Institut für Algebra

Unterlagen zur Vorlesung

Algebra und Diskrete Mathematik

LVA-Nummer: 368.170

Sommersemester 2024

Erhard Aichinger

Version 5. April 2024

Adresse:

Assoz.-Prof. Dr. Erhard Aichinger
Institut für Algebra, Johannes Kepler Universität Linz
4040 Linz, Österreich
e-mail: erhard.aichinger@jku.at

Version 5.4.2024

Druck: Kopierstelle, Abteilung Service, Universität Linz

Inhaltsverzeichnis

Teil 1

Ringe

KAPITEL 1

Ringe

1. Definition und Beispiele

DEFINITION 1.1. Eine algebraische Struktur $\mathbf{R} = (R, +, -, \cdot, 0)$ ist ein *Ring*, wenn $+, \cdot$ binäre Operationen auf R sind, $-$ eine unäre Operation auf R ist, und 0 ein Element aus R ist, sodass für alle $x, y, z \in R$ die folgenden Eigenschaften erfüllt sind:

(1) $x + 0 = x$ (0 ist rechtsneutral für $+$).
(2) $x + (-x) = 0$ ($-x$ ist additiv rechtsinvers zu x).
(3) $(x + y) + z = x + (y + z)$ ($+$ ist assoziativ).
(4) $x + y = y + x$ ($+$ ist kommutativ).
(5) $(x \cdot y) \cdot z = x \cdot (y \cdot z)$ ($\cdot$ ist assoziativ).
(6) $x \cdot (y + z) = x \cdot y + x \cdot z$ (Linksdistributivgesetz).
(7) $(x + y) \cdot z = x \cdot z + y \cdot z$ (Rechtsdistributivgesetz).

SATZ 1.2. *Sei $(R, +, -, \cdot, 0)$ ein Ring, und seien $x, y \in R$. Dann gilt*

(1) $-(-(x)) = x$
(2) $x \cdot 0 = 0 \cdot x = 0$.
(3) $-(x \cdot y) = (-x) \cdot y = x \cdot (-y)$.

BEWEIS. (1): $-(-x) = -(-x) + 0 = 0 + (-(-x)) = (x + (-x)) + (-(-x)) = x + ((-x) + (-(-x)) = x + 0 = x$. (2): Es gilt $x \cdot 0 = x \cdot (0 + 0) = x \cdot 0 + x \cdot 0$, also $0 = x \cdot 0 + (-(x \cdot 0)) = (x \cdot 0 + x \cdot 0) + (-(x \cdot 0)) = x \cdot 0 + (x \cdot 0 + (-(x \cdot 0))) = x \cdot 0 + 0 = x \cdot 0$. Die Identität $0 \cdot x = 0$ beweist man genauso. (3): Es gilt $(-x) \cdot y + x \cdot y = ((-x) + x) \cdot y = (x + (-x)) \cdot y = 0 \cdot y = 0$, also $(-x) \cdot y = -(x \cdot y)$. Die Identität $x \cdot (-y) = -(x \cdot y)$ beweist man genauso. □

Beispiele für Ringe: Sei V ein Vektorraum. Dann ist $(\mathrm{Hom}(V, V), +, -, \circ, 0)$ ein Ring, der *Endomorphismenring* von V. Für einen Körper K und $n \in \mathbb{N}$ ist die Menge der Matrizen $K^{n \times n}$ ein Ring.

DEFINITION 1.3. Sei $\mathbf{R} = (R, +, -, \cdot, 0)$ ein Ring.

(1) $e \in R$ ist ein *Einselement* von $\mathbf{R}$, wenn für alle $r \in R$ gilt, dass $e \cdot r = r \cdot e = r$. Wir bezeichnen dann die Struktur $(R, +, -, \cdot, 0, 1)$ mit $1 := e$ als *Ring mit Eins*.

(2) Ein Ring mit Eins $\mathbf{R}$ ist ein *Schiefkörper*, wenn $|R| \geq 2$ gilt und es für alle $x \in R$ mit $x \neq 0$ ein $y \in R$ mit $x \cdot y = y \cdot x = 1$ gibt.
(3) $\mathbf{R}$ ist *kommutativ*, wenn für alle $r, s \in R$ gilt: $r \cdot s = s \cdot r$.
(4) Ein *Körper* ist ein kommutativer Schiefkörper.
(5) Ein kommutativer Ring mit Eins $\mathbf{R}$ ist ein *Integritätsbereich*, wenn $|R| \geq 2$ und für alle $r, s \in R$ gilt: $r \cdot s = 0 \Rightarrow (r = 0 \vee s = 0)$.

Wir werden statt $\mathbf{R}$ oft auch einfach R für die algebraische Struktur $(R, +, -, \cdot, 0, 1)$ schreiben; mit ab meinen wir $a \cdot b$.

Beispiele für kommutative Ringe mit Eins: $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$, $\mathbb{Z}[i] = \{a + b\,i \mid a, b \in \mathbb{Z}\}$, der Polynomring $\mathbb{Q}[X]$ über $\mathbb{Q}$ in einer Variablen, der Polynomring $\mathbb{Q}[X_1, \ldots, X_n]$ in n Variablen.

2. Ideale

Definition 1.4. Sei R ein Ring, und sei I eine Untergruppe von $(R, +)$. I ist ein

(1) *Linksideal* von R, wenn für alle $r \in R$ und $i \in I$ gilt, dass $ri \in I$.
(2) *Rechtsideal* von R, wenn für alle $r \in R$ und $i \in I$ gilt, dass $ir \in I$.
(3) *Ideal* von R, wenn es ein Links- und ein Rechtsideal ist.

Aus dieser Definition sieht man, dass der Durchschnitt von Idealen von R wieder ein Ideal von R ist.

Definition 1.5. Sei R ein Ring, und sei A eine Teilmenge von R. Dann ist das *von A erzeugte Ideal* $\langle A \rangle_R$ definiert durch

$$\langle A \rangle_R := \bigcap \{I \mid I \text{ Ideal von } R \text{ und } A \subseteq I\}.$$

Für kommutative Ringe mit Eins beschreiben wir nun, welche Elemente in dem von A erzeugten Ideal liegen.

Satz 1.6. *Sei R ein kommutativer Ring mit Eins, und sei $A \subseteq R$. Dann gilt*

$$\langle A \rangle_R = \{\sum_{i=1}^{n} r_i a_i \mid n \in \mathbb{N}_0, a_1, \ldots, a_n \in A, r_1, \ldots, r_n \in R\}.$$

Beweis. Sei $J := \{\sum_{i=1}^{n} r_i a_i \mid n \in \mathbb{N}_0, a_1, \ldots, a_n \in A, r_1, \ldots, r_n \in R\}$. Da $0 \in J$, und da J abgeschlossen unter $+$ und unter Multipkation mit Elementen von R ist, ist J ein Ideal von R. Außerdem gilt offensichtlich $A \subseteq J$. J ist also ein Ideal von R mit $A \subseteq J$. Aus der Definition von $\langle A \rangle_R$ als Durchschnitt aller solchen Ideale sieht man also $\langle A \rangle_R \subseteq J$.

Um die Inklusion $J \subseteq \langle A \rangle_R$ zu zeigen, wählen wir ein Element $j \in J$. Es gibt also $n \in \mathbb{N}_0$, $a_1, \ldots, a_n \in A$ und $r_1, \ldots, r_n \in R$, sodass $j = \sum_{i=1}^{n} r_i a_i$. Aus der Definition von $\langle A \rangle_R$ sehen wir, dass $A \subseteq \langle A \rangle_R$ gilt. Damit liegt jedes a_i in $\langle A \rangle_R$. Da $\langle A \rangle_R$ ein Ideal von R ist, liegt also auch jedes Summand $r_i a_i$ in $\langle A \rangle_R$, und schließlich auch die Summe j. □

Übungsaufgaben 1.7.

(1) (Ideale im Matrixring) Zeigen Sie, dass der Ring $R := \mathbb{Q}^{2\times 2}$ aller 2×2-Matrizen über $\mathbb{Q}$ nur die Ideale $\{0\}$ und R hat, und dass jedes Linksideal von der Form $\{L \in \mathbb{Q}^{2\times 2} \mid \operatorname{row}(L) \subseteq U\}$ für einen Unterraum U von $\mathbb{Q}^2$ ist. Dabei ist $\operatorname{row}(L) = \operatorname{coim}(L)$ der von den Zeilen von L erzeugte Unterraum von $\mathbb{Q}^2$.
(2) (Erzeugen von Idealen) Bestimmen Sie jeweils, ob das von der Menge S erzeugte Ideal $\langle S \rangle$ des Rings R gleich dem ganzen Ring R ist!
   (a) $R = \mathbb{Z}$, $S = \{105, 70, 42, 30\}$.
   (b) $R = \mathbb{Z} \times \mathbb{Z}$, $S = \{(4, 3), (6, 5)\}$.
   (c) $R = \mathbb{Z}_{101}$, $S = \{[75]_{101}\}$.
(3) (Erzeugen von Idealen) Bestimmen Sie jeweils, ob das von der Menge S erzeugte Ideal $\langle S \rangle$ des Rings $\mathbb{R}[X, Y]$ gleich dem ganzen Ring $\mathbb{R}[X, Y]$ ist!
   (a) $S = \{XY, X^3Y + 1\}$.
   (b) $S = \{X^2Y, XY^2 + 1\}$.
   (c) $S = \{XY + X, 1 + Y^2\}$.

Definition 1.8. Sei R ein Ring, und sei I ein Ideal von R. Dann ist I *endlich erzeugt*, wenn es eine endliche Menge $A \subseteq R$ gibt, sodass $I = \langle A \rangle_R$. Wird ein Ideal von einem einzigen Element a erzeugt, so schreiben wir $I = (a)$. Ein Ideal von solcher Form heißt *Hauptideal*.

Wir bezeichnen die Menge aller Ideale eines Rings R mit $\operatorname{Id}(R)$.

Satz 1.9. *Sei R ein Ring. Dann sind äquivalent:*

(1) *Jedes Ideal von R ist endlich erzeugt.*
(2) *Es gibt keine Folge $(I_k)_{k\in\mathbb{N}}$ von Idealen mit $I_k \subset I_{k+1}$ für alle $k \in \mathbb{N}$. (Die Menge der Ideale erfüllt die* aufsteigende Kettenbedingung (ACC)*).*
(3) *Jede nichtleere Teilmenge $\mathcal{I}$ von Idealen von R besitzt ein maximales Element M, das heißt*

$$\forall \mathcal{I} \subseteq \operatorname{Id}(R) : \Big(\mathcal{I} \neq \varnothing \Rightarrow \big(\exists M \in \mathcal{I}\ \forall N \in \mathcal{I} : M \subseteq N \Rightarrow M = N\big)\Big).$$

Beweis. (2)⇒(1): Sei I ein Ideal von R, das nicht endlich erzeugt ist. Wir konstruieren nun rekursiv eine Folge $\langle i_k \mid k \in \mathbb{N} \rangle$ von Elementen von I. Wir setzen $i_1 := 0$. Für $n \in \mathbb{N}$ definieren wir nun i_{n+1}. Da das Ideal $\langle \{i_1, \ldots, i_n\} \rangle_R$ endlich erzeugt ist, gilt $\langle \{i_1, \ldots, i_n\} \rangle_R \neq I$. Es gibt also $j \in I$ mit $j \notin \langle \{i_1, \ldots, i_n\} \rangle_R$. Sei i_{n+1} ein solches j.

Wir definieren nun für $k \in \mathbb{N}$ das Ideal I_k durch

$$I_k := \langle \{i_1, \ldots, i_k\} \rangle_R .$$

Dann ist die Folge $\langle I_k \mid k \in \mathbb{N} \rangle$ eine streng monoton wachsende Folge von Idealen von R, im Widerspruch zur (ACC). (1)⇒(2): Sei $\langle I_k \mid k \in \mathbb{N} \rangle$ eine bezüglich $\subseteq$ streng monoton wachsende Folge von Idealen von R. Dann ist $I := \bigcup \{I_k \mid k \in \mathbb{N}\}$ ebenfalls ein Ideal von R. Dieses Ideal I ist nach Voraussetzung endlich erzeugt. Seien $m \in \mathbb{N}$ und $a_1, \ldots, a_m \in I$ so, dass $I = \langle a_1, \ldots, a_m \rangle_R$. Es gibt dann ein $N \in \mathbb{N}$, sodass $\{a_1, \ldots, a_m\} \subseteq I_N$. Dann gilt aber auch $I_{N+1} \subseteq I \subseteq I_N$, im Widerspruch zu $I_N \subset I_{N+1}$. Somit erfüllt (Id $R, \subseteq$) die (ACC). (2)⇒(3): Sei $\mathcal{I}$ eine nichtleere Menge von Idealen ohne maximales Element. Dann gibt es für jedes $M \in \mathcal{I}$ ein $N \in \mathcal{I}$ mit $M \subset N$. Wir konstruieren nun eine Folge aus $\mathcal{I}$ rekursiv: Sei I_1 ein Element aus $\mathcal{I}$, und für $n \geq 1$ sei I_{n+1} so, dass $I_n \subset I_{n+1}$. Dann ist $(I_n)_{n \in \mathbb{N}}$ eine aufsteigende Kette von Idealen, also erfüllt Id R die aufsteigende Kettenbedingung nicht. (3)⇒(2): Sei $(I_n)_{n \in \mathbb{N}}$ eine Folge von Idealen mit $I_n \subset I_{n+1}$ für alle $n \in \mathbb{N}$. Dann hat $\mathcal{I} := \{I_n \mid n \in \mathbb{N}\}$ kein maximales Element. □

Übungsaufgaben 1.10. Eine *geordnete Menge* $(M, \leq)$ ist ein Paar aus einer Menge und einer Ordnungsrelation (also einer reflexiven, transitiven und antisymmetrischen binären Relation) auf M. Eine geordnete Menge $(M, \leq)$ erfüllt die aufsteigende Kettenbedingung (ACC), wenn es keine injektive Funktion $f : \mathbb{N} \to M$ mit der Eigenschaft $f(i) < f(i+1)$ für alle $i \in \mathbb{N}$ gibt.

(1) Zeigen Sie: Eine geordnete Menge $(M, \leq)$ erfüllt die (ACC) genau dann, wenn es für jede schwach monoton wachsende Folge $\langle m_i \mid i \in \mathbb{N} \rangle$ aus M ein $N \in \mathbb{N}$ gibt, sodass für alle $k \in \mathbb{N}$ mit $k \geq N$ gilt: $m_k = m_N$.
(2) Zeigen Sie: Eine geordnete Menge M erfüllt die (ACC) genau dann, wenn jede nichtleere Teilmenge T von M ein in T maximales Element enthält.

Definition 1.11. Sei R ein kommutativer Ring mit Eins. R heißt *noethersch*[1], wenn jedes Ideal von R endlich erzeugt ist.

Definition 1.12. Sei R ein Ring. Ein Ideal I von R ist *maximal*, wenn $I \neq R$ ist und es kein Ideal J mit $I \subset J \subset R$ gibt.

In einem noetherschen Ring R ist jedes Ideal, das ungleich R ist, in einem maximalen Ideal enthalten. Aus dem Zornschen Lemma[2] folgt, dass das sogar für alle Ringe mit Eins gilt:

[1] Emmy Noether (1882-1935)

[2] Das Zornsche Lemma (Max Zorn (1906-1993), Kazimierz Kuratowski (1896-1980)) besagt:

> Sei $(M, \leq)$ eine geordnete Menge. Wir nehmen an, dass jede linear geordnete Teilmenge L von M eine obere Schranke in M hat. (Das heißt, dass es für jede linear geordnete Teilmenge L ein $m \in M$ gibt, sodass für alle $l \in L$ die Relation $l \leq m$ gilt.) Dann besitzt $(M, \leq)$ ein maximales Element.

SATZ 1.13. *Sei R ein Ring mit Eins, und sei I ein Ideal von R mit $I \neq R$. Dann gibt es ein maximales Ideal M von R mit $I \subseteq M$.*

BEWEIS. Sei

$$\mathcal{E} := \{J \mid J \text{ ist Ideal von } R \text{ und } I \subseteq J \neq R\}.$$

Um zu zeigen, dass $(\mathcal{E}, \subseteq)$ ein maximales Element hat, verwenden wir das Lemma von Zorn. Sei dazu $\mathcal{K}$ eine nichtleere Teilmenge von $\mathcal{E}$, die bezüglich $\subseteq$ linear geordnet ist. Wir setzen

$$S := \bigcup \{K \mid K \in \mathcal{K}\}.$$

Wir zeigen nun, dass S ein Ideal von R ist. Seien $i, j \in S$ und $r \in R$. Da $i \in S$, gibt es $K_1 \in \mathcal{K}$, sodass $i \in K_1$. Ebenso gibt es $K_2 \in \mathcal{K}$, sodass $j \in K_2$. Da $\mathcal{K}$ linear geordnet ist, gilt $K_1 \subseteq K_2$ oder $K_2 \subseteq K_1$. Wenn $K_1 \subseteq K_2$, so liegen $i + j$ und $r \cdot i$ in K_2; falls $K_2 \subseteq K_1$, liegen $i + j$ und $r \cdot i$ in K_1. In beiden Fällen liegen also $i + j$ und $r \cdot i$ in S. Somit ist S ein Ideal von R.

Nun zeigen wir, dass S in $\mathcal{E}$ liegt. Es gilt $I \subseteq S$. Es bleibt also zu zeigen, dass $S \neq R$. Nehmen wir an, $S = R$. Dann gilt $1 \in \bigcup \{K \mid K \in \mathcal{K}\}$. Es gibt also ein $K \in \mathcal{K}$ mit $1 \in K$. Dann gilt $K = R$. Somit gilt $R \in \mathcal{E}$, im Widerspruch zur Definition von $\mathcal{E}$. Es gilt also $S \neq R$, und somit $S \in \mathcal{E}$.

Das Zornsche Lemma liefert nun ein maximales Element M von $\mathcal{E}$. □

ÜBUNGSAUFGABEN 1.14.

(1) Sei R ein Ring, sei I ein endlich erzeugtes Ideal von R, und sei J ein Ideal von R mit $J \subseteq I$. Zeigen Sie, dass R ein Ideal M mit $J \subseteq M \subset I$ besitzt, sodass es kein Ideal N mit $M \subset N \subset I$ gibt.

3. Faktorringe und Homomorphiesatz

Sei R ein Ring mit Eins, und sei I ein Ideal von R. Wir definieren eine Relation $\sim_I$ auf R durch

$$a \sim_I b :\Leftrightarrow a - b \in I \text{ für } a, b \in R.$$

LEMMA 1.15. *Sei R ein Ring mit Eins, sei I ein Ideal von R, und sei $r \in R$. Dann gilt:*

(1) *Die Relation $\sim_I$ ist eine Äquivalenzrelation auf R.*
(2) *Die Äquivalenzklasse von r modulo $\sim_I$ ist gegeben durch $r/\sim_I := \{r + i \mid i \in I\}$. Wir schreiben für diese Klasse auch $[r]_I$ oder $r + I$.*

DEFINITION UND SATZ 1.16 (Faktorring). Sei R ein Ring mit Eins, sei I ein Ideal von R, und sei

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

die Faktormenge von R modulo $\sim_I$. Wir definieren nun

$$\begin{aligned}(r+I)\oplus(s+I) &:= (r+s)+I\\ \ominus(r+I) &:= (-r)+I\\ (r+I)\odot(s+I) &:= (r\cdot s)+I.\end{aligned}$$

Dann sind die Operationen $\oplus$, $\ominus$ und $\odot$ "wohldefiniert", und die algebraische Struktur $(R/I, \oplus, \ominus, \odot, 0+I, 1+I)$ ist ein Ring mit Eins.

Beweis. Wir zeigen nur die Wohldefiniertheit von $\odot$. Sei dazu

$$m := \{\big((r+I, s+I), r\cdot s+I\big) \mid r, s \in R\}.$$

Wir zeigen, dass m eine Funktion von $R/I \times R/I$ nach R/I ist. Dazu zeigen wir, dass für alle $a, b, c_1, c_2 \in R/I$ gilt: Wenn $((a,b),c_1) \in m$ und $((a,b),c_2) \in m$, so gilt $c_1 = c_2$. Seien also $a, b, c_1, c_2 \in R/I$. Dann gibt es $r_1, s_1 \in R$, sodass $r_1 + I = a$, $s_1 + I = b$ und $r_1 \cdot s_1 + I = c_1$. Ebenso gibt es $r_2, s_2 \in R$, sodass $r_2 + I = a$, $s_2 + I = b$ und $r_2 \cdot s_2 + I = c_2$. Da $r_2 \in r_2 + I$, gilt auch $r_2 \in r_1 + I$. Somit gibt es $i \in I$ mit $r_2 = r_1 + i$. Ebenso gibt es $j \in I$ mit $s_2 = s_1 + j$. Es gilt nun $r_2 \cdot s_2 = (r_1 + i)\cdot(s_1 + j) = r_1 \cdot s_1 + r_1 \cdot j + i \cdot s_1 + i \cdot j$. Für $i' := r_1 \cdot j + i \cdot s_1 + i \cdot j$ gilt $i' \in I$. Folglich gilt

$$r_2 \cdot s_2 + I = (r_1 \cdot s_1 + i') + I.$$

Nun gilt für alle $t \in R$, dass $(t + i') + I = t + I$, da $(t + i') + i_1 = t + (i' + i_1) \in t + I$ und $t + i_2 = t + i' + (i_2 - i') \in (t + i') + I$. Also gilt $r_2 \cdot s_2 + I = r_1 \cdot s_1 + I$. Folglich gilt $c_1 = c_2$. Die Relation m ist also wirklich funktional, somit ist $\odot$ wohldefiniert. □

Übungsaufgaben 1.17.

(1) Auf der Menge $\mathbb{Q}$ definieren wir die Relation

$$a \sim b :\Leftrightarrow \lfloor a \rfloor = \lfloor b \rfloor .$$

Wir definieren:

$$[a]_\sim \odot [b]_\sim := [a\,b]_\sim$$

Was ist das Problem an dieser "Definition"?

Für zwei Ringe mit Eins R, S ist die Abbildung $h : R \to S$ ein *Homomorphismus*, wenn für alle $r_1, r_2 \in R$ gilt, dass $h(r_1 + r_2) = h(r_1) + h(r_2)$, $h(-r_1) = -h(r_1)$, $h(r_1 \cdot r_2) = h(r_1) \cdot h(r_2)$, $h(0_R) = 0_S$ und $h(1_R) = 1_S$. (Die Bedingungen $h(-r_1) = h(r_1)$ und $h(0_R) = h(0_S)$ sind insofern überflüssig, als sie sich aus den anderen Bedingungen ergeben.) Bijektive (injektive, surjektive) Homomorphismen heißen auch *Isomorphismen* (*Monomorphismen*, *Epimorphismen*), Monomorphismen heißen auch *Einbettungen*. R ist ein *Unterring* von S, wenn $R \subseteq S$, $0_S \in R$, $1_S \in R$, $r_1 +_R r_2 = r_1 +_S r_2$, $r_1 \cdot_R r_2 = r_1 \cdot_S r_2$ für alle $r_1, r_2 \in R$ gilt.

SATZ 1.18 (Homomorphiesatz). *Seien R, S Ringe mit Eins, und sei $h : R \to S$ ein Homomorphismus. Dann ist* $\ker(h) := \{r \in R \mid h(r) = 0\}$ *ein Ideal von R,* $\mathrm{im}(h) := h(R)$ *ein Unterring von S, die Ringe $R/\ker(h)$ und* $\mathrm{im}(h)$ *sind isomorph, und $\hat{h}$ mit $\hat{h}(r + \ker(h)) := h(r)$ ist ein Isomorphismus.*

SATZ 1.19 (Korrespondenzsatz). *Sei R ein Ring mit Eins, und sei I ein Ideal von R. Sei $\Phi : \{J \in \mathrm{Id}(R) \mid I \subseteq J\} \to \mathrm{Id}(R/I)$, $\Phi(J) := \{j + I \mid j \in J\}$. Dann ist Φ bijektiv, und es gilt für alle Ideale J_1, J_2 von R mit $I \subseteq J_1$, $I \subseteq J_2$: $J_1 \subseteq J_2 \Leftrightarrow \Phi(J_1) \subseteq \Phi(J_2)$.*

BEWEIS. Wir zeigen zunächst, dass für jedes $J \in \mathrm{Id}(R)$ mit $I \subseteq J$ die Menge $\Phi(J)$ ein Ideal von R/I ist: Die Abbildung $\varphi := \{(r + I, r + J) \mid r \in R\}$ ist ein Homomorphismus von R/I nach R/J, und es gilt $\ker(\varphi) = \{r + I \mid r + J = 0 + J\} = \{r + I \mid r \in J\} = \Phi(J)$. Als Kern eines Homomorphismus ist $\Phi(J)$ daher ein Ideal von R/I.

