Mathematik für Informatik 2

Kapitel III: Algebraische Strukturen

§22 Gruppen und Homomorphismen

A) Gruppen

Def. 22.1 (a) Eine **Gruppe** ist ein Paar $(G, \cdot)$ mit einer Menge G, die nicht leer ist, und einer zweistelligen Operation $\cdot : G \times G \longrightarrow G : (g,h) \mapsto g \cdot h = gh$, so dass folgende Axiome gelten:

(G1) $\forall g,h,k \in G : (g \cdot h) \cdot k = g \cdot (h \cdot k)$ Assoziativgesetz

(G2) $\exists e \in G : \forall g \in G : e \cdot g = g$ Existenz eines Neutralen

(G3) $\forall g \in G \; \exists g' \in G : g' \cdot g = e$ Existenz von Inversen

(g': g^{-1})

(b) Eine Gruppe $(G, \cdot)$ heißt **abelsch**, wenn zudem (G4) gilt:

(G4) $\forall g,h \in G : g \cdot h = h \cdot g$ Kommutativgesetz

(c) Eine Gruppe $(G, \cdot)$ heißt **endlich**, wenn $|G| < \infty$. Sonst heißt sie **unendlich**.

Bsp. 22.3:

(a) $(\mathbb{Z}, +)$ ist eine abelsche Gruppe mit Neutralem 0 und $-g$ als Inverses zu g.

Genauso: $(\mathbb{Q}, +)$, $(\mathbb{R}, +)$, $(\mathbb{C}, +)$

Nicht: $(\mathbb{N}, +)$ keine Gruppe!

(b) $(\mathbb{Q} \setminus \{0\}, \cdot)$ ist eine abelsche Gruppe mit Neutralem 1 und $\frac{1}{g}$ als Inverses zu g.

Genauso: $(\mathbb{R} \setminus \{0\}, \cdot)$, $(\mathbb{C} \setminus \{0\}, \cdot)$

Nicht: $(\mathbb{Z} \setminus \{0\}, \cdot)$ ist keine Gruppe

(c) Sei M eine nicht-leere Menge.

Setze: $\mathrm{Sym}(M) := \{ f : M \to M \mid f \text{ ist bijektiv} \}$

Dann ist $(\mathrm{Sym}(M), \circ)$ eine Gruppe! (symmetrische Gruppe zu M)

$|M| \geq 3 \Rightarrow (\mathrm{Sym}(M), \circ)$ ist nicht abelsch?

Lemma 22.4: Sei $(G, \cdot)$ eine Gruppe.

(a) Sei $e \in G$ ein neutrales Element, dann gilt $g \cdot e = g \quad \forall g \in G$. Außerdem ist das Neutrale eindeutig bestimmt.

(b) Sei $g \in G$ und $g' \in G$ ein Inverses zu g, dann gilt auch $g \cdot g' = e$. Außerdem ist das Inverse eindeutig bestimmt.

Beweis:

Sei $g \in G$ und $g' \in G$ ein Inverses.

Zeige: $g \cdot g' = e$

- (G3) $\Rightarrow g'' \in G$: $g'' \cdot g' = e$
- $g \cdot g' \overset{(G2)}{=} e \cdot (g \cdot g') = (g'' \cdot g') \cdot (g \cdot g') \overset{(G1)}{=} g'' \cdot (g' \cdot (g \cdot g'))$

$\overset{(G1)}{=} g'' \cdot (\underbrace{(g' \cdot g)}_{=e} \cdot g') \overset{(G3)}{=} g'' \cdot (e \cdot g') \overset{(G2)}{=} g'' \cdot g' = e$

Rest: Ü.A.

(3)

Lemma 22.6: Sei $(G, \cdot)$ eine Gruppe, $g, h, a, b \in G$, $m, n \in \mathbb{Z}$.

(a) Kürzungsregeln:
- $g \cdot a = g \cdot b \Rightarrow a = b$
- $a \cdot g = b \cdot g \Rightarrow a = b$

(b) $(g^{-1})^{-1} = g$, $(g \cdot h)^{-1} = h^{-1} \cdot g^{-1}$

(c) $g^n \cdot g^m = g^{n+m}$, $(g^m)^n = g^{m \cdot n}$ (Potenzgesetze)

$g^n = \underbrace{g \cdot g \cdots g}_{n\text{-mal}}$, wenn $n > 0$

$g^{-n} = \underbrace{g^{-1} \cdot \cdots \cdot g^{-1}}_{n\text{-mal}}$ wenn $n > 0$

$g^0 := e$

Potenzgesetze in einer additiven Gruppe $(G,+)$

$(n\cdot g)+(m\cdot g) = (n+m)\cdot g$, $n\cdot(m\cdot g) = (n\cdot m)\cdot g$

Wenn $(G,+)$ Gruppe, dann schreibe $n\cdot g$ statt g^n

Beweis

(a) $g\cdot a = g\cdot b \Rightarrow (g^{-1}\cdot g)\cdot a = g^{-1}\cdot(g\cdot a) = g^{-1}\cdot(g\cdot b) = (g^{-1}\cdot g)\cdot b$

$e\cdot a = a$ $\qquad$ $b = e\cdot b$

(b) $g\cdot g^{-1} \overset{2.4}{=} e \Rightarrow g$ verhält sich wie das Inverse von g^{-1}

$\overset{\text{Eindeutigkeit}}{\Rightarrow} g = (g^{-1})^{-1}$

$(h^{-1}\cdot g^{-1})\cdot(g\cdot h) = h^{-1}\cdot(g^{-1}\cdot(g\cdot h)) = h^{-1}\cdot((g^{-1}\cdot g)\cdot h) = h^{-1}\cdot(e\cdot h)$ ($g^{-1}\cdot g = e$)

$= h^{-1}\cdot h = e \overset{2.4}{\Rightarrow} (g\cdot h)^{-1} = h^{-1}\cdot g^{-1}$

(c) ÜA. ☐

B) Untergruppen

Def. 22.7: Sei $(G,\cdot)$ eine Gruppe, $\emptyset \neq U \subseteq G$.

Dann heißt U eine Untergruppe von G

$:\Leftrightarrow$ (1) $\forall u,v \in U: u\cdot v \in U$ Abgeschlossenheit bzgl. "$\cdot$"

(2) $\forall u \in U: u^{-1} \in U$ " bzgl. Inverse

Notation: $U \leq G$

Prop. 22.8: Sei $(G,\cdot)$ eine Gruppe und $U \leq G$.

Dann ist $(U,\cdot)$ selbst eine Gruppe mit Neutralem e_G und Inversen u_G^{-1} zu $u \in U$.

Beweis: $\cdot : U\times U \to U : (u,v) \mapsto u\cdot v$ (wohldefiniert: $u\cdot v \in U$ nach (1))

- (G1) gezeigt von G
- (G2): $U \neq \emptyset \Rightarrow \exists u \in U \overset{(2)}{\Rightarrow} u^{-1} \in U \overset{(2)}{\Rightarrow} u^{-1}\cdot u \in U \Rightarrow \forall v \in U: e_G\cdot v = v$ ($u^{-1}\cdot u = e_G$)
- (G3): $u \in U \overset{(2)}{\Rightarrow} u_G^{-1} \in U \Rightarrow u_G^{-1}\cdot u = e_G = e_U$

☐

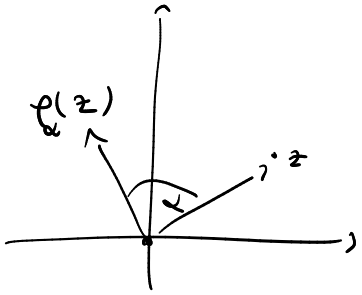
Bsp. 22.9:

(a) Ist $(G,\cdot)$ eine Gruppe, dann ist $G \leq G$ und $\{e_G\} \leq G$
(triviale Untergruppen)

(b) $\{1,-1\} \leq (\mathbb{Q}\setminus\{0\},\cdot)$

(c) $\alpha \in \mathbb{R} \Rightarrow \varphi_\alpha : \mathbb{R}^2 \to \mathbb{R}^2 : \begin{pmatrix} x \\ y \end{pmatrix} \mapsto \begin{pmatrix} \cos(\alpha)\cdot x - \sin(\alpha)\cdot y \\ \sin(\alpha)\cdot x + \cos(\alpha)\cdot y \end{pmatrix}$

Drehung um den Ursprung um den Winkel α

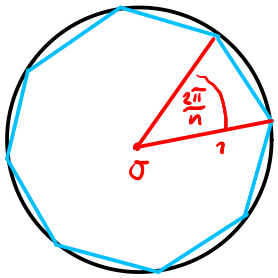


Setze: $SO(2) := \{\varphi_\alpha \mid \alpha \in \mathbb{R}\}$
$= \{\varphi_\alpha \mid \alpha \in [0, 2\pi)\}$

Beachte: $\varphi_\alpha \circ \varphi_\beta = \varphi_{\alpha+\beta} \in SO(2)$, $(\varphi_\alpha)^{-1} = \varphi_{-\alpha} \in SO(2)$

$\Rightarrow SO(2) \leq Sym(\mathbb{R}^2)$

(d) Sei E_n das reguläre n-Eck im $\mathbb{R}^2$.



