

①

18.12.

$$\begin{aligned}\mathbb{Z}_m &= \{[a]_m : a \in \mathbb{Z}\} \\ &= \{[0]_m, \dots, [m-1]_m\}.\end{aligned}$$

$$[a]_m + [b]_m = [a+b]_m$$

$$[a]_m \cdot [b]_m = [a \cdot b]_m$$

Wann ex.  $b \in \mathbb{Z}$  mit

$$[a]_m \cdot [b]_m = [1]_m ?$$

Sei ein  $b$  ex. genau dann,  
wenn  $\text{ggT}(a, m) = 1$ .

Dann heißt  $[a]_m$  in  $\mathbb{Z}_m$  invertierbar.

Für alle  $a, b \in \mathbb{Z}$  ex.  $\lambda, \mu \in \mathbb{Z}$   
mit  $\text{ggT}(a, b) = \overset{N}{\lambda} a + \mu b$ .

Insbesondere: Sei  $\text{ggT}(a, m) = 1$

$\Rightarrow$  ex.  $\lambda, \mu$  mit  $1 = \lambda a + \mu m$   
 $[\lambda]_m$  ist das Inverse von  $[a]_m$   
in  $\mathbb{Z}_m$ .

$\varphi(n)$  (phi von  $n$ ) ist die  
Eulersche  $\varphi$ -Funktion. ②

Beispiel:  $n = 10$

Zu 10 teilerfremd sind:

1, 3, 7, 9.

$$\Rightarrow \varphi(10) = 4.$$

$$\varphi(p \cdot q) = \varphi(p) \cdot \varphi(q).$$

In Teil d) des Beispiels ist  $p \neq q$  gemeint.

( $\leq$ )

Vielfache von  $p$  unterhalb von  $p \cdot q$ :

$p, p \cdot 2, \dots, p \cdot (q-1), p \cdot q$

Dies sind  $q$  Stück.

Vielfache von  $q \leq p \cdot q$ :

$1 \cdot q, 2 \cdot q, \dots, p \cdot q$ .

$\Rightarrow$  es gibt  $p+q-1$  Zahlen  $\leq p \cdot q$ ,  
die durch  $p$  oder  $q$  teilbar sind.

Teilerfremd zu  $p \cdot q$ :

$$p \cdot q - p - q + 1$$

$$(p-1)(q-1) = p \cdot q - p - q + 1$$

Beispiel:  $p = 3$ ,  $q = 5$

(3)

$$n = p \cdot q = 15.$$

↪ Zahlen  $\leq 15$ , die von 3 geteilt werden:

$$3, 6, 9, 12, 15$$

Zahlen  $\leq 15$ , die von 5 geteilt werden:

$$5, 10, 15.$$

Insgesamt gibt es  $5 + 3 - 1 = 7$  nat. Zahlen  $\leq 15$ , die nicht zu 15 teilerfremd sind.

→ Teilerfremd sind 8. Das sind:

$$1, 2, 4, 7, 8, 11, 13, 14.$$

## Beweis von Fermat-Euler:

(4)

Seien  $r_1, r_2, \dots, r_{\varphi(m)}$  die nat. Z.  $\leq m$ , die zu  $m$  teilerfremd sind.  
Betrachten die Restklassen

$$[r_1 \cdot n]_m, [r_2 \cdot n]_m, \dots, [r_{\varphi(m)} \cdot n]_m.$$

Beh: Diese  $\varphi(m)$  Restklassen sind paarweise verschieden.

Ang.  $[r_i \cdot n]_m = [r_j \cdot n]_m. (*)$

Es gibt  $[b]_m \in \mathbb{Z}_m$  mit  $[n]_m \cdot [b]_m = [i]_m$ , da  $\text{ggT}(n, m) = 1$ .

Multipliziere (\*) mit  $[n]_m$ .

$$[r_i \cdot n]_m \cdot [b]_m = [r_j \cdot n]_m \cdot [b]_m$$

$$[r_i]_m \cdot [n \cdot b]_m = [r_j]_m \cdot [n \cdot b]_m$$

$$[r_i]_m = [r_j]_m$$

$$\rightarrow r_i = r_j \Rightarrow i = j.$$

Fortsetzung vom Hauptbeweis:

Seien  $[a]_m, [b]_m$  in  $\mathbb{Z}_m$  inv. bar.

