Algebra

Leonhard Summerer
LaTeX-Satz: Anton Mosich

Wintersemester 2022

Inhaltsverzeichnis

Kapitel 1

Gruppen

1.1 Grundlagen

$M_1, M_2, M_1 \times M_2, \ldots$ Mengen
Relationen auf M ($a \mathfrak{R} b$ für $a, b \in M$)
$f\colon M_1 \to M_2, a \mapsto b$

Operationen:

- $f\colon M \times \cdots \times M \to M$ innere Operation
- $g\colon \Omega \times M \times \cdots \times M \to M, (\omega_1, a_2, \ldots, a_k) \mapsto g(\omega_1, a_2, \ldots, a_k)$ äußere Operation
- 0-äre Operation: zeichnet ein Element aus M aus
- unäre Operation: $f\colon M \to M$ (Bsp.: $M = \mathbb{Z}\colon x \mapsto -x$)
- binäre Operation: $f\colon M \times M \to M$ (Bsp.: $M = V$, mit V Vektorraum über $\mathbb{K}$: $(v_1, v_2) \mapsto v_1 + v_2$)

Algebra: Untersuchung von Mengen auf denen eine oder mehrere Operationen erklärt sind.

Definition 1.1.1:
Sei $G \neq \emptyset$ zusammen mit einer inneren, binären Operation $\circ$ heißt Gruppe $(G, \circ)$, falls:

G_1: $\forall a, b, c \in G\colon (a \circ b) \circ c = a \circ (b \circ c)$ Assoziativität

G_2: $\exists e \in G\colon \forall a \in G\colon a \circ e = e \circ a = a$ neutrales Element

G_3: $\forall a \in G\colon \exists a^{-1} \in G\colon a \circ a^{-1} = a^{-1} \circ a = e$ inverses Element

Gilt zusätzlich

G_4: $\forall a, b \in G\colon a \circ b = b \circ a$,

so heißt $(G, \circ)$ abelsch oder kommutativ.

Bemerkung 1.1.2:

- In einer Gruppe ist das neutrale Element stets eindeutig bestimmt. Angenommen e, e' seien neutral: $e = e \circ e' = e' \circ e = e'$
- In einer Gruppe ist das inverse Element zu einem Element a stets eindeutig bestimmt. Sei $\begin{cases} a \circ b = b \circ a = e \\ a \circ c = c \circ a = e \end{cases}$ $.c = c \circ e = c \circ (a \circ b) = (c \circ a) \circ b = e \circ b = b$
- In G_2, G_3 könnte man auf $\begin{cases} e \circ a = a \\ b \circ a = e \end{cases}$ reduzieren und $a \circ e = a, a \circ b = e$ folgern $(b = a^{-1})$
  Sei $b \circ a = e, c \circ b = e$

  $a = e \circ a = (c \circ b) \circ a = c \circ (b \circ a) = c \circ e$
  $a \circ e = (c \circ e) \circ e = c \circ e = c \circ (b \circ a) = (c \circ b) \circ a = e \circ a$
  $a \circ b = e \circ a \circ b = (c \circ b) \circ (a \circ b) = c \circ ((b \circ a) \circ b) = c \circ (e \circ b) = c \circ b = e$
- $(G, \circ)$ mit nur G_1 heißt Halbgruppe.
- $(G, \circ)$ mit nur G_1, G_2 heißt Monoid (Bsp.: $(\mathbb{N}, +)$ ist ein kommutativer Monoid).

Rechenregeln

Kürzungsregel:

- $a \circ b = a \circ c \implies b = c, b \circ a = c \circ a \implies b = c$
- $(a^{-1})^{-1} = a$
- $(a \circ b)^{-1} = b^{-1} \circ a^{-1}$

Gruppentafel: alle möglichen Verknüpfungen von je 2 Elementen aus G bestimmt die Gruppe eindeutig
Für $g \in G$ schreiben wir $g^2 \coloneqq g \circ g, g^n \coloneqq \underbrace{g \circ \cdots \circ g}_{n \text{ mal}}$ und es gilt $g^m \circ g^n = g^{m+n}$ für $m, n \in \mathbb{Z}$
Falls die Verknüpfung in einer abelschen Gruppe als $+$ geschrieben wird, so schreibt man $e = 0, g^n = n \cdot g, g^{-1} = -g$

Definition 1.1.3:
Sei $(G, \circ)$ eine Gruppe, $g \in G$.

- $|G| =: \operatorname{ord}(G), \operatorname{ord}_G(g) := \min\{n > 0 \colon g^n = e\}$ (kann auch ∞ sein)
- $\exp(G) := \min\{n > 0 \colon \forall g \in G \colon g^n = e\}$
- $Z(G) := \{h \in G \colon g \circ h = h \circ g \forall g \in G\}$ Zentrum von G
- $Z_G(g) := \{h \in G \colon g \circ h = h \circ g\}$ Zentralisator von g in G

Beispiel 1.1.4:

- $(\mathbb{Z}, +), (\mathbb{Q}, +), (\mathbb{R}, +), (\mathbb{C}, +)$
- $(\mathbb{Q} \setminus \{0\}, \cdot), (\mathbb{R} \setminus \{0\}, \cdot), (\mathbb{C} \setminus \{0\}, \cdot)$
- $(\mathbb{Z}_n, +)$
- Sei $\mathcal{S}_M := \{f \colon M \to M \colon f \text{ bijektiv}\}$ (Symmetrische Gruppe der Menge M) bildet eine Gruppe bezüglich der Verknüpfung von Abbildungen $\circ$. Ist $M = \{1, \ldots, n\}$ so schreiben wir $\mathcal{S}_n$. Es gilt $|\mathcal{S}_n| = n!$
- Sei M eine Menge, G eine Gruppe. $\mathrm{Abb(M, G)} := \{\mathrm{f} \colon \mathrm{M} \to \mathrm{G}\}$
  $(f_1 \cdot f_2)(m) := f_1(m) \cdot f_2(m)$
- Sei $\mathbb{K}$ Körper, $M_n(\mathbb{K})$: $n \times n$ Matrizen über $\mathbb{K}$.
  $\mathrm{GL}_n(\mathbb{K}) := \{A \in M_n(\mathbb{K}) \colon \det(A) \neq 0\}$ allgemeine lineare Gruppe.

1.2 Untergruppen, Erzeuger und zyklische Gruppen

Definition 1.2.1:

$\emptyset \neq H \subseteq G$ heißt Untergruppe $(H, \circ)$ von $(G, \circ)$ falls $(H, \circ)$ selbst die Eigenschaften $G_1 - G_3$ erfüllt. Wir schreiben dann $(H, \circ) \leq (G, \circ)$ beziehungsweise $H \leq G$. Insbesondere muss $\circ$ eine innere Operation auf H definieren, $e \in H$ und mit $a \in H$ auch $a^{-1} \in H$

Lemma 1.2.2:

$H \leq G \iff H \neq \emptyset \wedge \forall a, b \in H \colon ab^{-1} \in H$

Beweis. $H \neq \emptyset \implies \exists h \in H \implies hh^{-1} = e \in H$
Seien $\underbrace{a}_{=e}, b \in H$. Dann gilt: $eb^{-1} \in H$, das heißt $b^{-1} \in H$. Wegen $b^{-1} \in H$ folgt $a(b^{-1})^{-1} = ab \in H \implies ab \in H$. Die Umkehrung ist klar. □

Bemerkung 1.2.3:

- Für jede Gruppe G gilt: $\{e\}, G$ sind stets Untergruppen von G. Alle anderen Untergruppen von G heißen echte Untergruppen.
- Für zwei Untergruppen H_1, H_2 von G ist auch $H_1 \cap H_2$ eine Untergruppe. Allgemeiner: sind $(H_i)_{i \in I}$ Untergruppen von G, so ist $\bigcap_{i \in I} H_i$ eine Untergruppe von G.
- Für $g \in G$ ist $\langle g \rangle := \{g^n : n \in \mathbb{Z}\}$ die von g erzeugte Untergruppe von G. $\operatorname{ord}_G(g) = |\langle g \rangle|$

Definition 1.2.4:

Sei $\emptyset \neq S \subseteq G$. Dann heißt $\bigcap\limits_{\substack{H \leq G \\ S \subseteq H}} H$ die von S erzeugte Untergruppe in G: $\langle S \rangle$. $\langle S \rangle$ ist die kleinste Untergruppe, die S enthält.

Proposition 1.2.5:

$$\langle S \rangle = \{s_1 \circ \cdots \circ s_n : s_i \in S \cup S^{-1}, n \in \mathbb{N}\} (=: \bar{S})$$

Beweis.

- $S \subseteq \bar{S}$ ✓
- $\bar{S} \subseteq \langle S \rangle$ (da $\langle S \rangle$ eine Untergruppe von G ist, die S enthält)
- Behauptung: $\bar{S} \leq G$: Seien $a, b \in \bar{S}$. OBdA $a = s_1 \circ \cdots \circ s_n, t_1 \circ \cdots \circ t_m$ (mit $s_i, t_j \in S \cup S^{-1}$)
  $a \circ b^{-1} = s_1 \circ \cdots \circ s_n \circ t_m^{-1} \circ \cdots \circ t_1^{-1} \in \bar{S}$
  $\bar{S} \subseteq \langle S \rangle \implies \langle S \rangle \subseteq \bar{S}$

Alles in Allem: $\langle S \rangle = \bar{S}$ □

Definition 1.2.6:

- G heißt endlich erzeugt, falls $\exists S \subseteq G$ mit $|S| < \infty$ und $\langle S \rangle = G$.
- G heißt zyklisch, falls $\exists g \in G\colon \langle g \rangle = G$
- Jede endliche Gruppe ist endlich erzeugt.
  - $(\mathbb{Z}, +)$ ist von 1 erzeugt, also zyklisch.
  - $(\mathbb{R}, +)$ ist nicht endlich erzeugt, da überabzählbar

Satz 1.2.7:

Sei G eine zyklische Gruppe, $H \leq G$. Dann ist H zyklisch.

Beweis. Sei $G = \langle g \rangle$. $H \leq G \implies H \neq \emptyset$. Falls $H = \{e\}$, so ist H zyklisch. ✓
Falls $H \neq \{e\}$, so enthält H mindestens ein weiteres Element u.
$u = g^s$ mit $s \in \mathbb{Z}$ (oBdA sogar $s \in \mathbb{N}$, sonst $u \to u^{-1}$). Wir wählen nun unter allen $u = g^s$ mit $s \in \mathbb{N} \setminus \{0\}$ eines mit s minimal.
Behauptung: $H = \langle u \rangle = \langle g^s \rangle$
$\langle g^s \rangle \subseteq H$, weil $H \leq G$ die g^s enthält. Sei $h \in H$ beliebig. $h \in G \implies \exists m \in \mathbb{Z}\colon h = g^m$.
Es ist $m = l \cdot s + r$ mit $0 \leq r < s$. $h = g^m = g^{ls+r} \in H \implies \underbrace{g^{-ls}}_{\in H} \cdot g^{ls+r} = g^r \in H$. Weil s minimal gewählt wurde gilt $r = 0$, das heißt $h = g^{ls} \in \langle g^s \rangle$ □

Proposition 1.2.8:

Sei G eine endliche Gruppe, $g \in G$ mit $\mathrm{ord}_G(g) = k$. Dann gilt:

1. $g^n = e \iff k \mid n$
2. $\mathrm{ord}_G(g^t) = \frac{k}{\mathrm{ggT}(k,t)}$

Beweis. In der Übung □

Korollar 1.2.9:

Ist $\langle g \rangle = G$ eine endliche, zyklische Gruppe, so gibt es zu jeden Teiler d von $n := \mathrm{ord}(G)$ genau eine Untergruppe der Ordnung d: $H = \left\langle g^{\frac{n}{d}} \right\rangle$

Beweis. $G = \langle g \rangle \implies \operatorname{ord}_G(g) = n \overset{2.}{\implies} \operatorname{ord}_G(g^{\frac{n}{d}}) = \frac{n}{\operatorname{ggT}(n, \frac{n}{d})} = d$
Umgekehrt, sei $H' \leq G$ mit $|H'| = d$. Nach Theorem 1.2.7: H' ist zyklisch, $H' = \langle g^s \rangle$ mit s minimal, sodass $g^s \in H'$. Es ist $e = g^n \in H' \overset{1.}{\implies} s \mid n$
$|H'| = \operatorname{ord}(g^s) = \frac{n}{\operatorname{ggT}(n,s)} = \frac{n}{s} \implies d = \frac{n}{s} \implies s = \frac{n}{d}$ □

Proposition 1.2.10:

Sei G eine endliche, abelsche Gruppe, $a, b \in G$ mit $\operatorname{ord}_G(a) = r, \operatorname{ord}_G(b) = s$ mit $\underbrace{(r,s)}_{\text{Notation für } \operatorname{ggT}(r,s)} = 1$. Dann gilt $\operatorname{ord}_G(ab) = rs$.

Beweis. $a^r = e, b^s = e \implies a^{rs} = e, b^{rs} = e \overset{\text{abelsch}}{\implies} (ab)^{rs} = e \implies \operatorname{ord}_G(ab) \mid rs$
Angenommen: $\operatorname{ord}_G(ab) < rs$. Dann $\exists p \in \mathbb{P}$: $(ab)^{\frac{rs}{p}} = e$.
Sei oBdA $p \mid r$ ($\implies p \nmid s$, weil $(r,s) = 1$)

$$(ab)^{\frac{rs}{p}} = a^{\frac{rs}{p}} \cdot b^{\frac{rs}{p}} = (a^s)^{\frac{r}{p}} \cdot \underbrace{(b^s)^{\frac{r}{p}}}_{=e} = (a^s)^{\frac{r}{p}} = e$$

Die Ordnung von a und daher von a^s ist aber r und daher sicher $> \frac{r}{p}$. ↯

Für $p \in \mathbb{P}$ bezeichnet $\nu_p(n)$ die Vielfachheit von p in n.

Lemma 1.2.11:

Sei G endliche abelsche Gruppe. Dann gilt:

$$\forall g \in G\colon \operatorname{ord}_G(g) \mid \max_{h \in G}\{\operatorname{ord}_G(h)\}$$

Beweis. Sei $a \in G$ mit $\max_{h \in G}\{\operatorname{ord}_G(h)\} =: m$.
Angenommen: $\exists b \in G$ mit $=: \operatorname{ord}_G(b) \nmid m \implies \exists p \in \mathbb{P}$ mit $\underbrace{\nu_p(n)}_{=:e'} > \underbrace{\nu_p(m)}_{=:e}$

Betrachte die Elemente a^{p^e} und $b^{\frac{n}{p^{e'}}}$.

$$\operatorname{ord}_G\left(a^{p^e}\right) = \frac{m}{p^e}, \operatorname{ord}_G\left(b^{\frac{n}{p^{e'}}}\right) = p^{e'}$$

Dann ist $\operatorname{ggT}\left(a^{p^e}, b^{\frac{n}{p^{e'}}}\right) = 1 \implies \operatorname{ord}_g\left(a^{p^e} \cdot b^{\frac{n}{p^{e'}}}\right) = \frac{m}{p^e} \cdot p^{e'} = m \cdot p^{\overbrace{(e'-e)}^{\geq 1}} > m$ ↯

Satz 1.2.12:

Sei $\mathbb{K}$ ein Körper. Jede endliche Untergruppe G von $(\mathbb{K} \setminus \{0\}, \cdot)$ ist zyklisch.

Beweis. $m \coloneqq \max_{g\in G}\{\mathrm{ord}_G(g)\} = \mathrm{kgV}\{\mathrm{ord}_G(g)\colon g \in G\}$
$\Longrightarrow$ alle $g \in G$ sind Nullstellen des Polynoms $x^m - 1 \in \mathbb{K}[x]$. Ist $a \in G$ mit $\mathrm{ord}_G(a) = m$, so sind $a^0, a^1, \ldots, a^{m-1}$ paarweise verschiedene Nullstellen dieses Polynoms.
$\Longrightarrow$ $a^0, \ldots a^{m-1}$ sind alle Nullstellen von $x^m - 1$ (weil Polynom vom Grad m nur m Nullstellen haben kann) und es gilt $G = \langle a\rangle$ $\square$

Beispiel 1.2.13:

1. $\mathbb{K} = \mathbb{C}, \mathbb{E}_n \coloneqq \{x \in \mathbb{C}\colon x^n = 1\}$
2. $\mathbb{K} = \mathbb{Z}_p, p \in \mathbb{P}, \mathbb{Z}_p^* \coloneqq \{\bar{a} \in \mathbb{Z}_p\colon \bar{a} \neq \bar{0}\}$

1.3 Gruppenhomomorphismen

Definition 1.3.1:

Seien $(G, \circ)$ und $(H, \square)$ Gruppen. $\phi\colon G \to H$ heißt Gruppenhomomorphismus falls:

$$\forall a, b \in G\colon \phi(a \circ b) = \phi(a)\square\phi(b)$$

$\ker(\phi) \coloneqq \{g \in G\colon \phi(g) = e_H\}$
$\mathrm{im}(\phi) \coloneqq \{h \in H\colon \exists g \in G\colon \phi(g) = h\}$

Lemma 1.3.2:

$\phi\colon G \to H$ sei Gruppenhomomorphismus. Dann gilt:

1. $\phi(e_G) = e_H$
2. $\phi(a^{-1}) = \phi(a)^{-1}$
3. $\ker(\phi) \leq G, \mathrm{im}(\phi) \leq H$

Beweis.

1.
$$\begin{cases}\phi(e_G) = \phi(e_G \cdot e_G) = \phi(e_G) \cdot \phi(e_G)\\ \phi(e_G) = \phi(e_G) \cdot e_H\end{cases} \Longrightarrow e_H = \phi(e_G)$$

2.
$$\begin{cases}e_H = \phi(e_G) = \phi(aa^{-1}) = \phi(a) \cdot \phi(a^{-1})\\ e_H = \phi(a) \cdot \phi(a)^{-1}\end{cases} \Longrightarrow \phi(a^{-1}) = \phi(a)^{-1}$$

3. (a) $\phi(g) = \phi(g') = e_H \implies \phi(gg') = \phi(g) \cdot \phi(g') = e_H$
$\phi(g^{-1}) = \phi(g)^{-1} = e_H$

   (b) $h_1, h_2 \in \mathrm{im}(\phi)$. Seien $g_1, g_2 \in G$ mit $\phi(g_1) = h_1, \phi(g_2) = h_2$.
$\phi(g_1 g_2) = \phi(g_1) \cdot \phi(g_2) = h_1 h_2 \in \mathrm{im}(\phi)$
$\phi(g_1^{-1}) = \phi(g_1)^{-1} = h_1^{-1} \in \mathrm{im}(\phi)$ □

Bemerkung 1.3.3:

- Sei $\phi\colon G \to H$ Gruppenhomomorphismus. Falls
  - $G = H$: Endomorphismus
  - ϕ injektiv: Monomorphismus.
  - ϕ surjektiv: Epimorphismus.
  - ϕ bijektiv: Isomorphismus (falls $G = H$: Automorphismus)
- G, H, K seien Gruppen, $\phi\colon G \to H, \psi\colon H \to K$ Gruppenhomomorphismen. $\psi \circ \phi\colon G \to K$ ist Gruppenhomomorphismus.
- $\phi\colon G \to H$ Isomorphismus $\implies \phi^{-1}\colon H \to G$ auch Isomorphismus.
Seien $a, b \in H$. z.Z.: $\phi^{-1}(ab) = \phi^{-1}(a)\phi^{-1}(b)$. Seien $g, h \in G$ mit $\phi(g) = a, \phi(h) = b$. $\phi^{-1}(ab) = \phi^{-1}(\phi(g)\phi(h)) = \phi^{-1}(\phi(gh)) = gh = \phi^{-1}(a)\phi^{-1}(b)$ $^{-1}$ analog.

Beispiel 1.3.4:

- $G = (\mathbb{R}, +), H = (\mathbb{R}^*, \cdot), \phi\colon G \to H, x \mapsto e^x$ ist ein Monomorphismus. Wählt man $H = (\mathbb{R}^{+*}, \cdot)$ so erhält man einen Isomorphismus. log ist die zugehörige Umkehrabbildung.
- G, H Gruppen. $\phi\colon G \to H, g \mapsto e_H$ ist stets ein Gruppenhomomorphismus.
- $G = \mathbb{Z}, H = \mathbb{Z}_n, \phi\colon \mathbb{Z} \to \mathbb{Z}_n$,
$a \mapsto a + n\mathbb{Z}$ heißt der kanonische Epimorphismus.
- $G = \mathrm{GL}_n(\mathbb{K}), H = \mathbb{K}^*, \det\colon G \to H, A \mapsto \det A$ ist Epimorphismus.

$$\mathrm{SL}_n(\mathbb{Z}_p) \coloneqq \{A \in \mathrm{GL}_n(\mathbb{Z}_p)\colon \det A = 1\}$$

G, H Gruppen. $\mathrm{Hom}(G, H) \coloneqq \{\phi\colon G \to H, \phi \text{ Gruppenhomomorphismus}\}$
$\mathrm{Aut}(G) \coloneqq \{\phi\colon G \to G, \phi \text{ Isomorphismus}\}$ ist Gruppe bezüglich der Komposition von

Abbildungen $\circ$.
$\mathrm{Hom}(G,H) \neq \emptyset$

Sei $G = \langle g \rangle$ eine zyklische Gruppe. Bestimme $\mathrm{Aut}(G)$. Für jedes $a \in G$ gilt: $\exists s \in \mathbb{Z}$ mit $a = g^s \implies \phi(a) = \phi(g^s) = \phi(g)^s$
2 Fälle:

1. $|G| = \infty$ ($\implies$ G isomorph zu $(\mathbb{Z}, +)$)
   $\mathbb{Z} = \langle 1 \rangle \implies \langle \phi(1) \rangle = \mathbb{Z} \implies \phi(1) \in \{1, -1\}$
   $$\mathrm{Aut}(G) = \{\mathrm{id}, ()^{-1}\}$$
2. $|G| = n$. $G \underset{\mathrm{ord}_G(g)=|G|}{=} \langle g \rangle \implies \langle \phi(g) \rangle = G$
   $\mathrm{ord}_G(g^s) = \frac{|G|}{\mathrm{ggT}(|G|),s)} = |G| \implies \phi(g) = g^s$ mit $(\mathrm{ggT}(\underbrace{|G|}_{n}, s) = 1)$
   $$\mathrm{Aut}(G) = \{f_s \colon g \mapsto g^s \text{ mit } \mathrm{ggT}(s, |G|) = 1\}$$

Sei nun G eine beliebige Gruppe, $a \in G$. Dann definiert

$$\phi_a \colon G \to G, g \mapsto aga^{-1}$$

einen Automorphismus von G.

- injektiv: $aga^{-1} = h \iff g = a^{-1}ha$
- surjektiv: ✓

Solche Automorphismen heißen innere Automorphismen.

Bemerkung 1.3.5:
ϕ innerer Automorphismus $\implies \phi|_{Z(G)} = \mathrm{id}$

Beispiel 1.3.6:
$G = \mathrm{GL}_n(\mathbb{R})$
$\phi \colon G \to G, A \mapsto (A^t)^{-1}$ ist Automorphismus von G.

$$((AB)^t)^{-1} = (B^t A^t)^{-1} = (A^t)^{-1}(B^t)^{-1}$$

ϕ ist nicht innerer Automorphismus, denn $\begin{pmatrix} d & & \\ & \ddots & \\ & & d \end{pmatrix} \in Z(G)$.

$$\phi\left(\begin{pmatrix} d & & \\ & \ddots & \\ & & d \end{pmatrix}\right) = \begin{pmatrix} d^{-1} & & \\ & \ddots & \\ & & d^{-1} \end{pmatrix}$$

Proposition 1.3.7:
$\phi\colon G \to H$ Gruppenhomomorphismus. Dann gilt:

1. $U \leq G \implies \phi(U) \leq H$
2. $U' \leq H \implies \phi^{-1}(U') \leq G$
3. ϕ ist injektiv $\iff \ker(\phi) = \{e_G\}$

Beweis.

1. Seien $u_1, u_2 \in U, \phi(u_1)\phi(u_2) = \phi(u_1u_2) \in \phi(U), \phi(u_1^{-1}) = \phi(u_1)^{-1} \in \phi(U)$
2. $u_1, u_2 \in \phi^{-1}(U') \implies \phi(u_1), \phi(u_2) \in U' \implies \phi(u_1)\phi(u_2) = \phi(u_1u_2) \in U'$
   $\implies u_1u_2 \in \phi^{-1}(U')$
   Analog mit $\phi(u_1)^{-1}$.
3. $$\begin{aligned}\phi \text{ injektiv} &\iff (\phi(g) = \phi(h) \implies g = h)\\ &\iff (\phi(g)\phi(h)^{-1} = e_H \implies g = h)\\ &\iff (\phi(gh^{-1}) = e_H \implies g = h)\\ &\iff \ker(\phi) = e_G\end{aligned}$$

□

1.4 Nebenklassen, Normalteiler & Faktorgruppen

Definition 1.4.1:
Sei G eine Gruppe, $H \leq G, a \in G$.

$$Ha \coloneqq \{ha | h \in H\}$$

heißt Rechtsnebenklasse von G nach H.

$$aH \coloneqq \{ah | h \in H\}$$

heißt Linksnebenklasse von G nach H.
Achtung: im Allgemeinen sind aH, Ha keine Untergruppen von G.

$$Ha = Hb \iff \begin{cases} Ha \subseteq Hb \\ Hb \subseteq Ha \end{cases} \iff \begin{cases} a \in Hb \\ b \in Ha \end{cases} \iff \begin{cases} a = hb \\ b = h'a \end{cases}$$

für passende $h, h' \in H$

$$\iff a = hb \iff ab^{-1} \in H$$

Lemma 1.4.2:

Es gilt: $G = \bigcup_{a \in G} Ha, Ha \cap Hb = \emptyset$ oder $Ha = Hb$.

Beweis.

$$G = \bigcup_{a \in G} a \subseteq \bigcup_{a \in G} Ha$$

Falls $Ha \cap Hb \neq \emptyset$, dann gilt $ab^{-1} \in H$ und somit $Ha = Hb$.

Achtung: $Ha = aH$ ist im Allgemeinen nicht erfüllt, aber $|Ha| = |aH|$ gilt immer. □

Definition 1.4.3:

G/H bezeichnet die Menge aller Linksnebenklassen von G nach H.

$H\backslash G$ bezeichnet die Menge aller Rechtsnebenklassen von G nach H.

$\left|G/H\right| = |HG|$, denn $Ha = Hb \iff ab^{-1} \in H, aH = bH \iff ba^{-1} \in H$

$\left|G/H\right|$ heißt der Index von H in G und wird bezeichnet mit $[G : H]$

$G = \bigcup_{n=1}^{[G:H]} Ha_n$, wobei $Ha_i \neq Ha_j$ für $i \neq j$ falls $[G : H] < \infty$

Satz 1.4.4 (Satz von Lagrange):

Sei G eine Gruppe, $H \leq G$. Sind zwei der Größen $|G|, [G : H], |H|$ endlich, so ist es auch die Dritte. Es gilt:

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

Beweis. $|G| < \infty \implies |H|, [G : H] < \infty$. Seien also $|H|, [G : H] < \infty$. Sei $f : Ha \to Hb$, $ha \mapsto hb$. Dann ist f bijektiv. $h_1 b = h_2 b \implies h_1 = h_2 \implies h_1 a = h_2 a$. Es folgt $|Ha| = |Hb| \, \forall a, b \in G$ und somit $|Ha| = |H| \, \forall a \in G$. Dann gilt: $|G| = [G : H] \cdot |H|$ (da $[G : H] < \infty$ vorausgesetzt, daher $G = \bigcup_{n=1}^{[G:H]} Ha_n$). Insbesondere ist $|G| < \infty$. □

Korollar 1.4.5:

1. $H \leq G \implies |H| \mid |G|$
2. $g \in G \implies \mathrm{ord}_G(g) \mid |G|$
3. $g^{|G|} = e \forall g \in G$

Beweis.

1. ist klar
2. $\text{ord}_G(g) = |\langle g \rangle|$ und teilt daher $|G|$.
3. Weil $|G|$ ein Vielfaches von $\text{ord}_G(g)$ ist. □

Beispiel 1.4.6:

$G = \mathcal{S}_4$. Behauptung: $\mathcal{S}_4$ hat Untergruppen der Ordnung $1, 2, 3, 4, 6, 8, 12, 24$

1: $\{e\}$

2: $\langle (12) \rangle$ hat Ordnung 2

3: $\langle (123) \rangle$ hat Ordnung 3

4: $V_4 = \{\text{id}, (12)(34), (13)(24), (14)(23)\}$ (heißt Klein'sche Vierergruppe)

6: $\iota(\mathcal{S}_3) \hookrightarrow \mathcal{S}_4$ hat Ordnung 6

8: $D_4 = \langle (13), (1234) \rangle$ hat Ordnung 8

12: $\mathcal{A}_4 \coloneqq \{\sigma \in \mathcal{S}_4 \text{ mit } \text{sgn}(\sigma) = +1\}$

24: G

Nicht immer gibt es zu jedem Teiler der Gruppenordnung eine Untergruppe dieser Ordnung. Beispiel: $\mathcal{A}_4$ hat keine Untergruppe der Ordnung 6 (Übung)

Korollar 1.4.7:

$|G| = p \in \mathbb{P} \implies G$ ist zyklisch.

Beweis. Sei $g \in G, g \neq e$. $|\langle g \rangle|$ teilt $|G| = p \implies |\langle g \rangle| = p \implies \langle g \rangle = G$ □

Definition 1.4.8:

$N \leq G$ heißt Normalteiler, falls

$$\forall g \in G \colon gN = Ng$$

das heißt die Rechtsnebenklassen stimmen mit den Linksnebenklassen überein.

