Algebra (AL10)
Skript zur Vorlesung*

Manuel Bodirsky
Institut für Algebra,
manuel.bodirsky@tu-dresden.de

10. Mai 2025

*Emails mit Kommentaren und Verbesserungswünschen sind herzlich willkommen!

Inhaltsverzeichnis

Vorwort

Die Themenauswahl der Vorlesung basiert auf Vorlesungsunterlagen von Arno Fehm. Vielen Dank an Waltraud Lederle für viele Verbesserungsvorschläge zum Skript und an Sebastian Meyer für den Übungsbetrieb. Änderungen im Skript, nachdem die entsprechende Stelle in der Vorlesung behandelt wurde, werden rot markiert.

Literaturempfehlungen:

1. Christian Karpfinger, Kurt Meyberg: *Algebra: Gruppen – Ringe – Körper*, Springer, 3te Auflage, 2013.
2. Jens Carsten Jantzen, Joachim Schwermer: *Algebra*, Spinger, 2te Auflage, 2013.
3. Siegfried Bosch, *Algebra*, Springer, 9te Auflage, 2020.
4. Serge Lang, *Algebra*, Springer, 2002.

Kapitel 1

Gruppen

Zur Wiederholung (siehe Vorlesung LA10): eine *Gruppe* ist ein Tupel $\underline{G} = (G, \cdot, ^{-1}, 1)$ bestehend aus einer Menge G, einer binären Operation $\cdot\colon G^2 \to G$, einer einstelligen Operation $^{-1}\colon G \to G$, und einer nullstelligen Operation $1 \in G$ (d.h., einer Konstanten), so dass die folgenden Bedingungen erfüllt sind:

- $\cdot$ ist assoziativ,
- 1 ist neutrales Element bezüglich $\cdot$, d.h., $1 \cdot g = g \cdot 1 = g$ für alle $g \in G$, und
- für alle $g \in G$ ist das Element g^{-1} invers zu g, d.h., $g^{-1} \cdot g = g \cdot g^{-1} = 1$.

Wir erinnern uns, dass das neutrale Element 1 in $\underline{G}$ eindeutig bestimmt ist, also falls $x \in G$ so, dass $x \cdot g = g \cdot x = g$ für alle $g \in G$, dann gilt $x = 1$. Auch das Inverse ist in Gruppen eindeutig bestimmt, also falls $x, y \in G$ so dass $x \cdot y = y \cdot x = 1$, dann ist $y = x^{-1}$. Wenn man Gruppen angibt, so beschränkt man sich daher meist darauf, die Grundmenge und die Gruppenoperation zu beschreiben, da die Gruppe dadurch vollständig beschrieben wird. Häufig wird das gleiche Symbol für G und für $\underline{G}$ verwendet. Das Multiplikationssymbol wird häufig weggelassen; man schreibt dann also gf statt $g \cdot f$.

Beispiel 1.0.1. $\mathbb{R}$, $\mathbb{Q}$, $\mathbb{Z}$ sind Gruppen bezüglich der jeweiligen Additionsoperation als Gruppenoperation. △

Eine Gruppe ist *abelsch* falls $g \cdot h = h \cdot g$ für alle $g, h \in G$. Für abelsche Gruppen wird häufig auch $+$ anstatt $\cdot$, $-$ anstatt $^{-1}$, und 0 anstatt 1 geschrieben.

Beispiel 1.0.2. Für jeden Ring R bildet die Menge der Einheiten $R^\times$ eine Gruppe bezüglich der Multiplikation; zum Beispiel

- für jeden Körper $\mathbb{K}$ und jedes $n \in \mathbb{N}$ die Gruppe $\mathrm{GL}_n(\mathbb{K}) = (\mathbb{K}^{n \times n}, \cdot, ^{-1}, E_n)$,
- $\mathbb{Q}^\times = \mathbb{Q} \setminus \{0\}$,
- $\mathbb{Z}^\times = \{-1, 1\}$. △

Beispiel 1.0.3. Sei X eine Menge. Dann besteht die *symmetrische Gruppe* $\mathrm{Sym}(X)$ aus der Menge aller Permutationen von X zusammen mit der Hintereinanderausführung $\circ$ (Komposition) als Gruppenoperation. Für $\mathrm{Sym}(\{1,\dots,n\})$ schreiben wir auch S_n. △

Seien $k, n \in \mathbb{N}$ und seien $i_1, \dots, i_k \in \{1,\dots,n\}$ paarweise verschieden. Dann bezeichnet $(i_1 \dots i_k)$ die Permutation $\sigma \in S_n$, welche definiert wird durch

$$\begin{aligned} \sigma(i_j) &= i_{j+1} && \text{für } j \in \{1,\dots,k-1\} \\ \sigma(i_k) &= i_1 && \text{für } j \in \{1,\dots,k-1\} \\ \sigma(i) &= i && \text{für } j \in \{1,\dots,n\} \setminus \{i_1,\dots,i_k\}. \end{aligned}$$

Die Permutation $\sigma = (i_1 \dots i_k)$ heißt *k-Zykel*. Die Elemente von $\{1,\dots,n\} \setminus \{i_1,\dots,i_k\}$ heißen auch die *Fixpunkte* von σ.

Zwei Zykel $(i_1,\dots,i_k)$ und $(j_1,\dots,j_\ell)$ heißen *disjunkt* falls $\{i_1,\dots,i_k\} \cap \{j_1,\dots,j_k\} = \varnothing$. Disjunkte Zykel σ_1 und σ_2 *kommutieren*, d.h. es gilt $\sigma_1 \circ \sigma_2 = \sigma_2 \circ \sigma_1$. Jede Permutation $\sigma \in S_n$ kann geschrieben werden als $\sigma = \pi_1 \cdots \pi_k$ für disjunkte Zykel $\pi_1,\dots,\pi_k$; hierbei ist die Menge $\{\pi_1,\dots,\pi_k\}$ eindeutig, und wird *Zykelzerlegung* genannt.

Übung 1. Zeigen Sie, dass für jede Gruppe $(G,\cdot)$ gilt: In der Verknüpfungstafel für $\cdot$ tritt in jeder Zeile und in jeder Spalte jedes Element von G genau einmal auf.

Übung 2. Es sei $\underline{G}$ eine Gruppe, so dass $a^2 = 1$ für alle $a \in G$. Zeigen Sie, dass G abelsch ist.

1.1 Untergruppen

Wir erinnern uns weiterhin an die folgenden zentralen Definitionen (siehe Vorlesung LA10).

Definition 1.1.1 (Untergruppen)**.** Sei $\underline{G}$ eine Gruppe. Eine Teilmenge $H \subseteq G$ heißt *Untergruppe von* $\underline{G}$ falls

- $e \in H$,
- H abgeschlossen ist unter Inversenbildung, d.h., für jedes $h \in H$ ist $h^{-1} \in H$, und
- H abgeschlossen ist unter der Gruppenoperation, d.h., für alle $h_1, h_2 \in H$ ist $h_1 \cdot h_2 \in H$.

Wir schreiben dann auch $H \leq \underline{G}$, und schreiben $H < \underline{G}$ falls zusätzlich $H \neq G$ (manchmal ist es praktisch, auch die gleichbedeutende Schreibweise $\underline{G} \geq H$ beziehungsweise $\underline{G} > H$ zu verwenden).

Falls $H \leq \underline{G} = (G, \cdot, {}^{-1}, 1)$, dann erhalten wir durch Einschränkung der Gruppenoperation auf H eine Gruppe, nämlich $\underline{H} := (H; \cdot|_H, {}^{-1}|_H, 1)$.

Übung 3. Zeigen Sie: $H \leq \underline{G}$ genau dann, wenn $H \neq \varnothing$ und $ab^{-1} \in H$ für alle $a, b \in H$.

Lemma 1.1.2. *Sei $\underline{G}$ eine Gruppe. Zu jeder Menge $X \subseteq G$ gibt es eine kleinste Untergruppe von $\underline{G}$, die X enthält, nämlich*

$$\langle X \rangle := \bigcap_{X \subseteq H \leq \underline{G}} H$$

die von X erzeugte Untergruppe von $\underline{G}$. *Es gilt*

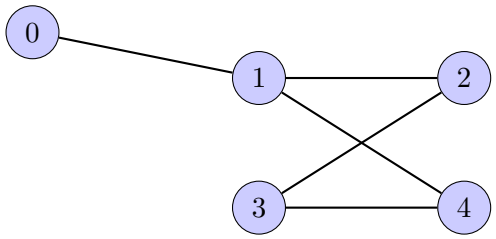
$$\langle X \rangle = \left\{ g_1^{\epsilon_1} \cdots g_r^{\epsilon_r} \mid r \in \mathbb{N}, g_1, \ldots, g_r \in X, \epsilon_1, \ldots, \epsilon_r \in \{1, -1\} \right\}.$$

Falls $g \in G$, so schreiben wir auch $\langle g \rangle$ anstatt $\langle \{g\} \rangle$.

Beispiel 1.1.3. Für $n \in \mathbb{Z}$ gilt $\langle n \rangle = \{0, -n, n, 2n, -2n, \ldots\} =: n\mathbb{Z} \leq \mathbb{Z}$. △

Beispiel 1.1.4. Eine *Transposition* ist ein 2-Zykel. Die Menge der Transpositionen in S_n erzeugt S_n (siehe Vorlesung LA10). Die Menge der Produkte von zwei Transpositionen erzeugt A_n, die alternierende Gruppe. △

Beispiel 1.1.5. Ein *Graph* ist ein Paar (V, E) wobei V eine beliebige Menge, und $E \subseteq \binom{V}{2}$ eine Menge von 2-elementigen Teilmengen von V. Graphen lassen sich gut graphisch illustrieren: der Graph $(\{0, 1, 2, 3, 4\}, \{\{0, 1\}, \{1, 2\}, \{3, 4\}, \{4, 1\})$ beispielsweise wie folgt.



Die *Automorphismengruppe* $\mathrm{Aut}(V, E)$ eines Graphen (V, E) besteht aus allen $\sigma \in \mathrm{Sym}(V)$ mit der Eigenschaft, dass $\{u, v\} \in E$ genau dann, wenn $\{\sigma(u), \sigma(v)\} \in E$. Es gilt $\mathrm{Aut}(V, E) \leq \mathrm{Sym}(V)$. △

Übung 4. Sei $\underline{G}$ eine Gruppe und $H_1, H_2 \leq \underline{G}$. Dann gilt $H_1 \cup H_2 \leq \underline{G}$ genau dann, wenn $H_1 \subseteq H_2$ oder $H_2 \subseteq H_1$.

Übung 5. Sei $(V, E) = \left(\{1, 2, 3, 4\}, \{\{1, 2\}, \{2, 3\}, \{3, 4\}, \{4, 1\}\} \right)$ (ein *Kreis der Länge vier*). Geben Sie eine Menge von Permutationen an, die $\mathrm{Aut}(V, E)$ erzeugt.

Übung 6. Finden sie einen Graphen (V, E) mit einer Bijektion $\sigma \in \mathrm{Sym}(V)$ so dass für alle $\{u, v\} \in E$ auch $\{\sigma(u), \sigma(v)\} \in E$, so dass σ aber kein Automorphismus ist. Zeigen Sie, dass dann V nicht endlich sein kann.

Übung 7. Zeigen Sie, dass $\mathrm{Sym}(X)$ für unendliches X nicht von den Transpositionen erzeugt wird.

Übung 8. Falls es eine endliche Menge $S \subseteq G$ gibt, so dass $G = \langle S \rangle$, so heißt $\underline{G}$ *endlich erzeugt*. Zeigen Sie, dass $(\mathbb{Q}; +)$ nicht endlich erzeugt ist.

Übung 9. Die *Kleinsche Vierergruppe* V_4 ist die Gruppe $(\{1, a, b, ab\}, \cdot)$, wobei $\cdot$ durch folgende *Verknüpfungstafel* (oder *Kompositionstabelle*) gegeben ist:

$\cdot$	1	a	b	ab
1	1	a	b	ab
a	a	1	ab	b
b	b	ab	1	a
ab	ab	b	a	1

Zeigen Sie: $V_4 \leq S_4$ (siehe Beispiele 1.0.3). (Diese Gruppe wird uns in Beispiel 1.6.2 wieder begegnen.)

1.2 Gruppenhomomorphismen

Gruppenhomomorphismen sind die wesentlichen strukturerhaltenden Abbildungen für Gruppen.

Definition 1.2.1 (Gruppenhomomorphismus)**.** Es seien $\underline{G}$ und $\underline{H}$ Gruppen. Eine Abbildung $\varphi\colon G \to H$ heißt *(Gruppen-) Homomorphismus (von $\underline{G}$ nach $\underline{H}$)* falls gilt

$$\varphi(g_1 \cdot g_2) = \varphi(g_1) \cdot \varphi(g_2).$$

Das Urbild von e unter φ heißt der *Kern* von φ. Die Menge aller Homomorphismen von $\underline{G}$ nach $\underline{H}$ wird mit $\mathrm{Hom}(\underline{G}, \underline{H})$ bezeichnet. Falls φ surjektiv ist, so nennt man $\underline{H}$ auch ein *homomorphes Bild von $\underline{G}$*.

Bemerkung 1.2.2. Bild und Kern eines Gruppenhomomorphismus sind Untergruppen: Falls φ ein Gruppenhomomorphismus von $\underline{G}$ nach $\underline{H}$ ist, so ist $\mathrm{Bild}(\varphi) \leq \underline{H}$ und $\mathrm{Kern}(\varphi) \leq \underline{G}$.

Ein *(Gruppen-) Isomorphismus* zwischen $\underline{G}$ und $\underline{H}$ ist ein bijektiver Gruppenhomomorphismus von $\underline{G}$ nach $\underline{H}$; falls es einen Isomorphismus zwischen $\underline{G}$ und $\underline{H}$ gibt, so heißen $\underline{G}$ und $\underline{H}$ *isomorph*, und wir schreiben $\underline{G} \cong \underline{H}$. Ein *(Gruppen-) Automorphismus* von $\underline{G}$ ist ein Isomorphismus zwischen $\underline{G}$ und $\underline{G}$.

Bemerkung 1.2.3. Falls $\varphi\colon \underline{G} \to \underline{G'}$ und $\psi\colon \underline{G'} \to \underline{G''}$ Gruppenhomomorphismen sind, so ist die Komposition $\psi \circ \varphi$ ein Gruppenhomomorphismus von $\underline{G} \to \underline{G''}$.

Bemerkung 1.2.4. Die Menge aller Automorphismen einer Gruppe $\underline{G}$ ist bezüglich der Komposition als Operation eine Gruppe, die mit $\mathrm{Aut}(\underline{G})$ bezeichnet wird.

Übung 10. Zeigen Sie, dass für jeden Gruppenhomomorphismus $\varphi\colon \underline{G} \to \underline{H}$ und jedes $g \in G$ gilt, dass $\varphi(g^{-1}) = \varphi(g)^{-1}$.

Übung 11. Es seien $\underline{G}$ und $\underline{H}$ Gruppen und X so, dass $\langle X \rangle = \underline{G}$. Falls $\varphi, \psi \in \mathrm{Hom}(\underline{G}, \underline{H})$ so, dass $\varphi|_X = \psi_X$, dann gilt $\varphi = \psi$.

Übung 12. Sei $\varphi \in \mathrm{Hom}(\underline{G}, \underline{H})$. Zeigen Sie die Behauptungen aus Bemerkung 1.2.2: $\mathrm{Bild}(\varphi) \leq \underline{H}$ und $\mathrm{Kern}(\varphi) \leq \underline{G}$.

Definition 1.2.5. Sei $\underline{G}$ eine Gruppe, $g \in G$, und $z \in \mathbb{Z}$. Dann definieren wir

$$g^z := \begin{cases} \underbrace{g \cdot \cdots \cdot g}_{z \text{ mal}} & \text{falls } z \geq 0 \\ \underbrace{(g \cdot \cdots \cdot g)}_{-z \text{ mal}}^{-1} & \text{falls } z < 0. \end{cases}$$

Übung 13. Sei $\varphi \in \mathrm{Hom}(\underline{G}, \underline{H})$ und $z \in \mathbb{Z}$, und $g \in G$. Dann gilt $\varphi(g^z) = \varphi(g)^z$.

Proposition 1.2.6 (Satz von Cayley)**.** *Jede Gruppe $\underline{G}$ ist isomorph zu einer Untergruppe von* $\mathrm{Sym}(G)$.

Beweis. Für $a \in G$, definiere $\tau_a \colon G \to G$ durch $g \mapsto ag$ (eine sogenannte *Linkstranslation*). Sei $\varphi \colon G \to \mathrm{Sym}(G)$ die durch $a \mapsto \tau_a$ gegebene Abbildung. Dann ist φ ein injektiver Gruppenhomomorphismus von $\underline{G}$ nach $\mathrm{Sym}(G)$, also ein Isomorphismus zwischen $\underline{G}$ und einer Untergruppe von $\mathrm{Sym}(G)$. □

Untergruppen von $\mathrm{Sym}(X)$ heißen *Permutationsgruppen (auf X)*. Für weitere wichtige Beispiele von Gruppenhomomorphismen benötigen wir den Begriff der *Konjugation*.

Definition 1.2.7 (Konjugation)**.** Sei $\underline{G}$ eine Gruppe und sei $x, g \in G$. Dann heißt gxg^{-1} die *Konjugation von x mit g*.

Bemerkung 1.2.8. Zwei Elemente $x_1, x_2 \in G$ heißen *konjugiert*, falls es ein $g \in G$ gibt mit $gx_1g^{-1} = x_2$. Dies definiert eine Äquivalenzrelation auf G.

Bemerkung 1.2.9. Die Abbildung $\mathrm{int}_g \colon G \to G$ gegeben durch $x \mapsto gxg^{-1}$ ist ein Automorphismus von $\underline{G}$; solche Automorphismen heißen auch *innere Automorphismen* von $\underline{G}$. Die Abbildung $g \mapsto \mathrm{int}_g$ ist ein Gruppenhomomorphismus $\mathrm{int} \colon \underline{G} \to \mathrm{Aut}(\underline{G})$. Die Menge aller inneren Automorphismen, also das Bild von int, wird mit $\mathrm{Inn}(G)$ bezeichnet. Der Kern von int ist die Menge

$$\begin{aligned} \{g \in G \mid \mathrm{int}_g = \mathrm{id}_G\} &= \{g \in G \mid g^{-1}xg = x \text{ für alle } x \in G\} \\ &= \{g \in G \mid xg = gx \text{ für alle } x \in G\} =: Z(G) \end{aligned}$$

und wird *Zentrum* von G genannt. Offensichtlicherweise ist genau dann $G = Z(G)$, wenn G abelsch ist.

Bemerkung 1.2.10. Konjugation in S_n erhält die Zykelstruktur von Permutationen $\sigma \in S_n$: das bedeutet, wenn $(a_1a_2\dots)(b_1b_2\dots)\cdots$ die Zykeldekomposition von σ ist (siehe Beispiel 1.0.3), dann gilt für jedes $\rho \in S_n$, dass

$$\rho\sigma\rho^{-1} = (\rho(a_1)\rho(a_2)\dots)(\rho(b_1)\rho(b_2)\dots).$$

Es genügt, nachzurechnen, dass beide Permutationen auf einem beliebig gewählten Element übereinstimmen. Wegen den Symmetrien der Zykelzerlegung genügt es sogar, dies für das Element $\rho(a_1)$ nachzuweisen. Es gilt

$$\begin{aligned}\rho\sigma\rho^{-1}(\rho(a_1)) &= \rho\sigma(a_1)\\ &= \rho(a_2).\end{aligned}$$

Übung 14. Beweisen Sie die Behauptungen in Bemerkung 1.2.9.

Übung 15. Zeigen Sie, dass es bis auf Isomorphie nur zwei Gruppen der Ordnung 4 gibt (welche?).

1.3 Ordnung und Index

Sei $\underline{G}$ eine Gruppe und $g \in G$. Dann heißt $|G|$ die *Ordnung* von $\underline{G}$. Die *Ordnung* eines Elementes $g \in G$ ist definiert als $\mathrm{Ord}(g) := |\langle g\rangle| \in \mathbb{N} \cup \{\infty\}$.

Beispiel 1.3.1. Sei $n \in \mathbb{N}$. Dann gelten

- $|S_n| = n!$,
- $|A_n| = n!/2$ für $n \geq 2$,
- Ist $\sigma \in S_n$ ein k-Zykel, so ist $\mathrm{Ord}(\sigma) = k$.
- Für $z \in \mathbb{Z} \setminus \{0\}$ gilt $\mathrm{Ord}(z) = \infty$, und $\mathrm{Ord}(0) = 1$. △

Bemerkung 1.3.2. Es ist $\langle g\rangle = \{1, g, g^{-1}, g^2, g^{-2}, \dots\}$ (siehe Definition 1.2.5). Ist $n := \mathrm{Ord}(g) \in \mathbb{N}$, so ist $\langle g\rangle = \{1, g, g^2, g^3, \dots, g^{n-1}\}$.

Definition 1.3.3. Seien $\underline{G}$ eine Gruppe und $A, B \subseteq G$. Dann heißt

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

das *Komplexprodukt* von A und B.

Definition 1.3.4 (Links- und Rechtsnebenklassen)**.** Sei $\underline{G}$ eine Gruppe, $H \leq \underline{G}$, und $g \in G$. Dann heißt

$$gH := \{g\} \cdot H = \{g \cdot b \mid b \in H\}$$

die *Linksnebenklasse von H bezüglich g* (oder *'nach g'*, oder *'von g modulo H'*). Analog heißt $Hg := H \cdot \{g\}$ die *Rechtsnebenklasse* von H bezüglich g. Wir schreiben $\underline{G}/H := \{gH \mid g \in G\}$ für die Menge aller Linksnebenklassen von H, und $H\backslash\underline{G} := \{Hg \mid g \in G\}$ für die Menge aller Rechtsnebenklassen von H.

Bemerkung 1.3.5. Für $h \in H$ gilt $hH = H = Hh$.

Lemma 1.3.6. *Seien $\underline{G}$ eine Gruppe, $H \leq \underline{G}$, und $a, b \in G$. Dann sind äquivalent:*

1. $aH = bH$;

2. $aH \cap bH \neq \emptyset$;

3. $a \in bH$;

4. $b^{-1}a \in H$.

Beweis. Aus 1. folgt trivialerweise 2., da $H \neq \emptyset$. Falls 2. gilt, so gibt es ein $c \in aH \cap bH$, also gibt es $h_1, h_2 \in H$ mit $c = ah_1 = bh_2$. Es folgt $a = bh_2h_1^{-1} \in bH$, und somit 3. Offensichtlich folgt 4. aus 3. Gilt 4., dann $a \in bH$ und folglich $aH \subseteq bH$. Da $b^{-1}a \in H$ ist auch das hierzu inverse Element $a^{-1}b$ ein Element von H. Entsprechend gilt $bH \subseteq aH$ und somit $aH = bH$. □

Zwei Nebenklassen von $H \leq \underline{G}$ sind entweder gleich oder disjunkt.

Lemma 1.3.7. *Sei $\underline{G}$ eine Gruppe, $H \leq \underline{G}$, und $a, b \in G$. Es gilt $aH = bH$ oder $aH \cap bH = \emptyset$.*

Beweis. Wenn aH und bH nicht disjunkt sind, gibt es ein $x \in aH \cap bH$. Also gilt $aH = xH = bH$ nach Lemma 1.3.6 (zweimal angewandt). □

Lemma 1.3.8. *$gH \mapsto Hg^{-1}$ ist eine wohldefinierte Bijektion $\underline{G}/H \to H\backslash\underline{G}$. Analoge Aussagen zu Lemma 1.3.6 und Lemma 1.3.7 gelten für Rechtsnebenklassen anstatt Linksnebenklassen.*

Definition 1.3.9. Sei $\underline{H} \leq \underline{G}$. Dann ist

$$(\underline{G} : H) := |\underline{G}/H| = |H\backslash\underline{G}|$$

der *Index* von H in $\underline{G}$.

Beispiel 1.3.10. $(S_n : A_n) = 2$ (siehe Beispiel 1.3.1) und $(\mathbb{Z} : n\mathbb{Z}) = n$ (siehe Beispiel 1.1.3). △

Man kann den Index leicht bestimmen, wenn man beachtet, dass jede Nebenklasse von H die gleiche Mächtigkeit hat wie H. Das ist deshalb richtig, weil die Abbildung $H \to g \circ H$ mit $h \mapsto g \circ h$ stets bijektiv ist. Die Nebenklassen von H zerlegen also die Menge G in gleichgroße disjunkte Teilmengen.

Satz 1.3.11 (Lagrange)**.** *Ist $\underline{G}$ endlich und $H \leq \underline{G}$, so gilt $|G| = |H| \cdot (\underline{G} : H)$.*

Weil $(G : H)$ ganzzahlig ist, teilt also die Ordnung einer Untergruppe einer endlichen Gruppe G stets die Ordnung der Gruppe. Es folgt, dass die Ordnung eines Elementes $a \in G$ ein Teiler ist von $|G|$.

Die folgende Aussage wird auch häufig der *kleine fermatsche Satz*, oder kurz der *kleine Fermat* genannt.

Korollar 1.3.12. *Sei $\underline{G}$ eine Gruppe der Ordnung $n \in \mathbb{N}$ und $a \in G$. Dann gilt $a^n = 1$.*

Beweis. Sei $H := \langle\{a\}\rangle$. Dann gilt $a^{|H|} = 1$ (siehe Bemerkung 1.3.2) und

$$a^{|G|} = a^{|H|\cdot(\underline{G}:H)} = 1^{(\underline{G}:H)} = 1\,. \qquad \square$$

Bemerkung 1.3.13. Nach dem Satz von Lagrange (Satz 1.3.11) ist die Ordnung jeder Untergruppe ein Teiler der Gruppenordnung. Umgekehrt gibt es im Allgemeinen jedoch nicht zu jedem Teiler d der Gruppenordnung eine Untergruppe der Ordnung d: zum Beispiel hat A_4 keine Untergruppe der Ordnung 6, obwohl 6 ein Teiler ist von $|A_4| = 4!/2 = 12$. Wir werden aber verschiedene Situationen kennenlernen, in denen dies der Fall ist (siehe Abschnitt 1.5, oder Abschnitt 1.10).

Übung 16. Zeigen Sie: das Komplexprodukt UV von zwei Untergruppen einer Gruppe G ist im allgemeinen keine Untergruppe von G.

Übung 17. Seien $\underline{A}$ und $\underline{B}$ Untergruppen von $\underline{G}$ mit teilerfremden Indizes. Beweisen Sie, dass $(\underline{G} : (A \cap B)) = (\underline{G} : A) \cdot (\underline{G} : B)$.

Übung 18. A_4 hat keine Untergruppe vom Index 6.

Übung 19. Sei $\sigma \in S_n$ mit Zykelzerlegung $\{\pi_1, \ldots, \pi_n\}$. Zeigen Sie, dass

$$\mathrm{Ord}(\sigma) = \mathrm{kgV}(\mathrm{Ord}(\pi_1), \ldots, \mathrm{Ord}(\pi_n)).$$

Übung 20. Sei $\underline{G}$ eine Gruppe und $A, B \leq \underline{G}$. Dann gilt genau dann $AB \leq \underline{G}$, wenn $AB = BA$.

1.4 Normalteiler und Quotientengruppen

Sei $\underline{G}$ eine Gruppe. Gewisse Untergruppen von $\underline{G}$ erlauben uns, Homomorphismen von $\underline{G}$ in andere Gruppen zu verstehen. Im folgenden unterscheiden wir notationell nicht mehr zwischen $\underline{G}$ und G, und lassen den Unterstrich weg.

Definition 1.4.1. Eine Untergruppe $H \leq G$ ist *normal* falls $ghg^{-1} \in H$ für alle $h \in H$ und $g \in G$. Eine normale Untergruppe von G heißt auch ein *Normalteiler* von G, und wir schreiben $H \trianglelefteq G$.

Bemerkung 1.4.2. Offensichtlicherweise gilt genau dann $H \trianglelefteq G$, wenn $Hg = gH$ für alle $g \in G$ gilt.

Beispiel 1.4.3. Falls G abelsch ist, so ist jede Untergruppe von $\underline{G}$ normal. $\triangle$

Beispiel 1.4.4. Jede Gruppe G ist ihr eigener Normalteiler. Alle anderen Normalteiler heißen *echte* Normalteiler. Jede Gruppe G hat weiterhin den Normalteiler $\{1\}$, den *trivialen* Normalteiler. $\triangle$

Beispiel 1.4.5. $\langle(123)\rangle$ ist eine normale Untergruppe von S_3, aber $\langle(12)\rangle$ ist es nicht. $\triangle$

Beispiel 1.4.6. Das Zentrum einer Gruppe G ist stets ein Normalteiler von G, i.e., $Z(G) \trianglelefteq G$ (siehe Bemerkung 1.2.9). $\triangle$

Lemma 1.4.7. *Sei $\varphi\colon G \to H$ ein Gruppenhomomorphismus. Dann ist* $\mathrm{Kern}(\varphi)$ *eine normale Untergruppe von G.*

Beweis. Für jedes $a \in G$ und $g \in \mathrm{Kern}(\varphi)$ gilt, dass

$$\varphi(a \cdot g \cdot a^{-1}) = \varphi(a) \cdot \underbrace{\varphi(g)}_{=1} \cdot \varphi(a^{-1}) = \varphi(a) \cdot \varphi(a)^{-1} = 1,$$

also ist $aga^{-1} \in \mathrm{Kern}(\varphi)$. □

Umgekehrt ist jeder Normalteiler der Kern eines geeignet gewählten Gruppenhomomorphismus, wie man aus der folgenden Proposition sieht.

Proposition 1.4.8. *Sei $N \trianglelefteq G$. Dann ist G/N mit dem Komplexprodukt eine Gruppe und $\pi_N\colon G \to G/N$ mit $g \mapsto gN$ ein surjektiver Gruppenhomomorphismus mit* $\mathrm{Kern}(\pi_N) = N$ *(die sogenannte* kanonische Projektion*).*

Beweis. Wir verwenden die Normalität von N, um nachzuweisen, dass das Komplexprodukt tatsächlich eine Operation auf den Linksnebenklassen definiert: falls $a, b \in G$, dann gilt

$$\begin{aligned}(aN) \cdot (bN) &= \{a\} \cdot \{N\} \cdot \{b\} \cdot N \\ &= \{a\} \cdot \{b\} \cdot \{N\} \cdot N = \{ab\} \cdot (NN) = (ab)N.\end{aligned}$$

Es folgt unmittelbar aus den Gruppeneigenschaften von G, dass das Komplexprodukt auf G/N assoziativ ist, dass $N = 1N$ das neutrale Element ist, und dass $a^{-1}N$ das inverse Element zu aN ist. □

Bemerkung 1.4.9. Eine Untergruppe $U \leq G$ ist genau dann normal, wenn $\sigma(U) = U$ für alle $\sigma \in \mathrm{Inn}(G)$ (Bemekung 1.2.9): denn falls U normal und $\sigma = \mathrm{int}_g$ für $g \in G$, dann ist $\mathrm{int}_g(U) = g^{-1}Ug = U$, und umgekehrt.

Übung 21. Es sei $A \leq G$ und $B \trianglelefteq G$. Zeigen Sie, dass $AB \leq G$ (Achtung: siehe Übung 16).

Übung 22. Es seien A und B Normalteiler von G. Zeigen Sie, dass $AB \trianglelefteq G$.

Übung 23. Verwenden Sie Bemerkung 1.4.9 und Bemerkung 1.2.10, um zu zeigen, dass $A_n \trianglelefteq S_n$ für jedes $n \in \mathbb{N}_{\geq 1}$.

Definition 1.4.10. Für $N \trianglelefteq G$ heißt G/N (gesprochen G *modulo* N) zusammen mit dem Komplexprodukt die *Quotientengruppe*[1] *von G nach N.*

Beispiel 1.4.11. Für $n \in \mathbb{Z}$ ist $n\mathbb{Z}$ normal (siehe Beispiel 1.1.3 und Beispiel 1.4.3). Dann ist $\mathbb{Z}/n\mathbb{Z}$ die aus LA10 bekannte Restklassengruppe der Ordnung n. △

Proposition 1.4.12 (Homomorphiesatz)**.** *Sei $\varphi\colon G \to H$ ein Gruppenhomomorphismus und $N \trianglelefteq G$ mit $N \subseteq \mathrm{Kern}(\varphi)$. Dann existiert genau ein Gruppenhomomorphismus*

$$\psi\colon G/N \to H \text{ mit } \varphi = \psi \circ \pi_N,$$

der sogenannte kanonische *Gruppenhomomorphismus von G/N nach H.*

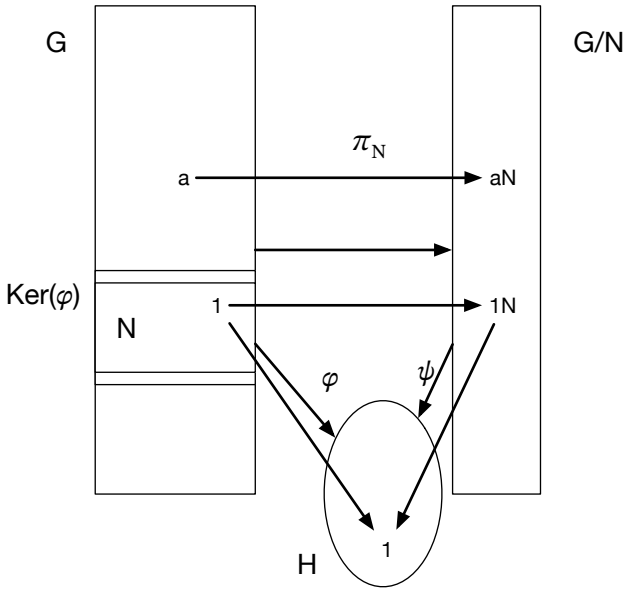


Abbildung 1.1: Illustration zum Homomorphiesatz (Proposition 1.4.12).

Siehe Abbildung 1.1 Es gilt:

$$\text{Bild}(\psi) = \text{Bild}(\varphi), \tag{1.1}$$
$$\text{Kern}(\psi) = \pi_N(\text{Kern}(\varphi)), \tag{1.2}$$
$$\text{Kern}(\varphi) = \pi_N^{-1}(\text{Kern}(\psi)). \tag{1.3}$$

Die Abbildung ψ ist genau dann injektiv, wenn $\text{Kern}(\psi) = \{N\}$.

Beweis. Wenn ein Gruppenhomomorphismus $\psi\colon G/N \to H$ mit $\varphi = \psi \circ \pi_N$ existiert, dann gilt für alle $a \in G$, dass $\psi(aN) = \psi(\pi_N(a)) = \varphi(a)$, also is ψ eindeutig. Für die Existenz von ψ zeigen wir zunächst, dass $\psi(aN) := \varphi(a)$ unabhängig von der Auswahl des Repräsentanten $a \in aN$ ist. Gelte also $aN = bN$ für $a, b \in G$. Dann folgt $b^{-1}a \in N$ (Lemma 1.3.6), und da $N \subseteq \text{Kern}(\varphi)$ gilt $\varphi(b^{-1}a) = 1$, also $\varphi(a) = \varphi(b)$. Man rechnet nun einfach nach, dass ψ ein Gruppenhomomorphismus ist. □

Korollar 1.4.13. *Ist $\varphi\colon G \to H$ ein* surjektiver *Gruppenhomomorphismus, so ist H isomorph zu $G/\text{Kern}(\varphi)$.*

Beweis. Nach dem Homomorphiesatz angewandt auf $N := \text{Kern}(\varphi)$ gibt es einen Gruppenhomomorphismus $\varphi\colon G/\text{Kern}(\varphi) \to H$ mit $\varphi = \psi \circ \pi_N$. □

Beispiel 1.4.14. In Bemerkung 1.2.9 hatten wir das Zentrum von G

$$Z(G) = \{g \in G \mid xg = gx \text{ für alle } x \in G\}$$

[1] Häufig wird die Quotientengruppe auch *Faktorgruppe* oder *Restklassengruppe* genannt.

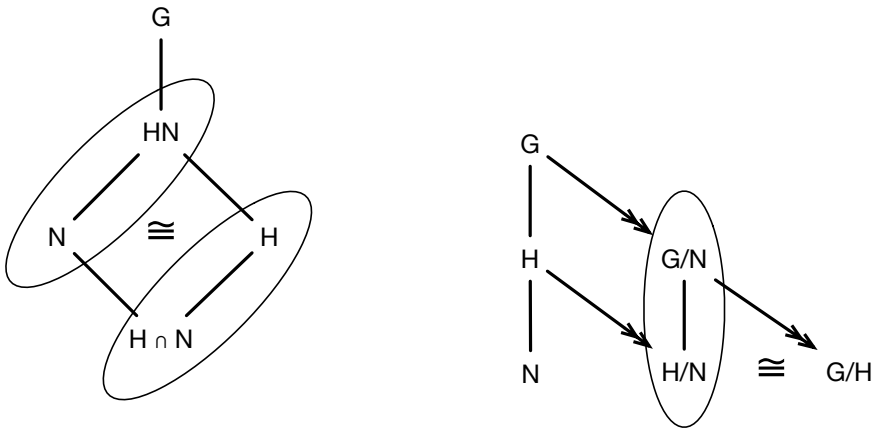


Abbildung 1.2: Illustration zu Proposition 1.4.15 (Diamantenisomorphiesatz, links) und zu Proposition 1.4.16 (Kürzungsisomorphiesatz, rechts). Eine aufsteigende Linie von A nach B bedeutet, dass $A \leq B$, und ein gerichteter Pfeil von A nach B bedeutet, dass es einen surjektiven Homomorphismus von A nach B gibt.

definiert als den Kern des Gruppenhomomorphismus $\mathrm{int}\colon G \to \mathrm{Aut}(G)$, der gegeben ist durch $g \mapsto \mathrm{int}_g$. Also ist die Gruppe der inneren Automorphismen von G (nämlich das Bild von int) isomorph zu G/Z. △

Aus dem Homomorphiesatz folgen weiterhin die sogenannten Isomorphiesätze.[2]

Proposition 1.4.15 (Diamantenisomorphiesatz)**.** *Sei G ein Gruppe, $H \leq G$, und $N \trianglelefteq G$. Dann gilt*

$$(H \cap N) \trianglelefteq H \text{ und } N \trianglelefteq HN \leq G$$

und der kanonische Homomorphismus $H/(H \cap N) \to (HN)/N$ ist ein Isomorphismus.

