Inhaltsverzeichnis

TEIL II: GRUPPEN

In der modernen Algebra versucht man die Zahlen ($\mathbb{Z}, \mathbb{Q}, \mathbb{R}, \ldots$) durch die Konzentration auf Rechenoperationen ($+, \cdot, \ldots$), oder allgemeiner auf *strukturelle Eigenschaften* dieser Operationen, zu verstehen. Als erstes Beispiel einer **algebraischen Struktur** werden wir den Begriff der **Gruppe** studieren.

3.1 Gruppen, Untergruppen und Gruppen-Homomorphismen

3.1.1 Gruppen

Definition 3.1.1 (*Gruppe*)

Eine **Gruppe** $(G, \circ)$ ist eine Menge G zusammen mit einer **Verknüpfung** (oder **Gruppenoperation**)

$$\begin{array}{rccc} \circ\colon & G \times G & \longrightarrow & G \\ & (a,b) & \mapsto & a \circ b\,, \end{array}$$

die folgende Bedingungen erfüllt:

(G1) Assoziativität: $(a \circ b) \circ c = a \circ (b \circ c) \quad \forall\, a, b, c \in G$.

(G2) Existenz eines neutralen Elementes: Es existiert ein $e \in G$ mit $e \circ a = a = a \circ e \quad \forall\, a \in G$.

(G3) Existenz inverser Elemente: Zu jedem $a \in G$ gibt es ein $a^{-1} \in G$ mit $a \circ a^{-1} = e = a^{-1} \circ a$.

Gilt zudem für alle $a, b \in G$: $a \circ b = b \circ a$ (*Kommutativität*), so nennen wir G eine **abelsche** Gruppe.
Die Anzahl $|G|$ der Elemente in G heißt **Ordnung** der Gruppe G.

Notation:

- Die Verknüpfung kann auch mit anderen Symbolen bezeichnet werden: z.B. $\cdot$, $+$, $\star$, $*$, $\heartsuit$, $\diamondsuit$, ... Typischerweise sind die Rechenoperationen Addition und Multiplikation Verknüpfungen.
- Wenn die Verknüpfung die Multiplikation $\cdot$ ist, schreiben wir auch ab statt $a \cdot b$. In diesem Fall ist das neutrale Element $e = 1$.
- Wenn die Verknüpfung die Addition $+$ ist, ist das neutrale Element $e = 0$ und wir bezeichnen das inverse Element von a mit $-a$ statt a^{-1}.

Beispiel 3.1.2

(a) $G = \mathbb{Z}$ mit Verknüpfung $\circ = +$ (die Addition) ist eine Gruppe.
Das neutrale Element ist $e = 0$ und das inverse Element von $a \in \mathbb{Z}$ ist $-a$.

(b) Ähnlich: $(\mathbb{Q}, +)$, $(\mathbb{R}, +)$ und $(\mathbb{C}, +)$ sind Gruppen.
Das neutrale Element ist $e = 0$ und das inverse Element von a ist $-a$.

(c) $G = \mathbb{Q} \setminus \{0\}$ mit Verknüpfung $\circ = \cdot$ (die Multiplikation) ist eine Gruppe.
Das neutrale Element ist $e = 1$ und das inverse Element von $a \in \mathbb{Q} \setminus \{0\}$ ist $a^{-1} = \frac{1}{a}$.

(d) Ähnlich: $(\mathbb{R} \setminus \{0\}, \cdot)$ und $(\mathbb{C} \setminus \{0\}, \cdot)$ sind Gruppen.
Das neutrale Element ist $e = 1$ und das inverse Element von a ist $a^{-1} = \frac{1}{a}$.

(e) $G = \{-1, 1\}$ mit Verknüpfung $\circ = \cdot$ (die Multiplikation) ist eine Gruppe.

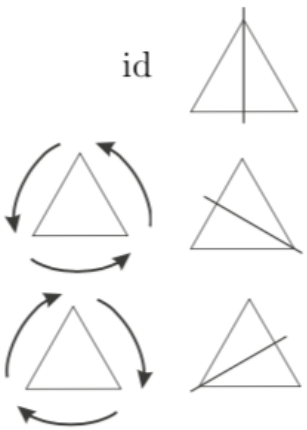
(f) $(\mathbb{Z}, +)$, $(\mathbb{Q}, +)$, $(\mathbb{R}, +)$, $(\mathbb{C}, +)$, $(\mathbb{Q} \setminus \{0\}, \cdot)$, $(\mathbb{R} \setminus \{0\}, \cdot)$, $(\mathbb{C} \setminus \{0\}, \cdot)$ sind alle abelsche Gruppen.

(g) Sei $X \neq \emptyset$ eine Menge. Die Menge

$$S(X) := \{\pi : X \longrightarrow X \mid \pi \text{ bijektive Abbildung}\}$$

der bijektiven Abbildungen zusammen mit der Komposition $\circ$ von Abbildungen als Verknüpfung ist eine Gruppe. Diese heißt die **symmetrische Gruppe auf** X.
Das neutrale Element ist Id_X, die identische Abbildung. Das inverse Element von $\pi : X \longrightarrow X$ ist die Umkehrabbildung π^{-1}.
Im Abschnitt 3.1.4 werden wir den Fall $X := \{1, \ldots, n\}$ untersuchen.

(h) Die Menge D_6 der Symmetrien eines regulären Dreieck bildet eine Gruppe. Die Elemente von D_6 sind die identische Abbildung, die Drehung um $\frac{2\pi}{3}$, die Drehung um $-\frac{2\pi}{3}$ (andere Richtung) und die drei Spiegelungen an einer Symmetrieachse des Dreiecks.



Die Veknüpfung ist die Komposition der Symmetrien. Diese Gruppe ist nicht abelsch, denn die Komposition einer Spiegelung mit einer Drehung und die Komposition derselben Drehung mit derselben Spiegelung ergeben nicht das gleiche Ergebnis.

Anmerkung 3.1.3

(a) $(\mathbb{Z}, \cdot)$ und $(\mathbb{Z}\setminus\{0\}, \cdot)$ sind keine Gruppen. Z.B. hat 2 kein inverses Element, da $2^{-1} = \frac{1}{2} \notin \mathbb{Z}$. Damit ist **(G3)** nicht erfüllt.

(b) $(\mathbb{Q}, \cdot)$ ist auch keine Gruppe. Die 0 hat kein inverses Element, da $0 \cdot a' \neq 1$ für alle $a' \in \mathbb{Q}$. Damit ist **(G3)** nicht erfüllt.

(c) Aus ähnlichen Gründen sind $(\mathbb{N}, +)$, $(\mathbb{N}_0, +)$, $(\mathbb{N}, \cdot)$, $(\mathbb{N}_0, \cdot)$, $(\mathbb{R}, \cdot)$, $(\mathbb{C}, \cdot)$ keine Gruppen.

Lemma 3.1.4 (*Eigenschaften der Gruppen*)

In jeder Gruppe $(G, \circ)$ gilt:

(a) Das neutrale Element ist eindeutig.

(b) Die Inversen der Elemente von G sind eindeutig.

(c) $(a \circ b)^{-1} = b^{-1} \circ a^{-1} \quad \forall\ a, b \in G$.

(d) $(a^{-1})^{-1} = a \quad \forall\ a \in G$.

(e) **(Kürzungsregel)**: Für alle $x, a, b \in G$ gilt:

$$x \circ a = x \circ b \Leftrightarrow a = b, \quad \text{und analog}$$
$$a \circ x = b \circ x \Leftrightarrow a = b\,.$$

Beweis:

(a) Falls $\widetilde{e}$ ein weiteres neutrales Element ist, so gilt $e \circ \widetilde{e} = e$ nach (G2).
Aber es gilt auch $e \circ \widetilde{e} = \widetilde{e}$ nach (G2), da e neutral ist.
Damit ist $e = \widetilde{e}$, also eindeutig bestimmt.

(b) Sei $a \in G$ mit inversem Element a^{-1}. Sei $\widetilde{a}$ ein weiteres inverses Element. Dann gilt:

$$\widetilde{a} \overset{(G2)}{=} e \circ \widetilde{a} \overset{(G3)}{=} (a^{-1} \circ a) \circ \widetilde{a} \overset{(G1)}{=} a^{-1} \circ (a \circ \widetilde{a}) \overset{(G3)}{=} a^{-1} \circ e \overset{(G2)}{=} a^{-1}$$

(c) (d) und (e): Aufgabe. ∎

3.1.2 Untergruppen

Ausgehend von einer Gruppe G kann man durch Einschränken der gegebenen Verknüpfung auf eine Teilmenge $U \subset G$ neue Gruppen erzeugen:

Definition 3.1.5 (*Untergruppe*)

Sei $(G, \circ)$ eine Gruppe. Eine Teilmenge $U \subseteq G$ heißt eine **Untergruppe** von G, wenn gelten:

$$e \in U, \qquad a \circ b \in U \qquad \text{und} \qquad a^{-1} \in U \qquad \forall\, a, b \in U.$$

In Zeichen schreiben wir: $(U, \circ) \leq (G, \circ)$ oder kurz $U \leq G$.
(Man sagt auch: U muss bezüglich der Gruppenoperationen abgeschlossen sein.)

Beispiel 3.1.6

(a) $U = G$ und $U = \{e\}$ sind immer Untergruppen von G.

(b) $(\mathbb{Z}, +)$ ist eine Untergruppe von $(\mathbb{Q}, +)$. Wir schreiben einfach $\mathbb{Z} \leq \mathbb{Q}$.

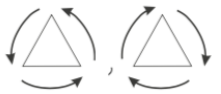
(c) Ähnlich: $\mathbb{Q} \leq \mathbb{R}$ und $\mathbb{R} \leq \mathbb{C}$ für die Addition.

(d) $(\mathbb{Q} \setminus \{0\}, \cdot)$ ist eine Untergruppe von $(\mathbb{R} \setminus \{0\}, \cdot)$.

(e) In D_6 (die Gruppe der Symmetrien eines regulären Dreieck) ist die Teilmenge

$$U = \{\mathrm{Id}_{D_6},\ \text{Drehung um } \frac{2\pi}{3},\ \text{Drehung um } -\frac{2\pi}{3}\}$$

$$= \left\{ \mathrm{Id}_{D_6}, \quad , \quad \right\}$$



eine Untergruppe.

(f) Die geraden Zahlen $2\mathbb{Z} = \{2 \cdot n \mid n \in \mathbb{Z}\} = \{\ldots, -6, -4, -2, 0, 2, 4, 6, \ldots\}$ bilden eine Untergruppe von $(\mathbb{Z}, +)$.
Dagegen bilden die ungeraden Zahlen $\{2n + 1 \mid n \in \mathbb{Z}\}$ keine Untergruppe von $(\mathbb{Z}, +)$, z.B. weil das neutrale Element 0 nicht darin enthalten ist.

Lemma 3.1.7 (*Untergruppenkriterium*)

Sei $(G, \circ)$ eine Gruppe. Eine Teilmenge $U \subseteq G$ ist eine Untergruppe von G genau dann, wenn

$$U \neq \emptyset \text{ und } a \circ b^{-1} \in U \qquad \forall\, a, b \in U\,.$$

Beweis: Aufgabe. ■

Im Allgemeinen ist es schwierig, alle Untergruppen einer Gruppe anzugeben oder auch nur ihre Anzahl zu bestimmen. Im Fall der Gruppe $\mathbb{Z}$ haben wir trotzdem eine einfache Antwort auf diese Frage:

Satz 3.1.8

Die Untergruppen von $(\mathbb{Z}, +)$ sind genau die Teilmengen U von $\mathbb{Z}$ der Form

$$U = n\mathbb{Z} = \{n \cdot k \mid k \in \mathbb{Z}\}\,,$$

wobei $n \in \mathbb{Z}_{\geq 0}$ ist.

(Anders gesagt ist $n\mathbb{Z}$ die Menge aller ganzzahligen Vielfachen von n.)

Beweis:

- Mit dem Untergruppenkriterium sieht man sofort, dass $n\mathbb{Z} \subset \mathbb{Z}$ eine Untergruppe ist.
- Sei umgekehrt $H \subset \mathbb{Z}$ eine beliebige Untergruppe. Entweder gilt $H = \{0\}$ (das neutrale Element muss darin enthalten sein) oder $H \supsetneq \{0\}$ und es gibt ein kleinstes Element $n > 0$ in H. Wir zeigen, dass dann $H = n\mathbb{Z}$ gilt: Sei $m \in H$ beliebig. Division mit Rest liefert eine Darstellung

$$m = q \cdot n + r$$

mit $q, r \in \mathbb{Z}$ und $0 \leq r < |n| = n$. Da $n \in H$ ist, ist auch $q \cdot m = m + m + \ldots + m$ (q-mal) Element von H. Damit ist $r = m - q \cdot n$ Element von H, da H eine Untergruppe ist. Aber nach der Definition von n (das kleinste Element in H mit $n > 0$) folgt $r = 0$, also $m = q \cdot n \in n\mathbb{Z}$. ■

3.1.3 Gruppen-Homomorphismen

Wir wollen nun verschiedene Gruppen miteinander in Beziehung setzen. In der Sprache der Mathematik bedeutet dies, dass wir *Abbildungen* zwischen Gruppen betrachten müssen. Dabei helfen uns allerdings beliebige Abbildungen nicht weiter. Wir benötigen Abbildungen, die mit den Gruppenoperationen „verträglich" sind. Diese speziellen Abbildungen heißen *Homomorphismen*.

Definition 3.1.9 (*Gruppen-Homomorphismus, Gruppen-Isomorphismus*)

Seien $(G, \circ)$ und $(H, \star)$ Gruppen. Eine Abbildung $\varphi : G \longrightarrow H$ heißt **(Gruppen)-Homomorphismus**, wenn

$$\varphi(a \circ b) = \varphi(a) \star \varphi(b) \qquad \forall\, a, b \in G\,.$$

(Man sagt, „*φ ist mit der Gruppenverknüpfung verträglich*".)

Ein bijektiver Gruppen-Homomorphismus heißt **Gruppen-Isomorphismus**.

Falls es ein Gruppen-Isomorphismus zwischen zwei Gruppen G and H existiert, dann schreiben wir auch $G \cong H$ und sagen, dass G und H **isomorph** sind.

Beispiel 3.1.10

(a) Die Abbildung

$$\begin{array}{rccc} \varphi: & (\mathbb{Z}, +) & \longrightarrow & (\mathbb{Z}, +) \\ & n & \mapsto & \varphi(n) = 2n \end{array}$$

ist ein Gruppen-Homomorphismus, denn für alle $m, n \in \mathbb{Z}$ gilt

$$\varphi(m + n) = 2(m + n) = 2m + 2n = \varphi(m) + \varphi(n)\,.$$

(b) Die Abbildung $\varphi : (\mathbb{R}, +) \longrightarrow (\mathbb{R}, +)$ mit $\varphi(x) = x + 1$, ist kein Gruppen-Homomorphismus, denn es ist z.B. $\varphi(0 + 0) = \varphi(0) = 1$, aber $\varphi(0) + \varphi(0) = 1 + 1 = 2$.

(c) Die Inklusion einer Untergruppe $U \subset G$ liefert einen injektiven Gruppen-Homomorphismus:

$$\begin{array}{ccc} (U, \circ) & \longrightarrow & (G, \circ) \\ u & \mapsto & u \end{array}$$

Z.B. ist die Abbildung $\varphi : (\mathbb{Z}, +) \longrightarrow (\mathbb{R}, +), n \mapsto n$ ein Gruppen-Homomorphismus.

(d) Die Abbildung

$$\begin{array}{rccc} \varphi\colon & \mathbb{Z} & \longrightarrow & n\mathbb{Z} \\ & k & \mapsto & n \cdot k \end{array}$$

ist ein Gruppen-Isomorphismus, denn sie ist ein Gruppen-Homomorphismus, injektiv und surjektiv (also bijektiv).

Definition 3.1.11 (*Kern, Bild*)

Sei $\varphi : G \longrightarrow H$ ein Gruppen-Homomorphismus.

(a) Der **Kern** von φ ist die Teilmenge $\ker(\varphi) := \{g \in G \,|\, \varphi(g) = e_H\}$.

(b) Das **Bild** von φ ist die Teilmenge $\varphi(G) := \{\varphi(g) \,|\, g \in G\}$. (Also das übliche Bild der Abbildung φ.)

Lemma 3.1.12 (*Eigenschaften der Gruppen-Homomorphismen*)

Seien $(G, \circ)$ und $(H, \star)$ Gruppen und sei $\varphi : G \longrightarrow H$ ein Gruppen-Homomorphismus. Dann gelten:

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

(b) Für alle $a \in G$ gilt $\varphi(a^{-1}) = \varphi(a)^{-1}$.

(c) Ist $\theta : H \longrightarrow K$ ein weiterer Gruppen-Homomorphismus, so ist auch die Verkettung $\theta \circ \varphi : G \longrightarrow K$ ein Gruppen-Homomorphismus.

(d) Der Kern von φ ist eine Untergruppe von G und das Bild von φ ist eine Untergruppe von H.

(e) φ ist injektiv genau dann, wenn $\ker(\varphi) = \{e_G\}$.

(f) φ ist surjektiv genau dann, wenn $\varphi(G) = H$.

(g) Ist φ bijektiv, so ist auch die Umkehrabbildung $\varphi^{-1} : H \longrightarrow G$ ein bijektiver Gruppen-Homomorphismus.

Beweis: Wir zeigen (a) und (e):

(a) Da G eine Gruppe ist, gilt zunächst $e_G = e_G \circ e_G$. Da H eine Gruppe ist, gilt $e_H \star \varphi(e_G) = \varphi(e_G)$. Damit gilt:

$$e_H \star \varphi(e_G) = \varphi(e_G) = \varphi(e_G \circ e_G) = \varphi(e_G) \star \varphi(e_G)\,,$$

da φ ein Gruppen-Homomorphismus ist. Nach der Kürzungsregel erhalten wir wie behauptet $e_H = \varphi(e_G)$.

(e) Wir haben zwei Richtungen zu zeigen:

'$\Rightarrow$': Sei φ injektiv. Nach (a) ist $\varphi(e_G) = e_H$, also $e_G \in \ker(\varphi)$. Wegen der Injektivität wird kein anderes Element von G auf e_H abgebildet, daher folgt $\ker(\varphi) = \{e_G\}$.

