Lineare Algebra 2

–

Algebraische Strukturen

Algebraische Strukturen in Linearer Algebra 1

- **Gruppen**: $(G, \cdot)$ – G Menge, $\cdot : G \times G \to G$ Ass: Klung
- **Körper**: $(K, +, \cdot)$ – K Menge, $+/\cdot : K \times K \to K$ Ass: Klungen
- **Ring**: $(R, +, \cdot)$ – R Menge, $+/\cdot : R \times R \to R$ "
- **k-Vektorraum**: $(V, +, \cdot)$ – V Menge, $+ : V \times V \to V$ Ass: Klung
  $\cdot : K \times V \to V$ "
- **K-Algebra**: $(A, +, 0, \cdot)$ – A Menge, $+/0 : A \times A \to A$ "
  $\cdot : K \times A \to A$ "

§1 Gruppen und Gruppenhomomorphismen

Def. 1.1:

(a) Eine **Gruppe** ist ein Tupel $(G, \cdot)$, wobei $G \neq \emptyset$ eine Menge und $\cdot : G \times G \to G$ eine Abbildung ist, so daß:

(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)

(b) $(G, \cdot)$ heißt **abelsch** $:\Leftrightarrow \forall\, g, h \in G : g \cdot h = h \cdot g$ (Kommutativgesetz)

(c) $|G|$ heißt die **Ordnung** von $(G, \cdot)$

(d) $(G, \cdot)$ heißt **endlich** $:\Leftrightarrow |G| < \infty$

Beispiele 1.2:

(a) $(\mathbb{Z}, +)$, $(\mathbb{Q}, +)$, $(\mathbb{R}, +)$, $(\mathbb{C}, +)$ sind abelsche Gruppen.

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

(c) $(\mathbb{Z}\setminus\{0\}, \cdot)$ ist **keine** Gruppe!
-1 ist ein Neutrales, aber 2 hat kein Inverses in $\mathbb{Z}\setminus\{0\}$!

(d) $G = \{e\}$ wird mit $e \cdot e = e$ eine abelsche Gruppe!

(e) $M \neq \emptyset$ Menge und $\mathrm{Sym}(M) := \{f : M \to M \mid f \text{ bijektiv}\}$
$\Rightarrow (\mathrm{Sym}(M), \circ)$ ist eine Gruppe, nicht-abelsch für $|M| \geq 3$

Lemma 1.3: Sei $(G, \cdot)$ eine Gruppe.

(a) $g' \cdot g = e \Rightarrow g \cdot g' = e$

(b) $e \in G$ mit $e \cdot g = g \ \forall g \in G \Rightarrow g \cdot e = g \ \forall g \in G$

(c) $\exists_1 e \in G : \forall g \in G : e \cdot g = g$ Eindeutigkeit des Neutralen

(d) $\forall g \in G \ \exists_1 g' \in G : g' \cdot g = e$ Eindeutigkeit des Inversen

Beweis:

(a) Zeige: $g' \cdot g = e \Rightarrow g \cdot g' = e$

(G3) $\Rightarrow \exists g'' \in G : g'' \cdot g' = e$

$\Rightarrow g \cdot g' \overset{(G2)}{=} e \cdot (g \cdot g') \overset{}{=} (g'' \cdot g') \cdot (g \cdot g') \overset{(G1)}{=} g'' \cdot (g' \cdot (g \cdot g'))$

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

(b) Zeige: $\forall g \in G : g \cdot e = g$

(G3) $\Rightarrow \exists g' \in G : g' \cdot g = e$

$\Rightarrow g \cdot e = g \cdot (g' \cdot g) \overset{(G1)}{=} (g \cdot g') \cdot g \overset{(a)}{=} e \cdot g \overset{(G2)}{=} g$

(c) Zeige: $e, \tilde{e} \in G : \forall g \in G : e \cdot g = \tilde{e} \cdot g = g \Rightarrow e = \tilde{e}$

$e = \tilde{e} \cdot e \overset{(b)}{=} \tilde{e}$

(d) Zeige: $g', g'' \in G : g' \cdot g = g'' \cdot g = e \Rightarrow g' = g''$

$g'' \overset{(b)}{=} g'' \cdot e = g'' \cdot (g' \cdot g) \overset{(a)}{=} g'' \cdot (g \cdot g') \overset{(G1)}{=} (g'' \cdot g) \cdot g' = e \cdot g' = g'$

Notation 1.4: Sei $(G, \cdot)$ eine Gruppe.

Dann:
- e_G oder 1_G bezeichnet das Neutrale
- g_G^{-1} bezeichnet das Inverse zu g
- Bezeichnen wir die Gruppenoperation mit $+$,

  dann: $\cdot$ 0_G bezeichnet das Nullpaar
  $\cdot$ $-g_G$ " " Inverse zu g.
- Schreibe meist nur: $e, 1, 0, g^{-1}, -g$

  sowie: gh statt $g \cdot h$.

Lemma 1.5:

Sei $(G, \cdot)$ eine Gruppe und $g, h, a, b \in G$.

Dann gelten:
- (a) $(g^{-1})^{-1} = g$
- (b) $(g \cdot h)^{-1} = h^{-1} \cdot g^{-1}$
- (c) $g \cdot a = g \cdot b \Rightarrow a = b$
  $a \cdot g = b \cdot g \Rightarrow a = b$

  } Kürzungsregeln

Beweis:

(c) Wurde schon in LA 1 bewiesen.

(a) Zeige: $(g^{-1})^{-1} = g$.

$g \cdot g^{-1} \overset{1.3}{=} e \overset{1.3}{\Rightarrow} g = (g^{-1})^{-1}$

$h^{-1} \cdot g^{-1} = (g \cdot h)^{-1}$ // 1.3

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

$(h^{-1} \cdot g^{-1}) \cdot (g \cdot h) \overset{G1}{=} h^{-1} \cdot (g^{-1} \cdot (g \cdot h)) \overset{G1}{=} h^{-1} \cdot ((g^{-1} \cdot g) \cdot h) \overset{G3}{=} h^{-1} \cdot (e \cdot h) \overset{G1}{=} h^{-1} \cdot h \overset{G2}{=} e$

Definition 1.6 (Potenzen)

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

Dann definieren wir:
- $g^0 := e$, sowie rekursiv
- $g^n := g \cdot g^{n-1}$ für $n \geq 1$
- $g^{-n} := (g^{-1})^n$ für $n \geq 1$

Bemerkung 1.8 (Potenzgesetze)

(a) $g^n \cdot g^m = g^{n+m}$ (b) $(g^n)^m = g^{n \cdot m}$

Def. 1.9:

Sei $(G, \cdot)$ eine Gruppe und $\emptyset \neq U \subseteq G$.

U heißt Untergruppe von G

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

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

Notation: $U \leq G$.

Proposition 1.10:

$U \leq G \Leftrightarrow U$ ist bez. $\cdot$ selbst eine Gruppe.

Beweis: "$\Rightarrow$"
- $U \neq \emptyset$, nach Voraussetzung
- $U \leq G \Rightarrow \forall u, v \in U : u \cdot v \in U$
  $\Rightarrow U \times U \longrightarrow U : (u, v) \mapsto u \cdot v \Rightarrow$ "$\cdot$" ist eine 2-stellige Op. auf U
  $\equiv$
- (G1) Seien $u, v, w \in U \Rightarrow u \cdot (v \cdot w) = (u \cdot v) \cdot w$ gilt schon in G
- (G2) $U \neq \emptyset \Rightarrow \exists u \in U \Rightarrow u_G^{-1} \in U \Rightarrow e_G = u_G^{-1} \cdot u \in U$
  Damit: $\forall v \in U : e_G \cdot v = v \Rightarrow e_G$ ist Neutrales in U
  $\Rightarrow e_G = e_U$

• (G3) Sei $u \in U \leq G \Rightarrow \exists\, u_G^{-1} \in G : u_G^{-1} \cdot u = e_G = e_U$

Weil $U \leq G$, gilt schon: $u_G^{-1} \in U \Rightarrow u_G^{-1} = u_U^{-1}$

. Also: U bzgl. $\cdot$ eine Gruppe.

"$\Leftarrow$" ÜA. ☐

Beisp: zu 1.11:

(a) $(G, \cdot)$ Gruppe $\Rightarrow \{e_G\}$ und G sind Untergruppen von G, die triviale Untergruppen.

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

(c) $G = Sym(\mathbb{R}^2) = \{f : \mathbb{R}^2 \to \mathbb{R}^2 \mid f \text{ bijektiv}\}$

Sei für $\alpha \in \mathbb{R}$: $\varphi_\alpha : \mathbb{R}^2 \to \mathbb{R}^2$ Drehung um den Ursprung um den Winkel α im Gegenuhrzeigersinn

Beachte: • φ_α ist bijektiv, mit $\varphi_\alpha^{-1} = \varphi_{-\alpha}$

• $\varphi_\alpha \circ \varphi_\beta = \varphi_{\alpha+\beta}$

• $\varphi_0 = id_{\mathbb{R}^2}$

Also: $SO(2) := \{\varphi_\alpha \mid \alpha \in \mathbb{R}\}$ ist eine Untergruppe von $Sym(\mathbb{R}^2)$.

(d) $G = \mathbb{Z}$ mit $+$ als Gruppenoperation.

Sei $u \in \mathbb{Z}$ fest gegeben. Dann:

$u \cdot \mathbb{Z} := \{u \cdot z \mid z \in \mathbb{Z}\} \leq \mathbb{Z}$.

Denn: • $0 = u \cdot 0 \in u \cdot \mathbb{Z} \Rightarrow u \cdot \mathbb{Z} \neq \emptyset$ und $u\mathbb{Z} \subseteq \mathbb{Z}$

• $u \cdot z,\ u \cdot \tilde{z} \in u \cdot \mathbb{Z} \Rightarrow u \cdot z + u \cdot \tilde{z} = u \cdot (z + \tilde{z}) \in u\mathbb{Z}$

• $u \cdot z \in u \cdot \mathbb{Z} \Rightarrow -(u \cdot z) = u \cdot (-z) \in u \cdot \mathbb{Z}$ ☐

Beachte: $u \cdot \mathbb{Z} \subseteq m \cdot \mathbb{Z} \iff m \mid u$

Lemma 1.12:

Sei $(G,\cdot)$ eine Gruppe, $U_i \leq G$ für $i \in I$.

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

Beweis: Ü A $\square$

Bemerkung 1.13:

$U, V \leq G \;\not\Longrightarrow\; U \cup V \leq G$

Denn: $U = 2\cdot\mathbb{Z},\; V = 3\cdot\mathbb{Z} \leq \mathbb{Z}$, $2 \in 2\cdot\mathbb{Z}$, $3 \in 3\cdot\mathbb{Z}$

aber: $2 + 3 = 5 \notin 2\cdot\mathbb{Z} \cup 3\mathbb{Z}$

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

Definition 1.14:

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

Dann heißt: $\langle M \rangle := \bigcap_{\substack{U \leq G \\ M \subseteq U}} U$ das Erzeugnis von M in G.

Beachte: $1.12 \Rightarrow \langle M \rangle \leq G$ ist die kleinste Untergruppe von G, die M enthält

Proposition 1.15: Sei $(G,\cdot)$ eine Gruppe, $M \subseteq G$.

Dann: $\langle M \rangle = \underbrace{\{e_G\} \cup \{g_1^{\alpha_1} \cdot \ldots \cdot g_n^{\alpha_n} \mid g_i \in M, \alpha_i \in \mathbb{Z}, n \in \mathbb{N}, n \geq 1\}}_{=:N}$

Beweis: "$\supseteq$" Sei $U \leq G$ mit $M \subseteq U$. Zeige: $N \subseteq U$

• $e_G \in U$ • $g_1, \dots, g_n \in \Pi \subseteq U$ und $\alpha_1, \dots, \alpha_n \in \mathbb{Z}$

$\Rightarrow g_1^{\alpha_1} \cdots g_n^{\alpha_n} \in U$

• Damit: $N \subseteq U \Rightarrow N \subseteq \bigcap_{\substack{U \leq G \\ \Pi \subseteq U}} U = \langle \Pi \rangle$

"$\subseteq$" Zeige: $N \leq G$ mit $\Pi \subseteq N$ (und damit: $\langle \Pi \rangle \subseteq N$)

• $g \in \Pi \Rightarrow g = g^1 \in N \Rightarrow \Pi \subseteq N$

• $e_G \in N \Rightarrow N \neq \emptyset$ und $N \subseteq G$

• Sei $u \in N \Rightarrow u = e_G$ oder $u = g_1^{\alpha_1} \cdots g_n^{\alpha_n}$

$\Rightarrow u^{-1} = e_G \in N$ oder $u^{-1} = g_n^{-\alpha_n} \cdots g_1^{-\alpha_1} \in N$

• Seien $u, v \in N \Rightarrow (u = e_G$ oder $u = g_1^{\alpha_1} \cdots g_n^{\alpha_n})$

und $(v = e_G$ oder $v = h_1^{\beta_1} \cdots h_m^{\beta_m})$

$\Rightarrow u \cdot v \in \{e_G, h_1^{\beta_1} \cdots h_m^{\beta_m}, g_1^{\alpha_1} \cdots g_n^{\alpha_n}, g_1^{\alpha_1} \cdots g_n^{\alpha_n} \cdot h_1^{\beta_1} \cdots h_m^{\beta_m}\} \subseteq N$ ☐

Beispiel 1.16:

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

Dann: $\langle g \rangle \overset{1.15}{=} \{g^k \mid k \in \mathbb{Z}\}$, dabei $g^k = \underbrace{g \cdot g \cdots g}_{k\text{-mal}}$

Beachte: $(\mathbb{Z}, +)$ und $n \in \mathbb{Z}$

$\Rightarrow \langle n \rangle = \{n \cdot k \mid k \in \mathbb{Z}\}$, $n \cdot k = \underbrace{n + n + \cdots + n}_{k\text{-mal}}$

$= n \cdot \mathbb{Z}$

Definition 1.17:

Eine Gruppe $(G, \cdot)$ heißt zyklisch, wenn es ein $g \in G$ gibt, so daß $G = \langle g \rangle$.

Bemerkung 1.18:

(a) **Division mit Rest:**

$\forall m, n \in \mathbb{Z},\ n \neq 0 \quad \exists_1\ q, r \in \mathbb{Z}: \quad m = q \cdot n + r \quad \text{mit } 0 \leq r < |n|$

(b) **Archimedisches Prinzip:**

jede nicht-leere Menge natürlicher Zahlen besitzt ein kleinstes Element.

Proposition 1.19: Sei $\mathcal{U} \subseteq \mathbb{Z}$. Dann gilt:

$\mathcal{U} \leq \mathbb{Z} \iff \exists\, u \in \mathbb{Z}: \mathcal{U} = u \cdot \mathbb{Z}$

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

Beweis: "$\Leftarrow$" $\mathcal{U} = u \cdot \mathbb{Z} \overset{1.11}{\Rightarrow} \mathcal{U} \leq \mathbb{Z}$

"$\Rightarrow$" Sei $\mathcal{U} \leq \mathbb{Z}$. 1. Fall: $\mathcal{U} = \{0\} \Rightarrow \mathcal{U} = 0 \cdot \mathbb{Z}$

2. Fall: $\mathcal{U} \neq \{0\}$

$\Rightarrow \exists\, m \in \mathcal{U},\ m \neq 0 \Rightarrow -m \in \mathcal{U}$ und $(m > 0$ oder $-m > 0)$

$\Rightarrow \exists\, u := \min \underbrace{\{m \in \mathcal{U} \mid m > 0\}}_{\subseteq \mathbb{N},\ \neq \emptyset} > 0$

Zeige: $\mathcal{U} = u \cdot \mathbb{Z}$.

"$\supseteq$" $u \cdot k \in u \cdot \mathbb{Z}$ mit $k \in \mathbb{Z} \Rightarrow u \cdot k \in \mathcal{U} \Rightarrow u \cdot \mathbb{Z} \subseteq \mathcal{U}$

"$\subseteq$" Sei $a \in \mathcal{U} \overset{\text{Div. R.}}{\Rightarrow} \exists\, q, r \in \mathbb{Z}: a = q \cdot u + r$ mit $0 \leq r < u$

$\Rightarrow r = a - q \cdot u \in \mathcal{U}$ und $0 \leq r < u$

($a \in \mathcal{U}$, $q \cdot u = u \cdot q \in \mathcal{U}$)

$\Rightarrow r = 0$, wegen Minimalität von u!

$\Rightarrow a = q \cdot u = u \cdot q \in u\mathbb{Z}$. ∎

Homomorphismen ≙ strukturerhaltende Abbildungen

Erinnerung: $(V,+,\cdot)$ und $(W,+,\cdot)$ K-Vektorräume

$f: V \to W$ K-linear $\iff$ $f(x+y) = f(x) + f(y)$

$f(\lambda \cdot x) = \lambda \cdot f(x)$

für alle $x, y \in V$, $\lambda \in K$

K-Vektorraum-Homomorphismus

Def. 1.20:

Seien $(G,\cdot)$ & $(H,*)$ zwei Gruppen.

$\alpha: G \to H$ heißt Gruppenhomomorphismus

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

Bsp. 1.21:

(a) Sei $(G,\cdot)$ und $U \leq G$.

$i_U: U \to G: u \mapsto u$ ist ein GH.

denn: $u, v \in U \Rightarrow i_U(u \cdot v) = u \cdot v = i_U(u) \cdot i_U(v)$.

(b) $a \in \mathbb{R} \Rightarrow m_a: \mathbb{R} \to \mathbb{R}: x \mapsto a \cdot x$ ist ein GH.

für $(\mathbb{R},+)$

denn: $m_a(x+y) = a \cdot (x+y) = a \cdot x + a \cdot y = m_a(x) + m_a(y)$

(c) Allgemein: $f: V \to W$ K-linear

$\Rightarrow f: (V,+) \to (W,+)$ ist G.H.

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

Dann: $L_g : G \to G : h \mapsto g \cdot h$
$R_g : G \to G : h \mapsto h \cdot g$
} keine G.H., wenn $g \neq e$

denn: $L_g(g \cdot g) = g^3 \neq g^4 = g^2 \cdot g^2 = L_g(g) \cdot L_g(g)$

↑ Kürzungsregel und $e \neq g$

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

Definiere: $i_g : G \to G : h \mapsto g \cdot h \cdot g^{-1}$

heißt Konjugation mit g

Beh: i_g ist ein bijektiver GH. mit $(i_g)^{-1} = i_{g^{-1}}$

Denn: Zeige: $i_g(h \cdot k) = i_g(h) \cdot i_g(k)$

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

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

Zeige: $(i_g \circ i_{g^{-1}}) = id_G$. Sei dazu $h \in G$

$\Rightarrow (i_g \circ i_{g^{-1}})(h) = i_g(i_{g^{-1}}(h)) = i_g((g^{-1}) \cdot h \cdot (g^{-1})^{-1}) =$

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

Analog: $i_{g^{-1}} \circ i_g = id_G$

$\Rightarrow i_g$ ist bijektiv mit $(i_g)^{-1} = i_{g^{-1}}$

Bemerke: $i_g = R_g \circ L_{g^{-1}}$

Also: Komposition von zwei Nicht-Homomorphismen kann ein Homomorphismus werden!

Lemma 1.22: $\alpha_1 : (G_1, \cdot) \to (G_2, *)$ und $\alpha_2 : (G_2, *) \to (G_3, \times)$ seien GH. $\Rightarrow$ $\alpha_2 \circ \alpha_1 : G_1 \to G_3$ ist ein GH.

Beweis: Seien $g, h \in G_1$.

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

$\Rightarrow$ $\alpha_2 \circ \alpha_1$ ist ein G.H. ☐

Def. 1.23: Sei $\alpha : (G, \cdot) \to (H, *)$ ein GH.

Dann: (a) α heißt Homomorphismus $:\Leftrightarrow$ α ist injektiv
(b) α " Epimorphismus $:\Leftrightarrow$ α ist surjektiv
(c) α " Isomorphismus $:\Leftrightarrow$ α ist bijektiv
(d) α " Endomorphismus $:\Leftrightarrow$ $(G, \cdot) = (H, *)$
(e) α " Automorphismus $:\Leftrightarrow$ α bijektiver Endomorphismus
(f) $(G, \cdot)$ und $(H, *)$ heißen isomorph
$:\Leftrightarrow \exists\ \alpha : (G, \cdot) \to (H, *)$ Isomorphismus

Bsp. 1.24:
(a) $0 \neq a \in \mathbb{R}$ $\Leftrightarrow$ m_a ein Isomorphismus mit $m_a^{-1} = m_{\frac{1}{a}}$
(b) $(G, \cdot)$ Gruppe und $g \in G$ $\Rightarrow$ i_g ist ein Automorphismus mit $(i_g)^{-1} = i_{g^{-1}}$

ⓒ $GL_n(K) = \{ A \in Mat_n(K) \mid A \text{ ist invertierbar} \}$

$\Rightarrow \det : (GL_n(K), \cdot) \longrightarrow (K \setminus \{0\}, \cdot)$

ist ein Epimorphismus (Determinanten-Multiplikationssatz)

Proposition 1.25: Sei $\alpha : (G, \cdot) \longrightarrow (H, *)$ ein G.H.

ⓐ $\alpha(e_G) = e_H$

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

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

ⓓ α bijektiv $\Rightarrow \alpha^{-1} : H \to G$ ist G.H.

ⓔ $U \leq G \Rightarrow \alpha(U) \leq H$. Insb.: $\mathrm{Im}(\alpha) = \alpha(G) \leq H$

ⓕ $V \leq H \Rightarrow \alpha^{-1}(V) \leq G$ Insb.: $\alpha^{-1}(\{e_H\}) \leq G$

$\ker(\alpha)$ Kern von α

Beweis: ⓐ $e_H * \alpha(e_G) = \alpha(e_G) = \alpha(e_G \cdot e_G) = \alpha(e_G) * \alpha(e_G) \overset{KR}{\Rightarrow} e_H = \alpha(e_G)$

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

ⓒ Sei zunächst $n \geq 0$. Zeige mit Induktion: $\alpha(g^n) = \alpha(g)^n$

$n = 0$: $\alpha(g^0) = \alpha(e_G) \overset{ⓐ}{=} e_H = \alpha(g)^0$ ✓

$n \to n+1$: $\alpha(g^{n+1}) = \alpha(g^n \cdot g) = \alpha(g^n) * \alpha(g) \overset{Ind.}{=} \alpha(g)^n * \alpha(g)$

$= \alpha(g)^{n+1}$

Sei $n > 0$: $\alpha(g^{-n}) = \alpha(g^{(-1)\cdot n}) = \alpha((g^{-1})^n) \overset{(n>0)}{=} \alpha(g^{-1})^n$

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

(d) Sei α bijektiv und $u, v \in H$.

Zeige: $\alpha^{-1}(u * v) = \alpha^{-1}(u) \cdot \alpha^{-1}(v)$.

Setze $g := \alpha^{-1}(u) \in G$ und $h := \alpha^{-1}(v) \in G$

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

Damit: $\alpha^{-1}(u * v) = \alpha^{-1}(\alpha(g) * \alpha(h)) \overset{\alpha \text{ G.H.}}{=} \alpha^{-1}(\alpha(g \cdot h))$

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

(e) Sei $\mathcal{U} \leq G$. Zeige: $\alpha(\mathcal{U}) \leq H$.

* $\mathcal{U} \neq \emptyset \Rightarrow \alpha(\mathcal{U}) \neq \emptyset$

* Seien $u, v \in \alpha(\mathcal{U}) \Rightarrow \exists\, g, h \in \mathcal{U} : u = \alpha(g), v = \alpha(h)$

$\Rightarrow u * v = \alpha(g) * \alpha(h) \overset{\alpha \text{ GH.}}{=} \alpha(g \cdot h) \in \alpha(\mathcal{U})$ ($g \cdot h \in \mathcal{U}$)

* Sei $u \in \alpha(\mathcal{U}) \Rightarrow \exists\, g \in \mathcal{U} : u = \alpha(g)$

$\Rightarrow u^{-1} = \alpha(g)^{-1} = \alpha(g^{-1}) \in \alpha(\mathcal{U})$ ($g^{-1} \in \mathcal{U}$)

(f) Sei $V \leq H$. Zeige: $\alpha^{-1}(V) \leq G$

* $V \leq H \Rightarrow e_H \in V \Rightarrow e_G \in \alpha^{-1}(\{e_H\}) \subseteq \alpha^{-1}(V) \Rightarrow \alpha^{-1}(V) \neq \emptyset$

* $g, h \in \alpha^{-1}(V) \Rightarrow \alpha(g), \alpha(h) \in V \Rightarrow \alpha(g) * \alpha(h) \in V$

$\alpha(g) * \alpha(h) = \alpha(g \cdot h)$

$\Rightarrow g \cdot h \in \alpha^{-1}(V)$

* $g \in \alpha^{-1}(V) \Rightarrow \alpha(g) \in V \Rightarrow \alpha(g)^{-1} \in V$

$\alpha(g)^{-1} = \alpha(g^{-1})$

$\Rightarrow g^{-1} \in \alpha^{-1}(V)$

☑

Lemma 1.26: Sei $\alpha : (G, \cdot) \to (H, *)$ ein G.H.

Dann: α ist injektiv $\iff$ $\ker(\alpha) = \{e_G\}$

Bew: "$\Rightarrow$" $g \in \ker(\alpha) \Rightarrow \alpha(g) = e_H \overset{!}{=} \alpha(e_G)$

$\overset{\alpha \text{ inj.}}{\Rightarrow} g = e_G \Rightarrow \ker(\alpha) = \{e_G\}$

"$\Leftarrow$" Sei $g, h \in G$: $\alpha(g) = \alpha(h)$

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

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

$\Rightarrow g \cdot h^{-1} = e_G \to g = h$ d.h. α ist injektiv. ☐

§2 Äquivalenzrelationen

Motivation 2.0:

- **Erinnerung:** Sei M eine Menge. Eine Familie $(M_i)_{i \in I}$ heißt eine **Partition** oder **disjunkte Zerlegung** von M, wenn
  ① $M = \bigcup_{i \in I} M_i$ und
  ② $M_i \cap M_j = \emptyset$ $\forall\, i, j \in I$ mit $i \neq j$

  Notation: $M = \dot{\bigcup}_{i \in I} M_i$

- **Ziel:** Teile die Elemente der Menge M nach geeigneten Gesichtspunkten in Schubladen ein, so daß jedes Element von M in genau einer Schublade ist.