Beweis. Es gilt $HN(HN)^{-1} \subseteq HNH^{-1} \subseteq HH^{-1}N \subseteq HN$, also $HN \leq G$. Weiterhin folgt $N \trianglelefteq HN$ aus $N \trianglelefteq G$. Dann ist die Einschränkung von π_N auf $H \subseteq HN$ ein surjektiver Gruppenhomomorphismus von H nach HN/N mit Kern $H \cap N$. Also $(H \cap N) \trianglelefteq H$, und nach Korollar 1.4.13 gilt $HN/N \cong H/(H \cap N)$. □

Siehe Abbildung 1.2 (links) für eine Illustration zu Proposition 1.4.15.

Proposition 1.4.16 (Kürzungsisomorphiesatz)**.** *Sei G eine Gruppe und $H, N \trianglelefteq G$ mit $N \subseteq H$. Dann $N \trianglelefteq H$ und $H/N \trianglelefteq G/N$. Der kanonische Gruppenhomomorphismus*

$$(G/N)/(H/N) \to G/H$$

ist ein Isomorphismus.

[2] Häufig werden diese auch *erster* beziehungsweise *zweiter Isomorphiesatz* genannt, aber die Konventionen sind hier unter den Autor:innen nicht eindeutig, und wir wählen daher Bezeichnungen, die sich nach dem jeweiligen Inhalt des Satzes richten.

Beweis. $N \trianglelefteq H$ ist offensichtlich. Der Kern von $\pi_H \colon G \to G/H$ enthält N, da $N \subseteq H$. Nach Satz 1.4.12 angewandt auf π_H gibt es einen Gruppenhomomorphismus $\psi \colon G/N \to G/H$. Dieser ist surjektiv, da $\text{Bild}(\psi) \overset{(1.1)}{=} \text{Bild}(\pi_H) = G/H$. Weiterhin gilt

$$\text{Kern}(\psi) \overset{(1.2)}{=} \pi_N(\text{Kern}(\pi_H)) = \pi_N(H) = H/N.$$

Insbesondere gilt $H/N \trianglelefteq G/N$. Korollar 1.4.13 angewandt auf ψ liefert dann einen Isomorphismus zwischen G/H und $(G/N)/(G/H)$. □

Siehe Abbildung 1.2 (rechts) für eine Illustration zu Proposition 1.4.16.

Proposition 1.4.17. *Sei G eine Gruppe und $H \leq G$ so, dass $(G : H) = 2$. Dann gilt $H \trianglelefteq G$.*

Beweis. Sei $g \in G \setminus H$. Nach Annahme ist $G/H = \{1H, gH\}$ und $N\backslash G = \{H1, Hg\}$. Da $1H = H = H1$, muss gelten $gH = Hg$. Falls $g \in H$ gilt $gH = H = Hg$ ohnehin, also $H \trianglelefteq G$. □

Korollar 1.4.18. *Für jedes $n \in \mathbb{N}_{\geq 1}$ gilt $A_n \trianglelefteq S_n$.*

1.5 Zyklische Gruppen

Eine Gruppe G heißt *zyklisch* falls $G = \langle g \rangle$ für ein $g \in G$. Äquivalent dazu ist, dass es einen surjektiven Gruppenhomomorphismus $\mathbb{Z} \to G$ gibt (siehe Bemerkung 1.3.2).

Beispiel 1.5.1. $\mathbb{Z} = \langle 1 \rangle$ ist zyklisch und abzählbar unendlich, und wird die *freie zyklische Gruppe* genannt. Die Gruppe $\mathbb{Z}/n\mathbb{Z}$ (Beispiel 1.4.11) ist zyklisch und hat Ordnung n. Die Permutationsgruppe $C_n := \langle (1, \ldots, n) \rangle$ ist ebenfalls zyklisch und von Ordnung n. △

Die Kleinsche Vierergruppe ist die kleinste Gruppe, die nicht zyklisch ist.

Übung 24. Zeigen Sie:

- alle Gruppen der Ordnung höchstens 3 sind zyklisch;
- die Kleinsche Vierergruppe (Übung 9) ist nicht zyklisch;
- alle anderen Gruppen der Ordnung vier sind nicht nicht-zyklisch.

Im Wesentlichen haben wir mit den Gruppen in Beispiel 1.5.1 bereits alle zyklischen Gruppen kennengelernt. Um das zu beweisen, zeigen wir zunächst das folgende Lemma.

Lemma 1.5.2. *Jede Untergruppe H von $\mathbb{Z}$ ist gleich $m\mathbb{Z}$ für ein $m \in \mathbb{N}$.*

Beweis. Falls $H = \{0\} = 0\mathbb{Z}$ so ist nichts zu zeigen. Ansonsten enthält H ein positives Element m; wir wählen so ein m kleinstmöglich. Dann gilt $m\mathbb{Z} \subseteq H$. Sei umgekehrt $a \in H$. Durch Division von a durch m mit Rest erhalten wir $a = mq + r$ für $q, r \in \mathbb{Z}$ so dass $0 \leq r < m$. Dann ist $r = a - mq \in H$. Da $r < m$ und m das kleinste positive Element von H ist, gilt $r = 0$. Also gilt $a = mq \in m\mathbb{Z}$ und damit $H \subseteq m\mathbb{Z}$. Daher $H = m\mathbb{Z}$. □

Proposition 1.5.3. *Sei G eine zyklische Gruppe. Dann ist G isomorph zu $\mathbb{Z}$, falls* $\mathrm{Ord}(G) = \infty$*, und zu $\mathbb{Z}/n\mathbb{Z}$, falls* $\mathrm{Ord}(G) = n < \infty$*.*

Beweis. Sei $\varphi\colon \mathbb{Z} \to G$ ein surjektiver Gruppenhomomorphismus. Wegen Korollar 1.4.13 ist G isomorph zu $\mathbb{Z}/\operatorname{Kern}(\varphi)$, also von der Gestalt $\mathbb{Z}/H$ für eine (normale) Untergruppe H von $\mathbb{Z}$. Nach Lemma 1.5.2 ist $H = m\mathbb{Z}$ für ein $m \in \mathbb{N}$, also ist G ist isomorph zu $\mathbb{Z}/m\mathbb{Z}$. Falls $m = 0$, dann ist $\mathbb{Z}/m\mathbb{Z} = \mathbb{Z}/\{0\}$ isomorph zu $\mathbb{Z}$. □

Bemerkung 1.5.4. Homomorphe Bilder zyklischer Gruppen sind zyklisch. Denn falls $\varphi\colon \mathbb{Z} \to G$ ein surjektiver Gruppenhomomorphismus ist, und $\psi\colon G \to H$ ein surjektiver Gruppenhomomorphismus ist, so ist $\psi \circ \varphi\colon \mathbb{Z} \to H$ surjektiver Gruppenhomomorphismus.

Bemerkung 1.5.5. Untergruppen zyklischer Gruppen sind zyklisch. Sei $\varphi\colon \mathbb{Z} \to G$ ein surjektiver Gruppenhomomorphismus und $H \leq G$. Dann ist $\varphi^{-1}(H)$ eine Untergruppe von $\mathbb{Z}$, also isomorph zu $m\mathbb{Z}$ nach Lemma 1.5.2. Also ist $x \mapsto \varphi(mx)$ ein surjektiver Gruppenhomomorphismus von $\mathbb{Z}$ nach H, und H ist zyklisch.

Korollar 1.5.6. *Sei G eine Gruppe mit Primzahlordnung. Dann ist $G = \langle a \rangle$ für jedes $a \in G \setminus \{1\}$, und $G \cong \mathbb{Z}/p\mathbb{Z}$.*

Beweis. Sei $a \in G \setminus \{1\}$. Nach Satz 1.3.11 teilt die Ordnung von $H := \langle a \rangle$ die Gruppenordnung p. Da H mit a und 1 mindestens zwei Elemente hat, gilt $|H| = p$. Damit ist $G = H$, und somit zyklisch. Die Aussage folgt nun aus Proposition 1.5.3. □

Lemma 1.5.7. *Ist G/Z zyklisch, so ist G abelsch.*

Beweis. Seien $g, h \in G$. Wähle $a \in G$ so, dass aZ ein Erzeuger ist von G/Z. Dann ist $gZ = (aZ)^m$ und $hZ = (aZ)^n$, für $n, m \in \mathbb{Z}$, also gibt es $b, c \in Z$ mit $g = a^m b$ und $h = a^n c$. Es folgt

$$gh = a^m b a^n c = a^{m+n} bc = a^n c a^m b = hg.$$ □

Lemma 1.5.8. *Jede zyklische Gruppe der Ordnung $n \in \mathbb{N}$ besitzt für jeden Teiler d von n (genau) eine Untergruppe der Ordnung d, nämlich $\langle a^{n/d} \rangle$.*

Übung 25. Für $m \in \mathbb{N}_{\geq 1}$ definiere $G_m := \{0, 1, \ldots, m-1\}$. Sei $\circ\colon (G_m)^2 \to G_m$ die durch $a \circ b := (a + b) \bmod m$ definierte Operation (also der Rest bei der Division von $a + b$ durch m). Zeigen Sie: $(G_m, \circ)$ ist isomorph zu $\mathbb{Z}/m\mathbb{Z}$.

Übung 26. Bestimmen Sie die Untergruppen von $\mathbb{Z}/m\mathbb{Z}$ für $m \in \mathbb{N} \setminus \{0\}$.

Übung 27. Für welche n ist A_n zyklisch? Für welche n ist A_n abelsch?

Übung 28. Zeigen Sie die folgenden Aussagen: $\mathbb{Z} \trianglelefteq \mathbb{Q}$. Jedes Element von $\mathbb{Q}/\mathbb{Z}$ hat endliche Ordnung. Für jedes $n \in \mathbb{N}_{\geq 1}$ besitzt $\mathbb{Q}/\mathbb{Z}$ genau eine Untergruppe der Ordnung n, und diese ist zyklisch.

Übung 29. Sei $\underline{G}$ eine zyklische Gruppe und $z \in \mathbb{Z}$. Zeigen Sie: $g \mapsto g^z$ (siehe Definition 1.2.5) ist ein Gruppenhomomorphismus von $\underline{G}$ nach $\underline{G}$.

1.6 Direkte Produkte

Das *direkte Produkt* von Gruppen $G_1, \dots, G_n$ ist die Gruppe mit Grundmenge $G_1 \times \cdots \times G_n$ (das kartesische Produkt) und *komponentenweiser* Multiplikation

$$(g_1, \dots, g_n) \cdot (h_1, \dots, h_n) := (g_1 h_1, \dots, g_n h_n).$$

Falls $G_1 = \cdots = G_n$, so schreiben wir auch G^n für $G_1 \times \cdots \times G_n$. In additiver Notation spricht man von der *direkten Summe* und schreibt $G_1 \oplus \cdots \oplus G_n$.

Bemerkung 1.6.1. Für jedes $j \in I$ ist die durch $(a_i)_{i \in I} \mapsto a_j$ gegebene Abbildung $\pi_j \colon \prod_{i \in I} G_i \to G_j$ ein Gruppenhomomorphismus.

Beispiel 1.6.2. Die Kleinsche Vierergruppe (Übung 9) ist isomorph zu $(\mathbb{Z}/2\mathbb{Z})^2$. △

Definition 1.6.3 (internes direktes Produkt)**.** Seien $H_1, \dots, H_n \leq G$. Dann ist G das *interne* (oder *innere*) *direkte Produkt* von $H_1, \dots, H_n$ falls die Abbildung $H_1 \times \cdots \times H_n \to G$ mit $(h_1, \dots, h_n) \mapsto h_1 \cdots h_n$ ein Gruppenisomorphismus ist.

Im Gegensatz dazu nennt man $H_1 \times \cdots \times H_n$ das *äußere* direkte Produkt von $H_1, \dots, H_n$. Üblicherweise identifiziert man die Elemente eines inneren Produktes G von $H_1, \dots, H_n$ mit $H_1 \times \cdots \times H_n$ entlang des Isomorphismus aus Definition 1.6.3. Das bedeutet für $n = 2$, dass $a \in H_1 \subseteq G$ mit $(a, 1) \in G$ identifiziert wird, $b \in H_2 \subseteq G$ mit $(1, b) \in H_2$ identifiziert wird, und $ab \in G$ mit $(a, b) \in G$ identifiziert wird.

Bevor wir den Zusammenhang zwischen inneren und äußeren direkten Produkten klären, beweisen wir das folgende fundamentale Lemma zu Normalteilern.

Lemma 1.6.4. *Seien $U, V \trianglelefteq G$ mit $U \cap V = \{1\}$. Dann gilt $uv = vu$ für alle $u \in U$ und $v \in V$.*

Beweis. Es gilt

$$U \ni u(\underbrace{vu^{-1}v^{-1}}_{\in U}) = (\underbrace{uvu^{-1}}_{\in V})v^{-1} \in V$$

und da $U \cap V = \{1\}$ gilt $uvu^{-1}v^{-1} = 1$, also $vu = uv$. □

Proposition 1.6.5. *Es seien $U, V \leq G$. Dann sind äquivalent:*

1. *G ist das interne direkte Produkt von U und V;*
2. *$UV = G$, $U, V \trianglelefteq G$, und $U \cap V = \{1\}$.*

Beweis. (1) ⇒ (2): seien $\pi_1 \colon G \to U$ und $\pi_2 \colon G \to V$ die Projektionshomomorphismen aus Bemerkung 1.6.1. Dann ist $\mathrm{Kern}(\pi_1) = V$ und $\mathrm{Kern}(\pi_2) = U$, also $U, V \trianglelefteq G$. Offensichtlicherweise gilt $U \cap V = \{1\}$ und $UV = G$.

(2) $\Rightarrow$ (1): Die Abbildung $\varphi\colon U \times V \to G$, die durch $(u, v) \mapsto uv$ gegeben ist, ist ein Homomorphismus, da

$$\begin{aligned}\varphi((u,v)\cdot(u',v')) &= uu'vv' \\ &= uvu'v' && \text{(Lemma 1.6.4)} \\ &= \varphi(u,v)\cdot\varphi(u',v').\end{aligned}$$

Ausserdem ist φ surjektiv, da $UV = G$, und somit ein Gruppenisomorphismus. □

Korollar 1.6.6. *Seien $H_1, \dots, H_n \leq G$. Dann sind äquivalent:*

- *G ist das interne direkte Produkt von $H_1, \dots, H_n$,*
- *$G = H_1 \cdots H_n$ und für alle $i \in \{1, \dots, n\}$ gilt $H_i \trianglelefteq G$ und $H_1 \cdots H_{i-1} \cap H_i = \{1\}$.*

Beweis. Der Beweis geht einfach mit Hilfe von vollständiger Induktion nach n und Proposition 1.6.5. □

Die folgende Aussage liegt dem chinesischen Restsatz zu Grunde.

Proposition 1.6.7. *Seien $a, b \in \mathbb{N}$ teilerfremd. Dann ist $(\mathbb{Z}/ab\mathbb{Z}, +)$ isomorph zu $\mathbb{Z}/a\mathbb{Z} \oplus \mathbb{Z}/b\mathbb{Z}$.*

Beweis. Die Abbildung $\varphi\colon \mathbb{Z} \to \mathbb{Z}/a\mathbb{Z} \oplus \mathbb{Z}/b\mathbb{Z}$ mit $z \mapsto (z + a\mathbb{Z}, z + b\mathbb{Z})$ ist surjektiv und erfüllt

$$\ker(\varphi) = \{z \in \mathbb{Z} \mid (a|z) \text{ und } (a|z)\} = \{z \in \mathbb{Z} \mid (ab|z)\} = ab\mathbb{Z}.$$

Nach Korollar 1.4.13 ist also $\text{Bild}(\varphi) = \mathbb{Z}/a\mathbb{Z} \oplus \mathbb{Z}/b\mathbb{Z}$ isomorph zu $\mathbb{Z}/\ker(\varphi) = \mathbb{Z}/ab\mathbb{Z}$. □

Korollar 1.6.8. *Jede endliche zyklische Gruppe ist direktes Produkt von zyklischen Gruppen von Primzahlpotenzordnung.*

Übung 30. Es seien $m, n \in \mathbb{N}_{\geq 1}$. Zeigen Sie die Umkehrung von Proposition 1.6.7, nämlich dass m und n teilerfremd sind, falls $\mathbb{Z}/mn\mathbb{Z}$ und $\mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$ isomorph sind.

Übung 31. Sei $U \leq G$ und $N \trianglelefteq G$ so, dass $G = UN$ und $U \cap N = \{1\}$. Zeigen Sie, dass jedes Element von G auf genau eine Weise in der Form uv mit $u \in U$ und $v \in N$ darstellt werden kann, und dass G/N zu U isomorph ist. Man nennt G das *semidirekte Produkt* von U mit N.

1.7 Abelsche Gruppen

In diesem Kapitel werden wir einen Satz aus der Vorlesung LA20 verwenden, um die endlich erzeugten abelschen Gruppen zu klassifizieren. Wir benötigen zunächst das folgende Lemma.

Lemma 1.7.1. *Jede Untergruppe von $\mathbb{Z}^k$, für $k \in \mathbb{N}$, wird von k Elementen erzeugt.*

Beweis. Wir zeigen die Aussage mit Hilfe von vollständiger Induktion nach k. Die Aussage ist trivial für $k = 0$. Sei nun $U \leq \mathbb{Z}^k$ für $k > 0$. Wir betrachten den Homomorphismus $\pi\colon U \to \mathbb{Z}$, der durch die Projektion $\pi(x_1, \ldots, x_k) := x_k$ gegeben ist (siehe Bemerkung 1.6.1). Es ist $\mathrm{Bild}(\pi) \leq \mathbb{Z}$ (siehe Bemerkung 1.2.2) und $\ker(\pi) \leq \mathbb{Z}^k$ ist von der Gestalt $\mathbb{Z}^{k-1} \times \{0\}$. Nach Lemma 1.5.2 ist $\pi(U) \leq \mathbb{Z}$ von der Gestalt $m\mathbb{Z} = \langle m \rangle$. Die Abbildung $\pi'(x_1, \ldots, x_k) \mapsto (x_1, \ldots, x_{k-1})$ ist ein Homomorphismus von $\mathrm{Kern}(\pi) \leq U$ nach $\mathbb{Z}^{k-1}$, also ist $\mathrm{Bild}(\pi') \leq \mathbb{Z}^{k-1}$ nach Induktionsvoraussetzung von der Gestalt $\langle \{h'_1, \ldots, h'_{k-1}\} \rangle \subseteq \mathbb{Z}^{k-1}$. Wählen $h_1, \ldots, h_{k-1}, h_k \in U$ so, dass $\pi(h_k) = m$ und $\pi'(h_i) = h'_i$ für alle $i \in \{1, \ldots, k-1\}$. Es genügt, folgendes zu zeigen.

Behauptung. $\langle h_1, \ldots, h_{k-1}, h_k \rangle = U$. Sei $u \in U$ beliebig. Sei $z \in \mathbb{Z}$ so, dass $\pi(u) = mz$. Dann gilt

$$\pi(u) = mz = z\pi(h_k) = \pi(zh_k).$$

Die letzte Gleichheit ist die additive Schreibweise von $\pi(g^z) = \pi(g)^z$ (Übung 13). Also gilt $\pi(u - zh_k) = 0$ und $u - zh_k \in \mathrm{Kern}(\pi)$. Daher gibt es $z_1, \ldots, z_{k-1}$, so dass $u - zh_k = z_1h_1 + \cdots + z_{k-1}h_{k-1}$. Somit liegt u in $\langle h_1, \ldots, h_{k-1}, h_k \rangle$. □

Beim Beweis des folgenden Satzes verwenden wir die Smith Normalform aus der Vorlesung LA20.

Satz 1.7.2 (Hauptsatz der endlich erzeugten abelschen Gruppen (Poincaré))**.** *Sei G eine endlich erzeugte abelsche Gruppe. Dann gibt es eindeutig bestimmte $s, t \in \mathbb{N}$ und positive ganze Zahlen $r_1, \ldots, r_s$ mit $r_i | r_j$ für alle $i, j \in \{1, \ldots, s\}$, $i < j$, so dass G isomorph ist zu*

$$\mathbb{Z}/r_1\mathbb{Z} \oplus \cdots \oplus \mathbb{Z}/r_s\mathbb{Z} \oplus \mathbb{Z}^t.$$

Beweis. Die Gruppe G wird durch $z \cdot g := zg$ (additive Schreibweise von Definition 1.2.5) ein $\mathbb{Z}$-Modul definiert (siehe Vorlesung LA20[3]). Seien $g_1, \ldots, g_k \in G$ so, dass

$$G = \langle g_1, \ldots, g_k \rangle.$$

Sei $\varphi\colon \mathbb{Z}^k \to G$ definiert durch $(x_1, \ldots, x_k) \mapsto x_1g_1 + \cdots + x_kg_k$. Man rechnet leicht nach, dass φ ein surjektiver $\mathbb{Z}$-Modul-Homomorphismus ist, und damit insbesondere ein surjektiver Gruppenhomomorphismus von $\mathbb{Z}^k$ nach G. Korollar 1.4.13 besagt nun, dass $\mathbb{Z}^k / \mathrm{Kern}(\varphi) \cong G$.

Nach Lemma 1.7.1 ist $\mathrm{Kern}(\varphi) \leq \mathbb{Z}^k$ von der Gestalt $\mathrm{Kern}(\varphi) = \langle h_1, \ldots, h_k \rangle$ für $h_1, \ldots, h_k \in \mathbb{Z}^k$. Es sei $A = (h_1 \ \ldots \ h_k)$ die quadratische Matrix mit Spaltenvektoren $h_1, \ldots, h_k$. Nach dem Satz aus LA20 zur Smith Normalform gibt es unimodulare[4] Matrizen $U, V \in \mathbb{Z}^{k \times k}$ so, dass $A = UDV$ mit $D = (d_{i,i})_{i \in \{1,\ldots,k\}} \in \mathbb{Z}^{k \times k}$ eine Diagonalmatrix mit $d_{i,i} \neq 0$ für alle $i \in \{1, \ldots, s\}$, $d_{i,i} = 0$ für alle $i \in \{s+1, \ldots, k\}$, und $d_{i,i} | d_{j,j}$ für alle $i, j \in \{1, \ldots, s\}$ (und D heißt dann die *Smith Normalform* von A). Seien

- $r_i := d_{i,i}$ für $i \in \{1, \ldots, s\}$,

[3] Zur Wiederholung: Moduln spielen für Ringe die gleiche Rolle wie Vektorräume für Körper.
[4] Zur Wiederholung: $U \in \mathbb{Z}^{k \times k}$ ist unimodular, falls $\det(U) \in \{+1, -1\}$; siehe LA20.

- $t := k - s$.

Dann ist

$$G \cong \mathbb{Z}^k / \operatorname{Kern}(\varphi) = \mathbb{Z}^k/(A\,\mathbb{Z}^k) = \mathbb{Z}^k/(UDV\,\mathbb{Z}^k) = \mathbb{Z}^k/(D\mathbb{Z}^k)$$
$$= \mathbb{Z}^k/(r_1\mathbb{Z} \oplus \cdots \oplus r_s\mathbb{Z}) = \mathbb{Z}/r_1\mathbb{Z} \oplus \cdots \oplus \mathbb{Z}/r_s\mathbb{Z} \oplus \mathbb{Z}^t. \qquad \square$$

Korollar 1.7.3. *Jede endliche abelsche Gruppe ist direktes Produkt von zyklischen Gruppen von Primzahlpotenzordnung.*

Beweis. Direkt aus Satz 1.7.2 und Korollar 1.6.8. $\square$

Korollar 1.7.4. *Sei G eine endliche abelsche Gruppe und p ein Primteiler von $|G|$. Dann hat G ein Element der Ordnung p.*

Beweis. Nach Satz 1.7.2 gibt es $s \in \mathbb{N}$ und positive ganze Zahlen $r_1, \ldots, r_s$ mit $r_i | r_j$ für alle $i, j \in \{1, \ldots, s\}$, $i < j$, so dass G isomorph ist zu

$$\mathbb{Z}/r_1\mathbb{Z} \oplus \cdots \oplus \mathbb{Z}/r_s\mathbb{Z}.$$

Sei $g \in G$ der Erzeuger von $\mathbb{Z}/r_s\mathbb{Z}$. Dann hat $\frac{r_s}{p}g$ die Ordnung p in $\mathbb{Z}/r_s\mathbb{Z}$, und das Element von G, welches $(0, \ldots, 0, \frac{r_s}{p}g)$ entspricht, hat die Ordnung p in G.[5] $\square$

Korollar 1.7.5. *Sei $\underline{K}$ ein Körper und sei G eine endliche Untergruppe von $(K \setminus \{0\}, \cdot)$. Dann ist G zyklisch.*

Beweis. Wegen des Hauptsatzes über endlich erzeugte abelsche Gruppen ist G isomorph zu $\mathbb{Z}/r_1\mathbb{Z} \times \cdots \times \mathbb{Z}/r_s\mathbb{Z}$. Für jedes $g \in G$ gilt $g^{r_s} = 1$, komponentenweise gerechnet nach Satz 1.3.12, da $r_i | r_s$ für alle $i \in \{1, \ldots, s\}$. Jedes $g \in G$ ist daher eine Nullstelle des Polynoms $X^{r_s} - 1$. Dieses Polynom ist vom Grad r_s und hat daher über K höchstens r_s Nullstellen. Da $|G| = r_1 \cdots r_s$, gilt also $r_1 \cdots r_s \leq r_s$, und somit $r_1 = \cdots = r_{s-1} = 1$, da $r_1 | r_s, \ldots, r_{s-1} | r_s$. Folglich ist G isomorph zu $(\mathbb{Z}_{r_s}, +)$ und somit zyklisch. $\square$

Insbesondere folgt der sogenannte Primitivwurzelsatz von Gauss: für jede Primzahl p ist $(\mathbb{Z}/p\mathbb{Z})^\times$ zyklisch.

Übung 32. Finden sie ein $n \in \mathbb{N}$, so dass $\mathbb{Z}/n\mathbb{Z}$ nicht zyklisch ist.

Übung 33. Wie viele abelsche Gruppen mit 2024 Elementen gibt es?

1.8 Gruppenwirkungen

Nach dem Satz von Cayley (Proposition 1.2.6) ist jede Gruppe G isomorph zu einer Permutationsgruppe. Im Beweis haben wir einen injektiven Homomorphismus von G nach $\operatorname{Sym}(G)$ angegeben. Diese Methode werden wir nun verallgemeinern.

[5] Alternativ kann das Korollar auch mit Hilfe von Lemma 1.5.8 bewiesen werden.

Definition 1.8.1. Eine *Wirkung*[6] einer Gruppe G auf einer Menge X ist eine Abbildung

$$G \times X \to X, \quad (g, x) \mapsto g \cdot x$$

so dass für alle $x \in X$ und $g, h \in G$ gilt

- $g \cdot (h \cdot x) = (gh) \cdot x$, und
- $1 \cdot x = x$.

Eine *G-Menge* ist eine Menge X zusammen mit einer Wirkung von G auf X. In diesem Fall schreibt man auch häufig $G \curvearrowright X$.

Beispiel 1.8.2. Ist K ein Körper, so wirkt $G = K^\times$ auf $X := K$ durch $y \cdot x := yx$ für $x \in K$ und $y \in K^\times$. △

Beispiel 1.8.3. Ist K ein Körper, so wirkt $G = \mathrm{GL}_n(K)$ auf K^n durch $A \cdot x := Ax$ für $x \in K^n$ und $A \in \mathrm{GL}_n(K)$. △

Beispiel 1.8.4. Jede Gruppe G wirkt auf $X := G$ durch Multiplikation von links (Linkstranslation): $g \cdot x := gx$ für $x \in X$ und $g \in G$ (analog für rechts). △

Beispiel 1.8.5. Jede Gruppe G wirkt auf $X := G$ durch *Konjugation*: $g \cdot x := gxg^{-1}$ für $x \in X$ und $g \in G$ (siehe Definition 1.2.7). △

Beispiel 1.8.6. Sei G eine Gruppe und $U \leq G$. Dann wirkt G auf den Linksnebenklassen G/U von U durch Multiplikation von links: $g \cdot hU := (gh)U$ für $g, h \in G$. △

Beispiel 1.8.7. Jede Gruppe wirkt auf der Menge $\mathrm{Sub}(G)$ aller Untergruppen von G durch Konjugation: $g \cdot H := \{ghg^{-1} \mid h \in H\}$ für $H \leq G$ und $g \in G$. △

Beispiel 1.8.8. Die symmetrische Gruppe $\mathrm{Sym}(X)$ wirkt auf X durch $\sigma \cdot x := g(x)$ für $x \in X$ und $\sigma \in \mathrm{Sym}(X)$. Analog wirkt die Automorphismengruppe eines Graphen (V, E) auf V (siehe Beispiel 1.1.5), und die Automorphismengruppe einer Gruppe G auf G (siehe Beispiel 1.2.4). △

Bemerkung 1.8.9. Für jede Wirkungen von G auf X ist die Abbildung $\sigma\colon G \to \mathrm{Sym}(X)$, die gegeben ist durch $\sigma(g)(x) := g \cdot x$ für $x \in X$ und $g \in G$, ein Homomorphismus von G nach $\mathrm{Sym}(X)$. Umgekehrt entspricht jedes $\sigma \in \mathrm{Hom}(G, \mathrm{Sym}(X))$ einer Gruppenwirkung von G auf X. Das Bild von σ ist eine Permutationsgruppe. Wir werden daher im folgenden Terminologie für Gruppenwirkungen stets auch für Permutationsgruppen verwenden, und uns dabei implizit auf diese Wirkung beziehen.

Definition 1.8.10. Eine Gruppenwirkung heißt *treu*, wenn der in Bemerkung 1.8.9 beschriebene Gruppenhomomorphismus von G nach $\mathrm{Sym}(X)$ injektiv ist.

Definition 1.8.11. Seien X eine G-Menge und $x \in X$. Die *Bahn* (oder der *Orbit*) *von x unter G* ist die Menge $G \cdot x := \{g \cdot x \mid g \in G\}$.

[6] Manche Autor:innen verwenden auch den Namen '(Gruppen-) Aktion' (vom Englischen 'group action') oder 'Gruppenoperation' anstatt 'Wirkung'.

Bemerkung 1.8.12. Zwei Bahnen von G sind entweder disjunkt oder gleich. Die Bahnen von G definieren daher eine Partition auf X.

Eine Wirkung heißt *transitiv*, wenn sie nur eine Bahn besitzt. Falls die Bahn von x nur ein Element besitzt, so nennt man x auch einen *Fixpunkt von* G. Die Menge aller Fixpunkte von G wird mit $\mathrm{Fix}_X(G)$ bezeichnet.

Übung 34. Bestimmen Sie die Fixpunkte der Automorphismengruppe des in Beispiel 1.8.8 abgebildeten Graphen.

Definition 1.8.13. Seien X eine G-Menge und $x \in X$. Dann ist der *Stabilisator von x in G* die Untergruppe $G_x := \{g \in G \mid g \cdot x = x\} \leq G$.

Übung 35. Zeigen Sie, dass $(S_n)_1$ (siehe Beispiel 1.0.3 und 1.8.8) isomorph ist zu S_{n-1}.

Lemma 1.8.14. *Sei X eine G-Menge und σ der Gruppenhomomorphismus $G \to \mathrm{Sym}(X)$ aus Bermerkung 1.8.9. Dann ist $\ker(\sigma) = \bigcap_{x\in X} G_x$. Insbesondere ist die Wirkung von G auf X genau dann treu, wenn $\bigcap_{x\in X} G_x = \{1\}$.*

Beweis. Es ist $g \in \bigcap_{x\in X} G_x$ genau dann, wenn $\sigma(g) = \mathrm{id}_X$, was wiederum genau dann der Fall ist, wenn $g \in \mathrm{Kern}(\sigma)$. □

Definition 1.8.15. Eine Wirkung von G auf X heißt *frei*, wenn $G_x = \{1\}$ für alle $x \in X$.

Beispiel 1.8.16. Die Wirkung von G auf G durch Multiplikation von links aus Beispiel 1.8.4 ist transitiv, frei, und treu. △

Beispiel 1.8.17. Die Wirkung von $\mathrm{Sym}(X)$ auf X aus Beispiel 1.8.8 ist transitiv und treu, aber für $|X| \geq 3$ nicht frei. △

Proposition 1.8.18 (Bahn-Stabilisator-Satz[7])**.** *Sei X eine G-Menge und $x \in X$. Dann gilt*

$$|Gx| = (G : G_x).$$

Beweis. Die durch $gG_x \mapsto g\cdot x$ gegebene Abbildung von G/G_x nach Gx ist wohldefiniert: denn wenn $gG_x = hG_x$, dann ist $h^{-1}g \in G_x$, also $h^{-1}g \cdot x = x$, also dann ist $g \cdot x = h \cdot x$. Weiterhin ist die Abbildung eine Bijektion. Die Surjektivität ist offensichtlich. Um die Injektivität nachzuweisen, nehmen wir an, dass $g \cdot x = h \cdot x$. Dann folgt dass $h^{-1}g \cdot x = x$, also $h^{-1}g \in G_x$ und daher $gG_x = hG_x$. □

Korollar 1.8.19 (Bahn-Zerlegungsformel[8])**.** *Ist X eine G-Menge und sei $\{x_1, \ldots, x_n\} \subseteq X$ ein Repräsentantensystem[9] der Bahnen unter G,*

$$|X| = \sum_{i\in\{1,\ldots,n\}} (G : G_{x_i}).$$

[7] Manche Autor:innen nennen diese Aussage auch die *Bahngleichung*.

[8] Manche Autor:innen nennen diese Aussage auch die *Bahnengleichung*.

[9] Ein *Repräsentantensystem* einer Partition $\mathcal{P}$ einer Menge X ist eine Menge $R \subseteq X$, so dass aus jeder Partitionsklasse $P \in \mathcal{P}$ genau ein Element $x \in P$ in R enthalten ist.

Im folgenden wichtig wird die Anwendung der Bahn-Zerlegungsformel auf die Konjugationswirkung von G auf G (Beispiel 1.8.5).

- Die Bahnen dieser Wirkung werden dann auch *Konjugationsklassen* von G genannt.
- Die Fixpunkte $x \in G$ dieser Wirkung sind wegen $axa^{-1} = x \iff ax = xa$ genau die Elemente des Zentrums $Z(G) = \{a \in G \mid ax = xa \text{ für alle } x \in G\}$ (Bemerkung 1.2.9).
- Der Stabilisator $G_x = \{a \in G \mid axa^{-1} = x\}$ ist gleich dem *Zentralisator* $Z_G(x) := \{a \in G \mid ax = xa\}$.

Korollar 1.8.20 (Klassengleichung)**.** *Sei G endlich mit Zentrum Z und sei $R \subseteq G$ ein Repräsentantensystem der Konjugationsklassen von G. Dann gilt*

$$|G| = \sum_{r \in R} G : Z_G(r) = |Z(G)| + \sum_{r \in R \setminus Z(G)} (G : Z_G(r)). \tag{1.4}$$

Beweis. Die Bahn-Zerlegungsformel (Korollar 1.8.19) liefert

$$|G| = \sum_{r \in R} G : G_r = \sum_{r \in R} G : Z_G(r).$$

Die Elemente $r \in Z(G)$ sind gerade die Fixpunkte der Konjugationswirkung, liegen also alle in paarweise verschiedenen Bahnen. Also gibt es genau $|Z(G)|$ Repräsentanten aus R, die in $Z(G)$ liegen. Falls $r \in Z(G)$, dann ist $Z_G(r) = G_r = G$, also $G : Z_G(r) = 1$. Also gilt $\sum_{r \in Z(G)} G : Z_G(r) = |Z(G)|$, und damit folgt (1.4). □

Übung 36. Zeigen Sie, dass der Zentralisator $Z_G(g)$ von g in G die größte Untergruppe $H \leq G$ mit $g \in Z(H)$ ist.

Übung 37. Sei X eine G-Menge. Dann heißt x ein *Fixpunkt von* $g \in G$ falls $g \cdot x = x$, und die Menge aller Fixpunkte von g wird mit $\mathrm{Fix}_X(g)$ bezeichnet. Das folgende Lemma ist wichtig in der Kombinatorik: es besagt, dass die Anzahl von Bahnen von G gleich der durchschnittlichen Anzahl von Fixpunkten der Gruppenelemente ist.

Lemma 1.8.21 (Lemma von Burnside[10]). *Sei X eine G-Menge und X/G die Menge der Bahnen von Elementen von X unter G. Dann gilt*

$$|X/G| = \frac{1}{|G|} \sum_{g \in G} \mathrm{Fix}_X(g).$$

Beweisen Sie dieses Lemma. Hinweise:

- Seien $B \subseteq X$ eine Bahn von G. Zeigen Sie: $\sum_{x \in B} |G_x| = \sum_{x \in B} \frac{|G|}{|B|} = |G|$.

[10] Das Lemma war bereits Frobenius bekannt.

- Betrachten Sie einen Graphen (siehe Beispiel 1.1.5) mit Knotenmenge $G \cup X$ mit einer Kante zwischen $g \in G$ und $x \in X$ falls $g \cdot x = x$. Zählen Sie dann die Kanten des Graphen auf zwei verschiedene Weisen.

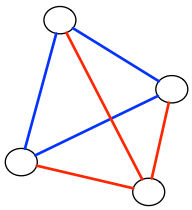
Übung 38. Wie viele Graphen mit drei Knoten gibt es, bis auf Isomorphie?

Hinweise.

- Betrachten sie die Wirkung von S_3 auf den zweielementigen Teilmengen von $\{1, 2, 3\}$, die gegeben ist durch $g \cdot \{a, b\} := \{g(a), g(b)\}$. Zeigen Sie: die gesuchte Zahl ist gleich der Anzahl der Bahnen dieser Wirkung.
- Verwenden Sie das Lemma von Burnside, um diese Zahl zu berechnen.

Übung 39. Auf wie viele Weisen können die Kanten des gleichseitigen Tetraeders T mit zwei Farben gefärbt werden, bis auf Rotationssymmetrien?

Hinweise.



- Geben Sie die Symmetrien von T mit Hilfe einer Permutationsgruppe auf der Menge der Kanten an. Wie viele Permutationen hat diese Gruppe?
- Zeigen Sie: die gesuchte Zahl ist gleich der Anzahl der Bahnen dieser Permutationsgruppe.
- Verwenden Sie das Lemma von Burnside, um diese Zahl zu berechnen.

1.9 p-Gruppen

Es sei p eine Primzahl. Eine endliche Gruppe G heißt *p-Gruppe*, falls die Ordnung von G eine Potenz von p ist, d.h., $|G| = p^k$ für ein $k \in \mathbb{N}$.

