Erinnerung Relation auf Menge X:

$$R \subseteq X \times X = \{(x,y);\ x,y \in X\}.$$

Schreiben

$$x \sim y, \quad \text{falls } (x,y) \in R.$$

Äquivalenzrelation: $R \subseteq X \times X$ mit

(i) R reflexiv: stets $x \sim x$,

(ii) R symmetrisch: stets $x \sim y \Rightarrow y \sim x$,

(iii) R transitiv: stets $x \sim y,\ y \sim z \Rightarrow x \sim z$.

Äquivalenzklasse von $x \in X$:

$$[x] := \{x' \in X;\ x' \sim x\} \subseteq X.$$

Haben für alle $x, y \in X$:

(*) $x \in [x]$,

(**) $[x] = [y] \Leftrightarrow x \sim y$,

(***) entweder $[x] = [y]$ oder $[x] \cap [y] = \emptyset$.

Insbesondere: X ist disjunkte Vereinigung seiner Äquivalenzklassen.

Beispiel Sei $n \in \mathbb{Z}_{\geq 1}$. Dann:

$$n\mathbb{Z} = \{nl;\ l \in \mathbb{Z}\} \leq \mathbb{Z}.$$

Haben Äquivalenzrelation auf $\mathbb{Z}$:

$$a \sim_{n\mathbb{Z}} b \;:\Longleftrightarrow\; a - b \in n\mathbb{Z}$$

$$\Longleftrightarrow\; r(a;n) - r(b;n) \in n\mathbb{Z}$$

$$\Longleftrightarrow\; r(a;n) = r(b;n)$$

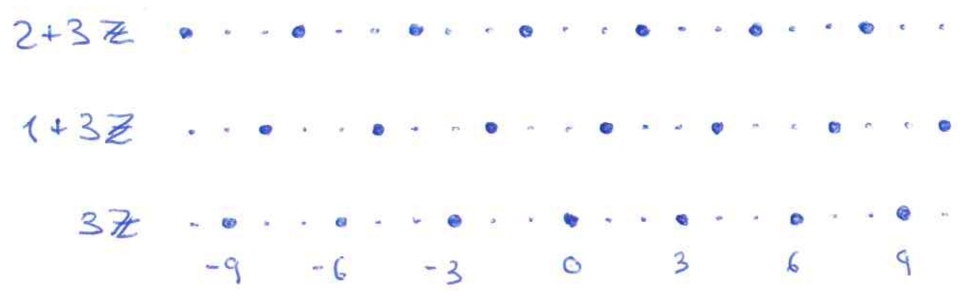
Zugehörige Äquivalenzklassen

$$n\mathbb{Z},\ 1+n\mathbb{Z},\ \dots,\ n-1+n\mathbb{Z}.$$

Insbesondere

$$\mathbb{Z} = n\mathbb{Z} \sqcup 1+n\mathbb{Z} \sqcup \dots \sqcup n-1+n\mathbb{Z}.$$

ZB. für $n = 3$



Definition Seien G Gruppe und $H \leq G$ Untergruppe.

(i) Nebenklasse (auch Linksnebenklasse) von $g \in G$:

$$gH := \{gh;\ h \in H\}$$

(ii) Homogener Raum zu H:

$$G/H := \{gH;\ g \in G\}$$

Satz Seien G Gruppe, $H \leq G$ Untergruppe. Dann erhält man Äquivalenzrelation auf G:

$$g_1 \sim_H g_2 :\Longleftrightarrow g_2^{-1} g_1 \in H.$$

Die Äquivalenzklasse von $g \in G$ ist

$$[g] = gH.$$

Weiter hat man disjunkte Vereinigung

$$G = \bigsqcup_{gH \in G/H} gH.$$

Beweis Zeigen "$\sim_H$" ist Äquivalenzrelation.

Reflexivität: Für jedes $g \in G$ gilt

$$g^{-1} g = e_G \in H \implies g \sim_H g.$$

Symmetrie: Seien $g_1, g_2 \in G$. Dann:

$$g_1 \sim_H g_2 \implies g_2^{-1} g_1 \in H$$
$$\implies (g_2^{-1} g_1)^{-1} \in H$$
$$\implies g_1^{-1} g_2 \in H \implies g_2 \sim_H g_1.$$

Transitivität: Seien $g_1, g_2, g_3 \in G$. Dann:

$$g_1 \sim_H g_2,\ g_2 \sim_H g_3 \implies g_3^{-1} g_2,\ g_2^{-1} g_1 \in H$$
$$\implies g_3^{-1} g_2 g_2^{-1} g_1 \in H$$
$$\implies g_3^{-1} g_1 \in H \implies g_1 \sim_H g_3.$$

Äquivalenzklassen: für $g, g' \in G$ gilt

$$g' \in [g] \iff g' \sim_H g$$
$$\iff g^{-1} g' \in H \iff g' \in gH.$$

$\square$

Definition G Gruppe, $H \leq G$ Untergruppe. *Index* von H in G:

$$[G:H] := |G/H|.$$

Satz von Lagrange G Gruppe und $H \leq G$ Untergruppe. Dann:

$$|G| = [G:H] \cdot |H|.$$

Insbes. für endliches G: $|H|$ teilt $|G|$.