- **Beispiel:**
  $M = \{$ Teilnehmer an der Übung zur Algebraischen Strukturen $\}$
  $M_i = \{$ Teilnehmer an Übungsgruppe Nr. $i\}$, $i = 1, \dots, 6$

- **Frage:**
  Was sind die wesentlichen Prinzipien, die bei der Einteilung beachtet werden müssen?

- **Antwort:** Für je drei Teilnehmer Alfred, Ben, Christoph gilt:
  ① Alfred ist in einer Übungsgruppe.
  ② Wenn Alfred in Bens Gruppe ist, ist Ben in Alfreds Gruppe.
  ③ Wenn Alfred in Bens Gruppe ist und Ben in Christophs Gruppe, dann ist Alfred auch in Christophs Gruppe.

Definition 2.1:

Sei M eine Menge und $R \subseteq M \times M$.

Dann heißt R eine Äquivalenzrelation auf M, wenn

(R1) $\forall x \in M : (x,x) \in R$ "Reflexivität"

(R2) $\forall x,y \in M$ mit $(x,y) \in R$ gilt: $(y,x) \in R$ "Symmetrie"

(R3) $\forall x,y,z \in M$ mit $(x,y), (y,z) \in R$ gilt: $(x,z) \in R$ "Transitivität"

Schreibweise: $x \sim y :\Leftrightarrow (x,y) \in R$.

Dann: (R1) $\forall x \in M : x \sim x$

(R2) $x \sim y \Rightarrow y \sim x$

(R3) $x \sim y \wedge y \sim z \Rightarrow x \sim z$

Wir nennen dann auch $\sim$ eine Äquivalenzrelation.

Die Menge $\bar{x} := \{y \in M \mid y \sim x\} = \{y \in M \mid (y,x) \in R\}$

heißt die Äquivalenzklasse von x.

Die Menge aller Äquivalenzklassen bez. $\sim$ sei $M/\sim := \{\bar{x} \mid x \in M\}$.

Beispiel 2.2:

(a) $M = \dot{\bigcup}_{i \in I} M_i$, dann definieren wir:

$x \sim y :\Leftrightarrow \exists i \in I : x,y \in M_i$

(R1) $x \in M \Rightarrow \exists i \in I : x \in M_i \Rightarrow x,x \in M_i \Rightarrow x \sim x$

(R2) $x \sim y \Rightarrow \exists i \in I : x,y \in M_i \Rightarrow y,x \in M_i \Rightarrow y \sim x$

(R3) $x \sim y, y \sim x \Rightarrow \exists i,j \in I : x,y \in M_i \wedge y,z \in M_j$

$\Rightarrow y \in M_i \cap M_j \neq \emptyset \Rightarrow M_i = M_j \Rightarrow x,z \in M_i \Rightarrow x \sim z$

Klar: $X \in \Pi_{\cdot} \Rightarrow \overline{X} = \Pi_{\cdot}$

(b) $\Pi = \mathrm{Mat}(m \times n, K)$, $A, B \in \Pi$

$A \sim B :\Leftrightarrow \exists\, T \in Gl_m(K),\ S \in Gl_n(K) : A = T \circ B \circ S$

$\overset{LA1}{\Leftrightarrow}$ A ist äquivalent zu B

Zeige: $\sim$ ist eine Äquivalenzrelation!

STOP

(R1) $A = \mathbb{1}_m \circ A \circ \mathbb{1}_n \Rightarrow A \sim A$

(R2) $A \sim B \Rightarrow \exists\, T \in Gl_m(K),\ S \in Gl_n(K) : A = T \circ B \circ S$

$\Rightarrow T^{-1} \circ A \circ S^{-1} = B \Rightarrow B \sim A$

(R3) $A \sim B,\ B \sim C \Rightarrow T, T' \in Gl_m(K),\ S, S' \in Gl_n(K)$:

$A = T \circ B \circ S,\ B = T' \circ C \circ S' \Rightarrow$

$A = \underbrace{T \circ T'}_{\in Gl_m(K)} \circ C \circ \underbrace{S' \circ S}_{\in Gl_n(K)} \Rightarrow A \sim C$

Was ist dabei die Äquivalenzklasse $\overline{A}$ von A?

Idee: Finde in $\overline{A}$ einen besonders schönen Vertreter, eine Normalform für $\overline{A}$!

LA1: $\mathrm{rang}(A) = r \Rightarrow A \sim \left(\begin{array}{c|c} \mathbb{1}_r & 0 \\ \hline 0 & 0 \end{array}\right)$

Normalform von $\overline{A}$.

Also: es gibt $\min\{m,n\}+1$ Äquivalenzklassen bez. $\sim$ auf Π.

© $\Pi = Mat_n(k)$, $A, B \in \Pi$

$A \sim B :\Leftrightarrow \exists\, T \in Gl_n(k) : A = T^{-1} \circ B \circ T$

$\Leftrightarrow$ A und B sind konjugiert

$\rightsquigarrow$ Jordansche Normalform

(d) $\Pi = \mathbb{Z} \times (\mathbb{Z} \setminus \{0\})$, $(p,q), (p',q') \in \Pi$

$(p,q) \sim (p',q') :\Leftrightarrow p \cdot q' = q \cdot p'$

Zeige: $\sim$ ist eine ÄR

Def.: $\frac{p}{q} := \overline{(p,q)} := \{ (p',q') \mid p \cdot q' = q \cdot p' \}$

$\mathbb{Q} := \{ \frac{p}{q} \mid (p,q) \in \mathbb{Z} \times (\mathbb{Z} \setminus \{0\}) \}$

Ziel: Führe auf $\mathbb{Q}$ neue Operationen ein!

$\frac{p}{q} + \frac{p'}{q'} := \frac{p \cdot q' + p' \cdot q}{q \cdot q'}$

$\frac{p}{q} \cdot \frac{p'}{q'} := \frac{p \cdot p'}{q \cdot q'}$

Problem: die Operationen verwenden die Vertreter, diese sind aber nicht eindeutig! (Wohldefiniertheit)

z.B.: $\frac{1}{2} + \frac{2}{3} = \frac{3+4}{6} = \frac{7}{6}$))?

$\overset{?}{=}$

$\frac{2}{4} + \frac{2}{3} = \frac{2 \cdot 3 + 4 \cdot 2}{12} = \frac{14}{12}$

$7 \cdot 12 = 6 \cdot 14$

$84 = 84$!

Prop. 2.3: Sei Π eine Menge und $\sim$ eine ÄR auf Π.

Dann gilt: $M = \dot{\bigcup_{\bar{x} \in \Pi/\sim}} \bar{x}$

Insbesondere: $\forall x, y \in \Pi$: $\bar{x} \cap \bar{y} = \emptyset$ oder $\bar{x} = \bar{y}$.

Beweis: • Zeige: $M = \bigcup_{\bar{x} \in M/\sim} \bar{x}$. Sei dazu $x \in M$.

$\Rightarrow x \in \bar{x} \subseteq \bigcup_{\bar{y} \in M/\sim} \bar{y}$ $\Rightarrow$ "$\subseteq$". Klar: "$\supseteq$"

• Zeige: Seien $\bar{x}, \bar{y} \in M/\sim$ mit $\bar{x} \neq \bar{y} \Rightarrow \bar{x} \cap \bar{y} = \emptyset$

Kontraposition: $\bar{x} \cap \bar{y} \neq \emptyset \Rightarrow \bar{x} = \bar{y}$

Seien $x, y \in M$ mit $\bar{x} \cap \bar{y} \neq \emptyset$. $\Rightarrow \exists z \in \bar{x} \cap \bar{y}$

$\Rightarrow z \sim x$ und $z \sim y$ $\overset{(R2)}{\Rightarrow}$ $x \sim z$ und $z \sim y$ $\overset{(R3)}{\Rightarrow}$ $\boxed{x \sim y}$.

Sei $u \in \bar{x}$ $\Rightarrow u \sim x$ $\overset{(R3)}{\Rightarrow} u \sim y$ $\Rightarrow u \in \bar{y} \Rightarrow \bar{x} \subseteq \bar{y}$

Analog: $\bar{y} \subseteq \bar{x}$. Damit: $\bar{x} = \bar{y}$ ✓

Korollar 2.4: Sei M eine endliche Menge, $\sim$ eine ÄR auf M und $M_1, \dots, M_k$ seien die paarweise verschiedenen Äquivalenzklassen von $\sim$.

Dann gilt: $|M| = |M_1| + |M_2| + \dots + |M_k|$

Beweis: $M = M_1 \dot{\cup} \dots \dot{\cup} M_k$ $\Rightarrow$ Behauptung ✓

§ 3 Die symmetrische Gruppe

Def. 3.1: Sei $n \in \mathbb{Z}$ mit $n \geq 1$.

(a) $S_n := \mathrm{Sym}(\{1,\dots,n\}) = \{\sigma : \{1,\dots,n\} \to \{1,\dots,n\} \mid \sigma \text{ bijektiv}\}$

heißt die **symmetrische Gruppe** vom Grad n.

Aus LA1 wissen wir, daß S_n mit der Verknüpfung von Abbildungen eine Gruppe ist, mit $id = id_{\{1,\dots,n\}}$ als Neutralem.

(b) Die Elemente von S_n heißen **Permutationen**.

Wir repräsentieren eine Permutation $\sigma \in S_n$ durch ihre **Wertetabelle**

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

Bsp. 3.2: Für $\begin{pmatrix} 1&2&3 \\ 2&1&3 \end{pmatrix}, \begin{pmatrix} 1&2&3 \\ 2&3&1 \end{pmatrix} \in S_3$ gilt:

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

Also: S_n ist nicht abelsch, $n \geq 3$.

Bemerkung 3.3:

(a) Die Reihenfolge der Zahlen in der 1. Zeile ist nicht wichtig!

z.B. $\begin{pmatrix} 1&2&3&4 \\ 2&3&1&4 \end{pmatrix} = \begin{pmatrix} 3&2&1&4 \\ 1&3&2&4 \end{pmatrix}$

Konvention: Schreibe sie in aufsteigender Reihenfolge!

(b) Invertieren ist einfach – tausche obere & untere Zeile!

i.e. $\sigma = \begin{pmatrix} 1&2&\dots&n \\ a_1&a_2&\dots&a_n \end{pmatrix} \Rightarrow \sigma^{-1} = \begin{pmatrix} a_1&a_2&\dots&a_n \\ 1&2&\dots&n \end{pmatrix}$

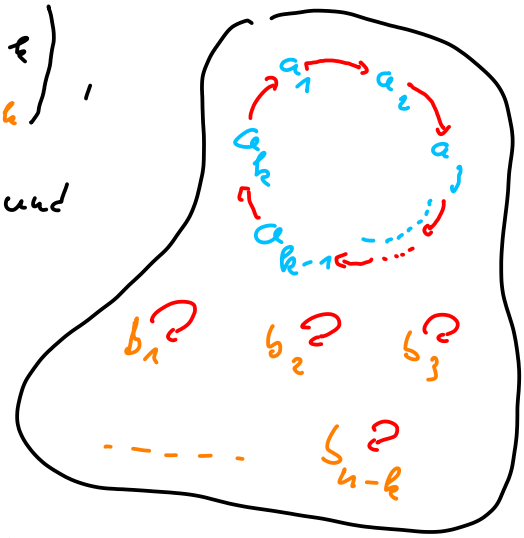
Def. 3.4:

(a) Ist $\{1,\dots,n\} = \{a_1,\dots,a_k\} \cup \{b_1,\dots,b_{n-k}\}$ und gilt

$$\sigma = \begin{pmatrix} a_1 & a_2 & \cdots & a_{k-1} & a_k & b_1 & b_2 & \cdots & b_{n-k} \\ a_2 & a_3 & \cdots & a_k & a_1 & b_1 & b_2 & \cdots & b_{n-k} \end{pmatrix},$$

dann heißt σ ein k-Zyklus und

wir schreiben: $\sigma = (a_1\ a_2\ \dots\ a_k)$



(b) Ein 2-Zyklus heißt auch eine **Transposition**!

$(i\ j)$ vertauscht i und j und lässt den Rest fest!

Bem. 3.5:

(a) Beachte: $(a_1\ a_2\ \dots\ a_k) = (a_2\ a_3\ \dots\ a_k\ a_1) = (a_3\ a_4\ \dots\ a_k\ a_1\ a_2) = \dots$

Konvention: beginne mit der kleinsten Zahl im Zyklus!

(b) $id = (1) = (2) = \dots = (n)$ ist der einzige 1-Zyklus!

Bsp. 3.6:

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

$$\tau = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 4 & 3 & 1 \end{pmatrix} \in S_4 \quad \Longrightarrow \quad \tau = (1\ 2\ 4)$$

? Der Zyklen-Schreibweise sieht man den Grad der Permutation nicht mehr an ?

Prop. 3.7: Für $\sigma \in S_n$ gibt es eine disjunkte Zerlegung

$$\{1,\dots,n\} = \dot{\bigcup_{i=1}^{t}} \{a_{i1},\dots,a_{ik_i}\} \quad \text{so, daß}$$

$$\sigma = (a_{11}\ \dots\ a_{1k_1}) \circ (a_{21}\ \dots\ a_{2k_2}) \circ \dots \circ (a_{t1}\ \dots\ a_{tk_t}).$$

Diese Darstellung von σ als Produkt p.w. disjunkter Zyklen heißt die **Zyklenzerlegung** von σ.

Beachte: $k_1 + k_2 + \dots + k_t = n$.

Beweis:

Definition für zwei Zahlen $a, b \in \{1, \dots, n\}$:

$$a \sim b \quad :\Leftrightarrow \quad \exists\, \nu \in \mathbb{Z} : \quad b = \sigma^{\nu}(a)$$

Zeige: $\sim$ ist eine Äq.R.

(R1) $a = id(a) = \sigma^0(a) \quad \Rightarrow \quad a \sim a$

(R2) $a \sim b \Rightarrow \exists\, \nu \in \mathbb{Z} : \quad b = \sigma^{\nu}(a)$

$\Rightarrow \quad \sigma^{-\nu}(b) = \sigma^{-\nu}(\sigma^{\nu}(a)) = \sigma^0(a) = a$

$\Rightarrow \quad b \sim a$

(R3) $a \sim b \;\wedge\; b \sim c \Rightarrow \exists\, \nu, \mu \in \mathbb{Z} : \; b = \sigma^{\nu}(a), \; c = \sigma^{\mu}(b)$

$\Rightarrow \quad c = \sigma^{\mu}(\sigma^{\nu}(a)) = \sigma^{\mu+\nu}(a) \Rightarrow a \sim c$

Zeige: $k := \min\{\ell > 0 \mid \sigma^{\ell}(a) = a\}$ existiert und es gilt $\bar{a} = \{a, \sigma(a), \dots, \sigma^{k-1}(a)\}$

Betrachte: $\{\sigma^{\ell}(a) \mid \ell > 0\} \subseteq \{1, \dots, n\}$

$\Rightarrow \quad \exists\; \ell > m > 0 : \quad \sigma^{\ell}(a) = \sigma^{m}(a)$

$\Rightarrow \quad \sigma^{\ell-m}(a) = \sigma^{m-m}(a) = \sigma^0(a) = a$

$\Rightarrow \quad \exists\; \ell - m > 0 : \quad \sigma^{\ell-m}(a) = a$

$\Rightarrow \quad k = \min\{\ell > 0 \mid \sigma^{\ell}(a) = a\}$ existiert nach dem archimedischen Prinzip!

z.z.: $\bar{a} = \{a, \sigma(a), \dots, \sigma^{k-1}(a)\}$

"$\supseteq$" $\quad \sigma^{\ell}(a) \sim a \;\; \forall \ell \in \mathbb{Z} \Rightarrow$ "$\supseteq$"

"$\subseteq$" $\quad$ Sei $b \sim a \Rightarrow \exists\, \nu \in \mathbb{Z} : \; b = \sigma^{\nu}(a)$

D.u.R $\Rightarrow \exists\, q, r \in \mathbb{Z}: \quad \nu = q \cdot k + r, \quad 0 \le r < k$

$\Rightarrow b = \sigma^{\nu}(a) = \sigma^{r+q\cdot k}(a) = \sigma^{r}\big(\underbrace{\sigma^{q\cdot k}(a)}_{=a}\big) = \sigma^{r}(a)$

$\in \{a, \dots, \sigma^{k-1}(a)\}$

Wähle für jede der Äquivalenzklassen einen Vertreter:

$\Rightarrow \exists\, a_{11}, \dots, a_{t1} \in \{1, \dots, n\}:$

$\{1, \dots, n\} = \dot{\bigcup_{i=1}^{t}} \overline{a_{i1}}$ mit $\overline{a_{i1}} = \{a_{i1}, \sigma(a_{i1}), \dots, \sigma^{k_i-1}(a_{i1})\}$

zudem: $|\overline{a_{i1}}| = k_i$.

Setze: $a_{ij} := \sigma^{j-1}(a_{i1}) \Rightarrow \overline{a_{i1}} = \{a_{i1}, a_{i2}, \dots, a_{ik_i}\}$

Es bleibt zu zeigen: $\sigma = \sigma_1 \circ \dots \circ \sigma_t$

mit $\sigma_i = (a_{i1}\ a_{i2}\ \dots\ a_{ik_i})$

Sei $b \in \{1, \dots, n\} = \dot{\bigcup_{i=1}^{t}} \{a_{i1}, \dots, a_{ik_i}\}$. z.z.: $\sigma(b) = (\sigma_1 \circ \dots \circ \sigma_t)(b)$

$\Rightarrow \exists_1\, i \in \{1, \dots, t\}: \quad b \in \overline{a_{i1}} = \{a_{i1}, \dots, a_{ik_i}\}$

$\Rightarrow \exists_1\, j \in \{1, \dots, k_i\}: \quad b = a_{ij} = \sigma^{j-1}(a_{i1})$

$\Rightarrow \sigma(b) = \sigma(\sigma^{j-1}(a_{i1})) = \sigma^{j}(a_{i1}) = \begin{cases} a_{i1}, & j = k_i \\ a_{i,j+1}, & j < k_i \end{cases} = \sigma_i(a_{ij}) = \sigma_i(b)$

Zudem: $b, \sigma(b) \notin \{a_{\ell 1}, \dots, a_{\ell k_\ell}\} = \overline{a_{\ell 1}}$ für $\ell \neq i$

$\Rightarrow \sigma_\ell(b) = b, \quad \sigma_\ell(\sigma(b)) = \sigma(b)$

$$\Rightarrow \left(\sigma_1 \circ \dots \sigma_i \circ \dots \circ \sigma_t\right)(i) = \left(\sigma_1 \circ \dots \circ \sigma_i\right)(i) =$$

$$= \left(\sigma_1 \circ \dots \circ \sigma_{i-1}\right)(\sigma(i)) = \sigma(i)$$

□

Prop. 3.7: Für $\sigma \in S_n$ gibt es eine disjunkte Zerlegung

$$\{1, \dots, n\} = \dot{\bigcup_{i=1}^{t}} \{a_{i1}, \dots, a_{ik_i}\} \quad \text{so, daß}$$

$$\sigma = (a_{11} \dots a_{1k_1}) \circ (a_{21} \dots a_{2k_2}) \circ \dots \circ (a_{t1} \dots a_{tk_t}).$$

Diese Darstellung von σ als Produkt p.w. disjunkter Zyklen heißt die Zykelzerlegung von σ.

Bem. 3.8:

(a) $\sigma = (a_1 \dots a_k)$, $\pi = (b_1 \dots b_\ell) \in S_n$ disjunkt Zykel

$$\Rightarrow \quad \pi \circ \sigma = \sigma \circ \pi$$

Beweis: Sei $c \in \{1, \dots, n\}$. z.z.: $(\pi \circ \sigma)(c) = (\sigma \circ \pi)(c)$

1. Fall: $c \in \{a_1, \dots, a_k\} \Rightarrow \sigma(c) \in \{a_1, \dots, a_k\}$

$\Rightarrow c, \sigma(c) \in \{b_1, \dots, b_\ell\}$

$\Rightarrow (\sigma \circ \pi)(c) = \sigma(\pi(c)) = \sigma(c) = \pi(\sigma(c)) = (\pi \circ \sigma)(c)$

2. Fall: $c \in \{b_1, \dots, b_\ell\}$. Analog.

3. Fall: $c \notin \{a_1, \dots, a_k\} \cup \{b_1, \dots, b_\ell\}$

$\Rightarrow \sigma(c) = \pi(c) = c \Rightarrow (\pi \circ \sigma)(c) = c = (\sigma \circ \pi)(c)$

□

(b) Wenn $\sigma = \sigma_1 \circ \dots \circ \sigma_t$ mit $\sigma_i = k_i$-Zyklus und $k_1 \geq \dots \geq k_t$, dann heißt $(k_1, k_2, \dots, k_t)$ der Zykeltyp von σ!

(c) Die Zykelzerlegung von σ in 3.7 ist eindeutig!

(d) Inversion in Zykeldarstellung ist einfach!

$$\sigma = (a_{11} \dots a_{1k_1}) \circ \dots \circ (a_{t1} \dots a_{tk_t})$$

$$\Rightarrow \sigma^{-1} = (a_{tk_t} \dots a_{t1}) \circ \dots \circ (a_{1k_1} \dots a_{11})$$

Kurz: Schreibe die Zykel in umgekehrter Reihenfolge!

(e) $\tau = (i\ j)$ Transposition $\Rightarrow \tau^{-1} = (j\ i) = (i\ j) = \tau$

Bsp. 3.9:

(a) $$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 5 & 6 & 3 & 1 & 4 & 2 \end{pmatrix}$$

$$\Rightarrow \sigma = (1\ 5\ 4) \circ (2\ 6) \circ (3) = (1\ 5\ 4) \circ (2\ 6)$$

(b) $n=1$: $S_1 = \{id\}$ $\quad |S_1| = 1 = 1!$

$n=2$: $S_2 = \{id, (1\,2)\}$ $\quad |S_2| = 2 = 2!$

$n=3$: $S_3 = \{id, (1\,2), (1\,3), (2\,3), (1\,2\,3), (1\,3\,2)\}$ $\quad |S_3| = 6 = 3!$

Stop

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

$$= (1\ 2\ 5)(3\ 4)(6\ 9)(7)(8) = (1\,2\,5)(3\,4)(6\,9)$$

Satz 3.10: $|S_n| = n!$

Beweisidee:

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

Möglichkeiten für $\sigma(i)$: $n \cdot (n-1) \cdot (n-2) \cdot (n-3) \cdots 3 \cdot 2 \cdot 1$

$= n!$ ☐

Proposition 3.11:

Jede Permutation in S_n, $n \geq 2$, läßt sich als Produkt von höchstens n Transpositionen schreiben.

Beweis: Sei $\sigma \in S_n$.

1. Fall: $\sigma = id \Rightarrow \sigma = (1\,2) \circ (1\,2)$.

2. Fall: $\sigma = (a_1 \dots a_k)$ ein k-Zyklus

$\Rightarrow \sigma = (a_1\, a_2) \circ (a_2\, a_3) \circ (a_3\, a_4) \circ \dots \circ (a_{k-1}\, a_k)$

3. Fall: $\sigma = (a_{11} \dots a_{1k_1}) \circ \dots \circ (a_{t1} \dots a_{tk_t})$

$\overset{\text{2. Fall}}{\Rightarrow}$ σ ist Produkt von $\sum_{i=1}^{t} (k_i - 1) = \sum_{i=1}^{t} k_i - t = n - t$ Transp.

☐

STOP

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

$= (1\,9\,8) \circ (2\,6\,3\,5\,4\,7) = (1\,9) \circ (9\,8) \circ (2\,6) \circ (6\,3) \circ (3\,5) \circ (5\,4) \circ (4\,7)$

Kor. 3.12:

Jede Permutation in S_n, $n \geq 2$, lässt sich als ein Produkt von Transpositionen aufeinanderfolgender Zahlen schreiben.

Beweis:

Wegen Prop. 3.11 reicht es, dies für Transpositionen der Zeigen: Sei $(i\,j)$ mit $i < j$ gegeben.

$$(i\,j) = (i\ i{+}1) \circ (i{+}1\ i{+}2) \circ \cdots \circ (j{-}2\ j{-}1) \circ (j{-}1\ j) \circ (j{-}2\ j{-}1) \circ \cdots \circ (i\ i{+}1)$$

□

Stop

Z.B.: $\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 5 & 4 & 1 & 3 \end{pmatrix} = (1\ 2\ 5\ 3\ 4)$

(3 5)

$= (1\,2)(2\,5)(5\,3)(3\,4)$

$= (1\,2)(2\,3)(3\,4)(4\,5)(3\,4)(2\,3)(3\,4)(4\,5)(3\,4)(3\,4)$

Bem. 3.13:

Eine Permutation lässt sich nicht auf eindeutige Art und Weise als Produkt von Transpositionen schreiben! ABER: die Parität der Anzahl der Transp ist eindeutig!

Def. 3.14: Sei $\sigma \in S_n$.

(a) Das Paar (i, j) heißt Fehlstand von σ, falls $i < j$, aber $\sigma(i) > \sigma(j)$.

