# Körper- und Galoistheorie

**Rainer Vogt**

**WS 2009/2010**

# Inhaltsverzeichnis

# Teil I
# Grundlagen

## 1 Gruppen

Zunächst wiederholen wir kurz die Inhalte der Anfängervorlesung zu diesem Thema.

**1.1 Definition:** Eine **Gruppe** ist eine Menge $G$ mit einer Verknüpfung

$$G \times G \to G, \quad (a, b) \mapsto a * b,$$

die folgende Axiomen erfüllt.

(1) Assoziativität: $\forall\, a, b, c \in G$ gilt: $(a * b) * c = a * (b * c)$.

(2) Existenz eines neutralen Elements: Es gibt ein $e \in G$, so dass

$$a * e = e * a = a \quad \forall\, a \in G$$

(3) Existens von Inversen: Zu jedem $a \in G$ gibt es ein $\overline{a} \in G$, so dass $a * \overline{a} = \overline{a} * a = e$.

Gilt außerdem

(4) $a * b = b * a \quad \forall\, a, b \in G$

heißt $G$ *kommutative* oder *abelsche* Gruppe.

Erfüllt die Verknüpfung nur (1) und (2), aber nicht notwendig (3) heißt $G$ *Monoid*.

**1.2 Bemerkung:** (1) Das neutrale Element ist eindeutig bestimmt.

(2) Jedes Element $a$ einer Gruppe besitzt genau ein Inserves, man bezeichnet es mit $a^{-1}$, falls man "multiplikativ schreibt" und mit $-a$, falls man additiv schreibt.

(3) Man kann in den Axiomen (2) und (3) jeweils den linken oder auch den mittleren Tem weglassen (Beweis?). Für einen Monoid muß man aber (2) vollständig fordern.

(4) In einer Gruppe gilt die **Kürzungsregel**:

$$ax = ay \Rightarrow x = y$$

(5) Ein **endlicher** Monoid, in dem die Kürzungsregel gilt, ist eine Gruppe (Beweis?).

(6) Vorsicht beim Invertieren: Das Inverse von $a \cdot b$ ist $b^{-1} \cdot a^{-1}$ und nicht $a^{-1} \cdot b^{-1}$.

## Unterstrukturen

**1.3 Definition:** Sei $(G, \cdot)$ ein Monoid oder eine Gruppe und $A \subset G$ eine Teilmenge. $A$ heißt *Untermonoid* bzw. *Untergruppe* von $G$, wenn die Verknüpfung $\cdot$ eine Verknüpfung auf $A$ definiert, so dass $(A, \cdot)$ ein Monoid mit demselben neutralen Element bzw. eine Gruppe mit demselben neutralen und denselben inversen Elementen ist. D.h. die Struktur der Obermenge schränkt zur selben Struktur auf der Untermenge ein.

**1.4 Beispiel:** $I = [0,1]$ mit der Verknüpfung $t_1 * t_2 = \max(t_1, t_2)$ ist ein Monoid mit 0 als neutralen Element. Für $0 \leq s < 1$ ist $[0, s]$ ein Untermonoid. Offensichtlich ist auch $(\{1\}, *)$ ein Monoid, aber KEIN Untermonoid von $I$.

Wir übersetzen die Definition 1.3 in ein nachprüfbares Kriterium.

**1.5 Satz:** (1) Eine Teilmenge $A$ eines Monoids $(M, \cdot)$ ist genau dann Untermonoid, wenn gilt

(i) $a, b \in A \Rightarrow a, b \in A$

(ii) $e \in A$

(2) Eine Teilmenge $A$ einer Gruppe $G$ ist genau dann Untergruppe, wenn gilt

(i) $A \neq \varnothing$

(ii) $a, b \in A \Rightarrow a \cdot b \in A$

(iii) $a \in A \Rightarrow a^{-1} \in A$

**1.6 Bemerkung:** Bedingungen (ii) und (iii) des Teiles (2) sind äquivalent zu

(iv) $a, b \in A \Rightarrow a \cdot b^{-1} \in A$

**1.7** Ist $M$ ein Monoid, dann ist die Teilmenge $M^*$ der invertierbaren Elementen von $M$ eine Untergruppe von $M$.

**1.8 Definition und Satz:** Ist $A$ eine beliebige Teilmenge einer Gruppe $G$, dann gibt es eine kleinste Untergruppe $\langle A\rangle$ von $G$, die $A$ enthält. D.h. ist $U$ eine Untergruppe von $G$, die $A$ enthält, dann gilt $\langle A\rangle \subset U$. Die Untergruppe $\langle A\rangle$ besteht aus allen endlichen Produkten (Wiederholungen sind erlaubt) von Elementen aus $A$ oder deren Inversen.

Der Beweis benutzt folgende einfache Tatsache.

**1.9** Ist $\{U_i, i \in J\}$ eine beliebige, nicht-leere Familie von Untergruppen einer Gruppe $G$, dann ist auch ihr Schnitt $\bigcap_{i\in J} U_i$ Untergruppe von $G$. □

**Beweis 1.8:** $\langle A\rangle = \bigcap\{U \subset G; U \text{ Untergruppe }, A \subset U\}$
Der zweite Teil ist dem Leser überlassen.

**1.10 Bezeichnung:** Ist $A$ Teilmenge einer Gruppe $G$ und gilt $G = \langle A\rangle$, dann heißt $A$ *Erzeugendensystem* von $G$.

Eine Gruppe heißt *zyklisch*, wenn sie von einem einzigen Element erzeugt wird.

**1.11 Beispiel:** (1) Die Gruppen $\mathbb{Z}/m$ sind zyklisch, $\mathbb{Z}$ ist zyklisch.

$$\mathbb{Z}/m = \langle\overline{1}\rangle, \quad \mathbb{Z}/m = \langle 1\rangle = \langle -1\rangle$$

(2) Sei $G$ Gruppe, $A = \varnothing \subset G$, dann ist $\langle A\rangle = \{e\}$.

(3) Sei $M$ eine beliebige Menge, dann bezeichnet $\Sigma_M$ die *Permutationsgruppe* von $M$, d.h. die Gruppe der bijektiven Abbildungen $M \to M$ mit der Komposition als Verknüpfung. $\Sigma_n$ bezeichnet die Permutationsgruppe von $\{1, 2, \ldots, n\}$. $\Sigma_3$ wird erzeugt von

$$\left\{\begin{pmatrix}1&2&3\\2&1&3\end{pmatrix}, \begin{pmatrix}1&2&3\\2&3&1\end{pmatrix}\right\}$$

**1.12 Definition:** Die *Ordnung* einer Gruppe $G$ ist die Anzahl $|G|$ ihrer Elemente. Die Ordnung $\mathrm{ord}(x)$ eines Elementes $x \in G$ ist die Ordnung von $\langle x\rangle$.

**1.13** $\mathrm{ord}(x)$ ist die kleinste Zahl $k \in \mathbb{N}$, $k > 0$, so dass $x^k = e$. Gibt es kein solches $k$, ist $\mathrm{ord}(x) = \infty$ (Beweis?).

# 2 Homomorphismen

Will man Mengen mit Struktur miteinander vergleichen und eine Theorie darüber entwickeln, betrachtet man strukturerhaltende Abbildungen zwischen ihnen. Wie der erste Abschnitt ist auch dieser eine Wiederholung.

**2.1 Definition:** Eine Abbildung $f : (M, \cdot) \to (N, *)$ von Monoiden heißt *Homomorphismus*, wenn

(1) $f(x \cdot y) = f(x) * f(y) \quad \forall x, y \in M$

(2) $f(e_M) = e_N$, wobei $e_M \in M$ und $e_N \in N$ die neutralen Elemente sind.

Eine Abbildung $f : (G, \cdot) \to (H, *)$ von Gruppen heißt *Homomorphismus*, wenn

(1) $f(x \cdot y) = f(x) * f(y) \quad \forall x, y \in G$

(2) $f(e_G) = e_H$

(3) $f(x^{-1}) = (f(x))^{-1} \quad \forall x \in G$

Bei Gruppen genügt es, nur die Bedingung (1) zu kontrollieren:

**2.2** Für eine Abbildung $f : (G, \cdot) \to (H, *)$ von Gruppen gilt:

$$f \text{ ist Homomorphismus} \iff f(x \cdot y) = f(x) * f(y) \quad \forall x, y \in G$$

**2.3 Definition:** Ein Homomorphismus $f : G \to H$ von Monoiden oder Gruppen heißt

(1) *Monomorphismus*, wenn $f$ injektiv ist,

(2) *Epimorphismus*, wenn $f$ surjektiv ist,

(3) *Isomorphismus*, wenn $f$ bijektiv ist, wir schreiben $G \cong H$.

Ein Homomorphismus $f : G \to G$ heißt *Endomorphismus*, ist $f$ außerdem bijektiv, heißt $f$ *Automorphismus*.

**2.4** (1) Ist $f : G \to H$ ein Isomorphismus, dann ist auch die Umkehrabbildung $f^{-1} : H \to G$ ein Isomorphismus.

(2) Die Identität und die Komposition zweier Homomorphismen sind Homomorphismen.

**2.5** Ist $G$ ein Monoid oder eine Gruppe, dann ist die Menge $End(G)$ der Endomorphismen von $G$ ein Monoid unter der Komposition, und für die Menge der invertierbaren Elemente in $End(G)$ gilt

$$End(G)^* = Aut(G) := \{f : G \to G; f \text{ist Automorphismus}\}.$$

**2.6 Übung**
$$\begin{aligned} End(\mathbb{Z},+) &\cong (\mathbb{Z},\cdot) && \text{als Monoide} \\ Aut(\mathbb{Z},+) &\cong (\{\pm 1\},\cdot) && \text{als Gruppen} \end{aligned}$$

Das letzte Beispiel wirft die Frage aus: Was passiert im allgemeinen Fall mit den invertierbaren Elementen eines Monoids unter einem Homomorphismus?

**2.7 Satz:** Ist $f : M \to N$ ein Monoidhomomorphismus, dann definiert die Einschränkung von $f$ auf $M^*$ einen Homomorphismus von Gruppen $f^* : M^* \to N^*$.

**Beweis:**: Wir müssen nur zeigen: Ist $x \in M^*$, dann ist $f(x) \in N^*$. Es gilt
$$\begin{aligned} e_N = f(e_M) &= f(x \cdot x^{-1}) = f(x) \cdot f(x^{-1}) \\ &= f(x^{-1} \cdot x) = f(x^{-1}) \cdot f(x) \end{aligned}$$
Also ist $f(x^{-1})$ invers zu $f(x)$, d.h. $f(x) \in \mathbb{N}^*$. □

Auch die folgenden Ergebnisse sind aus der Anfängervorlesung bekannt.

**2.8 Satz:** (1) Ist $f : G \to H$ ein Monoidhomomorphismus und sind $A \subset G$ und $B \subset H$ Untermonoide, so sind auch $f(A)$ und $f^{-1}(B)$ Untermonoide.

(2) Ist $f : G \to H$ ein Gruppenhomomorphismus und sind $A \subset G$ und $B \subset H$ Untergruppen, dann sind auch $f(A) \subset H$ und $f^{-1}(B) \subset G$ Untergruppen. Insbesonderre ist Kern $f = f^{-1}(e_H) = \{x \in G; f(x) = e_H\}$ eine Untergruppe von $G$.

(3) Ein *Gruppen*homomorphismus $f : G \to H$ ist genau dann injektiv, wenn Kern $f = \{e_G\}$. □

# 3 Normalteiler

**3.1 Bezeichnung:** Sei $G$ eine Gruppe und seien $A, B$ Teilmengen von $G$

$$\begin{aligned} A \cdot B &= \{a, b;\ a \in A, b \in B\} \\ A^{-1} &= \{a^{-1};\ a \in A\} \end{aligned}$$

**3.2 Regeln:**

(1) $(A \cdot B) \cdot C = A \cdot (B \cdot C)$,

(2) $e \cdot A = A \cdot e = A$,

(3) $A \cdot A^{-1} \neq \{e\}$, falls $|A| > 1$.

**3.3 Aufgabe:** Ist $U \subset G$ eine nicht-leere Teilmenge. Dann gilt:

$$U \text{ ist Untergruppe von } G \iff U \cdot U = U \text{ und } U^{-1} = U$$

(ist $U$ endlich, genügt auf der rechten Seite $U \cdot U = U$.)

**3.4 Definition:** Ist $U$ Untergruppe einer Gruppe $G$, dann heißt $x \cdot U$ *Links-* und $U \cdot x$ *Rechtsnebenklasse* von $x$ bezgl. $U$.

**3.5** (1) Ist $A$ Linksnebenklasse bzgl. $U$ und $x \in A$, gilt $A = x \cdot U$.

(2) Zwei Linksnebenklassen bzgl. $U$ sind disjunkt oder gleich.

(3) $x \cdot U = y \cdot U \iff x^{-1}y \in U$

(4) $|x \cdot U| = |y \cdot U| \; \forall \, x, y \in G$

Dasselbe gilt für Rechtsnebenklassen.

Die Beweise sind einfach und aus der Anfängervorlesung bekannt. Aus (3) und (4) folgt

**3.6 Satz von Lagrange:** Ist $U$ Untergruppe einer endlichen Gruppe $G$, dann ist $|U|$ eine Teiler von $|G|$.

**3.7 Bezeichnung:** Die Zahl $|G|/|U|$ heißt *Index* von $U$ in $G$ und wird $[G : U]$ bezeichnet. Der Index gibt die Anzahl der verschiedenen Linksnebenklassen und der verschiedenen Rechtsnebenklassen an.

**3.8 Definition:** Eine Untergruppe $N$ von $G$ heißt *Normalteiler*(wir schreiben $N \lhd U$), wenn eine der folgenden äquivalenten Aussagen erfüllt ist:

(1) $x \cdot N = N \cdot x \quad \forall \, x \in G \; (\iff xNx^{-1} = x^{-1}Nx = N \quad \forall \, x \in G)$

(2) $x \cdot N \cdot x^{-1} \subset N \quad \forall \, x \in G$

(3) $x^{-1} \cdot N \cdot x \subset N \quad \forall \, x \in G$

**3.9 Beispiel:** Es gibt durchaus Untergruppen $U$ geeigneter Gruppen $G$, so dass $x \cdot U \cdot x^{-1} \subset U$, aber $x \cdot U \cdot x^{-1} \neq U$ für ein $x$. Nach (3.8.1) kann ein solches $U$ kein Normalteiler sein:

$$U = \{\begin{pmatrix} 1 & n \\ 0 & 1 \end{pmatrix};\ n \in \mathbb{Z}\} \text{ ist Untergruppe von } GL_2(\mathbb{Q}).$$

Sei $x = \begin{pmatrix} 5 & 0 \\ 0 & 1 \end{pmatrix}$ aus $GL_2(\mathbb{Q})$. Dann gilt $x \cdot \begin{pmatrix} 1 & n \\ 0 & 1 \end{pmatrix} \cdot x^{-1} = \begin{pmatrix} 1 & 5n \\ 0 & 1 \end{pmatrix} \in U$. Also folgt $x \cdot U \cdot x^{-1} \subset U$ aber $x \cdot U \cdot x^{-1} \neq U$. □

Die Bedeutung der Normalteiler liegt in folgendem Satz.

**3.10 Satz:** Sei $N$ Normalteiler von $G$ und $G/N$ die Menge der Linksnebenklassen. Dann gilt

$$(x \cdot N) \cdot (y \cdot N) = (x \cdot y) \cdot N.$$

Also definiert die Verknüpfung (3.1) auf $G/N$ eine Verknüpfung. $G/N$ ist mit dieser Verknüpfung eine Gruppe und die Projektion

$$p : G \to G/N, \quad x \mapsto x \cdot N$$

ist eine Epimorphismus mit Kern $N$. □

**3.11 Bezeichnung:** Die Gruppe $G/N$ heißt *Faktorgruppe* von $G$ nach $N$.

**3.12 Beispiel:**
(1) $\{e\}$ und $G$ sind Normalteiler von $G$, die *trivialen* Normalteiler.

(2) Ist $f : G \to H$ ein Homomorphismus und $N \lhd H$, dann ist $f^{-1}(N)$ Normalteiler von $G$. Insbesondere gilt $\operatorname{Kern} f \lhd G$. Ist $f$ **surjektiv** und $U \lhd G$, dann ist $f(U) \lhd H$.

(3) Jede Untergruppe vom Index 2 ist Normalteiler.

(4) $\mathbb{Z}/m$ ist Faktorgruppe: $\mathbb{Z}/m = \mathbb{Z}/(m \cdot \mathbb{Z})$.

Faktorgruppen und Normalteiler spielen bei der Untersuchung von Gruppen eine große Rolle. Die wichtigsten Werkzeuge in diesem Zusammenhang sind die Isomorphiesätze:

**3.13 Homomorphisatz:** Gegeben seien $N \lhd G$ und ein Homomorphismus $f : G \to H$, so dass $N \subset \operatorname{Kern} f$. Dann ist

$$\overline{f} : G/N \to H, \quad x \cdot N \mapsto f(x)$$

ein wohldefinierter Homomorphismus mit

$$\operatorname{Kern} \overline{f} = (\operatorname{Kern} f)/N = \{x \cdot N \in G/N;\ f(x) = e\}.$$

**Beweis:** Wir müssen zeigen, dass $\overline{f}$ unabhängig von der Repräsentantenwahl ist, d.h. ist $y \in x \cdot N$, dann muß $f(y) = f(x)$ gelten:

$$y \in x \cdot N \iff y^{-1}x \in N \Rightarrow f(y^{-1}x) = e, \text{ da } N \subset \operatorname{Kern} f$$

Es folgt $f(y)^{-1} \cdot f(x) = e$, also $f(y) = f(x)$.
$\overline{f}$ ist Homomorphismus, denn

$$\overline{f}(x \cdot N \cdot y \cdot N) = \overline{f}(xyN) = f(xy) = f(x) \cdot f(y) = \overline{f}(xN) \cdot \overline{f}(yN)$$

Weiter gilt: $\overline{f}(x \cdot N) = e \iff f(x) = e \iff x \in \operatorname{Kern} f$. □

**3.14 Folgerung:** ist $f : G \to H$ ein Homomorphismus, dann ist

$$\overline{f} : G/\operatorname{Kern} f \to H, \quad x \cdot \operatorname{Kern} f \mapsto f(x)$$

ein Monomorphismus. Es folgt ($\cong$ bedeutet "isomorph")

$$\overline{f} : G/\operatorname{Kern} f \cong \operatorname{Bild} f.$$

□

**3.15 Folgerung:** (1) Ist $G$ eine zyklische Gruppe, dann ist $G$ zu einer Gruppe der Form $\mathbb{Z}/m$, $m \in \mathbb{N}$, isomorph.

(2) Ist $|G| = p$, $p$ prim, dann ist $G \cong \mathbb{Z}/p$.

**Beweis:** (1) Sei $G = \langle x \rangle$. Dann ist

$$f : \mathbb{Z} \to G, \quad k \mapsto x^k$$

ein Epimorphismus. Nach (3.14) ist $G \cong \mathbb{Z}/\operatorname{Kern} f$. Die Untergruppen von $\mathbb{Z}$ sind aber von der Form $m \cdot \mathbb{Z}$. Es folgt $G \cong \mathbb{Z}/m$, wobei

$$m = \begin{cases} |G|, & \text{falls } |G| \text{ endlich ist.} \\ 0, & \text{falls } |G| = \infty \end{cases}$$

(2) Sei $x \neq e$ aus $G$ beliebig. Dann ist $\langle x \rangle$ Untergruppe von $G$. Nach dem Satz von Lagrange ist $|\langle x \rangle| = p$, da $|\langle x \rangle| > 1$. Es folgt $G = \langle x \rangle$. Nach Teil 1 ist $G \cong \mathbb{Z}/p$. □

**3.16 Beispiel:** $f : (\mathbb{R}, +) \to (S^1, \cdot)$, $x \mapsto e^{2\pi i x}$, definiert einen Epimorphismus auf den Einheitskreis $S^1$ der komplexen Zahlen $(\mathbb{C}^*, \cdot)$, Kern $f = \mathbb{Z}$. Also folgt

$$(S^1, \cdot) \cong (\mathbb{R}, +)/(\mathbb{Z}, +).$$

Aus dem Homomorphiesatz kann man zwei wichtige Isomorphiesätze folgern:

**3.17 Erster Isomorphisatz:** Sei $N \lhd G$ und $U$ Untergruppe von $G$. Dann gilt

(1) $U \cdot N = N \cdot U$, und $N \cdot U$ ist Untergruppe von $G$.