'$\Leftarrow$': Es gelte nun $\ker(\varphi) = \{e_G\}$; wir müssen zeigen, dass φ injektiv ist. Seien also $a, b \in G$ mit $\varphi(a) = \varphi(b)$. Dann ist

$$e_H = \varphi(a) \circ \varphi(b)^{-1} = \varphi(a \circ b^{-1})$$

d.h. $a \circ b^{-1} \in \ker(\varphi)$. Aus $\ker(\varphi) = \{e_G\}$ folgt also $a \circ b^{-1} = e_G$ und damit $a = b$. Also ist φ injektiv.

Für (b), (c), (d), (f) und (g) siehe die Aufgaben. ■

3.1.4 Hauptbeispiel 1: Die symmetrische Gruppe

In Beispiel 3.1.2 haben wir gesehen, dass die Menge

$$S(X) := \{\pi : X \longrightarrow X \mid \pi \text{ bijektive Abbildung}\}$$

der bijektiven Abbildungen einer beliebigen Menge $X \neq \emptyset$ zusammen mit der Komposition $\circ$ von Abbildungen als Verknüpfung eine Gruppe ist: die **symmetrische Gruppe auf** X.
(Erinnerung: Das neutrale Element ist die identische Abbildung Id und das inverse Element von $\sigma \in S_n$ ist die Umkehrabbildung σ^{-1}.)

Wir konzentrieren uns nun auf den Fall $X = \{1, 2, \ldots, n\}$ mit $n \in \mathbb{N}$ eine natürliche Zahl.

Definition 3.1.13 (*Symmetrische Gruppe vom Grad n*)

Sei $n \in \mathbb{N}$ eine natürliche Zahl. Die symmetrische Gruppe auf $X = \{1, \ldots, n\}$ heißt **symmetrische Gruppe vom Grad** n und wir schreiben

$$S_n := S(\{1, \ldots, n\}) = \{\sigma : \{1, \ldots, n\} \longrightarrow \{1, \ldots, n\} \mid \sigma \text{ bijektiv}\}.$$

Die Elemente von S_n heißen **Permutationen**.

Die Elemente von S_n kann man durch ihre „Wertetabelle“ angeben: d.h. für $\sigma \in S_n$ schreiben wir

$$\sigma = \begin{pmatrix} 1 & 2 & \cdots & n \\ \sigma(1) & \sigma(2) & \cdots & \sigma(n) \end{pmatrix}.$$

Da in der unteren Reihe dieser Matrix eine Permutation, d.h. eine Anordnung der Zahlen $1, \ldots, n$ steht, kann man S_n auch als die Gruppe der Permutationen von n Elementen auffassen.
Ein Element von S_n, das genau zwei Elemente von $\{1, \ldots, n\}$ vertauscht, heißt **Transposition**.

Beispiel 3.1.14 (*Die symmetrische Gruppe vom Grad* 3)

Das neutrale Element in S_3, also die identische Abbildung auf $\{1, 2, 3\}$ ist die Permutation $\left(\begin{smallmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{smallmatrix}\right)$.
Das Element $\sigma \in S_3$ mit $\sigma(1) = 2$, $\sigma(2) = 3$ und $\sigma(3) = 1$ ist die Permutation $\left(\begin{smallmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{smallmatrix}\right)$.
Die Permutationen

$$\left(\begin{smallmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{smallmatrix}\right), \left(\begin{smallmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{smallmatrix}\right) \text{ und } \left(\begin{smallmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{smallmatrix}\right)$$

sind Transpositionen.
Es gilt:

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

Die Gruppe S_3 hat also 6 Elemente, d.h. $|S_3| = 6$.

Im Allgemeinen ist es einfach die Ordnung der symmetrischen Gruppe zu bestimmen:

Satz 3.1.15

Sei $n \in \mathbb{N}$ eine Natürliche Zahl. Dann gilt $|S_n| = n! := 1 \cdot 2 \cdot \cdots \cdot n$.
(D.h. n-Fakultät Elemente.)

Beweis: Um eine bijektive Abbildung $\sigma : \{1, \ldots, n\} \longrightarrow \{1, \ldots, n\}$ zu erhalten, gibt es n Möglichkeiten für $\sigma(1)$, sodann $n-1$ Möglichkeiten für $\sigma(2)$, ..., und schließlich noch 2 Möglichkeiten für $\sigma(n-1)$ und eine Möglichkeit für $\sigma(1)$. ■

Anmerkung 3.1.16

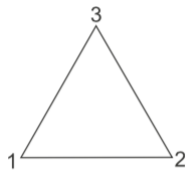
Für $n \geq 3$ ist die symmetrische Gruppe S_n niemals abelsch.

Z.B.: betrachten wir die Permutationen $\sigma = \left(\begin{smallmatrix} 1 & 2 & 3 & 4 & \cdots & n \\ 2 & 1 & 3 & 4 & \cdots & n \end{smallmatrix}\right)$ und $\tau = \left(\begin{smallmatrix} 1 & 2 & 3 & 4 & \cdots & n \\ 1 & 3 & 2 & 4 & \cdots & n \end{smallmatrix}\right)$ (d.h. wobei σ und τ die identische Abbildungen auf $\{4, \ldots, n\}$ sind), so gilt

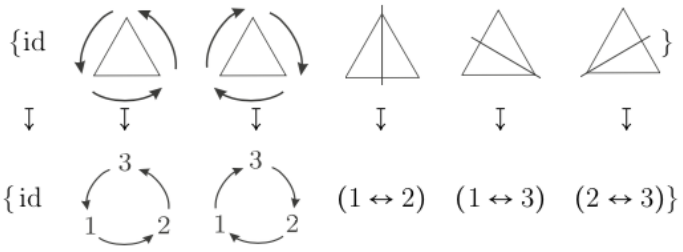
$$\sigma \circ \tau = \left(\begin{smallmatrix} 1 & 2 & 3 & 4 & \cdots & n \\ 2 & 3 & 1 & 4 & \cdots & n \end{smallmatrix}\right) \neq \left(\begin{smallmatrix} 1 & 2 & 3 & 4 & \cdots & n \\ 3 & 1 & 2 & 4 & \cdots & n \end{smallmatrix}\right) = \tau \circ \sigma .$$

Beispiel 3.1.17 (*Die Gruppe der Symmetrien des regulären Dreiecks als symmetrische Gruppe*)

Die Gruppe D_6 der Symmetrien des regulären Dreiecks aus Beispiel 3.1.2 kann man als symmetrische Gruppe sehen, indem man die Ecken des Dreiecks mit $1, 2, 3$ nummeriert:



Damit bilden wir einen Gruppen-Isomorphismus $\varphi : D_6 \longrightarrow S_3$ wie folgt:



Die Darstellung von Permutationen in Abbildungsschreibweise ist in der Praxis nicht sehr effizient. Z.B.: Für die Permutation

$$\sigma = \left(\begin{smallmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 2 & 3 & 1 & 4 & 5 & 6 \end{smallmatrix}\right) \in S_6$$

müssen wir uns die Bilder von $4, 5, 6$ nicht merken, da sie nicht permutiert werden, und die Bilder von $1, 2, 3$ können wir in dem Diagramm

codieren. Dies ist die Idee eines Zykels. Damit erhalten wir eine effizientere Schreibweise für Permutationen:

Definition 3.1.18 (*k-Zykel, disjunkte Zykel*)

Sei $1 \leq k \leq n$.

(a) Ein k-**Zykel** in S_n ist eine Permutation $\sigma \in S_n$ der Form

$$\begin{array}{rccll} \sigma\colon & \{1,\dots,n\} & \longrightarrow & \{1,\dots,n\} & \\ & a_1 & \mapsto & a_2 & \\ & a_2 & \mapsto & a_3 & \\ & \dots & \mapsto & \dots & \\ & a_{k-1} & \mapsto & a_k & \\ & a_k & \mapsto & a_1 & \\ & a & \mapsto & a, & \text{sonst,} \end{array}$$

die die Zahlen $a_1, \dots, a_k$ zyklisch vertauscht und alle anderen Zahlen fest lässt.
Notation: $\sigma = (a_1, a_2, \dots, a_k)$.

(b) Zwei Zykel $(a_1, a_2, \dots, a_k)$ und $(b_1, b_2, \dots, b_\ell)$ in S_n heißen **disjunkt**, wenn keine Zahl in beiden Zykeln vorkommt.

Beispiel 3.1.19

(a) Die obige Permutation

$$\sigma = \left(\begin{smallmatrix} 1&2&3&4&5&6 \\ 2&3&1&4&5&6 \end{smallmatrix}\right) \in S_6$$

ist ein 3-Zykel: $\sigma = (1, 2, 3)$.

(b) **Beachte**: die Darstellung als k-Zykel ist nicht eindeutig. Z.B. ist

$$(1, 2, 3) = (2, 3, 1) = (3, 1, 2)\,.$$

(c) Eine Transposition ist ein 2-Zykel, denn sie vertauscht genau 2 Zahlen. Mit der Zykel-Notation ist jede Transposition der Form (a_1, a_2).

(d) Ein 1-Zykel ist einfach die identische Abbildung.

(e) Mit der Zykel-Notation ist $S_3 = \{\mathrm{Id}, (1,2), (1,3), (2,3), (1,2,3), (1,3,2)\}$.

(f) Wir betrachten die Permutation

$$\sigma = \left(\begin{smallmatrix} 1&2&3&4&5&6&7 \\ 4&7&1&6&5&3&2 \end{smallmatrix}\right) \in S_7\,.$$

Dabei gilt:

$$1 \mapsto 4 \mapsto 6 \mapsto 3 \mapsto 1 \qquad \text{(Dies ist der 4-Zykel } (1,4,6,3)\,.\text{)}$$

$$2 \mapsto 7 \mapsto 2 \qquad \text{(Dies ist der 2-Zykel } (2,7)\,.\text{)}$$

$$5 \mapsto 5 \qquad \text{(Dies ist der 1-Zykel } (5)\,.\text{)}$$

Damit ist $\sigma = (1, 4, 6, 3) \circ (2, 7) \circ (5)$ eine Komposition von **disjunkten** Zykeln.
Nach Konvention schreibt man weder die 1-Zykel noch die Komposition $\circ$, d.h.

$$\sigma = (1, 4, 6, 3) \circ (2, 7) \circ (5) = (1, 4, 6, 3)(2, 7)\,.$$

Weiter gilt $(1,4,6,3) = (1,4)(4,6)(6,3)$ und somit hat σ auch eine Darstellung als Komposition von Transpositionen:

$$\sigma = (1,4)(4,6)(6,3)(2,7)\,.$$

Im Allgemeinen kann man immer Permutationen als Komposition von Zykeln und auch Komposition von Transpositionen darstellen:

Satz 3.1.20

(a) Jede Permutation $\sigma \in S_n$ lässt sich als Komposition disjunkter Zykel schreiben.

(b) Jede Permutation $\sigma \in S_n$ lässt sich als Komposition von Transpositionen schreiben.

Beweis:

(a) Kein formaler Beweis für diese Aussage. Die Methode ist wie im Beispiel 3.1.19(f).

(b) Es reicht zu zeigen, dass jeder k-Zykel $\sigma \in S_n$ sich als Komposition von Transpositionen schreiben lässt. Somit folgt (c) aus (a).
Aber offenbar ist

$$(a_1, a_2, \ldots, a_k) = (a_1, a_2) \circ (a_2, a_3) \circ \cdots \circ (a_{k-1}, a_k)$$

eine Komposition von $k-1$ Transpositionen. ■

Anmerkung 3.1.21

(a) **Beachte**: die Darstellungen von Permutationen als Komposition disjunkter Zykel und Komposition von Transpositionen im Satz 3.1.20 sind nicht eindeutig!

(b) Falls eine Permutation $\sigma \in S_n$ zwei verschiedene Darstellungen

$$\sigma = \tau_1 \circ \cdots \circ \tau_k = \rho_1 \circ \cdots \circ \rho_s$$

als Komposition von Transpositionen besitzt, so gilt $k \equiv s \mod 2$.

Anders gesagt ist die Parität der Anzahl der Transpositionen unabhängig von der Wahl der Darstellung von σ als Komposition von Transpositionen.

Definition 3.1.22 (*Gerade/ungerade Permutation*)

Sei $\sigma \in S_n$ eine Permutation und wähle eine Darstellung $\sigma = \tau_1 \circ \cdots \circ \tau_k$ von σ als Komposition von Transpositionen.

(a) Ist k gerade (d.h. $k \equiv 0 \mod 2$), so heißt σ eine **gerade** Permutation.

(b) Ist k ungerade (d.h. $k \equiv 1 \mod 2$), so heißt σ eine **ungerade** Permutation.

Beispiel 3.1.23

(a) Jede Transposition ist ungerade.

(b) Die identische Abbildung Id (d.h. das neutrale Element von S_n) ist gerade. (Für $n > 1$ ist z.B. $\mathrm{Id} = (1,2)(1,2)$.)

(c) $\sigma = (1,4)(4,6)(6,3)(2,7) \in S_7$ ist eine gerade Permutation.

Lemma 3.1.24

Die Abbildung

$$\begin{array}{rccl} \varepsilon\colon & (S_n, \circ) & \longrightarrow & (\{-1,1\}, \cdot) \\ & \sigma & \mapsto & \varepsilon(\sigma) = \begin{cases} 1\,, & \text{wenn } \sigma \text{ gerade ist,} \\ -1\,, & \text{wenn } \sigma \text{ ungerade ist} \end{cases} \end{array}$$

ist ein Gruppen-Homomorphismus.

Beweis: Seien $\sigma_1, \sigma_2 \in S_n$ zwei Permutationen. Dann gibt es vier Möglichkeiten:

(1) σ_1, σ_2 gerade $\Longrightarrow \sigma_1 \circ \sigma_2$ gerade $\Longrightarrow \varepsilon(\sigma_1 \circ \sigma_2) = 1 = 1 \cdot 1 = \varepsilon(\sigma_1) \cdot \varepsilon(\sigma_2)$.

(2) σ_1, σ_2 ungerade $\Longrightarrow \sigma_1 \circ \sigma_2$ gerade $\Longrightarrow \varepsilon(\sigma_1 \circ \sigma_2) = 1 = (-1) \cdot (-1) = \varepsilon(\sigma_1) \cdot \varepsilon(\sigma_2)$.

(3) σ_1 gerade und σ_2 ungerade $\Longrightarrow \sigma_1 \circ \sigma_2$ ungerade $\Longrightarrow \varepsilon(\sigma_1 \circ \sigma_2) = -1 = 1 \cdot (-1) = \varepsilon(\sigma_1) \cdot \varepsilon(\sigma_2)$.

(4) σ_1 ungerade und σ_2 gerade $\Longrightarrow \sigma_1 \circ \sigma_2$ ungerade $\Longrightarrow \varepsilon(\sigma_1 \circ \sigma_2) = -1 = (-1) \cdot 1 = \varepsilon(\sigma_1) \cdot \varepsilon(\sigma_2)$. ∎

Definition 3.1.25 (*Signum, alternierende Gruppe*)

Der Gruppen-Homomorphismus $\varepsilon : S_n \longrightarrow \{-1,1\}$ vom Lemma 3.1.24 heißt **Signum**. Außerdem heißt

$$A_n := \ker(\varepsilon) = \{\sigma \in S_n \mid \varepsilon(\sigma) = 1\}$$

alternierende Gruppe vom Grad n.

Anmerkung 3.1.26

Die alternierende Gruppe A_n ist eine Untergruppe von S_n, denn der Kern eines Gruppen-Homomorphismus ist immer eine Untergruppe nach Lemma 3.1.12(d).

Beispiel 3.1.27

In S_3 sind Id, $(1,2,3) = (1,2)(2,3)$, $(1,3,2) = (1,3)(3,2)$ gerade und $(1,2)$, $(1,3)$, $(2,3)$ ungerade. Daraus folgt

$$A_3 = \{\mathrm{Id}, (1,2,3), (1,3,2)\}\,.$$

Wir werden später beweisen, dass A_n für alle $n \geq 2$ genau halb so viele Elemente wie S_n hat.

Schließlich sehen wir, dass symmetrische Gruppen besonders wichtige Gruppen sind, da jede Gruppe G als Untergruppe einer symmetrischen Gruppen aufgefasst werden kann:

Satz 3.1.28 (*Satz von Cayley*)

Jede Gruppe G ist isomorph zu einer Untergruppe der symmetrischen Gruppe $S(G)$.
Inbesondere für $|G| < \infty$ können wir G als Untergruppe von S_n auffassen, wobei $n = |G|$ ist.

Beweis: Zunächst definieren wir ein Gruppen-Homomorphismus, indem wir setzen

$$\begin{array}{rccl} \varphi\colon & G & \longrightarrow & S(G) \\ & g & \mapsto & \varphi(g) := \begin{pmatrix} G & \longrightarrow & G \\ h & \mapsto & g \circ h \end{pmatrix}. \end{array}$$

(Siehe Blatt 6.)
Der Kern von φ ist

$$\ker(\varphi) = \{g \in G \mid \varphi(g) = \mathrm{Id}\} = \{g \in G \mid g \circ h = h \,\forall\, h \in G\}.$$

Aber $g \circ h = h \Rightarrow g = e$ nach der Kürzungsregel, da $h = e \circ h$ ist. Also ist $\ker(\varphi) = \{e\}$ und φ ist injektiv nach Lemma 3.1.12(d). Somit gilt

$$G \cong \mathrm{Bild}(\varphi)$$

und $\mathrm{Bild}(\varphi) = \varphi(G)$ ist eine Untergruppe der symmetrischen Gruppe $S(G)$ nach Lemma 3.1.12(d).
Schließlich ist G endlich, d.h. $|G| =: n < \infty$, so sind $S(G)$ und S_n isomorph. (Wir können einfach die Elemente von G nummerieren, d.h. $G = \{g_1, g_2, \ldots, g_n\}$, und die Mengen $\{g_1, g_2, \ldots, g_n\}$ und $\{1, 2, \ldots, n\}$ identifizieren, indem wir g_i mit i ersetzen.) Damit können wir G als Untergruppe von S_n auffassen. ∎

3.1.5 Hauptbeispiel 2: Die Gruppe der Restklassen modulo n

Sei $n \in \mathbb{N}$ eine Natürliche Zahl.