(b) Das Signum von σ wird definiert als:

$$\operatorname{sgn}(\sigma) := \begin{cases} 1, & \#\text{Fehlstände von } \sigma \text{ ist gerade} \\ -1, & \#\text{Fehlstände von } \sigma \text{ ist ungerade} \end{cases}$$

Bsp. 3.15:

(a) $\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 4 & 1 & 3 \end{pmatrix}$ $\Rightarrow$

(i,j)	$(1,2)$	$(1,3)$	$(1,4)$	$(2,3)$	$(2,4)$	$(3,4)$
$(\sigma(i),\sigma(j))$	$(2,4)$	$(2,1)$	$(2,3)$	$(4,1)$	$(4,3)$	$(1,3)$
Fehlstand	nein	ja	nein	ja	ja	nein

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

(b) $\tau = (i\,j)$ mit $i < j$ — Transposition

$\Rightarrow$ Fehlstände: $(i,i+1), (i,i+2), \dots, (i,j), (i+1,j), (i+2,j), \dots, (j-1,j)$

$(j-1)-(i+1) = j-i-2$

$\#\ = 2\cdot(j-i-2)+1$

$(j-1)-(i+1) = j-i-2$

$\Rightarrow \operatorname{sgn}(\tau) = -1$

Satz 3.16:

(a) Die Abb. $\operatorname{sgn}: (S_n, \circ) \longrightarrow (\{-1,1\}, \cdot)$ ist ein Gruppenhomom.

d.h. $\operatorname{sgn}(\sigma\circ\pi) = \operatorname{sgn}(\sigma)\cdot\operatorname{sgn}(\pi) \quad \forall \sigma, \pi \in S_n.$

(b) Wenn $\sigma = \tau_1 \circ \dots \circ \tau_k$ mit τ_i: Transp., dann

$$\operatorname{sgn}(\sigma) = (-1)^k$$

(c) Wenn $\sigma = \tau_1 \circ \dots \circ \tau_k = \tau_1' \circ \dots \circ \tau_\ell'$ mit τ_i, τ_i' Transp.,

dann: $k-\ell$ gerade!

Beweis:

① Zeige: $\tau = (i \; i+1)$ und $\sigma \in S_n$

$\Rightarrow sgn(\sigma \circ \tau) \overset{?}{=} -sgn(\sigma) \overset{3.15}{=} sgn(\sigma) \cdot sgn(\tau)$

1. Fall: $(i, i+1)$ ist ein Fehlstand von σ

$\Rightarrow \tau$ hebt diesen Fehlstand auf

$\Rightarrow \sigma \circ \tau$ hat genau 1 Fehlstand weniger als σ

$\Rightarrow -sgn(\sigma) = sgn(\sigma \circ \tau)$

2. Fall: $(i, i+1)$ kein Fehlstand von σ

$\Rightarrow \tau$ erzeugt ein Fehlstand

$\Rightarrow \sigma \circ \tau$ hat genau 1 Fehlstand mehr als σ

$\Rightarrow -sgn(\sigma) = sgn(\sigma \circ \tau)$

② Zeige: $\sigma = \tau_1 \circ \dots \circ \tau_k$ mit τ_i: Transp. benachbarter Zahlen

$\Rightarrow sgn(\sigma) = (-1)^k$

Ind. nach k: $k=1$: $sgn(\sigma) = sgn(\tau_1) = -1$ nach 3.15

$k-1 \mapsto k$: $sgn(\sigma) = sgn((\tau_1 \circ \dots \circ \tau_{k-1}) \circ \tau_k)$

$\overset{①}{=} -sgn(\tau_1 \circ \dots \circ \tau_{k-1}) \overset{Ind.}{=} -(-1)^{k-1} = (-1)^k$

③ Damit: $\sigma, \pi \in S_n \overset{3.12}{\Rightarrow} \exists \tau_1, \dots, \tau_k, \tau'_1, \dots, \tau'_\ell \in S_n$

Transp. benachbarter Zahlen so, dass $\sigma = \tau_1 \circ \dots \circ \tau_k$

$\pi = \tau'_1 \circ \dots \circ \tau'_\ell$

$\Rightarrow \sigma \circ \pi = \tau_1 \circ \dots \circ \tau_k \circ \tau'_1 \circ \dots \circ \tau'_\ell$

$\overset{②}{\Rightarrow} sgn(\sigma \circ \pi) \overset{②}{=} (-1)^{k+\ell} = (-1)^k \cdot (-1)^\ell \overset{②}{=} sgn(\sigma) \cdot sgn(\pi)$

④ Folgt aus ③ & Induktion.

⑤ ④ $\Rightarrow (-1)^k = sgn(\sigma) = (-1)^\ell \Rightarrow (-1)^{\ell-k} = 1 \Rightarrow \ell - k$ ist gerade ☐

Def. 3.17:

Sei $n \geq 2$. Dann heißt

$$A_n := \ker(\mathrm{sgn}) = \{\sigma \in S_n \mid \mathrm{sgn}(\sigma) = 1\}$$

die alternierende Gruppe vom Grad n.

Die Permutationen in A_n heißen gerade, die übrigen ungerade.

§4 Normalteiler und Faktorgruppen

A) Der Satz von Lagrange

Notation 4.0: Sei $(G, \cdot)$ eine Gruppe, $A, B \subseteq G$, $g \in G$.

- $A \cdot B := \{a \cdot b \mid a \in A, b \in B\}$
- $g \cdot A := \{g \cdot a \mid a \in A\}$
- $A \cdot g := \{a \cdot g \mid a \in A\}$

Proposition 4.1: Sei $(G, \cdot)$ und $U, V \leq G$, $|G| < \infty$.

Dann: $$|U \cdot V| = \frac{|U| \cdot |V|}{|U \cap V|}$$

Beweis: Definiere für $(u,v), (u',v') \in U \times V$:

$$(u,v) \sim (u',v') \; :\Leftrightarrow \; u \cdot v = u' \cdot v'$$

① Zeige: $\sim$ ist eine ÄR.

(R1) $u \cdot v = u \cdot v \Rightarrow (u,v) \sim (u,v)$

(R2) $(u,v) \sim (u',v') \Rightarrow u \cdot v = u' \cdot v' \Rightarrow u' \cdot v' = u \cdot v$
$\Rightarrow (u',v') \sim (u,v)$

(R3) $(u,v) \sim (u',v')$, $(u',v') \sim (u'',v'') \Rightarrow u \cdot v = u' \cdot v'$, $u' \cdot v' = u'' \cdot v''$
$\Rightarrow u \cdot v = u'' \cdot v'' \Rightarrow (u,v) \sim (u'',v'')$.

② Zeige: $u \cdot v = u' \cdot v' \Leftrightarrow \exists g \in U \cap V : u = u' \cdot g, \; v = g^{-1} \cdot v'$

"$\Leftarrow$" Sei $g \in U \cap V$ mit $u = u'g$, $v = g^{-1} \cdot v'$
$\Rightarrow u \cdot v = u' g \cdot g^{-1} v' = u' v'$

"$\Rightarrow$" Sei $uv = u'v' \Rightarrow \underbrace{(u')^{-1} \cdot u}_{\in U} = \underbrace{v' \cdot v^{-1}}_{\in V} \in U \cap V$

$=: g$
$\Rightarrow u = u' \cdot g, \; v = g^{-1} \cdot v'$

③ Zeige: Wenn $g, \tilde{g} \in U \cap V$ mit $u = u' g = u' \tilde{g}$, $v = g^{-1} v' = \tilde{g}^{-1} \cdot v'$

$\Rightarrow g = \tilde{g}$, d.h. g oben ist eindeutig.

Denn: $u' \cdot g = u' \cdot \tilde{g} \overset{\text{KR}}{\Rightarrow} g = \tilde{g}$

④ Zeige: $|\overline{(u,v)}| = |U \cap V|$

Denn: $\overline{(u',v')} = \{(u,v) \mid (u,v) \sim (u',v')\}$

$\overset{②}{=} \{(u' \cdot g, g^{-1} \cdot v') \mid g \in U \cap V\}$

$\Rightarrow |(u',v')| = |\{(u' \cdot g, g^{-1} \cdot v') \mid g \in U \cap V\}| \overset{③}{=} |U \cap V|$

⑤ $U \times V = \dot{\bigcup}_{x \in \frac{U \times V}{\sim}} x \Rightarrow |U \times V| = \sum_{x \in \frac{U \times V}{\sim}} |x| = \sum_{x \in \frac{U \times V}{\sim}} |U \cap V|$

$|U| \cdot |V|$

$= |U \cap V| \cdot$ Anzahl der Äquivalenzklassen

$= |U \cap V| \cdot |U \cdot V|$

$\Rightarrow |U \cdot V| = \frac{|U| \cdot |V|}{|U \cap V|}$. ☐

Bsp: $G = S_4$, $U = \langle (1234) \rangle$, $V = \langle (13), (24) \rangle$

Bestimme: $U \cdot V$, U, V, $U \cap V$

Stop

$U = \{id, (1234), (13)(24), (1432)\}$

$V = \{id, (13), (24), (13)(24)\}$

$U \cap V = \{id, (13)(24)\}$

$U \cdot V = \{id, (13), (1234), (14)(23), (24), (13)(24), (1432), (12)(34)\}$

U \ V	id	(13)	$(13)(24)$	(24)
id	id	(13)	$(13)(24)$	(24)
(1234)	(1234)	$(14)(23)$	(1432)	$(12)(34)$
$(13)(24)$	$(13)(24)$	(24)	id	(13)
(1432)	(1432)	$(12)(34)$	(1234)	$(14)(23)$

$8 = |U \cdot V| = \frac{|U| \cdot |V|}{|U \cap V|} = \frac{4 \cdot 4}{2}$

Proposition 4.2:

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

Für $g, h \in G$ definiere: $g \sim h :\Leftrightarrow g^{-1} \cdot h \in U$.

Dann ist $\sim$ eine ÄR auf G und die zu g gehörende Äquivalenzklasse $\bar{g} = g \cdot U$

Wir nennen gU die zu g gehörende Linksnebenklasse und g einen Repräsentanten der Linksnebenklasse.

Zudem: $G/U := \{g \cdot U \mid g \in U\}$ die Menge der Linksnebenklassen und es gilt, $|G : U| := |G/U|$ heißt der Index von U in G.

Beweis: Seien $g, h, k \in G$.

(R1) $g^{-1} \cdot g = e \in U \Rightarrow g \sim g$

(R2) $g \sim h \Rightarrow g^{-1} \cdot h \in U \Rightarrow U \ni (g^{-1} h)^{-1} = h^{-1} \cdot (g^{-1})^{-1} = h^{-1} \cdot g$

$\Rightarrow h \sim g$

(R3) $g \sim h,\ h \sim k \Rightarrow g^{-1} h,\ h^{-1} \cdot k \in U \Rightarrow U \ni g^{-1} h \cdot h^{-1} k = g^{-1} \cdot k$

$\Rightarrow g \sim k$

Also: $\sim$ ist eine ÄR.

Zeige: $\bar{g} = gU$.

"$\supseteq$" Sei $h \in gU \Rightarrow \exists u \in U : h = g \cdot u$

$\Rightarrow g^{-1} \cdot h = g^{-1} \cdot g \cdot u = u \in U \Rightarrow g \sim h \Rightarrow h \in \bar{g}$

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

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

Korollar 4.3:

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

Dann: (a) $gU = hU$ oder $gU \cap hU = \emptyset$

(b) $G = \dot{\bigcup_{\lambda \in G/U}} g_\lambda \cdot U$, wobei g_λ ein Repräsentant der Linksnebenklasse λ sein soll

Beweis: 4.2 + 2.3. ☐

Bemerkung 4.4:

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

Dann:
- $U = e \cdot U$ ist immer eine Linksnebenklasse
- $gU = hU \iff h \in gU$
- $u \cdot U = U \iff u \in U$

Bsp. 4.5: (a) $G = S_3$, $U = A_3 = \{id, (123), (132)\}$

$\Rightarrow$ • $A_3 = id \cdot A_3 = (123) \cdot A_3 = (132) \cdot A_3$

• $(12) \cdot A_3 = \{(12), (23), (13)\} = (23) \cdot A_3 = (13) \cdot A_3$

$\Rightarrow$ $S_3 = A_3 \dot\cup (12) \cdot A_3$ $\quad |S_3| = 6 = 3 \cdot 2 = |A_3| \cdot |S_3 : A_3|$

$\Rightarrow$ $S_3/A_3 = \{A_3, (12) \cdot A_3\}$, $|S_3 : A_3| = 2$

(b) Sei $(V, +, \cdot)$ ein K-VR und U ein Untervektorraum.

Dann: $x \sim y \iff \underbrace{-x + y}_{y - x} \in U \iff y \in \underbrace{x + U}_{\{x + u \mid u \in U\}}$

Also: $x + U$ = Linksnebenklasse von x bezüglich U
= Restklasse von x mod U im Faktorraum V/U

Bsp. 4.6: Sei $(G,\cdot) = (\mathbb{Z},+)$, $U = n\cdot\mathbb{Z}$ mit $n \geq 1$.

Dann hat U genau die n Linksnebenklassen:

$$\begin{aligned}
\overline{0} &= 0 + n\mathbb{Z} &&= n\cdot\mathbb{Z} \\
\overline{1} &= 1 + n\mathbb{Z} &&= \{1 + nz \mid z \in \mathbb{Z}\} \\
\overline{2} &= 2 + n\mathbb{Z} &&= \{2 + nz \mid z \in \mathbb{Z}\} \\
&\vdots && \vdots \\
\overline{n-1} &= (n-1) + n\mathbb{Z} &&= \{n-1 + nz \mid z \in \mathbb{Z}\}
\end{aligned}$$

Also: $|\mathbb{Z} : n\mathbb{Z}| = n$

Notation:

- $\mathbb{Z}_n := \mathbb{Z}/n\mathbb{Z} = \{\overline{0}, \overline{1}, \ldots, \overline{n-1}\}$
- $x \equiv y \pmod n \;:\Leftrightarrow\; y - x \in n\mathbb{Z}$

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

  Sage: x kongruent zu y modulo n

Beweis: * Sei $x \in \mathbb{Z}$. $\overset{\text{Div.A.}}{\Longrightarrow} \exists\, q, r \in \mathbb{Z} : x = q\cdot n + r,\ 0 \leq r \leq n-1$

$$\Rightarrow -r + x = q\cdot n = n\cdot q \in n\mathbb{Z} \Rightarrow r \sim x \Rightarrow x \in \overline{r} \in \{\overline{0}, \overline{1}, \ldots, \overline{n-1}\}$$

* Ang.: $\exists\, i, j$ mit $0 \leq i < j \leq n-1$ und $\overline{i} = \overline{j}$

$\Rightarrow n \mid j - i$ und $0 < j - i < n$ ↯

Also: $\overline{0}, \ldots, \overline{n-1}$ sind paarweise verschieden. ☐

Lemma 4.7: Sei $(G,\cdot)$ eine Gruppe, $U \leq G$, $g \in G$.

Dann: $l_g : U \longrightarrow gU : u \mapsto g\cdot u$ ist bijektiv.

Insbesondere: $|U| = |gU|$

Beweis: $g \cdot x$ $g \cdot y$

Seien $x, y \in U$ mit $l_g(x) = l_g(y) \overset{\text{KR}}{\Longrightarrow} x = y$

$\Rightarrow l_g$ ist injektiv.

Sei $x \in gU \Rightarrow \exists u \in U : x = g \cdot u = l_g(u) \Rightarrow l_g$ ist surjektiv. ✓

Satz von Lagrange 4.8:

Sei $(G, \cdot)$ eine endliche Gruppe, $U \leq G$.

Dann: $|G| = |U| \cdot |G:U|$

Insbesondere: $|U| \mid |G|$ und $|G:U| \mid |G|$.

Beweis:

Sei $G/U = \{g_1 \cdot U, \dots, g_k \cdot U\}$, wobei $g_1, \dots, g_k$ ein Vertretersystem für die Linksnebenklassen sein soll.

$\Rightarrow k = |G/U| = |G:U|$

Dann: $G = \dot{\bigcup}_{i=1}^{k} g_i U \Rightarrow |G| = \sum_{i=1}^{k} \underbrace{|g_i \cdot U|}_{=|U|} \overset{4.7}{=} \sum_{i=1}^{k} |U| = k \cdot |U|$

$= |G:U| \cdot |U|$.

□

Korollar 4.9:

(endlich)

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

Dann: $o(g) := |\langle g \rangle|$ ist ein Teiler von $|G|$

$\parallel$ ÜA

$\min\{l > 0 \mid g^l = e\}$

$o(g)$ heißt die Ordnung von g.

Beweis: Lagrange 4.8. □

Bsp. 4.10: ($G = S_3$)

Sei $U \leq S_3$. Bemerke: $|S_3| = 6$ und $|U| \mid 6$

$\Rightarrow |U| \in \{1, 2, 3, 6\}$

① $|U| = 1 \Rightarrow U = \{id\}$

② $|U| = 2 \Rightarrow U = \{id, \sigma\}$ und $o(\sigma) = 2$

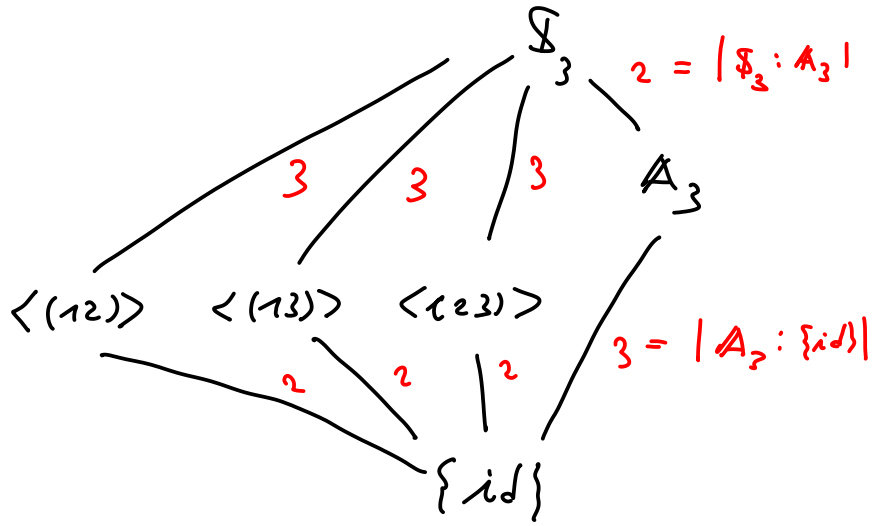
$\Rightarrow \sigma$ = 2-Zykel = Transposition

$\Rightarrow U = \langle (12) \rangle$ oder $U = \langle (13) \rangle$ oder $U = \langle (23) \rangle$

③ $|U| = 3 \Rightarrow U = \{id, \sigma, \pi\} \Rightarrow \sigma, \pi$ 3-Zykel

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

Untergruppendiagramm der S_3



B) Normalteiler

Motivation 4.11:

Sei $(G, \cdot)$ eine Gruppe, $U \leq G$, $G/U = \{g \cdot U \mid g \in G\}$.

Ziel: G/U soll eine Gruppe werden durch

$$(g \cdot U) \cdot (h \cdot U) = \{g \cdot u \cdot h \cdot u' \mid u, u' \in U\}$$

Problem:
* Ist $gU \cdot hU$ wieder eine Linksnebenklasse?
* Was ist ein Vertreter von $gUhU$?

Def. 4.12: Sei G eine Gruppe, $U \leq G$.

U heißt ein Normalteiler von G, wenn

$$\forall g \in G, u \in U: \quad g \cdot u \cdot g^{-1} \in U.$$

Notation: $U \trianglelefteq G$

Klar: $\{e\} \trianglelefteq G$ und $G \trianglelefteq G$.

Lemma 4.13: Sei $(G, \cdot)$ eine abelsche Gruppe.

Dann ist jede Untergruppe von G ein Normalteiler von G.

Beweis:

Seien $g \in G$ und $u \in U$, dann gilt:

$$g^{-1} \cdot u \cdot g = g^{-1} \cdot g \cdot u = e \cdot u = u \in U.$$

Also: $U \trianglelefteq G$. ☐

Beispiel 4.14:

(a) Sei $n \in \mathbb{Z}$, dann $n\cdot\mathbb{Z} \trianglelefteq \mathbb{Z}$.

(b) Sei $\mathcal{U} = \{id, (12)(34), (13)(24), (14)(23)\}$

Zeige: $\mathcal{U} \trianglelefteq S_4$

(1) z.z.: $\mathcal{U}$ abgeschlossen bzgl. Multiplikation

	id	$(12)(34)$	$(13)(24)$	$(14)(23)$
id	id	$(12)(34)$	$(13)(24)$	$(14)(23)$
$(12)(34)$	$(12)(34)$	id	$(14)(23)$	$(13)(24)$
$(13)(24)$	$(13)(24)$	$(14)(23)$	id	$(12)(34)$
$(14)(23)$	$(14)(23)$	$(13)(24)$	$(12)(34)$	id

Weil $|\mathcal{U}| < \infty$, folgt dann: $\mathcal{U} \leq S_4$

(2) z.z.: $\forall \sigma \in S_4, \pi \in \mathcal{U}: \sigma\circ\pi\circ\sigma^{-1} \in \mathcal{U}$

Sei $\sigma \in S_4$, $\pi \in \mathcal{U}$.

1. Fall: $\pi = id \Rightarrow \sigma\circ\pi\cdot\sigma^{-1} = \sigma\circ id\circ\sigma^{-1} = id \in \mathcal{U}$

2. Fall: $\pi \neq id \Rightarrow \pi$ hat Zyklentyp $(2,2)$

$\Rightarrow \sigma\circ\pi\circ\sigma^{-1}$ hat Zyklentyp $(2,2)$

d.h. $\sigma\circ\pi\circ\sigma^{-1}$ ist Doppeltransposition

$\Rightarrow \sigma\circ\pi\circ\sigma^{-1} \in \mathcal{U}$, weil die einzigen 3 Doppeltranspositionen von S_4 in $\mathcal{U}$ liegen

Also: $\mathcal{U} \trianglelefteq S_4$

Prop. 4.15:

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

Dann sind äquivalent:

(a) $U \trianglelefteq G$, d.h. $g \cdot u \cdot g^{-1} \in U \quad \forall g \in G, u \in U$

(b) $\forall g \in G: \; g^{-1} U g = U$ (oder $g U g^{-1} = U$)

(c) $\forall g \in G: \; gU = Ug$

(d) $\forall g, h \in G: \; (gU)\cdot(hU) = (gh)\cdot U$

Beweis:

(a) $\Rightarrow$ (b): Sei $g \in G$ beliebig $\Rightarrow$ $g^{-1} \cdot U \cdot g = \{ g^{-1} \cdot u \cdot g \mid u \in U \} \subseteq U$ (weil $U \trianglelefteq G$)

$\Rightarrow e \cdot U \cdot e = g \cdot (g^{-1} U g) \cdot g^{-1} \subseteq g \cdot U \cdot g^{-1}$ für jedes $g \in G$

$\{ e \cdot u \cdot e \mid u \in U \} = U$

Wende dies an mit g ersetzt durch g^{-1}:

$$U \subseteq g^{-1} \cdot U (g^{-1})^{-1} = g^{-1} U \cdot g$$

Also: $g^{-1} \cdot U \cdot g = U \quad \forall g \in G$

(b) $\Rightarrow$ (c): Sei $g \in G$.

$\overset{(b)}{\Rightarrow} g^{-1} U g = U \Rightarrow e \cdot U \cdot g = g \cdot (g^{-1} \cdot U \cdot g) = g \cdot U$

$U g$

(c) $\Rightarrow$ (d): Seien $g, h \in G$

$$(gU)(hU) = g \cdot (U \cdot h) \cdot U \overset{(c)}{=} g (hU) \cdot U = g \cdot h \cdot U \cdot U$$
$$= \{ g \cdot h \cdot u \cdot u' \mid u, u' \in U \} = \{ g \cdot h \cdot \tilde{u} \mid \tilde{u} \in U \} = g \cdot h \cdot U$$

(d) $\Rightarrow$ (a): Sei $g \in G$, $u \in U$

$\Rightarrow g \cdot u \cdot g^{-1} = \underbrace{g \cdot u}_{\in gU} \cdot \underbrace{g^{-1} \cdot e}_{g^{-1}U} \in gU \cdot g^{-1}U \overset{(d)}{=} g \cdot g^{-1} \cdot U$

$e \cdot U = U$

$\Rightarrow U \trianglelefteq G$ ✓

Bsp. 4.16: $U = \{id, (12)\} \leq S_3$.

Behauptung: U ist kein Normalteiler in der S_3!

Beweis: $(23) \circ (12) \circ (23) = (13) \notin U$

$g \quad u \quad g^{-1}$ ✓

Proposition 4.17: Sei $\alpha : G \longrightarrow H$ ein Gruppenhomomorphismus.

Behauptung: $\ker(\alpha) = \{g \in G \mid \alpha(g) = e_H\} \trianglelefteq G$

Beweis:

- 1.22 $\Rightarrow \ker(\alpha) \leq G$.
- Sei $g \in G$ und $u \in \ker(\alpha)$

$\Rightarrow \alpha(g \cdot u \cdot g^{-1}) = \alpha(g) \cdot \underbrace{\alpha(u)}_{=e_H} \cdot \alpha(g^{-1}) = \alpha(g) \cdot e_H \cdot \alpha(g)^{-1}$

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

$\Rightarrow g \cdot u \cdot g^{-1} \in \ker(\alpha)$. Also: $\ker(\alpha) \trianglelefteq G$ ✓

Bsp. 4.18:

(a) $sgn : S_n \longrightarrow \{1, -1\}$ G.H. $\Rightarrow A_n = \ker(sgn) \trianglelefteq S_n$

$= \{\sigma \in S_n \mid sgn(\pi) = 1\}$

(b) $\det : (GL_n(K), \cdot) \longrightarrow (K \setminus \{0\}, \cdot)$ ist ein G.H.,

denn: $A, B \in GL_n(K) \Rightarrow \det(A \cdot B) = \det(A) \cdot \det(B)$

$\Rightarrow$ det ein G.H.

Also: $SL_n(K) = \ker(\det) = \{A \in GL_n(K) \mid \det(A) = 1\} \trianglelefteq GL_n(K)$

spezielle lineare Gruppe

Lemma 4.19: Sei $(G, \cdot)$ eine Gruppe, $U \leq G$ und $N \trianglelefteq G$.

