JOHANNES KEPLER
UNIVERSITÄT LINZ | JKU

Unterlagen zur Vorlesung

Einführung in die Algebra und Diskrete Mathematik

Sommersemester 2012

Erhard Aichinger
Institut für Algebra
Johannes Kepler Universität Linz

Version 17. April 2012

Adresse:

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

Version 8.3.2012

Druck: Kopierstelle, Abteilung Service, Universität Linz

Inhaltsverzeichnis

KAPITEL 1

Elementare Zahlentheorie

Wir kürzen die Menge der ganzen Zahlen mit $\mathbb{Z}$ und die Menge $\{1, 2, 3, \ldots\}$ der natürlichen Zahlen mit $\mathbb{N}$ ab.

1. Primfaktorzerlegung

DEFINITION 1.1 (Primzahl). Eine Zahl $p \in \mathbb{N}$ ist genau dann eine *Primzahl*, wenn $p > 1$, und für alle $a, b \in \mathbb{N}$ mit $p = a \cdot b$ gilt, dass $a = 1$ oder $b = 1$.

DEFINITION 1.2 (Teilbarkeit). Seien $x, y \in \mathbb{Z}$. Die Zahl x *teilt* y genau dann, wenn es ein $z \in \mathbb{Z}$ gibt, sodass $y = z \cdot x$ ist.

Wir schreiben dann auch $x \mid y$, und die Zahl y ist ein *Vielfaches* von x.

DEFINITION 1.3 (Ideal). Eine Teilmenge I von $\mathbb{Z}$ ist ein *Ideal* von $\mathbb{Z}$, wenn

(1) $I \neq \emptyset$.
(2) Für alle $i, j \in I$ liegt auch $i - j$ in I.
(3) Für alle $z \in \mathbb{Z}$ und alle $i \in I$ liegt auch $z \cdot i$ in I.

BEISPIELE 1.4.

(1) Die Menge $\{z \cdot 2 \mid z \in \mathbb{Z}\}$ ist ein Ideal von $\mathbb{Z}$.
(2) Die Menge $\{z \cdot 5 \mid z \in \mathbb{Z}\}$ ist ein Ideal von $\mathbb{Z}$.
(3) Die Menge $\{0\}$ ist ein Ideal von $\mathbb{Z}$.
(4) $\mathbb{N}$ ist kein Ideal von $\mathbb{Z}$.

SATZ 1.5. *Sei I ein Ideal von $\mathbb{Z}$. Dann gibt es ein $a \in I$, sodass*

$$I = \{z \cdot a \mid z \in \mathbb{Z}\}. \tag{1.1}$$

Beweis: Sei I ein Ideal von $\mathbb{Z}$. Wir wollen ein $a \in I$ finden, sodass (1.1) erfüllt ist.

- *1. Fall: I enthält kein Element ungleich* 0*:* Dann gilt $I = \{0\}$, und wir wählen $a = 0$.
- *2. Fall: I enthält ein Element ungleich* 0*:* Dann gibt es auch ein $b \in I$ mit $b > 0$. Wir definieren a durch

$$a := \min\{b \in I \mid b > 0\}.$$

Nun zeigen wir, dass a das gewünschte Element ist, d.h., wir zeigen:

$$I = \{z \cdot a \mid z \in \mathbb{Z}\}. \tag{1.2}$$

"$\supseteq$": Sei x ein Element aus der Menge auf rechten Seite von (1.2). Dann gibt es ein $z \in \mathbb{Z}$, sodass $x = z \cdot a$. Nun liegt a in I, da wir ja a als ein Element von I ausgewählt haben. Wegen der Idealeigenschaft (2) aus Definition 1.3 liegt auch $z \cdot a$ in I. Somit liegt $x = z \cdot a$ auch in der linken Seite von (1.2).

"$\subseteq$": Wir fixieren $c \in I$ und zeigen, dass c ein Vielfaches von a ist. Durch Division erhalten wir $q \in \mathbb{Z}$, $r \in \{0, 1, \ldots, a-1\}$, sodass

$$c = q \cdot a + r.$$

Daher ist $r = c - q \cdot a$. Nun liegt c in I; ebenso liegt $a \in I$. Daher liegen auch $q \cdot a$ und $c - q \cdot a$ in I. Somit folgt, dass auch $r \in I$ liegt. Wegen $r < a$ folgt aus der Minimalität von a, dass $r = 0$ ist. Daher ist c ein Vielfaches von a. ■

Wir schreiben für $\{a \cdot z \mid z \in \mathbb{Z}\}$ auch $a \cdot \mathbb{Z}$ oder (a) und bezeichnen es als *das von a erzeugte Ideal*. Für ein Ideal I heißt jedes $b \in \mathbb{Z}$ mit $I = b \cdot \mathbb{Z}$ auch *erzeugendes Element* von I.

SATZ 1.6 (Fundamentallemma). *Sei p eine Primzahl, und seien $a, b \in \mathbb{Z}$. Falls p ein Produkt $a \cdot b$ teilt, so teilt p einen der beiden Faktoren a oder b.*

Beweis: Wir definieren I durch $I := \{x \in \mathbb{Z} : p \text{ teilt } a \cdot x\}$. Wir zeigen zunächst, dass I ein Ideal ist. Die Idealeigenschaften (1) und (2) aus Definition (1.3) folgen daraus, dass für alle $x_1, x_2 \in I$ und $u, v \in \mathbb{Z}$ auch $u \cdot x_1 + v \cdot x_2$ in I liegt. Das gilt, weil p, falls es $a \cdot x_1$ und $a \cdot x_2$ teilt, auch $a \cdot (u \cdot x_1 + v \cdot x_2)$ teilt. Wegen $0 \in I$ ist I nicht die leere Menge.

Das Ideal I besitzt ein erzeugendes Element c. Da wegen $p \in I$ das Ideal I nicht gleich $\{0\}$ ist, können wir $c > 0$ wählen. Wir erhalten also $I = (c)$.

Nun liegt p aber in I. Daher gibt es ein $z \in \mathbb{Z}$, sodass $p = z \cdot c$. Da p und c in $\mathbb{N}$ liegen, ist dieses z positiv. Da p prim ist, ist $z = 1$ oder $c = 1$.

- *1. Fall: $z = 1$:* Dann gilt $p = c$. Da laut Voraussetzung p die Zahl $a \cdot b$ teilt, gilt $b \in I$. Das heißt $b \in (c)$. Also ist b Vielfaches von $c = p$; p teilt also b.
- *2. Fall: $c = 1$:* Dann liegt 1 in I. Aus der Definition von I erhalten wir

$$p \mid a \cdot 1.$$

Somit teilt p die Zahl a. ■

SATZ 1.7 (Existenz und Eindeutigkeit der Primfaktorzerlegung). *Sei $\langle p_i \mid i \in \mathbb{N}\rangle = (2, 3, 5, 7, 11, \ldots)$ die Folge aller Primzahlen, und sei $n \in \mathbb{N}$. Dann gibt es genau eine Funktion $\alpha : \mathbb{N} \to \mathbb{N}_0$ mit folgenden Eigenschaften:*

(1) $\{i \in \mathbb{N} \mid \alpha(i) > 0\}$ *ist endlich.*
(2) $n = \prod_{i \in \mathbb{N}} p_i^{\alpha(i)}$.

Beweis: Wir zeigen zunächst durch Induktion nach n, dass es ein solches α gibt. Für $n = 1$ setzen wir $\alpha(i) := 0$ für alle $i \in \mathbb{N}$. Für $n > 1$ sei q der kleinste Teiler von n mit $q > 1$. Die Zahl q ist eine Primzahl; es gibt also $j \in \mathbb{N}$ mit $q = p_j$. Nach Induktionsvoraussetzung gibt es $\beta : \mathbb{N} \to \mathbb{N}_0$ mit

$$\frac{n}{q} = \prod_{i \in \mathbb{N}} p_i^{\beta(i)},$$

also gilt $n = p_j^{\beta(j)+1} \cdot \prod_{i \in \mathbb{N}\setminus\{j\}} p_i^{\beta(i)}$.

Nun zeigen wir die Eindeutigkeit. Seien $\alpha, \beta : \mathbb{N} \to \mathbb{N}_0$ so, dass $\{i \in \mathbb{N} \mid \alpha(i) > 0\}$ und $\{i \in \mathbb{N} \mid \beta(i) > 0\}$ beide endlich sind und

$$\prod_{i \in \mathbb{N}} p_i^{\alpha(i)} = \prod_{i \in \mathbb{N}} p_i^{\beta(i)}.$$

Wir zeigen, dass für alle $j \in \mathbb{N}$ gilt: $\alpha(j) = \beta(j)$. Sei dazu $j \in \mathbb{N}$. Wir nehmen an $\alpha(j) > \beta(j)$. Dann gilt

$$p_j^{\alpha(j)-\beta(j)} \prod_{i \in \mathbb{N}\setminus\{j\}} p_i^{\alpha(i)} = \prod_{i \in \mathbb{N}\setminus\{j\}} p_i^{\beta(i)}.$$

Nach Satz 1.6 teilt p_j also ein $p_i^{\beta(i)}$ mit $i \neq j$. Im Fall $\beta(i) = 0$ widerspricht das $p_j > 1$, im Fall $\beta(i) > 0$ gilt $p_j \mid p_i$. Da p_i eine Primzahl ist, gilt dann $p_i = p_j$, im Widerspruch zu $i \neq j$. ■

ÜBUNGSAUFGABEN 1.8.

(1) [**RU87**, p. 28] Sei p_n die n-te Primzahl, d. h. $p_1 = 2$, $p_2 = 3$, usw. Zeigen Sie

$$p_n \leq 2^{(2^{n-1})}.$$

Hinweis: Euklids Beweis, dass es unendlich viele Primzahlen gibt ([**Euk91**, Buch IX, Satz 20], 270 v.Chr.) beruht auf folgender Überlegung: Seien $q_1, q_2, \ldots, q_n$ Primzahlen. Dann ist der kleinste positive Teiler von $q_1 \cdot q_2 \cdots q_n + 1$ eine Primzahl, die von allen q_i verschieden ist.

(2) Sei p_n die n-te Primzahl, d. h. $p_1 = 2$, $p_2 = 3$, usw. Zeigen Sie, auch, ohne die Eindeutigkeit der Primfaktorzerlegung zu verwenden, dass folgendes gilt: Wenn

$$\begin{aligned} a &= \Pi\, p_i^{\alpha_i} \\ b &= \Pi\, p_i^{\beta_i}, \end{aligned}$$

wobei $\alpha_i, \beta_i \in \mathbb{N}_0$, und fast alle $\alpha_i, \beta_i = 0$ sind, dann gilt $a \mid b$ genau dann, wenn für alle $i \in \mathbb{N}$ gilt, dass $\alpha_i \leq \beta_i$ ist. (Zeigen Sie, dass diese Aussage für alle Primfaktorzerlegungen von a und b gilt. Folgt daraus die Eindeutigkeit der Primfaktorzerlegung?)

(3) Welche Zahlen $q \in \mathbb{N}$ erfüllen folgende Eigenschaft?
Für alle $a, b \in \mathbb{Z}$ mit $q \mid a \cdot b$ gilt $q \mid a$ oder es gibt ein $n \in \mathbb{N}$, sodass $q \mid b^n$.

(4) Zeigen Sie, dass der Durchschnitt beliebig vieler Ideale von $\mathbb{Z}$ wieder ein Ideal von $\mathbb{Z}$ ist.

2. Der größte gemeinsame Teiler

In diesem Abschnitt werden wir eine Methode vorstellen, den größten unter allen gemeinsamen Teilern zweier Zahlen zu finden: den *Euklidischen ggT-Algorithmus*.

DEFINITION 1.9 (Größter gemeinsamer Teiler). Für zwei Zahlen $a, b \in \mathbb{Z}$ (nicht beide 0) ist $\mathrm{ggT}(a, b)$ die größte Zahl $z \in \mathbb{N}$ mit $z \mid a$ und $z \mid b$.

Erstaunlicherweise lässt sich der ggT zweier Zahlen immer als Linearkombination dieser Zahlen schreiben.

SATZ 1.10. *Seien $a, b \in \mathbb{Z}$ (nicht beide 0). Dann gilt:*

(1) *Es gibt $u, v \in \mathbb{Z}$, sodass* $\mathrm{ggT}(a, b) = u \cdot a + v \cdot b$.
(2) *Der ggT ist nicht nur der größte der gemeinsamen Teiler, er ist auch Vielfaches jedes gemeinsamen Teilers.*

Die zweite Bedingung bedeutet, dass für alle $t \in \mathbb{Z}$ mit $t \mid a$ und $t \mid b$ automatisch auch $t \mid \mathrm{ggT}(a, b)$ erfüllt ist.

Beweis von Satz 1.10: Sei I definiert durch

$$I = \{ua + vb \mid u, v \in \mathbb{Z}\}.$$

I ist ein Ideal von $\mathbb{Z}$. Sei c ein positives erzeugendes Element von I. Wegen $a \in I$ gilt, dass a Vielfaches von c ist. Ebenso gilt $c \mid b$.

Wir zeigen nun, dass c nicht nur ein gemeinsamer Teiler von a und b ist, sondern dass c auch ein Vielfaches jedes weiteren gemeinsamen Teilers ist. Sei also $t \in \mathbb{N}$ eine Zahl, die a und b teilt. Es gilt: $a \in (t)$ und $b \in (t)$. Falls a und b in (t) liegen, muss aber jedes Element aus I in (t) liegen. Das gilt, weil (t) die Idealeigenschaften (1) und (2) von Definition 1.3 erfüllt. Es gilt also

$$I \subseteq (t).$$

Insbesondere liegt dann c in (t). Daher gilt $t \mid c$.

Die Zahl c wird also von jedem weiteren gemeinsamen Teiler von a und b geteilt, und ist somit der größte gemeinsame Teiler. ■

SATZ 1.11. *Seien $a, b, c \in \mathbb{Z}$, sodass* $\mathrm{ggT}(a, b) = 1$. *Falls $a \mid b \cdot c$, dann gilt auch $a \mid c$.*

Beweis: Es gibt $u, v \in \mathbb{Z}$, sodass

$$1 = u \cdot a + v \cdot b.$$

Weil $a \mid uac$, und da wegen $a \mid bc$ auch $a \mid vbc$ gilt, gilt auch

$$a \mid (ua + vb)c;$$

also auch $a \mid c$. ■

ÜBUNGSAUFGABEN 1.12.

(1) Seien $a, b, x \in \mathbb{N}$ und $u, v \in \mathbb{Z}$ so, dass
$$x = ua + vb.$$
Zeigen Sie: Wenn x sowohl a als auch b teilt, so gilt $x = \mathrm{ggT}(a, b)$.

(2) Seien $a, b \in \mathbb{N}$, $y \in \mathbb{Z}$ so, dass $a \mid y$, $b \mid y$, $\mathrm{ggT}(a,b) = 1$. Zeigen Sie (ohne Primfaktorzerlegung): $a \cdot b \mid y$.
(3) Seien $a, b \in \mathbb{Z}$ (nicht beide 0), und sei $k \in \mathbb{N}$. Zeigen Sie: $\mathrm{ggT}(ka, kb) = k\mathrm{ggT}(a,b)$. Gelingt es Ihnen, $\mathrm{ggT}(ka, kb) \mid \mathrm{ggT}(a,b)$ auch ohne Verwendung der Primfaktorenzerlegung zu zeigen?
(4) Seien $a, c \in \mathbb{Z}$, $b, d \in \mathbb{N}$. Zeigen Sie: Wenn die Brüche $\frac{a}{b}$ und $\frac{c}{d}$ gekürzt, und die Nenner b und d teilerfremd sind, so ist auch der Bruch $\frac{ad+bc}{bd}$ gekürzt.
(5) Sei $n \in \mathbb{N}$, und seien $a_1, a_2, \ldots, a_n$ in $\mathbb{N}$. Wir definieren G_1, G_2 und G_3 durch:
   (a) $G_1(a_1) := a_1$, $G_1(a_1, a_2, \ldots, a_n) = \mathrm{ggT}(G_1(a_1, a_2, \ldots, a_{n-1}), a_n)$.
   (b) $G_2(a_1, a_2, \ldots, a_n) := \max\{z \in \mathbb{N} : z \mid a_i \text{ für alle } i \in \{1, 2, \ldots, n\}\}$.
   (c) $G_3 := \min\{z \in \mathbb{N} : \text{ es gibt } \lambda_1, \lambda_2, \ldots, \lambda_n \in \mathbb{Z}, \text{ sodass } z = \sum_{i=1}^{n} \lambda_i a_i\}$.
   Zeigen Sie, dass G_1, G_2 und G_3 gleich sind.
(6) Sei p_n die n-te Primzahl, d. h. $p_1 = 2$, $p_2 = 3$, usw. Zeigen Sie, auch, ohne die Eindeutigkeit der Primfaktorzerlegung zu verwenden, dass folgendes gilt: Wenn

$$\begin{aligned} a &= \prod p_i^{\alpha_i} \\ b &= \prod p_i^{\beta_i}, \end{aligned}$$

wobei $\alpha_i, \beta_i \in \mathbb{N}_0$, und fast alle $\alpha_i, \beta_i = 0$ sind, dann gilt

$$\mathrm{ggT}(a,b) = \prod p_i^{\min(\alpha_i, \beta_i)}.$$

Es ist einfach, aus den Primfaktorzerlegungen von a und b den ggT von a und b zu bestimmen. Es kann aber sehr rechenaufwendig sein, die Primfaktorzerlegung einer Zahl zu bestimmen. Schneller kann man den ggT mit dem *Euklidischen Algorithmus* berechnen, der ohne die Primfaktorzerlegungen auskommt.

SATZ 1.13. *Seien $a, b \in \mathbb{Z}$, nicht beide 0 und sei $z \in \mathbb{Z}$. Dann gilt:*

$$\mathrm{ggT}\,(a,b) = \mathrm{ggT}\,(a + z \cdot b, b)\,.$$

So gilt zum Beispiel $\mathrm{ggT}\,(25,15) = \mathrm{ggT}\,(40,15)$.

Beweis: Wir zeigen, dass nicht nur der ggT, sondern sogar die Mengen der gemeinsamen Teiler der beiden Zahlenpaare gleich sind. Wir zeigen also

$$\{t \,:\, t \mid a \text{ und } t \mid b\} = \{t \,:\, t \mid a + zb \text{ und } t \mid b\}\,.$$

"$\subseteq$": Falls t sowohl a als auch b teilt, dann auch $a + zb$ und b. "$\supseteq$": Falls t sowohl $a + zb$, als auch b teilt, dann auch $a + zb - zb$ und b, also auch a und b.■

Das nützen wir jetzt möglichst geschickt aus, um $\mathrm{ggT}(147, 33)$ zu berechnen:

$$\begin{aligned} \mathrm{ggT}\,(147,33) &= \mathrm{ggT}\,(147 - 4 \cdot 33, 33) \\ &= \mathrm{ggT}\,(15, 33) \\ &= \mathrm{ggT}\,(15, 33 - 2 \cdot 15) \\ &= \mathrm{ggT}\,(15, 3) \\ &= \mathrm{ggT}\,(0, 3) \\ &= 3. \end{aligned}$$

Günstig ist es also, z so zu wählen, dass $a + zb$ der Rest von a bei der Division durch b wird.

Mit Hilfe des erweiterten Euklidischen Algorithmus findet man nicht nur den ggT von a und b, sondern auch $u, v \in Z$, sodass gilt:

$$ggT\,(a,b) = u \cdot a + v \cdot b.$$

BEISPIEL 1.14. Berechnen wir nochmals ggT(147, 33), und schreiben dies 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	$(15 = 1 \cdot 146 - 4 \cdot 33)$
3	-2	9	$(3 = -2 \cdot 147 + 9 \cdot 33)$
0			

ÜBUNGSAUFGABEN 1.15.

(1) Bestimmen Sie für a und b jeweils ggT(a, b), und zwei ganze Zahlen $u, v \in \mathbb{Z}$, sodass

$$\text{ggT}(a,b) = u \cdot a + v \cdot b.$$

(a) $a = 254$, $b = 120$.
(b) $a = 71$, $b = 79$.
(c) $a = 610$, $b = 987$.

3. Das kleinste gemeinsame Vielfache

Sind $a, b \in \mathbb{Z}$, so nennt man jede Zahl $c \in \mathbb{Z}$, die von a und b geteilt wird, ein gemeinsames Vielfaches von a und b. Unter allen gemeinsamen Vielfachen zeichnen wir das kleinste aus.

DEFINITION 1.16. Es seien $a, b \in \mathbb{Z} \setminus \{0\}$. Dann ist kgV (a, b) definiert durch

$$\text{kgV}\,(a,b) = \min\{v \in \mathbb{N} \,:\, a \mid v \text{ und } b \mid v\}.$$

Die Menge aller positiven gemeinsamen Vielfachen ist ja für $a, b \in \mathbb{Z} \setminus \{0\}$ nicht leer, da sie $|a \cdot b|$ enthält.

SATZ 1.17. *Seien $a, b \in \mathbb{Z}\setminus\{0\}$, und sei $s \in \mathbb{Z}$ so, dass $a \mid s$ und $b \mid s$. Dann gilt:* kgV $(a, b) \mid s$. *Jedes gemeinsame Vielfache ist also ein Vielfaches des* kgV.

Beweis: Wir betrachten $(a) = \{a \cdot z \,|\, z \in \mathbb{Z}\}$ und $(b) = \{b \cdot z \,|\, z \in \mathbb{Z}\}$. Der Durchschnitt zweier Ideale ist wieder ein Ideal, und da (a) und (b) Ideale sind, ist $(a) \cap (b)$ auch ein Ideal. Es gibt also $c \in \mathbb{Z}$, sodass

$$(c) = (a) \cap (b).$$

Wegen $c \in (a)$ ist c ein Vielfaches von a, und ebenso ein Vielfaches von b. Sei nun s ein weiteres gemeinsames Vielfaches von a und b. Da s in $(a) \cap (b)$ liegt, liegt s auch in (c), und ist somit Vielfaches von c. Also ist c das *kleinste* gemeinsame Vielfache und

teilt jedes gemeinsame Vielfache von a und b. ■

Zwischen ggT und kgV kann man folgenden Zusammenhang herstellen:

SATZ 1.18. *Seien $a, b \in \mathbb{N}$. Dann gilt* $\mathrm{ggT}(a,b) \cdot \mathrm{kgV}(a,b) = a \cdot b$.

Beweis: Wir verwenden die Primfaktorzerlegung von $a = \prod p_i^{\nu_i}$, und $b = \prod p_i^{\sigma_i}$. Aus dem Fundamentallemma (Satz 1.6) (bzw. Übung 1.12 (6)) kann man herleiten, dass dann gelten muss:

$$\begin{aligned} \mathrm{ggT}(a,b) &= \prod p_i^{\min(\nu_i,\sigma_i)} \\ \mathrm{kgV}(a,b) &= \prod p_i^{\max(\nu_i,\sigma_i)}. \end{aligned}$$

Daraus folgt:

$$\begin{aligned} \mathrm{ggT}(a,b) \cdot \mathrm{kgV}(a,b) &= \prod p_i^{\left(\min(\nu_i,\sigma_i)+\max(\nu_i,\sigma_i)\right)} \\ &= \prod p_i^{(\nu_i+\sigma_i)} \\ &= a \cdot b. \end{aligned}$$

■

ÜBUNGSAUFGABEN 1.19.

(1) Zeigen Sie ohne Verwendung der Primfaktorzerlegung, dass für alle $a, b \in \mathbb{N}$ gilt:

$$\mathrm{kgV}(a,b) \cdot \mathrm{ggT}(a,b) = a \cdot b.$$

Hinweis: Zeigen Sie dazu $ab \mid \mathrm{ggT}(a,b) \cdot \mathrm{kgV}(a,b)$ und $\mathrm{kgV}(a,b) \mid \frac{ab}{\mathrm{ggT}(a,b)}$.

(2) Seien $a, b, c \in \mathbb{N}$. Zeigen Sie:
   (a) $\mathrm{ggT}(\mathrm{ggT}(a,b),c) = \mathrm{ggT}(a,\mathrm{ggT}(b,c))$.
   (b) $\mathrm{kgV}(\mathrm{kgV}(a,b),c) = \mathrm{kgV}(a,\mathrm{kgV}(b,c))$.
   (c) $\mathrm{ggT}(\mathrm{kgV}(a,b),c) = \mathrm{kgV}(\mathrm{ggT}(a,c),\mathrm{ggT}(b,c))$.
   (d) $\mathrm{kgV}(\mathrm{ggT}(a,b),c) = \mathrm{ggT}(\mathrm{kgV}(a,c),\mathrm{kgV}(b,c))$.

(3) Sei $n \in \mathbb{N}$, und seien $a_1, a_2, \ldots, a_n$ in $\mathbb{N}$. Wir definieren K_1 und K_2 durch:
   (a) $K_1(a_1) := a_1$, $K_1(a_1, a_2, \ldots, a_n) = \mathrm{kgV}(K_1(a_1, a_2, \ldots, a_{n-1}), a_n)$.
   (b) $K_2(a_1, a_2, \ldots, a_n) := \min\{z \in \mathbb{N} : a_i \mid z \text{ für alle } i \in \{1, 2, \ldots, n\}\}$.

   Zeigen Sie, dass K_1 und K_2 gleich sind.

(4) Sei $n \in \mathbb{N}$, und seien $a_1, a_2, \ldots, a_n$ in $\mathbb{N}$. Wir definieren K_2 durch

$$K_2(a_1, a_2, \ldots, a_n) := \min\{z \in \mathbb{N} : a_i \mid z \text{ für alle } i \in \{1, 2, \ldots, n\}\}.$$

   Zeigen Sie, dass alle ganzen Zahlen, die Vielfaches eines jeden a_i sind, auch ein Vielfaches von $K_2(a_1, a_2, \ldots, a_n)$ sind.

(5) Sei p_n die n-te Primzahl, d. h. $p_1 = 2$, $p_2 = 3$, usw. Zeigen Sie, auch ohne die Eindeutigkeit der Primfaktorzerlegung zu verwenden, dass folgendes gilt: Wenn

$$\begin{aligned} a &= \prod p_i^{\alpha_i} \\ b &= \prod p_i^{\beta_i}, \end{aligned}$$

   wobei $\alpha_i, \beta_i \in \mathbb{N}_0$, und fast alle $\alpha_i, \beta_i = 0$ sind, dann gilt

$$\mathrm{kgV}(a,b) = \prod p_i^{\max(\alpha_i,\beta_i)}.$$

4. Lösen von Kongruenzen

DEFINITION 1.20. Sei $n \in \mathbb{Z}$. Dann definieren wir eine Relation $\equiv_n$ auf $\mathbb{Z}$ durch

$$a \equiv_n b :\Leftrightarrow n \mid a - b \text{ für } a, b \in \mathbb{Z}.$$

Für $a \equiv_n b$ schreiben wir auch $a \equiv b \pmod{n}$ und sagen: "a ist kongruent b modulo n."