Dann ist auch  $[a \cdot b]_m$  inv. bar.

Sei  $[c]_m$  invers zu  $[a]_m$ ,

$[d]_m$  invers zu  $[b]_m$ .

$$\textcircled{5} \quad \text{Dann ist } [a \cdot b \cdot c \cdot d]_m = [a \cdot c]_m \cdot [b \cdot d]_m \\ = [1]_m \cdot [1]_m = [1]_m.$$

Also ist  $[c \cdot d]_m$  das Inverse von  $[a \cdot b]_m$ .

$\Rightarrow [r_1 \cdot n]_m, [r_2 \cdot n]_m, \dots, [r_{\varphi(m)} \cdot n]_m$  sind invertierbar in  $\mathbb{Z}_m$ .

$$\Rightarrow \{[r_1]_m, \dots, [r_{\varphi(m)}]_m\} = \{[r_1 \cdot n]_m, \dots, [r_{\varphi(m)} \cdot n]_m\}$$

$$\Rightarrow [r_1 \cdot r_2 \cdot \dots \cdot r_{\varphi(m)}]_m = [(r_1 \cdot n) \cdot \dots \cdot (r_{\varphi(m)} \cdot n)]_m.$$

$$[r_1 \cdot r_2 \cdot \dots \cdot r_{\varphi(m)}]_m = [r_1 \cdot r_2 \cdot \dots \cdot r_{\varphi(m)}]_m \cdot [n^{\varphi(m)}]_m$$

$[r_1 \cdot r_2 \cdot \dots \cdot r_{\varphi(m)}]_m$  ist inv. bar in  $\mathbb{Z}_m$ .  $\Rightarrow$  K鰊nen durch  $[r_1 \cdot \dots \cdot r_{\varphi(m)}]_m$  teilen.

$$\Rightarrow [1]_m = [n^{\varphi(m)}]_m$$

$$\Rightarrow n^{\varphi(m)} \equiv 1 \pmod{m}. \quad \square$$

$[k]_m = [m^d]_N$  ist die verschlüsselte Nachricht,  $[k^e]_m$  die entschl. Nachricht.

$$\varphi = \phi$$

$$\begin{aligned}[7^16]_{143} &= \left[ ((7^2)^2)^2 \right]_{143} \quad (6) \\ &= \left[ ((49^2))^2 \right]_{143} = \left[ (2401^2) \right]_{143} \\ &= \left[ (\underbrace{\qquad}_\text{Zahl zwischen 0 und 143})^2 \right]_{143}\end{aligned}$$

Zahl zwischen 0 und 143.

$(\mathbb{N}, +, \cdot)$  ist eine algebraische Struktur.

Beispiele für 2-stellige Operationen:

$+, \cdot, \wedge, \vee, \cap, \cup, \dots$

Beispiele für 1-stellige Operationen:

$n \mapsto n'$  (Nachfolger)

$\sin$ ,

$\cdot(-1): \mathbb{R} \rightarrow \mathbb{R}; x \mapsto -x$ .

Beispiele für 0-stellige Operationen:

$f: M^0 \mapsto M$

$M^0 =$  Menge der Tupel von Elementen von  $M$  mit Länge 0.

$\emptyset$  ist das einzige Tupel der Länge 0.

$M^0 = \{\emptyset\}$ .

$f: M^0 \rightarrow M$  ist eindeutig durch  $f(\emptyset)$  bestimmt.

$f(\emptyset)$  ist irgendein Element von  $M$ .

0-stellige Operationen sind Konstanten in  $M$ .

②

$$f: A \rightarrow B, g: B \rightarrow C$$

$$gof: A \rightarrow C; x \mapsto g(f(x))$$

$$A = B = C$$

Satz: Sei  $f: A \rightarrow B, g: B \rightarrow C$ , beide bijektiv. Dann ist auch  $gof$  bijektiv.

Beweis: Injektivität: Seien  $a, a' \in A$  mit  $a \neq a'$ . Dann ist  $f(a) \neq f(a')$ . Also ist  $g(f(a)) \neq g(f(a'))$ , d.h.

$$(gof)(a) \neq (gof)(a') \Rightarrow gof \text{ ist inj.}$$

Surjektivität: Sei  $c \in C$ .