Achtung: $gN = Ng$ bedeutet nicht, dass $gn = ng \forall n \in N$!

Beispiel 1.4.9:

- $V_4, \mathcal{A}_4$ sind Normalteiler von $\mathcal{S}_4$.
- $\{e\}, G$ sind Normalteiler von G.
- In abelschen Gruppen sind alle Untergruppen normal.
- $\mathrm{SL}_n(\mathbb{K})$ ist Normalteiler von $\mathrm{GL}_n(\mathbb{K})$.
  Wir schreiben $U \leq G$ für Untergruppen, $N \trianglelefteq G$ für Normalteiler.

Lemma 1.4.10:

Die folgenden Aussagen sind äquivalent:

1. $N \trianglelefteq G$,
2. $\forall g \in G\colon gN \subseteq Ng$,
3. $\forall g \in G\colon gNg^{-1} \subseteq N$,
4. $\forall g \in G\colon gNg^{-1} = N$.

Beweis. (1) $\implies$ (2) : ✓
(2) $\implies$ (3) : ✓
(3) $\implies$ (4) : Es gilt $gNg^{-1} \subseteq N$ und $g^{-1}Ng \subseteq N \forall g \in G$. $N = (gg^{-1})N(gg^{-1}) = g(g^{-1}Ng)g^{-1} \subseteq gNg^{-1}$ Insgesamt: $N = gNg^{-1}$
(4) $\implies$ (1)✓ □

Proposition 1.4.11:

Sei $\phi \in \mathrm{Hom}(G, H)$. Dann ist $\ker(\phi) \trianglelefteq G$.

Beweis. Sei $N := \ker(\phi)$. Zu Zeigen: $gNg^{-1} \subseteq N \forall g \in G$. Sei $n \in N\colon \phi(gng^{-1}) = \phi(g)\overbrace{\phi(n)}^{e_H}\phi(g)^{-1} = \phi(g)\phi(g)^{-1} = e_H$, das heißt $gng^{-1} \in N$. □

Beispiel 1.4.12 (Anwendung):

- $\det\colon \mathrm{GL}_n(\mathbb{K}) \to \mathbb{K}^*$,
  $A \mapsto \det A$. Dann ist $\ker(\det) = \mathrm{SL}_n(\mathbb{K})$. Es folgt: $\mathrm{SL}_n(\mathbb{K}) \trianglelefteq \mathrm{GL}_n(\mathbb{K})$

- $\operatorname{sgn}\colon \mathcal{S}_4 \to \{\pm 1\}, \sigma \mapsto \operatorname{sgn}\sigma$. $\ker(\sigma) = \mathcal{A}_4$. Daher gilt $\mathcal{A}_4 \trianglelefteq \mathcal{S}_4$.

Existiert zu jedem Normalteiler $N \trianglelefteq G$ eine Gruppe H, und ein Homomorphismus $\phi\colon G \to H$ mit $N = \ker(\phi)$?

Satz 1.4.13:
Sei $N \trianglelefteq G$. Dann bilden die Linksnebenklassen $\{gN : g \in G\}$ eine Gruppe bezüglich der Verknüpfung $gN \cdot hN := (g \cdot h)N$. Diese Gruppe wird mit G/N bezeichnet und heißt Faktorgruppe oder Quotientengruppe von G nach N. Es gilt $\left|G/N\right| = \frac{|G|}{|N|}$.

Beweis. Die Verknüpfung $(gN)(hN) = (gh)N$ ist wohldefiniert. Sei $gN = g'N, hN = h'N$, das heißt $g' = \underbrace{gn_1}_{\in N, \text{ passend weil } N \trianglelefteq G}$ und $h' = hn_2$ für passende $n_1, n_2 \in N$. $(g'h')N = (gn_1hn_2)N = g(n_1h)n_2N = g(h\overbrace{n_3})n_2N = (gh)N$. Das Assoziativgesetz gilt, da es in G gilt. Das neutrale Element von G/N ist $eN = N$. Das inverse Element von $aN = a^{-1}N$.

Lagrange(Theorem 1.4.4) impliziert $[G : N] = \left|G/N\right| = \frac{|G|}{|N|}$. □

$\phi\colon G \to H$ Homomorphismus $\implies \ker(\phi) \trianglelefteq G$
$N \trianglelefteq G \implies G/N$ ist selbst eine Gruppe.

Beispiel 1.4.14:
$G = \mathbb{Z}, N = n\mathbb{Z}$.
$\underbrace{\mathbb{Z}/n\mathbb{Z}}_{\text{Faktorgruppe}} = \underbrace{\mathbb{Z}_n}_{\text{Gruppe der Restklassen}}$

G abelsch $\implies$ Jeder Quotient ist abelsch.

Beispiel 1.4.15:
$\mathcal{S}_n$ ist nicht ablesch für $n \geq 3$. $\mathcal{A}_n \trianglelefteq \mathcal{S}_n$. $\mathcal{S}_n/\mathcal{A}_n$ ist abelsch.

Proposition 1.4.16:
Sei $N \trianglelefteq G$. Dann existieren H und $\phi \in \operatorname{Hom}(G, H)$ mit $\ker(\phi) = N$.

Beweis. Wähle $H \coloneqq {}^{G}\!/_{N}$ und $\phi\colon G \to {}^{G}\!/_{N}, g \mapsto gN$ ist surjektiver Homomorphismus.

$$(gN)(hN) = g(Nh)N = g(hN)N = (gh)N$$

$g \in \ker(\phi) \iff gN = N \iff g \in N$, das heißt $N = \ker(\phi)$ □

Korollar 1.4.17:
$\phi \in \mathrm{Hom}(G, H)$ impliziert ${}^{G}\!/_{\ker(\phi)} \cong \phi(G)$

Beweis. $N \coloneqq \ker(\phi)$. Es ist ${}^{G}\!/_{N}$ Gruppe. Setze $f\colon {}^{G}\!/_{N} \to \phi(G)$, $gN \mapsto \phi(g)$. f ist wohldefiniert und injektiv, denn $gN = hN \iff gh^{-1} \in N = \ker(\phi) \iff \phi(g) = \phi(h)$. Surjektivität ist klar. f ist Homomorphismus:

$$f((gN)(hN)) = f(ghN) = \phi(gh) = \underbrace{\phi(g)}_{f(gN)}\underbrace{\phi(h)}_{f(hN)}$$

□

Der Homomorphiesatz besteht aus 3 Teilen:

- Theorem 1.4.11: $\ker\phi \trianglelefteq G$
- Theorem 1.4.16: $N \trianglelefteq G \implies \exists H, \phi \in \mathrm{Hom}(G, H)\colon N = \ker(\phi)$
- Theorem 1.4.17: $\phi \in \mathrm{Hom}(G, H) \implies {}^{G}\!/_{\ker(\phi)} \cong \phi(G)$

Beispiel 1.4.18 (Anwendung auf zyklische Gruppen):
Zu jedem $n \in \mathbb{N}$ existiert eine bis auf Isomorphie eindeutige zyklische Gruppe dieser Ordnung n, nämlich ${}^{\mathbb{Z}}\!/_{n\mathbb{Z}}$. Alle unendlichen zyklischen Gruppen sind isomorph zu $\mathbb{Z}$.

Beweis. Sei $G = \langle a\rangle = \{a^m\colon m \in \mathbb{Z}\}$. Setze $\phi\colon \mathbb{Z} \to G$, $m \mapsto a^m$ ist surjektiver Homomorphismus. $\ker(\phi) \trianglelefteq \mathbb{Z} \implies \exists n\colon \ker(\phi) = n\mathbb{Z}$ für ein $n \in \mathbb{N}$.
Falls $n = 0$, so ist $G \cong {}^{\mathbb{Z}}\!/_{\{0\}} \cong \mathbb{Z}$.
Falls $n \neq 0$, so ist $G \cong {}^{\mathbb{Z}}\!/_{n\mathbb{Z}}$ □

Satz 1.4.19 (1. Isomorphiesatz):
Sei G eine Gruppe, $U \leq G$ und $N \trianglelefteq G$. Dann ist $U \cdot N$ eine Untergruppe von G, $U \cap N \trianglelefteq U$ und ${}^{UN}\!/_{N} \cong {}^{U}\!/_{U \cap N}$

Beweis. Seien $u_1n_1, u_2n_2 \in UN$. Dann gilt

$$\begin{aligned}(u_1n_1)(u_2n_2)^{-1} &= (u_1n_1)(n_2^{-1}u_2^{-1}) = u_1(n_1n_2)u_2^{-1} = \\ &= u_1(n_3u_2^{-1}) = u_1(u_2^{-1}n_4) = (u_1u_2^{-1})n_4 \in UN\end{aligned}$$

mit $n_3, n_4 \in N$ passend gewählt $\implies UN \leq G$.

$N \trianglelefteq UN$ ist klar, da sogar $N \trianglelefteq G$. Sei ϕ der kanonische Epimorphismus $\phi\colon G \to {}^{G}\!/_{N}$, $g \mapsto gN$. Sei $\bar{\phi} \coloneqq \phi|_U$. $\bar{\phi}(u) = uN$ für $u \in U$. Für $v \in N$ gilt: $\bar{\phi}(u) = uN = u(vN) = (uv)N \in {}^{UN}\!/_{N}$. $\bar{\phi}\colon U \to {}^{UN}\!/_{N}$ ist homomorph. $\bar{\phi}$ ist surjektiv.

$$\ker(\bar{\phi}) = \{u \in U\colon \bar{\phi}(u) = e_{{}^{UN}\!/_{N}}\} = \{u \in U\colon \underbrace{\bar{\phi}(u)}_{=uN} = N\} = \{u \in U\colon u \in N\} = U \cap N$$

Homomorphiesatz liefert Behauptung. □

Beispiel 1.4.20 (Anwendung):

$$\underbrace{\left|{}^{UN}\!/_{N}\right|}_{=\frac{|UN|}{|N|}} = \underbrace{\left|{}^{U}\!/_{U \cap N}\right|}_{=\frac{|U|}{|U \cap N|}} \implies \frac{|U|\,|N|}{|U \cap N|} = |UN|$$

Satz 1.4.21 (2. Isomorphiesatz):
Sei G eine Gruppe, $K, H \trianglelefteq G, K \leq H$. Dann ist $K \trianglelefteq H$ und es gilt:

$${}^{G}\!/_{K}\!/_{{}^{H}\!/_{K}} \cong {}^{G}\!/_{H}$$

Beweis. $K \trianglelefteq H$ da normal in G. Betrachte $\phi\colon {}^{G}\!/_{K} \to {}^{G}\!/_{H}, gK \mapsto gH$.

- ϕ ist wohldefiniert, denn $gK = g'K \iff gg'^{-1} \in K \implies gg'^{-1} \in H \implies gH = g'H$.
- ϕ ist Homomorphismus, denn $\phi((gK)(g'K)) = \phi(gg'K) = gg'H = gHg'H = \phi(gK)\phi(g'K)$.
- ϕ ist surjektiv nach Konstruktion.
- $\ker(\phi) = \{x \in {}^{G}\!/_{K}\colon \phi(x) = e_{{}^{G}\!/_{H}}\} = \{x \in {}^{G}\!/_{K}\colon \phi(x)H\} = \{x \in {}^{G}\!/_{K}\colon xH = H\} = \{xK\colon x \in H\} = {}^{H}\!/_{K}$

Aus dem Homomorphiesatz folgt die Behauptung. □

Beispiel 1.4.22 (Anwendung):

$G = \mathbb{Z}, K \coloneqq n\mathbb{Z}, H = l\mathbb{Z}$ mit $l \mid n$.

$$\mathbb{Z}/n\mathbb{Z}/l\mathbb{Z}/n\mathbb{Z} \cong \mathbb{Z}/l\mathbb{Z}, \underbrace{\left|\mathbb{Z}/n\mathbb{Z}/l\mathbb{Z}/n\mathbb{Z}\right|}_{=\frac{\left|\mathbb{Z}/n\mathbb{Z}\right|(=n)}{\left|l\mathbb{Z}/n\mathbb{Z}\right|}} = \left|\mathbb{Z}/l\mathbb{Z}\right| = l \implies \left|l\mathbb{Z}/n\mathbb{Z}\right| = \frac{n}{l}$$

$l\mathbb{Z}/n\mathbb{Z}$ ist Untergruppe von $\mathbb{Z}/n\mathbb{Z}$ und daher zyklisch mit der Orndung $\frac{n}{l}$.

$$\implies l\mathbb{Z}/n\mathbb{Z} \cong \mathbb{Z}/\frac{n}{l}\mathbb{Z}$$

Definition 1.4.23:

Seien F, G, H Gruppen, $\phi \in \mathrm{Hom}(F, G), \psi \in \mathrm{Hom}(G, H)$. Dann heißt $F \xrightarrow{\phi} G \xrightarrow{\psi} H$ exakt bei oder in G, falls

$$\ker(\psi) = \mathrm{im}(\phi).$$

Für $F = \{e\}$ muss $\phi(e) = e_G$ gelten und Exaktheit bei G ist äquivalent zur Injektivität von ψ. Für $H = \{e\}$ muss $\psi(g) = e \forall g \in G$ und Exaktheit bei G ist äquivalent zur Surjektivität von ϕ.

Seien F, G, H multiplikativ geschrieben, so fasst man die Eigenschaften $\mathrm{im}(\phi) = \ker(\psi)$, ϕ surjektiv, ψ injektiv zusammen in der Aussage $1 \to F \xrightarrow{\phi} G \xrightarrow{\psi} H \to 1$ ist exakt bei F, G, H. und fasst dies zusammen in $1 \to F \xrightarrow{\phi} G \xrightarrow{\psi} H \to 1$ ist kurze exakte Sequenz.

Beispiel 1.4.24:

G sei Gruppe, $N \trianglelefteq G$, $\iota \colon N \to G$ die Inklusionsabbildung, $\pi \colon G \to G/N, g \mapsto gN$ der kanonische Epimorphismus. Dann ist

$$1 \to N \xrightarrow{\iota} G \xrightarrow{\pi} G/N \to 1$$

eine kurze exakte Sequenz.

1.5 Direkte Produkte

- Zerlegung von Gruppen
- Konstruktion von Gruppen aus geg. Gruppen

1. Isomorphiesatz: $U, V \trianglelefteq G, |UV| = \frac{|U||V|}{|U \cap V|}$, Sei $|U \cap V| = 1 \implies |UV| = |U|\,|V|$.

Falls $|G| = |U| \cdot |V|$, so gilt: $G = UV$ und jedes Element aus G kann eindeutig $g = uv$ mit $u \in U, v \in V$ geschrieben werden.
(denn ang. $g = u_1v_1 = u_2v_2 \implies \underset{\in U}{u_1^{-1}u_2} = \underset{\in V}{v_1v_2^{-1}} \implies u_1^{-1}u_2 = v_1v_2^{-1} \in U \cap V = \{e\} \implies v_1 = v_2 \wedge u_1 = u_2$)

Definition 1.5.1:
G heißt inneres Produkt ihrer Normalteiler $N_1, \ldots, N_k$, falls

1. $G = N_1 \cdot N_2 \cdots N_k$
2. $g = n_1 \cdots n_k$ mit $n_i \in N_i$ für $i = 1, \ldots, k$ ist eindeutig

Lemma 1.5.2:
Die Bedingungen 1 und 2 implizieren:

$$N_i \cap N_j = \{e\} \text{ für } i \neq j$$

$$ab = ba \forall a \in N_i, \forall b \in N_j$$

Beweis. Sei $x \in N_i \cap N_j$. Dann gilt:

$$x = e \cdots \underset{i\text{-te Stelle}}{\underset{|}{x}} e \cdots e = e \cdots \underset{j\text{-te Stelle}}{\underset{|}{x}} e \cdots e \overset{\text{Darstellung eindeutig}}{\Longrightarrow} x = e$$

Sei $a \in N_i, b \in N_j$, wobei $i \neq j$.

$$\left.\begin{array}{l} b \in N_j \implies aba^{-1} \in N_j \implies aba^{-1}b^{-1} \in N_j \\ a^{-1} \in N_i \implies ba^{-1}b^{-1} \in N_i \implies aba^{-1}b^{-1} \in N_i \end{array}\right\} \implies aba^{-1}b^{-1} \in N_i \cap N_j = \{e\}$$
$$\implies ab = ba \forall a \in N_i, b \in N_j \qquad \square$$

Satz 1.5.3:
Sei G eine Gruppe, $G_1, \ldots, G_k \leq G$, dann ist G das innere direkte Produkt von $G_1, \ldots, G_k$ genau dann, wenn:

1. $G = G_1 \cdots G_k$
2. $ab = ba$ für $a \in G_i, b \in G_j$ für $i \neq j$
3. $G_i \cap (G_1 \cdots G_{i-1} \cdot G_{i+1} \cdots G_k) = \{e\}$

Beweis. $\Longrightarrow$: 1. folgt aus der Definition, 2. aus Theorem 1.5.2.
3. Sei $x \in G_i \cap (G_1 \cdots G_{i-1} \cdot G_{i+1} \cdots G_k)$. $x = e \cdots exe \cdots e = a_1 \cdots a_{i-1} \cdot e \cdot a_{i+1} \cdots a_k$
wegen Eindeutigkeit
$\Longrightarrow x = e$

$\Longleftarrow$: 1. $\Longrightarrow a \in G, a = a_1 \cdots a_k$ mit $a_i \in G_i$.
Behauptung: $G_i \trianglelefteq G$. Sei $b \in G_i$. Zu Zeigen: $aba^{-1} \in G_i$

$$aba^{-1} = a_1 \cdots a_k b a_k^{-1} \cdots a_1^{-1} \overset{2.}{=} a_1 \cdots (a_i b a_i^{-1}) \cdots a_1 \overset{2.}{=} a_i b a_i^{-1} \in G_i \implies G_i \trianglelefteq G$$

Behauptung: $e = a_1 \cdots a_k \implies a_i = e,\ (i = 1, \ldots, k), a_i \in G_i$.

$$\begin{aligned} &\implies a_i^{-1} = a_1 \cdots a_{i-1} a_i^{-1} a_i a_{i+1} \cdots a_k = a_1 \cdots a_{i-1} \cdot a_{i+1} \cdots a_k \\ &\implies a_i^{-1} \in G_i \cap (G_1 \cdots G_{i-1} \cdot G_{i+1} \cdots G_k) \overset{3.}{=} \{e\} \\ &\implies e = e \cdots e \text{ ist eindeutig} \end{aligned} \tag{1.1}$$

Allgemein: ang. $a_1 \cdots a_k = b_1 \cdots b_k$ mit $a_i, b_i \in G_i$.

$$\begin{aligned} \implies a_1 b_1^{-1} a_2 \cdots a_k &= \underbrace{b_1 b_1^{-1}}_{e} b_2 \cdots b_k \\ a_1 b_1^{-1} a_2 b_2^{-1} \cdots a_k &= \underbrace{b_2 b_2^{-1}}_{e} b_3 \cdots b_k \\ \underbrace{a_1 b_1^{-1}}_{\in G_1} \cdots \underbrace{a_k b_k^{-1}}_{G_k} = e \implies a_1 b_i^{-1} = e \text{ wegen } 1.1 &\implies a_i = b_1 \forall i \end{aligned}$$ □

Korollar 1.5.4:
Für $k = 2$ ist G direktes Produkt von N_1 und N_2 genau dann, wenn

1. $N_1, N_2 \trianglelefteq G$
2. $G = N_1 N_2$ und
3. $N_1 \cap N_2 = \{e\}$

Beweis. 1., 3. klar. 2. folgt aus Theorem 1.5.2 □

Korollar 1.5.5:

G sei inneres Produkt seiner Normalteiler $N_1, \dots, N_k$. Dann gilt

$$|G| = |N_1| \cdots |N_k|$$

Beweis. Für $k = 2$ ist dies eine Folgerung aus dem 1. Isomorphiesatz 1.4.19.
$k > 2$: $G = (N_1 \cdots N_k)$. N_{k+1} mit $(N_1 \cdots N_k) \cap N_{k+1} = \{e\}$. Überdies gilt $(N_1 \cdots N_k) \trianglelefteq G$, denn $a \cdot N_1 \cdots N_k = N_1 a N_2 \cdots N_k = \cdots = N_1 \cdots N_k \cdot a$, da jedes $N_i \trianglelefteq G$.
Aus $k = 2$ folgt $|G| = |N_1 \cdots N_k| \, |N_{k+1}|$. Aus der Induktionsannahme folgt:

$$|N_1 \cdots N_k| = |N_1| \cdots |N_k| \text{, also } |G| = |N_1| \cdots |N_k| \cdot |N_{k+1}| \qquad \square$$

Umgekehrt sind $G_1, \dots, G_k$ Gruppen, so wollen wir auf $G_1 \times \cdots \times G_k$ eine Gruppenstruktur definieren, die $G_1 \times \cdots \times G_k$ zum äußeren Produkt macht.

Definition 1.5.6:

$G \coloneqq G_1 \times \cdots \times G_k = \{(g_1, \dots, g_k) \colon g_i \in G_i\}$ mit der Operation $gh \coloneqq (g_1 h_1, \dots, g_k h_k)$ heißt äußeres direktes Produkt der $G_1, \dots, G_k$ (falls $(G_i, +)$: äußere direkte Summe).

Bemerkung 1.5.7:

- $G_1 \times \cdots \times G_k$ abelsch $\iff \forall A_i \colon G_i$ abelsch
- $G_1 \times G_2 \cong G_2 \times G_1$
- $G \times H_1 \cong G \times H_2$ falls $H_1 \cong H_2$

Beispiel 1.5.8:

$(\mathbb{C}, +), \mathbb{R}, i\mathbb{R} \trianglelefteq \mathbb{C}$ und $\mathbb{C} = \mathbb{R} + i\mathbb{R}, \mathbb{R} \cap i\mathbb{R} = \{0\}$
$\mathbb{C}$ ist innere direkte Summe von $\mathbb{R}$ und $i\mathbb{R}$.
$\mathbb{C} \coloneqq \{(x, y) \colon x, y \in \mathbb{R}\} = \mathbb{R} \times \mathbb{R}$ ist äußere direkte Summe von $\mathbb{R}$ und $\mathbb{R}$.
$\mathbb{C} \cong \mathbb{R} + i\mathbb{R} \cong \mathbb{R} \times \mathbb{R}$

Satz 1.5.9:

Ist G das innere direkte Produkt seiner Normalteiler $N_i, i \in [k]$ und $H \coloneqq N_1 \times \cdots \times N_k$ das äußere direkte Produkt der Gruppen N_i, so ist $G \cong H$.

Beweis. $\phi\colon G \to H, g \mapsto (g_1, \ldots, g_k)$, wobei $g = g_1 \cdots g_k$ mit $g_i \in N_i$. Die Eindeutigkeit der Darstellung von g als $g_1 \cdots g_k$ mit $g_i \in G_i$ garantiert Wohldefiniertheit von ϕ. ϕ ist klarerweise surjektiv.

Sei $(g_1, \ldots, g_k) = (a_1, \ldots, a_k) \implies g_i = a_i, i \in [k] \implies g_1 \cdots g_k = a_1 \cdots a_k$, also ϕ injektiv.

ϕ ist Homomorphismus:

$$\phi((a_1 \cdots a_k) \cdot (b_1 \cdots b_k)) = \phi(\underbrace{a_1 b_1}_{\in N_1} \underbrace{a_2 b_2}_{\in N_2} \cdots a_k b_k) = (a_1 b_1, \ldots, a_k, b_k)$$
$$= (a_1, \ldots, a_k) \cdot (b_1, \ldots, b_k) = \phi(a_1, \ldots, a_k) \cdot \phi(b_1, \ldots b_k)$$

Gesamt: ϕ ist Isomorphismus. □

Lemma 1.5.10:

Seien G, H zyklische Gruppen $|G| = m, |H| = n$ mit $\mathrm{ggT}(m, n) = 1$, dann ist $|G \times H| = mn$. Jede zyklische Gruppe der Ordnung mn mit $\mathrm{ggT}(m, n) = 1$ ist direktes Produkt zweier Untergruppen U, V mit $|U| = m, |V| = n$.

Beweis. oBdA: $G = \mathbb{Z}/m\mathbb{Z}, H = \mathbb{Z}/n\mathbb{Z}$. Behauptung: $G \times H$ wird von $(1, 1)$ erzeugt. Es ist nämlich für $i \neq j \in \{0, 1, \ldots, mn - 1\} (i, i) \neq (j, j)$, denn aus $(i, i) = (j, j)$ folgt $i \equiv j \pmod m \wedge i \equiv j \pmod n$ und das ist wegen $(m, n) = 1$ zu $i \equiv j \pmod{mn}$ äquivalent.

$|G| = mn$ mit $(m, n) = 1 \overset{G \text{ zyklisch}}{\implies} \exists H_1, H_2 \leq G$ mit $|H_1| = m, |H_2| = n$. $H_1, H_2 \trianglelefteq G$, da G abelsch. $H_1 \cap H_2 = \{e\}$, denn $g \in H_1 \cap H_2 \implies \mathrm{ord}(g) \mid m \wedge \mathrm{ord}(g) \mid n \implies g = e$. $\implies |H_1 H_2| = |H_1|\,|H_2| = mn$ □

Korollar 1.5.11:

Sei $n \coloneqq \prod_{i=1}^{r} p_i^{\alpha_i}$ die Primfaktorzerlegung von n. Dann gilt

$$\mathbb{Z}/n\mathbb{Z} \cong \mathbb{Z}/p_1^{\alpha_1}\mathbb{Z} \times \cdots \times \mathbb{Z}/p_r^{\alpha_r}\mathbb{Z}$$

Beweis. Direkte Folgerung aus Lemma 1.5.10 □

Satz 1.5.12 (Hauptsatz für endlich erzeugte abelsche Gruppen):
Jede endlich erzeugte abelsche Gruppe G ist direktes Produkt zyklischer Untergruppen.

$$\exists r \in \mathbb{Z}^+, k_1, k_2, \ldots, k_s \in \mathbb{N} \text{ mit } k_1 \mid k_2 \mid k_3 \mid \cdots \mid k_s,$$

sodass

$$G \cong \mathbb{Z}^r \times \mathbb{Z}/k_1\mathbb{Z} \times \cdots \times \mathbb{Z}/k_s\mathbb{Z}$$

($k_1, \ldots, k_s$ sind eindeutig bestimmt)

Beweis. Hier gibt es einen „einfachen“ Induktionsbeweis, für eine etwas allgemeinere Form der Aussage folgt in Algebra 2 ein Beweis □

Beispiel 1.5.13 (Anwendung):
Sei $|G| = 200$ mit G abelsch. Wie viele nicht-isomorphe Gruppen gibt es?
$\rightarrow$ Finde alle $(k_1, k_2, \ldots, k_s)$ mit $k_1 \mid k_2 \mid \cdots \mid k_s$ und $\prod_{i=1}^{s} k_i = 200$.

$s = 1$: $k_1 = 200 = 2^3 \cdot 5^2$

$s = 2$: $(k_1, k_2) \in \{(2, 100), (10, 20), (5, 40)\}$

$s = 3$: $(k_1, k_2, k_3) \in \{(2, 2, 50), (2, 10, 10)\}$

Es gibt genau 6 paarweise nicht isomorphe abelsche Gruppen G mit $|G| = 200$.

Satz 1.5.14:
Sei G eine abelsche Gruppe mit $|G| = n$, $d \mid n$. Dann existiert $H \leq G$ mit $|H| = d$. (das heißt Folgerung aus Lagrange (Theorem 1.4.4) hinsichtlich der Ordnung von Untergruppen ist für abelsche Gruppen umkehrbar!)

Beweis. $G \cong \mathbb{Z}/k_1\mathbb{Z} \times \cdots \times \mathbb{Z}/k_s\mathbb{Z}$ mit $k_1 \mid \cdots \mid k_s$. $k_1 \cdots k_s = n.d \mid n \implies d = l_1 \cdots l_s$ mit $l_1 \cdots l_s = d$ und $l_i \mid k_i$ für $i = 1, \ldots, s$.
Rest im Proseminar □

1.6 Semidirekte Produkte

Inneres direktes Produkt: $G, N_1, N_2 \trianglelefteq G$ mit $N_1 N_2 = G$ & $N_1 \cap N_2 = \{e\} \implies G$ ist inneres direktes Produkt von N_1, N_2.

Dies ist der Fall, wenn $|G| = lm$ mit $(l, m) = 1$ und Normalteiler N_1, N_2 existieren mit $|N_1| = l, |N_2| = m$. $|N_1 N_2| = \frac{|N_1| \cdot |N_2|}{|N_1 \cap N_2|}$ und $|N_1 \cap N_2| = 1$, denn $g \in N_1 \cap N_2 \implies \operatorname{ord}(g) \mid l \wedge \operatorname{ord}(g) \mid m$, woraus wegen $(l, m) = 1, \operatorname{ord}(g) = 1$ folgt.

Wir wissen bereits (Theorem 1.4.19), dass für $H \leq G, N \trianglelefteq G$ gilt:

$$NH \leq G$$

Definition 1.6.1:

G heißt inneres semidirektes Produkt seiner Untergruppen H und N, falls

1. $N \trianglelefteq G$
2. $G = NH$
3. $N \cap H = \{e\}$

Man schreibt dafür $G = N \rtimes H$.

