Algebra SS 2017 (Prof. Henke)

Mitschrift David Holzmüller, Korrekturen Sam Thelin

4. September 2017

Inhaltsverzeichnis

Kapitel 1

Gruppen

Definition 1.1 (Gruppe)**.** Eine *Gruppe* $(G, *)$ ist eine Menge G mit einer binären Verknüpfung $* : G \times G \to G, (g, h) \mapsto g * h$, sodass gilt:

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

(G2) Es existiert $e \in G$, sodass für alle $a \in G$ gilt: $a * e = a = e * a$.

(G3) Für alle $a \in G$ existiert $a' \in G$ mit $a * a' = e = a' * a$.

Falls zusätzlich gilt:

(G4) $a * b = b * a$ für alle $a, b \in G$,

so heißt G *kommutativ/abelsch*. Wir nennen e neutrales Element, a' inverses Element zu a. $|G|$ heißt *Ordnung* der Gruppe G. Notation: Schreibe G statt $(G, *)$. Die Verknüpfung $*$ ist oft $+$ oder $\cdot$. Man spricht entsprechend von einer *additiven* beziehungsweise einer *multiplikativen* Gruppe. Wird die Gruppe additiv geschrieben, dann schreiben wir meist 0 und $-a$ statt e und a'. In der multiplikativen Schreibweise schreiben wir 1 und a^{-1} statt e und a'. Schreibe auch ab statt $a \cdot b$. Schreibe $a - b := a + (-b)$. (Brüche werden nicht geschrieben.)

Bemerkung 1.2.

(a) Das neutrale Element ist eindeutig: Seien e, f neutrale Elemente in G, dann folgt $e = e*f = f$. Beim ersten Gleichheitszeichen benutzt man, dass f neutrales Element ist; beim zweiten Gleichheitszeichen benutzt man, dass e neutrales Element ist.

(b) Sei $a \in G$. Das inverse Element a' zu a ist eindeutig: Seien a', a'' Inverse zu a. Dann gilt:

$$a' = a'e = a'(aa'') = (a'a)a'' = ea'' = a'' \ .$$

(c) Es gilt $(a^{-1})^{-1} = a$ und $(ab)^{-1} = b^{-1}a^{-1}$.

Beispiel 1.3.

(1) $G = \{e\}$ mit $e * e = e$, die „triviale Gruppe“, ist eine abelsche Gruppe. Die leere Menge ist keine Gruppe.

(2) Ist $(R, +, \cdot)$ ein Ring, dann ist $(R, +)$ eine abelsche Gruppe, z. B. $\mathbb{Z}, \mathbb{Z}_n, \mathbb{Q}, \mathbb{R}, \mathbb{C}$. Ist $(K, +, \cdot)$ eine Körper, dann ist $(K, +)$ eine abelsche Gruppe und $(K^\times, \cdot)$ eine abelsche Gruppe, wobei $K^\times = K \setminus \{0\}$, z. B. $\mathbb{Q}, \mathbb{R}, \mathbb{C}, \mathbb{Z}_p$, p Primzahl.

Beispiel 1.4.

(1) Ist $(V, +, \cdot)$ ein Vektorraum, dann ist $(V, +)$ eine abelsche Gruppe. Insbesondere ist $M_n(K) = \{n \times n\text{-Matrizen über dem Körper } K\}$ ein Vektorraum, also eine Gruppe bezüglich Matrixaddition.

(2) Die „allgemeine lineare Gruppe“:

- $\mathrm{GL}(V) \coloneqq \{f : V \to V \mid f \text{ linear und bijektiv}\}$ mit Komposition von Abbildungen ist eine Gruppe (im Allgemeinen nicht abelsch). Neutrales Element ist $\mathrm{id} : V \to V, x \mapsto x$. Eine Abbildung ist bijektiv genau dann, wenn sie invertierbar ist. Das Inverse zu einem Element $f \in \mathrm{GL}(V)$ ist seine Umkehrfunktion f^{-1}.
- $\mathrm{GL}_n(K) \coloneqq \{n \times n\text{-Matrizen über } K, \text{ die invertierbar sind}\}$ mit Matrixmultiplikation ist eine Gruppe. Das neutrale Element ist I_n. Im Allgemeinen gilt $AB \neq BA$. Ist $|K| = \infty$, so enthält $\mathrm{GL}_n(K)$ unendlich viele Elemente. Ist $|K| = q$, dann gilt

$$|\mathrm{GL}_n(K)| = (q^n - 1)(q^n - q)(q^n - q^2) \cdots (q^n - q^{n-1}).$$

  Beweis: Eine $n \times n$-Matrix ist invertierbar, genau dann, wenn sie aus n linear unabhängigen Zeilenvektoren besteht. Es gibt q^n verschiedene Vektoren im K^n. Um eine invertierbare Matrix zu bilden, darf die i-te Zeile nicht im Span der $i - 1$ Zeilen davor liegen; letzterer Span hat q^{i-1} Elemente.

(3) Definiere die *spezielle lineare Gruppe* $\mathrm{SL}_n(K) \coloneqq \{A \in \mathrm{GL}_n(K) \mid \det(A) = 1\}$, die *orthogonale Gruppe* $\mathrm{O}_n(K) \coloneqq \{A \in \mathrm{GL}_n(K) \mid AA^\top = I_n\}$ und die *spezielle orthogonale Gruppe* $\mathrm{SO}_n(K) = \{A \in \mathrm{O}_n(K) \mid \det(A) = 1\} = \mathrm{SL}_n(K) \cap \mathrm{O}_n(K)$. Dies sind Gruppen. Zum Beispiel ist $\mathrm{SL}_n(K)$ abgeschlossen bezüglich Multiplikation und Inversenbildung, da die Determinante multiplikativ ist.

Beispiel 1.5.

(a) Sei $X \neq \emptyset$ eine Menge. Definiere $S_X \coloneqq \{f : X \to X \mid f \text{ bijektiv}\}$. Dann ist $(S_X, \circ)$ mit der Komposition von Abbildungen eine Gruppe. Hierbei ist

$$(f \circ g)(x) \coloneqq f(g(x))$$

für alle $x \in X$ und $f, g \in S_X$. S_X heißt *symmetrische Gruppe auf* X. Neutrales Element ist id_X. Die Inverse zu f ist die Umkehrfunktion f^{-1}. Es ist S_X abelsch, genau dann, wenn $|X| \in \{1, 2\}$.

(b) Sei $X = \{1, \ldots, n\}$, für $n \in \mathbb{N}$. Dann heißt $S_n \coloneqq S_{\{1,\ldots,n\}}$ *symmetrische Gruppe vom Grad* n. Es gilt $|S_n| = n!$. Elemente in S_n heißen *Permutationen*. Wir benutzen die folgenden beiden Notationen für Permutationen:

Matrixnotation: Sei $\sigma : \{1, \ldots, n\} \to \{1, \ldots, n\}$ mit $\sigma(1) = a_1, \ldots, \sigma(n) = a_n$. Schreibe kurz

$$\sigma = \begin{bmatrix} 1 & \ldots & n \\ a_1 & \ldots & a_n \end{bmatrix}.$$

Zykelnotation: Sei $\{a_1, \ldots, a_r\} \subseteq \{1, \ldots, n\}$ mit paarweise verschiedenen Zahlen a_i. Definiere den *r-Zykel* $\sigma = (a_1 \ldots a_r)$ als die Abbildung $\sigma : \{1, \ldots, n\} \to \{1, \ldots, n\}$ mit

$$\begin{aligned} a_1 &\mapsto a_2 \\ a_2 &\mapsto a_3 \\ &\vdots \\ a_r &\mapsto a_1 \end{aligned}$$

und $\sigma(a) = a$ für alle $a \in \{1, \ldots, n\} \backslash \{a_1, \ldots, a_r\}$. r heißt *Länge* des Zykels $(a_1 \ldots a_r)$. 2-Zykel heißen *Transpositionen*. Zum Beispiel sei

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

dann ist $\sigma = (13)(245)$. Zwei Zykel $(a_1 \ldots a_r)$ und $(b_1 \ldots b_s)$ heißen *disjunkt*, falls $\{a_1, \ldots, a_r\} \cap \{b_1, \ldots, b_s\} = \emptyset$. Man sieht leicht: Disjunkte Zykel kommutieren.

Jede Permutation lässt sich eindeutig als Produkt disjunkter Zykel schreiben: Sei $\sigma \in S_n$. Betrachte die Menge $\{a, \sigma(a), \sigma^2(a), \ldots\} \subseteq \{1, \ldots, n\}$. Es gibt in der ersten Menge Wiederholungen. Angenommen, $\sigma^i(a) = \sigma^j(a)$ mit $i < j$. Nach Multiplikation mit $\sigma^{-i} = (\sigma^{-1})^i$ folgt $a = \sigma^{j-i}(a)$. Sei $k \geq 1$ minimal mit $\sigma^k(a) = a$. Dann ist $\{a, \sigma(a), \sigma^2(a), \ldots\} = \{a, \sigma(a), \sigma^2(a), \ldots, \sigma^{k-1}(a)\}$. Wiederholt man obiges Argument, so sieht man: alle Zahlen in der zweiten Menge sind verschieden. Wir erhalten also den Zykel $(a, \sigma(a), \sigma^2(a), \ldots, \sigma^{k-1}(a))$. Wiederhole nun diesen Vorgang mit einem Element in $\{1, \ldots, n\} \backslash \{a, \sigma(a), \sigma^2(a), \ldots, \sigma^{k-1}(a)\}$.

Sei $\sigma = \sigma_1 \cdots \sigma_k$ Darstellung von σ als Produkt disjunkter Zykeln der Längen $l_1, \ldots, l_k$. Ohne Einschränkung sei $l_1 \geq \ldots \geq l_k$. Dann heißt $(l_1, \ldots, l_k)$ *Zykeltyp von* σ. Also hat $\sigma = (13)(245) = (245)(13)$ den Zykeltyp $(3, 2)$. Es ist $(l_1, \ldots, l_k)$ ist eine Partition von n.

Bemerkung 1.6.

(a) Sei G eine Gruppe, $a \in G$. Die Abbildungen $r_a : G \to G, x \mapsto x \cdot a$ und $l_a : G \to G, x \mapsto a \cdot x$ sind bijektive Abbildungen, denn $(r_a)^{-1} = r_{a^{-1}}$ und $(l_a)^{-1} = l_{a^{-1}}$.

(b) Eine *Gruppentafel/Multiplikationstafel* von G ist eine Matrix, deren Zeilen und Spalten durch die Elemente von G indiziert sind. Die Einträge in „Zeile a“ sind die Bilder unter der Abbildung l_a von G. Die Einträge in „Spalte a“ sind die Bilder unter der Abbildung r_a von G. Aus (a) folgt, dass in jeder Zeile/Spalte jedes Element aus G genau einmal vorkommt; eine solche Matrix nennt man auch „lateinisches Quadrat“.

(c) Beispiele: Für $|G| = 1, 2, 3$ gibt es jeweils genau eine Multiplikationstafel:

$\cdot$	1
1	1

$\cdot$	1	a
1	1	a
a	a	1

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

$=$

$\cdot$	1	a	a^2
1	1	a	a^2
a	a	a^2	1
a^2	a^2	1	a

Die Multiplikationstafel für drei Elemente wurde hierbei mit $a^2 = b$ umgeschrieben. Dies entspricht dem Rechnen modulo drei. Für $|G| = 4$ gibt es zwei verschiedene Gruppentafeln. Diese zu finden, ist eine gute Übungsaufgabe. Hier ein erster Hinweis dazu: Sei $G = \{1, a, b, c\}$. Die erste Zeile und erste Spalte der Multiplikationstafel ergibt sich durch Multiplikation mit dem neutralen Element 1. Um die Matrix weiter auszufüllen, müssen wir nun Fälle unterscheiden. Betrachten Sie als ersten Fall: $a \cdot b = 1$. Warum gilt dann auch $b \cdot a = 1$? Füllen Sie nun den Rest der Matrix mit Hilfe der lateinischen-Quadrat-Eigenschaft aus. Welche Fälle müssen als nächstes betrachtet werden? Obwohl es mehr als zwei Fälle sind, warum gibt es nur zwei verschiedene Multiplikationstafeln?

Bemerkung 1.7. Seien G, H Gruppen. Eine Abbildung $\varphi : G \to H$ heißt *(Gruppen)homomorphismus*, falls

$$\varphi(x \cdot_G y) = \varphi(x) \cdot_H \varphi(y)$$

für alle $x, y \in G$. Falls zusätzlich

- φ injektiv ist, heißt φ Monomorphismus.
- φ surjektiv ist, heißt φ Epimorphismus.
- φ bijektiv ist, heißt φ Isomorphismus.
- $G = H$ ist, heißt φ Endomorphismus.
- φ bijektiv und $G = H$ ist, heißt φ Automorphismus.

Gruppe G heißt *isomorph* zu Gruppe H, falls es einen Isomorphismus $\varphi : G \to H$ gibt; schreibe dafür auch $G \simeq H$.

Beispiel 1.8. Seien V, W K-Vektorräume.

(1) Ist $T : V \to W$ linear, dann ist T ein Gruppenhomomorphismus, denn $T(v + w) = Tv + Tw$.

(2) Sei $n \in \mathbb{N}$, dann ist $\det : (\mathrm{GL}_n(K), \cdot) \to (K^\times, \cdot)$ ein Gruppenhomomorphismus, denn $\det(AB) = \det(A)\det(B)$.

Bemerkung 1.9.

(a) Sei $\varphi : G \to H$ ein Gruppenhomomorphismus, dann gilt für alle $g \in G$:

$$\varphi(1_G) = 1_H \text{ und } \varphi(g^{-1}) = \varphi(g)^{-1}.$$

(b) Die Komposition zweier Gruppenhomomorphismen ist ein Gruppenhomomorphismus. Das Inverse eines bijektiven Gruppenhomomorphismus ist ein Gruppenhomomorphismus. Isomorphie ist also eine Äquivalenzrelation. Die Äquivalenzklassen unter dieser Äquivalenzrelation heissen *Isomorphieklassen*.

(c) Isomorphe Gruppen verhalten sich oft gleich: Gilt eine Aussage für eine Gruppe G, dann auch für alle dazu isomorphen Gruppen. Zum Beispiel: Isomorphe Gruppen haben „im Wesentlichen“ dieselbe Multiplikationstafel: Ist $\varphi : G \to H$ ein Isomorphismus, so gilt insbesondere $\varphi(xy) = \varphi(x)\varphi(y)$. Damit sehen die Multiplikationstafeln der isomorphen Gruppen G und H wie folgt aus:

$\cdot_G$	y
x	$x \cdot y$

und

$\cdot_H$	$\varphi(y)$
$\varphi(x)$	$\varphi(x \cdot y)$

.

Macht man in der Gruppentheorie Eindeutigkeitsaussagen, so bedeutet dies oft Eindeutigkeit bis auf Isomorphie.

Beweis zu (a): Es gilt

$$\varphi(1) = \varphi(1 \cdot 1) = \varphi(1) \cdot \varphi(1) \ ,$$

also nach Multiplikation mit $\varphi(1)^{-1}$ auch $1 = \varphi(1)\varphi(1)\varphi(1)^{-1} = \varphi(1)$.

Außerdem gilt

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

Da das Inverse eines Gruppenelementes eindeutig bestimmt ist, folgt, dass $\varphi(g^{-1})$ das Inverse zu $\varphi(g)$ sein muss. □

Kapitel 2

Untergruppen

Definition 2.1. Sei G eine Gruppe, $U \subseteq G$ eine Teilmenge. Dann heißt U *Untegruppe* von G ($U \leq G$), wenn gilt:

(U1) $U \neq \emptyset$,

(U2) $a, b \in U \Rightarrow ab \in U$,

(U3) $a \in U \Rightarrow a^{-1} \in U$.

Bemerkung 2.2. Sei G eine Gruppe.

(a) Sei $U \leq G$ Untergruppe. Dann ist U eine Gruppe im Sinne von Definition 1.1.

(b) Seien $A, B \subseteq G, c \in G$. Definiere

$$\begin{aligned} A \cdot B &\coloneqq \{a \cdot b \mid a \in A, b \in B\} \\ c \cdot B &\coloneqq \{c \cdot b \mid b \in B\} = \{c\} \cdot B \\ B \cdot c &\coloneqq B \cdot \{c\} \\ A^{-1} &\coloneqq \{a^{-1} \mid a \in A\} \ . \end{aligned}$$

Dann gilt:

(i) $U \leq G \Leftrightarrow U \neq \emptyset, U \cdot U \subseteq U, U^{-1} \subseteq U \Leftrightarrow 1_G \in U, U \cdot U \subseteq U, U^{-1} \subseteq U$.

(ii) $U \leq G$ impliziert $U^{-1} = U$ (und $U \cdot U = U$). Siehe Bemerkung 1.2(c).

Beispiel 2.3.

(a) Sei G eine Gruppe. Dann ist $\{1\} \leq G$ und $G \leq G$.

(b) Es gilt $(\mathbb{Z}, +) \leq (\mathbb{Q}, +) \leq (\mathbb{R}, +) \leq (\mathbb{C}, +)$. Außerdem ist $(\{-1, 1\}, \cdot) \leq (\mathbb{Q}^\times, \cdot) \leq (\mathbb{R}^\times, \cdot) \leq (\mathbb{C}^\times, \cdot)$ und $(\{1, -1, i, -i\}, \cdot) \leq (\mathbb{C}^\times, \cdot)$.

Beispiel 2.4. Die Untergruppen von $(\mathbb{Z}, +)$ sind genau die Teilmengen $d \cdot \mathbb{Z}$, für $d \in \mathbb{Z}$ (oder $d \in \mathbb{N}_0$).

Beweis. (a) Behauptung: Sei $d \in \mathbb{Z}$. Dann ist $(d\mathbb{Z}, +) \leq (\mathbb{Z}, +)$.

Beweis.

(U1) $0 = d \cdot 0 \in d\mathbb{Z} \Rightarrow d\mathbb{Z} \neq \emptyset$.

(U2) $dz_1 + dz_2 = d(z_1 + z_2) \in d\mathbb{Z}$.

(U3) Es gilt $-(dz) = d(-z) \in d\mathbb{Z}$. □

(b) (i) Sei $U \subseteq \mathbb{Z}, U \neq \{0\}$ und $U \leq \mathbb{Z}$. Dann existiert $u \in U$ mit $u \neq 0$ und $-u \in U$. Somit gilt $U \cap \mathbb{N} \neq \emptyset$. Sei also $d \coloneqq \min(U \cap \mathbb{N})$.

(ii) Behauptung: $d\mathbb{Z} = U$.

Beweis. „$\subseteq$“: Da U Gruppe ist, gilt $U + U \subseteq U$, $-U \subseteq U$. Nach Definition ist $d \in U$. Daraus folgt $d, d+d, d+d+d, \ldots \in U$ und $-d, -d-d, -d-d-d, \ldots \in U$, also $d\mathbb{Z} \subseteq U$.
„$\supseteq$“: Sei $u \in U$, dann existiert $z \in \mathbb{Z}$ mit $u = dz+r$, und mit $0 \leq r < d$ (Division mit Rest). Da U eine Gruppe ist, folgt $r = u - dz \in U$. Da $d = \min(U \cap \mathbb{N})$ gilt, ist $r = 0$, also $u = dz \in d\mathbb{Z}$. Dies zeigt $U \subseteq d\mathbb{Z}$. □

Damit ist $U = d\mathbb{Z}$ gezeigt. □

Bemerkung 2.5. Sei $\varphi : G \to H$ ein Gruppenhomomorphismus. Dann heißt $\mathrm{Ker}(\varphi) = \{g \in G \mid \varphi(g) = 1_H\}$ Kern von φ und $\mathrm{im}(\varphi) = \{\varphi(g) \mid g \in G\}$ Bild von φ.
Dann ist φ injektiv genau dann, wenn $\mathrm{Ker}(\varphi) = \{1_G\}$. Und φ ist surjektiv, genau dann, wenn $\mathrm{im}(\varphi) = H$.

Beweis. Wir wissen $\varphi(1) = 1$.

(i) Sei φ injektiv. Sei $a \in \mathrm{Ker}(\varphi)$. Dann folgt $\varphi(a) = 1 = \varphi(1)$, also $a = 1$.

(ii) Sei $\mathrm{Ker}(\varphi) = \{1\}$ und $\varphi(x) = \varphi(y)$. Dann ist $1 = \varphi(x)\varphi(y)^{-1} = \varphi(xy^{-1})$, also $xy^{-1} \in \mathrm{Ker}(\varphi) = \{1\}$, also $xy^{-1} = 1$ und damit $x = y$. □

Lemma 2.6. *Sei $\varphi : G \to H$ ein Homomorphismus. Dann ist*

$$\mathrm{Ker}(\varphi) \leq G \text{ und } \mathrm{im}(\varphi) \leq H.$$

Beweis. Da $1 = \varphi(1)$ ist, folgt $\mathrm{Ker}(\varphi) \neq \emptyset$. Seien $x, y \in \mathrm{Ker}(\varphi)$, d. h. $1 = \varphi(x) = \varphi(y)$, dann ist $\varphi(xy) = \varphi(x)\varphi(y) = 1 \cdot 1 = 1$ und damit $xy \in \mathrm{Ker}(\varphi)$. Außerdem ist $\varphi(x^{-1}) = \varphi(x)^{-1} = 1^{-1} = 1$, also $x^{-1} \in \mathrm{Ker}(\varphi)$.
Der Teil $\mathrm{im}(\varphi) \leq H$ bleibt dem Leser als Übungsaufgabe überlassen. □

Beispiel 2.7.

(i) Sei $\sigma \in S_n$. Definiere $\mathrm{sgn}(\sigma) \coloneqq (-1)^{\omega(\sigma)}$, wobei

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

die Anzahl der Fehlstellen/Fehlstellungen von σ ist. Dann ist

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

Beispiel:

$$\sigma = \begin{bmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{bmatrix} = (13)(2) = (13) \ .$$

Wir haben $1 < 2$ und $3 > 2$, $1 < 3$ und $3 > 1$, $2 < 3$ und $2 > 1$. Also $\operatorname{sgn}((13)) = (-1)^3 = -1$. Die zweite Formel liefert

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

(ii) Dann ist $\operatorname{sgn} : (S_n, \cdot) \to (\{+1, -1\}, \cdot), \sigma \mapsto \operatorname{sgn}(\sigma)$ ein Gruppenhomomorphismus, denn:

$$\begin{aligned}\operatorname{sgn}(\sigma \cdot \pi) &= \prod_{i<j} \frac{\sigma(\pi(i)) - \sigma(\pi(j))}{i-j} = \prod_{i<j} \left(\frac{\sigma(\pi(i)) - \sigma(\pi(j))}{\pi(i) - \pi(j)} \cdot \frac{\pi(i) - \pi(j)}{i-j} \right) \\ &= \prod_{i<j} \frac{\sigma(\pi(i)) - \sigma(\pi(j))}{\pi(i) - \pi(j)} \cdot \prod_{i<j} \frac{\pi(i) - \pi(j)}{i-j} \\ &= \operatorname{sgn}(\sigma) \cdot \operatorname{sgn}(\pi) \ .\end{aligned}$$

(iii) Definiere die *alternierende Gruppe* $A_n \coloneqq \operatorname{Ker}(\operatorname{sgn})$. Nach Lemma 2.6 gilt $A_n \leq S_n$.

Lemma 2.8. *Sei G eine Gruppe und $U, V \leq G$.*

(a) $U \cap V \leq G$. Allgemeiner: Ist $U_i \leq G, i \in I$ für eine beliebige Indexmenge I, dann folgt $\cap_{i \in I} U_i \leq G$.

(b) $U \cup V \leq G \Leftrightarrow U \subseteq V$ oder $V \subseteq U$.

(c) $U \cdot V \leq G \Leftrightarrow U \cdot V = V \cdot U$.

Beweis.

(a) Da U, V Untergruppen sind, folgt $1_G \in U$ und $1_G \in V$, also auch $1_G \in U \cap V$. Seien $x, y \in U \cap V$. Dann folgt $x, y \in U$ und $x, y \in V$. Da U eine Gruppe ist, folgt $xy \in U, x^{-1} \in U, xy \in V, x^{-1} \in V$, also auch $xy \in U \cap V$ und $x^{-1} \in U \cap V$.

(b) Übung.

(c) (i) Da $U \leq G$ gilt, folgt $U^{-1} = U$ nach 2.2. Sei $UV \leq G$, dann folgt

$$UV = (UV)^{-1} = V^{-1}U^{-1} = VU.$$

(ii) Sei $UV = VU$. Da $1 \in U, 1 \in V$ gilt, folgt $1 = 1 \cdot 1 \in UV \neq \emptyset$. Außerdem gilt

$$\begin{aligned}(UV) \cdot (UV) &= U(VU)V = UUVV \subseteq UV \ , \\ (UV)^{-1} &= V^{-1}U^{-1} = VU = UV\end{aligned}$$

nach Voraussetzung. □

Definition 2.9. Sei $H \leq G, a \in G$. Wir nennen $aH = \{ah \mid h \in H\}$ Linksnebenklasse von H in G und $Ha = \{ha \mid h \in G\}$ Rechtsnebenklasse von H in G und schreiben

$$\begin{aligned}G/H &= \{aH \mid a \in G\} \\ H\backslash G &= \{Ha \mid a \in G\} \ ,\end{aligned}$$

gesprochen „G modulo H“. Definiere $[G : H] = \left| G/H \right|$, den *Index der Untergruppe H in G*.

Bemerkung 2.10.

(a) Es gilt $|aH| = |H| = |Ha|$ nach 1.6 (a).

(b) Es ist $aH = bH$ für alle $b \in aH$.

Beweis. „$\supseteq$“: $b \in aH \Rightarrow bH \subseteq aH$, da H abgeschlossen bezüglich Multiplikation ist.

„$\subseteq$“: Sei $b \in aH$, also existiert $h \in H$ mit $b = ah$. Für alle $\tilde{h} \in H$ gilt dann $a\tilde{h} = (ah)(h^{-1}\tilde{h}) = b(h^{-1}\tilde{h}) \in bH$. Dies zeigt $aH \subseteq bH$. □

Lemma 2.11.

(a) Die Relation $\sim_H$ auf G definiert durch $a \sim_H b :\Leftrightarrow a^{-1}b \in H$ ist eine Äquivalenzrelation, deren Äquivalenzklassen genau die Linksnebenklassen von H in G sind.

(b) Die Relation $\sim_H$ auf G definiert durch $a \sim_H b :\Leftrightarrow ab^{-1} \in H$ ist eine Äquivalenzrelation, deren Äquivalenzklassen genau die Rechtsnebenklassen von H in G sind.

Insbesondere ist

$$G = \bigcup_{a \in G} aH = \bigcupdot_{N \in G/H} N \ ,$$
$$G = \bigcup_{a \in G} Ha = \bigcupdot_{N \in H\backslash G} N \ .$$

Beweis. Es gilt $a^{-1}a = 1 \in H$, also $a \sim_H a$.
Sei $a \sim_H b$, dann ist $a^{-1}b \in H$ und somit auch $b^{-1}a = (a^{-1}b)^{-1} \in H$, d. h. $b \sim_H a$.
Seien jetzt $a \sim_H b$ und $b \sim_H c$. Dann folgt $a^{-1}b, b^{-1}c \in H$, also $a^{-1}c = (a^{-1}b)(b^{-1}c) \in H$, d. h. $a \sim_H c$.
Sei $[a]$ die Äquivalenzklasse von a, also $[a] = \{b \mid b \sim_H a\}$. Dann gilt $b \in [a] \Leftrightarrow a \sim_H b \Leftrightarrow \exists h \in H : a^{-1}b = h \Leftrightarrow \exists h \in H : b = ah \Leftrightarrow b \in aH$. Also $[a] = aH$. □

Theorem 2.12 (Lagrange)**.** *Sei $|G| < \infty, H \leq G$. Dann gilt*

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

insbesondere also $|H| \mid |G|$.

Beweis. Wähle ein Vertretersystem $T = \{a_1, \ldots, a_r\}$ der Linksnebenklassen, dann ist $r = [G : H]$. Da $G = \biguplus_{i=1}^{r} a_i H$ nach 2.11, folgt

$$|G| = \sum_{i=1}^{r} |a_i H| = \sum_{i=1}^{r} |H| = r \cdot |H| = [G : H] \cdot |H| \ .$$ □

Sei G eine endliche Gruppe. Angenommen m ist ein Teiler der Gruppenordnung $|G|$. Dann existiert nicht notwendigerweise eine Untergruppe H von G mit Ordnung $|H| = m$. Zum Beispiel hat die alternierende Gruppe A_4 zwölf Elemente; ihre Untergruppen lassen sich leicht bestimmen, insbesondere hat A_4 keine Untergruppe mit sechs Elementen.

Kapitel 3

Erzeugendensysteme von Gruppen

Sei G eine Gruppe.

Definition 3.1. Sei $S \subseteq G$ eine Teilmenge.

- Definiere das „Erzeugnis von S“ durch

$$\langle S \rangle \coloneqq \bigcap_{\substack{U \leq G \\ S \subseteq U}} U \overset{2.8}{\leq} G \ .$$

- S heißt *Erzeugendensystem von* G, falls $G = \langle S \rangle$.
- G heißt *endlich erzeugt*, falls ein endliches $S \subseteq G$ existiert mit $G = \langle S \rangle$.
- G heißt *zyklisch*, falls ein $g \in G$ existiert mit $\langle g \rangle = G$.

Beispiel 3.2. Es gilt

(a) $\langle \emptyset \rangle = \{1_G\}$.

(b) $(\mathbb{Z}, +) = \langle 1 \rangle = \langle -1 \rangle$ ist eine unendliche zyklische Gruppe. Insbesondere sind Erzeuger einer Gruppe nicht notwendigerweise eindeutig.

(c) $(\mathbb{Z}_n, +) = \langle \overline{1} \rangle$ ist eine zyklische Gruppe der Ordnung n.

(d) Ist $|G| = p$ eine Primzahl, dann ist G zyklisch: Nach Lagrange 2.12 gilt $U \leq G$ impliziert $|U| \in \{1, p\}$, d. h. $U = \{1_G\}$ oder $U = G$. Wähle $1 \neq x \in G$, dann folgt $\langle x \rangle = G$.

Bemerkung 3.3.

(a) $\langle S \rangle$ ist die kleinste Untergruppe von G mit $S \subseteq \langle S \rangle$.

Beweis. Sei H die kleinste Untergruppe von G mit $S \subseteq H$. Nach 3.1 folgt

$$\langle S \rangle = \bigcap_{\substack{U \leq G \\ S \subseteq U}} U = H \cap \bigcap_{\substack{U \leq G \\ S \subseteq U}} U \subseteq H \ .$$

Nach Definition ist H die kleinste Untergruppe von G, die S enthält, also folgt $H = \langle S \rangle$. □

(b) Sei $S \neq \emptyset$, dann ist

$$\langle S \rangle = \{ s_1 \cdots s_t \mid t \in \mathbb{N}_0, s_i \in S \cup S^{-1} \} \ .$$

Für $t = 0$ erhalten wir das leere Produkt, welches als 1 definiert ist. Insbesondere ist

$$\langle g \rangle = \{ g^i \mid i \in \mathbb{Z} \} \ ,$$

wobei

$$g^i \coloneqq \begin{cases} 1 & , i = 0 \\ \underbrace{g \cdots g}_{i \text{ mal}} & , i > 0 \\ \underbrace{g^{-1} \cdots g^{-1}}_{(-i) \text{ mal}} & , i < 0 \ . \end{cases}$$

(c) Sind die Elemente eines Erzeugendensystems von S paarweise vertauschbar, dann ist G abelsch.

(d) Sei $G = \langle S \rangle$. Dann ist ein Homomorphismus $\varphi : G \to H$ durch die Bilder von S eindeutig bestimmt.

Definition 3.4. Sei $g \in G$. Definiere $\operatorname{ord}(g)$, die *Ordnung von* g, als kleinstes $n \in \mathbb{N}_{>0}$ mit $g^n = 1$. Existiert keine solche Zahl, dann definiere $\operatorname{ord}(g) \coloneqq \infty$.
Beispiel in S_n : $\operatorname{ord}(12) = 2, \operatorname{ord}(123) = 3, \operatorname{ord}((12)(123)) = \operatorname{ord}(23) = 2, \operatorname{ord}((12)(345)) = 6$.
Beispiel in $(\mathbb{Z}_6, +)$: $\operatorname{ord}(0) = 1, \operatorname{ord}(1) = 6, \operatorname{ord}(2) = 3, \operatorname{ord}(3) = 2, \operatorname{ord}(4) = 3, \operatorname{ord}(5) = 6$.
In $(\mathbb{Z}_n, +)$: $\operatorname{ord}(1) = n, \operatorname{ord}(a) = \frac{n}{\operatorname{ggT}(a,n)}$.

Lemma 3.5. *Sei $g \in G$.*

(a) Sei $\operatorname{ord}(g) = n$. Dann folgt $\langle g \rangle = \{1, g, g^2, \ldots, g^{n-1}\}$ und $1, g, g^2, \ldots, g^{n-1}$ sind paarweise verschieden. Es ist $g^k = 1 \Leftrightarrow n \mid k$. Insbesondere: Ist G endlich, dann ist $\operatorname{ord}(g) \mid |G|$ nach 2.12 und damit $g^{|G|} = 1$.

(b) Sei $\operatorname{ord}(g) = \infty$, dann sind $g^i, i \in \mathbb{Z}$ alle verschieden.

(c) Sei $\operatorname{ord}(g) = n$ und $k \in \mathbb{Z}$. Dann gilt

$$\operatorname{ord}(g^k) = \frac{n}{\operatorname{ggT}(n,k)} \ .$$

Beweis.

(1) Sei $\operatorname{ord}(g) = n$. Schreibe $k \in \mathbb{Z}$ als $k = qn + r$ mit $0 \leq r < n$. Dann ist

$$g^k = (g^n)^q \cdot g^r = 1^q \cdot g^r = g^r \ .$$

Damit folgt $\langle g \rangle \subseteq \{1, g, g^2, \ldots, g^{n-1}\}$. Außerdem gilt $g^k = 1 \Leftrightarrow g^r = 1 \Leftrightarrow r = 0 \Leftrightarrow n \mid k$.

(2) Sei $g^i = g^j$, dann gilt $1 = g^{j-i}$.

- Ist $i < j$, dann folgt $\mathrm{ord}(g) < \infty$. Das zeigt (b).
- Sei $0 \leq i \leq j \leq n-1$ und $\mathrm{ord}(g) = n$, dann folgt $j-i = 0$, d. h. $i = j$ und damit ist $\langle g \rangle = \{1, g, g^2, \ldots, g^{n-1}\}$ und $1, g, g^2, \ldots, g^{n-1}$ sind paarweise verschieden.

Da $|\langle g \rangle| = n \mid |G|$ nach Lagrange, folgt mit (1), dass $g^{|G|} = 1$. Damit gilt (a).

(3) Übungsblatt. □

Bemerkung 3.6. Alle zyklischen Gruppen gleicher Ordnung n sind isomorph, insbesondere isomorph zu $(\mathbb{Z}_n, +)$. Alle unendlich zyklischen Gruppen sind isomorph, insbesondere isomorph zu $(\mathbb{Z}, +)$. Schreibe C_n für eine zyklische Gruppe der Ordnung n.

Theorem 3.7.

(a) Jede Untergruppe einer zyklischen Gruppe ist zyklisch.

(b) Sei $G = \langle g \rangle$ zyklisch von Ordnung n. Dann gilt: Zu jedem $d \mid n$ gibt es genau eine Untergruppe von G der Ordnung d, nämlich $\langle g^{n/d} \rangle =: C_d$.

(c) Seien $d \mid n$ und $e \mid n$ und $C_d, C_e \leq G$. Dann gilt $C_d \cap C_e = C_{\mathrm{ggT}(d,e)}$ und $C_d \cdot C_e = C_{\mathrm{kgV}(d,e)}$.

Beweis.

(a) Sei $H \leq G = \langle g \rangle$. Sei $S := \{k \in \mathbb{Z} \mid g^k \in H\}$, dann folgt $(S, +) \leq (\mathbb{Z}, +)$ nach 2.2. Nach 2.4 existiert $d \in \mathbb{N}_0$ mit $S = d\mathbb{Z} = \langle d \rangle$. Damit folgt $H = \langle g^d \rangle$.

(b) Übung.

(c) Übung. □

Beispiel: $C_{10} = \langle g \rangle = \{1, g, g^2, \ldots, g^9\}$. Dann ist $C_5 = \{1, g^2, g^4, g^6, g^8\} = \langle g^2 \rangle = \langle g^4 \rangle = \langle g^6 \rangle = \langle g^8 \rangle$ und $C_2 = \{1, g^5\} = \langle g^5 \rangle$, also $C_2 \cap C_5 = \{1\}$. Außerdem gilt $C_2 \cdot C_5 = C_{10}$.

Beispiel 3.8 (Diedergruppe D_{2n})**.** Die Symmetriegruppe des regelmäßigen n-Ecks $P \subseteq \mathbb{R}^2$ (bzw. eine hierzu isomorphe Gruppe) heißt *Diedergruppe* D_{2n}.

(a) Sei r die Rotation um $\frac{2\pi}{n}$ um das Zentrum von P, s eine fest gewählte Spiegelung von P. Dann ist $r^n = 1, s^2 = 1$. Nummeriere die Ecken von P mit $1, 2, \ldots, n$ gegen den Uhrzeigersinn. Sei $t \in D_{2n}$ eine beliebige Symmetrie von P. Betrachte tP. Da t abstandserhaltend ist, erhalten wir:

(i) Fall 1: Die Zahlen an den Ecken von tP sind gegen den Uhrzeigersinn, wobei die Ecke 1 in P auf die Stelle k in tP abgebildet wird, $k \in \{1, \ldots, n\}$. Dann folgt $tP = r^{k-1}(P)$, d. h. $t = r^{k-1}$ ist eine Rotation.

(ii) Fall 2: Die Zahlen an den Ecken von tP sind im Uhrzeigersinn. Dann sind die Zahlen in stP gegen den Uhrzeigersinn. Nach (i) gibt es ein $k \in \{1, \ldots, n\}$ mit $st = r^{k-1}$, also $t = sr^{k-1}$ eine Spiegelung. Diese Spiegelungen für verschiedene k sind alle verschieden.

Also ist $D_{2n} = \{1, r, r^2, \ldots, r^{n-1}, s, sr, sr^2, \ldots, sr^{n-1}\} = \langle r, s \rangle$.

(b) Es gilt $r^n = 1, s^2 = 1$ und $r^k \cdot s = s \cdot r^{-k}$. Dies beschreibt alle Relationen zwischen Erzeugern r und s, d. h.

$$D_{2n} = \langle r, s \mid r^n = 1 = s^2, r^k s = sr^{-k}, 1 \leq k \leq n \rangle \ .$$

Beispiel 3.9.

(a) S_n wird von Transpositionen erzeugt, denn $(a_1 \dots a_l) = (a_1 a_l) \cdots (a_1 a_3)(a_1 a_2)$.

(b) $A_n = \{\sigma \in S_n \mid \operatorname{sgn}(\sigma) = 1\}$ wird von der Menge der 3-Zykel erzeugt: Sei $\pi \in A_n \subseteq S_n$. Nach (a) können wir $\pi = \prod_{i=1}^{t} \pi_i$ als Produkt von Transpositionen π_i schreiben. Wegen

$$1 = \operatorname{sgn}(\pi) = \prod_{i=1}^{t} \operatorname{sgn}(\pi_i) = \prod_{i=1}^{t} (-1) = (-1)^t$$

ist t gerade. Schreibe

$$(ab)(cd) = \begin{cases} (acb)(acd) & \text{, falls disjunkt} \\ (acb) & \text{, falls o.B.d.A. } a = d, b \neq c. \end{cases}$$

Kapitel 4

Normalteiler und Quotientengruppe

Sei G eine Gruppe.

Definition 4.1. Sei $H \leq G, x \in G$. Dann heißt $xHx^{-1} = \{xhx^{-1} \mid h \in H\}$ zu H *konjugierte Untergruppe.*

Bemerkung 4.2.

(a) Ist $H \leq G$, dann ist auch $xHx^{-1} \leq G$ für alle $x \in G$, denn:

$$(xhx^{-1})(xh'x^{-1}) = x\underbrace{hh'}_{\in H}x^{-1} \in xHx^{-1}$$

$$(xhx^{-1})^{-1} \overset{1.2}{=} (x^{-1})^{-1}h^{-1}x^{-1} = xh^{-1}x^{-1} \in xHx^{-1} \ .$$

(b) Nach 1.6 gilt $|H| = |xHx^{-1}|$ für alle $x \in G$.

Definition 4.3. Eine Untergruppe $N \leq G$ heißt *normal* (*Normalteiler*), falls $xNx^{-1} = N$ für alle $x \in G$. Wir schreiben $N \trianglelefteq G$.

Bemerkung 4.4. Die folgenden Aussagen sind äquivalent:

(i) $N \trianglelefteq G$,

(ii) $gNg^{-1} = N$ für alle $g \in G$,

(iii) $gN = Ng$ für alle $g \in G$,

(iv) $gNg^{-1} \subseteq N$ für alle $g \in G$.

Beweis. (iv) $\Rightarrow$ (iii): Da $gNg^{-1} \subseteq N$ gilt, folgt $gN \subseteq Ng$. Außerdem gilt $ng = g(g^{-1}ng) \in gN$, da $g^{-1}Ng \subseteq N$ nach (iv) gilt. Damit folgt $Ng \subseteq gN$. □

Beispiel 4.5.

(a) $\{1\} \leq G$ und $G \leq G$ sind Normalteiler. Eine Gruppe $G \neq \{1\}$ heißt *einfach*, wenn sie nur die Normalteiler $\{1\}$ und G hat. Zum Beispiel ist C_p einfach, falls p prim ist.

(b) Ist G abelsch und $H \leq G$, dann ist auch $H \trianglelefteq G$.

(c) Sei $H \leq G$ mit $[G : H] = 2$. Dann ist $H \trianglelefteq G$.

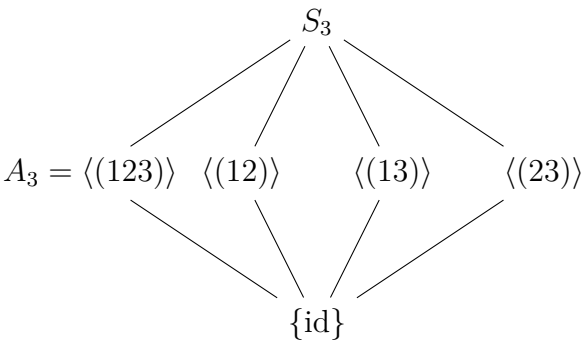
Beweis. Es gilt ${}^{G}\!/_{H} = \{H, G \setminus H\}$. Damit stimmen Links- und Rechtsnebenklassen von H überein. Damit folgt $H \trianglelefteq G$. □

Zum Beispiel: $A_n = \{\sigma \in S_n \mid \operatorname{sgn}(\sigma) = 1\} \leq S_n$. Sei $\tau \in S_n$ mit $\operatorname{sgn}(\tau) = -1$. Sei $\pi \in S_n$ mit $\operatorname{sgn}(\pi) = -1$. Dann gilt $\pi = \tau(\tau^{-1}\pi) \in \tau A_n$, denn $\operatorname{sgn}(1) = \operatorname{sgn}(\tau\tau^{-1}) = \operatorname{sgn}(\tau)\operatorname{sgn}(\tau^{-1}) = -\operatorname{sgn}(\tau^{-1})$, also $\operatorname{sgn}(\tau^{-1}) = -1$ und damit

$$\operatorname{sgn}(\tau^{-1}\pi) = \operatorname{sgn}(\tau^{-1})\operatorname{sgn}(\pi) = 1 \ .$$

Somit ist $\tau A_n = \{\pi \in S_n \mid \operatorname{sgn}(\pi) = -1\}$ und damit $[S_n : A_n] = 2$, d. h. $A_n \trianglelefteq S_n$. Insbesondere ist $|A_n| = \frac{1}{2}n!$ für $n \geq 2$.

(d) *Untergruppenverband* von S_3:



Es gilt $A_3 \trianglelefteq S_3$. Andererseits gilt $(13)(12)(13) = (23)$, also $(13)\langle(12)\rangle(13)^{-1} \not\subseteq \langle(12)\rangle$, also ist $\langle(12)\rangle$ und analog auch die verbleibenden beiden nichttrivialen Untergruppen keine Normalteiler. Diese drei von Transpositionen erzeugten Untergruppen sind zueinander konjugierte Untergruppen.

(e) Normal ist nicht transitiv: Es gilt

$$G = D_8 = \langle r, s \mid r^4 = 1 = s^2, rs = sr^3\rangle \trianglerighteq N_1 \coloneqq \langle r^2, s\rangle = \{r^2, sr^2, s, 1\}$$
$$N_1 \trianglerighteq N_2 \coloneqq \langle s\rangle = \{1, 2\} \ ,$$

aber $N_2 \not\trianglelefteq G$, denn:

$$r \cdot N_2 = \{r, rs\} = \{r, sr^3\}$$
$$N_2 \cdot r = \{r, sr\}$$

und damit $rN_2 \neq N_2 r$.

Bemerkung: N_1 heißt *Kleinsche Vierergruppe*. Es gilt $N_1 \simeq C_2 \times C_2$.

Proposition 4.6.

(a) Das Zentrum von G, $Z(G) \coloneqq \{g \in G \mid \forall x \in G : gx = xg\}$, ist ein Normalteiler von G.

(b) Die Kommutatoruntergruppe von G, $G' \coloneqq \langle\{[x, y] \mid x, y \in G\}\rangle$, wobei $[x, y] = xyx^{-1}y^{-1}$ der Kommutator von x und y ist, ist ein Normalteiler von G.

(c) Seien $H_i \trianglelefteq G$ für $i \in I$ (Indexmenge), dann ist auch $H \coloneqq \bigcap_{i\in I} H_i \trianglelefteq G$.

(d) Sei $\varphi : G \to H$ ein Homomorphismus. Dann gilt $U \leq H$ impliziert $\varphi^{-1}(U) \leq G$ und $U \trianglelefteq H$ impliziert $\varphi^{-1}(U) \trianglelefteq G$. Insbesondere ist

$$\mathrm{Ker}(\varphi) = \{g \in G \mid \varphi(g) = 1_H\} = \varphi^{-1}(\{1_H\}) \trianglelefteq G.$$

Beweis.

(a) Es gilt $1 \in Z(G)$.

Seien $g, h \in Z(G)$, dann folgt $(gh)x = g(hx) = g(xh) = (gx)h = (xg)h = x(gh)$ für alle $x \in G$ und damit $gh \in Z(G)$. Also gilt (U2).

Für (U3): Sei $g \in Z(G)$, dann ist $gx = xg$ für alle $x \in G$. Dann ist $x^{-1}g^{-1} = g^{-1}x^{-1}$. Also $yg^{-1} = g^{-1}y$ für alle $y \in G$, da $G^{-1} = G$. Also $g^{-1} \in Z(G)$. Nach 2.2 gilt $Z(G) \leq G$.

Da $xZ(G)x^{-1} = Z(G)$ für alle $x \in G$ gilt, folgt $Z(G) \trianglelefteq G$.

(b) Nach 3.1 ist $G' \leq G$. Seien $x, y, z \in G$. Dann ist

$$\begin{aligned} z[x,y]z^{-1} &= zxyx^{-1}y^{-1}z^{-1} = (zxz^{-1})(zyz^{-1})(zx^{-1}z^{-1})(zy^{-1}z^{-1}) \\ &= [zxz^{-1}, zyz^{-1}] \in G' \ . \end{aligned}$$

Mit einem analogen Argument (Einfügen von $z^{-1}z$ in ein Produkt von Kommutatoren und Benutzen von $[x,y]^{-1} = [y,x]$) folgt $zG'z^{-1} \subseteq G'$ für alle $z \in G$. Also gilt $G' \trianglelefteq G$.

(c) Nach 2.8 gilt $H = \bigcap_{i \in I} H_i \leq G$. Da $H \subseteq H_i$ für alle $i \in I$ und $H_i \trianglelefteq G$, folgt $xHx^{-1} \subseteq xH_ix^{-1} = H_i$ für alle $i \in I$ und jedes $x \in G$. Also gilt auch $xHx^{-1} \subseteq \bigcap_{i \in I} H_i = H$ für jedes $x \in G$. Mit 4.4 folgt $H \trianglelefteq G$.

(d) Übung. □

Beispiel 4.7. Wir berechnen das Zentrum einiger Gruppen:

(i) $Z(\mathrm{GL}_n(K)) = \{\lambda I_n \mid \lambda \in K^\times\} \simeq K^\times, \quad Z(\mathrm{GL}_n(K)) \overset{4.6}{\trianglelefteq} \mathrm{GL}_n(K)$.

(ii) $Z(\mathrm{SL}_n(K)) = \{\lambda I_n \mid \lambda \in K^\times, \lambda^n = 1\} \trianglelefteq \mathrm{SL}_n(K)$. Das bedeutet, dass $Z(\mathrm{SL}_n(K))$ isomorph zu $\{\lambda \in K^\times \mid \lambda^n = 1\}$, der Gruppe der n-ten Einheitswurzeln in K ist. Im Fall $K = \mathbb{C}$ ist dies die zyklische Gruppe $\{\exp\left(\frac{2\pi ik}{n}\right) \mid k \in \{0, \ldots, n-1\}\}$.

(iii) Es ist $Z(S_n) = \{\mathrm{id}\}$ für $n \geq 3$.

Beweis. Sei $\pi \in S_n$ und $\pi \neq \mathrm{id}$. Dann existiert $i \neq j$ mit $\pi(i) = j$. Sei $\sigma = (jk)$ mit $k \notin \{i, j\}$. Dann gilt $\sigma^{-1} = (jk)$. Außerdem gilt

$$\sigma^{-1}\pi\sigma(i) = \sigma^{-1}\pi(i) = \sigma^{-1}(j) = k$$

und damit $\sigma^{-1}\pi\sigma \neq \pi$, also $\pi \notin Z(S_n)$. Da $\pi \neq \mathrm{id}$ beliebig gewählt war, folgt $Z(S_n) = \{\mathrm{id}\}$. □

(iv) Es ist

$$Z(D_{2n}) = \begin{cases} \{\mathrm{id}\} & , n \text{ ungerade} \\ \{\mathrm{id}, r^{n/2}\} & , n \text{ gerade.} \end{cases}$$

Beweis. (Idee) Wir wissen $sr^i = r^{n-i}s$. Es gilt

$$sr^i = r^i s = sr^{-i} \Leftrightarrow r^i = r^{-i} \Leftrightarrow r^{2i} = 1 \Leftrightarrow 2i = n \Leftrightarrow i = \frac{n}{2} .$$

Damit ist gezeigt, dass r^i und s genau dann kommutieren, wenn $i = n/2$. Der Rest des Argumentes ist dem Leser überlassen. □

Theorem 4.8. *Sei G eine Gruppe und $N \trianglelefteq G$.*

(a) Die Menge ${}^{G}\!/_{N} = \{gN \mid g \in G\}$ mit Multiplikation

$$(aN) \cdot (bN) \coloneqq ab \cdot N$$

für alle $a, b \in G$ ist eine Gruppe, genannt Faktorgruppe *oder* Quotientengruppe von G modulo N. *Das neutrale Element ist $1 \cdot N = N$. Das Inverse zu aN ist $a^{-1}N$.*

(b) Die Abbildung $\pi : G \to {}^{G}\!/_{N}, a \mapsto aN$ ist ein Epimorphismus mit $\mathrm{Ker}(\pi) = N$. Sie heißt „kanonische Projektion".

Beweis. (i) Die Multiplikation ist wohldefiniert: Sei $aN = a'N, bN = b'N$. Das ist äquivalent dazu, dass $a^{-1}a' \in N, b^{-1}b' \in N$. Es ist zu zeigen, dass $abN = a'b'N$. Da $N \trianglelefteq G$ ist, folgt:

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

Damit folgt $abN = a'b'N$, also nach Definition $aN \cdot bN = abN = a'b'N = a'N \cdot b'N$.

(ii) Gruppenaxiome: Da G assoziativ ist, ist ${}^{G}\!/_{N}$ assoziativ, denn

$$\begin{aligned}(aN \cdot bN) \cdot cN &\overset{\text{Def}}{=} abN \cdot cN \overset{\text{Def}}{=} (ab)cN \\ &= a(bc)N = aN \cdot bcN = aN \cdot (bN \cdot cN)\end{aligned}$$

für alle $a, b, c \in G$.

(iii) Nach der Definition von π und der Multiplikation in der Quotientengruppe gilt

$$\pi(gh) = ghN = gN \cdot hN = \pi(g) \cdot \pi(h) .$$

Also ist π ein Homomorphismus mit $\mathrm{Ker}(\pi) = \{g \in G \mid gN = N\} = N$. □

Beispiel 4.9.

(a) Es ist $N \coloneqq n\mathbb{Z} = \langle n \rangle \overset{4.5}{\trianglelefteq} \mathbb{Z}$ mit

$${}^{\mathbb{Z}}\!/_{n\mathbb{Z}} = \{0 + n\mathbb{Z}, 1 + n\mathbb{Z}, \ldots, (n-1) + n\mathbb{Z}\} =: \mathbb{Z}_n$$

mit $(a + n\mathbb{Z}) + (b + n\mathbb{Z}) = (a + b) + n\mathbb{Z}$. Für $a + n\mathbb{Z}$ schreiben wir auch oft $\overline{a}$.