Wir definieren $\Psi : \mathrm{Id}(R/I) \to \mathrm{Id}(R)$, $\Psi(K) := \bigcup\{r + I \mid r \in R, r + I \in K\} = \bigcup K$. Die Abbildung $\psi = \{(r, (r+I)+K) \mid r \in R\}$ ist ein Homomorphismus von R nach $(R/I)/K$ und es gilt $\ker(\psi) = \{r \in R \mid (r + I) + K = 0 + K\} = \{r \in R \mid r + I \in K\} = \bigcup K$. Für die letzte Gleichheit beobachten wir, dass für jedes $r \in R$ mit $r + I \in K$ gilt, dass $r \in r + I \in K$, also $r \in \bigcup K$; für jedes $s \in \bigcup K$ gibt es ein $t \in R$ mit $s \in t + I \in K$. Wegen $s + I = t + I$ gilt dann $s + I \in K$ und somit $s \in \{r \in R \mid r + I \in K\}$. Somit ist $\Psi(K)$ ein Ideal.

Sei J ein Ideal von R mit $I \subseteq J$. Dann gilt $\Psi(\Phi(J)) = \Psi(\{j + I \mid j \in J\}) = \bigcup\{j + I \mid j \in J\}$. Wegen $I \subseteq J$ gilt $\bigcup\{j + I \mid j \in J\} = J$. Sei nun K ein Ideal von R/I. Dann gilt $\Phi(\Psi(K)) = \Phi(\bigcup K) = \{j + I \mid j \in \bigcup K\} = \{j + I \mid \exists r \in R : j \in r + I \in K\} = \{j + I \mid j + I \in K\} = K$. Daher sind Φ und Ψ zueinander inverse Bijektionen.

Für Ideale $I \subseteq J_1 \subseteq J_2$ von R gilt offensichtlich $\Phi(J_1) \subseteq \Phi(J_2)$. Seien nun $J_1, J_2 \in \mathrm{Id}(R)$ so, dass $I \subseteq J_1$, $I \subseteq J_2$ und $\Phi(J_1) \subseteq \Phi(J_2)$. Dann gilt auch $\Psi(\Phi(J_1)) \subseteq \Psi(\Phi(J_2))$ also $J_1 \subseteq J_2$. □

Ein Ring mit Eins R ist *einfach*, wenn er nur die Ideale $\{0\}$ und R hat. Beispiele für einfache Ringe sind Körper und die Matrixringe $K^{n\times n}$ über einem Körper K.

SATZ 1.20. *Sei R ein kommutativer Ring mit Eins mit $|R| \geq 2$. Dann ist R genau dann einfach, wenn R ein Körper ist.*

BEWEIS. Sei R ein Körper, und sei I ein Ideal von R. Wenn $I \neq 0$, dann gibt es $i \in I$ mit $i \neq 0$. Dann gilt für jedes $r \in R$, dass $r = ri^{-1}i \in I$, also $R = I$.

Wenn R einfach und $r \in R$ mit $r \neq 0$ ist, so ist $I := \{rs \mid s \in R\}$ ein Ideal mit $I \neq \{0\}$, also $1 \in I$. Somit gibt es $s \in R$ mit $rs = 1$. Folglich ist R ein Körper. □

KOROLLAR 1.21. *Sei R ein kommutativer Ring mit Eins, und sei M ein maximales Ideal von R. Dann ist R/M ein Körper.*

4. Ringkonstruktionen

4.1. Polynome und Potenzreihen. Sei R ein kommutativer Ring mit Eins, sei $n \in \mathbb{N}$, und seien

$$\begin{aligned} S &:= \{f \mid f : \mathbb{N}_0^n \to R\} \\ P &:= \big\{f \in S \mid \{\boldsymbol{e} \in \mathbb{N}_0^n \mid f(\boldsymbol{e}) \neq 0\} \text{ ist endlich}\big\}. \end{aligned}$$

Auf S definieren wir Addition und Subtraktion durch

$$(f+g)(\boldsymbol{e}) := f(\boldsymbol{e}) + g(\boldsymbol{e}),\ (f-g)(\boldsymbol{e}) := f(\boldsymbol{e}) - g(\boldsymbol{e})$$

für $f, g \in S$, $\boldsymbol{e} \in \mathbb{N}_0^n$. Für $\boldsymbol{a}, \boldsymbol{b} \in \mathbb{N}_0^n$ setzen wir $\delta(\boldsymbol{a}, \boldsymbol{b}) := 1$, wenn $\boldsymbol{a} = \boldsymbol{b}$ und $\delta(\boldsymbol{a}, \boldsymbol{b}) := 0$, wenn $\boldsymbol{a} \neq \boldsymbol{b}$. Die Multiplikation ist definiert durch

$$f \cdot g(\boldsymbol{e}) \sum_{(\boldsymbol{a},\boldsymbol{b}) \in \mathbb{N}_0^n \times \mathbb{N}_0^n} \delta(\boldsymbol{a}+\boldsymbol{b}, \boldsymbol{e}) f(\boldsymbol{a}) g(\boldsymbol{b}). \tag{1.1}$$

Für jedes $\boldsymbol{e} \in \mathbb{N}_0^n$ gibt es nur endlich viele $(\boldsymbol{a}, \boldsymbol{b}) \in \mathbb{N}_0^n \times \mathbb{N}_0^n$ mit $\boldsymbol{a} + \boldsymbol{b} = \boldsymbol{e}$, daher hat die Summe in (1.1) nur endlich viele Summanden $\neq 0$ und ist somit sinnvoll definiert. Für $e_1, \ldots, e_n \in \mathbb{N}_o$ schreiben wir $\overline{X}^{\boldsymbol{e}} = X_1^{e_1} \cdots X_n^{e_n}$ für die Funktion mit $\overline{X}^{\boldsymbol{e}}(\boldsymbol{e}) = 1$, $\overline{X}^{\boldsymbol{e}}(\boldsymbol{a}) = 0$ für $\boldsymbol{a} \neq \boldsymbol{e}$. Wir schreiben dann $f \in S$ als

$$f = \sum_{\boldsymbol{e} \in \mathbb{N}_0^n} f(\boldsymbol{e}) \overline{X}^{\boldsymbol{e}}.$$

Mit $\mathbf{1} := 1X_1^0 \cdots X_n^0$ und $\mathbf{0}$ der konstanten 0-Funktion von $\mathbb{N}_0^n$ nach R gilt dann, dass $(S, +, -, \cdot, \mathbf{0}, \mathbf{1})$ ein kommutativer Ring mit Eins ist, der *Ring der formalen Potenzreihen* mit Koeffizienten in R in n Variablen. Er wird mit $R[[X_1, \ldots, X_n]]$ bezeichnet. Die Menge P bildet einen Unterring von S, den *Polynomring in n Variablen* über R. Dieser Polynomring wird mit $R[X_1, \ldots, X_n]$ bezeichnet.

LEMMA 1.22. *Sei R ein kommutativer Ring mit Eins, seien $\boldsymbol{c}, \boldsymbol{d} \in \mathbb{N}_0^n$ und $r, s \in R$. Dann gilt $(r\overline{X}^{\boldsymbol{c}}) \cdot (s\overline{X}^{\boldsymbol{d}}) = (rs)\overline{X}^{\boldsymbol{c}+\boldsymbol{d}}$.*

BEWEIS. Sei $f := r\overline{X}^{\boldsymbol{c}}$ und $g := s\overline{X}^{\boldsymbol{d}}$. Dann gilt

$$\begin{aligned} (f \cdot g)(\boldsymbol{e}) &= \sum_{(\boldsymbol{a},\boldsymbol{b}) \in \mathbb{N}_0^n \times \mathbb{N}_0^n} \delta(\boldsymbol{a}+\boldsymbol{b}, \boldsymbol{e}) f(\boldsymbol{a}) g(\boldsymbol{b}) \\ &= \delta(\boldsymbol{c}+\boldsymbol{d}, \boldsymbol{e}) f(\boldsymbol{c}) g(\boldsymbol{d}) \\ &= \delta(\boldsymbol{c}+\boldsymbol{d}, \boldsymbol{e}) rs, \end{aligned}$$

und somit $f \cdot g = rs\overline{X}^{\boldsymbol{c}+\boldsymbol{d}}$. □

Sei R ein kommutativer Ring mit Eins, sei T ein kommutativer Ring mit Eins, der R als Unterring enthält, und sei $p \in R[X_1, \ldots, X_n]$. Seien $t_1, \ldots, t_n \in T$. Dann ist die Abbildung $\varepsilon : R[X_1, \ldots, X_n] \to T$,

$$\varepsilon(\sum_{(e_1,\ldots,e_n)\in E} c_{(e_1,\ldots,e_n)} X_1^{e_1} \cdots X_n^{e_n}) := \sum_{(e_1,\ldots,e_n)\in E} c_{(e_1,\ldots,e_n)} t_1^{e_1} \cdots t_n^{e_n}$$

ein Homomorphismus. Die interessante Eigenschaft ist dabei, dass $\varepsilon(p \cdot q) = \varepsilon(p) \cdot \varepsilon(q)$ gilt; diese Eigenschaft ist der Grund, dass wir die Multiplikation wie in (1.1) definiert haben. Wir bezeichnen dann $\varepsilon(p)$ auch als $\hat{p}(t_1, \ldots, t_n)$ oder einfach als $p(t_1, \ldots, t_n)$ und nennen $\hat{p}(t_1, \ldots, t_n)$ die *Auswertung* von p an der Stelle $(t_1, \ldots, t_n)$. Sei nun $U \subseteq T$. Der von R und U *erzeugte* Ring $R[U]$ ist definiert als der Durchschnitt aller Unterringe V von T mit $R \cup U \subseteq V$. Dann gilt

$$R[U] = \{\hat{p}(u_1, \ldots, u_n) \mid n \in \mathbb{N}_0, u_1, \ldots, u_n \in U, p \in R[X_1, \ldots, X_n]\}.$$

4.2. Quotientenkörper. Wir verallgemeinern jetzt die Konstruktion von $\mathbb{Q}$ aus $\mathbb{Z}$. Sei dazu D ein Integritätsbereich. Auf der Menge $\{(a, b) \in D^2 \mid b \neq 0\}$ definieren wir eine Relation durch $(a, b) \sim (c, d) :\Leftrightarrow ad = bc$. Diese Relation ist eine Äquivalenzrelation, und wir kürzen die Klasse $(a, b)/\!\sim$ mit $\frac{a}{b}$ ab. Mit $Q(D)$ bezeichnen wir die Faktormenge $\{(a, b) \in D^2 \mid b \neq 0\}/\!\sim$. Auf $Q(D)$ definieren wir $+$ durch $\frac{a}{b} + \frac{c}{d} := \frac{ad+bc}{bd}$, $-$ durch $-\frac{a}{b} := \frac{-a}{b}$, und $\cdot$ durch $\frac{a}{b} \cdot \frac{c}{d} := \frac{ac}{bd}$.

Satz und Definition 1.23. *Sei D ein Integritätsbereich. Dann ist $(Q(D), +, -, \cdot, \frac{0}{1}, \frac{1}{1})$ ein Körper. Er heißt der* Quotientenkörper *von D.*

Satz 1.24. *Sei D ein Integritätsbereich, sei K ein Körper, und sei φ ein Monomorphismus von D nach K. Dann ist $\psi : Q(D) \to K$, $\psi(\frac{a}{b}) := \varphi(a) \cdot (\varphi(b))^{-1}$ wohldefiniert und ein Monomorphismus vom Quotientenkörper von D nach K.*

Sei K ein Körper. Den Quotientenkörper des Polynomrings $K[X_1, \ldots, X_n]$ bezeichnet man als den Körper der *rationalen Funktionen vom Transzendenzgrad n über K*, und kürzt ihn mit $K(X_1, \ldots, X_n)$ ab.

Übungsaufgaben 1.25.

(1) Sei D ein Integritätsbereich, und sei $S \subseteq D \backslash \{0\}$ eine unter $\cdot$ abgeschlossene Teilmenge von D mit $1 \in S$. Zeigen Sie, dass $S^{-1}D := \{\frac{d}{s} \mid s \in S\}$ ein Unterring von $Q(D)$ ist. Man nennt diesen Unterring die *Lokalisierung* von R nach S.
(2) Beschreiben Sie für $D = \mathbb{Z}$ und $S = \{x \in \mathbb{Z} : 2 \nmid x\}$ jene Elemente von $\mathbb{Q}$, die in $S^{-1}D$ liegen.
(3) Beschreiben Sie für $D = \mathbb{Z}$ und $S = \{2^n \mid n \in \mathbb{N}_0\}$ jene Elemente von $\mathbb{Q}$, die in $S^{-1}D$ liegen.
(4) Welche reellen Zahlen liegen in $S^{-1}\mathbb{Z}$ für $S = \{10^n \mid n \in \mathbb{N}\}$?

KAPITEL 2

Teilbarkeit in Integritätsbereichen

1. Teilbarkeit und prime Elemente

DEFINITION 2.1 (Teilbarkeit). Sei R ein kommutativer Ring mit Eins, und seien $a, b \in R$. Dann gilt $a \mid b$, wenn es ein $r \in R$ gibt, sodass $b = ra$. In diesem Fall ist a ein *Teiler* von b und b ein *Vielfaches* von a.

DEFINITION 2.2. Sei R ein kommutativer Ring mit Eins.

- Ein Element $u \in R$ ist *invertierbar*, wenn es ein $v \in R$ mit $uv = 1$ gibt.
- Ein Element $p \in R$ ist *prim*, wenn es nicht invertierbar ist, und für alle $a, b \in R$ mit $p \mid ab$ gilt: $p \mid a$ oder $p \mid b$.
- Ein Element $r \in R$ ist *irreduzibel*, wenn es nicht invertierbar ist, und für alle $s, t \in R$ mit $r = st$ gilt: s ist invertierbar oder t ist invertierbar.
- Zwei Elemente $a, b \in R$ sind *assoziiert*, wenn es ein invertierbares Element $u \in R$ gibt, sodass $au = b$. Wir schreiben dann $a \sim b$ oder $a \sim_R b$.

LEMMA 2.3. *Sei R ein Integritätsbereich, und sei p ein primes Element von R mit $p \neq 0$. Dann ist p irreduzibel.*

BEWEIS. Sei p prim, $p \neq 0$, und seien $s, t \in R$ so, dass $p = st$. Dann gilt $p \mid st$. Da p prim ist, gilt $p \mid s$ oder $p \mid t$. Im Fall $p \mid s$ gibt es ein $s_1 \in R$, sodass $ps_1 = s$. Durch Multiplikation dieser Gleichung mit t erhalten wir $ps_1t = st = p$. Also gilt $p(s_1t-1) = 0$. Wegen $p \neq 0$ ist also t invertierbar. Im Fall $p \mid t$ erhalten wir analog, dass s invertierbar ist. □

ÜBUNGSAUFGABEN 2.4.

(1) Sei R ein kommutativer Ring mit Eins. Zeigen Sie jeweils, dass die angeführte Implikation für alle $x, y, z \in R$ gilt.
   (a) $(x \mid y \text{ und } x \mid z) \Rightarrow x \mid (y + z)$.
   (b) $x \mid y \Rightarrow x \mid zy$.
   (c) $(x \mid y \text{ und } y \mid z) \Rightarrow x \mid z$.
   (d) $x \mid y \Rightarrow zx \mid zy$.
(2) Sei R ein Integritätsbereich, und seien $x, y, z \in R$ mit $z \neq 0$. Zeigen Sie:
   (a) $x \mid y$ und $y \mid x \Leftrightarrow x$ und y sind assoziiert.
   (b) $x \mid y \Leftrightarrow xz \mid yz$.

(3) (Invertierbare Elemente) Sei R ein kommutativer Ring mit Eins. Zeigen Sie:
   (a) Das Produkt invertierbarer Elemente ist wieder invertierbar.
   (b) Jeder Teiler eines invertierbaren Elements ist invertierbar.
   (c) Ein Element $r \in R$ ist genau dann invertierbar, wenn das von r erzeugte Ideal (r) gleich R ist.

(4) (Invertierbare Elemente) Sei R ein kommutativer Ring mit Eins, sei u invertierbar, und seien v_1, v_2 so, dass $uv_1 = uv_2 = 1$. Zeigen Sie $v_1 = v_2$.

(5) (Assoziierte Elemente) Sei R ein kommutativer Ring mit Eins, und $a_1, a_2, b_1, b_2 \in R$. Wenn $a_1 \sim_R a_2$ und $b_1 \sim_R b_2$, so gilt $a_1 b_1 \sim_R a_2 b_2$.

(6) (Integritätsbereiche) Zeigen Sie, dass jeder endliche Integritätsbereich ein Körper ist. (*Hinweis:* Betrachten Sie für $r \neq 0$ die Abbildung $x \mapsto r \cdot x$.)

(7) (Integritätsbereiche) Zeigen Sie: Jeder Integritätsbereich, der kein Körper ist, besitzt eine unendlich absteigende Kette von Idealen $I_1 \supset I_2 \supset I_3 \supset \cdots$.

(8) (Prime Elemente) Sei R ein Integritätsbereich. Ein Ideal I von R ist *prim*, wenn $I \neq R$ und für alle $a, b \in R$ gilt: $a \cdot b \in I \Rightarrow (a \in I$ oder $b \in I)$. Zeigen Sie:
   (a) Ein Element r ist genau dann prim, wenn das Hauptideal (r) prim ist.
   (b) Wenn r prim und u invertierbar ist, so ist auch $r \cdot u$ prim.

(9) (Einfache Ringe) Ein Ring R ist *einfach*, wenn er keine Ideale außer $\{0\}$ und R hat. Zeigen Sie, dass die beiden folgenden Behauptungen äquivalent sind:
   (a) R ist ein einfacher kommutativer Ring mit Eins, und $|R| \geq 2$.
   (b) R ist ein Körper.

(10) (Irreduzible Elemente) Sei R ein Integritätsbereich, und sei $r \in R$ mit $r \neq 0$.
   (a) Zeigen Sie, dass folgende Bedingungen äquivalent sind.
      (i) r ist irreduzibel.
      (ii) Das Ideal (r) ist ein maximales Element in der Menge aller Hauptideale von R, die ungleich R sind.
   (b) Zeigen Sie: Wenn r irreduzibel ist, ist auch jedes zu r assoziierte Element irreduzibel.

2. Größte gemeinsame Teiler

DEFINITION 2.5. Sei R ein kommutativer Ring mit Eins, und sei A eine Teilmenge von R. Ein Element $d \in R$ ist ein *größter gemeinsamer Teiler* von A, wenn

(1) für alle $a \in A$ gilt $d \mid a$.
(2) für alle $d' \in R$ gilt: $(\forall a \in A : d' \mid a) \Rightarrow d' \mid d$.

Für zwei größte gemeinsame Teiler d_1, d_2 von A gilt also, dass $d_1 \mid d_2$ und $d_2 \mid d_1$. Wenn R ein Integritätsbereich ist, sind d_1 und d_2 assoziiert.

LEMMA 2.6. *Sei R ein Integritätsbereich, sei A eine Teilmenge von R, und seien $t \in R \setminus \{0\}$, $d_1, d_2 \in R$. Wir nehmen an, dass d_1 ein größter gemeinsamer Teiler von A und d_2 ein größter gemeinsamer Teiler von $tA = \{ta \mid a \in A\}$ ist. Dann sind td_1 und d_2 assoziiert.*

BEWEIS. Da td_1 jedes Element von tA teilt, gilt $td_1 \mid d_2$. Da t ein gemeinsamer Teiler von tA ist, gilt $t \mid d_2$. Sei $d_3 \in R$ so, dass $td_3 = d_2$. Da td_3 jedes Element in tA teilt und $t \neq 0$, teilt d_3 jedes Element in A, und somit gilt $d_3 \mid d_1$ und somit $td_3 \mid td_1$, also $d_2 \mid td_1$. □

ÜBUNGSAUFGABEN 2.7.

(1) Sei R ein kommutativer Ring mit Eins, und sei A eine Teilmenge von R. Ein Element $v \in R$ ist ein *kleinstes gemeinsames Vielfaches* von A, wenn für alle $a \in A$ gilt, dass $a \mid v$, und wenn für alle $v' \in R$, die von allen $a \in A$ geteilt werden, gilt, dass $v \mid v'$. Zeigen Sie: Wenn jede Teilmenge von R einen größten gemeinsamen Teiler hat, so hat auch jede Teilmenge von R ein kleinstes gemeinsames Vielfaches.

3. Euklidische Integritätsbereiche

DEFINITION 2.8. Sei R ein Integritätsbereich. Der Integritätsbereich R ist ein *Euklidischer Bereich*, wenn es eine Funktion $\delta : R \setminus \{0\} \to \mathbb{N}_0$ gibt, sodass folgendes gilt.

(1) Für alle $a, b \in R \setminus \{0\}$ gilt $\delta(a) \leq \delta(a\,b)$.
(2) Für alle $a, b \in R$ mit $a \neq 0$ gibt es $q, r \in R$, sodass
   (a) $b = a\,q + r$, und
   (b) $r = 0$ oder $\delta(r) < \delta(a)$.

SATZ 2.9. *Der Ring $\mathbb{Z}$ ist ein Euklidischer Bereich.*

BEWEIS. Die Funktion $\delta(z) := |z|$ für $z \in \mathbb{Z} \setminus \{0\}$ leistet das Gewünschte. □

SATZ 2.10. *Sei K ein Körper, und sei $K[X]$ der Polynomring über K. Dann ist $K[X]$ ein Euklidischer Bereich.*

BEWEIS. Wir setzen $\delta(f) := \deg(f)$. □

DEFINITION 2.11. Sei $\mathbb{Z}[i]$ die Teilmenge der komplexen Zahlen, die durch

$$\mathbb{Z}[i] := \{x + y\,i \mid x, y \in \mathbb{Z}\}$$

definiert ist. Als Operationen verwenden wir die Addition und Multiplikation der komplexen Zahlen. Dann nennen wir $\mathbb{Z}[i]$ den *Ring der Gaußschen ganzen Zahlen.*

SATZ 2.12. *$\mathbb{Z}[i]$ ist ein Euklidischer Bereich.*

BEWEIS. Als Unterring des Körpers $\mathbb{C}$ ist $\mathbb{Z}[i]$ ein Integritätsbereich. Wir definieren nun $\delta(x + y\,i) := x^2 + y^2$ für alle $x, y \in \mathbb{Z}$. Dann gilt $\delta(z_1 \cdot z_2) = \delta(z_1) \cdot \delta(z_2)$ für alle $z_1, z_2 \in \mathbb{Z}[i]$, und somit ist Eigenschaft (1) von Definition 2.8 erfüllt.

Seien nun $b, a \in \mathbb{Z}[i]$ mit $a \neq 0$, und seien $u', v' \in \mathbb{Q}$ so, dass $b = a \cdot (u' + v'\,i)$. Wir wählen nun $u, v \in \mathbb{Z}$, sodass $|u - u'| \leq \frac{1}{2}$ und $|v - v'| \leq \frac{1}{2}$. Sei nun

$$q := u + v\,i \text{ und } r := b - q\,a.$$

Für alle $x, y \in \mathbb{Q}$ definieren wir $\hat{\delta}(x + y\,i) := x^2 + y^2 = \det(\begin{pmatrix} x & -y \\ y & x \end{pmatrix})$. Dann gilt

$$\begin{aligned}\delta(r) &= \delta((u' + v'\,i) \cdot a - (u + v\,i) \cdot a) = \delta(a \cdot ((u' - u) + (v' - v)\,i)) \\ &= \hat{\delta}(a) \cdot \hat{\delta}((u' - u) + (v' - v)\,i) = \delta(a) \cdot ((u' - u)^2 + (v' - v)^2) \leq \delta(a) \cdot \frac{1}{2}.\end{aligned}$$

Da $a \neq 0$, gilt $\delta(a) = a\overline{a} \neq 0$, und somit gilt $\delta(r) < \delta(a)$. □

Definition 2.13. Ein Integritätsbereich R ist ein *Hauptidealbereich*, wenn es für jedes Ideal I von R ein $a \in R$ gibt, sodass $I = (a)$.