Beispiel 1.9.1. Eine zyklische Gruppe ist genau dann eine p-Gruppe, wenn sie von der Gestalt $\mathbb{Z}/p^k\mathbb{Z}$ ist; dies kann aus Proposition 1.5.3 abgelesen werden. △

Aufgrund des Satzes von Lagrange sind alle Untergruppen von p-Gruppen selbst wiederum p-Gruppen.

Lemma 1.9.2. *Sei G eine p-Gruppe der Ordnung p^k für $k \geq 1$. Dann teilt p die Ordnung des Zentrums von G; insbesondere gilt $|Z(G)| > 1$.*

Beweis. Jeder Index $(G : Z_G(r))$ in der Klassengleichung (1.4) ist für $r \in R \setminus Z(S)$ größer als 1, und daher als Teiler von $|G| = p^k$ durch p teilbar. Also sind die linke Seite und die Summe $\sum_{r \in R \setminus Z(G)} (G : Z_G(r))$ auf der rechten Seite durch p teilbar, und damit auch deren Differenz $|Z(G)|$. □

Lemma 1.9.2 erlaubt uns folgende informative Beschreibung der endlichen p-Gruppen (mehr dazu in Abschnitt 1.13).

Korollar 1.9.3. *Sei G eine p-Gruppe der Ordnung p^k. Dann gibt es Untergruppen $G_0, G_1, \dots, G_k$ von G mit $|G_i| = p^i$ und*

$$\{1\} = G_0 \trianglelefteq G_1 \trianglelefteq \cdots \trianglelefteq G_k = G.$$

Beweis. Per Induktion nach k. Der Fall $k = 0$ ist trivial. Für $k \geq 1$ ist $|Z(G)| > 1$ nach Lemma 1.9.2, Nach Korollar 1.7.4 finden wir ein Element $a \in Z(G)$ der Ordnung p. Da $a \in Z(G)$, gilt $\langle a \rangle \trianglelefteq G$, und nach dem Satz von Lagrange (Satz 1.3.11) ist $|G/\langle a \rangle| = p^{k-1}$.

Wir können also die Induktionsvoraussetzung auf $G/\langle a \rangle$ anwenden, und erhalten Untergruppen $H_0, H_1, \dots, H_k$ mit $|H_i| = p^i$ von $G/\langle a \rangle$ so dass

$$\{1\} = H_0 \trianglelefteq H_1 \trianglelefteq \cdots \trianglelefteq H_{k-1} = G/\langle a \rangle.$$

Für die kanonische Projektion $\pi \colon G \to G/\langle a \rangle$ definieren wir $G_{i+1} := \pi^{-1}(H_i)$. Dann gilt $|G_{i+1}| = p^{i+1}$ und

$$\{1\} := G_0 \trianglelefteq G_1 \trianglelefteq \cdots \trianglelefteq G_k.$$ □

Eine weitere Anwendung von Lemma 1.9.2 ist der folgende Nachweis, dass alle Gruppen der Ordnung p^2 abelsch sind.

Proposition 1.9.4. *Sei G eine Gruppe der Ordnung $|G| = p^2$. Dann ist G abelsch.*

Beweis. Nach Lemma 1.9.2 ist $|Z(G)| > 1$, also hat $G/Z(G)$ nach dem Satz von Lagrange die Ordnung 1 oder p. In beiden Fällen ist $G/Z(G)$ zyklisch (Korollar 1.5.6) und daher ist G nach Lemma 1.5.7 abelsch. □

Die folgende Aussage folgt aus aus Proposition 1.9.4 mit Hilfe des Hauptsatzes der endlich erzeugten abelschen Gruppen (Satz 1.7.2). Endliche abelsche Gruppen können auch mit Hilfe von p-Gruppen klassifiziert werden; für diesem alternativen Zugang ist es wichtig, die folgende Aussage auch ohne den Hauptsatz zu beweisen, was wir im folgenden tun werden.

Korollar 1.9.5. *Jede Gruppe der Ordnung p^2 ist isomorph zu $\mathbb{Z}_{p^2}$ oder zu $\mathbb{Z}_p \times \mathbb{Z}_p$*

Beweis. Wähle $z \in G \setminus \{1\}$. Falls $\langle z \rangle = G$, dann ist G isomorph zu $\mathbb{Z}_{p^2}$. Ansonsten ist $|\langle z \rangle| = p$ nach dem Satz von Lagrange. Wir können dann $a \in G \setminus \langle z \rangle$ wählen. Dann gelten:

- $|\langle z \rangle| = G$ und $|\langle a \rangle| = p$ nach dem Satz von Lagrange, da $z, a \neq 1$ und $\langle z \rangle, \langle a \rangle < G$. Daher $\langle a \rangle \cong \langle z \rangle \cong \mathbb{Z}/p\mathbb{Z}$ nach Korollar 1.5.6.
- $\langle a \rangle \cap \langle z \rangle = \{1\}$: denn falls es ein $b \in (\langle a \rangle \cap \langle z \rangle) \setminus \{1\}$ gäbe, dann wäre $\langle b \rangle = \langle a \rangle$ (Korollar 1.5.6), und damit wäre $a \in \langle z \rangle$, im Widerspruch zur Annahme.

Da G nach Proposition 1.9.4 abelsch ist, gilt $\langle z \rangle \langle a \rangle = \langle a \rangle \langle z \rangle$, und daher $\langle a \rangle \langle z \rangle \leq G$ nach Übung 20. Also ist $|\langle a \rangle \langle z \rangle| = p^2 = |G|$. Da $\langle z \rangle \trianglelefteq G$ und $\langle a \rangle \trianglelefteq G$ (da G abelsch) folgt mit Proposition 1.6.5, dass $G \cong \mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z}$. □

1.10 Die Sylow-Sätze

Eine Untergruppe H einer endlichen Gruppe G heißt eine *p-Sylow-Untergruppe von G* falls H eine p-Gruppe ist und $|H|$ die größte Potenz von p ist, die $|G|$ teilt. Die Sylow-Sätze machen Aussagen über die Existenz und Anzahl von p-Sylow-Untergruppen einer endlichen Gruppe und sind Grundstein für die Theorie endlicher Gruppen.

Satz 1.10.1 (erster Satz von Sylow)**.** *Es sei G eine endliche Gruppe und p eine Primzahl, so dass $p^k | G$ für ein $k \in \mathbb{N}$. Dann besitzt G eine Untergruppe der Ordnung p^k. Insbesondere hat G eine p-Sylow-Untergruppe.*

Beweis. Per Induktion über $|G|$. Die Aussage ist für $|G| = 1$ trivial. Teilt p die Ordnung des Zentrums von G, so folgt aus Korollar 1.7.4, dass $Z(G)$ eine Untergruppe H der Ordnung p besitzt. Dann teilt p^{k-1} die Ordnung $(G : H)$ von G/H, die nach Induktionsvoraussetzung eine Untergruppe K der Ordnung p^{k-1} besitzt. Das Urbild von K unter der kanonischen Projektion $\pi\colon G \to G/H$ ist eine Untergruppe von G der Ordnung p^k.

Es bleibt also nur der Fall zu betrachten, dass p die Ordnung des Zentrums nicht teilt. Die Aussage ist trivial für $k = 0$; ansonsten teilt p die Ordnung von G. Wegen der Klassengleichung (1.4) gibt es ein $g \in G \setminus Z(G)$, so dass der Index $(G : Z_G(g))$ von p nicht geteilt wird. Nach dem Satz von Lagrange wird also $|Z_G(g)|$ von p^k geteilt. Da $g \notin Z(G)$, gilt $(G : Z_G(g)) > 1$, also $|Z_G(g)| < |G|$, und nach Induktionsvoraussetzung besitzt $Z_G(g) \leq G$ eine Untergruppe der Ordnung p^k. □

Korollar 1.10.2 (Satz von Cauchy)**.** *Sei G eine endliche Gruppe und p ein Primteiler von $|G|$. Dann besitzt G ein Element der Ordnung p.*

Beweis. Nach Satz 1.10.1 besitzt G eine Untergruppe U der Ordnung p. Nach Korollar 1.5.6 ist U zyklisch, besitzt also ein Element der Ordnung p. □

Lemma 1.10.3. *Es sei G eine endliche Gruppe, $H \leq G$ eine p-Gruppe, und S eine p-Sylow-Untergruppe von G. Dann existiert ein $g \in G$ mit $H \subseteq gSg^{-1}$.*

Beweis. Sei $|G| = p^k q$ so, dass p nicht q teilt. Dann gilt $|S| = p^k$ nach Satz 1.10.1, also $|G/S| = q$ nach dem Satz von Lagrange (Satz 1.3.11). Wir betrachten die Wirkung von H auf den Linksnebenklassen G/S von S, die gegeben ist durch

$$(h, gS) \mapsto (hg)S$$

(Linkstranslation, siehe Beispiel 1.8.6). Nach dem Bahn-Stabilisator-Satz (Proposition 1.8.18) gilt für jedes $g \in G$

$$|H \cdot (gS)| = (H : H_{gS}).$$

Da H eine p-Gruppe ist, folgt $|H \cdot (gS)| = p^\ell$ für ein $\ell \in \mathbb{N}$. Wir haben bereits gesehen, dass p kein Teiler von $|G/S|$ ist. Da G/S durch die Bahnen partioniert wird, muss für mindestens eine Bahn $H \cdot gS$ gelten, dass $|H \cdot (gS)| = p^0 = 1$. Das heißt, $hgS = gS$ für alle $h \in H$. Da $1 \in S$ gilt $hg \in gS$, also $h \in gSg^{-1}$ und damit $H \subseteq gSg^{-1}$. □

Zwei Untergruppen H und H' von G heißen *konjugiert* in G, falls es ein $g \in G$ gibt mit $gHg^{-1} = H'$ (eine Äquivalenzrelation).

Satz 1.10.4 (zweiter Satz von Sylow)**.** *Jede p-Gruppe $U \leq G$ ist in einer p-Sylow-Untergruppe enthalten. Alle p-Sylow-Untergruppen von G sind konjugiert zueinander.*

Beweis. Direkte Konsequenz von Lemma 1.10.3. □

Satz 1.10.5 (dritter Satz von Sylow)**.** *Sei G eine endliche Gruppe und p Primteiler von $|G|$. Die Anzahl der p-Sylow-Untergruppen teilt $|G|$ und ist kongruent zu 1 modulo p.*

Im Beweis von Satz 1.10.5 werden wir die Wirkung von G auf der Menge $\mathrm{Sub}(G)$ der Untergruppen von G betrachten (Beispiel 1.8.7). Für $H \leq G$ ist $G \cdot H$ dann die Konjugationsklasse von H. Der Stabilisator

$$G_H = \{a \in G \mid aHa^{-1} = H\} = \{a \in G \mid aH = Ha\} =: N_G(H)$$

wird auch der *Normalisator* von H in G genannt.[11]

Bemerkung 1.10.6. Sei G eine Gruppe und $X \subseteq G$. Dann ist $N_G(X)$ als Stabilisator der Konjugationswirkung insbesondere eine Untergruppe von G.

Das folgende Beispiel zeigt, dass der Normalisator von $H \subseteq G$ kein Normalteiler von G sein muss.

Beispiel 1.10.7. $N_{S_3}(\{(23)\}) \leq S_3$ ist kein Normalteiler von S_3. Denn $N_{S_3}(\{(23)\}) = \{(23), 1\}$, und $(12)(23)(12)^{-1} = (13)$. △

Bemerkung 1.10.8. Sei $U \leq G$. Dann gilt $U \trianglelefteq N_G(U)$. Denn für $a \in N_G(U) = \{a \in G \mid aU = Ua\}$ gilt $aU = Ua$ und somit $U \trianglelefteq N_G(U)$.

Übung 40. Sei $U \leq G$. Dann gilt genau dann $U \trianglelefteq G$, wenn $N_G(U) = G$.

Übung 41. Sei $U \trianglelefteq V \leq G$. Zeigen Sie: $V \subseteq N_G(U)$.

Beweis von Satz 1.10.5. Sei $\mathcal{S}_p$ die Menge aller p-Sylow-Untergruppen von G. Für $H \in \mathcal{S}_p$ ist auch $g \cdot H := gHg^{-1} \in \mathcal{S}_p$. Wir betrachten die Wirkung von G auf $\mathcal{S}_p$ durch Konjugation. Nach Satz 1.10.4 ist diese Wirkung transitiv, und nach Satz 1.10.1 ist $\mathcal{S}_p$ nicht leer, also gibt es ein $S \in \mathcal{S}_p$ und $G \cdot S = \mathcal{S}_p$. Wir wenden den Bahn-Stabilisator-Satz (Proposition (1.8.18)) an und erhalten, dass

$$|\mathcal{S}_p| = |G \cdot S| = (G : G_S). \tag{1.5}$$

Also ist $|\mathcal{S}_p|$ ein Teiler von $|G|$.

Wir betrachten nun die Wirkung von S auf $\mathcal{S}_p$ durch Konjugation. Sei $K \in \mathcal{S}_p$. Der Bahn-Stabilisator-Satz (Proposition (1.8.18)) angewandt auf $S \cdot K$ liefert $|S \cdot K| = (S : S_K)$, also ist $|S \cdot K|$ ein Teiler von $|S|$ und von der Gestalt p^ℓ für ein $\ell \in \mathbb{N}$. Es gilt $\ell = 0$ genau dann, wenn $K = S$: zum einen gilt $S \cdot S = \{S\}$. Zum anderen folgt aus

[11] Der Normalisator $N_G(H) = \{a \in G \mid aH = Ha\}$ ist für beliebige Mengen $H \subseteq G$ definiert, nicht bloß für Untergruppen H.

$1 = |S \cdot K| = (S : S_K)$, dass $S = S_K = N_S(K)$. Klarerweise gilt $N_S(K) \subseteq N_G(K)$ und $K \trianglelefteq N_G(K)$ (Bemerkung 1.10.8). Es sind also sowohl S als auch K p-Sylowgruppen in $N_G(K)$, und daher gibt es nach dem zweiten Satz von Sylow (Satz 1.10.4) ein $b \in N_G(K)$ mit $S = bKb^{-1}$. Da $K \trianglelefteq N_G(K)$ folgt $S = K$.

Daher hat die Bahnzerlegungsformel (Korollar 1.8.19) die Gestalt

$$|\mathcal{S}_p| = 1 + \sum_{i \in \{1,\dots,|\mathcal{S}_p/S|-1\}} p^{\ell_i}$$

für $\ell_1, \dots, \ell_s \geq 1$. Also ist $|\mathcal{S}_p|$ kongruent zu 1 modulo p. □

1.11 Einfache Gruppen

Eine Gruppe $G \neq \{1\}$ heißt *einfach*[12], wenn G und $\{1\}$ ihre einzigen Normalteiler sind. In anderen Worten: G ist einfach, wenn G keine nicht-trivialen echten Normalteiler besitzt (siehe Beispiel 1.4.4). Die einfachen Gruppen können als die 'Bausteine' der Gruppentheorie betrachtet werden. Das *Hölder-Programm*:

- Klassifiziere alle endlichen einfachen Gruppen.
- Beschreibe, wie sich beliebige endliche Gruppen aus einfachen zusammensetzen.

Beispiel 1.11.1. Jede Gruppe G mit Primzahlordnung ist offensichtlich einfach, denn $\{1\}$ und G sind die einzigen Untergruppen (Satz 1.3.11). △

Bemerkung 1.11.2. Tatsächlich sind die Gruppen der Gestalt $\mathbb{Z}/p\mathbb{Z}$ bis auf Isomorphie die einzigen einfachen zyklischen Gruppen: dies folgt aus der Klassifikation der zyklischen Gruppen 1.5.3 und Lemma 1.5.8.

Bemerkung 1.11.3. Auch eine endliche abelsche Gruppe ist genau dann einfach, wenn sie isomorph ist zu $\mathbb{Z}/p\mathbb{Z}$ für p prim: denn wenn G abelsch und einfach, folgt $\langle a \rangle = G$ für alle $a \in G \setminus \{1\}$, und die Aussage folgt aus der vorherigen Bemerkung.

Bemerkung 1.11.4. Auch eine p-Gruppe ist genau dann einfach, wenn sie isomorph ist zu $\mathbb{Z}/p\mathbb{Z}$ für p prim (folgt aus Lemma 1.9.2; folgt auch aus Korollar 1.9.3).

Übung 42. Zeigen Sie, dass A_3 einfach ist, aber S_3 und V_4 (Beispiel 9) nicht einfach sind.

Übung 43. Zeigen Sie, dass A_4 eine eindeutige Untergruppe der Ordnung 4 hat, welche nicht zyklisch und nicht einfach ist.

Übung 44. Bestimmen Sie die Normalteiler von S_4.

Satz 1.11.5 (Galois 1830)**.** *Für $n \geq 5$ ist A_n einfach.*

Beweis. Sei $N \trianglelefteq A_5$ mit $\sigma \in N \setminus \{1\}$. Zu zeigen ist, dass $N = A_5$.

[12] Englisch 'simple'.

Behauptung 1. A_n wird von 3-Zykeln erzeugt. Jede Permutation wird nach Beispiel 1.1.4 von Transpositionen erzeugt, und jedes Element von A_n ist ein Produkt von einer geraden Zahl von Transpositionen. Die Gleichungen

$$(12)\circ(23) = (123)$$
$$(12)\circ(34) = (12)\circ(23)\circ(23)\circ(34) = (123)\circ(234)$$

zeigen, dass jedes Element von A_n auch ein Produkt von 3-Zykeln ist.

Behauptung 2 (Cauchy 1815). Je zwei 3-Zykeln sind in A_n konjugiert: seien $\pi_1 = (123) \in A_n$ und $\pi_2 = (ijk) \in A_n$. Sei $\rho \in S_n$ so, dass $\rho(1) = i$, $\rho(2) = j$, und $\rho(3) = k$. Dann ist $\rho\pi_1\rho^{-1} = \pi_2$ (siehe Bemerkung 1.2.10). Falls $\rho \in A_n$ haben wir Behauptung 2 bewiesen. Falls $\rho \notin A_n$, dann ist $\rho\circ(45) \in A_n$, und wir haben

$$\rho(45)\pi_2(\rho(45))^{-1} = \rho(45)\pi_2(45)\rho^{-1} = \rho\pi_2\rho^{-1}\pi_2$$

und wieder folgt Behauptung 2.

Aus Behauptung 2 folgt, dass wenn $N \trianglelefteq G$ einen 3-Zykel enthält, dann auch alle anderen 3-Zykel. Wegen Behauptung 1 genügt es also zu zeigen, dass N einen 3-Zykel δ enthält.

Jede Zykelzerlegung $\pi_1\cdots\pi_k$ von σ (Beispiel 1.0.3) fällt in mindestens einen der folgenden drei Fälle.

1. $\{\pi_1,\dots,\pi_k\}$ enthält einen Zykel der Länge mindestens 4, etwa $\pi_1 = (1234\dots)$. Dann gilt für $\tau := (123) \in A_n$, dass

$$N \ni \sigma(\tau\sigma^{-1}\tau^{-1}) = (\sigma\tau\sigma^{-1})\tau^{-1} = (234)(321) = (214) =: \delta.$$

2. Der längste Zykel in $\{\pi_1,\dots,\pi_k\}$ hat Länge 3. Falls $k = 1$ besteht σ aus nur einem 3-Zykel, und wir haben $\delta := \sigma = \pi_1$ bereits gefunden. Ansonsten können wir ohne Beschränkung der Allgemeinheit annehmen, dass $\pi_1 = (123)$ und $\pi_2 = (456)$ oder $\pi_2 = (45)$. Für $\tau := (124) \in A_n$ gilt

$$N \ni \sigma(\tau\sigma^{-1}\tau^{-1}) = (\sigma\tau\sigma^{-1})\tau^{-1} = (235)(142) = (14352) =: \rho$$

   und die Behauptung folgt aus dem ersten Fall mit ρ statt σ.

3. $\{\pi_1,\dots,\pi_k\}$ besteht nur aus Transpositionen; ausserdem gilt $k \geq 2$ da $\sigma \in A_n$. Wir nehmen ohne Beschränkung der Allgemeinheit an, dass $\pi_1 = (12)$ und $\pi_2 = (34)$. Für $\tau = (135) \in A_n$ gilt

$$N \ni \sigma(\tau\sigma^{-1}\tau^{-1}) = (\sigma\tau\sigma^{-1})\tau^{-1} = (24\sigma(5))(153) =: \rho.$$

   Falls $\sigma(5) = 5$, dann erhalten wir $\rho = (12453)$, und die Behauptung folgt mit ρ statt σ aus dem ersten Fall. Falls $\sigma(5) \neq 5$, dann sind die beiden Zykel $(24\sigma(5))$ und (153) disjunkt, und die Behauptung folgt mit ρ statt σ aus dem zweiten Fall. □

Korollar 1.11.6. *Für $n \neq 4$ hat S_n nur die Normalteiler 1, A_n, und S_n.*

Beweis. Sei $N \trianglelefteq S_n$. Für $n \leq 3$ siehe Übung 42. Für $n \geq 5$ wende das Diamantenisomorphielemma (Proposition 1.4.15) auf S_n, N, und $A_n \leq S_n$ an: wir erhalten, dass $A_n \cap N \trianglelefteq A_5$, also ist $A_n \cap N = \{1\}$ oder $A_n \cap N = A_n$ nach Satz 1.11.5. Im ersten Fall muss gelten $N = \{1\}$, und im zweiten muss gelten $N \in \{A_n, S_n\}$. □

Weitere wichtige Beispiele von (endlichen und unendlichen) einfachen Gruppen gewinnt man aus der folgenden Konstruktion.

Beispiel 1.11.7. Sei $\mathbb{K}$ ein Körper. Wir betrachten wir für $n \in \mathbb{N}$ zunächst die Menge $\mathrm{SL}(n, \mathbb{K})$ aller Matrizen $A \in \mathbb{K}^{n \times n}$ mit Determinante 1; diese Menge ist eine Untergruppe von $\mathrm{GL}(n, \mathbb{K})$, die *spezielle lineare Gruppe vom Grad n über dem Körper* $\mathbb{K}$. Diese hat das Zentrum

$$Z := Z(\mathrm{SL}(n, \mathbb{K})) = \mathrm{SL}(n, \mathbb{K}) \cap \mathbb{K}E_n = \mu_n(\mathbb{K})E_n$$

wobei $\mu_n(\mathbb{K})$ für die Menge der *n-ten Einheitswurzeln in* $\mathbb{K}$ steht, also der Elemente $r \in \mathbb{K}$ mit $r^n = 1$. Denn wenn $A \in \mathbb{K}^{n \times n}$ mit allen Matrizen in $\mathrm{SL}(n, \mathbb{K})$ kommutiert, dann insbesondere mit der Elementarmatrix E_{ij}, die Einträge 1 auf der Diagonalen und an Stelle i, j hat. Es gilt für verschiedene $i, j \in \{1, \ldots, n\}$ genau dann $AE_{ij} = E_{ij}A$, wenn

$$\sum_{k=1}^{n} a_{ki} E_{kj} = \sum_{l=1}^{n} a_{jl} E_{il}.$$

Dies ist äquivalent zu

- $a_{ki} = 0$ für alle $k \neq i$,
- $a_{jl} = 0$ für alle $l \neq k$, und
- $a_{ii} = a_{jj}$.

Also ist M von der Gestalt aE_n für $a \in \mathbb{K}$. Da $M \in \mathrm{SL}(n, \mathbb{K})$, gilt $a \in \mu_n(\mathbb{K})$.

Das Zentrum ist stets ein Normalteiler; der Quotient $\mathrm{PSL}(n, \mathbb{K}) := \mathrm{SL}(n, \mathbb{K})/Z$ heißt *projektive lineare Gruppe vom Grad n über dem Körper* $\mathbb{K}$, und ist einfach, falls $n = 2$ und $\mathbb{K}$ mindestens vier Elemente hat, oder falls $n \geq 3$. Wir werden einen Beweis führen für $n = 2$ (Proposition 1.13.25); für den Fall $n \geq 3$ verweisen wir auf das Lehrbuch von Lang [3] (Chapter VIII, Paragraph 9) oder von Jantzen und Schwermer (Kapitel 2, Anhang B). △

Bemerkung 1.11.8. Ende der 1970er Jahre wurden die endlichen einfachen Gruppen vollständig klassifiziert: diese bestehen aus

1. den zyklischen Gruppen von Primzahlordnung (siehe Beispiel 1.11.3);
2. den alternierenden Gruppen A_n für $n \geq 5$ (siehe Satz 1.11.5);
3. Endliche einfache Gruppen vom Lie-Typ (deren Definition sprengt den Rahmen der Vorlesung); Beispiel 1.11.7 fällt in diese Kategorie.

4. weiterhin 26 *sporadischen Gruppen* (5 davon bereits in den Jahren 1862 und 1873 von Mathieu entdeckt, die letzte soganannte *Monstergruppe* erst 1973 im Rahmen des Klassifikationsprogrammes gefunden und 1980 vollständig konstruiert).

1.12 Kompositionsreihen

Sei G eine Gruppe.

Definition 1.12.1. Eine *Normalreihe von* G (der Länge n) ist eine Folge von Untergruppen

$$G = G_0 > G_1 > \cdots > G_n = \{1\}$$

mit $G_i \trianglelefteq G_{i-1}$ für $i \in \{1, \ldots, n\}$. Die Quotientengruppen G_{i-1}/G_i heißen die *Faktoren* der Normalreihe, die Gruppen G_i die *Terme* der Normalreihe.

Bemerkung 1.12.2. Die Bedingung $G_i \trianglelefteq G_{i-1}$ für alle $i \in \{1, \ldots, n\}$ impliziert *nicht*, dass $G_j \trianglelefteq G = G_0$ für $j \in \{2, \ldots, n\}$.

Bemerkung 1.12.3. Jede Gruppe G besitzt die (triviale) Kompositionsreihe $G = G_0 > G_1 = \{1\}$.

Eine Normalreihe $\mathcal{G} = (G_0, \ldots, G_n)$ von G ist eine *Verfeinerung* einer Normalreihe $\mathcal{H} = (H_0, \ldots, H_m)$ von G, wenn jeder Term von $\mathcal{H}$ isomorph zu einem Term von $\mathcal{G}$ ist. Die Verfeinerung ist *echt*, falls $n > m$. Zwei Normalreihen $\mathcal{G}$ und $\mathcal{H}$ heißen *äquivalent*, wenn $\mathcal{G}$ Verfeinerung von $\mathcal{H}$ ist und umgekehrt $\mathcal{H}$ Verfeinerung von $\mathcal{G}$ ist. In anderen Worten, $\mathcal{G}$ und $\mathcal{H}$ sind genau dann äquivalent, wenn $n = m$ und es ein $\pi \in S_n$ gibt, so dass H_i für jedes $i \in \{1, \ldots, n\}$ isomorph zu $G_{\pi(i)}$ ist.

Bemerkung 1.12.4. Verfeinerung ist transitiv und definiert daher auf der Menge der Normalreihen eine Ordnungsrelation, mit $\mathcal{H} \leq \mathcal{G}$ falls $\mathcal{G}$ eine Verfeinerung ist von $\mathcal{H}$.

Lemma 1.12.5 (Verfeinerungslemma)**.** *Falls $G \trianglelefteq G'$ und $N \trianglelefteq G'/G$ so, dass $\{1\} < N < G'/G$, dann gibt es ein H mit $G \trianglelefteq H \trianglelefteq G'$ und $G < H < G'$. Falls G'/G abelsch, dann sind G'/H und H/G ebenfalls abelsch.*

Beweis. Sei $\psi := \varphi_N \circ \varphi_G$ die Komposition der kanonischen Projektion $\varphi_G \colon G' \to G'/G$ mit der kanonischen Projektion $\varphi_N \colon (G'/G) \to (G'/G)/N$ und sei $H := \mathrm{Kern}(\psi) \leq G'$. Offenbar gelten $\psi(G) = \varphi_N \circ \varphi_G(G) = \varphi_N(\{1\}) = \{1\}$, also $G \leq H$.

Falls $H = G$, dann ist $\mathrm{Kern}(\varphi_N \circ \varphi_G) = H = G = \mathrm{Kern}(\varphi_G)$, und damit $N = \mathrm{Kern}(\varphi_N) = \{1\}$. Falls $H = G'$, dann ist $\mathrm{Kern}(\varphi_N \circ \varphi_G) = H = G'$, also $N = G'/G$.

Falls G'/G abelsch, dann ist $H/G \leq G'/H$ klarerweise auch abelsch. Weiterhin ist G'/H das homomorphe Bild von G'/G bezüglich des kanonischen Homomorphismus von G'/G nach G'/H, also ebenfalls abelsch. □

Eine *Kompositionsreihe* ist eine Normalreihe, die maximal bezüglich Verfeinerung ist.

Lemma 1.12.6. *Eine Normalreihe ist genau dann eine Kompositionsreihe, wenn alle ihre Faktoren einfache Gruppen sind.*

Beweis. Falls es ein $H \trianglelefteq G_{i-1}$ gibt mit $G_i < H$, dann folgt aus $G_i \trianglelefteq G_i$, dass $G_i \trianglelefteq H$. Nach dem Kürzungsisomorphiesatz (Proposition 1.4.15) gilt $H/G_i \trianglelefteq G_{i-1}/G_i$ und

$$(G_{i-1}/G_i)/(H/G_i) \cong G_{i-1}/H.$$

Da $G_i < H$, ist $H/G_i \neq \{1\}$. Da $H < G_{i-1}$, ist $G_{i-1}/H \neq \{1\}$. Also ist H/G_i ein echter, nichttrivialer Normalteiler des Faktors G_{i-1}/G_i.

Umgekehrt, falls G_{i-1}/G_i einen echten, nichttrivialen Normalteiler N besitzt, dann gibt es nach dem Verfeinerungslemma (Lemma 1.12.5) ein H mit $G_i < H < G_{i-1}$ mit $G \trianglelefteq H$ und $H \trianglelefteq G'$. Also ist

$$G = G_0 > G_1 > \cdots > G_{i-1} > H > G_i > \cdots > G_n = \{1\}$$

eine echte Verfeinerung der ursprünglichen Kompositionsreihe. □

Bemerkung 1.12.7. Jede Normalreihe einer endlichen Gruppe besitzt eine Verfeinerung, die eine Kompositionsreihe ist. Insbesondere besitzt jede endliche Gruppe eine Kompositionsreihe.

Das folgende Beispiel zeigt, dass unendliche Gruppen keine Kompositionsreihe besitzen müssen.

Beispiel 1.12.8. $\mathbb{Z}$ besitzt keine Kompositionsreihe: denn nach Lemma 1.5.2 sind alle Untergruppen von $\mathbb{Z}$ isomorph zu $m\mathbb{Z}$, für $m \in \mathbb{N}$, aber $m\mathbb{Z}/\{e\}$ ist nicht einfach. △

Beispiel 1.12.9. S_3 has die Kompositionsreihe $S_3 > A_3 > 1$ (siehe Beispiel 42) mit den Faktoren $S_3/A_3 \cong \mathbb{Z}/2\mathbb{Z}$ und $A_3/\{1\} \cong A_3 \cong \mathbb{Z}/3\mathbb{Z}$. △

Beispiel 1.12.10. S_4 has die Kompositionsreihe $S_4 > A_4 > V_4 > H > 1$ wobei $H = \langle (12)(34) \rangle$ mit den Faktoren $S_4/A_4 \cong \mathbb{Z}/2\mathbb{Z}$, $A_4/V_4 \cong \mathbb{Z}/3\mathbb{Z}$, $V_4/H \cong \mathbb{Z}/2\mathbb{Z}$ (Beispiel 1.6.2), und $H/\{1\} \cong H \cong \mathbb{Z}/2\mathbb{Z}$. △

Beispiel 1.12.11. S_n, für $n \geq 5$, hat die Kompositionsreihe $S_n > A_n > 1$ mit den Faktoren $S_5/A_5 \cong \mathbb{Z}/2\mathbb{Z}$ und $A_n/\{1\} \cong A_n$. △

Satz 1.12.12 (Jordan-Hölder)**.** *Je zwei Kompositionsreihen einer endlichen Gruppe G sind äquivalent.*

Beweis. Beweis per Induktion nach der minimalen Länge einer Kompositionsreihe

$$G = A_0 > A_1 > \cdots > A_m = \{1\}.$$

Sei $G = B_0 > B_1 > \cdots > B_n = \{1\}$ eine weitere Kompositionsreihe. Ist $A_1 = B_1$, so folgt die Behauptung durch Anwenden der Induktionsvoraussetzung auf A_1. Ansonsten ist $G = A_1B_1$: Denn wenn $A_1 \neq B_1$, können ohne Beschränkung der Allgemeinheit annehmen, dass $B_1 \setminus A_1 \neq \emptyset$, also $A_1 < A_1B_1$. Weiterhin ist $A_1B_1 \trianglelefteq G$ (Übung 22), und da G/A_1 einfach ist, muss gelten $A_1B_1 = G$.

Also gilt nach Proposition 1.4.15 (Diamantenisomorphielemma)

$$G/A_1 = A_1B_1/A_1 \cong B_1/(A_1 \cap B_1)$$
$$G/B_1 = A_1B_1/B_1 \cong A_1/(A_1 \cap B_1).$$

Da G/A_1 und G/B_1 einfach sind, ist $H = A_1 \cap B_1$ ein maximaler Normalteiler von A_1 und von B_1. Sei $H = H_0 > H_1 > \cdots > H_p = \{1\}$ eine Kompositionsreihe von H. Nach Induktionsvoraussetzung haben die beiden Kompositionsreihen

$$A_1 > A_2 > \cdots > A_m = \{1\}$$
$$\text{und } A_1 > H > H_1 > \cdots > H_p = \{1\}$$

von A_1 die gleiche Länge $m - 1 = p - 1$, und isomorphe Faktoren. Analoges gilt für die beiden Kompositionsreihen

$$B_1 > B_2 > \cdots > B_n = \{1\}$$
$$\text{und } B_1 > H > H_1 > \cdots > H_p = \{1\}$$

von B_1. Also $m = p = n$. Wegen $G/A_1 \cong B_1/H$ und $G/B_1 \cong A_1/H$ folgt auch, dass die beiden ursprünglichen Kompositionsreihen von G isomorphe Kompositionsfaktoren haben. □

Bemerkung 1.12.13. Es gilt sogar, dass je zwei Normalreihen einer beliebigen Gruppe G äquivalente Verfeinerungen besitzen (der *Satz von Schreier*). Daraus folgt der Satz von Jordan-Hölder unmittelbar. Umgekehrt folgt der Satz von Schreier für endliche Gruppen aus dem Satz von Jordan-Hölder (Übung 48).

Alle Kompositionsreihen einer endlichen Gruppe G haben daher (bis auf Isomorphie) die gleichen Faktoren, welche wir daher die *Kompositionsfaktoren von* G nennen. Das folgende Beispiel zeigt, dass eine Gruppe nicht eindeutig von ihren Kompositionsfaktoren bestimmt wird (auch nicht, wenn man Mehrfachauftreten mit berücksichtigt).

Beispiel 1.12.14 (Diedergruppen). Für $n \in \{3, 4, \dots\}$ sei D_{2n} die Automorphismengruppe des Graphen (siehe Beispiel 1.1.5)

$$C_n := (\{0, 1, \dots, n-1\}; \{(x, y) : |x - y| = 1 \mod n\})$$

Offensichtlich ist die Permutation $\sigma := (012 \dots n-1)$ ein Automorphismus von C_n. Falls n gerade ist, so ist $\tau := (0\ n-1)(1\ n-2) \dots (n/2-1\ n/2)$ ein Automorphismus der Ordnung 2, und falls $n = 2k+1$, so ist $\tau := (0\ n-1)(1\ n-2) \dots (k-1\ k+1)$ ein Automorphismus der Ordnung 2. Es ist einfach zu sehen, dass in jedem Fall ganz D_{2n} von $\{\sigma, \tau\}$ erzeugt wird, und dass $|D_{2n}| = 2n$. Die Gruppe D_{2n} wird auch die *Diedergruppe der Ordnung* $2n$ genannt. Wir berechnen die Kompositionsfaktoren von D_8. Zunächst stellen wir fest, dass D_8 wegen $|D_8| = 8 = 2^3$ eine p-Gruppe für $p = 2$ ist. Dann besitzt D_8 eine Untergruppe G_1 der Ordnung 2^2 (Lemma 1.10.1). Dann gilt $(D_8 : G_1) = 2$ und $G_1 \trianglelefteq D_8$ (Proposition 1.4.17). Die p-Gruppe G_1 wiederum besitzt eine normale Untergruppe G_2 der Ordnung 2. Also hat D_8 drei Kompositionsfaktoren, und alle drei isomorph zu $\mathbb{Z}/2\mathbb{Z}$. △

Beispiel 1.12.15. (Quaternionengruppe) Die *Quaternionengruppe* Q_8 hat die Elemente

$$\{1, -1, i, -1, j, -j, k, -k\}$$

und die Gruppenoperation $\cdot$, die definiert ist durch

$$\begin{aligned}
1 \cdot a = a \cdot 1 = a & \qquad && \text{für alle } a \in Q_8 \\
-1 \cdot a = a \cdot -1 = -a & && \text{für alle } a \in Q_8 \\
-1 \cdot -1 = 1 & && \\
a \cdot a = -1 & && \text{für alle } a \in \{i, j, k\} \\
i \cdot j = k & \qquad j \cdot k = i && \qquad k \cdot i = j \\
j \cdot i = -k & \qquad k \cdot j = -i && \qquad i \cdot k = -j
\end{aligned}$$

Auch Q_8 ist eine p-Gruppe mit $p = 2$; wie im letzten Beispiel sind daher alle Kompositionsfaktoren isomorph zu $\mathbb{Z}/2\mathbb{Z}$, und es gibt genau drei davon, da $|Q_8| = 8$. Allerdings hat Q_8 im Gegensatz zu D_8 nur ein Element der Ordnung 2, nämlich -1. Die beiden Gruppen Q_8 und D_8 sind also nicht isomorph. △

Übung 45. Bestimmen Sie die Ordnung der Elemente von Q_8 (Beispiel 1.12.15).

Übung 46. Zeigen Sie, dass Q_8 nicht abelsch ist, dass aber alle Untergruppen von Q_8 abelsch sind.

Übung 47. Finden sie zwei nicht-isomorphe Gruppen, die die gleichen Kompositionsfaktoren haben, aber kleiner sind als D_8 und Q_8.

