$\langle \mathbb{Z}; - \rangle$:

assoz.: $((a-b)-c) \stackrel{?}{=} (a-(b-c))$

$\quad\;\; \| \qquad\qquad\qquad\qquad \downarrow$

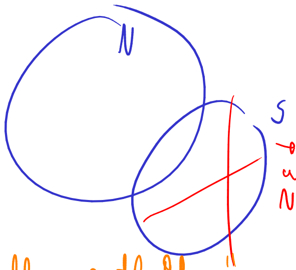
$a-b-c \neq a-b+c$ ×

Gegenbsp! $a=b=0$, $c=1$

$\overset{G}{\overset{\|}{\langle \mathcal{P}(\mathbb{N}); \cap \rangle}}$:

assoz.: "$\cap$" assoziativ ✓

neutrales Element:



→ dann wäre $N \cap S \neq S$

N so dass $\forall S \in G \;\; N \cap S = S$

$\Rightarrow \;\; S \subseteq N$ für jedes S "N muss alles enthalten"

$\Rightarrow$ insbesondere $\mathbb{N} \subseteq N$. Da $N \in \mathcal{P}(\mathbb{N}) \Leftrightarrow N \subseteq \mathbb{N}$ gilt also $N = \mathbb{N}$.

Für $\mathbb{N}$ gilt $\mathbb{N} \cap S = S$ für alle S. ✓

inverse:

Für alle S gibt es $\hat{S}$ s.d.

$S \cap \hat{S} = \mathbb{N}$?

Aber dann $\mathbb{N} \subseteq S$ → Gegenbsp.: $\neg\exists X \;\; \emptyset \cap X = \mathbb{N} \Rightarrow$ kein Inverses

(angenommen $\emptyset \cap X = \mathbb{N} \Rightarrow \mathbb{N} \subseteq \emptyset$ ↯)

Let $\langle G; *, \hat{}, e \rangle$ be a group and define

$$H = \{a \in G \mid \forall b \in G \;\; a * b = b * a\}$$

(i.e. all commutative elements of H). Prove that H is a subgroup of G.

1. $e \in H$:

Sei $b \in H$.

$e * b = b = b * e$

$\Rightarrow e \in H$

2. Sei $a, b \in H$ und $c = a * b$.

z.Z.: $c \in H$. Also $\forall d \in G \;\; d * c = c * d$

Sei $d \in G$. Wir müssen natürlich irgendwie die Def. von H anwenden

$\Rightarrow \; d * c = \underbrace{d * a}_{} * b \qquad = c * d$

$= a * \underbrace{d * b}_{} \qquad (a \in H)$

$= a * b * d \qquad (b \in H)$

3. Sei $\underline{a \in H}$. $\boxed{\text{Sei } b \in G.}$ z.Z: $\hat{a} * b = b * \hat{a}$

ich weiss nur über a etwas

$\Rightarrow$ ich muss irgendwie das "^" wegbekommen

$$\Rightarrow \hat{a} * b = \widehat{\widehat{(\hat{a} * b)}}$$ $\Rightarrow$ Trick

$$= \widehat{(\hat{b} * a)}$$ ⇝ jetzt kann ich $a \in H$ anwenden

$$= \widehat{(a * \hat{b})} \quad (a \in H)$$

$$= b * \hat{a}$$

Let H, H' subgroups of G. Prove

$$H \cup H' \text{ is a subgroup of } G \implies \underbrace{H \subseteq H' \text{ or } H' \subseteq H}_{A \;\vee\; B \;\equiv\; \neg A \to B}.$$

Nehme an $H \cup H'$ ein Subgroup von G und $\underbrace{H \not\subseteq H'}_{\neg A}$.

$\Rightarrow$ es gibt ein $a \in H$ mit $a \notin H'$.

Sei $h \in H'$. z.Z. $h' \in H$.

$\Rightarrow a * h \in H \cup H'$

Angenommen $a * h \in H$:

$\Rightarrow \hat{a} * a * h \in H$ (H abgeschlossen bez. $*$, ^)

$\Rightarrow \hat{a} * a * h = h \in H$

Nehme an $a * h \in H'$.

$\Rightarrow a * h * \hat{h} = a \in H'$ ↯

Also $a * h \in H'$ wie gewünscht.

---

g ist eine "generator" von $\langle \mathbb{Z}_n; \oplus \rangle \iff \gcd(n, g) = 1$.

g generator wenn: $|\langle g \rangle = \{0, g, g^2, \dots, g^{ord(g)-1}\}| = \mathbb{Z}_n$.

$\iff ord(g) = n$

Durch potenzieren erreichen wir also jedes Element in $\mathbb{Z}_n$.