Satz 2.14. *Jeder Euklidische Bereich ist ein Hauptidealbereich.*

Beweis. Sei R ein Euklidischer Bereich, und sei I ein Ideal von R. Wenn $I = \{0\}$, so gilt $I = (0)$. Wenn $I \neq 0$, so wählen wir ein $a \in I \setminus \{0\}$, für das $\delta(a)$ minimal ist. Sei nun $b \in I$, und seien $q, r \in R$ so, dass $b = q\,a + r$ und ($r = 0$ oder $\delta(r) < \delta(a)$). Da $r = b - q\,a \in I$, kann $\delta(r) < \delta(a)$ wegen der Minimalität von $\delta(a)$ nicht gelten. Also gilt $r = 0$ und $b = q\,a \in (a)$. Somit gilt $I = (a)$. □

Satz 2.15. *Sei R ein Hauptidealbereich. Dann besitzt jede Teilmenge A von R einen größten gemeinsamen Teiler.*

Beweis. Sei $d \in R$ so, dass (d) das von A erzeugte Ideal ist. Da jedes Element von A in (d) liegt, gilt $\forall a \in A : d \mid a$. Sei nun d' ein weiterer gemeinsamer Teiler von A. Da $d \in \langle A \rangle_R$, gibt es $n \in \mathbb{N}_0$, $a_1, \ldots, a_n \in A$ und $r_1, \ldots, r_n \in R$ mit $d = \sum_{i=1}^{n} r_i a_i$. Da d' jedes a_i teilt, gilt dann auch $d' \mid d$. Somit ist d ein größter gemeinsamer Teiler von A. □

In einem Euklidischen Bereich kann für eine endliche Menge die Menge aller größten gemeinsamen Teiler $\mathrm{ggTM}(A)$ von $A = \{a_1, \ldots, a_n\}$ dadurch ausrechnen, dass

(1) $\mathrm{ggTM}(\varnothing) = \{0\}$, $\mathrm{ggTM}(A) = \mathrm{ggTM}(A \setminus \{0\})$,
(2) $\mathrm{ggTM}(\{a_1, \ldots, a_n\}) = \mathrm{ggTM}(\{r_1, a_2, \ldots, a_n\})$, wenn $a_1 \neq 0$, $a_2 \neq 0$, $\delta(a_1) \geq \delta(a_2)$, und $a_1 = qa_2 + r_1$ mit $q \in R$ und ($r_1 = 0$ oder $\delta(r_1) < \delta(a_2)$).

Die Gleichheiten der Form $\mathrm{ggTM}(B) = \mathrm{ggTM}(C)$ gelten dabei stets deswegen, weil B und C die gleichen gemeinsamen Teiler haben. Durch diese Gleichheiten erhält man ein $d \in R$ mit $\mathrm{ggTM}(A) = \mathrm{ggTM}(\{d\})$, also ist d ein größter gemeinsamer Teiler. Durch Buchführung erhält man auch $r_1, \ldots r_n \in R$ mit $\sum_{i=1}^{n} r_i a_i = d$ (erweiterter Euklidischer Algorithmus).

Beispiel: Wir berechnen $\mathrm{ggT}(147, 33)$, und schreiben das so:

	147	33	
147	1	0	$(147 = 1 \cdot 147 + 0 \cdot 33)$
33	0	1	$(33 = 0 \cdot 147 + 1 \cdot 33)$
15	1	-4	$(15 = 1 \cdot 147 - 4 \cdot 33)$
3	-2	9	$(3 = -2 \cdot 147 + 9 \cdot 33)$
0			

Das ermöglicht noch nicht alle ggT-Berechnungen: obwohl es in $\mathbb{Q}[X, Y]$ stets größte gemeinsame Teiler gibt, kann man diese nicht (direkt) mit dem Euklidischen Algorithmus ausrechnen.

BEISPIEL 2.16. Der Polynomring $\mathbb{Q}[X, Y]$ ist kein Hauptidealbereich.

BEWEIS. Sei $I := \{p \in \mathbb{Q}[X, Y] \mid \overline{p}(0, 0) = 0\}$. Dann gilt $X \in I$ und $Y \in I$. Wenn I ein Hauptideal ist, so gibt es $f \in I$ mit $f \mid X$ und $f \mid Y$. Also gilt $\deg_X(f) = 0$ und $\deg_Y(f) = 0$, und somit ist f ein konstantes Polynom. Da $f \in I$, gilt $\overline{f}(0, 0) = 0$, und somit $f = 0$. Das ist ein Widerspruch zu $f \mid X$. Somit ist I kein Hauptideal. □

SATZ 2.17. *Sei R ein Hauptidealbereich, und sei $p \in R$ ein irreduzibles Element von R. Dann ist p prim.*

BEWEIS. Seien $a, b \in R$ so, dass $p \mid a\,b$. Sei $J := \{s\,p + t\,a \mid s, t \in R\}$ das von $\{p, a\}$ erzeugte Ideal von R. Da J ein Hauptideal ist, gibt es $c \in J$ mit $(c) = J$. Dann gilt $c \mid p$ und $c \mid a$. Sei $d \in R$ so, dass $c\,d = p$. Da p irreduzibel ist, ist c invertierbar oder d invertierbar. Wenn c invertierbar ist, so gilt $1 \in J$. Also gibt es $s', t' \in R$ mit $s'p + t'a = 1$. Dann gilt $s'pb + t'ab = b$, und somit $p \mid b$. Wenn d invertierbar ist, so gilt wegen $c \mid a$ auch $p = c\,d \mid a\,d$. Da d invertierbar ist, gilt $a\,d \mid a$, und somit $p \mid a$. □

ÜBUNGSAUFGABEN 2.18.

(1) Sei R ein Hauptidealbereich, und sei r ein irreduzibles Element von R.
   (a) Zeigen Sie, dass (r) ein maximales Ideal von R ist.
   (b) Zeigen Sie, dass $R/(r)$ ein Integritätsbereich ist. Was bedeutet das für das Element r?
(2) Zeigen Sie, dass $\mathbb{Z}[X]$ kein Hauptidealbereich ist.

4. Eine Anwendung in der Zahlentheorie

Wir brauchen zunächst folgende Beobachtung:

LEMMA 2.19. *Sei p eine ungerade Primzahl. Dann gilt:*

(1) *Für jedes $x \in \{1, \ldots, p-1\}$ gibt es ein $y \in \{1, \ldots, p-1\}$ mit $x \cdot y \equiv 1 \pmod{p}$.*
(2) *Für jedes $x \in \mathbb{Z}$ gilt: wenn $x^2 \equiv 1 \pmod{p}$, so gilt $x \equiv 1 \pmod{p}$ oder $x \equiv -1 \pmod{p}$.*

(3) $(p-1)! \equiv -1 \pmod{p}$ *und* $(\frac{p-1}{2}!)^2 \equiv (-1)^{\frac{p-3}{2}} \pmod{p}$.

BEWEIS. (1) Da $\mathrm{ggT}(x,p) = 1$, gibt es $u, v \in \mathbb{Z}$ mit $ux + vp = 1$. Somit gilt für $y := u \bmod p$, dass $y\,x \equiv 1 \pmod{p}$. (2) Die Zahl p ist als Primzahl in $\mathbb{Z}$ irreduzibel, und folglich ein primes Element von $\mathbb{Z}$. Wenn also $p \mid x^2 - 1 = (x+1)(x-1)$, so gilt $p \mid x+1$ oder $p \mid x-1$. (3) Für jedes $x \in \{2, \ldots, p-2\}$ gibt es ein $y \in \{2, \ldots, p-2\}$ mit $x\,y \equiv 1 \pmod{p}$. Dieses y erfüllt $y \neq x$. Somit gilt $\prod_{i=2}^{p-2} i \equiv 1 \pmod{p}$, also $(p-1)! \equiv -1 \pmod{p}$. Für $i \in \{1, \ldots, \frac{p-1}{2}\}$ gilt $-i \equiv p - i \pmod{p}$, also gilt

$$-1 \equiv_p (p-1)! = \prod_{i=1}^{\frac{p-1}{2}} i \cdot \prod_{i=1}^{\frac{p-1}{2}} (p-i)$$
$$\equiv_p (\frac{p-1}{2}!) \cdot (-1)^{\frac{p-1}{2}} \cdot (\frac{p-1}{2}!) = (\frac{p-1}{2}!)^2 \cdot (-1)^{\frac{p-1}{2}}.$$

□

Wir beweisen nun den folgenden Satz:

SATZ 2.20. *Sei p eine Primzahl mit $p \equiv 1 \pmod{4}$. Dann gibt es $a, b \in \mathbb{N}$, sodass $a^2 + b^2 = p$.*

BEWEIS. Sei $x := \frac{p-1}{2}!$. Wegen Lemma 2.19 gilt dann

$$x^2 \equiv -1 \pmod{p}. \tag{2.1}$$

Im Ring $\mathbb{Z}[i]$ gilt natürlich ebenfalls $p \mid (1 + x^2)$, also $p \mid (1 + x\,i) \cdot (1 - x\,i)$. Da jedes Vielfache von p im Ring $\mathbb{Z}[i]$ einen durch p teilbaren Realteil hat, gilt in $\mathbb{Z}[i]$ weder $p \mid (1 + x\,i)$ noch $p \mid (1 - x\,i)$. Im Ring $\mathbb{Z}[i]$ ist p also nicht prim. Wegen Satz 2.12 und Satz 2.14 ist $\mathbb{Z}[i]$ ein Hauptidealbereich. Somit ist wegen Satz 2.17 jedes irreduzible Element von $\mathbb{Z}[i]$ prim. Also ist p in $\mathbb{Z}[i]$ nicht irreduzibel. Es gibt folglich $a, b, c, d \in \mathbb{Z}$, sodass $p = (a+b\,i)(c+d\,i)$, und $a+b\,i$ und $c+d\,i$ nicht invertierbar sind. Sei $N(u+v\,i) := u^2 + v^2$ für alle $u, v \in \mathbb{Z}$. Dann gilt

$$p^2 = N(p) = N((a + b\,i)(c + d\,i)) = N(a + b\,i) \cdot N(c + d\,i) = (a^2 + b^2)(c^2 + d^2).$$

Alle Elemente $z \in \mathbb{Z}[i]$ mit $N(z) = 1$ sind invertierbar. Somit muss $a^2 + b^2 = p$ gelten. Die Zahlen $a' := |a|$ und $b' := |b|$ leisten also das Gewünschte. □

KAPITEL 3

Faktorielle Integritätsbereiche

1. Definition und Zerlegung in irreduzible Elemente

DEFINITION 3.1. Sei R ein Integritätsbereich. R ist *faktoriell*, wenn folgendes gilt:

(1) Für alle $r \in R \setminus \{0\}$, die nicht invertierbar sind, gibt es ein $s \in \mathbb{N}$ und irreduzible $f_1, \ldots, f_s \in R$, sodass
$$r = f_1 \cdots f_s.$$
(2) Für alle $m, n \in \mathbb{N}$ und für alle irreduziblen $f_1, \ldots, f_m, g_1, \ldots, g_n \in R$ mit
$$f_1 \cdots f_m = g_1 \cdots g_n$$
gilt $m = n$, und es gibt eine bijektive Abbildung $\pi : \{1, \ldots, m\} \to \{1, \ldots, n\}$, sodass für alle $i \in \{1, \ldots, m\}$ gilt: $f_i \sim_R g_{\pi(i)}$.

DEFINITION 3.2. Sei R ein Integritätsbereich, und sei $I \subseteq R$. I ist eine *vollständige Auswahl irreduzibler Elemente*, wenn alle $i \in I$ irreduzibel sind und es für jedes irreduzible $f \in R$ genau ein $i \in I$ mit $f \sim_R i$ gibt.

DEFINITION 3.3 (Zerlegung). Sei R ein Integritätsbereich, und sei $I \subseteq R$ eine vollständige Auswahl irreduzibler Elemente von R. Sei $a \in \mathbb{R} \setminus \{0\}$. Eine Funktion $\alpha : I \to \mathbb{N}_0$ ist eine *Zerlegung* von a, wenn

(1) $\{i \in I \mid \alpha(i) \neq 0\}$ ist endlich.
(2) $a \sim_R \prod_{i \in I} i^{\alpha(i)}$.

Dabei definieren wir für alle $i \in I$, dass $i^0 := 1$ ist. Ebenso ist ein Produkt $\prod_{i \in \varnothing} r_i$ immer gleich 1. Wir schreiben $\prod_{i \in I} r_i$ nur, wenn $\{i \in I \mid i \neq 1\}$ endlich ist, und meinen damit $\prod_{i \in I, r_i \neq 1} r_i$.

LEMMA 3.4. *Sei R ein faktorieller Integritätsbereich und sei I eine vollständige Auswahl irreduzibler Elemente von R. Seien $a, b \in R \setminus \{0\}$, sei α eine Zerlegung von a bezüglich I und β eine Zerlegung von b bezüglich I. Dann sind äquivalent:*

(1) $a \mid b$.
(2) *Für alle $i \in I$ gilt $\alpha(i) \leq \beta(i)$.*

BEWEIS. Wir beweisen nur (1)⇒(2). Sei $r \in R$ so, dass $ar = b$. Wir nehmen an, dass es ein $i_0 \in I$ gibt, sodass $\alpha(i_0) > \beta(i_0)$. Dann gilt

$$r \cdot i_0^{\alpha(i_0)} \cdot \prod_{\substack{i \in I \\ i \neq i_0}} i^{\alpha(i)} \sim_R i_0^{\beta(i_0)} \cdot \prod_{\substack{i \in I \\ i \neq i_0}} i^{\beta(i)}.$$

Es gibt also ein invertierbares $u_1 \in R$, sodass

$$u_1 \cdot r \cdot i_0^{\alpha(i_0)} \cdot \prod_{\substack{i \in I \\ i \neq i_0}} i^{\alpha(i)} = i_0^{\beta(i_0)} \cdot \prod_{\substack{i \in I \\ i \neq i_0}} i^{\beta(i)}.$$

Da R ein Integritätsbereich ist und $i_0^{\beta(i_0)} \neq 0$, gilt

$$u_1 \cdot r \cdot i_0^{\alpha(i_0)-\beta(i_0)} \prod_{\substack{i \in I \\ i \neq i_0}} i^{\alpha(i)} = \prod_{\substack{i \in I \\ i \neq i_0}} i^{\beta(i)}.$$

Der Ring R ist faktoriell. Also gibt es ein invertierbares Element $u_2 \in R$ und ein $s \in \mathbb{N}_0$ und irreduzible Elemente $r_1, \ldots, r_s \in R$ sodass $r = u_2 r_1 \cdots r_s$. Es gilt dann

$$u_1 u_2 r_1 \cdots r_s \cdot i_0^{\alpha(i_0)-\beta(i_0)} \prod_{\substack{i \in I \\ i \neq i_0}} i^{\alpha(i)} = \prod_{\substack{i \in I \\ i \neq i_0}} i^{\beta(i)}. \tag{3.1}$$

Falls $\{i \in I \mid \beta(i) > 0 \text{ und } i \neq i_0\} = \varnothing$, so ist i_0 invertierbar, im Widerspruch dazu, dass i_0 irreduzibel ist. Wenn die rechte Seite von (3.1) aus einer positiven Anzahl von Faktoren besteht, können wir verwenden, dass R faktoriell ist. Wir erhalten dann ein $i_1 \in I$ mit $i_1 \neq i_0$ und $i_1 \sim_R i_0$. Das ist unmöglich, da I keine verschiedenen assoziierten Elemente enthält. □

KOROLLAR 3.5 (Eindeutigkeit der Zerlegung). *Sei R ein faktorieller Integritätsbereich und sei I eine vollständige Auswahl irreduzibler Elemente von R. Sei $f \in R \setminus \{0\}$. Dann gibt es genau eine Zerlegung $\alpha : I \to \mathbb{N}_0$ von f.*

BEWEIS. Wir zeigen zunächst, dass es ein α mit den geforderten Eigenschaften gibt. Wenn f invertierbar ist, so definieren wir α durch $\alpha(i) = 0$ für alle $i \in I$. Es gilt $f \sim_R 1$, also ist (2) aus Definition 3.3 erfüllt. Wenn f nicht invertierbar ist, so gibt es $s \in \mathbb{N}$ und irreduzible Elemente $g_1, \ldots, g_s \in R$, sodass

$$f = g_1 \cdots g_s.$$

Seien nun $i_1, \ldots, i_s \in I$ und $u_1, \ldots, u_s$ invertierbare Elemente von R, sodass für alle $j \in \{1, \ldots, s\}$ gilt: $g_j = u_j i_j$. Es gilt dann $f = (u_1 \cdots u_s) \cdot (i_1 \cdots i_s)$. Für $i \in I$ definieren wir $\alpha(i)$ als die Anzahl der Elemente von $\{j \in \{1, \ldots, s\} \mid i_j = i\}$. Um die Eindeutigkeit

zu zeigen, fixieren wir $\alpha, \beta : I \to \mathbb{N}_0$, sodass beide Funktionen nur an endlich vielen Stellen nicht 0 sind, und

$$\prod_{i \in I} i^{\alpha(i)} \sim_R \prod_{i \in I} i^{\beta(i)}.$$

Wegen Lemma 3.4 gilt dann $\alpha = \beta$. □

SATZ 3.6. *Sei R ein faktorieller Integritätsbereich, und sei $A \subseteq R$. Dann besitzt A einen größten gemeinsamen Teiler.*

BEWEIS. Sei I eine Auswahl irreduzibler Elemente, und sei für jedes Element $a \in I$ die Abbildung $\alpha_a : I \to \mathbb{N}_0$ eine Zerlegung von a. Wenn $A = \varnothing$, ist 0 ein größter gemeinsamer Teiler. Im Fall $A \neq \varnothing$ ist wegen Lemma 3.4 das Element $d := \prod_{i \in I} i^{\min\{\alpha_a(i) \mid a \in A\}}$ ein größter gemeinsamer Teiler. □

In einem faktoriellen Integritätsbereich besitzt auch jede Menge A ein kleinstes gemeinsames Vielfaches, also ein v, das Vielfaches aller $a \in A$ ist und das jedes weitere gemeinsame Vielfache von A teilt. Wenn für unendlich viele $i \in I$ gilt, dass $\max\{\alpha_a(i) \mid a \in A\} > 0$, so ist $v = 0$, ansonsten kann v mit $v = \prod_{i \in I} i^{\max\{\alpha_a(i) \mid a \in A\}}$ berechnet werden.

ÜBUNGSAUFGABEN 3.7.

(1) Sei R ein faktorieller Integritätsbereich, seien $a, b \in R$, sei d ein größter gemeinsamer Teiler von $\{a, b\}$, und sei v ein kleinstes gemeinsames Vielfaches von $\{a, b\}$. Zeigen Sie, dass $dv \sim_R ab$.

2. Beschreibung faktorieller Integritätsbereiche

Faktorielle Integritätsbereiche lassen sich in folgender Weise charakterisieren:

SATZ 3.8. *Sei R ein Integritätsbereich. Dann sind äquivalent:*

(1) *R erfüllt die* (ACC) *für Hauptideale, und jedes irreduzible Element von R ist prim.*
(2) *R ist faktoriell.*

BEWEIS. (1)⇒(2). Wir zeigen zunächst, dass sich jedes nicht invertierbare Element $r \neq 0$ in ein Produkt von irreduziblen Elementen zerlegen lässt. Dazu nehmen wir an, dass es ein nicht invertierbares Element $r \neq 0$ gibt, das sich nicht zerlegen lässt. Wir wählen $r \in R \setminus \{0\}$ so, dass (r) maximal in der Menge

$$\{(r') \mid r' \text{ ist nicht invertierbar und nicht Produkt von irreduziblen Elementen}\}$$

ist. Da r nicht invertierbar ist, gilt $(r) \neq R$. Nun wählen wir $s \in R$ so, dass (s) maximal in der Menge

$$\{(s') \mid (r) \subseteq (s') \neq R\}$$

ist. Wir zeigen als erstes, dass s irreduzibel ist. Wenn $s = s_1 s_2$, so gilt $(s) \subseteq (s_1)$ und $(s) \subseteq (s_2)$. Wenn s_1 nicht invertierbar ist, so gilt wegen der Maximalität von (s) die Gleichheit $(s) = (s_1)$. Folglich gibt es $t \in R$, sodass $s_1 = ts$, also $s_1 = ts_1 s_2$. Da $s_1 \neq 0$, ist s_2 invertierbar. Somit ist s irreduzibel. Da $r \in (s)$, gibt es $t_1 \in R$, sodass $r = t_1 s$. Wenn t_1 invertierbar ist, so ist r irreduzibel, im Widerspruch zur Wahl von r. Wenn t_1 nicht invertierbar ist, so gilt $(r) \subseteq (t_1) \neq R$. Wenn nun $(r) = (t_1)$, so gibt es ein $s_1 \in R$ mit $t_1 = s_1 r = s_1 t_1 s$. Da $t_1 \neq 0$, ist dann $s_1 s = 1$ und s somit invertierbar. Also gilt $(r) \neq (t_1)$. Wegen der Maximalität von (r) lässt sich t_1 als Produkt von irreduziblen Elemente schreiben. Fügen wir zu diesem Produkt noch s dazu, haben wir auch r als Produkt irreduzibler Elemente geschrieben, im Widerspruch zur Wahl von r. Somit lässt sich jedes nicht invertierbare Element $\neq 0$ in irreduzible Elemente zerlegen.

Nun zeigen wir die Eindeutigkeit. Seien $m, n \in \mathbb{N}$, und $f_1, \ldots, f_m, g_1, \ldots, g_n$ irreduzible Elemente, sodass $f_1 \cdots f_m = g_1 \cdots g_n$. Wir zeigen durch Induktion nach $\min(m, n)$, dass sich die f_i und g_j zueinander assoziieren lassen. Wenn $m = 1$, so gilt, da f_1 irreduzibel ist, auch $n = 1$, und somit $f_1 = g_1$. Wenn $n = 1$, so gilt analog $m = 1$ und $f_1 = g_1$. Wenn $m \geq 2$ und $n \geq 2$, dann gilt $f_1 \mid g_1 \cdots g_n$. Da f_1 nach Voraussetzung prim ist, teilt es eines der g_i. Da g_i irreduzibel ist, gilt $f_1 \sim_R g_i$. Es gibt also ein invertierbares $u \in R$, sodass $g_i = u \cdot f_1$. Wir wenden nun die Induktionsvoraussetzung auf $(uf_2) \cdot f_3 \cdots f_m = g_1 \cdots g_{i-1} g_{i+1} \cdots g_n$ an.

(2)⇒(1): Sei R ein faktorieller Ring, und sei $(a_1) \subseteq (a_2) \subseteq (a_3) \subseteq \ldots$ eine Kette von Hauptidealen. Wir nehmen an $(a_1) \neq (0)$. Dann gilt $a_n \mid a_{n-1} \mid \cdots \mid a_3 \mid a_2 \mid a_1$. Sei I eine vollständige Auswahl von irreduziblen Elementen, und sei α_k eine Zerlegung von a_k bezüglich I. Es gilt dann nach Lemma 3.4 für alle $i \in I$: $\alpha_k(i) \leq \alpha_1(i)$. Da es nur endlich viele $\beta : I \to \mathbb{N}_0$ mit der Eigenschaft $\beta(i) \leq \alpha_1(i)$ für alle $i \in I$ gibt, und da die Folgen $(\alpha_k(i))_{k \in \mathbb{N}}$ wegen Lemma 3.4 für alle $i \in I$ schwach monoton fallend sind, gibt es ein $N \in \mathbb{N}$, sodass für $k \geq N$ gilt: $\alpha_k = \alpha_N$. Dann gilt aber auch $(a_k) = (a_N)$.

Wir zeigen nun, dass jedes irreduzible Element von R prim ist. Sei dazu f irreduzibel, und seien $a, b \in R$ so, dass $f \mid ab$. Zu zeigen ist, dass f mindestens eines der Elemente a oder b teilt. Wegen $f \mid ab$ gibt es $r \in R$, sodass

$$fr = ab.$$

Wenn $a = 0$, so gilt $f \mid a$; wenn $b = 0$, so gilt $f \mid b$. Wir nehmen nun an, dass $a \neq 0$ und $b \neq 0$. Wenn a invertierbar ist, dann gilt $fra^{-1} = b$, und somit $f \mid b$; wenn b invertierbar ist, gilt $f \mid a$. Es bleibt der Fall, dass a, b beide $\neq 0$ und beide nicht invertierbar sind. Dann gibt es $m, n \in \mathbb{N}$ und irreduzible Elemente $a_1, \ldots, a_m, b_1, \ldots, b_n \in R$, sodass

$$a = a_1 \cdots a_m \text{ und } b = b_1 \cdots b_n.$$

Falls r invertierbar ist, dann ist fr irreduzibel, und wegen der Eindeutigkeit der Zerlegung zu einem a_i oder b_j assoziiert. Wenn fr zu einem a_i assoziiert ist, dann gilt $fr \mid a$, und somit $f \mid a$; wenn fr zu einem b_j assoziiert ist, dann gilt $f \mid b$.

Wenn r nicht invertierbar ist, dann gibt es $l \in \mathbb{N}$ und irreduzible Elemente $r_1, \ldots, r_l \in R$, sodass

$$fr_1 \cdots r_l = a_1 \cdots a_m \cdot b_1 \cdots b_n.$$

Wegen der Eindeutigkeit der Zerlegung ist f zu einem a_i oder b_j assoziiert. Es gilt also wieder $f \mid a$ oder $f \mid b$. □

Definition 3.9. Ein Integritätsbereich R ist ein *Hauptidealbereich*, wenn es für jedes Ideal I von R ein $a \in R$ gibt, sodass $I = (a)$.