SATZ 1.21. *Seien $a, c \in \mathbb{Z}$ (nicht beide = 0), und sei $b \in \mathbb{Z}$. Dann sind die folgenden Bedingungen äquivalent:*

(1) *Die Kongruenz $ax \equiv b \pmod{c}$ ist lösbar, d. h., es gibt $y \in \mathbb{Z}$ sodass $c \mid a \cdot y - b$.*
(2) $\mathrm{ggT}(a, c)$ *teilt b.*

Beweis: (1) $\Rightarrow$ (2): Sei x eine Lösung, d.h. $c \mid ax - b$. Falls c die Zahl $ax - b$ teilt, dann gilt erst recht

$$\mathrm{ggT}(a, c) \mid ax - b.$$

$\mathrm{ggT}(a, c)$ teilt a, also gilt $\mathrm{ggT}(a, c) \mid b$.

(2) $\Rightarrow$ (1): Aufgrund der Voraussetzungen existiert ein $z \in \mathbb{Z}$, sodass

$$\mathrm{ggT}(a, c) \cdot z = b.$$

Aus dem erweiterten Euklidischen Algorithmus bekommen wir $u, v \in \mathbb{Z}$ mit

$$ggT(a, c) = u \cdot a + v \cdot c.$$

Es gilt dann

$$(ua + vc) \cdot z = b,$$

also

$$a \cdot uz + c \cdot vz = b,$$

und somit

$$a \cdot (uz) \equiv b \pmod{c}.$$

Also ist $x := uz$ Lösung von $ax \equiv b \pmod{c}$. ■

SATZ 1.22. *Seien $a, c \in \mathbb{Z}$ (nicht beide = 0), und sei $b \in \mathbb{Z}$. Sei x_0 eine Lösung von*

$$ax \equiv b \pmod{c}. \tag{1.3}$$

Dann ist die Lösungsmenge von (1.3) *gegeben durch:*

$$L = \left\{ x_0 + k \cdot \frac{c}{ggT(a, c)} \mid k \in \mathbb{Z} \right\}.$$

Beweis: "$\supseteq$": Wir setzen zunächst $x_0 + k\frac{c}{\mathrm{ggT}(a,c)}$ ein und erhalten

$$\begin{aligned} a\left(x_0 + k\tfrac{c}{\mathrm{ggT}(a,c)}\right) &= ax_0 + ak\tfrac{c}{\mathrm{ggT}(a,c)} \\ &\equiv_c b + ak\tfrac{c}{\mathrm{ggT}(a,c)} \\ &= b + ck\tfrac{a}{\mathrm{ggT}(a,c)} \\ &\equiv_c b. \end{aligned}$$

Daher ist $x_0 + k\frac{c}{\mathrm{ggT}(a,c)}$ wirklich eine Lösung.

"$\subseteq$": Sei x_1 Lösung von $ax \equiv b \pmod{c}$. Zu zeigen ist: $\frac{c}{\mathrm{ggT}(a,c)} \mid \left(x_1 - x_0\right)$. Da x_1 und x_0 Lösungen sind, gilt $ax_1 \equiv b \pmod{c}$ und $ax_0 \equiv b \pmod{c}$. Daher gilt

$$a\left(x_1 - x_0\right) \equiv 0 \pmod{c},$$

oder, äquivalent dazu,

$$c \mid a\left(x_1 - x_0\right).$$

Daher gilt auch

$$\frac{c}{\mathrm{ggT}\,(a,c)} \mid \frac{a}{\mathrm{ggT}\,(a,c)} \cdot \left(x_1 - x_0\right).$$

Da

$$\mathrm{ggT}\left(\frac{c}{\mathrm{ggT}\,(a,c)}, \frac{a}{\mathrm{ggT}\,(a,c)}\right) = 1,$$

gilt

$$\frac{c}{\mathrm{ggT}\,(a,c)} \mid \left(x_1 - x_0\right).$$

■

KOROLLAR 1.23. *Seien $a, c \in \mathbb{Z}$ (nicht beide $= 0$), sei $b \in \mathbb{Z}$, sodass $\mathrm{ggT}(a,c) \mid b$, und sei x_0 eine Lösung von $ax \equiv b \pmod{c}$ ist. Dann ist die Kongruenz $ax \equiv b \pmod{c}$ äquivalent zu $x \equiv x_0 \left(\mathrm{mod}\ \frac{c}{\mathrm{ggT}(a,c)}\right)$.*

ÜBUNGSAUFGABEN 1.24.

(1) Lösen Sie die Gleichung

$$207x \equiv 18 \pmod{1989}$$

in $\mathbb{Z}$!

(2) Bestimmen Sie für alle $a, c \in \mathbb{N}$, $b \in \mathbb{Z}$, wieviele Lösungen in $\{0, 1, \ldots, c-1\}$ die Gleichung $a \cdot x \equiv b \pmod{c}$ hat.

Wir betrachten nun Systeme von zwei Kongruenzen, also Systeme der Form

$$\begin{aligned} x &\equiv a_1 \left(\mathrm{mod}\ m_1\right) \\ x &\equiv a_2 \left(\mathrm{mod}\ m_2\right), \end{aligned}$$

wobei $m_1, m_2 \in \mathbb{N}$ und $a_1, a_2 \in \mathbb{Z}$.

BEISPIELE 1.25. Das System

$$\begin{aligned} x &\equiv 1 \pmod 2 \\ x &\equiv 0 \pmod 4 \end{aligned}$$

kann nicht lösbar sein, denn eine Lösung $x \in \mathbb{Z}$ müsste sowohl gerade als auch ungerade sein. Das System

$$\begin{aligned} x &\equiv 1 \pmod 2 \\ x &\equiv 2 \pmod 5 \end{aligned}$$

hingegen hat zum Beispiel die Lösung $x = 7$.

SATZ 1.26. *Seien* $a_1, a_2 \in \mathbb{Z}$, $m_1, m_2 \in \mathbb{N}$. *Das System*

$$\begin{aligned} x &\equiv a_1 \pmod{m_1} \\ x &\equiv a_2 \pmod{m_2} \end{aligned}$$

ist genau dann lösbar, wenn $\text{ggT}(m_1, m_2) \mid (a_1 - a_2)$.

Beweis: "⇒": Wir nehmen an, dass x Lösung ist. Dann gilt: $m_1 \mid (x - a_1)$ und $m_2 \mid (x - a_2)$. Daher gilt auch $\text{ggT}(m_1, m_2) \mid (x - a_1)$ und $\text{ggT}(m_1, m_2) \mid (x - a_2)$, und somit

$$\text{ggT}(m_1, m_2) \mid (x - a_2) - (x - a_1) = (a_1 - a_2).$$

"⇐" Es gibt $u, v \in \mathbb{Z}$, sodass

$$\begin{aligned} u \cdot m_1 + v \cdot m_2 &= ggT(m_1, m_2) \\ k \cdot u \cdot m_1 + k \cdot v \cdot m_2 &= a_1 - a_2 \\ a_2 + k \cdot v \cdot m_2 &= \underbrace{a_1 - k \cdot u \cdot m_1}_{=x} \end{aligned}$$

daher ist $x := a_1 - kum_1$ Lösung des Systems. □

Der Beweis liefert auch gleich ein Lösungsverfahren.

Beispiel: Wir lösen:

$$\begin{aligned} x &\equiv 2 \pmod{15} \\ x &\equiv 8 \pmod{21} \end{aligned}$$

Da $\text{ggT}(15, 21) = 3$ und $3 \mid (2 - 8)$ ist das System lösbar. Wir berechnen jetzt diesen ggT und *Kofaktoren* (d.h. Koeffizienten für eine Linearkombination von 15 und 21, die den ggT ergibt).

	21	15
21	1	0
15	0	1
6	1	-1
3	-2	3

und erhalten daraus $3 = 3 \cdot 15 - 2 \cdot 21$.

$$\begin{aligned} 3 \cdot 15 - 2 \cdot 21 &= 3 \\ (-6) \cdot 15 + 4 \cdot 21 &= 2 - 8 \\ \underbrace{8 + 4 \cdot 21}_{=92} &= \underbrace{2 + 6 \cdot 15}_{=92} \end{aligned}$$

Daher erhalten wir eine Lösung: $x = 92$.

Der folgende Satz gibt an, wie wir aus einer Lösung der Kongruenz alle Lösungen erhalten.

SATZ 1.27. *Sei x_0 eine Lösung von*

$$\begin{aligned} x &\equiv a_1 \pmod{m_1} \\ x &\equiv a_2 \pmod{m_2}. \end{aligned}$$

Dann gilt für die Lösungmenge L

$$L = \left\{ x_0 + k \cdot \mathrm{kgV}\left(m_1, m_2\right) \mid k \in \mathbb{Z} \right\}.$$

Beweis: "$\supseteq$": Wir setzen

$$x_0 + k \cdot \mathrm{kgV}\left(m_1, m_2\right)$$

in die erste Kongruenz ein und erhalten

$$\left(x_0 + k \cdot \mathrm{kgV}\left(m_1, m_2\right)\right) \equiv a_1 \pmod{m_1}.$$

Das gleiche gilt für die zweite Kongruenz.

"$\subseteq$": Wir fixieren $x_1 \in L$. Um zu zeigen, dass $x_1 \in \left\{ x_0 + k \cdot \mathrm{kgV}\left(m_1, m_2\right) \mid k \in \mathbb{Z} \right\}$, zeigen wir, dass $x_1 - x_0$ ein Vielfaches von $\mathrm{kgV}\left(m_1, m_2\right)$ ist. Wir wissen ja, dass

$$\begin{aligned} x &\equiv a_1 \pmod{m_1} \\ x &\equiv a_2 \pmod{m_2} \end{aligned}$$

Daher gilt $\left(x_1 - x_0\right) \equiv 0 \pmod{m_1}$ und somit $m_1 \mid \left(x_1 - x_0\right)$. Ebenso zeigt man, dass $m_2 \mid \left(x_1 - x_0\right)$ gilt.

Da das kgV jedes gemeinsame Vielfache teilt, gilt $\mathrm{kgV}\left(m_1, m_2\right) \mid \left(x_1 - x_0\right)$. ■

ÜBUNGSAUFGABEN 1.28.

(1) Lösen Sie folgendes System von Kongruenzen!

$$\begin{aligned} x &\equiv 22 \pmod{26} \\ x &\equiv 26 \pmod{37} \end{aligned}$$

(2) Seien $m_1, m_2 \in \mathbb{N}$. Wieviele Lösungen in $\{0, 1, \ldots, m_1 \cdot m_2 - 1\}$ hat das System

$$\begin{aligned} x &\equiv a_1 \pmod{m_1} \\ x &\equiv a_2 \pmod{m_2}? \end{aligned}$$

Die folgenden Sätze zeigen uns, wie man das Lösen von Systemen aus mehr als zwei Kongruenzen auf das Lösen von Systemen aus zwei Kongruenzen zurückführen kann. Der erste Satz zeigt, dass man ein System von Kongruenzen durch eine einzige Kongruenz ersetzen kann – vorausgesetzt, man kennt zumindest *eine* Lösung des Systems.

SATZ 1.29. *Seien* $r \in \mathbb{N}$, $m_1, m_2, \ldots, m_r \in \mathbb{N}$ *und* $a_1, a_2, \ldots, a_r \in \mathbb{Z}$. *Falls das System*

$$\begin{aligned} x &\equiv a_1 \pmod{m_1} \\ x &\equiv a_2 \pmod{m_2} \\ &\vdots \\ x &\equiv a_r \pmod{m_r} \end{aligned} \tag{1.4}$$

eine Lösung x_0 *hat, dann ist* (1.4) *äquivalent zu*

$$x \equiv x_0 \pmod{\mathrm{kgV}(m_1, m_2, \ldots, m_r)}.$$

Beweisskizze: Falls x_0 eine Lösung ist, dann ist auch jedes

$$x_0 + k \cdot \mathrm{kgV}(m_1, m_2, \ldots, m_r)$$

eine Lösung. Andererseits haben zwei verschiedene Lösungen die gleichen Reste modulo jedem m_i, ihre Differenz ist daher ein gemeinsames Vielfaches der m_i und somit ein Vielfaches des kgV. ■

Wir schreiben:

$$\begin{aligned} kgV(m_1, m_2) &=: m_1 \vee m_2 \\ ggT(m_1, m_2) &=: m_1 \wedge m_2. \end{aligned}$$

Es gilt dann:

PROPOSITION 1.30. *Seien* $a, b, c \in \mathbb{N}$. *Dann gilt:*

(1) $a \wedge (a \vee b) = a$,
(2) $a \vee (a \wedge b) = a$,
(3) $(a \wedge b) \wedge c = a \wedge (b \wedge c)$,
(4) $(a \vee b) \vee c = a \vee (b \vee c)$,
(5) $a \wedge (b \vee c) = (a \wedge b) \vee (a \wedge c)$,
(6) $a \vee (b \wedge c) = (a \vee b) \wedge (a \vee c)$.

Der folgende Satz sagt, wann ein System von Kongruenzen lösbar ist.

SATZ 1.31 (Chinesischer Restsatz). *Seien* $r \in \mathbb{N}$, $a_1, \ldots, a_r \in \mathbb{Z}$, $m_1, \ldots, m_r \in \mathbb{Z} \setminus \{0\}$. *Dann sind folgende drei Aussagen äquivalent.*

(1) *Es gibt* $x \in \mathbb{Z}$, *sodass*

$$\begin{aligned} x &\equiv a_1 \pmod{m_1} \\ x &\equiv a_2 \pmod{m_2} \\ &\vdots \\ x &\equiv a_r \pmod{m_r}. \end{aligned}$$

(2) *Für alle $i, j \in \{1, 2, \ldots, r\}$ ist das System*

$$\begin{aligned} x &\equiv a_i \pmod{m_i} \\ x &\equiv a_j \pmod{m_j} \end{aligned}$$

lösbar.

(3) *Für alle $i, j \in \{1, 2, \ldots, r\}$ gilt*

$$\operatorname{ggT}(m_i, m_j) \mid a_i - a_j.$$

Beweis: "(1) $\Rightarrow$ (2)" ist offensichtlich. "(2) $\Leftrightarrow$ (3)" gilt wegen Satz 1.26.

"(3) $\Rightarrow$ (1)": Wir zeigen durch Induktion nach r, dass jedes System aus r Kongruenzen, für das die Bedingung (3) erfüllt ist, lösbar ist. Ein System aus zwei Kongruenzen ist wegen Satz 1.26 lösbar. Um ein System von r (mit $r \geq 3$) Kongruenzen zu lösen, bestimmen wir zuerst nach Induktionsvoraussetzung ein y sodass

$$y \equiv a_2 \pmod{m_2}, \ldots, y \equiv a_r \pmod{m_r}.$$

Wegen Satz 1.29 ist $x \equiv a_1 \pmod{m_1}, \ldots, x \equiv a_r \pmod{m_r}$ äquivalent zu

$$\begin{aligned} x &\equiv a_1 \pmod{m_1} \\ x &\equiv y \pmod{m_2 \vee \ldots \vee m_r}. \end{aligned} \tag{1.5}$$

Jetzt müssen wir zeigen, dass (1.5) lösbar ist. Das gilt nach Satz 1.26 genau dann, wenn

$$m_1 \wedge (m_2 \vee \ldots \vee m_r) \mid y - a_1. \tag{1.6}$$

Es gilt $a \wedge (b \vee c) = (a \wedge b) \vee (a \wedge c)$. Daher ist (1.6) äquivalent zu

$$(m_1 \wedge m_2) \vee (m_1 \wedge m_3) \vee \ldots \vee (m_1 \wedge m_r) \mid y - a_1.$$

Wir zeigen dazu, dass für $i > 1$ gilt:

$$(m_1 \wedge m_i) \mid (y - a_1). \tag{1.7}$$

Wir wissen aber

$$y - a_1 \equiv_{m_i} a_i - a_1 \equiv_{(m_i \wedge m_1)} 0.$$

Das beweist, dass für alle $i > 1$ gilt $(m_i \wedge m_1) \mid (y - a_1)$. Nun ist jedes gemeinsame Vielfache eine Vielfaches des kleinsten gemeinsamen Vielfachen, und somit gilt (1.6). ■

BEISPIEL 1.32. Wir lösen folgendes System

$$\begin{aligned} x &\equiv 2 \pmod{15} \\ x &\equiv 8 \pmod{21} \\ x &\equiv 7 \pmod{55} \end{aligned} \tag{1.8}$$

Wir kennen bereits die Lösungen von $x \equiv 2 \pmod{15}$, $x \equiv 8 \pmod{21}$. Das System (1.8) ist daher äquivalent zu

$$\begin{aligned} x &\equiv 92 \pmod{105} \\ x &\equiv 7 \pmod{55}. \end{aligned}$$

Wir berechnen ggT$(55, 105)$ und die Kofaktoren nach dem Euklidschen Algorithmus und erhalten

	105	55
105	1	0
55	0	1
50	1	-1
5	-1	2
0		

und daher

$$\begin{aligned} (-1) \cdot 105 + 2 \cdot 55 &= 5 \\ (-17) \cdot 105 + 34 \cdot 55 &= 92 - 7 \\ 7 + 34 \cdot 55 &= 92 + 17 \cdot 105. \end{aligned}$$

Daraus erhalten wir also, dass 1877 die Lösung ist, also geben wir die Lösungsmenge folgendermaßen an:

$$\begin{aligned} L &= \{x \in \mathbb{Z} \mid x \equiv 1877 \pmod{1155}\} \\ &= \{x \in \mathbb{Z} \mid x \equiv 722 \pmod{1155}\}. \end{aligned}$$

ÜBUNGSAUFGABEN 1.33.

(1) Finden Sie alle Lösungen in $\mathbb{Z}$ von

$$\begin{aligned} x &\equiv 26 \pmod{56} \\ x &\equiv 82 \pmod{84} \\ x &\equiv 124 \pmod{126}. \end{aligned}$$

(2) Finden Sie alle Lösungen in $\mathbb{Z}$ von

$$\begin{aligned} x &\equiv 3 \pmod{4} \\ x &\equiv 8 \pmod{9} \\ x &\equiv 1 \pmod{25}. \end{aligned}$$

(3) Seien $a, b, c \in \mathbb{Z}$. Bestimmen Sie für alle $a, b, c \in \mathbb{Z}$, ob die Gleichung

$$a \cdot x + b \cdot y = c$$

in $\mathbb{Z} \times \mathbb{Z}$ lösbar ist, und bestimmen Sie alle Lösungen.

(4) Bestimmen Sie eine Lösung in $\mathbb{Z}^3$ von

$$12x + 15y + 20z = 1.$$

(5) Bestimmen Sie alle Lösungen in $\mathbb{Z}^3$ von

$$12x + 15y + 20z = 1.$$

(6) Sei T eine endliche Teilmenge von $\mathbb{Z}$. Eine Funktion $f : T \to \mathbb{Z}$ heißt *kompatibel* genau dann, wenn für alle $x_1, x_2 \in T$ mit $x_1 \neq x_2$ der Quotient $\frac{f(x_1)-f(x_2)}{x_1-x_2}$ ganzzahlig ist.

Sei f eine beliebige kompatible Funktion auf einer endlichen Teilmenge T von $\mathbb{Z}$, und sei $z \in \mathbb{Z} \setminus T$. Zeigen Sie: Es gibt eine kompatible Funktion $g : T \cup \{z\} \to \mathbb{Z}$, sodass $g(t) = f(t)$ für alle $t \in T$.

Hinweis: Die Funktion g heißt *kompatible Erweiterung* von f auf $T \cup \{z\}$. Sie müssen nur ein passendes $g(z)$ finden. Stellen Sie dazu ein System von Kongruenzen auf, von dem $g(z)$ Lösung sein muss, und zeigen Sie, dass dieses System lösbar ist.

(7) Eine Funktion $f : \mathbb{Z} \to \mathbb{Z}$ heißt *kompatibel* genau dann, wenn für alle $x_1, x_2 \in \mathbb{Z}$ mit $x_1 \neq x_2$ der Quotient $\frac{f(x_1)-f(x_2)}{x_1-x_2}$ ganzzahlig ist. Zeigen Sie, dass folgende Funktionen kompatibel sind:
   (a) $f(x) = x^n$ für $n \in \mathbb{N}$,
   (b) $f(x) = 12 \binom{x}{4}$.

(8) Eine Funktion $f : \mathbb{Z} \to \mathbb{Z}$ heißt *kompatibel* genau dann, wenn für alle $x_1, x_2 \in \mathbb{Z}$ mit $x_1 \neq x_2$ der Quotient $\frac{f(x_1)-f(x_2)}{x_1-x_2}$ ganzzahlig ist. Zeigen Sie, dass die Menge der kompatiblen Funktionen von $\mathbb{Z}$ überabzählbar ist.

KAPITEL 2

Teilbarkeit in Integritätsbereichen

1. Kommutative Ringe mit Eins

DEFINITION 2.1. Eine Algebra $(R, +, -, \cdot, 0, 1)$ ist ein *kommutativer Ring mit Eins*, wenn $+, \cdot$ binäre Operationen auf R sind, $-$ eine unäre Operation auf R ist, und $0, 1$ Elemente aus R sind, sodass für alle $x, y, z \in R$ die folgenden Eigenschaften erfüllt sind:

(1) $x + 0 = x$
(2) $x + (-x) = 0$
(3) $(x + y) + z = x + (y + z)$
(4) $x + y = y + x$
(5) $(x \cdot y) \cdot z = x \cdot (y \cdot z)$
(6) $x \cdot y = y \cdot x$
(7) $x \cdot 1 = x$
(8) $x \cdot (y + z) = x \cdot y + x \cdot z$.

SATZ 2.2. *Sei* $(R, +, -, \cdot, 0, 1)$ *ein kommutativer Ring mit* 1*, und seien* $x, y \in R$*. Dann gilt*

(1) $-(-(x)) = x$
(2) $x \cdot 0 = 0$.
(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): $x \cdot 0 = x \cdot 0 + 0 = x \cdot 0 + (x \cdot 0 + (-x \cdot 0)) = (x \cdot 0 + x \cdot 0) + (-x \cdot 0) = x \cdot (0 + 0) + (-x \cdot 0) = x \cdot 0 + (-x \cdot 0) = 0$. (3): Wir verwenden jetzt außer den bei der Definition von kommutativen Ringen verwendeten Gleichungen auch die Folgerungen, dass für alle $z \in R$ auch $(-z) + z = 0$ und $0 + z = z$ gilt. $-(x \cdot y) = -(x \cdot y) + x \cdot 0 = -(x \cdot y) + x \cdot (y + (-y)) = -(x \cdot y) + (x \cdot y + x \cdot (-y)) = (-(x \cdot y) + x \cdot y) + x \cdot (-y) = 0 + x \cdot (-y) = x \cdot (-y)$. Mithilfe des Kommutativgesetzes folgt nun auch $(-x) \cdot y = -(x \cdot y)$. ■

2. Ideale

DEFINITION 2.3. Sei R ein kommutativer Ring mit Eins. Eine nichtleere Teilmenge I von R ist ein *Ideal* von R, wenn für alle $r \in R$ und $i, j \in I$ auch $r \cdot i \in I$ und $i + j \in I$ gilt.

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

DEFINITION 2.4. Sei R ein kommutativer Ring mit Eins, und sei A eine Teilmenge von R. Dann ist das *von A erzeugte Ideal* $\langle A\rangle_R$ definiert durch

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

SATZ 2.5. *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 jeder Summand $r_i a_i$ in $\langle A\rangle_R$, und schließlich auch die Summe j. ■

DEFINITION 2.6. Sei R ein kommutativer Ring mit Eins, und sei I ein Ideal von R. Das Ideal I ist ein *Hauptideal* von R, wenn es ein $a \in R$ gibt, sodass $I = \langle\{a\}\rangle_R$. Wir schreiben für $\langle\{a\}\rangle_R = Ra$ auch kürzer (a).

ÜBUNGSAUFGABEN 2.7.

(1) (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) $R = \mathbb{Z}_{101}$, $S = \{[75]_{101}\}$.

(2) (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) $S = \{xy + x, 1 + y^2\}$.

(3) (Zornsches Lemma) Sei R ein kommutativer Ring mit Eins. Ein Ideal von R ist *maximal*, wenn es ein maximales Element in

$$\{I \mid I \text{ ist Ideal von } R \text{ und } I \neq R\}$$

ist. Zeigen Sie, dass jedes von R verschiedene Ideal in einem maximalen Ideal von R enthalten ist! Wo verwenden Sie, dass R ein Einselement hat?

3. Integritätsbereiche

Ein kommutativer Ring mit Eins R ist ein *Integritätsbereich*, wenn er zumindest zwei Elemente hat und für alle a, b mit $a \neq 0$ und $b \neq 0$ auch $ab \neq 0$ gilt.

DEFINITION 2.8. 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 $b = ra$.

DEFINITION 2.9. 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 2.10. *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 2.11.

(1) (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.
(2) (Integritätsbereiche) Zeigen Sie, dass jeder endliche Integritätsbereich ein Körper ist. (*Hinweis:* Betrachten Sie für $r \neq 0$ die Abbildung $x \mapsto r \cdot x$.)
(3) (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.
(4) (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.
(5) (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.

4. Euklidische Integritätsbereiche

DEFINITION 2.12. 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 $b \neq 0$ gibt es $q, r \in R$, sodass
   (a) $a = b\,q + r$, und
   (b) $r = 0$ oder $\delta(r) < \delta(b)$.

SATZ 2.13. *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 2.14. *Sei K ein Körper, und sei $K[t]$ der Polynomring über K. Dann ist $K[t]$ ein Euklidischer Bereich.*

Beweis: Wir setzen $\delta(f) := \deg(f)$. ■

DEFINITION 2.15. Sei $\mathbb{Z}[i]$ die Teilmenge der komplexen Zahlen, die durch

$$\mathbb{Z}[i] := \{a + b\,i \mid a, b \in \mathbb{Z}\}$$

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 2.16. *$\mathbb{Z}[i]$ 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 2.12 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

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

Dann gilt

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

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

DEFINITION 2.17. Ein Integritätsbereich R ist ein *Hauptidealbereich*, wenn es für jedes Ideal I von R ein $a \in R$ gibt, sodass $I = (a)$.

SATZ 2.18. *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 $I = (a)$. ■

BEISPIEL 2.19. 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 $\deg_y(f) = 0$ und $\deg_x(f) = 0$, 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. ■

5. Faktorielle Integritätsbereiche

DEFINITION 2.20. Sei R ein Integritätsbereich. R ist *faktoriell*, wenn folgendes gilt:

(1) Für alle $r \in R\backslash\{0\}$, 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: $f_i \sim_R g_{\pi(i)}$.