Dann: (a) $U \cdot N \leq G$ (b) $N \trianglelefteq U \cdot N$ (c) $U \cap N \trianglelefteq U$

Beweis: (a) • klar: $U \cdot N = \{u \cdot n \mid u \in U, n \in N\} \subseteq G$ ($u \cdot n \in G$)

• klar: $e = e \cdot e \in U \cdot N \Rightarrow U \cdot N \neq \emptyset$ ($e \in U$, $e \in N$)

• Seien $u \cdot n, u' \cdot n' \in U \cdot N$ mit $u, u' \in U$, $n, n' \in N$

$\Rightarrow n \cdot u' \in N \cdot u' = u' \cdot N \Rightarrow \exists \tilde{n} \in N : n \cdot u' = u' \cdot \tilde{n}$

$\Rightarrow (u \cdot n) \cdot (u' \cdot n') = u \cdot (u \cdot u') \cdot n' = u \cdot (u' \cdot \tilde{n}) \cdot n' = (u \cdot u') \cdot (\tilde{n} \cdot n') \in U \cdot N$ ($u \cdot u' \in U$, $\tilde{n} \cdot n' \in N$)

• Sei $u \cdot n \in U \cdot N$ mit $u \in U$, $n \in N$

$\Rightarrow (u \cdot n)^{-1} = n^{-1} \cdot u^{-1} \in N \cdot u^{-1} = u^{-1} \cdot N \subseteq U \cdot N$ ($u^{-1} \in U$)

Also: $U \cdot N \leq G$

(b) $N = \{n \mid n \in N\} = \{e \cdot n \mid n \in N\} \subseteq U \cdot N$ ($e \in U$, $n \in N$)

Weil N bzgl. "$\cdot$" Gruppe, folgt: $N \leq U \cdot N$

Zudem: $g \in U \cdot N \Rightarrow g \in G \Rightarrow g \cdot N = N g \Rightarrow N \trianglelefteq U \cdot N$ ($N \trianglelefteq G$)

(c) Zeige: $\mathcal{U} \cap N \trianglelefteq \mathcal{U}$

* $\mathcal{U} \leq G$ & $N \trianglelefteq G$ $\Rightarrow$ $\mathcal{U} \cap N \leq G$ und $\mathcal{U} \cap N \subseteq \mathcal{U}$

$\Rightarrow$ $\mathcal{U} \cap N \leq \mathcal{U}$

* Sei $g \in \mathcal{U}$, $u \in \mathcal{U} \cap N$.

$\Rightarrow$ $g \cdot u \cdot g^{-1} = g \cdot u \cdot g^{-1} \in \mathcal{U} \cap N$

$\mathcal{U}$ $\mathcal{U}$ $\mathcal{U}$ $\in \mathcal{U}$; G N G $\in N$

* Also: $\mathcal{U} \cap N \trianglelefteq \mathcal{U}$. ◻

Bsp. 4.20: $\mathcal{U} = \langle (12) \rangle$, $\mathcal{U}' = \langle (23) \rangle \leq S_3$

$\Rightarrow$ $\mathcal{U} \cdot \mathcal{U}' = \{ id, (12), (23), (123) \} \not\leq S_3$, Wegen Lagrange! weil $4 \nmid 6 = |S_3|$

Beachte auch: $|\mathcal{U} \cdot \mathcal{U}'| = \frac{|\mathcal{U}| \cdot |\mathcal{U}'|}{|\mathcal{U} \cap \mathcal{U}'|} = \frac{2 \cdot 2}{1} = 4$ $= |\mathcal{U} \cdot \mathcal{U}'|$

Also: in 4.19 (c) ist es wichtig, daß N ein Normalteiler ist ▽

C) Faktorgruppe

Satz 4.21 (Faktorgruppe)

Sei $(G,\cdot)$ eine Gruppe und $U \leq G$ ein Normalteiler.

① $\bar{g} \cdot \bar{h} = \overline{g \cdot h} \quad \forall \bar{g}, \bar{h} \in G/U$

② G/U ist mit dieser Operation eine Gruppe, die sog. Faktorgruppe von G nach U
$\bar{e}$ ist das neutrale Element in G/U; $\bar{g}^{-1}$ ist das Inverse von $\bar{g}$ in G/U.

③ Wenn G abelsch ist, dann ist auch G/U abelsch.

④ $\pi : G \twoheadrightarrow G/U : g \mapsto \bar{g}$ ist ein Gruppenepimorphismus mit $\ker(\pi) = U$.
π heißt die Restklassenabbildung von G/U.

Beweis: ① 3.19 $\Rightarrow \bar{g} \cdot \bar{h} = (gU) \cdot (hU) = (gh) \cdot U = \overline{gh}$

② Seien $\bar{g}, \bar{h}, \bar{k} \in G/U$

Assoziativgesetz: $(\bar{g} \cdot \bar{h}) \cdot \bar{k} \overset{①}{=} \overline{gh} \cdot \bar{k} \overset{①}{=} \overline{(g \cdot h) \cdot k} = \overline{g \cdot (h \cdot k)}$
$\overset{①}{=} \bar{g} \cdot \overline{h \cdot k} \overset{①}{=} \bar{g} \cdot (\bar{h} \cdot \bar{k})$

Neutrales: $\bar{e} \cdot \bar{g} \overset{①}{=} \overline{e \cdot g} = \bar{g}$

Inverse: $\bar{g}^{-1} \cdot \bar{g} \overset{①}{=} \overline{g^{-1} \cdot g} = \bar{e}$

$\Rightarrow (G/U, \cdot)$ ist eine Gruppe.

③ G abelsch und $\bar{g}, \bar{h} \in G/U \Rightarrow \bar{g} \cdot \bar{h} \overset{①}{=} \overline{gh} = \overline{hg} \overset{①}{=} \bar{h} \cdot \bar{g}$

④ Zeige: $\pi : G \to G/U : g \mapsto \bar{g}$ ist G.H.

Seien $g, h \in G$. $\Rightarrow \pi(g \cdot h) = \overline{gh} \overset{①}{=} \bar{g} \cdot \bar{h} = \pi(g) \cdot \pi(h)$
$\Rightarrow \pi$ ist ein G.H.

Zeige: π ist surjektiv.

Sei $\bar{g} \in G/U \Rightarrow \pi(g) = \bar{g} \Rightarrow \pi$ ist surjektiv

Zeige: $\ker(\pi) = U$. Beweis: $g \in \ker(\pi) \Leftrightarrow \bar{e} = \pi(g) = \bar{g}$
$\Leftrightarrow g \in U$ ($\bar{e} = U$, $\bar{g} = gU$)

Bsp. 4.22:

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

mit $\bar{x} + \bar{y} = \overline{x+y}$ für $x, y \in \mathbb{Z}$.

Bemerkung 4.23:

(a) Sei $(G, \cdot)$ eine Gruppe und $N \trianglelefteq G$.

$$\{U \leq G \mid N \subseteq U\} \xrightarrow[\text{bijektiv}]{1:1} \{\bar{U} \mid \bar{U} \leq G/N\}$$

$$U \longmapsto U/N$$

$$\{M \trianglelefteq G \mid N \subseteq M\} \xrightarrow[\text{bijektiv}]{1:1} \{\bar{M} \mid \bar{M} \trianglelefteq G/N\}$$

$$M \longmapsto M/N$$

(b) Wenden wir (a) auf $(\mathbb{Z}_n, +)$ an für $n > 0$, dann erhalten wir:

$$\bar{U} \leq \mathbb{Z}_n \iff \exists\, m \in \{1, \dots, n\} \text{ mit } m \mid n : \bar{U} = \frac{m\cdot\mathbb{Z}}{n\mathbb{Z}} = \langle \bar{m} \rangle$$

Def. 4.24:

Für $a, b \in \mathbb{Z} \setminus \{0\}$ definiere $ggT(a,b) := \min\{k > 0 \mid a \text{ und } b \text{ teilen } k\}$

$=$ kleinstes gemeinsames Vielfaches von a & b.

und $ggT(0,c) = ggT(c,0) = 0 \quad \forall c \in \mathbb{Z}$.

Korollar 4.25:

Seien $m, n \in \mathbb{Z}_{>0}$ und $\bar{m} \in \mathbb{Z}_n$. Dann gilt:

$$o(\bar{m}) = \frac{ggT(m,n)}{m} = \text{Ordnung von } \bar{m} \text{ in } \mathbb{Z}_n.$$

Beweis:

$$o(\bar{m}) = \min\{k > 0 \mid \underbrace{k \cdot \bar{m}}_{=} = \bar{0}\}$$

$$\left(\underbrace{\bar{m} + \dots + \bar{m}}_{k\text{-mal}} = \overline{\underbrace{m + \dots + m}_{k\text{-mal}}} = \overline{k \cdot m}\right)$$

$$= \min\{k>0 \mid \overline{k \cdot m} = \overline{0}\}$$

$$= \min\{k>0 \mid n \text{ teilt } k \cdot m\}$$

$$= \frac{m \cdot \min\{k>0 \mid n \text{ teilt } k \cdot m\}}{m}$$

$$= \frac{\min\{\ell>0 \mid \exists k>0 : \ell = m \cdot k \text{ und } n \text{ teilt } m \cdot k\}}{m} \qquad \ell = m \cdot k$$

$$= \frac{\min\{\ell>0 \mid m \text{ teilt } \ell \text{ und } n \text{ teilt } \ell\}}{m}$$

$$= \frac{kgv(m,n)}{m}$$

□

D) Homomorphiesatz

Homomorphiesatz 4.26

Sei $\alpha: G \to H$ ein Gruppenhomomorphismus.

Dann $\bar{\alpha}: \frac{G}{\ker(\alpha)} \to \operatorname{Im}(\alpha) : \bar{g} = g \cdot \ker(\alpha) \mapsto \alpha(g)$

ist ein Isomorphismus.

Insbesondere: $\frac{G}{\ker(\alpha)} \cong \operatorname{Im}(\alpha)$.

Beweis:

Zeige: $\bar{\alpha}$ ist wohldefiniert, d.h. $\bar{g} = \bar{h} \Rightarrow \bar{\alpha}(\bar{g}) = \bar{\alpha}(\bar{h})$

Seien $\bar{g} = \bar{h} \Rightarrow g \sim h \Rightarrow g^{-1} h \in \ker(\alpha)$

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

$\Rightarrow \bar{\alpha}(\bar{g}) = \alpha(g) = \alpha(h) = \bar{\alpha}(\bar{h}) \Rightarrow \alpha$ ist wohldefiniert.

Zeige: $\bar{\alpha}$ ist ein G.H.

Seien $\bar{g}, \bar{h} \in \frac{G}{\ker(\alpha)}$. $\Rightarrow \bar{\alpha}(\bar{g} \cdot \bar{h}) = \bar{\alpha}(\overline{g \cdot h}) =$

$\alpha(g \cdot h) = \alpha(g) \cdot \alpha(h) = \bar{\alpha}(\bar{g}) \cdot \bar{\alpha}(\bar{h})$

(α G.H.)

Zeige: $\bar{\alpha}$ ist injektiv.

$\bar{g} \in \ker(\bar{\alpha}) \Leftrightarrow e_H = \bar{\alpha}(\bar{g}) = \alpha(g) \Leftrightarrow g \in \ker(\alpha)$

$\hookrightarrow \bar{g} = g \cdot \ker(\alpha) = \ker(\alpha) = e_{G/\ker(\alpha)}$

Also: $\ker(\bar{\alpha}) = \{ e_{G/\ker(\alpha)} \} \Rightarrow \bar{\alpha}$ ist injektiv.

Zeige: $\bar{\alpha}$ surjektiv, d.h. $\operatorname{Im}(\bar{\alpha}) = \operatorname{Im}(\alpha)$. "$\supseteq$" klar

"$\subseteq$" Sei $h \in \operatorname{Im}(\alpha) \Rightarrow \exists g \in G: h = \alpha(g) = \bar{\alpha}(\bar{g}) \Rightarrow h \in \operatorname{Im}(\bar{\alpha})$

Beispiel 4.27: $(G,\cdot) = (\mathbb{Z},+)$, $(H,*) = (\mathbb{C}\setminus\{0\},\cdot)$

$\alpha : \mathbb{Z} \longrightarrow \mathbb{C}\setminus\{0\} ; z \longmapsto i^z = e^{z\cdot\frac{\pi i}{2}}$ ist ein Gruppenhomomorphismus, denn: $\alpha(z+z') = i^{z+z'} = i^z \cdot i^{z'} = \alpha(z)\cdot\alpha(z')$

Also: Homomorphiesatz $\Rightarrow$ $\mathbb{Z}/\mathrm{Kern}(\alpha) \cong \mathrm{Im}(\alpha)$

Dabei:
- $\mathrm{Im}(\alpha) = \langle i \rangle = \{ i^z \mid z \in \mathbb{Z} \} = \{ i^1 = i,\ i^2 = -1,\ i^3 = -i,\ i^4 = 1 \}$
- $\mathrm{Kern}(\alpha) = \{ z \in \mathbb{Z} \mid 1 = \alpha(z) = i^z \} = o(i)\cdot\mathbb{Z} = 4\cdot\mathbb{Z}$
- $o(i) = \min\{n>0 \mid i^4 = 1\} = 4$

Damit: $\mathbb{Z}/4\mathbb{Z} = \mathbb{Z}/\mathrm{Kern}(\alpha) \cong \mathrm{Im}(\alpha) = \{1,-1,i,-i\}$

Korollar 4.28: Sei $n \geq 2$.

Dann: $S_n/A_n = S_n/\mathrm{Kern}(\mathrm{sgn}) \cong \mathrm{Im}(\mathrm{sgn}) = \{1,-1\}$

$\Rightarrow |A_n| = \frac{|S_n|}{|S_n : A_n|} = \frac{n!}{2}$

Isomorphiesätze 4.29

Sei $(G,\cdot)$ eine Gruppe

(a) Seien $U \leq G$ und $N \trianglelefteq G$.

Dann: $U\cdot N/N \cong U/U\cap N$

(b) Seien $M, N \trianglelefteq G$ mit $M \subseteq N$.

Dann: $\frac{G/M}{N/M} \cong G/N$

Beweis: (a) ✓ A.

(b) Betrachte die Abb. $\alpha : G \to \frac{G/H}{N/H} : g \mapsto (gH) \cdot N/H$

Zeige: α ist G.H.

Seien $g, h \in G$. $\Rightarrow \alpha(g \cdot h) = \big((g \cdot h) \cdot H\big) \cdot N/H =$

$= \big((g \cdot H)(h \cdot H)\big) \cdot N/H = \Big[(gH) \cdot N/H\Big] \cdot \Big[(hH) \cdot N/H\Big] = \alpha(g) \cdot \alpha(h)$

Zeige: α ist surjektiv

Sei $(gH) \cdot N/H \in \frac{G/H}{N/H} \Rightarrow \alpha(g) = gH \cdot N/H \Rightarrow \alpha$ surjektiv.

Zeige: $\ker(\alpha) = N$.

$g \in \ker(\alpha) \iff (gH) \cdot N/H = \alpha(g) = e_{\left(\frac{G/H}{N/H}\right)} = N/H$

$\iff gH \in N/H \iff g \in N$

Damit: Hom.satz $\Rightarrow \quad \frac{G}{\ker(\alpha)} \cong \operatorname{Im}(\alpha) = \frac{G/H}{N/H}$

$\frac{G}{N} \ni gN \longmapsto (gH) \cdot N/H$

✓

E) Zyklische Gruppen

Satz 4.30:

Sei $(G, \cdot)$ eine zyklische Gruppe, d.h. $G = \langle g \rangle$.

(a) $|G| = \infty$: Dann: $\alpha : \mathbb{Z} \xrightarrow{\cong} G : z \mapsto g^z$ ist ein Isomorphismus

(b) $|G| = n < \infty$: Dann: $\overline{\alpha} : \mathbb{Z}_n \xrightarrow{\cong} G : \overline{z} \mapsto g^z$ ist ein Isomorphismus.

Beweis: Betrachte die Abbildung $\alpha : \mathbb{Z} \to G : z \mapsto g^z$.

Wegen $\alpha(z+z') = g^{z+z'} = g^z \cdot g^{z'} = \alpha(z) \cdot \alpha(z')$, ist α ein G.H.

Außerdem: $\mathrm{Im}(\alpha) = \{\alpha(z) \mid z \in \mathbb{Z}\} = \{g^z \mid z \in \mathbb{Z}\} = \langle g \rangle = G$

$\Rightarrow$ α ist surjektiv.

Erinnerung: $o(g) \overset{!}{=} \min\{n > 0 \mid g^n = e\}$ ⊗

1. Fall: $|G| = \infty$ (= $|\langle g \rangle| = o(g)$) $\Rightarrow$ $g^n \neq e \ \forall n \in \mathbb{N} \Rightarrow g^z \neq e \ \forall z \in \mathbb{Z} \setminus \{0\}$

$\Rightarrow \ker(\alpha) = \{z \in \mathbb{Z} \mid g^z = \alpha(z) = e\} = \{0\}$

$\Rightarrow$ α ist injektiv $\Rightarrow$ (a)

2. Fall: $|G| = n < \infty$ (= $|\langle g \rangle| = o(g)$) $\Rightarrow \ker(\alpha) = \{z \in \mathbb{Z} \mid g^z = \alpha(z) = e\}$

$\overset{\otimes}{=} n \cdot \mathbb{Z}$

$\overset{\text{Homsatz}}{\Rightarrow}$ $\mathbb{Z}/n\mathbb{Z} = \mathbb{Z}/\ker(\alpha) \cong \mathrm{Im}(\alpha) = G$

$\cup$ $\cup$

$z \longmapsto \alpha(z) = g^z$

□

Korollar 4.31:

Sei $(G,\cdot)$ eine Gruppe, $g \in G$ mit $o(g) = n < \infty$ und $m \in \mathbb{Z} \setminus \{0\}$.

Dann: $o(g^m) = \frac{ggT(m,n)}{|m|}$.

Beweis: o.E. $m > 0$ (denn: $o(g^{-m}) = o((g^m)^{-1}) = o(g^m)$)

4.30 $\Rightarrow$ $\varphi : \mathbb{Z}_n \longrightarrow \langle g \rangle : \bar{z} \mapsto g^z$

$\overset{\text{ÜA}}{\Rightarrow}$ $o(\underbrace{\varphi(\bar{m})}_{= o(g^m)}) = o(\bar{m}) \overset{4.25}{=} \frac{ggT(m,n)}{m}$ ☐

Korollar 4.32:

Sei $G = \langle g \rangle$ eine zyklische Gruppe mit $|G| = n < \infty$

Dann: (a) $U \leq G \iff \exists\, 1 \leq m \leq n$ mit $m \mid n$: $U = \langle g^m \rangle$

(b) Sei $m \mid n$ mit $1 \leq m \leq n$; dann $|\langle g^m \rangle| = \frac{n}{m}$.

Insbesondere: G hat für jeden Teiler d der Ordnung $|G| = n$ genau eine Untergruppe der Ordnung d.

Beweis: Deshalb: 4.30 $\Rightarrow$ $G \cong \mathbb{Z}_n$

$\Rightarrow$ Untergruppen von G stehen in 1:1-Beziehung zu Teilern von $\mathbb{Z}_n$

$\Rightarrow$ (a) mit 4.23 und (b) mit 4.31. ☐

Korollar 4.33:

Jede Untergruppe einer zyklischen Gruppe ist zyklisch!

§6 Ringe und Körper

A) Ringe und Körper

Def. 6.1: (a) Ein **Ring mit Eins** ist ein Tripel $(R, +, \cdot)$ bestehend aus einer nicht-leeren Menge und zwei zweistelligen Operationen $+: R \times R \to R$ und $\cdot : R \times R \to R$, so daß folgende Axiome erfüllt sind:

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

(2) $\forall x, y, z \in R : (x \cdot y) \cdot z = x \cdot (y \cdot z)$ (Assoziativgesetz)

(3) $\exists 1_R \in R : \forall x \in R : 1_R \cdot x = x \cdot 1_R = x$ (Einselement)

(4) $\forall x, y, z \in R : x \cdot (y + z) = x \cdot y + x \cdot z$ und $(y + z) \cdot x = y \cdot x + z \cdot x$ (Distributivgesetz)

(b) Ein Ring mit Eins $(R, +, \cdot)$ heißt **kommutativ**, wenn: $\forall x, y \in R : x \cdot y = y \cdot x$.

(c) Ist $(R, +, \cdot)$ ein Ring mit Eins, so heißt $x \in R$ eine **Einheit** in R, wenn $\exists x' \in R : x \cdot x' = x' \cdot x = 1_R$. x' heißt das Inverse von x.

Notation: $R^* := \{ x \in R \mid x \text{ ist Einheit} \}$, $\frac{1}{x} = x^{-1}$ für das Inverse von x.

(d) Ein kommutativer Ring mit Eins $(R, +, \cdot)$ heißt **Körper**, falls $R^* = R \setminus \{0\}$. Insbesondere gilt dann: $1_R \neq 0_R$.

Bemerkung 6.2:

- Wir sagen meist "R ist ein Ring" und unterschlagen dabei $+$ und $\cdot$!
- Notation: . schreibe xy statt $x \cdot y$, $x - y$ statt $x + (-y)$.
  . schreibe 0 statt 0_R, 1 statt 1_R.
- $(R^*, \cdot)$ ist eine Gruppe, die **Einheitengruppe** von R.
  Insb.: das Neutrale 1_R und die Inversen sind eindeutig.
- $(K, +, \cdot)$ ist ein Körper $\Leftrightarrow$ $(K, +)$ und $(K \setminus \{0\}, \cdot)$ sind abelsche Gruppen und $\forall x, y, z \in K : x \cdot (y + z) = x \cdot y + x \cdot z$

Bsp. 6.3: (a) $(\mathbb{Z}, +, \cdot)$ ist ein kommutativer Ring mit Eins.

(b) $(\mathbb{Q}, +, \cdot)$, $(\mathbb{R}, +, \cdot)$, $(\mathbb{C}, +, \cdot)$ sind Körper.

(c) Sei $(R, +, \cdot)$ ein Ring mit Eins und Π eine Menge.

Setze: $R^{\Pi} := \{ f : \Pi \to R \mid f \text{ Abbildung} \}$.

$f + g : \Pi \to R : m \mapsto f(m) + g(m)$

$f \cdot g : \Pi \to R : m \mapsto f(m) \cdot g(m)$

$1 : \Pi \to R : m \mapsto 1_R$

Dann ist $(R^{\Pi}, +, \cdot)$ ein Ring mit Eins 1.

(d) Sei k ein Körper. Dann $(Mat_n(k), +, 0)$ ist ein nicht-kommutativer Ring mit Eins ($n \geq 2$). Dabei, $(Mat_n(k))^* = Gl_n(k)$

$\begin{pmatrix} 1 & & 0 \\ & \ddots & \\ 0 & & 1 \end{pmatrix}$

(e) Seien R und S zwei kommutative Ringe mit 1.

Dann: $R \times S$ durch $(r, s) + (r', s') := (r + r', s + s')$

$(r, s) \cdot (r', s') := (r \cdot r', s \cdot s')$

ein kommutativer Ring mit Eins $(1_R, 1_S)$

Zudem: $(R \times S)^* = R^* \times S^*$

Def. 6.4:

Sei R ein kommutativer Ring mit Eins und $a_k \in R$ für $k \in \mathbb{N}$.

Wir nennen den Ausdruck $\sum_{n=0}^{\infty} a_k \cdot t^k$ eine formale Potenzreihe in der Veränderlichen t mit Koeffizienten in R

Die Menge $R[[t]] := \{ \sum_{n=0}^{\infty} a_k \cdot t^k \mid a_k \in R \}$ heißt der Ring der formalen Potenzreihen in der Veränderlichen t mit Koeffizienten in R.

Für zwei formale Potenzreihen $f = \sum_{k=0}^{\infty} a_k \cdot t^k$ und $g = \sum_{k=0}^{\infty} b_k \cdot t^k$

definiere:

- $f + g := \sum_{k=0}^{\infty} (a_k + b_k) \cdot t^k$
- $f \cdot g := \sum_{k=0}^{\infty} \left(\sum_{i=0}^{k} a_i \cdot b_{k-i} \right) \cdot t^k = \sum_{h=0}^{\infty} \left(\sum_{i+j=h} a_i \cdot b_j \right) \cdot t^h$

Bemerke:

- $f = g \iff a_k = b_k$ für alle $k \in \mathbb{N}$
- Falls $a_k = 0$ für alle $k \geq n$, schreibe: $f = \sum_{k=0}^{n} a_k \cdot t^k$

Satz 6.5

Sei R ein kommutativer Ring mit Eins.

Dann $R[[t]]$ ist ein kommutativer Ring mit Eins $t^0 = 1$.

Beweis:

① **Zeige:** $(R[[t]], +)$ ist eine abelsche Gruppe

Folgt aus der Def. von $+$ & $(R, +)$ abelsche Gruppe.

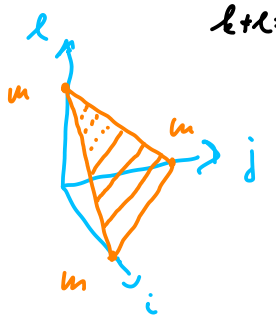
② **Zeige:**

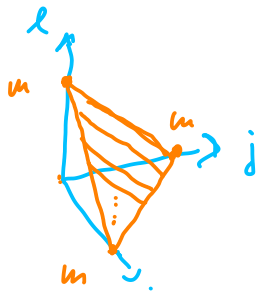
- ist assoziativ.

Seien $f = \sum_{i=0}^{\infty} a_i \cdot t^i$, $g = \sum_{j=0}^{\infty} b_j \cdot t^j$, $h = \sum_{l=0}^{\infty} c_l \cdot t^l \in R[[t]]$.

Berechne:

$$\sum_{k+l=m} \left(\sum_{i+j=k} a_i \cdot b_j \right) \cdot c_l = \sum_{i+j+l=m} a_i \cdot b_j \cdot c_l = \sum_{i+k=m} a_i \cdot \sum_{j+l=k} b_j \cdot c_l$$





$$\Rightarrow (f \cdot g) \cdot h = \left(\sum_{k=0}^{\infty} \left(\sum_{i+j=k} a_i \cdot b_j \right) \cdot t^k \right) \cdot h = \sum_{m=0}^{\infty} \overbrace{\left(\sum_{k+l=m} \left(\sum_{i+j=k} a_i \cdot b_j \right) c_l \right) \cdot t^m}$$

$$= \sum_{m=0}^{\infty} \Big(\sum_{i+k=m} a_i \cdot \sum_{j+l=k} b_j \cdot c_l \Big) \cdot t^m = f \cdot \Big(\sum_{k=0}^{\infty} \Big(\sum_{j+l=k} b_j c_l \Big) \cdot t^k \Big) = f \cdot (g \cdot h)$$

③ Zu zeigen: $t^0 = \sum_{k=0}^{\infty} e_k \cdot t^k$ mit $e_k = \begin{cases} 0, & k>0 \\ 1, & k=0 \end{cases}$ ist die Eins

$$t^0 \cdot f = \sum_{k=0}^{\infty} \Big(\underbrace{\sum_{i+j=k} e_i \cdot a_j}_{= a_k} \Big) \cdot t^k = \sum_{k=0}^{\infty} a_k \cdot t^k = f$$

④ Distributivgesetz folgt aus dem Distributivgesetz in R

$$f \cdot (g+h) = \sum_{k=0}^{\infty} \Big(\sum_{i+j=k} a_i \cdot (b_j + c_j) \Big) \cdot t^k = \sum_{k=0}^{\infty} \Big(\sum_{i+j=k} a_i b_j + \sum_{i+j=k} a_i c_j \Big) \cdot t^k$$

$$= \sum_{k=0}^{\infty} \Big(\sum_{i+j=k} a_i b_j \Big) \cdot t^k + \sum_{\zeta=0}^{\infty} \Big(\sum_{i+j=k} a_i c_j \Big) \cdot t^k = f \cdot g + f \cdot h$$

⑤ Kommutativgesetz folgt unmittelbar aus dem Kommutativgesetz in R !

