Notizen zur Vorlesung

“Einführung in die Algebra und Diskrete Mathematik”

Erhard Aichinger

Mitarbeit: Bernd Langensteiner und Peter Mayr.

Alle Rechte vorbehalten

Linz, im Mai 2005

Univ.-Doz. Dr. Erhard Aichinger
Institut für Algebra
Johannes Kepler Universität Linz

e-mail: erhard@algebra.uni-linz.ac.at
1. Auflage im Mai 2005.

Druck: Universitätsdruckerei Linz

Vorwort

Bernd Langensteiner hat es übernommen, eine Mitschrift meiner Vorlesung *Einführung in die Algebra* (Sommersemester 2000) zu einer Rohversion des vorliegenden Skriptums auszuarbeiten. Für die Mithilfe bedanke ich mich auch bei Waltraud Eidljörg, Barbara Fattinger und Peter Mayr.

Damit dieses Skriptum eines Tages druckreif wird, bitte ich alle Leser, mir Fehler mitzuteilen (am besten per e-mail). Zur Vorlesung möchte ich die Bücher [**Robinson, 2003**] und [**Lidl and Pilz, 1998**] empfehlen.

Linz, im Mai 2005 E.A.

Inhaltsverzeichnis

Vorwort 2

Kapitel 1. Rechnen in den ganzen Zahlen 4
1. Primfaktorzerlegung 4
2. Größter gemeinsamer Teiler und kleinstes gemeinsames Vielfaches 7
3. Lösen von Kongruenzen 12
4. Der Ring $\mathbb{Z}_n$ 19
5. Ein public-key-encryption system: das RSA-Verfahren 24
6. Die Multiplikativität der Eulerschen φ-Funktion 27

Kapitel 2. Gruppen 31
1. Motivation 31
2. Definition einer Gruppe 31
3. Beispiele für Gruppen 34
4. Permutationsgruppen und der Satz von Cayley 38
5. Sätze von Lagrange und Fermat 43
6. Die Abzähltheorie von Pólya 45
7. Kongruenzrelationen auf Gruppen 50

Kapitel 3. Ausgewählte Kapitel der Diskreten Mathematik 54
1. Graphen 54
2. Der Satz von Ramsey 57

Kapitel 4. Polynome und Körper 62
1. Körper 62
2. Polynome 63
3. Zerfällungskörper 64
4. Irreduzible Polynome über $\mathbb{Q}$ 65

Kapitel 5. Endliche Körper 66
1. Primkörper 66
2. Die multiplikative Gruppe eines endlichen Körpers 67
3. Körper aus irreduziblen Polynomen 69
4. Existenz irreduzibler Polynome 70

Literaturverzeichnis 73

KAPITEL 1

Rechnen in den ganzen Zahlen

Die Summe, das Produkt und die Differenz zweier ganzer Zahlen sind wieder eine ganze Zahl. Man kann aber innerhalb von $\mathbb{Z}$ nicht uneingeschränkt dividieren; so ist etwa 5 nicht durch 7 teilbar. In diesem Kapitel untersuchen wir die Teilbarkeit. Die Disziplin, die sich tiefgehend mit Teilbarkeit und Primzahlen beschäftigt, heißt *Zahlentheorie* [**Remmert and Ullrich, 1987**].

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 folgende beiden Bedingungen gelten:

(1) Es gilt $p > 1$.
(2) Für alle $a, b \in \mathbb{N}$ mit $p = a \cdot b$ gilt $a = 1$ oder $b = 1$.

Definition 1.2 (Teilbarkeit). Für $x, y \in \mathbb{Z}$ gilt

$$x \textit{ teilt } y$$

genau dann, wenn es ein $z \in \mathbb{Z}$ gibt, sodass $y = z \cdot x$ ist.

Wir schreiben dann auch $x|y$; die Zahl y heißt ein *Vielfaches* von x;

Definition 1.3 (Ideal). Eine Teilmenge I von $\mathbb{Z}$ ist ein *Ideal* von $\mathbb{Z}$, falls sie alle folgenden Eigenschaften erfüllt:

(1) Für alle $i, j \in I$ liegt auch $i - j$ in I.
(2) Für alle $z \in \mathbb{Z}$ und alle $i \in I$ liegt auch $z \cdot i$ in I.
(3) I ist nicht die leere Menge.

Beispiele:

(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 1.4. *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 1.5 (Fundamentallemma). *Sei p eine Primzahl, und seien $a, b \in Z$. Falls p ein Produkt $a \cdot b$ teilt, so teilt p einen der beiden Faktoren a oder b.*

Beweis: Wir definieren I durch

$$I := \{x \in \mathbb{Z} \mid p \text{ teilt } a \cdot x\}.$$

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 $z \in Z$, 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 1.6. *Jede natürliche Zahl besitzt eine Zerlegung in Primfaktoren*
$$a = p_1 \cdot \ldots \cdot p_n.$$

Beweisskizze: Wir zerlegen a, bis es nicht mehr geht. □

Satz 1.7. *Die Primfaktorenzerlegung einer natürlichen Zahl $a \geq 2$ ist bis auf die Reihenfolge der Primfaktoren eindeutig. Wenn also*
$$a = p_1 \cdot \ldots \cdot p_n = q_1 \cdot \ldots \cdot q_m$$
und alle p_i, q_i Primzahlen sind, dann gilt $m = n$, und es gibt eine bijektive Abbildung $\pi : \{1, \ldots, n\} \to \{1, \ldots, m\}$, sodass $p_i = q_{\pi(i)}$.

Beweis: Wir zeigen das mit Induktion nach a. Für $a = 2$ ist der Satz klar[1].

Nun sei $a > 2$, außerdem sei
$$a = p_1 \ldots p_n = q_1 \ldots q_m.$$
Da p_1 die Zahl a teilt, erhalten wir aus dem Fundamentallemma, Satz 1.5, dass es ein $j \in \{1, 2, \ldots m\}$ gibt, sodass $p_1 \mid q_j$.[2] Da q_j prim ist, gilt $p_1 = q_j$. Wenn $n = 1$ ist, also $a = p_1$, dann gilt $q_1 q_2 \ldots q_m = q_j$, also $m = 1$ und $j = 1$. Somit sind die beiden Zerlegungen von a gleich. Wenn $n \neq 1$, dann gilt
$$a' = p_2 \cdot \ldots \cdot p_n = q_1 \cdot \ldots \cdot q_{j-1} \cdot q_{j+1} \cdot \ldots \cdot q_m,$$

[1] Warum eigentlich? – Die einzige Zerlegung von 2 ist $2 = 2$, denn würde in einer Zerlegung von 2 eine Primzahl ≥ 3 vorkommen, wäre auch das Produkt ≥ 3 und könnte also nicht 2 ergeben. Aus dem gleichen Grund kann auch 2 nur einmal in einer Zerlegung von 2 vorkommen.

So einfach – und sinnlos – diese Überlegungen auch scheinen, so scheint es doch, also würden wir implizit unbewiesene Behauptungen, verwenden, etwa die Behauptung, dass das Produkt von natürlichen Zahlen immer größer gleich jedem der Faktoren ist. Um solche Behauptungen zu beweisen, würden wir brauchen:

(1) Eine Definition der Menge $\mathbb{N}$.
(2) Eine Definition der Operationen $+$ und $\cdot$.
(3) Eine Definition der Relation $<$.

[2] Das Fundamentallemma gibt allerdings nur darüber Auskunft, was passiert, wenn p_1 ein Produkt zweier Faktoren teilt. Wie bewältigen Sie die formale Spielerei, zu zeigen, dass wir auch für $m \neq 2$ erhalten, dass p_1 irgendein q_j teilt?

wobei diese beiden Zerlegungen von a' nach Induktionsvoraussetzung "gleich" sind. $\square$

Übungsaufgaben 1.8.

(1) [**Remmert and Ullrich, 1987**, 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 ([**Euklid, 1991**, 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

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

wobei $\alpha_i, \beta_i \in \mathbb{N}_0$, und fast alle $\alpha_i, \beta_i = 0$ sind, dann gilt $a|b$ genau dann, wenn für alle i $\alpha_i \leq \beta_i$ 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 $q|a \cdot b$ gilt $q|a$ oder es gibt ein $n \in \mathbb{N}$, sodass $q|b^n$.

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

2. Größter gemeinsamer Teiler und kleinstes gemeinsames Vielfaches

2.1. Der größte gemeinsame Teiler. Zwei ganze Zahlen haben stets einen gemeinsamen Teiler, nämlich 1. In diesem Abschnitt werden wir eine Methode vorstellen, den größten unter allen gemeinsamen Teilern zu finden: den *Euklidischen ggT-Algorithmus.*

Definition 1.9 (Größter gemeinsamer Teiler). Für zwei Zahlen $a, b \in \mathbb{Z}$ (nicht beide 0) ist 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*

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

(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 $a|bc$ 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 $a|y$, $b|y$, $\mathrm{ggT}\,(a, b) = 1$. Zeigen Sie (ohne Primfaktorzerlegung): $a \cdot b|y$.

(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, $\mathrm{ggT}\,(ka, kb)|\mathrm{ggT}\,(a, b)$ 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) $G_2(a_1, a_2, \ldots, a_n) := \max\{z \in \mathbb{N} \mid z | a_i \text{ für alle } i \in \{1, 2, \ldots, n\}\}$.
   (c) $G_3 := \min\{z \in \mathbb{N} \mid \text{ es gibt } \lambda_1, \lambda_2, \ldots, \lambda_n \in \mathbb{Z}, \text{ sodass } z = \sum_{i=1}^{n} \lambda_i a_i\}$.
   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

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

2.2. Der Euklidische ggT-Algorithmus. 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

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

"$\subseteq$": 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: 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 1.14.

(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) $a = 610$, $b = 987$.

2.3. 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 1.15. Es seien $a, b \in \mathbb{Z} \setminus \{0\}$. Dann ist kgV (a, b) definiert durch

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

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

Satz 1.16. *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:*

$$\text{kgV}\ (a,b) \mid s.$$

Jedes gemeinsame Vielfache ist also ein Vielfaches des kgV *.*

Beweis: Wir betrachten $(a) = \{a \cdot z \mid z \in \mathbb{Z}\}$ und $(b) = \{b \cdot z \mid z \in \mathbb{Z}\}$. 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. $\square$

Zwischen ggT und kgV kann man folgenden Zusammenhang herstellen:

Satz 1.17. *Seien $a, b \in \mathbb{N}$. Dann gilt*

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

Beweis: Wir verwenden die Primfaktorzerlegung von $a = \prod p_i^{\nu_i}$, und $b = \prod p_i^{\sigma_i}$. Aus dem Fundamentallemma (Satz 1.5) kann man herleiten, dass dann gelten muss:

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

Daraus folgt:

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

$\square$

Übungsaufgaben 1.18.