LEMMA 2.21. *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 $p \mid a \cdot b$. 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 $p \mid a$. ■

SATZ 2.22. *Jeder Hauptidealbereich ist faktoriell.*

Beweis: Sei G die Menge aller $r \in R \setminus \{0\}$, die nicht invertierbar sind und sich nicht als Produkt endlich vieler irreduzibler Elemente schreiben lassen. Wir nehmen an $G \neq \emptyset$. Sei
$$\mathcal{A} := \{(r) \mid r \in G\}$$
Wir betrachten zunächst den Fall, dass die geordnete Menge $(\mathcal{A}, \subseteq)$ ein maximales Element hat. Sei A ein solches maximales Element, und sei $a \in G$ so, dass $(a) = A$. Da a nicht irreduzibel und nicht invertierbar ist, gibt es nicht invertierbare Elemente $b, c \in R$ mit $b\,c = a$. Nun gilt $(a) \subseteq (c)$. Wenn $(a) = (c)$, so gibt es $d \in R$ mit $d\,a = c$. Dann gilt $a = b\,c = b\,d\,a$, also $a(1 - bd) = 0$. Da R ein Intergritätsbereich ist, gilt $a = 0$ oder $bd = 1$. Wenn $a = 0$, so gilt $A \notin \mathcal{A}$, ein Widerspruch. Wenn $bd = 1$, so ist b invertierbar, ebenfalls ein Widerspruch. Also gilt $(a) \neq (c)$. Wegen der Maximalität von (a) gilt $(c) \notin \mathcal{A}$. Also gilt $c \notin G$. Da c nicht invertierbar ist, lässt sich c als Produkt endlich vieler irreduzibler Elemente schreiben. Da $(a) \subsetneq (b)$, erhält man genauso, dass sich b als Produkt endlich vieler irreduzibler Elemente schreiben lässt. Somit ist auch

a ein Produkt endlich vieler irreduzibler Elemente, im Widerspruch zu $a \in G$. Der Fall, dass $(\mathcal{A}, \subseteq)$ ein maximales Element hat, kann also nicht eintreten.

Wir betrachten nun den Fall, dass $(\mathcal{A}, \subseteq)$ kein maximales Element hat. Dann gibt es eine Folge $(a_i)_{i\in\mathbb{N}}$ aus G, sodass $(a_1) \subsetneq (a_2) \subsetneq (a_3)\cdots$. Wir bilden nun die Menge $A := \cup_{i\in\mathbb{N}}(a_i)$. Die Menge A ist ein Ideal des Rings R. Da R ein Hauptidealbereich ist, gibt es ein $b \in A$ mit $(b) = A$. Wegen $b \in A$ gibt es ein $j \in \mathbb{N}$, sodass $b \in (a_j)$. Dann gilt auch $(b) \subseteq (a_j)$, und somit $(a_{j+1}) \subseteq (b) \subseteq (a_j)$, im Widerspruch zu $(a_j) \subsetneq (a_{j+1})$. Daher kann auch der Fall, dass $(\mathcal{A}, \subseteq)$ kein maximales Element hat, nicht eintreten.

Insgesamt gilt also $G = \emptyset$; somit lässt sich jedes nicht invertierbare Element von $R\setminus\{0\}$ als Produkt endlich vieler irreduzibler Elemente schreiben.

Wir zeigen nun die Eindeutigkeit der Zerlegung, indem wir die Eigenschaft (2) aus Definition 2.20 durch Induktion nach m zeigen. Wenn $m = 1$, so gilt $f_1 \mid g_1\cdots g_n$. Wegen Lemma 2.21 gibt es dann ein $j \in \{1, \ldots, n\}$, sodass $f_1 \mid g_j$. Da g_j irreduzibel ist, gibt es ein invertierbares Element $u \in R$ mit $g_j = u\, f_1$. Somit gilt $f_1 = u f_1 \prod_{\substack{i=1\\ i\neq j}}^{n} g_i$, also $1 = u \cdot \prod_{\substack{i=1\\ i\neq j}}^{n} g_i$. Damit ist jedes g_i mit $i \neq j$ invertierbar, und folglich gilt $n = 1$ und $j = 1$.

Sei nun $m > 1$. Wegen $f_1 \mid g_1\cdots g_n$ und Lemma 2.21 gibt es daher ein $j \in \{1, \ldots, n\}$, sodass $f_1 \mid g_j$. Da g_j irreduzibel ist, gibt es ein invertierbares $u \in R$ mit $u f_1 = g_j$. Außerdem gilt $n > 1$, denn falls $n = 1$, so gilt $f_1 f_2 \mid g_1$, im Widerspruch dazu dass g_1 irreduzibel ist. Es gilt also

$$f_2 \cdot f_3\cdots f_m = (ug_1)g_2g_3\cdots g_{j-1} \cdot g_{j+1}\cdots g_n.$$

Nach Induktionsvoraussetzung gibt es eine bijektive Abbildung $\sigma : \{2, \ldots, m\} \to \{1, \ldots, n\}\setminus\{j\}$, sodass $f_i \sim g_{\sigma(i)}$ für alle $i \in \{2, \ldots, m\}$. Somit leistet $\pi := \sigma \cup \{(1, j)\}$ das Gewünchte. ■

ÜBUNGSAUFGABEN 2.23.
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. 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) $a \sim_R \Pi_{i\in I}\, i^{\alpha(i)}$.

Dabei definieren wir für alle $i \in I$, dass $i^0 := 1$ ist. Ebenso ist ein Produkt $\Pi_{i\in\emptyset}$ immer gleich 1.

(1) Zeigen Sie: 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:
   (a) $a \mid b$.

(b) Für alle $i \in I$ gilt $\alpha(i) \leq \beta(i)$.

(2) 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.

6. Eine Anwendung in der Zahlentheorie

Wir brauchen zunächst folgende Beobachtung:

LEMMA 2.24. *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) Wenn $p \mid x^2 - 1 = (x+1)(x-1)$, so gilt wegen des Fundamentallemmas (Satz 1.6) $p \mid x+1$ 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 2.25. *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 2.24 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 2.16 und Satz 2.18 ist $\mathbb{Z}[i]$ ein Hauptidealbereich. Somit ist wegen Lemma 2.21 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

Restklassenringe

1. Faktorringe

DEFINITION 3.1 (Ring). Eine Algebra $(R, +, -, \cdot, 0, 1)$ ist ein *Ring mit Eins*, wenn $+, \cdot$ binäre Operationen auf R sind, $-$ eine unäre Operation auf R ist, und $0, 1$ Elemente aus R sind, sodass für alle $x, y, z \in R$ die folgenden Eigenschaften erfüllt sind:

(1) $x + 0 = x$
(2) $x + (-x) = 0$
(3) $(x + y) + z = x + (y + z)$
(4) $x + y = y + x$
(5) $(x \cdot y) \cdot z = x \cdot (y \cdot z)$
(6) $x \cdot (y + z) = x \cdot y + x \cdot z$
(7) $(x + y) \cdot z = x \cdot z + y \cdot z$
(8) $x \cdot 1 = 1 \cdot x = x$

DEFINITION 3.2 (Ideal). Sei $\boldsymbol{R} = (R, +, -, \cdot, 0, 1)$ ein Ring mit Eins. Eine Teilmenge I von R ist ein *Ideal von* $\boldsymbol{R}$, wenn $I \neq \emptyset$ und für alle $i, j \in I$ und $r \in R$ gilt: $i - j \in I$, $r \cdot i \in I$, $i \cdot r \in I$.

DEFINITION 3.3 (Restklasse). Sei $\boldsymbol{R}$ ein Ring mit Eins, und sei I ein Ideal von $\boldsymbol{R}$. Wir definieren eine Relation $\sim_I$ auf R durch

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

LEMMA 3.4. *Sei $\boldsymbol{R}$ ein Ring mit Eins, sei I ein Ideal von $\boldsymbol{R}$, 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 $r + I$.*

LEMMA 3.5. *Sei $\boldsymbol{R}$ ein Ring, sei I ein Ideal von $\boldsymbol{R}$, und seien $a_1, a_2, b_1, b_2 \in R$ mit $a_1 \sim_I a_2$ und $b_1 \sim_I b_2$. Dann gilt $a_1 + b_1 \sim_I a_2 + b_2$, $-a_1 \sim_I -a_2$, und $a_1 \cdot b_1 \sim_I a_2 \cdot b_2$.*

DEFINITION UND SATZ 3.6 (Faktorring). Sei $\boldsymbol{R}$ ein Ring, sei I ein Ideal von $\boldsymbol{R}$, 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.

ÜBUNGSAUFGABEN 3.7.

(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"?

2. Der Ring $\mathbb{Z}_n$

DEFINITION 3.8 ($\mathbb{Z}_n$). 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.

$\mathbb{Z}_n$ hat n Elemente, und zwar $[0]_n, [1]_n, \ldots, [n-1]_n$.

SATZ 3.9 (Invertierbarkeit). *Sei $n \in \mathbb{N}$ und $a \in \mathbb{Z}$. Dann ist $[a]_n$ genau dann invertierbar in $\mathbb{Z}_n$, wenn* $\mathrm{ggT}(a, n) = 1$.

Beweis: Die Klasse $[a]_n$ ist genau dann invertierbar, wenn es ein $x \in \mathbb{Z}$ mit $a \cdot x \equiv 1 \pmod{n}$ gibt. Diese Kongruenz ist genau dann lösbar, wenn $\mathrm{ggT}(a, n) \mid 1$. ■

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

LEMMA 3.10. *Seien a, b invertierbare Elemente aus $\mathbb{Z}_n$. Dann ist auch a·b invertierbar.*

DEFINITION 3.11 (Euler'sche φ–Funktion). Sei $n \in \mathbb{N}$, $n > 1$. Dann ist $\varphi(n)$ definiert durch

$$\begin{aligned} \varphi(n) &:= \left|\left\{a \in \mathbb{Z}_n \,:\, a \text{ invertierbar}\right\}\right| = \\ &= \left|\left\{x \in \{1, 2, \ldots, n-1\} \,:\, \mathrm{ggT}(x, n) = 1\right\}\right| . \end{aligned}$$

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

SATZ 3.12 (Satz von Euler). *Sei $n \in \mathbb{N}$, $n > 1$, $a \in \mathbb{Z}$,* $\mathrm{ggT}(a, n) = 1$. *Dann gilt:*

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

Wir überprüfen diesen Satz durch zwei Beispiele:

- Gilt $7^{\varphi(12)} \equiv 1 \pmod{12}$? Ja, denn es ist $7^4 \equiv 1 \pmod{12}$,
- Gilt $3^{\varphi(5)} \equiv 1 \pmod{5}$? Ja, denn es gilt $3^4 \equiv 1 \pmod{5}$.

Beweis von Satz 3.12: Seien $n \in \mathbb{N}$ und $a \in \mathbb{Z}$. Wir nehmen an, dass $\mathrm{ggT}(a,n) = 1$. Sei

$$I := \left\{ x \in \mathbb{Z}_n \,|\, x \text{ ist invertierbar} \right\}.$$

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

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

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 $\mathrm{ggT}(a,n) = 1$, 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:

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

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

$$\begin{aligned} y \cdot \prod_{x \in I} x &= y \cdot \left(\prod_{x \in I} x \right) . \left([a]_n \right)^{\varphi(n)} \\ [1]_n &= \left([a]_n \right)^{\varphi(n)}, \end{aligned}$$

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

KOROLLAR 3.13. *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 $z \in \mathbb{Z}$ beliebig, aber fest, 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 3.14.

(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 $2^n - 1$?

3. Das RSA-Verfahren

SATZ 3.15. *Seien p, q Primzahlen, $p \neq q$ und seien $a \in \mathbb{Z}$, $s \in \mathbb{N}_0$. Dann gilt:*

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

Beweis:

- *1. Fall:* $\mathrm{ggT}(a, pq) = 1$*:* Wir wissen, dass $a^{p-1} \equiv 1 \pmod{p}$ gilt (Satz von Euler), daher gilt auch $\left(a^{p-1}\right)^{(q-1)\cdot s} \equiv 1 \pmod{p}$. 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:* $\mathrm{ggT}(a, pq) = p$*:* Da der $\mathrm{ggT}(a, q) = 1$ 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 $p \cdot q \mid \left(a^{(q-1)\cdot(p-1)\cdot s} - 1\right) \cdot a$.
- *3. Fall:* $\mathrm{ggT}(a, pq) = q$*:* Beweis genauso wie im 2. Fall.
- *4. Fall:* $\mathrm{ggT}(a, pq) = p \cdot q$*:* Dann ist zu zeigen, dass $0 \equiv 0 \pmod{pq}$. ■

ÜBUNGSAUFGABEN 3.16.

(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:

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

Beim RSA-Verschlüsselungsverfahren wählt der Systementwerfer zwei Primzahlen p, q, sodass $n = pq$ nicht in verfügbarer Zeit faktoriserbar ist, berechnet $\phi := (p-1)(q-1)$, wählt für e eine beliebige Zahl mit $1 < e < \phi$ und $\mathrm{ggT}(e, \phi) = 1$, 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 $D : \mathbb{Z}_n \to \mathbb{Z}_n$, $D(c) := c^d$.

4. Die Multiplikativität der Eulerschen φ-Funktion

SATZ 3.17 (Multiplikativität der φ-Funktion). *Seien $n, m \in \mathbb{N}$, $n \geq 2$, $m \geq 2$. Wenn n, m relativ prim sind, dann gilt $\varphi(n \cdot m) = \varphi(n) \cdot \varphi(m)$.*

Der Beweis der Multiplikativität erfordert noch etwas Information über Ringe.

SATZ UND DEFINITION 3.18. *Seien R_1 und R_2 Ringe mit Eins sind. Wir definieren auf der Menge $R_1 \times R_2$ Operationen durch*

- $\begin{pmatrix} r_1 \\ r_2 \end{pmatrix} +_{R_1 \times R_2} \begin{pmatrix} s_1 \\ s_2 \end{pmatrix} := \begin{pmatrix} r_1 +_{R_1} s_1 \\ r_2 +_{R_2} s_2 \end{pmatrix}$
- $\begin{pmatrix} r_1 \\ r_2 \end{pmatrix} \cdot_{R_1 \times R_2} \begin{pmatrix} s_1 \\ s_2 \end{pmatrix} := \begin{pmatrix} r_1 \cdot_{R_1} s_1 \\ r_2 \cdot_{R_2} s_2 \end{pmatrix}$
- $-_{R_1 \times R_2} \begin{pmatrix} r_1 \\ r_2 \end{pmatrix} := \begin{pmatrix} -_{R_1} r_1 \\ -_{R_2} r_2 \end{pmatrix}$.

Dann ist

$$(R_1 \times R_2, +_{R_1 \times R_2}, -_{R_1 \times R_2}, \cdot_{R_1 \times R_2}, \begin{pmatrix} 0_{R_1} \\ 0_{R_2} \end{pmatrix}, \begin{pmatrix} 1_{R_1} \\ 1_{R_2} \end{pmatrix})$$

ein Ring mit Eins. Er ist das direkte Produkt von R_1 und R_2.

$R_1 \times R_2$ mit diesen Operationen erfüllt also alle Ring mit Eins-Rechengesetze.

Rechnen wir zum Beispiel in $\mathbb{Z}_4 \times \mathbb{Z}_5$.

$$\begin{pmatrix} [3]_4 \\ [4]_5 \end{pmatrix} \cdot \begin{pmatrix} [2]_4 \\ [3]_5 \end{pmatrix} = \begin{pmatrix} [2]_4 \\ [2]_5 \end{pmatrix}$$

$R_1 \times R_2$ heißt das *direkte Produkt* von R_1 und R_2.

DEFINITION 3.19. R, S seien Ringe mit Eins. Die Abbildung $\varphi : R \to S$ heißt Ring mit Eins-Homomorphismus: $\Leftrightarrow$

$$\begin{aligned} \forall r_1, r_2 \in R: \quad & \varphi\left(r_1 +_R r_2\right) = \varphi\left(r_1\right) +_S \left(r_2\right), \\ & \varphi\left(-_R r_1\right) = -_S \varphi\left(r_1\right), \\ & \varphi\left(r_1 \cdot_R r_2\right) = \varphi\left(r_1\right) \cdot_S \varphi\left(r_2\right), \\ & \varphi\left(0_R\right) = 0_S, \\ & \varphi\left(1_R\right) = 1_S. \end{aligned}$$

Ein surjektiver Homomorphismus heißt auch *Epimorphismus*, ein injektiver Homomorphismus auch *Monomorphismus* und ein bijektiver Homomorphismus auch *Isomorphismus*.

BEISPIELE 3.20.

- $\varphi : \mathbb{Z} \to \mathbb{Z}_5, \ x \mapsto [x]_5$ ist surjektiv, also ist φ ein Epimorphismus.

- Wir untersuchen $\alpha : \mathbb{Z}_5 \to \mathbb{Z},\ [x]_5 \mapsto x$. Hier ergibt sich folgendes Problem: $\alpha\left([3]_5\right) = 3$, und $\alpha\left([3]_5\right) = \alpha\left([8]_5\right) = 8$. — Das Problem ist, dass α nicht wohldefiniert ist. Man kann das auch so ausdrücken, dass man sagt, dass die Relation
$$\alpha = \left\{\left([x]_5, x\right) \mid x \in \mathbb{Z}\right\}$$
nicht funktional (d. h. eine Funktion = Graph einer Funktion) ist. Sie ist nicht funktional, weil $\left([2]_5, 2\right) \in \alpha$ und $\left([2]_5, 7\right) \in \alpha$.

SATZ 3.21. *Seien $n, m \in \mathbb{N}$ mit* $\mathrm{ggT}(n, m) = 1$. *Dann ist die Abbildung*
$$\begin{array}{rccc} \varphi & : & \mathbb{Z}_{m\cdot n} & \longrightarrow & \mathbb{Z}_n \times \mathbb{Z}_m \\ & & [x]_{m\cdot n} & \longmapsto & \left([x]_n, [x]_m\right) \end{array}$$
ein Ring mit Eins-Isomorphismus.

Beweis: Wir führen den Beweis in drei Schritten.

(1) φ ist wohldefiniert: Zu zeigen ist, dass für alle $y, z \in \mathbb{Z}$ mit $[y]_{m\cdot n} = [z]_{m\cdot n}$ die Gleichheiten $[y]_n = [z]_n$ und $[y]_m = [z]_m$ gelten. Zu zeigen ist ist also, dass für alle $y, z \in \mathbb{Z}$ gilt:
$$m \cdot n \mid y - z \Rightarrow (m \mid y - z \wedge n \mid y - z).$$
Das ist aber offensichtlich

(2) φ ist Homomorphismus: Wir überprüfen die Homomorphismuseigenschaft für $+$. Wir berechnen dazu
$$\begin{aligned} \varphi\left([x]_{n\cdot m} + [y]_{n\cdot m}\right) &= \varphi\left([x+y]_{n\cdot m}\right) \\ &= \left([x+y]_n, [x+y]_m\right) \\ &= \left([x]_n + [y]_n, [x]_m + [y]_m\right) \\ &= \begin{pmatrix} [x]_n \\ [x]_m \end{pmatrix} + \begin{pmatrix} [y]_n \\ [y]_m \end{pmatrix} \\ &= \varphi\left([x]_{n\cdot m}\right) + \varphi\left([y]_{n\cdot m}\right). \end{aligned}$$

(3) φ ist bijektiv: Da beide Mengen endlich und gleich groß sind, reicht es, zu zeigen, dass φ injektiv ist. Wir nehmen also an $\varphi\left([x]_{nm}\right) = \varphi\left([y]_{nm}\right)$. Das heißt $\left([x]_n, [x]_m\right) = \left([y]_n, [y]_m\right)$. Daher gilt $n \mid x - y$ und $m \mid x - y$. Da der $\mathrm{ggT}(n, m) = 1$ ist, gilt: $n \cdot m \mid x - y$. Wir erhalten daher $[x]_{nm} = [y]_{nm}$. Die Abbildung φ ist also injektiv, somit surjektiv und damit bijektiv. ■

Wenn der $\mathrm{ggT}(n, m) = 1$ ist, dann ist $\mathbb{Z}_n \times \mathbb{Z}_m$ also isomorph zu $\mathbb{Z}_{n\cdot m}$. Da Isomorphismen die Invertierbarkeit erhalten, haben beide Ringe gleich viele invertierbare Elemente. Daraus können wir jetzt die Multiplikativität der φ−Funktion, also Satz 3.17, herleiten.

Beweis von Satz 3.17:

(1) 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 $a \cdot c = [1]_n$, und $b \cdot d = [1]_m$, 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.

(2) Anzahl der invertierbaren Elemente in $\mathbb{Z}_{n \cdot m}$: Hier gibt es $\varphi(n \cdot m)$ invertierbare Elemente (nach der Definition von φ).

Damit haben wir gezeigt, dass

$$\varphi(n \cdot m) = \varphi(n) \cdot \varphi(m)$$

für alle $n, m \in \mathbb{N}$ mit $\mathrm{ggT}(n, m) = 1$. ■

Aus der Primfaktorzerlegung von n und aus $\varphi(p^\alpha) = p^\alpha - p^{\alpha-1}$ kann man jetzt leicht $\varphi(n)$ durch

$$\begin{aligned}
\varphi(n) &= \varphi\left(\prod p_i^{\alpha_i}\right) \\
&= \prod \varphi\left(p_i^{\alpha_i}\right) \\
&= \prod p_i^{\alpha_i}\left(1 - \tfrac{1}{p_i}\right) \\
&= \prod p_i^{\alpha_i} \cdot \prod\left(1 - \tfrac{1}{p_i}\right) \\
&= n \cdot \prod\left(1 - \tfrac{1}{p_i}\right)
\end{aligned}$$

berechnen.

BEISPIEL 3.22. $\varphi(12) = 12 \cdot \left(1 - \frac{1}{2}\right) \cdot \left(1 - \frac{1}{3}\right) = 4 = 2 \cdot 2 = \varphi(3) \cdot \varphi(4)$.

ÜBUNGSAUFGABEN 3.23.

(1) Für das RSA-Verfahren wählen wir $p = 5, q = 11$ und $k = 13$. Chiffrieren Sie $(01, 22, 03, 08)$ und dechiffrieren Sie das Ergebnis !
(2) 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!
(3) (Mathematica) Entschlüsseln Sie (verbotenerweise) die Nachricht $(2, 3, 5, 7, 11, 13)$, die mit $k = 13$ und $pq = 1334323339$ verschlüsselt wurde.
(4) (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).

KAPITEL 4

Gruppen

1. Symmetriegruppen von geometrischen Objekten

Wir werden in diesem Kapitel folgendes Problem lösen: Wir wollen die Seitenflächen eines Würfels mit zwei Farben (rot und blau) einfärben. Wieviele Färbungen gibt es? Dabei sehen wir zwei Färbungen als gleich an, wenn sie durch Drehen des Würfels ineinander übergeführt werden können. So gibt es z. B. nur eine Färbung, bei der eine Fläche rot ist, und alle anderen Flächen blau sind.

2. Definition einer Gruppe

DEFINITION 4.1. $(G, \cdot, i, \mathsf{e})$ 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, sodass für alle $x, y, z \in G$ folgende Eigenschaften gelten:

(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 4.2. 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

$$f_1 \circ f_2(x) = f_1(f_2(x)) \text{ für alle } x \in X,$$

$i(f_1)$ als die inverse Funktion zu f_1; mit id_X bezeichnen wir die identische Funktion auf X. Dann ist $(S_X, \circ, i, \mathrm{id}_X)$ eine Gruppe.

SATZ 4.3. *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 4.4.

(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 4.3, 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 $x, y, z \in H$ gelten: $(x \cdot y) \cdot z = x \cdot (y \cdot z)$, $\mathsf{e} \cdot x = x$, $x \cdot i(x) = \mathsf{e}$.
   (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. D. h., zeigen Sie: 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.) Zeigen Sie $i_1 = i_2$ und $\mathsf{e}_1 = \mathsf{e}_2$.

Es ist erfreulich, dass man Satz 4.3 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:

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

3. Beispiele für Gruppen

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

BEISPIEL 4.5 (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
$$(\mathrm{GL}(n, p), \cdot, {}^{-1}, \mathrm{E}^{(n)})$$
eine Gruppe, die *allgemeine lineare Gruppe*.
(2) Sei $\mathrm{SL}(n, p) := \{A \in GL(n, p) \mid \det A = 1\}$. Dann ist
$$(\mathrm{SL}(n, p), \cdot, {}^{-1}, \mathrm{E}^{(n)})$$
eine Gruppe, die *spezielle lineare Gruppe*.

BEISPIEL 4.6 (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 $n \geq 2$, 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.

DEFINITION 4.7. Eine Gruppe $(G, \cdot)$ heißt *zyklisch*, wenn es ein $g \in G$ gibt, sodass
$$G = \{g^n \mid n \in \mathbb{N}\} \cup \{(g^{-1})^n \mid n \in \mathbb{N}\} \cup \{1_G\}.$$

BEISPIEL 4.8 (Zyklische Gruppen).

(1) Sei $n \in \mathbb{N}$. $(\mathbb{Z}_n, +)$ ist eine zyklische Gruppe mit n Elementen.
(2) Sei $n \in \mathbb{N}$. $(\{x \in \mathbb{C} \mid x^n = 1\}, \cdot)$ ist eine zyklische Gruppe mit n Elementen.
(3) $(\mathbb{Z}, +)$ ist eine zyklische Gruppe.

BEISPIEL 4.9 (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.

ÜBUNGSAUFGABEN 4.10.

(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.

Wir bezeichnen nun eine Drehung des Quadrats um 90° gegen den Uhrzeigersinn mit a und eine Spiegelung an der y-Achse mit b. Was können wir nun aus a und b zusammenbauen? Überlegen wir uns zunächst einmal die folgenden beiden Beispiele:

(1) $b \cdot a = a^3 \cdot b$

(2) $baba = a^3bba = a^3 1a = a^4 = 1$.

Wir können die Symmetrieabbildungen also auf zwei Arten darstellen:

(1) Als Matrizen;
(2) Als Worte in a und b. So ist $aaabba$ eine Symmetrieabbildung. Beim Rechnen berücksichtigen wir, dass $a^4 = 1$, $b^2 = 1$, und $ba = a^3b$ gilt. Damit 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 Symmetrieoperationen (=Symmetrieabbildungen) des Quadrats, die man als D_4 (Diedergruppe mit 8 Elementen) bezeichnet, auch oft so an:

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

ÜBUNGSAUFGABEN 4.11.

(1) 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 $\{-1 - i, 1 - i, 1 + i, -1 + i\}$?
(2) Wir betrachten in $\mathbb{R}^2$ das Sechseck mit den Eckpunkten $\{(\mathrm{Re}(z), \mathrm{Im}(z)) \,|\, z \in \mathbb{C},\ z^6 = 1\}$. Bestimmen Sie alle Deckabbildungen, die dieses Sechseck auf sich selbst abbilden.
(3) Wir betrachten in $\mathbb{R}^2$ das Sechseck mit den Eckpunkten $\{(\mathrm{Re}(z), \mathrm{Im}(z)) \,|\, z \in \mathbb{C},\ z^6 = 1\}$. 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*.)
(4) * 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 $w_1 * w_2 = w_2 * w_1$.

BEISPIEL 4.12 (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

BEISPIEL 4.13. Permutationsgruppen und die Zyklenschreibweise Für $n \in \mathbb{N}$ sei

$$S_n := \{f : \{1, 2, \ldots, n\} \to \{1, 2, \ldots, n\} \,|\, f \text{ ist bijektiv }\}.$$

Diese Gruppe hat $n!$ Elemente, sie 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 $f : \{1, \ldots, n\} \to \{1, \ldots, n\}$, $f(i_1) = i_2$, $f(i_2) = i_3$, …, $f(i_{m-1}) = i_m$, $f(i_m) = i_1$, $f(j) = j$ 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

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 2 & 1 & 5 & 4 \end{pmatrix} = \begin{pmatrix} 1 & 3 \end{pmatrix}\begin{pmatrix} 4 & 5 \end{pmatrix} = \begin{pmatrix} 3 & 1 \end{pmatrix}\begin{pmatrix} 5 & 4 \end{pmatrix} = \begin{pmatrix} 5 & 4 \end{pmatrix}\begin{pmatrix} 3 & 1 \end{pmatrix}$$

und

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 3 & 5 & 4 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 & 5 \end{pmatrix}.$$

DEFINITION 4.14. Eine Gruppe $(G, \cdot, ^{-1}, 1)$ ist *abelsch*, wenn für alle $x, y \in G$ gilt, dass $x \cdot y = y \cdot x$.