Im Fall $n = 3$ erhalten wir $\mathbb{Z}_3 = \{\overline{0}, \overline{1}, \overline{2}\}$ mit Additionstabelle

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

(b) Sei $G = \mathbb{Z}_6$ und $N = \{\overline{0}, \overline{3}\}$, dann gilt $N \trianglelefteq G$ nach 4.5. Es gilt

$$G/N = \mathbb{Z}_6/\{\overline{0}, \overline{3}\} = \{\overline{0} + N, \overline{1} + N, \overline{2} + N\}$$

und $\overline{3} + N = \overline{3} + \{\overline{0}, \overline{3}\} = \{\overline{3}, \overline{0}\} = \overline{0} + N$. Entsprechend folgt $\overline{4} + N = \overline{1} + N$ und $\overline{5} + N = \overline{2} + N$. Damit ergibt sich eine Additionstabelle analog zu (a).

Kapitel 5

Isomorphiesätze

Sei G eine Gruppe, $N \trianglelefteq G$. Was ist der „Isomorphietyp“ von ${}^{G}\!/_{N}$, d. h. welche bekannte Gruppe ist dazu isomorph?

Bemerkung 5.1. Sei $N \leq G$ eine Untergruppe. Dann ist $N \trianglelefteq G$ genau dann, wenn N der Kern eines Homomorphismus von G ist.

Beweis. Sei N der Kern eines Homomorphismus $\varphi : G \to U$. Nach 4.6 ist $N = \mathrm{Ker}(\varphi) \trianglelefteq G$. Umgekehrt, nach 4.8 ist $\pi : G \to {}^{G}\!/_{N}, g \mapsto gN$ ein Homomorphismus mit Kern N. □

Beispiel 5.2.

(1) Die Abbildung $\mathrm{sgn} : S_n \to \{\pm 1\}, \pi \mapsto \mathrm{sgn}(\pi)$ ist ein Epimorphismus (für $n > 1$). Was ist der Isomorphietyp von ${}^{S_n}\!/_{\mathrm{Ker}(\mathrm{sgn})} = {}^{S_n}\!/_{A_n}$? Aus Beispiel 4.5 wissen wir:

$$ {}^{S_n}\!/_{\mathrm{Ker}(\mathrm{sgn})} = {}^{S_n}\!/_{A_n} = \{A_n, \tau A_n\}, $$

wobei $\mathrm{sgn}(\tau) = -1$ ist. Also ist ${}^{S_n}\!/_{\mathrm{Ker}(\mathrm{sgn})} \simeq C_2 \simeq \{\pm 1\} = \mathrm{im}(\mathrm{sgn})$.

(2) Sei $\varphi : \mathbb{R}^\times \to \mathbb{R}^\times, r \mapsto |r|$. Dann ist φ ein Homomorphismus mit

$$ \begin{aligned} \mathrm{Ker}(\varphi) &= \{r \in \mathbb{R}^\times \mid |r| = 1\} = \{\pm 1\}, \\ \mathrm{im}(\varphi) &= \{|r| \mid r \in \mathbb{R}^\times\} = \mathbb{R}^{\mathrm{pos}} = (0, \infty) \ . \end{aligned} $$

Was ist der Isomorphietyp von ${}^{\mathbb{R}^\times}\!/_{\{\pm 1\}}$? Man sieht leicht, dass gilt:

$$ {}^{\mathbb{R}^\times}\!/_{\{\pm 1\}} = {}^{\mathbb{R}^\times}\!/_{\mathrm{Ker}(\varphi)} \simeq \mathbb{R}^{\mathrm{pos}} = \mathrm{im}(\varphi), $$

mittels der Abbildung $r \cdot \{\pm 1\} \mapsto |r|$.

(3) Betrachte den Epimorphismus $\det : \mathrm{GL}_n(K) \to K^\times, A \mapsto \det(A)$. Was ist der Isomorphietyp von ${}^{\mathrm{GL}_n(K)}\!/_{\mathrm{SL}_n(K)}$? Gilt ${}^{\mathrm{GL}_n(K)}\!/_{\mathrm{SL}_n(K)} \simeq \mathrm{im}(\det) \simeq K^\times$? Ja.

Theorem 5.3 (Homomorphiesatz)**.** *Sei $\varphi : G \to H$ ein Homomorphismus. Dann ist*

$$ {}^{G}\!/_{\mathrm{Ker}(\varphi)} \simeq \mathrm{im}(\varphi) $$

vermöge der Abbildung $g\,\mathrm{Ker}(\varphi) \mapsto \varphi(g)$.

Beweis. Sei $N \coloneqq \operatorname{Ker}(\varphi)$. Definiere $\overline{\varphi} : {}^{G}\!/_{N} \to \operatorname{im}(\varphi)$, durch $gN \mapsto \varphi(g)$.

(i) Sei $gN = g'N$, dann ist $g = g'n$ für ein $n \in N$. Damit folgt

$$\varphi(g) = \varphi(g'n) = \varphi(g')\underbrace{\varphi(n)}_{=1} = \varphi(g') \ ,$$

also $\overline{\varphi}(gN) = \overline{\varphi}(g'N)$. Also ist $\overline{\varphi}$ wohldefiniert.

(ii) Es gilt:

$$\overline{\varphi}(gN \cdot hN) = \overline{\varphi}(ghN) = \varphi(gh) = \varphi(g)\varphi(h) = \overline{\varphi}(gN)\overline{\varphi}(hN) \ .$$

Also ist $\overline{\varphi}$ ein Homomorphismus.

(iii) Nach Definition ist die Abbildung $\overline{\varphi}$ surjektiv. Sei $\overline{\varphi}(gN) = \overline{\varphi}(hN)$, dann folgt $\varphi(g) = \varphi(h)$ und damit $1 = \varphi(h)^{-1}\varphi(g) = \varphi(h^{-1}g)$. Es folgt $h^{-1}g \in \operatorname{Ker}(\varphi) = N$, also $h^{-1}gN \subseteq N$, also $gN \subseteq hN$ und damit auch $gN = hN$. Also ist $\overline{\varphi}$ injektiv und damit ein Isomorphismus. □

Korollar 5.4. *Sei G endlich und $\varphi : G \to H$ ein Homomorphismus. Dann folgt aus 5.3, dass*

$$|G| = |\operatorname{Ker}(\varphi)| \cdot |\operatorname{im}(\varphi)| \ .$$

Die Isomorphiesätze sind Anwendungen des Homomorphiesatzes:

Theorem 5.5. *Sei G eine Gruppe.*

(a) 1. Isomorphiesatz: Sei $N \trianglelefteq G, H \leq G$. Dann ist $NH \leq G$ mit

$${}^{(HN)}\!/_{N} \simeq {}^{H}\!/_{(H \cap N)} \ .$$

(Ist $H \trianglelefteq G$, so ist $HN \trianglelefteq G$.)

(b) 2. Isomorphiesatz: Seien $N, H \trianglelefteq G$ mit $N \leq H \leq G$. Dann ist

$$\left({}^{G}\!/_{N}\right)\!/\left({}^{H}\!/_{N}\right) \simeq {}^{G}\!/_{H} \ .$$

Beweis.

(a) (i) $N \trianglelefteq G$ impliziert $HN = NH$, da $hN = Nh$ für alle $h \in H$. Aus 2.8 folgt, dass $HN \leq G$. Da $N \trianglelefteq G$, ist auch $N \trianglelefteq HN$, denn HN ist eine Teilmenge von G.

(ii) Betrachte den Homomorphismus

$$\begin{aligned} \varphi : H &\overset{\text{Einbettung}}{\hookrightarrow} HN \overset{\text{kan. Proj.}}{\longrightarrow} {}^{HN}\!/_{N} \\ h &\mapsto \ h \ \mapsto hN \ . \end{aligned}$$

Dann gilt

$$\operatorname{Ker}(\varphi) = \{h \in H \mid hN = N\} = \{h \in H \mid h \in N\} = H \cap N \ ,$$

Nach 4.6 gilt insbesondere $H \cap N \trianglelefteq H$. Nach 5.4 gilt:

$${}^{H}\!/_{(H \cap N)} = {}^{H}\!/_{\operatorname{Ker}(\varphi)} \simeq \operatorname{im}(\varphi) = {}^{(HN)}\!/_{N} \ ,$$

wobei $h(H \cap N) \mapsto hN$.

(b) (i) Da $N \trianglelefteq G$ und $H \subseteq G$ gilt, folgt $N \trianglelefteq H$. Also ist ${}^{H}\!/_{N} \leq {}^{G}\!/_{N}$ eine Untergruppe. Da $H \trianglelefteq G$ ist, folgt:

$$gN \cdot hN \cdot g^{-1}N = \underbrace{ghg^{-1}}_{\in H} \cdot N \in {}^{H}\!/_{N} \ .$$

Also ist ${}^{H}\!/_{N} \trianglelefteq {}^{G}\!/_{N}$.

(ii) Betrachte

$$\varphi : G \xrightarrow{\pi_1} {}^{G}\!/_{N} \xrightarrow{\pi_2} \left({}^{G}\!/_{N}\right)\!/\left({}^{H}\!/_{N}\right) \ ,$$
$$g \mapsto gN \mapsto gN\left({}^{H}\!/_{N}\right) \ ,$$

dann ist φ ein Epimorphismus mit

$$\mathrm{Ker}(\varphi) = \{g \in G \mid \pi_1(g) = gN \in {}^{H}\!/_{N}\} = \{g \in G \mid g \in H\} = H \ .$$

Nach 5.4 gilt also:

$${}^{G}\!/_{H} = {}^{G}\!/_{\mathrm{Ker}(\varphi)} \simeq \mathrm{im}(\varphi) = \left({}^{G}\!/_{N}\right)\!/\left({}^{H}\!/_{N}\right)$$

mit $gH \mapsto gN\left({}^{H}\!/_{N}\right)$. □

Beispiel 5.6. Wir geben Beispiele zu den Isomorphiesätzen an:

(1) (a) Sei $G = \mathbb{Z}, H = 5\mathbb{Z}$, und $N = 3\mathbb{Z}$. Dann ist $H \cap N = 5\mathbb{Z} \cap 3\mathbb{Z} = 15\mathbb{Z}$ und $H + N = 5\mathbb{Z} + 3\mathbb{Z} = \mathbb{Z}$, denn $1 = 5 \cdot (-1) + 3 \cdot 2$. Mit dem ersten Isomorphiesatz 5.5 (a) folgt

$${}^{\mathbb{Z}}\!/_{3\mathbb{Z}} = {}^{H+N}\!/_{N} \simeq {}^{H}\!/_{H \cap N} = {}^{5\mathbb{Z}}\!/_{15\mathbb{Z}} \ .$$

(b) Seien $n, m \in \mathbb{N}$. Dann ist $N := mn\mathbb{Z} \subseteq H := m\mathbb{Z} \subseteq G := \mathbb{Z}$. Also gilt nach dem zweiten Isomorphiesatz 5.5 (b):

$$\left({}^{\mathbb{Z}}\!/_{mn\mathbb{Z}}\right)\!/\left({}^{m\mathbb{Z}}\!/_{mn\mathbb{Z}}\right) = \left({}^{G}\!/_{N}\right)\!/\left({}^{H}\!/_{N}\right) \simeq {}^{G}\!/_{H} = {}^{\mathbb{Z}}\!/_{m\mathbb{Z}} \ .$$

(2) Sei K ein Körper und $n \in \mathbb{N}$.

(a) Sei $D := \{\lambda I_n \mid \lambda \in K^\times\} \leq \mathrm{GL}_n(K)$. Es gilt $D \simeq K^\times$ vermöge $\lambda I_n \mapsto \lambda$. Da $A \cdot \lambda I_n \cdot A^{-1} = \lambda I_n \in D$ für alle $A \in \mathrm{GL}_n(K)$ gilt, ist $D \trianglelefteq \mathrm{GL}_n(K)$. Definiere $\mathrm{PGL}_n(K) := {}^{\mathrm{GL}_n(K)}\!/_{D}$, genannt *projektive lineare Gruppe*.

(b) Sei $G := \mathrm{GL}_n(K), N := D$, und $H := \mathrm{SL}_n(K)$. Dann ist

$$H \cap N = \mathrm{SL}_n(K) \cap D = \{\lambda I_n \mid \lambda^n = 1\} =: \mu_n(K) \simeq \{\lambda \in K^\times \mid \lambda^n = 1\}.$$

Wir definieren die *projektive speziell lineare Gruppe* $\mathrm{PSL}_n(K)$ durch

$$\begin{aligned} \mathrm{PSL}_n(K) &:= {}^{\mathrm{SL}_n(K)}\!/_{\mu_n(K)} = {}^{\mathrm{SL}_n(K)}\!/_{(\mathrm{SL}_n(K) \cap D)} \\ &= {}^{H}\!/_{(H \cap N)} \overset{5.5\,(a)}{\simeq} {}^{(HN)}\!/_{N} = {}^{(\mathrm{SL}_n(K) \cdot D)}\!/_{D} \\ &\overset{2.8}{\leq} {}^{\mathrm{GL}_n(K)}\!/_{D} = \mathrm{PGL}_n(K) \ . \end{aligned}$$

Theorem 5.7 (Untergruppenkorrespondenz)**.**

(a) Jede Untergruppe von G/N *hat die Form* H/N *für* $H \leq G$ *mit* $N \subseteq H$*.*

(b) Die Abbildung

$$\{H \leq G \mid N \subseteq H\} \to \left\{\text{Untergruppen von } G/N\right\}, H \mapsto H/N$$

ist bijektiv und inklusionserhaltend mit Umkehrabbildung $H' \mapsto \pi^{-1}(H')$*, wobei*

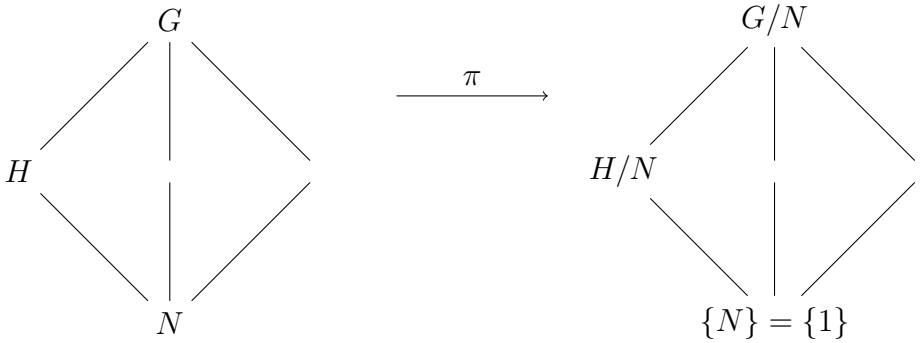
$$\pi : G \to G/N, g \mapsto gN$$

die natürliche Projektion ist.

(c) Es gilt $H \trianglelefteq G \Leftrightarrow H/N \trianglelefteq G/N$*.*

Beweis. Sei H' eine Untergruppe von G/N. Nach 4.6 ist $\pi^{-1}(H')$ eine Untergruppe von G mit $N \subseteq \pi^{-1}(H')$ und $\pi^{-1}(H')/N = H'$. □

Bemerkung: Dieses Theorem zeigt, dass durch die Abbildung $\pi : G \to G/N$ ein Verbandsisomorphismus induziert wird:



Beispiel 5.8.

(a) Sei $V_4 \coloneqq \{\mathrm{id}, (12)(34), (13)(24), (14)(23)\} \leq S_4$. Sei $\pi \in S_4$, dann ist

$$\pi(ab)(cd)\pi^{-1} = (\pi a, \pi b)(\pi c, \pi d) \in V_4 \ .$$

Damit folgt $V_4 \trianglelefteq S_4$.

(b) Es gilt $S_3 = \{\mathrm{id}, (12), (13), (23), (123), (132)\} \leq S_4$. Ausserdem ist $V_4 \cap S_3 = \{\mathrm{id}\}$. Mit 2.8 folgt $V_4S_3 = S_3V_4 \leq S_4$. Es ist

$$\begin{aligned} \overbrace{(14)(23)}^{\in V_4} \cdot \overbrace{(13)}^{\in S_3} &= (1234) \in V_4S_3 \\ \mathrm{id} \cdot (12) &= (12) \in V_4S_3 \ , \end{aligned}$$

also $S_4 = \langle (12), (1234) \rangle \subseteq V_4S_3 \subseteq S_4$ (vgl. Blatt 3) und damit $S_4 = V_4S_3$. Dann folgt mit dem ersten Isomorphiesatz:

$$S_3 \simeq S_3/(V_4 \cap S_3) \simeq (V_4S_3)/V_4 = S_4/V_4 \ .$$

Dieser Isomorphismus ist gegeben durch $\pi \mapsto \pi(V_4 \cap S_3) \mapsto \pi V_4$.

(c) Nach der Untergruppenkorrespondenz sieht der entsprechende Teil des Untergruppenverbandes von S_4 analog dem Bild in Beispiel 4.5 aus.

Die Gruppe S_4 hat 30 verschiedene Untergruppen U mit den folgenden Ordnungen:

$\lvert U\rvert$	1	2	3	4	6	8	12	24
#	1	9	4	7	4	3	1	1

Zum Beispiel hat S_4 sechs verschiedene Transpositionen, außerdem drei Elemente die Produkte von zwei Transpositionen sind. Diese Elemente haben Ordnung zwei, und erzeugen jeweils eine Untergruppe isomorph zu C_2. Damit hat S_4 neun verschiedene Untergruppen mit zwei Elementen.

Kapitel 6

Endlich erzeugte abelsche Gruppen

Definition 6.1. Gegeben seien Gruppen G_1, G_2.

(a) Dann ist $G_1 \times G_2 = \{(x_1, x_2) \mid x_1 \in G_1, x_2 \in G_2\}$ mit der Multiplikation

$$(x_1, x_2)(y_1, y_2) \coloneqq (x_1 \cdot_{G_1} y_1, x_2 \cdot_{G_2} y_2)$$

eine Gruppe (siehe Blatt 1). $G_1 \times G_2$ heißt (äußeres) direktes Produkt von G_1 und G_2.

(b) Es gilt: $Z(G_1 \times G_2) = Z(G_1) \times Z(G_2)$. Außerdem ist $G_1 \times G_2$ genau dann abelsch, wenn G_1 und G_2 abelsch sind.

Bemerkung 6.2. Die Abbildungen

$$\iota_1 : G_1 \to G_1 \times G_2, x \mapsto (x, 1)$$
$$\iota_2 : G_2 \to G_1 \times G_2, y \mapsto (1, y)$$

sind Monomorphismen. Die Abbildungen

$$\pi_1 : G_1 \times G_2 \to G_1, (x, y) \mapsto x$$
$$\pi_2 : G_1 \times G_2 \to G_2, (x, y) \mapsto y$$

sind Epimorphismen. Dann gelten die Eigenschaften:

(i)

$$\operatorname{im}(\iota_1) = G_1 \times \{1\} = \operatorname{Ker}(\pi_2) \overset{4.6}{\trianglelefteq} G_1 \times G_2 \ ,$$
$$\operatorname{im}(\iota_2) = \{1\} \times G_2 = \operatorname{Ker}(\pi_1) \trianglelefteq G_1 \times G_2 \ .$$

(ii) $(G_1 \times \{1\}) \cdot (\{1\} \times G_2) = G_1 \times G_2$.

(iii) $(G_1 \times \{1\}) \cap (\{1\} \times G_2) = \{(1, 1)\}$

Definition 6.3. Eine Gruppe G heißt (inneres) direktes Produkt von G_1, G_2, falls

(i) $G_1, G_2 \trianglelefteq G$,

(ii) $G_1 \cdot G_2 = G$,

(iii) $G_1 \cap G_2 = \{1\}$.

Bemerkung 6.4.

(a) Ist $G = G_1 \times G_2$ äußeres direktes Produkt, dann folgt mit 6.2, dass G inneres direktes Produkt von $G_1 \times \{1\}$ und $\{1\} \times G_2$ ist.

(b) Ist G inneres direktes Produkt von G_1 und G_2, dann gilt $G_1 \times G_2 \simeq G = G_1G_2$ vermöge $(x_1, x_2) \mapsto x_1x_2$.

Beweis.

(i) Da $G_1, G_2 \trianglelefteq G$, gilt für $x_1 \in G_1$ und $x_2 \in G_2$:

$$\underbrace{(x_1 \underbrace{x_2}_{\in G_2} x_1^{-1})}_{\in G_2} \underbrace{x_2^{-1}}_{\in G_2} = \underbrace{x_1}_{\in G_1} \underbrace{(x_2 \underbrace{x_1^{-1}}_{\in G_1} x_2^{-1})}_{\in G_1} \in G_1 \cap G_2 = \{1\} \ .$$

Damit folgt $x_1x_2x_1^{-1}x_2^{-1} = 1$, also $x_1x_2 = x_2x_1$.

(ii) Sei $\varphi : G_1 \times G_2 \to G, (g_1, g_2) \mapsto g_1 \cdot g_2$. Dann ist

$$\begin{aligned}\varphi((x_1, x_2) \cdot (y_1, y_2)) &= \varphi((x_1y_1, x_2y_2)) = x_1(y_1x_2)y_2 \\ &\overset{\text{(i)}}{=} (x_1x_2)(y_1y_2) = \varphi(x_1, x_2)\varphi(y_1, y_2) \ ,\end{aligned}$$

also ist φ ein Epimorphismus.

(iii) Sei $(g_1, g_2) \in \mathrm{Ker}(\varphi)$. Dann gilt $g_1 \cdot g_2 = 1$, also $g_1 = g_2^{-1} \in G_1 \cap G_2 = \{1\}$, folglich $g_1 = g_2 = 1$ und damit $\mathrm{Ker}(\varphi) = \{(1, 1)\}$. Also ist φ ein Isomorphismus. □

Beispiel 6.5. (1) Die Gruppe $\mathbb{C}^\times$ ist kommutativ. Es gilt

(i) $S^1 := \{z \in \mathbb{C}^\times \mid |z| = 1\} \trianglelefteq \mathbb{C}^\times$ und $\mathbb{R}^{\mathrm{pos}} \trianglelefteq \mathbb{C}^\times$.

(ii) $\mathbb{R}^{\mathrm{pos}} \cdot S^1 = \{re^{i\varphi} \mid r \in \mathbb{R}^{\mathrm{pos}}, 0 \leq \varphi < 2\pi\} = \mathbb{C}^\times$.

(iii) $\mathbb{R}^{\mathrm{pos}} \cap S^1 = \{1\}$.

Damit ist $\mathbb{C}^\times = \mathbb{R}^{\mathrm{pos}} \cdot S^1$ ein direktes Produkt.

(2) Da $(14)(123)(14) = (234) \notin S_3$ ist, gilt $S_3 \not\trianglelefteq S_4$ in Beispiel 5.8. Also ist S_4 kein direktes Produkt von V_4 und S_3. Es gilt aber $V_4 \trianglelefteq S_4$, $V_4 \cap S_3 = \{\mathrm{id}\}$ und $V_4 \cdot S_3 = S_4$.

Theorem 6.6. *Jede endlich erzeugte abelsche Gruppe ist ein (endliches) Produkt zyklischer Gruppen.*

Beweis. Sei $(G, +)$ eine abelsche Gruppe, erzeugt von k Elementen. Wir führen eine Induktion über k durch. Für $k = 1$ ist G nach Definition 3.1 zyklisch.
Sei also $k > 1$.

(a) Wähle $a_1, \ldots, a_k \in G$ und $n_1, \ldots, n_k \in \mathbb{Z}$ mit

(i) $\langle a_1, \ldots, a_k\rangle = G$,

(ii) $n_1a_1 + \ldots + n_ka_k = 0$,

(iii) $|n_1| \neq 0$ minimal mit (i) und (ii) .

(b) Angenommen, es lassen sich keine solchen Elemente finden, dann gibt es keine Nullrelation in G. Dann ist die Abbildung $\mathbb{Z}^k \to G, (n_1, \ldots, n_k) \mapsto n_1a_1 + \ldots + n_ka_k$ ein Isomorphismus und $G \simeq \mathbb{Z}^k$ liefert die Behauptung.

(c) O.E. gibt es also Werte a_i und n_i mit (i) - (iii) und $n_1 > 0$. Wir zeigen $n_1 \mid n_2$. Aus Symmetriegründen folgt $n_1 \mid n_i$ für alle $i \in \{1, \ldots, k\}$. Schreibe $n_2 = q \cdot n_1 + r$ mit $0 \leq r \leq n_1 - 1$. Es ist

$$\begin{aligned} 0 &= n_1a_1 + (qn_1 + r)a_2 + n_3a_3 + \ldots + n_ka_k \\ &= ra_2 + n_1(a_1 + qa_2) + n_3a_3 + \ldots + n_ka_k \end{aligned}$$

und $G = \langle a_1, a_2, \ldots, a_k\rangle = \langle a_2, a_1 + qa_2, a_3, \ldots, a_k\rangle$. Aus Bedingung (iii) folgt $r = 0$, also $n_1 \mid n_2$. Analog folgt $n_1 \mid n_i$ für alle $i \in \{1, \ldots, k\}$.

(d) Sei $a_1' \coloneqq a_1 + \frac{n_2}{n_1}a_2 + \ldots + \frac{n_k}{n_1}a_k \in G$. Dann ist $\langle a_1', a_2, \ldots, a_k\rangle = \langle a_1, \ldots, a_k\rangle = G$. Sei $\phi : \langle a_1'\rangle \times \langle a_2, \ldots, a_k\rangle \to G, (u, v) \mapsto u + v$. Dann ist ϕ ein Epimorphismus. Wir zeigen, dass ϕ injektiv ist: Sei $\phi(u, v) = 0$. Sei $u = ma_1', v = m_2a_2 + \ldots + m_ka_k$. Es ist $n_1a_1' \overset{\text{(ii)}}{=} 0$ und mit (iii) $\operatorname{ord}(a_1') = n_1$: Angenommen, $0 < n < n_1$ mit $n = \operatorname{ord}(a_1')$. Dann ist

$$na_1' = na_1 + \frac{nn_2}{n_1}a_2 + \ldots + \frac{nn_k}{n_1}a_k = 0 \ .$$

Dies liefert einen Widerspruch zu (iii). Also $\langle a_1'\rangle \simeq \mathbb{Z}_{n_1}$. O.E. wähle $0 \leq m < n_1$ in $u = ma_1'$. Dann ist

$$0 = \phi(u, v) = u + v = ma_1' + m_2a_2 + \ldots + m_ka_k \ ,$$

also $m = 0$, d. h. $u = 0$. Damit ist $v = u + v = \phi(u, v) = 0$. Dies zeigt $\operatorname{Ker}(\varphi) = \{0\}$, d. h. φ ist ein Isomorphismus. Damit gilt $G \simeq \mathbb{Z}_{n_1} \times \langle a_2, \ldots, a_k\rangle$. Nach Induktionsvoraussetzung ist G damit ein Produkt zyklischer Gruppen. □

Korollar 6.7. *Sei G endliche abelsche Gruppe, dann ist $G \simeq \mathbb{Z}_{n_1} \times \mathbb{Z}_{n_2} \times \ldots \times \mathbb{Z}_{n_t}$ mit $1 < n_1 \leq n_2 \leq \ldots \leq n_t$ und $n_1 \mid n_2 \mid \ldots \mid n_t$, wobei t und $n_1, \ldots, n_t$ eindeutig durch G bestimmt sind. Die n_i heißen die* Elementarteiler von G.

Beweis. Existenz folgt aus 6.6, die Eindeutigkeit wird hier nicht bewiesen. □

Bemerkung 6.8. Es gilt $\mathbb{Z}_m \times \mathbb{Z}_n$ zyklisch $\Leftrightarrow \operatorname{ggT}(m, n) = 1$. In diesem Fall ist

$$\mathbb{Z}_m \times \mathbb{Z}_n = \mathbb{Z}_{mn}.$$

Beweis. „⇐“: Sei der grösste gemeinsame Teiler $\operatorname{ggT}(m, n) = 1$.

(i) Sei $t \coloneqq \operatorname{ord}(1, 1)$. Dann folgt $(0, 0) = t \cdot (1, 1) = (t, t)$ in $\mathbb{Z}_m \times \mathbb{Z}_n$, also $m \mid t, n \mid t$. Mit $\operatorname{ggT}(m, n) = 1$ folgt $mn \mid t$.

(ii) Da $mn(1, 1) = (mn, mn) = (0, 0)$ gilt, folgt $t \mid mn$ mit Lemma 3.5 (a), also $mn = \operatorname{ord}(1, 1)$. Da $|\mathbb{Z}_m \times \mathbb{Z}_n| = m \cdot n = \operatorname{ord}(1, 1)$ gilt, folgt $\mathbb{Z}_m \times \mathbb{Z}_n = \langle(1, 1)\rangle$.

„⇒“: Sei $\mathbb{Z}_m \times \mathbb{Z}_n$ zyklisch. Sei $d \coloneqq \operatorname{ggT}(m, n)$. Sei $m' = m/d, n' = n/d$. Sei $(x, y) \in \mathbb{Z}_m \times \mathbb{Z}_n$. Dann ist

$$m'dn'(x, y) = (m'dn'x, m'dn'y) = (mn'x, nm'y) = (0, 0)$$

in $\mathbb{Z}_m \times \mathbb{Z}_n$. Mit Lemma 3.5 (a) folgt $\operatorname{ord}(x, y) \mid m'dn'$. Angenommen $d > 1$, dann ist $m'dn' < mn$, und $\mathbb{Z}_m \times \mathbb{Z}_n$ hat kein Element der Ordnung mn. Also gilt $d = 1$. □

Korollar 6.9 (Hauptsatz für endlich erzeugte abelsche Gruppen)**.** *Sei G endlich erzeugte abelsche Gruppe. Dann existieren eindeutige $r, m \in \mathbb{N}$ und bis auf Reihenfolge eindeutige Primzahlpotenzen $p_1^{k_1}, \ldots, p_m^{k_m}$ (nicht notwendigerweise verschieden) mit*

$$G \simeq \mathbb{Z}^r \times \mathbb{Z}_{p_1^{k_1}} \times \ldots \times \mathbb{Z}_{p_m^{k_m}} \ .$$

Beweis. Das Korollar folgt aus 6.7 und 6.8. □

Beispiel 6.10. Ist $|G| = 16$ mit G abelsch, dann ist G isomorph zu einer der Gruppen $C_{16}, C_2 \times C_8, C_4 \times C_4, C_2 \times C_2 \times C_4$ oder $C_2 \times C_2 \times C_2 \times C_2$.

Kapitel 7

Operationen von Gruppen auf Mengen

Sei G eine Gruppe und K ein Körper.

Definition 7.1. Sei $\emptyset \neq X$ eine Menge. Dann heißt X eine *G-Menge* (bzw. G *operiert auf* X), wenn es eine Abbildung $* : G \times X \to X, (g, x) \mapsto g * x$ gibt mit

(O1) $1 * x = x$ für alle $x \in X$,

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

Typischerweise schreiben wir $\cdot$ statt $*$. Es ergibt sich in der Regel aus dem Zusammenhang, ob es sich bei einem Punkt $\cdot$ um Gruppenmultiplikation oder um die Operation der Gruppe auf einer Menge handelt.

Bemerkung 7.2.

(a) Sei X eine G-Menge, $g \in G$. Dann ist $\tau_g : X \to X, x \mapsto g \cdot x$ bijektiv; die Inverse ist $\tau_{g^{-1}}$. Also ist $\tau_g \in S_X$. Sei $\tau : G \to S_X, g \mapsto \tau_g$. Dann ist

$$\tau_{gh}(x) = (gh) \cdot x \overset{(O2)}{=} g \cdot (h \cdot x) = \tau_g(\tau_h(x)) = (\tau_g \circ \tau_h)(x)$$

für alle $x \in X$. Somit gilt $\tau_{gh} = \tau_g \circ \tau_h$ für alle $g, h \in G$. Damit gilt

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

also ist τ ein Homomorphismus.

(b) Umgekehrt, jeder Homomorphismus $\varphi : G \to S_X$, mit $g \mapsto \varphi_g$ definiert eine G-Menge X durch

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

denn $1 \cdot x = \varphi_1(x) = \mathrm{id}(x) = x$ und

$$(gh) \cdot x = \varphi_{gh}(x) = (\varphi_g \circ \varphi_h)(x) = \varphi_g(\varphi_h(x)) = g \cdot (h \cdot x) \ .$$

Ist die Abbilung τ injektiv, so sagt man die Operation von G auf X ist *treu*. Äquivalent, die Operation von G auf X ist treu, falls das einzige Element mit $gx = x$ für alle $x \in X$ das neutrale Element ist.

Beispiel 7.3. Es gibt unzählige Beispiele, in denen Gruppen auf Mengen operieren. Hier erste Beispiele:

(1) Sei $U \leq G$. Definiere $X := {}^{G}\!/_{U} = \{xU \mid x \in G\}$. Definiere $G \times X \to X$, durch $(g, xU) \mapsto (gx)U =: g \cdot (xU)$. Dann ist X eine G-Menge.

- Diese Operation ist wohldefiniert: Sei $xU = \tilde{x}U$. Dann existiert $u \in U$ mit $x = \tilde{x}u$. Dann ist

$$gxU = g\tilde{x}uU = g\tilde{x}U \ .$$

- Zu $x, y \in G$ existiert ein Element $g \in G$ mit $g \cdot x = y$. Das heißt, zu Nebenklassen $xU, yU \in X$ existiert ein Element $g \in G$ mit $g(xU) = yU$. (Man sagt, die Operation ist transitiv.)

(2) (a) Die Gruppe G operiert auf der Menge $X = G$ durch Gruppenmultiplikation von links: $G \times X \to X, (g, x) \mapsto g \cdot x$. Die Gruppenaxiome von G implizieren, dass X eine G-Menge ist. Nach Bemerkung 7.2 ist $\tau : G \to S_G$, mit $\tau_g = l_g$ ein Homomorphismus (siehe 1.6). Sei $l_g = l_h$, dann ist $g \cdot x = h \cdot x$ für alle $x \in G = X$. Dann folgt mit der Wahl $x = 1$ insbesondere $g = h$. Somit ist τ ein Monomorphismus.

Satz von Cayley: Jede (endliche) Gruppe G ist isomorph zu einer Untergruppe einer (endlichen) symmetrischen Gruppe.

(b) G operiert auf $X = G$ durch Rechtsmultiplikation: $G \times X \to X, (g, x) \mapsto x \cdot g^{-1}$, denn

$$(gh) * x \overset{\text{Def}}{=} x \cdot (gh)^{-1} \overset{1.2}{=} x(h^{-1}g^{-1}) \overset{(G1)}{=} (x \cdot h^{-1}) \cdot g^{-1} \overset{\text{Def}}{=} g * (h * x) \ .$$

Definition 7.4. Sei X eine G-Menge. Für $x \in X$ heißt

(i) $\mathcal{O}_x := G \cdot x := \{g \cdot x \mid g \in G\}$ die *Bahn von x unter G*. Die Operation heißt *transitiv*, falls X unter G nur eine Bahn besitzt. (Äquivalent: Für alle $x, y \in X$ existiert $g \in G$ mit $g \cdot x = y$.)

(ii) $G_x := \mathrm{Stab}_G(x) := \{g \in G \mid g \cdot x = x\}$ *Stabilisator von x in G*. Es ist $\mathrm{Stab}_G(x) = G$ genau dann, wenn $g \cdot x = x$ für alle $g \in G$. In diesem Fall nennt man x *Fixpunkt* der Operation. Schreibe X^G für die Menge aller Fixpunke von X unter der Operation von G.

Lemma 7.5. *Sei X eine G-Menge. Dann ist*

(i) $\mathrm{Stab}_G(x) \leq G$.

(ii) $\mathrm{Stab}_G(a \cdot x) = a \cdot \mathrm{Stab}_G(x) \cdot a^{-1}$. *Elemente in der gleichen Bahn haben also konjugierte Stabilisatoren.*

Beweis.

(i) Es gilt $1x = x$, also $1 \in \mathrm{Stab}_G(x)$. Seien $g, h \in \mathrm{Stab}_G(x)$. Dann folgt $gx = x = hx$, also $(gh)x = g(hx) = gx = x$ und damit $gh \in \mathrm{Stab}_G(x)$. Außerdem gilt $g^{-1}x = g^{-1}(gx) = (g^{-1}g)x = 1 \cdot x = x$. Somit ist $g^{-1} \in \mathrm{Stab}_G(x)$.

(ii) Sei $a \in G$. Dann gilt:

$$\begin{aligned} g \in \mathrm{Stab}_G(ax) &\Leftrightarrow ax = g(ax) = (ga)x \\ &\Leftrightarrow x = (a^{-1}ga)x \\ &\Leftrightarrow a^{-1}ga \in \mathrm{Stab}_G(x) \\ &\Leftrightarrow g \in a \cdot \mathrm{Stab}_G(x) \cdot a^{-1} \ . \end{aligned}$$

□

Bemerkung 7.6. Sei X eine G-Menge. Definiere $\sim$ auf X durch

$$x, y \in X, x \sim y \Leftrightarrow \exists g \in G : gx = y \ .$$

Dann ist $\sim$ eine Äquivalenzrelation. Es ist

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

Insbesondere ist X disjunkte Vereinigung der Bahnen.

Theorem 7.7 (Bahnensatz)**.** *Sei X eine G-Menge. Dann ist die Abbildung*

$$G \cdot x \to {}^{G}\!/_{\mathrm{Stab}(x)}, a \cdot x \mapsto a\,\mathrm{Stab}(x)$$

wohldefiniert und bijektiv. Insbesondere ist $|G \cdot x| = [G : \mathrm{Stab}(x)]$.

Beweis. Es gilt $ax = bx \Leftrightarrow x = a^{-1}bx \Leftrightarrow a^{-1}b \in \mathrm{Stab}(x) \Leftrightarrow a\,\mathrm{Stab}(x) = b\,\mathrm{Stab}(x)$. Daher ist die Abbildung wohldefiniert und injektiv. Ausserdem ist die Abbildung surjektiv nach Definition. □

Korollar 7.8. *Sei X eine G-Menge. Sei $\{x_i\}_{i \in I}$ ein Vertretersystem der Bahnen von X unter G. Dann ist*

$$|X| \overset{7.6}{=} \sum_{i \in I} |Gx_i| = |X^G| + \sum_{i \in I, x_i \notin X^G} |Gx_i| \ ,$$

wobei X^G die Menge aller Fixpunkte unter G ist, d. h. der Bahnen der Länge eins, ist. Mit 7.7 folgt

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

Beispiel 7.9.

(a) G operiert auf $X = G$ durch *Konjugation*, d. h. $* : G \times X \to X, (g, x) \mapsto g \cdot x \cdot g^{-1}$. Dann ist X eine G-Menge: Seien $g, h \in G$. Dann ist

$$\begin{aligned} (1, x) &\mapsto 1 \cdot x \cdot 1^{-1} = x \\ (gh, x) &\mapsto (gh)x(gh)^{-1} = g(hxh^{-1})g^{-1} = g * (h * x) \end{aligned}$$

für alle $x \in G$.

(b) Die Bahn $G \cdot x = \{gxg^{-1} \mid g \in G\} =: \mathcal{C}_x$ heißt *Konjugationsklasse* von x. Elemente $a, b \in G$ heißen *konjugiert*, $a \sim b$, falls $g \in G$ existiert mit $b = gag^{-1}$, also falls a, b in derselben Bahn liegen.

Der Stabilisator $\mathrm{Stab}_G(x) = \{g \in G \mid gx = xg\} =: C_G(x)$ heißt *Zentralisator von x in G*. Beachte, dass $Z(G)$ gleich der disjunkten Vereinigung aller Konjugationsklassen der Länge eins und gleich der Menge X^G aller Fixpunkte von X unter G ist. Sei $\{x_i\}_{i \in I}$ ein Vertretersystem der Bahnen von X unter G. Also gilt:

$$|G| \overset{7.8}{=} |Z(G)| + \sum_{x_i \notin Z(G)} [G : C_G(x_i)] \qquad (\text{„Klassengleichung“})$$

(c) Sei $N \trianglelefteq G$. Dann ist N disjunkte Vereinigung von Konjugationsklassen.

Beweis. Sei $x \in N$. Da N normal ist, ist $gxg^{-1} \in N$ für alle $g \in G$. Also $\mathcal{C}_x \subseteq N$. Damit ist $N = \bigcup_{x \in N} \mathcal{C}_x$, wobei die Vereinigung nach Übergang zu einem geeigneten Vertretersystem disjunkt wird. □

Beispiel 7.10. Zwei Permutationen $\alpha, \beta \in S_n$ sind konjugiert genau dann, wenn sie denselben Zykeltyp haben.

Beweis.

(i) Sei $\sigma = \prod \sigma_i$ ein Produkt disjunkter Zykeln σ_i. Sei $\pi \in S_n$. Nach Blatt 1 gilt:

$$\pi(a_1, \ldots, a_l)\pi^{-1} = (\pi a_1, \ldots, \pi a_l) \ ,$$

also folgt

$$\begin{aligned} \pi\sigma\pi^{-1} &= \pi \left(\prod \sigma_i \right) \pi^{-1} \\ &= (\pi\sigma_1\pi^{-1})(\pi\sigma_2\pi^{-1}) \cdots (\pi\sigma_l\pi^{-1}) \ . \end{aligned} \qquad (*)$$

Somit haben σ und $\pi\sigma\pi^{-1}$ den gleichen Zykeltyp.

(ii) Seien $\alpha, \beta \in S_n$ Permutationen, geschrieben als Produkt disjunkter Zykeln, mit gleichem Zykeltyp. Dann lassen sich die Elemente in den Zykeln von α wie in $(*)$ mit einer Permutation π so umpermutieren, dass sich korrespondierende Zykel in β ergeben. Das heißt $\pi\alpha\pi^{-1} = \beta$ und damit $\alpha \sim \beta$. □

Beispiel 7.11. Die Gruppe $G = \mathrm{GL}_n(K)$ operiert auf $X = K^n$ durch Matrixmultiplikation.

(i) Es ist

$$\begin{aligned} \mathcal{O}_0 &= \{A \cdot 0 \mid A \in \mathrm{GL}_n(K)\} = \{0\} \\ \mathcal{O}_{e_1} &= \{A \cdot e_1 \mid A \in \mathrm{GL}_n(K)\} = K^n \setminus \{0\} \ . \end{aligned}$$

Somit ist $X = K^n = \mathcal{O}_0 \cup \mathcal{O}_{e_1}$. Es ist

$$\mathrm{Stab}_G(e_1) = \{A \in \mathrm{GL}_n \mid Ae_1 = e_1\} = \left\{ \begin{pmatrix} 1 & a_2 & \ldots & a_n \\ 0 & & & \\ \vdots & & A' & \\ 0 & & & \end{pmatrix} \;\middle|\; A' \in \mathrm{GL}_{n-1}(K) \right\} \ .$$

(ii) Sei $|K| = q < \infty$. Dann ist $|\mathcal{O}_{e_1}| = q^n - 1$ und $|\operatorname{Stab}_G(e_1)| = q^{n-1} \cdot |\operatorname{GL}_{n-1}(K)|$. Mit 7.7 folgt

$$|\operatorname{GL}_n(K)| = |\mathcal{O}_{e_1}| \cdot |\operatorname{Stab}_G(e_1)| = (q^n - 1) \cdot q^{n-1} \cdot |\operatorname{GL}_{n-1}(K)| \ .$$

Induktiv folgt

$$|\operatorname{GL}_n(K)| = q^{\frac{n(n-1)}{2}}(q^n - 1)(q^{n-1} - 1) \cdots (q - 1) \ .$$

Kapitel 8

Sylowsätze

Sei G eine Gruppe und p eine Primzahl.

Definition 8.1.

(a) Eine Gruppe G mit $|G| = p^n$, für $n \in \mathbb{N}$, heißt eine *p-Gruppe*.

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

Bemerkung 8.2. Sei G eine p-Gruppe.

(a) Operiert G auf einer Menge X, dann gilt $|X| \equiv |X^G| \pmod{p}$.

(b) Sei $|G| > 1$, dann gilt $|Z(G)| \geq 2$.

Beweis.

(a) Nach 7.8 gilt

$$|X| = |X^G| + \sum_{x_i \notin X^G} [G : \mathrm{Stab}(x_i)] \equiv |X^G| \pmod{p},$$

denn alle $[G : \mathrm{Stab}(x_i)]$ werden von p geteilt.

(b) Die Gruppe G operiere auf $X = G$ durch Konjugation. Dann folgt

$$0 \equiv |G| \equiv |X| \overset{7.9}{\equiv} |Z(G)| \pmod{p}.$$

Somit gilt $p \mid |Z(G)|$, also hat das Zentrum der Gruppe G mindestens zwei Elemente: $|Z(G)| \geq 2$. □

Beispiel 8.3.

(1) Sei $G = S_3$, dann ist $|G| = 2^1 \cdot 3^1$. Es gilt $\mathrm{Syl}_3(G) = \{A_3\}$ und $\mathrm{Syl}_2(G) = \{\langle(12)\rangle, \langle(13)\rangle, \langle(23)\rangle\}$. Beachte, die drei Sylow-2-Untergruppen von S_3 sind konjugiert zueinander.

(2) Sei $G = \mathrm{GL}_n(\mathbb{Z}_p)$, dann ist

$$|G| = p^{n(n-1)/2} \cdot \underbrace{(p^n-1)(p^{n-1}-1)\cdots(p-1)}_{\equiv \pm 1 \pmod p} .$$

Sei U_n die Menge der oberen Dreiecksmatrizen aus $\mathbb{Z}_p^{n\times n}$ mit Diagonaleinträgen 1 (siehe Blatt 1). Da $|U_n| = p^{n(n-1)/2}$ ist, folgt $U_n \in \mathrm{Syl}_p(G)$.

Theorem 8.4 (Sylow)**.** *Sei* $|G| = p^m \cdot q$ *mit* $\mathrm{ggT}(p,q) = 1$.

1. *Für jedes* $1 \le k \le m$ *gibt es eine Untergruppe in* G *der Ordnung* p^k.
2. *Sei* $H \le G$ *mit* $|H| = p^k$, $1 \le k \le m$. *Sei* $S \in \mathrm{Syl}_p(G)$. *Dann existiert* $g \in G$ *mit* $H \le gSg^{-1}$.
3. $n_p \mid q$ *und* $n_p \equiv 1 \pmod p$.

Beachtenswert ist, dass in diesen Sätzen keinerlei Voraussetzung an die Gruppe G gestellt werden, und trotzdem starke Aussagen über die Gruppe G gemacht werden können. Bevor wir die Sätze beweisen, hier zwei direkte Konsequenzen aus den Sylowsätzen:

Korollar 8.5 (Cauchy)**.** *Sei* G *eine endliche Gruppe und* p *eine Primzahl, welche die Gruppenordnung teilt. Dann enthält* G *ein Element der Ordnung* p.

Beweis. Nach dem Satz von Sylow 8.4 enthält G eine Untergruppe H mit $|H| = p$. Also $H \simeq C_p$ und damit existiert $g \in H$ mit $\mathrm{ord}(g) = p$. □

Korollar 8.6. *Sei* $P \in \mathrm{Syl}_p(G)$. *Dann gilt* $P \trianglelefteq G$ *genau dann, wenn* $\mathrm{Syl}_p(G) = \{P\}$.

Beweis. Theorem 8.4 und die Definition von Normalteiler 4.3. □

Beweis 8.7 (des ersten Sylowsatzes)**.** Wir verwenden Induktion nach der Ordnung $|G|$ der Gruppe G. Sei $|G| = p^m \cdot q$ mit $\mathrm{ggT}(p,q) = 1$. Die Gruppe G operiert auf $X = G$ durch Konjugation:

$$\cdot : G \times X \to X, (g,x) \mapsto gxg^{-1} .$$

Sei $\{x_i\}_{i\in I} \subseteq G$ ein Vertretersystem der nicht-zentralen Konjugationsklassen von g (d. h. $x_i \notin Z(G)$). Nach der Klassengleichung 7.9 gilt:

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

und $C_G(x_i)$ ist eine echte Untergruppe von G für alle $i \in I$.

(i) Sei $p \nmid |Z(G)|$. Da p Teiler der Gruppenordnung $|G|$ ist, existiert ein Index $i \in I$ mit $p \nmid [G : C_G(x_i)] = \frac{|G|}{|C_G(x_i)|}$. Dann ist $|C_G(x_i)| = p^m \cdot q'$ mit $\mathrm{ggT}(p,q') = 1$ und $|C_G(x_i)| < |G|$. Nach Induktionsvoraussetzung hat $C_G(x_i)$ eine Untergruppe der Ordnung p^k. Also hat G eine Untergruppe der Ordnung p^k.

(ii) Sei $p \mid |Z(G)|$. Nach Definition ist $Z(G)$ abelsch und endlich. Nach dem Hauptsatz für endlich erzeugte abelsche Gruppen 6.6 ist $Z(G)$ isomorph zu einem Produkt zyklischer Gruppen $\mathbb{Z}_{n_i}$, mit $|Z(G)| = \prod n_j$. Also existiert ein Index j mit $p \mid n_j$. Nach 3.7 existiert $g \in \mathbb{Z}_{n_j} \leq Z(G)$ mit $\text{ord}(g) = p$. Ist $k = 1$, so ist die Behauptung an dieser Stelle bewiesen. Sei also $k > 1$. Wegen $g \in Z(G)$ folgt $\langle g \rangle \trianglelefteq G$ mit

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

Nach Induktionsvoraussetzung existiert eine Untergruppe $U \leq G/\langle g \rangle$ mit $|U| = p^{k-1}$. Nach der Untergruppenkorrespondenz 5.7 existiert eine Untergruppe $V \leq G$ mit $\langle g \rangle \subseteq V$ und mit $V/\langle g \rangle = U$. Es ist $|V| = |U| \cdot |\langle g \rangle| = p^k$. □

Beweis 8.8 (des zweiten Sylowsatzes)**.** Sei $|G| = p^m \cdot q$ mit $\text{ggT}(p, q) = 1$. Sei $H \leq G$ mit $|H| = p^k$, für $k \leq m$, und sei $S \in \text{Syl}_p(G)$. Die Gruppe H operiert auf $X := G/S$ durch Multiplikation:

$$H \times X \to X, (h, gS) \mapsto hg \cdot S \ .$$

Nach Beispiel 7.3 ist diese Operation wohldefiniert. Es gilt:

$$|X| = \left| G/S \right| = [G : S] = q.$$

Nach 8.2 gilt $|X^H| \equiv |X| = q \pmod{p}$. Nach Voraussetzung ist $p \nmid q$, also folgt $p \nmid |X^H|$. Damit ist die Fixpunktmenge $X^H \neq \emptyset$, das heisst, es existiert $g \in G$ mit $gS \in X^H$. Es gilt also $hgS = gS$ für alle $h \in H$, und folglich ist $g^{-1}hg \in S$ für alle $h \in H$, also auch $H \subseteq gSg^{-1}$. □

Lemma 8.9. *Sei $|G| = p^m \cdot q$ mit $\text{ggT}(p, q) = 1$. Sei $S \in \text{Syl}_p(G)$. Sei H eine p-Untergruppe von G mit $H \subseteq \text{Stab}_G(S) := \{g \in G \mid gSg^{-1} = S\}$. Dann ist $H \subseteq S$.*

Beweis.

(i) Es ist $S \leq \text{Stab}(S)$. Da $gS = Sg$ für alle $g \in \text{Stab}(S)$ gilt, folgt auch $S \trianglelefteq \text{Stab}(S)$.

(ii) Nach Voraussetzung ist $H \leq \text{Stab}(S)$. Aus der Definition des Stabilisators folgt $HS = SH$, mit 2.8 gilt also $HS \leq \text{Stab}(S)$, und mit (i) auch $S \trianglelefteq HS$. Nach dem 1. Isomorphiesatz 5.5 (a) folgt

$$HS/S \simeq H/H \cap S \ .$$

Da H eine p-Gruppe ist, ist also auch HS/S eine p-Gruppe.

(iii) Da $G \geq HS \geq S$ gilt, folgt mit 2.12

$$[HS : S] \mid [G : HS][HS : S] = [G : S] = q \ .$$

Wegen $\text{ggT}(p, q) = 1$ folgt aber $p \nmid \frac{|HS|}{|S|}$. Nach (ii) ist HS eine p-Gruppe, also gilt $HS/S = \{1\}$, beziehungsweise $HS = S$, und damit $H \subseteq S$. □

Man spricht bei der Menge $\mathrm{Stab}_G(S) = \{g \in G \mid gSg^{-1}\}$ auch von einem *Normalisator*. Allgemeiner G operiert auf der Menge X aller Untergruppen von G durch Konjugation. Dann heisst $N_G(U) \coloneqq \{g \in G \mid gU = Ug\} = \mathrm{Stab}_G(U) \leq G$ *Normalisator* von U in G. Ist U Normalteiler in G, so ist $N_G(U) = G$. Man sieht leicht: U ist Normalteiler in $N_G(U)$, und ist $V \leq G$ mit $U \trianglelefteq V$, so ist $V \subseteq N_G(U)$. Der Normalisator $N_G(U)$ ist also die größte Untergruppe von G, in der U normal ist.

Beweis 8.10 (des dritten Sylowsatzes)**.**

(a) Sei $|G| = p^m q$ mit $\mathrm{ggT}(p, q) = 1$ und $n_p \coloneqq |\operatorname{Syl}_p(G)|$. Behauptung: $n_p \mid q$.

G operiert auf $X = \operatorname{Syl}_p(G)$ durch Konjugation. Sei $S \in \operatorname{Syl}_p(G)$. Aus dem zweiten Sylowsatz folgt, dass $X = \mathcal{O}_S$ die Bahn von S ist (d. h. die Operation ist transitiv). Nach 7.7 und 2.12 folgt

$$|X| = |\mathcal{O}_S| = [G : \mathrm{Stab}(S)] \mid [G : \mathrm{Stab}(S)][\mathrm{Stab}(S) : S] = [G : S] = q \ ,$$

also ist $|X| = n_p \mid q$.