(2) $N \cap U \lhd U$, $N \lhd U \cdot N$.

(3) $U/U \cap N \to U \cdot N/N$, $u \cdot (U \cap N) \mapsto u \cdot N$, ist ein Isomorphismus.

**Beweis:** (1) $U \cdot N = \bigcup_{u \in U} u \cdot N = \bigcup_{u \in U} N \cdot u = N \cdot U$. Es folgt $(U \cdot N) \cdot (U \cdot N) = U \cdot U \cdot N \cdot N = U \cdot N$ und $(U \cdot N)^{-1} = N^{-1} \cdot U^{-1} = N \cdot U = UN$. Hier haben wir (3.3) benutzt und aus (3.3) folgt, dass $U \cdot N$ Untergruppe von $G$ ist.
(2), (3) Da $N = eN \subset U \cdot N$ und $N \lhd G$, ist $N \lhd U \cdot N$. Betrachte nun

$$f : U \to (U \cdot N)/N, \quad u \mapsto u \cdot N = u \cdot e \cdot N$$

$f$ ist ein Homomorphismus, da $N \lhd G$. Weiter ist $f$ surjektiv, denn ist $u \cdot n \cdot N \in (U \cdot N)/N$, so gilt $u \cdot n \cdot N = u \cdot N = f(u)$.
Kern $f = \{u \in U; u \cdot N = N\} = \{u \in U;\ u \in N\} = U \cap N$. Aus (3.14) folgt der Teil (3), da $U \cap N = \text{Kern}\, f$, folgt Teil (2). □

**3.18 Zweiter Isomorphisatz:** Seien $N_1, N_2$ Normalteiler von $G$ und $N_1 \subset N_2$. Dann ist $N_2/N_1 \lhd G/N_1$ und

$$(G/N_1)/(N_2/N_1) \to G/N_2, \quad (x \cdot N_1)(N_2/N_1) \mapsto x \cdot N_2$$

ist eine Isomorphismus.

**Beweis:** $f : G/N_1 \to G/N_2$, $x \cdot N_1 \mapsto x \cdot N_2$ ist ein Epimorphismus und Kern $f = \{x \cdot N_1 : x \cdot N_2 = N_2\} = \{x \cdot N_1;\ x \in N_2\} = N_2/N_1$. Aus (3.14) folgt das Resultat. □
Anwendungen dieser Resultate werden wir später sehen.

# 4 Produkte

Um eine Gruppe besser verstehen zu können, versucht man oft, sie in kleinere Bausteine zu zerlegen.

**4.1 Satz und Definition:** Sind $G$ und $H$ Monoide oder Gruppen, dann ist das *Produkt* $G \times H$ mit der Verknüpfung

$$(g_1, h_1) \cdot (g_2, h_2) := (g_1 \cdot g_2, h_1 \cdot h_2)$$

wieder ein Monoid bzw. eine Gruppe. Der Nachweis der Gruppenaxiome (Monoidaxiome) ist trivial.

**4.2 Bemerkung:** Wir können $G$ und $H$ im Falle von Gruppen als Normalteiler von $G \times H$ auffassen. Die Einbettungen sind gegeben durch

$$\begin{aligned} G \subset G \times H, &\quad g \mapsto (g, e_H) \\ H \subset G \times H, &\quad h \mapsto (e_G, h) \end{aligned}$$

Da $(g_1, h_1) \cdot (g, e_H) \cdot (g_1, h_1)^{-1} = (g_1, h_1) \cdot (g, e_H) \cdot (g_1^{-1}, h_1^{-1}) = (g_1 \cdot g \cdot g_1^{-1}, h_1 \cdot e_h \cdot h_1^{-1}) = (g_1 \cdot g \cdot g_1^{-1}, e_H) \in G$, ist $G$ tatsächlich Normalteiler. Analog verhält es sich für $H$.
Die beiden Projektionen

$$G \xleftarrow{p_1} G \times H \xrightarrow{p_2} H$$

sind Epimorphismen. Beachte: $\operatorname{Kern} p_1 = H$, $\operatorname{Kern} p_2 = G$ und

$$\overline{p}_2 : (G \times H)/G \cong H, \qquad \overline{p}_1 : (G \times H)/H \cong G$$

Wir wollen nun ein Kriterium dafür angeben, wann eine Gruppe $G$ das Produkt zweier anderer Gruppen ist.

**4.3 Definition:** Eine Gruppe $G$ heißt *inneres Produkt* zweier Untergruppen $U$ und $V$, wenn die Abbildung

$$f : U \times V \to G \quad (u, v) \mapsto u \cdot v$$

ein Isomorphismus ist.

**4.4 Beispiel:** $\mathbb{Z}/6$ ist inneres Produkt von $U = \langle \overline{3} \rangle = \{\overline{0}, \overline{3}\}$ und $V = \langle \overline{2} \rangle = \{\overline{0}, \overline{2}, \overline{4}\}$

$$f : U \times V \to \mathbb{Z}/6, \quad (u, v) \to u + v$$

ist ein Homomorphismus:

$$\begin{array}{rcccl} f((u_1,v_1)+(u_2,v_2)) & = & f(u_1+u_2,v_1+v_2) & = & u_1+u_2+v_1+v_2 \\ & = & u_1+v_1+u_2+v_2 & = & f(u_1,v_1)+f(u_2+v_2) \end{array}$$

$f$ ist surjektiv, denn

$$f(k\cdot\overline{3},k\cdot\overline{4}) = k\cdot\overline{3}+k\cdot\overline{4} = k\cdot\overline{3+4} = k\cdot\overline{1} = \overline{k}$$

Da $|U\times V| = 2\cdot 3 = 6 = |\mathbb{Z}/6|$, ist $f$ bijektiv.
Da $U\cong\mathbb{Z}/2$ und $V\cong\mathbb{Z}/3$, erhalten wir als Folgerung

$$\mathbb{Z}/6\cong\mathbb{Z}/2\times\mathbb{Z}/3.$$

**4.5 Satz:** $U$ und $V$ seien Untergruppen einer Gruppe $G$. Dann sind äquivalent

(1) $G$ ist inneres Produkt von $U$ und $V$

(2) $U\lhd G,\quad V\lhd G,\quad G = U\cdot V,\quad U\cap V = \{e\}$

(3) (a) $\forall x\in G\ \exists|u\in U$ und $\exists|v\in V$ mit $x = u\cdot v$
(b) $u\cdot v = v\cdot u\ \forall u\in U,\ \forall v\in V$

Wir zeigen zunächst

**4.6 Lemma:** Mit den Bezeichnungen aus 4.3 und 4.5 gilt

(1) $u\cdot v = v\cdot u\ \forall u\in U,\ \forall v\in V \iff f: U\times V\to G$ ist Homomorphismus

(2) $U\lhd G$, $V\lhd G$, $U\cap V = \{e\}\Rightarrow f: U\times V\to G$ ist Monomorphismus

**Beweis:**:

(1) Da

$$f((u_1,v_1)\cdot(u_2,v_2)) = f(u_1\cdot u_2, v_1\cdot v_2) = u_1\cdot u_2\cdot v_1\cdot v_2$$

und

$$f(u_1,v_1)\cdot f(u_2,v_2) = u_1\cdot v_1\cdot u_2\cdot v_2,$$

ist $f$ genau dann ein Homomorphismus, wenn

$$u_1\cdot u_2\cdot v_1\cdot v_2 = u_1\cdot v_1\cdot u_2\cdot v_2\quad\forall u_1,u_2\in U,\quad\forall v_1,v_2\in V$$

Gleichheit gilt sicherlich, wenn $u_2\cdot v_1 = v_1\cdot u_2$. Ist umgekehrt $f$ ein Homomorphismus, erhalten wir $u_2\cdot v_1 = v_1\cdot u_2$, indem wir $u_1 = v_2 = e$ setzen.

(2) Sei $u \in U$ und $v \in V$. Da $U$ und $V$ Normalteiler sind, folgt $v^{-1} \cdot u \cdot v \in U$ und $u^{-1} \cdot v^{-1} \cdot u \in V$, da $v^{-1} \in V$ ist. Es folgt

$$u^{-1} \cdot v^{-1} \cdot u \cdot v \in u^{-1} \cdot U = U \text{ und } u^{-1} \cdot v^{-1} \cdot u \cdot v \in V \cdot v = V$$

Also ist $u^{-1} \cdot v^{-1} \cdot u \cdot v \in U \cap V = \{e\}$. Es folgt $u \cdot v = v \cdot u$. Nach (1) ist somit $f$ ein Homomorphismus.

Ist nun $f(u,v) = u \cdot v = e$, so folgt $u = v^{-1} \in U \cap V = \{e\}$, also $u = e$ und $v = e$. Es folgt Kern $f = \{(e,e)\}$, also ist $f$ injektiv.

□

**Beweis 4.5:** (1) ⇒ (2) Wir erinnern daran, dass wir $U$ als Untergruppe von $U \times V$ auffassen können: $U = \{(u,e); u \in U\}$. Dasselbe gilt für $V$. Dann gilt

$$f(U) = U, \text{ weil } f(u,e) = u, \text{ und } f(V) = V.$$

Da $f$ ein Isomorphismus ist und $U$ und $V$ Normalteiler von $U \times V$ sind, sind $U = f(U)$ und $V = f(V)$ Normalteiler in $G$. Weiter gilt in $U \times V$

$$U \cdot V = \{(u,e) \cdot (e,v) = (u,v);\ u \in U,\ v \in V\} = U \times V$$
$$U \cap V = \{(e,e)\}$$

Also folgt $U \cdot V = f(U) \cdot f(V) = f(U \cdot V) = f(U \times V) = G$ und $U \cap V = f(U) \cap f(V) = f(U \cap V) = f(e,e) = e$.

(2) ⇒ (1) Nach 4.6.2 ist $f : U \times V \to G$ aus 4.3 ein Monomorphismus. Da außerdem $G = U \cdot V$, ist jedes $x \in G$ von der Form

$$x = u \cdot v = f(u,v)$$

für ein $u \in U$ und ein $v \in V$. Also ist $f$ surjektiv.

(1) ⟺ (3) Ein Teil der Äquivalenz ist in 4.6.1 bewiesen. Nun ist $f$ aber genau dann bijektiv, wenn es zu jedem $x \in G$ genau ein $u \in U$ und genau ein $v \in V$ gibt, so dass $x = u \cdot v$. □

Als Anwendung zeigen wir

**4.7 Satz:** Sind $k$ und $l$ teilerfremd, so gilt $\mathbb{Z}/(k \cdot l) \cong \langle \overline{k} \rangle \times \langle \overline{l} \rangle \cong \mathbb{Z}/l \times \mathbb{Z}/k$

**Beweis:** Da $\mathbb{Z}/(k \cdot l)$ abelsch ist, sind $\langle \overline{k} \rangle$ und $\langle \overline{l} \rangle$ Normalteiler. Da $\langle \overline{k} \rangle$ aus den Restklassen der Vielfachen von $k$ und $\langle \overline{l} \rangle$ aus der Restklassen der Vielfachen von $l$ besteht, besteht $\langle \overline{k} \rangle \cap \langle \overline{l} \rangle$ aus den Restklassen der gemeinsamen Vielfachen von $k$ und $l$. Da $k$ und $l$ teilerfremd ist, ist $k \cdot l$ das kleinste gemeinsame Vielfache, aber $\overline{k \cdot l} = \overline{0}$. Es folgt $\langle \overline{k} \rangle \cap \langle \overline{l} \rangle = \{\overline{0}\}$. Nach 4.6 ist

$$f : \langle \overline{k} \rangle \times \langle \overline{l} \rangle \to \mathbb{Z}/kl, \quad (x,y) \mapsto x + y$$

ein Monomorphismus. Da $\text{ord}(\overline{k}) = l$ und $\text{ord}(\overline{l}) = k$ ist $|\langle\overline{k}\rangle \times \langle\overline{l}\rangle| = k \cdot l = |\mathbb{Z}/(kl)|$. Also ist $f$ auch surjektiv, und $\langle\overline{k}\rangle \cong \mathbb{Z}/(l)$ und $\langle\overline{l}\rangle \cong \mathbb{Z}/(k)$. □

Durch Induktion erhalten wir

**4.8 Folgerung:** Ist $n = p_1^{r_1} \cdot \ldots \cdot p_k^{r_k}$ mit paarweise verschiedenen Primzahlen $p_i$, so gilt

$$\mathbb{Z}/n \cong \mathbb{Z}/p_1^{r_1} \times \ldots \times \mathbb{Z}/p_k^{r_k}.$$

# 5 G-Mengen

**5.1 Definition:** Sei $(G, \cdot)$ eine Gruppe und $M$ eine Menge. Eine *Operation* von $G$ auf $M$ *von links* ist eine Abbildung

$$G \times M \to M, \quad (g, x) \mapsto g * x,$$

so dass

(1) $(g_1 \cdot g_2) * x = g_1 * (g_2 * x) \quad \forall g_1, g_2 \in G, \ \forall x \in M$

(2) $e * x = x \quad \forall x \in X$

Eine Operation von *rechts* ist eine Abbildung

$$M \times G \to M, \quad (x, g) \mapsto x * g,$$

so dass

(1) $x * (g_1 \cdot g_2) = (x * g_1) * g_2 \quad \forall g_1, g_2 \in G, \ \forall x \in M$

(2) $x * e = x \quad \forall x \in X$

Eine $G$-Menge ist eine Menge $M$ mit einer $G$-Operation.

**5.2 Beispiele:**

(1) Ist $U$ Untergruppe von $G$, dann operiert $U$ von links und rechts auf $G$.

$$\begin{array}{l} U \times G \to G, \quad (u, g) \mapsto u \cdot g \\ G \times U \to G, \quad (g, u) \mapsto g \cdot u \end{array} \quad \textit{Translationsoperationen}$$

(2) Die *Konjugationsoperation* einer Untergruppe $U$ auf der Gruppe $G$ ist definiert durch

$$U \times G \to G, \quad (u, g) \mapsto u \cdot g \cdot u^{-1}.$$

(3) Die Gruppe $\{\pm 1, \cdot\}$ operiert auf $\mathbb{R}^2$ durch

$$\{\pm 1, \cdot\} \times \mathbb{R}^2 \to \mathbb{R}^2, \quad (\pm 1, (x_1, x_2)) \mapsto (\pm x_1, \pm x_2).$$

(4) Die Permutationsgruppe $\Sigma_M$ operiert auf der Menge $M$

$$\Sigma_M \times M \to M, \quad (f, x) \mapsto f(x).$$

Das letzte Beispiel ist typisch. Operiert eine Gruppe $G$ auf einer Menge $M$, kann man jedes Element $g \in G$ als Permutation $\pi_g$ von $M$ auffassen: wir definieren

$$\pi_g : M \to M, \quad x \mapsto g * x.$$

Dann gilt

$$\pi_{g_1 \cdot g_2} = \pi_{g_1} \circ \pi_{g_2} \text{ und } \pi_e = \mathrm{id}$$

denn $\pi_e(x) = e * x = x = \mathrm{id}(x)$ und

$$\pi_{g_1 \cdot g_2}(x) = (g_1 \cdot g_2) * x = g_1 * (g_2 * x) = \pi_{g_1}(\pi_{g_2}(x)) = (\pi_{g_1} \circ \pi_{g_2})(x).$$

Insbesondere ist $\pi_g$ bijektiv, denn $\pi_{g^{-1}}$ ist die Umkehrabbildung. Wir erhalten also eine Abbildung

$$\alpha : G \to \Sigma_M, \quad g \mapsto \pi_g.$$

**5.3 Satz:** Die Abbildung $\alpha$ ist ein Homomorphismus.

**Beweis:** $\alpha(g_1 \cdot g_2) = \pi_{g_1 \cdot g_2} = \pi_{g_1} \circ \pi_{g_2} = \alpha(g_1) \circ \alpha(g_2)$. □

**5.4 Definition:** Ist $\alpha$ injektiv, spricht man von einer *effektiven* Operation von $G$ auf $M$.

Die Linkstranslation von $G$ auf sich selbst

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

ist effektiv. In diesem Fall nennt man $\pi_g$ die Linkstranslation $l_g : G \to G$ mit $g \in G$. Gilt $\alpha(g) = l_g = \mathrm{id}$, dann folgt $e = \mathrm{id}(e) = l_g(e) = g \cdot e = g$. Also ist Kern $\alpha = \{e\}$ und $\alpha$ ist injektiv. Wir erhalten den

**5.5 Satz von Caley** (1821-1895): Jede Gruppe $G$ ist isomorph zu einer Untergruppe der Permutationsgruppe $\Sigma_G$.

**5.6 Definition:** Sei $M$ eine Menge mit Linksoperatoren von $G$.

(1) $M^G := \{x \in M; g * x = x \quad \forall g \in G\}$ heißt *Fixpunktmenge* der Operation.

(2) Für $x \in M$ heißt

$$G * x := \{g * x; g \in G\} \subset M$$

die *Bahn* oder der *Orbit* von $x$ unter der Operation.

(3) Für $x \in M$ heißt die Menge

$$G_x := \{g \in G;\ g * x = x\} \subset G$$

die *Standuntergruppe* von $x$.

Wie die Definition schon sagt, ist $G_x$ eine Untergruppe von $G$. Da $e * x = x$, ist $e \in G_x$. Ist $g \in G_x$, also $g * x = x$, dann folgt

$$g^{-1} * x = g^{-1} * (g * x) = (g^{-1} \cdot g) * x = e * x = x$$

Also ist $g^{-1} \in G_x$. Sind $g_1, g_2 \in G_x$, so gilt

$$(g_1 \cdot g_2) * x = g_1 * (g_2 * x) = g_1 * x = x$$

Also ist $g_1 \cdot g_2 \in G_x$. Somit ist $G_x$ Untergruppe von $G$.

**5.7 Beispiel:** Wir betrachten die Konjugationsoperation von $G$ auf sich (Beispiel 5.2.3). Die Fixpunktgruppe ist das *Zentrum* $Z(G)$ von $G$.

$$\begin{aligned} Z(G) &= \{x \in G;\ g \cdot x = x \cdot g\} \\ &= \{x \in G;\ g \cdot x \cdot g^{-1} = x\ \forall g \in G\} \end{aligned}$$

Die Bahn von $x \in G$ wird oft mit $x^G$ bezeichnet und heißt *Konjugationsklasse* von $x$.

$$x^G = \{g \cdot x \cdot g^{-1};\ g \in G\}$$

Die Standuntergruppe von $x$ wird oft mit $Z(x)$ bezeichnet und heißt *Zentralisator* von $x$

$$Z(x) = \{g \in G;\ g \cdot x \cdot g^{-1} = x\} = \{g \in G; g \cdot x = x \cdot g\}$$

und besteht aus allen Elementen von $G$, die mit $x$ kommutieren.

Operiert $G$ auf $M$, können wir eine Relation auf $M$ definieren durch

$$x \sim y \iff \exists\ g \in G \text{ mit } y = g * x$$

$x \sim x$, denn $x = e * x$

$x \sim y \Rightarrow y \sim x$, denn aus $y = g * x$ folgt $g^{-1} * y = x$

$x \sim y\ \wedge\ y \sim z \Rightarrow x \sim z$, denn aus $y = g_1 * x$ und $z = g_2 * y$ folgt

$z = g_2 * (g_1 * x) = (g_1 \cdot g_2) * x$

Also ist $\sim$ eine Äquivalenzrelation. Die Äquivalenzklasse von $x$ ist die Bahn von $x$, und wir erhalten.

