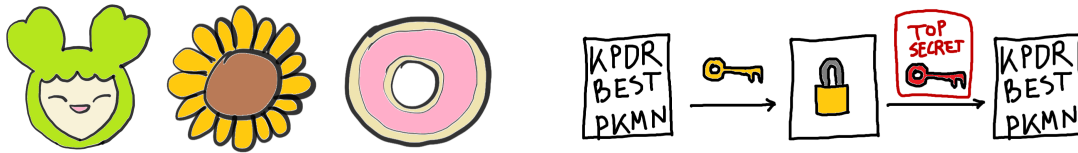


# Algebraische Strukturen

Arbeitsgemeinschaft am Heinrich-Hertz-Gymnasium (2023/24)



Dokument: Jordi Kling (✉ [jordikling@posteo.de](mailto:jordikling@posteo.de))

Stand: 18.06.2024

## Inhalte

---

- **Gruppen** (symmetrische Gruppe, orthogonale Gruppe der Euklidischen Ebene, Drehgruppe, Dieder-Gruppe, ...)
- **Untergruppen** und der **Satz von Lagrange** (Äquivalenzrelationen und Nebenklassen)
- Addition und Multiplikation von **Restklassen** (diskrete/r Exponentialfunktion und Logarithmus, Satz von Euler und von Fermat, Chinesischer Restsatz), Anwendungen in der **Kryptographie** (Diffie-Hellman-Schlüsselaustausch und RSA-Verschlüsselungsverfahren)
- **Homomorphismen** und Isomorphismen von Gruppen, Quotientengruppen, Homomorphiesatz

(Ringe und Körper haben wir leider nicht geschafft.)

## Inhaltsverzeichnis

---

<b>I Gruppen</b>	<b>2</b>
§1 Definitionen und Beispiele . . . . .	2
Die symmetrische Gruppe . . . . .	8
Die orthogonale Gruppe der Euklidischen Ebene . . . . .	12
Gruppen als Symmetrien . . . . .	17
§2 Untergruppen und der Satz von Lagrange . . . . .	20
§3 Restklassen und Zahlentheorie . . . . .	31
Die diskrete Exponentialfunktion und der Diffie-Hellman-Schlüsselaustausch . . . . .	35
Der Satz von Euler und das RSA-Verfahren . . . . .	38
§4 Isomorphie von Gruppen . . . . .	45
Der Homomorphiesatz . . . . .	51

# I Gruppen

Im ersten langen Kapitel beschäftigen wir uns mit **Gruppen** — dies sind Mengen zusammen mit einer Verknüpfung, die bestimmte Eigenschaften erfüllt. Besagte Eigenschaften *kennen* wir schon von den Grundrechenarten auf den Zahlenbereichen und verallgemeinern sie auf abstrakte Mengen.

Gruppen sind ein zentraler mathematischer Denkgegenstand mit umfangreicher Theorie. Sie tauchen in so gut wie jedem Zweig der Mathematik auf — auch außerhalb der abstrakten Algebra.

Besonders interessant werden für uns **Restklassen** sein (ganze Zahlen modulo  $n$ ) — vor allem deren Rolle in der **Kryptographie**, wenn  $n$  eine sehr große Primzahl ist. Ein allgegenwärtiges Beispiel ist die Ver- und Entschlüsselung geheimer Nachrichten mittels des RSA-Verfahrens.

## §1 — Definitionen und Beispiele

In diesem Unterkapitel führen wir verschiedene algebraische Strukturen ein und leiten der Reihe nach die Definition einer **Gruppe** her.

Wir beschäftigen uns etwas ausführlicher mit Beispielen von Gruppen als **Symmetrien** von Mengen (symmetrische Gruppe, orthogonale Gruppe der Euklidischen Ebene).

◇ — ◇ — ◇

Sei immer  $M$  eine nichtleere Menge.

### Definition 1.1 (Verknüpfung)

Eine **Verknüpfung**  $\circ$  auf  $M$  ordnet je zwei Elementen  $a, b \in M$  ein weiteres Element aus  $M$  zu, geschrieben  $a \circ b$  (gesprochen “ $a$  Kringel  $b$ ” oder “ $a$  verknüpft mit  $b$ ”).

Mit anderen Worten ist eine Verknüpfung auf  $M$  eine Abbildung  $\circ : M \times M \rightarrow M$ , und zwar mit der Vorschrift  $(a, b) \mapsto a \circ b$ .

*Zur Erinnerung* — Das **kartesische Produkt** zweier Mengen  $A$  und  $B$  ist die Menge  $A \times B = \{(a, b) \mid a \in A \text{ und } b \in B\}$  der geordneten Paare (Tupel) mit Einträgen in  $A$  und  $B$ . (*Jeder kennt das zweidimensionale kartesische Koordinatensystem  $\mathbb{R} \times \mathbb{R}$ .*)

Betrachten wir zunächst einige Beispiele und Nicht-Beispiele für Verknüpfungen.

### Beispiel 1.2 (Beispiele für Verknüpfungen)

- ①  $M := \mathbb{N} = \{1, 2, 3, \dots\}$  mit  $\circ :=$  Addition oder  $\circ :=$  Multiplikation
- ② Die Subtraktion ist **keine** Verknüpfung auf  $\mathbb{N}$ , denn  $1 - 2 \notin \mathbb{N}$ ; aber auf  $\mathbb{Z}$ .
- ③  $M := \mathbb{Q}$  mit  $a \circ b := \frac{1}{2}(a + b)$  (*Dies ist der Mittelwert von  $a$  und  $b$ .*)

Spannender ist der Fall, wenn  $M$  keine Menge von Zahlen ist:

- ④ Sei  $M$  die Menge aller Zeichenketten über dem Alphabet  $\{a, \dots, z\}$ . Die **Konkatenation** von  $x := "x_1 \dots x_n"$  und  $y := "y_1 \dots y_m"$  sei definiert durch  $x \circ y := "x_1 \dots x_n y_1 \dots y_m"$  (wobei  $n, m \in \mathbb{N}_0$ ), also durch das Aneinanderhängen der Zeichenketten. Dies ist eine Verknüpfung auf  $M$ .

⋮

- ⑤ Definiere die **Hintereinanderausführung** zweier Abbildungen  $f : X \rightarrow Y$  und  $g : Y \rightarrow Z$  als die Abbildung  $g \circ f : X \rightarrow Z$  mit  $(g \circ f)(x) := g(f(x))$ .

Dann ist auf der Menge  $M := \text{Abb}(X, X)$  aller Abbildungen  $X \rightarrow X$  eine Verknüpfung definiert durch  $(f, g) \mapsto f \circ g$ .

*Beispiel* —  $X := \mathbb{R}$ ,  $f(x) := 2x + 1$ ,  $g(x) := 3x^2$

- $f \circ g$  ist gegeben durch  $(f \circ g)(x) = 2 \cdot 3x^2 + 1 = 6x^2 + 1$ .
- $g \circ f$  ist gegeben durch  $(g \circ f)(x) = 3 \cdot (2x + 1)^2$ .

Dies führt uns zu unserer ersten, recht langweiligen algebraischen Struktur.

### Definition 1.3 (*Magma*)

Ein **Magma** (“*das Magma*”, “*mehrere Magmen*”) besteht aus einer nichtleeren Menge  $M$  und einer Verknüpfung  $\circ$  auf  $M$ .

Wir schreiben dafür  $(M, \circ)$  — oder einfach nur  $M$ , falls  $\circ$  aus dem Kontext klar ist.<sup>1</sup>

Magmen sind deswegen langweilig, weil wir keine Ansprüche an die zugrunde liegende Verknüpfung haben, die sie interessant machen könnten. Aus der Grundschule kennen wir jedoch bereits einige *gute* Eigenschaften, die eine Verknüpfung haben kann.

### Definition 1.4 (*Eigenschaften von Verknüpfungen*)

Eine Verknüpfung  $\circ$  auf  $M$  heißt...

- ① ... **assoziativ**, falls  $(a \circ b) \circ c = a \circ (b \circ c)$  für alle  $a, b, c \in M$  gilt.
- ② ... **kommutativ**, falls  $a \circ b = b \circ a$  für alle  $a, b \in M$  gilt.

### Bemerkung 1.5

- ① Bei assoziativen Verknüpfungen dürfen die Klammern also weggelassen werden. Anstelle von  $(a \circ b) \circ c$  oder  $a \circ (b \circ c)$  schreibe dann auch einfach  $a \circ b \circ c$ .
- ② Bei kommutativen Verknüpfungen spielt die Reihenfolge der Elemente also keine Rolle.

### Beispiel 1.6 (*Beispiele für assoziative oder kommutative Verknüpfungen*)

- ① Die Addition und Multiplikation auf  $\mathbb{N}$  sind beide sowohl assoziativ als auch kommutativ.
- ② Die Subtraktion auf  $\mathbb{Z}$  ist **weder** assoziativ **noch** kommutativ.
- ③ Die Mittelwertbildung auf  $\mathbb{Q}$  ist...
  - ... **nicht** assoziativ, denn  $(1 \circ 2) \circ 3 = \frac{3}{2} \circ 3 = \frac{9}{4}$ , aber  $1 \circ (2 \circ 3) = 1 \circ \frac{5}{2} = \frac{7}{4}$ .
  - ... kommutativ, denn  $a \circ b = \frac{1}{2}(a + b) = \frac{1}{2}(b + a) = b \circ a$ .

<sup>1</sup>Dabei handelt es sich um **Notationsmissbrauch**, denn man muss sich aus dem Kontext erschließen, ob einfach nur die Menge  $M$  gemeint ist, oder die Menge  $M$  zusammen mit der Verknüpfung  $\circ$ .

④ Die Konkatenation von Zeichenketten ist...

- ... assoziativ, denn für  $x := "x_1 \dots x_n"$ ,  $y := "y_1 \dots y_m"$ , und  $z := "z_1 \dots z_\ell"$  gilt  $(x \circ y) \circ z = x \circ (y \circ z) = "x_1 \dots x_n y_1 \dots y_m z_1 \dots z_\ell"$ .
- ... **nicht** kommutativ, denn zum Beispiel ist  $"x" \circ "y" = "xy"$ , aber  $"y" \circ "x" = "yx"$ .

⑤ Die Hintereinanderausführung von Abbildungen  $X \rightarrow X$  ist...

- ... assoziativ. Um  $(f \circ g) \circ h = f \circ (g \circ h) \in \text{Abb}(X, X)$  zu zeigen, müssen wir überprüfen, dass die Funktionswerte dieser beiden Abbildungen für alle  $x \in X$  übereinstimmen. Sei also  $x \in X$  beliebig. Dann gilt wie gewünscht:

$$((f \circ g) \circ h)(x) = (f \circ g)(h(x)) = f(g(h(x))), \text{ und}$$

$$(f \circ (g \circ h))(x) = f((g \circ h)(x)) = f(g(h(x))).$$

- ... **nicht** kommutativ. In **Beispiel 1.2** ⑤ haben wir schon explizite  $f, g \in \text{Abb}(\mathbb{R}, \mathbb{R})$  mit  $f \circ g \neq g \circ f$  gesehen.

Es stellt sich heraus, dass Assoziativität eine Eigenschaft ist, die eine Verknüpfung wenigstens haben sollte, um sinnvoll zu sein. Dies führt zur nächsten algebraischen Struktur.

### Definition 1.7 (Halbgruppe)

Eine **Halbgruppe** ist ein Magma mit assoziativer Verknüpfung.

Betrachtet man die wohlbekannte Halbgruppe  $(\mathbb{Z}, +)$ , fällt auf, dass eine Zahl ganz besonders ist: Die Null, denn für alle  $x \in \mathbb{Z}$  gilt bekanntlich  $0 + x = x$  und  $x + 0 = x$ . (*Sie tut also nichts.*)

Auch diesen Gedanken möchten wir verallgemeinern.

### Definition 1.8 (Neutrales Element)

Sei  $M$  ein Magma. Ein Element  $e \in M$  heißt **neutrales Element**, falls  $e \circ a = a$  und  $a \circ e = a$  für alle  $a \in M$  gilt.

Die Null ist also neutral in  $(\mathbb{Z}, +)$ , und die Eins ist neutral in  $(\mathbb{Z}, \cdot)$ . Darüber hinaus gibt es jeweils **keine** weitere Zahl mit der entsprechenden Eigenschaft.

Auch dies ist ein allgemeines Resultat, das allein aus der Definition von Neutralität folgt.

### Satz 1.9 (Eindeutigkeit des neutralen Elements)

Falls ein Magma ein neutrales Element besitzt, ist dieses **eindeutig** bestimmt.

*Beweis.* Seien  $e_1, e_2 \in M$  neutrale Elemente. Wir möchten  $e_1 = e_2$  schließen. Betrachte dazu den Term  $e_1 \circ e_2$ .

- Einerseits ist  $e_1$  neutral (von links), also  $e_1 \circ e_2 = e_2$ .
- Andererseits ist  $e_2$  neutral (von rechts), also  $e_1 \circ e_2 = e_1$ .

Daraus folgt  $e_1 = e_2$  wie gewünscht.



Halbgruppen mit neutralem Element sind wiederum interessanter als Halbgruppen ohne neutrales Element, deswegen gibt es auch für diese algebraische Struktur einen neuen Namen.

### Definition 1.10 (*Monoid*)

Ein **Monoid** ist eine Halbgruppe mit neutralem Element.

### Bemerkung 1.11

- ① Die Eindeutigkeit des neutralen Elements rechtfertigt die allgemeine Schreibweise  $e \in M$  für das neutrale Element eines Monoids  $M$ .

Man sagt auch,  $e \in M$  ist ein **ausgezeichnetes** Element, weil man in jedem Monoid sagen kann: “*Das da.*”

- ② Anstelle von “ $e$ ” gibt es manchmal auch alternative Schreibweisen.
- Im Falle einer plus-ähnlichen Verknüpfung  $\circ = +$  schreibt man auch  $e = 0$ .
  - Im Falle einer mal-ähnlichen Verknüpfung  $\circ = \cdot$  schreibt man auch  $e = 1$ .

### Beispiel 1.12 (*Beispiele für Monoide*)

- ① Die ganzen Zahlen mit der Addition sind ein Monoid. Das neutrale Element ist 0.
- ② Die ganzen Zahlen mit der Multiplikation sind ein Monoid. Das neutrale Element ist 1.
- ③ Die Zeichenketten mit der Konkatenation sind ein Monoid. Das neutrale Element ist die leere Zeichenkette  $\varepsilon := ""$ .
- ④ Die Abbildungen  $X \rightarrow X$  mit der Hintereinanderausführung sind ein Monoid. Das neutrale Element ist die **Identität**  $\text{id}_X : X \rightarrow X$ , gegeben durch  $\text{id}_X(x) := x$ .
- ⑤ Kein Monoid bilden zum Beispiel die natürlichen Zahlen mit der Addition, da hier  $0 \notin \mathbb{N}$ .

Im Folgenden möchten wir noch das Konzept der **Gegenzahl** bzw. des **Kehrwerts** verallgemeinern. Für  $x \in \mathbb{R}$  waren das die durch  $x + ? = 0$  bzw. (falls  $x \neq 0$ )  $x \cdot ? = 1$  definierten reellen Zahlen, notiert mit  $-x$  bzw.  $\frac{1}{x}$ .

### Definition 1.13 (*Inverses Element*)

Sei  $M$  ein Monoid. Ein Element  $a \in M$  heißt **invertierbar**, falls es ein  $b \in M$  gibt mit  $b \circ a = e$  und  $a \circ b = e$ . In diesem Fall heißt  $b$  **invers** zu  $a$ .

Bemerke auch hier wieder, dass die Notation  $-x$  bzw.  $\frac{1}{x}$  im bekannten reellen Fall Eindeutigkeit der jeweiligen Zahl impliziert (es gibt keine zwei Gegenzahlen bzw. Kehrwerte einer Zahl), was auch allgemein wieder der Fall ist.

### Satz 1.14 (*Eindeutigkeit der inversen Elemente*)

Falls ein Element eines Monoids invertierbar ist, ist das inverse Element eindeutig bestimmt.

Der Beweis verläuft ganz ähnlich zu dem der Eindeutigkeit des neutralen Elements.

*Beweis.* Seien  $b_1, b_2 \in M$  invers zu  $a \in M$ . Wir möchten  $b_1 = b_2$  schließen. Betrachte dazu den Term  $b_1 \circ a \circ b_2$ . Weil  $\circ$  assoziativ ist, dürfen beliebig Klammern gesetzt werden.

- Einerseits ist  $b_1$  invers zu  $a$  (von links), also  $(b_1 \circ a) \circ b_2 = e \circ b_2 = b_2$ .
- Andererseits ist  $b_2$  invers zu  $a$  (von rechts), also  $b_1 \circ (a \circ b_2) = b_1 \circ e = b_1$ .

Daraus folgt  $b_1 = b_2$  wie gewünscht. ♥

### Bemerkung 1.15

- ① Die Eindeutigkeit des zu  $a$  inversen Elements (sofern existent) rechtfertigt die allgemeine Schreibweise  $a^{-1}$ .
- ② ⚠ **VORSICHT!** Dies ist eine abstrakte Notation. Man könnte genauso gut  $a'$  oder  $\bar{a}$  schreiben (zum Beispiel), was allerdings nicht üblich ist. Der Exponent  $-1$  ist in diesem Moment erstmal bedeutungslos.

Im Allgemeinen ist damit nicht der Kehrwert gemeint. Bezüglich der Addition ganzer Zahlen ist zum Beispiel  $a^{-1} = -a$ . Auch  $\sin^{-1}$  (kommt daher) ist nicht dasselbe wie der Kehrwert des Sinus!

Für inverse Elemente gibt es allgemeine Rechenregeln.

### Satz 1.16 (Rechenregeln für inverse Elemente)

Sei  $M$  ein Monoid, und seien  $a, b \in M$  invertierbar. Dann gilt:

- ①  $e$  ist invertierbar, und zwar mit  $e^{-1} = e$ .
- ②  $a^{-1}$  ist invertierbar, und zwar mit  $(a^{-1})^{-1} = a$ .
- ③  $a \circ b$  ist invertierbar, und zwar mit  $(a \circ b)^{-1} = b^{-1} \circ a^{-1}$ . (⚠ Reihenfolge beachten!)

*Beweis.* Der Beweis erfolgt leicht durch Nachrechnen.

- ① Es gilt  $e \circ e = e$ .
- ② Es gilt  $a \circ a^{-1} = e$  und  $a^{-1} \circ a = e$ . (So lesen:  $a$  ist linksinvers bzw. rechtsinvers zu  $a^{-1}$ .)
- ③ Es gilt...
  - ... von links:  $b^{-1} \circ a^{-1} \circ a \circ b = b^{-1} \circ e \circ b = b^{-1} \circ b = e$ , sowie
  - ... von rechts:  $a \circ b \circ b^{-1} \circ a^{-1} = a \circ e \circ a^{-1} = a \circ a^{-1} = e$ .



Wie sich herausstellt, führt die zusätzliche Forderung von Invertierbarkeit aller Elemente zu einem sehr interessanten mathematischen Denkobjekt mit umfangreicher Theorie.

### Definition 1.17 (Gruppe)

Eine **Gruppe** ist ein Monoid, in dem jedes Element invertierbar ist.

Gruppen sind die zentrale algebraische Struktur, die wir in diesem Kurs betrachten.

Bevor wir zu interessanteren Beispielen von Gruppen kommen, greifen wir zunächst die altbekannten Beispiele und Nicht-Beispiele wieder auf.

### Beispiel 1.18 (*Beispiele für Gruppen*)

- ① Die rationalen Zahlen mit der Addition sind eine Gruppe.

Das neutrale Element ist  $e = 0 \in \mathbb{Q}$ .

Das zu  $\frac{p}{q} \in \mathbb{Q}$  inverse Element ist  $(\frac{p}{q})^{-1} = -\frac{p}{q} \in \mathbb{Q}$ .

- ② Die rationalen Zahlen mit der Multiplikation sind zwar ein Monoid mit neutralem Element  $e = 1 \in \mathbb{Q}$ , aber **keine** Gruppe.

Der Grund ist, dass  $0 \cdot ? = 1$  nicht lösbar, also 0 nicht invertierbar ist.

- ③ Aber  $\mathbb{Q} \setminus \{0\}$  mit der Multiplikation ist eine Gruppe.

Das zu  $\frac{p}{q} \in \mathbb{Q} \setminus \{0\}$  inverse Element ist  $(\frac{p}{q})^{-1} = \frac{q}{p} \in \mathbb{Q} \setminus \{0\}$ . (Hier wirklich der Kehrwert.)

- ④ Die Zeichenketten mit der Konkatenation sind **keine** Gruppe.

Zum Beispiel ist "x" nicht invertierbar, denn egal was man (von links oder rechts) anhängt, die Zeichenkette enthält immer noch "x" und ist damit insbesondere nicht leer.

- ⑤ Die Selbstabbildungen  $X \rightarrow X$  mit der Hintereinanderausführung sind **keine** Gruppe.

Betrachte zum Beispiel den wohlbekannten Fall  $X := \mathbb{R}$  und  $f(x) := x^2$ . Es müsste eine Abbildung  $g$  geben mit  $x \xrightarrow{f} x^2 \xrightarrow{g} x$  für alle  $x \in \mathbb{R}$ , also  $g \circ f = \text{id}_{\mathbb{R}}$ .

Das geht aber **nicht**, denn zum Beispiel gilt  $f(2) = 4 = f(-2)$ ; das heißt,  $g$  müsste 4 **gleichzeitig** auf 2 und  $-2$  abbilden (also zwei Funktionswerte  $g(4)$  besitzen).

Bevor wir uns mit weiteren Beispielen von Gruppen auseinandersetzen, möchten wir noch kurz zwei allgemeine Konstrukte betrachten.

### Definition 1.19 (*Triviale Gruppe*)

Sei  $e$  irgendein Objekt. Die einelementige Menge  $G := \{e\}$  zusammen mit der einzigmöglichen Verknüpfung  $(e, e) \mapsto e$  heißt die **triviale Gruppe**.

Man überzeugt sich leicht davon, dass die triviale Gruppe wirklich eine Gruppe ist.

### Definition 1.20 (*Einheitengruppe*)

Sei  $M$  ein Monoid. Dann heißt

$$M^\times := \{a \in M \mid a \text{ ist invertierbar}\}$$

die **Einheitengruppe** von  $M$ .

Auch hier überzeugt man sich davon, dass  $M^\times$  tatsächlich eine Gruppe ist:

- Die Assoziativität wird von  $M$  geerbt.
- Aus **Satz 1.16** folgt  $e \in M^\times$ , sowie  $a^{-1} \in M^\times$  und  $a \circ b \in M^\times$  für alle  $a, b \in M^\times$ .

### Beispiel 1.21 (Beispiele für Einheitengruppen)

- ①  $(\mathbb{Q}, \cdot)^\times = \mathbb{Q} \setminus \{0\}$
- ② Zeichenketten $^\times = \{\varepsilon\}$  (die triviale Gruppe), wobei  $\varepsilon := ""$  (leere Zeichenkette)
- ③ Sei  $G$  eine Gruppe. Dann ist  $G^\times = G$ .

Nun zum ersten nicht-langweiligen Beispiel einer Gruppe (also kein Zahlenbereich).

### Die symmetrische Gruppe

Wir überlegen uns im Folgenden, welche Elemente in  $\text{Abb}(X, X)^\times$  enthalten sind. Wir haben zum Beispiel schon gesehen, dass für  $f(x) := x^2$  gilt, dass  $f \notin \text{Abb}(\mathbb{R}, \mathbb{R})^\times$  (siehe [Beispiel 1.18 \(5\)](#)).

Dazu starten wir mit etwas Vokabular.

### Definition 1.22 (Injektive, surjektive, bijektive Abbildung)

Eine Abbildung  $f : X \rightarrow Y$  heißt...

- ① ... **injektiv**, falls für alle  $x_1, x_2 \in X$  gilt: Wenn  $f(x_1) = f(x_2)$ , dann  $x_1 = x_2$ .  
Mit anderen Worten —  $f$  bildet verschiedene  $x$ -Werte auch auf verschiedene  $y$ -Werte ab. Jedes  $y \in Y$  wird höchstens einmal “getroffen”.
- ② ... **surjektiv**, falls es für alle  $y \in Y$  ein  $x \in X$  gibt mit  $f(x) = y$ .  
Mit anderen Worten — Jedes  $y \in Y$  wird mindestens einmal “getroffen”.
- ③ ... **bijektiv**, falls sie injektiv und surjektiv ist, es also für jedes  $y \in Y$  genau ein  $x \in X$  gibt mit  $f(x) = y$ .