Setze: $\mathcal{U} := \{\varphi_\alpha \in SO(2) \mid \varphi_\alpha(E_n) = E_n\}$
$\overset{!!}{=} \{\varphi_\alpha \mid \alpha = k\cdot\frac{2\pi}{n}, k = 0,\dots,n-1\}$

Beh: $\mathcal{U} \leq SO(2)$

Denn:
- $id_{\mathbb{R}^2} \in \mathcal{U} \leq SO(2) \Rightarrow \mathcal{U} \neq \emptyset$
- Seien $\varphi_\alpha, \varphi_\beta \in \mathcal{U}$
$\Rightarrow (\varphi_\alpha \circ \varphi_\beta)(E_n) = \varphi_\alpha(\underbrace{\varphi_\beta(E_n)}_{=E_n}) = \varphi_\alpha(E_n) = E_n$
$\Rightarrow \varphi_\alpha \circ \varphi_\beta \in \mathcal{U}$
- Sei $\varphi_\alpha \in \mathcal{U} \Rightarrow \varphi_\alpha^{-1}(E_n) = \varphi_\alpha^{-1}(\varphi_\alpha(E_n)) = (\varphi_\alpha^{-1}\circ\varphi_\alpha)(E_n)$
$= E_n = id_{\mathbb{R}^2}(E_n)$
$\Leftarrow \varphi_\alpha^{-1} \in \mathcal{U}$
- Damit: $\mathcal{U} \leq SO(2)$. ∎

(e) Sei $n \in \mathbb{Z}$.

Dann ist $n\cdot\mathbb{Z} := \{n\cdot z \mid z \in \mathbb{Z}\}$ ist Untergruppe von $(\mathbb{Z},+)$

Beweis:

- $0 = n\cdot 0 \in n\cdot\mathbb{Z} \subseteq \mathbb{Z}$, also: $n\cdot\mathbb{Z} \neq \emptyset$
- Sei $n\cdot z,\ n\cdot z' \in n\cdot\mathbb{Z}$

  $\Rightarrow$. $n\cdot z + n\cdot z' = n\cdot(\underbrace{z+z'}_{\in\mathbb{Z}}) \in n\cdot\mathbb{Z}$

  . $-(n\cdot z) = n\cdot(\underbrace{-z}_{\in\mathbb{Z}}) \in n\cdot\mathbb{Z}$

$\Rightarrow n\cdot\mathbb{Z} \leq \mathbb{Z}$ ☐

Beachte: $m, n \in \mathbb{Z} \Rightarrow \big(m\cdot\mathbb{Z} \subseteq n\cdot\mathbb{Z} \Leftrightarrow m$ ist ein Vielfaches von n

$\Leftrightarrow n \mid m \big)$

(f) $\cdot\ (\mathbb{Z},+) \leq (\mathbb{Q},+) \leq (\mathbb{R},+) \leq (\mathbb{C},+)$

$\cdot\ (\mathbb{Q}\setminus\{0\},\cdot) \leq (\mathbb{R}\setminus\{0\},\cdot) \leq (\mathbb{C}\setminus\{0\},\cdot)$

Lemma 22.11

Sei $(G,\cdot)$ eine Gruppe und $U_i \leq G$ mit $i \in I$ = Indexmenge

Dann: $\bigcap_{i\in I} U_i \leq G$.

Beweis: Ü A. ☐

Bem. 22.12:

Gilt: $2\cdot\mathbb{Z} \cup 3\cdot\mathbb{Z} \leq \mathbb{Z}$?!!

$2 + 3 = 5$ ↯ (kein Vielfaches von 2, kein Vielfaches von 3)

$\Rightarrow$ $2\cdot\mathbb{Z} \cup 3\cdot\mathbb{Z}$

Also: $2\mathbb{Z} \cup 3\mathbb{Z} \not\leq \mathbb{Z}$

Def. 22.12: Sei $(G,\cdot)$ eine Gruppe, $M \subseteq G$.

Dann heißt $\langle M \rangle := \bigcap_{\substack{U \leq G \\ M \subseteq U}} U$ = Durchschnitt aller Untergruppen, die M enthalten $\leq G$ (22.11)

das Erzeugnis von M (in G) und ist

die kleinste Untergruppe, die M enthält.

Prop. 22.13 Sei $(G,\cdot)$ eine Gruppe, $M \subseteq G$.

Dann: $\langle M \rangle = \{ g_1^{\alpha_1} \cdots g_n^{\alpha_n} \mid g_1, \dots, g_n \in M,\ \alpha_1, \dots, \alpha_n \in \mathbb{Z},\ n \geq 0 \}$

Beweis:

"$\supseteq$" $\left.\begin{array}{l} g_1, \dots, g_n \in M,\ \alpha_1, \dots, \alpha_n \in \mathbb{Z} \\ M \subseteq U \leq G \end{array}\right\} \Rightarrow g_1^{\alpha_1} \cdots g_n^{\alpha_n} \in U$

$\Downarrow$

$g_1^{\alpha_1} \cdots g_n^{\alpha_n} \in \bigcap_{\substack{V \leq G \\ M \subseteq V}} V = \langle M \rangle$

"$\subseteq$" Zeige: Rechte Seite ist eine Ugr. von G, die M enthält

- $g_1^{\alpha_1} \cdots g_n^{\alpha_n} \in R.S.$, $g_{n+1}^{\alpha_{n+1}} \cdots g_m^{\alpha_m} \in R.S.$

$\Rightarrow$
- $g_1^{\alpha_1} \cdots g_n^{\alpha_n} \cdot g_{n+1}^{\alpha_{n+1}} \cdots g_m^{\alpha_m} \in R.S.$
- $(g_1^{\alpha_1} \cdots g_n^{\alpha_n})^{-1} = g_n^{-\alpha_n} \cdots g_1^{-\alpha_1} \in R.S.$
- leeres Produkt $= e_G$ liegt in R.S.

$\left.\begin{array}{l} \\ \\ \\ \end{array}\right\} \Rightarrow R.S. \leq G$

- $g \in M \Rightarrow g^1 \in R.S. \Rightarrow M \subseteq R.S.$

Damit $\langle M \rangle = \bigcap_{\substack{U \leq G \\ M \subseteq U}} U \subseteq R.S.$ ☐

Bsp. 22.14: Sei $(G,\cdot)$ eine Gruppe und $g \in G$.

$$\Rightarrow \quad \langle g \rangle = \bigcap_{\substack{U \leq G \\ g \in U}} U = \{ g^k \mid k \in \mathbb{Z} \}$$ ist zyklische Gruppe

Konkreter: $G = \mathbb{Z}$, "$\cdot$" = "$+$", $n \in \mathbb{Z}$

$$\langle n \rangle = \{ k \cdot n \mid k \in \mathbb{Z} \} = \{ n \cdot z \mid z \in \mathbb{Z} \} = n \cdot \mathbb{Z}$$

Def. 22.15:
Eine Gruppe $(G,\cdot)$ heißt zyklisch, wenn ein $g \in G$ existiert, s.d. $G = \langle g \rangle = \{ g^k \mid k \in \mathbb{Z} \}$.

Prop. 22.16:

$U \leq \mathbb{Z} \quad \Leftrightarrow \quad \exists\, n \geq 0 : \; U = \langle n \rangle = n \cdot \mathbb{Z}$

Insbesondere: Jede Untergruppe von $(\mathbb{Z},+)$ ist zyklisch!

Beweis: "$\Leftarrow$" $U = n \cdot \mathbb{Z} \Rightarrow U \leq G$ nach Bsp. 22.9.

"$\Rightarrow$" Sei $U \leq \mathbb{Z}$.

1. Fall: $U = \{0\} \Rightarrow U = \langle 0 \rangle = 0 \cdot \mathbb{Z}$

2. Fall: $U \neq \{0\} \Rightarrow \exists\, 0 \neq z \in U \Rightarrow$ z oder $-z$ ist positiv ($z \in U$, $-z \in U$)

$$\Rightarrow \quad \{ m \in \mathbb{N} \mid 0 \neq m \in U \} \neq \emptyset$$

$$\overset{\text{Archim. Prinzip}}{\Rightarrow} \quad \exists \; n := \min \{ m \in \mathbb{N} \mid 0 \neq m \in U \}$$

Zeige: $U \overset{!}{=} \langle n \rangle = n \cdot \mathbb{Z}$

- $n \in U \Rightarrow n \cdot z \in U \;\; \forall z \in \mathbb{Z} \Rightarrow n \cdot \mathbb{Z} \subseteq U$
- Sei $u \in U \overset{\text{D.m.R.}}{\Rightarrow} \exists q, r \in \mathbb{Z} : u = q \cdot n + r$ mit $0 \leq r < n$

$$\Rightarrow \quad r = \underbrace{u}_{\in U} - q \cdot \underbrace{n}_{\in U} \in U \quad \overset{n = \min\{\dots\}}{\Rightarrow} \quad r = 0$$

$$\Rightarrow \quad u = q \cdot n = n \cdot q \in n \cdot \mathbb{Z} \Rightarrow U \subseteq n \cdot \mathbb{Z}.$$ □

c) Gruppenhomomorphismen

Def. 22.17 Seien $(G,\cdot)$ und $(H,*)$ zwei Gruppen.

