Äquivalenzrelation: reflexiv, symmetrisch, transitiv

R_n = "Rest beim Teilen durch n"

z.B. $2 R_5 7$ → Äquivalenzklassen:

$\bar{2} = \{2, 7, 12, 17, 22, -3, -8, -13, \dots\}$

$-3 = (-1) \cdot 5 + 2$

$2, 7, \quad 7-2 = 5 \quad 12-2 = 10$

$22-7 = 15$

$7 \equiv 2 \mod 5$ $\quad 12 \equiv 7 \mod 5$ "$\equiv$" = "ist kongruent"

$\bar{7} = \bar{2} = \overline{12}$ $\quad \{\bar{0}, \bar{1}, \dots, \bar{4}\}$

$16 \equiv 1 \mod 5$ $\quad 10 \equiv 17 \mod 7$

Beispiele zum Rechnen mit Restklassen:

- $\mathbb{Z}/7\mathbb{Z} = \{\bar{0}, \bar{1}, \bar{2}, \dots, \bar{6}\}$

  $\bar{5} \oplus \bar{6} = \overline{(5+6) \mod 7} = \overline{11 \mod 7} = \bar{4}$

  $\bar{5} \odot \bar{6} = \overline{30 \mod 7} = \bar{2}$

- Rechnen mit Uhrzeiten: $\mathbb{Z}/12\mathbb{Z}$

  $\bar{4} \oplus \bar{9} = \overline{13} = \bar{1}$

- in $\mathbb{Z}/8\mathbb{Z}$: $\bar{7} \odot (\bar{2} \oplus \bar{6}) = \bar{7} \odot \bar{8} = \bar{7} \odot \bar{0} = \overline{7 \cdot 0} = \bar{0}$.

- in $\mathbb{Z}/10\mathbb{Z}$: $\bar{7} \odot (\bar{2} \oplus \bar{6}) = \bar{7} \odot \bar{8} = \overline{56} = \bar{6}$.

  $\bar{7} \odot (\bar{4} \oplus \bar{6}) = \bar{7} \odot \bar{0} = \bar{0}$.

- in $\mathbb{Z}/13\mathbb{Z}$: $(\overline{12})^{1000} = (\overline{-1})^{1000} = \overline{(-1)^{1000}} = \bar{1}$

Hashing: 10 Personen

A: 10 B: 20 C: 30 D: 2 E: 12
F: 23 G: 18 H: 40

modulo 10:

0	1	2	3	4	5	6	7	8	9
A	B	C	D	E	F			G	

Lineare Sondierung

0	1	2	3	4	5	6	7	8	9
A	B	D	E	F		H		G	C

B: eigentlich auf 0 $\xrightarrow{+1^2}$ 1 ← Schritt 1
C: eigentlich auf 0, $\xrightarrow{-1^2}$ ← Schritt 2 = 2·1
H: ~~eigent~~ ~~Schritt 3~~

$+1 = 1$: schon belegt
$-1^2 = 9$: — " —
$+2^2 = 4$: — " —
$-2^2 = 6$: ✓

modulo 13: A: 10, B: 20, C: 30, D: 2, E: 12
F: 23, G: 24, H: 40

0	1	2	3	4	5	6	7	8	9	10	11	12
	G	D		C			B			A	F	E
		3.6.					4.5.			2.	0.	1.

Hashing mit quadrat. Sondierung mod 13

p: Primzahl $\quad p \neq 2$

$p \bmod 4 \in \{\bar{1}, \bar{3}\}$

Gruppe $\begin{cases} \mathbb{Z}: & + : \underline{\text{Addition}}, \underline{\text{neutrales Element}}: 0;\ a+0=a \\ & \underline{\text{inverses Element}} \text{ bzgl. } + \\ & a+(-a)=0. \end{cases}$

Gruppe $\begin{cases} \mathbb{Q}: & + \text{ Addition, neutrales Element } 0 \\ & \text{inverses } -a. \end{cases}$

Ring $\begin{cases} \mathbb{Z}: & (+ \text{ Addition mit } 0 \text{ und Inversem}) \\ \text{und } \mathbb{Z}: & (\cdot \text{ Multiplikation}) \ \underline{\text{neutrales Element}} \text{ bzgl. Mult.: } 1 \\ & \text{kein Inverses bzgl } \cdot \ (\text{z.B. gibt es keine ganze Zahl } z, \text{ s.d. } 2 \cdot z = 1) \end{cases}$

Körper $\begin{cases} \mathbb{Q}: & (+ \text{ Addition, neutr. Element bzgl } +: 0, \\ & \text{Inverse El. bzgl } +: -a) \\ \mathbb{Q}\setminus 0: & (\cdot \text{ Multiplikation, neutrales Element: } 1 \\ & \text{inverses El. von } \frac{p}{q} \in \mathbb{Q}: \frac{q}{p} \ (\text{für } pq \neq 0)) \end{cases}$

$\mathbb{R}$: Körper

$\mathbb{C}$: -"- der komplexen Zahlen

+ evtl. Kommutativgesetz, Distributivgesetz, Assoziativitätsgesetz.

