A l g e b r a

Wintersemester 20²⁴/₂₅ Prof. Dr. Frederik Marks

Version: 28. Januar 2025

Mitschrift der Vorlesung *Algebra* im Wintersemester 20²⁴/₂₅, vorgetragen von Prof. Marks.

Inhaltsverzeichnis

0 Einführung

Algebra bedeutet **Rechnen mit Gleichungen**. Wir konzentrieren uns auf Polynomialgleichungen:

- Systeme linearer Gleichungen betrachtet man in der linearen Algebra
- Quadratische Gleichungen wie $x^2 + ax + b = 0$ lernt man in der Schule zu lösen (Mitternachtsformel).
- Kubische Gleichungen wie z. B. $x^3 + ax = b$ mit $a, b > 0$ sind schon schwieriger. Eine Lösung ist gegeben durch
$$x = \sqrt[3]{\frac{b}{2} + \sqrt{\left(\frac{b}{2}\right)^2 + \left(\frac{a}{3}\right)^3}} + \sqrt[3]{\frac{b}{2} - \sqrt{\left(\frac{b}{2}\right)^2 + \left(\frac{a}{3}\right)^3}}.$$
- Gleichungen von Grad 4 können durch endliche Wurzelausdrücke aufgelöst werden (Cardano 1545).
- Für Gleichungen von Grad 5 ist dies im Allgemeinen nicht möglich (Abel 1884).

Moderner Zugang (Galois 1830): Gruppentheorie, Körpererweiterung, ... (Algebra)
Galoistheorie, Auflösbarkeit von Polynomgleichungen,... (Algebra 2)

Highlights in diesem Semester:

- *Sylowsätze zur Struktur endlicher Gruppen.*

  Idee: Untersuche Gruppen ausgehend von ihren Untergruppen, deren Ordnung eine maximale Primpotenz ist.

- *Konstruktion mit Zirkel und Lineal.*

  Fragestellung: Welche Objekte in der Ebene erhalten wir mittels Elementarkonstruktionen? Würfelverdopplung? Quadratur des Kreises? Winkeldreiteilung? Regelmäßige n-Ecke?

  Idee: Nutze Theorie der Körpererweiterung.

1 Gruppen

Definition 1.1. Eine **Gruppe** $(G, *)$ ist eine Menge G mit einer binären Verknüpfung

$$*\colon G \times G \to G, (g, h) \mapsto g * h,$$

so dass gilt:

(G1) $(a * b) * c = a * (b * c)$ für alle $a, b, c \in G$ ($*$ assoziativ),

(G2) Es existiert ein $e \in G$, sodass für alle $a \in G$ gilt $a * e = a = e * a$ (e neutrales Element),

(G3) Für alle $a \in G$ existiert ein $a' \in G$, sodass $a * a' = e = a' * a$ (a' inverses Element zu a).

Gilt zusätzlich

(G4) $a * b = b * a$ für alle $a, b \in G$, so heißt $(G, *)$ **kommutativ** oder **abelsch**.

Die **Ordnung** von $(G, *)$ ist $|G|$.

Notation: Wir schreiben meist G statt $(G, *)$. Dabei ist $*$ oft entweder $+$ (**additive Gruppe**) oder $\cdot$ (**multiplikative Gruppe**). Dann schreibe 0 statt e bzw. $-a$ statt a' sowie $a-b := a+(-b)$, schreibe 1 statt e bzw. a^{-1} statt a' sowie $ab := a \cdot b$.

Bemerkung 1.2. (i) Das neutrale Element einer Gruppe G ist eindeutig:
Sind e, f neutrale Element in G, so gilt $e = e * f = f$ nach (G2).

(ii) Inverse Elemente in G sind eindeutig:
Seien a' und a'' Inverse zu $a \in G$. Dann gilt

$$a' \overset{(G2)}{=} a' * e \overset{(G3)}{=} a' * (a * a'') \overset{(G1)}{=} (a' * a) * a'' \overset{(G3)}{==} e * a'' \overset{(G2)}{=} a''$$

(iii) Für inverse Elemente in G gilt $(a')' = a$ und $(a * b)' = b' * a'$.

Beispiel 1.3. 1. $(R, +, \cdot)$ ein Ring $\implies$ $(R, +)$ abelsche Gruppe.
$(K, +, \cdot)$ ein Körper $\implies$ $(K, +)$ und $(K \setminus \{0\}, \cdot)$ abelsche Gruppe
$(V, +, \cdot)$ ein Vektorraum $\implies$ $(V, +)$ abelsche Gruppe.
Zum Beispiel $V = M_n(K) := \{n \times n\text{-Matrizen über einem Körper } K\}$.

2. $\mathrm{GL}_n(K) := \{\text{invertierbare } n \times n\text{-Matrizen über einem Körper } K\}$ bildet eine Gruppe bzgl. Matrizenmultiplikation - die **allgemeine lineare Gruppe**. Diese ist für $n \geq 2$ nicht abelsch.

   Weitere Beispiele:

   - $\mathrm{SL}_n(K) := \{A \in \mathrm{GL}_n(K) \mid \det A = 1\}$ - die **spezielle lineare Gruppe**.
   - $\mathrm{O}_n(K) := \{A \in \mathrm{GL}_n(K) \mid AA^\top = E_n\}$ - die **orthogonale Gruppe**.

3. $G = \{e\}$ ist die **triviale Gruppe**.

   Für $|G| = 2$ mit $G = \{1, g\}$, dann erhalten wir die eindeutige **Multiplikationstafel**:

$\cdot$	1	g
1	1	g
g	g	1

Für $|G| = 3$ mit $G = \{1, g, h\}$, dann erhalten wir die eindeutige Multiplikationstafel:

$\cdot$	1	g	h
1	1	g	h
g	g	h	1
h	h	1	g

Für $|G| = 4$ wird es schwieriger.

4. **Symmetriegruppen:** Sei G die Menge der **Kongruenzabbildungen** (längenerhaltend, flächenerhaltend, winkelerhaltend) eines geometrischen Objektes auf sich selbst.

5. Sei $X \neq \emptyset$ eine Menge. Die **symmetrische Gruppe** auf X ist gegeben durch $S_X = \{f : X \to X \mid f \text{ bijektiv}\}$ mit der gewöhnlichen Komposition von Abbildungen.

   Für $X = \{1, \dots, n\}$ mit $n \in \mathbb{N}$ erhalten wir die **symmetrische Gruppe vom Grad** n und schreiben $S_X = S_n$.

   Die Elemente in S_n heißen **Permutationen** und es gilt

$$|S_n| = n!.$$

   Matrixnotation: Die Permutation $\sigma : \{1, \dots, n\} \to \{1, \dots, n\}$ mit $\sigma(i) = a_i$ für $1 \leq i \leq n$ schreiben wir auch als

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & \dots & n \\ a_1 & a_2 & a_3 & \dots & a_n \end{pmatrix}.$$

   Zykelnotation: Sei $\{a_1, \dots, a_r\} \subseteq \{1, \dots, n\}$ mit a_i paarweise verschieden. Dann ist der **Zykel** $\sigma = (a_1, \dots, a_r)$ **der Länge** r definiert als die Permutation $\sigma \in S$ mit

$$\begin{aligned} \sigma(a_1) &= a_2 \\ \sigma(a_2) &= a_3 \\ &\vdots \\ \sigma(a_r) &= a_1 \end{aligned}$$

   und $\sigma(a) = a$ für alle $a \in \{1, \dots, n\} \setminus \{a_1, \dots, a_r\}$. Zykel der Länge 2 heißen **Transpositionen**. Zwei Zykel $(a_1 \dots a_r)$ und $(b_1 \dots b_s)$ heißen **disjunkt**, falls

$$\{a_1, \dots, a_r\} \cap \{b_1, \dots, b_r\} = \emptyset.$$

   Disjunkte Zykel kommutieren und jede Permutation lässt sich eindeutig als Komposition disjunkter Zykel schreiben.

   Zum Beispiel

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

   entspricht der Permutation (13)(245) in Zykelschreibweise.

6. Seien G und H Gruppen. Dann wird auch $G \times H$ zu einer Gruppe durch

$$(g_1, h_1) * (g_2, h_2) := (g_1 *_G g_2, h_1 *_H h_2).$$

   $G \times H$ heißt das **direkte Produkt** von G und H.

Definition 1.4. Seien G und H Gruppen

(a) Eine Abbildung $\varphi\colon G \to H$ heißt **Gruppenhomomorphismus**, falls

$$\varphi(g_1 *_G g_2) = \varphi(g_1) *_H \varphi(g_2)$$

für alle $g_1, g_2 \in G$. Ist φ auch bijektiv, sprechen wir von einem **Isomorphismus**. Die Gruppen G und H heißen dann **isomorph** und wir schreiben $G \cong H$.

(b) H heißt **Untergruppe** von G, falls $H \subseteq G$ und die Inklusionsabbildung $H \to G$ ein Gruppenhomomorphismus ist. Wir schreiben $H \leq G$.

Bemerkung 1.5. (i) Sei $\varphi\colon G \to H$ ein Gruppenhomomorphismus. Dann gilt

$$\varphi(1_G) = 1_H,$$

denn es gilt

$$\varphi(1_G) = \varphi(1_G 1_G) = \varphi(1_G)\varphi(1_G)$$

und Multiplikation mit $\varphi(1_G)^{-1}$ liefert

$$1_H = \varphi(1_G).$$

Zudem gilt

$$\varphi(g^{-1}) = \varphi(g)^{-1},$$

denn

$$\varphi(g)\varphi(g^{-1}) = \varphi(gg^{-1}) = \varphi(1_G) = 1_H = \cdots = \varphi(g^{-1})\varphi(g).$$

Nutze Bemerkung 1.2 (ii) zum Beweis der Eindeutigkeit.

(ii) Isomorphie ist eine Äquivalenzrelation. Isomorphe Gruppen betrachten wir als wesensgleich, in Hinblick auf Eigenschaften, Multiplikationstafeln, Eindeutigkeitsaussagen etc.

(iii) Sei G eine Gruppe und $H \subseteq G$. Dann ist $H \leq G$ Untergruppe genau dann, wenn

- $1_G \in H$,
- $h_1, h_2 \in H \;\Rightarrow\; h_1 h_2 \in H$,
- $h \in H \;\Rightarrow\; h^{-1} \in H$.

Beispiel 1.6. 1. $\det\colon \mathsf{GL}_n(K) \to K \setminus \{0\}$ ist ein Gruppenhomomorphismus, da $\det(AB) = \det(A)\det(B)$ für alle $A, B \in \mathsf{GL}_n(K)$. $\mathsf{SL}_n(K) \leq \mathsf{GL}_n(K)$ und $\mathrm{O} \leq \mathsf{GL}_n(K)$ sind Untergruppen.

2. $\exp\colon \mathbb{R} \to \mathbb{R}_{>0}$ ist ein Gruppenisomorphismus, da $\exp(x+y) = \exp(x)\exp(y)$ für alle $x, y \in \mathbb{R}$.

3. Sei $G = \{\mathrm{id}, \gamma_A, \gamma_B\}$ die Symmetriegruppe eines Rechtecks wie in Beispiel 1.3 (4). Dann ist G isomorph zum direkten Produkt $S_1 \times S_2$. Ein Isomorphismus ist gegeben durch $G \to S_1 \times S_2$ mit

$$\begin{aligned} \mathrm{id} &\mapsto (\mathrm{id}, \mathrm{id}) \\ \gamma_A &\mapsto (\mathrm{id}, (12)) \\ \gamma_B &\mapsto ((12), \mathrm{id}) \\ \gamma_{180^\circ} &\mapsto ((12), (12)) \end{aligned}$$

vergleiche Multiplikationstafeln.

4. Für $n \in \mathbb{N}$ ist $\varphi\colon S_n \to S_{n+1}$ mit

$$\varphi(\sigma) = \begin{pmatrix} 1 & \dots & n & n+1 \\ \sigma(1) & \dots & \sigma(n) & n+1 \end{pmatrix}$$

ein injektiver Gruppenhomomorphismus, d.h. S_n ist isomorph zu einer Untergruppe von S_{n+1}.

5. Sei G eine Gruppe und $g \in G$. Dann ist die Abbildung

$$C_g\colon G \to G, \quad h \mapsto ghg^{-1},$$

genannt **Konjugation mit** g, ein Gruppenisomorphismus mit

$$(C_g)^{-1} = C_{g^{-1}}.$$

Die Abbildungen

$$\begin{aligned} L_g\colon G \to G, &\quad h \mapsto gh \\ R_g\colon G \to G, &\quad h \mapsto hg, \end{aligned}$$

genannt **Links-** und **Rechtsmultiplikation mit** g, sind im Allgemeinen keine Gruppenhomomorphismus, aber bijektiv!

6. Sei $\varphi\colon G \to H$ ein Gruppenhomomorphismus. Dann sind $Ker(\varphi) := \{g \in G \mid \varphi(g) = 1_H\}$ (**Kern von** φ) und $\mathrm{Im}(\varphi) = \{\varphi(g) \mid g \in G\}$ (**Bild von** φ) Untergruppen von G bzw. H. Zudem ist φ injektiv genau dann, wenn $Ker(\varphi) = \{1_G\}$.

Beweis. „Nur dann“: Sei $g \in G$ mit $\varphi(g) = 1_H$. Da $\varphi(1_G) = 1_H$, folgt $g = 1_G$.
„Dann“: Seien $a, b \in G$ mit $\varphi(a) = \varphi(b)$. Da $1_H = \varphi(a)\varphi(b)^{-1} = \varphi(ab^{-1})$, folgt $ab^{-1} = 1_G$ und somit $a = b$. □

Satz 1.7 (Satz von Cayley)**.** *Jede Gruppe ist isomorph zu einer Untergruppe einer symmetrischen Gruppe, d.h. einer Gruppe von Bijektionen.*

Beweis. Sei G eine Gruppe. Wir konstruieren einen injektiven Gruppenhomomorphismus $\varphi\colon G \to S_G = \{f\colon G \to G \mid f \text{ bijektiv}\}$ durch $g \mapsto L_g$ (siehe Beispiele 1.3 (5) und 1.6 (5)).
Z.z.: φ ist Gruppenhomomorphismus. Seien $g, h \in G$. Dann gilt für alle $a \in G$

$$\varphi(gh)(a) = L_{gh}(a) = (gh)(a) = g(ha) = L_g(ha) = (L_g \circ L_h)(a) = (\varphi(g) \circ \varphi(h))(a)$$

und somit $\varphi(gh) = \varphi(g) \circ \varphi(h)$.
<u>Z.z.: φ ist injektiv:</u> Seien $g, h \in G$ mit

$$L_g = \varphi(g) = \varphi(h) = L_h.$$

Dann gilt

$$g = L_g(1_G) = L_h(1_G) = h.$$

Ist G endlich mit $|G| = n$, so ist G isomorph zu einer Untergruppe von S_n, der symmetrischen Gruppe vom Grad n. □

Beispiel 1.8. Für $\sigma \in S_n$ definiere $\operatorname{sgn}(\sigma) = (-1)^{\omega(\sigma)}$, wobei

$$\omega(\sigma) = |\{(i,j) \mid 1 \leq i < j \leq n, \sigma(j) < \sigma(i)\}|,$$

genannt die **Anzahl der Fehlstände von** σ. Dann ist

$$\operatorname{sgn}(\sigma) = \prod_{i<j} \frac{\sigma(i) - \sigma(j)}{i - j}.$$

Zum Beispiel ist für

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

das Signum

$$\operatorname{sgn}(\sigma) = \frac{3-2}{1-2} \cdot \frac{3-1}{1-3} \cdot \frac{2-1}{2-3} = (-1)^3 = -1.$$

σ hat 3 Fehlstände. Die Abbildung $\operatorname{sgn}\colon S_n \to (\{-1, 1\}, \cdot)$ ist ein Gruppenhomomorphismus, da für $\sigma, \pi \in S_n$ gilt

$$\operatorname{sgn}(\sigma\pi) = \prod_{i<j} \frac{\sigma(\pi(i)) - \sigma(\pi(j))}{i - j} = \prod_{i<j} \frac{\sigma(\pi(i)) - \sigma(\pi(j))}{\pi(i) - \pi(j)} \cdot \prod_{i<j} \frac{\pi(i) - \pi(j)}{i - j} = \operatorname{sgn}(\sigma) \cdot \operatorname{sgn}(\pi)$$

Nach Beispiel 1.6 (6) ist $A_n := \operatorname{Ker}(\operatorname{sgn})$ Untergruppe von S_n. A_n heißt die **alternierende Gruppe vom Grad** n.
Zum Beispiel ist für $S_3 = \{\mathrm{id}, (12), (13), (23), (123), (132)\}$:

$$A_3 = \{\mathrm{id}, (123), (132)\}.$$

Definition 1.9. Sei G eine Gruppe und $H \leq G$. Für $g \in G$ heißt

$$gH := \{gh \mid h \in H\} \qquad \textbf{(Linksnebenklasse von } H \textbf{ in } G\textbf{)}$$
$$Hg := \{hg \mid h \in H\} \qquad \textbf{(Rechtsnebenklasse von } H \textbf{ in } G\textbf{)}$$

Schreibe $G/H = \{gH \mid g \in G\}$ und $H \backslash G = \{Hg \mid g \in G\}$. Definiere $[G : H] := |{}^{G}/{}_{H}|$.

Bemerkung 1.10. (i) Nach Beispiel 1.6 (5) gilt

$$|gH| = |H| = |Hg|$$

für alle $g \in G$.

(ii) Nach Aufgabe M.1.3 definieren die Relationen $a \sim_1 b \Leftrightarrow a^{-1}b \in H$ bzw. $a \sim_2 b \Leftrightarrow ab^{-1} \in H$ Äquivalenzrelationen auf G. Die Äquivalenzklassen sind genau die Links- bzw. Rechtsnebenklassen von H in G.

Insbesondere gilt

$$G = \bigcup_{g\in G} gH = \bigsqcup_{N\in G/H} N,$$
$$G = \bigcup_{g\in G} Hg = \bigsqcup_{N\in H\backslash G} N$$

Beweis. Für $[a] = \{b \mid a_1 \sim_1 b\}$ gilt: $b \in [a] \Leftrightarrow a^{-1}b \in H \Leftrightarrow \exists h \in H : a^{-1}b = h \Leftrightarrow \exists h \in H : b = ah \Leftrightarrow b \in aH$. □

Satz 1.11 (Satz von Lagrange)**.** *Sei G eine endliche Gruppe und $H \leq G$. Dann gilt*

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

Insbesondere also $|H|\,\Big|\,|G|$ ($|H|$ teilt $|G|$).

Beweis. Wähle $\{g_1, \dots, g_r\} \subseteq G$, so dass

$$G = \bigsqcup_{j=1}^{r} g_i H$$

gilt, d.h. $[G : H] = r$. Dann gilt

$$|G| = \sum_{j=1}^{r} |g_j H| = \sum_{j=1}^{r} |H| = r|H| = [G : H] \cdot |H|.$$

□

Definiert $g_1 H * g_2 H := g_1 g_2 H$ eine Gruppenstruktur auf der G/H?

<u>Problem:</u> Wohldefiniertheit.

Beispiel 1.12. Sei $G = S_3$ und $H = \{\mathrm{id}, (12)\}$. Da $|G| = 6$ und $|H| = 2$, folgt mit Satz 1.11, dass $[G : H] = 3$. Es gibt also 3 Linksnebenklassen:

$$\mathrm{id}H = H, \quad (23)H = \{(23), (132)\} \quad \text{und} \quad (13)H = \{(13), (123)\}$$

Wir erhalten

$$(23)H * (13)H = (123)H$$

und

$$(23)H = (132)H * (13)H = (12)H.$$

$(123)H \neq (12)H$ und wir folgern:
Wir brauchen eine stärkere Bedingung als $H \leq G$ Untergruppe.

Definition 1.13. Sei G eine Gruppe und $H \leq G$.

(a) Für $g \in G$ heißt $gHg^{-1} = \{ghg^{-1} \mid h \in H\}$ die **zu H konjugierte Untergruppe**. Nach Beispiel 1.6 (5), (6) gilt $gHg^{-1} \leq G$ mit $|gHg^{-1}| = |H|$ für alle $g \in G$.

(b) $H \leq G$ heißt **normale Untergruppe** oder auch **Normalteiler**, falls

$$gHg^{-1} = H \quad \text{für alle } g \in G.$$

Wir schreiben $H \trianglelefteq G$.

Bemerkung 1.14. Die folgenden Aussagen sind äquivalent

(i) $H \trianglelefteq G$.

(ii) $gH = Hg$ für alle $g \in G$, d.h. für jedes $g \in G$ stimmt die Linksnebenklasse mit der Rechtsnebenklasse überein.

(iii) $gHg^{-1} \subseteq H$ für alle $g \in G$.

Beweis. „(iii) $\Rightarrow$ (ii)“: Sei $g \in G$. Nach Voraussetzung gilt $gH \subseteq Hg$ sowie für $h \in H : hg = g(g^{-1}hg) \in gH$, also auch $Hg \subset gH$, wie gewünscht. $\square$

Beispiel 1.15. (1) $\{1_G\} \trianglelefteq G$ und $G \trianglelefteq G$ sind Normalteiler.

Eine Gruppe $G \neq \{1_G\}$ heißt **einfach**, wenn sie nur die trivialen Normalteiler $\{1_G\}$ und G hat.

(2) Ist G abelsch, so ist jede Untergruppe Normalteiler.

(3) Sei $H \leq G$ mit $[G : H] = 2$, dann gilt $H \trianglelefteq G$.

Beweis.

$$[G : H] = 2 \implies G/H = \{H, G \backslash H\}$$

Damit stimmen Links- und Rechtsnebenklassen überein. $\square$

Betrachte zum Beispiel die alternierende Gruppe $A_n \leq S_n$ mit $A_n = \{\sigma \in S_n \mid \operatorname{sgn}(\sigma) = 1\}$ für $n \geq 2$. Für $\pi \in S_n$ mit $\operatorname{sgn}(\pi) = -1$ gilt

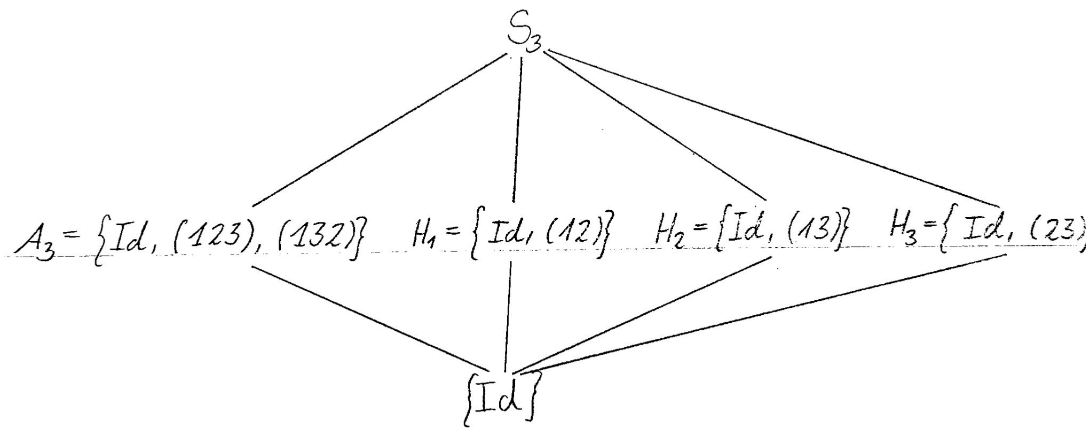
$$\pi A_n = \{\sigma \in S_n \mid \operatorname{sgn}(\sigma) = -1\}$$

Beweis. $\subseteq$: Gilt, da sgn Gruppenhomomorphimus ist.

$\supseteq$: Sei $\sigma \in S_n$ mit $\operatorname{sgn}(\sigma) = -1$. Dann gilt $\sigma = \pi(\pi^{-1}\sigma) \in \pi A_n$, da $\operatorname{sgn}(\pi^{-1}\sigma) = \operatorname{sgn}(\pi^{-1})\operatorname{sgn}(\sigma) = (-1)^2 = 1$. $\square$

Es folgt, dass $[S_n : A_n] = 2$ und damit $A_n \trianglelefteq S_n$. Insbesondere ist nach Satz 1.11 $|A_n| = n!/2$, da z.B. $(13)H_1(13) = H_3$.

(4) Die symmetrische Gruppe S_3 hat folgende Untergruppen:



Es gilt $A_3 \trianglelefteq S_3$. H_1, H_2, H_3 sind jedoch keine Normalteiler, da zum Beispiel $(13)H_1(13) = H_3$.

Satz 1.16. *Sei G eine Gruppe und $H \trianglelefteq G$.*

*(a) Die Menge $G/H = \{gH \mid g \in G\}$ mit Multiplikation $(aH) \cdot (bH) = (ab)H$ für alle $a, b \in G$ ist eine Gruppe. Sie heißt **Faktorgruppe** oder **Quotientengruppe**.*

*(b) Die Abbildung $\pi\colon G \to G/H$ mit $g \mapsto gH$ ist ein surjektiver Gruppenhomomorphismus mit $\operatorname{Ker}(\pi) = H$. π heißt **kanonische Projektion**.*

Beweis. (a) Die Multiplikation ist wohldefiniert. Sei $aH = a'H$ und $bH = b'H$ bzw. $a^{-1}a' \in H$ und $b^{-1}b' \in H$.

<u>Z.z.: $abH = a'b'H$ bzw. $(ab)^{-1}a'b' \in H$.</u>

$$(ab)^{-1}a'b' = b^{-1}a^{-1}a'b' = b^{-1}\underbrace{(a^{-1}a')}_{\in H}b\underbrace{(b^{-1}b')}_{\in H} \in H$$

Gruppenaxiome:

(G1) Multiplikation in G und in G/H assoziativ.

(G2) H ist neutrales Element in G/H.

(G3) Das Inverse zu gH ist $g^{-1}H$.

(b) Für alle $a, b \in G$ gilt

$$\pi(ab) = (ab)H = aH \cdot bH = \pi(a) \cdot \pi(b).$$

Also ist π ein Gruppenhomomorphismus mit

$$\operatorname{Ker}(\pi) = \{g \in G \mid gH = H\} = H$$

□

Beispiel 1.17. Betrachte $n\mathbb{Z} \trianglelefteq \mathbb{Z}$ für $n \in \mathbb{N}$ mit

$$\mathbb{Z}/n\mathbb{Z} = \{n\mathbb{Z}, 1 + n\mathbb{Z}, \ldots, (n-1) + n\mathbb{Z}\} =: \mathbb{Z}_n,$$

wobei $(a + n\mathbb{Z}) + (b + n\mathbb{Z}) = (a + b) + n\mathbb{Z}$. Statt $a + n\mathbb{Z}$ schreiben wir auch $\bar{a}$.
Wir können auch Normalteiler in $\mathbb{Z}/n\mathbb{Z}$ betrachten, zum Beispiel

$$H = \{\bar{0}, \bar{3}\} \trianglelefteq \mathbb{Z}_6.$$

H ist offensichtlich Untergruppe und auch noch Normalteiler, da $\mathbb{Z}_6$ abelsch ist. Es gilt

$$\mathbb{Z}_6/H = \{H, \bar{1} + H, \bar{2} + H\} \cong \mathbb{Z}_3$$

Proposition 1.18. Sei $H \leq G$ eine Untergruppe. Dann gilt $H \trianglelefteq G$ genau dann, wenn H Kern eines Gruppenhomomorphismus ist, der in G startet.