### Definition 1.23 (Umkehrabbildung)

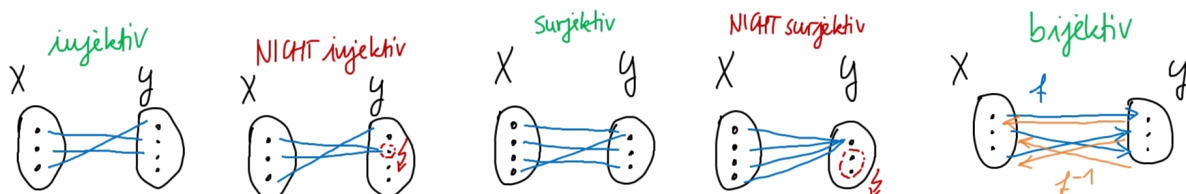
Sei  $f : X \rightarrow Y$  bijektiv. Die in diesem Falle definierbare Abbildung  $f^{-1} : Y \rightarrow X$  mit

$$y \mapsto \underline{\text{dasjenige}} \ x \in X \text{ mit } f(x) = y$$

heißt die **Umkehrabbildung** von  $f$ .

Sie erfüllt  $f^{-1}(f(x)) = x$  für alle  $x \in X$  und  $f(f^{-1}(y)) = y$  für alle  $y \in Y$ , also  $f^{-1} \circ f = \text{id}_X$  bzw.  $f \circ f^{-1} = \text{id}_Y$ .

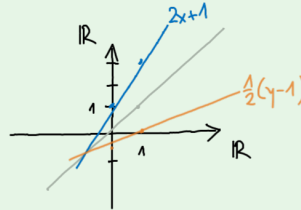
Die Begriffe werden im Folgenden primitiv illustriert.





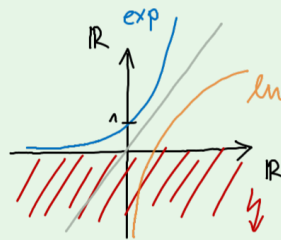
### Beispiel 1.24 (Beispiele für injektive, surjektive, bijektive Abbildungen)

- ① Sei  $X := Y := \mathbb{R}$  und  $f(x) := 2x + 1$ . Dann ist  $f$  bijektiv, und die Umkehrabbildung ist gegeben durch  $f^{-1}(y) = \frac{1}{2}(y - 1)$ .



- ② Sei  $X := Y := \mathbb{R}$  und  $f(x) := \exp(x)$  (die natürliche **Exponentialfunktion**). Dann ist  $f$  injektiv, weil streng monoton wachsend, aber nicht surjektiv, denn es gilt  $\exp(x) > 0$  für alle  $x \in \mathbb{R}$ .

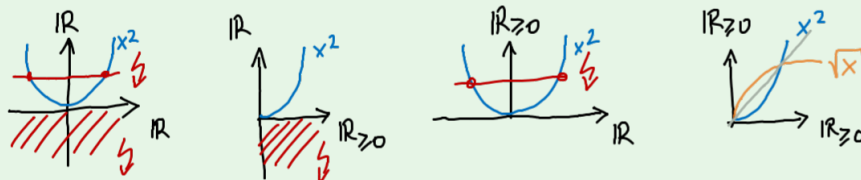
Für  $Y := \mathbb{R}_{>0}$  ist  $\exp$  aber bijektiv. Die Umkehrabbildung heißt dann  $\ln : \mathbb{R}_{>0} \rightarrow \mathbb{R}$  (der natürliche **Logarithmus**).



- ③ Sei  $X \subset \mathbb{R}$  und  $f(x) := x^2$ .

- Für  $X := Y := \mathbb{R}$  ist  $f$  weder injektiv noch surjektiv.
- Für  $X := \mathbb{R}_{\geq 0}$  und  $Y := \mathbb{R}$  ist  $f$  injektiv, aber nicht surjektiv.
- Für  $X := \mathbb{R}$  und  $Y := \mathbb{R}_{\geq 0}$  ist  $f$  nicht injektiv, aber surjektiv.
- Für  $X := Y := \mathbb{R}_{\geq 0}$  ist  $f$  bijektiv.

Die Umkehrabbildung ist die Wurzelfunktion  $\sqrt{\cdot} : \mathbb{R}_{\geq 0} \rightarrow \mathbb{R}_{\geq 0}$ .



Die folgende Bemerkung liefert äquivalente Aussagen zu Injektivität und Surjektivität, die aus algebraischer Sicht interessant sind.

### Bemerkung 1.25 (Linksinverse und rechtsinverse Abbildung)

- ① Genau dann ist  $f : X \rightarrow Y$  injektiv, wenn es eine **linksinverse** Abbildung  $g : Y \rightarrow X$  gibt mit  $g \circ f = \text{id}_X$ . (Eventuell nicht eindeutig!)
- ② Genau dann ist  $f : X \rightarrow Y$  surjektiv, wenn es eine **rechtsinverse** Abbildung  $h : Y \rightarrow X$  gibt mit  $f \circ h = \text{id}_Y$ . (Eventuell nicht eindeutig!)
- ③ Im bijektiven Falle sind  $g$  und  $h$  jeweils eindeutig, und es gilt  $g = h = f^{-1} : Y \rightarrow X$ .

Den umfangreichen Beweis haben wir im Unterricht nicht besprochen. Der Vollständigkeit halber wird er im Folgenden aber geführt.

*Beweis.*

**Zu ①.**

“ $\implies$ ”: Sei  $f$  injektiv. Wir konstruieren solch ein  $g : Y \rightarrow X$  mit  $g \circ f = \text{id}_X$  explizit.

Sei  $y \in Y$ . Dann gibt es zwei Fälle, die eintreten können:

- Es gibt kein  $x \in X$  mit  $f(x) = y$ . In diesem Falle definiere  $g(y)$  als irgendein  $x \in X$  (die konkrete Wahl spielt keine Rolle).
- Es gibt, weil  $f$  nach Voraussetzung injektiv ist, genau ein  $x \in X$  mit  $f(x) = y$ . In diesem Falle definiere  $g(y) := x$ .

Dann gilt per Konstruktion  $g(f(x)) = x$  für alle  $x \in X$ . Die Wahlfreiheit im ersten Punkt erklärt, dass  $g$  eventuell nicht eindeutig bestimmt ist.

“ $\impliedby$ ”: Es existiere  $g : Y \rightarrow X$  mit  $g \circ f = \text{id}_X$ . Wir wollen zeigen, dass  $f$  injektiv ist.

Betrachte  $x_1, x_2 \in X$  mit  $f(x_1) = f(x_2)$ . Dann gilt auch  $g(f(x_1)) = g(f(x_2))$ . Gemäß der Voraussetzung  $g \circ f = \text{id}_X$  bedeutet das aber  $x_1 = x_2$ . Also ist  $f$  injektiv.

**Zu ②.**

“ $\implies$ ”: Sei  $f$  surjektiv. Wir konstruieren  $h : Y \rightarrow X$  mit  $f \circ h = \text{id}_Y$  wieder explizit.

Sei  $y \in Y$ . Dann gibt es, weil  $f$  nach Voraussetzung surjektiv ist, mindestens ein  $x \in X$  mit  $f(x) = y$  (eventuell mehrere). Wähle davon jeweils eins aus, und setze  $h(y) := x$ . Dann gilt  $f(h(y)) = f(x) = y$  per Konstruktion.

Die Wahlfreiheit erklärt, dass  $h$  eventuell nicht eindeutig bestimmt ist.

“ $\impliedby$ ”: Es existiere  $h : Y \rightarrow X$  mit  $f \circ h = \text{id}_Y$ . Wir wollen zeigen, dass  $f$  surjektiv ist.

Sei  $y \in Y$ . Wir wollen ein  $x \in X$  finden mit  $f(x) = y$ . Dies ist schnell getan, denn  $x := h(y)$  erfüllt  $f(x) = f(h(y)) = y$  gemäß der Voraussetzung  $f \circ h = \text{id}_Y$ .

**Zu ③.**

Sei  $f$  bijektiv (also injektiv und surjektiv), und seien  $g$  und  $h$  zu  $f$  links- bzw. rechtsinverse Abbildungen. Dann betrachten wir genau wie im Beweis von [Satz 1.14](#) den Ausdruck  $g \circ f \circ h$  auf zwei Weisen und schließen daraus  $g = h$ .

Nenne diese Abbildung  $f^{-1} : Y \rightarrow X$ . Wegen  $f^{-1} \circ f = \text{id}_X$  und  $f \circ f^{-1} = \text{id}_Y$  ist dies auch wirklich die Umkehrabbildung aus [Definition 1.23](#). ♥

Mit diesem Vokabular können wir die invertierbaren Elemente von  $\text{Abb}(X, X)$  beim Namen nennen.

### Definition 1.26 (*Symmetrische Gruppe über einer beliebigen Menge*)

Sei  $X$  irgendeine Menge.<sup>2</sup> Dann heißt

$$\text{Sym}(X) := \text{Abb}(X, X)^\times = \{f : X \rightarrow X \mid f \text{ ist bijektiv}\}$$

die **symmetrische Gruppe** über  $X$ .

Das heißt, die symmetrische Gruppe über  $X$  besteht aus allen **bijektiven** (also umkehrbaren) Abbildungen  $X \rightarrow X$ .

- Das neutrale Element ist (nach wie vor) die Identität  $\text{id}_X$  mit der Vorschrift  $x \mapsto x$ .
- Das zu  $f \in \text{Sym}(X)$  inverse Element ist die (in diesem Falle existente) Umkehrabbildung  $f^{-1}$ .

Interessant ist vor allem der Sonderfall  $X := \{1, 2, \dots, n\}$ , wobei  $n \in \mathbb{N}$ .

### Definition 1.27 (*Symmetrische Gruppe*)

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

$$\text{Sym}(n) := \text{Sym}(\{1, 2, \dots, n\})$$

heißt die **symmetrische Gruppe** vom Grad  $n$ .

Für die weitere Veranschaulichung hilfreich ist, dass  $\text{Sym}(n)$  nur endlich viele Elemente enthält.

### Bemerkung 1.28 (*Permutation*)

- ① Jedes Element von  $\text{Sym}(n)$ , also jede bijektive Abbildung  $\{1, 2, \dots, n\} \rightarrow \{1, 2, \dots, n\}$ , entspricht genau einer **Permutation** (einer Umordnung) der geordneten Liste  $[1, 2, \dots, n]$ .
- ② Deswegen ist die Anzahl der Elemente von  $\text{Sym}(n)$  gegeben durch  $n! = n \cdot (n-1) \cdot \dots \cdot 2 \cdot 1$  (aus der Kombinatorik schon bekannt).

Für kleine  $n \in \mathbb{N}$  können wir die Elemente von  $\text{Sym}(n)$  schnell und explizit hinschreiben. Dabei schreiben wir  $\frac{1}{\sigma_1} \frac{2}{\sigma_2} \dots \frac{n}{\sigma_n}$  für die durch  $i \mapsto \sigma_i$  definierte Abbildung (wie eine Wertetabelle).

Die Identität ist dann also  $\frac{1}{1} \frac{2}{2} \dots \frac{n}{n}$ , und  $\left( \frac{1}{\sigma_1} \frac{2}{\sigma_2} \dots \frac{n}{\sigma_n} \right)^{-1} = \frac{\sigma_1}{1} \frac{\sigma_2}{2} \dots \frac{\sigma_n}{n}$ .

### Beispiel 1.29 (*Symmetrische Gruppen kleinen Grades*)

- ① Im Falle  $X := \{1\}$  gibt es überhaupt nur eine Abbildung  $X \rightarrow X$ , nämlich die mit der Vorschrift  $1 \mapsto 1$ . Diese ist bijektiv.

Die Gruppe  $\text{Sym}(1) = \left\{ \frac{1}{1} \right\}$  ist also trivial.

⋮

<sup>2</sup>Der Fall  $X = \emptyset$  ist explizit erlaubt, aber wird hier nicht weiter untersucht.

- ② Im Falle  $X := \{1, 2\}$  sind die bijektiven Abbildungen  $X \rightarrow X$  genau die Identität und die Vertauschung  $1 \leftrightarrow 2$ .

$$\text{Das heißt, } \text{Sym}(2) = \left\{ \begin{array}{cc} 1 & 2 \\ 1 & 2 \end{array}, \begin{array}{cc} 1 & 2 \\ 2 & 1 \end{array} \right\}.$$

- ③ Im Falle  $X := \{1, 2, 3\}$  gibt es

- die Identität,
- die einfachen Vertauschungen  $1 \leftrightarrow 2$ ,  $1 \leftrightarrow 3$ ,  $2 \leftrightarrow 3$ , sowie
- die zyklischen Vertauschungen  $1 \rightarrow 2 \rightarrow 3 \rightarrow 1$  und  $1 \rightarrow 3 \rightarrow 2 \rightarrow 1$ .

$$\text{Das heißt, } \text{Sym}(3) = \left\{ \begin{array}{ccc} 1 & 2 & 3 \\ 1 & 2 & 3 \end{array}, \begin{array}{ccc} 1 & 2 & 3 \\ 2 & 1 & 3 \end{array}, \begin{array}{ccc} 1 & 2 & 3 \\ 3 & 2 & 1 \end{array}, \begin{array}{ccc} 1 & 2 & 3 \\ 1 & 3 & 2 \end{array}, \begin{array}{ccc} 1 & 2 & 3 \\ 2 & 3 & 1 \end{array}, \begin{array}{ccc} 1 & 2 & 3 \\ 3 & 1 & 2 \end{array} \right\}.$$

Danach wird es mit dem Hinschreiben anstrengend, denn  $\text{Sym}(4)$  enthält 24 Elemente,  $\text{Sym}(5)$  enthält 120 Elemente, und so fort. (Und für unendliche Mengen  $X$  enthält  $\text{Sym}(X)$  offensichtlich unendlich viele Elemente.)

Im Allgemeinen war die Hintereinanderausführung von Abbildungen zwischen beliebigen Mengen **nicht** unbedingt kommutativ. Dies ist auch bei  $\text{Sym}(n)$  der Fall.

### Bemerkung 1.30

Genau dann ist  $\text{Sym}(n)$  kommutativ, wenn  $n \leq 2$ .

*Beweis.* Für  $n = 1$  und  $n = 2$  überzeugt man sich leicht von der Kommutativität.

Für  $n \geq 3$  betrachte zum Beispiel

- $\begin{array}{cccc} 1 & 2 & 3 & \cdots \\ 2 & 3 & 1 & \cdots \end{array} \circ \begin{array}{cccc} 1 & 2 & 3 & \cdots \\ 2 & 1 & 3 & \cdots \end{array} = \begin{array}{cccc} 1 & 2 & 3 & \cdots \\ 3 & 2 & 1 & \cdots \end{array}$ , bzw. anders herum
- $\begin{array}{cccc} 1 & 2 & 3 & \cdots \\ 2 & 1 & 3 & \cdots \end{array} \circ \begin{array}{cccc} 1 & 2 & 3 & \cdots \\ 2 & 3 & 1 & \cdots \end{array} = \begin{array}{cccc} 1 & 2 & 3 & \cdots \\ 1 & 3 & 2 & \cdots \end{array}.$

Die resultierenden Abbildungen sind unterschiedlich. ♥

Die symmetrische Gruppe ist unter anderem deswegen interessant, weil man jede Gruppe  $G$  (mit beliebig abstrakter Verknüpfung) als Teilmenge von  $\text{Sym}(G)$  (mit der Verknüpfung von Abbildungen) interpretieren kann. Dies können wir aber jetzt noch nicht präzise formulieren.

## Die orthogonale Gruppe der Euklidischen Ebene

Die Gruppe  $\text{Sym}(\mathbb{R}^2)$  ist riesig und enthält alle möglichen “wilden” Selbstabbildungen der Zahlenebene  $\mathbb{R}^2 := \mathbb{R} \times \mathbb{R}$ . (Die einzige Voraussetzung ist Bijektivität.)

Wir erhalten eine deutlich interessantere Gruppe, wenn wir mehr Struktur auf unserer Menge  $X := \mathbb{R}^2$  fordern, und mehr Ansprüche an die darauf lebenden Abbildungen stellen.

### Definition 1.31 (Euklidische Ebene)

Die **Euklidische Ebene** ist die Menge  $\mathbb{R}^2$  zusammen mit unserem üblichen Verständnis von Längen und Winkeln.

Das bedeutet, der Abstand  $d(P, Q)$  zwischen zwei Punkten  $P, Q \in \mathbb{R}^2$  sei gegeben durch die Länge der verbindenden Strecke, also  $d(P, Q) := |\overline{PQ}|$ .

Die Existenz eines Konzepts von *Abstand* (in der Form obiger Abbildung  $d : \mathbb{R}^2 \times \mathbb{R}^2 \rightarrow \mathbb{R}_{\geq 0}$ ) erlaubt es uns zu untersuchen, wie die Anwendung von  $f \in \text{Sym}(\mathbb{R}^2)$  ebendiesen Abstand zwischen Punkten beeinflusst.

### Definition 1.32 (Isometrie der Euklidischen Ebene)

Eine Abbildung  $f \in \text{Sym}(\mathbb{R}^2)$  heißt eine **Isometrie** (der Euklidischen Ebene),<sup>3</sup> falls sie die Abstände zwischen beliebigen Paaren von Punkten **unverändert** lässt.

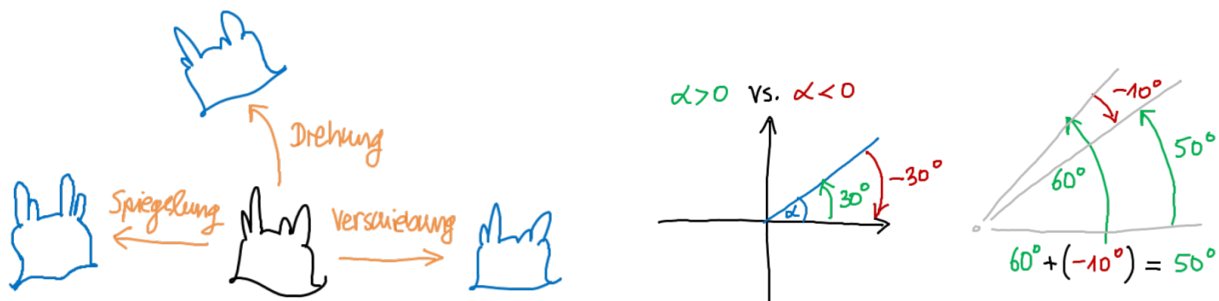
Das heißt, für alle Punkte  $P, Q \in \mathbb{R}^2$  gilt mit  $P' := f(P)$  und  $Q' := f(Q)$ , dass  $d(P', Q') = d(P, Q)$ , also  $|\overline{P'Q'}| = |\overline{PQ}|$ .

Isometrien der Euklidischen Ebene sind zum Beispiel Verschiebungen, Drehungen, und Spiegelungen (siehe Abbildung unten). Man nennt sie auch **Bewegungen** oder **Kongruenzabbildungen**. Sie verändern den Abstand zwischen je zwei Punkten nicht, Form und Größe bleibt also erhalten.

Im Folgenden sei  $\alpha \in \mathbb{R}$  immer ein **orientierter** Winkel, gemessen im Gradmaß.

- $\alpha > 0$  bedeutet, dass der Winkel im mathematischen Uhrzeigersinn gemessen wird.
- $\alpha < 0$  bedeutet, dass der Winkel entgegen dem mathematischen Uhrzeigersinn gemessen wird.

Die nachfolgende Abbildung (rechts) soll dies illustrieren.



### Definition 1.33 (Den Ursprung fixierende Drehungen und Spiegelungen)

Für einen orientierten Winkel  $\alpha \in \mathbb{R}$  definiere...

- ① ...  $d_\alpha \in \text{Sym}(\mathbb{R}^2)$  als die **Drehung** um den Koordinatenursprung um den Winkel  $\alpha$ .

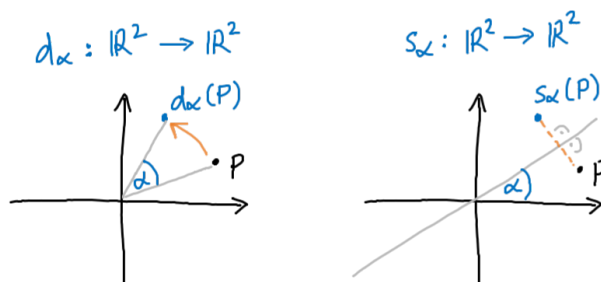
Wir schreiben  $D := \{d_\alpha \mid \alpha \in \mathbb{R}\}$  für die Menge all dieser Drehungen.

- ② ...  $s_\alpha \in \text{Sym}(\mathbb{R}^2)$  als die **Spiegelung** an der Ursprungsgeraden, die zur  $x$ -Achse den Winkel  $\alpha$  einschließt.

Wir schreiben  $S := \{s_\alpha \mid \alpha \in \mathbb{R}\}$  für die Menge all dieser Spiegelungen.

<sup>3</sup>Man braucht eigentlich nur  $f : \mathbb{R}^2 \rightarrow \mathbb{R}^2$  zu fordern, denn man kann zeigen, dass Isometrien des  $\mathbb{R}^2$  automatisch bijektiv sind. Das können wir aber nicht im Rahmen dieses Kurses.

Die Abbildungen sind nachfolgend skizziert.



Wie man leicht feststellt, sind die Abbildungen  $d_\alpha$  und  $s_\alpha$  jeweils periodisch in  $\alpha$ .

### Bemerkung 1.34

- ① Für alle  $\alpha \in \mathbb{R}$  ist  $d_\alpha = d_{\alpha+360}$  dieselbe Abbildung.  
(Denn eine Drehung um 360 Grad bewirkt nichts.)
- ② Für alle  $\alpha \in \mathbb{R}$  ist  $s_\alpha = s_{\alpha+180}$  dieselbe Abbildung.  
(Denn eine Drehung der Ursprungsgeraden um 180 Grad führt diese einfach in sich selbst über, gespiegelt wird dann also an derselben Geraden.)

Klar ist auch, dass es sich bei den  $d_\alpha$  und  $s_\alpha$  um Isometrien handelt — es sind Sonderfälle von Drehungen und Spiegelungen, und zwar diejenigen, die den Ursprung auf sich selbst abbilden.

In Wahrheit — und das ist viel spannender — gilt aber sogar die umgekehrte Aussage!

### Satz 1.35 (Charakterisierung der den Ursprung fixierenden Isometrien)

Sei  $f$  eine Isometrie der Euklidischen Ebene, die den Ursprung auf sich selbst abbildet.  
Dann gilt entweder  $f = d_\alpha$  oder  $f = s_\alpha$  für ein  $\alpha \in \mathbb{R}$ .

Den Beweis können wir im Rahmen dieses Kurses leider nicht erbringen, da er viel Grundwissen aus der Universität voraussetzt.

Die für diesen Kurs interessantere Aussage ist, dass wir eine Gruppenstruktur vorliegen haben.

### Satz 1.36 (Drehgruppe der Euklidischen Ebene)

Die Menge  $D \subset \text{Sym}(\mathbb{R}^2)$  trägt die Struktur einer kommutativen Gruppe.  
Man nennt sie auch die **Drehgruppe** der Euklidischen Ebene.

*Beweis.*

- Wir müssen prüfen, dass  $\circ$  wirklich eine Verknüpfung auf  $D$  ist, die Hintereinanderausführung zweier Drehungen also wieder eine Drehung ist.

Davon sind wir aber überzeugt, denn wenn  $d_\alpha, d_\beta \in D$ , dann ist auch  $d_\beta \circ d_\alpha = d_{\alpha+\beta} \in D$ .

⋮

- Wir müssen die Existenz des neutralen Elements prüfen.

Diese ist gegeben, denn  $\text{id}_{\mathbb{R}^2} = d_0 \in D$ .

- Zuletzt müssen wir noch die Existenz der inversen Elemente prüfen.

Aber auch diese gibt es alle, denn  $(d_\alpha)^{-1} = d_{-\alpha} \in D$ .

Folglich ist  $D$  wirklich eine Gruppe. Wegen  $d_\beta \circ d_\alpha = d_{\alpha+\beta} = d_\alpha \circ d_\beta$  ist sie kommutativ. ♥

Die Spiegelungen  $S$  bilden übrigens **keine** Gruppe, denn zum Beispiel ist  $\text{id}_{\mathbb{R}^2} = d_0 \notin S$ , aber es ist auch  $s_\beta \circ s_\alpha \notin S$ . (Zum Beispiel ist immer  $s_\alpha \circ s_\alpha = \text{id}_{\mathbb{R}^2} \notin S$ , also zweimal dieselbe Spiegelung hat am Ende nichts getan.)