Eine Abbildung $\alpha: G \to H$ heißt **Gruppenhomomorphismus**

$:\Leftrightarrow \forall g,\tilde{g} \in G: \quad \alpha(g\cdot\tilde{g}) = \alpha(g) * \alpha(\tilde{g})$

Bsp. 22.18:

(a) Sei $a \in \mathbb{R}$ und betrachte $(\mathbb{R},+)$.

$\Rightarrow m_a: \mathbb{R} \to \mathbb{R}: x \mapsto a\cdot x$ ist ein G.H.

Denn: Seien $x, y \in \mathbb{R}$

$\Rightarrow m_a(x+y) = a\cdot(x+y) = a\cdot x + a\cdot y = m_a(x) + m_a(y)$

(b) Sei $(G,\cdot)$ eine Gruppe und $g \in G$, $g \neq e$

- $L_g: G \to G: h \mapsto g\cdot h$ $>$ sind keine G.H.
- $R_g: G \to G: h \mapsto h\cdot g$

Denn: $L_g(g\cdot g) = g\cdot(g\cdot g) = g^3$ ✗

$L_g(g)\cdot L_g(g) = (g\cdot g)\cdot(g\cdot g) = g^4$

Sonst: $g^3 = g^4 \overset{KR}{\Rightarrow} e = g$ ↯ ($e\cdot g^3$, $g\cdot g^3$)

(c) Sei $(G,\cdot)$ eine Gruppe, $g \in G$.

Dann ist $i_g: G \to G: h \mapsto \underbrace{g\cdot h\cdot g^{-1}}_{=:h^g}$ ist ein G.H.

(Konjugation mit g)

Denn: Seien $h, \tilde{h} \in G$.

$\Rightarrow i_g(h\cdot\tilde{h}) = g\cdot(h\cdot\tilde{h})\cdot g^{-1} = g\cdot h\cdot e\cdot\tilde{h}\cdot g^{-1} = g\cdot h\cdot g^{-1}\cdot g\cdot\tilde{h}\cdot g^{-1}$

$= (g\cdot h\cdot g^{-1})\cdot(g\cdot\tilde{h}\cdot g^{-1}) = i_g(h)\cdot i_g(\tilde{h})$

Beachte: $i_g = R_{g^{-1}} \circ L_g$

Lemma 22.19

Seien $\alpha_1 : (G_1, \cdot) \longrightarrow (G_2, *)$ und $\alpha_2 : (G_2, *) \longrightarrow (G_3, \times)$ G.H.

Dann: $\alpha_2 \circ \alpha_1 : (G_1, \cdot) \longrightarrow (G_3, \times)$ ist ein G.H.

Beweis:

Seien $g, h \in G_1$

α_1 ist G.H.

$$\Rightarrow (\alpha_2 \circ \alpha_1)(g \cdot h) = \alpha_2(\alpha_1(g \cdot h)) = \alpha_2(\alpha_1(g) * \alpha_1(h))$$

$$\overset{\alpha_2 \text{ ist G.H.}}{=} \alpha_2(\alpha_1(g)) \times \alpha_2(\alpha_1(h)) = (\alpha_2 \circ \alpha_1)(g) \times (\alpha_2 \circ \alpha_1)(h)$$

□

Def. 22.20:

Sei $\alpha : (G, \cdot) \longrightarrow (H, *)$ ein G.H.

(a) α heißt Isomorphismus $:\Leftrightarrow$ α ist bijektiv.

(b) Wir sagen $(G, \cdot)$ und $(H, *)$ sind isomorph,

wenn: $\exists\ \alpha : G \to H$ Isomorphismus

Notation: $G \cong H$

Bsp. 22.21:

(a) $m_a : \mathbb{R} \to \mathbb{R}; x \mapsto a \cdot x$ ist Isomorphismus $\Leftrightarrow$ $a \neq 0$

Dann dann: $m_a^{-1} = m_{\frac{1}{a}}$!

(b) $i_g : G \to G; h \mapsto g \cdot h \cdot g^{-1}$ ist ein Isomorphismus

mit $(i_g)^{-1} = i_{g^{-1}}$

Denn: $i_{g^{-1}}(i_g(h)) = (g^{-1})\left(g \cdot h \cdot g^{-1}\right)\left(g^{-1}\right)^{-1}$

$$= \underbrace{g^{-1} \cdot g}_{=e} \cdot h \cdot \underbrace{g^{-1} \cdot (g^{-1})^{-1}}_{=e} = h$$

$\Rightarrow i_{g^{-1}} \circ i_g = id_G$. Umgekehrt genauso. □

Prop. 22.22 · Sei $\alpha : (G,\cdot) \longrightarrow (H,*)$ ein Gruppenhomom.

(a) $\alpha(e_G) = e_H$ (b) $\alpha(g^{-1}) = \alpha(g)^{-1}$ $\forall g \in G$

(c) $\alpha(g^n) = (\alpha(g))^n$ $\forall g \in G$ $\forall n \in \mathbb{Z}$

(d) α bijektiv $\Rightarrow$ $\alpha^{-1} : H \longrightarrow G$ ist ein Gruppenhomomorphismus.

(e) $U \leq G \Rightarrow \alpha(U) \leq H$ "Bild von U unter α"

(f) $V \leq H \Rightarrow \alpha^{-1}(V) = \{g \in G \mid \alpha(g) \in V\} \leq G$ "Urbild von V unter α"

(g) $\mathrm{Im}(\alpha) := \alpha(G) = \{\alpha(g) \mid g \in G\} \leq H$ "Bild von α"

(h) $\mathrm{Kern}(\alpha) := \alpha^{-1}(e_H) = \{g \in G \mid \alpha(g) = e_H\} \leq G$ "Kern (α)"

Beweis (a) $e_H * \alpha(e_G) = \alpha(e_G) = \alpha(e_G \cdot e_G) = \alpha(e_G) * \alpha(e_G)$

$\overset{KR}{\Rightarrow}$ $e_H = \alpha(e_G)$

(b) $\alpha(g^{-1}) * \alpha(g) = \alpha(g^{-1} \cdot g) = \alpha(e_G) \overset{(a)}{=} e_H \Rightarrow \alpha(g^{-1}) = (\alpha(g))^{-1}$

(c) (1) $n \geq 0$: Induktion nach n

$n = 0$: $\alpha(g^0) = \alpha(e_G) = e_H = (\alpha(g))^0$ ✓

$n-1 \mapsto n$: $\alpha(g^n) = \alpha(g^{n-1} \cdot g) = \alpha(g^{n-1}) * \alpha(g) \overset{\text{Ind.}}{=} (\alpha(g))^{n-1} * \alpha(g)$

$= (\alpha(g))^n$

(2) $n < 0$: $\Rightarrow -n > 0 \Rightarrow \alpha(g^n) = \alpha\left((g^{-1})^{-n}\right) \overset{(1)}{=} (\alpha(g^{-1}))^{-n}$

$\overset{(b)}{=} \left((\alpha(g))^{-1}\right)^{-n} = (\alpha(g))^n$

(d) Sei α bijektiv. Seien $u, v \in H$. Setze: $g := \alpha^{-1}(u)$, $h := \alpha^{-1}(v)$

$\Rightarrow$ $\alpha(g) = u$, $\alpha(h) = v$

$\Rightarrow$ $\alpha^{-1}(u * v) = \alpha^{-1}(\alpha(g) * \alpha(h)) = \alpha^{-1}(\alpha(g \cdot h)) = g \cdot h$

$= \alpha^{-1}(u) \cdot \alpha^{-1}(v)$

$\Rightarrow$ α^{-1} ist Gr.-H.