Erinnerung: Für $a, b \in \mathbb{Z}$ heißt a *kongruent zu* b *modulo* n, wenn $n|(a-b)$. In Zeichen schreiben wir

$$a \equiv b \mod n.$$

Dies ist eine Äquivalenzrelation. Die Äquivalenzklasse von a ist

$$\overline{a} = \{b \in \mathbb{Z} \mid a \equiv b \mod n\} = \{a + k \cdot n \mid k \in \mathbb{Z}\} =: a + n\mathbb{Z}$$

und heißt **Restklasse** von a modulo n.
Somit ist $a \equiv b \mod n \Leftrightarrow \overline{a} = \overline{b}$. Insbesondere gilt

$$\begin{array}{rl} \overline{0} & = \overline{n} = \overline{2n} = \overline{3n} = \ldots \\ \overline{1} & = \overline{1+n} = \overline{1+2n} = \overline{1+3n} = \ldots \\ \overline{2} & = \overline{2+n} = \overline{2+2n} = \overline{2+3n} = \ldots \\ \cdots & = \cdots \\ \overline{n-1} & = \overline{(n-1)+n} = \overline{(n-1)+2n} = \overline{(n-1)+3n} = \ldots. \end{array}$$

Somit gibt es genau n verschiedenen Restklassen modulo n:

$$\overline{0}, \overline{1}, \ldots, \overline{n-1}.$$

Lemma-Definition 3.1.29 (*Gruppe der Restklassen modulo n*)

Sei $n \in \mathbb{N}$. Die Menge

$$\mathbb{Z}/n := \{\overline{0}, \overline{1}, \ldots, \overline{n-1}\}$$

der Restklassen modulo n zusammen mit der Verknüpfung (Addition)

$$\begin{array}{rccc} + : & \mathbb{Z}/n \times \mathbb{Z}/n & \longrightarrow & \mathbb{Z}/n \\ & (\overline{a}, \overline{b}) & \mapsto & \overline{a} + \overline{b} := \overline{a+b}\,, \end{array}$$

bildet eine Gruppe, die **Gruppe der Restklassen modulo** n (mit neutralem Element $\overline{0}$ und Inversem $-\overline{a} = \overline{-a}$ von $\overline{a} \in \mathbb{Z}/n$).

Beweis:

- Da $\overline{a} + \overline{b} := \overline{a+b}$ in Termen von Äquivalenzklassen definiert ist, müssen wir zunächst zeigen, dass diese Verknüpfung wohldefiniert ist, d.h. nicht von der Wahl der Repräsentanten a und b abhängt: anders gesagt für $\overline{a_1} = \overline{a_2}$ und $\overline{b_1} = \overline{b_2}$ müssen wir zeigen, dass $\overline{a_1} + \overline{a_2} = \overline{b_1} + \overline{b_2}$.

  Aber aus $\overline{a_1} = \overline{a_2}$ und $\overline{b_1} = \overline{b_2}$ folgen $a_1 - a_2 = n \cdot k_1$ und $b_1 - b_2 = n \cdot k_2$ mit Zahlen $k_1, k_2 \in \mathbb{Z}$ und somit gilt

  $$\overline{a_1} + \overline{b_1} = \overline{a_1 + b_1} = \overline{a_2 + n \cdot k_1 + b_2 + n \cdot k_2} = \overline{a_2 + b_2 + n \cdot (k_1 + k_2)} = \overline{a_2 + b_2} = \overline{a_2} + \overline{b_2}\,.$$

- Die Addition in $\mathbb{Z}/n$ ist assoziativ, da die Addition in $\mathbb{Z}$ schon assoziativ ist $\Longrightarrow$ **(G1)** gilt.
- Das neutrale Element ist die Restklasse von 0: $\overline{a} + \overline{0} = \overline{a+0} = \overline{a}$ und $\overline{0} + \overline{a} = \overline{0+a} = \overline{a}$ für alle $\overline{a} \in \mathbb{Z}/n \Longrightarrow$ **(G2)** gilt.
- Das inverse Element von $\overline{a} \in \mathbb{Z}/n$ ist $\overline{-a}$, da $\overline{a} + \overline{-a} = \overline{a-a} = \overline{0}$ und $\overline{-a} + \overline{a} = \overline{-a+a} = \overline{0}$ gelten $\Longrightarrow$ **(G3)** gilt. ■

Beispiel 3.1.30

Für $n = 3$ ist $\mathbb{Z}/3 = \{\overline{0}, \overline{1}, \overline{2}\}$ mit

$$\begin{aligned} \overline{0} &= \{\ldots, -6, -3, 0, 3, 6, \ldots\} = 0 + 3\mathbb{Z} = 3\mathbb{Z} \\ \overline{1} &= \{\ldots, -5, -2, 1, 4, 7, \ldots\} = 1 + 3\mathbb{Z} \\ \overline{2} &= \{\ldots, -4, -1, 2, 5, 8, \ldots\} = 2 + 3\mathbb{Z} \end{aligned}$$

Siehe auch Beispiel 2.1.8.

(**Beachte**: die Restklasse $\overline{0} = 3\mathbb{Z}$ ist eine Untergruppe von $\mathbb{Z}$, aber die Restklassen $\overline{1} = 1 + 3\mathbb{Z}$ und $\overline{2} = 2 + 3\mathbb{Z}$ sind keine Untergruppen von $\mathbb{Z}$ nach Satz 3.1.8.)

Die Verknüpfung kann man z.B. durch die **Gruppentafel** beschreiben:

$+$	$\overline{0}$	$\overline{1}$	$\overline{2}$
$\overline{0}$	$\overline{0}$	$\overline{1}$	$\overline{2}$
$\overline{1}$	$\overline{1}$	$\overline{2}$	$\overline{0}$
$\overline{2}$	$\overline{2}$	$\overline{0}$	$\overline{1}$

Beispielsweise gilt $\overline{2} + \overline{2} = \overline{2+2} = \overline{4} = \overline{1}$.

Beispiel 3.1.31 (*Untergruppen von* $\mathbb{Z}/n$)

(a) Für jeden Teiler a von n ist die Teilmenge

$$\{\overline{0}, \overline{a}, \overline{2a}, \ldots, \overline{(d-1)a}\} \subset \mathbb{Z}/n$$

mit $d := \frac{n}{a}$ eine Untergruppe von $\mathbb{Z}/n$. (Siehe die Aufgaben.)
Z.B. für $n = 6$ liefert $a = 2$ ($\Rightarrow d = 3$) die Untergruppe

$$\{\overline{0}, \overline{2}, \overline{4}\} \subset \mathbb{Z}/6$$

und $a = 3$ ($\Rightarrow d = 2$) liefert die Untergruppe

$$\{\overline{0}, \overline{3}\} \subset \mathbb{Z}/6\,.$$

Ausserdem liefert $a = 1$ ($\Rightarrow d = 6$) die ganze Gruppe $\mathbb{Z}/6$ selbst und $a = 6$ ($\Rightarrow d = 1$) liefert die *triviale* Untergruppe $\{\overline{0}\} \subset \mathbb{Z}/6$.

(b) Die Untergruppe $\{\overline{0}, \overline{2}, \overline{4}\}$ von $\mathbb{Z}/6$ kann man mit der Gruppe $\mathbb{Z}/3$ *identifizieren*, da die Abbildung

$$\begin{array}{rccc} \varphi: & (\{\overline{0}, \overline{2}, \overline{4}\}, +) & \longrightarrow & (\mathbb{Z}/3, +) \\ & \overline{0} = 0 + 6\mathbb{Z} & \mapsto & \overline{0} = 0 + 3\mathbb{Z} \\ & \overline{2} = 2 + 6\mathbb{Z} & \mapsto & \overline{1} = 1 + 3\mathbb{Z} \\ & \overline{4} = 4 + 6\mathbb{Z} & \mapsto & \overline{2} = 2 + 3\mathbb{Z} \end{array}$$

ein Gruppen-Isomorphismus ist.
(Es ist klar, dass φ bijektiv ist und es gilt $\varphi(\overline{a} + \overline{b}) = \varphi(\overline{a}) + \varphi(\overline{b})$ $\forall\ \overline{a}, \overline{b} \in \{\overline{0}, \overline{2}, \overline{4}\}$.)

Im Kapitel 2 haben wir den Chinesischen Restsatz für Kongruenzgleichungen in $\mathbb{Z}$ bewiesen. (Siehe Satz 2.4.1.) Mithilfe der Gruppen der Restklassen modulo n können wir diesen Satz umformulieren, wie folgt:

Satz 3.1.32 (*Chinesischer Restsatz in Termen der Gruppentheorie*)

Sind $m, n \in \mathbb{N}$ teilerfremd (d.h. ggT$(m, n) = 1$), so gilt

$$\mathbb{Z}/mn \cong \mathbb{Z}/m \times \mathbb{Z}/n\,.$$

Beweis (Sketch): Ein Gruppen-Isomormisphmus zwischen $\mathbb{Z}/mn$ und $\mathbb{Z}/m \times \mathbb{Z}/n$ erhalten wir durch die Abbildung

$$\begin{array}{rccc} \varphi: & \mathbb{Z}/mn & \longrightarrow & \mathbb{Z}/m \times \mathbb{Z}/n \\ & a + mn\mathbb{Z} & \mapsto & (a + m\mathbb{Z}, a + n\mathbb{Z})\,. \end{array}$$

(Beachte: Mit der "quer"-Notation für die Restklassen würden wir $\varphi(\overline{a}) = (\overline{a}, \overline{a})$ schreiben, aber dies ist verwirrend, da die Restklassen von a in $\mathbb{Z}/m$, $\mathbb{Z}/n$ und $\mathbb{Z}/mn$ nicht die gleichen Mengen bezeichnen.)

Es muss nun gezeigt werden, dass die Abbildung φ:

- wohldefiniert,
- ein Gruppen-Homomorphismus,
- injektiv und surjektiv ist. (Dies ist eine Anwendung vom Satz 2.4.1.) Siehe die Aufgaben (Blatt 6). ■

3.2 Operationen von Gruppen auf Mengen und Faktorgruppen

3.2.1 Operationen von Gruppen auf Mengen

Ziel: Die Struktur der Gruppen und Mengen, wie z.B. geometrische Objekte und ihre Symmetrien, besser verstehen!

Sei stets $(G, \circ)$ eine Gruppe.

Definition 3.2.1 (*Operation einer Gruppe auf einer Menge*)

Sei M eine nicht-leere Menge. Eine **Operation von** G **auf** M ist eine Abbildung

$$\begin{array}{ccc} G \times M & \longrightarrow & M \\ (g, m) & \mapsto & g.m \end{array}$$

mit folgenden Eigenschaften:

(GM1) $e.m = m \quad \forall\, m \in M$;

(GM2) $(g \circ h).m = g.(h.m) \quad \forall\, g, h \in G$ und $\forall\, m \in M$.

Wir sagen auch, dass G **auf** X **operiert**.

(In dieser Definition ist e das neutrale Element von G.)

Beispiel 3.2.2

(a) Die symmetrische Gruppe S_n operiert auf der Menge $M = \{1, 2, \ldots, n\}$ durch

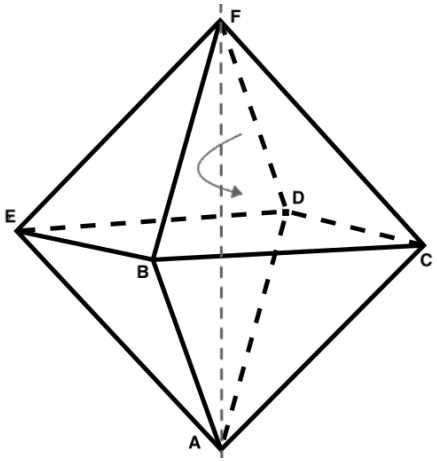
$$\begin{array}{ccc} S_n \times \{1, 2, \ldots, n\} & \longrightarrow & \{1, 2, \ldots, n\} \\ (\sigma, a) & \mapsto & \sigma.a = \sigma(a), \end{array}$$

da $\mathrm{Id}.a = \mathrm{Id}(a) = a$ für alle $a \in \{1, 2, \ldots, n\}$ ist $\Longrightarrow$ **(GM1)** gilt, und es gilt

$$(\sigma \circ \tau).a = (\sigma \circ \tau)(a) = \sigma(\tau(a)) = \sigma.(\tau.a) \quad \forall\, a \in \{1, 2, \ldots, n\}$$

$\Longrightarrow$ **(GM2)** gilt.

(b) Die Gruppe $G = \mathbb{Z}/4$ Operiert auf dem regulären Oktaeder



durch Drehungen:

- Die Restklasse $\overline{1}$ operiert durch eine Drehung um $+90°$, d.h.

  $\overline{1}.B = C$, $\overline{1}.C = D$, $\overline{1}.D = E$, $\overline{1}.E = B$ und A und F sind fest ($\overline{1}.A = A$, $\overline{1}.F = F$).

- Die Restklasse $\overline{2}$ operiert durch eine Drehung um $+180°$, d.h.

  $\overline{2}.B = D$, $\overline{2}.C = E$, $\overline{2}.D = B$, $\overline{2}.E = C$ und A und F sind fest.

- Die Restklasse $\overline{3}$ operiert durch eine Drehung um $+270°$, d.h.

  $\overline{3}.B = E$, $\overline{3}.C = B$, $\overline{3}.D = C$, $\overline{3}.E = D$ und A und F sind fest.

- Die Restklasse $\overline{0} = \overline{4}$ (das neutrale Element in $G = \mathbb{Z}/4$) operiert durch eine Drehung um $+360° = 0°$. Damit sind die Ecken A, B, C, D, E, F fest.

(Siehe auch `Beamer_Woche_7.pdf`.)

(c) Die Gruppe G operiert auf der Menge $M = G$ selbst durch die Verknüpfung:

$$\begin{array}{ccc} G \times G & \longrightarrow & G \\ (g, m) & \mapsto & g.m := g \circ m \end{array}$$

Um Operationen von Gruppen auf Mengen zu verstehen, studieren wir einerseits die Elemente der Menge, die fest sind, und anderseits die Elemente, die sich bewegen:

Definition 3.2.3 (*Bahn, Stabilisator*)

Sei G eine Gruppe, die auf einer Menge M operiert, und sei $m \in M$. Dann ist

(i) $G.m := \{g.m \mid g \in G\} \subseteq M$ die **Bahn** von m, und

(ii) $\mathrm{Stab}_G(m) := \{g \in G \mid g.m = m\}$ der **Stabilisator** von m in G.

Bemerkung 3.2.4

Der Stabilisator $\mathrm{Stab}_G(m)$ von $m \in M$ in G ist eine Untergruppe von G.

Beweis: Wir überprüfen, dass $\mathrm{Stab}_G(m)$ die drei Bedingungen der Definition einer Untergruppe erfüllt:

(i) $e.m = m$ nach (GM1) $\Rightarrow e \in \mathrm{Stab}_G(m)$.

(ii) $g, h \in \mathrm{Stab}_G(m) \Rightarrow (g \circ h).m \overset{(GM2)}{=} g.(h.m) = g.m = m$, also $g \circ h \in \mathrm{Stab}_G(m)$.

(iii) $g \in \mathrm{Stab}_G(m) \Rightarrow m \overset{(GM1)}{=} e.m = (g^{-1} \circ g).m \overset{(GM2)}{=} g^{-1}.(g.m) = g^{-1}.m$, also $g^{-1} \in \mathrm{Stab}_G(m)$. ■

Beispiel 3.2.5

(a) Betrachte erneut die Operation der symmetrischen Gruppe S_n auf der Menge $M = \{1, 2, \ldots, n\}$, d.h.

$$\begin{array}{ccc} S_n \times \{1, 2, \ldots, n\} & \longrightarrow & \{1, 2, \ldots, n\} \\ (\sigma, a) & \mapsto & \sigma.a = \sigma(a)\,. \end{array}$$

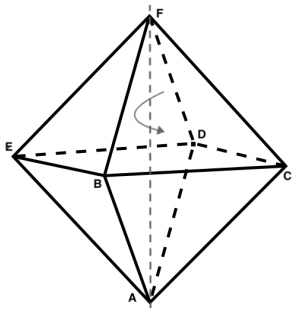
Z.B. ist die Bahn von $a = 1$ die Teilmenge $S_n.1 = \{\sigma.1 \mid \sigma \in S_n\} = \{\sigma(1) \mid \sigma \in S_n\}$. Es gilt

$$\mathrm{Id}(1) = 1,\ (1,2)(1) = 2,\ (1,3)(1) = 3 \ldots \text{ und } (1,n)(1) = n$$

Somit ist $S_n.1 = \{1, 2, \ldots, n\} = M$, d.h. die ganze Menge M.
Der Stabilisator von $a = n$ in S_n ist

$$\mathrm{Stab}_{S_n}(n) := \{\sigma \in S_n \mid \sigma(n) = n\} = S_{n-1}\,.$$

(b) Sei $G \times \{A, B, C, D, E, F\} \longrightarrow \{A, B, C, D, E, F\}$ die Operation der Gruppe $G = \mathbb{Z}/4$ auf dem regulären Oktaeder durch Drehungen vom Beispiel 3.2.2(b).



· Die Ecken A und F sind fest unter dieser Operation, deswegen sind die Bahnen von A und F einfach

$$\mathbb{Z}/4.A = \{A\} \text{ und } \mathbb{Z}/4.F = \{F\}$$

· Anderseits werden die Ecken B, C, D und F unter dieser Operation vertauscht:

$$\overline{0}.B = B,\ \overline{1}.B = C,\ \overline{2}.B = D, \overline{3}.B = D \quad \Longrightarrow \quad \mathbb{Z}/4.B = \{B, C, D, E\}$$

Ähnlich: die Bahnen von C, D und E sind auch die Teilmenge $\{B, C, D, E\}$.