$r: M \times M \to M, \quad (x,y) \longmapsto x \, r \, y$

↑ Verknüpfung

$r(x,y) = x \, r \, y$

$+ \quad \cdot \quad \oplus \quad \odot \quad * \quad \circ$

$f: M \to N \qquad g: N \to S \qquad g \circ f: M \to S$

$id: N \to N$

$n \longmapsto n$

$id \circ f = f$

neutrales Element.

$(\mathbb{Z}, +)$: Gruppe:

+ Verknüpfung

0 neutrales El.

inv. Element von einem beliebigen $z \in \mathbb{Z}$: $-z \in \mathbb{Z}$

und Assoz. gesetz: für $a, b, c \in \mathbb{Z}$ gilt:

$(a+b)+c = a+(b+c)$.

$2+3 = 3+2$. : Kommutativität

da

bzw. gilt: $a+b = b+a \quad \forall a, b \in \mathbb{Z}$: kommutative Gruppe

Bsp: $+$: kommutativ

$\cdot$: — " —

$\oplus \, \odot$: $\bar{a} \oplus \bar{b} = \overline{a+b} = \overline{b+a} = \bar{b} \oplus \bar{a}$

in $\mathbb{Z}/n\mathbb{Z}$ ↑ in $\mathbb{Z}$

$\bar{a} \odot \bar{b} = \overline{a \cdot b} = \overline{b \cdot a} = \bar{b} \odot \bar{a}$.

$\circ$: $g: \mathbb{Z} \to \{1,2,3\}, \quad f: \mathbb{Q} \to \mathbb{Z}$

$g \circ f: \mathbb{Q} \to \{1,2,3\}$

$\circ$ ist nicht kommutativ:

$f: \mathbb{R} \to \mathbb{R}$, $x \mapsto x^2$ $\quad (f(x) = x^2)$ $\qquad$ $g: \mathbb{R} \to \mathbb{R}$, $x \mapsto x+2$ $\quad (g(x) = x+2)$

$g \circ f: \mathbb{R} \to \mathbb{R}$

$x \to x^2 \mapsto x^2 + 2$

$g \circ f(x) = g(\underbrace{f(x)}_{= x^2}) = x^2 + 2$

$f \circ g: \mathbb{R} \to \mathbb{R}$

$x \mapsto x+2 \mapsto (x+2)^2 = x^2 + 4x + 4$

$\Rightarrow g \circ f(x) \neq f \circ g(x)$

$1 = \frac{1}{1}$ $\quad 2 = \frac{2}{1}$ $\quad 3 = \frac{3}{1}$

Wann erbt eine Teilmenge einer Gruppe die Gruppenstruktur?

z.B. $(\mathbb{Z}, +) \subset (\mathbb{Q}, +)$

$(\mathbb{Q}, +)$: Gruppe mit neutralem El. 0, inversem El. $-a \in \mathbb{Q}$ zu $a \in \mathbb{Q}$

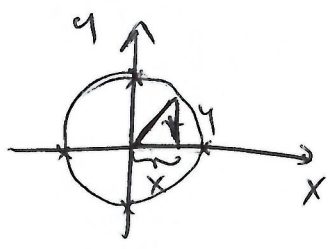
Untergruppe $(\mathbb{N}, +) \subset (\mathbb{Q}, +)$: keine Gruppe weil $0 \notin \mathbb{N}$ und das inverse El. für $a \in \mathbb{N}$ $(-a) \notin \mathbb{N}$.

$-2 \notin \mathbb{N}$

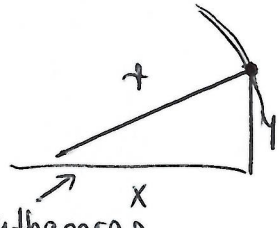
keine Untergruppe

Untergruppe $\Leftarrow$

- Abgeschlossenheit bzgl $+$: für alle $a, b \in \mathbb{Z}$ gilt $a+b \in \mathbb{Z}$.
- Abgeschlossenheit bzgl Inversenbildung $(-)$: für alle $a \in \mathbb{Z}$ ist $-a \in \mathbb{Z}$.