Übung 48. Zeigen Sie, dass für endliche Gruppen der Satz von Jordan Hölder (Satz 1.12.12) auch den Satz von Schreier impliziert (siehe Bemerkung 1.12.13).

1.13 Auflösbare Gruppen

Eine Gruppe heißt *auflösbar* wenn sie eine Normalreihe mit abelschen Faktoren besitzt.

Bemerkung 1.13.1. Die auflösbaren endlichen Gruppen spielen eine wichtige Rolle in der Theorie der Auflösbarkeit algebraischer Gleichungen. Diesem Zusammenhang haben sie ihren Namen zu verdanken.

Beispiel 1.13.2. S_3 hat die Kompositionsfaktoren $\mathbb{Z}/2\mathbb{Z}$ und $\mathbb{Z}/3\mathbb{Z}$ (Beispiel 1.12.9) und ist daher auflösbar. △

Beispiel 1.13.3. S_4 hat die Kompositionsfaktoren $\mathbb{Z}/2\mathbb{Z}$ und $\mathbb{Z}/3\mathbb{Z}$ (Beispiel 1.12.10) und ist daher auflösbar. △

Beispiel 1.13.4. S_n, für $n \geq 5$, hat die Kompositionsfaktoren $\mathbb{Z}/2\mathbb{Z}$ und Gruppe A_n. Die Gruppe A_n ist nicht zyklisch (Übung 27), und daher ist S_n nicht auflösbar. △

Beispiel 1.13.5. Alle endlichen abelschen Gruppen sind auflösbar: denn endliche Gruppen besitzen eine Kompositionsreihe, und endliche einfache abelsche Faktoren sind zyklisch (siehe Beispiel 1.11.3). △

Beispiel 1.13.6. Alle p-Gruppen sind auflösbar. Damit also inbesondere D_8 aus Beispiel 1.12.14 und Q_8 aus Beispiel 1.12.15. △

Proposition 1.13.7. *Für eine endliche Gruppe G sind äquivalent:*

1. *Alle Kompositionsfaktoren von G sind zyklisch.*
2. *G hat eine Normalreihe mit zyklischen Faktoren.*
3. *G ist auflösbar, d.h., hat eine Normalreihe mit abelschen Faktoren.*
4. *G hat eine Normalreihe mit auflösbaren Faktoren.*

Beweis. Die Implikationen 1. $\Rightarrow$ 2. $\Rightarrow$ 3. sind trivial. Die Implikation 3. $\Rightarrow$ 4. folgt aus Beispiel 1.13.5: abelsche Gruppen sind auflösbar. Für die Implikation 3. $\Rightarrow$ 1., verfeinere eine Normalreihe von G mit abelschen Faktoren zu einer Kompositionsreihe von G mit abelschen Faktoren (Lemma 1.12.5 und Bemerkung 1.12.7). Da jede endliche einfache abelsche Gruppe zyklisch ist (Bemerkung 1.11.3), sind alle Kompositionsfaktoren zyklisch. Den Beweis der Implikation 4. $\Rightarrow$ 3 verschieben wir auf Korollar 1.13.23. □

Zur Charakterisierung auflösbarer Gruppen werden wir den Begriff des Kommutators verwenden (manche Autor:innen verwenden den Zugang über Kommutatoren, um auflösbare Gruppen zu definieren).

Definition 1.13.8 (Kommutator)**.** Sind a und b Elemente einer Gruppe G, so bezeichnet man

$$[a,b] := aba^{-1}b^{-1}$$

als den *Kommutator* von a und b.

Der Name Kommutator erklärt sich aus folgender Bemerkung.

Bemerkung 1.13.9. Elemente a und b einer Gruppe kommutieren genau dann (also $ab = ba$), wenn $[a,b] = 1$. Es gilt $[a,b]^{-1} = (aba^{-1}b^{-1})^{-1} = bab^{-1}a^{-1} = [b,a]$.

Bemerkung 1.13.10. Ausdrücke der Gestalt $aba^{-1}b^{-1}$ sind uns bereits begegnet

- im Beweis von Lemma 1.6.4, welches eine wichtige Rolle für das innere direkte Produkt spielte, und
- im Beweis der Einfachheit von A_n für $n \geq 5$ (Satz 1.11.5).

Wieder verwenden wir Komplexschreibweise: für $H, K \subseteq G$ definieren wir

$$[H,K] := \langle \{[h,k] \mid h \in H, k \in K\} \rangle.$$

Die *Kommutatoruntergruppe von G* ist definiert als $\langle [G,G] \rangle$.

Lemma 1.13.11. *$H := \langle [G,G] \rangle$ ist ein Normalteiler von G.*

Beweis. Seien $g \in G, h \in H$. Dann gilt $h = [a_1,b_1]\cdots[a_k,b_k]$ für $a_1, b_1, \ldots, a_k, b_k \in G$. Wegen

$$xhx^{-1} = x[a_1,b_1]\cdots[a_k,b_k]x^{-1} = x[a_k,b_k]x^{-1}\cdots x[a_k,b_k]x^{-1}$$
$$\text{und } x[a_i,b_i]x^{-1} = xaba^{-1}b^{-1}x^{-1} = xax^{-1}xbx^{-1}xa^{-1}x^{-1}xb^{-1}x^{-1} = [xa_ix^{-1}, xb_ix^{-1}]$$

ist xhx^{-1} ein Produkt von Kommutatoren, also in H. Es folgt, dass $H \trianglelefteq G$. □

Bemerkung 1.13.12. Eine Gruppe ist genau dann abelsch, wenn wenn die Kommutatoruntergruppe trivial ist, soll heißen, wenn $\langle [G,G] \rangle = [G,G] = \{1\}$ (siehe Bemerkung 1.13.9).

Diese Bemerkung werden wir wie folgt verallgemeinern.

Lemma 1.13.13. *Sei $N \trianglelefteq G$. Dann ist G/N genau dann abelsch, wenn $\langle [G,G] \rangle \subseteq N$.*

Beweis. Die Quotientengruppe G/N ist genau dann abelsch, wenn $aNbN = bNaN$ für alle $a, b \in G$. Da $aNbN = abN$ und $bNaN = baN$ ist dies genau dann der Fall, wenn $a^{-1}b^{-1}abN = N$ für alle $a, b \in G$, also wenn $[a,b] \in N$ für alle $a, b \in G$. □

Korollar 1.13.14. *Für jede Gruppe G ist $G/\langle [G,G] \rangle$ abelsch.*

Beispiel 1.13.15. Wir rechnen von Hand nach

$$\langle [S_3, S_3] \rangle = \{(123), (132), 1\} = A_3$$

oder lesen das aus dem folgendem Lemma ab. △

Lemma 1.13.16. *Für jedes $n \in \mathbb{N}_{\geq 1}$ gilt $\langle [S_n, S_n] \rangle = A_n$.*

Beweis. Die Fälle $n \in \{1, 2\}$ sind klar. Ansonsten gilt für verschiedene $a, b, c \in \{1, \dots, n\}$, dass

$$(abc) = (acb)^2 = (ac)(cb)(ac)(cb) = [(ac), (cb)].$$

Also folgt $A_5 \subseteq \langle [S_n, S_n] \rangle$ aus Behauptung 1 im Beweis von Satz 1.11.5. Wegen $|S_n/A_n| = 2$ (Korollar 1.4.18) ist S_n/A_n abelsch, also gilt $\langle [S_n, S_n] \rangle \subseteq A_5$ nach Lemma 1.13.13. □

Beispiel 1.13.17. Es gilt

$$\langle [A_4, A_4] \rangle = \{(12)(34), (13)(23), (14)(23), 1\} = V_4.$$ △

Lemma 1.13.18. *Für $n \geq 5$ gilt $\langle [A_n, A_n] \rangle = A_n$.*

Beweis. Nach Lemma 1.13.11 ist $H := \langle [A_n, A_n] \rangle \trianglelefteq A_n$, also $H \in \{\{1\}, A_n\}$, da A_n einfach ist (Satz 1.11.5). Da A_n für $n \geq 5$ nicht abelsch ist ist (Übung 27), gilt $H \neq \{1\}$ (Bemerkung 1.13.12). Also $H = A_n$. □

Definition 1.13.19 (Kommutatorreihe)**.** Die Kommutatorreihe

$$G = G^{(0)} \geq G^{(1)} \geq \cdots$$

einer Gruppe G ist induktiv definiert durch $G^{(0)} := G$ und $G^{(n+1)} := \langle [G^{(n)}, G^{(n)}] \rangle$.

Satz 1.13.20. *Sei $G = G_0 > G_1 > \cdots > G_n$ eine Normalreihe mit abelschen Faktoren; wir fordern ausnahmsweise nicht, dass $G_n = \{1\}$. Dann gilt $G^{(i)} \leq G_i$ für alle $i \leq n$. Insbesondere ist eine Gruppe ist genau dann auflösbar, wenn $G^{(n)} = \{1\}$ für ein $n \in \mathbb{N}$.*

Beweis. Per Induktion nach n: ist $G^{(n)} \leq G_n$ und G_n/G_{n+1} ist abelsch, so ist $G^{(n+1)} \subseteq G_{n+1}$ nach Lemma 1.13.13. Ist $G^{(n)} = \{1\}$, so ist

$$G = G^{(0)} > G^{(1)} > \cdots > G^{(n)} = \{1\}$$

eine Normalreihe (siehe Lemma 1.13.11), deren Faktoren nach Lemma 1.13.13 abelsch sind. □

Korollar 1.13.21. *Ist G auflösbar und $H \leq G$, so ist auch H auflösbar.*

Das kleinste n mit $G^{(n)} = \{1\}$ heißt die *Stufe* von G.

Korollar 1.13.22. *Sei $N \trianglelefteq G$ so, dass G/N auflösbar und N auflösbar. Dann ist auch G auflösbar.*

Beweis. Sei n die Stufe von N und m die Stufe von G/N. Dann gilt $G^{(m)} \leq N$. Es folgt $G^{(n+m)} \leq N^{(m)} = \{1\}$. Dann ist G auflösbar nach Satz 1.13.20. □

Wir können nun auch bequem den Beweis der Implikation 4. $\Rightarrow$ 3. in Proposition 1.13.7 nachholen.

Korollar 1.13.23. *Falls eine Gruppe eine Normalreihe mit auflösbaren Faktoren besitzt, dann ist sie auflösbar.*

Beweis. Aus Korollar 1.13.22 mit vollständiger Induktion. □

Bemerkung 1.13.24. Die folgenden tiefen Sätze sprengen den Rahmen dieser Vorlesung:

- *Satz von Burnside:* ist $|G| = p^a q^b$ für Primzahlen p und q, so ist G auflösbar.
- *Satz von Feit-Thompson:* Ist $|G|$ ungerade, so ist G auflösbar.

Wir werden diese Sätze weder in der Vorlesung noch den Übungen verwenden; allerdings ist es gut (zum Beispiel für Plausibilitätsprüfungen), sie zu kennen.

Wir beenden das Kapitel zur Gruppentheorie mit einem Nachtrag zu Abschnitt 1.11 (Einfache Gruppen); im Beweis verwenden wir wieder den Begriff des Kommutators.

Proposition 1.13.25. *Sei $\mathbb{K}$ ein Körper mit mindestens vier Elementen. Dann ist $G := \mathrm{PSL}(2, \mathbb{K})$ einfach.*

Beweis. Wird nicht im Unterricht behandelt, für Interessierte. WIRD NOCH BEARBEITET. Zunächst stellen wir fest, dass G erzeugt wird von den Matrizen der Gestalt

$$X(b) := \begin{pmatrix} 1 & b \\ 0 & 1 \end{pmatrix} \text{ und } Y(c) := \begin{pmatrix} 1 & 0 \\ c & 1 \end{pmatrix} \text{ für } b, c \in \mathbb{K}.$$

Multiplikation mit diesen Matrizen von links und von rechts entspricht der Addition eines Vielfachen einer Zeile zu einer anderen, beziehungsweise der Addition eines Vielfachen einer Spalte zu einer anderen (siehe LA10). Eine gegebene Matrix aus G kann

durch solche Operationen in die Einheitsmatrix überführt werden, und daraus folgt die Behauptung.

Es sei B die (echte) Untergruppe von G der Matrizen der Gestalt

$$\begin{pmatrix} a & b \\ 0 & d \end{pmatrix}$$

wobei $a, b, d \in \mathbb{K}$ und $ad = 1$. Diese Untergruppe ist maximal in G:

Wir zeigen, dass G seine eigene Kommutatoruntergruppe ist, also dass $G = \langle [G, G] \rangle$. Da $|\mathbb{K}| \geq 4$ gibt es ein Element $z \in \mathbb{K} \setminus \{-\}$ mit $z^2 \neq 1$. Dann gilt TODO.

Sei $H \trianglelefteq G$. Es genügt zu zeigen, dass $H \leq Z(\mathrm{SL}(2, \mathbb{K}))$ oder $G \subseteq H$.

Wir zeigen zunächst, dass

$$Z(\mathrm{PSL}(2, \mathbb{K})) = \bigcap_{g \in \mathrm{SL}(2, \mathbb{K})} gBg^{-1}.$$

Sei $w := \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$.

□

Kapitel 2

Ringe

Erinnerung von LA20: ein *Ring (mit Eins)* $\underline{R}$ ist eine abelsche Gruppe $(R, +, -, 0)$ mit einer zweistelligen Operation $\cdot$ (Multiplikation) und einem Element $1 \in R$ (dem *Einselement*), so dass für alle $x, y, z \in R$ folgendes gilt.

$$\begin{aligned}
(x \cdot y) \cdot z &= x \cdot (y \cdot z) && \text{(Assoziativität von } \cdot\text{)} \\
1 \cdot x &= x && \text{(Eins ist neutrales Element bezüglich } \cdot\text{)} \\
x(y + z) &= xy + xz && \text{(linke Distributiviät von von } \cdot \text{ über } +\text{)} \\
(x + y)z &= xz + yz && \text{(rechte Distributiviät von von } \cdot \text{ über } +\text{)}
\end{aligned}$$

Der Ring $\underline{R}$ heißt *kommutativ* falls weiterhin gilt $x \cdot y = y \cdot x$ für alle $x, y \in R$.

Bemerkung 2.0.1. Die Rechenregeln $0 \cdot x = x \cdot 0 = 0$ und $(-x)y = -(xy) = x(-y)$, für beliebige Elemente $x, y \in R$, die wir von Körpern kennen, gelten auch in Ringen $\underline{R}$.

Beispiel 2.0.2. Jeder Körper ist ein Ring mit Eins. Weiterhin: die ganzen Zahlen $\mathbb{Z}$, die Restklassenringe $\mathbb{Z}/n\mathbb{Z}$, der Nullring mit $R = \{0\}$ (und $0 = 1$). Matrizenringe liefern Beispiele für nicht-kommutative Ringe. Polynomringe $\underline{R}[X]$ sind kommutativ, falls $\underline{R}$ kommutativ ist. △

Definition 2.0.3 (Unterring)**.** Ein *Unterring* (oder *Teilring*) ist eine Untergruppe U von $(R, +, -, 0)$, die die 1 enthält und abgeschlossen ist unter Multiplikation: das bedeutet, dass für alle $x, y \in U$ auch $x \cdot y \in U$.

Bemerkung 2.0.4. Sei S ein Unterring von $\underline{R}$ und $a \in R$. Dann schreiben wir $\underline{S}[a]$ für den kleinsten Unterring von $\underline{R}$, der $S \cup \{a\}$ enthält; man sagt auch, der Ring $\underline{S}[a]$ entsteht aus S durch *Adjunktion von a*. Zum Beispiel entsteht $\mathbb{Q}[\sqrt{2}]$ aus dem Unterring $\mathbb{Q}$ von $\mathbb{R}$ (äquivalent: dem Unterring $\mathbb{Q}$ von $\mathbb{C}$) durch Adjunktion von $\sqrt{2}$.

Definition 2.0.5 (Ringhomomorphismus)**.** Ein *Ringhomomorphismus* ist eine Abbildung $\varphi\colon R \to R'$ zwischen zwei Ringen $\underline{R}$ und $\underline{R}'$, so dass

$$\begin{aligned}
\varphi(x + y) &= \varphi(x) + \varphi(y) \\
\varphi(x \cdot y) &= \varphi(x) \cdot \varphi(y) \\
\varphi(1) &= 1.
\end{aligned}$$

Ein *Ringisomorphismus* ist ein bijektiver Ringhomomorphismus. Ein *Ringautomorphismus von* $\underline{R}$ ist ein Ringisomorphismus zwischen $\underline{R}$ und $\underline{R}$. Ein *Ringendomorphismus von* $\underline{R}$ ist ein Ringhomomorphismus von $\underline{R}$ nach $\underline{R}$. Das Präfix *Ring-* kann weggelassen werden, wenn es dadurch nicht zu Verwirrungen kommt.

Mit der folgenden Definition können aus bekannten Ringen weitere Ringe konstruiert werden.

Definition 2.0.6 (Produkte)**.** Für eine Familie $(\underline{R}_i)_{i\in I}$ von Ringen erhalten wir auf der Menge $R := \prod_{i\in I} R_i$ durch komponentenweise Addition und Multiplikation einen Ring $\underline{R} = \prod_{i\in I} \underline{R}_i$, das *direkte Produkt*. Ist $1_{\underline{R}_i}$ das Einselement von $\underline{R}_i$, so ist $(1_{\underline{R}_i})_{i\in I}$ das Einslement von $\underline{R}$.

Übung 49. Ein Ring ist genau dann der Nullring, wenn $0 = 1$.

2.1 Teilbarkeit, Nullteiler und Einheiten

Sei $\underline{R}$ ein Ring. Wir schreiben $a|b$, und nennen a einen *Teiler* von b, falls es ein $r \in R$ gibt mit $ar = b$. Offensichtlicherweise ist die Teilbarkeitsrelation transitiv, soll heißen, falls $a|b$ und $b|c$, dann gilt auch $a|c$. Ein Element $a \in R$ heißt

- ein *Nullteiler* falls es ein $b \in R \setminus \{0\}$ gibt mit $ab = 0$.
- eine *Einheit* falls es ein $b \in R$ gibt so dass $ab = ba = 1$.

Die Menge der Einheiten in $\underline{R}$ wird mit $\underline{R}^\times$ bezeichnet. Mit dieser Terminologie ist ein Körper ein kommutativer Ring, so dass $0 \neq 1$ und jedes Element, welches nicht Null ist, eine Einheit ist.

Bemerkung 2.1.1. Im Nullring gibt es offensichtlich keine Nullteiler. Falls $\underline{R}$ nicht der Nullring ist, dann ist $0 \in R$ ein Nullteiler, der *triviale* Nullteiler. Ein Ring heißt *nullteilerfrei*, wenn er keinen nicht-trivialen Nullteiler besitzt.

Bemerkung 2.1.2. Nullteiler sind keine Einheiten: denn wenn es ein $b \in R \setminus \{0\}$ gibt mit $ab = 0$, und a ein Inverses a^{-1} besitzt, dann wäre $b = 1b = a^{-1}ab = a^{-1}0 = 0$, ein Widerspruch.

Beispiel 2.1.3. Der Ring $\mathbb{Z}$ ist nullteilerfrei und hat die Einheiten $\{+1, -1\}$. Der Ring $\mathbb{Z}/n\mathbb{Z}$ ist genau dann nullteilerfrei, wenn n eine Primzahl ist. △

Lemma 2.1.4. *Sei $\underline{R}$ ein Ring und $a, b, c \in R$ so, dass a ist kein Nullteiler. Falls $ab = ac$, dann gilt $a = 0$ or $b = c$.*

Beweis. Angenommen, $a \neq 0$. Falls $ab = ac$ dann gilt $a(b - c) = 0$. Da $a \neq 0$ kein Nullteiler, muss gelten $b - c = 0$. □

Definition 2.1.5. Sei $\underline{R}$ ein Ring und $M \subseteq R$ nicht leer. Dann heißt $d \in R$ ein *größter gemeinsamer Teiler von* M, in Zeichen $\mathrm{ggT}(M)$, falls gilt

- $d|a$ für jedes $a \in M$;
- wenn $d'|a$ für jedes $a \in M$, dann $d'|d$.

Bemerkung 2.1.6. Im Namen *größter gemeinsamer Teiler* bezieht sich 'groß' auf die Teilbarkeitsrelation; im Ring $\mathbb{Z}$ sind die größten Teiler einer natürlichen Zahl bezüglich der gewöhnlichen Ordnung gleich den größten Teilern bezüglich der Teilbarkeitsrelation, mit der Ausnahme von der Null, die von allen Zahlen geteilt wird.

Falls $M = \{a_1, \ldots, a_n\}$, schreiben wir auch $\mathrm{ggT}(a_1, \ldots, a_n)$ anstatt $\mathrm{ggT}(M)$. Falls $1 \in \mathrm{ggT}(a_1, \ldots, a_n)$, so nennen wir $a_1, \ldots, a_n$ *teilerfremd*. Kleinste gemeinsame Vielfache von M, in Zeichen $\mathrm{kgV}(M)$, sind analog definiert. In beliebigen Ringen kann es sein, dass es nicht-leere Mengen $M \subseteq R$ gibt, zu denen kein ggT oder kein kgV existiert (siehe Beispiel 2.5.11) später im Text).

Übung 50. Zeigen Sie, dass für $R = \mathbb{Z}$ die Definition aus diesem Abschnitt, dass die Zahlen $a_1, \ldots, a_n \in R$ teilfremd sind, mit der gewöhnlichen und als bekannt vorausgesetzten Definition übereinstimmt.

Übung 51. Welche der folgenden Strukturen sind Ringe? Welche der Ringe sind nullteilerfrei, und welche sind Körper?

1. $(\mathbb{N}, +, \cdot)$.
2. $(\mathbb{Z}, +, \cdot)$.
3. $(\mathbb{Z}/15\mathbb{Z}, +, \cdot)$.
4. $(\mathbb{Z}/5\mathbb{Z}, +, \cdot)$.
5. $(\mathbb{Z}/3\mathbb{Z}, +, \cdot)^2$.
6. $(\{\text{wahr}, \text{falsch}\}, \vee, \wedge)$.

2.2 Polynomringe

Die folgende Definition ist eine Wiederholung aus LA10. Wir beschränken uns in der Darstellung hier auf kommutative Ringe $\underline{R}$.

Definition 2.2.1 (Polynomring)**.** Der *Polynomring* in einer Variablen X über R hat die Grundmenge

$$R[X] = \left\{ \sum_{i \geq 0} a_i X^i \mid a_i \in R \text{ fast alle } 0 \right\}$$

mit komponentenweiser Addition

$$\sum_{i \geq 0} a_i X^i + \sum_{i \geq 0} b_i X^i := \sum_{i \geq 0} (a_i + b_i) X^i$$

und der Multiplikation

$$\left(\sum_{i\geq 0} a_i X^i\right)\cdot\left(\sum_{j\geq 0} b_j X^j\right) := \sum_{k\geq 0}\left(\sum_{i+j=k} a_i b_j\right) X^k.$$

Sei $f = \sum_{i=0}^{n} a_i X^i \in \underline{R}[X]$ ein Polynom mit $a_n \neq 0$. Weitere Wiederholungen aus LA20: Der Koeffizient $\ell(f) := a_n$ heißt der *Leitkoeffizient*, und der Koeffizient a_0 heißt der *konstante Koeffizient*. Das Polynom f heißt *normiert*, falls $\ell(f) = 1$. Der *Grad* von p ist dann definiert als $\operatorname{grad}(f) := n$. Weiterhin definieren wir $\operatorname{grad}(0) := -\infty$. Für Polynome $f, g \in \underline{R}[X]$ gelten dann (siehe LA20):

- $\operatorname{grad}(f+g) \leq \max(\operatorname{grad}(f), \operatorname{grad}(g))$,
- $\operatorname{grad}(fg) \leq \operatorname{grad}(f) + \operatorname{grad}(g)$,
- Ist $f \neq 0$ und $\ell(g)$ ist kein Nullteiler, so ist $\operatorname{grad}(fg) = \operatorname{grad}(f) + \operatorname{grad}(g)$.

Lemma 2.2.2. *Ist $\underline{R}$ nullteilerfrei, so auch $\underline{R}[X]$, und $\underline{R}[X]^\times = \underline{R}^\times$.*

Beweis. Sind $f, g \in R[X]\setminus\{0\}$, dann ist $\operatorname{grad}(f), \operatorname{grad}(g) \neq -\infty$, und es gilt $\operatorname{grad}(fg) = \operatorname{grad}(f) + \operatorname{grad}(g) \neq -\infty$, also $fg \neq 0$. Ist $fg = 1$, so ist $\operatorname{grad}(f) + \operatorname{grad}(g) = \operatorname{grad}(fg) = \operatorname{grad}(1) = 0$, also $\operatorname{grad}(f) + \operatorname{grad}(g) = 0$, also $f, g \in R$. □

2.2.1 Der Auswertungshomomorphismus

Auch dieser Abschnitt ist zu einem großen Teil eine Wiederholung aus LA10.

Lemma 2.2.3 (Universelle Eigenschaft des Polynomrings)**.** *Ist $\varphi\colon S \to R$ ein Ringhomomorphismus und $a \in R$, so gibt es genau einen Ringhomomorphismus $\varphi_a\colon S[X] \to R$ mit $\varphi_a|_S = \varphi$ und $\varphi_a(X) = a$.*

Beweis. Die Abbildung φ_a, die gegeben wird durch

$$\sum_{i=0}^{n} b_i X^i \mapsto \sum_{i\geq 0} \varphi(b_i) a^i \qquad \text{(Auswertungshomomorphismus)},$$

ist ein Ringhomomorphismus. Für die Addition ist dies offensichtlich, und für die Multiplikation rechnen wir nach

$$\begin{aligned}\varphi_a\left(\left(\sum_{i\geq 0} b_i X^i\right)\cdot\left(\sum_{j\geq 0} c_j X^j\right)\right) &= \varphi_a\left(\sum_{k\geq 0}\left(\sum_{i+j=k} b_i c_j\right) X^k\right)\\ &= \sum_{k\geq 0}\left(\sum_{i+j=k} \varphi(b_i)\varphi(c_j)\right) a^k\\ &= \left(\sum_{i\geq 0} \varphi(b_i) a^i\right)\cdot\left(\sum_{j\geq 0} \varphi(c_j) a^j\right) = \varphi_a\left(\sum_{i\geq 0} b_i X^i\right)\cdot\varphi_a\left(\sum_{j\geq 0} c_j X^j\right)\end{aligned}$$

Es ist φ_a auch offensichtlich der einzige Ringhomomorphismus mit den geforderten Eigenschaften, da $\varphi_a(\sum_{i=0}^n b_i X^i) = \sum_{i=0}^n \varphi_a(b_k X^i)$, da φ_a Gruppenhomomorphismus, weiterhin $\varphi_a(b_k X^i) = \varphi_a(b_k)\varphi_a(X)^i$ da φ_a die Multiplikation bewahrt, und daher folgt mit den geforderten Eigenschaften von φ_a, dass $\varphi_a(\sum_{i=0}^n b_i X^i) = \sum_{i=0}^n \varphi(b_i)a^i$. □

Bemerkung 2.2.4. Wenn $f, g \in R[X]$ sind, dann bezeichnet $f(g(X))$ das Polynom aus $R[X]$, welches man gewinnt durch 'Einsetzen' von g in f. Formal kann man das wie folgt definieren. Nach Lemma 2.2.3 gibt es ein $\phi\colon R[X] \to R[X]$ mit $\phi|_R = \mathrm{id}_R$ und $\phi(X) = g(X)$. Dann definieren wir $f(g(X))$ als $\phi(f)$.

Übung 52. Angenommen $f, g, h \in R[X]$ sind so, dass $f = gh$. Dann gilt auch $f(x+1) = g(x+1)h(x+1)$.

Bemerkung 2.2.5. Sei $\underline{S}$ ein Unterring von $\underline{R}$ und $a \in R$, und sei φ_a die Abbildung aus Lemma 2.2.3 für die Inklusionsabbildung $\varphi\colon S \to R$. Dann sind die Elemente von $\underline{S}[a]$ (siehe Bemerkung 2.0.4) genau das Bild von $\underline{S}[X]$ unter φ_a.

Übung 53. Zeigen Sie: die Unterringe $\mathbb{Z}[\sqrt{2}]$ und $\mathbb{Z}[\sqrt{3}]$ von $\mathbb{R}$ sind nicht isomorph.

Übung 54. Ringautomorphismen eines Ringes R sind bijektive Ringhomomorphismen von R auf sich selbst. Für zwei Ringe R und S mit $R \subseteq S$ sei $\mathrm{Aut}(S|R)$ die Menge der Ringautomorphismen von S, deren Einschränkung auf R die Identität ist. Zeigen Sie, dass $\mathrm{Aut}(R[X]|R)$ eine Untergruppe hat, die isomorph ist zu $(R, +)$.

2.2.2 Polynomdivision

Polynomdivision hatten wir bereits in LA10 für Polynome über einem Körger erwähnt; wir geben hier eine etwas formalere Darstellung, diesmal für Polynomringe über einem beliebigen Ring.

Lemma 2.2.6 (Polynomdivision)**.** *Sei $g \in R[X] \setminus \{0\}$ mit Leitkoeffizient $\ell(g) \in \underline{R}^\times$. Dann gibt es für jedes $f \in R[X]$ eindeutig bestimmte $q, r \in R[X]$ mit $f = qg + r$ und* $\mathrm{grad}(r) < \mathrm{grad}(g)$.

Beweis. Sei $f = \sum_{i=0}^n a_i X^i$ mit $a_n \neq 0$ und $g = \sum_{j=0}^m b_j X^j$ mit $b_m \neq 0$. Nach Voraussetzung hat b_m ein multiplikativ Inverses b_m^{-1}. Die Existenz von $q, r \in R[X]$ zeigen wir mit Induktion nach n: für $n < m$ setze $q = 0$ und $r = f$. Für $n \geq m$ wenden wir die Induktionsannahme auf $f_1 := f - a_n b_m^{-1} X^{n-m} g$ an, welches kleineren Grad hat als f. Wir erhalten $q_1, r_1 \in R[X]$ mit $f_1 = q_1 g + r_1$ und $\mathrm{grad}(r_1) < m$. Dann ist

$$f = q_1 g + r_1 + a_n b_m^{-1} X^{n-m} g = (q_1 + a_n b_m^{-1} X^{n-m})g + r_1$$

wir haben also mit $q := q_1 + a_n b_m^{-1} X^{n-m}$ und $r := r_1$ die gesuchten Polynome gefunden.

Für die Eindeutigkeit, seien $q', r' \in R[X]$ mit $f = q'g + r'$ und $\mathrm{grad}(r') < \mathrm{grad}(g)$. Subtraktion liefert $(q' - q)g = r - r'$. Da $g \neq 0$ und $\ell(g)$ kein Nullteiler, gilt

$$\mathrm{grad}(q' - q) + \mathrm{grad}(g) = \mathrm{grad}(r - r').$$

Da $\mathrm{grad}(r) < m$ und $\mathrm{grad}(r') < m$, ist $\mathrm{grad}(r - r') < m$, also $\mathrm{grad}(q' - q) + \mathrm{grad}(g) < m$. Dies kann nur für $q' = q$ richtig sein. In diesem Fall folgt aber $r = r'$. □

Die folgenden Korollare wurde bereits in LA10 behandelt.

Korollar 2.2.7. *Ist $p \in R[X]$ und $a \in R$ mit $p(a) = 0$ (es ist a also eine Nullstelle von p), so ist $p = (X - a) \cdot q$ mit $q \in R[X]$.*

Korollar 2.2.8. *Ist R nullteilerfrei, so hat $p \in R[X] \setminus \{0\}$ höchstens $\operatorname{grad}(p)$ viele Nullstellen in R.*

2.2.3 Euklidische Ringe

Ringe, die die wichtige Eigenschaft von Polynomringen aus Lemma 2.2.6 teilen, haben einen Namen verdient.

Definition 2.2.9. Ein kommutativer nullteilerfreier Ring $\underline{R}$ heißt *euklidisch*, falls es eine Abbildung $\varphi\colon R \setminus \{0\} \to \mathbb{N}$ gibt, so dass es für beliebige $a, b \in R$ mit $b \neq 0$ Elemente $q, r \in R$ gibt mit $a = qb + r$ und $\varphi(r) < \varphi(b)$ oder $r = 0$. Die Funktion φ wird dann auch der *euklidische Betrag* oder die *euklidische Norm* genannt.

Beispiel 2.2.10. Körper sind trivialerweise euklidisch: der euklidische Betrag φ kann beliebig gewählt werden. Falls $\underline{K}$ ein Körper ist, dann zeigt Lemma 2.2.6, dass $\underline{K}[X]$ ein euklidischer Ring ist, mit der Gradfunktion für φ. Ein weiteres Beispiel für einen euklidischen Ring ist $\mathbb{Z}$, mit dem gewöhnlichen Betrag für φ. △

Wie in $\mathbb{Z}$ kann in einem euklidischen Ring $\underline{R}$ mit dem euklidischen Algorithmus zu $a_1, a_2 \in R$ ein größter gemeinsamer Teiler von a_1 und a_2 berechnet werden.

Satz 2.2.11 (Der euklidische Algorithmus)**.** *Sei $\underline{R}$ ein Ring mit euklidischem Betrag φ. Sei $a_1 \in R$ und $a_2 \in R \setminus \{0\}$. Definiere Elemente $a_3, a_4, \ldots$ induktiv wie folgt*

$$a_i = q_i a_{i+1} + a_{i+2} \text{ für } q_i \in R \text{ und } \varphi(a_{i+1}) < \varphi(a_{i+2})$$

bis $a_{n+1} = 0$. Dann gilt $a_n \in \operatorname{ggT}(a_1, a_2)$.

Beweis. Sei n so gewält, dass $a_n \neq 0$ und $a_{n+1} = 0$. Da $a_{n-1} = q_{n-1}a_n + a_{n+1}$, gilt $a_n | a_{n-1}$. Da $a_{n-2} = q_{n-2}a_{n-1} + a_n$, folgt daraus wiederum, dass $a_n | a_{n-2}$. Analog fahren wir so fort und erhalten $a_n | a_{n-3}, \ldots, a_n | a_1$. Also ist a_n ein gemeinsamer Teiler von a_1 und a_2. Falls $t \in R$ so, dass $t | a_1$ und $t | a_2$, dann $t | a_3$, $\ldots$, $t | a_n$. Also ist $a_n \in \operatorname{ggT}(a_1, a_2)$. □

Übung 55. Zeigen Sie, dass der Unterring $\mathbb{Z}[i]$ von $\mathbb{C}$ ein euklidischer Ring ist (die Elemente von $\mathbb{Z}[i]$ werden auch die *ganzen Gauß'schen Zahlen* genannt). Zeigen Sie dafür, dass $z \mapsto z\bar{z}$ einen euklidischen Betrag auf $\mathbb{Z}[i] \setminus \{0\}$ definiert.

2.2.4 Polynome in vielen Variablen

Sei $\underline{R}$ ein Ring. Wir werden häufig mit Polynomen über $\underline{R}$ in vielen Variablen arbeiten. Polynome über zwei Variablen X_1, X_2 sind definiert als $\underline{R}[X_1, X_2] := (\underline{R}[X_1])[X_2]$, und analog definieren wir induktiv die Menge $\underline{R}[X_1, \ldots, X_n]$ der Polynome über endlich vielen Variablen $X_1, \ldots, X_n$. Da wir $\underline{R}$ als Teilring von $\underline{R}[X_1]$ auffassen, und $\underline{R}[X_1]$ als

Teilring von $\underline{R}[X_1, X_2]$, so ist auch $\underline{R}$ ein Unterring von $\underline{R}[X_1, X_2]$. Jedes Element p von $\underline{R}[X_1, X_2]$ können wir schreiben als $\sum_{i=0}^{n} p_i X_2^i$ mit $p_0, \ldots, p_n \in R[X_1]$. Schreiben wir p_i in der Form $\sum_{j=0}^{m_i} a_{ij} X_1^j$ mit $a_{ij} \in R$, so erhalten wir für p die eindeutige Darstellung

$$p = \sum_{i,j \geq 0} a_{i,j} X_1^j X_2^i$$

mit höchstens endlich vielen von Null verschiedenen $a_{ij} \in R$. Analog haben Elemente $p \in \underline{R}[X_1, \ldots, X_n]$ eine eindeutige Darstellung der Gestalt

$$p = \sum_{i_1, \ldots, i_k \geq 0} a_{i_1, \ldots, i_k} X_1^{i_1} \ldots X_k^{i_k}.$$

Wir wollen allerdings auch Polynome in unendlich vielen Variablen betrachten. Dazu betrachten wir für eine beliebige Menge I die Menge $\mathbb{N}^{(I)}$ aller Abbildungen f von I nach $\mathbb{N}$, so dass $f(i) = 0$ für alle bis auf endlich viele $i \in I$. Die Abbildung, die konstant 0 ist, wird ebenfalls mit 0 bezeichnet. Wir definieren auf $\mathbb{N}^{(I)}$ die Addition $f + g$ komponentenweise, durch $(f + g)(i) := f(i) + g(i)$ für $i \in I$. Der Ring $R[X_i \mid i \in I]$ ist nun wie folgt definiert:

- die Grundmenge ist die Menge aller Funktionen a von $\mathbb{N}^{(I)}$ nach R, so dass $a(f) = 0$ für fast alle $f \in \mathbb{N}^{(I)}$.
- Für $a, b \in R[X_i \mid i \in I]$ definieren wir $(a + b)(f) := a(f) + b(f)$ und

$$(a \cdot b)(f) := \sum_{f_1 + f_2 = f} a(f_1) b(f_2).$$

Es sei δ_{fg} die Kroneckerfunktion auf $\mathbb{N}^{(I)}$, also $\delta_{fg} = 1$ falls $f = g$ und 0 sonst. Dann identifizieren wir $u \in R$ mit dem Element aus $R[X_i \mid i \in I]$, welches 0 auf u abbildet und alle übrigen Elemente von $\mathbb{N}^{(I)}$ auf 0 abbildet. Für $i \in I$ schreiben wir f_i für die Funktion $j \mapsto \delta_{ij}$, und X_i für das Element aus $R[X_i \mid i \in I]$, welches f_i auf 1 abbildet und alle übrigen Elemente von $\mathbb{N}^{(I)}$ auf 0 abbildet. Dann läßt sich jedes Element $a \in R[X_i \mid i \in I]$ schreiben als $\sum_{f \in \mathbb{N}^{(I)}} a(f) \prod_{i \in I} X_i^{f(i)}$. Diese Definition verallgemeinert die von oben: wir erhalten $\underline{R}[X_1, \ldots, X_n]$ mit Hilfe der neuen Definition für $I = \{1, \ldots, n\}$.