Es gilt nach wie vor: jedes $g \in G$ kann eindeutig als $g = nh$ mit $n \in N, h \in H$ dargestellt werden, das heißt $N \times H \to G, (n, h) \mapsto nh$ ist bijektiv. Angenommen $n_1 h_1 = n_2 h_2 \implies \underbrace{n_2^{-1} n_1}_{\in N} = \underbrace{h_2 h_1^{-1}}_{\in H} \implies n_2^{-1} n_1 = e = h_2 h_1^{-1} \implies n_2 = n_1, h_2 = h_1$

Es gilt im Allgemeinen nicht mehr: $nh = hn$! Das bedeutet $(n_1 h_1)(n_2 h_2) \overset{\text{i.A.}}{\neq} (n_1 n_2 h_1 h_2)$
Für festes $h \in H$ ist $\gamma_h \colon N \to N$,
$n \mapsto hnh^{-1}$. $\gamma_h \in \operatorname{Aut}(N)$ und setze $\gamma \colon H \to \operatorname{Aut}(N), h \mapsto \gamma_h$. γ ist ein Homomorphismus: $\gamma_{hh'}(n) = hh'n(hh')^{-1} = h \underbrace{(h'nh'^{-1})}_{\gamma_{h'}(n)} h^{-1} = \gamma_h(\gamma_{h'}(n)) = \gamma_h \circ \gamma_{h'}(n)$ G ist durch N, H und γ eindeutig definiert, denn $(n_1 h_1) \cdot (n_2 h_2) = n_1 \gamma_{h_1}(n_2) \cdot h_1 h_2 = n_1 h_1 n_2 h_1^{-1} h_1 h_2 = n_1 h_1 n_2 h_2$.
Dieses Produkt ist direkt $\iff (n_1 h_1)(n_2 h_2) = n_1 n_2 h_1 h_2 \iff \gamma_h(n) = n \forall h \in H \iff$ $\gamma \colon H \to \operatorname{Aut}(N)$ ist trivialer Homomorphismus.

Beispiel 1.6.2:

$G = \mathfrak{S}_4$.

- $V_4 \trianglelefteq \mathfrak{S}_4$. Wir betrachten $H = \{\sigma \in \mathfrak{S}_4 \colon \sigma(4) = 4\}$. $|V_4| = 4, |H| = 6, V_4 \cap H = \{\mathrm{id}\} \implies \mathfrak{S}_4 = V_4 \rtimes H$.
- $\mathcal{A}_4 \trianglelefteq \mathfrak{S}_4, \langle (34) \rangle \,.\, |\mathcal{A}_4| = 12, |\langle (34) \rangle| = 2, \mathcal{A}_4 \cap \langle (34) \rangle = \{\mathrm{id}\} \implies \mathfrak{S}_4 = \mathcal{A}_4 \rtimes \langle (34) \rangle$

Umgekehrt: Seien N, H Gruppen und $\gamma \colon H \to \operatorname{Aut}(N), h \mapsto \gamma_h$ ein Homomorphismus. Dann bildet die Menge aller Paare (n, h) mit $n \in N, h \in H$ zusammen mit der Verknüpfung

$(n_1, h_1)(n_2, h_2) \coloneqq (n_1\gamma_{h_1}(n_2), h_1h_2)$ eine Gruppe $G = N \rtimes_\gamma H$, das äußere semidirekte Produkt von N und H vermöge γ.

- Assoziativität:

$$\begin{aligned}(n_1\gamma_{h_1}(n_2), h_1h_2)(n_3, h_3) &= (n_1\gamma_{h_1}(n_2)\gamma_{h_1h_2}(n_3), h_1h_2h_3)\\ &= (n_1\gamma_{h_1}(n_2)\gamma_{h_1}(\gamma_{h_2}(n_3)), h_1h_2h_3)\\ &= (n_1\gamma_{h_1}(n_2\gamma_{h_2}(n_3)), h_1h_2h_3)\\ &= (n_1, h_1)(n_2\gamma_{h_2}(n_3), h_2h_3) = (n_1, h_1)((n_2, h_2)(n_3, h_3))\end{aligned}$$

- Neutrales Element: (e_N, e_H) ist das neutrale Element.

$$(e_N, e_H)(n, h) = (e_N\gamma_{e_H}(n), e_Hh) = (n, h)$$

- Inverses Element: $(n, h)^{-1} \coloneqq (\gamma_h^{-1}(n^{-1}), h^{-1})$ erfüllt

$$(n, h)(n, h)^{-1} = (n, h)^{-1}(n, h) = (e_N, e_H).$$

$$(\gamma_h^{-1}(n^{-1}), h^{-1})(n, h) = (\underbrace{\gamma_h^{-1}(n^{-1})\gamma_{h^{-1}}(n)}_{\gamma_{h^{-1}}(e_N)=e_N}, h^{-1}h) = (e_N, e_H)$$

Sei $N^* \coloneqq \{(n, e_H) \colon n \in N\} \subseteq G$, $H^* \coloneqq \{(e_N, h) \colon h \in H\} \subseteq G$. Dann gilt $N^*, H^* \leq G$.

$$(n_1, e_H)(n_2, e_H) = (n_1\underbrace{\gamma_{e_H}(n_2)}_{n_2}, e_H) \in N^*$$

$$(e_N, h_1)(e_N, h_2) = (e_N\gamma_{h_1}(e_N), h_1h_2) = (e_N, h_1h_2) \in H^*$$

$N \trianglelefteq G$ als Kern des surjektiven Homomorphismus

$$\pi \colon G \to H, (n, h) \mapsto h.$$

$N^* \cap H^* = \{(e_N, e_H)\} = \{e_G\}$. $G = N^*H^*$ wegen $(n, h) = \underbrace{(n, e_H)}_{\in N^*}\underbrace{(e_N, h)}_{\in H^*} \implies G$ ist inneres semidirektes Produkt von N^* und H^*.

Bemerkung 1.6.3:
$G = N \rtimes_\gamma H$ liefert die kurze exakte Sequenz

$$1 \to N \xrightarrow{\iota} G \xrightarrow{\pi} H \to 1$$

Es existiert $j \colon H \to G$ mit $\pi \circ j = \mathrm{id}_H (j(h) = (e_N, h))$.

Beispiel 1.6.4:

1. Diedergruppen. Sei $N \coloneqq \mathbb{Z}/k\mathbb{Z}, H \coloneqq \mathbb{Z}/2\mathbb{Z}.D_k \coloneqq \mathbb{Z}/k\mathbb{Z} \rtimes_\gamma \mathbb{Z}/2\mathbb{Z}$, wobei $\gamma\colon \mathbb{Z}/2\mathbb{Z} \to \mathrm{Aut}(\mathbb{Z}/k\mathbb{Z}), h \mapsto \gamma_h \coloneqq \begin{cases}\gamma_0(n) = n \\ \gamma_1(n) = -n\end{cases}$ heißt Diedergruppe ($k \geq 2$).

   - $k = 2 : \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \cong V_4$
   - $k = 3 : \mathbb{Z}/3\mathbb{Z} \rtimes_\gamma \mathbb{Z}/2\mathbb{Z} \cong \mathcal{S}_3$
   - $k = 4 : \mathbb{Z}/4\mathbb{Z} \rtimes_\gamma \mathbb{Z}/2\mathbb{Z}$

   D_k ist die Gruppe der Symmetrien des regelmäßigen k-Ecks. Die Drehungen um den Winkel $\frac{2r\pi}{k} (0 \leq r \leq k-1) \leftrightarrow \mathbb{Z}/k\mathbb{Z}$ Die Spiegelungen $\leftrightarrow \mathbb{Z}/2\mathbb{Z}$

2. Sei V ein Vektorraum, $\mathrm{GL}(V)$ die Gruppe der Vektorraumautomorphismen. $T(V)$ die Gruppe der Translationen von $V (\cong V)$. $A\,\mathrm{GL}(V) \coloneqq V \rtimes_\theta \mathrm{GL}(V)$, wobei $\theta\colon \mathrm{GL}(V) \to \mathrm{Aut}(V) (= \mathrm{GL}(V))$,
   $f \mapsto (v \to f(v))$ heißt die affine Gruppe von V. Die Verknüpfung ist dann folgende: $(v, f)(w, g) = (v + f(w), f \circ g)$.

3. Erinnerung: $\mathcal{S}_4 = V_4 \rtimes H$ mit $H \coloneqq \{\sigma \in \mathcal{S}_4 : \sigma(4) = 4\}$.
   $\mathcal{S}_4 = (\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}) \rtimes_\theta \mathcal{S}_3$, wobei $\theta : \mathcal{S}_3 \to \mathrm{Aut}(\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z})$ Die Vektorraumautomorphismen von $\mathbb{K}^n$ sind $\mathrm{GL}_n(\mathbb{K})$, diese sind genau die Gruppenautomorphismen von K^n.

$$\mathrm{Aut}(\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}) = \mathrm{GL}_2(\mathbb{Z}/2\mathbb{Z})$$

$$\mathrm{GL}_2(\mathbb{Z}/2\mathbb{Z}) = \left\{ \begin{pmatrix}1 & 0\\ 0 & 1\end{pmatrix}, \begin{pmatrix}0 & 1\\ 1 & 0\end{pmatrix}, \underbrace{\begin{pmatrix}1 & 1\\ 0 & 1\end{pmatrix}}_{\text{hat Ordnung 2}}, \begin{pmatrix}1 & 0\\ 1 & 1\end{pmatrix}, \underbrace{\begin{pmatrix}1 & 1\\ 1 & 0\end{pmatrix}}_{\text{hat Ordnung 3}}, \begin{pmatrix}0 & 1\\ 1 & 1\end{pmatrix} \right\}$$

Definiere θ durch $\begin{cases}\theta((123)) = \begin{pmatrix}1 & 1\\ 1 & 0\end{pmatrix} \\ \theta((12)) = \begin{pmatrix}1 & 1\\ 0 & 1\end{pmatrix}\end{cases}$

1.7 Gruppenaktionen

Definition 1.7.1:
Sei G eine Gruppe, S eine Menge. G operiert auf S (von links), falls eine Abbildung

$$\alpha\colon G \times S \to S, (g, s) \mapsto gs$$

existiert mit

1. $e_G s = s \forall s \in S$
2. $(hg)s = h(gs) \forall g, h \in G, \forall s \in S$

Bemerkung 1.7.2:
Für festes $g \in G$ ist $\tau_g\colon S \to S, s \mapsto gs$ bijektiv, denn sie besitzt ein als Inverse die Abbildung $\tau_{g^{-1}}$. $(\tau_{g^{-1}} \circ \tau_g)(s) = g^{-1}(gs) = (g^{-1}g)s = e_G s = s$. Es ist $\tau_{gh} = \tau_g \circ \tau_h$, also ist $\tau\colon G \to \mathfrak{S}(S), g \mapsto \tau_g$ ein Gruppenhomomorphismus. Umgekehrt definiert jeder Gruppenhomomorphismus $\tau : G \to \mathfrak{S}(S)$ eine Aktion von G auf S.

Definition 1.7.3:
Sei $\alpha\colon G \times S \to S$ eine Aktion von G auf S, $X \subseteq S, s \in S, g \in G$

- $G \cdot s = Gs = \{gs\colon g \in G\}$ heißt der Orbit (die Bahn) von s unter der Aktion von G.
- ${}^{S}\!/_{G} \coloneqq \{Gs\colon s \in S\}$ ist die Menge aller Orbits der Aktion von G.
- $G_X \coloneqq \{g \in G\colon gX = X\}$ heißt der Stabilisator von X. (es muss nicht $gx = x \forall x \in X$ gelten!)
- $G_{\{s\}} =: G_s = \{g \in G\colon gs = s\}$ heißt Stabilisator von $s \in S$.
- $s \in S$ heißt Fixpunkt der Aktion α, falls $gs = s \forall g \in G$ (das heißt $G_s = G$).
- Die Menge aller Fixpunkte der Aktion α wird mit S^G bezeichnet.
- Die Aktion α heißt transitiv, falls $\forall s_1, s_2 \in S \exists g \in G\colon gs_1 = s_2$.

Bemerkung 1.7.4:

α ist transitiv genau dann, wenn $\forall s \in S\colon S = Gs$.

- $\Longleftarrow$: Sei nämlich $s_1 = g_1 s, s_2 = g_2 s$. Wähle $g \coloneqq (g_2 g_1^{-1})$. Dann gilt: $(g_2 g_1^{-1}) s_1 = (g_2 g_1^{-1}) g_1 s = g_2 s = s_2$
- $\Longrightarrow$: Angenommen für ein $s_1 \in S$ gelte $Gs_1 \neq S$, das heißt $\exists s_2 \in S$ mit $gs_1 \neq s_2 \forall g \in G$, sodass α nicht transitiv ist.

Beispiel 1.7.5:

1. $G = \mathfrak{S}_n, S = \{1, \ldots, n\}, \alpha\colon \mathfrak{S}_n \times \{1, \ldots, n\} \to \{1, \ldots, n\}, (\sigma, i) \mapsto \sigma(i)$.
   Der Stabilisator $(\mathfrak{S}_n)_i$ besteht genau aus den Permutationen, die i als Fixpunkt haben.

   Sei $\langle \sigma \rangle$ die von $\sigma \in \mathfrak{S}_n$ erzeugte Untergruppe von $\mathfrak{S}_n$ und wir betrachten die Einschränkung von α auf $\langle \sigma \rangle$. $(\sigma^k, i) \mapsto \sigma^k(i)$. Die Orbits dieser Aktion haben die Gestalt $(i, \sigma(i), \sigma^2(i), \ldots, \sigma^r(i))$ und entsprechen daher genau den Zyklen der Permutation σ.

2. Sei $H \leq G, \alpha\colon H \times G \to G, (h, g) \mapsto gh^{-1} = \alpha(h, g)$. $\alpha(e, g) \mapsto g$✓ $\alpha(h_1 h_2, g) = g(h_1 h_2)^{-1} = (gh_2^{-1}) h_1^{-1} = \alpha(h_2, g) h_1^{-1} = \alpha(h_1, \alpha(h_2, g))$. Der Orbit $H_g = \{\alpha(h, g) : h \in H\} = \{gh^{-1} : h \in H\} = gH$ entspricht der Linksnebenklasse gH.

   G/H = Menge der Orbits = Menge der Linksnebenklassen. ($\nexists$ Fixpunkt, falls $H \neq \{e\}$)

3. G Gruppe, $H \leq G$. G/H: Linksnebenklassen von G nach H.

   $$\alpha\colon G \times G/H \to G/H, (g, g'H) \mapsto gg'H$$

   Behauptung: α ist transitiv. Seien $g_1 H, g_2 H$ beliebige Linksnebenklassen. Dann ist $(g_2 g_1^{-1}) g_1 H = g_2 (g_1^{-1} g_1) H = g_2 H$.

4. $\alpha\colon G \times G \to G, (g, h) \mapsto gh$. Dann ist α Aktion wegen $\exists e \in G$ und G erfüllt das Assoziativgesetz.

5. $\alpha\colon \mathrm{GL}(V) \times V \to V, (f, v) \mapsto f(v)$. $V = 0$ ist ein einpunktiger Orbit. $V \neq 0$ hat als Orbit $V \setminus \{0\}$.

   $\mathrm{End}(V)$:Vektorraumendomorphismen von V.

   $$\beta\colon \mathrm{GL}(V) \times \mathrm{End}(V) \to \mathrm{End}(V), (f, g) \mapsto fgf^{-1}$$

   $V = \mathbb{K}^n\colon \mathrm{GL}_n(\mathbb{K}) \times M_{n \times n}(\mathbb{K}) \to M_{n \times n}(\mathbb{K}), (S, A) \mapsto SAS^{-1}$. Orbit von A besteht aus allen zu A ähnlichen Matrizen.

Proposition 1.7.6:

$\alpha\colon G \times S \to S$ sei eine Aktion.

1. Für $X \subseteq S$ ist G_X eine Untergruppe von G (die Stabilisatoruntergruppe von X).
2. Definiert man $s_1 \sim s_2 :\iff \exists g \in G$ mit $s_1 = gs_2$, so ist $\sim$ eine Äquivalenzrelation auf S.
3. Für $s \in S$ ist $f\colon {}^{G}\!/_{G_s} \to Gs, gG_s \mapsto gs$ eine Bijektion von der Menge der Linksnebenklassen von G_s auf den Orbit Gs

Beweis. 1. $X \subseteq S, e \in G_X \implies G_X \neq \emptyset$. Seien $g, h \in G_X$, das heißt $gX = X$ und $hX = X$. Es folgt $(gh)X \underset{\text{Aktion}}{=} g(hX) = gX = X$, also $gh \in G_X$. Weiters: $g^{-1}X = g^{-1}(gX) = (g^{-1}g)X = eX = X$, also $g^{-1} \in G_X$. Also $G_X \leq G$.

2. Sei $s \in S$. Dann ist $e \cdot s = s$, also $s \sim s$. Für $s_1, s_2 \in S$ mit $s_1 = gs_2$ folgt $g^{-1}(s_1) = g^{-1}(gs_2) \underset{\text{Aktion}}{=} (g^{-1}g)(s_2) = es_2 = s_2$. Für $s_1, s_2, s_3 \in S$ mit $s_1 = gs_2, s_2 = hs_3$ gilt $s_1 = gs_2 = g(hs_3) = (gh)s_3$. Also ist $\sim$ eine Äquivalenzrelation.

   Folgerung: ${}^{S}\!/_{\sim} = {}^{S}\!/_{G}$, daher $S = \bigcup_{s \in S} Gs$ und $Gs \cap Gt = \emptyset$ oder $Gs = Gt$.

3. Seien $g_1, g_2 \in G$ und $g_1 s = g_2 s \iff (g_1^{-1}g_2)s = s \iff g_1^{-1}g_2 \in G_s$. Diese Äquivalenz liefert Wohldefiniertheit und Injektivität von f. Die Surjektivität ist klar. □

Korollar 1.7.7:

Die Länge des Orbits von s unter G ist der Index der Stabilisatoruntergruppe von s in G.

$$|Gs| = [G : G_s]$$

Beweis. Direkte Folgerung aus Theorem 1.7.6. □

Korollar 1.7.8 (Bahngleichung/Orbitzerlegungsformel):

Sei $\alpha : G \times S \to S$ die Aktion von G auf einer endlichen Menge S. Dann gilt:

$$|S| = \sum_{i \in I} \left| {}^{G}\!/_{G_{s_i}} \right| = \sum_{i \in I} [G : G_{s_i}],$$

wobei $G_{s_i}, i \in I$ ein Repräsentantensystem für die disjunkten Orbits der Aktion α durchläuft.

Beweis. Direkte Folgerung aus Theorem 1.7.6 □

Alternativ:

$$|S| = \left|S^G\right| + \sum_{i \in \tilde{I}} [G : G_{s_i}],$$

wobei G_{s_i} die disjunkten Orbits der Länge > 1 durchläuft.

Beispiel 1.7.9:
$\alpha \colon G \times G \to G, (g,h) \mapsto ghg^{-1}$ „Konjugation“.
$H, H' \leq G$ heißen konjugiert, falls sie im selben Orbit bezüglich α liegen, das heißt $\exists g \in G : gHg^{-1} = H'$. Für $h \in G$: der Orbit $Gh = \{ghg^{-1} : g \in G\}$ heißt Konjugationsklasse von h. Der Stabilisator G_h von $h \in G$ bezüglich α ist genau der Zentralisator $Z_G(h)$. Der Stabilisator G_H von $H \leq G$ bezüglich α ist der Normalisator $N_G(H)$ (das ist die größte Untergruppe von G, in der H normal ist).

Lemma 1.7.10 (Lemma von Burnside):
Sei $\alpha : G \times S \to S$ eine Aktion einer endlichen Gruppe G auf der endlichen Menge S. Dann gilt: $\left|S/G\right| = \frac{1}{|G|} \cdot \sum_{g \in G} |S^g|$, wobei $S^g := \{s \in S : gs = s\}$

Beweis. Setze $T := \{(g,s) \in G \times S : gs = s\}$. $|T|$ kann auf 2 verschiedene Arten ermittelt werden.

1. für jedes feste $g \in G$: zähle $s \in S$ mit $gs = s$ und summiere über alle $g \in G$.
2. für jedes feste $s \in S$: zähle $g \in G$ mit $gs = s$ und summiere über alle $s \in S$.

1. $\sum_{g \in G} |S^g|$
2. $\sum_{s \in S} |G_s|$

$\sum_{s \in S} |G_s| = \sum_{i=1}^{|S/G|} \sum_{y \in Gs_i} |G_y|$, wobei $G_{S_1}, \ldots, G_{S_{|S/G|}}$ ein Repräsentantensystem für die disjunkten Orbits bildet. Für $y, y' \in Gs_i$ gilt $|G_y| = |G_{y'}| = |G_{s_i}|$, daher ist $\sum_{y \in G_{s_i}} |G_y| = |G_{s_i}| \cdot \underbrace{|Gs_i|}_{[G:G_{s_i}]} = |G|$. Schlussendlich $\sum_{s \in S} |G_s| = \sum_{i=1}^{|S/G|} |G| = \left|S/G\right| |G|$ □

1.8 Die Sylow-Sätze

Definition 1.8.1:
Eine endliche Gruppe G mit $|G| = p^r$ für ein $r \geq 1, p \in \mathbb{P}$ heißt p-Gruppe.

Proposition 1.8.2:
Sei $\alpha\colon G \times S \to S$ die Aktion einer p-Gruppe G auf einer endlichen Menge S. Dann gilt $|S| \equiv \left|S^G\right| \mod p$.

Beweis. $|S| = \left|S^G\right| + \sum \left|{}^{G}\!/_{G_{x_i}}\right|$. Aus $|G| = p^r = \left|{}^{G}\!/_{G_{x_i}}\right| \cdot |Gx_i|$ folgt, dass $p \mid \sum \left|{}^{G}\!/_{G_{x_i}}\right|$. Daraus folgt die Behauptung. □

Korollar 1.8.3:
Sei G eine p-Gruppe, dann ist $|G| \equiv |Z(G)| \mod p$ und $|Z(G)| > 1$.

Beweis. Sei $\alpha\colon G \times G \to G$ die Konjugation, nach Theorem 1.8.2 gilt $|G| \equiv |Z(G)| \mod p$. Wegen $|G| = p^r$ gilt $|Z(G)| \equiv 0 \mod p$, daher folgt $|Z(G)| > 1$. □

Korollar 1.8.4:
Jede Gruppe G der Ordnung p^2 ist abelsch.

Beweis. Es gilt nach Theorem 1.8.3: $|Z(G)| \in \{p, p^2\}$. Angenommen es gelte $|Z(G)| = p$. Wegen $Z(G) \trianglelefteq G$, können wir die Gruppe ${}^{G}\!/_{Z(G)}$ bilden. $\left|{}^{G}\!/_{Z(G)}\right| = p \implies {}^{G}\!/_{Z(G)}$ ist zyklisch, das heißt $\exists x \in G$ mit ${}^{G}\!/_{Z(G)} = \langle xZ(G)\rangle$. Jedes $gZ(G)$ lässt sich als $(xZ(G))^r = x^r Z(G)$ schreiben (für geeignetes r). $g = x^r a$ mit $a \in Z(G)$ Daher gilt für $g, h \in G$:

$$\begin{aligned} gh &= x^r \cdot a \cdot x^s \cdot b \ (h = x^s \cdot \underbrace{b}_{\in Z(G)}) \\ &= x^r x^s ab = x^{r+s} ab = x^s b x^r a = hg \end{aligned}$$

□

Definition 1.8.5:

Sei $p \in \mathbb{P}, G$ eine endliche Gruppe der Ordnung $p^r \cdot m$ mit $r \geq 1, \text{ggT}(m,p) = 1$. Eine Untergruppe $H \leq G$ mit $|H| = p^r$ heißt p-Sylow Untergruppe von G. $\text{Syl}_p(G)$ bezeichnet die Menge aller p-Sylow Untergruppen von G.

Beispiel 1.8.6:

$G = \mathfrak{S}_4, |\mathfrak{S}_4| = 24 = 2^3 \cdot 3$. Wir betrachten die Untergruppen

$$\begin{aligned} H &:= \langle (1234), (24) \rangle \text{ hat Ordnung 8.} \\ H' &:= \langle (1243), (23) \rangle \text{ hat Ordnung 8.} \\ H'' &:= \langle (1324), (34) \rangle \text{ hat Ordnung 8.} \end{aligned}$$

Dann gilt $H, H', H'' \in \text{Syl}_2(\mathfrak{S}_4)$. Es gilt sogar $\text{Syl}_2(\mathfrak{S}_4) = \{H, H', H''\}$. Wir betrachten die Untergruppen

$$\begin{aligned} J &:= \langle (123) \rangle \text{ hat Ordnung 3.} \\ J' &:= \langle (124) \rangle \text{ hat Ordnung 3.} \\ J'' &:= \langle (134) \rangle \text{ hat Ordnung 3.} \\ J''' &:= \langle (234) \rangle \text{ hat Ordnung 3.} \end{aligned}$$

$\text{Syl}_3(\mathfrak{S}_4) = \{J, J', J'', J'''\}$

Satz 1.8.7 (1. Sylowsatz):

$|G| = p^r \cdot m$ mit $r \geq 1, (m,p) = 1$. Dann enthält G mindestens eine p-Sylow Untergruppe.

Beweis. Sei $S := \{X \subseteq G : |X| = p^r\}, \alpha \colon G \times S \to S, (g,X) \mapsto gX$ liefert eine Aktion. Es gilt: $|S| = \binom{p^r m}{p^r} = \frac{p^r m (p^r m - 1) \cdots (p^r m - p^r + 1)}{p^r (p^r - 1) \cdots 1}$ und $p \nmid |S|$. Bezeichnet $\nu_p(n)$ die Vielfachheit von p in n, so gilt: $\nu_p(p^r \cdot m - i) = \nu_p(p^r - i)$. Wir wissen $S = \bigcup_{X \in S} GX$. Wegen $p \nmid |S|$ gilt $p \nmid |\bigcup_{X \in S} GX| \implies \exists X \in S : p \nmid |GX|$.

Wegen $\underbrace{|G|}_{=p^r m} = \underbrace{|GX|}_{p^r \nmid} \cdot |G_X|$ folgt $p^r \mid |G_X|$. Behauptung: Es gilt sogar $|G_X| = p^r$. G_X operiert auf X durch Multiplikation, die Orbits $G_X x$ entsprechen den Rechtsnebenklassen von G_X. Jeder Orbit hat genau $|G_X|$ Elemente, daher gilt $|G_X| \mid \underbrace{|X|}_{=p^r}$ und daher folgt $|G_X| = p^r$. Somit ist G_X eine p-Sylow Untergruppe von G. $\square$

Satz 1.8.8 (2. Sylowsatz):
Seien P, Q zwei p-Sylow Untergruppen von G. Dann sind P und Q konjugiert, das heißt $\exists g \in G$ mit $gPg^{-1} = Q$. Die Gruppe G agiert auf $\mathrm{Syl}_p(G)$ durch Konjugation und diese Aktion ist transitiv.

Beweis. G operiert auf der Menge der Linksnebenklassen von G nach Q, also auf G/Q. $P \leq G$, die Einschränkung der Aktion auf P liefert eine Aktion von P auf G/Q. Laut Voraussetzung gilt: $p \nmid \left|G/Q\right|$. Es folgt: diese Aktion hat mindestens einen Fixpunkt. Sei $h \in Q$ dieser Fixpunkt, das heißt $g(hQ) = hQ$ für alle $g \in P$.

$$ghQ = hQ \iff gh \in hQ \iff g \in hQh^{-1} \forall g \in P \iff P \subseteq hQh^{-1}$$

Wegen $|P| = |Q|$ folgt $P = hQh^{-1}$ □

Korollar 1.8.9:
Jede p-Untergruppe von G ist in einer p-Sylow Untergruppe von G enthalten.

Beweis. Wähle im 2. Sylowsatz 1.8.8 für P die p-Untergruppe von G, für Q eine p-Sylow Untergruppe von G. Bis auf den letzten Schritt folgt das gleiche, insbesondere $P \subseteq hQh^{-1}$. Da Q schon p-Sylow Untergruppe ist, ist hQh^{-1} auch eine. □

Korollar 1.8.10:
$\left|\mathrm{Syl}_p(G)\right| = 1 \iff$ die p-Sylow Untergruppe von G ist Normalteiler.

Beweis. Folgt unmittelbar aus dem 2. Sylowsatz 1.8.8. □

Satz 1.8.11 (3. Sylowsatz):
1. $\left|\mathrm{Syl}_p(G)\right| \mid m$
2. $\left|\mathrm{Syl}_p(G)\right| \equiv 1 \mod p$

Beweis.

1. Sei $P \in \mathrm{Syl}_p(G)$. G operiert auf $\mathrm{Syl}_p(G)$ durch Konjugation, diese Aktion hat nur einen Orbit nach dem 2. Sylowsatz 1.8.8. Es folgt: $\mathrm{Syl}_p(G) = GP$, insbesondere $\left|\mathrm{Syl}_p(G)\right| = |GP|$.

$$|GP| = \left|{}^{G}\!/_{G_P}\right| = \left|{}^{G}\!/_{N_G(P)}\right| = [G : N_G(P)] \tag{1.2}$$

Es ist $P \leq N_G(P)$ und

$$[G : P] = [G : N_G(P)] \cdot [N_G(P) : P] \tag{1.3}$$

Kombiniert man die beiden Aussagen (1.2, 1.3), folgt $\left|\mathrm{Syl}_p(P)\right| \mid \underbrace{\left|{}^{G}\!/_{P}\right|}_{m}$

2. Durch Einschränkung dieser Aktion auf P erhalten wir eine Aktion von P auf $\mathrm{Syl}_p(G)$. Behauptung: P ist der einzige Fixpunkt dieser Aktion. Sei Q ein Fixpunkt der Aktion, das heißt $gQg^{-1} = Q \forall g \in P$. Das bedeutet: $P \subseteq N_G(Q)$. Wir wenden nun den 2. Sylowsatz 1.8.8 in $N_G(Q)$ an auf die p-Sylow Untergruppen P und Q von $N_G(Q) : \exists g \in N_G(Q) : Q = gQg^{-1} = P$.

Daher gilt: $\left|\mathrm{Syl}_p(G)\right| \equiv \underset{\left|\mathrm{Syl}_p(G)^G\right|}{1} \mod p$ □

Beispiel 1.8.12:

Jede Gruppe G der Ordnung 143 ist zyklisch.