(b) Sei $|G| = p^m q$ mit $\mathrm{ggT}(p, q) = 1$ und $n_p \coloneqq |\operatorname{Syl}_p(G)|$. Behauptung: $n_p \equiv 1 \pmod p$.

Sei $S \in \operatorname{Syl}_p(G)$. Die Gruppe S operiert auf $X = \operatorname{Syl}_p(G)$ durch Konjugation. Beachte, S ist ein Fixpunkt dieser Operation. Sei jetzt S' ein weiterer Fixpunkt unter dieser Operation, also $gS'g^{-1} = S'$ für alle $g \in S$. Dann ist $g \in \mathrm{Stab}_G(S')$ für alle $g \in S$ und somit $S \subseteq \mathrm{Stab}_G(S')$. Nach 8.9 folgt $S \subseteq S'$. Wegen $|S| = |S'|$ folgt $S = S'$. Somit ist S der einzige Fixpunkt dieser Operation, d. h. $|X^S| = 1$. Dies zeigt

$$n_p = |\operatorname{Syl}_p(G)| = |X| \overset{8.2}{\equiv} |X^S| = 1 \pmod p \ . \qquad \square$$

Mit den Sylowsätzen können wir die Struktur von Gruppen kleiner Ordnung genauer untersuchen.

Beispiel 8.11. Sei $|G| = 2p$ mit $2 \neq p$ prim. Dann ist $G \simeq C_{2p}$ oder $G \simeq D_{2p}$.

Beweis. (i) Nach 8.4 (3) gilt $n_p \mid 2 = q$ und $n_p \equiv 1 \pmod p$ und damit $n_p = 1$. Damit folgt $\operatorname{Syl}_p(G) = \{P\}$, mit 8.6 folgt $P \trianglelefteq G$ mit $C_p \simeq P = \langle x \rangle$, für ein Element $x \in G$.

(ii) Es gilt $|\operatorname{Syl}_2(G)| \geq 1$. Sei $Q \in \operatorname{Syl}_2(G)$, also $Q \simeq C_2$. Da „$C_2 \cap C_p = \{1\}$“, folgt $P \cap Q = \{1\}$. Damit existiert $y \in G \setminus P$ mit $\mathrm{ord}(y) = 2$. Da $|G| = 2p$ und $x^i \neq yx^j$ (sonst $y = x^{i-j} \in P$, Widerspruch), folgt $G = \{1, x, x^2, \ldots, x^{p-1}, y, yx, yx^2, \ldots, yx^{p-1}\}$. Nach Lagrange: $\mathrm{ord}(yx) \mid |G| = 2p$, also $\mathrm{ord}(yx) \in \{1, 2, p, 2p\}$.

(iii) Da $P \trianglelefteq G$ gilt, folgt $yxy^{-1} = x^i$ für ein i, also $(yx)^2 = yxyx = yxy^{-1}x = x^{i+1} \in P$. Induktiv folgt $(xy)^k \in P$ genau dann, wenn k gerade ist. Mit (ii) folgt $\mathrm{ord}(yx) \in \{2, 2p\}$.

(iv) Ist $\mathrm{ord}(yx) = 2p$, so gilt $G \simeq C_{2p}$. Sei also $\mathrm{ord}(yx) = 2$. Dann ist $yxyx = 1$ und damit $yxy^{-1} = x^{-1}$. Damit ist

$$G = \langle x, y \mid x^p = 1 = y^2, yxy^{-1} = x^{-1} \rangle = D_{2p} \ . \qquad \square$$

Das Beispiel zeigt insbesondere, dass es bis auf Isomorphie nur zwei Gruppen der Ordnung sechs, der Ordnung zehn, der Ordnung 14 etc gibt. Betrachten wir Gruppen mit kleiner Elementzahl, so haben wir bisher die folgende Klassifikation erreicht:

$\|G\|$	Isomorphietyp
1	$\{1\}$
2	C_2
3	C_3
4	$C_4, C_2 \times C_2 = V_4$
5	C_5
6	$C_6, D_6 = S_3$
7	C_7
8^*	$C_8, C_4 \times C_2, C_2 \times C_2 \times C_2, D_8, Q_8$
9^*	$C_9, C_3 \times C_3$
10	C_{10}, D_{10}
11	C_{11}
12^*	$C_{12}, C_2 \times C_6, D_{12}, A_4, U$
13	C_{13}
14	C_{14}, D_{14}
15^*	C_{15}

Es ist an dieser Stelle noch offen, dass es genau zwei nicht-abelsche Gruppen der Ordnung acht gibt, nämlich D_8 und Q_8. Wir kennen bereits vier Gruppen der Ordnung zwölf. Hier gibt es noch eine weitere Gruppe U mit zwölf Elementen:

$$U = \langle x, y \mid x^6 = 1, x^3 = y^2, yx = x^{-1}y \rangle.$$

Eine weitere Anwendung unserer bisherigen Sätze zeigt, dass Gruppen der Ordnung p^2 immer abelsch sind. Dies klassifiziert die Gruppen der Ordnung neun in der Tabelle oben. Hat eine Gruppe G die Ordnung $|G| = pq$, mit $p < q$ Primzahlen, so gilt: Ist p kein Teiler von $q-1$, dann ist G zyklisch (dies klassifiziert die Gruppen der Ordnung 15), andernfalls gibt es bis auf Isomorphie zwei Gruppen der Ordnung pq, einmal C_{pq}, und eine weitere nicht-abelsche Gruppe.

Kapitel 9

Auflösbare Gruppen

Eine Gruppe $G \neq \{1\}$ heißt *einfach*, falls sie nur Normalteiler $\{1\}$ und G hat. Anfang der 80er Jahre des letzten Jahrhunderts gelang die Klassifikation aller endlichen einfachen Gruppen. Ihr Beweis ist mehrere Bücher lang.

Theorem 9.1 (Klassifikation endlicher einfacher Gruppen)**.** *Die endlichen einfachen Gruppen sind:*

(1) Die zyklischen Gruppen C_p, für p Primzahl;

(2) A_n, für $n \geq 5$;

(3) endliche Gruppen vom Lie-Typ wie $\mathrm{PSL}_n(\mathbb{F}_q)$, für $n > 2$ und $q > 3$;

(4) 26 sogenannte sporadische Gruppen wie z. B. das Babymonster mit $\approx 4 \cdot 10^{33}$ Elementen und das Monster mit $\approx 8 \cdot 10^{53}$ Elementen.

In dieser Vorlesung wollen wir die Klasse aller endlichen auflösbaren Gruppen beschreiben. Wir werden sehen, dass diese Gruppen dadurch charakterisiert sind, dass sie aus einfachen zyklischen Gruppen zusammengeklebt sind. Was hier Zusammenkleben heisst, wird im Laufe dieser Vorlesung verdeutlicht. In den 60er Jahren zeigten Feit und Thompson, dass jede Gruppe ungerader Ordnung auflösbar ist. Auch diesen Satz können wir hier nicht beweisen, er sagt aber, dass es sich bei den auflösbaren Gruppen um eine grosse Klasse von Gruppen handelt.

Beispiel 9.2. A_n ist einfach für $n \geq 5$.

Beweis. (a) Sei $\{1\} \neq N \trianglelefteq A_n$. Wir zeigen $N = A_n$. Da $N \neq \{1\}$ ist, existiert $\mathrm{id} \neq \gamma \in N$. Entweder ist γ ein 3-Zykel oder die Zerlegung als Produkt disjunkter Zykel hat eine Gestalt wie in folgender Tabelle. Da N Normalteiler ist, ist mit $\gamma \in N$ auch $(\pi\gamma\pi^{-1})\gamma^{-1} \in N$ für alle $\pi \in A_n$.

Wir haben:

	γ	wähle $\pi \in A_n$	$\pi\gamma\pi^{-1}\gamma^{-1}$
(i)	$(a_1a_2a_3a_4\ldots)\cdots$	$(a_2a_1a_3)$	$(a_1a_3a_4)$
(ii)	$(a_1a_2a_3)(a_4a_5\ldots)\cdots$	$(a_3a_2a_4)$	$(a_1a_5a_2a_4a_3) \rightsquigarrow$ weiter in (i)
(iii)	$(a_1a_2)(a_3a_4)(a_5a_6)\cdots$	$(a_2a_1a_3)$	$(a_1a_4)(a_2a_3) \rightsquigarrow$ weiter in (iv)
(iv)	$(a_1a_2)(a_3a_4)$	$(a_2a_1a_5)$	$(a_1a_2a_5)$

Also enthält N mindestens einen 3-Zykel.

(b) Angenommen der 3-Zykel $(a_1a_2a_3)$ liegt im Normalteiler N. Wähle $\pi = (a_3a_4a_5) \in A_n$. Da $N \trianglelefteq A_n$ ist, folgt

$$\pi\gamma\pi^{-1} \overset{\text{Blatt 1}}{=} (\pi a_1, \pi a_2, \pi a_3) = (a_1a_2a_4) \in N.$$

Damit sind alle 3-Zykel der Form (a_1, a_2, x) mit $x \in \{1, \ldots, n\} \setminus \{a_1, a_2\}$ in N. Wiederholen des Arguments liefert, dass alle 3-Zykel in N liegen. Nach 3.9 ist

$$A_n = \langle \text{ Menge aller 3-Zykel } \rangle \subseteq N \subseteq A_n.$$

Also gilt $N = A_n$. □

Definition 9.3.

(a) Sei G eine Gruppe. Sei

$$\begin{aligned} G^{(0)} &:= G \\ G^{(1)} &:= G' = \langle [a, b] \mid a, b \in G \rangle \\ G^{(n)} &:= (G^{(n-1)})' \end{aligned}$$

für $n \geq 2$ mit $[a, b] := aba^{-1}b^{-1}$. Dabei heißt $G^{(n)}$ die *n-te Kommutatorgruppe*.

(b) Eine Gruppe G heißt *auflösbar*, falls es ein $n \in \mathbb{N}$ gibt mit $G^{(n)} = \{1\}$.

Beispiel 9.4.

(a) Eine Gruppe G ist abelsch genau dann, wenn $G' = \{1\}$. Ist also G abelsch, dann ist G auflösbar. Also sind A_1, A_2, A_3 auflösbar. Nach Aufgabe 5.1 ist $A_4' = V_4$ und damit $A_4^{(2)} = V_4' = \{1\}$. Also ist A_4 auflösbar.

(b) Sei G eine einfache auflösbare Gruppe. Dann ist $G \simeq C_p$, p prim.

Beweis. Nach 4.6 ist $G' \trianglelefteq G$, und da G nach Voraussetzung auflösbar ist, ist $G' \not\trianglelefteq G$. Da G einfach ist, folgt $G' = \{1\}$. Damit ist G abelsch. Da G einfach und abelsch ist, folgt $G \simeq C_p$, mit p Primzahl. □

(c) Mit (b) folgt nun, dass alle einfachen nicht-abelschen Gruppen nicht auflösbar sind. Insbesondere ist A_n für $n \geq 5$ nicht auflösbar, und $A_n' = A_n$. Nach Aufgabe 5.1 ist $S_n' = A_n$. Für $n \geq 5$ ist dann $S_n^{(i)} = A_n^{(i-1)} = A_n$ für alle $i \in \mathbb{N}$, also ist S_n nicht auflösbar.

Definition 9.5. Eine Folge von Untergruppen

$$\{1\} = G_0 \trianglelefteq G_1 \trianglelefteq \ldots \trianglelefteq G_n = G$$

mit $G_{i-1} \trianglelefteq G_i$ für $1 \leq i \leq n$ heißt *Normalreihe*. Hierbei heißt n *Länge* der Normalreihe. Die Gruppen G_i/G_{i-1} heißen *Faktoren* der Normalreihe von G. Unter Umständen werden die Faktoren auch als Subquotienten der Normalreihe bezeichnet.
Beachte: Jede Gruppe hat die Normalreihe $\{1\} \trianglelefteq G$, d. h. jede Gruppe besitzt mindestens eine Normalreihe.

Lemma 9.6. *Sei $N \trianglelefteq G$. Nach Aufgabe 5.1 ist G/N genau dann abelsch, wenn $G' \subseteq N$. Insbesondere ist G/G' abelsch.*

Proposition 9.7. *G ist genau dann auflösbar, wenn G eine Normalreihe mit abelschen Faktoren hat.*

Beweis. „⇒“: Sei G auflösbar, d. h. es existiert $r \in \mathbb{N}$ mit $G^{(r)} = \{1\}$. Nach 4.6 ist $G' \trianglelefteq G$. Also ist

$$\{1\} = G^{(r)} \trianglelefteq G^{(r-1)} \trianglelefteq G^{(r-2)} \trianglelefteq \ldots \trianglelefteq G' \trianglelefteq G$$

eine Normalreihe. Nach 9.6 sind alle Faktoren abelsch.
„⇐“:

(i) Sei $\{1\} = N_r \trianglelefteq N_{r-1} \trianglelefteq \ldots \trianglelefteq N_1 \trianglelefteq N_0 = G$ eine Normalreihe mit abelschen Faktoren. Wir zeigen $G^{(i)} \leq N_i$ für alle i. Dann folgt $G^{(r)} \leq N_r = \{1\}$, also $G^{(r)} = \{1\}$, d. h. G auflösbar.

(ii) Wir führen eine Induktion nach i durch: G/N_1 ist abelsch nach Voraussetzung. Mit 9.6 folgt, dass $G' = G^{(1)} \leq N_1$. Sei nun $G^{(i-1)} \leq N_{i-1}$ für $i \geq 2$. Nach Voraussetzung ist N_{i-1}/N_i abelsch, also folgt mit 9.6, dass $N'_{i-1} \leq N_i$. Somit folgt $G^{(i)} = (G^{(i-1)})' \leq N'_{i-1} \leq N_i$. □

Proposition 9.8.

(1) Untergruppen und homomorphe Bilder von auflösbaren Gruppen sind auflösbar. Insbesondere: Ist G auflösbar und $N \trianglelefteq G$, dann ist G/N auflösbar.

(2) Sei $N \trianglelefteq G$ und seien N und G/N auflösbar, dann ist G auflösbar.

Beweis.

(1) (a) Sei $H \leq G$ und G auflösbar mit $G^{(r)} = \{1\}$. Dann ist $H^{(r)} \leq G^{(r)} = \{1\}$, also H auflösbar.

(b) Sei $\varphi : G \to H$ ein Homomorphismus und sei G auflösbar mit $G^{(r)} = \{1\}$. Es ist $\varphi([a,b]) = [\varphi(a), \varphi(b)]$ für alle $a, b \in G$. Damit folgt

$$\varphi(G') = \varphi(\langle [a,b] \mid a,b \in G \rangle) = \langle [\varphi(a), \varphi(b)] \mid \varphi(a), \varphi(b) \in \varphi(G) \rangle = \varphi(G)' \,.$$

Induktiv folgt $\varphi(G)^{(r)} = \varphi(G^{(r)}) = \varphi(\{1\}) = \{1\}$. Somit ist $\varphi(G)$ auflösbar.
Da $\pi : G \to G/N, g \mapsto gN$ ein surjektiver Homomorphismus ist, folgt insbesondere, dass $G/N = \pi(G)$ auflösbar ist.

(2) Benutze die Untergruppenkorrespondenz 5.7 und 9.7: Seien $\{1\} = N_0 \trianglelefteq \ldots \trianglelefteq N_t = N$ und $\{1_{G/N}\} = N/N \trianglelefteq N_{t+1}/N \trianglelefteq \ldots \trianglelefteq N_{t+s}/N = G/N$ Normalreihen mit abelschen Faktoren. Dann folgt

$$\{1\} = N_0 \trianglelefteq N_1 \trianglelefteq \ldots \trianglelefteq N_t = N \trianglelefteq N_{t+1} \trianglelefteq N_{t+2} \trianglelefteq \ldots \trianglelefteq N_{t+s} = G$$

mit abelschen Faktoren N_i/N_{i-1} bzw. mit abelschen Faktoren

$$N_{t+i}/N_{t+i-1} \overset{5.5\,(b)}{\simeq} \left(N_{t+i}/N\right)\Big/\left(N_{t+i-1}/N\right) .$$

Nach 9.7 ist damit G auflösbar. □

Beispiel 9.9. Sei G eine p-Gruppe, dann ist G auflösbar.

Beweis. Induktion nach $|G|$. Nach 4.6 ist $Z(G) \trianglelefteq G$ und nach 8.6 ist $Z(G) \neq \{1\}$. Entweder ist G abelsch und damit auflösbar oder $\{1\} \neq Z(G) \trianglelefteq G$. Sei also jetzt G nicht abelsch. Nach Definition ist $Z(G)$ abelsch, also auflösbar. Die Quotientengruppe $G/Z(G)$ ist eine p-Gruppe mit echt kleinerer Ordnung als $|G|$. Nach Induktionsvoraussetzung ist also $G/Z(G)$ auflösbar. Mit 9.8 folgt, dass G auflösbar ist. □

Definition 9.10. Eine Normalreihe von G heißt *Kompositionsreihe von* G, falls alle ihre Faktoren einfach sind. Die Faktoren einer Kompositionsreihe heißen *Kompositionsfaktoren.*

Bemerkung 9.11. Jede endliche Gruppe hat eine Kompositionsreihe. Die Gruppe $\mathbb{Z}$ hat keine Kompositionsreihe.

Beweis. Wir beweisen die Aussage per Induktion nach $|G|$. Ist G einfach, dann ist $\{1\} \trianglelefteq G$ eine Kompositionsreihe. Andernfalls wähle N als maximalen Normalteiler in G, der nicht G selbst ist. Nach 5.7 folgt, dass G/N einfach ist. Nach Induktionsvoraussetzung hat N eine Kompositionsreihe $\{1\} = N_0 \trianglelefteq \ldots \trianglelefteq N_t = N$. Damit ist $\{1\} = N_0 \trianglelefteq N_1 \trianglelefteq \ldots \trianglelefteq N_t = N \trianglelefteq G$ eine Kompositionsreihe von G. □

Theorem 9.12 (Jordan-Hölder)**.** *Sei G eine endliche Gruppe. Dann sind alle Kompositionsreihen von G äquivalent, d. h. sie haben gleiche Länge und bis auf Isomorphie und Umsortierung die gleichen Kompositionsfaktoren.*

Beweisidee. Seien

$$\{1\} = G_0 \trianglelefteq \ldots \trianglelefteq G_r = G, \tag{9.1}$$
$$\{1\} = H_0 \trianglelefteq \ldots \trianglelefteq H_s = G \tag{9.2}$$

Kompositionsreihen von G. Mache Induktion nach r. Ist $r = 1$, so ist G einfach, und die Behauptung folgt. Sei also $r > 1$, und die Behauptung sei korrekt für alle Gruppen mit einer Kompositionsreihe der Länge $< r$. Wir haben zwei Fälle: Im ersten Fall ist $G_{r-1} = H_{s-1}$, dann hat G_{r-1} die Kompositionsreihe $\{1\} = H_0 \trianglelefteq \ldots \trianglelefteq H_{s-1} = G_{r-1}$. Nach Induktionsvoraussetzung ist $s - 1 = r - 1$, und die beiden Kompositionsreihen sind äquivalent. Also ist $r = s$ und die Behauptung folgt.
Im zweiten Fall ist $G_{r-1} \neq H_{s-1}$. Zeige $G_{r-1}H_{s-1} = G$. Die Gruppe $K \coloneqq G_{r-1} \cap H_{s-1}$ hat eine Kompositionsreihe der Länge t , die sich jeweils zu einer Kompositionsreihe von G_{r-1} beziehungsweise H_{s-1} der Länge $t+1$ fortsetzen lässt. Nach Induktionsvoraussetzung, zuerst angewandt auf G_{r-1}, beziehungsweise im zweiten Schritt angewandt auf H_{s-1}, folgt $r-1 = t+1$ und dann $r-1 = t+1 = s-1$, und die beiden Kompositionsreihen von G_{r-1} sowie die beiden Kompositionsreihen von H_{s-1} sind äquivalent. Die Kompositionsreihe von K lässt sich über G_{r-1} als auch über H_{s-1} zu einer Kompositionsreihe der Länge $t+2$ von G fortsetzen. Unter Benutzung des Isomorphiesatzes folgt, dass diese beiden Fortsetzungen äquivalent sind. Äquivalenz von Kompositionsreihen ist eine Äquivalenzrelation. Damit folgt, dass die Kompositionsreihen (9.1) und (9.2) äquivalent sind. □

Beispiel 9.13.

(1) Es ist $\{1\} \trianglelefteq A_3 \trianglelefteq S_3$ eine Kompositionsreihe mit Kompositionsfaktoren isomorph zu C_3 und C_2. Genauso ist $\{1\} \trianglelefteq \langle x^2 \rangle \trianglelefteq C_6 = \langle x \rangle$ und $\{1\} \trianglelefteq \langle x^3 \rangle \trianglelefteq C_6 = \langle x \rangle$. Also hat auch C_6 die Kompositionsfaktoren C_2 und C_3. Dieses Beispiel demonstriert auch den Satz von Jordan-Hölder.

(2) Eine Gruppe G mit Kompositionsreihe ist auflösbar genau dann, wenn ihre Kompositionsfaktoren alle isomorph zu Gruppen C_p mit p Primzahl sind.

Beweis. „$\Leftarrow$“: Seien alle Kompositionsfaktoren von G isomorph zu Gruppen C_p, mit p Primzahl. Da C_p abelsch ist, ist die Kompositionsreihe von G eine Normalreihe mit abelschen Faktoren, also ist G auflösbar.

„$\Rightarrow$“: Sei G auflösbar. Sei H/K ein Kompositionsfaktor von G, wobei $K \trianglelefteq H \leq G$. Da G auflösbar ist, ist nach 9.8 die Untergruppe H auflösbar, und damit ist auch H/K auflösbar. Folglich sind alle Kompositionsfaktoren von G einfache auflösbare Gruppen. Mit 9.4 folgt die Behauptung. □

Kapitel 10

Ringe und Ideale

In diesem Kapitel führen wir analog zur Gruppentheorie die Grundbegriffe der Ringtheorie ein: Ringe, Teilringe, Ringhomomorphismen und Ideale, in Analogie zu Gruppen, Untergruppen, Gruppenhomomorphismen und normalen Untergruppen.

Definition 10.1. Eine nichtleere Menge R mit binären Verknüpfungen

$$+ : R \times R \to R, (x, y) \mapsto x + y$$
$$\cdot : R \times R \to R, (x, y) \mapsto x \cdot y$$

heißt *Ring*, falls gilt:

(i) $(R, +)$ eine abelsche Gruppe mit Nullelement 0 und Inversen $-a$ von $a \in R$ ist;

(ii) die Multiplikation ist assoziativ und distributiv bezüglich der Addition, d. h. für alle $a, b, c \in R$ gilt

$$a(b + c) = ab + ac$$
$$(a + b)c = ac + bc \ ;$$

(iii) es existiert $0 \neq 1 \in R$ mit $a \cdot 1 = a = 1 \cdot a$ für alle $a \in R$.

Ein Ring heißt *kommutativ*, falls $ab = ba$ für alle $a, b \in R$ gilt. Schreibe $a^0 := 1$ und $a^n := a^{n-1} \cdot a$ für alle $n \in \mathbb{N}$.

Die Definition eines Ringes variiert je nach Quelle. Bisweilen werden auch Ringe ohne Einselement als Ringe bezeichnet, und auch in dieser Vorlesung ist die Benutzung des Begriffs nicht immer einheitlich. Fast immer bedeutet Ring aber Ring mit Einselement.

Bemerkung 10.2.

(a) Es ist $a \cdot 0 = 0 = 0 \cdot a$ für alle $a \in R$, denn $a \cdot 0 = a \cdot (0 + 0) = a \cdot 0 + a \cdot 0$ und somit, nach Addition des additiven Inversen $-a \cdot 0$, folgt $0 = a \cdot 0$.

(b) Angenommen, $1 = 0$ in einem Ring R. Dann ist $a = a \cdot 1 = a \cdot 0 = 0$ für alle $a \in R$, also $R = \{0\}$. Nach unserer Definition betrachten wir also $R = \{0\}$ nicht als Ring.

Definition 10.3. Sei R ein Ring und $S \subseteq R$. Dann ist S ein *Teilring* oder *Unterring* von R, $S \leq R$, falls:

(i) $1_R \in S$,

(ii) $a, b \in S \Rightarrow a - b \in S$,

(iii) $a, b \in S \Rightarrow a \cdot b \in S$.

Äquivalent hierzu ist: Teilmenge $S \subseteq R$ ist ein Ring, falls S mit den eingeschränkten Operationen von R ein Ring im Sinne von Definition 10.1 ist.

Beispiel 10.4.

(1) $\mathbb{Z} \leq \mathbb{Q} \leq \mathbb{R} \leq \mathbb{C}$ sind kommutative Ringe. Die natürlichen Zahlen $(\mathbb{N}, +, \cdot)$ bilden keinen Ring. Die geraden Zahlen $(2\mathbb{Z}, +, \cdot)$ bilden keinen Ring (aber einen Ring ohne Eins). Der Restklassenring $(\mathbb{Z}_n, +, \cdot)$ von $\mathbb{Z}$ modulo n ist ein kommutativer Ring.

(2) Sei R ein kommutativer Ring. Dann heißt

$$R[X] \coloneqq \{a_0 + a_1 X + \ldots + a_n X^n \mid n \in \mathbb{N}_0, a_i \in R, 0 \leq i \leq n\}$$

Polynomring in einer Variablen X über dem Ring R. Es gilt $R \leq R[X]$.

(3) Sei M eine abelsche Gruppe. Dann ist

$$\mathrm{End}(M) = \{\varphi : M \to M \mid \varphi \text{ Gruppenhomomorphismus}\}$$

ein Ring mit Einselement id und

$$\begin{aligned}(f + g)(x) &\coloneqq f(x) + g(x)\\ (f \circ g)(x) &\coloneqq f(g(x))\end{aligned}$$

für alle $f, g \in \mathrm{End}(M), x \in M$.

(4) Sei $d \in \mathbb{Z}$. Definiere

$$\mathbb{Z}[\sqrt{d}] \coloneqq \{a + b\sqrt{d} \mid a, b \in \mathbb{Z}\} \ ,$$

dann ist $\mathbb{Z}[\sqrt{d}] \leq \mathbb{C}$, denn

$$\begin{aligned}1 &= 1 + 0\sqrt{d} \in \mathbb{Z}[\sqrt{d}]\\ (a + b\sqrt{d}) \pm (c + r\sqrt{d}) &= \underbrace{(a \pm c)}_{\in\mathbb{Z}} + \underbrace{(b \pm r)}_{\in\mathbb{Z}}\sqrt{d} \in \mathbb{Z}[\sqrt{d}]\\ (a + b\sqrt{d})(c + r\sqrt{d}) &= \underbrace{(ac + bdr)}_{\in\mathbb{Z}} + \underbrace{(ar + bc)}_{\in\mathbb{Z}}\sqrt{d} \in \mathbb{Z}[\sqrt{d}] \ .\end{aligned}$$

$\mathbb{Z}[\sqrt{-1}] = \mathbb{Z}[i]$ heißt Ring der ganzen Gaußschen Zahlen.

(5) Sei R ein Ring. Dann heißt $Z(R) \coloneqq \{a \in R \mid \forall y \in R : ay = ya\}$ Zentrum von R. Es ist $Z(R) \leq R$.

Definition 10.5. Seien R, S Ringe. Eine Abbildung $\varphi : R \to S$ heißt *Homomorphismus* oder *Ringhomomorphismus*, falls

- $\varphi(1_R) = 1_S$,

- $\varphi(a+b) = \varphi(a) + \varphi(b)$,
- $\varphi(a \cdot b) = \varphi(a) \cdot \varphi(b)$,

für alle $a, b \in R$. Falls zusätzlich

- φ injektiv ist, heißt φ Monomorphismus.
- φ surjektiv ist, heißt φ Epimorphismus.
- φ bijektiv ist, heißt φ Isomorphismus.
- $R = S$ ist, heißt φ Endomorphismus.
- φ bijektiv und $R = S$ ist, heißt φ Automorphismus.

Ring R heißt *isomorph* zu Ring S, falls es einen Isomorphismus $\varphi : R \to S$ gibt; wir schreiben $R \simeq S$.

Bemerkung 10.6. Jeder Ringhomomorphismus $\varphi : R \to S$ ist ein Gruppenhomomorphismus bezüglich $+$. Also gilt nach 1.9, dass $\varphi(0) = 0$ und $\varphi(-a) = -\varphi(a)$ für alle $a \in R$. Definiere $\mathrm{Ker}(\varphi) \coloneqq \{a \in R \mid \varphi(a) = 0_S\}$. Dann ist nach 2.5 die Abbildung φ genau dann injektiv, wenn $\mathrm{Ker}(\varphi) = \{0_R\}$.

Beispiel 10.7.

(a) Seien R, S Ringe. Dann ist $R \times S$ ein Ring mit komponentenweiser Addition und Multiplikation:

$$(r_1, s_1) + (r_2, s_2) \coloneqq (r_1 + r_2, s_1 + s_2)$$
$$(r_1, s_1) \cdot (r_2, s_2) \coloneqq (r_1 \cdot r_2, s_1 \cdot s_2) \ .$$

Das Nullelement ist $0 = (0_R, 0_S)$ und das Einselement ist $1 = (1_R, 1_S)$. Nach unserer Definition ist $R \simeq R \times \{0\}$ kein Teilring von $R \times S$, denn $(1,1) \notin R \times \{0\}$, also ist $R \times \{0\}$ kein Teilring von $R \times S$.

(b) Sei $S \leq R$. Die Einbettung $i : S \to R, s \mapsto s$ ist ein Monomorphismus von Ringen.

(c) Sei K ein Körper. Dann ist $(M_n(K), +, \cdot)$ ein Ring. Sei V ein K-Vektorraum mit einer n-elementigen Basis B von V. Dann ist $\mathrm{End}_K(V) = \{f : V \to V \mid f \text{ linear}\}$ ein Ring mit

$$(f+g)(x) \coloneqq f(x) + g(x)$$
$$(f \circ g)(x) \coloneqq f(g(x))$$

für alle $f, g \in \mathrm{End}_K(V)$ und $x \in V$.

Dann ist $\psi = \psi_B : \mathrm{End}_K(V) \to M_n(K), T \mapsto M_B(T)$ ein Ringisomorphismus, wobei $M_B(T)$ die darstellende Matrix von T bezüglich der Basis B ist, denn:

$$\psi(\mathrm{id}) = I_n \ ,$$
$$\psi(S+T) = M_B(S+T) = M_B(S) + M_B(T) = \psi(S) + \psi(T) \ ,$$
$$\psi(S \circ T) = M_B(S \circ T) = M_B(S) \cdot M_B(T) = \psi(S) \cdot \psi(T) \ .$$

Die Abbildung ψ ist injektiv, da $\mathrm{Ker}(\psi) = \{0\}$. Sei $A \in M_n(K)$, dann ist $\psi(T_A) = A$, also ψ surjektiv, wobei T_A die lineare Abbildung ist, die durch Multiplikation mit A gegeben ist. Folglich ist ψ ein Isomorphismus.

Definition 10.8. Sei R ein Ring, und $(I,+) \leq (R,+)$ eine Untergruppe. Dann heißt

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

Wir schreiben $I \trianglelefteq R$ oder genauer $I \trianglelefteq_l R$ bzw. $I \trianglelefteq_r R$ bzw. $I \trianglelefteq_2 R$.

Beispiel 10.9.

(1) Die Ideale in $R \coloneqq \mathbb{Z}$ sind genau $I \coloneqq n\mathbb{Z}$ für $n \in \mathbb{N}_0$, siehe 2.4.

(2) Sei K ein Körper und $R \coloneqq M_2(K)$. Dann ist

$$I \coloneqq \left\{ \begin{pmatrix} a & 0 \\ b & 0 \end{pmatrix} \;\middle|\; a, b \in K \right\}$$

eine Untergruppe von $(R,+)$. Für alle $r \in R, i \in I$ ist $ri \in I$, aber

$$\begin{pmatrix} a & 0 \\ b & 0 \end{pmatrix} \begin{pmatrix} 1 & 1 \\ 0 & 0 \end{pmatrix} = \begin{pmatrix} a & a \\ b & b \end{pmatrix} \notin I \text{ für } (a,b) \neq (0,0) \; .$$

Somit ist I ein Links-, aber kein Rechtsideal.

(3) Sei R ein Ring. Dann ist $\{0\} \trianglelefteq R$ und $R \trianglelefteq R$. Für $a \in R$ ist $(a) = Ra \coloneqq \{ra \mid r \in R\}$ ein Linksideal in R. Es heißt das *von a erzeugte Ideal* in R und ist das kleinste Ideal in R, das a enthält. Analog definiert man das von a erzeugte Rechtsideal $(a) = aR \coloneqq \{ar \mid r \in R\}$. Ist der Ring R kommutativ, so gilt $aR = Ra$, und (a) ist ein zweiseitiges Ideal.

(4) Sei $\varphi : R \to S$ ein Ringhomomorphismus. Dann ist $\operatorname{Ker}(\varphi) \trianglelefteq R$ und $\operatorname{im}(\varphi) \leq S$ ein Teilring.

Bemerkung 10.10. Ist $I \trianglelefteq R, 1 \in I$, dann ist $r \cdot 1 = r \in I$ für alle $r \in R$. Also ist $I = R$.

Lemma 10.11. *Seien $I, J \trianglelefteq R$. Dann gilt:*

(a) $I \cap J \trianglelefteq R$;

(b) $I + J \trianglelefteq R$;

(c) $I \cdot J \trianglelefteq R$, wobei $I \cdot J \coloneqq \{\sum_{k=1}^{n} i_k j_k \mid n \in \mathbb{N}, i_k \in I, j_k \in J, 1 \leq k \leq n\}$;

(d) Ist $I \trianglelefteq_2 R$ und $S \leq R$ ein Teilring, dann ist $I + S \leq R$ ein Teilring.

Es gilt $I \cdot J \subseteq I \cap J$ (für geeignete Versionen des Idealbegriffs).

Beweis.

(b) Da $I, J \leq R$ Untergruppen sind, gilt nach 2.8, dass $I + J \leq R$ eine Untergruppe ist. Sei also $x \in I + J$. Dann existieren $i \in I, j \in J$ mit $x = i + j$. Sei $r \in R$. Dann folgt $rx = ri + rj \in I + J$, weil $I \trianglelefteq R, J \trianglelefteq R$. □

Definition 10.12.

(a) Definiere das von $a_1, \ldots, a_s \in R$ erzeugte Ideal

$$(a_1, \ldots, a_s) \coloneqq Ra_1 + Ra_2 + \ldots + Ra_s = \{r_1a_1 + \ldots + r_sa_s \mid r_i \in R\} \overset{10.11\,(b)}{\trianglelefteq} R \ .$$

Es ist das kleinste Ideal in R, das die Elemente $a_1, \ldots, a_s$ enthält.

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

Beispiel 10.13. Ideale in $\mathbb{Z}$ sind Hauptideale nach 10.9 und

$$\begin{aligned} n\mathbb{Z} + m\mathbb{Z} &= \mathrm{ggT}(n,m) \cdot \mathbb{Z} \ , \\ n\mathbb{Z} \cap m\mathbb{Z} &= \mathrm{kgV}(n,m) \cdot \mathbb{Z} \ , \\ n\mathbb{Z} \cdot m\mathbb{Z} &= nm\mathbb{Z} \ . \end{aligned}$$

Satz 10.14. *Sei R ein Ring, $I \trianglelefteq_2 R$. Dann ist ${}^{R}\!/_{I} \coloneqq \{r + I \mid r \in R\}$ die Quotientengruppe von $(R,+)$ modulo $(i,+)$ mit Addition $(r+I)+(s+I) \coloneqq (r+s)+I$ für alle $r, s \in R$, siehe 4.8. Definiere die Multiplikation*

$$\cdot : {}^{R}\!/_{I} \times {}^{R}\!/_{I} \to {}^{R}\!/_{I}$$

durch $(r+I)(s+I) \coloneqq rs+I$ für $r, s \in R$. Dann ist $({}^{R}\!/_{I}, +, \cdot)$ ein Ring, der Quotientenring von R modulo I. *Die Abbildung $\pi : R \to {}^{R}\!/_{I}, r \mapsto r + I$ ist ein Ringepimorphismus.*

Beweis.

(i) Die Multiplikation ist wohldefiniert: Sei $r + I = r' + I$ und $s + I = s' + I$, d. h. $r - r' \in I$ und $s - s' \in I$. Da $I \trianglelefteq_2 R$ gilt, folgt:

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

Also folgt $rs + I = r's' + I$.

(ii) Die Ringaxiome des Quotientenrings R/I folgen aus den Ringaxiomen von R. Zum Beispiel ist das Einselement $1_R + I$, denn $(1 + I) \cdot (r + I) = 1 \cdot r + I = r \cdot 1 + I = (r + I) \cdot (1 + I)$.

(iii) Nach 4.8 ist π ein Gruppenepimorphismus. Es gilt $\pi(1) = 1 + I$ und

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

für alle $r, s \in R$. Damit ist π ein Ringepimorphismus. □

Kapitel 11

Strukturs\"atze f\"ur Ringe

Sei R ein Ring. Wir beweisen in Analogie zur Gruppentheorie in Kapitel 5 die Strukturs\"atze f\"ur Ringe.

Theorem 11.1 (Idealkorrespondenz)**.** *Sei $\varphi : R \to S$ ein Ringhomomorphismus. Dann gilt:*

(a) Ist $J \trianglelefteq S$, so ist $\varphi^{-1}(J) \trianglelefteq R$. Insbesondere ist $\mathrm{Ker}(\varphi) = \varphi^{-1}(\{0\}) \trianglelefteq_2 R$.

(b) Ist φ surjektiv, dann existiert eine Bijektion zwischen den Idealen I von R mit $\mathrm{Ker}(\varphi) \subseteq I$ und den Idealen J von S durch $I \mapsto \varphi(I)$ mit Umkehrfunktion $J \mapsto \varphi^{-1}(J)$.

Beweis.

(a) Sei $J \trianglelefteq S$. Nach Definition ist $(J,+) \leq (S,+)$ eine Untergruppe. Nach 4.6 ist $\varphi^{-1}(J) \leq (R,+)$ eine Untergruppe. Sei $x \in \varphi^{-1}(J)$, d. h. $\varphi(x) \in J$. Sei $r \in R$. Da $J \trianglelefteq S$ ist, folgt

$$\varphi(r \cdot x) = \underbrace{\varphi(r)}_{\in S} \cdot \underbrace{\varphi(x)}_{\in J} \in J$$

und damit $r \cdot x \in \varphi^{-1}(J)$ für alle $x \in \varphi^{-1}(J), r \in R$. Also ist $\varphi^{-1}(J) \trianglelefteq R$.

(b) (i) Sei $I \trianglelefteq R$. Dann ist $(I,+) \leq (R,+)$ Untergruppe, und damit nach 2.6 auch $(\varphi(I),+) \leq (S,+)$ Untergruppe. Außerdem gilt:

$$S \cdot \varphi(I) \overset{\varphi \text{ surjektiv}}{=} \varphi(R) \cdot \varphi(I) \overset{\varphi \text{ Homom.}}{\subseteq} \varphi(\underbrace{R \cdot I}_{=I}) = \varphi(I) \ .$$

Also ist $\varphi(I) \trianglelefteq S$.

(ii)
- Sei $J \trianglelefteq S$. Nach Definition des Urbilds gilt $\varphi(\varphi^{-1}(J)) = J$.
- Sei $I \trianglelefteq R$. Ist $i \in I$, dann ist $i \in \varphi^{-1}(\varphi(i))$, also $I \subseteq \varphi^{-1}(\varphi(I))$.
  Sei $x \in \varphi^{-1}(\varphi(I))$, d. h. $\varphi(x) \in \varphi(I)$. Dann existiert $i \in I$ mit $\varphi(x) = \varphi(i)$.
  Somit ist $0 = \varphi(x) - \varphi(i) = \varphi(x - i)$, also $x - i \in \mathrm{Ker}(\varphi) \subseteq I$, also $x \in I$.
  Folglich gilt $I = \varphi^{-1}(\varphi(I))$. □

Bemerkung 11.2. Die Voraussetzung in 11.1, dass φ surjektiv ist, ist wichtig: Sei $i : \mathbb{Z} \hookrightarrow \mathbb{Q}, z \mapsto z$. Dann ist i ein (injektiver) Ringhomomorphismus. Sei $J \coloneqq m\mathbb{Z}$ mit $m \geq 2$. Dann ist $J = i(J) \not\trianglelefteq \mathbb{Q}$, denn $\frac{1}{2} \cdot m \notin J$.

Theorem 11.3 (Homomorphiesatz, Isomorphiesätze)**.**

(a) Sei $\varphi : R \to S$ ein Ringhomomorphismus. Dann ist

$$R/\mathrm{Ker}(\varphi) \simeq \mathrm{im}(\varphi)$$

ein Ringisomorphismus.

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

$$S + I/I \simeq S/S \cap I$$

ein Ringisomorphismus, wobei $S + I$ nach 10.11 ein Ring ist.

(c) Seien $I \subseteq J$ zweiseitige Ideale in R. Dann ist

$$\left(R/I\right)\Big/\left(J/I\right) \simeq R/J$$

ein Ringisomorphismus, wobei J/I nach 11.1 ein Ideal in R/I ist.

Beweis. Die Beweise dieser Aussagen folgen aus den Beweisen der entsprechenden Aussagen für Gruppen in 5.3 und 5.5, wobei zu prüfen bleibt, ob die in Kapitel 5 angegebenen Abbildungen auch Ringhomomorphismen sind. Wir demonstrieren dies an Aussage (a): Nach 5.3 ist $\overline{\varphi} : R/\mathrm{Ker}(\varphi) \to \mathrm{im}(\varphi), r + \mathrm{Ker}(\varphi) \mapsto \varphi(r)$ ein Gruppenisomorphismus. Außerdem ist $\overline{\varphi}(1 + \mathrm{Ker}(\varphi)) = \varphi(1) = 1$ und

$$\begin{aligned}\overline{\varphi}((a + \mathrm{Ker}(\varphi))(b + \mathrm{Ker}(\varphi))) &= \overline{\varphi}(ab + \mathrm{Ker}(\varphi) = \varphi(ab) = \varphi(a)\varphi(b) \\ &= \overline{\varphi}(a + \mathrm{Ker}(\varphi)) \cdot \overline{\varphi}(b + \mathrm{Ker}(\varphi)) \ ,\end{aligned}$$

also ist der in 5.3 angegebene Gruppenisomorphismus auch ein Ringisomorphismus. □

Beispiel 11.4. Sechs Professoren halten Vorlesungen zu den folgenden Zeiten:

Prof	Erste Vorlesung	Weitere Vorlesungen
A	Montag	alle 2 Tage
B	Dienstag	alle 3 Tage
C	Mittwoch	alle 4 Tage
D	Donnerstag	jeden Tag
E	Freitag	alle 6 Tage
F	Samstag	alle 5 Tage

Sonntags fallen Vorlesungen aus. Gibt es einen Sonntag, an dem alle Professoren ihre Vorlesung ausfallen lassen müssen? Wir übersetzen das gestellte Problem in die mathematische Sprache: Nummeriere die Tage durch die natürlichen Zahlen, angefangen bei 1 am Montag in der ersten Woche. Wir suchen $x \in \mathbb{N}$ mit $7 \mid x$ und

$$\begin{aligned}1 + 2x_1 &= x \\ 2 + 3x_2 &= x \\ 3 + 4x_3 &= x \\ 4 + 1x_4 &= x \\ 5 + 6x_5 &= x \\ 6 + 5x_6 &= x\end{aligned}$$

Dieses Kongruenzgleichungssystem enthält redundante Information: Professor D muss an jedem Sonntag seine Vorlesung ausfallen lassen. Die Zahl x ist Lösung der fünften Gleichung genau dann, wenn x Lösung der ersten beiden Gleichungen ist: $6 \mid x-5$ genau dann, wenn $2 \mid x-5 = x-1$ und $3 \mid x-5 = x-2$. Ist x Lösung der vierten Gleichung, so ist x auch eine Lösung der ersten Gleichung. Die erste, vierte und fünfte Gleichung sind also automatisch erfüllt, falls die anderen drei Gleichungen eine Lösung haben. Unser Problem reduziert sich also dazu, alle Lösungen $x \in \mathbb{N}$ des folgenden Kongruenzsystems zu finden:

$$\begin{aligned} x &\equiv 0 \pmod 7 \\ x &\equiv 2 \pmod 3 \\ x &\equiv 3 \pmod 4 \\ x &\equiv 1 \pmod 5 \ . \end{aligned}$$

Der Beweis der Surjektivität der Abbildung ψ im folgenden Theorem 11.5 beinhaltet die Strategie zur Lösung von Kongruenzgleichungen. Es sei dem Leser als Übungsaufgabe überlassen, Theorem 11.5 auf t paarweise *teilerfremde* zweiseitige Ideale $I_1, \ldots, I_t$ zu verallgemeinern. Hierbei heissen zweiseitige Ideale I_1 und I_2 eines Ringes R teilerfremd, falls $I_1 + I_2 = R$ ist.

Theorem 11.5. *Sei R ein Ring und $I_1, I_2 \trianglelefteq_2 R$ mit $I_1 + I_2 = R$. Dann ist*

$$R/I_1 \cap I_2 \simeq R/I_1 \times R/I_2$$

ein Ringisomorphismus, vermöge $(r + I_1 \cap I_2) \mapsto (r + I_1, r + I_2)$.

Beweis.

(a) Definiere $\psi : R \mapsto R/I_1 \times R/I_2$ durch $r \mapsto (r + I_1, r + I_2)$. Dann ist ψ ein Ringhomomorphismus. Aus $(0 + I_1, 0 + I_2) = 0 = \psi(r) = (r + I_1, r + I_2)$ folgt $\mathrm{Ker}(\psi) = I_1 \cap I_2$. Ist ψ surjektiv, dann folgt mit 11.3 (a), dass

$$R/I_1 \cap I_2 = R/\mathrm{Ker}(\varphi) \simeq \mathrm{im}(\varphi) = R/I_1 \times R/I_2 \ .$$

(b) Wir zeigen, dass ψ surjektiv ist: Sei $(b + I_1, a + I_2) \in R/I_1 \times R/I_2$. Da $R = I_1 + I_2$ ist, existieren $u_1 \in I_1$ und $u_2 \in I_2$ mit $1 = u_1 + u_2$.

Es gilt

$$\begin{aligned} \psi(u_1) &= (u_1 + I_1, u_1 + I_2) \\ &= (0 + I_1, (1 - u_2) + I_2) \\ &= (0 + I_1, 1 + I_2) \ . \end{aligned}$$

Analog folgt $\psi(u_2) = (1 + I_1, 0 + I_2)$. Da ψ ein Homomorphismus ist, folgt

$$\begin{aligned} \psi(au_1 + bu_2) &= \psi(a)\psi(u_1) + \psi(b)\psi(u_2) \\ &= (a + I_1, a + I_2)(0 + I_1, 1 + I_2) + (b + I_1, b + I_2)(1 + I_1, 0 + I_2) \\ &= (a \cdot 0 + I_1, a \cdot 1 + I_2) + (b \cdot 1 + I_1, b \cdot 0 + I_2) \\ &= (0 + I_1, a + I_2) + (b + I_1, 0 + I_2) \\ &= (b + I_1, a + I_2) \ . \end{aligned}$$

Also ist ψ surjektiv. □

Korollar 11.6. *Sei $m = \prod_{i=1}^{t} m_i$ eine Zerlegung in paarweise teilerfremde Zahlen m_i. Dann ist*

$$\mathbb{Z}/m\mathbb{Z} \simeq \mathbb{Z}/m_1\mathbb{Z} \times \ldots \times \mathbb{Z}/m_t\mathbb{Z} \ ,$$

vermöge $x + m\mathbb{Z} \mapsto (x + m_1\mathbb{Z}, \ldots, x + m_t\mathbb{Z})$. Insbesondere gibt es zu Zahlen $c_1, \ldots, c_t \in \mathbb{Z}$ eine eindeutige Zahl x modulo m mit

$$x \equiv c_i \pmod{m_i}, \qquad 1 \leq i \leq t \ .$$

Beweis. Induktion nach t unter Verwendung von 11.5. Da die m_i paarweise teilerfremd sind, folgt $\mathrm{ggT}(\prod_{i=1}^{t-1} m_i, m_t) = 1$. Es gilt:

$$m_1 \cdots m_{t-1}\mathbb{Z} \cap m_t\mathbb{Z} \overset{10.13}{=} \mathrm{kgV}(\prod_{i=1}^{t-1} m_i, m_t)\mathbb{Z} = m\mathbb{Z} \ , \tag{11.1}$$

$$m_1 \cdots m_{t-1}\mathbb{Z} + m_t\mathbb{Z} \overset{10.13}{=} \mathrm{ggT}(\prod_{i=1}^{t-1} m_i, m_t)\mathbb{Z} = \mathbb{Z} \ . \tag{11.2}$$

Nach (11.2) ist die Voraussetzung von Theorem 11.5 erfüllt. Es folgt also

$$\begin{aligned} \mathbb{Z}/m\mathbb{Z} &\overset{(11.1)}{=} \mathbb{Z}/m_1 \cdots m_{t-1}\mathbb{Z} \cap m_t\mathbb{Z} \overset{11.5}{\simeq} \mathbb{Z}/m_1 \cdots m_{t-1}\mathbb{Z} \times \mathbb{Z}/m_t\mathbb{Z} \\ &\overset{\text{Ind Vor}}{\simeq} \mathbb{Z}/m_1\mathbb{Z} \times \ldots \times \mathbb{Z}/m_t\mathbb{Z} \ . \end{aligned}$$

□

Bemerkung 11.7. Seien $a, b \in \mathbb{Z}$ mit $b \neq 0$. Ohne Einschränkung sei $a > b$. Der euklidische Algorithmus besteht aus wiederholter Division mit Rest: Setze $a =: r_{-2}, b =: r_{-1}$,

$$\begin{aligned} a &= q_0 \cdot b + r_0, & 0 \leq r_0 < b \\ b &= q_1 \cdot r_0 + r_1, & 0 \leq r_1 < r_0 \\ r_0 &= q_2 \cdot r_1 + r_2, & 0 \leq r_2 < r_1 \\ &\vdots \\ r_{n-2} &= q_n r_{n-1} + r_n, & 0 \leq r_n < r_{n-1} \end{aligned}$$

mit $r_n = 0$. Dann ergibt sich aus den obigen Gleichungen:

$$\mathrm{ggT}(a, b) = \mathrm{ggT}(b, r_0) = \mathrm{ggT}(r_0, r_1) = \ldots = \mathrm{ggT}(r_{n-1}, r_n) = \mathrm{ggT}(r_{n-1}, 0) = r_{n-1} \ .$$

Wende den euklidischen Algorithmus rückwärts an:

$$\begin{aligned} \mathrm{ggT}(a, b) &= r_{n-1} = r_{n-3} - q_{n-1} r_{n-2} \\ &= r_{n-3} - q_{n-1}(r_{n-4} - q_{n-2} r_{n-3}) \\ &= \underbrace{(-q_{n-1})}_{\in \mathbb{Z}} r_{n-4} + \underbrace{(1 + q_{n-1} q_{n-2})}_{\in \mathbb{Z}} r_{n-3} \\ &\vdots \\ &= x \cdot r_{-2} + y \cdot r_{-1} \\ &= x \cdot a + y \cdot b \end{aligned}$$

mit $x, y \in \mathbb{Z}$. Dies ist die Aussage des Lemmas von Bézout: Ist $d = \mathrm{ggT}(a, b)$, dann existieren $x, y \in \mathbb{Z}$ mit $d = xa + yb$.

Beispiel 11.8. Wir machen ein Beispiel zum Euklidischen Algorithmus. Es ist $\mathrm{ggT}(5,7) = 1$. Es ist

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

also

$$\begin{aligned} 1 &= 5 - 2 \cdot 2 \\ &= 5 - 2(7-5) \\ &= \underbrace{(-2) \cdot 7}_{\in 7\mathbb{Z}} + \underbrace{3 \cdot 5}_{\in 5\mathbb{Z}} \ . \end{aligned}$$

Beispiel 11.9.

(a) Finde $x \in \mathbb{Z}$ mit

$$\begin{aligned} x &\equiv 0 \pmod 7 \\ x &\equiv 1 \pmod 5 \ . \end{aligned}$$

Wegen $\mathrm{ggT}(5,7) = 1$ gilt $5\mathbb{Z} + 7\mathbb{Z} = \mathbb{Z}$. Schreibe $1 = u_1 + u_2 = 3 \cdot 5 + (-2) \cdot 7 = 15 + (-14) \in 5\mathbb{Z} + 7\mathbb{Z}$. Nach 11.5 ist

$$\begin{aligned} x &\equiv 0 \cdot 15 + 1 \cdot (-14) \pmod{35} \\ &\equiv 21 \pmod{35} \ . \end{aligned}$$

(b) Finde $x \in \mathbb{Z}$ mit

$$\begin{aligned} x &\equiv 2 \pmod 3 \\ x &\equiv 3 \pmod 4 \ . \end{aligned}$$

Da $\mathrm{ggT}(3,4) = 1$, können wir 11.5 anwenden: $1 = (-3) + 4 =: u_1 + u_2$, also $x \equiv 2 \cdot 4 + 3 \cdot (-3) \equiv -1 \equiv 11 \pmod{12}$.