· Die Stabilisatoren der Ecken sind:

$$\begin{aligned}
\mathrm{Stab}_{\mathbb{Z}/4}(A) &= \{\overline{a} \in \mathbb{Z}/4 \mid \overline{a}.A = A\} = \mathbb{Z}/4 \\
\mathrm{Stab}_{\mathbb{Z}/4}(F) &= \{\overline{a} \in \mathbb{Z}/4 \mid \overline{a}.F = F\} = \mathbb{Z}/4 \\
\mathrm{Stab}_{\mathbb{Z}/4}(B) &= \{\overline{a} \in \mathbb{Z}/4 \mid \overline{a}.B = B\} = \{\overline{0}\} \\
\mathrm{Stab}_{\mathbb{Z}/4}(C) &= \{\overline{a} \in \mathbb{Z}/4 \mid \overline{a}.C = C\} = \{\overline{0}\} \\
\mathrm{Stab}_{\mathbb{Z}/4}(D) &= \{\overline{a} \in \mathbb{Z}/4 \mid \overline{a}.D = D\} = \{\overline{0}\} \\
\mathrm{Stab}_{\mathbb{Z}/4}(E) &= \{\overline{a} \in \mathbb{Z}/4 \mid \overline{a}.E = E\} = \{\overline{0}\}
\end{aligned}$$

Siehe auch `Beamer_Woche_7.pdf`.

Anmerkung 3.2.6 (*Eine Äquivalenzrelation*)

Das Bilden der Bahnen definiert eine Äquivalenzrelation $\sim$ auf der Menge M wie folgt: für $m_1, m_2 \in M$ definiere

$$m_1 \sim m_2 \quad \Leftrightarrow \quad \exists\, g \in G \text{ mit } g.m_1 = m_2\,.$$

Somit sind die Äquivalenzklassen genau die Bahnen der Operation von G auf M.

Es folgt, dass je zwei Bahnen $G.m_1$ und $G.m_2$ entweder gleich oder disjunkt sind (siehe Satz 1.5.6 im Skript AGS von J. Böhm).

Weiter nennen wir jedes Element $m \in G.m_1$ einen **Repräsentanten der Bahn** $G.m_1$, denn $G.m = G.m_1$. Ein **vollständiges Repräsentantensystem** der Bahnen ist eine Teilmenge $R \subset M$, sodass jede Bahn $G.m$ genau ein Element von R enthält.

Dann ist M die disjunkte Vereinigung der Bahnen:

$$M = \bigcup_{m \in R} G.m\,,$$

denn eine Äquivalenzrelation partitioniert die Menge in die Äquivalenzklassen.

Beispiel 3.2.7

Die Operation der Gruppe $G = \mathbb{Z}/4$ auf dem regulären Oktaeder partitioniert die Menge der Ecken in 3 Bahnen:

$$\{A, B, C, D, E, F\} = \mathbb{Z}/4.A \cup \mathbb{Z}/4.B \cup \mathbb{Z}/4.F = \{A\} \cup \{B, C, D, E\} \cup \{F\}$$

und $R = \{A, B, F\}$ ist vollständiges Repräsentantensystem der Bahnen.

3.2.2 Die Bahnengleichung

In diesem Abschnitt versuchen wir eine Formel zu entwickeln, um die Elemente der Bahnen einer Operation zu zählen. Diese Formel ist die sogenannte **Bahnengleichung**.

Analog zur Operation einer Gruppe $(G, \circ)$ auf sich selbst (Beispiel 3.2.2(c)) kann man auch die Operation einer Untergruppe $H \leq G$ durch die Verknüpfung betrachten, d.h. die Operation

$$\begin{array}{ccc} H \times G & \longrightarrow & G \\ (h, g) & \mapsto & h.g := h \circ g \end{array}$$

der Untergruppe H auf der Menge G.
Die Bahnen dieser Operation sind die Teilmengen $H \circ g = \{h \circ g \mid h \in H\}$ der Menge G.

Definition 3.2.8 (*Nebenklassen*)

(a) Die Bahnen $H \circ g = \{h \circ g \mid h \in H\}$ der obigen Operation heißen **Rechtsnebenklassen** von G nach H und wir bezeichnen mit

$$G/H := \{H \circ g \mid g \in G\}$$

die Menge aller Rechtsnebenklassen.

(b) Die **Linksnebenklassen** von G nach H sind die Teilmengen $g \circ H = \{g \circ h \mid h \in H\}$.

(c) Falls die **Rechtsnebenklassen** und die **Linksnebenklassen** gleich sind, d.h. $H \circ g = g \circ H$ für alle $g \in G$, so nennen wir diese einfach die **Nebenklassen** von G nach H.
(Es ist Z.B. der Fall, wenn die Gruppe G ablesch ist.)

Beispiel 3.2.9

Sei $H := n\mathbb{Z}$ mit $n \in \mathbb{N}$ eine Untergruppe von $(\mathbb{Z}, +)$. (Erinnerung: alle Untergruppen von $\mathbb{Z}$ haben die Form $n\mathbb{Z}$.) In diesem Fall ist die Operation von H auf $\mathbb{Z}$

$$\begin{array}{ccc} n\mathbb{Z} \times \mathbb{Z} & \longrightarrow & \mathbb{Z} \\ (n \cdot k, a) & \mapsto & n \cdot k + a = a + n \cdot k\,. \end{array}$$

Da $\mathbb{Z}$ abelsch ist, sind die Bahnen dieser Operation die Nebenklassen

$$\{a + n \cdot k \mid k \in \mathbb{Z}\} = a + n\mathbb{Z} = \overline{a}\,,$$

d.h. genau die Restklassen modulo n.
In diesem Fall ist die Menge der Nebenklassen $\mathbb{Z}/n\mathbb{Z} = \mathbb{Z}/n$, die Gruppe der Restklassen modulo n.

Satz 3.2.10 (*Indexformel, Satz von Lagrange*)

Sei $H \leq G$ eine Untergruppe. Dann gilt

$$|G| = |H| \cdot |G/H|\,.$$

Insbesondere in einer endlichen Gruppe G teilt die Ordnung jeder Untergruppe die Ordnung von G.

Beweis: Wir bemerken zunächst, dass jede Rechtsnebenklasse von G nach H genauso viele Elemente wie H hat, da die Abbildung

$$\begin{array}{ccc} H & \longrightarrow & H \circ g \\ h & \mapsto & h \circ g \end{array}$$

bijektiv ist. (Aufgabe.) Anders gesagt ist $|H| = |H \circ g|$ für alle $g \in G$.
Nach Anmerkung 3.2.6 ist die Menge G die disjunkte Vereinigung aller Bahnen der Operation

$$\begin{array}{ccc} H \times G & \longrightarrow & G \\ (h, g) & \mapsto & h.g := h \circ g \end{array}$$

d.h.

$$G = \bigcup_{g \in R} H \circ g \,,$$

wobei $R \subseteq G$ ein vollständiges Repräsentantensystem der Bahnen (= Rechtsnebenklassen) ist. Also falls $|G| < \infty$ gilt

$$|G| = \sum_{g \in R} |H \circ g| = \sum_{g \in R} |H| = |R| \cdot |H| = |G/H| \cdot |H| \,.$$

Ist $|G| = \infty$, dann auch $|G/H| = \infty$ oder $|H| = \infty$ und es gilt $\infty = |G| = |H| \cdot |G/H| = \infty$. ■

Damit können wir die gesuchte Formel formulieren und beweisen:

Satz 3.2.11 (*Bahnengleichung*)

Sei $G \times M \longrightarrow M, (g, m) \mapsto g.m$ eine Operation einer Gruppe G auf einer Menge M. Dann gelten:

(a) Ist $m \in M$, so ist die Abbildung

$$\begin{array}{ccc} G/\mathrm{Stab}_G(m) & \longrightarrow & G.m \\ \mathrm{Stab}_G(m) \circ g & \mapsto & g^{-1}.m \end{array}$$

bijektiv. Insbesondere ist $|G/\mathrm{Stab}_G(m)| = |G.m|$.

(b) **Bahnformel:** Ist $m \in M$, so gilt $|G.m| = \frac{|G|}{|\mathrm{Stab}_G(m)|}$.

(c) **Bahnengleichung:** Es gilt

$$|M| = \sum_{m \in R} \frac{|G|}{|\mathrm{Stab}_G(m)|} \,,$$

wobei R ein vollständiges Repräsentantensystem der Bahnen ist.

Beweis:

(a)
- Die Abbildung ist tatsächlich wohldefiniert (Aufgabe).
- Die Abbildung ist offenbar surjektiv nach Definition.
- Die Abbildung ist injektiv, denn für $g_1, g_2 \in G$

$$g_1^{-1}.m = g_2^{-1}.m \;\Rightarrow\; (g_1 \circ g_1^{-1}).m = (g_1 \circ g_2^{-1}).m \;\Rightarrow\; m = (g_1 \circ g_2)^{-1}.m \;\Rightarrow\; g_1 \circ g_2^{-1} \in \mathrm{Stab}_G(m) \,.$$

Somit ist

$$g_2^{-1}.m = (e \circ g_2^{-1}).m = (g_1^{-1} \circ g_1 \circ g_2^{-1}).m = g_1^{-1}.((g_1 \circ g_2^{-1}).m) = g_1^{-1}.m \,.$$

(b) Nach (a) gilt $|G/\mathrm{Stab}_G(m)| = |G.m|$ und nach der Indexformel ist $|G| = |\mathrm{Stab}_G(m)| \cdot |G/\mathrm{Stab}_G(m)|$. Damit gilt:

$$|G| = |\mathrm{Stab}_G(m)| \cdot |G.m| \qquad \Longrightarrow \qquad |G.m| = \frac{|G|}{|\mathrm{Stab}_G(m)|}$$

(c) Nach Anmerkung 3.2.6 ist die Menge M die disjunkte Vereinigung der Bahnen

$$M = \bigcup_{m \in R} G.m$$

und zusammen mit (b) gilt

$$|M| = \sum_{m \in R} |G.m| = \sum_{m \in R} \frac{|G|}{|\mathrm{Stab}_G(m)|}\,.$$

■

Beispiel 3.2.12

Nach Beispiel 3.2.2(b) und Beispiel 3.2.5(b) gilt für die Operation der Gruppe $G = \mathbb{Z}/4$ auf dem regulären Oktaeder

$$M = \{A, B, C, D, E, F\} = \mathbb{Z}/4.A \cup \mathbb{Z}/4.B \cup \mathbb{Z}/4.F$$

(disjunkte Vereinigung der Bahnen) und die Bahnengleichung ist

$$|M| = \frac{|\mathbb{Z}/4|}{|\mathrm{Stab}_{\mathbb{Z}/4}(A)|} + \frac{|\mathbb{Z}/4|}{|\mathrm{Stab}_{\mathbb{Z}/4}(B)|} + \frac{|\mathbb{Z}/4|}{|\mathrm{Stab}_{\mathbb{Z}/4}(F)|} = \frac{|\mathbb{Z}/4|}{|\mathbb{Z}/4|} + \frac{|\mathbb{Z}/4|}{|\{\overline{0}\}|} + \frac{|\mathbb{Z}/4|}{|\mathbb{Z}/4|} = 1 + 4 + 1 = 6\,.$$

3.2.3 Faktorgruppen

Wir studieren nun die Untergruppen $H \leq G$ so, dass die Menge der Rechtsnebenklassen

$$G/H = \{H \circ g \mid g \in G\}$$

(siehe Definition 3.2.8) wieder eine Gruppe ist.

In Beispiel 3.2.9 haben wir gesehen, dass es z.B. der Fall ist, wenn $G = \mathbb{Z}$ und $H = n\mathbb{Z}$ sind, da die Menge der Rechtsnebenklassen $\mathbb{Z}/n\mathbb{Z}$ mit der Gruppe $\mathbb{Z}/n$ der Restklassen modulo n übereinstimmt. Aber es ist nicht wahr im Allgemeinen, dass die Menge der Rechtsnebenklassen G/H zu einer Gruppe wird.

Satz-Definition 3.2.13

Sei $(G, \circ)$ eine Gruppe und sei $H \leq G$ eine Untergruppe. Dann sind die folgenden Bedingungen äquivalent:

(a) Die Menge $G/H = \{H \circ g \mid g \in G\}$ der Rechtsnebenklassen ist eine Gruppe mit Verknüpfung

$$\begin{array}{rccl} \cdot\colon & G/H \times G/H & \longrightarrow & G/H \\ & (H \circ g_1, H \circ g_2) & \mapsto & (H \circ g_1) \cdot (H \circ g_2) := H \circ (g_1 \circ g_2)\,, \end{array}$$

neutralem element $H \circ e = H$ und inversem Element $(H \circ g)^{-1} = H \circ g^{-1}$ von $H \circ g \in G/H$.

(b) Die Rechtsnebenklassen und die Linksnebenklassen stimmen übereien, d.h. $H \circ g = g \circ H$ für alle $g \in G$.

Eine Untergruppe $H \leq G$, die die äquivalenten Bedingungen (a) und (b) erfüllt, heißt **Normalteiler** von G und die zugehörige Gruppe G/H heißt die **Faktorgruppe** von G nach H.

Anmerkung 3.2.14

In Bedingung (b) gilt:

$H \circ g = g \circ H$ für alle $g \in G \quad \Longleftrightarrow \quad H = g \circ H \circ g^{-1} = \{g \circ h \circ g^{-1} \mid h \in H\}$ für alle $g \in G$.

Deswegen können wir Bedingung (b) mit folgender Bedingung

$$\text{(b')} \qquad \text{für alle } g \in G \text{ und } h \in H \text{ ist } g \circ h \circ g^{-1} \in H$$

ersetzten, falls notwendig.

Beweis:

(a)⇒(b'): Wir nehmen an, dass $(G/H, \cdot)$ eine Gruppe ist. Sei $g \in G$. Dann ist $H \circ g^{-1} = H \circ (h \circ g^{-1})$ für alle $h \in H$ (dieselbe Rechtsnebenklasse) und somit gilt

$$H \circ e = (H \circ g) \cdot (H \circ g^{-1}) = (H \circ g) \cdot (H \circ (h \circ g^{-1}))$$

wegen der wohldefiniertheit der Verknüpfung. Damit ist

$$H = H \circ e = (H \circ g) \cdot (H \circ (h \circ g^{-1})) = H \circ (g \circ h \circ g^{-1})$$

und wir erhalten $g \circ h \circ g^{-1} \in H$ für alle $h \in H$.

(b)⇒(a): Sobald die Verknüpfung $\cdot : G/H \times G/H \longrightarrow G/H$ wohldefiniert ist, kann man genauso wie im Beweis von Lemma-Definition 3.1.29 zeigen, dass **(G1)**, **(G2)** und **(G3)** gelten.
(Die Argumente sind gleich: ersetze einfach G/H mit $\mathbb{Z}/n = \mathbb{Z}/n\mathbb{Z}$, $\cdot$ mit $+$, $H \circ g$ mit $\overline{a} = a + n\mathbb{Z} = n\mathbb{Z} + a$, e mit 0 und $(H \circ g)^{-1}$ mit $-\overline{a}$.)

Deswegen müssen wir zeigen, dass $\cdot : G/H \times G/H \longrightarrow G/H$ wohldefiniert ist, wenn (b) gilt.

Also nehmen wir an, dass $H \circ g = g \circ H$ für alle $g \in G$ gilt. Seien $g_1, g_2, g_1', g_2' \in G$ so, dass $H \circ g_1 = H \circ g_1'$ und $H \circ g_2 = H \circ g_2'$ gilt. Dann ist zu zeigen, dass $(H \circ g_1) \cdot (H \circ g_2) = (H \circ g_1') \cdot (H \circ g_2')$ ist.
Nach (b) gilt $H \circ g_1 = g_1 \circ H$ und $H \circ g_1' = g_1' \circ H$. Damit erhalten wir

$$\begin{aligned}
(H \circ g_1) \cdot (H \circ g_2) &= H \circ (g_1 \circ g_2) \\
&= H \circ H \circ g_1 \circ g_2 \\
&= H \circ g_1 \circ H \circ g_2 \\
&= H \circ g_1' \circ H \circ g_2' \\
&= H \circ H \circ g_1' \circ g_2' \\
&= H \circ (g_1' \circ g_2') = (H \circ g_1') \cdot (H \circ g_2').
\end{aligned}$$

■

Beispiel 3.2.15

(a) Die Untergruppe $H = \{e\}$ von G ist stets ein Normalteiler. Die zugehörige Faktorgruppe ist $G/H = \{\{e\} \circ g \mid g \in G\}$, also die Gruppe G selbst.

(b) Die Untergruppe $H = G$ von G ist stets ein Normalteiler. Die zugehörige Faktorgruppe ist $G/G = \{G \circ e\}$, die nur eine Nebenklasse enthält.

(c) In $\mathbb{Z}$ ist jede Untergruppe $H = n\mathbb{Z}$ ein Normalteiler, da $\mathbb{Z}$ abelsch ist. Die zugehörige Faktorgruppe ist $\mathbb{Z}/n\mathbb{Z} = \mathbb{Z}/n$, d.h. die Gruppe der Restklassen modulo n.

(d) (Gegenbeispiel) In $G = S_3$ ist die Untergruppe $H_1 = \{\mathrm{Id}, (1,2)\}$ kein Normalteiler, da $(2,3) \circ H_1 = \{(2,3), (1,3,2)\}$ und $H_1 \circ (2,3) = \{(2,3), (1,2,3)\}$.

Lemma 3.2.16

Ist $\varphi : G \longrightarrow F$ ein Gruppen-Homomorphismus, so ist $\ker(\varphi)$ ein Normalteiler von G. Insbesondere ist die Menge der Nebenklassen $G/\ker(\varphi)$ stets eine Gruppe.