Satz 3.10. *Jeder Hauptidealbereich ist faktoriell.*

Beweis. Sei R ein Hauptidealbereich. Da jedes Ideal von R endlich erzeugt ist, erfüllt R die (ACC) für Ideale, also insbesondere für Hauptideale. Wegen Satz 2.17 ist jedes irreduzible Element von R prim. □

3. Teilbarkeit in Polynomringen

In diesem Kapitel zeigen wir, dass für einen faktoriellen Integritätsbereich R der Polynomring $R[X]$ ebenfalls ein faktorieller Integritätsbereich ist.

Definition 3.11. Sei R ein kommutativer Ring mit Eins, sei $n \in \mathbb{N}_0$, und sei $f = \sum_{i=0}^{n} f_i X^i \in R[X]$. Das Polynom f ist *primitiv*, wenn es kein primes $p \in R$ gibt, das alle Koeffizienten f_i $(i = 0, \ldots, n)$ teilt.

Lemma 3.12 (Gaußsches Lemma). *Sei R ein kommutativer Ring mit Eins, und seien $f, g \in R[X]$ primitiv. Dann ist $f \cdot g$ ebenfalls primitiv.*

Beweis. Wir nehmen an, dass $f \cdot g$ nicht primitiv ist. Dann gibt es ein primes $p \in R$, das alle Koeffizienten von $f \cdot g$ teilt. Wir bezeichen mit $[f]_{(p)}$ das Polynom $\sum_{i=0}^{\deg f}(f_i + (p))X^i$ im Ring $R/(p)\,[X]$. Es gilt also dann $[f \cdot g]_{(p)} = 0$. Da (p) prim ist, ist $R/(p)$ ein Integritätsbereich. Daher ist auch $R/(p)[X]$ ein Integritätsbereich (der führende Koeffizient des Produkts zweier Polynome ist das Produkt der führenden Koeffizienten dieser zwei Polynome). Da $[f \cdot g]_{(p)} = [f]_{(p)} \cdot [g]_{(p)}$, muss also $[f]_{(p)}$ oder $[g]_{(p)}$ gleich 0 sein. Wenn $[f]_{(p)}$ gleich 0 ist, dann teilt p alle Koeffizienten von f, und f ist somit nicht primitiv; $[g]_{(p)} = 0$ bedeutet, dass g nicht primitiv ist. □

Für einen faktoriellen Integritätsbereich fixieren wir eine Funktion $\gcd : \mathcal{P}(R) \to R$ mit der Eigenschaft, dass für jedes $A \subseteq R$ das Element $\gcd(A)$ ein größter gemeinsamer Teiler von A ist. Für ein Polynom $f = \sum_{i=0}^{n} f_i X^i \in R[X]$ ist $\mathrm{c}(f) := \gcd(\{f_0, f_1, \ldots, f_n\})$

der *Inhalt* von f. Wenn $f \neq 0$, so gibt es dann genau ein Polynom $\tilde{f}$ mit $f = \mathrm{c}(f) \cdot \tilde{f}$. Dieses Polynom $\tilde{f}$ heißt der *primitive Anteil von* f. Wir definieren $\tilde{0} := 1$.

LEMMA 3.13. *Sei R ein faktorieller Integritätsbereich, seien $f, g \in R[X]$ und sei $r \in R$. Dann gilt:*

(1) $\mathrm{c}(rf) \sim_R r\,\mathrm{c}(f)$.
(2) $\tilde{f}$ *ist ein primitives Polynom.*
(3) $\mathrm{c}(fg) \sim_R \mathrm{c}(f)\,\mathrm{c}(g)$.
(4) *Wenn $f \neq 0$ und $g \neq 0$, so gibt ein invertierbares $u \in R$ mit $u\,\widetilde{(fg)} = \tilde{f}\tilde{g}$.*

BEWEIS. (1) Wegen Lemma 2.6 gilt $\mathrm{c}(rf) = \gcd(\{rf_0, \ldots, rf_n\}) \sim_R r \gcd(\{f_0, \ldots, f_n\}) = r\,\mathrm{c}(f)$.

(2) Es gilt $\mathrm{c}(f) = \mathrm{c}(\mathrm{c}(f)\tilde{f}) \sim_R \mathrm{c}(f)\,\mathrm{c}(\tilde{f})$. Sei u ein invertierbares Element von R mit $\mathrm{c}(f)u = \mathrm{c}(f)\,\mathrm{c}(\tilde{f})$. Dann gilt $\mathrm{c}(f)(u - \mathrm{c}(\tilde{f})) = 0$. Wenn $\mathrm{c}(f) = 0$, dann gilt $f = 0$ und somit $\tilde{f} = 1$, somit ist $\tilde{f}$ primitiv. Wenn $\mathrm{c}(\tilde{f}) = u$, so teilt jedes prime $p \in R$, das alle Koeffizienten von $\tilde{f}$ teilt, auch u und ist somit invertierbar und damit nicht prim. Also ist $\tilde{f}$ primitiv.

(3) Es gilt $\mathrm{c}(fg) = \mathrm{c}(\mathrm{c}(f)\tilde{f}\,\mathrm{c}(g)\tilde{g}) = \mathrm{c}(\mathrm{c}(f)\,\mathrm{c}(g)\tilde{f}\tilde{g}) \sim_R \mathrm{c}(f)\,\mathrm{c}(g)\,\mathrm{c}(\tilde{f}\tilde{g})$. Wegen Lemma 3.12 ist $\tilde{f}\tilde{g}$ primitiv, also ist $\mathrm{c}(\tilde{f}\tilde{g})$ ein invertierbares Element von R, und somit gilt $\mathrm{c}(f)\,\mathrm{c}(g)\,\mathrm{c}(\tilde{f}\tilde{g}) \sim_R \mathrm{c}(f)\,\mathrm{c}(g)$.

(4) Es gilt $fg = \mathrm{c}(fg)\widetilde{(fg)}$ und $fg = \mathrm{c}(f)\,\mathrm{c}(g)\tilde{f}\tilde{g}$. Wegen (3) gibt es ein invertierbares $u \in R$ mit $\mathrm{c}(fg) = u\,\mathrm{c}(f)\,\mathrm{c}(g)$, also gilt $u\,\mathrm{c}(f)\,\mathrm{c}(g)\widetilde{(fg)} = \mathrm{c}(f)\,\mathrm{c}(g)\tilde{f}\tilde{g}$ und wegen $f, g \neq 0$ somit auch $u\,\widetilde{(fg)} = \tilde{f}\tilde{g}$. □

SATZ 3.14. *Sei R ein faktorieller Integritätsbereich, seien $f, g \in R[X]$, und sei $Q(R)$ der Quotientenkörper von R. Dann sind äquivalent:*

(1) $f \mid g$ *in* $R[X]$.
(2) $f \mid g$ *in* $Q(R)[X]$ *und* $\mathrm{c}(f) \mid \mathrm{c}(g)$.

BEWEIS. (1)⇒(2): Sei $q \in R[X]$ so, dass $g = qf$. Dann gilt $\mathrm{c}(g) = \mathrm{c}(qf) \sim_R \mathrm{c}(q)\,\mathrm{c}(f)$, also gilt $\mathrm{c}(f) \mid \mathrm{c}(g)$.

(2)⇒(1): In $Q(R)[X]$ gilt $\tilde{f} \mid f \mid g$. Sei $h \in Q(R)[X]$ so, dass $g = h\tilde{f}$, und sei $r \in R \setminus \{0\}$ so, dass $rh \in R[X]$. Dann gilt $rg = (rh)\tilde{f}$. Es gilt dann

$$\begin{aligned} \mathrm{c}(rh) &\sim_R \mathrm{c}(rh)\,\mathrm{c}(\tilde{f}) \\ &\sim_R \mathrm{c}(rh\tilde{f}) \\ &= \mathrm{c}(rg) \\ &\sim_R r\,\mathrm{c}(g), \end{aligned}$$

Also gilt $r \mid \mathrm{c}(rh)$. Also sind alle Koeffizienten von rh durch r teilbar, und somit gilt $h \in R[X]$. □

KOROLLAR 3.15. *Sei R ein ein faktorieller Integritätsbereich, und seien $f, g \in R[X]$. Wir nehmen an, dass f primitiv ist und dass $f \mid g$ in $Q(R)[X]$ gilt. Dann gilt $f \mid g$ auch in $R[X]$.*

BEWEIS. Da $\mathrm{c}(f)$ invertierbar ist, ist Bedingung (2) von Satz 3.14 erfüllt. □

LEMMA 3.16. *Sei R ein faktorieller Integritätsbereich, sei $Q(R)$ sein Quotientenkörper, und sei $f \in R[X]$. Dann sind äquivalent:*

(1) *f ist ein irreduzibles Element von $R[X]$.*
(2) *Es gibt ein irreduzibles Element $r \in R$ mit $f = rX^0$, oder f ist primitiv und f ist ein irreduzibles Element von $Q(R)[X]$.*

BEWEIS. (1)⇒(2): Sei f ein irreduzibles Element von $R[X]$. Es gilt

$$f = \mathrm{c}(f)\tilde{f},$$

daher ist einer der Faktoren $\mathrm{c}(f)$ und $\tilde{f}$ invertierbar in $R[X]$.

Im Fall, dass $\mathrm{c}(f)$ invertierbar ist, zeigen wir, dass f in $Q(R)[X]$ irreduzibel ist.

Wenn f in $Q(R)[X]$ invertierbar ist, so so gilt $\deg(f) = 0$ und daher gilt $f \sim_R \mathrm{c}(f)X^0$, und f ist damit auch in $R[X]$ invertierbar, im Widerspruch dazu, dass f irreduzibel in $R[X]$ ist.

Sei nun g ein Teiler von f in $Q(R)[X]$. Es gibt dann $a \in Q(R) \setminus \{0\}$, sodass ag primitiv ist. Dann gilt in $Q(R)[X]$, dass $ag \mid f$ und wegen der Primitivität von ag daher auch $ag \mid f$ in $R[X]$. Wenn ag invertierbar in $R[X]$ ist, so gilt $\deg(ag) = 0$ und damit $\deg(g) = 0$. Wenn ag zu f in $R[X]$ assoziiert ist, so gilt $f \mid ag$ in $R[X]$, also auch $f \mid g$ in $Q(R)[X]$, und somit sind f und g assoziiert in $Q(R)[X]$. Somit ist f irreduzibel in $Q(R)[X]$.

Im Fall, dass $\tilde{f}$ invertierbar in $R[X]$ ist, gilt wegen $f = \mathrm{c}\, f\tilde{f}$, dass f und $\mathrm{c}(f)$ in $R[X]$ assoziiert sind. in $R[X]$. Somit ist auch $\mathrm{c}(f)$ ein irreduzibles Element in $R[X]$, und damit auch irreduzibel in R.

(2)⇒(1): Wenn r ein irreduzibles Element von R ist, so ist rX^0 irreduzibel in $R[X]$. Wir nehmen nun an, dass f in $Q(R)[X]$ irreduzibel ist und $\mathrm{c}(f)$ in R invertierbar ist. Da f in $Q(R)[X]$ nicht invertierbar ist, ist f auch in $R[X]$ nicht invertierbar. Um zu zeigen, dass f irreduzibel in $R[X]$ ist, wählen wir einen Teiler g von f in $R[X]$. Es gilt dann $\mathrm{c}(g) \mid \mathrm{c}(f)$ in R, also ist $\mathrm{c}(g)$ invertierbar, und g somit primitiv. Wenn $\deg(g) = 0$, so ist g daher gleich uX^0 für ein invertierbares $u \in R$, und somit ist g invertierbar in $R[X]$. Wenn $\deg(g) = \deg(f)$, so gilt $f \mid g$ in $Q(R)[X]$ und somit wegen Satz 3.14 und

$\mathrm{c}(f) \mid \mathrm{c}(g)$ in R, auch $f \mid g$ in $R[X]$. Somit sind f und g assoziiert in $R[X]$. Also ist f irreduzibel in $R[X]$. □

SATZ 3.17. *Sei R ein faktorieller Integritätsbereich. Dann ist auch $R[X]$ faktoriell.*

BEWEIS. Wir zeigen als erstes, dass $R[X]$ die (ACC) für Hauptideale erfüllt. Sei $a_1 \in R[X] \setminus \{0\}$, und sei $(a_1) \subseteq (a_2) \subseteq \cdots$ eine Folge von Hauptidealen. Für jedes $i \in \mathbb{N}$ wählen wir $r_i \in R$ und ein primitives $b_i \in R[X]$ so, dass $a_i = r_i\, b_i$. Wegen Satz 3.14 ist dann $(r_1)_R \subseteq (r_2)_R \subseteq \cdots$ eine aufsteigende Kette von Idealen in R und $(b_1)_{Q(R)[X]} \subseteq (b_2)_{Q(R)[X]} \subseteq \cdots$ eine aufsteigende Kette von Idealen in $Q(R)[X]$. R ist faktoriell, und erfüllt daher die (ACC) für Hauptideale. Der Ring $Q(R)[X]$ ist ein Polynomring über einem Körper. Als solcher ist er ein Hauptidealbereich (jedes Ideal I wird von jedem Polynom kleinsten Grades in $I \setminus \{0\}$ erzeugt), und somit faktoriell. Es gibt also ein $N \in \mathbb{N}$, sodass für alle $k \geq N$ gilt: $(r_N)_R = (r_k)_R$ und $(b_N)_{Q(R)[X]} = (b_k)_{Q(R)[X]}$. Es gilt also $b_N \mid b_k$ in $Q(R)[X]$ und $r_N \mid r_k$ in R. Somit gilt $a_N \mid a_k$ in $R[X]$, und somit $(a_k)_{R[X]} = (a_N)_{R[X]}$.

Nun zeigen wir, dass jedes irreduzible Element in $R[X]$ prim ist. Sei dazu $f \in R[X]$ irreduzibel, und seien $a, b \in R[X] \setminus \{0\}$ so, dass $f \mid a \cdot b$. Wir wollen nun zeigen, dass f in $R[X]$ entweder a oder b teilt. Wir unterscheiden zwei Fälle nach Lemma 3.16.

Wenn $f = rX^0$ mit einem irreduziblen $r \in R$ ist, so gilt $r = \mathrm{c}(f) \mid \mathrm{c}(a)\,\mathrm{c}(b)$. Da R faktoriell ist, ist r prim in R, und somit gilt $r \mid \mathrm{c}(a)$ oder $r \mid \mathrm{c}(b)$, und folglich $rX^0 \mid a$ oder $rX^0 \mid b$.

Im anderen Fall ist f wegen Lemma 3.16 primitiv und irreduzibel in $Q(R)[X]$. Der Ring $Q(R)[X]$ ist ein Polynomring über einem Körper, folglich euklidisch, daher ein Hauptidealbereich und somit faktoriell. Also ist f prim in $Q(R)[X]$ und es gilt daher $f \mid a$ oder $f \mid b$ in $Q(R)[X]$. Wegen Korollar 3.15 gilt dann $f \mid a$ oder $f \mid b$ in $R[X]$.

Also ist f prim in in $R[X]$. □

KOROLLAR 3.18. *Sei R ein faktorieller Integritätsbereich und $k \in \mathbb{N}$. Dann ist $R[X_1, \ldots, X_k]$ faktoriell.*

4. Größte gemeinsame Teiler im Polynomring

SATZ 3.19. *Sei R ein faktorieller Integritätsbereich, und seien $f_1, \ldots, f_n \in R[X] \setminus \{0\}$. Es sei d_1 ein größter gemeinsamer Teiler von $\mathrm{c}(f_1), \ldots, \mathrm{c}(f_n)$ in R, und d_2 ein größter gemeinsamer Teiler von $f_1, \ldots, f_n$ in $Q(R)[X]$. Wir nehmen an, dass d_2 primitiv in $R[X]$ ist. Dann ist $d_1 d_2$ ein größter gemeinsamer Teiler von $f_1, \ldots, f_n$ in $R[X]$.*

BEWEIS. Wir zeigen zunächst, dass $d_1 d_2$ alle f_i teilt. Sei $i \in \{1, \ldots, n\}$. Da $d_1 \mid \mathrm{c}(f_i)$ in R und $d_2 \mid f_i$ in $Q(R)[X]$, liefert Satz 3.14 auch $d_1 d_2 \mid f_i$ in $R[X]$.

Sei nun $d' \in R[X]$ so, dass d' in $R[X]$ alle f_i teilt. Dann gilt wegen Satz 3.14, dass $\mathrm{c}(d')$ alle $\mathrm{c}(f_i)$ in R teilt, und dass $\tilde{d'}$ alle f_i in $Q(R)[X]$ teilt. Da d_1 ein größter gemeinsamer Teiler in R ist, gilt $\mathrm{c}(d') \mid d_1$ in R. Da d_2 ein größter gemeinsamer Teiler in $Q(R)[X]$ ist, gilt $\tilde{d'} \mid d_2$ in $Q(R)[X]$. Außerdem gilt $d_1 \mid \mathrm{c}(d_1 d_2)$. Wegen Satz 3.14 gilt daher $d' \mid d_1 d_2$ in $R[X]$. □

Übungsaufgaben 3.20.

(1) (Größter gemeinsamer Teiler) Seien $f, g \in \mathbb{Q}[X, Y]$ gegeben durch

$$\begin{aligned} f &= XY^2 + X^2Y^3 \\ g &= Y + XY + XY^2 + X^2Y^2. \end{aligned}$$

   (a) Bestimmen Sie einen größten gemeinsamen Teiler von f und g in $\mathbb{Q}(X)[Y]$.
   (b) Bestimmen Sie einen größten gemeinsamen Teiler von f und g in $\mathbb{Q}(Y)[X]$.
   (c) Bestimmen Sie einen größten gemeinsamen Teiler von f und g in $\mathbb{Q}[X, Y]$.
   (d) Bestimmen Sie einen größten gemeinsamen Teiler von f und g in $\mathbb{Q}(X, Y)$.

   Dabei ist $\mathbb{Q}(X)$ der Quotientenkörper von $\mathbb{Q}[X]$.

(2) (Größter gemeinsamer Teiler) Seien $f, g \in \mathbb{Q}[X, Y]$ gegeben durch

$$\begin{aligned} f &= XY + X^3Y + X^2Y^2 + XY^3 \\ g &= X + X^3 + Y + 2X^2Y + 2XY^2 + Y^3 \end{aligned}$$

   (a) Bestimmen Sie einen größten gemeinsamen Teiler von f und g in $\mathbb{Q}(X)[Y]$.
   (b) Bestimmen Sie einen größten gemeinsamen Teiler von f und g in $\mathbb{Q}(Y)[X]$.
   (c) Bestimmen Sie einen größten gemeinsamen Teiler von f und g in $\mathbb{Q}[X, Y]$.
   (d) Bestimmen Sie einen größten gemeinsamen Teiler von f und g in $\mathbb{Q}(X, Y)$.

(3) (Größter gemeinsamer Teiler) Berechnen Sie größte gemeinsame Teiler von $f = 3220 + 5520X + 2300X^2 + 460X^3 + 460X^4$ und $g = -230 - 230X + 46X^3 + 46X^4$ in $\mathbb{Z}[X]$ und $\mathbb{Q}[X]$.

KAPITEL 4

Restklassenringe

1. Restklassenringe von $\mathbb{Z}$

DEFINITION 4.1 ($\mathbb{Z}_n$). Sei $\mathbb{Z}$ der Ring der ganzen Zahlen, sei $n \in \mathbb{N}$, und sei (n) das von n erzeugte Hauptideal von $\mathbb{Z}$. Dann bezeichnen wir den Ring $\mathbb{Z}/(n)$ als den *Ring der ganzen Zahlen modulo* n, und kürzen ihn mit $\mathbb{Z}_n$ ab.

Wir bezeichnen das Element $x + (n)$ auch mit $[x]_n$; $\mathbb{Z}_n$ hat genau die n Elemente $[0]_n, [1]_n, \ldots, [n-1]_n$. Wir schreiben $a \equiv_n b$ oder $a \equiv b \pmod{n}$, wenn $n \mid a - b$.

SATZ 4.2 (Invertierbarkeit). *Sei $n \in \mathbb{N}$ und $a \in \mathbb{Z}$. Dann ist $[a]_n$ genau dann invertierbar in $\mathbb{Z}_n$, wenn $\gcd(a, n) = 1$.*

BEWEIS. Wenn $\gcd(a, n) = 1$, so gibt es nach dem Euklidischen Algorithmus u und v in $\mathbb{Z}$, sodass $ua + vn = 1$. Dann gilt $[u]_n[a]_n = [1]_n$. Wenn $[a]_n$ invertierbar ist, dann gibt es ein $x \in \mathbb{Z}$ mit $[x]_n[a]_n = [1]_n$, also $n \mid xa - 1$. Dann gilt auch $\gcd(a, n) \mid xa - 1$ und wegen $\gcd(a, n) \mid xa$ auch $\gcd(a, n) \mid 1$, also $\gcd(a, n) = 1$. □

Da in jedem kommutativen Ring mit Eins das Produkt invertierbarer Elemente wieder invertierbar ist, erhalten wir:

LEMMA 4.3. *Seien a, b invertierbare Elemente aus $\mathbb{Z}_n$. Dann ist auch $a \cdot b$ invertierbar.*

DEFINITION 4.4 (Euler'sche φ−Funktion). Sei $n \in \mathbb{N}$. Wir definieren $\varphi(1) := 1$ und, wenn $n > 1$,

$$\varphi(n) := |\{a \in \mathbb{Z}_n \,:\, a \text{ invertierbar}\}| = |\{x \in \{1, 2, \ldots, n-1\} \,:\, \gcd(x, n) = 1\}|.$$

Beispiele: $\varphi(12) = |\{1, 5, 7, 11\}| = 4$ und $\varphi(8) = |\{1, 3, 5, 7\}| = 4$.

SATZ 4.5 (Satz von Euler). *Sei $n \in \mathbb{N}$, $n > 1$, $a \in \mathbb{Z}$, $\gcd(a, n) = 1$. Dann gilt:*

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

So gilt etwa $7^{\varphi(12)} = 7^4 \equiv_{12} 1$ und $3^{\varphi(5)} = 3^4 \equiv_5 1$.

BEWEIS. Beweis von Satz 4.5: Seien $n \in \mathbb{N}$ und $a \in \mathbb{Z}$. Wir nehmen an, dass $\gcd(a, n) = 1$. Sei

$$I := \{x \in \mathbb{Z}_n \mid x \text{ ist invertierbar}\}.$$

Wir wissen bereits, dass $|I| = \varphi(n)$. Wir definieren

$$\begin{array}{rccc} f & : & I & \longrightarrow & I \\ & & x & \longmapsto & x \cdot [a]_n \end{array}$$

und zeigen, dass f injektiv ist. Dazu fixieren wir $x, y \in I$ mit $f(x) = f(y)$. Das heißt: $x \cdot [a]_n = y \cdot [a]_n$. Da $\gcd(a, n) = 1$, gibt es $b \in \mathbb{Z}$ mit $[a]_n \cdot [b]_n = [1]_n$. Wir erhalten also $x \cdot [a]_n \cdot [b]_n = y \cdot [a]_n \cdot [b]_n$ und damit $x = y$. Daher ist f injektiv. Die Funktion f ist folglich eine bijektive Abbildung von I nach I. Es gilt also:

$$\prod_{x \in I} x = \prod_{x \in I} f(x) = \prod_{x \in I} (x \cdot [a]_n) = \left(\prod_{x \in I} x \right) \cdot ([a]_n)^{\varphi(n)}.$$

Sei $y \in \mathbb{Z}_n$ das Inverse zu $\prod_{x \in I} x$. Dann gilt:

$$y \cdot \prod_{x \in I} x = y \cdot \left(\prod_{x \in I} x \right) \cdot ([a]_n)^{\varphi(n)},$$

und somit $[1]_n = ([a]_n)^{\varphi(n)}$ und folglich $1 \equiv a^{\varphi(n)} \pmod{n}$. □

KOROLLAR 4.6. *Sei p eine Primzahl, und sei $z \in \mathbb{Z}$. Dann gilt*

$$z^p \equiv z \pmod{p}.$$

Falls p kein Teiler von z ist, gilt

$$z^{p-1} \equiv 1 \pmod{p}.$$

BEWEIS. Wir wählen eine Primzahl p und $z \in \mathbb{Z}$ und nehmen an, dass p die Zahl z nicht teilt. Wir wissen, dass $\varphi(p) = p - 1$, und daher gilt nach dem Satz von Euler

$$z^{p-1} \equiv 1 \pmod{p}.$$

Da $p \mid (z^{p-1} - 1)$, gilt auch $p \mid (z^p - z)$, und somit $z^p \equiv z \pmod{p}$.

Wenn $p \mid z$, dann teilt p sowohl z als auch z^p. □

ÜBUNGSAUFGABEN 4.7.

(1) ([**RU87**]) Zeigen Sie, dass für jede natürliche Zahl n die Zahl $n^5 - n$ ein Vielfaches von 30 ist.
(2) Zeigen Sie, dass für alle $a, b \in \mathbb{Z}_p$ gilt:

$$(a + b)^p = a^p + b^p.$$

(3) Seien m, n natürliche Zahlen. Wann ist $2^m - 1$ ein Teiler von $2^n - 1$?