Die Gruppe S_3 ist nicht abelsch:

$$\left.\begin{array}{l} \begin{pmatrix} 1 & 2 \\ 1 & 3 \end{pmatrix} \circ \begin{pmatrix} 1 & 3 \\ 1 & 2 \end{pmatrix} = \begin{pmatrix} 1 & 3 & 2 \\ 1 & 2 & 3 \end{pmatrix} \\ \begin{pmatrix} 1 & 3 \\ 1 & 3 \end{pmatrix} \circ \begin{pmatrix} 1 & 2 \\ 1 & 2 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix} \end{array}\right] \neq .$$

Insgesamt gilt, dass S_n genau dann abelsch ist, wenn $n \geq 2$. Wenn $n \geq 3$, dann ist S_n nicht abelsch.

ÜBUNGSAUFGABEN 4.15.

(1) Sei $(G, \cdot)$ eine abelsche Gruppe mit n Elementen. Zeigen Sie, dass für jedes $g \in G$ gilt: $g^n = 1_G$. *Hinweis:* Für $G := (\mathbb{Z}_n^*, \cdot)$ ist das der Satz von Euler. *Bemerkung: Dieser Satz gilt nicht nur für abelsche, sondern für alle Gruppen.*

4. Permutationsgruppen und der Satz von Cayley

DEFINITION 4.16. Seien $\boldsymbol{G} := (G, \cdot_G, i_G, 1_G)$ und $\boldsymbol{H} := (H, \cdot_H, i_H, 1_H)$ Gruppen. $\boldsymbol{H}$ ist eine *Untergruppe von* $\boldsymbol{G}$, wenn $H \subseteq G$ und für alle $h_1, h_2 \in H$ gilt $h_1 \cdot_H h_2 = h_1 \cdot_G h_2$, $i_G(h_1) = i_H(h_1)$, $1_G = 1_H$.

Wir unterscheiden hier also auch in der Notation zwischen der algebraischen Struktur $\boldsymbol{G} = (G, \cdot_G, i_G, 1_G)$ und ihrer Trägermenge G; G heißt auch das *Universum* von $\boldsymbol{G}$. Wenn aus dem Kontext klar ist, ob die Gruppe oder die Menge gemeint ist, bezeichnet man oft sowohl die algebraische Struktur als auch ihre Trägermenge mit dem gleichen Buchstaben; so kann etwa S_n sowohl die Menge aller Bijektionen auf $\{1, \ldots, n\}$ als auch die Gruppe dieser Bijektionen mit der Hintereinanderausführung als Gruppenmultiplikation sein.

DEFINITION 4.17. Sei $\boldsymbol{G} = (G, \cdot, i, 1)$ eine Gruppe. Die Menge H heißt *Trägermenge einer Untergruppe* oder *Subuniversum* von $\boldsymbol{G}$, wenn $1_G \in H$ und für alle $h_1, h_2 \in H$ auch $h_1 \cdot h_2 \in H$ und $h_1^{-1} \in H$ gilt.

Wenn H ein Subuniversum von $\boldsymbol{G}$ ist, so ist $(H, \cdot|_{H\times H}, {}^{-1}|_H, 1_G)$ ist eine Untergruppe von $\boldsymbol{G}$.

ÜBUNGSAUFGABEN 4.18.

(1) Sei $(G, \cdot, {}^{-1}, 1)$ eine Gruppe und sei H eine nichtleere Teilmenge von G, sodass für alle $h_1, h_2 \in H$ auch $h_1^{-1} \cdot h_2$ in H liegt. Zeigen Sie, dass H dann Trägermenge einer Untergruppe von $(G, \cdot, {}^{-1}, 1)$ ist.
(2) Sei $(G, \cdot, {}^{-1}, 1)$ eine Gruppe und sei H eine nichtleere Teilmenge von G, sodass für alle $h_1, h_2 \in H$ auch $h_1 \cdot h_2$ in H liegt. Muss H dann Trägermenge einer Untergruppe von $(G, \cdot, {}^{-1}, 1)$ sein?
(3) Sei $(G, \cdot, {}^{-1}, 1)$ eine Gruppe und sei H eine nichtleere Teilmenge von G, sodass für alle $h_1 \in H$ auch ${h_1}^{-1}$ in H liegt. Muss H dann Trägermenge einer Untergruppe von $(G, \cdot, {}^{-1}, 1)$ sein?
(4) Sei $(G, \cdot, {}^{-1}, 1)$ eine Gruppe, sei H eine nichtleere Teilmenge von G, und sei e ein Element von H. Wir nehmen an, dass $(H, \cdot|_{H\times H}, {}^{-1}|_H, e)$ eine Gruppe ist. Zeigen Sie $e = 1_G$.
(5) Sei $(G, \cdot, {}^{-1}, 1)$ eine Gruppe und sei H eine endliche nichtleere Teilmenge von G, sodass für alle $h_1, h_2 \in H$ auch $h_1 \cdot h_2$ in H liegt. Muss H dann Trägermenge einer Untergruppe von $(G, \cdot, {}^{-1}, 1)$ sein?

Wir bestimmen die Trägermengen von Untergruppen der Gruppe S_3 und erhalten

(1) $\{\mathrm{id}\}$,
(2) $\{\mathrm{id}, (12)\}$,
(3) $\{\mathrm{id}, (13)\}$,

(4) $\{\mathrm{id}, (23)\}$,
(5) $\{\mathrm{id}, (123), (132)\}$,
(6) S_3.

ÜBUNGSAUFGABEN 4.19.

(1) Welche der folgenden Mengen sind Trägermengen von Untergruppen der Gruppe S_n? ($n \geq 2$).
   (a) $A = \{f \in S_n \mid f(1) = 1\}$;
   (b) $B = \{f \in S_n \mid f(2) > f(1)\}$;
   (c) * $C = \{f \in S_n \mid \forall k \in \{1, 2, \ldots, n\} : f(k) \equiv k \cdot f(1) \pmod{n}\}$.
   Berechnen Sie die Anzahl der Elemente von A, B, und C!

DEFINITION 4.20. Seien $(G, \cdot, ^{-1}, 1)$, $(H, \odot, ^{-1_H}, 1_H)$ Gruppen. Eine Abbildung $\varphi : G \to H$ heißt Gruppenhomomorphismus $:\Leftrightarrow$

(1) $\varphi(g_1 \cdot g_2) = \varphi(g_1) \odot \varphi(g_2)$ für alle $g_1, g_2 \in G$,
(2) $\varphi(g_1^{-1}) = (\varphi(g_1))^{-1_H}$,
(3) $\varphi(1) = 1_H$.

BEISPIEL 4.21. Sei $G := (\mathbb{R}^+, \cdot)$ und sei $H := (\mathbb{R}, +)$. Dann ist $\varphi : \mathbb{R} \to \mathbb{R}^+, x \mapsto \ln(x)$ ein Homomorphismus.

BEISPIEL 4.22. Die Abbildung

$$\begin{aligned} \varphi : \quad & \mathbb{Z} \to \mathbb{Z}_n \\ & x \mapsto [x]_n \end{aligned}$$

ist ein Gruppenhomomorphismus von $(\mathbb{Z}, +)$ nach $(\mathbb{Z}_n, +)$.

DEFINITION 4.23. Gruppenomomorphismen, die injektiv sind, heißen *Monomorphismen*; surjektive Gruppenhomomorphismen heißen *Epimorphismen*, bijektive *Isomorphismen*. Homomorphismen einer Gruppe in sich selbst heißen *Endomorphismen*, bijektive Endomorphismen heißen *Automorphismen*.

BEISPIEL 4.24. Seien $\boldsymbol{H}$ und $\boldsymbol{K}$ die Untergruppen von S_3 mit den Trägermengen

$$H := \{(), (1, 2, 3), (1, 3, 2)\}, K := \{(), (1, 2)\}.$$

Dann ist $\boldsymbol{H}$ isomorph zur Gruppe $(\mathbb{Z}_3, +)$, und $\boldsymbol{K}$ isomorph zur Gruppe $(\mathbb{Z}_2, +)$.

ÜBUNGSAUFGABEN 4.25.

(1) Wir haben einen Gruppenhomomorphismus als eine Abbildung $\varphi : \boldsymbol{G} \to \boldsymbol{H}$ definiert, die folgende drei Bedingungen erfüllt:
   (a) $\varphi(g_1 \cdot_{\boldsymbol{G}} g_2) = \varphi(g_1) \cdot_{\boldsymbol{H}} \varphi(g_2)$ für alle $g_1, g_2 \in G$;
   (b) $\varphi(g_1^{-1_{\boldsymbol{G}}}) = (\varphi(g_1))^{-1_{\boldsymbol{H}}}$ für alle $g_1 \in G$;
   (c) $\varphi(1_{\boldsymbol{G}}) = 1_{\boldsymbol{H}}$.
   Seien $\boldsymbol{G}$ und $\boldsymbol{H}$ Gruppen, und sei ψ eine Abbildung, die die erste Bedingung

   $$\psi(g_1 \cdot_{\boldsymbol{G}} g_2) = \psi(g_1) \cdot_{\boldsymbol{H}} \psi(g_2) \text{ für alle } g_1, g_2 \in G$$

   erfüllt. Zeigen Sie, dass ψ dann ein Gruppenhomomorphismus ist, das heißt, zeigen Sie, dass ψ auch die anderen beiden Bedinungen erfüllt. *Hinweis:* Starten Sie mit der dritten Bedingung!
(2) Finden Sie alle Gruppenendomorphismen von $(\mathbb{Z}_n, +)$! Wieviele davon sind Automorphismen?

(3) Die Ordnung eines Gruppenelements g ist das kleinste $n \in \mathbb{N}$, sodass $g^n = 1$. Sei φ ein Gruppenhomomorphismus. Seien $\boldsymbol{G}$ und $\boldsymbol{H}$ 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.
(4) Finden Sie das kleinste $m \in \mathbb{N}$, sodass die Gruppe $(\mathbb{Z}_{30}, +)$ in die symmetrische Gruppe $\boldsymbol{S}_m$ einbettbar ist!
(5) Finden Sie eine 4-elementige Untergruppe der S_4, die nicht isomorph zur $\mathbb{Z}_4$ ist.
(6) 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.
(7) 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.
(8) 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.
(9) Seien $n, m \in \mathbb{N}$. Finden Sie alle Homomorphismen von $(\mathbb{Z}_n, +)$ nach $(\mathbb{Z}_m, +)$.
(10) Zeigen Sie, dass die Abbildung $f : G \to G, g \mapsto g^{-1}$ genau dann ein Homomorphismus ist, wenn G abelsch ist.
(11) Sei $\boldsymbol{G}$ 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:

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

Geben Sie einen Gruppenisomorphismus von $\boldsymbol{H}$ nach $\boldsymbol{G}$ an!

DEFINITION 4.26. Die Gruppe A heißt *einbettbar* in die Gruppe G (geschrieben als $A \hookrightarrow G$), wenn es einen Monomorphismus von A nach G gibt.

Sei φ der Monomorphismus von A nach G. Da das Bild $\varphi(A) = \{\varphi(a) \mid a \in A\}$ Trägermenge einer Untergruppe von G ist, ist A dann sogar isomorph zu einer Untergruppe von G.

BEISPIEL 4.27. Ist S_3 einbettbar in S_4 ? Wir betrachten folgende Abbildung:

$$\begin{array}{rcccc} \varphi & : & S_3 & \longrightarrow & S_4 \\ & & f & \longmapsto & \varphi(f), \end{array}$$

wobei $\varphi(f)$ definiert ist durch

$$\begin{array}{rcccc} \varphi(f) & : & \{1,2,3,4\} & \longrightarrow & \{1,2,3,4\} \\ & & x & \longmapsto & \begin{cases} f(x) & \text{falls } x \leq 3 \\ 4 & \text{falls } x = 4. \end{cases} \end{array}$$

Die Abbildung φ ist ein Monomorphismus; S_3 ist also einbettbar in S_4.

BEISPIEL 4.28. Ist $(\mathbb{Z}_4, +)$ in S_4 einbettbar? Da

$$\{id, \begin{pmatrix} 1 & 2 & 3 & 4 \end{pmatrix}, \begin{pmatrix} 1 & 3 \end{pmatrix} \begin{pmatrix} 2 & 4 \end{pmatrix}, \begin{pmatrix} 1 & 4 & 3 & 2 \end{pmatrix}\}$$

Trägermenge einer Untergruppe von S_4 ist, die isomorph zur Gruppe $(\mathbb{Z}_4, +)$ ist, gilt $(\mathbb{Z}_4, +) \hookrightarrow S_4$.

Der Satz von Cayley besagt, dass jede Gruppe in irgendeine Gruppe S_X einbettbar ist; anders gesagt: jede Gruppe ist isomorph zu irgendeiner Untergruppe irgendeiner S_X.

SATZ 4.29 (Satz von Cayley). *Sei $\boldsymbol{G} = (G, \cdot, ^{-1}, 1)$ eine Gruppe. Dann ist $\boldsymbol{G}$ einbettbar in $(S_G, \circ, ^{-1}, id_G)$.*

Eine n-elementige Gruppe ist also isomorph zu einer Untergruppe der S_n.

Beweis: Sei

$$\begin{aligned} \Phi: \quad G &\to S_G \\ g &\mapsto \Phi(g) \end{aligned},$$

wobei

$$\begin{aligned} \Phi(g): \quad G &\to G \\ x &\mapsto g \cdot x. \end{aligned}$$

Wir zeigen nun einige Eigenschaften von Φ:

(1) *Für alle $g \in G$ ist $\Phi(g)$ eine bijektive Abbildung von G nach G.* Wir fixieren $g \in G$, und zeigen als erstes, dass $\Phi(g)$ injektiv ist. Dazu fixieren wir $x, y \in G$ so, dass $\Phi(g)(x) = \Phi(g)(y)$. Es gilt dann $g \cdot x = g \cdot y$, daher auch $g^{-1} \cdot (g \cdot x) = g^{-1} \cdot (g \cdot y)$, und somit $x = y$. Um zu zeigen, dass $\Phi(g)$ surjektiv ist, fixieren wir $y \in G$ und suchen ein x mit $\Phi(g)(x) = y$. Wir finden dieses x als $x := g^{-1} \cdot y$.
(2) Φ *ist injektiv.* Seien $g, h \in G$. Wir nehmen an, dass $\Phi(g) = \Phi(h)$ gilt. Dann gilt auch $\Phi(g)(1) = \Phi(h)(1)$, also $g \cdot 1 = h \cdot 1$. Daher gilt $g = h$.
(3) Φ *ist Homomorphismus.* Dazu ist zu zeigen:

$$\forall g, h \in G : \Phi(g \cdot h) = \Phi(g) \circ \Phi(h)$$

Wir fixieren $g, h \in G$ und zeigen:

$$\forall x \in G : \Phi(g \cdot h)(x) = (\Phi(g) \circ \Phi(h))(x). \tag{4.1}$$

Wir fixieren $x \in G$ und berechnen beide Seiten von (4.1). Die linke Seite erhalten wir durch

$$\Phi(g \cdot h)(x) = (g \cdot h) \cdot x.$$

Die rechte Seite:

$$\begin{aligned} (\Phi(g) \circ \Phi(h))(x) &= \Phi(g)(\Phi(h)(x)) \\ &= \Phi(g)(h \cdot x) \\ &= g \cdot (h \cdot x). \end{aligned}$$

Daher ist Φ ein Monomorphismus. ■

BEISPIEL 4.30. Wir betten $(\mathbb{Z}_3, +)$ in die Gruppe $S_{\{[0]_3,[1]_3,[2]_3\}}$ ein.

$$\begin{aligned} &[0]_3 \mapsto \varphi_0, \quad \varphi_0(x) = [0]_3 + x, \quad \varphi_0 = ([0]_3)([1]_3)([2]_3) = () \\ &[1]_3 \mapsto \varphi_1, \quad \varphi_1(x) = [1]_3 + x, \quad \varphi_1 = ([0]_3\,[1]_3\,[2]_3) \\ &[2]_3 \mapsto \varphi_2, \quad \varphi_2(x) = [2]_3 + x, \quad \varphi_2 = ([0]_3\,[2]_3\,[1]_3) \end{aligned}$$

5. Sätze von Lagrange und Fermat

SATZ 4.31. *Sei H eine Trägermenge einer Untergruppe von $(G,\cdot)$. Wir definieren auf G eine Relation durch*

$$x \sim_H y :\Leftrightarrow x^{-1} \cdot y \in H.$$

Dann ist $\sim_H$ eine Äquivalenzrelation. Außerdem gilt:

(1) $x \sim_H y \Leftrightarrow x \in y \cdot H = \{y \cdot h \mid h \in H\}$;
(2) *Die Äquivalenzklasse von y bezüglich $\sim_H$ ist die Menge $y \cdot H$;*
(3) *Alle Äquivalenzklassen haben gleich Kardinalität, und die Kardinalität einer solchen Klasse ist $|H|$.*

Beweis: Wir zeigen zunächst, dass $\sim_H$ eine Äquivalenzrelation ist.

- $\sim_H$ *ist reflexiv:* Wir fixieren $x \in G$. Zu zeigen ist $x \sim_H x$. Das gilt, falls $x^{-1} \cdot x$ in H liegt. Da H Trägermenge einer Untergruppe von $(G,\cdot)$ ist, gilt $1 \in H$.
- $\sim_H$ *ist symmetrisch:* Wir fixieren $x, y \in G$ mit $x \sim_H y$. Zu zeigen ist $y \sim_H x$, also $y^{-1} \cdot x \in H$. Da $x^{-1} \cdot y \in H$ und H Trägermenge einer Untergruppe ist, liegt auch $(x^{-1} \cdot y)^{-1}$ in H. Daher gilt auch $y^{-1} \cdot (x^{-1})^{-1} = y^{-1} \cdot x \in H$.
- $\sim_H$ *ist transitiv:* Wir fixieren $x, y, z \in G$, sodass $x \sim_H y$ und $y \sim_H z$. Zu zeigen ist $x \sim_H z$. Da $x^{-1} \cdot y \in H$ und $y^{-1} \cdot z \in H$, gilt auch $x^{-1} \cdot y \cdot y^{-1} \cdot z \in H$, und daher $x^{-1} \cdot z \in H$.

Nun zeigen wir die drei angegebenen Eigenschaften von $\sim_H$:

(1) "⇒": Sei $x \sim_H y$. Zu zeigen ist $x \in y \cdot H$. Da $x \sim_H y$, gilt $x^{-1} \cdot y \in H$. Es gibt also $h \in H$ mit $x^{-1} \cdot y = h$. Dann gilt $x^{-1} = h \cdot y^{-1}$, und damit auch $x = y \cdot h^{-1}$. Somit gilt $x \in y \cdot H$. "⇐": Sei $h \in H$ so, dass $x = y \cdot h$. Dann ist $y^{-1} \cdot x = h$, somit gilt $y \sim_H x$, und, da $\sim_H$ symmetrisch ist, gilt auch $x \sim_H y$.
(2) Sei $y \in G$. Wir suchen die Menge

$$[y]_\sim := \{x \in G \mid x \sim_H y\}.$$

Wegen Eigenschaft (1) ist diese Menge gegeben durch $\{x \in G \mid x \sim_H y\} = y \cdot H$. Die Menge $[y]_\sim$ schreibt man oft auch als $y/\sim$.
(3) Für alle $y \in G$ ist die Abbildung

$$\begin{array}{rccc} \psi & : & H & \longrightarrow & y \cdot H \\ & & h & \longmapsto & y \cdot h \end{array}$$

bijektiv.

Die letzte Eigenschaft sagt, dass alle Äquivalenzklassen der Relation $\sim_H$ gleich viele Elemente haben. Das ergibt folgende Konsequenz:

SATZ 4.32 (Satz von Lagrange). *Sei H Trägermenge einer Untergruppe der endlichen Gruppe $(G,\cdot)$. Dann gilt: $|H|$ teilt $|G|$.*

Die Anzahl der Elemente von G heißt auch *die Ordnung* von G. Der Satz von Lagrange sagt also, dass die Ordnung einer Untergruppe ein Teiler der Ordnung der Gruppe ist.

DEFINITION 4.33. Sei G eine Gruppe und $g \in G$. Die kleinste Untergruppe von G, die g enthält, heißt die von g erzeugte Untergruppe. Wir kürzen die Trägermenge der von g erzeugten Untergruppe mit $\langle g \rangle$ ab.

Wie kann $\langle g \rangle$ aussehen?

(1) *Fall: Es gibt $n \in \mathbb{N}$ mit $g^n = 1$:* Dann gilt $\langle g \rangle = \{g^1, g^2, \ldots, g^m = 1\}$, wobei m das kleinste $m \in \mathbb{N}$ mit $g^m = 1$ ist. Die Gruppe $(\langle g \rangle, \cdot)$ ist dann isomorph zu $(\mathbb{Z}_m, +)$.
(2) *Fall: Es gibt kein $n \in \mathbb{N}$ mit $g^n = 1$:* Dann gilt $\langle g \rangle = \{\ldots, g^{-2}, g^{-1}, 1_G, g, g^2, \ldots\}$. Die Gruppe $(\langle g \rangle, \cdot)$ ist dann isomorph zu $(\mathbb{Z}, +)$.

Eine Gruppe G die ein $g \in G$ besitzt, sodass $\langle g \rangle = G$, heißt *zyklisch*. Jede zyklische Gruppe ist isomorph zu einem $(\mathbb{Z}_m, +)$ $(m \in \mathbb{N})$, oder zu $(\mathbb{Z}, +)$.

DEFINITION 4.34. Sei $(G, \cdot)$ eine Gruppe, und sei g ein Element von G. Mit $\operatorname{ord}(g)$ (*Ordnung von g*) bezeichnen wir das kleinste $m \in \mathbb{N}$, sodass $g^m = 1_G$, falls es ein solches m gibt; sonst schreiben wir $\operatorname{ord} g = \infty$.

BEISPIEL 4.35. Wir berechnen die Ordnung zweier Elemente der Gruppe $(\mathbb{Z}_5 \backslash \{0\}, \cdot)$. Es gilt $\operatorname{ord}([2]_5) = |\langle g \rangle| = |\{2, 4, 3, 1\}| = 4$, und $\operatorname{ord}([4]_5) = |\{4, 1\}| = 2$.

SATZ 4.36 (Satz von Fermat). *Sei $(G, \cdot)$ eine endliche Gruppe und sei $g \in G$. Dann gilt:*

(1) $\operatorname{ord}(g)$ *teilt* $|G|$*;*
(2) $g^{|G|} = 1_G$.

Beweis: (1) Die Gruppe $(\langle g \rangle, \cdot)$ hat $\operatorname{ord}(g)$ Elemente. Nach dem Satz von Lagrange teilt also $\operatorname{ord}(g)$ die Zahl $|G|$. (2) Aus der Definition von $\operatorname{ord}(g)$ erhalten wir $g^{\operatorname{ord}(g)} = 1_G$. Daher gilt auch $g^{|G|} = (g^{\operatorname{ord}(g)})^{\frac{|G|}{\operatorname{ord}(g)}} = 1_G$. ■

Der Satz von Fermat liefert auch ein Ergebnis aus der Zahlentheorie. Für $\mathbb{Z}_n^* := \{[x]_n \mid x \in \mathbb{Z} \text{ und } \operatorname{ggT}(x, n) = 1\}$ hat die Gruppe $(\mathbb{Z}_n^*, \cdot)$ genau $\varphi(n)$ Elemente. Für jedes Element a dieser Gruppe gilt daher $a^{\varphi(n)} = [1]_n$.

Für jede Permutation $\pi \in S_n$ gilt: $\pi^{n!} = \mathrm{id}$. Das hat Konsequenzen in der Kryptologie: Eine Verschlüsselungsabbildung E ist oft eine Permutation einer endlichen Menge; es gibt also ein $n \in \mathbb{N}$, sodass $E^n(x) = x$. Kennt man also $E(x)$ und die Funktion E, so iteriert man die Anwendung von E so lange, bis man $E^{n+1}(x) = E(x)$ erhält. Dann ist $E^n(x)$ der gesuchte Klartext (*repeated encryption*).

6. Die Abzähltheorie von Pólya

PROBLEM 4.37. *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.*

DEFINITION 4.38 (Gruppenoperation). Sei $(G, \cdot)$ eine Gruppe und X eine Menge. Eine Verknüpfung $* : G \times X \to X$ heißt Gruppenoperation, falls gilt:

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

Diese Gruppenoperationen geben uns eine Möglichkeit, ein mathematisches Modell 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:

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

Jede Symmetrieoperation des Quadrats ist eine Permutation der vier Eckpunkte. Alle Symmetrieoperationen erhalten wir aus folgendem Dialog mit GAP [**GAP99**]. 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 4.39. Sei G eine Gruppe, X eine Menge und $*$ eine Gruppenoperation von G auf X. Wir bezeichnen ξ und η in X als G-äquivalent, falls es ein $g \in G$ gibt, sodass $\xi = g * \eta$. Wir schreiben dafür $\xi \approx_G \eta$.

Es gilt also

$$\xi \approx_G \eta :\Leftrightarrow \exists g \in G : g * \xi = \eta.$$

SATZ 4.40. *Sei G eine Gruppe, X eine Menge und $*$ eine Gruppenoperation von G auf X. Dann gilt:*

(1) *$\approx_G$ ist eine Äquivalenzrelation.*
(2) *Für ein $\xi \in X$ ist die Äquivalenzklasse $\xi/\approx_G = \{\eta \in X \mid \eta \approx_G \xi\}$ gegeben durch*

$$\{\eta \in X \mid \eta \approx_G \xi\} = \{g * \xi \mid g \in G\}.$$

$G * \xi := \{g * \xi \mid g \in G\}$ heißt "Bahn" oder "Orbit" von ξ unter der Operation von G. Wenn wir also die nichtäquivalenten Färbungen des Quadrats zählen wollen, dann müssen wir die *Anzahl der Bahnen* der Gruppenoperation von D_4 auf der Menge der Färbungen X berechnen. Diese Anzahl der Bahnen erhalten wir aus folgendem Satz:

SATZ 4.41 (Frobenius-Burnside-Lemma). *Sei G eine endliche Gruppe, sei X eine Menge, und sei $*$ eine Gruppenoperation von G auf X. Sei n die Anzahl der Bahnen von G auf X. Dann gilt:*

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

wobei $\mathrm{Fix}\,(g) = \{\xi \in X \mid g * \xi = \xi\}$

BEISPIEL 4.42. Bevor wir diesen Satz beweisen, wenden wir ihn auf das Abzählproblem an. Wir berechnen also $\mathrm{Fix}\,(g)$ für alle Elemente $g \in G$. Wir tun das zum Beispiel für $g = (1,4,3,2)$. Eine Färbung α liegt in $\mathrm{Fix}\,(g)$, falls für alle $z \in \{1,2,3,4\}$ gilt: $\alpha(z) = \alpha(g(z))$. Damit gilt: $\alpha(1) = \alpha(4)$, $\alpha(4) = \alpha(3)$, $\alpha(3) = \alpha(2)$, $\alpha(2) = \alpha(1)$. Also liegen in $\mathrm{Fix}\,(g)$ 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 $\mathrm{Fix}\,(g)$, 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. Der Satz von Burnside-Frobenius 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 4.43. 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 Frobenius-Burnside-Lemma erhalten wir für diese Anzahl $n = \frac{1}{|G|} \sum_{g \in G} |\mathrm{Fix}(g)|$ mit $\mathrm{Fix}(g) = \{\varphi \in X \mid g * \varphi = \varphi\}$.