(1) Zeigen Sie ohne Verwendung der Primfaktorzerlegung, dass für alle $a, b \in \mathbb{N}$ gilt:
$$\text{kgV}\,(a,b) \cdot \text{ggT}\,(a,b) = a \cdot b.$$
Hinweis: Zeigen Sie dazu $ab | \text{ggT}\,(a,b) \cdot \text{kgV}\,(a,b)$ und $\text{kgV}\,(a,b) | \frac{ab}{\text{ggT}\,(a,b)}$.

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

(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) $K_1(a_1) := a_1$, $K_1(a_1, a_2, \ldots, a_n) = \text{kgV}\,(K_1(a_1, a_2, \ldots, a_{n-1}), a_n)$.
   (b) $K_2(a_1, a_2, \ldots, a_n) := \min\{z \in \mathbb{N} \mid a_i | z \text{ für alle } i \in \{1, 2, \ldots, n\}\}$.
   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
$$K_2(a_1, a_2, \ldots, a_n) := \min\{z \in \mathbb{N} \mid a_i | z \text{ für alle } i \in \{1, 2, \ldots, n\}\}.$$
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

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

3. Lösen von Kongruenzen

Bisher haben wir bei gegebenem $n \in \mathbb{Z}$ die Elemente in $\mathbb{Z}$ danach unterschieden, ob sie durch n teilbar sind oder nicht, d. h., ob sie bei Division durch n den Rest 0 oder einen von 0 verschiedenen Rest haben. Die Elemente mit einem von 0 verschiedenen Rest kann man dadurch weiter unterteilen, dass man alle Elemente mit dem gleichen Rest in eine Klasse zusammenfasst, die man dann eine *Restklasse bezüglich* n nennt. Elemente aus derselben Restklasse heißen *kongruent modulo* n.

Definition 1.19. 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 1.20. *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 $c | a \cdot y - b$.

(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 $ax \equiv b\,(\bmod c)$. $\square$

SATZ 1.21. *Seien $a, c \in \mathbb{Z}$ (nicht beide $= 0$), und sei $b \in \mathbb{Z}$. Sei x_0 eine Lösung von*

$$ax \equiv b \pmod{\text{c}}\,. \tag{3.1}$$

Dann ist die Lösungsmenge von (3.1) *gegeben durch:*

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

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

$$\begin{array}{rcl} a\left(x_0 + k\frac{c}{\text{ggT}\,(a,c)}\right) & = & ax_0 + ak\frac{c}{\text{ggT}\,(a,c)} \\ & \equiv_c & b + ak\frac{c}{\text{ggT}\,(a,c)} \\ & = & b + ck\frac{a}{\text{ggT}\,(a,c)} \\ & \equiv_c & b. \end{array}$$

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

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

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

oder, äquivalent dazu,

$$c \mid a\,(x_1 - x_0)\,.$$

Daher gilt auch

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

Da

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

gilt

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

$\square$

Bemerkung: Das System $ax \equiv b \pmod{c}$ ist also äquivalent zu

$$x \equiv x_0 \left(\bmod \frac{c}{\text{ggT}\,(a,c)}\right),$$

wobei x_0 eine spezielle Lösung von $ax \equiv b \pmod{c}$ ist.

ÜBUNGSAUFGABEN 1.22.

(1) Lösen Sie die Gleichung
$$207\,x \equiv 18 \pmod{1989}$$
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
$$\begin{aligned} x &\equiv a_1 \pmod{m_1} \\ x &\equiv a_2 \pmod{m_2}\,, \end{aligned}$$
wobei $m_1, m_2 \in \mathbb{N}$ und $a_1, a_2 \in \mathbb{Z}$.

Beispiele: 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 $x = 7$. Es stellt sich daher die Frage, wann und wie solche Systeme lösbar sind.

Satz 1.23. *Seien $a_1, a_2 \in \mathbb{Z}$, $m_1, m_2 \in \mathbb{N}$. Das System*
$$\begin{aligned} x &\equiv a_1 \pmod{\mathrm{m}_1} \\ x &\equiv a_2 \pmod{\mathrm{m}_2} \end{aligned}$$
ist genau dann lösbar, wenn gilt
$$\mathrm{ggT}\ (m_1, m_2) \mid a_1 - a_2.$$

Beweis: "$\Rightarrow$": 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 $\mathrm{ggT}\ (m_1, m_2) \mid (x - a_1)$ und $\mathrm{ggT}\,(m_1, m_2) | (x - a_2)$, und somit
$$\mathrm{ggT}\ (m_1, m_2) \mid (x - a_2) - (x - a_1) = (a_1 - a_2)\,.$$

"$\Leftarrow$" 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 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 1.24. *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

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

Beweis: "$\supseteq$": Wir setzen

$$x_0 + k \cdot \text{kgV}\ (m_1, m_2)$$

in die erste Kongruenz ein und erhalten

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

Das gleiche gilt für die zweite Kongruenz.

"$\subseteq$": Wir fixieren $x_1 \in L$. Um zu zeigen, dass $x_1 \in \{x_0 + k \cdot \text{kgV}\ (m_1, m_2) \mid k \in \mathbb{Z}\}$, zeigen wir, dass $x_1 - x_0$ ein Vielfaches von kgV (m_1, m_2) 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 $(x_1 - x_0) \equiv 0 \pmod{m_1}$ und somit $m_1 \mid (x_1 - x_0)$. Ebenso zeigt man, dass $m_2 \mid (x_1 - x_0)$ gilt.

Da das kgV jedes gemeinsame Vielfache teilt, gilt kgV $(m_1, m_2) \mid (x_1 - x_0)$. □

Übungsaufgaben 1.25.

(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 1.26. *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*

$$\begin{aligned} x &\equiv a_1 \pmod{m_1} \\ x &\equiv a_2 \pmod{m_2} \\ &\vdots \\ x &\equiv a_r \pmod{m_r} \end{aligned} \tag{3.2}$$

eine Lösung x_0 hat, dann ist (3.2) *äquivalent zu*

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

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

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

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 1.27. *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 1.28 (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*
$$\mathrm{ggT}\ (m_i, m_j) \mid a_i - a_j.$$

Beweis: "(1) $\Rightarrow$ (2)" ist offensichtlich. "(2) $\Leftrightarrow$ (3)" gilt wegen Satz 1.23.

"(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 1.23 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 1.26 ist $x \equiv a_1 \pmod{m_1}, \ldots, x \equiv a_r \pmod{m_r}$ äquivalent zu
$$\begin{aligned} x &\equiv a_1 \pmod{m_1} \\ x &\equiv y \pmod{m_2 \vee \ldots \vee m_r}. \end{aligned} \tag{3.3}$$

Jetzt müssen wir zeigen, dass (3.3) lösbar ist. Das gilt nach Satz 1.23 genau dann, wenn
$$m_1 \wedge (m_2 \vee \ldots \vee m_r) \mid y - a_1. \tag{3.4}$$

Es gilt $a \wedge (b \vee c) = (a \wedge b) \vee (a \wedge c)$. Daher ist (3.4) 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:

$$(m_1 \wedge m_i) \mid (y - a_1). \tag{3.5}$$

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 $(m_i \wedge m_1)|(y - a_1)$. Nun ist jedes gemeinsame Vielfache eine Vielfaches des kleinsten gemeinsamen Vielfachen, und somit gilt (3.4). □

Beispiel: Wir lösen folgendes System

$$\begin{aligned} x &\equiv 2 \pmod{15} \\ x &\equiv 8 \pmod{21} \\ x &\equiv 7 \pmod{55} \end{aligned} \tag{3.6}$$

Wir kennen bereits die Lösungen von $x \equiv 2 \pmod{15}$, $x \equiv 8 \pmod{21}$. Das System (3.6) ist daher äquivalent zu

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

Wir berechnen $\operatorname{ggT}(55, 105)$ 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 1.29.

(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) $f(x) = \frac{x \cdot (x-1)}{2}$.

(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.

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

In $\mathbb{Z}$ definieren wir für $n \in \mathbb{N}$ die Relation $\equiv_n$ durch

$$a \equiv_n b :\Leftrightarrow n \mid b - a.$$

Die Relation $\equiv_n$ ist eine Äquivalenzrelation. Die Äquivalenzklasse von $a \in \mathbb{Z}$ ist

$$\{a + z \cdot n \mid z \in \mathbb{Z}\} =: [a]_n\,.$$

Die Faktormenge bezeichnen wir mit $\mathbb{Z}_n$.

$$\mathbb{Z}_n = \{[a]_n \mid a \in \mathbb{Z}\}\,.$$

$\mathbb{Z}_n$ hat n Elemente, und zwar $[0]_n, [1]_n, \ldots, [n-1]_n$. Auf $\mathbb{Z}_n$ definieren wir $\oplus$ und $\odot$ durch:

$$\begin{aligned} [a]_n \oplus [b]_n &:= [a+b]_n \\ [a]_n \odot [b]_n &:= [a \cdot b]_n . \end{aligned}$$

Wir müssen zeigen, dass $\oplus$ und $\odot$ wohldefiniert sind; wir geben hier nur den Beweis für die Wohldefiniertheit von $\odot$. Wir wählen also $a, a', b, b' \in \mathbb{Z}$ sodass $[a]_n = [a']_n$ und $[b]_n = [b']_n$. Zu zeigen ist, dass dann

$$[a \cdot b]_n = [a' \cdot b']_n$$

gilt. Es ist also zu zeigen:

$$\begin{aligned} &n \mid a \cdot b - a' \cdot b' \\ &n \mid a \cdot b - ab' + ab' - a'b' \\ &n \mid a \cdot (b - b') + b' \cdot (a - a') . \end{aligned}$$

Das gilt, denn laut Vorraussetzung gilt $n \mid (b - b')$ und $n \mid (a - a')$. Daher ist $[a \cdot b]_n = [a' \cdot b']_n$, und somit ist das Ergebnis von $[a]_n \odot [b]_n$ unabhängig von der Auswahl der Repräsentanten.

Wir geben nun ein Beispiel für eine *nicht* wohldefinierte Operation. Auf der Menge $\mathbb{Q}$ definieren wir die Relation

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

Wir definieren:

$$\lfloor a \rfloor \odot \lfloor b \rfloor := \lfloor a \cdot b \rfloor .$$

$$\begin{array}{lll} a = 0.1 & b = 100 & \lfloor 0.1 \cdot 100 \rfloor = 10 \\ a' = 0 & b' = 100 & \lfloor 0 \cdot 100 \rfloor = 0 \end{array}$$

Da $0 \not\sim 10$, ist die Operation $\odot$ ist also nicht wohldefiniert.

Mengen mit Operationen bezeichnet man als *algebraische Strukturen*. Strukturen, in denen man drei Operationen zur Verfügung hat, die bestimmte, von den Grundrechnungsarten in ganzen Zahlen bekannte, Rechengesetze erfüllen, heißen *Ringe*. Wir betrachten im folgenden Ringe mit Eins; ein Ring mit Eins hat zwei zweistellige Operationen $(+, \cdot)$, eine einstellige Operation $(-)$ und zwei nullstellige Operationen $(0, 1)$.