Beweis. „$\Rightarrow$“: Folgt aus Satz 1.16 (b).
„$\Leftarrow$“: Sei $\varphi\colon G \to G'$ Gruppenhomomorphismus und $H = \mathrm{Ker}(\varphi)$. Nach Beispiel 1.6 (6) ist $H \leq G$ Untergruppe. Sei nun $g \in G$ und $h \in H$. Dann gilt

$$\varphi(ghg^{-1}) = \varphi(g)\varphi(h)\varphi(g)^{-1} = \varphi(g)1_{G'}\varphi(g)^{-1} = 1_{G'}$$

Es folgt $gHg^{-1} \subseteq H$ und $H \trianglelefteq G$ ist Normalteiler nach Bemerkung 1.14. $\square$

Beispiel 1.19. (1) Nach Beispiel 1.8 ist $\mathrm{sgn}\colon S_n \to (\{-1,1\},\cdot)$ für $n > 1$ ein surjektiver Gruppenhomomorphismus. Nach Beispiel 1.15 (3) gilt

$$S_n/\mathrm{Ker}(\mathrm{sgn}) = S_n/A_n = \{A_n, \pi A_n\},$$

wobei $\mathrm{sgn}(\pi) = -1$. Insbesondere gilt

$$S_n/\mathrm{Ker}(\mathrm{sgn}) \cong \mathbb{Z}_2 \cong (\{-1,1\},\cdot) = \mathrm{Im}(\mathrm{sgn}).$$

(2) Sei $\varphi\colon \mathbb{R}\setminus\{0\}$ mit $x \mapsto |x|$. Dann ist φ ein Gruppenhomomorphismus mit $\mathrm{Ker}(\varphi) = \{\pm 1\}$ und $\mathrm{Im}(\varphi) = \mathbb{R}_{>0}$.
Es gilt

$$\mathbb{R}\setminus\{0\}/\mathrm{Ker}(\varphi) = \mathbb{R}\setminus\{0\}/(\{-1,1\},\cdot) \cong \mathbb{R}_{>0} = \mathrm{Im}\varphi$$

(3) Nach Beispiel 1.6 (1) ist $\det\colon \mathsf{GL}_n(K) \to K\setminus\{0\}$ ein surjektiver Gruppenhomomorphismus. Es gilt $\mathrm{Ker}(\det) = \mathsf{SL}_n(K)$, sowie

$$\mathsf{GL}_n(K)/\mathrm{Ker}(\det) = \mathsf{GL}_n(K)/\mathsf{SL}_n(K)) \cong K\setminus\{0\} = \mathrm{Im}(\det).$$

Anstatt diesen Isomorphismus explizit nachzuprüfen, beweisen wir

Satz 1.20 (Homomorphiesatz)**.** *Sei $\varphi\colon G \to H$ ein Gruppenhomomorphismus. Dann gilt*

$$G/\mathrm{Ker}(\varphi) \cong \mathrm{Im}(\varphi).$$

Insbesondere gilt $|G| = |\mathrm{Ker}(\varphi)| \cdot |\mathrm{Im}(\varphi)|$ für G endlich.

Beweis. Betrachte die Abbildung $\bar\varphi\colon G/\mathrm{Ker}(\varphi) \to \mathrm{Im}(\varphi)$ mit $g\mathrm{Ker}(\varphi) \mapsto \varphi(g)$.
$\bar\varphi$ ist wohldefiniert, da für $g\mathrm{Ker}(\varpi) = g'\mathrm{Ker}(\varphi)$ gilt: Es existiert ein $x \in \mathrm{Ker}(\varphi)$ mit $g = g'x$ und somit

$$\varphi(g) = \varphi(g'x) = \varphi(g')\varphi(x) = \varphi(g')1_H = \varphi(g')$$

$\bar\varphi$ ist Gruppenhomomorphismus, da für $g, g' \in G$ gilt:

$$\bar\varphi(g\mathrm{Ker}(\varphi)g'\mathrm{Ker}(\varphi)) = \bar\varphi(gg'\mathrm{Ker}(\varphi)) = \varphi(gg') = \varphi(g)\varphi(g') = \bar\varphi(g\mathrm{Ker}(\varphi))\bar\varphi(g'\mathrm{Ker}(\varphi))$$

$\bar\varphi$ ist nach Konstruktion surjektiv.
$\bar\varphi$ ist injektiv, da aus $\bar\varphi(g\mathrm{Ker}(\varphi)) = \varphi(g) = 1_H$ folgt, dass $g \in \mathrm{Ker}(\varphi)$ und somit $g\mathrm{Ker}(\varphi) = \mathrm{Ker}(\varphi) = 1_{(G/\mathrm{Ker}(\varphi))}$ (siehe Beispiel 1.6 (6)). $\bar\varphi$ ist also ein Gruppenisomorphismus, so dass

$$G/\mathrm{Ker}(\varphi) \cong \mathrm{Im}(\varphi).$$

Für endliche Gruppen G folgt schließlich mit Satz 1.11

$$|G| = |\mathrm{Ker}(\varphi)| \cdot |\mathrm{Im}(\varphi)|.$$

$\square$

Satz 1.21 (Isomorphiesätze). *Sei G eine Gruppe und $H_1, H_2 \leq G$ Untergruppen.*

(a) Ist $H_1 \trianglelefteq G$ Normalteiler, so gilt $H_1H_2 = H_2H_1 \leq G$ und

$$H_1H_2/H_1 \cong H_2/(H_1 \cap H_2).$$

(b) Sind $H_1, H_2 \trianglelefteq G$ Normalteiler mit $H_1 \leq H_2 \leq G$, so gilt

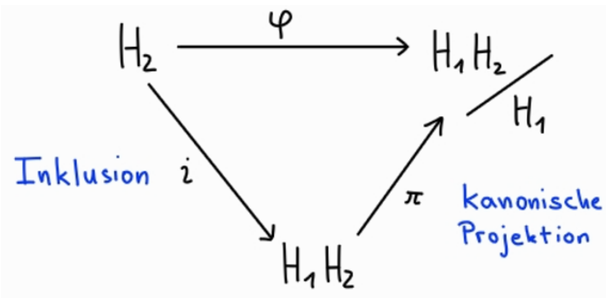
$$\frac{G/H_1}{H_2/H_1} \cong G/H_2$$

Beweis. (a) Da $H_1 \trianglelefteq G$, gilt $h_2H_1 = H_1h_2$ für alle $h_2 \in H_2$. Somit $H_1H_2 = H_2H_1$. H_1H_2 ist Untergruppe, da $1_G \in H_1H_2$ und daher $1_G = 1_G1_G \in H_1$. Für $h_1, h_1' \in H$ und $h_2, h_2' \in H_2$ gilt

$$(h_1h_2)(h_1'h_2') = h_1(\underbrace{h_2h_1'}_{\in H_1H_2})h_2' \in H_1H_2$$

Für $h_1 \in H_1, h_2 \in H_2$ gilt $(h_1h_2)^{-1} = h_2^{-1}h_1^{-1} \in H_2H_1 = H_1H_2$. Da $H_1 \trianglelefteq G$, gilt auch $H_1 \trianglelefteq H_1H_2$.

Betrachte nun den Homomorphismus



mit $\varphi(h_2) = h_2H_1$. Dann gilt

$$\mathrm{Ker}(\varphi) = \{h_2 \in H_2 \mid h_2H_1 = H_1\} = H_1 \cap H_2$$

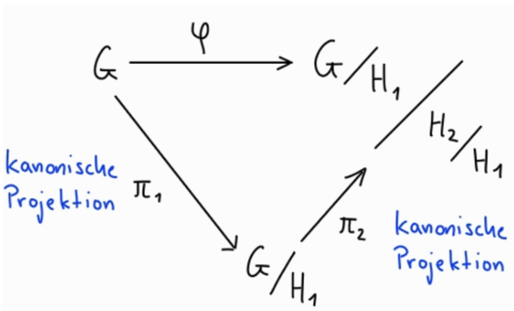
Da φ nach Konstruktion surjektiv, (nutze $H_1H_2 = H_2H_1$), folgt mit Satz 1.20

$$H_2/H_1 \cap H_2 = H_2/\mathrm{Ker}(\varphi) \cong \mathrm{Im}(\varphi) = H_1H_2/H_1.$$

(b) Nach Voraussetzung gilt $H_1 \trianglelefteq H_2$. Die Faktorgruppe H_2/H_1 wird zur Untergruppe von G/H_1. Es gilt sogar $H_2/H_1 \trianglelefteq G/H_1$, da für alle $g \in G, h_2 \in H_2$ gilt:

$$gH_1h_2H_1g^{-1}H_1 = \underbrace{gh_2g^{-1}}_{\in H_2,\text{ da } H_2 \trianglelefteq G} H_1.$$

Betrachte nun den Homomorphismus



mit $\varphi(g) = gH_1(H_2/H_1)$. Dann gilt

$$\operatorname{Ker}(\varphi) = \{g \in G \mid gH_1 \in {}^{H_2}\!/_{H_1}\} = H_2.$$

Da φ nach Konstruktion surjektiv ist (als Komposition surjektiver Abbildungen), folgt wieder mit Satz 1.20:

$${}^{G}\!/_{H_2} = {}^{G}\!/_{\operatorname{Ker}(\varphi)} \cong \operatorname{Im}(\varphi) = {}^{G/H_1}\!/_{H_2/H_1}.$$

□

Beispiel 1.22. (1) Sei $G = \mathbb{Z}$, $H_1 = 3\mathbb{Z} \trianglelefteq G$ und $H_2 = 5\mathbb{Z} \trianglelefteq G$. Dann ist $H_1 \cap H_2 = 15\mathbb{Z}$ und $H_1 + H_2 = \mathbb{Z}$, da $1 = 5(-1) + 3 \cdot 2$. Satz 1.21 (a) liefert

$$\mathbb{Z}_3 = {}^{\mathbb{Z}}\!/_{3\mathbb{Z}} = {}^{H_1 + H_2}\!/_{H_1} \cong {}^{H_2}\!/_{H_1 \cap H_2} = {}^{5\mathbb{Z}}\!/_{15\mathbb{Z}}.$$

(2) Sei $G = \mathbb{Z}$, $H_1 = mn\mathbb{Z} \trianglelefteq G$ und $H_2 = m\mathbb{Z} \trianglelefteq G$ für $m, n \in \mathbb{N}$. Dann liefert Satz 1.21 (b)

$$\mathbb{Z}_m = {}^{\mathbb{Z}}\!/_{m\mathbb{Z}} = {}^{G}\!/_{H_2} \cong {}^{G/H_1}\!/_{H_2/H_1} = {}^{\mathbb{Z}/mn\mathbb{Z}}\!/_{m\mathbb{Z}/mn\mathbb{Z}}.$$

Wie sehen Untergruppen von Faktorgruppen aus? Im Beweis von Satz 1.21 (b) haben wir verwendet, dass für eine Gruppe G mit $N \trianglelefteq G$ und $N \leq H \leq G$ gilt:

$${}^{H}\!/_{N} \leq {}^{G}\!/_{N}.$$

Der Beweis zeigt zudem, dass $H \trianglelefteq G \;\Leftrightarrow\; H/N \trianglelefteq G/N$.

Sind alle Untergruppen von G/N von dieser Form? – **Ja!**

Satz 1.23. *Die Abbildung $\{H \leq G \mid N \leq H\} \to \{$Untergruppen von $G/N\}$ mit $H \mapsto H/N$ ist bijektiv.*

Beweis. Betrachte die kanonische Projektion $\pi\colon G/N$ mit $g \mapsto gN$. Ist $H' \leq G/N$ eine Untergruppe, so gilt

$$N \leq \pi^{-1}(H') = \{g \in G \mid \pi(g) \in H'\} \leq G$$

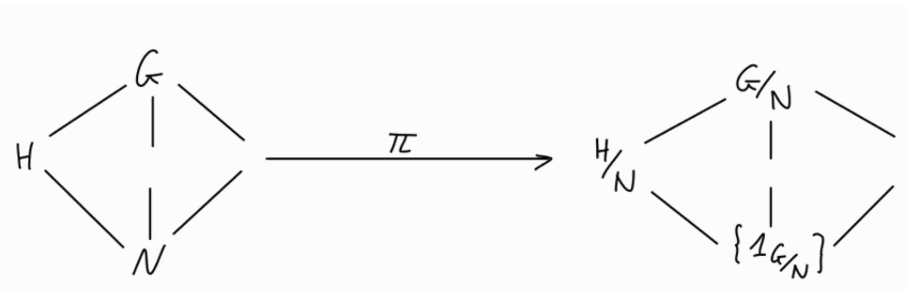
- $g \in N \;\Rightarrow\; \pi(g) = 1_{G/N} \in H'$, also $g \in \pi^{-1}(H')$. Insbesondere $1_G \in \pi^{-1}(H')$.
- $g_1, g_2 \in \pi^{-1}(H') \;\Rightarrow\; g_1g_2 \in \pi^{-1}(H')$, da $\pi(g_1g_2) = \underbrace{\pi(g_1)}_{\in H'}\underbrace{\pi(g_2)}_{\in H'} \in H'$.
- $g \in \pi^{-1}(H') \;\Rightarrow\; g^{-1} \in \pi^{-1}(H')$, da $\pi(g^{-1}) = \pi(g)^{-1} \in H'$.

Die Umkehrabbildung zur gegebenen Abbildung in der Aussage liefert die Zuordnung $H' \mapsto \pi^{-1}(H')$, da

$${}^{\pi^{-1}(H')}\!/_{N} = H' \quad \text{sowie} \quad \pi^{-1}(H/N) = H$$

□

Bemerkung 1.24. Die Bijektion in Satz 1.23 ist inklusionserhaltend und zeigt, dass die kanonische Projektion $\pi\colon G \to G/N$ einen Isomorphismus von Untergruppenverbänden induziert:



2 Endlich erzeugte Gruppen

Definition 2.1. Sei G eine Gruppe und $S \subseteq G$ eine Teilmenge. Definiere

$$\langle S \rangle := \bigcap_{H \leq G, S \subseteq H} H \leq G.$$

$\langle S \rangle$ heißt **die von S erzeugte Untergruppe** von G.

Falls $G = \langle S \rangle$, so heißt S **Erzeugendensystem** von G. Hat G ein endliches Erzeugendensystem, so heißt G **endlich erzeugt**. Gibt es ein $g \in G$ mit $G = \langle \{g\} \rangle =: \langle g \rangle$, so heißt G **zyklisch**.

Bemerkung 2.2. (i) Nach Konstruktion ist $\langle S \rangle$ die kleinste Untergruppe von G, die S enthält.

(ii) Für $S \neq \emptyset$ ist $\langle S \rangle = \{s_1 \cdots s_t \mid t \in \mathbb{N}, s_i \in S \cup S^{-1}\}$.

Insbesondere ist für $g \in G$:

$$\langle g \rangle = \{g^n \mid n \in \mathbb{Z}\} \quad \text{mit} \quad g^n := \begin{cases} 1_G, & n = 0 \\ \underbrace{g \cdots g}_{n-\text{mal}}, & n > 0 \\ \underbrace{g^{-1} \cdots g^{-1}}_{(-n)-\text{mal}}, & n < 0 \end{cases}$$

Wir wollen zunächst zyklische Gruppen besser verstehen!

Beispiel 2.3. (1) $(\mathbb{Z}, +) = \langle 1 \rangle = \langle -1 \rangle$ ist eine zyklische Gruppe.

$(\mathbb{Z}_m, +) = \langle \bar{1} \rangle$ ist eine zyklische Gruppe der Ordnung m.

(2) Sei G eine Gruppe mit $|G| = p$ Primzahl. Dann ist G zyklisch.

Beweis. Sei $1_G \neq g \in G$ und betrachte $\langle g \rangle \leq G$. Nach Satz 1.11 $|\langle g \rangle|$ teilt $|G| = p$. Da $\langle g \rangle > 1$ nach Voraussetzung folgt $|\langle g \rangle| = p$. Somit $G = \langle g \rangle$. □

Satz 2.4. *(a) Eine Gruppe G ist zyklisch genau dann, wenn es einen surjektiven Gruppenhomomorphismus von der Form $\mathbb{Z} \to G$ gibt.*

(b) Für eine zyklische Gruppe G gilt:

$$G \cong \begin{cases} \mathbb{Z}, & |G| = \infty, \\ \mathbb{Z}_m, & |G| = m. \end{cases}$$

Zudem ist jede Untergruppe von G wieder zyklisch.

Beweis. (a) „⇒“: Sei $G = \langle g \rangle = \{g^n \mid n \in \mathbb{Z}\}$. Definiere einen Gruppenhomomorphismus $\mathbb{Z} \to G$ durch $m \mapsto g^n$. Dieser ist nach Voraussetzung surjektiv.

„⇐“: Sei $\varphi \colon \mathbb{Z} \to G$ ein surjektiver Gruppenhomomorphismus. Definiere $g := \varphi(1) \in G$.

<u>Behauptung</u>: $G = \langle g \rangle$.

Die Inklusion $\langle g\rangle \subseteq G$ ist klar. Sei nun $h \in G$ beliebig. Da φ surjektiv ist, existiert $n \in \mathbb{Z}$ mit $\varphi(n) = h$. Da φ Gruppenhomomorphismus, gilt

$$h = \varphi(n) = \begin{cases} \underbrace{\varphi(1)\cdots\varphi(1)}_{n-\text{mal}}, & n \geq 0 \\ \underbrace{\varphi(1)^{-1}\cdots\varphi(1)^{-1}}_{n-\text{mal}}, & n < 0 \end{cases}$$

Daraus folgt $h = g^n \in \langle g\rangle$.

(b) Sei G zyklisch und $\varphi\colon \mathbb{Z} \to G$ ein surjektiver Gruppenhomomorphismus, der nach (a) existiert. Nach Satz 1.20 gilt

$$G \cong \mathbb{Z}/_{\mathrm{Ker}(\varphi)}.$$

Nach Aufgabe M.1.4. wissen wir, dass $\mathrm{Ker}(\varphi) = m\mathbb{Z}$ für ein $m \in \mathbb{N}_0$. Damit folgt der erste Teil der Behauptung.

Sei nun $H \leq G$. Dann ist $\varphi^{-1}(H)$ eine Untergruppe von $\mathbb{Z}$ (siehe Beweis zu Satz 1.23) und somit erneut $\varphi^{-1}(H) = m\mathbb{Z}$, $m \in \mathbb{N}_0$. Insbesondere ist $\varphi^{-1}(H) = \langle m\rangle \leq \mathbb{Z}$. Da φ surjektiv ist, gilt $\varphi(\varphi^{-1}(H)) = H$ und H wird von $\varphi(n)$ erzeugt.

□

Definition 2.5. Sei G eine Gruppe und $g \in G$. Die **Ordnung von** g ist definiert als die Ordnung $\langle g\rangle$, der von g erzeugten zyklischen Untergruppe von G.
Wir schreiben $\mathrm{ord}(g)$ für die Ordnung von g.

Bemerkung 2.6. Ist $\mathrm{ord}(g) = m \in \mathbb{N}$ bzw. $\langle g\rangle \cong \mathbb{Z}_m$ mit $\langle g\rangle = \{1_G, g, \ldots, g^{m-1}\}$ nach Satz 2.4 (b), so gilt $g^n = 1_G$ genau dann, wenn $n \in m\mathbb{Z}$.
Ist G endlich, so gilt $\mathrm{ord}(g)$ teilt $|G|$ nach Satz 1.11 und somit $g^{|G|} = 1_G$ (**Kleiner Fermat'scher Satz**).
Ist $\mathrm{ord}(g) = \infty$ bzw. $\langle g\rangle \cong \mathbb{Z}$, so sind die g^n mit $n \in \mathbb{Z}$ paarweise verschieden.

Beispiel 2.7. (1) Für $\bar{a} \in \mathbb{Z}_m$ mit $m \in \mathbb{N}$ gilt $\mathrm{ord}(\bar{a}) = \frac{m}{\mathrm{ggT}(a,m)}$. Zum Beispiel hat $\bar{8} \in \mathbb{Z}_{12}$ die Ordnung $\frac{12}{\mathrm{ggT}(8,12)} = \frac{12}{4} = 3$.

(2) Für $n \geq 3$ sei D_n die Symmetriegruppe eines regelmäßigen n-Ecks in $\mathbb{R}^2$. Diese heißt auch **Diedergruppe**. Für $n = 3$ gilt $D_3 \cong S_3$.

Im Allgemeinen enthält D_n genau n Drehungen und n Spiegelungen, so dass $|D_n| = 2n$. Sei r eine Drehung um $\frac{2\pi}{n}$ und s eine beliebige Spiegelung. Dann gilt $\mathrm{ord}(r) = n$ und $\mathrm{ord}(s) = 2$, sowie $D_n = \{\mathrm{id}, r, r^2, \ldots, r^{n-1}, s, sr, sr^2, \ldots, sr^{n-1}\} = \langle\{r, s\}\rangle$.

Welche Gruppen können wir aus zyklischen Gruppen zusammensetzen?

Definition 2.8. Eine Gruppe G heißt **inneres direktes Produkt** von G_1 und G_2, falls

- $G_1, G_2 \trianglelefteq G$.
- $G_1 \cdot G_2 = G$.
- $G_1 \cap G_2 = \{1_G\}$.

Bemerkung 2.9. (i) Ist $G = G_1 \times G_2$ (äußeres) direktes Produkt der Gruppen G_1 und G_2, so ist G inneres direktes Produkt von $G_1 \times \{1_G\}$ und $\{1_G\} \times G_2$.

(ii) Ist G inneres direktes Produkt von G_1 und G_2, so gilt

$$G \cong G_1 \times G_2.$$

Beweis. Betrachte die Abbildung $\varphi\colon G_1 \times G_2$ mit $(g_1, g_2) \mapsto g_1 g_2$. Da $\underbrace{g_1 g_2 g_1^{-1}}_{\in G_2} g_2^{-1} = g_1 (\underbrace{g_2 g_1^{-1} g_2^{-1}}_{\in G_1}) \in G_1 \cap G_2 = \{1_G\}$, folgt $g_1 = g_2$. Somit gilt $\varphi((g_1, g_2)(h_1, h_2)) = \varphi(g_1 h_1, g_2 h_2) = g_1(h_1 g_2) h_2 = (g_1 g_2)(h_1 h_2) = \varphi((g_1, g_2))\varphi((h_1, h_2))$. φ ist zudem bijektiv nach Voraussetzung. $\square$

Beispiel 2.10. (1) Die abelsche Gruppe $\mathbb{C} \setminus \{0\}$ ist inneres direktes Produkt von $\mathbb{R}_{>0}$ und $S^1 := \{z \in \mathbb{C} \mid |z| = 1\}$.

(2) Nach Aufgabe S.2.2. gilt

$$V_4 = \{\mathrm{id}, (12)(34), (13)(24), (14)(23)\} \trianglelefteq S_4$$

mit $S_4/V_4 \cong S_3$. Die S_3 ist isomorph zu einer Untergruppe H von S_4 (Beispiel 1.6 (4)), so dass $V_4 \cdot H = S_4$ und $V_4 \cap H = \{\mathrm{id}\}$. Aber S_4 ist nicht inneres direktes Produkt von V_4 und H, da H kein Normalteiler von S_4.

Theorem 2.11. *Jede endlich erzeugte abelsche Gruppe ist ein endliches inneres direktes Produkt zyklischer Gruppen.*

Beweis. Sei $(G, +)$ abelsche Gruppe, erzeugt von $S = \{a_1, \ldots, a_k\} \subseteq G$.
Induktion über k: Für $k = 1$ ist G zyklisch.
Betrachte den surjektiven Gruppenhomomorphismus

$$\varphi_S\colon \mathbb{Z}^k \to G \quad \text{mit} \quad (n_1, \ldots, n_k) \mapsto n_1 a_1 + \cdots + n_k a_k.$$

Sei $\pi\colon \mathbb{Z}^k \to \mathbb{Z}$ die Projektion auf die erste Komponente, also

$$\pi((n_1, \ldots, n_k)) = n_1.$$

Das Bild von $\operatorname{Ker}(\varphi_S)$ unter π ist Untergruppe von $\mathbb{Z}$ und somit von der Form $d\mathbb{Z}$ für $d \in \mathbb{N}_0$. Sei o.B.d.A. S so gewählt, dass d minimal ist. Falls $d = 0$, so ist $\langle a_1 \rangle \cap \langle S \setminus \{a_1\} \rangle = \{0_G\}$ und $\operatorname{ord} a_1 = \infty$, d.h. G ist inneres direktes Produkt von $\langle a_1 \rangle$ und $\langle S \setminus \{a_1\} \rangle$, wobei $\langle a_1 \rangle \cong \mathbb{Z}$.
Auf $S \setminus \{a_1\}$ können wir die Induktionsvoraussetzung anwenden.
Falls $d > 0$, wähle $(n_1, \ldots, n_k) \in \operatorname{Ker}(\varphi_S)$ mit $n_1 = d$. Sei $2 \leq i \leq k$. Division mit Rest liefert $q_i, d_i \in \mathbb{Z}$ mit

$$n_i = q_i d + d_i \quad \text{und} \quad 0 \leq d_i < d.$$

Definiere $S_i := \{b_1, \ldots, b_k\}$ durch $b_1 = a_i$ und $b_i = a_1 + q_i a_i$ und $b_j = a_j$ sonst. Dann ist auch S_i Erzeugendensystem von G. Zudem liegt der Vektor

$$(d_i, n_2, \ldots, i, \ldots, n_k) \in \mathbb{Z}^k$$

im Kern von φ_{S_i}, da

$$d_i b_1 + d b_i = (n_i - q_i d) a_i + d(a_1 + q_i a_i) = n_i a_i + n_1 a_1$$

und weil $(n_1, \ldots, n_k) \in \mathrm{Ker}(\varphi_S)$. Wegen der Minimalität von d ist $1 \leq d_i < d$ ausgeschlossen, d.h.

$$d_i = 0 \quad \text{und} \quad d \Big| n_i.$$

Setze nun $x_i = \frac{n_i}{d}$ für $1 \leq i \leq k$. Insbesondere $x_1 = 1$. Dann wird G von der Menge

$$\Big\{ \underbrace{\sum_{i=1}^{k} x_i a_i}_{=:a}, a_2, \ldots, a_k \Big\}$$

mit $\langle a \rangle \cap \langle \{a_2, \ldots, a_k\} \rangle = \{0_G\}$. Denn ein Element im Schnitt hat die Form

$$m_1 a = \sum_{i=2}^{k} m_i a_i$$

für $(m_1, \ldots, m_k) \in \mathbb{Z}^k$, so dass m_1 im Bild von $\mathrm{Ker}(\varphi_S)$ unter π liegt, also ein Vielfaches von d ist. Es gilt aber bereits

$$da = n_1 a_1 + \cdots + n_k a_k = 0_G.$$

Somit ist G inneres direktes Produkt von $\langle a \rangle$ und $\langle S \setminus \{a_1\} \rangle$, wobei $\langle a \rangle \cong \mathbb{Z}_d$. Nun können wir erneut die Induktionsvoraussetzung anwenden. $\square$

Korollar 2.12 (Hauptsatz für endlich erzeugte abelsche Gruppen)**.** *Sei G eine endlich erzeugte Gruppe. Dann existieren eindeutige $r, t \in \mathbb{N}_0$ sowie bis auf Reihenfolge eindeutig bestimmte Primzahlpotenzen*

$$1 < p_1^{k_1} \leq \cdots \leq p_t^{k_t} \quad \textit{mit} \quad G \cong \mathbb{Z}^r \times \mathbb{Z}_{p_1^{k_1}} \times \cdots \times \mathbb{Z}_{p_t^{k_t}}.$$

Beweis. Die Existenz folgt aus Theorem 2.11 zusammen mit Bemerkung 2.9 (ii) und Aufgabe M.3.3. Letztere besagt, dass für $m, n \in \mathbb{N}$ mit $\mathrm{ggT}(m, n) = 1$ gilt $\mathbb{Z}_{nm} \cong \mathbb{Z}_n \times \mathbb{Z}_m$. Die Eindeutigkeit können/wollen wir hier nicht beweisen. $\square$

Was können wir im nicht-abelschen Fall tun? Eine Klassifikation aller endlich erzeugten oder endlichen Gruppen ist hoffnungslos. Im Jahr 1982 hat man die Klassifikation aller endlichen einfachen Gruppen abgeschlossen, also aller endlichen Gruppen mit genau zwei (trivialen) Normalteilern. Dies war ein Mammutprojekt!