$= \{(x,y) \in \mathbb{R}^2 \mid \underbrace{x^2 + y^2 = r^2}_{\text{Lösungsmenge der Gleichung}}\}$ = Kreis



Pythagoras.

Elliptische Kurven:

Menge = Punkte auf Kurve $\cup \{\infty\}$

Verknüpfung: ? Gerade durch P & Q → Berechen den Schnittpunkt mit Menge = R, Spiegle R an x-Achse → $P \oplus Q$.

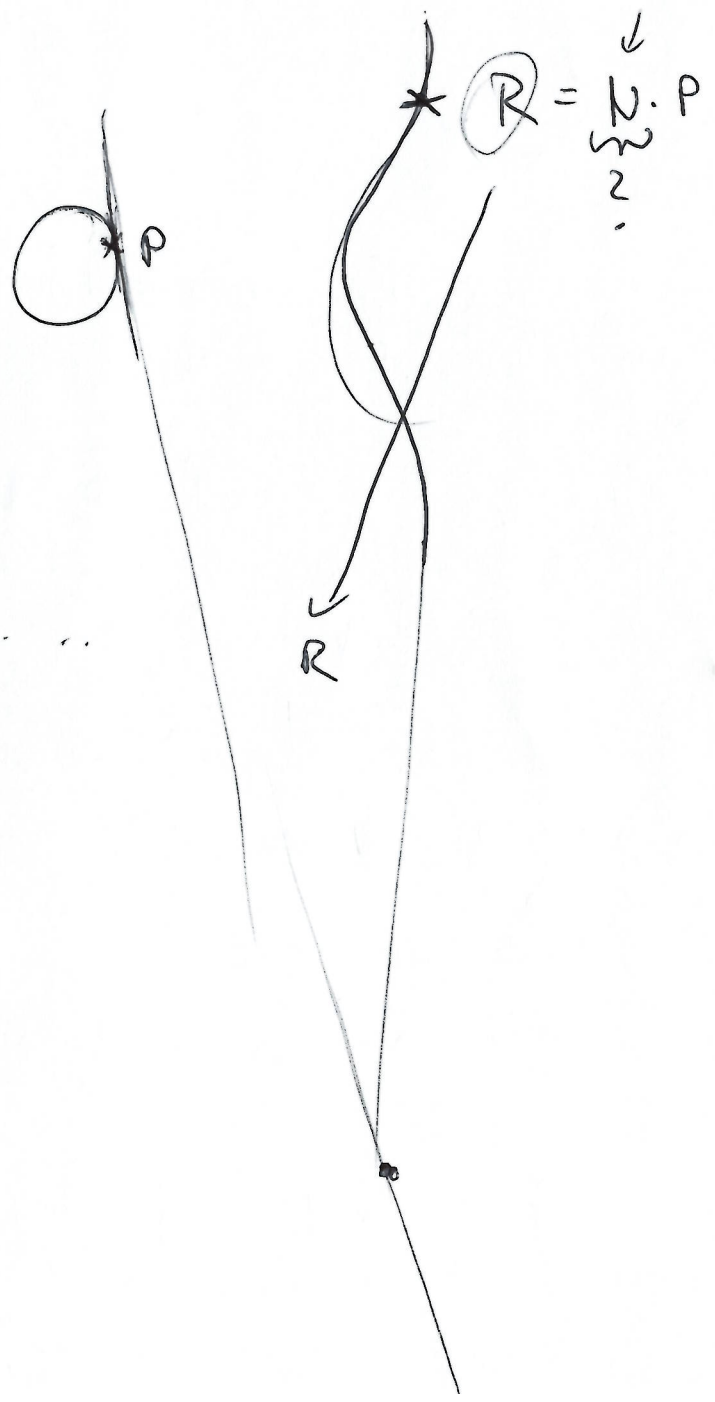
neutrales Element: ∞ ✓

inveses Element: ? für P ist $-P$ der gespiegelte an der x-Achse und $-\infty = \infty$ $\{=\infty\}$

man kann zeigen: das Assoziativgesetz gilt.

$\oplus$ ist außerdem kommutativ: $P \oplus Q = Q \oplus P$

z.B. 10^{10}



$P \oplus P$ $\quad 2P \oplus P$ ~~$P \oplus P \oplus P$~~

$P, 2 \cdot P, 3 \cdot P, 4 \cdot P \ldots$

$2P \oplus 2P$

$4P \oplus 4P$

$8P \oplus 8P$