Definition 1.30. $(R, +, -, \cdot, 0, 1)$ heißt *Ring mit Eins* genau dann, wenn 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) $(x + y) \cdot z = x \cdot z + y \cdot z$

(7) $x \cdot (y + z) = x \cdot y + x \cdot z$
(8) $1 \cdot x = x$
(9) $x \cdot 1 = x$.

So ist zum Beispiel $(\mathbb{Z}, +, -, \cdot, 0, 1)$ ein Ring mit Eins. Ebenso bilden die 2×2-Matrizen den Ring mit Eins $(\mathrm{Mat}_2(\mathbb{R}), +, -, \cdot, 0, E)$, wobei 0 die Nullmatrix und E die Einheitsmatrix ist.

Satz 1.31. *Sei $(R, +, -, \cdot, 0, 1)$ ein Ring mit Eins. Dann gelten für alle $x, y \in R$ folgende Eigenschaften:*

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

Nun fragen wir uns, ob die Eigenschaft $\forall x, y \in R : x \cdot y = y \cdot x$ in jedem Ring R gilt, und beobachten, dass diese Eigenschaft in $\mathbb{Z}$ gilt, im Ring aller reellen 2×2 Matrizen aber nicht.

Wir betrachten jetzt den Ring $(\mathbb{Z}_n, +, -, \cdot, [0]_n, [1]_n)$ und geben (auf der Suche nach einer "Division") folgende Definition.

Definition 1.32. Ein Element $a \in \mathbb{Z}_n$ heißt *invertierbar*, falls es ein $b \in \mathbb{Z}_n$ gibt, sodass

$$a \cdot b = [1]_n .$$

Beispiel: Betrachten wir etwa $\mathbb{Z}_6$:

$[1]_6$	ist invertierbar	$[1]_6 \cdot [1]_6 = [1]_6$
$[2]_6$	ist nicht invertierbar	
$[3]_6$	ist nicht invertierbar	
$[4]_6$	ist nicht invertierbar	
$[5]_6$	ist invertierbar	$[5]_6 \cdot [5]_6 = [1]_6$
$[0]_6$	ist nicht invertierbar	

Beispiel: In $\mathbb{Z}_5$ gilt:

$$\begin{aligned} [1]_5 \cdot [1]_5 &= [1]_5 \\ [2]_5 \cdot [3]_5 &= [1]_5 \\ [3]_5 \cdot [2]_5 &= [1]_5 \\ [4]_5 \cdot [4]_5 &= [1]_5 \end{aligned}$$

$[0]_5$ ist aber nicht invertierbar.

Der folgende Satz gibt an, welche Elemente in $\mathbb{Z}_n$ invertierbar sind.

Satz 1.33 (Invertierbarkeit). *Sei $n \in \mathbb{N}$ und $a \in \mathbb{Z}$. Dann ist $[a]_n$ genau dann invertierbar in $\mathbb{Z}_n$, wenn* $\operatorname{ggT}(a,n) = 1$.

Beweis: $[a]_n$ invertierbar $\Leftrightarrow \exists x \in \mathbb{Z} : a \cdot x \equiv 1 \pmod{n} \Leftrightarrow \operatorname{ggT}(a,n)$ teilt $1 \Leftrightarrow \operatorname{ggT}(a,n) = 1$. □

Satz 1.34. *Seien a, b invertierbare Elemente aus $\mathbb{Z}_n$. Dann ist auch $a \cdot b$ invertierbar.*

Beweis: Seien $u, v \in \mathbb{Z}_n$ so, dass $a \cdot u = [1]_n$ und $b \cdot v = [1]_n$. Dann gilt: $a \cdot b \cdot v \cdot u = [1]_n$. □

Definition 1.35 (Euler'sche φ–Funktion). Sei $n \in \mathbb{N}$, $n > 1$. Dann ist $\varphi(n)$ definiert durch

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

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

Satz 1.36 (Satz von Euler). *Sei $n \in \mathbb{N}$, $n > 1$, $a \in \mathbb{Z}$,* $\operatorname{ggT}(a,n) = 1$. *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 1.36: Wir wählen $n \in \mathbb{N}$ und $a \in \mathbb{Z}$ beliebig aber fest, und nehmen an, dass $\operatorname{ggT}(a,n) = 1$. Sei

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

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

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

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 $\operatorname{ggT}(a,n) = 1$, 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. Nun zeigen wir:

$$f(I) = I.$$

"$\subseteq$": Wir fixieren $x \in f(I)$. Es gibt also $y \in I$, sodass $x = y \cdot [a]_n$. Da $y \in I$, ist y invertierbar, und somit ist auch $y \cdot [a]_n = x$ invertierbar.

"$\supseteq$": Sei $x \in I$. Wir wählen $b \in \mathbb{Z}$ mit $[b]_n \cdot [a]_n = [1]_n$. Das Element $x \cdot [b]_n$ ist invertierbar und es gilt $f(x \cdot [b]_n) = x$. Also ist x wirklich das Bild eines invertierbaren Elements und liegt somit in $f(I)$.

Die Funktion f ist also eine bijektive Abbildung von I nach I.

Es gilt also:

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

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

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

$$[1]_n = ([a]_n)^{\varphi(n)}$$

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

□

Korollar 1.37. *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 $p|(z^{p-1}-1)$, gilt auch $p|(z^p - z)$, und somit $z^p \equiv z \pmod{p}$.

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

Übungsaufgaben 1.38.

(1) ([**Remmert and Ullrich, 1987**]) 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 $2^n - 1$?

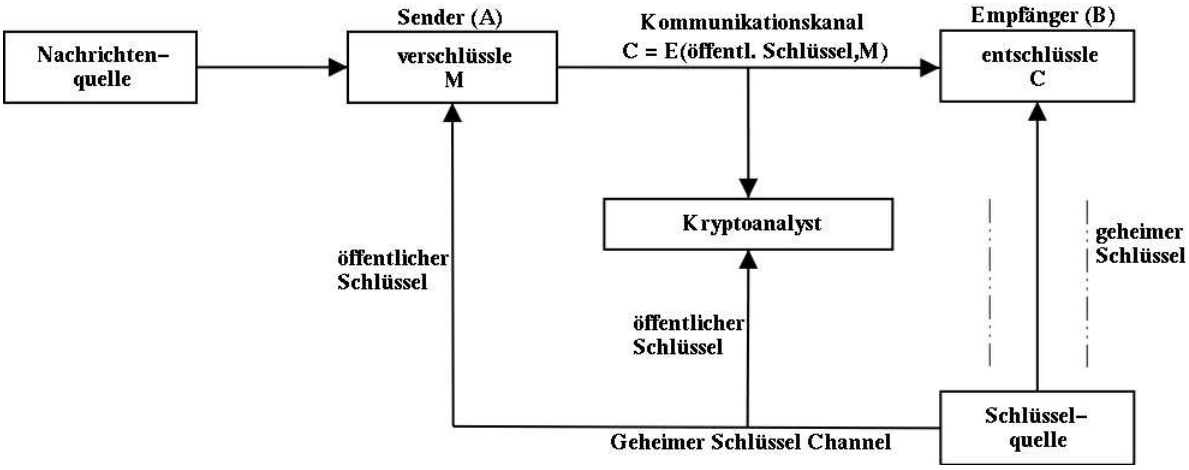
5. Ein public-key-encryption system: das RSA-Verfahren

Zur Verschlüsselung ist folgendes Verfahren denkbar: um 0/1-Folgen geheim zu übertragen, einigt man sich zuerst mit dem Empfänger über eine (zufällige) 0/1-Folge Z, die man z. B. durch Münzwurf oder einen Zufallszahlengenerator bestimmt. Um eine Nachricht M zu senden, addiert man zu M bitweise Z, und sendet $M + Z$. Der Empfänger dekodiert das zu $(M + Z) + Z = M$. Ein solches Verfahren hat aber den Nachteil, dass sich Sender und Empfänger über den Schlüssel Z einigen müssen.

Das folgende RSA−Verschlüsselungsverfahren benötigt den vorherigen, geheimen Austausch von Schlüsseln *nicht*. Es wurde von R. Rivest, A. Shamir und L. Adleman entwickelt (cf. [**Rivest et al., 1978**]) und funktioniert so:

Jeder, der von anderen verschlüsselte Informationen empfangen will, gibt in einem veröffentlichten *Verzeichnis*, also in einer Art Telefonbuch, seinen Chiffrierschlüssel E (seine Verschlüsselungsfunktion E) bekannt, hält aber seinen Dechiffrierschlüssel D (seine Entschlüsselungsfunktion D) geheim. Will A an B eine Nachricht übermitteln, so chiffriert er sie mit dem Chiffrierschlüssel E_B von B, den A dem öffentlich zugänglichen Verzeichnis entnimmt. B dechiffriert anschließend die erhaltene Nachricht mit seinem Dechiffrierschüssel D_B.

Es erscheint zunächst so, als ob durch E_B jedem automatisch auch D_B, die "inverse Funktion" zu E_B, bekannt ist. Rivest, Shamir und Adleman haben aber eine Klasse von Funktionen gefunden, für die man E_B sehr wohl bekannt geben kann, ohne dabei "automatisch" D_B zu verraten. Solche Funktionen heißen auch "trapdoor-functions".



Quelle: Pilz G., Lidl R., *Applied Abstract Algebra*, [**Lidl and Pilz, 1998**].

Zusammenfassend suchen wir also eine Verschlüsselungsfunktion E (encipher) und eine Entschlüsselungsfunktion D, sodass gilt

(1) $D(E(M)) = M$, M ist die Nachricht (message).
(2) $E(M)$ und $D(E(M))$ können effizient berechnet werden.
(3) E kann veröffentlicht werden, ohne dass man daraus D rekonstruieren kann.
(4) Manchmal fordert man auch $E(D(M)) = M$.

Und dazu brauchen wir etwas Zahlentheorie:

Satz 1.39. *Seien p, q Primzahlen, $p \neq q$ und seien $a, s \in \mathbb{Z}$. Dann gilt:*

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

Beweis:

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

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

  Damit gilt insgesamt:

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

- *2. Fall:* ggT $(a, pq) = p$*:* Da der 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 ja, 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:* ggT $(a, pq) = q$*:* Beweis genauso wie im 2. Fall.
- *4. Fall:* ggT $(a, pq) = p \cdot q$*:* Dann ist zu zeigen, dass $0 \equiv 0 \pmod{pq}$. □

Übungsaufgaben 1.40.

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

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

Versuchen wir nun, D und E zu finden: Seien p, q Primzahlen, und sei $k \in \mathbb{Z}$ mit ggT $(k, (p-1)\cdot(q-1)) = 1$. Dann definieren wir E durch

$$\begin{aligned} E : \mathbb{Z}_{pq} &\to \mathbb{Z}_{pq} \\ x &\mapsto x^k. \end{aligned}$$

Wir bestimmen ein $t \in \mathbb{Z}$, sodass

$$k \cdot t \equiv 1 \,(\text{mod } \; (p-1) \cdot (q-1))\,,$$

und definieren D durch

$$\begin{aligned} D : \mathbb{Z}_{pq} &\to \mathbb{Z}_{pq} \\ x &\mapsto x^t. \end{aligned}$$

Nun ist D zu E invers, d.h. $D\left(E\left(x\right)\right) = \left(x^k\right)^t = x^{1+s(p-1)\cdot(q-1)} = x$.