(e) Sei $U \leq G$. Seien $u, v \in \alpha(U) \Rightarrow \exists g, h \in U$:

$u = \alpha(g)$, $v = \alpha(h)$

$\Rightarrow$. $u * v = \alpha(g) * \alpha(h) = \alpha(\underbrace{g \cdot h}_{\in U, \text{ weil } U \leq G}) \in \alpha(U)$

. $u^{-1} = \alpha(g)^{-1} \overset{⑥}{=} \alpha(\underbrace{g^{-1}}_{\in U, \text{ weil } U \leq G}) \in \alpha(U)$

⑦ analog ⑧ folgt aus ② ⑨ folgt aus ⑦. ☐

Lemma 22.23

Ein G.H. $\alpha : (G, \cdot) \to (H, *)$ ist injektiv $\Leftrightarrow$ $\ker(\alpha) = \{e_G\}$

Proof:

"$\Rightarrow$" . 22.22 $\Rightarrow$ $e_H = \alpha(e_G) \Rightarrow e_G \in \ker(\alpha) \Rightarrow \{e_G\} \subseteq \ker(\alpha)$

. $g \in \ker(\alpha) \Rightarrow \alpha(g) = e_H = \alpha(e_G) \overset{\alpha \text{ injektiv}}{\Rightarrow} g = e_G \Rightarrow \ker(\alpha) \subseteq \{e_G\}$

"$\Leftarrow$" Seien $g, h \in G$ mit $\alpha(g) = \alpha(h)$

$\Rightarrow$ $e_H = \alpha(g)^{-1} * \alpha(h) = \alpha(g^{-1}) * \alpha(h) = \alpha(g^{-1} \cdot h)$

$\Rightarrow$ $g^{-1} \cdot h \in \ker(\alpha) = \{e_G\} \Rightarrow g^{-1} \cdot h = e_G \Rightarrow h = g$

$\Rightarrow$ α ist injektiv ☐

§ 23 Die symmetrische Gruppe S_n

Def. 23.1

. Eine bijektive Abbildung $\sigma : \{1, \dots, n\} \to \{1, \dots, n\}$ heißt eine Permutation.

. $S_n := \mathrm{Sym}(\{1, \dots, n\}) = \{\sigma : \{1, \dots, n\} \to \{1, \dots, n\} \mid \text{bijektiv}\}$ heißt die symmetrische Gruppe vom Grad n

. Eine Permutation $\sigma \in S_n$ ist eindeutig durch ihre Wertetabelle festgelegt.

$$\sigma \triangleq \begin{pmatrix} 1 & 2 & 3 & 4 & \dots & n-1 & n \\ \sigma(1) & \sigma(2) & \sigma(3) & \sigma(4) & & \sigma(n-1) & \sigma(n) \end{pmatrix}$$

#Möglichkeiten: n $n-1$ $n-2$ $n-3$ $\dots$ 2 1

Beachte, es kommt nicht auf die Reihenfolge der Spalten an:

d.h. wenn $\{1, \dots, n\} = \{a_1, \dots, a_n\}$, dann

$$\sigma = \begin{pmatrix} a_1 & a_2 & \dots & a_n \\ \sigma(a_1) & \sigma(a_2) & \dots & \sigma(a_n) \end{pmatrix}$$

Bem. 23.2:

- $(S_n, \circ)$ ist eine Gruppe, wobei $\circ$ = Verkettung von Abb.
- $|S_n| = n \cdot (n-1) \cdot (n-2) \cdots 2 \cdot 1 = n!$

Bsp. 23.3:

- $n \geq 3 \Rightarrow (S_n, \circ)$ ist nicht abelsch

  Sei $\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & \cdots & n \\ 2 & 1 & 3 & 4 & \cdots & n \end{pmatrix}$, $\tau = \begin{pmatrix} 1 & 2 & 3 & 4 & \cdots & n \\ 2 & 3 & 1 & 4 & \cdots & n \end{pmatrix}$

  $\Rightarrow (\sigma \circ \tau)(1) = \sigma(\tau(1)) = \sigma(2) = 1$ $\Rightarrow \sigma \circ \tau \neq \tau \circ \sigma$

  $(\tau \circ \sigma)(1) = \tau(\sigma(1)) = \tau(2) = 3$ #

- $n = 3$: $\sigma = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}$, $\tau = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}$

  $\Rightarrow \sigma \circ \tau = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix} \circ \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}$ ≠

  $\tau \circ \sigma = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix} \circ \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix}$

Beachte: $\begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix} = \begin{pmatrix} 2 & 1 & 3 \\ 1 & 2 & 3 \end{pmatrix} = \begin{pmatrix} 3 & 1 & 2 \\ 3 & 2 & 1 \end{pmatrix}$

Bem. 23.4: (Inversion von Permutationen)

$\sigma = \begin{pmatrix} a_1 & a_2 & \cdots & a_n \\ \sigma(a_1) & \sigma(a_2) & \cdots & \sigma(a_n) \end{pmatrix} \Rightarrow \sigma^{-1} = \begin{pmatrix} \sigma(a_1) & \sigma(a_2) & \cdots & \sigma(a_n) \\ a_1 & a_2 & \cdots & a_n \end{pmatrix}$

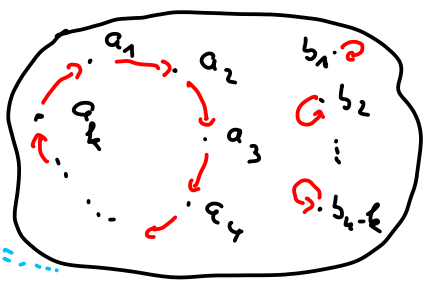
d.h. Inversion bedeutet die beiden Zeilen tauschen!

z.B.: $\sigma = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix} \Rightarrow \sigma^{-1} = \begin{pmatrix} 3 & 1 & 2 \\ 1 & 2 & 3 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}$

Def. 23.5:

(a) Sei $\{1, \ldots, n\} = \{a_1, \ldots, a_k\} \cup \{b_1, \ldots, b_{n-k}\}$, $k \geq 2$

Dann heißt $\sigma = \begin{pmatrix} a_1 & a_2 & \cdots & a_{k-1} & a_k & b_1 & \cdots & b_{n-k} \\ a_2 & a_3 & \cdots & a_k & a_1 & b_1 & \cdots & b_{n-k} \end{pmatrix}$



ein k-Zykel.

!: $(a_1\, a_2\, a_3 \cdots a_k) = (a_k\, a_1\, a_2 \cdots a_{k-1}) = \ldots$

(b) Ein 2-Zykel heißt auch **Transposition**, d.h. es gibt zwei Zahlen $i, j \in \{1,\dots,n\}$, die von der Transposition (ij) vertauscht werden.

(c) Schreibe: id statt $id_{\{1,\dots,n\}}$

Bem. 23.6:

- $\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 1 & 3 & 2 \end{pmatrix} \in S_4$, $\quad \tau = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 4 & 1 & 3 & 2 & 5 \end{pmatrix} \in S_5$

  $= (1\,4\,2)$ $\qquad$ $= (1\,4\,2)$

  In solche Zykelschreibweise wird es in welcher S_n die Permutation liegt.

- $\tau = (i\,j) \Rightarrow \tau^{-1} = (i\,j) \Rightarrow \tau^2 = id$

- $|S_2| = 2$, $|S_3| = 6$, $|S_4| = 24$, $\dots$, $|S_{60}| \approx 10^{82}$

Satz 23.7

(a) Jede Permutation lässt sich als Produkt disjunkter Zykel schreiben.

(b) " " " " " " von Transpositionen schreiben.

(c) " " " " " " " " verschiedener Zahlen schreiben.

(d) $\exists_1$ G.H. $sgn: (S_n, \circ) \to (\{1,-1\}, \cdot)$ s.d. $sgn(\tau) = -1$ für jede Transposition τ. (Signum)

Insbesondere: σ = Produkt von k Transp. $\Rightarrow sgn(\sigma) = (-1)^k$

(e) $\forall\, \sigma \in S_n$: $sgn(\sigma) = sgn(\sigma^{-1})$

(f) $A_n := \ker(sgn) = \{\sigma \in S_n \mid sgn(\sigma) = 1\}$ und $\tau = (i\,j) \in S_n$

$\Rightarrow S_n = A_n \cup A_n\tau$, wobei $A_n\tau = \{\sigma \circ \tau \mid \sigma \in A_n\}$

Bem. 23.8:

- sgn G.H. $\Rightarrow sgn(\sigma \circ \tau) = sgn(\sigma) \cdot sgn(\tau)$ $\forall \sigma, \tau$
- $\sigma = \tau_1 \circ \dots \circ \tau_k$ mit τ_i = Transposition $\Rightarrow sgn(\sigma) = \prod_{i=1}^{k} sgn(\tau_i) = (-1)^k$