$143 = 11 \cdot 13$, daher besitzt G 13 beziehungsweise 11-Sylow Untergruppen. $\underbrace{|\mathrm{Syl}_{11}(G)| \mid 13}_{\implies \in \{1,13\}}, \underbrace{|\mathrm{Syl}_{11}| \equiv 1 \mod 11}_{\in \{1,12,23,\dots\}}$ Es folgt: $|\mathrm{Syl}_{11}(G)| = 1 \implies S_{11} \trianglelefteq G$. S_{11} ist die einzige 11-Sylow Untergruppe von G.

Analog: $|\mathrm{Syl}_{13}(G)|$ teilt 11 und ist $\equiv 1 \mod 13$, also $\exists! S_{13} \trianglelefteq G$. G enthält die Normalteiler S_{11} und S_{13}. $S_{11} \cap S_{13} = \{e\}$. Es folgt wegen $|S_{11}| \cdot |S_{13}| = 11 \cdot 13 = 143$ und $|S_{11} \cap S_{13}| = 1$, dass $G = S_{11}S_{13}$. Daher gilt auch $G \cong S_{11} \times S_{13} \cong {}^{\mathbb{Z}}\!/_{11\mathbb{Z}} \times {}^{\mathbb{Z}}\!/_{13\mathbb{Z}} \cong {}^{\mathbb{Z}}\!/_{143\mathbb{Z}}$

Beispiel 1.8.13:

p, q seien verschiedene Primzahlen. Jede Gruppe G mit $|G| = p \cdot q$ hat einen nicht-trivialen Normalteiler.

Beweis. oBdA: $p < q$.

$$\left|\mathrm{Syl}_q(G)\right| \equiv 1 \mod q \implies \in \{1, q+1, 2q+1, \dots\}$$

$\left|\mathrm{Syl}_q(G)\right| \mid p$. Wegen $p < q$ kommt nur $\left|\mathrm{Syl}_q(G)\right| = 1$ in Frage. Darum ist die p-Sylow Untergruppe Normalteiler. Könnten wir zeigen, dass auch $\left|\mathrm{Syl}_p(G)\right| = 1$, so wäre G zyklisch.

$\left|\mathrm{Syl}_p(G)\right| \equiv 1 \mod p$ und teilt q, daher $\left|\mathrm{Syl}_p(G)\right| \in \{1, q\}$. Wäre $\left|\mathrm{Syl}_p(G)\right| = q$, so folgte $q \equiv 1 \mod p$. Jede Gruppe G mit $|G| = pq, p < q$ verschiedene Primzahlen mit $q \not\equiv 1 \mod p$ ist zyklisch.

Beispiel 1.8.14:

Wie viele Elemente der Ordnung 5 gibt es in einer Gruppe G mit $|G| = 20$?

$20 = 4 \cdot 5 \implies \exists 5-$Sylow Untergruppen. $|\mathrm{Syl}_5(G)| \equiv 1 \mod 5$ und teilt 4 $\implies |\mathrm{Syl}_5(G)| = 1$. $\exists! H \leq G$ mit $|H| = 5$, also 4 Elemente der Ordnung 5.

Beispiel 1.8.15:

Bestimmung einer p-Sylow Untergruppe von $\mathrm{GL}_n\left(\mathbb{Z}/p\mathbb{Z}\right)$.

Zunächst: $\left|\mathrm{GL}_n\left(\mathbb{Z}/p\mathbb{Z}\right)\right|$?

$$\begin{pmatrix} * & * & \cdots & * \\ \vdots & & & \\ * & \cdots & \cdots & * \end{pmatrix}, * \in \mathbb{Z}/p\mathbb{Z}$$

1. Zeile: $p^n - 1$ Möglichkeiten

2. Zeile: $p^n - p$ Möglichkeiten

3. Zeile: $p^n - p^2$ Möglichkeiten

$\vdots$

n. Zeile: $p^n - p^{n-1}$ Möglichkeiten

Es folgt $\left|\mathrm{GL}_n\left(\mathbb{Z}/p\mathbb{Z}\right)\right| = \overbrace{(p^n-1)}^{\nu_p=0}\overbrace{(p^n-p)}^{\nu_p=1}\cdots\overbrace{(p^n-p^{n-1})}^{\nu_p=n-1}$. $\nu_p((\)\cdots(\)) = 0 + 1 + \cdots + (n-1) = \frac{n(n-1)}{2}$ Für jede p-Sylow Untergruppe H von G muss $|H| = p^{\frac{n(n-1)}{2}}$ und umgekehrt. Die Matrizen der Gestalt

$$\begin{pmatrix} 1 & * & \cdots & * \\ 0 & \ddots & \ddots & \vdots \\ \vdots & \ddots & \ddots & * \\ 0 & \cdots & 0 & 1 \end{pmatrix}$$

bilden eine Untergruppe von $\mathrm{GL}_n(\mathbb{Z}_p)$ mit Ordnung $p^{\frac{n(n-1)}{2}}$.

1.9 Einfache Gruppen

Definition 1.9.1:
G heißt einfach, falls $N \trianglelefteq G \implies N \in \{\{e\}, G\}$

Proposition 1.9.2:
Alle Gruppen G mit $|G| < 60, |G| \notin \mathbb{P}$ sind nicht einfach.

Beweis. $|G| = p^k \cdot q (p, q$ verschiedene Primzahlen) mit $q \not\equiv 1 \mod p \implies G$ nicht einfach.
$|G| = 36 = 2^2 \cdot 3^2$. Angenommen: $|\mathrm{Syl}_3(G)| > 1$ (falls $= 1$, so ist die 3-Sylow normal) dann gilt: $|\mathrm{Syl}_3(G)| = 4$. G operiert auf $\mathrm{Syl}_3(G)$ durch Konjugation. Diese Aktion induziert einen Gruppenhomomorphismus $G \to \mathcal{S}_{\mathrm{Syl}_3(G)}, g \mapsto \tau_g : S \mapsto gSg^{-1}$. Wegen $|G| = 36$ und $\left|\mathcal{S}_{\mathrm{Syl}_3(G)}\right| = 24$ ist τ nicht injektiv. Folglich gilt $\ker(\tau) \neq \{e\}$. Weiters gilt $\ker(\tau) \neq G$. Wäre $\ker(\tau) = G$, so folgte $gSg^{-1} = S \forall g \in G$ was einen Widerspruch zum 2. Sylowsatz 1.8.8 ergäbe. Somit ist $\ker(\tau)$ ein echter Normalteiler von G. □

Satz 1.9.3:
$\mathcal{A}_5$ ist einfach.

Beweis. Angenommen $\mathcal{A}_5$ habe einen Normalteiler U.

1. Fall: $5 \mid |U|$. Dann enthält U eine Untergruppe der Ordnung 5, also eine 5-Sylow Untergruppe von $\mathcal{A}_5$, zum Beispiel $\langle\sigma\rangle$, wobei σ ein 5-Zyklus ist. Nach dem 2. Sylowsatz 1.8.8 ist jede andere 5-Sylow Untergruppe zu σ konjugiert. Daher wegen $U \trianglelefteq \mathcal{A}_5$ in U enthalten, sodass U alle 5-Zyklen enthält. Davon gibt es 24. Es folgt: $|U| = 30$.

Ein analoges Vorgehen zeigt, dass auch alle 3-Zykel in U enthalten sind. Davon gibt es 20, also $U\mathcal{A}_5$

2. Fall: $3 \mid |U|$ Wir zeigen wieder, dass U alle 3-Zykel enthält. Es folgt $|U| \geq 21$, damit muss schon $|U| = 30$ gelten. Da U auch alle 5-Zykel enthält, folgt wie vorher ein Widerspruch.

Die einzigen verbleibenden Möglichkeiten für $|U|$ sind $|U| = 2$ und $|U| = 4$. Dann enthält U ein Element der Ordnung 2, also der Gestalt $(ab)(cd)$. oBdA $(12)(34) \in U$.

- $(125)(12)(34)(152) = (52)(34) \in U$ wegen $U \trianglelefteq \mathcal{A}_5$.
- $(215)(12)(34)(251) = (15)(34) \in U$ wegen $U \trianglelefteq \mathcal{A}_5$.
- $(345)(12)(34)(354) = (12)(54) \in U$ wegen $U \trianglelefteq \mathcal{A}_5$. □

Bemerkung 1.9.4:

- $|G| = p \implies G$ einfach.
- $\mathcal{A}_n, n \geq 5$ ist einfach.
- $\mathrm{SL}_2(\mathbb{Z}_7)/\{\pm I\} =: \mathrm{PSL}_2(\mathbb{Z}_7)$ hat Ordnung 168 und ist einfach.

+ insgesamt 16 Familien von Matrixgruppen, die alle einfach sind.

∃ 26 weitere Gruppen („sporadische Gruppen“) (kleinste hat Ordnung 7920, die größte $8 \cdot 10^{54}$ und wird Monstergruppe genannt.)

Kapitel 2

Ringe

2.1 Grundlagen

Definition 2.1.1:
$(R, +, \cdot)$ heißt Ring, falls

R_1: $(R, +)$ ist eine abelsche Gruppe.

R_2: $(R, \cdot)$ erfüllt: $\forall a, b, c \in R : a(bc) = (ab)c$.

R_3: $\forall a, b, c \in R : \begin{cases} a(b+c) = ab + ac \\ (a+b)c = ac + bc \end{cases}$.

Falls $(R, +, \cdot)$ zusätzlich

R_4: $\exists 1 \in R : 1 \cdot a = a \cdot 1 = a \forall a \in R$ gilt, so heißt $(R, +, \cdot)$ unitär (Ring mit 1)

R_5: $\forall a, b \in R : ab = ba$ gilt, so heißt $(R, +, \cdot)$ kommutativ.

Folgerung 2.1.2:

- $0 \cdot a = a \cdot 0 = 0 \forall a \in R$
- $(-a) \cdot b = a(-b) = -(ab) \forall a, b \in R$
- $(-a)(-b) = ab \forall a, b \in R$
- $a(b - c) = ab - ac \forall a, b, c \in R$
- $(\sum_{i=1}^{n} a_i)(\sum_{j=1}^{m} b_j) = \sum_{i=1}^{n} \sum_{j=1}^{m} a_i b_j$

Bemerkung 2.1.3:

$R = (\mathbb{Z}, +, \cdot)$ ist unitärer Ring.
$R' = (2\mathbb{Z}, +, \cdot)$ ist ein Ring, aber nicht unitär.
$\{0\}$ ist ein Ring, sogar ein unitärer Ring!

Beispiel 2.1.4:

- $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$
- $\left(\mathbb{Z}/n\mathbb{Z}, +, \cdot\right)$ ist Ring wenn man $(a + n\mathbb{Z})(b + n\mathbb{Z}) \coloneqq ab + n\mathbb{Z}$
- $M_{n\times n}(\mathbb{K})$ ist nicht kommutativer, unitärer Ring (bezüglich Matrizenmultiplikation).
- Ist G abelsche Gruppe, so ist

$$\mathrm{End}(G) = \{\varphi : (G, +) \to (G, +), \varphi \text{ Gruppenhomomorphismus}\}$$

ein Ring bezüglich

$$(\varphi + \psi)(g) \coloneqq \varphi(g) + \psi(g)$$
$$(\varphi \cdot \psi)(g) \coloneqq \varphi(\psi(g))$$

und heißt Endomorphismenring von G. $\mathrm{End}((\mathbb{Z}, +)) \cong (\mathbb{Z}, +, \cdot)$.

Weitere Begriffe: (in unitären Ringen)

Definition 2.1.5:

Sei $a \in R$. Falls $\exists b \in R$ mit $ab = 1$, so heißt b Rechtsinverses von a. Falls $ba = 1$, so heißt b Linksinverses von a.

Falls a ein Rechtsinverses b_1 und ein Linksinverses b_2 besitzt und diese übereinstimmen, so heißt $b \coloneqq b_1 = b_2$ Inverses von a.

Man sagt a ist eine Einheit in R. R^* bezeichnet die Menge aller Einheiten von R.

Also ist $\mathbb{R}^* = \mathbb{R} \setminus \{0\}$

Definition 2.1.6:

Gilt in einem Ring R: $R^* = R \setminus \{\overset{\text{neutrales Element bezüglich } +}{\overset{|}{0}}\}$, so heißt R Schiefkörper.

Analog zu Rechts- und Linksinversen definieren wir Rechts- und Linksnullteiler durch: falls $\exists b \in R \setminus \{0\}$ mit $ab = 0$ (bzw. $ba = 0$), so heißt a Rechts-/Linksnullteiler. Falls beides zutrifft, so heißt a Nullteiler.

Für $a, x, y \in R, a$ <u>kein</u> Nullteiler gilt:

$$ax = ay \implies x = y \wedge xa = ya \implies x = y$$
$$\Updownarrow$$
$$ax - ay = 0 \iff a(x - y) = 0$$

da a kein Nullteiler folgt $x - y = 0$.

Definition 2.1.7:

Ein kommutativer Ring mit Eins, in dem $1 \neq 0$ und der keine Nullteiler besitzt, heißt Integritätsbereich.

Beispiel 2.1.8:

- $\left(\mathbb{Z}/6\mathbb{Z}\right)^* = \{1 + 6\mathbb{Z}, 5 + 6\mathbb{Z}\}$.
  $\left(\mathbb{Z}/p\mathbb{Z}\right)^* = \{1 + p\mathbb{Z}, \ldots, p - 1 + p\mathbb{Z}\} = \mathbb{Z}/p\mathbb{Z} \setminus \{0 + p\mathbb{Z}\}$
  $(R^*, \cdot)$ bilden eine Gruppe für jeden kommutativen Ring R mit 1.
  Weil $\mathbb{Z}/p\mathbb{Z}$ Körper, folgt: $\left(\mathbb{Z}/p\mathbb{Z}\right)^*$ ist zyklisch, daher $\cong \mathbb{Z}/(p-1)\mathbb{Z}$
- $\left(\mathbb{Z}/15\mathbb{Z}\right)^* = \{\overline{1}, \overline{2}, \overline{4}, \overline{7}, \overline{8}, \overline{11}, \overline{13}, \overline{14}\}$ ist nicht zyklisch (nachrechnen).
- $M_{n\times n}(R)^* = \{A \in M_{n\times n}(R) : \det(A) \in R^*\}$

2.2 Teilringe & Homomorphismen

Definition 2.2.1:

Sei $(U, +)$ eine additive Untergruppe von $(R, +)$. Falls U bezüglich $\cdot$ abgeschlossen ist, das heißt $\forall a, b \in U$ gilt $ab \in U$, so heißt $(U, +, \cdot)$ Teilring von $(R, +, \cdot)$. Falls

$(R, +, \cdot)$ ein Ring mit 1 ist, so muss zusätzlich $1 \in U$ gelten. Wir schreiben dann $(U, +, \cdot) \leq (R, +, \cdot)$.

Bemerkung 2.2.2:

R unitär und $(U, +)$ bezüglich $\cdot$ abgeschlossen impliziert nicht notwendig U unitär (siehe $R = \mathbb{Z}, U = n\mathbb{Z}$).

$$Z(R) \coloneqq \{a \in R : ab = ba \forall b \in R\}$$

ist Teilring von R.

Beispiel 2.2.3:

$M_{n\times n}(U) \leq M_{n\times n}(R)$ falls $U \leq R$.

Definition 2.2.4:

$\varphi : (R, +, \cdot) \to (S, \oplus, \odot)$ heißt Ringhomomorphismus, falls $\forall r, s \in R$

1. $\varphi(r + s) = \varphi(r) \oplus \varphi(s)$
2. $\varphi(r \cdot s) = \varphi(r) \odot \varphi(s)$
3. $\varphi(1_R) = 1_S$ falls R, S Ringe mit 1 sind.

Achtung: $\varphi(r) = 0 \forall r \in R$ definiert einen Ringhomomorphismus, aber keinen Ringhomomorphismus von Ringen mit 1.

Analog zu Gruppenhomomorphismen definiert man: Mono-, Epi- und Isomorphismus. Ist $\varphi : R \to S$ ein Ringisomorphismus, so ist $\varphi^{-1} : S \to R$ auch einer. (Übungsaufgabe 42)

Man zeigt analog: $\varphi : R \to S$ Ringhomomorphismus $\implies$

1. $\varphi^{-1}(\{0_S\}) \coloneqq \ker(\varphi) \leq R$
2. $\varphi(R) \coloneqq \mathrm{im}(\varphi) \leq S$
3. $\varphi(0_R) = (0_S)$

Beweise sind jeweils Einzeiler.

Sei R ein Ring mit 1. $\chi\colon \mathbb{Z} \to R$,
$n \mapsto \underbrace{1_R + \cdots + 1_R}_{n \text{ mal}} =: n \cdot 1_R$ ist der einzige Ringhomomorphismus. Es ist $\ker(\chi) = \{0\}$ oder $d\mathbb{Z}$ für ein $d \in \mathbb{N} \setminus \{1\}$. Dieses d heißt die Charakteristik ($\text{char}(R)$) von R. $\text{char}(R) = 0 \iff \chi$ injektiv. Falls $\text{char}(R) \neq 0$ so ist $\text{char}(R) = d$ die kleinste natürliche Zahl für die $d \cdot 1_r = 0$. Wegen $\text{im}(\chi) \leq R$ folgt, dass jeder Ring einen Teilring $\mathbb{P}(R)$, den Primring von R enthält, der isomorph zu $\mathbb{Z}$ bzw. $\mathbb{Z}/d\mathbb{Z}$ ist.

Für Integritätsbereiche R gilt sogar: $\text{char}(R) = 0$ oder $\text{char}(R) = p$, prim (Übung 46). Falls R ein Integritätsbereich mit $\text{char}(R) = p$, dann gilt:

$$\begin{matrix} x^p + y^p = (x+y)^p \\ x^p y^p = (xy)^p \end{matrix} \forall x, y \in R$$

sodass: $\text{Frob}_p\colon R \to R$,
$x \mapsto x^p$ ein Ringhomomorphismus ist, der sogenannte Frobeniushomomorphismus.

2.3 Ideale & Quotientenringe

Definition 2.3.1:

Sei $0 \neq I \leq R$ sei eine additive Untergruppe. Dann heißt I

Linksideal , falls $RI \subseteq I$

Rechtsideal , falls $IR \subseteq I$

Schreibe $I \lhd R$, falls I Rechts- und Linksideal ist.

Folgerung 2.3.2:

- $I \lhd R \implies I$ ist bezüglich $\cdot$ abgeschlossen.
- $\{0\}$ und R sind Ideale von R.
- Falls $1_R \in I$, so folgt $I = R$.

Beispiel 2.3.3:

- $R = \mathbb{Z}, I = n\mathbb{Z}$ für ein beliebiges $n \in \mathbb{N}$
- in $M_{n\times n}(R)$ ist $M^{(i)}_{n\times n}(R) := \left\{ \begin{pmatrix} 0 & \cdots & 0 & * & 0 & \cdots & 0 \\ \vdots & & \vdots & \vdots & \vdots & & \\ 0 & \cdots & 0 & * & 0 & \cdots & 0 \end{pmatrix}, * \in R \right\}$ ein Linksideal, aber kein Rechtsideal.

In Übungsaufgabe 50: $R = \mathbb{R}.M_{n\times n}(\mathbb{R})$ besitzt keine echten Ideale.

Sei $T \subseteq R$ eine beliebige Teilmenge, R ein Ring mit 1. Dann ist $(T) \coloneqq \bigcap_{\substack{I \lhd R \\ T \subseteq I}} I$ das kleinste Ideal von R, das T enthält, das von T erzeugte Ideal. In Übungsaufgabe 48 wird gezeigt, dass der Durchschnitt beliebig vieler Ideale stets wieder ein Ideal ist. Im Fall $T = \{a_1, \dots, a_s\}$ schreiben wir $(a_1, \dots, a_s)$, im Fall $T = \{a\}$ so heißt (a) das von a erzeugte Hauptideal.

Für jedes $a \in R$ ist $Ra = \{ra : r \in R\}$ ein Linksideal und aR ein Rechtsideal von R. $(a) = \{x_1 + \dots + x_n : n \in N, x_i \in RaR \text{ für } i = 1, \dots, n\}$. Falls R kommutativ ist, so gilt $(a) = aR = Ra$ und allgemeiner $(T) = \{\sum_{\text{endlich}} r_i a_i : r_i \in R, a_i \in T\}$.

Wir betrachten in diesem Abschnitt nur mehr Ringe mit 1

Lemma 2.3.4:
Sei $\phi\colon R \to S$ ein Ringhomomorphismus. Dann ist $\ker(\phi) \lhd R$.

Beweis. Wir wissen bereits $\ker(\phi) \leq (R, +)$. Für $r \in R, s \in \ker(\phi)$ gilt:

$$\phi(rs) = \phi(r)\underbrace{\phi(s)}_{=0} = 0, \text{ das heißt } rs \in \ker(\phi),$$
$$\phi(sr) = \underbrace{\phi(s)}_{=0}\phi(r) = 0, \text{ das heißt } sr \in \ker(\phi).$$

□

Lemma 2.3.5:
Sei $\phi\colon R \to S$ ein Ringhomomorphismus, $I \lhd R, J \lhd S$. Dann ist $\phi^{-1}(J) \lhd R$. Falls zusätzlich ϕ surjektiv ist, gilt auch $\phi(I) \lhd S$.

Beweis. Übungsaufgabe 48 □

Beispiel 2.3.6:
$\phi\colon \mathbb{Z} \to \mathbb{Q}, z \mapsto z$. $m\mathbb{Z} \lhd \mathbb{Z}, \phi(m\mathbb{Z})$ ist aber kein Ideal in $\mathbb{Q}$.

Für $I \lhd R$ ist I insbesondere Normalteiler von $(R, +)$, da R bezüglich $+$ kommutativ ist. ${}^{(R,+)}\!/_{(I,+)}$ ist also eine abelsche Gruppe. Wir definieren nun eine Ringstruktur auf ${}^{R}\!/_{I}$.

Satz 2.3.7:
Sei $I \triangleleft R$. Dann ist R/I mit den Verknüpfungen $\begin{matrix}(a+I)+(b+I) \coloneqq a+b+I \\ (a+I)\cdot(b+I) \coloneqq ab+I\end{matrix}$ ein Ring und $\phi\colon R \to R/I, r \mapsto r+I$ ein Ringepimorphismus.

Beweis. Bezüglich $+$ ist die Aussage bereits in der Gruppentheorie gezeigt. R_1✓
$\cdot$ ist wohldefiniert: seien $a', b' \in R$ mit $a' = a+x, b' = b+y$ mit $x, y \in I$.

$$(a'+I)(b'+I) = (a+x+I)(b+y+I) = ab + \underbrace{ay}_{\in I} + \underbrace{xb}_{\in I} + \underbrace{xy}_{\in I} + I = ab+I$$

R_2, R_3 gelten in R/I, da sie in R gelten.
ϕ ist Homomorphismus, da $+, \cdot$ so definiert sind, dass Homomorphie gilt. Einselement von R/I ist $1+I$. □

Satz 2.3.8 (Homomorphiesatz für Ringe):
Sei $I \triangleleft R$. Dann ist R/I homomorphes Bild von R. Der Kern eines Ringhomomorphismus $\phi\colon R \to S$ ist ein Ideal in R und es gilt:

$$R/\ker(\phi) \cong \phi(R).$$

Beweis. Die Abbildung $R/\ker(\phi) \to \phi(R), r \mapsto r+\ker(\phi)$ ist wohldefiniert und wegen $r+\ker(\phi) = s+\ker(\phi) \iff r-s \in \ker(\phi) \iff \phi(r) = \phi(s)$ auch injektiv, surjektiv nach Konstruktion. □

Definition 2.3.9:
Seien I, J Ideale von R.

$$\begin{aligned} I \cap J &\coloneqq \{x \in R | x \in I \wedge x \in J\} \triangleleft R \\ I + J &\coloneqq \{x+y | x \in I, y \in J\} \triangleleft R \\ IJ &\coloneqq \left\{\sum_{i=1}^{n} x_i y_i | x_i \in I, y_i \in J, n \in \mathbb{N}\right\} \end{aligned}$$

Bemerkung 2.3.10:

$I \cap J, I + J$ und IJ sind Ideale in R.

$$R(I+J) = \underbrace{RI}_{\subseteq I} + \underbrace{RJ}_{\subseteq J} \subseteq I + J$$

und analog $(I+J)R$. Für $r \in R$ gilt

$$r \sum_{i=1}^{n} x_i y_i = \sum_{i=1}^{n} \underbrace{(rx_i)}_{\in I} y_i = \sum_{i=1}^{n} x_i' y_i$$

$$\left(\sum_{i=1}^{n} x_i y_i \right) r = \sum_{i=1}^{n} x_i \underbrace{y_i r}_{\in J} = \sum_{i=1}^{n} x_i y_i'$$

Weiters:

- $I + J = (I \cup J)$
- $IJ \subseteq I \cap J$.

Satz 2.3.11 (1. Isomorphiesatz):

Sei R ein Ring, $I \triangleleft R, T \leq R$. Dann ist $T + I$ ein Teilring von R, $T \cap I$ ein Ideal von T und es gilt:

$$T + I \big/ I \cong T \big/ T \cap I.$$

Beweis. in dem Proseminar □

Satz 2.3.12 (2. Isomorphiesatz):

Sei R ein Ring, $I, J \triangleleft R$ mit $I \subseteq J$. Dann ist $J \big/ I$ ein Ideal von $R \big/ I$ und es gilt

$$R \big/ I \big/ J \big/ I \cong R \big/ J.$$

Beweis. Sei $\phi\colon R \big/ I \to R \big/ J, r + I \mapsto r + J$. ϕ ist wohldefiniert: $r + I = r' + I \iff r - r' \in I \implies r - r' \in J \implies r + J = r' + J$

ϕ ist Homomorphismus:

$+$ wurde schon in Theorem 1.4.21 gezeigt

· $\phi((r+I)(s+I)) = \phi(rs+I) = rs+J = (r+J)(s+J) = \phi(r+I)\phi(s+I)$

und surjektiv. $\ker(\phi) = \{r+I \in {}^{R}\!/_{I} : \phi(r+I) = J\} = \{r+I \in {}^{R}\!/_{I} : r \in J\} = {}^{J}\!/_{I}$.
Mithilfe des Homomorphiesatzes 2.3.8 folgt die Behauptung. □

Beispiel 2.3.13:

Für $d \mid n$ gilt $n\mathbb{Z} \leq d\mathbb{Z}$, beides Ideale in $\mathbb{Z}$. Aus dem 2. Isomorphiesatz 2.3.12 folgt somit: ${}^{\mathbb{Z}}\!/_{n\mathbb{Z}}/{}^{d\mathbb{Z}}\!/_{n\mathbb{Z}} \underset{\text{als Ringe!}}{\cong} {}^{\mathbb{Z}}\!/_{d\mathbb{Z}}$.

ACHTUNG: Gruppentheorie: es gilt sogar ${}^{d\mathbb{Z}}\!/_{n\mathbb{Z}} \underset{\text{als Gruppe}}{\cong} {}^{\mathbb{Z}}\!/_{\frac{n}{d}\mathbb{Z}}$, aber <u>nicht</u> als Ringisomorphismus.

$$\begin{array}{ccc} (dk+n\mathbb{Z})(dk'+n\mathbb{Z}) & = & d(dkk')+n\mathbb{Z} \\ \downarrow & & \downarrow \\ (k+\frac{n}{d}\mathbb{Z})(k'+\frac{n}{d}\mathbb{Z}) & \neq & dkk'+\frac{n}{d}\mathbb{Z} \end{array}$$

2.4 Produkte & Algebren

Definition 2.4.1:

Seien $(R, \boxplus, \boxdot)$ und $(S, \oplus, \odot)$ Ringe. Dann ist $R \times S$ mit den Verknüpfungen

$$\begin{aligned} + &: (r,s)+(r',s') = (r \boxplus r', s \oplus s') \\ \cdot &: (r,s)\cdot(r',s') = (r \boxdot r', s \odot s') \end{aligned}$$

ein Ring, das sogenannte direkte Produkt $R \times S$ von R und S.

- Sind R, S Ringe mit 1, so ist auch $R \times S$ einer, $1_{R\times S} = (1_R, 1_S)$.
- $R \times S$ ist kommutativ $\iff$ R & S kommutativ.
- $(R \times S)^* = R^* \times S^*$
- R, S Integritätsbereich $\overset{\text{i.A.}}{\not\Longrightarrow}$ $R \times S$ Integritätsbereich.

$$(r, 0_S)(0_R, s) = (0_R, 0_S) = 0_{R\times S}$$

- Für beliebige Indexmenge I bezeichnet $\prod_{i\in I} R_i = \{(r_i)_{i\in I} : r_i \in R_i\}$ das direkte Produkt der R_i.

$$\bigoplus_{i\in I} R_i := \{(r_i)_{i\in I} \colon r_i \in R_i, r_i = 0 \text{ für alle bis auf endlich viele } i\}$$

heißt direkte Summe der R_i.

Proposition 2.4.2:

$$I \triangleleft R \times S \iff I = I_R \times I_S \text{ mit } I_R \triangleleft R, I_S \triangleleft S$$

Beweis. im Proseminar □

Definition 2.4.3:

Ein Ring $(A, +, \cdot)$ heißt Algebra über dem Körper $\mathbb{K}$, falls eine Skalarmultiplikation $\bullet \colon \mathbb{K} \times A \to A$ existiert, sodass $(A, +, \bullet)$ ein $\mathbb{K}$-Vektorraum ist und

$$\forall x, y \in A, \lambda \in \mathbb{K} \colon \lambda \bullet (xy) = (\lambda \bullet x)y = x(\lambda \bullet y).$$

Beispiel 2.4.4:

1. $M_{n\times n}(\mathbb{K})$ und allgemeiner $\mathrm{End}(V)$, wobei V ein $\mathbb{K}$-Vektorraum.
2. $\mathbb{K}[x]$
3. $\mathrm{Abb}(\mathrm{M} \to \mathbb{K})$

Analog zu Ringen: kommutative/unitäre Algebren. ϕ Algebrahomomorphismus $\iff$ ϕ Ringhomomorphismus und $\phi(\lambda x) = \lambda\phi(x) \forall \lambda \in \mathbb{K}, x \in A$.