Dann ex. ein  $b \in B$  mit  $g(b) = c$ .

Dann ex. ein  $a \in A$  mit  $b = f(a)$ ,

Also ist  $(gof)(a) = g(f(a)) = g(b) = c$ .

$$(f \circ \text{id}_A)(x) = f(\text{id}_A(x)) = f(x)$$

$$\rightarrow f \circ \text{id}_A = f$$

$$(\text{id}_A \circ f)(x) = \text{id}_A(f(x)) = f(x)$$

$$\rightarrow \text{id}_A \circ f = f.$$

(3)

### Beweis von Lemma 7.5:

Angenommen,  $e$  und  $e'$  sind beide neutral. Dann gilt:

$$e = e * e' = e'. \quad \square$$

Bemerkung: Ist  $b$  zu  $a$  invers, so ist auch  $a$  zu  $b$  invers.

Sind  $a, b$  invertierbar, so ist auch  $a * b$  inv. bar, falls  $*$  das Assoz. Gesetz erfüllt.

Sei nämlich  $c$  zu  $a$  invers und  $d$  zu  $b$ . Dann gilt:

$$\begin{aligned} (a * b) * (d * c) &= (a * (b * d)) * c \\ &= (a * e) * c = a * c = c \\ (d * c) * (a * b) &= e \end{aligned}$$

$\Rightarrow d * c$  ist zu  $a * b$  invers.

$$((a * b)^{-1} = b^{-1} * a^{-1}).$$

$v = \text{Mathe}$ ,  $w = \text{klausur}$

$v \cap w = \text{Matheklausur}$ ,

$\lambda$ : das leere Wort. (Wort der Länge 0)

$$(a, \dots a_n \sim b, \dots b_m) \sim c_1, \dots c_k$$

$$= a, \dots a_n b, \dots b_m c_1, \dots c_k$$

$$= a, \dots a_n \sim (b, \dots b_m \sim c_1, \dots c_k)$$

$\Rightarrow (A^*, \sim)$  ist Halbgruppe.

$(\mathbb{Z}_m \setminus \{[0]_m\}, \cdot)$  ist unter Umständen kein Monoid!

Beispiel:  $m = 15$ .

$$[3]_{15} \cdot [5]_{15} = [15]_{15} = [0]_{15}.$$

$\Rightarrow \cdot$  ist keine 2-stellige Operation auf  $\mathbb{Z}_{15} \setminus \{[0]_{15}\}$ !

Sei  $f: A \rightarrow A$  Bijektion.

$f^{-1}: A \rightarrow A$  ist so definiert, dass für jedes  $a \in A$  und  $b \in A$  gilt:

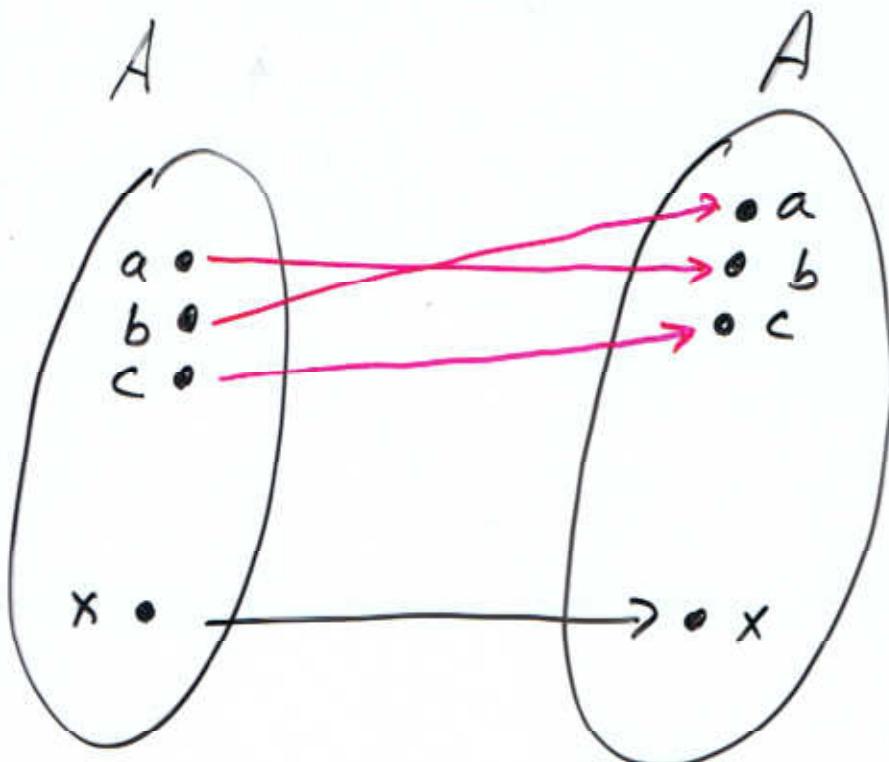
ist  $f(a) = b$ , so ist  $f^{-1}(b) = a$ ,