□

Lemma 5.6:
Sei R ein Ring mit Eins und $x, y, z \in R$.

Dann: ⓐ $-(-x) = x$ ⓑ $x+y=z \iff x = z-y$

ⓒ $-(x+y) = -x-y$ ⓓ $0 \cdot x = x \cdot 0 = 0$

ⓔ $(-x) \cdot y = x \cdot (-y) = -(xy)$

ⓕ $(-x) \cdot (-y) = xy$ ⓖ $x \cdot (y-z) = xy - xz$

ⓗ $x \in R^* \Rightarrow x^{-1} \in R^*$ und $(x^{-1})^{-1} = x$

ⓘ Ist $1_R = 0_R$, dann ist $R = \{0_R\}$ der Nullring.

Beweis: ⓐ – ⓒ & ⓗ: Lemma 1.25, da $(R,+)$ & $(R^*,\cdot)$ Gruppe (abelsch)

(d) $0 + 0 \cdot x = 0 \cdot x = (0+0) \cdot x = 0 \cdot x + 0 \cdot x \overset{K_R}{\Longrightarrow} 0 = 0 \cdot x$

Analog: $x \cdot 0 = 0$

(e) $(-x) \cdot y + xy = (-x+x) \cdot y = 0 \cdot y \overset{(d)}{=} 0 \Rightarrow (-x) \cdot y = -(xy)$

Analog: $x \cdot (-y) = -(xy)$

(f) $(-x) \cdot (-y) \overset{(e)}{=} -(x \cdot (-y)) \overset{(e)}{=} -(-(xy)) = xy$

(g) $x \cdot (y-z) = x \cdot (y + (-z)) = xy + x \cdot (-z) \overset{(e)}{=} xy + (-(xz)) = xy - xz$

(i) Wenn $1_R = 0_R$, dann gilt für $x \in R$:

$x = 1_R \cdot x = 0_R \cdot x = 0_R \Rightarrow R = \{0_R\}$.

□

B) Unterringe

Def. 6.7:

Sei R ein Ring mit $1 \neq 0$ und $S \subseteq R$.

Dann heißt S ein Unterring von R, wenn:

① $1_R \in S$ ② $\forall x, y \in S: x + y \in S$

③ $\forall x \in S: -x \in S$ ④ $\forall x, y \in S: x \cdot y \in S$

Wenn zudem R ein Körper ist und zusätzlich

⑤ $\forall 0 \neq x \in S: x^{-1} \in S$

dann heißt S ein Teilkörper von R

Bemerkung: $(S, +, \cdot)$ ist als Unterring von R selbst ein Ring mit 1!

Beispiel 6.8:

- $\mathbb{Z}$ ein Unterring von $\mathbb{Q}$, $\mathbb{R}$ und $\mathbb{C}$.
- $\mathbb{Q}$ ist ein Teilkörper von $\mathbb{R}$ und $\mathbb{C}$.

Def. 6.9:

Sei R ein kommutativer Ring mit Eins.

Dann heißt $R[t] := \left\{ \sum_{k=0}^{n} a_k \cdot t^k \mid a_k \in R,\ n \in \mathbb{N} \right\}$ der Polynomring in der Variablen t mit Koeffizienten in R, und die Elemente von $R[t]$ heißen Polynome.

Für $0 \neq f = \sum_{k=0}^{n} a_k \cdot t^k \in R[t]$ heißt $\deg(f) := \max\{k \mid a_k \neq 0\}$ der Grad von f und $lc(f) := a_{\deg(f)}$ heißt der Leitkoeffizient.

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

Satz 6.10:

Sei R ein kommutativer Ring mit Eins.

Dann ist $R[t]$ ein Unterring von $R(t)$.

Zudem: $\forall f, g \in R[t]$:

- $\deg(f+g) \leq \max\{\deg(f), \deg(g)\}$
- $\deg(f \cdot g) \leq \deg(f) + \deg(g)$
- $\deg(f \cdot g) = \deg(f) + \deg(g) \iff lc(f) \cdot lc(g) \neq 0$

Beweis:

Zeige: $R[t]$ ein Unterring von $R(t)$

- $1_{R(t)} = t^0 \in R[t]$
- Seien $f, g \in R[t]$

$\Rightarrow$ - $\deg(f+g) \overset{!}{\leq} \max\{\deg(f), \deg(g)\} \Rightarrow f+g \in R[t]$
- $\deg(f \cdot g) \overset{!}{\leq} \deg(f) + \deg(g) \Rightarrow f \cdot g \in R[t]$
- $f = \sum_{i=0}^{n} a_i t^i \Rightarrow -f = \sum_{i=0}^{n} (-a_i) \cdot t^i \in R[t]$

Zeige noch die Gradformel: o.E. $f \neq 0 \neq g$

Sei $f = \sum_{k=0}^{n} a_k \cdot t^k$ mit $a_n \neq 0$, $g = \sum_{k=0}^{m} b_k \cdot t^k$ mit $b_m \neq 0$.

1. Fall: $m < n$ $\Rightarrow$ $f+g = \sum_{k=0}^{m} (a_k + b_k) \cdot t^k + \sum_{k=m+1}^{n} a_k \cdot t^k$

$\Rightarrow \deg(f+g) = n = \max\{\deg(f), \deg(g)\}$

(f: $a_n \neq 0$; $\deg(f) = n$; $\deg(g) = m$)

2. Fall: $m = n$ $\Rightarrow$ $f+g = \sum_{k=0}^{n} (a_k + b_k) \cdot t^k$

$\Rightarrow \deg(f+g) \leq n = \max\{\deg(f), \deg(g)\}$

3. Fall: $m \to n$ $\Longrightarrow$ (wie im 2. Fall) $\deg(f+g) = m = \max\{\deg(f), \deg(g)\}$

Zudem: $f \cdot g = \sum_{k=0}^{m+n} \left(\sum_{i+j=k} a_i \cdot b_j \right) \cdot t^k$

und für $k = m+n$ gilt: $\sum_{i+j=m+n} a_i \cdot b_j = a_n \cdot b_m$

$\Rightarrow \deg(f \cdot g) \leq m+n = \deg(f) + \deg(g)$ mit

("$=$" $\Longleftrightarrow$ $a_n \cdot b_m \neq 0$)

(a_n: $\mathrm{lc}(f)$, b_m: $\mathrm{lc}(g)$)

$\square$

c) Ringhomomorphismen

Def. 6.11:

Seien R und S zwei Ringe mit Eins.

Eine Abbildung $\varphi: R \to S$ heißt Ringhomomorphismus, wenn:

1. $\forall x, y \in R$: $\varphi(x+y) = \varphi(x) + \varphi(y)$
2. $\forall x, y \in R$: $\varphi(x \cdot y) = \varphi(x) \cdot \varphi(y)$
3. $\varphi(1_R) = 1_S$

Sei $\varphi : R \to S$ ein Ringhomomorphismus, dann:

* φ heißt ein Monomorphismus $:\Leftrightarrow$ φ ist injektiv
* φ " " Epimorphismus $:\Leftrightarrow$ φ ist surjektiv
* φ " " Isomorphismus $:\Leftrightarrow$ φ ist bijektiv
* φ " " Automorphismus $:\Leftrightarrow$ φ ist bijektiv und $R = S$.

Bem. 6.12:

(a) $\varphi : R \to S$ Isomorphismus $\Rightarrow$ $\varphi^{-1} : S \to R$ ein Isomorphismus

(b) $\varphi : R \to S$ ein Ringhomom. $\Rightarrow$ $\mathrm{Im}(\varphi)$ ist ein Unterring von S

(c) $\varphi : R \to S$ ein Ringhomom. $\Rightarrow$ (φ injektiv $\Leftrightarrow$ $\ker(\varphi) = [0]$)
$\ker(\varphi) = \{x \in R \mid \varphi(x) = 0\}$

(d) $R \hookrightarrow R[t] : a \mapsto a \cdot t^0$ ist ein Monomorphismus
Deshalb schreiben: $3t^3 + 5t + 2$ statt $3t^3 + 5t^1 + 2t^0$

(e) Sei R ein kommutativer Ring mit 1 und S Ring mit Eins und sei $b \in S$ und $R \subseteq S$.
$\Rightarrow$ $\phi_b : R[t] \to S : f \mapsto f(b)$ ist ein Ringhomomorphismus
$\sum_{i=0}^{n} a_i t^i$ $\sum_{i=0}^{n} a_i b^i$ (Einsetzhomomorphismus)

D) Ideale

Def. 6.13:

Sei R ein kommutativer Ring mit Eins, $\emptyset \neq I \subseteq R$.
Dann heißt I ein Ideal von R, falls

(1) $\forall a, b \in I$: $a + b \in I$

(2) $\forall a \in I, x \in R$: $x \cdot a \in I$

Notation: $I \trianglelefteq R$

Bem. 6.14:

(a) Sei R ein kommut. Ring mit Eins und I ein Ideal in R.

Dann: $(I,+)$ ist ein Normalteiler von $(R,+)$

Denn: $\cdot\ a \in I \Rightarrow -a = (-1)\cdot a \in I$ (R, I) $\Rightarrow (I,+) \leq (R,+)$ ($I \trianglelefteq R$, Untergruppe)

$\Rightarrow (I,+)$ ist Normalteiler von $(R,+)$, da $(R,+)$ abelsch ist!

(b) Wenn $I \trianglelefteq R$ und $a_1, \dots, a_n \in I$ und $x_1, \dots, x_n \in R$,

dann: $x_1 \cdot a_1 + \dots + x_n \cdot a_n \in I$

d.h. I ist abgeschlossen bzgl. endlicher Linearkombinationen.

Denn: Ind. nach n:

$n=1$: $x_1 \cdot a_1 \in I$ nach (2)

$n-1 \to n$: $x_1 a_1 + \dots + x_n \cdot a_n = \underbrace{\underbrace{(x_1 \cdot a_1 + \dots + x_{n-1} \cdot a_{n-1})}_{\in I \text{ Ind.}} + \underbrace{x_n \cdot a_n}_{\in I\ (2)}}_{\in I\ (1)}$

(3)

STOP

Bsp: (a) $R = \mathbb{Z}$, $I = \{3 \cdot z \mid z \in \mathbb{Z}\}$

Zeige: $I \trianglelefteq R$

Denn:
- $3 \cdot 0 = 0$ ist in I $\Rightarrow I \neq \emptyset$
- $3 \cdot z + 3 \cdot z' = 3 \cdot (z + z') \in I$
- $x \cdot (3 \cdot z) = 3 \cdot (x \cdot z) \in I$ ($x \in \mathbb{Z}$, $z \in I$, $x \cdot z \in \mathbb{Z}$)

(3)

(5) $R = \mathbb{Q}[t]$, $I = \{ f \in \mathbb{Q}[t] \mid f(0) = 0 \}$

Zeige: $I \trianglelefteq R$.

Beweis:
- Sei $f = 0$ das Nullpolynom, dann: $f(0) = 0$
  $\Rightarrow f \in I \Rightarrow I \neq \emptyset$
- Seien $f, g \in I \Rightarrow f(0) = 0,\ g(0) = 0$
  $\Rightarrow (f+g)(0) = f(0) + g(0) = 0 + 0 = 0$
  $\Rightarrow f + g \in I$
- Sei $f \in I$, $g \in \mathbb{Q}[t] = R$
  $\Rightarrow (g \cdot f)(0) = g(0) \cdot f(0) = g(0) \cdot 0 = 0$
  $\Rightarrow g \cdot f \in I$. ☐

Def. 6.15: Sei R ein kommutativer Ring mit Eins und $\Pi \subseteq R$.
Dann heißt $\langle \Pi \rangle := \bigcap_{\substack{I \trianglelefteq R \\ \Pi \subseteq I}} I$ das Erzeugnis von Π in I.
$\langle \Pi \rangle$ / $\langle \Pi \rangle_R$

Prop. 6.16: Sei R ein kommut. Ring mit Eins, $\emptyset \neq \Pi \subseteq R$.

Dann: $\langle \Pi \rangle = \left\{ \sum_{k=1}^{n} x_k \cdot a_k \mid a_k \in \Pi,\ x_k \in R,\ n \geq 1 \right\} \trianglelefteq R$
$\langle \Pi \rangle_R$

Beweis:

Setze $\mathfrak{J} := \left\{ \sum_{k=1}^{n} x_k \cdot a_k \mid a_k \in \Pi,\ x_k \in R,\ n \geq 1 \right\}$.

Zeige: $\mathfrak{J} \trianglelefteq R$ mit $\Pi \subseteq \mathfrak{J}$

- Sei $a \in \Pi \Rightarrow a = 1 \cdot a \in \mathfrak{J} \Rightarrow \Pi \subseteq \mathfrak{J} \Rightarrow \mathfrak{J} \neq \emptyset$
- Seien $a = x_1 a_1 + \dots + x_n a_n$, $b = y_1 b_1 + \dots + y_m b_m \in \mathfrak{J}$ mit $a_i, b_i \in \Pi$, $x_i, y_i \in R$. Dann: $a + b = x_1 a_1 + \dots + x_n a_n + y_1 b_1 + \dots + y_m b_m \in \mathfrak{J}$

- Sei $a = x_1 a_1 + \dots + x_n a_n \in \mathfrak{J}$ mit $a_i \in \Pi$, $x_i \in R$ und sei $x \in R$

$$\Rightarrow x \cdot a = \underbrace{(x \cdot x_1)}_{\in R} \cdot a_1 + \dots + \underbrace{(x \cdot x_n)}_{\in R} \cdot a_n \in \mathfrak{J}$$

$\underline{①}$ zeige: $\langle \Pi \rangle = \bigcap_{\substack{I \trianglelefteq R \\ \Pi \subseteq I}} I \subseteq \mathfrak{J}$

- Sei $a = x_1 a_1 + \dots + x_n a_n \in \mathfrak{J}$ mit $x_i \in R$, $a_i \in \Pi$ und sei $I \trianglelefteq R$ mit $\Pi \subseteq I$

$$\Rightarrow a = x_1 a_1 + \dots + x_n a_n \in I \Rightarrow a \in \bigcap_{\substack{I \trianglelefteq R \\ \Pi \subseteq I}} I = \langle \Pi \rangle$$

$$\Rightarrow \mathfrak{J} \subseteq \langle \Pi \rangle.$$

□

Bsp. 6.17:

ⓐ Sei R ein kommut. Ring mit Eins und $a, b \in R$.

Dann: - $\langle a \rangle_R = \{ x \cdot a \mid x \in R \}$ (Hauptideal)

- $\langle a, b \rangle_R = \{ x \cdot a + y \cdot b \mid x, y \in R \}$

ⓑ Sei $R = \mathbb{Z}$ und $\mathcal{U} \subseteq \mathbb{Z}$. Dann gleichwertig:

① $\mathcal{U}$ ist ein Ideal von $(\mathbb{Z}, +, \cdot)$

② $\mathcal{U}$ ist eine Untergruppe von $(\mathbb{Z}, +)$

③ $\exists\, u \in \mathbb{N}$: $\mathcal{U} = u \cdot \mathbb{Z} \overset{ⓐ}{=} \langle u \rangle_{\mathbb{Z}}$

Denn: ① ⇒ ②: 6.14 ② ⇒ ③: 1.19

③ ⇒ ①: $u \cdot \mathbb{Z} \overset{ⓐ}{=} \langle u \rangle_{\mathbb{Z}}$ □

E) Faktorringe

Satz 6.18:

Sei R ein kommut. Ring mit Eins und $I \trianglelefteq R$.

Dann wird die Faktorgruppe $(R/I, +)$ durch

$$\bar{x} \cdot \bar{y} := \overline{x \cdot y} \quad \text{für } \bar{x}, \bar{y} \in R/I$$

zu einem kommutativen Ring mit Eins $1_{R/I} = \overline{1_R}$.

Wir nennen $(R/I, +, \cdot)$ den Faktorring von R nach I.

Beweis:

Zeige: "$\cdot$" ist wohldefiniert, d.h. $\bar{x} = \bar{x'}$, $\bar{y} = \bar{y'} \Rightarrow \overline{x \cdot y} = \overline{x' \cdot y'}$.

Sei $\bar{x} = \bar{x'}$ und $\bar{y} = \bar{y'} \Rightarrow \exists\, a, b \in I : x = x' + a,\ y = y' + b$

$$\Rightarrow x \cdot y = (x' + a) \cdot (y' + b) = x' \cdot y' + \underbrace{(x' \cdot b + a \cdot y' + a \cdot b)}_{\in I}$$

($x' \cdot b \in I$, $a \cdot y' \in I$, $a \cdot b \in I$)

$$\Rightarrow \overline{x \cdot y} = \overline{x' \cdot y'}.$$

Rechne die Axiome für einen Ring nach:

- $(R/I, +)$ ist eine abelsche Gruppe ✓
- $\overline{1_R} \cdot \bar{x} = \overline{1_R \cdot x} = \bar{x}$ für alle $\bar{x} \in R/I$
- $(\bar{x} \cdot \bar{y}) \cdot \bar{z} = \overline{x \cdot y} \cdot \bar{z} = \overline{(x \cdot y) \cdot z} = \overline{x \cdot (y \cdot z)} = \bar{x} \cdot \overline{y z} = \bar{x} \cdot (\bar{y} \cdot \bar{z})$ $\forall \bar{x}, \bar{y}, \bar{z} \in R/I$
- $\bar{x} \cdot \bar{y} = \overline{x \cdot y} = \overline{y \cdot x} = \bar{y} \cdot \bar{x}$ $\forall \bar{x}, \bar{y} \in R/I$
- $\bar{x} \cdot (\bar{y} + \bar{z}) = \bar{x} \cdot \overline{y + z} = \overline{x \cdot (y + z)} = \overline{x \cdot y + x z} = \overline{xy} + \overline{xz} = \bar{x} \cdot \bar{y} + \bar{x} \cdot \bar{z}$
  $\forall \bar{x}, \bar{y}, \bar{z} \in R/I$

□

Bsp. 6.19:

(a) $n \in \mathbb{N} \Rightarrow (\mathbb{Z}_n = \mathbb{Z}/n\mathbb{Z}, +, \cdot)$ ein kommut. Ring mit Eins

z.B.: $n = 2$: $\mathbb{Z}_2 = \{\bar{0}, \bar{1}\}$

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

$\cdot$	$\bar{0}$	$\bar{1}$
$\bar{0}$	$\bar{0}$	$\bar{0}$
$\bar{1}$	$\bar{0}$	$\bar{1}$

$n = 4$: $\mathbb{Z}_4 = \{\bar{0}, \bar{1}, \bar{2}, \bar{3}\}$

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

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

(1) $R = \mathbb{Z}_2[t]$, $I = \langle t^2 + t + 1 \rangle$, $\mathbb{Z}_2 = \{0, 1\}$

Bestimme $R/I = \dfrac{\mathbb{Z}_2[t]}{\langle t^2+t+1 \rangle} = \{ \bar{0}, \bar{1}, \bar{t}, \overline{t+1} \}$

STOP

Beachte: $\overline{t^2} = \bar{t}^2 - \underbrace{\overline{t^2+t+1}}_{=\bar{0}} = \overline{t^2 - t^2 - t - 1} = \overline{-t-1}$

$= \overline{t+1}$

So kann man zeigen, daß alle Polynome Linearen Grades Restklassen der Form $\bar{0}$, $\bar{1}$, $\overline{t+1}$ oder $\bar{t}$ sind!

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

·	$\bar{0}$	$\bar{1}$	$\bar{t}$	$\overline{t+1}$
$\bar{0}$	$\bar{0}$	$\bar{0}$	$\bar{0}$	$\bar{0}$
$\bar{1}$	$\bar{0}$	$\bar{1}$	$\bar{t}$	$\overline{t+1}$
$\bar{t}$	$\bar{0}$	$\bar{t}$	$\overline{t+1}$	$\bar{1}$
$\overline{t+1}$	$\bar{0}$	$\overline{t+1}$	$\bar{1}$	$\bar{t}$

- $\bar{t} \cdot \overline{t+1} = \bar{t}^2 + \bar{t} = \overline{t+1} + \bar{t} = \overline{2t+1} = \bar{1}$
- $\overline{t+1} \cdot \overline{t+1} = \overline{t^2+1} = \overline{t+1} + \bar{1} = \bar{t}$

Beachte: R/I ist in dem Fall sogar ein Körper!

$\cong \mathbb{F}_2[t]/\langle t^2+t+1 \rangle$

F) Homomorphiesatz:

Homomorphiesatz 6.20:

Seien R und S zwei kommut. Ring mit Eins und sei $\varphi: R \to S$ ein Ringhomomorphismus.

① Dann: ⓑ $\overline{\varphi}: \frac{R}{\ker(\varphi)} \xrightarrow{\cong} \operatorname{Im}(\varphi) : \overline{x} \mapsto \varphi(x)$

ist ein Ringisomorphismus.

ⓒ $\ker(\varphi) \trianglelefteq R$.

Beweis:

Beachte: φ ist ein Gruppenhom. von $(R,+)$ nach $(S,+)$ (*)

$\Rightarrow$ $\ker(\varphi)$ ist ein Normalteiler von $(R,+)$

d.h. insb.: $\ker(\varphi) \neq \emptyset$ und abgeschlossen bzgl. $+$

Sei nun $x \in R$, $a \in \ker(\varphi)$.

$\Rightarrow$ $\varphi(x \cdot a) = \varphi(x) \cdot \underbrace{\varphi(a)}_{=0} = \varphi(x) \cdot 0 = 0 \Rightarrow x \cdot a \in \ker(\varphi)$

Damit: $\ker(\varphi) \trianglelefteq R$

Zudem: (*) $\Rightarrow$ $\overline{\varphi}$ ist ein Gruppenisomorphismus

↑ Homomorphiesatz für Gruppen

Zu zeigen noch: $\overline{\varphi}(\overline{x} \cdot \overline{y}) = \overline{\varphi}(\overline{x}) \cdot \overline{\varphi}(\overline{y})$ und $\overline{\varphi}(\overline{1_R}) = 1_S$

- Seien $\overline{x}, \overline{y} \in \frac{R}{\ker(\varphi)}$ $\Rightarrow$ $\overline{\varphi}(\overline{x} \cdot \overline{y}) = \overline{\varphi}(\overline{x \cdot y}) = \varphi(x \cdot y)$
  $= \varphi(x) \cdot \varphi(y) = \overline{\varphi}(\overline{x}) \cdot \overline{\varphi}(\overline{y})$
- $\overline{\varphi}(\overline{1_R}) = \varphi(1_R) = 1_S$

□

Stop

Bsp.: $\varphi : \mathbb{Z}[t] \longrightarrow \mathbb{Q} : f \mapsto f(1)$

Zeige: (a) φ ist ein Gruppenhomom.
(b) Bestimme $\ker(\varphi)$
(c) Bestimme $\mathrm{Im}(\varphi)$

Zu (a): . $\varphi(f \dot{+} g) = (f \dot{+} g)(1) = f(1) \dot{+} g(1) = \varphi(f) \dot{+} \varphi(g)$

. $\varphi(1) = 1$

Zu (b): $\ker(\varphi) = \{ f \in \mathbb{Z}[t] \mid f(1) = 0 \} = \langle t-1 \rangle_{\mathbb{Z}[t]}$

Idee: D.u.R $\Rightarrow$ $f \in \ker(\varphi)$: $f = q \cdot (t-1) + r$

u.t $q, r \in \mathbb{Z}[t]$ und $\deg(r) < 1$, d.h. $r \in \mathbb{Z}$

$\Rightarrow$ $0 = f(1) = q(1) \cdot (1-1) + r = r$

$\Rightarrow$ $f = q \cdot (t-1)$

Zu (c): $\mathrm{Im}(\varphi) = \{ \underbrace{f(1)}_{\in \mathbb{Z}} \mid f \in \mathbb{Z}[t] \} = \mathbb{Z}$

Homsatz: $\dfrac{\mathbb{Z}[t]}{\langle t-1 \rangle_{\mathbb{Z}[t]}} = \dfrac{\mathbb{Z}[t]}{\ker(\varphi)} \cong \mathrm{Im}(\varphi) = \mathbb{Z}$

§ 7 Teilbarkeit in Ringen

A) Integritätsbereiche

Def. 7.1: Sei R ein kommutativer Ring mit Eins und $a \in R$.

(a) a heißt **Nullteiler** in R $:\Leftrightarrow \exists\, b \in R \setminus \{0\} : a \cdot b = 0$

(b) R heißt **Integritätsbereich** / **nullteilerfrei**, falls 0 der einzige Nullteiler ist.

Bsp. 7.1:

(a) $R \neq$ Nullring $\Rightarrow$ 0 ist ein Nullteiler, da $0 \cdot 1 = 0$ ($1 \neq 0$)

(b) $a \in R^*$ $\Rightarrow$ a kein Nullteiler

Denn: STOP

$a \cdot b = 0 \Rightarrow b = 1 \cdot b = (a^{-1} \cdot a) \cdot b = a^{-1} \cdot (a \cdot b) = a^{-1} \cdot 0 = 0$ ✓

(c) K Körper $\Rightarrow$ K ist ein IB z.B.: $\mathbb{Q}, \mathbb{R}, \mathbb{C}$

Denn: $0 \neq a \in K \Rightarrow a$ ist Einheit $\Rightarrow a$ kein NT ✓

(d) $\mathbb{Z}$ ist ein ID.

