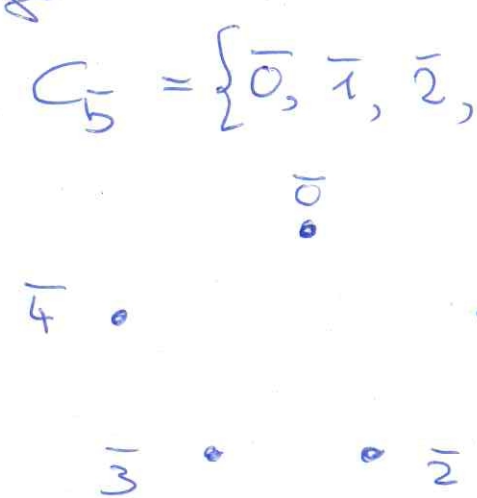
Beispiel Betrachte fünfelementige Menge

$$C_5 = \{\bar{0}, \bar{1}, \bar{2}, \bar{3}, \bar{4}\}$$



"Rechnen" in C_5:

$\bar{3} + \bar{4}$:= "starte bei $\bar{4}$, gehe 3 Plätze weiter"

$= \bar{2}$

Ebenso:

$\bar{0} + \bar{2} = \bar{2} = \bar{2} + \bar{0}$, $\quad \bar{2} + \bar{3} = \bar{0} = \bar{3} + \bar{2}$,

$\bar{1} + (\bar{2} + \bar{3}) = \bar{1} + \bar{0} \quad (\bar{1} + \bar{2}) + \bar{3} = \bar{3} + \bar{3}$

$= \bar{1}$. $\qquad = \bar{1}$.

Rechenregeln in C_5:

(G1) Für alle $\bar{a}, \bar{b}, \bar{c} \in C_5$ gilt

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

(G2) Für jedes $\bar{a} \in C_5$ gilt

$$\bar{a} + \bar{0} = \bar{a} = \bar{0} + \bar{a}$$

(G3) Für jedes $\bar{a} \in C_5$ gibt es $\bar{b} \in C_5$ mit

$$\bar{a} + \bar{b} = \bar{0} = \bar{b} + \bar{a}$$

nämlich

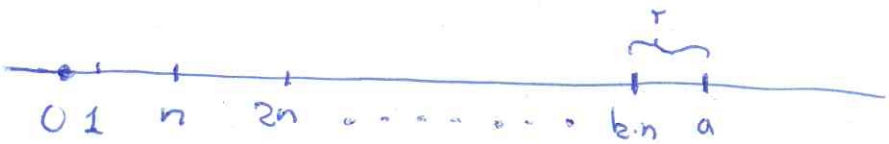
$$\bar{b} := \begin{cases} \overline{5-a}, & \bar{a} = \bar{1}, \bar{2}, \bar{3}, \bar{4}, \\ \bar{0}, & \bar{a} = \bar{0}. \end{cases}$$

(Ab) Für alle $\bar{a}, \bar{b} \in C_5$ gilt

$$\bar{a} + \bar{b} = \bar{b} + \bar{a}$$

Erinnerung (Division mit Rest).

Es sei $n \in \mathbb{N}_{\geq 1}$. **Idee**: Gegeben $a \in \mathbb{Z}$, approximiere a von unten durch Vielfache von n:



Genauer: Jedes $a \in \mathbb{Z}$ hat eine eindeutige Darstellung

$$a = kn + r, \quad \text{wobei } k = \max(l \in \mathbb{Z};\ ln \leq a)$$
$$r = a - k \cdot n$$

Dabei: $0 \leq r < n$. Nenne r den **Rest von a modulo n**. Schreibe

$r(a;n)$ für r,

$k(a;n)$ für k.

Beispiel $n = 5$ und $a = 4, 7, -3$:

$4 = 0 \cdot 5 + 4$, also $r(4;5) = 4$,

$7 = 1 \cdot 5 + 2$, also $r(7;5) = 2$,

$-3 = (-1) \cdot 5 + 2$ also $r(-3;5) = 2$.