Bemerkung 2.2.12. Ganz analog zum Beweis von Lemma 2.2.3 erhalten wir auch für $\underline{R}[X_i \mid i \in I]$ den Begriff des Einsetzungshomomorphismus. Für jeden Ringhomomorphismus $\varphi\colon S \to R$ und jedes $a\colon I \to R$ gibt es genau einen Ringhomomorphismus $\varphi_a\colon S[X_i \mid i \in I] \to R$ mit $\varphi_a|_S = \varphi$ und $\varphi_a(X_i) = a(i)$.

Bemerkung 2.2.13. Es gibt für Polynomringe in vielen Variablen keine Entsprechung zur Polynomdivision 2.2.6, und wir werden später sehen, dass bereits der Ring $\mathbb{Q}[X_1, X_2]$ nicht euklidisch ist (Beispiel 2.4.34).

2.3 Integritätsringe

Ein nullteilerfreier kommutativer Ring $\underline{R}$ (mit Eins) mit mehr als einem Element heißt *Integritätsring* (auch: *Integritätsbereich*). Ein Ring $\underline{R}$ ist also genau dann ein Integritätsring, wenn $(R \setminus \{0\}, \cdot)$ ein kommutatives Monoid ist.

Bemerkung 2.3.1. Aus Lemma 2.1.4 folgt, dass in einem Integritätsring $\underline{R}$ für alle $a, b, c \in R$ mit $ab = ac$ gilt, dass $a = 0$ or $b = c$; sprich, wir können kürzen, wie wir das von Körpern kennen.

Beispiel 2.3.2. Offenbar sind alle Körper $\mathbb{K}$ und der Ring $\mathbb{Z}$ Integritätsringe. Falls $\underline{R}$ ein Integritätsring ist, dann auch $\underline{R}[X_1, \ldots, X_n]$. Denn wenn n und m die Grade von Polynomen $\varphi \in \underline{R}[X]$ und $\psi \in \underline{R}[X]$ sind, dann ist $n + m$ der Grad von $\varphi \cdot \psi \in \underline{R}[X]$, und daher gibt es keine nicht-trivialen Nullteiler. △

Bemerkung 2.3.3. Jeder Unterring eines Körpers ist ein Integritätsring.

2.3.1 Teilbarkeitsregeln

Zwei Elemente a, b eines Ringes $\underline{R}$ heißen *assoziiert*, wenn $a|b$ und $b|a$; wir schreiben dann $a \sim b$. Offenbar definiert Assoziiertheit eine Äquivalenzrelation auf R.

Bemerkung 2.3.4. In einem Integritätsring sind zwei Elemente a, b genau dann assoziiert, wenn es eine Einheit $u \in R^\times$ gibt mit $a = ub$. Denn falls es $u, v \in R$ gibt mit $a = ub$ und $vu = 1$, dann gilt $a|b$, da aber $va = b$, gilt auch $b|a$. Umgekehrt seien $c, d \in R$ so, dass $b = ca$ und $a = db$. Dann folgt $a = db = dca$, also wegen der Kürzungsregel (Bemerkung 2.3.1) folgt, dass $a = 0$ oder $dc = 1$. Falls $a = 0$, dann ist auch $b = ca = 0$, und $a \sim b$. Falls $dc = 1$, sind $d, c \in R^\times$, und wieder folgt $a \sim b$.

Wenn größte gemeinsame Teiler existieren (siehe Abschnitt 2.1), so sind sie bis auf Multiplikation mit einer Einheit eindeutig, wie das folgende Lemma zeigt.

Lemma 2.3.5. *Ist $d \in \mathrm{ggT}(M)$ für $M \subseteq R$ nicht leer, dann gilt*

$$\begin{aligned}\mathrm{ggT}(M) &= \{a \mid a \sim d\} \\ &= \{ud \mid u \in R^\times\}.\end{aligned}$$

Beweis. Sei $d' \in \mathrm{ggT}(M)$. Dann gilt $d|d'$ und $d'|d$, also $d \sim d'$. Die zweite Gleichung folgt aus Bemerkung 2.3.4. □

2.3.2 Der Quotientenkörper

Wir werden im folgenden sehen, dass sich aus jedem Integritätsring $\underline{R}$ ein Körper $\underline{K}$ gewinnen lässt, der $\underline{R}$ als Unterring enthält, der sogenannte *Quotientenköper* (auch *Körper der Brüche* genannt). Es folgt dann, dass ein Ring genau dann ein Integritätsring ist, wenn er isomorph ist zu einem Unterring eines Körpers.

Sei $\sim$ die Äquivalenzrelation[1] auf $R \times (R \setminus \{0\})$ die definiert wird durch $(a, s) \sim (a', s')$ genau dann wenn

$$as' = a's.$$

Wir schreiben $\frac{a}{s}$ für die Äquivalenzklasse von (a, s).

Definition 2.3.6. Sei $\underline{R}$ ein kommutativer Integritätsring. Der *Quotientenkörper von* $\underline{R}$ ist der Ring $\underline{Q} = \mathrm{Quot}(R)$ mit Grundmenge

$$Q := (R \times (R \setminus \{0\})/_\sim$$

in dem die Multiplikation definiert wird durch

$$\frac{a}{s}\frac{a'}{s'} := \frac{aa'}{ss'}.$$

Man rechnet leicht nach, dass dies wohldefiniert ist, und dass die Multiplikation ein Einselement hat, nämlich $\frac{1}{1}$, und assoziativ ist. Addition wird definiert durch

$$\frac{a}{s} + \frac{a'}{s'} := \frac{s'a + sa'}{ss'}.$$

Auch hier rechnet man die Wohldefiniertheit leicht nach, dass $\frac{0}{1}$ ein neutralen Element bezüglich der Addition ist, und dass Addition und Mulitplikation auch sonst die Körperaxiome erfüllen.

Bemerkung 2.3.7. Die Abbildung $f\colon R \to Q$, die gegeben ist durch $f(a) := \frac{a}{1}$, ist ein injektiver Ringhomomorphismus. Jedes Element von $f(R)$ hat ein Inverses in Q: das Inverse von $\frac{s}{1}$ ist $\frac{1}{s}$. Wir identifizieren die Elemente von R mit ihren Bildpunkten in Q unter f, und betrachten also $\underline{R}$ als einen Unterring von $\underline{Q}$.

Bemerkung 2.3.8. Ist R der Unterring eines Körpers K, so ist $\mathrm{Quot}(R)$ isomorph zu einem Teilkörper von K via $\frac{a}{b} \mapsto a \cdot b^{-1}$. Wir identifizieren $\mathrm{Quot}(R)$ dann mit diesem Teilkörper.

Beispiel 2.3.9. $(\mathbb{Q}; +, \cdot)$ ist der Quotientenkörper von $(\mathbb{Z}; +, \cdot)$. △

Beispiel 2.3.10. Falls $\underline{K}$ der Quotientenkörper von $\underline{R}$ ist, dann bezeichnen wir den Quotientenkörper von $\underline{R}[X_1, \ldots, X_n]$ mit $\underline{K}(X_1, \ldots, X_n)$; seine Elemente heißen *rationale Funktionen*. Jede rationale Funktion kann geschrieben werden als $\frac{\varphi}{\psi}$ für Polynome $\varphi, \psi \in \underline{R}[X_1, \ldots, X_n]$. △

2.4 Ideale

Ideale sind die ringtheoretische Entsprechung von Normalteilern in der Gruppentheorie. Für $I \subseteq R$ und $r \in R$ schreiben wir rI für $\{ru \mid u \in I\}$ und Ir für $\{ur \mid u \in I\}$.

[1] Äquivalenzrelation werden häufig mit dem Symbol $\sim$ bezeichnet; hier allerdings nicht zu verwechseln mit Assoziiertheit aus Abschnitt 2.3.1, für welche wir ebenfalls $\sim$ verwenden.

Definition 2.4.1 (Ideal)**.** Eine Teilmenge $I \subseteq R$ heißt *Ideal von* $\underline{R}$, in Zeichen $I \trianglelefteq \underline{R}$, falls

- $rI \subseteq I$ und $Ir \subseteq I$ für alle $r \in R$, und
- $(I; +)$ ist eine Untergruppe von $(R; +)$.

Die folgenden Bemerkungen erklären, warum Ideale eine zentrale Rolle beim Studium von Ringen spielen.

Bemerkung 2.4.2. Jeder Ring hat

- das Ideal $\{0\}$, das *Nullideal*, und
- das Ideal R, das *triviale Ideal*. Von R verschiede Ideale heißen *echte Ideale*.

Ein Ideal von $\underline{R}$ ist genau dann das triviale Ideal, wenn es die 1 enthält.

Bemerkung 2.4.3. Ein Ideal ist genau dann ein Unterring, wenn es trivial ist: denn Unterringe müssen nach Definition 2.0.3 die 1 enthalten, und umgekehrt ist das triviale Ideal trivialerweise ein Unterring. Es ist also kein echtes Ideal ein Unterring. Umgekehrt ist beispielsweise $\mathbb{Z}$ ein Unterring von $\mathbb{Q}$, der kein Ideal ist.

Wir erinnern uns aus LA20, dass jeder Ring $\underline{R}$ als $\underline{R}$-Modul betrachtet werden kann. Die Ideale von $\underline{R}$ sind dann genau die Grundmengen von Untermoduln von $\underline{R}$.

Bemerkung 2.4.4. Sind $I, J \trianglelefteq \underline{R}$, so sind auch $I + J \trianglelefteq \underline{R}$ und $I \cap J \trianglelefteq \underline{R}$. Allgemeiner ist der Schnitt von Familien $(I_i)_{i \in F}$ von Idealen von $\underline{R}$ wieder ein Ideal von $\underline{R}$. Insbesondere existiert zu jeder Teilmenge $A \subseteq R$ ein kleinstes Ideal (A) von $\underline{R}$, das A enthält. Es gilt

$$(A) = \left\{ \sum_{i=1}^{n} r_i a_i \mid n \in \mathbb{N}, r_i \in R, a_i \in A \right\}.$$

Bemerkung 2.4.5. Für jeden Ringhomomorphismus $h \colon \underline{R} \to \underline{S}$ ist der Kern von h

$$K := \{r \in R \mid h(r) = 0\}$$

ein Ideal:

- K ist eine Untergruppe von $(R, +)$ da f ein Gruppenhomomorphismus ist (i.e., ein Homomorphismus von $(R; +, 0)$ nach $(S; +, 0)$);
- Falls $x \in K$ und $r \in R$, dann ist auch $rx \in K$, da $f(rx) = f(r)f(x) = f(r) \cdot 0 = 0$.

Die folgende Bemerkung zeigt, dass jedes Ideal I von $\underline{R}$ der Kern ist eines geeignet gewählten Ringhomomorphismus.

Bemerkung 2.4.6 (Faktorringe). Für jedes Ideal I von $\underline{R}$ ist auf

$$R/I = \{a + I \mid a \in R\}$$

durch Komplexaddition und Komplexmultiplikation ein Ring $\underline{R}/I$ definiert.[2] Der Homomorphismus $h\colon \underline{R} \to \underline{R}/I$, der r auf $r+I$ abbildet, wird der *kanonische Homomorphismus von $\underline{R}$ nach $\underline{R}/I$* genannt.

Übung 56. Es sei $\varphi\colon R \to S$ ein surjektiver Ringhomomorphismus. Zeigen Sie, dass $R/\operatorname{Kern}(\varphi) \cong S$.

Übung 57. Zeigen Sie, dass ein Ideal genau dann das Einheitsideal ist, wenn es eine Einheit enthält.

Übung 58. Beschreiben Sie explizit die Addition und Multiplikation im Ring $R[X]/(X^2)$.

2.4.1 Hauptideale

Für jedes $a \in R$ ist $Ra = aR = (\{a\})$ ein Ideal von $\underline{R}$, das *durch a erzeugte Hauptideal von $\underline{R}$*. Es wird mit (a) bezeichnet.

Beispiel 2.4.7. $(0) = \{0\}$, das *Nullideal*, ist ein Hauptideal. △

Beispiel 2.4.8. $(1) = R$, das *triviale Ideal* oder *Einheitsideal*, ist ein Hauptideal. △

Bemerkung 2.4.9. Für Elemente a, b eines kommutativen Ringes sind äquivalent:

- $b \in (a)$,
- $a|b$,
- $(b) \subseteq (a)$.

Beispiel 2.4.10. Für $\underline{R} = \mathbb{Z}$, $a = 2$, und $b = 4$, gilt $4 \in (2) = \{0, 2, -2, 4, -4, \dots\}$ und $(2) \supseteq (4) = \{0, 4, -4, 8, -8, \dots\}$. △

Beispiel 2.4.11. Sei $\underline{R}$ ein Ring. Dann besteht das Ideal (X) des Polynomrings $\underline{R}[X]$ aus der Menge aller $p \in \underline{R}[X]$, bei denen der konstanten Koeffizient gleich Null ist. Sei h der kanonische Homomorphismus von $\underline{R}[X]$ nach $\underline{R}[X]/(X)$, der gegeben durch $h(f) := f + (X)$ für $f \in \underline{R}[X]$. Dann ist die Einschränkung von h auf $\underline{R}$ ein Isomorphismus zwischen $\underline{R}$ und $\underline{R}[X]/(X)$: jedes Element von $\underline{R}[X]/(X)$ kann geschrieben werden als $p + (X)$, wobei $p \in \underline{R}[X]$. Sei u der konstante Koeffizient von p. Dann ist $p + (X) = u + (X)$, und $h(u) = u + (X)$. Also ist h' surjektiv. Es ist h' auch injektiv, da $u + (X) = v + (X)$ impliziert, dass $u = v$. Es gilt also

$$\underline{R} \cong \underline{R}[X]/(X).$$ △

Proposition 2.4.12. *Ein kommutativer Ring $\underline{R}$ ist genau dann ein Körper, wenn $\{0\}$ und $\underline{R}$ die einzigen Ideale von $\underline{R}$ sind.*

[2] Der Faktorring wird häufig auch Quotientenring genannt; der Begriff darf nicht verwechselt werden mit dem Quotientenkörper aus Definition 2.3.6, welcher daher auch *Körper der Brüche* genannt wird.

Beweis. Genau dann ist $\underline{R}$ ein Körper, wenn jedes Element von $R \setminus \{0\}$ eine Einheit ist. Falls $\underline{R}$ ein Körper ist, dann enthält jedes nicht-triviale Ideal I eine Einheit u mit Inversem v. Dann gilt für jedes $r \in R$, dass

$$r = r(vu) = (rv)u \in I$$

also $R = I$. Umgekehrt, falls $\{0\}$ und R die einzigen Ideale von $\underline{R}$ sind, dann betrachten wir $u \in R \setminus \{0\}$. Nach Annahme ist $(u) = R$ und daher $1 \in (u)$. Also gibt es ein $v \in R$ mit $1 = uv$, und u ist eine Einheit. □

Für jede endliche Familie $\{I_j\}_{j \in A}$ von Idealen von $\underline{R}$ ist die Summe $\sum_{j \in A} I_j$ ein Ideal von $\underline{R}$. Falls $A \subseteq R$, dann ist $\sum_{a \in A}(a) = (A)$ das kleinste Ideal von $\underline{R}$, das A enthält (siehe Bemerkung 2.4.4). Falls $A = \{a_1, \ldots, a_n\}$ wird dieses mit $(a_1, \ldots, a_n)$ bezeichnet.

Definition 2.4.13. Ein Integritätsring $\underline{R}$ heißt *Hauptidealring* (auch *Hauptidealbereich*), falls jedes Ideal von $\underline{R}$ ein Hauptideal ist.

Offenbar sind Körper Hauptidealringe (siehe Proposition 2.4.12). Weitere Beispiele für Hauptideale gewinnen wir aus folgender Proposition.

Proposition 2.4.14. *Jeder euklidische Ring ist ein Hauptidealring.*

Beweis. Es sei $\underline{R}$ ein euklidischer Ring und $\varphi\colon R \setminus \{0\} \to \mathbb{N}$ ein euklidischer Betrag. Es sei $I \neq (0)$ ein Ideal von $\underline{R}$. Wähle $b \in I \setminus \{0\}$ so, dass $\varphi(b)$ kleinstmöglich. Dann gilt $(b) \subseteq I$. Wir zeigen, dass auch umgekehrt $I \subseteq (b)$: zu jedem $a \in I$ existieren $q, r \in R$ mit $a = qb + r$ und $r = 0$ oder $\varphi(r) < \varphi(b)$. Wegen $r = a - qb \in I$ und der Minimalitätseigenschaft von b ist der zweite Fall nicht möglich, so dass $r = 0$ und $a = qb \in (b)$. □

Beispiel 2.4.15. Aus Proposition 2.4.14 folgt, dass $\mathbb{Z}$ und für jeden Körper $\underline{K}$ auch der Polynomring $\underline{K}[X]$ Hauptidealringe sind, da diese Ringe euklidisch sind (Beispiel 2.2.10). △

Abbildung 2.1 gibt einen Überblick über wichtige Eigenschaften von Ringen (manche davon werden erst im weiteren Verlauf vorgestellt), zusammen mit Beispielen, die zeigen, dass die dargestellte Kette von Inklusionen strikt ist.

Beispiel 2.4.16. $\mathbb{Z}[X]$ ist zwar ein Integritätsring, aber *kein* Hauptidealring: zum Beispiel ist das Ideal $(2, X)$ kein Hauptideal. Denn angenommen, es gäbe ein $a \in \mathbb{Z}[X]$, so dass $(2, X) = (a)$. Da $2 \in (a)$, muss es ein $r \in \mathbb{Z}[X]$ geben so dass $2 = ra$. Der Grad von ra ist gleich dem Grad von r plus dem Grad von a. Also ist r ein konstantes Polynom, und daher ein Element von $\mathbb{Z}$. Da 2 prim ist, ist $a \in \{-2, -1, 1, 2\}$. Falls $a \in \{-1, 1\}$, dann wäre jedes Polynom ein Vielfaches von a, im Widerspruch zu $(a) \neq R$. Falls $a \in \{-2, 2\}$, dann $X \in (a) = (2) = (-2)$, und daher $X = 2q$ für ein $q \in \mathbb{Z}[X]$, was unmöglich ist. Wir werden später diese Aussage mit Hilfe von allgemeinerer Aussagen herleiten (Beispiel 2.4.33). △

Übung 59. Zeigen Sie, dass $u \in R$ genau dann eine Einheit ist, wenn $(u) = R$.

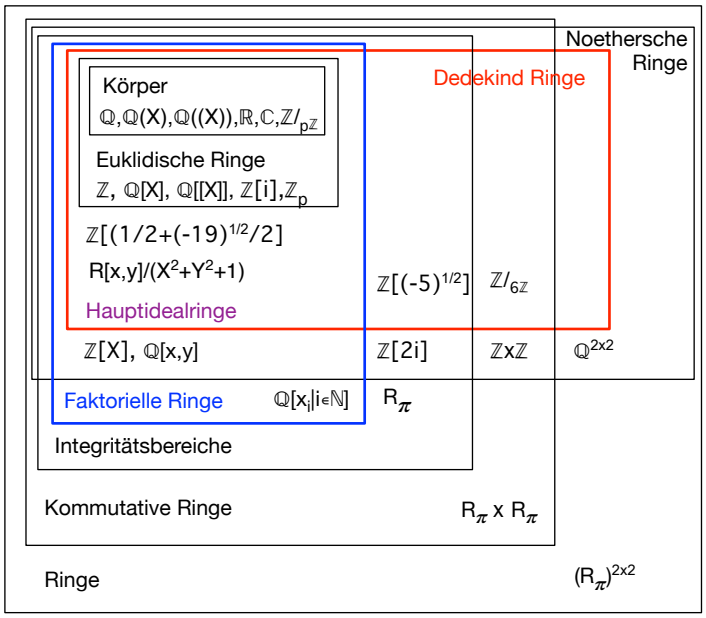


Abbildung 2.1: Wichtige Eigenschaften und Beispiele von Ringen.

Lemma 2.4.17. *Seien a, b Elemente eines Hauptidealringes R. Dann gibt es $t \in \mathrm{ggT}(a,b)$ und $v \in \mathrm{kgV}(a,b)$, und es gilt $(a)+(b)=(t)$ und $(a)\cap(b)=(v)$.*

Beweis. Da R Hauptidealring ist, existiert ein $t \in R$ mit $(t)=(a)+(b)$. Es folgt $(a)\subseteq(t)$, $(b)\subseteq(t)$, und somit $t|a$ und $t|b$. Gilt $s|a$ und $s|b$, so folgt $(t)=(a)+(b)\subseteq(s)$, also $s|t$. Daher ist $t \in \mathrm{ggT}(a,b)$.

Da R Hauptidealring ist, existiert ein $v \in R$ mit $(v)=(a)\cap(b)$. Wegen $(v)\subseteq(a)$ gilt $a|v$, und analog $b|v$. Ist $u \in R$ mit $a|u$ und $b|u$, so folgt $(u)\subseteq(a)\cap(b)=(v)$, also $v|u$. Daher ist $v \in \mathrm{kgV}(a,b)$. □

Für $\underline{R}=\mathbb{Z}$ wird die folgende Aussage auch das *Lemma von Bézout* genannt.

Korollar 2.4.18. *Sei R ein Hauptidealring und $a, b \in R$. Dann gibt es $x, y \in R$, so dass $xa+yb \in \mathrm{ggT}(a,b)$.*

Beweis. Nach Lemma 2.4.17 gilt $(a)+(b)=(t)$ für ein $t \in \mathrm{ggT}(a,b)$. □

Übung 60. Seien $p \in \mathbb{N}$ eine Primzahl, und $a, b \in \mathbb{Z}$. Zeigen Sie: $p|ab$ impliziert $p|a$ oder $p|b$.

Übung 61. Zeigen Sie, dass im Ring $\mathbb{Z}$ gilt, dass $(6,8)=(2)$.

Übung 62. Der Ring $R[X,Y]/(X^2+Y^2+1)$ ist ein Hauptidealring, aber nicht euklidisch (schwer).

Übung 63. Die invertierbaren Elemente eines Rings bilden bezüglich der Multiplikation eine Gruppe, die *Einheitengruppe*. Zeigen Sie:

- Die Einheitengruppe von $\mathbb{Z}/8\mathbb{Z}$ is isomorph zu $(\mathbb{Z}/2\mathbb{Z})^2$.
- Die Einheitengruppe eines endlichen Körpers mit n Elementen ist isomorph zu $\mathbb{Z}/(n-1)\mathbb{Z}$.
- Die Einheitengruppe von $\mathbb{Z}[\sqrt{-1}] = \mathbb{Z}[i] \leq \mathbb{C}$ ist $\{-1, +1, i, -i\}$.
- Sei $d < -1$. Dann ist die Einheitengruppe von $\mathbb{Z}[\sqrt{d}] \leq \mathbb{C}$ gleich $\{-1, 1\}$.
- Die Einheitengruppe von $\mathbb{Z}[\sqrt{2}]$ ist unendlich.

2.4.2 Primideale

Primzahlen haben die folgende wichtige Eigenschaft: teilt eine Primzahl p ein Produkt ab ganzer Zahlen a, b, so teilt p wenigstens einen der Faktoren a oder b (Übung 60). Das motiviert die folgende Definition.

Definition 2.4.19 (Primideale und Primelemente)**.** Ein Ideal I von $\underline{R}$ heißt *Primideal* (oder *prim*) falls $I \neq R$, und für alle $a, b \in R$ mit $ab \in I$ ist auch $a \in I$ oder $b \in I$. Ein Element $r \in R$ heisst *prim in* $\underline{R}$ (oder *Primelement von* $\underline{R}$) falls das Ideal (r) von $\underline{R}$ prim ist.

Beispiel 2.4.20. Die Primideale von $\mathbb{Z}$ sind (0) und die Ideale der Gestalt (p), für p eine Primzahl. △

Bemerkung 2.4.21. Falls a eine Einheit, dann ist $(a) = R$ nicht prim (siehe Übung 59).

Übung 64. In Integritätsringen R gilt: p ist genau dann prim, wenn für alle $x, y \in R$ gilt, dass aus $p|xy$ folgt, dass $p|x$ oder $p|y$.

Proposition 2.4.22. *Ein Ideal I eines Rings $\underline{R}$ ist genau dann prim, wenn $\underline{R}/I$ ein Integritätsring ist.*

Beweis. Sei I ein Primideal. Dann ist $\underline{R}/I \neq \{I\}$, da $I \neq R$. Also hat $\underline{R}/I$ mehr als ein Element. Um zu zeigen, dass $\underline{R}/I$ keine nicht-trivialen Nullteiler hat, betrachten wir $A = a + I \in \underline{R}/I$ und $B = b + I \in \underline{R}/I$ so dass $AB = 0$. Das bedeutet, dass $(a + I)(b + I) = ab + I = I$, also $ab \in I$. Da I prim, gilt $a \in I$ oder $b \in I$. Also ist $A = 0$ oder $B = 0$. Damit ist $\underline{R}/I$ nullteilerfrei, und daher auch ein Integritätsring.

Umgekehrt: angenommen $\underline{R}/I$ ist Integritätsring. Dann muss $\underline{R}/I$ mehr als ein Element haben, und $I \neq R$. Sei $ab \in I$. Dann ist $0 = I = (ab) + I = (a + I)(b + I)$, also $a + I = 0$ oder $b + I = 0$, also $a \in I$ oder $b \in I$. □

Sei $\underline{R}$ ein kommutativer Ring. Dann ist die Abbildung $h\colon \mathbb{Z} \to R$, die gegeben ist durch

$$h(n) := \underbrace{1 + \cdots + 1}_{n \text{ times}},$$

ein Ringhomomorphismus. Der Kern von h ist das Ideal $(n) = n\mathbb{Z}$. Falls (n) ein Primideal ist, dann gilt $n = 0$ or $n = p$ für eine Primzahl p.

- Im ersten Fall hat $\underline{R}$ einen Unterring, der isomorph ist zu $\mathbb{Z}$, und wir sagen, dass $\underline{R}$ *Charakteristik* 0 besitzt (in Symbolen: $\mathrm{char}(\underline{R}) = 0$).
- Im zweiten Fall $n = p$ hat $\underline{R}$ einen Unterring isomorph zu $\mathbb{Z}/n\mathbb{Z}$, und wir sagen, dass $\underline{R}$ *Charakteristik* p besitzt (in Symbolen: $\mathrm{char}(\underline{R}) = p$).

Falls $\underline{K}$ ein Körper ist, dann hat $\underline{K}$ Charakteristik 0 or $p > 0$. Im ersten Fall enthält $\underline{K}$ eine (eindeutig bestimmte) isomorphe Kopie[3] von $\mathbb{Q}$, und im zweiten Fall eine (eindeutig bestimmte) isomorphe Kopie von $\mathbb{F}_q$. In beiden Fällen heißt der entsprechende Teilkörper der *Primkörper* (von $\underline{K}$).

Übung 65. Es sei K ein Körper, $a \in K$ und $f \in K[X]$, so dass $f(a) \neq 0$. Dann gilt für alle $n \in \mathbb{N}$, dass $nf := \underbrace{f + \cdots + f}_{n \text{ mal}}$ genau dann von $(X - a)$ geteilt wird, wenn $\mathrm{char}(K) | n$.

2.4.3 Irreduzible Elemente

Sei $\underline{R}$ ein Integritätsring.

Definition 2.4.23. Es sei $r \in R \setminus \{0\}$ keine Einheit. Dann heißt r

- *irreduzibel in* $\underline{R}$ (auch: *unzerlegbar in* $\underline{R}$), falls aus $r = ab$ für $a, b \in R$ folgt, dass a oder b eine Einheit in $\underline{R}$ ist,
- *reduzibel in* $\underline{R}$ (auch: *zerlegbar in* $\underline{R}$), wenn r nicht irreduzibel ist, also falls $r = ab$ für $a, b \in R \setminus R^\times$.

Bemerkung 2.4.24. Falls $r \in R$ eine Einheit oder 0 ist, so nennen wir r weder reduzibel noch irreduzibel.

Beispiel 2.4.25. Die irreduziblen Elemente von $\mathbb{Z}$ sind genau die Zahlen $\{p \mid p \text{ prim}\} \cup \{-p \mid p \text{ prim}\}$, und dies sind auch genau die Primelemente von $\mathbb{Z}$. △

Beispiel 2.4.26. Das Polynom $X^2 - 1 \in \mathbb{Z}[X]$ ist reduzibel, da $X^2 - 1 = (X - 1)(X + 1)$, und die Faktoren $X - 1$ und $X + 1$ in $\mathbb{Z}[X]$ keine Einheiten sind. △

Beispiel 2.4.27. Sei $a \in K$. Dann ist das Polynom $X - a$ in $K[X]$ irreduzibel: denn falls $f, g \in K[X]$ so, dass $fg = (X - a)$, dann gilt $\mathrm{grad}(f) + \mathrm{grad}(g) = \mathrm{grad}(X - a) = 1$. Dann muss gelten $\mathrm{grad}(f) = 0$ oder $\mathrm{grad}(g) = 0$, also ist f oder g eine Einheit. △

Proposition 2.4.28. *Jedes Primelement eines Integritätsrings ist irreduzibel.*

Beweis. Angenommen, $(p) \neq \{0\}$ ist ein Primideal und $p = ab$. Dann ist $ab = p \in (p)$, und nach der Definition von Primidealen gilt $a \in (b)$ oder $b \in (p)$. Falls $a \in (p)$, dann gilt $a = pr$ für ein $r \in R$. Daraus folgt, dass $p = ab = prb$, also $rb = 1$ (Lemma 2.1.4) und b ist eine Einheit. Falls $b \in (p)$ zeigt man analog, dass a eine Einheit ist. Also ist p irreduzibel. □

[3] Mit einer *isomorphen Kopie* eines Körpers K in einem Körper L ist ein Teilkörper von L gemeint, der isomorph zu K ist.

Wir werden im nächsten Abschnitt eine Umkehrung dieser Aussage in Hauptidealringen kennenlernen (Proposition 2.4.31). Im allgemeinen gilt die Umkehrung nicht, wie wir in Beispiel 2.5.2 sehen werden.

2.4.4 Maximale Ideale

Ein Ideal I von $\underline{R}$ heißt *maximal* falls $I \neq R$ und falls es kein Ideal $J \neq R$ gibt, welches I echt enthält.

Proposition 2.4.29. *Ein Ideal I eines kommutativen Rings $\underline{R}$ ist genau dann maximal, wenn $\underline{R}/I$ ein Körper ist.*

Beweis. Nach Proposition 2.4.12 ist $\underline{R}/I$ genau dann ein Körper, wenn $\{0\}$ das einzige echte Ideal von $\underline{R}/I$ ist. Es ist J genau dann ein Ideal von $\underline{R}/I$, wenn $\bigcup J$ ein Ideal von $\underline{R}$ ist, welches I enthält; also ist I genau dann maximal, wenn $\{0\}$ das einzige echte Ideal von $\underline{R}/I$ ist. □

Korollar 2.4.30. *Jedes maximale Ideal eines kommutativen Rings $\underline{R}$ ist prim.*

Beweis. Ist I ein maximales Ideal, so ist $\underline{R}/I$ ein Körper (Proposition 2.4.29), also inbesondere ein Integritätsring. Proposition 2.4.22 impliziert daher, dass I prim ist. □

In Hauptidealringen hat diese Aussage eine Umkehrung. Wir beweisen auch gleich die bereits angekündigte Umkehrung von Proposition 2.4.28 für Hauptidealringe.

Proposition 2.4.31. *Sei $\underline{R}$ ein Hauptidealring und sei $I = (p) \neq \{0\}$ ein Ideal. Dann sind äquivalent.*

1. *p ist prim;*
2. *p ist irreduzibel;*
3. *I ist maximal;*
4. *I ist prim.*

Beweis. (1) $\Rightarrow$ (2) folgt aus Proposition 2.4.28.

Für (2) $\Rightarrow$ (3) sei p irreduzibel. Falls I ein Ideal von $\underline{R}$ ist, welches (p) enthält, then ist I nach Annahme ein Hauptideal, also $I = (m)$ für ein $m \in R$. Da $p \in (m)$, gibt es ein $r \in R$ so dass $p = rm$. Aber p ist irreduzibel, und so ist nach Definition r oder m eine Einheit. Falls r eine Einheit ist, dass gilt $(p) = (m)$, und falls m eine Einheit ist, dass gilt $(m) = R$. Es folgt, dass I maximal ist.

(3) $\Rightarrow$ (4) folgt aus Korollar 2.4.30.

(4) $\Rightarrow$ (1) gilt per Definition. □

Korollar 2.4.32. *Sei $\underline{R}$ ein kommutativer Ring, so dass $\underline{R}[X]$ ein Hauptidealring ist. Dann ist $\underline{R}$ ein Körper.*

Beweis. Per Annahme ist $\underline{R}[x]$ insbesondere ein Integritätsring, und daher ist auch $\underline{R}$ ein Integritätsring. Proposition 2.4.22 impliziert also, dass das nicht-triviale Ideal (X) in $\underline{R}[X]$ prim ist, da $\underline{R}[X]/(X)$ isomorph ist zum Integritätsring $\underline{R}$ (siehe Beispiel 2.4.11). Proposition 2.4.31 impliziert, dass (X) maximal ist. Also ist $\underline{R}[X]/(X)$ ein Körper nach Proposition 2.4.29. □

Beispiel 2.4.33. Es folgt, dass $\mathbb{Z}[X]$ kein Hauptidealring ist, denn $\mathbb{Z}$ ist ein kommutativer Ring, aber kein Körper. △

Beispiel 2.4.34. Es folgt, dass $\mathbb{Q}[X,Y]$ kein Hauptidealring ist: denn $\mathbb{Q}[X,Y] = \underline{R}[Y]$ für $\underline{R} := \mathbb{Q}[X]$, allerdings ist $\underline{R}$ kein Körper. △

Der Beweis der nächsten Aussage verwendet das Lemma von Zorn (siehe LA20).

Satz 2.4.35 (Existenz maximaler Ideale)**.** *Jedes echte Ideal I von $\underline{R}$ ist in einem maximalen Ideal von $\underline{R}$ enthalten.*

Beweis. Die Menge $\mathcal{A}$ aller echten Ideale J von $\underline{R}$ mit $I \subseteq J$ ist wegen $I \in \mathcal{A}$ nicht leer und eine geordnete Menge bezüglich Inklusion. Sei $\mathcal{K} \subseteq \mathcal{A}$ eine Kette in $\mathcal{A}$, d.h., falls $B, B' \in \mathcal{K}$, dann ist $B \subseteq B'$ oder $B' \subseteq B$. Dann ist $C := \bigcup \mathcal{K}$ offenbar ebenfalls ein Ideal von $\underline{R}$. Da $1 \notin B$ für alle $B \in \mathcal{K}$ (siehe Bemerkung 2.4.2), ist $1 \notin \bigcup \mathcal{K} = C$, also ist C ein echtes Ideal von $\underline{R}$ und damit eine obere Schranke von $\mathcal{K}$ in $\mathcal{A}$. Somit ist das Lemma von Zorn anwendbar, und liefert ein maximales Ideal M von $\underline{R}$, welches I enthält. □

Proposition 2.4.36. *Sei $\underline{K}$ ein Körper und $p \in \underline{K}[X]$ irreduzibel. Dann ist $\underline{K}[X]/(p)$ ein Körper.*

Beweis. Da p irreduzibel ist, so ist das Ideal (p) des Hauptidealrings $\underline{K}[X]$ maximal nach Proposition 2.4.31. Also ist $\underline{K}[X]/(p)$ ein Körper nach Proposition 2.4.29. □

2.5 Faktorielle Ringe

Jedes Element von $\mathbb{N} \setminus \{0\}$ lässt sich schreiben als Produkt von Primzahlen; viele Integritätsringe teilen diese Eigenschaft, die einen Namen verdient hat. Ein Integritätsring $\underline{R}$ heißt *faktoriell*[4], wenn jedes $a \in R \setminus (R^\times \cup \{0\})$ ein Produkt von Primelementen ist.

Proposition 2.5.1. *Jeder Hauptidealring ist faktoriell.*

Beweis. Sei $\underline{R}$ ein Hauptidealring und $a \in R \setminus (\{0\} \cup R^\times)$. Ist a prim, so ist nichts zu zeigen. Andernfalls ist a reduzibel (Proposition 2.4.31) und kann geschrieben werden als $a = bc$ für $b, c \in R \setminus R^\times$. Das gleiche Argument kann man dann für b und für c wiederholen, so dass nur zu zeigen bleibt, dass das Verfahren nach endlich vielen Schritten abbricht. Sei $(a_1) \subseteq (a_2) \subseteq \cdots$ eine aufsteigende Folge von Hauptidealen in $\underline{R}$. Dann ist $A := \bigcup_{i \in \mathbb{N}} (a_i)$ ein Ideal, also nach Annahme ein Hauptideal, also von der Gestalt $A = (a)$ für ein $a \in R$. Also gibt es ein $i \in \mathbb{N}$, so dass $a \in (a_i)$. Dann gilt $(a_i) = (a_j) = A$ für alle $j \geq i$. □

[4] Auch *'Gaußscher Ring'*; im Englischen *'unique factorization domain'*.

Beispiel 2.5.2. Der Unterring $R = \mathbb{Z}[\sqrt{-5}] = \{a + b\sqrt{-5} \mid a, b \in \mathbb{Z}\}$ von $\mathbb{C}$ (siehe Bemerkungen 2.0.4 und 2.2.5) ist ein Integritätsring (siehe Bemerkung 2.3.3), aber nicht faktoriell: wir werden unzerlegbare Elemente angeben, die keine Primelemente sind.

Die Abbildung $z \mapsto \bar{z}$ (komplexe Konjugation) ist ein Automorphismus von R (zur Erinnerung: $\overline{a + b\sqrt{-5}} = a - b\sqrt{-5}$). Wir definieren $N\colon R \to \mathbb{N}$ durch $z \mapsto z\bar{z}$. Es ist also $N(a + b\sqrt{-5}) = (a^2 - 5b^2)$. Für $u, v \in R$ gilt $N(uv) = uv\overline{uv} = u\bar{u}v\bar{v} = N(u)N(v)$. Es ist $u \in R$ genau dann eine Einheit, wenn $N(u) = 1$: denn wenn es ein $v \in R$ gibt mit $uv = 1$, dann haben wir

$$1 = N(1) = N(uv) = N(u)N(v)$$

also $N(u) = 1$. Umgekehrt folgt aus $N(u) = u\bar{u} = 1$ direkt, dass u eine Einheit ist.

