$ mit $\overline{\varphi}|_R = \varphi$ und $\overline{\varphi}(x_i) = s_i$ $(i = 1, \ldots, n)$, nämlich*

$$\overline{\varphi}\left(\sum_{(k_1,\ldots,k_n)\in\mathbb{N}_0^n} r_{(k_1,\ldots,k_n)}x_1^{k_1}\ldots x_n^{k_n}\right) = \sum_{(k_1,\ldots,k_n)\in\mathbb{N}_0^n} \varphi(r_{(k_1,\ldots,k_n)})s_1^{k_1}\ldots s_n^{k_n}$$

Beweis: $\overline{\varphi}$ muss diese Form haben, wenn es ein Ringhomomorphismus sein soll. Es bleibt zu zeigen, dass es sich tatsächlich um einen Homomorphismus handelt:
Bezüglich + gilt die Bedingung offensichtlich, es bleibt die Bedingung für $\cdot$. Sei dazu im Folgenden $\overline{k} = (k_1, \ldots, k_n)$:

$$\begin{aligned}
\overline{\varphi}(fg) &= \overline{\varphi}\left(\left(\sum_{\overline{k}} a_{\overline{k}}x_1^{k_1}\ldots x_n^{k_n}\right)\left(\sum_{\overline{l}} b_{\overline{l}}x_1^{l_1}\ldots x_n^{l_n}\right)\right) \\
&= \overline{\varphi}\left(\sum_{\overline{k}}\sum_{\overline{l}+\overline{m}=\overline{k}} a_{\overline{l}}b_{\overline{m}}x_1^{k_1}\ldots x_n^{k_n}\right) \\
&= \sum_{\overline{k}}\varphi\left(\sum_{\overline{l}+\overline{m}=\overline{k}} a_{\overline{l}}b_{\overline{m}}\right)s_1^{k_1}\ldots s_n^{k_n} \\
&= \sum_{\overline{k}}\sum_{\overline{l}+\overline{m}=\overline{k}} \varphi(a_{\overline{l}})\varphi(b_{\overline{m}})s_1^{k_1}\ldots s_n^{k_n} \\
&= \sum_{\overline{k}}\sum_{\overline{l}+\overline{m}=\overline{k}} \varphi(a_{\overline{l}})s_1^{l_1}\ldots s_n^{l_n}\varphi(b_{\overline{m}})s_1^{m_1}\ldots s_n^{m_n} \\
&= \left(\sum_{\overline{k}}\varphi(a_{\overline{k}})s_1^{k_1}\ldots s_n^{k_n}\right)\left(\sum_{\overline{l}}\varphi(b_{\overline{l}})s_1^{l_1}\ldots s_n^{l_n}\right)
\end{aligned}$$

$$\begin{aligned} &= \overline{\varphi}\Big(\sum_{\overline{k}} a_{\overline{k}} x_1^{k_1} \dots x_n^{k_n}\Big)\overline{\varphi}\Big(\sum_{\overline{l}} b_{\overline{l}} x_1^{l_1} \dots x_n^{l_n}\Big) \\ &= \overline{\varphi}(f)\overline{\varphi}(g) \end{aligned}$$

□

Satz 28.4 *Sei R ein Ring mit Eins, dann gilt*

1. $(R[x_1, \dots, x_k])[x_{k+1}, \dots, x_n] \simeq R[x_1, \dots, x_n]$
2. *Für jede Permutation $\pi \in S_n$ ist* $R[x_1, \dots, x_n] \simeq R[x_{\pi(1)}, \dots, x_{\pi(n)}]$

Beweis:

1. Sei $\varphi : R[x_1, \dots, x_k] \to R[x_1, \dots, x_n]$ die Einbettung von $R[x_1, \dots, x_k]$ in $R[x_1, \dots, x_n]$: $\sum a_{(l_1,\dots,l_k)} x_1^{l_1} \cdot \dots \cdot x_k^{l_k} \mapsto \sum a_{(l_1,\dots,l_n)} x_1^{l_1} \cdot \dots \cdot x_k^{l_k}$, wobei für alle $(l_1, \dots, l_n)$ mit einem $l_i \neq 0$ für ein $i > k$ $a_{(l_1,\dots,l_n)} = 0$ sei.
   Es gibt einen Einsetzhomomorphismus $\overline{\varphi} : (R[x_1, \dots, x_k])[x_{k+1}, \dots, x_n] \to R[x_1, \dots, x_n]$ mit $\overline{\varphi}|_{R[x_1,\dots,x_k]} = \varphi$ und $\overline{\varphi}(x_i) = x_i$ für $i = k+1, \dots, n$.
   Dieser ist gegeben durch
   $$\overline{\varphi}\Big(\sum_{(l_{k+1},\dots,l_n)} \Big(\sum_{(m_1,\dots,m_k)} a_{(m_1,\dots,m_k)}^{[l_{k+1},\dots,l_n]} x_1^{m_1} \dots x_k^{m_k}\Big) x_{k+1}^{l_{k+1}} \dots x_n^{l_n}\Big) = \sum_{(l_1,\dots,l_n)} a_{(l_1,\dots,l_n)} x_1^{l_1} \dots x_n^{l_n}$$
   wobei $(l_1, \dots, l_n) = (m_1, \dots, m_k, l_{k+1}, \dots, l_n)$ sei.
   $\overline{\varphi}$ ist offenbar surjektiv, die Injektivität folgt leicht: wenn
   $$\sum_{(l_1,\dots,l_n)} a_{(l_1,\dots,l_n)} x_1^{l_1} \dots x_n^{l_n} = 0$$
   ist, dann muss für alle n-tupel $(l_1, \dots, l_n)$ $a_{(l_1,\dots,l_n)} = 0$ sein, damit ist jedoch auch
   $$\sum_{(l_{k+1},\dots,l_n)} \Big(\sum_{(m_1,\dots,m_k)} a_{(m_1,\dots,m_k)}^{[l_{k+1},\dots,l_n]} x_1^{m_1} \dots x_k^{m_k}\Big) x_{k+1}^{l_{k+1}} \dots x_n^{l_n} = 0$$
   also $\operatorname{Ker} \overline{\varphi} = \{0\}$.
2. Analog definiert der Einsetzhomomorphismus zu $\psi = \mathrm{id}_R : R \to R$ mit $\overline{\psi}(x_i) = x_{\pi(i)}$ einen Isomorphismus $\overline{\psi} : R[x_1, \dots, x_n] \to R[x_{\pi(1)}, \dots, x_{\pi(n)}]$.

□

Korollar 28.5

- $R[x_1, \dots, x_n] \simeq R[x_1][x_2] \dots [x_n]$
- $R[x_1, \dots, x_n] \simeq R[x_{k+1}, \dots, x_n][x_1, \dots, x_n]$

Kapitel 29

Teilbarkeit in kommutativen Ringen mit Eins

Definition 29.1 Sei R ein kommutativer Ring mit Eins, $R \neq \{0\}$, $a, b \in R$. a *teilt* b (geschrieben $a \mid b$), wenn es ein $c \in R$ mit $ac = b$ gibt. a heißt dann ein *Teiler* von b, b ein *Vielfaches* von a.

Bemerkung: Es gelten folgende Beziehungen:

1. $\forall a \in R$: $a \mid 0$, da $a \cdot 0 = 0$.
2. $\forall a \in R$: $1 \mid a$, da $1 \cdot a = a$. Auch für alle $b \in E(R)$ gilt $\forall a \in R$: $b \mid a$, da $b \cdot (b^{-1}a) = a$.
3. a ist Einheit $\iff a \mid 1$
4. $a \mid b \wedge b \mid c \implies a \mid c$ ($ad = b$, $bd' = c \Rightarrow add' = c$)

Proposition 29.2 Sei R kommutativer Ring mit Eins, $R \neq \{0\}$, $a, b \in R$. Dann gilt

1. $a \mid b \iff (b) \subseteq (a)$
2. Wenn b Einheit ist und $a \mid b$, dann ist a Einheit (jeder Teiler einer Einheit ist eine Einheit).
3. Wenn a Nullteiler ist und $a \mid b$, dann ist b Nullteiler (jedes Vielfache eines Nullteilers ist ein Nullteiler).

Beweis:

1. In einem kommutativen Ring mit Eins gilt $(a) = Ra = \{ra \mid r \in R\} = \{b \in R \mid a \mid b\}$, also $a \mid b \Rightarrow b \in (a)$ und damit $(b) \subseteq (a)$. Wenn umgekehrt $(b) \subseteq (a)$ ist, dann folgt $b \in (a) = Ra$ und damit $a \mid b$.

2. $bb' = 1$, $b = ad \Rightarrow adb' = 1$, also ist a Einheit.

3. $aa' = 0$ für ein $a' \neq 0$, $b = ad \Rightarrow ba' = ada' = aa'd = 0$, also ist b Nullteiler.

□

Definition 29.3 Sei R ein kommutativer Ring mit Eins und $a, b \in R$. Wir definieren

- $a \sim b \ :\Leftrightarrow \ (a \mid b \wedge b \mid a)$ („a und b teilen einander gegenseitig“)
- $a \approx b \ :\Leftrightarrow \ \exists$ Einheit u: $b = ua$ („a und b sind *assoziiert*“)

Proposition 29.4 Sei R ein kommutativer Ring mit Eins, $a, b \in R$.

1. $\sim$ und $\approx$ sind Äquivalenzrelationen.
2. $a \approx b \Longrightarrow a \sim b$
3. Ist R Integritätsbereich, gilt sogar $a \approx b \Longleftrightarrow a \sim b$.
4. a Einheit, $a \sim b \Longrightarrow b$ Einheit; a Nullteiler, $a \sim b \Longrightarrow b$ Nullteiler.

Beweis:

1. - Reflexivität: $a \mid a$ ist erfüllt, und 1 ist eine Einheit, für die $a = 1a$ gilt.
   - Symmetrie: für $\sim$ offensichtlich; gilt $b = ua$ für eine Einheit u, dann ist $a = u^{-1}b$ für die Einheit u^{-1}.
   - Transitivität: für $\sim$ klar, weil $\mid$ transitiv ist. Gilt $b = ua$, $c = vb$ für Einheiten u, v, dann folgt $c = vua$, und vu ist Einheit.
2. $b = ua \Rightarrow a \mid b$, $a = u^{-1}b \Rightarrow b \mid a$; insgesamt also $a \sim b$.
3. Es gelte $a \mid b$ und $b \mid a$. Falls $b = 0$ ist, folgt $a = bc = 0$, also $a = b$ und damit $a \approx b$. Sei andernfalls $ad = b$ und $bc = a$. Dann gilt $b = ad = bcd$ $\Rightarrow b(1 - cd) = 0$, und weil R als Integritätsbereich keine Nullteiler enthält, muss $cd = 1$ sein. Also sind c, d Einheiten und damit $a \approx b$.
4. folgt aus den Punkten 2. und 3. der vorigen Proposition.

□

Korollar 29.5 Sei R ein kommutativer Ring mit Eins und $a, b \in R$. Dann gilt $(a) = (b) \Leftrightarrow a \sim b$. Wenn R ein Integritätsbereich ist, dann gilt auch $(a) = (b) \Leftrightarrow a \approx b$.

Beweis: Diese Tatsache folgt aus $(a) \subseteq (b) \Leftrightarrow b \mid a$.

Definition 29.6 Sei R ein kommutativer Ring mit Eins. $p \in R$ heißt *prim*, wenn $p \neq 0$ und p keine Einheit ist und $p \mid ab \Rightarrow p \mid a \vee p \mid b$ erfüllt.
$c \in R$ heißt *irreduzibel*, wenn $c \neq 0$ und c keine Einheit ist und $c = ab \Rightarrow$ (a Einheit $\vee\, b$ Einheit) gilt.

Bemerkung: Ist p prim und $p \mid a_1 \dots a_n$, dann gibt es ein i, sodass $p \mid a_i$ (folgt leicht mit Induktion nach n).

Satz 29.7 *Sei R ein Integritätsbereich, $p \in R$. Dann gilt:*

$$p \text{ prim} \implies p \text{ irreduzibel}$$

Beweis: Es sei p prim und $p = ab$. Dann gilt insbesondere $p \mid ab$ und damit $p \mid a$ oder $p \mid b$, o.B.d.A. gelte ersteres. Dann ist $pd = a$ für ein $d \in R$, also $p = ab = pdb \Rightarrow p(1 - db) = 0$. Weil p kein Nullteiler ist, muss $1 - db = 0$, also $db = 1$ sein. Damit ist jedoch b eine Einheit.
Folglich ist p irreduzibel.

□

Proposition 29.8 Sei R ein kommutativer Ring mit Eins, $p, c \in R$. Dann gilt:

- p prim $\Longleftrightarrow$ (p) ist Primideal $\neq \{0\}$.
- c irreduzibel $\Longleftrightarrow$ $(c) \neq \{0\}$, (c) ist maximal unter den Hauptidealen $\neq R$ (d.h. $\forall d \in R : (c) \subsetneq (d) \Rightarrow (d) = R$).

Beweis: als Übung.

Lemma 29.9 Sei R ein kommutativer Ring mit Eins, $p, p', c, c' \in R$.

- Wenn p prim ist und $p \sim p'$, dann ist p' prim.
- Wenn c irreduzibel ist und $c \sim c'$, dann ist c' irreduzibel.

Beweis: Sei p prim und $p \sim p'$. Weil p weder Einheit noch Nullteiler ist, trifft dies auch auf p' zu. Wenn $p' \mid ab$, dann muss wegen $p \mid p'$ auch $p \mid ab$ gelten, somit $p \mid a$ oder $p \mid b$. Wegen $p' \mid p$ folgt daraus aber weiters, dass $p' \mid a$ oder $p' \mid b$ gilt. Also ist p' prim.
Sei c irreduzibel und $c \sim c'$. Wiederum kann c' weder Einheit noch Nullteiler sein. Angenommen, es sei $c' = ab$, wobei weder a noch b Einheit ist. Es ist $c' = cd$ und $c = cd'$, daher $c = cd'd \Rightarrow c(1 - d'd) = 0$. Weil c kein Nullteiler ist, muss somit $d'd = 1$ sein, also sind d, d' Einheiten. Aus $cd = c' = ab$ folgt dann $c = abd'$. Weil a keine Einheit und c irreduzibel ist, muss daher bd' Einheit sein. Weil d Einheit ist, muss damit auch $bd'd = b$ Einheit sein, was einen Widerspruch darstellt. Also ist c' irreduzibel.

□

Kapitel 30

ZPE-Ringe

Definition 30.1 Ein Integritätsbereich R heißt *ZPE-Ring*, wenn

- Für alle $a \in R$, $a \neq 0$, a keine Einheit, gibt es $n \in \mathbb{N}$ und irreduzible $c_1, \ldots, c_n \in R$, sodass $a = c_1 \cdot \ldots \cdot c_n$. D.h., jedes $a \neq 0$, das keine Einheit ist, ist Produkt von Irreduziblen.
- Wenn $c_1, \ldots, c_n$ und $d_1, \ldots, d_m$ irreduzibel sind und $c_1 \cdot \ldots \cdot c_n = d_1 \cdot \ldots \cdot d_m$ gilt, dann ist $n = m$ und es gibt eine Permutation $\pi \in S_n$, sodass $c_i \approx d_{\pi(i)}$ $(i = 1, \ldots, n)$. D.h., die Darstellung als Produkt von Irreduziblen ist eindeutig bis auf die Reihenfolge und Assoziiertheit.

Bemerkung: ZPE steht für „Zerlegung in Primfaktoren eindeutig“.

Beispiel: $\mathbb{Z}$ ist ein ZPE-Ring, $K[x_1, \ldots, x_n]$ (für einen Körper K) ist ein ZPE-Ring.

Proposition 30.2 Sei R ein ZPE-Ring, $p \in R$. Dann gilt: p prim $\iff$ p irreduzibel.

Beweis: („$\Rightarrow$“) ist bereits bekannt, wir zeigen nun die Umkehrung. Sei dazu p irreduzibel (also kein Nullteiler und keine Einheit) und $a, b \in R$ mit $p \mid ab$. Dann ist $pd = ab$ für ein $d \in R$. Wäre a eine Einheit, würde $pda^{-1} = b$, also $p \mid b$ gelten, ebenso $p \mid a$, wenn b Einheit wäre. Sei daher jetzt weder a noch b Einheit. Wäre nun d eine Einheit, dann müsste $p = (d^{-1}a)b$ gelten, wobei weder $d^{-1}a$ noch b Einheit ist, im Widerspruch zur Irreduzibilität.
Damit haben a,b,d Darstellungen als Produkte irreduzibler Faktoren: $a = a_1 \ldots a_k$, $b = b_1 \ldots b_l$, $d = d_1 \ldots d_n$. Es folgt dann $pd_1 \ldots d_n = a_1 \ldots a_k b_1 \ldots b_l$, also $n + 1 = k + l$, und nach Umordnung sind die Faktoren der linken und rechten Seite paarweise assoziiert. Insbesondere existiert ein a_i mit $p \approx a_i$ oder ein b_j mit $p \approx b_j$, o.B.d.A. sei ersteres der Fall. Dann gilt insbesondere

$p \mid a_i$ und damit $p \mid a$.
Also folgt in jedem Fall $p \mid ab \;\Rightarrow\; p \mid a \vee p \mid b$, d.h., p ist prim.

□

Satz 30.3 *Sei R ein Integritätsbereich. Dann gilt: R ist genau dann ZPE-Ring, wenn*

$\forall a \in R,\ a \neq 0,\ a$ *keine Einheit,* $\exists n \in \mathbb{N},\ p_1, \ldots, p_n$ *prim, sodass* $a = p_1 \ldots p_n$

Beweis: Ist R ein ZPE-Ring, dann folgt die Behauptung aus der Definition und der vorangegangenen Proposition.
Es gelte umgekehrt die Bedingung der rechten Seite. Weil prime Elemente auch irreduzibel sind, ist die Existenz einer Darstellung als Produkt irreduzibler Elemente gegeben, zu zeigen bleibt die Eindeutigkeit. Seien dazu $c_1, \ldots, c_n, d_1, \ldots, d_m$ irreduzibel, sodass $c_1 \ldots c_n = d_1 \ldots d_m$. Wir wissen, dass es prime Elemente $p_1, \ldots, p_k$ gibt, sodass $p_1 \ldots p_k = c_1 \ldots c_n = d_1 \ldots d_m$. Wir zeigen nun, dass $k = n$ ist und eine Permutation $\sigma \in S_n$ existiert, sodass $p_i \approx c_{\sigma(i)}$, und zwar durch Induktion nach $\max(k, n)$:

- Ist $\max(k, n) = 1$, dann gilt $p_1 = c_1$, also ist die Behauptung erfüllt.
- $p_1 \mid c_1 \ldots c_n$ und p_1 ist prim, also existiert ein i_1, sodass $p_1 \mid c_{i_1}$. Daher ist $c_{i_1} = p_1 u$. c_{i_1} ist dabei irreduzibel und p_1 keine Einheit, also muss u Einheit sein und damit $c_{i_1} \approx p_i$. Es folgt $p_1 \ldots p_k = p_1 u c_{i_1} \ldots c_{i_1-1} c_{i_1+1} \ldots c_n$. Man kann kürzen und erhält $p_2 \ldots p_k = (u c_{i_1}) \ldots c_{i_1-1} c_{i_1+1} \ldots c_n$. Links stehen $k-1$ prime Faktoren, rechts $n-1$ irreduzible Faktoren, also kann man die Induktionsvoraussetzung anwenden:
  Es folgt $k - 1 = n - 1 \;\Rightarrow\; k = n$ und es gibt eine bijektive Funktion $\sigma : \{2, \ldots, k\} \to \{1, \ldots, n\} \setminus \{i_1\}$ mit $p_i \approx c_{\sigma(i)}$. Erweitert man diese durch $\sigma(1) = i_1$, dann ist $\sigma \in S_n$, und es gilt weiterhin $p_i \approx c_{\sigma(i)}$.

Analog ist auch $m = k = n$, und es gibt ein $\rho \in S_m$, sodass $p_i \approx d_{\rho(i)}$, daher $c_i \approx p_{\sigma^{-1}(i)} \approx d_{\rho\sigma^{-1}(i)}$ und $\rho\sigma^{-1} \in S_n$.

□

Proposition 30.4 (Primfaktorzerlegung) Sei R ein ZPE-Ring, $\mathbb{P}$ ein Repräsentantensystem der Assoziiertenklassen von primen Elementen von R (d.h. $\forall q \in R$, q prim, $\exists! p \in \mathbb{P}$ mit $p \approx q$).
Dann hat jedes $a \neq 0$ eine eindeutige Darstellung in der Form

$$a = u_a \cdot \prod_{p \in \mathbb{P}} p^{\nu_p(a)}$$

wobei u_a Einheit ist, $\nu_p(a) \in \mathbb{N}_0$ und nur endlich viele $\nu_p(a) \neq 0$ sind.
Dabei ist $\nu_p(a)$ nur von der Assoziiertenklasse von p (und nicht von der Wahl des Repräsentantensystems $\mathbb{P}$) abhängig. D.h., wenn $\mathbb{P}'$ ein anderes Repräsentationsystem ist und $a = u'_a \cdot \prod_{p' \in \mathbb{P}'} p'^{\nu_{p'}(a)}$, dann gilt $p \approx p' \Rightarrow \nu_p(a) = \nu_{p'}(a)$.

Beweis: als Übung.

Bemerkung: Es gelte die Konvention $\prod_{p \in \mathbb{P}} p^0 = 1$, d.h. unendliche Produkte von 1 sind 1.

Bemerkung: Es gilt $a \mid b \Leftrightarrow \forall p \in \mathbb{P}\ \nu_p(a) \leq \nu_p(b)$ und $a \approx b \Leftrightarrow \forall p \in \mathbb{P}\ \nu_p(a) = \nu_p(b)$.

Proposition 30.5 Sei R ein ZPE-Ring, $a \in R$, $a \neq 0$ keine Einheit, dann gibt es eindeutig bestimmte Hauptideale $(p_1), \ldots, (p_n)$ mit $(a) = (p_1) \ldots (p_n)$.

Beweis: als Übung.

Definition 30.6 Sei R ein Ring, $\mathcal{I}$ eine Menge von Idealen in R. R erfüllt die *aufsteigende Kettenbedingung* für Ideale aus $\mathcal{I}$, wenn für alle Folgen $I_n,\ n \in \mathbb{N}$ von Idealen $I_n \in \mathcal{I}$ mit $I_1 \subseteq I_2 \subseteq \ldots \subseteq I_n \ldots$ ein $N \in \mathbb{N}$ existiert, sodass $I_n = I_N\ \forall n \geq N$.

Satz 30.7 *Jeder ZPE-Ring erfüllt die aufsteigende Kettenbedigung für Hauptideale.*

Beweis: Wir wissen $a \mid b \Leftrightarrow (b) \subseteq (a)$ und $a \approx b \Leftrightarrow (b) = (a)$ bzw. $(a \mid b \wedge a \not\approx b) \Leftrightarrow (b) \subsetneq (a)$. Eine aufsteigende Kette von Hauptidealen $(a_1) \subseteq (a_2) \subseteq \ldots$ entspricht daher einer absteigenden Teilerkette $a_1, a_2, \ldots$ (d.h. $\ldots \mid a_n \mid a_{n-1} \mid \ldots \mid a_2 \mid a_1$). Jedes a_i teilt a_1, aber a_1 hat nur endlich viele nichtassoziierte Teiler, also gibt es nur endlich viele verschiedene Hauptideale unter den (a_i).

□

Satz 30.8 *Ein Integritätsbereich R ist genau dann ZPE-Ring, wenn R die aufsteigende Kettenbedingung für Hauptideale erfüllt und jedes irreduzible Element prim ist.*

Beweis: Es wurde bereits gezeigt, dass jeder ZPE-Ring die beiden Bedingungen erfüllt. Sei nun R ein beliebiger Integritätsbereich, der beide Eigenschaften erfüllt. Sei

$S = \{a \in R \mid a \neq 0,\ a \text{ keine Einheit}, \nexists c_1, \ldots, c_n \text{ irreduzibel mit } a = c_1 \ldots c_n\}$

Es ist zu zeigen, dass $S = \emptyset$. Angenommen, $a \in S$. Wenn $a = bc$, dann ist $b \in S$ oder $c \in S$ ($a \neq 0 \Rightarrow b, c \neq 0$; wären b, c Einheiten oder Produkte von Irreduziblen, dann auch a, also wäre $a \notin S$). Wegen $a \in S$ ist a insbesondere nicht irreduzibel, also existieren b, c (beide keine Einheiten), sodass $a = bc$ und $a \not\approx b$, $a \not\approx c$.
Damit können wir induktiv eine Folge $a = a_0, a_1, \ldots$ definieren, sodass $a_i \in S$, $a_{n+1} \mid a_n$, $a_{n+1} \not\approx a_n$. Es ergibt sich eine aufsteigende Hauptidealkette $(a_0) \subsetneqq (a_1) \subsetneqq \ldots$, im Widerspruch zur ersten Bedingung. Also gibt es für jedes $a \neq 0$, das keine Einheit ist, eine Darstellung der Form $a = c_1 \ldots c_n$ mit irreduziblen c_i. Wegen der zweiten Bedingung sind die c_i auch prim, also ist nach Satz 30.3 R ein ZPE-Ring.

□

Definition 30.9 Sei R ein Integritätsbereich. R heißt *Hauptidealbereich*, wenn $\forall I \trianglelefteq R \; \exists r \in R$ mit $I = (r)$ (Ein beliebiger Ring, in dem jedes Ideal ein Hauptideal ist, heißt *Hauptidealring*).

Bemerkung: In einem kommutativen Ring mit Eins gilt für $p, c \in R$:

- p prim $\iff$ (p) ist Primideal $\neq \{0\}$.
- c irreduzibel $\iff$ $(c) \neq \{0\}$, (c) ist maximal unter den Hauptidealen $\neq R$.

Daher gilt in einem Hauptidealbereich:

$$c \text{ irreduzibel} \iff (c) \text{ ist maximales Ideal } \neq \{0\}$$

Beispiel: $\mathbb{Z}$ ist ein Hauptidealbereich, $K[x]$ ist ein Hauptidealbereich für jeden Körper K (wird noch gezeigt).

Beispiel: $\mathbb{Z}[x]$, $K[x, y]$ (oder allgemein $K[x_1, \ldots, x_n]$ für $n > 1$) für einen Körper K sind ZPE-Ringe, aber keine Hauptidealbereiche.