Lemma G Gruppe, $H \leq G$. Dann, für jedes $g \in G$:

$$|gH| = |H|.$$

Beweis Haben bijektive Abbildung

$$L_g : H \to gH, \quad h \mapsto gh.$$

Umkehrabbildung: $(L_g)^{-1} = L_{g^{-1}}$. $\square$

Beweis Satz von Lagrange Wissen:

$$G = \bigsqcup_{gH \in G/H} gH, \quad |gH| = |H|, \quad |G/H| = [G:H].$$

Falls $|G| = \infty$: $|H| = \infty$ oder $|G/H| = \infty$.

Falls $|G| < \infty$: Haben

$$|G| = \sum_{gH \in G/H} |gH| = \sum_{gH \in G/H} |H| = |G/H| \cdot |H|.$$

$\square$

Folgerung G endl. Gruppe mit $|G|$ Primzahl. Dann: G, $\{e_G\}$ einzige Untergrp. von G.

Definition Seien G Gruppe, $g \in G$.

(i) Die von g *erzeugte Untergruppe* ist

$$\langle g \rangle := \{g^n ; n \in \mathbb{Z}\} \leq G.$$

(ii) Die *Ordnung* von g ist

$$\mathrm{ord}(g) := |\langle g \rangle|.$$

Folgerung G endl. Gruppe, $g \in G$. Dann ist $\mathrm{ord}(g)$ Teiler von $|G|$.

Folgerung G endl. Gruppe, $|G|$ Primzahl. Dann: $G = \langle g \rangle$ für jedes $e_G \neq g \in G$.

Definition G Gruppe. Nenne $H \leq G$ *Normalteiler* ($H \trianglelefteq G$), falls für alle $g \in G$:

$$gHg^{-1} := \{ghg^{-1};\ h \in H\} = H.$$

Bemerkung G abelsche Gruppe. Dann ist jedes $H \leq G$ Normalteiler.

Bemerkung G Gruppe. $H \leq G$ genau dann Normalteiler, wenn für alle $g \in G$:

$$gH = \{gh;\ h \in H\} = \{hg;\ h \in H\} =: Hg.$$

Beispiel Betrachte $GL(2;\mathbb{Q})$ und

$$U(2;\mathbb{Q}) := \left\{\begin{pmatrix} 1 & a \\ 0 & 1 \end{pmatrix};\ a \in \mathbb{Q}\right\} \leq GL(2;\mathbb{Q}).$$

Dann: $U(2;\mathbb{Q})$ kein Normalteiler:

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

und

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

Es gibt also $A \in GL(2;\mathbb{Q})$ mit

$$A \cdot U(2;\mathbb{Q}) \neq U(2;\mathbb{Q}) \cdot A.$$

Konstruktion G Gruppe, $H \trianglelefteq G$.

Faktorgruppe: G/H mit

$$G/H \times G/H \to G/H,\quad (g_1H, g_2H) \mapsto g_1g_2H.$$

Neutrales Element und Inversenbildung:

$$e_{G/H} = e_G H, \qquad (gH)^{-1} = g^{-1}H.$$

Weiter hat man surjektiven Gruppenhom.

$$\pi: G \to G/H, \quad g \mapsto gH.$$

Dabei: $\mathrm{kern}(\pi) = H$.

Beweis Wohldefiniertheit der Verknüpfung: Betrachte

$$g_1H = g_1'H, \qquad g_2H = g_2'H.$$

Wegen $H \trianglelefteq G$: $g_2'H = Hg_2'$. Damit

$$g_1g_2H = g_1g_2'H \overset{\circ}{=} g_1Hg_2'$$
$$= g_1'Hg_2' \overset{\circ}{=} g_1'g_2'H.$$

Jetzt klar: G/H Gruppe, π surj. Grphom.
Zu $\mathrm{kern}(\pi) = H$: Haben

$$\pi(g) = e_{G/H} \iff gH = e_G H \iff g \in H.$$

$\square$

__Homomorphiesatz__ Seien $\varphi : G \to H$ Gruppenhom., $N \trianglelefteq G$ mit $N \subseteq \mathrm{kern}(\varphi)$. Dann hat man kommut. Diagramm

$$\begin{tikzcd} G \arrow[rr, "\varphi : g \mapsto \varphi(g)"] \arrow[dr, "\pi : g \mapsto gN"'] & & H \\ & G/N \arrow[ur, "\bar{\varphi} : gN \mapsto \varphi(g)"'] & \end{tikzcd}$$

von Gruppenhom., wobei $\bar{\varphi} : G/N \to H$ eindeutig bestimmt. Weiter:

(i) $\bar{\varphi}$ injektiv $\iff$ $N = \mathrm{kern}(\varphi)$

(ii) $\bar{\varphi}$ surjektiv $\iff$ φ surjektiv.