2. Das RSA-Verfahren

SATZ 4.8. *Seien p, q Primzahlen, $p \neq q$ und seien $a \in \mathbb{Z}$, $s \in \mathbb{N}_0$. Dann gilt:*

$$a^{1+s(p-1)(q-1)} \equiv a \pmod{pq}.$$

Beweis:

- *1. Fall:* $\gcd(a, pq) = 1$*:* Wir wissen, dass $a^{p-1} \equiv 1 \pmod{p}$ gilt (Satz von Euler), daher gilt auch $(a^{p-1})^{(q-1)\cdot s} \equiv 1 \pmod{p}$. Somit ist p ein Teiler von $a^{(p-1)\cdot(q-1)\cdot s} - 1$ und damit auch von $a^{(p-1)\cdot(q-1)\cdot s+1} - a$. Ebenso zeigen wir

  $$q \mid a^{(p-1)\cdot(q-1)\cdot s+1} - a.$$

  Damit gilt insgesamt:

  $$pq \mid a^{(p-1)\cdot(q-1)\cdot s+1} - a.$$

- *2. Fall:* $\gcd(a, pq) = p$*:* Da der $\gcd(a, q) = 1$ ist, gilt mit dem Satz von Euler $a^{q-1} \equiv 1 \pmod{q}$, und somit $a^{(q-1)\cdot(p-1)} \equiv 1 \pmod{q}$. Das heißt

  $$q \mid a^{(q-1)\cdot(p-1)\cdot s} - 1.$$

  Wir wissen, dass $p \mid a$. Daher gilt $pq \mid \left(a^{(q-1)\cdot(p-1)\cdot s} - 1\right) \cdot a$.
- *3. Fall:* $\gcd(a, pq) = q$*:* Beweis genauso wie im 2. Fall.
- *4. Fall:* $\gcd(a, pq) = pq$*:* Dann ist zu zeigen, dass $0 \equiv 0 \pmod{pq}$. □

Beim RSA-Verschlüsselungsverfahren wählt der Systementwerfer zwei Primzahlen p, q, sodass $n = p\,q$ nicht in verfügbarer Zeit faktoriserbar ist, berechnet $\phi := (p-1)(q-1)$, wählt für e eine beliebige Zahl mit $1 < e < \phi$ und $\gcd(e, \phi) = 1$, und berechnet d so, dass $d\,e \equiv 1 \pmod{\phi}$.

Der öffentliche Schlüssel ist (n, e), der private Schlüssel (n, d). Die Verschlüsselungsfunktion ist gegeben durch $E : \mathbb{Z}_n \to \mathbb{Z}_n$, $E(m) := m^e$, die Entschlüsselungsfunktion durch $D : \mathbb{Z}_n \to \mathbb{Z}_n$, $D(c) := c^d$.

ÜBUNGSAUFGABEN 4.9.

(1) Sei $n = p_1 \cdot p_2 \cdot \cdots \cdot p_k$, wobei die p_i lauter verschiedene Primzahlen sind, und sei $s \in \mathbb{N}$. Zeigen Sie, dass für alle $a \in \mathbb{Z}$ gilt:

$$a^{1+s\cdot\prod_{i=1}^{k}(p_i-1)} \equiv a \pmod{n}.$$

(2) Für das RSA-Verfahren wählen wir $p = 5, q = 11$ und $k = 13$. Chiffrieren Sie $(01, 22, 03, 08)$ und dechiffrieren Sie das Ergebnis!

(3) Frau Huber sendet Herrn Müller mit dem RSA-Verfahren die Nachricht PMOXY. Herr Müller weiß, dass Frau Huber das RSA-Verfahren mit $(n = 35, k = 5)$ verwendet hat (A=0, Z=25). Entschlüsseln Sie die Nachricht! (*Bemerkung:* Warum ist es überhaupt ungünstig, einzelne Buchstaben zu verschlüsseln?)

(4) (Mathematica) Entschlüsseln Sie (verbotenerweise) die Nachricht $(2, 3, 5, 7, 11, 13)$, die mit $k = 13$ und $pq = 1334323339$ verschlüsselt wurde.
(5) (Mathematica) [**LP98**, p. 265] In einem RSA-System ist $n = pq = 32954765761773295963$ und $k = 1031$. Bestimmen Sie t, und entschlüsseln Sie die Nachricht

$$899150261120482115$$

(A = 0, Z = 25).
(6) Sei n eine ungerade Primzahl, und seien $r, s \in \mathbb{N}$ so, dass $n - 1 = 2^s \cdot r$ und r ungerade ist. Sei a eine ganze Zahl, die kein Vielfaches von n ist. Zeigen Sie, dass dann $a^r \equiv 1 \pmod{n}$ gilt, oder dass es ein $j \in \{0, 1, \ldots, s-1\}$ mit $a^{2^j \cdot r} \equiv -1 \pmod{n}$ gibt. *Hinweis:* Dieser Satz ist die Basis für den *Rabin-Miller Test*, um nachzuprüfen, ob eine Zahl eine Primzahl ist.

3. Die Multiplikativität der Eulerschen φ-Funktion

Satz 4.10 (Multiplikativität der φ-Funktion). *Seien $n, m \in \mathbb{N}$. Wenn $\gcd(n, m) = 1$, dann gilt $\varphi(nm) = \varphi(n) \cdot \varphi(m)$.*

Wir benutzen im Beweis das direkte Produkt von Ringen:

Satz und Definition 4.11. *Seien R_1 und R_2 Ringe mit Eins. Wir definieren auf der Menge $R_1 \times R_2$ Operationen durch*

$$\$ \binom{r_1}{r_2} +_{R_1 \times R_2} \binom{s_1}{s_2} := \binom{r_1 +_{R_1} s_1}{r_2 +_{R_2} s_2}, \quad \binom{r_1}{r_2} \cdot_{R_1 \times R_2} \binom{s_1}{s_2} := \binom{r_1 \cdot_{R_1} s_1}{r_2 \cdot_{R_2} s_2}, \quad -_{R_1 \times R_2} \binom{r_1}{r_2} := \binom{-_{R_1} r_1}{-_{R_2} r_2}.$$

Dann ist $(R_1 \times R_2, +_{R_1 \times R_2}, -_{R_1 \times R_2}, \cdot_{R_1 \times R_2}, \binom{0_{R_1}}{0_{R_2}}, \binom{1_{R_1}}{1_{R_2}})$ ein Ring mit Eins. Er ist das direkte Produkt von R_1 und R_2.

In $\mathbb{Z}_4 \times \mathbb{Z}_5$ rechnet man zum Beispiel $\binom{[3]_4}{[4]_5} \cdot \binom{[2]_4}{[3]_5} = \binom{[2]_4}{[2]_5}$.

Satz 4.12. *Seien $n, m \in \mathbb{N}$ mit $\gcd(n, m) = 1$. Dann ist die Abbildung*

$$\begin{array}{rccc} \psi & : & \mathbb{Z}_{nm} & \longrightarrow & \mathbb{Z}_n \times \mathbb{Z}_m \\ & & [x]_{nm} & \longmapsto & ([x]_n, [x]_m) \end{array}$$

ein Isomorphismus dieser Ringe mit Eins.

Beweis. Wir zeigen als erstes, dass ψ wohldefiniert ist. Dazu zeigen wir, dass für alle $y, z \in \mathbb{Z}$ mit $[y]_{nm} = [z]_{nm}$ auch die Gleichheiten $[y]_n = [z]_n$ und $[y]_m = [z]_m$ gelten. Seien dazu $y, z \in \mathbb{Z}$ mit $[y]_{nm} = [z]_{nm}$. Dann gilt $nm \mid y - z$, also $n \mid y - z$ und $m \mid y - z$ und somit $[y]_n = [z]_n$ und $[y]_m = [z]_m$.

Wir zeigen nun, dass ψ ein Homomorphismus ist und überprüfen dazu die Homomorphismuseigenschaft für $+$. Es gilt

$$\begin{aligned}\psi\left([x]_{nm}+[y]_{nm}\right) &= \psi\left([x+y]_{nm}\right)\\ &= \left([x+y]_n, [x+y]_m\right)\\ &= \left([x]_n+[y]_n, [x]_m+[y]_m\right)\\ &= \begin{pmatrix}[x]_n\\ [x]_m\end{pmatrix}+\begin{pmatrix}[y]_n\\ [y]_m\end{pmatrix}\\ &= \psi\left([x]_{nm}\right)+\psi\left([y]_{nm}\right).\end{aligned}$$

Die Homomorphismuseigenschaft für $\cdot$ zeigt man genau so.

Als nächstes zeigen wir, dass ψ bijektiv und damit ein Isomorphismus ist. Da beide Mengen endlich und gleich groß sind, reicht es, zu zeigen, dass ψ injektiv ist. Wir nehmen also $\psi\left([x]_{nm}\right)=\psi\left([y]_{nm}\right)$ an. Dann gilt $\left([x]_n, [x]_m\right)=\left([y]_n, [y]_m\right)$, und somit $n \mid x-y$ und $m \mid x-y$. Da $\gcd(n,m)=1$, gilt dann $nm \mid x-y$, und folglich $[x]_{nm}=[y]_{nm}$. Die Abbildung ψ ist also injektiv, somit surjektiv und damit bijektiv. □

Beweis von Satz 4.10. Seien $n, m \in \mathbb{N}$ so, dass $\gcd(n,m)=1$. Wir berechnen als erstes die Anzahl der invertierbaren Elemente von $\mathbb{Z}_n \times \mathbb{Z}_m$: Wir zeigen, dass $\binom{a}{b} \in \mathbb{Z}_n \times \mathbb{Z}_m$ genau dann invertierbar ist, wenn a invertierbar in $\mathbb{Z}_n$ und b invertierbar in $\mathbb{Z}_m$ ist. Dazu fixieren wir zunächst $\binom{a}{b} \in \mathbb{Z}_n \times \mathbb{Z}_m$ und nehmen an, dass $\binom{a}{b}$ invertierbar ist; es gibt also $\binom{c}{d} \in \mathbb{Z}_n \times \mathbb{Z}_m$, sodass $\binom{a}{b} \cdot \binom{c}{d} = 1_{\mathbb{Z}_n \times \mathbb{Z}_m} = \binom{[1]_n}{[1]_m}$. Daher ist a in $\mathbb{Z}_n$ invertierbar (mit Inversem c), ebenso b in $\mathbb{Z}_m$ (mit Inversem d). Nun fixieren wir $a \in \mathbb{Z}_n$, $b \in \mathbb{Z}_m$, beide invertierbar. Falls $ac=[1]_n$, und $bd=[1]_m$, dann ist $\binom{c}{d}$ das Inverse zu $\binom{a}{b}$. In $\mathbb{Z}_n$ gibt es $\varphi(n)$ invertierbare Elemente, in $\mathbb{Z}_m$ gibt es $\varphi(m)$ invertierbare Elemente, und somit gibt es in $\mathbb{Z}_n \times \mathbb{Z}_m$ genau $\varphi(n) \cdot \varphi(m)$ invertierbare Elemente.

Wir bestimmen nun die Anzahl der invertierbaren Elemente in $\mathbb{Z}_{nm}$: Der Ring $\mathbb{Z}_{nm}$ besitzt nach der Definition von φ genau $\varphi(nm)$ invertierbare Elemente.

Wegen Satz 4.12 sind die Ringe $\mathbb{Z}_{nm}$ und $\mathbb{Z}_n \times \mathbb{Z}_m$ isomorph und besitzen somit gleich viele invertierbare Elemente. Somit gilt $\varphi(nm)=\varphi(n)\cdot\varphi(m)$. □

Aus der Primfaktorzerlegung von $n=\prod_{i\in A} p_i^{\alpha_i}$ mit $\alpha_i \geq 1$ für alle $i \in A$ und aus $\varphi(p^\alpha)=p^\alpha-p^{\alpha-1}$ für Primzahlen p und $\alpha>0$ kann man jetzt leicht $\varphi(n)$ durch

$$\begin{aligned}\varphi(n) &= \varphi\left(\textstyle\prod_{i\in A} p_i^{\alpha_i}\right)\\ &= \textstyle\prod_{i\in A} \varphi\left(p_i^{\alpha_i}\right)\\ &= \textstyle\prod_{i\in A} p_i^{\alpha_i}\left(1-\frac{1}{p_i}\right)\\ &= \textstyle\prod_{i\in A} p_i^{\alpha_i} \cdot \prod_{i\in A}\left(1-\frac{1}{p_i}\right)\\ &= n \cdot \textstyle\prod_{i\in A}\left(1-\frac{1}{p_i}\right)\end{aligned}$$

berechnen.

BEISPIEL 4.13. $\varphi(12) = 12 \cdot \left(1 - \frac{1}{2}\right) \cdot \left(1 - \frac{1}{3}\right) = 4 = 2 \cdot 2 = \varphi(3) \cdot \varphi(4)$.

4. Zerlegungen

LEMMA 4.14. *Sei R ein Ring, und seien A, B Ideale von R. Dann ist $A + B := \{a + b \mid a \in A, b \in B\}$ ein Ideal von R.*

SATZ 4.15. *Sei R ein Ring, und seien A, B Ideale von R mit $A + B = R$. Dann sind die Ringe $R/(A \cap B)$ und $R/A \times R/B$ isomorph.*

BEWEIS. Sei $h : R \to R/A \times R/B$, $h(r) := (r + A, r + B)$. Dann gilt $\ker(h) = A \cap B$. Wir zeigen nun, dass h surjektiv ist. Seien dazu $r, s \in R$. Wegen $A + B = R$ gibt es $a \in A$ und $b \in B$ mit $a + b = r - s$. Also gilt $s + b = r - a$ und somit gilt $h(r - a) = (r + a + A, s + b + B) = (r + A, s + B)$. Wegen des Homomorphiesatzes sind $R/\ker(h)$ und $h(R)$ isomorph. □

Der *Chinesische Restsatz* (Satz 4.17) bestimmt die Lösbarkeit bestimmter Systeme von Kongruenzen. Dazu brauchen wir zunächst einen Zusammenhang zwischen gcd, lcm und der Summe und dem Durchschnitt von Hauptidealen.

SATZ 4.16. *Sei R ein Hauptidealbereich, und seien $a, b \in R$.*

(1) $(a) + (b) = (\gcd(a, b))$.
(2) $(a) \cap (b) = (\mathrm{lcm}(a, b))$.
(3) $(a) + ((b) \cap (c)) = ((a) + (b)) \cap ((a) + (c))$.

BEWEIS. (1) Sei d ein Erzeuger von $(a) + (b)$. Dann gilt $a \in (d)$ und $b \in (d)$, also $d \mid a$ und $d \mid b$. Sei d' ein weiterer Teiler von a und b. Dann gilt $(a) \subseteq (d')$ und $(b) \subseteq (d')$, also $(a) + (b) \subseteq (d')$ und somit $(d) \subseteq (d')$. Folglich gilt $d \in (d')$, also $d' \mid d$. Daher ist d ein größter gemeinsamer Teiler von $\{a, b\}$. Da $\gcd(a, b)$ auch ein größter gemeinsamer Teiler von $\{a, b\}$ ist, sind d und $\gcd(a, b)$ assoziiert in R und erzeugen daher das gleiche Ideal. Somit gilt $(d) = (\gcd(a, b))$.

(2) Sei v ein Erzeuger von $(a) \cap (b)$. Dann gilt $v \in (a)$ und $v \in (b)$, also $a \mid v$ und $b \mid v$. Sei v' ein weiteres gemeinsames Vielfaches von $\{a, b\}$. Dann gilt $v' \in (a) \cap (b)$, also $v' \in (a) \cap (b)$. Somit gilt $v' \in (v)$, also $v \mid v'$. Daher ist v ein kleinstes gemeinsames Vielfaches von $\{a, b\}$. Da alle kleinsten gemeinsamen Vielfachen zueinander assoziiert sind und daher das gleiche Ideal erzeugen, gilt $(v) = (\mathrm{lcm}(a, b))$.

(3) Sei I eine Auswahl irreduzibler Elemente von R und sei $a = \prod_{i\in I} i^{\alpha(i)}$, $b = \prod_{i\in I} i^{\beta(i)}$, $c = \prod_{i\in I} i^{\gamma(i)}$. Dann gilt

$$\begin{aligned}
(a) + ((b) \cap (c)) &= (a) + (\operatorname{lcm}(b,c)) \\
&= (a) + (\prod_{i\in I} i^{\max(\beta(i),\gamma(i))}) \\
&= (\gcd(a, \prod_{i\in I} i^{\max(\beta(i),\gamma(i))})) \\
&= (\gcd(\prod_{i\in I} i^{\alpha(i)}, \prod_{i\in I} i^{\max(\beta(i),\gamma(i))})) \\
&= (\prod_{i\in I} i^{\min(\alpha(i),\, \max(\beta(i),\gamma(i)))}) \\
&= (\prod_{i\in I} i^{\max(\min(\alpha(i),\beta(i)),\, \min(\alpha(i),\gamma(i)))} \\
&= (\operatorname{lcm}(\prod_{i\in I} i^{\min(\alpha(i),\beta(i))}, \prod_{i\in I} i^{\min(\alpha(i),\gamma(i))})) \\
&= (\prod_{i\in I} i^{\min(\alpha(i),\beta(i))}) \cap (\prod_{i\in I} i^{\min(\alpha(i),\gamma(i))}) \\
&= (\gcd(a,b)) \cap (\gcd(a,c)) \\
&= ((a) + (b)) \cap ((a) + (c)).
\end{aligned}$$

□

Für $n \in \mathbb{N}_0$ ist $\underline{n} := \{1, 2, \ldots, n\}$. In einem Ring R schreiben wir $x \equiv y \pmod{m}$, wenn $x - y$ in dem von m erzeugten Hauptideal liegt.

Satz 4.17 (Chinesischer Restsatz). *Sei R ein Hauptidealbereich, sei $n \in \mathbb{N}$, und seien $a_1, \ldots, a_n, m_1, \ldots, m_n \in R$. Dann sind äquivalent:*

(1) *Es gibt $x \in R$ mit $x \equiv a_i \pmod{m_i}$ für alle $i \in \underline{n}$.*
(2) *Für alle $i, j \in \underline{n}$ liegt $a_i - a_j$ im Ideal $(m_i) + (m_j)$.*

Beweis. (1)⇒(2): Es gilt $a_j - a_j = (a_i - x) + (x - a_j) \in (m_i) + (m_j)$. (2)⇒(1): Induktion nach n. Wenn $n = 1$, so leistet $x := a_1$ das Gewünschte. Sei nun $n \geq 2$. Nach Induktionsvoraussetzung gibt es ein x_0 mit $x_0 \equiv a_i \pmod{m_i}$ für $i \in \underline{n-1}$. Für $i \in \underline{n-1}$ gilt $x_0 \equiv_{(m_i)} a_i \equiv_{(m_i)+(m_n)} a_n$, also $x_0 - a_n \in (m_i) + (m_n)$. Somit gilt

$$x_0 - a_n \in \bigcap_{i\in\underline{n-1}} \big((m_i) + (m_n)\big).$$

Wegen Satz 4.16 gilt daher auch

$$x_0 - a_n \in \big(\bigcap_{i\in\underline{n-1}} (m_i)\big) + (m_n).$$

Seien $y \in \bigcap_{i \in \underline{n-1}}(m_i)$ und $z \in (m_n)$ so, dass $x_0 - a_n = y + z$. Dann gilt $x_0 - y = a_n + z$, und somit erfüllt $x := a_n + z$ die Bedingung $x \equiv a_i \pmod{m_i}$ für alle $i \in \underline{n}$. □

Algorithmisch kann man Systeme von Kongruenzen über einem Euklidischen Bereich R mit linearer Algebra über R, also mit der Hermite-Normalform lösen.

KAPITEL 5

Übersicht über einige Klassen von Ringen

Wir fassen die wichtigsten Eigenschaften von Integritätsbereichen zusammen.

SATZ 5.1. *Sei R ein Integritätsbereich. Dann gilt:*

(1) *R ist Körper $\Rightarrow$ R ist ein Euklidischer Bereich.*
(2) *R ist ein Euklidischer Bereich $\Rightarrow$ R ist ein Hauptidealbereich.*
(3) *R ist ein Hauptidealbereich $\Rightarrow$ R ist faktoriell.*

BEWEIS. (1) Wir setzen $\delta(x) = 1$ für alle $x \in R \setminus \{0\}$.

(2) Satz 2.14.

(3) Satz 3.10. □

Übersicht über einige Klassen von Ringen:

Kommutative Ringe mit Eins:
Es gilt: Produkt primitiver Polynome ist primitiv (Lemma 3.12). Faktorringe modulo maximalen Idealen sind Körper.

Beispiele für kommutative Ringe mit Eins, die keine Integritätsbereiche sind: $\mathbb{Z}_n$ für $n \notin \{0\} \cup \mathbb{P} \cup \{-p \mid p \in \mathbb{P}\}$, $\mathbb{Q}[X_1, \ldots, X_n]/(f)$, wenn f nicht 0 und nicht irreduzibel ist.

Integritätsbereiche:
Es gilt: prime Elemente $\neq 0$ sind irreduzibel; $a \mid b$ und $b \mid a$ impliziert, dass a und b assoziiert sind.

Beispiele für Integritätsbereiche, die nicht faktoriell sind: $\mathbb{Z}[\sqrt{-5}] = \{a + b\sqrt{5}i \mid a, b, \in \mathbb{Z}\} \cong \mathbb{Z}[X]/(X^2 + 5) \cong \{\begin{pmatrix} a & -\sqrt{5}b \\ \sqrt{5}b & a \end{pmatrix} \mid a, b \in \mathbb{Z}\}$. Da $X^2 + 5$ irreduzibel und somit prim ist, ist dieser Ring ein Integritätbereich. Wegen $\det(AB) = \det(A)\det(B)$ gilt für jedes invertierbare Element $\det(\begin{pmatrix} a & -\sqrt{5}b \\ \sqrt{5}b & a \end{pmatrix}) \in \{-1, +1\}$, also $a^2 + 5b^2 = 1$, und somit $a \in \{-1, +1\}$ und $b = 0$. Die Elemente $2, 3, 1 + \sqrt{5}i, 1 - \sqrt{5}i$ sind alle irreduzibel, nicht assoziiert, und es gilt $2 \cdot 3 = (1 + \sqrt{5}i)(1 - \sqrt{5}i)$.

Faktorielle Integritätsbereiche:
Es gilt: irreduzible Elemente sind prim, (ACC) für Hauptideale, gcd's und lcm's existieren immer.

Beispiele für faktorielle Integritätsbereiche, die keine Hauptidealbereiche sind: $\mathbb{Z}[X]$, $\mathbb{Q}[X_1, \ldots, X_n]$ für $n \geq 2$.

Hauptidealbereiche:
Es gilt: (ACC) für Ideale, Idealverband ist distributiv, also $I+(J\cap K) = (I+J)\cap(I+K)$ und $I \cap (J + K) = (I \cap J) + (I \cap K)$ für alle Ideale I, J, K, Chinesischer Restsatz (Satz 4.17), $\gcd(A)$ ist in der Form $\sum_{i=1}^{n} r_i a_i$ mit $n \in \mathbb{N}_0$, $a_1, \ldots, a_n \in A$ und $r_1, \ldots, r_n \in R$ darstellbar.

Beispiel für einen Hauptidealbereich, der nicht Euklidisch ist: $\mathbb{Z}[\frac{1+\sqrt{19}i}{2}]$ (J. C. Wilson, 1973).

Euklidische Bereiche:
Es gilt: gcd's können mit dem Euklidischen Algorithmus ausgerechnet werden.

Beispiele für Euklidische Bereiche, die keine Körper sind: $\mathbb{Z}, \mathbb{Z}[i], \mathbb{Q}[X], \mathbb{Q}[[X]]$.

Körper:
Es gilt: Für einen Körper K ist der Polynomring $K[X]$ euklidisch, K ist einfach.

Beispiele: $\mathbb{Q}$, $\mathbb{Z}_p$ für p prim, $D/(r)$ für einen Hauptidealbereich D und ein irreduzibles Element r, also etwa $\mathbb{Q}[X]/(X^2 - 2)$, R/M für einen kommutativen Ring mit Eins R und ein maximales Ideal M, Quotientenkörper eines Integritätsbereiches.

Teil 2

Gruppen

KAPITEL 6

Gruppen, Untergruppen, Homomorphismen

1. Definition von Gruppen

DEFINITION 6.1. $(G, \cdot, i, \mathsf{e})$ ist eine *Gruppe*, wenn G eine nichtleere Menge, $\cdot$ eine zweistellige Operation auf G, i eine einstellige Operation auf G, und e ein Element von G ist, und für alle $x, y, z \in G$ gilt:

(1) $(x \cdot y) \cdot z = x \cdot (y \cdot z)$;
(2) $\mathsf{e} \cdot x = x$;
(3) $i(x) \cdot x = \mathsf{e}$.