Beweis: Setze $H := \ker(\varphi)$. Seien $g \in G$ und $h \in H$. Dann ist $\varphi(h) = e_F$ nach Definition des Kerns und es gilt

$$\varphi(g \circ h \circ g^{-1}) = \varphi(g) \circ \underbrace{\varphi(h)}_{=e_F} \circ \varphi(g)^{-1} = \varphi(g) \circ e_F \circ \varphi(g)^{-1} = \varphi(g) \circ \varphi(g)^{-1} = e_F \,.$$

Somit ist $g \circ h \circ g^{-1} \in \ker(\varphi) = H$ und Bedingung (b') gilt. Also ist $\ker(\varphi)$ ein Normalteiler von G und $G/\ker(\varphi)$ ist eine Gruppe nach Satz-Definition 3.2.13. ■

Satz 3.2.17 (*Homomorphiesatz*)

Sei $\varphi : G \longrightarrow F$ ein Gruppen-Homomorphismus. Dann gilt

$$G/\ker(\varphi) \cong \mathrm{Bild}(\varphi) \,.$$

Beweis (Sketch): Wir definieren einen Gruppen-Isomorphismus

$$\begin{array}{rccc} \overline{\varphi}: & G/\ker(\varphi) & \longrightarrow & \mathrm{Bild}(\varphi) \\ & \ker(\varphi) \circ g & \mapsto & \varphi(g) \ . \end{array}$$

■

Beispiel 3.2.18

Nach Lemma 3.2.16 ist die alternierende Gruppe A_n stets ein Normalteiler von S_n, da A_n als Kern des Signums

$$\varepsilon : S_n \longrightarrow \{-1, 1\}, \sigma \mapsto \varepsilon(\sigma)$$

definiert wird. Weiter ist das Signum surjektiv nach Definition und somit ist $\mathrm{Bild}(\varphi) = \{-1, 1\}$. Nach dem Homomorphiesatz gilt nun

$$S_n/A_n \cong \{-1, 1\} \,.$$

Somit ist

$$|S_n/A_n| = |\{-1, 1\}| = 2$$

und nach der Indexformel ist $|S_n| = |A_n| \cdot |S_n/A_n|$. Daraus folgt

$$|A_n| = \frac{1}{2}|S_n| \,.$$

3.2.4 Hauptbeispiel 3: Die zyklischen Gruppen

Mit dem Homomorphiesatz können wir eine wichtige Familie von Gruppen klassifizieren: Die sogenannten *zyklischen Gruppen*.

Definition 3.2.19 (*Erzeugnis, Ordnung eines Elements, zyklische Gruppe*)

(a) Für eine nicht-leere Teilmenge E einer Gruppe $(G, \circ)$ definiert man $\langle E \rangle$ als die kleinste Untergruppe von G, die alle Elemente von E enthält. Diese Untergruppe nennt man **das Erzeugnis von** E.

(b) Ist $E = \{g_1, \ldots, g_n\}$ endlich, so schreibt man statt $\langle E \rangle = \langle \{g_1, \ldots, g_n\} \rangle$ kurz $\langle g_1, \ldots, g_n \rangle$.

(c) Ist $E = \{g\}$ (einelementig) für ein Element $g \in G$, so heißt die Untergruppe $\langle g \rangle$ **zyklisch**. Weiter ist $o(g) := |\langle g \rangle|$ die **Ordnung von** g.

(c) Falls G selbst der Form $G = \langle g \rangle$ für ein $g \in G$ ist, so heißt G eine **zyklische Gruppe**.

Anmerkung 3.2.20

(a) Ist $(G, \circ)$ eine Gruppe und $g \in G$, dann setzen wir

$$g^m := \begin{cases} g \circ g \circ \ldots \circ g \quad (m - \text{mal}) & \text{falls } m > 0, \\ e & \text{falls } m = 0, \\ g^{-1} \circ g^{-1} \circ \ldots \circ g^{-1} \quad ((-m) - \text{mal}) & \text{falls } m < 0. \end{cases}$$

Somit ist

$$\langle g \rangle = \{ g^m \mid m \in \mathbb{Z} \},$$

da dies die kleinste Untergruppe von G ist, die g enthält.

(b) Die Indexformel liefert: In einer endlichen Gruppe G ist die Ordnung eines Elements $g \in G$ ein Teiler der Gruppenordnung $|G|$, d.h. $o(g) \mid |G|$.

(c) Jede Gruppe G mit $|G|$ prim ist zyklisch.
Beweis: Die Teiler von $|G|$ sind 1 und $|G|$. Damit erhalten wir aus der Indexformel, dass G nur die Untergruppen $\{e\}$ und G besitzt. Somit ist für jedes $g \in G \setminus \{e\}$ schon $\{e\} \neq \langle g \rangle = G$.

Beispiel 3.2.21 (*Klassifikation zyklischer Gruppen*)

Sei $(G, \circ)$ eine zyklische Gruppe und sei $g \in G$ mit $G = \langle g \rangle$. Wir klassifizieren die zyklischen Gruppen wie folgt:

1. Mithilfe der Anmerkung sehen wir, dass die Abbildung

$$\begin{array}{rccc} \varphi : & (\mathbb{Z}, +) & \longrightarrow & \langle g \rangle = G \\ & m & \mapsto & g^m \end{array}$$

ein surjektiver Gruppen-Homomorphismus ist. Insbesondere ist $\text{Bild}(\varphi) = G$.

2. Ist $o(g)$ unendlich, so ist $\ker(\varphi) = \{m \in \mathbb{Z} \mid g^m = e\} = \{0\} \Rightarrow \varphi$ ist injektiv $\Rightarrow \varphi$ ist bijektiv $\Rightarrow \varphi$ ist ein Gruppen-Isomorphismus, d.h.

$$(\mathbb{Z}, +) \cong (G, \circ).$$

3. Ist $o(g)$ endlich, so ist $\ker(\varphi) = n\mathbb{Z}$ für ein $n > 0$ (da $\ker(\varphi)$ eine Untergruppe ist und alle Untergruppen von $\mathbb{Z}$ sind der Form $n\mathbb{Z}$) und der Homomorphiesatz liefert

$$\begin{array}{ccc} \mathbb{Z}/n\mathbb{Z} = \mathbb{Z}/n & \xrightarrow{\cong} & \langle g \rangle = G \\ \overline{m} & \mapsto & g^m \ . \end{array}$$

   Insbesondere gilt: $g^{|<g>|} = g^n = g^0 = 1$, da $\overline{n} = \overline{0}$ in $\mathbb{Z}/n$.

Somit haben wir gezeigt: *Jede zyklische Gruppe G endlicher Ordnung ist isomorph zu* $(\mathbb{Z}/n, +)$ *mit* $n = |G|$*, jede zyklische Gruppe unendlicher Ordnung ist isomorph zu* $(\mathbb{Z}, +)$.

TEIL III: RINGE

Wir führen jetzt die 2. algebraische Struktur der Vorlesung ein: die Ring-Struktur. Diese besteht aus einer Menge R zusammen mit zwei Verknüpfungen $+$ und $\cdot$, wobei $(R,+)$ eine abelsche Gruppe bildet. Die ganzen Zahlen $\mathbb{Z}$ zusammen mit der üblichen Addition und Multiplikation von Zahlen werden einen Ring bilden, den wir als Prototyp für allgemeinere Ergebnisse nutzen werden.

Analogien zwischen Gruppen und Ringen:

Algebraische Struktur:	Gruppe $(G,\circ)$	$\longleftrightarrow$	Ring $(R,+,\cdot)$
Unterstrukturen:	Untergruppe	$\longleftrightarrow$	Unterring
	Normalteiler	$\longleftrightarrow$	Ideal
Abbildungen:	Gruppen-Homomorphismen	$\longleftrightarrow$	Ring-Homomorphismen
Prototyp-Beispiel:	$(\mathbb{Z},+)$	$\longleftrightarrow$	$(\mathbb{Z},+,\cdot)$
Anderes typisches Beispiel:	Die Gruppe $(\mathbb{Z}/n,+)$ der Restklassen modulo n	$\longleftrightarrow$	Der Ring $(\mathbb{Z}/n,+,\cdot)$ der Restklassen modulo n

Als Anwendung werden wir in diesem Kapitel erste Schritte in der Kryptographie unternehmen.

4.1 Ringe – Grundbegriffe

4.1.1 Ringe, Unterringe, Ring-Homomorphismen

Als erste Aufgabe möchten wir die Begriffe, mit den wir bei den Gruppen gearbeitet haben, zur Welt der Ringen übertragen.

Definition 4.1.1 (*Ring*)

Ein **Ring** (oder **Ring mit Eins**) $(R,+,\cdot)$ ist eine Menge R zusammen mit zwei Verknüpfungen

$$+ : \; R\times R \longrightarrow R, \quad (a,b)\mapsto a+b \qquad \text{(die \textbf{Addition} des Ringes)}$$
$$\cdot : \; R\times R \longrightarrow R, \quad (a,b)\mapsto a\cdot b \qquad \text{(die \textbf{Multiplikation} des Ringes)}$$

für die gilt:

(R1) $(R,+)$ ist eine abelsche Gruppe.
(Dabei bezeichnen wir mit 0 das neutrale Element diser Addition und mit $-a$ das inverse Element von $a\in R$ bzg. der Addition.)

(R2) Die Multiplikation ist **assoziativ**, d.h. $(a\cdot b)\cdot c = a\cdot(b\cdot c) \quad \forall\, a,b,c\in R$.

(R3) Für alle $a, b, c \in R$ gilt die **Distributivität**:

$$\begin{aligned} a \cdot (b + c) &= a \cdot b + a \cdot c \\ (a + b) \cdot c &= a \cdot c + b \cdot c \end{aligned}$$

(R4) **Existenz eines Einselementes (= neutralen Elementes) für die Multiplikation**: Es existiert ein Element $1_R \in R$ mit $1_R \cdot a = a = a \cdot 1_R \quad \forall\, a \in R$.

Gilt zudem für alle $a, b \in R$, $a \cdot b = b \cdot a$ (*Kommutativität*), so nennen wir R ein **kommutativer Ring**.

Definition 4.1.2 (*Körper*)

Ein Ring $(R, +, \cdot)$ heißt **Körper**, wenn folgende Bedingungen gelten:

(K1) $R \neq \{0\}$.

(K2) R ist kommutativ.

(K3) Jedes Element $a \in R \setminus \{0\}$ besitzt ein inverses Element, d.h. ein Element $a^{-1} \in R$ mit $a \cdot a^{-1} = 1_R = a^{-1} \cdot a$.

Beispiel 4.1.3

(a) $(\mathbb{Z}, +, \cdot)$ ist ein kommutativer Ring. (Bedingungen $(R1) - (R4)$ haben wir eigentlich schon in Aufgabe 4, Blatt 3 überprüft.)

(b) $(\mathbb{Z}, +, \cdot)$ ist kein Körper.
Z.B. hat 2 kein inverses Element bzg. der Multiplikation, da $2^{-1} = \frac{1}{2} \notin \mathbb{Z}$. Damit ist **(K2)** nicht erfüllt.

(c) $(\mathbb{Q}, +, \cdot)$, $(\mathbb{R}, +, \cdot)$, $(\mathbb{C}, +, \cdot)$ sind kommutative Ringe. Diese sind sogar Körper, da jedes Element $a \neq 0$ ein inverses Element besitzt: $a^{-1} = \frac{1}{a}$.)

(d) $(\{0\}, +, \cdot)$ ist ein Ring. Dabei muss das Einselement 1_R gleich 0 sein, da die Menge $\{0\}$ nur ein Element hat. Dieser Ring heißt der **Nullring**.

(e) Das kartesische Produkt $R_1 \times R_2$ von zwei Ringen R_1 und R_2 ist ein Ring mit komponentweiser Addition

$$(a_1, a_2) + (b_1, b_2) = (a_1 + b_1, a_2 + b_2)$$

und komponentweiser Multiplikation

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

Das Einselement ist $1_{R_1 \times R_2} = (1_{R_1}, 1_{R_2})$.

Anmerkung 4.1.4 (*Eigenschaften der Ringen*)

(a) Mit derselben Rechnung wie in Lemma 3.1.4 für Gruppen zeigt man, dass das Einselement und multiplikativ inverse Elemente eindeutig sind.

(b) In jedem Ring $(R, +, \cdot)$ gelten die folgenden Rechenregeln:

- $0 \cdot a = 0 = a \cdot 0 \quad \forall\ a \in R$;
- $(-a) \cdot b = a \cdot (-b) = -(a \cdot b) \quad \forall\ a, b \in R$;
- $(-a) \cdot (-b) = a \cdot b \quad \forall\ a, b \in R$.

Definition 4.1.5 (*Unterring*)

Sei $(R, +, \cdot)$ ein Ring. Eine Teilmenge $S \subseteq R$ heißt **Unterring** (oder **Teilring**) von R, wenn $(S, +)$ eine Untergruppe von $(R, +)$ ist, $a \cdot b \in S$ für alle $a, b \in S$ und $1_R \in S$.
(Somit ist $(S, +, \cdot)$ selbst ein Ring.)

(Man sagt auch, dass S bezüglich der Addition und der Multiplikation abgeschlossen sein muss.)

Beispiel 4.1.6

(a) Z.B. ist $(\mathbb{Z}, +, \cdot)$ ein Unterring von $(\mathbb{Q}, +, \cdot)$, von $(\mathbb{R}, +, \cdot)$ und von $(\mathbb{C}, +, \cdot)$.

(b) Der Nullring ist ein Unterring jedes Ringes.

Definition 4.1.7 (*Ring-Homomorphismus*)

Ein **Ring-Homomorphismus** ist eine Abbildung $\varphi : R \longrightarrow S$ zwischen zwei Ringen R und S mit

$$\begin{aligned} \varphi(a + b) &= \varphi(a) + \varphi(b)\,, \\ \varphi(a \cdot b) &= \varphi(a) \cdot \varphi(b)\,, \\ \varphi(1_R) &= 1_S\,. \end{aligned}$$

Ein bijektiver Ring-Homomorphismus heißt **Ring-Isomorphismus** und wir sagen, dass R und S **isomorph** sind (in Zeichen: $R \cong S$), wenn es einen Ring-Isomorphismus $\varphi : R \longrightarrow S$ gibt.

Anmerkung 4.1.8

Das Bild $\mathrm{Bild}(\varphi) = \varphi(R)$ eines Ring-Homomorphismus $\varphi : R \longrightarrow S$ ist ein Unterring von S. Der Kern von φ ist

$$\ker(\varphi) := \{r \in R \mid \varphi(r) = 0_S\} \subset R\,,$$

also der Kern von φ als Gruppen-Homomorphismus. Somit gilt: φ ist injektiv $\iff \ker(\varphi) = \{0_R\}$.
(Beachte: Der Kern ist im Allgemeinen kein Unterring von R.)

4.1.2 Polynomringe

Definition 4.1.9 (*Polynome*)

Sei R ein kommutativer Ring. Der **Polynomring $R[X]$ über R in der Unbestimmten X** ist die Menge

$$R[X] = \{0\} \cup \{f = a_0 + a_1 X^1 + \ldots + a_n X^n \mid n \in \mathbb{N}_0, a_i \in R, a_n \neq 0\}$$

Dabei nennen wir $\deg(f) := n$ der **Grad** von f und wir setzen $\deg(0) = -\infty$. Die Addition von

Polynomen ist

$$\begin{aligned}&(a_0 + a_1X^1 + \ldots + a_nX^n) + (b_0 + b_1X^1 + \ldots + b_mX^m)\\ &= (a_0 + b_0) + (a_1 + b_1)X^1 + \ldots + (a_n + b_n)X^n + b_{n+1}X^{n+1} + \ldots + b_mX^m\end{aligned}$$

wobei wir o.B.d.A. annehmen, dass $n \leq m$ ist, und die Multiplikation von Polynomen ist

$$(a_0 + a_1X^1 + \ldots + a_nX^n) \cdot (b_0 + b_1X^1 + \ldots + b_mX^m) = c_0 + c_1X^1 + \ldots + c_{n+m}X^{n+m}$$

wobei $c_k = \sum_{j=0}^{k} a_j \cdot b_{k-j}$ $(1 \leq k \leq n + m)$.
Das Einselement ist das Polynom $f = 1$ (d.h. $a_0 = a_n = 1$).

Beispiel 4.1.10

In $\mathbb{Z}[X]$ ist z.B.

$$(X^2 + X + 1) + (X + 1) = X^2 + 2X + 2\,, \text{ und}$$
$$(X^2 + X + 1) \cdot (X + 1) = X^3 + 2X^2 + 2X + 1\,.$$

Der Grad von $X^2 + X + 1$ ist 2 und der Grad von $X + 1$ ist 1.

Schreiben wir nun $X^2+X+1 = f(X)$, $X+1 = g(X)$, $X^2+2X+2 = h(X)$, $X^3+2X^2+2X+1 = k(X)$ und setzen wir den Wert $X = 2$ in, so erhalten wir

$$f(2) = 7, \qquad g(2) = 3, \qquad h(2) = 10, \qquad k(2) = 21$$

Somit gilt

$$f(2) + g(2) = 7 + 3 = 10 = h(2) \qquad \text{und} \qquad f(2) \cdot g(2) = 7 \cdot 3 = 21 = k(2)\,,$$

Wir sehen also, dass das Einsetzen von Werte und die Addition/Multiplikation von Polynomen kompatibel sind.

Nützlich werden Polynome dadurch, dass die Rechenoperationen kompatibel mit dem Einsetzen von Werten für die Variable X sind. Es spielt dann keine Rolle ob man erst mit Polynomen rechnet und dann Werte einsetzt oder erst einsetzt und mit diesen Werten die entsprechende Rechenoperation durchführt, d.h. Einsetzen ist ein Ring-Homomorphismus.

Beispiel 4.1.11 (*Der Einsetzungs-Homomorphismus*)

Sei R ein kommutativer Ring, der ein Unterring eines Ringes S ist und sei $s \in S$. (Z.B. $R = \mathbb{Z}$ und $S = \mathbb{Q}, \mathbb{R}$ oder $\mathbb{C}$.) Dann folgt aus der Definition der Addition und der Multiplikation in $R[X]$, dass

$$\begin{array}{rccc}\varphi_s: & R[X] & \longrightarrow & S\\ & f(X) = a_0 + a_1X^1 + \ldots + a_nX^n & \mapsto & f(s) = a_0 + a_1 \cdot s^1 + \ldots + a_n \cdot s^n\end{array}$$

ein Ring-Homomorphismus ist.
Ein Element $s \in S$ mit $f(s) = 0$ heißt eine **Nullstelle** des Polynoms $f(X)$.

Z.B. ist 2 eine Nullstelle von $f(X) = X - 2 \in \mathbb{Z}[X]$, da $f(2) = 2 - 2 = 0$.
Die Zahlen 2 und -3 sind Nullstellen vom Polynom $g(X) = X^2 + X - 6$, da $g(X) = (X-2)(X+3)$.

Aber das Polynom $h(X) = X^2 + 1$ hat keine Nullstelle $s \in \mathbb{Z}$, und auch keine Nullstelle in $\mathbb{R}$. Um eine Nullstelle von $h(X)$ zu haben, brauchen wir den Ring der komplexen Zahlen $(\mathbb{C}, +, \cdot)$.