__Beweis__ Zeigen Wohldefiniertheit von

$$\bar{\varphi} : G/N \to H, \quad gN \mapsto \varphi(g)$$

Seien $g, g' \in G$ mit $g'N = gN$. Dann:

$$g^{-1}g' \in N \Rightarrow g^{-1}g' = n \text{ mit } n \in N.$$

Damit:

$$\varphi(g') = \varphi(gn) = \varphi(g)\varphi(n) \overset{N \subseteq \mathrm{kern}(\varphi)}{=} \varphi(g).$$

Somit $\bar{\varphi}$ wohldefiniert. Jetzt klar: $\bar{\varphi} \circ \pi = \varphi$ und $\bar{\varphi}$ eind. bestimmt.

Zeigen: $\bar{\varphi}$ ist Gruppenhom.: Haben

$$\bar{\varphi}(g_1N g_2N) = \bar{\varphi}(g_1g_2N) = \varphi(g_1g_2)$$
$$= \varphi(g_1)\varphi(g_2) = \bar{\varphi}(g_1N)\bar{\varphi}(g_2N).$$

Zu (i). Zu zeigen:

$$\mathrm{kern}(\bar{\varphi}) = \{e_G N\} \iff \mathrm{kern}(\varphi) = N.$$

"$\Rightarrow$": Haben

$$\mathrm{kern}(\varphi) = \varphi^{-1}(e_H) = \pi^{-1}(\bar{\varphi}^{-1}(e_H)) = \pi^{-1}(e_G N) = N.$$

"$\Leftarrow$": Haben

$$\bar{\varphi}(gN) = e_H \iff \varphi(g) = e_H$$
$$\iff g \in N \iff gN = e_G N.$$

Zu (ii). Wegen π surj.: $\mathrm{Bild}(\bar{\varphi}) = \mathrm{Bild}(\varphi)$. $\square$

Satz Sei $\varphi: G \to G'$ Gruppenhom.
Dann: $\ker(\varphi) \trianglelefteq G$.

Beweis Setze $H := \ker(\varphi)$. Dann, für jedes $h \in H$ und $g \in G$:

$$\begin{aligned}\varphi(ghg^{-1}) &= \varphi(g)\varphi(h)\varphi(g)^{-1} \\ &= \varphi(g)\, e_{G'}\, \varphi(g)^{-1} \\ &= e_{G'}.\end{aligned}$$

Somit $ghg^{-1} \in H$, d.h., $gHg^{-1} = H$. $\square$

Satz Seien $\varphi: G \to G'$ surj. Grp.hom., $H := \ker(\varphi)$. Dann hat man Iso

$$\overline{\varphi}: G/H \to G', \quad gH \mapsto \varphi(g).$$

Beweis HomSatz: $\overline{\varphi}$ ist wohldef. Gruppenhom. Weiter:

$H = \ker(\varphi) \Rightarrow \overline{\varphi}$ injektiv,

φ surjektiv $\Rightarrow \overline{\varphi}$ surjektiv. $\square$

Beispiel Sei $n \in \mathbb{Z}_{\geq 1}$. Haben $n\mathbb{Z} \trianglelefteq \mathbb{Z}$, Faktorgruppe $\mathbb{Z}/n\mathbb{Z}$ mit den El.

$$n\mathbb{Z},\ 1+n\mathbb{Z},\ \ldots,\ (n-1)+n\mathbb{Z}.$$

Verknüpfung in $\mathbb{Z}/n\mathbb{Z}$:

$$(a+n\mathbb{Z}) + (b+n\mathbb{Z}) = (a+b)+n\mathbb{Z}.$$

Beh.: Haben Iso

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

Betrachte dafür

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

Wissen: φ_n surj. Hom., $\ker(\varphi_n) = n\mathbb{Z}$.

HomSatz:

$$\begin{tikzcd} \mathbb{Z} \arrow[rr, "\varphi_n"] \arrow[dr, "\pi"'] & & C_n \\ & \mathbb{Z}/n\mathbb{Z} \arrow[ur, "\overline{\varphi}_n : a+n\mathbb{Z} \mapsto \overline{r(a;n)}"'] & \end{tikzcd}$$

kommutativ, $\overline{\varphi}_n$ Hom. Satz von eben: $\overline{\varphi}_n$ Isomorphismus.

Ab jetzt: $C_n = \mathbb{Z}/n\mathbb{Z}$, $\overline{a} = a+n\mathbb{Z}$.