Betrachtet man jedoch die Gesamtheit aller Drehungen und Spiegelungen aus  $D$  bzw.  $S$ , dann trägt diese Menge doch wieder die Struktur einer Gruppe (diesmal aber **nicht** kommutativ), nämlich der namensgebenden für diesen Unterabschnitt.

### Satz 1.37 (Orthogonale Gruppe der Euklidischen Ebene)

Die Menge  $O(\mathbb{R}^2) := D \cup S \subset \text{Sym}(\mathbb{R}^2)$  trägt die Struktur einer Gruppe.

Man nennt sie auch die **orthogonale Gruppe** der Euklidischen Ebene.

Übrigens schreibt man man auch  $SO(\mathbb{R}^2) := D$  für die sogenannte **spezielle orthogonale Gruppe** der Euklidischen Ebene. (Wir sagen aber nach wie vor einfach "Drehgruppe".)

Der Beweis ist nochmal ein bisschen rechenlastiger als der zur Drehgruppe. Daher starten wir mit einem kleinen Lemma, das Rechenregeln für Drehungen und Spiegelungen beschreibt.

### Lemma 1.38 (Rechenregeln für Drehungen und Spiegelungen)

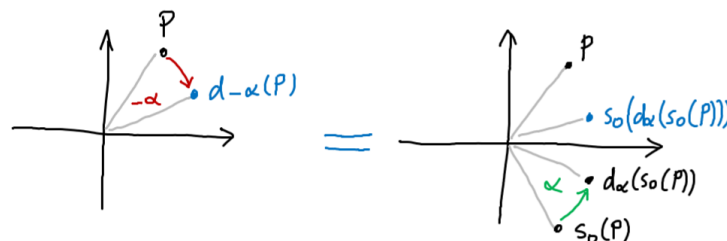
Sei  $\alpha \in \mathbb{R}$  ein orientierter Winkel. Dann gilt:

- ①  $d_{-\alpha} = s_0 \circ d_\alpha \circ s_0$
- ②  $s_\alpha = d_\alpha \circ s_0 \circ d_{-\alpha}$
- ③  $s_\alpha = d_{2\alpha} \circ s_0$

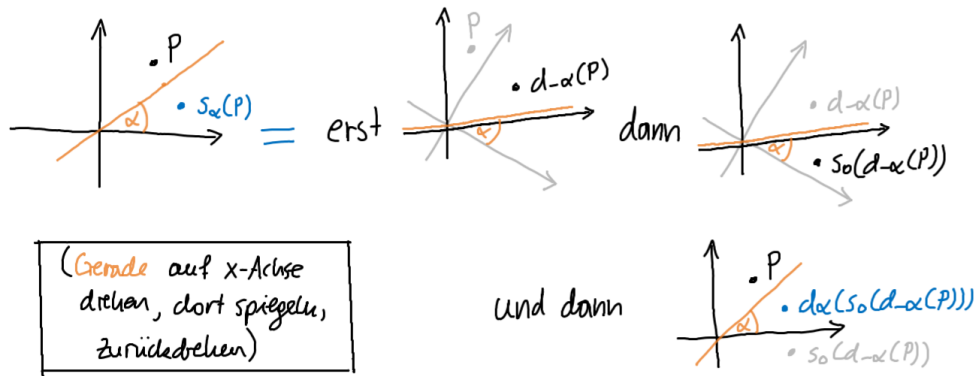
(Dabei ist  $s_0$  die Spiegelung an der  $x$ -Achse.)

*Beweis.*

**Zu ①.** Das ist geometrisch klar. Hier ein Bild:



Zu ②. Das ist auch geometrisch klar. Hier noch ein Bild:



Zu ③. Wende erst ② und dann ① an. Benutze  $s_0 \circ s_0 = \text{id}_{\mathbb{R}^2}$  (zweimal Spiegeln tut nichts).

Genauer gilt  $s_\alpha \stackrel{(2)}{=} d_\alpha \circ s_0 \circ d_{-\alpha} \stackrel{(1)}{=} d_\alpha \circ s_0 \circ s_0 \circ d_\alpha \circ s_0 = d_\alpha \circ d_\alpha \circ s_0 = d_{2\alpha} \circ s_0$ . ♥

Mit diesen Rechenregeln gerüstet können wir zum Beweis des eigentlichen Satzes voranschreiten.

*Beweis (von Satz 1.37).*

- Wir müssen prüfen, dass  $\circ$  wirklich eine Verknüpfung auf  $O(\mathbb{R}^2)$  ist, die Hintereinanderausführung zweier Drehungen und/oder Spiegelungen also wieder eine Drehung oder Spiegelung ist.

Wir unterscheiden vier Fälle.

- **Fall 1:** Es wird zweimal gedreht.

Dass  $d_\beta \circ d_\alpha = d_{\alpha+\beta}$  wieder eine Drehung ist, wissen wir aber schon.

- **Fall 2:** Erst wird gedreht, dann gespiegelt:

$$\begin{aligned}
 s_\beta \circ d_\alpha &= d_{2\beta} \circ s_0 \circ d_\alpha && (\text{Rechenregel } ③) \\
 &= d_{2\beta} \circ s_0 \circ s_0 \circ d_{-\alpha} \circ s_0 && (\text{Rechenregel } ① \text{ auf } d_\alpha \text{ angewendet}) \\
 &= d_{2\beta} \circ d_{-\alpha} \circ s_0 \\
 &= d_{2\beta-\alpha} \circ s_0 \\
 &= s_{\beta-\frac{1}{2}\alpha} && (\text{Rechenregel } ③ \text{ rückwärts})
 \end{aligned}$$

Dies ist also in Wahrheit eine Spiegelung.

- **Fall 3:** Erst wird gespiegelt, dann gedreht:

$$\begin{aligned}
 d_\beta \circ s_\alpha &= d_\beta \circ d_{2\alpha} \circ s_0 && (\text{Rechenregel } ③) \\
 &= d_{\beta+2\alpha} \circ s_0 \\
 &= s_{\frac{1}{2}\beta+\alpha} && (\text{Rechenregel } ③ \text{ rückwärts})
 \end{aligned}$$

Dies ist also ebenfalls eine Spiegelung.



– **Fall 4:** Es wird zweimal gespiegelt:

$$\begin{aligned} s_\beta \circ s_\alpha &= d_{2\beta} \circ s_0 \circ d_{2\alpha} \circ s_0 && (\text{zweimal Rechenregel } \textcircled{3}) \\ &= d_{2\beta} \circ d_{-2\alpha} && (\text{Rechenregel } \textcircled{1}) \\ &= d_{2(\beta-\alpha)} \end{aligned}$$

Dies ist also eine Drehung.

Insgesamt ist  $\circ$  also wirklich eine Verknüpfung auf  $O(\mathbb{R}^2)$ .

- *Existenz des neutralen Elements.*

Das neutrale Element ist nach wie vor  $\text{id}_{\mathbb{R}^2} = d_0 \in D \subset O(\mathbb{R}^2)$ .

- *Existenz der inversen Elemente.*

Die inversen Elemente sind  $(d_\alpha)^{-1} = d_{-\alpha} \in D \subset O(\mathbb{R}^2)$  sowie  $(s_\alpha)^{-1} = s_\alpha \in S \subset O(\mathbb{R}^2)$ .

Alles zusammen zeigt, dass  $O(\mathbb{R}^2)$  wirklich eine Gruppe ist. Sie ist offensichtlich **nicht** kommutativ, denn  $d_\beta \circ s_\alpha \neq s_\alpha \circ d_\beta$ , oder auch  $s_\beta \circ s_\alpha \neq s_\alpha \circ s_\beta$ . ♥

## Gruppen als Symmetrien

Abschließend wollen wir uns noch anschauen, wie Symmetrien von Formen in der Euklidischen Ebenen durch Gruppen beschrieben werden können.

### Definition 1.39 (*Dieder-Gruppen und zyklische Gruppen*)

Für  $n \in \mathbb{N} = \{1, 2, 3, \dots\}$  definiere die zugehörige...

- ① ... **Dieder-Gruppe** (sprich “*Di-Eder*”)

$$\text{Di}(n) := \{d_{360k/n} \mid k \in \mathbb{Z}\} \cup \{s_{180k/n} \mid k \in \mathbb{Z}\} \subset O(\mathbb{R}^2),$$

- ② ... **zyklische Gruppe**  $C(n) := \text{Di}(n) \cap D = \{d_{360k/n} \mid k \in \mathbb{Z}\}$ .

Obwohl die Variable  $k$  in der Definition die ganzen Zahlen durchläuft, sind diese Mengen endlich. (Die Wahl  $k \in \mathbb{Z}$  in der Definition hat rein rechnerische Vorteile.)

### Bemerkung 1.40 (*Anzahl der Elemente der Dieder-Gruppen*)

Wegen der 360-Grad- bzw. 180-Grad-Periodizität der Abbildungen  $d_\alpha$  und  $s_\alpha$  im Index  $\alpha$  (siehe **Bemerkung 1.34**) gilt

- $|\text{Di}(n) \cap D| = |C(n)| = n$  (das heißt,  $\text{Di}(n)$  enthält  $n$  Drehungen),
- $|\text{Di}(n) \cap S| = n$  (das heißt,  $\text{Di}(n)$  enthält  $n$  Spiegelungen).

Insgesamt enthält  $\text{Di}(n)$  also  $2n$  Elemente.

Wir betrachten einige Beispiele für kleine  $n \in \mathbb{N}$ .

### Beispiel 1.41 (Beispiele kleiner Dieder-Gruppen)

Die ersten Dieder-Gruppen und zyklischen Gruppen sind

- ①  $\text{Di}(1) = \{d_0, s_0\}$  und  $\text{C}(1) = \{d_0\} = \{\text{id}_{\mathbb{R}^2}\}$  (die triviale Gruppe),
  - ②  $\text{Di}(2) = \{d_0, d_{180}, s_0, s_{90}\}$  und  $\text{C}(2) = \{d_0, d_{180}\}$ ,
  - ③  $\text{Di}(3) = \{d_0, d_{120}, d_{240}, s_0, s_{60}, s_{120}\}$  und  $\text{C}(3) = \{d_0, d_{120}, d_{240}\}$ ,
  - ④  $\text{Di}(4) = \{d_0, d_{90}, d_{180}, d_{270}, s_0, s_{45}, s_{90}, s_{135}\}$  und  $\text{C}(4) = \{d_0, d_{90}, d_{180}, d_{270}\}$ ,
- und so weiter.

Wir wollen uns noch kurz vergewissern, dass die Dieder-Gruppen und zyklischen Gruppen wirklich Gruppen sind.

### Satz 1.42 (Dieder-Gruppen und zyklische Gruppen sind Gruppen)

Für jedes  $n \in \mathbb{N}$  sind  $\text{Di}(n)$  und  $\text{C}(n)$  wirklich Gruppen.

*Beweis.* Wir führen den Beweis für  $\text{Di}(n)$ . Der Beweis für  $\text{C}(n)$  ist darin auch enthalten.

- Die Hintereinanderausführung ist wirklich eine Verknüpfung auf  $\text{Di}(n)$ .

Wir benutzen die Formeln aus dem Beweis des vorigen Satzes.

- **Fall 1:**  $d_{360\ell/n} \circ d_{360k/n} = d_{360(\ell+n)/n} = d_{360(\ell+k)/n} \in \text{Di}(n)$
- **Fall 2:**  $s_{180\ell/n} \circ d_{360k/n} = s_{180\ell/n-180k/n} = s_{180(\ell-k)/n} \in \text{Di}(n)$
- **Fall 3:**  $d_{360\ell/n} \circ s_{180k/n} = s_{180\ell/n+180k/n} = s_{180(\ell+k)/n} \in \text{Di}(n)$
- **Fall 4:**  $s_{180\ell/n} \circ s_{180k/n} = d_{2 \cdot (180\ell/n-180k/n)} = d_{360(\ell-k)/n} \in \text{Di}(n)$

- Existenz des neutralen Elements.

Es gilt  $\text{id}_{\mathbb{R}^2} = d_0 = d_{360 \cdot 0/n} \in \text{Di}(n)$ .

- Existenz der inversen Elemente.

Es gilt  $(d_{360k/n})^{-1} = d_{360(-k)/n} \in \text{Di}(n)$  sowie  $(s_{180k/n})^{-1} = s_{180k/n} \in \text{Di}(n)$ .

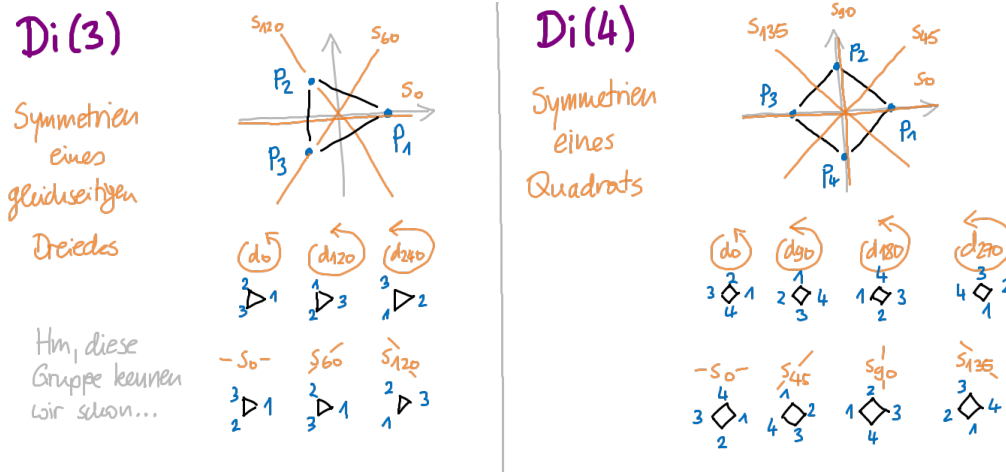
Folglich ist  $\text{Di}(n)$  wirklich für alle  $n \in \mathbb{N}$  eine Gruppe. ♥

Wie sich herausstellt, beschreiben die Dieder-Gruppen genau das, was wir unter **Symmetrien** gewisser geometrischen Formen in der Euklidischen Ebene verstehen. (Genauer sei eine *Symmetrie* einer geometrischen Form eine Isometrie, die diese Form wieder in sich selbst überführt.)

### Bemerkung 1.43 (Symmetrien regelmäßiger Polygone)

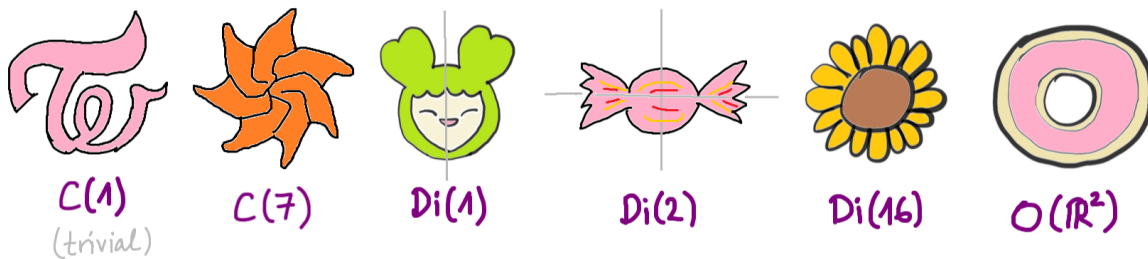
Sei  $n \geq 3$ . Dann beschreibt  $\text{Di}(n)$  genau die Symmetrien eines regelmäßigen  $n$ -Ecks in der Euklidischen Ebene.

Dies soll durch die folgende Abbildung veranschaulicht werden.



(In diesem Bild sei  $P_i := d_{360(i-1)/n}(1, 0)$  für  $i \in \{1, \dots, n\}$  und  $n = 3$  bzw.  $n = 4$ .)

Man kann natürlich auch Symmetrien von Formen betrachten, bei denen es sich nicht unbedingt um regelmäßige Polygone handelt. Diese beschränken sich dann allerdings nicht nur auf Dieder-Gruppen, wie die folgende Abbildung illustriert.



Wir können zum Beispiel Folgendes beobachten:

- Die Symmetrien einer geometrischen Form, deren einzige Symmetrie "Nichtstun" ist, werden durch die triviale Gruppe beschrieben — hier implementiert durch  $C(1)$ .
- Die Symmetrien eines Kreises sind genau die orthogonale Gruppe der Euklidischen Ebene.
- Ein Windrad besitzt keine Spiegelsymmetrien. Die Gruppe der Symmetrien ist zyklisch.

Wir können Gruppen also nun auch als Symmetrien verstehen. Damit schließen wir den ersten Abschnitt der zahlreichen Beispiele.

## §2 — Untergruppen und der Satz von Lagrange

Im vergangenen Abschnitt haben wir schon gesehen, dass Teilmengen einer Gruppe auch selbst die Struktur dieser Gruppe tragen können (oder auch nicht). Zum Beispiel ist die Drehgruppe  $D$  eine Gruppe innerhalb der orthogonalen Gruppe  $O(\mathbb{R}^2)$  (die Spiegelungen  $S$  aber nicht, weil sie keine Gruppe bilden, da es zum Beispiel kein neutrales Element gibt).

Diese Idee wollen wir in diesem Abschnitt verallgemeinern. Darüber hinaus wollen wir den sogenannten **Satz von Lagrange** formulieren und beweisen, der eine interessante Verbindung zwischen abstrakter Algebra und Zahlentheorie beschreibt.

Sei im Folgenden  $(G, \circ)$  eine Gruppe und  $H \subset G$  eine nichtleere Teilmenge. Dann erhalten wir eine Abbildung  $\circ : H \times H \rightarrow G$  (eventuell wird nicht innerhalb von  $H$  verknüpft).

### Definition 2.1 (Untergruppe)

Eine nichtleere Teilmenge  $H \subset G$  heißt eine **Untergruppe** von  $(G, \circ)$ , falls  $(H, \circ)$  selbst wieder eine Gruppe ist. Wir schreiben in diesem Fall auch  $H \leq G$ .

Dies ist genau dann der Fall, wenn die folgenden Bedingungen erfüllt sind:

- ① Für alle  $a, b \in H$  gilt  $a \circ b \in H$ . Das heißt,  $\circ$  definiert eine Verknüpfung auf  $H$ .
- ② Für das neutrale Element  $e \in G$  gilt  $e \in H$ .
- ③ Für alle  $a \in H$  gilt  $a^{-1} \in H$ .

Tatsächlich ist uns dieses Konzept nicht neu, denn wir haben in den vergangenen Stunden ab und zu gezeigt, dass Teilmengen die Gruppenstruktur einer größeren Menge erben.

### Beispiel 2.2 (Beispiele für Untergruppen)

- ① Die geraden Zahlen sind eine Untergruppe der ganzen Zahlen (mit der Addition).  
Die ungeraden Zahlen nicht, denn die Summe zweier ungerader Zahlen ist immer gerade.
- ②  $\mathbb{Z} \leq \mathbb{Q} \leq \mathbb{R}$  mit  $\circ = +$   
Allerdings ist  $\mathbb{N}$  keine Untergruppe, denn  $0 \notin \mathbb{N}$ , und es gibt auch keine Inversen.  
Auch  $(\mathbb{R} \setminus \mathbb{Q}) \cup \{0\}$  ist keine Untergruppe, denn zum Beispiel ist  $\pi + (2 - \pi) = 2 \in \mathbb{Q}$ .
- ③  $\mathbb{Q} \setminus \{0\} \leq \mathbb{R} \setminus \{0\}$  mit  $\circ = \cdot$
- ④  $C(n) \leq D = SO(\mathbb{R}^2) \leq O(\mathbb{R}^2) \leq \text{Sym}(\mathbb{R}^2)$ , aber  $S \subset O(\mathbb{R}^2)$  ist keine Untergruppe.
- ⑤ Auch  $C(n) \leq \text{Di}(n) \leq O(\mathbb{R}^2) \leq \text{Sym}(\mathbb{R}^2)$ .
- ⑥ Für  $a, b \in \mathbb{R}$  definiere die Abbildung  $f_{a,b} : \mathbb{R} \rightarrow \mathbb{R}$  durch  $f_{a,b}(x) := ax + b$ . Dann gilt  $f_{a,b} \in \text{Sym}(\mathbb{R})$ , wann immer  $a \neq 0$ . (Was ist die Umkehrabbildung?)  
Sei nun  $L := \{f_{a,b} \mid a \neq 0 \text{ und } b \in \mathbb{R}\}$  (dies ist die Menge der nicht-konstanten linearen Abbildungen). Dann kann man leicht nachrechnen, dass  $L \leq \text{Sym}(\mathbb{R})$  gilt. (Warum?)

Die drei Eigenschaften in **Definition 2.1** lassen sich auch bequem zu einer einzigen äquivalenten Bedingung zusammenfassen, dem sogenannten **Untergruppenkriterium**.

### Satz 2.3 (Untergruppenkriterium)

Die folgenden Aussagen sind äquivalent:

- ①  $H \leq G$
- ② Für alle  $a, b \in H$  gilt  $a \circ b^{-1} \in H$ .

*Beweis.*

“ $\implies$ ”: Seien  $a, b \in H$ . Wegen Definition 2.1 ③ ist  $b^{-1} \in H$ . Wegen Definition 2.1 ① ist dann auch  $a \circ b^{-1} \in H$ .

“ $\impliedby$ ”: Seien  $a, b \in H$ .

Betrachte zuerst das Paar  $(a, a)$ . Dann ist  $e = a \circ a^{-1} \in H$  (Definition 2.1 ②).

Betrachte danach das Paar  $(e, a)$ . Dann ist  $a^{-1} = e \circ a^{-1} \in H$  (Definition 2.1 ③).

Betrachte zuletzt das Paar  $(a, b^{-1})$ . Dann ist  $a \circ b = a \circ (b^{-1})^{-1} \in H$  (Definition 2.1 ①). ♥

Vorbereitend für den weiteren Verlauf des Kurses möchten wir die Untergruppen der ganzen Zahlen (mit der Addition) betrachten.

### Satz 2.4 (Untergruppen der ganzen Zahlen)

Für  $m \in \mathbb{Z}$  definiere die Menge

$$m\mathbb{Z} := \{mk \mid k \in \mathbb{Z}\} = \{\dots, -3m, -2m, -m, 0, m, 2m, 3m, \dots\}.$$

Dies ist für jedes  $m \in \mathbb{Z}$  eine Untergruppe von  $(\mathbb{Z}, +)$ .

Konkret bedeutet das

- $0\mathbb{Z} = \{0\}$ ,
- $1\mathbb{Z} = \mathbb{Z} = -1\mathbb{Z}$ ,
- $2\mathbb{Z} = \{\dots, -6, -4, -2, 0, 2, 4, 6, \dots\} = -2\mathbb{Z}$  (die geraden Zahlen),
- $3\mathbb{Z} = \{\dots, -9, -6, -3, 0, 3, 6, 9, \dots\} = -3\mathbb{Z}$  (die durch drei teilbaren Zahlen),

und so weiter.

Wir rechnen leicht nach, dass  $m\mathbb{Z}$  für jedes  $m \in \mathbb{Z}$  eine Untergruppe von  $(\mathbb{Z}, +)$  ist.

*Beweis.* Seien  $a, b \in m\mathbb{Z}$ . Dann gibt es  $k, \ell \in \mathbb{Z}$  mit  $a = mk$  und  $b = m\ell$ .

Dann gilt  $a + (-b) = mk - m\ell = m(k - \ell) \in m\mathbb{Z}$ .

Nach dem Untergruppenkriterium bedeutet das  $m\mathbb{Z} \leq \mathbb{Z}$ . ♥

Viel spannender ist jedoch der folgende Fakt: Das sind bereits alle möglichen Untergruppen von  $\mathbb{Z}$ , was wir auch sogleich beweisen werden.

### Satz 2.5 (Charakterisierung der Untergruppen der ganzen Zahlen)

Sei  $H \leq \mathbb{Z}$ . Dann ist  $H = m\mathbb{Z}$  für ein  $m \in \mathbb{N}_0$ .

Die wesentliche Idee des Beweises besteht darin, dass wir für  $m \neq 0$  jedes  $h \in \mathbb{Z}$  schreiben können als  $h = mq + r$  mit eindeutig bestimmten Zahlen  $q \in \mathbb{Z}$  und  $0 \leq r \leq m-1$ , also **Division mit Rest** durchführen.

Zum Beispiel gilt für  $h = 17$  und  $m = 5$ , dass  $q = 3$  und  $r = 2 \in \{0, 1, 2, 3, 4\}$ , also  $17 = 5 \cdot 3 + 2$ , und diese Schreibweise ist eindeutig.