Satz 30.10 *Jeder Hauptidealbereich R ist ein ZPE-Ring.*

Beweis: Nach Voraussetzung ist R ein Integritätsbereich. Wir zeigen, dass R die aufsteigende Kettenbedigung für Hauptideale erfüllt und jedes irreduzible Element auch prim ist:

- Sei $(a_1) \subseteq (a_2) \subseteq \ldots$ eine Kette von Hauptidealen und $I = \bigcup_{n \in \mathbb{N}} (a_n)$. Die Vereinigung einer Kette von Idealen ist (wie bereits gezeigt) ein Ideal, daher ist $I = (r)$ für ein $r \in R$. Weil $r \in \bigcup_{n \in \mathbb{N}} (a_n)$ ist, muss

es ein n_0 geben, sodass $r \in (a_{n_0})$. Dann gilt $\forall n \geq n_0\ r \in (a_n)$, also $\bigcup_{n\in\mathbb{N}}(a_n) = I = (r) \subseteq (a_n)$ für alle $n \geq n_0$ und damit $(a_n) = I$ für alle $n \geq n_0$, d.h. R erfüllt die aufsteigende Kettenbedingung für Hauptideale.

- Sei c irreduzibel. Dann ist $c \neq 0$ und keine Einheit. Also $(c) \neq \{0\}$ und $(c) \neq R$. Außerdem ist (c) ein maximales Ideal und daher ein Primideal. Damit muss c auch prim sein.

Es folgt, dass R ein ZPE-Ring ist.

□

Definition 30.11 Sei R ein kommutativer Ring mit Eins, $a_1, \ldots, a_n \in R$. $d \in R$ heißt *größter gemeinsamer Teiler* von $a_1, \ldots, a_n$, wenn gilt:

- $d \mid a_i$ für alle i.
- Gilt für ein $c \in R$ $c \mid a_i$ für alle i, dann folgt $c \mid d$.

Bemerkung: Wenn d größter gemeinsamer Teiler von $a_1, \ldots, a_n$ ist und $d \sim d'$, dann ist auch d' größter gemeinsamer Teiler von $a_1, \ldots, a_n$. Wenn umgekehrt d, d' beide größte gemeinsame Teiler sind, dann gilt $d \sim d'$.
Der größte gemeinsame Teiler ist also bis auf $\sim$ (gegenseitiges Teilen) eindeutig bestimmt, man schreibt $d \sim \mathrm{ggT}(a_1, \ldots, a_n)$ oder auch $\mathrm{ggT}(a_1, \ldots, a_n) = d$, obwohl d nur ein möglicher ggT ist.

Bemerkung: d ist ggT von $a_1, \ldots, a_n$ genau dann, wenn d ein Erzeuger des kleinsten Hauptideals ist, das $a_1, \ldots, a_n$ enthält, d.h. $(a_1, \ldots, a_n) \subseteq (d)$ und $(a_1, \ldots, a_n) \subseteq (c) \ \Rightarrow\ (d) \subseteq (c)$.
Der ggT muss aber nicht immer existieren!

Proposition 30.12 Sei R ein ZPE-Ring und $a_1, \ldots, a_n \in R$. Dann existiert ein $\mathrm{ggT}(a_1, \ldots, a_n)$. Wenn $a_i = u_i \cdot \prod_{p\in\mathbb{P}} p^{\nu_p(a_i)}$ die Primfaktorzerlegung von a_i ist, dann ist $d = \prod_{p\in\mathbb{P}} p^{\min_i \nu_p(a_i)}$ ein ggT von $a_1, \ldots, a_n$. Er ist bis auf Assoziativität eindeutig.

Beweis: Sei d wie oben gegeben. Dann gilt $d \mid a_j$ für alle j, da $\forall p \in \mathbb{P}\ \nu_p(d) = \min_i \nu_p(a_i) \leq \nu_p(a_j)$; wenn für ein $c \in R$ $c \mid a_i\ \forall i$ gilt, dann folgt $\forall i\ \forall p \in \mathbb{P}\ \nu_p(c) \leq \nu_p(a_i)$, also $\forall p \in \mathbb{P}\ \nu_p(c) \leq \min_i \nu_p(a_i) \leq \nu_p(d)$, daher $c \mid d$.
Der ggT ist, falls er existiert, bis auf $\sim$ eindeutig. In Integritätsbereichen, insbesondere also in ZPE-Ringen, ist dies gleichbedeutend dazu, dass der ggT eindeutig bis auf $\approx$ ist.

□

Lemma 30.13 Sei R ein kommutativer Ring mit Eins, $a_1, \ldots, a_n, d \in R$. $(d) = (a_1, \ldots, a_n)$ gilt genau dann, wenn d ggT von $a_1, \ldots, a_n$ ist und $r_1, \ldots, r_n$ mit $d = r_1 a_1 + \ldots + r_n a_n$ existieren.

Beweis: In kommutativen Ringen mit Eins ist $(a_1, \ldots, a_n) = a_1 R + \ldots + a_n R = Ra_1 + \ldots + Ra_n$. Ist dies ein Hauptideal (d), dann muss d ggT sein (weil dann (d) jedenfalls auch das kleinste Hauptideal ist, das $a_1, \ldots, a_n$ enthält), und d lässt sich als Linearkombination von $a_1, \ldots, a_n$ darstellen.
Es sei umgekehrt $d = \mathrm{ggT}(a_1, \ldots, a_n)$ und $d = r_1 a_1 + \ldots + r_n a_n$. Dann ist $d \in Ra_1 + \ldots + Ra_n = (a_1, \ldots, a_n)$ und damit $(d) \subseteq (a_1, \ldots, a_n)$. Da d ggT ist, gilt insbesondere $d \mid a_i$ für alle i, daher $a_i \in (d) = Rd$, damit $\{a_1, \ldots, a_n\} \subseteq (d)$ und schließlich $(a_1, \ldots, a_n) \subseteq (d)$, zusammen also $(a_1, \ldots, a_n) = (d)$.

□

Beispiel: In den ZPE-Ringen $\mathbb{Z}[x]$ und $K[x, y]$ ist der ggT im Allgemeinen nicht als Linearkombination darstellbar. So sind etwa $2, x \in \mathbb{Z}[x]$ mit $\mathrm{ggT}(2, x) = 1$, aber 1 ist nicht in der Form $2p + qx$ darstellbar. Ebenso sind $x, y \in K[x, y]$ mit $\mathrm{ggT}(x, y) = 1$, aber 1 ist nicht in der Form $px + qy$ darstellbar.

Korollar 30.14 Sei R ein Hauptidealbereich, $a_1, \ldots, a_n \in R$. Dann existiert ein $\mathrm{ggT}(a_1, \ldots, a_n)$, nämlich jedes d mit $(d) = (a_1, \ldots, a_n)$. Jeder solche ggT lässt sich als R-Linearkombination von $a_1, \ldots, a_n$ darstellen.

Kapitel 31

Euklidische Ringe, Hauptidealringe

Definition 31.1 Sei R ein kommutativer Ring. R heißt *Euklidischer Ring*, wenn es eine „*Rangfunktion*“ $\rho : R \setminus \{0\} \to \mathbb{N}_0$ gibt, sodass gilt:
$\forall a, b \in R$ mit $b \neq 0$ $\exists q, r \in R$ mit $a = qb + r$ und $r = 0 \vee \rho(r) < \rho(b)$ („Division mit Rest“). Ein Integritätsbereich, der zugleich Euklidischer Ring ist, heißt *Euklidischer Bereich*.

Bemerkung: Wenn $u \neq 0$ ein Element eines Euklidischen Ringes derart ist, dass $\rho(u) = \min\{\rho(r) \,|\, r \in R \setminus \{0\}\}$, dann ist u eine Einheit (wir werden sehen, dass jeder Euklidische Ring ein Einselement hat). Wenn die Rangfunktion die Eigenschaft $\rho(ab) \geq \rho(a)$ erfüllt, gilt auch die Umkehrung, d.h. für jede Einheit u gilt $\rho(u) = \min\{\rho(r) \,|\, r \in R \setminus \{0\}\}$. Diese Bedingung wird oft in der Definition von Euklidischen Bereichen gefordert.

Beispiel: $\mathbb{Z}$ ist ein Euklidischer Bereich, $\rho(n) = |n|$; für $a, b \in \mathbb{Z}$ mit $b \neq 0$ gibt es stets $q, r \in \mathbb{Z}$ mit $a = qb + r$ und $r = 0 \vee |r| < |b|$.
Man sieht, dass q, r nicht eindeutig sein müssen, z.B. ist bei der Division von 10 durch 3 $10 = 3 \cdot 3 + 1$ oder $10 = 4 \cdot 3 - 2$; nicht einmal, wenn man absolut kleinsten Rest fordert, ist die Eindeutigkeit gegeben. So ist etwa $9 = 1 \cdot 6 + 3 = 2 \cdot 6 - 3$.

Beispiel: $\mathbb{Z}[i], \mathbb{Z}[\sqrt{2}]$ und $\mathbb{Z}[\sqrt{-2}]$ sind Euklidische Ringe ($\mathbb{Z}[c]$ bezeichnet dabei den von $\mathbb{Z} \cup \{c\}$ erzeugten Unterring von $\mathbb{C}$) bezüglich folgender Rangfunktionen:

- $\rho(a + bi) = a^2 + b^2$ für $\mathbb{Z}[i]$
- $\rho(a + b\sqrt{2}) = |a^2 - 2b^2|$ für $\mathbb{Z}[\sqrt{2}]$

- $\rho(a + b\sqrt{-2}) = a^2 + 2b^2$ für $\mathbb{Z}[\sqrt{-2}]$

Satz 31.2 *Jeder Euklidische Ring ist ein Hauptidealring mit Eins.*

Beweis: Sei R ein Euklidischer Ring und $I \trianglelefteq R$. Wenn $I = \{0\}$, dann ist $I = (0)$. Sei also $I \neq \{0\}$. Wähle $b \in I$ so, dass $\rho(b) = \min\{\rho(a) \mid a \in I, a \neq 0\}$ (dieses Minimum existiert, da es ein $a \in I$ mit $a \neq 0$ gibt und somit die Menge nichtleer ist).
Sei jetzt $a \in I$ beliebig. Wir führen eine Division mit Rest durch: $a = qb + r$, wobei $r = 0$ oder $\rho(r) < \rho(b)$ ist. Da $r = a - qb$ in I liegt, muss wegen der Minimalität von $\rho(b)$ ersteres gelten, also $r = 0$ und damit $a = qb$. Es folgt $I \subseteq Rb \subseteq I$, also $I = Rb = (b)$, d.h. jedes Ideal ist ein Hauptideal.
Auch für $I = R$ gibt es ein $e \in R$, sodass $Re = R$. Sei e' derart, dass $e'e = e$ ist. Dann folgt für ein $r \in R$: $\exists r' \in R$ mit $r'e = r$, und damit $e'r = e'r'e = r'e'e = r'e = r$. Also ist e' Einselement in R.

□

Bemerkung: Es gelten die Implikationen:

- Euklidischer Bereich ⇒ Hauptidealbereich
- Hauptidealbereich ⇒ ZPE-Ring

Bezüglich des ggT gilt:

1. In einem ZPE-Ring existiert $\mathrm{ggT}(a_1, \ldots, a_n)$ immer.
2. In einem Hauptidealbereich existiert der ggT und lässt sich als Linearkombination anschreiben.
3. In einem Euklidischen Bereich haben wir einen effektiven Algorithmus, um $d = \mathrm{ggT}(a_1, \ldots, a_n)$ und $r_1, \ldots, r_n$ mit $d = r_1a_1 + \ldots + r_na_n$ zu finden, nämlich den Euklidischen Algorithmus, der im Folgenden vorgestellt wird.

Euklidischer Algorithmus:

Seien R ein Euklidischer Ring, $a, b \in R$ und $b \neq 0$. Wir definieren induktiv Folgen $q_i, r_i \in R$ für $i \geq 0$:

- $r_0 := b$, $r_{-1} := a$
- q_0 und r_1 seien derart, dass $a = q_0b + r_1$ und $r_1 = 0 \vee \rho(r_1) < \rho(b)$.

- Wenn $q_0, \ldots, q_k$ und $r_0, \ldots, r_{k+1}$ mit $k \neq 0$ bereits definiert sind, dann wähle q_{k+1} und r_{k+2} derart, dass $r_k = q_{k+1}r_{k+1} + r_{k+2}$ mit $r_{k+2} = 0 \vee \rho(r_{k+2}) < \rho(r_{k+1})$.

Dieses Verfahren bricht ab, wenn $r_{k+1} = 0$ ist. Dies tritt nach spätestens $\rho(b)$ Schritten auf, weil $\rho(r_k)$ eine streng monoton fallende Folge in $\mathbb{N}_0$ ist. Das letzte r_k mit $r_k \neq 0$ (d.h. mit $r_k \neq 0$, $r_{k+1} = 0$) ist dann $\mathrm{ggT}(a, b)$.

Beweis: Sei $d = r_{n+1}$ und $r_{n+2} = 0$. Wir haben zu zeigen, dass einerseits $d \,|\, a, d \,|\, b$ und andererseits $c \,|\, a, c \,|\, b \;\Rightarrow\; c \,|\, d$ gilt:

- Wir zeigen $d \,|\, r_k$ für $k = n+1, n, \ldots, 0, -1$ mit Induktion:
  Für $k = n+1$ ist $d = r_{n+1}$, also auch $d \,|\, r_{n+1}$; für $k = n+2$ ist $r_{n+2} = 0$, also auch $d \,|\, r_{n+2}$. Gilt nun $d \,|\, r_k$ für $k > l$, dann folgt aus $d \,|\, r_{l+1}$, $d \,|\, r_{l+2}$ und $r_l = q_{l+1}r_{l+1} + r_{l+2}$, dass auch $d \,|\, r_l$ gelten muss.
  Damit ist insbesondere gezeigt, dass $d \,|\, r_{-1} = a$ und $d \,|\, r_0 = b$.

- Angenommen, $c \,|\, a, c \,|\, b$. Wir zeigen mit Induktion, dass dann $c \,|\, r_k$ für alle $k \geq -1$ gilt:
  Für $k = -1, 0$ ist die Bedingung nach Voraussetzung erfüllt. Gilt nun $c \,|\, r_k$ für $k < l$, dann folgt aus $c \,|\, r_{l-1}$, $c \,|\, r_{l-2}$ und $r_l = r_{l-2} - q_{l-1}r_{l-1}$, dass auch $c \,|\, r_l$ gelten muss.
  Damit ist insbesondere gezeigt, dass $c \,|\, r_{n+1} = d$.

Also muss $d = \mathrm{ggT}(a, b)$ sein.

□

Man kann auch jene Koeffizienten α, β finden, für die $\alpha a + \beta b = d$ ist:
Wir definieren dazu induktiv α_l, β_l für $l = n, n-1, \ldots, 0$ durch $\alpha_n = 1$, $\beta_n = -q_n$ sowie $\alpha_{l-1} = \beta_l$ und $\beta_{l-1} = \alpha_l - q_{l-1}\beta_l$. Dann gilt $d = \alpha_l r_{l-1} + \beta_l r_l$, also insbesondere $d = \alpha_0 a + \beta_0 b$.

Beweis: Für $l = n$ gilt $d = r_{n+1} = 1 \cdot r_{n-1} - q_n r_n = \alpha_n r_{n-1} + \beta_n r_n$ nach Definition. Wenn nun die Behauptung für $k > l$ gilt, dann folgt

$$\begin{aligned} \alpha_l r_{l-1} + \beta_l r_l &= \beta_{l+1} r_{l-1} + (\alpha_{l+1} - q_l \beta_{l+1}) r_l \\ &= \alpha_{l+1} r_l + \beta_{l+1}(r_{l-1} - q_l r_l) \\ &= \alpha_{l+1} r_l + \beta_{l+1} r_{l+1} \\ &= d \end{aligned}$$

□

Kapitel 32

Ring der Brüche, Lokalisierung, Quotientenkörper

Bemerkung: Man erhält den Körper der rationalen Zahlen aus dem Ring der ganzen Zahlen durch $\mathbb{Q} := \{(a,b) \,|\, b \in \mathbb{Z} \setminus \{0\}\}/\sim$, wobei $\sim$ durch $(a,b) \sim (c,d) \;:\Leftrightarrow\; ad = bc$ definiert ist. Die Elemente von $\mathbb{Q}$ sind Äquivalenzklassen von Paaren bezüglich $\sim$, und man schreibt $\frac{a}{b}$ für die Klasse von (a,b). Die Addition ist durch $\frac{a}{b} + \frac{c}{d} = \frac{ad+bc}{bd}$ gegeben, die Multiplikation durch $\frac{a}{b} \cdot \frac{c}{d} = \frac{ac}{bd}$.
Diese Konstruktion wird im Folgenden verallgemeinert.

Bemerkung: Die Definition einer multiplikativ abgeschlossenen Menge wurde bereits formuliert:
Sei $S \neq \emptyset$ eine Teilmenge eines Ringes R. S heißt *multiplikativ abgeschlossen*, wenn $a, b \in S \;\Rightarrow\; ab \in S$ gilt.

Beispiel: Einige multiplikativ abgeschlossene Mengen:

1. Sei R ein kommutativer Ring, $P \trianglelefteq R$ ein Primideal und $S = R \setminus P$. Die Eigenschaft $ab = P \;\Rightarrow\; a \in P \vee b \in P$ von P ist äquivalent zur Eigenschaft $a \in S \wedge b \in S \;\Rightarrow\; ab \in S$, und wegen $P \neq R$ ist $S \neq \emptyset$.

2. Sei R ein kommutativer Ring. Dann ist S, definiert als Menge der Nicht-Nullteiler, multiplikativ abgeschlossen: wenn a, b keine Nullteiler sind und $(ab)c = 0$, dann würde $a(bc) = 0$, also $bc = 0$ und damit $c = 0$ folgen. Also kann ab dann auch kein Nullteiler sein.
   Im Spezialfall, dass R ein Integritätsbereich ist, ist $S = R \setminus \{0\}$ multiplikativ abgeschlossen.

Lemma 32.1 Sei R ein kommutativer Ring, $S \subseteq R$ multiplikativ abgeschlossen.

1. Die auf $R \times S$ durch $(r,s) \sim (r',s') \ :\Leftrightarrow \ \exists t \in S$ mit $t(rs' - r's) = 0$ definierte Relation ist Äquivalenzrelation.
   Wenn S keine Nullteiler enthält, dann hat die Relation die einfachere Form $(r,s) \sim (r',s') \ \Leftrightarrow \ rs' - r's = 0$.
   Wir bezeichnen die Äquivalenzklasse von (r,s) bezüglich $\sim$ mit $\frac{r}{s}$ und die Menge der Äquivalenzklassen $(R \times S)/\sim = \{\frac{r}{s} \mid r \in R, s \in S\}$ mit $S^{-1}R$.

2. Wenn $0 \in S$, dann ist $|S^{-1}R| = 1$.

3. Für beliebige $s,t \in S$, $r \in R$ gilt: $\frac{r}{s} = \frac{rt}{st}$, $\frac{s}{s} = \frac{t}{t}$, $\frac{0}{s} = \frac{0}{t}$.

Beweis: als Übung.

Bemerkung: Im Folgenden sei immer $0 \notin S$.

Satz 32.2 (Ring der Brüche) *Sei R ein kommutativer Ring, $S \subseteq R$ multiplikativ abgeschlossen. $S^{-1}R$ sei wie oben definiert. Dann bildet $S^{-1}R$ bezüglich der Addition $\frac{r}{s} + \frac{r'}{s'} = \frac{rs'+r's}{ss'}$ und der Multiplikation $\frac{r}{s} \cdot \frac{r'}{s'} = \frac{rr'}{ss'}$ einen kommutativen Ring mit Eins, wobei $0_{S^{-1}R} = \frac{0}{s}$ und $1_{S^{-1}R} = \frac{s}{s}$ ($s \in S$ beliebig). Außerdem gilt:*

1. *Wenn $R \neq \{0\}$ ein kommutativer nullteilerfreier Ring und $0 \notin S$ ist, dann ist $S^{-1}R$ ein Integritätsbereich.*

2. *Wenn $s,t \in S$, dann ist $\frac{t}{s}$ eine Einheit in $S^{-1}R$ mit dem Inversen $\frac{s}{t}$.*

3. *Wenn $R \neq \{0\}$ ein kommutativer nullteilerfreier Ring und $S = R \setminus \{0\}$ ist, dann ist $S^{-1}R$ ein Körper (der Quotientenkörper).*

Beweis:

- $+$ ist wohldefiniert: sei $\frac{r}{s} = \frac{\rho}{\sigma}$ und $\frac{r'}{s'} = \frac{\rho'}{\sigma'}$. Zu zeigen ist dann, dass $\frac{r}{s} + \frac{r'}{s'} = \frac{\rho}{\sigma} + \frac{\rho'}{\sigma'}$ gilt:
  Sei dazu $t \in S$ mit $t(r\sigma - \rho s) = 0$ und $t' \in S$ mit $t'(r'\sigma' - \rho' s') = 0$.
  Dann gilt:

$$\begin{aligned} tt'((rs' + r's)\sigma\sigma' - (\rho\sigma' + \rho'\sigma)ss') &= tt'(rs'\sigma\sigma' - r's\sigma\sigma' - \rho\sigma' ss' + \rho'\sigma ss') \\ &= t(r\sigma - \rho s)t's'\sigma' - t'(r'\sigma' - \rho' s')ts\sigma \\ &= 0t's'\sigma' - 0ts\sigma = 0 \end{aligned}$$

  Also ist $\frac{rs'+r's}{ss'} = \frac{\rho\sigma'+\rho'\sigma}{\sigma\sigma'}$.

- Analog folgt, dass $\cdot$ wohldefiniert ist.

- Assoziativität von +:
$$\left(\frac{r}{s}+\frac{r'}{s'}\right)+\frac{r''}{s''}=\frac{(rs'+r's)s''+r''ss'}{ss's''}=\frac{rs's''+r'ss''+r''ss'}{ss's''}$$
$$\frac{r}{s}+\left(\frac{r'}{s'}+\frac{r''}{s''}\right)=\frac{rs's''+(r's''+r''s')s}{ss's''}=\frac{rs's''+r'ss''+r''ss'}{ss's''}$$
Also sind die beiden Ausdrücke gleich.
- Neutrales Element $\frac{0}{s}$ (nach dem vorigen Lemma ist s beliebig): $\frac{r}{s}+\frac{0}{s}=\frac{rs+0s}{s^2}=\frac{rs}{s^2}=\frac{r}{s}$ (Kürzen ist nach dem vorigen Lemma möglich).
- Die Operation + ist kommutativ, weil R kommutativ ist.
- Das Inverse von $\frac{r}{s}$ bezüglich + ist $\frac{-r}{s}$: $\frac{r}{s}+\frac{-r}{s}=\frac{rs+(-r)s}{s^2}=\frac{0}{s^2}=0_{S^{-1}R}$
- Die Assoziativität von $\cdot$ ist klar. $\cdot$ ist überdies kommutativ, weil R kommutativ ist.
- Distributivgesetz:
$$\begin{aligned}\left(\frac{r}{s}+\frac{r'}{s'}\right)\frac{r''}{s''} & \\ &= \frac{(rs'+r's)r''}{ss's''}\\ &= \frac{rs'r''+r'sr''}{ss's''}\\ &= \frac{rr''s's''+r'r''ss''}{ss's''s''}\\ &= \frac{rr''}{ss''}+\frac{r'r''}{s's''}\end{aligned}$$
- Einselement $\frac{t}{t}$ (nach dem vorigen Lemma ist t beliebig): $\frac{r}{s}\cdot\frac{t}{t}=\frac{rt}{st}=\frac{r}{s}$ (Kürzen ist nach dem vorigen Lemma möglich).

Damit sind alle Eigenschaften eines kommutativen Ringes mit Eins gezeigt. Es bleiben die zusätzlichen Eigenschaften:

1. $S^{-1}R$ ist ein kommutativer Ring mit Eins. Es bleibt noch zu zeigen, dass $1\neq 0$ ist und es keine Nullteiler in $S^{-1}R$ gibt:
Aus $\frac{0}{s}=\frac{s}{s}$ würde $t(0s-ss)=0$ für ein $t\in S$ folgen. Damit wäre jedoch $s^2t=0\in S$, ein Widerspruch.
Angenommen, es wäre $\frac{r}{s}\cdot\frac{r'}{s'}=\frac{0}{t}$. Dann folgt $t'rr't=0$ für ein $t'\in S$. Damit ist $(tt')(rr')=0$ und somit $rr'=0$, weil $tt'\in S\neq 0$ sein muss und R keine Nullteiler enthält. Daher $r=0\vee r'=0$, also $\frac{r}{s}=0_{S^{-1}R}$ oder $\frac{r'}{s'}=0_{S^{-1}R}$.

2. $s,t \in S \Rightarrow \frac{s}{t} \cdot \frac{t}{s} = \frac{st}{st} = 1_{S^{-1}R}$.

3. Wenn $S = R \setminus \{0\}$, dann gilt $\forall \frac{r}{s}$ mit $r \neq 0$: $\frac{s}{r} \in S^{-1}R$, also hat jedes Element $\neq 0_{S^{-1}R}$ ein Inverses in $S^{-1}R$.

□

Satz 32.3 *Sei S eine multiplikativ abgeschlossene Teilmenge eines kommutativen Ringes R, $0 \notin S$.*

1. *$\varphi_S : R \to S^{-1}R$, definiert durch $r \mapsto \frac{rs}{s}$ (dabei ist $s \in S$ beliebig) ist ein Ringhomomorphismus, und für alle $s \in S$ gilt: $\varphi_S(s)$ ist Einheit in $S^{-1}R$.*

2. *$\operatorname{Ker} \varphi_S = \{r \in R \mid \exists s \in S \text{ mit } rs = 0\}$*

3. *Wenn S keine Nullteiler enthält, dann ist φ_S injektiv.*

Beweis:

1. - φ_S ist wohldefniert: $s,t \in S$, $r \in R \Rightarrow \frac{rs}{s} = \frac{rt}{t}$, da $trs - srt = 0$.
   - $\varphi_S(r+r') = \frac{(r+r')s}{s} = \frac{rs+r's}{s} = \frac{rs^2+r's^2}{s^2} = \frac{rs}{s} + \frac{r's}{s} = \varphi_S(r) + \varphi_S(r')$
   - $\varphi_S(rr') = \frac{rr's}{s} = \frac{rr's^2}{s^2} = \frac{rs}{s} \cdot \frac{r's}{s} = \varphi_S(r) \cdot \varphi_S(r')$
   - Ist $s \in S$, dann ist $\varphi_S(s) = \frac{s^2}{s}$ Einheit mit dem Inversen $\frac{s}{s^2}$, wie zuvor gezeigt wurde.