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:

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

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

BEISPIEL 4.44. Wieviele verschiedene Färbungen eines Sechsecks gibt es, wenn wir zwei Färbungen als gleich betrachten, wenn sie durch Spiegelungen und Drehungen des Sechsecks ineinander übergehen? Wieder sollen drei Eckpunkte rot und drei blau sein. Wir erhalten folgende Tabelle:

()	$\binom{6}{3} = 20$
(26)(35)(1)(4)	4
(13)(46)(2)(5)	4
(15)(24)(3)(6)	4
$4 \times$ (12)(36)(45)	0
$2 \times$ (123456)	0
$2 \times$ (135)(246)	2

Wir bekommen nun für die Anzahl n der Bahnen $n = \frac{1}{12} \cdot (20 + 12 + 4) = 3$.

Beweis von Satz 4.41: Wir zählen die Elemente der Menge F auf zwei Arten, wobei

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

Wir erhalten

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

und

$$|F| = \sum_{\xi \in X} |\{g \in G : g * \xi = \xi\}|.$$

Die Menge $\{g \mid g * \xi = \xi\}$ heißt *Stabilisator von* ξ. Wir schreiben dafür auch $\mathrm{Stab}_G(\xi)$. Wir zeigen zunächst, dass für alle $\xi \in X$ gilt:

$$|G * \xi| = |\{g * \xi \ : \ g \in G\}| = \text{ Größe des Orbits von } \xi = \frac{|G|}{|\mathrm{Stab}_G(\xi)|} \tag{4.2}$$

Die Abbildung $\phi : G \to G * \xi, g \mapsto g * \xi$ ist surjektiv. Außerdem gilt $\phi(g) = \phi(h)$, falls $g * \xi = h * \xi$. Das gilt genau dann, wenn $g^{-1} \cdot h \in \mathrm{Stab}_G(\xi)$. Nun ist $S := \mathrm{Stab}_G(\xi)$ eine Untergruppe von G. Die Gleichheit $\phi(g) = \phi(h)$ gilt also genau dann, wenn $g^{-1} \cdot h \in S$. Jedes Element in $G * \xi$ hat also genau $|S|$ Urbilder unter ϕ, und es gilt:

$$|S| \cdot |G * \xi| = |G|.$$

Wir bekommen also:

$$\begin{aligned} \sum_{\xi \in X} |\{g \in G : g * \xi = \xi\}| &= \sum_{\xi \in X} |\mathrm{Stab}_G(\xi)| \\ &= \sum_{\xi \in X} \frac{|G|}{|G * \xi|}. \end{aligned}$$

Wir wählen nun Repräsentanten für die Orbits. Wir wählen also $\xi_1, \xi_2, \ldots, \xi_n$ so, dass $G * \xi_i \cap G * \xi_j = \emptyset$, und $G * \xi_1 \cup G * \xi_2 \cup \cdots \cup G * \xi_n = X$. Alle Elemente η in $G * \xi_1$ erfüllen $G * \eta = G * \xi_1$. Wir verwenden diese Eigenschaft, und rechnen:

$$\begin{aligned} \sum_{\xi \in X} \frac{|G|}{|G * \xi|} &= \sum_{j=1}^{n} |G * \xi_j| \cdot \frac{|G|}{|G * \xi_j|} \\ &= n \cdot |G|. \end{aligned}$$

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

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

■.

ÜBUNGSAUFGABEN 4.45.

(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 [**GAP99**]):

```
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) ]
```

7. Kongruenzrelationen auf Gruppen

DEFINITION 4.46. Sei $(G, \circ)$ eine Gruppe, und sei $\sim$ eine Relation auf G. Diese Relation $\sim$ ist *kompatibel* mit $\circ$, wenn für alle $g_1, g_2, h_1, h_2 \in G$ mit $g_1 \sim g_2$ und $h_1 \sim h_2$ auch

$$g_1 \circ h_1 \sim g_2 \circ h_2$$

gilt. Eine Äquivalenzrelation auf G, die kompatibel mit $\circ$ ist, heißt *Kongruenzrelation* von $(G, \circ)$.

Beispiel: Auf der Gruppe $(\mathbb{Z}, +)$ ist die Relation $\sim$, die durch

$$x \sim y :\Leftrightarrow 5 \text{ teilt } x - y$$

definiert ist, eine Kongruenzrelation.

ÜBUNGSAUFGABEN 4.47.

(1) Sei $(G, \circ)$ eine Gruppe, und sei $\sim$ eine Kongruenzrelation auf $(G, \circ)$. Seien $a, b \in G$ so, dass $a \sim b$. Zeigen Sie $a^{-1} \sim b^{-1}$.

SATZ UND DEFINITION 4.48. *Sei $\boldsymbol{G} = (G, \cdot, i, 1)$ eine Gruppe und α eine Kongruenzrelation von $\boldsymbol{G}$. Wir definieren nun Verknüpfungen auf der Faktormenge G/α durch*

$$(g_1/\alpha) \circ (g_2/\alpha) := (g_1 \cdot g_2)/\alpha$$

und

$$i'(g_1/\alpha) := i(g_1)/\alpha.$$

Dann sind $\circ$ und i' wohldefiniert. Außerdem ist $(G/\alpha, \circ, i', 1/\alpha)$ eine Gruppe, die Faktorgruppe *von $\boldsymbol{G}$ nach α.*

Wir beschreiben jetzt alle Kongruenzrelationen auf einer Gruppe.

DEFINITION 4.49. Sei $\boldsymbol{G}$ eine Gruppe, und sei $N \subseteq G$. N ist ein *Normalteiler* von $\boldsymbol{G}$, wenn N Trägermenge einer Untergruppe von $\boldsymbol{G}$ ist, und für alle $g \in G$ und für alle $n \in N$ auch $g^{-1} \cdot n \cdot g \in N$ liegt.

BEISPIELE 4.50.

- Sei $G = (\mathbb{Z}, +)$, $N = \{5 \cdot z \mid z \in \mathbb{Z}\}$. Dann ist N ein Normalteiler von $(\mathbb{Z}, +)$.
- Sei $(G, \cdot)$ abelsch. Dann ist jede Trägermenge einer Untergruppe ein Normalteiler von G.
- In S_3 sind folgende Untergruppen Normalteiler: Es gilt $(132) \circ (12) \circ (123) = (13)$, daher ist die Menge $\{(),\ (12)\}$ kein Normalteiler.

SATZ 4.51. *Sei $(G, \cdot)$ eine Gruppe, und sei $\sim$ eine Relation auf G. Dann sind folgende Aussagen äquivalent:*

(1) *Die Relation $\sim$ ist eine Kongruenzrelation auf G.*
(2) *Es gibt einen Normalteiler N von $(G, \cdot)$, sodass für alle $x, y \in G$ gilt : $x \sim y \Leftrightarrow x^{-1} \cdot y \in N$.*

Beweis: Wir zeigen zunächst die Implikation (1) $\Rightarrow$ (2):

Wir fixieren eine Kongruenzrelation $\sim$ auf G. Wir behaupten, dass

$$N := \{x \in G \mid x \sim 1_G\}$$

ein Normalteiler ist, und dass die Bedingung

$$x \sim y \Leftrightarrow x^{-1} \cdot y \in N \tag{4.3}$$

erfüllt ist. Zunächst zeigen wir, dass N Trägermenge einer Untergruppe von $(G, \cdot)$ ist. Wir fixieren $x, y \in N$ und zeigen $x^{-1} \in N$. Wir wissen, dass $x \sim 1_G$ gilt. Da $\sim$ eine Kongruenzrelation ist, gilt auch $x^{-1} \cdot x \sim x^{-1} \cdot 1_G$. Daher gilt $1_G \sim x^{-1}$ und somit auch $x^{-1} \in N$. Nun zeigen wir, dass auch $x \cdot y \in N$ liegt. Wir wissen $x \sim 1_G$ und $y \sim 1_G$; also gilt $x \cdot y \sim 1_G \cdot 1_G = 1_G$, und daher liegt $x \cdot y$ in N.

Um zu zeigen, dass N ein Normalteiler von $(G, \cdot)$ ist, fixieren wir $g \in G$ und $n \in N$ und zeigen $g^{-1} \cdot n \cdot g \in N$. Das Element $g^{-1} \cdot n \cdot g$ liegt in N, falls $g^{-1} \cdot n \cdot g \sim 1_G$ gilt. Wir wissen, dass $n \sim 1_G$ gilt. Daher gilt $g^{-1} \cdot n \sim g^{-1}$ und $g^{-1} \cdot n \cdot g \sim 1_G$.

Nun zeigen wir, dass die Eigenschaft (4.3) ebenfalls erfüllt ist: wir zeigen zuerst die Implikation "⇒". Wir fixieren $x, y \in G$ mit $x \sim y$. Dann gilt auch $x^{-1} \cdot x \sim x^{-1} \cdot y$, und somit liegt $x^{-1} \cdot y$ in N. Für "⇐" fixieren wir $x, y \in G$ mit $x^{-1} \cdot y \in N$. Es gilt dann $x^{-1} \cdot y \sim 1_G$, und daher auch $x \cdot x^{-1} \cdot y \sim x \cdot 1_G$, und somit $y \sim x$.

Jetzt zeigen wir die Implikation (2) ⇒ (1): Sei N ein Normalteiler von G und $\sim$ definiert durch

$$x \sim y \Leftrightarrow x^{-1} \cdot y \in N.$$

Wir müssen zeigen, dass $\sim$ eine Kongruenzrelation ist. Dazu fixieren wir $x_1, x_2, y_1, y_2 \in G$ mit $x_1 \sim x_2$ und $y_1 \sim y_2$. Zu zeigen ist $x_1 \cdot y_1 \sim x_2 \cdot y_2$, d.h.,

$$(x_1 \cdot y_1)^{-1} \cdot x_2 \cdot y_2 \in N,$$

also

$$y_1^{-1} \cdot x_1^{-1} \cdot x_2 \cdot y_2 \in N.$$

Wir haben ein $n \in N$, sodass $x_1^{-1} \cdot x_2 = n$. Dann ergibt sich

$$\begin{aligned} y_1^{-1} \cdot x_1^{-1} \cdot x_2 \cdot y_2 &= y_1^{-1} \cdot n \cdot y_2 \\ &= y_1^{-1} \cdot n \cdot y_1 \cdot y_1^{-1} \cdot y_2. \end{aligned}$$

Der letzte Ausdruck liegt in N.

Wenn $(G, \cdot)$ eine Gruppe und N ein Normalteiler von $(G, \cdot)$ ist, dann ist $\sim_N := \{(x, y) \in G \times G \mid x^{-1} \cdot y \in N\}$ eine Kongruenzrelation von $(G, \cdot)$. Die Faktorgruppe $(G/\sim_N, \circ)$ mit $(g \cdot N) \circ (h \cdot N) := (g \cdot h) \cdot N$ schreibt man auch einfach als G/N. Die Gruppe G/N heißt *Faktorgruppe* von G modulo N.

SATZ 4.52. *Seien $(G, \cdot)$ und $(H, \cdot)$ Gruppen und sei $\varphi : G \to H$ ein Homomorphismus. Dann ist* $\mathrm{Ker}(\varphi) = \{x \mid \varphi(x) = 1_H\}$ *ein Normalteiler von G. Außerdem gilt für alle $x, y \in G$, dass $x^{-1} \cdot y$ genau dann in* $\mathrm{Ker}(\varphi)$ *liegt, falls $\varphi(x) = \varphi(y)$.*

Für einen Gruppenhomomorphismus φ von $(G, \cdot)$ nach $(H, \cdot)$ bezeichnen wir mit $\mathrm{Im}(\varphi)$ die Menge $\{\varphi(g) \mid g \in G\}$. Die Menge $\mathrm{Im}(\varphi)$ ist dann Trägermenge einer Untergruppe von $(H, \cdot)$, und es gilt folgender Satz:

SATZ 4.53. *Seien $(G, \cdot)$ und $(H, \cdot)$ Gruppen und sei $\varphi : G \to H$ ein Homomorphismus. Dann ist die Gruppe* $(\mathrm{Im}(\varphi), \cdot)$ *isomorph zur Faktorgruppe* $G/\mathrm{Ker}(\varphi)$.

SATZ 4.54 (Satz von Sylow – 1. Teil). *Sei p eine Primzahl, sei $a \in N$, und sei $m \in \mathbb{N}$ so, dass* $\mathrm{ggT}(p, m) = 1$. *Sei G eine Gruppe mit $p^a \cdot m$ Elementen. Dann hat G eine Untergruppe mit p^a Elementen.*

Für den Beweis, siehe z.B. [**Rob03**].

8. Direkte Produkte von Gruppen

Man kann für zwei Gruppen $\boldsymbol{G}, \boldsymbol{H}$ ihr *direktes Produkt* definieren. Dieses Produkt hat als Trägermenge $G \times H$, die Operationen werden komponentenweise ausgeführt. Die folgende Definition ist allgemeiner:

SATZ UND DEFINITION 4.55. *Sei I eine nichtleere Menge, und für jedes $i \in I$ sei $\boldsymbol{G_i}$ eine Gruppe. Dann definieren wir $\prod\langle \boldsymbol{G_i} \mid i \in I\rangle$ als eine algebraische Struktur mit Trägermenge $\prod_{i\in I} G_i$. Seien $a = \langle a_i \mid i \in I\rangle$ und $b = \langle b_i \mid i \in I\rangle \in \prod_{i\in I} G_i$. Wir definieren $a \circ b := \langle a_i \circ_{G_i} b_i \mid i \in I\rangle$ und $a^{-1} := \langle a_i^{-1} \mid i \in I\rangle$. Dann ist $\prod\langle \boldsymbol{G_i} \mid i \in I\rangle := (\prod_{i\in I} G_i, \circ, {}^{-1}, \langle 1_{G_i} \mid i \in I\rangle)$ eine Gruppe, das* direkte Produkt der $\boldsymbol{G_i}$.

KAPITEL 5

Abelsche Gruppen

1. Erzeugen von Untergruppen

DEFINITION 5.1. Sei $\boldsymbol{G} = (G, \cdot)$ eine Gruppe, und sei $T \subseteq G$. Die *von T erzeugte Untergruppe* von $\boldsymbol{G}$ ist die Untergruppe von $\boldsymbol{G}$, deren Trägermenge durch $H := \bigcap\{U \mid T \subseteq U \subseteq G, U$ ist Subuniversum von $\boldsymbol{G}\}$ gegeben ist.

SATZ 5.2. *Sei $\boldsymbol{A} = (A, +)$ eine abelsche Gruppe, und seien $t_1, \ldots, t_n \in A$. Dann ist die Trägermenge H der von $\{t_1, \ldots, t_n\}$ erzeugten Untergruppe von $\boldsymbol{A}$ gegeben durch $H := \{z_1 * t_1 + \cdots + z_n * t_n \mid z_1, \ldots, z_n \in \mathbb{Z}\}$.*

DEFINITION 5.3. Eine Gruppe $\boldsymbol{G}$ heißt *endlich erzeugt*, wenn es eine endliche Teilmenge T von G gibt, sodass die von T erzeugte Untergruppe von $\boldsymbol{G}$ die gesamte Gruppe $\boldsymbol{G}$ ist.

2. Die Charakterisierung endlich erzeugter abelscher Gruppen

SATZ 5.4 ([**Pil84**, Satz 15.5]). *Für jede endlich erzeugte abelsche Gruppe $\boldsymbol{G}$ gibt es natürliche Zahlen $k, r \in \mathbb{N}_0$, $t_1, \ldots, t_k \in \mathbb{N}$ und Primzahlen $p_1, \ldots, p_k$ (nicht notwendigerweise verschieden), sodass $\boldsymbol{G} \cong \mathbb{Z}_{p_1^{t_1}} \times \cdots \times \mathbb{Z}_{p_k^{t_k}} \times \mathbb{Z}^r$.*

LEMMA 5.5. *Sei G eine abelsche Gruppe, sei $k \in \mathbb{N}$, seien $g_1, \ldots, g_k \in G$, und seien $n_1, \ldots, n_k \in \mathbb{Z}$. Wir nehmen an, dass* $\mathrm{ggT}(n_1, \ldots, n_k) = 1$. *Dann gibt es $h_1, \ldots, h_k \in G$, sodass*

$$h_1 = \sum_{i=1}^{k} n_i * g_i,$$

und

$$\langle g_1, \ldots, g_k \rangle = \langle h_1, \ldots, h_k \rangle .$$

Beweis: Wir zeigen durch Induktion, dass für alle $n \in \mathbb{N}$ die Aussage $A(n)$ gilt, die so definiert ist:

> Für alle $n_1, \ldots, n_k \in \mathbb{Z}$, sodass $\mathrm{ggT}(n_1, \ldots, n_k) = 1$ und $\sum_{i=1}^{k} |n_i| = n$, und für alle $g_1, \ldots, g_k \in G$ gibt es $h_1, \ldots, h_k \in G$ sodass $h_1 = \sum_{i=1}^{k} n_i * g_i$ und $\langle g_1, \ldots, g_k \rangle = \langle h_1, \ldots, h_k \rangle$.

$A(1)$ ist unmittelbar klar. Wir fixieren nun $n \geq 2$ und nehmen an, $A(i)$ gilt für alle $i \in \mathbb{N}$ mit $i < n$. Seien $n_1, \ldots, n_k \in \mathbb{Z}$. Wir nehmen an, dass $\mathrm{ggT}(n_1, \ldots, n_k) = 1$ und $\sum_{i=1}^{k} |n_i| = n$. Seien $g_1, \ldots, g_k \in G$. Da $\mathrm{ggT}(n_1, \ldots, n_k) = 1$ und $\sum_{i=1}^{k} |n_i| \geq 2$, sind zumindest zwei $n_i \neq 0$. Seien $a, b \in \{1, \ldots, k\}$ so, dass $a \neq b$ und $|n_a| \geq |n_b| > 0$. Wir setzen nun

$$h_1 := \sum_{i=1}^{k} n_i * g_i.$$

Es gilt

$$h_1 = \sum_{i=1}^{k} |n_i| * (\mathrm{sgn}(n_i) * g_i).$$

Wir setzen $g_i' := \mathrm{sgn}(n_i) * g_i$ für $i = 1, \ldots, k$. Es gilt also

$$h_1 = |n_a| * g_a' + |n_b| * g_b' + \sum_{i \in \{1,\ldots,k\} \setminus \{a,b\}} |n_i| * g_i'.$$

Somit gilt

$$h_1 = (|n_a| - |n_b|) * g_a' + |n_b| * (g_a' + g_b') + \sum_{i \in \{1,\ldots,k\} \setminus \{a,b\}} |n_i| * g_i'.$$

Da $|n_a| - |n_b| + |n_b| < |n_a| + |n_b|$, gibt es nach Induktionsvoraussetzung $h_2, \ldots, h_k \in G$, sodass

$$\left\langle \{g_a', g_a' + g_b'\} \cup \{g_i' \mid i \in \{1, \ldots, k\} \setminus \{a, b\}\} \right\rangle = \left\langle h_1, \ldots, h_k \right\rangle.$$

Es gilt

$$\begin{aligned} &\left\langle \{g_a', g_a' + g_b'\} \cup \{g_i' \mid i \in \{1, \ldots, k\} \setminus \{a, b\}\} \right\rangle \\ &\quad \supseteq \left\langle \{g_a', g_b'\} \cup \{g_i' \mid i \in \{1, \ldots, k\} \setminus \{a, b\}\} \right\rangle \\ &\quad = \left\langle g_1', g_2', \ldots, g_k' \right\rangle \\ &\quad = \left\langle g_1, g_2, \ldots, g_k \right\rangle. \end{aligned} \tag{5.1}$$

Somit haben wir die gewünschten $h_1, \ldots, h_k$ gefunden. ■

Beweis von Satz 5.4: Wir wählen ein k in $\mathbb{N}$, sodass $\boldsymbol{G}$ durch k Elemente erzeugbar ist, und definieren

$$E := \{(g_1, \ldots, g_k) \in G^k \mid \left\langle g_1, \ldots, g_k \right\rangle = G\}.$$

Jedem $(g_1, \ldots, g_k) \in G^k$ sei das Tupel $(\operatorname{ord} g_1, \ldots, \operatorname{ord} g_k) \in (\mathbb{N} \cup \{\infty\})^k$ zugeordnet. Wir ordnen $(\mathbb{N} \cup \{\infty\})^k$ lexikographisch, und wählen ein $(a_1, \ldots, a_k) \in G^k$, für das das zugeordnete Tupel minimal ist. Sei $l \in \{0, \ldots, k\}$ so, dass $\operatorname{ord} a_{l+1} = \cdots = \operatorname{ord} a_k = \infty$ und $\operatorname{ord} a_1, \ldots, \operatorname{ord} a_l \in \mathbb{N}$. Wir zeigen nun, dass die Gruppe $\boldsymbol{G}$ isomorph zur Gruppe $\boldsymbol{H}$ ist, wobei

$$\boldsymbol{H} := \mathbb{Z}_{\operatorname{ord} a_1} \times \mathbb{Z}_{\operatorname{ord} a_2} \times \cdots \times \mathbb{Z}_{\operatorname{ord} a_l} \times \mathbb{Z}^{k-l}.$$

Dazu betrachten wir die Abbildung

$$\begin{array}{rccc} \varphi & : & \mathbb{Z}^k & \longrightarrow & G \\ & & (z_1, \ldots, z_k) & \longmapsto & \sum_{i=1}^{k} z_i * a_i. \end{array}$$

Wir sehen leicht, dass φ ein Homomorphismus und surjektiv ist. Wir bestimmen nun den Kern von φ. Offensichtlich gilt

$$(\operatorname{ord} a_1)\mathbb{Z} \times (\operatorname{ord} a_2)\mathbb{Z} \times \cdots \times (\operatorname{ord} a_l)\mathbb{Z} \times \{0\}^{k-l} \subseteq \operatorname{Ker}(\varphi). \tag{5.2}$$

Wir zeigen nun, dass in (5.2) sogar Gleichheit gilt. Nehmen wir an, es gibt ein Element in $\operatorname{Ker}(\varphi)$, das nicht in der linken Seite von (5.2) liegt. Dann gibt es auch ein Element $(z_1, \ldots, z_k) \in \mathbb{Z}^k \setminus \{(0, \ldots, 0)\}$, sodass $0 \leq z_j < \operatorname{ord} a_j$ für alle $j \in \{1, \ldots, l\}$ und $(z_1, \ldots, z_k) \in \operatorname{Ker}(\varphi)$. Es gilt also

$$\sum_{i=1}^{k} z_i * a_i = 0.$$

Sei $j \in \{1, \ldots, k\}$ minimal, sodass $z_j \neq 0$. Wir definieren $z := \operatorname{ggT}(z_1, \ldots, z_k)$. Dann gilt

$$z * \left(\sum_{i=j}^{k} \frac{z_i}{z} * a_i\right) = 0.$$

Da $\operatorname{ggT}(\frac{z_1}{z}, \ldots, \frac{z_k}{z}) = 1$, gibt es nach Lemma 5.5 $b_j, \ldots, b_k \in G$, sodass

$$b_j = \sum_{i=j}^{k} \frac{z_i}{z} * a_i$$

und $\langle b_j, \ldots, b_k \rangle = \langle a_j, \ldots, a_k \rangle$. Daher gilt

$$\langle a_1, \ldots, a_{j-1}, a_j, \ldots, a_k \rangle = \langle a_1, \ldots, a_{j-1}, b_j, \ldots, b_k \rangle .$$

Wegen $z * b_j = 0$ gilt $\operatorname{ord} b_j \leq z \leq z_j < \operatorname{ord} a_j$; daher ist das Tupel

$$(\operatorname{ord} a_1, \ldots, \operatorname{ord} a_{j-1}, \operatorname{ord} b_j, \ldots, \operatorname{ord} b_k)$$

lexikographisch kleiner als das Tupel

$$(\operatorname{ord} a_1, \ldots, \operatorname{ord} a_{j-1}, \operatorname{ord} a_j, \ldots, \operatorname{ord} a_k);$$

das ist ein Widerspruch zur Wahl von $a_1, \ldots, a_k$. Daher muss in (5.2) Gleichheit gelten.

Wegen des Homomorphiesatzes ist G isomorph zu $\mathbb{Z}^k/\operatorname{Ker}(\varphi)$, es gilt also

$$G \cong \mathbb{Z}^k / \big((\operatorname{ord} a_1)\mathbb{Z} \times (\operatorname{ord} a_2)\mathbb{Z} \times \cdots \times (\operatorname{ord} a_l)\mathbb{Z} \times \{0\}^{k-l}\big).$$

Nun gilt für den Epimorphismus $\psi : \mathbb{Z}^k \to \mathbb{Z}_{\operatorname{ord} a_1} \times \cdots \times \mathbb{Z}_{\operatorname{ord} a_l} \times \mathbb{Z}^{k-l}$, $(x_1, \ldots, x_k, x_{k+1}, \ldots, x_l) \mapsto ([x_1]_{a_1}, \ldots, [x_k]_{a_k}, x_{k+1}, \ldots, x_l)$, dass $\operatorname{Ker}(\varphi) = \operatorname{Ker}(\psi)$. Also ist G auch isomorph zu $\operatorname{Im}(\psi)$, und somit gilt

$$G \cong \mathbb{Z}_{\operatorname{ord} a_1} \times \cdots \times \mathbb{Z}_{\operatorname{ord} a_l} \times \mathbb{Z}^{k-l}. \tag{5.3}$$

Sei $\operatorname{ord} a_1 = q_1^{\alpha_1} \cdots q_s^{\alpha_s}$, wobei alle q_i verschiedene Primzahlen sind. Da für relativ prime $a, b \in \mathbb{Z}$ gilt, dass $\mathbb{Z}_{ab}$ isomorph zu $\mathbb{Z}_a \times \mathbb{Z}_b$ ist, ist $\mathbb{Z}_{\operatorname{ord} a_j}$ isomorph zu $\prod_{i=1}^{s} \mathbb{Z}_{q_i^{\alpha_i}}$. Folglich gewinnt man aus (5.3) die gewünschte Zerlegung von $\boldsymbol{G}$ in ein Produkt zyklischer Gruppen von Primzahlpotenzordnung und Kopien von $\mathbb{Z}$. ■

Die Darstellung einer endlich erzeugten abelschen Gruppe als direktes Produkt von zyklischen Gruppen von Primzahlpotenzordnung und von Kopien von $\mathbb{Z}$ ist eindeutig.