Definition 2.4.5:

Ein Ring/Algebra heißt einfach, wenn er/sie keine nicht-trivialen Ideale besitzt und nicht degeneriert ist (das heißt es gilt nicht $x \cdot y = 0 \forall x, y, \in R/A$).

Beispiel 2.4.6:

Sei R ein kommutativer Ring.

$$R \text{ einfach} \iff R \text{ ist Körper.}$$

$\Longleftarrow$ **:** Sei R Körper, $I \triangleleft R$ mit $I \neq (0)$.$\exists a \neq 0$ in I. R Körper $\implies \exists a^{-1} \in R \underbrace{a^{-1}}_{\in R} \underbrace{a}_{\in I} \in I$, das heißt $1 \in I \implies I = R$.

$\Longrightarrow$ **:** Sei $a \in R$.$(a) = 0 \vee (a) = R \implies \exists r \in R$ mit $ra = 1$, also $r = a^{-1}$, das heißt $a \in R^* \implies R$ ist Körper.

Beispiel 2.4.7:

$M_{n\times n}(\mathbb{K})$ ist keine einfache Algebra, $\mathbb{R}$, $\mathbb{C}$ sind einfache Algebren.

Definition 2.4.8:

Eine endlichdimensionale, einfache Algebra A über $\mathbb{K}$, für die $Z(A) = \mathbb{K} \cdot 1_A$, heißt zentral-einfach.

$\mathbb{R}$ ist eine zentral-einfache Algebra über $\mathbb{R}$, $\mathbb{C}$ ebenso, aber $\mathbb{C}$ ist nicht zentral-einfach über $\mathbb{R}$.

2.5 Kommutative Ringe und Integritätsbereiche

In diesem Abschnitt bezeichnet R stets einen kommutativen Ring mit Eins.

Definition 2.5.1:

$\mathcal{P} \triangleleft R$ heißt Primideal, falls $\mathcal{P} \neq R$ und

$$\forall r, s \in R\colon rs \in \mathcal{P} \implies r \in \mathcal{P} \vee s \in \mathcal{P}$$

Beispiel 2.5.2:

$R = \mathbb{Z}$: (m) ist prim $\iff m \in \mathbb{P} \vee m = 0$.

Satz 2.5.3:
$I \triangleleft R$ ist Primideal $\iff$ ${}^{R}\!/_{I}$ ist Integritätsbereich.

Beweis.

$$\begin{aligned} {}^{R}\!/_{I} \text{ ist Integritätsbereich} &\iff {}^{R}\!/_{I} \neq \{0\} \wedge \Big((r+I)(s+I) = 0+I \\ &\qquad \implies r+I = 0+I \vee s+I = 0+I \Big) \\ &\iff R \neq I \wedge (rs \in I \implies r \in I \vee s \in I) \\ &\iff I \text{ ist Primideal.} \end{aligned}$$

□

Proposition 2.5.4:
Ist $\phi\colon R \to S$ ein Ringhomomorphismus, $J \triangleleft S$ ein Primideal, dann ist $\phi^{-1}(J) \triangleleft R$ auch ein Primideal.

Beweis. Sei $I \coloneqq \phi^{-1}(J)$.

$$rs \in I \implies \phi(rs) = \phi(r)\phi(s) \in J$$

Weil $J \triangleleft S$ Primideal ist, gilt $\phi(r) \in J \vee \phi(s) \in J$ und somit $r \in I \vee s \in I$. □

Definition 2.5.5:
$m \triangleleft R$ heißt maximales Ideal, falls $m \neq R$ und $m \subseteq I \triangleleft R \implies m = I \vee I = R$.

Beispiel 2.5.6:
$R = \mathbb{Z}.(m)$ ist maximal $\iff m \in \mathbb{P}$. $\{0\}$ ist in $\mathbb{Z}$ kein maximales Ideal und $\{0\}$ ist maximal genau dann, wenn R einfach ist, das heißt wenn R ein Körper ist.

Satz 2.5.7:
$I \triangleleft R$ ist maximal $\iff$ ${}^{R}\!/_{I}$ ist ein Körper.

Beweis. $\Longrightarrow$**:** Sei $I \triangleleft R$ maximal. Dann gilt $I \neq R$ und somit ${}^{R}\!/_{I} \neq \{0\}$. Für $a + I \neq I$ betrachten wir das von I und a erzeugte Ideal $J := \{x + ay | x \in I, y \in R\}$. Dann gilt $J \supsetneq I$ und wegen I maximal folgt $J = R$. $\Longrightarrow \exists \alpha \in I : \alpha + ay = 1$. Das heißt $\alpha + ay + I = 1 + I$ in ${}^{R}\!/_{I}$ und wegen $\alpha \in I$: $(a + I)(y + I) = ay + I = 1 + I$, sodass $a + I \in \left({}^{R}\!/_{I}\right)^{*}$

$\Longleftarrow$**:** Sei ${}^{R}\!/_{I}$ ein Körper. Sei $I \subsetneq J \subseteq R$. Sei $a \in J \setminus I$, dann ist $a + I \neq 0 + I$ und $\exists b \in R$ mit $\underbrace{(a + I)(b + I)}_{ab+I} = 1 + I$. $1 - ab \in I \subset J$. Wegen $a \in J$ ist auch $ab \in J$ und somit $(1 - ab) + ab = 1 \in J \implies J = R$. □

Proposition 2.5.8:

$\phi : R \to S$ Ringhomomorphismus, $J \triangleleft S$ maximal. Falls ϕ surjektiv ist, so folgt $\phi^{-1}(J) \triangleleft R$ maximal.

Beweis. Sei $I \triangleleft R$ mit $\phi^{-1}(J) \subseteq I$. Dann gilt $\ker(\phi) \subseteq I$. Da ϕ surjektiv ist, ist $\phi(I) \triangleleft S$ das J enthält. Wegen J maximal folgt $\phi(I) = J \vee \phi(I) = S$. Es folgt: $\phi^{-1}(\phi(I)) = I$ wegen $\ker(\phi) \subseteq I$. Es folgt also $I = \phi^{-1}(J) \vee I = \phi^{-1}(S) = R$, das heißt $\phi^{-1}(J)$ ist maximal. □

Beispiel 2.5.9:

Die Surjektivität von ϕ ist wesentlich! $R = \mathbb{Z}, S = \mathbb{Q}, \phi : \mathbb{Z} \hookrightarrow \mathbb{Q}$. $\{0\}$ ist maximal in $\mathbb{Q}$, aber $\phi^{-1}(\{0\}) = \{0\}$ ist nicht maximal in $\mathbb{Z}$.

Wiederholung:

Lemma 2.5.10 (Zorn):

Sei $(M, \leq)$ eine nichtleere, partiell geordnete Menge. Besitzt jede totalgeordnete Teilmenge von M eine obere Schranke in M, so besitzt M ein maximales Element. ($m \in M$ heißt maximal, falls $\forall x \in M : m \leq x \implies m = x$)

Satz 2.5.11:

Sei R ein kommutativer Ring mit Eins, $R \neq \{0\}$. Dann enthält R ein maximales Ideal.

Beweis. Sei Σ die Menge aller Ideale $\neq R$ von R. Σ ist bezüglich $\subseteq$ partiell geordnet und $\Sigma \neq \emptyset$ wegen $\{0\} \in \Sigma$. Ist $T \subseteq \Sigma$ eine totalgeordnete Teilmenge, so ist $\bigcup_{I \in T} I$ eine obere Schranke, die in Σ liegt. Es gilt nämlich $\forall x, y \in \bigcup_{I \in T} I \colon x \in I_1, y \in I_2$, oBdA: $I_1 \subseteq I_2 \implies x + y \in I_2 \to x + y \in \bigcup_{I \in T} I$. Analog bezüglich $\cdot$ und die Absorptionseigenschaft $rx \in \bigcup_{I \in T} I$ für $r \in R$ folgt ebenso.

Überdies gilt: $\bigcup_{I \in T} I \neq R$, da $\forall I \in T \colon 1 \notin I$ und daher auch $1 \notin \bigcup_{I \in T} I$. Nach dem Lemma von Zorn 2.5.10 enthält Σ ein bezüglich $\subseteq$ maximales Element, dieses ist ein maximales Ideal von R. □

Lemma 2.5.12:
Sei $I \triangleleft R$, R/I der Quotientenring. Dann entsprechen die Ideale $\bar{J}$ von R/I bijektiv den Idealen J von R, welche I enthalten.

Beweis. Sei $\Pi \colon R \to R/I$ der kanonische Epimorphismus. Sei $\bar{J} \triangleleft R/I$. Dann ist $\Pi^{-1}\left(\bar{J}\right) =: J \triangleleft R$ und $\Pi^{-1}\left(\bar{J}\right) \supseteq \Pi^{-1}\left(0_{R/I}\right) = \ker(\Pi) = I$.

Umgekehrt, sei $J \triangleleft R$ mit $J \supseteq I$. $\bar{J} := \Pi(J) \triangleleft R/I$, da Π surjektiv ist. Es gilt:

$$\Pi^{-1}(\Pi(J)) = J \text{ wegen } \ker(\Pi) = I \subseteq J.$$
$$\Pi(\Pi^{-1}(\bar{J})) = \bar{J} \text{ wegen } \Pi \text{ surjektiv.}$$
□

Korollar 2.5.13:
Sei $I \triangleleft R$ ein echtes Ideal. Dann existiert ein maximales Ideal m von R, das I enthält.

Beweis. Anwendung von Theorem 2.5.11 auf R/I liefert ein maximales Ideal $\bar{m}$ in R/I. Dieses Ideal entspricht eindeutig einem Ideal m von R, das I enthält. Da die Bijektion von $\phi \colon R \to R/I, r \mapsto r + I$ induziert wird, ist sie inklusionserhaltend. $\implies$ $m \triangleleft R$ ist maximal. □

Korollar 2.5.14:
Sei R ein kommutativer Ring mit Eins, $I \triangleleft R$ maximal $\implies$ $I \triangleleft R$ prim.

Beweis. I maximal $\iff$ R/I ist Körper $\implies$ R/I ist Integritätsbereich $\iff$ I ist prim. □

Proposition 2.5.15:
Sei R ein endlicher Integritätsbereich. Dann ist R ein Körper.

Beweis. Sei $f_a \colon R \to R, r \mapsto ar$. f_a für ein $a \in R$. f_a ist injektiv, denn $ar_1 = ar_2 \iff ar_1 - ar_2 = a(r_1 - r_2) = 0 \implies r_1 = r_2 \underset{|R|<\infty}{\implies} f_a$ ist surjektiv $\implies \exists r \in R$ mit $\underbrace{f_a(r)}_{ar} = 1 \square$

Korollar 2.5.16:
Ist $\left|{}^{R}\!/_{I}\right| < \infty$, so ist I genau dann maximal, wenn es prim ist.

$R = \mathbb{Z}$. (m) ist prim $\iff m = p \in \mathbb{P} \vee m = 0$.
$\left|{}^{\mathbb{Z}}\!/_{m\mathbb{Z}}\right| < \infty \implies (m)$ ist genau dann maximal, wenn $m \in \mathbb{P}$.
(0) ist nicht maximal.

Definition 2.5.17:
Für zwei Ideale $I, J \triangleleft R$ schreiben wir $I \mid J :\iff J \subseteq I$.

Achtung, I und J sind hier „umgedreht“. Für $6\mathbb{Z} \subseteq 2\mathbb{Z} \wedge 2 \mid 6$ erscheint diese Definition natürlich.

Definition 2.5.18:
I, J heißen teilerfremd, falls $I + J = R$

Bemerkung 2.5.19:
Falls $I + J = R$, so folgt $IJ = I \cap J$ ($IJ \subseteq I \cap J$ gilt immer!).
Sei nämlich $x \in I \cap J$ und $r, s \in R, r \in I, s \in J$ mit $r + s = 1$.

$$x = x \cdot 1 = x(r+s) = \underbrace{x}_{\in J}\underbrace{r}_{\in I} + \underbrace{x}_{\in I}\underbrace{s}_{\in J} \in IJ$$

Beispiel 2.5.20:
$R = \mathbb{Z}, (m), (n) \triangleleft \mathbb{Z}. m\mathbb{Z} + n\mathbb{Z} = d\mathbb{Z}$ mit $d \mid m \wedge d \mid n$ und $h \mid m \wedge h \mid n \implies h \mid d$, das heißt $d = \mathrm{ggT}(m, n)$.

Definition 2.5.21:
Für $I \triangleleft R$ schreiben wir

$$r \equiv s \pmod{I} :\iff r - s \in I (r, s \in R).$$

$\equiv_I$ definiert eine Äquivalenzrelation auf R, die mit $+, \cdot$ verträglich ist, also

$$\begin{cases} r \equiv s \pmod{I} \\ r' \equiv s' \pmod{I} \end{cases} \implies \begin{cases} r + r' \equiv s + s' \pmod{I} \\ r \cdot r' \equiv s \cdot s' \pmod{I} \end{cases}$$

, also eine Kongruenzrelation.

Satz 2.5.22 (Chinesischer Restsatz):
Sei R ein kommutativer Ring mit Eins, $x_1, \ldots, x_n \in R, I_1, \ldots, I_n \triangleleft R$ mit $\forall i \neq j \colon I_i + I_j = R$. Dann existiert ein $x \in R$ mit $x \equiv x_i \pmod{I_i}$ für $i = 1, \ldots, n$.

Beweis. Halte zunächst $i \in \{1, \ldots, n\}$ fest. Dann ist laut Voraussetzung: $I_i + I_j = R (j \neq i)$

$$\begin{aligned} &\implies \exists a_{i_j} \in I_i, b_j \in I_j \text{ mit } a_{i_j} + b_j = 1 \\ &\implies 1 = \prod_{j \neq i} (a_{i_j} + b_j) \in I_i + \prod_{j \neq i} I_j \end{aligned}$$

Dies liefert eine Darstellung $1 = y_i + z_i (1 \leq i \leq n)$ mit $y_i \in I_i$ und $z_i \in \prod_{i \neq j} I_j$. Dies bedeutet:

$$\begin{aligned} &z_i \equiv 1 \pmod{I_i} \\ &z_i \equiv 0 \pmod{I_j} \text{ für } i \neq j \left(\text{denn } \prod_{j \neq i} I_j \subseteq I_j \right) \end{aligned}$$

$$x \coloneqq x_1 \underbrace{z_1}_{\equiv 0 \pmod{I_i}} + \cdots + \underbrace{x_i \underbrace{z_i}_{\equiv 1 \pmod{I_i}}}_{\equiv x_i \pmod{I_i}} + \cdots x_n \underbrace{z_n}_{\equiv 0 \pmod{I_i}} \text{ erfüllt } x \equiv x_i \pmod{I_i} \qquad \square$$

Korollar 2.5.23:
Seien $I_1, \dots, I_n$ paarweise teilerfremde Ideale von R. Dann gilt:

$$R/I_1 \cap \dots \cap I_n \cong R/I_1 \times \dots \times R/I_n$$

Beweis. Sei

$$\phi\colon R \to R/I_1 \times \dots \times R/I_n, x \mapsto (x \pmod{I_1}, \dots, x \pmod{I_n}).$$

ϕ ist Ringhomomorphismus, da $\equiv_{I_i}$ eine Kongruenzrelation ist. Nach dem Chinesischen Restsatz 2.5.22 ist ϕ surjektiv.

$$\ker(\phi) = \{x \in R | x \equiv 0 \pmod{I_i}, i = 1, \dots, n\} = I_1 \cap \dots \cap I_n$$

Homomorphiesatz liefert die Behauptung. □

Beispiel 2.5.24 (Anwendung in $\mathbb{Z}$.):

- $N = p_1^{\alpha_1} \cdots p_k^{\alpha_k} \implies \mathbb{Z}/n\mathbb{Z} \cong \mathbb{Z}/p_1^{\alpha_1}\mathbb{Z} \times \dots \times \mathbb{Z}/p_k^{\alpha_k}\mathbb{Z}$ als Ringe!
- Sind $m, n \in \mathbb{Z}$ mit $\mathrm{ggT}(m, n) = 1$, so gilt:

$$\left(\mathbb{Z}/mn\mathbb{Z}\right)^* \cong \left(\mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}\right)^* = \left(\mathbb{Z}/m\mathbb{Z}\right)^* \times \left(\mathbb{Z}/n\mathbb{Z}\right)^*$$

$$\begin{aligned}\left|\left(\mathbb{Z}/mn\mathbb{Z}\right)\right| &= |\{r \in \{1, \dots, mn-1\} \colon (r, mn) = 1\}| \\ &= |\{r \in \{1, \dots, m-1\} \colon (r, m) = 1\}| \cdot |r \in \{1, \dots, n-1\} \colon (r, n) = 1\}|\end{aligned}$$

Für Integritätsbereiche R kann man stets eine Einbettung in einen Körper (Quotientenkörper von R) vornehmen, analog zur Einbettung von $\mathbb{Z}$ in $\mathbb{Q}$. Auf $(R \times R^*)$ wird eine Äquivalenzrelation definiert durch

$$(r, s) \sim (r', s') :\iff rs' - r's = 0$$

Auf $R \times R^*/\sim$ ist eine Körperstruktur durch

$$\begin{aligned}(a, b) + (c, d) &:= (ad + bc, bd) \\ (a, b) \cdot (c, d) &:= (ac, bd)\end{aligned}$$

$(0, r)$ ist neutrales Element bezüglich $+$, (r, r) ist Einselement. $(a, b)^{-1} = (b, a)$ für $a, b \in R^*$.

Ist R ein kommutativer Ring mit Eins, $S \subseteq R$ eine multiplikativ abgeschlossene Teilmenge (das heißt $1 \in S \wedge (a, b \in S \implies ab \in S)$), so ist auf $R \times S$ eine Äquivalenzrelation definiert durch:

$$(r, s) \sim (r', s') :\Longleftrightarrow \exists u \in S \text{ mit } (rs' - sr') \cdot u = 0$$

Reflexivität und Symmetrie sind klar, Transitivität: $(r', s') \sim (r'', s'')$ d.h. $\exists u' \in S$: $(r's'' - s'r'')u' = 0$ Es ist dann $(rs'' - sr'')s'uu' = 0$, denn

$$\underbrace{rs'u(u's'')} - \underbrace{r''s'u'(us)}$$

$$= -r'su(u's'') + r's''u'(us) = 0$$

$(r, s) \to \frac{r}{s}$. Die Menge aller Äquivalenzklassen $\frac{r}{s}$ bezeichnet man mit $S^{-1}R$. Auf $S^{-1}R$ definiere $\frac{a}{s} + \frac{b}{t} \coloneqq \frac{at+bs}{st}$, $\frac{a}{s} \cdot \frac{b}{t} \coloneqq \frac{ab}{st}$. Wohldefiniertheit überprüfen!

$(S^{-1}R, +, \cdot)$ wird zu einem kommutativen Ring mit Eins und heißt Lokalisierung von R nach S. Neutrales Element: $\frac{0}{1}$, Eins: $\frac{1}{1}$

$$\varphi_S \colon R \to S^{-1}R, r \mapsto \frac{r}{1}$$

Für $s \in S$ ist $\varphi_S(s) = \frac{s}{1} \in (S^{-1}R)^*$ wegen $\frac{s}{1} \cdot \frac{1}{s} = \frac{s}{s}$.
φ ist im Allgemeinen nicht injektiv.

$$\begin{aligned}\ker(\varphi) &= \left\{r \in R : \frac{r}{1} = \frac{0}{1}\right\} \\ &= \{r \in R : \exists u \in S : ru = 0\}\end{aligned}$$

Bemerkung 2.5.25:

- φ ist trivial, falls $0 \in S$.
- φ ist injektiv, falls $0 \notin S \wedge R$ ist Integritätsbereich.

Beispiel 2.5.26:

- R Integritätsbereich, $S = R \setminus \{0\}$ liefert für $S^{-1}R$ den Quotientenkörper von R.
- R kommutativer Ring mit Eins, $\mathcal{P}$ sei Primideal von R. Setze

  $$S \coloneqq R \setminus \mathcal{P}$$

  S ist multiplikativ abgeschlossen, da $\mathcal{P}$ prim. $(R \setminus \mathcal{P})^{-1}R =: R_{\mathcal{P}}$ heißt Lokalisierung von R bei $\mathcal{P}$. $R_{\mathcal{P}}$ ist kommutativer Ring mit Eins mit genau

einem maximalen Ideal $m := \left\{\frac{r}{s} : r \in \mathcal{P}, s \in R \setminus \mathcal{P}\right\}$. m ist maximal, da jedes $\frac{r'}{s} \notin m$ erfüllt $r' \in R \setminus \mathcal{P}$, das heißt $\frac{r'}{s} \cdot \frac{s}{r'} = \frac{1}{1}$ und ist invertierbar, sodass jedes Ideal, das r' enthält schon ganz $R_{\mathcal{P}}$ ist.

Ein kommutativer Ring mit Eins, der genau ein maximales Ideal besitzt, heißt lokaler Ring.

- $R = \mathbb{Z}, \mathcal{P} = (2), \mathbb{Z}_{(2)} = \left\{x = \frac{p}{q} : q \equiv 1 \pmod 2\right\}$
- $R = \mathbb{Z}, S = 2\mathbb{Z} \setminus \{0\}$

$$S^{-1}\mathbb{Z} = \left\{x = \frac{p}{q} : q \equiv 0 \pmod 2\right\} = \mathbb{Q}$$

- $R = \mathbb{Z}, S = \{1, 2, 2^2, \dots\}, S^{-1}\mathbb{Z} = \left\{x = \frac{p}{q} : \exists k \in \mathbb{N} : q = 2^k\right\}$

2.6 Teilbarkeit, faktorielle Ringe

R sei ab jetzt stets Integritätsbereich.

Definition 2.6.1:
a heißt Teiler von b (schreibe $a \mid b$):$\iff \exists c \in R : b = ac$.

Bemerkung 2.6.2:

- $a \mid a, 1 \mid a, a \mid 1 \iff a \in R^*$
- $a \mid b \iff b \in (a) \iff (b) \subseteq (a) \iff (a) \mid (b)$
- $a \sim b$: a heißt zu b assoziiert, falls $a \mid b \wedge b \mid a$. Dies ist äquivalent mit $(a) = (b)$. Es ist $a \sim b \iff b = ua$ mit $u \in R^*$ (denn $a \sim b \iff \begin{cases} b = ac \\ a = bd \end{cases}$ Es folgt $b = bdc$ und R ist IB $\implies 1 = cd$, woraus $c, d \in R^*$ folgt.)
- in $R = \mathbb{Z}$: $a \sim b \iff a = \pm b$.

Definition 2.6.3:

Ein Element $d \in R$ heißt ein größter gemeinsamer Teiler, ggT, von a, b, falls:

- $d \mid a \wedge d \mid b$
- $\forall d' \in R\colon d' \mid a \wedge d' \mid b \implies d' \mid d$

ACHTUNG: In Integritätsbereichen muss nicht immer ein ggT zu je zwei Elementen existieren! Auch wenn einer existiert, so ist er nicht eindeutig, da er mit beliebigen Einheiten multipliziert werden kann.

Beispiel 2.6.4:

$R = \mathbb{Z} + \mathbb{Z}\sqrt{-5} = \left\{x + y\sqrt{-5}\colon x, y \in \mathbb{Z}\right\}$.

$a := 2 + 2\sqrt{-5} = 2(1 + \sqrt{-5})$ $\qquad 2 \mid a \wedge 2 \mid b$

$b := 6 = 2 \cdot 3 = (1 + \sqrt{-5})(1 - \sqrt{-5})$ $\qquad 1 + \sqrt{-5} \mid a \wedge 1 + \sqrt{-5} \mid b$

Angenommen $\exists d := \alpha + \beta\sqrt{-5}$ ein ggT von a, b, so muss gelten:

$$2 \mid d \wedge 1 + \sqrt{-5} \mid d$$

$2 \mid \alpha + \beta\sqrt{-5} \implies \alpha, \beta \equiv 0 \pmod 2$
$\alpha + \beta\sqrt{-5} \mid 2 + 2\sqrt{-5} \iff \left(\frac{\alpha}{2} + \frac{\beta}{2}\sqrt{-5} \mid \left(1 + \sqrt{-5}\right)\right)$
$\implies d = \pm 2 \vee d = \pm(2 + 2\sqrt{-5})$
Angenommen $d = \pm(2+2\sqrt{-5})$. $(x+y\sqrt{-5})(2+2\sqrt{-5}) = 6 \iff (x+y\sqrt{-5})(1+\sqrt{-5}) = 3 \iff \begin{cases} x - 5y = 3 \\ x + y = 0 \end{cases} \iff \begin{cases} 6x = 3 \\ x + y = 0 \end{cases}$
$x = \frac{1}{2} \notin \mathbb{Z}$
Angenommen $d = \pm 2 \implies 1 + \sqrt{-5} \mid 2$
$(x + y\sqrt{-5})(1 + \sqrt{-5}) = 2 \iff \begin{cases} x - 5y = 2 \\ x + y = 0 \end{cases} \iff \begin{cases} 6x = 2 \\ x = y \end{cases}$ ↯

Fazit: in $\mathbb{Z} + \mathbb{Z}\sqrt{-5}$ haben a, b keinen ggT!

Zwischenrechnung für oben:

Behauptung: $(x+y\sqrt{-5})(u+v\sqrt{-5}) = 1+\sqrt{-5} \implies x+y\sqrt{-5} = \pm(1+\sqrt{-5}) \vee u + v\sqrt{-5} = \pm(1 + \sqrt{-5})$ Dann gilt auch: $(x - y\sqrt{-5})(u - v\sqrt{-5}) = 1 - \sqrt{-5}$ $\implies (x^2 + 5y^2)(u^2 + 5v^2) = 6$, was nur 2 Möglichkeiten zulässt: $1 \cdot 6 = 6, 2 \cdot 3 = 6$. Wegen $x^2 + 5y^2 = 2/3$ hat keine Lösung in $\mathbb{Z} \times \mathbb{Z}$, bleibt nur $(x^2 + 5y^2) = 1 \wedge (u^2 + 5v^2) = 6$ übrig, woraus $x = \pm 1, u = \pm 1, v = \pm 1$ folgt.

Definition 2.6.5:

Sei $p \in R \setminus R^*, p \neq 0$.

$$p \text{ heißt prim} :\iff \forall a, b \in R\colon p \mid ab \implies p \mid a \vee p \mid b$$

$$p \text{ heißt irreduzibel} :\iff \forall a, b \in R\colon p = ab \implies a \in R^* \vee b \in R^*$$

Proposition 2.6.6:

1. a ist irreduzibel $\iff$ $(a) \neq (0)$ ist maximal in der Menge aller Hauptideale von R.
2. a ist prim $\iff$ (a) ist Primideal $\neq (0)$.
3. a ist prim $\implies$ a ist irreduzibel.

Beweis.

1. $$\begin{aligned} a \text{ sei irreduzibel} &\iff (a \neq 0, a \notin R^*, a = bc \wedge b \notin R^* \implies c \in R^*) \\ &\iff ((a) \neq (0), (a) \neq R, (a) = (bc) \wedge (b) \neq R \implies (c) = R) \\ &\iff ((a) \neq (0), (a) \neq R, (a) \subsetneq (c) = R) \\ &\iff (a) \text{ maximal in der Menge der Hauptideale von } R \end{aligned}$$

2. Sei p prim
$$\begin{aligned} &\iff p \notin R^*, p \neq 0 \wedge p \mid ab \implies p \mid a \vee p \mid b \\ &\iff (p) \neq R, (p) \neq (0) \wedge (ab) \subseteq (p) \implies (a) \subseteq (p) \vee (b) \subseteq (p) \\ &\iff (p) \neq R, (p) \neq (0) \wedge ab \in (p) \implies a \in (p) \vee b \in (p) \end{aligned}$$

3. Sei p prim und $p = ab$. Es folgt $p \mid ab \implies p \mid a \vee p \mid b$. oBdA sei $p \mid a$, das heißt $\exists c \in R$ mit $pc = a$. Dann gilt: $p = ab = pcb$ und da R Integritätsbereich ist, folgt $cb = 1$ das heißt $b \in R^*$ und p ist daher irreduzibel. □

Definition 2.6.7:

Ein Integritätsbereich R heißt Hauptidealbereich, wenn jedes Ideal von R ein Hauptideal ist (das heißt, von einem Element erzeugt wird).

Lemma 2.6.8:

In einem Hauptidealbereich existiert zu je zwei Elementen stets ein ggT. Er ist bis auf Einheiten eindeutig bestimmt.

Beweis. Sei R ein Hauptidealbereich (HIB, englisch: Principal Ideal Domain, PID). $a, b \in R$. $\text{ggT}(a,b) = d \iff (a) + (b) = (d)$. Ist $I := aR + bR$, so gilt $(a) \in I \wedge (b) \in I$ und $I = (\tilde{d})$. Es folgt:

$$\tilde{d} \mid a \wedge \tilde{d} \mid b \implies \tilde{d} \mid d \qquad \text{(Definition des ggT 2.6.3)}$$
$$d \mid a \wedge d \mid b \implies d \mid c \forall c \in I \implies d \mid \tilde{d}$$

$(d) = (\tilde{d})$ impliziert $d = u\tilde{d}$ mit $u \in R^*$. □

Bemerkung 2.6.9:

Im Theorem 2.6.4: in $\mathbb{Z} + \mathbb{Z}[\sqrt{-5}]$ existiert der ggT von $2 + 2\sqrt{-5}$ und 6 nicht, denn das von 2 und $1 + \sqrt{-5}$ erzeugte Ideal ist kein Hauptideal.