- mehr als 500 Fachartikel,
- mehr als 100 MathematikerInnen,
- Zeitraum von über 50 Jahren,
- Einsatz von Computern.

Die endlichen einfachen Gruppen sind von der Form

(1) Zyklische Gruppe $\mathbb{Z}_p$ mit p Primzahl.

(2) Alternierende Gruppen A_n für $n \geq 5$.

(3) Endliche Gruppen vom Lie-Typ, z.B.

$$\mathsf{PSL}_(K) := {}^{\mathsf{SL}_n(K)}\!\big/\!{}_{Z(\mathsf{SL}_n(K))} = {}^{\mathsf{SL}_n(K)}\!\big/\!{}_{\{\lambda E_n \mid \lambda^n = 1\}}$$

für $n > 2$ und einen endlichen Körper K.

(4) 26 sporadische Gruppen mit bis zu ungefähr $8 \cdot 10^{53}$ Elementen, die sogenannten Monster!

Beispiel 2.13. Die alternierende Gruppe A_4 ist nicht einfach nach Aufgabe S.2.2. Aber für $n \geq 5$ ist A_n einfach.

Beweis. Sei $\{\mathrm{id}\} \neq N \trianglelefteq A_n$. Wir zeigen, dass $N = A_n$.
Schritt 1: N enthält einen Zykel der Länge 3.
Sei $\mathrm{id} \neq \sigma \in N$. Ist σ kein Zykel der Länge 3, so gilt einer der folgenden Fälle:

(i) $\sigma = (a_1a_2a_3a_4\ldots)\ldots$

(ii) $\sigma = (a_1a_2a_3)(a_4a_5a_6)\ldots$

(iii) $\sigma = (a_1a_2)(a_3a_4)(a_5a_6)\ldots$

(iv) $\sigma = (a_1a_2)(a_3a_4)$

Da N Normalteiler ist, gilt $(\pi\sigma\pi^{-1})\sigma^{-1} \in N$ für alle $\pi \in A_n$. Im Fall (i) wähle $\pi = (a_2a_1a_3)$.

$$(\pi\sigma\pi^{-1})\sigma^{-1} = (a_2a_1a_3)\sigma(a_1a_2a_3)\sigma^{-1} = (a_1a_3a_4).$$

Im Fall (ii) wähle $\pi = (a_3a_2a_4)$.

$$(\pi\sigma\pi^{-1})\sigma^{-1} = (a_3a_2a_4)\sigma(a_2a_3a_4)\sigma^{-1} = (a_1a_5a_2a_4a_3)$$

und weiter im Fall (i). Im Fall (iii) wähle $\pi = (a_2a_1a_3)$:

$$(\pi\sigma\pi^{-1})\sigma^{-1} = (a_2a_1a_3)\sigma(a_1a_2a_3)\sigma^{-1} = (a_1a_4)(a_2a_3).$$

Im Fall (iv) wähle $\pi = (a_2a_1a_5)$:

$$(\pi\sigma\pi^{-1})\sigma^{-1} = (a_2a_1a_5)\sigma(a_1a_2a_5)\sigma^{-1} = (a_1a_2a_5).$$

Also enthält N einen Zykel der Länge 3.
Schritt 2: $N = A_n$.
Sei $(a_1a_2a_3) \in N$. Da $N \trianglelefteq A_n$ ist, gilt:

$$(a_3a_4a_5)(a_1a_2a_3)(a_4a_3a_5) = (a_1a_2a_4) \in N.$$

Insbesondere sind alle Zykel der Form (a_1a_2x) in N mit $x \in \{1, \ldots, n\} \setminus \{a_1, a_2\}$. Wiederholen des Arguments zeigt, dass alle Zykel der Länge 3 in N enthalten sind. Da A_n nach Aufgabe M.3.2. von diesen Zykeln erzeugt wird, folgt $N = A_n$. □

▌ Warum sind endliche einfache Gruppen so wichtig?

Definition 2.14. Sei G ein Gruppe. Eine Folge von Untergruppen

$$\{1_G\} = G_0 \trianglelefteq G_1 \trianglelefteq G_2 \trianglelefteq \cdots \trianglelefteq G_n = G$$

heißt **Normalreihe der Länge** n. Die Faktoren G_i/G_{i-1} heißen **Faktoren** der Normalreihe. Eine Normalreihe von G heißt **Kompositionsreihe**, falls alle ihre Faktoren einfach sind. Die Faktoren einer Kompositionsreihe heißen **Kompositionsfaktoren**.

Bemerkung 2.15. (i) Jede Gruppe G hat die Normalreihe $\{1_G\} \trianglelefteq G$.

(ii) Jede endliche Gruppe G hat eine Kompositionsreihe.

Induktion nach $|G|$. Ist G einfach, dann ist $\{1_G\} \trianglelefteq G$ Kompositionsreihe. Ist andernfalls $N \trianglelefteq G$ maximaler echter Normalteiler. nach Satz 1.23 ist G/N einfach und N hat nach Induktionsvoraussetzung eine Kompositionsreihe

$$\{1_G\} = N_0 \trianglelefteq N_1 \trianglelefteq \cdots \trianglelefteq N_t = N.$$

Dann ist $\{1_G\} = N_0 \trianglelefteq N_1 \trianglelefteq \cdots \trianglelefteq N_t = N \trianglelefteq G$ eine Kompositionsreihe von G.

(iii) Die Gruppe $\mathbb{Z}$ hat keine Kompositionsreihe (nutze Klassifikation der Untergruppen von $\mathbb{Z}$).

Theorem 2.16. *Sei G eine endliche Gruppe. Dann alle Kompositionsreihen von G* ***äquivalent****, das heißt sie haben die selbe Länge und bis auf Isomorphie und Reihenfolge die selben Kompositionsfaktoren.*

Beweis. Betrachte die folgenden Kompositionsreihen:

(I) $\{1_G\} = G_0 \trianglelefteq G_1 \trianglelefteq \cdots \trianglelefteq G_r = G$,

(II) $\{1_G\} = H_0 \trianglelefteq H_1 \trianglelefteq \cdots \trianglelefteq H_s = G$.

Induktion nach r: Für $r = 1$ ist G einfach. Also auch $G = H_1$.
Sei $r > 1$.
Fall 1: $G_{r-1} = H_{s-1}$. Dann hat G_{r-1} die Kompositionsreihen $\{1_G\} = G_0 \trianglelefteq \cdots \trianglelefteq G_{r-1}$ und $\{1_G\} = H_0 \trianglelefteq \cdots \trianglelefteq H_{s-1} = G_{r-1}$. Nach Induktionsvoraussetzung sind diese beiden und somit auch die ursprünglichen beiden Kompositionsreihen **(I)** und **(II)** von G äquivalent.
Fall 2: $G_{r-1} \neq H_{s-1}$. Betrachte $G_{r-1} \trianglelefteq G_{r-1} \ldots H_{s-1} \trianglelefteq G$. Da $G_{r-1} \neq H_{s-1}$ und G_r/G_{r-1} und G/H_{s-1} einfach, folgt mit Satz 1.23, dass $G_{r-1}H_{s-1} = G$. Sei $J = G_{r-1} \cap H_{s-1}$ mit $J \trianglelefteq G$. Nach Satz 1.21 (a) gilt

$$G/G_{r-1} = G_{r-1}H_{s-1}/G_{r-1} \cong H_{s-1}/J$$

sowie

$$G/H_{s-1} = H_{s-1}G_{r-1}/H_{s-1} \cong G_{r-1}/J$$

d.h. H_{s-1}/J und G_{r-1}/J sind einfach. Nach Bemerkung 2.15 (ii) hat J eine Kompositionsreihe

$$\{1_G\} = J_0 \trianglelefteq J_1 \trianglelefteq \cdots \trianglelefteq J_t = J.$$

Diese induziert die folgenden beiden Kompositionsreihen von G:

(III) $\{1_G\} = J_0 \trianglelefteq \cdots \trianglelefteq J_t = J \trianglelefteq G_{r-1} \trianglelefteq G$,

(IV) $\{1_G\} = J_0 \trianglelefteq \cdots \trianglelefteq J_t = J \trianglelefteq H_{s-1} \trianglelefteq G$.

Diese sind äquivalent, da bis auf Isomorphie nur die letzten beiden Faktoren vertauscht werden. Nach Induktionsvoraussetzung sind auch die Kompositionsreihen **(I)** und **(III)** von G äquivalent. Insbesondere gilt $r - 1 = t + 1$. Somit liefert **(IV)** eine Kompositionsreihe von H_{s-1} der Länge $r - 1$, die nach Induktionsvoraussetzung äquivalent ist zu $\{1_G\} = H_0 \trianglelefteq \cdots \trianglelefteq H_{s-1}$. Folglich sind auch die Kompositionsreihen **(II)** und **(IV)** äquivalent. Dies liefert die gewünschte Äquivalenz von **(I)** und **(II)**. □

Beispiel 2.17. $\mathbb{Z}_6$ hat die Kompositionsreihen $\{\bar{0}\} \trianglelefteq \langle\bar{2}\rangle \trianglelefteq \mathbb{Z}_6$ und $\{\bar{0}\} \trianglelefteq \langle\bar{3}\rangle \leq \mathbb{Z}_6$ mit Kompositionsfaktoren isomorph zu $\mathbb{Z}_2$ und $\mathbb{Z}_3$.
Die symmetrische Gruppe S_3 hat die Kompositionsreihe $\{\mathrm{id}\} \trianglelefteq A_3 \trianglelefteq S_3$, deren Kompositionsfaktoren auch isomorph zu $\mathbb{Z}_2$ und $\mathbb{Z}_3$ sind. Aber $\mathbb{Z}_6 \cong \mathbb{Z}_2 \times \mathbb{Z}_3 \ncong S_3$!

Wir haben gesehen, dass sich endliche abelsche Gruppen, auf im Wesentlichen, eindeutige Art und Weise, aus einfachen Gruppen zusammenkleben lassen. Aber welche Gruppen können wir aus einfachen zyklischen Gruppen zusammenkleben?

Definition 2.18. Eine Gruppe G heißt **auflösbar**, wenn G eine Normalreihe mit abelschen Faktoren hat, d.h. es gibt eine Folge von Untergruppen

$$\{1_G\} = G_0 \trianglelefteq G_1 \trianglelefteq \cdots \trianglelefteq G_n = G$$

mit G_i/G_{i-1} abelsch für alle $1 \leq i \leq n$.

Bemerkung 2.19. Auflösbare Gruppen werden uns in der Algebra II helfen zu entscheiden, ob Gleichungen durch endliche Wurzelausdrücke aufgelöst werden können (siehe Kapitel 0).

Beispiel 2.20. (1) Abelsche Gruppen sind auflösbar. Nach Theorem 2.11 bzw. 2.12 wissen wir, dass wir endliche abelsche Gruppen aus einfachen zyklischen Gruppen zusammenkleben können.

(2) Jede einfache auflösbare Gruppe G ist isomorph zu $\mathbb{Z}_p$, p prim.

Beweis. Da G einfach, existiert nur die triviale Normalreihe $\{1_G\} \trianglelefteq G$. Da G auflösbar ist, folgt, dass G abelsch ist und abelsche Gruppen ohne echten Normalteiler sind isomorph zu $\mathbb{Z}_p$. □

(3) Die alternierende Gruppe A_n mit $n \in \mathbb{N}$ ist auflösbar genau dann, wenn $n \leq 4$.

Beweis. Für $n \leq 3$ ist A_n abelsch und dadurch auflösbar. Für $n = 4$ betrachte die Normalreihe $\{1_G\} \trianglelefteq V_4 \trianglelefteq A_4$ mit Faktoren $V_4 \cong \mathbb{Z}_2 \times \mathbb{Z}_2$ und $A_4/V_4 \cong \mathbb{Z}_3$ (siehe Aufgabe S.2.2.). Für $n \geq 5$ nutze Beispiel 2.13. □

(4) Man kann zeigen, dass endliche Gruppen ungerader Ordnung auflösbar stets auflösbar sind. (**Satz von Feit-Thompson** (1963))

(5) Die kleinste nicht auflösbare Gruppe ist die A_5.

Proposition 2.21. Sei G eine auflösbare Gruppe.

(a) Jede Untergruppe von $H \leq G$ ist auflösbar.

(b) Ist $N \trianglelefteq G$ Normalteiler, so ist auch G/N auflösbar.

Beweis. Sei $\{1_G\} = G_0 \trianglelefteq G_1 \trianglelefteq \cdots \trianglelefteq G_n = G$ eine Normalreihe von G mit der Eigenschaft G_i/G_{i-1} abelsch für alle $i \in \{1, \ldots, n\}$.

(a) Betrachte die induzierte Normalreihe der Form

$$\{1_G\} = G_0 \cap H \trianglelefteq G_1 \cap H \trianglelefteq \cdots \trianglelefteq G_n \cap H = H.$$

Nach Satz 1.21 (a) gilt für alle $i \in \{1, \dots, n\}$

$$G_i \cap H \big/ G_{i-1} \cap H = G_i \cap H \big/ G_{i-1} \cap G_i \cap H \cong G_{i-1} \cdot (G_i \cap H) \big/ G_{i-1} \leq G_i \big/ G_{i-1}$$

Da G_i/G_{i-1} abelsch ist, so ist auch $(G_i \cap H)/(G_{i-1} \cap H)$ abelsch. Somit ist H auflösbar.

(b) Betrachte die durch die kanonische Projektion $\pi\colon G \to G/N$ induzierte Normalreihe der Form $\{1_{G/N}\} = \pi(G_0) \trianglelefteq \pi(G_1) \trianglelefteq \cdots \trianglelefteq \pi(G_n) = G/N$. Für $i \in \{1, \dots, n\}$ erhalten wir einen surjektiven Gruppenhomomorphismus

$$\varphi\colon G_i \to \pi(G_i) \big/ \pi(G_{i-1})$$

durch $g_i \mapsto \pi(g_i)\pi(G_{i-1})$ mit

$$G_{i-1} \trianglelefteq \mathrm{Ker}(\varphi) \trianglelefteq G_i.$$

Nach Satz 1.20 und Satz 1.21 (b) gilt

$$\pi(G_i) \big/ \pi(G_{i-1}) \cong G_i \big/ \mathrm{Ker}(\varphi) \cong G_i/G_{i-1} \big/ \mathrm{Ker}(\varphi)/G_{i-1}.$$

Da G_i/G_{i-1} abelsch ist, so sind auch deren Quotienten abelsch und somit insbesondere $\pi(G_i)/\pi(G_{i-1})$. Also ist G/N auflösbar.

$\square$

Satz 2.22. *Sei G eine Gruppe mit Kompositionsreihe. Dann ist G auflösbar genau dann, wenn alle Kompositionsfaktoren von G isomorph zu $\mathbb{Z}_p$ für p Primzahl.*

Beweis. „$\Leftarrow$“: Folgt unmittelbar, da $\mathbb{Z}_p$ abelsch ist.
„$\Rightarrow$“: Sei G_i/G_{i-1} ein Kompositionsfaktor von G mit $G_{i-1} \trianglelefteq G_i \leq G$. Da G auflösbar ist, sind nach Proposition 2.21 sowohl G_i als auch G_i/G_{i-1} auflösbar. Da G_i/G_{i-1} zudem einfach ist, folgt die Behauptung mit Beispiel 2.20 (2). $\square$

3 Operationen von Gruppen auf Mengen

Definition 3.1. Sei G eine Gruppe und $X \neq \emptyset$ eine Menge. Dann heißt X **G-Menge**, wenn es eine Abbildung $*\colon G \times X \to X$, $(g, x) \mapsto g * x$ gibt mit

(O1) $1_G * x = x$ für alle $x \in X$. (Das neutrale Element operiert neutral)

(O2) $g * (h * x) = (gh) * x$ für alle $g, h \in G$ und alle $x \in X$.

Wir sagen G **operiert auf** X und schreiben oft $\cdot$ statt $*$.

Bemerkung 3.2. Sei X eine G-Menge und $g \in G$. Dann ist $\tau_g\colon X \to X$ mit $x \mapsto g \cdot x$ bijektiv mit Inverse τ_{g-1}. Also ist τ_g Element der symmetrischen Gruppe S_X. Die Abbildung $\tau\colon G \to S_X$ mit $g \mapsto \tau_g$ ist Gruppenhomomorphismus, da für alle $g, h \in G$ und $x \in X$ gilt:

$$\tau(gh)(x) = \tau_{gh}(x) = (gh)x = g(hx) = \tau_g(\tau_h(x)) = \tau(g) \circ \tau_h(x) = \tau(g) \circ \tau(h)(x)$$

Umgekehrt macht jeder Gruppenhomomorphismus $\varphi\colon G \to S_X$ mit $g \mapsto \varphi_g$ X zu einer G-Menge durch $G \times X \to X$ mit $(g, x) \mapsto \varphi_g(x)$. Denn $1_G \cdot x = \varphi_{1_G}(x) = \mathrm{id}(x) = x$ für alle $x \in X$ und

$$g(hx) = \varphi_g(\varphi_h(x)) = (\varphi_g \circ \varphi_h)(x) = \varphi_{gh}(x) = (gh)x$$

für alle $g, h \in G$ und $x \in X$.

Ist die Abbildung τ injektiv bzw. ist $g = 1_G$ das einzige Element aus G mit $gx = x$ für alle $x \in X$, so heißt die Operation von G auf X **treu**.

Beispiel 3.3. (1) G operiert auf sich selbst durch Linksmultiplikation. Sei $X = G$ und $G \times X \to X$ mit $(g, x) \mapsto gx$. **(O1)** und **(O2)** sind erfüllt, da G eine Gruppe ist. Die Operation ist treu $\rightsquigarrow$ siehe Satz von Cayley (Satz 1.7).

(2) Sei $H \subseteq G$. Dann operiert G auf G/H durch $G \times (G/H) \to G/H$ mit $(g, xH) \mapsto (gx)H$. Diese Operation ist im Allgemeinen nicht treu, da für $g \in G$ gilt $(gx)H = xH$ für alle $x \in G$ genau dann, wenn $x^{-1}gx \in H$ für alle $x \in G$, was genau dann der Fall ist, wenn $g \in xHx^{-1}$ für alle $x \in G$. Für $H \trianglelefteq G$ zum Beispiel gilt $xHx^{-1} = H$ für alle $x \in G$.

(3) Betrachte das Quadrat mit Eckpunkten $v_1, \dots, v_4$. Sei $G = \mathbb{Z}_4$ und $X = \{v_1, v_2, v_3, v_4\}$. Dann operiert G treu auf X durch Drehung, zum Beispiel

$$\begin{aligned}(\bar{1}, v_1) &\mapsto v_2\\ (\bar{1}, v_2) &\mapsto v_3\\ (\bar{1}, v_3) &\mapsto v_4\\ (\bar{1}, v_4) &\mapsto v_1.\end{aligned}$$

Mit Hilfe von **(O1)** und **(O2)** legt dies die gewünschte Abbildung $G \times X \to X$ fest.

Definition 3.4. Sei X eine G-Menge. Für $x \in X$ heißt

(a) $Gx := \{gx \mid g \in G\}$ die **Bahn von x unter G**.

Die Operation heißt **transitiv**, falls die Menge X unter G nur eine Bahn besitzt, das heißt für alle $x, y \in X$ existiert $g \in G$ mit $gx = y$.

(b) $\mathrm{Stab}_G(x) := \{g \in G \mid gx = x\}$ der **Stabilisator von x in G**.

Mit $\mathrm{Stab}_G(x) = G$, das heißt $gx = x$ für alle $g \in G$, so heißt x **Fixpunkt der Operation**. Schreibe X^G für die Menge aller Fixpunkte der Operation.

Bemerkung 3.5. Sei X eine G-Menge.

(i) Definiere auf X eine Äquivalenzrelation $x \sim y \;:\Leftrightarrow\; \exists g \in G : gx = y$. Als Äquivalenzklassen erhalten wir genau die Bahnen unter G. Für $x \in X$ gilt

$$[x] = \{y \in X \mid x \sim y\} = \{y \in X \mid \exists g \in G : gx = y\} = \{gx \mid g \in G\} = Gx.$$

Insbesondere ist X die disjunkte Vereinigung von Bahnen

(ii) Für $xinX$ ist $\mathrm{Stab}_G(x) \leq G$, da

$$\begin{aligned} 1_G &\in \mathrm{Stab}_G(x) \\ \forall g, h \in \mathrm{Stab}_G(x) &: (gh)x = g(hx) = gx = x \\ \forall g \in \mathrm{Stab}_G(x) &: g^{-1}x = g^{-1}(gx) = (g^{-1}g)x = 1_G x = x. \end{aligned}$$

Es gilt für $a \in G$, dass $\mathrm{Stab}_G(ax) = a\mathrm{Stab}_G(x)a^{-1}$, da $g \in \mathrm{Stab}_G(ax)$ genau dann, wenn $g(ax) = ax$ genau dann, wenn $(a^{-1}ga)x = x$ genau dann, wenn $a^{-1}ga \in \mathrm{Stab}_G(x)$. Äquivalent zu $g \in a\mathrm{Stab}_G(x)a^{-1}$.

Beispiel 3.6. (1) Die Operationen in Beispiel 3.3 sind alle transitiv und, abgesehen vom trivialen Fall, fixpunktfrei.

Im Beispiel 3.3 (1) und (3) sind die Stabilisatoren trivial, also $\mathrm{Stab}_G(x) = \{1_G\}$ für alle $x \in X$. In Beispiel 3.3 (2) erhalten wir als Stabilisatoren die zu H konjugierten Untergruppen.

(2) G operiert auf sich selbst durch Konjugation. Sei dazu $X = G$ und $G \times X \to X$ mit $(g, x) \mapsto gxg^{-1}$. Diese Operation ist im Allgemeinen weder treu noch transitiv. Die Bahn $Gx = \{gxg^{-1} \mid g \in G\} =: C_x$ heißt **Konjugationsklasse von x**. Der Stabilisator $\mathrm{Stab}_G(x) = \{g \in G \mid gx = xg\} =: C_G$ heißt **Zentralisator von x in G**. Das Zentrum von G entspricht genau der Menge X^G bzw. der Vereinigung aller 1-elementigen Konjugationsklassen.

Sei $G = \mathsf{GL}_n(K)$ für $n \in \mathbb{N}$ und einen Körper K. Dann enthält die Konjugationsklasse $C_{\mathfrak{A}}$ einer Matrix $\mathfrak{A} \in \mathsf{GL}_n(K)$ genau die zu $\mathfrak{A}$ ähnlichen Matrizen in $\mathsf{GL}_n(K)$.

Fixpunkte der Operation sind genau die Matrizen

$$\begin{bmatrix} \lambda & & \\ & \ddots & \\ & & \lambda \end{bmatrix}$$

mit $\lambda \in K \setminus \{0\}$.