(c) Finde $x \in \mathbb{Z}$ mit

$$\begin{aligned} x &\equiv 21 \pmod{35} \\ x &\equiv 11 \pmod{12} \ . \end{aligned}$$

Es ist $\mathrm{ggT}(35,12) = 1$. Es ist

$$\begin{aligned} 35 &= 2 \cdot 12 + 11 \\ 12 &= 1 \cdot 11 + 1 \ . \end{aligned}$$

Damit folgt

$$\begin{aligned} 1 &= 12 - 11 \\ &= 12 - (35 - 2 \cdot 12) \\ &= \underbrace{(-35)}_{\in 35\mathbb{Z}} + \underbrace{3 \cdot 12}_{\in 12\mathbb{Z}} \ . \end{aligned}$$

Mit 11.5 folgt

$$\begin{aligned} x &\equiv 21 \cdot 36 + 11 \cdot (-35) \\ &\equiv 371 \pmod{420} , \end{aligned}$$

da $420 = 12 \cdot 35$ ist. Am Tag 371, einem Sonntag, müssen also alle sechs Professoren in Beispiel 11.4 zum ersten mal ihre Vorlesung ausfallen lassen.

Kapitel 12

Einheiten und Nullteiler

Definition 12.1. Sei R ein Ring.

(a) Definiere $R^\times := \{a \in R \mid \exists b \in R : ab = 1 = ba\}$. Dann ist $(R^\times, \cdot)$ eine Gruppe, genannt *Gruppe der Einheiten/Einheitengruppe in* R. Ein Element $a \in R^\times$ heißt *Einheit* oder *invertierbar*.

(b) Ein Ring mit $R^\times = R \setminus \{0\}$ heißt *Schiefkörper*. Ein kommutativer Schiefkörper heißt *Körper*.

Die Einheitengruppe ist eine Gruppe: Seien $x, y \in R^\times$, dann ist $x\tilde{x} = 1 = \tilde{x}x$, also $x^{-1} \in R^\times$, und es ist $y\tilde{y} = 1 = \tilde{y}y$; wegen $xy\tilde{y}\tilde{x} = x \cdot 1 \cdot \tilde{x} = 1 = \tilde{y} \cdot 1 \cdot y = \tilde{y}\tilde{x}xy$ ist auch $xy \in R^\times$. Ausserdem ist natürlich das Einselement 1 in $R^\times$.

Bemerkung 12.2. Sei R ein kommutativer Ring. Dann ist äquivalent:

(a) R ist Körper (d. h. $R^\times = R \setminus \{0\}$).

(b) R hat nur zwei Ideale: $\{0\}$ und R.

(c) Für jeden Ring S und jeden Ringhomomorphismus $\varphi : R \to S$ ist φ injektiv.

Angenommen R ist ein Körper. Sei $0 \neq I$ ein Ideal in R. Dann existiert $0 \neq x \in I$. Da x invertierbar ist, folgt $1 = x^{-1}x \in I$, also ist $I = R$. Dies zeigt (a) impliziert (b). Angenommen R hat nur zwei Ideale. Es ist $\varphi(1) = 1$, also ist $\mathrm{Ker}(\varphi) \neq R$ ein Ideal in R, also ist $\mathrm{Ker}(\varphi) = 0$, und die Abbildung φ ist injektiv. Dies zeigt (b) impliziert (c). Es ist eine Übungsaufgabe für den Leser, die noch fehlende Implikation (c) impliziert (a) zu zeigen.

Beispiel 12.3.

(1) Es gilt $\mathbb{Z}^\times = \{1, -1\}$. Ist K ein Körper, dann ist $K^\times = K \setminus \{0\}$, zum Beispiel ist $\mathbb{Q}^\times = \mathbb{Q} \setminus \{0\}$.

(2) Es ist $\mathbb{Z}[i]^\times = \{1, -1, i, -i\}$: Sei $w \in \mathbb{Z}[i]^\times$, dann existiert $z \in \mathbb{Z}[i]$ mit $1 = wz$. Komplex konjugieren ergibt $1 = 1 \cdot 1 = wz\overline{wz} = |w|^2 \cdot |z|^2$. Auf der rechten Seite der letzten Gleichung steht ein Produkt positiver ganzer Zahlen. Damit folgt:

$$1 = |w|^2 = (x + iy)(x - iy) = x^2 + y^2 \text{ mit } x, y \in \mathbb{Z},$$

also ist $x = \pm 1, y = 0$ oder $x = 0, y = \pm 1$.

(3) Ist K ein Körper, dann ist $M_n(K)^\times = \mathrm{GL}_n(K)$.

(4) Seien R, S Ringe. Dann gilt $(R \times S)^\times = R^\times \times S^\times$, denn:

$$\begin{aligned}(x,y) \in (R\times S)^\times &\Leftrightarrow \exists(\tilde{x},\tilde{y}) \in R\times S : (x,y)(\tilde{x},\tilde{y}) = (1,1) = (\tilde{x},\tilde{y})(x,y)\\ &\Leftrightarrow \exists(\tilde{x},\tilde{y}) \in R\times S : (x\tilde{x}, y\tilde{y}) = (1,1) = (\tilde{x}x, \tilde{y}y)\\ &\Leftrightarrow \exists(\tilde{x},\tilde{y}) \in R\times S : x\tilde{x} = 1 = \tilde{x}x, y\tilde{y} = 1 = \tilde{y}y\\ &\Leftrightarrow (x,y) \in R^\times \times S^\times \ .\end{aligned}$$

(5) Sei $n \geq 2$ und $\mathbb{Z}_n \coloneqq {}^{\mathbb{Z}}\!/_{n\mathbb{Z}} = \{\overline{0}, \ldots, \overline{n-1}\}$ mit $\overline{a} \coloneqq a + n\mathbb{Z}$. Dann ist

$$a + n\mathbb{Z} \in \mathbb{Z}_n^\times \Leftrightarrow \mathrm{ggT}(a,n) = 1 \ .$$

Insbesondere ist $\mathbb{Z}_n$ genau dann ein Körper, wenn $\mathbb{Z}_n^\times = \mathbb{Z}_n \setminus \{0\}$. Dies ist äquivalent dazu, dass $\mathrm{ggT}(a,n) = 1$ für $1 \leq a \leq n-1$, also dazu, dass n eine Primzahl ist.

Beweis.

(a) Sei $\mathrm{ggT}(a,n) = 1$. Nach dem Lemma von Bézout existieren $x, y \in \mathbb{Z}$ mit $ax + ny = 1$. Es folgt

$$1 + n\mathbb{Z} = ax + ny + n\mathbb{Z} = ax + n\mathbb{Z} = (a + n\mathbb{Z})(x + n\mathbb{Z}) \ ,$$

also ist $(a + n\mathbb{Z})$ eine Einheit in $\mathbb{Z}_n^\times$.

(b) Sei $a + n\mathbb{Z} \in \mathbb{Z}_n^\times$. Dann existiert $b \in n\mathbb{Z}$ mit $(a + n\mathbb{Z})(b + n\mathbb{Z}) = 1 + n\mathbb{Z}$, also $ab + n\mathbb{Z} = 1 + n\mathbb{Z}$. Es folgt $1 \in ab + n\mathbb{Z}$ und damit $1 = ab + nx$ für ein $x \in \mathbb{Z}$. Dann folgt aber $\mathrm{ggT}(a,n) = 1$. □

Bemerkung 12.4. Definiere die Eulersche ϕ-Funktion $\phi : \mathbb{N} \to \mathbb{N}, m \mapsto \phi(m) \coloneqq |\mathbb{Z}_m^\times|$. Diese Funktion ist ein Beispiel einer sogenannten zahlentheoretischen Funktion (siehe definierende Eigenschaft (b) unten). Es gilt:

(a) $m = \sum_{d|m} \phi(d)$.

(b) Sei $m = m_1 m_2$ mit $\mathrm{ggT}(m_1, m_2) = 1$. Dann ist $\phi(m) = \phi(m_1) \cdot \phi(m_2)$.

(c) Es gilt

$$\phi(m) = m \cdot \prod_{\substack{p|m \\ p \text{ prim}}} \left(1 - \frac{1}{p}\right) \ .$$

Beispiel: Wir berechnen kleine Werte der ϕ-Funktion per Hand. Zum Beispiel hat $\mathbb{Z}_4^\times$ genau die Einheiten $1, 3$ nach 12.3. Es gilt:

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

Beweis.

(a) (i) Sei $G = \langle g \rangle$ eine zyklische Gruppe der Ordnung m. Dann ist

$$\operatorname{ord}(g^i) \overset{3.5}{=} \frac{\operatorname{ord}(g)}{\operatorname{ggT}(m,i)} = \frac{m}{\operatorname{ggT}(m,i)} \ .$$

Folglich ist jedes Element g^i mit $\operatorname{ggT}(m,i) = 1$ Erzeuger von G. Die Anzahl der Erzeuger von G ist also $|\mathbb{Z}_m^\times| = \phi(m)$.

(ii) Sei $d \mid m$. Nach Theorem 3.7 (b) gibt es genau eine Untergruppe $C_d \leq G$ mit d Elementen. Da C_d zyklisch ist, hat C_d genau $\phi(d)$ viele Elemente der Ordnung d. Umgekehrt, jedes Element aus G der Ordnung d liegt in C_d. Ist $g \in G$, dann ist $\operatorname{ord}(g) \mid |G| = m$. Außerdem ist $G = \dot{\bigcup}_{d|m}\{\text{Elemente in } G \text{ der Ordnung } d\}$. Also ist $m = |G| = \sum_{d|m} \phi(d)$.

(b) Nach 11.6 gilt $\mathbb{Z}_{m_1 m_2} \simeq \mathbb{Z}_{m_1} \times \mathbb{Z}_{m_2}$ für teilerfremde Zahlen m_1 und m_2. Damit folgt

$$\mathbb{Z}_{m_1 m_2}^\times \simeq (\mathbb{Z}_{m_1} \times \mathbb{Z}_{m_2})^\times \overset{12.3}{=} \mathbb{Z}_{m_1}^\times \times \mathbb{Z}_{m_2}^\times$$

und daher $\phi(m_1 m_2) = \phi(m_1) \cdot \phi(m_2)$.

(c) (i) Sei p eine Primzahl und $n \in \mathbb{N}$. Sei $X \coloneqq \{1, 2, \ldots, p-1, p, p+1, \ldots, 2p, \ldots, p^n\}$. Streiche alle Vielfachen von p aus X. Die neue Menge enthält nur Zahlen teilerfremd zu p^n. Damit folgt $\phi(p^n) = p^n - p^{n-1} = p^n \left(1 - \frac{1}{p}\right)$.

(ii) Sei $m = \prod_{i=1}^t p_i^{n_i}$ eine Primfaktorzerlegung mit paarweise verschiedenen p_i, $n_i \in \mathbb{N}$. Dann folgt

$$\begin{aligned} \phi(m) &\overset{\text{(b)}}{=} \prod_{i=1}^t \phi(p_i^{n_i}) \overset{\text{(i)}}{=} \prod_{i=1}^t p_i^{n_i} \left(1 - \frac{1}{p_i}\right) \\ &= m \prod_{i=1}^t \left(1 - \frac{1}{p_i}\right) = m \prod_{p|m} \left(1 - \frac{1}{p}\right) \ . \end{aligned}$$

□

Bemerkung 12.5. Wir interessieren uns dafür, den Ring $\mathbb{Z}$ genauer zu verstehen, und seine Eigenschaften zu verallgemeinern.

(a) Es gelten die folgenden Rechenregeln in $\mathbb{Z}$:

(i) $ab = 0 \Rightarrow a = 0$ oder $b = 0$.

(ii) $ax = bx \Rightarrow a = b$ (für $x \neq 0$).

Wieso gelten diese Rechenregeln? Der Ring $\mathbb{Z}$ lässt sich in den Körper $\mathbb{Q}$ der rationalen Zahlen einbetten. Aus den Körperaxiomen folgen dann die obigen Rechenregeln:

(b) Sei K ein Körper.

(i) Sei $ab = 0$. Ist $b \neq 0$, so existiert $b^{-1} \in K$. Dann folgt $0 = 0b^{-1} = abb^{-1} = a$. Insgesamt folgt $a = 0$ oder $b = 0$.

(ii) Sei $ax = bx$. Angenommen $x \neq 0$, dann existiert $x^{-1} \in K$ und es folgt $a = axx^{-1} = bxx^{-1} = b$.

(c) Es gibt Ringe, in denen diese Regeln nicht gelten: Sei $R = \mathbb{Z}_6$. Dann ist

(i) $\overline{2} \cdot \overline{3} = \overline{0}$, aber $\overline{2} \neq \overline{0}, \overline{3} \neq \overline{0}$.

(ii) $\overline{2} \cdot \overline{2} = \overline{5} \cdot \overline{2}$, aber $\overline{2} \neq \overline{5}$.

Definition 12.6.

(a) Ein Element $0 \neq a \in R$ heißt *Nullteiler*, falls es $0 \neq b \in R$ mit $ab = 0$ oder $ba = 0$ gibt.

(b) Ein kommutativer Ring R ohne Nullteiler heißt *Integritätsbereich* (IB).

Ob das Nullelement eines Ringes als Nullteiler zugelassen wird, ist kulturell unterschiedlich. Lässt man Null als Nullteiler zu, so ist ein Integritätsbereich ein kommutativer Ring R, in dem es außer Null keine Nullteiler gibt.

Beispiel 12.7.

(1) Nach 12.5 ist jeder Körper K ein Integritätsbereich. Sei R ein Integritätsbereich und $R' \leq R$ ein Teilring, dann ist auch R' ein Integritätsbereich. Zum Beispiel ist $\mathbb{Z}[\sqrt{d}] \leq \mathbb{C}$ ein Teilring, also ist $\mathbb{Z}[\sqrt{d}]$ ein Integritätsbereich.

(2) Sei R ein endlicher Integritätsbereich. Dann ist R ein Körper.

Beweis. Sei $0 \neq x \in R$. Sei $l_x : R \to R, r \mapsto x \cdot r$ Linksmultiplikation mit x. Sei $xr = xs$, dann folgt $0 = xr - xs = x(r - s)$. Da $x \neq 0$ ist und es in R keine Nullteiler gibt, folgt $r - s = 0$, also $r = s$. Daher ist l_x injektiv. Da R endlich ist und $l_x : R \hookrightarrow R$, ist l_x auch surjektiv. Da $1 \in R$ ist, existiert $r \in R$ mit $l_x(r) = 1$. Damit ist $xr = 1$, also x invertierbar für alle $x \in R \setminus \{0\}$. □

(3) Sei $a \in R^\times$ eine Einheit, dann ist a kein Nullteiler: Sei $ab = 0$. Da $a \in R^\times$ ist, existiert $a^{-1} \in R$. Damit ist $b = a^{-1}ab = a^{-1} \cdot 0 = 0$. Somit ist a kein Nullteiler.

(4) Ist K ein Körper und $n \geq 2$, dann hat $M_n(K)$ Nullteiler. Zum Beispiel für $n = 2$:

$$\begin{pmatrix} 0 & x \\ 0 & y \end{pmatrix} \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix} = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix} .$$

Allgemein sind alle $E_{ij} \in M_n(K)$ Nullteiler.

(5) Seien R, S Ringe (z. B. Integritätsbereiche). Dann hat der Ring $R \times S$ Nullteiler: $(r, 0)(0, s) = (0, 0)$ für $r \neq 0, s \neq 0$.

(6) Sei $R = \mathbb{Z}_n$ mit $n \geq 2$. Dann ist $0 + n\mathbb{Z} \neq a + n\mathbb{Z}$ ein Nullteiler genau dann, wenn $\mathrm{ggT}(a, n) > 1$.

Beweis. Sei $d := \mathrm{ggT}(a, n) > 1$. Dann folgt $d \mid a$ und $d \mid n$. Also existieren $x, y \in \mathbb{Z}$ mit $dx = a$ und $dy = n$. Insbesondere ist hierbei $1 < y < n$. Dann ist $nx = dyx = dx \cdot y = ay$. Damit folgt $0 + n\mathbb{Z} = nx + n\mathbb{Z} = ay + n\mathbb{Z} = (a + n\mathbb{Z})(y + n\mathbb{Z})$. Da $y + n\mathbb{Z} \neq 0$ gilt, ist $0 + n\mathbb{Z} \neq a + n\mathbb{Z}$ ein Nullteiler. Die Rückrichtung folgt mit (3). □

Bemerkung 12.8. Wir wissen, dass $\mathbb{Z} \hookrightarrow \mathbb{Q}$ ein Teilring ist. Wir imitieren dies für Integritätsbereiche. Sei R ein Integritätsbereich. Definiere eine Relation $\sim$ auf $R \times R \setminus \{0\}$ durch:

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

Dann ist $\sim$ eine Äquivalenzrelation. Zum Beispiel sei $(a, b) \sim (r, s)$ und $(r, s) \sim (x, y)$. Dann folgt $br = as$ und $sx = ry$. Wir wollen $(a, b) \sim (x, y)$, d. h. $bx = ay$ zeigen. Es ist $bry = asy$ und $sxb = ryb$, also auch $say = sbx$. Da $s \neq 0$ und R Integritätsbereich ist, folgt $ay = bx$, d. h. $\sim$ ist transitiv. Schreibe $\frac{r}{s} := [(r, s)]$ für die Äquivalenzklasse von (r, s). Es ist $\frac{r}{s} = \frac{x}{y}$ genau dann, wenn $sx = ry$.

Theorem 12.9. *Sei R ein Integritätsbereich. Sei* $\mathrm{Quot}(R) := \{\frac{r}{s} \mid r \in R, s \in R \setminus \{0\}\}$. *Definiere*

$$\frac{r}{s} + \frac{x}{y} := \frac{ry + sx}{sy}$$

und

$$\frac{r}{s} \cdot \frac{x}{y} := \frac{rx}{sy} \ .$$

Dann ist $(\mathrm{Quot}(R), +, \cdot)$ *ein Körper. Die Abbildung* $\varepsilon : R \to \mathrm{Quot}(R), r \mapsto \frac{r}{1}$ *ist ein Monomorphismus von Ringen.*

Beweis.

(a) Die Operationen sind wohldefiniert: Sei $\frac{a}{b} = \frac{a'}{b'}$ und $\frac{x}{y} = \frac{x'}{y'}$. Dann folgt $(a, b) \sim (a', b')$ und $(x, y) \sim (x', y')$, also nach Definition $ba' = ab'$ und $yx' = xy'$. Es folgt für die Multiplikation:

$$ab'xy' = ba'yx'$$

und damit auch

$$(ax)(b'y') = (by)(a'x') \ .$$

Nach Definition von $\sim$ folgt $(ax, by) \sim (a'x', b'y')$, also

$$\frac{a}{b} \cdot \frac{x}{y} = \frac{ax}{by} = \frac{a'x'}{b'y'} = \frac{a'}{b'} \cdot \frac{x'}{y'} \ .$$

Ähnlich folgt, dass auch die Addition wohldefiniert ist.

(b) Die Ringaxiome zu prüfen, sei dem Leser überlassen. Das Nullelement in $\mathrm{Quot}(R)$ ist $\frac{0}{1}$, das Einselement ist $\frac{1}{1}$; das additive Inverse zu $\frac{a}{b}$ ist $\frac{-a}{b}$; das multiplikative Inverse zu $\frac{a}{b}$ ist $\frac{b}{a}$ für $a, b \neq 0$. Es sei dem Leser überlassen, zu prüfen, dass ϵ ein Ringhomomorphismus ist. Ist $\frac{r}{1} = \frac{s}{1}$, so folgt $r = s$, also ist die Abbildung ϵ injektiv. □

Beispiel 12.10. Es ist $\mathrm{Quot}(\mathbb{Z}) = \mathbb{Q}$. Ist K ein Körper, dann ist $\mathrm{Quot}(K) \simeq K$. Der Polynomring $K[X]$ über einem Körper K ist ein Integritätsbereich nach 13.6. Der *Körper* $K(X)$ *der rationalen Funktionen* ist definiert durch

$$K(X) = \mathrm{Quot}(K[X]) = \left\{ \frac{f}{g} \;\middle|\; f \in K[X], g \in K[X] \setminus \{0\} \right\} \ .$$

Kapitel 13

Polynomringe

Definition 13.1. Sei R ein Ring. Der *Polynomring $R[X]$ in einer Variablen X* besteht aus allen formalen Summen

$$f \coloneqq \sum_{i=0}^{n} a_i X^i, \quad n \in \mathbb{N}_0, a_i \in R \text{ für } 1 \leq i \leq n \ .$$

Wir nennen f ein *Polynom*, und schreiben $f = \sum_{i \geq 0} a_i X^i$; hierbei setzen wir $a_i = 0$ für alle $i \geq n+1$. Definiere auf $R[X]$ Addition und Multiplikation von Polynomen durch:

$$\left(\sum_{i \geq 0} a_i X^i\right) + \left(\sum_{i \geq 0} b_i X^i\right) \coloneqq \sum_{i \geq 0} (a_i + b_i) X^i$$
$$\left(\sum_{i \geq 0} a_i X^i\right) \cdot \left(\sum_{i \geq 0} b_i X^i\right) \coloneqq \sum_{i \geq 0} c_i X^i$$

mit

$$c_i \coloneqq \sum_{p=0}^{i} a_p b_{i-p} = \sum_{p+q=i} a_p b_q \ .$$

Bemerkung 13.2.

(a) Die Ringaxiome von R implizieren die Ringaxiome von $R[X]$. Hierbei gilt für Polynome $f = \sum a_i X^i, g = \sum b_i X^i$ und $h = \sum d_i X^i$: Der i-te Summand von $(f \cdot g) \cdot h$ ist

$$\begin{aligned} \sum_{p=0}^{i} c_p d_{i-p} &= \sum_{p=0}^{i} \left(\sum_{q=0}^{p} a_q b_{p-q}\right) d_{i-p} \\ &= \sum_{p=0}^{i} \sum_{q=0}^{p} a_q b_{p-q} d_{i-p} \\ &= \sum_{r+s+t=i} a_r b_s d_t \ . \end{aligned}$$

(b) Formal gesehen sind Polynome Folgen (a_i), mit $a_i \in R$, wobei nur endlich viele a_i ungleich Null sind. Setze $X \coloneqq (0, 1, 0, 0, \ldots)$, dann folgt mit der obigen Multiplikationsformel

$$X^2 = X \cdot X = (0, 1, 0, 0, \ldots) \cdot (0, 1, 0, 0, \ldots) = (0, 0, 1, 0, 0, \ldots) \ .$$

Induktiv folgt, dass $X^j = (b_i)$ ist mit $b_i = 0$ für $i \neq j$ und $b_j = 1$. Für $a \in R$, definiere $a \cdot (b_i) = (a \cdot b_i)$, dann entspricht die Folge (a_i) genau der formalen Summe $\sum a_i X^i$ aus Definition 13.1. Aus der formalen Definition von Polynomen folgt, dass zwei Polynome $f = \sum a_i X^i$ und $g = \sum b_i X^i$ genau dann gleich sind, wenn $a_i = b_i$ ist für alle Indizes i. Zum Beispiel ist X^2+X nicht das Nullpolynom, da es Koeffizienten ungleich Null hat.

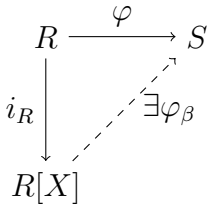
(c) Sei $n \geq 2$. Definiere induktiv $R[X_1, \ldots, X_n] \coloneqq R[X_1, \ldots, X_{n-1}][X_n]$, den Polynomring über R in n Unbestimmten $X_1, \ldots, X_n$.

Theorem 13.3 (Universelle Eigenschaft des Polynomrings)**.** *Sei $\varphi : R \to S$ ein Ringhomomorphismus von kommutativen Ringen und sei $\beta \in S$. Dann gibt es genau einen Ringhomomorphismus*

$$\varphi_\beta : R[X] \mapsto S$$

mit $\varphi_\beta \circ i_R = \varphi$ und $\varphi_\beta(X) = \beta$. Hierbei ist $i_R : R \hookrightarrow R[X], r \mapsto r$, die kanonische Einbettung von R als Teilring von $R[X]$.

Bemerkung: Die Abbildung φ_β heißt *Einsetzungshomomorphismus*.
Das Theorem besagt, dass das folgende Diagramm kommutiert:



Beweis. Wir definieren die Abbildung φ_β durch

$$\varphi_\beta(\sum_i a_i X^i) = \sum_i \varphi(a_i)\beta^i \ . \tag{13.1}$$

Dann ist $\varphi_\beta(1 \cdot X^0) = \varphi(1) \cdot \beta^0 = 1$ und

$$\begin{aligned}
\varphi_\beta\left(\left(\sum_i a_i X^i\right)\left(\sum_i b_i X^i\right)\right) &= \varphi_\beta\left(\sum_i \left(\sum_{p=0}^{i} a_p b_{i-p}\right) X^i\right) \\
&\overset{(13.1)}{=} \sum_i \varphi\left(\sum_{p=0}^{i} a_p b_{i-p}\right) \cdot \beta^i \\
&\overset{\varphi \text{ Homom.}}{=} \sum_i \sum_{p=0}^{i} \varphi(a_p)\varphi(b_{i-p}) \cdot \beta^i \\
&\overset{\text{Mult}}{=} \left(\sum_i \varphi(a_i)\beta^i\right)\left(\sum_i \varphi(b_i)\beta^i\right) \\
&= \varphi_\beta\left(\sum_i a_i X^i\right)\varphi_\beta\left(\sum_i b_i X^i\right) \ .
\end{aligned}$$

Im vorletzten Schritt wurde benutzt, dass S kommutativ ist. Nachrechnen der verbleibenden Eigenschaften $\varphi_\beta(f + g) = \varphi_\beta(f) + \varphi_\beta(g)$ für alle $f, g \in R[X]$ liefert, dass φ_β ein Ringhomomorphismus ist. □

Bemerkung 13.4. Polynome sind im Allgemeinen keine Funktionen:

(a) Sei R ein kommutativer Ring. Sei X eine nicht-leere Menge. Dann ist die Menge $\mathrm{Abb}(X, R) = \{f : X \to R\}$ mit

$$(f+g)(x) \coloneqq f(x) + g(x) \ ,$$
$$(f \cdot g)(x) \coloneqq f(x) \cdot g(x)$$

ein Ring. Auf Übungsblatt 7 wird dieser Ring mit R^X bezeichnet.

(b) Sei nun $X \coloneqq R$. Sei $\varphi_a : R \to R, x \mapsto a$ und $\mathrm{id}_R : R \to R, x \mapsto x$. Die Abbildung φ_1 ist das Einselement in $\mathrm{Abb}(R, R)$. Definiere $\varphi : R \to \mathrm{Abb}(R, R)$ mit $a \mapsto \varphi_a$. Dann ist φ ein Ringhomomorphismus. Mit 13.3 folgt, dass genau ein Ringhomomorphismus $\Phi : R[X] \to \mathrm{Abb}(R, R)$ existiert mit $\Phi \circ i_R = \varphi$ und mit $\Phi(X) = \mathrm{id}_R$. Sei $f = \sum_{i \geq 0} a_i X^i$ ein Polynom in $R[X]$. Dann ist

$$\begin{aligned} \overline{f} \ &\coloneqq \ \Phi(f) = \Phi\left(\sum_i a_i X^i\right) \\ &\overset{13.3}{=} \sum_i \varphi(a_i)\,\mathrm{id}_R^i = \sum_i \varphi_{a_i}\,\mathrm{id}_R^i \ . \end{aligned}$$

Die Abbildung $\overline{f} : R \to R$ ist also gegeben durch

$$\overline{f}(x) = \sum_i \varphi_{a_i}(x)\,\mathrm{id}_R(x)^i = \sum_i a_i x^i \ .$$

(c) Im Allgemeinen ist es wichtig, zwischen dem Polynom f und der Polynomfunktion $\overline{f}$ zu unterscheiden, denn der Homomorphismus Φ ist im Allgemeinen nicht injektiv. Zum Beispiel gilt für $R = \mathbb{Z}_2$: Es ist $|\mathrm{Abb}(\mathbb{Z}_2, \mathbb{Z}_2)| = 4$. Aber $\mathbb{Z}_2[X]$ hat unendlich viele Elemente, nämlich unter anderem $1 \cdot X^t$ für $t \in \mathbb{N}_0$. Alternativ, das Polynom $f = X^2 + X$ ist nicht das Nullpolynom (siehe 13.2), aber $\overline{f}$ ist die Nullfunktion, denn $\overline{f}(0) = 0$ und $\overline{f}(1) = 0$. Ist hingegen $R = \mathbb{R}$ oder $R = \mathbb{C}$, so ist die Abbildung Φ injektiv. Angenommen $\overline{f} = \Phi(f) = 0$, die Nullfunktion. Dann hat die Funktion $\overline{f}$ jedes Element $r \in R$ als Nullstelle, hat also unendlich viele Nullstellen. Polynome vom Grad n haben höchstens n Nullstellen. Also ist das Polynom $f = 0$, und die Abbildung Φ ist injektiv. In diesem Fall können Polynome und Polynomfunktionen identifiziert werden.

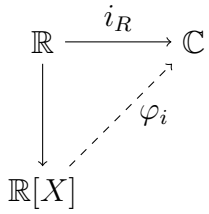
Bemerkung 13.5. Sei $R \leq S$ ein Teilring. Sei $\varphi : R \hookrightarrow S, r \mapsto r$ Einbettung. Sei $\beta \in S$. Dann ist

$$\mathrm{im}(\varphi_\beta) = \left\{ \sum_{i=0}^{n} a_i \beta^i \;\middle|\; n \in \mathbb{N}_0, a_i \in R \right\}$$

ein Teilring von S, der kleinste Teilring von S, der R und β enthält. Wir definieren $R[\beta] := \mathrm{im}(\varphi_\beta)$, und lesen $R[\beta]$ als „R *adjungiert* β“. Zum Beispiel ist $\mathbb{Z}[i] = \{a + bi \mid a, b \in \mathbb{Z}\}$ und $\mathbb{Z}[\sqrt[3]{2}] = \{a + b\sqrt[3]{2} + c(\sqrt[3]{2})^2 \mid a, b, c \in \mathbb{Z}\}$.

Beispiel 13.6.

(a) Die Abbildung $\varphi_i : \mathbb{R}[X] \to \mathbb{C}, f \mapsto f(i)$ ist ein Ringhomomorphismus nach 13.3.



Da $\varphi_i(a+bX) = a+bi$ ist, ist die Abbildung φ_i surjektiv. Mit dem Homomorphiesatz 11.3 folgt

$$\mathbb{R}[X]/(X^2+1) = \mathbb{R}[X]/\mathrm{Ker}(\varphi_i) \simeq \mathrm{im}(\varphi_i) \simeq \mathbb{C} \ .$$

Das Polynom X^2+1 hat die Nullstelle i und somit ist $X^2+1 \in \mathrm{Ker}(\varphi_i)$. In 14.6 werden wir sehen, dass in $\mathbb{R}[X]$ jedes Ideal ein Hauptideal ist. Damit folgt recht leicht, dass $\mathrm{Ker}(\varphi_i) = (X^2+1)$, wobei (X^2+1) das von X^2+1 erzeugte Ideal ist. Siehe Beispiel 15.9.

(b) Sei $p \in \mathbb{N}$, mit $p \geq 2$. Die Abbildung $\varphi : \mathbb{Z}[X] \to \mathbb{Z}_p[X]$, $\sum a_i X^i \mapsto \sum \overline{a_i} X^i$, mit $\overline{a_i} \coloneqq a_i \bmod p$ ist ein Ringhomomorphismus nach 13.3.

Bemerkung 13.7 (Gradformel)**.** Sei $f = \sum a_i X^i$ und $g = \sum b_i X^i$ Polynome in $R[X]$.

(a) Definiere den *Grad von* f, $\deg(f)$, als

$$\deg(f) = \max\{i \mid a_i \neq 0\}$$

mit der Konvention $\deg(0) = -\infty$. Sei $n = \deg(f)$. Der Koeffizient a_n heißt *Leitkoeffizient* von f. Das Polynom f heißt *normiert*, falls der Leitkoeffizient von f eins ist.

(b) Sei $\deg(f) = n$, und $\deg(g) = m$. Dann ist

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

In der letzten Formel gilt bisweilen Gleichheit. Der Koeffizient von X^{n+m} in $f \cdot g$ ist $a_n b_m$, und ist damit ungleich Null, falls a_n oder b_m kein Nullteiler ist. In diesem Fall – also insbesondere wenn R ein Integritätsbereich ist – gilt $\deg(f \cdot g) = \deg(f) + \deg(g)$. Diese Formel wird als *Gradformel* bezeichnet.

Beispiel 13.8.

(a) In $\mathbb{Z}_6[X]$ gilt $(2x^7-1) \cdot (3x^2+1) = 6x^9 + 2x^7 - 3x^2 - 1 = 2x^7 - 3x^2 - 1$, also

$$\deg((2x^7-1)(3x^2+1)) = 7 < 9 = \deg(2x^7-1) + \deg(3x^2+1) \ .$$

(b) Es ist R ein Integritätsbereich genau dann, wenn $R[X]$ ein Integritätsbereich ist. Ist R ein Integritätsbereich, dann ist $R[X]^\times = R^\times$.

Beweis.

(i) „⇐“: Siehe 12.7.

„⇒“: Sei R ein Integritätsbereich. Seien $f, g \in R[X]$ mit $f \cdot g = 0$ und $g \neq 0$. Nach 13.7 folgt $-\infty = \deg(0) = \deg(f \cdot g) = \deg(f) + \deg(g)$. Damit folgt $\deg(f) = -\infty$, d. h. $f = 0$. Also hat der Ring $R[X]$ keine Nullteiler.

(ii) Sei $f \in R[X]^\times$, dann existiert ein Polynom $g \in R[X]$ mit $1 = f \cdot g$. Mit der Gradformel 13.7 folgt

$$0 = \deg(1) = \deg(f \cdot g) = \deg(f) + \deg(g) \ .$$

Es folgt, dass $\deg(f) = 0 = \deg(g)$ und damit $f = a_0 \in R$ und $g = b_0 \in R$ mit $a_0 b_0 = 1$. Also ist $f \in \mathbb{R}^\times$. Das zeigt $R[X]^\times = R^\times$. □

Theorem 13.9 (Division mit Rest in $R[X]$)**.** *Sei R ein Ring. Sei $g = \sum_{i=0}^{d} b_i X^i \in R[X]$ mit Leitkoeffizent $b_d \in R^\times$. Dann existieren zu $f \in R[X]$ eindeutige $q, r \in R[X]$ mit*

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

wobei $\deg(r) < d$.

Bemerkung: In den folgenden Anwendungen wird dieses Theorem typischerweise für einen Körper R angewandt; in diesem Fall ist der Leitkoeffizient eines beliebigen Polynoms dann immer eine Einheit.

Beweis.

(a) *Eindeutigkeit*: Angenommen, $f = qg + r = q'g + r'$ mit $\deg(r) < d, \deg(r') < d$. Dann ist $(q - q')g = r' - r$. Es folgt mit 13.7

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

wobei wir benutzt haben, dass die Einheit b_d kein Nullteiler ist (siehe 12.7). Es folgt $\deg(q - q') = -\infty$, also $q - q' = 0$, d. h. $q = q'$ und damit auch $r = r'$.

(b) *Existenz*: Wir machen Induktion nach $\deg f =: n$. Ist $\deg f < d$, wähle $q = 0$ und $r = f$, und die Behauptung folgt. Sei nun $\deg(f) \geq d$. Sei $f = \sum_{i=0}^{n} a_i X^i$. Setze

$$f_1 \coloneqq f - a_n b_d^{-1} X^{n-d} g \ .$$

Dann ist $\deg(f_1) < \deg(f)$. Nach Induktionsvoraussetzung existieren $q_1, r_1 \in R[X]$ mit $f_1 = q_1 \cdot g + r_1$, und mit $\deg(r_1) < d$. Es folgt

$$\begin{aligned} f &= f_1 + a_n b_d^{-1} X^{n-d} g = (q_1 g + r_1) + a_n b_d^{-1} X^{n-d} g \\ &= (q_1 + a_n b_d^{-1} X^{n-d}) g + r_1 \end{aligned}$$

mit $\deg(r_1) < d$. □

Kapitel 14

Euklidische Ringe

Im Ring der ganzen Zahlen $\mathbb{Z}$ haben wir eine Division mit Rest. Diese ermöglicht es uns, den größten gemeinsamen Teiler (siehe 11.7) und das kleinste gemeinsame Vielfache zweier Zahlen zu berechnen; für Zahlen $a, b \in \mathbb{Z}$ ist $\mathrm{kgV}(a,b) = a \cdot b / \mathrm{ggT}(a,b)$. Division mit Rest war auch der Schlüssel, um in 2.4 zu zeigen, dass alle Ideale in $\mathbb{Z}$ Hauptideale sind. In Kapiel 13 haben wir gesehen, dass es weitere Ringe gibt, die eine Division mit Rest haben. Dies motiviert uns solche Ringe in diesem Kapitel genauer zu studieren.

Definition 14.1. Ein Integritätsbereich R heißt *euklidischer Ring* oder *euklidisch*, falls es eine Abbildung $\delta : R \setminus \{0\} \to \mathbb{N}_0$ gibt mit: Für alle $a, b \in R$ mit $b \neq 0$ existieren $q, r \in R$ mit $a = qb + r$ mit $r = 0$ oder $\delta(r) < \delta(b)$.
Wir nennen δ *euklidische Funktion* oder *Gradfunktion*.

Beispiel 14.2.

(1) Sei K ein Körper. Seien $a, b \in K$ mit $b \neq 0$. Dann ist $a = (ab^{-1})b + 0$, d. h. $q = ab^{-1}$ und $r = 0$. Also ist K euklidisch, wobei die Gradfunktion δ beliebig gewählt werden kann.

(2) Der Ring der ganzen Zahlen $\mathbb{Z}$ mit $\delta(z) = |z|$ für alle $z \in \mathbb{Z} \setminus \{0\}$ ist euklidisch:

Sei $S = \{m \in \mathbb{Z} \mid m \geq 0, m = a - nb, n \in \mathbb{Z}\}$. Dann ist $S \neq \emptyset$. Sei $r := \min S$. Definiere q durch die Gleichung $r = a - qb$. Da $r \in S$ ist, ist $q \in \mathbb{Z}$. Nach Definition gilt also $a = qb + r$ mit $0 \leq r < |b|$.

Es wird in Definition 14.1 nicht gefordert, dass die Division mit Rest eindeutig ist. Es gilt zum Beispiel $7 = 2 \cdot 3 + 1 = 3 \cdot 3 + (-2)$. In beiden Fällen gilt $\delta(r) < \delta(b)$.

(3) Sei K ein Körper. Dann ist der Polynomring $K[X]$ euklidisch mit $\delta(f) := \deg(f)$. Siehe 13.8 und 13.9.

Beispiel 14.3.

(a) Sei $R := \mathbb{Z}[\sqrt{d}] = \{a + b\sqrt{d} \mid a, b \in \mathbb{Z}\}$ für $d \in \{-2, -1, 2, 3\}$ mit $\delta : R \setminus \{0\} \to \mathbb{N}_0$, definiert durch $\delta(x + y\sqrt{d}) = |x^2 - dy^2|$. Dann ist R euklidisch.

(b) Sei $R := \mathbb{Z}[w_d] = \{a + bw_d \mid a, b \in \mathbb{Z}\}$ mit $w_d := \frac{1}{2}(1 + \sqrt{d})$ für $d \in \{-11, -7, -3, 5\}$ mit $\delta : R \setminus \{0\} \to \mathbb{N}_0, x + yw_d \mapsto (x + yw_d)(x + y\overline{w_d})$ wobei $\overline{w_d} := \frac{1}{2}(1 - \sqrt{d})$. Dann ist R euklidisch.

Der Ring R heißt der *Ring der ganzen Zahlen* im Körper $\mathbb{Q}[\sqrt{d}]$.

Beweis.

(i) Sei $d \neq 1$ eine quadratfreie ganze Zahl, also so, dass kein Quadrat einer natürlichen Zahl ≥ 2 die Zahl d teilt. Definiere $N : \mathbb{Q}[\sqrt{d}] \to \mathbb{Q}$ durch

$$N(x + y\sqrt{d}) = x^2 - dy^2 = (x + y\sqrt{d})(x - y\sqrt{d}).$$

Die Funktion N wird als Normfunktion bezeichnet. Schreibe $\bar{z} = x - y\sqrt{d}$ für $z = x + y\sqrt{d}$. Man nennt $\bar{z}$ das zu z konjugierte Element. Ist d negativ, so entspricht dies genau der komplexen Konjugation. Es ist $N(z) = z \cdot \overline{z}$ und $\overline{z_1 \cdot z_2} = \overline{z_1} \cdot \overline{z_2}$. Damit folgt, dass die Norm N multiplikativ ist, also $N(z_1 \cdot z_2) = N(z_1) \cdot N(z_2)$ für alle $z_1, z_2 \in \mathbb{Q}[\sqrt{d}]$ gilt. Da die Betragsfunktion multiplikativ ist, ist auch $\delta = |N|$ multiplikativ.

(ii) Seien $a, b \in R$ mit $b \neq 0$. Da $R \leq \mathbb{C}$ ist, können wir im Körper $\mathbb{C}$ bzw. in $\mathbb{Q}[\sqrt{d}]$ rechnen. Sei $a = x + y\sqrt{d}$ und $b = s + t\sqrt{d}$ für $x, y, s, t \in \mathbb{Z}$. Es gilt:

$$\begin{aligned} ab^{-1} &= \frac{x + y\sqrt{d}}{s + t\sqrt{d}} \cdot \frac{s - t\sqrt{d}}{s - t\sqrt{d}} \\ &= \frac{(\dots) + (\dots)\sqrt{d}}{s^2 - dt^2} \\ &= \frac{(\dots)}{s^2 - dt^2} + \frac{(\dots)}{s^2 - dt^2}\sqrt{d} = u + v\sqrt{d} \end{aligned}$$

für geeignete rationale Zahlen $u, v \in \mathbb{Q}$. Auch wenn es nicht relevant für diesen Beweis ist, merken wir an: Diese Rechnung zeigt, dass $b^{-1} \in \mathbb{Q}[\sqrt{d}]$ ist. Damit ist also $\mathbb{Q}[\sqrt{d}]$ ein Körper, wobei $b^{-1} = \overline{b}N(b)^{-1}$ ist.

(iii) Wähle $m, n \in \mathbb{Z}$ mit $|u - m| \leq \frac{1}{2}$ und $|v - n| \leq \frac{1}{2}$. Setze $\alpha \coloneqq u - m \in \mathbb{Q}, \beta \coloneqq v - n \in \mathbb{Q}$, d. h. $|\alpha| \leq \frac{1}{2}$ und $|\beta| \leq \frac{1}{2}$. Setze $q \coloneqq m + n\sqrt{d} \in R$. Die Zahlen $x, y \in \mathbb{Q}$ beziehungsweise in $\mathbb{Z}$ sind eindeutig durch die Zahl $z = x + y\sqrt{d}$ bestimmt. Trägt man die Zahl aus $\mathbb{Z}[\sqrt{d}]$ in ein Koordinatensystem ein, so entsprechen sie gerade ganzzahligen Gitterpunkten im Koordinatensystem. Geometrisch gesehen ist dann q der Punkt im Gitter mit kürzestem Abstand zum Punkt ab^{-1} im Koordinatensystem. Setze $r \coloneqq a - qb \in R$. Dann gilt

$$r = (u + v\sqrt{d})b - (m + n\sqrt{d})b = b((u - m) + (v - n)\sqrt{d}) = b(\alpha + \beta\sqrt{d}) \ .$$

Dann ist:

$$\begin{aligned} \delta(\alpha + \beta\sqrt{d}) = |\alpha^2 - d\beta^2| &= \begin{cases} \alpha^2 + 2\beta^2 & \text{, für } d = -2 \\ \alpha^2 + \beta^2 & \text{, für } d = -1 \\ |\alpha^2 - 2\beta^2| & \text{, für } d = 2 \\ |\alpha^2 - 3\beta^2| & \text{, für } d = 3 \end{cases} \\ &\leq \begin{cases} \alpha^2 + 2\beta^2 & \text{, für } d \in \{-2, -1, 2\} \\ \max\{\alpha^2, 3\beta^2\} & \text{, für } d = 3 \end{cases} \leq \frac{3}{4} < 1 \ . \end{aligned}$$

Es folgt $\delta(r) = \delta(b(\alpha + \beta\sqrt{d})) = \delta(b) \cdot \delta(\alpha + \beta\sqrt{d}) < \delta(b)$.

Damit ist (a) bewiesen, (b) wird ähnlich bewiesen. □

Definition 14.4. Ein Intigritätsbereich R heißt Hauptidealring (HIR), falls jedes Ideal $I \trianglelefteq R$ ein Hauptideal ist, d. h. es existiert $x \in R$ mit $I = (x) = \langle x \rangle$.

Theorem 14.5. *Jeder euklidiche Ring ist ein Hauptidealring.*

Beweis. Wir imitieren den Beweis für $\mathbb{Z}$, siehe 10.9 beziehungsweise 2.4. Ist $I = \{0\}$, dann ist I ein Hauptideal, erzeugt durch das Nullelement. Sei also $\{0\} \neq I \trianglelefteq R$. Wähle $0 \neq d \in I$ mit $\delta(d)$ minimal in $\delta(I \setminus \{0\})$, d. h. $\delta(d) \leq \delta(x)$ für alle $x \in I \setminus \{0\}$. Da $d \in I$ ist, folgt $\langle d \rangle = (d) \subseteq I$. Sei also $x \in I$. Da R euklidisch ist, existieren $q, r \in R$ mit $x = qd + r$ und $r = 0$ oder $\delta(r) < \delta(d)$. Es ist $r = x - qd \in I$. Da $\delta(d)$ minimal ist, folgt $r = 0$. Also ist $x = q \cdot d \in \langle d \rangle$, und damit ist $I = \langle d \rangle$ ein Hauptideal. □

Korollar 14.6. *Die Ringe $\mathbb{Z}, K[X]$ für K Körper und $\mathbb{Z}[i]$ sind Hauptidealringe.*

Beispiel 14.7.

(a) Der Polynomring $\mathbb{Z}[X]$ ist kein Hauptidealring, also nicht euklidisch.

(b) Ist K ein Körper, dann ist $K[X, Y]$ kein Hauptidealring, also nicht euklidisch.

Beweis. Sei $I \coloneqq \langle 2, X \rangle \trianglelefteq \mathbb{Z}[X]$. Da $1 \notin I$, ist $I \neq \mathbb{Z}[X]$. Angenommen, I ist ein Hauptideal. Dann existiert $0 \neq f \in \mathbb{Z}[X]$ mit $I = \langle f \rangle$. Da $2 \in I = \langle f \rangle$, existiert $g \in \mathbb{Z}[X]$ mit $2 = f \cdot g$. Nach 13.7 ist $0 = \deg(2) = \deg(fg) = \deg(f) + \deg(g)$. Damit folgt $\deg(f) = 0$, d. h. $f = a_0 \in \mathbb{Z}$. Da $a_0 \mid 2$ gilt, ist $a_0 \in \{\pm 1, \pm 2\}$. Angenommen, $a_0 = \pm 1$, dann ist $I = \mathbb{Z}[X]$, Widerspruch. Angenommen, $a_0 = \pm 2$, dann ist $X \notin \langle a_0 \rangle = \langle f \rangle = I$. Also ist I kein Hauptideal. □

Beispiel 14.8. Sei $R = \mathbb{Z}[w_d] = \{a + bw_d \mid a, b \in \mathbb{Z}\}$ mit $w_d = w = \frac{1}{2}(1 + \sqrt{-19})$. Dann ist R nicht euklidisch, aber R ist ein Hauptidealring.

Beweis. Wir zeigen hier nur, dass R nicht euklidisch ist. Um zu zeigen, dass R ein Hauptidealring ist, imitiert man den Beweis von 14.5. Die Funktion $\delta = |N|$ in Beispiel 14.3 ist für R keine euklidische Funktion, sondern lediglich eine sogenannte schwach-euklidische Funktion. Für diese schwach-euklidischen Funktionen lässt sich ein analoges Resultat zu 14.5 zeigen.

(a) (i) Es ist $w \cdot \overline{w} = \frac{1}{2} \cdot \frac{1}{2}(1 + \sqrt{-19})(1 - \sqrt{-19}) = \frac{1}{4} \cdot 20 = 5$ und $w + \overline{w} = 1$. Es folgt

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

für alle $a, b \in \mathbb{Z}$. Komplexe Konjugation ist multiplikativ, also ist die Abbildung $N : R \to \mathbb{N}_0$ definiert durch $N(a + bw) = a^2 + 5b^2 + ab$ multiplikativ.

(ii) Wir bestimmen die Einheiten des Rings R.

- Sei $x \in R^\times$. Dann existiert $y \in R$ mit $1 = xy$. Folglich ist $1 = N(1) = N(xy) = N(x) \cdot N(y)$. Da der Bildbereich von N die natürlichen Zahlen sind, folgt $N(x) = 1$.
- Sei $x = a + bw \in R$ mit $N(x) = 1$. Dann ist $1 = N(x) = \frac{1}{2}(a+b)^2 + \frac{1}{2}a^2 + \frac{9}{2}b^2$, also $b = 0$, d. h. $a = \pm 1$. Dies zeigt $R^\times = \{\pm 1\}$.

(b) (i) Angenommen, $R = \mathbb{Z}[w]$ ist euklidisch mit Gradfunktion δ. Wähle $0 \neq x \in R \setminus R^\times$ so, dass $\delta(x)$ minimal ist in $\delta(R \setminus \{0, 1, -1\})$.
Sei $y \in R \setminus \{0, 1, -1\}$. Da R euklidisch ist, existieren $q, r \in R$ mit $y = q \cdot x + r$ mit $r = 0$ oder $\delta(r) < \delta(x)$. Die Wahl von x impliziert, dass $r = 0$ oder $r \in R^\times = \{1, -1\}$ ist. Sei $S \coloneqq {}^{R}\!/_{\langle x \rangle}$. Da $x \notin R^\times$ ist, ist $\langle x \rangle \neq R$. Der Ring S enthält also mindestens zwei Elemente. Da $y = qx + r$ mit $r \in \{0, 1, -1\}$, folgt $y + \langle x \rangle = r + \langle x \rangle$. Daher enthält S höchstens drei Elemente. Da $(S, +)$ eine Gruppe ist, folgt mit 1.6, dass $S \simeq {}^{\mathbb{Z}}\!/_{2\mathbb{Z}}$ oder $S \simeq {}^{\mathbb{Z}}\!/_{3\mathbb{Z}}$ als Gruppe, und damit (u. a. wegen $2 \cdot 2 = 2(1 + 1) = 2 \cdot 1 + 2 \cdot 1 = 2 + 2 = 1$) auch als Ring.

(ii) Es ist $-19 = (2w - 1)^2 = 4w^2 - 4w + 1$, also $0 = 4w^2 - 4w + 20$ und damit $0 = w^2 - w + 5$. Folglich ist w Nullstelle von $X^2 - X + 5$. Sei $I \trianglelefteq R$. Dann ist

$$\begin{aligned} 0 + I &= (w^2 - w + 5) + I \\ &= (w + I)^2 - (w + I) + (5 + I) \ , \end{aligned}$$

also ist $w + I \in {}^{R}\!/_{I}$ eine Nullstelle von $X^2 - X + 5$. Im Ring $S = {}^{R}\!/_{\langle x \rangle}$ gibt es keine Nullstelle von $X^2 - X + 5$:
In $\mathbb{Z}_2$:

$$\begin{aligned} 0^2 - 0 + 5 &= 1 \neq 0 \\ 1^2 - 1 + 5 &= 1 \neq 0 \ . \end{aligned}$$

In $\mathbb{Z}_3$:

$$\begin{aligned} 0^2 - 0 + 5 &= 2 \neq 0 \\ 1^2 - 1 + 5 &= 2 \neq 0 \\ 2^2 - 2 + 5 &= 1 \neq 0 \ . \end{aligned}$$

Dies ist ein Widerspruch.

Also ist R nicht euklidisch. □

Kapitel 15

Maximale Ideale und Primideale

Definition 15.1. Sei R ein kommutativer Ring.

(a) $I \trianglelefteq R$ heißt *Primideal*, falls $I \neq R$ und $a, b \in I$ mit $ab \in I$ impliziert $a \in I$ oder $b \in I$.

(b) $I \trianglelefteq R$ heißt *maximales Ideal*, falls $I \neq R$ und kein Ideal $J \trianglelefteq R$ existiert mit $I \subsetneq J \subsetneq R$.

Proposition 15.2. *Sei R ein Integritätsbereich, $I \trianglelefteq R$. Dann gilt:*

(a) I Primideal $\Leftrightarrow {}^{R}\!/_{I}$ Integritätsbereich.

(b) I maximal $\Leftrightarrow {}^{R}\!/_{I}$ Körper.

Insbesondere sind maximale Ideale immer auch Primideale.

Beweis. Da R kommutativ ist, ist ${}^{R}\!/_{I}$ ein kommutativer Ring nach 10.14.

(a) „$\Rightarrow$“: Seien $a+I$ und $b+I \in {}^{R}\!/_{I}$ mit $(a+I)(b+I) = 0+I$. Es folgt $ab+I = 0+I$, also $ab \in I$. Da I ein Primideal ist, folgt $a \in I$ oder $b \in I$, also $a+I = 0+I$ oder $b+I = 0+I$.

„$\Leftarrow$“: Sei $ab \in I$. Dann ist $0+I = ab+I = (a+I)(b+I)$. Da ${}^{R}\!/_{I}$ ein Integritätsbereich ist, folgt $a+I = 0+I$ oder $b+I = 0+I$. Damit folgt $a \in I$ oder $b \in I$.