Definition 2.6.10:

Ein Integritätsbereich R heißt faktoriell (UFD = unique factorisation domain) falls jedes $r \in R, r \neq 0, r \notin R^*$ eine Zerlegung $r = p_1 \cdots p_s$ in Primelemente $p_1, \ldots, p_s$ besitzt.

Bemerkung 2.6.11:

Diese Zerlegung ist bis auf Einheiten eindeutig.

Angenommen $r = p_1 \cdots p_n = q_1 \cdots q_m$ mit p_i, q_j prim, oBdA $n \leq m$. $p_1 \mid q_1 \cdots q_m$ und p_1 ist prim $\implies \exists i$: $p_1 \mid q_i$, oBdA $i = 1$. Also: $p_1 \mid q_1$, das heißt $\exists u_1 \in R$ mit $q_1 = u_1 p_1$. q_1 ist prim $\implies$ q_1 ist irreduzibel und wegen $p_1 \notin R^*$ folgt $u_1 \in R^*$.

Durch Iteration dieses Verfahrens folgt $n = m$ und

$$\{q_1, \ldots, q_n\} = \{u_1 p_1, \ldots u_n p_n\}.$$

Wir zeigen nun, dass jeder Hauptidealbereich faktoriell ist.

Lemma 2.6.12:

Sei R ein HIB und $I_1 \subseteq I_2 \subseteq I_3 \subseteq \cdots$ eine aufsteigende Folge von Idealen von R. Dann existiert ein $N\colon I_N = I_{N+1} = \cdots$. Man sagt die aufsteigende Folge von Idealen wird stationär.

Beweis. Sei $I_1 \subseteq I_2 \subseteq \cdots$ eine aufsteigende Folge von Idealen von R.

$$I \coloneqq \bigcup_{n=1}^{\infty} I_n$$

ist ein Ideal von R. Dann existiert ein $a \in R$ mit $I = (a)$. Wegen $a \in I$ folgt: $\exists N\colon a \in I_N$. Dann ist $(a) \subseteq I_N$ und $I_N \subseteq (a)$ und somit $I_N = I_{N+1} = \cdots$. □

Definition 2.6.13:

Ein kommutativer Ring mit Eins in dem jede aufsteigende Folge von Idealen stationär wird, heißt noetherscher Ring.

Lemma 2.6.14:

R ist noethersch $\iff$

1. jede nichtleere Menge M von Idealen von R besitzt in M ein maximales Element bezüglich $\subseteq$.
2. Jedes Ideal von R ist endlich erzeugt

Beweis.

1. Angenommen $\exists M$, die kein maximales Element besitzt. Es folgt:

   $$\forall I_1 \in M\colon \exists I_2 \in M\colon I_1 \subsetneq I_2.$$

   Induktiv konstruiert man so eine echt aufsteigende Kette von Idealen beliebiger Länge. Ein Widerspruch zu R ist noethersch.

   Umgekehrt, besitzt laut Voraussetzung jede Menge von Idealen ein maximales Element, insbesondere jede aufsteigende Folge von Idealen.

2. Angenommen $I \triangleleft R$ ist nicht endlich erzeugt, $\{a_1, a_2, \dots\}$ ein Erzeugendensystem. Dann ist $\langle a_1 \rangle \subseteq \langle a_1, a_2 \rangle \subseteq \langle a_1, a_2, a_3 \rangle \cdots$ eine aufsteigende Folge von Idealen. Würde

diese Folge stationär, so wäre I von nur endlich vielen Elementen erzeugbar. Ein Widerspruch zur Voraussetzung.

Umgekehrt: Für jede aufsteigende Kette $I_1 \subseteq I_2 \subseteq \cdots$ ist auch $I := \bigcup_{n=1}^{\infty} I_n$ ein Ideal und endlich erzeugt nach Voraussetzung. Sei $\langle a_1, \ldots, a_s \rangle = I$. Dann gilt $a_1, \ldots, a_s \in I$ und somit $a_1 \in I_{n_1}, \ldots, a_s \in I_{n_s}$, woraus $\{a_1, \ldots, a_s\} \subseteq I_{\underbrace{\max\{n_i\}}_{=:N}}$ folgt, und es gilt $I_N = I_{N+1} = \cdots$. R ist daher noethersch. □

Lemma 2.6.15:
R sei ein noetherscher Integritätsbereich. Dann besitzt jedes Element $r \in R, r \neq 0, r \notin R^*$ eine Zerlegung in irreduzible Elemente.

Beweis. Angenommen $\exists x_0 \in R, x_0 \neq 0, x_0 \in R^*$, das keine solche Zerlegung besitzt. Dann ist x_0 nicht irreduzibel, sodass $x_0 = a_0 b_0$ mit $a_0, b_0 \neq 0, \notin R^*$. Nicht beide können eine Zerlegung in irreduzible Elemente besitzen, oBdA $a_0 =: x_1$ hat keine. Es ist $x_1 \mid x_0$, aber $x_1 \not\sim x_0$. Durch Iteration dieses Prozesses erhalten wir eine Folge $x_0, x_1, \ldots$ von Elementen aus R mit $(x_0) \subsetneqq (x_1) \subsetneqq (x_2) \subsetneqq \cdots$. Dies liefert einen Widerspruch zu R ist noethersch. □

Lemma 2.6.16:
In Hauptidealbereichen gilt stets: p irreduzibel $\implies$ p prim.

Beweis.

$$\begin{aligned} p \text{ irreduzibel} &\iff (p) \text{ ist maximal in der Menge der Hauptideale von } R. \\ &\iff (p) \text{ ist maximal} \implies (p) \text{ ist Primideal} \\ &\iff p \text{ ist prim.} \end{aligned}$$

□

Satz 2.6.17:
R ist HIB $\implies$ R ist faktoriell.

Beweis. R HIB $\implies$ R ist noethersch $\implies$ jedes $r \in R$ besitzt eine Zerlegung in irreduzible Elemente $\overset{2.6.16}{\implies}$ jedes Element aus R besitzt eine Zerlegung in prime Elemente, das heißt R ist faktoriell. □

Satz 2.6.18:
Sei R faktorieller Integritätsbereich.

1. $r \in R$ ist prim $\iff$ r ist irreduzibel.
2. Jedes $x \neq 0$ besitzt eine bis auf Einheiten eindeutige Zerlegung
$$x = \varepsilon \cdot \prod_{p \in \mathcal{P}} p^{\nu_p(x)}$$
mit $\varepsilon \in R^*, \nu_p(x) \in \mathbb{N}, \nu_p(x) = 0$ für alle bis auf endlich viele $p, \mathcal{P}$: Vertretersystem von Primelementen$/\sim$
3. $\forall x, y \in R\colon \exists\, \mathrm{ggT}(x, y)$.

Beweis.

1. x ist irreduzibel hat auch eine Zerlegung $x = p_1 \cdots p_r$ mit $p_1, \ldots, p_r$ prim $\implies$ $p_1, \ldots, p_r \notin R^*$ $\implies$ $r = 1, x = p_1$ und x ist prim.
2. ist gezeigt. ✓
3. Sei
$$x = \varepsilon_1 \prod_{p \in \mathcal{P}} p^{\nu_p(x)}, y = \varepsilon_2 \prod_{p \in \mathcal{P}} p^{\nu_p(y)}.$$
Setze $d \coloneqq \mathrm{ggT}(x, y) = \prod_{p \in \mathcal{P}} p^{\min\{\nu_p(x), \nu_p(y)\}}$. Dann gilt: $d \mid x \wedge d \mid y$. Ist $\tilde{d} \mid x, \tilde{d} \mid y$, so ist $\nu_p(\tilde{d}) \leq \nu_p(x)$ und $\nu_p(\tilde{d}) \leq \nu_p(y) \forall p \in \mathcal{P}$. $\implies$ $\nu_p(\tilde{d}) \leq \min\{\nu_p(x), \nu_p(y)\}$ und somit $\tilde{d} \mid d$. □

2.7 Quadratische Zahlenkörper und Zahlringe

Definition 2.7.1:
Für $d \neq 0, 1$ quadratfrei definiere
$$\mathbb{Q}\left(\sqrt{d}\right) \coloneqq \left\{a + b\sqrt{d} \mid a, b \in \mathbb{Q}\right\} \subseteq \mathbb{C}.$$
$\mathbb{Q}\left(\sqrt{d}\right)$ heißt quadratischer Zahlkörper.

Ein Element $\alpha + \beta\sqrt{d}, (\alpha, \beta) \in \mathbb{Q} \times \mathbb{Q}$, heißt ganz in $\mathbb{Q}\left(\sqrt{d}\right)$, falls das normierte Polynom $f \in \mathbb{Q}[x]$ von kleinstem Grad mit $f\left(\alpha + \beta\sqrt{d}\right) = 0$ schon in $\mathbb{Z}[x]$ liegt (das heißt $\alpha + \beta\sqrt{d}$

Nullstelle eines normierten Polynoms aus $\mathbb{Z}[x]$ ist). Falls $\alpha \in \mathbb{Q} \cap \mathbb{Q}\left(\sqrt{d}\right), \alpha = \frac{a}{b}$, so hat $f(x) = bx - a$ eine Nullstelle in $\frac{a}{b}$, liegt in $\mathbb{Z}[x]$, ist normiert $\iff b = 1$. $\alpha = \frac{a}{b}$ ist ganz in $\mathbb{Q}\left(\sqrt{d}\right) \iff b = \pm 1$.

Für $\alpha + \beta\sqrt{d} \in \mathbb{Q}\left(\sqrt{d}\right) \setminus \mathbb{Q}$:

$$\left(x - \left(\alpha + \beta\sqrt{d}\right)\right)\left(x - \left(\alpha - \beta\sqrt{d}\right)\right) = x^2 - 2\alpha x + \left(\alpha^2 - d\beta^2\right) \in \mathbb{Q}[x]$$

$\alpha + \beta\sqrt{d}$ ist ganz $\iff P(x) \in \mathbb{Z}[x]$.

$P(x) \in \mathbb{Z}[x] \iff 2\alpha \in \mathbb{Z} \wedge \alpha^2 - d\beta^2 \in \mathbb{Z}$.

1. Fall: $\alpha \in \mathbb{Z} \wedge \alpha^2 - d\beta^2 \in \mathbb{Z} \iff (\alpha, \beta) \in \mathbb{Z} \times \mathbb{Z}$

2. Fall: $\alpha = \frac{u}{2}$, dann muss auch $\beta = \frac{v}{2}$. $\frac{u^2}{4} - \frac{dv^2}{4} \in \mathbb{Z} \iff u^2 - db^2 \equiv 0 \pmod 4$. Es ist $u^2 \equiv 1 \pmod 4 \wedge v^2 \equiv 1 \pmod 4$. Falls $d \equiv 2, 3 \pmod 4$: diese Gleichung ist nie erfüllt. Falls aber $d \equiv 1 \pmod 4$ ist sie immer erfüllt.

Wir erhalten:

$$\alpha + \beta\sqrt{d} \text{ ist ganz in } \mathbb{Q}\left(\sqrt{d}\right) \iff \begin{cases} \alpha, \beta \in \mathbb{Z} & \text{für } d \equiv 2, 3 \pmod 4 \\ (\alpha, \beta \in \mathbb{Z}) \vee (2\alpha, 2\beta \in \mathbb{Z} & \text{mit } 2\alpha \equiv 2\beta \pmod 2) \end{cases}$$

Definition 2.7.2:

Der Ring $\mathcal{O}_d$ der ganzen Zahlen in $\mathbb{Q}\left(\sqrt{d}\right)$ ist $\mathbb{Z} + \mathbb{Z}\omega$, wobei $\omega = \frac{1+\sqrt{d}}{2}$ für $d \equiv 1 \pmod 4$ und $\omega = \sqrt{d}$ für $d \equiv 2, 3 \pmod 4$.

Überprüfe: $\mathcal{O}_d$ ist wirklich ein Ring.

Definition 2.7.3:

In $\mathbb{Q}\left(\sqrt{d}\right)$ definieren wir die Norm von $\alpha + \beta\sqrt{d}$ durch

$$\mathcal{N}\left(\alpha + \beta\sqrt{d}\right) = \left(\alpha + \beta\sqrt{d}\right)\left(\alpha - \beta\sqrt{d}\right) = \alpha^2 - d\beta^2$$

Es gilt: $\mathcal{N}(xy) = \mathcal{N}(x)\mathcal{N}(y)$ für $x, y \in Q\left(\sqrt{d}\right)$ ($\mathcal{N}$ ist multiplikativ).

Bemerkung 2.7.4:

$x \in \mathcal{O}_d^* \iff \mathcal{N}(x) = \pm 1 (\in \mathbb{Z}^*)$

$x \in \mathcal{O}_d^* \iff \exists y \in \mathcal{O}_d \colon xy = 1$. Es folgt $\mathcal{N}(xy) = \mathcal{N}(x)\mathcal{N}(y) = 1$. $\mathcal{N}(x), \mathcal{N}(y) \in \mathbb{Z}$ (klar falls $x, y \in \mathbb{Z} + \mathbb{Z}\sqrt{d}$, $\frac{u^2}{4} + \frac{v^2}{4}d = \frac{u^2+v^2d}{4} \in \mathbb{Z}$). $\implies \mathcal{N}(x) \in \pm 1$.

Falls $\mathcal{N}(x) = \pm 1, x = \alpha + \beta\sqrt{d}$, $\implies \left(\alpha + \beta\sqrt{d}\right)\left(a - \beta\sqrt{d}\right) = \pm 1$, das heißt $x \in \mathcal{O}_d^*$.

Für welche d ist $\mathcal{O}_d$ faktoriell und wie weist man es nach? Es sind jedenfalls nicht alle $\mathcal{O}_d$ sind faktoriell, z.B. $\mathcal{O}_{-5}$ ist es nicht! Siehe dazu Theorem 2.6.4.

In $\mathcal{O}_{-5} = \mathbb{Z} + \mathbb{Z}\sqrt{-5}$ gilt $6 = 2 \cdot 3 = \left(1 + \sqrt{-5}\right)\left(1 - \sqrt{-5}\right)$. Wir wissen bereits: $1 + \sqrt{-5}$ ist irreduzibel in $\mathcal{O}_{-5}$. Wäre $\mathcal{O}_{-5}$ faktoriell, so folgte daraus: $1 + \sqrt{-5}$ ist prim. $1 + \sqrt{-5} \mid 2 \vee 1 + \sqrt{-5} \mid 3$, was aber nicht der Fall ist.

$\mathcal{O}_{10}$ ist auch nicht faktoriell, $6 = 2 \cdot 3 = \left(4 + \sqrt{10}\right)\left(4 - \sqrt{10}\right)$

Definition 2.7.5:

Eine Funktion $\nu \colon R \setminus \{0\} \to \mathbb{Z}^+$ mit $\nu(mn) \geq \nu(m) \forall m, n \in R \setminus \{0\}$ heißt euklidische Normfunktion auf dem Integritätsbereich R, falls für $m, n \in R, m \neq 0$ Elemente $q, r \in R$ existieren mit $n = qm + r$ und $\nu(r) < \nu(m)$ oder $r = 0$. Der Ring R heißt dann euklidischer Ring.

Beispiel 2.7.6:

1. $R = \mathbb{Z}, \nu = |\cdot|$. Satz von der Division mit Rest liefert: $\mathbb{Z}$ ist euklidisch.
2. $R = \mathbb{Z} + \mathbb{Z}i (= \mathcal{O}_{-1}), \nu = \mathcal{N}$. Seien $a, b \in \mathbb{Z}[i]$. Zu zeigen: $\exists q, r \in \mathbb{Z}[i]$ mit $a = qb + r$ und $\underbrace{\mathcal{N}(r) < \mathcal{N}(b)}_{\text{sogar } \mathcal{N}(r) \leq \frac{\mathcal{N}(b)}{2}} \vee r = 0$. Schreiben $\frac{a}{b} = \xi + i\eta$ mit $\xi, \eta \in \mathbb{Q}$.

   Es existieren $k, l \in \mathbb{Z}$ mit $|\xi - k| \leq \frac{1}{2}, |\eta - l| \leq \frac{1}{2}$. $\mathcal{N}((\xi + i\eta) - (k + il)) = \mathcal{N}(\underbrace{(\xi - k)}_{|\cdot| \leq \frac{1}{2}} + i \underbrace{(\eta - l)}_{|\cdot| \leq \frac{1}{2}}) \leq \frac{1}{2}$ Setze nun: $q \coloneqq k + il, r = a - qb$

$$\begin{aligned} \mathcal{N}(r) = \mathcal{N}(a - qb) = \mathcal{N}(a - (k + il)b) = \mathcal{N}(b\left(\frac{a}{b} - (k + il)\right)) \\ = \mathcal{N}(b) \cdot \underbrace{\mathcal{N}(\frac{a}{b} - (k + il))}_{\leq \frac{1}{2}} \leq \frac{1}{2}\mathcal{N}(b) \end{aligned}$$

   Es folgt: $\mathbb{Z}[i]$ ist euklidisch mit $\nu = \mathcal{N}$.

Satz 2.7.7:

R euklidisch $\implies$ R HIB ($\implies$ R faktoriell)

Beweis. Sei $I \triangleleft R$. Ist $I = \{0\} \implies I = (0)$.
Falls $I \neq (0)$, so existiert ein $0 \neq a \in I$ mit $\nu(a)$ ist minimal. $(a) \in I$ und wir behaupten:

$(a) = I$. Sei $b \in I$. Dann ist $b = qa + r$ mit $q, r \in R$ und $\nu(r) < \nu(a)$ oder $r = 0$ (da R euklidisch!). $r = \underbrace{b}_{\in I} - \underbrace{q}_{\in I}\underbrace{a}_{\in I} \in I$, ein Widerspruch zu $\nu(a)$ minimal, es sei denn $r = 0$ und $b \in (a)$. Da b beliebig war, folgt $(a) = I$. □

$\mathcal{O}_{-43}$ ist HIB, aber nicht euklidisch.

Kapitel 3

Polynomringe

3.1 Grundlagen

$\mathcal{F} \coloneqq \{f\colon \mathbb{N} \to R \mid |\text{support}(f)| < \infty\}$, wobei $|\text{support}(f)| \coloneqq \{n \in \mathbb{N} | f(n) \neq 0\}$

Wir versehen $\mathcal{F}$ mit folgenden Operationen:

$$
\begin{aligned}
&+\colon \mathcal{F} \times \mathcal{F} \to \mathcal{F} \\
&\quad (f+g)(n) = f(n) + g(n) \\
&\cdot_R\colon R \times \mathcal{F} \to \mathcal{F} \\
&\quad (r \cdot_R f)(n) = r \ \cdot f(n) \\
&\star\colon \mathcal{F} \times \mathcal{F} \to \mathcal{F} \qquad\qquad \text{Faltung} \\
&\quad (f \star g)(n) = \sum_{k+l=n} f(k)g(l)
\end{aligned}
$$

Mit diesen Operationen wird $\mathcal{F}$ zu einer kommutativen R-Algebra.

$$\delta_n\colon m \mapsto \delta_n(m) = \begin{cases} 1 & m = n \\ 0 & \text{sonst} \end{cases}$$

Dann ist $\delta_n \in \mathcal{F}$. Jedes $f \in \mathcal{F}$ kann man darstellen als $\sum_n f(n)\delta_n$. δ_0 ist Einselement in $\mathcal{F}$: $(f \star \delta_0)(n) = \sum_{k+l=n} f(k)\delta_0(l) = f(n)$. Weiters gilt: $\delta_1^k = \delta_k$ für $k = 0, 1, \ldots$ ($f^k \coloneqq \underbrace{f \star f \ldots}_{k-\text{mal}}$). Angenommen $\delta_1^j = \delta_j$ sei für alle $n < k$ bereits gezeigt. Dann ist

$$
\begin{aligned}
\delta_1^j(n) &= (\delta_1^{j-1} \star \delta_1)(n) = \delta_{j-1} \star \delta_1(n) = \sum_{k+n=n} \delta_{j-1}(l)\delta_1(k) \\
&= \sum_{k+l=n} \delta_{j-1}(k)\delta_1(l) \\
&= \underbrace{\delta_{j-1}(j-1)}_{=1}\delta_1(n-j+1) + \delta_{j-1}(n-1)\underbrace{\delta_1(1)}_{=1} \qquad (\delta_1(1)\delta_{n-1}(n-1), \text{ falls } n = j) \\
&= \begin{cases} 1 & \text{für } n = j \\ 0 & \text{sonst} \end{cases} \implies \delta_1^j(n) = \delta_j(n) \forall n \\
&\implies \delta_1^j = \delta_j
\end{aligned}
$$

$\Longrightarrow$ jedes $f \in \mathcal{F}$ hat Darstellung als $\sum_{n \in \text{support}(f)} f(n)\delta_1^n$.

Definition 3.1.1:

Die Abbildungen $f \in \mathcal{F}$ heißen Polynome. $\mathcal{F}$ heißt Polynomring/Algebra in δ_1 über R.

$$\mathcal{F} =: R[\delta_1]$$

$$\delta_1 := X,\ f(X) = \sum_{i=0}^{d} a_i X^i \text{ mit } a_i := f(i)$$

$$\Longrightarrow\ f \leftrightarrow (a_0, \ldots, a_d)$$

$$(a_0, a_1, a_2) \star (b_0, b_1) = (a_0 b_0, a_0 b_1 + a_1 b_0, a_2 b_0 + b_1 a_1, a_2 b_1)$$
$$\hat{=}(a_0 + a_1 X + a_2 X^2)(b_0 + b_1 X) = a_0 b_0 + (a_0 b_1 + a_1 b_0)X + (a_1 b_2 + a_2 b_0)X^2 + a_2 b_1 X^3$$

a_0: konstanter Koeffizient.
$d := \max n \colon a_n \neq 0$ heißt führender Koeffizient, $d := \deg(f)$. Für Polynomringe in d Variablen, betrachte

$$\mathcal{F} := \{f \colon \mathbb{N} \to R \mid |\text{support}(f)| < \infty\}$$

liefert $f(X_1, \ldots, X_d) = \sum_{(i_1, \ldots, i_d)} a_{i_1, \ldots, i_d} X_1^{i_1} \cdot \ldots \cdot X_d^{i_d}$

$$\deg(f) := \sup\{i_1 + \cdots + i_d \colon a_{i_1, \ldots, i_d} \neq 0\} \text{ falls } f \neq 0.$$

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

Satz 3.1.2:

Sei R Integritätsbereich, dann gilt für $\deg \colon R[X_1, \ldots, X_d] \to \mathbb{N} \cup \{-\infty\}$, $P \mapsto \deg(P)$:

1. $\deg(PQ) = \deg(P) + \deg(Q)$.
2. $\deg(P + Q) \leq \max\{\deg(P), \deg(Q)\}, P, Q \neq 0$.

Beweis. $(d = 1)$
Sei $P(X) = \sum_{i=0}^{n} a_i X^i, Q(X) = \sum_{j=0}^{m} b_j X^j (a_n \neq 0 \neq b_m)$.

1. $PQ(x)$ hat führenden Koeffizienten $a_n b_m \neq 0$ (Da R IB).

$$\Longrightarrow\ \deg(PQ) = n + m.$$

2. Falls $m < n$ oder $m < n$, so ist der führende Koeffizient von $P + Q$ gerade b_m oder a_n. Falls $n = m$: führender Koeffizient von $P + Q$ hat Index $\leq n (= m)$. $\square$

Korollar 3.1.3:
R ist Integritätsbereich $\implies$ $R[X]$ ist Integritätsbereich, $(R[X])^* = R^*$

Beweis. Seien $f, g \neq 0$ in $\mathbb{R}[X]$. Dann ist $\deg(f) > -\infty$ und $\deg(g) > -\infty$, also $\deg(fg) = \deg(f) + \deg(g) > -\infty \implies fg \neq 0$
Sei $0 \neq f \in R[X]$ und $g \in R[X]$ mit $f \cdot g = 1$.

$$\deg(fg) = 0 = \underbrace{deg(f)}_{>-\infty} + \underbrace{\deg(g)}_{>-\infty} \implies \deg(f) = 0 = \deg(g).$$

Also können wir f, g mit konstanten Koeffizienten identifizieren, für diese gilt $\underbrace{f_0 g_0}_{\in R^*} = 1 \implies$
f, g sind Einheiten, also in $(R[X])^*$. $\square$

Satz 3.1.4:
Seien R, S kommutative Ringe mit Einselement, $R \leq S$. Dann definiert die Abbildung

$$\mathrm{ev}_a \colon R[X] \to S, P \mapsto P(a)$$

einen Ringhomomorphismus für alle $a \in S$.
ev_a heißt Evaluationsabbildung an der Stelle a.

Beweis. Die Homomorphie ist direkte Konsequenz der Definitionen von $+, \star$ in $R[X]$ für kommutative Ringe mit 1. Durch Auswertung an allen $a \in S$ erhalten wir eine Funktion

$$f_P \colon S \to S, a \mapsto \mathrm{ev}_a(P) = P(a),$$

die P zugeordnete Polynomfunktion. $\square$

Wir sagen: P hat in a eine Nullstelle $\iff$ $P \in \ker(\mathrm{ev}_a)$. Für $P, Q \in R[X], f_P, f_Q$ die zugehörigen Polynomfunktionen gilt

$$f_P = f_Q \iff P - Q \in \bigcap_{a \in S} \ker(\mathrm{ev}_a) \iff \bigcap_{a \in S} \ker(\mathrm{ev}_a) = \{0\}.$$

Beispiel 3.1.5:
$R = \mathbb{Z}/5\mathbb{Z}, P(X) = X^5, Q(X) = X.$

X	X^5
0	0
1	1
2	$32 = 2$
3	3
4	4

$\implies f_P = f_Q \wedge P \neq Q \implies X^5 - X \in \bigcap_{a \in \mathbb{Z}/5\mathbb{Z}} \ker(\mathrm{ev}_a)$

3.2 Wann ist $R[X]$ faktoriell?

Sei zunächst R unitärer Ring.

Satz 3.2.1:
Seien $f, g \in R[X]$, der führende Koeffizient von f sei eine Einheit in $R \implies \exists$ eindeutig bestimmte Polynome $q, r \in R[X]$ mit $\deg(r) < \deg(f) \vee r = 0$ mit $g = qf + r$.

Beweis. Ist $g = 0$ oder $\deg(g)$, so wähle $q = 0, r = g$ ✓

Induktion nach $\deg(g) =: n$ Induktionsanfang: $n = 0$ ✓(in R kann jedes Element (g) durch Einheit (f) geteilt werden)
Angenommen die Aussage ist für Polynome g von Grad $< n$ bereits gezeigt. Sei $f(x) = \varepsilon X^m + aX^{m-1} + \ldots, g(x) = bX^n + cX^{n-1} + \ldots, \varepsilon \in R^*, a, b, c \in R$, $m \leq n$. Betrachte $g_1 := g - b\varepsilon^{-1}X^{n-m}f = (bX^n + cX^{n+1} + \ldots) - b\varepsilon^{-1}X^{n-m}(\varepsilon X^m + aX^{m-1}) = 0X^n + (X - b\varepsilon^{-1}a)X^{n-1}$. $g_1 = 0$ oder $\deg(g_1) < n$, sodass nach Induktionsvoraussetzung: $\exists q_1, r \in R[X]$ mit $g_1 = q_1 \cdot f + r$ und $\deg(r) < \deg(f)$ Es folgt:

$$g = g_1 + b\varepsilon^{-1}X^{n-m}f = (\underbrace{q_1 + b\varepsilon^{-1}X^{n-m}}_{=:q})f + r.$$

Eindeutigkeit: $g = qf + r = q_1 f + r_1$ mit den entsprechenden Bedingungen an $\deg(r), \deg(r_1)$. Daraus folgt: $r - r_1 = (q_1 - q)f$. Falls $q_1 \neq q$, so ist $\deg(r - r_1) =$ da der führende Koeffizient von f kein Nullteiler ist!
$\deg((q_1 - q)f) \overset{|}{=} \deg(q_1 - q) + \deg(f) \implies \deg(r - r_1) \geq \deg(f)$, ein Widerspruch zu $\deg(r), \deg(r_1) < \deg(f)$. □

Korollar 3.2.2:
Sei R ein KRE, $f \in R[X]$. Es ist $f(a) = 0 \iff f(X) = (X - a)q(X)$ mit $q \in R[X]$. (das bedeutet: $\ker(\mathrm{ev}_a) = ((X - a))$)

Beweis. Teile f durch $X - a$ mit Rest. Nach dem vorigen Theorem 3.2.1 gilt: $f(X) = (X-a)q(X) + r(X)$ mit $\deg(r) < 1$. Falls $r(X) \neq 0$, so muss $r(X) = r \in R$ gelten. Wende nun ev_a an: $f(a) = r \implies r = 0$. Die Umkehrung ist klar. □

Es ist essenziell dass R kommutativ ist:

Beispiel 3.2.3:

R sei nicht kommutativ, $a, b \in R$ mit $ab \neq ba$. $f(X) := X^2 + (a-b)X - ab$. Dann ist $f(b) = b^2 + ab - b^2 - ab = 0$. Angenommen $\exists q(X) \in R[X]$ mit $f(X) = (X-b)q(X)$. Dann gilt $\deg(q) = 1$, der führende Koeffizient von q ist 1. Es muss sogar $q(X) = X + a$ gelten. $(X-b)(X+a) =: g(x)$

$$g(a) = (a-b)2a = 2a^2 - 2ba \neq f(a) = a^2 + a^3 - ba - ab = 2a^2 - (ab + ba).$$

Satz 3.2.4:

Sei $\mathbb{K}$ ein Körper. Dann ist $\mathbb{K}[X]$ faktoriell.