BEISPIEL 6.2. Sei X eine Menge, und sei $S_X := \{f : X \to X \mid f \text{ ist bijektiv}\}$. Für $f_1, f_2 \in S_X$ definieren wir $f_1 \circ f_2$ durch $f_1 \circ f_2(x) = f_1(f_2(x))$ für alle $x \in X$, und $i(f_1)$ als die zu f_1 inverse Funktion f_1^{-1}. Wir bezeichnen die identische Funktion auf X als id_X. Dann ist $(S_X, \circ, i, \mathrm{id}_X)$ eine Gruppe, die *symmetrische Gruppe* auf X. Für $X = \{1, 2, \ldots, n\}$ bezeichnen wir S_X auch als S_n.

SATZ 6.3. *Sei $(G, \cdot, i, \mathsf{e})$ eine Gruppe. Dann gilt:*

(1) *Für alle $z \in G$: $z \cdot \mathsf{e} = z$;*
(2) *Für alle $z \in G$: $i(i(z)) = z$;*
(3) *Für alle $z \in G$: $z \cdot i(z) = \mathsf{e}$.*

Beweis: Wir zeigen zunächst (1), und wählen dazu $z \in G$. Es gilt

$$\begin{aligned} z \cdot \mathsf{e} &= \mathsf{e} \cdot (z \cdot \mathsf{e}) \\ &= (\mathsf{e} \cdot z) \cdot \mathsf{e} \\ &= ((i(i(z)) \cdot i(z)) \cdot z) \cdot \mathsf{e} \\ &= ((i(i(z)) \cdot i(z)) \cdot z) \cdot (i(z) \cdot z) \\ &= (i(i(z)) \cdot (i(z) \cdot z)) \cdot (i(z) \cdot z) \\ &= (i(i(z)) \cdot \mathsf{e}) \cdot (i(z) \cdot z) \\ &= i(i(z)) \cdot (\mathsf{e} \cdot (i(z) \cdot z)) \\ &= i(i(z)) \cdot (i(z) \cdot z) \\ &= (i(i(z)) \cdot i(z)) \cdot z \\ &= \mathsf{e} \cdot z \\ &= z. \end{aligned}$$

Nun zeigen wir (2). Wir wählen $z \in G$ und rechnen:

$$\begin{aligned} i(i(z)) &= i(i(z)) \cdot \mathsf{e} \\ &= i(i(z)) \cdot (i(z) \cdot z) \\ &= (i(i(z)) \cdot i(z)) \cdot z \\ &= \mathsf{e} \cdot z \\ &= z. \end{aligned}$$

Für (3) berechnen wir

$$\begin{aligned} z \cdot i(z) &= i(i(z)) \cdot i(z) \\ &= \mathsf{e}. \end{aligned}$$

Übungsaufgaben 6.4.

(1) Sei $(G, \cdot, i, \mathsf{e})$ eine Gruppe. Zeigen Sie, dass für alle $a, b \in G$ die Gleichung $a \cdot x = b$ genau eine Lösung hat.
(2) Sei $(G, \cdot, i, \mathsf{e})$ eine Gruppe. Benutzen Sie das vorige Übungsbeispiel, um zu zeigen, dass $i(\mathsf{e}) = \mathsf{e}$, und dass für alle $x, y \in G$ gilt:
$$i(x \cdot y) = i(y) \cdot i(x).$$
(3) * Sei $(G, \cdot, i, \mathsf{e})$ eine Gruppe. Zeigen Sie durch eine Kette von Gleichungen wie im Beweis von Satz 6.3, dass $i(\mathsf{e}) = \mathsf{e}$, und dass für alle $x, y \in G$ gilt:
$$i(x \cdot y) = i(y) \cdot i(x).$$
(4) Finden Sie eine Menge H, eine Funktion $\cdot$ von $H \times H$ nach H, eine Funktion i von H nach H, und ein Element $\mathsf{e} \in H$, sodass alle folgende Eigenschaften erfüllt sind:
   (a) Für alle $x, y, z \in H$ gilt: $(x \cdot y) \cdot z = x \cdot (y \cdot z)$, $\mathsf{e} \cdot x = x$, $x \cdot i(x) = \mathsf{e}$.
   (b) $(H, \cdot, i, \mathsf{e})$ ist keine Gruppe.

(5) Zeigen Sie, dass bei einer Gruppe G die Funktion, die das inverse Element bestimmt, und das neutrale Element der Gruppe, bereits durch die zweistellige Gruppenoperation vollständig bestimmt sind. Zeigen Sie dazu:
Seien $(G, \circ, i_1, \mathsf{e}_1)$ und $(G, \circ, i_2, \mathsf{e}_2)$ zwei Gruppen. (Die beiden Gruppen haben also die Trägermenge G und die zweistellige Operation $\circ$ gemeinsam.)
Dann gilt $i_1 = i_2$ und $\mathsf{e}_1 = \mathsf{e}_2$.

Es ist erfreulich, dass man Satz 6.3 automatisch beweisen lassen kann; die theoretische Grundlage dafür ist die Methode von Knuth und Bendix [**KB70**], die z. B. in [**Buc82**] beschrieben wird. Eine Implementation dieses Algorithmus, der "Larch"-prover, liefert bei Eingabe der Gleichungen

$$\begin{aligned} e * x &= x \\ i(x) * x &= e \\ (x * y) * z &= x * (y * z) \end{aligned}$$

innerhalb weniger Sekunden folgende Konsequenzen aus diesen Gleichungen:

$$\begin{aligned} \text{group.1:} \quad & e * x = x \\ \text{group.2:} \quad & i(x) * x = e \\ \text{group.3:} \quad & x * y * z = x * (y * z) \\ \text{group.4:} \quad & i(y) * (y * z) = z \\ \text{group.6:} \quad & z * e = z \\ \text{group.8:} \quad & i(e) = e \\ \text{group.10:} \quad & i(i(z)) = z \\ \text{group.11:} \quad & z * i(z) = e \\ \text{group.12:} \quad & z * (i(z) * g) = g \\ \text{group.24:} \quad & i(g * y) = i(y) * i(g) \end{aligned}$$

2. Beispiele für Gruppen

In manchen der folgenden Beispiele geben wir eine Gruppe $(G, \cdot, i, \mathsf{e})$ einfach als $(G, \cdot)$ an.

Beispiel 6.5 (Permutationsgruppen und die Zyklenschreibweise). Für $n \in \mathbb{N}$ ist $S_n = \{f : \{1, 2, \ldots, n\} \to \{1, 2, \ldots, n\} \mid f \text{ ist bijektiv}\}$. Diese Gruppe hat $n!$ Elemente und heißt die *symmetrische Gruppe vom Grad n*. Der *Wirkungsbereich* einer Permutation f ist die Menge aller $j \in \{1, \ldots, n\}$ mit $f(j) \neq j$. Einige Elemente von S_n bezeichnen wir als *Zyklen*. Seien dazu $i_1, \ldots, i_m$ paarweise verschiedene Zahlen in $\{1, \ldots, n\}$. Mit $(i_1, i_2, \ldots, i_m)$ bezeichnen wir die Abbildung $f : \{1, \ldots, n\} \to \{1, \ldots, n\}$, $f(i_1) = i_2$, $f(i_2) = i_3$, $\ldots$, $f(i_{m-1}) = i_m$, $f(i_m) = i_1$, $f(j) = j$ für $j \in \{1, \ldots, n\} \setminus \{i_1, \ldots, i_m\}$. Ein f, das sich so schreiben lässt, heißt auch *Zyklus der Länge m*. Jedes Element der S_n lässt sich als Produkt endlich vieler Zyklen mit paarweise disjunktem Wirkungsbereich

schreiben, so gilt zum Beispiel

$$\left(\begin{smallmatrix}1&2&3&4&5\\3&2&1&5&4\end{smallmatrix}\right) = (1,3)(4,5) = (3,1)(5,4) = (5,4)(3,1)$$

und

$$\left(\begin{smallmatrix}1&2&3&4&5\\2&3&5&4&1\end{smallmatrix}\right) = (1,2,3,5).$$

BEISPIEL 6.6 (Matrixgruppen). Seien $n \in \mathbb{N}$, $p \in \mathbb{P}$.

(1) Sei $\mathrm{GL}(n,p)$ die Menge aller regulären $n \times n$-Matrizen über $\mathbb{Z}_p$. Dann ist $(\mathrm{GL}(n,p), \cdot, ^{-1}, E_n)$ eine Gruppe, die *allgemeine lineare Gruppe*.
(2) Sei $\mathrm{SL}(n,p) := \{A \in \mathrm{GL}(n,p) \mid \det A = 1\}$. Dann ist $(\mathrm{SL}(n,p), \cdot, ^{-1}, E_n)$ eine Gruppe, die *spezielle lineare Gruppe*.

BEISPIEL 6.7 (Restklassen von $\mathbb{Z}$ mit Addition). Für $n \in \mathbb{N}$ ist $(\mathbb{Z}_n, +)$ eine Gruppe, die *zyklische Gruppe* mit n Elementen.

BEISPIEL 6.8 (Restklassen von $\mathbb{Z}$ mit Multiplikation).

(1) Sei $n \geq 2$. Dann ist $(\mathbb{Z}_n, \cdot)$ keine Gruppe.
(2) Sei $n \geq 2$. $(\mathbb{Z}_n \backslash \{[0]_n\}, \cdot)$ ist genau dann eine Gruppe, wenn n eine Primzahl ist.
(3) Sei $n \in \mathbb{N}$, und sei $\mathbb{Z}_n^* := \{[x]_n \mid x \in \mathbb{Z} \text{ und } \mathrm{ggT}(x,n) = 1\}$. Dann ist $(\mathbb{Z}_n^*, \cdot, ^{-1}, [1]_n)$ eine Gruppe mit $\varphi(n)$ Elementen, die *multiplikative Gruppe modulo n*.

BEISPIEL 6.9 (Symmetriegruppen geometrischer Objekte). Wir zeichnen das Quadrat mit den Eckpunkten $(-1,-1)$, $(1,-1)$, $(1,1)$, $(-1,1)$, und betrachten alle bijektiven linearen Abbildungen von $\mathbb{R}^2$ nach $\mathbb{R}^2$, die das Quadrat auf sich selbst abbilden (diese Abbildungen bezeichnen wir als *Symmetrieabbildungen*). Die Hintereinanderausführung zweier Symmetrieabbildungen ist wieder eine Symmetrieabbildung. Die identische Abbildung ist eine Symmetrieabbildung, und zu jeder Symmetrieabbildung d ist die inverse Abbildung wieder eine Symmetrieabbildung. Die Menge aller Symmetrieabbildungen, mit der Hintereinanderausführung als zweistelliger Operation, ist eine Gruppe. Für das Quadrat gibt es genau 8 Symmetrieabbildungen.

BEISPIEL 6.10 (Endlich präsentierte Gruppen). Sei G die 8-elementige Gruppe der Symmetrieabbildungen eines Quadrats. Wir bezeichnen nun eine Drehung des Quadrats um 90° gegen den Uhrzeigersinn mit a und eine Spiegelung an der y-Achse mit b. Wir können dann jede der 8 Symmetrieabbildungen als Produkt von a's und b's schreiben. Man kann mit diesen Produkten rechnen, wenn man berücksichtigt, dass $a^4 = 1$, $b^2 = 1$, und $ba = a^3b$ gilt. So gilt etwa $baab = a^3bab = a^6b^2 = a^2$. Insgesamt können wir jedes Wort zu einem Wort aus der Menge $\{1, a, aa, aaa, b, ab, aab, aaab\}$ umformen, das die gleiche Symmetrieabbildung darstellt. Daher gibt man diese Gruppe der Symmetrieabbildungen des Quadrats, die man als D_4 (Diedergruppe mit 8 Elementen) bezeichnet, auch oft so an:

$$D_4 = \langle \underbrace{a, b}_{\text{Erzeuger}} \mid \underbrace{a^4 = 1, b^2 = 1, ba = a^3b}_{\text{definierende Relationen } R} \rangle.$$

Formal bildet man dazu die Menge W aller Wörter über dem Alphabet $\{a, b, a^{-1}, b^{-1}\}$ und bezeichnet w_1 und w_2 in W als äquivalent bezüglich der definierenden Relationen R, wenn w_1, w_2 für alle Gruppen G und für alle $a, b \in G$ mit $a^4 = 1, b^2 = 1, ba = a^3b$ das gleiche Element aus G ergeben. Die Faktormenge nach dieser Äquivalenzrelation ist dann die von den Erzeugern $\{a, b\}$ und den Relationen R *präsentierte* Gruppe.

Beispiel 6.11 (Gruppen, die durch die Gruppentafel gegeben sind). Wir definieren eine Gruppenoperation auf $\{0, 1, 2, 3\}$ durch

+	0	1	2	3
0	0	1	2	3
1	1	0	3	2
2	2	3	0	1
3	3	2	1	0

Übungsaufgaben 6.12.

(1) Bestimmen Sie die Matrixdarstellung der acht linearen Abbildungen, die das Quadrat mit den Eckpunkten $(-1, -1)$, $(1, -1)$, $(1, 1)$, $(-1, 1)$ in sich selbst überführen.
(2) Wir betrachten alle Abbildungen $\{f : \mathbb{C} \to \mathbb{C}\}$, die sich als Hintereinanderausführung der Funktionen $x \to i \cdot x$ und $x \to \overline{x}$ schreiben lassen. (Dabei ist $\overline{a + bi} := a - bi$).
   (a) Wieviele Funktionen lassen sich daraus zusammenbauen?
   (b) Was machen diese Funktionen mit den Punkten $\{-1 - i, 1 - i, 1 + i, -1 + i\}$?
(3) Wir betrachten in $\mathbb{R}^2$ das Sechseck mit den Eckpunkten $\{(\mathrm{Re}(z), \mathrm{Im}(z)) \mid z \in \mathbb{C},\ z^6 = 1\}$. Bestimmen Sie alle Deckabbildungen, die dieses Sechseck auf sich selbst abbilden.
(4) Wir betrachten in $\mathbb{R}^2$ das Sechseck mit den Eckpunkten $\{(\mathrm{Re}(z), \mathrm{Im}(z)) \mid z \in \mathbb{C},\ z^6 = 1\}$. Wie können Sie die Gruppe aller Symmetrieoperationen dieses Sechseckes durch Worte in a und b angeben? Was sind die "Rechenregeln"? (Diese Rechenregeln bezeichnet man auch als *definierende Relationen.*)
(5) * Als "Wort" betrachten wir eine endliche Folge von Buchstaben aus $\{a, b, c, \ldots, z\}$. Diese Worte verknüpfen wir durch Aneinanderhängen, also z.B. $afc * gff = afcgff$. Für manche Worte w_1, w_2 gilt $w_1 * w_2 = w_2 * w_1$, zum Beispiel $aaa * aa = aa * aaa$, oder, komplizierter, $avd * avdavd = avdavd * avd$. Beschreiben Sie alle Wortpaare (w_1, w_2), sodass $w_1 * w_2 = w_2 * w_1$.

3. Untergruppen und Homomorphismen

Definition 6.13. Sei $(G, \cdot)$ eine Gruppe. Eine nichtleere Teilmenge H von G ist eine *Untergruppe* von G, wenn für alle $h_1, h_2 \in H$ auch dass auch $h_1^{-1} \in H$ und $h_1 \cdot h_2 \in H$ gilt.

Der Durchschnitt von Untergruppen ist wieder eine Untergruppe. Für $A \subseteq G$ definieren wir *die von A erzeugte Untergruppe* $\langle A \rangle$ als den Schnitt aller Untergruppen H von G mit $A \subseteq H$. Es gilt dann:

SATZ 6.14. *Sei G eine Gruppe, $A \subseteq G$. Dann gilt*

$$\langle A \rangle = \{a_1^{e_1} \cdots a_n^{e_n} \mid n \in \mathbb{N}_0, a_1, \ldots, a_n \in A, e_1, \ldots, e_n \in \{-1, +1\}\}.$$

Wir schreiben auch $\langle a_1, \ldots, a_n \rangle$ für $\langle \{a_1, \ldots, a_n\} \rangle$.

SATZ 6.15 (Satz von Lagrange[1]). *Sei G eine endliche Gruppe, und sei H eine Untergruppe von G. Dann ist $|H|$ ein Teiler von $|G|$.*

BEWEIS. Wir definieren auf G eine Relation $\sim_H$. Für $a, b \in G$ gelte $a \sim_H b$ genau dann, wenn es $h \in H$ mit $ah = b$ gibt. Also gilt $a \sim_H b$ genau dann, wenn $a^{-1}b \in H$. Diese Relation $\sim_H$ ist eine Äquivalenzrelation auf G. Die Äquivalenzklasse von a ist $\{ah \mid h \in H\} =: aH$. Die Abbildung $\lambda_a : H \to aH$, $\lambda_a(h) := ah$, ist bijektiv, daher hat die Klasse aH gleich viele Elemente wie H. Da sich G also in lauter Klassen von $|H|$ Elementen partitionieren lässt, gilt $|H| \mid |G|$. □

Für eine endliche Gruppe heißt $|G|$ auch die *Ordnung* von G.

DEFINITION 6.16. Seien G, H Gruppen. Eine Funktion $f : G \to H$ ist ein *Homomorphismus*, wenn für alle $a, b \in G$ gilt, dass $f(a \cdot b) = f(a) \cdot f(b)$.

Ein Homomorphismus erfüllt $f(1_G) = f(1_G \cdot 1_G) = f(1_G) \cdot f(1_G)$. Durch Multiplikation mit $(f(1_G))^{-1}$ erhält man $1_H = f(1_G)$. Weiters gilt $f(a^{-1}) = f(a)^{-1}$ für alle $a \in G$.

ÜBUNGSAUFGABEN 6.17.

(1) Die *Ordnung* eines Gruppenelements g ist das kleinste $n \in \mathbb{N}$, sodass $g^n = 1$. Sei φ ein Gruppenhomomorphismus. Seien G und H endliche Gruppen, und sei $\varphi : G \to H$ ein Gruppenhomomorphismus. Zeigen Sie, dass für jedes $g \in G$ die Ordnung von g ein Vielfaches der Ordnung von $\varphi(g)$ ist.
(2) Finden Sie das kleinste $m \in \mathbb{N}$, sodass die Gruppe $(\mathbb{Z}_{30}, +)$ in die symmetrische Gruppe S_m einbettbar ist!
(3) Finden Sie eine 4-elementige Untergruppe der S_4, die nicht isomorph zur $\mathbb{Z}_4$ ist.
(4) Seien G und H Gruppen, sei h ein Homomorphismus von G nach H. Sei A Trägermenge einer Untergruppe von G. Zeigen Sie, dass $h(A)$ Trägermenge einer Untergruppe von H ist.
(5) Seien G und H Gruppen, sei h ein Homomorphismus von G nach H. Sei B Trägermenge einer Untergruppe von H. Zeigen Sie, dass $h^{-1}(B) = \{x \in G \mid h(x) \in B\}$ Trägermenge einer Untergruppe von G ist.

[1] Joseph-Louis Lagrange, 1736-1813

(6) Zeigen Sie, dass ein Homomorphismus, der die Eigenschaft

$$\text{für alle } x \in G : h(x) = 1_H \Rightarrow x = 1_G$$

erfüllt, injektiv ist.

(7) Sei $n \in \mathbb{N}$. Finden Sie alle Homomorphismen von $(\mathbb{Z}_n, +)$ nach $(\mathbb{Z}_n, +)$. Welche sind bijektiv?

(8) Zeigen Sie, dass die Abbildung $f : G \to G, g \mapsto g^{-1}$ genau dann ein Homomorphismus ist, wenn G *abelsch* ist, also $x \cdot y = y \cdot x$ für alle $x, y \in G$ gilt.

(9) Sei G die Gruppe $((\mathbb{Z}_2)^n, \star)$ mit der Verknüpfung

$$(x_1, x_2, \ldots, x_n) \star (y_1, y_2, \ldots, y_n) := (x_1 \oplus y_1, x_2 \oplus y_2, \ldots, x_n \oplus y_n),$$

wobei $\oplus$ die Addition modulo 2 ist. Sei X eine Menge mit n Elementen, und sei $\mathcal{P}(X)$ die Potenzmenge von X. Zeigen Sie:

$H := (\mathcal{P}(X), \Delta)$ ist eine Gruppe. (Finden Sie das Inverse zu $Y \subseteq X$, und das Einselement.)

Geben Sie einen Gruppenisomorphismus von H nach G an!

DEFINITION 6.18. Sei N eine Untergruppe von G. N ist ein *Normalteiler* von G, wenn für alle $g \in G$ und $n \in N$ auch $g^{-1}ng \in N$ gilt.

SATZ 6.19. *Sei $f : G \to H$ ein Homomorphismus. Dann ist* $\ker(f) := \{g \in G \mid f(g) = 1_H\}$ *ein Normalteiler von G.*

SATZ 6.20. *Seien G eine Gruppe und N ein Normalteiler von G. Für $g \in G$ definieren wir $gN := \{gn \mid n \in N\}$ und*

$$G/N := \{gN \mid g \in G\}.$$

Auf G/N definieren wir $\odot$ durch $gN \odot hN := (gh)\,N$ und $(gN)^{-1} := g^{-1}\,N$. Dann sind $\odot$ und $^{-1}$ wohldefiniert, und $(G/N, \odot, ^{-1}, 1N)$ ist eine Gruppe, die Faktorgruppe *von G nach N.*

BEWEIS. Wir nehmen an, dass $g_1N = g_2N$ und $h_1N = h_2N$. Dann gibt es $n_1, n_2 \in N$ mit $g_1 = g_2n_1$ und $h_1 = h_2n_2$. Dann gilt $g_1h_1 = g_2n_1h_2n_2 = g_2h_2h_2^{-1}n_1h_2n_2$. Da N ein Normalteiler ist, gilt $h_2^{-1}n_1h_2 \in N$ und somit $n_3 := h_2^{-1}n_1h_2n_2 \in N$, und wegen $g_1h_1 = g_2h_2n_3$ gilt $g_1h_1 \in (g_2h_2)\,N$, also $(g_1h_1)\,N = (g_2h_2)\,N$. Weiters gilt $g_1^{-1} = (g_2n_1)^{-1} = n_1^{-1}g_2^{-1} = g_2^{-1}\underbrace{g_2n_1^{-1}g_2^{-1}}_{=:n_4} = g_2^{-1}n_4$, also $g_1^{-1}N = g_2^{-1}N$. Somit sind die Operationen wohldefiniert. Assoziativität, Neutralität von $1N$ und $(xN)^{-1}(xN) = 1N$ rechnet man direkt nach. □

SATZ 6.21 (Homomorphiesatz). *Seien G, H Gruppen, und sei f ein Homomorphismus von G nach H. Dann ist* $\mathrm{im}(f) := f(G)$ *eine Untergruppe von H und $N := \ker(G)$ ein Normalteiler von G. Weiters ist $\hat{f} : G/N \to \mathrm{im}(f)$, $\hat{f}(gN) := f(g)$, ein Isomorphismus.*

KAPITEL 7

Zyklische und abelsche Gruppen

1. Zyklische Gruppen

DEFINITION 7.1. Eine Gruppe G ist *zyklisch*, wenn es ein $a \in G$ mit $G = \langle a \rangle$ gibt.

DEFINITION 7.2. Sei G eine Gruppe, sei $a \in G$ und $z \in \mathbb{Z}$. Die Potenz a^z definieren wir als $a \cdots a$ (z Faktoren), wenn $z > 0$. Weiters ist $a^0 := 1_G$ und $a^z := (a^{-1})^{-z}$ für $z < 0$.

LEMMA 7.3. *Sei $(G, \cdot)$ eine Gruppe, sei $a \in G$, und sei $\varphi : \mathbb{Z} \to G$ definiert durch $\varphi(z) = a^z$ für $z \in \mathbb{Z}$. Dann ist φ ein Homomorphismus von $(\mathbb{Z}, +)$ nach $(G, \cdot)$.*

BEWEIS. Wir zeigen als erstes, dass für alle $x \in \mathbb{Z}$ gilt, dass $a^{x+1} = a^x \cdot a$. Für $x \geq 0$ ergibt sich das aus der Definition von a^{x+1}. Sei nun $x < 0$. Dann gilt $a^x \cdot a = (a^{-1})^{-x} \cdot a = (a^{-1})^{-x-1} = a^{x+1}$. Wegen $a^{x-1} \cdot a = a^x$ gilt daher auch $a^{x-1} = a^x \cdot a^{-1}$ für alle $x \in \mathbb{Z}$. Wir zeigen nun $a^{x+y} = a^x + a^y$ durch Induktion nach $|y|$. Wenn $y = 0$, so gilt $a^{x+0} = a^x = a^x \cdot 1 = a^x \cdot a^0$. Wenn $y > 0$, so gilt $a^{x+y} = a^{(x+y-1)+1} = a^{x+(y-1)} \cdot a = (a^x \cdot a^{y-1}) \cdot a = a^x \cdot (a^{y-1} \cdot a) = a^x \cdot a^y$. Wenn $y < 0$, so gilt $a^{x+y} = a^{(x+y+1)-1} = a^{x+(y+1)} \cdot a^{-1} = (a^x \cdot a^{y+1}) \cdot a^{-1} = a^x \cdot (a^{y+1} \cdot a^{-1}) = a^x \cdot a^y$. □

Wenn $G = \langle a \rangle$ zyklisch ist, gilt für diesen Homomorphismus φ auch $a \in \mathrm{im}(\varphi)$, und somit $\langle a \rangle \subseteq \mathrm{im}(\varphi)$. Also ist φ surjektiv, und somit gilt $G = \{a^z \mid z \in \mathbb{Z}\}$.