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

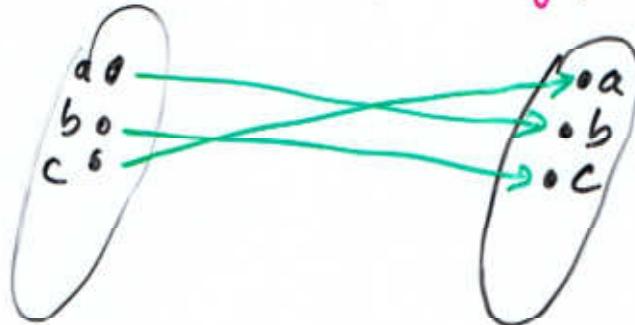
$$\Rightarrow f^{-1} \circ f = id_A.$$

$$\text{Ähnlich: } f \circ f^{-1} = id_A.$$

5



Rote Funktion ist  $f$ .

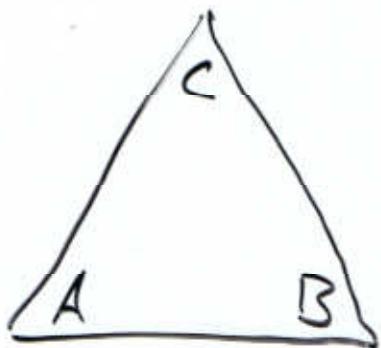


Grüne Funktion:  $g$ .

Um zu zeigen, dass  $(\mathbb{Z}_m^*, \cdot)$  eine Gruppe ist, müssen wir zeigen,

1. • ist 2-stellige Operation auf  $\mathbb{Z}_m^*$ , d.h., f.z.  $a, b \in \mathbb{Z}_m^*$  ist  $a \cdot b \in \mathbb{Z}_m^*$
2. • ist assoziativ
3. ex. ein neutrales Element ( $[1]_m$ )
4. ex. Inverse in  $\mathbb{Z}_m^*$ .

Erlaubte Transformationen: ⑥  
Spiegelungen, Drehungen, Translationen



$$\text{id}_{\mathbb{R}^2}: \begin{aligned} A &\mapsto A \\ B &\mapsto B \\ C &\mapsto C \end{aligned} \quad \begin{pmatrix} A & B & C \\ A & B & C \end{pmatrix}$$

Drehung um  $120^\circ$ :

$$\begin{aligned} A &\mapsto B \\ B &\mapsto C \\ C &\mapsto A \end{aligned} \quad \begin{pmatrix} A & B & C \\ B & C & A \end{pmatrix}$$

---

Beispiel in  $\mathbb{R}_\Delta$ :

$$r^2 = s$$

$$s^2 = r$$

$x \circ r$  entspricht der Permutation

$$\begin{pmatrix} A & B & C \\ A & C & B \end{pmatrix}. \quad \text{Damit gilt } x \circ r = y$$

Wichtig: Die Komposition von je zweien dieser Transformationen ist wieder eine der sechs Transformationen.

D

## Beweis von Lemma 7.13

a)  $ab = ac$ .

Multipliziere diese Gleichung von links mit  $a^{-1}$ .

$$a^{-1}ab = a^{-1}ac$$

$$e b = e c$$

$$b = c$$

$$ba = ca$$

Multipliziere von rechts mit  $a^{-1}$ .

$$baa^{-1} = caa^{-1}$$

$$b e = c e$$

$$b = c.$$

b)  $ax = b$ . Multipliziere von links mit  $a^{-1}$ .

$$x = a^{-1}b$$

Probe:  $a, a^{-1}b = eb = b$ .

Analog:  $xa = b$

$$x = ba^{-1}, \square$$