*Beweis.* Sei  $H \leq \mathbb{Z}$ . Falls  $H = \{0\}$  ist, sind wir sofort fertig mit  $m = 0$ .

Sei also  $H \neq \{0\}$ . Dann enthält  $H$  eine von null verschiedene Zahl. Wegen  $-h \in H \implies h \in H$  (Definition 2.1 (3)) enthält  $H$  sogar eine positive Zahl.

Bezeichne mit  $m$  die **kleinste** positive Zahl in  $H$ . Wir möchten zeigen, dass  $H = m\mathbb{Z}$  gilt.

“ $m\mathbb{Z} \subset H$ ”: Das folgt aus  $m \in H$  und den Untergruppen-Eigenschaften aus Definition 2.1. (Denn  $2m = m + m \in H$ , dann auch  $-2m \in H$ , ... Allgemein folgt  $mk \in H$  für alle  $k \in \mathbb{Z}$ .)

“ $H \subset m\mathbb{Z}$ ”: Sei  $h \in H$ . Schreibe  $h = mq + r$  für gewisse  $q \in \mathbb{Z}$  und  $r \in \{0, 1, \dots, m-1\}$ .

Wegen  $h \in H$  und  $m \in H$  folgt aus den Untergruppen-Eigenschaften auch  $r = h - mq \in H$ .

Der Rest  $r \in H$  erfüllt  $0 \leq r \leq m-1$ , aber gleichzeitig war  $m \in H$  die **kleinste** positive Zahl. Dann muss also in Wahrheit  $r = 0$  sein!

Das wiederum bedeutet  $h = mq$ , also  $h \in m\mathbb{Z}$ .

◇ — ◇ — ◇

Insgesamt haben wir also  $H = \{0\} = 0\mathbb{Z}$  oder aber  $H = m\mathbb{Z}$  gezeigt, wobei  $m \neq 0$  die kleinste positive Zahl in  $H$  ist. ♥

Bemerkenswert ist, dass dieser Satz die Untergruppen der ganzen Zahlen komplett charakterisiert (jede Untergruppe ist von der Form  $m\mathbb{Z}$ ). Im Allgemeinen ist es **nicht** möglich zu sagen, wie die Untergruppen einer beliebigen Gruppe aussehen.

Für den Fall, dass eine Gruppe  $G$  **endlich** viele Elemente hat (also  $|G| = n$  für ein  $n \in \mathbb{N}$  gilt), liefert der **Satz von Lagrange** aber eine interessante Aussage über die Anzahl der Elemente einer Untergruppe  $H \leq G$ .

### Satz 2.6 (Satz von Lagrange)

Sei  $G$  eine Gruppe mit **endlich** vielen Elementen, und sei  $H \leq G$ .

Dann ist  $|H|$  ein Teiler von  $|G|$ .

Diese Aussage wirkt auf den ersten Blick möglicherweise etwas unspektakulär. Bei genauerem Hinsehen ist sie allerdings doch sehr interessant, denn sie verbindet abstrakte Algebra ( $H \leq G$  gemäß der abstrakten Definition 2.1) mit ganz konkreter Zahlentheorie (Teilbarkeit).

Wir können den Satz von Lagrange noch nicht beweisen, wollen dies aber zeitnah tun. Dazu benötigen wir etwas Vokabular.

### Definition 2.7 (*Relation*)

Eine **Relation** zwischen zwei Mengen  $X$  und  $Y$  ordnet jedem Paar  $(x, y) \in X \times Y$  einen Wahrheitswert zu (also “wahr” oder “falsch”).

Man sagt bei “wahr”, dass  $x$  mit  $y$  **in Relation steht** (bzw. bei “falsch”, dass  $x$  dies nicht tut).  
Im Falle identischer Mengen  $X = Y$  spricht man von einer Relation auf  $X$ .

Wie immer schauen wir uns zunächst ein paar Beispiele an.

### Beispiel 2.8 (*Beispiele für Relationen*)

- ① Sei  $X := Y := \{1, 2, 3\}$ . Dann ist “ $<$ ” eine Relation auf  $X$ . Die Wahrheitswerte für alle Paare in  $X \times X$  sind unten tabelliert.

$(1, 1) \mapsto$	falsch	$(1, 2) \mapsto$	wahr	$(1, 3) \mapsto$	wahr
$(2, 1) \mapsto$	falsch	$(2, 2) \mapsto$	falsch	$(2, 3) \mapsto$	wahr
$(3, 1) \mapsto$	falsch	$(3, 2) \mapsto$	falsch	$(3, 3) \mapsto$	falsch

- ② Sei  $X := Y :=$  die Menge aller Menschen. Dann ist “ $(x, y) \mapsto x$  und  $y$  sind Geschwister” eine Relation auf  $X$ .

- ③ **Funktionen sind (besondere) Relationen!**

Seien  $X$  und  $Y$  irgendwelche Mengen (im Allgemeinen natürlich  $X \neq Y$ ).

Eine Relation zwischen  $X$  und  $Y$  heißt eine **Funktion**  $X \rightarrow Y$ , falls gilt:

Jedes  $x \in X$  steht mit genau einem  $y \in Y$  in Relation.

In diesem Falle ist für jedes  $x \in X$  die Schreibweise

$f(x) :=$  dasjenige  $y \in Y$ , das mit  $x \in X$  in Relation steht

sinnvoll definiert, und man schreibt  $f : X \rightarrow Y$  mit  $x \mapsto f(x)$ .

Man nennt diese Eigenschaften einer Relation auch **linkstotal** (jedes  $x \in X$ ) bzw. **rechts-eindeutig** (genau ein  $y \in Y$ ).

Dies widerspricht nicht dem Konzept einer Funktion, das man schon aus der Schule kennt (es wird nichts anderes definiert). Mathematiker bevorzugen diese Definition jedoch, weil sie auch dann korrekt ist, wenn man  $f(x) = \dots$  nicht als Formel hinschreiben kann.

Wir betrachten im Folgenden günstige Eigenschaften, die eine Relation haben kann.

### Definition 2.9 (*Äquivalenzrelation*)

Eine Relation  $\sim$  auf  $X$  heißt...

- ① ... **reflexiv**, falls  $x \sim x$  für alle  $x \in X$  gilt.  
② ... **symmetrisch**, falls für alle  $x, y \in X$  aus  $x \sim y$  auch  $y \sim x$  folgt.

⋮

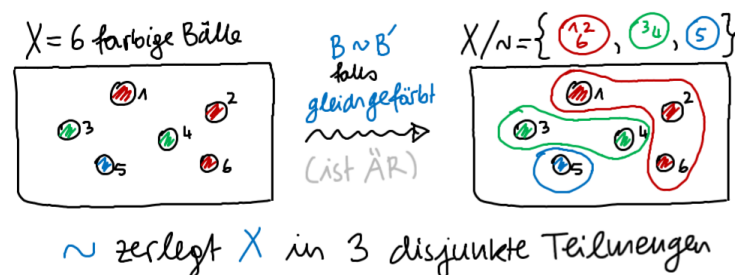
- ③ ... **transitiv**, falls für alle  $x, y, z \in X$  aus  $x \sim y$  und  $y \sim z$  auch  $x \sim z$  folgt.
- ④ ... eine **Äquivalenzrelation**, falls sie reflexiv, symmetrisch, und transitiv ist.

Bei den Beispielen aus **Beispiel 2.8** handelt es sich jeweils **nicht** um eine Äquivalenzrelation, wie wir unten sehen.

### Beispiel 2.10 (Nicht-Beispiele für Äquivalenzrelationen)

- ① Sei  $X := \{1, 2, 3\}$  und  $\sim$  die “<”-Relation. Diese ist...
  - ... **nicht** reflexiv, denn zum Beispiel ist  $1 \not< 1$ ;
  - ... **nicht** symmetrisch, denn zum Beispiel ist  $1 < 2$ , aber  $2 \not< 1$ ;
  - ... sehr wohl transitiv, denn für alle  $x, y, z \in \mathbb{R}$  folgt (ganz allgemein) aus  $x < y$  und  $y < z$  auch  $x < z$ .
- ② Sei  $X$  die Menge aller Menschen und  $\sim$  die Geschwister-Relation. Diese ist...
  - ... **nicht** reflexiv, da man (per Definition) niemals sein eigener Bruder bzw. seine eigene Schwester ist;
  - ... symmetrisch;
  - ... transitiv.

Die besondere Eigenschaft von Äquivalenzrelationen ist, dass sie die Grundmenge in die Teilmengen der jeweils äquivalenten Elemente **überschneidungsfrei** zerlegen, wie das folgende Bild veranschaulichen soll.



Dies wollen wir formalisieren. Sei im Folgenden immer  $\sim$  eine **Äquivalenzrelation** auf  $X$ .

### Definition 2.11 (Äquivalenzklasse und Quotientenmenge)

- ① Die zu  $x \in X$  gehörige **Äquivalenzklasse** ist die Menge aller zu  $x$  äquivalenten Elemente,

$$[x] := \{y \in X \mid x \sim y\} \subset X.$$

- ② Die **Quotientenmenge** von  $\sim$  ist die Menge aller Äquivalenzklassen,

$$X/\sim := \{[x] \mid x \in X\}.$$

Dies ist also eine Menge von Teilmengen von  $X$ .



Die Quotientenmenge  $X/\sim$  stellt dabei eine überschneidungsfreie Zerlegung der Grundmenge  $X$  in die Äquivalenzklassen bezüglich  $\sim$  dar. Genauer gilt, dass je zwei Äquivalenzklassen gemäß dem folgenden Satz entweder **disjunkt** oder **identisch** sind. (Und natürlich enthält jedes  $[x]$  mindestens ein Element, nämlich  $x$ , denn  $\sim$  ist reflexiv.)

**Satz 2.12** (*Äquivalenzklassen sind entweder disjunkt oder identisch*)

Für alle  $x, y \in X$  gilt: Entweder ist  $[x] \cap [y]$  leer, oder aber  $[x] = [y]$ .

Betrachte dazu das folgende Lemma.

**Lemma 2.13**

Wenn  $y \in [x]$ , dann  $[x] = [y]$ .

*Beweis.* Die Voraussetzung  $y \in [x]$  ist gleichbedeutend mit  $x \sim y$ .

Sei nun  $z \in [x]$  beliebig. Dies bedeutet  $z \sim x$ . Wegen  $x \sim y$  ist dies gleichbedeutend mit  $z \sim y$ , also äquivalent zu  $z \in [y]$ . Daraus folgt  $[x] = [y]$ . ♥

Nun zum Beweis des vorigen Satzes:

*Beweis (von Satz 2.12).* Sei  $[x] \cap [y]$  nichtleer. Dann gibt es ein  $z \in [x] \cap [y]$ . Das heißt  $z \in [x]$  sowie  $z \in [y]$ . Also  $[x] = [z] = [y]$  nach Lemma 2.13. ♥

Den Nicht-Beispielen aus Beispiel 2.10 gegenüberstellen wollen wir jetzt Beispiele, in denen die Relation wirklich eine Äquivalenzrelation ist. Insbesondere interessiert uns jeweils, wie die Äquivalenzklassen aussehen.

**Beispiel 2.14** (*Beispiele für Äquivalenzrelationen*)

- ① Sei  $X := \mathbb{R}$  und  $\sim$  die Gleichheit zweier Zahlen (dies ist offensichtlich eine Äquivalenzrelation, und zwar eine sehr langweilige).

Die Äquivalenzklassen sind dann die einelementigen Mengen  $[x] = \{x\}$ .

Die Quotientenmenge ist  $\mathbb{R}/\sim = \{\{x\} \mid x \in \mathbb{R}\}$ . (Dies ist im Wesentlichen  $\mathbb{R}$  selbst, denn die zugrunde liegende Äquivalenzrelation tut nichts Nichttriviales.)

- ② Sei  $X$  die Menge aller Schüler\*innen des Hertz-Gymnasiums und  $x \sim y$  genau dann, wenn  $x$  und  $y$  in dieselbe Klasse gehen.

Die Äquivalenzklassen sind  $[x] = \text{Klasse, in die } x \text{ geht}$ .

Die Quotientenmenge ist  $X/\sim = \text{Menge aller Klassen}$ .

- ③ Sei  $X := \mathbb{Z} \times \mathbb{Z} \setminus \{0\}$ . Definiere  $(a, b) \sim (c, d)$  genau dann, wenn  $ad = bc$  gilt.

Innerhalb von  $\mathbb{R}$  kann man diese Gleichung umstellen zu  $\frac{a}{b} = \frac{c}{d}$ . Die Äquivalenzklasse  $[(a, b)]$  enthält also alle Paare  $(c, d)$ , sodass  $\frac{c}{d}$  in  $\mathbb{R}$  denselben Bruch darstellt wie  $\frac{a}{b}$ .

In Wahrheit haben wir auf diese Weise die rationalen Zahlen  $\mathbb{Q} := X/\sim$  mittels der ganzen Zahlen  $\mathbb{Z}$  **konstruiert**, denn die Äquivalenzklassen sind genau alle verschiedenen Darstellungen  $\frac{c}{d}$  (als Paar  $(c, d) \in X$  von Zähler und Nenner) des jeweiligen Bruchs  $\frac{a}{b}$ .

- ④ Sei  $X$  irgendeine Menge von Mengen. Wir definieren die Relation  $\overset{1:1}{\longleftrightarrow}$  durch  $A \overset{1:1}{\longleftrightarrow} B$  genau dann, wenn es eine **bijektive** (umkehrbare) Abbildung  $f : A \rightarrow B$  gibt.

Dies ist wirklich eine Äquivalenzrelation:

- Weil die Identität  $\text{id}_A : A \rightarrow A$  bijektiv ist, ist  $\overset{1:1}{\longleftrightarrow}$  reflexiv.
- Weil eine bijektive Abbildung  $f : A \rightarrow B$  eine (ebenfalls bijektive) Umkehrabbildung  $f^{-1} : B \rightarrow A$  besitzt, ist  $\overset{1:1}{\longleftrightarrow}$  symmetrisch.
- Wenn es bijektive Abbildungen  $f : A \rightarrow B$  und  $g : B \rightarrow C$  gibt, dann ist die Abbildung  $g \circ f : A \rightarrow C$  ebenfalls bijektiv (mit Umkehrabbildung  $f^{-1} \circ g^{-1}$ ). Also ist  $\overset{1:1}{\longleftrightarrow}$  auch transitiv.

Die Äquivalenzklassen fassen alle Mengen **gleicher Mächtigkeit** zusammen. Wir nennen sie **Kardinalzahlen**, geschrieben  $|A| := [A]$ .

In diesem Sinne, also mit  $|A|$  als Äquivalenzklasse, gilt:

- Jede endliche Menge mit  $n \in \mathbb{N}_0$  Elementen hat die Mächtigkeit  $| \{1, 2, \dots, n\} |$ .
- $|\mathbb{N}| = |\mathbb{Z}| = |m\mathbb{Z}| = |\mathbb{Z}^n| = |\mathbb{Q}|$  (sogenannte **abzählbar** unendliche Mengen)
- $|\mathbb{R}| = |[0, 1]| = |\mathbb{R} \setminus \mathbb{Q}| = |\mathbb{R}^n|$  (sogenannte **überabzählbar** unendliche Mengen)
- $|\mathbb{N}| \neq |\mathbb{R}|$  (die reellen Zahlen sind "größer" als die natürlichen Zahlen)

Damit sind wir gut ausgerüstet für den Beweis des Satzes von Lagrange.

### Lemma 2.15 (Induzierte Äquivalenzrelation einer Untergruppe)

Sei  $G$  eine Gruppe, und sei  $H \leq G$ .

Definiere  $a \sim b$  genau dann, wenn  $b = a \circ h$  für ein  $h \in H$  gilt.

Dann gilt: Dies ist eine Äquivalenzrelation auf  $G$ .

*Beweis.* Wir müssen Reflexivität, Symmetrie, und Transitivität zeigen.

- **Reflexivität.** Es ist  $a \sim a$ , denn  $a = a \circ e$ , und  $e \in H$  nach Definition 2.1 (2).
- **Symmetrie.** Gelte  $a \sim b$ , also  $b = a \circ h$  für ein  $h \in H$ . Daraus folgt  $a = b \circ h^{-1}$ , also  $b \sim a$ , denn  $h^{-1} \in H$  nach Definition 2.1 (3).
- **Transitivität.** Gelte  $a \sim b$  und  $b \sim c$ , also  $b = a \circ h$  und  $c = b \circ h'$  für gewisse  $h, h' \in H$ . Dann ist  $c = a \circ (h \circ h')$ , also  $a \sim c$ , denn  $h \circ h' \in H$  nach Definition 2.1 (1).

Also ist  $\sim$  wirklich eine Äquivalenzrelation. (Beachte, dass wir im Beweis jede Untergruppeneigenschaft einmal benutzt haben.) ♥

Die Äquivalenzklassen sind dann von der Form

$$[a] = \{b \in G \mid b = a \circ h \text{ für ein } h \in H\} = \{a \circ h \mid h \in H\} \subset G.$$

Wir schreiben dann einfach  $a \circ H$  für diese Menge.

### Definition 2.16 (*Linksnebenklasse*)

- ① Solch eine Äquivalenzklasse  $a \circ H \subset G$  heißt eine **Linksnebenklasse** von  $H$  (zu  $a \in G$ ).
- ② Wir bezeichnen die Quotientenmenge mit  $G/H$  (gesprochen “ $G$  modulo  $H$ ”).

Essentiell für den Beweis des Satzes von Lagrange ist die Erkenntnis, dass alle Linksnebenklassen gleichmächtig sind.

### Bemerkung 2.17 (*Gleichmächtigkeit der Linksnebenklassen*)

Jede Linksnebenklasse  $a \circ H$  steht in 1-zu-1-Relation mit  $H$ . (Denn  $h \mapsto a \circ h$  ist eine bijektive Abbildung  $H \rightarrow a \circ H$  mit der Umkehrabbildung  $g \mapsto a^{-1} \circ g$ .)

Insbesondere besitzen alle Linksnebenklassen die Mächtigkeit  $|H|$ .

Bevor wir den Satz von Lagrange beweisen, betrachten wir zunächst (wie immer) ein paar Beispiele.

### Beispiel 2.18 (*Beispiele für Linksnebenklassen*)

- ① Betrachte  $G := \mathbb{Z}$  und  $H := 3\mathbb{Z}$ .

Die Linksnebenklassen sind dann  $0 + 3\mathbb{Z}$ ,  $1 + 3\mathbb{Z}$ , und  $2 + 3\mathbb{Z}$ . Dies sind **alle** Klassen, denn  $3 + 3\mathbb{Z}$  ist wieder  $3\mathbb{Z}$ , und so fort.

Die Quotientenmenge ist also  $\mathbb{Z}/3\mathbb{Z} = \{0 + 3\mathbb{Z}, 1 + 3\mathbb{Z}, 2 + 3\mathbb{Z}\}$  (sie enthält drei Elemente).

Das funktioniert natürlich für jede Untergruppe  $m\mathbb{Z}$ . Die Quotientenmenge  $\mathbb{Z}/m\mathbb{Z}$  enthält dann genau  $m$  Elemente, und zwar eines für jeden möglichen Rest bei Division durch  $m$ . Deshalb nennen wir diese Klassen auch **Restklassen**. Im nächsten Abschnitt werden wir uns ausführlich mit ihnen beschäftigen.

- ② Betrachte  $G := \mathbb{R}$  und  $H := \mathbb{Z}$ .

Die Linksnebenklassen sind dann von der Form  $x + \mathbb{Z}$  mit  $x \in \mathbb{R}$ .

Wegen  $\mathbb{Z} = 1 + \mathbb{Z}$  gilt allgemein  $x + \mathbb{Z} = (x + 1) + \mathbb{Z}$  für alle  $x \in \mathbb{R}$ . Deshalb ist

$$\mathbb{R}/\mathbb{Z} = \{x + \mathbb{Z} \mid 0 \leq x < 1\}$$

bereits eine vollständige Beschreibung aller Linksnebenklassen.

Vorstellen kann man sich  $\mathbb{R}/\mathbb{Z}$  als **Kreis**. Jeder Punkt im halboffenen Intervall  $[0, 1)$  entspricht einer anderen Linksnebenklasse, und wegen  $0 \sim 1$  sind die Enden des Intervalls miteinander verbunden.


Mit einem guten Verständnis dieser Konstruktion können wir schlussendlich zum Beweis des Satzes von Lagrange voranschreiten.

*Beweis (von Satz 2.6).* Sei  $G$  eine Gruppe mit **endlich** vielen Elementen, und sei  $H \leq G$ . Dann besteht die Quotientenmenge  $G/H$  (bezüglich der Äquivalenzrelation aus Lemma 2.15) aus **endlich** vielen Linksnebenklassen  $a_1 \circ H$ ,  $a_2 \circ H$ , ...,  $a_r \circ H$ . Jede dieser  $r$  Klassen hat

⋮

Mächtigkeit  $|H|$  (siehe **Bemerkung 2.17**).

Weil  $G/H$  die Menge  $G$  überschneidungsfrei zerlegt, folgt  $|G| = r|H|$ .

Also ist  $|H|$  ein Teiler von  $|G|$ . 


Wir haben es geschafft! Das ist ein wichtiger Meilenstein.

Der Satz von Lagrange zieht sofort eine interessante Konsequenz nach sich, wenn die Anzahl der Elemente einer Gruppe prim ist.

### **Korollar 2.19** (*Untergruppen von Gruppen primer Mächtigkeit*)

Sei  $G$  eine Gruppe mit  $|G| = p$  für eine **Primzahl**  $p$ , und sei  $H \leq G$ .

Dann ist entweder  $H = \{e\}$  oder  $H = G$ . (Es gibt also keine nicht-trivialen Untergruppen.)

*Beweis.* Nach Satz von Lagrange ist  $|H|$  ein Teiler von  $|G| = p$ , also entweder  $|H| = 1$  oder aber  $|H| = p$ . Daraus folgt  $H = \{e\}$  bzw.  $H = G$ . 

Wir nähern uns nun dem Ende des zweiten Abschnitts und betrachten Potenzen von Gruppenelementen (ganz analog zu den Potenzen reeller Zahlen).

### **Definition 2.20** (*Potenzen*)

Sei  $G$  eine Gruppe, sei  $g \in G$ , und sei  $n \in \mathbb{N}$ . Wir definieren

①  $g^0 := e$ ,

②  $g^n := g \circ g \circ \dots \circ g$  ( $n$  mal),

③  $g^{-n} := (g^{-1})^n$ .

Insgesamt ist dadurch also  $g^k$  für alle  $k \in \mathbb{Z}$  definiert.


Wir kennen das bereits von der Multiplikation auf  $\mathbb{R} \setminus \{0\}$  (also  $x^0 = 1$  und  $x^{-n} = \frac{1}{x^n}$ ). Tatsächlich sind diese Definitionen aus einem bestimmten Grund so gewählt. Tut man das nämlich auf diese Weise, so erhält man eine ganz praktische Rechenregel.

### **Satz 2.21** (*Potenzgesetz*)

Sei  $G$  eine Gruppe. Dann gilt das **Potenzgesetz**

$$g^k \circ g^\ell = g^{k+\ell}$$

für alle  $g \in G$  und  $k, \ell \in \mathbb{Z}$ .

*Beweis.* Zähle den Faktor “ $g$ ” (es ist eine Fallunterscheidung notwendig). 

Zuletzt möchten wir uns noch mit einer weiteren Eigenschaft befassen, die Gruppen besitzen können.

### Definition 2.22 (Erzeugte Untergruppe)

Sei  $G$  eine Gruppe, und sei  $g \in G$ . Die Menge

$$\langle g \rangle := \{g^k \mid k \in \mathbb{Z}\} \subset G$$

heißt die von  $g$  **erzeugte Untergruppe** von  $G$ .

Der Name ist gerechtfertigt, denn dass es sich bei  $\langle g \rangle$  wirklich um eine Untergruppe handelt, folgt sofort aus dem Potenzgesetz ([Satz 2.20](#)) zusammen mit dem Untergruppenkriterium ([Satz 2.3](#)).

*Beweis.* Seien  $a, b \in \langle g \rangle$ .

Dann gilt  $a = g^k$  und  $b = g^\ell$  für gewisse  $k, \ell \in \mathbb{Z}$ .

Daraus folgt  $a \circ b^{-1} = g^k \circ (g^\ell)^{-1} = g^{k-\ell} \in \mathbb{Z}$  wie gewünscht. ♥

Wird eine Gruppe auf diese Art und Weise erzeugt, spricht man von einer **zyklischen** Gruppe.