Satz 3.7 (Bahnensatz). *Sei X eine G-Menge und $x \in X$. Dann erhalten wir die bijektive Abbildung*

$$Gx \to {}^{G}\!/_{\mathrm{Stab}_G(x)} \quad \textit{mit} \quad gx \mapsto g\mathrm{Stab}_G(x).$$

*Ist G endlich, so folgt $|G| = |Gx| \cdot |\mathrm{Stab}_G(x)|$, die sogenannte **Bahnformel**.*

Beweis. Die Zuordnung ist wohldefiniert und injektiv, da für alle $g, h \in G$ gilt:

$$gx = hx \;\Leftrightarrow\; x = g^{-1}hx \;\Leftrightarrow\; g^{-1}h \in \mathrm{Stab}_G(x) \;\Leftrightarrow\; g\mathrm{Stab}_G(x) = h\mathrm{Stab}_G(x)$$

Zudem ist die Abbildung surjektiv nach Konstruktion. Die Bahnformel folgt mit Satz 1.11. □

Korollar 3.8. *Sei X eine endliche G-Menge und $\{x_i\}_{i\in I}$ ein Repräsentantensystem der Bahnen von X unter G. Dann gilt*

$$|X| \overset{\text{Bem.3.5(i)}}{=} \sum_{i\in I} |Gx_i| = |X^G| + \sum_{x_i \notin X^G} |Gx_i| \overset{\text{Satz.3.7}}{=} |X^G| + \sum_{x_i \notin X^G} [G : \mathrm{Stab}_G(x_i)].$$

Ist $X = G$ und G operiert durch Konjugation, so folgt

$$|G| \overset{\text{Bsp.3.6(2)}}{=} |Z(G)| + \sum_{x_i \notin Z(G)} |C_{x_i}| = |Z(G)| + \sum_{x_i \notin Z(G)} [G : C_G(x_i)].$$

Die sogenannte ***Klassengleichung****.*

Beispiel 3.9. Die Gruppe $G = \mathsf{GL}_n(K)$ operiert treu auf $X = K^n$ durch Matrizenmultiplikation. Bahnen:

$$G\mathfrak{o}_{K^n} = \{\mathfrak{o}_{K^n}\}, \quad G\mathfrak{e}_1 = K^n \setminus \{\mathfrak{o}_{K^n}\}$$

Insbesondere gilt $K^n = G\mathfrak{o}_{K^n} \cup G\mathfrak{e}_1$. Zudem ist

$$\mathrm{Stab}_G(\mathfrak{e}_1) = \{\mathfrak{A} \in \mathsf{GL}_n(K) \mid \mathfrak{A}\mathfrak{e}_1 = \mathfrak{e}_1\} = \left\{ \begin{bmatrix} 1 & a_2 & \dots & a_n \\ 0 & & & \\ \vdots & & \mathfrak{A}' & \\ 0 & & & \end{bmatrix} \;\middle|\; \mathfrak{A}' \in \mathsf{GL}_{n-1}(K) \right\}.$$

Sei nun $|K| = q < \infty$. Mit der Bahnformel gilt

$$\begin{aligned} |\mathsf{GL}_n(K)| &= |G\mathfrak{e}_1| \cdot |\mathrm{Stab}_G(\mathfrak{e}_1)| \\ &= (q^n - 1)q^{n-1} \cdot |\mathsf{GL}_{n-1}(K)| \end{aligned}$$

Induktiv erhalten wir

$$|\mathsf{GL}_n(K)| = q^{\frac{n(n-1)}{2}}(q^n - 1)(q^{n-1} - 1)\dots(q - 1)$$

▌ Wie helfen uns Gruppenoperationen, die Struktur endlicher Gruppen zu verstehen?

Definition 3.10. (a) Eine Gruppe der G der Ordnung $|G| = p^n$ für eine Primzahl p und $n \in \mathbb{N}$ heißt p-**Gruppe**.

(b) Sei $|G| = p^n \cdot q$ mit p Primzahl und $\mathrm{ggT}(p, q) = 1$. Dann heißt $H \leq G$ p-**Sylowuntergruppe** von G, falls $|H| = p^n$. Schreibe $\mathsf{Syl}_p(G)$ für die Menge aller p-Sylowuntergruppen von G.

Bemerkung 3.11. (i) Ist G eine p-Gruppe und X eine endliche G-Menge, so gilt $|X| \equiv |X^G| \mod p$.

Beweis. Nach Korollar 3.8 gilt für ein Repräsentantensystem $\{x_i\}_{i\in I}$ der Bahnen von X:

$$|X| \equiv |X^G| + \sum_{x_i \notin X^G} [G : \mathrm{Stab}_G(x_i)].$$

Nach Satz 1.11 teilt $[G : \mathrm{Stab}_G(x_i)]$ die Ordnung von G. Für $x_i \notin G$ ist $[G : \mathrm{Stab}_G(x_i)] > 1$ und somit gilt

$$p \Big| [G : \mathrm{Stab}_G(x_i)].$$

□

(ii) Für eine p-Gruppe G ist das Zentrum $Z(G) \neq \{1_G\}$.

Beweis. Die Klassengleichung aus Korollar 3.8 liefert

$$0 \equiv |G| \equiv |Z(G)| \mod p.$$

Also teilt p die Ordnung von $Z(G)$. □

Beispiel 3.12. (1) Die abelsches Gruppen $\mathbb{Z}_p, \mathbb{Z}_p \times \mathbb{Z}_p$ und $\mathbb{Z}_{p^2}$ sind p-Gruppen. Die Diedergruppe D_4 ist eine 2-Gruppe mit $|Z(D_4)| = 2$.

(2) $G = S_3$ mit $|G| = 2 \cdot 3$ ist keine p-Gruppe. Es gilt

$$\begin{aligned} \mathsf{Syl}_2(G) &= \{\langle(12)\rangle, \langle(13)\rangle, \langle(23)\rangle\} \\ \mathsf{Syl}_3(G) &= \{A_3\}. \end{aligned}$$

(3) Sei $G = \mathsf{GL}_n(\mathbb{Z}_p)$ für $n \in \mathbb{N}$. Nach Beispiel 3.9 gilt

$$|G| = p^{\frac{n(n-1)}{2}} \underbrace{(p^n - 1)(p^{n-1} - 1) \dots (p - 1)}_{\equiv \pm 1 \mod p}.$$

Sei

$$U_n := \left\{ \mathfrak{A} \in \mathsf{GL}_n(\mathbb{Z}_p) \mid \mathfrak{A} = \begin{bmatrix} \bar{1} & & * \\ & \ddots & \\ 0 & & \bar{1} \end{bmatrix} \right\} \leq \mathsf{GL}_n(\mathbb{Z}_p).$$

Da $|U_n| = p^{\frac{n(n-1)}{2}}$, ist U_n p-Sylowuntergruppe von $\mathsf{GL}_n(\mathbb{Z}_p)$.

Theorem 3.13 (Sylow-Sätze)**.** *Sei $|G| = p^n \cdot q$ mit p Primzahl und $\mathrm{ggT}(p, q) = 1$.*

(a) Zu jedem $k \in \{1, \dots, n\}$ existiert eine Untergruppe $H \leq G$ mit $|H| = p^k$.

(b) Sei $H \leq G$ mit $|H| = p^k$ für $k \in \{1, \dots, n\}$. Sei $S \in \mathsf{Syl}_p(G)$. Dann existiert $g \in G$ mit $H \leq gSg^{-1}$.

(c) $|\mathsf{Syl}_p(G)|$ teilt q und $|\mathsf{Syl}_p(G)| \equiv 1 \mod p$.

Korollar 3.14. *Sei G eine endliche Gruppe und p eine Primzahl.*

(a) p teilt $|G|$ nur dann, wenn ein $g \in G$ existiert mit $\mathrm{ord}(g) = p$. ***Satz von Cauchy***

(b) Sei $S \in \mathsf{Syl}_p(G)$. Dann gilt

$$S \trianglelefteq G \;\Leftrightarrow\; \mathsf{Syl}_p(G) = \{S\}.$$

Beweis. (a) Nach Theorem 3.13 (a) gibt es eine Untergruppe $H \leq G$ mit $|H| = p$. Nach Kapitel 2 gilt $H \cong \mathbb{Z}_p$. Somit existiert ein $g \in H$ mit $\mathrm{ord}(g) = p$.

(b) Nach Theorem 3.13 (b) sind alle p-Sylowuntergruppen konjugiert zu S.

□

Beweis der Sylowsätze. (a) Induktion über $|G| = p^n \cdot q$: G operiert auf sich selbst durch Konjugation (siehe Beispiel 3.6 (2)). Sei $\{x_i\}_{i \in I}$ ein Repräsentantensystem der nicht-zentralen Konjugationsklassen. Die Klassengleichung liefert

$$|G| = |Z(G)| + \sum_{i \in I} [G : C_G(x_i)].$$

Fall 1:

Angenommen p teilt nicht $|Z(G)|$. Da p aber $|G|$ teil, existiert ein $i \in I$, so dass p nicht $[G : C_G(x_i)] = \frac{|G|}{|C_G(x_i)|}$ teilt. Somit gilt $|C_G(x_i)| = p^n \cdot q'$ mit $\mathrm{ggT}(p, q') = 1$ und $|C_G(x_i)| < |G|$. Nach Induktionsvoraussetzung hat $C_G(x_i)$ eine Untergruppe der Ordnung p^k für alle $k \in \{1, \dots, n\}$. Also gilt dies auch für G.

Fall 2:

Angenommen p teilt $|Z(G)|$. Schreibe

$$Z(G) \cong \mathbb{Z}_{n_1} \times \cdots \times \mathbb{Z}_{n_s}$$

mit $1 < n_1 \leq \cdots \leq n_s$ und $n_1 | \dots | n_s$ (siehe Aufgabe M.4.1). Sei $j \in \{1, \dots, s\}$ mit $p | n_j$. In $\mathbb{Z}_{n_j}$ existiert somit ein Element der Ordnung p. Sei entsprechend $g \in Z(G)$ mit $\mathrm{ord}(g) = p$. Für $k = 1$ folgt die Behauptung. Sei also $k > 1$. Da $g \in Z(G)$, folgt $\langle g \rangle \trianglelefteq G$ mit

$$\left| {}^{G}\!/_{\langle g \rangle} \right| = p^{n-1} \cdot q.$$

Nach Induktionsvoraussetzung existiert eine Untergruppe $U \leq G/\langle g \rangle$ mit $|U| = p^{k-1}$. Satz 1.23 liefert uns eine Untergruppe $\langle g \rangle \leq H \leq G$ mit $H/\langle g \rangle = U$. Also gilt

$$|H| = |U| \dots |\langle g \rangle| = p^{k-1} \cdot p = p^k.$$

(b) Sei $H \leq G$ mit $|H| = p^k$ für $k \leq n$. Sei $S \in \mathsf{Syl}_p(G)$. Zu zeigen ist, dass ein $g \in G$ existiert mit $H \leq gSg^{-1}$.

Die Gruppe H operiert auf G/S durch Multiplikation (vgl. Beispiel 3.3 (4)). Es ist $|G/S| = q$. Mit Bemerkung 3.11 (i) gilt für die Fixpunktmenge dieser Operation

$$\left| {}^{G}\!/_{S}{}^{H} \right| \equiv \left| {}^{G}\!/_{S} \right| = q \mod p.$$

Da nach Voraussetzung $p \nmid |(G/S)^H|$. Somit existiert ein Fixpunkt $gS \in (G/S)^H$ für $g \in G$, d.h.

$$hgS = gS$$

für alle $h \in H$. Also $H \leq gSg^{-1}$, wie gewünscht.

(c) Zeige zunächst: $|\mathsf{Syl}_p(G)| \mid q$.

G operiert auf $\mathsf{Syl}_p(G)$ durch Konjugation. Sei $S \in \mathsf{Syl}_p(G)$. Nach Teil (b) entspricht die Bahn von S unter G ganz $\mathsf{Syl}_p(G)$, d.h. die Operation ist transitiv. Der Bahnsatz liefert

$$|\mathsf{Syl}_p(G)| \overset{\text{Satz 3.7}}{=} [G : \mathrm{Stab}_G(S)] \Big| [G : \mathrm{Stab}_G(S)] \cdot [\mathrm{Stab}_G(S) : S] \overset{\text{Satz 1.11}}{=} [G : S] = q.$$

Verbleibt zu zeigen: $|\mathsf{Syl}_p(G)| \equiv 1 \mod p$.

Sei $S \in \mathsf{Syl}_p(G)$. S operiert auf $\mathsf{Syl}_p(G)$ durch Konjugation. Inbesondere ist S auch Fixpunkt dieser Operation. Sei $S' \in \mathsf{Syl}_p(G)$ ein weiterer Fixpunkt, d.h.

$$gS'g^{-1} = S'$$

für alle $g \in S$. Daraus folgt

$$S \subseteq \mathrm{Stab}_G(S') := \{g \in G \mid gS'g^{-1} = S'\} \quad \textbf{Normalisator von } S' \textbf{ in } G$$

Behauptung: $S \subseteq S'$ und somit $S = S'$ wegen $|S| = |S'| < \infty$.

Es gilt $S' \trianglelefteq \mathrm{Stab}_G(S')$. Somit folgt $SS' = S'S \leq \mathrm{Stab}_G(S')$. Nach Satz 1.21 (a) erhalten wir

$$SS'/S' = S/S \cap S'.$$

Da S p-Gruppe, ist $(SS')/S$ trivial oder auch eine p-Gruppe. Da $S' \leq SS' \leq G$, erhalten wir

$$[SS' : S'] \Big| [G : SS'] \cdot [SS' : S'] \overset{\text{Satz 1.11}}{=} [G : S'] = q.$$

Da $\mathrm{ggT}(p, q) = 1$, folgt $p \nmid [SS' : S']$ und somit muss $|(SS')/S'| = 1$ bzw. $SS' = S'$. Also gilt $S \subseteq S'$ und somit $S = S'$ wie gewünscht.

Damit ist S der einzige Fixpunkt der Operation von S auf $\mathsf{Syl}_p(G)$ durch Konjugation. Bemerkung 3.11 (i) liefert nun $|\mathsf{Syl}_p(G)| \equiv 1 \mod p$.

□

Als Anwendung wollen wir die Struktur von Gruppen kleiner Ordnung besser verstehen und alle Gruppen bis Ordnung 15 klassifizieren!

Korollar 3.15. *(a) Sei $|G| = 2p$ mit $p \neq 2$ Primzahl. Dann gilt $G \cong \mathbb{Z}_{2p}$ oder $G \cong D_p$ (Diedergruppe).*

(b) Sei $|G| = pq$ mit $p < q$ Primzahlen, so dass $p \nmid q - 1$. Dann gilt $G \cong \mathbb{Z}_{pq} \cong \mathbb{Z}_p \times \mathbb{Z}_q$.

Beweis. (a) Nach Theorem 3.13 (c) gilt $|\mathsf{Syl}_p(G)| \mid 2$ und $|\mathsf{Syl}_p(G)| \equiv 1 \mod p$, also $\mathsf{Syl}_p(G) = \{S\}$ mit $S \cong \mathbb{Z}_p$. Sei $S = \langle g \rangle$ für ein $g \in G$ und $h \in G \setminus S$ mit $\mathrm{ord}(h) = 2$ (ein solches h existiert zum Beispiel nach Korollar 3.14 (a)). Es folgt, dass

$$G = \{1_G, g, g^2, \ldots, g^{p-1}, h, hg, hg^2, \ldots, hg^{p-1}\}.$$

Da $hg \notin S$, gilt $\mathrm{ord}(hg) = 2p$ oder $\mathrm{ord}(hg) = 2$. Im ersten Fall erhalten wir $G \cong \mathbb{Z}_{2p}$, im zweiten $G \cong D_p$.

(b) Nach Theorem 3.13 (c) gilt:

$$\begin{aligned} |\mathsf{Syl}_p(G)| \mid q \quad &\text{und} \quad |\mathsf{Syl}_p(G)| \equiv 1 \mod p, \\ |\mathsf{Syl}_q(G)| \mid p \quad &\text{und} \quad |\mathsf{Syl}_q(G)| \equiv 1 \mod q. \end{aligned}$$

Insbesondere ist $|\mathsf{Syl}_p(G)| \in \{1, q\}$. Aber $q \equiv 1 \mod p$ bedeutet $p \mid q-1$. Ein Widerspruch! Daraus folgt $\mathsf{Syl}_p(G) = \{S\}$ mit $S \cong \mathbb{Z}_p$. Ebenso ist $|\mathsf{Syl}_q(G)| \in \{1, p\}$. Da $p < q$, ist $p \equiv 1 \mod q$ aber nicht möglich, d.h. $\mathsf{Syl}_q(G) = \{H\}$ mit $H \cong \mathbb{Z}_q$.

Nach Korollar 3.14 (b) gilt $S, H \trianglelefteq G$. Zudem ist $S \cdot H = G$ und $S \cap H = \{1_G\}$. G ist also inneres direktes Produkt von S und H. Damit folgt die Behauptung (vgl. Bemerkung 2.9 (ii) und Aufgabe M.3.3).

□

Beispiel 3.16.

$\lvert G\rvert$	Mögliche Isomorphietypen
2	$\mathbb{Z}_2$
3	$\mathbb{Z}_3$
4	$\mathbb{Z}_4, \mathbb{Z}_2 \times \mathbb{Z}_2$ (siehe Aufgabe M.1.1)
5	$\mathbb{Z}_5$
6	$\mathbb{Z}_6, S_3 = D_3$ (siehe Korollar 3.15 (a))
7	$\mathbb{Z}_7$
8	$\mathbb{Z}_8, \mathbb{Z}_4 \times \mathbb{Z}_2, \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2, D_4, Q_8$

Q_8 heißt die **Quaternionengruppe**. Sie lässt sich zum Beispiel schreiben als Untergruppe von $\mathsf{SL}_2(\mathbb{C})$ erzeugt von den Matrizen

$$\mathfrak{A} = \begin{bmatrix} i & 0 \\ 0 & -i \end{bmatrix} \quad \text{und} \quad \mathfrak{B} = \begin{bmatrix} 0 & -1 \\ 1 & 0 \end{bmatrix}$$

Es gilt $Q_8 = \{\pm\mathfrak{E}_2, \pm\mathfrak{A}, \pm\mathfrak{B}, \pm\mathfrak{A}\mathfrak{B}\}$ und $\mathfrak{A}^2 = \mathfrak{B}^2 = (\mathfrak{A}\mathfrak{B})^2 = -\mathfrak{E}_2$.

9	$\mathbb{Z}_9, \mathbb{Z}_3 \times \mathbb{Z}_3$ (siehe Aufgabe M.6.1 (b))
10	$\mathbb{Z}_{10}, D_5$ (siehe Korollar 3.15 (a))
11	$\mathbb{Z}_{11}$
12	$\mathbb{Z}_{12}, \mathbb{Z}_2 \times \mathbb{Z}_6, D_6, A_4, H$

Die Gruppe H können wir zum Beispiel als Untergruppe von $S_3 \times \mathbb{Z}_4$ realisieren. Sei dazu $H = \{(\sigma, x) \mid \operatorname{sgn}(\sigma) = 1 \Leftrightarrow x \text{ gerade}\} \trianglelefteq S_3 \times \mathbb{Z}_4$, also

$$\begin{aligned} H = \{&(\mathrm{id}, \bar{0}), (\mathrm{id}, \bar{2}), ((123), \bar{0}), ((132), \bar{0}), ((123), \bar{2}), ((132), \bar{2}), \\ &((12), \bar{1}), ((12), \bar{3}), ((13), \bar{1}), ((13), \bar{3}), ((23), \bar{1}), ((23), \bar{3})\} \end{aligned}$$

H wird zum Beispiel erzeugt von $a = ((123), \bar{2})$ und $b = ((12), \bar{1})$. mit $\operatorname{ord}(a) = 6, a^3 = b^2, ba = a^{-1}b$.

13	$\mathbb{Z}_{13}$
14	$\mathbb{Z}_{14}, D_7$ (siehe Korollar 3.15 (a))
15	$\mathbb{Z}_{15}$ (siehe Korollar 3.15 (b))

4 Ringe

Definition 4.1. Ein **Ring** $(R, +\cdot)$ ist eine Menge mit binären Verknüpfungen

$$\begin{aligned} +\colon R \times R \to R \quad &\text{mit} \quad (r,s) \mapsto r + s \\ \cdot\colon R \times R \to R \quad &\text{mit} \quad (r,s) \mapsto r \cdot s, \end{aligned}$$

so dass gilt

(R1) $(R, +)$ ist eine abelsche Gruppe.

(R2) Für alle $a, b, c \in R$ gilt $(a \cdot b) \cdot c = a \cdot (b \cdot c)$ ($\cdot$ **ist assoziativ**).

(R3) Für alle $a, b, c \in R$ gilt $a \cdot (b + c) = a \cdot b + a \cdot b$ und $(a + b) \cdot c = a \cdot c + b \cdot c$. (**Distributivgesetze**)

(R4) Es existiert $1 \in R$ mit $a \cdot 1 = a = 1 \cdot a$ (**Ring mit Eins**).

(R5) Gilt $a \cdot b = b \cdot a$ für alle $a, b \in R$, so heißt R **kommutativ**.

Für $a \cdot b$ schreiben wir auch ab.

Bemerkung 4.2. (i) Es gilt $a \cdot 0 = 0 = 0 \cdot a$ für alle $a \in R$.

$$a \cdot 0 = a \cdot (0 + 0) = a \cdot 0 + a \cdot 0 \;\Rightarrow\; a \cdot 0 = 0$$

$0 \cdot a = 0$ folgt analog.

(ii) Es gilt $(-a)b = -(ab) = a(-b)$ für alle $a, b, c \in R$.

$$(-a)b + ab = (-a + a)b = 0 \cdot b = 0$$

Daraus folgt $(-a)b = -(ab)$ und die zweite Gleichung analog.

(iii) Das Einselement in R ist eindeutig. Ist $1_R = 0_R$, so gilt $R = \{0_R\}$.

Beispiel 4.3. (1) $\mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}$ sind kommutative Ringe. $(\mathbb{Z}_n, +, \cdot)$ ist ein kommutativer Ring.

(2) Sei R ein kommutativer Ring. Dann heißt

$$R[x] := \{a_0 + a_1 x + \cdots + a_n x^n \mid n \in N_0, a_i \in R, 0 \leq i \leq n\}$$

Polynomring in einer Variablen x **über** R und $f \in R[x]$ heißt **Polynom**.

<u>Addition:</u>

$$\sum_{i=0}^{n} a_i x^i + \sum_{i=0}^{m} b_i x^i := \sum_{i=0}^{\max\{m,n\}} (a_i + b_i) x^i$$

<u>Multiplikation:</u>

$$\left(\sum_{i=0}^{n} a_i x^i\right) \cdot \left(\sum_{i=0}^{n} b_i x^i\right) := \sum_{i=0}^{n+m} \left(\sum_{p+q=i} a_p b_q\right) x_i,$$

wobei $a_i := 0$ für alle $i \geq n + 1$ und $b_i := 0$ für alle $i \geq m + 1$. Es gilt $0_{R[x]} = 0_R$ und $1_{R[x]} = 1_R$. Formal sind Polynome Folgen $(a_i)_{i \in \mathbb{N}_0}$ mit $a_i = 0$ für alle bis auf endlich viele Folgenglieder. Setze dazu

$$1_R := (1, 0, 0, 0, \dots) \quad \text{und} \quad x := (0, 1, 0, 0, \dots).$$

Induktiv folgt $x^j = (\underbrace{0, \dots, 0}_{j \text{ Nullen}}, 1, 0, \dots)$. Das Polynom $\sum_{i=0}^{n} a_i x^i$ entspricht genau der Folge $(a_i)_{i \in \mathbb{N}_0}$. Zwei Polynome $\sum_{i=0}^{n} a_i x_i$ und $\sum_{i=0}^{m} b_i x^i$ sind gleich genau dann, wenn $(a_i)_{i \in \mathbb{N}_0} = (b_i)_{i \in \mathbb{N}_0}$.

(3) Sei $(G,+)$ eine abelsche Gruppe. Dann ist

$$\mathrm{End}(G) := \{\varphi\colon G \to G \mid \varphi \text{ Gruppenhomomorphimus}\}$$

ein Ring durch

$$\begin{aligned}(\varphi+\psi)(g) &:= \varphi(g)+\psi(g)\\ (\varphi\cdot\psi) &:= \varphi(\psi(g))\end{aligned}$$

für alle $\varphi,\psi \in \mathrm{End}(G), g \in G$. Es gilt $0_{\mathrm{End}(G)} = (\varphi\colon g \mapsto 0_G)$ und $1_{\mathrm{End}(G)} = \mathrm{id}_G$. End heißt **Endomorphismenring von** G.

(4) Sei $n \in \mathbb{Z}$. Dann ist $\mathbb{Z}[\sqrt{n}] := \{a + b\sqrt{n} \mid a,b \in \mathbb{Z}\}$, sprich $\mathbb{Z}$ **adjungiert** $\sqrt{n}$, ein Ring durch

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

(vergleiche Multiplikation in $\mathbb{C}$). Es gilt $0_{\mathbb{Z}[\sqrt{n}]} = 0_{\mathbb{Z}}$ und $1_{\mathbb{Z}[\sqrt{n}]} = 1_{\mathbb{Z}}$. $\mathbb{Z}[\sqrt{-1}] = \mathbb{Z}[i]$ heißt **Ring der Gaußschen Zahlen**.

(5) Seien R und S Ringe. Dann ist $R \times S$ ein Ring durch komponentenweise Addition und Multiplikation. Es gilt $0_{R\times S} = (0_R, 0_S)$ und $1_{R\times S} = (1_R, 1_S)$.

Definition 4.4. Seien R und S Ringe

(a) Eine Abbildung $\varphi\colon R \to S$ heißt **Ringhomomorphismus**, falls

- $\varphi(1_R) = 1_S$.
- $\varphi(a+b) = \varphi(a)+\varphi(b)$.
- $\varphi(a\cdot b) = \varphi(a)\cdot\varphi(b)$.

für alle $a,b,c \in R$. Ist φ zusätzlich bijektiv, sprechen wir von einem **Isomorphismus**. Die Ringe R und S sind dann isomorph. Schreibe $R \cong S$.

(b) S heißt **Unterring** von R, falls $S \subseteq R$ und die Inklusionsabbildung $S \to R$ ein Ringhomomorphismus ist. Schreibe dafür $S \leq R$.

Bemerkung 4.5. (i) Jeder Ringhomomorphismus $\varphi\colon R \to S$ ist ein Gruppenhomomorphismus bezüglich $+$. Insbesondere ist φ injektiv genau dann, wenn

$$\mathrm{Ker}(\varphi) := \{a \in R \mid \varphi(a) = 0_S\} = \{0_R\}.$$

(siehe Beispiel 1.6 (6)).

(ii) Isomorphe Ringe betrachten wir als wesensgleich.

(iii) Sei R ein Ring und $S \subseteq R$. Dann gilt

$$S \leq R \text{ Unterring } \Leftrightarrow\ 1_R \in S, (S,+) \leq (R,+) \text{ und } a,b \in S \ \Rightarrow\ a\cdot b \in S.$$

Beispiel 4.6. (1) Es gilt $\mathbb{Z} \leq \mathbb{Q} \leq \mathbb{R} \leq \mathbb{C}$ sowie $\mathbb{Z}[\sqrt{n}] \leq \mathbb{C}$. Das **Zentrum**

$$Z(R) := \{a \in R \mid ar = ra \text{ alle } r \in R\}$$

ist Unterring eines Rings R. Für R kommutativ ist $R \leq R[x]$.

(2) Sei K ein Körper und V ein K-Vektorraum mit Basis

$$B = (v_1, \ldots, v_n)$$

für $n \in \mathbb{N}$. Dann ist $\mathrm{End}_K(V) = \{\varphi\colon V \to V \mid \varphi \text{ linear}\}$ ein Ring (vgl. Beispiel 4.3 (3)). Wir erhalten einen Ringisomorphismus $\mathrm{End}_K(V) \xrightarrow{\sim} M_n(K)$ mit $\varphi \mapsto M_B(\varphi)$, wobei $M_B(\varphi)$ die darstellende Matrix von φ bezüglich B ist.