2. Sei $\varphi_S(r) = 0_{S^{-1}R} = \frac{0}{s}$. Dann folgt $\frac{rs}{s} = \frac{0}{s}$, also $trs^2 - ts0 = 0$ für ein $t \in S$. Damit ist jedoch $r(ts^2) = 0$ und $ts^2 \in S$.
   Sei umgekehrt $rs = 0$ für ein $s \in S$. Dann ist $\varphi_S(r) = \frac{rs}{s} = \frac{0}{s} = 0_{S^{-1}R}$, also $r \in \operatorname{Ker} \varphi_S$.

3. Wenn S keine Nullteiler enthält, dann kann es für $r \in R$ nur dann ein $s \in S$ mit $rs = 0$ geben, wenn $r = 0$ ist. In diesem Fall ist dann $\operatorname{Ker} \varphi_S = \{0\}$, also φ_S injektiv.

Bemerkung: Wenn R ein Ring mit Eins ist und $1 \in S$, dann hat φ_S die einfache Form $\varphi_S(r) = \frac{r}{1}$.

Bemerkung: Wenn S nur aus Einheiten von R besteht, dann ist $\varphi_S : R \to S^{-1}R$ ein Isomorphismus, d.h. $R \simeq S^{-1}R$ (die Injektivität folgt, weil S nur Einheiten, also keine Nullteiler enthält, die Surjektivität ist gegeben, weil $\frac{r}{s} = \frac{rs^{-1}s}{s} = \varphi_S(rs^{-1})$ für alle $r \in R, s \in S$ ist).

BEMERKUNG: Wenn T nur aus Einheiten von R besteht und S und $S' = S \cup T$ multiplikativ abgeschlossen sind, dann ist $S^{-1}R \simeq S'^{-1}R$ (Beweis als Übung). D.h., die Erweiterung der möglichen Nenner um Einheiten bringt nichts Neues. Daher können wir immer $1 \in S$ annehmen, wenn R ein Einselement hat. Damit ist (wie in der ersten Bemerkung festgehalten) $\varphi_S = \frac{r}{1}$.
Wenn S keine Nullteiler enthält, fassen wir R als Unterring von $S^{-1}R$ auf, wobei wir $r \in R$ mit $\frac{r}{1}$ bzw. $\frac{rs}{s}$ identifizieren.

Lemma 32.4 Seien R, T Ringe mit Eins, $g : R \to T$ ein Ringhomomorphismus.

1. Wenn ein Nicht-Nullteiler von T in $\operatorname{Im} g$ liegt, dann ist $g(1) = 1$.
2. Wenn $g(1) = 1$, dann gilt für jede Einheit $u \in R$: $g(u)^{-1} = g(u^{-1})$ (insbesondere ist dann $g(u)$ auch Einheit).

Beweis: als Übung.

Satz 32.5 (Universelle Eigenschaft des Rings der Brüche) *Sei S eine multiplikativ abgeschlossene Teilmenge eines kommutativen Ringes R, $S^{-1}R = \{\frac{r}{s} \mid r \in R, s \in S\}$ der Ring der Brüche und $\varphi : R \to S^{-1}R$ durch $\varphi(r) = \frac{rs}{s}$ definiert.*
Wenn T ein kommutativer Ring mit Eins ist und $f : R \to T$ ein Ringhomomorphismus, sodass für alle $s \in S$ $f(s)$ eine Einheit in T ist, dann gibt es genau einen Ringhomomorphismus $\overline{f} : S^{-1}R \to T$ mit $\overline{f} \circ \varphi = f$. Wenn f injektiv ist, dann auch $\overline{f}$.

Beweis: Definiere $\overline{f}(\frac{r}{s}) = f(r)f(s)^{-1}$. Dann sind alle Bedingungen erfüllt:

- $\overline{f}$ ist wohldefiniert: sei $\frac{r}{s} = \frac{r'}{s'}$ und $t \in S$ mit $t(rs' - r's) = 0$. Dann ist
  $0 = f(0) = f(t)(f(r)f(s') - f(r')f(s)) = f(t)f(s)f(s')(f(r)f(s)^{-1} - f(r')f(s')^{-1})$
  Weil $f(t)f(s)f(s')$ Einheit und daher kein Nullteiler ist, muss somit $f(r)f(s)^{-1} = f(r')f(s')^{-1}$ sein.
- $\overline{f}$ ist Homomorphismus bezüglich $+$:

$$\begin{aligned}
\overline{f}\left(\frac{r}{s} + \frac{r'}{s'}\right) &= \overline{f}\left(\frac{rs' + r's}{ss'}\right) \\
&= f(rs' + r's)f(ss')^{-1} \\
&= f(rs')f(ss')^{-1} + f(r's)f(ss')^{-1} \\
&= \overline{f}\left(\frac{rs'}{ss'}\right) + \overline{f}\left(\frac{r's}{ss'}\right) \\
&= \overline{f}\left(\frac{r}{s}\right) + \overline{f}\left(\frac{r'}{s'}\right)
\end{aligned}$$

- $\overline{f}$ ist Homomorphismus bezüglich $\cdot$:

$$\begin{aligned}\overline{f}\left(\frac{r}{s}\cdot\frac{r'}{s'}\right) &= \overline{f}\left(\frac{rr'}{ss'}\right)\\ &= f(rr')f(ss')^{-1}\\ &= f(r)f(s)^{-1}f(r')f(s')^{-1}\\ &= \overline{f}\left(\frac{r}{s}\right)\cdot\overline{f}\left(\frac{r'}{s'}\right)\end{aligned}$$

- $\overline{f}\circ\varphi(r) = \overline{f}(\frac{rs}{s}) = f(rs)f(s)^{-1} = f(r)f(s)f(s)^{-1} = f(r)$, d.h. $\overline{f}\circ\varphi = f$.

Angenommen, g wäre ein anderer Ringhomomorphismus, der alle diese Bedingungen erfüllt. Für alle $s \in S$ ist $f(s)$ Einheit in T. $S \neq \emptyset$, daher gibt es ein $s \in S$, für das $f(s) = g(\varphi(s)) \in \operatorname{Im} g$ Einheit in T und damit kein Nullteiler ist. Nach dem vorigen Lemma gilt dann $g(1) = 1$, und für alle Einheiten $u \in S^{-1}R$ ist $g(u)$ Einheit mit $g(u)^{-1} = g(u^{-1})$. Damit ist jedoch

$$\begin{aligned}g\left(\frac{r}{s}\right) &= g\left(\frac{rs}{s}\frac{s}{s^2}\right) = g(\varphi(r)\varphi(s)^{-1}) = g(\varphi(r))g(\varphi(s)^{-1})\\ &= g(\varphi(r))g(\varphi(s))^{-1} = f(r)f(s)^{-1} = \overline{f}\left(\frac{r}{s}\right)\end{aligned}$$

Also ist $\overline{f}$ eindeutig bestimmt.
Wenn f injektiv ist, dann ist $\operatorname{Ker} f = \{0\}$, also kann $0 = \overline{f}(\frac{r}{s}) = f(r)f(s)^{-1}$ nur dann gelten, wenn $f(r) = 0$, also $r = 0$ gilt. Damit ist jedoch $\operatorname{Ker}\overline{f} = \{0_{S^{-1}R}\}$, also $\overline{f}$ injektiv.

□

BEMERKUNG: $S^{-1}R$ und φ_S sind durch diese universelle Eigenschaft bis auf Isomorphie eindeutig bestimmt, d.h. wenn R' ein kommutativer Ring mit Eins und $\psi : R \to R'$ ein Ringhomomorphismus ist, sodass $\forall s \in S\ \psi(s)$ Einheit in R' ist und R', ψ die Eigenschaft erfüllen, dass für alle kommutativen Ringe T mit Eins und alle Ringhomomorphismen $f : R \to T$ derart, dass $f(s)$ für alle $s \in S$ Einheit ist, ein eindeutiger Ringhomomorphismus $\overline{f} : R' \to T$ mit $\overline{f} \circ \psi = f$ existiert, dann gibt es einen Isomorphismus $g : S^{-1}R \to R'$ mit $g \circ \varphi_S = \psi$ und $g^{-1} \circ \psi = \varphi_S$.

Korollar 32.6 Sei R ein Integritätsbereich, $K = S^{-1}R$ mit $S = R \setminus \{0\}$ sein Quotientenkörper. R sei Unterring von K durch die Einbettung $r \mapsto \frac{r}{1}$.

1. Wenn F ein Körper und $f : R \to F$ ein Ringmonomorphismus ist, dann gibt es genau einen Körpermonomorphismus $\overline{f} : K \to F$ mit $\overline{f}|_R = f$.

2. Wenn F ein Körper mit $R \leq F$ ist, dann gibt es einen Körper $K' \simeq K$ mit $R \leq K' \leq F$, wobei $K' = \{rs^{-1} \mid r \in R, s \in R \setminus \{0\}\}$.

Beweis:

1. Weil $f : R \to F$ ein Ringmonomorphismus, also injektiv, ist, gilt für alle $r \in R \setminus \{0\}$ $f(r) \neq 0$, also ist $f(r)$ invertierbar. Nach der universellen Eigenschaft existiert ein Monomorphismus $\overline{f} : K \to F$ mit $\overline{f} \circ \mathrm{incl}_{R \hookrightarrow K} = f$, d.h. $\overline{f}|_R = f$.

2. $f = \mathrm{incl}_{R \hookrightarrow F}$ ist ein Ringmonomorphismus, also gibt es nach 1. einen Monomorphismus $\overline{f} : K \to F$ mit $\overline{f}|_R = f$. Wählt man $K' = \mathrm{Im}\,\overline{f}$, dann ist $K \simeq K'$, und weil wir wissen, dass $\overline{f}(\frac{r}{s}) = f(r)f(s)^{-1} = rs^{-1}$ ist, hat K' die angegebene Form.

□

Lemma 32.7 Sei R ein kommutativer Ring, $I \trianglelefteq R$ und $S \subseteq R$ multiplikativ abgeschlossen mit $0 \notin S$. Dann ist $\varphi_S(I) \cdot (S^{-1}R)$ ein Ideal in $S^{-1}R$ und es gilt $\varphi_S(I) \cdot (S^{-1}R) = \{\frac{i}{s} \mid i \in I, s \in S\} =: S^{-1}I$ (alle Elemente, die eine Bruchdarstellung mit Zähler in I haben).

Beweis: Seien $i \in I$ und $\frac{r}{t} \in S^{-1}R$: dann ist $\frac{is}{s} \cdot \frac{r}{t} = \frac{isr}{st} = \frac{ir}{t} \in \{\frac{i}{s} \mid i \in I\}$, und wegen $\frac{i}{s} + \frac{i'}{s'} = \frac{is'+i's}{ss'} \in S^{-1}I$ für $\frac{i}{s}, \frac{i'}{s'} \in S^{-1}I$ gilt damit $\varphi_S(I) \cdot S^{-1}R = \{\varphi_S(i_1)\frac{r_1}{t_1} + \ldots + \varphi_S(i_n)\frac{r_n}{t_n} \mid n \in \mathbb{N},\ i_j \in I,\ \frac{r_j}{t_j} \in S^{-1}R\} \subseteq S^{-1}I$.
Seien umgekehrt $i \in I$ und $s \in S$. Dann ist $\frac{i}{s} = \frac{is}{s}\frac{s}{s^2} \in \varphi_S(I) \cdot S^{-1}R$, also gilt auch die umgekehrte Inklusion.
Es bleibt zu zeigen, dass es sich um ein Ideal handelt: wegen $0_{S^{-1}R} \in S^{-1}I$ ist jedenfalls $S^{-1}I \neq \emptyset$. Aus $\frac{i}{s}, \frac{i'}{s'} \in S^{-1}I$ folgt $\frac{i}{s} - \frac{i'}{s'} = \frac{is'-i's}{ss'} \in S^{-1}I$, und aus $\frac{i}{s} \in S^{-1}I$, $\frac{r}{t} \in S^{-1}R$ folgt $\frac{i}{s} \cdot \frac{r}{t} = \frac{ir}{st} \in S^{-1}I$. Also ist $S^{-1}I$ ein Ideal.

□

Bemerkung: Aus $\frac{r}{s} \in S^{-1}I$ folgt im Allgemeinen nicht, dass $r \in I$, sondern nur, dass es $i \in I$, $t \in S$ mit $\frac{r}{s} = \frac{i}{t}$ gibt.

Lemma 32.8 Sei P ein Primideal, $P \cap S = \emptyset$. Dann gilt $\frac{r}{s} \in S^{-1}P \Rightarrow r \in P$.

Beweis: Sei $\frac{r}{s} \in S^{-1}P$ und $p \in P$, $t \in S$ mit $\frac{r}{s} = \frac{p}{t}$. Dann ist $rtt' = pst' \in P$ für ein $t' \in S$. Weil $tt' \in S$ liegt und $S \cap P = \emptyset$ ist, ist dies nur möglich, wenn $r \in P$.

□

Lemma 32.9 Sei $J \trianglelefteq S^{-1}R$. Dann ist $\varphi_S^{-1}(J)$ ein Ideal von R und $\varphi_S^{-1}(J) = \{r \in R \,|\, \exists s \in S : \ \frac{r}{s} \in J\}$ (alle Zähler, die in Bruchdarstellungen von Elementen in J vorkommen).

Beweis: Sei r so, dass $\frac{rs}{s} \in J$ (d.h. $r \in \varphi_S^{-1}(J)$). Dann ist auch $\frac{r}{s} = \frac{rs}{s} \cdot \frac{s}{s^2} \in J$, also $r \in \{r \in R \,|\, \exists s \in S : \ \frac{r}{s} \in J\}$.
Sei umgekehrt r so, dass für ein $s \in S$ $\frac{r}{s} \in J$. Dann ist auch $\frac{r}{s} \cdot \frac{s^2}{s} = \frac{rs}{s} = \varphi_S(r) \in J$, also $r \in \varphi_S^{-1}(J)$.

□

Satz 32.10 *Sei R ein kommutativer Ring, $S \subseteq R$ multiplikativ abgeschlossen und $0 \notin S$.*

1. *Sei $I \trianglelefteq R$. Dann gilt $S^{-1}I = S^{-1}R \ \Leftrightarrow \ I \cap S \neq \emptyset$*
2. *Sei $J \trianglelefteq S^{-1}R$. Dann gilt $S^{-1}(\varphi_S^{-1}(J)) = J$, insbesondere hat jedes Ideal von $S^{-1}R$ die Form $S^{-1}I$ für ein Ideal $I \trianglelefteq R$.*
3. *Eine Bijektion zwischen allen Primidealen $P \trianglelefteq R$ mit $P \cap S = \emptyset$ und allen Primidealen von $S^{-1}R$ ist gegeben durch $P \mapsto S^{-1}P$ mit der inversen Abbildung $Q \mapsto \varphi_S^{-1}(Q)$.*

Beweis:

1. Sei $S^{-1}I = S^{-1}R$. Dann gibt es $i \in I$ und $s \in S$ mit $1 = \frac{i}{s}$, also $\frac{s}{s} = \frac{i}{s}$. Damit haben wir $ts^2 = tsi$ für ein $t \in S$, und $ts^2 \in S$ (weil S multiplikativ abgeschlossen ist) sowie $tsi \in I$ (weil I ein Ideal ist). Daher ist $ts^2 = tsi \in I \cap S$ und folglich $I \cap S \neq \emptyset$.
   Sei umgekehrt $i \in I \cap S$. Dann ist $\frac{i}{i} = 1 \in S^{-1}I$. Ein Ideal, das das Einselement enthält, muss jedoch bekanntermaßen mit dem ganzen Ring übereinstimmen, d.h. $S^{-1}I = S^{-1}R$.

2. $\varphi_S^{-1}(J)$ ist die Menge aller Zähler, die in Bruchdarstellungen von Elementen aus J vorkommen, $S^{-1}\varphi_S^{-1}(J)$ folglich die Menge aller Brüche mit solchen Zählern. Dazu gehören aber jedenfalls alle Elemente von J, also $J \subseteq S^{-1}\varphi_S^{-1}(J)$.
   Sei $\frac{r}{s} \in S^{-1}\varphi_S^{-1}(J)$. Dann gibt es ein Element der Form $\frac{r}{t}$ ($t \in S$) in J, und damit ist aber auch $\frac{r}{t} \cdot \frac{t}{s} = \frac{r}{s} \in J$, weil J Ideal ist. Also gilt auch $S^{-1}\varphi_S^{-1}(J) \subseteq J$.

3. Ist P ein Primideal von R mit $P \cap S = \emptyset$, dann ist $S^{-1}P$ ein Primideal von $S^{-1}R$; ist umgekehrt Q ein Primideal von $S^{-1}R$, dann ist $\varphi_S^{-1}Q$ ein Primideal von R, und $S \cap \varphi_S^{-1}Q = \emptyset$. (Beweise als Übung)

Damit ist die Abbildung $S^{-1} : P \mapsto S^{-1}P$ eine Abbildung der Primideale von R mit $P \cap S = \emptyset$ auf die Primideale von $S^{-1}R$, und φ_S^{-1} ist eine Abbildung der Primideale von $S^{-1}R$ auf die Primideale von R mit $P \cap S = \emptyset$.
In 2. wurde gezeigt, dass $S^{-1} \circ \varphi_S^{-1} = \mathrm{id}$ ist. Damit S^{-1} und φ_S^{-1} invers zueinander sind, muss auch noch gezeigt werden, dass $\varphi_S^{-1}S^{-1}P = P$ für alle Primideale von R mit $P \cap S = \emptyset$ gilt.
$\varphi_S^{-1}S^{-1}P$ ist die Menge aller Zähler, die in Bruchdarstellungen von $S^{-1}P$ vorkommen. Jedenfalls gilt daher $P \subseteq \varphi_S^{-1}S^{-1}P$. Wegen Lemma 32.8 hat aber jedes Element von $S^{-1}P$ nur Darstellungen mit Zähler in P, daher gilt auch $\varphi_S^{-1}S^{-1}P \subseteq P$.

□

Korollar 32.11 Sei R ein kommutativer Ring und P ein Primideal von R. Sei weiters $S = R \setminus P$. Dann heißt $R_P := S^{-1}R$ *Lokalisierung* von R bei P.
Jedes Ideal von R_P hat die Form $S^{-1}I$ für ein Ideal $I \subseteq P$, und eine Bijektion zwischen den Primidealen von R, die in P enthalten sind, und allen Primidealen von R_P ist durch $Q \mapsto S^{-1}Q = Q_P$ mit der Inversen $J \mapsto \varphi_S^{-1}(J)$ gegeben.
Insbesondere ist $P_P = S^{-1}P$ das einzige maximale Ideal von R_P (da $I \subseteq P \Rightarrow S^{-1}I \subseteq S^{-1}P$).

Definition 32.12 Ein Ring R heißt *lokal*, wenn er genau ein maximales Ideal hat.

Bemerkung: Nach dem vorigen Korollar ist R_P lokal für jedes Primideal $P \trianglelefteq R$.

Bemerkung: Ein Ring mit Eins R ist genau dann lokal, wenn die Nichteinheiten von R ein Ideal bilden (Beweis als Übung).

Bemerkung: Viele Autoren setzen in der Definition von *lokal* voraus, daß der Ring Noethersch ist, und nennen Ringe, die nach unserer Definition lokal sind, quasi-lokal.

Kapitel 33

Faktorisierung in Polynomringen

Satz 33.1 (Polynomdivision) *Sei R ein Ring mit Eins, $f, g \in R[x]$, und der Leitkoeffizient von g sei eine Einheit in R. Dann existieren eindeutig bestimmte Polynome $q, r \in R[x]$ mit $f = qg + r$, wobei $r = 0$ oder $\deg r < \deg g$ ist.*

Beweis: Wir zeigen zuerst die Existenz. Wenn $f = 0$ oder $\deg f < \deg g$, dann kann $f = 0g + f$ gewählt werden, d.h. $q = 0$ und $r = f$. Sei andernfalls $n = \deg f \geq \deg g = m$. Induktion nach n:

- Für $n = 0$ ist auch $m = 0$, d.h. g ist konstant und eine Einheit in R. Damit ist $f = fg^{-1}g + 0$, d.h. $q = fg^{-1}$ und $r = 0$.
- Sei $f = \sum_{i=0}^{n} a_i x^i$, wobei $a_n \neq 0$, $g = \sum_{j=0}^{m} b_j x^j$, $m \leq n$ und b_m eine Einheit. $a_n x^{n-m} b_m^{-1} g$ ist ein Polynom vom Grad n mit dem Leitkoeffizienten a_n, also ist $\deg(f - a_n x^{n-m} b_m^{-1} g) \leq n-1$. Nach der Induktionsvoraussetzung existieren $\tilde{q}$ und $\tilde{r}$ in $R[x]$ mit $f - a_n x^{n-m} b_m^{-1} g = \tilde{q}g + \tilde{r}$, wobei $\tilde{r} = 0$ oder $\deg \tilde{r} < \deg g$ ist. Damit ist aber $f = (\tilde{q} + a_n x^{n-m} b_m^{-1})g + \tilde{r}$, also $q = \tilde{q} + a_n x^{n-m} b_m^{-1}$ und $r = \tilde{r}$.

Zu zeigen bleibt die Eindeutigkeit der Darstellung. Es sei dazu $f = qg + r = q'g + r'$ mit $r = 0 \vee \deg r < \deg g$ und $r' = 0 \vee \deg r' < \deg g$. Dann folgt $r - r' = (q' - q)g$. Da der Leitkoeffizient von g kein Nullteiler ist, gilt für alle $h \in R[x]$ mit $h \neq 0$: $\deg hg \geq \deg g$. Wäre also $q' - q \neq 0$, dann müsste $\deg(q' - q)g \geq \deg g$, andererseits aber $\deg r - r' \leq \max(\deg r, \deg r') < \deg g$ sein, ein Widerspruch. Also gilt $q' - q = 0$ und damit $r' - r = 0$, also $q = q'$ und $r = r'$.

□

Korollar 33.2 Sei K ein Körper. Dann ist $K[x]$ ein Euklidischer Bereich mit der Rangfunktion deg. Zusätzlich sind q, r immer eindeutig bestimmt.

Beweis: Weil K ein Integritätsbereich ist, trifft dies auch auf $K[x]$ zu. Jedes $f \in K[x]$ hat eine Einheit als Leitkoeffizienten, weil es außer 0 nur Einheiten in K gibt.
Außerdem ist die Eigenschaft $\deg(fg) \geq \deg(f)$ der Rangfunktion auch erfüllt, weil für $f, g \in R[x]$ mit $f, g \neq 0$ der Leitkoeffizient jeweils eine Einheit ist und daher $\deg(fg) = \deg f + \deg g \geq \deg f$ gilt.

□

Satz 33.3 (Restsatz) *Sei R ein Ring mit Eins, $f = \sum_{k=0}^{n} a_k x^k \in R[x]$ und $c \in R$. Definiere $f(c) := \sum_{k=0}^{n} a_k c^k \in R$. Dann gibt es genau ein $q \in R[x]$ mit $f(x) = q(x)(x-c) + f(c)$.*

Beweis:

$$\begin{aligned} f(x) - f(c) &= \sum_{k=0}^{n} a_k x^k - \sum_{k=0}^{n} a_k c^k = \sum_{k=0}^{n} a_k (x^k - c^k) \\ &= \sum_{k=0}^{n} a_k (x^{k-1} + x^{k-2}c + \ldots + c^{k-1})(x-c) = q(x)(x-c) \end{aligned}$$

also gibt es ein solches Polynom.
Zu zeigen bleibt die Eindeutigkeit. Diese folgt aber aus der Eindeutigkeit der Koeffizienten bei Division mit Rest von f durch $(x-c)$.

□

Korollar 33.4 Wenn $f \in R[x]$ ist, $c \in R$ und $f(c) := \sum_{k=0}^{n} a_k c^k \in R$, dann gilt $f(x) = q(x)(x-c) + d \;\Rightarrow\; d = f(c)$.

Beweis: Folgt aus dem Restsatz und der Eindeutigkeit der Koeffizienten bei Division mit Rest. Für ein kommutatives R folgt diese Tatsache natürlich aus der Definition des Einsetzhomomorphismus.

□

Korollar 33.5 Sei R ein Ring mit Eins, $f \in R[x]$ und $c \in R$. Dann gilt:

$$f(c) = 0 \iff \exists q \in R[x] : \; f(x) = q(x)(x-c)$$

Beweis: Es gelte $f(x) = q(x)(x-c)$ für ein $q \in R[x]$. Nach dem Restsatz ist andererseits $f(x) = \tilde{q}(x)(x-c) + f(c)$. Aus der Eindeutigkeit der Division mit Rest folgt damit $q = \tilde{q}$ und $f(c) = 0$.
Die Umkehrung ergibt sich sofort aus dem Restsatz.

□

Definition 33.6 Sei S ein kommutativer Ring mit Eins, $R \leq S$. $c \in S$ heißt *Nullstelle* (oder *Wurzel*) des Polynoms $f \in R[x]$, wenn $f(c) = 0$ ist.

Satz 33.7 *Sei E ein Integritätsbereich, $D \leq E$, $f \in D[x]$ und $f \neq 0$. Wenn $\deg f = n$, dann hat f höchstens n verschiedene Nullstellen in E.*

Beweis: Seien $c_1, \ldots, c_m$ verschiedene Nullstellen von f. Wir zeigen mit Induktion nach m, dass es ein Polynom q gibt, sodass $f(x) = q(x)(x - c_1)(x - c_2)\ldots(x - c_m)$:

- Für $m = 1$ gibt es nach dem Restsatz ein Polynom q mit $f(x) = q(x)(x - c_1)$.
- Induktionsschritt: nach Voraussetzung gibt es ein Polynom q, sodass $f(x) = q(x)(x - c_1)\ldots(x - c_{m-1})$. Die c_i sind verschieden, also ist $c_m - c_i \neq 0$ für alle i. Nach dem Einsetzhomomorphismus ist $0 = f(c_m) = q(c_m)(c_m - c_1)\ldots(c_m - c_{m-1})$. Da E ein Integritätsbereich ist, muss daher $q(c_m) = 0$ sein.
  Nach Induktionsvoraussetzung gibt es also ein $\tilde{q}$ mit $q = \tilde{q}(x - c_m)$, und es gilt somit $f(x) = \tilde{q}(x)(x - c_1)\ldots(x - c_m)$.

Da $\deg((x - c_1)\ldots(x - c_m)) = m$ gilt und wegen $f \neq 0$ auch $q \neq 0$ ist, folgt $m \leq \deg q + m = \deg f$ (weil E Integritätsbereich ist).

□

Beispiel: $R = M_2(\mathbb{Z})$ ist kein Integritätsbereich. Das Polynom $x^2 - I$ hat unendlich viele Nullstellen, nämlich etwa $\begin{pmatrix} 1 & \lambda \\ 0 & -1 \end{pmatrix}$ für alle $\lambda \in \mathbb{Z}$.