### Definition 2.23 (Zyklische Gruppe)

Eine Gruppe  $G$  heißt **zyklisch**, falls  $G = \langle g \rangle$  für ein  $g \in G$  gilt.

In diesem Falle heißt  $g$  ein **Erzeuger** von  $G$ . (Eventuell ist  $g$  aber nicht eindeutig bestimmt!)

Wir untersuchen unsere üblichen Verdächtigen auf Zyklizität.

### Beispiel 2.24 (Beispiele für zyklische Gruppen)

- ① Die ganzen Zahlen sind zyklisch, denn es gilt  $\mathbb{Z} = \langle 1 \rangle = \langle -1 \rangle$ .

Es gibt keine weiteren Erzeuger als  $\pm 1$ , denn für jedes andere  $m \in \mathbb{Z}$  ist zum Beispiel  $1 \notin \langle m \rangle$ , also  $\langle m \rangle \neq \mathbb{Z}$ .

- ② Die rationalen Zahlen sind nicht zyklisch.

Gäbe es ein  $\frac{a}{b} \in \mathbb{Q}$  mit  $\mathbb{Q} = \langle \frac{a}{b} \rangle$ , dann wäre zum Beispiel  $\frac{a}{2b} \notin \langle \frac{a}{b} \rangle = \mathbb{Q}$ . (Widerspruch!)

- ③ Die zyklischen Gruppen  $C(n)$  (siehe [Definition 1.39](#) ②) sind zyklische Gruppen.

In der Tat ist  $C(n) = \{d_{360 \cdot k/n} \mid k \in \mathbb{Z}\} = \langle d_{360/n} \rangle$ .

Endliche zyklische Gruppen sehen “gleich” aus, wie wir an späterer Stelle noch zeigen werden.

### Satz 2.25 (Form endlicher zyklischer Gruppen)

Sei  $G$  eine **endliche** zyklische Gruppe mit Erzeuger  $g \in G$  und  $|G| = n$ .

Dann ist  $G = \{e, g, g^2, \dots, g^{n-1}\}$ , diese Elemente sind alle verschieden, und es gilt  $g^n = e$ .

*Beweis.* Später. ♥

Nicht sofort offensichtlich scheint noch der folgende Satz über Gruppen primer Mächtigkeit, obwohl er sofort mit den uns zur Verfügung stehenden Mitteln zu beweisen ist.

**Satz 2.26** (*Gruppen primer Mächtigkeit sind zyklisch*)

Sei  $G$  eine Gruppe mit  $|G| = p$  für eine **Primzahl**  $p$ .

Dann ist  $G$  zyklisch, und jedes  $g \neq e$  ist ein Erzeuger von  $G$ .

*Beweis.* Betrachte irgendein  $g \neq e$ . Dann ist  $\langle g \rangle \neq \{e\}$  (denn  $\langle g \rangle$  enthält zumindest die zweielementige Menge  $\{e, g\}$ ).

Gemäß dem **Korollar 2.19** aus dem Satz von Lagrange muss also  $\langle g \rangle = G$  sein, denn  $\{e\}$  und  $G$  sind die einzigen beiden Untergruppen von  $G$ . ♥

Damit sind wir schon gut vorbereitet für den nächsten Abschnitt!

Wie bereits in **Beispiel 2.18** (1) getan betrachten wir die Quotientenmenge  $\mathbb{Z}/m\mathbb{Z}$  für ein  $m \in \mathbb{N}$ .

### Definition 3.1 (Restklasse)

- ① Schreibe abkürzend  $\mathbb{Z}_m := \mathbb{Z}/m\mathbb{Z} = \{0 + m\mathbb{Z}, 1 + m\mathbb{Z}, \dots, (m-1) + m\mathbb{Z}\}$ .
- ② Wir bezeichnen die Elemente  $r + m\mathbb{Z}$  der Quotientenmenge  $\mathbb{Z}_m$  als **Restklassen** und schreiben  $\bar{r} := r + m\mathbb{Z}$ , also  $\mathbb{Z}_m = \{\bar{0}, \bar{1}, \dots, \overline{m-1}\}$  (also auch  $\bar{0} = \overline{m}$  und so weiter).
- ③ Statt  $x \sim y$ , also  $\bar{x} = \bar{y} \in \mathbb{Z}_m$ , schreiben wir auch  $x = y \pmod{m}$ .

Beachte, dass es sich bei den Objekten  $\bar{r}$  nach wie vor um **Mengen** handelt (nämlich alle ganzen Zahlen, die bei Division durch  $m$  den Rest  $r$  haben).

Dennoch wollen wir die Elemente von  $\mathbb{Z}_m$  wie Zahlen behandeln und insbesondere eine Addition sowie eine Multiplikation einführen.

Dies erfolgt so, wie es intuitiv eigentlich klar ist, wenn man die analoge Uhr lesen kann (die mit den Zeigern, und Stunden 1 bis 12 — also Elementen von  $\mathbb{Z}_{12}$ ). Ist es zum Beispiel 11 Uhr und man wartet 5 Stunden, so ist es danach 16 = 4 Uhr. Berechnet wurde  $\overline{11} + \bar{5} = \overline{16} = \bar{4}$  (denn  $\overline{16}$  und  $\bar{4}$  sind in  $\mathbb{Z}_{12}$  dieselbe “Zahl”).

Dies führt zur folgenden Definition von Addition und Multiplikation von Restklassen.

### Definition 3.2 (Addition und Multiplikation von Restklassen)

Wir definieren auf  $\mathbb{Z}_m$  eine...

- ① ... **Addition** durch  $\bar{a} + \bar{b} := \overline{a + b}$ ,
- ② ... **Multiplikation** durch  $\bar{a} \cdot \bar{b} := \overline{a \cdot b}$ .

⚠ *Beachte, dass für jedes  $m \in \mathbb{N}$  ein anderes  $+$  und  $\cdot$  definiert wird, aber das Symbol immer dasselbe ist! (Und auch dasselbe wie für die Rechenoperationen auf den reellen Zahlen.)*

Wir müssen die Definition allerdings noch auf ihre Korrektheit überprüfen. Genauer müssen wir garantieren, dass die jeweils rechte Seite **unabhängig** von der konkreten Wahl von  $a$  und  $b$  ist.

Ganz konkret haben wir oben  $\overline{11} + \bar{5} = \bar{4}$  ausgerechnet. Es ist aber zum Beispiel auch  $\overline{11} = \overline{-1}$  und  $\bar{4} = \overline{30}$ . Addition dieser beiden Restklassen gemäß der obigen Definition liefert  $\overline{-1} + \overline{30} = \overline{29}$ , was in der Tat dasselbe ist wie  $\bar{5}$ .

Wir müssen zeigen, dass das immer so ist. Anders gesagt wäre es Unsinn, wenn bei  $\overline{a + b}$  für unterschiedliche **Repräsentanten** der Klassen  $\bar{a}$  und  $\bar{b}$  auch unterschiedliche Werte herauskämen. Die nachzuweisende Eigenschaft heißt deswegen **Repräsentantenunabhängigkeit**.

*Beweis.* Seien  $a, a', b, b' \in \mathbb{Z}$  mit  $\bar{a} = \bar{a'}$  und  $\bar{b} = \bar{b'}$  (modulo  $m$ ). Dann gibt es  $k, \ell \in \mathbb{Z}$  mit  $a' = a + mk$  und  $b' = b + m\ell$ .

- ① Dann wäre  $\bar{a'} + \bar{b'}$  definiert worden als  $\overline{a + mk + b + m\ell} = \overline{a + b + m(k + \ell)} = \overline{a + b}$ .
- ② Dann wäre  $\bar{a'} \cdot \bar{b'}$  definiert worden als  $\overline{(a + mk)(b + m\ell)} = \overline{ab + m(a\ell + bk + mk\ell)} = \overline{ab}$ .

Die Definitionen von Addition und Multiplikation sind folglich wirklich korrekt. ♥

Da wir nun wissen, dass es sich wirklich um Verknüpfungen auf  $\mathbb{Z}_m$  handelt, können wir diese auf ihre algebraischen Eigenschaften untersuchen.

### Satz 3.3 (Restklassen bilden additive Gruppe)

$(\mathbb{Z}_m, +)$  ist eine kommutative, zyklische Gruppe.

*Beweis.* Wir überprüfen zuerst die Gruppeneigenschaften.

- **Assoziativität.** Diese wird einfach von  $\mathbb{Z}$  geerbt. Genauer gilt

$$(\bar{a} + \bar{b}) + \bar{c} = \overline{a + b} + \bar{c} = \overline{(a + b) + c} = \overline{a + (b + c)} = \bar{a} + \overline{b + c} = \bar{a} + (\bar{b} + \bar{c}).$$

- **Neutrales Element.**  $e = \bar{0}$
- **Inverse Elemente.**  $-\bar{a} = \overline{-a}$

Damit ist  $(\mathbb{Z}_m, +)$  schonmal eine Gruppe.

- **Kommutativität.** Diese wird wieder von  $\mathbb{Z}$  geerbt,  $\bar{a} + \bar{b} = \overline{a + b} = \overline{b + a} = \bar{b} + \bar{a}$ .
- **Zyklizität.**  $\mathbb{Z}_m = \langle \bar{1} \rangle$

Damit ist alles gezeigt. ♥

Mit der Multiplikation ist es etwas schwieriger. Wir fassen zuerst zusammen, was offensichtlich ist.

### Satz 3.4 (Restklassen bilden multiplikatives Monoid)

$(\mathbb{Z}_m, \cdot)$  ist ein kommutatives Monoid.

*Beweis.* Assoziativität und Kommutativität werden wieder von  $\mathbb{Z}$  geerbt (ersetze in den obigen Beweisen einfach “+” durch “·”). Das neutrale Element ist  $e = \bar{1}$ . ♥

**Frage:** Wann ist  $\bar{a} \in \mathbb{Z}_m$  bezüglich der Multiplikation invertierbar? Dass das manchmal der Fall ist und manchmal nicht, zeigt beispielhaft die Verknüpfungstabelle von  $\mathbb{Z}_4$ .

$\downarrow \cdot \rightarrow$	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$
$\bar{0}$	$\bar{0}$	$\bar{0}$	$\bar{0}$	$\bar{0}$
$\bar{1}$	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$
$\bar{2}$	$\bar{0}$	$\bar{2}$	$\bar{0}$	$\bar{2}$
$\bar{3}$	$\bar{0}$	$\bar{3}$	$\bar{2}$	$\bar{1}$

Aus der Tabelle wird ersichtlich, dass...

- ...  $\bar{0}$  und  $\bar{2}$  in  $\mathbb{Z}_4$  **nicht** invertierbar sind (keine  $\bar{1}$  in der jeweiligen Zeile),
- ...  $\bar{1}^{-1} = \bar{1}$  und  $\bar{3}^{-1} = \bar{3}$  gilt.

Wir überlegen uns eine algebraische Bedingung an die Invertierbarkeit von  $\bar{a} \in \mathbb{Z}_m$ .



### Lemma 3.5

Genau dann ist  $\bar{a} \in \mathbb{Z}_m$  invertierbar, wenn es  $b, k \in \mathbb{Z}$  gibt mit  $ab + mk = 1$ .

*Beweis.* Genau dann ist  $\bar{a} \in \mathbb{Z}_m$  invertierbar, wenn es  $\bar{b} \in \mathbb{Z}_m$  gibt mit  $\bar{a} \cdot \bar{b} = \bar{1}$ , also  $\overline{ab} = \bar{1}$ . Dies ist genau dann der Fall, wenn  $ab + mk = 1$  für ein  $k \in \mathbb{Z}$  gilt. ♥

Wie sich herausstellt, ist das genau dann der Fall, wenn  $a$  und  $m$  **teilerfremd** sind, was wir in einem Augenblick auch beweisen werden.

### Satz 3.6 (Multiplikative Invertierbarkeit einer Restklasse)

Genau dann ist  $\bar{a} \in \mathbb{Z}_m$  invertierbar, wenn  $\text{ggT}(a, m) = 1$  gilt.

Dem Beweis (folgt gleich) zugrunde liegt das sogenannte **Lemma von Bézout**.

### Lemma 3.7 (Lemma von Bézout)

Seien  $x, y \in \mathbb{N}$ . Dann gibt es  $s, t \in \mathbb{Z}$  mit  $sx + ty = \text{ggT}(x, y)$ .

Zum Beispiel ist  $\text{ggT}(69, 420) = 3 = 67 \cdot 69 + (-11) \cdot 420$ . Wie man  $s$  und  $t$  berechnen kann, sehen wir auch gleich. Zuerst der Beweis des Lemmas.

*Beweis.* Für gegebene  $x, y \in \mathbb{N}$  betrachte die Menge  $H_{x,y} := \{sx + ty \mid s, t \in \mathbb{Z}\} \subset \mathbb{Z}$ .

Man überzeugt sich leicht davon, dass  $H_{x,y} \subset \mathbb{Z}$  eine Untergruppe ist. Gemäß Satz 2.5 ist dann  $\{0\} \neq H_{x,y} = d\mathbb{Z}$  für ein  $d \in \mathbb{N}$ .

Wir wollen  $d = \text{ggT}(x, y)$  zeigen.

- Wegen  $d \in d\mathbb{Z}$  gilt  $d \in H_{x,y}$ . Das heißt, es gibt  $s, t \in \mathbb{Z}$  mit  $d = sx + ty$ . Daraus folgt, dass  $\text{ggT}(x, y)$  ein Teiler von  $d$  ist.
- Wegen  $x, y \in H_{x,y}$  gilt  $x, y \in d\mathbb{Z}$ . Damit teilt  $d$  sowohl  $x$  als auch  $y$ . Also ist  $d$  auch ein Teiler von  $\text{ggT}(x, y)$ .

Zusammen folgt  $\text{ggT}(x, y) = d = sx + ty$  für gewisse  $s, t \in \mathbb{Z}$ . ♥

Es gilt auch die folgende Umkehrung des Lemmas, die leichter einzusehen ist.

### Lemma 3.8 (Umkehrung des Lemmas von Bézout)

Seien  $x, y \in \mathbb{N}$ . Es gebe  $s, t \in \mathbb{Z}$  so, dass  $sx + ty = 1$  ist. Dann folgt  $\text{ggT}(x, y) = 1$ .

*Beweis.* Da  $\text{ggT}(x, y)$  sowohl ein Teiler von  $x$  als auch von  $y$  ist, ist  $\text{ggT}(x, y)$  auch ein Teiler von  $sx + ty$ . Wegen  $sx + ty = 1$  folgt sofort  $\text{ggT}(x, y) = 1$ . ♥

Nun noch zum Beweis der Aussage über die Invertierbarkeit von  $\bar{a} \in \mathbb{Z}_m$ , falls  $a$  und  $m$  teilerfremd sind (und nur in diesem Falle).

*Beweis (von Satz 3.6).*

Zur Erinnerung — Nach Lemma 3.5 ist  $\bar{a} \in \mathbb{Z}_m$  genau dann invertierbar, wenn  $ab + mk = 1$  für gewisse  $b, k \in \mathbb{Z}$  gilt.

“ $\implies$ ”: Gelte  $ab + mk = 1$  für gewisse  $b, k \in \mathbb{Z}$ . Nach Umkehrung des Lemmas von Bézout (Lemma 3.8) folgt  $\text{ggT}(a, m) = 1$ .

“ $\impliedby$ ”: Gelte  $\text{ggT}(a, m) = 1$ . Nach Lemma von Bézout (Lemma 3.7) gibt es  $b, k \in \mathbb{Z}$  mit  $ab + mk = 1$ .

Insgesamt ist  $\bar{a} \in \mathbb{Z}_m$  also genau dann invertierbar, wenn  $\text{ggT}(a, m) = 1$  gilt. ♥

### Bemerkung 3.9 (Erweiterter Euklidischer Algorithmus)

Die Koeffizienten  $s, t \in \mathbb{Z}$  aus dem Lemma von Bézout kann man mithilfe des **erweiterten Euklidischen Algorithmus** berechnen (für eine Anleitung siehe Wikipedia).

Insbesondere kann man damit im Falle  $\text{ggT}(a, m) = 1$  das inverse Element  $\bar{a}^{-1}$  berechnen.

Wir wollen uns kurz die beispielhafte Berechnung solch eines inversen Elements anschauen.

### Beispiel 3.10 (Berechnung einer multiplikativ inversen Restklasse)

Was ist das inverse Element von  $\overline{69}$  in  $\mathbb{Z}_{421}$  bezüglich der Multiplikation?

◇ — ◇ — ◇

Zunächst ist  $\text{ggT}(69, 421) = 1$ , also existiert  $\overline{69}^{-1}$  wirklich.

Mithilfe des erweiterten Euklidischen Algorithmus berechnen wir  $1 = (-61) \cdot 69 + 10 \cdot 421$ .

Daraus folgt  $\overline{69}^{-1} = \overline{-61} = \overline{360}$ .

Invertierbarkeit **jedes** Elements  $\bar{a} \in \mathbb{Z}_m$  (wobei  $\bar{a} \neq \bar{0}$ ) bezüglich der Multiplikation liegt also genau dann vor, wenn  $\text{ggT}(a, m) = 1$  für **alle**  $a \in \{1, 2, \dots, m-1\}$  gilt. Das ist immer dann der Fall, wenn  $m$  eine **Primzahl** ist.

### Satz 3.11 (Restklassen ohne Null modulo Primzahl bilden multiplikative Gruppe)

Schreibe  $\mathbb{Z}_m^* := \mathbb{Z}_m \setminus \{0\} = \{\bar{1}, \bar{2}, \dots, \overline{m-1}\}$ .

Genau dann ist  $(\mathbb{Z}_m^*, \cdot)$  eine Gruppe, wenn  $m = p$  eine **Primzahl** ist.

*Beweis.* “ $\implies$ ”: Wir zeigen die Kontraposition.

Sei  $m$  also **keine** Primzahl. Dann gibt es  $a, b < m$  mit  $m = ab$ , also

$$\bar{a} \cdot \bar{b} = \overline{ab} = \overline{m} = \bar{0} \notin \mathbb{Z}_m^*.$$

Das bedeutet, dass die Multiplikation in diesem Fall nicht einmal eine Verknüpfung auf  $\mathbb{Z}_m^*$  definiert, bezüglich der eine Gruppenstruktur vorliegen könnte.

“ $\impliedby$ ”: Sei  $m = p$  eine Primzahl. Dann gibt es **keine**  $a, b < p$  mit  $p = ab$ , also ist  $\bar{a} \cdot \bar{b} \neq \bar{0}$  für alle  $\bar{a}, \bar{b} \in \mathbb{Z}_p^*$ . Damit ist die Multiplikation wirklich eine Verknüpfung auf  $\mathbb{Z}_p^*$ .

⋮

Weil  $p$  eine Primzahl ist, gilt außerdem  $\text{ggT}(a, p) = 1$  für alle  $a \in \{1, 2, \dots, p-1\}$ . Wegen **Satz 3.6** bedeutet das, dass jedes  $\bar{a} \in \mathbb{Z}_p^*$  bezüglich der Multiplikation invertierbar, und  $\mathbb{Z}_p^*$  somit eine Gruppe ist. ♥

## Die diskrete Exponentialfunktion und der Diffie-Hellman-Schlüsselaustausch

Wie wir sehr bald sehen werden, spielen die Gruppen  $\mathbb{Z}_p^*$  für sehr große Primzahlen (600 Stellen) in der Kryptographie eine zentrale Rolle.

Zunächst aber noch ein paar Begrifflichkeiten.

### Bemerkung 3.12 (*Primitivwurzel*)

- ① Man kann zeigen (wir nicht), dass  $\mathbb{Z}_p^*$  immer eine zyklische Gruppe ist.  
Einen Erzeuger von  $\mathbb{Z}_p^*$  nennt man auch eine **Primitivwurzel** modulo  $p$ .
- ② **Nicht** jedes  $\bar{a} \in \mathbb{Z}_p^*$  ist eine Primitivwurzel.
- ③ Es ist **kein** effizienter Algorithmus bekannt, mit dem man alle Primitivwurzeln modulo einer gegebenen Primzahl berechnen könnte.

### Beispiel 3.13 (*Beispiele für Primitivwurzeln*)

Betrachte  $p = 7$ , also  $\mathbb{Z}_7^* = \{\bar{1}, \bar{2}, \bar{3}, \bar{4}, \bar{5}, \bar{6}\}$ . Dann ist...

- ① ...  $\bar{3}$  eine Primitivwurzel;  
(Denn:  $\bar{3} \xrightarrow{\cdot \bar{3}} \bar{2} \xrightarrow{\cdot \bar{3}} \bar{6} \xrightarrow{\cdot \bar{3}} \bar{4} \xrightarrow{\cdot \bar{3}} \bar{5} \xrightarrow{\cdot \bar{3}} \bar{1} \xrightarrow{\cdot \bar{3}} \bar{3} \xrightarrow{\cdot \bar{3}} \dots$ )
- ② ...  $\bar{2}$  **nicht**, genauer  $\langle \bar{2} \rangle = \{\bar{1}, \bar{2}, \bar{4}\} \neq \mathbb{Z}_7^*$ .  
(Denn:  $\bar{2} \xrightarrow{\cdot \bar{2}} \bar{4} \xrightarrow{\cdot \bar{2}} \bar{1} \xrightarrow{\cdot \bar{2}} \bar{2} \xrightarrow{\cdot \bar{2}} \dots$ )

Die scheinbar “chaotische” Reihenfolge der Werte  $\{\bar{1}, \bar{a}, \bar{a}^2, \dots, \bar{a}^{p-2}\}$  (wobei  $\bar{a}$  eine Primitivwurzel modulo  $p$  sei) macht  $\mathbb{Z}_p^*$  unter anderem auch interessant für Pseudozufallszahlengeneratoren (englisch “pseudo random number generator”, kurz “PRNG”). (Ohne an dieser Stelle auf irgendwelche Implementierungsdetails eingehen zu wollen.)

### Definition 3.14 (*Diskrete Exponentialfunktion und diskreter Logarithmus*)

Sei  $G$  eine endliche und zyklische Gruppe mit Erzeuger  $g \in G$  und  $|G| = n \in \mathbb{N}$ .

- ① Wegen  $g^{x+nk} = g^x$  für alle  $x, k \in \mathbb{Z}$  (siehe **Satz 2.25**) ist die Abbildung

$$\exp_g : \mathbb{Z}_n \rightarrow G \text{ durch } \exp_g(x + n\mathbb{Z}) := g^x$$

unabhängig von der Wahl des Repräsentanten der Klasse  $x + n\mathbb{Z}$  definiert.

Man nennt sie die **diskrete Exponentialfunktion** zur Basis  $g$ .

- ② Weil  $G$  zyklisch ist, durchläuft  $g^x$  alle Elemente  $y \in G$ . Insbesondere gibt es für jedes  $y \in G$  genau eine Klasse  $x + n\mathbb{Z} \in \mathbb{Z}_n$  mit  $\exp_g(x + n\mathbb{Z}) = y$ .

⋮

Dies definiert die Umkehrabbildung

$$\log_g : G \rightarrow \mathbb{Z}_n \text{ durch } \log_g(y) := \text{diejenige Klasse } x + n\mathbb{Z} \text{ mit } g^x = y.$$

Sie heit der **diskrete Logarithmus** zur Basis  $g$ .

Natrlich htte man  $\exp_g$  stattdessen auch auf  $\mathbb{Z}$  (statt auf  $\mathbb{Z}_{|G|}$ ) und auch fr nicht-zyklische, nicht-endliche Gruppen  $G$  definieren knnen, aber dann verlre die Gleichung  $g^x = y$  fr gegebene  $g, y \in G$  ihre (eindeutige) Lsbarkeit.

### Bemerkung 3.15 (*Einfachere Notation im Falle primer Restklassengruppen*)

Sei speziell  $G := \mathbb{Z}_p^*$ , also  $|G| = p - 1$ , und  $g := \bar{a}$  eine Primitivwurzel von  $G$ . Dann sind

$$\exp_{\bar{a}} : \mathbb{Z}_{p-1} \rightarrow \mathbb{Z}_p^* \text{ und } \log_{\bar{a}} : \mathbb{Z}_p^* \rightarrow \mathbb{Z}_{p-1}$$

Abbildungen zwischen verschiedenen Restklassengruppen (nmlich der additiven Gruppe  $\mathbb{Z}_{p-1}$  und der multiplikativen Gruppe  $\mathbb{Z}_p^*$ ).

Zur Vermeidung einer verwirrenden Notation lassen wir alle quivalenzklassen weg (keine Querstriche) und schreiben der Einfachheit halber (vergleiche Definition 3.1 (3))...