(3) Sei $\varphi\colon R \to S$ ein Ringhomomorphismus von kommutativen Ringen und $s \in S$. Dann erhalten wir einen Ringhomomorphismus $\varphi_s\colon R[x] \to S$ durch

$$\sum_i a_i x^i \mapsto \sum_i \varphi(a_i) s^i.$$

φ_s heißt **Einsetzungshomomorphismus**. In der Tat gilt

$$\begin{aligned}
\varphi_s\left(\left(\sum_i a_i x^i\right) \cdot \left(\sum_i b_i x^i\right)\right) &= \varphi_s\left(\sum_i \left(\sum_{p=0}^{i} a_p b_{i-p}\right) x^i\right) \\
&= \sum_i \varphi\left(\sum_{p=0}^{i} a_p b_{i-p}\right) s^i \\
&= \sum_i \sum_{p=0}^{i} \varphi(ap)\varphi(b_{i-p}) s^i \\
&= \sum_i \left(\sum_i \varphi(a_i) s^i\right)\left(\sum_i \varphi(b_i) s^i\right) \\
&= \varphi_s\left(\sum_i a_i x^i\right) \varphi_s\left(\sum_i b_i x^i\right)
\end{aligned}$$

φ_s ist der eindeutige Ringhomomorphismus mit $\varphi_s(x) = s$, der das folgende Diagramm kommutieren lässt.

$$\begin{tikzcd}
R \arrow[r, "\varphi"] \arrow[d, "\text{Inklusion}"'] & S \\
R[x] \arrow[ur, "\varphi_s"] &
\end{tikzcd}$$

Ist $R \leq S$ und $\varphi\colon R \to S$ die Inklusionsabbildung, so ist $\mathrm{Im}(\varphi_s) = \{\sum_{i=0}^{n} a_i s^i \mid n \in \mathbb{N}_0, a_i \in R, 0 \leq i \leq n\} =: R[s]$ („R **adjungiert** S“), der kleinste Unterring von S, der R und s enthält (vgl. Beispiel 4.3 (4)).

Ist $S = \mathrm{Abb}(R, R)$ mit punktweiser Addition und Multiplikation (siehe Aufgabe M.7.1) und $\varphi\colon R \to \mathrm{Abb}(R, R)$ der Ringhomomorphismus mit

$$a \mapsto (\varphi_a\colon x \mapsto a),$$

So ist $\varphi_{\mathrm{id}_R}\colon R[x] \to \mathrm{Abb}(R,R)$ gegeben durch

$$\sum_i a_i x^i \longmapsto \left(\sum_i \varphi(a_i)\mathrm{id}_R^i = \sum_i \varphi_{a_i}\mathrm{id}_R^i : x \mapsto \sum_i a_i x^i\right)$$

φ_{id_R} schickt ein Polynom auf die zugehörige Polynomfunktion. Da φ_{id_R} im Allgemeinen nicht injektiv ist, müssen wir zwischen Polynomen und Polynomfunktionen unterscheiden! Zum Beispiel: $x^2 + x$ ist nicht das Nullpolynom, die zugehörige Polynomfunktion

$$\mathbb{Z}_2 \to \mathbb{Z}_2 \quad \text{mit} \quad x \mapsto x^2 + x$$

aber die Nullfunktion.

> Wir wollen Quotienten von Ringen betrachten. Unterringe eignen sich dazu nicht. Wir brauchen ein neues Konzept.

Definition 4.7. Sei R ein Ring und $(I,+) \leq (R,+)$ eine Untergruppe. Dann heißt

- I **Linksideal**, wenn $r \cdot i \in I$ für alle $r \in R, i \in I$.
- I **Rechtsideal**, wenn $i \cdot r \in I$, für alle $r \in R, i \in I$.
- **zweiseitiges Ideal**, wenn I Links- und Rechtsideal ist.

Schreibe $I \trianglelefteq R$ oder genauer $I \trianglelefteq_\ell R$ bzw. $I \trianglelefteq_r R$ bzw. $I \trianglelefteq_2 R$. Ist R kommutativ, ist diese Unterscheidung nicht notwendig!

Bemerkung 4.8. (i) Ist $I \trianglelefteq R$ und $1_R \in I$, so ist $I = R$. Insbesondere sind Ideale mit $I \triangleleft R$ (echt in R) nach unserer Definition keine Unterringe.

(ii) Seien $I, J \trianglelefteq R$. Dann gilt $I \cap J \trianglelefteq R$, sowie

$$\begin{aligned} I + J &:= \{i + j \mid i \in I, j \in J\} \trianglelefteq R \\ I \cdot J &:= \left\{\sum_{k=1}^{n} i_k j_k \mid n \in \mathbb{N}, i_k \in I, j_k \in J, 1 \leq k \leq n\right\} \trianglelefteq R \end{aligned}$$

(iii) Für $a_1, \ldots, a_s \in R$ heißt

$$(a_1, \ldots, a_s) := Ra_1 + \cdots + Ra_s = \{r_1 a_1 + \cdots + r_s a_s \mid r_i \in R\} \trianglelefteq_\ell R$$

das von $a_1, \ldots, a_s$ **erzeugte Linksideal in** R. Es ist das kleinste Linksideal in R, das $a_1, \ldots, a_s$ enthält. Analog können wir Rechtsideale und zweiseitige Ideale in R erzeugen.

Ein Ideal, das von einem Element erzeugt wird, heißt **Hauptideal**.

Beispiel 4.9. (1) $\{0_R\}$ und R sind Hauptideale eines Rings R.

(2) Ideale in $R = \mathbb{Z}$ sind Hauptideale und von der Form $n\mathbb{Z}$ für $n \in \mathbb{N}_0$.

(3) Sei $R = M_2(K)$ für einen Körper K. Sei I das von

$$\begin{bmatrix} 1 & 0 \\ 0 & 0 \end{bmatrix} \in R$$

erzeugte Linksideal, d.h.

$$I = R\begin{bmatrix}1 & 0\\ 0 & 0\end{bmatrix} = \left\{\begin{bmatrix}a & 0\\ b & 0\end{bmatrix} : a, b \in K\right\}$$

I ist jedoch kein zweiseitiges Ideal in R, da z. B.

$$\begin{bmatrix}1 & 0\\ 1 & 0\end{bmatrix} \cdot \begin{bmatrix}1 & 1\\ 1 & 0\end{bmatrix} = \begin{bmatrix}1 & 1\\ 1 & 1\end{bmatrix} \notin I.$$

Zweiseitige Ideale in $R = M_2(K)$ sind trivial (siehe Aufgabe M.7.3).

(4) Ist $\varphi\colon R \to S$ ein Ringhomomorphismus, so gilt

$$\mathrm{Ker}(\varphi) \trianglelefteq_2 R \quad \text{und} \quad \mathrm{Im}(\varphi) \leq S.$$

Zweiseitige Ideale sind in der Tat genau Kerne von Ringhomomorphismen (vgl. Proposition 1.18).

Satz 4.10. *Sei R ein Ring und $I \trianglelefteq_2 R$. Dann wird die Quotientengruppe $R/I = \{r + I \mid r \in R\}$ zu einem Ring durch*

$$(r + I) \cdot (s + I) := rs + I \quad \textit{für } r, s \in R$$

*$(R/I, +, \cdot)$ heißt **Quotientenring von R modulo I**. Die Abbildung $\pi\colon R \to R/I$ mit $r \mapsto r + I$ ist surjektiver Ringhomomorphismus mit $\mathrm{Ker}(\pi) = I$.*

Beweis. Die Multiplikation ist wohldefiniert:
Sei $r + I = r' + I$ und $s + I = s' + I$ bzw. $r' - r \in I$ und $s - s' \in I$. Zu zeigen ist also $rs + I = r's' + I$ bzw. $rs - r's' \in I$.

$$rs - r's' = -r' \underbrace{(s' - s)}_{\in I} - \underbrace{(r' - r)}_{\in I} s \in I,$$

da $I \trianglelefteq_2 R$. Die Ringaxiome für R/I folgen aus den Ringaxiomen für R. Insbesondere ist $1_{R/I} = 1_R + I$. Die Projektion π ist ein surjektiver Gruppenhomomorphismus mit $\mathrm{Ker}(\pi) = I$ nach Satz 1.16. Zudem gilt $\pi(1_R) = 1_{R/I}$ sowie

$$\pi(r \cdot s) = r \cdot s + I = (r + I) \cdot (s + I) = \pi(r) \cdot \pi(s)$$

für alle $r, s \in R$. Also ist π auch ein Ringhomomorphismus. □

Analog zur Gruppentheorie gilt der

Satz 4.11 (Homomorphiesatz und Isomorphiesätze). *(a) Sei $\varphi\colon R \to S$ ein Ringhomomorphismus. Dann gilt*

$$R/\mathrm{Ker}(\varphi) \cong \mathrm{Im}(\varphi).$$

(b) Sei $S \leq R$ und $I \trianglelefteq_2 R$. Dann gilt

$$I + S/I \cong S/I \cap S.$$

(c) Seien $I \leq J$ zweiseitige Ideale in R. Dann gilt

$$R/I \big/ _{J/I} \cong R \big/ _J.$$

Beweis. Aussagen folgen analog zu Satz 1.20 und Satz 1.21. Die dort konstruierten Gruppenisomorphismen sind Ringisomorphismen. In (b) gilt zudem, dass $I + S \leq R$ nach Aufgabe S.7.3. $\square$

Beispiel 4.12. Betrachte den Einsetzungshomomorphismus $\varphi_i \colon \mathbb{R}[x] \to \mathbb{C}$ mit $f \mapsto f(i)$ (siehe Beispiel 4.6 (3)). Wir haben durch Inklusion

$$\begin{tikzcd}
\mathbb{R} \arrow[r, "\varphi=\text{Inklusion}"] \arrow[d, "\text{Inklusion}"'] & \mathbb{C} \\
R[x] \arrow[ur, "\varphi_i"] &
\end{tikzcd}$$

mit $\mathrm{Im}(\varphi_i) = \mathbb{R}[i] = \mathbb{C}$. Es gilt $\mathrm{Ker}(\varphi_i) = (x^2+1) \trianglelefteq \mathbb{R}[x]$ (dazu später mehr) und mit Satz 4.11 (a) folgt $R[x]/(x^2+1) \cong \mathbb{C}$.

Satz 4.13 (Idealkorrespondenz)**.** *Sei $\varphi \colon R \to S$ ein Ringhomomorphismus. Dann gilt*

(a) Ist $J \trianglelefteq S$, so gilt $\varphi^{-1}(J) = \{a \in R \mid \varphi(a) \in J\} \trianglelefteq R$.

(b) Ist φ surjektiv, so existiert eine Bijektion

$$\begin{aligned}\{I \trianglelefteq R \mid \mathrm{Ker}(\varphi) \subseteq I\} &\to \{\textit{Ideale in } S\} \\ I &\mapsto \varphi(I).\end{aligned}$$

Beweis. (a) Im Beweis von Satz 1.23 haben wir gesehen, dass

$$\varphi^{-1}(J), +) \leq (R, +).$$

Sei nun $a \in \varphi^{-1}(J)$ und $r \in R$. OBdA verstehen wir $\trianglelefteq$ als $\trianglelefteq_\ell$. Dann gilt

$$\varphi(ra) = \underbrace{\varphi(r)}_{\in S}\underbrace{\varphi(a)}_{\in J} \in J$$

da $J \trianglelefteq S$. Also $ra \in \varphi^{-1}(J)$ und somit $\varphi^{-1}(J) \trianglelefteq R$.

(b) Die Zuordnung ist wohldefiniert , da für $I \trianglelefteq R$ gilt:

$$(\varphi(I), +) \leq (S, +)$$

und weil φ surjektiv ist, existiert $r \in R$, so dass $\varphi(r) = s$, gilt

$$s\varphi(i) = \varphi(r)\varphi(i) = \varphi(\underbrace{ri}_{\in I}) \in \varphi(I)$$

für alle $s \in S$ und alle $i \in I$. Die Umkehrabbildung ist gegeben durch die Zuordnung aus **(a)**

$$S \trianglerighteq J \mapsto \varphi^{-1}(J) \trianglelefteq R,$$

wobei offensichtlich $\mathrm{Ker}(\varphi) \leq \varphi^{-1}(J)$. In der Tat gilt $\varphi(\varphi^{-1}(J)) = J$ nach Definition und da φ surjektiv. Wir vergewissern uns noch, dass auch $I = \varphi^{-1}(\varphi(I))$.

„$\subseteq$“: Für alle $i \in I$ gilt $i \in \varphi^{-1}(\varphi(i))$, also $I \subseteq \varphi^{-1}(\varphi(I))$.

„$\supseteq$“: Sei $r \in \varphi^{-1}(\varphi(I))$, d.h. $\varphi(r) \in \varphi(I)$. Dann existiert $i \in I$ mit $\varphi(r) = \varphi(i)$. Somit gilt $\varphi(r-i) = \varphi(r) - \varphi(i) = 0_S$, also $r - i \in \mathrm{Ker}(\varphi) \subseteq I$. Es folgt $r \in I$ und daher $\varphi^{-1}(\varphi(I)) \subseteq I$.

$\square$

Bemerkung 4.14. Die Surjektivität von φ aus Satz 4.13 ist wichtig! Betrachte die Inklusion $\varphi\colon \mathbb{Z} \to \mathbb{Q}$. $I := n\mathbb{Z} \trianglelefteq \mathbb{Z}$ für $n \in \mathbb{N}$. Dann ist $\varphi(I) = I$, aber kein Ideal in $\mathbb{Q}$, da z. B. $\frac{1}{2} \cdot n \notin I$ für n ungerade.

Satz 4.15. *Sei R ein Ring und $I_1, I_2 \trianglelefteq_2 R$ mit $I_1 + I_2 = R$. Dann gilt*

$$R/_{I_1 \cap I_2} \cong R/_{I_1} \times R/_{I_2} \quad \textit{mittels} \quad (r + I_1 \cap I_2) \mapsto (r + I_1, r + I_2)$$

Beweis. Die Zuordnung $r \mapsto (r + I_1, r + I_2)$ liefert einen Ringhomomorphismus $\psi\colon R/I_1 \times R/I_2$ mit $\mathrm{Ker}(\psi) = I_1 \cap I_2$. Die Behauptung ist nun, dass ψ surjektiv ist.
Sei $(a + I_1, b + I_2) \in R/I_1 \times R/I_2$. Da $I_1 + I_2 = R$ existiert $i_1 \in I_1, i_2 \in I_2$ mit $i_1 + i_2 = 1_R$. Es gilt

$$\psi(i_1) = (i_1 + I_1, i_1 + I_2) = (0_R + I_1, (1_R - i_2) + I_2) = (0_R + I_1, 1_R + I_2).$$

Analog folgt $\psi(i_2) = (1_R + I_1, 0_R + I_2)$. Wir erhalten

$$\begin{aligned}
\psi(bi_1 + ai_2) &= \psi(b)\psi(i_1) + \psi(a)\psi(i_2) \\
&= (b + I_1, b + I_2) \cdot (0_R + I_1, 1_R + I_2) + (a + I_1, a + I_2) \cdot (1_R + I_1, 0_R + I_2) \\
&= (0_R + I_1, b + I_2) + (a + I_1, 0_R + I_2) \\
&= (a + I_1, b + I_2)
\end{aligned}$$

Somit ist ψ surjektiv. Nach Satz 4.11 (a) folgt

$$R/_{I_1 \cap I_2} = R/_{\mathrm{Ker}(\psi)} \cong \mathrm{Im}(\psi) = R/_{I_1} \times R/_{I_2}.$$

$\square$

Korollar 4.16. *Sei $m \in \mathbb{N}$ und $m = \prod_{i=1}^{t} m_i$ eine Zerlegung in paarweise teilerfremde $m_i \in \mathbb{N}$. Dann gilt*

$$\mathbb{Z}/_{m\mathbb{Z}} \cong \mathbb{Z}/_{m_1\mathbb{Z}} \times \cdots \times \mathbb{Z}/_{m_t\mathbb{Z}} \quad \textit{mittels} \quad x + m\mathbb{Z} \mapsto (x + m_1\mathbb{Z}, \ldots, x + m_t\mathbb{Z}).$$

Insbesondere gibt es zu $c_1, \ldots, c_t \in \mathbb{Z}$ stets eine eindeutige Zahl x modulo m mit

$$x \equiv c_i \mod m_i \quad \textit{für} \quad 1 \leq i \leq t.$$

Genannt ***Chinesischer Restsatz****.*

Beweis. Induktion nach t: Für $t = 1$ ist nichts zu zeigen. Sei $t > 1$. Es gilt

$$\prod_{i=1}^{t-1} m_i\mathbb{Z}_i, m_t\mathbb{Z} \trianglelefteq \mathbb{Z}$$

mit

$$\prod_{i=1}^{t-1} m_i\mathbb{Z} + m_t\mathbb{Z} = \operatorname{ggT}\left(\prod_{i=1}^{t-1} m_i, m_t\right)\mathbb{Z} = \mathbb{Z}$$

und

$$\prod_{i=1}^{t-1} m_i\mathbb{Z} \cap m_t\mathbb{Z} = \operatorname{kgv}\left(\prod_{i=1}^{t-1} m_i, m_t\right)\mathbb{Z} = m\mathbb{Z}.$$

Daraus folgt, dass

$$\mathbb{Z}/m\mathbb{Z} \overset{\text{Satz 4.15}}{\cong} \mathbb{Z}/\prod_{i=1}^{t-1} m_i\mathbb{Z} \times \mathbb{Z}/m_t\mathbb{Z} \overset{\text{IV}}{\cong} \mathbb{Z}/m_1\mathbb{Z} \times \cdots \times \mathbb{Z}/m_t\mathbb{Z}$$

□

Beispiel 4.17. Finde $x \in \mathbb{Z}$ mit $x \equiv 1 \mod 5$ und $x \equiv 0 \mod 7$. Da $\operatorname{ggT}(5,7) = 1$, gilt $5\mathbb{Z} + 7\mathbb{Z} = \mathbb{Z}$. Bestimme $a, b \in \mathbb{Z}$ mit $5a + 7b = 1$ (siehe Lemma von Bézout). Division mit Rest bzw. der euklidische Algorithmus liefert

$$\begin{aligned} 7 &= 1 \cdot 5 + 2 \\ 5 &= 2 \cdot 2 + 1 \\ 2 &= 1 \cdot 2 + 0 \end{aligned}$$

und somit $1 = 5 - (2 \cdot 2) = 5 - 2 \cdot (7 - 5) = 3 \cdot 5 - 2 \cdot 7$. Dem Beweis von Satz 4.15 folgend, wähle nun

$$x := 0 \cdot 15 + 1 \cdot (-14)$$

mit $x = -14 \equiv 21 \mod 35$. Dies ist nun die eindeutige Zahl x modulo 35 mit $x \equiv 1 \mod 5$ und $x \equiv 0 \mod 7$ (siehe Korollar 4.16).

5 Einheiten, Nullteiler und euklidische Ringe

Im Folgenden sei $R \neq \{0_R\}$ ein Ring.

Definition 5.1. Elemente der Menge $R^\times := \{a \in R \mid \exists b \in R : ab = 1_R = ba\}$ heißen **Einheiten von** R oder **invertierbar**. Ein Ring mit $R^\times = R \setminus \{0_R\}$ heißt **Schiefkörper**. Ein kommutativer Schiefkörper heißt **Körper**.

Bemerkung 5.2. (i) $(R^\times)$ bildet eine Gruppe, die **Einheitengruppe in** R.

(ii) Sei R kommutativ. Es gilt R ist genau dann ein Körper, wenn R nur die Ideale $\{0_R\}$ und R hat.

Beweis. „$\Leftarrow$“: Sei $\{0_R\} \neq I \trianglelefteq R$ und $x \in I \setminus \{0_R\}$. Nach Voraussetzung ist x invertierbar, so dass $xx^{-1} = 1_R \in I$. Also $I = R$.

„$\Rightarrow$“: Sei $a \in R \setminus \{0_R\}$ und $I = (a) \trianglelefteq R$. Da $I \neq \{0_R\}$, gilt $I = R$ und somit existiert $b \in R$ mit $ab = 1_R$. Also $a \in R^\times$. □

Beispiel 5.3. (1) Es ist $\mathbb{Z}^\times = \{1, -1\}$ und $\mathbb{Q}^\times = \mathbb{Q} \setminus \{0\}$.

(2) Es gilt $\mathbb{Z}[i]^\times = \{1, -1, i, -i\}$ (als Gruppe isomorph zu $\mathbb{Z}_4$).

Beweis. Sei $w \in \mathbb{Z}[i]^\times$ und $z \in \mathbb{Z}[i]$ mit $wz = 1$. Komplexe Konjugation liefert $1 = 1 \cdot 1 = wz\overline{wz} = |w|^2 \cdot |z|^2$, d.h. $1 = |w|^2 = |a + ib|^2 = a^2 + b^2$ für $a, b \in \mathbb{Z}$. Also entweder $a = \pm 1$ und $b = 0$ oder $a = 0$ und $b = \pm 1$. □

(3) Es gilt $\mathbb{Z}_n^\times = \{\bar{a} \in \mathbb{Z}_n \mid \mathrm{ggT}(a, n) = 1\}$ für $n > 1$. Insbesondere ist $\mathbb{Z}_n$ ein Körper genau dann, wenn n Primzahl.

Beweis. Sei $\bar{a} \in \mathbb{Z}_n^\times$. Dann existiert $\bar{b} \in \mathbb{Z}_n$ mit $\bar{a} \cdot \bar{b} = \overline{ab} = \bar{1}$, d.h. $ab \equiv 1 \mod n$. Also existiert $c \in \mathbb{Z}$ mit $ab + cn = 1$ und $\mathrm{ggT}(a, n) = 1$. Sei $\mathrm{ggT}(a, n) = 1$. Dann existieren $b, c \in \mathbb{Z}$ mit $ab + cn = 1$. Daraus folgt

$$\bar{a} \cdot \bar{b} = \overline{ab} = \overline{1 - cn} = \bar{1} - \overline{cn} = \bar{1}.$$

Also $\bar{a} \in \mathbb{Z}_n^\times$. □

Die Zuordnung $n \mapsto |\mathbb{Z}_n^\times|$ definiert eine Abbildung $\varphi \colon \mathbb{N} \to \mathbb{N}$, die **Eulersche φ-Funktion** genannt wird. Es gilt $\varphi(1) := 1$ sowie

$$\begin{array}{lll} \varphi(2) = |\mathbb{Z}_2^\times| = 1 & \varphi(4) = |\mathbb{Z}_4^\times| = 2 & \varphi(6) = |\mathbb{Z}_6^\times| = 2 \\ \varphi(3) = |\mathbb{Z}_3^\times| = 2 & \varphi(5) = |\mathbb{Z}_5^\times| = 4 & \varphi(7) = |\mathbb{Z}_7^\times| = 6 \end{array}$$

φ ist multiplikativ, d.h. für $n = n_1 n_2$ mit $\mathrm{ggT}(n_1, n_2) = 1$ gilt:

$$\varphi(n) = \varphi(n_1) \cdot \varphi(n_2).$$

Beweis. Nach Korollar 4.16 gilt $\mathbb{Z}_n \cong \mathbb{Z}_{n_1} \times \mathbb{Z}_{n_2}$ und somit

$$\mathbb{Z}_n^\times \cong (\mathbb{Z}_{n_1} \times \mathbb{Z}_{n_2})^\times = \mathbb{Z}_{n_1}^\times \times \mathbb{Z}_{n_2}^\times.$$

□

Wir wollen im Folgenden wesentliche Eigenschaften von $\mathbb{Z}$ abstrahieren:

- Für alle $a, b, c \in \mathbb{Z}$ gilt: $a \cdot b = 0 \Rightarrow a = 0 \vee b = 0$.
- Existenz einer Division mit Rest.
- Existenz einer eindeutigen Primfaktorzerlegung.

Definition 5.4. Ein Element $a \in R \setminus \{0_R\}$ heißt **Nullteiler**, falls ein Element $b \in R \setminus \{0_R\}$ existiert mit $ab = 0_R$ oder $ba = 0_R$. Ein kommutativer Ring ohne Nullteiler heißt **Integritätsbereich**.

Beispiel 5.5. (1) Jeder Körper K ist Integritätsbereich, da für $a, b \in K$ mit $b \neq 0_K$ gilt: $ab = 0_K \Rightarrow abb^{-1} = 0_K b^{-1} = 0_K$. Allgemein sind Einheiten niemals Nullteiler.

Ist R Integritätsbereich und $S \leq R$, so ist auch S Integritätsbereich. Insbesondere ist zum Beispiel $\mathbb{Z}[\sqrt{n}] \leq \mathbb{C}$ ein Integritätsbereich für $n \in \mathbb{Z}$. Endliche Integritätsbereiche sind Körper. Insbesondere ist $\mathbb{Z}_n$ ein Integritätsbereich genau dann, wenn n Primzahl (siehe Beispiel 5.3 (3)).

Beweis. Betrachte $a \in R \setminus \{0_R\}$ und die Abbildung $\varphi_a \colon R \to R$ mit $r \mapsto ar$. φ_a ist injektiv, da aus $ar_1 = ar_2$ folgt $0_R = ar_1 - ar_2 = a(r_1 - r_2)$ und somit $r_1 - r_2 = 0_R$ bzw. $r_1 = r_2$. Da R endlich, ist φ_a sogar bijektiv, d.h. es existiert $r \in R$ mit $\varphi_a(r) = ar = 1_R$. Also ist $a \in R^\times$ und R ein Körper. $\square$

(2) Sind R und S nicht-triviale Ringe, so hat $R \times S$ stets Nullteiler, da $(r, 0_S) \cdot (0_R, S) = 0_{R \times S}$ für $r \neq 0_R$ und $s \neq 0_S$.

(3) Die Standardmatrizen $\mathfrak{E}_{ij}$ sind Nullteiler in $M_n(K)$ für $n \geq 2$ und einem Körper K.

Analog zur Einbettung $\mathbb{Z} \to \mathbb{Q}$ können wir jeden Integritätsbereich R in einen Körper einbetten. Betrachte dazu die Äquivalenzrelation auf $R \times R \setminus \{0_R\}$ gegeben durch

$$(r, s) \sim (x, y) \;:\Leftrightarrow\; sx = ry.$$

Reflexivität und Symmetrie gelten, da R kommutativ ist. Für Transitivität betrachte $(a, b) \sim (r, s)$ und $(r, s) \sim (x, y)$, d.h. $br = as$ und $sx = ry$. Dann gilt $say = asy = bry = bsx = sbx$. Da $s \neq 0_R$ und R Integritätsbereich, folgt $ay = bx$ und somit $(a, b) \sim (x, y)$, wie gewünscht. Schreibe $\frac{r}{s} := [(r, s)]$ für die Äquivalenzklasse von (r, s). Dann ist

$$\frac{r}{s} = \frac{x}{y} \Leftrightarrow sx = ry.$$

$\mathrm{Quot}(R) := \{\frac{r}{s} \mid r \in R, s \in R \setminus \{0_R\}\}$ heißt **Quotientenkörper von** R.