Beispiel: $R = \mathbb{Z}_9$ ist kein Integritätsbereich, x^2 hat die Nullstellen $\overline{0}$, $\overline{3}$ und $\overline{6}$.

Beispiel: $R = \mathbb{H}$ sei der Schiefkörper (nicht kommutativ!) der rationalen Quaternionen. Das Polynom $x^2 + 1$ hat in $\mathbb{H}$ die Nullstellen $\pm i$, $\pm j$, $\pm k$, obwohl $\mathbb{H}$ keine Nullteiler enthält!

Kapitel 34

Formale Ableitung – mehrfache Nullstellen

Definition 34.1 Sei D ein Integritätsbereich, $f \in D[x]$, $f \neq 0$, $c \in D$. Sei $m \in \mathbb{N}_0$ maximal, sodass $\exists g \in D[x]$ mit $f(x) = g(x)(x-c)^m$ (m maximal, sodass $(x-c)^m \mid f$ in $D[x]$). Dieses maximale m existiert, weil m durch $\deg f$ beschränkt ist, wegen

$$(x-c)^m g(x) = f(x),\ f \neq 0 \ \Rightarrow\ \deg f = \deg g + m \geq m.$$

(Hier haben wir verwendet, dass D ein Integritätsbereich ist!).

Wenn $m = 1$, dann heißt c *einfache Nullstelle* von f. Wenn $m > 1$, dann heißt c *mehrfache Nullstelle* von f. In beiden Fällen heißt c m-fache Nullstelle von f. m heißt *Vielfachheit* der Nullstelle c von f.

Definition 34.2 Sei R ein Ring mit Eins, $f(x) = \sum_{k=0}^{n} a_k x^k \in R[x]$. Die *formale Ableitung* von f ist das Polynom

$$f' = \sum_{k=1}^{n} k a_k x^{k-1} = \sum_{k=0}^{n-1} (k+1) a_{k+1} x^k$$

Bemerkung: Es gilt $f = a_0 \in R \ \Rightarrow\ f' = 0$, aber nicht die Umkehrung. So ist etwa die Ableitung von $f(x) = a_0 + a_1 x^p + a_2 x^{2p}$ über einem Ring mit $\chi(R) = p$ auch $f' = p a_1 x^{p-1} + 2p a_2 x^{2p-1} = 0$.

Lemma 34.3 Sei R ein kommutativer Ring mit Eins, $f, g \in R[x]$, $c \in R$, $n \in \mathbb{N}$. Dann gilt:

1. $(cf)' = cf'$

2. $(f+g)' = f' + g'$
3. $(fg) = f'g + fg'$
4. $(f^n)' = nf^{n-1}f'$

Beweis:

1. trivial.
2. trivial.
3. Sei $f = \sum_{k=0}^{n} a_k x^k$ und $g = \sum_{l=0}^{m} b_l x^l$. Dann gilt $fg = \sum_{k=0}^{n+m}(\sum_{j=0}^{k} a_j b_{k-j})x^k$ und somit

$$(fg)' = \sum_{k\geq 0}(k+1)\left(\sum_{j=0}^{k+1} a_j b_{k+1-j}\right)x^k$$

und andererseits

$$\begin{aligned} f'g + fg' &= \sum_{k\geq 0}\left(\sum_{j=0}^{k}(j+1)a_{j+1}b_{k-j} + \sum_{j=0}^{k} a_j(k+1-j)b_{k+1-j}\right)x^k \\ &= \sum_{k\geq 0}\left(\sum_{j=1}^{k+1} j a_j b_{k+1-j} + \sum_{j=0}^{k} a_j(k+1-j)b_{k+1-j}\right)x^k \\ &= \sum_{k\geq 0}\left(\sum_{j=0}^{k+1} j a_j b_{k+1-j} + \sum_{j=0}^{k+1} a_j(k+1-j)b_{k+1-j}\right)x^k \\ &= \sum_{k\geq 0}\left(\sum_{j=0}^{k+1}(k+1)a_j b_{k+1-j}\right)x^k \end{aligned}$$

Also $(fg)' = f'g + fg'$.

4. Induktion nach n:
   - Für $n = 1$ gilt die Behauptung trivialerweise.
   - Es gelte $(f^{n-1})' = (n-1)f^{n-2}f'$. Dann folgt $(f^n)' = (ff^{n-1})' = f'f^{n-1} + f(f^{n-1})' = f'f^{n-1} + f(n-1)f^{n-2}f' = nf^{n-1}f'$.

□

Proposition 34.4 Sei D ein Integritätsbereich, $c \in D$ eine Nullstelle von $f \in D[x]$. c ist genau dann mehrfache Nullstelle, wenn $f'(c) = 0$ bzw. $(x-c) \mid f'$ in $D[x]$.

Beweis: Weil c Nullstelle ist, gilt nach dem Restsatz $f(x) = g(x)(x-c)^m$ für ein $m \geq 1$. Sei m maximal mit dieser Eigenschaft. Dann gilt $g(c) \neq 0$ (weil sonst nach dem Restsatz $(x-c) \mid g$ und damit $(x-c)^{m+1} \mid f$ gelten würde). Im Fall einer einfachen Nullstelle ($m = 1$) folgt: $f'(x) = g'(x)(x-c) + g(x)$, also $f'(c) = g(c) \neq 0$ (Einsetzhomomorphismus) und daher auch $(x-c) \nmid f'$. Im Fall einer mehrfachen Nullstelle ($m > 1$) folgt: $f'(x) = g'(x)(x-c)^m + mg(x)(x-c)^{m-1}$. Weil $m - 1 > 0$ ist, kann man $(x-c)$ herausheben, und es gilt $(x-c) \mid f'$ und damit auch $f'(c) = 0$.

□

Korollar 34.5 Sei D ein Integritätsbereich, $c \in D$, $f \in D[x]$. c ist genau dann mehrfache Nullstelle von f, wenn $f(c) = 0$ und $f'(c) = 0$ gilt bzw. wenn $(x-c)$ ein gemeinsamer Teiler von f und f' ist.

Definition 34.6 Zwei Elemente a, b eines Integritätsbereiches heißen *relativ prim*, wenn $\forall c \in D\ (c \mid a \wedge c \mid b \ \Rightarrow\ c$ ist Einheit).

Bemerkung: Wenn $\mathrm{ggT}(a,b)$ existiert, dann ist „a, b relativ prim“ äquivalent zu $\mathrm{ggT}(a,b) \approx 1$.

Korollar 34.7 Sei D ein Integritätsbereich, $f \in D[x]$. Wenn f und f' relativ prim sind, dann hat f keine mehrfachen Nullstellen in D.

Definition 34.8 Ein Polynom $f \in R[x]$ heißt *irreduzibel* über R (bzw. irreduzibel in $R[x]$), wenn f ein irreduzibles Element von $R[x]$ ist (d.h. f ist weder Einheit noch Nullteiler, und aus $f = gh$ folgt, dass g oder h Einheit in $R[x]$ ist).

Bemerkung: Wenn D, E Integritätsbereiche mit $D \leq E$ sind, dann gilt weder „f irreduzibel in $D[x] \Rightarrow f$ irreduzibel in $E[x]$“ noch die Umkehrung.

Beispiel: $f(x) = 2x^2 + 2 \in \mathbb{Z}[x] \subseteq \mathbb{R}[x] \subseteq \mathbb{C}[x]$.

- f ist nicht irreduzibel in $\mathbb{Z}[x]$: $f(x) = 2(x^2+1)$, und 2, (x^2+1) sind keine Einheiten.
- f ist irreduzibel in $\mathbb{R}[x]$, da $\deg f = 2$ und f keine Nullstellen in $\mathbb{R}$ hat (siehe Lemma 34.12).
- f ist nicht irreduzibel in $\mathbb{C}[x]$: $f(x) = 2(x+i)(x-i)$, und $2(x+i)$, $(x-i)$ sind keine Einheiten.

Definition 34.9 Ein Polynom f heißt *linear*, wenn $\deg f = 1$.

Lemma 34.10 Sei D ein Integritätsbereich.

1. Wenn $c \in D$, dann ist c irreduzibel in $D[x]$ genau dann, wenn c in D irreduzibel ist.
2. Ist u eine Einheit in D und $c \in D$, dann ist $ux + c$ irreduzibel in $D[x]$.
3. Sind a, b relativ prim in D, $a \neq 0$, dann ist $ax + b$ irreduzibel in $D[x]$.

Beweis:

1. $c = 0$ ist weder in D noch in $D[x]$ irreduzibel, daher kann $c \neq 0$ angenommen werden. Weiters wissen wir bereits, dass c genau dann Einheit in $D[x]$ ist, wenn es auch in D Einheit ist. Wenn $fg = c$ ist, dann folgt aus $c \in D$ wegen $\deg(fg) = \deg f + \deg g$ auch $f, g \in D$. Daher gilt $fg = c$ für Nicht-Einheiten f, g in $D[x]$ genau dann, wenn dies auch in D der Fall ist. Folglich ist c genau dann irreduzibel in $D[x]$, wenn es auch in D irreduzibel ist.
2. Spezialfall von 3.
3. Angenommen, $ax+b = f(x)g(x)$ für Polynome $f, g \in D[x]$. Aus $\deg f + \deg g = 1$ folgt $\deg f = 0$, $\deg g = 1$ oder umgekehrt, o.B.d.A. $\deg f = 0$. Das bedeutet $f = c \in D$, $g = a'x + b'$ mit $a' \neq 0$. Es gilt dann $ax + b = c(a'x + b') = ca'x + cb'$. Damit ist jedoch c gemeinsamer Teiler von a und b, also ist c Einheit.

□

Korollar 34.11 Ist K ein Körper, dann ist jedes lineare Polynom in $K[x]$ irreduzibel.

Bemerkung: Ist R kein Integritätsbereich, sondern nur kommutativer Ring mit Eins, dann muss nicht einmal x irreduzibel sein. So ist etwa in $\mathbb{Z}_6[x]$ $(2x + 3)(3x - 4) = 6x^2 + 9x - 8x - 12 = x$, und weder $2x + 3$ noch $3x - 4$ ist Einheit (weil schon das jeweilige a_0 keine Einheit ist).

Lemma 34.12 Sei K ein Körper, $f \in K[x]$, $f \neq 0$.

1. f hat genau dann einen Linearfaktor (d.h. einen Teiler vom Grad 1) in $K[x]$, wenn f eine Nullstelle in K hat.
2. Wenn $\deg f = 2$ oder $\deg f = 3$, dann ist f genau dann irreduzibel über K, wenn f keine Nullstelle in K hat.

3. Die Aussagen 1. und 2. gelten auch noch, wenn K nur ein Integritätsbereich ist, aber f *normiert* ist (d.h. der Leitkoeffizient ist 1).

Beweis:

1. Ist $f(x) = g(x)(ax + b)$ mit $a \neq 0$, dann ist $-ba^{-1}$ eine Nullstelle von f in K (ist K nur Integritätsbereich, aber f normiert, dann muss a Einheit sein, denn a, multipliziert mit dem Leitkoeffizienten von g, ergibt den Leitkoeffizienten von f, also 1).
   Die Umkehrung folgt aus dem Restsatz.

2. Wenn $f = gh$, dann ist $\deg g + \deg h = \deg f$, und weil Polynome vom Grad 0 in $K[x]$ Einheiten sind, sind $1, 1$ bzw. $2, 1$ die einzigen Möglichkeiten für die Grade von g und h. Daher muss f in diesem Fall einen Linearfaktor und damit eine Nullstelle haben, d.h. f nicht irreduzibel $\Rightarrow$ f hat Nullstelle.
   Hat andererseits f eine Nullstelle c, dann gilt $f(x) = g(x)(x - c)$ für ein $g \in K[x]$ mit $\deg g \geq 1$, d.h. weder g noch $(x - c)$ ist Einheit, und damit ist f auch nicht irreduzibel.

Satz 34.13 *Seien K und D Körper, $K \subseteq D$ und $f \in K[x]$.*

1. *Wenn $\mathrm{ggT}(f, f') \approx 1$ in $K[x]$, dann hat f keine mehrfachen Nullstellen in D.*

2. *Wenn f irreduzibel in $K[x]$ ist und f in D eine Nullstelle hat, dann gilt:*
$$f \text{ hat mehrfache Nullstelle in } D \iff f' = 0$$

Beweis:

1. $K[x]$ ist ein Euklidischer Bereich, also insbesondere ein Hauptidealbereich, daher existiert $\mathrm{ggT}(f, f') = d$, und er lässt sich als Linearkombination $d(x) = h(x)f(x) + k(x)f'(x)$ darstellen. Wenn $c \in D$ eine mehrfache Nullstelle ist, dann gilt $f(c) = 0$ und $f'(c) = 0$, also $d(c) = 0$, was einen Widerspruch zu $d \approx 1$ darstellt ($d \approx 1$ bedeutet, dass d eine Einheit in $K[x]$, also eine Konstante $\neq 0$ ist).

2. Wenn f irreduzibel ist und $g \in K[x]$ mit $g \mid f$, dann ist g Einheit oder $g \approx f$ in $K[x]$.
   Im Falle, dass $f' \neq 0$, kann ein Teiler von f, der $f \approx g$ erfüllt, wegen $\deg f' < \deg f$ nicht auch f' teilen. Daher muss jeder gemeinsame Teiler von f und f' eine Einheit sein, und es folgt aus 1., dass f keine

mehrfachen Nullstellen hat.
Ist andererseits $f' = 0$, dann ist jede Nullstelle von f auch Nullstelle von f', also mehrfache Nullstelle von f.

□

Kapitel 35

Polynome über ZPE-Ringen

Lemma 35.1 Ist D ein ZPE-Ring, K sein Quotientenkörper und $\frac{a}{b} \in K$, dann existieren $r, s \in D$ mit $s \neq 0$, $\mathrm{ggT}(r,s) = 1$ und $\frac{a}{b} = \frac{r}{s}$ (gekürzte Darstellung).

Beweis: Wenn $\mathrm{ggT}(a,b) = d$, dann ist $\frac{a}{b} = \frac{a'd}{b'd} = \frac{a'}{b'}$ mit $\mathrm{ggT}(a',b') = 1$.

□

Satz 35.2 *Sei D ein ZPE-Ring, K sein Quotientenkörper, $f(x) = \sum_{k=0}^{n} a_k x^k \in D[x]$. Wenn $\frac{c}{d} \in K$ mit $\mathrm{ggT}(c,d) = 1$ und $f(\frac{c}{d}) = 0$, dann gilt $c \mid a_0$ und $d \mid a_n$.*

Beweis: Aus $\sum_{k=0}^{n} a_k \frac{c^k}{d^k} = 0$ ergibt sich durch Multiplikation mit d^n:
$\sum_{k=0}^{n} d^{n-k} a_k c^k = 0$. Damit ist

$$a_0 d^n = -a_1 c d^{n-1} - a_2 c^2 d^{n-2} - \ldots - a_n c^n$$

Weil c die rechte Seite teilt, muss es auch $a_0 d^n$ teilen, weil aber $\mathrm{ggT}(c,d) = 1$ ist, folgt $c \mid a_0$.
Andererseits ist

$$a_n c^n = -a_0 d^n - a_1 c d^{n-1} - \ldots - a_{n-1} d c^{n-1}$$

Weil d die rechte Seite teilt, muss es auch $a_n c^n$ teilen, weil aber $\mathrm{ggT}(c,d) = 1$ ist, folgt $d \mid a_n$.

□

Definition 35.3 Sei D ein ZPE-Ring, $f(x) = \sum_{k=0}^{n} a_k x^k \in D[x]$, $f \neq 0$. Dann heißt $\mathrm{ggT}(a_0, \ldots, a_n)$ der *Inhalt* des Polynoms f. Wenn $\mathrm{ggT}(a_0, \ldots, a_n) \approx 1$, dann heißt f *primitives* Polynom. Man schreibt den Inhalt als $C(f)$.

Lemma 35.4 Sei D ein ZPE-Ring, $f \in D[x]$, $f \neq 0$, $a \in D$. Dann gilt:

1. $C(af) = aC(f)$
2. Zu f existiert ein primitives Polynom $\tilde{f}$ mit $f = C(f)\tilde{f}$.

Beweis: als Übung.

Lemma 35.5 (Lemma von Gauß) Sei D ein ZPE-Ring, $f, g \in D[x]$ primitive Polynome. Dann ist fg primitiv.

Beweis: Es genügt zu zeigen, dass für jedes prime Element $p \in D$ ein Koeffizient c von fg existiert, sodass $p \nmid c$ (dann haben die Koeffizienten von fg keinen nichttrivialen gemeinsamen Teiler).
Sei also $p \in D$ prim, $f = \sum a_k x^k$, $g = \sum b_k x^k$, $fg = \sum c_k x^k$. Wähle n minimal, sodass $p \nmid a_n$ und m minimal, sodass $p \nmid b_m$ (existieren, weil f und g primitiv sind). Dann ist $c_{n+m} = \sum_{j+k=n+m} a_j b_k$. Für $j < n$ gilt aber $p \mid a_j$ und damit $p \mid a_j b_k$. Für $j > n$ ist andererseits $k < m$, daher $p \mid b_k$ und $p \mid a_j b_k$. Also ist $c_{n+m} \equiv a_n b_m \mod p$, und weil p prim ist und weder a_n noch b_m teilt, teilt p auch $a_n b_m$ nicht, also $p \nmid c_{n+m}$.

□

Korollar 35.6 Sei D ein ZPE-Ring, $f, g \in D[x]$, $f, g \neq 0$. Dann gilt $C(fg) = C(f)C(g)$.

Beweis: Es gilt $f = C(f)\tilde{f}$ und $g = C(g)\tilde{g}$ für primitive Polynome $\tilde{f}$ und $\tilde{g}$. Damit ist $C(fg) = C(C(f)\tilde{f}C(g)\tilde{g}) = C(f)C(g)C(\tilde{f}\tilde{g}) = C(f)C(g)$, da nach dem Lemma von Gauß $C(\tilde{f}\tilde{g}) = 1$ ist.

□

Lemma 35.7 Sei D ein ZPE-Ring, K sein Quotientenkörper. Sind f,g primitiv in $D[x]$, dann gilt $f \approx g$ in $D[x]$ genau dann, wenn es auch in $K[x]$ gilt.

Beweis: („⇒“) Es gelte $f \approx g$ in $D[x]$, d.h. es gibt eine Einheit $u \in D[x]$ (u ist also auch Einheit in D) mit $f = ug$. Dann ist insbesondere $u \in K \setminus \{0\}$ und damit auch Einheit in $K[x]$, daher $f \approx g$ in $K[x]$.
(„⇐“) Es sei $f = \frac{c}{d}g$ für ein $\frac{c}{d} \in K \setminus \{0\}$. Es gelte o.B.d.A. $\mathrm{ggT}(c, d) = 1$ (eine solche gekürzte Darstellung existiert). Dann folgt aus $df = cg$:

$$d = d \cdot 1 \approx dC(f) \approx C(df) = C(cg) \approx cC(g) \approx c \cdot 1 \approx c$$

in D, also $c \approx d$ in D.

Es ist daher $c = dv$ für eine Einheit $v \in D$, damit $\frac{c}{d} = v$ und schließlich $f = vg$, also $f \approx g$ in $D[x]$.

□

BEMERKUNG: Die Aussage „$f \approx g$ in $D[x] \Longrightarrow f \approx g$ in $K[x]$“ gilt auch für beliebige Integritätsbereiche.

Lemma 35.8 Sei D ein ZPE-Ring, K sein Quotientenkörper, $f \in D[x]$, $f \neq 0$, und f primitiv. Dann gilt:

$$f \text{ irreduzibel in } D[x] \iff f \text{ irreduzibel in } K[x]$$

Beweis: Es sei f irreduzibel in $D[x]$. Angenommen, es gäbe $g, h \in K[x]$, keine Einheiten, mit $f = gh$. Dann folgt $\deg g \geq 1$ und $\deg h \geq 1$ (weil $f, g, h \neq 0$). Seien $a, b \in D$ derart, dass $ag = g_1 \in D[x]$ und $bh = h_1 \in D[x]$. Es existieren primitive Polynome $\tilde{g}$ und $\tilde{h}$ mit $g_1 = C(g_1)\tilde{g}$ und $h_1 = C(h_1)\tilde{h}$. Es ist $\deg g = \deg g_1 = \deg \tilde{g}$ und $\deg h = \deg h_1 = \deg \tilde{h}$.
In $D[x]$ gilt $abf = g_1 h_1$, daher $ab \approx C(abf) = C(g_1 h_1) = C(g_1)C(h_1)$. Also existiert eine Einheit $u \in D$ mit $uab = C(g_1)C(h_1)$.
$abf = g_1 h_1 = uab\tilde{g}\tilde{h}$, also $f = u\tilde{g}\tilde{h}$, wobei $u\tilde{g}, \tilde{h} \in D[x]$ mit $\deg(u\tilde{g}), \deg \tilde{h} \geq 1$, also keine Einheiten, sind. Dies ist jedoch ein Widerspruch zur Irreduzibilität von f in $D[x]$.
Sei umgekehrt f irreduzibel in $K[x]$. Angenommen, es gäbe $g, h \in D[x]$, keine Einheiten, mit $f = gh$. Dann muss g oder h Einheit in $K[x]$ sein, o.B.d.A. sei g Einheit.
Dann ist $g \in K \setminus \{0\}$, $\deg g = 0$, und da $g \in D[x]$ ist, auch $g \in D$. Es folgt $1 \approx C(f) \approx C(gh) = gC(h)$ in D, d.h. $g \mid 1$, also ist g Einheit auch in D und damit in $D[x]$.

□

Satz 35.9 *Ist D ein ZPE-Ring, dann ist auch $D[x]$ ZPE-Ring.*

Beweis:

- Existenz der Zerlegung in irreduzible Elemente:
  Wenn $c \in D \subseteq D[x]$ und $c = p_1 \dots p_m$, wobei die p_i irreduzibel in D sind, dann sind sie das auch in $D[x]$.
  Sei jetzt $\deg f \geq 1$. $f = C(f)\tilde{f}$, wobei $\tilde{f}$ primitiv ist. $C(f)$ lässt sich als Produkt irreduzibler Elemente schreiben, also genügt es zu zeigen, dass sich jedes primitive Polynom $\tilde{f}$ als Produkt irreduzibler Elemente schreiben lässt.

K sei der Quotientenkörper. Dann ist $K[x]$ ein Euklidischer Bereich, also ein ZPE-Ring. Damit lässt sich $\tilde{f}$ als $\tilde{f} = h_1 \dots h_n$ mit irreduziblen $h_i \in K[x]$ schreiben. Es gibt weiters $a_i \in D$ ($a_i \neq 0$), sodass $a_i h_i = g_i \in D[x]$ und primitive $\tilde{g}_i \in D[x]$ mit $g_i = C(g_i)\tilde{g}_i$. Dann ist $\tilde{g}_i = \frac{a_i}{C(g_i)} h_i$, und in $K[x]$ gilt damit $\tilde{g}_i \approx h_i$, also ist $\tilde{g}_i$ irreduzibel in $K[x]$, weil h_i irreduzibel in $K[x]$ ist. Weil überdies $\tilde{g}_i$ primitiv ist, ist es auch irreduzibel in $D[x]$.
Es gilt $a_1 \dots a_n \tilde{f} = g_1 \dots g_n = C(g_1) \dots C(g_n)\tilde{g_1} \dots \tilde{g_n}$, und weil $\tilde{f}$ und $\tilde{g_1} \dots \tilde{g_n}$ primitiv in $D[x]$ sind, muss $a_1 \dots a_n \approx C(g_1) \dots C(g_n)$ in D gelten. Somit existiert eine Einheit $u \in D$ mit $C(g_1) \dots C(g_n) = u a_1 \dots a_n$. Damit ergibt sich $a_1 \dots a_n \tilde{f} = u a_1 \dots a_n \tilde{g_1} \dots \tilde{g_n}$, also $\tilde{f} = (u\tilde{g_1})\tilde{g_2} \dots \tilde{g_n}$, d.h. $\tilde{f}$ hat eine Zerlegung in Irreduzible.

- Eindeutigkeit der Zerlegung in irreduzible Elemente:
  Sei $f = p_1 \dots p_n g_1 \dots g_m$ mit konstanten irreduziblen $p_i \in D$ und irreduziblen Polynomen g_i mit $\deg g_i \geq 1$.
  Weil g_i irreduzibel ist, ist es auch primitiv (sonst wäre $C(g_i)\tilde{g}_i$ eine nichttriviale Zerlegung). Also ist auch $g_1 \dots g_m$ primitiv.
  Daher ist $C(f) \approx p_1 \dots p_n$. Wenn weiters $f = q_1 \dots q_k h_1 \dots h_l$ mit konstanten irreduziblen $q_i \in D$ und irreduziblen Polynomen h_i mit $\deg h_i \geq 1$ ist, dann gilt auch $C(f) \approx q_1 \dots q_k$. Wegen der Eindeutigkeit der Zerlegung in D folgt $k = n$, und es gibt eine Permutation $\pi \in S_n$ mit $p_i \approx q_{\pi(i)}$. Durch Kürzen erhält man $g_1 \dots g_m = (uh_1) \dots h_l$.
  $g_1, \dots, g_m, uh_1, \dots, h_l$ sind irreduzibel in $D[x]$, und sie sind primitiv, also sind sie auch irreduzibel in $K[x]$. Aufgrund der Eindeutigkeit der Zerlegung in $K[x]$ gilt damit $m = l$, und es gibt eine Permutation $\sigma \in S_m$ mit $g_i \approx h_{\sigma(i)}$ in $K[x]$. Weil $g_i, h_{\pi(i)}$ jedoch primitiv sind, gilt dies auch in $D[x]$.

□

Satz 35.10 (Eisensteinsches Irreduzibilitätskriterium) *Sei D ein ZPE-Ring, K sein Quotientenkörper. Sei weiters $f = \sum_{k=0}^{n} a_k x^k \in D[x]$ mit $\deg f \geq 1$. Wenn es ein irreduzibles $p \in D$ gibt, sodass $p \nmid a_n$, $p \mid a_i$ für $i = 0, \dots, n-1$, und $p^2 \nmid a_0$, dann ist f irreduzibel in $K[x]$.*

Beweis: $f = C(f)\tilde{f}$, $\tilde{f} = \sum_{k=0}^{n} a'_k x^k$. Wegen $p \nmid a_n = C(f)a'_n$ gilt $p \nmid a'_n$, analog $p^2 \nmid a'_0$.
Wegen $p \nmid a_n$ teilt p auch $C(f)$ nicht, daher gilt wegen $p \mid a_i = C(f)a'_i$ auch $p \mid a'_i$ für $i = 0, \dots, n-1$. Wir zeigen nun, dass $\tilde{f}$ in $D[x]$ irreduzibel ist:
Angenommen, es wäre $\tilde{f} = gh$, wobei $g, h \in D[x]$ keine Einheiten sind. Dann ist $\deg g \geq 1$ und $\deg h \geq 1$ (eine Konstante, die $\tilde{f}$ teilt, teilt auch $C(\tilde{f}) = 1$).