Der Entwerfer des Systems gibt $n = p \cdot q$ und k öffentlich bekannt. Die für das Entschlüsseln notwendige Zahl t wird geheimgehalten und nicht weitergegeben. Ein unberechtigter Entschlüsseler wird versuchen, aus $p \cdot q$ und k das geheime t zu rekonstruieren. Zur Bestimmung des geheimen Decodierschlüssels t müßte er folgende Kongruenz lösen:

$$k \cdot t \equiv 1 \;\; (\text{mod } \; (p-1) \cdot (q-1))\,.$$

Das erfordert jedoch nach derzeitigem Wissensstand die Kenntnis der Primfaktorenzerlegung $n = p \cdot q$ von n. Wenn man n aber groß genug wählt (150 - 200 Dezimalstellen), dann kann man n nicht (schnell genug) faktorisieren.

Fassen wir zunächst nochmals zusammen, was jeder der Beteiligten eines **RSA-Kryptosystems** zu tun hat:

- Aufgaben für den, der das System entwirft ("key source"):
  (1) Wähle zwei Primzahlen p, q mit $p \cdot q \geq 10^{130}$,, die ungefähr gleich groß sind, und berechne $n := pq$.
  (2) Wähle $k \in \mathbb{Z}$ so, dass ggT $(k, (p-1) \cdot (q-1)) = 1$.
  (3) Berechne $t \in \mathbb{Z}$, sodass $k \cdot t \equiv 1 \;\; (\text{mod } \; (p-1) \cdot (q-1))\,.$
  (4) Information an den Verschlüsseler: $(n; k)\,.$
  (5) Information an den Entschlüsseler: $(n; t)\,.$
- Aufgaben für den Verschlüsseler beim Verschlüsseln der Nachricht $M \in \mathbb{Z}_n$.
  (1) Berechne $E\left(M\right) := M^k$ (Rechnung in $\mathbb{Z}_n$).
  (2) Sende $C := E\left(M\right)$.
- Aufgaben für den Entschlüssler beim Entschlüsseln des empfangenen Kryptogramms C.
  (1) $D\left(C\right) = C^t$ (in $\mathbb{Z}_n$).

Die wichtigsten Anwendungen des RSA-Verfahrens sind **die Übertragung geheimer Daten** und **digitale Unterschriften**, durch die gesichert wird, dass eine Nachricht wirklich authentisch ist, also vom angegebenen Absender stammt.

Stellen wir uns vor, der Absender A besitzt den öffentlich bekannten Chiffrierschlüssel E_A und den geheimen Dechiffrierschlüssel D_A, und der Empfänger B besitzt die Schlüssel E_B und D_B, die wie oben ausgeführt berechnet werden können. Nun schickt A an B eine Nachricht M in der Form $(E_B(D_A(M)))$. A wendet also

auf M zunächst seinen geheimen Dechiffrierschlüssel D_A und dann darauf den öffentlich bekannten Schlüssel E_B von B an. Dabei hat die Anwendung von D_A die Funktion einer Unterschrift; denn nur A kennt D_A, und daher kann nur A den so verschlüsselten Text gesandt haben. B dechiffriert die Nachricht anschließend durch:

$$E_A(D_B(E_B(D_A(M)))) = M.$$

Die übermittelte Nachricht $E_B(D_A(M))$ ist höchstens für B lesbar, da nur B den Schlüssel D_B kennt und somit nur B den Text $D_A(M)$ herstellen kann. Da E_A für B jedoch bekannt ist, kann B jetzt $E_A(D_A(M))$ bilden und so die ursprüngliche Nachricht M erhalten.

6. Die Multiplikativität der Eulerschen φ-Funktion

Wir beweisen nun noch einen wichtigen Satz der elementaren Zahlentheorie.

Satz 1.41 (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 1.42. *Falls R_1 und R_2 Ringe mit Eins sind, dann ist*

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

wieder ein Ring mit Eins. Dabei sind die Verknüpfungen auf $R_1 \times R_2$ definiert durch

- $\begin{pmatrix} r_1 \\ r_2 \end{pmatrix} +_{R_1 \times R_2} \begin{pmatrix} s_1 \\ s_2 \end{pmatrix} := \begin{pmatrix} r_1 +_{R_1} s_1 \\ r_2 +_{R_2} s_2 \end{pmatrix}$
- $\begin{pmatrix} r_1 \\ r_2 \end{pmatrix} \cdot_{R_1 \times R_2} \begin{pmatrix} s_1 \\ s_2 \end{pmatrix} := \begin{pmatrix} r_1 \cdot_{R_1} s_1 \\ r_2 \cdot_{R_2} s_2 \end{pmatrix}$
- $-_{R_1 \times R_2} \begin{pmatrix} r_1 \\ r_2 \end{pmatrix} := \begin{pmatrix} -_{R_1} r_1 \\ -_{R_2} r_2 \end{pmatrix}$
- $0_{R_1 \times R_2} := \begin{pmatrix} 0_{R_1} \\ 0_{R_2} \end{pmatrix}$
- $1_{R_1 \times R_2} := \begin{pmatrix} 1_{R_1} \\ 1_{R_2} \end{pmatrix}$.

$R_1 \times R_2$ mit diesen Operationen erfüllt auch 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 1.43. R, S seien Ringe mit Eins. Die Abbildung $\varphi : R \to S$ heißt Ring mit Eins-Homomorphismus: $\Leftrightarrow$

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

Definition 1.44. Ein Homomorphismus φ heißt:

- *Epimorphismus* $:\Leftrightarrow \varphi$ ist surjektiv;
- *Monomorphismus* $:\Leftrightarrow \varphi$ ist injektiv;
- *Isomorphismus* $:\Leftrightarrow \varphi$ ist bijektiv.

Beispiel: Wollen wir uns dies zunächst an zwei Beispielen veranschaulichen.

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

Definition 1.45. Sei R ein Ring mit Eins. Dann heißt $r \in R$ *invertierbar*, falls es ein $y_r \in R$ gibt, sodass

$$r \cdot y_r = 1_R \text{ und } y_r \cdot r = 1_R.$$

Satz 1.46. *Seien $n, m \in \mathbb{N}$ mit* ggT $(n, m) = 1$. *Dann ist die Abbildung*

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

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 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. $\square$

Wenn der 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 $\varphi-$Funktion, also Satz 1.41, herleiten.

Beweis von Satz 1.41:

(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 ist

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

für $n,m\in\mathbb{N}$ mit ggT $(n,m)=1$ bewiesen. $\square$

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. Dazu noch ein Beispiel:

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

Übungsaufgaben 1.47.

(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) [**Lidl and Pilz, 1998**, 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 2

Gruppen

1. Motivation

Im 19.Jahrhundert suchte man Lösungsformeln für Gleichungen der Form

$$x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0 = 0$$

mit $a_1, a_2, \ldots, a_{n-1} \in \mathbb{Q}$. Für eine quadratische Gleichung der Form $x^2+px+q = 0$ erhalten wir die Lösungen durch $x_{1,2} = -\frac{p}{2} \pm \sqrt{\left(\frac{p}{2}\right)^2 - q}$. Gleichungen dritten Grades der Form $x^3 + ax^2 + bx + c = 0$ kann man mit den Cardano'schen Lösungsformeln lösen; die ersten Lösungsformeln stammen von Tartaglia und Scipione del Ferro (ca. 1515). Für diese Lösungsformeln braucht man die komplexen Zahlen, auch wenn alle Lösungen reell sind. Luigi Ferrari (ca. 1545) fand Lösungsformeln für Gleichungen vom Grad 4. In allen diesen Formeln wird ein Verfahren angeben, die Lösung aus den Koeffizienten durch Verwendung der 4 Grundrechnungsarten und dem Ziehen von Quadratwurzeln und n-ten Wurzeln ($n \in \mathbb{N}$) zu bestimmen. Die Suche nach einer Auflösungsformel für Gleichungen fünften Grades blieb erfolglos. Gegen Ende des 18. und Anfang des 19. Jahrhunderts gelang es Ruffini, Abel und Galois, zu beweisen, dass es Gleichungen 5. Grades gibt, deren Lösungen sich nicht durch die vier Grundrechnungsarten und Wurzelziehen finden lassen (cf. [**Rotman, 1998, Robinson, 2003**]). Zum Beweis dieses Resultats wurden Vertauschungen der Wurzeln eines Polynoms studiert.

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

Eine Gruppe ist eine algebraische Struktur

$$(G, \cdot, i, \mathsf{e}),$$

wobei $\cdot$ eine zweistellige Verknüpfung ist, i einstellig, und e ein Element von G ist.

Definition 2.1. Eine Menge G zusammen mit den Operationen $\cdot : G \times G \to G$, $i : G \to G$ und einem Element $\mathsf{e} \in G$ ist genau dann eine *Gruppe*, wenn 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: 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.

In jeder Gruppe gelten folgende Gleichungen.

Satz 2.2. *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 $z \in G$ beliebig, aber fest. 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 $z \in G$ beliebig, aber fest, 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 2.3.

(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 2.2, 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 2.2 automatisch beweisen lassen kann; die theoretische Grundlage dafür ist die Methode von Knuth und Bendix [**Knuth and Bendix, 1970**], die z. B. in [**Buchberger, 1982**] 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:

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

3. Beispiele für Gruppen

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

3.1. Matrixgruppen.

(1) Sei $\mathrm{GL}\,(n,p)$ die Menge aller regulären $n \times n$-Matrizen über $\mathbb{Z}_p$.

$$\left(\mathrm{GL}(n,p), \cdot, {}^{-1}, \mathrm{E}^{(n)}\right)$$

ist eine Gruppe.

(2) Sei $\mathrm{SL}\,(n,p) := \{A \in GL\,(n,p) \mid \det A = 1\}$.

$$\left(\mathrm{SL}(n,p), \cdot^{-1}, \mathrm{E}^{(n)}\right)$$

ist eine Gruppe.

3.2. Restklassen von $\mathbb{Z}$ mit Multiplikation.

(1) Sei $n \geq 2$. Dann ist $(\mathbb{Z}_n, \cdot)$ keine Gruppe.
(2) Sei $n \geq 2$. $(\mathbb{Z}_n \setminus \{[0]_n\}, \cdot)$ 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.

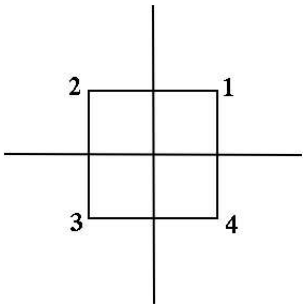
3.3. Zyklische Gruppen. Eine Gruppe $(G, \cdot)$ heißt *zyklisch*, wenn es ein $g \in G$ gibt, sodass

$$G = \{g^n \mid n \in \mathbb{N}\} \cup \{(g^{-1})^n \mid n \in \mathbb{N}\} \cup \{1_G\}.$$

(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.