Satz 5.6. *Sei R ein Integritätsbereich. Dann ist $\mathrm{Quot}(R)$ ein Körper durch*

$$\frac{r}{s} + \frac{x}{y} := \frac{ry + sx}{sy} \quad \text{und} \quad \frac{r}{s} \cdot \frac{x}{y} := \frac{rx}{sy}.$$

Die Abbildung $i \colon R \to \mathrm{Quot}(R)$ mit $r \mapsto \frac{r}{1_R}$ ist ein injektiver Ringhomomorphismus. i heißt ***kanonische Einbettung****.*

Beweis. Die Operationen sind wohldefiniert:
Sei $\frac{r}{s} = \frac{r'}{s'}$ und $\frac{x}{y} = \frac{x'}{y'}$, d.h. $sr' = rs'$ und $yx' = xy'$. Dann gilt

$$\frac{ry + sx}{sy} = \frac{rys'y' + sxs'y'}{sys'y'} = \frac{syr'y' + sys'x'}{sys'y'} = \frac{r'y' + s'x'}{s'y'}$$

sowie

$$\frac{rx}{sy} = \frac{rxs'y'}{sys'y'} = \frac{syr'x'}{sys'y'} = \frac{r'x'}{s'y'}.$$

Die Ringaxiome sind leicht nachzurechnen. Es gilt $0_{\text{Quot}(R)} = \frac{0_R}{1_R}$, $1_{\text{Quot}(R)} = \frac{1_R}{1_R}$ und für $\frac{r}{s} \in \text{Quot}(R)$ mit $r, s \neq 0_R$ ist $-\frac{r}{s} = \frac{-r}{s}$ und $\left(\frac{r}{s}\right)^{-1} = \frac{s}{r}$. Damit wird Quot$(R)$ zum Körper. Die Abbildung i ist offensichtlich ein Ringhomomorphismus und injektiv, da $\frac{r}{1_R} = \frac{s}{1_R}$ genau dann gilt, wenn $r = s$. □

Bemerkung 5.7. Wir können R als Unterring von Quot(R) betrachten. Quot(R) ist der kleinste Körper (eindeutig bis auf Isomorphie), der R enthält.

Zurück zu Polynomen und weiter mit

Definition 5.8. Sei R ein kommutativer Ring und $f = \sum a_i x^i \in R[x]$. Der **Grad von** f ist gegeben durch $\deg(f) := \max\{i \mid a_i \neq 0_R\}$. Setze $\deg(0_{R[x]}) := -\infty$. Ist $\deg(f) = n$, so heißt a_n **Leitkoeffizient** von f. Das Polynom heißt **normiert**, falls der Leitkoeffizient 1_R ist.

Bemerkung 5.9. (i) Seien f und g Polynome in $R[x]$. Dann gilt

$$\begin{aligned}\deg(f+g) &\leq \max\{\deg(f), \deg(g)\}\\ \deg(f \cdot g) &\leq \deg(f) + \deg(g).\end{aligned}$$

Ist das Produkt der Leitkoeffizienten von f und g ungleich 0_R, so gilt $\deg(f \cdot g) = \deg(f) + \deg(g)$ - **Gradformel** genannt. Dies ist stets erfüllt, wenn R Integritätsbereich ist. Andererseits gilt zum Beispiel in $\mathbb{Z}_6[x]$:

$$\deg((\bar{2}x^7 + \bar{1}) \cdot (\bar{3}x^2)) = \deg(\bar{3}x^2) = 2 < 9 = \deg(\bar{2}x^7 + \bar{1}) + \deg(\bar{3}x^2).$$

(ii) R ist Integritätsbereich genau dann, wenn $R[x]$ Integritätsbereich (siehe Gradformel und Beispiel 5.5 (1)). In diesem Fall gilt $R[x]^\times = R^\times$.

Beweis. Sei $f \in R[x]^\times$, d.h. es existiert $g \in R[x]$ mit $f \cdot g = 1_{R[x]}$. Die Gradformel liefert $\deg(f) = \deg(g) = 0$, d.h. $f = a_0 \in R$ und $g = b_0 \in R$ mit $a_0 b_0 = 1_R$. □

Satz 5.10 (Division mit Rest in Polynomringen)**.** *Seien $f, g \in R[x]$, wobei der Leitkoeffizient b_m von g eine Einheit in R ist. Dann existieren eindeutige $q, r \in R[x]$ mit $\deg(r) < m$ und*

$$f = q \cdot g + r.$$

Beweis. **Existenz:** Induktion nach $n := \deg(f)$.
Ist $n < m$, wähle $q = 0_{R[x]}$ und $r = f$. Sei also $n \geq m$. Für $f = \sum_i a_i x^i$ setze $f_1 := f - a_n b_m^{-1} x^{n-m} g \in R[x]$. Dann ist $\deg(f_1) < \deg(f)$. Nach Induktionsvoraussetzung existieren $q_1, r_1 \in R[x]$ mit $\deg(r_1) < m$ und $f_1 = q_1 \cdot g + r_1$. Es folgt, dass

$$\begin{aligned}f = f_1 + a_n b_m^{-1} x^{n-m} g &= q_1 g + r_1 + a_n b_m^{-1} x^{n-m} g\\ &= \underbrace{(q_1 + a_n b_m^{-1} x^{n-m})}_{=:q} g + \underbrace{r_1}_{=:r}\end{aligned}$$

Eindeutigkeit: Angenommen, $f = q \cdot g + r = q'g + r'$ mit $\deg(r), \deg(r') < m$. Dann ist $(q - q')g = r' - r$. Es folgt

$$m > \deg(r' - r) = \deg((q - q') \cdot g) = \deg(q - q') + \underbrace{\deg(g)}_{=m}$$

(Gradformel). Daraus folgt $q - q' = 0_{R[x]}$ und somit $q = q'$ und somit $r = r'$. □

Wir interessieren uns allgemeiner für Ringe, die eine Division mit Rest zulassen.

Definition 5.11 (Euklidische Ringe)**.** Ein Integritätsbereich R heißt **euklidischer Ring** oder kurz **euklidisch**, wenn es eine Abbildung $\delta \colon R \setminus \{0\} \to \mathbb{N}_0$ gibt, so dass für alle $a, b \in R$ mit $b \neq 0_R$ existieren $q, r \in R$ mit $a = q \cdot b + r$ und $r = 0_R$ oder $\delta(r) < \delta(b)$. Wir nennen δ **Gradfunktion**.

Beispiel 5.12. (1) Sei K ein Körper und seien $a, b \in K$ mit $b \neq 0_K$. Dann ist

$$a = \underbrace{(ab^{-1})}_{=:q}b + \underbrace{0_K}_{=:r}.$$

Also ist K euklidisch mit beliebiger Gradfunktion

(2) $\mathbb{Z}$ mit $\delta(n) := |n|$ für $n \in \mathbb{Z} \setminus \{0\}$ ist euklidisch.

Beweis. Seien $a, b \in \mathbb{Z}$ mit $b \neq 0$. Sei $r := \min\{m \in \mathbb{N}_0 \mid m = a - nb, n \in \mathbb{Z}\}$. Wähle $q := \frac{a-r}{b} \in \mathbb{Z}$. Es folgt $a = qb + r$ mit $0 \leq r < |b|$. □

Die Eindeutigkeit von q und r bei der Division mit Rest ist weder gefordert noch ist sie hier gegeben! Zum Beispiel gilt

$$7 = 2 \cdot 3 + 1 = 3 \cdot 3 + (-2).$$

(3) Ist K ein Körper, so ist $K[x]$ euklidisch mit $\delta(f) := \deg(f)$ für $f \in K[x] \setminus \{0_{K[x]}\}$ (siehe Satz 5.10).

(4) $\mathbb{Z}[i]$ mit $\delta(a + bi) := a^2 + b^2$ für $a + bi \in \mathbb{Z}[i] \setminus \{0\}$ ist euklidisch.

Beweis. Für alle $z = x + yi \in \mathbb{C}$ existieren $a, b \in \mathbb{Z}$ mit $|x - a| \leq 1/2$ und $|y - b| \leq 1/2$. Dann gilt $|z - (a + bi)|^2 = |(x - a) + (y - b)i|^2 \leq 2 \cdot 1/4 < 1$. Insbesondere gibt es für $f, g \in \mathbb{Z}[i]$ mit $g \neq 0$ ein $q := a + bi \in \mathbb{Z}[i]$, so dass

$$\left| \frac{f}{g} - q \right|^2 < 1.$$

Setze $r := f - qg \in \mathbb{Z}[i]$. Falls $r \neq 0$, so gilt $\delta(r) = |f - qg|^2 < |g|^2 = \delta(g)$, wie gewünscht. □

Dies lässt sich veranschaulichen mit $f = 2 + i$, $g = -1 - i$. $fg^{-1} = -3/2 + 1/2i$. Wähle z.B. $q_1 = -1 + i$ und $r_1 = f - q_1 g = 2 + i - 2 = i$ oder $q_2 = -2$ und $r_2 = (2 + i) - (2 + 2i) = -i$.

Definition 5.13. Ein Integritätsbereich R heißt **Hauptidealring**, wenn jedes Ideal $I \trianglelefteq R$ ein Hauptideal ist, d.h. $I = (r)$ für ein $r \in R$.

Satz 5.14. *Jeder euklidische Ring ist Hauptidealring.*

Beweis. Sei R euklidisch mit $\{0_R\} \neq I \trianglelefteq R$. Wähle $b \in I \setminus \{0_R\}$ mit $\delta(b)$ minimal. Es gilt $(b) \subseteq I$. Sei nun $a \in I$. Dann existieren $q, r \in R$ mit $a = qb + r$ und $r = 0_R$ oder $\delta(r) < \delta(b)$. Da $r = a - qb \in I$ und $\delta(b)$ minimal, folgt $r = 0_R$. Somit ist $a = qb \in (b)$ und $(b) = I$. $\square$

Beispiel 5.15. (1) Ein Körper $K, \mathbb{Z}, K[x]$ und $\mathbb{Z}[i]$ sind Hauptidealringe nach Beispiel 5.12.

(2) $\mathbb{Z}[x]$ ist kein Hauptidealring und insbesondere nicht euklidisch.

Beweis. Betrachte $I := (2, x) \trianglelefteq \mathbb{Z}[x]$. Da $1 \notin I$, ist $I \neq \mathbb{Z}[x]$. Angenommen $I = (f)$ für ein Polynom $f \in \mathbb{Z}[x] \setminus \{0\}$. Dann existiert $g \in \mathbb{Z}[x]$ mit $f \cdot g = 2$. Mit der Gradformel folgt $\deg(f) = 0$, also $f = a_0 \in \mathbb{Z}$ mit $a_0 \mid 2$. Da $I \neq \mathbb{Z}[x]$, ist $a_0 \in \{\pm 1\}$ ausgeschlossen. Also $a_0 \in \{\pm 2\}$. Aber dann gilt $x \notin (a_0) = (f) = I$. Ein Widerspruch. $\square$

(3) $\mathbb{Z}\left[\frac{1}{2} + \frac{1}{2}\sqrt{-19}\right]$ ist nicht euklidisch, aber ein Hauptidealring,

$\mathbb{Z}\left[\frac{1}{2} + \frac{1}{2}\sqrt{-11}\right]$ hingegen ist euklidisch.

Beweisidee. Sei $w = \frac{1}{2} + \frac{1}{2}\sqrt{-19} \in \mathbb{C}$. Dann gilt $w\bar{w} = \frac{1}{4} + \frac{19}{4} = \frac{20}{4} = 5$, sowie $w + \bar{w} = 1$. Für $a, b \in \mathbb{Z}$ folgt

$$\begin{aligned}(a + bw) \cdot \overline{(a + bw)} &= (a + bw) \cdot (a + b\bar{w}) = a^2 + ab(w + \bar{w}) + b^2 w\bar{w} = a^2 + ab + 5b^2 \\ &= \frac{1}{2}(a + b)^2 + \frac{1}{2}a^2 + \frac{9}{2}b^2 \geq 0.\end{aligned}$$

Die Abbildung $N\colon \mathbb{Z}[w] \to \mathbb{N}_0$ mit $a + bw \mapsto a^2 + ab + 5b^2$ ist multiplikativ, da komplexe Konjugation multiplikativ ist.

Behauptung: $\mathbb{Z}[w]^\times = \{\pm 1\}$.

Sei $x \in \mathbb{Z}[w]^\times$ und $y \in \mathbb{Z}[w]$ mit $xy = 1$. Dann gilt

$$1 = N(1) = N(xy) = N(x)N(y).$$

Also $N(x) = 1$. Schreibe $x = a + bw$. Dann folgt

$$\frac{1}{2}(a + b)^2 + \frac{1}{2}a^2 + \frac{9}{2}b^2 = 1$$

und somit $b = 0$ und $a \in \{\pm 1\}$. Das zeigt die Behauptung.

Angenommen, $\mathbb{Z}[w]$ ist euklidisch mit Gradfunktion $\delta\colon \mathbb{Z}[w] \setminus \{0\} \to \mathbb{N}_0$ Wähle $x \in \mathbb{Z}[w] \setminus \{\pm 1, 0\}$ mit $\delta(x)$ minimal. Sei $y \in \mathbb{Z}[w]$. Dann existiert $q, r \in \mathbb{Z}[w]$ mit $y = qx + r$ und $r = 0$ oder $\delta(r) < \delta(x)$. Nach Wahl von x muss $r = 0$ oder $r \in \{\pm 1\}$. Somit gilt für den Quotientenring $\mathbb{Z}[w]/(x)$: $|\mathbb{Z}[w]/(x)| \in \{2, 3\}$. Daraus folgt

$$\mathbb{Z}[w]/(x) \cong \mathbb{Z}_2 \quad \text{oder} \quad \mathbb{Z}[w]/(x) \cong \mathbb{Z}_3$$

(Isomorphie von Ringen!). Wir führen dies zu einem Widerspruch!

Für $w = \frac{1}{2} + \frac{1}{2}\sqrt{-19}$ gilt

$$w^2 - w + 5 = \frac{1}{4} + \frac{1}{2}\sqrt{-19} - \frac{19}{4} - \frac{1}{2} - \frac{1}{2}\sqrt{-19} + 5 = 0.$$

Insbesondere gilt für $\bar{w} = w + (x) \in \mathbb{Z}[w]/(x)$ (Überstrich heißt hier Restklasse) : $\bar{w}^2 - \bar{w} + \bar{5} = \bar{0}$. Aber kein Element in $\mathbb{Z}_2$ oder $\mathbb{Z}_3$ erfüllt diese Gleichung:

<u>in $\mathbb{Z}_2$:</u> $\bar{0}^2 - \bar{0} + \bar{5} = \bar{1}$ und $\bar{1}^2 - \bar{1} + \bar{5} = \bar{1}$.

<u>in $\mathbb{Z}_3$:</u> $\bar{0}^2 - \bar{0} + \bar{5} = \bar{2}$, $\bar{1}^2 - \bar{1} + \bar{5} = \bar{2}$ und $\bar{2}^2 - \bar{2} + \bar{5} = \bar{1}$.

Ein Widerspruch. Insbesondere liefert die obige Abbildung $N\colon \mathbb{Z}[w] \to \mathbb{N}_0$ mit $a + bw \mapsto a^2 + ab + 5b^2$ keine gewünschte Gradfunktion. Mit Hilfe dieser Funktion lässt sich aber zeigen, dass $\mathbb{Z}[w]$ Hauptidealring ist. Dazu verallgemeinert man das Vorgehen aus dem Beweis vom Satz 5.14. Für $w' = \frac{1}{2} + \frac{1}{2}\sqrt{-11} \in \mathbb{C}$ liefert die Abbildung $N' : \mathbb{Z}[w'] \to \mathbb{N}_0$ mit $a + bw' \mapsto (a + bw')(a + b\bar{w}')$ aber eine Gradfunktion, die $\mathbb{Z}[w']$ zum euklidischen Ring macht. Dabei gilt

$$w' \cdot \bar{w}' = \frac{1}{4} + \frac{11}{4} = \frac{12}{4} = 3.$$

und

$$(a + bw')(a + b\bar{w}') = a^2 + ab(w' + \bar{w}') + b^2 w'\bar{w}' = a^2 + ab + 3b^2 \geq 0.$$

Nun können wir ähnlich argumentieren wie in Beispiel 5.12 (4). $\square$

6 Maximale Ideale, Primideale und faktorielle Ringe

Im Folgenden sei $R \neq \{0_R\}$ ein kommutativer Ring.

Definition 6.1. $I \trianglelefteq R$ heißt **Primideal**, wenn $I \neq R$ und für alle $a, b \in R$ mit $ab \in I$ gilt $a \in I$ oder $b \in I$.
$I \trianglelefteq R$ heißt **maximales Ideal**, wenn $I \neq R$ und für alle $J \trianglelefteq R$ mit $I \subseteq J \subseteq R$ gilt $J = I$ oder $J = R$.

Beispiel 6.2. Sei $I := n\mathbb{Z} \trianglelefteq \mathbb{Z}$ für $n \in \mathbb{N}_0$. Dann gilt

$$\begin{aligned} I \text{ Primideal} \quad &\Leftrightarrow \quad n = 0 \quad \text{oder} \quad n \text{ Primzahl} \\ I \text{ maximales Ideal} \quad &\Leftrightarrow \quad n \text{ Primzahl.} \end{aligned}$$

Allgemeiner erhalten wir

Proposition 6.3. Sei $I \trianglelefteq R$ mit $I \neq R$. Dann gilt I Primideal genau dann, wenn R/I Integritätsbereich ist. I ist maximales Ideal genau dann, wenn R/I Körper ist. Insbesondere sind maximale Ideale stets Primideale.

Beweis. Sei I ein Primideal und $a + I, b + I \in R/I$ mit $(a + I)(b + I) = 0_{R/I}$. Dann gilt $ab \in I$ und somit $a \in I$ oder $b \in I$ bzw. $a + I = 0_{R/I}$ oder $b + I = 0_{R/I}$. Also ist R/I Integritätsbereich. Ist umgekehrt R/I ein Integritätsbereich und $ab \in I$, so gilt $(a + I)(b + I) = 0_{R/I}$ und somit $a + I = 0_{R/I}$ oder $b + I = 0_{R/I}$ bzw. $a \in I$ oder $b \in I$. Also ist I Primideal.
Für den zweiten Teil nutze, dass

$$I \text{ maximales Ideal} \quad \overset{\text{Satz 4.13 (b)}}{\Leftrightarrow} \quad R/I \text{ hat nur die Ideale } \{0_{R/I}\} \text{ und } R/I \quad \overset{\text{Satz 5.2 (ii)}}{\Leftrightarrow} \quad R/I \text{ Körper.}$$

□

Satz 6.4. *R besitzt ein maximales Ideal.*

Beweis. Wir nutzen das *Lemma von Zorn*: Jede halbgeordnete Menge ($M \neq \emptyset$ mit $\leq$ reflexiv, transitiv, antisymmetrisch), in der jede Kette eine obere Schranke hat, enthält ein maximales Element.
Sei $M := \{I \trianglelefteq R \mid I \neq R\} \neq \emptyset$. M ist halbgeordnet durch Inklusion. Sei $\emptyset \neq K \subseteq M$ eine Kette in M, d.h. für alle $I_1, I_2 \in K$ gilt $I_1 \subseteq I_2$ oder $I_2 \subseteq I_1$. Die Menge K ist somit geordnet. Setze $J := \bigcup_{I \in K} I$ und zeige $J \in M$.
Seien $a_1, a_2 \in J$. Dann existieren $I_1, I_2 \in K$ mit $a_1 \in I_1$ und $a_2 \in I_2$. Sei o. B. d. A. $I_1 \subseteq I_2$. Da $I_2 \trianglelefteq R$ gilt $a_1 - a_2 \in I_2 \subseteq J$ und $ra_i \in I_2 \subseteq J$ für alle $r \in R$ und $i = 1, 2$. Also ist J ein Ideal in R. Zudem gilt, dass $J \neq R$, da sonst $1_R \in J$ und somit $1_R \in I$ für ein $I \in K$. Ein Widerspruch. Es folgt $J \in M$ und J ist obere Schranke von K. Das *Lemma von Zorn* liefert ein maximales Element $I_{\max}$ in M. $I_{\max}$ ist nach Definition ein maximales Ideal. □

Beispiel 6.5. (1) Sei K ein Körper und $a \in K$. Der Einsetzungshomomorphismus $\varphi_a \colon K[x] \to K$ mit $f \mapsto f(a)$ ist surjektiv. Nach Beispiel 5.15 (1) ist $K[x]$ Hauptidealring und es folgt

$$\operatorname{Ker}(\varphi_a) = (x - a).$$

Nach Satz Satz 4.11 (a) ist

$$K[x]\big/(x - a) \cong K.$$

Somit ist $(x-a)$ ein maximales Ideal in $K[x]$ nach Proposition 6.3. Im Allgemeinen ist aber nicht jedes maximale Ideal in $K[x]$ von dieser Form. Für $K=\mathbb{R}$ gilt nach Beispiel 4.12

$$\mathbb{R}[x] \big/ (x^2+1) \cong \mathbb{C}.$$

Somit ist (x^2+1) ein maximales Ideal in $\mathbb{R}[x]$.

(2) Primideale in einem Integritätsbereich R induzieren stets Primideale im Polynomring $R[x]$. Betrachte für $I \trianglelefteq R, I \neq R$ den Ringhomomorphismus

$$\varphi\colon R \to \left(R \big/ I\right)[x], \quad r \mapsto r+I.$$

Der Einsetzungshomomorphismus

$$\varphi_x\colon R[x] \to \left(R \big/ I\right)[x], \quad \sum a_i x^i \mapsto \sum (a_i+I)x^i$$

ist surjektiv mit $\operatorname{Ker}(\varphi_x) = \{\sum a_i x^i \mid a_i \in I\} =: I(x) \trianglelefteq R[x]$. Satz 4.11 (a) liefert $R[x]/I[x] \cong (R/I)[x]$. Nun gilt:

$$I \text{ Primideal} \overset{\text{Prop. } 6.3}{\Leftrightarrow} R \big/ I \text{ Integritätsbereich} \overset{\text{Bem. } 5.9 \text{ (ii)}}{\Leftrightarrow} R[x] \big/ I[x] \text{ Integritätsbereich}$$
$$\overset{\text{Prop. } 6.3}{\Leftrightarrow} I[x] \text{ Primideal.}$$

Im Allgemeinen ist aber nicht jedes Primideal in $R[x]$ von dieser Form. Für $R=\mathbb{Z}$ gilt $\mathbb{Z}[x]/x \cong \mathbb{Z}$. Somit ist (x) Primideal in $\mathbb{Z}[x]$ nach Proposition 6.3. Aber $(x) = \{a_1x + a_2x^2 + \cdots + a_nx^n \mid a_i \in \mathbb{Z}, n \in \mathbb{N}\}$ ist nicht von der Form $I[x]$ für $I \trianglelefteq \mathbb{Z}$. Beachte, dass

$$(x) \subsetneq (2,x) \subsetneq \mathbb{Z}[x].$$

Das Primideal (x) ist nicht maximal. Es ist enthalten im maximalen Ideal $(2,x)$ von $\mathbb{Z}[x]$ (siehe Beispiel 5.15 und Aufgabe W.10.6).

Wir wollen Primideale und maximale Ideale in Integritätsbereichen mittels ausgezeichneter Elemente besser verstehen.

Definition 6.6. Sei R Integritätsbereich und $a,b \in R$.

(a) Wir sagen a **teilt** b, wenn es ein $c \in R$ gibt mit $a \cdot c = b$. Wir schreiben $a \mid b$.

(b) Das Element a heißt **assoziiert** zu b, wenn $a \mid b$ und $b \mid a$. Wir schreiben $a \sim b$.

(c) Ein Element $p \in R \setminus \{0\}$ heißt **prim** oder **Primelement**, wenn $p \notin R^\times$ und $p \mid ab$ nur dann, wenn $p \mid a$ oder $p \mid b$.

(d) Ein Element $u \in R \setminus \{0\}$ heißt **unzerlegbar** oder **irreduzibel**, wenn $u \notin R^\times$ und $u = ab$ nur dann, wenn $a \in R^\times$ oder $b \in R^\times$.

Bemerkung 6.7. (i) Es gilt

$$\begin{array}{ccccc} a \mid b & \Leftrightarrow & b \in (a) & \Leftrightarrow & (b) \subseteq (a) \\ a \sim b & \Leftrightarrow & (a) = (b) & \Leftrightarrow & \exists c \in R^\times : u = cb \end{array}.$$

Vergleiche Aufgabe M.8.5. Assoziiertheit ist eine Äquivalenzrelation.

(ii) Primelemente sind stets unzerlegbar.

Beweis. Sei $p \in R$ prim mit $p = ab$ für $a, b \in R$. Folglich gilt $p \mid a$ oder $p \mid b$. O. B. d. A. gelte $p \mid a$, d. h. es existiert $c \in R$, so dass $pc = a$. Also ist $p = ab = pcb$. Da R Integritätsbereich folgt $cb = 1_R$ und $b \in R^\times$. Somit ist p unzerlegbar. $\square$

Die Umkehrung gilt im Allgemeinen nicht (siehe Beispiel 6.8 (2)).

Beispiel 6.8. (1) In $\mathbb{Z}$ sind n und $-n$ assoziiert für $n \in \mathbb{Z} \setminus \{0\}$. Die Primelemente sind genau die unzerlegbaren Elemente und gegeben durch

$$\{\pm p \mid p \text{ Primzahlen}\}.$$

(2) $2 \in \mathbb{Z}[\sqrt{-5}]$ ist unzerlegbar, aber nicht prim.