(b) „$\Rightarrow$“: Sei I ein maximales Ideal in R. Mit 11.1 und da I maximal in R ist, folgt, dass ${}^{R}\!/_{I}$ nur die Ideale $\{0\}$ und ${}^{R}\!/_{I}$ hat. Nach 12.2 ist damit ${}^{R}\!/_{I}$ ein Körper.

„$\Leftarrow$“: Sei ${}^{R}\!/_{I}$ ein Körper. Dann hat ${}^{R}\!/_{I}$ nach 12.2 nur die Ideale $\{0\}$ und ${}^{R}\!/_{I}$. Mit 11.1 folgt, dass es kein Ideal echt zwischen I und R gibt, also ist I nach Definition 15.1 maximal. □

Beispiel 15.3. Sei $R = \mathbb{Z}$ und $p \in \mathbb{N}_0$.

(a) Dann ist $p\mathbb{Z} \trianglelefteq \mathbb{Z}$ Primideal genau dann, wenn ${}^{\mathbb{Z}}\!/_{p\mathbb{Z}}$ ein Integritätsbereich ist, also wenn p prim oder $p = 0$ ist.

(b) Dann ist $p\mathbb{Z} \trianglelefteq \mathbb{Z}$ maximal genau dann, wenn ${}^{\mathbb{Z}}\!/_{p\mathbb{Z}}$ ein Körper ist, also genau dann, wenn p prim ist.

(c) Für $n, m \in \mathbb{Z}$ gilt $n \mid m$ genau dann, wenn $m\mathbb{Z} \subseteq n\mathbb{Z}$. Sei $m \in \mathbb{Z}\backslash\{\pm 1\}$. Sei $p \mid m$ mit p Primzahl, dann ist $m\mathbb{Z} \subseteq p\mathbb{Z}$, also ist jedes Ideal $m\mathbb{Z}$ Teilmenge eines maximalen Ideals von $\mathbb{Z}$.

Definition 15.4. Sei $\emptyset \neq M$ eine Menge mit einer Relation $\leq$. Dann ist $\leq$ eine *Halbordnung* auf M (beziehungsweise M heißt *partiell geordnet*), falls $\leq$ reflexiv und transitiv ist, und falls für $a, b \in M$ mit $a \leq b$ und $b \leq a$ gilt, dass $a = b$ ist (also $\leq$ *anti-symmetrisch* ist). Eine Halbordnung auf M heißt eine *Ordnung* auf M (beziehungsweise M heißt *total geordnet*), falls für $a, b \in M$ immer $a \leq b$ oder $b \leq a$ gilt.

Beispiel 15.5.

(a) Auf $\mathbb{Z}$ ist die übliche $\leq$-Relation eine Ordnung.

(b) Sei $\emptyset \neq X$ und $\mathcal{P}(X) = \{U \subseteq X\}$. Dann ist die Mengeninklusion eine Halbordnung auf X.

Definition 15.6.

(a) Sei $\emptyset \neq M$ eine Menge mit Halbordnung $\leq$. Dann heißt $\emptyset \neq K \subseteq M$ eine *Kette* in M, falls $\leq$ auf K eine Ordnung ist.

(b) Ein Element $s \in M$ heißt *obere Schranke* der Kette $K \subseteq M$, falls $a \leq s$ für alle $a \in K$ ist.

(c) Ein Element $m \in M$ heißt *maximal*, wenn für alle $a \in M$ gilt: $m \leq a \Rightarrow m = a$.

Bemerkung 15.7. Das Lemma von Zorn sagt: Jede induktiv geordnete Menge M hat ein maximales Element. Hierbei ist M induktiv geordnet, falls jede Kette $K \subseteq M$ eine obere Schranke hat. Das Lemma von Zorn ist äquivalent zum Auswahlaxiom.

Theorem 15.8. *Jeder kommutative Ring hat ein maximales Ideal.*

Beweis. (a) Sei $M \coloneqq \{I \trianglelefteq R, I \neq R\}$. Es ist $\{0\} \trianglelefteq R$, also $M \neq \emptyset$. Die Menge M ist partiell geordnet durch Mengeninklusion. Sei $T \subseteq M$ eine Kette. Setze $\hat{I} \coloneqq \bigcup_{J \in T} J$. Wir zeigen $\hat{I} \trianglelefteq R$, d. h. $\hat{I} \in M$. Falls dies gilt, dann folgt $J \subseteq \hat{I}$ für alle $J \in K$. Damit ist $\hat{I}$ eine obere Schranke von T, also ist M induktiv geordnet. Mit dem Lemma von Zorn folgt, dass M ein maximales Element $\mathcal{M}$ hat. Das bedeutet $\mathcal{M} \in M$, also $\mathcal{M} \trianglelefteq R$, und wenn $\mathcal{M} \subseteq I$ für $I \trianglelefteq R$ gilt, dann ist $\mathcal{M} = I$ nach 15.6. Also folgt, dass $\mathcal{M}$ ein maximales Ideal von R im Sinne von 15.1 ist.

(b) Seien $x, x' \in \hat{I}$. Dann existieren $J, J' \in T$ mit $x \in J$ und $x' \in J'$. Ohne Einschränkung sei $J' \subseteq J$. Dann folgt $x, x' \in J$. Da $J \trianglelefteq R$ ist, folgt $x - x' \in J \subseteq \hat{I}$ und $rx \in J \subseteq \hat{I}$ für alle $r \in R$. Also folgt $\hat{I} \trianglelefteq R$. Angenommen, $\hat{I} = R$. Dann ist $1 \in \hat{I} = \bigcup T$. Also existiert $J \in T$ mit $1 \in J$, also $J = R$. Dies ist ein Widerspruch zu $J \in T \subseteq M$. □

Beispiel 15.9.

(1) Die maximalen Ideale von $\mathbb{C}[X]$ sind genau die Hauptideale, die von linearen Polynomen $X - a$ für $a \in \mathbb{C}$, erzeugt werden. Es existiert also eine Bijektion zwischen komplexen Zahlen und maximalen Idealen in $\mathbb{C}[X]$.

Beweis.

(a) Sei $\varphi_a : \mathbb{C}[X] \to \mathbb{C}, f \mapsto f(a)$ der Einsetzungshomomorphismus. Da $\mathbb{C}[X]$ ein Hauptidealring ist, existiert ein Polynom $g \in \mathbb{C}[X]$ mit $\mathrm{Ker}(\varphi_a) = \langle g \rangle$. Insbesondere ist $g(a) = 0$. Aus der Schule wissen wir, dann folgt $X - a \mid g$. Damit folgt $\langle g \rangle \subseteq \langle X - a \rangle$. Da $\varphi_a(X - a) = a - a = 0$, folgt $\mathrm{Ker}(\varphi_a) = \langle X - a \rangle$. Mit 11.3 folgt, dass

$$\mathbb{C}[X]/\mathrm{Ker}(\varphi_a) \simeq \mathrm{im}(\varphi_a) \simeq \mathbb{C}$$

ein Körper ist. Mit 15.2 folgt, dass $\mathrm{Ker}(\varphi_a) = \langle x - a \rangle \trianglelefteq \mathbb{C}[X]$ maximal ist.

(b) Sei $\mathcal{M} \trianglelefteq \mathbb{C}[X]$ maximal. Da $\mathbb{C}[X]$ ein Hauptidealring ist, existiert ein Polynom $f \in \mathbb{C}[X]$ mit $\mathcal{M} = \langle f \rangle$. Da $\langle f \rangle = \langle \lambda f \rangle$ für $\lambda \in \mathbb{C}^\times$ ist, können wir ohne Einschränkung annehmen, das f normiert ist. Jedes Polynom in $\mathbb{C}[X]$ positiven Grades hat eine Nullstelle in $\mathbb{C}$. Sei $a \in \mathbb{C}$ eine Nullstelle von f. Dann ist $f(a) = 0$, also $X - a \mid f$. Damit ist $\langle f \rangle \subseteq \langle X - a \rangle \subseteq \mathbb{C}[X]$. Angenommen $\langle X - a \rangle = \mathbb{C}[X]$, dann existiert $g \in \mathbb{C}[X]$ mit $(X - a)g = 1$. Mit der Gradformel 13.7 ergibt sich ein Widerspruch: $0 = \deg(1) = \deg(X - a) + \deg(g) = 1 + \deg(g)$. Also ist $\langle X - a \rangle \neq \mathbb{C}[X]$. Nach Voraussetzung ist $\mathcal{M} \trianglelefteq \mathbb{C}[X]$ maximal, also gilt $\mathcal{M} = \langle f \rangle = \langle X - a \rangle$. □

(2) Sei $\varphi : \mathbb{R}[X] \to \mathbb{C}$ definiert durch $f \mapsto f(i)$. Da $\varphi(a + bX) = a + bi$, ist der Einsetzungshomomorphismus φ surjektiv. Da $\mathbb{R}[X]$ Hauptidealring ist, existiert ein Polynom $g \in \mathbb{R}[X]$ mit $\langle g \rangle = \mathrm{Ker}(\varphi)$. Wegen $\varphi(X^2 + 1) = i^2 + 1 = -1 + 1 = 0$, ist $X^2 + 1 \in \mathrm{Ker}(\varphi)$. Dann ist $g \mid X^2 + 1$. Schreibe $g \cdot h = X^2 + 1$ für ein $h \in \mathbb{R}[X]$. Mit der Gradformel 13.7 folgt $2 = \deg(X^2 + 1) = \deg(gh) = \deg(g) + \deg(h)$. Wäre $\deg(g) = 0$, so folgt $\mathrm{Ker}(\varphi) = \mathbb{C}[X]$, ein Widerspruch zu $\varphi(1) = 1$. Es gibt kein Polynom in $\mathbb{R}[X]$ vom Grad eins mit Nullstelle i. Also ist $\deg(g) \neq 1$. Also folgt $\deg(g) = 2$ und $\deg(h) = 0$. Damit folgt $g = \mu(X^2 + 1)$ für ein $\mu \in \mathbb{R}^\times$, und $\mathrm{Ker}(\varphi) = \langle X^2 + 1 \rangle$. Mit 11.3 gilt

$$\mathbb{C}[X]/\mathrm{Ker}(\varphi) \simeq \mathrm{im}(\varphi) \simeq \mathbb{C}$$

ist ein Körper, also ist $\mathrm{Ker}(\varphi) = \langle X^2 + 1 \rangle$ nach 15.2 ein maximales Ideal in $\mathbb{R}[X]$.

Beispiel 15.10.

(a) Sei R ein kommutativer Ring und $I \trianglelefteq R$. Wende 13.3 an auf den Ringhomomorphismus $R \xrightarrow{\pi} R/I \hookrightarrow (R/I)[X]$. Dann existiert genau ein Ringhomomorphismus $\varphi : R[X] \to (R/I)[X]$ mit $\varphi(r) = r + I$ für alle $r \in R$ und $\varphi(X) = X$. Nach dem Beweis von 13.3 ist

$$\varphi\left(\sum_i a_i X^i\right) = \sum_i (a_i + I) X^i \ ,$$

also ist φ surjektiv. Ausserdem ist

$$\mathrm{Ker}(\varphi) = \left\{ \sum_i a_i X^i \mid a_i \in I \right\} =: I[X] \trianglelefteq R[X] \ .$$

Mit 11.3 gilt

$$R[X]/I[X] \simeq (R/I)[X] \ .$$

(b) Es ist $I \trianglelefteq R$ Primideal genau dann, wenn der Quotientenring ${}^{R}\!/_{I}$ ein Integritätsbereich ist, siehe 15.2. Nach 13.8 und (a) passiert dies genau dann, wenn $\left({}^{R}\!/_{I}\right)[X]$ beziehungsweise ${}^{R[X]}\!/_{I[X]}$ ein Integritätsbereich ist. Nach 15.2 ist dies äquivalent dazu, dass $I[X] \trianglelefteq R[X]$ Primideal ist. Wir können also Primideale von R hochheben zu Primidealen im Polynomring $R[X]$. Im Allgemeinen hat der Polynomring $R[X]$ aber mehr Primideale als R. Betrachte zum Beispiel den Ring $R = \mathbb{Z}$. Dann ist $\langle X\rangle = \{a_1X + a_2X^2 + \ldots + a_nX^n \mid n \in \mathbb{N}, a_i \in R\} \neq I[X]$ für $I \trianglelefteq \mathbb{Z}$. Wir zeigen: $\langle X\rangle \trianglelefteq \mathbb{Z}[X]$ ist Primideal. Betrachte den Einsetzungshomomorphimus

$$\psi : \mathbb{Z}[X] \to \mathbb{Z}, f \mapsto f(0) \ .$$

Dann ist ψ ein Epimorphismus mit $\mathrm{Ker}(\psi) = \langle X\rangle$. Nach 11.3 ist

$${}^{\mathbb{Z}[X]}\!/_{\langle X\rangle} \simeq \mathbb{Z}$$

ein Integritätsbereich. Mit 15.2 folgt, dass $\langle X\rangle$ ein Primideal in $\mathbb{Z}[X]$ ist. Wir merken an, da $\langle X\rangle \subsetneq \langle X, 2\rangle \subsetneq R[X]$, ist dieses Primideal nicht maximal.

Kapitel 16

Faktorielle Ringe

Wir wollen die Existenz und Eindeutigkeit der Primfaktorzerlegung im Ring der ganzen Zahlen besser verstehen. Welche Eigenschaften von $\mathbb{Z}$ sind dafür verantwortlich, dass eine Zerlegung in Primfaktoren existiert und eindeutig ist? Hierfür verallgemeinern wir das Problem auf Integritätsbereiche. Zunächst müssen wir uns mit der Frage auseinandersetzen, was Primzahlen in einem beliebigen Integritätsbereich sein sollen.

Definition 16.1. Sei R ein Integritätsbereich und $a, b \in R$.

(a) Ein Element a *teilt* b, geschrieben $a \mid b$, falls $c \in R$ existiert mit $a \cdot c = b$. Dies ist äquivalent zu $b \in \langle a \rangle$ und zu $\langle b \rangle \subseteq \langle a \rangle$.

(b) Ein Element a heißt *assoziiert* zu b, geschrieben $a \sim b$, falls $a \mid b$ und $b \mid a$. Dies ist äquivalent zu $\langle a \rangle = \langle b \rangle$ und zu $\exists u \in \mathbb{R}^\times$ mit $a = ub$. Assoziiertheit ist eine Äquivalenzrelation. Im Ring der ganzen Zahlen ist zum Beispiel die Zahl n assoziiert zu $-n$.

Beweis. Angenommen, $a \sim b$ mit $a \neq 0 \neq b$. Dann folgt $a \mid b$ und $b \mid a$. Also existieren $u, v \in R$ mit $au = b$ und $bv = a$. Es folgt $b = au = bvu$. Da R ein Integritätsbereich ist, und $b \neq 0$, können wir kürzen. Es folgt $1 = vu$, also ist $u \in R^\times$ und $a = ub$.

Rest: Nachrechnen. □

Bemerkung 16.2. Eine Primzahl in $\mathbb{N}$ ist eine natürliche Zahl $p \neq 1$, die genau die Teiler $\{1, p\}$ in $\mathbb{N}$ hat. Sei p eine Primzahl und seien $a, b \in \mathbb{Z}$ mit $p \mid ab$. Dann folgt $p \mid a$ oder $p \mid b$. Der folgende kurze Beweis zeigt, dass diese Charakterisierung von Primzahlen eine Konsequenz aus der Division mit Rest in $\mathbb{Z}$ ist.

Beweis. Angenommen, $p \nmid a$. Da p nur Teiler $\{1, p\}$ hat, folgt $\mathrm{ggT}(a, p) = 1$. Nach Bézout existieren $x, y \in \mathbb{Z}$ mit $ax + py = 1$. Also ist $b = abx + pby$ und wegen $p \mid ab$ folgt $p \mid b$. □

Definition 16.3. Sei R ein Integritätsbereich.

(a) Ein Element $0 \neq p \in R$ heißt *prim* oder *Primelement*, falls $p \notin R^\times$ und $p \mid ab$ impliziert $p \mid a$ oder $p \mid b$ (für $a, b \in R$).

(b) Ein Element $0 \neq u \in R$ heißt *unzerlegbar* oder *irreduzibel*, falls $u \notin R^\times$ und $u = ab$ impliziert $a \in R^\times$ oder $b \in R^\times$ (für $a, b \in R$).

Bemerkung 16.4. Im Ring der ganzen Zahlen fallen die Konzepte Primzahl, Primelement und unzerlegbares Element zusammen. Im Allgemeinen gilt: jedes Primelement ist unzerlegbar. Im nächsten Beispiel sehen wir, dass die Umkehrung falsch ist.

Beweis. Sei $0 \neq p \in R \setminus R^\times$ prim. Sei $p = ab$ für $a, b \in R$. Also $p \mid ab$. Da p prim ist, folgt $p \mid a$ oder $p \mid b$. Ohne Einschränkung sei $p \mid a$, d. h. es existiert $x \in R$ mit $px = a$. Folglich ist $p = ab = pxb$, und da R Integritätsbereich ist, folgt $1 = xb$, also $b \in R^\times$. □

Beispiel 16.5. Die Umkehrung von 16.4 ist falsch. Sei $R = \mathbb{Z}[\sqrt{-5}] \leq \mathbb{C}$, d. h. R Integritätsbereich. Es ist $6 = 2 \cdot 3 = (1 + \sqrt{-5})(1 - \sqrt{-5})$, wobei $2, 3, 1 + \sqrt{-5}, 1 - \sqrt{-5}$ unzerlegbar sind, aber nicht prim. Dies ist auch ein Beispiel für eine Faktorisierung eines Elementes in unzerlegbare Elemente, die nicht eindeutig ist.

Beweis. (a) Sei $N : R \to \mathbb{N}_0, a + b\sqrt{-5} \mapsto a^2 + 5b^2$. Dann ist N multiplikativ. Wie in 14.8 folgt $x \in R^\times$ genau dann, wenn $N(x) = 1$. In unserer Situation ergibt sich – wie auch in vielen anderen solchen Ringen – dass $R^\times = \{\pm 1\}$ ist.

(b) Sei $2 = x \cdot y$ für $x, y \in R$. Es folgt $4 = N(2) = N(xy) = N(x)N(y)$. Damit ist $N(x) \in \{1, 2, 4\}$. Es gibt keine $a, b \in \mathbb{Z}$ mit $x = a + b\sqrt{-5}$ und $N(x) = a^2 + 5b^2 = 2$. Ist $N(x) = 1$, dann ist $x \in R^\times$. Ist $N(x) = 4$, dann ist $N(y) = 1$, also $y \in R^\times$. Also ist 2 unzerlegbar.

(c) Es gilt $2 \mid (1 + \sqrt{-5})(1 - \sqrt{-5}) = 6 = 2 \cdot 3$. Sei $2 \mid x$, dann existiert $y \in R$ mit $2y = x$. Dann ist $N(x) = N(2)N(y) = 4N(y)$, insbesondere $N(2) = 4 \mid N(x)$. Es ist $N(1 \pm \sqrt{-5}) = 6$ und $4 \nmid 6$. Somit ist $2 \nmid (1 \pm \sqrt{-5})$. Also ist 2 nicht prim. □

Proposition 16.6. *(a) In einem Integritätsbereich R gilt für $0 \neq p \in R$:*

(i) $\langle p \rangle \trianglelefteq R$ Primideal $\Leftrightarrow$ p prim.

(ii) $\langle u \rangle \trianglelefteq R$ maximal $\Rightarrow$ u unzerlegbar.

(b) In einem Hauptidealring R gilt auch: Ist $u \in R$ unzerlegbar, dann ist $\langle u \rangle \trianglelefteq R$ maximal. Insbesondere gilt also in einem Hauptidealring, dass die Definitionen von unzerlegbar und von prim äquivalent sind.

Beweis.

(a) (i) „$\Rightarrow$“: Sei $\langle p \rangle \trianglelefteq R$ ein Primideal, d. h. $p \neq 0, p \notin R^\times$. Sei $p \mid ab$, dann folgt $ab \in \langle p \rangle$, also $a \in \langle p \rangle$ oder $b \in \langle p \rangle$. Damit ist $p \mid a$ oder $p \mid b$. Also ist p prim.

„$\Leftarrow$“: Sei $p \in R$ prim, d. h. $p \neq 0$, $p \notin R^\times$. Dann ist $\langle p \rangle \neq \{0\}$ und $\langle p \rangle \neq R$. Sei also $ab \in \langle p \rangle$. Dann folgt $p \mid ab$. Da p prim ist, ist dann $p \mid a$ oder $p \mid b$, d. h. $a \in \langle p \rangle$ oder $b \in \langle p \rangle$. Also ist $\langle p \rangle$ ein Primideal.

(ii) Ist $\langle u \rangle$ maximal, dann ist es nach 15.2 auch ein Primideal, also ist u nach (i) prim und damit nach 16.4 unzerlegbar.

(b) (i) Sei u unzerlegbar. Sei $\langle u \rangle \subseteq I \subsetneq R$ mit $I \trianglelefteq R$. Da R ein Hauptidealring ist, existiert $b \in R$ mit $I = \langle b \rangle$. Da $I \neq R$ ist, ist $b \notin R^\times$. Da $\langle u \rangle \subseteq \langle b \rangle$ ist, folgt $b \mid u$, d. h. $\exists a \in R$ mit $ab = u$. Da $b \notin R^\times$ und u unzerlegbar ist, folgt $a \in R^\times$, d. h. $b \sim u$. Es folgt $I = \langle b \rangle = \langle u \rangle$. Also ist $\langle u \rangle$ maximales Ideal in R.

(ii) Nach 16.4 gilt prim impliziert unzerlegbar. Umgekehrt, sei u unzerlegbar, dann ist $\langle u \rangle \trianglelefteq R$ maximal, also $\langle u \rangle$ Primideal nach 15.2, also u prim. □

Definition 16.7. Ein Integritätsbereich R heißt *faktoriell*, falls gilt:

(i) Jedes Element in $R \setminus (\{0\} \cup R^\times)$ ist endliches Produkt von unzerlegbaren Elementen.

(ii) Ist $p_1 \cdot \ldots \cdot p_m = q_1 \cdot \ldots \cdot q_n$ mit p_i, q_j unzerlegbar, dann folgt $m = n$ und nach Umsortierung $p_i \sim q_i$ für $1 \leq i \leq m$.

Es gibt verschiedene Beweise, um zu zeigen, dass jede Nicht-Einheit im Ring der ganzen Zahlen eine Primfaktorzerlegung hat. Wir orientieren uns am folgenden Argument: Sei $a \neq 1$ eine natürliche Zahl. Entweder ist a bereits unzerlegbar, dann exisitiert eine Zerlegung von a als endliches Produkt von unzerlegbaren Elementen. Oder a ist zerlegbar. Dann ist $a = a_1 b_1$, wobei weder a_1 noch b_1 eine Einheit ist. Da a_1 und b_1 echt kleiner als a sind, gibt es nach Induktionsvoraussetzung jeweils eine Zerlegung von a_1 und von b_1 als endliches Produkt von unzerlegbaren Elementen. Also lässt sich auch a als endliches Produkt unzerlegbarer Elemente schreiben. Da in Ringen im Allgemeinen keine Ordnungsrelation existiert, muss das induktive Argument in diesem Beweis ersetzt werden. Dazu benötigen wir die folgende Hilfsaussage:

Lemma 16.8. *Sei R ein Hauptidealring und $I_t \trianglelefteq R$ for $t \in \mathbb{N}$ mit $I_1 \subseteq I_2 \subseteq \ldots \subseteq I_t \subseteq I_{t+1} \subseteq \ldots$. Dann existiert $n \in \mathbb{N}$ mit $I_t = I_n$ für alle $t \geq n$, d. h. die Idealkette wird stationär.*

Beweis. Sei $I \coloneqq \bigcup_{t\in\mathbb{N}} I_t$. Wie in 15.7 gilt $I \trianglelefteq R$. Da R ein Hauptidealring ist, existiert $d \in I$ mit $I = \langle d \rangle = \bigcup_{t\in\mathbb{N}} I_t$, also existiert $n \in \mathbb{N}$ mit $d \in I_n$. Sei $t \geq n$, dann ist $I_n \subseteq I_t \subseteq I = \langle d \rangle \subseteq I_n$. Dies zeigt $I_t = I_n$ für alle $t \geq n$. □

Theorem 16.9. *Jeder Hauptidealring R ist faktoriell.*

Beweis.

(a) Wir wollen $0 \neq a \in R \setminus R^\times$ als Produkt von unzerlegbaren Elementen schreiben.

(i) Angenommen, a ist unzerlegbar, dann sind wir fertig. Sei also a zerlegbar, d. h. es existieren $a_1, b_1 \in R$ mit $a = a_1 b_1 \in R \setminus R^\times$ mit $a = a_1 b_1$. Dann ist $a_1 \mid a$ (und $a_1 \nsim a$), also $\langle a \rangle \subsetneq \langle a_1 \rangle$. Wiederhole das Argument: Entweder sind bereits a_1 und b_1 unzerlegbar, dann endet der Prozess. Oder aber mindestens eines der beiden Elemente – ohne Einschränkung sei dies a_1 – ist zerlegbar; dann existieren $a_2, b_2 \in R \setminus R^\times$ mit $a_1 = a_2 b_2$ und damit ist $\langle a \rangle \subsetneq \langle a_1 \rangle \subsetneq \langle a_2 \rangle$. Nach wiederholter Anwendung erhalten wir eine aufsteigende Kette von Idealen. Mit 16.8 folgt, dass diese Kette stationär wird, etwa bei $\langle a_n \rangle$. Setze $q_1 \coloneqq a_n$. Dann ist q_1 unzerlegbar mit $a = q_1 \cdot a'$.

(ii) Wiederhole den Prozess in (i) für a'. Dann erhalten wir ein unzerlegbares Element q_2 mit $a' = q_2 \cdot a''$, d. h. $a = q_1 q_2 a''$ etc. Wir erhalten hierbei wiederum eine aufsteigende Idealkette $\langle a \rangle \subseteq \langle a' \rangle \subseteq \langle a'' \rangle \ldots$. Nach 16.8 muss diese Idealkette stationär werden, etwa bei $\langle a^{(m)} \rangle$. Dann ist $a^{(m)} = q_m$ unzerlegbar, und damit $a = q_1 \cdots q_m$ endliches Produkt unzerlegbarer Elemente q_i, mit $1 \leq i \leq m$.

(b) Sei $a = p_1 \cdot \ldots \cdot p_m = q_1 \cdot \ldots \cdot q_n$ mit p_i, q_j unzerlegbar. Da R Hauptidealring ist, sind p_i, q_j prim, siehe 16.8. Da $p_1 \mid q_1 \cdot \ldots \cdot q_n$ und p_1 prim ist, existiert j mit $p_1 \mid q_j$. Ohne Einschränkung sei $j = 1$, d. h. $p_1 \mid q_1$. Also existiert $u \in R$ mit $p_1 u = q_1$. Da q_1 unzerlegbar ist, muss einer der beiden Faktoren eine Einheit sein. Da aber

p_1 unzerlegbar ist, folgt $u \in R^\times$. Also ist $p_1 \sim q_1$. Wir kürzen mit p_1 und erhalten $p_2 \cdot \ldots \cdot p_m = q_2' \cdot q_3 \cdot \ldots \cdot q_n$ mit $q_2' \sim q_2$. Induktiv folgt $m = n$ und nach Umsortierung gilt $p_i \sim q_i$ für $1 \leq i \leq m$. □

Bemerkung 16.10.

(a) Wir haben gezeigt: Ist R Integritätsbereich, in dem jede aufsteigende Kette von Hauptidealen abbricht und in dem die Konzepte von unzerlegbar und prim übereinstimmen, dann ist R faktoriell.

(b) Ist R faktoriell, dann sind die Definitionen von unzerlegbar und prim äquivalent.

Beweis. Sei p unzerlegbar und $p \mid ab$. Dann existiert $x \in R$ mit $px = ab$. Schreibe x, a, b als Produkt von unzerlegbaren Elementen. Da R faktoriell ist und p unzerlegbar, muss p (bis auf Assoziiertheit) in der Zerlegung von ab vorkommen, also entweder in der Zerlegung von a oder in der von b. Dies zeigt $p \mid a$ oder $p \mid b$. □

Kapitel 17

Polynomringe über faktoriellen Ringen

Sei R ein Integritätsbereich mit Quotientenkörper $K = \mathrm{Quot}(R)$. Der größte gemeinsame Teiler zweier Zahlen $a, b \in \mathbb{Z}$ wird in der Schule definiert als die größte ganze Zahl, die sowohl a als auch b teilt. In Integritätsbereichen haben wir im allgemeinen keine Ordnungsrelation, können also zwei Elemente nicht bezüglich ihrer Größe vergleichen. Ähnliches gilt für die Definition des kleinsten gemeinsamen Vielfachen zweier ganzen Zahlen. Das Problem kann folgendermaßen umgangen werden:

Bemerkung 17.1. Seien $a, b \in \mathbb{Z}$.

(a) Sei $d = \mathrm{ggT}(a, b)$. Dann existieren $x, y \in \mathbb{Z}$ mit $d = ax + by$, also $d\mathbb{Z} = a\mathbb{Z} + b\mathbb{Z}$. Ist also $e \mid a$ und $e \mid b$, dann gilt $e \mid d$.

(b) Sei $m \coloneqq \mathrm{kgV}(a, b)$. Wegen $a\mathbb{Z} \cap b\mathbb{Z} = \mathrm{kgV}(a, b)\mathbb{Z} = m\mathbb{Z}$ gilt: Ist $a \mid n$ und $b \mid n$, dann folgt $n \in m\mathbb{Z}$, also ist $m \mid n$.

Die folgende Definition des größten gemeinsamen Teilers und kleinsten gemeinsamen Vielfachen zweier Elemente eines Integritätsbereiches entspricht also der in der Schule üblichen Definition:

Definition 17.2. Sei R ein Integritätsbereich und $a, b \in R$.

(a) Ein Element $d \in R$ heißt größter gemeinsamer Teiler von a und b, kurz $\mathrm{ggT}(a, b) = d$, falls:

  (i) $d \mid a$ und $d \mid b$;

  (ii) $e \mid a$ und $e \mid b$ impliziert $e \mid d$.

(b) Ein Element $m \in R$ heißt kleinstes gemeinsames Vielfaches, kurz $\mathrm{kgV}(a, b) = m$, falls:

  (i) $a \mid m$ und $b \mid m$;

  (ii) $a \mid n$ und $b \mid n$ impliziert $m \mid n$.

Beispiel 17.3. Größte gemeinsame Teiler und kleinste gemeinsame Vielfache müssen nicht existieren. Zum Beispiel sei $R = \mathbb{Z}[\sqrt{-5}]$. Wähle $a = 6$ und $b = 2 + 2\sqrt{-5}$.

(i) Angenommen, $d = \mathrm{ggT}(a, b)$. Benutze die Normfunktion N aus Beispiel 16.5. Da $d \mid a$ und $d \mid b$ gilt, folgt $N(d) \mid N(a) = 36$ und $N(d) \mid N(b) = 24$.

(ii) Außerdem gilt $2 \mid a$ und $2 \mid b$, also nach Definition des größten gemeinsamen Teilers gilt auch $2 \mid d$. Es folgt also $4 = N(2) \mid N(d)$. Genauso gilt $1 + \sqrt{-5} \mid a$ und $1 + \sqrt{-5} \mid b$, also $1 + \sqrt{-5} \mid d$, also $6 \mid N(d)$. Mit (i) folgt: $N(d) = 12$. Aber es existieren keine $x, y \in \mathbb{Z}$ mit $x^2 + 5y^2 = 12$. Damit existiert kein $d \in R$ mit $N(d) = 12$. Also existiert $\mathrm{ggT}(a, b)$ nicht.

Bemerkung 17.4. Sei R ein Integritätsbereich mit $a, b \in R$.

(a) Falls $\mathrm{ggT}(a, b)$ bzw. $\mathrm{kgV}(a, b)$ existieren, dann sind sie nur eindeutig bis auf Multiplikation mit einer Einheit, also bis auf Assoziiertheit.

(b) Im faktoriellen Ring R existieren größte gemeinsame Teiler und kleinste gemeinsame Vielfache: Wähle ein Vertretersystem $\mathbb{P}_R$ der Klassen assoziierter Primelemente. Zum Beispiel in $\mathbb{Z}$ wähle $\mathbb{P}_\mathbb{Z} = \{\text{Primzahlen in } \mathbb{N}\}$, im Polynomring $R = K[X]$ mit K beliebiger Körper, wähle als Vertretersystem $\mathbb{P}_R$ die Menge unzerlegbarer normierter Polynome. Seien nun $a, b \in R$ mit Primfaktorzerlegung

$$a = \varepsilon(a) p_1^{a_1} \cdot \ldots \cdot p_n^{a_n}$$
$$b = \varepsilon(b) p_1^{b_1} \cdot \ldots \cdot p_n^{b_n}$$

mit $a_i, b_i \in \mathbb{N}_0, \varepsilon(a), \varepsilon(b) \in R^\times$ und $p_i \in \mathbb{P}_R$ mit $p_i \nsim p_j$ für $i \neq j$. Dann ist

$$\mathrm{ggT}(a, b) = \prod_i p_i^{\min\{a_i, b_i\}},$$
$$\mathrm{kgV}(a, b) = \prod_i p_i^{\max\{a_i, b_i\}}.$$

Nach der Wahl eines Repräsentantensystems $\mathbb{P}_R$ sind größter gemeinsamer Teiler und kleinstes gemeinsames Vielfaches eindeutig bestimmt.

(c) Sei R ein Integritätsbereich mit $a, b \in R$. Nach 10.11 ist $\langle a \rangle + \langle b \rangle$ ein Ideal. Angenommen dies ist ein Hauptideal, etwa $\langle a \rangle + \langle b \rangle = \langle d \rangle$. Dann ist $d = \mathrm{ggT}(a, b)$ und Bézouts Lemma gilt in R, das heißt, es existieren $x, y \in R$ mit $ax + by = d$. Nach 10.11 ist $\langle a \rangle \cap \langle b \rangle$ ein Ideal. Ist $\langle a \rangle \cap \langle b \rangle = \langle m \rangle$ ein Hauptideal, dann ist $m = \mathrm{kgV}(a, b)$.

(d) Sei R ein euklidischer Ring mit Gradfunktion δ. Seien $a, b \in R$. Wie für ganze Zahlen $\mathbb{Z}$ läßt sich der größte gemeinsame Teiler mit Hilfe des euklidischen Algorithmus bestimmen, also mit wiederholter Division mit Rest. Ebenso kann man wie für ganze Zahlen ein Analogon zu Bézouts Lemma beweisen.

Sei für den Rest dieses Kapitels R faktoriell mit Quotientenkörper $K = \mathrm{Quot}(R)$.

Definition 17.5. Sei $f = \sum_{i=0}^n a_i X^i \in R[X]$. Definiere

(i) den *Inhalt* $c(f)$ des Polynoms f durch $c(f) \coloneqq \mathrm{ggT}(a_0, \ldots, a_n) \in R$. Im Englischen sagt man *content*. Da der größte gemeinsame Teiler nur bis auf Assoziertheit bestimmt ist, ist $c(f)$ eine Assoziiertenklasse von Elementen aus R. Die Assoziiertenklasse von $1 \in R$ besteht genau aus den Einheiten von R.

(ii) f primitiv genau dann, wenn $c(f) = 1$, beziehungsweise genauer, wenn $c(f) \in R^\times$ ist. Zum Beispiel: Ist $f = 15X + 50 \in \mathbb{Z}[X]$, dann ist $c(f) = 5$. Jedes normierte Polynom ist primitiv. Beachte $c(af) = a \cdot c(f)$ für $a \in R$.

Lemma 17.6 (von Gauß, 1. Version)**.** *Seien $f, g \in R[X]$ primitiv, dann ist $f \cdot g$ primitiv.*

Beweis. Sei $p \in R$ prim. Nach 13.3 ist die Abbildung

$$\varphi : R[X] \to {}^{R}\!/_{\langle p \rangle}[X], \sum a_i X^i \mapsto \sum (a_i + \langle p \rangle) X^i$$

ein Ringhomomorphismus. Da f, g primitiv sind, folgt $\varphi(f) \neq 0$ und $\varphi(g) \neq 0$. Nach 15.2 und 16.6 ist ${}^{R}\!/_{\langle p \rangle}$ ein Integritätsbereich. Nach 13.8 ist ${}^{R}\!/_{\langle p \rangle}[X]$ ein Integritätsbereich. Damit folgt $\varphi(f \cdot g) = \varphi(f) \cdot \varphi(g) \neq 0$. Also ist $f \cdot g$ primitiv. □

Definition 17.7. Sei $f \in K[X]$. Sei $a \in R$ so, dass $af \in R[X]$. Definiere

$$c_K(f) \coloneqq \frac{c(af)}{a} ,$$

genannt Inhalt von f. Beispiel: $f \coloneqq \frac{5}{4}x + \frac{25}{6} = \frac{1}{12}(15x + 50) = \frac{5}{12}(3x + 10)$, wobei $3x + 10$ primitiv ist. Also ist $c_K(f) = \frac{5}{12}$.

Bemerkung 17.8.

(1) Ist $f \in R[X] \subseteq K[X]$, so gilt $c_K(f) = c(f)$, insbesondere ist die Definition von c_K also eine Fortsetzung der Definition des Inhaltes in 17.5 von $R[X]$ auf $K[X]$.

(2) Es ist $c_K(f)$ wohldefiniert: Seien $a, b \in R$ mit af und bf in $R[X]$. Mit 17.5 folgt $c(abf) = ac(bf) = bc(af)$, also

$$\frac{c(bf)}{b} = \frac{c(af)}{a} .$$

(3) Es gilt $c_K(f) \in R$ genau dann, wenn $f \in R[X]$.

Beweis. „⇐“ ist klar nach Definition.

„⇒“: Sei $c_K(f) = \frac{c(af)}{a} \in R$, dann folgt $a \mid c(af)$ in R. Damit teilt a jeden Koeffizienten aus af (in R). Somit ist $f \in R[X]$. □

(4) Beachte $\frac{af}{c(af)}$ ist primitiv. Der sogenannte *primitive Teil* f_0 von $f \in K[X]$ ist definiert durch

$$f_0 \coloneqq \frac{f}{c_K(f)} = \frac{f}{\left(\frac{c(af)}{a}\right)} = \frac{af}{c(af)} \in R[X].$$

Es ist also $f = c_K(f) \cdot f_0$. Diese Darstellung von f ist eindeutig bis auf Assoziiertheit: Sei $f = \frac{b}{d} f_0 = \frac{r}{s} f_0'$ mit $b, d, r, s \in R$ und $f_0, f_0' \in R[X]$ jeweils primitiv. Dann ist $sbf_0 = rdf_0'$. Da $c(sbf_0) = c(rdf_0')$ mit f_0 und f_0' jeweils primitiv, folgt $sb \sim rd$. Also exisitiert eine Einheit $u \in R^\times$ mit $sbu = rd$. Dann folgt $\frac{b}{d} \cdot u = \frac{r}{s}$ und $f_0' = u^{-1} f_0$.

Lemma 17.9 (von Gauß, 2. Version)**.** *Seien $f, g \in K[X]$, dann ist $c_K(f \cdot g) = c_K(f) \cdot c_K(g)$. Hierbei bedeutet Gleichheit in der letzten Gleichung, dass die Assoziertenklassen $c_K(f \cdot g)$ und $c_K(f) \cdot c_K(g)$ gleich sind, beziehungsweise die Elemente $c_K(f \cdot g)$ und $c_K(f) \cdot c_K(g)$ aus R assoziiert sind.*

Beweis. Es ist $f \cdot g = c_K(f)c_K(g)f_0 \cdot g_0$. Da $f_0, g_0 \in R[X]$ primitiv sind, folgt mit 17.6, dass $f_0 \cdot g_0 \in R[X]$ primitiv ist. Somit ist $c_K(f \cdot g) \sim c_K(f) \cdot c_K(g)$. □

Proposition 17.10. *Sei R faktoriell mit $K = \mathrm{Quot}(R)$. Sei $f \in R[X]$. Dann gilt:*

(a) Ist $f = g \cdot h$ eine Zerlegung mit $g, h \in K[X] \setminus K^\times$, dann ist $f \overset{17.9}{=} (c(f)g_0) \cdot h_0$ eine Zerlegung in $R[X]$. Insbesondere, ist f unzerlegbar in $R[X], \deg(f) \geq 1$, dann ist f unzerlegbar in $K[X]$.

(b) Ist f unzerlegbar in $K[X]$ und f primitiv, dann ist f unzerlegbar in $R[X]$.

(c) Sei $g \in R[X]$ mit $f \mid g$ in $K[X]$ und f primitiv, dann ist $f \mid g$ in $R[X]$.

(d) Sei f normiert und $g \in K[X]$ normiert mit $g \mid f$ in $K[X]$, dann ist $g \in R[X]$.

Zum Beispiel ist $f = 2X \in \mathbb{Z}[X]$ nicht primitiv, und unzerlegbar über $\mathbb{Q}$, aber zerlegbar über $\mathbb{Z}$.

Beweis.

(a) Es sei $f = g \cdot h$ mit $g, h \in K[X] \setminus K^\times$. Dann ist

$$f = g \cdot h = c_K(g) \cdot c_K(h) \cdot g_0 \cdot h_0 = \underbrace{(c(f) \cdot g_0)}_{\in R[X]} \cdot \underbrace{h_0}_{\in R[X]} .$$

Nach 17.8 (4) sind $g_0, h_0 \in R[X]$. Da $f \in R[X]$ ist $c_K(f) = c(f) \in R$ nach 17.8 (1). Damit ist f zerlegbar über R.

(b) Sei $f = g \cdot h$ mit $g, h \in R[X]$. Da f unzerlegbar über K ist, folgt g oder h ist in $K[X]^\times = K^\times$. Ohne Einschränkung sei $\deg(g) = 0$. Dann folgt $g \in R$. Da f primitiv ist, folgt $1 = c(f) = c(g)c(h) = g \cdot c(h)$, also $g \in R^\times$. Die letzte Gleichung ist eine Gleichung von Assoziiertenklassen. Also ist f unzerlegbar in $R[X]$.

(c) Übung.

(d) Übung. □

Bemerkung 17.11. Sei R ein Integritätsbereich und $a \in R$ unzerlegbar. Mit der Gradformel 13.7 folgt a unzerlegbar in $R[X]$: Angenommen $a = fg$ für $f, g \in R[X]$. Dann ist $0 = \deg a = \deg f + \deg g$, also $\deg f = \deg g = 0$. Damit sind $f, g \in R$. Da a unzerlegbar in R ist, muss f oder g eine Einheit in R sein. Da $R[X]^\times = R^\times$, folgt a ist unzerlegbar in $R[X]$.

Theorem 17.12. *Ist R faktoriell, dann ist $R[X]$ faktoriell. Die unzerlegbaren Elemente von $R[X]$ sind*

(i) unzerlegbare Elemente in R,

(ii) alle primitiven Polynome aus $R[X]$, die unzerlegbar in $K[X]$ sind.

Beweis.

(a) *Existenz*: Induktion über $\deg(f)$.

Sei also $\deg(f) = n \geq 1$. Schreibe $f = c(f) \cdot f_0$.

(i) Da R faktoriell ist, ist entweder $c(f) \in R^\times$ oder $c(f) = \prod f_i$ mit f_i unzerlegbar in R. Nach 17.11 sind die Elemente f_i unzerlegbar in $R[X]$.

(ii) Entweder ist f_0 unzerlegbar oder $f_0 = g \cdot h$ mit $g, h \in R[X] \setminus R^\times$, wobei $R[X]^\times = R^\times$. Angenommen, $g \in R$, so folgt $1 = c(f_0) = c(g)c(h) = gc(h)$ und damit $g \in R^\times = R[X]^\times$. Also ist $\deg(g) \neq 0$ und $\deg(h) \neq 0$, also $\deg(g) \leq n-1, \deg(h) \leq n-1$. Mit der Induktionsvoraussetzung folgt die Behauptung.

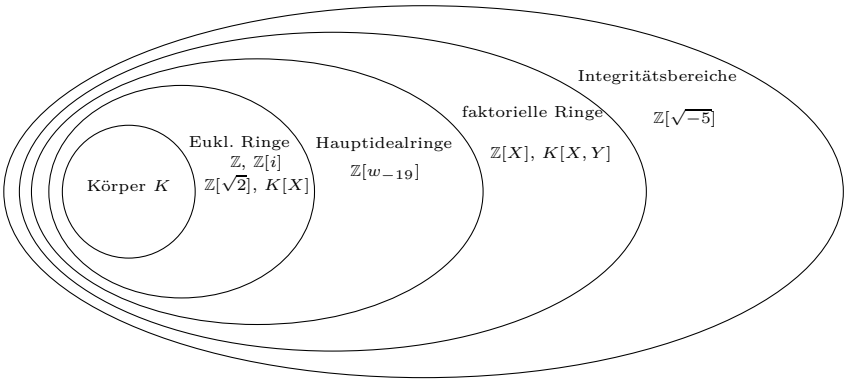
(b) *Eindeutigkeit*:

(i) Seien $f = c_1 \cdots c_k p_1 \cdots p_r = d_1 \cdots d_l q_1 \cdots q_s$ Faktorisierungen in unzerlegbare Elemente in $R[X]$, wobei p_i, q_j primitiv vom Grad ≥ 1 und $c_i, d_j \in R$ unzerlegbar sind. Dann sind nach 17.6 auch $p_1 \cdots p_r$ und $q_1 \cdots q_s$ primitiv und der Inhalt von f entspricht $c_1 \cdots c_k = u \cdot d_1 \cdots d_l$ mit $u \in R^\times$. Nach Voraussetzung ist R faktoriell, also folgt $k = l$ und nach Umsortierung $c_i \sim d_i$ für $1 \leq i \leq k$. Da $R[X]$ ein Integritätsbereich ist, folgt durch Kürzen, dass $p_1 \cdots p_r = \tilde{u} q_1 \cdots q_s$ mit $\tilde{u} \in R^\times$.

(ii) Nach Voraussetzung sind p_i, q_j unzerlegbar in $R[X]$, also sind nach 17.10(b) die Elemente p_i, q_j unzerlegbar in $K[X]$. Da $K[X]$ ein Hauptidealring ist, ist $K[X]$ faktoriell; also folgt aus $p_1 \cdots p_r = \tilde{u} q_1 \cdots q_s$, dass $r = s$ und nach Umsortierung $p_i \sim q_i$ in $K[X]$ für $1 \leq i \leq r$. Nach 16.1 folgt $p_i \mid q_i$ und $q_i \mid p_i$ in $K[X]$. Da p_i, q_i primitiv sind, folgt mit 17.10 (c), dass $p_i \mid q_i$ und $q_i \mid p_i$ in $R[X]$. Nach 16.1 ist damit $p_i \sim q_i$ in $R[X]$. □

Korollar 17.13. *Sei K ein beliebiger Körper und R ein faktorieller Ring. Dann sind $R[X_1, \ldots, X_n]$ und $K[X_1, \ldots, X_n]$ faktoriell.*

Die bewiesenen Zusammenhänge der letzten Kapitel zwischen den verschiedenen Arten von Ringen lassen sich diagrammatisch darstellen. Mit der Grafik angegeben sind jeweils Beispiele von Ringen, die in eine bestimmte Klasse von Ringen gehören.



Kapitel 18

Faktorisieren in Polynomringen

Sei R faktoriell mit Quotientenkörper $K = \mathrm{Quot}(R)$.

Definition 18.1. Ein Element $a \in R$ heißt *Nullstelle* von $f \in R[X]$, falls $f(a) = 0$.

Theorem 18.2. *Sei R faktoriell mit Quotientenkörper $K = \mathrm{Quot}(R)$ und sei $f \in R[X]$ mit $\deg f = n \geq 0$.*

(a) Dann ist $a \in R$ Nullstelle von f genau dann, wenn $f = (X - a)g$ mit $g \in R[X]$. In diesem Fall gibt es eine eindeutige Darstellung

$$f = (X - a)^m \cdot h, h \in R[X], h(a) \neq 0, m \in \mathbb{N} \ .$$

Die Zahl $m_{a,f} \coloneqq m$ heißt Vielfachheit *der Nullstelle a von f.*

(b) f hat höchstens n verschiedene Nullstellen.

Beweis. (a) Sei $f \in R[X] \subseteq K[X]$. Nach 14.6 ist $K[X]$ euklidisch. Sei $\deg f = n \geq 1$ und sei $a \in R$ eine Nullstelle von f. Dann existieren $g, r \in K[X]$ mit

$$f = (X - a) \cdot g + r \ ,$$

wobei $\deg(r) < \deg(X - a) = 1$. Damit folgt $r \in K$. Außerdem gilt $0 = f(a) = (a-a)g(a)+r$, also folgt $r = 0$. Dies zeigt $f = (X-a)g$ mit $g \in K[X]$. Das Polynom $X - a$ ist primitiv in $R[X]$ und $X - a \mid f$ in $K[X]$. Mit 17.10 folgt $X - a \mid f$ in $R[X]$. Durch Induktion existiert eine Darstellung von f als $f = (X - a)^m \cdot h$ mit $h \in R[X]$ und $h(a) \neq 0$. Die Eindeutigkeit von m (beziehungsweise der Darstellung von f) folgt aus $R[X]$ faktoriell.

(b) Wir führen eine Induktion nach $n = \deg f$ durch. Sei b eine Nullstelle von f mit $b \neq a$. Dann ist

$$0 = f(b) = \underbrace{(b - a)}_{\neq 0} g(b) \ ,$$

also $g(b) = 0$ und $\deg(g) \leq n-1$. Also hat g höchstens $n-1$ verschiedene Nullstellen, d. h. f hat höchstens n verschiedene Nullstellen. □

Zum Vergleich sei nochmals darauf hingewiesen, dass es andere Beispiele gibt: Der Ring $\mathbb{Z}_8$ ist kein Integritätsbereich, erfüllt also nicht die Voraussetzung von 18.2. Das Polynom $X^2 - 1 = (X - 1)(X + 1) = (X - 3)(X + 3)$ hat über $\mathbb{Z}_8$ vier verschiedene Nullstellen: ± 1 und ± 3. Das Polynom hat also auch keine eindeutige Faktorisierung in unzerlegbare Elemente.

Definition 18.3. Die formale Ableitung $Df = f'$ eines Polynoms $f = \sum_{i=0}^{n} a_i X^i$ ist definiert als

$$Df := f' := \sum_{i=1}^{n} i a_i X^{i-1} .$$

Hierbei ist

$$ia_i := \underbrace{a_i + \ldots + a_i}_{i \text{ mal}} .$$

Bemerkung: Aus der Analysis wissen wir, dass man die Vielfachheit einer Nullstelle über die Ableitung beschreiben kann. Dies lässt sich hier auch zeigen. Hierzu zeigt man, dass die üblichen Ableitungsregeln gelten. Der Mittelwertsatz in der Analysis impliziert, dass eine differenzierte Funktion identisch Null ist genau dann, wenn sie konstant war. Dies gilt hier nicht mehr. Zum Beispiel hat $f = X^p - 1$ die Ableitung $f' = pX^{p-1} = 0$ in $\mathbb{Z}_p[X]$.

Lemma 18.4. *Seien $f, g \in R[X]$ und $a, b \in R$. Dann ist*

(a) $D(af + bg) = aDf + bDg$, *(Linearität),*

(b) $D(f \cdot g) = D(f) \cdot g + f \cdot D(g)$ *(Produktregel).*

Um die Rechnung einfach zu halten, beweise man hierbei die Produktregel für Monome und nutze dann die Linearität der formalen Ableitung, um die allgemeine Produktregel zu beweisen.

Proposition 18.5. *Sei $f \in R[X]$. Ein Element $a \in R$ ist mehrfache Nullstelle von f, also $m_{a,f} \geq 2$, genau dann, wenn a gemeinsame Nullstelle von f und f' ist.*

Beweis. „⇐“: Sei $f(a) = 0$. Dann existiert $g \in R[X]$ mit $f = (X - a)g$ nach 18.2. Mit 18.4 folgt $f' = g + (X - a)g'$, also $0 = f'(a) = g(a)$. Folglich ist $g = (X - a)\tilde{g}$ für $\tilde{g} \in R[X]$ bzw. $f = (X - a)^2 \cdot \tilde{g}$. Also ist $m_{a,f} \geq 2$.
„⇒“: Sei $f = (X - a)^m \cdot g$ mit $m \geq 2$, $g \in R[X]$ und $g(a) \neq 0$ nach 18.2. Mit 18.4 folgt

$$f' = m(X - a)^{m-1} \cdot g + (X - a)^m \cdot g'$$

und damit $f'(a) = 0$. □

Beispiel 18.6.

(a) Nach dem Fundamentalsatz der Algebra sind die unzerlegbaren Elemente in $\mathbb{C}[X]$ die Polynome $aX + b$, mit $0 \neq a, b \in \mathbb{C}$.