**5.8** Zwei Bahnen $G*x$ und $G*y$ sind entweder gleich oder disjunkt. Damit zerfällt $M$ in disjunkte Bahnen.

**5.9 Lemma:** Sei $\mu : G\times M \to M$ eine Operation von $G$ auf $M$. Sei $\mathcal{P}(M)$ die Potenzmenge von $M$ und $\mathcal{P}_k(M)$ die Menge aller $k$-elementigen Teilmengen von $M$. Dann definiert $\mu$ Operationen

$$\begin{matrix} G\times\mathcal{P}(M)\to\mathcal{P}(M) \\ G\times\mathcal{P}_k(M)\to\mathcal{P}_k(M) \end{matrix} \qquad (g,X)\mapsto g\cdot X = l_g(X)$$

**Beweis:** Ist $X \in \mathcal{P}_k(X)$, dann ist $g\cdot X = \{g\cdot x;\, x\in X\} \in \mathcal{P}_k(X)$, weil $li_g$ bijektiv ist. □

**5.10 Beispiel:** Wir wenden (5.9) auf $G$ mit der Konjugationsoperation an. Ist $U$ eine Untergruppe, dann wird die Standuntergruppe von $U$ mit

$$N_G(U) = \{g\in G;\, gU^{-1}g = U\}$$

bezeichnet und *Normalteiler* von $U$ genannt. $N_G(U)$ ist die größte Untergruppe von $G$, die $U$ als Normalteiler enthält. D.h. ist $V$ Untergruppe von $G$ und $U \lhd V$, dann folgt $V \subset N_G(U)$.

**5.11 Satz:** Sei $M$ eine $G$-Menge und $x\in M$. Dann ist die Abbildung

$$f : G/G_x \to G\cdot x, \quad g\cdot G_x \mapsto g\cdot x$$

bijektiv.

**Beweis:** $f$ ist wohldefiniert und injektiv: $g\cdot G_x = h\cdot G_x \iff g^{-1}\cdot h \in G_x \iff (g^{-1}\cdot h)x = x \iff h\cdot x = g\cdot x$. Offensichtlich ist $f$ surjektiv. □

**5.12 Folgerung:** Sei $M$ eine $G$-Menge.

(1) Ist $G$ endlich und $x\in M$, dann gilt $|G| = |G_x|\cdot|G\cdot x|$.

(2) Ist $M$ endlich, dann gilt

$$|M| = |M^G| + \sum_{i=1}^{n}\big[G : G_{x_i}\big]$$

wobei $\{x_1,\ldots,x_n\}$ ein vollständiges Repräsentantensystem für die verschiedenen Orbits $G\cdot x_i$ mit mehr als einem Element ist, so dass $[G : G_{x_i}] = |G\cdot x_i| > 1$. □

# 6 p-Gruppen und die Sylowsätze

**6.1 Definition:** Sei $p$ prim. Eine endliche Gruppe $G$ heißt *$p$-Gruppe*, falls $|G| = p^k$. Ist $|G| = m \cdot p^k$ mit $p \nmid m$, so heißt eine Untergruppe $S < G$ *$p$-Sylowuntergruppe*, falls $|S| = p^k$.

**6.2 Lemma:** Operiert eine $p$-Gruppe $G$ auf einer endlichen Menge $M$, so gilt

$$|M| \equiv |M^G| \qquad \mod p$$

**Beweis:**: Nach (5.12.2) gilt

$$|M| = |M^G| + \sum_{i=1}^{n} [G : G_{x_i}]$$

wobei $G_{x_i}$ echte Untergruppe von $G$ ist. Es folgt $[G : G_{x_i}] \equiv 0 \mod p$. □

**6.3 Satz:** Sei $G$ eine $p$-Gruppe, $|G| = p^k$, $k > 0$. Dann ist das Zentrum $Z(G) \neq \{e\}$.

**Beweis:**: Betrachte die Konjugationsoperation von $G$ auf sich. Dann ist $Z(G)$ die Fixpunktmenge. Also nach 6.2

$$|Z(G)| \equiv |G| = p^k \equiv 0 \qquad \mod p$$

Damit hat $Z(G)$ mindestens $p$ Elemente. □

**6.4 Aufgabe:** Zeigen Sie: (1) $G/Z(G)$ zyklisch $\Rightarrow G$ abelsch.
(2) $|G| = p^2$, $p$ prim $\Rightarrow G$ abelsch (benutzen Sie 6.3).

**6.5** Für jedes fest gewählt $g \in G$ ist

$$\varphi : G \to G, \quad x \mapsto g \cdot x \cdot g^{-1}$$

ein Automorphismus. Also ist mit $U$ auch $\varphi(U) = g \cdot U \cdot g^{-1}$ eine Untergruppe von $G$, und ist $U$ Sylowuntergruppe, dann auch $g \cdot U \cdot g^{-1}$.

**6.6 Die Sylowsätze:** (Ludwig Sylow, 1832-1918, norwegischer Gymnasiallehrer) Sei $G$ eine endliche Gruppe der Ordnung $|G| = p^k \cdot m$ mit $p \nmid m$. Dann gilt:

(1) $G$ besitzt Untergruppen $U_1 < U_2 < \ldots < U_k$ mit $|U_i| = p^i$, insbesondere ist $U_k$ eine $p$-Sylowuntergruppe $S$.

(2) Die Anzahl $n_p$ der verschiedenen $p$-Sylowuntergruppen von $G$ erfüllt

$$n_p \equiv 1 \mod p, \quad \text{und} \quad n_p \text{ teilt } m.$$

(3) Jede $p$-Untergruppe $H$ in $G$ ist in einer $p$-Sylowuntergruppe enthalten.

(4) Alle $p$-Sylowuntergruppen von $G$ sind konjugiert.

**6.7 Lemma:** Ist $p \nmid m$, dann gilt für $1 \le s \le k$

$$\binom{mp^k}{p^s} = m \cdot p^{k-s} \cdot \binom{mp^k - 1}{p^s - 1}, \quad \text{und} \quad p \nmid \binom{mp^k - 1}{p^s - 1}$$

**Beweis:**:

$$\begin{aligned}\binom{mp^k}{p^s} &= \frac{m \cdot p^k \cdot (mp^k - 1) \cdot \ldots \cdot (mp^k - p^s + 1)}{p^s \cdot (p^s - 1) \cdot \ldots 1} \\ &= m \cdot p^{k-s} \cdot \binom{mp^k - 1}{p^s - 1} \\ &= m \cdot p^{k-s} \cdot \prod_{i=1}^{p^s-1} \frac{mp^k - i}{i}\end{aligned}$$

Wir betrachten die Faktoren im Zähler des Produktes: Für $1 \le i \le p^s - 1$ gilt

$$mp^k - i = q \cdot p^r \iff i = mp^k - qp^r$$

(wir wählen $r$ maximal, d.h. $p \nmid q$). Angenommen $r \ge k$, dann klammern wir $p^k$ aus und erhalten $i = p^k(m - qp^{r-k}) \ge p^k$, was wegen $i \le p^s - 1 < p^k$ unmöglich ist. Also ist $r < k$ und $i = p^r(mp^{k-r} - q)$. Damit läßt sich $p^r$ im Faktor $mp^k - i$ des Zählers gegen $p^r$ im Faktor $i$ des Nenners kürzen, d.h. das Produkt hat nach Kürzen keinen Faktor $p$ im Zähler. □

**Beweis von 6.6:** Sei $\mathcal{X} = \mathcal{P}_{p^s}(G)$ $1 \le s \le k$. Bekanntlich gilt $|\mathcal{X}| = \binom{n}{p^s}$. Unter der Linkstranslation mit $g \in G$ zerfällt $\mathcal{X}$ in disjunkte Orbits, und wir erhalten

$$\binom{n}{p^s} = |\mathcal{X}| = |G \cdot X_1| + \ldots + |G \cdot X_r| = \frac{|G|}{|S_1|} + \ldots + \frac{|G|}{|S_r|}$$

wobei $S_i$ die Standuntergruppe der *Menge* $X_i$ ist, d.h. $g \in S_i$ bildet $X_i$ bijektiv nach $X_i$ ab. Da $p^{k-s+1} \nmid \binom{n}{p^s}$ nach 6.7, gibt es mindestens einen Summanden, etwa $\frac{|G|}{|S_1|}$, der nicht durch $p^{k-s+1}$ teilbar ist. Da $p^k \mid |G|$, folgt $p^s \mid |S_1|$. Sei nun $x \in X_1$. Da $S_1$ Standuntergruppe von $X_1$ ist, folgt $S_1 \cdot x \subset X_1$. Aber Rechttranslation mit $x$ ist bijektiv. Es folgt

$$|S_1| = |S_1 \cdot x| \le |X_1| = p^S. \quad \text{Also } |S_1| = p^s.$$

Mit $s = k$ erhalten wir eine Sylowuntergruppe $S_1 = U_k$ von $G$.

Wir wenden unsere Überlegungen nun auf $U_k$ an mit $s = k-1$ und erhalten eine Untergruppe $U_{k-1}$ der Ordnung $p^{k-1}$. Durch Abwärtsinduktion folgt Teil (1) von 6.7.

Sei nun $S$ eine $p$-Sylowuntergruppe. Sei nun $H < G$ eine $p$-Gruppe. Die Zuordnung

$$H \times G/S \to G/S, \quad (h, g \cdot S) \mapsto h \cdot g \cdot S \qquad (*)$$

definiert eine Operation von $H$ auf $G/S$. Nach 6.3 gilt

$$|(G/S)^H| \equiv |G/S| = m \not\equiv 0 \qquad \mod p.$$

Also besitzt diese Operation Fixpunkte, d.h. es gibt eine Nebenklasse $g \cdot S$ mit $h \cdot g \cdot S = g \cdot S$ für alle $h \in H$. Es folgt

$$\begin{array}{rl} H \cdot g & \subset H \cdot g \cdot S = g \cdot S \\ H & < g \cdot S \cdot g^{-1} \end{array} \qquad (A)$$

Ist $H$ selbst Sylowuntergruppe, so folgt wegen $|H| = p^k = |g \cdot S \cdot g^{-1}|$, dass

$$H = g \cdot S \cdot g^{-1}$$

Das beweist (3) und (4).

Für (2) wenden wir diese Überlegungen auf $H = S$ an. Wir erhalten

$$|G/S| \equiv |(G/S)^S| \mod p$$

und $g \cdot S \in (G/S)^S \iff S = g \cdot S \cdot g^{-1}$ nach (A)

Aber $g \cdot S \cdot g^{-1} = S \iff g \in N_G(S)$, so dass

$$|G/S| \equiv |(G/S)^S| = |N_G(S)/S| \not\equiv 0 \mod p \qquad (**)$$

Betrachten wir jetzt die Bahn $\mathcal{E}$ von $S$ unter der Konjugationsoperation, also die Konjugationsklasse von $S$. Dann gilt nach 6.6

$$n_p \overset{def}{=} |\mathcal{E}| = \frac{|G|}{|N_G(S)|} = \frac{|G/S|}{|N_G(S)/S|} \equiv 1 \qquad \mod p$$

wegen $(**)$. Da $m = |G/S| = n_p \cdot |N_G(S)/S|$, folgt $n_p$ teilt $m$.

Beim letzten Schritt argumentieren wir im Restklassenkörper modulo $p$. Die Restklassen von $|G/S|$ und $|N_G(S)/S|$ sind gleich und von 0-Klassen verschieden. Die Division im Restklassenkörper ergibt daher die Restklasse von 1. □

Für Anwendungen vermerken wir als Konsequenz aus 6.5 und 6.6.4.

**6.8** Hat eine endliche Gruppe $G$ genau eine $p$-Sylowuntergruppe $S$, dann ist $S$ Normalleiter.

**6.9 Satz:** Hat $G$ für jeden Primteiler $p$ von $|G|$ genau eine $p$-Sylowuntergruppe, dann ist $G$ inneres Produkt seiner Sylowuntergruppen.

**Beweis:**: Seien $p_1, \ldots, p_k$ die Primteiler von $|G|$ und $S_1, \ldots, S_k$ die zugehörigen Sylowuntergruppen. Durch Induktion nach $l$ zeigen wir, dass

$$f : S_1 \times \ldots \times S_l \to G, \quad (x_1, \ldots, x_l) \mapsto x_1 \cdot \ldots \cdot x_l$$

ein Monomorphismus ist. Da $|S_1 \times \ldots \times S_k| = |G|$, folgt die Behauptung.

Für $l = 1$ ist nichts zu zeigen.

Induktionsschritt von $l-1$ nach $l$: Nach Induktionsannahme ist

$$U = f(S_1 \times \ldots \times S_{l-1}) = S_1 \cdot \ldots \cdot S_{l-1}$$

eine Untergruppe von $G$ isomorph zu $S_1 \times \ldots \times S_{l-1}$. Da

$$\begin{aligned} g \cdot S_1 \cdot \ldots \cdot S_{l-1} \cdot g^{-1} &= g \cdot S_1 \cdot g^{-1} \cdot g \cdot S_2 \cdot g^{-1} \ldots g \cdot S_{l-1} \cdot g^{-1} \\ &= S_1 \cdot S_2 \cdot \ldots \cdot S_{l-1}, \end{aligned}$$

ist $U \triangleleft G$. Nach 6.8 ist $S_l \triangleleft G$. Weiter ist $U \cap S_l$ Untergruppe von $U$ und von $S_l$. Da $|U|$ und $|S_l|$ teilerfremd sind, folgt $U \cap S_l = \{e\}$. Nach 5.6 ist

$$f : U \times S_l \to G \quad , (u, x) \mapsto u \cdot x$$

injektiv. □

**6.10 Satz:** Seien $p < q$ Primzahlen und $q \not\equiv 1 \mod p$, dann ist jede Gruppe der Ordnung $pq$ isomorph zu $\mathbb{Z}/pq$.

**Beweis:**: $n_p = 1 \mod p$ und $n_p \mid q$. Da $q$ prim ist, folgt $n_p = 1$ oder $n_p = q$. Da aber $q \not\equiv 1 \mod p$, erhalten wir $n_p = 1$, $n_q \equiv 1 \mod q$ und $n_q | p$. Da $p < q$, folgt $n_q = 1$.

Nach 6.9 ist $G \cong S_p \times S_q$. Weiter gilt $S_p \times S_q \cong \mathbb{Z}/p \times \mathbb{Z}/q \cong \mathbb{Z}/p \cdot q$ nach 3.15 und 4.7. □

**6.11 Beispiel:** Ist $G$ eine Gruppe der Ordnung 45, dann ist $G$ abelsch.

**Beweis:**: $45 = 3^2 \cdot 5$
$n_3 \equiv 1 \mod 3$ und $n_3 \mid 5$. Es folgt $n_3 = 1$.
$n_5 \equiv 1 \mod 5$ und $n_5 \mid 9$. Es folgt $n_5 = 1$.
Also $G \cong S_3 \times S_5$. Da $|S_5| = 5$ ist $S_5 \cong \mathbb{Z}/5$. Da $|S_3| = 9$, ist $S_3$ nach 6.5 abelsch.
Also ist $G$ abelsch. □

Der Beweis von 6.11 lässt sich verallgemeinern:

**6.12 Aufgabe:** Es seien $p < q$ Primzahlen und $G$ eine Gruppe. Zeigen Sie: $G$ ist abelsch, wenn eine der folgenden Bedingungen erfüllt ist:

(1) $|G| = p^2 \cdot q$ und $q \not\equiv 1 \mod p$ und $p^2 \not\equiv 1 \mod q$

(2) $|G| = p \cdot q^2$ und $q^2 \not\equiv 1 \mod p$

(3) $|G| = p^2 \cdot q^2$ und $p^2 \not\equiv 1 \mod q$ und $q^2 \not\equiv 1 \mod p$

Die Bedeutung dieses Resultats liegt im Struktursatz für endlich erzeugte abelsche Gruppen.

**6.13 Struktursatz:** Sei $G$ eine endlich erzeugte abelsche Gruppe. Dann gilt:

(1) $G \cong \mathbb{Z}^r \times T$, $r \geq 0$ und $T$ endlich.

(2) Ist $p_1^{k_1} \cdot \ldots \cdot p_s^{k_s}$ mit $p_1 < p_2 < \ldots p_s$ die Primfaktorzerlegung von $|T|$, dann gilt
$$T \cong S_{p_1} \times \ldots \times S_{p_s}$$
wobei $S_{p_i}$ die $p_i$-Sylowuntergruppe von $T$ ist.

(3) Ist $S$ eine abelsche $p$-Gruppe, $|S| = p^k$, dann ist $S$ von der Form
$$S \cong \mathbb{Z}/p^{r_1} \times \ldots \times \mathbb{Z}/p^{r_t}$$
$r_1 \leq r_2 \leq \ldots \leq r_t$ und $r_1 + r_2 + \ldots + r_k = k$.

Teil (2) ist ein Spezialfall von 6.10. Die Beweise der Teile (1) und (3) müssen wir aus Zeitgründen schuldig bleiben

# 7 Permutationsgruppen

Wir verwenden die Zykelschreibweise für Permutationen: Sei $[n] : \{1, 2, \ldots, n\}$ und $\sigma \in \Sigma_n$. Ist $\langle\sigma\rangle$ die von $\sigma$ erzeugte Untergruppe von $\Sigma_n$, dann ist
$$\langle\sigma\rangle \times [n] \to [n], \quad (\sigma^k, s) \mapsto \sigma^k(s)$$
eine Operation von $\langle\sigma\rangle$ auf $[n]$ und
$$B(s, \sigma) := \{\sigma^k(s); k \in \mathbb{Z}\}$$

ist die Bahn von $s$ unter dieser Operation. Nach (5.8) zerfällt $[n]$ in disjunkte Bahnen

$$[n] = B(s_1, \sigma) \sqcup \ldots \sqcup B(s_r, \sigma).$$

Wir definieren neue Permutationen $\sigma_1, \ldots, \sigma_r$ aus $\Sigma_n$ durch

$$\sigma_i(t) = \begin{cases} \sigma(t), & \text{falls } t \in B(s_i, \sigma) \\ t & \text{sonst} \end{cases}$$

d.h. $\sigma_i$ permutiert die Element aus $B(s_i, \sigma)$ wie $\sigma$ und lässt die übrigen fest. Es folgt

$$\sigma = \sigma_1 \circ \sigma_2 \circ \ldots \circ \sigma_r.$$

**7.1 Definition:** Eine Permutation $\varphi \in \Sigma_n$ heißt *r-Zykel*, wenn es eine $r$-elementige Teilmenge $T = \{t_1, \ldots, t_r\}$ von $[n]$ gibt, so dass

$$\varphi(t_i) = \begin{cases} t_{i+1} & 1 \le i \le r-1 \\ t_1 & i = r \end{cases}$$

und $\varphi(s) = s \; \forall s \notin T$. Wir nennen $T$ den *Träger* von $\varphi$. Es gilt

$$T = \{t_1, \varphi(t_1), \varphi^2(t_1), \ldots, \varphi^{r-1}(t_1)\}.$$

Zwei Zykel heißen *disjunkt*, falls ihre Träger disjunkt sind.

Wir haben gezeigt

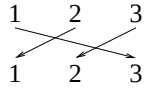
**7.2 Satz:** Jede Permutation $\sigma \in \Sigma_n$ ist eine Komposition disjunkter Zykel. Die Zerlegung ist bis auf Reihenfolge

Aus 7.1 folgt sofort

**7.3** Für disjunkte Zykel $\varphi, \psi \in \Sigma_n$ gilt $\varphi \circ \psi = \psi \circ \varphi$.

**7.4 Bezeichnung:** Ein Zykel ist eindeutig durch seinen **zyklisch geordneten** Träger definiert, wobei die Ordnung durch die Abbildungsvorschrift (7.1) gegeben ist. Daher benutzen wir oft den Träger als Bezeichnung für einen Zykel.

**7.5 Beispiele:**

(1) $\sigma$ : 

ist ein Zykel: $\sigma = (1,3,2) = (3,2,1) = (2,1,3)$

(2) Die Permutation $\varphi: \begin{array}{ccccccccc} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ \downarrow & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow \\ 2 & 5 & 7 & 4 & 8 & 3 & 6 & 1 & 9 \end{array}$

besitzt die Zykelzerlegung $\varphi = (1,2,5,8) \circ (3,7,6) \circ (4) \circ (9)$. Beachte, dass die Permutation (4) und (9) Identitäten sind. Deshalb ist auch die Beziehungsweise

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

üblich, d.h. 1-Zykel werden in der Zykelzerlegung oft ignoriert.

**7.6 Bezeichnung:** Ein 2-Zykel heißt *Transposition*.

**7.7 Satz:** $\Sigma_n$ wird von der Menge $A = \{(i, i+1); i = 1 \ldots, n-1\}$ von Transposition erzeugt, d.h. jede Permutation ist Komposition von Transpositionen aus $A$.

**Beweis:**

(i) Jede Permutation ist nach (7.2) Komposition von Zykeln; also genügt es, den Satz für Zykel $(i_1, \ldots, i_k)$ zu zeigen.