In der Tat besagt der Fundamentalsatz der Algebra, dass jedes Polynom $f(X) \in \mathbb{C}[X]$ vom Grad $n \in \mathbb{N}$ genau n Nullstellen hat:

Satz 4.1.12 (*Fundamentalsatz der Algebra*)

Jedes Polynom $f \in \mathbb{C}[X]$ vom Grad $n = \deg(f)$ zerfällt in Linearfaktoren

$$f = (X - c_1) \cdot \ldots \cdot \ldots \cdot (X - c_n)$$

mit $c_i \in \mathbb{C}$, hat also mit Vielfachheit gezählt genau n Nullstellen in $\mathbb{C}$.

Der Beweis ist leider nicht erreichbar mit den Methoden, die wir in dieser Vorlesung entwickeln.

4.2 Der Ring der Restklassen modulo n

4.2.1 $\mathbb{Z}/n$ als Ring

Lemma-Definition 4.2.1 (*Ring der Restklassen modulo n*)

Sei $n \in \mathbb{N}$. Dann ist die Gruppe $(\mathbb{Z}/n, +)$ der Restklassen modulo n zusammen mit der Multiplikation

$$\begin{array}{rccc} \cdot : & \mathbb{Z}/n \times \mathbb{Z}/n & \longrightarrow & \mathbb{Z}/n \\ & (\overline{a}, \overline{b}) & \mapsto & \overline{a} \cdot \overline{b} := \overline{a \cdot b}\,, \end{array}$$

ein kommutativer Ring mit Einselement $\overline{1}$, genannt **Ring der Restklassen modulo** n.

Beweis:

- Da $\overline{a} \cdot \overline{b} = \overline{a \cdot b}$ in Termen von Äquivalenzklassen definiert ist, müssen wir wieder zeigen, dass diese Multiplikation wohldefiniert ist, d.h. nicht von der Wahl der Repräsentanten a und b abhängt: anders gesagt für $\overline{a_1} = \overline{a_2}$ und $\overline{b_1} = \overline{b_2}$ müssen wir zeigen, dass $\overline{a_1} \cdot \overline{a_2} = \overline{b_1} \cdot \overline{b_2}$.

  Aber aus $\overline{a_1} = \overline{a_2}$ und $\overline{b_1} = \overline{b_2}$ folgen $a_1 - a_2 = n \cdot k_1$ und $b_1 - b_2 = n \cdot k_2$ mit Zahlen $k_1, k_2 \in \mathbb{Z}$ und somit gilt

$$\begin{aligned} \overline{a_1} \cdot \overline{b_1} = \overline{a_1 \cdot b_1} &= \overline{(a_2 + n \cdot k_1) \cdot (b_2 + n \cdot k_2)} = \\ &= \overline{a_2 \cdot b_2 + n \cdot (a_2 k_2 + k_1 b_2 + n k_1 k_2)} = \overline{a_2 \cdot b_2} = \overline{a_2} \cdot \overline{b_2}\,. \end{aligned}$$

- Die Multiplikation in $\mathbb{Z}/n$ ist assoziativ, da die Addition in $\mathbb{Z}$ schon assoziativ ist $\Longrightarrow$ **(R2)** gilt.
- Die Distributivität gilt in $\mathbb{Z}/n$, da die Distributivität schon in $\mathbb{Z}$ gilt $\Longrightarrow$ **(R3)** gilt.
- Das Einselement ist die Restklasse von 1: $\overline{a} \cdot \overline{1} = \overline{a \cdot 1} = \overline{a}$ und $\overline{1} \cdot \overline{a} = \overline{1 \cdot a} = \overline{a}$ für alle $\overline{a} \in \mathbb{Z}/n$ $\Longrightarrow$ **(R4)** gilt.
- Schließlich gilt die Kommutativität in $\mathbb{Z}/n$, da die Kommutativität schon in $\mathbb{Z}$ gilt. ∎

Beispiel 4.2.2

Die Multiplikation in $\mathbb{Z}/n$ kann man auch durch die **Multiplikationstafel** beschreiben.

Die Multiplikationstafeln von $\mathbb{Z}/3$ und $\mathbb{Z}/4$ sind z.B. gegeben durch:

$\cdot$	$\overline{0}$	$\overline{1}$	$\overline{2}$
$\overline{0}$	$\overline{0}$	$\overline{0}$	$\overline{0}$
$\overline{1}$	$\overline{0}$	$\overline{1}$	$\overline{2}$
$\overline{2}$	$\overline{0}$	$\overline{2}$	$\overline{1}$

und

$\cdot$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$
$\overline{0}$	$\overline{0}$	$\overline{0}$	$\overline{0}$	$\overline{0}$
$\overline{1}$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$
$\overline{2}$	$\overline{0}$	$\overline{2}$	$\overline{0}$	$\overline{2}$
$\overline{3}$	$\overline{0}$	$\overline{3}$	$\overline{2}$	$\overline{1}$

Damit sehen wir, dass $\mathbb{Z}/3$ ein Körper ist, da jedes Element $\overline{m} \in \mathbb{Z}/3 \setminus \{\overline{0}\} = \{\overline{1}, \overline{2}\}$ invertierbar bezüglich der Multiplikation ist.
Dagegen ist $\mathbb{Z}/4$ kein Körper, da die Restklasse $\overline{2}$ kein inverses Element besitzt.

4.2.2 Die Einheiten von $\mathbb{Z}/n$ und die eulersche φ-Funktion

Definition 4.2.3

Sei $(R, +, \cdot)$ ein kommutativer Ring. Ein Element $u \in R$ heißt **Einheit** von R (oder **invertierbar**), wenn ein $w \in R$ existiert mit

$$w \cdot u = u \cdot w = 1_R$$

(d.h., w ist ein inverses Element von u bzg. der Multiplikation). Die Menge der Einheiten wird mit $R^\times$ bezeichnet.
Mit u ist offenbar auch w eine Einheit und $(R^\times, \cdot)$ bildet eine Gruppe, die **Einheitengruppe** von R.

Beispiel 4.2.4

(a) Ein kommutativer Ring R mit $R \neq \{0\}$ ist genau dann ein Körper, wenn $R^\times = R \setminus \{0\}$.
(Nach Beispiel 4.2.2 ist $\mathbb{Z}/3$ ein Körper mit Einheitengruppe $\mathbb{Z}/3 \setminus \{\overline{0}\} = \{\overline{1}, \overline{2}\}$.)

(b) Nach Beispiel 4.2.2 sind die Einheiten von $\mathbb{Z}/4$ die Restklassen $\overline{1}$ und $\overline{3}$.

Anmerkung 4.2.5

Ein Element $\overline{a} \in \mathbb{Z}/n$ ist genau dann eine Einheit, wenn es ein $\overline{b} \in \mathbb{Z}/n$ gibt mit $\overline{a} \cdot \overline{b} = \overline{1}$, d.h., wenn es $b, k \in \mathbb{Z}$ gibt mit

$$a \cdot b + n \cdot k = 1\,.$$

Solche b und k erhalten wir mit dem erweiterten Euklidischen Algorithmus, wenn $\mathrm{ggT}(a, n) = 1$. Haben wir umgekehrt eine solche Darstellung von 1, dann müssen natürlich a und n teilerfremd sein (denn jeder gemeinsame Teiler teilt auch 1). Somit können wir die Elemente der Einheitengruppe beschreiben:

$$\boxed{(\mathbb{Z}/n)^\times = \{\overline{a} \in \mathbb{Z}/n \mid \mathrm{ggT}(a, n) = 1\}}$$

Die Einheiten von $\mathbb{Z}/n$ heißen auch **prime Restklassen** und $(\mathbb{Z}/n)^\times$ **prime Restklassengruppe**.

Als direkte Folgerung erhalten wir:

Folgerung 4.2.6

Der Ring $(\mathbb{Z}/n, +, \cdot)$ ist ein Körper genau dann, wenn n eine Primzahl ist.

Beispiel 4.2.7

Die Restklasse $\overline{8} \in \mathbb{Z}/15$ hat ein Inverses, d.h. $\overline{8} \in (\mathbb{Z}/15)^\times$, denn

$$\mathrm{ggT}(8, 15) = 1\,.$$

Mit dem erweiterten Euklidischen Algorithmus erhalten wir eine Darstellung des größten gemeinsamen Teilers

$$1 = 2 \cdot 8 + (-1) \cdot 15\,,$$

also ist

$$\overline{8}^{-1} = \overline{2}\,.$$

Definition 4.2.8 (*Eulersche φ-Funktion*)

Die eulersche φ-Funktion ist die Funktion $\varphi : \mathbb{N} \longrightarrow \mathbb{Z}$, definiert durch

$$\varphi(n) = |(\mathbb{Z}/n)^\times| = |\{m \in \mathbb{N} \mid 1 \leq m \leq n \text{ und } \mathrm{ggT}(m, n) = 1\}|$$

gibt also für n die Ordnung der Einheitengruppe $(\mathbb{Z}/n)^\times$ an.

Lemma 4.2.9 (*Ser Satz von Euler*)

Für alle $a, n \in \mathbb{Z}$ mit $n \geq 1$ und $\mathrm{ggT}(a, n) = 1$ gilt

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

Beweis: Erinnerung: die Ordnung jedes Elements g einer Gruppe G teilt die Gruppenordnung $|G|$ und $g^{o(g)} = e$. Damit ist

$$g^{|G|} = e\,.$$

Angewendet auf $\overline{a} \in (\mathbb{Z}/n)^\times$ erhalten wir

$$\overline{a}^{|(\mathbb{Z}/n)^\times|} = \overline{a}^{\varphi(n)} = \overline{a^{\varphi(n)}} = \overline{1} \text{ in } (\mathbb{Z}/n)^\times \qquad \Longleftrightarrow \qquad a^{\varphi(n)} \equiv 1 \mod n\,.$$

■

Ist nun p eine Primzahl, so gilt $\varphi(p) = p - 1$ und der Satz von Euler liefert

$$a^{p-1} \equiv 1 \mod p \qquad \text{falls } p \nmid a\,,$$

also $a^p \equiv a \mod p$ falls $p \nmid a$. Außerdem: $p|a \Rightarrow a^p \equiv 0 \equiv a \mod p$. Somit erhalten wir als Corollar:

Folgerung 4.2.10 (*Kleiner Satz von Fermat*)

Ist p eine Primzahl und $a \in \mathbb{Z}$, dann gilt

$$a^p \equiv a \mod p\,.$$

Zur Berechnung der eulerschen φ-Funktion verwendet man in der Praxis, dass sie *multiplikativ* über teilerfremde Produkte ist. Dazu bemerken wir zunächst: Der durch den Chinesischen Restsatz gegebene Gruppen-Isomorphismus ist tatsächlich ein Ring-Isomorphismus:

Satz 4.2.11 (*Chinesischer Restsatz, Ring-Version*)

Sind $m, n \in \mathbb{N}$ teilerfremd (d.h. ggT$(m, n) = 1$), so ist die Abbildung

$$\begin{array}{rccc} f: & \mathbb{Z}/mn & \longrightarrow & \mathbb{Z}/m \times \mathbb{Z}/n \\ & a + mn\mathbb{Z} & \mapsto & (a + m\mathbb{Z}, a + n\mathbb{Z}) \,. \end{array}$$

ein Ring-Isomorphismus.

Erinnerung: wir schreiben $a + mn\mathbb{Z}$, $a + m\mathbb{Z}$ und $a + n\mathbb{Z}$ anstelle von $\overline{a}$, da die Restklassen modulo mn, modulo m und modulo n nicht gleich sind.

Beweis: Wir wissen schon, dass f ein Gruppen-Isomorphismus ist. (Insbesondere ist f bijektiv.)
Nun gilt

$$\begin{aligned} f((a + mn\mathbb{Z}) \cdot (b + mn\mathbb{Z})) &= f(a \cdot b + mn\mathbb{Z}) \\ &= (a \cdot b + m\mathbb{Z}, a \cdot b + n\mathbb{Z}) \\ &= ((a + m\mathbb{Z}) \cdot (b + m\mathbb{Z}), (a + n\mathbb{Z}) \cdot (b + n\mathbb{Z})) \\ &= ((a + m\mathbb{Z}), (a + n\mathbb{Z})) \cdot ((b + m\mathbb{Z}), (b + n\mathbb{Z})) \\ &= f(a + mn\mathbb{Z}) \cdot f(b + mn\mathbb{Z}) \end{aligned}$$

und $f(1 + mn\mathbb{Z}) = (1 + m\mathbb{Z}, 1 + n\mathbb{Z})$. Somit ist f ein Ring-Homomorphismus, also ein Ring-Isomorphismus. ■

Folgerung 4.2.12

(a) Sind $m, n \in \mathbb{N}$ teilerfremd , so ist

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

(b) Ist $n = p \cdot q$ das Produkt von zwei Primzahlen, so gilt

$$\varphi(n) = (p - 1) \cdot (q - 1) \,.$$

(c) Ist $n \in \mathbb{N}$ und $n = p_1^{r_1} \cdot \ldots \cdot p_s^{r_s}$ eine Primfaktorzerlegung von n (d.h. $p_1, \ldots, p_r$ sind paarweise verschiedene Primzahlen), so ist

$$\varphi(n) = \varphi(p_1^{r_1}) \cdot \ldots \cdot \varphi(p_s^{r_s})$$

und $\varphi(p_i^{r_i}) = p_i^{r_i - 1}(p_i - 1)$.

Beweis: (a) Nach dem Chinesischen Restsatz ist

$$\begin{array}{rccc} f: & \mathbb{Z}/mn & \longrightarrow & \mathbb{Z}/m \times \mathbb{Z}/n \\ & a + mn\mathbb{Z} & \mapsto & (a + m\mathbb{Z}, a + n\mathbb{Z}) \,. \end{array}$$

ein Ring-Isomorphismus. Damit ist eine Restklasse $\overline{a} = a + mn\mathbb{Z} \in \mathbb{Z}/mn$ genau dann eine Einheit, wenn $f(a + mn\mathbb{Z}) = (a + m\mathbb{Z}, a + n\mathbb{Z})$ eine Einheit in $\mathbb{Z}/m \times \mathbb{Z}/n$ ist. D.h.

$$(\mathbb{Z}/mn)^\times = (\mathbb{Z}/m \times \mathbb{Z}/n)^\times = (\mathbb{Z}/m)^\times \times (\mathbb{Z}/n)^\times$$

und wir erahlten

$$\varphi(m \cdot n) = |(\mathbb{Z}/mn)^\times| = |(\mathbb{Z}/m)^\times| \cdot |(\mathbb{Z}/n)^\times| = \varphi(m) \cdot \varphi(n) \,.$$

(b) Da p und q Primzahlen sind, gilt $\varphi(p) = p - 1$ und $\varphi(q) = q - 1$. Somit folgt Aussage (b) aus (a).

(c) Aufgabe (Blatt 9). ■

4.3 Anwendung: Das RSA-Verfahren

Die Eulersche φ-Funktion bildet die Grundlage für eines der bekanntesten und meist benutzten Kryptosysteme: das **RSA-Verfahren**. Es wurde 1977/78 von R. Rivest, A. Shamir und L. Adleman am MIT entwickelt.

4.3.1 Das Prinzip

Wir betrachten das folgende Problem (siehe auch `BeamerWoche9.pdf`):

Problem 4.3.1

Bob (der Sender) will Alice (der Empfänger) eine Nachricht schicken, ohne dass Eve diese lesen oder unbemerkt verändern kann, falls sie die Nachricht abfängt.

Die Lösung ist, die Nachricht zu verschlüsseln. Genauer: im RSA-Verfahren besteht die Verschlüsselung aus zwei Schlüsseln:

- einem öffentlichen, und
- einem privaten Schlüssel.

Mit dem öffentlichen Schlüssel kann man Nachrichten verschlüsseln, aber nicht entschlüsseln. Deshalb wird dieser Schlüssel öffentlich zur Verfügung gestellt, z. B. im Internet. Hier kann den Schlüssel dann jeder benutzen, um Nachrichten zu verschlüsseln, die aber nur der Empfänger (= derjenige, der den öffentlichen Schlüssel anbietet) wieder entschlüsseln kann. Zum Entschlüsseln braucht man den privaten Schlüssel, und den kennt nur der Empfänger.

Anmerkung 4.3.2

Das RSA-Verfahren verschlüsselt und entschlüsselt nur Zahlen in Zahlen, daher muss erst der Klartext mit einem öffentlich bekannten Alphabet in eine Zahlenfolge (numerical Encoding) übersetzt werden.

4.3.2 Das RSA-Verfahren

Das RSA-Verfahren basiert auf der folgenden mathematischen Aussage:

Satz 4.3.3

Seien p, q zwei verschiedene Primzahlen und sei $N := p \cdot q$. Ferner sei $0 < e < N$ mit $\mathrm{ggT}(e, \varphi(N)) = 1$ und $0 < d < N$ mit $d \cdot e \equiv 1 \mod \varphi(N)$. Dann gilt für jedes $0 \leq m < N$:

$$(m^e)^d \equiv m \mod N.$$

Beweis: Es gilt $\mathrm{ggT}(m, N) \in \{1, p, q\}$.

1. Fall: $\mathrm{ggT}(m, N) = 1$. Nach dem Satz von Euler ist

$$m^{\varphi(N)} \equiv 1 \mod N$$

und wegen $d \cdot e \equiv 1 \mod \varphi(N)$ gibt es ein $k \in \mathbb{Z}$ mit $de = 1 + k \cdot \varphi(N)$. Also ist

$$(m^e)^d = m^{1+k\varphi(N)} = m \cdot (m^{\varphi(N)})^k \equiv m \cdot 1^k = m \mod N\,.$$

2. Fall: $\mathrm{ggT}(m, N) = p$. Wir benutzen hier den Chinesischen Restsatz. Zunächst impliziert $m \equiv 0 \mod p$, dass

$$m^{ed} \equiv m \equiv 0 \mod p$$

ist. Wegen $q \nmid m$ folgt aus dem Satz von Euler, dass

$$m^{q-1} \equiv 1 \mod q$$

ist. Aus $\varphi(N) = (p-1)(q-1)$ folgt dann ebenso $m^{ed} \equiv m \mod q$. Mit dem Chinesischen Restsatz erhalten wir dann $m^{ed} \equiv m \mod N$, wie behauptet.