3.4. 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*).



Es kann höchstens 8 solche linearen Abbildungen geben, denn 1 kann auf höchstens vier Ecken landen, 2 muss zu 1 benachbart bleiben (höchstens zwei Möglichkeiten), 3 muss die andere zu 1 benachbarte Stelle einnehmen und ist also, ebenso wie 4, durch die Lage von 1 und 2 bereits fixiert. Es gibt also höchstens $4 \cdot 2 \cdot 1 \cdot 1$ Symmetrieabbildungen.

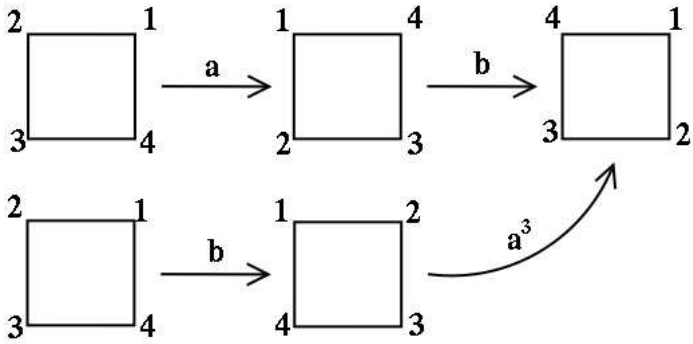
Die Hintereinanderausführung zweier Symmetrieabbildungen ist wieder eine Symmetrieabbildung. Die identische Abbildung ist eine Symmetrieabbildung, und zu jeder Symmetrieabbildung d ist die inverse Abbildung wieder eine Symmetrieabbildung. Die Menge aller Symmetrieabbildungen, mit der Hintereinanderausführung als zweistelliger Operation, ist eine Gruppe.

Übungsaufgaben 2.4.

(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) $baba = a^3bba = a^31a = a^4 = 1$.

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:

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

Übungsaufgaben 2.5.

(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 $\{(\mathrm{Re}(z), \mathrm{Im}(z)) \mid z \in \mathbb{C},\ z^6 = 1\}$. Bestimmen Sie alle Deckabbildungen, die dieses Sechseck auf sich selbst abbilden.
(3) Wir betrachten in $\mathbb{R}^2$ das Sechseck mit den Eckpunkten $\{(\mathrm{Re}(z), \mathrm{Im}(z)) \mid z \in \mathbb{C},\ z^6 = 1\}$. Wie können Sie die Gruppe aller Symmetrieoperationen dieses Sechseckes durch Worte in a und b angeben? Was sind die "Rechenregeln"? (Diese Rechenregeln bezeichnet man auch als *definierende Relationen.*)
(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 $w_1 * w_2 = w_2 * w_1$.

3.5. 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
```

Eine Gruppentafel sieht also so aus:

	g_j
g_i	$g_i \circ g_j$

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

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

Wir können jedes Element von S_3 so anschreiben:

$$\begin{pmatrix} 1 & 2 & 3 \\ f(1) & f(2) & f(3) \end{pmatrix}.$$

Damit können wir

$$S_3$$

schreiben als:

$$S_3 = \left\{ \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix} \right\}.$$

Kürzer ist die *Zyklenschreibweise*:

$$S_3 = \left\{ (), \begin{pmatrix} 1 & 2 \end{pmatrix}, \begin{pmatrix} 1 & 3 \end{pmatrix}, \begin{pmatrix} 2 & 3 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \end{pmatrix}, \begin{pmatrix} 1 & 3 & 2 \end{pmatrix} \right\}.$$

Wie die Zyklenschreibweise Permutationen kodiert, geht aus folgendem Beispiel hervor.

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

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

In S_3 gibt es x, y, sodass $x \cdot y \neq y \cdot x$.

Definition 2.6. Eine Gruppe $(G, \cdot, ^{-1}, 1)$ ist *abelsch*, wenn für alle $x, y \in G$ die Gleichung $x \cdot y = y \cdot x$ gilt.

Die Gruppe S_3 ist nicht abelsch:

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

Wir sehen also: wenn $n \geq 3$, dann ist S_n nicht abelsch.

Übungsaufgaben 2.7.

(1) Geben Sie Beispiele für Gruppen an, die bis jetzt noch nicht erwähnt wurden.
(2) 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 2.8. Sei $(G, \cdot, ^{-1}, 1_G)$ eine Gruppe und sei $H \subseteq G$. H heißt *Trägermenge einer Untergruppe* von G :$\Leftrightarrow$

(1) $1_G \in H$
(2) $\forall h_1, h_2 \in H : h_1 \cdot h_2 \in H$ und $h_1^{-1} \in H$.

$(H, \cdot\,|_{H\times H}, ^{-1}|_H, 1_G)$ ist dann eine Untergruppe von G.

Übungsaufgaben 2.9.

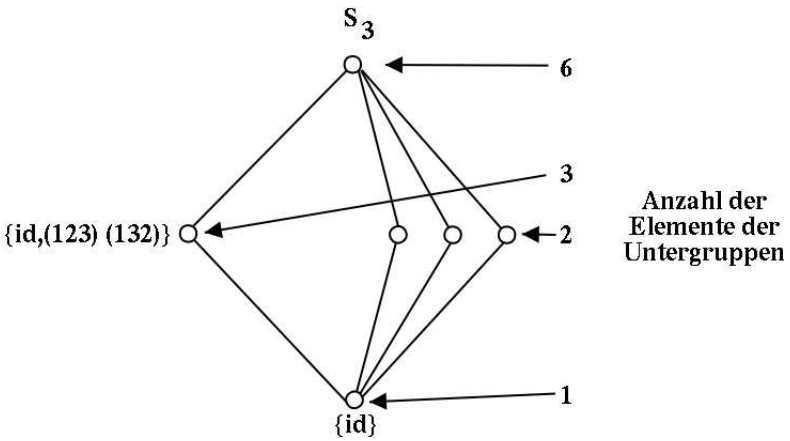
(1) Sei $\big(G, \cdot, ^{-1}, 1\big)$ eine Gruppe und sei H eine nichtleere Teilmenge von G, sodass für alle $h_1, h_2 \in H$ auch $h_1^{-1} \cdot h_2$ in H liegt. Zeigen Sie, dass H dann Trägermenge einer Untergruppe von $\big(G, \cdot, ^{-1}, 1\big)$ ist.
(2) Sei $\big(G, \cdot, ^{-1}, 1\big)$ eine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

Wir bestimmen die Trägermengen von Untergruppen der Gruppe $\mathbf{S}_3$ 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.

Die Trägermengen der Untergruppen kann man durch $\subseteq$ ordnen, und wir erhalten folgendes Hasse-Diagramm.



Übungsaufgaben 2.10.

(1) Welche der folgenden Mengen sind Trägermengen von Untergruppen der Gruppe $\mathbf{S}_n$? ($n \geq 2$).
  (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 2.11. 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) $\varphi\left(g_1^{-1}\right) = (\varphi(g_1))^{-1_H}$,
(3) $\varphi(1) = 1_H$.

Beispiele:

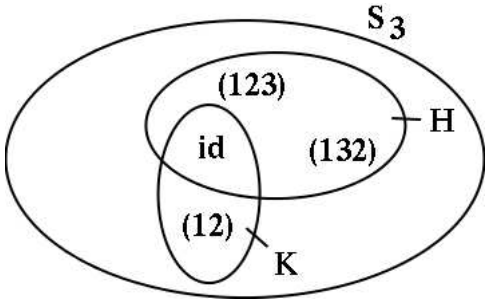
(1) Sei $G := (\mathbb{R}^+, \cdot)$ und sei $H := (\mathbb{R}, +)$. Dann ist $\varphi : \mathbb{R} \to \mathbb{R}^+, x \mapsto \ln(x)$ ein Homomorphismus.
(2) Die Abbildung
$$\begin{aligned} \varphi : \quad & \mathbb{Z} \to \mathbb{Z}_n \\ & x \mapsto [x]_n \end{aligned}$$
ist ein Homomorphismus von $(\mathbb{Z}, +)$ nach $(\mathbb{Z}_n, +)$.

Definition 2.12. Homomorphismen, die

- *injektiv* sind, heißen *Monomorphismen*
- *surjektiv* sind, heißen *Epimorphismen*
- *bijektiv* sind, heißen *Isomorphismen*
- Homomorphismen von $G \to G$ heißen *Endomorphismen.*

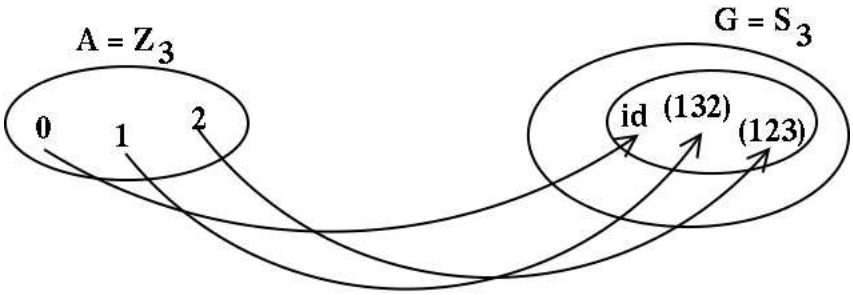
Bijektive Endomorphismen heißen *Automorphismen.*

Beispiel: Seien **H** und **K** die Untergruppen von S_3 mit den Trägermengen



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

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



Übungsaufgaben 2.13.

(1) Wir haben einen Gruppenhomomorphismus als eine Abbildung $\varphi : \mathbf{G} \to \mathbf{H}$ definiert, die folgende drei Bedingungen erfüllt:
   (a) $\varphi(g_1 \cdot_{\mathbf{G}} g_2) = \varphi(g_1) \cdot_{\mathbf{H}} \varphi(g_2)$ für alle $g_1, g_2 \in G$;
   (b) $\varphi(g_1{}_{\mathbf{G}}^{-1}) = (\varphi(g_1))_{\mathbf{H}}^{-1}$ für alle $g_1 \in G$;
   (c) $\varphi(1_{\mathbf{G}}) = 1_{\mathbf{H}}$.
   Seien **G** und **H** Gruppen, und sei ψ eine Abbildung, die die erste Bedingung
   $$\psi(g_1 \cdot_{\mathbf{G}} g_2) = \psi(g_1) \cdot_{\mathbf{H}} \psi(g_2) \text{ für alle } g_1, g_2 \in G$$
   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 $\mathbf{G}$ und $\mathbf{H}$ 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 $\mathbf{S}_m$ 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 $\mathbf{G}$ 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:
$\mathbf{H} := (\mathcal{P}(X), \Delta)$ ist eine Gruppe. (Finden Sie das Inverse zu $Y \subseteq X$, und das Einselement.)
Geben Sie einen Gruppenisomorphismus von $\mathbf{H}$ nach $\mathbf{G}$ an!

Definition 2.14. Die Gruppe A heißt *einbettbar* in G (geschrieben als $A \hookrightarrow G$), wenn es einen Monomorphismus von A nach G gibt.

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

Also gilt: einbettbar in ... $\Leftrightarrow$ isomorph zu einer Untergruppe von ....

Beispiel:

(1) Ist S_3 einbettbar in S_4 ? Wir betrachten folgende Abbildung:

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

wobei $\varphi(f)$ definiert ist durch

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

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

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

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

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 sagt, dass jede Gruppe in irgendeine Gruppe S_X einbettbar ist; anders gesagt: jede Gruppe ist isomorph zu irgendeiner Untergruppe irgendeiner S_X.

Satz 2.15 (Satz von Cayley). *Sei* $\mathbf{G} = (G, \cdot, ^{-1}, 1)$ *eine Gruppe. Dann gilt:* $\mathbf{G}$ *ist einbettbar in* $(S_G, \circ, ^{-1}, id_G)$.

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

Beweis: Sei

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

wobei

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

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

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

5. Sätze von Lagrange und Fermat

Satz 2.16. *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) "$\Rightarrow$": 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 $x \in y \cdot H$. "$\Leftarrow$": 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

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

bijektiv.

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

Satz 2.17 (Satz von Lagrange). *Sei H Trägermenge einer Untergruppe von $(G, \cdot)$, wobei G endlich ist. 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 2.18. 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 $(Z, +)$.

Definition 2.19. 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: Wir berechnen die Ordnung zweier Elemente der Gruppe $(\mathbb{Z}_5 \setminus \{0\}, \cdot)$. Es gilt $\operatorname{ord}([2]_5) = |\langle g \rangle| = |\{2, 4, 3, 1\}| = 4$, und $\operatorname{ord}([4]_5) = |\{4, 1\}| = 2$.

Satz 2.20 (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: Die Gruppe $(\langle g \rangle, \cdot)$ hat $\operatorname{ord}(g)$ Elemente. Nach dem Satz von Lagrange teilt also $\operatorname{ord}(g)$ die Zahl $|G|$. Die zweite Eigenschaft zeigen wir so: 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

Wir lösen folgendes Problem: 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 2.21 (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:

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

Jede Symmetrieoperation des Quadrats ist eine Permutation der vier Eckpunkte. Alle Symmetrieoperationen erhalten wir aus folgendem Dialog mit GAP [**GAP, 1999**]. 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:

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

wobei

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

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

Definition 2.22. 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 2.23. *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 2.24 (Frobenius-Burnside-Lemma). *Sei G eine 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 $\mathrm{Fix}\,(g) = \{\xi \in X \mid g * \xi = \xi\}$

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: 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 ist gegeben durch

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

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

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

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
$3 \times (135)\,(246)$	2
$4 \times (14)\,(25)\,(36)$	0

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

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 des Satzes von Frobenius-Burnside: 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 $\mathrm{stab}_G(\xi) = G_\xi$. Wir zeigen zunächst, dass für alle $\xi \in X$ gilt:

$$|G * \xi| = |\{g * \xi \mid g \in G\}| = \text{ Größe des Orbits von } \xi = \frac{|G|}{|\mathrm{stab}_G\, \xi|} \tag{6.1}$$

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:

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

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 2.25.

(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 [**GAP, 1999**]):