(ii) $(i_1, \ldots, i_k) = (i_1, i_k) \circ (i_1, i_{k-1}) \circ \ldots \circ (i_1, i_3) \circ (i_1, i_2)$

Also genügt es, den Satz für beliebige Transpositionen $(i, j)$ und $i < j$ zu zeigen.

(iii) Sei $(i, j)$ Transposition mit $i < j$. Wir beweisen durch Induktion nach $j - i$, daß $(i, j)$ Komposition von Permutation aus $A$ ist. Für $j - i = 1$ ist $(i, j)$ aus $A$.

Induktionsschritt: $(i, j) = (i, j-1) \circ (j-1, j) \circ (i, j-1)$

$(j-1, j) \in A$, und nach Induktion ist $(i, j-1)$ Komposition von Transpositionen aus $A$.

□

Wir definieren einen Homomorphismus

$$f : \Sigma_n \to \{\pm 1, \cdot\} \cong \mathbb{Z}/2$$

durch

$$f(\sigma) := \det(e_{\sigma(1)}, \ldots, e_{\sigma(n)}),$$

wobei $e_i \in \mathbb{R}^n$ der $i$-te Einheitsvektor ist. Fassen wir $(z_1, \ldots, z_n)$ mit $z_i \in \mathbb{R}^n$ als Matrix mit den Spaltenvektoren $z_1, \ldots, z_n$ auf, so gilt

$$(z_1, \ldots, z_n) \cdot (e_{\sigma(1)}, \ldots, e_{\sigma(n)}) = z_{\sigma(1)}, \ldots, z_{\sigma(n)}).$$

Es folgt

$$\begin{aligned} f(\sigma)\cdot f(\tau) &= \det(e_{\sigma(1)},\ldots,e_{\sigma(n)})\cdot\det(e_{\tau(1)},\ldots,e_{\tau(n)}) \\ &= \det((e_{\sigma(1)},\ldots,e_{\sigma(n)})\cdot(e_{\tau(1)},\ldots,e_{\tau(n)})) \\ &= \det(e_{\sigma\tau(1)},\ldots,e_{\sigma\tau(n)}) = f(\sigma\circ\tau) \end{aligned}$$

**7.8 Bezeichnung:** $f(\sigma)$ heißt *Vorzeichen* von $\sigma$ und wir schreiben sign für $f$. Eine Permutation $\sigma$ heißt *gerade*, falls $\operatorname{sign}\sigma = 1$ und sonst *ungerade*.

**7.9 Folgerung:** Eine Permutation ist genau dann gerade, wenn sie sich als Komposition einer geraden Anzahl von Transpositionen darstellen läßt.

**7.10 Definition:** $A_n := Kern(\operatorname{sign}:\Sigma_n\to\{\pm1,\cdot\})$ heißt *alternierende Gruppe* von $[n]$.

**7.11** $[\Sigma_n : A_n] = 2$. Also $A_n \lhd \Sigma_n$.

Wir wollen $A_n$ näher untersuchen.

**7.12 Satz:** Für $n \geq 3$ wird $A_n$ von 3-Zykeln erzeugt. (3-Zykeln sind gerade!)

**Beweis:**: $x \in A_n$ ist Produkt einer geraden Anzahl $x = \tau_1\circ\sigma_1\circ\ldots\circ\tau_k\circ\sigma_k$ von Transposition. Wir untersuchen 3 Fälle:

$$\begin{array}{lcll} \tau_r = \sigma_r & \Longleftrightarrow & \tau_r\circ\sigma_r = Id & |T_{\sigma_r}\cap T_{\tau_r}| = 2 \\ \tau_r\circ\sigma_r & = & (i,j)\circ(i,k) = (i,k,j) & |T_{\sigma_r}\cap T_{\tau_r}| = 1 \\ \tau_r\circ\sigma_r & = & (i,j)\circ(k,l) = (j,l,k)\circ(i,k,j) & T_{\sigma_r}\cap T_{\tau_r} = \varnothing \end{array}$$

□

Wie kommen nun zur zentralen Aussage über $A_n$.

**7.13 Definition:** Eine Gruppe $G$ heißt *einfach*, wenn sie nur die trivialen Normalteiler $\{e\}$ und $G$ besitzt.

**7.14 Satz:** Für $n \neq 4$ ist $A_n$ einfach.

Da $|A_1| = |A_2| = 1$ und $|A_3| = 3$, sind $A_1, A_2, A_3$ einfach. Für $n > 4$ benötigen wir einen Hilfssatz.

**7.15 Lemma:** Für $n \geq 5$ sind je zwei 3-Zykel $(a,b,c)$ und $(i,j,k)$ in $A_n$ *konjugiert*, d.h. es gibt ein $\sigma \in A_n$, so dass $\sigma\circ(a,b,c)\circ\sigma^{-1} = (i,j,k)$.

**Beweis:**: Wähle eine beliebige Permutation $\pi \in \Sigma_n$, so dass $\pi(a) = i$, $\pi(b) = k$.

Dann gilt $\pi \circ (a,b,c) \circ \pi^{-1} : \begin{array}{l} i \mapsto j \\ j \mapsto k \\ k \mapsto i \end{array}$ und $t \mapsto f$ für $t \notin \{i,j,k\}$.

Also $\pi \circ (a,b,c) \circ \pi^{-1} = (i,j,k)$. Ist $\pi \in A_n$, sind wir fertig. Falls das nicht der Fall ist, nehmen wir zwei Elemente $s * t \in [n]$ mit $s,t \notin \{a,b,c\}$. Da $n \geq 5$, ist das möglich. Dann ist $\pi \circ (s,t) \in A_n$, und es gilt

$$(\pi \circ (s,t)) \circ (a,b,c) \circ (s,t) \circ \pi^{-1} = \pi \circ (a,b,c) \circ \pi^{-1} = (i,j,k).$$

Also ist $\sigma = \pi \circ (s,t)$ das gesuchte Element. □

**Beweis 7.14:** Sei $n \geq 5$, $H \lhd A_n$ und $H \neq \{e\}$. Wir müssen zeigen, dass $H = A_n$. Dafür genügt es zu zeigen, daß $H$ einen 3-Zykel enthält: Denn da $H$ Normalteiler ist, liegen nach (7.15) alle 3-Zykel in $H$. Aus (7.12) folgt dann $H = A_n$.

Sei $\sigma \neq id$ aus $H$. Dann muß $\sigma$ mindestens 3 Elemente permutieren, sonst wäre es einer Transposition (die nicht in $A_n$ liegt). Betrachte die Zykelzerlegung von $\sigma$.

**1. Fall:** $\sigma = (a_1, \ldots, a_k) \circ \overline{\sigma}$ mit $k > 3$, d.h. $\sigma$ enthält einen $k$-Zykel mit $k > 3$. Dann ist (da $Tr_{\overline{\sigma}} \cap \{a_1, \ldots, a_k\} = \varnothing$).

$$\begin{aligned} H \ni \sigma \quad &\circ \quad \underbrace{(a_1,a_2,a_3) \circ \sigma^{-1} \circ (a_1,a_2,a_3)^{-1}}_{\in H, \text{ da } h \lhd A_n \text{ und } (a_1,a_2,a_3) \in A_k} \\ &= (a_1, \ldots, a_k) \circ (a_1,a_2,a_3) \circ (a_k, \ldots, a_1) \circ (a_3,a_2,a_1) \\ &= (a_1 a_4 a_2) \end{aligned}$$

**2. Fall:** $\sigma$ enthält nur Tranpositionen und 3-Zykel. Da 3-Zykel gerade sind, muß $\sigma$ eine gerade Zahl von Transpositionen enthalten.

(a) $\sigma$ enthält keine Transposition, ist aber nicht selbst 3-Zykel, d.h.

$$\sigma = (a_1 a_2 a_3) \circ (a_4 a_5 a_6) \circ \overline{\sigma}.$$

$$\begin{aligned} H \ni \sigma \circ (a_1 a_2 a_4) \circ \sigma^{-1} \circ (a_1 a_2 a_4)^{-1} &= \\ = (a_1 a_2 a_3) \circ (a_4 a_5 a_6) \circ (a_1 a_2 a_4) \circ (a_6 a_5 a_4) \circ (a_3 a_2 a_1) \circ (a_4 a_2 a_1) &\\ = (a_1 a_4 a_3 a_5 a_2) & \end{aligned}$$

und wir sind im Fall 1.

(b) $\sigma$ enthält mindestens zwei Transpositionen und läßt keine Elemente $a_5$ fest:

$$\sigma = (a_1 a_2) \circ (a_3 a_4) \circ (a_5) \circ \overline{\sigma}$$

Dann gilt

$$\begin{aligned} H \ni \sigma &\circ (a_1a_2a_5) \circ \sigma^{-1} \circ (a_1a_2a_5)^{-1} \\ &= (a_1a_2) \circ (a_3a_4) \circ (a_1a_2a_5) \circ (a_1a_2) \circ (a_3a_4) \circ (a_5a_2a_1) \\ &= (a_1a_2) \circ (a_1a_2a_5) \circ (a_1a_2) \circ (a_5a_2a_1) = (a_1a_2a_5) \end{aligned}$$

(c) Besteht $\sigma$ nur aus 2 Transpositionen, läßt es ein Element fest, da $n \geq 5$. Also bleibt der Fall, daß $\sigma$ mindestens 4 Transpositionen enthält oder 2 Tranpositionen und mindestens 3-Zykel.

Im zweiten Fall zerlegen wir $\sigma$

$$(a_1a_2) \circ (a_3a_4) \circ (a_5 - a_6a_7) \circ \tau = (a_1a_2) \circ (a_3a_4) \circ (a_5a_6) \circ \overbrace{(a_6a_7) \circ \tau}^{\overline{\sigma}}$$

In beiden Fällen ist $\sigma$ von der Form

$$(a_1a_2) \circ (a_3a_4) \circ (a_5a_6) \circ \overline{\sigma}$$

und $\overline{\sigma}$ enthält nicht $a_1, \ldots, a_5$. Es folgt: $\overline{\sigma}$ vertauscht mit $(a_1a_2a_5)$. Also

$$\begin{aligned} H \ni \sigma &\circ (a_1a_2a_5) \circ \sigma^{-1} \circ (a_1a_2a_5)^{-1} \\ &= (a_1a_2) \circ (a_3a_4) \circ (a_5a_6) \circ (a_1a_2a_5) \circ (a_5a_6) \circ (a_3a_4) \\ &\quad \circ (a_1a_2) \circ (a_5a_2a_1) \\ &= (a_1a_5) \circ (a_2a_6) \circ (a_3) \circ (a_4) \end{aligned}$$

Wir sind also im Fall (b). □

**7.16 Aufgabe:** Zeigen Sie, dass das Zentrum $Z(\Sigma_n)$ von $\Sigma_n$ für $n \geq 3$ nur aus dem neutralen Element besteht.

**7.17 Aufgabe:** Sei

$$\mathcal{V}_4 = \{e, (12) \circ (34), (13) \circ (24), (14) \circ (23)\} \subset \Sigma_4.$$

Zeigen Sie:

(1) $\mathcal{V}_4 \lhd \Sigma_4$

(2) (2) $\Sigma_4/\mathcal{V}_4 \cong \Sigma_3$

(3) (3) $\mathcal{V}_4 \cong \mathbb{Z}/2 \times \mathbb{Z}/2$.

# 8 Auflösbare Gruppen

**8.1 Definition:** Sei $G$ eine Gruppe

(1) Eine *Subnormalreihe* ist eine Sequenz

$$G = G_0 \rhd G_1 \rhd G_2 \rhd \dots$$

Die Faktorgruppen $G_i/G_{i+1}$ heißen *Faktoren* der Reihe. Die Anzahl der **nicht-trivialen** Faktoren heißt *Länge* der Reihe.

(2) Gilt $G_i \lhd G \,\forall\, i$, spricht man von einer *Normalreihe*.

(3) Sind alle Faktoren der Subnormalreihe nicht-trivial und einfach, spricht man von einer *Kompositionsreihe*.

**8.2 Definition:** $G$ heißt *auflösbar*, wenn $G$ eine endliche Subnormalreihe mit abelschen Faktoren besitzt.

**8.3 Beispiel:** (1) $\Sigma_3$ hat die Kompositionsreihe

$$\Sigma_3 \rhd A_3 \rhd \{e\}$$

denn $\Sigma_3/A_3 \cong \mathbb{Z}/2$ und $A_3 \cong \mathbb{Z}/3$. Da die Faktoren abelsch sind, ist $\Sigma_3$ auflösbar.

(2) $\Sigma_4$ hat die Kompositionsreihe

$$\Sigma_4 \rhd A_4 \rhd \mathcal{V}_4 \rhd \langle (13) \circ (24) \rangle \rhd \{e\}$$

mit den Faktoren

$$\Sigma_4/A_4 \cong \mathbb{Z}/2, \quad A_4/_{\mathcal{V}}4 \cong \mathbb{Z}/3, \quad \mathcal{V}_4/\langle\tau\rangle \cong \mathbb{Z}/2, \quad \langle\tau\rangle/\{e\} \cong \mathbb{Z}/2,$$

wobei $\tau = (13) \circ (24)$. Da die Faktoren abelsch sind, ist $\Sigma_4$ auflösbar.

(3) Für $n \geq 5$ hat $\Sigma_n$ die Kompositionsreihe (nach (7.14))

$$\Sigma_n \rhd A_n \rhd \{e\}$$

mit den Faktoren $\Sigma_n/A_n \cong \mathbb{Z}/2$, $A_n/\{e\} \cong A_n$. Da $A_n$ der einzige echte Normalteiler von $\Sigma_n$ ist, ist $\Sigma_n$ **nicht** auflösbar.

(4) $n > 1$ habe die Primfaktorzerlegung $n = p_1 \cdot p_2 \cdot \ldots \cdot p_r$. Dann ist

$$\begin{array}{ccccccc} \mathbb{Z}/n & \rhd & \mathbb{Z}/\dfrac{n}{p_1} & \rhd & \mathbb{Z}/\dfrac{n}{p_1 \cdot p_2} & \rhd & \ldots \\ \| & & \| & & \| & & \\ \langle x \rangle & & \langle x p_1 \rangle & & \langle x p_1 p_2 \rangle & & \end{array}$$

eine Kompositionsreihe der Länge $r$ mit Faktoren isomorph zu $\mathbb{Z}/p_1, \mathbb{Z}/p_2, \ldots$

(5) Jede abelsche Gruppe ist auflösbar.

### 8.4 Konstruktion von Subnormalreihen

Sei $G$ eine Gruppe und $G' = [G, G]$ die Untergruppe, die von allen Elemente der Form

$$[x, y] := xyx^{-1}y^{-1}$$

erzeugt wird. $[x, y]$ heißt *Kommutator* (denn $x \cdot y = y \cdot x \iff [x, y] = 0$), und $[G, G]$ *Kommutatoruntergruppe* von $G$.

**8.5 Aufgabe:** Zeigen Sie:

(1) $[G, G] \lhd G$

(2) $G/[G, G]$ ist abelsch.

(3) Sei $f : G \to H$ ein Homomorphismus und Bild $f$ abelsch. Dann gilt Kern $f \supset [G, G]$.

(4) Ist $f : G \to H$ ein Homomorphismus, $H$ abelsch und $p : G \to G/[G, G]$ die Projektion, dann gibt es genau einen Homomorphismus

$$\overline{f} : G/[G, G] \to H,$$

so dass $\overline{f} \circ p = f$.

**8.6 Definition und Satz:** Wir definieren induktiv: $G^{(0)} = G$, $G^{(i+1)} = [G^{(i)}, G^{(i)}]$. Dann ist $G = G^{(0)} \rhd G^{(1)} \rhd G^{(2)} \rhd \ldots$ eine Normalreihe, genannt *derivierte Reihe* von $G$.

**Beweis:** Wir müssen noch zeigen, dass $G^{(i)} \lhd G$. Das folgt aus

**8.7** $U \lhd G \Rightarrow [U,U] \lhd G$

denn sind $x, y \in U$, also $[x,y] \in [U,U]$, so folgt

$$\begin{aligned} g[x,y] \cdot g^{-1} &= gxyx^{-1}y^{-1}g^{-1} \\ &= gxg^{-1}gyg^{-1}gx^{-1}g^{-1}gy^{-1}g^{-1} \\ &= [gxg^{-1}, gyg^{-1}] \in [U,U]. \end{aligned}$$

Da jedes Element in $[U,U]$ Produkt von Elementen dieser Form ist (beachte, dass $[x,y]^{-1} = [y,x]$), folgt die Behauptung.

□

**8.8 Satz:** $G$ ist genau dann auflösbar, wenn die derivierte Reihe endlich ist, d.h. wenn $G^{(k)} = \{e\}$ für ein $k$.

**Beweis:** Ist die derivierte Reihe endlich, so ist $G$ wegen (8.5.2) auflösbar. Sei umgekehrt

$$G = G_0 \rhd G_1 \rhd \ldots \rhd G_k = \{e\}$$

eine Subnormalreihe mit abelschen Faktoren.

**Behauptung:** $G^{(i)} < G_i$ (da dann $\{e\} < G^{(k)} < G_k = \{e\}$, also $G^{(k)} = \{e\}$, folgt der Satz.)

**Beweis:** durch Induktion nach $i$: Für $i = 0$ ist das klar.

Sei nun $G^{(i)} < G_i$. Da $G_i/G_{i+1}$ abelsch ist, gilt nach (8.5.3)

$$G_{i+1} = \mathrm{Kern}(G_i \to G_i/G_{i+1}) > [G_i, G_i] > [G^{(i)}, G^{(i)}] = G^{(i+1)}.$$

□

**8.9 Satz:** (1) $G$ auflösbar $\Rightarrow$ jede Untergruppe von $G$ ist auflösbar.

(2) $U \lhd G$. Dann gilt $G$ auflösbar $\iff$ $U$ und $G/U$ sind auflösbar.

**Beweis:** (1) $U < G \Rightarrow [U,U] < [G,G] \Rightarrow$ (induktiv) $U^{(i)} < G^{(i)}$

(2) "$\Rightarrow$": $G$ auflösbar $\Rightarrow$ $U$ auflösbar nach (1).

Ist $p : G \to G/U$ die Projektion und $[x \cdot U, y \cdot U]$ ein Kommutator in $G/U$, so gilt

$$[x \cdot U, y \cdot U] = [p(x), p(y)] = p([x,y])$$

Also gilt $[G/U, G/U] = p([G,G])$ und induktiv $(G/U)^{(i)} = p(G^{(i)})$

"$\Leftarrow$": Seien

$$U = U_0 \rhd U_1 \rhd \ldots \rhd U_r = 1 \qquad G/U = K_0 \rhd K_1 \rhd \ldots \rhd K_t = 1$$

Subnormalreihen von $U$ und $G/U$ mit abelschen Faktoren.
Setzen wir $G_i = p^{-1}(K_i)$, so gilt $K_i = G_i/U$ und $G_{i+1} \lhd G_i$, da $K_{i+1} \lhd K_i$.
Beachte, dass $p^{-1}(1) = U$, also $G_t = U$. Damit ist

$$G = G_0 \rhd G_1 \rhd \ldots \rhd G_t = U \rhd U_1 \rhd \ldots \rhd U_r = 1$$

eine Subnormalreihe aus $G$. Die Quotienten $G_t/U_1$, $U_i/U_{i=1}$ sind abelsch. Dasselbe gilt für

$$G_i/G_{i+1} \cong (G_i/U)/(G_{i+1}/U) = K_i/K_{i+1}.$$

□

# 9 Ringe

**9.1 Definition:** Ein *Ring* ist eine Menge $R$ mit zwei Verknüpfungen + und $\cdot$, so dass gilt

(1) $(R, +)$ ist abelsche Gruppe mit neutralem Element 0

(2) $(R, \cdot)$ ist ein Monoid mit neutralem Element 1

(3) Es gelten die Distributivgesetze

$$a \cdot (b + c) = a \cdot b + a \cdot c, \quad (b + c) \cdot a = b \cdot a + c \cdot a \quad \forall a, b, c \in R$$

Ist $(R, \cdot)$ kommutativ, sprechen wir von einem *kommutativen Ring*.