Beweis. $\mathbb{K}$ Körper $\implies$ jedes $a \in \mathbb{K}, a \neq 0$, ist eine Einheit. Daher ist $\deg\colon \mathbb{K}[X] \to \mathbb{N}$ eine euklidische Normfunktion auf $\mathbb{K}[X]$. Daher ist $\mathbb{K}[X]$ euklidisch $\implies$ $\mathbb{K}[X]$ ist HIB $\implies$ $\mathbb{K}[X]$ faktoriell. □

Sei R ein faktorieller Ring. Wir wissen bereits: zu $a_1, \ldots, a_n \in R$ existiert stets ein ggT.

Definition 3.2.5:

Sei $f(X) \in R[X]$ mit $f(X) = a_m X^m + \cdots + a_1 X + a_0$. Dann heißt jeder ggT von $(a_0, \ldots, a_m)$ ein Inhalt ($I(f)$) von f.

$I(f)$ ist daher bis auf Einheiten von R eindeutig festgelegt. f heißt primitiv, falls 1 ein Inhalt von f ist. Schreibe $I(f) = 1$.

Jedes $f \in R[X]$ kann als $I(f) \cdot f^*$ geschrieben werden, mit f^* primitiv.

Lemma 3.2.6 (Lemma von Gauß):

Für $f, g \in R[X]$ gilt $I(fg) = I(f)I(g) \cdot \varepsilon$ mit $\varepsilon \in R^*$.

Beweis. Schreibe $f = I(f) \cdot f^*$, $g = I(g) \cdot g^*$.

$$I(I(f)f^*I(g)g^*) = I(I(f)f^*)I(I(g)g^*) \iff \cancel{I(f)I(g)}I(f^*g^*) = \cancel{I(f)}I(f^*)\cancel{I(g)}I(g^*).$$

Es genügt also zu zeigen: f, g primitiv $\implies fg$ primitiv.

Angenommen π sei ein irreduzibles Element von R, das jeden Koeffizienten von $fg =: h$ teilt. Die Koeffizienten von h haben die Gestalt

$$\left(f(X) \coloneqq \sum_{i=0}^{n} f_i X^i, g(X) \coloneqq \sum_{j=0}^{m} g_j X^j\right) h_k = \sum_{i+j=k} f_i g_j.$$

Es gilt also $\pi | h_k, \forall k$. Seien f_r, g_s die ersten nicht durch π teilbaren Koeffizienten von f beziehungsweise g. $\begin{pmatrix} f_r \not\equiv 0 \pmod{\pi}, i < r \implies f_i \equiv 0 \pmod{\pi} \\ g_s \not\equiv 0 \pmod{\pi}, j < s \implies g_j \equiv 0 \pmod{\pi} \end{pmatrix}$. Dann ist

$$h_r + s = \sum_{i+j=r+s} f_i g_j \equiv f_r g_s \pmod{\pi}.$$

Nach Voraussetzung ist $h_{r+s} \equiv 0 \pmod{\pi}$, also $f_r g_s \equiv 0 \pmod{\pi}$. Weil R faktoriell ist, folgt aus π irreduzibel auch π ist prim. Daher gilt $f_r \equiv 0 \pmod{\pi}$ oder $g_s \equiv 0 \pmod{\pi}$, ein Widerspruch zur Wahl von r beziehungsweise s. □

Satz 3.2.7:

Sei R ein faktorieller Ring. Dann ist auch $R[X]$ faktoriell.

Beweis. Sei $f \in R[X]$. Wir werden zeigen: f lässt sich als Produkt von Primelementen in $R[X]$ darstellen. Wir schreiben: $f = I(f) \cdot f^*$. Sei K der Quotientenkörper von R. $f \in R[X] \implies f \in K[X]$, $K[X]$ ist faktoriell und daher gilt $f^* = \tilde{f}_1 \cdots \tilde{f}_s$ mit $\tilde{f}_1, \ldots, \tilde{f}_s$ irreduzible Polynome in $K[X]$. Durch Multiplikation mit dem kgV der Koeffizienten erhalten wir $f^* = \varepsilon_k \cdot f_1 \cdots f_s$, wobei $f_1, \ldots, f_s \in R[X]$ irreduzibel und primitiv, ε_k eine Einheit in K.
$f_1, \ldots, f_s$ primitiv $\overset{3.2.6}{\implies}$ $f_1 \cdots f_s$ primitiv $\implies$ ε_k ist Einheit in R. R faktoriell $\implies$ $\varepsilon_k \cdot I(f)$ ist Produkt von irreduziblen Elementen in R, $\varepsilon_k \cdot I(f) = e \cdot \pi_1 \cdots \pi_r$. ($e \in R^*, \pi_i \in R$ irreduzibel). $\pi_1, \ldots, \pi_r$ sind prim in $R \implies (\pi_1), \ldots, (\pi_r)$ Primideale in R, das heißt ${}^{R}\!/_{\pi_i R}$ ist IB $\implies \left({}^{R}\!/_{\pi_i R}\right)[X]$ ist IB. Es gilt: ${}^{R}\!/_{\pi_i R}[X] \cong {}^{R[X]}\!/_{\pi_i R[x]}$ und ist daher IB $\implies \pi_i R[X]$ ist Primideal in $R[X] \implies \pi_i$ Primelement in $R[X]$.

Es bleibt also noch zu zeigen: $f_1, \ldots, f_s$ sind prim in $R[X]$. Klarerweise gilt: $f_i R[X] \subseteq f_i K[X] \cap R[X]$. Für die umgekehrte Inklusion: sei $g = f_i \cdot r$ mit $r \in K[X], g \in R[X]$. Schreibe $r = \frac{a}{b} r_0$ mit $r_0 \in R[X]$ primitiv, $a, b \in R, \mathrm{ggT}(a, b) = 1$.

$$g = f_i r \implies bg = b f_i r = a f_i r_0$$

Es folgt: $bI(g) \sim I(bg) = I(a f_i r_0) \sim a \overbrace{I(f_i)}^{1} \overbrace{I(r_0)}^{1}$. Folglich gilt:

$$b \mid a \implies \frac{a}{b} \in R \implies r \in R[X] \implies g \in f_i R[X].$$

□

Bemerkung 3.2.8:

- K Körper $\implies$ $K[X]$ faktoriell, sogar euklidisch & HIB.
- R faktorieller Ring $\implies$ $R[X]$ faktoriell, im Allgemeinen weder euklidisch noch HIB (siehe $R = \mathbb{Z}$).

Korollar 3.2.9:

$R[X_1, \ldots, X_n]$ ist faktoriell wenn R faktoriell ist.

Beweis. Beweis per Induktion nach n. IA: $n = 1$: Theorem 3.2.7
Sei gezeigt, dass $R[X_1, \ldots, X_{n-1}]$ faktoriell ist. $R[X_1, \ldots, X_n] \cong (R[X_1, \ldots, X_{n-1}])[X_n]$ und dies ist faktoriell nach IV und der Aussage für $n = 1$. □

Achtung: $\mathbb{K}[X, Y]$ ist faktoriell, aber kein HIB! Bsp: in $\mathbb{R}[X, Y]$ ist (X, Y) kein HI. (Übung)

3.3 Irreduzibilität von Polynomen

Bemerkung 3.3.1:

Ist R faktoriell, $K = QK(R)$, so gilt: f irreduzibel in $R[X]$ $\implies$ f irreduzibel in $K[X]$.

Beweis. f irreduzibel $\implies$ f ist primitiv. Angenommen f reduzibel in $K[X]$, das heißt $f = gh$ mit $g, h \in K[X]$. Schreibe dann $\tilde{g} = \lambda g, \tilde{h} = \mu h$, wobei $\lambda, \mu \in R, \tilde{g}, \tilde{h} \in R[X]$. Es ist dann: $\lambda\mu f = \tilde{g}\tilde{h}$ und $\tilde{g}\tilde{h}$ ist primitiv nach Lemma von Gauß 3.2.6, und somit muss $\lambda\mu \in R^*$ gelten, sodass f reduzibel in $R[X]$. Dies ist ein Widerspruch zur Voraussetzung $\implies$ f irreduzibel in $K[X]$. □

Wir schreiben: $f(X) = a_n X^n + \ldots a_1 X + a_0, a_i \in R$.

Satz 3.3.2 (Kriterium von Eisenstein):

Sei R ein faktorieller Ring, $f \in R[X]$ wie angegeben. Es existiere ein Primelement $\mathcal{P}$ mit

$$\begin{cases} a_i \equiv 0 \pmod{\mathcal{P}} & \text{für } i = 0, \ldots, n-1, \\ a_0 \not\equiv 0 \pmod{\mathcal{P}^2}, \\ a_n \not\equiv 0 \pmod{\mathcal{P}}. \end{cases}$$

dann ist f irreduzibel (in $R[X]$).

Beweis. oBdA sei f primitiv. Angenommen $f = (\underbrace{b_0 + \ldots b_r X^r}_{b(X)})(\underbrace{c_0 + \cdots + c_s X^s}_{c(X)})$ mit $b_i, c_i \in R$. $\deg(b), \deg(c) > 0$. Es gilt: $b_0 c_0 = a_0$. Es ist $a_0 \equiv 0 \pmod{\mathcal{P}} \implies b_0 \equiv 0 \pmod{\mathcal{P}} \vee c_0 \equiv 0 \pmod{\mathcal{P}}$, aber nicht beides (wegen $a_0 \not\equiv 0 \pmod{\mathcal{P}^2}$)! Sei oBdA $c_0 \not\equiv \pmod{\mathcal{P}}$.
Wegen $a_n \not\equiv 0 \pmod{\mathcal{P}}$ existiert zumindest ein b_k mit $b_k \not\equiv 0 \pmod{\mathcal{P}}$. Ist k minimal mit $b_k \not\equiv 0 \pmod{\mathcal{P}}$, so folgt $a_k = \underbrace{(b_0 c_k + b_1 c_{k-1} + \cdots + b_{k-1} c_1)}_{\equiv 0 \pmod{\mathcal{P}}} + b_k c_0 \equiv 0 \pmod{\mathcal{P}}$, da $k < n (\deg(b), \deg(c) \geq 1)$, ein Widerspruch zu $b_k \not\equiv 0 \pmod{\mathcal{P}} \wedge c_0 \not\equiv 0 \pmod{\mathcal{P}}$.
Somit ist f irreduzibel. □

Beispiel 3.3.3 (Anwendungen):
$R = \mathbb{Z}, p \in \mathbb{P}$.

- $X^n - p, X^n + p$ sind irreduzibel über $\mathbb{Z}[X]$.
  $\implies \sqrt[n]{p} \notin \mathbb{Q}$. (da $X^n - p$ auch irreduzibel über $\mathbb{Q}[X]$ und $\sqrt[n]{p}$ Nullstelle von $X^n - p$ ist)

- $f(X) = X^{p-1} + X^{p-2} + \cdots + X + 1$ ist irreduzibel über $\mathbb{Z}[X]$. $(X-1)f(X) = X^p - 1$. Setze $X = Y + 1$.

  $$(X-1)f(X) = Y f(Y+1) = (Y+1)^p - 1 = \sum_{i=1}^{p} \binom{p}{i} Y^i = Y \sum_{i=1}^{p} \binom{p}{i} Y^{i-1}.$$

  Es gilt $\binom{p}{i} \equiv 0 \pmod{p}$ für $1 \leq i \leq p-1$, sodass $f(Y+1)$ die Bedingungen für die Anwendung von Theorem 3.3.2 erfüllt ($f(Y+1) = Y^{p-1} + \binom{p}{p-1} Y^{p-2} + \cdots + \binom{p}{2} Y + \binom{p}{1}$). $\implies \underbrace{f(Y+1)}_{=f(X)}$ ist irreduzibel.

  Allgemeiner gilt: Sei $a \in R^*, b \in R$. Dann gilt: $f(X) \in R[X]$ ist irreduzibel $\iff f(aX + b) \in R[X]$ ist irreduzibel.

  Übung: Hinweis: Betrachte $\sigma \colon R[X] \to R[X], f(X) \mapsto f(aX + b)$ und zeige σ ist Homomorphismus, sogar Isomorphismus.

Reduktionskriterium. Sei R faktoriell, $\mathcal{P}$ Primelement von R. Die Reduktion $\mod \mathcal{P}$

$$R[X] \to {}^{R}\!/_{\mathcal{P}R}[X], f \mapsto f \pmod{\mathcal{P}} =: \bar{f}$$

ist ein Ringhomomorphismus.

Beispiel 3.3.4:

$$3X^3 - 7X^2 + 2X + 5 \in \mathbb{Z}[X]$$
$$\text{mod } 2\colon X^3 + X^2 + 1$$

Proposition 3.3.5:
Sei $f = \sum_{i=0}^{n} a_i X^i \in R[X]$, $\mathcal{P}$ ein Primelement von R mit $a_n \not\equiv 0 \pmod{\mathcal{P}}$. (das heißt $\deg(\bar{f}) = \deg(f)$).

Ist $\bar{f}$ irreduzibel in ${}^{R}\!/_{\mathcal{P}R}[X]$, so ist f irreduzibel in $R[X]$ oder $f = r\tilde{f}$ mit $r \in R, \tilde{f}$ irreduzibel in $R[X]$.

Beispiel 3.3.6:
$f(X) = (3X+1)(X+2)$ ist reduzibel in $\mathbb{Z}[X]$, aber $f \mod 3$ ist irreduzibel über ${}^{\mathbb{Z}}\!/_{3\mathbb{Z}}[X]$.

$f(X) = 4X^2 + 4$ ist reduzibel in $\mathbb{Z}[X]$, aber $f \mod 3 = X^2 + 1$ ist irreduzibel über ${}^{\mathbb{Z}}\!/_{3\mathbb{Z}}[X]$.

Beweis (von Theorem 3.3.5). Sei f reduzibel in $R[X]$ als $f = gh$ mit $\deg g, \deg h \geq 1$. Dann gilt $\bar{f} = \overline{gh} = \bar{g}\bar{h}$ mit $\deg \bar{g}, \deg \bar{h} \geq 1$. Daher sind $\bar{g}, \bar{h}$ keine Einheiten in ${}^{R}\!/_{\mathcal{P}R}[X]$ (denn ${}^{R}\!/_{\mathcal{P}R}$ ist IB, Einheiten in ${}^{R}\!/_{\mathcal{P}R}[X]$ sind die Einheiten von ${}^{R}\!/_{\mathcal{P}R}$). Also ist $\bar{f}$ reduzibel in ${}^{R}\!/_{\mathcal{P}R}[X]$. □

Beispiel 3.3.7:
Zeige, dass $f(X) = X^4 + 3X^3 + X^2 + 6X + 2$ irreduzibel in $\mathbb{Z}[X]$ ist. $f \mod 3 = X^4 + X^2 + 2$. Zeige: $X^4 + X^2 + 2$ ist irreduzibel über ${}^{\mathbb{Z}}\!/_{3\mathbb{Z}}[X]$. $X^4 + X^2 + 2$ hat keine Nullstelle in ${}^{\mathbb{Z}}\!/_{3\mathbb{Z}} \implies$ einzige mögliche Zerlegung $f = gh$ mit $\deg g = \deg h = 2$. Dafür gibt es zwei Möglichkeiten.

$$\left(X^2 + aX + 1\right)\left(X^2 + bX + 2\right) \tag{3.1}$$
$$\left(2X^2 + aX + 1\right)\left(2X^2 + bX + 2\right)$$

3.1 liefert uns folgende Kongruenzen:

$$\begin{cases} a+b \equiv 0 \pmod 3, \\ 2a+b \equiv 0 \pmod 3, \\ 3+ab \equiv 1 \pmod 3. \end{cases}$$

Die ersten beiden implizieren $a \equiv 0 \pmod 3$, ein Widerspruch zur dritten.

Irreduzible Polynome in $\mathbb{C}[X]$. Fundamentalsatz der Algebra: jedes nicht-konstante Polynom aus $\mathbb{C}[X]$ besitz) mindestens eine Nullstelle. Sei also $\deg(f) \geq 1$, Dann $\exists a \in \mathbb{C}$: $f(a) = 0$ und daher $f(X) = (X-a) \cdot q(X)$ mit $q(X) \in \mathbb{C}[X], \deg(q) < \deg(f)$.

Irreduzible Polynome in $\mathbb{R}[X]$. Sei $R[X] \ni f = (X-\alpha_1) \cdots (X-\alpha_n)$ mit $\alpha_i \in \mathbb{C}$, das heißt $f(\alpha_i) = 0, i = 1, \ldots, n$. $f(\alpha_i) = 0 \implies \overline{f(\alpha_i)} = 0 \iff f(\overline{\alpha_i}) = 0$. Schreibe $f(X) = \underbrace{(X-\alpha_1)(X-\bar{\alpha}_1)}_{X^2-(\alpha_1+\overline{\alpha_1})X+\alpha_1\overline{\alpha_1} \in \mathbb{R}[X]} (X-\alpha_2)(X-\bar{\alpha}_2) \cdots (X-\alpha_k)(X-\bar{\alpha}_k)(X-\alpha_{2k+1}) \cdots (X-\alpha_n)$ mit $\alpha_{2k+1}, \ldots, \alpha_n \in \mathbb{R}$. Die irreduziblen Polynome $/\mathbb{R}[X]$ haben Grad 1 oder Grad 2, in letzterem Fall muss die Diskriminante negativ sein.

Beispiel 3.3.8:

$X^4 + 1$ ist reduzibel in $\mathbb{C}[X]$ und in $\mathbb{R}[X]$.

$$X^4 + 1 = \left(X^2 + \sqrt{2}X + 1\right)\left(X^2 - \sqrt{2}X + 1\right)$$

Kapitel 4

Anwendungen in der elementaren Zahlentheorie

4.1 Die Ringe $\mathbb{Z}$ und $\mathbb{Z}/n\mathbb{Z}$

$\mathbb{Z}$ ist ein HIB, $\{m\mathbb{Z} : m \in \mathbb{N}\}$ enthält alle Ideale von $\mathbb{Z}$.

Korollar 4.1.1:
Seien $a_1, \ldots, a_n \in \mathbb{Z} \setminus \{0\}$ mit $\text{ggT}(a_1, \ldots, a_n) = d$. Dann $\exists x_1, \ldots, x_n \in \mathbb{Z}$ mit $a_1x_1 + \cdots + a_nx_n = d$.
$a_1x_1 + \cdots + a_nx_n = s$ hat eine Lösung $\iff d \mid s$.

Beweis. $I := \{a_1x_1 + \cdots + a_nx_n : x_1, \ldots, x_n \in \mathbb{Z}\}$ ist Ideal in $\mathbb{Z}$. $\implies I = m\mathbb{Z}$ und $a_1x_1 + \cdots + a_nx_n = m$ hat Lösung. z.Z.: $d = m$. $a_1, \ldots, a_n \in I$, sodass $m \mid a_i, i = 1, \ldots, n$ und daher $m \mid d$.
$d \mid a_i, i = 1, \ldots, n \implies d \mid a_1x_1 + \cdots + a_nx_n = m$.

Ist $(x_1, \ldots, x_n)$ Lösung von $a_1x_1 + \cdots + a_nx_n = d$, so ist $(x_1\frac{s}{d}, \ldots, x_n\frac{s}{d})$ eine von $a_1x_1 + \cdots + a_nx_n = s$. $d \mid s$, da d stets $a_1x_1 + \cdots + a_nx_n$ teilt. □

$n = 2$**:** $a, b \in \mathbb{Z} \setminus \{0\}, \text{ggT}(a, b) = d, c \in Z.(x_0, y_0)$ eine Lösung von $ax + by = c$. Dann sind alle Lösungen von $ax + by = c$ von der Gestalt $(x_0 + \frac{b}{d}t, y_0 - \frac{a}{d}t)$ für ein $t \in \mathbb{Z}$.

Beweis. Das sind Lösungen (einsetzen!).

$$\left.\begin{aligned} ax + by &= c \\ ax_0 + by_0 &= c \end{aligned}\right\} \implies a(x - x_0) + b(y - y_0) = 0 \tag{4.1}$$
$$\iff a(x - x_0) = -b(y - y_0)$$
$$\iff \frac{a}{d}(x - x_0) = \frac{-b}{d}(y - y_0)$$

Es folgt: $\frac{b}{d} \mid (x - x_0)$, das heißt $\exists t \in \mathbb{Z}: (x - x_0) = \frac{b}{d}t$. Durch Einsetzen in 4.1 ergibt sich $y - y_0 = \frac{-a}{d}t$. Daraus folgt die Behauptung. □

Sei R ein kommutativer Ring. Ist $\equiv$ eine Kongruenzrelation, so ist $\{a \in R \colon a \equiv 0\}$ ein Ideal von R. Ist I ein Ideal von R, so ist durch $a \equiv b \pmod{I} \iff a - b \in I$ eine Kongruenzrelation definiert. Die Zuordnungen sind invers zueinander.

$\mathbb{Z}/m\mathbb{Z}$ ist Körper $\iff m \in \mathbb{P}$.

Beweis. Ist $m \notin \mathbb{P}$, so hat $\mathbb{Z}/m\mathbb{Z}$ Nullteiler, diese sind nicht invertierbar. Umgekehrt, bei $a + m\mathbb{Z} \neq 0 + m\mathbb{Z}$ betrachten wir $au + mv = 1$. Das hat eine Lösung $(u, v) \in \mathbb{Z} \times \mathbb{Z}$, da $\operatorname{ggT}(a, m) = 1$. $\implies (a + m\mathbb{Z})(u + m\mathbb{Z}) = 1 + m\mathbb{Z}$. □

4.2 Die Struktur von $\left(\mathbb{Z}/m\mathbb{Z}\right)^*$

$\left(\mathbb{Z}/m\mathbb{Z}\right)^*$ heißt prime Restklassengruppe mod m.

$$\left|\left(\mathbb{Z}/m\mathbb{Z}\right)^*\right| =: \varphi(m) \qquad \text{„Eulersche } \varphi\text{-Funktion“}$$

φ ist multiplikativ $:\iff \varphi(mn) = \varphi(m)\varphi(n)$ falls $(m, n) = 1$. Es gilt: R, S seien KREs. Dann ist $(R \times S)^* = R^* \times S^*$.

Lemma 4.2.1:
Ist $f \colon R \to S$ ein Ringisomorphismus, so gilt:

$$f(R^*) = S^*$$

Beweis. Sei $x \in R^*$. Dann existiert $y \in R$ mit $xy = 1_R$.

$$1_S = f(1_R) = f(xy) = f(x)f(y) \implies f(x) \in S^*$$

Die Umkehrung folgt durch Anwendung dieser Überlegung auf $f^{-1} \colon S \to R$. □

Korollar 4.2.2:
Sei $\operatorname{ggT}(m, n) = 1$. Dann gilt:

$$f^* \colon \left(\mathbb{Z}/mn\mathbb{Z}\right)^* \to \left(\mathbb{Z}/m\mathbb{Z}\right)^* \times \left(\mathbb{Z}/n\mathbb{Z}\right)^*, x + mn\mathbb{Z} \mapsto (x + m\mathbb{Z}, x + n\mathbb{Z})$$

ist ein Gruppenisomorphismus. Insbesondere $\varphi(mn) = \varphi(m)\varphi(n)$.

Beweis. $\mathbb{Z}/mn\mathbb{Z} \cong \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$ nach Chinesischem Restsatz 2.5.22 ($(m, n) = 1$) Es folgt:

$$\begin{aligned} \left(\mathbb{Z}/mn\mathbb{Z}\right)^* &\cong \left(\mathbb{Z}/m\mathbb{Z}\right)^* \times \left(\mathbb{Z}/n\mathbb{Z}\right)^* && \text{nach dem Theorem 4.2.1.} \\ &= \left(\mathbb{Z}/m\mathbb{Z}\right)^* \times \left(\mathbb{Z}/n\mathbb{Z}\right)^* \end{aligned}$$

□

Korollar 4.2.3:
Für $m \in \mathbb{N}$ gilt:

$$\varphi(m) = m \prod_{p|m} \left(1 - \frac{1}{p}\right).$$

Beweis. Für $m = 1$: ✓
Sonst sei $m = p_1^{\alpha_1} \cdot \cdots \cdot p_k^{\alpha_k} \implies \varphi(m) = \varphi(p_1^{\alpha_1}) \cdots \varphi(p_k^{\alpha_k})$.
Behauptung: $\varphi(p^\alpha) = p^\alpha - p^{\alpha-1}$ ($p^{\alpha-1}$ = #Vielfache von p zwischen 1 und p^α.)
$\implies \varphi(m) = \left(p_1^{\alpha_1} - p_1^{\alpha_1-1}\right) \cdots (p^{\alpha_k} - p^{\alpha_k-1}) = p_1^{\alpha_1}\left(1 - \frac{1}{p_1}\right) \cdots p_k^{\alpha_k}\left(1 - \frac{1}{pk}\right) =$
$m\left(1 - \frac{1}{p_1}\right) \cdots \left(1 - \frac{1}{p_k}\right) \implies$ Behauptung.
Es ist $|\mathbb{Z}_m^*| = \varphi(m)$. Für $a \in \mathbb{Z}_m^*$ gilt daher $a^{\varphi(m)} = a^{|\mathbb{Z}_m^*|} = 1$.
$a^{\varphi(m)} \equiv 1 \pmod{m}$ „kleiner Satz von Fermat“
$m = p \in \mathbb{P}. a^{p-1} \equiv 1 \pmod{m}$ für $(a, m) = 1$ oder $a^p \equiv a \pmod{m}$ für beliebige m. □

Definition 4.2.4:
Sei $m \in \mathbb{N}$ eine Zahl für die $\left(\mathbb{Z}/m\mathbb{Z}\right)^*$ zyklisch ist und g ein Erzeuger von $\left(\mathbb{Z}/m\mathbb{Z}\right)^*$.
Dann heißt g Primitivwurzel mod m.

Behauptung: Falls es eine Primitivwurzel (PW) mod m gibt, so gibt es $\varphi(\varphi(m))$ viele.

Beweis.

$$\left|\left(\mathbb{Z}/m\mathbb{Z}\right)^*\right| = \varphi(m).$$

Ist $\langle g \rangle = \left(\mathbb{Z}/m\mathbb{Z}\right)^*$, so ist $\langle g^s \rangle = \left(\mathbb{Z}/m\mathbb{Z}\right)^* \iff \text{ggT}\left(s, \underbrace{\left|\left(\mathbb{Z}/m\mathbb{Z}\right)^*\right|}_{\varphi(m)}\right) = 1$ □

Behauptung: $\left(\mathbb{Z}/p\mathbb{Z}\right)^*$ ist für $p \in \mathbb{P}$ zyklisch. (Denn $\mathbb{Z}/p\mathbb{Z}$ ist Körper und $\left(\mathbb{Z}/p\mathbb{Z}\right)^* \subseteq \left(\mathbb{Z}/p\mathbb{Z}\right)^*$)
Es gilt sogar: $\left(\mathbb{Z}/p^m\mathbb{Z}\right)^*$ ist zyklisch.
Sei g eine PW mod p.

Lemma 4.2.5:
Es gilt: $g^{p-1} \not\equiv 1 \pmod{p^2}$ oder $(g+p)^{p-1} \not\equiv 1 \pmod{p^2}$

Beweis. Angenommen $g^{p-1} \equiv 1 \equiv (g+p)^{p-1} \pmod{p^2}$.
$(g+p)^{p-1} = g^{p-1} + p(p-1)g^{p-2} + \underbrace{\cdots}_{\equiv 0 \pmod{p^2}} \pmod{p^2}$. $(g+p)^{p-1} \equiv 1 \pmod{p^2} \wedge g^{p-1} \equiv 1 \pmod{p^2} \implies p(p-1)g^{p-2} \equiv 0 \pmod{p^2}$. Das hieße $(p-1)g^{p-2} \equiv 0 \pmod{p} \implies g^{p-2} \equiv 0 \pmod{p}$. g ist aber PW. ↯

Satz 4.2.6:
Sei $p > 2$ prim, g Primitivwurzel $\mod p$ für die $g^{p-1} \not\equiv 1 \pmod{p^2}$. Dann ist g Primitivwurzel $\mod p^s$ für alle $s \geq 1$.

Beweis. Wir zeigen zunächst durch Induktion, dass $g^{(p-1)\cdot p^{s-2}} \not\equiv 1 \pmod{p^s}$ $\forall s \geq 2$.
Induktionsanfang: $s = 2$ nach Voraussetzung erfüllt. Sei bereits gezeigt, dass $g^{(p-1)\cdot p^{s-2}} \not\equiv 1 \pmod{p^s} = 1 + ap^{s-1}$ mit $p \nmid a$.

$$g^{(p-1)\cdot p^{s-1}} = (1+ap^{s-1})^p = 1 + pap^{s-1} + \frac{r(p-1)}{2}a^2p^{2s-2} + \underbrace{\sum_{i=3}^{p}\binom{p}{i}\cdot a^i p^{(s-1)i}}_{\equiv 0 \pmod{p^{s+1}}\, s\geq 2, i\geq 3}$$

$$\equiv 1 + ap^s + \underbrace{\frac{p-1}{2}\cdot a^2 p^{2s-1}}_{\equiv 0 \pmod{p^{s+1}}\, s\geq 2} \equiv 1 + ap^s \pmod{p^{s+1}} \not\equiv 1 \pmod{p^{s+1}} \quad \square$$

$\operatorname{ord}_{p^s}(g) \coloneqq e$ $e \mid \varphi(p^s) = (p-1)p^{s-1}$. Zudem gilt: g PW $\mod p \implies g^{p-1} \equiv 1 \pmod{p} \implies p-1 \mid e$. Insgesamt $\frac{e}{p-1}p^{s-1} \implies \frac{e}{p-1} = p^k$ mit $k \leq s-1$. Wäre $\frac{e}{p-1} \leq s-2$, so folgte $g^{(p-1)\cdot p^{s-2}} \equiv 1 \pmod{p^s}$, ↯ zu Theorem 4.2.6
Also gilt $k = s-1$ und damit $e = (p-1)p^{s-1} = \varphi(p^s) \implies g$ Primitivwurzel.