Beispiel 23.9

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 5 & 4 & 3 & 1 \end{pmatrix} \in S_5$$

$$\Rightarrow \sigma = (1\ 2\ 5) \circ (3\ 4)$$

Bsp. 23.10

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 3 & 8 & 7 & 1 & 4 & 5 & 6 & 9 & 2 \end{pmatrix}$$

$$= \underbrace{(1\ 3\ 7\ 6\ 5\ 4)}_{=:\tau} \circ \underbrace{(2\ 8\ 9)}_{=:\pi}$$

$$\tau = (1\ 3\ 7\ 6\ 5\ 4) = \underbrace{(1\ 3)(3\ 7)(7\ 6)(6\ 5)(5\ 4)}_{=:\tau'}$$

a	$\tau(a)$	$\tau'(a)$
1	3	3
4	1	1
6	5	5
⋮	⋮	⋮

$$\pi = (2\ 8)(8\ 9)$$

$$\Rightarrow \quad \sigma = \tau \circ \pi = (1\ 3)(3\ 7)(7\ 6)(6\ 5)(5\ 4)(2\ 8)(8\ 9)$$

$$\Rightarrow \quad \operatorname{sgn}(\sigma) = (-1)^7 = -1$$

$$\omega = (3\ 7) = \underbrace{(3\ 4)(4\ 6)(6\ 5)(5\ 7)(7\ 6)(6\ 5)(5\ 4)(4\ 3)}_{=:\omega'}$$

a	$\omega(a)$	$\omega'(a)$
3	7	7
7	3	3
5	5	5
2	2	2

Bsp. 23.11

$S_3 = \{ \underbrace{id}_{\parallel \begin{pmatrix}1&2&3\\1&2&3\end{pmatrix}}, \begin{pmatrix}1&2&3\\2&1&3\end{pmatrix}, \begin{pmatrix}1&2&3\\3&2&1\end{pmatrix}, \begin{pmatrix}1&2&3\\1&3&2\end{pmatrix}, \begin{pmatrix}1&2&3\\2&3&1\end{pmatrix}, \begin{pmatrix}1&2&3\\3&1&2\end{pmatrix} \}$

$\begin{pmatrix}1&2&3\\1&2&3\end{pmatrix} = (1)(2)(3)$ $\quad \begin{pmatrix}1&2&3\\2&1&3\end{pmatrix} = (12)$ $\quad \begin{pmatrix}1&2&3\\3&2&1\end{pmatrix} = (13)$ $\quad \begin{pmatrix}1&2&3\\1&3&2\end{pmatrix} = (1)(23) = (23)$ $\quad \begin{pmatrix}1&2&3\\2&3&1\end{pmatrix} = (123) = (12)(23)$ $\quad \begin{pmatrix}1&2&3\\3&1&2\end{pmatrix} = (132) = (13)(32)$

Sgn: $1 \quad -1 \quad -1 \quad -1 \quad (-1)^2 = 1 \quad (-1)^2 = 1$

$\Rightarrow A_3 = \{ id, \underbrace{(123)}_{d}, \underbrace{(132)}_{d^{-1}} \} \leq S_3$

$(123) \circ (132) = (1)(2)(3) = id$

$(12573)^{-1} = (37521)$

$\Rightarrow S_3 = A_3 \dot\cup A_3 \circ (12) \dot\cup A_3 \circ \underbrace{(13)}_{(123)\circ(12)} \dot\cup A_3 \circ \underbrace{(23)}_{(132)\circ(12)}$

Denn: $A_3 \circ (12) = \{ (12), (123)\circ(12), (132)\circ(12) \}$

§ 24 Der Satz von Lagrange und Faktorgruppen

A) Linksnebenklassen

Notation 24.1: Sei $(G, \cdot)$ eine Gruppe, $A, B \subseteq G$, $g \in G$.

Dann:
- $A \cdot B := \{ a \cdot b \mid a \in A, b \in B \}$
- $g \cdot A := \{ g \cdot a \mid a \in A \}$ = Linksnebenklasse von A bez. g.

Beachte: $A, B, C \subseteq G \Rightarrow (A \cdot B) \cdot C = A \cdot (B \cdot C)$

$= \{ a \cdot b \cdot c \mid a \in A, b \in B, c \in C \}$

Proposition 2.2 Sei $(G,\cdot)$ eine Gruppe, $U \leq G$, $g, h \in G$

Definiere: $g \sim h \;:\Leftrightarrow\; g^{-1}h \in U$

Dann ist $\sim$ eine Äquivalenzrelation auf G

Zudem: Äquivalenzklasse von g bzgl. $\sim$ ist $\overline{g} = g \cdot U = \{g \cdot u \mid u \in U\}$

(Linksnebenklasse von U bzgl. g)

Setze: $\cdot\ G/U := \{\overline{g} \mid g \in G\}$ = Menge aller Linksnebenklassen von U

$\cdot\ |G:U| := |G/U|$ = Anzahl der Linksnebenklassen von U

heißt der Index von U in G.

Beweis: (Ä1) Reflexivität: $g^{-1}g = e \in U \Rightarrow g \sim g$

(Ä2) Symmetrie: $g \sim h \Rightarrow g^{-1}h \in U \Rightarrow U \ni (g^{-1}h)^{-1} = h^{-1}(g^{-1})^{-1} = h^{-1}g$

$\Rightarrow h \sim g$

(Ä3) Transitivität: $g \sim h,\ h \sim k \Rightarrow g^{-1}h,\ h^{-1}k \in U$

$\Rightarrow U \ni (g^{-1}h)\cdot(h^{-1}k) = g^{-1}\cdot h h^{-1} \cdot k = g^{-1}k$

$\Rightarrow g \sim k$

Zeige noch: $\overline{g} = \{h \in G \mid h \sim g\} \overset{!}{=} gU$

"$\supseteq$" Sei $u \in U$. z.z.: $g \cdot u \sim g$ (d.h. $g \cdot u \in \overline{g}$)

Aber: $(g\cdot u)^{-1} \cdot g = u^{-1} g^{-1} g = u^{-1} \in U \Rightarrow g \cdot u \sim g$

"$\subseteq$" Sei $h \in G$ mit $h \sim g \Rightarrow h^{-1}g \in U$

$\Rightarrow (h^{-1}g)^{-1} \in U \Rightarrow g \cdot U \ni g \cdot (g^{-1}h) = g g^{-1} h = h$

$g^{-1}(h^{-1})^{-1} = g^{-1}h$

Korollar 24.3

Sei $(G, \cdot)$ eine Gruppe und $\mathcal{U} \leq G$.

Dann: $\forall g, h \in G$: $g\cdot\mathcal{U} \cap h\cdot\mathcal{U} = \emptyset$ oder $g\cdot\mathcal{U} = h\cdot\mathcal{U}$

$$G = \dot{\bigcup_{\lambda \in G/\mathcal{U}}} \lambda = \dot{\bigcup_{\lambda \in G/\mathcal{U}}} g_\lambda \cdot \mathcal{U}$$

wobei $g_\lambda \in \lambda$ ein Repräsentant der Linksnebenklasse ist.

Bsp. 24.4:

$G = S_3$, $\mathcal{U} = A_3$

$$\Rightarrow A_3 = \{id, (123), (132)\} = id \circ A_3 = (123) \circ A_3$$

$$(12) \circ A_3 = \{(12), (12)(123), (12)(132)\} = \{(12), (23), (13)\}$$

$$\Rightarrow S_3 = A_3 \dot\cup (12) \circ A_3 = id \circ A_3 \dot\cup (12) \circ A_3$$

$$S_3 / A_3 = \{A_3, (12) \circ A_3\} = \{\overline{id}, \overline{(12)}\}$$

Bem. 24.5:

$\mathcal{U} \leq G \rightarrow \overline{e} = e \cdot \mathcal{U} = \mathcal{U}$

d.h. $\mathcal{U}$ selbst ist immer eine $\mathcal{U}$-Nebenklasse von $\mathcal{U}$

$\forall u \in \mathcal{U}: u \cdot \mathcal{U} = \{u \cdot v \mid v \in \mathcal{U}\} = \mathcal{U}$

Prop. 24.6:

Sei $(G, \cdot) = (\mathbb{Z}, +)$, $\mathcal{U} = n\cdot\mathbb{Z}$ für ein $n \geq 1$.

Die Linksnebenklassen von $\mathcal{U}$ in G sind genau die folgenden n Mengen:

$$\overline{0} = 0 + n\mathbb{Z} = n\cdot\mathbb{Z} = \{n \cdot z \mid z \in \mathbb{Z}\}$$
$$\overline{1} = 1 + n\mathbb{Z} = \{1 + n\cdot z \mid z \in \mathbb{Z}\}$$
$$\overline{2} = 2 + n\mathbb{Z} = \{2 + n\cdot z \mid z \in \mathbb{Z}\} = \{z \in \mathbb{Z} \mid z \text{ hat den Rest 2 bei Division durch } n\}$$
$$\vdots \qquad\qquad \vdots$$
$$\overline{n-1} = (n-1) + n\mathbb{Z} = \{(n-1) + n\cdot z \mid z \in \mathbb{Z}\}$$

Insbesondere: $|\mathbb{Z} : n\mathbb{Z}| = n$.