(b) Sei $f = \sum_{i=0}^{n} \gamma_i X^i \in \mathbb{R}[X]$. Über $\mathbb{C}$ gilt $f = \gamma_n \prod_{i=1}^{n} (X - \alpha_i)$. Entweder ist $\alpha_i \in \mathbb{R}$ oder $\alpha_i \in \mathbb{C} \setminus \mathbb{R}$. Sei $\alpha \in \mathbb{C} \setminus \mathbb{R}$ mit $f(\alpha) = 0$. Dann ist

$$f(\overline{\alpha}) = \sum_{i=0}^{n} \gamma_i \overline{\alpha}^i = \overline{\sum_{i=0}^{n} \gamma_i \alpha^i} = \overline{f(\alpha)} = 0 .$$

Es gilt

$$(X - \alpha)(X - \overline{\alpha}) = X^2 + (-\alpha - \overline{\alpha})X + \alpha\overline{\alpha} = X^2 - \underbrace{2\,\mathrm{Re}(\alpha)}_{\in \mathbb{R}} X + \underbrace{|\alpha|^2}_{\in \mathbb{R}} \in \mathbb{R}[X] .$$

Also ist

$$f = \gamma_n \prod_{\substack{\alpha\in\mathbb{R}\\ f(\alpha)=0}} (X-\alpha) \prod_{\substack{\alpha\in\mathbb{C}\\ f(\alpha)=0\\ \mathrm{Im}(\alpha)>0}} (X^2 - 2\,\mathrm{Re}(\alpha) + |\alpha|^2)\ .$$

Unzerlegbare Elemente in $\mathbb{R}[X]$ sind also

- lineare Polynome mit Koeffizienten in $\mathbb{R}$;
- quadratische Polynome in $\mathbb{R}[X]$ mit negativer Diskriminante.

Bemerkung 18.7. Sei $F \in K[X]$ mit $\deg F \geq 1$. Dann existiert $a(=$ kgV(Nenner der Koeffizienten von $F)) \in R$ mit $f \coloneqq a \cdot F \in R[X]$. Angenommen f ist unzerlegbar in $R[X]$. Nach 17.10 ist dann auch f unzerlegbar in $K[X]$, und damit auch F unzerlegbar in $K[X]$. Wir studieren deshalb Unzerlegbarkeit von Polynomen im Folgenden über R.

Theorem 18.8 (Reduktionskriterium)**.** *Sei R faktorieller Ring, S ein Integritätsbereich und $\varphi : R \to S$ ein Ringhomomorphismus mit Fortsetzung $\phi : R[X] \to S[X]$, wobei $\phi(X) = X$ ist. Sei $f \in R[X]$ primitiv mit*

(i) $\deg f = \deg \phi(f)$,

(ii) $\phi(f)$ *unzerlegbar über* S,

Dann ist f unzerlegbar über R.

Beweis. Sei $f = g \cdot h$ mit $g, h \in R[X]$. Da ϕ Ringhomomorphismus, ist $\phi(f) = \phi(g) \cdot \phi(h)$. Mit der Gradformel 13.7 folgt

$$\deg g + \deg h = \deg f \overset{\text{(i)}}{=} \deg \phi(f) = \deg \phi(g) + \deg \phi(h).$$

Nach Definition von ϕ, ist $\deg \phi(g) \leq \deg g$ und $\deg \phi(h) \leq \deg h$. Also folgt $\deg \phi(g) = \deg g$ und $\deg \phi(h) = \deg h$. Da $\phi(f)$ nach Voraussetzung unzerlegbar ist, folgt $\phi(g) \in S^\times$ oder $\phi(h) \in S^\times$, wobei $S[X]^\times = S^\times$ nach 13.8. Ohne Einschränkung sei $\phi(g) \in S^\times$. Da $0 = \deg \phi(g) = \deg g$ ist, folgt $g \in R$. Da f primitiv ist, folgt $1 = c(f) = c(g) \cdot c(h) = g \cdot c(h)$ und damit $g \in R^\times$. Also ist f unzerlegbar in $R[X]$. □

Theorem 18.9 (Eisenstein-Kriterium)**.** *Sei R faktorieller Ring, $f = \sum_{i=0}^{n} a_i X^i \in R[X]$ primitiv mit $a_n \neq 0$. Sei $p \in R$ prim mit*

(i) $p \mid a_0, \ldots, p \mid a_{n-1}$,

(ii) $p \nmid a_n$,

(iii) $p^2 \nmid a_0$.

Dann ist f unzerlegbar in $R[X]$, also auch in $K[X]$.

Beweis. Sei $f = gh$ mit $g = \sum_{i=0}^{r} b_i X^i$ und $h = \sum_{i=0}^{s} c_i X^i$ wobei $r + s = n$. Um einen Widerspruch zu erhalten, nehmen wir an, dass $r, s \geq 1$ sind. Berechne die Koeffizienten a_u mittels der Koeffizienten b_i und c_j. Es ist $a_0 = b_0 \cdot c_0$. Nach Voraussetzung ist $p \mid b_0 c_0$ und $p^2 \nmid b_0 c_0$. Ohne Einschränkung sei $p \mid b_0$, also gilt $p \nmid c_0$. Nach Voraussetzung ist $p \mid a_1 = b_0 c_1 + b_1 c_0$, dann folgt $p \mid b_1$. Genauso folgt aus $p \mid a_2 = b_0 c_2 + b_1 c_1 + b_2 c_0$,

dass $p \mid b_2$ ist. Induktiv folgt aus $p \mid a_i$ für $0 \leq i \leq r < n$, dass $p \mid b_i$ für alle $0 \leq i \leq r$. Andererseits ist nach Voraussetzung $p \nmid a_n = b_r \cdot c_s \neq 0$, also $p \nmid b_r$; dies ist ein Widerspruch. Alternativ zur Induktion, definiere

$$t + 1 := \min\{i \mid 0 \leq i \leq r, p \nmid b_i\} \leq r.$$

Es ist

$$a_{t+1} = \sum_{j=0}^{t+1} b_j c_{t+1-j} = b_{t+1}c_0 + \sum_{j=0}^{t} b_j c_{t+1-j} \ .$$

Da $p \mid b_j$ für $0 \leq j \leq t$ und $p \nmid b_{t+1}c_0$ gilt, folgt $p \nmid a_{t+1}$. Dies ist ein Widerspruch zu (i), denn $t + 1 \leq r = n - s < n$. Also ist $r = 0$ oder $s = 0$. Ohne Einschränkung sei also $g = b_0$. Nach Voraussetzung ist f primitiv, also ist $b_0 \in R^\times$. Damit ist das Polynom f unzerlegbar. □

Beispiel 18.10. (1) Sei $f = 2X^4+10X^3+25X+30 \in \mathbb{Z}[X]$. Dann gelten die Voraussetzungen von 18.9, also $5 \nmid 2, 5 \mid 10, 5 \mid 25, 5 \mid 30$ und $25 \nmid 30$. Da $\mathrm{ggT}(2, 10, 25, 30) = 1$ gilt, folgt mit 18.9, dass f unzerlegbar in $\mathbb{Z}[X]$ ist.

(2) Sei $R = \mathbb{Z}, S = \mathbb{Z}_2$ und $\varphi : \mathbb{Z} \to \mathbb{Z}_2$ die natürliche Projektion. Sei $n \in \mathbb{Z}$ ungerade und $f = X^5 + nX^2 + 1 \in \mathbb{Z}[X]$. Da $c(f) = 1$ ist, ist f primitiv. Definiere die Fortsetzung von ϕ wie in 18.8 durch $\phi : \mathbb{Z}[X] \to \mathbb{Z}_2[X], \sum a_i X^i \mapsto \sum \overline{a_i} X^i$. Hierbei ist $\overline{a_i} = a_i \mod 2$. Dann ist

$$\phi(f) = X^5 + X^2 + 1 \in \mathbb{Z}_2[X] \ .$$

(a) Es ist $1^5 + 1^2 + 1 = 3 = 1$ in $\mathbb{Z}_2$ und $0^5 + 0^2 + 1 = 1$ in $\mathbb{Z}_2$. Also folgt, dass $\phi(f)$ keine Nullstelle in $\mathbb{Z}_2$ hat. Also hat $\phi(f)$ keinen linearen Faktor, ist also kein Produkt eines Polynoms vom Grad eins mit einem Polynom vom Grad vier.

(b) Angenommen, $\phi(f)$ hat einen quadratischen unzerlegbaren Teiler. Wir zählen alle quadratischen Polynome in $\mathbb{Z}_2[X]$ auf, und überprüfen, ob sie zerlegbar sind:

- $X^2 = X \cdot X$ ist nicht unzerlegbar;
- $X^2 + 1 = (X + 1)^2$ ist nicht unzerlegbar;
- $X^2 + X = X(X + 1)$ ist nicht unzerlegbar;
- $X^2 + X + 1$ ist unzerlegbar, da es keine Nullstelle in $\mathbb{Z}_2$ hat.

Division mit Rest zeigt, dass $X^2 + X + 1$ kein Teiler von $\phi(f) = X^5 + X^2 + 1$ über $\mathbb{Z}_2$ ist. Also lässt sich $\phi(f)$ nicht schreiben als Produkt eines Polynoms vom Grad zwei mit einem Polynom vom Grad drei.

Aus (a) und (b) folgt, dass $\phi(f)$ unzerlegbar ist. Mit 18.8 ist f unzerlegbar in $\mathbb{Z}[X]$ und nach dem Gauß-Lemma 17.10 damit auch unzerlegbar in $\mathbb{Q}[X]$.

Kapitel 19

Körpererweiterungen

In diesem Kapitel lernen wir die Grundlagen der Körpertheorie kennen. Als ein erstes Ziel wollen wir zeigen, dass jeder endliche Körper Primzahlpotenz viele Elemente hat.

Definition 19.1. Seien L und K Körper.

(a) Ist $K \leq L$ ein Teilring, so heißt K *Teilkörper* bzw. L heißt *Erweiterungskörper* bzw. $K \leq L$ heißt *Körpererweiterung* (KE). Schreibe hierfür L/K, gelesen „L über K“. Ein Körper M heißt *Zwischenkörper*, falls $K \leq M \leq L$ ist.

(b) Ein Ringhomomorphismus $\varphi : K \to L$ heißt *Körperhomomorphismus*. Nach 12.2 ist $\operatorname{Ker}(\varphi) = \{0\}$, also φ injektiv.

Bemerkung 19.2. Sei L/K eine Körpererweiterung. Dann ist L ein K-Vektorraum mit der Addition $+ : L \times L \to L$ von L und der Einschränkung $\cdot : K \times L \to L$ der Multiplikation von L. Schreibe $[L : K] \coloneqq \dim_K L$ für die K-Vektorraumdimension von L, genannt *Grad* der Körpererweiterung L/K. Eine Körpererweiterung L/K heißt *endlich*, falls $[L : K] < \infty$, sie heißt *unendlich*, falls $[L : K] = \infty$.

Beispiel 19.3. $[L : K] = 1$ impliziert $L = K$. Es gilt $[\mathbb{C} : \mathbb{R}] = 2$, da $\mathbb{C}$ als $\mathbb{R}$-Vektorraum die Basis $\{1, i\}$ hat. Es ist $[\mathbb{R} : \mathbb{Q}] = \infty$.

Bemerkung 19.4. Sei K ein Körper. Dann ist

$$\Pi(K) \coloneqq \bigcap_{K' \leq K} K'$$

der kleinste Teilkörper von K, genannt *Primkörper* von K.
Betrachte den Ringhomomorphismus $\gamma : \mathbb{Z} \to K, z \mapsto z \cdot 1_K$. Nach 11.3 ist $\mathbb{Z}/\operatorname{Ker}(\gamma) \simeq \operatorname{im}\gamma \leq K$ Teilring, also ist $\operatorname{im}\gamma$ ein Integritätsbereich. Nach 15.2 ist $\operatorname{Ker}\gamma \trianglelefteq \mathbb{Z}$ ein Primideal. Die Primideale von $\mathbb{Z}$ wurden in 15.3 klassifiziert. Wir unterscheiden zwei Fälle:

(a) Sei $\operatorname{Ker}\gamma = \{0\}$. Dann ist

$$n \cdot 1_K = \underbrace{1_k + \ldots + 1_k}_{n \text{ mal}} \neq 0$$

für alle $n \in \mathbb{N}$. Definiere

$$\gamma' : \mathbb{Q} \to K, \frac{a}{b} = ab^{-1} \mapsto \gamma(a)\gamma(b)^{-1} \ .$$

Dann ist γ' ein Körperhomomorphismus. Nach 19.1 ist γ' injektiv. Da $\mathbb{Q}$ keinen echten Teilkörper hat, folgt $\Pi(K) \simeq \mathbb{Q}$. Wir identifizieren $\gamma'(\mathbb{Q})$ mit $\mathbb{Q}$, haben damit also $\mathbb{Q} \leq K$.

(b) Sei $\operatorname{Ker}\gamma = p\mathbb{Z}$, mit p Primzahl. Dann ist

$$\underbrace{1_K + \ldots + 1_K}_{p \text{ mal}} = 0_K$$

und $\mathbb{Z}_p = \mathbb{Z}/p\mathbb{Z} \simeq \operatorname{im}\gamma \leq K$. Da $\mathbb{Z}_p$ keinen echten Teilkörper hat (dieser wäre eine Untergruppe von $\mathbb{Z}_p$, benutze Lagrange 2.12), folgt $\Pi(K) \simeq \mathbb{Z}_p$. Wir identifizieren $\gamma(\mathbb{Z})$ mit $\mathbb{Z}_p$, haben damit also $\mathbb{Z}_p \leq K$.

Definition 19.5. Sei R ein Ring mit 1. Definiere die *Charakteristik* $\operatorname{char} R$ als

$$\operatorname{char} R = \begin{cases} 0 & \text{, falls } n \cdot 1_R \neq 0 \text{ für alle } n \in \mathbb{N} \\ \min\{n \in \mathbb{N} \mid n \cdot 1_R = 0\} & \text{, sonst.} \end{cases}$$

Falls $R = K$ ein Körper ist, dann ist

$$\operatorname{char} K = \begin{cases} 0 & \text{, falls } \Pi(K) \simeq \mathbb{Q} \\ p & \text{, falls } \Pi(K) \simeq \mathbb{Z}_p. \end{cases}$$

Beispiel 19.6. Es ist $\operatorname{char}\mathbb{Z} = \operatorname{char}\mathbb{Q} = \operatorname{char}\mathbb{R} = \operatorname{char}\mathbb{C} = \operatorname{char}\mathbb{Z}[\sqrt{d}] = 0$. Ist $R \leq S$ Teilring, dann ist $\operatorname{char} R = \operatorname{char} S$. Es ist $\operatorname{char}\mathbb{Z}/n\mathbb{Z} = n$ für $n \in \mathbb{N}^{\geq 2}$.
Sei $I \trianglelefteq K[X]$ maximal, K ein Körper mit $\operatorname{char} K = p$ prim, dann folgt

$$\operatorname{char}\left(K[X]/I\right) = p \ .$$

Es ist $p \cdot (1 + I) = p \cdot 1 + I = 0 + I$. Angenommen es existiert eine Primzahl $q < p$ mit $q \cdot (1 + I) = 0 + I$. Dann ist $q \in I$. Ausserdem ist $0 \neq q \in \mathbb{Z}_p \leq K$, weshalb q eine Einheit in K ist. Aus $q \in I$ folgt damit $I = K[X]$, ein Widerspruch.

Theorem 19.7. *Jeder endliche Körper K hat Primzahlpotenz viele Elemente: $|K| = p^n$, wobei p eine Primzahl ist und $n \in \mathbb{N}$.*

Beweis. Da $|K| < \infty$ ist, ist $\Pi(K) \simeq \mathbb{Z}_p$ für eine Primzahl p. Nach 19.2 ist K ein $\mathbb{Z}_p$-Vektorraum, also existiert eine $\mathbb{Z}_p$-Basis $\{v_1, \ldots, v_n\}$ von K. Damit folgt

$$K = \left\{ \sum_{i=1}^{n} \lambda_i v_i \mid \lambda_i \in \mathbb{Z}_p \right\} \ .$$

Also $|K| = p^n$. □

Theorem 19.8 (Gradformel)**.** *Sei $K \leq L \leq M$ Körpererweiterung.*

(a) M/K ist endlich genau dann, wenn M/L und L/K endlich sind. In diesem Fall gilt:

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

(b) Ist $\{b_1, \dots b_m\}$ eine L-Basis von M und $\{a_1, \dots, a_l\}$ eine K-Basis von L, dann ist

$$S \coloneqq \{a_j b_i \mid 1 \leq j \leq l, 1 \leq i \leq m\}$$

eine K-Basis von M.

Beweis. (i) Ist M/L unendlich, so existiert eine unendliche Menge von Vektoren in M, die linear unabhängig sind über L. Dann sind diese Vektoren erst recht linear unabhängig über K. Ist L/K unendlich, so existiert eine unendliche Menge von Vektoren in L, die linear unabhängig sind über K. Da $L \subseteq M$, existieren unendlich viele Vektoren in M, die linear unabhängig sind über K. Zusammen mit Aussage (b) impliziert dies Aussage (a).

(ii) Sei $x \in M$, dann existiert $\lambda_i \in L$ mit $x = \sum_{i=1}^{m} \lambda_i b_i$. Da $\lambda_i \in L$ gilt, existieren $\mu_{ij} \in K$ mit

$$x = \sum_{i=1}^{m} \left(\sum_{j=1}^{l} \mu_{ij} a_j \right) b_i \ .$$

Also folgt $x \in \mathrm{Span}_K(S)$.

(iii) Sei $0 = \sum_{i=1}^{m} \sum_{j=1}^{l} \mu_{ij} a_j b_i = \sum_{i=1}^{m} \left(\sum_{j=1}^{l} \mu_{ij} a_j \right) b_i$ mit $\mu_{ij} \in K$. Da $\sum_{j=1}^{l} \mu_{ij} a_j \in L$, und die Vektoren $\{b_1, \dots, b_m\}$ nach Voraussetzung linear unabhängig sind über L, folgt $\sum_{j=1}^{l} \mu_{ij} a_j = 0$ für alle i. Da $\{a_1, \dots, a_l\}$ linear unabhängig über K ist, folgt $\mu_{ij} = 0$ für alle i, j. Also ist S linear unabhängig über K. □

Bemerkung 19.9. Sei L/K eine Körpererweiterung. Sei $a \in L$. Nach 13.5 ist

$$K[a] = \{\sum_{i=0}^{n} \lambda_i a^i \mid n \in \mathbb{N}_0, \lambda_i \in K\} = \{f(a) \mid f \in K[X]\} \subseteq L \ .$$

Es ist $K[a]$ der kleinste Ring, der K und a enthält. Als Teilmenge eines Körpers L ist $K[a]$ ein Integritätsbereich. Definiere

$$K(a) \coloneqq \mathrm{Quot}(K[a]) = \left\{ \frac{f(a)}{g(a)} \mid f, g \in K[X], g(a) \neq 0 \right\} \ ,$$

vgl. 12.9. Dann ist $K(a)$ der kleinste Körper, der K und a enthält.

Definition 19.10. Sei L/K eine Körpererweiterung und $S \subseteq L$.

(a) Definiere $K[S]$ als kleinsten Teilring von L, der K und S enthält, d. h.

$$K[S] = \bigcap_{\substack{K \leq R \leq L \text{ Teilring} \\ S \subseteq R}} R \ .$$

Wir sagen, $K[S]$ entsteht aus K durch *Ringadjunktion von S*.

(b) Definiere $K(S)$ als kleinsten Teilkörper von L, der K und S enthält, d. h.

$$K(S) = \bigcap_{\substack{K \leq K' \leq L \text{ Teilkörper} \\ S \subseteq K'}} K' = \mathrm{Quot}(K[S]) \ .$$

Wir sagen, $K(S)$ entsteht aus K durch *Körperadjunktion* von S.

Bemerkung 19.11.

(a) Sei L/K Körpererweiterung mit $S_1, S_2 \subseteq L$. Dann ist $K[S_1][S_2] = K[S_1 \cup S_2]$ und $K(S_1)(S_2) = K(S_1 \cup S_2)$.

Ist $S = \{a_1, \ldots, a_n\} \subseteq L$, dann schreibe

$$K[S] = K[a_1, \ldots, a_n] = K[a_i \mid 1 \leq i \leq n]$$
$$K(S) = K(a_1, \ldots, a_n) = K(a_i \mid 1 \leq i \leq n) \ .$$

(b) Eine Körpererweiterung L/K heißt *endlich erzeugt*, falls es $S \subseteq L$ endlich gibt mit $L = K(S)$. Jede endliche Körpererweiterung L/K ist endlich erzeugt: Sei $\{v_1, \ldots, v_n\}$ eine K-Basis von L, dann folgt

$$L = \{\sum_{i=1}^{n} \lambda_i v_i \mid \lambda_i \in K\} \subseteq K(v_1, \ldots, v_n) \subseteq L,$$

also ist $L = K(v_i \mid 1 \leq i \leq n)$.

Beispiel 19.12. Aus dem Beweis von 14.5 folgt $\mathbb{Q}[\sqrt{d}] = \{a + b\sqrt{d} \mid a, b \in \mathbb{Q}\} = \mathbb{Q}(\sqrt{d})$.

(a) Sei $K \coloneqq \mathbb{Q}(\sqrt{2}), L = K(\sqrt{3}) = \mathbb{Q}(\sqrt{2}, \sqrt{3})$. Man kann leicht nachrechnen, dass $\sqrt{3} \notin \mathbb{Q}(\sqrt{2}) = K$ ist. Sei $0 \neq x \in K[\sqrt{3}] = \{\alpha + \beta\sqrt{3} \mid \alpha, \beta \in K\}$. Sei $x = \alpha + \beta\sqrt{3}$. Dann folgt

$$x^{-1} = \underbrace{\frac{\alpha}{\alpha^2 - 3\beta^2}}_{\in K} - \underbrace{\frac{\beta}{\alpha^2 - 3\beta^2}}_{\in K} \cdot \sqrt{3} \in K[\sqrt{3}] \ .$$

Hierbei ist $\alpha^2 - 3\beta^2 = (\alpha + \beta\sqrt{3})(\alpha - \beta\sqrt{3}) \neq 0$. Damit ist jedes Element in $K[\sqrt{3}]$ invertierbar, also ist $L = K(\sqrt{3}) = K[\sqrt{3}]$.

(b) Körper $K = \mathbb{Q}(\sqrt{2})$ hat die $\mathbb{Q}$-Basis $\{1, \sqrt{2}\}$. Körper $L = K(\sqrt{3})$ hat die K-Basis $\{1, \sqrt{3}\}$. Nach 19.8 folgt, dass $\{1, \sqrt{2}, \sqrt{3}, \sqrt{6}\}$ eine $\mathbb{Q}$-Basis von L ist.

Definition 19.13. Sei L/K eine Körpererweiterung. Ein Element $a \in L$ heißt *algebraisch* über K, falls $0 \neq f \in K[X]$ existiert mit $f(a) = 0$. Andernfalls heißt a *transzendent* über K.

Lemma 19.14. *Sei L/K Körpererweiterung. Dann ist $a \in L$ algebraisch über K genau dann, wenn $\{a^i \mid i \in \mathbb{N}_0\}$ linear abhängig ist.*

Beweis.

(a) Sei $a \in L$ algebraisch über K. Nach 19.3 existiert dann $0 \neq f \in K[X]$ mit $f(a) = 0$. Sei $f = \sum_{i=0}^{n} \lambda_i X^i$ mit $\lambda_i \in K$. Dann folgt $0 = \sum_{i=0}^{n} \lambda_i a^i$, wobei nicht alle λ_i Null sind. Also ist $\{1, a, a^2, \ldots, a^n\}$ linear abhängig und damit auch $\{a^i \mid i \in \mathbb{N}_0\}$.

(b) Angenommen, $\{a^i \mid i \in \mathbb{N}_0\} \subseteq L$ ist linear abhängig über K. Dann existiert eine endliche Teilmenge in $\{a^i \mid i \in \mathbb{N}_0\}$, die linear abhängig ist. Also existiert $k \in \mathbb{N}$, sodass $\{1, a, a^2, \ldots, a^k\} \subseteq L$ linear abhängig ist. Also existieren $\lambda_i \in K$, die nicht alle Null sind, mit

$$0 = \lambda_0 \cdot 1 + \lambda_1 \cdot a + \lambda_2 \cdot a^2 + \ldots + \lambda_k a^k \ .$$

Setze $f \coloneqq \sum_i \lambda_i X^i \in K[X]$, dann ist $f \neq 0$ und $f(a) = 0$. Nach 19.13 ist a algebraisch über K.

□

Beispiel 19.15.

(a) Es ist $\sqrt{2} \in \mathbb{R}$ ist eine Nullstelle von $X^2 - 2 \in \mathbb{Q}[X]$. Also ist $\sqrt{2}$ algebraisch über $\mathbb{Q}$.

(b) Sei $z \in \mathbb{C}$. Dann ist z eine Nullstelle von $f = (X - z)(X - \overline{z}) = X^2 - 2\,\mathrm{Re}(z) + |z|^2 \in \mathbb{R}[X]$, also ist jede komplexe Zahl z algebraisch über $\mathbb{R}$.

(c) Sei $K < L < M$ Körpererweiterung, und sei $a \in M$ algebraisch über K. Nach Definition existiert also ein Polynom $f \in K[X]$ mit $f(a) = 0$. Da $K[X] \subseteq L[X]$, ist $f \in L[X]$ mit Nullstelle a. Also ist auch a algebraisch über L.

(d) Man bezeichnet $\overline{\mathbb{Q}} \coloneqq \{a \in \mathbb{C} \mid a \text{ algebraisch über } \mathbb{Q}\}$ als Menge aller *algebraischen Zahlen* und $\mathbb{C} \setminus \overline{Q}$ als Menge aller *transzendenten Zahlen*. Es gibt überabzählbar viele transzendente Zahlen, zum Beispiel sind $e, \pi, \sum_{n=1}^{\infty} 10^{-n!}$ transzendent.

Beweis. $\mathbb{Q}$ ist abzählbar, also gibt es abzählbar viele Polynome $f \in \mathbb{Q}[X], f = \sum_{i=0}^{n} a_i X^i$ mit $\deg f = n \in \mathbb{N}$. Jedes Polynom $0 \neq f = \sum_{i=0}^{n} a_i X^i$ vom Grad n hat höchstens n Nullstellen in $\mathbb{C}$. Da $\mathbb{N}$ abzählbar ist, gibt es daher nur abzählbar viele algebraische Elemente. Somit ist $\mathbb{C} \setminus \overline{\mathbb{Q}}$ überabzählbar. □

Kapitel 20

Einfache Körpererweiterungen

Das Polynom $X^2 - 2$ hat keine Nullstelle über den rationalen Zahlen $K \coloneqq \mathbb{Q}$. Erweitert man den Zahlenbereich zum Beispiel zu $L \coloneqq \mathbb{Q}[\sqrt{2}]$, dann hat $X^2 - 2$ eine Nullstelle im Erweiterungskörper L von K. Genauso, das Polynom X^2+1 hat keine Nullstelle in $K \coloneqq \mathbb{Q}$, aber es besitzt eine Nullstelle im Erweiterungskörper $L \coloneqq \mathbb{Q}[\sqrt{i}]$ von K. Zunächst wollen wir in diesem Kapitel einfache Körpererweiterungen verstehen. Als Anwendung zeigen wir, dass es zu jedem unzerlegbaren Polynom über K einen Erweiterungskörper L gibt, in dem dieses Polynom eine Nullstelle besitzt. Es sei immer L/K eine Körpererweiterung.

Definition 20.1. Sei $a \in L$ algebraisch über K. Das *Minimalpolynom $m_{a,K}$ von a über K* ist das normierte Polynom kleinsten Grades in $K[X]$ mit $m_{a,K}(a) = 0$. Wir schreiben $[a : K] \coloneqq \deg(m)$.

Proposition 20.2. *Sei $a \in L$ algebraisch über K.*

(a) Das Minimalpolynom $m_{a,K}$ existiert und ist eindeutig bestimmt.

(b) Für $f \in K[X]$ gilt: $f(a) = 0 \Leftrightarrow m_{a,K} \mid f$ in $K[X]$.

(c) $m_{a,K}$ ist unzerlegbar in $K[X]$.

Beweis. Sei $m \coloneqq m_{a,K}$.

(i) Existenz: Da a algebraisch ist über K, existiert $0 \neq g \in K[X]$ mit $g(a) = 0$. Wähle ein solches Polynom kleinsten Grades und multipliziere es mit dem Inversen des Leitkoeffizienten.

(ii) Sei $f \in K[X]$ mit $f(a) = 0$. Dann existieren $q, r \in K[X]$ mit $f = q \cdot m + r$ und $\deg r < \deg m$. Dann folgt $0 = r(a)$. Da m Minimalpolynom ist, also minimalen Grades ist mit Nullstelle a, folgt $r = 0$. Also ist $f = q \cdot m$, d. h. $m \mid f$ in $K[X]$.

(iii) Seien m_1, m_2 Minimalpolynome von a über K. Dann folgt $m_1(a) = 0 = m_2(a)$. Sei $p \coloneqq m_1 - m_2$, dann ist $\deg(p) < \deg(m_1)$, da m_1 und m_2 gleichen Grades sind, beide mit Leitkoeffizient Eins. Außerdem ist $p(a) = 0$. Angenommen, $p \neq 0$, dann folgt nach Normierung von p ein Widerspruch zu m_1 Minimalpolynom. Also ist $p = 0$, und damit $m_1 = m_2$.

(iv) Sei $m = r \cdot s$ mit $r, s \in K[X]$ und $\deg r, \deg s < m$. Dann folgt

$$0 = m(a) = \underbrace{r(a)}_{\in L} \cdot \underbrace{s(a)}_{\in L} .$$

Da L ein Integritätsbereich ist, folgt $r(a) = 0$ oder $s(a) = 0$. Nach Normierung von r oder s ergibt dies einen Widerspruch zu m Minimalpolynom. □

Definition 20.3. Eine Körpererweiterung L/K heißt *einfach*, falls es ein Element $a \in L$ gibt mit $L = K(a)$. Das Element a heißt dann *primitiv*.

Theorem 20.4. *Sei L/K eine Körpererweiterung.*

(a) Sei $a \in L$ transzendent über K. Dann gilt:

(i) $K(a) \simeq K(X) \overset{12.10}{=} \mathrm{Quot}(K[X]) = \left\{\frac{f}{g} \mid f, g \in K[X], g \neq 0\right\}$.

(ii) $[K(a) : K] = \infty$.

(b) Sei $a \in L$ algebraisch über K mit Minimalpolynom $m = m_{a,K}$. Dann gilt

(i) $K(a) = K[a] \simeq {}^{K[X]}\!/_{\langle m \rangle}$;

(ii) $[K(a) : K] = \deg(m) = [a : K] =: n$;

(iii) $\{1, a, a^2, \ldots, a^{n-1}\}$ *ist eine K-Basis von $K[a]$.*

Bemerkung 20.5.

(a) Sei $0 \neq f \in K[X]$ unzerlegbar mit $f(a) = 0$. Nach 20.2 (b) ist dann $f = \lambda \cdot m_{a,K}$ mit $\lambda \in K^\times$. Es folgt $\langle f \rangle = \langle m \rangle$, also $K[a] \simeq {}^{K[X]}\!/_{\langle f \rangle}$.

(b) Ist a transzendent, dann ist $K(X)/K$ endlich erzeugt, aber $[K(X) : K] = \infty$. Eine endlich erzeugte Körpererweiterung ist also nicht notwendigerweise endlich, siehe 19.11 (b).

Beweis von 20.4.

(a) (i) Sei $a \in L$ transzendent über K. Dann ist die Menge $\{1, a, a^2, \ldots\}$ linear unabhängig, also $[K(a) : K] = \infty$.

(ii) Die Abbildung $\psi : K[X] \to K[a], f \mapsto f(a)$ ist ein surjektiver Ringhomomorphismus. Da a transzendent ist, ist $f(a) \neq 0$ für alle $0 \neq f \in K[X]$. Damit ist $\operatorname{Ker} \psi = \{0\}$, also ist ψ ein Isomorphismus. Damit folgt

$$K(a) \overset{19.9}{=} \mathrm{Quot}(K[a]) \simeq \mathrm{Quot}(K[X]) \overset{12.10}{=} K(X) \ .$$

(b) (i) Die Abbildung $\psi : K[X] \to K[a], f \mapsto f(a)$ ist ein Epimorphismus mit $\operatorname{Ker} \psi = \langle m \rangle$ nach 20.2 (b). Es folgt

$$K[a] = \operatorname{im} \psi \overset{11.3}{\simeq} {}^{K[X]}\!/_{\operatorname{Ker} \psi} = {}^{K[X]}\!/_{\langle m \rangle} \ .$$

Nach 20.2 (c) ist m unzerlegbar. Da $K[X]$ ein Hauptidealring ist, folgt nach 16.6, dass $\langle m \rangle \trianglelefteq K[X]$ maximal ist. Nach 15.2 ist damit $K[a] \simeq {}^{K[X]}\!/_{\langle m \rangle}$ ein Körper, also $K[a] = K(a)$.

(ii) Sei $n = \deg(m)$. Dann ist $B \coloneqq \{1, a, a^2, \ldots, a^{n-1}\}$ linear unabhängig über K. Für $b \in K(a)$ existiert $f \in K[X]$ mit $b = f(a)$. Schreibe $f = q \cdot m + r$ mit $\deg(r) < \deg(m) = n$. Dann ist $b = f(a) = q(a)m(a) + r(a) = r(a) \in \mathrm{Span}_K(B)$. Also ist B eine K-Basis von $K[a]$. □

Definition 20.6. Eine Körpererweiterung L/K heißt *algebraisch*, falls alle $a \in L$ algebraisch über K sind. Eine Körpererweiterung L/K ist transzendent, falls es ein $a \in L$ gibt, welches transzendent über K ist.

Beispiel 20.7.

(a) Jede endliche Körpererweiterung L/K ist algebraisch: Sei $a \in L$ transzendent über K. Mit 20.4 folgt $[K(a) : K] = \infty$. Da $K \subseteq K(a) \subseteq L$ ist, folgt L/K unendlich nach 19.8.

(b) Betrachte $\sqrt{d} \in \mathbb{R}$ mit d quadratfrei. Dann ist $\sqrt{d}$ eine Nullstelle von $X^2 - d \in \mathbb{Q}[X]$ und somit

$$[\mathbb{Q}[\sqrt{d}] : \mathbb{Q}] = \deg(m_{\sqrt{d},\mathbb{Q}}) = 2 \ .$$

Daher ist $\mathbb{Q}[\sqrt{d}]/\mathbb{Q}$ algebraisch.

Theorem 20.8. *Sei $K \leq L \leq M$ Körpererweiterung. Dann gilt:*

(a) L/K endlich $\Leftrightarrow \exists a_1, \ldots, a_n \in L$ algebraisch mit $L = K(a_1, \ldots, a_n)$.

(b) M/K algebraisch $\Leftrightarrow$ M/L und L/K algebraisch.

Beweis.

(a) (i) Aus L/K endlich folgt nach 19.11, dass L/K endlich erzeugt ist und nach 20.7, dass L/K algebraisch ist.

(ii) Seien $a_1, \ldots, a_n \in L$ algebraisch über K mit $L = K(a_1, \ldots, a_n)$. Da a_i algebraisch ist über K, ist a_i auch algebraisch über $K(a_1, \ldots, a_{i-1})$, siehe 19.15. Daher ist

$$K(a_1, \ldots, a_{i-1})(a_i)/K(a_1, \ldots, a_{i-1})$$

endlich nach 20.4 (b). Wir erhalten eine endliche Kette von Körpererweiterung:

$$K \subseteq K(a_1) \subseteq K(a_1)(a_2) = K(a_1, a_2) \subseteq \ldots \subseteq K(a_1, \ldots, a_n) = L \ ,$$

wobei jede einzelne Erweiterung endlich ist. Mit 19.8 folgt induktiv, dass L/K endlich ist.

(b) (i) Sei M/K algebraisch.

- Nach Definition 20.6 ist a algebraisch über K für alle $a \in M$. Wegen $K[X] \subseteq L[X]$ ist damit a algebraisch über L für alle $a \in M$. Nach 20.6 ist M/L algebraisch.
- Sei $a \in L$. Da $L \subseteq M$ gilt, ist $a \in M$. Dann ist a algebraisch über K. Nach Definition 20.6 ist damit L/K algebraisch.

(ii) Seien M/L und L/K algebraisch. Sei $a \in M$. Dann ist a algebraisch über L. Sei $m_{a,L}$ das Minimalpolynom von a über L, also

$$m_{a,L} = X^n + b_{n-1}X^{n-1} + \ldots + b_1X + b_0$$

mit $b_i \in L$. Nach Voraussetzung ist b_i algebraisch über K. Betrachte

$$K \subseteq K(b_1, \ldots, b_{n-1}) \subseteq K(b_0, \ldots, b_{n-1}, a).$$

Da die b_i algebraisch über K sind, ist nach (a) die erste Körpererweiterung in der Kette endlich. Die zweite Körpererweiterung in der Kette ist endlich nach 20.4, da a algebraisch über $K(b_0, \ldots, b_{n-1})$ ist. Nach 19.8 ist $K(b_0, \ldots, b_{n-1}, a)/K$ damit endlich, nach 20.7 also algebraisch. Damit ist a algebraisch über K, für jedes $a \in M$. Also ist M/K algebraisch. □

Theorem 20.9 (Satz von Kronecker)**.** *Sei K ein Körper und $f \in K[X]$ unzerlegbar. Dann existiert eine algebraische Körpererweiterung L/K, so dass f eine Nullstelle a in L hat und $L = K(a)$ ist. Insbesondere ist $[L : K] = \deg(f)$.*

Beweis.

(a) Nach 14.6 und 16.6 ist $\langle f \rangle \trianglelefteq K[X]$ maximal. Nach 15.2 ist damit $L \coloneqq {}^{K[X]}\!/_{\langle f \rangle}$ ein Körper. Sei

$$\pi : K[X] \mapsto L = {}^{K[X]}\!/_{\langle f \rangle}, \text{ mit } g \mapsto g + \langle f \rangle$$

die kanonische Projektion. Die Einschränkung eines Ringhomomorphismus ist wieder ein Ringhomomorphismus. Also ist $\pi_K : K \to L$ ein Körperhomomorphismus. Nach 19.1 ist $\pi|_K$ injektiv. Identifiziere $\pi(K)$ mit K, d. h. $K \leq L$ und $\pi(b) = b$ für alle $b \in K$.

(b) Sei $a \coloneqq \pi(X) = X + \langle f \rangle \in L$. Sei $f = \sum b_i X^i$ und $b_i \in K$. Wir benutzen, dass π ein Homomorphismus ist. Dann ist

$$\begin{aligned} f(a) &= \sum b_i \pi(X)^i = \sum \pi(b_i)\pi(X)^i = \pi\left(\sum b_i X^i\right) \\ &= \pi(f) = f + \langle f \rangle = 0 + \langle f \rangle = 0_L \ . \end{aligned}$$

Also ist $a \in L$ eine Nullstelle des Polynoms f.

(c) Es ist f unzerlegbar in $K[X]$ mit Nullstelle $a \in L$. Nach 20.4 und 20.5 ist damit

$${}^{K[X]}\!/_{\langle f \rangle} = {}^{K[X]}\!/_{\langle m_{a,K} \rangle} \simeq K[a].$$

Da a algebraisch ist über K, folgt mit 20.7, dass $L \simeq K[a]$ algebraisch ist. Außerdem ist $[L : K] = \deg(m_{a,K}) = \deg(f)$. □

Kapitel 21

Konstruktionen mit Zirkel und Lineal

In diesem Kapitel betrachten wir eine Anwendung der bisherigen Körpertheorie: Welche geometrischen Figuren in der Ebene lassen sich – in endlich vielen Schritten – mit Zirkel und Lineal konstruieren? Die klassischen Probleme sind:

1. Delisches Problem: Läßt sich zu einem Würfel der Seitenlänge eins, mit Zirkel und Lineal, ein Würfel doppelten Volumens konstruieren?

2. Quadratur des Kreises: Lässt sich zu einem gegebenen Kreis, mit Zirkel und Lineal, ein Quadrat gleichen Flächeninhalts konstruieren?

3. Lässt sich ein beliebiger Winkel mit Zirkel und Lineal in drei gleiche Teile zerlegen?

4. Lässt sich zu einer gegebenen natürlichen Zahl n mit Zirkel und Lineal ein regelmäßiges n-Eck konstruieren?

Identifiziere die Zeichenebene $\mathbb{R}^2$ mit $\mathbb{C}$. Um etwas konstruieren zu können, müssen mindestens zwei Punkte gegeben sein. Ohne Einschränkung bezeichnen wir diese Punkte als 0 und 1. Elementare Operationen bei Konstruktionen mit Zirkel und Lineal (ohne Maßeinheiten) sind:

(i) Zeichne eine Gerade $g(P, Q)$ durch zwei gegebene Punkte P, Q.

(ii) Zeichne einen Kreis $k(P, Q)$ bzw. $k(P, r)$ mit Mittelpunkt P durch Q bzw. mit Radius $r = |Q_1Q_2|$, wobei P, Q, Q_1, Q_2 gegebene Punkte sind.

Ein elementarer Konstruktionsschritt besteht dann aus dem Schneiden zweier Geraden, zweier Kreise oder einer Geraden mit einem Kreis. Hierdurch werden bis zu zwei neue Punkte konstruiert.

Definition 21.1. Gegeben ist $\{0, 1\} \subseteq M \subseteq \mathbb{C}$. Eine Zahl $z = x+iy \in \mathbb{C}$ heißt *konstruierbar*, falls (x, y) konstruierbar ist, d. h. genau dann, falls (x, y) in endlich vielen elementaren Konstruktionsschritten aus M konstruiert werden kann. Schreibe $\hat{M}$ für die Menge aller aus M konstruierbaren Punkte. Außerdem schreiben wir $\overline{M} = \{\overline{z} \in \mathbb{C} \mid z \in M\}$, wobei $\overline{z}$ das komplex Konjugierte zu z ist.

Proposition 21.2. *Sei $\{0,1\} \subseteq M \subseteq \mathbb{C}$ gegeben. Dann gilt:*

(a) $\hat{M}$ ist ein Körper mit $\mathbb{Q} \leq \hat{M} \leq \mathbb{C}$;

(b) $z \in \hat{M} \Rightarrow \overline{z} \in \hat{M}$;

(c) $z \in \hat{M} \Rightarrow \sqrt{z} \in \hat{M}$.

Beweis. Zeichne die Gerade durch die gegebenen Punkte 0 und 1. Dies entspricht der x-Achse im Koordinatensystem. Zeichen eine Senkrechte durch den Punkt 0. Dies entspricht der y-Achse. Wir bezeichnen im Folgenden konstruierte Punkte durch die entsprechende komplexe Zahl in diesem Koordinatensystem. Aus der Schule wissen wir, wie man mit Zirkel und Lineal einen Winkel halbiert, und wie man eine Senkrechte auf eine gegebene Gerade durch einen gegebenen Punkt konstruiert. Seien nun $z_1, z_2 \in \hat{M}$.

(i) Addition/Subtraktion: Für $-z_1$ schneide die Gerade durch 0 und z_1 mit dem Kreis mit Mittelpunkt 0 durch z_1. Für $z_1 + z_2$ schneide Kreise mit Mittelpunkt z_1 und Radius $|0z_2| = |z_2|$ bzw. Mittelpunkt z_2 und Radius $|0z_1| = |z_1|$. Damit sind also $-z_1$ und $z_1 + z_2$ in $\hat{M}$.

(ii) Komplexe Konjugation: Zeichne die Senkrechte auf die x-Achse durch den gegebenen Punkt $z_1 = a + bi \in M$. Diese schneidet die x-Achse in b. Ein Kreis um b durch z_1 schneidet diese Senkrechte in z_1 und $\overline{z_1}$.

(iii) Multiplikation: Schreibe die gegebenen komplexen Zahlen in Polarkoordinaten, etwa $z_j = r_j e^{i\varphi_j}$ für $j \in \{1,2\}$. Dann ist

$$z_1 z_2 = r_1 \cdot r_2 e^{i(\varphi_1 + \varphi_2)}$$

Um das Produkt zweier komplexen Zahlen z_1 und z_2 mit Zirkel und Lineal zu konstruieren, muss man also zum einen die gegebenen Winkel φ_1 und φ_2 mit Zirkel und Lineal addieren, zum anderen muss man die Multiplikation der gegebenen Längen r_1 und r_2 der Vektoren z_1 und z_2 konstruieren. Wie man zwei gegebene Winkel mit Zirkel und Lineal addiert, sei dem Leser überlassen.

Die Multiplikation der positiven reellen Zahlen r_1 und r_2 geht wie folgt: Trage mit dem Zirkel die gegebene Zahl r_1 auf der x-Achse ab. Zeichne die Senkrechte durch 1, und trage mit dem Zirkel auf dieser die gegebene Zahl r_2 ab. Im Koordinatensystem haben wir damit die komplexe Zahl $1 + ir_2$ konstruiert. Zeichne eine Gerade l durch 0 und $1 + ir_2$. Zeichne die Senkrechte durch die Zahl r_1 auf der x-Achse. Diese schneidet die Gerade l in einem Punkt. Mit dem Strahlensatz folgt, dass dieser Punkt der komplexen Zahl $r_1 + i(r_1 r_2)$ entspricht. Damit ist $r_1 \cdot r_2 \in \hat{M}$.

(iv) Division: Sei $0 \neq z = re^{i\varphi}$. Dann ist $z^{-1} = r^{-1}e^{-i\varphi}$. Wir müssen also r^{-1} aus einer gegebenen positiven reellen Zahl r konstruieren. Zeichne die Gerade durch 0 und 1, also die x-Achse. Trage die Zahl r auf der x-Achse ab. Zeichne die Senkrechte durch r und trage auf dieser eine Strecke der Länge eins ab. Damit erhalten wir im Koordinatensystem die komplexe Zahl $r + i$. Zeichne die Gerade l durch 0 und den Punkt $r + i$. Zeichne die Senkrechte auf die x-Achse durch 1. Mit dem Strahlensatz folgt, dass diese die Gerade l im Punkt $1 + r^{-1}i$ schneidet. Die reelle Zahl r^{-1} und damit auch die komplexe Zahl z^{-1} sind also konstruierbar.

(v) Wurzelziehen: Sei $z = re^{i\varphi}$. Dann ist $\sqrt{z} = \sqrt{r}e^{i\varphi/2}$. Für die Berechung von $\sqrt{r}$ bilde einen Kreis mit Mittelpunkt $(r-1)/2$ und Radius $(r+1)/2$, dieser schneidet die reelle Achse also in -1 und r. Schneide diesen Kreis mit der Geraden $i\mathbb{R}$ und erhalte den Schnittpunkt ih. Betrachte $x = |ih-1|, y = |r-ih|$. Nach dem Satz des Thales und dem Satz des Pythagoras gilt

$$r^2 + 2r + 1 = (r+1)^2 = x^2 + y^2 = (h^2+1) + r^2 + h^2 \ ,$$

also $2r = 2h^2$ und damit $r = h^2$. Also ist $h = \sqrt{r}$ und damit $\sqrt{z}$ in $\hat{M}$. □

Bemerkung 21.3. Sei $\mathbb{Q} \leq L \leq \mathbb{C}$ ein Zwischenkörper, $i \in L$ und $\overline{L} = L$. Seien $z = a+bi$ und $w = c+di$ in L mit korrespondierenden Punkten $P = (a,b)$ beziehungsweise $Q = (c,d)$. Insbesondere sind also $a, b, c, d \in \mathbb{R}$.

(a) Ist $a + bi \in L$, dann folgt $a, b \in L \cap \mathbb{R}$: Sei $a + bi \in L$. Wegen $L = \overline{L}$ folgt $a - bi \in L$. Da L ein Körper ist, folgt

$$a = \frac{1}{2}(z + \overline{z}), ib = \frac{1}{2}(z - \overline{z}) \in L \ .$$

Da $i \in L$ ist, folgt $b = (-i)ib \in L$.

(b) Sei die Gerade $g(P,Q) = \overline{PQ}$ gegeben durch $y = mx + q$ mit $m, q \in \mathbb{R}$. Dann folgt $m, q \in L \cap \mathbb{R}$: Es gilt

$$m = \pm\frac{d-b}{c-a} \in L \cap \mathbb{R}.$$

Da $q = y - mx$ ist, folgt durch Einsetzen eines Punktes, zum Beispiel des Punktes P, dass $q = b - ma \in L \cap \mathbb{R}$ ist.

(c) Sei $k(P,Q)$ gegeben durch $(x-a)^2 + (y-b)^2 = r^2$. Dann folgt

$$r^2 = (c-a)^2 + (d-b)^2 \in L \cap \mathbb{R} \ .$$

Insgesamt gilt also: Geradengleichungen und Kreigleichungen, definiert durch Punkte aus L, haben Koeffizienten in L.

Lemma 21.4. *Sei $\mathbb{Q} \leq L \leq \mathbb{C}$ ein Zwischenkörper, $i \in L$ und $\overline{L} = L$. Sei $\alpha = u + iv \in \mathbb{C}$ in einem elementaren Konstruktionsschritt aus L konstruierbar. Dann ist $[L(\alpha) : L] \leq 2$ und $\overline{L(\alpha)} = L(\alpha)$.*

Beweis. Seien P, Q, R, S konstruierbare Punkte, also in L.

- 1. Fall: $\alpha = u + iv$ ist Schnittpunkt der beiden Geraden $y = mx + q$ und $y = nx + p$ mit $m, n, p, q \in L \cap \mathbb{R}$. Lineare Algebra impliziert, dass das zugehörige lineare Gleichungssystem eine Lösung $u, v \in L$ hat. Also ist $\alpha = u + iv \in L$, und $[L(\alpha) : L] = 1$ und $\overline{L(\alpha)} = L(\alpha)$.
- 2. Fall: Sei $\alpha = u + iv \in g(P,Q) \cap k(R,S)$. Sei $y = mx + q$ die Gleichung von $g(P,Q)$ und $(x-c)^2 + (y-d)^2 = r^2$ die Gleichung von $k(R,S)$. Nach 21.3 sind $m, q, c, d, r^2 \in L \cap \mathbb{R}$. Man löst dieses nicht-lineare Gleichungssystem, in dem man

in der Kreisgleichung die Variable y durch die Geradengleichung substituiert. Für den Lösungspunkt (u, v) gilt damit:

$$r^2 = (u-c)^2 + (r-d)^2 = (n-c)^2 + (mu+q-d)^2.$$

Also ist u Nullstelle einer quadratischen Gleichung mit Koeffizienten in $L \cap \mathbb{R}$. Die Lösung u dieser Gleichung kann reell oder komplex sein. In beiden Fällen ist $\overline{u}$ auch Lösung dieser quadratischen Gleichung, siehe 18.6(b). Also ist $\overline{u} \in L(u)$. Elemente in $L(u)$ sind Polynome in u mit Koeffizienten in L. Wegen $L = \overline{L}$ ist das komplex Konjugierte eines solchen Polynoms ein Polynom in $\overline{u}$ mit Koeffizienten in L. Also ist $\overline{L(u)} = L(u)$. Mit 21.3 folgt, dass auch $v = mu+q \in L(u)$ ist. Nach Voraussetzung ist $i \in L$, also ist auch $\alpha = u + iv \in L(u)$, also $L(\alpha) \subseteq L(u)$. Nach Konstruktion, siehe 20.4, ist $[L(u) : L] \leq 2$, nach der Gradformel 19.8 gilt also $[L(\alpha) : L] \leq 2$. Entweder ist damit $L(\alpha) = L$ oder $L(\alpha) = L(u)$. In beiden Fällen gilt also $\overline{L(\alpha)} = L(\alpha)$.

- 3. Fall: Sei $\alpha = u + iv$ Lösung von

$$(x-a)^2 + (y-b)^2 = r^2$$
$$(x-c)^2 + (y-d)^2 = s^2$$

mit $a, b, c, d, r^2, s^2 \in L \cap \mathbb{R}$. Bilde die Differenz der Gleichungen. Man erhält eine lineare Gleichung in x, y. Dann sind die gemeinsamen Lösungen der beiden quadratischen Gleichungen gleich den Lösungen einer der quadratischen Gleichungen und der neuen Geradengleichung. Damit folgt die Behauptung aus Fall 2. □

Theorem 21.5. *Sei $\{0,1\} \subseteq M \leq \mathbb{C}$. Ein Element $z \in \mathbb{C}$ ist genau dann aus M konstruierbar, wenn eine endliche Kette von Körpern existiert,*

$$\mathbb{Q}(M \cup \overline{M}) = L_0 \leq L_1 \leq \ldots \leq L_r,$$

mit $[L_i : L_{i-1}] \leq 2$ und $z \in L_r$.

Beweis. „⇒“: Da $\{0,1\} \subseteq M$, ist $i \in \hat{M}$. Da z konstruierbar ist, erhält man z aus M in endlich vielen elementaren Konstruktionsschritten. Es existieren also endlich viele konstruierbare Zahlen $z_1 = i$, $z_2, \ldots, z_r \in \hat{M}$ mit $z = z_r$. Setze $L_j := L_{j-1}(z_j)$ mit $1 \leq i \leq r$. Dann ist $L_0 \leq L_1 \leq L_2 \leq \ldots \leq L_r$ und nach 21.4 gilt $[L_i : L_{i-1}] \leq 2$.
„⇐“: Wir führen eine Induktion nach r durch. Nach 21.2 sind alle Elemente in $L_0 := \mathbb{Q}(M \cup \overline{M})$ konstruierbar. Angenommen, alle Elemente aus L_{i-1} sind konstruierbar. Sei $[L_i : L_{i-1}] = 2$. Nach 19.8 existiert $a \in L_i$ mit $L_i = L_{i-1}(a)$. Es existieren also $p, q \in L_{i-1}$ mit $m_{a,L_{i-1}} = X^2 + pX + q$ (siehe 20.4). Somit ist nach 21.2 die Zahl

$$a = -\frac{p}{2} \pm \sqrt{\left(\frac{p}{2}\right)^2 - q}$$

aus L_{i-1} konstruierbar. Nach 21.2 ist also jedes Element aus $L_i = L_{i-1}(a)$ konstruierbar. □

Korollar 21.6. *Jede aus $M = \{0,1\}$ konstruierbare Zahl $z \in \mathbb{C}$ ist algebraisch über $\mathbb{Q}$ und $[z : \mathbb{Q}] = 2^k$ für ein $k \in \mathbb{N}_0$.*

Beweis. Die Behauptung folgt aus 19.8 und 21.5: Nach Voraussetzung ist $M = \{0, 1\}$, also ist $\mathbb{Q}(M \cup \overline{M}) = \mathbb{Q}$. Sei z aus M konstruierbar. Es existiert also eine Körperkette $\mathbb{Q} = L_0 \leq L_1 \leq \ldots \leq L_r$ mit $[L_i : L_{i-1}] \leq 2$ und $z \in L_r$. Die Körpererweiterung $L_r/\mathbb{Q}$ ist endlich, nach 20.7 ist also z algebraisch über $\mathbb{Q}$. Die zweite Behauptung folgt aus $\mathbb{Q} \leq \mathbb{Q}(z) \leq L_r$ und der Gradformel. □

Beispiel 21.7.