```
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 2.26. 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* auf $(G, \circ)$.

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 2.27.

(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 $a^{-1} \sim b^{-1}$.

Sei $(G, \circ)$ eine Gruppe und sei $\sim$ eine Kongruenzrelation Auf der Menge $G/_\sim$ aller Klassen modulo $\sim$ definieren wir folgende Verknüpfung $\circledcirc$.

$$g_1/_\sim \circledcirc g_2/_\sim := (g_1 \circ g_2)/_\sim \quad \text{für alle } g_1, g_2 \in G.$$

Wir müssen nachweisen, dass $\circledcirc$ wohldefiniert ist. Dazu ist zu zeigen, dass $g \sim g'$ und $h \sim h'$ impliziert, dass $g \circ h \sim g' \circ h'$ gilt. Das gilt, weil $\sim$ eine Kongruenzrelation ist.

Wir beschreiben jetzt alle Kongruenzrelationen auf einer Gruppe.

SATZ 2.28. *Sei $(G, \circ)$ 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 eine Untergruppe $(N, \circ)$ von $(G, \circ)$, sodass gilt:*
  (a) $\forall g \in G \, \forall n \in N \; : \; g^{-1} \circ n \circ g \in N$ *(Normalteilereigenschaft)*
  (b) $\forall x, y \in G \; : \; x \sim y \Leftrightarrow x^{-1} \circ y \in N$

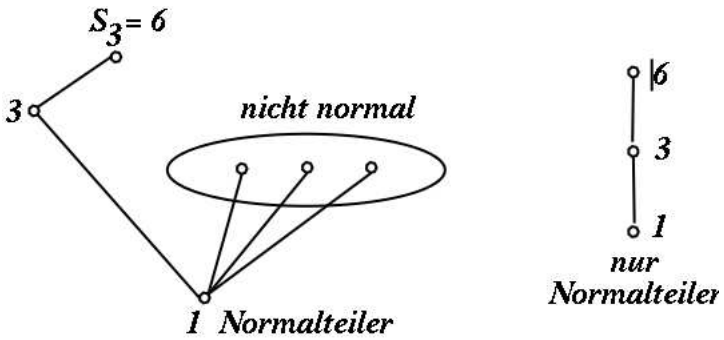
Wenn N die Trägermenge einer Untergruppe von $(G, \circ)$ ist, die die Eigenschaft

$$\text{für alle } g \in G,\, n \in N \; : \; g^{-1} \circ n \circ g \in N$$

erfüllt, dann heißt N *Normalteiler* von $(G, \circ)$.

Beispiele:

- 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.

Beweis von Satz 2.28: 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

$$x \sim y \Leftrightarrow x^{-1} \cdot y \in N \tag{7.1}$$

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

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

Nun zeigen wir, dass die Eigenschaft (7.1) ebenfalls erfüllt ist: wir zeigen zuerst die Implikation "$\Rightarrow$". Wir fixieren $x, y \in G$ mit $x \sim y$. Dann gilt auch $x^{-1} \circ x \sim x^{-1} \circ y$, und somit liegt $x^{-1} \circ y$ in N. Für "$\Leftarrow$" fixieren wir $x, y \in G$ mit $x^{-1} \circ y \in N$. Es gilt dann $x^{-1} \circ y \sim 1_G$, und daher auch $x \circ x^{-1} \circ y \sim x \circ 1_G$, und somit $y \sim x$.

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

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

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 $x_1 \circ y_1 \sim x_2 \circ y_2$, d.h.,

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

also

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

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

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

Der letzte Ausdruck liegt in N.

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

Satz 2.29. *Seien $(G, \cdot)$ und $(H, \cdot)$ Gruppen und sei $\varphi : G \to H$ ein Homomorphismus. Dann ist $\ker \varphi = \{x \mid \varphi(x) = 1_H\}$ ein Normalteiler von G. Außerdem gilt für alle $x, y \in G$, dass $x^{-1} \cdot y$ genau dann in $\ker \varphi$ liegt, falls $\varphi(x) = \varphi(y)$.*

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

Satz 2.30. *Seien $(G, \cdot)$ und $(H, \cdot)$ Gruppen und sei $\varphi : G \to H$ ein Homomorphismus. Dann ist die Gruppe $(\operatorname{im} \varphi, \cdot)$ isomorph zur Faktorgruppe $G/\ker \varphi$.*

Satz 2.31 (Satz von Sylow). *Sei p eine Primzahl, sei $a \in N$, und sei $m \in \mathbb{N}$ so, dass* $\operatorname{ggT}(p, m) = 1$. *Sei G eine Gruppe mit $p^a \cdot m$ Elementen. Dann hat G eine Untergruppe mit p^a Elementen.*

Beispiel: Jede 12-elementige Gruppe hat eine Untergruppe mit 4 Elementen.

KAPITEL 3

Ausgewählte Kapitel der Diskreten Mathematik

1. Graphen

1.1. Definition eines Graphen.

Definition 3.1. 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 xy eine Kante des Graphen ist.

Ein Graph heißt *einfach*, wenn zwischen zwei Knoten immer höchstens eine Kante verläuft. Unsere Definition eines Graphen lässt keine Schleifen, also Kanten mit dem gleichen Anfangs- und Endpunkt zu.

Definition 3.2. 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 3.3.

(1) Sei (V, E, I) ein Graph. Zeigen Sie:
$$|I| = \sum_{v \in V} \mathrm{Grad}\,(v).$$
(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 $\sum_{v \in V} \mathrm{Grad}\,(v)$ 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 $\sum_{v \in V} \mathrm{Grad}\,(v)$ das Doppelte der Kantenanzahl ist.

1.2. Eulersche Wege.

Definition 3.4. Sei $k \in \mathbb{N}_0$. Eine Folge $(x_0, e_1, x_1, e_2, x_2, \ldots, e_k, x_k)$ 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 $x_k = x_0$.

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 3.5. 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 3.6. *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 sei v ein Knoten. Die Folge (v) ist ein Eulerscher Kreis der Länge 0. Wenn der Graph eine Kante e_1 von x_0 nach x_1 enthält, so

verlängern wir 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 $x_0 e_1 x_1 \dots e_k x_k$ mit $k \in \mathbb{N}$ gefunden. Wir bilden nun einen neuen Graphen G', indem wir aus G die Kanten $e_1, \dots, e_k$ 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. □

1.3. Planare Graphen.

Definition 3.7. Ein Graph ist *planar*, wenn er sich in $\mathbb{R}^2$ "überschneidungsfrei zeichnen lässt".

Definition 3.8. 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 3.9 (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 3.10. *Sei G ein einfacher planarer Graph. Dann hat G einen Knoten, dessen Grad höchstens 5 ist.*

Beweis: ([**Aigner and Ziegler, 1998**]) Sei G ein einfacher ebener Graph, und seien v, e, f die Anzahl der Knoten, Kanten, Flächen. Wir nehmen $v \geq 3$ an. Wir bilden die Menge

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

Für jede Fläche a definieren wir die Menge seiner 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 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 $v - e + f \leq 0$ im Widerspruch zur Eulerschen Flächenformel. □

Übungsaufgaben 3.11.

(1) [**Aigner and Ziegler, 1998**, p.59] Sei G ein einfacher planarer Graph mit $v \geq 3$ Knoten und e Kanten. Dann gilt $e \leq 3v - 6$.
(2) [**Aigner and Ziegler, 1998**, 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 3.12. *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*).

2. Der Satz von Ramsey

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. Eine *Partition* einer Menge U in t Teilmengen ist (in diesem Kapitel) eine Folge $(A_1, A_2, \ldots, A_t)$ von Teilmengen von U, sodass $A_1 \cup A_2 \cup \cdots \cup A_t = U$ ist, und für alle $i, j \in \{1, 2, \ldots, t\}$ mit $i \neq j$ die Menge $A_i \cap A_j$ leer ist.

