Erinnerung Gruppe: Menge $G \neq \emptyset$ mit Verknüpfung

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

sodass

(G1) μ ist assoziativ, d.h., haben stets

$$g_1(g_2 g_3) = (g_1 g_2) g_3,$$

(G2) es gibt neutrales El., d.h., $e \in G$ mit

$$eg = g = ge \text{ für alle } g \in G,$$

(G3) jedes $g \in G$ hat Inverses $g^{-1} \in G$, d.h.

$$g^{-1} g = e = g g^{-1}.$$

Nenne G abelsch, falls zusätzlich

(Ab) stets $g_1 g_2 = g_2 g_1$.

Schreiben abelsche Gruppen oft additiv:

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

Dabei: 0_G neutrales El., $-g$ Inverses zu $g \in G$ und $g - g'$ für $g + (-g')$.

Beispiel $(\mathbb{Z}, +)$ ist abelsche Gruppe.

Definition Ordnung einer Menge X:

$$|X| := \text{Anzahl der Elemente von } X.$$

Beispiel Zu jedem $n \in \mathbb{Z}_{\geq 1}$ gibt es eine abelsche Gruppe der Ordnung n:

$$C_n := \{\overline{0}, \overline{1}, \overline{2}, \ldots, \overline{n-1}\}$$

hat genau n Elemente. Betrachte Verknüpfung

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

wobei r der Rest von $a+b$ mod. n, d.h.

$$a + b = kn + r, \quad k, r \in \mathbb{Z}, \; 0 \leq r < n.$$

Dann $(C_n, +)$ abelsche Gruppe.

Weiter:

* Neutrales Element: $\overline{0}$
* Inverses zu $\overline{a}$ mit $1 \leq a \leq n-1$:

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

__Beispiel__ X Menge. Gruppe der *Permutationen* von X:

$$S(X) := \{\varphi : X \to X;\ \varphi \text{ bijektiv}\}$$

mit Komposition als Verknüpfung:

$$S(X) \times S(X) \to S(X), \quad (\sigma, \tau) \mapsto \sigma \circ \tau.$$

Spezialfall: $X_n := \{1, 2, \ldots, n\}$ liefert *symmetrische Gruppe*:

$$S_n := S(X_n).$$

Elemente von S_n werden durch Wertetabellen dargestellt. z.B. in S_3:

$$\begin{bmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{bmatrix} : X_3 \to X_3, \quad 1 \mapsto 2,\ 2 \mapsto 3,\ 3 \mapsto 1.$$

Für $i, j \in X_n$ mit $i \neq j$ hat man *Transposition*:

$$(i,j) : X_n \to X_n, \quad \begin{array}{l} i \mapsto j \\ j \mapsto i \\ k \mapsto k \text{ für } k \neq i,j \end{array}$$

Haben $|S_n| = n!$. Für $n \geq 3$ ist S_n nicht abelsch. z.B. in S_3:

$$\begin{bmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{bmatrix} \circ \begin{bmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{bmatrix} = \begin{bmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{bmatrix},$$

$$\begin{bmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{bmatrix} \circ \begin{bmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{bmatrix} = \begin{bmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{bmatrix}.$$

__Beispiel__ $\mathbb{K}$ Körper. *Allgemeine lineare Gruppe*:

$$GL(n; \mathbb{K}) := \{A \in Mat(n,n; \mathbb{K});\ A \text{ invertierbar}\}$$

mit Matrizenmultiplikation als Verknüpfung:

$$GL(n; \mathbb{K}) \times GL(n; \mathbb{K}) \to GL(n; \mathbb{K}), \quad (A, B) \mapsto A \cdot B.$$

Für $n \geq 2$ ist $GL(n; \mathbb{K})$ nicht abelsch. z.B. in $GL(2; \mathbb{Q})$:

$$\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \cdot \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix},$$

$$\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \cdot \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} = \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix}.$$

Erinnerung G Gruppe. Untergruppe: $H \subseteq G$ mit

$$e_G \in H, \quad h_1, h_2 \in H \Rightarrow h_1 h_2 \in H, \quad h \in H \Rightarrow h^{-1} \in H.$$

und induzierter Verknüpfung $(h_1, h_2) \mapsto h_1 h_2$.