- ① ...  $\exp_a(x) = a^x = y \pmod{p}$ ,
- ② ...  $\log_a(y) = x \pmod{p-1}$ .

### Beispiel 3.16 (*Beispiele fr Exponentialfunktion und Logarithmus*)

Betrachte  $G := \mathbb{Z}_7^*$ , also  $|G| = 6$ , mit Primitivwurzel  $g := \bar{3}$ .

- ① Es ist  $\exp_{\bar{3}}(4 + 6\mathbb{Z}) = \bar{3}^4 = \bar{4} \in \mathbb{Z}_7^*$ .

Wir schreiben auch einfach  $\exp_3(4) = 3^4 = 4 \pmod{7}$ .

- ② Umgekehrt ist  $\log_{\bar{3}}(\bar{4}) = 4 + 6\mathbb{Z} \in \mathbb{Z}_6$ .

Wir schreiben auch einfach  $\log_3(4) = 4 \pmod{6}$ .

Interessant fr die Kryptographie ist nun ganz konkret die folgende Eigenschaft von Exponentialfunktion und Logarithmus.

### Bemerkung 3.17 (*Exponentialfunktion ist Einwegfunktion*)

Sei  $G := \mathbb{Z}_p^*$  fr eine **sehr** groe Primzahl (600 Stellen), und  $\bar{a}$  eine Primitivwurzel.

Dann ist  $\exp_{\bar{a}}$  eine sogenannte **Einwegfunktion**. Genauer gilt:

- ① Fr alle  $x$  ist  $\exp_a(x) = a^x \pmod{p}$  einfach zu berechnen.
- ② Es ist **kein** Algorithmus bekannt, der die Gleichung  $\log_a(y) = x \pmod{p-1}$  fr gegebenes  $y$  effizienter lst als die Brute-Force-Methode.

Anwendung findet dieser Fakt zum Beispiel im folgenden kryptographischen Verfahren.

### Beispiel 3.18 (Diffie-Hellman-Schlüsselaustausch)

(Nach Whitfield Diffie und Martin Hellman.)

Andreas und Bruno<sup>4</sup> möchten sicher miteinander kommunizieren. Dazu wählen sie für dieses Beispiel ein **symmetrisches** Verschlüsselungsverfahren. Das heißt, für Ver- und Entschlüsselung einer Nachricht wird derselbe geheime Schlüssel  $s$  benutzt.



◇ — ◇ — ◇

**Problem.** Wie können Andreas und Bruno einen sicheren Schlüssel  $s$  vereinbaren, möglicherweise auch über einen unsicheren Kanal? — Ein Angreifer, der  $s$  kennt, könnte schließlich jede Nachricht mitlesen.

◇ — ◇ — ◇

**Lösung.** Andreas und Bruno vereinbaren eine sehr große Primzahl  $p$  und eine Primitivwurzel  $\bar{a} \in \mathbb{Z}_p^*$ . Diese Informationen sind öffentlich und auch für einen potentiellen Angreifer sichtbar (das ist aber egal). Wir rechnen hier der Einfachheit halber mit  $p = 73$  und  $a = 5$ .

Danach denken sich Andreas und Bruno jeweils eine geheime Zahl  $\bar{x}_A, \bar{x}_B \in \mathbb{Z}_{p-1}$  aus, zum Beispiel  $x_A = 42 \pmod{72}$  und  $x_B = 69 \pmod{72}$ . Diese Zahlen kennen nur Andreas bzw. Bruno selbst!

Dann berechnet...

- ... Andreas die Zahl  $y_A := \exp_a(x_A) \pmod{p}$ , also  $y_A = 5^{42} = 70 \pmod{73}$ , und schickt diese Bruno;
- ... Bruno die Zahl  $y_B := \exp_a(x_B) \pmod{p}$ , also  $y_B = 5^{69} = 66 \pmod{73}$ , und schickt diese Andreas.

Diese Zahlen sind wieder öffentlich einsehbar.

Zum Schluss berechnet...

- ... Andreas den Schlüssel  $s_A := y_B^{x_A} \pmod{p}$ , also  $s_A = 66^{42} = 27 \pmod{73}$ ;
- ... Bruno den Schlüssel  $s_B := y_A^{x_B} \pmod{p}$ , also  $s_B = 70^{69} = 27 \pmod{73}$ .

Andreas und Bruno haben dieselbe Zahl  $s_A = s_B =: s$  berechnet.

◇ — ◇ — ◇

**Erklärung.** Dieses Verfahren funktioniert aus den folgenden Gründen:

- ①  $s_A = y_B^{x_A} = (a^{x_B})^{x_A} = a^{x_B x_A} = a^{x_A x_B} = (a^{x_A})^{x_B} = y_A^{x_B} = s_B \pmod{p}$
- ② Um aus den öffentlichen Informationen  $p, a, y_A, y_B$  den geheimen Schlüssel  $s$  zu berechnen, müsste ein Angreifer eine der beiden geheimen Zahlen  $x_A = \log_a(y_A) \pmod{p-1}$  oder  $x_B = \log_a(y_B) \pmod{p-1}$  kennen. Der dafür benötigte diskrete Logarithmus ist für sehr große Primzahlen aber in der Praxis nicht berechenbar, und das Verfahren somit sicher.

## Der Satz von Euler und das RSA-Verfahren

Für den Rest dieses Abschnitts arbeiten wir auf ein weiteres kryptographisches Verfahren hin — das **RSA-Verfahren**, mit dem Nachrichten ver- und entschlüsselt werden können, und dessen Korrektheit wir als grandioses Finale auch wieder beweisen werden. Wie immer benötigen wir aber erst einige Vorbereitungen...

### Definition 3.19 (Eulersche Phi-Funktion)

Die **Eulersche Phi-Funktion** ordnet jeder natürlichen Zahl  $n \in \mathbb{N}$  die Anzahl  $\varphi(n)$  aller Zahlen  $k \in \{1, 2, \dots, n\}$  mit  $\text{ggT}(k, n) = 1$  zu.

Im Moment können wir  $\varphi(n)$  leider nur durch Nachzählen berechnen. Später lernen wir aber eine Formel kennen, die die Primfaktorzerlegung von  $n$  benutzt.

### Beispiel 3.20 (Beispiele für Werte der Eulerschen Phi-Funktion)

- ① Es ist  $\varphi(10) = 4$ , denn die  $k \in \{1, 2, \dots, 10\}$  mit  $\text{ggT}(k, 10) = 1$  sind genau  $\{1, 3, 7, 9\}$ .
- ② Für jede **Primzahl**  $p$  gilt  $\varphi(p) = p - 1$ .

*Zur Erinnerung* — Die Einheitengruppe  $M^\times$  eines Monoids  $M$  bestand aus allen invertierbaren Elementen von  $M$ .

### Bemerkung 3.21 (Multiplikative Einheitengruppe der Restklassen)

Die multiplikative Einheitengruppe  $\mathbb{Z}_m^\times$  umfasst  $\varphi(m)$  Elemente, denn nach **Satz 3.6** sind das genau alle Klassen  $\bar{a} \in \mathbb{Z}_m$  mit  $\text{ggT}(a, m) = 1$ .

⚠ Die Einheitengruppe  $\mathbb{Z}_m^\times$  ist trotz ähnlicher Notation nicht zu verwechseln mit  $\mathbb{Z}_m^* = \mathbb{Z}_m \setminus \{\bar{0}\}$ , aber im Falle  $m = p$  für eine Primzahl  $p$  stimmen diese Mengen (sogar Gruppen) überein.

Essentiell für die Funktionsweise des an späterer Stelle erläuterten RSA-Verfahrens ist der **Satz von Euler** bzw. der daraus folgende **kleine Satz von Fermat**.

### Satz 3.22 (Satz von Euler)

Seien  $a, n \in \mathbb{N}$  mit  $\text{ggT}(a, n) = 1$ . Dann gilt  $a^{\varphi(n)} = 1 \pmod{n}$ .

*Beweis.* Betrachte  $G := \mathbb{Z}_n^\times$ . Wegen  $\text{ggT}(a, n) = 1$  ist  $\bar{a} \in G$ .

Sei  $k \in \mathbb{N}$  der kleinste Exponent mit  $\bar{a}^k = \bar{1}$ , und betrachte die von  $\bar{a}$  erzeugte Untergruppe  $H := \langle \bar{a} \rangle = \{\bar{a}, \bar{a}^2, \dots, \bar{a}^{k-1}, \bar{1}\} \subset G$ .

Nach dem Satz von Lagrange ist  $|H| = k$  ein Teiler von  $|G| = \varphi(n)$ , also gilt  $\varphi(n) = \ell k$  für ein gewisses  $\ell \in \mathbb{N}$ .

Daraus folgt  $a^{\varphi(n)} = a^{\ell k} = (a^k)^\ell = 1^\ell = 1 \pmod{n}$  wie gewünscht. ♥

<sup>4</sup>Ehre gebührt allen Teilnehmern der ersten Instanz dieser Arbeitsgemeinschaft.

Der kleine Satz von Fermat ist einfach nur der Satz von Euler mit der zusätzlichen Voraussetzung, dass  $n = p$  eine Primzahl ist.

### Korollar 3.23 (Kleiner Satz von Fermat)

Sei  $p$  eine **Primzahl** und sei  $a \in \mathbb{N}$  **kein** Vielfaches von  $p$ . Dann gilt  $a^{p-1} = 1 \pmod{p}$ .

*Beweis.* Das folgt sofort aus dem Satz von Euler für  $n = p$ , wobei  $\varphi(p) = p - 1$ . ♥

Das folgende Beispiel ist eine nette Spielerei, die die Anwendung des Satzes von Euler illustriert.

### Beispiel 3.24 (Beispiel für die Anwendung des Satzes von Euler)

Was sind die letzten beiden Ziffern von  $69^{42}$ ?

◇ — ◇ — ◇

Bezeichne mit  $x \in \{0, 1, \dots, 99\}$  die letzten beiden Ziffern von  $69^{42}$ , also  $x = 69^{42} \pmod{100}$ .

Wegen  $\text{ggT}(69, 100) = 1$  ist der Satz von Euler anwendbar, also  $69^{\varphi(100)} = 1 \pmod{100}$ . Durch Nachzählen erhalten wir  $\varphi(100) = 40$ . (Oder noch etwas geschickter: Wir subtrahieren von  $100 = 2^2 \cdot 5^2$  die Vielfachen von 2 und die von 5, und addieren die doppelt abgezogenen Vielfachen von 10 wieder hinzu, also  $\varphi(100) = 100 - 50 - 20 + 10 = 40$ .)

Daraus folgt  $x = 69^{42} = 69^{40} \cdot 69^2 = 1 \cdot 69^2 = 4761 = 61 \pmod{100}$ , die letzten beiden Ziffern von  $69^{42}$  sind also 61.

Eine wichtige Eigenschaft von  $\varphi$ , die für die Herleitung einer Formel eine zentrale Rolle spielt, ist ihre Multiplikativität. Genauer gilt:

### Satz 3.25 (Multiplikativität der Eulerschen Phi-Funktion)

Seien  $n, m \in \mathbb{N}$  **teilerfremd** (!), also es gelte  $\text{ggT}(n, m) = 1$ .

Dann ist  $\varphi(nm) = \varphi(n)\varphi(m)$ .

Wir betrachten dazu das folgende einleitende Beispiel. (Der Beweis des Satzes folgt später.)

### Beispiel 3.26 (Lösungen eines Gleichungssystems)

Was sind die Lösungen  $x \in \mathbb{Z}$  des folgenden Gleichungssystems?

①  $x = 2 \pmod{5}$

②  $x = 3 \pmod{7}$

◇ — ◇ — ◇

Wir finden die Lösungen durch Ausprobieren heraus.

①  $x \in \{\dots, -3, 2, 7, 12, \mathbf{17}, 22, 27, 32, 37, 42, 47, \mathbf{52}, \dots\}$

②  $x \in \{\dots, -4, 3, 10, \mathbf{17}, 24, 31, 38, 45, \mathbf{52}, \dots\}$

⋮

Wie man sieht, löst  $x = 17$  das Gleichungssystem, genauso wie jede andere Zahl aus  $17 + 35\mathbb{Z}$ . Die Lösungen des Gleichungssystems sind genau alle  $x \in 17 + 35\mathbb{Z}$  (ohne Beweis).

Das einleitende Beispiel motiviert den folgenden allgemeinen Satz.

### Satz 3.27 (*Chinesischer Restsatz*)

Seien  $n, m \in \mathbb{N}$  teilerfremd, also  $\text{ggT}(n, m) = 1$ ; und seien  $a, b \in \mathbb{Z}$  beliebig.

Dann hat das Gleichungssystem

$$\textcircled{1} \quad x = a \pmod{n}$$

$$\textcircled{2} \quad x = b \pmod{m}$$

eine Lösung  $x \in \mathbb{Z}$ , und diese ist eindeutig modulo  $nm$ .

(Die Lösungsmenge ist also von der Form  $x + nm\mathbb{Z}$  für eine ganze Zahl  $x$ .)

*Beweis.* Wir zeigen Existenz und Eindeutigkeit der behaupteten Lösung getrennt.

- **Eindeutigkeit.** Seien  $x, y \in \mathbb{Z}$  zwei Lösungen des Gleichungssystems. Wir wollen zeigen, dass in Wahrheit  $x = y \pmod{nm}$  gilt.

Da beide Zahlen das Gleichungssystem lösen, gilt sowohl  $x = a = y \pmod{n}$  als auch  $x = b = y \pmod{m}$ , also  $x - y = 0 \pmod{n}$  und  $x - y = 0 \pmod{m}$ .

Folglich ist  $x - y$  sowohl ein ganzzahliges Vielfaches von  $n$  als auch von  $m$ . Damit ist  $x - y$  also auch ein ganzzahliges Vielfaches von  $\text{kgV}(n, m)$ .

Wegen der Voraussetzung  $\text{ggT}(n, m) = 1$  gilt aber einfach  $\text{kgV}(n, m) = nm$ , also ist  $x - y = 0 \pmod{nm}$ , das heißt  $x = y \pmod{nm}$  wie behauptet.

- **Existenz.** Wir konstruieren eine Lösung  $x$  des Gleichungssystems ganz explizit.

Wegen  $\text{ggT}(n, m) = 1$  ist sowohl  $\bar{n} \in \mathbb{Z}_m$  als auch  $\bar{m} \in \mathbb{Z}_n$  invertierbar. Bezeichne die Inversen mit  $\bar{r} := \bar{n}^{-1} \in \mathbb{Z}_m$  bzw.  $\bar{s} := \bar{m}^{-1} \in \mathbb{Z}_n$ . (Also gilt  $rn = nr = 1 \pmod{m}$  und  $sm = ms = 1 \pmod{n}$ .)

Setze  $x := msa + nrb \in \mathbb{Z}$ . Dann löst  $x$  wirklich das Gleichungssystem, denn:

$$\textcircled{1} \quad x = 1 \cdot a + 0 = a \pmod{n}$$

$$\textcircled{2} \quad x = 0 + 1 \cdot b = b \pmod{m}$$

Folglich ist  $x = msa + nrb$  die eindeutige (modulo  $nm$ ) Lösung des Gleichungssystems. ♥

Wir überzeugen uns exemplarisch von der Korrektheit des Satzes am einleitenden **Beispiel 3.26**.

### Beispiel 3.28 (*Beispiel für die Anwendung des Chinesischen Restsatzes*)

In der Situation von **Beispiel 3.26** sind  $n = 5$  und  $m = 7$  sowie  $a = 2$  und  $b = 3$ .

Die Voraussetzung des Chinesischen Restsatzes ist mit  $\text{ggT}(5, 7) = 1$  erfüllt. Es gibt also eine eindeutige Lösung  $x$  modulo  $5 \cdot 7 = 35$ .

⋮



Wir berechnen  $r = 5^{-1} = 3 \pmod{7}$  (denn  $3 \cdot 5 = 15 = 1 \pmod{7}$ ) und  $s = 7^{-1} = 3 \pmod{5}$  (denn  $3 \cdot 7 = 21 = 1 \pmod{5}$ ).

Dann ist  $x = 7 \cdot 3 \cdot 2 + 5 \cdot 3 \cdot 3 = 87 = 17 \pmod{35}$  genau die Lösung, die wir bereits durch Ausprobieren “herausgefunden” haben (*Jetzt ist aber alles wasserdicht.*)

Mithilfe des Chinesischen Restsatzes können wir nun auch die Multiplikativität der Eulerschen Phi-Funktion beweisen. Dafür noch ein schnelles Lemma.

### Lemma 3.29

Seien  $n, m, x \in \mathbb{N}$ .

Dann ist  $\text{ggT}(x, nm) = 1$  äquivalent zu  $\text{ggT}(x, n) = 1$  und  $\text{ggT}(x, m) = 1$ .

Mit anderen Worten ist  $\bar{x} \in \mathbb{Z}_{nm}^\times$  äquivalent zu  $\bar{x} \in \mathbb{Z}_n^\times$  und  $\bar{x} \in \mathbb{Z}_m^\times$ .

*Beweis.* Bezeichne mit  $N, M$ , und  $X$  jeweils die Menge der Primfaktoren von  $n, m$ , bzw.  $x$ . Dann hat  $nm$  die Primfaktoren  $N \cup M$ .

Genau dann ist  $\text{ggT}(x, nm) = 1$ , wenn  $X \cap (N \cup M) = \emptyset$ . Dies ist genau dann der Fall, wenn  $X \cap N = \emptyset = X \cap M$ , also wenn sowohl  $\text{ggT}(x, n) = 1$  als auch  $\text{ggT}(x, m) = 1$  gilt. ♥

Nun zum eigentlichen Beweis der Multiplikativität von  $\varphi$ .

*Beweis (von Satz 3.25).* Zu zeigen ist  $\varphi(nm) = \varphi(n)\varphi(m)$ , wann immer  $\text{ggT}(n, m) = 1$ .

Wir betrachten dafür die Abbildung  $f : \mathbb{Z}_{nm}^\times \rightarrow \mathbb{Z}_n^\times \times \mathbb{Z}_m^\times$  gegeben durch

$$f(x + nm\mathbb{Z}) := (x + n\mathbb{Z}, x + m\mathbb{Z}).$$

Diese ist korrekt definiert:

- Wenn  $x = y \pmod{nm}$ , dann gilt insbesondere  $x = y \pmod{n}$  sowie  $x = y \pmod{m}$ . Also  $f(x + nm\mathbb{Z}) = f(y + nm\mathbb{Z})$ ; das heißt,  $f$  ist wirklich repräsentantenunabhängig.
- Wenn  $\bar{x} \in \mathbb{Z}_{nm}^\times$ , dann auch  $\bar{x} \in \mathbb{Z}_n^\times$  sowie  $\bar{x} \in \mathbb{Z}_m^\times$  nach dem obigen Lemma 3.29. Das heißt,  $f$  bildet wirklich in die Teilmenge  $\mathbb{Z}_n^\times \times \mathbb{Z}_m^\times$  von  $\mathbb{Z}_n \times \mathbb{Z}_m$  ab.

Betrachte  $(a + n\mathbb{Z}, b + m\mathbb{Z}) \in \mathbb{Z}_n^\times \times \mathbb{Z}_m^\times$ . Dann gibt es gemäß dem Chinesischen Restsatz (dessen Voraussetzung mit  $\text{ggT}(n, m) = 1$  erfüllt ist) genau ein  $x + nm\mathbb{Z} \in \mathbb{Z}_{nm}$  — wegen Lemma 3.29 sogar in  $\mathbb{Z}_{nm}^\times$  — mit

$$f(x + nm\mathbb{Z}) = (a + n\mathbb{Z}, b + m\mathbb{Z}).$$

Das bedeutet,  $f$  ist eine bijektive Abbildung.

Weil  $f$  eine bijektive Abbildung zwischen endlichen Mengen ist, folgt, dass Start- und Zielmenge gleich viele Elemente haben müssen.

Die Anzahl der Elemente der Start- und Zielmenge ist aber gegeben durch  $|\mathbb{Z}_{nm}^\times| = \varphi(nm)$  bzw.  $|\mathbb{Z}_n^\times \times \mathbb{Z}_m^\times| = \varphi(n)\varphi(m)$  (siehe Bemerkung 3.21), woraus die Behauptung folgt. ♥

Um ein besseres Gefühl für die im Beweis auftretende Abbildung  $f$  zu erhalten, betrachten wir das folgende Beispiel.

**Beispiel 3.30** (*Beispiel für die Bijektion zwischen den Einheitengruppen*)

Seien  $n = 3$  und  $m = 4$ , also  $\text{ggT}(n, m) = 1$  und  $nm = 12$ .

Dann gilt  $\mathbb{Z}_3^\times = \{\bar{1}, \bar{2}\}$ ,  $\mathbb{Z}_4^\times = \{\bar{1}, \bar{3}\}$ , und  $\mathbb{Z}_{12}^\times = \{\bar{1}, \bar{5}, \bar{7}, \bar{11}\}$ .

Die Zielmenge der Abbildung  $f$  ist  $\mathbb{Z}_3^\times \times \mathbb{Z}_4^\times = \{(\bar{1}, \bar{1}), (\bar{2}, \bar{1}), (\bar{1}, \bar{3}), (\bar{2}, \bar{3})\}$ .

Dann ist  $f : \mathbb{Z}_{12}^\times \rightarrow \mathbb{Z}_3^\times \times \mathbb{Z}_4^\times$  gegeben durch

$$\begin{array}{c|cccc} \bar{x} & \bar{1} & \bar{5} & \bar{7} & \bar{11} \\ \hline f(\bar{x}) & (\bar{1}, \bar{1}) & (\bar{2}, \bar{1}) & (\bar{1}, \bar{3}) & (\bar{2}, \bar{3}) \end{array}.$$

Wir leiten nun endlich eine Formel für  $\varphi(n)$  her. Dafür zuerst das folgende Lemma.

**Lemma 3.31** (*Wert der Eulerschen Phi-Funktion einer Primzahlpotenz*)

Sei  $p$  eine Primzahl und  $m \in \mathbb{N}$ . Dann gilt  $\varphi(p^m) = p^m - p^{m-1}$ .

*Beweis.* Genau dann ist  $\text{ggT}(k, p^m) \neq 1$ , wenn  $k$  ein Vielfaches von  $p$  ist.

Die Vielfachen von  $p$  sind genau  $\{p, 2p, 3p, \dots, p^{m-1}p = p^m\}$ . Dies sind  $p^{m-1}$  Zahlen.

Folglich ist  $\varphi(p^m) = p^m - p^{m-1}$ . ♥

**Satz 3.32** (*Formel für die Eulersche Phi-Funktion*)

Für alle  $n \in \mathbb{N}$  gilt

$$\varphi(n) = n \prod_{p \in P(n)} \left(1 - \frac{1}{p}\right),$$

wobei  $P(n)$  die Menge der Primfaktoren von  $n$  sei. (Zum Beispiel ist  $P(100) = \{2, 5\}$ .)

*Beweis.* Sei  $n = p_1^{m_1} p_2^{m_2} \dots p_r^{m_r}$  die Primfaktorzerlegung von  $n$ , also  $P(n) = \{p_1, p_2, \dots, p_r\}$ .

Wir berechnen

$$\begin{aligned} \varphi(n) &= \varphi(p_1^{m_1} p_2^{m_2} \dots p_r^{m_r}) && \text{(Primfaktorzerlegung)} \\ &= \varphi(p_1^{m_1}) \varphi(p_2^{m_2}) \dots \varphi(p_r^{m_r}) && \text{(Multiplikativität von } \varphi) \\ &= (p_1^{m_1} - p_1^{m_1-1}) (p_2^{m_2} - p_2^{m_2-1}) \dots (p_r^{m_r} - p_r^{m_r-1}) && \text{(Lemma 3.31)} \\ &= p_1^{m_1} \left(1 - \frac{1}{p_1}\right) p_2^{m_2} \left(1 - \frac{1}{p_2}\right) \dots p_r^{m_r} \left(1 - \frac{1}{p_r}\right) && \text{(ausklammern)} \\ &= n \prod_{p \in P(n)} \left(1 - \frac{1}{p}\right) \end{aligned}$$

wie gewünscht. ♥

Damit sind wir nicht mehr aufs Nachzählen angewiesen, wie das folgende Beispiel illustriert.