**Bemerkung:** In der Algebra betrachtet man auch Ringe ohne Einselement 1.

**9.2 Konvention:** In dieser Vorlesung verstehen wir unter **Ring** einen kommutativen Ring mit 1.

**9.3 Definition:** $a \in (R, +, \cdot)$ heißt *Einheit*, wenn $a$ ein rechts- und ein linksinverses Element besitzt (die dann gleich sind). Die Gruppe der Einheiten von $(R, \cdot)$ wird mit $R^*$ bezeichnet.

**9.4 Definition:** Ein *Unterring* von $R$ ist eine Teilmenge $S \subset R$, so dass $S$ unter den Verknüpfungen + und $\cdot$ auf $R$ selbst ein Ring ist.

**9.5** Sei $S \subset R$, dann ist $S$ genau dann Unterring, wenn

(i) $S \neq \varnothing$

(ii) $x, y \in S \Rightarrow x - y \in S$ und $x \cdot y \in S$

(iii) $1 \in S$

**9.6 Definition:** Seien $a, b \in R\backslash\{0\}$ und sei $a \cdot b = 0$. Dann heißen $a$ und $b$ *Nullteiler*. Besitzt $R$ keinerlei Nullteiler, so heißt $R$ *nullteilerfrei*.

**9.7 Definition:** Ein *Integritätsring* ist ein nullteilerfreier Ring $R$. Ein Ring $R$, für den $R^* = R\backslash\{0\}$ ist, heißt *Körper*.

**9.8 Definition:** Eine Abbildung $f : R \to S$ heißt *Homomorphismus von Ringen*, wenn

$$f(x+y) = f(x) + f(y) \quad f(x \cdot y) = f(x) \cdot f(y) \quad \forall x, y \in R$$

und

$$f(1_R) = 1_S$$

**9.9** Ist $f : R \to S$ ein Ringhomomorphismus und $T \subset S$ ein Unterring, dann ist $f(R)$ ein Unterring von $S$ und $f^{-1}(T)$ ein Unterring von $R$.

**9.10 Definition:** Sei $R$ ein Ring. Eine Untergruppe $U$ von $(R, +)$ heißt *Ideal*, wenn gilt: $u \in U,\ r \in R \Rightarrow r \cdot u \in U$.

Ist $U \subset R$ ein Ideal, dann gilt für die übliche Multiplikation der Nebenklassen

$$(x+U) \cdot (y+U) = x \cdot y + x \cdot U + U \cdot y + U \cdot U \subset x \cdot y + U + U + U = x \cdot y + U$$

Da die Nebenklassena$\overline{x} = x + U$ eine disjunkte Zerlegung von $R$ bilden, wird jedem Paar $(\overline{x}, \overline{y})$ von Nebenklassen unter der üblichen Multiplikation **eindeutig** die Nebenklasse $\overline{x \cdot y}$ zugeordnet, denn

$$\overline{x} \cdot \overline{y} = (x+U) \cdot (y+U) \subset xy + U = \overline{x \cdot y}$$

Der folgende Satz ist damit trivial.

**9.11 Satz:** (1) Ist $U \subset R$ ein Ideal in einem Ring $R$, so ist $R/U$ unter

$$\overline{x} + \overline{y} := \overline{x+y} \quad \overline{x} \cdot \overline{y} := \overline{x \cdot y}$$

mit $\overline{x} = x + U$ ein Ring.

(2) Die Projektion $p : R \to R/U$ ist ein Ringhomomorphismus.

(3) Jedes Ideal ist Kern eines Ringhomomorphismus'. Umgekehrt ist der Kern eines Ringhomomorphismus' ein Ideal.

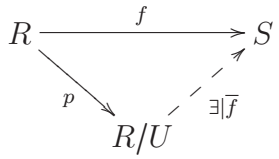
Wir erinnern an die **Isomorphiesätze:**

**9.12** (1) Ist $f : R \to S$ ein **Ringepimorphismus** mit Kern $U$. Dann ist die Abbildung

$$\{J \subset S; J \text{ Ideal }\} \to \{I \subset R; I \text{ Ideal }, U \subset I\}, \quad J \mapsto f^{-1}(J)$$

bijektiv. Also ist jedes Ideal $J \subset R/U$ von der Form $I/U$, wobei $I \subset R$ ein Ideal ist, das $U$ enthält.

(2) Ist $f : R \to S$ ein Ringhomomorphismus mit Kern $U$, dann gibt es genau einen Ringmonomorphismus $\overline{f} : R/U \to S$, so dass




Insbesondere gilt: $\overline{f} : R/U \cong$ Bild $f$ als Ring.

(3) Sei $R$ ein Ring mit Idealen $U \subset J \subset R$. Dann ist $J/U$ ein Ideal von $R/U$ und

$$(R/U)/(J/U) \cong R/J$$

(4) Sind $U, J$ Ideale von $R$, dann auch $U + J$, genannt *Summenideal* von $U$ und $J$, und es gilt

$$(U + J)/U \cong J/U \cap J$$

**9.13 Aufgabe:**

(1) Ist $\{U_\alpha, \alpha \in A\}$ eine Familie von Idealen in $R$, dann ist auch $\bigcap\limits_{\alpha \in A} U_\alpha$ ein Ideal.

(2) Ist $J_1 \subset J_2 \subset J_3 \subset \ldots$ eine aufsteigende Kette von Idealen in $R$, dann ist auch $\bigcup\limits_{n=1}^{\infty} J_n$ ein Ideal in $R$.

**9.14 Definition:** Sei $A \subset R$ eine Teilmenge. Das kleinste Ideal $I(A)$ von $R$, das $A$ enthält, heißt das von **A** *erzeugte Ideal*:

$$I(A) = \bigcap \{U \subset R;\ U \text{ Ideal }, A \subset U\}$$

Ein Ideal, das von einem einzigen Element erzeugt wird, heißt *Hauptideal*. Statt $I(\{a\})$ schreiben wir nur $(a)$.

Wir wollen die Form eines Hauptideals bestimmen: Zunächst enthält $(a)$ die von $a$ erzeugte zyklische Gruppe $< a >= \{n \cdot a;\ n \in \mathbb{Z}\}$, weiterhin alle Kombinationen $r \cdot n \cdot a$. Da $1 \in R$ und damit auch $n = 1 + \ldots 1 \in R$, sind diese von der Form $r \cdot a$. Also

**9.15** $(a) = \{r \cdot a; r \in R\} = R \cdot a$.

**9.16 Definition:** Ein *Hauptidealring* oder PID (für "principal ideal domain") ist ein Integritätsring, in dem jedes Ideal ein Hauptideal ist.

**9.17 Aufgabe:** Sind $U, J \subset R$ Ideale, dann definieren wir das *Produktideal* $U \cdot J$ als das von der Menge $\{u \cdot j; u \in U, j \in J\}$ erzeugte Ideal. Ist $K \subset R$ ein weiteres Ideal, gilt

(a) $U \cdot J \subset U \cap J$

(b) $U \cdot (J + K) = U \cdot J + U \cdot K, \quad (J + K) \cdot U = J \cdot U + K \cdot U$

**9.18 Beispiel:** Der Ring $\mathbb{Z}$ ist ein Hauptidealring.
Damit sind die Ideale von $\mathbb{Z}$ von der Form $(n)$ mit $n \in \mathbb{N}$. Die Quotientenringe $\mathbb{Z}/(n)$ sind die Restklassenringe $\mathbb{Z}/n$. Bezeichnet $\overline{k}$ die Restklasse von $k \in \mathbb{Z}$ modulo $n$, dann gilt

$$\begin{aligned} \overline{k} \in (\mathbb{Z}/n)^* &\iff \mathrm{ggT}(k, n) = 1 \\ \overline{k} \in \mathbb{Z}/n \text{ ist Nullteiler} &\iff \mathrm{ggT}(k, n) > 1 \end{aligned}$$

**9.19 Definition:** Ein Ring $R$ heißt *einfach*, wenn 0 und $R$ seine einzigen Ideale sind.

**9.20 Definition:** Ein Ideal $J$ von $R$ heißt *maximal*, wenn $J \neq R$ und aus $J \subset U \subset R$, $U$ Ideal, folgt $J = U$ oder $U = R$.

Aus (9.12.1) erhalten wir sofort für Ideale $J \neq R$.

**9.21** $J \subset R$ ist maximal $\iff R/J$ ist einfach.

Aus folgenden Grund sind maximale Ideale von Bedeutung.

**9.22 Satz:** Sei $R$ ein Ring und $J$ ein Ideal. Dann gilt $J \subset R$ maximal $\iff$ $R/J$ ist Körper.

Der Beweis von (9.22) folgt mit (9.21) aus

**9.23 Satz:** (1) Jeder Körper ist einfach.

(2) Jeder einfache Ring ist ein Körper.

**Beweis:**: (1) Sei $R$ ein Körper und $J \neq 0$ eine Ideal aus $R$. Sei $x \neq 0$ aus $J$. Dann ist $r = (r \cdot x^{-1}) \cdot x \in J$, also $J = R$.

(2) Sei $R$ ein einfacher Ring und $x \neq 0$. Wir müssen zeigen, dass $x$ ein Inverses besitzt. Sei $(x)$ das von $x$ erzeugte Ideal. Nach (9.15) ist $(x) = \{r \cdot x; r \in R\}$. Da $(x) = R$, gibt es ein $r \in R$ mit $r \cdot x = 1$. Also ist $x \in R^*$. □

**9.24 Beispiel:** In $\mathbb{Z}$ gilt: $m|n$ ($m$ *teilt* $n$) $\iff (n) \subset (m)$.
Also it $(m)$ genau dann maximal, wenn $m$ prim ist. Wir erhalten

$$\mathbb{Z}/n \text{ ist Körper} \iff n \in \mathbb{N} \text{ ist prim.}$$

Wir schließen mit einer Aufgabe.

**9.25 Aufgabe:** Zwei Ideale $I$ und $J$ eines Ringes $R$ heißen *coprim*, wenn $I + J = R$ ist.
Zeigen Sie:

(1) Sind $I$ und $J_1, \ldots, J_k$ Ideale, so dass $I$ und $J_l$ coprim sind für alle $l = 1, \ldots, k$, dann ist $I$ coprim zu $J_1 \cap \ldots \cap J_k$.

(2) Sind $J_1, \ldots, J_k$ Ideale in $R$, dann ist

$$p : R/\bigcap_{i=1}^{k} J_i \to R/J_1 \times \ldots \times R/J_k, \quad \overline{x} \mapsto (p_1(x), \ldots, (p_k(x))$$

ein injektiver Ringhomomorphismus, wobei $p_i : R \to R/J_i$ die Projektion ist.

(3) Sind in (2) die Ideale $J_i$ paarweise coprim, so ist $p$ ein Isomorphismus.

# 10 Teilerlehre in Ringen

**10.1 Definition:** Ein Ideal $P$ in einem Ring $R$ heißt *Primideal*, wenn $P \neq R$ und für Ideale $J_1, J_2$ von $R$ gilt: $J_1 \cdot J_2 \subset P \Rightarrow J_1 \subset P$ oder $J_2 \subset P$.

**10.2 Lemma:** Sei $P \neq R$ ein Ideal von $R$. Dann sind äquivalent

(1) $P$ ist ein Primideal.

(2) Für alle $a, b \in R$ gilt: $a \cdot b \in P \Rightarrow a \in P$ oder $b \in P$

**Beweis:**:(1)⇒(2): Sei $a \cdot b \in P$. Da

$$(a) \cdot (b) = R \cdot a \cdot R \cdot b = R \cdot a \cdot b = (a \cdot b) \subset P,$$

folgt $(a) \subset P$ oder $(b) \subset P$ und damit $a \in P$ oder $b \in P$.
(2)⇒(1): Seien $A, B$ Ideale in $R$ mit $A \cdot B \subset P$. Angenommen $A \notin P$ und $B \notin P$, dann gibt es ein $a \in A \backslash P$ und ein $b \in B \backslash P$. Da aber $a \cdot b \in P$, gilt $a \in P$ oder $b \in P$, ein Widerspruch. □

In $\mathbb{Z}$ stimmen die Primideale mit dem maximalen Idealen überein. Es ist daher zu vermuten, dass beide Begriffe ähnliche Eigenschaften haben und auch in anderen Fällen übereinstimmen. Wir zeigen als Resultat in dieser Richtung (vgl. 9.22).

**10.3 Satz:** Ist $R$ ein Ring, so gilt

$$J \subset R \text{ ist Primideal } \iff R/J \text{ ist Integritätsring.}$$

**Beweis:**: "⇒" seien $\overline{r}, \overline{s} \in R/J$ mit $\overline{r} \cdot \overline{s} = \overline{0}$. Dann gilt $r \cdot s \in J$. Also $r \in J$ oder $s \in J$ nach(10.2), d.h. $\overline{r} = \overline{0}$ oder $\overline{s} = \overline{0}$. Also ist $R/J$ nullteilerfrei.
"⇐" Sei $a \cdot b \in J$. Dann gilt $\overline{0} = \overline{a \cdot b} = \overline{a} \cdot \overline{b}$. Also $\overline{a} = \overline{0}$ oder $\overline{b} = \overline{0}$, d.h. $a \in J$ oder $b \in J$. Nach (10.2) ist $J$ Primideal. □

**10.4 Folgerung:** Jedes maximale Ideal ist prim.

**10.5 Definition:** Sei $R$ ein Ring, $a, b, c \in R$.

(1) $a$ *teilt* $b$, in Zeichen $a|b$, wenn es ein $x \in R$ gibt, so dass $a \cdot x = b$.

(2) $a$ ist *assoziiert* zu $b$, in Zeichen $a \sim b$, wenn $a|b$ und $b|a$.

(3) $c$ heißt *prim*, wenn $c \neq 0$, $c \notin R^*$ und aus $c|a \cdot b$ folgt, dass $c|a$ oder $c|b$.

(4) $c$ heißt *irreduzibel* , wenn $c \neq 0$, $c \notin R^*$ und aus $c = a \cdot b$ folgt, dass $a \in R^*$ oder $b \in R^*$.

**10.6** In einem Ring gilt

(1) $a \sim b \iff (a) = (b)$

(2) $c \neq 0$, $c \notin R^*$. Dann gilt: $c$ prim $\iff (c)$ ist Primideal.

**Beweis:**:

(1) $a \sim b \iff a|b$ und $b|a \iff (b) \subset (a)$ und $(a) \subset (b)$.

(2) $c$ prim $\iff$ $\{a \cdot b \in (c) \Rightarrow a \in (c)$ oder $b \in (c)\}$ $\iff$ $(c)$ Primideal (10.2).

□

In Integritätsringen $R$ kann man mehr zeigen. Denn es gilt

**10.7** In Integritätsringen $R$ kann man kürzen. D.h. für $x \neq 0$ gilt

$$a \cdot x = b \cdot x \iff a = b.$$

**Beweis:**: $a \cdot x = b \cdot x \iff (a-b) \cdot x = 0 \iff a - b = 0$, da $R$ nullteilerfrei ist. □

**10.8** In einem Integritätsring $R$ gilt

(1) $a \sim b \iff \exists u \in R^*$ mit $a = u \cdot b$.

(2) Jedes Primelement ist irreduzibel.

(3) Seien $a, b \in R$. Dann gilt: $\{(a) = R$ oder $(a) = (b)\} \Rightarrow (b) \subset (a) \iff a|b$. Ist $b$ irreduzibel, gilt auch die Umkehrung.

**Beweis:**:

(1) "$\Leftarrow$": $a = u \cdot b \Rightarrow b|a$. Weil auch $a \cdot u^{-1} = b$ ist, folgt $a|b$ und somit $a \sim b$.

"$\Rightarrow$": $a \sim b$ bedeutet $a|b$ und $b|a$. Also gibt es $x, y \in R$ mit $a \cdot x = b$ und $b \cdot y = a$. Es folgt $a \cdot x \cdot y = b \cdot y = a$. Ist $a = 0$, folgt $b = 0$, und $u = 1$ tut's. Ist $a \neq 0$, können wir kürzen und erhalten $x \cdot y = 1$, also $y \in R^*$.

(2) Sei $c$ prim und $c = a \cdot b$. Dann gilt $a \cdot b \in (c)$, also $a \in (c)$ oder $b \in (c)$, etwa $a \in (c)$. Dann gibt es ein $x \in R$ mit $a = x \cdot c = x \cdot b \cdot a$. Da $a \neq 0$, kann man kürzen: $1 = x \cdot b$; also $b \in R^*$.

(3) Der erste Teil ist trivial. Sei $b$ irreduzibel und $(b) \subset (a)$. Dann gilt $b = a \cdot x$ für ein $x \in R$. Es folgt $a \in R^*$ und damit $a \sim 1$ nach (1), d.h. $(a) = R$, oder $x \in R^*$ und damit $a \sim b$, d.h. $(a) = (b)$.

□

**10.9** In einem Hauptidealring $R$ gilt für $b \neq 0$.

$$b \text{ irreduzibel} \iff (b) \text{ maximal} \iff b \text{ prim}.$$

**Beweis:**: $b$ irreduzibel $\overset{(10.8.3)}{\iff}$ $(b)$ maximal $\overset{(10.4)}{\iff}$ $(b)$ prim und $b \neq 0$ $\overset{(10.6)}{\iff}$ $b$ prim $\overset{(10.8)}{\iff}$ $b$ irreduzibel □

Wir wollen jetzt das Problem der einfachen Primfaktorzerlegung angehen.

**10.10 Definition:** Ein *faktorieller* Ring (UFD= "unique factorization domain") ist ein Integritätsring $R$, in dem sich jedes $a \neq 0$, $a \notin R^*$ als Produkt von Primelementen schreiben lässt.

**10.11 Satz:** In einem faktoriellen Ring $R$ gilt

(1) Jedes irreduzibel Element ist prim.

(2) Ist $a \neq 0$, $a \notin R^*$, und sind

$$a = p_i \cdot \ldots \cdot = q_1 \cdot \ldots \cdot q_s$$

zwei Zerlegungen von $a$ in Primelemente, dann ist $r = s$ und nach einer Umnummerierung der $q_i$ gibt es zu jedem $p_i$ ein $u_i \in R^*$ mit $q_i = u_i \cdot p_i$.

D.h. die Primfaktorzerlegung von $a$ ist bis auf Reihenfolge und Multiplikation mit Einheiten eindeutig.

**Beweis:**:

(1) Sei $a$ irreduzibel und $p$ ein Primfaktor von $a$, also $a = p \cdot x$. Dann gilt $x \in R^*$, da $a$ irreduzibel und $p \notin R^*$ ist. Es folgt $a \sim p$, also ist $a$ prim nach (10.6).

(2) $p_1 | q_1 \cdot \ldots \cdot q_s$. Da $p_1$ prim ist, gibt es ein $i$, so dass $p_1 | q_i$ (wende die Definition (10.5) induktiv an). Wir nummerieren die $q_i$ so um, dass $p_1 | q_1$. Da $q_1$ irreduzibel ist und $p_1 \notin R^*$, folgt aus (10.8.3), dass $(p_1) = (q_1)$. Also gibt es ein $u_1 \in R^*$, so dass $q_1 = u_i p_1$ nach (10.8.1). Es folgt

$$p_1 \cdot p_2 \cdot \ldots \cdot p_r = p_1 \cdot u_1 \cdot q_2 \cdot \ldots \cdot q_s$$

Wir kürzen und erhalten

$$q_2 \cdot \ldots \cdot p_r = (u_1 \cdot q_2) \cdot q_3 \cdot \ldots \cdot q_s$$

Da $(u_1 \cdot q_2)$ ebenfalls prim ist, können wir induktiv fortfahren. Es folgt $r = s$ und die Aussage des Satzes

□

Bisher kennen wir keine Beispiele für ein UFD, es sei denn, wir glauben den in der Schule nie bewiesenen Satz, dass jedes Element aus $\mathbb{Z}$ eine eindeutige Primfaktorzerlegung im obigem Sinne hat. Z.B. gilt

$$6 = 2 \cdot 3 = 3 \cdot 2 = (-2) \cdot (-3) = (-3) \cdot (-2)$$

Aus der Einführung in die Algebra wissen wir

**10.12 Beispiel:** Jeder Hauptidealring ist faktoriell.

Um neue Beispiele zu finden, müssen wir also Hauptidealringe konstruieren. Dazu führen wir einen neuen Typ von Ring ein, der Eigenschaften besitzt, die an die ganzen Zahlen erinnern.