Denn: $\mathbb{Z}$ ist ein Unterring des IB $\mathbb{Q}$ enthalten.

(e) $\mathbb{Z}[\sqrt{-5}] = \{a + b \cdot \sqrt{-5} \mid a, b \in \mathbb{Z}\}$ ist ein IB,

wobei $\sqrt{-5} = i \cdot \sqrt{5}$. (Addition & Multiplikation in $\mathbb{C}$)

Denn: STOP

Zeige: $\mathbb{Z}[\sqrt{-5}]$ ist Unterring von $\mathbb{C}$

Seien $a + b\sqrt{-5},\ c + d\sqrt{-5} \in \mathbb{Z}[\sqrt{-5}] \neq \emptyset$

- $(a + b\sqrt{-5}) + (c + d\sqrt{-5}) = \underbrace{(a + c)}_{\in \mathbb{Z}} + \underbrace{(b + d)}_{\in \mathbb{Z}} \cdot \sqrt{-5} \in \mathbb{Z}[\sqrt{-5}]$
- $-(a + b\sqrt{-5}) = \underbrace{(-a)}_{\in \mathbb{Z}} + \underbrace{(-b)}_{\in \mathbb{Z}} \cdot \sqrt{-5} \in \mathbb{Z}[\sqrt{-5}]$
- $(a + b\sqrt{-5}) \cdot (c + d\sqrt{-5}) = \underbrace{(ac - 5bd)}_{\in \mathbb{Z}} + \underbrace{(ad + bc)}_{\in \mathbb{Z}} \cdot \sqrt{-5} \in \mathbb{Z}[\sqrt{-5}]$

Zudem: $\mathbb{Z}[\sqrt{-5}]$ als Teilring von $\mathbb{C}$ ein IB. ✓

(f) R IB $\Longrightarrow$ $R[t]$ ist IB und $R[t]^* = R^*$

Denn:

- $f, g \in R[t] \setminus \{0\} \Rightarrow \underset{\in R}{l_c(f)} \neq 0 \neq \underset{\in R}{l_c(g)} \Rightarrow l_c(f) \cdot l_c(g) \neq 0$ (R IB)

  $\Rightarrow \deg(f \cdot g) = \underbrace{\deg(f)}_{\geq 0} + \underbrace{\deg(g)}_{\geq 0} \geq 0 \Rightarrow f \cdot g \neq 0$

- Sei $f \in R[t]^* \Rightarrow \exists\, g \in R[t] : f \cdot g = 1$

  $\Rightarrow 0 = \deg(1) = \deg(f \cdot g) = \underbrace{\deg(f)}_{\geq 0} + \underbrace{\deg(g)}_{\geq 0} \Rightarrow \deg(f) = \deg(g) = 0$

  $\Rightarrow f, g \in R$ und $f \cdot g = 1 \Rightarrow f \in R^*$

- Sei $f \in R^* \Rightarrow \exists\, g \in R \subseteq R[t] : f \cdot g = 1 \Rightarrow f \in R[t]^*$ ✓

(g) $\mathbb{Z}_4 = \mathbb{Z}/4\mathbb{Z}$ ist kein IB

Denn: $\overline{2} \cdot \overline{2} = \overline{4} = \overline{0}$ ($\overline{2} \neq \overline{0}$, $\overline{2} \neq \overline{0}$) $\Rightarrow \overline{2}$ ist ein Nullteiler ✓

Lemma 7.3 (Kürzungsregeln)

Sei R ein IB und $a, b, c \in R$ mit $a \neq 0$.

Dann: (a) $a \cdot b = a \cdot c \Rightarrow b = c$

(b) $b \cdot a = c \cdot a \Rightarrow b = c$

Beweis: (a) $a \cdot b = a \cdot c \Rightarrow 0 = a \cdot b - a \cdot c = a \cdot (b - c)$

$\overset{a \neq 0}{\Longrightarrow}$ (Def. NT) $b - c = 0 \Rightarrow b = c$

(b) folgt aus (a) mit Kommutativgesetz. ✓

Def. 7.4: Sei R ein ID und $a, b \in R$.

(a) b teilt a $:\Leftrightarrow \exists\, c \in R : a = b \cdot c$

Notation: $b \mid a$

(b) $g \in R$ heißt ein größter gemeinsamer Teiler von a und b

$:\Leftrightarrow$ (1) $g \mid a$ und $g \mid b$

(2) $\forall\, h \in R$ mit $h \mid a$ und $h \mid b$ gilt $h \mid g$

Notation: $ggT(a,b) := \{ g \in R \mid g \text{ ist ein größter gem. Teiler von } a \text{ u. } b \}$

(c) $k \in R$ heißt ein kleinstes gemeinsames Vielfaches von a und b

$:\Leftrightarrow$ (1) $a \mid k$ und $b \mid k$

(2) $\forall\, l \in R$ mit $a \mid l$ und $b \mid l$ gilt $k \mid l$

Notation: $kgV(a,b) := \{ k \in R \mid k \text{ ist kleinst. gem. Vielfaches von } a \text{ u. } b \}$

Bsp. 7.5:

(a) $f = t - 1 \in \mathbb{Q}[t]$ und $g = t^n - 1 \in \mathbb{Q}[t]$, $n \geq 1$.

$$\Rightarrow g = (t-1) \cdot (t^{n-1} + t^{n-2} + t^{n-3} + \dots + t + 1) = f \cdot \sum_{k=0}^{n-1} t^k$$

$\Rightarrow f \mid g$ in $\mathbb{Q}[t]$

(b) $a = 9$, $b = 2 + \sqrt{-5}$, $c = 2 - \sqrt{-5}$, $d = 3 \in \mathbb{Z}[\sqrt{-5}]$

Dann: • $a = 9 = (2+\sqrt{-5}) \cdot (2-\sqrt{-5}) = b \cdot c \Rightarrow b \mid a$ in $\mathbb{Z}[\sqrt{-5}]$

• $d \nmid b$

denn: Ang. $d \mid b$ in $\mathbb{Z}[\sqrt{-5}]$

$\Rightarrow \exists\, e = x + y \cdot \sqrt{-5}$ mit $x, y \in \mathbb{Z}$: $b = d \cdot e$

$\Rightarrow 9 = |b|^2 = |d|^2 \cdot |e|^2 = 9 \cdot (x^2 + 5y^2)$ ($|d|^2 = 9$, $|e|^2 = x^2 + 5y^2 \in \mathbb{N}$)

$\Rightarrow x^2 + 5y^2 = 1 \Rightarrow y^2 = 0 \wedge x^2 = 1 \Rightarrow y = 0, x = \pm 1 \Rightarrow b = \pm d$ ($2+\sqrt{-5} = \pm 3$) ↯

(c) $\mathrm{ggT}(6,8) = \{2, -2\}$, $\mathrm{kgV}(6,8) = \{24, -24\}$

gemeinsame Teiler von 6 & 8: $1, 2, -1, -2$

Lemma 7.6:

Sei R ein IB und $a, b \in R$.

Dann: (a) $b \mid a \iff \langle a \rangle_R \subseteq \langle b \rangle_R$

d.h. jedes Vielfache von a ist ein Vielfaches von b

(b) Es sind äquivalent: (1) $b \mid a$ und $a \mid b$

(2) $\langle a \rangle_R = \langle b \rangle_R$ (3) $\exists u \in R^* : a = b \cdot u$

d.h. a & b unterscheiden sich nur um eine Einheit (als Faktor)

Beweis: (a) "$\Rightarrow$" Sei $b \mid a \Rightarrow \exists c \in R : a = b \cdot c$

Sei nun $x \in \langle a \rangle_R \Rightarrow \exists r \in R : x = a \cdot r \overset{a = b \cdot c}{=} (b \cdot c) \cdot r = b \cdot \underbrace{(c \cdot r)}_{\in R} \in \langle b \rangle_R$

Also: $\langle a \rangle_R \subseteq \langle b \rangle_R$

"$\Leftarrow$" Sei $\langle a \rangle_R \subseteq \langle b \rangle_R \Rightarrow a \in \langle a \rangle_R \subseteq \langle b \rangle_R \Rightarrow \exists r \in R : a = b \cdot r \Rightarrow b \mid a$

(b) (1) $\Rightarrow$ (2): folgt aus (a)

(2) $\Rightarrow$ (3): 1. Fall: $a = 0 \Rightarrow b \in \langle b \rangle_R = \langle a \rangle_R = \{0\} \Rightarrow b = 0 \overset{1 \cdot b}{=} a$

2. Fall: $a \neq 0 \Rightarrow a \in \langle b \rangle_R$ und $b \in \langle a \rangle_R$

$\Rightarrow \exists u, v \in R : a = b \cdot u$ und $b = a \cdot v$

$\Rightarrow a \overset{a \cdot 1}{=} a \cdot v \cdot u \underset{a \neq 0}{\Rightarrow} 1 = v \cdot u \Rightarrow u \in R^*$

(3) $\Rightarrow$ (1): $a = b \cdot u$ mit $u \in R^* \Rightarrow b = a \cdot u^{-1}$

$\Downarrow$ $\Downarrow$

$b \mid a$ $a \mid b$

□

Lemma 7.7:

Sei R ein ID und $a, b, g, h \in R$.

(a) $g \in ggT(a,b) \iff$ (1) $\langle a,b\rangle_R \subseteq \langle g\rangle_R$

(2) $\forall\, l \in R$ mit $\langle a,b\rangle_R \subseteq \langle l\rangle_R$ gilt $\langle g\rangle_R \subseteq \langle l\rangle_R$

(b) $h \in kgV(a,b) \iff$ (1) $\langle h\rangle_R \subseteq \langle a\rangle_R \cap \langle b\rangle_R$

(2) $\forall\, l \in R$ mit $\langle l\rangle_R \subseteq \langle a\rangle_R \cap \langle b\rangle_R$ gilt $\langle l\rangle_R \subseteq \langle h\rangle_R$

(c) $g \in ggT(a,b) \Rightarrow ggT(a,b) = \{u \cdot g \mid u \in R^*\}$

(d) $h \in kgV(a,b) \Rightarrow kgV(a,b) = \{u \cdot h \mid u \in R^*\}$

Beweis: (a) & (b): folgen aus Def. + 7.6

(c) & (d): Üb A.

B) Faktorielle Ringe

Motivation 7.8: Sei $p \in \mathbb{Z}$, $p > 1$.

Dann: p ist eine Primzahl

$\Leftrightarrow$ $1, -1, p, -p$ sind die einzigen Teiler von p.

$\Leftrightarrow$ ($p = a \cdot b \Rightarrow a \in \mathbb{Z}^* = \{1,-1\}$ oder $b \in \mathbb{Z}^* = \{1,-1\}$)

{ a & b sind Teiler von p und nicht beide können p v $-p$ sein }

$\Leftrightarrow$ ($p \mid a \cdot b \Rightarrow p \mid a$ oder $p \mid b$)

{ bedeutet Primfaktorzerlegung von a und b }

Def. 7.9: Sei R ein IB.

(a) $0 \neq p \in R \setminus R^*$ heißt irreduzibel $:\Leftrightarrow$ ($p = a \cdot b \Rightarrow a \in R^*$ oder $b \in R^*$)

(b) $0 \neq p \in R \setminus R^*$ heißt prim $:\Leftrightarrow$ ($p \mid a \cdot b \Rightarrow p \mid a$ oder $p \mid b$)

(c) R heißt faktoriell (oder ZPE-Ring)

$:\Leftrightarrow$ jedes $0 \neq a \in R \setminus R^*$ ist ein Produkt von endlich vielen Primelementen.

Bsp. 7.10:

(a) In $\mathbb{Z}$ gilt: prim $\triangleq$ irreduzibel. (folgender Bew. später)

(b) k = Körper und $f \in k[t]$ mit $\deg(f) = 1 \Rightarrow f$ irreduzibel

denn: Sei $f = g \cdot h \Rightarrow 1 = \deg(f) = \underbrace{\deg(g)}_{\geq 0} + \underbrace{\deg(h)}_{\geq 0}$

$\Rightarrow$ o.E. $\deg(h) = 1 \wedge \deg(g) = 0 \Rightarrow g \in k \setminus \{0\} = k^* = k[t]^*$

$\Rightarrow f$ irreduzibel ⊡

(c) $f = 2t + 2 \in \mathbb{Z}[t]$ ist nicht irreduzibel

denn: $f = 2 \cdot (t+1)$ mit $2, t+1 \notin \mathbb{Z}[t]^* = \mathbb{Z}^* = \{1,-1\}$

(d) R IB, $p, q \in R$ irred. und $p \mid q \Rightarrow \langle p \rangle_R = \langle q \rangle_R$

denn: $p \mid q \Rightarrow \exists u \in R: q = u \cdot p \underset{q \text{ irr.}, p \notin R^*}{\Longrightarrow} u \in R^* \Rightarrow \langle p \rangle_R = \langle q \rangle_R$

Lemma 7.11:

Ist R ID und $p \in R$ prim, dann ist p irreduzibel.

Beweis:

Sei $p = a \cdot b$ mit $a, b \in R$. $\Rightarrow p \mid a \cdot b \underset{p \text{ prim}}{\Rightarrow} p \mid a$ o.E. oder $p \mid b$

o.E.: $p \mid a \Rightarrow \exists u \in R: a = p \cdot u \Rightarrow p \underset{p \neq 0}{=} a \cdot b = p \cdot u \cdot b$

$\Rightarrow 1 = u \cdot b \Rightarrow b \in R^*$. Also: p irreduzibel. ☐

Bsp. 7.12:

(a) p irreduzibel $\not\Rightarrow$ p prim

Bsp.: $R = \mathbb{Z}[\sqrt{-5}]$, $a = 9$, $b = 2 + \sqrt{-5}$, $c = 2 - \sqrt{-5}$, $d = 3$

7.6 $\Rightarrow d \nmid b$. Analog: $d \nmid c$

Aber: $d = 3 \mid 9 = b \cdot c \Rightarrow d$ ist nicht prim

Zeige: d ist irreduzibel in $\mathbb{Z}[\sqrt{-5}]$.

Sei $f = x + y \cdot \sqrt{-5}$, $g = u + v \cdot \sqrt{-5}$ mit $d = f \cdot g$

$\Rightarrow 9 = |d|^2 = |f|^2 \cdot |g|^2 = \underbrace{(x^2 + 5 \cdot y^2)}_{\in \mathbb{N}} \cdot \underbrace{(u^2 + 5 \cdot v^2)}_{\in \mathbb{N}}$ $*_3$ $*_3$

$\Rightarrow$ o.E.: $x^2 + 5y^2 = 1$ und $u^2 + 5 \cdot v^2 = 9$

$\Downarrow$

$x = \pm 1, y = 0$

$\Downarrow$

$g = \pm 1 \in \mathbb{Z}[\sqrt{-5}]^*$

$\Rightarrow d$ ist irreduzibel ☐

(b) R faktoriell $\Rightarrow$ (f irreduzibel $\Leftrightarrow$ f prim)

Insbesondere: $\mathbb{Z}[\sqrt{-5}]$ nicht faktoriell

① zeige: "⇐" 7.11

"⇒" Sei f irreduzibel $\overset{R \text{ fakt.}}{\Rightarrow}$ $\exists\, q_1, \dots, q_k$ prim: $f = q_1 \cdots q_k$

Ang.: $k \geq 2$. $\Longrightarrow$ f irred. $\Rightarrow q_1 \notin R^*$ $q_2 \cdots q_k \in R^* \Rightarrow q_2 \in R^*$ ↯ q_2 prim

Also: $f = q_1$ ist prim ①

Korollar 7.13:

Für $0 \neq n \in \mathbb{Z}$ sind ①:

(a) $\mathbb{Z}_n$ ist ein Körper. (b) $\mathbb{Z}_n$ ist ein ID.

(c) n ist prim in $\mathbb{Z}$ (d) n ist irreduzibel in $\mathbb{Z}$.

Beweis:

(a) ⇒ (b): 7.2 (c)

(b) ⇒ (c): Sei $a, b \in \mathbb{Z}$ mit $n \mid a \cdot b$ $\Rightarrow$ $\bar{a} \cdot \bar{b} = \overline{a \cdot b} \overset{!}{=} \bar{0} \in \mathbb{Z}_n$

$\Rightarrow$ ($\mathbb{Z}_n$ ID) $\bar{a} = 0$ oder $\bar{b} = \bar{0}$ $\Rightarrow$ $n \mid a$ oder $n \mid b$

Also: n ist prim

(c) ⇒ (d): 7.11

(d) ⇒ (a): Es reicht zu zeigen, daß $\mathbb{Z}_n$ genau 2 Ideale hat!

Sei $I \trianglelefteq \mathbb{Z}_n$ $\Rightarrow$ $(I, +) \leq (\mathbb{Z}_n, +)$ Untergruppe

$\Rightarrow$ (Lagrange) $n = |\mathbb{Z}_n| = |I| \cdot |\mathbb{Z}_n : I|$ $\Rightarrow$ (n irred.) $|I| = 1$ oder $|I| = n$

$\Rightarrow$ $I = \{0\}$ oder $I = \mathbb{Z}_n$ $\Rightarrow$ $\mathbb{Z}_n$ Körper!

⑤

Bem. 7.14:

(a) R faktoriell und $0 \neq a \in R \setminus R^*$ $\Rightarrow$ die Darstellung von a als Produkt von Primelementen ist bis auf Reihenfolge eindeutig

d.h. $a = p_1 \cdots p_r = q_1 \cdots q_s$ mit p_i, q_j prim

dann: $r = s$ und nach Umnummerierung gilt $\langle p_i \rangle_R = \langle q_i \rangle_R$ $\forall i = 1, \dots, r$

⑤ R faktoriell, $a = u \cdot p_1^{m_1} \cdots p_r^{m_r}$, $b = v \cdot p_1^{n_1} \cdots p_r^{n_r}$

mit $u, v \in R^*$, p_i prim und $\langle p_i \rangle_R \neq \langle p_j \rangle_R$ für $i \neq j$

$\Rightarrow$ $p_1^{\min\{m_1,n_1\}} \cdots p_r^{\min\{m_r,n_r\}} \in ggT(a,b)$

$p_1^{\max\{m_1,n_1\}} \cdots p_r^{\max\{m_r,n_r\}} \in kgV(a,b)$

C) Euklidische Ringe

Def. 7.15:

Sei R ein IB. Dann heißt R euklidischer Ring, wenn es eine Funktion $\nu : R \setminus \{0\} \to \mathbb{N}$ gibt, so daß gilt:

$\forall a, b \in R \setminus \{0\} \; \exists q, r \in R : \; a = q \cdot b + r$ mit $r = 0$ oder $\nu(r) < \nu(b)$.

Man nennt dies eine Division mit Rest von a durch b und ν eine Euklidische Funktion für R.

Bsp. 7.16:

$\mathbb{Z}$ ist ein euklidischer Ring mit euklidischer Funktion $|\cdot| : \mathbb{Z} \to \mathbb{N}$.

Denn: $\forall a, b \in \mathbb{Z} \setminus \{0\} : \; \exists q, r \in \mathbb{Z} : \; a = q \cdot b + r$ mit $|r| < |b|$

Prop. 7.17:

Sei R ein kommut. Ring mit Eins und $f, g \in R[t]$ mit $lc(f) \in R^*$.

Dann: $\exists_1 \; q, r \in R[t] : \; g = q \cdot f + r$ mit $\deg(r) < \deg(f)$

Beweis:

Existenz: Sei $f = \sum_{i=0}^{n} a_i t^i$, $g = \sum_{i=0}^{m} b_i t^i$ mit $a_n \in R^*$ und $b_m \neq 0$.

Induktion nach $m = \deg(g)$:

$m = n = 0$: $q = \frac{b_0}{a_0}$, $r = 0$ ✓

$0 \leq m < n$: $q = 0$, $r = 0$ ✓

} → Induktionsanfang $m = 0$ ✓

$0 \leq n \leq m$ & $m > 0$:

Setze $g' := g - \frac{b_m}{a_n} \cdot f \cdot t^{m-n} \in R[t]$

$\Rightarrow \deg(g') < \deg(g)$

$\overset{\text{Ind.}}{\Rightarrow} \exists\, q', r \in R[t] : g' = q' \cdot f + r$ und $\deg(r) < \deg(f)$

$g' = g - \frac{b_m}{a_n} \cdot f \cdot t^{m-n}$

$\Rightarrow g = \underbrace{(q' + \frac{b_m}{a_n} \cdot t^{m-n})}_{=: q} \cdot f + r$ und $\deg(r) < \deg(f)$ $\in R[t]$

Eindeutigkeit:

Sei $g = q \cdot f + r = q' \cdot f + r'$ mit $\deg(r), \deg(r') < \deg(f)$.

$\Rightarrow (q - q') \cdot f = r' - r$ und $\deg(r - r') \leq \max\{\deg(r), \deg(r')\} < \deg(f)$

$\deg(q - q') + \deg(f)$

$\Rightarrow q - q' = 0 \Rightarrow q = q'$ und $r' - r = 0 \Rightarrow r = r'$ ☐

Korollar 7.18:

Wenn k ein Körper ist, dann ist $k[t]$ ein euklidischer Ring mit $\deg$ als euklidischer Funktion.

Beispiel 7.19:

$g = 5t^3 + 2t^2 - 3, \quad f = t + 2 \in \mathbb{Q}[t]$

$$5\cdot t^3 + 2t^2 \quad -3 \;:\; (t+2) = \underbrace{5t^2 - 4\cdot t + 16}_{\text{“}q\text{”}} + \frac{-35}{t+2}$$

$$\begin{array}{r} 5t^3 + 10t^2 \\ \hline -8t^2 \quad -3 \\ -8t^2 - 16t \\ \hline 16t - 3 \\ 16t + 32 \\ \hline -35 \end{array}$$

$\Rightarrow$ $r = -35$

$$\Rightarrow \quad g = (5t^2 - 8t + 16)\cdot f - 35$$

Motivation 7.20 (Euklidischer Algorithmus)

Ziel: Bestimme einen ggT von 84 und 30!

$84 = 2^2 \cdot 3 \cdot 7$ $\qquad$ $30 = 2 \cdot 3 \cdot 5$

$\rightsquigarrow$ $g = 2 \cdot 3 = 6 \in ggT(84, 30)$

Alternativ: mithilfe Division mit Rest!

① $84 = 2 \cdot 30 + 24$

② $30 = 1 \cdot 24 + 6$ $\quad 6 \in ggT(84, 30)$

③ $24 = 4 \cdot 6 + 0$

Wieso geht das ?!?!

Satz 7.21 (Euklidischer Algorithmus)

Input: R euklidischer Ring mit euklidischer Fkt. $\nu : R \setminus \{0\} \to \mathbb{N}$
sowie $a, b \in R \setminus \{0\}$

Output: $g \in ggT(a, b)$

Algorithmus:

① Setze $r_0 := a$, $r_1 := b$, $k := 2$

② Solange $(r_{k-1} \neq 0)$:
- Wähle $r_k, q_{k-1} \in R$ mit $r_{k-2} = q_{k-1} \cdot r_{k-1} + r_k$ und
$(r_k = 0$ oder $\nu(r_k) < \nu(r_{k-1}))$
- $k \mapsto k+1$

③ Gib r_{k-2} zurück

Beweis:

Terminierung:

Beachte: solange $r_{k-1} \neq 0$, können wir den D.u.R. in (2) durchführen und erhalten $r_k, q_{k-1} \in \mathbb{R}$ wie oben!

D.h. wir erhalten:

(1)	$r_0 = q_1 \cdot r_1 + r_2$,	$(k=2)$	$\nu(r_2) < \nu(r_1)$ oder $r_2 = 0$
(2)	$r_1 = q_2 \cdot r_2 + r_3$,	$(k=3)$	$\nu(r_3) < \nu(r_2)$ oder $r_3 = 0$
(3)	$r_2 = q_3 \cdot r_3 + r_4$,	$(k=4)$	$\nu(r_4) < \nu(r_3)$ oder $r_4 = 0$
	$\vdots$		

$\Rightarrow$ $\nu(r_1) > \nu(r_2) > \nu(r_3) > \dots$ ist eine absteigende Folge natürlicher Zahlen!

$\Rightarrow$ die Folge und das Verfahren müssen abbrechen, d.h. nach endlichen vielen Schritten gilt $r_n = 0$

Korrektheit:

Zeige mit Induktion nach $n := \#(\text{Durchläufe der Schleife})$

daß $r_n \in ggT(r_0, r_1)$

I.A.: $n=1$: $r_2 = 0$ und $r_0 = q_1 \cdot r_1 \Rightarrow r_1 \in ggT(r_0, r_1)$

I.S.: $n \geq 2$: Betrachte nun die letzten $n-1$ Durchläufe der Schleife.