3. Fall: $\mathrm{ggT}(m, N) = q$: Analog (tausche p und q). ■

<u>Das RSA-Verfahren</u>.

1. Schritt: Öffentlichen Schlüssel anlegen. (Alice)

1a. Eine Schranke N ermitteln:
Wähle $p \neq q$ zwei (große) Primzahlen;
Setze $N := p \cdot q$.

1b. Eine Zahl e ermitteln:
Berechne $\varphi(N) = (p-1) \cdot (q-1)$;
Wähle eine beliebige Zahl $1 < e < \varphi(N)$ mit $\mathrm{ggT}(e, \varphi(N)) = 1$.

Der **öffentliche Schlüssel** ist dann das 2-Tupel (e, N). Dieser wird veröffentlicht.

2. Schritt: Privaten Schlüssel anlegen. (Alice)

2a. Berechne mit Hilfe des euklidischen Algorithmus eine Zahl d mit

$$e \cdot d \equiv 1 \mod \varphi(N)\,.$$

Der **private Schlüssel** ist dann das 2-Tupel (d, N). Dieser muss geheim bleiben.

3. Schritt: Nachricht verschlüsseln. (Bob mit dem öffentlichen Schlüssel (e, N).)

3a. Die Nachricht $1 < m < N$ wird mit ihrer Restklasse $\overline{m} \in \mathbb{Z}/N$ identifiziert.

3b. Die Nachricht wird durch

$$s := m^e \mod N$$

verschlüsselt.

Dieses s schickt Bob dann an Alice.

4. Schritt: Nachricht entschlüsseln. (Alice mit dem privaten Schlüssel (d, N).)

4a. Die Nachricht wird nach Sartz 4.3.3 durch

$$m := s^d \mod N$$

entschlüsselt.

Beispiel 4.3.4

Sei $p = 47$ und $q = 71$. Somit ist $N = p \cdot q = 3337$ und $\varphi(N) = (p-1)(q-1) = 46 \cdot 70 = 3220$. Abhängig von $\varphi(N)$ wird eine zufällige Zahl e mit $\varphi(N) > e > 1$ gewählt, wobei $\mathrm{ggT}(e, \varphi(N)) = 1$ sein muss. Wir wählen zum Beispiel

$$e = 79\,.$$

Aus e und $\varphi(N)$ können wir nun d mit dem euklidischen Algorithmus ausrechnen:

$$de \equiv 1 \mod \varphi(N) \qquad \Longleftrightarrow \qquad d \equiv 79^{-1} \equiv 1019 \mod 3220$$

Somit haben wir die beiden Schlüssel:

$$\text{Öffentlicher Schlüssel} = (e, N) = (79, 3337)$$
$$\text{Privater Schlüssel} = (d, N) = (1019, 3337)$$

Bob kann nun seine Nachricht

$$m = 688$$

verschlüsseln und Alice schicken:

$$s = m^e = 688^{79} \equiv 1570 \mod 3337$$

Alice kann dann dieses Chiffrat entschlüsseln. Dafür verwendet sie den privaten Schlüssel und sie bekommt:

$$m = s^d = 1570^{1019} \equiv 688 \mod 3337$$

Anmerkung 4.3.5

(a) **Sicherheit und Sicherheitslücken:**
Die Sicherheit des RSA-Verfahren beruht auf dem Problem, Zahlen der Form $N = pq$ mit $p, q \in \mathbb{P}$ zu faktorisieren. Bisher hat es noch keiner geschafft, diese Zahlen effektiv und schnell zu zerlegen. Deswegen ist es wichtig *große* Primzahlen $p, q \in \mathbb{P}$ zu wählen. Selbst mit einem Computer braucht man in der Praxis bis zu einem Jahr, falls $pq \lesssim 10^{150}$ gilt. Für $pq \simeq 10^{300}$ würde Eve viele tausend Jahre und viele tausend Computer benötigen, um die Faktorisierung zu erreichen.
Es ist aber auch nicht bewiesen, dass es sich bei der Primfaktorzerlegung von $N = pq$ um ein prinzipiell schwieriges Problem handelt.

(b) **Beispiele von Anwendungsgebiete**:

- Internet- und Telefonie-Infrastruktur: X.509-Zertifikate
- E-Mail-Verschlüsselung: OpenPGP, S/MIME
- Authentifizierung Telefonkarten
- Kartenzahlung: EMV
- RFID Chip auf dem deutschen Reisepass / Schweizer Reisepass.
- Electronic Banking: HBCI
- Übertragungs-Protokolle: IPsec, TLS, SSH, WASTE

4.4 Anwendung: Diffie-Hellman Schlüsselaustausch

Anmerkung 4.4.1

Eine wesentliche Schwachstelle von RSA liegt darin, dass ein Angreifer, wenn er den privaten Schlüssel einer Person in Besitz bringt, alle an diese Person gerichteten Nachrichten lesen kann. Dies gilt auch für verschlüsselte Nachrichten der Vergangenheit, die von dem Angreifer aufgezeichnet wurden. Der Diffie-Hellman Schlüsselaustausch hat dieses Problem nicht (dies bezeichnet man als *perfect forward secrecy*), da kein privater Schlüssel verwendet wird. Man geht folgendermaßen vor:

1. **Schritt:** **Alice** und **Bob** einigen sich auf eine zyklische Gruppe $G = \langle g \rangle$ und einen Erzeuger g der Gruppe.

2. **Schritt:** **Alice** wählt eine zufällige ganze Zahl $0 \leq a < |G|$, berechnet

$$g^a$$

(dies ist ein Element der Gruppe G) und sendet dies an Bob.

3. **Schritt:** **Bob** wählt eine zufällige Zahl $0 \leq b < |G|$ berechnet

$$g^b$$

und sendet dies an Alice.

4. **Schritt:** **Alice** berechnet $(g^b)^a$ und **Bob** berechnet $(g^a)^b$. Bob und Alice teilen dann das *Geheimnis*

$$(g^b)^a = (g^a)^b$$

Zum Entschlüsseln muss ein Angreifer aus g^b die Zahl b bestimmen. Dies nennt man auch die *Berechnung eines diskreten Logarithmus*.
Das Diffie-Hellman-Verfahren basiert darauf, dass typischerweise Potenzieren schnell durchführbar ist, aber umgekehrt die Berechnung eines Logarithmus aufwändig ist. Natürlich muss $|G|$ groß genug sein, für kleine Gruppen kann man alle Möglichkeiten durchprobieren.

Beispiel 4.4.2

Alice und **Bob** einigen sich auf die zyklische Gruppe $G = (\mathbb{Z}/11)^\times$ mit Erzeuger $g = \overline{2}$:

$$(\mathbb{Z}/11)^\times = \langle\overline{2}\rangle = \{\overline{2}, \overline{4}, \overline{8}, \overline{5}, \overline{10}, \overline{9}, \overline{7}, \overline{3}, \overline{6}, \overline{1}\}$$

Alice wählt $a = 3$ und sendet

$$\overline{2}^3 = \overline{8}\,.$$

Bob wählt $b = 9$ und sendet

$$\overline{2}^9 = \overline{512} = \overline{6}$$

Beide teilen das Geheimnis $\overline{8}^9 = \overline{6}^3 = \overline{7}$.

4.5 Anwendung: Pollards $(p-1)$-Faktorisierung

Siehe Blatt 9.

4.6 Ideale und Faktorringe

Ab jetzt nehmen wir an, dass alle Ringe, die wir betrachten, **kommutativ** sind.

In diesem Abschnitt wollen wir die Konstruktion des Rings $(\mathbb{Z}/n, +, \cdot)$ verallgemeinern. Dazu untersuchen wir, inwieweit man der Faktorgruppe die Struktur eines Ringes geben kann.

Um eine Faktorgruppe G/H aus einer Gruppe zu bilden, brauchen wir, dass H ein *Normalteiler* ist. Haben wir nun einen Ring $(R, +, \cdot)$, so ist jede Untergruppe $(I, +)$ von $(R, +)$ ein Normalteiler, da die Addition kommutativ ist. Wir können also die Faktorgruppe $(R/I, +)$ bilden, wobei

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

d.h. die Menge der Nebenklassen. (Erinnerung: in diesem Fall stimmen die Rechstnebenklassen und die Linksnebenklassen überein und wir sprechen einfach von Nebenklassen.) Zur Vereinfachung schreiben wir diese Nebenklassen auch mit der *quer*-Notation, d.h.

$$\overline{r} = r + I\ ,$$

sodass die Elemente aus R/I wie die Elemente aus $\mathbb{Z}/n$ aussehen. Wir sehen nun, dass R/I eigentlich einen Ring bildet, wenn wir an I die folgenden Bedingungen stellen:

Definition 4.6.1 (*Ideal*)

Eine Teilmenge I eines kommutativen Ringes $(R, +, \cdot)$ heißt ein **Ideal** von R, wenn gilt:

(i) $(I, +)$ ist eine Untergruppe der abelsche Gruppe $(R, +)$; und

(ii) $r \cdot a \in I$ für alle $a \in I$ und $\forall\, r \in R$.

Satz 4.6.2 (*Faktorringe*)

Sei $I \subset R$ ein Ideal eines kommutativen Ringes $(R, +, \cdot)$. Dann trägt die Faktorgruppe $(R/I, +)$ die Struktur eines kommutativen Ringes mit (repräsentantenweiser) Multiplikation:

$$\begin{array}{rccc} \cdot : & R/I \times R/I & \longrightarrow & R/I \\ & (\overline{r_1}, \overline{r_2}) & \mapsto & \overline{r_1} \cdot \overline{r_2} := \overline{r_1 \cdot r_2}\,, \end{array}$$

Das neutrale Element von R/I bezüglich der Multiplikation $\cdot$ ist $\overline{1} = 1+I$. Wir bezeichnen $(R/I, +, \cdot)$ als **Faktorring** von R nach I.

Beweis:

- Die Multiplikation ist wohldefiniert: Ist $\overline{r_1'} = \overline{r_1}$ und $\overline{r_2'} = \overline{r_2}$, so ist $r_1' = r_1 + b_1$ und $r_2' = r_1 + b_2$ mit $b_1, b_2 \in I$. Damit gilt

  $$\overline{r_1'} \cdot \overline{r_2'} = \overline{r_1' \cdot r_2'} = \overline{(r_1 + b_1) \cdot (r_2 + b_2)} = \overline{r_1 \cdot r_2 + r_1 \cdot b_2 + b_1 \cdot r_2 + b_1 \cdot b_2}$$

  Aber $r_1 \cdot b_2, b_1 \cdot r_2, b_1 \cdot b_2 \in I$ nach (ii) der Definition eines Ideals. Es folgt, dass

  $$r_1 \cdot b_2 + b_1 \cdot r_2 + b_1 \cdot b_2 \in I\,,$$

  da $(I, +)$ eine Untergruppe ist. Damit ist

  $$\overline{r_1 \cdot r_2 + r_1 \cdot b_2 + b_1 \cdot r_2 + b_1 \cdot b_2} = \overline{r_1 \cdot r_2}$$

  und

  $$\overline{r_1'} \cdot \overline{r_2'} = \overline{r_1 \cdot r_2}\,.$$

- R/I ist ein kommutativer Ring mit Eins: Aufgabe, Blatt 9. ∎

Ideale spielen also eine wichtige Rolle in der Ringtheorie.

Beispiel 4.6.3

(a) Sind $I_1, I_2 \subset R$ Ideale, dann auch deren Durchschnitt $I_1 \cap I_2$. (Aufgabe, Blatt 9.)

(b) Seien $a_1, \ldots, a_n \in R$. Dann ist

$$(a_1, \ldots, a_n) := \{\sum_{i=1}^{n} r_i \cdot a_i \mid r_i \in R\}$$

ein Ideal, das **von dem Erzeugendensystem $a_1, \ldots, a_n$ erzeugte Ideal**.

(c) Ist $n \in \mathbb{N}_0$, so ist

$$n\mathbb{Z} = \{n \cdot a \mid a \in \mathbb{Z}\} = (n)$$

ein Ideal von $\mathbb{Z}$ und der Faktorring ist $\mathbb{Z}/n\mathbb{Z} = \mathbb{Z}/n$. Weiter sind die Ideale von $\mathbb{Z}$ genau die Untergruppen $n\mathbb{Z}$ mit $n \in \mathbb{Z}$.

(d) Ist $\varphi : R \longrightarrow S$ ein Ring-Homomorphismus (d.h. zwischen zwei kommutativen Ringen R und S), so ist der Kern

$$\ker(\varphi) = \{r \in R \mid \varphi(r) = 0\}$$

ein Ideal von R, denn ist $r' \in R$ und $\varphi(r) = 0$, so auch

$$\varphi(r' \cdot r) = \varphi(r') \cdot \varphi(r) = \varphi(r') \cdot 0 = 0\,.$$

Satz 4.6.4 (*Homomorphiesatz für kommutative Ringe*)

Sei $\varphi : R \longrightarrow S$ ein Ring-Homomorphismus zwischen zwei kommutativen Ringen R und S. Dann gilt

$$R/\ker(\varphi) \cong \text{Bild}(\varphi)\,.$$

Beweis: Dank dem Homomorphiesatz für Gruppen haben wir einen Gruppen-Isomorphismus

$$\begin{array}{rccc} \overline{\varphi}: & R/\ker(\varphi) & \longrightarrow & \text{Bild}(\varphi) \\ & \overline{r} = r + \ker(\varphi) & \mapsto & \varphi(r)\ . \end{array}$$

Weiter ist $\overline{\varphi}$ ein Ring-Homomorphismus, denn

$$\overline{\varphi}(\overline{r_1} \cdot \overline{r_2}) = \overline{\varphi}(\overline{r_1 \cdot r_2}) = \varphi(r_1 \cdot r_2) = \varphi(r_1) \cdot \varphi(r_2) = \overline{\varphi}(\overline{r_1}) \cdot \overline{\varphi}(\overline{r_2})\,.$$

■

4.7 Integritätsringe und Körper

Wir wollen nun Körper besser verstehen.

Definition 4.7.1 (*Nullteiler, Integritätsring*)

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

(a) Ein Element $a \in R$ heißt **Nullteiler** von R, wenn ein $x \in R \setminus \{0\}$ existiert mit $a \cdot x = 0$.

(b) Der Ring R heißt **Integritätsring** (oder **Integritätsbereich**), wenn er keine Nullteiler außer 0 besitzt.
(Insbesondere kann ein Integritätsring nicht der Nullring sein.)

Anmerkung 4.7.2

- Ein kommutativer Ring $R \neq \{0\}$ ist ein Integritätsring, wenn für alle $a, b \in R$ gilt: ist $ab = 0$, so ist bereits $a = 0$ oder $b = 0$
- Ein Element eines kommutativen Ringes R kann nicht sowohl eine Einheit und ein Nullteiler sein, denn ist a eine Einheit und $a \cdot x = 0$, dann ist $x = a^{-1} \cdot a \cdot x = a^{-1} \cdot 0 = 0$ (wobei a^{-1} das inverse Element von a ist).

Beispiel 4.7.3

(a) Ein Körper K ist ein Integritätsring nach Definition: K ist kommutativ, $K \neq \{0\}$ und es gilt $K^\times = K \setminus \{0\}$. Somit ist null der einzige Nullteiler in K.
Insbesondere sind $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$, $\mathbb{Z}/p$ (mit p eine Primzahl) Integritätsringe.

(b) Jeder Unterring $S \neq \{0\}$ eines Integritätsringes ist offensichtlich wieder ein Integritätsring. Insbesondere ist der Ring $(\mathbb{Z}, +, \cdot)$ ein Integritätsring, da $\mathbb{Z}$ ein Unterring von $\mathbb{Q}$ ist.

(c) $\mathbb{Z}/6 = \{\overline{0}, \overline{1}, \ldots, \overline{5}\}$ ist kein Integritätsring: die Restklassen $\overline{0}$, $\overline{2}$, $\overline{3}$, $\overline{4}$ sind Nullteiler. (Dagegen sind die Restklassen $\overline{1}$ und $\overline{5}$ Einheiten.)

(d) Ist R ein Integritätsring, dann auch $R[X]$.
Außerdem gilt die **Gradformel**: Für $f(X), g(X) \in R[X]$ ist

$$\deg(f(X) \cdot g(X)) = \deg(f(X)) + \deg(g(X)) .$$

Damit kann man zeigen, dass $R[X]^\times = R^\times$ ist. (Die Einheiten sind also konstante Polynome.) (Aufgabe, Blatt 10.)

(e) (**Quotientenkörper**): Für Integritätsringe R können wir analog zur Konstruktion von $\mathbb{Q}$ aus $\mathbb{Z}$ durch Bruchrechnen den **Quotientenkörper**

$$Q(R) := \left\{ \frac{a}{b} \mid a \in R, b \in R \setminus \{0_R\} \right\}$$

bilden.
Z. B. ist für einen Körper K

$$Q(K[X]) = \left\{ \frac{f}{g} \mid f \in K[X], g \in K[X] \setminus \{0\} \right\} =: K(X)$$

der **Körper der rationalen Funktionen** von K.

Für *endliche* Integritätsringe besteht keine Notwendigkeit für die Quotientenkörperkonstruktion. Diese sind schon Körper:

Satz 4.7.4

Jeder endliche Integritätsring ist ein Körper.

Beweis: Aufgabe, Blatt 10. ■

Damit erhalten wir erneut, dass die Ringe der Resklassen modulo p für p eine Primzahl Körper sind:

Folgerung 4.7.5

Ist p eine Primzahl, so ist $\mathbb{Z}/p = \mathbb{Z}/p\mathbb{Z} =: \mathbb{F}_p$ ein Körper.

Anmerkung 4.7.6 (*Endliche Körper*)

(a) Beachte: der Ring $\mathbb{Z}/m$, wobei m keine Primzahl ist, ist kein Körper, da dieser kein Integritätsring ist. (Aufgabe, Blatt 10.)

(b) Man kann zeigen, dass es bis auf Isomorphie zu jeder Primzahlpotenz p^r genau einen Körper K mit $|K| = p^r$ Elementen gibt. Dieser wird als $\mathbb{F}_{p^r}$ bezeichnet.