**10.13 Definition:** Ein *euklidischer Ring* ist ein Integritätsring $R$ mit einer Abbildung

$$\delta : R\backslash\{0\} \to \mathbb{N},$$

so dass

(1) $\delta(x) \leq \delta(x \cdot y) \quad \forall x, y \in R\backslash\{0\}$

(2) zu $b \in R\backslash\{0\}$ und $a \in R$ existieren $q, r \in R$, so dass

$$a = q \cdot b + r, \qquad \text{wobei } r = 0 \text{ oder } \delta(r) < \delta(b).$$

**10.14 Beispiel:**

(1) $\mathbb{Z}$ mit $\delta(x) = |x|$ ist ein euklidischer Ring.

(2) Der Polynomring $\mathbb{K}[x]$ über einem Körper ist euklidisch mit $\delta(P) = gradP$.

**10.15 Satz:** Jeder euklidische Ring $R$ ist ein Hauptidealring.

**Beweis:** Sei $J \neq 0$ ein Ideal in $R$. Wähle $a \in J$ derart, dass $\delta(a) = \min\{\delta(x); x \in J\backslash\{0\}\}$. Da $a \in J$, folgt $(a) \in J$.
Sei umgekehrt $x \in J$ beliebig. Da $a \neq 0$, gibt es $q, r \in R$ mit

$$x = q \cdot a + r, \qquad \text{wobei } r = 0 \text{ oder } \delta(r) < \delta(a).$$

$r = x - q \cdot a \in J$, da $x$ und $a$ aus $J$ sind. Nach Wahl von $a$, kann daher $\delta(r) < \delta(a)$ nicht zutreffen. Es folgt $r = 0$ und damit $x \in (a)$. □
Die euklidische Ringstruktur hat weitere Vorteile.

**10.16 Satz:** In einem euklidischen Ring $R$ gilt

(1) $\delta(1) \leq \delta(x) \quad \forall x \in R\backslash\{0\}$

(2) $x \in R^* \iff \delta(x) = \delta(1)$

**Beweis:**:

(1) Nach (10.13.1) gilt $\delta(1) \leq \delta(1 \cdot x) = \delta(x)$

(2) $x \in R^* \Rightarrow \exists y \in R$ mit $x \cdot y = 1 \Rightarrow \delta(1) \leq \delta(x) \leq \delta(x \cdot y) = \delta(1)$.

Sei umgekehrt $\delta(x) = \delta(1)$. Dann gibt es $q, r \in R$ mit

$$1 = q \cdot x + r, \qquad \text{wobei } r = 0 \text{ oder } \delta(r) < \delta(x) = \delta(1).$$

Nach (1) ist $\delta(r) < \delta(1)$ nicht möglich. Also ist $r = 0$ und $q = x^{-1}$. □

In euklidischen Ringen kann man darüber hinaus größte gemeinsame Teiler auf einfache Weise finden. Wir wollen jetzt, ausgehend von den Vorüberlegungen zu Anfang des Paragraphen, den Begriff des $ggT$ bzw $kgV$ in beliebigen kommutativen Ringen definieren.

**10.17 Definition:** Sei $R$ ein Ring und seien $a_1, \ldots, a_n \in R$. Wir nennen $d \in R$ **einen** $ggT(a_1, \ldots, a_n)$, wenn

(i) $d|a_i \ \forall i$

(ii) $r|a_i \ \forall i \Rightarrow r|d$

Wir nennen $v \in R$ **ein** $kgV(a_1, \ldots, a_n)$, wenn

(i) $a_i|v \ \forall i$

(ii) $a_i|r \ \forall i \Rightarrow v|r$

**10.18 Aufgabe:**

(1) Sei $R$ ein Ring und seien $a_1, \ldots, a_n \in R$. Sei $d$ ein $ggT(a_1, \ldots, a_n)$ und $v$ ein $kgV(a_1, \ldots, a_n)$. Zeigen Sie:

   (i) $d'$ ist ein $ggT(a_1, \ldots, a_n) \iff d$ und $d'$ sind assoziiert.

   (ii) $v'$ ist ein $kgV(a_1, \ldots, a_n) \iff v$ und $v'$ sind assoziiert.

(2) Sei $R$ ein Hauptidealring und $a_1, \ldots, a_n \in R$. Zeigen Sie

(i) $d$ ist $ggT(a_1,\ldots,a_n) \iff (d) = (a_1) + \ldots + (a_n)$

(ii) $v$ ist $kgV(a_1,\ldots,a_n) \iff (v) = (a_1) \cap \ldots \cap (a_n)$

Insbesondere gibt es in Hauptidealringen stets größte gemeinsame Teiler und kleinste gemeinsame Vielfache.

**10.19 Warnung:** In faktoriellen Ringen braucht (10.18.2) nicht zu gelten! Hier haben wir aber eine andere Möglichkeit, den $ggT$ oder das $kgV$ zu finden, eine Möglichkeit, die man in der Schule für $R = \mathbb{Z}$ intensiv nutzt.

**10.20 Satz:** In einem faktoriellen Ring existieren $ggT(a_1,\ldots,a_n)$ und $kgV(a_1,\ldots,a_n)$.

**10.21 Konstruktion von $ggT(a,b)$, $kgV(a,b)$:** Seien

$$a = p_1^{r_i} \ldots p_n^{r_n} \text{ und } b = p_1^{s_1} \ldots p_n^{s_n} \text{ mit } 0 \le r_i,\ 0 \le s_i$$

Primfaktorzerlegungen von $a$ und $b$. Dann ist

$$d = p_1^{t_1} \cdot \ldots \cdot p_n^{t_n} \text{ mit } t_i = \min(r_i, s_i),\ i = 1,\ldots,n$$

ein $ggT(a,b)$ und

$$v = p_1^{u_1} \cdot \ldots \cdot p_n^{u_n} \text{ mit } u_i = \max(r_i, s_i),\ i = 1,\ldots,n$$

ein $kgV(a,b)$.
Der Beweis ist trivial und der allgemeine Fall $ggT(a_1,\ldots,a_n)$ wird entsprechend behandelt.

**10.22 Bemerkung:** Aus (10.18) erhalten wir: Ist $R$ ein Hauptidealring und $d = ggT(a,b)$, dann besitzt $d$ eine Darstellung

$$d = r \cdot a + s \cdot b \text{ mit } r, s \in R$$

Diese Darstellung findet in der Zahlentheorie viele Anwendungen. In euklidischen Ringen gibt es konstruktive Verfahren für das Auffinden solcher Darstellungen.

**10.23 Der euklidische Algorithmus:** Sei $R$ euklidischer Ring .
Sei $r_0 \in R$ und $r_1 \in R\backslash\{0\}$. Wir konstruieren induktiv eine Folge

$$r_0, r_1, r_2, \ldots \quad \text{mit } \delta(r_1) > \delta(r_2) > \ldots \qquad (*)$$

durch

$$r_{i-1} = q_i \cdot r_i + r_{i+1} \text{ mit } r_{i+1} = 0 \text{ oder } \delta(r_{i+1}) < \delta(r_i). \qquad (**)$$

Da $\delta(r_1) > \delta(r_2) > \ldots$, muss die Folge abbrechen. D.h. es gibt ein $n$ mit

$$r_n \neq 0, \text{ aber } r_{n+1} = 0.$$

Dann ist

$$r_n = ggT(r_0, r_1).$$

Der Beweis folgt sofort aus $(**)$.
Induktiv konstruiert man eine Darstellung(Abwärtsinduktion)

$$r_n = a_i \cdot r_{i-1} + b_i r_i \quad a_i, b_i \in R,$$

beginnend mit

$$r_n = r_{n-2} - q_{n-1} r_{n-1} \quad \text{aus } (**)$$

**Induktionschritt:** Sei $r_n = a_i r_{i-1} + b_i r_i$
Aus $(**)$ erhalten wir $r_{i-2} - q_{i-1} r_{i-1} = r_i$. Also

$$r_n = a_i \cdot r_{i-1} + b_i(r_{i-2} - q_{i-1} r_{i-1}) = b_i r_{i-2} + (a_i - b_i q_{i-1}) r_{i-1}$$

So gewinnen wir die Darstellung

$$r_n = ggT(r_0, r_1) = a_1 r_0 + b_1 r_1.$$

**10.24 Beispiel:** Für große Zahlen ist (10.23) eine gute Methode, den $ggT$ zu berechnen: $r_0 = 17640$, $r_1 = 2772$

$$\begin{aligned} 17640 &= 6 \cdot 2772 + 1008 \\ 2772 &= 2 \cdot 1008 + 756 \\ 1008 &= 1 \cdot 756 + 252 \\ 756 &= 3 \cdot 252 + 0 \end{aligned}$$

Also: $252 = ggT(17640, 2772)$.

# 11 Polynomringe

Aus der Einführung in die Algebra wissen wir

**11.1 Satz:** Der Polynomring $\mathbb{K}[X]$ über einem Körper $\mathbb{K}$ ist euklidisch mit $\delta(f) = \operatorname{grad} f$.

Wir wollen nun Polynomringe über beliebigen Ringen $R$ studieren.

Für mathematische Untersuchungen ist folgende Eigenschaft des Polynomrings von Bedeutung

**11.2 Satz:** Sei $i : R \to R[X]$ der Monomorphismus von Ringen, der $r \in R$ auf das konstante Polynom $r \in R[X]$ abbildet. Sei $f : R \to R'$ ein Ringhomomorphismus in einen kommutativen Ring $R'$ und $z \in R'$. Dann gibt es genau einen Ringhomomorphismus $h : R[X] \to R'$, so dass

(1) $h \circ i = f$ (2) $h(X) = z$.

**Beweis:** Wir beginnen mit der Eindeutigkeit von $h$. Ist $R \subset R[X]$ der Unterring der konstanten Polynome und $r \in R$, dann gilt

$$\begin{aligned} h(r) = h(i(r)) &= f(r) \quad \text{wegen Bedingung (1)} \\ h(X^i) &= z^i \quad \text{wegen Bedingung (2)} \end{aligned}$$

Es folgt:

$$h\left(\sum_{i=0}^{n} a_i X^i\right) = \sum_{i=0}^{n} h(a_i) \cdot h(X^i) = \sum_{i=0}^{n} f(a_i) \cdot z^i \qquad (*)$$

Damit muß $h$ die Form $(*)$ haben. Offensichtlich erfüllt ein solches $h$ die Bedingungen (1) und (2). Wir müssen also nur nachweisen, daß $(*)$ einen Ringhomomorphismus definiert, aber das ist eine einfache Rechnung. □

Wir erinnern an die

**11.3 Gradformeln:** Sei $R$ ein Ring, und seien $f, g \in R[X] \backslash \{0\}$. Dann gilt

(1) $\operatorname{grad}(f+g) \leq \max(\operatorname{grad} f, \operatorname{grad} g)$

(2) $\operatorname{grad}(f \cdot g) \leq \operatorname{grad}(f) + \operatorname{grad}(g)$. Genauer gilt: Sind $a_m$ bzw. $b_n$ die *Leitkoeffizienten* von $f$ bzw. $g$, so folgt

$$\operatorname{grad}(f \cdot g) \begin{cases} = \operatorname{grad} f + \operatorname{grad} g, & \text{falls } a_m \cdot b_n \neq 0 \\ < \operatorname{grad} f + \operatorname{grad} g, & \text{falls } a_m \cdot b_n = 0 \end{cases}$$

Der Beweis von (11.3) ist trivial. Als Folgerung erhalten wir

**11.4 Satz:** Sei $R$ ein Integritätsring. Dann gilt:

(1) $R[X]$ ist ein Integritätsring, und $R[X]^* = R^*$.

(2) Ist $J \subset R$ ein Primideal, so ist $R[X] \cdot J$ ein Primideal in $R[X]$.

**Beweis:**: (1) folgt aus (11.3).
(2) Die Projektion $p : R \to R/J$ definiert einen Ringhomomorphismus

$$R[X] \to (R/J)[X]$$

mit Kern $J \cdot R[X]$. Da $R/J$ ein Integritätsring ist, ist auch $(R/J)[X]$ nach (1) ein Integritätsring. Damit ist $R[X] \cdot J$ nach (10.3) prim. □

**Zur Erinnerung:** $r \in R$ heißt *Nullstelle* des Polynoms $f = \sum_{i=0}^{n} a_i X^i \in R[X]$, wenn $f(r) := \sum_{i=0}^{n} a_i \cdot r^i = 0 \in R$.
Hierbei benutzen wir, daß jedes Polynom $f \in R[X]$ eine *Einsetzabbildung*

$$E_f : R \to R, \quad r \mapsto f(r)$$

definiert. $E_f$ ist i.a. **kein** Homomorphismus.
Aus der Einführung in die Algebra kennen wir die

**11.5 Division mit Rest:** Sei $R$ ein Ring, $f = \sum_{i=0}^{n} a_i X^i$, $g = \sum_{j=0}^{n} a_j X^j \in R[X]$ mit $b_m \in R^*$. Dann gibt es $q, r \in R[X]$, so daß

$$f = q \cdot g + r \quad \text{mit } r = 0 \text{ oder } \operatorname{grad} r < \operatorname{grad} g$$

**11.6 Satz:** Ist $R$ ein Ring und $r \in R$ eine Nullstelle von $f \in R[X]$, dann ist das lineare Polynom $X - r$ ein Teiler von $f$ in $R[X]$.

**11.7 Satz:** Ist $R$ ein **Integritätsring** und $f \in R[X]$ ein Polynom von Grad $n \geq 1$, dann hat $f$ höchstens $n$ Nullstellen.

Ein einfacher Test für Nullstellen ist

**11.8 Satz von Vieta:** Sei $R$ faktoriell und $K$ sein Quotientenkörper (s. nächster Abschnitt). Sei $f = \sum_{i=0}^{n} a_i X^i$ aus $R[X]$, seien $r, s \in R$ teilerfremd, $s \neq 0$ und $f\left(\frac{r}{s}\right) = 0$ in $K$. Dann gilt:

$$r \mid a_0 \text{ und } s \mid a_n$$

**Beweis:**:

$$\begin{aligned} 0 = s^n \cdot f\left(\tfrac{r}{s}\right) = \sum_{i=0}^{n} a_i \cdot s^{n-i} \cdot r^i &= a_0 s^n + r \cdot \sum_{i=1}^{n} a_i \cdot s^{n-i} \cdot r^{i-1} \\ &= s \sum_{i=0}^{n-1} a_i s^{n-i-1} \cdot r^i + a_n r^n \end{aligned}$$

Da $ggT(r,s) = 1$, folgt aus der eindeutigen Primfaktorzerlegung $r \mid a_0$ und $s \mid a_n$. □

Mehrfachnullstellen sind in vielen Fragen von Bedeutung.

**11.9 Definition:** Sei $R$ ein Ring. $r \in R$ heißt *n-fache Nullstelle* von $f \in R[X]$, falls $(X-r)^n$ Teiler von $f$, aber $(X-r)^{n+1}$ **kein** Teiler von $f$ ist. Für $n = 1$ sprechen wir von *einfachen*, für $n > 1$ von *mehrfachen* Nullstellen.

Für die Untersuchung mehrfacher Nullstellen ist die formale Ableitung von Polynomen von Bedeutung.

**11.10 Definition:** Sei $f = \sum_{i=0}^{n} a_i \cdot X^i \in R[X]$. Dann heißt

$$f' := \sum_{i=1}^{n} i \cdot a_i X^{i-1}$$

die *Ableitung* von $f$.

**11.11 Aufgabe: (Ableitungsregeln)** $\forall f, g \in R[X]$, $\forall r \in R$ gilt

$$\begin{aligned} (f+g)' &= f' + g' \\ (r \cdot f)' &= r \cdot f' \\ (f \cdot g)' &= f' \cdot g + f \cdot g' \\ (f^n)' &= n \cdot f^{n-1} \cdot f' \end{aligned}$$

**11.12** Sei $a \in R$ und $f \neq 0$ aus $R[X]$. Dann gilt

$$a \text{ mehrfache Nullstelle von } f \iff f'(a) = f(a) = 0$$

**Beweis:**: "⇒" $(X-a)^n$ teilt $f$ für ein $n > 1$, d.h. $f = q \cdot (X-a)^n$. Also gilt $f(a) = 0$ und

$$f' = q' \cdot (X-a)^n + n \cdot q \cdot (X-a)^{n-1}$$

Da $n - 1 > 0$, ist $f'(a) = 0$.

"⇐" Nach (11.9) ist $(X-a)$ Teiler von $f$ und $f'$, d.h. $f = g \cdot (X-a)$, $f' = h \cdot (X-a)$. Also gilt $f' = (X-a) \cdot g' + g = h \cdot (X-a)$. Es folgt $(X-a) \mid g$, d.h. $g = q \cdot (X-a)$. Also $f = q \cdot (X-a)^2$. □

**11.13 Satz:** Sei $K$ ein Körper und $R$ ein Ring, der $K$ als Unterring enthält. Dann gilt für $f \in K[X]$:

(1) Sind $f$ und $f'$ teilerfremd in $K[X]$, dann hat $f$ in $R$ keine mehrfachen Nullstellen.

(2) Ist $f$ irreduzibel, so gilt:

$f$ hat keine mehrfachen Nullstellen in $R$
$\iff$ $f'$ ist nicht das Nullpolynom oder $f$ hat keine Nullstelle

**Beweis:**:

(1) Ist $ggT(f, f') = 1$, gibt es $g, h \in K[X]$ mit $g \cdot f + h \cdot f' = 1$. Da diese Gleichung auch in $R[X]$ gilt, können $f$ und $f'$ keine gemeinsamen Nullstellen haben. (Hier benutzen wir, daß $K[X]$ euklidisch ist.)

(2) "$\Rightarrow$" Sei $a$ Nullstelle von $f$. Nach (11.12) ist $f'(a) \neq 0$, also $f' \neq 0$.

"$\Leftarrow$" Da $f$ irreduzibel ist, sind $f$ und $f'$ teilerfremd in $K[X]$. Also hat $f$ nach (1) keine mehrfachen Nullstellen.

□

Für unsere späteren Untersuchungen sind Primelemente in $R[X]$ wichtig. Wir wollen eine Methode vorstellen, solche Elemente zu finden.

**11.14 Definition:** Sei $R$ faktoriell. $f = \sum_{i=0}^{n} a_i \cdot X^i$ heißt *primitiv*, wenn $ggT(a_0, \ldots, a_n) = 1$

**11.15 Satz:** Sei $R$ ein faktorieller Ring und $K$ sein Quotientenkörper. Seien $f, g \in R[X]$, und sei $g$ primitiv. Ist $g$ ein Teiler von $f$ in $K[X]$, dann ist $g$ ein Teiler von $f$ in $R[X]$.