Beweis. Betrachte $N\colon \mathbb{Z}[\sqrt{-5}] \to \mathbb{N}_0$ mit $a + b\sqrt{-5} \mapsto a^2 + 5b^2$. Wie in Beispiel 5.15 (3), folgt

$$\mathbb{Z}[\sqrt{-5}]^\times = \{x \in \mathbb{Z}[\sqrt{-5}] \mid N(x) = 1\} = \{\pm 1\} \not\ni 2.$$

Schreibe $2 = xy$ mit $x, y \in \mathbb{Z}[\sqrt{-5}]$. Dann gilt $4 = N(2) = N(xy) = N(x)N(y)$. Da es kein $a, b \in \mathbb{Z}$ mit $N(a + b\sqrt{-5}) = a^2 + 5b^2 = 2$, folgt $N(x) = 1$ oder $N(y) = 1$, d. h. 2 ist unzerlegbar. Aber $2 \mid (1 + \sqrt{-5})(1 - \sqrt{-5}) = 6 = 2 \cdot 3$ und $2 \mid x$ mit $x \in \mathbb{Z}[\sqrt{-5}]$ bedeutet, dass $y \in \mathbb{Z}[\sqrt{-5}]$ existiert mit $2y = x$ und somit $N(x) = N(2y) = N(2)N(y) = 4 \cdot N(y)$, also insbesondere $4 \mid N(x)$. Da $N(1 \pm \sqrt{-5}) = 6$, teilt 2 weder $1 + \sqrt{-5}$ noch $1 - \sqrt{-5}$ und ist daher nicht prim. $\square$

Proposition 6.9. (a) Sei R ein Integritätsbereich und $p \in R \setminus \{0_R\}$. Dann gilt

$$(p) \trianglelefteq R \text{ Primideal} \Leftrightarrow p \text{ prim}$$
$$(p) \trianglelefteq R \text{ maximal} \Leftrightarrow p \text{ unzerlegbar}$$

(b) Sei R ein Hauptidealring und $u \in R$ unzerlegbar. Dann ist $(u) \trianglelefteq R$ maximal. Insbesondere sind die unzerlegbaren Elemente in R genau die Primelemente und ein Ideal $\{0_R\} \neq I \trianglelefteq R$ ist maximal genau dann, wenn I ein Primideal ist.

Beweis. (a)

$$(p) \trianglelefteq R \text{ Primideal} \overset{\text{Def.}}{\Leftrightarrow} (p) \neq R, \forall a, b \in R : ab \in (p) \Rightarrow a \in (p) \vee b \in (p)$$
$$\overset{\text{Bem. 6.7 (1)}}{\Leftrightarrow} p \notin R^\times \wedge \forall a, b \in R : p \mid ab \Rightarrow p \mid a \vee p \mid b \overset{\text{Def.}}{\Leftrightarrow} p \text{ prim}.$$

Sei nun $(p) \trianglelefteq R$ maximal. Nach Proposition 6.3 ist $(p) \trianglelefteq R$ Primideal und somit p prim. Aber dann ist p unzerlegbar nach Bemerkung 6.7 (2).

(b) Sei R ein Hauptidealring und $u \in R$ unzerlegbar. Sei weiter $I \trianglelefteq R$ mit $(u) \subseteq I \subsetneq R$. Schreibe $I = (a)$ mit $a \notin R^\times$. Da $(u) \subseteq (a)$, folgt $a \mid u$, d.h. es existiert $b \in R$ mit $ab = u$. Da u unzerlegbar ist und $a \notin R^\times$, gilt $b \in R^\times$, d. h. $u \sim a$ bzw. $(u) = (a)$. Also ist $(u) \trianglelefteq R$ maximal.

Insbesondere ist (u) ein Primideal und u somit prim, d. h. die unzerlegbar Elemente in R stimmen mit den Primelementen überein.

$\square$

Beispiel 6.10. (1) Nach dem Fundamentalsatz der Algebra sind die unzerlegbaren Elemente in $\mathbb{C}[x]$ Polynome der Form $wx + z$ mit $w, z \in \mathbb{C}$ und $w \neq 0$. Da $\mathbb{C}[x]$ Hauptidealring ist, sind die maximalen Ideale in $\mathbb{C}[x]$ nach Proposition 6.9 genau die Ideale der Form $(x - z)$ mit $z \in \mathbb{C}$ (siehe auch Beispiel 6.5 (1)). $\{0\}$ ist das einzige Primideal in $\mathbb{C}[x]$, das nicht maximal ist.

(2) Unzerlegbare Elemente in $\mathbb{R}[x]$ sind genau

- lineare Polynome,
- quadratische Polynome ohne reelle Nullstellen.

Nutze dazu, dass ein Polynom $f \in \mathbb{R}[x]$ mit Nullstelle $w \in \mathbb{C} \setminus \mathbb{R}$ auch $\bar{w} \in \mathbb{C} \setminus \mathbb{R}$ als Nullstelle hat. Da $(x - w)(x - \bar{w}) \in \mathbb{R}[x]$, haben wir ein Polynom vo, Grad 2 in $\mathbb{R}[x]$ gefunden, das f teilt. Da auch $\mathbb{R}[x]$ Hauptidealring ist, sind die maximalen Ideale in $\mathbb{R}[x]$ wiederum nach Proposition 6.9 genau die Ideale der Form $(x - z)$ mit $z \in \mathbb{R}$ und $(x^2 + ax + b)$ mit $a, b \in \mathbb{R}$ und $a^2 - 4b < 0$. Diese entsprechen bijektiv den Elementen der abgeschlossenen oberen komplexen Halbebene.

(3) Unzerlegbare Elemente in allgemeinen Polynomringen sind gewöhnlich schwieriger zu klassifizieren (dazu später mehr). Zum Beispiel gibt es in $\mathbb{Z}[x]$ für jedes $n \in \mathbb{N}_0$ ein unzerlegbares Polynom vom Grad n. Für $n \neq 0$ gibt es auch in $\mathbb{Z}_p[x]$ mit p Primzahl stets ein unzerlegbares Polynom vom Grad n.

> Wir wollen verstehen, in welchen Integritätsbereichen sich nicht-invertierbare Elemente ungleich Null, auf eindeutige Weise, als endliche Produkte unzerlegbarer Elemente schreiben lassen.

Definition 6.11. Ein Integritätsbereich R heißt **faktoriell**, wenn gilt

- Jedes Element in $R \setminus (R^\times \cup \{0_R\})$ ist endliches Produkt unzerlegbarer Elemente.
- Ist $p_1 \cdot \ldots \cdot p_m = q_1 \cdot \ldots \cdot q_n$ mit p_i, q_j unzerlegbar, dann folgt $m = n$ und nach Umsortierung $p_i \sim q_i$ für $1 \leq i \leq m$.

Beispiel 6.12. $\mathbb{Z}$ ist faktoriell. Bis auf Vorzeichen und Reihenfolge existiert für jedes $n \in \mathbb{Z} \setminus \{0, \pm 1\}$ eine eindeutige Zerlegung in Primelemente bzw. unzerlegbare Elemente. Die Existenz einer solchen Zerlegung lässt sich wie folgt begründen:
Entweder ist $n > 1$ unzerlegbar oder $n = ab$ mit $1 < a, b < n$. Induktiv existieren gewünschte Zerlegungen für a und b und somit auch für n.
Wir nutzen, dass $(\mathbb{Z}, \leq)$ eine geordnete Menge ist. Im Allgemeinen existiert in Ringen keine solche Ordnungsrelation und wir müssen anders argumentieren.

Satz 6.13. *Jeder Hauptidealring R ist faktoriell.*

Beweis. 1. Hauptidealringe sind **noethersch**, d.h. für jede aufsteigende Kette von Idealen $I_1 \subseteq I_2 \subseteq I_2 \subseteq \ldots$ in R existiert ein $n \in \mathbb{N}$ mit $I_n = I_{n+1} = \ldots$. Setze dazu $I := \bigcup_{t \in \mathbb{N}} I_t \trianglelefteq R$ (siehe Beweis von Satz 6.4). Dann existiert $r \in R$ mit $I = (r)$ und somit ein $n \in \mathbb{N}$ mit $r \in I_n$. Es folgt $I_n = I_{n+1} = \ldots$, wie gewünscht.

Nun sei $a \in R \setminus (R^\times \cup \{0_R\})$. Ist a zerlegbar, so existieren $a_1, b_1 \in R \setminus (R^\times \cup \{0_R\})$ mit $a = a_1 b_1$. Dann gilt $a_1 \mid a$ und $a_1 \not\sim a$, d. h. $(a) \subsetneq (a_1)$. Ist auch a_1 zerlegbar, so existieren $a_2, b_2 \in R \setminus (R^\times \cup \{0_R\})$ mit $a_1 = a_2 b_2$. Wir erhalten $(a) \subsetneq (a_1) \subsetneq (a_2)$ und nach wiederholter Anwendung

$$(a) \subsetneq (a_1) \subsetneq (a_2) \subsetneq (a_3) \subsetneq \dots .$$

Da diese Kette stationär werden muss, finde wir $q_1 \in R$ unzerlegbar mit $a = q_1 a'$. Wiederholen wir diesen Prozess für a', finden wir $q_2 \in R$ unzerlegbar mit $a = q_1 q_2 a''$ usw. Da auch die Kette von Idealen

$$(a) \subsetneq (a') \subsetneq (a'') \subsetneq \dots$$

stationär werden muss, ist $a = q_1 \cdot \dots \cdot q_n$ endliches Produkt unzerlegbarer Elemente.

2. In Hauptidealringen sind die unzerlegbaren Elemente genau die Primelemente (siehe Proposition 6.9 (b)).

   Sei nun $a = p_1 \cdot \dots \cdot p_m = q_1 \cdot \dots \cdot q_n$ mit p_i, q_j unzerlegbar. Da $p_1 \mid q_1 \cdot \dots \cdot q_n$ und p_1 prim, existiert $j \in \{1, \dots, n\}$ mit $p_1 \mid q_j$. Sei o. B. d. A. $j = 1$. Also existiert $c \in R$ mit $p_1 c = q_1$. Da q_1 unzerlegbar ist folgt, $c \in R^\times$ und $p_1 \sim q_1$. Kürzen liefert

$$p_2 \cdot \dots \cdot p_m = q_2' \cdot q_3 \cdot \dots \cdot q_n$$

   mit $q_2' \sim q_2$. Induktiv folgt $m = n$ und nach Umsortierung $p_i \sim q_i$ für $1 \leq i \leq m$.

$\square$

Bemerkung 6.14. Sei R ein faktorieller Ring und $p \in R$. Dann gilt

$$p \text{ prim} \quad \Leftrightarrow \quad p \text{ unzerlegbar.}$$

Beweis. „$\Leftarrow$“: Seien $a, b \in R$ mit $p \mid ab$, d. h. es existiert $c \in R$ mit $pc = ab$. Betrachte Zerlegungen von a, b, c in unzerlegbare Elemente. Da R faktoriell und p unzerlegbar ist, muss p bis auf Assoziiertheit in der Zerlegung von ab vorkommen und somit in der von a oder von b. Also $p \mid a$ oder $p \mid b$. $\square$

Definition 6.15. Sei R ein Integritätsbereich und $a, b \in R$.

(a) $d \in R$ heißt **größter gemeinsamer Teiler** von a und b, wenn $d \mid a \wedge d \mid b$ sowie für alle $e \in R$ gilt $e \mid a \wedge e \mid b$ nur dann, wenn $e \mid d$.

(b) $m \in R$ heißt **kleinstes gemeinsames Vielfaches** von a und b, wenn $a \mid m \wedge b \mid m$ sowie für alle $n \in R$ gilt $a \mid n \wedge b \mid n$ nur dann, wenn $m \mid n$.

Bemerkung 6.16. (i) Existieren ggT und kgV, so sind sie nur eindeutig bis auf Multiplikation mit einer Einheit.

(ii) In einem faktoriellen Ring existieren stets ggT und kgV.

Sei P_R ein Repräsentantensystem der Klassen assoziierter Primelemente und seien $a, b \in R \setminus \{0_R\}$ mit $a = \Sigma_a p_1^{a_1} \cdots p_n^{a_n}$ und $b = \Sigma_b p_1^{b_1} \cdots p_n^{b_n}$ für $a_i, b_i \in \mathbb{N}_0, \Sigma_a, \Sigma_b \in R^\times, p_i \in P_R$ mit $p_i \not\sim p_j$ für $i \neq j$. Dann ist $\prod_i p_i^{\min(a_i, b_i)}$ ein ggT und $\prod_i p_i^{\max(a_i, b_i)}$ ein kgV der Elemente a und b.

(iii) In einem euklidischen Ring lässt sich ein ggT mit Hilfe des euklidischen Algorithmus bestimmen, also durch wiederholte Division mit Rest (vgl. Beispiel 4.17 und Aufgabe V.8.1, M.11.5, M.11.6).

Beispiel 6.17. In $\mathbb{Z}[\sqrt{-5}]$ existiert kein ggT von $x = 6$ und $y = 2 + 2\sqrt{-5}$.

Beweis. Angenommen, d sei ein solcher ggT. Sei $N\colon \mathbb{Z}[\sqrt{-5}] \to \mathbb{N}_0$ mit $a + b\sqrt{-5} \mapsto a^2 + 5b^2$ wie in Beispiel 6.8 (2). Dann gilt $N(d) \mid N(x) = 36$ und $N(d) \mid N(y) = 24$.
Da 2 sowohl x als auch y teilt, folgt $2 \mid d$ und somit $4 = N(2) \mid N(d)$. Ebenso teilt $1 + \sqrt{-5}$ sowohl x als auch y, so dass $6 = N(1 + \sqrt{-5}) \mid N(d)$. Es folgt $N(d) = 12$. Aber es existieren keine $a, b \in \mathbb{Z}$ mit $N(a + b\sqrt{-5}) = 12$. Ein Widerspruch. □

Wir zeigen nun, dass für R faktoriell auch $R[x]$ ein faktorieller Ring ist!

Definition 6.18. Sei R ein faktorieller Ring und $f = \sum_{i=0}^{n} a_i x^i \in R[x]$. Die Menge aller ggT von $a_0, a_1, \ldots, a_n$ heißt **Inhalt** von f. Wir schreiben $\mathrm{cont}_R(f)$. Wir nennen f **primitiv**, wenn $\mathrm{cont}_R(f) = R^\times$.

Beispiel 6.19. (1) Ist K ein Körper, so ist jedes Polynom $f \in K[x] \setminus \{0_{K[x]}\}$ primitiv.

(2) $f = 2x + 2$ ist nicht primitiv in $\mathbb{Z}[x]$, jedoch in $\mathbb{Q}[x]$. Es gilt $\mathrm{cont}_{\mathbb{Z}}(f) = \{\pm 2\}$ und $\frac{1}{2}f = x + 1$ ist primitiv in $\mathbb{Z}[x]$.

Lemma 6.20. *Sei R ein faktorieller Ring mit Quotientenkörper $\mathrm{Quot}(R)$*

(a) Ist $f \in R[x] \setminus \{0_{R[x]}\}$ und $d \in \mathrm{cont}_R(f)$, so ist $\frac{1}{d}f \in R[x]$ primitiv.

(b) Ist $f \in R[x]$ primitiv und $c \in \mathrm{Quot}(R)$ mit $cf \in R[x]$, so ist $c \in R$.

(c) Ist $f \in \mathrm{Quot}(R)[x] \setminus \{0_{R[x]}\}$, so gibt es $c \in \mathrm{Quot}(R) \setminus \{0_R\}$ und $g \in R[x]$ primitiv mit $f = cg$.

Beweis. (a) Folgt aus der Definition vom ggT.

(b) Schreibe $f = \sum_{i=0}^{n} a_i x^i$ und $c = \frac{a}{b}$ für $a, b \in R$ teilerfremd und $b \neq 0_R$. Da $cf \in R[x]$, gilt $\frac{aa_i}{b} \in R$ für $i = 0, \ldots, n$. Somit ist jeder Primteiler $p \in R$ von b auch Primteiler von a_i für $i = 0, \ldots, n$. Da f primitiv ist, existiert kein solcher gemeinsamer Primteiler, d. h. $b \in R^\times$ bzw. $c = \frac{a}{b} \in R$.

(c) Schreibe $f = \sum_{i=0}^{n} \frac{a_i}{b_i} x^i$ mit $a_i \in R, b_i \in R \setminus \{0_R\}$. Dann ist $f' := (b_0 \cdots b_n) \cdot f \in R[x] \setminus \{0_{R[x]}\}$ und für $d \in \mathrm{cont}_R(f')$ gilt nach **(a)**, dass $g := \frac{1}{d} \cdot f' \in R[x]$ primitiv. Insbesondere folgt für $c := \frac{d}{b_0 \cdots b_n} \in \mathrm{Quot}(R) \setminus \{0_R\}$, dass $c \cdot g = f$.

□

Beispiel 6.21. Für $f = x^2 + 3x + \frac{1}{5} \in \mathbb{Q}[x]$ ist $f = c \cdot g$ mit $g = 5x^2 + 15x + 1$ in $\mathbb{Z}[x]$ primitiv und $c = \frac{1}{5} \in \mathbb{Q}$.

Bemerkung 6.22. Sei R Integritätsbereich und $p \in R$ prim. Dann ist p auch prim im Polynomring $R[x]$.

Beweis. Betrachte dazu das Primideal $I = (p) \trianglelefteq R$. Nach Beispiel 6.5 (2) induziert I das Primideal $I(x) := \{\sum_i a_i x^i \mid a_i \in I\} \trianglelefteq R[x]$. Aber es gilt $I(x) = (p)$ in $R[x]$. Somit ist p Primelement in $R[x]$ nach Proposition 6.9. □

Theorem 6.23 (Lemma von Gauß)**.** *Sei R ein faktorieller Ring mit Quotientenkörper $\mathrm{Quot}(R)$.*

(a) Sind $f, g \in R[x]$ primitiv, so ist auch $f \cdot g$ primitiv.

(b) Ist $f \in R[x]$ primitiv und prim in $\mathrm{Quot}(R)[x]$, so ist f prim in $R[x]$.

(c) $R[x]$ ist faktorieller Ring.

Beweis. (a) Angenommen, $f \cdot g$ ist nicht primitiv. Dann existiert ein $p \in R$ mit

$$p \mid f \cdot g \quad \text{in } R[x].$$

Nach Bemerkung 6.22 ist p prim in $R[x]$, d. h. $p \mid f$ oder $p \mid g$. Aber dann teilt p alle Koeffizienten des entsprechenden Polynoms. Dies widerspricht der Annahme, dass f, g primitiv.

(b) Nach Voraussetzung ist $f \neq 0_{R[x]}$ und $f \notin R[x]^\times$. Seien $g, h \in R[x]$ mit $f \mid gh$ in $R[x]$. Da f prim in $\mathrm{Quot}(R)[x]$ ist, teilt f entweder g oder h in $\mathrm{Quot}(R)[x]$. Gelte o. B. d. A. $f \mid g$ in $\mathrm{Quot}(R)[x]$ und $g \neq 0_{R[x]}$, d. h.

$$\exists k \in \mathrm{Quot}(R)[x] \setminus \{0_{R[x]}\} \text{ mit } f \cdot k = g.$$

<ins>Genügt zu zeigen:</ins> $k \in R[x]$.

Nutze Lemma 6.20 **(c)** und schreibe $k = c \cdot q$ mit $c \in \mathrm{Quot}(R) \setminus \{0_R\}$ und $q \in R[x]$ primitiv. Es folgt $g = f \cdot k = c \cdot (f \cdot q)$, wobei $f \cdot q$ nach Teil **(a)** primitiv ist. Mit Lemma 6.20 **(b)** folgt $c \in R$ und somit $k = c \cdot q \in R[x]$.

(c) $R[x]$ ist Integritätsbereich und es gilt $R[x]$ ist faktoriell genau dann, wenn jedes Element in $R[x] \setminus (R^\times \cup \{0_R\})$ endliches Produkt von Primelementen ist.

„$\Rightarrow$“: Folgt mit Bemerkung 6.14.

„$\Leftarrow$“: Primelemente sind unzerlegbar. Die Eindeutigkeit der Zerlegung folgt wie im Beweis von Satz 6.13.

Sei also $f \in R[x] \setminus (R^\times \cup \{0_R\})$. Ist $\deg(f) = 0$, d.h. $f \in R$, so existiert eine endliche Zerlegung in Primelemente von R. Nach Bemerkung 6.22 ist dies auch eine Zerlegung in Primelemente von $R[x]$. Sei also $\deg(f) \geq 1$ und f somit keine Einheit in $\mathrm{Quot}(R)[x]$. Nach Satz 6.13 ist $\mathrm{Quot}(R)[x]$ faktoriell, d. h. es existieren $q_1, \ldots, q_n \in \mathrm{Quot}(R)[x]$ prim mit $f = q_1 \cdots q_n$. Nutze Lemma 6.20 **(c)** und schreibe $q_i = c_i p_i$ mit $c_i \in \mathrm{Quot}(R) \setminus \{0_R\}$ und $p_i \in R[x]$ primitiv. Da $q_i \sim p_i$ in $\mathrm{Quot}(R)[x]$, ist auch p_i prim in $\mathrm{Quot}(R)[x]$. Nach Teil **(b)** ist p_i dann auch prim in $R[x]$.

Nach Teil **(a)** ist zudem $p := p_1 \cdots p_n \in R[x]$ primitiv, so dass

$$f = (c_1 \cdots c_n) \cdot p \in R[x]$$

mit Lemma 6.20 **(b)** impliziert, dass $c := c_1 \cdots c_n \in R$. Ist $c \in R^\times$, so liefert $f = c \cdot p_1 \cdots p_n$ eine gewünschte Zerlegung. Andernfalls schreibe $c = a_1 \cdots a_m$ mit $a_j \in R$ prim. Da die a_j auch prim in $R[x]$ sind, ist $f = a_1 \cdots a_m \cdot p_1 \cdots p_n$ eine gewünschte Zerlegung von f in Primelemente von $R[x]$.

□

Hierarchie kommutativer Ringe.

> Wir wollen noch Kriterien kennenlernen, um zu entscheiden, ob ein gegebenes Polynom (z. B. in $\mathbb{Z}[x]$ oder $\mathbb{Q}[x]$) unzerlegbar ist.

Satz 6.24 (Eisenstein-Kriterium)**.** *Sei R ein faktorieller Ring und $f := \sum_{i=0}^{n} a_i x^i \in R[x] \setminus R^\times$ primitiv. Gibt es ein Primelement $p \in R$, so dass $p \mid a_0, \ldots, a_{n-1}$ und $p^2 \nmid a_0$, so ist f unzerlegbar in $R[x]$.*

Beweis. Sei $f = g \cdot h$ für $g, h \in R[x]$. Schreibe $g = \sum_{i=0}^{k} b_i x^i$ mit $\deg(g) = k$ und $h = \sum_{j=0}^{\ell} c_j x^j$ mit $\deg(h) = \ell$.
Ist $k = 0$, so ist $g \in R$ Teiler aller Koeffizienten von f, d. h. $g \in R^\times$, da f primitiv. Analog ist $h \in R^\times$ für $\ell = 0$.
Angenommen $0 < k, \ell < n$. Für $s = 0, \dots, n$ erhalten wir

$$a_s = \sum_{i+j=s} b_i c_j. \tag{1}$$

Sei $p \in R$ Primelement wie in der Voraussetzung gefordert. Da $p \mid a_0 = b_0 c_0$. Gelte o. B. d. A. $p \mid b_0$. Da $p^2 \nmid a_0$, gilt dann $p \nmid c_0$. Wir zeigen nun per Induktion, dass

$$p \mid b_i \quad \text{für alle } i \in \{0, \dots, k\}.$$

Die Aussage gelte für alle Indizes von 0 bis $i - 1$. Mit (1) erhalten wir

$$b_i c_0 = a_i - b_{i-1} c_1 - b_{i-2} c_2 - \cdots - b_0 c_i.$$

Nach Induktionsvoraussetzung und da $p \mid a_i$ für $i \le k < n$, folgt $p \mid b_i c_0$. Aber $p \nmid c_0$ und somit $p \mid b_i$, d. h. p teilt jeden Koeffizienten von g. Insbesondere bedeutet dies $p \mid b_k c_\ell = a_n$, was im Widerspruch zur Annahme steht, dass f primitiv ist. □

Beispiel 6.25. Sei $f = x^5 - 4x + 2$ in $\mathbb{Z}[x]$. Das Polynom f ist primitiv und die Primzahl $p = 2$ teilt alle Koeffizienten bis auf den Leitkoeffizienten und den konstanten Teil von f nur einfach. Nach Satz 6.24 ist f unzerlegbar in $\mathbb{Z}[x]$.

Das Eisenstein-Kriterium lässt sich jedoch nicht unmittelbar nutzen, um Unzerlegbarkeit in $K[x]$ für einen Körper K zu untersuchen. Wir können uns aber wie folgt behelfen:

Satz 6.26. *Sei R ein faktorieller Ring mit Quotientenkörper $\mathrm{Quot}(R)$. Dann ist $f \in R[x] \setminus R$ unzerlegbar in $R[x]$ genau dann, wenn f primitiv in $R[x]$ ist und unzerlegbar in $\mathrm{Quot}(R)[x]$.*

Beweis. Nach Theorem 6.23 **(c)** ist $R[x]$ faktoriell und somit gilt „prim=unzerlegbar“ in $R, R[x]$ und $\mathrm{Quot}(R)[x]$. Die Implikation „$\Leftarrow$“ ist dann genau Theorem 6.23 **(c)**.
„$\Rightarrow$“: Sei $f \in R[x] \setminus R$ unzerlegbar in $R[x]$. Nach Voraussetzung ist f primitiv in $R[x]$ und keine Einheit in $\mathrm{Quot}(R)[x]$. Sei nun $f = gh$ mit $g, h \in \mathrm{Quot}(R)[x] \setminus \{0_{R[x]}\}$ und schreibe mit Lemma 6.20 **(c)**

$$g = c \cdot p$$
$$h = d \cdot q$$

für $c, d \in \mathrm{Quot}(R) \setminus \{0_R\}$ und $p, q \in R[x]$ primitiv. Es folgt $f = (c \cdot d) \cdot p \cdot q \in R[x]$. $p \cdot q$ ist primitiv nach Theorem 6.23 **(a)** und somit $c \cdot d \in R$ nach Lemma 6.20 **(b)**. Da f unzerlegbar in $R[x]$ ist, müssen zwei der Faktoren cd, p, q Einheiten in $R[x]$ sein, d. h. in $R^\times$ liegen. Dann ist aber $g = c \cdot p$ oder $h = d \cdot q$ eine Einheit in $\mathrm{Quot}(R)[x]$, wie gewünscht. □

Somit sind nicht-konstante unzerlegbare Polynome in $\mathbb{Z}[x]$, wie $f = x^5 - 4x + 2$ aus Beispiel 6.25, auch unzerlegbar in $\mathbb{Q}[x]$.
Unzerlegbarkeit in $\mathbb{Z}[x]$ lässt sich auch modulo einer Primzahl p untersuchen.

Satz 6.27. *Sei R ein faktorieller Ring, $p \in R$ prim und $f = \sum_{i=0}^n a_i x^i \in R[x]$ primitiv mit $p \nmid a_n$. Ist das Bild von f unter*

$$\begin{aligned} \phi_p \colon R[x] &\to {}^{R}\!\big/_{(p)}[x], \\ \sum_i a_i x^i &\mapsto \sum_i (a_i + (p)) x^i \end{aligned}$$

unzerlegbar in $(R/(p))[x]$, so ist f unzerlegbar in $R[x]$.