Anmerkung 4.7.7 (*Charakteristik*)

Sei K ein Körper und $\chi : \mathbb{Z} \longrightarrow K$ der Ring-Homomorphismus definiert durch

$$\chi(m) := \begin{cases} \sum_{i=1}^{m} 1_R = \underbrace{1_R + \ldots + 1_R}_{m\text{-mal}} & \text{falls } m > 0\,, \\ 0 & \text{falls } m = 0\,, \\ -\sum_{i=1}^{-m} 1_R = \underbrace{(-1_R) + \ldots + (-1_R)}_{(-m)\text{-mal}} & \text{falls } m < 0\,. \end{cases}$$

Der Kern von χ ist ein Ideal von $\mathbb{Z}$, also hat die Form

$$\ker(\chi) = p\mathbb{Z}$$

für ein $p \in \mathbb{Z}_{\geq 0}$. Man nennt dies Zahl die **Charakteristik** von K und schreibt $\operatorname{char}(K) = p$. Zwei Fälle können auftreten:

- $p = 0$, d.h. χ ist injektiv. In diesem Fall ist $\mathbb{Z}$ und damit auch $\mathbb{Q}$ ein Unterring von K.
- $p > 0$. Dann ist
$$\mathbb{Z}/p\mathbb{Z} \longrightarrow \text{Bild}(\chi) \subset K$$
nach dem Homomorphiesatz injektiv, also der Körper $\mathbb{F}_p = \mathbb{Z}/p$ ein Unterring von K (und damit ein Integritätsring). Somit muss p eine Primzahl sein, denn wäre $p = a \cdot b$ mit $a, b > 1$, dann $\overline{a} \cdot \overline{b} = \overline{0}$ in $\mathbb{Z}/p$, also sind $\overline{a}, \overline{b} \neq \overline{0}$ Nullteiler: Widerspruch.

Jeder Körper enthält also entweder $\mathbb{Q}$ oder $\mathbb{F}_p$ für eine Primzahl p.

4.8 Euklidische Ringe

Wir wollen nun Division mit Rest und den Euklidischen Algorithmus übertragen. Diese Algorithmen funktionieren völlig analog zu denen in $\mathbb{Z}$, wenn wir Ringe mit den folgenden Eigenschaften betrachten:

Definition 4.8.1

Ein **euklidischer Ring** ist ein Integritätsring R zusammen mit einer Abbildung

$$d : R \setminus \{0\} \longrightarrow \mathbb{N}_0$$

sodass für je zwei Elemente $a, b \in R \setminus \{0\}$ Elemente $q, r \in R$ existieren mit

(i) $a = q \cdot b + r$; und

(ii) $r = 0$ oder $d(r) < d(b)$.

Wir bezeichnen dies als **Division von a durch b mit Rest r**. Die Abbildung d heißt **euklidische Norm**.

Beispiel 4.8.2 (*Hauptbeispiele*)

(a) Der Ring $\mathbb{Z}$ ist euklidisch mit euklidischer Norm

$$\begin{array}{rccc} d: & \mathbb{Z}\setminus\{0\} & \longrightarrow & \mathbb{N}_0 \\ & m & \mapsto & d(m) := |m| \end{array}$$

(die Betragsabbildung) und der üblichen Division mit Rest.

(b) Ist K ein Körper, so ist der Polynomring $R = K[X]$ euklidisch mit euklidischer Norm

$$\begin{array}{rccc} d: & K[X]\setminus\{0\} & \longrightarrow & \mathbb{N}_0 \\ & f & \mapsto & d(f) := \deg(f) \end{array}$$

(die Gradabbildung) und der üblichen Polynomdivision.

Beispiel 4.8.3

In $\mathbb{Q}[X]$ die Division mit Rest von $a = X^2 + \frac{1}{2}X + \frac{1}{2}$ durch $b = 2X - 1$ liefert:

$$\begin{aligned} X^2 + \frac{1}{2}X + \frac{1}{2} &= (\frac{1}{2}X)\cdot(2X-1) + (X + \frac{1}{2}) \\ &= \ldots \\ &= \underbrace{(\frac{1}{2}X + \frac{1}{2})}_{q}\cdot\underbrace{(2X-1)}_{b} + \underbrace{1}_{r} \end{aligned}$$

also $d(r) = 0 < 1 = d(b)$.

Analog zu den ganzen Zahlen $\mathbb{Z}$ definiert man in jedem Integritätsring einen größten gemeinsamen Teiler (ggT) und ein kleinstes gemeinsame Vielfache (kgV). Diese sind eindeutig bis auf Multiplikation mit Einheiten (die jedes Element von R teilen).
Außerdem kann in euklidischen Ringen wie in $\mathbb{Z}$ den euklidische Algorithmus zur Bestimmung des ggT durchgeführt werden.

Satz 4.8.4 (*Euklidischer Algorithmus*)

Ist R ein euklidischer Ring, so terminiert die sukzessive Division mit Rest von $a_1, a_2 \in R\setminus\{0\}$ und liefert eine Darstellung

$$\mathrm{ggT}(a_1, a_2) = a_1\cdot u + a_2\cdot v$$

mit $u, v \in R$.

Beispiel 4.8.5

Wir bestimmen den größten gemeinsamen Teiler von

$$f_1 = X^4 + X^3 \quad \text{und} \quad f_2 = X^4 - 1$$

in $\mathbb{Q}[X]$ mit dem euklidischen Algorithmus:

$$\begin{aligned} X^4 + X^3 &= 1 \cdot (X^4 - 1) + (X^3 + 1) \\ X^4 - 1 &= X \cdot (X^3 + 1) + (-X - 1) \\ (X^3 + 1) &= (-X^2) \cdot (-X - 1) + (-X^2 + 1) \\ &= (-X^2 + X) \cdot (-X - 1) + (X + 1) \\ &= (-X^2 + X - 1) \cdot (-X - 1) + 0 \end{aligned}$$

Die Reste sind rot markiert und wir erhalten $\mathrm{ggT}(f_1, f_2) = -X - 1$. Da der ggT nur bis auf Multiplikation mit Elementen aus $\mathbb{Q}[X]^\times = \mathbb{Q}^\times = \mathbb{Q} \setminus \{0\}$ eindeutig ist (jedes Element ist durch eine Einheit teilbar), können wir genauso schreiben

$$\mathrm{ggT}(f_1, f_2) = (-1) \cdot (-X - 1) = (X + 1)\,.$$

4.9 Hauptidealringe und Faktorielle Ringe

4.9.1 Hauptidealringe: Eigenschaften

Definition 4.9.1

Ein Integritätsring R heißt R **Hauptidealring**, falls jedes Ideal von R von einem einzigen Element erzeugt ist. (Anders gesagt ist jedes Ideal I von R der Form $I = (a) = \{r \cdot a \mid r \in R\}$ für ein $a \in R$).

Beispiel 4.9.2 (*Hauptidealring*)

Der Ring $(\mathbb{Z}, +, \cdot)$ der ganzen Zahlen ist ein Hauptidealring, da jedes Ideal von $\mathbb{Z}$ der Form

$$n\mathbb{Z} = \{n \cdot r \mid r \in \mathbb{Z}\} = (n) \qquad (n \in \mathbb{N}_0)$$

ist.

Satz 4.9.3

Jeder euklidische Ring ist ein Hauptidealring.

Beweis: Sei R ein euklidischer Ring mit euklidischer Norm $d : R \setminus \{0\} \longrightarrow \mathbb{N}_0$ und sei I ein Ideal von R.

- Falls $I = \{0\}$ ist, dann gilt $I = (0)$.
- Falls $I \neq \{0\}$ ist, betrachten wir $b \in I \setminus \{0\}$ mit $d(b)$ minimal. Sei nun $a \in I$ beliebig und schreibe $a = q \cdot b + r$ mit $r = 0$ oder $d(r) < d(b)$. Da $a, b \in I$, so ist auch $r \in I$, denn $r = a - q \cdot b$ ist. Also muss $r = 0$ sein, denn sonst hätten wir ein Element kleinerer Norm (als b) gefunden. Somit ist $a \in (b)$ und es folgt $I \subset (b) \subset I$, also $I = (b)$. ∎

Anmerkung 4.9.4 (*Faktorielle Ringe*)

Es kann gezeigt werden, dass Hauptidealringe eigentlich sogenanten **faktorielle Ringe** sind, d.h. es gibt eine bis auf Einheiten eindeutige Primfaktorisierung (ohne Beweis). Insbesondere existiert der ggT und ist bis auf Einheiten eindeutig.

Mithilfe des ggT können wir zu jedem Ideal einen Erzeuger angeben:

Lemma 4.9.5

Ist R ein Hauptidealring, dann gilt $(a_1, a_2) = \big(\mathrm{ggT}(a_1, a_2)\big)$ für alle $a_1, a_2 \in R$.

Beweis: Nach Definition eines Hauptidealringes existiert $a \in R$ mit

$$(a_1, a_2) = (a)\,.$$

Somit gilt $a_1, a_2 \in (a)$ und es existieren $r_1, r_2 \in R$ mit $a_1 = r_1 \cdot a$ und $a_2 = r_2 \cdot a$, also $a|a_1$ und $a|a_2$. Umgekehrt ist $a \in (a_1, a_2)$ und somit existieren $u, v \in R$ mit $a = u \cdot a_1 + v \cdot a_2$. Deswegen ist jeder gemeinsamer Teiler von a_1 und a_2 schon ein Teiler von a, also $a = \mathrm{ggT}(a1, a2)$. Die Behauptung folgt. ■

Beispiel 4.9.6

(a) In $\mathbb{Z}$ gilt $(100, 30) = (10)$.

(b) In $\mathbb{Q}[X]$ gilt $(X^4 + X^3, X^4 - 1) = (X + 1)$ nach Beispiel 4.8.5.

Manchmal haben Polynomringe $R[X]$ die gleichen Eigenschaften als den Ring R selbst. Dies gilt z.B. für faktorielle Ringe:

Satz 4.9.7 (*Satz von Gauß, Ohne Beweis*)

Sei R ein Integritätsring. Dann gilt:

$$R \text{ faktoriell} \quad \Longleftrightarrow \quad R[X] \text{ faktoriell.}$$

Beispiel 4.9.8

(a) Der Polynomring $\mathbb{Z}[X]$ ist kein Hauptidealring (aber faktoriell): Aufgabe, Blatt 10.

(b) Sei K ein Körper. Der Integritätsring $R := K[X, Y, Z, W]/(XY - ZW)$ ist nicht faktoriell, denn

$$\overline{X} \cdot \overline{Y} = \overline{Z} \cdot \overline{W}$$

(Damit gibt es keine bis auf Einheiten eindeutige Primfaktorisierung.)

4.9.2 Der Chinesicher Restsatz in Hauptidealringe

Wir wollen nun das Lösen von simultanen Kongruenzen, das wir in Teil I über dem Ring $\mathbb{Z}$ der ganzen Zahlen bewiesen haben, allgemeiner für einen Hauptidealring R betrachten. Errinerung: In $\mathbb{Z}$ gilt

$$x \equiv a \mod n \qquad \Longleftrightarrow \qquad \overline{x} = \overline{a} \text{ in } \mathbb{Z}/n = \mathbb{Z}/n\mathbb{Z}\,.$$

Dabei ist $n\mathbb{Z}$ ein Ideal von $\mathbb{Z}$.
Nach Satz 4.6.2 können wir den Faktorring R/I von R nach einem beliebigen Ideal I bilden, das heißt *modulo I rechnen*.

Zunächst brauchen wir einen Begriff der *Teilerfremdheit* für Ideale.

Definition 4.9.9

Seien $I_1, I_2 \subset R$ Ideale eines kommutativen Ringes R.

(a) Die **Summe** von I_1 und I_2 ist $I_1 + I_2 := \{a_1 + a_2 \mid a_1 \in I_1, a_2 \in I_2\}$. (Dies ist offensichtlich ein Ideal von R.)

(b) Der **Durchschnitt** von I_1 und I_2 ist $I_1 \cap I_2$. (Dies ist offensichtlich ein Ideal von R.)

(c) I_1 und I_2 heißen **coprim**, wenn $I_1 + I_2 = R$. (Beachte: dabei gilt $R = (1)$.)

Lemma 4.9.10

Ist R ein Hauptidealring und $a_1, a_2 \in R$, dann gelten

$$(a_1) + (a_2) = (a_1, a_2) = \big(\mathrm{ggT}(a_1, a_2)\big)$$

und

$$(a_1) \cap (a_2) = \big(\mathrm{kgV}(a_1, a_2)\big)\,.$$

Insbesondere gilt: (a_1) und (a_2) sind coprim $\iff \mathrm{ggT}(a_1, a_2) = 1$ (bis auf Multiplikation mit einer Einheit).

Beweis: Die 1. Aussage ist Lemma 4.9.5. Zweite Aussage: Aufgabe, Blatt 10. ■

Damit können wir eine allgemeine Version des Chinesischen Restsatzes formulieren:

Satz 4.9.11 (*Chinesischer Restsatz für Hauptidealringe*)

Sei R ein Hauptidealring und $(a_1), \ldots, (a_s)$ paarweise coprime Ideale. Dann ist die Abbildung

$$\begin{array}{ccc} R/\big((a_1) \cap \ldots \cap (a_s)\big) & \longrightarrow & R/(a_1) \times \cdots \times R/(a_2) \\ \overline{r} = r + (a_1) \cap \ldots \cap (a_s) & \mapsto & (\overline{r} = r + (a_1), \ldots, \overline{r} = r + (a_s)) \end{array}$$

ein Ring-Isomorphismus.

Beweis (Sketch): Die Abbildung

$$\begin{array}{rccc} f: & R & \longrightarrow & R/(a_1) \times \cdots \times R/(a_2) \\ & r & \mapsto & (\overline{r} = r + (a_1), \ldots, \overline{r} = r + (a_s))\,. \end{array}$$

ist ein surjektiver Ringhomomorphismus mit Kern $\ker(f) = (a_1) \cap \ldots \cap (a_s)$. Somit liefert der Homomorphiesatz einen Ring-Isomorphismus wie verlangt:

$$R/\big((a_1) \cap \ldots \cap (a_s)\big) \cong R/(a_1) \times \cdots \times R/(a_2)\,.$$

■

Beispiel 4.9.12

Falls $R = \mathbb{Z}$ ist, so erhalten wir erneut Satz 4.2.11: Für $n_1, \ldots n_s \in \mathbb{N}$ teilerfremd gilt

$$\mathbb{Z}/\big((n_1) \cap \ldots \cap (n_s)\big) \cong \mathbb{Z}/(n_1) \times \mathbb{Z}/(n_s)\,,$$

wobei $\mathbb{Z}/(n_1) = \mathbb{Z}/n_1\mathbb{Z} = \mathbb{Z}/n_1, \ldots, \mathbb{Z}/(n_s) = \mathbb{Z}/n_s\mathbb{Z} = \mathbb{Z}/n_s$ und nach Lemma 4.9.10 ist

$$(n_1) \cap \ldots \cap (n_s) = (\mathrm{kgV}(n_1, \ldots, n_s)) = (n_1 \cdot \ldots \cdot n_s)\,.$$

Also erhalten wir

$$\mathbb{Z}/(n_1 \cdot \ldots \cdot n_s) \cong \mathbb{Z}/n_1 \times \cdots \times \mathbb{Z}/n_s\,.$$

Beispiel 4.9.13

Wir bestimmen die Lösungsmenge L in $\mathbb{Q}[X]$ der simultanen Kongruenzen

$$\begin{aligned} f(X) &\equiv 3 \mod X+1 \\ f(X) &\equiv 2+X \mod X^2+X+1\,. \end{aligned}$$

Mit dem euklidischen Algorithmus erhalten wir, dass $X+1$ und X^2+X+1 teilerfremd sind und

$$1 = \mathrm{ggT}(X+1, X^2+X+1) = \underbrace{(-X)}_{u}\cdot(X+1) + \underbrace{1}_{v}\cdot(X^2+X+1)$$

Wenn wir die Lösungsformel in $\mathbb{Z}$ von Teil I übertragen (siehe Beweis von Satz 2.4.1), dann erhalten wir eine Lösung:

$$\begin{aligned} Z(X) &= (2+X)\cdot u\cdot(X+1) + 3\cdot v\cdot(X^2+X+1) \\ &= (2+X)\cdot(-X)\cdot(X+1) + 3\cdot 1\cdot(X^2+X+1) \\ &= \ldots \\ &= -X^3+X+3 \end{aligned}$$

Damit ist die Lösungsmenge

$$\begin{aligned} L &= \{(-X^3+X+3) + g(X)\cdot(X+1)\cdot(X^2+X+1) \mid g(X)\in\mathbb{Q}[X]\} \\ &= \{(-X^3+X+3) + g(X)\cdot(X^3+2X^2+2X+1) \mid g(X)\in\mathbb{Q}[X]\} \\ &= \{(-X^3+X+3) + 1\cdot(X^3+2X^2+2X+1) + g'(X)\cdot(X^3+2X^2+2X+1) \mid g'(X)\in\mathbb{Q}[X]\} \\ &= \{(2X^2+3X+4) + g'(X)\cdot(X^3+2X^2+2X+1) \mid g'(X)\in\mathbb{Q}[X]\} \\ &= (2X^2+3X+4) + (X^3+2X^2+2X+1)\mathbb{Q}[X] \\ &= \overline{(2X^2+3X+4)} \end{aligned}$$

Insbesondere können wir eine eindeutige Lösung $2X^2+3X+4$ von Grad <3 durch Division mit Rest von $-X^3+X+3$ nach X^3+2X^2+2X+1 finden.
Anders formuliert: der Chinesische Restsatz gibt den Ring-Isomorphismus:

$$\mathbb{Q}[X]/\big((X+1)\cdot(X^2+X+1)\big) \cong \mathbb{Q}[X]/(X+1) \times \mathbb{Q}[X]/(X^2+X+1)$$

unter dem die Lösungsmenge L der simultanen Kongruenzen das eindeutige Urbild von $(\overline{3}, \overline{2+X})$ ist, d.h.

$$L = \overline{(2X^2+3X+4)} \mapsto (\overline{3}, \overline{2+X})\,.$$

Beachte: wir nutzen hier, dass $\mathbb{Q}[X]$ euklidisch ist, indem wir die Division mit Rest von Polynomen verwenden.