$\overset{\text{Ind.}}{\Rightarrow}$ $r_n \in ggT(r_1, r_2)$

Zeige: $r_n \in ggT(r_0, r_1)$

- $r_n \in ggT(r_1, r_2) \Rightarrow r_n \mid r_1$ und $r_n \mid r_2$

$\Rightarrow$ $r_n \mid q_1 \cdot r_1 + r_2 = r_0$

• Sei $r \in R$ mit $r \mid r_0$ und $r \mid r_1$

$\Rightarrow \quad r \mid r_0 - q_1 \cdot r_1 = r_2$

$\Rightarrow \quad r \mid r_n$

$r_n \in ggT(r_1, r_2)$

Also: $\quad r_n \in ggT(r_0, r_1)$ ☒

Bsp. 7.22:

Sei $r_0 = t^5 + t^3 + \bar{2} \cdot t^2 + \bar{2}, \quad r_1 = t^3 + \bar{2} \cdot t^2 + t + \bar{2} \in \mathbb{Z}_5[t]$

STOP

(1) $r_0 = q_1 \cdot r_1 + r_2 = [\, t^2 + \bar{3} t + \bar{4} \,] \cdot r_1 + [\, \bar{4} t^2 + \bar{4} \,]$

D.m.R.:

$t^5 + t^3 + \bar{2} t^2 + \bar{2} : (t^3 + \bar{2} t^2 + t + \bar{2}) = t^2 + \bar{3} \cdot t + \bar{4} =: q_1$

$t^5 + \bar{2} t^4 + t^3 + \bar{2} \cdot t^2$

$\bar{3} t^4 + \bar{2}$

$\bar{3} t^4 + t^3 + \bar{3} t^2 + t$

$\bar{4} t^3 + \bar{2} t^2 + \bar{4} t + \bar{2}$

$\bar{4} t^3 + \bar{3} t^2 + \bar{4} t + \bar{3}$

$\bar{4} t^2 + \bar{4} = r_2$

(2) $r_1 = q_2 \cdot r_2 + r_3 = [\, \bar{4} \cdot t + \bar{3} \,] \cdot r_2 + [\, 0 \,]$

D.m.R.:

$t^3 + \bar{2} t^2 + t + \bar{2} : (\bar{4} t^2 + \bar{4}) = \bar{4} \cdot t + \bar{3} =: q_2$

$t^3 + t$

$\bar{2} t^2 + \bar{2}$

$\bar{2} \cdot t^2 + \bar{2}$

$0 = r_3$

Also: $\quad r_2 = \bar{4} t^2 + \bar{4} \in ggT(r_0, r_1)$

$\Rightarrow \quad t + \bar{1} \in ggT(r_0, r_1)$ ☐

D) Der Polynomring

Lemma 7.23:

Sei S ein Ring mit 1 und R ein kommutativer Unterring von S und $b \in S$. Dann ist die Abbildung

$$\phi_b : R[t] \to S : f \mapsto f(b),$$

mit $f(b) = \sum_{k=0}^{n} a_k \cdot b^k$ für $f = \sum_{k=0}^{n} a_k t^k$, ein Ringhomomorphismus.

Für ein konstantes Polynom $f = a_0 \cdot t^0$ gilt $\phi_b(f) = f(b) = a_0$, und falls $R = S$, dann ist ϕ_b auch surjektiv.

Beweis:

Seien $f = \sum_{k=0}^{n} a_k t^k$, $g = \sum_{i=0}^{m} b_i t^i \in R[t]$, $a_k = 0 \ \forall k \notin \{0, \dots, n\}$, $b_k = 0 \ \forall k \notin \{0, \dots, m\}$

$$\Rightarrow \cdot \ \phi_b(f+g) = \phi_b\left(\sum_{k=0}^{\max(m,n)} (a_k + b_k) \cdot t^k\right) = \sum_k (a_k + b_k) \cdot b^k = \sum_k a_k \cdot b^k + \sum_k b_k \cdot b^k$$

$$= f(b) + g(b) = \phi_b(f) + \phi_b(g)$$

$$\cdot \ \phi_b(f \cdot g) = \phi_b\left(\sum_{k=0}^{m+n} \left(\sum_{i+j=k} a_i \cdot b_j\right) \cdot t^k\right) = \sum_{k=0}^{m+n} \left(\sum_{i+j=k} a_i b_j\right) \cdot b^k$$

$$= \sum_{k=0}^{n} a_i b^i \cdot \sum_{j=0}^{m} b_j \cdot b^j = f(b) \cdot g(b) = \phi_b(f) \cdot \phi_b(g)$$

$$\cdot \ \phi_b(a_0 \cdot t^0) = a_0 \cdot b^0 = a_0 \cdot 1_S = a_0 \Rightarrow \phi_b(1_{R[t]}) = 1_S$$

$\Rightarrow \phi_b$ ist ein Ringhomomorphismus

Sei nun also $R = S$:

Für $a \in R$ gilt: $\phi_b(a \cdot t^0) = a \Rightarrow \phi_b$ ist surjektiv

□

Def. 7.24:

Sei S ein Ring mit 1 und R ein kommut. Teilring von S.

$b \in S$ heißt Nullstelle von $f \in R[t]$ in S $:\Leftrightarrow$ $f(b) = \phi_b(f) = 0$

Prop. 7.25:

Sei R ein kommut. Ring mit 1 und $b \in R$ sei Nst. von $g \in R[t]$.

Dann: $\exists\ q \in R[t] : \quad g = q \cdot (t-b)$

Wir nennen $t-b$ dann einen Linearfaktor von g.

Insbesondere, wenn $\left(\begin{matrix}\deg(g) \geq 2 \\ \text{und } R \text{ IB}\end{matrix}\right)$, dann ist g nicht irreduzibel.

Beweis:

D.m.R. $\Rightarrow \exists\ q, r \in R[t] : \quad g = q \cdot (t-b) + r$ und $\deg(r) < \deg(t-b) = 1$

$\Rightarrow \quad r = r_0 \cdot t^0$ mit $r_0 \in R$

$\Rightarrow \quad 0 = \phi_b(g) = \phi_b(q \cdot (t-b) + r) = q(b) \cdot \underbrace{(b-b)}_{=0} + r(b) = r_0 \cdot b^0 = r_0$

$\Rightarrow \quad r = r_0 \cdot t^0 = 0 \quad \Rightarrow \quad g = q \cdot (t-b).$

Sei jetzt R IB und $\deg(g) \geq 2$.

$\Rightarrow \quad 2 \leq \deg(g) = \deg(q \cdot (t-b)) = \deg(q) + \deg(t-b) = \deg(q) + 1$

$\Rightarrow \quad \deg(q) \geq 1 \quad \Rightarrow \quad q \in R^* = R[t]^*$ und $t-b \in R^* = R[t]^*$

$\Rightarrow$ g nicht irreduzibel. ☐

Bsp. 7.26:

$f = t^5 + t^4 + t^3 + t^2 + t + \bar{1} \in \mathbb{Z}_2[t]$

$\Rightarrow \quad f(\bar{1}) = \bar{1} + \bar{1} + \bar{1} + \bar{1} + \bar{1} + \bar{1} = \bar{0}$

$\Rightarrow \quad f = (t^4 + t^2 + \bar{1}) \cdot (t - \bar{1})$

D.m.R.

Satz 7.27:

Sei R ein IB und $0 \neq f \in R[t]$.

Dann gilt f hat höchstens $\deg(f)$ viele Nullstellen in R.

Beweis: ü.A. ☐

E) Hauptidealringe

Def. 7.28:

Ein IB R heißt **Hauptidealring**, wenn jedes Ideal in R ein Hauptideal ist, d.h. $\forall\, I \trianglelefteq R \;\exists\, a \in R : I = \langle a \rangle_R$.

Satz 7.29:

Jeder **euklidische Ring** ist ein **Hauptidealring**.

Insbesondere: $\mathbb{Z}$ und $k[t]$ sind Hauptidealringe.

Beweis:

Sei R ein eukl. Ring mit eukl. Funktion $\nu : R \setminus \{0\} \to \mathbb{N}$ und sei $\{0\} \neq I \trianglelefteq R$.

Betrachte: $\Pi := \{ \nu(a) \mid 0 \neq a \in I \} \subseteq \mathbb{N}$ $\neq \emptyset$

$\overset{AP}{\Rightarrow} \exists\, n := \min(\Pi) \Rightarrow \exists\, b \in I \setminus \{0\} : \nu(b) = n = \min(\Pi)$

Zeige: $I = \langle b \rangle_R$.

"$\supseteq$" Sei $r \in R \Rightarrow r \cdot b \in I \Rightarrow \langle b \rangle_R \subseteq I$.

"$\subseteq$" Sei $a \in I \underset{\text{D.m.R.}}{\Rightarrow} \exists\, q, r \in R : a = q \cdot b + r$ und $(r = 0$ oder $\nu(r) < \nu(b))$

$\Rightarrow r = a - q \cdot b \in I$ ($a \in I$, $q \cdot b \in I$) $\Longrightarrow r = 0 \Rightarrow a = q \cdot b \in \langle b \rangle_R$

$\Rightarrow I \subseteq \langle b \rangle_R$

□

Satz 7.30 (Bézout-Identität)

Sei R ein HIR und $g, a, b \in R$.

Dann: $g \in ggT(a,b) \iff \langle g \rangle_R = \langle a, b \rangle_R$

Insbesondere:
- $g \in ggT(a,b) \Rightarrow \exists\, r, s \in R : g = r \cdot a + s \cdot b$
- $1 \in ggT(a,b) \Rightarrow \exists\, r, s \in R : 1 = r \cdot a + s \cdot b$

Bézout Identität

Beweis:

"$\Rightarrow$" Sei $g \in ggT(a,b)$. Z.z.: $\langle g \rangle_R = \langle a,b \rangle_R$.

Bemerke: R HIR $\Rightarrow \exists h \in R : \langle a,b \rangle_R = \langle h \rangle_R$

$\Rightarrow$ • $\langle h \rangle_R = \langle a,b \rangle_R \overset{7.7}{\subseteq} \langle g \rangle_R$ ($g \in ggT(a,b)$)

• $a,b \in \langle h \rangle_R \Rightarrow h \mid a \wedge h \mid b \Rightarrow h \mid g$

$\Rightarrow \langle h \rangle_R \supseteq \langle g \rangle_R$

$\Rightarrow \langle g \rangle_R = \langle h \rangle_R = \langle a,b \rangle_R$.

"$\Leftarrow$" Sei $\langle a,b \rangle_R = \langle g \rangle_R \Rightarrow \langle a,b \rangle_R \subseteq \langle g \rangle_R$ (1)

Sei zudem $h \in R$ s.t. $\langle a,b \rangle_R \subseteq \langle h \rangle_R$

$\Rightarrow \langle g \rangle_R = \langle a,b \rangle_R \subseteq \langle h \rangle_R$ (2)

7.7 + (1) + (2) $\Rightarrow g \in ggT(a,b)$ ☐

Bem. 7.31:

In einem eukl. Ring können wir $r,s \in R$ mit $r \cdot a + s \cdot b \in ggT(a,b)$ mit dem euklid. Alg. berechnen!

Bsp: $a = 136$, $b = 51$

$\Rightarrow$ (1) $136 = 2 \cdot 51 + 34$

(2) $51 = 1 \cdot 34 + \boxed{17} \in ggT(a,b) = ggT(136,51)$

(3) $34 = 2 \cdot 17 + 0$

$\Rightarrow 17 \overset{(2)}{=} 51 - 1 \cdot 34$

$\overset{(1)}{=} 51 - 1 \cdot (136 - 2 \cdot 51)$

$= 3 \cdot 51 - 1 \cdot 136$

$= s \cdot b + r \cdot a \Rightarrow s = 3,\ r = -1$

Korollar 7.32:

Für $0 \neq n \in \mathbb{N}$ gilt: $\mathbb{Z}_n^* = \{ \bar{a} \in \mathbb{Z}_n \mid 1 \in ggT(a,n) \}$

Beweis:

"$\subseteq$" Sei $\bar{a} \in \mathbb{Z}_n^* \Rightarrow \exists\, \bar{b} \in \mathbb{Z}_n : \bar{1} = \bar{a} \cdot \bar{b} = \overline{a \cdot b}$

$\Rightarrow 1 - a \cdot b \in n \cdot \mathbb{Z} \Rightarrow \exists\, z \in \mathbb{Z} : 1 - a \cdot b = n \cdot z$

$\Rightarrow 1 = a \cdot b + n \cdot z \in \langle a, n \rangle_{\mathbb{Z}}$

$\Rightarrow \langle 1 \rangle_{\mathbb{Z}} = \langle a, n \rangle_{\mathbb{Z}} \Rightarrow 1 \in ggT(a,n)$.

"$\supseteq$" Sei $1 \in ggT(a,n) \overset{\text{B.Z.}}{\Rightarrow} \exists\, r, s \in \mathbb{Z} : 1 = r \cdot a + s \cdot n$

$\Rightarrow \bar{1} = \overline{r \cdot a + s \cdot n} = \bar{r} \cdot \bar{a} + \bar{s} \cdot \underbrace{\bar{n}}_{\bar{0}} = \bar{r} \cdot \bar{a} \Rightarrow \bar{a} \in \mathbb{Z}_n^*$

□

Bem. 7.33:

Der Beweis von 7.32 ist konstruktiv, d.h. wir können zu a und n mit $1 \in ggT(a,n)$ das Inverse $\bar{a}^{-1}$ von $\bar{a} \in \mathbb{Z}_n$ berechnen!

z.B.: $a = 5$, $n = 12$

① $12 = 2 \cdot 5 + 2$

② $5 = 2 \cdot 2 + 1 \in ggT(5, 12)$

③ $2 = 2 \cdot 1 + 0$

$\Rightarrow 1 \overset{②}{=} 5 - 2 \cdot 2 \overset{①}{=} 5 - 2 \cdot (12 - 2 \cdot 5)$

$= 5 \cdot 5 - 2 \cdot 12 = 5 \cdot a - 2 \cdot n$

$\Rightarrow \bar{1} = \bar{5} \cdot \bar{a} \in \mathbb{Z}_{12} \Rightarrow \bar{a}^{-1} = \bar{5}$

Lemma 7.34:

Sei R ein HIR, $a \in R$ irreduzibel, $b \in R \setminus \langle a \rangle_R$.

Dann: $1 \in ggT(a,b)$. Insb.: $\exists r,s \in R: 1 = r \cdot a + s \cdot b$

Beweis:

Es reicht z.Z.: $g \in ggT(a,b) \Rightarrow g \in R^*$

Sei $g \in ggT(a,b) \Rightarrow \langle g \rangle_R \overset{7.30}{=} \langle a,b \rangle_R \supsetneq \langle a \rangle_R$

$\Rightarrow \exists c \in R: a = g \cdot c$ und $c \notin R^*$

$\overset{a \text{ irred.}}{\Rightarrow} g \in R^* \Rightarrow 1 \in ggT(a,b)$ ☐

Lemma 7.35:

Sei R ein HIR und $a \in R$ irreduzibel, dann ist a prim.

Beweis:

Ang: a nicht prim

$\Rightarrow \exists b,c \in R: a \mid b \cdot c$, aber $a \nmid b$, $a \nmid c$

$\Rightarrow b \in R \setminus \langle a \rangle_R \wedge c \in R \setminus \langle a \rangle_R$

$\overset{7.34}{\Rightarrow} \exists r,s,r',s' \in R: 1 = r \cdot a + s \cdot b = r' \cdot a + s' \cdot c$

$\Rightarrow 1 = 1 \cdot 1 = (ra + sb) \cdot (r'a + s'c)$

$= \underbrace{r \cdot a \cdot r' \cdot a}_{\in \langle a \rangle_R} + \underbrace{r \cdot a \cdot s' \cdot c}_{\in \langle a \rangle_R} + \underbrace{s \cdot b \cdot r' a}_{\in \langle a \rangle_R} + \underbrace{s \cdot s' \cdot b \cdot c}_{\in \langle a \rangle_R} \in \langle a \rangle_R$

$\Rightarrow a \in R^*$ ↯ a irreduzibel

☐

Satz 7.36

Jeder HIR ist faktoriell.

Insbesondere: $\mathbb{Z}$ und $K[t]$ sind faktoriell!

Beweis:

Wegen 7.35 reicht es z.z.:

Jedes $0 \neq a \in R \setminus R^*$ ist Produkt von endl. vielen Irreduziblen!

Ang: $\exists\, 0 \neq a \in R \setminus R^*$: a ist nicht Produkt von endlich vielen irreduziblen Elementen!

$\Rightarrow$ a ist nicht irreduzibel

$\Rightarrow$ $\exists\, b, c \in R \setminus R^*$: $a = b \cdot c$

$\Rightarrow$ • $\langle a \rangle_R \subsetneq \langle b \rangle_R$ und $\langle a \rangle_R \subsetneq \langle c \rangle_R$

• b oder c ist nicht Prod. von endl. vielen Irred.

$\Rightarrow$ o.E.: b ist nicht Prod. von endl. vielen Irred.

Setze: $a_0 := a$ und $a_1 := b$

Fahre mit a_1 wie mit a_0 fort und konstruiere rekursiv eine Folge von Idealen:

$$\langle a_0 \rangle_R \subsetneq \langle a_1 \rangle_R \subsetneq \langle a_2 \rangle_R \subsetneq \langle a_3 \rangle_R \subsetneq \dots \quad (*)$$

Setze: $I := \bigcup_{i=0}^{\infty} \langle a_i \rangle_R$

Zeige: $I \trianglelefteq R$. Seien $x, y \in I \Rightarrow \exists\, i, j : x \in \langle a_i \rangle_R,\ y \in \langle a_j \rangle_R$

$\Rightarrow$ o.E.: $i \leq j \Rightarrow x \in \langle a_i \rangle_R \subseteq \langle a_j \rangle_R$ (*) und $y \in \langle a_j \rangle_R$

$\Rightarrow x + y \in \langle a_j \rangle_R \subseteq I$. Zudem: $\forall r \in R : r \cdot x \in \langle a_i \rangle_R \subseteq I$.

Da R ein HIR ist, gilt: $\exists\, s \in R : \langle s \rangle_R = I = \bigcup_{i=0} \langle a_i \rangle_R$

$\Rightarrow \exists i : s \in \langle a_i \rangle_R \Rightarrow \langle a_{i+1} \rangle_R \subseteq I = \langle s \rangle_R \subseteq \langle a_i \rangle_R$ ↯ zu (*)

F) Fundamentalsatz der elementaren Zahlentheorie

Folgerung 7.37:

Für jede ganze Zahl $z \neq z \in \mathbb{Z} \setminus \{-1, 1\}$ gibt es eindeutig bestimmte Primzahlen $p_1, \dots, p_k \in \mathbb{P} = \{p > 0 \mid p \text{ prim}\}$ und positive Zahlen $u_1, \dots, u_k \in \mathbb{Z}_{>0}$, so dass $z = \operatorname{sgn}(z)\, p_1^{u_1} \cdot \dots \cdot p_k^{u_k}$

Hier $\operatorname{sgn}(z) := \begin{cases} +1, & z > 0 \\ -1, & z < 0 \end{cases}$.

Notation: $n_p(z) := \max\{n \in \mathbb{N} \mid p^n \mid z\}$ für $p \in \mathbb{P}$, $z \in \mathbb{Z} \setminus \{0\}$

$\rightarrow$ $n_p(z) = \begin{cases} u_i, & p = p_i \\ 0, & p \notin \{p_1, \dots, p_k\} \end{cases}$

und

$$z = \operatorname{sgn}(z) \cdot \prod_{p \in \mathbb{P}} p^{n_p(z)}.$$

Wir nennen diese Darstellung von z ihre **Primfaktorzerlegung**.

Bemerkung: $a, b \in \mathbb{Z} \setminus \{0\}$

$\Rightarrow$ $\operatorname{ggT}(a,b) := \prod_{p \in \mathbb{P}} p^{\min\{n_p(a), n_p(b)\}} \in \operatorname{ggT}(a,b)$

$\operatorname{kgV}(a,b) := \prod_{p \in \mathbb{P}} p^{\max\{n_p(a), n_p(b)\}} \in \operatorname{kgV}(a,b)$

□

Satz 7.38 (Euklid)

Es gibt unendlich viele Primzahlen in $\mathbb{Z}$.

Beweis: Ang.: $\#\mathbb{P} < \infty$

$\Rightarrow \mathbb{P} = \{p_1, \dots, p_k\} \neq \emptyset$ für ein $k \in \mathbb{N}$ (ω_2)

Setze: $z := p_1 \cdots p_k + 1 \in \mathbb{Z}_{>1}$

$\overset{2.37}{\Rightarrow} \exists\, p \in \mathbb{P} : p \mid z$

$\Rightarrow \exists\, i : p = p_i$

$\Rightarrow p_i \mid z - (p_1 \cdots p_k) = 1$ ↯

Also: $\#\mathbb{P} = \infty$ ☐

G) Der Chinesische Restsatz

Motivation 7.39

Gegeben: $n_1 = 2, \; n_2 = 3, \; n_3 = 7$

und $a_1 = 1, \; a_2 = 2, \; a_3 = 3.$

Finde: eine ganze Zahl $x \in \mathbb{Z}$, so daß

$x \equiv a_1 \pmod{n_1} \equiv 1 \pmod 2$

$x \equiv a_2 \pmod{n_2} \equiv 2 \pmod 3$

$x \equiv a_3 \pmod{n_3} \equiv 3 \pmod 7$

Ist $0 \le x < n_1 \cdot n_2 \cdot n_3 = 42$ möglich?

Beachte: n_1, n_2 & n_3 sind p.w. teilerfremd!

STOP

① $x \equiv 1 \pmod 2 \Rightarrow x \in \{1, 3, 5, 7, 11, 13, 15, 17, 19, 21, \dots\}$

② $x \equiv 2 \pmod 3 \Rightarrow x \in \{5, 8, 11, 14, 17, 20, \dots\}$

③ $x \equiv 3 \pmod 7 \Rightarrow x \in \{10, 17, 24, \dots\}$

Also: $x = 17$ tut's!

Lemma 7.40:

Seien $n_1, \dots, n_r \in \mathbb{Z} \setminus \{0\}$ und $N_i := \frac{n_1 \cdots n_r}{n_i}$ für $i = 1, \dots, r$.

und seien $n_1, \dots, n_r$ p.w. teilerfremd,

d.h. $1 \in ggT(n_i, n_j)$ für $i \neq j$

Dann: n_i und N_i sind teilerfremd für $i = 1, \dots, r$.

Beweis: Sei $i \in \{1, \dots, r\}$ fest vorgegeben.

Vor. $\Rightarrow$ $1 \in ggT(n_i, n_j)$ für $j \neq i$

$\overset{\text{Bézout}}{\Rightarrow}$ $\exists\, r_j, s_j \in \mathbb{Z}$: $1 = r_j \cdot n_i + s_j \cdot n_j$

$\Rightarrow$ $1 = \prod_{j \neq i} 1 = \prod_{j \neq i} (r_j \cdot n_i + s_j \cdot n_j)$

Multipliziert man die rechte Seite aus, so gibt es genau 1 Summanden, in dem n_i nicht vorkommt, nämlich $\prod_{j \neq i} s_j \cdot n_j = \prod_{j \neq i} n_j \cdot \prod_{j \neq i} s_j = N_i \cdot \prod_{j \neq i} s_j$

$\Rightarrow \exists\, z \in \mathbb{Z}$: $1 = n_i \cdot z + N_i \cdot \prod_{j \neq i} s_j \in \langle n_i, N_i \rangle_{\mathbb{Z}}$

$\Rightarrow$ $1 \in ggT(n_i, N_i)$, d.h. n_i und N_i sind teilerfremd. ☐

Lemma 7.41:

Seien $n_1, \dots, n_r \in \mathbb{Z} \setminus \{0\}$ paarweise teilerfremd und

sei $a \in \mathbb{Z} \setminus \{0\}$ mit $n_i \mid a$ für alle $i = 1, \dots, r$.

Dann: $n_1 \cdots n_r \mid a$.

Beweis: Induktion nach r: $r=1$: ✓

$r \geq 2$: Ind. $\Rightarrow$ $N_r := n_1 \cdots n_{r-1} \mid a$, $n_r \mid a$

$\Rightarrow$ $\exists\, b, c \in \mathbb{Z}$: $a = b \cdot N_r = c \cdot n_r$ $\circledast$

7.40 $\Rightarrow$ $1 \in ggT(n_r, N_r) \Rightarrow \exists x, y \in \mathbb{Z}: 1 = x \cdot n_r + y \cdot N_r$

$\Rightarrow$ $a = a \cdot 1 = a \cdot x \cdot n_r + a \cdot y \cdot N_r \underset{\circledast}{=} b \cdot N_r \cdot x \cdot n_r + c \cdot n_r \cdot y \cdot N_r$

$= n_r \cdot N_r \cdot (b \cdot x + c \cdot y) = n_1 \cdots n_r \cdot (b \cdot x + c \cdot y)$

$\Rightarrow$ $n_1 \cdots n_r \mid a$. ☐

Chinesischer Restsatz 7.42

Seien $n_1, \ldots, n_r \in \mathbb{Z} \setminus \{0\}$ p.w. teilerfremd, $N := n_1 \cdots n_r$, $N_i = \frac{N}{n_i}$.

ⓐ $\forall\, a_1, \ldots, a_r \in \mathbb{Z}$ $\exists\, x \in \mathbb{Z}$:

$$\left.\begin{aligned} x &\equiv a_1 \pmod{n_1} \\ x &\equiv a_2 \pmod{n_2} \\ &\vdots \\ x &\equiv a_r \pmod{n_r} \end{aligned}\right\} \circledast$$

Kongruenzgleichungssystem

ⓑ Wenn $\overline{x}_i = \overline{N}_i^{-1} \in \mathbb{Z}_{n_i}$ für $i = 1, \ldots, r$, dann ist

$x' := \sum_{i=1}^{r} N_i \cdot x_i \cdot a_i \in \mathbb{Z}$ eine Lösung für $\circledast$.

ⓒ x'' löst $\circledast$ $\Leftrightarrow$ $x'' - x' \in N \cdot \mathbb{Z}$

Insb.: die Lösung von $\circledast$ ist modulo N eindeutig!

ⓓ $\alpha: \mathbb{Z}_{n_1 \cdots n_r} \xrightarrow{\cong} \mathbb{Z}_{n_1} \times \mathbb{Z}_{n_2} \times \cdots \times \mathbb{Z}_{n_r}$

Ψ $\qquad\qquad$ Ψ

$\overline{x}_{n_1 \cdots n_r} \longmapsto (\overline{x}_{n_1}, \overline{x}_{n_2}, \ldots, \overline{x}_{n_r})$

ist ein Isomorphismus von Ringen, und

$\alpha|: \mathbb{Z}^*_{n_1 \cdots n_r} \xrightarrow{\cong} \mathbb{Z}^*_{n_1} \times \cdots \times \mathbb{Z}^*_{n_r}$ ist ein Gruppenisomorphismus.

Beweis: (b) 7.40 $\Rightarrow 1 \in \mathrm{ggT}(n_i, N_i) \Rightarrow \overline{N_i} \in \mathbb{Z}_{n_i}^*$

$\Rightarrow \exists\, x_i \in \mathbb{Z} : \overline{x_i} = \overline{N_i}^{-1}$

Setze: $x' := \sum_{i=1}^{r} N_i \cdot x_i \cdot a_i \in \mathbb{Z}$

$\Rightarrow \overline{x'} = \sum_{j=1}^{r} \overline{N_j} \cdot \overline{x_j} \cdot \overline{a_j} = \overline{N_i} \cdot \overline{x_i} \cdot \overline{a_i} = \overline{a_i} \in \mathbb{Z}_{n_i}$ ($= \overline{1}$)

$\left(\begin{cases} \overline{N_j} = \overline{0} & j \neq i \\ \overline{N_i} & j = i \end{cases} \right.$ weil $n_i \mid N_j$

$\Rightarrow x' \equiv a_i \pmod{n_i}$ für alle $i = 1, \dots, r$

(a) folgt aus (b).