SATZ 5.6. *Seien $k, l, r, s \in \mathbb{N}_0$, $t_1, \ldots, t_k \in \mathbb{N}$, $u_1, \ldots, u_l \in \mathbb{N}$, seien $p_1, \ldots, p_k$ (nicht notwendigerweise verschiedene) Primzahlen, und seien $q_1, \ldots, q_l$ (nicht notwendigerweise verschiedene Primzahlen). Seien*

$$\begin{aligned} \boldsymbol{G} &:= \mathbb{Z}_{p_1^{t_1}} \times \cdots \times \mathbb{Z}_{p_k^{t_k}} \times \mathbb{Z}^r \\ \boldsymbol{H} &:= \mathbb{Z}_{q_1^{u_1}} \times \cdots \times \mathbb{Z}_{q_l^{u_l}} \times \mathbb{Z}^s. \end{aligned}$$

Wir nehmen an, dass

$$\boldsymbol{G} \cong \boldsymbol{H}.$$

Außerdem nehmen wir an, dass die Faktoren in folgender Weise geordnet sind: Für alle $i, j \in \{1, \ldots, k\}$ mit $i \leq j$ gilt $p_i > p_j$ oder ($p_i = p_j$ und $t_i \geq t_j$), und für alle $i, j \in \{1, \ldots, l\}$ mit $i \leq j$ gilt $q_i > q_j$ oder ($q_i = q_j$ und $s_i \geq s_j$).

Dann gilt $r = s$, $k = l$, und für alle $i \in \{1, \ldots, k\}$: $p_i = q_i$.

KAPITEL 6

Ausgewählte Kapitel der Diskreten Mathematik

1. Graphen

DEFINITION 6.1. Ein *Graph* ist ein Tripel (V, E, I), wobei V, E endliche Mengen sind, $V \neq \emptyset$, $I \subseteq V \times E$, und für alle $e \in E$ die Menge $\{v \in V \mid (v, e) \in I\}$ zweielementig ist. Die Elemente aus V sind die *Knoten*, die Elemente aus E die *Kanten* des Graphen.

Falls $(v, e) \in I$, dann sagen wir, dass die Kante e mit dem Knoten v inzidiert. Falls $x, y \in V$ so sind, dass es ein $e \in E$ gibt, sodass $(x, e) \in I$ und $(y, e) \in I$, dann sagen wir, dass *e zwischen x und y verläuft.*

DEFINITION 6.2. Ein Graph heißt *einfach*, wenn zwischen zwei Knoten immer höchstens eine Kante verläuft.

Die hier verwendete Definition eines Graphen lässt keine Schleifen, also Kanten mit dem gleichen Anfangs- und Endpunkt zu.

DEFINITION 6.3. Sei (V, E, I) ein Graph, und sei v ein Knoten des Graphen. Dann ist der *Grad* von v definiert als die Anzahl der Kanten, die mit v inzidieren.

ÜBUNGSAUFGABEN 6.4.

(1) Sei (V, E, I) ein Graph. Zeigen Sie:
$$|I| = \sum_{v \in V} \text{Grad}\,(v).$$
(2) Sei (V, E, I) ein Graph. Zeigen Sie:
$$|I| = 2 \cdot |E|.$$
(3) Zeigen Sie, dass ein Graph eine gerade Anzahl von Knoten ungeraden Grades hat.
(4) Geben Sie eine Definition von Graphen, die Schleifen zulässt. Definieren Sie den Grad eines Knoten so, dass $\sum_{v \in V} \text{Grad}\,(v)$ das Doppelte der Kantenanzahl ist.
(5) Geben Sie eine Definition von Graphen, die Schleifen zulässt, und die es erlaubt, dass zwischen zwei Knoten mehr als eine Kante verläuft. Definieren Sie den Grad eines Knoten so, dass $\sum_{v \in V} \text{Grad}\,(v)$ das Doppelte der Kantenanzahl ist.

2. Eulersche Wege

DEFINITION 6.5. Sei $k \in \mathbb{N}_0$. Eine Folge $(x_0, e_1, x_1, e_2, x_2, \ldots, e_k, x_k)$ von Knoten und Kanten eines Graphen heißt *Verbindung der Länge k*, wenn alle x_i Knoten und alle e_k Kanten des Graphen sind, und außerdem für alle $i \in \{1, 2, \ldots, k\}$ die Knoten x_{i-1} und x_i

genau die Knoten sind, die mit e_i inzidieren. Eine Verbindung heißt *Weg*, wenn alle e_i voneinander verschieden sind. Ein Weg ist *geschlossen*, wenn $x_k = x_0$.

DEFINITION 6.6. Zwei Knoten eines Graphen sind *verbunden*, wenn es eine Verbindung mit Anfang x_0 und Ende x_k gibt. Die Relation "verbunden sein" ist eine Äquivalenzrelation auf den Knoten. Ihre Äquivalenzklassen heißen *Zusammenhangskomponenten* des Graphen. Ein Graph mit nur einer Zusammenhangskomponente heißt *zusammenhängend*.

DEFINITION 6.7. Ein geschlossener Weg in einem Graphen heißt *Eulerscher Kreis*, wenn er jede Kante des Graphen genau einmal enthält.

Der Name kommt daher, dass sich Euler überlegt hat, ob es einen Spaziergang über die sieben Brücken Königsbergs gibt, bei dem man über jede Brücke genau einmal geht.

SATZ 6.8. *Ein Graph enthält genau dann einen Eulerschen Kreis, wenn nur höchstens eine Zusammenhangskomponente Kanten enthält, und jeder Knoten geraden Grad hat.*

Beweis: Wir zeigen zunächst, dass die Bedingung, dass jeder Knoten geraden Grad hat, notwendig ist. Sei k die Länge des Weges, sei v ein Knoten, und sei

$$I(v) := \{i \in \{0, \ldots, k-1\} \mid x_i = v\}.$$

Dann inzidiert v mit allen Kanten in $\{e_i \mid i \in I(v)\} \cup \{e_{i+1} \mid i \in I(v)\}$. Der Knoten v inzidiert nur mit Kanten in dieser Menge: Wenn v mit einer Kante e inzidiert, muss e irgendwo im Eulerschen Kreis vorkommen, und somit gleich irgendeinem e_i sein. Dann ist aber entweder x_{i-1} oder x_i gleich v. Außerdem sind für $i, j \in I(v)$ mit $i \neq j$ die Mengen $\{e_i, e_{i+1}\}$ und $\{e_j, e_{j+1}\}$ disjunkt: wenn $e_i = e_{j+1}$, dann gilt auch $i = j+1$. Somit ist $x_j e_i x_i$ ein Teil des Kreises. Da $x_i = x_j = v$, inzidiert e_i nur mit v – ein Widerspruch zur Schleifenfreiheit des Graphen. Somit inzidiert v mit einer geraden Anzahl von Knoten.

Da ein Eulerscher Kreis nur Knoten der gleichen Zusammenhangskomponente enthält, müssen alle Kanten zwischen Knoten in der gleichen Zusammenhangskomponente verlaufen.

Wir zeigen nun, dass die Bedingung, dass jeder Knoten geraden Grad hat, hinreichend ist. Wir gehen mit Induktion nach der Anzahl der Kanten vor. Wenn der Graph keine Kanten enthält, so wählen wir einen Knoten v. Die Folge (v) ist ein Eulerscher Kreis der Länge 0. Wenn der Graph eine Kante e_1 enthält, so seien x_0 und x_1 die mit e_1 inzidierenden Knoten, sodass $x_0 e_1 x_1$ ein Weg ist. Wir verlängern diesen Weg, bis wieder nicht mehr weiter können. Da alle Knoten geraden Grad haben, kann das erst passieren, wenn wir ein k mit $x_k = x_0$ gefunden haben. Wir haben also einen Weg $x_0 e_1 x_1 \ldots e_k x_k$ mit $k \in \mathbb{N}$ gefunden. Wir bilden nun einen neuen Graphen G', indem wir aus G die Kanten $e_1, \ldots, e_k$ entfernen. Jeder Knoten von G' hat geraden Grad. Wir können nach Induktionsvoraussetzung in jeder Zusammenhangskomponente Z von G', die zumindest eine Kante enthält, einen Eulerschen Kreis $C(Z)$ finden. Jede dieser Komponenten

enthält zumindest ein x_i, und dann auch eine damit inzidierende Kante. Also können wir jeden Kreis $C(Z)$ an den Kreis $x_0 e_1 \cdots x_k$ anhängen. ■

3. Planare Graphen

DEFINITION 6.9. Ein Graph ist *planar*, wenn er sich in $\mathbb{R}^2$ "überschneidungsfrei zeichnen lässt".

DEFINITION 6.10. Ein ebener Graph ist ein Paar (G, Z), wobei G ein planarer Graph und Z eine überschneidungsfreie Zeichnung von G in $\mathbb{R}^2$ ist.

SATZ 6.11 (Euler). *Sei G ein zusammenhängender, ebener Graph mit v Knoten und e Kanten, der die Ebene in f Flächen unterteilt. Dann gilt*

$$v - e + f = 2.$$

Beweisskizze: Wir zeigen, dass für jeden ebenen Graphen mit z Zusammenhangskomponenten die Gleichung $v - e + f = 1 + z$ gilt. Das kann man durch Induktion nach der Kantenanzahl zeigen. ■

SATZ 6.12. *Sei G ein einfacher planarer Graph. Dann hat G einen Knoten, dessen Grad höchstens* 5 *ist.*

Beweis: ([**AZ98**]) Wir fixieren eine überschneidungsfreie Zeichnung des Graphen und bezeichnen mit v, e und f die Anzahl der Knoten, Kanten, beziehungsweise Flächen dieser Zeichnung. Wir nehmen an, dass $v \geq 3$ und dass G zusammenhängend ist. Wir bilden die Menge

$$F = \{(x, y, a) \mid x \in V, y \in V, \text{ von } x \text{ nach } y \text{ verläuft eine Kante von } V, \\ a \text{ ist die Fläche, die rechts von } xy \text{ liegt,} \\ \text{wenn man von } x \text{ nach } y \text{ geht.}\}$$

Für jede Fläche a definieren wir die Menge ihrer Begrenzungsseiten als

$$\{(x, y) \in V^2 \mid (x, y, a) \in F\}.$$

Für jedes $i \in \mathbb{N}$ sei f_i die Anzahl der Flächen mit genau i Begrenzungsseiten. Es gilt

$$f = \sum_{i \in \mathbb{N}} f_i,$$

$$|F| = 2e,$$

und

$$|F| = \sum_{i \in \mathbb{N}} f_i \cdot i.$$

Da G einfach und zusammenhängend ist, gilt $f_1 = f_2 = 0$, und somit

$$2e - 3f \geq 0.$$

Für jedes $i \in \mathbb{N}$ sei v_i die Anzahl der Knoten vom Grad i. Für die Inzidenzrelation I zwischen Knoten und Kanten gilt

$$|I| = 2e$$

und

$$|I| = \sum_{i \in \mathbb{N}} v_i \cdot i.$$

Ausserdem gilt

$$\sum_{i \in \mathbb{N}} v_i = v.$$

Wenn wir annehmen, dass alle Knoten Grad ≥ 6 haben, so gilt $v_1 = v_2 = \cdots = v_5 = 0$. Also gilt $2e - 6v \geq 0$. Also gilt $(2e - 6v) + 2(2e - 3f) \geq 0$, somit $-6v + 6e - 6f$ $v - e + f \leq 0$ im Widerspruch zur Eulerschen Flächenformel. ■

ÜBUNGSAUFGABEN 6.13.

(1) [**AZ98**, p.59] Sei G ein einfacher planarer Graph mit $v \geq 3$ Knoten und e Kanten. Dann gilt $e \leq 3v - 6$.
(2) [**AZ98**, p.59] Zeigen Sie, dass die Graphen K_5 (der vollständige Graph mit 5 Knoten) und $K_{3,3}$ (der vollständige bipartite Graph mit 2 mal 3 Knoten) nicht planar sind.

SATZ 6.14. *Sei G ein einfacher planarer Graph. Dann kann man die Knoten von G so mit* 6 *Farben färben, dass keine zwei Knoten, zwischen denen eine Kante verläuft, die gleiche Farbe haben.*

Es reichen sogar 4 (statt 6) Farben (*Vierfarbensatz*).

4. Der Satz von Ramsey

SATZ 6.15 (Satz von Ramsey). *Seien $p, t, n \in \mathbb{N}$. Dann gibt es eine Zahl $N \in \mathbb{N}$, sodass folgendes erfüllt ist:*

> *Sei X eine Menge mit N Elementen. Wir färben jede p-elementige Teilmenge von X mit einer von t Farben. Dann gibt es eine Menge $Y \subseteq X$ mit n Elementen, sodass alle p-elementigen Teilmengen von Y die gleiche Farbe haben.*

Für eine Menge X und eine Zahl $p \in \mathbb{N}$ bezeichnen wir mit $\binom{X}{p}$ die Menge aller p-elementigen Teilmengen von X. Dann kann man Satz 6.15 auch so formulieren:

SATZ 6.16. *Seien $p, t, n \in \mathbb{N}$. Dann gibt es eine Zahl $N \in \mathbb{N}$, sodass folgendes erfüllt ist:*

> *Für alle Mengen X mit $|X| = N$ und für alle Funktionen $c : \binom{X}{p} \to \{1, 2, \ldots, t\}$ gibt es eine Menge $Y \subseteq X$ mit n Elementen, sodass c auf $\binom{Y}{p}$ konstant ist.*

Das kleinste N, für das die Aussage erfüllt ist, bezeichnen wir mit $r(p,t,n)$ (Ramsey-Zahl). Dabei bezeichnen wir eine Funktion $f : A \to B$ als konstant, wenn $\forall a_1, a_2 \in A : f(a_1) = f(a_2)$ gilt; somit ist für jedes B jede Funktion $f : \emptyset \to B$ konstant.

Wir betrachten Spezialfälle:

- $p = 1, n = 2$: Es gibt ein N, sodass für jede Menge X mit N Elementen folgendes gilt: Wenn man die Elemente von X in t Klassen aufteilt, so gibt es zwei Elemente, die in der gleichen Klasse liegen. Daraus sehen wir $r(1,t,2) = t+1$. (Schubfachprinzip)

ÜBUNGSAUFGABEN 6.17.

(1) Berechnen Sie $r(1,t,n)$ für alle $t, n \in \mathbb{N}$.

Weitere Spezialfälle:

- $p = 2, t = 2, n = 3$: Man weiß, dass $r(2,2,3) = 6$ ist. Das heißt:
  Wenn man jede 2-elementige Teilmengen einer 6-elementigen Menge entweder rot oder blau färbt, dann gibt es drei Elemente a, b, c, sodass $\{a,b\}$, $\{a,c\}$ und $\{b,c\}$ die gleiche Farbe haben.

  Das kann man auch so formulieren:
  Sei K_6 der vollständige Graph mit 6 Knoten und $\binom{6}{2}$ Kanten. Wir färben jede Kante entweder rot oder blau. Dann enthält der Graph ein einfärbiges Dreieck, also drei Knoten x, y, z, sodass xy, xz und yz die gleiche Farbe haben.

ÜBUNGSAUFGABEN 6.18.

(1) Zeigen Sie $r(2,2,3) \leq 6$.
(2) Zeigen Sie $r(2,3,3) \leq 17$.
(3) Zeigen Sie $r(2,k,3) \leq (r(2,k-1,3)-1) \cdot k + 2$.
(4) (Lästiger Spezialfall I) Berechnen Sie $r(p,t,p)$!
(5) (Lästiger Spezialfall II) Sei $p \leq n$. Was ist $r(p,1,n)$?
(6) (Lästiger Spezialfall III) Sei $p > n$. Was ist $r(p,t,n)$?

LEMMA 6.19. *Seien $p, t \in \mathbb{N}$. Dann sind folgende Aussagen äquivalent:*

(1) *Für alle $n \in \mathbb{N}$ gibt es ein $N \in \mathbb{N}$, sodass es für jede Färbung der p-elementigen Teilmengen von $\{1, 2, \ldots, N\}$ mit t Farben eine n-elementige Teilmenge Y von $\{1, 2, \ldots, N\}$ gibt, sodass alle p-elementigen Teilmengen von Y die gleiche Farbe haben.*
(2) *Für alle $n \in \mathbb{N}$ gibt es ein $M \in \mathbb{N}$, sodass folgendes gilt: für jede M-elementige Teilmenge X der natürlichen Zahlen und für jede Färbung der p-elementigen Teilmengen von X mit t Farben gibt es eine n-elementige Teilmenge Y von X, sodass alle p-elementigen Teilmengen von Y, die das gleiche minimale Element haben, die gleiche Farbe haben.*

Beweis: (2) ⇒ (1): Wir fixieren $n \in \mathbb{N}$. Wegen (2) gibt es ein M, sodass es für jede Färbung der p-elementigen Teilmengen von $\{1, 2, \ldots, M\}$ mit t Farben eine $(t(n-1)+1)$-elementige Teilmenge Y von $\{1, 2, \ldots, M\}$ gibt, sodass alle p-elementigen Teilmengen von Y, die das gleiche minimale Element haben, die gleiche Farbe haben. Wir behaupten, dass $N := M$ in (1) das Gewünschte leistet. Wir fixieren eine Färbung der p-elementigen Teilmengen von $\{1, 2, \ldots, M\}$ mit t Farben, und wählen eine $(t(n-1)+1)$-elementige Teilmenge Y wie oben. Für jede Farbe f der t Farben definieren wir die Menge $M_f := \{x \in Y \mid$ jede p-elementige Teilmenge von Y mit x als minimalem Element hat die Farbe $f\}$. Eine der Mengen M_f hat zumindest n Elemente. Alle p-elementigen Teilmengen von M_f haben dann die gleiche Farbe. ■

Beweis des Satzes von Ramsey (Satz 6.15): Wir definieren ein Prädikat

$$R(N, p, t, n)$$

dadurch, dass $R(N, p, t, n)$ gilt, wenn es für alle N-elementigen Mengen X und für alle Färbungen $c : \binom{X}{p} \to \{1, \ldots, t\}$ eine n-elementige Teilmenge Y von X gibt, sodass c auf $\binom{Y}{p}$ konstant ist.

Wir definieren ein Prädikat

$$S(M, p, t, n)$$

dadurch, dass $S(M, p, t, n)$ gilt, wenn es für alle M-elementigen Teilmengen X von $\mathbb{N}$ und für alle Färbungen $c : \binom{X}{p} \to \{1, \ldots, t\}$ einen n-elementige Menge $Y \subseteq X$ gibt, sodass für alle $A, B \in Y$ mit $\min(A) = \min(B)$ gilt, dass $c(A) = c(B)$.

Wir wählen nun $t \in \mathbb{N}$, und zeigen durch Induktion nach p, dass $\forall p \in \mathbb{N}\,(\forall n \in \mathbb{N}\,\exists N \in \mathbb{N} : R(N, p, t, n))$ gilt.

- $p = 1$: Wir fixieren $n \in \mathbb{N}$. Dann leistet $N := t(n-1)+1$ das Gewünschte.
- Sei nun $p \geq 2$. Wir zeigen als erstes, dass die Eigenschaft (2) aus Lemma 6.19 gilt. Diese Eigenschaft lässt sich als $\forall n \in \mathbb{N}\exists M \in \mathbb{N} : S(M, p, t, n)$ abkürzen. Wir zeigen diese Eigenschaft durch Induktion nach n.
  - Für $n \leq p$ leistet $M := p$ das Gewünschte.
  - Wir fixieren $n > p$. Mit der Induktionsvoraussetzung der Induktion nach n produzieren wir ein M für $n-1$. M ist also so, dass $S(M, p, t, n-1)$ gilt. Es gibt dann also für alle $X \subseteq \mathbb{N}$ mit $|X| = M$ und für alle $c : \binom{X}{p} \to \{1, \ldots, t\}$ eine $(n-1)$-elementige Teilmenge Y von X, sodass für alle $P, Q \in \binom{Y}{p}$ mit $\min(P) = \min(Q)$ gilt, dass $c(P) = c(Q)$.
    Wegen der Induktionsvoraussetzung der Induktion nach p gibt es eine Zahl $N \in \mathbb{N}$, sodass $R(N, p-1, t, M)$ gilt. N ist dann so, dass es für jede Menge X_1 mit $|X_1| = N$ und für jede Funktion $c : \binom{X_1}{p-1} \to \{1, \ldots, t\}$ ein $Y_1 \subseteq X_1$ mit $|Y_1| = M$ gibt, sodass c auf $\binom{Y_1}{p}$ konstant ist.
    Wir behaupten nun, dass für

$$M' := 1 + N$$

die Eigenschaft $S(M', p, t, n)$ erfüllt ist. Wir fixieren dazu eine M'-elementige Teilmenge $X = \{x_1, \ldots, x_{M'}\}$ von $\mathbb{N}$ (mit $x_1 < x_2 < \cdots < x_{M'}$) und eine Färbung c der p-elementigen Teilmengen von X mit t Farben. Wir geben nun jeder $(p-1)$-elementigen Teilmenge Z von $X \setminus \{x_1\}$ die Farbe von $\{x_1\} \cup Z$; wir definieren also $c' : \binom{X \setminus \{x_1\}}{p-1} \to \{1, \ldots, t\}$ durch $c'(Z) := c(Z \cup \{x_1\})$. Wir finden dann wegen $R(N, p-1, t, M)$ eine M-elementige Teilmenge A von $X \setminus \{x_1\}$, sodass alle $(p-1)$-elementigen Teilmengen von A unter der Färbung c' die gleiche Farbe haben.

Wegen $S(M, p, t, n-1)$ gibt es eine $(n-1)$-elementige Teilmenge B von A, sodass alle p-elementigen Teilmengen von B mit dem gleichen minimalen Element unter der Färbung c die gleiche Farbe haben.

Wir behaupten, dass $B \cup \{x_1\}$ eine n-elementige Teilmenge von X ist, sodass für alle p-elementigen Teilmengen P_1, P_2 von B mit $\min(P_1) = \min(P_2)$ gilt, dass $c(P_1) = c(P_2)$. Wir wählen dazu zwei p-elementige Teilmengen P_1, P_2 von $B \cup \{x_1\}$ mit dem gleichen minimalen Element. Ist dieses Element x_1, so haben wegen $c(P_1) = c'(P_1 \setminus \{x_1\}) = c'(P_2 \setminus \{x_1\}) = c(P_2)$ die Mengen P_1, P_2 die gleiche Farbe unter c, da $P_1 \setminus \{x_1\}$ und $P_2 \setminus \{x_1\}$ $(p-1)$-elementige Teilmengen von A sind. Ist dieses Element nicht x_1, dann sind P_1, P_2 beide p-elementige Teilmengen von B mit dem gleichen minimalen Element und haben daher die gleiche Farbe.

Somit gilt $S(M', p, t, n)$. Das beendet den Induktionsschritt nach n.

Wir haben jetzt also $\forall n \in \mathbb{N}\, \exists M \in \mathbb{N} : S(M, p, t, n)$, gezeigt; es gilt also gilt die Eigenschaft (2) von Lemma 6.19, und folglich auch (1) von Lemma 6.19. Wir zeigen nun $\forall n \in \mathbb{N}\, \exists N \in \mathbb{N} : R(N, p, t, n)$. Sei dazu $n \in \mathbb{N}$. Wir wählen als N die aus Eigenschaft (1) von Lemma 6.19 gewonnene Zahl. Sei $X = \{x_1, \ldots, x_N\}$ eine N-elementige Menge, und sei $c : \binom{X}{p} \to \{1, \ldots, t\}$. Für eine p-elementige Teilmenge von $\{1, \ldots, N\}$ sei $c'(A) := c(\{x_i \mid i \in A\})$. Wegen Lemma 6.19 (1) hat $\{1 \ldots, N\}$ dann eine n-elementige Teilmenge B, sodass $c'|_{\binom{B}{p}}$ konstant ist. Sei $Y := \{x_i \mid i \in B\}$. Dann ist c auf $\binom{Y}{p}$ konstant. Das beendet den Induktionsschritt der Induktion nach p. ■

ÜBUNGSAUFGABEN 6.20.

(1) (Induktionsbeweis im Satz von Ramsey) Seien $R, M : \mathbb{N}_0 \times \mathbb{N}_0 \to \mathbb{N}_0 \cup \{\infty\}$. Die Funktionen R, M erfüllen:
   (a) $R(0, n) \in \mathbb{N}_0$ für alle $n \in \mathbb{N}_0$.
   (b) $M(0, n) \in \mathbb{N}_0$ für alle $n \in \mathbb{N}_0$.
   (c) $R(n, 0) \in \mathbb{N}_0$ für alle $n \in \mathbb{N}_0$.
   (d) $M(n, 0) \in \mathbb{N}_0$ für alle $n \in \mathbb{N}_0$.
   (e) $R(p, n) \leq M(p, 2n)$ für alle $p, n \in \mathbb{N}_0$.
   (f) Für alle $p, n \in \mathbb{N}_0 \setminus \{0\}$ mit $M(p, n-1) \in \mathbb{N}_0$ gilt:

$$M(p, n) \leq 1 + R(p-1, M(p, n-1)).$$

Zeigen Sie, dass für alle $a, b \in \mathbb{N}_0$ gilt: $R(a, b) \in \mathbb{N}_0$. Zeigen Sie also, dass R nie den Funktionswert ∞ annimmt.

SATZ 6.21 (Erdős-Szekeres). *Sei $n \in \mathbb{N}$, $n \geq 3$. Dann gibt es eine Zahl N, sodass jede Menge von N Punkten in der Ebene, von denen keine drei auf einer Geraden liegen, n Punkte enthält, die die Eckpunkte eines konvexen n-Ecks sind.*

Beweis: Der Fall $n = 3$ ist offensichtlich. Sei nun $n = 4$. Wir setzen $N := 5$, und wählen 5 Punkte in der Ebene. Wenn die konvexe Hülle der 5 Punkte ein Viereck oder Fünfeck ist, so gibt es ein konvexes Viereck. Nehmen wir nun an, dass die konvexe Hülle ein Dreieck A, B, C ist. Dann liegt der vierte Punkt D im Inneren des Dreiecks. Die drei Geraden durch D und A, durch D und B, und durch D und C teilen das Dreieck ABC in 6 Flächen. Je nachdem, in welcher dieser Flächen der fünfte Punkt E liegt, erhalten wir ein konvexes Viereck.

Sei nun $n > 4$. Wir wählen $N := r(4, 2, n)$. Sei X eine Menge von N Punkten. Wir färben nun jede Teilmenge von 4 Punkten mit d, wenn die konvexe Hülle ein Dreieck ist, und mit v, wenn die konvexe Hülle ein Viereck ist. Nach dem Satz von Ramsey gibt es eine n-elementige Teilmenge Y von X, sodass alle 4-elementigen Teilmengen die gleiche Farbe haben.

Wenn diese Farbe d ist, so haben wir $n \geq 5$ Punkte gefunden, unter denen keine 4 ein konvexes Viereck bilden, im Widerspruch zum bereits gezeigten Fall $n = 4$.