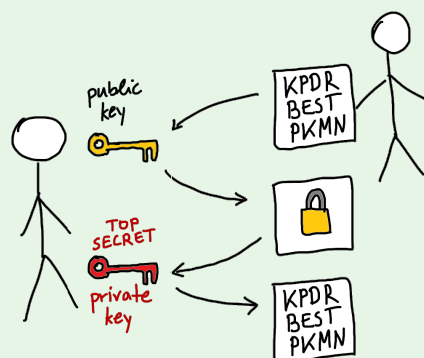
### Beispiel 3.33 (Berechnung beispielhafter Werte der Eulerschen Phi-Funktion)

- ① Sei  $n = 100 = 2^2 \cdot 5^2$ , also  $P(100) = \{2, 5\}$ .  
Dann gilt  $\varphi(100) = 100 \cdot (1 - \frac{1}{2}) \cdot (1 - \frac{1}{5}) = 40$ .
- ② Sei  $n = 2024 = 2^3 \cdot 11 \cdot 23$ , also  $P(2024) = \{2, 11, 23\}$ .  
Dann gilt  $\varphi(2024) = 2024 \cdot (1 - \frac{1}{2}) \cdot (1 - \frac{1}{11}) \cdot (1 - \frac{1}{23}) = 880$ .

Als grandioses Finale dieses Abschnitts können wir endlich das RSA-Verfahren formulieren und sogar dessen Richtigkeit beweisen!

### Beispiel 3.34 (RSA-Verfahren)

Beim **RSA-Verfahren** (nach *Rivest, Shamir, und Adleman*) handelt es sich um ein **asymmetrisches** Verschlüsselungsverfahren. Das heißt, für das Ver- und Entschlüsseln einer Nachricht werden verschiedene Schlüssel benutzt — nämlich der **öffentliche Schlüssel** bzw. der **private Schlüssel** des Empfängers — wie das folgende Bild illustriert.



◇ — ◇ — ◇

**Quintessenz.** Die dem RSA-Verfahren zugrunde liegende Einwegfunktion (für den Begriff vergleiche **Bemerkung 3.17**) ist das Multiplizieren von Primzahlen. Genauer gilt:

- Es ist sehr einfach, das Produkt von Primzahlen zu berechnen.
- Es ist sehr schwierig, die Primfaktorzerlegung einer gegebenen Zahl zu finden.

Für hinreichend große Primzahlen (in der Praxis mehr als 600 Stellen) ist es quasi unmöglich, die Primfaktoren einer Zahl gezielt herauszufinden.

◇ — ◇ — ◇

**Vorsicht.** ⚠ Wir betrachten an dieser Stelle nur die grundlegende mathematische Funktionsweise des Verfahrens. Auf Optimierungen, die das Verfahren resistent gegen Angriffe machen, gehen wir hier nicht ein. Das ist Gegenstand der Kryptographie.

◇ — ◇ — ◇

**Schlüssel-Erzeugung.** Zunächst erzeugen wir für den Empfänger ein Schlüsselpaar. Dazu nehmen wir aus Sicht des Empfängers folgende Schritte vor:

- Wähle zwei sehr große Primzahlen  $p$  und  $q$ . (**Geheim!**)
- Berechne  $n := pq$ . Dies ist öffentliche Information. (Aufgrund der Größe der Zahl ist es praktisch nicht möglich,  $p$  und  $q$  anhand von  $n$  zu bestimmen.)
- Berechne  $\varphi(n) = \varphi(p)\varphi(q) = (p-1)(q-1)$ . (**Geheim!**)
- Wähle irgendeine Zahl  $\bar{e} \in \mathbb{Z}_{\varphi(n)}^\times$ . Dies ist der **öffentliche Schlüssel** des Empfängers.
- Berechne  $\bar{d} := \bar{e}^{-1} \in \mathbb{Z}_{\varphi(n)}^\times$ . Dies ist der **private Schlüssel** des Empfängers. (**Geheim!**)

◇ — ◇ — ◇

**Ver- und Entschlüsseln.** Die relevanten öffentlichen Informationen sind  $n$  und der öffentliche Schlüssel  $\bar{e} \in \mathbb{Z}_{\varphi(n)}^\times$ . Die relevante geheime Information ist der private Schlüssel  $\bar{d} \in \mathbb{Z}_{\varphi(n)}^\times$  des Empfängers.

Sei nun  $\bar{m} \in \mathbb{Z}_n^\times$ , also mit  $\text{ggT}(m, n) = 1$ , die zu verschlüsselnde Nachricht.<sup>5</sup> (Wir kümmern uns hier nicht darum, aus einem Text solch eine Zahl umkehrbar zu erzeugen.)

- Zum **Verschlüsseln** berechnet der Absender die Zahl  $\bar{c} := \bar{m}^e \in \mathbb{Z}_n^\times$ .  
(Das ist wohldefiniert, denn  $e$  ist zwar modulo  $\varphi(n)$  definiert, aber wegen  $\text{ggT}(m, n) = 1$  ist  $m^{\varphi(n)} = 1$  gemäß dem Satz von Euler.)
- Zum **Entschlüsseln** berechnet der Empfänger die Zahl  $\bar{m}' := \bar{c}^d \in \mathbb{Z}_n^\times$ .  
(Auch das ist wohldefiniert, denn auch  $d$  ist zwar modulo  $\varphi(n)$  definiert, aber wegen  $\bar{c} \in \mathbb{Z}_n^\times$  gilt auch  $\text{ggT}(c, n) = 1$  und somit wieder  $c^{\varphi(n)} = 1$  gemäß dem Satz von Euler.)

◇ — ◇ — ◇

**Korrektheit.** Das Verfahren ist korrekt, wie wir im nachfolgenden Satz zeigen werden, also  $\bar{m}' = \bar{m} \in \mathbb{Z}_n^\times$ . (Verschlüsseln und danach Entschlüsseln liefert also wieder den Eingangstext.)

### Satz 3.35 (Korrektheit des RSA-Verfahrens)

Das RSA-Verfahren ist korrekt.

Das heißt, mit den Bezeichnungen aus dem vorigen Beispiel gilt  $m^{ed} = m \pmod{n}$ .

Der Beweis benutzt den **Satz von Euler**.

*Beweis.* Per Definition von  $\bar{d} := \bar{e}^{-1} \in \mathbb{Z}_{\varphi(n)}^\times$  gilt  $ed = 1 \pmod{\varphi(n)}$ .

Das bedeutet  $ed - 1 = 0 \pmod{\varphi(n)}$ ; das heißt,  $ed - 1$  ist ein Vielfaches von  $\varphi(n)$ , also  $ed - 1 = k\varphi(n)$  für ein  $k \in \mathbb{Z}$ .

Wegen der Voraussetzung  $\text{ggT}(n, m) = 1$  folgt  $m^{\varphi(n)} = 1 \pmod{n}$  aus dem Satz von Euler.

Daraus folgt

$$m^{ed} = m^{ed-1}m = m^{k\varphi(n)}m = 1^k m = m \pmod{n}$$

wie behauptet und wir sind fertig.



<sup>5</sup>Die Voraussetzung  $\text{ggT}(n, m) = 1$  ist nicht essentiell. Das RSA-Verfahren funktioniert auch ohne sie, und zwar auf Basis des kleinen Satzes von Fermat anstatt des Satzes von Euler. Der Beweis ist mit der zusätzlichen Voraussetzung aber ein bisschen kürzer.

In diesem Abschnitt werden wir formalisieren, was es für zwei Gruppen bedeutet, “im Wesentlichen gleich” zu sein. Als motivierendes Beispiel vergleichen wir die Verknüpfungstafeln der Restklassengruppe  $\mathbb{Z}_3 = \{\bar{0}, \bar{1}, \bar{2}\}$  und der zyklischen Gruppe  $C(3) = \{\text{id}, d_{120}, d_{240}\}$  (siehe Definition 1.39 (2)).

$\mathbb{Z}_3$				$C(3)$			
$\downarrow + \rightarrow$	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\downarrow \circ \rightarrow$	id	$d_{120}$	$d_{240}$
$\bar{0}$	$\bar{0}$	$\bar{1}$	$\bar{2}$	id	id	$d_{120}$	$d_{240}$
$\bar{1}$	$\bar{1}$	$\bar{2}$	$\bar{0}$	$d_{120}$	$d_{120}$	$d_{240}$	id
$\bar{2}$	$\bar{2}$	$\bar{0}$	$\bar{1}$	$d_{240}$	$d_{240}$	id	$d_{120}$

Dabei fällt auf, dass beide Verknüpfungstafeln dasselbe Muster beschreiben. Identifiziert man nämlich  $\bar{0} \leftrightarrow \text{id}$ ,  $\bar{1} \leftrightarrow d_{120}$ , und  $\bar{2} \leftrightarrow d_{240}$ , so sind auch die Verknüpfungstafeln identisch.

Wir können diese Beobachtung auch algebraisch formulieren. Sei dafür  $f : \mathbb{Z}_3 \rightarrow C(3)$  gegeben durch  $f(\bar{0}) := \text{id}$ ,  $f(\bar{1}) := d_{120}$ , und  $f(\bar{2}) := d_{240}$ . Dann sind die folgenden Aktionen identisch:

- in  $\mathbb{Z}_3$  zwei Elemente  $\bar{k}$  und  $\bar{\ell}$  verknüpfen
- diese beiden Elemente mittels  $f$  nach  $C(3)$  abbilden, dort verknüpfen, und das Ergebnis mittels  $f^{-1}$  wieder nach  $\mathbb{Z}_3$  abbilden

In Formeln bedeutet das  $\bar{k} + \bar{\ell} = f^{-1}(f(\bar{k}) \circ f(\bar{\ell}))$ , oder umgestellt  $f(\bar{k} + \bar{\ell}) = f(\bar{k}) \circ f(\bar{\ell})$ .

Dies führt zu den folgenden Definitionen.

#### Definition 4.1 (Homomorphismus und Isomorphismus)

Seien  $(G, \circ_G)$  und  $(H, \circ_H)$  zwei Gruppen.

- ① Eine Abbildung  $f : G \rightarrow H$  heißt ein **Homomorphismus**, falls

$$f(g_1 \circ_G g_2) = f(g_1) \circ_H f(g_2)$$

für alle  $g_1, g_2 \in G$  gilt.

- ② Ein Homomorphismus  $f : G \rightarrow H$ , der zusätzlich **bijektiv** ist, heißt ein **Isomorphismus**. Falls es einen Isomorphismus  $f : G \rightarrow H$  gibt, heißen die Gruppen  $G$  und  $H$  **isomorph**, geschrieben  $G \cong H$ .

Isomorphe Gruppen haben also dieselbe Gruppenstruktur (gleiche Verknüpfungstafeln), auch wenn die zugrunde liegenden Objekte ganz verschieden sein können. Zum Beispiel haben wir gerade  $\mathbb{Z}_3 \cong C(3)$  mittels der oben definierten Abbildung  $f$  gesehen, aber die Elemente von  $\mathbb{Z}_3$  sind Restklassen, und die von  $C(3)$  sind Drehungen des  $\mathbb{R}^2$ .

#### Beispiel 4.2 (Beispiele für Homomorphismen und Isomorphismen)

- ① Seien  $G$  irgendeine Gruppe, und sei  $g \in G$  beliebig. Betrachte die Abbildung  $f : \mathbb{Z} \rightarrow G$  gegeben durch  $f(k) := g^k$ . Diese ist ein Homomorphismus wegen

$$\begin{aligned} f(k + \ell) &= g^{k+\ell} = g^k \circ g^\ell = f(k) \circ f(\ell), \\ &\vdots \end{aligned}$$

aber im Allgemeinen **kein** Isomorphismus.

- ② Das motivierende Beispiel lässt sich zu  $\mathbb{Z}_n \cong C(n) = \langle d_{360/n} \rangle$  verallgemeinern.

Betrachte dafür die Abbildung  $f : \mathbb{Z}_n \rightarrow C(n)$  gegeben durch  $f(\bar{k}) := d_{360k/n}$ . (Für  $n = 3$  ist das genau die Abbildung aus dem motivierenden Beispiel.)

Diese ist wohldefiniert wegen  $f(\overline{k+nt}) = d_{360k/n+360t} = d_{360k/n} = f(\bar{k})$ , und ein Homomorphismus wegen

$$f(\overline{k+\ell}) = f(\overline{k+\ell}) = d_{360(k+\ell)/n} = d_{360k/n+360\ell/n} = d_{360k/n} \circ d_{360\ell/n} = f(\bar{k}) \circ f(\bar{\ell}).$$

Sie ist offensichtlich auch bijektiv, also ein Isomorphismus.

- ③ Es ist  $(\mathbb{R}, +) \cong (\mathbb{R}_{>0}, \cdot)$ , also Multiplikation positiver Zahlen ist im Wesentlichen nichts anderes als Addition reeller Zahlen.

Betrachte dazu die natürliche Exponentialfunktion  $\exp : \mathbb{R} \rightarrow \mathbb{R}_{>0}$ , gegeben durch  $\exp(x) = e^x$ . Aus dem Regelunterricht wissen wir, dass diese bijektiv ist; die Umkehrabbildung ist der natürliche Logarithmus  $\ln : \mathbb{R}_{>0} \rightarrow \mathbb{R}$ .

Sie ist ein Homomorphismus, denn

$$\exp(x+y) = e^{x+y} = e^x \cdot e^y = \exp(x) \cdot \exp(y),$$

insgesamt also ein Isomorphismus.

- ④ Betrachte die additive Gruppe  $\mathbb{R}$  und die Drehgruppe  $SO(\mathbb{R}^2) = \{d_\alpha \mid \alpha \in \mathbb{R}\}$  der Euklidischen Ebene. Dann ist die durch  $f(\alpha) := d_\alpha$  definierte Abbildung  $f : \mathbb{R} \rightarrow SO(\mathbb{R}^2)$  ein Homomorphismus, denn

$$f(\alpha + \beta) = d_{\alpha+\beta} = d_\alpha \circ d_\beta = f(\alpha) \circ f(\beta).$$

Sie ist **kein** Isomorphismus, da sie nicht injektiv ist, denn es gilt  $f(\alpha) = f(\alpha + 360)$  für alle  $\alpha \in \mathbb{R}$ .

- ⑤ Man kann sie aber injektiv, also zu einem Isomorphismus machen.

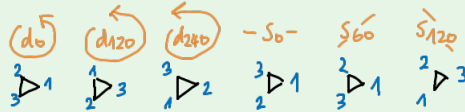
Dafür betrachten wir die Quotientenmenge  $\mathbb{R}/360\mathbb{Z}$  (vergleiche **Beispiel 2.18 (2)**) und definieren  $[\alpha] + [\beta] := [\alpha + \beta]$  komplett analog zur Addition von Restklassen. (Dies ist wirklich eine Gruppe mit  $e = [0]$  und  $-[\alpha] = [-\alpha]$ .)

Die Abbildung  $f : \mathbb{R}/360\mathbb{Z} \rightarrow SO(\mathbb{R}^2)$  mit  $f([\alpha]) := d_\alpha$  ist dann repräsentantenunabhängig definiert — wegen  $f([\alpha + 360]) = d_{\alpha+360} = d_\alpha = f([\alpha])$  — und, analog zum vorigen Beispiel, ein Homomorphismus.

Da  $[\alpha]$  und  $[\alpha + 360]$  in der Startmenge  $\mathbb{R}/360\mathbb{Z}$  dasselbe Objekt beschreiben, ist  $f$  nun auch injektiv, und damit ein Isomorphismus. Wir haben die Gruppe der Drehungen also mit einem “Kreis” (und der Addition von Punkten darauf) identifiziert.

- ⑥ Betrachte die Dieder-Gruppe  $Di(3) = \{\text{id}, d_{120}, d_{240}, s_0, s_{60}, s_{120}\}$  der Symmetrien eines gleichseitigen Dreiecks sowie die symmetrische Gruppe  $Sym(3)$  der Permutationen der Menge  $\{1, 2, 3\}$ .

Nummeriert man die Ecken des Dreiecks mit  $\{1, 2, 3\}$ , entspricht jede Isometrie in  $Di(3)$  genau einer Permutation in  $Sym(3)$ , wie das folgende Bild zeigt.



Dies ist ein Isomorphismus.

Für  $n \neq 3$  liefert diese Identifikation zwar immer noch einen Homomorphismus, aber wegen  $|\text{Di}(n)| = 2n$  und  $|\text{Sym}(n)| = n!$  ist dieser dann nicht mehr bijektiv.

Wie wir gleich sehen werden, handelt es sich bei der Isomorphie von Gruppen um eine Äquivalenzrelation. Das bedeutet, dass es Sinn macht, vom **Isomorphietyp** einer Gruppe zu sprechen (alle Gruppen desselben Isomorphietyps sind paarweise isomorph, und Gruppen verschiedener Isomorphietypen sind nicht isomorph).

### Satz 4.3 (Neue Homomorphismen aus alten)

- ① Seien  $f : G \rightarrow H$  und  $f' : H \rightarrow K$  Homomorphismen (bzw. Isomorphismen).  
Dann ist auch  $f' \circ f : G \rightarrow K$  ein Homomorphismus (bzw. Isomorphismus).
- ② Sei  $f : G \rightarrow H$  ein Isomorphismus.  
Dann ist auch  $f^{-1} : H \rightarrow G$  ein Isomorphismus

*Beweis.*

**Zu ①.** Seien  $g_1, g_2 \in G$ . Dann gilt

$$\begin{aligned}
 (f' \circ f)(g_1 \circ_G g_2) &= f'(f(g_1 \circ_G g_2)) && \text{(Definition der Hintereinanderausführung)} \\
 &= f'(f(g_1) \circ_H f(g_2)) && (f \text{ ist ein Homomorphismus}) \\
 &= f'(f(g_1)) \circ_K f'(f(g_2)) && (f' \text{ ist ein Homomorphismus}) \\
 &= (f' \circ f)(g_1) \circ_K (f' \circ f)(g_2) && \text{(Definition der Hintereinanderausführung)}
 \end{aligned}$$

wie gewünscht. Falls  $f$  und  $f'$  beide Isomorphismen — also insbesondere bijektiv — sind, ist auch  $f' \circ f$  bijektiv, und somit ein Isomorphismus.

**Zu ②.** Seien  $h_1, h_2 \in H$ . Dann gibt es genau ein  $g_1 \in G$  bzw.  $g_2 \in G$  mit  $h_1 = f(g_1)$  und  $h_2 = f(g_2)$ , und es gilt

$$\begin{aligned}
 f^{-1}(h_1 \circ_H h_2) &= f^{-1}(f(g_1) \circ_H f(g_2)) \\
 &= f^{-1}(f(g_1 \circ_G g_2)) && (f \text{ ist ein Homomorphismus}) \\
 &= g_1 \circ_G g_2 && \text{(Eigenschaft der Umkehrabbildung)} \\
 &= f^{-1}(h_1) \circ_G f^{-1}(h_2)
 \end{aligned}$$

wie gewünscht.



#### Korollar 4.4 (Isomorphie von Gruppen ist Äquivalenzrelation)

Die Isomorphie von Gruppen ist eine Äquivalenzrelation.

*Beweis.* Isomorphie von Gruppen ist...

- ... reflexiv, denn jede Gruppe ist zu sich selbst isomorph ( $G \cong G$ ) mittels der Identität.
- ... symmetrisch wegen Satz 4.3 (2): Wenn  $G \cong H$  ist, dann gibt es einen Isomorphismus  $f : G \rightarrow H$ . Der referenzierte Satz gibt uns einen Isomorphismus  $H \rightarrow G$ , nämlich  $f^{-1}$ . Folglich ist auch  $H \cong G$ .
- ... transitiv wegen Satz 4.3 (1): Wenn  $G \cong H$  und  $H \cong K$  ist, dann gibt es Isomorphismen  $f : G \rightarrow H$  und  $f' : H \rightarrow K$ . Der referenzierte Satz gibt uns einen Isomorphismus  $G \rightarrow K$ , nämlich  $f' \circ f$ . Folglich ist auch  $G \cong K$ .

Damit sind alle Eigenschaften einer Äquivalenzrelation erfüllt. ♥

Damit können wir Beispiel 4.2 (2) sogar noch weiter verallgemeinern. Zyklische Gruppen sehen nämlich *alle* aus wie  $\mathbb{Z}$  oder  $\mathbb{Z}_n$ . Genauer gesagt definieren zyklische Gruppen für jede Anzahl von Elementen jeweils einen eigenen Isomorphietyp.

#### Satz 4.5 (Isomorphietyp zyklischer Gruppen)

Sei  $G$  eine zyklische Gruppe. Dann gilt eine der folgenden beiden Aussagen.

- ① Falls  $G$  unendlich viele Elemente besitzt, ist  $G$  isomorph zu  $\mathbb{Z}$ .
- ② Falls  $|G| = n$  für ein  $n \in \mathbb{N}$  gilt, ist  $G$  isomorph zu  $\mathbb{Z}_n$ .

*Beweis.*

**Zu ①.** Sei  $g \in G$  ein Erzeuger.

Weil  $G$  unendlich viele Elemente besitzt, gibt es kein  $k \in \mathbb{N}_0$  mit  $g^k = e$  abgesehen von  $k = 0$ . (Falls doch, wäre  $g^{x+k} = g^x$  für alle  $x \in \mathbb{Z}$ , und es gäbe höchstens  $k$  verschiedene Elemente.)

Betrachte den durch  $f(k) := g^k$  definierten Homomorphismus  $f : \mathbb{Z} \rightarrow G$  aus Beispiel 4.2 (1).

Weil  $G$  zyklisch ist, ist jedes  $y \in G$  von der Form  $y = g^x$  für ein  $x \in \mathbb{Z}$ . Also ist  $f$  surjektiv.

Genau dann gilt  $g^k = g^\ell$ , wenn  $g^{k-\ell} = e$ . Nach der anfänglichen Bemerkung ist dies äquivalent zu  $k - \ell = 0$ , also  $k = \ell$ . Damit ist  $f$  auch injektiv.

Insgesamt ist  $f$  bijektiv, also ein Isomorphismus.

**Zu ②.** Sei wieder  $g \in G$  ein Erzeuger. Wegen  $|G| = n$  ist  $G = \{e, g, g^2, \dots, g^{n-1}\}$ , wobei all diese Elemente paarweise verschieden sind, und es gilt  $g^n = e$  (siehe Satz 2.25).

Definiere  $f : \mathbb{Z}_n \rightarrow G$  durch  $f(\bar{k}) := \exp_g(k + n\mathbb{Z}) = g^k$ . Wegen

$$f(\bar{k} + \bar{\ell}) = f(\overline{k + \ell}) = g^{k+\ell} = g^k \circ g^\ell = f(\bar{k}) \circ f(\bar{\ell})$$

ist  $f$  ein Homomorphismus.

⋮



Offensichtlich definiert  $f$  eine 1-zu-1-Zuordnung zwischen den Restklassen  $\bar{0}, \bar{1}, \bar{2}, \dots, \overline{n-1}$  und den Gruppenelementen  $e, g, g^2, \dots, g^{n-1}$ . Damit ist  $f$  sogar ein Isomorphismus. (Die Umkehrabbildung ist der diskrete Logarithmus  $\log_g$ .) ♥

Wir wollen jetzt noch Eigenschaften von Homomorphismen beweisen, die ganz automatisch gelten und nur aus der definierenden Eigenschaft  $f(g_1 \circ_G g_2) = f(g_1) \circ_H f(g_2)$  folgen.

#### Satz 4.6 (*Eigenschaften von Homomorphismen*)

Sei  $f : G \rightarrow H$  ein Homomorphismus. Dann gilt...

- ① ...  $f(e_G) = e_H$ ,
- ② ...  $f(g^{-1}) = f(g)^{-1}$  für alle  $g \in G$ .

Mit anderen Worten bilden Homomorphismen neutrale auf neutrale und inverse auf inverse Elemente ab.

*Beweis.*

**Zu ①.** Aus  $f(e_G) = f(e_G \circ_G e_G) = f(e_G) \circ_H f(e_G)$  folgt nach Verknüpfung mit  $f(e_G)^{-1}$  von links (oder genauso gut von rechts), dass  $e_H = f(e_G)$  gilt.

**Zu ②.** Wir berechnen  $f(g) \circ_H f(g^{-1}) = f(g \circ_G g^{-1}) = f(e_G) = e_H$ . Das bedeutet, dass  $f(g^{-1})$  das zu  $f(g)$  inverse Element in  $H$  ist, also  $f(g^{-1}) = f(g)^{-1}$ . ♥

Wir definieren die folgenden interessanten Teilmengen zu einem Homomorphismus.

#### Definition 4.7 (*Kern und Bild*)

Sei  $f : G \rightarrow H$  ein Homomorphismus.