(a) Delisches Problem: Gegeben ist ein Würfel mit o. E. Kantenlänge 1. Konstruiere mit Zirkel und Lineal einen Würfel doppelten Volumens, d. h. mit Kantenlänge $a = \sqrt[3]{2}$. Hier ist $M = \{0, 1\}$. Es ist $m_{a,\mathbb{Q}} = X^3 - 2 \in \mathbb{Q}[X]$. Beachte: $X^3 - 2$ ist unzerlegbar nach dem Eisenstein-Kriterium für $p = 2$. Damit ist $[a : \mathbb{Q}] = 3$, was keine Zweierpotenz ist. Nach 21.6 ist also $a = \sqrt[3]{2}$ nicht mit Zirkel und Lineal konstruierbar.

(b) Quadratur des Kreises: Gegeben ist ein Kreis, o. E. mit Radius 1. Konstruiere mit Zirkel und Lineal ein Quadrat gleichen Flächeninhalts, also mit Seitenlänge $a = \sqrt{\pi}$. Angenommen, $\sqrt{\pi} \in \hat{M}$ für $M = \{0, 1\}$. Nach 21.1 ist $\sqrt{\pi}\sqrt{\pi} = \pi \in \hat{M}$. Aber π ist transzendent. Nach 21.6 ist also $a = \sqrt{\pi}$ nicht konstruierbar.

(c) Winkeldreiteilung: Gewisse Winkel wie 180°, 270°, ... lassen sich mit Zirkel und Lineal dreiteilen. Sei $\alpha \in [0, 2\pi]$ gegeben. Sei $\zeta = e^{i\alpha}$. Die Dreiteilung von α ist gleichbedeutend mit der Konstruktion von $z = e^{i\alpha/3}$ aus $M = \{0, 1, \zeta\}$. Wähle $\alpha = 60° = \pi/3$. Dann ist

$$e^{i\alpha} = \cos(\alpha) + i \sin(\alpha) = \frac{1}{2} + i \cdot \frac{\sqrt{3}}{2} \ .$$

Beachte: $\zeta \in \widehat{\{0, 1\}}$. Die Frage ist also: Lässt sich $e^{i\alpha/3}$ aus $M = \{0, 1\}$ mit Zirkel und Lineal konstruieren?

(i) Die Additionstheoreme ergeben allgemein

$$\cos(3\beta) = 4\cos^3\beta - 3\cos\beta$$

für beliebiges β.

(ii) Setze $\beta = \alpha/3$. Dann folgt:

$$\frac{1}{2} = \cos(\alpha) = \cos(3\beta) = 4\cos(\beta)^3 - 3\cos(\beta) \ .$$

Es folgt, dass $z = \cos(\beta)$ eine Nullstelle von $4X^3 - 3X - 1/2$ ist und daher auch von $f = 8X^3 - 6X - 1$. Über dem Körper $\mathbb{Z}_7$ ist das Polynom $\overline{f} = X^3 + X - 1$ unzerlegbar. Mit dem Reduktionskriterium 18.8 und 17.10 folgt, dass $f \in \mathbb{Q}[X]$ unzerlegbar ist. Nach 20.2 ist $[z : \mathbb{Q}] = 3$. Nach 21.6 ist z nicht konstruierbar. Somit ist auch $e^{i\alpha/3}$ nicht aus $M = \{0, 1\}$ oder aus $M = \{0, 1, \zeta\}$ konstruierbar.

Kapitel 22

Algebraischer Abschluss

Definition 22.1. Ein Körper K heißt *algebraisch abgeschlossen*, falls eine der folgenden äquivalenten Bedingungen gilt:

(a) Jedes $f \in K[X] \setminus K$ hat mindestens eine Nullstelle in K.

(b) Jedes $f \in K[X] \setminus K$ zerfällt in ein Produkt linearer Faktoren: $f = \prod_{i=1}^{n} f_i$ mit $f_i \in K[X]$ und $\deg f_i = 1$ für alle i.

(c) Jedes unzerlegbare, normierte Polynom hat die Form $X - a$, für ein $a \in K$.

(d) Ist L/K algebraisch, dann ist $L = K$.

Beweis. (i) Angenommen Aussage (c) gilt. Sei L/K eine algebraische Körpererweiterung. Sei $a \in L$. Dann ist a algebraisch über K. Sei m das Minimalpolynom von a über K. Insbesondere ist $m \in K[X]$ unzerlegbar. Nach (c) ist $\deg m = 1$, also $m = X - a \in K[X]$. Es folgt also $L = K$.

(ii) Angenommen Aussage (d) gilt. Sei $f \in K[X]$ ein nicht-konstantes Polynom. Der Polynomring $K[X]$ ist faktoriell. Schreibe $f = f_1 \cdots f_n$ als Produkt von unzerlegbaren polynomen $f_i \in K[X]$. Nach 20.4 enthält $L \coloneqq K[X]/\langle f_1 \rangle$ eine Nullstelle a von f_1, also auch von f, und L/K ist algebraisch. Nach (d) gilt dann $L = K$. Also ist $a \in K$ eine Nullstelle von f. □

Definition 22.2. Sei L/K eine Körpererweiterung. Dann ist L *algebraischer Abschluss* von K, falls gilt:

(i) L/K ist algebraisch;

(ii) L ist algebraisch abgeschlossen.

Der Fundamentalsatz der Algebra sagt, dass jedes nicht-konstante Polynom mit Koeffizienten in $\mathbb{C}$ eine Nullstelle in $\mathbb{C}$ hat. Der Körper $\mathbb{C}$ ist also algebraisch abgeschlossen. Sei $K \leq \mathbb{C}$. Dann ist die Menge $\overline{K} \coloneqq \{z \in \mathbb{C} \mid z \text{ algebraisch über } K\}$ ein algebraischer Abschluss von K. Hierzu zeige man, dass die Körpererweiterung $K(a, b)$ algebraisch ist über K, für Elemente $a, b \in \overline{K}$. Da $a \pm b, a \cdot b, a^{-1} \in K(a, b)$, folgt insbesondere, dass $\overline{K}$ ein Körper ist. Nach Definition ist $\overline{K}/K$ algebraisch. Zu zeigen bleibt noch, dass $\overline{K}$ algebraisch abgeschlossen ist. Sei f ein nicht-konstantes Polynom in $\overline{K}[X]$. Dann hat f eine Nullstelle $a \in \mathbb{C}$. Nach 20.4 ist $\overline{K}(a)/\overline{K}$ eine algebraische Erweiterung. Da auch $\overline{K}/K$ algebraisch ist, folgt mit 20.8, dass auch $\overline{K}(a)/K$ algebraisch ist. Es ist also insbesondere

a ein algebraisches Element über K. Damit folgt aber $a \in \overline{K}$. Also hat das Polynom f eine Nullstelle in $\overline{K}$. Nach 22.1 ist also $\overline{K}$ algebraisch abgeschlossen, und damit ein algebraischer Abschluss von K.

Proposition 22.3. *Sei K ein Körper. Dann existiert eine algebraische Körpererweiterung L/K, sodass jedes $f \in K[X] \setminus K$ eine Nullstelle in L hat.*

Beweis. Setze $I \coloneqq K[X] \setminus K$ als Indexmenge und $R \coloneqq K[X_i \mid i \in I]$. Nach Definition sind Elemente in R Polynome in endlich vielen Variablen X_i. Addition und Multiplikation von Elementen in R ist entsprechend definiert wie in einem Polynomring in endlich vielen Variablen, genauer in der Vereinigungsmenge der Variablen der beiden Polynome. Sei $A \coloneqq \langle f(X_f) \mid f \in I \rangle \trianglelefteq R$.

(a) Behauptung: $A \neq R$.

Beweis. Angenommen, $1 \in A$. Dann existieren $f_i = f_i(X_{f_i}) \in A$ und $g_i \in R$ mit $1 = \sum_{i=1}^{n} f_i g_i$. Wiederholte Anwendung von 20.9 gibt: Es existiert eine Körpererweiterung F/K, sodass jedes f_i für $i \in \{1, \ldots, n\}$ eine Nullstelle $a_i \in F$ hat. Sei $\varphi : R \to F[X_i \mid i \in I]$ der Einsetzungshomomorphismus definiert durch $\varphi|_K = \mathrm{id}, \varphi(X_{f_i}) = a_i$ und $\varphi(X_f) = X_f$ für f sonst. Es ist $\varphi(f_i(X_{f_i})) = f_i(a_i) = 0$. Also ist

$$1 = \varphi(1) = \sum_{i=1}^{n} \underbrace{\varphi(f_i)}_{=0} \varphi(g_i) = 0 \ ,$$

ein Widerspruch. Also ist $1 \notin A$, beziehungsweise $A \neq R$. □

(b) Der Ring ${}^{R}\!/_{A}$ hat ein maximales Ideal nach 15.8. Nach 11.1 existiert $M \trianglelefteq R$ maximal mit $A \subseteq M \subseteq R$. Nach 15.2 ist dann $R/M =: L$ ein Körper. Nach 19.1 ist $K \hookrightarrow R = K[X_i \mid i \in I] \xrightarrow{\pi} {}^{R}\!/_{M} = L$ injektiv. Identifiziere K mit einem Teilkörper in L, d. h. $K \leq L$. Diese Identifizierung bedeutet auch, dass $\pi(\lambda) = \lambda$ ist für alle $\lambda \in K$.

(c) Sei $f \in K[X] \setminus K$, etwa $f = \sum \lambda_i X^i$ mit $\lambda_i \in K$. Dann ist

$$\begin{aligned} f(\pi(X_f)) &= \sum \lambda_i \pi(X_f)^i = \sum \pi(\lambda_i)\pi(X_f)^i \\ &= \pi\left(\sum \lambda_i X_f^i\right) = \pi(\underbrace{f(X_f)}_{\in A \subseteq M}) = 0 + M = 0_L \ . \end{aligned}$$

Also hat f eine Nullstelle in L für alle $f \in K[X] \setminus K$.

(d) Sei $a \in L$. Dann ist $a \in K(X_f + M \mid f \in J)$ mit $J \subseteq I$ endlich. Nach (c) sind die Elemente $X_f + M$ algebraisch. Mit 20.8 und 20.7 folgt, dass a algebraisch ist über K. Also ist L/K algebraisch. □

Bemerkung 22.4. Seien K_i Körper mit $K_0 \subseteq K_1 \subseteq K_2 \subseteq \ldots$. Dann ist $K \coloneqq \bigcup_{i \geq 0} K_i$ ein Körper: Um dies zu sehen, seien $a, b \in K$. Dann existieren i, j mit $a \in K_i$ und $b \in K_j$. Ohne Einschränkung sei $i \leq j$. Dann ist $K_i \subseteq K_j$, also $a, b \in K_j$. Da K_j ein Körper ist, folgt $a \pm b, a^{-1}, ab \in K_j \subseteq K$.

Theorem 22.5. *Jeder Körper K hat einen algebraischen Abschluss.*

Beweis.

(a) Sei $K_0 = K$. Nach 22.3 existiert eine algebraische Körpererweiterung K_1/K_0, sodass alle Polynome in $K_0[X] \setminus K_0$ eine Nullstelle in K_1 haben. Wiederhole das Argument mit K_1 etc. Wir erhalten eine Körperkette $K_0 \leq K_1 \leq K_2 \leq \ldots$ mit K_i/K_{i-1} algebraisch. Setze $\overline{K} := \bigcup_{i\geq 0} K_i$. Nach 22.4 ist $\overline{K}$ ein Körper. Sei $a \in \overline{K}$. Dann existiert ein Index j mit $a \in K_j$. Nach 20.8 ist K_j/K algebraisch, und damit a algebraisch über K. Also ist $\overline{K}/K$ algebraisch.

(b) Sei $f = \sum_{i=0}^{n} a_i X^i \in \overline{K}[X] \setminus \overline{K}$. Dann existiert j mit $a_0, \ldots, a_n \in K_j$, d. h. $f \in K_j[X]$. Nach (a) hat f eine Nullstelle in $K_{j+1} \subseteq \overline{K}$. Dann hat f eine Nullstelle in $\overline{K}$. Nach 22.1 ist $\overline{K}$ algebraisch abgeschlossen. □

Bemerkung 22.6. Seien K und K' Körper, sei $\sigma : K \to K'$ ein Homomorphismus. Sei

$$\sigma^* : K[X] \to K'[X], \quad \sum_{i=0}^{n} \lambda_i X^i \mapsto \sum_{i=0}^{n} \sigma(\lambda_i) X^i,$$

siehe 13.3, mit $X \mapsto X$. Sei σ bijektiv, also ist auch σ^* bijektiv.

(a) Ist $f \in K[X]$ unzerlegbar über K, dann ist $\sigma^*(f)$ unzerlegbar über K'. Also ist

$$K[X]\big/\langle f\rangle \simeq K'[X]\big/\langle \sigma^*(f)\rangle$$

nach 11.3 vermöge

$$g + \langle f\rangle \mapsto \sigma^* g + \langle \sigma^* f\rangle \ .$$

(b) Seien L/K und L'/K' Körpererweiterungen, $\varphi : L \to L'$ ein Homomorphismus mit $\varphi|_K = \sigma$. Sei $g = \sum \lambda_i X^i \in K[X]$ und sei $a \in L$. Dann ist

$$(\sigma^* g)(\varphi(a)) = \sum \sigma(\lambda_i)\varphi(a)^i = \sum \varphi(\lambda_i)\varphi(a)^i = \varphi\left(\sum \lambda_i a^i\right) = \varphi(g(a)) \ .$$

Also ist $a \in L$ eine Nullstelle von $g \in K[X]$ genau dann, wenn $\varphi(a) \in L'$ eine Nullstelle von $\sigma^* g \in K'[X]$ ist. Hierbei benutzen wir, dass $\varphi(g(a)) = 0$ impliziert, dass $g(a)$ im Kern von φ liegt. Nach 19.1 sind Körperhomomorphismen injektiv, haben also trivialen Kern. Daher folgt $g(a) = 0$.

Proposition 22.7. *Seien K und K' Körper, sei $\sigma : K \to K'$ ein Isomorphismus mit Fortsetzung σ^* wie in 22.6. Seien L/K und L'/K' Körpererweiterungen. Sei $a \in L$.*

(a) Sei $a' \in L'$ mit $m_{a',K'} = \sigma^* m_{a,K}$. Dann existiert genau ein Isomorphismus

$$\varphi : K(a) \to K'(a')$$

mit $\varphi(a) = a'$ und $\varphi|_K = \sigma$.

(b) $\#\{\varphi : K(a) \to L' \mid \varphi|_K = \sigma\} = \#\{a' \in L' \mid \sigma^*(m_{a,K})(a') = 0\}$.

Beweis. (a) Sei $m = m_{a,K}$. Die Komposition von

$$K(a) = K[a] \overset{20.4}{\xrightarrow{\sim}} K[X]/\langle m\rangle \overset{22.6}{\xrightarrow{\sim}} K'[X]/\langle \sigma^* m\rangle \overset{20.4}{\xrightarrow{\sim}} K'[a'] = K'(a'),$$
$$g(a) \mapsto g + \langle m\rangle \mapsto \sigma^* g + \langle \sigma^* m\rangle \mapsto (\sigma^* g)(a')$$

ist ein Isomorphismus mit $a \mapsto a'$ und $\lambda \mapsto \sigma(\lambda)$ für $\lambda \in K$.

(b) Dies folgt aus (a) und 22.6, denn danach ist $\varphi \mapsto \varphi(a)$ eine Bijektion. □

Definition 22.8. Seien L_1/K und L_2/K Körpererweiterungen. Sei $\varphi : L_1 \to L_2$ ein Ringhomomorphismus. Dann heißt φ ein *K-Homomorphismus*, falls $\varphi|_K = \mathrm{id}_K$. Ist zusätzlich φ bijektiv, dann heißt φ *K-Isomorphismus*; ist zusätzlich $L_1 = L_2$, dann heißt φ *K-Automorphismus*.

Theorem 22.9.

(a) Sei L/K eine algebraische Körpererweiterung und M ein algebraisch abgeschlossener Körper. Sei ferner $\sigma : K \to M$ ein Homomorphismus. Dann existiert ein Homomorphismus $\varphi : L \to M$ mit $\varphi|_K = \sigma$.

(b) Sei $\sigma : K \xrightarrow{\sim} K'$ ein Isomorphismus. Seien $\overline{K}$ und $\overline{K'}$ algebraische Abschlüsse von K bzw. K'. Dann existiert ein Isomorphismus $\varphi : \overline{K} \to \overline{K'}$ mit $\varphi|_K = \sigma$.

(c) Seien L_1 und L_2 algebraische Abschlüsse von K. Dann existiert ein K-Isomorphismus von L_1 nach L_2.

Beweis.

(a) (i) Sei L/K algebraisch. Sei $X := \{(K', \tau') \mid K \le K' \le L, \tau'|_K = \sigma\}$. Definiere $(K', \tau') \le (K'', \tau'') :\Leftrightarrow K' \le K''$ und $\tau''|_{K'} = \tau'$. Dann ist $\le$ eine partielle Ordnung auf X. Sei $Y = \{(K_i, \tau_i) \mid i \in I\} \subseteq X$ total geordnet. Wir erhalten eine Körperkette, total geordnet durch Inklusion. Nach 22.5 ist $\bigcup_{i\in I} K_i$ ein Teilkörper von L. Da $\tau_j|_{K_i} = \tau_i$ für $K_i \le K_j$ gilt, ist $\bigcup \tau_i : \bigcup K_i \to M$ wohldefiniert, wobei $x \in K_j$ abgebildet wird auf $\tau_j(x)$. Also ist $(\bigcup K_i, \bigcup \tau_i) \in X$ eine obere Schranke von Y. Nach dem Lemma von Zorn (15.7) hat X ein maximales Element (L', τ').

(ii) Behauptung: $L' = L$. Angenommen $a \in L \setminus L'$. Da L/K algebraisch, ist a algebraisch über K. Nach 22.7 existiert ein Homomorphismus $\alpha : L'(a) \to M$, der den Homomorphismus $\tau' : L' \to M$ fortsetzt. Dies widerspricht der Maximalität von (L', τ'). Also ist $L' = L$.

(b) Setze $L := \overline{K}$ und $M := \overline{K'}$ in Aussage (a). Dann existiert ein Homomorphismus $\varphi : \overline{K} \to \overline{K'}$ mit $\varphi|_K = \sigma$. Nach 19.1 ist φ injektiv. Zu zeigen ist, dass φ auch surjektiv ist. Es ist

$$K' = \sigma(K) = \varphi(K) \subseteq \varphi(\overline{K}) \subseteq \overline{K'}$$

mir $\overline{K'}/K'$ algebraisch nach Voraussetzung. Nach 20.8 sind damit die beiden Teilerweiterungen in der letzen Körperkette algebraisch. Nach 19.1 ist $\varphi(\overline{K}) \simeq \overline{K}$ und $\overline{K}$ ist algebrasich abgeschlossen. Mit 22.1 folgt $\varphi(\overline{K}) = \overline{K'}$. Also ist φ bijektiv.

(c) Dies ist ein Spezialfall von (b) mit $K = K'$ und $\sigma = \mathrm{id}_K$. □

Kapitel 23

Endliche Körper

In diesem Kapitel wollen wir die endlichen Körper klassifizieren. Wir beginnen mit einem Beispiel.

Beispiel 23.1.

(a) Sei p eine Primzahl. Sei $f \in \mathbb{Z}_p[X]$ unzerlegbar und $\deg f = n$. Nach 16.6 ist dann $\langle f \rangle \trianglelefteq \mathbb{Z}_p[X]$ maximal. Mit 15.2 folgt, dass $L \coloneqq {}^{\mathbb{Z}_p[X]}\!/_{\langle f \rangle}$ ein Körper ist. Nach 19.6 ist $\operatorname{char} L = p$, also ist Primkörper $\Pi(L) \simeq \mathbb{Z}_p$. Wir identifizieren $\Pi(L)$ mit $\mathbb{Z}_p$, betrachten also $\mathbb{Z}_p$ als Teilkörper von L. Da $\{1 + I, X + I, \ldots, X^{n-1} + I\} \subseteq L$ eine $\mathbb{Z}_p$-Basis von L ist, folgt $|L| = p^n$.

(b) Sei $p = 2$. Durch Überprüfen auf Nullstellen in $\mathbb{Z}_2$, und bei Polynomen vom Grad vier durch Überprüfen, dass $X^2 + X + 1$ kein Teiler ist (siehe 18.10), sieht man, dass die folgenden Polynome unzerlegbar über $\mathbb{Z}_2$ sind:

$$\begin{aligned} f_2 &\coloneqq X^2 + X + 1 \\ f_3^{(1)} &\coloneqq X^3 + X + 1 \\ f_3^{(2)} &\coloneqq X^3 + X^2 + 1 \\ f_4^{(1)} &\coloneqq X^4 + X + 1 \\ f_4^{(2)} &\coloneqq X^4 + X^3 + 1 \\ f_4^{(3)} &\coloneqq X^4 + X^3 + X^2 + X + 1 \ . \end{aligned}$$

Damit existieren Körper mit $2^2, 2^3, 2^4$ Elementen. Es stellen sich die Fragen: Existiert zu jedem Paar (p, n) mit p Primzahl und n eine natürliche Zahl ein Körper mit p^n Elementen? Wieviele verschiedene Körper existieren zu einem gegeben Tupel (p, n)? Liefern verschiedene unzerlegbare Polynome f_n gleichen Grades n Körper, die zueinander isomorph sind oder nicht?

(c) Wir betrachten ein Beispiel genauer. Definiere $I \coloneqq \langle X^2 + X + 1 \rangle \trianglelefteq \mathbb{Z}_2[X]$ und $L \coloneqq {}^{\mathbb{Z}_2[X]}\!/_{I}$. Dann besteht der Körper L aus genau vier Elementen:

$$L = \{0 + I, 1 + I, X + I, (X + 1) + I\}.$$

Wir berechnen die Verknüpfungstafeln für die Addition und Multiplikation von L. Wir schreiben $\overline{a} \coloneqq a + I$. Dann erhalten wir:

$+$	$\overline{0}$	$\overline{1}$	$\overline{X}$	$\overline{X+1}$
$\overline{0}$	$\overline{0}$	$\overline{1}$	$\overline{X}$	$\overline{X+1}$
$\overline{1}$	$\overline{1}$	$\overline{0}$	$\overline{X+1}$	$\overline{X}$
$\overline{X}$	$\overline{X}$	$\overline{X+1}$	$\overline{0}$	$\overline{1}$
$\overline{X+1}$	$\overline{X+1}$	$\overline{X}$	$\overline{1}$	$\overline{0}$,

$\cdot$	$\overline{0}$	$\overline{1}$	$\overline{X}$	$\overline{X+1}$
$\overline{0}$	$\overline{0}$	$\overline{0}$	$\overline{0}$	$\overline{0}$
$\overline{1}$	$\overline{0}$	$\overline{1}$	$\overline{X}$	$\overline{X+1}$.
$\overline{X}$	$\overline{0}$	$\overline{X}$	$\overline{X+1}$	$\overline{1}$
$\overline{X+1}$	$\overline{0}$	$\overline{X+1}$	$\overline{1}$	$\overline{X}$

Es gibt nur zwei Gruppen der Ordnung vier. Es gilt hier also $(L,+) \simeq \mathbb{Z}_2 \times \mathbb{Z}_2 \not\simeq \mathbb{Z}_4$. Im allgemeinen ist die additive Gruppe eines Körpers L mit p^n Elementen nicht zyklisch: Sei $x \in L$. Dann ist $(a + \cdots + a) = p \cdot a = 0$. Also ist die (additive) Ordnung von a echt kleiner als p^n für $n > 1$.

Die Multiplikationstafel wird mit Hilfe von 10.14 berechnet. Zum Beispiel gilt:

$$(X+I)(X+I) = X^2 + I = X^2 - (X^2 + X + 1) + I = -X - 1 + I = X + 1 + I \ .$$

Hier haben wir benutzt, dass die Charakteristik des Körpers zwei ist. In diesem Beispiel können wir die Gruppenstruktur zur Berechnung der Multiplikationstafel benutzen: Da $(L^\times, \cdot)$ eine Gruppe ist und es nur eine Gruppe mit drei Elementen gibt, gilt $(L^\times, \cdot) \simeq \mathbb{Z}_3$. Erzeuger der Gruppe ist ein Element ungleich dem Einselement, also zum Beispiel $\overline{X} = X + I$. Damit folgen die restlichen Einträge der Multiplikationstafel ohne weiteres Rechnen. Wir erhalten in diesem Beispiel, dass $L^\times$ eine zyklische Gruppe ist. Dies gilt allgemeiner:

Proposition 23.2. *Sei K ein Körper und* $\operatorname{char} K = p > 0$. *Sei $G \leq (K^\times, \cdot)$ eine endliche Untergruppe. Dann ist G zyklisch.*

Beweis. Nach Voraussetzung ist G eine endliche abelsche Gruppe. Nach 6.7 existieren $n_1 \mid n_2 \mid \ldots \mid n_r \in \mathbb{N}$ mit $|G| = \prod_{i=1}^r n_i$ und $G \simeq \mathbb{Z}_{n_1} \times \mathbb{Z}_{n_2} \times \ldots \times \mathbb{Z}_{n_r}$. Aufgrund der Teilbarkeitsrelation der Elementarteiler n_i und 3.5 gilt für alle $x \in G$:

$$x^{n_r} = (x_1, \ldots, x_r)^{n_r} = (x_1^{n_r}, \ldots, x_r^{n_r}) = (1, \ldots, 1) \ .$$

Das Polynom $X^{n_r} - 1 \in K[X]$ hat maximal n_r Nullstellen nach 18.2, also ist $|G| \leq n_r$, d. h. $n_1 = \ldots = n_{r-1} = 1$ und $n_r = |G|$. Also ist $G \simeq \mathbb{Z}_{n_r}$ eine zyklische Gruppe. □

Definition 23.3. Sei $0 \neq f \in K[X] \setminus K$. Eine Körpererweiterung Z über K heißt *Zerfällungskörper* von f über K (kurz ZFK), falls es ein $\lambda \in K$ und $a_1, \ldots, a_n \in Z$ gibt mit $f = \lambda \cdot \prod_{i=1}^n (X - a_i)$ und $Z = K(a_1, \ldots, a_n)$. Nach 20.8 und 20.7 ist Z/K algebraisch.

Beispiel 23.4.

(a) Sei $d \in \mathbb{Q}$ mit $\sqrt{d} \notin \mathbb{Q}$. Dann ist $\mathbb{Q}(\sqrt{d})$ ein Zerfällungskörper von $X^2 - d \in \mathbb{Q}[X]$. Es gilt $[\mathbb{Q}(\sqrt{d}) : \mathbb{Q}] = 2$ nach 20.4.

(b) Sei $a = \sqrt[3]{2}$ und $\xi = e^{2\pi i/3}$. Dann hat $f := X^3 - 2 \in \mathbb{Q}[X]$ in $\mathbb{C}$ die Nullstellen $\{a, a\xi, a\xi^2\}$. Der Zerfällungskörper von f ist also $\mathbb{Q}(a, \xi)$. Hier gilt $[\mathbb{Q}(a, \xi) : \mathbb{Q}] = 6$.

(c) (i) Sei $f = X^p - X \in \mathbb{Z}_p[X]$ und p eine Primzahl. Dann ist $\mathbb{Z}_p^\times$ eine Gruppe mit $p - 1$ Elementen. Mit 3.5 folgt $a^{p-1} = 1$ in $\mathbb{Z}_p$ für alle $a \in \mathbb{Z}_p^\times$. Also gilt $a^p = a$ für alle $a \in \mathbb{Z}_p$. Somit ist a eine Nullstelle von f. Es ist also $\mathbb{Z}_p$ gleich der Menge aller Nullstellen von $f = X^p - X$. Wir verallgemeinern dies in diesem Kapitel.

(ii) Nach (i) ist $X^{p-1}-1=(X-1)(X-2)\cdot\ldots\cdot(X-(p-1))$. Setze $X=0$. Dann folgt

$$-1\equiv(-1)^{p-1}(p-1)!\equiv(p-1)!\pmod p\ .$$

Dieses Resultat aus der Zahlentheorie heißt der Satz von Wilson.

Theorem 23.5. *Der Zerfällungskörper Z von $f\in K[X]/K$ existiert und ist eindeutig bis auf K-Isomorphie.*

Beweis. Existenz: Sei $\overline{K}$ der algebraische Abschluss von K. Zu $f\in K[X]\setminus K$ existiert $\lambda\in K$ und $a_i\in\overline{K}$, $i\in I$ mit $f=c\cdot\prod_i(x-a_i)$. Setze $Z:=K(a_i\mid i\in I)$.
Eindeutigkeit: Sei Z' ein Zerfällungskörper von f über K. Sei $\overline{Z'}$ algebraischer Abschluss von Z'. Nach 20.8 ist damit $\overline{Z'}/K$ algebraisch. Also ist $\overline{Z'}$ algebraischer Abschluss von K. Da $\overline{K}$ und $\overline{Z'}$ algebraische Abschlüsse von K sind, existiert nach 22.9 (b) ein Isomorphismus $\psi:\overline{K}\to\overline{Z'}$ mit $\psi|_K=\mathrm{id}$. Hierbei ist

$$\begin{aligned}f=\psi^*f&=\psi^*\left(c\prod(X-a_i)\right)\\&=c\cdot\prod(X-\psi(a_i))\ .\end{aligned}$$

Somit sind $\{\psi(a_i)\mid i\in I\}\subseteq Z'$ die Nullstellen von f. Es folgt $Z'=K(\psi(a_i)\mid i\in I)=\psi(K(a_i\mid i\in I))=\psi(Z)$. Also sind Z und Z' K-isomorph. □

Bemerkung 23.6. Wie im Eindeutigkeitsbeweis von 23.5 zeigt man: Sei $\sigma:K\to K'$ ein Isomorphismus. Sei $f\in K[X]\setminus K$ und sei Z ein Zerfällungskörper von f über K. Sei Z' ein Zerfällungskörper von σ^*f über K'. Dann existiert ein Isomorphismus $\psi:Z\to Z'$ mit $\psi|_K=\sigma$.

Definition 23.7. Sei p eine Primzahl, und $q=p^n$ für $n\in\mathbb{N}$. Definiere $\mathbb{F}_q=\mathrm{GF}(q)$ als Zerfällungskörper von $X^q-X\in\mathbb{Z}_p[X]$. Nach 23.4 (c) ist $\mathbb{F}_p=\mathbb{Z}_p$.

Lemma 23.8. *Sei K ein Körper und* $\operatorname{char}K=p>0$.

(a) Dann ist $F:K\to K$ mit $x\mapsto x^p$ ein Monomorphismus. Insbesondere ist

$$(x+y)^{p^n}=x^{p^n}+y^{p^n}$$

für alle $x,y\in K$. Die Abbildung F heißt Frobenius-Homomorphismus.

(b) Ist $|K|<\infty$, so ist F ein Automorphismus. Insbesondere: Zu $y\in K$ existiert genau ein $x\in K$ mit $x^p=y$, d. h. jedes Element in K hat eine eindeutige p-te Wurzel.

Beweis. Es ist

$$\begin{aligned}F(1)&=1^p=1\\F(xy)&=(xy)^p=x^p\cdot y^p=F(x)\cdot F(y)\\F(x+y)&=(x+y)^p=\sum_{i=0}^{p}\binom{p}{i}x^iy^{p-i}=x^p+y^p\ ,\end{aligned}$$

denn $p\mid\binom{p}{i}$ für $1\le i\le p-1$. Induktiv folgt hieraus

$$(x+y)^{p^n}=x^{p^n}+y^{p^n}$$

Jeder Körperhomomorphismus ist injektiv nach 19.1. Da K endlich ist, folgt auch F surjektiv. □

Proposition 23.9. *Es ist* $|\mathbb{F}_q| = q$.

Beweis. Sei $f = X^q - X \in \mathbb{Z}_p[X]$. Nach Definition 23.3 existiert $N = \{a_i \mid i \in I\} \subseteq \mathbb{F}_q$ mit $f = \prod_i (X - a_i)$. Wir zeigen $N = \mathbb{F}_q$ und $|N| = q$.

(a) Seien $a_i, a_j \in N$ mit $a_j \neq 0$. Dann folgt $a_i^q = a_i, a_j^q = a_j$ und somit nach 23.8 auch

$$(a_i \pm a_j)^q = a_i^q \pm a_j^q = a_i \pm a_j$$
$$(a_i \cdot a_j^{-1})^q = a_i^q \cdot (a_j^q)^{-1} = a_i a_j^{-1} \ .$$

Somit ist $N \subseteq \mathbb{F}_q$ ein Teilkörper, der alle Nullstellen von f enthält. Folglich ist $N = \mathbb{F}_q$ Zerfällungskörper von f.

(b) Da $f' = qX^{q-1} - 1 = -1$ in $\mathbb{Z}_p[X]$ ist, ist $f'(a_i) = -1 \neq 0$. Damit ist jedes $a_i \in N$ eine einfache Nullstelle von f. Es folgt $q = |N| = |\mathbb{F}_q|$. □

Theorem 23.10. *Sei p eine Primzahl und $n \in \mathbb{N}$. Schreibe $q = p^n$.*

(a) Der Zerfällungskörper $\mathbb{F}_q$ von $f = X^q - X \in \mathbb{Z}_p[X]$ ist eine Körpererweiterung von $\mathbb{Z}_p = \mathbb{F}_p$ mit q Elementen, also mit $[\mathbb{F}_q : \mathbb{F}_p] = n$, und

$$\mathbb{F}_q = \{\textit{alle Nullstellen von } f = X^q - X\}.$$

(b) Bis auf Isomorphie ist $\mathbb{F}_q$ der einzige Körper mit p^n Elementen.

(c) Ist $g \in \mathbb{F}_p[X]$ unzerlegbar mit $\deg g = n$, dann ist

$$\mathbb{F}_q \simeq {}^{\mathbb{F}_p[X]}\!/_{\langle g \rangle} \ .$$

Jedes $a \in \mathbb{F}_q$, welches Nullstelle von g in $\mathbb{F}_q$ ist, ist ein primitives Element, d. h. $\mathbb{F}_q = \mathbb{F}_p(a)$.

(d) Ein Teilkörper von $\mathbb{F}_{p^n}$ hat Ordnung p^d mit $d \mid n$ und es gibt genau einen Teilkörper für jedes solche d. Weitere Teilkörper existieren nicht.

Beweis.

(a) Nach 23.5 existiert $\mathbb{F}_q$ und ist eindeutig bis auf $\mathbb{Z}_p$-Isomorphie. Nach 23.9 ist $\mathbb{F}_q$ gleich der Menge der Nullstellen von $X^q - X$. Aus 19.7 folgt $[\mathbb{F}_q : \mathbb{F}_p] = n$.

(b) Sei K ein Körper mit $q = p^n$ Elementen. Dann ist $\operatorname{char} K = p$. Die multiplikative Gruppe $K^\times$ ist nach 23.2 eine zyklische Gruppe mit $q - 1$ Elementen. Also ist $a^{q-1} = 1$ für alle $a \in K^\times$ und damit $a^q = a$ für alle $a \in K$, siehe 3.5. Folglich ist jedes $a \in K$ Nullstelle von $f = X^q - X \in \mathbb{Z}_p[X]$. Damit ist K ein Zerfällungskörper von f und damit $K \simeq \mathbb{F}_q$ nach 23.5.

(c) Nach 23.1 ist $L \coloneqq {}^{\mathbb{F}_p[x]}\!/_{\langle g \rangle}$ eine Körpererweiterung von $\mathbb{Z}_p = \mathbb{F}_p$ und

$$[L : \mathbb{F}_p] = \deg(g) =: n$$

und damit $|L| = p^n$. Mit (b) folgt $L \simeq \mathbb{F}_q$. Ist a Nullstelle von g in $\mathbb{F}_q$, so folgt mit 20.4:

$${}^{\mathbb{F}_p[x]}\!/_{\langle g \rangle} \simeq \mathbb{F}_p(a) \ .$$

Somit ist $\mathbb{F}_q = \mathbb{F}_p(a)$. Hier haben wir benutzt, dass man das Minimalpolynom $m_{a,\mathbb{F}_p}$ von a durch Normieren des Polynoms g erhält, und die von $m_{a,\mathbb{F}_p}$ und g erzeugten Ideale gleich sind.

(d) Übung. □

Kapitel 24

Galoiserweiterungen

Der Hauptsatz der Galoistheorie liefert eine (Inklusion-umkehrende) Bijektion zwischen einer bestimmten endlichen Gruppe und ihren Untergruppen, sowie einer bestimmten Körpererweiterung und all ihren Zwischenkörpern. Die Körpererweiterungen, für die eine solche Korrespondenz existiert, sind die sogenannten Galoiserweiterungen; bei der in der Korrespondenz vorkommenden Gruppe handelt es sich um eine sogenannte Galoisgruppe. In diesem Kapitel führen wir Galoisgruppen und Galoiserweiterungen ein.

Bemerkung 24.1. Sei L/K eine Körpererweiterung.

(a) Die Menge $\mathrm{Aut}(L) \coloneqq \{f : L \to L \mid f \text{ Automorphismus}\}$ aller Körperautomorphismen von L, zusammen mit der Komposition $\circ$ von Abbildungen, ist eine Gruppe. Die Teilmenge $\mathrm{Aut}(L/K) \coloneqq \{f \in \mathrm{Aut}(L) \mid f|_K = \mathrm{id}_K\} \subseteq \mathrm{Aut}(L)$ ist eine Untergruppe von $\mathrm{Aut}(L)$.

Ist $K \leq Z \leq L$ ein Zwischenkörper, dann ist $\mathrm{Aut}(L/Z) \leq \mathrm{Aut}(L/K)$ eine Untergruppe: ist $\sigma \in \mathrm{Aut}(L/Z)$, also $\sigma|_Z = \mathrm{id}_Z$, so ist auch $\sigma|_K = \mathrm{id}_K$.

(b) Wir wiederholen 22.6 und 22.7 im Spezialfall $L = L'$ und $K = K'$, sowie eines K-Automorphismus von L.

(i) Sei $g \in K[X]$ und sei $\sigma \in \mathrm{Aut}(L/K)$. Da $g(\sigma(a)) = \sigma(g(a))$ folgt: Es ist $a \in L$ eine Nullstelle von g genau dann, wenn $\sigma(a) \in L$ eine Nullstelle von g ist.

(ii) Sei $L = K(a)$ und $b \in L$ eine Nullstelle von $m_{a,K}$. Dann existiert genau ein Isomorphismus $\varphi : K(a) \to K(b)$ mit $a \mapsto b$ und $\varphi|_K = \mathrm{id}$. Es gibt also eine Bijektion zwischen $\{b \in L \mid b \text{ ist NS von } m_{a,K}\}$ und $\mathrm{Aut}(L/K)$.

(c) Sei L/K algebraisch und $\sigma : L \to L$ ein K-Homomorphismus. Dann ist σ ein K-Isomorphismus: Sei $a \in L$. Sei N die Menge aller Nullstellen des Minimalpolynoms $m_{a,K}$ in L. Dann ist $\sigma|_N : N \to N$ eine Bijektion. Also existiert zu $a \in N$ ein Element $b \in N$ mit $\sigma(b) = a$. Also ist σ surjektiv. Mit 19.1 folgt die Behauptung. Die Voraussetzung, dass die Körpererweiterung L/K algebraisch ist, kann nicht weggelassen werden: Die Abbildung $K(X) \to K(X)$, definiert durch $f(X) \to f(X^2)$ ist kein Isomorphismus.

Beispiel 24.2.

(a) Das Polynom $m_{i,\mathbb{R}} = X^2 + 1 \in \mathbb{R}[X]$ hat die Nullstellen $\{\pm i\} \subseteq \mathbb{C}$. Definiere Körperhomomorphismen

$$\sigma_0 : \mathbb{C} \to \mathbb{C} \text{ mit } i \mapsto i \text{ und } \sigma_0|_{\mathbb{R}} = \mathrm{id}$$
$$\sigma_1 : \mathbb{C} \to \mathbb{C} \text{ mit } i \mapsto -i \text{ und } \sigma_1|_{\mathbb{R}} = \mathrm{id}\ .$$

Dann ist $\sigma_0 = \mathrm{id}_{\mathbb{C}}$ und σ_1 ist die komplexe Konjugation, $x + iy \to x - iy$. Also ist $\mathrm{Aut}(\mathbb{C}/\mathbb{R}) = \{\sigma_0, \sigma_1\} \simeq \mathbb{Z}_2$.

(b) Sei $L = \mathbb{Q}(a) \subseteq \mathbb{R}$ mit $a = \sqrt[3]{2}$ und sei $K = \mathbb{Q}$. Das Polynom $m_{a,K} = X^3 - 2$ hat die Nullstellen $\{a, \xi a, \xi^2 a\}$ mit $\xi = e^{2\pi i/3}$. Da $a\xi, a\xi^2 \in \mathbb{C} \setminus \mathbb{R}$ ist, folgt $\mathrm{Aut}(\mathbb{Q}(a)/\mathbb{Q}) = \{\mathrm{id}\}$.

Bemerkung 24.3. Zur Vereinfachung beweisen wir in dieser Vorlesung die Galoiskorrespondenz nur für endliche Körpererweiterungen der Charakteristik Null. Diese haben die folgende fundamentale Eigenschaft: *Sei K ein Körper mit* $\mathrm{char}\, K = 0$. *Sei $f \in K[X]$ unzerlegbar und sei L eine Körpererweiterung von K. Dann hat f keine mehrfachen Nullstellen in L.* Ein unzerlegbares Polynom mit dieser Eigenschaft heißt separabel. Der Beweis der letzten Aussage ist Übungsaufgabe. Von jetzt an seien Körpererweiterungen endlich und in Charakteristik Null. Die in diesem Kapitel präsentierten Resultate sind ohne diese zusätzliche Voraussetzung unter Umständen nicht richtig.

Theorem 24.4 (Satz vom primitiven Element)**.** *Sei L/K eine endliche Körpererweiterung mit* $\mathrm{char}\, K = 0$. *Dann ist L/K einfach, d. h. es existiert $c \in L$ mit $L = K(c)$.*

Bemerkung: Dieser Satz gilt allgemeiner für endliche separable Körpererweiterungen beliebiger Charakteristik. Eine Körpererweiterung L/K ist separabel, falls jedes Element $a \in L$ separabel über K ist. Und ein Element $a \in L$ ist separabel über K, genau dann, wenn das Minimalpolynom $m_{a,K}$ in einem beliebigen Erweiterungskörper keine mehrfachen Nullstellen besitzt, also separabel ist. Hat ein Körper K die Charakteristik Null, so ist nach obiger Bemerkung jede algebraische Erweiterung L von K separabel.

Beweis.

(i) Sei $L = K(a, b)$ mit $a, b \in L$ algebraisch über K. Sei Z ein Zerfällungskörper von $m_{a,K} \cdot m_{b,K} \in K[X]$. Dann existieren $a_1, \ldots, a_r \in Z$ mit $m_{a,K} = \prod_{i=1}^{r}(X - a_i)$ und $b_1, \ldots, b_s \in Z$ mit $m_{b,K} = \prod_{j=1}^{s}(X - b_j)$. Hierbei sind $\{a_1, \ldots, a_r\}$ paarweise verschieden nach 24.3 und genauso sind $\{b_1, \ldots, b_s\}$ paarweise verschieden. Ohne Einschränkung sei $a = a_1$ und $b = b_1$. Da K unendlich viele Elemente hat, existiert $\lambda \in K$ mit

$$a + \lambda b \neq a_i + \lambda b_j$$

für alle $1 \leq i \leq r$ und $2 \leq j \leq s$. Hierbei ist

$$\lambda \neq \frac{a_i - a_1}{b_1 - b_j}\ .$$

Definiere $c \coloneqq a + \lambda b \in K(a, b)$. Es gilt $K(c) \subseteq K(a, b)$.

(ii) Definiere $h(x) \coloneqq m_{a,K}(c - \lambda x) \in K(c)[X]$. Dann ist

$$h(b_1) = m_{a,K}(c - \lambda b_1) = m_{a,K}(a) = 0$$

und

$$h(b_j) = m_{a,K}(\underbrace{a_1 + \lambda b_1 - \lambda b_j}_{\neq a_i}) \neq 0$$

für $j \geq 2$. Daher ist

$$\mathrm{ggT}_{K(c)}(m_{b,K}, h) = \mathrm{ggT}_Z(m_{b,K}, h) = X - b \ .$$

Es folgt $b \in K(c)$ und damit $a = c - \lambda b \in K(c)$. Mit (i) folgt $K(c) = K(a, b)$. Die Behauptung folgt jetzt induktiv (mit 20.8). □

Korollar 24.5. *Sei L/K endlich und* $\mathrm{char}\, K = 0$. *Dann ist* $|\operatorname{Aut}(L/K)| \leq [L : K]$.

Beweis. Nach 24.4 existiert $a \in L$ mit $L = K(a)$. Damit folgt

$$|\operatorname{Aut}(L/K)| \overset{24.1}{=} \#\{\text{NS von } m_{a,K} \text{ in } L\} \leq [a : K] = [K(a) : K] = [L : K]$$

nach 18.2 und 20.4 . □

Definition 24.6. Eine endliche Körpererweiterung L/K in Charakteristik Null heißt *galoissch* oder *Galoiserweiterung*, falls für die Anzahl der K-Automorphismen von L gilt: $|\operatorname{Aut}(L/K)| = [L : K]$. Im Falle einer Galoiserweiterung schreiben wir $\mathrm{Gal}(L/K) := \operatorname{Aut}(L/K)$, genannt die *Galoisgruppe von* L/K.

Theorem 24.7. *Sei L/K eine endliche Körpererweiterung und* $\mathrm{char}\, K = 0$. *Dann sind äquivalent:*

(a) L/K ist galoissch.

(b) L ist Zerfällungskörper eines Polynoms über K.

(c) Ist $g \in K[X]$ unzerlegbar mit einer Nullstelle in L, so zerfällt g in L in Linearfaktoren.

Beweis. Nach 24.4 existiert ein Element $a \in L$ mit $L = K(a)$.
(a) $\Rightarrow$ (b): Es gilt

$$\#\{\text{NS von } m_{a,K} \text{ in } L\} \overset{24.1}{=} |\operatorname{Gal}(L/K)| \overset{\text{(a)}}{=} [L : K] = [K(a) : K] \overset{20.4}{=} \deg(m_{a,K}) \ .$$

Damit ist L Zerfällungskörper von $m_{a,K}$.
(b) $\Rightarrow$ (c): Sei L Zerfällungskörper von $f \in K[X]$. Sei Z Zerfällungskörper von $f \cdot g \in K[X]$, d. h. $L \subseteq Z$. Sei $b \in L$ Nullstelle von g und sei $c \in Z$ eine Nullstelle von g.

(i) Es ist $g \in K[X]$ unzerlegbar mit Nullstellen $b, c \in Z$. Nach 22.7 existiert ein K-Isomorphismus $\varphi : K(b) \to K(c)$, d. h. $[K(b) : K] = [K(c) : K]$.

(ii) Da L Zerfällungskörper von f über K ist, ist $L(b)$ Zerfällungskörper von f über $K(b)$ und $L(c)$ Zerfällungskörper von f über $K(c)$. Nach 23.6 existiert ein Isomorphismus $\hat{\varphi} : L(b) \to L(c)$ mit $\hat{\varphi}|_{K(b)} = \varphi$. Mit (i) folgt $[L(b) : K(b)] = [L(c) : K(c)]$.

(iii) Es folgt:

$$\begin{aligned}[L : K] &\overset{b \in L}{=} [L(b) : K] \overset{19.8}{=} [L(b) : K(b)][K(b) : K] \\ &\overset{\text{(i), (ii)}}{=} [L(c) : K(c)][K(c) : K] = [L(c) : K] = [L(c) : L][L : K] \ ,\end{aligned}$$

also ist $[L(c) : L] = 1$. Damit haben wir gezeigt, dass $c \in L$ ist für alle Nullstellen c von g. Dies zeigt, dass g über L in Linearfaktoren zerfällt.

(c) $\Rightarrow$ (a): Das Polynom $m_{a,K} \in K[X]$ ist unzerlegbar mit Nullstelle a in L. Aus (c) folgt, dass $m_{a,K}$ über L in Linearfaktoren zerfällt und nach 24.3 sind alle Nullstellen einfach. Nach 18.2 hat $m_{a,K}$ also $\deg(m_{a,K}) = [a : K]$ viele verschiedene Nullstellen. Somit ist

$$|\operatorname{Aut}(L/K)| \overset{24.1}{=} [a : K] \overset{20.4}{=} [K(a) : K] = [L : K] \ .$$

Nach 24.6 ist L/K daher galoissch. □

Definition 24.8. Sei $0 \neq f \in K[X]$ mit Zerfällungskörper L. Wir definieren

$$\operatorname{Gal}(f) \coloneqq \operatorname{Gal}(L/K) = \operatorname{Aut}(L/K) \ ,$$

genannt *Galoisgruppe von f*.

Lemma 24.9. *Sei $f \in K[X]$ mit $\deg f = n > 0$.*

(a) Die Galoisgruppe $\operatorname{Gal}(f)$ permutiert die Nullstellen von f in seinem Zerfällungskörper. Insbesondere folgt $\operatorname{Gal}(f) \leq S_n$.

(b) Sei f unzerlegbar über K, dann folgt $\deg(f) \mid |\operatorname{Gal}(f)|$.

Beweis.

(a) Sei L ein Zerfällungskörper von f über K. Sei $N_f \coloneqq \{$ NS von f in $L\}$. Dann ist also $L = K(N_f)$. Die Galoisgruppe $\operatorname{Gal}(f)$ operiert auf N_f durch

$$\operatorname{Gal}(f) \times N_f \to N_f, (\sigma, a) \mapsto \sigma \cdot a \coloneqq \sigma(a)$$

Nach 24.1 ist $\sigma \cdot a \in N_f$. Sei $\sigma \in \operatorname{Gal}(f)$ mit $\sigma(a) = a$ für alle $a \in N_f$. Da $L = K(N_f)$ ist, folgt $\sigma = \mathrm{id}$. Also operiert $\operatorname{Gal}(f)$ treu auf N_f. Nach 7.2 ist also $\operatorname{Gal}(f) \hookrightarrow S_{|N_f|} = S_n$.

(b) Sei $a \in L$ Nullstelle von f. Dann folgt $K(a) \leq L$ und $m_{a,K} = \lambda \cdot f$ für ein $\lambda \in K^\times$. Nach 19.8 ist $n = \deg(f) = \deg(m_{a,K}) \overset{20.4}{=} [K(a) : K] \mid [L : K]$. Da L ein Zerfällungskörper von f ist, ist L/K galoissch nach 24.7, d. h. $|\operatorname{Gal}(f)| = [L : K]$. Also gilt $\deg(f) \mid |\operatorname{Gal}(f)|$. □

Bemerkung 24.10.

(1) Sei $K \leq Z \leq L$ eine Körpererweiterung mit L/K galoissch. Dann ist L/Z galoissch. Im Allgemeinen ist Z/K nicht galoissch.

Beweis.

(a) Nach 24.7 ist L Zerfällungskörper eines Polynoms $f \in K[X]$. Also ist $L = K(N_f)$ mit $N_f = \{\text{NS von } f \text{ in } L\}$. Es folgt $L = K(N_f) \subseteq Z(N_f) \subseteq L$. Also ist L Zerfällungskörper von $f \in Z[X]$ und damit L/Z galoissch nach 24.7.

(b) Betrachte $\mathbb{Q} \leq \mathbb{Q}(a) \leq \mathbb{Q}(a, \xi)$ mit $a = \sqrt[3]{2}$ und $\xi = e^{2\pi i/3}$. Der Körper $\mathbb{Q}(a, \xi)$ ist Zerfällungskörper von $X^3 - 2 \in \mathbb{Q}[X]$. Also ist $\mathbb{Q}(a, \xi)/\mathbb{Q}$ galoissch nach 24.7. Nach 24.2 ist $|\operatorname{Aut}(\mathbb{Q}(a)/\mathbb{Q})| = 1 \neq 3 = [\mathbb{Q}(a) : \mathbb{Q}]$. Also ist $\mathbb{Q}(a)/\mathbb{Q}$ nicht galoissch. □

(2) Sei K ein Körper mit $\operatorname{char} K = 0$. Sei L/K eine Körpererweiterung mit $[L : K] = 2$. Dann ist L/K galoissch.