Also ist diese Farbe v. Wir zeigen nun, dass die konvexe Hülle von Y ein konvexes n-Eck ist. Sei $Y' \subseteq Y$ eine minimale Teilmenge, deren konvexe Hülle gleich der konvexen Hülle von Y ist. Y' ist nun die Menge der Eckpunkte eines konvexen $|Y'|$-Ecks. Wenn $Y' = Y$, so haben wir ein konvexes n-Eck gefunden. Wenn $D \in Y$ und $D \notin Y'$, so liegt D im Inneren der konvexen Hülle von Y'. Es gibt dann $A, B, C \in Y'$, sodass D im Inneren des Dreiecks ABC liegt. Dann ist die Farbe von $\{A, B, C, D\}$ gleich d, im Widerspruch dazu, dass alle Teilmengen von Y die Farbe v haben. ■

SATZ 6.22. *Sei $t \in \mathbb{N}$. Dann gibt es ein N, sodass es für jede Gruppe G mit $|G| > N$ und jede Aufteilung von $G \setminus \{1\}$ in t Klassen eine Klasse gibt, die drei verschiedene Elemente x, y, z mit $z = x \cdot y$ enthält.*

Beweis: Sei $N := r(2, t, 4)$, $s := |G| - 1$, und sei $G = \{1, x_1, \ldots, x_s\}$. Wir färben die Teilmenge $\{i, j\}$ von $\{1, \ldots, s\}$ mit der Nummer der Klasse von $x_{\min(i,j)}^{-1} x_{\max(i,j)}$. Seien $a < b < c < d \in \{1, \ldots, s\}$ so, dass alle zweielementigen Teilmengen von $\{a, b, c, d\}$ die gleiche Farbe haben. Da $x_b^{-1} x_c \neq x_b^{-1} x_d$, ist zumindest eines dieser beiden Elemente ungleich $x_a^{-1} x_b$. Ohne Beschränkung der Allgemeinheit sei $x_a^{-1} x_b \neq x_b^{-1} x_d$. Es gilt $(x_a^{-1} x_b) \cdot (x_b^{-1} x_d) = (x_a^{-1} x_d)$. Diese drei Elemente sind paarweise verschieden. ■

ÜBUNGSAUFGABEN 6.23.

(1) Sei $t \in \mathbb{N}$. Zeigen Sie, dass es eine Zahl N gibt, sodass für jede Aufteilung der Menge $\{1, 2, \ldots, N\}$ in t Klassen es eine Klasse gibt, die zwei verschiedene Zahlen und deren Summe enthält.
(2) Zeigen Sie den “unendlichen” Satz von Ramsey:

Sei M eine unendliche Menge. Wir färben jede p-elementige Teilmenge von M mit einer von endlich vielen Farben. Dann gibt es eine unendliche Teilmenge T von M, sodass alle p-elementigen Teilmengen von T die gleiche Farbe haben.

Hinweis: Nehmen Sie an, M sei abzählbar unendlich. Gehen Sie mit Induktion nach p vor. Konstruieren Sie eine Folge $(a_1, a_2, \ldots)$ von Elementen in M, sodass alle Teilmengen von $\{a_i \mid i \in \mathbb{N}\}$, die das gleiche "minimale Element" besitzen, die gleiche Farbe haben. (Der Beweis steht auch im Artikel "Ramsey's Theorem" in `http://en.wikipedia.org/wiki`.)

(3) Verwenden Sie Übung (2), um zu zeigen, dass jede reelle Zahlenfolge eine monoton fallende oder eine streng monoton steigende Teilfolge enthält.

(4) (Dicksons Lemma) Für zwei Vektoren $v, w \in \mathbb{N}_0^k$ schreiben wir $v \leq' w$ falls für alle $i \in \{1, \ldots, k\} : v_i \leq w_i$. Sei $(v_1, v_2, \ldots)$ eine Folge von Vektoren in $\mathbb{N}_0^k$. Dann gibt es eine (unendliche) Teilfolge, die bezüglich $\leq'$ schwach monoton aufsteigend ist. *Hinweis:* Verwenden Sie den unendlichen Ramseysatz für eine bestimmte Färbung von Paaren von Vektoren mit 2^k Farben.

KAPITEL 7

Körper aus Polynomringen

DEFINITION 7.1. Eine algebraische Struktur $\boldsymbol{R}$ ist ein *Körper*, wenn $\boldsymbol{R}$ ein kommutativer Ring mit Eins ist, R zumindest zwei Elemente hat, und alle Elemente $x \in R \setminus \{0\}$ invertierbar sind.

SATZ 7.2. *Sei $\boldsymbol{R}$ ein Hauptidealbereich, und sei f ein irreduzibles Element von $\boldsymbol{R}$. Dann ist $\boldsymbol{R}/(f)$ ein Körper.*

Beweis: Sei $x \in R$ so, dass $x+(f) \neq 0+(f)$. Wir zeigen, dass $x+(f)$ invertierbar in $R/(f)$ ist. Sei dazu I das von $\{x, f\}$ erzeugte Ideal, und sei $z \in R$ so, dass $(z) = I$. Dann gilt $z \mid f$, also ist z entweder assoziiert zu f oder invertierbar. Wenn z assoziiert zu f ist, so gilt wegen $z \mid x$ auch $f \mid x$. Dann gilt aber $x \in (f)$, und somit $x + (f) = 0 + (f)$. Folglich ist z invertierbar. Dann gilt $1 \in I$, und es gibt somit $u, v \in R$, sodass $ux + vf = 1$. Dann gilt $(u + (f))(x + (f)) + (v + (f))(f + (f)) = 1 + (f)$, also $(u + (f))(x + (f)) = 1 + (f)$. Folglich ist $x + (f)$ invertierbar. ■

KOROLLAR 7.3. *Sei p eine Primzahl. Dann ist $\mathbb{Z}_p$ ein Körper.*

KOROLLAR 7.4. *Sei K ein Körper und sei f ein irreduzibles Element aus dem Polynomring $K[t]$. Dann ist $K[t]/(f)$ ein Körper.*

Wir definieren den Grad des Nullpolynoms als -1.

LEMMA 7.5. *Sei K ein Körper, und sei $f \in K[t]$. Das Polynom f ist ein invertierbares Element von $K[t]$, wenn* $\deg(f) = 0$. *Das Polynom f ist ein irreduzibles Element von $K[t]$, wenn* $\deg(f) \geq 1$ *und für alle $g, h \in K[t]$ mit $f = g \cdot h$ gilt* $\deg(g) = 0$ *oder* $\deg(h) = 0$.

Für einen Körper K nennen wir ein irreduzibles Element von $K[t]$ auch ein *über K irreduzibles Polynom*.

1. Irreduzible Polynome über $\mathbb{Q}$

DEFINITION 7.6. Sei R ein kommutativer Ring mit Eins, sei $n \in \mathbb{N}_0$, und sei $f = \sum_{i=0}^{n} f_i t^i \in R[t]$. Das Polynom f ist *primitiv*, wenn es kein primes $p \in R$ gibt, das alle Koeffizienten f_i $(i = 0, \ldots, n)$ teilt.

LEMMA 7.7 (Gaußsches Lemma). *Sei R ein kommutativer Ring mit Eins, und seien $f, g \in R[t]$ 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. Da f und g primitiv sind, teilt p weder alle Koeffizienten von f noch alle Koeffizienten von g. Sei k maximal, sodass $p \nmid f_k$, und sei l maximal, sodass $p \nmid g_l$. Wir berechnen den Koeffizienten von t^{k+l} von $f \cdot g$ und erhalten $(f \cdot g)_{k+l} = \sum_{i=0}^{k+l} f_{(k+l)-i} g_i$. Für $i < l$ gilt $p \mid f_{(k+l)-i}$, und für $i > l$ gilt $p \mid g_i$. Da $p \mid (f \cdot g)_{k+l}$, gilt also $p \mid f_k g_l$. Da p prim ist, teilt es daher einen der beiden Faktoren, im Widerspruch zur Wahl von k und l. ■

DEFINITION 7.8. Sei $a = \sum_{i=1}^{n} a_i t^i \in \mathbb{Z}[t]$, $a \neq 0$. Wir definieren den *Inhalt von a* durch $\mathrm{cont}(a) := \mathrm{ggT}(a_0, a_1, \ldots, a_n)$.

SATZ 7.9. *Sei $f \in \mathbb{Z}[t] \setminus \{0\}$, seien $g, h \in \mathbb{Q}[t]$ so, dass $f = g \cdot h$, und seien $\alpha, \beta \in \mathbb{Z} \setminus \{0\}$ so, dass $\alpha g \in \mathbb{Z}[t]$ und $\beta h \in \mathbb{Z}[t]$. Wir setzen:*

$$\begin{aligned} \gamma &:= \tfrac{1}{\alpha\beta} \cdot \mathrm{cont}(\alpha g) \cdot \mathrm{cont}(\beta h), \\ g' &:= \tfrac{1}{\mathrm{cont}(\alpha g)} \alpha g, \\ h' &:= \tfrac{1}{\mathrm{cont}(\beta h)} \beta h. \end{aligned}$$

Dann gilt $f = \gamma (g' \cdot h')$ und $\gamma \in \mathbb{Z}$, $g' \in \mathbb{Z}[t]$, $h' \in \mathbb{Z}[t]$.

Beweis: Die Gleichung $f = \gamma (g' \cdot h')$ erhält man unmittelbar durch Nachrechnen. Wir zeigen nun, dass $\gamma \in \mathbb{Z}$. Seien $\delta, \varepsilon \in \mathbb{Z} \setminus \{0\}$ so, dass $\gamma = \frac{\delta}{\varepsilon}$ und $\mathrm{ggT}(\delta, \varepsilon) = 1$. Dann gilt $\varepsilon f = \delta (g' \cdot h')$. Da $f \in \mathbb{Z}[t]$, teilt ε alle Koeffizienten von $\delta (g' \cdot h')$. Wegen $\mathrm{ggT}(\delta, \varepsilon) = 1$ teilt ε alle Koeffizienten von $g' \cdot h'$. Nun sind g' und h' primitiv. Wegen des Gaußschen Lemmas (Lemma 7.7) ist $g' \cdot h'$ ebenfalls primitiv, also gilt $\varepsilon \in \{1, -1\}$. Folglich gilt $\gamma \in \mathbb{Z}$. ■

SATZ 7.10 (Eisenstein-Kriterium). *Seien $n \in \mathbb{N}$, p Primzahl, $a = \sum_{i=0}^{n} a_i t^i \in \mathbb{Z}[t]$ so, dass*

(1) $p \mid a_0, \ldots, p \mid a_{n-1}$,
(2) $p \nmid a_n$,
(3) $p^2 \nmid a_0$.

Dann ist a ein irreduzibles Element von $\mathbb{Q}[t]$ (also ein über $\mathbb{Q}$ irreduzibles Polynom).

Beweis: Wenn a nicht irreduzibel ist, gibt es $b, c \in \mathbb{Q}[t]$ vom Grad ≥ 1, sodass $a = b c$. Wegen Satz 7.9 gibt es dann auch $r, s \in \mathbb{Z}[t]$ sodass $a = r s$ und $\deg(r) \geq 1$, $\deg(s) \geq 1$. Sei $k := \deg(r)$, $l := \deg(s)$. Dann gilt $k + l = n$. Wegen $p \nmid a_n$ gilt $p \nmid r_k$ und $p \nmid s_l$. Wir zeigen nun, dass für alle $k_1 \in \mathbb{N}_0$ mit $k_1 < k$ und für alle $l_1 \in \mathbb{N}_0$ mit $l_1 < l$ gilt, dass $p \mid r_{k_1}$ und $p \mid s_{l_1}$. Sei dazu k_2 minimal mit $p \nmid r_{k_2}$, und sei l_2 minimal mit $p \nmid s_{l_2}$. Dann ist der Koeffizient von $t^{k_2 + l_2}$ des Polynoms a nicht durch p teilbar. Somit gilt $k_2 + l_2 = n$, und somit $k_2 = k$, $l_2 = l$. Also gibt es Polynome $u, v \in \mathbb{Z}[t]$, sodass $r = r_k t^k + p u$ und

$s = s_l t^l + pv$. Somit gilt $a_0 = (r \cdot s)_0 = \overline{r}(0) \cdot \overline{s}(0) = p \cdot \overline{u}(0) \cdot p \cdot \overline{v}(0)$. Folglich ist a_0 ein Vielfaches von p^2, im Widerspruch zur Annahme. ■

ÜBUNGSAUFGABEN 7.11.

(1) Seien $f, g \in \mathbb{Z}[t] \setminus \{0\}$. Zeigen Sie, dass $\operatorname{cont}(f \cdot g) = \operatorname{cont}(f) \cdot \operatorname{cont}(g)$.
(2) Sei $a \in \mathbb{Z}[t]$, $n := \deg a$, und sei r eine rationale Nullstelle von $a = a_0 t^0 + \cdots + a_n t^n$. Zeigen Sie, dass es $p, q \in \mathbb{Z}$ gibt, sodass $r = \frac{p}{q}$ und $p \mid a_0$, $q \mid a_n$.

2. Quotientenkörper

Wir verallgemeinern jetzt die Konstruktion von $\mathbb{Q}$ aus $\mathbb{Z}$.

Sei dazu $\boldsymbol{D}$ 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 $Q(\boldsymbol{D})$ bezeichnen wir die Faktormenge $\{(a, b) \in D^2 \mid b \neq 0\}/\!\sim$. Auf $Q(\boldsymbol{D})$ definieren wir + durch $\frac{a}{b} + \frac{c}{d} := \frac{ad+bc}{bd}$, − durch $-\frac{a}{b} := \frac{-a}{b}$, und · durch $\frac{a}{b} \cdot \frac{c}{d} := \frac{ac}{bd}$.

SATZ UND DEFINITION 7.12. *Sei $\boldsymbol{D}$ ein Integritätsbereich. Dann ist $(Q(D), +, -, \cdot, \frac{0}{1}, \frac{1}{1})$ ein Körper. Er heißt der* Quotientenkörper *von $\boldsymbol{D}$.*

SATZ 7.13. *Sei $\boldsymbol{D}$ ein Integritätsbereich, sei $\boldsymbol{K}$ ein Körper, und sei φ ein Ring-mit-Eins-Monomorphismus von $\boldsymbol{D}$ nach $\boldsymbol{K}$. Dann ist $\psi : \boldsymbol{Q}(\boldsymbol{D}) \to \boldsymbol{K}$, $\psi(\frac{a}{b}) := \varphi(a) \cdot (\varphi(b))^{-1}$ wohldefiniert und ein Ring-mit-Eins-Monomorphismus vom Quotientenkörper von $\boldsymbol{D}$ nach $\boldsymbol{K}$.*

Sei $\boldsymbol{K}$ ein Körper. Den Quotientenkörper des Polynomrings $\boldsymbol{K}[t_1, \ldots, t_n]$ bezeichnet man als den Körper der *rationalen Funktionen vom Transzendenzgrad n über $\boldsymbol{K}$*, und kürzt ihn mit $\boldsymbol{K}(t_1, \ldots, t_n)$ ab.

KAPITEL 8

Endliche Körper

1. Definition und einfache Eigenschaften endlicher Körper

DEFINITION 8.1. Ein kommutativer Ring mit Eins $\boldsymbol{R} = (R, +, -, \cdot, 0, 1)$ ist ein *Körper* wenn

(1) $|R| \geq 2$,
(2) Für alle $x \in R \setminus \{0\}$ gibt es ein $y \in R$ mit $x \cdot y = 1$.

ÜBUNGSAUFGABEN 8.2.

(1) Zeigen Sie, dass es in einem Körper für jedes x höchstens ein y mit $x \cdot y = 1$ geben kann.
(2) Zeigen Sie, dass das Produkt zweier Elemente in einem Körper nur dann 0 ist, wenn einer der Faktoren gleich 0 ist.

In einem Körper hat jedes Element $a \neq 0$ genau ein multiplikativ inverses Element; wir bezeichnen es mit a^{-1}. Für jede Primzahl p ist der Ring $\mathbb{Z}_p$ ein Körper.

DEFINITION 8.3. Sei $\boldsymbol{E} = (E, +, -, \cdot, 0, 1)$ ein Körper, und sei $K \subseteq E$. Die Menge K ist dann *Trägermenge eines Unterkörpers* von $\boldsymbol{E}$, wenn

(1) $0 \in K$, $1 \in K$,
(2) für alle $x, y \in K$ gilt $x + y \in K$, $x - y \in K$, $x \cdot y \in K$,
(3) für alle $x \in K$ gilt $x^{-1} \in K$.

Wenn K Trägermenge eines Unterkörpers von $\boldsymbol{E}$ ist, so ist $\boldsymbol{K} = (K, +|_{K\times K}, -|_K, \cdot|_{K\times K}, 0, 1)$ selbst ein Körper. Wir bezeichnen $\boldsymbol{K}$ dann als *Unterkörper* von $\boldsymbol{E}$, und $\boldsymbol{E}$ als *Erweiterung* von $\boldsymbol{K}$.

ÜBUNGSAUFGABEN 8.4.

(1) Zeigen Sie: Der Durchschnitt beliebig vieler Trägermengen von Unterkörpern eines Körpers ist wieder Trägermenge eines Unterkörpers.
(2) Sei $\boldsymbol{E}$ ein endlicher Körper, und sei $K \subseteq E$ mit $|K| \geq 2$ so, dass für alle $x, y \in K$ auch $x + y$ und $x \cdot y$ in K liegen. Zeigen Sie, dass K Trägermenge eines Unterkörpers von $\boldsymbol{E}$ ist.

Der Durchschnitt aller Unterkörper eines Körpers $\boldsymbol{E}$ ist wieder ein Körper, er heißt *Primkörper* von $\boldsymbol{E}$.

SATZ 8.5. *Sei $\boldsymbol{E}$ ein endlicher Körper. Dann gibt es eine Primzahl p, sodass der Primkörper von $\boldsymbol{E}$ isomorph zu $\mathbb{Z}_p$ ist.*

Beweis: Offensichtlich sind alle $a*1$ mit $a \in \mathbb{Z}$ in jedem Unterkörper von $\boldsymbol{E}$ enthalten. Da $\boldsymbol{E}$ endlich ist, gibt es $a, b \in \mathbb{N}$ mit $a > b$ und $a * 1 = b * 1$, also $(a - b) * 1 = 0$. Wir zeigen nun, dass

$$\min\{n \in \mathbb{N} \mid n * 1 = 0\}$$

eine Primzahl ist. Sei p dieses Minimum. Wenn es $c, d < p$ gibt, sodass $cd = p$, dann gilt $(c * 1) \cdot (d * 1) = 0$, also entweder $c * 1 = 0$ oder $d * 1 = 0$. Das widerspricht der Minimalität von p. Die Abbildung

$$\begin{array}{rccc} \Phi & : & \mathbb{Z} & \longrightarrow & E \\ & & z & \longmapsto & z * 1 \end{array}$$

ist ein Ring mit Eins-Homomorphismus. Sie hat den Primkörper von $\boldsymbol{E}$ als Bild, ihr Kern ist $p\mathbb{Z}$. Der Primkörper von $\boldsymbol{E}$ ist also isomorph zu $\mathbb{Z}/p\mathbb{Z} = \mathbb{Z}_p$. ■

Sei $\boldsymbol{E}$ ein Körper. Das kleinste $p \in \mathbb{N}$ sodass $p * 1 = 0$ heißt *Charakteristik* von $\boldsymbol{E}$. Wenn es kein solches $p \in \mathbb{N}$ gibt, dann definieren wir die Charakteristik von $\boldsymbol{E}$ als 0.

ÜBUNGSAUFGABEN 8.6.

(1) Bestimmen Sie den Primkörper des Körpers der komplexen Zahlen.
(2) Zeigen Sie, dass der Primkörper eines beliebigen Körpers entweder isomorph zu $\mathbb{Z}_p$ für irgendeine Primzahl p, oder isomorph zu $\mathbb{Q}$ ist.

SATZ 8.7. *Die Anzahl der Elemente eines endlichen Körpers ist eine Primzahlpotenz.*

Wir beweisen folgende stärkere Aussage:

SATZ 8.8. *Sei $\boldsymbol{K}$ ein Unterkörper des endlichen Körpers $\boldsymbol{E}$. Dann gibt es ein $n \in \mathbb{N}$, sodass $|E| = |K|^n$.*

Beweis: Durch die skalare Multiplikation $* : K \times E \to E$, $k * e := k \cdot e$ wird $(E, +, -, 0; *)$ zu einem Vektorraum über K. Wegen der Endlichkeit von K hat K eine endliche Basis $B = (b_1, \ldots, b_n)$. Die Abbildung, die jedem $e \in E$ sein Koordinatentupel $(e)_B$ zuordnet, ist eine Bijektion von E nach K^n. ■

Satz 8.8 folgt nun, wenn man als $\boldsymbol{K}$ den Primkörper von $\boldsymbol{E}$ wählt.

SATZ 8.9. *Sei $\boldsymbol{E}$ ein Körper der Charakteristik p mit $q = p^m$ Elementen. Dann gilt für alle $x, y \in E$:*

(1) $(x + y)^p = x^p + y^p$.
(2) $x^q = x$.

Beweis: (1): Nach dem binomischen Lehrsatz gilt

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

Da $\binom{p}{i}$ für alle $i \in \{1, 2, \ldots, p - 1\}$ Vielfache von p sind, gilt $(x + y)^p = x^p + y^p$.

(2): Wir verwenden den Satz von Fermat für die Gruppe $(E^*, \cdot)$ und erhalten, dass alle $x \neq 0$ die Gleichung $x^{q-1} = 1$ erfüllen. ■

ÜBUNGSAUFGABEN 8.10.

(1) Sei $\boldsymbol{K}$ ein Körper der Charakteristik p, sei $m \in \mathbb{N}$, und seien $x, y \in K$. Zeigen Sie: $(x+y)^{p^m} = x^{p^m} + y^{p^m}$.
(2) Sei $\boldsymbol{K}$ ein Körper, und sei $f \in \boldsymbol{K}[x]$. Seien $\alpha_1, \alpha_2, \ldots, \alpha_k \in K$ paarweise verschiedene Nullstellen von f. Zeigen Sie, dass $\prod(x - \alpha_i)$ ein Teiler von f in $\boldsymbol{K}[x]$ ist.
(3) Zeigen Sie, dass ein Polynom in $\boldsymbol{K}[x]$ vom Grad $\leq n$, das $n+1$ verschiedene Nullstellen hat, automatisch das Nullpolynom sein muss.
(4) Sei $\boldsymbol{K}$ ein Körper der Charakteristik p und sei $\xi \in K$.
   (a) Zeigen Sie mithilfe des Satzes, dass für alle $z \in \mathbb{Z}$ die Kongruenz $z^p \equiv z \pmod{p}$ gilt, dass das Polynom
   $$f(x) := (x+\xi)^p - x^p - \xi^p$$
   zumindest p Nullstellen hat (probieren Sie $n * \xi$ mit $n \in \mathbb{Z}$).
   (b) Bestimmen Sie den Grad dieses Polynoms.
   (c) Schließen Sie daraus, dass $p \mid \binom{p}{i}$ für alle $i \in \{1, 2, \ldots, p-1\}$, und dass für alle $\alpha, \beta \in K$ gilt: $(\alpha+\beta)^p = \alpha^p + \beta^p$.

SATZ 8.11. *Die multiplikative Gruppe eines endlichen Körpers ist zyklisch.*

Wir zeigen diesen Satz mithilfe des folgenden Satzes.

SATZ 8.12. *Sei $\boldsymbol{A} = (A, \cdot)$ eine abelsche Gruppe mit neutralem Element* 1. *Wenn es für jedes $n \in \mathbb{N}$ höchstens n Elemente in A mit $x^n = 1$ gibt, dann ist $\boldsymbol{A}$ zyklisch.*

Beweis: Sei $h := |A|$. Falls $h = 1$, ist $\boldsymbol{A}$ klarerweise zyklisch. Wir nehmen also nun $h \geq 2$ an. Wir bilden die Primfaktorzerlegung von h und finden also $N \in \mathbb{N}$, Primzahlen $p_1, p_2, \ldots, p_N$ und $r_1, r_2, \ldots, r_N \in \mathbb{N}$ sodass

$$h = \prod_{m=1}^{N} {p_m}^{r_m}.$$

Wir werden nun für jedes $i \in \{1, 2, \ldots, N\}$ ein Element a_i und ein Element $b_i \in A$ wählen: Da $\frac{h}{p_i} < h$, gibt es ein Element $a_i \in A$, sodass ${a_i}^{\frac{h}{p_i}} \neq 1$. Wir setzen

$$b_i := {a_i}^{\frac{h}{{p_i}^{r_i}}}.$$

Es gilt dann (Satz von Fermat)

$${b_i}^{{p_i}^{r_i}} = 1. \tag{8.1}$$

Sei nun k die Ordnung von b_i, also das kleinste $n \in \mathbb{N}$, sodass $(b_i)^n = 1$. Da $k \mid {p_i}^{r_i}$ gibt es ein $s_i \in \{0, 1, \ldots, r_i\}$, sodass $k = {p_i}^{s_i}$. Wir zeigen nun

$$s_i = r_i. \tag{8.2}$$

Nehmen wir an $s_i \leq r_i - 1$. Dann gilt

$${b_i}^{{p_i}^{r_i - 1}} = 1,$$

also

$${a_i}^{\frac{h}{p_i}} = 1.$$

Das widerspricht der Wahl von a_i; dieser Widerspruch beweist (8.2). Die Ordnung von b_i ist also $p_i^{r_i}$. Wir bilden nun

$$c = \prod_{i=1}^{N} b_i.$$

Klarerweise gilt $c^h = 1$. Wir zeigen nun, dass c wirklich Ordnung h hat. Wenn c kleinere Ordnung hätte, dann gibt es ein $j \in \{1, \ldots, N\}$, sodass $c^{\frac{h}{p_j}} = 1$. Daher gilt

$$\prod_{i=1}^{N} b_i^{\frac{h}{p_j}} = 1. \tag{8.3}$$

Falls $i \neq j$, so gilt $p_i^{r_i} \mid \frac{h}{p_j}$. Wegen (8.1) sind also Faktoren in (8.3) mit $i \neq j$ gleich 1. Wir erhalten also

$$b_j^{\frac{h}{p_j}} = 1.$$

Da b_j wegen (8.2) die Ordnung $p_j^{r_j}$ hat, gilt $p_j^{r_j} \mid \frac{h}{p_j}$. Daher gilt $p_j^{r_j+1} \mid h$, was im Widerspruch zur Primfaktorzerlegung von h steht. Das Element c hat also wirklich Ordnung h, und ist somit ein erzeugendes Element für die Gruppe $\boldsymbol{A}$. ■

Aus dem Satz 8.12 folgt nun direkt der Satz 8.11, da in jedem Körper und für jedes n das Polynom $x^n - 1$ höchstens n Nullstellen hat.

ÜBUNGSAUFGABEN 8.13.

(1) Sei $(A, \cdot)$ eine Gruppe, und sei $a \in A$ und $n \in \mathbb{N}$ so, dass $a^n = 1$. Zeigen Sie, dass n ein Vielfaches der Ordnung von a ist.