Korollar 4.2.7:
Sei $p > 2$ prim. Dann ist $\left(\mathbb{Z}/p^k\mathbb{Z}\right)^*$ zyklisch $\forall k \geq 1$.

Korollar 4.2.8:
Sei $p > 2$. Ist g ungerade PW $\mod p^k$, so ist g auch PW $\mod 2p^k$.

Beweis.

$$\operatorname{ord}_{2p^k}(g) = \operatorname{kgV}(\operatorname{ord}_2(g), \operatorname{ord}_{p^k}(g)) = \operatorname{ord}_{p^k}(g) = \varphi(p^k) = \varphi(2p^k) \quad \square$$

Weiters gilt: Falls g eine gerade PW $\mod p^k$ ist, so ist $g + p^k$ eine ungerade! $\implies \left(\mathbb{Z}/2p^k\mathbb{Z}\right)^*$ ist zyklisch.

Beispiel 4.2.9:

Sei nun $p = 2$, es gilt:

- $\operatorname{ord}_{2^k}(5) = 2^{k-2} = \frac{\varphi(2^k)}{2}$
- Für $k \geq 2$ ist $\mathfrak{Z} := \{(-1)^i 5^j : i \in \{0,1\}, 0 \leq j < 2^{k-2}\}$ ist eine primes Restsystem $\mod 2^k$.

Satz 4.2.10:

Sei $k \geq 2$, dann ist $f : \overbrace{\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2^{k-2}\mathbb{Z}}^{\text{additive Gruppen}} \to \left(\mathbb{Z}/2^k\mathbb{Z}\right)^*$, $(i,j) \mapsto (-1)^i 5^j + 2^k\mathbb{Z}$ ein Isomorphismus.

Satz 4.2.11 (Satz von Gauß):

Sei $m \in \mathbb{N}$. $\left(\mathbb{Z}/m\mathbb{Z}\right)^*$ ist zyklisch $\iff m = p^k \vee m = 2p^k$ für ungerade Primzahl $p, k \geq 1$ oder $m = 1, 2, 4$

Beweis. Angenommen $\left(\mathbb{Z}/m\mathbb{Z}\right)^*$ sei zyklisch, $m \neq p^k, p \neq 2p^k, m \neq 2^k$. $\implies \exists$ ungerade Primzahl q mit $m = q^n \cdot m'$ mit $\operatorname{ggT}(q, m') = 1, m' > 1$. Sei also a mit $\operatorname{ggT}(a, m) = 1$, das heißt $a \in \left(\mathbb{Z}/m\mathbb{Z}\right)^*$.

$$\operatorname{ord}_m(a) = \operatorname{kgV}(\operatorname{ord}_{q^n}(a), \operatorname{ord}_m(a)) \leq \operatorname{kgV}(\varphi(q^n), \varphi(m')) > \varphi(q^n) \cdot \varphi(m'),$$

da $\varphi(q^n) \equiv 0 \pmod 2, \varphi(m') \equiv 0 \pmod 2$, da $4 \mid m'$ falls m gerade.

$$\operatorname{ord}_m(a) > \varphi(q^n) \cdot \varphi(m') = \varphi(q^n \cdot m') = \varphi(m) \qquad \square$$

Sei $m = 2^{\alpha_1} p_2^{\alpha_2} \cdots p_k^{\alpha_k}$. Dann gilt

$$\text{für } \begin{cases} \alpha_1 \leq 2: & \left(\mathbb{Z}/m\mathbb{Z}\right)^* \cong \left(\mathbb{Z}/2^{\alpha_1}\mathbb{Z}\right)^* \times \left(\mathbb{Z}/p_2^{\alpha_2}\mathbb{Z}\right)^* \times \cdots \times \left(\mathbb{Z}/p_k^{\alpha_k}\mathbb{Z}\right)^* \\ \alpha_1 > 2: & \left(\mathbb{Z}/m\mathbb{Z}\right)^* \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2^{k-2}\mathbb{Z} \times \left(\mathbb{Z}/p_2^{\alpha_2}\mathbb{Z}\right)^* \times \cdots \times \left(\mathbb{Z}/p_k^{\alpha_k}\mathbb{Z}\right)^* \end{cases}$$

und alle auftretenden Faktoren sind zyklische Gruppen.

4.3 Algebraische Kongruenzen

Kongruenzen vom Typ $f(x) \equiv 0 \pmod{m}$, wobei $f(x) = \sum_{i=0}^{n} a_i x^i, a_i \in \mathbb{Z}$.

Satz 4.3.1 (Satz von Lagrange):
Sei $p \in \mathbb{P}, f(x) \equiv 0 \pmod{p}$ eine algebraische Kongruenz vom Grad n. Dann hat f höchstens n Nullstellen $\mod p$.

Beweis. $p \in \mathbb{P} \implies {}^{\mathbb{Z}}\!/_{p\mathbb{Z}}$ ist Körper $\implies {}^{\mathbb{Z}}\!/_{p\mathbb{Z}}[X]$ ist IB $\implies f \in {}^{\mathbb{Z}}\!/_{p\mathbb{Z}}[X]$ vom Grad n hat höchstens n Nullstellen. □

Proposition 4.3.2:
Sei $f \in \mathbb{Z}[X], f \neq 0, L_f(m)$ die Anzahl der $\mod m$ inkongruenten Lösungen von $f(x) \equiv 0 \pmod{m}$. Dann ist L_f multiplikativ, das heißt $L_f(mn) = L_f(m) \cdot L_f(n)$ falls $(m, n) = 1$.

Beweis. Für $k \in \mathbb{N}$ sei A_k die Menge der Restklassen $\bar{x} \mod k$, für die $f(\bar{x}) \equiv 0 \pmod{k}$ (sodass $L_f(k) = |A_k|$). Wir wissen: $g\colon {}^{\mathbb{Z}}\!/_{mn\mathbb{Z}} \to {}^{\mathbb{Z}}\!/_{m\mathbb{Z}} \times {}^{\mathbb{Z}}\!/_{n\mathbb{Z}}$,
$x + mn\mathbb{Z} \mapsto (x + m\mathbb{Z}, x + n\mathbb{Z})$ ist ein Isomorphismus.

$g(A_{mn}) \overset{\text{z.z.}}{=} A_m \times A_n$.

Ist $f(x) \equiv 0 \pmod{mn}$, so folgt $f(x) \equiv 0 \pmod{m}$ und $f(x) \equiv 0 \pmod{n} \implies g(A_{mn}) \subseteq A_m \times A_n$.

Umgekehrt: Sei $f(x) \equiv 0 \pmod{m}, f(y) \equiv 0 \pmod{n}$ (also $(x, y) \in A_m \times A_n$). Nach dem Chinesischen Restsatz 2.5.22 gibt es mit $(m, n) = 1$ eine Restklasse $z \mod m \cdot n$ mit $z \equiv x \pmod{m}, z \equiv y \pmod{n}$. Damit ist $f(z) \equiv 0 \pmod{mn} \implies g(A_{mn}) \supseteq A_m \times A_n$.

$$L_f(mn) = |A_m n| = |g(A_{mn})| = |A_m \times A_n| = |A_m| \cdot |A_n| = L_f(m) \times L_f(n)$$ □

Anwendung auf Kongruenzen $f(x) \equiv 0 \pmod{m}, m = p_1^{\alpha_1} \cdots p_k^{\alpha_k}$.

$$f(x) \equiv 0 \pmod{m} \iff f(x) \equiv 0 \pmod{p_i^{\alpha_i}}\ i = 1, \ldots, k$$

Beispiel 4.3.3:
Sei $f(x) = x^3 + 19x^2 - x + 2 \equiv 0 \pmod{21}$.

$$f(x) \equiv 0 \pmod{3} \quad \text{hat Lösungen } 1, 2$$
$$f(x) \equiv 0 \pmod{7} \quad 1, 2, 6$$

$\longrightarrow$ Bestimme alle $z \mod 21$ mit $\begin{cases} z \equiv a_i \pmod{3} & a_i \in \{1, 2\} \\ z \equiv b_j \pmod{7} & b_j \in \{1, 2, 6\} \end{cases}$ Lösungen mod 21 sind: $1, 2, 8, 13, 16, 20$.

$f(x) \equiv 0 \pmod{p^\alpha}, \alpha > 1$

1. Schritt: Löse $f(x) \equiv 0 \pmod{p}$ durch Einsetzen. Seien die Lösungen von $f(x) \equiv 0 \pmod{p^e}$ bekannt für ein $1 \leq e \leq \alpha$. Bezeichne die Menge der $\bmod p^e$ inkongruenten Lösungen mit A_e. Angenommen $x_0 \in A_e \iff f(x_0) \equiv 0 \pmod{p^e} \implies f(x_0) \equiv 0 \pmod{p^{e-1}} \implies x_0 \equiv a \pmod{p^{e-1}}$, also $x_0 = a + yp^{e-1}$.

$$f(X) \coloneqq \sum_{k=0}^{n} a_k X^k \implies f(X) = \sum_{k=0}^{n} \frac{f^{(k)}(a)}{k!}(X-a)^k$$
$$\implies f(x) - f(a) = \underbrace{\left(\sum_{k=1}^{n} \frac{f^{(k)}(a)}{k!}(X-a)^{k-1}\right)}_{q(X)}(X-a)$$

Dann ist $q(a) = f'(a)$. Setze x_0 für X und betrachte die resultierende Kongruenz $\bmod p^e$:

$$-f(a) \equiv (y \cdot p^{e-1})q(x_0) \pmod{p^e} \implies \frac{-f(a)}{p^{e-1}} \equiv y \cdot q(x_0) \pmod{p}$$
$$p^{e-1} \equiv y \cdot q(a) \equiv y \cdot f'(a) \pmod{p}$$

Insgesamt:

$$\frac{-f(a)}{p^{e-1}} \equiv y f'(a) \pmod{p}. \tag{4.2}$$

Kongruenz vom Typ:

$$b \equiv ay \pmod{m} \text{ lösbar} \iff ay - b = \lambda m$$
$$\iff ay - \lambda m = b \text{ lösbar}$$
$$\iff \mathrm{ggT}(a, m) \mid b$$

3 Fälle:

1. $f'(a) \not\equiv 0 \pmod{p}$. Dann ist $\mathrm{ggT}(f'(a), p) = 1$ und daher die Kongruenz eindeutig lösbar. Dann hat a genau eine Fortsetzung $a + yp^{e-1}$ in A_e, wobei y die eindeutige Lösung von **??** ist.
2. $f'(a) \equiv 0 \pmod{p} \wedge f(a) \equiv o \pmod{p}$. Dann ist jedes $y \in \mathbb{Z}/p\mathbb{Z}$ Lösung von **??** und a hat p Fortsetzungen zu Lösungen $a + yp^{e-1}$ in A_e.
3. $f'(a) \equiv 0 \pmod{p} \wedge f(a) \not\equiv 0 \pmod{p}$. Dann hat a keine Fortsetzung in A_e.

Beispiel 4.3.4:

$$f(X) = X^3 + 3X^2 + 4X + 8,\ f(X) \equiv 0 \pmod{16}$$
$$f'(X) = 3X^2 + 6X + 4 \equiv X^2 \equiv X \pmod{2}$$

mod 2**:** 0, 1 sind Lösungen.

mod 4**:**

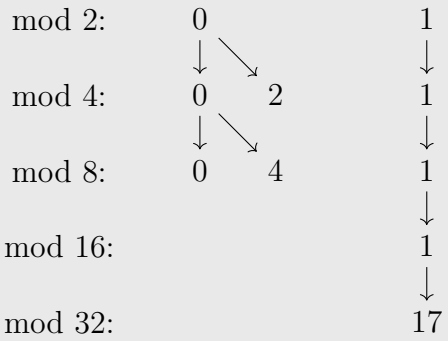
- Fortsetzungen von 0: $\frac{-f(0)}{2} \equiv 0 \equiv y \cdot 0 \pmod 2 \implies$ Fortsetzungen von 0 sind $y = 0 + 0 \cdot 2$ und $0 + 1 \cdot 2$, also 0, 2.
- Fortsetzungen von 1: $\frac{-f(1)}{2} \equiv 0 \equiv 1 \pmod 2 \implies$ Fortsetzung von 1 ist $1 + 0 \cdot 2 = 1$.

$\implies$ Lösungen mod 4: $0, 1, 2$.

mod 8**:**

- Fortsetzung von 0: $\frac{-f(0)}{4} \equiv 0 \equiv y \cdot 0 \pmod 2 \implies$ Fortsetzungen von 0 sind $0 + 0 \cdot 4 = 0$ und $0 + 1 \cdot 4 = 4$.
- Fortsetzung von 1: $\frac{-f(1)}{4} \equiv 0 \equiv y \cdot 1 \pmod 2 \implies$ Fortsetzung von 1 ist $1 + 0 \cdot 4 = 1$.
- Fortsetzung von 2: $\frac{-f(2)}{4} \equiv 1 \equiv y \cdot 0 \pmod 2 \implies \nexists$ Fortsetzung von 2.

mod 16**:** Übung, nur 1 hat die Fortsetzung $1 + 0 \cdot 8 = 1$.



4.4 Potenzreste & quadratische Reste

Sei nun $f(X) = X^n - a$. Wir können $X^n \equiv a \pmod m$ reduzieren zu $X^n \equiv a \pmod{p^\alpha}$ für Primzahlpotenzen. Wir beschränken uns auf den Fall $\text{ggT}(a, p) = 1 \implies a \in \left(\mathbb{Z}/p^\alpha\mathbb{Z}\right)^*$ und wir wissen $\left(\mathbb{Z}/p^\alpha\mathbb{Z}\right)^*$ ist zyklisch. $\exists$ PW mod p^α!

Sei $m \in \mathbb{N}$ mit $\left(\mathbb{Z}/m\mathbb{Z}\right)^*$ zyklisch. Sei g eine PW mod m.

Definition 4.4.1:
Für $a \in \left(\mathbb{Z}/m\mathbb{Z}\right)^*$ sei $I_g(a) \in \{0, 1, \ldots, \varphi(m) - 1\}$ so gewählt, dass $a \equiv g^{I_g(a)} \pmod{m}$. Dann heißt die Abbildung

$$I_g \colon \left(\mathbb{Z}/m\mathbb{Z}\right)^* \to \mathbb{Z}/\varphi(m)\mathbb{Z}, a \mapsto I_g(a)$$

zahlentheoretischer Logarithmus (zur Basis g).

Beispiel 4.4.2:
$m = 7, g = 3$.

$a \in \left(\mathbb{Z}/7\mathbb{Z}\right)^*$:	1	2	3	4	5	6
$I_3(a) \in \mathbb{Z}/6\mathbb{Z}$:	0	2	1	4	5	3

Es gilt: $g^i \equiv g^j \pmod{m} \iff i \equiv j \pmod{\varphi(m)}$. (Übung, Satz von Fermat)

Proposition 4.4.3:
Für $a, b \in \left(\mathbb{Z}/m\mathbb{Z}\right)^*, g$ PW $\mod m$ gilt:

$$I_g(ab) \equiv I_g(a) + I_g(b) \pmod{\varphi(m)}$$

Beweis.

$$g^{I_g(ab)} \equiv ab \equiv g^{I_g(a)} \cdot g^{I_g(b)} \equiv g^{I_g(a)+I_g(b)} \pmod{m}$$
$$I_g(ab) \equiv I_g(a) + I_g(b) \pmod{\varphi(m)}$$

Durch Induktion: $I_g(a^n) = nI_g(a)$. □

Beispiel 4.4.4 (Anwendungen):

1. $ax \equiv b \pmod{m}$ mit $\mathrm{ggT}(ab, m) = 1, \exists$ PW $g \pmod{m}$.

$$\iff I_g(ax) \equiv I_g(b) \pmod{\varphi(m)}$$
$$\iff I_g(a) + I_g(x) \equiv I_g(b) \pmod{\varphi(m)}$$
$$\iff I_g(x) \equiv I_g(b) - I_g(a) \pmod{\varphi(m)}$$

Beispiel: $2x \equiv 5 \pmod 7, g = 3$

$$\begin{aligned} &\iff I_3(x) \equiv I_3(5) - I_3(2) \pmod 6 \\ &\iff I_3(x) \equiv 3 \pmod 6 \iff x \equiv 6 \pmod 7 \end{aligned}$$

2. $ax^n \equiv b \pmod m$ mit selben Voraussetzungen wie bei 1.

$$\begin{aligned} &\iff I_g(ax^n) \equiv I_g(b) \pmod{\varphi(m)} \\ &\iff nI_g(x) \equiv I_g(b) - I_g(a) \pmod{\varphi(m)} \end{aligned}$$

und diese ist genau dann lösbar, wenn

$$\mathrm{ggT}(\varphi(m), n) \mid (I_g(b) - I_g(a)).$$

Beispiel:

$$\begin{aligned} 2x^5 \equiv 6 \pmod 7 &\iff 5I_3(x) \equiv I_3(6) - I_3(2) \pmod 6 \\ &\iff 5I_3(x) \equiv 1 \pmod 6 \\ &\iff I_3(x) \equiv 5 \pmod 6 \\ &\iff x \equiv 5 \pmod 7 \end{aligned}$$

3. $ab^x \equiv c \pmod m, \mathrm{ggT}(abc, m) = 1$

$$\begin{aligned} &\iff I_g(ab^x) \equiv I_g(c) \pmod{\varphi(m)} \\ &\iff xI_g(b) \equiv I_g(c) - I_g(a) \pmod{\varphi(m)} \end{aligned}$$

und diese Kongruenz ist lösbar, genau dann wenn

$$\mathrm{ggT}(I_g(b), \varphi(m)) \mid (I_g(c) - I_g(a)).$$

Beispiel:

$$\begin{aligned} 2 \cdot 3^x \equiv 5 \pmod 7 &\iff XI_3(3) \equiv I_3(5) - I_3(2) \pmod 6 \\ &\iff X \equiv 3 \pmod 6 \end{aligned}$$

Definition 4.4.5:
Seien $m \in \mathbb{N}, a \in \left(\mathbb{Z}/m\mathbb{Z}\right)^*$. a heißt n-ter Potenzrest mod m, wenn $X^n \equiv a \pmod m$ lösbar ist, das heißt a ist n-te Potenz in $\left(\mathbb{Z}/m\mathbb{Z}\right)^*$. Für $n = 2$ heißt a quadratischer Rest.

Satz 4.4.6:
Seien $m, n, d \in \mathbb{N}$ mit $d = \text{ggT}(n, \varphi(m)), a \in Z$ mit $\text{ggT}(a, m) = 1$. Ist $\left(\mathbb{Z}/m\mathbb{Z}\right)^*$ zyklisch, so ist a genau dann n-ter Potenzrest $\mod m$, wenn $a^{\frac{\varphi(m)}{d}} \equiv 1 \pmod m$. Die Kongruenz $X^n \equiv a \pmod m$ hat genau d inkongruente Lösungen $\mod m$.

Beweis.

$$\begin{aligned}
X^n \equiv a \pmod m &\iff n\underbrace{I_g(X)}_{y} \equiv I_g(a) \pmod{\varphi(m)} \text{ lösbar } (g \text{ eine PW } \mod m) \\
&\iff d \mid I_g(a) (\text{und die Kongruenz hat genau } d \text{ Lösungen}) \\
&\iff \varphi(m) \mid \frac{\varphi(m) I_g(a)}{d} (\text{beide Seiten mit } \frac{\varphi(m)}{d} \text{ multipliziert}) \\
&\iff g^{\frac{I_g(a)\varphi(m)}{d}} \equiv -1 \pmod m \\
&\iff \underbrace{\left(g^{I_g(a)}\right)^{\frac{\varphi(m)}{d}}}_{a} \equiv 1 \pmod m.
\end{aligned}$$

□

Satz 4.4.7:
Seien $m, n \in \mathbb{N}, d \coloneqq \text{ggT}(m, n)$. Dann bilden die n-ten Potenzreste $a \in \left(\mathbb{Z}/m\mathbb{Z}\right)^*$ eine Untergruppe von $\left(\mathbb{Z}/m\mathbb{Z}\right)^*$ ($\coloneqq P_n$). Ist $\left(\mathbb{Z}/m\mathbb{Z}\right)^*$ zyklisch, so ist $|P_n| = \frac{\varphi(n)}{d}$.

Beweis. Seien a, b n-te Potenzreste, das heißt $\exists x, y \colon x^n \equiv a \pmod m, y^n \equiv b \pmod m$. Dann ist $(xy)^n \equiv ab \pmod n$ also ab n-ter Potenzrest. Darüber hinaus gilt: $x^n \equiv a \pmod m \implies \text{ggT}(x, m) = 1$, das heißt x ist invertierbar in $\mathbb{Z}/m\mathbb{Z}$, also in $\left(\mathbb{Z}/m\mathbb{Z}\right)^*$.

$$\left(x^{-1}\right)^n \equiv a^{-1} \pmod m.$$

Ist $\left(\mathbb{Z}/m\mathbb{Z}\right)^*$ zyklisch, so existiert eine Primitivwurzel $g \pmod m$.
$a^{\frac{\varphi(n)}{d}} \equiv 1 \pmod m \iff \frac{\varphi(m)}{d} I_g(a) \equiv 0 \pmod{\varphi(m)}$, diese Kongruenz hat genau $\text{ggT}(\frac{\varphi(m)}{d}, \varphi(m)) = \frac{\varphi(m)}{d}$ Lösungen. □

Korollar 4.4.8:
Wähle $m = p, p \in \mathbb{P}$ ungerade, $n = 2$. $\left(\mathbb{Z}/p\mathbb{Z}\right)^*$ enthält genau $\frac{p-1}{2}$ quadratische Reste (QR) und $\frac{p-1}{2}$ quadratische Nichtreste (QNR)

Definition 4.4.9:
Sei $p \neq 2$ prim, $a \in \mathbb{Z}$ mit $(a,p) = 1$.

$$\left(\frac{a}{p}\right) := \begin{cases} 1 & \text{falls } a \text{ QR} \mod p \\ -1 & \text{falls } a \text{ QNR} \mod p \end{cases} \text{ heißt } \textit{Legendre-Symbol}$$

Bemerkung 4.4.10:
Falls $a \equiv a' \pmod p \implies \left(\frac{a}{p}\right) = \left(\frac{a'}{p}\right)$.

Satz 4.4.11 (Eulersches Kriterium):
Sei $p \neq 2$ prim, $(a,p) = 1$. Dann gilt: $\left(\frac{a}{p}\right) \equiv a^{\frac{p-1}{2}} \pmod p$

Beweis. Wir wissen bereits $\left(\frac{a}{p}\right) = 1 \iff a \text{ QR} \mod p \iff a^{\frac{p-1}{2}} \equiv 1 \pmod p$. Ist a QNR, so ist $a^{\frac{p-1}{2}} \not\equiv \pmod p$, aber $a^{p-1} \equiv 1 \pmod p$ (kleiner Fermat).

$$\underbrace{a^{p-1} - 1}_{\equiv 0 \pmod p} \equiv \underbrace{\left(a^{\frac{p-1}{2}} - 1\right)}_{\not\equiv 0 \pmod p} \cdot \left(a^{\frac{p-1}{2}} + 1\right) \pmod p \implies a^{\frac{p-1}{2}} + 1 \equiv 0 \pmod p.$$

□

Korollar 4.4.12:
Seien $a_1, \ldots, a_k \in \mathbb{Z}, (a_1, \ldots, a_k) = 1$. Dann gilt

$$\left(\frac{a_1 \cdots a_k}{p}\right) = \left(\frac{a_1}{p}\right) \cdots \left(\frac{a_k}{p}\right)$$

Beweis. Einsetzen ins Eulersche Kriterium. □

Korollar 4.4.13 (erster Ergänzungssatz):

$$\left(\frac{-1}{p}\right) = (-1)^{\frac{p-1}{2}}$$

Daher gilt $\left(\frac{-1}{p}\right) = 1 \iff p \equiv 1 \pmod 4$.

Satz 4.4.14 (Lemma von Gauß):
Sei $p \neq 2$ prim, $(a,p) = 1$). Seien r_i die Reste bei Division mit absolut kleinstem Rest $a \cdot i$ durch $p, 1 \leq i \leq \frac{p-1}{2}$. Dann gilt: $\left(\frac{a}{p}\right) = \operatorname{sgn}(r_1) \cdot \operatorname{sgn}(r_2) \cdots \operatorname{sgn}\left(r_{\frac{p-1}{2}}\right)$.

Beweis. Wir behaupten zunächst: $\left\{|r_1|, \ldots, \left|r_{\frac{p-1}{2}}\right|\right\} = \left\{1, \ldots, \frac{p-1}{2}\right\}$.
$|r_i| \leq \frac{p}{2}, r_i \neq 0, r_i \neq \frac{p}{2}$ weil $(a,p) = 1$ beziehungsweise $p \neq 2$. Angenommen $|r_i| = |r_j| \implies r_i = \pm r_j \implies a \cdot i \equiv \pm a \cdot j \pmod p \implies i \geq I_J \pmod p \implies i \equiv j \pmod p$ wegen $1 \leq i, j \leq \frac{p-1}{2}$.

$$\begin{aligned}
\left(\frac{p-1}{2}\right)! \cdot \operatorname{sgn}(r_1) \cdots \operatorname{sgn}\left(r_{\frac{p-1}{2}}\right) &= |r_1| \cdots \left|r_{\frac{p-1}{2}}\right| \cdot \operatorname{sgn}(r_1) \cdots \operatorname{sgn}\left(r_{\frac{p-1}{2}}\right) \\
&= r_1 \cdots r_{\frac{p-1}{2}} \\
&\equiv (a \cdot 1) \cdots \left(a \cdot \frac{p-1}{2}\right) \pmod p \\
&\equiv a^{\frac{p-1}{2}} \cdot \left(\frac{p-1}{2}\right)! \pmod p \\
\implies \operatorname{sgn}(r_1) \cdots \operatorname{sgn}\left(r_{\frac{p-1}{2}}\right) &\equiv a^{\frac{p-1}{2}} \equiv \left(\frac{a}{p}\right) \pmod p
\end{aligned}$$

□

Korollar 4.4.15 (zweiter Ergänzungssatz):

$$\left(\frac{2}{p}\right) = (-1)^{\frac{p^2-1}{8}} = \begin{cases} 1 & \text{falls } p \equiv 1 \vee 7 \pmod 8 \\ -1 & \text{falls } p \equiv 3 \vee 5 \pmod 8 \end{cases}$$

Beweis.

$p = 8k+1$:	$r_{2k+1}, \ldots, r_{4k}$	sind negativ, das sind	$2k$	Stück.
$p = 8k+3$:	$r_{2k+1}, \ldots, r_{4k}, r_{4k+1}$	sind negativ, das sind	$2k+1$	Stück.
$p = 8k+5$:	$r_{2k+2}, \ldots, r_{4k+2}$	sind negativ, das sind	$2k+1$	Stück.
$p = 8k+7$:	$r_{2k+2}, \ldots, r_{4k+3}$	sind negativ, das sind	$2k+2$	Stück.

□

Satz 4.4.16 (quadratisches Reziprozitätsgesetz):
Seien p, q ungerade Primzahlen. Dann gilt:

$$\left(\frac{p}{q}\right) \cdot \left(\frac{q}{p}\right) = (-1)^{\frac{p-1}{2} \cdot \frac{q-1}{2}}$$

Beispiel 4.4.17:

- $\left(\frac{53}{37}\right) = \left(\frac{16}{37}\right) = \left(\frac{2}{37}\right) = 1$
- $$\left(\frac{223}{\underbrace{997}_{\equiv 1 \pmod 4}}\right) = \left(\frac{997}{223}\right) = \left(\frac{118}{223}\right) = (-1)^{\frac{223-1}{2}} \cdot \left(\frac{118}{223}\right) =$$
$$= -\left(\frac{2}{223}\right)\left(\frac{59}{223}\right) = -\left(\frac{\overbrace{59}^{\equiv 3 \pmod 4}}{\underbrace{223}_{\equiv 3 \pmod 4}}\right) = +\left(\frac{223}{59}\right) = \left(\frac{-13}{59}\right) =$$
$$= (-1)^{\frac{59-1}{2}}\left(\frac{13}{59}\right) = -\left(\frac{13}{59}\right) = -\left(\frac{59}{13}\right) = -\left(\frac{7}{13}\right) = -\left(\frac{13}{7}\right) =$$
$$= -\left(\frac{-1}{7}\right) = -(-1) = 1$$

$\Longrightarrow$ 223 ist quadratischer Rest mod 997.
Wenig rechnen verglichen mit Eulerschem Kriterium $223^{498} \pmod p$.

Beispiel 4.4.18:
Es existieren unendlich viele Primzahlen $p \equiv 1 \pmod 4$.

Beweis. Angenommen $p_1, \ldots, p_s$ seien alle Primzahlen $\equiv 1 \pmod 4$. $N \coloneqq p_1 \cdots p_s$. Betrachte $(2N)^2 + 1$. Sei q ein Primteiler von $(2N)^2 + 1$, dann kann q nicht aus $\{p_1, \ldots, p_s\}$ sein, also $q \equiv 3 \pmod 4$. $(2N)^2 + 1 \equiv 0 \pmod q \iff (2N)^2 \equiv -1 \pmod q$, das heißt -1 ist QR mod q, also $\left(\frac{-1}{q}\right) = 1$. Nach erstem Ergänzungssatz $\Longrightarrow q \equiv 1 \pmod 4$ ↯

Warnung:

Auch wenn ich mir in der Vorlesung gründlich Mühe gebe ordentlich mitzuschreiben, sind mit Sicherheit zahlreiche Tippfehler in meiner Mitschrift. Wenn dir einer auffällt, gib mir unbedingt Bescheid. Schreib dazu einfach per WhatsApp oder E-Mail (anton@mosich.at) wo der Fehler ist, und was richtig wäre.