Sei $g = \sum_{k=0}^{m} b_k x^k$ mit $b_m \neq 0$ und $h = \sum_{k=0}^{l} c_k x^k$ mit $c_l \neq 0$. Es gilt $m, l \geq 1$, also auch $m, l < n$, weil $m + l = n$.
$p^2 \nmid a'_0 = b_0 c_0$, aber $p \mid a'_0$, daher teilt p genau eines der Elemente b_0, c_0, o.B.d.A. $p \mid b_0$, $p \nmid c_0$.
Sei k minimal, sodass $p \nmid b_k$ (existiert, weil p nicht alle a'_i teilt). Dann ist $0 < k \leq m < n$. Es ist jedoch $a'_k = b_0 c_k + b_1 c_{k-1} + \ldots + b_k c_0$. Weil $p \mid a'_k$ und $p \mid b_i$ für $i < k$ gilt, folgt damit aber $p \mid b_k c_0$, also entweder $p \mid b_k$ oder $p \mid c_0$, ein Widerspruch.
Damit ist gezeigt, dass $\tilde{f}$ in $D[x]$ irreduzibel ist; da es primitiv ist, ist es auch irreduzibel in $K[x]$; weil zudem $\tilde{f} \approx f$ in $K[x]$, ist f auch irreduzibel in $K[x]$.

□

Beispiel: $3x^3 + 12x^2 + 18 \in \mathbb{Z}[x]$ ist ($p = 2$) irreduzibel in $\mathbb{Q}[x]$ (aber nicht in $\mathbb{Z}[x]$!).

Bemerkung: Dieser Satz ermöglicht die Konstruktion von irreduziblen Polynomen beliebig hohen Grades über einem ZPE-Ring wie z.B. $\mathbb{Z}$.

Teil III

Gruppentheorie, 2.Teil

Kapitel 36

Freie Abelsche Gruppen

BEMERKUNG: Im folgenden werden alle Gruppen Abelsch (kommutativ) sein und additiv geschrieben werden. Damit ändern sich auch alle weiteren Notationen:

additiv	multiplikativ
$+$	$\cdot$
$a+b$	ab
$-a$	a^{-1}
$a-b$	ab^{-1}
na	a^n
$H+K$	HK
0	e

BEMERKUNG: In einer kommutativen Gruppe $(G,+)$ gilt für Untergruppen $H, K \leq G$:

$$H \vee K = \langle H \cup K \rangle = H + K = \{h + k \,|\, h \in H, k \in K\}$$

BEMERKUNG: Ist $(G,+)$ kommutativ und $X \subseteq G$, dann gilt

$$\langle X \rangle = \{k_1x_1 + \ldots + k_nx_n \,|\, n \in \mathbb{N}_0,\ x_1, \ldots, x_n \in X \text{ verschieden},\ k_1, \ldots, k_n \in \mathbb{Z}\}$$

Definition 36.1 Eine Teilmenge X einer kommutativen Gruppe A heißt *Basis* von A, wenn gilt:

- $\langle X \rangle = A$ (X ist Erzeugendensystem von A)
- Für alle paarweise verschiedenen $x_1, \ldots, x_n \in X$ und alle $k_1, \ldots, k_n \in \mathbb{Z}$ gilt: aus $k_1x_1 + \ldots + k_nx_n = 0$ folgt $\forall i : k_i = 0$ (X ist $\mathbb{Z}$-linear unabhängige Menge)

Eine Abelsche Gruppe, die eine Basis besitzt, heißt *freie Abelsche Gruppe*.

BEMERKUNG: $\{0\}$ gilt als frei Abelsch mit Basis $\emptyset$.

BEMERKUNG: Ist $\varphi : A \to B$ ein Isomorphismus, dann ist $\{x_i \mid i \in I\}$ genau dann Basis von A, wenn $\{\varphi(x_i) \mid i \in I\}$ eine Basis von B ist.

BEMERKUNG: Ist C die innere direkte Summe von $A, B \subseteq C$ sowie X eine Basis von A und Y eine Basis von B, dann ist $X \cup Y$ eine Basis von C.

Satz 36.2 *Sei A eine kommutative Gruppe. Dann sind folgende Aussagen äquivalent:*

- *A hat eine Basis $X = \{x_i \mid i \in I\} \neq \emptyset$.*
- *A ist innere direkte Summe der unendlichen zyklischen Untergruppen $\langle x_i \rangle$.*
- *$\sum_{i \in I} \mathbb{Z} \simeq A$ mit einem Isomorphismus $\varphi : \sum_{i \in I} \mathbb{Z} \to A$, der $\varphi(e_i) = x_i$ erfüllt. Dabei ist $e_i = (k_j)_{j \in I}$ mit $k_j = \begin{cases} 1 & i = j \\ 0 & i \neq j \end{cases}$.*

Beweis:

- (1. $\Rightarrow$ 2.): Da X $\mathbb{Z}$-linear unabhängig ist, gilt $\forall x \in X,\ k \in \mathbb{Z}\ kx = 0 \Rightarrow k = 0$, daher ist $\langle x \rangle$ unendlich. Wegen der Kommutativität von A ist $\langle x \rangle$ für alle $x \in X$ ein Normalteiler, und es gilt $A = \langle \bigcup_{x \in X} \langle x \rangle \rangle$, da $A = \langle X \rangle$.
  Es bleibt noch zu zeigen, dass für alle $i \in I$ $\langle x_i \rangle \cap \langle \bigcup_{j \neq i} \langle x_j \rangle \rangle = \{0\}$ gilt. Sei dazu $a \in \langle x_i \rangle \cap \langle \bigcup_{j \neq i} \langle x_j \rangle \rangle$. Dann gibt es $j_1, \ldots, j_m \in I \setminus \{i\}$ und $k_1, \ldots, k_m, l \in \mathbb{Z}$ mit $a = lx_i = k_1 x_{j_1} + \ldots + k_m x_{j_m}$. Es folgt

$$k_1 x_{j_1} + \ldots + k_m x_{j_m} - l x_i = 0 \Rightarrow k_r = 0, l = 0 \Rightarrow a = 0$$

- (2. $\Rightarrow$ 3.): Wir definieren $\varphi : \sum_{i \in I} \mathbb{Z} \to A$ durch $\varphi((k_i)_{i \in I}) = k_{i_1} x_{i_1} + \ldots + k_{i_n} x_{i_n}$, wobei $\{i_1, \ldots, i_n\} = \{i \in I \mid k_i \neq 0\}$. Dann ist φ surjektiv, weil $X \subseteq \operatorname{Im} \varphi \leq A$ gilt. φ ist injektiv, weil X $\mathbb{Z}$-linear unabhängig ist und somit

$$\begin{aligned} & k_{i_1} x_{i_1} + \ldots + k_{i_n} x_{i_n} = l_{i_1} x_{i_1} + \ldots + l_{i_n} x_{i_n} \\ \Rightarrow\ & (k_{i_1} - l_{i_1}) x_{i_1} + \ldots + (k_{i_n} - l_{i_n}) x_{i_n} = 0 \\ \Rightarrow\ & k_{i_j} = l_{i_j} \end{aligned}$$

gilt. φ ist ein Homomorphismus, weil A kommutativ ist und somit

$$\begin{aligned}\varphi((k_i + l_i)_{i\in I}) &= (k_{i_1} + l_{i_1})x_{i_1} + \ldots + (k_{i_n} + l_{i_n})x_{i_n} \\ &= k_{i_1}x_{i_1} + \ldots + k_{i_n}x_{i_n} + l_{i_1}x_{i_1} + \ldots + l_{i_n}x_{i_n} \\ &= \varphi((k_i)_{i\in I}) + \varphi((l_i)_{i\in I})\end{aligned}$$

folgt.

- (3. $\Rightarrow$ 1.): Wir zeigen dazu, dass $(e_i)_{i\in I}$ eine Basis von $\sum_{i\in I}\mathbb{Z}$ ist: wenn $(k_i)_{i\in I}$ ein Element von $\sum_{i\in I}\mathbb{Z}$ ist, dann lässt es sich als $(k_i)_{i\in I} = k_{i_1}e_{i_1} + \ldots + k_{i_n}e_{i_n}$ mit $\{i_1, \ldots, i_n\} = \{i \in I \mid k_i \neq 0\}$ schreiben. Also ist $(e_i)_{i\in I}$ ein Erzeugendensystem.
  Ist andererseits $k_{i_1}e_{i_1} + \ldots + k_{i_n}e_{i_n} = 0$, wobei die i_j paarweise verschieden sind, dann folgt $(l_i)_{i\in I} = 0$ mit

$$l_i = \begin{cases} k_{i_j} & i = i_j \in \{i_1, \ldots, i_n\} \\ 0 & \text{sonst} \end{cases}$$

  also $l_i = 0\ \forall i$ und in weiterer Folge $k_{i_j} = 0\ \forall j$. Also ist $(e_i)_{i\in I}$ auch $\mathbb{Z}$-linear unabhängig.

□

Satz 36.3 *Sei A eine freie Abelsche Gruppe mit Basis X und $i : X \to A$ die Einbettung von X in A ($i(x) = x$). Dann gibt es für alle Abelschen Gruppen H und alle Funktionen $f : X \to H$ genau einen Gruppenhomomorphismus $\overline{f} : A \to H$ mit $\overline{f} \circ i = f$ ($\overline{f}|_X = f$).*

Beweis: Da X ein Erzeugendensystem von A ist, folgt für zwei Gruppenhomomorphismen $\overline{f}, \overline{g}$ mit $\overline{f}|_X = \overline{g}|_X$ auch, dass $\overline{f} = \overline{g}$ auf ganz A gilt. Also gibt es höchstens einen solchen Gruppenhomomorphismus.
Sei andererseits $\overline{f}$ durch

$$\overline{f}(k_1x_{i_1} + \ldots + k_nx_{i_n}) = k_1f(x_{i_1}) + \ldots + k_nf(x_{i_n})$$

gegeben. Dann ist $\overline{f}$ wohldefiniert, weil jedes $x \in A$ genau eine Darstellung der Form $k_1x_{i_1} + \ldots + k_nx_{i_n}$ hat. Die Tatsache $\overline{f}|_X = f$ ist unmittelbar ersichtlich, und dass es sich um einen Gruppenhomomorphismus handelt, lässt sich leicht nachprüfen. Also gibt es tatsächlich einen eindeutigen Homomorphismus, der die Bedingungen erfüllt.

□

BEMERKUNG: Wenn A eine Abelsche Gruppe mit $\emptyset \neq X \subseteq A$ ist, sodass für jede Abelsche Gruppe H und jede Funktion $f : X \to H$ genau ein Gruppenhomomorphismus $\overline{f} : A \to H$ mit $\overline{f}|_X = f$ existiert, dann ist A eine freie Abelsche Gruppe mit Basis X (Beweis als Übung).

Satz 36.4 *Je zwei Basen einer freien Abelschen Gruppe sind gleichmächtig.*

Beweis: Wir unterscheiden die folgenden beiden Fälle:

1. Es gibt eine endliche Basis $X \subseteq A$. In diesem Fall betrachten wir $\mathrm{Hom}(A, \mathbb{Z}_2) = \{\overline{f} : A \to \mathbb{Z}_2 \,|\, \overline{f} \text{ ist Gruppenhomomorphismus}\}$. Nach vorigem Satz gibt es eine Bijektion $\varphi : \mathbb{Z}_2^X \to \mathrm{Hom}(A, \mathbb{Z}_2)$, der jeder Funktion $f : X \to \mathbb{Z}_2$ einen Homomorphismus $\varphi(f) = \overline{f}$ zuordnet. Also ist $|\mathrm{Hom}(A, \mathbb{Z}_2)| = |\mathbb{Z}_2^X| = 2^{|X|}$. Für jede weitere Basis Y muss ebenso $|\mathrm{Hom}(A, \mathbb{Z}_2)| = 2^{|Y|}$ gelten. Es folgt dann $2^{|X|} = 2^{|Y|} \Rightarrow |X| = |Y|$.

2. Alle Basen sind unendlich. In diesem Fall zeigen wir, dass für jede unendliche Basis X $|X| = |A|$ gilt. Dabei ist $|X| \leq |A|$ klar, weil $X \subseteq A$ ist.
   Für $x \in X$ gilt $|\langle x \rangle| = |\mathbb{Z}| = \aleph_0$. Sei nun $S = \bigcup_{n \in \mathbb{N}} X^n$ und für $s = (x_1, \ldots, x_n) \in S$

   $$A_s = \langle x_1, \ldots, x_n \rangle = \langle x_1 \rangle \oplus \ldots \oplus \langle x_n \rangle \simeq \mathbb{Z} \oplus \ldots \oplus \mathbb{Z}$$

   Dann ist $|A_s| = |\mathbb{Z}^n| = \aleph_0$ und $A = \bigcup_{s \in S} A_s$, also $|A| \leq |S| \cdot \aleph_0$. Weil $|X^n| = |X|$ für unendliches X gilt, folgt weiters $|S| \leq |\mathbb{N}| \cdot |X| = |X|$ und damit $|A| \leq |S| \cdot \aleph_0 \leq |X| \cdot \aleph_0 = |X|$ ($|X| \cdot \aleph_0 = |X|$, falls X unendlich ist).

□

Definition 36.5 Sei A eine freie Abelsche Gruppe und X eine Basis. Dann heißt $|X|$ der *Rang* von A.

Korollar 36.6 Sei A_1 eine freie Abelsche Gruppe mit Basis X_1 und A_2 eine freie Abelsche Gruppe mit Basis X_2. Dann gilt $A_1 \simeq A_2 \Leftrightarrow |X_1| = |X_2|$.

Beweis: "⇒": Ist $\varphi : A_1 \to A_2$ ein Isomorphismus, dann ist $f(X_1)$ eine Basis von A_2 mit $|f(X_1)| = |X_1|$, also folgt $|X_2| = |f(X_1)| = |X_1|$.
"⇐": Sei umgekehrt $g : X_1 \to X_2$ eine Bijektion. Dann lässt sich diese zu einem Homomorphismus $\varphi : A_1 \to A_2$ fortsetzen, der $\varphi \circ i_1 = i_2 \circ g$ erfüllt (dabei sind i_1, i_2 die Inklusionen von X_1, X_2 in A_1, A_2). Ebenso lässt sich g^{-1} zu einem Homomorphismus ψ fortsetzen, der $\psi \circ i_2 = i_1 \circ g^{-1}$ erfüllt.

Dann ist $\psi \circ \varphi$ ein Homomorphismus mit $\psi \circ \varphi \circ i_1 = \psi \circ i_2 \circ g = i_1 \circ g^{-1} \circ g = i_1$, d.h. $\psi \circ \varphi$ ist die eindeutige Fortsetzung von i_1 zu einem Homomorphismus. id_{A_1} ist jedoch auch eine Fortsetzung von i_1 zu einem Homomorphismus, also gilt $\psi \circ \varphi = \mathrm{id}_{A_1}$ und analog auch $\varphi \circ \psi = \mathrm{id}_{A_2}$. Damit sind φ und ψ sogar Isomorphismen.

□

Satz 36.7 *Jede Abelsche Gruppe mit Erzeugendensystem X ist homomorphes Bild einer freien Abelschen Gruppe vom Rang $|X|$.*

Beweis: Sei $(G, +)$ Abelsch und $G = \langle X \rangle$, wobei $X = \{x_i \mid i \in I\}$. Sei $A = \sum_{i \in I} \mathbb{Z}$ die freie Abelsche Gruppe und $f : \{e_i \mid i \in I\} \to X$ durch $f(e_i) = x_i$ gegeben. Dann erfüllt jener eindeutige Homomorphismus $\varphi : A \to G$ mit $\varphi|_{\{e_i \mid i \in I\}} = f$ das Gewünschte. φ ist surjektiv, weil $X = \mathrm{Im}\, f \subseteq \mathrm{Im}\, \varphi$ gilt und X ein Erzeugendensystem von G ist.

□

Kapitel 37

Matrizenumformungen

Definition 37.1 Gegeben sei eine Matrix $A \in M_{n\times m}(R)$. Eine *elementare Zeilenoperation* ist das Addieren des λ-fachen der j-ten Zeile zur i-ten Zeile von A für $i \neq j$ und $\lambda \in R$. Dies entspricht einer Multiplikation von A mit der Matrix $E_{ij}(\lambda)$ von links ($A \mapsto E_{ij}(\lambda) \cdot A$) – dabei ist $E_{ij}(\lambda)$ jene Matrix, die durch Hinzufügen des Eintrags λ an der Stelle (i, j) (i-te Zeile, j-te Spalte) aus der Einheitsmatrix entsteht.
Analog ist eine *elementare Spaltenoperation* das Addieren des λ-fachen der j-ten Spalte zur i-ten Spalte von A für $i \neq j$ und $\lambda \in R$. Dies entspricht einer Multiplikation von A mit der Matrix $E_{ji}(\lambda)$ von rechts ($A \mapsto A \cdot E_{ji}(\lambda)$).

Bemerkung: Mit $E_{ij}(\lambda)$ ist dabei stets eine Matrix der passenden Größe gemeint – wenn A eine $n \times m$-Matrix ist, dann soll in $E_{ij}(\lambda) \cdot A$ $E_{ij}(\lambda)$ eine $n \times n$-, in $A \cdot E_{ij}(\lambda)$ eine $m \times m$-Matrix sein.

Bemerkung: Wir können uns im Folgenden auf elementare Zeilen- und Spaltenoperationen beschränken und auf Zeilen- oder Spaltenvertauschungen verzichten. Durch elementare Zeilenumformungen lässt sich nämlich ein Vertauschen der Zeilen i und j mit anschließender Multiplikation der j-ten Zeile mit -1 erreichen: man addiert die j-te Zeile zur i-ten, anschließend subtrahiert man die i-te von der j-ten, und schließlich addiert man wieder die j-te zur i-ten. Danach steht in der j-ten Zeile die ursprüngliche i-te, negativ genommen, und in der i-ten die ursprüngliche j-te.
Daher lässt sich jede Permutation von Zeilen (und analog auch von Spalten) – bei ungeraden Permutationen mit zusätzlichem Multiplizieren einer Zeile mit -1 – durch elementare Zeilenumformungen darstellen.
Im Folgenden wird es jedoch auf Multiplikation von Zeilen oder Spalten mit -1 nie ankommen: wir können statt einer Permutation von Zeilen oder Spalten stets die angeführte modifizierte Permutation verwenden.

Lemma 37.2 Sei A eine $n \times m$-Matrix mit Eintragungen in einem Euklidischen Ring R. Durch elementare Zeilen- und Spaltenumformungen kann A auf eine Form $A' = (a'_{ij})$ gebracht werden, wobei a'_{11} alle Eintragungen von A' teilt.

Beweis: O.B.d.A. darf angenommen werden, dass A nicht die Nullmatrix ist (andernfalls erfüllt A bereits die Bedingung). Dann lässt sich durch elementare Zeilen- und Spaltenumformungen $a_{11} \neq 0$ erreichen. Wir behaupten nun, dass wir A auf eine Form $B = (b_{ij})$ mit $\rho(b_{11}) < \rho(a_{11})$ bringen können, wenn a_{11} noch nicht alle Einträge teilt. Ist diese Behauptung gezeigt, dann folgt das Gewünschte, denn da die Folge $\rho(a_{11}) > \rho(b_{11}) > \ldots$ nur endlich sein kann, bricht diese Umformungskette nach endlich vielen Schritten ab, sodass dann a'_{11} tatsächlich alle Einträge teilt.
Der Beweis dieser Behauptung erfolgt in zwei Schritten:

1. Falls a_{11} nicht alle Eintragungen der ersten Zeile und der ersten Spalte teilt (o.B.d.A. sei ersteres der Fall), dann gibt es ein j, sodass $a_{11} \nmid a_{1j}$. Wir können eine Division mit Rest durchführen: $a_{1j} = qa_{11} + r$ mit $r \neq 0$ und $\rho(r) < \rho(a_{11})$. Wir ziehen nun das q-fache der ersten Spalte von der j-ten Spalte ab. Dann steht r in der Position $(1, j)$ und lässt sich durch Vertauschung in die erste Spalte bringen. Wir erhalten ein B mit $\rho(b_{11}) = \rho(r) < \rho(a_{11})$.

2. Falls a_{11} alle Eintragungen der ersten Zeile und der ersten Spalte teilt, kann man derart elementare Zeilen- und Spaltenumformungen machen, dass in der ersten Zeile und Spalte außer a_{11} nur noch Nullen stehen. Wir erhalten eine Matrix B, in der a_{11} genau dann b_{ij} teilt, wenn a_{11} a_{ij} teilt (bei allen Umformungen wurden stets nur Vielfache von a_{11} abgezogen). An zumindest einer Stelle muss daher ein b_{ij} stehen, das von a_{11} nicht geteilt wird. Durch Addition der i-ten Zeile zur ersten Zeile kann man diesen Eintrag in die erste Zeile bringen, wobei an der Stelle $(1, 1)$ weiterhin a_{11} steht. Damit haben wir das Problem auf den ersten Fall zurückgeführt.

□

Satz 37.3 *Sei A eine $n \times m$-Matrix über einem Euklidischen Ring R. Dann kann A durch elementare Zeilen- und Spaltenumformungen auf Diagonalform $B = \mathrm{diag}(b_1, \ldots, b_k)$ $(k = \min(n, m))$ gebracht werden, sodass $b_1 \mid b_2 \mid \ldots \mid b_k$.*

Beweis: Wir führen eine Induktion nach $\max(m, n)$ durch: falls $\max(m, n) = 1$ ist, hat die Matrix bereits die gewünschte Form. Andernfalls sei A eine Matrix mit $max(m, n) > 1$. Durch elementare Zeilen- und Spaltenoperationen

kann man A auf die Form $A' = (a'_{ij})$ mit $a'_{11} \mid a'_{ij}$ für alle i, j bringen (nach dem vorigen Lemma). Dann ist $a'_{1j} = q_j a'_{11}$ und $a'_{j1} = r_j a'_{11}$. Für alle $j > 1$ zieht man nun das q_j-fache der ersten Spalte von der j-ten Spalte und das r_j-fache der ersten Zeile von der j-ten Zeile ab. Dadurch werden in der ersten Zeile und in der ersten Spalte alle Einträge außer dem ersten zu 0.
Wir erhalten eine Matrix B mit $b_{11} = a'_{11}$ als einzigem Element $\neq 0$ in der ersten Zeile bzw. Spalte. Alle übrigen Einträge haben die Form $b_{ij} = a'_{ij} - q_j a'_{i1} = a'_{ij} - q_j r_i a'_{11}$ und sind daher durch $a'_{11} = b_{11}$ teilbar. Wenn man nun also die erste Zeile und Spalte von B weglässt, so kann man auf die verbliebene Matrix C die Induktionsvoraussetzung anwenden:
C kann durch elementare Zeilen- und Spaltenoperationen auf Diagonalgestalt $\mathrm{diag}(c_1, \ldots, c_l)$ mit $c_1 \mid c_2 \mid \ldots \mid c_l$ gebracht werden, wobei diese Operationen auch gleich auf ganz B angewandt werden können. Sie ändern auch nichts an der Tatsache, dass b_{11} alle Einträge von C teilt. Man erhält daher wie gewünscht eine Matrix der Gestalt $\mathrm{diag}(b_{11}, c_1, \ldots, c_l)$ mit $b_{11} \mid c_1 \mid \ldots \mid c_l$.

□

Kapitel 38

Endlich erzeugte Abelsche Gruppen

Lemma 38.1 Sei $(M, +)$ eine Abelsche Gruppe, M' eine Untergruppe. Wenn sowohl M' als auch M/M' die Eigenschaft haben, dass jede Untergruppe endlich erzeugt ist, dann hat auch M diese Eigenschaft.

Beweis: Sei $N \leq M$. Dann ist $N \cap M'$ endlich erzeugt durch gewisse $n_1, \ldots, n_s \in N \cap M'$, und auch $\overline{N} = (N + M')/M'$ ist endlich erzeugt durch gewisse $l_1 + M', \ldots, l_t + M'$ mit $l_1, \ldots, l_t \in N$.
$l_1, \ldots, l_t, n_1, \ldots, n_s$ erzeugen dann N: sei dazu $g \in N$. Dann ist $g + M' = r_1(l_1 + M') + \ldots + r_t(l_t + M')$ für gewisse $r_1, \ldots, r_t \in \mathbb{Z}$. Damit lässt sich g in der Form

$$g = r_1 l_1 + \ldots + r_t l_t + m'$$

mit einem $m' \in M'$ (das auch in N liegen muss, da $g, l_1, \ldots, l_t$ in N liegen) darstellen. Es gibt daher $k_1, \ldots, k_s \in \mathbb{Z}$, sodass $m' = k_1 n_1 + \ldots + k_s n_s$. Es folgt

$$g = r_1 l_1 + \ldots + r_t l_t + k_1 n_1 + \ldots + k_s n_s$$

□

Lemma 38.2 Jede Untergruppe einer endlich erzeugten Abelschen Gruppe ist endlich erzeugt.

Beweis: Sei M erzeugt durch $m_1, \ldots, m_t$. Wir führen eine Induktion nach t durch:

- Für $t = 1$ ist M zyklisch. Wir wissen bereits, dass dann jede Untergruppe auch zyklisch ist.

- Die Behauptung gelte für alle Gruppen mit $t-1$ Erzeugern. Sei nun $M' = \langle m_t \rangle$. Dann wird M/M' von den $t-1$ Elementen $m_i + M'$ $(i = 1, \ldots, t-1)$ erzeugt. Nach Induktionsvoraussetzung ist jede Untergruppe von M' und jede Untergruppe von M/M' endlich erzeugt. Nach dem vorigen Lemma ist somit jede Untergruppe von M endlich erzeugt.

□

Lemma 38.3 Seien $(F, +)$ eine Abelsche Gruppe und $v_1, \ldots, v_n \in F$. Dann gelten die folgenden Aussagen:

- Seien $1 \leq i, j \leq n$, $i \neq j$ und $\lambda \in \mathbb{Z}$. Wenn $w_j = v_j + \lambda v_i$ und $w_k = v_k$ für $k \neq j$ definiert werden, dann erzeugen $v_1, \ldots, v_n$ und $w_1, \ldots, w_n$ dieselbe Untergruppe von F.
- Wenn $v_1, \ldots, v_n$ eine Basis von F ist und $w_1, \ldots, w_n$ wie in 1. gewählt werden, dann ist auch $w_1, \ldots, w_n$ eine Basis von F.