Behauptung 1. Das Element $3 \in R$ ist kein Primelement in R. Wir haben $3|9$ und $9 = (2 + \sqrt{-5})(2 - \sqrt{-5})$. Allerdings teilt 3 weder $2 + \sqrt{-5}$ noch $2 - \sqrt{-5}$.

Behauptung 2. Das Element $3 \in R$ ist unzerlegbar in R. Denn angenommen $3 = ab$ für $a, b \in R$, dann gilt $9 = N(3) = N(ab) = N(a)N(b)$, also $N(a) \in \{1, 3, 9\}$. Falls $N(a) = 1$ dann ist a eine Einheit, wie wir oben gesehen haben. Falls $N(a) = 9$, dann ist $N(b) = 1$, und b ist eine Einheit. Falls $N(a) = 3$, dann schreiben wir $a = r + s\sqrt{-5}$, und erhalten $3 = N(a) = r^2 - 5s^2$ für $r, s \in \mathbb{Z}$, was nicht sein kann, da $r^2 - 5s^2 \equiv r^2 - s^2 \not\equiv 3 \mod 4$. △

2.5.1 Zerlegungen in irreduzible Elemente

Wir haben im letzten Abschnitt gesehen, dass in Ringen R, die kein Hauptidealring sind, nicht jedes irreduzible Element auch prim sein muss; umgekehrt aber schon (Proposition 2.4.28), und daraus folgt unmittelbar das folgende Lemma.

Lemma 2.5.3. *In jedem faktoriellen Ring R ist jedes $x \in R \setminus (R^\times \cup \{0\})$ ein Produkt von irreduziblen Elementen.*

Die Zerlegung aus Lemma 2.5.3 ist in faktoriellen Ringen im Wesentlichen eindeutig.

Lemma 2.5.4. *Sei $\underline{R}$ ein faktorieller Ring. Sind $p_1, \dots, p_r, q_1, \dots, q_r \in R$ unzerlegbar mit $p_1 \dots p_r = q_1 \cdots q_s$, so gilt $r = s$ und es gibt ein $\pi \in S_r$, so dass $p_i \sim q_{\pi(i)}$ für alle $i \in \{1, \dots, r\}$.*

Beweis. Wir nehmen ohne Beschränkung der Allgemeinheit an, dass $r \leq s$, und beweisen die Aussage mit vollständiger Induktion nach s. Wir behaupten, dass jedes $p \in \{p_1, \dots, p_r\}$ ein Primelement ist. Denn in einem faktoriellen Ring ist $p = o_1 \dots o_t$ für Primelemente $o_1, \dots, o_t$; da p irreduzibel, gilt $t = 1$ und p ist prim. Also $p|q_i$ für ein $i \in \{1, \dots, s\}$. Da q_i irreduzibel ist, ist $q_i = pu$ für eine Einheit u, also $p \sim q_i$ (Bemerkung 2.3.4). Falls $s = 1$ sind wir fertig. Da $\underline{R}$ kommutativ ist, können wir um p kürzen und erhalten die Aussage aus der Induktionsvoraussetzung. □

Beispiel 2.5.5. Der Ring $\mathbb{Z}$ ist faktoriell, und jedes Element $a \in \mathbb{Z}$ kann geschrieben werden als Produkt $a = p_1 \cdots p_n$ von irreduziblen Elementen $p_1, \ldots, p_n$ (equivalent: Primelementen), und diese Darstellung ist eindeutig bis auf Reihenfolge und Einheiten (bedeutet hier: Vorzeichen). △

Die Eigenschaften von faktoriellen Ringen aus den letzten beiden Lemmata können verwendet werden, um faktorielle Ringe zu charakterisieren. Wir sagen, dass R die *Primbedingung* erfüllt, wenn jedes irreduzible Element von R auch prim ist.

Satz 2.5.6. *Es sei R ein Integritätsring. Dann sind q̈uivalent.*

1. *R ist faktoriell.*
2. *jedes Element $a \in R \setminus (R^\times \cup \{0\})$ lässt sich als Produkt $a = u_1 \cdots u_n$ von irreduziblen Elementen $u_1, \ldots, u_n \in R$ schreiben, und diese Darstellung ist bis auf Reihenfolge und Einheiten eindeutig (siehe Lemma 2.5.4),*
3. *jedes Element $a \in R \setminus (R^\times \cup \{0\})$ lässt sich als Produkt $a = u_1 \cdots u_n$ von irreduziblen Elementen $u_1, \ldots, u_n \in R$ schreiben, und R erfüllt die Primbedingung.*
4. *für jede aufsteigende Folge $(a_0) \subseteq (a_1) \subseteq \cdots$ von Hauptidealen gibt es ein $k \in \mathbb{N}$, so dass $(a_i) = (a_k)$ für alle $i \geq k$, und R erfüllt die Primbedingung.*

Beweis. (1) $\Rightarrow$ (2): die ist Lemma 2.5.3 und Lemma 2.5.4.

(2) $\Rightarrow$ (3): Seien $u \in R$ irreduzibel und $a, b \in R$ mit $u|ab$. Wir müssen zeigen, dass $u|a$ oder $u|b$. Es existiert ein $d \in R$, so dass $ud = ab$. Gilt $a = 0$, so gilt $u|a$. Ist a eine Einheit, so folgt $u|b$. Die gleichen Aussagen gelten für b anstatt für a. Wir können also annehmen, dass a und b nicht Null und keine Einheiten sind. Es folgt, dass $d \neq 0$, da R nullteilerfrei, und d keine Einheit, da u unzerlegbar ist. Nach Voraussetzung existieren Zerlegungen $a = p_1 \cdots p_n$, $b = q_1 \cdots q_m$, und $d = v_1 \cdots v_k$ mit irreduziblen Faktoren. Wir erhalten also die Zerlegung

$$uv_1 \cdots v_k = ud = ab = p_1 \cdots p_n \cdot q_1 \cdots q_m \cdot v_1 \cdots v_k.$$

Nach Voraussetzung existiert also ein $i \in \{1, \ldots, n\}$ mit $u \sim p_i$, oder ein $j \in \{1, \ldots, m\}$ mit $u \sim q_j$. Im ersten Fall gilt $u|a$ und im zweiten Fall $u|b$.

Offenbar gilt (3) $\Rightarrow$ (1).

(2) $\Rightarrow$ (4): es genügt zu zeigen, dass jedes Hauptideal $(a) \neq (0)$ in nur endlich vielen anderen Hauptidealen enthalten ist. Sei $b \in R$ so, dass $(a) \subseteq (b) \subseteq R$. Dann gibt es $c \in R \setminus \{0\}$ mit $a = bc$. Nach Voraussetzung können wir a, b, und c als Produkte unzerlegbarer Elemente schreiben, also $a = p_1 \cdots p_r$, $b = q_1 \cdots q_s$, $c = q_1' \cdots q_t'$. Da die Darstellung von $a = p_1 \cdots p_r = q_1 \cdots q_s \cdot q_1' \cdots q_t'$ bis auf Reihenfolge und Einheiten eindeutig ist, folgt $r \geq s$ und für jedes $j \in \{1, \ldots, s\}$ gibt es ein $i_j \in \{1, \ldots, r\}$ mit $q_j \sim p_{i_j}$. Also gilt $(b) = (p_{i_1} \cdots p_{i_s}) = (p_{i_1}) \cdots (p_{i_s})$. Insbesondere gibt es nur endlich viele solcher Hauptideale (b).

(4) $\Rightarrow$ (1): der Beweis ist ähnlich zum Beweis von Proposition 2.5.1. Sei $a \in R \setminus (\{0\} \cup R^\times)$. Falls a prim ist, so bleibt nichts zu zeigen. Andernfalls ist a reduzibel,

da R die Primbedingung erfüllt. Also kann a geschrieben werden als $a = bc$ für $b, c \in R \setminus R^\times$. Das gleiche Argument kann man für b und für c wiederholen. Nach Annahme bricht das Verfahren nach endlich vielen Schritten ab, und wir erhalten die gewünschte Primfaktorzerlegung. □

In Hauptidealringen R besitzen je zwei Elemente einen größten gemeinsamen Teiler, in anderen Worten: $\mathrm{ggT}(a, b)$ ist für alle $a, b \in R$ nicht leer (siehe Lemma 2.4.17). Diese Aussage gilt auch für faktorielle Ringe (Lemma 2.5.10 weiter unten). Um das einfach zu sehen, wählen wir ein Repräsentantensystem $\mathcal{P}$ für die Primelemente von R, soll heißen, $\mathcal{P}$ ist eine Menge von Primelementen von R, so dass aus jeder Klasse von assoziierten Primelementen genau eines in $\mathcal{P}$ ist.

Beispiel 2.5.7. In $\mathbb{Z}$ ist die Menge der Primzahlen $\{p_1, p_2, \dots\}$ ein Repräsentantensystem der Primelemente. Ein anderes Repräsentantensystem wäre $\{-p_1, -p_2, \dots\}$. △

Beispiel 2.5.8. Für $R = \mathbb{Q}[X]$ ist $R^\times = \mathbb{Q} \setminus \{0\}$ ist die Menge der normierten irreduziblen $f \in \mathbb{Q}[X]$ ein Repräsentantensystem der Primelemente. △

Proposition 2.5.9. *Sei R faktoriell. Dann kann jedes $a \in R \setminus \{0\}$ geschrieben werden als*

$$a = u_a \prod_{p \in \mathcal{P}} p^{v_p(a)}$$

mit $u_a \in R^\times$ und $v_p(a) \in \mathbb{N}$. Hierbei ist $v_p(a) = 0$ für alle bis auf endlich viele $p \in \mathcal{P}$. Diese Schreibweise von a ist bis auf die Reihenfolge der Faktoren eindeutig.

Beweis. Eine direkte Konsequenz auf Satz 2.5.6. □

Lemma 2.5.10. *Seien R faktoriell und $a_1, \dots, a_n \in R \setminus \{0\}$. Dann ist $\mathrm{ggT}(a_1, \dots, a_n)$ nicht leer.*

Beweis. Wir verwenden Proposition 2.5.9. Es gilt dann

$$\prod_{p \in \mathcal{P}} p^{\min(v_p(a_1), \dots, v_p(a_n))} \in \mathrm{ggT}(a_1, \dots, a_n).$$ □

Das folgende Beispiel zeigt, dass Lemma 2.5.10 in beliebigen Ringen nicht gilt.

Beispiel 2.5.11. Im Unterring $R = \mathbb{Z}[\sqrt{-5}] = \{a + b\sqrt{-5} \mid a, b \in \mathbb{Z}\}$ von $\mathbb{C}$ aus Beispiel 2.5.2 haben die Elemente $u := 9 = (2 + \sqrt{-5}) \cdot (2 - \sqrt{-5})$ und $v := 3(2 + \sqrt{-5})$ keinen ggT. Denn angenommen, $d = (a + b\sqrt{-5}) \in \mathrm{ggT}(u, v)$. Da $3|d$ und $d|9$ folgt $9 = N(3)|N(d)|N(9) = 81$ für $N\colon R \to \mathbb{N}$ aus Beispiel 2.5.2. Also ist $N(d) \in \{9, 27, 81\}$. Wir schließen alle drei Fälle aus:

- Modulo 4 gerechnet ist $N(d) = a^2 + 5b^2$ kongruent zu $a^2 + b^2$, also nicht kongruent zu 3 modulo 4; daher ist $N(d) = 27$ nicht möglich.
- Falls $N(d) = 9$, dann folgt aus $9 = N(2 + \sqrt{-5}) = N(3)$, dass $d \in \{3, -3\}$ und $d \in \{2 + \sqrt{-5}, 2 - \sqrt{-5}\}$, ein Widerspruch.

- Falls $N(d) = 81$, dann folgt aus $81 = N(3(2+\sqrt{-5})) = N(9)$, dass $d \in \{-9, 9\}$ und $d \in \{3(2+\sqrt{-5}), 3(2-\sqrt{-5})\}$, ein Widerspruch. △

Wir geben ein weiteres Beispiel eines nicht faktoriellen Ringes an.

Beispiel 2.5.12. Für $i \in \mathbb{N}$ sei $\pi_i := \pi^{-2^i}$. Sei $R_\pi := \mathbb{Q}[\pi_i \mid i \in \mathbb{N}] \subseteq \mathbb{R}$. Dann erfüllt R die Eigenschaft 4. aus Satz 2.5.6 nicht, weil $(\pi_0) \subset (\pi_1) \subset \cdots$. Insbesondere ist R_π nicht faktoriell. △

2.5.2 Der Satz von Gauß

Auch die Ringe $\mathbb{Z}[X]$ und $\mathbb{Q}[X, Y]$ sind faktoriell. Das folgt aus folgendem Satz.

Satz 2.5.13 (Gauß)**.** *Sei R ein faktorieller Ring. Dann ist $R[X]$ ebenfalls faktoriell.*

Beispiel 2.5.14. Da $\mathbb{Z}$ euklidisch (Beispiel 2.2.10), und damit ein Hauptidealring und faktoriell ist, so ist wegen Satz 2.5.13 auch $\mathbb{Z}[X]$ faktoriell, aber kein Hauptidealring (siehe Beispiel 2.4.16). △

Beispiel 2.5.15. Da $\mathbb{Q}[X]$ euklidisch (Beispiel 2.2.10), und damit ein Hauptidealring und faktoriell ist, ist wegen Satz 2.5.13 auch $\mathbb{Q}[X, Y]$ faktoriell, aber kein Hauptidealring (siehe Beispiel 2.4.34). △

Unsere Beweisstrategie für Satz 2.5.13 ist, sich den Ring R als Unterring seines Quotientenkörpers $K = \mathrm{Quot}(R)$ zu denken, und entsprechend $R[X]$ als Unterring von $K[X]$. Denn $K[X]$ ist ein euklidischer Ring, also faktoriell. Von der eindeutigen Zerlegung der Polynome aus $R[X]$ in irreduzible Polynome aus $K[X]$ schließen wir dann auf die entsprechenden Zerlegungen in $R[X]$. Hierzu wird es wichtig sein, zu verstehen, wann ein Ideal in $R[X]$ prim ist.

Jedes Ideal $I \trianglelefteq R$ erzeugt das folgende Ideal von $R[X]$.

$$IR[X] = \{a_0 + a_1X + \cdots + a_nX^n \in R[X] \mid a_0, \ldots, a_n \in I\}$$

Lemma 2.5.16. *Sei R ein Ring und $I \trianglelefteq R$ ein Ideal. Dann gilt $R[X]/IR[X] \cong R/I[X]$.*

Beweis. Wir verwenden Übung 56 (eine Variante für Ringe von Korollar 1.4.13 zum Homomorphiesatz für Gruppen). Sei $\varphi\colon R[X] \to R/I[X]$ der surjektive Ringhomomorphismus, der gegeben ist durch $(a_0+a_1X+\cdots+a_nX^n) \mapsto (a_0+I)+(a_1+I)X+\cdots+(a_n+I)X^n$. Dann ist $\mathrm{Kern}(\varphi) = \{(a_0 + a_1X + \cdots + a_nX^n) \mid a_0, a_1, \ldots, a_n \in I\} = IR[X]$. Nach Übung 56 ist $R[X]/IR[X] = R[X]/\mathrm{Kern}(\varphi) \cong R/I[X]$. □

Korollar 2.5.17. *Falls I ein Primideal von R ist, dann ist $IR[X]$ ein Primideal in $R[X]$.*

Beweis. Falls I ein Primideal von R ist, dann ist R/I ein Integritätsring (Proposition 2.4.22). Daher ist $R/I[X]$ ebenfalls ein Integritätsring (Beispiel 2.3.2). Da $R/I[X] \cong R[X]/IR[X]$ (Lemma 2.5.16), ist $R[X]/IR[X]$ ein Integritätsbereich, und $IR[X]$ ein Primideal von $R[X]$ (Proposition 2.4.22, Rückrichtung). □

Sei $f = \sum_{i=1}^{n} a_i X^i \in R[X] \setminus \{0\}$. Dann definieren wir den *Inhalt von* f als

$$I(f) := \mathrm{ggT}(a_0, a_1, \ldots, a_n).$$

Wir verwenden Komplexschreibweise; offenbar gilt dann für $k \in R$, dass $I(kf) = kI(f)$. Das Polynom f heißt *primitiv*, falls $1 \in I(f)$, also wenn $a_0, a_1, \ldots, a_n$ teilerfremd sind.

Beispiel 2.5.18. Jedes normierte Polynom aus $R[X]$ ist primitiv. Für einen Köper K ist jedes $f \in K[X] \setminus \{0\}$ primitiv. △

Lemma 2.5.19. *Sei R ein faktorieller Ring, $K := \mathrm{Quot}(R)$, und $f \in K[X] \setminus \{0\}$. Dann kann f geschrieben werden als $f = \frac{a}{b} f_0$ für $a, b \in R \setminus \{0\}$ mit $1 \in \mathrm{ggT}(a, b)$ und einem primitiven $f_0 \in R[X]$. Ist f sogar aus $R[X]$, so gilt dann $b \sim 1$ und $a \in I(f)$.*

Beweis. Sei $f = \sum_{i=0}^{n} c_i X^i$, wobei $c_i = \frac{r_i}{s_i}$ mit $r_i \in R$, $s_i \in R \setminus \{0\}$. Dann ist $s := s_1 \cdots s_n \neq 0$, und $sf \in R[X]$. Wähle $d \in I(sf)$. Dann ist $sf = df_0$ für ein primitives $f_0 \in R[X]$, und $f = \frac{d}{s} f_0$. Wähle $t \in \mathrm{ggT}(d, s)$. Dann gibt es $a, b \in R \setminus \{0\}$ mit $at = d$ und $bt = s$, und es gilt $f = \frac{a}{b} f_0$ und $1 \in \mathrm{ggT}(a, b)$.

Sei nun $f \in R[X]$. Es gilt $bf = af_0$, also

$$a \in aI(f_0) = I(af_0) = I(bf) = bI(f)$$

und $b | a$. Da $1 \in \mathrm{ggT}(a, b)$ folgt $b \sim 1$ und $a \in I(f)$. □

Bemerkung 2.5.20. Falls $f = \frac{a}{b} f_0 \in K[X] \setminus \{0\}$ wie in Lemma 2.5.19 irreduzibel in $K[X]$ ist, dann ist f_0 irreduzibel in $R[X]$. Denn wenn f_0 reduzibel ist, dann lässt sich f_0 schreiben als $f_0 = g_1 \cdot g_2$ für $g_1, g_2 \in R[X] \setminus (R^\times \cup \{0\})$. Da f_0 primitiv ist, so sind auch g_1 und g_2 primitiv. Also ist $f = (\frac{a}{b} g_1) g_2$ ebenfalls reduzibel, da $\frac{a}{b} g_1 \notin K$ und $g_2 \notin K$.

Bemerkung 2.5.21. Die Umkehrung von 2.5.20 gilt auch; siehe Übung 67.

Beweis von Satz 2.5.13 (Satz von Gauß). Sei $K := \mathrm{Quot}(R)$; dann ist $K[X]$ euklidisch (Beipspiel 2.2.10), also Hauptidealring und faktoriell (Proposition 2.5.1). Sei $f \in R[X] \setminus \{0\} \subseteq K[X]$. Also gilt $f = p_1 \cdots p_r$ für irreduzible $p_1, \ldots, p_r \in K[X]$. Mit Lemma 2.5.19 gibt es für jedes $i \in \{1, \ldots, r\}$ ein $a_i \in K$ und ein primitives $q_i \in R[X]$ mit $p_i = a_i q_i$. Die q_i sind irreduzibel in $R[X]$ (Bemerkung 2.5.20). Es gilt $f = a q_1 \cdots q_r$ für ein $a \in K \setminus \{0\}$. Mit dem zweiten Teil von Lemma 2.5.19 folgt, dass $a \in I(f) \subseteq R$. Da R faktoriell ist, können wir auch a als Produkt irreduzibler Elemente $a_1, \ldots, a_s \in R$ schreiben, die dann auch irreduzibel in $R[X]$ sind. Insgesamt erhalten wir f also als Produkt irreduzibler Elemente in $R[X]$.

Wir müssen noch nachweisen, dass jeder der Faktoren $a_1, \ldots, a_s, q_1, \ldots, q_r$ prim in $R[X]$ ist. Für jedes $i \in \{1, \ldots, s\}$ ist (a_i) ein Primideal in R, da R faktoriell ist. Und damit ist (a_i) nach Korollar 2.5.17 auch ein Primideal in $R[X]$.

Für jedes $i \in \{1, \ldots, r\}$ ist q_i irreduzibel in $R[X]$, also ist (q_i) ein Primideal im Hauptidealring $K[X]$ (Proposition 2.4.31), und $K[X]/(q_i)$ ist ein Integritätsring (Proposition 2.4.22).

Die Komposition ψ der Einbettung von $R[X]$ nach $K[X]$ mit dem kanonischen Homomorphismus von $K[X]$ nach $K[X]/(q_i)$ ist ein Ringhomomorphismus von $R[X]$ nach $K[X]/(q_i)$. Das Bild von ψ ist der Unterring $R[X]/(q_i)$ von $K[X]/(q_i)$, ein Integritätsring. Also ist (q_i) ein Primideal von $R[X]$ nach Proposition 2.4.22. □

Bemerkung 2.5.22. Die folgenden Übungen 66, 67, 68, 69, 70 sind allesamt verwandt.

Übung 66. Ein Element $f \in R[X]$ ist genau dann prim, wenn gilt

- f ist ein Primelement von R, oder
- f ist primitiv und ein Primelement in $\mathrm{Quot}(R)[X]$.

Übung 67. Zeigen Sie: falls $f = \frac{a}{b} f_0 \in K[X] \setminus \{0\}$ wie in Lemma 2.5.19, dann ist f genau dann irreduzibel in $K[X]$, wenn f_0 irreduzibel in $R[X]$ (wegen Bemerkung 2.5.20 ist nur noch die Rückrichtung zu zeigen).

Übung 68. Sei R ein faktorieller Ring. Das Produkt zweier primitiver Polynome aus $R[X]$ ist primitiv.

Übung 69. Sei R faktoriell und $f, g \in R[X] \setminus \{0\}$. Dann gilt $I(fg) = I(f)I(g)$.

Übung 70. Ein Polynom $f \in R[X]$ vom Grad mindestens eins ist genau dann irreduzibel, wenn f in $\mathrm{Quot}(R)[X]$ irreduzibel und primitiv ist.

Übung 71. Ein *Dedekindring* ist ein Integritätsring, in dem sich jedes nicht-triviale Ideal ausser dem Nullideal als ein Produkt von Primidealen schreiben lässt. Zeigen Sie, dass jeder Hauptidealring auch ein Dedekindring ist.

Übung 72. Zeigen Sie, dass $\mathbb{Z}[\sqrt{-5}]$ ein Dedekindring ist, der nicht faktoriell ist.

Übung 73. Zeigen Sie, dass $\mathbb{Q}[x, y]$ ein Beispiel eines faktoriellen Ringes ist, der kein Dedekindring ist.

Übung 74. Zeigen Sie, dass ein Dedekindring genau dann ein faktorieller Ring ist, wenn er ein Hauptidealring ist.

2.6 Irreduzibilitätskriterien

Sei R ein faktorieller Ring und $K = \mathrm{Quot}(R)$. In diesem Abschnitt suchen wir hinreichende (und praktische!) Kriterien dafür, dass $f \in K[X]$ irreduzibel ist.

Bemerkung 2.6.1. Ist $c \in K^\times$, so ist f genau dann irreduzibel, wenn cf irreduzibel ist. Falls $\mathrm{grad}(f) = 1$, dann ist f irreduzibel und hat eine Nullstelle in K. Ist $\mathrm{grad}(f) \geq 2$ und hat f eine Nullstelle in K, so ist f reduzibel. Ist $\deg(f) \leq 3$ und hat f keine Nullstelle in K, so ist f irreduzibel.

Bemerkung 2.6.2. Ob ein gegebenes Polynom $p = \sum_{i=0}^{n} a_i X^i \in \mathbb{Q}[X]$ einen Teiler der Gestalt $aX + b$ mit $a, b \in \mathbb{Q}$ hat, läßt sich einfach überprüfen: es genügt, zu verifizieren, ob $-\frac{b}{a}$ ist eine Nullstelle von p ist. Falls sogar $p \in \mathbb{Z}[X]$, und wir nach einem Teiler der Gestalt $aX + b$ für $a, b \in \mathbb{Z}$ suchen, dann muss a ein Teiler von a_n sein und b ein

Teiler von a_0, und wir können a und b bei kleinem a_n und a_0 durch Ausprobieren finden. Weiterhin gibt es numerische Verfahren, wie zum Beispiel das Newton Verfahren, um nach Nullstellen von Polynomen zu suchen.

Bemerkung 2.6.3. Bemerkenswerterweise gibt es einen Algorithmus, der eine Faktorisierung eines gegebenen Polynoms aus $\mathbb{Q}[X]$ berechnet, und dessen Laufzeit polynomiell ist in der Bitlänge aller Koeffizieten des gegebenen Polynoms [4]. Insbesondere können wir also ein gegebenes Polynom aus $\mathbb{Q}[X]$ auf Irreduzibilität testen. Der entsprechende Algorithmus sprengt allerdings den Rahmen dieser Vorlesung.

Der folgende Kriterium kann in vielen Situationen verwendet werden, um die Irreduzibilität eines gegebenen Polynoms nachzuweisen.

Satz 2.6.4 (Eisensteinsches Irreduzibilitätskriterium)**.** *Sei* $K = \mathrm{Quot}(R)$ *und* $f = a_0 + a_1X + \cdots + a_nX^n \in R[X]$ *mit* $1 \in I(f)$*, und* $p \in R$ *prim mit*

- $p^2 \nmid a_0$*,*
- $p|a_0, \ldots, p|a_{n-1}$*, und*
- $p \nmid a_n$*.*

Dann ist f *irreduzibel in* $R[X]$ *und in* $K[X]$*.*

Beweis. Angenommen, es gibt $g = \sum_{i=0}^{k} b_iX^i \in R[X]$ und $h = \sum_{i=0}^{l} c_iX^i \in R[X]$ so dass $f = gh$, $k + l = n$. Ohne Beschränkung der Allgemeinheit können wir annehmen, dass $p|b_0$. Da $p^2 \nmid a_0$ gilt also $p \nmid c_0$. Falls $p|b_k$, dann $p|a_n$, im Widerspruch zu unseren Annahmen. Definiere $m := \min(\{i \mid p \nmid b_i\})$. Es gilt dann $a_m = b_0c_m + \cdots + b_{m-1}c_1 + b_mc_0$ (wobei $b_i = 0$ für $i > k$ und $c_i = 0$ für $i > l$), und es ist a_m nicht durch p teilbar, denn $b_0c_m + \cdots + b_{m-1}c_1$ sind durch p teilbar, nicht aber b_mc_0. Daher ist $m = n$, und somit $k = n$ und $l = 0$. Also ist f irreduzibel in $R[X]$. Die Irreduzibilität in $K[X]$ folgt dann mit Übung 67. □

Bemerkung 2.6.5. Falls $f = a_0 + a_1X + \cdots + a_nX^n \in R[X]$ normiert ist, gelten $1 \in I(f)$ und $p \nmid a_n$ automatisch, und für das Eisensteinkriterium bleiben lediglich die Bedingungen $p^2 \nmid a_0$ und $p|a_0, \ldots, p|a_{n-1}$ zu testen.

Beispiel 2.6.6. Das Polynom $X^3 - 2 \in \mathbb{Z}[X]$ ist irreduzibel in $\mathbb{Z}[X]$ und sogar in $\mathbb{Q}[X]$, da wir das Eisensteinkriterium mit $p = 2 \in \mathbb{Z}$ anwenden können: $4 \nmid (-2)$ und $2|(-2)$. (In $\mathbb{R}[X]$ hingegen ist $X^3 - 2$ reduzibel, da es die Nullstelle $\sqrt[3]{2} \in \mathbb{R}$, also den Linearfaktor $(X - \sqrt[3]{2}) \in \mathbb{R}[X]$ besitzt.) △

Beispiel 2.6.7. Es sei K ein Körper. Wir betrachten den Körper $K(t) = \mathrm{Quot}(K[t])$ der rationalen Funktionen über K in einer formalen Variable t. Dann ist das Polynom $X^n - t \in K(t)[X]$ irreduzibel. Es ist nämlich $R := K[t]$ faktoriell, $t \in R$ ist prim, und $X^n - t$ ein primitives Polynom in $R[X]$ (denn $\mathrm{ggT}(1, -t) = 1$), und wir können daher das Eisensteinkriterium mit $p := t$ anwenden. △

Das folgende Beispiel zeigt, dass das Eisensteinkriterium nur ein hinreichendes, nicht aber ein notwendiges Kriterium für Irreduzibilität ist.

Beispiel 2.6.8. Für eine Primzahl p erfüllt das Polynom

$$f := X^{p-1} + X^{p-2} + \cdots + X + 1 \in \mathbb{Z}[X]$$

das Eisensteinkriterium nicht. Aber es ist irreduzibel. Um das zu zeigen, genügt es zu zeigen, dass $f(X+1)$ irreduzibel ist (denn falls $f = gh$, dann gilt auch $f(X+1) = g(X+1)h(X+1)$; siehe Übung 52). Offenbar gilt

$$(X^{p-1} + X^{p-2} + \cdots + X + 1)(X-1) = X^p - 1,$$

und daher $f(X) = \frac{X^p-1}{X-1}$. Also gilt auch

$$f(X+1) = \frac{(X+1)^p - 1}{X} = X^{p-1} + \binom{p}{1}X^{p-2} + \cdots + \binom{p}{p-1}.$$

Nun sieht man, dass die Voraussetzungen des Eisensteinschen Kriteriums für das (normierte) Polynom $f(X+1)$ erfüllt sind:

- $p^2 \nmid \binom{p}{p-1} = p$, und
- $p \mid \binom{p}{k}$ für alle $k \in \{1, \ldots, p-1\}$: denn $\binom{p}{k} = \frac{p\cdot(p-1)\cdots(p-k+1)}{1\cdots k}$ besitzt im Zähler einen Primfaktor p, im Nenner aber nicht. △

Bemerkung 2.6.9. Das Polynom $f = \frac{X^p-1}{X-1} = X^{p-1} + X^{p-2} + \cdots + X + 1 \in \mathbb{Z}[X]$ aus dem vorigen Beispiel heisst das *p-te Kreisteilungspolynom*. Die Nullstellen von $X^n - 1$ in $\mathbb{C}$ heißen die *n-ten Einheitwurzeln*. Sie bilden eine zyklische Gruppe der Ordnung n, und werden erzeugt von $\eta_n := e^{2\pi i/n}$. Elemente der Ordnung n heißen *primitive n-te Einheitswurzeln*. Die Nullstellen von f in $\mathbb{C}$ sind genau die primitiven p-ten Einheitswurzeln.

Kapitel 3

Körper

Wiederholung: ein Körper ist ein kommutativer Ring R, in dem eine der folgenden äquivalenten Bedingungen gilt:

1. $R^\times = R \setminus \{0\}$;
2. (0) ist ein maximales Ideal;
3. (0) ist das einzige echte Ideal;
4. (0) ist das einzige Primideal.

Für 1. $\Leftrightarrow$ 2. hatten wir Proposition 2.4.12. 2. $\Rightarrow$ 3. und 3. $\Rightarrow$ 4. sind trivial. 4. $\Rightarrow$ 2. gilt, da jedes Ideal in einem maximalen enthalten ist (Satz 2.4.35), und maximale Ideale prim sind (Korollar 2.4.30).

Bemerkung 3.0.1. Wenn K ein Körper ist, dann ist jeder Ringhomomorphismus $\varphi\colon K \to R$ in einen anderen Ring injektiv, oder $|R| = 1$. Denn $\mathrm{Kern}(\varphi) \trianglelefteq K$ ist ein Ideal, und damit gleich (0) oder K; im ersten Fall ist φ injektiv, und im zweiten Fall erfüllt R die Gleichung $1 = \varphi(1) = \varphi(0) = 0$, ist also der Nullring mit $|R| = 1$. Jeder *Körperhomomorphismus*, also jeder Ringhomomorphismus zwischen Körpern, ist daher injektiv.

Bemerkung 3.0.2. Wenn K ein Körper ist, dann ist der Durchschnitt einer Familie von Teilkörpern von K selbst wieder ein Teilkörper von K.

Bemerkung 3.0.3. Wenn K ein Körper ist, dann gibt es genau einen Ringhomomorphismus $\varphi\colon \mathbb{Z} \to K$, und $\mathrm{Kern}(\varphi) \trianglelefteq \mathbb{Z}$ ist prim.

Definition 3.0.4. Die *Charakteristik* von K ist definiert als $\mathrm{char}(K) := p \in \{2, 3, 5, \dots\}$ mit $\mathrm{Kern}(\varphi) = (p)$ für das $\varphi\colon \mathbb{Z} \to K$ aus Bemerkung 3.0.3.

Beispiel 3.0.5. Es gilt $\mathrm{char}(\mathbb{Q}) = 0$ und $\mathrm{char}(\mathbb{F}_p) = p$. Ist K_0 ein Teilkörper von K, so ist $\mathrm{char}(K_0) = \mathrm{char}(K)$. △

Definition 3.0.6. Der *Primkörper* von K ist der kleinste Teilkörper von K (siehe Bemerkung 3.0.2).

Lemma 3.0.7. *Sei F der Primkörper von K. Dann gilt*

- *$\mathrm{char}(K) = 0$ genau dann, wenn $F \cong \mathbb{Q}$, und*
- *$\mathrm{char}(K) = p > 0$ genau dann, wenn $F = \mathbb{F}_p := \mathbb{Z}/p\mathbb{Z}$.*

Übung 75. Falls $|K| = p^n$ mit p prim, so gilt $\mathrm{char}(K) = p$.

Übung 76. Sei $p \in \mathbb{R}[X]$ ein Polynom vom Grad 3. Begründen Sie, dass $\mathbb{R}[X]/(p)$ kein Körper ist.

3.1 Körpererweiterungen

Ist K ein Teilkörper von L, so nennt man L eine *Körpererweiterung von K*, auch geschrieben $L|K$. Wir schreiben $[L : K]$ für die Dimension $\dim_K(L) \in \mathbb{N} \cup \{\infty\}$ des K-Vektorraumes L; diese wir auch *(Körper)grad* der Körpererweiterung $L|K$ genannt. Die Körpererweiterung $L|K$ heißt

- *echt* falls $L \neq K$, und
- *endlich* falls $[L : K] < \infty$.

Lemma 3.1.1. *Falls $M|L$ und $L|K$ Körpererweiterungen, so ist $M|K$ ebenfalls eine Körpererweiterung und es gilt*

$$[M : K] = [M : L] \cdot [L : K].$$

Beweis. Da $u_1, \ldots, u_n \in L$ linear unabhängig über K, und $v_1, \ldots, v_m \in M$ linear unabhängig über L, so sind $u_1v_1, u_1v_2, \ldots, u_nv_m$ linear unabhängig über K. □

Beispiel 3.1.2. $[\mathbb{C} : \mathbb{R}] = 2$ und $[\mathbb{R} : \mathbb{Q}] = \infty$. Auch $[\mathbb{Q}(X) : \mathbb{Q}] = \infty$, denn $1, X, X^2, \ldots$ sind linear unabhängig über $\mathbb{Q}$. △

Ist $L|K$ eine Körpererweiterung und $a_1, \ldots, a_n \in L$, dann schreiben wir

- $K[a_1, \ldots, a_n]$ für den kleinsten Unterring von L, der $K \cup \{a_1, \ldots, a_n\}$ enthält (der von $a_1, \ldots, a_n$ über K erzeugte Unterring von L).
- $K(a_1, \ldots, a_n)$ für die Körpererweiterung von K, die aus dem kleinsten Teilkörper von L besteht, der $K \cup \{a_1, \ldots, a_n\}$ enthält (also der von $a_1, \ldots, a_n$ über K erzeugte Teilkörper von L). Diese wird auch die *von $a_1, \ldots, a_n$ erzeugte Körpererweiterung von K* genannt; man sagt auch, $K(a_1, \ldots, a_n)$ entsteht durch *Adjunktion* von $a_1, \ldots, a_n$ zu K. Noch allgemeiner bezeichnet $K(A)$ für eine beliebige Teilmenge $A \subseteq L$ den kleinsten Teilkörper von L, der $K \cup A$ enthält. Falls A und B Teilkörper von L sind, so gilt offensichtlich $A(B) = B(A) =: AB$, das *Körperkompositum* von A und B.
- $L|K$ heißt *endlich erzeugt*, wenn es $a_1, \ldots, a_n \in L$ gibt mit $L = K(a_1, \ldots, a_n)$.

- $L|K$ heißt *einfach*, wenn es ein $a \in L$ mit $L = K(a)$ gibt.

Bemerkung 3.1.3. Die Notation $K[a]$ ist konsistent mit der Notation $K[X]$ (mit $L = K[X]$). Die Notation $K(a)$ ist konsistent mit der Notation $K(X)$ (mit $L = K(X)$).

Bemerkung 3.1.4. Ist $L|K$ endlich, so ist $L|K$ endlich erzeugt. Aber zum Beispiel $K(X)|K$ ist endlich erzeugt und unendlich.

Seien $L_1|K$ und $L_2|K$ Körpererweiterungen. Ein Ringhomomorphismus $\varphi\colon L_1 \to L_2$ ist ein *K-Homomorphismus* falls $\varphi|_K = \mathrm{id}_K$. Schreiben dann $\varphi\colon L_1 \to_K L_2$. Weiterhin steht $\mathrm{Hom}_K(L_1, L_2)$ für die Menge aller K-Homomorphismen von L_1 nach L_2. Ein *K-Isomorphismus* ist ein K-Homomorphismus, der zudem ein Ringisomorphismus ist. Falls es einen solchen K-Isomorphismus zwischen L_1 und L_2 gibt, so heißen L_1 und L_2 *K-isomorph*, und wir schreiben $L_1 \cong_K L_2$.

Bemerkung 3.1.5. Der Ring $K[a_1, \ldots, a_n]$ ist das Bild des K-Homomorphismus

$$K[X_1, \ldots, X_n] \to L$$

der gegeben ist durch $f \mapsto f(a_1, \ldots, a_n)$ (der Auswertungshomomorphismus, siehe Abschnitt 2.2). Der Körper $K(a_1, \ldots, a_n)$ hat die Elemente

$$\{\frac{c}{d} \mid c, d \in K[a_1, \ldots, a_n], d \neq 0\}$$

und ist isomorph zu $\mathrm{Quot}(K[a_1, \ldots, a_n])$.