Beweis:

- Sei $m \in \mathbb{Z}$ $\overset{\text{D.m.R.}}{\Longrightarrow} \exists q, r \in \mathbb{Z}: m = q\cdot n + r$ mit $0 \leq r < n$

$\Rightarrow (-r) + m = -r + n\cdot q + r = n\cdot q \in n\mathbb{Z} = \mathcal{U} \Rightarrow r \sim m \Rightarrow m \sim r \Rightarrow m \in \overline{r}$

- Ang: $\exists 0 \leq i < j \leq n-1$ mit $\overline{i} = \overline{j}$, d.h. $i \sim j \Rightarrow -i + j \in \mathcal{U} = n\cdot\mathbb{Z}$

$n-1 \geq j \geq j-i > 0$ ↯

□

Notation 24.7

- $n \geq 1$:
  - Schreibe $\mathbb{Z}_n$ statt $\mathbb{Z}/n\mathbb{Z}$
  - $\bar{a}$ schreibe auch $\bar{a}_n$
- Seien $x, y \in \mathbb{Z}$.

  Schreibe: $x \equiv y \pmod n$ "x kongruent y modulo n"

  $:\Leftrightarrow$ $n \mid x - y$

  $\Leftrightarrow$ x und y haben bei Div. m. R. durch n denselben Rest

  Damit: $\bar{a}_n = \{ x \mid x \equiv a \pmod n \}$

B) Der Satz von Lagrange

Lemma 24.9

Sei G eine Gruppe, $\mathcal{U} \leq G$ und $g \in G$.

Dann: $L_g : \mathcal{U} \longrightarrow g\mathcal{U} : u \longmapsto g \cdot u$ ist bijektiv

Insbesondere: $|\mathcal{U}| = |g\mathcal{U}|$

Beweis:

Zeige: L_g ist injektiv

Seien $u, u' \in \mathcal{U}$ mit $L_g(u) = L_g(u')$, d.h. $g \cdot u = g \cdot u'$ $\overset{KR}{\Longrightarrow}$ $u = u'$ $\Rightarrow L_g$ injektiv

Zeige: L_g ist surjektiv

Sei $x \in g\mathcal{U} \Rightarrow \exists u \in \mathcal{U}: x = g \cdot u \doteq L_g(u) \Rightarrow L_g$ ist surjektiv ☐

Satz von Lagrange 24.10

Sei G eine endliche Gruppe und $\mathcal{U} \leq G$.

Dann: $|G| = |\mathcal{U}| \cdot |G : \mathcal{U}|$. Insbesondere: $|\mathcal{U}|$ und $|G:\mathcal{U}|$ teilen von $|G|$

Beweis: $\cdot\ |G| < \infty \Rightarrow |G:U| = |G/U| < \infty$ (also $= k$)

$\Rightarrow \exists g_1, \dots, g_k \in G: \quad G/U = \{g_1U, \dots, g_kU\}$

$\Rightarrow G = g_1U \cup \dots \cup g_kU$

$\Rightarrow |G| = |g_1U| + \dots + |g_kU| \overset{24.9}{=} \underbrace{|U| + \dots + |U|}_{k\text{-mal}} = k \cdot |U| = |G:U| \cdot |U|$ ($|g_1U| = |U|$, $|g_kU| = |U|$)

∎

Korollar 24.11

Sei G eine Gruppe, $g \in G$. Setze: $o(g) := |\langle g \rangle|$ die Ordnung von g.

Wenn $|G| < \infty$, dann: $o(g) \mid |G|$.

Bem. 24.12:

Beweis: $\langle g \rangle = \{g^n \mid n \in \mathbb{Z}\} = \{g^0, g^1, \dots, g^{n-1}\}$ (Wenn $o(g) = n < \infty$)

$\Rightarrow o(g) = \inf\{k \geq 1 \mid g^k = e\} \in \mathbb{N} \cup \{\infty\}$

Bsp. 24.13

$\cdot\ S_3 = \{id, (12), (23), (13), (123), (132)\}$, $|S_3| = 3! = 6$

$\cdot\ U \leq S_3 \overset{\text{Lagrange}}{\Rightarrow} |U| \in \{1, 2, 3, 6\}$

$\cdot\ |U| = 1: \Rightarrow U = \{id\}$

$\cdot\ |U| = 6: \Rightarrow U = S_3$

$\cdot\ |U| = 2: \Rightarrow \exists\ id \neq d \in U \Rightarrow 1 \neq o(d) \mid |U| = 2$

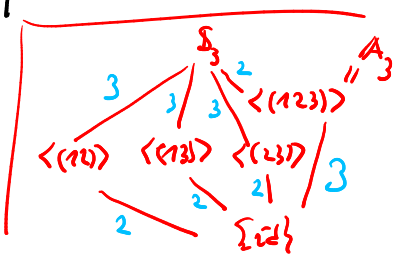
$\Rightarrow o(d) = 2 \Rightarrow d^2 = id \Rightarrow d \in \{(12), (23), (13)\}$

$\Rightarrow U = \{id, (12)\}$ ($= \langle (12) \rangle$) oder $U = \{id, (13)\}$ ($= \langle (13) \rangle$) oder $U = \{id, (23)\}$ ($= \langle (23) \rangle$)

$\cdot\ |U| = 3: \Rightarrow id \neq d \in U \Rightarrow 1 \neq o(d) \mid |U| = 3$

$\Rightarrow o(d) = 3 \Rightarrow d \in \{(123), (132)\}$

$\Rightarrow U = \langle d \rangle = \{id, (123), (132)\} = \langle (123) \rangle$



c) Faktorgruppe

Satz 24.14 Sei $(G,\cdot)$ eine abelsche Gruppe, $U \leq G$.

Dann:
- $\bar{g}\cdot\bar{h} = \overline{g\cdot h} \quad \forall g,h \in G$
- $(G/U,\cdot)$ ist eine abelsche Gruppe; die sogenannte Faktorgruppe von G modulo U
- Zudem:
  - $\bar{e} = U$ ist das Neutrale in G/U
  - $(\bar{g})^{-1} = \overline{g^{-1}}$ ist das Inverse zu $\bar{g}$ in G/U
- $\pi : G \to G/U ; g \mapsto \bar{g}$ ist ein surjektiver Gruppenhomom.

Beweis: $\bar{g}\cdot\bar{h} = gU\cdot hU \overset{\text{G abelsch}}{=} g\cdot h\cdot \underbrace{U\cdot U}_{U} = g\cdot h\cdot U = \overline{g\cdot h}$

"$\subseteq$" $u,v \in U$ ($\hat{=} u,v$)
"$\supseteq$" $u \in U \Rightarrow u = e\cdot u \in U\cdot U$ ($\hat{=} u$ $\hat{=} u$)

- zeige: $(G/U,\cdot)$ ist abelsche Gruppe
  - $(\bar{g}\cdot\bar{h})\cdot\bar{k} = \overline{g\cdot h}\cdot\bar{k} = \overline{(g\cdot h)\cdot k} = \overline{g\cdot(h\cdot k)} = \bar{g}\cdot\overline{h\cdot k} = \bar{g}\cdot(\bar{h}\cdot\bar{k})$
  - $\bar{e}\cdot\bar{g} = \overline{e\cdot g} = \bar{g} \Rightarrow \bar{e}$ ist ein Neutrales
  - $\bar{g}^{-1}\cdot\bar{g} = \overline{g^{-1}g} = \bar{e} \Rightarrow \overline{g^{-1}}$ ist das Inverse zu $\bar{g}$
  - $\bar{g}\cdot\bar{h} = \overline{g\cdot h} = \overline{h\cdot g} = \bar{h}\cdot\bar{g} \Rightarrow G$ abelsch!
  - $\pi(g\cdot h) = \overline{g\cdot h} = \bar{g}\cdot\bar{h} = \pi(g)\cdot\pi(h) \Rightarrow \pi$ ist Homom. ☐

Bem. 24.15

Rechenregeln in G/U:

1. $\bar{g}\cdot\bar{h} = \overline{g\cdot h}$
2. $\bar{g}^{-1} = \overline{g^{-1}}$
3. $\bar{e} = \bar{u} \quad \forall u \in U$ ist das Neutrale in G/U

Kor. 24.16

Für $n \in \mathbb{Z}$ ist $(\mathbb{Z}_n, +)$ eine abelsche Gruppe,

Wsbz: $\bar{x} + \bar{y} = \overline{x+y}$

Bemerkung 24.17

① Rechnen in $\mathbb{Z}_{12}$: Wenn jetzt 9 Uhr ist, wie spät ist es in 5 Stunden?

$$\bar{9} + \bar{5} = \overline{9+5} = \overline{14} = \overline{2+1\cdot 12} = \bar{2} \quad \in \mathbb{Z}_{12}$$

Also: 2 Uhr!