(c) "$\Rightarrow$": Sei $x'' \in \mathbb{Z}$ Lösung von (*) ($\in n_i\mathbb{Z}$)

$\Rightarrow x'' \equiv a_i \pmod{n_i} \Rightarrow x'' - a_i \in n_i \cdot \mathbb{Z}$ und $x' - a_i \in n_i\mathbb{Z}$

$\Rightarrow x'' - x' = (x'' - a_i) - (x' - a_i) \in n_i\mathbb{Z}$

$\Rightarrow n_i \mid x'' - x'$ für $i = 1, \dots, r \overset{7.41}{\Rightarrow} N = n_1 \cdots n_r \mid x'' - x'$

"$\Leftarrow$": $x'' - x' \in N \cdot \mathbb{Z} \Rightarrow \exists\, c : x'' - x' = c \cdot N = n_i \cdot c \cdot N_i$

$\Rightarrow n_i \mid x'' - x' = (x'' - a_i) - (x' - a_i) \Rightarrow n_i \mid x'' - a_i$

$\Rightarrow x'' \equiv a_i \pmod{n_i}$ für $i = 1, \dots, r \Rightarrow x''$ löst (*).

(d) **Behauptung:** $\alpha : \mathbb{Z} \longrightarrow \mathbb{Z}_{n_1} \times \mathbb{Z}_{n_2} \times \cdots \times \mathbb{Z}_{n_r}$ ist offenbar ein Ringhomom.

$x \longmapsto (\overline{x}_{n_1}, \overline{x}_{n_2}, \dots, \overline{x}_{n_r}) = \alpha(x)$

Dabei: $\cdot\ (\overline{a}_1, \dots, \overline{a}_r) \in \mathbb{Z}_{n_1} \times \cdots \times \mathbb{Z}_{n_r} \overset{\text{(c)}}{\Rightarrow} \exists\, x \in \mathbb{Z} : (\overline{x}_1, \dots, \overline{x}) = (\overline{a}_1, \dots, \overline{a}_r)$, d.h. α ist surjektiv!

$\cdot\ x \in \ker(\alpha) \Leftrightarrow x \equiv 0 \pmod{n_1}$, $x \equiv 0 \pmod{n_2}$, $\dots$ $\overset{\text{(c)}}{\Leftrightarrow} x - 0 \in N \cdot \mathbb{Z}$ (0 löst das System)

D.h. $\ker(\alpha) = N\cdot\mathbb{Z}$ $\Rightarrow$ (Hom.satz) $\tilde{\alpha}: \mathbb{Z}/\ker(\alpha) = \mathbb{Z}/N\mathbb{Z} \xrightarrow{\sim} \mathrm{Im}(\alpha) = \mathbb{Z}_{n_1} \times \cdots \times \mathbb{Z}_{n_r}$

ψ: $\bar{x}_N \mapsto (\bar{x}_{n_1}, \ldots, \bar{x}_{n_r})$ $\in$

- Beachte: Ein Ringisomorphismus bildet Einheiten auf Einheiten ab, d.h.

$$\tilde{\alpha}|: \mathbb{Z}_N^* \xrightarrow{\sim} \left(\mathbb{Z}_{n_1} \times \cdots \times \mathbb{Z}_{n_r}\right)^* = \mathbb{Z}_{n_1}^* \times \cdots \times \mathbb{Z}_{n_r}^*$$

(3)

Beispiel 7.43:

$n_1 = 2$, $n_2 = 3$, $n_3 = 7$, $a_1 = 1$, $a_2 = 2$, $a_3 = 3$

$N_1 = n_2 \cdot n_3 = 3\cdot 7 = 21$, $N_2 = n_1 \cdot n_3 = 2\cdot 7 = 14$, $N_3 = n_1 \cdot n_2 = 2\cdot 3 = 6$

$N = n_1 n_2 \cdot n_3 = 42$

(1) Bestimme x_1 s.t. $\bar{x}_1 = \bar{N}_1^{-1} \in \mathbb{Z}_{n_1} = \mathbb{Z}_2$

$\bar{N}_1 = \bar{1} \in \mathbb{Z}_2 \Rightarrow x_1 = 1$

(2) Bestimme x_2 s.t. $\bar{x}_2 = \bar{N}_2^{-1} \in \mathbb{Z}_{n_2} = \mathbb{Z}_3$

$\bar{N}_2 = \bar{2} \in \mathbb{Z}_3 \Rightarrow x_2 = 2$

(3) Bestimme x_3 s.t. $\bar{x}_3 = \bar{N}_3^{-1} \in \mathbb{Z}_{n_3} = \mathbb{Z}_7$

$\bar{N}_3 = \bar{6} \in \mathbb{Z}_7 \Rightarrow x_3 = -1$
$= -\bar{1}$

Also: $x' = N_1 \cdot x_1 \cdot a_1 + N_2 \cdot x_2 \cdot a_2 + N_3 \cdot x_3 \cdot a_3$

$= 21 \cdot 1 \cdot 1 + 14 \cdot 2 \cdot 2 + 6 \cdot (-1) \cdot 3 = 21 + 56 - 18 = 59$

$\equiv 17 \pmod{42}$

$\Rightarrow$ Lös $= \{17 + k\cdot 42 \mid k \in \mathbb{Z}\}$

(3)

§ 8 Das Lemma von Zorn & Maximale Ideale

Def. 8.1 Sei Π eine Menge.

(a) Eine Relation $\leq$ heißt Ordnungsrelation oder eine Teilordnung auf Π, falls:

(1) $\forall x \in \Pi: \quad x \leq x$ (Reflexivität)

(2) $\forall x, y \in \Pi$ mit $x \leq y$ und $y \leq x$: $\quad x = y$ (Anti-symmetrie)

(3) $\forall x, y, z \in \Pi$ mit $x \leq y$ und $y \leq z$: $\quad x \leq z$ (Transitivität)

(b) Eine Teilordnung heißt Totalordnung, falls für alle $x, y \in \Pi$ gilt: $x \leq y$ oder $y \leq x$.

(c) Eine Totalordnung heißt eine Wohlordnung, wenn jede nicht-leere Teilmenge von Π ein minimales Element besitzt.

Definition 8.2: Sei $(\Pi, \leq)$ eine teilgeordnete Menge.

(a) Eine totalgeordnete Teilmenge K von Π heißt eine Kette in Π.

(b) $s \in \Pi$ heißt obere Schranke einer Kette K in Π, falls $\forall x \in K: \quad x \leq s$.

(c) $x \in \Pi$ heißt maximal in Π, falls: $\nexists y \in \Pi: \quad x < y$.

(d) Für eine Kette K in Π und $x \in \Pi$ heißt

$I(K, x) := \{ y \in K \mid y < x \}$ das Initialsegment von K bis einschließlich x.

Bem. 8.3:
- $\emptyset$ ist eine Kette in Π!
- $I(K, x)$ ist wieder eine Kette!
- alle $s \in \Pi$ sind obere Schranken von $\emptyset$.

Satz (Lemma von Zorn) 8.4

Sei $(\Pi, \leq)$ eine teilgeordnete Menge.

Wenn jede Kette in Π eine obere Schranke hat, dann enthält Π ein maximales Element!

Beweis:

Annahme: Π hat kein maximales Element.

1. Schritt: Konstruiere eine Abb. $f : \{k \subseteq \Pi \mid k \text{ Kette}\} \longrightarrow \Pi$ mit der Eigenschaft: $\forall\, x \in k : \; x < f(k)$

Sei k eine Kette in Π

$\Rightarrow$ $S_k := \{s \in \Pi \mid s \text{ ist ob. Schranke von } k\} \neq \emptyset$

$\Rightarrow$ Wähle $s_k \in S_k$ und betrachte: $T_k := \{x \in \Pi \mid s_k < x\} \neq \emptyset$

$\Rightarrow$ Wähle $t_k \in T_k$ und setze: $f(k) := t_k$.

2. Schritt: Eine Kette k in Π heißt konform zu f, wenn

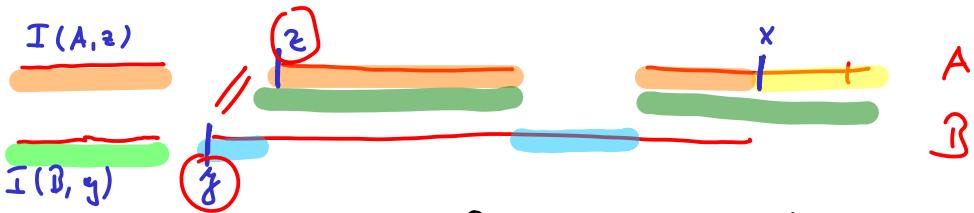
① k ist wohlgeordnet.

② $\forall\, x \in k : \; f(I(k,x)) = x$.

3. Schritt: Zeige: $\forall$ A, B konforme Ketten mit $A \setminus B \neq \emptyset$:

$\exists\, x \in A : \; B = I(A,x)$

Falsches Bild:



Setze: $x := \min(A \setminus B) = \min\{\alpha \in A \mid \alpha \notin B\}$

$\Rightarrow$ $I(A,x) = \{\alpha \in A \mid \alpha < x\} \subseteq B$

Aug: $I(A,x) \overset{\subseteq}{\neq} B$

Setze: $y := \min(B \setminus I(A,x)) = \min\{\beta \in B \mid \beta \notin I(A,x)\}$

$\Rightarrow$ $A \setminus I(B,y) \supseteq A \setminus B \neq \emptyset$

$\Rightarrow$ $z := \min(A \setminus I(B,y)) = \min\{\alpha \in A \mid \alpha \notin I(B,y)\}$ existiert

Zeige: $I(A,z) = I(B,y)$

"$\subseteq$" $\delta \in I(A,z) \Rightarrow \delta \in A$ und $\delta < z$

$\Rightarrow \delta \in I(B,y)$

"$\supseteq$" $\delta \in I(B,y) \Rightarrow \delta \in B$ und $\delta < y$

$\Rightarrow \delta \in I(A,x)$

Ang.: $z \leq \delta < x$

$\Rightarrow z \in B$ (da $x = \min\{\alpha \in A \mid \alpha \notin B\} \wedge z < x$)

$\Rightarrow z \leq \delta < y \Rightarrow z \in I(B,y)$ y ist Def. von z

Also: $\delta < z \Rightarrow \delta \in I(A,z)$

Damit: $x \geq z = f(I(A,z)) = f(I(B,y)) = y$ (*)

f: A konform zu f — f: B konform zu f

1. Fall: $x = z \overset{(*)}{\Rightarrow} x = z = y \in B$ ($y = x = \min(A \setminus B)$)

2. Fall: $x > z \Rightarrow y \overset{(*)}{=} z \in I(A,x)$ ($y = \min(B \setminus I(A,x))$)

Also ist die Annahme $I(A,x) \subsetneq B$ falsch und es folgt: $I(A,x) = B$!

4. Schritt: Satz: $V := \bigcup_{A \subseteq M,\ A \text{ f-konforme Kette}} A$.

Zeige: $\forall$ A f-konforme Kette & $\forall x \in A$: $I(A,x) = I(V,x)$

"$\subseteq$" $A \subseteq V \Rightarrow I(A,x) = \{y \in A \mid y < x\} \subseteq \{y \in V \mid y < x\} = I(V,x)$

"$\supseteq$" $y \in I(V,x) \Rightarrow \exists$ B f-konforme Kette: $y \in B$

1. Fall: $A = B \Rightarrow y \in I(A,x)$

2. Fall: $A \neq B \Rightarrow A \setminus B \neq \emptyset$ oder $B \setminus A \neq \emptyset$

$\overset{\text{3. Schritt}}{\Rightarrow}$ $\exists v \in A : B = I(A,v)$ oder $\exists u \in B : A = I(B,u)$

$\Downarrow$ $\Downarrow$

$y \in I(A,v)$ $y < x < u$

$\Downarrow$ $\Downarrow$

$y \in A$ $y \in I(B,u) = A$

$\Downarrow$ $\Downarrow$

$y \in I(A,x)$ $y \in I(A,x)$

5. Schritt: Zeige: V ist eine zu f konforme Kette.

① z.z.: V totalgeordnet

Sei $x,y \in V \Rightarrow \exists A, B$ konf. Ketten: $x \in A$ und $y \in B$

$\overset{\text{3. Schritt}}{\Rightarrow}$ o.E. $A \subseteq B \Rightarrow x,y \in B \Rightarrow x \leq y$ oder $y \leq x$

(B totalgeord.)

② z.z.: V wohlgeordnet

Sei $\emptyset \neq U \subseteq V$. $\Rightarrow \exists x \in U \Rightarrow \exists A$ konf. Kette: $x \in A$

Sei $y \in U$ mit $y < x$

$\Rightarrow y \in I(V,x) \overset{\text{4. Schr.}}{=} I(A,x) \subseteq A$

$\Rightarrow \min(U) = \min\{y \in U \mid y \leq x\} = \min\{y \in U \cap A \mid y \leq x\} = \min(U \cap A)$

existiert, weil A wohlgeordnet!

Also: V wohlgeordnet!

③ z.z.: $\forall x \in V : f(I(V,x)) = x$.

Sei $x \in V \Rightarrow \exists A$ konf. Kette: $x \in A$

$\overset{\text{4. Schritt}}{\Rightarrow}$ $I(V,x) = I(A,x)$

$\Rightarrow x = f(I(A,x)) = f(I(V,x))$

(A f-konform)

6. Schritt: Setze: $x := f(V) \in \Pi$.

Zeige: $V \cup \{x\}$ ist eine f-konforme Kette

① z.z.: $V \cup \{x\}$ ist total geordnet

klar, da V total geordnet und x echt größer als jedes Element in V!

② z.z.: $V \cup \{x\}$ ist wohlgeordnet

Sei $\emptyset \neq U \subseteq V \cup \{x\}$

1. Fall: $U = \{x\} \Rightarrow \min(U) = x$

2. Fall: $U \neq \{x\} \Rightarrow \exists\, z = \min(U \setminus \{x\})$, da V wohlgeord.

$\Rightarrow z \leq y \quad \forall y \in U$

③ z.z.: $\forall y \in V \cup \{x\} : f(I(V \cup \{x\}, y)) = y$

Sei $y \in V \cup \{x\}$.

1. Fall: $y \neq x \Rightarrow y \in V \Rightarrow I(V \cup \{x\}, y) = I(V, y)$

$\overset{V \text{ konfl.}}{\Rightarrow} y = f(I(V, y)) = f(I(V \cup \{x\}, y))$

2. Fall: $y = x \Rightarrow I(V \cup \{x\}, x) = V$

$\Rightarrow f(I(V \cup \{x\}, y)) = f(V) = x$

7. Schritt: $V \cup \{x\}$ f-konform

$\Rightarrow V \cup \{x\} \subseteq \bigcup_{\substack{A \text{ f-kt.} \\ A \subseteq \Pi}} A = V \Rightarrow x \in V$

$x = f(V)$ ↯ $f(V) > y \ \forall y \in V$

Also: Π besitzt ein maximales Element ⊥

B) Maximale Ideale

Def. 8.6:
Sei R ein kommutativer Ring mit 1. Dann heißt ein Ideal $m \neq R$ maximal, wenn es kein Ideal I in R gibt mit $m \subsetneq I \subsetneq R$. Notation: $m \trianglelefteq_{\max} R$

Bsp. 8.7:

(a) k Körper $\overset{\text{Lem 19}}{\Rightarrow}$ $\{0\}$ ist ein maximales Ideal (weil $\{0\}$ das einzige echte Ideal in k ist).

(b) In $\mathbb{Z}$ ist $\{0\}$ kein maximales Ideal, weil $\{0\} \subsetneq 2\mathbb{Z} \subsetneq \mathbb{Z}$.

Prop. 8.8:
Sei R ein komm. Ring mit 1 und $I \trianglelefteq R$.
Dann: $\exists\, m \trianglelefteq_{\max} R : I \subseteq m$.

Beweis:
Setze: $\Pi := \{ J \trianglelefteq R \mid I \subseteq J \}$
$\Rightarrow \Pi$ ist bezüglich der Inklusion '$\subseteq$' teilgeordnet!
Sei $K \overset{\neq}{\subseteq} \Pi$ eine Kette in Π.
Setze: $S := \bigcup_{J \in K} J$.
Zeige: S ist eine obere Schranke für K in Π!

- z.z.: $I \subseteq S$ und $S \neq \emptyset$
  $K \neq \emptyset \Rightarrow \exists\, J \in K \Rightarrow I \overset{\#}{\neq} \emptyset \subseteq J \subseteq S$
- z.z.: $S \trianglelefteq R$
  Seien $x, x' \in S$ und $r \in R$
  $\Rightarrow \exists\, J, J' \in K : x \in J$ und $x' \in J'$
  K total geordnet $\Rightarrow J \subseteq J'$ oder $J' \subseteq J \Rightarrow$ o.E. $J \subseteq J'$

$\Rightarrow \quad x, x' \in \mathfrak{J}' \quad \Rightarrow \quad x + x' \in \mathfrak{J}' \subseteq S$

Zudem: $r \cdot x \in \mathfrak{J} \subseteq S$

- z.z.: $S \subsetneq R$

  Ang: $S = R \quad \Rightarrow \quad 1 \in R = S \quad \Rightarrow \exists\, \mathfrak{J} \in k : 1 \in \mathfrak{J}$ ↯ $\mathfrak{J} \neq R$

  Also: $S \subsetneq R$.

- Also: $S \in \Pi$ und $\mathfrak{J} \subseteq S \ \forall \mathfrak{J} \in k$, d.h. S ist obere Schranke von k

Damit folgt aus dem Lemma von Zorn:

$\exists\, m \in \Pi$ maximal bez. Inklusion

$\Rightarrow \quad m \subsetneq R$ und $I \subseteq m$ und $\nexists\, \mathfrak{J}^{\neq R}: m \subsetneq \mathfrak{J} \subsetneq R$

$\Rightarrow \quad m$ s. R und $I \subseteq m$ ☐

Kor. 8.9:

Ist $R^{\neq \{0\}}$ ein kommut. Ring mit 1, dann enthält R maximale Ideale.

Beweis:

8.8 mit $I = \{0\}$ ☐

Prop. 8.11:

Ein kommut. Ring mit 1 ist genau dann ein Körper, wenn er nur die Ideale $\{0\}$ und R enthält und diese verschieden sind.

Beweis: üA 19. ☐

Prop. 8.12:

Sei R ein kommut. Ring mit 1 und $m \subsetneq R$.

Dann: m s. $R \quad (\Leftrightarrow \quad R/m$ ist ein Körper.

Beweis:

Beachte: $\{ I \trianglelefteq R \mid \mathfrak{m} \subseteq I \} \xrightarrow{1:1} \{ \overline{I} \trianglelefteq R/\mathfrak{m} \}$

$I \longmapsto I/\mathfrak{m}$

Also: $R/\mathfrak{m}$ hat genau zwei Ideale $R/\mathfrak{m}$ und $\{0\}$

$\overset{8.11}{\Updownarrow}$ $\Leftrightarrow$ $\nexists\, I \trianglelefteq R$ mit $\mathfrak{m} \subsetneq I \subsetneq R$.

$R/\mathfrak{m}$ ist Körper ☺

Bsp. 9.13:

(a) $\mathbb{Z}/2\cdot\mathbb{Z}$ ist ein Körper $\Rightarrow$ $2\mathbb{Z} \trianglelefteq \mathbb{Z}$

(b) $\langle t-a \rangle \trianglelefteq k[t]$ mit $a \in k$ ist ein maximales Ideal

Zeige: $\varphi : k[t] \twoheadrightarrow k$, $f \longmapsto f(a)$ ist ein Ringhom. mit $\ker(\varphi) = \langle t-a \rangle$

Dann: "$\supseteq$" $f = g \cdot (t-a)$ mit $g \in k[t]$

$\Rightarrow \varphi(f) = g(a) \cdot (a-a) = 0$

"$\subseteq$" $f \in \ker(\varphi) \overset{\text{D.u.R.}}{\Rightarrow}$ $f = q \cdot (t-a) + r$ mit $\deg(r) < 1$

$\Rightarrow 0 = f(a) = q(a) \cdot (a-a) + r = r$

$\Rightarrow f = q \cdot (t-a) \in \langle t-a \rangle$.

Damit: Hom.Satz $\Rightarrow$ $k[t]/\langle t-a \rangle = k[t]/\ker\varphi \cong \mathrm{Im}(\varphi) = k$ ist Körper

$\Rightarrow \langle t-a \rangle \trianglelefteq k[t]$.

c) Maximale Ideale und Irreduzibilität in HIR

Korollar 8.14:

Sei R ein HIR und $0 \neq p \in R \setminus R^*$.

Dann sind äquivalent:

(a) p ist irreduzibel.

(b) $\langle p \rangle \trianglelefteq R$ maximales Ideal

(c) $R/\langle p \rangle$ ist ein Körper.

Beweis:

(b) $\Leftrightarrow$ (c): 8.12

(a) $\Rightarrow$ (b): Sei p irreduzibel und $I \trianglelefteq R$ mit $\langle p \rangle \subseteq I \subseteq R$.

R HIR $\Rightarrow \exists\, a \in R : I = \langle a \rangle \Rightarrow p \in \langle a \rangle$ ($I = \langle p \rangle$)

$\Rightarrow \exists\, b \in R : p = a \cdot b \Rightarrow a \in R^*$ oder $b \in R^*$

(p irred.; $I = \langle a \rangle = R$; $\langle a \rangle = \langle p \rangle = I$)

$\Rightarrow I \trianglelefteq R$

(c) $\Rightarrow$ (a): Sei $R/\langle p \rangle$ ein Körper.

Seien $a, b \in R$ mit $p \mid a \cdot b$

$\Rightarrow \overline{a \cdot b} = \overline{0} \in R/\langle p \rangle \Rightarrow \overline{a} = \overline{0}$ oder $\overline{b} = \overline{0}$

($\overline{a} \cdot \overline{b}$; $p \mid a$; $p \mid b$)

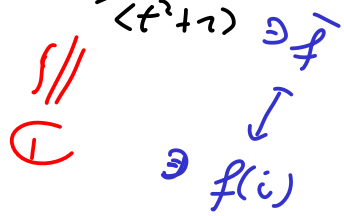
Also: p ist prim $\Rightarrow p$ ist irred. ∎

Bsp. 8.15:

$t^2+1 \in \mathbb{R}[t]$ hat keine Nst. in $\mathbb{R}$

$\Rightarrow$ t^2+1 ist irreduzibel $\Rightarrow$ $\mathbb{R}[t]/\langle t^2+1\rangle$ ist ein Körper

$\uparrow$ Lej $(t^2+1)=2$



□

D) Beweis des Basisergänzungssatzes

Basisergänzungssatz 8.16

Sei V ein k-Vektorraum mit Erzeugendensystem E und sei F eine linear unabhängige Teilfamilie von E.

Dann: $\exists$ Basis B von V s.d. $F \subseteq B \subseteq E$.

Beweis:

Setze: $\Pi := \{ G \mid G$ Teilfamilie von E, $F \subseteq G$, G lin. unabh.$\}$

$\Rightarrow F \in \Pi \Rightarrow \Pi \neq \emptyset$

Beachte: Π ist bzgl. der Inklusion "$\subseteq$" teilgeordnet.

Zeige: Jede Kette in Π hat obere Schranke in Π.

Sei $K \neq \emptyset$ eine Kette in Π.

Setze: $S := \bigcup_{G \in K} G$

z.z.: S ist lin. unabh.

Seien $x_1, \dots, x_n \in S$ und $\lambda_1, \dots, \lambda_n \in k$ s.d. $\sum_{i=1}^{n} \lambda_i x_i = 0$

$\Rightarrow \exists\, G_i \in K : x_i \in G_i$ für $i = 1, \dots, n$

$\Rightarrow \exists\, j : \forall i = 1, \dots, n : G_j \supseteq G_i \ni x_i \Rightarrow x_1, \dots, x_n \in G_j$

$\uparrow$ K total geordnet

$\Rightarrow$ G_j lin. unabh. $\Rightarrow \lambda_1, \dots, \lambda_n = 0 \Rightarrow S$ lin. unabh.

Klar: $F \subseteq G \subseteq S$ $\forall G \in K$ und $G \subseteq E$ $\forall G \in K$ $\Rightarrow S = \bigcup_{G \in K} G \subseteq E$

Also: $S \in M$ und $G \subseteq S$ $\forall G \in K$ $\Rightarrow S$ ist obere Schranke von K

Lemma von Zorn $\Rightarrow \exists B \in \Pi$ maximal bzgl. "$\subseteq$"

Zu zeigen: B ist eine Basis von V (dann fertig, weil $F \subseteq B \subseteq E$)

- $B \in \Pi \Rightarrow B$ ist linear unabhängig
- Ang.: B ist kein ES von V

  $\Rightarrow \exists x \in E : x \notin B$ und $x \notin \mathrm{Lin}(B)$

  $\Rightarrow B \cup \{x\}$ ist linear unabhängig.

  Denn: $\lambda \cdot x + \sum_{i=1}^{n} \lambda_i x_i = 0$ mit $x_i \in B$, $\lambda_1, \dots, \lambda_n, \lambda = 0$

  $\Rightarrow \lambda x = \sum_{i=1}^{n} (-\lambda_i) \cdot x_i \in \mathrm{Lin}(B) \Rightarrow \lambda = 0$ ($x \notin \mathrm{Lin}(B)$)

  $\Rightarrow \lambda_1 x_1 + \dots + \lambda_n x_n = 0 \Rightarrow \lambda_1 = \dots = \lambda_n = 0$ (B linear unabh.)

  Zudem: $F \subseteq B \cup \{x\} \subseteq E$

  $\Rightarrow B \cup \{x\} \in \Pi$ $\lightning$ B maximal in Π

- Also: B ist ein ES von V und damit eine Basis von V

  und $F \subseteq B \subseteq \Pi$ $\square$