Beweis: als Übung.

Lemma 38.4 Sei $(F, +)$ eine freie Abelsche Gruppe mit Basis $e_1, \ldots, e_n$, und seien $w_1, \ldots, w_m \in F$. Wenn $A \in M_{n \times n}(\mathbb{Z})$ jene Matrix ist, deren k-te Zeile die Koeffizienten von w_k zur Basis $e_1, \ldots, e_n$ enthält, d.h. $w_k = a_{k1}e_1 + \ldots + a_{kn}e_n$, dann gilt:

- $A \cdot E_{ji}(\lambda)$ ist jene Matrix, deren k-te Zeile die Koeffizienten von w_k zur Basis $e'_1, \ldots, e'_n$ mit $e'_j = e_j + \lambda e_i$ und $e'_l = e_l$ $(l \neq j)$ enthält.
- $E_{ji}(\lambda) \cdot A$ ist jene Matrix, deren k-te Zeile die Koeffizienten von w'_k zur Basis $e_1, \ldots, e_n$ mit $w'_i = w_i + \lambda w_j$ und $w'_l = e_l$ $(l \neq i)$ enthält.

Beweis: als Übung.

Satz 38.5 *Sei $(F, +)$ eine freie Abelsche Gruppe vom Rang n, G eine Untergruppe. Dann existieren eine Basis $e_1, \ldots, e_n$ von F und $d_1, \ldots, d_n \in \mathbb{N}_0$ mit $d_1 \mid \ldots \mid d_n$, sodass $G = \langle d_1 e_1, \ldots, d_n e_n \rangle$. Insbesondere ist G eine freie Abelsche Gruppe mit Basis $d_1 e_1, \ldots, d_k e_k$, wobei d_k der letzte Wert $\neq 0$ ist.*

Beweis: G ist als Untergruppe einer endlich erzeugten Gruppe endlich erzeugt, und zwar durch Elemente $g_1, \ldots, g_m$. Dabei darf angenommen werden, dass $m \geq n$ ist, da man sonst beliebige Elemente von G hinzufügen kann. Sei $A = (a_{ij})$ die Matrix der Koeffizienten der g_i zur Basis $e_1, \ldots, e_n$, d.h. $g_i = a_{i1}e_1 + \ldots + a_{in}e_n$.

A kann durch elementare Spaltenoperationen (was einem Übergang zu einer anderen Basis von F entspricht) und elementare Zeilenoperationen (was einem Übergang zu einem anderen Erzeugendensystem von G entspricht) sowie durch Zeilen- und Spalten vertauschungen (welche einem Umordnen der Basis von F bzw. des Erzeugendensystems von G entsprechen) auf die Form $A' = \mathrm{diag}(d_1, \ldots, d_n)$ mit $d_1 \mid \ldots \mid d_n$ gebracht werden, wobei A' wieder eine Matrix von Koeffizienten von einem Erzeugendensystem von G zu einer Basis von F ist; d.h., es existiert eine Basis $e'_1, \ldots, e'_n$, sodass $g'_i = a'_{i1}e'_1 + \ldots + a'_{in}e'_n$ $(1 \leq i \leq n)$ ein Erzeugendensystem von G ist. Wegen der speziellen Gestalt von A' ist $g'_i = d_i e'_i$ mit $d_1 \mid \ldots \mid d_n$.

□

Satz 38.6 *Sei G eine endlich erzeugte Abelsche Gruppe. Dann gibt es Zahlen $m_1, \ldots, m_r \in \mathbb{N}$ $(r \geq 0)$ mit $m_1 \mid \ldots \mid m_r$ und $m_1 > 1$, sodass*

$$G \simeq Z_{m_1} \oplus \ldots \oplus \mathbb{Z}_{m_r} \oplus H$$

mit $H = \sum_{i=1}^{s} \mathbb{Z}$ $(s \geq 0)$ ist.

Bemerkung: In dieser Darstellung sind $m_1, \ldots, m_r$ und s eindeutig bestimmt (wird später bewiesen). $m_1, \ldots, m_r$ heißen *invariante Faktoren* von G.

Beweis: Sei G erzeugt von n Elementen und F die freie Abelsche Gruppe vom Rang n. Dann gibt es einen Epimorphismus $f : F \to G$. Sei K dessen Kern. Nach dem ersten Isomorphiesatz gilt dann $G \simeq F/K$. Nach dem vorigen Satz gibt es eine Basis $e_1, \ldots, e_n$ von F und $d_1, \ldots, d_n \in \mathbb{N}_0$ mit $d_1 \mid \ldots \mid d_n$, sodass $K = \langle d_1 e_1, \ldots, d_n e_n \rangle = \langle d_1 e_1 \rangle \oplus \ldots \oplus \langle d_n e_n \rangle$ ist. Es folgt

$$\begin{aligned} G \simeq F/K &\simeq (\langle e_1 \rangle \oplus \ldots \oplus \langle e_n \rangle)/(\langle d_1 e_1 \rangle \oplus \ldots \oplus \langle d_n e_n \rangle) \\ &= \langle e_1 \rangle / \langle d_1 e_1 \rangle \oplus \ldots \oplus \langle e_1 \rangle / \langle d_1 e_1 \rangle \\ &\simeq \mathbb{Z}/(d_1\mathbb{Z}) \oplus \ldots \oplus \mathbb{Z}/(d_n\mathbb{Z}) \end{aligned}$$

wobei die vorletzte Gleichheit nach Korollar 13.12 gilt. Für $d_i = 1$ fällt $\mathbb{Z}/(d_i\mathbb{Z}) = \mathbb{Z}/\mathbb{Z} = \{0\}$ weg, für $d_i = 0$ ist $\mathbb{Z}/(d_i\mathbb{Z}) = \mathbb{Z}/\{0\} = \mathbb{Z}$. Sei nun $(d_1, \ldots, d_n) = (1, \ldots, 1, d_j, \ldots, d_k, 0, \ldots, 0)$, wobei am Schluss genau s Nullen stehen. Die Werte $d_j, \ldots, d_k$ sind dann unsere $m_1, \ldots, m_r$, und es gilt in der Tat

$$G \simeq Z_{m_1} \oplus \ldots \oplus \mathbb{Z}_{m_r} \oplus H$$

□

Lemma 38.7 Für $m, n \in \mathbb{N}$ mit $\mathrm{ggT}(m,n) = 1$ gilt $\mathbb{Z}_{mn} \simeq \mathbb{Z}_m \oplus \mathbb{Z}_n$.

Beweis: Dieses Lemma ist eine unmittelbare Folgerung aus dem Chinesischen Restsatz, angewandt auf $\mathbb{Z}$.

Korollar 38.8 Ist $m = p_1^{\alpha_1} \cdot \ldots \cdot p_k^{\alpha_k}$, wobei $p_1, \ldots, p_k$ verschiedene Primzahlen und $\alpha_i \in \mathbb{N}$ sind, dann gilt

$$\mathbb{Z}_m \simeq \mathbb{Z}_{p_1^{\alpha_1}} \oplus \ldots \oplus \mathbb{Z}_{p_k^{\alpha_k}}$$

Beweis: durch Induktion nach k.

Satz 38.9 *Sei G eine endlich erzeugte Abelsche Gruppe. Dann existieren Primzahlen $p_1, \ldots, p_k$ ($k \geq 0$), $n_1, \ldots, n_k \in \mathbb{N}$, $\alpha_{ij} \in \mathbb{N}$ und $s \in \mathbb{N}_0$, sodass*

$$G \simeq \mathbb{Z}_{p_1^{\alpha_{11}}} \oplus \ldots \oplus \mathbb{Z}_{p_1^{\alpha_{1n_1}}} \oplus \ldots \oplus \mathbb{Z}_{p_k^{\alpha_{k1}}} \oplus \ldots \oplus \mathbb{Z}_{p_k^{\alpha_{kn_k}}} \oplus H$$

mit $H = \sum_{i=1}^{s} \mathbb{Z}$.

Beweis: Dieser Satz folgt unmittelbar aus $G \simeq \mathbb{Z}_{m_1} \oplus \ldots \oplus \mathbb{Z}_{m_r} \oplus H$ und $\mathbb{Z}_{m_i} \simeq \mathbb{Z}_{p_1^{\alpha_{1i}}} \oplus \ldots \oplus \mathbb{Z}_{p_k^{\alpha_{ki}}}$.

□

Bemerkung: Die Potenzen $p_i^{\alpha_{ij}}$, die hierbei vorkommen, sind ebenso wie s eindeutig und heißen *Elementarteiler* von G.

Eindeutigkeit der invarianten Faktoren und Elementarteiler:

Lemma 38.10 Sei $(A, +)$ eine Abelsche Gruppe, $m \in \mathbb{N}$ und p eine Primzahl. Folgende Mengen sind Untergruppen von A:

1. $mA = \{ma \,|\, a \in A\}$
2. $A[m] = \{a \in A \,|\, ma = 0\} = \{a \in A \,|\, |a| \Big| m\}$
3. $A(p) = \{a \in A \,|\, \exists n \in \mathbb{N}_0 : \ |a| = p^n\} = \{a \in A \,|\, \exists n \in \mathbb{N}_0 : \ p^n a = 0\} = \bigcup_{n=0}^{\infty} A[p^n]$
4. $A_t = \{a \in A \,|\, \exists n \in \mathbb{N} : na = 0\} = \{a \in A \,|\, |a| \text{ ist endlich}\}$

Bemerkung: Für nichtkommutative Gruppen ist im Allgemeinen keine dieser Mengen eine Untergruppe!

Beweis: Alle diese Mengen sind nichtleer, da 0 enthalten ist. Wir zeigen jeweils $a, b \in G$ (wobei G die jeweilige Menge ist) $\Rightarrow a - b \in G$:

1. $ma - mb = m(a - b)$
2. $ma = 0$, $mb = 0 \Rightarrow m(a - b) = ma - mb = 0 - 0 = 0$
3. $p^n a = 0$, $p^m b = 0 \Rightarrow p^\mu a = p^\mu b = 0$ für $\mu = \max(m, n)$, also $p^\mu(a-b) = p^\mu a - p^\mu b = 0 - 0 = 0$
4. $ma = 0$, $nb = 0 \Rightarrow (mn)a = (mn)b = 0 \Rightarrow (mn)(a - b) = (mn)a - (mn)b = 0 - 0 = 0$

□

Lemma 38.11 Für die eben definierten Gruppen gelten folgende Zusammenhänge:

1. $\mathbb{Z}_{p^n}[p] \simeq \mathbb{Z}_p$
2. $p^m\mathbb{Z}_{p^n} \simeq \mathbb{Z}_{p^{n-m}}$ (für $m < n$)
3. $(\sum_{i\in I} G_i)[m] = \sum_{i\in I}(G_i[m])$ und $m\sum_{i\in I} G_i = \sum_{i\in I} mG_i$
4. Wenn $f : G \to H$ ein Gruppenisomorphismus ist, dann ist $f|_{G_t} : G_t \to H_t$ auch ein Gruppenisomorphismus, und für eine Primzahl p ist $f|_{G(p)} : G(p) \to H(p)$ ebenso ein Gruppenisomorphismus.

Beweis:

1. Es gilt $|\overline{p^{n-1}}| = p$ in $\mathbb{Z}_{p^n}$. Daher genügt es zu zeigen, dass $\mathbb{Z}_{p^n}[p] = \langle\overline{p^{n-1}}\rangle$ ist. Jedenfalls gilt $\langle\overline{p^{n-1}}\rangle \subseteq \mathbb{Z}_{p^n}[p]$. Ist andererseits $k \in \mathbb{Z}$ derart, dass $p\overline{k} = \overline{0}$ in $\mathbb{Z}_{p^n}$ gilt, dann muss $p^n|pk$ und in weiterer Folge $p^{n-1}|k$ gelten. Also ist $\overline{k} = m\overline{p^{n-1}}$ in $\mathbb{Z}_{p^n}$, und es folgt, dass $\mathbb{Z}_{p^n}[p]$ von $\overline{p^{n-1}}$ erzeugt wird.
2. $p^m\mathbb{Z}_{p^n} = \{p^m\overline{k} \mid k \in \mathbb{Z}\} = \{k\overline{p^m} \mid k \in \mathbb{Z}\} = \langle\overline{p^m}\rangle$; nun ist $|\overline{p^m}| = p^{n-m}$ in $\mathbb{Z}_{p^n}$, also ist $p^m\mathbb{Z}_{p^n}$ die zyklische Gruppe der Ordnung p^{n-m}.
3. folgt unmittelbar aus $m(a_i)_{i\in I} = (ma_i)_{i\in I}$
4. folgt unmittelbar aus der Tatsache, dass für einen Isomorphismus f $|f(g)| = |g|$ $\forall g \in G$ gilt.

□

Lemma 38.12 Sei p eine Primzahl und $G \simeq \sum_{i=1}^{r} \mathbb{Z}_{p^{\alpha_i}} \simeq \sum_{j=1}^{r'} \mathbb{Z}_{p^{\beta_j}}$ $(r, r' \in \mathbb{N}, \alpha_i, \beta_j \in \mathbb{N})$. Dann gilt $r = r'$ und $\forall n \in \mathbb{N}$ $|\{i \mid \alpha_i = n\}| = |\{j \mid \beta_j = n\}|$.

Beweis: Wir zeigen, dass für alle n

$$a(n) := |\{i \,|\, \alpha_i \geq n\}| = |\{j \,|\, \beta_j \geq n\}| =: b(n)$$

gilt. Dann folgt die Behauptung wegen $|\{i \,|\, \alpha_i = n\}| = a(n) - a(n-1)$ und $|\{j \,|\, \beta_j = n\}| = b(n) - b(n-1)$.
Dazu zeigen wir, dass $|(p^{n-1}G)[p]| = p^{a(n)}$ gilt: $p^{n-1}\mathbb{Z}_{p^\alpha} \neq \{0\} \Leftrightarrow \alpha \geq n$; $G = \sum_{i=1}^{r} \mathbb{Z}_{p^{\alpha_i}}$. Also folgt

$$p^{n-1}G = \sum_{i=1}^{r} p^{n-1}\mathbb{Z}_{p^{\alpha_i}} \simeq \sum_{k=1}^{a(n)} p^{n-1}\mathbb{Z}_{p^{\alpha_{i_k}}} = \sum_{k=1}^{a(n)} \mathbb{Z}_{p^{\alpha_{i_k}-n+1}}$$

wobei die i_k genau jene sind, für die $\alpha_{i_k} \geq n$ ist. Daraus ergibt sich weiter

$$(p^{n-1}G)[p] = \sum_{k=1}^{a(n)} \mathbb{Z}_{p^{\alpha_{i_k}-n+1}}[p] \simeq \sum_{k=1}^{a(n)} \mathbb{Z}_p$$

und daher die Behauptung. Analog gilt auch $|(p^{n-1}G)[p]| = p^{b(n)}$ und damit $p^{a(n)} = p^{b(n)} \;\Rightarrow\; a(n) = b(n)$.

□

Lemma 38.13 Sei G eine Abelsche Gruppe und $G \simeq H_1 \oplus G_1 \simeq H_2 \oplus G_2$, wobei G_1, G_2 endlich und H_1, H_2 frei Abelsch mit den Rängen s_1, s_2 sind. Dann gilt $G_1 \simeq G_2 \simeq G_t$, $H_1 \simeq H_2 \simeq G/G_t$ und $s_1 = s_2$.

Beweis: $(a, b) \in H_1 \oplus G_1$ hat genau dann endliche Ordnung, wenn $a = 0$ ist, also folgt $G_t \simeq (H_1 \oplus G_1)_t = \{0\} \oplus G_1 \simeq G_1$ und analog auch $G_2 \simeq G_t$. Es folgt weiters

$$G/G_t \simeq (H_1 \oplus G_1)/(\{0\} \oplus G_1) \simeq H_1/\{0\} \oplus G_1/G_1 \simeq H_1 \oplus \{0\} \simeq H_1$$

und analog $G/G_t \simeq H_2$, daher $H_1 \simeq H_2$ und $s_1 = s_2$.

□

Satz 38.14 *Sei G eine endlich erzeugte Abelsche Gruppe. Dann gilt*

1. *In jeder Darstellung von G als direkte Summe zyklischer Gruppen ist die Anzahl der vorkommenden unendlichen Faktoren dieselbe.*

2. Wenn

$$\begin{aligned} G &\simeq \mathbb{Z}_{p_1^{\alpha_{11}}} \oplus \ldots \oplus \mathbb{Z}_{p_1^{\alpha_{1n_1}}} \oplus \ldots \oplus \mathbb{Z}_{p_k^{\alpha_{k1}}} \oplus \ldots \oplus \mathbb{Z}_{p_k^{\alpha_{kn_k}}} \oplus \sum_{i=1}^{s} \mathbb{Z} \\ &\simeq \mathbb{Z}_{p_1^{\beta_{11}}} \oplus \ldots \oplus \mathbb{Z}_{p_1^{\beta_{1m_1}}} \oplus \ldots \oplus \mathbb{Z}_{p_k^{\beta_{k1}}} \oplus \ldots \oplus \mathbb{Z}_{p_k^{\beta_{km_k}}} \oplus \sum_{i=1}^{s'} \mathbb{Z} \end{aligned}$$

gilt, wobei $p_1, \ldots, p_k$ verschiedene Primzahlen sind und $\alpha_{ij}, \beta_{ij} \in \mathbb{N}_0$, dann gilt $s = s'$, und für jedes p_i gilt

$$\forall n \in \mathbb{N} \; |\{j \,|\, \alpha_{ij} = n\}| = |\{j \,|\, \beta_{ij} = n\}|$$

(*Eindeutigkeit der Elementarteiler*).

3. Wenn

$$G \simeq \mathbb{Z}_{m_1} \oplus \ldots \oplus \mathbb{Z}_{m_r} \oplus \sum_{i=1}^{s} \mathbb{Z} \simeq \mathbb{Z}_{n_1} \oplus \ldots \oplus \mathbb{Z}_{n_t} \oplus \sum_{i=1}^{s'} \mathbb{Z}$$

mit $1 < m_1 \,|\, \ldots \,|\, m_r$ und $1 < n_1 \,|\, \ldots \,|\, n_t$ gilt, dann ist $r = t$, $s = s'$ und $m_i = n_i$ $(1 \leq i \leq r)$ (*Eindeutigkeit der invarianten Faktoren*).

Beweis:

1. Nach dem vorigen Lemma ist die Anzahl der unendlichen Faktoren gleich dem Rang von G/G_t, also in allen Darstellungen dieselbe.

2. Wegen 1. gilt $s = s'$ jedenfalls. Für alle i gilt weiters

$$G(p_i) \simeq \mathbb{Z}_{p_i^{\alpha_{i1}}} \oplus \ldots \oplus \mathbb{Z}_{p_i^{\alpha_{in_i}}} \simeq \mathbb{Z}_{p_i^{\beta_{i1}}} \oplus \ldots \oplus \mathbb{Z}_{p_i^{\beta_{im_i}}}$$

weil $|(a_1, \ldots, a_m)| = \mathrm{kgV}(|a_1|, \ldots, |a_m|)$ ist und dies somit nur genau dann eine Potenz von p_i sein kann, wenn $a_l = 0$ in allen Faktoren außer den $\mathbb{Z}_{p_i^k}$ ist. Nach dem Lemma 38.12 sind damit die vorhandenen Potenzen von p_i dieselben.

3. Wieder folgt $s = s'$ aus 1. Seien nun $p_1, \ldots, p_k$ die Potenzen, die eines der m_i oder n_i teilen. Nun kann man die m_i, n_i in der Form $m_i = \prod_{j=1}^{k} p_j^{\alpha_{ij}}$ bzw. $n_i = \prod_{j=1}^{k} p_j^{\beta_{ij}}$ schreiben. Es folgt

$$G \simeq \sum_{j=1}^{k} \sum_{i=1}^{r} \mathbb{Z}_{p_j^{\alpha_{ij}}} \oplus \mathbb{Z}^s \simeq \sum_{j=1}^{k} \sum_{i=1}^{t} \mathbb{Z}_{p_j^{\beta_{ij}}} \oplus \mathbb{Z}^s$$

Wegen 2. muss dann $\forall i\ \forall n\ |\{j \mid \alpha_{ij} = n\}| = |\{j \mid \beta_{ij} = n\}|$ gelten. Da $m_i\ m_{i+1}$ teilen soll, wird m_r von allen übrigen m_i geteilt, also ergibt sich für alle j:

$$\alpha_{rj} = \max\{\alpha_{ij} \mid i = 1, \ldots, r\} = \max\{\beta_{ij} \mid i = 1, \ldots, t\} = \beta_{tj}$$

Daher ist $m_r = n_t$, analog dann $m_{r-1} = n_{t-1}$ etc. und $r = t$.

□

Teil IV

Körpertheorie

Kapitel 39

Körpererweiterungen

Definition 39.1 Wenn F, K Körper mit $K \leq F$ sind, dann heißt das Paar K, F eine *Körpererweiterung* (geschrieben $F : K$). F heißt *Erweiterungskörper* von K.

Bemerkung: Wenn $F : K$ eine Körpererweiterung ist, dann ist F ein K-Vektorraum: $(F, +)$ ist eine Abelsche Gruppe, die Skalarmultiplikation $K \times F \to F$ ist die Einschränkung der Multiplikation in F auf Paare in $K \times F$.

Definition 39.2 Sei $F : K$ eine Körpererweiterung. Die Dimension von F als K-Vektorraum heißt *Grad* der Körpererweiterung $F : K$, man schreibt $[F : K] = \dim_K F$.

Lemma 39.3 Seien K, E, F Körper mit $K \leq E \leq F$; sei B eine Basis von F als E-Vektorraum, C eine Basis von E als K-Vektorraum. Dann ist $D = (d_{(c,b)})_{(c,b)\in C\times B}$ mit $d_{(c,b)} = cb$ eine Basis von F als K-Vektorraum.

Beweis: Sei $f \in F$. Dann existieren $b_1, \ldots, b_n \in B$ und $e_1, \ldots, e_n \in E$, sodass $f = e_1 b_1 + \ldots + e_n b_n$. Weiters existieren $c_1, \ldots, c_m \in C$ und $k_{ij} \in K$, sodass $e_i = \sum_{j=1}^{m} k_{ij} c_j$, also $f = \sum_{i=1}^{n} \sum_{j=1}^{m} k_{ij} c_j b_i$.
f ist daher K-Linearkombination von Elementen der Form $c_j b_i$, also ist D Erzeugendensystem.
Es bleibt zu zeigen, dass D linear unabhängig über K ist: seien $c_1, \ldots, c_m \in C$, $b_1, \ldots, b_n \in B$, $k_{ij} \in K$, sodass $\sum_{1\leq i\leq n, 1\leq j\leq m} k_{ij} c_j b_i = 0$. Dann ist $\sum_{i=1}^{n} (\sum_{j=1}^{m} k_{ij} c_j) b_i = 0$, und der Ausdruck in der Klammer liegt für alle i in E. Da B eine E-linear unabhängige Menge ist, folgt $\sum_{j=1}^{m} k_{ij} c_j = 0$ für alle i und damit (da C linear unabhängig über K ist) auch $k_{ij} = 0$ für alle Paare i, j.
Also muss D K-linear unabhängig sein.

□

Korollar 39.4 Für Körper K, E, F mit $K \leq E \leq F$ gilt $[F : K] = [F : E][E : K]$.

BEMERKUNG: Da wir immer mit mehreren Körpern arbeiten, ist es wesentlich, festzuhalten, über welchem Körper eine Menge linear unabhängig ist!

Definition 39.5 Sei $F : K$ eine Körpererweiterung, $S \subseteq F$. Der von S über K *erzeugte Unterring* von F ist definiert als

$$K[S] = \bigcap_{\substack{R \text{ Ring} \\ K \cup S \subseteq R \subseteq F}} R$$

(dies ist einfach der von $K \cup S$ erzeugte Unterring von F).
Der von S über K *erzeugte Unterkörper* ist definiert als

$$K(S) = \bigcap_{\substack{E \text{ Körper} \\ K \cup S \subseteq E \subseteq F}} E$$

der von $K \cup S$ erzeugte Unterkörper von F).

BEMERKUNG: $K(S)$ ist ebenso wie $K[S]$ wohldefiniert, da der Durchschnitt von Körpern wieder ein Körper ist (Beweis analog zu dem für Ringe).
Wenn $S = \{s_1, \ldots, s_n\}$, dann schreibt man $K[s_1, \ldots, s_n]$ für $K[\{s_1, \ldots, s_n\}]$ und $K(s_1, \ldots, s_n)$ für $K(\{s_1, \ldots, s_n\})$.