- ① Der **Kern** von  $f$  ist die Menge  $\ker(f) := \{g \in G \mid f(g) = e_H\} \subset G$  (steht für "kernel").
- ② Das **Bild** von  $f$  ist die Menge  $\text{im}(f) := \{f(g) \mid g \in G\} \subset H$  (steht für "image").

Diese Mengen sind deswegen interessant, weil es sich jeweils um eine Untergruppe handelt.

#### Satz 4.8 (*Kern und Bild sind Untergruppen*)

Sei  $f : G \rightarrow H$  ein Homomorphismus. Dann gilt...

- ① ...  $\ker(f) \leq G$ ,
- ② ...  $\text{im}(f) \leq H$ .

*Beweis.* Wir benutzen jeweils das Untergruppenkriterium sowie Satz 4.6.

**Zu ①.** Seien  $g_1, g_2 \in \ker(f)$ . Dann gilt  $f(g_1) = f(g_2) = e_H$ . Daraus folgt  $f(g_1 \circ_G g_2^{-1}) = f(g_1) \circ_H f(g_2)^{-1} = e_H \circ_H e_H^{-1} = e_H$ , also  $g_1 \circ_G g_2^{-1} \in \ker(f)$ .

**Zu ②.** Seien  $h_1, h_2 \in \text{im}(f)$ . Dann gilt  $h_1 = f(g_1)$  und  $h_2 = f(g_2)$  für gewisse  $g_1, g_2 \in G$ . Daraus folgt  $h_1 \circ_H h_2^{-1} = f(g_1) \circ_H f(g_2)^{-1} = f(g_1 \circ_G g_2^{-1}) \in \text{im}(f)$ . ♥

Betrachten wir zunächst ein paar Beispiele.

### Beispiel 4.9 (*Beispiele für Kern und Bild*)

- ① Für  $a \in \mathbb{Z}$  beliebig betrachte  $f_a : \mathbb{Z} \rightarrow \mathbb{Z}$  definiert durch  $f_a(x) := ax$ . Dann ist...
  - ...  $f_0$  die Nullfunktion, also  $\ker(f_0) = \mathbb{Z}$  und  $\text{im}(f_0) = \{0\} = 0\mathbb{Z}$ ;
  - ...  $f_a$  für jedes  $a \neq 0$  injektiv, und es gilt  $\ker(f_a) = \{0\}$  sowie  $\text{im}(f_a) = a\mathbb{Z}$ .
- ② Betrachte  $f : \mathbb{R} \rightarrow \text{O}(\mathbb{R}^2)$  definiert durch  $f(\alpha) := d_\alpha$ .  
Dann ist  $\ker(f) = 360\mathbb{Z}$  und  $\text{im}(f) = \text{SO}(\mathbb{R}^2)$ .
- ③ Für eine beliebige Gruppe  $G$  und ein beliebiges  $g \in G$  betrachte  $f_g : \mathbb{Z} \rightarrow G$  definiert durch  $f_g(k) := g^k$ .

Das Bild von  $f$  ist die von  $g$  erzeugte Untergruppe,  $\text{im}(f_g) = \langle g \rangle$ .

Der Kern von  $f$  ist eine Untergruppe von  $\mathbb{Z}$ . Insbesondere ist  $\ker(f_g) = d\mathbb{Z}$  für ein  $d \in \mathbb{N}_0$ . Daraus folgt  $g^d = e$  bzw.  $g^{x+kd} = g^x$  für alle  $x, k \in \mathbb{Z}$  (und dieses  $d$  ist die *kleinste* "Periode"). Das bedeutet wiederum...

- ... im Falle  $|\langle g \rangle| = \infty$ , dass  $d = 0$ , also  $\ker(f_g) = \{0\}$ ;
- ... im Falle  $|\langle g \rangle| < \infty$ , dass  $d = |\langle g \rangle|$ , also  $\ker(f_g) = |\langle g \rangle| \mathbb{Z}$ .

Damit haben wir übrigens auch endlich **Satz 2.25** bewiesen. Denn wenn  $G$  zyklisch ist mit  $|G| = n < \infty$  und Erzeuger  $g \in G$ , dann ist  $G = \langle g \rangle = \{e, g, g^2, \dots, g^{n-1}\}$  (diese Elemente sind paarweise verschieden), und es gilt wirklich  $g^n = e$ .

Kern und Bild sind auch deswegen interessant, weil sie in direkter Beziehung mit Injektivität und Surjektivität stehen.

### Satz 4.10 (*Kern und Injektivität bzw. Bild und Surjektivität*)

Sei  $f : G \rightarrow H$  ein Homomorphismus.

- ① Genau dann gilt  $\ker(f) = \{e_G\}$ , wenn  $f$  injektiv ist.
- ② Genau dann gilt  $\text{im}(f) = H$ , wenn  $f$  surjektiv ist.

*Beweis.*

**Zu ①.** Sei zunächst  $f$  injektiv. Dann gilt für jedes  $g \neq e_G$  auch  $f(g) \neq f(e_G) = e_H$ . Also ist  $\ker(f) = \{e_G\}$ .

Gelte umgekehrt  $\ker(f) = \{e_G\}$ . Seien  $g_1, g_2 \in G$  mit  $f(g_1) = f(g_2)$ . Dann folgt durch Umstellen  $f(g_1 \circ_G g_2^{-1}) = e_H$ . Nach Voraussetzung bedeutet das  $g_1 \circ_G g_2^{-1} = e_G$ , also  $g_1 = g_2$ . Damit ist  $f$  injektiv.

**Zu ②.** Das folgt sofort aus den Definitionen von Bild und Surjektivität. ♥

Erinnern wir uns noch einmal an die (verallgemeinerte) symmetrische Gruppe  $\text{Sym}(G)$  der *bijektiven* Abbildungen  $G \rightarrow G$  (siehe **Definition 1.26**). In Wahrheit kann jede Gruppe  $G$  (mit beliebig abstrakter Verknüpfung) wie folgt als Untergruppe von  $\text{Sym}(G)$  interpretiert werden.

### Satz 4.11 (*Satz von Cayley*)

Sei  $G$  irgendeine Gruppe. Dann ist  $G$  isomorph zu einer Untergruppe von  $\text{Sym}(G)$ .

*Beweis.* Unser Ziel ist ein Isomorphismus zwischen  $G$  und einer Untergruppe von  $\text{Sym}(G)$ .

Bezeichne mit  $*$  die Verknüpfung auf  $G$  und mit  $\circ$  die Verknüpfung auf  $\text{Sym}(G)$  (und zwar die Hintereinanderausführung von Funktionen).

Wir betrachten für ein Element  $g \in G$  die zugehörige **Linksverknüpfung**, also die Abbildung  $\ell_g : G \rightarrow G$  mit  $\ell_g(a) := g * a$ . Diese ist bijektiv, denn die Umkehrabbildung ist  $\ell_{g^{-1}}$  (die Linksverknüpfung mit  $g^{-1}$ ). Insbesondere ist  $\ell_g \in \text{Sym}(G)$ .

Sei nun  $f : G \rightarrow \text{Sym}(G)$  definiert durch  $f(g) := \ell_g$ . Dann ist  $f \dots$

- ... ein Homomorphismus, denn  $f(g * g') = \ell_{g * g'} = \ell_g \circ \ell_{g'} = f(g) \circ f(g')$  wegen

$$\ell_{g * g'}(a) = (g * g') * a = g * (g' * a) = \ell_g(\ell_{g'}(a)) = (\ell_g \circ \ell_{g'})(a)$$

für alle  $a \in G$ .

- ... injektiv. Wir zeigen  $\ker(f) = \{e_G\}$  (siehe [Satz 4.10 \(1\)](#)). Gelte  $f(g) = \ell_g = \text{id}_G$ . Dann ist  $f(g)(a) = g * a = a = \text{id}_G(a)$  für alle  $a \in G$ , also zwangsläufig  $g = e_G$ .

Wenn  $f : G \rightarrow \text{Sym}(G)$  ein injektiver Homomorphismus ist, dann ist  $f : G \rightarrow \mathbf{im}(f)$  ein Isomorphismus (denn die Einschränkung des Bildes macht die Abbildung surjektiv).

Damit ist  $\mathbf{im}(f)$  eine Untergruppe von  $\text{Sym}(G)$ , die zu  $G$  isomorph ist. ♥

Dieses Resultat ist ein sehr schönes, denn wir können nun jede *abstrakte* Gruppe mit einer ganz *konkreten* Gruppe von Permutationen identifizieren. Dadurch ist es insbesondere möglich, die Theorie über Permutationsgruppen auf beliebige Gruppen anzuwenden.

### Der Homomorphiesatz

Zum krönenden Abschluss dieses Kurses wollen wir noch etwas tiefer in die abstrakte Algebra eintauchen und uns Antworten auf die folgenden Fragen überlegen:

- Unter welcher Bedingung an eine Untergruppe  $H \leq G$  erbt die Quotientenmenge  $G/H$  die Gruppenstruktur von  $G$ , wie es prototypisch bei  $\mathbb{Z}/m\mathbb{Z} = \mathbb{Z}_m$  der Fall war?
- Wie lautet die allgemeine Konstruktion, um Homomorphismen zu Isomorphismen zu machen? (Vergleiche die Abbildungen  $\alpha \mapsto d_\alpha$  bzw.  $[\alpha] \mapsto d_\alpha$  aus [Beispiel 4.2 \(5\)](#).)
- Wie hängen Kern und Bild einer Gruppe zusammen?

Antworten auf diese Fragen liefert der sogenannte **Homomorphiesatz**, auf den wir in den letzten Zügen dieses Kurses hinarbeiten werden.

### Definition 4.12 (*Konjugationsabbildung*)

Sei  $G$  eine Gruppe, und sei  $g \in G$  beliebig.

Die **Konjugation** mit  $g$  ist die Abbildung  $c_g : G \rightarrow G$  definiert durch  $c_g(a) := g \circ a \circ g^{-1}$ .

Die Konjugation mit  $g$  ist, wie man leicht nachrechnet, für jedes  $g \in G$  ein Isomorphismus zwischen  $G$  und sich selbst (ein sogenannter **Automorphismus**). Folglich ist  $c_g(H) = \{g \circ h \circ g^{-1} \mid h \in H\}$  für jede Untergruppe  $H \leq G$  selbst wieder eine Untergruppe, und es gilt  $c_g(H) \cong H$ .

Wir interessieren uns im Folgenden für diejenigen Untergruppen von  $G$ , die von der Konjugation mit  $g$  in sich selbst überführt — man sagt auch **invariant gelassen** — werden.

#### Definition 4.13 (Normalteiler)

Sei  $G$  eine Gruppe, und sei  $K \leq G$  eine Untergruppe.

Falls  $c_g(k) \in K$  für alle  $k \in K$  und alle  $g \in G$  gilt, dann heißt  $K$  ein **Normalteiler** von  $G$ .

Wir schreiben dann auch  $K \trianglelefteq G$ .

Insbesondere gilt für Normalteiler  $K \trianglelefteq G$  nicht nur  $c_g(K) \cong K$ , sondern wegen  $c_g(K) \subset K$  (gemäß der Definition) sogar  $c_g(K) = K$ , also echte Gleichheit (und nicht nur Isomorphie).

Wie man leicht nachrechnet, ist jeder Kern eines Homomorphismus automatisch ein Normalteiler der Startgruppe.

#### Satz 4.14 (Kerne sind Normalteiler)

Sei  $f : G \rightarrow H$  ein Homomorphismus.

Dann ist  $\ker(f) \trianglelefteq G$ .

*Beweis.* Wir wollen  $c_g(a) \in \ker(f)$  für jedes  $a \in \ker(f)$  und jedes  $g \in G$  nachrechnen.

Sei also  $a \in \ker(f)$ ; das heißt,  $f(a) = e_H$ . Dann gilt für jedes  $g \in G$

$$f(c_g(a)) = f(g \circ_G a \circ_G g^{-1}) = f(g) \circ_H \underbrace{f(a)}_{=e_H} \circ_H f(g^{-1}) = f(g \circ_G g^{-1}) = f(e_G) = e_H,$$

also  $c_g(a) \in \ker(f)$ . ♥

Spannender ist jedoch die folgende Aussage: Umgekehrt ist auch jeder Normalteiler der Kern eines Gruppenhomomorphismus!

Wir erinnern uns dafür an den **Satz von Lagrange** zurück. Genauer erinnern wir uns an die für dessen Beweis in **Lemma 2.15** eingeführte Äquivalenzrelation

$$a \sim b \iff \text{es gibt ein } h \in H \text{ mit } b = a \circ_G h \iff a^{-1} \circ_G b \in H$$

zurück, mittels der wir die Quotientenmenge  $G/H = \{a \circ_G H \mid a \in G\}$  der Linksnebenklassen eingeführt hatten.

Für  $G := \mathbb{Z}$  und  $H := m\mathbb{Z}$ , also  $G/H = \mathbb{Z}_m$ , haben wir in **Definition 3.2** unter anderem die von  $\mathbb{Z}$  geerbte Addition

$$[a] +_{\mathbb{Z}/m\mathbb{Z}} [b] := [a +_{\mathbb{Z}} b]$$

definiert. Wie sich herausstellt, ist diese Konstruktion immer dann möglich (die Verknüpfung auf  $G/H$  also korrekt definiert), wenn die herausgeteilte Untergruppe  $H$  ein Normalteiler von  $G$  ist.

### Satz 4.15 (Quotientengruppe)

Sei  $G$  eine Gruppe, und sei  $K \trianglelefteq G$  ein Normalteiler von  $G$ . Dann gilt:

- ① Die Menge  $G/K$  der Linksnebenklassen erbt von  $G$  auf natürliche Weise eine Gruppenstruktur mittels  $[a] \circ_{G/K} [b] := [a \circ_G b]$ .

Wir nennen  $G/K$  die **Quotientengruppe** von  $G$  und  $K$ .

- ② Die **Projektionsabbildung**  $\pi : G \rightarrow G/K$ , definiert durch  $\pi(a) := [a]$ , ist ein surjektiver Homomorphismus, und es gilt  $\ker(\pi) = K$ .

*Beweis.*

**Zu ①.** Wir müssen zeigen, dass die Definition  $[a] \circ_{G/K} [b] := [a \circ_G b]$  nicht von den gewählten Repräsentanten abhängt (wie beim Beweis der Korrektheit von Definition 3.2).

Genau dann gilt  $a \sim b$ , wenn es ein  $k \in K$  mit  $b = a \circ_G k$  gibt. Umgestellt bedeutet das genau  $a^{-1} \circ_G b \in K$ .

Wir müssen zeigen: Wenn  $[a_1] = [a_2]$  und  $[b_1] = [b_2]$  gilt, dann gilt auch  $[a_1] \circ_{G/K} [b_1] = [a_2] \circ_{G/K} [b_2]$ , also  $[a_1 \circ_G b_1] = [a_2 \circ_G b_2]$ .

Es gelte also  $a_1 \sim a_2$  und  $b_1 \sim b_2$ ; das heißt,  $a_1^{-1} \circ_G a_2 \in K$  bzw.  $b_1^{-1} \circ_G b_2 \in K$ .

Wir berechnen (und lassen dabei  $\circ_G$  der Lesbarkeit halber weg)

$$(a_1 b_1)^{-1} a_2 b_2 = b_1^{-1} \underbrace{a_1^{-1} a_2}_{\in K} b_2 \in b_1^{-1} K b_2 = b_1^{-1} K (b_1 b_1^{-1}) b_2 = \underbrace{(b_1^{-1} K b_1)}_{=K} \underbrace{(b_1^{-1} b_2)}_{\in K} = K.$$

Dabei gilt  $c_{b_1^{-1}}(K) = b_1^{-1} K b_1 = K$ , weil nach Voraussetzung  $K \trianglelefteq G$  ist.

Diese Rechnung zeigt  $a_1 \circ_G b_1 \sim a_2 \circ_G b_2$ , also ist  $[a] \circ_{G/K} [b]$  wirklich korrekt definiert!

Dass  $\circ_{G/K}$  eine Gruppenstruktur auf  $G/K$  definiert, folgt sofort daraus, dass  $\circ_G$  eine Gruppenstruktur auf  $G$  ist, und wir das Produkt der Repräsentanten (in  $G/K$ ) als den Repräsentanten des Produkts (in  $G$ ) definiert haben.

Das neutrale Element ist  $e_{G/K} = [e_G] = e_G \circ_G K = K$ .

**Zu ②.** Die Projektionsabbildung  $\pi : G \rightarrow G/K$ , definiert durch  $\pi(a) := [a]$ , ist offensichtlich surjektiv. Sie ist per Konstruktion ein Homomorphismus, denn es gilt

$$\pi(a \circ_G b) = [a \circ_G b] = [a] \circ_{G/K} [b] = \pi(a) \circ_{G/K} \pi(b).$$

Es gilt  $\ker(\pi) = \{k \in K \mid \pi(k) = e_{G/K}\} = \{k \in K \mid [k] = K\} = K$  wie behauptet. ♥

Das führt uns schon zur Formulierung des Homomorphiesatzes.

### Satz 4.16 (Homomorphiesatz)

Seien  $G$  und  $H$  zwei Gruppen, und sei  $f : G \rightarrow H$  ein Homomorphismus.

Sei darüber hinaus  $K \trianglelefteq G$  ein Normalteiler von  $G$ , und bezeichne mit  $\pi : G \rightarrow G/K$  die Projektion auf die Quotientengruppe (wie im vorigen Satz).

⋮

Dann gilt sind die folgenden Aussagen äquivalent:

- ①  $K \subset \ker(f)$
- ② Es gibt genau einen Homomorphismus  $f' : G/K \rightarrow H$  mit  $f = f' \circ \pi$ .

Gleichbedeutend mit dieser Aussage ist, dass das folgende Diagramm **kommutiert** (es also keine Rolle spielt, entlang welcher Pfeile man sich bewegt).

$$\begin{array}{ccc} G & \xrightarrow{f} & H \\ \pi \downarrow & \nearrow \exists! f' & \\ G/K & & \end{array}$$

Man sagt auch,  $f : G \rightarrow H$  **induziert** eine eindeutige Abbildung  $f' : G/K \rightarrow H$ .

*Beweis.*

“ $\implies$ ”: Gelte zunächst  $K \subset \ker(f)$ . Dann ist  $f' : G/K \rightarrow H$  durch

$$f'([a]) := f(a)$$

korrekt definiert. Denn wenn  $a_1 \sim a_2$  ist, gilt  $a_1^{-1} \circ_G a_2 \in K \subset \ker(f)$ , also  $f(a_1^{-1} \circ_G a_2) = e_H$ . Daraus folgt

$$f'([a_2]) = f(a_2) = f(a_1 \circ_G a_1^{-1} \circ_G a_2) = f(a_1) \circ_H f(a_1^{-1} \circ_G a_2) = f(a_1) = f'([a_1]),$$

was die Unabhängigkeit von der Wahl des Repräsentanten zeigt.

Diese Abbildung ist ein Homomorphismus, denn es gilt

$$f'([a] \circ_{G/K} [b]) = f'([a \circ_G b]) = f(a \circ_G b) = f(a) \circ_H f(b).$$

Per Konstruktion ist  $f(a) = f'([a]) = f'(\pi(a)) = (f' \circ \pi)(a)$ , also  $f = f' \circ \pi$ .

Die Eindeutigkeit von  $f'$  folgt daraus, dass  $\pi$  surjektiv ist. (Aus  $f' \circ \pi = f = f'' \circ \pi$  folgt  $f' = f''$  zum Beispiel per Anwendung der Rechtsinversen  $\pi^{-1}$ , siehe **Bemerkung 1.25**.)

“ $\impliedby$ ”: Es gebe nun umgekehrt solch einen Homomorphismus  $f'$ .

Sei  $k \in K$ . Dann ist  $\pi(k) = K = e_{G/K}$ , also  $f(k) = f'(\pi(k)) = f'(e_{G/K}) = e_H$ . Das bedeutet  $k \in \ker(f)$ , also  $K \subset \ker(f)$ . ♥

Wir können auch eine Aussage darüber treffen, wann  $f'$  injektiv ist.

#### Satz 4.17 (Addendum zum Homomorphiesatz)

Seien  $f : G \rightarrow H$  und  $f' : G/K \rightarrow H$  genau wie im vorigen Satz. Dann gilt:

Genau dann ist  $f'$  injektiv, wenn  $K = \ker(f)$  ist.

*Beweis.*

“ $\implies$ ”: Sei  $f'$  injektiv. Sei  $k \in \ker(f)$ . Wir berechnen

$$f'(K) = f'(e_{G/K}) = e_H = f(k) = f'(\pi(k)) = f'(k \circ_G K),$$

also  $K = k \circ_G K$ . Dann ist  $k \in K$ , also  $\ker(f) \subset K$ . Weil nach Voraussetzung des Homomorphiesatzes auch umgekehrt  $K \subset \ker(f)$  gilt, folgt insgesamt  $K = \ker(f)$  wie behauptet.

“ $\Leftarrow$ ”: Gelte umgekehrt  $K = \ker(f)$ . Gelte  $f'(a \circ_G K) = f'(b \circ_G K)$ , also  $f'(\pi(a)) = f'(\pi(b))$ , also  $f(a) = f(b)$ . Daraus folgt

$$f(a^{-1} \circ_G b) = f(a)^{-1} \circ_H f(b) = e_H,$$

also  $a^{-1} \circ_G b \in \ker(f) = K$ . Das bedeutet  $a \circ_G K = b \circ_G K$ , also ist  $f'$  injektiv. ♥

Den gloriosen Abschluss liefert das folgende Korollar, das Kern und Bild miteinander verbindet.

#### Korollar 4.18 (Erster Isomorphiesatz)

Sei  $f : G \rightarrow H$  ein Homomorphismus.

Dann gilt  $G/\ker(f) \cong \text{im}(f)$ .

*Beweis.*

Wegen  $K = \ker(f)$  ist  $f' : G/\ker(f) \rightarrow H$  injektiv.

Dann ist  $f' : G/\ker(f) \rightarrow \text{im}(f')$  bijektiv, also ein Isomorphismus.

Wegen  $f = f' \circ \pi$  ist insbesondere  $\text{im}(f) = \text{im}(f')$ , also folgt  $G/\ker(f) \cong \text{im}(f)$ . ♥

#### Beispiel 4.19 (Anwendungen des ersten Isomorphiesatzes)

- ① Betrachte (erneut)  $G := \mathbb{R}$ ,  $H := \text{O}(\mathbb{R}^2)$ , und  $f : G \rightarrow H$  gegeben durch  $f(\alpha) := d_\alpha$ .

Dann gilt  $\ker(f) = 360\mathbb{Z}$  und  $\text{im}(f) = \text{SO}(\mathbb{R}^2)$ , also  $\mathbb{R}/360\mathbb{Z} \cong \text{SO}(\mathbb{R}^2)$  mittels des durch  $f'([\alpha]) = f(\alpha) = d_\alpha$  gegebenen Isomorphismus (vergleiche [Beispiel 4.2 \(5\)](#)).

- ② Sei  $n$  ein Teiler von  $m$ . Betrachte  $G := n\mathbb{Z}$ ,  $H := \mathbb{Z}_{m/n}$ , und  $f : G \rightarrow H$  gegeben durch  $f(nx) := \bar{x}$ . (Dies ist offensichtlich ein Homomorphismus.)

Genau dann ist  $f(nx) = \bar{x} = \bar{0} \in \mathbb{Z}_{m/n}$ , wenn  $x$  ein Vielfaches von  $m/n$  ist, also  $nx$  ein Vielfaches von  $m$ . Das bedeutet  $\ker(f) = m\mathbb{Z}$ .

Aus dem ersten Isomorphiesatz folgt, weil  $f$  surjektiv ist,  $n\mathbb{Z}/m\mathbb{Z} \cong \mathbb{Z}_{m/n}$ . (Für  $n = 1$  steht dort einfach nur, dass  $\mathbb{Z}_m$  isomorph zu sich selbst ist.)

- ③ Betrachte  $G := \mathbb{R}^* := \mathbb{R} \setminus \{0\}$  und  $H := \mathbb{R}_{>0}$  (jeweils mit der Multiplikation), sowie  $f : \mathbb{R}^* \rightarrow \mathbb{R}_{>0}$  gegeben durch  $f(x) := |x|$ .

Dies ist ein Homomorphismus, denn  $f(xy) = |xy| = |x||y| = f(x)f(y)$  (Eigenschaft des Betrags), und es ist  $\ker(f) = \{\pm 1\} \cong \mathbb{Z}_2$ .

Aus dem ersten Isomorphiesatz folgt, weil  $f$  surjektiv ist,  $\mathbb{R}^*/\{\pm 1\} \cong \mathbb{R}_{>0}$ .

Ende 😊