② Rechnen in $\mathbb{Z}_{24}$: Wenn jetzt 9 Uhr ist, wie spät war es vor 55 Stunden?

$$\bar{9} - \overline{55} = \overline{9-55} = \overline{-46} = \overline{2-2\cdot 24} = \bar{2} \quad \in \mathbb{Z}_{24}$$

Also: 2 Uhr

③ Rechnen in $\mathbb{Z}_7$: Montag = 1, Dienstag = 2, ..., Sonntag = 7

Wenn heute Montag ist, welcher Wochentag ist in 52 Tagen?

$$\bar{1} + \overline{51} = \overline{1+51} = \overline{52} = \overline{3+7\cdot 7} = \bar{3} \in \mathbb{Z}_7$$

Also: Mittwoch

Beispiel 24.18 Wenn G nur wenige Elemente hat, können wir die Operation $\cdot$ in einer Gruppentafel festhalten!

z.B.: Rechnen in $\mathbb{Z}_n$ mit $n = 2, 3, 4$

+	$\bar{0}$	$\bar{1}$
$\bar{0}$	$\bar{0}$	$\bar{1}$
$\bar{1}$	$\bar{1}$	$\bar{0}$

+	$\bar{0}$	$\bar{1}$	$\bar{2}$
$\bar{0}$	$\bar{0}$	$\bar{1}$	$\bar{2}$
$\bar{1}$	$\bar{1}$	$\bar{2}$	$\bar{0}$
$\bar{2}$	$\bar{2}$	$\bar{0}$	$\bar{1}$

+	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$
$\bar{0}$	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$
$\bar{1}$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{0}$
$\bar{2}$	$\bar{2}$	$\bar{3}$	$\bar{0}$	$\bar{1}$
$\bar{3}$	$\bar{3}$	$\bar{0}$	$\bar{1}$	$\bar{2}$

§ 25 Ringe und Körper

A) Ringe

Definition 25.1

(a) Ein **Ring mit Eins** ist eine nicht-leere Menge R mit zwei 2-stelligen Operationen $+ : R \times R \to R$ und $\cdot : R \times R \to R$, so dass folgende Axiome gelten:

(1) $(R, +)$ ist eine abelsche Gruppe mit Neutralem 0.

(2) $(a \cdot b) \cdot c = a \cdot (b \cdot c) \quad \forall a, b, c \in R$

(3) $\exists\, 1 \in R : \forall a \in R : \quad 1 \cdot a = a \cdot 1 = a$

(4) $\forall a, b, c \in R : \quad a \cdot (b + c) = a \cdot b + a \cdot c$
und $(b + c) \cdot a = b \cdot a + c \cdot a$ } Distributivgesetze

(b) Ein Ring mit Eins heißt **kommutativ**, wenn: $\forall a, b \in R : \quad a \cdot b = b \cdot a$

(c) Sei $(R, +, \cdot)$ ein Ring mit Eins und $a \in R$.
Dann: a heißt **Einheit** in R $:\Leftrightarrow \exists\, a^{-1} \in R : \; a \cdot a^{-1} = a^{-1} \cdot a = 1$

$\cdot \; R^* := \{ a \in R \mid a \text{ ist Einheit} \}$

Bsp. 25.3

(a) $(\mathbb{Z}, +, \cdot)$ ist kommutativer Ring mit 1.
Es gilt: $\mathbb{Z}^* = \{1, -1\}$

(b) Sei M eine beliebige Menge und $(R, +, \cdot)$ ein Ring mit Eins.
Setze: $\cdot \; R^M := \{ f : M \to R \mid f \text{ ist Abbildung} \}$

$\cdot \; f + g : M \to R$ mit $(f+g)(m) = f(m) + g(m) \quad \forall m \in M$

$\cdot \; f \cdot g : M \to R$ mit $(f \cdot g)(m) = f(m) \cdot g(m) \quad \forall m \in M$

Dann ist $(R^M, +, \cdot)$ ein Ring mit Eins, wobei:

$\cdot \; 0 : M \to R : m \mapsto 0$ ist das Neutrale bez. der Addition

$\cdot \; 1 : M \to R : m \mapsto 1$ ist " " " " Multipl.

(c) $\cdot\ Mat_2(\mathbb{R}) := \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \mid a,b,c,d \in \mathbb{R} \right\}$

$\cdot\ \begin{pmatrix} a & b \\ c & d \end{pmatrix} + \begin{pmatrix} a' & b' \\ c' & d' \end{pmatrix} := \begin{pmatrix} a+a' & b+b' \\ c+c' & d+d' \end{pmatrix}$

$\cdot\ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \cdot \begin{pmatrix} a' & b' \\ c' & d' \end{pmatrix} := \begin{pmatrix} a\cdot a' + b\cdot c' & a\cdot b' + b\cdot d' \\ c\cdot a' + d\cdot c' & c\cdot b' + d\cdot d' \end{pmatrix}$

Dann: $(Mat_2(\mathbb{R}), +, \cdot)$ ist ein Ring mit Eins, nicht kommutativ

mit $\cdot \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}$ als Neutralem bzg. $+$

$\cdot \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$ " " " $\cdot$

B) Rechenregeln in Ringen

Lemma 25.4

Sei R ein Ring mit Eins, dann gelten die üblichen Rechenregeln.

Insbesondere:

Wenn $1_R = 0_R$, dann gilt $R = \{0_R\}$

Beweis:

Sei $a \in R \Rightarrow a = 1_R \cdot a = 0_R \cdot a = 0_R \Rightarrow R = \{0_R\}$. ☐

Def. & Prop. 25.5:

Sei R ein Ring mit Eins und S ein Teilmenge von R.

Dann heißt S ein Unterring oder Teilring von R

$:\Leftrightarrow$ (1) $1_R \in S$ (2) $a+b \in S$ $\forall a,b \in S$

(3) $-a \in S$ $\forall a \in S$ (4) $a \cdot b \in S$ $\forall a,b \in S$

Ein Unterring ist bzg. $+$ und $\cdot$ immer selbst ein Ring.

Bsp. 25.6:

Offenbar: $(\mathbb{C}, +, \cdot)$ ist kommutativer Ring mit Eins.

Setze: $\mathbb{Z}[i] := \{ a + b \cdot i \mid a,b \in \mathbb{Z} \}$ ist ein Unterring von $\mathbb{C}$,

also selbst ein kommutativer Ring mit Eins (ganze Gaußsche Zahlen).

Denn: (1) $1 + 0 \cdot i \in \mathbb{Z}[i]$ (3) $a + b \cdot i \in \mathbb{Z}[i] \Rightarrow -(a+b\cdot i) = (-a) + (-b)\cdot i \in \mathbb{Z}[i]$

(2) & (4) Seien $(a+b\cdot i), (c+d\cdot i) \in \mathbb{Z}[i] \Rightarrow (a+b\cdot i) + (c+d\cdot i) = (a+c) + (b+d)\cdot i \in \mathbb{Z}[i]$

und $(a+b\cdot i)\cdot(c+d\cdot i) = (a\cdot c - b\cdot d) + (a\cdot d + b\cdot c)\cdot i \in \mathbb{Z}[i]$. ☐

C) Körper

Def. 25.7: Ein kommutativer Ring mit Eins $(R, +, \cdot)$ heißt ein Körper, wenn $R^* = R \setminus \{0\}$.

Bemerkung 25.8:
Sei K eine nicht-leere Menge und $+ : K \times K \to K$, $\cdot : K \times K \to K$.
Dann: $(K, +, \cdot)$ ist ein Körper
$\Leftrightarrow$ (1) $(K, +)$ ist eine abelsche Gruppe
(2) $(K \setminus \{0\}, \cdot)$ ist " abelsche Gruppe
(3) Distributivgesetze gelten.

Bsp. 25.9:
- $(\mathbb{Q}, +, \cdot)$, $(\mathbb{R}, +, \cdot)$, $(\mathbb{C}, +, \cdot)$ sind Körper
- $(\mathbb{Z}, +, \cdot)$ ist kein Körper!

Lemma 25.10
Wenn $(K, +, \cdot)$ ein Körper ist und $a, b \in K \setminus \{0\}$,
dann gilt: $a \cdot b \neq 0$.

Beweis:
$K \setminus \{0\}$ ist Gruppe bzgl. $\cdot$ $\Rightarrow$ $K \setminus \{0\}$ ist bzgl. $\cdot$ abgeschlossen,
d.h. wenn $a, b \in K \setminus \{0\}$, dann $a \cdot b \in K \setminus \{0\}$. ☐

D) Der Ring $\mathbb{Z}_n$

Satz 25.11
Die Menge $\mathbb{Z}_n = \mathbb{Z}/n\mathbb{Z} = \{\bar{0}, \bar{1}, \bar{2}, \ldots, \overline{n-1}\}$ ist mit der Addition $\bar{a} + \bar{b} = \overline{a+b}$ und der Multiplikation $\bar{a} \cdot \bar{b} = \overline{ab}$
ein kommutativer Ring mit Eins $\bar{1}$.

Beweis: • 24.6 $\Rightarrow (\mathbb{Z}_n, +)$ ist eine abelsche Gruppe

• Zeige: • $\cdot$ ist wohldefiniert, d.h. die Definition hängt nicht von den gewählten Vertretern a und b ab.