Beweis. ϕ_p ist ein surjektiver Ringhomomorphismus nach Beispiel 6.5 **(2)** und bildet daher Einheiten auf Einheiten ab. Nach Voraussetzung ist $f \neq 0_{R[x]}$ und keine Einheit in $R[x]$.
Sei $f = gh$ mit $g, h \in R[x]$. Da $p \nmid a_n$, teilt p auch nicht die Leitkoeffizienten von g und h, d. h.

$$\deg(f) = \deg(\phi_p(f)), \quad \deg(g) = \deg(\phi_p(g)), \quad \deg(h) = \deg(\phi_p(h)).$$

Betrachte $\phi_p(f) = \phi_p(g)\phi_p(h)$ in $R/(p)[x]$. Da $\phi_p(f)$ unzerlegbar und sei o. B. d. A. $\phi_p(g)$ eine Einheit in $R/(p)[x]$. Da $R/(p)$ Integritätsbereich ist, folgt $\phi_p(g) \in (R/(p))^\times$ und somit

$$\deg(g) = \deg(\phi_p(g)) = 0.$$

Also ist $g \in R$ Teiler aller Koeffizienten von f. Mit f primitiv in $R[x]$ erhalten wir $g \in R^\times = R[x]^\times$, wie gewünscht. □

Beispiel 6.28. Das primitive Polynom $f = x^4 + x^3 + x^2 + x + 1$ ist unzerlegbar in $\mathbb{Z}[x]$ und somit nach Satz 6.26 auch in $\mathbb{Q}[x]$ (vgl. Aufgabe M.12.1 (b)). Nach Satz 6.27 genügt es zu zeigen, dass $\bar{f} = x^4 + x^3 + x^2 + \bar{1}$ unzerlegbar in $\mathbb{Z}_2$ ist. Wäre $\bar{f}$ zerlegbar, müsste es einen unzerlegbaren Faktor vom Grad 1 oder 2 haben und somit geteilt werden von $x, x + \bar{1}$ oder $x^2 + x + \bar{1}$. Dies lässt sich mittels Polynomdivision jedoch einfach ausschließen.

7 Körpererweiterung

Ein Körper ist ein kommutativer von Null verschiedener Ring, in dem jedes Element ungleich Null eine Einheit ist. Wir kennen bereits $\mathbb{Q}, \mathbb{R}, \mathbb{C}, \mathbb{Z}_p$ für p Primzahl sowie den Quotientenkörper $\mathrm{Quot}(R)$ und den Quotientenring R/I für einen Integritätsbereich R und $I \trianglelefteq R$ maximal (siehe Proposition 6.3).
Ringhomomorphismen zwischen Körpern heißen auch **Körperhomomorphismen**. Bijektive Körperhomomorphismen heißen **Körperisomorphismen**.
Da Körper nur triviale Ideale besitzen, sind Körperhomomorphismus stets injektiv.

Definition 7.1. Seien K und L Körper.

(a) Ist $K \leq L$ ein Unterring, so heißt K **Teilkörper** von L und L **Erweiterungskörper** von K. Wir sprechen von der **Körpererweiterung** $K \leq L$ und schreiben L/K.

(b) Ist L/K eine Körpererweiterung, so ist L ein K-Vektorraum und $[L : K] := \dim_K(L) \in \mathbb{N} \cup \{\infty\}$ heißt **Grad der Körpererweiterung** (vgl. Aufgabe M.13.1). Die Körpererweiterung L/K heißt **endlich**, wenn $[L : K] < \infty$.

Beispiel 7.2. Es gilt $[\mathbb{C} : \mathbb{R}] = 2$, da C als $\mathbb{R}$-Vektorraum die Basis $\{1, i\}$ hat. Es ist $[\mathbb{R} : \mathbb{Q}] = \infty$. Im Allgemeinen gilt $[L : K] = 1$ nur dann, wenn $L = K$.

Definition 7.3. Sei K ein Körper.

(a) Dann heißt der Schnitt
$$\Pi(K) := \bigcap_{K' \leq K} K'$$
aller Teilkörper der **Primkörper** von K.

(b) Die **Charakteristik** von K ist definiert als
$$\mathrm{char}(K) := \begin{cases} 0 & \forall n \in \mathbb{N} : n \cdot 1_K := 1_K + \cdots + 1_K \neq 0_K, \\ \min\{n \in \mathbb{N} \mid n \cdot 1_K = 0_K\} & \text{sonst.} \end{cases}$$

Bemerkung 7.4. (i) $\Pi(K)$ ist nach Konstruktion der kleinste Teilkörper von K.

(ii) Betrachte den Ringhomomorphismus $\varphi_K \colon \mathbb{Z} \to K$ mit
$$n \mapsto \begin{cases} n \cdot 1_K & n \geq 1, \\ 0_K & n = 0, \\ -n \cdot (-1_K) & n \leq -1. \end{cases} .$$
Dann gilt $\mathrm{Ker}(\varphi_K) = \mathrm{char}(K) \cdot \mathbb{Z} \leq \mathbb{Z}$ (vgl. Aufgabe S.7.2).

Satz 7.5. *Sei K ein Körper. Ist $\mathrm{char}(K) \neq 0$, so gilt $\mathrm{char}(K) = p$ für eine Primzahl p und $\Pi(K) \cong \mathbb{Z}_p$. Ist $\mathrm{char}(K) = 0$, so gilt $\Pi(K) \cong \mathbb{Q}$.*

Beweis. Nutze Bemerkung 7.4 (ii). Ist $\mathrm{char}(K) = n > 1$, so gilt $\mathrm{Ker}(\varphi_K) = n\mathbb{Z} \trianglelefteq \mathbb{Z}$. Der Homomorphiesatz liefert
$$\mathbb{Z}_n = \mathbb{Z}/n\mathbb{Z} = \mathbb{Z}/\mathrm{Ker}(\varphi_K) \cong \mathrm{Im}(\varphi_K) \leq K.$$

Da K Körper ist, ist $\mathbb{Z}_n$ nullteilerfrei und $n = p$ somit Primzahl. Insbesondere ist $\mathbb{Z}_p \cong \operatorname{Im}(\varphi_K)$ ein Körper mit $\Pi(K) \subseteq \operatorname{Im}(\varphi_K)$. Da zudem $1_K \in \Pi(K)$ und $\Pi(K)$ abgeschlossen unter Addition ist, folgt $\Pi(K) = \operatorname{Im}(\varphi_K) \cong \mathbb{Z}_p$, wie gewünscht.
Sei nun $\operatorname{char}(K) = 0$ und $\varphi_K \colon \mathbb{Z} \to K$ somit injektiv. Nach Aufgabe M.9.1 gilt mit $\psi_K\left(\frac{a}{b}\right) = \varphi_K(a) \cdot \varphi_K(b)^{-1}$. Da $\mathbb{Q}$ Körper ist, folgt ψ_K injektiv und $\mathbb{Q} \cong \operatorname{Im}(\psi_K) \leq K$. Somit ist $\Pi(K) \subseteq \operatorname{Im}(\psi_K)$. Da $\mathbb{Q}$ (wie zuvor auch $\mathbb{Z}_p$) keinen echten Teilkörper hat, gilt $\Pi(K) = \operatorname{Im}(\psi_K) \cong \mathbb{Q}$. $\square$

Beispiel 7.6. (1) $\mathbb{Q}, \mathbb{R}, \mathbb{C}$ haben Charakteristik 0 und den Primkörper $\mathbb{Q}$. $\mathbb{Z}_p$ mit p prim hat Charakteristik p und ist selbst ein Primkörper.

(2) Sei K ein Körper und $I \trianglelefteq K[x]$ maximal. Nach Proposition 6.3 ist $K[x]/I$ ein Körper und mit Satz 7.5 folgt

$$\operatorname{char}\left({}^{K[x]}\!/\!_{I}\right) = \operatorname{char}(K)$$
$$\Pi\left({}^{K[x]}\!/\!_{I}\right) \cong \Pi(K).$$

Beweis. Sei $\operatorname{char}(K) = 0$. Angenommen, es gibt eine Primzahl p mit $p \cdot 1_{K[x]/I} 0_{K[x]/I}$ bzw. $p \cdot (1_K + I) = p \cdot 1_K + I = 0_K + I$. Dann ist $p \cdot 1_K \in I$. Nach Voraussetzung ist aber $p \cdot 1_K \neq 0$ und $p \cdot 1_K$ somit eine Einheit in K bzw. in $K[x]$, sodass $I = K[x]$. Ein Widerspruch. Also $\operatorname{char}(K[x]/I) = 0$. Der Fall $\operatorname{char}(K) = p$ folgt analog. $\square$

Korollar 7.7. *Sei K ein endlicher Körper. Dann gibt es eine Primzahl p und $n \in \mathbb{N}$ mit $|K| = p^n$.*

Beweis. Da $|K| < \infty$, folgt mit Satz 7.5, dass $\Pi(K) \cong \mathbb{Z}_p$ für p prim. Dadurch wird K zum endlich dimensionalen $\mathbb{Z}_p$-Vektorraum. Ist $\{v_1, \ldots, v_n\}$ eine entsprechende Basis von K, so folgt

$$K = \left\{ \sum_{i=1}^{n} \lambda_i v_i \mid \lambda_i \in \mathbb{Z}_p \right\}.$$

Also $|K| = p^n$, wie gewünscht. $\square$

Beispiel 7.8 (Der Körper mit vier Elementen)**.** Sei $K := \mathbb{Z}_2[x]/(x^2 + x + \bar{1})$. Da $x^2 + x + \bar{1}$ unzerlegbar in $\mathbb{Z}_2[x]$ ist, ist K ein Körper nach Kapitel 6.
Nach Beispiel 7.6 (2) gilt $\operatorname{char}(K) = 2$ und $\Pi(K) \cong \mathbb{Z}_2$. Schreibe $I := (x^2 + x + \bar{1}) \trianglelefteq \mathbb{Z}_2[x]$. Als $\mathbb{Z}_2$-Vektorraum hat K die Basis $\{\bar{1} + I, x + I\}$, so dass $K = \{\bar{0} + I, \bar{1} + I, x + I, (x + \bar{1}) + I\}$. Es gilt z. B. $(x + I)^2 = (x + \bar{1}) + I$ und $(x + I) \cdot ((x + \bar{1}) + I) = \bar{1} + I$ (siehe Aufgabe M.13.3).

Ausblick: Für jede Primzahl p und $n \in \mathbb{N}$ gibt es bis auf Isomorphie genau einen Körper mit p^n Elementen.

Definition 7.9. Sei L/K eine Körpererweiterung. Ein Element heißt $\alpha \in L$ heißt **algebraisch über** K, wenn es ein Polynom $f \in K[x] \setminus \{0_{K[x]}\}$ mit $f(\alpha) = 0_L$ existiert. Andernfalls heißt $\alpha \in L$ **transzendent über** K. Die Körpererweiterung L/K heißt **algebraisch**, wenn jedes $\alpha \in L$ algebraisch über K ist.

Beispiel 7.10. (1) Ist L/K eine Körpererweiterung, so ist jedes Element $\alpha \in K$ algebraisch über K, da es Nullstelle des Polynoms $x - \alpha \in K[x]$ ist.

(2) $\alpha = \sqrt{2} \in \mathbb{R}$ ist algebraisch über $\mathbb{Q}$, da α Nullstelle von $x^2 - 2 \in \mathbb{Q}[x]$ ist. Die Körpererweiterung $\mathbb{R}/\mathbb{Q}$ ist nicht algebraisch, da mit $\mathbb{Q}$ auch $\mathbb{Q}[x]$ abzählbar ist und jedes Polynom in $\mathbb{Q}[x]$ nur endlich viele Nullstellen hat. Somit gibt es in $\mathbb{R}$ nur abzählbar viele Elemente, die algebraisch über $\mathbb{Q}$ sind. Beispiele transzendenter Elemente über $\mathbb{Q}$ sind π und e.

(3) Die Körpererweiterung $\mathbb{C}/\mathbb{R}$ ist algebraisch, da $\alpha = a+bi \in \mathbb{C}$ Nullstelle von $(x-a)^2+b^2 \in \mathbb{R}[x]$ ist.

Definition 7.11. Sei L/K eine Körpererweiterung und $M \subseteq L$ eine Teilmenge.

(a) Den Schnitt

$$K(M) := \bigcap_{K \leq K' \leq L, M \subseteq K'} K'$$

aller Teilkörper K' von L, die $K \cup M$ enthalten, nennen wir K **adjungiert** M. $K(M)$ ist der kleinste Zwischenkörper $K \leq K(M) \leq L$ von L/K, der M enthält. Ist $M = \{\alpha_1, \ldots, \alpha_n\}$ endlich, schreiben wir auch $K(\alpha_1, \ldots, \alpha_n)$ statt $K(M)$.

(b) Eine Körpererweiterung $K(\alpha)/K$ für $\alpha \in L$ nennen wir **einfach**. Das Element α heißt dann **primitiv**.

Bemerkung 7.12. Sei L/K eine Körpererweiterung. Für $\alpha \in L$ betrachten den Einsetzungshomomorphismus $\varphi_\alpha \colon K[x] \to L$ mit $f \mapsto f(\alpha)$ und $K[\alpha] = \mathrm{Im}(\varphi_\alpha) = \{f(\alpha) \mid f \in K[x]\} \leq K(\alpha) \leq L$ (siehe Beispiel 4.6 (3)).
α ist transzendent über K genau dann, wenn φ_α injektiv ist. In dem Fall gilt $K[\alpha] \cong K[x]$ und

$$K[\alpha] \cong \mathrm{Quot}(K[x]) = \left\{ \frac{f}{g} \mid f, g \in K[x], g \neq 0_{K[x]} \right\}$$

mit $[K(\alpha) : K] = \infty$.

Ist α algebraisch, erhalten wir das folgende Resultat:

Satz 7.13. *Sei L/K eine Körpererweiterung und $\alpha \in L$ algebraisch über K.*

(a) Es gibt ein eindeutig bestimmtes normiertes Polynom $\mu_\alpha \in K[x] \setminus \{0_{K[x]}\}$ kleinsten Grades, so dass $\mu_\alpha(\alpha) = 0_L$ (μ_α heißt ***Minimalpolynom*** *von α über K).*

(b) Das Minimalpolynom μ_α von α über K ist unzerlegbar in $K[x]$. Es ist das eindeutige normierte unzerlegbare Polynom in $K[x]$ mit α als Nullstelle.

(c) Es gilt $K[x]/(\mu_\alpha) \cong K[\alpha] = K(\alpha)$ und $[K(\alpha) : K] = \deg(\mu_\alpha)$. Insbesondere ist die einfache Körpererweiterung $K(\alpha)/K$ endlich.

Beweis. (a) Betrachte wieder den Einsetzungshomomorphismus $\varphi_\alpha \colon K[x] \to L$. Da $K[x]$ Hauptidealring ist, gilt $\mathrm{Ker}(\varphi_\alpha) = (\mu_\alpha)$ für ein $\mu_\alpha \in K[x]$. Wähle μ_α normiert. Da $\alpha \in L$ algebraisch über K, gilt $\mu_\alpha \neq 0_{K[x]}$. Sei $f \in K[x] \setminus \{0_{K[x]}\}$ mit $f(\alpha) = 0_L$. Dann gilt $f \in \mathrm{Ker}(\varphi_\alpha)$ und somit existiert $g \in K[x] \setminus \{0_{K[x]}\}$ mit $f = \mu_\alpha \cdot g$. Die Gradformel liefert $\deg(f) = \deg(g) + \deg(\mu_\alpha) \geq \deg(\mu_\alpha)$. Angenommen, f ist ebenfalls normiertes Polynom kleinsten Grades mit Nullstelle α. Dann muss g konstant sein, und da μ_α und f normiert, folgt $g = 1_K$ bzw. $f = \mu_\alpha$.

(b) Schreibe $\mu_\alpha = f \cdot g$ mit $f, g \in K[x] \setminus \{0_{K[x]}\}$. Wir müssen zeigen, dass $\deg(f) = 0$ oder $\deg(g) = 0$. Angenommen, $0 < \deg(f), \deg(g) < \deg(\mu_\alpha)$. Dann liefert

$$\mu_\alpha(\alpha) = f(\alpha) \cdot g(\alpha) = 0_L,$$

dass α Nullstelle von f oder g ist. Dies widerspricht der Minimalität des Grades von μ_α.

(c) Nach Teil (b) und Kapitel 6 ist $K[x]/(\mu_\alpha)$ ein Körper. Der Homomorphiesatz liefert

$$K[x]/(\mu_\alpha) = K[x]/\mathrm{Ker}(\varphi_\alpha) \cong \mathrm{Im}(\varphi_\alpha) = K[\alpha].$$

Da $K[\alpha]$ also bereits Körper ist, folgt $K[x] = K(\alpha)$ und

$$[K(\alpha) : K] = \dim_K(K(\alpha)) = \dim_K\left(K[x]/(\mu_\alpha)\right) = \deg(\mu_\alpha).$$

□

Korollar 7.14. *Sei L/K eine Körpererweiterung und $\alpha \in L$ algebraisch über K mit $\deg(\mu_\alpha) = n$. Dann ist $B = \{1_K, \alpha, \ldots, \alpha^{n-1}\}$ eine Basis von $K(\alpha)$ als K-Vektorraum.*

Beweis. Nach Satz 7.13 gilt $K(\alpha) = K[\alpha] = \{f(\alpha) \mid f \in K[x]\}$. Insbesondere enthält $K(\alpha)$ die lineare Hülle

$$\begin{aligned} \mathrm{Lin}_K(1_K, \alpha, \ldots, \alpha^{n-1}) &= \{\lambda_0 1_K + \lambda_1\alpha + \cdots + \lambda_{n-1}\alpha^{n-1} \mid \lambda_i \in K\} \\ &= \{f(\alpha) \mid f \in K[x], \deg(f) \leq n-1\}. \end{aligned}$$

Sei umgekehrt $f \in K[x]$ gegeben. Division mit Rest liefert $q, r \in K[x]$ mit $f = q \cdot \mu_\alpha + r$ und $\deg(r) < \deg \mu_\alpha = n$. Damit gilt

$$f(\alpha) = q(\alpha) \cdot \underbrace{\mu_\alpha(\alpha)}_{=0_L} + r(\alpha) = r(\alpha) \in \mathrm{Lin}_K(1_K, \alpha, \ldots, \alpha^{n-1}).$$

Es folgt $K(\alpha) = \mathrm{Lin}_K(1_K, \alpha, \ldots, \alpha^{n-1})$. Wir zeigen lineare Unabhängigkeit. Seien $\lambda_0, \lambda_1, \ldots, \lambda_{n-1} \in K$ mit $\lambda_0 1_K + \lambda_1\alpha + \cdots + \lambda_{n-1}\alpha^{n-1} = 0_L$. Dann ist $f = \lambda_0 + \lambda_1 x + \cdots + \lambda_{n-1}x^{n-1} \in K[x]$ mit $f(\alpha) = 0_L$ und

$$\deg(f) \leq n - 1 < \deg(\mu_\alpha).$$

Es folgt, dass $f = 0_{K[x]}$ und somit $\lambda_0 = \lambda_1 = \cdots = \lambda_{n-1} = 0_K$. □

Beispiel 7.15. (1) Das Minimalpolynom von $\alpha = \sqrt{2}$ über $\mathbb{Q}$ ist $\mu_\alpha = x^2 - 2 \in \mathbb{Q}[x]$. Es folgt $\mathbb{Q}(\sqrt{2}) = \mathbb{Q}[\sqrt{2}] = \{a + b\sqrt{2} \mid a, b \in \mathbb{Q}\}$

(2) Das Minimalpolynom von $\alpha = \sqrt[3]{2}$ über $\mathbb{Q}$ ist $\mu_\alpha = x^3 - 2$. Beachte, dass $x^3 - 2$ nach Eisenstein bezüglich $p = 2$ unzerlegbar in $\mathbb{Z}[x]$ ist und somit auch $\mathbb{Q}[x]$ nach Satz 6.26. Es gilt $\mathbb{Q}(\sqrt[3]{2}) = \mathbb{Q}[\sqrt[3]{2}] = \{a + b\sqrt[3]{2} + c\sqrt[3]{4} \mid a, b, c \in \mathbb{Q}\}$.

(3) Betrachte die sechste Einheitswurzel $\alpha = e^{2\pi/6} \in \mathbb{Q}$. Dann ist α Nullstelle von $f = x^6 - 1 \in \mathbb{Q}[x]$. Da $f = (x^3 - 1)(x^3 + 1)$ ist f nicht Minimalpolynom von α über $\mathbb{Q}$. Mit $\alpha^3 = -1$ ist α Nullstelle von $g = x^3 + 1 = (x + 1)(x^2 - x + 1)$ und wir erhalten das Minimalpolynom $\mu_\alpha = x^2 - x + 1$ von α über $\mathbb{Q}$.

Wir wollen den Zusammenhang zwischen endlichen Körpererweiterungen und der Adjunktion algebraischer Elemente besser verstehen.

Satz 7.16 (Gradformel)**.** *Sei $K \subseteq L \subseteq M$ Körper. Dann ist die Körpererweiterung M/K endlich genau dann, wenn M/L und L/K endliche Körpererweiterungen sind. In diesem Fall gilt $[M:K] = [M:L] \cdot [L:K]$.*

Beweis. Ist die $\dim_L(M) = \infty$, so gibt es in M eine unendliche Menge linear unabhängiger Vektoren über L. Diese sind auch linear unabhängig über K, d.h. $\dim_K(M) = \infty$.
Ebenso folgt aus $\dim_K(L) = \infty$, dass $\dim_K(M) = \infty$.
Seien M/L und L/K endliche Körpererweiterungen und $\{\alpha_1, \dots, \alpha_n\} \subset L$ eine Basis von L als K-Vektorraum sowie $\{\beta_1, \dots, \beta_n\} \subset M$ eine Basis von M als L-Vektorraum.
Genügt zu zeigen: $B := \{\alpha_i\beta_j \mid i \in \{1, \dots, n\}, j \in \{1, \dots, m\}\}$ ist Basis von M als K-Vektorraum. Sei $\gamma \in M$ beliebig. Schreibe $\gamma = \sum_{j=1}^m \mu_j\beta_j$ mit $\mu_1, \dots, \mu_m \in L$. Jedes μ_j lässt sich schreiben als Linearkombination

$$\mu_j = \lambda_{1j}\alpha_1 + \dots + \lambda_{nj}\alpha_n$$

mit $\lambda_{1n}, \dots, \lambda_{nj} \in K$. Insgesamt erhalten wir

$$\gamma = \sum_{j=1}^m \mu_j\beta_j = \sum_{j=1}^m \sum_{i=1}^n \lambda_{ij}\alpha_i\beta_j \in \mathrm{Lin}_K(B).$$

Für lineare Unabhängigkeit betrachte $\lambda_{ij} \in K$ mit

$$\sum_{j=1}^m \sum_{i=1}^n \lambda_{ij}\alpha_i\beta_j = \sum_{j=1}^m \underbrace{\left(\sum_{i=1}^n \lambda_{ij}\alpha_i\right)}_{=0_L}\beta_j = 0_M.$$

$= 0_L$, da $\{\beta_1, \dots, \beta_m\}$ linear unabhängig über L sind. Es folgt

$\lambda_{ij} = 0_K$ für alle $i \in \{1, \dots, n\}, j \in \{1, \dots, m\}$, da $\{\alpha_1, \dots, \alpha_n\}$ linear unabhängig über K.

□

Korollar 7.17. *(a) Ist L/K eine endliche Körpererweiterung, so ist L/K algebraisch über $L = K(\alpha_1, \dots, \alpha_n)$ für geeignete $\alpha_1, \dots, \alpha_n \in L$.*

(b) Ist L/K eine Körpererweiterung mit $\alpha_1, \dots, a_n \in L$ algebraisch über K, so ist $K(\alpha_1, \dots, \alpha_n)/K$ endlich und somit algebraisch.

Beweis. (a) Angenommen, es gibt $\alpha \in L$ transzendent über K. Wir erhalten Körpererweiterungen $K \leq K(\alpha) \leq L$, wobei $K(\alpha)/K$ nach Bemerkung 7.12 nicht endlich ist. Also ist L/K nicht endlich nach Satz 7.16. Ein Widerspruch. Somit ist L/K algebraisch.

Zudem gilt $L = K(\alpha_1, \dots, \alpha_n)$ für jede Basis $\{\alpha_1, \dots, \alpha_n\} \subset L$ von L als K-Vektorraum.

(b) Betrachte die endliche Kette von Körpererweiterungen

$$K \leq K(\alpha_1) \leq K(\alpha_1)(\alpha_2) = K(\alpha_1, \alpha_2) \leq \dots \leq K(\alpha_1, \dots, \alpha_n).$$

Da $\alpha_i \in L$ algebraisch über K ist, ist α_i algebraisch über $K(\alpha_1, \dots, \alpha_{i-1})$. Nach Satz 7.13 sind die Körpererweiterungen

$$K(\alpha_1, \dots, \alpha_i) = {}^{K(\alpha_1, \dots, a_{i-1})(\alpha_i)}\!\big/\!{}_{K(\alpha_1, \dots, \alpha_{i-1})}$$

endlich. Mit Satz 7.16 folgt induktiv, dass auch $K(\alpha_1, \dots, \alpha_n)/K$ endlich ist.

□

Beispiel 7.18. Betrachte die Körper $\mathbb{Q} \leq \mathbb{Q}(\sqrt{2}) \leq \mathbb{Q}(\sqrt{2}, i)$. Nach Satz 7.16 gilt

$$[\mathbb{Q}(\sqrt{2}, i) : \mathbb{Q}] = [\mathbb{Q}(\sqrt{2}, i) : \mathbb{Q}(\sqrt{2})] \cdot [\mathbb{Q}(\sqrt{2}) : \mathbb{Q}].$$

Nach Beispiel 7.15 (1) gilt $[\mathbb{Q}(\sqrt{2}) : \mathbb{Q}] = 2$ und $\{1, \sqrt{2}\}$ ist Basis von $\mathbb{Q}(\sqrt{2})$ als $\mathbb{Q}$-Vektorraum. Das Minimalpolynom von $\alpha = 1$ über $\mathbb{Q}(\sqrt{2})$ ist $\mu_\alpha = x^2 + 1 \in \mathbb{Q}(\sqrt{2})[x]$, d.h. auch $[\mathbb{Q}(\sqrt{2}, i) : \mathbb{Q}(\sqrt{2})] = 2$ und somit $[\mathbb{Q}(\sqrt{2}, i) : \mathbb{Q}] = 4$.
Der Beweis von Satz 7.16 zeigt, dass $\{1, \sqrt{2}, i, i\sqrt{2}\}$ eine Basis von $\mathbb{Q}(\sqrt{2}, i)$ als $\mathbb{Q}$-Vektorraum ist.