**Beweis:**: Sei $f = g \cdot h$ in $K[X]$. Da $K$ der Quotientenkörper ist, gibt es ein $a \in R$, etwa das Produkt der Nenner der Koeffizienten, so daß $a \cdot h \in R[X]$. Wir klammern aus $a \cdot h$ den $ggT$ der Koeffizienten aus und erhalten $a \cdot h = b \cdot \overline{h}$ mit primitivem $\overline{h}$. Indem wir gegebenfalls kürzen, dürfen wir annehmen, daß $ggT(a, b) = 1$. Dann gilt

$$a \cdot f = a \cdot g \cdot h = b \cdot g \cdot \overline{h}, \quad ggT(a, b) = 1,\ g, \overline{h} \in R[X] \text{ primitiv}$$

Sei $p \in R$ Primteiler von $a$. Nach (11.4.2) ist $p$ prim in $R[X]$, also Primteiler von $b \cdot g \cdot h$ in $R[X]$. Da $g$ und $\overline{h}$ primitiv sind, kann $p$ kein Primteiler von $g$ oder $\overline{h}$ sein. Da $ggT(a, b) = 1$, ist $p$ auch kein Teiler von $b$. Das ist unmöglich! Es folgt, daß $a$ keine Primteiler besitzt, d.h. $a \in R^*$, und damit $h = a^{-1} \cdot (a \cdot h) \in R[X]$. □

Die Bedeutung des Satzes liegt in

**11.16 Folgerung:** Sei $R$ faktoriell und $f \in R[X]$ sei primitiv. Sei $K$ der Quotientenkörper von $R$. Dann gilt

$$f \text{ prim in } R[X] \iff f \text{ prim in } K[X]$$

**Beweis:**: "⇒": Da $K[X]$ euklidisch ist, genügt es zu zeigen, daß $f$ irreduzibel ist. Wir nehmen an, daß $f = g \cdot h$ in $K[X]$, wobei $g$ den Leitkoeffizienten 1 hat und $\operatorname{grad} g$, $\operatorname{grad} h \geq 1$ ist (ist etwa $\operatorname{grad} g = 0$, so ist $g$ eine Einheit in $K[X]$). Indem wir $g$ mit einem geeignetem Element $a \in R$ multiplizieren, dürfen wir annehmen, daß $a \cdot g$ ein primitives Polynom in $R[X]$ ist (s. Beweis 11.15). Also hat $f$ eine Zerlegung ($a^{-1}$ existiert in $K$)

$$f = (a \cdot g) \cdot (a^{-1} \cdot h) = \overline{g} \cdot \overline{h}$$

in $K[X]$, wobei $f, \overline{g} \in R[X]$ primitiv sind. Nach (11.16) ist $\overline{g}$ Teiler von $f$ in $R[X]$, und da $\operatorname{grad} g < \operatorname{grad} f$ ist, ist $f$ reduzibel. Da $f$ prim und $R[X]$ nach (11.4) ein Integritätsring ist, ist das nach (10.8.2)) unmöglich.
"⇐": $f \mid g \cdot h$ in $R[X] \Rightarrow f \mid g \cdot h$ in $K[X] \Rightarrow f \mid g$ oder $f \mid h$ in $K[X]$ $\overset{(11.16)}{\Longrightarrow} f \mid g$ oder $f \mid h$ in $R[X]$. Also ist $f$ prim in $R[X]$. □

**11.17 Beispiel:** $f = X^3 + aX^2 + bX + c \in \mathbb{Z}[X]$ ist genau dann in $\mathbb{Q}[X]$ irreduzibel, wenn $f$ keine Nullstelle in $\mathbb{Z}$ hat. Letzteres ist sicher dann der Fall, wenn für jedenTeiler $t$ und $c$ in $\mathbb{Z}$ gilt $f(t) \neq 0$.

Zum Abschluss erinnern wir, ohne den Beweis zu wiederholen, an das

**11.18 Einstein'sches Irreduzibilitätskriterium:** Sei $R$ ein faktorieller Ring, $f = \sum_{i=0}^{n} a_i X^i \in R[X]$ ein primitives Polynom vom Grad $n > 0$. Gibt es ein Primelement $p \in R$, so dass $p \nmid a_n$, $p \mid a_i$ für $0 \leq i < n$ und $p^2 \nmid a_0$, dann ist $f$ irreduzibel in $R[X]$.

**11.19 Beispiel:** (1) Ist $p \in \mathbb{Z}$ prim, dann ist $X^n - p$ irreduzible in $\mathbb{Z}[X]$ und $\mathbb{Q}[X]$ für $n > 0$.

(2) Ist $p$ prim, dann ist

$$f(X) = 1 + X + X^2 + \ldots + X^{p-1}$$

irreduzibel in $\mathbb{Z}[X]$.

**Beweis:**(2) $f(X)$ irreduzibel $\iff$ $f(X+1)$ irreduzibel.
Da $(X-1) \cdot f(X) = X^p - 1$, gilt $X \cdot f(X+1) = (X+1)^p - 1 = \sum_{i=1}^{n} \binom{p}{i} \cdot X^i$, also

$$f(X+1) = \sum_{i=0}^{p-1} \binom{p}{i+1} \cdot X^i.$$

Aus (11.18) folgt die Irreduzibilität von $f(X+1)$. □

# 12 Lokalisierungen

Fr jeden Ring $R$ wollen wir seinen *Quotientenkörper*, den Körper seiner Brüche, konstruieren. Wir müssen also die multiplikativen Inversen hinzufügen, die in $R$ fehlen. Die dafür nötige Konstruktion führen wir in etwas größerer Allgemeinheit durch.

Sei $S \subset R$ eine Teilmenge. Wir wollen $R$ um die multiplikativen Inversen der Elemente von $S$ "erweitern". Sind $x, y \in S$ und haben wir $x^{-1}$ und $y^{-1}$, dann haben wir auch $(x \cdot y)^{-1} = y^{-1} \cdot x^{-1}$. Wir dürfen daher annehmen, dass $S$ multiplikativ abgeschlossen ist.

**12.1 Konstruktion:** Sei $(R, +, \cdot)$ ein Ring und $(S, \cdot)$ ein Untermonoid von $(R, \cdot)$. Wir definieren

$$S^{-1}R = (R \times S)/\sim$$

mit der Relation

$$(r_1, s_1) \sim (r_s, s_2) \iff \exists t \in S \text{ so dass } r_1 \cdot s_2 \cdot t = r_2 \cdot s_1 \cdot t.$$

Behauptung: Dies ist eine Äquivalenzrelation

$\sim$ ist reflexiv: $(r, s) \sim (r, s)$, denn $1 \in S$ und $r \cdot s \cdot 1 = r \cdot s \cdot 1$.

$\sim$ ist symmetrisch, da aus $r_1 \cdot s_2 \cdot t = r_2 \cdot s_1 \cdot t$ folgt $r_2 \cdot s_1 \cdot t = r_1 \cdot s_2 \cdot t$.

$\sim$ ist transitiv: $(r_1, s_1) \sim (r_2, s_2)$ und $(r_2, s_2) \sim (r_3, s_3)$. Dann gibt es $t_1, t_2 \in S$ mit

$$r_1 \cdot s_2 \cdot t_1 = r_2 \cdot s_1 \cdot t_1 \quad \text{und} \quad r_2 \cdot s_3 \cdot t_2 = r_3 \cdot s_2 \cdot t_2.$$

Es folgt

$$\begin{aligned} r_1 \cdot s_3 \cdot (s_2 \cdot t_1 \cdot t_2) &= r_2 \cdot s_3 \cdot s_1 \cdot t_1 \cdot t_2 = r_3 \cdot s_2 \cdot t_2 \cdot s_1 \cdot t_1 \\ &= r_3 \cdot s_1 \cdot (s_2 \cdot t_1 \cdot t_2) \end{aligned}$$

Da $s_2 \cdot t_1 \cdot t_2 \in S$, folgt $(r_1, s_1) \sim (r_3, s_3)$.

Die Äquivalenzklasse von $(r, s)$ wird suggestiv mit $\frac{r}{s}$ bezeichnet. Wir definieren nun

$$\frac{r_1}{s_1} \cdot \frac{r_2}{s_2} = \frac{r_1 \cdot r_2}{s_1 \cdot s_2} \qquad \frac{r_1}{s_1} + \frac{r_2}{s_2} = \frac{r_1 \cdot s_2 + r_2 \cdot s_1}{s_1 \cdot s_2}$$

Man sieht sofort, dass diese Verknüpfungen kommutativ sind, falls sie wohldefiniert sind. Für den Nachweis der Wohldefiniertheit braucht man daher nur zu zeigen:

Ist $(r_1, s_1) \sim (r_1', s_1')$, dann folgt

$$\begin{aligned} (r_1 \cdot r_2, s_1 \cdot s_2) &\sim (r_1' \cdot r_2, s_1' \cdot s_2) && (*) \\ (r_1 \cdot s_2 + r_2 \cdot s_1, s_1 \cdot s_2) &\sim (r_1' \cdot s_2 + r_2 \cdot s_1', s_1' \cdot s_2) && (**) \end{aligned}$$

Nach Voraussetzung gibt es ein $t \in S$, so dass $r_1 \cdot s_1' \cdot t = r_1' \cdot s_1 \cdot t$.
Es folgt

$$r_1 \cdot r_2 \cdot s_1' \cdot s_2 \cdot t = r_1' \cdot r_2 \cdot s_1 \cdot s_2 \cdot t,$$

also gilt $(*)$, und

$$\begin{aligned}(r_1 \cdot s_2 + r_2 \cdot s_1) \cdot s_1' \cdot s_2 \cdot t &= r_1 \cdot s_2 \cdot s_1' \cdot s_2 \cdot t + r_2 \cdot s_1 \cdot s_1' \cdot s_2 \cdot t \\ &= r_1' \cdot s_2 \cdot s_1 \cdot s_2 \cdot t + r_2 \cdot s_1 \cdot s_1' \cdot s_2 \cdot t \\ &= (r_1' \cdot s_2 + r_2 \cdot s_1') \cdot s_1 \cdot s_2 \cdot t,\end{aligned}$$

also gilt auch $(**)$.
$S^{-1}R$ ist ein Ring, die Axiome verifiziert man durch Nachrechnen. Das neutrale Element der Addition ist $\frac{0}{1}$, das der Multiplikation ist $\frac{1}{1}$. Die Elemente $\frac{s_1}{2_2}$ mit $s_1, s_2 \in S$ sind invertierbar: Das Inverse ist $\frac{s_2}{s_1}$, denn

$$\frac{s_1}{s_2} \cdot \frac{s_2}{s_1} = \frac{s_1 \cdot s_2}{s_1 \cdot s_2} = \frac{1}{1}$$

denn $(s_1 \cdot s_2, s_1 \cdot s_2) \sim (1,1)$, da $s_1 \cdot s_2 \in S$.

**12.2 Satz:** Die Abbildung $i_R : R \to S^{-1}R$, $r \mapsto \frac{r}{1}$ ist ein Ringhomomorphismus. Ist $R$ ein Integritätsring und $0 \notin S$, dann ist $i_R$ injektiv (also der Übergang von $R$ und $S^{-1}R$ eine Ringerweiterung).

**Beweis:**
$$\begin{aligned} i_R(r_1 + r_2) &= \frac{r_1 + r_2}{1} = \frac{r_1}{1} + \frac{r_2}{1} = i_R(r_1) + i_R(r_2) \\ i_R(r_1 \cdot r_2) &= \frac{r_1 \cdot r_2}{1} = \frac{r_1}{1} \cdot \frac{r_2}{1} = i_R(r_1) + \cdot i_R(r_2) \\ i_R(1) &= \frac{1}{1}\end{aligned}$$

Damit ist $i_R$ ein Ringhomomorphismus.
Sei nun $i_R(r_1) = i_R(r_2)$, also $\frac{r_1}{1} = \frac{r_2}{1}$. Es gibt also ein $t \in S$, so dass $r_1 \cdot t = r_2 \cdot t$. Ist $R$ ein Integritätsring, gilt die Kürzungsregel. Ist $0 \notin S$, also $t \neq 0$, folgt $r_1 = r_2$, so das $i_R$ injektiv ist. □

**12.3 Satz und Definition:** Ist $R$ ein Integritätsring, dann ist $S = R\backslash\{0\}$ ein Untermonoid von $(R, \cdot)$ und $S^{-1}R$ ist ein Körper, genannt *Quotientenkörper* oder *Körper der Brüche* von $R$. Nach (12.2) ist $i_R$ injektiv, so dass $R$ als Unterring des Körpers $S^{-1}R$ aufgefasst werden kann. □

**12.4 Aufgabe:** Sei $(R, +, \cdot)$ ein kommutativer Ring und $(S, \cdot)$ ein Untermonoid von $(R, \cdot)$. Dann gilt:

(1) Ist $f : R \to T$ ein Ringhomomorphismus in einen beliebigen Ring $T$, so daß $f(s) \in T^*$ für alle $s \in S$, dann gibt es genau einen Ringhomomorphimus, $\overline{f} : S^{-1}R \to T$, so daß $\overline{f} \circ i_R = f$.

(2) Ist $Q(R)$ ein Ring und $j_R : R \to Q(R)$ ein Ringhomomorphismus, so daß $j_R(s) \in (Q(R))^*$ für alle $s \in S$ und das Paar $(Q(R), j_R)$ die Aussage des Teils (1) wie $(S^{-1}R, i_R)$ erfüllt, dann gibt es genau einen *Ringisomorphismus* $h : S^{-1}R \cong Q(R)$, so daß $h \circ i_R = j_R$.

In der Algebra wird die Konstruktion (12.1) auch oft für Untermonoide $S \neq R\backslash\{0\}$ eingesetzt. Den wichtigsten Fall möchte ich kurz vorstellen.

**12.5** Ist $P \subset R$ ein Primideal in einem Ring $R$. Dann ist $S := \{r \in R; r \notin P\}$ ein Untermonoid von $(R, \cdot)$.

**Beweis:**: Da $P \neq R$, ist $1 \in S$. Sind $x, y \in S$, so ist $x \cdot y \in S$. Denn aus $x \cdot y \in P$ folgt $x \in P$ oder $y \in P$ nach (10.2). □

**12.6 Definition:** Sei $R$ ein Ring, $P \subset R$ ein Primideal und $S := R\backslash P$. Dann heißt $R_P := S^{-1}R$ *Lokalisierung* von $R$ an der Stelle $P$ (alle Elemente $x \notin P$ sind invertierbar gemacht).

**12.7 Satz:** $R_P$ hat genau ein maximales Ideal, nämlich das von $i_R(P)$ erzeugte Ideal.

**Beweis:**:

$$J = \{[\frac{p}{s}]; p \in P, s \in S = R\backslash P\}$$

ist das von $i_R(P)$ erzeugte Ideal. Denn offensichtlich ist $J$ ein Ideal, das $i_R(P)$ enthält, und da $\frac{p}{s} = \frac{1}{s} \cdot \frac{p}{1}$ ist, ist $\frac{p}{s}$ in dem von $i(P)$ erzeugten Ideal enthalten. Ist $\frac{r}{t} \notin J$, dann ist $r \in S$ und $\frac{r}{t}$ ist invertierbar mit Inversen $\frac{t}{r}$. Also ist $J$ maximal.

Ist umgekehrt $I \subset R_P$ maximal und $\frac{r}{s} \in I$, so ist $\frac{r}{s} \in J$. Andernfalls wäre $r \notin P$, also $\frac{r}{s}$ invertierbar, aber $I$ enthält keine invertierbaren Elemente. □

**12.8 Bemerkung und Definition:** Ringe mit genau einem maximalen Ideal spielen in der algebraischen Geometrie eine wichtige Rolle. Sie werden *lokale Ringe* genannt.

# Teil II
# Körper

## 13 Algebraische Erweiterungen

In diesem Paragraphen sei $K$ stets ein Körper. Damit ist $K[X]$ euklidisch.

**13.1 Konstruktion:** Sei $f \in K[X]$ irreduzibel. Dann ist das von $f$ erzeugte Ideal nach (10.9) maximal, also $F := K[X]/(f)$ ein Körper. Die Abbildung

$$i : K \subset K[X] \xrightarrow{\text{proj}} K[X]/(f) = F$$

ist ein Homomorphismus von Körpern.

**13.2** Jeder Homomorphismus $\varphi : K \longrightarrow F$ von Körpern ist injektiv.

**Beweis:**: $\operatorname{Kern}\varphi$ ist ein Ideal. Da $\varphi(1) = 1$ ist, ist $\operatorname{Kern}\varphi \neq K$. Da $K$ einfach ist, ist $\operatorname{Kern}\varphi = \{0\}$. □

Man kann daher $K$ als Unterkörper von $F$ in der Konstruktion (13.1) auffassen. Wir sprechen von einer „Körpererweiterung“.

**13.3 Definition:** Sind $K \subset L \subset F$ Körper, heißt $K$ *Unterkörper* von $F$, $F$ *Oberkörper* von $K$ und $L$ *Zwischenkörper* der *Körpererweiterung* $K \subset F$. Statt $K \subset F$ schreiben wir auch "$K/F$ sei Körpererweiterung".

Konstruktion 13.1 liefert uns also Körpererweiterungen. Wir können aber noch mehr sagen: Da wir $K$ vermöge des Monomorphismus' $i$ als Unterkörper von $F$ auffassen, können wir jedes $g \in K[X]$ auch als Element von $F[X]$ betrachten.

**13.4** Sei $\alpha$ die Restklasse von $X$ in $K[X]/(f) = F$, sei $g \in K[X]$ und $\text{proj} : K[X] \longrightarrow F$ die Projektion. Dann gilt

(1) $\text{proj}(g) = g(\alpha)$

(2) $f(\alpha) = 0$

**Beweis:** Sei $g = \Sigma_{i=0}^{n} a_i \cdot X^i$. Da proj ein Ringhomomorphismus ist und für $a \in K$ gilt $\text{proj}(a) = i(a) = a$ (nach unserer Definition von $K$ als Unterkörper von $F$), folgt

$$\text{proj}(g) = \Sigma_{i=0}^{n} a_i \cdot \text{proj}(X)^i = \Sigma_{i=0}^{n} a_i \cdot \alpha^i = g(\alpha)$$

(2) folgt, da $\text{proj}(f) = 0$. □

Damit ist $f$ über $F$ reduzibel. Indem wir das Verfahren für die irreduziblen Teiler von $f$ in $F[X]$ fortsetzen, erhalten wir

**13.5 Satz:** Ist $K$ ein Körper und $f \in K[X]$, dann gibt es eine Körpererweiterung $K \subset F$, so daß $f$ über $F$ in Linearfaktoren zerfällt.

**13.6 Definition:** Sei $f \in K[X]$. Dann heißt ein Erweiterungskörper $K \subset F$ *Zerfällungskörper* von $f$, wenn $f$ in $F[X]$ in Linearfaktoren zerfällt und es keinen Zwischenkörper $K \subset L \subset F$ gibt, so daß $L \neq F$ und $f$ in $L[X]$ in Linearfaktoren zerfällt.

Mit Zerfällungskörpern werden wir uns im nächsten Abschnitt beschäftigen.

**13.7 Definition:** Sei $K \subset F$ eine Körpererweiterung. $\alpha \in F$ heißt *algebraisch über* $K$, falls es ein $f \neq 0$ in $K[X]$ gibt, so daß $f(\alpha) = 0$. Gibt es kein solches Polynom, dann heißt $\alpha$ *transzendent über* $K$. Ist jedes $\alpha \in F$ algebraisch über $K$, heißt $K \subset F$ *algebraische Erweiterung.*

**13.8 Bezeichnung:** Sei $K$ Unterkörper eines Ringes $R$ und $M \subset R$ eine beliebige Teilmenge. Mit $K[M]$ und $K(M)$ bezeichnen wir den kleinsten Unterring bzw. den kleinsten Unterkörper von $R$, der $K$ und $M$ enthält.

**13.9 Aufgabe:** Sei $K$ Unterkörper eines Ringes $R$. Zeigen Sie:

(1) $K[M]$ existiert, aber $K(M)$ braucht es nicht zu geben.

(2) Ist $\alpha \in R$, dann ist $K[\alpha] = \{a_0 + a_1\alpha + \cdots + a_n\alpha^n;\ n \in \mathbb{N},\ a_i \in K \text{ für } i = 0, \ldots, n\}$.

(3) Ist $R$ ein Körper, dann existiert $K(M)$. Für $\alpha \in R$ ist dann $K(\alpha)$ der Körper der Brüche von $K[\alpha]$.

Sei $F/K$ Körpererweiterung mit $\alpha \in F$. Betrachte die *Einsetzabbildung*

$$\begin{aligned} E_\alpha : K[X] &\longrightarrow F \\ \Sigma_{i=0}^n\ a_i X^i &\longmapsto \Sigma_{i=0}^n\ a_i \cdot \alpha^i \end{aligned}$$

Aus 13.7 folgt:

**13.10**

$\alpha$ algebraisch über $K \iff \operatorname{Kern} E_\alpha \neq \{0\}$
$\alpha$ transzendent über $K \iff \operatorname{Kern} E_\alpha = \{0\} \iff E_\alpha$ ist injektiv.