Seien $\bar{a} = \bar{c}$ und $\bar{b} = \bar{d}$

$\Rightarrow \exists\, x \in \mathbb{Z}: \quad a = c + x \cdot n$

$\exists\, y \in \mathbb{Z}: \quad b = d + y \cdot n$

$\Rightarrow a \cdot b = (c + xn) \cdot (d + yn) = c \cdot d + c \cdot y \cdot n + d \cdot x \cdot n + x \cdot n \cdot y \cdot n$

$= c \cdot d + (cy + dx + xyn) \cdot n$

$\Rightarrow \overline{a \cdot b} = \overline{c \cdot d}$

$\Rightarrow$ • ist wohldefiniert

Der Rest folgt aus $\mathbb{Z}$. ☐

Bsp. 25.12

$\bar{3}, \bar{2} \in \mathbb{Z}_6$ $\Rightarrow$ $\bar{3} \cdot \bar{2} = \overline{3 \cdot 2} = \bar{6} = \bar{0} \in \mathbb{Z}_6$

$\bar{3} \neq \bar{0}$, $\bar{2} \neq \bar{0}$

$\Rightarrow$ $\mathbb{Z}_6$ ist kein Körper

Korollar 25.13

$\mathbb{Z}_n$ ist ein Körper $\Leftrightarrow$ n ist Primzahl

Beweis:

"$\Rightarrow$" Sei n keine Primzahl $\Rightarrow n = a \cdot b$ mit $1 < a, b < n$

$\Rightarrow \bar{a}, \bar{b} \neq \bar{0}$ und $\bar{a} \cdot \bar{b} = \overline{a \cdot b} = \bar{n} = \bar{0}$

$\Rightarrow \mathbb{Z}_n$ ist kein Körper. $\lightning$

"$\Leftarrow$" Sei n eine Primzahl und $\bar{a} \in \mathbb{Z}_n$, $0 < a \leq n-1$

zu zeigen: $\bar{a}$ hat ein multiplikatives Inverses

Definition: $\alpha : \mathbb{Z}_n \longrightarrow \mathbb{Z}_n \; ; \; \bar{x} \longmapsto \bar{a} \cdot \bar{x} = \overline{a \cdot x}$

Angenommen $\bar{x}, \bar{y} \in \mathbb{Z}_n$ mit $0 \le y < x \le n-1$ und $\alpha(\bar{x}) = \alpha(\bar{y})$

$\Rightarrow \quad \overline{a \cdot x} = \overline{a \cdot y} \quad \Rightarrow \quad n$ teilt $a \cdot x - a \cdot y$

$a \cdot (x-y)$

$\Rightarrow$ die Primzahl n kommt in der Primfaktorzerlegung von $a \cdot (x-y)$ vor

$0 < x - y \le n-1$ (wird nicht von n geteilt)

$0 < a \le n-1$ (wird nicht von n geteilt)

Also: α ist injektiv

$\Rightarrow$ ($\uparrow$ wie $\mathbb{Z}_n$ endlich + 5.6) α ist surjektiv $\Rightarrow \exists \bar{x} : \alpha(\bar{x}) = \bar{1}$

$\bar{a} \cdot \bar{x} = \bar{x} \cdot \bar{a}$

$\bar{x} = \bar{a}^{-1}$

∎

Beispiel 25.14

- $\mathbb{F}_2 = \{0, 1\} \xrightarrow{\cong} \mathbb{Z}_2 = \{\bar{0}, \bar{1}\}$
  $0 \longmapsto \bar{0}$
  $1 \longmapsto \bar{1}$

- $\mathbb{F}_p = \{0, 1, \dots, p-1\} \xrightarrow{\cong} \mathbb{Z}_p = \{\bar{0}, \dots, \overline{p-1}\}$
  $a \longmapsto \bar{a}$

  (p: Primzahl)

Beispiel 25.6 (d): Sei R ein kommutativer Ring mit Eins.

Dann heißt ein formaler Ausdruck der Form

$\sum_{k=0}^{\infty} a_k \cdot t^k$ mit $a_k \in R$ und t eine Veränderliche

eine formale Potenzreihe mit Koeffizienten a_k in R.

Setze:
$$R[[t]] := \left\{ \sum_{k=0}^{\infty} a_k \cdot t^k \mid a_k \in R \right\} = \text{Menge aller Potenzreihen über } R$$

- $\sum_{k=0}^{\infty} a_k \cdot t^k + \sum_{k=0}^{\infty} b_k \cdot t^k := \sum_{k=0}^{\infty} (a_k + b_k) \cdot t^k$
- $\sum_{k=0}^{\infty} a_k \cdot t^k \cdot \sum_{l=0}^{\infty} b_l \cdot t^l := \left(\sum_{k=0}^{\infty} \sum_{l=0}^{\infty} a_k \cdot b_l \cdot t^{k+l} \right) = \sum_{n=0}^{\infty} \left(\sum_{k+l=n} a_k \cdot b_l \right) \cdot t^n$
  $\sum_{k=0}^{n} a_k \cdot b_{n-k}$
- $\sum_{k=0}^{\infty} a_k \cdot t^k = \sum_{k=0}^{\infty} b_k \cdot t^k \iff a_k = b_k \quad \forall k = 0, \dots, \infty$

Damit: $(R[[t]], +, \cdot)$ ist ein kommutativer Ring mit $1_{R[[t]]} = t^0$

Kurzschreibweise: Wenn $a_k = 0$ für alle $k \geq n+1$, dann schreibe $\sum_{k=0}^{n} a_k \cdot t^k$ statt $\sum_{k=0}^{\infty} a_k \cdot t^k$

---

§ 26 Der Polynomring $K[t]$

In diesem Abschnitt sei K stets ein Körper.

A) Grundlegende Eigenschaften von $K[t]$

Def 26.1

Eine formale Potenzreihe der Form $\sum_{k=0}^{n} a_k \cdot t^k \in K[[t]]$ heißt ein **Polynom** mit Koeffizienten in K in der Veränderlichen t.

Die Menge aller solcher Polynome
$$K[t] := \left\{ \sum_{k=0}^{n} a_k \cdot t^k \mid a_k \in K, \ n \in \mathbb{N} \right\}$$
heißt der **Polynomring** über K in t.

Bem. 26.2 Die Addition und Multiplikation auf $K[t]$ liefert für Polynome $\sum_{k=0}^{n} a_k \cdot t^k$ und $\sum_{k=0}^{m} b_k \cdot t^k$:

$$\sum_{k=0}^{n} a_k \cdot t^k + \sum_{k=0}^{m} b_k \cdot t^k = \sum_{k=0}^{\max\{m,n\}} (a_k + b_k) \cdot t^k$$

($a_k = 0 \ \forall k > n$, $b_k = 0 \ \forall k > m$)

$$\sum_{k=0}^{n} a_k \cdot t^k \cdot \sum_{\ell=0}^{m} b_\ell \cdot t^\ell = \sum_{i=0}^{n+m} \left(\sum_{k+\ell=i} (a_k \cdot b_\ell) \right) \cdot t^i$$

$a_n \cdot b_m$ // $i = n+m$

$$= \sum_{i=0}^{n+m} \left(\sum_{k=0}^{i} a_k \cdot b_{i-k} \right) \cdot t^i$$

Prop. 26.3
$K[t]$ ist ein Unterring von $K\{t\}$, insbesondere ist $K[t]$ ein kommutativer Ring mit Eins $1 = t^0$.

Bemerkung 26.4
Schreibe $3t^2 + 2t + 5$ statt $3t^2 + 2t^1 + 5t^0$.

Def. 26.5
Sei $f = \sum_{k=0}^{n} a_k \cdot t^k$ mit $a_n \neq 0$, dann heißt $\deg(f) := n$ der Grad von f und $lc(f) := a_n$ der Leitkoeffizient von f.

Setze: $\deg(0) := -\infty$ und $lc(0) := 0$.

Wenn $lc(f) = 1$, heißt f normiert.

Bem. 26.6: $\deg(f) \leq 0 \iff f$ ist ein konstantes Polynom „$a_0 \cdot t^0$ für ein $a_0 \in K$"

Lemma 26.7: (Gradformeln)
Sei $f, g \in K[t] \setminus \{0\}$
Dann:
$$\deg(f+g) \leq \max\{\deg(f), \deg(g)\}$$
$$\deg(f \cdot g) = \deg(f) + \deg(g)$$

Bsp. 16.8:

$f = 2t+1$, $g = -2t+1 \in \mathbb{Q}[t]$

$\Rightarrow$ $f+g = 2$, $d_g(f+g) = 0 < 1 = \max\{d_g(f), d_g(g)\}$

$f \cdot g = (2t+1)\cdot(-2t+1) = -4t^2+1$, $d_g(f\cdot g) = 2$

$= d_g(f) + d_g(g)$