Satz 3.13. *Seien $p, t, n \in \mathbb{N}$. Dann gibt es eine Zahl $N \in \mathbb{N}$, sodass folgendes erfüllt ist:*

Für jede Menge X mit $|X| \geq N$ und jede Partition von $\binom{X}{p}$ in t Teilmengen der Form

$$\binom{X}{p} = A_1 \cup A_2 \cup \cdots \cup A_t$$

gibt es eine n-elementige Teilmenge Y von X und ein $j \in \{1, 2, \ldots, t\}$, sodass $\binom{Y}{p} \subseteq A_j$. (Das heißt, dass alle alle p-elementigen Teilmengen von Y in der gleichen Klasse der Partition sind).

Äquivalent ist:

Satz 3.14. *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.

Das kleinste N, für das die Aussage erfüllt ist, bezeichnen wir mit $r(p, t, n)$ (Ramsey-Zahl).

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 3.15.

(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 3.16.

(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 3.17. *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) $\Rightarrow$ (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. $\square$

Beweis des Satzes von Ramsey: Wir definieren ein Prädikat

$$G(p,t,n)$$

dadurch, dass $G(p,t,n)$ wahr ist, wenn der Satz von Ramsey für p,t,n gilt, das heißt, wenn es ein N gibt, sodass für alle N-elementigen Mengen und alle Färbungen der p-elementigen Teilmengen .... Wir wissen, dass z.B. $G(2,2,3)$ wahr ist.

Wir beweisen jetzt, dass $G(p,t,n)$ für alle $p,t,n \in \mathbb{N}$ gilt, durch Induktion nach p.

- $p = 1$: Wir fixieren $t, n \in \mathbb{N}$. Dann leistet $N := t(n-1)+1$ das Gewünschte.
- Wir fixieren $p \geq 2$ und $t \in \mathbb{N}$. Wir zeigen nun, dass die Eigenschaft (2) aus Lemma 3.17 gilt. Wir zeigen diese Eigenschaft durch Induktion nach n.

– Für $n \leq p$ leistet $M := p$ das Gewünschte.
– Wir fixieren $n > p$. Mit der Induktionsvoraussetzung produzieren wir ein M für $n-1$. Wir behaupten nun, dass

$$M' := 1 + r(p-1, t, M)$$

das Gewünschte leistet. Wir fixieren dazu eine Färbung der p-elementigen Teilmengen von $X = \{1, 2, \ldots, M'\}$ mit t Farben.
Wir geben nun jeder $p-1$-elementigen Teilmenge Z von $X \setminus \{1\}$ die Farbe von $\{1\} \cup Z$. Wir finden dann (wegen der Induktionsvoraussetzung der Induktion nach p) eine M-elementige Teilmenge A von $X \setminus \{1\}$, sodass alle $p-1$-elementigen Teilmengen von A die gleiche Farbe haben.
Wir wählen nun nach Induktionsvoraussetzung (der Induktion nach n) eine $(n-1)$-elementige Teilmenge B von A, sodass alle p-elementigen Teilmengen von B mit dem gleichen minimalen Element die gleiche Farbe haben.
Wir behaupten, dass $B \cup \{1\}$ das Gewünschte leistet. Wir wählen dazu zwei p-elementige Teilmengen P_1, P_2 von $B \cup \{1\}$ mit dem gleichen minimalen Element. Ist dieses Element 1, so haben P_1, P_2 die gleiche Farbe, da alle p-elementigen Teilmengen von $A \cup \{1\}$, die 1 enthalten, die gleiche Farbe haben.
Ist dieses Element nicht 1, dann sind P_1, P_2 beide p-elementige Teilmengen von B und haben daher die gleiche Farbe. □

Satz 3.18 (Erdős-Szekeres). *Sei $n \in \mathbb{N}$. 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.*

Hinweis zum Beweis: Für $n = 4$ funktioniert $N := 5$. Für $n > 4$ kann man $N := r(4, 2, n)$ wählen.

Satz 3.19. *Sei $t \in \mathbb{N}$. Dann gibt es ein N, sodass es für jede Gruppe $\mathbf{G}$ mit mehr als N Elementen 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.*

Hinweis zum Beweis: $N := r(2, t, 4) + 1$. Sei $G = \{1, x_1, \ldots, x_N\}$ Wir färben die Menge $\{x_i, x_j\}$ mit der Farbe von $x_{\min(i,j)}^{-1} \cdot x_{\max(i,j)}$. □

Übungsaufgaben 3.20.

(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) (Dixons 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 4

Polynome und Körper

1. Körper

Definition 4.1. Ein kommutativer Ring mit Eins $\mathbf{R} = (R, +, -, \cdot, 0, 1)$ 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 4.2.

(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 4.3. Sei $\mathbf{E} = (E, +, -, \cdot, 0, 1)$ ein Körper, und sei $K \subseteq E$. Die Menge K ist dann *Trägermenge eines Unterkörpers* von $\mathbf{E}$, 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 $x \in K \setminus \{0\}$ gilt $x^{-1} \in K$.

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

Übungsaufgaben 4.4.

(1) Zeigen Sie: Der Durchschnitt beliebig vieler Trägermengen von Unterkörpern eines Körpers ist wieder Trägermenge eines Unterkörpers.
(2) Sei $\mathbf{E}$ 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 $\mathbf{E}$ ist.

2. Polynome

Definition 4.5. Sei $\mathbf{K}$ kommutativer Ring mit Eins. Dann ist $K[t] := \{a \in K^{\mathbb{N}_0} \mid \exists i \in \mathbb{N}\ \forall j \in \mathbb{N} : j \geq i \Rightarrow a_j = 0\}$.

Definition 4.6. Addition und Multiplikation auf $K[t]$.

Definition 4.7. Sei $f \in K[t]$. $\deg f := \ldots$, $\deg 0 := -1$.

Mit $t = (0, 1, 0, \ldots)$ gilt $a = (a_0, a_1, \ldots) = \sum_{i=0}^{\deg a} a_i t^i$.

Definition 4.8. Sei $\mathbf{K}$ Körper, und seien $f, g \in K[t]$.

(1) f *teilt* g, wenn es $q \in K[t]$ gibt, sodass $g = q \cdot f$.
(2) f ist *invertierbar*, wenn $\deg f = 0$.
(3) f ist *irreduzibel über* $\mathbf{K}$ (ein irreduzibles Polynom in $K[t]$), wenn $\deg f \geq 1$ und für alle $a, b \in K[t]$ mit $a \cdot b = f$ entweder a oder b Grad 0 hat.
(4) f ist *normiert*, wenn es führenden Koeffizienten 1 hat.

Satz 4.1. *Sei* $\mathbf{K}$ *Körper, und seien* $f, g \in K[t]$. *Wenn* $f \neq 0$, *so gibt es* $q, r \in K[t]$ *mit* $g = q \cdot f + r$ *und* $\deg r < \deg f$.

Definition 4.9. Sei $(R, +, \cdot)$ ein Ring, und sei $I \subseteq R$. I ist ein *Ideal* von $\mathbf{R}$, wenn für alle $i, j \in I$ und $r \in R$ gilt: $i - j \in I$, $r \cdot i \in I$, $i \cdot r \in I$.

Kongruenzrelationen und Ideale eines Ringes sind einander durch $\alpha \mapsto 0/\alpha$ bijektiv zugeordnet.

Satz 4.2 ($\mathbf{K}[t]$ ist Hauptidealbereich). *Sei* $\mathbf{K}$ *ein Körper, und sei* I *ein Ideal von* $\mathbf{K}[t]$. *Dann gibt es* $f \in K[t]$ *mit* $I = \{p \cdot f \mid p \in K[t]\} = (f)$.

Wenn $I \neq 0$, *dann gilt für jedes* f *mit* $\deg f = \min\{\deg i \mid i \in I \setminus \{0\}\}$, *dass* $I = (f)$.

Satz 4.3 (ggT in $\mathbf{K}[t]$). *Sei* $\mathbf{K}$ *ein Körper, und seien* $f, g \in K[t]$, *nicht beide* 0. *Dann gibt es genau ein* $d \in K[t]$, *sodass*

(1) $d|f$, $d|g$.
(2) *Für alle* u *mit* $u|f$ *und* $u|g$ *gilt* $u|d$.
(3) d *ist normiert.*

Dieses d *heißt der* ggT *von* f *und* g. *Es gibt* $u, v \in K[t]$, *sodass* $u \cdot f + v \cdot g = d$.

Beweisskizze: Wir wählen für d einen normierten Erzeuger des Ideals $I = \{u \cdot f + v \cdot g \mid u, v \in K[t]\}$.

Satz 4.4. *Sei* $\mathbf{K}$ *Körper,* $f \in K[t]$ *irreduzibel über* $\mathbf{K}$. *Dann ist* $\mathbf{K}[t]/(f)$ *ein Körper.*

3. Zerfällungskörper

SATZ 4.5. *Sei* $\mathbf{K}$ *ein Körper, und sei* f *ein normiertes Polynom in* $\mathbf{K}[t]$ *vom Grad* n*. Dann gibt es einen Erweiterungskörper* $\mathbf{E}$ *von* $\mathbf{K}$*, sodass jeder in* $\mathbf{E}[t]$ *irreduzible Teiler von* f *Grad* 1 *hat.*

Beweis: Wir beweisen folgende Aussage durch Induktion nach n:

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

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

DEFINITION 4.10. Sei $\mathbf{F}$ ein Körper, und sei $f \in F[t]$, $n := \deg f \geq 1$, und sei $\mathbf{E}$ ein Körper. $\mathbf{E}$ heißt *Zerfällungskörper* von f über $\mathbf{F}$, wenn er ein Erweiterungskörper von $\mathbf{F}$ ist, und es $a, e_1, \ldots, e_n \in E$ gibt, sodass

$$f = a \prod_{i=1}^{n} (t - e_i),$$

und $\mathbf{E}$ der von F und $\{e_1, e_2, \ldots, e_n\}$ erzeugte Unterkörper von $\mathbf{E}$ ist.

SATZ 4.6. *Für jedes nichtkonstante Polynom* f *über einem Körper* $\mathbf{K}$ *gibt es einen Zerfällungskörper von* f *über* $\mathbf{K}$*.*

[1] $\mathbf{L}$ ist zunächst kein Erweiterungskörper von $\mathbf{K}$, da K keine Teilmenge von L ist. Man kann aber leicht einen Körper $\mathbf{L}'$ angeben, der zu $\mathbf{L}$ isomorph ist, und $\mathbf{K}$ als Unterkörper enthält, indem man in $\mathbf{L}$ jedes konstante Polynom $(k_0, 0, 0, \ldots)$ durch k_0 ersetzt.