In $\langle \mathbb{Z}_n; \oplus \rangle$ gilt $g^k = \underbrace{g \oplus g \oplus \dots \oplus g}_{k \text{ Mal}} = R_n(k \cdot g)$

Also $g^k = 0 \iff R_n(k \cdot g) = 0$

$\iff n \mid k \cdot g$

$k \cdot g$ gibt 0, sobald wir ein vielfaches von n erreicht haben.

Wenn wir $ord(g)$ suchen, suchen wir das kleinste Vielfache $k \cdot g$, s.d. $n \mid k \cdot g$

Bsp.: $n = 8$, $g = 3$

$\underset{k=1}{3} \to \underset{k=2}{6} \to \underset{k=3}{9} \to \dots \to \underset{k=8}{24}$

Also folgt

$\operatorname{ord}(g) = k \iff g^k = 0$ und für alle $\ell \geq 1$:

$\ell g = 0 \Rightarrow \ell \geq k$

Also: $\operatorname{ord}(g) = n \iff$ für jedes $\ell \geq 1$ gilt

gilt: $\underline{n \mid \ell \cdot g} \Rightarrow \ell \geq n$ (Vielfaches von g)

(Also $n \mid \ell \cdot g$ und $\underline{g \mid \ell \cdot g} \Rightarrow \ell \geq n \Rightarrow n \cdot g \mid \ell \cdot g$)

gilt sowieso

$\iff \operatorname{lcm}(n, g) = n \cdot g$

$\iff \gcd(n, g) = \frac{n \cdot g}{\operatorname{lcm}(n \cdot g)} = 1$

Bsp.: $\langle \mathbb{Z}_5 ; \oplus \rangle$

1 generiert $\mathbb{Z}_5$

4 generiert $\mathbb{Z}_5$

9 generiert $\mathbb{Z}_{4096}$

$\gcd(m, n) = 1 \implies \langle (1,1) \rangle = \langle \mathbb{Z}_m ; \oplus \rangle \times \langle \mathbb{Z}_n ; \oplus \rangle$

Nehme an $\gcd(m, n) = 1$.

$(1,1)^k = (1^k, 1^k)$

$= (R_m(k \cdot 1), R_n(k \cdot 1))$

$= (0, 0)$

$\iff m \mid k$ und $n \mid k$

Für $k = m \cdot n$ gilt also $(1,1)^k = (0,0)$

Um zu zeigen $\operatorname{ord}((1,1)) = m \cdot n$ brauchen wir:

1. $(1,1)^{m \cdot n} = (0,0)$ ( )
2. $(1,1)^\ell \neq (0,0)$ für $\ell < k$

Für $\ell < k$ gilt:

da m, n kein Primfaktor zusammen haben, müssen wir alle in das lcm reinpacken, um $m \mid \operatorname{lcm}$ und $n \mid \operatorname{lcm}$ zu haben.

$\gcd(m, n) = 1 \Rightarrow \operatorname{lcm}(m, n) = m \cdot n$

$\Rightarrow$ für $\ell < m \cdot n$ gilt $m \nmid \ell$ oder $n \nmid \ell$

$\Rightarrow$ für $\ell < m \cdot n$ gilt $(1,1)^\ell \neq (0,0)$

$\langle \mathbb{Z}_3; \oplus \rangle \times \langle \mathbb{Z}_4; \oplus \rangle = G$

$\langle (0,1) \rangle \qquad \langle (1,0) \rangle$

$\{(0,0)\}, \; G, \; \{0\} \times \mathbb{Z}_4, \; \mathbb{Z}_3 \times \{0\}$ } diese sind einfach

Idee: nehme einzelne Elemente und generiere alle Potenzen.

$\mathbb{Z}_3 \times \mathbb{Z}_4$

~~(0,0)~~	$\underline{(0,1)}$	$\underline{(0,2)}$	(0,3)
(1,0)	$\underline{(1,1)}$	$\underline{(1,2)}$	$\underline{(1,3)}$
(2,0)	$\underline{(2,1)}$	$\underline{(2,2)}$	$\underline{(2,3)}$

Nach dem Lemma im Skript generieren alle ___ die ganze Gruppe.

Wir betrachten zuerst die Gruppe generiert von nur einem Element, dann die, die von zwei generiert werden usw. ... → alle Kombinationen.

Aber immer ohne ___ weil dann generieren wir die ganze Gruppe und bekommen nichts Neues!

Wir können auch ausnützen, dass einige Elemente die gleiche Subgroup generieren oder wenn $\langle a \rangle \subseteq \langle b \rangle$.

$\Rightarrow$ wir müssen sie nicht kombinieren.

$(0,2)$: $\{(0,2), (0,0)\}$

$\vdots$