Satz 39.6 *Seien K, F Körper, $K \leq F$, $u, u_i \in F$ $(i = 1, \ldots, n)$ und $S \subseteq F$ (für die Aussagen 1.-3. genügt es, wenn F ein kommutativer Ring mit Eins ist). Dann gilt:*

1. $K[u] = \{a_0 + a_1 u + \ldots + a_n u^n \mid n \in \mathbb{N}_0, a_i \in K\} = \{f(u) \mid f \in K[x]\}$
2. $K[u_1, \ldots, u_n] = \{\sum_{(k_1,\ldots,k_n) \in \mathbb{N}_0^n} a_{(k_1,\ldots,k_n)} u_1^{k_1} \ldots u_n^{k_n} \mid a_{(k_1,\ldots,k_n)} \in K,$ *nur endlich viele* $a_{(k_1,\ldots,k_n)}$ *sind* $\neq 0\}$, *d.h.*

$$K[u_1, \ldots, u_n] = \{f(u_1, \ldots, u_n) \mid f \in K[x_1, \ldots, x_n]\}$$

3. $K[S] = \{f(s_1, \ldots, s_n) \mid n \in \mathbb{N},\ f \in K[x_1, \ldots, x_n],\ s_1, \ldots, s_n \in S\}$
4. $K(u) = \{f(u)g(u)^{-1} \mid f, g \in K[x],\ g(u) \neq 0\}$
5. $K(u_1, \ldots, u_n) = \{f(u_1, \ldots, u_n)g(u_1, \ldots, u_n)^{-1} \mid f, g \in K[x_1, \ldots, x_n],$ $g(u_1, \ldots, u_n) \neq 0\}$

6. $K(S) = \{f(s_1, \ldots, s_n)g(s_1, \ldots, s_n)^{-1} \mid n \in \mathbb{N},\ f, g \in K[x_1, \ldots, x_n],$
$s_1, \ldots, s_n \in S,\ g(s_1, \ldots, s_n) \neq 0\}$

Beweis: Wir beweisen nur 6., denn 3. funktioniert analog, und alle anderen Aussagen sind Spezialfälle von 3. oder 6.
Sei E die Menge auf der rechten Seite. Dann gilt jedenfalls offensichtlich $K \cup S \subseteq E$. Jeder Unterkörper von F, der $K \cup S$ enthält, muss E enthalten, da die Elemente von E nur durch Summen, Produkte und Inversenbildung aus Elementen von $K \cup S$ gebildet werden. Also ist $E \subseteq K(S)$. Es muss nur noch gezeigt werden, dass E tatsächlich ein Körper ist:
$E \neq \emptyset$ und $E \setminus \{0\} \neq \emptyset$, weil $K \subseteq E$.
Seien $a, b \in E$, wobei $a = \frac{f(s_1,\ldots,s_n)}{g(s_1,\ldots,s_n)}$ und $b = \frac{h(t_1,\ldots,t_m)}{k(t_1,\ldots,t_m)}$ sei. Fasst man f, g, h, k als Polynome in $[x_1, \ldots, x_n, y_1, \ldots, y_m]$ auf, ergibt sich hiermit:

$$a - b = \frac{f(s_1, \ldots, t_m)}{g(s_1, \ldots, t_m)} - \frac{h(s_1, \ldots, t_m)}{k(s_1, \ldots, t_m)} = \frac{(fk - hg)(s_1, \ldots, t_m)}{(gk)(s_1, \ldots, t_m)}$$

und $(gk)(s_1, \ldots, t_m) = g(s_1, \ldots, s_n)k(t_1, \ldots, t_m) \neq 0$, also $a - b \in E$.
Wenn $b \neq 0$ ist, dann gilt außerdem:

$$ab^{-1} = \frac{f(s_1, \ldots, t_m)}{g(s_1, \ldots, t_m)} \cdot \frac{k(s_1, \ldots, t_m)}{h(s_1, \ldots, t_m)} = \frac{(fk)(s_1, \ldots, t_m)}{(gh)(s_1, \ldots, t_m)}$$

und $(gh)(s_1, \ldots, t_m) = g(s_1, \ldots, s_n)h(t_1, \ldots, t_m) \neq 0$, also $ab^{-1} \in E$.
Damit ist E ein Unterkörper von F, der $K \cup S$ enthält.

□

Bemerkung: $K[s_1, \ldots, s_n] = K[s_1, \ldots, s_{n-1}][s_n] = \ldots = K[s_1][s_2] \ldots [s_n]$ und $K(s_1, \ldots, s_n) = K(s_1, \ldots, s_{n-1})(s_n) = \ldots = K(s_1)(s_2) \ldots (s_n)$.

Definition 39.7 Sei $F : K$ eine Körpererweiterung und $u \in F$.
u heißt *algebraisch* über K, wenn $\exists f \in K[x],\ f \neq 0$, mit $f(u) = 0$. Andernfalls, d.h., wenn aus $f \in K[x]$ und $f(u) = 0$ bereits $f = 0$ folgt, heißt u *transzendent* über K.

Beispiel: $i \in \mathbb{C}$ ist algebraisch über $\mathbb{Q}$: es ist Nullstelle von $x^2 + 1 \in \mathbb{Q}[x]$.
$\sqrt{n} \in \mathbb{R}$ ist für $n \in \mathbb{N}$ algebraisch über $\mathbb{Q}$: es ist Nullstelle von $x^2 - n \in \mathbb{Q}[x]$.
e, π sind hingegen transzendent über $\mathbb{Q}$.

Bemerkung: Trivialerweise ist $u \in F$ algebraisch über F, da es Nullstelle von $x - u \in F[x]$ ist. Wenn $K \leq E \leq F$ ist und $u \in F$ algebraisch über K, dann ist es auch algebraisch über E. Ist $u \in F$ transzendent über E, dann ist es auch transzendent über K.

BEMERKUNG: Ist $K \leq F$ und $u \in F$ algebraisch über K, dann gibt es ein normiertes Polynom $f \in K[x]$ mit $f(u) = 0$ (ergibt sich durch Multiplikation mit dem Inversen c^{-1} des Leitkoeffizienten).

Definition 39.8 Eine Körpererweiterung $F : K$ heißt *algebraisch* , wenn jedes $u \in F$ algebraisch über K ist. Andernfalls (d.h., wenn ein $u \in F$ existiert, das transzendent über K ist) heißt die Körpererweiterung *transzendent* .

Definition 39.9 Eine Körpererweiterung $F : K$ heißt *einfach* , wenn es ein $u \in F$ mit $F = K(u)$ gibt.

Definition 39.10 (Körper der rationalen Funktionen über K) Man definiert $K(x) := \{\frac{f}{g} \mid f, g \in K[x],\ g \neq 0\}$ (der Quotientenkörper von $K[x]$). K wird in $K(x)$ via $k \mapsto \frac{k}{1}$ eingebettet; $K(x)$ wird als Körper tatsächlich von $K \cup \{x\}$ erzeugt, also ist die Schreibweise $K(x)$ gerechtfertigt.

Lemma 39.11 Sei R ein Ring, K ein Körper und $\varphi : K \to R$ ein Ringhomomorphismus. Dann ist φ injektiv oder $\varphi = 0$.

Beweis: $\operatorname{Ker}\varphi \trianglelefteq K$, K hat als Körper aber nur die Ideale $\{0\}$ und K. Für $\operatorname{Ker}\varphi = \{0\}$ ist φ injektiv, für $\operatorname{Ker}\varphi = K$ ist $\varphi = 0$.

□

Satz 39.12 (Transzendente Körpererweiterungen) *Sei $F : K$ eine Körpererweiterung, $u \in F$ transzendent über K. Dann ist $K(x) \simeq K(u)$ mittels eines Isomorphismus $\varphi : K(x) \to K(u)$ mit $\varphi(x) = u$ und $\varphi|_K = \mathrm{id}_K$.*

Beweis: Sei $\psi : K[x] \to K(u)$ der Einsetzhomomorphismus mit $\psi(x) = u$ und $\psi|_K = \mathrm{incl}_{K \hookrightarrow K(u)}$ (d.h. $\psi(f) = f(u)$ für $f \in K[x]$). Da $\psi(f) = f(u) \neq 0$ für alle $f \in K[x] \setminus \{0\}$ ist, also $\psi(f)$ für alle $f \in K[x] \setminus \{0\}$ invertierbar ist, kann ψ auf den Quotientenkörper $K(x)$ von $K[x]$ fortgesetzt werden: es gibt einen Homomorphismus $\overline{\psi} : K(x) \to K(u)$ mit $\overline{\psi}|_{K[x]} = \psi$.
Es gilt dann $\overline{\psi}|_K = \psi|_K = \mathrm{id}_K$ und $\overline{\psi}(x) = \psi(x) = u$, und wir wissen auch, wie $\overline{\psi}$ definiert ist: $\overline{\psi}(\frac{f}{g}) = \psi(f)\psi(g)^{-1} = f(u)g(u)^{-1}$
Man erhält $\operatorname{Im}\overline{\psi} = \{f(u)g(u)^{-1} \mid f, g \in K[x],\ g \neq 0\} = K(u)$ ($g \neq 0$ ist äquivalent zu $g(u) \neq 0$, weil u transzendent ist), d.h. $\overline{\psi}$ ist surjektiv. Weil zudem $\overline{\psi} \neq 0$ ist ($\overline{\psi}|_K = \mathrm{id}$, also jedenfalls $\overline{\psi} \neq 0$), muss nach dem vorigen Lemma $\overline{\psi}$ auch injektiv sein, d.h. $\overline{\psi}$ ist Isomorphismus, der zudem auch $\overline{\psi}(x) = u$ und $\overline{\psi}|_K = \mathrm{id}_K$ erfüllt.

□

Satz 39.13 (Algebraische Körpererweiterungen) *Sei $F : K$ eine Körpererweiterung, $u \in F$ algebraisch über K. Dann gilt:*

1. *Es existiert genau ein normiertes Polynom $g \in K[x]$, sodass $\forall f \in K[x]$ $(f(u) = 0 \Leftrightarrow g \mid f$ in $K[x])$, und dieses g ist irreduzibel in $K[x]$.*
2. *$K(u) = K[u] \simeq K[x]/(g)$; $\overline{\varphi} : K[x]/(g) \to K[u]$ mit $\overline{\varphi}(f + (g)) = f(u)$ ist ein Isomorphismus.*
3. *Sei $n = \deg g$, dann ist $\{1, u, u^2, \ldots, u^{n-1}\}$ eine K-Basis von $K(u)$, also $[K(u) : K] = n = \deg g$.*

Beweis:

1. Sei $\varphi : K[x] \to F$ der Einsetzhomomorphismus mit $\varphi(x) = u$, $\varphi \mid_K = \mathrm{incl}_{K \hookrightarrow F}$, d.h. $\varphi(f) = f(u)$. Dann ist $\mathrm{Im}\,\varphi = K[u]$, $\mathrm{Ker}\,\varphi = \{f \in K[x] \mid f(u) = 0\} \neq \{0\}$, weil u algebraisch über K ist.
   Es existiert daher ein $g \neq 0$, sodass $\mathrm{Ker}\,\varphi = (g) = gK[x]$ ist (weil $K[x]$ als Euklidischer Bereich auch Hauptidealbereich ist). Man kann g normiert wählen, dann ist es eindeutig bestimmt (es gilt $(g) = (h) \Leftrightarrow g \approx h$, und es existiert genau eine Einheit u, sodass ug normiert ist).
   Also gibt es genau ein normiertes Polynom g, sodass $f \in \mathrm{Ker}\,\varphi \Leftrightarrow f \in gK[x]$ (d.h. $f(u) = 0 \Leftrightarrow g \mid f$ in $K[x]$)

2. Wir haben zu zeigen, dass $K[u]$ ein Körper ist:
   Nach dem 1.Isomorphiesatz gilt $K[u] = \mathrm{Im}\,\varphi \simeq K[x]/(\mathrm{Ker}\,\varphi) = K[x]/(g)$ mit dem angegebenen Isomorphismus. Weil $K[u] \subseteq F$ ein Integritätsbereich ist, ist (g) ein Primideal von $K[x]$. Da $(g) \neq \{0\}$ ist, muss g prim und daher auch irreduzibel sein. Somit ist (g) maximal unter den Hauptidealen $\neq K[x]$, und weil $K[x]$ ein Hauptidealbereich ist, muss damit (g) ein maximales Ideal sein. Daher ist $K[x]/(g) \simeq K[u]$ ein Körper, und es folgt $K(u) = K[u]$.

3. $K(u) = K[u] = \{f(u) \mid f \in K[x]\}$, also hat jedes Element von $K(u)$ die Form $f(u)$ für ein $f \in K[x]$.
   Sei $f \in K[x]$ beliebig gewählt. Dann lässt es sich als $f(x) = q(x)g(x) + r(x)$ mit $r = 0$ oder $\deg r < \deg g = n$ schreiben. Wendet man den Einsetzhomomorphismus an, ergibt sich $f(u) = q(u)g(u) + r(u) = r(u)$, also hat jedes $a \in K(u)$ die Form $a = r(u)$ mit einem $r = a_0 + \ldots + a_{n-1}x^{n-1}$. Damit ist $a = a_0 + \ldots + a_{n-1}u^{n-1}$, also erzeugt $\{1, \ldots, u^{n-1}\}$ $K(u)$ als Vektorraum über K.

Wenn andererseits $a_0 + \ldots + a_{n-1}u^{n-1} = 0$ ist, dann folgt $g \mid r = a_0 + \ldots + a_{n-1}x^{n-1}$, und weil $\deg r = n - 1 < \deg g$ ist, muss $r = 0$, also $a_i = 0\ \forall i$ sein. Also ist $\{1, \ldots, u^{n-1}\}$ linear unabhängig über K.

□

Definition 39.14 Sei $F : K$ eine Körpererweiterung, $u \in F$ algebraisch über K. Jenes eindeutig bestimmte normierte Polynom $g \in K[x]$, für das $\forall f \in K[x]\ f(u) = 0 \Leftrightarrow g \mid f$ in $K[x]$ gilt, heißt das *Minimalpolynom* von u über K; $n = \deg g$ heißt der *Grad* von u über K ($\deg g = [K(u) : K]$ nach dem vorigen Satz). Man sagt, u ist algebraisch vom Grad n über K.

BEMERKUNG: $u \in K \Leftrightarrow x - u$ ist Minimalpolynom von u über K.

Lemma 39.15 Sei $F : K$ eine Körpererweiterung, $u \in F$ algebraisch über K, $g \in K[x]$. g ist genau dann Minimalpolynom von u, wenn $g(u) = 0$ ist und g sowohl normiert als auch irreduzibel ist.

Beweis: Wenn g Minimalpolynom ist, erfüllt es jedenfalls alle diese Eigenschaften.
Umgekehrt mögen alle diese Eigenschaften für ein Polynom g gelten. Sei h das Minimalpolynom. Dann gilt $g(x) = h(x)k(x)$ für ein Polynom $k \in K[x]$. Weil g irreduzibel ist, muss k eine Einheit sein (h ist keine Einheit, weil $h(u) = 0$). Es folgt $g \approx h$, also existiert eine Einheit u mit $ug = h$. Weil g, h beide normiert sind, folgt $g = h$.

□

Definition 39.16 Eine Körpererweiterung $F : K$ heißt *endlich-dimensional* , wenn $[F : K] = \dim_K F = n \in \mathbb{N}$ endlich ist.
Eine Körpererweiterung $F : K$ heißt *endlich-erzeugt* , wenn es $u_1, \ldots, u_n \in F$ gibt, sodass $F = K(u_1, \ldots, u_n)$.

BEMERKUNG: Trivialerweise gilt die Inklusion „endlich-dimensional ⇒ endlich-erzeugt“, denn eine Basis erzeugt F als K-Vektorraum, also erst recht als Körper.

Lemma 39.17 Ist eine Körpererweiterung $F : K$ endlich-dimensional, dann ist sie endlich-erzeugt und algebraisch.

Beweis: Dass $F : K$ endlich-erzeugt ist, wurde bereits festgehalten. Sei nun $b_1, \ldots, b_n$ eine K-Basis von F. Dann hat jedes $a \in F$ die Form $a_1b_1 + \ldots + a_nb_n$ für gewisse $a_i \in K$.
Sei $u \in F$. Wir zeigen, dass u algebraisch von einem Grad $\leq n$ ist: $K(u)$ ist ein

K-Vektorraum und ein Teilraum von F, daher gilt $\dim_K K(u) \leq \dim_K F = n$. Somit sind $1, u, \ldots, u^n$ K-linear abhängig. Es gibt also $a_0, \ldots, a_n \in K$, die nicht alle gleich 0 sind, mit $0 = a_0 + a_1 u + \ldots + a_n u^n$, d.h. u ist Nullstelle von $f(x) = a_0 + a_1 x + \ldots + a_n x^n \in K[x]$, und $f \neq 0$.

□

Lemma 39.18 Sei $F : K$ eine Körpererweiterung, wobei $F = K(s_1, \ldots, s_n)$, und alle s_i algebraisch über K sind. Dann ist $F : K$ endlich-dimensional.

Beweis: s_i ist algebraisch über K, also auch über $K(s_1, \ldots, s_{i-1})$. Deswegen gilt $K(s_1, \ldots, s_i) = K(s_1, \ldots, s_{i-1})(s_i) = K(s_1, \ldots, s_{i-1})[s_i]$, und $[K(s_1, \ldots, s_{i-1})[s_i] : K(s_1, \ldots, s_{i-1})] =: m_i$ ist endlich. Es folgt:

$$\begin{aligned} [F : K] &= [K(s_1, \ldots, s_n) : K] \\ &= [K(s_1, \ldots, s_n) : K(s_1, \ldots, s_{n-1})] \ldots [K(s_1) : K] \\ &= m_n \ldots m_1 \end{aligned}$$

Damit ist $[F : K]$ endlich.

□

Proposition 39.19 Eine Körpererweiterung $F : K$ ist genau dann endlich-dimensional, wenn $F : K$ endlich-erzeugt und algebraisch ist.

Beweis: Folgerung aus den vorigen Lemmata.

Lemma 39.20 Sei $F : K$ eine Körpererweiterung, $F = K(S)$, und alle $s \in S$ algebraisch über K. Dann ist $F : K$ algebraisch.

Beweis: Sei $u \in F$, dann existieren $s_1, \ldots, s_n \in S$, sodass $u \in K(s_1, \ldots, s_n)$ (weil $u = f(s_1, \ldots, s_n) g(s_1, \ldots, s_n)^{-1}$ für gewisse $f, g \in K[x]$, $s_1, \ldots, s_n \in S$ ist). Weil $K(s_1, \ldots, s_n)$ endlich-dimensional ist, muss damit u algebraisch sein.

□

Lemma 39.21 Seien K, E, F Körper mit $K \leq E \leq F$. Ist $F : E$ algebraisch und $E : K$ algebraisch, dann auch $F : K$.

Beweis: Wir zeigen, dass für alle $u \in F$ ein Körper $\tilde{F}$ mit $u \in \tilde{F}$ existiert, für den $[\tilde{F} : K]$ endlich ist. Damit wäre dann u algebraisch über K:
u ist algebraisch über E, daher existieren $e_0, \ldots, e_n \in E$ (nicht alle $= 0$) mit $0 = e_0 + e_1 u + \ldots + e_n u^n$. Damit ist u algebraisch über $K(e_0, \ldots, e_n)$. Weil

jedes e_i algebraisch über K ist, ist nach Lemma 39.18 $[K(e_0, \ldots, e_n) : K]$ endlich. Damit ist jedoch $u \in K(e_0, \ldots, e_n, u)$, und

$$[K(e_0, \ldots, e_n, u) : K] = [K(e_0, \ldots, e_n, u) : K(e_0, \ldots, e_n)][K(e_0, \ldots, e_n) : K]$$

ist endlich, weil u algebraisch über $K(e_0, \ldots, e_n)$ und daher $[K(e_0, \ldots, e_n, u) : K(e_0, \ldots, e_n)]$ endlich ist.
Also ist jedes $u \in F$ auch algebraisch über K.

□

Satz 39.22 (Adjunktion einer Nullstelle) *Sei K ein Körper, $f \in K[x]$ und $\deg f \geq 1$. Dann gilt:*

1. *Es existiert eine Körpererweiterung $F : K$ mit $F = K(u)$, sodass $f(u) = 0$ und $[K(u) : K] \leq \deg f$.*
2. *Wenn f irreduzibel über K ist und $K(u)$,$K(v)$ einfache Erweiterungen von K mit $f(u) = 0$ und $f(v) = 0$ sind, dann existiert ein Körperisomorphismus $\varphi : K(u) \to K(v)$ mit $\varphi(u) = v$ und $\varphi(k) = k$ für alle $k \in K$. Zudem gilt $[K(u) : K] = \deg f$.*

Beweis: Wir zeigen die Aussage für ein irreduzibles f (ansonsten kann man einen irreduziblen Faktor von f wählen und auf diesen den Rest des Beweises anwenden):
Weil f irreduzibel ist, ist (f) ein maximales Ideal in $K[x]$, daher ist $K[x]/(f)$ ein Körper. Sei $\pi : K[x] \to K[x]/(f)$ die kanonische Projektion. Dann ist $\pi|_K : K \to K[x]/(f)$ injektiv, da $\operatorname{Ker} \pi|_K = K \cap (f) = \{0\}$ ist.
Also ist K via $k \mapsto k + (f)$ eingebettet in $K[x]/(f) =: F$, d.h. $F : K$ ist eine Körpererweiterung. Sei ferner $u := x + (f) \in F$. Dann gilt:

$$f(u) = f(x) + (f) = f + (f) = (f) = 0 + (f) = 0_F$$

Also $f(u) = 0$. F wird von $u = x + (f) = \pi(x)$ erzeugt, da $K[x]$ von x erzeugt wird.
Weil f irreduzibel ist, ist f bis auf eine multiplikative Konstante Minimalpolynom von u über K, es gilt also $[K(u) : K] = \deg f$. Nach der Charakterisierung einfacher algebraischer Körpererweiterungen (Satz 39.13) muss zudem $K(u) \simeq K[x]/(f) \simeq K(v)$ sein, wobei für den Isomorphismus $\varphi : K(u) \to K(v)$, der sich ergibt, offensichtlich $\varphi(u) = v$ und $\varphi(k) = k$ für alle $k \in K$ sein muss.

□

Lemma 39.23 Seien K, L Körper und $\varphi : K \to L$ ein Isomorphismus. Dann sind auch $\overline{\varphi} : K[x] \to L[x]$, definiert durch $\overline{\varphi}(a_0 + a_1 x + \ldots + a_n x^n) = \varphi(a_0) + \varphi(a_1)x + \ldots + \varphi(a_n)x^n$, und $\tilde{\varphi} : K(x) \to L(x)$, definiert durch $\tilde{\varphi}(\frac{f}{g}) = \frac{\overline{\varphi}(f)}{\overline{\varphi}(g)}$, Isomorphismen.

Beweis: $\overline{\varphi}$ ist als Einsetzhomomorphismus mit $\overline{\varphi}|_K = \varphi$, $\overline{\varphi}(x) = x$, ein Ringhomomorphismus. $\overline{\varphi}$ ist surjektiv, weil φ surjektiv ist, und $\operatorname{Ker} \overline{\varphi} = \{0\}$, da $\operatorname{Ker} \varphi = \{0\}$.
Sei weiters $\psi = \mathrm{incl}_{L[x] \hookrightarrow L(x)} \circ \varphi$. Dann ist ψ injektiv, weil φ und incl injektiv sind. ψ ist fortsetzbar auf $K(x)$, die Fortsetzung $\tilde{\varphi} : K(x) \to L(x)$ ist auch injektiv, und es gilt $\tilde{\varphi}(\frac{f}{g}) = \frac{\overline{\varphi}(f)}{\overline{\varphi}(g)}$. Weil $\overline{\varphi}$ surjektiv ist, trifft dies überdies auch auf $\tilde{\varphi}$ zu.

□

Bemerkung: Wir bezeichnen $\overline{\varphi}$ und $\tilde{\varphi}$ im Folgenden nur noch mit φ.

Satz 39.24 *Seien $F : K$ und $E : L$ Körpererweiterungen, $u \in F$, $v \in E$, und $\varphi : K \to L$ ein Körperisomorphismus.*

1. *Wenn u transzendent über K und v transzendent über L ist, dann gibt es einen Isomorphismus $\overline{\varphi} : K(u) \to L(v)$ mit $\overline{\varphi}(u) = v$ und $\overline{\varphi}|_K = \varphi$.*

2. *Wenn es ein irreduzibles Polynom f gibt, sodass $f(u) = 0$, $\varphi(f)(v) = 0$, dann gibt es ebenso einen Isomorphismus $\overline{\varphi} : K(u) \to L(v)$ mit $\overline{\varphi}(u) = v$ und $\overline{\varphi}|_K = \varphi$.*

Beweis:

1. Weil u transzendent über K ist, gibt es einen Isomorphismus $\sigma : K(x) \to K(u)$ mit $\sigma|_K = \mathrm{id}$ und $\sigma(x) = u$. Ebenso gibt es einen Isomorphismus $\rho : L(x) \to L(v)$ mit $\rho|_L = \mathrm{id}$ und $\rho(x) = v$.
   Damit erfüllt jedoch der Isomorphismus $\overline{\varphi} := \rho \circ \varphi \circ \sigma^{-1} : K(u) \to L(v)$ die Bedingungen:

   $$\overline{\varphi}(u) = \rho(\varphi(\sigma^{-1}(u))) = \rho(\varphi(x)) = \rho(x) = v$$

   und $\overline{\varphi}(k) = \rho(\varphi(k)) = \varphi(k)$ für alle $k \in K$, also $\overline{\varphi}|_K = \varphi$.

2. Weil f irreduzibel über K ist, ist auch $\varphi(f)$ irreduzibel über L. O.B.d.A. darf angenommen werden, dass f normiert ist (ansonsten ist cf für eine Einheit c normiert und weiterhin irreduzibel). Dann ist auch $\varphi(f)$ normiert, weil $\varphi(1) = 1$.
   Wir wissen bereits, dass $\sigma : K[x]/(f) \to K[u] = K(u)$ mit $\sigma(h + (f)) =$

$h(u)$ ein Isomorphismus ist. Ebenso ist $\rho : L[x]/(\varphi(f)) \to L[v] = L(v)$ mit $\sigma(h + (\varphi(f))) = h(v)$ ein Isomorphismus.
Nach dem Korrespondenzsatz gibt es zudem einen Isomorphismus $\psi : K[x]/(f) \to L[x]/(\varphi(f))$, definiert durch $\psi(h + (f)) = \varphi(h) + (\varphi(f))$. Wie in 1. erfüllt dann $\overline{\varphi} := \rho \circ \psi \circ \sigma^{-1} : K(u) \to L(v)$ die Bedingungen.

□

Korollar 39.25 Seien E, F Erweiterungskörper von K und $u \in E$, $v \in F$ algebraisch über K. Dann gibt es genau dann ein irreduzibles Polynom f mit $f(u) = 0$ und $f(v) = 0$, wenn es einen Isomorphismus $\overline{\varphi} : K(u) \to K(v)$ mit $\overline{\varphi}(u) = v$ und $\overline{\varphi}|_K = \mathrm{id}$ gibt.

Beweis: Wenn es ein solches Polynom gibt, folgt die Existenz von $\overline{\varphi}$ aus dem vorigen Satz mit $\varphi = \mathrm{id}_K$.
Wenn umgekehrt ein solcher Isomorphismus existiert, dann kann $f = a_0 + \ldots + a_n x^n$ als das Minimalpolynom von u gewählt werden. Es gilt dann

$$f(v) = a_0 + \ldots + a_n v^n = \overline{\varphi}(a_0 + \ldots + a_n u^n) = \overline{\varphi}(f(u)) = \overline{\varphi}(0) = 0$$

□

Proposition 39.26 Sei $K : F$ eine Körpererweiterung. Dann ist $E := \{u \in F \mid u \text{ ist algebraisch über } K\}$ ein Körper.

Beweis: $K(E)$ ist ein Körper, und er wird über K von algebraischen Elementen erzeugt. Also ist $K(E) : K$ algebraisch und folglich $K(E) \subseteq E$. Somit ist $E = K(E)$ ein Körper.

□

Beispiel: $\mathbb{A} = \{z \in \mathbb{C} \mid z \text{ ist algebraisch über } \mathbb{Q}\}$ ist ein nicht endlichdimensionaler algebraischer Erweiterungskörper.