2. Körper aus irreduziblen Polynomen

SATZ 8.14. *Sei $\boldsymbol{K}$ ein Körper, und sei $f \in \boldsymbol{K}[x]$ irreduzibel über $\boldsymbol{K}$. Dann ist $\boldsymbol{K}[x]/(f)$ ein Körper.*

Als Quotient eines kommutativen Ringes mit 1 ist $\boldsymbol{K}[x]/(f)$ wieder ein kommutativer Ring mit 1. Es reicht also zu zeigen, dass jedes $h \in \boldsymbol{K}[x]/(f)$ mit $h \neq 0 + (f)$ invertierbar ist. Sei $h' \in \boldsymbol{K}[x]$ so, dass $h = h' + (f)$. Da f irreduzibel ist, und h' kein Vielfaches von f ist, gilt $\mathrm{ggT}(h', f) = 1$. Es gibt also $u, v \in \boldsymbol{K}[x]$, sodass $u \cdot h' + v \cdot f = 1$. Es gilt also $(u + (f)) \cdot (h' + (f)) = u \cdot h' + (f) = (1 - v \cdot f) + (f) = 1 + (f)$. ■

Wenn $\boldsymbol{K}$ ein endlicher Körper mit q Elementen ist, und f ein über $\boldsymbol{K}$ irreduzibles Polynom vom Grad n, dann ist $\boldsymbol{K}[x]/(f)$ also ein Körper mit q^n Elementen. Wir brauchen also zunächst irreduzible Polynome.

SATZ 8.15. *Sei $\boldsymbol{K}$ ein endlicher Körper mit q Elementen, und sei f ein irreduzibles Polynom vom Grad n. Dann gilt $f \mid x^{q^n} - x$.*

Wir betrachten den Körper $\boldsymbol{K}[x]/(f)$. Dieser Körper hat q^n Elemente. Es gilt also wegen Satz 8.9 (2) $(x + (f))^{q^n} = x + (f)$. Das bedeutet $f \mid x^{q^n} - x$.■

SATZ 8.16. *Sei $\boldsymbol{K}$ ein Körper mit q Elementen. Dann gilt $\prod_{v \in K}(x - v) = x^q - x$.*

Beweis: Beide Polynome haben q Nullstellen: für das linke Polynom ist das offensichtlich; für das rechte eine Konsequenz aus dem Satz von Fermat bzw. aus Satz 8.9. Die Differenz dieser beiden Polynome hat also mindestens q Nullstellen, und einen Grad $\leq q - 1$. Die Differenz ist also das Nullpolynom. ■

LEMMA 8.17. *Sei $\boldsymbol{K}$ ein endlicher Körper mit q Elementen, sei $m \in \mathbb{N}$, und sei f ein über $\boldsymbol{K}$ irreduzibles Polynom vom Grad m. Sei $\boldsymbol{E}$ ein Erweiterungskörper von $\boldsymbol{K}$ mit q^m Elementen. Dann zerfällt f in $\boldsymbol{E}[x]$ in ein Produkt lauter linearer Polynome.*

Beweis: Da $\deg f = m$, gilt nach Satz 8.15, dass f das Polynom $x^{q^m} - x$ teilt. Nach Satz 8.16 gilt

$$\prod_{a \in E}(x - a) = x^{q^m} - x.$$

Das Polynom f ist auch ein Polynom in $\boldsymbol{E}[x]$. Jeder über $\boldsymbol{E}$ irreduzible Teiler von f in $\boldsymbol{E}[x]$ teilt also eines der Polynome in $\{x - b \mid b \in E\}$. Das bedeutet, dass f in $\boldsymbol{E}[x]$ vollständig in Linearfaktoren zerfällt. ■

Wir bezeichnen ein Polynom f als *normiert*, wenn sein führender Koeffizient (also der Koeffizient von $x^{\deg(f)}$) gleich 1 ist.

SATZ 8.18. *Sei p eine Primzahl, sei $m \in \mathbb{N}$, und sei $q = p^m$. Sei f ein normiertes, über $\mathbb{Z}_p$ irreduzibles Polynom in $\mathbb{Z}_p[x]$ vom Grad m. Dann ist jeder Körper mit q Elementen zu $\mathbb{Z}_p[x]/(f)$ isomorph.*

Beweis: Sei $\boldsymbol{E}$ ein Körper mit q Elementen. Wegen Lemma 8.17 wissen wir, f eine Nullstelle in $\boldsymbol{E}[x]$ hat. Sei $b \in E$ so, dass $\overline{f}(b) = 0$. Wir bilden nun die Abbildung

$$\begin{array}{rccc} \Phi & : & \mathbb{Z}_p[x] & \longrightarrow & E \\ & & g & \longmapsto & g(b). \end{array}$$

Die Abbildung Φ ist ein Ring mit Eins-Homomorphismus. Ihr Kern ist $\{g \in \mathbb{Z}_p[x] \mid g(b) = 0\}$. Sei h der normierte Erzeuger des Ideals $\ker \Phi$. Da $f \in \ker \Phi$, gilt $h \mid f$. Da f irreduzibel über $\mathbb{Z}_p$ ist, ist h entweder von Grad 0 oder gleich f. Im Fall, dass h vom Grad 0 ist, gilt wegen $h(b) = 0$, dass h das Nullpolynom ist, was $h \mid f$ widerspricht. Also ist $h = f$. Es gilt also nach dem Homomorphiesatz, dass $\mathbb{Z}_p[x]/(f)$ isomorph zu $\boldsymbol{E}$ ist. ■

3. Existenz irreduzibler Polynome

Wir geben im folgenden einen Beweis dafür, dass es für jedes n und für jeden endlichen Körper $\boldsymbol{K}$ ein irreduzibles Polynom vom Grad n über $\boldsymbol{K}$ gibt.

SATZ 8.19. *Sei $\boldsymbol{K}$ ein Körper, und sei f ein normiertes Polynom in $\boldsymbol{K}[x]$ vom Grad n. Dann gibt es einen Erweiterungskörper $\boldsymbol{E}$ von $\boldsymbol{K}$, sodass jeder in $\boldsymbol{E}[x]$ irreduzible Teiler von f Grad 1 hat.*

Wir beweisen folgende Aussage durch Induktion nach n:

> Für jeden Körper $\boldsymbol{K}$ und jedes Polynom $f \in \boldsymbol{K}[x]$ vom Grad n gibt es einen Erweiterungskörper $\boldsymbol{E}$ von $\boldsymbol{K}$, sodass jeder in $\boldsymbol{E}[x]$ irreduzible Teiler von f Grad 1 hat.

Für $n = 1$ ist die Aussage klar. Wir fixieren nun einen Körper $\boldsymbol{K}$ und ein Polynom $f \in \boldsymbol{K}[x]$ mit $\deg f = n > 1$. Wir zerlegen f in ein Produkt von normierten, über $\boldsymbol{K}$ irreduziblen Polynomen in $\boldsymbol{K}[x]$. Sei g einer der irreduziblen Faktoren. Wir bilden den Körper $\boldsymbol{L} := \boldsymbol{K}[x]/(g)$. Wir zeigen nun, dass $x + (g)$ eine Nullstelle von f ist. Dazu berechnen wir $\overline{f}(x+(g)) = \sum_{i=0}^{\deg f} f_i \cdot (x+(g))^i$. Wir wissen, wie man in Quotienten, also in $\boldsymbol{K}[x]/(g)$ rechnet, und erhalten $\sum_{i=0}^{\deg f} f_i \cdot (x+(g))^i = (\sum_{i=0}^{\deg f} f_i \cdot x^i) + (g)$. Wir wissen, das jedes Polynom $f = (f_0, f_1, f_2, \ldots, f_{\deg f}, 0, 0, \ldots)$ die Eigenschaft $f = \sum_{i=0}^{\deg f} f_i \cdot x^i$ erfüllt, da ja $x^0 = (1, 0, 0, \ldots)$, $x^1 = (0, 1, 0, 0, \ldots)$, $x^2 = (0, 0, 1, 0, 0, \ldots)$, …. Also gilt $(\sum_{i=0}^{\deg f} f_i \cdot x^i) + (g) = f + (g)$. Da $g \mid f$, gilt $f + (g) = 0 + (g)$. Also ist $x + (g)$ eine Nullstelle von f in $\boldsymbol{L}$. Da f eine Nullstelle l in $\boldsymbol{L}$ hat, gibt es $h \in \boldsymbol{L}[x]$, sodass $f = (x - l) \cdot h$. Da h kleineren Grad als f hat, gibt es nach nach Induktionsvorraussetzung einen Erweiterungskörper $\boldsymbol{M}$ von $\boldsymbol{L}$, sodass jeder in $\boldsymbol{M}[x]$ irreduzible Teiler des Polynoms h Grad 1 hat. In $\boldsymbol{M}[x]$ hat jeder irreduzible Teiler von f also Grad 1. ■

SATZ 8.20. *Sei $\boldsymbol{K}$ ein endlicher Körper, und sei $n \in \mathbb{N}$. Dann gibt es ein über $\boldsymbol{K}$ irreduzibles Polynom vom Grad n in $\boldsymbol{K}[x]$.*

Beweis: Sei $q := \boldsymbol{K}$. Es gibt einen Erweiterungskörper $\boldsymbol{E}$ von $\boldsymbol{K}$, in dem $x^{q^n} - x$ in lauter Linearfaktoren zerfällt. Wir bilden

$$L := \{e \in E \mid e^{q^n} - e = 0\}.$$

Mit Satz 8.9 (1) erhalten wir, dass $\boldsymbol{L}$ ein Unterkörper von $\boldsymbol{E}$ ist; mit mit Satz 8.9 (2), dass $\boldsymbol{L}$ ein Erweiterungskörper von $\boldsymbol{K}$ ist. Da $x^{q^n} - x$ über $\boldsymbol{E}$ in lauter Linearfaktoren zerfällt, gibt es $e_1, e_2, \ldots, e_{q_n} \in E$, sodass

$$x^{q^n} - x = \prod_{r}^{q^n} (x - e_r).$$

Mithilfe der Ableitung zeigt man wieder, dass $x^{q^n} - x$ quadratfrei ist, und dass daher alle e_i verschieden sind. Alle e_i liegen in $\boldsymbol{L}$. Der Körper $\boldsymbol{L}$ hat daher mindestens q^n Elemente. Da $x^{q^n} - x$ in $\boldsymbol{E}$ höchstens q^n Nullstellen haben kann, hat $\boldsymbol{L}$ höchstens q^n Elemente.

Sei nun α ein erzeugendes Element der multiplikativen Gruppe $(L^*, \cdot)$ von $\boldsymbol{L}$, und sei $f \in \boldsymbol{K}[x]$ ein normiertes, erzeugendes Element des Ideals

$$I = \{g \in \boldsymbol{K}[x] \mid \overline{g}(\alpha) = 0\}.$$

Wegen $x^{q^n} - x \in I$ gilt $I \neq \{0\}$. Wir zeigen nun:

(8.4) $\qquad f$ ist ein irreduzibles Element von $\boldsymbol{K}[x]$.

Wir nehmen an, es gibt normierte $f_1, f_2 \in \boldsymbol{K}[x]$ sodass $f = f_1 \cdot f_2$. Dann gilt $\overline{f_1}(\alpha) \cdot \overline{f_2}(\alpha) = 0$. Wenn nun $\overline{f_1}(\alpha) = 0$, so gilt $f \mid f_1$, und somit $f_2 = 1$. Das beweist (8.4).

Die Abbildung

$$\begin{array}{rccc} \Phi & : & \boldsymbol{K}[x] & \longrightarrow & \boldsymbol{L} \\ & & g & \longmapsto & g(\alpha) \end{array}$$

ist surjektiv ($\Phi(x^k) = \alpha^k$ für alle k); ihr Kern ist I. Wir wissen, das $\boldsymbol{L}$ genau q^n Elemente hat. $\boldsymbol{K}[x]/I$ hat daher ebenfalls genau q^n Elemente, und somit gilt $\deg f = n$. Das Polynom f ist also irreduzibel vom Grad n. ■

DEFINITION 8.21 (Möbiusfunktion). Wir definieren $\mu : \mathbb{N} \to \{-1, 0, 1\}$ durch

$$\mu(n) = \begin{cases} (-1)^k, \text{ falls } n = p_1 \cdot p_2 \cdots p_k \text{ mit } p_i \neq p_j \text{ für } i \neq j, \\ 1 \text{ falls } n = 1, \\ 0 \text{ sonst.} \end{cases}$$

SATZ 8.22. *Die Anzahl N der irreduziblen Polynome vom Grad n über einem Körper mit q Elementen ist gegeben durch*

$$N = \frac{1}{n} \sum_{d \mid n} \mu(d) q^{\frac{n}{d}}.$$

Beweis: [**Wil99**, p.49].

ÜBUNGSAUFGABEN 8.23.

(1) Leiten Sie aus diesem Satz her, dass es über jedem endlichen Körper für jedes n ein irreduzibles Polynom vom Grad k gibt.

Für Polynome $f, g \in \boldsymbol{K}[x]$ bezeichnen wir mit $f \circ g$ das Polynom, das man erhält, wenn man g in f einsetzt.

SATZ 8.24. *Sei $\boldsymbol{K}$ ein Körper mit q Elementen, sei $n \in \mathbb{N}$, und sei $f \in \boldsymbol{K}[x]$. Dann gilt*

$$f \circ x^{q^n} = x^{q^n} \circ f.$$

Beweis: Sei p die Charakteristik von $\boldsymbol{K}$. Es gibt dann ein m, sodass $q = p^m$. Es gilt dann

$$\begin{aligned} x^{q^n} \circ f &= f^{q^n} \\ &= (\sum_{i=0}^{\deg f} f_i x^i)^{(q^n)} \\ &= (\sum_{i=0}^{\deg f} f_i x^i)^{(p^{mn})} \\ &= \sum_{i=0}^{\deg f} f_i^{p^{mn}} (x^i)^{(p^{mn})} \\ &= \sum_{i=0}^{\deg g} f_i^{q^n} (x^i)^{(q^n)} \\ &= \sum_{i=0}^{\deg f} f_i (x^{(q^n)})^i \\ &= f \circ x^{(q^n)}. \blacksquare \end{aligned}$$

In einem Euklidischen Bereich kann man einen größten gemeinsamen Teiler von a, b definieren, zum Beispiel als einen Erzeuger des von a und b erzeugten Ideals. Wenn wir aus jeder Klasse konjugierter Elemente einen Repräsentanten auswählen, so können wir ggT sogar als Funktion definieren.

SATZ 8.25. *Sei $\boldsymbol{E}$ ein Euklidischer Bereich, und sei $f \in E$, f nicht invertierbar, und seien $n, m \in \mathbb{N}_0$, nicht beide* 0. *Dann gilt* $\mathrm{ggT}(f^m - 1, f^n - 1) = f^{\mathrm{ggT}(n,m)} - 1$.

Beweis: Wir beweisen den Satz durch Induktion nach $\max(m, n)$. Wenn $m = n = 1$, dann gilt der Satz offensichtlich. Sei nun $\max(m, n) > 1$.

- *Fall* $m = 0$ oder $n = 0$: offensichtlich.
- *Fall* $m > n \geq 1$: Es gilt $\mathrm{ggT}(f^m - 1, f^n - 1) = \mathrm{ggT}(f^m - 1 - f^{m-n} \cdot (f^n - 1), f^n - 1)$, da beide Polynompaare die gleichen gemeinsamen Teiler haben. Durch ausrechnen erhalten wir $\mathrm{ggT}(f^m - 1, f^n - 1) = \mathrm{ggT}(f^{m-n} - 1, f^n - 1)$. Da $m > n$, gilt $\max(m - n, n) < \max(m, n)$. Nach Induktionsannahme gilt also $\mathrm{ggT}(f^{m-n} - 1, f^n - 1) = f^{\mathrm{ggT}(m-n,n)} - 1 = f^{\mathrm{ggT}(m,n)} - 1$.
- *Fall* $n > m \geq 1$: analog.
- *Fall* $m = n$: offensichtlich. ■

KOROLLAR 8.26.

(1) *Sei $\boldsymbol{K}$ ein Körper, sei f ein normiertes Polynom in $\boldsymbol{K}[x]$ mit* $\deg(f) \geq 1$, *und seien $m, n \in \mathbb{N}$. Dann gilt* $\mathrm{ggT}(f^m - 1, f^n - 1) = f^{\mathrm{ggT}(n,m)} - 1$.
(2) *Seien $f, m, n \in \mathbb{N}$ mit $f \geq 2$. Dann gilt* $\mathrm{ggT}(f^m - 1, f^n - 1) = f^{\mathrm{ggT}(n,m)} - 1$.

SATZ 8.27. *Sei $\boldsymbol{K}$ ein endlicher Körper mit q Elementen, und sei $n \in \mathbb{N}$. Sei F die Menge aller über $\boldsymbol{K}$ irreduziblen, normierten Polynome in $\boldsymbol{K}[x]$, deren Grad ein Teiler von n ist. Dann gilt*

$$\prod_{f \in F} f = x^{q^n} - x.$$

Beweis: Wir zerlegen $x^{q^n} - x$ in ein Produkt normierter, über $\boldsymbol{K}$ irreduzibler Polynome; wir finden also $k \in \mathbb{N}$ und normierte irreduzible Polynome $g_1, g_2, \ldots, g_k$, sodass

$$x^{q^n} - x = \prod_{i=1}^{k} g_i \,.$$

Als erstes zeigen wir, dass alle g_i verschieden sind. Nehmen wir an, dass es ein Polynom h mit $\deg h \geq 1$ gibt, sodass $h^2 \mid x^{q^n} - x$. Dann gibt es $a \in \boldsymbol{K}[x]$, sodass

$$h^2 \cdot a = x^{q^n} - x.$$

Durch Differenzieren erhalten wir

$$2hh'a + h^2a' = q^n * x^{q^n - 1} - 1,$$

und da q^n ein Vielfaches der Charakteristik von $\boldsymbol{K}$ ist, gilt

$$h(2h'a + ha') = -1.$$

Das ist aber nicht möglich, weil $\deg h \geq 1$. Sei also $G = \{g_i \mid i \in \{1, 2, \ldots, k\}\}$. Dann gilt, weil alle g_i verschieden sind, $x^{q^n} - x = \prod_{g \in G} g$. Wir zeigen nun noch

$$F = G. \tag{8.5}$$

$\subseteq$: Sei also $f \in F$ ein normiertes, über $\boldsymbol{K}[x]$ irreduzibles Polynom, dessen Grad (=: d) ein Teiler von n ist. Wir müssen zeigen, dass f das Polynom $x^{q^n} - x$ teilt. Dazu betrachten wir den Körper $\boldsymbol{K}[x]/(f)$. Dieser Körper hat q^d Elemente. Es gilt also wegen Satz 8.9 (2) $(x + (f))^{q^d} = x + (f)$. Das bedeutet

$$f \mid x^{q^d} - x.$$

Wir zeigen nun

$$x^{q^d} - x \mid x^{q^n} - x. \tag{8.6}$$

Dazu zeigen wir $x^{q^d - 1} - 1 \mid x^{q^n - 1} - 1$. Wir berechnen $\mathrm{ggT}(x^{q^d - 1} - 1, x^{q^n - 1} - 1)$. Nach Lemma 8.26 gilt $\mathrm{ggT}(x^{q^d - 1} - 1, x^{q^n - 1} - 1) = x^{\mathrm{ggT}(q^d - 1, q^n - 1)} - 1 = x^{(q^{\mathrm{ggT}(d,n)})} - 1 = x^{q^d} - 1$; das impliziert (8.6). Wir erhalten also $f \mid x^{q^n} - x$. Somit (Fundamentallemma) liegt $f \in G$.
$\supseteq$: Sei g ein normiertes irreduzibles Polynom, das $x^{q^n} - x$ teilt. Wir müssen zeigen, dass $d := \deg g$ ein Teiler von n ist. Der Körper $\boldsymbol{K}[x]/(g)$ hat q^d Elemente. Es gilt also $g \mid x^{q^d} - x$. Falls $g \neq x$, gilt $g \mid \mathrm{ggT}(x^{q^d - 1} - 1, x^{q^n - 1} - 1) = x^{\mathrm{ggT}(g^d - 1, q^n - 1)} - 1 = x^{(q^{\mathrm{ggT}(n,d)} - 1)} - 1$. Sei $r := \mathrm{ggT}(n, d)$. Es gilt also $g \mid x^{q^r} - x$. Wir zeigen nun, dass jedes Element von

$\boldsymbol{K}[x]/(g)$ eine Nullstelle von $x^{q^r} - x$ ist. Sei dazu $h \in \boldsymbol{K}[x]$. Wir berechnen $(h + (g))^{(q^r)}$. Es gilt

$$\begin{aligned}(h + (g))^{(q^r)} &= h^{(q^r)} + (g) \\ &= (x^{(q^r)} \circ h) + (g) \\ &= (h \circ x^{(q^r)}) + (g) \\ &= (\sum_{i=0}^{\deg h} h_i x^{i \cdot q^r}) + (g).\end{aligned}$$

Es gilt $x^{(q^r)} \equiv x \pmod{g}$, also für alle $i \in \mathbb{N}_0$ auch $x^{i \cdot q^r} \equiv x^i \pmod{g}$. Insgesamt erhalten wir also

$$(h + (g))^{(q^r)} = h + (g),$$

und somit ist jedes Element aus $\boldsymbol{K}[x]/(g)$ eine Nullstelle von $x^{q^r} - x$. Da $r \geq 1$, ist $x^{q^r} - x$ nicht das Nullpolynom. Es hat also höchstens q^r Nullstellen. Der Körper $\boldsymbol{K}[x]/(g)$ hat q^d Elemente. Es gilt also $d \leq r$, also $d \leq \mathrm{ggT}(n, d)$. Das bedeutet, dass d ein Teiler von n ist. Das Polynom g liegt also in der Menge F. ■

4. Test auf Irreduzibilität

Der folgende Satz liefert einen Test, ob ein Polynom irreduzibel über einem endlichen Körper mit q Elementen ist.

SATZ 8.28. *Sei $\boldsymbol{K}$ ein Körper mit q Elementen, sei $n \in \mathbb{N}$ und sei $f \in K[x]$ mit* $\deg(f) = n$. *Äquivalent sind:*

(1) *Für alle $i \in \{1, 2, \ldots, \lfloor \frac{n}{2} \rfloor\}$ gilt:*

$$\mathrm{ggT}(f, x^{q^i} - x) = 1.$$

(2) *f ist irreduzibel über $\boldsymbol{K}$.*

Beweis: (1)⇒(2): Wenn f nicht irreduzibel über $\boldsymbol{K}$ ist, so gibt es ein über $\boldsymbol{K}$ irreduzibles Polynom $g \in \boldsymbol{K}[t]$ mit $g \mid f$, $1 \leq \deg(g) \leq \lfloor \frac{n}{2} \rfloor$. Sei $i := \deg(g)$. Dann gilt wegen Satz 8.15 $g \mid (x^{q^i} - x)$,und somit $g \mid \mathrm{ggT}(f, x^{q^i} - x)$, im Widerspruch zu $\mathrm{ggT}(f, x^{q^i} - x) = 1$. (2)⇒(1): Wenn f über $\boldsymbol{K}$ irreduzibel ist, $i \in \{1, \ldots, \lfloor \frac{n}{2} \rfloor\}$, und $\mathrm{ggT}(f, x^{q^i} - x) \neq 1$, so gilt $f \mid x^{q^i} - x$. Wegen Satz 8.27 ist der Grad von f dann ein Teiler von i; somit gilt $n \leq i$, im Widerspruch zu $i \leq \lfloor \frac{n}{2} \rfloor$. ■

SATZ 8.29. *Sei $\boldsymbol{K}$ ein Körper mit q Elementen, sei $n \in \mathbb{N}$ und sei $f \in K[x]$ mit* $\deg(f) = n$, $\mathrm{ggT}(f, f') = 1$, *und seien $f_1, \ldots, f_r$ über $\boldsymbol{K}$ irreduzible Polynome mit $\prod_{i=1}^{r} f_i = f$. Sei Q die $n \times n$-Matrix, an deren (i, j)-ter Stelle der Koeffizient von x^{i-1} des Polynoms $x^{q \cdot (j-1)} \bmod f$ steht. Dann ist die Dimension des Nullraums von $Q - I$ gleich r.*

Es gilt $(Q - I) \cdot \begin{pmatrix} a_0 \\ \vdots \\ a_n \end{pmatrix} = 0$ genau dann, wenn für das Polynom $a := \sum_{j=0}^{n-1} a_j x^{q^j}$ gilt, dass $a(x^q) - a(x)$ ein Vielfaches von f ist. Wegen Satz 8.24 gilt $a(x^q) = a(x)^q$.

Wir zeigen nun, dass $f \mid a(x)^q - a(x)$ genau dann gilt, wenn es $\alpha_1, \ldots, \alpha_r \in K$ gibt, sodass für alle $i \in \{1, \ldots, r\}$ gilt, dass $f_i \mid (a(x) - \alpha_i)$. Wenn es $(\alpha_1, \ldots, \alpha_r) \in K^r$ mit dieser Eigenschaft gibt, so gilt für jedes i, dass $f_i \mid (a(x) - \alpha_i) \mid \prod_{\beta \in K}(a(x) - \beta)$. Wegen Satz 8.16 gilt also $f_i \mid (a(x)^q - a(x)$. Da alle f_i irreduzibel und paarweise verschieden sind (wegen $\mathrm{ggT}(f, f') = 1$), gilt also $f \mid a(x)^q - a(x)$. Sei nun umgekehrt a so, dass $f \mid a(x)^q - a(x)$, und $i \in \{1, \ldots, r\}$. Dann gilt $f_i \mid \prod_{\beta \in K}(a(x) - \beta)$. Da f_i irreduzibel über $\boldsymbol{K}$ ist, teilt es einen der Faktoren.

Wegen des Chinesischen Restsatzes gibt es für jedes r-Tupel $(\alpha_1, \ldots, \alpha_r) \in K^r$ genau ein Polynom a vom Grad $\leq n-1$, sodass $f_i \mid a(x) - \alpha_i$ für alle $i \in \{1, \ldots, r\}$. Folglich hat das Gleichungssystem $(Q - I) \cdot a = 0$ genau q^r Lösungen, die Dimension des Nullraums ist also r. ■

Literaturverzeichnis

[AZ98] M. Aigner and G. M. Ziegler, *Proofs from THE BOOK*, Springer Berlin-Heidelberg, 1998.

[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.

[Euk91] Euklid, *Die Elemente*, Wissenschaftliche Buchgesellschaft, Darmstadt, 1991, Buch I–XIII. [Book I–XIII], Based on Heiberg's text, Translated from the Greek and edited by Clemens Thaer.

[GAP99] The GAP Group, Aachen, St. Andrews, *GAP – Groups, Algorithms, and Programming, Version 4.1*, 1999, (`http://www-gap.dcs.st-and.ac.uk/~gap`).

[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.

[Pil84] G. F. Pilz, *Algebra – ein Reiseführer durch die schönsten Gebiete*, Universitätsverlag Rudolf Trauner, Linz, 1984.

[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.

[Wil99] W. Willems, *Codierungstheorie*, de Gruyter, Berlin, New York, 1999.