Bemerkung: Rechnen in C_5: Stets

$$\overline{a} + \overline{b} = \overline{r(a+b;5)}$$

Definition (Innere) Verknüpfung auf einer Menge X: Abbildung

$$\kappa : X \times X \to X, \quad (x_1, x_2) \mapsto \kappa(x_1, x_2)$$

Übliche Schreibweisen:

$\kappa(x_1, x_2) =: x_1 * x_2$

$\kappa(x_1, x_2) =: x_1 \cdot x_2$ "multiplikativ"

$\kappa(x_1, x_2) =: x_1 + x_2$ "additiv".

Definition Gruppe: nichtleere Menge G mit Verknüpfung

$$G \times G \to G, \quad (g_1, g_2) \mapsto g_1 * g_2,$$

sodass gilt:

(G1) "$*$" ist assoziativ, d.h. für je drei $g_1, g_2, g_3 \in G$ gilt

$$g_1 * (g_2 * g_3) = (g_1 * g_2) * g_3$$

(G2) "$*$" hat neutrales Element, d.h., es gibt $e \in G$, sodass für alle $g \in G$ gilt:

$$e * g = g = g * e$$

(G3) Jedes $g \in G$ hat Inverses bezüglich "$*$", d.h. zu jedem $g \in G$ gibt es $g' \in G$ mit

$$g' * g = e = g * g'$$

Eine Gruppe G mit Verknüpfung "$*$" heisst abelsch (kommutativ), falls zusätzlich zu (G1), (G2), (G3):

(Ab) "$*$" ist kommutativ, d.h. für je zwei $g_1, g_2 \in G$ gilt

$$g_1 * g_2 = g_2 * g_1$$

Schreibweise $(G, *)$ bzw. $(G, +)$ für Gruppe G mit Verknüpfung "$*$" bzw. "$+$".

Bemerkung Wir kennen schon einige abelsche Gruppen:

$$(\mathbb{C}, +), \quad (\mathbb{Z}, +), \quad (\mathbb{Q}, +), \quad (\mathbb{R}, +)$$

$$(\mathbb{Q} \setminus \{0\}, \cdot), \quad (\mathbb{R} \setminus \{0\}, \cdot).$$

Satz Es sei $(G,*)$ Gruppe. Dann:

(i) G besitzt genau ein neutrales El.

(ii) Jedes $g \in G$ besitzt genau ein Inverses.

Beweis Zu (i). Wegen (G2) gibt es ein neutrales El. $e \in G$.

Es sei $e' \in G$ weiteres neutrales El. Dann:

$$e' = e * e' = e.$$

Zu (ii). Es sei $g \in G$. Wegen (G3) hat g Inverses g'.

Es sei g'' weiteres Inverses zu g. Dann:

$$g' = g' * (\underbrace{g * g''}_{e})$$

$$\overset{(G1)}{=} (\underbrace{g' * g}_{e}) * g'' = g''. \quad \square$$

Notation für neutrale und inverse El.:

Verknüpfg.:	"$*$"	"$\cdot$"	"$+$"
Neutrales:	e_G	1_G	0_G
Inverses:	g^{-1}	$\bar{g}^{1}$	$-g$

Satz Es seien $(G,*)$ Gruppe und $g \in G$.

(i) Ist $g' \in G$ mit $g' * g = e_G$, so gilt $g' = g^{-1}$.

(ii) Ist $g' \in G$ mit $g * g' = e_G$, so gilt $g' = g^{-1}$

Beweis Wir zeigen (i). Es gilt:

$$g' = g' * (g * g^{-1})$$

$$= (g' * g) * g^{-1} = g^{-1}. \quad \square$$

Definition Es seien $(G,*)$ und $(H,*)$ Gruppen. Eine Abbildung $\varphi: G \to H$ heisst *Gruppenhomomorphismus*, falls

$$\varphi(g_1 * g_2) = \varphi(g_1) * \varphi(g_2)$$

für alle $g_1, g_2 \in G$ gilt.