Übung 77. Sei $L|K$ eine Körpererweiterung und $a \in L$. Dann gilt $[K(a) : K] = 1$ genau dann, wenn $a \in K$.

Übung 78. Ist $[L : K]$ eine Primzahl, so gibt es keinen echten Teilkörper F von L, der K echt enthält.

Übung 79. Ist $L = K(a)$ und $b = ra + s \in L$ für $r \in K^\times$ und $s \in K$, dann ist $L = K(b)$.

3.2 Algebraische Erweiterungen

Für den ganzen Abschnitt sei $L|K$ eine Körpererweiterung.

Definition 3.2.1. Sei $a \in L$. Gibt es ein $f \in K[X] \setminus \{0\}$ mit $f(a) = 0$, so heißt a *algebraisch über K*, und ansonsten *transzendent über K*.

Beispiel 3.2.2. Jedes Element $a \in K$ ist algebraisch über K, denn a ist Nullstelle des Polynoms $X - a$. △

Beispiel 3.2.3. $\sqrt{2} \in \mathbb{R}$ ist algebraisch über $\mathbb{Q}$, denn $\sqrt{2}$ ist Nullstelle des Polynoms $X^2 - 2$. △

Beispiel 3.2.4. $i \in \mathbb{C}$ ist algebraisch über $\mathbb{R}$, nämlich Nullstelle von $X^2 + 1 \in \mathbb{R}[X]$. △

Beispiel 3.2.5. Das Element $X \in K(X)$ ist transzendent über K, denn für jedes $p \in K[X]$ mit $p(X) = 0$ folgt $p = 0$ (denn $p(X) = p$). △

Beispiel 3.2.6. $e \in \mathbb{R}$ ist transzendent über $\mathbb{Q}$ (Hermite 1873) und $\pi \in \mathbb{R}$ ist transzendent über $\mathbb{Q}$ (Lindemann 1882). Die Beweise sind nicht einfach und sprengen den Rahmen dieser Vorlesung. Es ist nicht bekannt, ob $\pi + e$ algebraisch über $\mathbb{Q}$ ist (es ist nicht einmal bekannt, ob $\pi + e$ rational ist). △

Lemma 3.2.7. *Ein Element $a \in L$ ist genau dann algebraisch über K, wenn $1, a, a^2, \ldots$ linear abhängig über K sind.*

Beweis. Die Elemente $1, a, a^2, \ldots$ von L sind genau dann linear abhängig über K, wenn es ein $n \in \mathbb{N}$ und $(b_0, b_1, \ldots, b_n) \in K^n \setminus \{(0, \ldots, 0)\}$ gibt mit $b_0 + b_1 a + b_2 a^2 + \cdots + b_n a^n = 0$. Dies ist genau dann der Fall, wenn $p(a) = 0$ für das Polynom $p = b_n X^n + \cdots + b_2 X^2 + b_1 X + b_0 \in K[X] \setminus \{0\}$. Offensichtlich gilt auch die Umkehrung. □

Lemma 3.2.8. *Sei $a \in L$ und $\varphi_a \colon K[X] \to K[a]$ der Auswertungshomomorphismus, also die Abbildung $f \mapsto f(a)$.*

- *a ist genau dann algebraisch über K, wenn $\operatorname{Kern}(\varphi_a) \neq \{0\} = (0)$. In diesem Fall ist $\operatorname{Kern}(\varphi_a) = (f_a)$ mit einem eindeutig bestimmten normierten irreduziblen $f_a \in K[X]$, dem* Minimalpolynom von a über K.
- *a ist genau dann transzendent über K, wenn φ_a ein Isomorphismus zwischen $K[X]$ und $K[a]$ ist.*

Beweis. Der Auswertungshomomorphismus ist surjektiv, denn

$$K[a] = \{p(a) \mid p \in K[X]\}$$

die rechte Seite der Gleichung ist offensichtlich eine Teilmenge der linken. Weiterhin ist die rechte Seite ist ein Teilkörper von L und enthält a, also eine Teilmenge der linken. Falls a transzendent über K ist, dann ist $\operatorname{Kern}(\varphi_a) = \{0\}$, also ist φ_a ein Isomorphismus.

Wenn a algebraisch über K ist, dann gibt es ein $f \in K[X] \setminus \{0\}$ mit $f(a) = 0$, also $f \in \operatorname{Kern}(\varphi_a)$. Nach dem Homomorphiesatz ist das Bild von φ_a isomorph zu $K[X]/\operatorname{Kern}(\varphi_a)$. Das Bild von φ_a ist als Teilmenge von L nullteilerfrei, und damit auch $K[X]/\operatorname{Kern}(\varphi_a)$. Da $I_a := \operatorname{Kern}(\varphi_a) \neq \{0\}$, ist $K[X]/I_a$ sogar ein Integritätsring, und damit ist I_a ein Primideal von $K[X]$ (Proposition 2.4.22). Da $K[X]$ ein Hauptidealring ist, wird I_a von einem irreduziblen Element f_a erzeugt (Proposition 2.4.31); wir können f_a normiert wählen, und mit dieser Eigenschaft ist f_a eindeutig. □

In anderen Worten: das Minimalpolynom von a über K ist das eindeutig bestimmte normierte irreduzible Polynom $f_a \in K[X]$ mit $f(a) = 0$.

Übung 80. Sei $L|K$ eine Körpererweiterung und $a \in L$. Zeigen Sie, dass die folgenden Aussagen äquivalent sind:

- f_a ist das Minimalpolynom von a über K;
- f_a ist das Polynom mit Leitkoeffizient 1, welches die Nullstelle a besitzt, und alle anderen solchen Polynome teilt.

- f_a ist das normierte Polynom kleinsten Grades mit Nullstelle a.

Übung 81. Bestimmen Sie das Minimalpolynom der reellen Zahl $\sqrt{2}+\sqrt{3}$ über $\mathbb{Q}$.

Übung 82. Es sei $L|K$ eine Körpererweiterung und $a \in L$ algebraisch über K. Zeigen Sie: für jedes $p \in K[X]$ gilt genau dann $p(a) = 0$, wenn $f_a|P$.

Übung 83. Es sei E ein *Zwischenkörper von* $L|K$, das bedeutet: $L|E$ und $E|K$ sind Körpererweiterungen. Sei $a \in L$ algebraisch über K. Dann ist a auch algebraisch über E (warum?). Es sei $f_{a,K}$ das Minimalpolynom von a über K und $f_{a,E}$ das Minimalpolynom von a über E. Zeigen Sie: $f_{a,E}|f_{a,K}$. Finden Sie ein Beispiel, wo $f_{a,E} \neq f_{a,K}$.

Aus dem Beweis von Lemma 3.2.8 ergeben sich direkt die folgenden Aussagen.

Lemma 3.2.9. *Sei $a \in L$.*

- *Ist a algebraisch über K, so gilt $K(a) = K[a] \cong K[X]/(f_a)$ und*

$$[K(a) : K] = \operatorname{grad}(f_a) < \infty.$$

- *Ist a transzendent über K, so gilt $K[a] \cong K[X]$, $K(a) \cong K(X)$, und*

$$[K(a) : K] = \infty.$$

Beweis. Sei a algebraisch über K. Offenbar gilt $K[a] \subseteq K(a)$. Sei f_a das Minimalpolynom von a über K (Lemma 3.2.8). Dann ist (f_a) ein maximales Ideal nach Proposition 2.4.31, und $K[a] \cong K[X]/(f_a)$ ist ein Körper nach Proposition 2.4.29. Also gilt $K[a] = K(a)$. Um zu zeigen, dass $[K(a) : K] \geq \operatorname{grad}(f_0)$, zeigen wir, dass $1, a, \ldots, a^{n-1}$ linear unabhängig sind. Seien $k_0, k_1, \ldots, k_{n-1} \in K$ so, dass $k_0 + k_1 a + \cdots + k_{n-1}a^{n-1} = 0$. Dann ist $p := k_0 + k_1 X + \cdots + k_{n-1}X^{n-1} \in \operatorname{Kern}(\varphi_a)$, also $f_a|p$; da $\operatorname{grad}(p) < n$, muss gelten $p = 0$, also $k_0 = k_1 = \cdots = k_{n-1} = 0$. Um zu zeigen, dass $[K(a) : K] \leq \operatorname{grad}(f_a)$, zeigen wir, dass $K(a)$ erzeugt wird von $1, a, \ldots, a^{n-1}$. Sei $b \in K(a)$. Dann hat b die Gestalt $p(a)$ für ein $p \in K[X]$. Schreibe p als $qf_a + r$ für $q, r \in K[X]$ und $\operatorname{grad}(r) < \operatorname{grad}(f_a)$. Also ist $p(a) = q(q)0 + r(a) = r(a)$. Also gibt es $k_0, k_1, \ldots, k_{n-1} \in K$ mit $b = \sum_{i=0}^{n-1} k_i a^i$, was zu zeigen war.

Sei nun a transzendent über K. Dann ist $\frac{p}{q} \mapsto \frac{p(a)}{q(a)}$ ein Isomorphismus zwischen $K(X)$ und $K(a)$, und $[K(a) : K] = \infty$ nach Lemma 3.2.7. □

Korollar 3.2.10. *Genau dann ist $a \in L$ algebraisch über K, wenn $[K(a) : K] < \infty$.*

Definition 3.2.11. Eine Körpererweiterung $L|K$ heißt *algebraisch* falls jedes $a \in L$ algebraisch über K ist.

Lemma 3.2.12. *Sei $L|K$ endlich. Dann ist $L|K$ algebraisch.*

Beweis. Sei $a \in L$. Es gilt $[K(a) : K] \leq [L : K] < \infty$, also ist a algebraisch nach Korollar 3.2.10. □

Proposition 3.2.13. *Die folgenden Aussagen sind äquivalent.*

1. *$L|K$ ist endlich.*
2. *$L|K$ ist endlich erzeugt und algebraisch.*
3. *$L = K(a_1, \dots, a_n)$ für $a_1, \dots, a_n \in L$ algebraisch über K.*

Beweis. 1. $\Rightarrow$ 2.: Ist $L|K$ endlich, so auch endlich erzeugt (Bemerkung 3.1.4). Nach Lemma 3.2.12 ist L algebraisch.
2. $\Rightarrow$ 3.: ist offensichtlich.
3. $\Rightarrow$ 1.: Für $i \in \{1, \dots, n\}$, sei $K_i := K(a_1, \dots, a_i)$, so dass

$$K \subseteq K_1 \subseteq K_2 \subseteq \cdots \subseteq K_n = L.$$

Es ist $[K(a_1) : K]$ endlich nach Korollar 3.2.10. Da a_i algebraisch ist über K hat a_i ein Minimalpolynom $f_{a_i} \in K[X]$ über K. Dann bezeugt f_{a_i} für $i \geq 2$ insbesondere, dass a_i algebraisch ist über K_{i-1}, und damit ist $[K_i(a_1) : K_{i-1}]$ endlich nach Korollar 3.2.10. Mit Lemma 3.1.1 folgt

$$[L : K] = [K(a_1, \dots, a_n) : K] \leq [K_n : K_{n-1}] \cdots [K_1 : K] < \infty. \qquad \square$$

Bemerkung 3.2.14. Nicht jede algebraische Erweiterung ist endlich! Siehe Beispiel 3.2.19.

Übung 84. Falls a algebraisch ist über K, und b algebraisch ist über K, dann sind auch $a - b$, $a + b$, ab, und $\frac{a}{b}$ algebraisch über K.[1]

Proposition 3.2.15. *Seien $L|M$ und $M|K$ Körpererweiterungen. Dann ist $L|K$ genau dann algebraisch, wenn $L|M$ und $M|K$ algebraisch sind.*

Beweis. Die Vorwärtsimplikation ist klar. Für die Rückrichtung sei $a \in L$. Sei $f_a = \sum_{i=0}^{n} a_i X^i$ das Minimalpolynom von a über M. Definiere $M_0 := K(a_0, a_1, \dots, a_n)$. Dann ist $f_a \in M_0[X]$, also $[M_0(a) : M_0] < \infty$. Somit ist

$$\begin{aligned} [K(a) : K] &\leq [K(a, a_0, \dots, a_n) : K] \\ &= [M_0(a) : M_0] \cdot [M_0 : K] && \text{(Lemma 3.1.1)} \\ &< \infty \cdot \infty < \infty && \text{(Proposition 3.2.13),} \end{aligned}$$

und daher ist a algebraisch über K. $\square$

Lemma 3.2.16. *Die Menge*

$$\bar{K}^L := \{b \in L \mid b \text{ ist algebraisch über } K\}$$

ist ein Teilkörper von L, und heißt der (relative) algebraische Abschluss von K in L.

[1] Die Frage, wie man aus dem Minimalpolynom von a und b das Minimalpolynom von Differenz, Produkt, Summe und Quotient von a und b berechnet, ist interessant, und ich verweise auf [5].

Beweis. Sei K' der kleinste Teilkörper von L, der $\bar{K}^L$ enthält. Dann ist K' nach Proposition 3.2.15 algebraisch über K, also gilt $K' \subseteq \bar{K}^L$ und somit ist $\bar{K}^L = K'$ ein Teilkörper von L. □

Korollar 3.2.17. *Ist $a \in L$ algebraisch über $\bar{K} := \bar{K}^L$, so ist $a \in \bar{K}$.*

Beweis. Ist a algebraisch über $\bar{K}$, so ist $\bar{K}(a)|\bar{K}$ algebraisch nach Proposition 3.2.13. Also ist $\bar{K}(a)|K$ algebraisch nach Proposition 3.2.15. Insbesondere ist a algebraisch über K, und daher gilt $a \in \bar{K}$. □

Beispiel 3.2.18. Für $\mathbb{C}|\mathbb{R}$ gilt $\bar{\mathbb{R}}^{\mathbb{C}} = \mathbb{C}$. △

Beispiel 3.2.19. *Der Körper der algebraischen Zahlen* ist $\bar{\mathbb{Q}}^{\mathbb{C}} \subseteq \mathbb{C}$. Die Inklusion ist strikt; es gilt sogar $|\bar{\mathbb{Q}}^{\mathbb{C}}| < |\mathbb{C}|$ (warum?). Die Erweiterung $\bar{\mathbb{Q}}^{\mathbb{C}}|\mathbb{Q}$ ist algebraisch und unendlich, denn $[\bar{\mathbb{Q}}^{\mathbb{C}} : \mathbb{Q}] \geq [\mathbb{Q}(\zeta_p) : \mathbb{Q}] = p - 1$ wobei ζ_p eine Einheitswurzel ungleich 1 ist. △

Für einfache algebraische Erweiterungen gibt es einen eigenen Begriff.

Definition 3.2.20 (Wurzelkörper)**.** Sei K ein Körper und $f \in K[X]$ mit $\operatorname{grad}(f) \geq 1$. Ein *Wurzelkörper von f* ist eine Erweiterung $L|K$ der Form $L = K(a)$ mit $f(a) = 0$.

3.2.1 Zerfällungskörper

Bisher sind wir stets von einer gegebenen Körpererweiterung $L|K$ ausgegangen. Das besondere an Satz 3.2.22 ist, dass für ein beliebigen Körper K eine Erweiterung $L|K$ *konstruiert* wird, die ein Wurzelkörper ist für ein gegebenes nicht konstantes Polynom. Die Ideen dafür stecken bereits im folgenden Lemma; die Aussagen darin haben wir im Prinzip bereits gesehen.

Lemma 3.2.21 (Wurzellemma)**.** *Seien $L = K(a)$ und $f \in K[X]$ mit $f(a) = 0$. Dann ist $[L : K] \leq n := \operatorname{grad}(f)$. Ist f irreduzibel, so ist $[L : K] = n$ und $K[X]/(f)$ ist isomorph zu L.*

Beweis. Nach Lemma 3.2.9 gilt $[L : K] = \operatorname{grad}(f_a)$, und da $f_a|f$ gilt $[L : K] \leq \operatorname{grad}(f)$. Falls $f \in K[X]$ irreduzibel ist, dann gilt $f \sim f_a$, also $[L : K] = n$ nach Lemma 3.2.9, und $g + (f) \mapsto g(a)$ definiert ein Isomorphismus zwischen $K[X]/(f)$ und L. □

Satz 3.2.22 (Wurzelsatz; Kronecker 1882)**.** *Zu jedem $f \in K[X]$ mit $\operatorname{grad}(f) \geq 1$ gibt es einen Wurzelkörper $L|K$. Falls f irreduzibel ist, so ist $L|K$ in folgendem Sinn eindeutig: sind $L_1 = K(a_1)$ und $L_2 = K(a_2)$ mit $f(a_1) = 0 = f(a_2)$, so gibt es genau einen K-Isomorphismus $\varphi\colon L_1 \to L_2$ mit $\varphi(a_1) = a_2$.*

Beweis. Für irreduzibles f stellen wir zunächst fest, dass $K[X]/(f)$ nach Proposition 2.4.29 ein Körper ist, da (f) ein maximales Ideal ist (Proposition 2.4.31). Die Einschränkung des kanonischen Homomorphismus $\pi\colon K[X] \to K[X]/(f)$ auf K ist ein Körperhomomorphismus, also injektiv (Bemerkung 3.0.1). Wir identifizieren die Elemente von K mit ihrem Bild unter dieser Abbildung, und erhalten auf diese Weise aus $K[X]/(f)$ eine Körpererweiterung $L|K$. Wir zeigen nun, dass $L|K$ ein Wurzelkörper

von f ist. Das Polynom f ist von der Gestalt $\sum_{i=0}^{n} c_i X^i$. Betrachten nun $a := X+(f) \in L$. Dann gilt in L

$$f(a) = \sum_{i=0}^{n} c_i a^i = \sum_{i=0}^{n} c_i (X + (f))^i = \sum_{i=0}^{n} c_i X^i + (f) = f + (f) = (f) = 0.$$

Jedes Element $\sum_{i=0}^{k} d_i X^i + (f)$ von L lässt sich schreiben als $\sum_{i=0}^{k} d_i a^i$, also $L = K(a)$ und L ist Wurzelkörper von K. Die Eindeutigkeit von L bis auf K-Isomorphie folgt aus Lemma 3.2.21: $K(a_1) \cong K[X]/(f) \cong K(a_2)$. Jeder Isomorphismus ist eindeutig durch $\phi(a_1) = \phi(a_2)$ festgelegt.

Falls nun f reduzibel ist, wählen wir einen irreduziblen Faktor g von f (denn $K(x)$ ist faktoriell, Lemma 2.5.3); dann ist $K[X]/(g)$ isomorph zu einem Wurzelkörper $K(a)$ von g, der dann auch Wurzelkörper ist von f. □

Wir werden die Ideen aus dem Satz 3.2.22 zu Wurzelkörpern nun in zweierlei Hinsicht verallgemeinern:

- Statt nach einer einfachen Körpererweiterung von K zu suchen, in der ein gegebenes $f \in K[X]$ eine Nullstelle hat, suchen wir nun nach einem Erweiterungskörper L, in dem f *vollständig* in Linearfaktoren zerfällt. Von diesem können wir im allgemeinen nicht erwarten, dass er einfach ist; er soll aber kleinstmöglich sein in dem Sinn, dass er von der Gestalt $K(a_1, \ldots, a_n)$ ist, wobei $a_1, \ldots, a_n$ die Nullstellen von f in L sind.
- Weiterhin wollen wir das nicht nur für ein Polynom f, sondern für eine beliebige Menge von Polynomen $P \subseteq K[X]$ gleichzeitig tun.

Dies führt uns zu folgendem Begriff.

Definition 3.2.23 (Zerfällungskörper[2])**.** Sei $P \subseteq K[X]$. Ein Erweiterungskörper L von K heißt *Zerfällungskörper von P über K*, falls

- jedes $f \in P$ über L in Linearfaktoren zerfällt, also $f = c \cdot \prod_{i=1}^{n}(X - a_i)$ für $c \in K$ und $a_1, \ldots, a_n \in L$, und
- $L = K(\bigcup_{f \in P} \{a \in L \mid f(a) = 0\})$.

Falls $L|K$ ein Zerfällungskörper von $P = \{f\}$ über K ist, so nennen wir ihn auch *Zerfällungskörper von f über K*.

Proposition 3.2.24. *Zu jedem $f \in K[X]$ existiert ein Zerfällungskörper über K.*

Beweis. Aus Satz 3.2.22 mit vollständiger Induktion nach n. □

Lemma 3.2.25. *Ist $L|K$ ein Zerfällungskörper von $f \in K[X]$ mit $\operatorname{grad}(f) = n \in \mathbb{N}$, so ist $[L : K] \leq n!$.*

[2] Englisch: *splitting field*; französisch: *corps de décomposition*.

Beweis. Aus Lemma 3.2.21, wieder per vollständiger Induktion nach n. □

Beispiel 3.2.26. Sei $f \in K(X)$ mit $\operatorname{grad}(f) = 2$. Dann ist jeder Wurzelkörper von f schon ein Zerfällungskörper. △

Beispiel 3.2.27. Sei $f \in K(X)$ mit $\operatorname{grad}(f) = 3$. Hier unterscheiden wir zwei Fälle.

- f is irreduzibel. Sei $K_1 := K(a)$ ein Wurzelkörper von f. Dann ist $f = (X - a)f_1$ für $f_1 \in K_1[X]$ vom Grad 2. Ist f_1 reduzibel in $K_1[X]$, so ist K_1 bereits ein Zerfällungskörper von f, und $[K_1 : K] = 3$. Falls f_1 irreduzibel in $K_1[X]$ ist (zum Beispiel, falls $f = (X^3 - 2)$), dann ist jeder Wurzelkörper K_2 von f_1 ein Zerfällungskörper von f mit $[K_2 : K] = 3 \cdot 2 = 6$.
- f ist reduzibel. Dann ist f von der Gestalt $f = (X - a)f_1$ für $f_1 \in K[X]$ vom Grad 2. Ist f_1 ebenfalls reduzibel in $K[X]$, so ist K bereits ein Zerfällungskörper von f. Ist f_1 irreduzibel in $K[X]$, dann ist jeder Wurzelkörper K_1 von f_1 ein Zerfällungskörper von f mit $[K_1 : K] = 2$. △

Wir wollen nun zeigen, dass die Zerfällungskörper von $P \subseteq K[X] \setminus K$ bis auf K-Isomorphie eindeutig bestimmt sind. Die Existenz werden wir erst im nächsten Abschnitt zeigen. Sei $\varphi\colon K \to K'$ ein Körperhomomorphismus und $f = \sum_{i=0}^{n} a_i X^i \in K[X]$. Dann schreiben wir f^φ für das Polynom $\sum_{i=0}^{n} \varphi(a_i) X^i$ aus $K'[X]$.

Lemma 3.2.28 (Fortsetzungslemma)**.** *Es seien $\varphi\colon K \to K'$ ein Körperisomorphismus, $P \subseteq K[X] \setminus K$, und $P' := \{f^\varphi \mid f \in P\}$. Ist L Zerfällungskörper von P über K und L' Zerfällungskörper von P' über K', dann kann φ zu einem Isomorphismus von L auf L' fortgesetzt werden.*

Beweis. Für eine einfachere Notation werden wir annehmen, dass $K' = K$ und φ die identische Abbildung ist; der allgemeine Fall folgt aus diesem. Es sei $\mathcal{F}$ die Menge aller Fortsetzungen von φ zu Isomorphismen zwischen Teilkörpern von L und von L'. Wir definieren auf $\mathcal{F}$ eine Ordnungsrelation $\leq$, nämlich $\sigma \leq \tau$ falls τ eine Fortsetzung von σ ist. Die Menge $\mathcal{F}$ enthält φ, ist also nicht leer. Sei $\mathcal{K}$ eine Kette in $(\mathcal{F}, \leq)$. Dann ist die Vereinigung der Definitionsbereiche der Elemente von $\mathcal{K}$ ein Teilkörper E von L, der K enthält. Falls $a \in E$ und $\rho, \sigma \in \mathcal{K}$, dann können wir ohne Beschränkung der Allgemeinheit annehmen, dass $\rho \leq \sigma$, da $\mathcal{K}$ eine Kette ist. Inbesondere gilt $\rho(a) = \sigma(a)$ für alle a im Definitionsbereich von ρ. Wir können daher für $a \in E$ ein beliebiges $\rho \in \mathcal{K}$ mit a im Definitionsbereich wählen, und erhalten mit $\chi(a) := \rho(a)$ eine wohldefinierte Erweiterung $\chi\colon E \to L'$ von φ. Man rechnet einfach nach, dass χ ein Homomorphismus, und eine obere Schranke von $\mathcal{K}$ ist. Nach dem Zornschen Lemma gibt es also in $\mathcal{F}$ ein maximales Element $\psi\colon F \to L'$.

Behauptung 1. $F = L$. Sei $f \in P$ und $a \in L$ mit $f(a) = 0$. Da L' Zerfällungskörper von P' über $K' = K$, hat $f \in P = P'$ eine Wurzel in L'. Nach Satz 3.2.22 kann man ψ daher zu einem injektiven Homomorphismus von $F(a)$ nach L' fortsetzen. Wegen der Maximalität von ψ folgt $F(a) = F$ und somit $a \in F$. Daraus folgt $F = L$.

Behauptung 2. $\psi(F) = L'$. Sei $a' \in L'$. Da L' Zerfällungskörper von $P' = P$ über K, gibt es ein $f \in P$ mit $f(a') = 0$. Da L Zerfällungskörper von P über K ist, zerfällt f

über L in Linearfaktoren, also $f = c(X - a_1)\cdots(X - a_n)$ für $c, a_1, \ldots, a_n \in L$. Dann gilt $f = \psi(c)(X - \psi(a_1))\cdots(X - \psi(a_n))$. Da $f(a') = 0$, ist $a' \in \{\psi(a_1), \ldots, \psi(a_n)\} \subseteq \psi(F)$, was zu zeigen war. □

Als unmittelbare Konsequenz für $K = K'$ erhalten wir den folgenden Satz.

Satz 3.2.29. *Alle Zerfällungskörper von $P \subseteq K[X] \setminus K$ sind bis auf K-Isomorphie eindeutig bestimmt.*

3.2.2 Der algebraische Abschluss

Wir haben den relativen algebraischen Abschluss von K bezüglich einer Körpererweiterung $L|K$ bereits in Lemma 3.2.16 definiert. Der Begriff des algebraischen Abschlusses eines Körpers läßt sich aber auch *absolut* definieren, d.h., ohne Bezug auf einen Oberkörper L. Dieses Thema führt die Inhalte aus den letzten beiden Kapiteln weiter.

Definition 3.2.30. Der Körper K heißt *algebraisch abgeschlossen* falls jedes $f \in K[X]$ mit $\operatorname{grad}(f) \geq 1$ eine Nullstelle in K besitzt.

Bemerkung 3.2.31. Falls K algebraisch abgeschlossen ist, dann ist K sein eigener Zerfällungskörper bezüglich $P := K[X] \setminus K$.

Beispiel 3.2.32. Das klassische Beispiel ist der Körper der komplexen Zahlen $\mathbb{C}$; wir werden diesen Satz später beweisen. △

Lemma 3.2.33. *Die folgenden Aussagen sind äquivalent.*

1. *K ist algebraisch abgeschlossen.*
2. *Jedes $f \in K[X]$ vom Grad mindestens 1 zerfällt über K in Linearfaktoren.*
3. *K hat keine echten algebraischen Erweiterungen.*

Beweis. $1 \Rightarrow 2$: sei $f \in K[X]$ mit $n := \operatorname{grad}(f) \geq 1$. Der Beweis ist per Induktion nach n. Es hat f nach Voraussetzung eine Nullstelle $a \in K$. Dann ist $f = (X - a)g$ für ein $g \in K[X]$. Falls $\operatorname{grad}(g) = 0$ ist nichts weiter zu zeigen. Falls $\operatorname{grad}(g) \geq 1$, dann zerfällt g nach Induktionsvoraussetzung über K in Linearfaktoren, und damit auch f.

$2 \Rightarrow 3$: wenn $L|K$ algebraisch und $a \in L$, dann zerfällt insbesondere f_a in Linearfaktoren, und damit ist $a \in K$, also $L = K$.

$3 \Rightarrow 1$: Sei $f \in K[X]$ mit $\operatorname{grad}(f) \geq 1$. Nach Satz 3.2.22 existiert ein Wurzelkörper $L|K$ zu f, und damit auch $a \in L$ mit $f(a) = 0$. Da K nach Voraussetzung keine echten algebraischen Erweiterungen besitzt, ist $L = K$, und damit hat f eine Nullstelle in K. □

Definition 3.2.34. L ist *ein algebraischer Abschluss* von K, falls L algebraisch abgeschlossen ist und $L|K$ algebraisch ist.

Proposition 3.2.35. *Alle algebraischen Abschlüsse von K sind K-isomorph.*

Beweis. Seien L und L' algebraische Abschlüsse von K. Dann sind L wie auch L' Zerfällungskörper von $P := K[X] \setminus K$ über K, und es folgt aus Satz 3.2.29, die K-Isomorie von L und L'. □

Beispiel 3.2.36. $\mathbb{C}$ ist ein algebraischer Abschluss von $\mathbb{R}$, nicht aber von $\mathbb{Q}$, da $\mathbb{C}|\mathbb{Q}$ nicht algebraisch ist. △

Das folgende Beispiel zeigt, dass der relative algebraische Abschluss von K in L im allgemeinen kein algebraischer Abschluss von K ist.

Beispiel 3.2.37. Wir betrachten die Körpererweiterung $\mathbb{R}|\mathbb{Q}$. Das Polynom $X^2 + 1 \in \mathbb{Q}[X]$ hat im (relativen) algebraischen Abschluss $\bar{\mathbb{Q}}^{\mathbb{R}}$ von $\mathbb{Q}$ in $\mathbb{R}$ keine Nullstellen. Im algebraischen Abschluss $\bar{\mathbb{Q}}^{\mathbb{C}}$ von $\mathbb{Q}$ in $\mathbb{C}$ dagegen schon. Der Körper der algebraischen Zahlen (Beispiel 3.2.19) ist ein algebraischer Abschluss von $\mathbb{Q}$. △

Lemma 3.2.38. *Es sei $L|K$ eine Körpererweiterung. Ist L algebraisch abgeschlossen, so ist der relative algebraische Abschluss $\bar{K}^L$ von K ein algebraischer Abschluss von K.*

Beweis. Da $\bar{K}^L$ per Definition algebraisch über K ist, müssen wir blos zeigen, dass $\bar{K}^L$ algebraisch abgeschlossen ist. Sei $f \in \bar{K}^L[X]$ mit $\operatorname{grad}(f) \geq 1$. Da L algebraisch abgeschlossen ist, hat f in L eine Nullstelle a. Also ist a algebraisch über K, und damit $a \in \bar{K}^L$. Also besitzt f eine Nullstelle in $\bar{K}^L$. □

Im Beweis der folgenden Aussage steckt via Satz 2.4.35 das Lemma von Zorn (LA20).[3]

Satz 3.2.39 (Steinitz 1910)**.** *Jeder Körper K besitzt einen bis auf K-Isomorphie eindeutig bestimmten algebraischen Abschluss.*

Beweis. Betrachte $\mathcal{F} := K[X] \setminus K$; für jedes $f \in \mathcal{F}$ sei X_f eine formale Variable. Es sei $R := K[\{X_f \mid f \in \mathcal{F}]$ der Polynomring in unendlich vielen Variablen (Abschnitt 2.2.4) mit dem Ideal $I := (f(X_f) \mid f \in \mathcal{F}) \trianglelefteq R$. Dann ist I ein echtes Ideal von R und nach Satz 2.4.35 ist I in einem maximalen Ideal $M \trianglelefteq R$ enthalten. Dann ist $L_1 := R/M$ ein Körper (Lemma 2.4.36), in welchem jedes Polynom aus $\mathcal{F}$ eine Nullstelle besitzt (siehe Beweis von Satz 3.2.22).

Wir wiederholen diese Konstruktion für L_1 anstatt K, und erhalten eine weitere Körpererweiterung L_2, und auf diese Weise eine unendliche Kette

$$K = L_0 \subseteq L_1 \subseteq L_2 \subseteq \cdots$$

von Körpererweiterungen (siehe Abbildung 3.1). Dann ist $L := \bigcup_{i \in \mathbb{N}} L_i$ algebraisch abgeschlossen (warum?!), und $\bar{K}^L$ ein algebraischer Abschluss von K. Die Eindeutigkeit haben wir bereits in Proposition 3.2.35 bewiesen. □

[3] Allerdings folgt umgekehrt das Lemma von Zorn *nicht* aus diesem Satz; es ist bekannt, dass dieser äquivalent ist zum Kompaktheitssatz der Logik erster Stufe. Für eine Übersicht siehe [1], Anhang A.2.

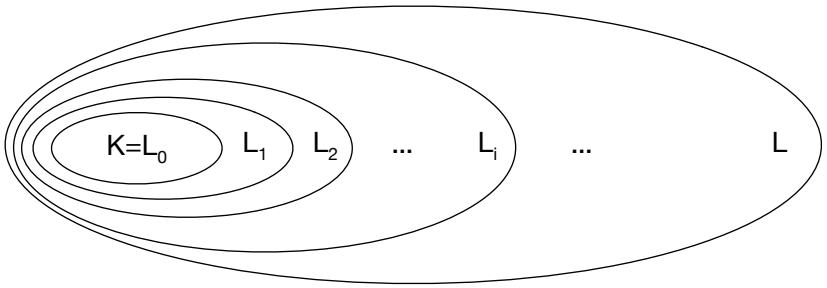


Abbildung 3.1: Die Kettenkonstruktion des algebraischen Abschlusses von K aus dem Beweis von Satz 3.2.39.

Definition 3.2.40 (algebraischer Abschluss)**.** Den bis auf K-Isomorphie eindeutig bestimmten algebraischen Abschluss von K bezeichnen wir mit $\bar{K}$.

Korollar 3.2.41. *Zu jedem $P \subseteq K[X]$ gibt es einen Zerfällungskörper über K.*

Beweis. Der Teilkörper von $\bar{K}$, der aus K durch Adjunktion von allen Nullstellen von Polynomen aus P hervorgeht, leistet das Gewünschte. □

Übung 85. Sei $L|K$ eine algebraische Erweiterung von K. Dann gilt $\bar{K} \cong_K \bar{L}$.

Bemerkung 3.2.42. Man kann zeigen, dass L_1 aus dem Beweis von Satz 3.2.39 bereits ein algebraischer Abschluss von K ist (Übung 10 in Abschnitt 3.7 in [2]), und damit K-isomorph zu $\bar{K}$ (Proposition 3.2.35) ist. Die Kettenkonstruktion im Beweis ist allerdings bequemer, um die Existenz von $\bar{K}$ zu zeigen.

3.2.3 Körperautomorphismen

Sei $L|K$ eine algebraische Körpererweiterung.

Definition 3.2.43. K-Isomorphismen von L nach L heißen auch *K-Automorphismen von L*. Die Menge aller K-Automorphismen wird mit $\mathrm{Aut}(L|K)$ bezeichnet, und heisst die *Automorphismengruppe* von $L|K$ (auch: *Galoisgruppe* von $L|K$).

Offenbar ist $\mathrm{Aut}(L|K) \subseteq \mathrm{Sym}(L)$ eine Permutationsgruppe.

Lemma 3.2.44. *Sei $L|K$ algebraisch. Dann ist jeder K-Homomorphismus $\varphi\colon L \to L$ ein K-Automorphismus von L.*

Beweis. Wir haben bereits bemerkt, dass φ injektiv ist (Bemerkung 3.0.1), und es bleibt blos die Surjektivität zu zeigen. Sei $a \in L$. Da a algebraisch über K ist, hat es ein Minimalpolynom f_a; es seien $a_1, \ldots, a_n$ alle Wurzeln von f_a. Sei $E := K(a_1, \ldots, a_n)$. Dann ist $E|K$ endlich (Proposition 3.2.13). Da $\varphi(a) \in \{a_1, \ldots, a_n\}$, ist $\varphi|_E$ eine injektive K-lineare Abbildung des endlichdimensionalen K-Vektorraums E in sich selbst, und damit auch surjektiv. Es existiert also ein $b \in E \subseteq L$ mit $\varphi(b) = a$, und daher ist φ surjektiv. □

Satz 3.2.45. *Sei E ein Zwischenkörper von $\bar{K}|K$. Dann läßt sich jeder K-Homomorphismus von E nach $\bar{K}$ zu einem K-Automorphismus von $\bar{K}$ fortsetzen.*

Beweis. Jeder K-Homomorphismus φ von E nach $\bar{K}$ ist ein Körperisomorphismus zwischen E und einem Teilkörper E' von $\bar{K}$ (Bemerkung 3.0.1). Nach Satz 3.2.28 angewandt auf $L := L' := \bar{K}$, $P := K[X] \setminus X$, $K := E$, und $K' := L'$ läßt sich φ auf einen K-Automorphismus von $\bar{K}$ fortsetzen. □

Definition 3.2.46. Zwei Elemente $a, b \in \bar{K}$ heißen *K-konjugiert*, wenn es einen $\sigma \in \mathrm{Aut}(\bar{K}|K)$ gibt mit $\sigma(a) = b$.

Offenbar ist K-Konjugiertheit eine Äquivalenzrelation auf $\bar{K}$.

Beispiel 3.2.47. In $\mathbb{C}|\mathbb{R}$ sind i und $-i$ konjugiert. Beide haben das Minimalpolynom $X^2 + 1$. △

Lemma 3.2.48. *Seien $a, b \in \bar{K}$. Dann sind a und b genau dann K-konjugiert, wenn $f_a = f_b$, das heißt, wenn sie das gleiche Minimalpolynom besitzen.*

Beweis. Wenn $\varphi \in \mathrm{Aut}(\bar{K}|K)$ so, dass $\varphi(a) = b$, dann ist $f_a(b) = f_a(\varphi(a)) = \varphi(f_a(a)) = \phi(0) = 0$, also $f_b | f_a$. Analog zeigt man $f_b | f_a$, und daher $f_b = f_a$ wegen der Eindeutigkeit des Minimalpolynoms.

Die umgekehrte Richtung folgt aus Satz 3.2.22: nach diesem Satz existiert zu $f_a = f_b$ ein Wurzelkörper $L|K$, und ein K-Automorphismus φ von L mit $\varphi(a) = b$. Nach Satz 3.2.45 können wir annehmen, dass $\bar{K}|L$ (Übung 85). Dann läßt sich φ nach Satz 3.2.45 zu einem Automorphismus von $\bar{K}$ fortsetzen. □

3.3 Separable Polynome

Jedes Polynom $f \in K[X]$ zerfällt über seinem algebraischen Abschluss $\bar{K}$ in Linearfaktoren. Häufig ist es dabei so, bei einem irreduziblen f keiner der Linearfaktoren mehrfach auftritt. In anderen Worten: häufig (aber nicht immer!) sind alle Nullstellen von f in $\bar{K}$ einfache Nullstellen.