Beweis. Nach 24.4 existiert $c \in L$ mit $L = K(c)$. Da

$$2 = [L : K] = [K(c) : K] \overset{20.4}{=} [c : K],$$

also $2 = \deg m_{c,K}$. Da $m_{c,K} = (X - c)q$ mit $\deg q = 1$ und $q \in L[X]$ ist, folgt $m_{c,K} = (X - c)(X - d)$ für $d \in L$. Also ist L Zerfällungskörper von $m_{c,K}$. Mit 24.7 folgt, dass L/K galoissch ist. □

(3) Galoissch ist nicht transitiv:

(a) Betrachte $\mathbb{Q} \subseteq \mathbb{Q}(\sqrt{2}) \subseteq \mathbb{Q}(\sqrt[4]{2})$. Da $(\sqrt[4]{2})^2 = \sqrt{2}$ gilt, ist

$$[\mathbb{Q}(\sqrt[4]{2}) : \mathbb{Q}(\sqrt{2})] = 2,$$
$$[\mathbb{Q}(\sqrt{2}) : \mathbb{Q}] = 2\ .$$

Hierbei ist zu prüfen, dass $\sqrt[4]{2} \notin \mathbb{Q}(\sqrt{2})$ ist. Nach (2) sind $\mathbb{Q}(\sqrt[4]{2})/\mathbb{Q}(\sqrt{2})$ und $\mathbb{Q}(\sqrt{2})/\mathbb{Q}$ galoissch.

(b) Nach 19.8 ist $[\mathbb{Q}(\sqrt[4]{2}) : \mathbb{Q}] = 4$. Das Polynom $f = X^4 - 2$ hat Nullstellen $a, -a, ia, -ia$, wobei $a = \sqrt[4]{2}$. Dann hat f Nullstelle a in $\mathbb{Q}(a)$, zerfällt aber nicht in Linearfaktoren über $\mathbb{Q}(a)$. Nach 24.7 (c) ist $\mathbb{Q}(a)/\mathbb{Q} = \mathbb{Q}(\sqrt[4]{2})/\mathbb{Q}$ nicht galoissch.

Kapitel 25

Hauptsatz der Galoistheorie

In diesem Kapitel beweisen wir den Hauptsatz der Galoistheorie. Im Falle einer galoisschen Körpererweiterung L/K liefert dieser eine inklusionsumkehrende Korrespondenz zwischen den Untergruppen der Galoisgruppe $\mathrm{Gal}(L/K)$ und den Zwischenkörpern, die zwischen K und L liegen. Um diese Korrespondenz vollständig zu beschreiben, benötigen wir die folgende Definition:

Definition 25.1. Sei L ein Körper und sei $G \leq \mathrm{Aut}(L)$ eine Untergruppe. Definiere $L^G \coloneqq \{a \in L \mid \sigma(a) = a \text{ für alle } \sigma \in G\}$, genannt *Fixkörper von G in L*. Dann ist $L^G \leq L$ Teilkörper.

Beweis. Da $\sigma(0) = 0$ und $\sigma(1) = 1$ für alle $\sigma \in G$, folgt $0, 1 \in L^G$. Seien $a, b \in L^G$ mit $b \neq 0$, d. h. $\sigma(a) = a$ und $\sigma(b) = b$ für alle $\sigma \in G$. Dann ist

$$\begin{aligned}\sigma(a \pm b) &= \sigma(a) \pm \sigma(b) = a \pm b \\ \sigma(a \cdot b^{-1}) &= \sigma(a) \cdot \sigma(b)^{-1} = ab^{-1}\end{aligned}$$

für alle $\sigma \in G$. Also ist $a \pm b, ab^{-1} \in L^G$. □

Beispiel 25.2. Sei $L = \mathbb{C}$ und $G = \{\sigma_0 = \mathrm{id}_{\mathbb{C}}, \sigma_1 = (z \mapsto \overline{z})\}$. Dann ist $\mathbb{Z}_2 \simeq G \leq \mathrm{Aut}(L)$ und

$$L^G = \{a \in \mathbb{C} \mid \sigma_0(a) = a, \sigma_1(a) = a\} = \{a \in \mathbb{C} \mid \overline{a} = a\} = \mathbb{R} \leq \mathbb{C}\ .$$

Lemma 25.3 (Lemma von Artin)**.** *Sei L ein Körper und $G \leq \mathrm{Aut}(L)$ eine endliche Untergruppe. Dann ist L eine Körpererweiterung über L^G mit $[L : L^G] \leq |G|$. (Wir zeigen $[L : L^G] = |G|$ in 25.4.)*

Beweis.

(a) Sei $G = \{\sigma_1, \ldots, \sigma_n\}$ mit $|G| = n$. Ohne es weiter zu erwähnen, benutzen wir in diesem Beweis wiederholt, dass die Elemente aus G Körperhomomorphismen sind. Sei $K = L^G \subseteq L$. Nach 19.2 ist L ein K-Vektorraum. Wir zeigen: Beliebige $n + 1$ Vektoren aus L sind linear abhängig über K. Dann folgt $[L : K] \leq n = |G|$.

(b) Seien $a_1, \ldots, a_{n+1} \in L$. Das homogene LGS über L,

$$\sum_{i=1}^{n+1} \sigma_j(a_i) x_i = 0, \qquad 1 \leq j \leq n, \tag{25.1}$$

besteht aus n Gleichungen in $n+1$ Variablen. Da die Anzahl der Variablen größer ist als die Anzahl der Gleichungen, folgt, dass der Lösungsraum von (25.1) mindestens eindimensional ist. Insbesondere: Ist $x = (x_1, \dots, x_{n+1})$ Lösung von (25.1), so ist auch λx mit $\lambda \in K$ Lösung von (25.1). Sei $\sigma \in G$. Dann gilt:

$$\sum_{i=1}^{n+1} \sigma_j(a_i)\sigma(x_i) = \sigma\left(\sum_{i=1}^{n+1}(\sigma^{-1} \circ \sigma_j)(a_i)x_i\right) .$$

Also ist x eine Lösung von (25.1) genau dann, wenn $\sigma x \coloneqq (\sigma x_1, \dots, \sigma x_{n+1})$ eine Lösung von (25.1) ist.

(c) Wähle eine nicht-triviale Lösung von (25.1), die mit maximal vielen Nullen beginnt und so normiert ist, dass der erste Eintrag $\neq 0$ Eins ist. Eine solche Lösung existiert nach (b). Das heißt, es existiert $0 \leq s \leq n$ mit

$$x = (0, \dots, 0, 1, x_{s+2}, \dots, x_{n+1})$$

ist Lösung von (25.1). Sei $\sigma \in G$. Nach (b) ist

$$\sigma x = (0, \dots, 0, 1, \sigma x_{s+2}, \dots, \sigma x_{n+1})$$

eine Lösung von (25.1). Ebenfalls nach (b) ist dann auch

$$y \coloneqq x - \sigma(x) = (0, \dots, 0, 0, x_{s+2} - \sigma x_{s+2}, \dots, x_{n+1} - \sigma x_{n+1})$$

eine Lösung von (25.1). Nach Wahl von x muss y die Nulllösung sein, da y mehr Nullen am Anfang hat als x. Also ist $\sigma x_t = x_t$ für $1 \leq t \leq n+1$, d. h. $\sigma(x) = x$. Folglich ist $x_i \in L^G = K$ für alle $i \in \{1, \dots, n+1\}$.

(d) Wähle $\sigma_j = \mathrm{id}$ in (25.1) und x wie in (c). Dann ist

$$\sum_{i=1}^{n+1} a_i x_i = 0$$

und nicht alle $x_i \in K$ sind Null. Somit ist die Menge $\{a_1, \dots, a_{n+1}\} \subseteq L$ linear abhängig über K. □

Proposition 25.4. *Sei L/K endlich und* $\operatorname{char} K = 0$. *Dann gilt: L/K galoissch, genau dann, wenn $K = L^G$ mit $G \leq \mathrm{Aut}(L)$. In diesem Fall gilt, dass* $\mathrm{Gal}(L/K) = G$, *d. h.* $[L : K] = |G|$.

Beweis.

(a) (i) Sei $K = L^G$ mit $G \leq \mathrm{Aut}(L)$. Sei $\lambda \in K$, dann ist $\sigma(\lambda) = \lambda$ für alle $\sigma \in G$. Also ist $\sigma|_K = \mathrm{id}_K$ für alle $\sigma \in G$. Somit ist $G \leq \mathrm{Aut}(L/K) = \mathrm{Gal}(L/K)$.

(ii) Da L/K endlich ist und $\operatorname{char} K = 0$, folgt $|\operatorname{Gal}(L/K)| \overset{24.5}{\leq} [L : K] \overset{25.3}{\leq} |G| \overset{\text{(i)}}{\leq} |\operatorname{Gal}(L/K)|$. Also ist $G = \mathrm{Gal}(L/K)$ und $|G| = [L : K] = [L : L^G]$. Nach 24.6 folgt, dass L/K galoissch ist.

(b) Sei L/K galoissch. Sei $G = \mathrm{Gal}(L/K)$. Dann ist $G \leq \mathrm{Aut}(L)$ und nach (a) gilt: $L/L^G = L/L^{\mathrm{Gal}(L/K)}$ ist galoissch mit Galoisgruppe $\mathrm{Gal}(L/L^G) = G = \mathrm{Gal}(L/K)$. Nach Voraussetzung ist auch L/K galoissch. Aus

$$[L : L^G] \overset{24.6}{=} |G| = |\operatorname{Gal}(L/K)| \overset{24.6}{=} [L : K] \overset{19.8}{=} [L : L^G][L^G : K]$$

folgt $[L^G : K] = 1$, also $L^G = K$. □

Theorem 25.5 (Hauptsatz der Galoistheorie, Teil 1)**.** *Sei L/K endlich und galoissch mit* $\operatorname{char} L = 0$*. Sei*

$$\mathcal{Z} := \{Z \mid K \leq Z \leq L \text{ } \textit{Zwischenkörper}\}$$
$$\mathcal{U} := \{U \mid U \leq \operatorname{Gal}(L/K) \text{ } \textit{Untergruppe}\} \ .$$

Definiere

$$\psi : \mathcal{Z} \to \mathcal{U}, Z \mapsto \operatorname{Gal}(L/Z)$$
$$\phi : \mathcal{U} \to \mathcal{Z}, G \mapsto L^G \ .$$

Dann ist ψ inklusionsumkehrende bijektive Abbildung mit $\psi^{-1} = \phi$ und $[L : Z] = |\operatorname{Gal}(L/Z)|$.

Beweis.

(a) Sei $G \in \mathcal{U}$, also $G \leq \operatorname{Gal}(L/K) \leq \operatorname{Aut}(L)$. Nach 25.4 ist L/L^G galoissch mit $\operatorname{Gal}(L/L^G) = G$. Insbesondere ist $[L : L^G] \overset{24.6}{=} |G|$. Also ist

$$G \xrightarrow{\phi} L^G \xrightarrow{\psi} \operatorname{Gal}(L/L^G) = G \ ,$$

d. h. $\psi \circ \phi = \mathrm{id}_{\mathcal{U}}$.

(b) Sei $Z \in \mathcal{Z}$, also $K \leq Z \leq L$. Nach Voraussetzung ist L/K galoissch, also nach 24.10 auch L/Z galoissch. Nach 25.4 ist $Z = L^G$ für $G = \operatorname{Gal}(L/Z)$. Also ist

$$Z \xrightarrow{\psi} G = \operatorname{Gal}(L/Z) \xrightarrow{\phi} L^G = L^{\operatorname{Gal}(L/Z)} = Z \ ,$$

d. h. $\phi \circ \psi = \mathrm{id}_{\mathcal{Z}}$.

(c) Seien $Z_1, Z_2 \in \mathcal{Z}$ mit $Z_1 \leq Z_2$. Dann ist $\operatorname{Gal}(L/Z_2) \leq \operatorname{Gal}(L/Z_1)$. Somit ist die Bijektion ψ inklusionsumkehrend. □

Theorem 25.6 (Hauptsatz der Galoistheorie, 2. Teil)**.** *Sei $K \leq Z \leq L$ eine endliche Körpererweiterung mit* $\operatorname{char} L = 0$ *und L/K galoissch. Dann sind äquivalent:*

(a) Z/K galoissch.

(b) $\operatorname{Gal}(L/Z) \trianglelefteq \operatorname{Gal}(L/K)$.

(c) $\sigma(Z) \subseteq Z$ für alle $\sigma \in \operatorname{Gal}(L/K)$.

In diesem Fall gilt:

$$\operatorname{Gal}(L/K)\big/\operatorname{Gal}(L/Z) \simeq \operatorname{Gal}(Z/K) \ .$$

Bemerkung: $\sigma(Z) \subseteq Z$ impliziert $\sigma(Z) = Z$, siehe 24.1(c).

Beweis.

(i) Wir zeigen (a) impliziert (c). Sei Z/K galoissch. Nach 24.7 ist Z Zerfällungskörper eines Polynoms $0 \neq f \in K[X]$. Dann ist also $Z = K(a_1, \ldots, a_n)$, wobei das Polynom f gegeben ist durch $f = \lambda \cdot \prod_{i=1}^{n}(X - a_i)$ mit $\lambda \in K$ und $a_i \in Z$. Sei $\sigma \in \operatorname{Gal}(L/K)$, dann folgt $\sigma(a_i) = a_j$ mit $1 \leq j \leq n$ nach 24.1 für alle $1 \leq i \leq n$. Es folgt $\sigma(Z) \subseteq K(a_1, \ldots, a_n) \subseteq Z$ für alle $\sigma \in \operatorname{Gal}(L/K)$.

(ii) Wir zeigen (c) impliziert (b) impliziert (a). Wir definieren die Abbildung

$$F : \mathrm{Gal}(L/K) \to \mathrm{Gal}(Z/K) \text{ mit } \sigma \mapsto \sigma|_Z.$$

Nach Voraussetzung (c) ist $\sigma(Z) \subseteq Z$, also ist $\sigma|_Z \in \mathrm{Gal}(Z/K)$. Also ist F wohldefinierter Gruppenhomomorphismus mit

$$\mathrm{Ker}\, F = \{\sigma \in \mathrm{Gal}(L/K) \mid \sigma|_Z = \mathrm{id}_Z\} = \mathrm{Gal}(L/Z) \overset{4.6}{\trianglelefteq} \mathrm{Gal}(L/K).$$

Nach dem Homomorphiesatz für Gruppen folgt

$$\mathrm{Gal}(L/K)\big/\mathrm{Gal}(L/Z) \simeq \mathrm{im}\, F \leq \mathrm{Gal}(Z/K)\ .$$

Da L/K galoissch ist, folgt mit 24.10, dass L/Z galoissch ist. Also ist

$$|\,\mathrm{Gal}(Z/K)| \overset{24.5}{\leq} [Z:K] \overset{19.8}{=} \frac{[L:K]}{[L:Z]} \overset{24.6}{=} \frac{|\,\mathrm{Gal}(L/K)|}{|\,\mathrm{Gal}(L/Z)|} = |\,\mathrm{im}\, F| \leq |\,\mathrm{Gal}(Z/K)|\ .$$

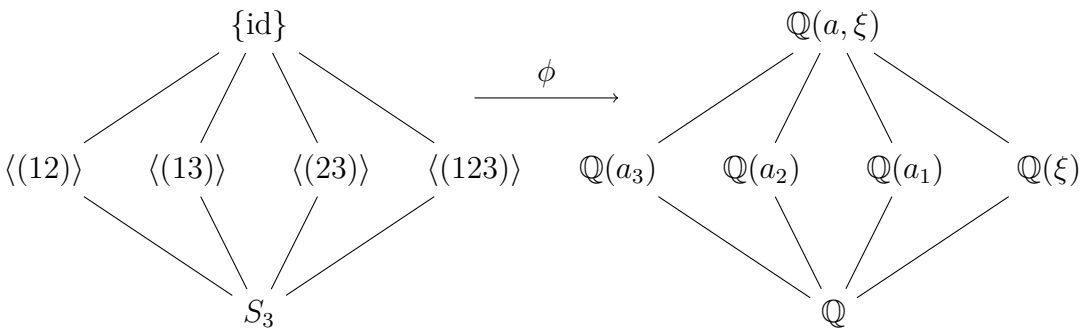
Dies zeigt $|\,\mathrm{Gal}(Z/K)| = [Z:K]$. Nach 24.6 ist also Z/K galoissch mit

$$\mathrm{Gal}(L/K)\big/\mathrm{Gal}(L/Z) \simeq \mathrm{Gal}(Z/K)\ . \qquad \square$$

Beispiel 25.7.

(a) Sei $f = X^3 - 2 \in \mathbb{Q}[X]$. Sei $a = \sqrt[3]{2}$ und $\xi = e^{2\pi i/3}$. Die Nullstellen von f sind $a_1 = a, a_2 = a\xi, a_3 = a\xi^2$. Dann ist $L := \mathbb{Q}(a,\xi) = \mathbb{Q}(a_1,a_2,a_3)$ Zerfällungskörper von f. Nach 24.7 ist $L/\mathbb{Q}$ galoissch mit $|\,\mathrm{Gal}(f)| = |\,\mathrm{Gal}(L/\mathbb{Q})| = [L:\mathbb{Q}] = 6$. Nach 24.9 ist $\mathrm{Gal}(f) \leq S_3$. Es folgt also $\mathrm{Gal}(f) = S_3$.

(b) Wir erhalten die folgende Korrespondenz zwischen dem Untergruppenverband von S_3 und dem Zwischenkörperverband von $L/\mathbb{Q}$:



Wir berechnen die Fixkörper, die zu den Untergruppen der S_3 korrespondieren: Die Galoisgruppe $\mathrm{Gal}(f)$ permutiert die Nullstellen $\{a_1,a_2,a_3\}$. Setze zum Beispiel $G = \langle(12)\rangle = \{\sigma_0, \sigma_{12}\}$. Hierbei ist σ_0 die Identitätsabbildung. Die Abbildung σ_{12} ist definiert durch $\sigma_{12}|_{\mathbb{Q}} = \mathrm{id}$ und σ_{12} vertauscht die Nullstellen a_1 und a_2, während die Nullstelle a_3 fest bleibt:

$$a_1 \mapsto a_2, \quad a_2 \mapsto a_1, \quad a_3 \mapsto a_3.$$

Dann ist also $a_3 \in L^G$, und wegen $a_2 \neq \sigma_{12}(a_2)$ ist $L^G \neq L$. Es ist also

$$6 = [L:\mathbb{Q}] = \underbrace{[L:L^G]}_{\neq 1} \cdot [L^G : \mathbb{Q}(a_3)] \cdot \underbrace{[\mathbb{Q}(a_3):\mathbb{Q}]}_{=3}.$$

Damit folgt $[L : \mathbb{Q}(a_3)] = 1$, also ist $L^G = \mathbb{Q}(a_3)$.

Als nächstes betrachten wir die Untergruppe $G = \langle(123)\rangle = \{\sigma_0, \sigma_{123}, \sigma_{132}\}$ von S_3. Hierbei ist wieder σ_0 die Identitätsabbildung und zum Beispiel $\sigma := \sigma_{123}$ definiert durch $a_1 \mapsto a_2, a_2 \mapsto a_3, a_3 \mapsto a_1$ und $\sigma|_{\mathbb{Q}} = \mathrm{id}$. Es ist $\xi = \frac{a\xi}{a} = \frac{a_2}{a_1}$. Also ist

$$\sigma(\xi) = \sigma\left(\frac{a_2}{a_1}\right) = \frac{\sigma(a_2)}{\sigma(a_1)} = \frac{a_3}{a_2} = \frac{a\xi^2}{a\xi} = \xi.$$

Es ist $\sigma(a_1) \neq a_1$, also ist $L^G \neq L$. Da $\sigma_{132} = \sigma_{123}^{-1}$ ist $\xi \in L^G$, und damit ist $\mathbb{Q}(\xi) \subseteq L^G \neq L$. Mit einem Gradargument wie oben folgt $\mathbb{Q}(\xi) = L^G$. Man beachte auch, da $G \triangleleft S_3$, folgt mit 25.6, dass die Körpererweiterung $L/\mathbb{Q}(\xi)$ galoissch ist.

Kapitel 26

Kreisteilungspolynome

Sei K ein Körper, dann ist $K^\times$ eine multiplikative Gruppe. Eine *Einheitswurzel* ist ein Element $z \in K^\times$ endlicher Ordnung. Gilt hierbei $z^n = 1$ so heißt z eine *n-te Einheitswurzel*. Ist sogar $\operatorname{ord} z = n$, so ist z eine *primitive* n-te Einheitswurzel. Wir schreiben

$$E_n(K) = \{n\text{-te Einheitswurzel in } K\}$$
$$E_n'(K) = \{z \in E_n(K) \mid z \text{ primitiv}\} .$$

Die Menge $E_n(K)$ ist eine Gruppe bezüglich Multiplikation, und als endliche Untergruppe von $K^\times$ ist also $E_n(K)$ zyklisch, siehe 23.2. Sei K_n der Zerfällungskörper von $X^n - 1 \in K[X]$. Ist $\operatorname{char} K \nmid n$, so folgt mit 18.2 und 18.5, dass $E_n(K_n) \simeq \mathbb{Z}_n$. Da $E_n(K) \leq E_n(K_n)$ Untergruppe ist, folgt mit 3.7, dass $E_n(K) \simeq \mathbb{Z}_d$ ist für $d \mid n$. Ist $\operatorname{ord} z = n$, so ist $\operatorname{ord} z^k = n$ genau dann, wenn $(n, k) = 1$ ist, siehe 3.5. Es folgt, dass $E_n'(K_n) \simeq \mathbb{Z}_n^\times$ ist.

Wir betrachten im Folgenden die gewöhnlichen komplexen n-ten Einheitswurzeln, und bestimmen das Minimalpolynom einer primitiven n-ten Einheitswurzel. Als Anwendung hiervon, und als Anwendung des Hauptsatzes der Galoistheorie charakterisieren wir, für welche natürlichen Zahlen n das regelmäßige n-Eck mit Zirkel und Lineal konstruierbar ist.

Definition 26.1. Das Polynom $\phi_n := \prod_{z \in E_n'(\mathbb{C})}(x - z) \in \mathbb{C}[X]$ heißt *n-tes Kreisteilungspolynom*.

Beispiel 26.2. Nach Definition ist ϕ_n normiert. Wir sehen in 26.5, dass $\phi_n \in \mathbb{Z}[X]$ ist, somit ist ϕ_n primitiv (siehe 17.5). Sei $\varphi(n) := |\mathbb{Z}_n^\times|$ die Eulersche phi-Funktion, siehe 12.4. Nach Definition ist also $\deg \phi_n = \varphi(n)$. Wir berechnen einige kleine Kreisteilungspolynome:

n	1	2	3	4
$X^n - 1$	$X - 1$	$X^2 - 1$	$X^3 - 1$	$X^4 - 1$
E_n	$\{1\}$	$\{\pm 1\}$	$\{1, \zeta, \zeta^2\}$	$\{\pm 1, \pm i\}$
E_n'	$\{1\}$	$\{-1\}$	$\{\zeta, \zeta^2\}$	$\{\pm i\}$
ϕ_n	$X - 1$	$X + 1$	$(X - \zeta)(X - \zeta^2) = X^2 + X + 1$	$(X - i)(X + i) = X^2 + 1$,

Heirbei ist $\zeta := e^{2\pi i/3}$, und man sieht anhand eines Bildes zur Vektoraddition von ζ und ζ^2, dass $\zeta + \zeta^2 = -1$ ist.

Die Berechnung von Kreisteilungspolynomen mittels 26.1 wird schnell mühselig. Das folgende Lemma hilft uns, weitere Kreisteilungspolynome zu berechnen.

Lemma 26.3. *Es gilt $X^n - 1 = \prod_{d \mid n} \phi_d$.*

Beweis. Es ist $\mathbb{Z}_n = \dot\bigcup_{d|n}\{\text{Elemente in } \mathbb{Z}_n \text{ der Ordnung } d\}$. Also ist

$$E_n(\mathbb{C}) = \bigcup_{d|n}\dot{} \, E'_d(\mathbb{C})$$

Damit folgt $X^n - 1 = \prod_{d|n} \phi_d$. □

Beispiel 26.4. Mit der Aussage des letzten Lemmas lassen sich Kreisteilungspolynome rekursiv berechnen.

(a) Sei p prim. Dann ist $X^p - 1 = \phi_1 \cdot \phi_p$, also

$$\phi_p = \frac{X^p - 1}{X - 1} = X^{p-1} + X^{p-2} + \ldots + X + 1 \; .$$

(b) Es gilt $X^8 - 1 = \phi_1 \cdot \phi_2 \cdot \phi_4 \cdot \phi_8 = (X-1)(X+1)(X^2+1) \cdot \phi_8 = (X^4 - 1) \cdot \phi_8$. Also folgt

$$\phi_8 = \frac{X^8 - 1}{X^4 - 1} = X^4 + 1 \; .$$

Theorem 26.5. *Es ist $\phi_n \in \mathbb{Z}[X]$.*

Beweis. Wir führen den Beweis durch Induktion nach n. Sei die Behauptung wahr für alle $d < n$. Dann ist

$$f_n \coloneqq \prod_{\substack{d|n \\ d \neq n}} \phi_d \in \mathbb{Z}[X] \subseteq \mathbb{Q}[X]$$

normiert und primitiv. Also existieren $q, r \in \mathbb{Q}[X]$ mit $X^n - 1 = q \cdot f_n + r$ und $\deg r < \deg f_n$. Nach 26.3 gilt $X^n - 1 = \phi_n \cdot f_n$. Also ist $(\phi_n - q) f_n = r \in \mathbb{C}[X]$ und

$$\deg(\phi_n - q) + \deg f_n = \deg r < \deg f_n \; .$$

Also ist $r = 0$ und damit $\phi_n = q \in \mathbb{Q}[X]$. Also ist $f_n \mid X^n - 1$ in $\mathbb{Q}[X]$. Da f_n primitiv ist, folgt mit 17.10 (d), dass $f_n \mid X^n - 1$ in $\mathbb{Z}[X]$, d. h. $\phi_n \in \mathbb{Z}[X]$.[1] □

Theorem 26.6 (Unzerlegbarkeit der Kreisteilungspolynome)**.** *Sei $n \in \mathbb{N}$ und z eine n-te Einheitswurzel.*

(a) Ist $m \in \mathbb{N}$ mit $\mathrm{ggT}(n, m) = 1$, so haben z und z^m dasselbe Minimalpolnom.

(b) Sei $\zeta_n \coloneqq e^{2\pi i/n} \in \mathbb{C}$. Dann hat ζ_n das Minimalpolynom ϕ_n über $\mathbb{Q}$.

Beweis. Wir benutzen wiederholt, dass $\mathbb{Z}[X]$ und $\mathbb{Z}_p[X]$ (für p prim) faktoriell sind, siehe 17.12, also eine eindeutige Primfaktorzerlegung haben.

(a) (i) Sei zunächst $m = p$ eine Primzahl. Angenommen, $f = \min_{z,\mathbb{Q}}$ und $g \coloneqq \min_{z^p,\mathbb{Q}}$ und $f \neq g$. Da z und z^m Nullstellen von $X^n - 1$ sind, folgt $f \mid X^n - 1$ und $g \mid X^n - 1$ in $\mathbb{Q}[X]$ nach 20.2. Da $f \neq g$ jeweils unzerlegbar sind, und die Primfaktorzerlegung in $\mathbb{Q}[X]$ eindeutig ist, existiert $h \in \mathbb{Q}[X]$ mit $X^n - 1 = f \cdot g \cdot h$. Da $X^n - 1, f$ und g normiert sind, ist auch h normiert. Mit 17.10 (d) folgt $f, g, h \in \mathbb{Z}[X]$.

[1] Alternativ: Da der Leitkoeffizient von f_n gleich 1 und damit eine Einheit in $\mathbb{Z}$ ist, existieren $q, r \in \mathbb{Z}[X]$ mit $X^n - 1 = q \cdot f_n + r$, siehe 13.9. Nach 26.3 gilt $X^n - 1 = \phi_n \cdot f_n$, also $(\phi_n - q) f_n = r \in \mathbb{Z}[X]$ und wegen $\deg(\phi_n - q) + \deg f_n = \deg r < \deg f_n$ folgt $r = 0$, also $\phi_n = q \in \mathbb{Z}[X]$.

(ii) Rechne modulo p. Schreibe $\overline{q} \coloneqq \sum \overline{a_i} X^i$ für $q = \sum a_i X^i$ mit $\overline{a_i} \coloneqq a_i \bmod p$. Wegen $\operatorname{ggT}(p, n) = 1$, ist $(X^n - 1)' = nX^{n-1} \neq 0$. Mit 17.12 folgt, dass

$$\operatorname{ggT}_{\mathbb{Z}_p[X]}(X^n - 1, nX^{n-1}) = 1 \ .$$

Ist $q = \operatorname{ggT}(\overline{f}, \overline{g})$, dann folgt $q^2 \mid \overline{f}\,\overline{g}\,\overline{h} = X^n - 1$. Wegen $\operatorname{ggT}(p, n) = 1$ hat $X^n - 1$ keine mehrfachen Primfaktoren. Es folgt

$$1 = q = \operatorname{ggT}(\overline{f}, \overline{g}) \ .$$

(iii) Da z^p Nullstelle von g ist, ist z Nullstelle von $g(X^p)$. Nach 20.2 ist $f \mid g(X^p)$ in $\mathbb{Q}[X]$. Außerdem ist f primitiv, also auch $f \mid g(X^p) \in \mathbb{Z}[X]$ nach 17.10 (c). Somit existiert $q \in \mathbb{Z}[X]$ mit $f \cdot q = g(X^p)$. Reduziere modulo p. Nach 23.8 gilt in $\mathbb{Z}_p[X]$:

$$(aX^i)^p = a^p (X^p)^i = a(X^p)^i, \text{ also } \overline{g(X)}^p = \overline{g(X^p)} = \overline{f} \cdot \overline{q} \ .$$

Damit ist $\operatorname{ggT}(\overline{f}, \overline{g}) \neq 1$, ein Widerspruch zu (ii). Also ist $f = g$. Damit haben also z und z^p dasselbe Minimalpolynom.

(iv) Sei $m \in \mathbb{N}$ mit $\operatorname{ggT}(m, n) = 1$. Sei $m = p_1 \cdot \ldots \cdot p_r$ mit p_i prim. Mit (iii) folgt:

- z und z^{p_1} haben dasselbe Minimalpolynom.
- z^{p_1} und $(z^{p_1})^{p_2} = z^{p_1 p_2}$ haben dasselbe Minimalpolynom.
- Etc.

Induktiv folgt also, dass z und z^m dasselbe Minimalpolynom haben.

(b) Sei $f \coloneqq \min_{\zeta_n, \mathbb{Q}}$. Dann ist f nach (a) das Minimalpolynom aller anderen primitiven n-ten Einheitswurzeln. Somit ist $\deg f \geq |\mathbb{Z}_n^\times| = \varphi(n) = \deg \phi_n$. Mit 20.2 folgt $\deg f = \deg \phi_n$, also $f = \phi_n$. □

Proposition 26.7. *Wir benutzen die Notation aus Kapitel 21. Sei $\{0, 1\} \subseteq M \subseteq \mathbb{C}$ und $K = \mathbb{Q}(M \cup \overline{M})$. Sei $z \in \mathbb{C}$ algebraisch über K. Sei L Zerfällungskörper von $m_{z,K} \in K[X]$. Ist $[L : K] = 2^k$ für ein $k \in \mathbb{N}_0$, dann ist $z \in \hat{M}$.*

Beweis. Die Körpererweiterung L/K ist galoissch nach 24.7. Mit 24.6 folgt

$$|\operatorname{Gal}(L/K)| = [L : K] = 2^k \ .$$

Nach 9.9 ist $\operatorname{Gal}(L/K)$ auflösbar. Wegen 9.13 existiert eine Kompositionsreihe mit zyklischen Faktoren, d. h.

$$\{\mathrm{id}\} = N_r \trianglelefteq N_{r-1} \trianglelefteq \ldots \trianglelefteq N_0 = \operatorname{Gal}(L/K)$$

mit ${}^{N_i}\!/_{N_{i+1}} \simeq C_2$ für alle i. Nach 25.5 existiert eine Körperkette

$$K = L_0 < L_1 < \ldots < L_r = L$$

mit $L_i \coloneqq L^{N_i}$ mit $[L : L_i] = |\operatorname{Gal}(L/L_i)| = |N_i| = 2^{r-i}$. Nach 19.8 folgt $[L_i : L_{i-1}] = 2$ für $1 \leq i \leq r$. Da $z \in L$ ist, folgt $z \in \hat{M}$, siehe 21.5. □

Theorem 26.8. *Das regelmäßige n-Eck ist genau dann mit Zirkel und Lineal konstruierbar, wenn $\varphi(n)$ eine Zweierpotenz ist.*

Beweis. Ohne Einschränkung sei $M = \{0, 1\}$, d. h. $\mathbb{Q}(M \cup \overline{M}) = \mathbb{Q}$. Das regelmäßige n-Eck ist aus M genau dann konstruierbar, wenn $e^{2\pi i/n} =: \zeta_n \in \mathbb{C}$ konstruierbar ist.

(a) Sei $\zeta_n \in \hat{M}$. Nach 21.6 und 26.6 folgt

$$\varphi(n) = [\zeta_n : \mathbb{Q}] = [\mathbb{Q}(\zeta_n) : \mathbb{Q}] = 2^k \ .$$

(b) Sei $\varphi(n) = 2^k$. Dann folgt mit 26.6:

$$[\mathbb{Q}(\zeta_n) : \mathbb{Q}] = [\zeta_n : \mathbb{Q}] = \varphi(n) = 2^k \ .$$

Nach 26.7 ist dann ζ_n konstruierbar. □

Bemerkung 26.9. Um zu verstehen, wann das regelmässige n-Eck konstruierbar ist, bleibt also zu verstehen, wann $\varphi(n)$ eine Potenz von Zwei ist.

(a) *Behauptung:* Ist $2^b + 1$ eine Primzahl für $b \in \mathbb{N}$, dann ist b eine Zweierpotenz.

Beweis. Angenommen, b ist keine Zweierpotenz. Dann ist $b = c \cdot q$ mit $q > 1$ ungerade, d. h. $c < b$. Es ist

$$X^q - Y^q = (X - Y)(X^{q-1} + X^{q-2}Y + \ldots + XY^{q-2} + Y^{q-1}) \ .$$

Setze $X = 2^c, Y = -1$. Dann existiert also ein $z \in \mathbb{Z}$ mit

$$2^b + 1 = (2^c + 1)z,$$

also $2^c + 1 \mid 2^b + 1$ mit $c < b$, und damit ist $2^b + 1$ nicht prim. □

(b) Eine Primzahl der Form $2^{2^n} + 1$ heißt *Fermatsche Primzahl*: Mit der Bezeichnung $F_n := 2^{2^n} + 1$ ist

$$\begin{aligned} F_0 &= 3 \\ F_1 &= 5 \\ F_2 &= 17 \\ F_3 &= 257 \\ F_4 &= 65537 \ . \end{aligned}$$

Es ist ein offenes Problem, ob es weitere Fermatsche Primzahlen gibt.

(c) *Behauptung:* Sei $n \in \mathbb{N}$. Dann ist $\varphi(n)$ eine Zweierpotenz genau dann, wenn $n = 2^m \cdot p_1 \cdot \ldots \cdot p_r$ mit $r, m \geq 0$ ist, wobei $p_1, \ldots, p_r$ paarweise verschiedene Fermatsche Primzahlen sind.

Beweis. Sei $n = \prod_i p_i^{n_i}$ Primfaktorzerlegung. Nach 12.4 folgt

$$\varphi(n) = \prod_i (p_i - 1)p_i^{n_i - 1} \ . \tag{26.1}$$

Angenommen, $\varphi(n)$ ist eine Zweierpotenz. Dann folgt $n_i = 1$ für alle ungeraden p_i und $p_i - 1$ ist eine Zweierpotenz. Also ist $p_i = 2^{b_i} + 1$ für $b_i \in \mathbb{N}_0$. Nach (a) gilt $b_i = 2^{a_i}$ für $a_i \in \mathbb{N}_0$. Also ist $p_i = 2^{2^{a_i}} + 1$ eine Fermatsche Primzahl. Die Rückrichtung des Beweises folgt direkt aus (26.1). □

Kapitel 27

Auflösbarkeit von Polynomgleichungen

Bei einer allgemeine quadratische Gleichung gibt die Mitternachtsformel oder pq-Formel die Lösungen dieser Gleichung an. Wir wollen zeigen, dass es für die allgemeine Polynomgleichung fünften Grades keine Lösungsformel gibt, genauer, dass sich die Nullstellen der Gleichung fünften Grades nicht aus den Koeffizienten dieser Gleichung, Körperoperationen und komplexem Wurzelziehen bestimmen lassen.

Definition 27.1. Sei L/K eine Körpererweiterung.

(a) Eine Körpererweiterung $L = K(a)$ heißt *einfache Radikalerweiterung*, falls es ein $n \in \mathbb{N}$ gibt mit $a^n \in K$.

(b) Eine Körpererweiterung L/K heißt *Radikalerweiterung* (kurz RE), falls es eine endliche Kette von Körpern gibt,

$$K = K_0 \leq K_1 \leq \ldots \leq K_m = L,$$

mit K_i/K_{i-1} einfache Radikalerweiterung, (wobei hierbei n variieren darf).

Beispiel 27.2.

(a) Die Körpererweiterung $\mathbb{Q}(\sqrt{2}, \sqrt[3]{1+\sqrt{2}})$ über $\mathbb{Q}$ ist eine Radikalerweiterung, denn

$$\mathbb{Q} \subseteq \mathbb{Q}(\sqrt{2}) \subseteq \mathbb{Q}(\sqrt{2})(\sqrt[3]{b})$$

mit $b = 1 + \sqrt{2} \in \mathbb{Q}(\sqrt{2})$.

(b) Sei $K \leq L \leq M$ eine Körpererweiterung, sodass L/K und M/L Radikalerweiterungen sind. Dann ist auch M/K eine Radikalerweiterung.

Definition 27.3. Ein Polynom $f = X^n + a_{n-1}X^{n-1} + \ldots + a_1 + a_0 \in \mathbb{C}[X]$ heißt (durch Radikale) *auflösbar*, falls es eine Radikalerweiterung von $\mathbb{Q}(a_0, a_1, \ldots, a_{n-1})$ gibt, die alle Nullstellen von f enthält.

Beispiel 27.4. Sei $f = X^2 + px + q \in \mathbb{C}[X]$. Wir lösen die Gleichung $f = 0$ durch quadratische Ergänzung. Hierbei gilt

$$\left(X + \frac{p}{2}\right)^2 = \frac{p^2}{4} - q.$$

Die Gleichung $f = 0$ hat also die Nullstellen

$$x_{1,2} = -\frac{p}{2} \pm \sqrt{\frac{p^2}{4} - q} \in \mathbb{Q}\left(p, q, \sqrt{\frac{p^2}{4} - q}\right).$$

Da $\mathbb{Q}\left(p, q, \sqrt{\frac{p^2}{4} - q}\right)/\mathbb{Q}(p, q)$ eine Radikalerweiterung ist, ist f durch Radikale auflösbar. Polynome vom Grad drei (mittels Cardanischer Formeln) und vier sind ebenfalls durch Radikale auflösbar.

Beispiel 27.5. Wir suchen in diesem Kapitel nach einem Kriterium, wann Polynomgleichungen auflösbar sind. Hierzu benötigen wir, dass die folgende Galoisgruppe abelsch ist.

(a) Sei $L = K(z)$ mit $z^n \in K$. Sei ζ eine primitive n-te Einheitswurzel in K. Dann hat das Polynom $f \coloneqq X^n - z^n \in K[X]$ die Nullstellen $\{\zeta^k z \mid 1 \leq k \leq n\}$, und damit ist L ein Zerfällungskörper von $f \in K[X]$. Nach 24.7 ist damit L/K galoissch.

(b) Sei $F : \mathrm{Gal}(L/K) \to (\mathbb{Z}_n, +)$ mit $\sigma_i \mapsto l_i$, wobei $\sigma_i(z) = \zeta^{l_i} z$ angenommen werden kann, denn mit z ist auch $\sigma(z)$ eine Nullstelle von f. Wir zeigen, dass F ein injektiver Gruppenhomomorphismus ist.

(i) Wegen $\zeta^{l_j} \in K$ ist $(\sigma_i \circ \sigma_j)(z) = \sigma_i(\zeta^{l_j} z) = \sigma_i(\zeta^{l_j}) \cdot \sigma_i(z) = \zeta^{l_j} \cdot \sigma_i(z) = \zeta^{l_j + l_i} z$, also folgt $F(\sigma_i \circ \sigma_j) = l_i + l_j = F(\sigma_i) + F(\sigma_j)$. Also ist F ein Gruppenhomomorphismus.

(ii) Angenommen, $F(\sigma_i) = 0 + n\mathbb{Z}$. Dann folgt $\sigma_i(z) = \zeta^0 z = z$, also $\sigma_i = \mathrm{id}_L$. Dies zeigt, dass F injektiv ist, d. h. $\mathrm{Gal}(L/K) \leq (\mathbb{Z}_n, +)$ Untergruppe. Nach 3.7 ist damit $\mathrm{Gal}(L/K)$ zyklisch, insbesondere abelsch.

Proposition 27.6. *Sei L/K eine Radikalerweiterung und* $\operatorname{char} K = 0$*. Dann existiert eine Radikalerweiterung M/L, sodass M/K galoissch (und Radikalerweiterung) ist.*

Beweis. Induktion nach $[L : K]$: Sei $K = K_0 \leq K_1 \leq \ldots \leq K_{m-1} \leq K_m = L$ mit K_i/K_{i-1} einfache Radikalerweiterung für alle i.

(a) Sei $m = 1$. Sei $L = K(\lambda)$ mit $\lambda^n \in K$. Sei ζ eine primitive n-te Einheitswurzel im Zerfällungskörper von $X^n - 1 \in L[X]$. Sei $M \coloneqq L(\zeta)$. Dann enthält M alle Nullstellen $\{\zeta^k \lambda \mid 1 \leq k \leq m\}$ von $X^n - \lambda^n \in K[X]$. Somit ist M Zerfällungskörper von $X^n - \lambda^n \in K[X]$. Nach 24.7 ist M/K galoissch und $K \leq L \leq M$, wobei M/L und L/K Radikalerweiterungen sind, d. h. M/K ist eine Radikalerweiterung.

(b) Sei $m > 1$. Ohne Einschränkung sei $K_{m-1} \neq L$, und es sei $L = K_{m-1}(\mu)$ mit $\mu^n \in K_{m-1}$. Es ist $[K_{m-1} : K] < [L : K]$. Nach Induktionsvoraussetzung existiert eine Radikalerweiterung M'/K_{m-1} mit M'/K galoissch. Definiere

$$f \coloneqq \prod_{\sigma \in \mathrm{Gal}(M'/K)} (X^n - \sigma(\mu^n)) .$$

Für alle $\tau \in \mathrm{Gal}(M'/K)$ gilt, unter Benutzung von 1.6 und mit der Notation von 22.6:

$$\tau^* f = \prod_{\sigma \in \mathrm{Gal}(M'/K)} (X^n - (\tau \circ \sigma)(\mu^n)) = f .$$

Also liegt jeder Koeffizient von f im Fixkörper ${M'}^{\mathrm{Gal}(M'/K)} = K$, siehe 25.4, und somit ist $f \in K[X]$. Sei M Zerfällungskörper von f über M'. Dann entsteht M aus M' durch Adjunktion von n-ten Wurzeln von $\sigma(\mu^n)$. Somit ist M/M' eine Radikalerweiterung. Da auch M'/K_{m-1} nach Induktionsvoraussetzung eine Radikalerweiterung ist, ist M/K_{m-1} eine Radikalerweiterung. Nach Konstruktion, für $\sigma = \mathrm{id}$, ist $\mu \in M$, also $L \subseteq M$. Wieder nach der Induktionsvoraussetzung ist M'/K galoissch, also ist M' Zerfällungskörper von $g \in K[X]$. Da M Zerfällungskörper von $f \in M'[X]$ ist, ist M Zerfällungskörper von $f \cdot g \in K[X]$, d. h. nach 24.7 folgt M/K galoissch. □

Theorem 27.7 (Galois)**.** *Sei* $\mathrm{char}\, K = 0$ *und* $f \in K[X] \setminus K$*. Sei* L *Zerfällungskörper von* f *über* K*. Ist* f *durch Radikale auflösbar, dann ist* $\mathrm{Gal}(L/K)$ *eine auflösbare Gruppe. (Die Umkehrung dieses Satzes gilt ebenfalls.)*

Beweis.

(a) (i) Ist f durch Radikale auflösbar, dann ist L/K eine Radikalerweiterung. Nach 27.6 gibt es eine Radikalerweiterung M/L mit M/K galoissch. Dann existieren $z_1, \ldots, z_r \in M$ und $n_i \in \mathbb{N}$ mit $M = K(z_1, \ldots, z_r)$ und $z_i^{n_i} \in K(z_1, \ldots, z_{i-1})$ für $1 \leq i \leq r$. Sei $n_0 \coloneqq n_1 \cdot n_2 \cdot \ldots \cdot n_r$. Sei M' Zerfällungskörper von $g \coloneqq X^{n_0} - 1 \in M[X]$. Sei H die Menge der Nullstellen von g in M'. Nach 18.5 hat g keine doppelten Nullstellen. Dann ist $H \leq (M')^\times$ eine endliche Untergruppe mit $|H| = n_0$. Nach 23.2 ist dann $H \simeq \mathbb{Z}_{n_0}$.

Sei z_0 ein Erzeuger von H, d. h. z_0 ist eine primitive n_0-te Einheitswurzel. Dann ist $M' = M(H) = M(z_0) = K(z_0, z_1, \ldots, z_r)$ mit

$$\begin{aligned} z_0^{n_0} &\in K \\ z_1^{n_1} &\in K \subseteq K(z_0) \\ z_2^{n_2} &\in K(z_1) \subseteq K(z_0, z_1) \\ &\text{etc.,} \end{aligned}$$

d. h. M'/K ist eine Radikalerweiterung.

(ii) Wir wissen, dass M/K galoissch ist. Nach 24.7 ist M Zerfällungskörper von $0 \neq h \in K[X]$, also ist M' Zerfällungskörper von $g \cdot h \in K[X]$. Nach 24.7 ist M'/K galoissch.

Insgesamt haben wir also, dass M'/K galoissch und eine Radikalerweiterung ist, und M' enthält alle n_0-ten Einheitswurzeln.

(b) (i) Wir wenden die Galoiskorrespondenz an. Setze hierzu

$$\begin{aligned} G &\coloneqq \mathrm{Gal}(M'/K) \\ K_i &\coloneqq K(z_0, z_1, \ldots, z_i) \\ G_i &\coloneqq \mathrm{Gal}(M'/K_i) \end{aligned}$$

für $0 \leq i \leq r$.

Da $K_{-1} \coloneqq K \leq K_0 \leq K_1 \leq \ldots \leq K_r = M'$ ist, folgt mit 25.5, dass

$$\{\mathrm{id}\} = G_r \leq G_{r-1} \leq \ldots \leq G_0 \leq G =: G_{-1} \,. \tag{27.1}$$

Für $i \geq 1$ enthält der Körper K_{i-1} das Element $z_0^{n_0/n_i}$ mit $\mathrm{ord}(z_0^{n_0/n_i}) \overset{3.5}{=} n_i$. Ist $i = 0$, so ist $K_0 = K(z_0)$ mit $\mathrm{ord}(z_0) = n_0$. Daher ist K_i/K_{i-1} eine einfache

n_i-Radikalerweiterung, die eine primitive n_i-te Einheitswurzel enthält. Nach 27.5 ist K_i/K_{i-1} galoissch mit abelscher Galoisgruppe. Nach 25.6 folgt damit, dass $G_i \trianglelefteq G_{i-1}$ mit

$$G_{i-1}/G_i \simeq \mathrm{Gal}(M'/K_{i-1})/\mathrm{Gal}(M'/K_i) \simeq \mathrm{Gal}(K_i/K_{i-1}) \ .$$

(ii) Nach (i) ist (27.1) eine Normalreihe von G mit abelschen Faktoren. Nach 9.7 ist G daher eine auflösbare Gruppe. Nach Voraussetzung und 24.7 ist L/K galoissch. Nach 25.6 ist $\mathrm{Gal}(M'/L) \trianglelefteq \mathrm{Gal}(M'/K)$ mit

$$\mathrm{Gal}(M'/K)/\mathrm{Gal}(M'/L) \simeq \mathrm{Gal}(L/K) \ .$$

Nach 9.8 folgt, dass $\mathrm{Gal}(L/K)$ auflösbar ist. □

Beispiel 27.8.

(a) Sei $f = X^5 - 4X + 2 \in \mathbb{Q}[X]$. Nach 18.9 mit $p = 2$ ist f unzerlegbar. Es ist

$$f - 2 = X^5 - 4X = X(X^4 - 4) = X(X^2 - 2)(X^2 + 2) \ .$$

Der Graph von $f - 2$ hat also drei reelle Nullstellen, und lässt sich damit leicht zeichnen. Der Graph von f entseht aus dem Graphen von $f-2$ durch Verschiebung um zwei in y-Richtung. Kurvendiskussion liefert $\max f > 0$ und $\min f < 0$. Damit hat f insbesondere drei reelle Nullstellen. Wir wollen zeigen, dass f nicht durch Radikale auflösbar ist.

(b) (i) Allgemeiner, sei $f \in \mathbb{Q}[X]$ unzerlegbar und $\deg f = 5$. Sei L ein Zerfällungskörper von f, d. h. $L = \mathbb{Q}(a_1, \ldots, a_5)$, wobei $f = \lambda \prod_{i=1}^{5}(X - a_i)$ mit $\lambda \in \mathbb{Q}$. Angenommen, $a_1, a_2, a_3 \in \mathbb{R} \setminus \mathbb{Q}$ und $a_4, a_5 \in \mathbb{C} \setminus \mathbb{R}$. Nach 18.6 gilt $a_5 = \overline{a_4}$.

(ii) Nach 24.7 ist $L/\mathbb{Q}$ galoissch. Nach 24.9 ist $\mathrm{Gal}(L/\mathbb{Q}) = \mathrm{Gal}(f)$ isomorph zu einer Untergruppe G von S_5 mit $5 = \deg(f) \mid |G|$. Nach 8.5 existiert $\pi \in G$ mit $\mathrm{ord}(\pi) = 5$, d. h. π ist ein 5-Zykel.

(iii) Für $i \in \{1, \ldots, 5\}$ gilt $\overline{a_i} \in \{a_1, \ldots, a_5\}$. Also ist $\overline{L} = L$. Die Abbildung $L \to L$, definiert durch $z \mapsto \overline{z}$ liegt in $\mathrm{Gal}(L/\mathbb{Q})$. Da $\overline{\overline{z}} = z$, ist die Abbildung komplexe Konjugation ein Element der Ordnung zwei. Genauer gilt $\tau \coloneqq (45) \in G$.

(iv) Wir sortieren die fünf Nullstellen wiederholt um. Durch Umsortierung der Nullstellen a_i sei ohne Einschränkung $\pi = (12345)$. Es ist $\pi = (12345) = (23451) = (34512) = \ldots$. Ohne Einschränkung sei hierbei also $\tau = (1a)$ mit $2 \leq a \leq 5$. Da 5 prim ist, sind π, π^2, π^3 und π^4 jeweils 5-Zykel mit

$$\begin{aligned} \pi &: 1 \mapsto 2, \\ \pi^2 &: 1 \mapsto 3, \\ \pi^3 &: 1 \mapsto 4 \\ \pi^4 &: 1 \mapsto 5 \ , \end{aligned}$$

Es gilt also $\pi^{a-1} : 1 \mapsto a$. Also ist $\pi^{a-1} = (1a\ldots) \in G$. Ohne Einschränkung sei also $\pi = (12345)$ und $\tau = (12)$. Wegen $S_5 = \langle \pi, \tau \rangle \subseteq G \subseteq S_5$ gilt $G = S_5 \simeq \mathrm{Gal}(L/\mathbb{Q})$. Nach 9.4 ist $\mathrm{Gal}(L/\mathbb{Q})$ nicht auflösbar. Nach 27.7 ist f nicht durch Radikale auflösbar.

Theorem 27.9.

(a) Das allgemeine Polynom vom Grad ≤ 4 ist durch Radikale auflösbar.

(b) Polynome mit abelscher Galoisgruppe sind durch Radikale auflösbar.

(c) Das allgemeine Polynom vom Grad $n \geq 5$ ist nicht durch Radikale auflösbar.

Beispiele von Polynomen mit abelscher Galoisgruppe sind die Kreisteilungspolynome ϕ_n. Nach 26.6 ist das Kreisteilungspolynom ϕ_n das Minimalpolynom von $\zeta_n := e^{2\pi i/n}$ über $\mathbb{Q}$ und $L := \mathbb{Q}(\zeta_n)$ ist Zerfällungskörper von $\phi_n \in \mathbb{Q}[X]$. Nach 24.7 ist die Körpererweiterung $L/\mathbb{Q}$ galoissch. Ist $\sigma \in \mathrm{Gal}(L/\mathbb{Q})$, so ist nach 24.1 das Element $\sigma(\zeta_n)$ eine Nullstelle von ϕ_n. Also existiert $1 \leq k_\sigma \leq n$ mit $(k_\sigma, n) = 1$ und $\sigma(\zeta_n) = \zeta^{k_\sigma}$. Definiere die Abbildung

$$F : \mathrm{Gal}(L/\mathbb{Q}) \to (\mathbb{Z}_n^\times, \cdot) \text{ mit } \sigma \mapsto k_\sigma.$$

Dann ist F ein Monomorphismus, also die Galoisgruppe $\mathrm{Gal}(L/\mathbb{Q})$ isomorph zu einer Untergruppe von $\mathbb{Z}_n^\times$.