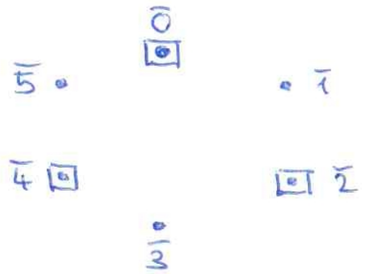
Schreiben

$$H \leq G$$

falls $H \subseteq G$ Untergruppe. Jedes $H \leq G$ ist Gruppe mit $e_H = e_G$.

Beispiel Für $n \in \mathbb{Z}$: $n\mathbb{Z} \leq \mathbb{Z}$. Für $n = 3$:

Beispiel Haben $\{\bar{0}, \bar{2}, \bar{4}\} \leq C_6 = \{\bar{0}, \bar{1}, \dots, \bar{5}\}$



Erinnerung G, H Gruppen. Nenne $\varphi: G \to H$ Gruppenhomomorphismus, falls stets

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

Jeder Gruppenhomomorphismus $\varphi: G \to H$ erfüllt

$$\varphi(e_G) = e_H, \qquad \varphi(g^{-1}) = \varphi(g)^{-1}.$$

Weiter: Komposition von Gruppenhom. ist wieder Gruppenhom.

Beispiel Für jedes $n \in \mathbb{Z}_{\geq 1}$ hat man surjektiven Gruppenhom.:

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

Beispiel Betrachte S_n. Signum von $\sigma \in S_n$:

$$\mathrm{sg}(\sigma) := \prod_{1 \leq i < j \leq n} \frac{\sigma(j) - \sigma(i)}{j - i} = (-1)^{m(\sigma)}$$

mit $m(\sigma) :=$ Anzahl Fehlstände von σ, d.h. Paare i, j mit

$$i < j, \qquad \sigma(i) > \sigma(j).$$

Signum liefert Gruppenhomomorphismus

$$\mathrm{sg}: S_n \to \{\pm 1\}, \quad \sigma \mapsto \mathrm{sg}(\sigma).$$

Beispiel $\mathbb{K}$ Körper. Haben Gruppenhom.

$$\det: GL(n; \mathbb{K}) \to \mathbb{K}^*, \quad A \mapsto \det(A).$$

Definition Ein Gruppenhom. $\varphi: G \to H$ heisst *Isomorphismus*, falls es einen Gruppenhom. $\psi: H \to G$ gibt mit

$$\psi \circ \varphi = \mathrm{id}_G, \qquad \varphi \circ \psi = \mathrm{id}_H.$$

Satz Sei $\varphi: G \to H$ Gruppenhom. Dann sind äquivalent:

(i) φ ist Isomorphismus.

(ii) φ ist bijektiv.

Beweis "(i) $\Rightarrow$ (ii)" klar, denn φ hat Umkehrabb.

Zu "(ii) $\Rightarrow$ (i)". Wegen φ bijektiv gibt es Umkehrabb. $\psi: H \to G$.

Z.z.: ψ ist Hom. Haben für $h_1, h_2 \in H$:

$$h_1 h_2 = \varphi(\psi(h_1))\varphi(\psi(h_2)) = \varphi(\psi(h_1)\psi(h_2)).$$

Jetzt ψ anwenden:

$$\psi(h_1 h_2) = \psi(h_1)\psi(h_2).$$

Somit ψ Gruppenhom. $\square$

Definition Sei $\varphi: G \to H$ Gruppenhom.

$$\mathrm{kern}(\varphi) := \{g \in G;\ \varphi(g) = e_H\} = \varphi^{-1}(e_H),$$

$$\mathrm{Bild}(\varphi) := \{\varphi(g);\ g \in G\} = \varphi(G).$$

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

$$\mathrm{kern}(\pi) = \{a \in \mathbb{Z};\ r(a;n) = 0\} = n\mathbb{Z},$$

$$\mathrm{Bild}(\pi) = \{\overline{r(a;n)};\ a \in \mathbb{Z}\} = C_n.$$

Beispiel Für $\mathrm{sg}: S_n \to \{\pm 1\}$:

$$\mathrm{kern}(\mathrm{sg}) = A_n := \{\sigma \in S_n;\ \mathrm{sg}(\sigma) = 1\}.$$

A_n heisst *alternierende Gruppe*.