Zerfällungskörper eines Polynoms:

Definition 39.27 Sei $f \in K[x]$, $\deg f \geq 1$, und $F : K$ eine Körpererweiterung. f *zerfällt* über F (in Linearfaktoren), wenn in $F[x]$ gilt: $f(x) = a(x - b_1) \cdot \ldots \cdot (x - b_n)$ $(a, b_i \in F)$.

Definition 39.28 Ein Körper K mit der Eigenschaft, dass jedes $f \in K[x]$ mit $\deg f \geq 1$ in $K[x]$ zerfällt, heißt *algebraisch abgeschlossen* .

BEISPIEL: $\mathbb{C}$ ist algebraisch abgeschlossen (Fundamentalsatz der Algebra).

BEMERKUNG: Die Eigenschaft, dass K algebraisch abgeschlossen ist, ist äquivalent dazu, dass jedes nicht konstante Polynom in $K[x]$ eine Nullstelle in K hat.

Definition 39.29 Sei K ein Körper, $f \in K[x]$ mit $\deg f \geq 1$. Ein Erweiterungskörper F von K heißt *Zerfällungskörper* von f über K, wenn

- f zerfällt über F.
- $F = K(u_1, \ldots, u_n)$, wobei $u_1, \ldots, u_n$ die Nullstellen von f sind.

Satz 39.30 *Sei K ein Körper, $f \in K[x]$, $\deg f = n \geq 1$. Dann existiert ein Zerfällungskörper F von f über K mit $[F : K] \leq n!$.*

Beweis: Durch Induktion nach n:

- $n = 1$: $f(x) = ax + b$, $a, b \in K$, $a \neq 0$. Dann zerfällt $f = a(x + \frac{b}{a})$ bereits über K, also ist K Zerfällungskörper, und es gilt $K = K(-\frac{b}{a})$ und $[K : K] = 1$.
- $n > 1$: Sei $E : K$ eine Erweiterung mit $[E : K] \leq n$, $E = K(u)$ und $f(u) = 0$ (die Existenz einer solchen Erweiterung wurde bereits gezeigt). In $E[x]$ gilt dann $f(u) = 0 \Rightarrow x - u \,|\, f$, also existiert ein $g \in E[x]$ mit $f(x) = (x - u)g(x)$, $\deg g = n - 1$.
  Nach Induktionsvoraussetzung gibt es einen Zerfällungskörper F von g über E, und $[F : E] \leq (n-1)!$. Es folgt klarerweise $[F : K] = [F : E][E : K] \leq (n-1)!n = n!$, und f zerfällt über F. Außerdem gilt $F = E(v_1, \ldots, v_m)$, wobei $v_1, \ldots, v_m$ die Nullstellen von g (und damit auch von f) sind. Weil zudem $E = K(u)$ ist, gilt $F = K(u, v_1, \ldots, v_m)$, d.h. F wird von den Nullstellen von f erzeugt.

□

Lemma 39.31 Sei $F : K$ eine Körpererweiterung, $f, f_1 \in K[x]$ und $f_1 \,|\, f$ in $K[x]$. Wenn f über F zerfällt, dann auch f_1, und jede Wurzel von f_1 ist Wurzel von f.

Beweis: In $F[x]$ gilt: $f(x) = a(x - b_1) \ldots (x - b_n) = f_1(x)g(x)$, $f_1, g \in K[x]$, $a, b_i \in F$. Weil $F[x]$ ein ZPE-Ring ist, sind die $(x - b_i)$ die eindeutig bestimmten irreduziblen Faktoren von f, also ist $f_1 = a_1(x - b_{i_1}) \ldots (x - b_{i_m})$ mit $\{i_1, \ldots, i_m\} \subseteq \{1, \ldots, n\}$.

□

Satz 39.32 *Sei $\varphi : K \to L$ ein Körperisomorphismus und $f \in K[x]$ mit $\deg f \geq 1$. Sei F der Zerfällungskörper von f über K und E der Zerfällungskörper von $\varphi(f)$ über L. Dann gibt es einen Isomorphismus $\overline{\varphi} : F \to E$ mit $\overline{\varphi}|_K = \varphi$.*

Beweis: Durch Induktion nach $[F : K]$:

- $[F : K] = 1$ heißt $F = K$, d.h. $f(x) = a(x-b_1)\dots(x-b_n)$ mit $a, b_i \in K$. Dann zerfällt $\varphi(f) = \varphi(a)(x - \varphi(b_1))\dots(x - \varphi(b_n))$ auch über L, d.h. $E = L$. Damit erfüllt $\overline{\varphi} = \varphi$ die Bedingung.

- Sei nun $[F : K] > 1$, d.h. f zerfällt nicht über K; In $F[x]$ gilt $f(x) = a(x - b_1)\dots(x - b_n)$ mit $a, b_i \in F$, und es gibt ein i mit $b_i \notin K$. Sei $b = b_i$ mit $b_i \notin K$ ein solches Element und f_1 das Minimalpolynom von b über K. Dann gilt $f_1 \mid f$ in $K[x]$. Da f über F zerfällt, zerfällt f_1 auch über F, und zudem gilt $\deg f_1 = [K(b) : K] > 1$ (weil $b \notin K$).
  Weil φ ein Isomorphismus ist, gilt auch $\varphi(f_1) \mid \varphi(f)$ in $L[x]$. Weil $\varphi(f)$ über E zerfällt, trifft dies damit auch auf $\varphi(f_1)$ zu. Daher existiert eine Wurzel $c \in E$ von $\varphi(f_1)$.
  Damit ist f_1 ein irreduzibles Polynom, $f_1(b) = 0$, $\varphi(f_1)(c) = 0$. Es wurde bereits gezeigt, dass man in diesem Fall φ auf einfache Erweiterungen fortsetzen kann (Satz 39.24), d.h. es gibt einen Isomorphismus $\tilde{\varphi} : K(b) \to L(c)$ mit $\tilde{\varphi}|_K = \varphi$ und $\tilde{\varphi}(b) = c$.
  Man kann nun die Induktionsvoraussetzung auf $F : K(b)$ anwenden (F ist Zerfällungskörper von f über $K(b)$, E ist Zerfällungskörper von $\varphi(f)$ über $K(c)$, und $[F : K(b)] < [F : K]$, da $[K(b) : K] > 1$), d.h. es exisitiert ein Isomorphismus $\overline{\varphi} : F \to E$, für den $\overline{\varphi}|_{K(b)} = \tilde{\varphi}$ (und daher $\overline{\varphi}|_K = \varphi$) ist.

□

Definition 39.33 Sei K ein Körper, $M \subseteq K[x]$ eine Menge von Polynomen mit Grad ≥ 1. Ein Erweiterungskörper F von K heißt Zerfällungskörper von M über K, wenn

- Jedes $f \in M$ zerfällt über F.

- $F = K(S)$, wobei S die Menge alle Nullstellen von Polynomen in M ist.

Bemerkung: Für endliches M ergibt sich nichts Neues: der Zerfällungskörper von $f_1, \dots, f_n$ ist der Zerfällungskörper von $f_1 \cdot \ldots \cdot f_n$.

Definition 39.34 F heißt *algebraischer Abschluss* von K, wenn $F : K$ algebraische Erweiterung und F algebraisch abgeschlossen ist.

Proposition 39.35 Sei K ein Körper und $F : K$ eine Körpererweiterung. Dann ist F genau dann algebraischer Abschluss von K, wenn F Zerfällungskörper der Menge aller (irreduziblen) Polynome in $K[x]$ mit Grad ≥ 1 über K ist.

Satz 39.36 *Jeder Körper hat einen algebraischen Abschluss; je zwei algebraische Abschlüsse sind K-isomorph (über einen Isomorphismus, der eingeschränkt auf K die Identität ist).*

Kapitel 40

Endliche Körper

Lemma 40.1 Sei K ein endlicher Körper. Dann gibt es eine Primzahl p mit $\chi(K) = p$, und Π_K (der von 1_K erzeugte Unterring) ist isomorph zu $\mathbb{Z}_p = \mathbb{Z}/(p\mathbb{Z})$.

Beweis: Weil K Körper ist, ist K insbesondere nullteilerfreier Ring. Damit ist nach Proposition 20.4 $\chi(K)$ Primzahl oder 0. Wenn $\chi(K) = 0$, dann gilt nach Satz 20.6, dass $\Pi_K \simeq \mathbb{Z} \leq K$, was nicht möglich ist, weil K als endlich vorausgesetzt wurde. Andernfalls ist $\chi(K) = p$ eine Primzahl und $\Pi_K \simeq \mathbb{Z}_p$.

□

Lemma 40.2 Seien F, K endliche Körper mit $K \subseteq F$. Dann ist $|F| = |K|^{[F:K]}$.

Beweis: F ist ein K-Vektorraum der Dimension $[F : K] = n$. Für eine Basis $b_1, \ldots, b_n$ ist damit eine Bijektion $\varphi : F \to K^n$ durch $\varphi(a) = (a_1, \ldots, a_n)$ mit $a = \sum_{i=1}^{n} a_i b_i$ gegeben. Es folgt unmitttelbar $|F| = |K|^{[F:K]}$.

□

Korollar 40.3 Ist K ein endlicher Körper, dann gibt es eine Primzahl p und ein $n \in \mathbb{N}$, sodass $\chi(K) = p$, $|K| = p^n$.

Beweis: Dass $\chi(K) = p$ eine Primzahl ist, wurde bereits gezeigt. Weil $\mathbb{Z}_p \simeq \Pi_K$ ein Körper $\leq K$ ist, gilt damit $|K| = p^n$ mit $n = [K : \mathbb{Z}_p]$.

□

Lemma 40.4 Sei K ein endlicher Körper mit $|K| = q$. Dann gilt $\forall a \in K\ a^q = a$ (d.h. jedes $a \in K$ ist Nullstelle des Polynoms $x^q - x$).

Beweis: $0^q = 0$ gilt offensichtlich. Die Elemente $a \neq 0$ bilden eine Gruppe K^* bezüglich $\cdot$ mit $|K^*| = q - 1$, also gilt $a^{q-1} = 1_K$ für alle $a \neq 0$ und damit $a^q = a$.

□

Lemma 40.5 Sei R ein kommutativer Ring mit 1 und $\chi(R) = p$ prim. Dann ist $\varphi : R \to R$, $\varphi(x) = x^p$ ein Ring-Homomorphismus (Frobenius-Homomorphismus). Ist R ein Körper, dann ist φ injektiv. Ist R ein endlicher Körper, dann ist φ ein Automorphismus.

Beweis: als Übung.

Lemma 40.6 Sei F ein Körper und $\psi : F \to F$ ein Automorphismus. Dann ist $\operatorname{Fix}\psi := \{a \in F \mid \psi(a) = a\}$ ein Körper.

Beweis: als Übung.

Satz 40.7 *Sei K ein Körper mit $|K| = q$ und $n \in \mathbb{N}$. Dann gibt es einen Körper F mit $K \subseteq F$ und $|F| = q^n$.*

Beweis: Sei F der Zerfällungskörper von $f(x) = x^{q^n} - x$ über K und $U = \{a \in F \mid a^{q^n} - a = 0\}$. Dann ist U die Menge der Nullstellen von f in F, also $U = \operatorname{Fix}\psi$, wobei $\psi : F \to F$ mit $\psi(x) = x^{q^n}$ ein Körperautomorphismus ist ($q = p^m$, wobei $p = \chi(K) = \chi(F)$, also ist $\psi = \varphi^{mn}$, wobei $\varphi : x \mapsto x^p$ der Frobeniushomomorphismus ist.
Also ist U ein Körper, der nur aus den Nullstellen von f besteht. Ausserdem ist K in U enthalten, da für alle $a \in K$ gilt $a^q = a$ und damit auch $a^{q^n} = a$. Damit ist $U = F$.
Weil $f' = (x^{q^n} - x)' = -1$ über K ist, hat f keine mehrfachen Nullstellen in F, also ist $|U| = \deg(x^{q^n} - x) = q^n$, d.h. $U = F$ erfüllt die Bedingung.

□

Korollar 40.8 Ist p eine Primzahl und $n \in \mathbb{N}$, dann gibt es einen Körper K mit $K = p^n$.

Beweis: durch Anwendung des Satzes auf $\mathbb{Z}_p$.

Satz 40.9 *Seien K, F endliche Körper mit $K \subseteq F$ und $|F| = q = p^n$. Dann ist F Zerfällungskörper von $x^q - x$ über K.*

Beweis: Für alle $a \in F$ gilt $a^q = a$, also ist jedes Element von F Nullstelle von $x^q - x$. Weil F somit q verschiedene Nullstellen von $x^q - x$ enthält, zerfällt $x^q - x$ über F ($x^q - x = \prod_{\alpha \in F}(x - \alpha)$ in $F[x]$). F besteht zudem nur aus

allen Nullstellen von $x^q - x$, also wird F von diesen auch erzeugt. Somit ist F Zerfällungskörper von $x^q - x$.

□

Korollar 40.10 Je zwei Körper der Ordnung p^n sind isomorph.

Beweis: Zwei solche Körper K, L müssten beide $\mathbb{Z}_p$ enthalten, weil ihre Charakteristik p ist. Damit sind beide Zerfällungskörper von $x^{p^n} - x$, und der Isomorphismus $\mathrm{id} : \mathbb{Z}_p \to \mathbb{Z}_p$ lässt sich auf $K \to L$ fortsetzen.

□

Lemma 40.11 Sei G eine endliche Abelsche Gruppe, sodass für jeden Teiler d von $|G|$ höchstens d Elemente $g \in G$ mit $g^d = e$ existieren. Dann ist G zyklisch.

Beweis: Durch Induktion nach $n = |G|$:

- $n = 1$: G ist trivialerweise zyklisch.
- $n > 1$: Sei $\psi(m) = |\{g \in G \,|\, |g| = m\}|$. Dann ist entweder $\psi(n) = 0$ oder G zyklisch und $\psi(n) = \varphi(n)$.
  Für $m \,|\, n$, $m < n$, gilt $G[m] := \{g \in G \,|\, g^m = e\} \leq G$, und $|G[m]| \leq m < n$. Daher ist nach Induktionsvoraussetzung $G[m]$ zyklisch.
  Außerdem liegt jedes $g \in G$ mit $|g| = m$ in $G[m]$, also $\psi(m) = |\{g \in G[m] \,|\, |g| = m\}|$.
  Wenn $|G[m]| = m$, dann folgt aus der Tatsache, dass $G[m]$ zyklisch ist, $\psi(m) = |\{g \in G[m] \,|\, |g| = m\}| = \varphi(m)$.
  Wenn $|G[m]| < m$, dann gibt es kein $g \in G[m]$ mit $|g| = m$, also $\psi(m) = 0$.
  Nun gilt
  $$\sum_{d \,|\, n} \varphi(d) = n = |G| = \sum_{d \,|\, n} \psi(d)$$
  Weil $\psi(d) \leq \varphi(d)$ für alle Teiler d von n gilt, muss damit $\psi(d) = \varphi(d)$ für alle Teiler und insbesondere $\psi(n) = \varphi(n)$ gelten, d.h. G ist zyklisch.

□

Korollar 40.12 Sei K Körper und G eine endliche Gruppe mit $(G, \cdot) \leq (K^*, \cdot)$. Dann ist G zyklisch.

Beweis: In K hat das Polynom $x^d - 1$ höchstens d Nullstellen, also gibt es auch in G höchstens d Elemente $g \in G$ mit $g^d = 1$. Mit dem soeben gezeigten Satz folgt die Behauptung.

□

Korollar 40.13 Ist K ein endlicher Körper, dann ist $(K^*, \cdot)$ zyklisch. Insbesondere ist $\mathbb{Z}_p^*$ zyklisch; ein Erzeuger von $\mathbb{Z}_p^*$ heißt *Primitivwurzel* modulo p.

Korollar 40.14 Sind K, F endliche Körper mit $K \subseteq F$, dann ist $F = K(u)$ eine einfache Erweiterung.

Beweis: Wähle u als Erzeuger von $(F^*, \cdot)$. Dann ist $F = \{0\} \cup \{u^k \mid k \in \mathbb{Z}\} \subseteq K(u)$ und somit $F = K(u)$.

□

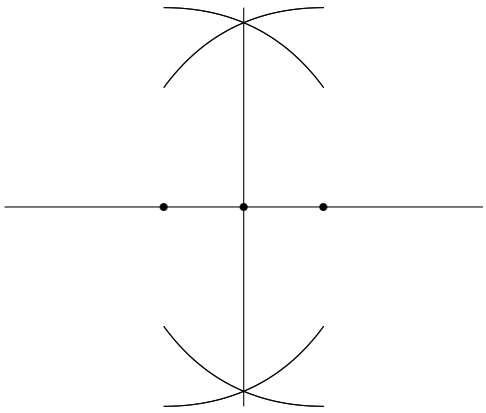
Kapitel 41

Konstruktion mit Zirkel und Lineal

Bemerkung: Wir betrachten in diesem Kapitel die Konstruktion von Zahlen mit Zirkel und Lineal. Gegeben seien dazu die Punkte $(0,0)$ und $(1,0)$ sowie ein Zirkel und ein Lineal, mit denen Konstruktionen durchzuführen sind. Man kann mit ihnen aus vorhandenen Punkten neu konstruieren:

- Schnittpunkte von Kreisen und/oder Geraden
- Geraden mit dem Lineal durch bereits vorhandene Punkte
- Kreise mit dem Zirkel, wenn der Mittelpunkt bereits vorhanden ist und der Radius die Distanz zweier bereits vorhandener Punkte ist.

Beispiel: Mittelpunkte von Strecken lassen sich konstruieren:



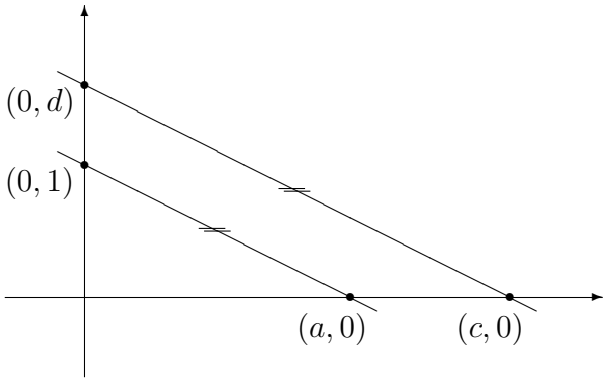
Definition 41.1 Wir nennen eine Zahl $z \in \mathbb{R}$ *konstruierbar*, wenn sie Koordinate eines konstruierbaren Punktes ist.

Proposition 41.2 Seien c, d konstruierbare Zahlen. Dann sind auch kostruierbar:

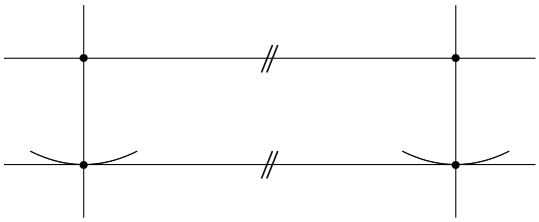
1. $c + d$ und $c - d$
2. cd und, falls $d \neq 0$, auch $\frac{c}{d}$.

Beweis:

1. trivial ($c + d$ und $c - d$ ergeben sich durch Abschlagen der Längen c, d auf einer beliebigen Geraden)
2. Die folgende Zeichnung zeigt, wie man für $d \neq 0$ mit Hilfe des Strahlensatzes $\frac{c}{d}$ konstruiert:



Man zeichnet eine Gerade durch $(0, d)$ und $(c, 0)$ und eine Parallele dazu durch $(0, 1)$. Der Schnittpunkt dieser Parallelen mit der x-Achse hat dann die Koordinaten $(a, 0)$ mit $a : 1 = c : d$, also $a = \frac{c}{d}$.
Das Parallelverschieben ist mit Zirkel und Lineal möglich:



Sind $c = d = 0$, dann ist $cd = 0$ natürlich auch konstruierbar. Ist nun o.B.d.A. $d \neq 0$, dann ist – wie soeben gezeigt – $\frac{1}{d}$ und damit auch $cd = \frac{c}{\frac{1}{d}}$ konstruierbar.

□

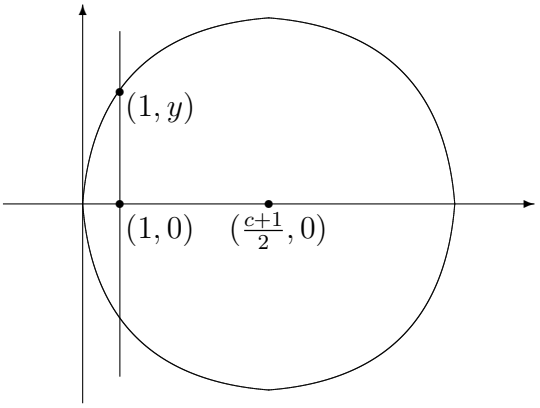
Korollar 41.3 $\mathbb{K}$, die Menge der konstruierbaren Zahlen, ist ein Körper.

Beweis: $0, 1 \in \mathbb{K}$, somit ist $\mathbb{K} \neq \emptyset$ und $\mathbb{K} \setminus \{0\} \neq \emptyset$. Weil zudem $c, d \in \mathbb{K} \Rightarrow c - d \in \mathbb{K}$ und $c, d \in \mathbb{K}^* \Rightarrow \frac{c}{d} \in \mathbb{K}^*$ gilt, ist $\mathbb{K}$ ein Körper.

□

Proposition 41.4 $c \in \mathbb{K} \Rightarrow \sqrt{c} \in \mathbb{K}$

Beweis: Man zeichne einen Kreis mit Mittelpunkt $(\frac{c+1}{2}, 0)$ und Radius $\frac{c+1}{2}$. Dann hat der Schnittpunkt der Normalen auf die x-Achse durch $(1, 0)$ mit dem Kreis die Koordinaten $(1, \sqrt{c})$:



$$\begin{aligned} y^2 &= \left(\frac{c+1}{2}\right)^2 - \left(\frac{c+1}{2} - 1\right)^2 \\ &= \frac{c^2 + 2c + 1}{4} - \frac{c^2 - 2c + 1}{4} \\ &= \frac{4c}{4} = c \end{aligned}$$

□

Korollar 41.5 Sind K, F Körper mit $K \subseteq \mathbb{K}$, $K \subseteq F \subseteq \mathbb{R}$ und $[F : K] = 2$, dann ist $F \subseteq \mathbb{K}$.

Beweis: Aus $[F : K] = 2$ folgt $F = K(u)$, wobei u algebraisch von Grad 2 über K ist. Damit ist u Nullstelle eines irreduziblen Polynoms $x^2 + px + q$ mit $p, q \in K$, $p^2 \geq 4q$. Wähle $v := u + \frac{p}{2} \in K$. Dann ist $K(u) = K(v)$, und $v^2 = (u + \frac{p}{2})^2 = u^2 + pu + \frac{p^2}{4} = \frac{p^2}{4} - q \in K$. Damit ist $K(v) \subseteq \mathbb{K}$, weil v als Quadratwurzel konstruierbar ist.

□

Korollar 41.6 Wenn $u \in \mathbb{R}$ ist, sodass es Körper $F_0, \ldots, F_n$ mit $\mathbb{Q} = F_0 \subseteq \ldots \subseteq F_n = \mathbb{Q}[u]$ und $[F_{i+1} : F_i] = 2$ gibt, dann ist u konstruierbar.

BEMERKUNG: Ist andererseits u aus K mit Zirkel und Lineal in einem Schritt konstruierbar, d.h. u entsteht als Koordinate des Schnittpunktes von Kreisen/Geraden, sodass Kreismittelpunkte in $K \times K$, Radien in K liegen und Geraden durch zwei Punkte in $K \times K$ führen, dann ist $[K(u) : K] \leq 2$ (d.h. $u \in K$ oder $[K(u) : K] = 2$).
Dies ergibt sich daraus, dass die Schnittpunkte von Kreisen und Geraden Lösungen maximal quadratischer Gleichungen sind (Beweis als Übung).

Korollar 41.7 $u \in \mathbb{R}$ ist genau dann konstruierbar, wenn es Körper $F_0, \ldots, F_n$ mit $\mathbb{Q} = F_0 \subseteq \ldots \subseteq F_n = \mathbb{Q}[u]$ und $[F_{i+1} : F_i] = 2$ gibt. Insbesondere ist der Grad des Minimalpolynoms von u über $\mathbb{Q}$ eine Zweierpotenz 2^n für ein $n \in \mathbb{N}$.

Proposition 41.8 (Delisches Problem) Es ist unmöglich, aus einem gegebenen Würfel (dem Einheitswürfel) einen Würfel mit doppelten Volumen zu konstruieren.

Beweis: Die Seitenlänge eines solchen Würfels ist $\sqrt[3]{2}$, eine Nullstelle des Polynoms $x^3 - 2$. Dieses Polynom ist irreduzibel über $\mathbb{Q}$ (da der Grad 3 ist und das Polynom keine Nullstelle in $\mathbb{Q}$ hat). Damit ist $[\mathbb{Q}(\sqrt[3]{2}) : \mathbb{Q}] = 3$, also keine Zweierpotenz. Folglich ist $\sqrt[3]{2}$ nicht konstruierbar.

□

Proposition 41.9 (Winkeldreiteilung) Es gibt keine Konstruktion mit Zirkel und Lineal, mit der aus einem gegebenen Winkel φ der Winkel $\frac{\varphi}{3}$ konstruiert werden kann.

Beweis: Wir wissen, dass der Winkel 60° konstruierbar ist (gleichseitiges Dreieck). Wäre eine Winkeldreiteilung möglich, müsste 20° und damit auch $\cos 20°$ konstruierbar sein. $\cos 20°$ ist aber algebraisch vom Grad 3:
Es gilt $\cos 3\varphi = 4\cos^3 \varphi - 3\cos \varphi$ (Beweis mit Hilfe der Additionstheoreme).
Damit folgt mit $\alpha := \cos 20°$: $\frac{1}{2} = \cos 60° = 4\alpha^3 - 3\alpha$.
Also ist α Nullstelle von $8x^3 - 6x - 1$. Dieses Polynom ist über $\mathbb{Q}$ irreduzibel, denn der Grad ist 3, und eine Nullstelle müsste die Form $\frac{c}{d}$ mit $\mathrm{ggT}(c, d) = 1$ und $c \mid -1$, $d \mid 8$ haben. Dafür kämen nur $1, -1, \frac{1}{2}, -\frac{1}{2}, \frac{1}{4}, -\frac{1}{4}, \frac{1}{8}, -\frac{1}{8}$ in Frage, doch keiner dieser Brüche ist Nullstelle.
Also ist α algebraisch vom Grad 3 und daher nicht konstruierbar.

□

Index