SATZ 7.4. *Sei $(G, \cdot)$ eine zyklische Gruppe. Dann ist G zu $(\mathbb{Z}, +)$ isomorph, oder es gibt ein $n \in \mathbb{N}$, sodass G zu $(\mathbb{Z}_n, +)$ isomorph ist.*

BEWEIS. Sei $a \in G$ ein Erzeuger von G, und sei $\varphi(z) := a^z$ für $z \in \mathbb{Z}$. Da G zyklisch ist, ist φ surjektiv. Sei $N := \{z \in \mathbb{Z} \mid a^z = 1_G\}$. Dann ist N ein Normalteiler von $(\mathbb{Z}, +)$, und wegen des Homomorphiesatzes ist G isomorph zu $\mathbb{Z}/N$. N ist auch ein Ideal des Rings $(\mathbb{Z}, +, \cdot)$. Somit gibt es ein $n \in \mathbb{N}_0$, sodass $N = \{tn \mid t \in \mathbb{Z}\}$. Wenn $n = 0$, so ist $\mathbb{Z}/N$ isomorph zu $(\mathbb{Z}, +)$. Wenn $n > 0$, so ist $\mathbb{Z}/N$ die Gruppe $(\mathbb{Z}_n, +)$. □

SATZ 7.5. *Seien $a, b \in \mathbb{N}$ mit $\gcd(a, b) = 1$. Dann ist $(\mathbb{Z}_{ab}, +)$ isomorph zu $\mathbb{Z}_a \times \mathbb{Z}_b$.*

BEWEIS. Die Abbildung $\varphi : \mathbb{Z} \to \mathbb{Z}_a \times \mathbb{Z}_b$, $x \mapsto ([x]_a, [x]_b)$ erfüllt $\ker(\varphi) = \{x \in \mathbb{Z} : a \mid x \text{ und } b \mid x\} = \{x \in \mathbb{Z} : ab \mid x\}$. Somit ist $\mathbb{Z}/\ker(\varphi)$ isomorph zu $\mathbb{Z}_{ab}$. Da wegen des Homomorphiesatzes $\mathrm{im}(\varphi)$ somit ab Elemente hat, gilt $\mathrm{im}(\varphi) = \mathbb{Z}_a \times \mathbb{Z}_b$, und somit $\mathbb{Z}_{ab} \cong \mathbb{Z}_a \times \mathbb{Z}_b$. □

KOROLLAR 7.6. *Jede endliche zyklische Gruppe ist direktes Produkt von zyklischen Gruppen von Primzahlpotenzordnung.*

SATZ 7.7 (Satz von Fermat[1]). *Sei $(G, \cdot)$ eine endliche Gruppe, sei $g \in G$, und sei* $\operatorname{ord}(g) := \min\{k \in \mathbb{N} \mid g^k = 1\}$. *Dann gilt $|\langle g\rangle| = \operatorname{ord}(g)$, $\operatorname{ord}(g) \mid |G|$, und $g^{|G|} = 1$.*

BEWEIS. Wir betrachten $\varphi : \mathbb{Z} \to G$, $\varphi(z) = g^z$. Nach dem Homomorphiesatz ist $\langle g\rangle$ isomorph zu $\mathbb{Z}/N$, wobei $N := \{k \in \mathbb{Z} \mid g^k = 1\}$. Die Menge N ist auch ein Ideal des Rings $(\mathbb{Z}, +, \cdot)$. Da G endlich ist, gilt $N \neq \{0\}$, und somit wird N vom kleinsten positiven $n \in N$, also von $n = \operatorname{ord}(g)$ erzeugt. Folglich gilt $Z/N = \mathbb{Z}_n$, und somit hat $\langle g\rangle$ genau n Elemente. Wegen des Satzes von Lagrange gilt also $n \mid |G|$ und somit auch $g^{|G|} = (g^n)^{|G|/n} = 1^{|G|/n} = 1$. □

2. Endlich erzeugte abelsche Gruppen

Eine Gruppe G ist *abelsch*, wenn für alle $g, h \in G$ gilt, dass $g \cdot h = h \cdot g$. Jede zyklische Gruppe ist abelsch. Endlich erzeugte abelsche Gruppen lassen sich ebenfalls gut beschreiben. Wir benützen dazu folgenden Satz über die Smith-Normalform.

SATZ 7.8 (Smith-Normalform[2], cf. [**Kau22**, Satz 135]). *Sei $k \in \mathbb{N}$ und $A \in \mathbb{Z}^{k\times k}$. Dann gibt es $U, V \in \mathbb{Z}^{k\times k}$ und $D \in \mathbb{N}_0^{k\times k}$, sodass $D = UAV$, $\det(U) \in \{-1, +1\}$, $\det(V) \in \{-1, +1\}$, $D(i, j) = 0$ für $i, j \in \{1, \dots, k\}$ mit $i \neq j$, und $D(1, 1) \mid D(2, 2) \mid \cdots \mid D(k, k)$.*

SATZ 7.9 (Hauptsatz über endlich erzeugte abelsche Gruppen (Poincaré[3])). *Sei $(G, +)$ eine abelsche Gruppe, die von einer endlichen Menge erzeugt wird. Dann gibt es $r, s \in \mathbb{N}_0$ und $m_1, \dots, m_r \in \mathbb{N}$, sodass $m_1 \mid m_2 \mid \cdots \mid m_r$ und G isomorph zu $\mathbb{Z}_{m_1} \times \cdots \times \mathbb{Z}_{m_r} \times \mathbb{Z}^s$ ist.*

BEWEIS. Die abelsche Gruppe G wird durch

$$zg = \underbrace{g + \ldots + g}_{z \text{ Summanden}} \text{ für } z \geq 0 \text{ und } zg = (-z)(-g) \text{ für } z < 0$$

ein $\mathbb{Z}$-Modul. Sei $G = \langle g_1, \dots, g_k\rangle$, und sei

$$\varphi : \mathbb{Z}^k \to G,\ (x_1, \dots, x_k) \mapsto x_1 g_1 + \cdots + x_k g_k.$$

Es gilt $\varphi((x_1, \dots, x_n) + (y_1, \dots, y_n)) = \varphi((x_1 + y_1, \dots, x_n + y_n)) = (x_1 + y_1)g_1 + \cdots + (x_n + y_n)g_n = x_1 g_1 + \cdots + x_n g_n + y_1 g_1 + \cdots + y_n g_n = \varphi((x_1, \dots, x_n)) + \varphi((y_1, \dots, y_n))$ und $\varphi(z\,(x_1, \dots, x_n)) = \varphi((zx_1, \dots, zx_n)) = zx_1\, g_1 + \cdots + zx_n\, g_n = z(x_1 g_1 + \cdots + x_n g_n) =$

[1] Pierre de Fermat, 1607-1665
[2] Henry J. S. Smith, 1826-1883
[3] Jules H. Poincaré, 1854-1912

$z\varphi((x_1, \dots, x_n))$. Also ist φ ein $\mathbb{Z}$-Modul-Isomorphismus. Sei e_i der i-te Einheitsvektor. Wegen $\varphi(e_i) = g_i$ ist φ surjektiv.

Der Homomorphiesatz besagt nun, dass $\mathbb{Z}^k/\ker\varphi \cong \operatorname{im}\varphi$, also gilt für $K := \ker\varphi$ wegen der Surjektivität von φ, dass $\mathbb{Z}^k/K$ isomorph zu G ist. Wegen [**Kau22**, Satz 126] ist der Modul K endlich erzeugt (aus dem Beweis geht sogar hervor, dass K eine Basis mit höchstens k Elementen hat). Also gibt es eine Matrix $A \in \mathbb{Z}^{k\times k}$, sodass K der von den Spalten von A erzeugte Untermodul $S(A)$ von $\mathbb{Z}^k$ ist. Sei $D = UAV$ die Zerlegung von A in die Smith-Normalform. Wir betrachten nun die Abbildung

$$\psi : \mathbb{Z}^k/S(A) \to \mathbb{Z}^k/S(D),\ \psi([x]_{\sim_{S(A)}}) = [Ux]_{\sim_{S(D)}}.$$

Die Abbildung ψ ist wohldefiniert: Seien $x, y \in \mathbb{Z}^k$ so, dass $[x]_{\sim_{S(A)}} = [y]_{\sim_{S(A)}}$. Dann gilt $x - y \in S(A)$. Es gibt also $v \in \mathbb{Z}^k$, sodass $x - y = Av$. Somit gilt $Ux - Uy = U(x-y) = UAv = UAVV^{-1}v = D(V^{-1}v) \in S(D)$, und folglich $[Ux]_{\sim_{S(D)}} = [Uy]_{\sim_{S(D)}}$. Also ist ψ wohldefiniert.

Wir zeigen nun, dass ψ ein Isomorphismus zwischen $\mathbb{Z}$-Moduln ist. Seien dazu $x, y \in \mathbb{Z}^k$ und $z \in \mathbb{Z}$. Wegen $\psi([x]_{\sim_{S(A)}} + [y]_{\sim_{S(A)}}) = \psi([x+y]_{\sim_{S(A)}}) = [U(x+y)]_{\sim_{S(D)}} = [Ux]_{\sim_{S(D)}} + [Uy]_{\sim_{S(D)}} = \psi([x]_{\sim_{S(A)}}) + \psi([y]_{\sim_{S(A)}})$ und $\psi(z[x]_{\sim_{S(A)}}) = \cdots = z\psi([x]_{\sim_{S(A)}})$ ist ψ ein $\mathbb{Z}$-Modul-Homomorphismus. Für die Injektivität wählen wir x, y mit $\psi([x]_{\sim_{S(A)}}) = \psi([y]_{\sim_{S(A)}})$. Dann gilt $Ux - Uy \in S(D)$, also gibt es $v \in \mathbb{Z}^n$ mit $Ux - Uy = Dv$. Dann gilt $x - y = U^{-1}Dv = U^{-1}UAVv = A(Vv) \in S(A)$, und somit gilt $[x]_{\sim_{S(A)}} = [y]_{\sim_{S(A)}}$. Für die Surjektivität fixieren wir $[y]_{\sim_{S(D)}} \in \mathbb{Z}^k$. Dann gilt $\psi([U^{-1}y]_{\sim_{S(A)}}) = [y]_{\sim_{S(D)}}$, also ist ψ surjektiv. Insgesamt ist ψ also ein $\mathbb{Z}$-Modul-Isomorphismus.

Sei nun $r := \max(\{0\} \cup \{i \in \{1, \dots, k\} \mid D(i,i) \neq 0\})$, $m_i := D(i,i)$ für $i \in \{1, \dots, r\}$ und

$$\alpha : \mathbb{Z}^k \to \mathbb{Z}_{m_1} \times \cdots \times \mathbb{Z}_{m_r} \times \mathbb{Z}^{k-r},\ \alpha(x_1, \dots, x_k) := ([x_1]_{m_1}, \dots, [x_r]_{m_r}, x_{r+1}, \dots, x_k).$$

Man sieht leicht, dass α surjektiv ist, und dass $\ker\alpha = S(D)$. Also ist $\mathbb{Z}^k/S(D)$ wegen des Homomorphiesatzes isomorph zu $\mathbb{Z}_{m_1} \times \cdots \times \mathbb{Z}_{m_r} \times \mathbb{Z}^{k-r}$.

Insgesamt ist dann G isomorph zu $\mathbb{Z}_{m_1} \times \cdots \times \mathbb{Z}_{m_r} \times \mathbb{Z}^{k-r}$. □

KOROLLAR 7.10. *Jede endliche abelsche Gruppe ist direktes Produkt von zyklischen Gruppen von Primzahlpotenzordnung.*

KOROLLAR 7.11. *Sei K ein Körper, und sei G eine endliche Untergruppe von $(K \setminus \{0\}, \cdot)$. Dann ist G zyklisch.*

BEWEIS. Wegen des Hauptsatzes über endlich erzeugte abelsche Gruppen ist G isomorph zu $\mathbb{Z}_{m_1} \times \cdots \times \mathbb{Z}_{m_r}$ mit $m_1 \mid m_2 \mid \cdots \mid m_r$. Alle Elemente x in G erfüllen $x^{m_r} = 1$. Das Polynom $X^{m_r} - 1$ ist vom Grad m_r und hat daher über K höchstens m_r Nullstellen. Also gilt $m_1 \cdots m_r \leq m_r$, und somit $m_1 = \cdots = m_{r-1} = 1$. Folglich ist G isomorph zu $(\mathbb{Z}_{m_r}, +)$ und somit zyklisch. □

KAPITEL 8

Gruppenoperationen und Abzählprobleme

1. Gruppenoperationen und das Burnside-Lemma

DEFINITION 8.1 (Gruppenoperation). Sei $(G, \cdot)$ eine Gruppe und X eine Menge. Eine Funktion $* : G \times X \to X$ ist eine *Gruppenoperation* von G auf X, wenn

(1) für alle $x \in X : 1_G * x = x$;
(2) für alle $g, h \in G$ und $x \in X : g * (h * x) = (g \cdot h) * x$.

BEISPIELE 8.2.

(1) Sei $X = \{1, \ldots, n\}$ und $G = S_n$. Dann wird durch $g * x := g(x)$ eine Gruppenoperation definiert.
(2) Seien X, Y Mengen, und sei G eine Untergruppe von S_X. Sei $f \in Y^X$ und $g \in G$. Dann wird durch
$$g * f\,(x) := f(g^{-1}(x))$$
eine Gruppenoperation von G auf Y^X definiert.
(3) Sei G eine Gruppe und sei $X := G$. Dann ist die Operation $g * x := gxg^{-1}$ eine Gruppenoperation.
(4) Sei G eine Gruppe und sei $X := G$. Dann ist die Operation $g * x := gx$ eine Gruppenoperation.

SATZ 8.3. *Sei $*$ eine Gruppenoperation von G auf X. Dann ist die Abbildung $\varphi : G \to S_X$ mit $\varphi(g)\,(x) := g * x$ ein Gruppenhomomorphismus von G nach $(S_X, \circ)$.*

BEWEIS. Für $g, h \in G$ und $x \in X$ gilt $\varphi(g \cdot h)\,(x) = (g \cdot h) * x = g * (h * x) = g * (\varphi(h)\,(x)) = \varphi(g)(\varphi(h)\,(x)) = (\varphi(g) \circ \varphi(h))\,(x)$. □

SATZ 8.4 (Satz von Cayley[1]). *Sei $(G, \cdot)$ eine Gruppe, und sei $X := G$. Dann ist G zu einer Untergruppe von S_X isomorph.*

BEWEIS. Wir betrachten die Gruppenoperation $g * x := g \cdot x$ von G auf X. Die Abbildung φ aus Satz 8.3 ist ein Homomorphismus mit Kern $N := \{g \in G \mid \forall x \in G : g * x = x\}$. Wegen $N = \{1_G\}$ ist φ injektiv, und somit ist $\mathrm{im}(\varphi)$ eine zu G isomorphe Untergruppe von S_X. □

[1] Arthur Cayley, 1821-1895

KOROLLAR 8.5. *Sei $n \in \mathbb{N}$, und sei G eine endliche Gruppe mit n Elementen. Dann ist G zu einer Untergruppe der S_n isomorph.*

Wir betrachten nun folgendes Abzählproblem.

PROBLEM 8.6. *Auf wieviele Arten kann man die Ecken eines Quadrats mit drei Farben färben? Dabei sehen wir zwei Färbungen als gleich an, wenn man sie durch Drehungen oder Spiegelungen des Quadrats ineinander überführen kann.*

Diese Gruppenoperationen geben uns eine Möglichkeit, eine mathematische Beschreibung für das Färbeproblem zu finden. Eine Färbung ist eine Funktion von der Menge der Ecken $\{1,2,3,4\}$ in die Menge der Farben $\{r,b,g\}$. Die Menge aller Färbungen X ergibt sich also als:

$$X = \big\{ f \mid f : \{1,2,3,4\} \to \{r,b,g\} \big\}.$$

Jede Symmetrieoperation des Quadrats ist eine Permutation der vier Eckpunkte. Alle Symmetrieoperationen erhalten wir aus folgendem Dialog mit GAP [**GAP12**]. Diese Symmetriegruppe nennen wir D_4.

```
gap> D4 := Group ((1,2,3,4), (1,2)(3,4));
Group([ (1,2,3,4), (1,2)(3,4) ])
gap> AsList (D4);
[ (), (2,4), (1,2)(3,4), (1,2,3,4), (1,3),
  (1,3)(2,4), (1,4,3,2), (1,4)(2,3) ]
gap>
```

Zwei Färbungen α, β sind gleich, wenn es ein g aus der "Symmetriegruppe" gibt, sodass für alle Eckpunkte $z \in \{1,2,3,4\}$ gilt:

$$\beta(g(z)) = \alpha(z).$$

Wir definieren nun eine Gruppenoperation von D_4 auf der Menge X der Färbungen:

$$\begin{array}{rccc} * & : & G \times X & \longrightarrow & X \\ & & (g,\alpha) & \longmapsto & g * \alpha, \end{array}$$

wobei

$$\begin{array}{rccc} g * \alpha & : & \{1,2,3,4\} & \longrightarrow & \{1,2,3,4\} \\ & & z & \longmapsto & \alpha(g^{-1}(z)). \end{array}$$

(Die näherliegende Definition $g * \alpha(z) := \alpha(g(z))$ ergibt keine Gruppenoperation.)

DEFINITION 8.7. Sei G eine Gruppe, X eine Menge und $*$ eine Gruppenoperation von G auf X. Wir bezeichnen x und y in X als *G-äquivalent*, falls es ein $g \in G$ gibt, sodass $y = g * x$ und schreiben dafür $x \approx_G y$.

SATZ 8.8. *Sei G eine Gruppe, X eine Menge und $*$ eine Gruppenoperation von G auf X. Dann gilt:*

(1) $\approx_G$ *ist eine Äquivalenzrelation auf* X.
(2) *Für jedes* $x \in X$ *ist die Äquivalenzklasse* $x/\approx_G = \{y \in X \mid x \approx_G y\}$ *gegeben durch* $x/\approx_G = \{g * x \mid g \in G\}$.

Die Menge $G * x := \{g * x \mid g \in G\}$ heißt *Bahn* oder *Orbit* von x unter der Operation von G. Wenn wir also in Problem 8.6 die nichtäquivalenten Färbungen des Quadrats zählen wollen, so müssen wir die *Anzahl der Bahnen* der Gruppenoperation von D_4 auf der Menge der Färbungen X berechnen.

DEFINITION 8.9. Sei G eine Gruppe, X eine Menge und $*$ eine Gruppenoperation von G auf X, und $x \in X$. Die Menge $G_x := \{g \in G \mid g * x = x\}$ ist der *Stabilisator* von x.

Der Stabilisator G_x ist eine Untergruppe von G.

SATZ 8.10. *Sei* G *eine Gruppe,* X *eine Menge,* $*$ *eine Gruppenoperation von* G *auf* X*, und sei* $x \in X$*. Dann gilt:*

(1) *Für alle* $g, h \in G$ *gilt:* $g * x = h * x \Leftrightarrow g \sim_{G_x} h$.
(2) $|G * x| \cdot |G_x| = G$.

BEWEIS. (1) Wenn $g * x = h * x$, so gilt $x = (g^{-1}h) * x$, also $g^{-1}h \in G_x$. Wegen $h = g(g^{-1}h)$ gilt $g \sim_{G_x} h$. Wenn $g = hs$ mit $s \in G_x$, so gilt $g*x = (hs)*x = h*(s*x) = h * x$.

(2) Aus (1) erhalten wir, dass $|G * x| = |\{gG_x : g \in G\}|$. Also besteht G aus genau $|G * x|$ Nebenklassen von G_x, von denen jede $|G_x|$ Elemente hat. □

Die Anzahl der Bahnen erhalten wir nun aus folgendem Satz:

SATZ 8.11 (Burnside-Lemma[2]). *Sei* G *eine endliche Gruppe, sei* X *eine endliche Menge, und sei* $*$ *eine Gruppenoperation von* G *auf* X*. Sei* n *die Anzahl der Bahnen von* G *auf* X*. Dann gilt:*

$$n = \frac{1}{|G|} \cdot \sum_{g \in G} |\operatorname{Fix}(g)|,$$

wobei $\operatorname{Fix}(g) = \{x \in X \mid g * x = x\}$.

BEWEIS. Wir zählen die Elemente der Menge F auf zwei Arten, wobei

$$F := \{(g, x) \mid g \in G, x \in X, g * x = x\}.$$

Wir erhalten

$$|F| = \sum_{g \in G} |\{x \in X : g * x = x\}| = \sum_{g \in G} |\operatorname{Fix}(g)|$$

[2]William Burnside 1852-1927; das Lemma stammt von Augustin L. Cauchy (1789-1857) und Georg Frobenius (1849-1917)

und, unter Verwendung von Satz 8.10,

$$|F| = \sum_{x \in X} |\{g \in G : g * x = x\}| = \sum_{x \in X} |G_x| = \sum_{x \in X} \frac{|G|}{|G * x|}.$$

Wir wählen nun Repräsentanten für die Orbits. Wir wählen also $x_1, x_2, \ldots, x_n \in X$ so, dass $G * x_i \cap G * x_j = \varnothing$ für $i \neq j$, und $G * x_1 \cup G * x_2 \cup \cdots \cup G * x_n = X$. Alle Elemente y in $G * x_i$ erfüllen $G * y = G * x_i$. Wir verwenden diese Eigenschaft und erhalten

$$\sum_{x \in X} \frac{|G|}{|G * x|} = \sum_{i=1}^{n} |G * x_i| \cdot \frac{|G|}{|G * x_i|} = n \cdot |G|.$$

Die Anzahl der Elemente von F ist also $n \cdot |G|$. Wir erhalten also:

$$\sum_{g \in G} |\operatorname{Fix}(g)| = |G| \cdot n.$$

□

Wir wenden nun das Burnside-Lemma auf die Frage in Problem 8.6 an. Wir berechnen dazu $\operatorname{Fix}(g)$ für alle Elemente $g \in G$. Wir tun das zum Beispiel für $g = (1, 2, 3, 4)$. Eine Färbung α liegt in $\operatorname{Fix}(g)$, falls für alle $z \in \{1, 2, 3, 4\}$ gilt: $\alpha(z) = \alpha(g^{-1}(z))$. Damit gilt: $\alpha(1) = \alpha(4)$, $\alpha(4) = \alpha(3)$, $\alpha(3) = \alpha(2)$, $\alpha(2) = \alpha(1)$. Also liegen in $\operatorname{Fix}(g)$ alle Färbungen, die alle 4 Eckpunkte gleich färben. Das sind, bei drei Farben, genau drei Stück. Für $g = (1, 2)(3, 4)$ liegen genau jene Färbungen in $\operatorname{Fix}(g)$, die $\alpha(1) = \alpha(2)$ und $\alpha(3) = \alpha(4)$ erfüllen. Das sind $3 \cdot 3 = 9$ Stück. Für $g = (1, 3)$ werden genau die Färbungen von g fixiert, bei denen 1 und 3 gleich gefärbt werden. Das sind 27 Färbungen. Das Burnside-Lemma ergibt also für die Anzahl n der Färbungen

$$n = \frac{1}{8}(3^4 + 3^3 + 3^2 + 3^1 + 3^3 + 3^2 + 3^1 + 3^2).$$

Es gibt also 21 verschiedene Färbungen.

Beispiel 8.12. Wir färben ein Sechseck mit den Farben rot und blau so, dass drei Ecken rot und drei Ecken blau sind. Zwei Färbungen des Sechsecks seien gleich, wenn sie durch Drehung ineinander übergeführt werden können. Wieviele Färbungen gibt es?

Die Menge X aller Färbungen mit drei roten Ecken ist gegeben durch

$$X = \{\varphi \mid \varphi : \{1, 2, \ldots, 6\} \to \{r, b\}, |g^{-1}(\{r\})| = 3, |g^{-1}(\{b\})| = 3\}.$$

Auf dieser Menge X operiert die Gruppe G (Untergruppe der S_6) durch

$$g * \varphi(z) := \varphi(g^{-1}(z))$$

Wir suchen die Anzahl der Bahnen der Gruppe G auf X. Nach dem Burnside-Lemma erhalten wir für diese Anzahl $n = \frac{1}{|G|} \sum_{g \in G} |\operatorname{Fix}(g)|$ mit $\operatorname{Fix}(g) = \{\varphi \in X \mid g * \varphi = \varphi\}$.