Definition 3.3.1. Sei $a \in K$. Dann heißt

$$v(f, a) := \sup(k \in \mathbb{N} : (X - a)^k | f\} \in \mathbb{N} \cup \{\infty\}$$

die *Vielfachheit von a bezüglich f*. Falls $v(f, a) \geq 1$, so ist a eine Nullstelle von f, und falls $v(f, a) = 1$, so heißt a eine *einfache* Nullstelle von f.

Bemerkung 3.3.2. Ist $L|K$ eine Erweiterung und $g \in K[X]$, so gilt $g|f$ in $K[X]$ genau dann, wenn $g|f$ in $L[X]$. Insbesondere ändert sich $v(f, a)$ nicht, wenn wir K durch L ersetzen.

Definition 3.3.3. Ein Polynom $f \in K[X]$ heißt *separabel*, wenn jede Nullstelle $a \in \bar{K}$ von f einfach ist, und sonst *inseparabel*.

Beispiel 3.3.4. Das Polynom $X^3 - 2 \in \mathbb{R}[X]$ ist separabel, da es in $\mathbb{C}$ drei verschiedene komplexe Nullstellen hat. Über dem Körper $\mathbb{F}_3$ dagegen gilt $X^3 - 2 = (X+1)^3$, und daher hat $X^3 - 2$ eine dreifache Nullstelle in $\mathbb{F}_3$. △

Bemerkung 3.3.5. Für $f \neq 0$ gilt

$$|\{a \in K \mid f(a) = 0\}| \leq \sum_{a \in K} v(f,a) \leq \sum_{a \in \bar{K}} v(f,a) = \operatorname{grad}(f).$$

Insbesondere ist f genau dann separabel, wenn f genau $\operatorname{grad}(f)$ viele verschiedene Nullstellen in $\bar{K}$ hat.

Im folgenden werden wir praktische Kriterien kennenlernen, um zu testen, ob f separabel ist. Aus Schule bekannt ist der Begriff Ableitung einer Funktion. Wir geben hier nochmals die Definition der (formalen) Ableitung eines Polynoms, welcher bereits in LA10 behandelt wurde.

Definition 3.3.6. Sei $f = \sum_{i=0}^{n} a_i X^i \in K[X]$. Dann ist die *(formale) Ableitung von* f ist definiert als

$$f' := \sum_{i=1}^{n} i a_i X^{i-1} \in K[X]$$

Bemerkung 3.3.7. Statt f' wird bisweilen auch $\frac{1}{dX} f(X)$ geschrieben.

Es gelten die folgenden Ableitungsregeln.

Lemma 3.3.8. *Für $f, g \in K[X]$ und $a, b \in K$ gelten*

- $(af + bg)' = af' + bg'$ *(Linearität),*
- $(fg)' = f'g + fg'$ *(Produktregel),*
- $f(g(X))' = f'(g(X)\dot{g}'(X)$ *(Kettenregel).*

Das folgende ist eine allgemeinere Formulierung von einem Lemma aus LA10.

Lemma 3.3.9. *Es sei L ein Zerfällungskörper von $f \in K[X]$. Dann ist $a \in L$ genau dann mehrfache Wurzel von f, wenn $f(a) = 0 = f'(a)$.*

Beweis. Falls a mehrfache Wurzel von f ist, so gilt in $L[X]$, dass $f = (X-a)^2 g$ für ein $g \in L[X]$. Also $f' = 2(X-a)g + (X-a)^2 g'$, und $f'(a) = 0$.

Falls a dagegen einfache Wurzel von f ist, so gilt in $L[X]$, dass $f = (X-a)q$ für ein $q \in L[X]$ mit $q(a) \neq 0$. Dann gilt $f' = q + (X-a)q'$, also $f'(a) = q(a) \neq 0$. □

Lemma 3.3.10 (Separabilitätskriterium)**.** *Sei $f \in K[X] \setminus \{0\}$. Dann ist f genau dann separabel, wenn $1 \in \operatorname{ggT}(f, f')$.*

Beweis. Sind f und f' teilerfremd, dann existieren $q, r \in K[X]$ mit $qf + rf' = 1$ (siehe Korollar 2.4.18). Falls es eine mehrfache Wurzel $a \in \bar{K}$ von f gäbe, wäre $f(a) = 0 = f'(a)$ nach Lemma 3.3.9, und damit $0 = qf(a) + fr'(a)$, im Widerspruch zu $qf + rf' = 1$. Also hat f keine mehrfache Nullstelle.

Haben f und f' dagegen einen gemeinsamen nicht-konstanten Teiler $t \in K[X]$, dann hat t eine Wurzel a in $\bar{K}$, und nach Lemma 3.3.9 ist f mehrfache Nullstelle. □

Lemma 3.3.11. *Sei $f \in K[X]$ irreduzibel. Dann ist f genau dann separabel, wenn $f' \neq 0$.*

Beweis. Falls f mehrfache Nullstellen in $\bar{K}$ hat, dann haben f und f' einen nicht-konstanten gemeinsamen Teiler $t \in K[X]$ nach Lemma 3.3.10. Da f irreduzibel und $t|f$, so ist $f = ct$ für ein $c \in K$, und insbesondere $\operatorname{grad}(t) = \operatorname{grad}(f)$. Da $\operatorname{grad}(f) > \operatorname{grad}(f')$ und $t|f'$ folgt $f' = 0$. Umgekehrt, falls $f' = 0$, dann haben f und f' den nicht-konstanten gemeinsamen Teiler f, und f hat mehrfache Nullstellen in $\bar{K}$ nach Lemma 3.3.10. □

Korollar 3.3.12. *Falls $\operatorname{char}(K) = 0$, so ist jedes irreduzible $f \in K[X]$ separabel.*

Beweis. Falls $f \in K$ ist f trivialerweise separabel. Ansonsten gilt wegen $\operatorname{char}(K) = 0$, dass $f' \neq 0$, und die Aussage folgt aus Lemma 3.3.11. □

Es gibt allerdings Körper K mit $\operatorname{char}(K) > 0$ mit irreduziblen Polynomen in $K[X]$, die nicht separabel sind, wie das folgende Beispiel zeigt.

Beispiel 3.3.13. Sei $K := \mathbb{F}_p(t) = \operatorname{Quot}(\mathbb{F}_p[t])$. Dann ist das Polynom

$$f = X^p - t \in K(t)[X]$$

irreduzibel (Beispiel 2.6.7), und nach Lemma 3.3.11 inseparabel, da $f' = pX^{p-1} = 0$.

Proposition 3.3.14 (Inseparabilitätskriterium)**.** *Sei $f \in K[X]$ irreduzibel und $\operatorname{char}(K) = p > 0$. Dann ist f genau dann inseparabel, wenn es ein $q \in K[X]$ gibt mit $f = q(X^p)$.*

Beweis. Sei $f = \sum_{i=0}^{n} a_i X^i$. Nach Lemma 3.3.11 ist f genau dann inseparabel, wenn $f' = 0$, also wenn $ia_i = 0$ für jedes $i \in \{1, \dots, n\}$. Für die durch p teilbaren i gilt ohnehin $i \cdot a_i = 0$. Falls $p \nmid i$, so gilt genau dann $ia_i = 0$, wenn $a_i = 0$. Also ist f genau dann inseparabel, wenn f geschrieben werden kann als $f = \sum_{i=0}^{d} b_i X^{ip}$ für $b_1, \dots, b_k \in K$, also von der Gestalt $f = q(X^p)$ ist für ein $q \in K[X]$. □

Proposition 3.3.14 verallgemeinert die Beobachtung aus Beispiel 3.3.13, denn $f = X^p - t = q(X^p)$ für $q = X - t \in K[X]$. In einem Körper der Charakteristik $p > 0$ nimmt die binomische Formel für p-Potenzen eine besonders einfache Gestalt an.

Lemma 3.3.15 (Erstisträumchen)**.** *Sei p eine Primzahl und R ein Integritätsring der Charakteristik p. Dann gilt für $a, b \in R$ und $r \in \mathbb{N}$, dass*[4]

$$(a+b)^{p^r} = a^{p^r} + b^{p^r}$$
$$\text{und } (a-b)^{p^r} = a^{p^r} - b^{p^r}.$$

[4] Im englischen Wikipedia findet sich diese Gleichung unter dem Eintrag 'freshman's dream', und im französischen unter 'rêve du première année'.

Beweis. Per vollständiger Induktion nach r. Für $r = 1$ nutzen wir, dass

$$\binom{p}{k} = \frac{p(p-1)\cdots(p-k+1)}{k!}$$

für $k \in \{1, \dots, p-1\}$ den Primfaktor p besitzt, im Nenner aber nicht, also durch p teilbar ist. Also ist $(a+b)^p = \sum_{k=0}^{p} \binom{p}{k} a^k b^{p-k} = a^p + b^p$. Falls $p > 3$ ungerade, so gilt

$$\begin{aligned}(a-b)^p &= \sum_{k=0}^{p} \binom{p}{k} a^k (-b)^{p-k} \\ &= -\binom{p}{0} a^0 b^p + \binom{p}{k} a^1 b^{p-1} - \cdots + \binom{p}{p} a^p b^0 = a^p - b^p.\end{aligned}$$

Falls $p = 2$, so gilt $(a-b)^p = (a+b)^p = a^p + b^p = a^p - b^p$. Im Induktionsschritt rechnen wir $(a+b)^{p^r} = ((a+b)^p)^{p^{r-1}} = (a^p + b^p)^{p^{r-1}} = a^{p^r} + b^{p^r}$. □

Lemma 3.3.16 (Separierungslemma)**.** *Sei $f \in K[X]$ irreduzibel und $\mathrm{char}(K) = p > 0$. Sei $r \in \mathbb{N}$ maximal, so dass $f = g(X^{p^r})$ für ein $g \in K[X]$. Dann ist g irreduzibel, separabel, und jede Nullstelle von f hat Vielfachheit p^r.*

Beweis. Wenn $g = rs$, dann ist $f = r(X^{p^r})(s(X^{p^r})$, und da f irreduzibel ist, muss auch $g \in K[X]$ irreduzibel sein. Wir wenden nun Proposition 3.3.14 an auf das Polynom $g \in K[X]$: da r maximal gewählt war, gibt es kein $q \in K[X]$ mit $g = q(X^p)$. Also besagt Proposition 3.3.14, dass g separabel ist. Sei nun $g = (X - a_1)\cdots(X - a_n)$ für $a_1, \dots, a_n \in \bar{K}$. Sei $c_i \in \bar{K}$ die Nullstelle von $X^{p^r} - a_i$, so dass $a_i = c_i^{p^r}$. Dann ist

$$\begin{aligned}f = g(X^{p^r}) &= (X^{p^r} - a_1)\cdots(X^{p^r} - a_n) \\ &= (X^{p^r} - c_1^{p^r})\cdots(X^{p^r} - c_n^{p^r}) \\ &= (X - c_1)^{p^r}\cdots(X - c_n)^{p^r}, \qquad \text{(Lemma 3.3.15)}\end{aligned}$$

und daher hat jede Nullstelle von f in $\bar{K}$ die Vielfachheit p^r. □

Übung 86. Sei $f \in K[X] \setminus \{0\}$. Für $a \in K$ gilt $v(f', a) \geq v(f, a) - 1$. Die Ungleichung ist genau dann strikt, wenn $\mathrm{char}(K) | v(f, a)$.

3.3.1 Separable Körpererweiterungen

Ein Element a eines Erweiterungskörpers L von K heißt *separabel über K* wenn a algebraisch über K ist und sein Minimalpolynom f_a separabel ist, und *inseparabel* sonst. Eine Körpererweiterung $L|K$ heißt *separabel* wenn jedes Element aus L separabel über K ist. Separable Körpererweiterungen sind also stets algebraisch.

Beispiel 3.3.17. $L|K$ eine algebraische Körpererweiterung. Falls $\mathrm{char}(K) = 0$, dann ist $L|K$ separabel (Korollar 3.3.12). △

Bemerkung 3.3.18. Sei $L = K(a)$ eine einfache algebraische Körpererweiterung und f_a das Minimalpolynom von a über K. Dann gilt

$$\begin{aligned}[L : K] &= \operatorname{grad}(f) && \text{(Lemma 3.2.9)}\\ &\geq |\{x \in \bar{K} \mid f(x) = 0\}| \\ &= |\operatorname{Hom}_K(L, \bar{K})| && \text{(Satz 3.2.22).}\end{aligned}$$

Definition 3.3.19. Sei $L|K$ algebraisch. Dann heißt $[L : K]_s := |\operatorname{Hom}_K(L, \bar{K})|$ der *Separabilitätsgrad* von $L|K$.

Bemerkung 3.3.20. Falls $L = K(a)$ eine einfache algebraische Körpererweiterung ist, dann gilt $[L : K] \geq [L : K]_s$, und Gleicheit gilt genau dann, wenn $L|K$ separabel ist.

Lemma 3.3.21 (Separabilitätsgradformel)**.** *Sei M ein Zwischenkörper einer algebraischen Körpererweiterung $L|K$. Dann gilt*

$$[L : K]_s = [L : M]_s \cdot [M : K]_s.$$

Inbesondere ist $[M : K]_s \leq [L : K]_s$.

Beweis. Es seien $\{\sigma_i \mid i \in I\} := \operatorname{Hom}_K(M, \bar{K})$ wobei die σ_i alle verschieden sind, und $\{\tau_j \mid j \in J\} := \operatorname{Hom}_M(L, \bar{K})$ wobei die τ_j alle verschieden sind. Für jedes $i \in I$ hat σ_i eine Fortsetzung $\bar{\sigma}$ auf ganz $\bar{K}$ (Lemma 3.2.45). Es genügt zu zeigen, dass

- $\operatorname{Hom}_K(L, \bar{K}) = \{\bar{\sigma}_i \circ \tau_j \mid i \in I, j \in J\}$, und
- die Abbildungen $\bar{\sigma}_i \circ \tau_j$ für alle $(i, j) \in I \times J$ verschieden sind.

Für jedes $i \in I, j \in J$ ist $\bar{\sigma}_i \circ \tau_j \in \operatorname{Hom}_K(L, \bar{K})$. Umgekehrt sei $\tau \in \operatorname{Hom}_K(L, \bar{K})$. Es gilt $\tau|_M \in \operatorname{Hom}_K(M, \bar{K})$, also gibt es ein $i \in I$ mit $\tau|_M = \sigma_i$. Dann ist $\bar{\sigma}_i^{-1} \circ \tau \in \operatorname{Hom}_M(L, \bar{K})$, also gibt es ein $j \in J$ mit $\bar{\sigma}^{-1} \circ \tau = \tau_j$. Somit gilt $\tau = \sigma_i \circ (\bar{\sigma}^{-1} \circ \tau) = \sigma_i \circ \tau_j$.

Um die zweite Eigenschaft zu zeigen, sei $\bar{\sigma}_i \circ \tau_j = \bar{\sigma}_i' \circ \tau_j'$. Da $\tau_j|_M = \mathrm{id}_M = \tau_j'|_M$ gilt $\sigma_i = \sigma_i'$ und damit $i = i'$. Also $\bar{\sigma}_i = \bar{\sigma}_i'$ und somit $\tau_j = \tau_j'$, also $j = j'$. □

Lemma 3.3.22. *Sei $L|K$ endlich und $p = \mathrm{char}(K) \geq 0$. Dann ist $[L : K] = p^l \cdot [L : K]_s$ für ein $l \geq 0$. Insbesondere: $[L : K]_s \leq [L : K]$ und $[L : K]_s$ ist ein Teiler von $[L : K]$.*

Extra nice

Beweis. Sei $L = K(a_1, \ldots, a_n)$. Falls $p = 0$, dann gilt $[K(a_1) : K] = [K(a_1) : K]_s$ (Bemerkung 3.3.20), also

$$[K(a_1) : K] = \underbrace{0^0}_{=1} \cdot [K(a_1) : K]_s$$

und die Aussage folgt per Induktion nach n mit Lemma 3.3.21 und Lemma 3.1.1. Falls $p > 0$, so verfahren wir analog, und verwenden zusätzlich Lemma 3.3.16, welche besagt, dass $[K(a_1) : K] = p^r [K(a_1) : K]_s$ für ein $r \in \mathbb{N}$. □

Proposition 3.3.23. *Sei $L|K$ endlich. Dann sind äquivalent:*

1. $L|K$ *ist separabel.*
2. $L = K(a_1, \ldots, a_n)$ *für* $a_1, \ldots, a_n$ *separabel über* K.
3. $[L : K]_s = [L : K]$.

Beweis. Die Implikation von 1. nach 2. ist trivial. Die Implikation von 2. nach 3. folgt aus Bemerkung 3.3.20 und vollständiger Induktion nach n. Für die Implikation von 3. nach 1., sei $a \in L$. Nach Lemma 3.3.22 gilt $[K(a) : K] = p^\ell \cdot [K(a) : K]$ für ein $l \in \mathbb{N}$. Wir erhalten

$$\begin{aligned} [L : K] &= [L : K(a)] \cdot [K(a) : K] && \text{(Lemma 3.1.1)} \\ &\geq [L : K(a)]_s \cdot p^\ell \cdot [K(a) : K]_s && \text{(Lemma 3.3.22)} \\ &= p^\ell [L : K]_s && \text{(Lemma 3.3.21)} \end{aligned}$$

Falls nun $[L : K]_s = [L : K]$, dann ist $l = 0$, und a ist separabel (Bemerkung 3.3.20). □

Korollar 3.3.24. *Der* relative separable Abschluss von K in L

$$\bar{K}_s^L := \{a \in L \mid a \text{ separabel über } K\}$$

ist ein Teilkörper von L *und eine separable Erweiterung von* K.

Beweis. Seien $a, b \in \bar{K}_s^L$. Dann sind $-a$, $a + b$, und ab in $K(a, b)$. Der Körper $K(a, b)$ ist eine separable Körpererweiterung von K nach Proposition 3.3.23. Also sind $-a$, $a + b$, und ab ebenfalls in $\bar{K}_s^L$. □

Übung 87. Zeigen Sie: sei M ein Zwischenkörper einer algebraischen Körpererweiterung $L|K$. Dann ist $L|K$ genau dann separabel, wenn $L|M$ und $M|K$ separabel sind.

Der relative separable Abschluss wird in Abschnitt 3.3.3 eine wichtige Rolle spielen.

Lemma 3.3.25. *Sei* $L|K$ *eine Körpererweiterung und* $a \in L$ *algebraisch über* K. *Falls* $\mathrm{char}(K) = p > 0$, *dann ist* a *genau dann separabel über* K, *wenn* $K(a^p) = K(a)$.

Beweis. Sei zunächst a separabel über K. Offensichtlicherweise gilt $K(a^p) \subseteq K(a)$; es genügt daher zu zeigen, dass $a \in K(a^p)$. Es ist a auch separabel über $K(a^p)$, denn das Minimalpolynom von a über $K(a^p)$ teilt das Minimalpolynom von a über K (Übung 83). Offenbar ist a eine Nullstelle von $X^p - a^p \in K(a^p)[X]$. Da $X^p - a^p = (X - a)^p$ (Lemma 3.3.15), ist das Minimalpolynom von a über $K(a^p)$ gleich $(X - a)$, da a separabel über $K(a^p)$ ist. Es folgt $a \in K(a^p)$.

Sei nun a inseparabel über K, und sei f_a das Minimalpolynom von a über K. Nach Proposition 3.3.14 kann man also f_a schreiben als $q(X^p)$ für ein $q \in K[X]$. Dann gilt

$$[K(a) : K] = \mathrm{grad}(f_a) > \mathrm{grad}(q) = [K(a^p) : K]$$

also insbesondere $K(a) \neq K(a^p)$. □

3.3.2 Vollkommene Körper

Wir hatten am Anfang von Abschnitt 3.3 bereits erwähnt, dass *'häufig'* die irreduziblen $f \in K[X]$ im algebraischen Abschluss von $\bar{K}$ in paarweise verschiedene Linearfaktoren zerfallen, also separabel sind. In diesem Abschnitt gehen wir der Frage nach, für welche Körper *alle* irreduziblen Polynome separabel sind. Auch dies ist für überraschend viele Körper der Fall, und hat einen Namen verdient.

Definition 3.3.26. Ein Körper K heißt *vollkommen*[5] falls jedes irreduzible $f \in K[X]$ separabel ist.

Beispiel 3.3.27. Ist $\mathrm{char}(K) = 0$, so ist K vollkommen (Korollar 3.3.12). Auch alle algebraisch abgeschlossenen Körper $K = \bar{K}$ (auch die mit Charakteristik $p > 0$, wie zum Beispiel der algebraische Abschluss von $\mathbb{F}_p$) sind vollkommen: denn die einzigen irreduziblen Polynome in $K[X]$ sind von der Form $X - c$ für $c \in K$, und damit separabel. △

Wir wollen nun ein notwendiges und hinreichendes Kriterium für vollkommene Körper K finden. Dazu wird ein gewisser Endomorphismus von K wichtig.

Lemma 3.3.28. *Sei $\mathrm{char}(K) = p > 0$. Die Abbildung $\varphi_p \colon K \to K$ gegeben durch $x \mapsto x^p$ ist ein injektiver Endomorphismus von K.*

Beweis. Bemerkenswert im Beweis ist, dass φ_p auch die Addition bewahrt: Für $a, b \in K$ ist $(a+b)^p = a^p + b^p$, da $p \mid \binom{p}{i}$ für alle $i \in \{1, \dots, p-1\}$. Als Körperhomomorphismus ist φ_p injektiv (Bemerkung 3.0.1). □

Definition 3.3.29. Die Abbildung φ_p aus Lemma 3.3.28 heißt *Frobenius-Endomorphismus* von K.

Lemma 3.3.30. *Ein Körper K ist genau dann vollkommen, wenn $\mathrm{char}(K) = 0$ oder $\mathrm{char}(K) = p > 0$ und der Frobenius-Endomorphismus ist surjektiv, kurz: $\varphi_p(K) = K$.*

Beweis. Nur für den Fall $\mathrm{char}(K) = p > 0$ bleibt etwas zu zeigen. Sei φ_p surjektiv, und $f \in K[X]$ sei irreduzibel. Angenommen, f wäre inseparabel. Dann existiert nach Proposition 3.3.14 ein $q = \sum_{i=0}^{n} a_i X^i \in K[X]$ mit $f = q(X^p)$. Wegen der Surjektivität von φ_p gibt es für jedes $i \in \{0, \dots, n\}$ ein $b_i \in K$ mit $a_i = \varphi_b(b_i) = b_i^p$. Mit Lemma 3.3.15 folgt

$$f = q(X^p) = \sum_{i=0}^{n} b_i^p X^{ip} = \left(\sum_{i=0}^{n} b_i X^i \right)^p$$

im Widerspruch zur Irreduzibilität von f.

Sei nun φ_p nicht surjektiv, und wähle $b \in K \setminus \varphi_p(K)$. Sei L ein Zerfällungskörper von $X^p - b$, und $a \in L$ so, dass $a^p = b$. Dann ist $K(b) = K(a^p) \subsetneq K(a)$, da $b \notin \varphi_p(K)$. Aus $K(a^b) \neq K(a)$ folgt aus Lemma 3.3.25, dass a inseparabel über K ist. □

[5] Im Englischen *'perfect field'*, im Französischen *'corps parfait'*.

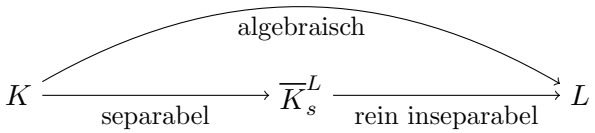


Abbildung 3.2: Algebraische Körpererweiterungen $L|K$ haben den relativen separablen Abschluss $\overline{K}_s^L$ als Zwischenkörper, der rein inseparabel in L liegt.

Korollar 3.3.31. *Jeder endliche Körper ist vollkommen.*

Wir kennen bereits Beispiele von nicht vollkommenen Körpern.

Beispiel 3.3.32. Sei K ein Körper der Charakteristik $p > 0$. Dann ist der Körper $K(X) = \mathrm{Quot}(K[X])$ der rationalen Funktionen in der Unbestimmten X nicht vollkommen. Für $K = \mathbb{F}_p$ haben wir das bereits in Beispiel 3.3.13 gesehen.

Alternativ kann man das mit Lemma 3.3.30 sehen, denn das Polynom $X \in K(X)$ liegt nicht im Bild des Frobenius Endomorphismus. Denn angenommen es gäbe $u, v \in K[X]$, $q \neq 0$, mit $X = (\frac{u}{v})^p$, dann folgt daraus, dass $Xv^p = u^p$. Schreiben $u = \sum_{i=0}^n a_i X^i$ und $v = \sum_{j=0}^m b_j X^j$, so liefert das $\sum_{i=0}^n a_i^p X^{ip} = \sum_{j=0}^m b_j^p X^{jp+1}$. Koeffizientenvergleich liefert $a_i = 0$ und $b_j = 0$ für alle $i \in \{1, \dots, n\}$ und $j \in \{0, \dots, m\}$ (zum Beispiel, falls $p = 2$, dann haben die X links nur gerade Exponenten, und die X rechts nur ungerade Exponenten), im Widerspruch zur Annahme $q \neq 0$. △

Übung 88. Sei $L|K$ algebraisch. Zeige: falls K vollkommen ist, so ist auch L vollkommen.

3.3.3 Rein Inseparable Körpererweiterungen

Wir betrachten in diesem Abschnitt einen Extremfall von nicht separablen algebraischen Körpererweiterungen. Eine algebraische Körpererweiterung $L|M$ heißt *rein inseparabel*, wenn *jedes* $a \in L \setminus K$ inseparabel über K ist.

Bemerkung 3.3.33. Falls $L|K$ algebraisch ist, dann ist jedes $a \in L \setminus \bar{K}_s^L$ inseparabel über $\bar{K}_s^L$. Also ist $L|\bar{K}_s^L$ rein inseparabel; siehe Abbildung 3.2.

Beispiel 3.3.34. Die unechte Erweiterung $K|K$ ist trivialerweise rein inseparabel; dies ist offenbar die einzige Körpererweiterung von K, die separabel und rein inseparabel zugleich ist. △

Bevor wir ein Beispiel für eine echte einfache und rein inseparable Körpererweiterung angeben, beweisen wir die folgenden Charakterisierungen von rein inseparablen Erweiterungen.

Proposition 3.3.35. *Sei K mit $\mathrm{char}(K) = p > 0$. Dann sind äquivalent:*

1. *$L|K$ ist rein inseparabel.*
2. *Für jedes $a \in L$ gibt es ein $r \in \mathbb{N}$ mit $a^{p^r} \in K$.*

3. *Für jedes $a \in L$ ist das Minimalpolynom über K von der Gestalt $X^{p^r} - a^{p^r}$ für ein $r \in \mathbb{N}$.*

4. *Jedes $a \in L$ ist die* einzige *Nullstelle eines Polynoms $f \in K[X]$.*

5. $[L : K]_s = 1$.

Beweis. 1. $\Rightarrow$ 2. : Sei $a \in L$, und f_a das Minimalpolynom von a über K. Wie in Lemma 3.3.16 sei $r \in \mathbb{N}$ maximal, so dass $f_a = g(X^{p^r})$ für ein $g \in K[X]$. Dann besagt Lemma 3.3.16, dass g separabel ist. Da a^{p^r} Nullstelle von g ist, ist a^{p^r} separabel, muss also in K sein.

2. $\Rightarrow$ 3. : Falls $a \in K$ dann ist das Minimalpolynom $(X - a)$, und die Aussage stimmt für $r = 0$. Sei also $a \in L \setminus K$. Es ist a^{p^r} Nullstelle des Polynoms $X^{p^r} - a^{p^r}$, welches per Annahme in $K[X]$ liegt. Weiterhin ist $X^{p^r} - a^{p^r} = (X - a)^{p^r}$ (Lemma 3.3.15), also irreduzibel in $K[X]$, da $a \notin K$. Also ist $X^{p^r} - a^{p^r}$ das Minimalpolynom von a über K.

3. $\Rightarrow$ 4. : Sei $a \in L$. Nach Voraussetzung ist das Minimalpolynom von a über K von der Gestalt $X^{p^r} - a^{p^r}$ für ein $r \in \mathbb{N}$. Da $X^{p^r} - a^{p^r} = (X - a)^{p^r}$ (Lemma 3.3.15), ist a die einzige Nullstelle von f_a.

4. $\Rightarrow$ 5. : Sei $\sigma\colon L \to \bar{K}$ ein K-Homomorphismus. Da $f(\sigma(a)) = \sigma(f(a)) = 0$, und a die einzige Nullstelle von f ist, muss also gelten $\sigma(a) = a$. Somit ist σ eindeutig festgelegt, und es gilt $[L : K]_s = 1$.

5. $\Rightarrow$ 1. : Sei $a \in L$ separabel über K. Dann folgt mit Lemma 3.3.21 aus $[L : K] = 1$, dass $[K(a) : K]_s = 1$. Andererseits gilt $[K(a) : K]_s = [K(a) : K]$, da a separabel ist über K (Proposition 3.3.23). Also ist $a \in K$. □

Beispiel 3.3.36. Die Körpererweiterung $\mathbb{F}_p(t)|\mathbb{F}_p(t^p)$ ist ein Beispiel für eine echte einfache Körpererweiterung, die rein inseparabel ist. Dazu genügt es wegen Proposition 3.3.35 (2), nachzurechnen, dass für jedes $a \in \mathbb{F}_p(t)$ gilt, dass $a^p \in \mathbb{F}_p(t^p)$. Seien $u(t) = \sum_{i=0}^{n} u_i t^i \in \mathbb{F}_p[t]$ und $v(t) = \sum_{i=0}^{m} v_i t^i \in \mathbb{F}_p[t] \setminus \{0\}$. Dann gilt aufgrund von Lemma 3.3.15, dass

$$\left(\frac{u}{v}\right)^p = \frac{(\sum_{i=0}^{n} u_i t^i)^p}{(\sum_{i=0}^{m} v_i t^i)^p} = \frac{\sum_{i=0}^{n} u_i^p t^{pi}}{\sum_{i=0}^{m} v_i^p t^{pi}} \in \mathbb{F}_p(t^p). \qquad \triangle$$

Bemerkung 3.3.37. Es gilt $[L : K]_s = [\bar{K}_s^L : K]$, denn

$$\begin{aligned} [L : K]_s &= [L : \bar{K}_s^L]_s \cdot [\bar{K}_s^L : K]_s && \text{(Lemma 3.3.21)} \\ &= [\bar{K}_s^L : K]_s && \text{(Proposition 3.3.35 da } L|\bar{K}_s^L \text{ rein inseparabel)} \\ &= [\bar{K}_s^L : K] && \text{(Proposition 3.3.23 da } \bar{K}_s^L|K \text{ separabel).} \end{aligned}$$

Manche Autor:innen verwenden diese Gleichung sogar, um $[L : K]_s$ zu definieren.

Übung 89. Sei $L|K$ eine endliche rein inseparable Körpererweiterung und sei $p := \mathrm{char}(K) > 0$. Zeigen Sie: $[L : K]$ ist eine Potenz von p.

3.3.4 Der Satz vom primitiven Element

Sei $L = K(a)$; dann heißt a ein *primitives Element* von $L|K$.

Beispiel 3.3.38. Es seien $a, b \in \mathbb{Q}$. Der Teilkörper $\mathbb{Q}(\sqrt{a}, \sqrt{b})$ von $\mathbb{R}$ besitzt ein primitives Element, denn es gilt $\mathbb{Q}(\sqrt{a}, \sqrt{b}) = \mathbb{Q}(\sqrt{a} + \sqrt{b})$. Lediglich $\subseteq$ muss gezeigt werden. Es gilt $(\sqrt{a} + \sqrt{b})(\sqrt{a} - \sqrt{b}) = a - b$. Also ist

$$\sqrt{a} - \sqrt{b} = \frac{a - b}{\sqrt{a} + \sqrt{b}} \in \mathbb{Q}(\sqrt{a} + \sqrt{b})$$

und damit sind auch $2\sqrt{a}$, $2\sqrt{b}$, und folglich auch $\sqrt{a}$ und $\sqrt{b}$ Elemente von $\mathbb{Q}(\sqrt{a} + \sqrt{b})$.

Satz 3.3.39 (Satz vom primitiven Element)**.** *Sei $L = K(a_1, \ldots, a_n)$ eine endliche Erweiterung von K. Ist höchstens eines der a_i inseparabel über K, so ist $L|K$ einfach (besitzt also ein primitives Element).*

Beweis. Falls K endlich ist, so ist auch L endlich, da L ein endlichdimensionaler K-Vektorraum ist. Dann ist $L^\times$ zyklisch nach Korollar 1.7.5. Also gibt es ein $a \in L$ mit $L^\times = \langle a \rangle$, also $L = K(a)$. Im folgenden sei K also unendlich.

Es genügt, den Fall $L = K(a, b)$ mit b separabel über K zu betrachten; der allgemeine Fall folgt dann mit Induktion nach n. Seien $a_1, \ldots, a_n$ die K-Konjugierten von a und $b = b_1, \ldots, b_m$ die K-Konjugierten von b. Da K unendlich ist, können wir ein $c \in K$ wählen mit $c \neq \frac{a_i - a}{b - b_j}$ für $i \in \{1, \ldots, n\}$ und $j \in \{2, \ldots, m\}$. Dann gilt

$$d := a + cb \notin \{a_i + cb_j \mid i \in \{1, \ldots, n\}, j \in \{2, \ldots, m\}\}.$$

Behauptung: $L = K(d)$.
Seien f_a und f_b die Minimalpolynome von a und b über K und $h := f_a(d - cX) \in K(d)$. Es haben f_b und h die gemeinsame Nullstelle b, da $h(b) = f_a(d - cb) = f_a(a) = 0$. Es ist b auch die einzige gemeinsame Nullstelle. Um das zu sehen, sei $g \in \mathrm{ggT}(f_b, h) \subseteq K(d)$. Da $g|f_b$ so sind alle Nullstellen von g in $\bar{K}$ aus der Menge $\{b_1, \ldots, b_m\}$ (Lemma 3.2.48). Allerdings gilt für jedes $i \in \{1, \ldots, n\}$ und $j \in \{2, \ldots, m\}$, dass $a_i \notin d - cb_j$, also $h(b_j) = f_a(d - cb_j) \neq 0$. Da g auch h teilt, ist $g(b_j) \neq 0$, und $b = b_1$ ist tatsächlich die einzige Nullstelle von g. Weil b separabel ist, gilt $g = (X - b)$, und weil $g \in K(d)$ folgt dass $b \in K(d)$ und $a = d - cb \in K(d)$. Es folgt, dass $L = K(d)$. □

Korollar 3.3.40. *Jede endliche separable Körpererweiterung ist einfach.*

Korollar 3.3.41. *Jede endliche Erweiterung eines endlichen Körpers ist einfach.*

Beweis. Endliche Erweiterungen eines endlichen Körpers sind endliche Körper, also separabel nach Korollar 3.3.31. Die Aussage folgt dann aus Korollar 3.3.40. □

Wir werden nun ein Beispiel für eine endliche Körpererweiterung kennenlernen, die nicht einfach ist.

Beispiel 3.3.42. Sei $L = \mathbb{F}_p(s,t) = \mathbb{F}_p(s)(t)$ für formale Variablen s und t, und sei $K = \mathbb{F}_p(s^p, t^p)$. Dann ist $L|K$ endlich, denn der Grad $[L : K]$ berechnet sich mit Lemma 3.1.1 wie folgt:

$$[L : K] = [L : K(s)] \cdot [K(s) : K] = p^2.$$

Denn $[K(s) : K] = p$, da s das Minimalpolynom $X^p - s$ über K besitzt (siehe Beispiel 3.3.13). Analog zeigt man, dass $[L : K(s)] = p$. Aber $L|K$ ist nicht einfach: denn wenn es ein $a \in L$ gäbe mit $K(a) = L$, dann hätte das Minimalpolynom f_a von a den Grad p^2 (Lemma 3.2.9). Allerdings ist $a^p \in K$, also ist a auch eine Nullstelle von $X^p - a^p \in K[X]$, welches strikt kleineren Grad hat, ein Widerspruch zur Definition des Minimalpolynoms. △

Kapitel 4

Galoistheorie

4.1 Normale Erweiterungen

Sei $L|K$ eine algebraische Erweiterung.

Definition 4.1.1. $L|K$ heißt *normal*, falls jedes irreduzible $f \in K[X]$, das eine Nullstelle in L hat, über L in Linearfaktoren zerfällt.

Beispiel 4.1.2. $K|K$ ist normal. $\bar{K}|K$ ist normal. Jede Erweiterung $L|K$ vom Grad 2 ist normal. △

Beispiel 4.1.3. $\mathbb{Q}(\sqrt[3]{2})|\mathbb{Q}$ ist nicht normal: das Polynom $X^3 - 2$ ist irreduzibel in $\mathbb{Q}[X]$ (Beispiel 2.6.6), hat die Nullstelle $\sqrt[3]{2}$ in $\mathbb{Q}(\sqrt[3]{2})$, und zerfällt in $\mathbb{Q}(\sqrt[3]{2})$, das $X^3 - 2 = (X - 2^{1/3})(X^2 + 2^{1/3}X + 2^{2/3})$. Aber $(X^2 + 2^{1/3}X + 2^{2/3})$ ist kein Linearfaktor, und irreduzibel über $\mathbb{Q}(\sqrt[3]{2})$. △

Literaturverzeichnis

[1] M. Bodirsky. Automorphism groups, 2023. Course Notes, TU Dresden, `https://wwwpub.zih.tu-dresden.de/~bodirsky/Automorphism-Groups.pdf`.

[2] S. Bosch. *Lineare Algebra*. Springer-Lehrbuch. Springer, Berlin ; Heidelberg, 4., überarb. aufl. edition, 2008.

[3] S. Lang. *Algebra*. Springer, 2002. Revised third edition.

[4] A. K. Lenstra, H. W. Lenstra, Jr., and L. Lovász. Factoring polynomials with rational coefficients. *Math. Ann.*, 261:515–534, 1982.

[5] T. von Oertzen. *Das Konstruktionsproblem*. PhD thesis, Saarland University, Germany, 2004.