Beispiel Für jede Gruppe G ist $id_G: G \to G$ ein Gruppenhom.

Satz Es seien $(G,*)$ und $(H,*)$ Grp. und $\varphi: G \to H$ Gruppenhom. Dann:

$$\varphi(e_G) = e_H, \quad \varphi(\bar{g}^1) = \varphi(g)^{-1} \text{ für alle } g \in G$$

Beweis Es gilt:

$$\varphi(e_G) = \varphi(e_G * e_G) = \varphi(e_G) * \varphi(e_G)$$

Multiplikation mit $\varphi(e_G)^{-1}$ liefert

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

Weiter:

$$\varphi(\bar{g}^1) * \varphi(g) = \varphi(\bar{g}^1 * g) = \varphi(e_G) = e_H$$

Voriger Satz: $\varphi(\bar{g}^1) = \varphi(g)^{-1}$. □

Konstruktion Es sei $n \in \mathbb{N}_{\geq 1}$. Betrachte

$$C_n := \{\bar{0}, \dots, \overline{n-1}\}$$

Definieren Verknüpfung "+" auf C_n:

$$\bar{a} + \bar{b} := \overline{r(a+b;n)}$$

Satz $(C_n, +)$ ist abelsche Gruppe mit neutralem Element $\bar{0}$. Für $\bar{0} \neq \bar{a} \in C_n$ ist das Inverse

$$-\bar{a} = \overline{n-a}$$

Man hat surjektiven Gruppenhom.:

$$\pi: \mathbb{Z} \to C_n, \quad a \mapsto \overline{r(a;n)}$$

Dabei gilt für alle $a, b \in \mathbb{Z}$:

$$\pi(a) = \pi(b) \Leftrightarrow n \text{ teilt } a-b.$$

Lemma. Es seien $n \in \mathbb{N}_{\geq 1}$, $a, b \in \mathbb{Z}$.

Dann sind äquivalent:

(i) $r(a;n) = r(b;n)$.

(ii) n teilt $a-b$.

Beweis. Division mit Rest:

$$a = \underbrace{k_a}_{\uparrow} n + \underbrace{r_a}_{\uparrow}, \qquad b = k_b n + r_b$$

$k(a;n)$ $\quad$ $r(a;n)$

Zu "(i) $\Rightarrow$ (ii)". Es gilt:

$$(a-b) = (k_a n + r_a) - (k_b n + r_b) = (k_a - k_b) n.$$

Zu "(ii) $\Rightarrow$ (i)". Die Zahl n teilt

$$(a-b) + (k_b - k_a) n = (a - k_a n) - (b - k_b n)$$
$$= r_a - r_b.$$

Wegen $-n < r_a - r_b < n$: $r_a = r_b$. $\square$

Beweis Satz. Betrachte zunächst

$$\pi : \mathbb{Z} \to C_n, \quad a \mapsto \overline{r(a;n)}$$

Die Abb. π ist surjektiv: Für $0 \leq a < n$:

$$\pi(a) = \overline{r(a;n)} = \bar{a}.$$

Weiter, für alle $a, b \in \mathbb{Z}$:

$$\pi(a) = \pi(b) \iff \overline{r(a;n)} = \overline{r(b;n)}$$
$$\iff r(a;n) = r(b;n)$$
$$\overset{\text{Lemma}}{\iff} n \text{ teilt } a-b$$

Die Abb. π ist Grp.hom.: Für alle $a, b \in \mathbb{Z}$:

$$\pi(a+b) = \pi(k_a n + r_a + k_b n + r_b)$$
$$= \pi(r_a + r_b)$$
$$\overset{\text{Def. Add.}}{=} \bar{r}_a + \bar{r}_b = \pi(a) + \pi(b).$$

Damit bequem (G1), ..., (Ab). Etwa (Ab):

$$\bar{a} + \bar{b} = \pi(a) + \pi(b)$$
$$= \pi(a+b)$$
$$= \pi(b+a)$$
$$= \pi(b) + \pi(a) = \bar{b} + \bar{a}. \quad \square$$