Welche Permutationen auf $\{1, 2, \ldots, 6\}$ liegen in der "Drehgruppe des Sechsecks"? Wir finden die Drehungen:

$$G = \{(), (123456), (135)(246), (14)(25)(36), (153)(264), (165432)\}.$$

Wir erhalten die Tabelle:

	$\lvert \operatorname{Fix}(g) \rvert$
$1 \times ()$	$\binom{6}{3} = 20$
$2 \times (123456)$	0
$2 \times (135)(246)$	2
$1 \times (14)(25)(36)$	0

Die Anzahl der Bahnen ergibt sich als $n = \frac{1}{6} \cdot (20 + 2 \cdot 2) = 4$.

ÜBUNGSAUFGABEN 8.13.

(1) Wir färben die Ecken eines regelmäßigen Fünfecks mit den Farben rot, blau, und gelb.
   (a) Wieviele Möglichkeiten gibt es, die Ecken zu färben, wenn wir zwei Färbungen als gleich ansehen, wenn sie durch eine Drehung des Fünfecks ineinander übergeführt werden können?
   (b) Wieviele Möglichkeiten gibt es, die Ecken zu färben, wenn wir zwei Färbungen als gleich ansehen, wenn sie durch Drehungen und eine Spiegelungen des Fünfecks ineinander übergeführt werden können. (Hinweis: es gibt jetzt 10 Symmetrieoperationen.)

(2) Wir färben Flächen eines Würfels.
   (a) Wieviele verschiedene Färbungen gibt es, wenn wir zwei Farben nehmen und zwei Färbungen als gleich betrachten, wenn sie durch eine Symmetrieoperation des Würfels ineinander übergeführt werden können. Dabei operiert auf den Flächen $\{1, 2, 3, 4, 5, 6\}$ des Würfels die Untergruppe der S_6, die von

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

   erzeugt wird. Ihre Elemente entnehmen Sie dem folgenden Dialog mit GAP (steht für Groups - Algorithms -Programming, ein in Aachen und St. Andrews entwickeltes, im wesentlichen frei verfügbares Gruppentheoriesystem [**GAP12**]):

```
gap> G := Group ((4,2,3,5), (1,2,6,5), (3,1,4,6));
Group([ (2,3,5,4), (1,2,6,5), (1,4,6,3) ])
gap> Size (G);
24
gap> AsList (G);
[ (), (2,3,5,4), (2,4,5,3), (2,5)(3,4), (1,2)(3,4)(5,6), (1,2,3)(4,6,5),
  (1,2,4)(3,6,5), (1,2,6,5), (1,3,2)(4,5,6), (1,3,6,4), (1,3)(2,5)(4,6),
  (1,3,5)(2,6,4), (1,4,2)(3,5,6), (1,4,6,3), (1,4)(2,5)(3,6),
  (1,4,5)(2,6,3),
  (1,5,6,2), (1,5,4)(2,3,6), (1,5,3)(2,4,6), (1,5)(2,6)(3,4), (1,6)(3,4),
  (1,6)(2,3)(4,5), (1,6)(2,4)(3,5), (1,6)(2,5) ]
```

(b) Wieviele verschiedene Färbungen gibt es mit 3, wieviele mit n Farben?

(3) Auf wieviele verschiedene Arten können Sie die Ecken eines Quadrats mit drei Farben färben, wenn jede Farbe wirklich vorkommen soll? Dabei sind zwei Färbungen gleich, wenn sie durch eine Symmetrieoperation des Quadrats ineinander übergeführt werden können.

```
gap> G := Group ((1,2,3,4), (1,2) (3,4));
Group([ (1,2,3,4), (1,2)(3,4) ])
gap> Size (G);
8
gap> AsList (G);
[ (), (2,4), (1,2)(3,4), (1,2,3,4), (1,3), (1,3)(2,4), (1,4,3,2), (1,4)(2,3) ]
```

(4) Auf wieviele verschiedene Arten können Sie die Ecken eines Quadrats mit drei Farben färben, wenn zwei Färbungen dann als gleich angesehen werden, wenn sie durch Vertauschung der Farben ineinander übergeführt werden können? Das Quadrat dürfen wir dabei nicht bewegen. Außerdem müssen bei einer Färbung nicht alle 3 Farben vorkommen. *Hinweis:* Sie brauchen eine neue Gruppenoperation. Es operiert jetzt die S_3 auf den Färbungen. Aber wie?

```
gap> G := Group ((1,2), (1,2,3));
Group([ (1,2), (1,2,3) ])
gap> AsList (G);
[ (), (2,3), (1,2), (1,2,3), (1,3,2), (1,3) ]
```

2. Der Satz von Sylow

Wegen des Satzes von Lagrange teilt die Ordnung jeder Untergruppe die Gruppenordnung. Der Satz von Sylow garantiert, dass es für bestimmte Teiler der Gruppenordnung tatsächlich Untergruppen dieser Ordnung gibt.

LEMMA 8.14 (Lucas[3]). *Sei p eine Primzahl, und seien $a, m \in \mathbb{N}_0$. Dann gilt $\binom{p^a m}{p^a} \equiv m \pmod{p}$.*

BEWEIS. Im Polynomring $\mathbb{Z}_p[X]$ gilt $(X+1)^p = X^p+1$: wegen des Satzes von Fermat gilt $x^p \equiv x \pmod{p}$ für alle $x \in \mathbb{Z}$; folglich hat das Polynom $(X+1)^p - (X^p+1)$ über $\mathbb{Z}_p$ genau p Nullstellen und Grad $< p$ und ist daher das Nullpolynom. Durch Induktion folgt $(X+1)^{p^k} = X^{p^k} + 1$ für alle $k \in \mathbb{N}_0$.

Wir betrachten nun den Koeffizienten von X^{p^a} in $(X+1)^{p^a m}$. Aus dem binomischen Lehrsatz folgt, dass dieser Koeffizient gleich $[\binom{p^a m}{p^a}]_p$ ist. Nun gilt in $\mathbb{Z}_p[X]$, dass $(X+1)^{p^a m} = ((X+1)^{p^a})^m = (X^{p^a}+1)^m$. Der Koeffizient von X^{p^a} in diesem Polynom ist $[m]_p$. Also gilt $[\binom{p^a m}{p^a}]_p = [m]_p$. □

[3]Édouard Lucas 1842-1891

SATZ 8.15 (Erster Isomorphiesatz). *Sei G eine Gruppe, sei H eine Untergruppe von G und sei N ein Normalteiler von G. Dann ist $HN = \{hn \mid h \in H, n \in H\}$ eine Untergruppe von G, $N \cap H$ ein Normalteiler von H, und die Gruppen $(HN)/N$ und $H/(N \cap H)$ sind isomorph.*

BEWEIS. Für $h_1, h_2 \in H$ und $n_1, n_2 \in N$ gilt

$$h_1 n_1 h_2 n_2 = h_1 h_2 h_2^{-1} n_1 h_2 n_2 = (h_1 h_2)((h_2^{-1} n_1 h_2) n_2) \in HN$$

und

$$(h_1 n_1)^{-1} = n_1^{-1} h_1^{-1} = (h_1^{-1} h_1) n_1^{-1} h_1^{-1} = h_1^{-1}(h_1 n_1^{-1} h_1^{-1}) \in HN.$$

Daher ist HN eine Untergruppe von G. Sei nun $\varphi : H \to HN/N$ gegeben durch $\varphi(h) := hN$. Dann ist φ wegen $\varphi(h) = hN = (hn)N$ surjektiv, und es gilt $\ker(\varphi) = \{h \in H \mid hN = 1N\} = \{h \in H \mid h \in N\} = H \cap N$. Aus dem Homomorphiesatz folgt nun, dass $H \cap N$ ein Normalteiler von H ist, und dass $H/(H \cap N)$ isomorph zu $(HN)/N$ ist. □

DEFINITION 8.16. Sei G eine endliche Gruppe, und sei p eine Primzahl. Eine Untergruppe H von G ist eine *p-Sylow-Untergruppe*, wenn es ein $a \in \mathbb{N}_0$ gibt, sodass $|H| = p^a$ und $p^{a+1} \nmid |G|$.

In einer Gruppe mit 72 Elementen hat eine 5-Sylow-Untergruppe 1 Element, eine 2-Sylow-Untergruppe 8 Elemente, und eine 3-Sylow-Untergruppe 9 Elemente.

SATZ 8.17 (Satz von Sylow[4]). *Sei G eine endliche Gruppe, und sei p eine Primzahl. Dann gilt:*

1. *G besitzt eine p-Sylow-Untergruppe.*
2. *Sei n_p die Anzahl der p-Sylow-Untergruppen von G. Dann gilt $n_p \equiv 1 \pmod{p}$ und $n_p \mid |G|$.*
3. *Für alle p-Sylow-Untergruppen H_1, H_2 gibt es ein $g \in G$ mit $gH_1g^{-1} = H_2$.*
4. *Sei $n \in \mathbb{N}$. Jede Untergruppe von G mit p^n Elementen ist in einer p-Sylow-Untergruppe enthalten.*

BEWEIS. (cf. **[Rob03]**) Seien $a, m \in \mathbb{N}$ so, dass $|G| = p^a m$ und $p \nmid m$.

(1) Es sei

$$\mathcal{S} := \binom{G}{p^a} := \{X \mid X \subseteq G, |X| = p^a\}.$$

Wir definieren eine Gruppenoperation $*_1$ von G auf $\mathcal{S}$ durch $g *_1 X := \{gx \mid x \in X\}$ für $g \in G$, $X \in \mathcal{S}$. Es gilt $|\mathcal{S}| = \binom{p^a m}{p^a}$. Wegen des Satzes von Lucas gilt $p \nmid |\mathcal{S}|$. Da $\mathcal{S}$ die disjunkte Vereinigung aller G-Orbits von G auf $\mathcal{S}$ ist, gibt es einen Orbit $\mathcal{S}_1$ von G auf $\mathcal{S}$, sodass $p \nmid |\mathcal{S}_1|$. Sei nun $X_1 \in \mathcal{S}_1$ und P der Stabilisator G_{X_1} von X_1. Es gilt dann

[4]Peter L. M. Sylow 1832-1918

$|\mathcal{S}_1| = |G *_1 X_1| = |G|/|P|$. Da $p \nmid |\mathcal{S}_1|$, gilt $p^a \mid |P|$. Um zu zeigen, dass $|P| \leq p^a$, wählen wir $x \in X_1$ und betrachten die Abbildung $\varphi : P \to G$, $\varphi(p) = px$. Für jedes $p \in P$ gilt $p *_1 X_1 = X_1$, also gilt $px \in X_1$. Die Abbildung φ ist injektiv: wenn $p_1 x = p_2 x$, so gilt $p_1 = p_1 x x^{-1} = p_2 x x^{-1} = p_2$. Somit gilt $|P| \leq |X_1| = p^a$. Also gilt insgesamt $|P| = p^a$. Wir fixieren diese p-Sylow-Untergruppe P jetzt für den Rest des Beweises.

(4) Sei

$$\mathcal{T} := \{gPg^{-1} \mid g \in G\}.$$

Wir definieren nun eine Gruppenoperation $*_2$ von P auf $\mathcal{T}$ durch $h *_2 S := hSh^{-1}$ für $h \in P$, $S \in \mathcal{T}$. Der Orbit von P ist $\{P\}$, da für alle $h \in P$ gilt, dass $hPh^{-1} = P$. Wir zeigen nun, dass $\{P\}$ der einzige einelementige Orbit der Gruppenoperation $*_2$ ist. Sei dazu $P_1 \in \mathcal{T}$ so, dass $hP_1h^{-1} = P_1$ für alle $h \in P$ gilt. Sei $N := \{g \in G \mid gP_1g^{-1} = P_1\}$. Dann ist N eine Untergruppe von G, $P_1 \subseteq N$, und P_1 ist ein Normalteiler von N. Aufgrund der Annahme $\forall h \in P : hP_1h^{-1} = P_1$ gilt $P \subseteq N$. Somit ist wegen Satz 8.15 das Produkt PP_1 eine Untergruppe von N, und es gilt $|PP_1/P_1| = P/(P_1 \cap P)$. Also ist die Anzahl der Elemente von PP_1 eine Potenz von p. Wegen $P \subseteq PP_1$ gilt daher $PP_1 = P$. Also gilt $P_1 \subseteq P$, und somit $P_1 = P$. Somit ist $\{P\}$ der einzige einelementige Orbit von P auf $\mathcal{T}$. Da wegen Satz 8.10 die Größe eines Orbits immer ein Teiler der Gruppenordnung, also von $|P|$ ist, haben alle anderen Orbits eine durch p teilbare Anzahl von Elementen. Somit erhalten wir

$$|\mathcal{T}| \equiv 1 \pmod{p}. \tag{8.1}$$

Wir zeigen nun:

> Für alle $n \in \mathbb{N}$ und alle Untergruppen P_2 von G mit p^n Elementen gibt es $P_3 \in \mathcal{T}$ mit $P_2 \subseteq P_3$.

Sei dazu $n \in \mathbb{N}_0$ und P_2 eine Untergruppe von G mit p^n Elementen. P_2 operiert auf $\mathcal{T}$ durch $h *_3 S := hSh^{-1}$ für $h \in P_2, S \in \mathcal{T}$. Wegen (8.1) können nicht alle Orbits von $*_3$ ein Vielfaches von p an Elementen haben. Da die Größe jedes Orbits ein Teiler von $|P_2|$ und somit eine Potenz von p ist, gibt es also $P_3 \in \mathcal{T}$, sodass $\{P_3\}$ ein Orbit von P_2 auf $\mathcal{T}$ ist. Es gilt also für alle $g \in P_2 : gP_3g^{-1} = P_3$. Somit ist P_2 eine Teilmenge von $N_1 := \{g \in G \mid gP_3g^{-1} = P_3\}$. Es gilt $P_3 \subseteq N_1$ und auch, dass P_3 ein Normalteiler von N_1 ist. Also ist P_2P_3 eine Untergruppe von G, und P_2P_3/P_3 ist isomorph zu $P_2/(P_2 \cap P_3)$. Somit ist die Anzahl der Elemente von P_2P_3 eine Potenz von p, und wegen $|P_3| = p^a$ gilt sogar $P_2P_3 = P_3$, also $P_2 \subseteq P_3$. Somit ist P_2 in einem Element von $\mathcal{T}$ als Untergruppe enthalten. Das beweist (4).

(2) Sei H eine p-Sylow-Untergruppe. Wegen (4) gibt es $g \in G$ mit $H \subseteq gPg^{-1}$. Da $|H| = p^a = |gPg^{-1}|$, gilt $H = gPg^{-1}$. Folglich ist jede p-Sylow-Untergruppe von G in $\mathcal{T}$ enthalten. Wegen (8.1) gilt nun $n_p \equiv 1 \pmod{p}$. Wir betrachten nun die Gruppenoperation $*_4$ von G auf $\mathcal{T}$, die durch $g *_4 T := gTg^{-1}$ gegeben ist. $\mathcal{T}$ besitzt nur einen einzigen Orbit bezüglich $*_4$, daher gilt $|\mathcal{T}| \mid |G|$ und somit $n_p \mid |G|$. Das beweist (2).

(3) Seien H_1, H_2 p-Sylow-Untergruppen von G. Dann gilt $H_1 \in \mathcal{T}$ und $H_2 \in \mathcal{T}$, also gibt es $g_1, g_2 \in G$ mit $H_1 = g_1 P g_1^{-1}$ und $H_2 = g_2 P g_2^{-1}$. Insgesamt gilt dann $H_1 = g_1 g_2^{-1} H_2 (g_1 g_2^{-1})^{-1}$. □

KAPITEL 9

Generatoren für Permutationsgruppen

Wir betrachten Untergruppen der S_n, die durch ihre Generatoren gegeben sind, zum Beispiel durch $a := (1,2)(3,4)$, $b := (1,5,6)$. Eine grundlegende Frage ist, wie viele der $n!$ Elemente der S_n in der Untergruppe $G := \langle a, b\rangle$ liegen. Man könnte die Elemente aufzählen. Wesentlich schneller kann man dieses Problem aber durch folgende Beobachtungen lösen:

(1) G operiert auf $\{1,\dots,n\}$ durch $g * x := g(x)$.
(2) Für alle $x \in \{1,\dots,n\}$ gilt $|G| = |G * x| \cdot |G_x|$.
(3) Der Orbit von 1 ist $\{1,2,5,6\}$.
(4) *Das Lemma von Schreier*, das Generatoren des Stabilisators G_1 von 1 liefert.

Sei dazu G eine Gruppe und H eine Untergruppe von G. Eine Teilmenge T ist eine *Transversale* durch die Linksnebenklassen von H, wenn für alle $g \in G$ gilt: $|T \cap (gH)| = 1$. Für jedes $g \in G$ bezeichnen wir mit $\overline{g}$ jenes Element aus T, das $\overline{g}H = gH$ erfüllt.

Satz 9.1 (Lemma von Schreier[1]). *Sei G eine Gruppe, sei S eine Teilmenge von G mit $\langle S\rangle = G$ und sei H eine Untergruppe von G. Sei T eine Transversale durch die Linksnebenklassen von H mit $1 \in T$. Dann gilt $H = \langle\{\overline{st}^{-1}st \mid s \in S, t \in T\}\rangle$.*

Beweis. Sei $U := \{\overline{st}^{-1}st \mid s \in S, t \in T\}$. Wir zeigen als erstes durch Induktion, dass es für alle $n \in \mathbb{N}$, alle $\varepsilon_1,\dots,\varepsilon_n \in \{-1,+1\}$ und alle $s_1,\dots,s_n \in S$ Elemente $u_1,\dots,u_n \in U$ und $t \in T$ gibt, sodass

$$s_1^{\varepsilon_1}\cdots s_n^{\varepsilon_n} = tu_1^{\varepsilon_1}\cdots u_n^{\varepsilon_n}.$$

Für $n = 0$ setzen wir $t := 1$. Sei nun $n \geq 1$. Nach Induktionsvoraussetzung gibt es $t_1 \in T$ und $u_2,\dots,u_n \in U$, sodass

$$s_2^{\varepsilon_2}\cdots s_n^{\varepsilon_n} = t_1u_2^{\varepsilon_2}\cdots u_n^{\varepsilon_n}.$$

Im Fall $\varepsilon_1 = 1$ verwenden wir $s_1t_1 = \overline{s_1t_1}\,\overline{s_1t_1}^{-1}s_1t_1$. Wir setzen $t := \overline{s_1t_1}$ und $u_1 := \overline{s_1t_1}^{-1}s_1t_1$ und erhalten $s_1t_1 = tu_1$ und somit $s_1^{\varepsilon_1}\cdots s_n^{\varepsilon_n} = s_1s_2^{\varepsilon_2}\cdots s_n^{\varepsilon_n} = s_1t_1u_2^{\varepsilon_2}\cdots u_n^{\varepsilon_n} = tu_1u_2^{\varepsilon_2}\cdots u_n^{\varepsilon_n} = tu_1^{\varepsilon_1}u_2^{\varepsilon_2}\cdots u_n^{\varepsilon_n}$.

[1] Otto Schreier 1901-1929

Im Fall $\varepsilon_1 = -1$ beobachten wir zunächst, dass $(s_1^{-1}t_1)H = \overline{s_1^{-1}t_1}H$, und somit $t_1 H = (s_1 s_1^{-1} t_1)H = s_1 \overline{s_1^{-1}t_1} H$ und folglich $t_1 = \overline{s_1 \overline{s_1^{-1}t_1}}$. Also gilt

$$s_1^{-1}t_1 = \overline{s_1^{-1}t_1}\,\overline{s_1^{-1}t_1}^{-1} s_1^{-1}t_1 = \overline{s_1^{-1}t_1}\left(t_1^{-1}s_1\overline{s_1^{-1}t_1}\right)^{-1} = \overline{s_1^{-1}t_1}\left(\overline{s_1\overline{s_1^{-1}t_1}}^{-1} s_1\overline{s_1^{-1}t_1}\right)^{-1}.$$

Wir setzen $t := \overline{s_1^{-1}t_1}$ und $u_1 := \overline{s_1\overline{s_1^{-1}t_1}}^{-1} s_1\overline{s_1^{-1}t_1}$. Nun gilt $u_1 \in U$ und $s_1^{-1}t_1 = tu_1^{-1}$, und somit insgesamt $s_1^{\varepsilon_1}\cdots s_n^{\varepsilon_n} = tu_1^{\varepsilon_1}\cdots u_n^{\varepsilon_n}$.

Wir zeigen nun, dass $\langle U\rangle = H$. Für $\subseteq$ wählen wir $u = \overline{st}^{-1}st \in U$. Da $\overline{st}\,H = st\,H$, gilt auch $1\,H = \overline{st}^{-1}st\,H = uH$. Also gilt $u \in H$. Für $\supseteq$ wählen wir $h \in H$ und finden $n \in \mathbb{N}$, $t \in T$, $u_1, \ldots, u_n \in U$ und $\varepsilon_1, \ldots, \varepsilon_n \in \{-1, 1\}$ mit $h = tu_1^{\varepsilon_1}u_2^{\varepsilon_2}\cdots u_n^{\varepsilon_n}$. Da alle u_i in H liegen, gilt auch $t \in H$, und somit $t = 1$. Also gilt $h = u_1^{\varepsilon_1}u_2^{\varepsilon_2}\cdots u_n^{\varepsilon_n} \in \langle U\rangle$. □

Als Beispiel betrachten wir die Untergruppe der S_6, die von $a := (1,2)(3,4)$ und $b := (1,5,6)$ erzeugt wird. Wir bestimmen mithilfe des Lemmas von Schreier Generatoren für den Stabilisator G_1 von G. Der Orbit $G * 1$ ist $O_1 := \{1,2,5,6\}$. Repräsentanten für die Nebenklassen von G_1 sind $\{1, a, b, b^2\}$. Nun gilt zum Beispiel für $s := a$ und $t := b$, dass $\overline{st}^{-1}st = \overline{ab}^{-1}ab$. Wegen $ab * 1 = 5$ gilt $\overline{ab} = b$, also gilt $\overline{ab}^{-1}ab = b^{-1}ab = (2,6)(3,4)$. Insgesamt erhält man für die Generatoren von G_1 die Menge $S_1 := \{(2,5,6), (2,5)(3,4), (2,6)(3,4)\}$. Es gilt also $|G| = |G_1| \cdot |O_1| = 4\,|G_1| = 4\,|\langle S_1\rangle|$.

Wir berechnen nun die Ordnung der Gruppe $G_1 = \langle S_1\rangle$ durch $|G_1| = |(G_1)_2| \cdot |O_2|$, wobei $(G_1)_2$ der Stabilisator von 2 in G_1 ist. Der Orbit von 2 ist $O_2 = \{2,5,6\}$, Repräsentanten sind $R_2 = \{(), (2,5,6), (2,6,5)\}$. Durch das Lemma von Schreier erhält man $(G_1)_2 = \langle (3,4)(5,6)\rangle$.

Durch Fortsetzen dieses Verfahrens erhalten wir $((G_1)_2)_3 = \{()\}$ und somit $|(G_1)_2| = 1 \cdot |\{3,4\}| = 2$, also $|G_1| = 2 \cdot |O_2| = 2 \cdot 3$ und somit $|G| = 2 \cdot 3 \cdot 4 = 24$.

Eventuell erhält man bei diesem Verfahren sehr viele Generatoren für die auftretenden Stabilisatoren. Diese Generatoren kann man etwa mit "Jerrums Filter" (cf. **[Cam99]**) reduzieren.

Literaturverzeichnis

[Buc82] B. Buchberger, *Algebraic simplification*, Computer algebra – symbolic and algebraic computation (B. Buchberger, G.E. Collins, and R. Loos, eds.), Springer-Verlag Wien, 1982, pp. 11–43.

[Cam99] P. J. Cameron, *Permutation groups*, London Mathematical Society Student Texts, vol. 45, Cambridge University Press, Cambridge, 1999.

[GAP12] The GAP Group, *GAP – Groups, Algorithms, and Programming, Version 4.5.6*, 2012.

[Kau22] M. Kauers, *Lineare Algebra und Analytische Geometrie*, Lecture notes for a course at JKU Linz, Austria, 2022.

[KB70] D. E. Knuth and P. B. Bendix, *Simple word problems in universal algebras*, Computational Problems in Abstract Algebra (Proc. Conf., Oxford, 1967), Pergamon, Oxford, 1970, pp. 263–297.

[LP98] R. Lidl and G. F. Pilz, *Applied abstract algebra*, second ed., Springer-Verlag, New York, 1998.

[Rob03] D. J. S. Robinson, *An introduction to abstract algebra*, Walter de Gruyter, Berlin – New York, www.deGruyter.com, 2003.

[RU87] R. Remmert and P. Ullrich, *Elementare Zahlentheorie*, Birkhäuser Verlag, Basel, 1987.