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

Definition 4.11. Sei $a = \sum_{i=1}^{n} a_i t^i \in \mathbb{Z}[t]$, $a \neq 0$. Wir definieren den *Inhalt von* a durch $\operatorname{cont}(a) := \operatorname{ggT}(a_0, a_1, \ldots, a_n)$.

Lemma 4.12. *Seien* $f, g \in \mathbb{Z}[t] \setminus \{0\}$. *Dann gilt* $\operatorname{cont}(f \cdot g) = \operatorname{cont}(f) \cdot \operatorname{cont}(g)$.

Satz 4.7. *Sei* $f \in \mathbb{Z}[t] \setminus \{0\}$, *seien* $g, h \in \mathbb{Q}[t]$ *so, dass* $f = g \cdot h$, *und seien* $\alpha, \beta \in \mathbb{Z}$ *so, dass* $\alpha\, g \in \mathbb{Z}[t]$ *und* $\beta\, h \in \mathbb{Z}[t]$. *Wir setzen:*

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

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

Satz 4.8 (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) $p | a_0, \ldots, p | a_{n-1}$,
(2) $p \not| a_n$,
(3) $p^2 \not| a_0$.

Dann ist a *ein in* $\mathbb{Q}[t]$ *irreduzibles Polynom.*

Satz 4.9. *Sei* $a \in \mathbb{Z}[t]$, $n := \deg a$, *und sei* r *eine rationale Nullstelle von* $a = a_0 t^0 + \cdots + a_n t^n$. *Dann gibt es* $p, q \in \mathbb{Z}$, *sodass* $r = \frac{p}{q}$ *und* $p | a_0$, $q | a_n$.

KAPITEL 5

Endliche Körper

1. Primkörper

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

SATZ 5.1. *Sei* $\mathbf{E}$ *ein endlicher Körper. Dann gibt es eine Primzahl* p*, sodass der Primkörper von* $\mathbf{E}$ *isomorph zu* $\mathbb{Z}_p$ *ist.*

Beweis: Offensichtlich sind alle $a * 1$ mit $a \in \mathbb{Z}$ in jedem Unterkörper von $\mathbf{E}$ enthalten. Da $\mathbf{E}$ 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

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

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

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

ÜBUNGSAUFGABEN 5.2.

(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 5.3. *Die Anzahl der Elemente eines endlichen Körpers ist eine Primzahlpotenz.*

Wir beweisen folgende stärkere Aussage:

SATZ 5.4. *Sei* $\mathbf{K}$ *ein Unterkörper des endlichen Körpers* $\mathbf{E}$*. 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 E hat E 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 5.4 folgt nun, wenn man als **K** den Primkörper von **E** wählt.

Satz 5.5. *Sei* **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 5.6.

(1) Sei **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 **K** ein Körper, und sei $f \in \mathbf{K}[x]$. 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 $\mathbf{K}[x]$ ist.
(3) Zeigen Sie, dass ein Polynom in $\mathbf{K}[x]$ vom Grad $\leq n$, das $n + 1$ verschiedene Nullstellen hat, automatisch das Nullpolynom sein muss.
(4) Sei **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 $p | \binom{p}{i}$ für alle $i \in \{1, 2, \ldots, p-1\}$, und dass für alle $\alpha, \beta \in K$ gilt: $(\alpha + \beta)^p = \alpha^p + \beta^p$.

2. Die multiplikative Gruppe eines endlichen Körpers

Satz 5.7. *Die multiplikative Gruppe eines endlichen Körpers ist zyklisch.*

Wir zeigen diesen Satz mithilfe des folgenden Satzes.

Satz 5.8. *Sei* $\mathbf{A} = (A, \cdot)$ *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* $\mathbf{A}$ *zyklisch.*

Beweis: Sei $h := |A|$. Falls $h = 1$, ist $\mathbf{A}$ 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)

$$b_i^{{p_i}^{r_i}} = 1. \tag{2.1}$$

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

$$s_i = r_i. \tag{2.2}$$

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 (2.2). 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

$$\prod_{i=1}^{N} b_i^{\frac{h}{p_j}} = 1. \tag{2.3}$$

Falls $i \neq j$, so gilt ${p_i}^{r_i} | \frac{h}{p_j}$. Wegen (2.1) sind also Faktoren in (2.3) mit $i \neq j$ gleich 1. Wir erhalten also

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

Da b_j wegen (2.2) die Ordnung ${p_j}^{r_j}$ hat, gilt ${p_j}^{r_j}|\frac{h}{p_j}$. Daher gilt ${p_j}^{r_j+1}|h$, 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 $\mathbf{A}$. $\square$

Aus dem Satz 5.8 folgt nun direkt der Satz 5.7, da in jedem Körper und für jedes n das Polynom $x^n - 1$ höchstens n Nullstellen hat.

Übungsaufgaben 5.9.

(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.

3. Körper aus irreduziblen Polynomen

Satz 5.10. *Sei $\mathbf{K}$ ein Körper, und sei $f \in \mathbf{K}[x]$ irreduzibel über $\mathbf{K}$. Dann ist $\mathbf{K}[x]/(f)$ ein Körper.*

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

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

Satz 5.11. *Sei $\mathbf{K}$ ein endlicher Körper mit q Elementen, und sei f ein irreduzibles Polynom vom Grad n. Dann gilt $f|x^{q^n} - x$.*

Wir betrachten den Körper $\mathbf{K}[x]/(f)$. Dieser Körper hat q^n Elemente. Es gilt also wegen Satz 5.5 (2) $(x + (f))^{q^n} = x + (f)$. Das bedeutet

$$f|x^{q^n} - x. \quad \square$$

Satz 5.12. *Sei $\mathbf{K}$ ein Körper mit q Elementen. Dann gilt*

$$\prod_{\nu \in K} (x - \nu) = x^q - x.$$

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 5.5. Die Differenz dieser beiden Polynome hat also mindestens q Nullstellen, und einen Grad $\leq q - 1$. Die Differenz ist also das Nullpolynom. $\square$

Lemma 5.13. *Sei $\mathbf{K}$ ein endlicher Körper mit q Elementen, sei $m \in \mathbb{N}$, und sei f ein über $\mathbf{K}$ irreduzibles Polynom vom Grad m. Sei $\mathbf{E}$ ein Erweiterungskörper*

von $\mathbf{K}$ *mit* q^m *Elementen. Dann zerfällt* f *in* $\mathbf{E}[x]$ *in ein Produkt lauter linearer Polynome.*

Beweis: Da $\deg f = m$, gilt nach Satz 5.11, dass f das Polynom $x^{q^m} - x$ teilt. Nach Satz 5.12 gilt

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

Das Polynom f ist auch ein Polynom in $\mathbf{E}[x]$. Jeder über $\mathbf{E}$ irreduzible Teiler von f in $\mathbf{E}[x]$ teilt also eines der Polynome in $\{x - b \mid b \in E\}$. Das bedeutet, dass f in $\mathbf{E}[x]$ 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 5.14. *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 $\mathbf{E}$ ein Körper mit q Elementen. Aus dem Lemma 5.13 wissen wir, dass f eine Nullstelle in $\mathbf{E}$ hat. Sei $b \in E$ so, dass $\overline{f}(b) = 0$. Wir bilden nun die Abbildung

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

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 $h|f$. 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 $h|f$ widerspricht. Also ist $h = f$. Es gilt also nach dem Homomorphiesatz, dass $\mathbb{Z}_p[x]/(f)$ isomorph zu $\mathbf{E}$ ist. □

4. Existenz irreduzibler Polynome

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

Satz 5.15. *Sei* $\mathbf{K}$ *ein Körper, und sei* f *ein normiertes Polynom in* $\mathbf{K}[x]$ *vom Grad* n*. Dann gibt es einen Erweiterungskörper* $\mathbf{E}$ *von* $\mathbf{K}$*, sodass jeder in* $\mathbf{E}[x]$ *irreduzible Teiler von* f *Grad* 1 *hat.*

Wir beweisen folgende Aussage durch Induktion nach n:

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

Für $n = 1$ ist die Aussage klar. Wir fixieren nun einen Körper $\mathbf{K}$ und ein Polynom $f \in \mathbf{K}[x]$ mit $\deg f = n > 1$. Wir zerlegen f in ein Produkt von normierten, über $\mathbf{K}$ irreduziblen Polynomen in $\mathbf{K}[x]$. Sei g einer der irreduziblen Faktoren. Wir bilden den Körper $\mathbf{L} := \mathbf{K}[x]/(g)$. 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 $\mathbf{K}[x]/(g)$ 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 $x^0 = (1, 0, 0, \ldots)$, $x^1 = (0, 1, 0, 0, \ldots)$, $x^2 = (0, 0, 1, 0, 0, \ldots), \ldots$. Also gilt $(\sum_{i=0}^{\deg f} f_i \cdot x^i) + (g) = f + (g)$. Da $g|f$, gilt $f + (g) = 0 + (g)$. Also ist $x + (g)$ eine Nullstelle von f un $\mathbf{L}$. Da f eine Nullstelle l in $\mathbf{L}$ hat, gibt es $h \in \mathbf{L}[x]$, sodass $f = (x - l) \cdot h$. Da h kleineren Grad als f hat, gibt es nach nach Induktionsvorraussetzung einen Erweiterungskörper $\mathbf{M}$ von $\mathbf{L}$, sodass jeder in $\mathbf{M}[x]$ irreduzible Teiler des Polynoms h Grad 1 hat. In $\mathbf{M}[x]$ hat jeder irreduzible Teiler von f also Grad 1. □

Satz 5.16. *Sei $\mathbf{K}$ ein endlicher Körper, und sei $n \in \mathbb{N}$. Dann gibt es ein über $\mathbf{K}$ irreduzibles Polynom vom Grad n in $\mathbf{K}[x]$.*

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

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

Mit Satz 5.5 (1) erhalten wir, dass $\mathbf{L}$ ein Unterkörper von $\mathbf{E}$ ist; mit mit Satz 5.5 (2), dass $\mathbf{L}$ ein Erweiterungskörper von $\mathbf{K}$ ist. Da $x^{q^n} - x$ über $\mathbf{E}$ in lauter Linearfaktoren zerfällt, gibt es $e_1, e_2, \ldots, e_{q_n} \in E$, sodass

$$x^{q^n} - x = \prod_{r=1}^{q^n} (x - e_r).$$

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

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

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

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

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

Wir nehmen an, es gibt normierte $f_1, f_2 \in \mathbf{K}[x]$ 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 $f|f_1$, und somit $f_2 = 1$. Das beweist (4.1).

Die Abbildung

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

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

Literaturverzeichnis

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

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

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

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

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

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

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

[Rivest et al., 1978] Rivest, R. L., Shamir, A., and Adleman, L. (1978). A method for obtaining digital signatures and public-key cryptosystems. *Comm. ACM*, 21(2):120–126.

[Robinson, 2003] Robinson, D. J. S. (2003). *An Introduction to Abstract Algebra*. Walter de Gruyter, Berlin – New York, www.deGruyter.com.

[Rotman, 1998] Rotman, J. J. (1998). *Galois theory*. Springer-Verlag, New York, second edition.