Beispiel Für $\det: GL(n;\mathbb{K}) \to \mathbb{K}^*$:

$$\mathrm{kern}(\det) = SL(n;\mathbb{K}) := \{A \in GL(n;\mathbb{K});\ \det(A) = 1\}.$$

$SL(n;\mathbb{K})$ heisst *spezielle lineare Gruppe*.

Bemerkung Sei $\varphi: G \to H$ Gruppenhom.

(i) $H' \leq H \Rightarrow \varphi^{-1}(H') \leq G$,

(ii) $G' \leq G \Rightarrow \varphi(G') \leq H$.

Insbes. sind kern und Bild von Gruppenhom. stets Untergruppen.

Satz Sei $\varphi: G \to H$ Gruppenhom. Dann sind äquivalent:

(i) φ ist injektiv.

(ii) $\operatorname{kern}(\varphi) = \{e_G\}$.

Beweis Zu "(i) $\Rightarrow$ (ii)". Haben $\varphi(e_G) = e_H$. Somit $\{e_G\} \subseteq \operatorname{kern}(\varphi)$. Wegen φ injektiv:

$$\{e_G\} = \operatorname{kern}(\varphi).$$

Zu "(ii) $\Rightarrow$ (i)". Seien $g_1, g_2 \in G$ mit $\varphi(g_1) = \varphi(g_2)$. Dann:

$$e_H = \varphi(g_2)^{-1}\varphi(g_1) = \varphi(g_2^{-1} g_1).$$

Also

$$g_2^{-1} g_1 \in \operatorname{kern}(\varphi) \Rightarrow g_2^{-1} g_1 = e_G \Rightarrow g_1 = g_2. \quad \square$$

Konstruktion Seien $G_1, \ldots, G_r$ Gruppen.

Direktes Produkt: $G_1 \times \ldots \times G_r$ mit der komponentenweisen Verknüpfung

$$(g_1, \ldots, g_r)(h_1, \ldots, h_r) := (g_1 h_1, \ldots, g_r h_r).$$

$G_1 \times \ldots \times G_r$ ist Gruppe.

Neutrales El. und Inversenbildung:

$$e_{G_1 \times \ldots \times G_r} = (e_{G_1}, \ldots, e_{G_r}), \quad (g_1, \ldots, g_r)^{-1} = (g_1^{-1}, \ldots, g_r^{-1}).$$

Haben surjektive Gruppenhom.:

$$\pi_i : G_1 \times \ldots \times G_r \to G_i, \ (g_1, \ldots, g_r) \mapsto g_i.$$

Bemerkung $G_1, \ldots, G_r$ Gruppen. Dann:

$$G_1 \times \ldots \times G_r \text{ abelsch} \iff G_1, \ldots, G_r \text{ abelsch}.$$

Bemerkung Seien G_1, G_2, H Gruppen und $\varphi_i: H \to G_i$ Gruppenhom., $i = 1, 2$.

Dann hat man kommut. Diagramm von Gruppenhom.:

$$\begin{tikzcd} & G_1 \times G_2 \arrow[dl, "\pi_1"'] \arrow[dr, "\pi_2"] & \\ G_1 & & G_2 \\ & H \arrow[ul, "\varphi_1"] \arrow[ur, "\varphi_2"'] \arrow[uu, "\varphi"] & \end{tikzcd}$$

wobei $\varphi: H \to G_1 \times G_2$ eindeutig bestimmt und gegeben durch

$$\varphi(h) = (\varphi_1(h), \varphi_2(h)).$$