**13.11 Satz:** Sei $K \subset F$ Körpererweiterung und $\alpha \in F$ algebraisch über $K$. Dann gibt es genau ein normiertes Polynom $f \in K[X]$, so daß $\operatorname{Kern} E_\alpha = (f)$. Dieses $f$ ist irreduzibel, und $E_\alpha$ induziert einen Isomorphismus

$$K[X]/(f) \cong K(\alpha) = K[\alpha].$$

**Beweis:**: Da $\alpha$ algebraisch ist, ist $\operatorname{Kern} E_\alpha \neq \{0\}$, wird also von einem Polynom $f \neq 0$ erzeugt. Wir dürfen annehmen, daß $f$ normiert ist. Angenommen, $f$ ist reduzibel, d.h. $f = g \cdot h$ mit $\operatorname{grad} g$, $\operatorname{grad} h \geq 1$, dann gilt

$$0 = f(\alpha) = g(\alpha) \cdot h(\alpha),$$

etwa $g(\alpha) = 0$. Dann ist $g \in \operatorname{Kern} E_\alpha$, also $f$ Teiler von $g$. Das ist unmöglich, da $\operatorname{grad} g < \operatorname{grad} f$.
Aus Aufgabe (13.9) folgt, daß Bild $E_\alpha = K[\alpha]$, so daß $K[\alpha] \cong K[X]/(f)$ nach dem Isomorphiesatz. Da $f$ irreduzibel ist, ist $K[X]/(f)$ ein Körper. Also ist $K[\alpha]$ bereits ein Körper. Es folgt $K[\alpha] = K(\alpha)$. □

**13.12 Definition:** Das eindeutig gegebene Polynom aus Satz 13.11 heißt das *Minimalpolynom* von $\alpha$ über $K$.

**13.13 Zusammenfassung:** Sei $F/K$ Körpererweiterung, $\alpha \in F$ algebraisch über $K$. Dann sind für $f \in K[X]$ folgende Aussagen äquivalent:

(1) $f$ ist Minimalpolynom von $\alpha$ über $K$.

(2) $f$ ist normiert, irreduzibel in $K[X]$ und $f(\alpha) = 0$.

(3) $f$ ist das normierter Polynom kleinsten Grades, für das $f(x) = 0$ ist.

(4) $f$ ist normiert, $f(\alpha) = 0$ und aus $g(\alpha) = 0$ mit $g \in K[X]$ folgt $f$ teilt $g$.

Weiterhin gilt:
$K[\alpha] = K(\alpha) \cong K[X]|(f)$, wobei $f$ das Minimalpolynom von $\alpha$ ist.
$K[a] \cong K^n$ mit Basis $\{1, a, a^2, \ldots, a^{n-1}\}$, falls $\operatorname{grad} f = n$ (Beweis s. 13.15).

Ist $K \subset F$ Körpererweiterung, dann definieren die Addition und Multiplikation in $F$ eine $K$-Vektorraumstruktur auf $F$.

**13.14 Definition:** $\dim_K F$ heißt *Grad* der Körpererweiterung $K \subset F$ und wird oft

$$\dim_K F = [F : K]$$

bezeichnet. Ist $[F : K] < \infty$, spricht man von einer *endlichen Körpererweiterung.*

Die Bezeichnung Grad kommt von folgendem Ergebnis

**13.15 Satz:** Ist $K \subset F$ Körpererweiterung, $\alpha \in F$ algebraisch über $K$ mit Minimalpolynom $f$. Dann ist $[K(\alpha) : K] = \operatorname{grad} f$, und $\mathcal{B} = \{1, \alpha, \alpha^2, \ldots, \alpha^{n-1}\}$ ist $K$-Basis von $K(\alpha)$, wobei $n = \operatorname{grad} f$.

**Beweis:** Nach 13.11 ist jedes $x \in K[\alpha] = K(\alpha)$ von der Form $x = g(\alpha)$ mit $g \in K[X]$. Nach dem Divisionsalgorithmus gibt es $q, r \in K[X]$, so dass $g = q \cdot f + r$ mit $r = 0$ oder $\operatorname{grad} r < \operatorname{grad} f$. Es folgt

$$x = g(\alpha) = q(\alpha) \cdot f(\alpha) + r(\alpha) = 0 + r(\alpha) = r(\alpha).$$

Ist $x \neq 0$, folgt, dass $x$ eine $K$-Linearkombination von $1, \alpha, \ldots, \alpha^{n-1}$ ist, weil $\operatorname{grad} r < \operatorname{grad} f$. Damit erzeugt $\{1, \alpha, \ldots, \alpha^{n-1}\}$ den $K$-Vektorraum $K(\alpha)$. Das Erzeugendensystem ist linear unabhängig, weil aus

$$c_0 \cdot 1 + c_1 \cdot \alpha + \ldots + c_{n-1} \cdot \alpha^{n-1} = 0 \quad \text{mit } c_i \in K$$

folgt, dass $g(\alpha) = 0$ für $g = c_0 + c_1 \cdot X^1 + \ldots + c_{n-1} X^{n-1} \in K[X]$. Da $f$ das Minimalpolynom von $\alpha$ ist und $\operatorname{grad} g < \operatorname{grad} f$, ist $g$ das Nullpolynom. □

**13.16 Beispiele:** $f = X^2 + X + 1$ ist irreduzibel über $\mathbb{Q}$, da $f$ über $\mathbb{Z}$ irreduzibel ist (s. 11.5 und 11.8). Sei $\alpha$ die Restklasse von $X$ im Körper $K = \mathbb{Q}[X]/(f)$. Nach (13.4) und (13.13) ist $f$ das Minimalpolynom von $\alpha$ über $\mathbb{Q}$, also $K$ ein 2-dimensionaler $\mathbb{Q}$-Vektorraum mit Basis $\{1, \alpha\}$, $\alpha = \bar{X}$

$$\mathbb{Q}[X]/(f) \cong \mathbb{Q} \times \mathbb{Q}.$$

Damit ist die Addition komponentenweise gegeben. Wir bestimmen die Multiplikation, ohne $\alpha$ zu kennen: $(a_0, a_1)$ und $(b_0, b_1)$ werden durch die Polynome $a_0 + a_1 X$ bzw. $b_0 + b_1 X$ repräsentiert. Das Produkt wird durch

$$(a_0 + a_1 X) \cdot (b_0 + b_1 X) = a_0 b_0 + (a_0 b_1 + a_1 b_0) X + a_1 b_1 X^2 \qquad (*)$$

repräsentiert. Da $\bar{f} = \bar{0}$ in $\mathbb{Q}[X]/(f)$, ist $\bar{X}^2 = -\bar{X} - \bar{1}$. Damit ist $(*)$ äquivalent zu

$$a_0 b_0 + (a_0 b_1 + a_1 b_0) \cdot X - a_1 b_1 X - a_1 b_1 = (a_0 b_0 - a_1 b_1) + (a_0 b_1 + a_1 b_0 - a_1 b_1) X.$$

Damit erhalten wir als Multiplikation

$$(a_0, a_1) \cdot (b_0, b_1) = (a_0 b_0 - a_1 b_1, a_0 b_1 + a_1 b_0 - a_1 b_1).$$

**13.17 Aufgabe:** Sei $K \subset F$ eine Körpererweiterung. Zeigen Sie:

(1) Genau dann gilt $[F : K] < \infty$, wenn es eine endliche Menge $M \subset F$ von über $K$ algebraischen Zahlen gibt, so daß $F = K(M)$.

(2) Ist $[F : K] < \infty$, so ist die Körpererweiterung $K \subset F$ algebraisch.

**13.18 Gradschachtelungsformel:** Gegeben seien endliche Körpererweiterungen $K \subset L$ und $L \subset F$. Sei $\{y_1, \ldots, y_k\}$ eine $K$-Basis von $L$ und $\{z_1, \ldots, z_n\}$ eine $L$-Basis von $F$. Dann ist $\{y_i z_j;\ i = 1, \ldots, k,\ j = 1, \ldots, n\}$ eine $K$-Basis von $F$. Insbesondere ist $K \subset F$ endliche Körpererweiterung und

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

**Beweis:**: Sei $\mathcal{B} = \{y_i \cdot z_j;\ i = 1, \ldots, k;\ j = 1, \ldots, n\}$

$\mathcal{B}$ erzeugt $F$ als $K$-Vektorraum:

Sei $x \in F$. Da $\{z_1, \ldots, z_n\}$ $L$-Basis von $F$ ist, gibt es $b_1, \ldots, b_n \in L$, so daß $x = \Sigma_{j=1}^{n} b_j z_j$.

Da $\{y_1, \ldots, y_k\}$ $K$-Basis von $L$ ist, gibt es zu jedem $b_j$ Elemente $a_{1_j}, \ldots, a_{k_j}$ aus $K$, so daß

$$b_j = \Sigma_{i=1}^{k} a_{ij} y_i.$$

Also

$$x = \sum_{i=1}^{k} \sum_{j=1}^{n} a_{ij} \cdot y_i z_j \qquad \text{mit } a_{ij} \in K.$$

$\mathcal{B}$ ist linear unabhängig: Sei $\sum\limits_{i=1}^{k} \sum\limits_{j=1}^{n} c_{ij} y_i \cdot z_j = 0$ mit $c_{ij} \in K$. Dann gilt $0 = \sum\limits_{j=1}^{n} \Big( \sum\limits_{i=1}^{k} c_{ij} y_i \Big) \cdot z_j$ mit $\Sigma_{i=1}^{k} c_{ij} y_i \in L$. Da $\{z_1, \ldots, z_n\}$ über $L$ linear unabhängig ist, folgt $\Sigma_{i=1}^{k} c_{ij} y_i = 0$ für alle $j$. Da $\{y_1, \ldots, y_k\}$ über $K$ linear unabhängig ist, folgt daraus

$$c_{ij} = 0 \quad \forall\ i = 1, \ldots, k \quad \forall\ j = 1, \ldots, n.$$

□

**13.19 Aufgabe:** (1) Für Körper $K \subset L \subset F$ ist $K \subset F$ genau dann eine algebraische Erweiterung, wenn $K \subset L$ und $L \subset F$ algebraische Erweiterungen sind.

(2) Sei $F/K$ algebraisch und $R$ ein Ring, so dass $K \subset R \subset F$, dann ist $R$ ein Körper.

**13.20 Transzendente Zahlen, ein kurzer Bericht:**
$z \in \mathbb{C}$ heißt *transzendent*, wenn $z$ über $\mathbb{Q}$ tranzendent ist.

1844 Lionville konstruiert tranzendente Zahlen z.B. $\sum_{n=0}^{\infty} \frac{1}{10^{n!}}$.

1873 Hermite: $e$ ist transzendent.

1873 Cantor: Es gibt überabzählbar viele transzendent Zahlen.

1892 Lindemann: $\pi$ ist transzendent.

1934 Gelford-Schneider: $\alpha, \beta$ seien algebraisch über $\mathbb{Q}$, $\alpha \neq 0, 1$, $\beta \notin \mathbb{Q}$. Dann ist $\alpha^\beta$ transzendent.

Offene Probleme:

(1) Ist Eulers Konstante

$$\gamma = \lim_{n\to\infty} \left( \sum_{k=1}^{n} \frac{1}{k} - \log n \right)$$

transzendent?

(2) Sind $e + \pi$ und $e - \pi$ transzendent?

**13.21 Die kleinsten Unterkörper:**
Sei $R$ ein Ring. Dann gibt es genau einen Ringhomomorphismus

$$\varphi : \mathbb{Z} \to \mathbb{R}$$

gegeben durch $n \mapsto n = 1 + 1 + \ldots + 1$, $n$-mal. Der Kern $\varphi$ ist ein Ideal $(m) \in \mathbb{Z}$, $m \geq 0$.

**13.22 Definition:** Dieses $m \in \mathbb{N}$ heißt *Charakteristik* von $R$, $m = \mathrm{char}(R)$.

Um zu betonen, dass $(\mathbb{Z}/p, +, \cdot)$ ein Körper ist, bezeichnen wir es mit $\mathbb{F}_p$ (hier steht $\mathbb{F}$ für das englische Wort "field").

**13.23 Satz:** Für einen Körper $K$ gilt:

(1) $\mathrm{char}(K)$ ist prim oder 0.

(2) Ist $\mathrm{char}(K) = 0$, so ist $\mathbb{Q}$ in eindeutiger Weise Unterkörper von $K$.

(3) Ist $\mathrm{char}(K) = p > 0$, so ist $\mathbb{F}_p$ in eindeutiger Weise Unerkörper von $K$.

(4) $\mathbb{Q}$ bzw. $\mathbb{F}_p$ sind dann die kleinsten Unterkörper von $K$.

**Beweis:** Ist $\mathrm{char}(K) = k \cdot l$ mit $k, l > 1$, dann ist $\varphi(k) \cdot \varphi(l) = \varphi(k \cdot l) = 0$. Da $\varphi(k) \neq 0$ und $\varphi(l) \neq 0$, hat $K$ Nullteiler, ist also kein Körper.
Ist $\mathrm{char}(K) = 0$, so ist $\varphi$ injektiv und erweitert nach (12.4) auf eindeutige Weise zu einem Körperhomomorphismus $\mathbb{Q} \to \mathbb{K}$, der nach (9.23) injektiv ist.
Ist $\mathrm{char}(K) = p$, so ist $\overline{\varphi} : \mathbb{Z}/\operatorname{Kern}\varphi = \mathbb{Z}/p \to K$ injektiv.
Die Minimalität folgt aus der Eindeutigkeit von $\varphi$. □

# 14 Zerfällungskörper und algebraischer Abschluss

In diesem Abschnitt bezeichnen $K$ und $F$ stets Körper.

**14.1 Definition:** Eine Körpererweiterung $F/K$ heißt *einfach*, wenn es ein $\alpha \in F$ gibt, so dass $F = K(\alpha)$. Ein solches $\alpha$ heißt *primitives Element* der einfachen Körpererweiterung $F/K$.

**14.2 Satz:** Sei $K(\alpha)/K$ einfache Körpererweiterung und $\varphi_0 : K \to F$ ein Körperhomomorphismus. Dann gilt:

(1) Ist $\alpha$ transzendent über $K$, dann definiert $\varphi \mapsto \varphi(\alpha)$ eine Bijektion

$$\left\{ \begin{array}{c} \text{Körperhomomorphismen} \\ \varphi : K(\alpha) \to F \text{ mit } \varphi|K = \varphi_0 \end{array} \right\} \cong \left\{ \begin{array}{c} x \in F;\ x \text{ ist transzendent} \\ \text{über } \varphi_0(K) \end{array} \right\}$$

Insbesondere ist $\varphi(\alpha)$ transzendent über $\varphi_0(K)$.

(2) Ist $\alpha$ algebraisch über $K$ mit Minimalpolynom $f \in K[X]$, dann definiert $\varphi \mapsto \varphi(\alpha)$ eine Bijektion

$$\left\{ \begin{array}{c} \text{Körperhomomorphismen} \\ \varphi : K(\alpha) \to F \text{ mit } \varphi|K = \varphi_0 \end{array} \right\} \cong \left\{ \begin{array}{c} \text{Nullstellen von} \\ \varphi_0(f) \in (\varphi_0 K)[X] \text{ in } F \end{array} \right\}$$

Insbesondere ist $\varphi(\alpha)$ Nullstelle von $\varphi_0(f)$.

**Beweis:** Beachte, dass $\varphi_0$ injektiv ist, also $\varphi_0(K)$ isomorph zu $K$ ist. $\varphi_0(f)$ erhält man aus $f$ durch Anwenden von $\varphi_0$ auf die Koeffizienten.
Ist $\alpha$ transzendent, dann ist $K[\alpha] \cong K[X]$ und $K[\alpha]$ ist der Unterring von $K(\alpha)$ aller Polynome in der Variablen $\alpha$. Nach 11.2 gibt es zu jedem $x \in F$ genau einen Ringhomomorphismus

$$\overline{\varphi_0} : K[\alpha] \to F \text{ mit } \overline{\varphi_0}|K = \varphi_0,\ \overline{\varphi_0}(\alpha) = x.$$

Wir fragen uns nun, wann sich $\overline{\varphi_0}$ auf den Quotientenkörper erweitern läßt. Nach 14.1 gibt es genau eine solche Erweiterung, falls $\overline{\varphi_0}(g) \neq 0 \ \forall g \neq 0$ aus $K[\alpha]$. Für $g = \sum_{i=0}^{n} b_i \alpha^i$ gilt

$$\overline{\varphi_0}(g) = \sum_{i=0}^{n} \varphi_0(b_i) \cdot x^i \qquad x = \overline{\varphi_0}(\alpha).$$

Die rechte Seite ist genau dann nie Null für $g \neq 0$, wenn

$$Ev_x : (\varphi_0 K)[X] \to F$$

injektiv ist, d.h. wenn $x$ transzendent über $\varphi_0(K)$ ist.

(2) Sei $f = \sum_{i=0}^{n} b_i \cdot X^i$ und $\varphi : K(\alpha) = K[\alpha] \to F$ eine Erweiterung von $\varphi_0$. Da

$$0 = \varphi(0) = \varphi(\sum_{i=0}^{n} b_i \cdot \alpha^i) = \sum_{i=0}^{n} \varphi_0(b_i) \cdot (\varphi(\alpha))^i,$$

ist $\varphi(\alpha)$ Nullstelle von $\varphi_0(f) \in (\varphi_0 K)[X]$ in $F$.
Ist umgekehrt $x$ eine Nullstelle von $\varphi_0(f)$, dann ist

$$f \in \text{Kern}(K[X] \to F;\ g(X) \mapsto (\varphi_0(g))(x)).$$

Da $f$ irreduzibel ist, folgt $(f)$ ist der ganze Kern. Wir erhalten also eine Abbildung

$$K[\alpha] \cong K[X]/(f) \to F, \quad \overline{g} \mapsto g(x), \quad \alpha = \overline{X} \mapsto x.$$

□

**14.3 Definition:** Sei $mathcalF \subset K[X]$ eine Menge von Polynomen. Sei $F/K$ eine Körpererweiterung. Wir sagen $F$ *zerfällt* $\mathcal{F}$, wenn jedes nichtkonstante Polynom $f$ aus $\mathcal{F}$ in $F[X]$ ein Produkt von Linearfaktoren ist. Ist $A \subset F$ die Menge aller Nullstellen aller Polynome aus $\mathcal{F}$ und gilt außerdem $F = K(A)$, heißt $F$ *Zerfällungskörper* von $\mathcal{F}$ und wird $\text{Zer}(\mathcal{F})$ bezeichnet.

Wir wollen uns mit der Existenz und Eindeutigkeit von Zerfällungskörpern beschäftigen.

Ist $\mathcal{F} \subset K[X]$ eine endliche Menge, dann gibt es nach 13.5 eine Körpererweiterung $F/K$, so dass jedes Polynom aus $\mathcal{F}$ über $F$ in Linearfaktoren, zerfällt. Ist $A \subset F$ die Menge der Nullstellen dieser Linearfaktoren, dann ist $K(A) \subset F$ ein Zerfällungskörper von $\mathcal{F}$. Wir erhalten

**14.4 Satz:** Ist $\mathcal{F} \subset K[X]$ endlich, dann existiert ein Zerfällungskörper $\mathrm{Zer}(\mathcal{F})$.

Für allgemeine $\mathcal{F}$ und zur Formulierung der Eindeutigkeit von Zerfällungskörpern empfiehlt es sich, im algebraischen Abschluss von $K$ zu arbeiten.

**14.5 Definition:** Ein Körper $K$ heißt *algebraisch abgeschlossen*, wenn jedes nicht-konstante Polynom aus $K[X]$ in Linearfaktoren zerfällt. Ist $F/K$ eine Körpererweiterung, dann heißt $F$ *algebraischer Abschluss* von $K$, falls $K \subset F$ algebraische Erweiterung und $F$ algebraisch abgeschlossen ist. Ein solches $F$ wird mit $\overline{K}$ bezeichnet.

**14.6 Satz:** Jeder Körper $K$ besitzt eine algebraische abgeschlossene Erweiterung $K \subset F$.

Der Beweis benutzt Zorn's Lemma, das zum Auswahlaxiom äquivalent ist. Wir erinnern:

**14.7 Auswahlaxiom:** Sei $J \neq \emptyset$ eine Menge und $\{M_j; j \in M\}$ eine Familie von Mengen $M_j \neq \emptyset$. Dann gibt es eine *Auswahlfunktion*

$$f : J \to \coprod_{j \in J} M_j$$

mit $f(j) \in M_j$.

**14.8 Zorn's Lemma:** Sei $(M, \leq)$ eine partiell geordnete Menge, so dass jede total geordnete Teilmenge eine obere Schranke besitzt. Dann hat $M$ ein maximales Element.

Wir verwenden Zorn's Lemma im Beweis von

**14.9 Lemma:** Sei $I \neq R$, $I \neq R$, eine Ideal in einem Ring $R$. Dann gibt es ein maximales Ideal $U$ in $R$ mit $I \subset U$.

**Beweis:** Sei $M$ die Menge aller Ideale $J$ mit $J \neq R$ und $I \subset J$. Die Inklusion $J_1 \subset J_2$ definiert auf $M$ eine partielle Ordnung.
Jede total geordnete Teilmenge $\{J_\alpha; \alpha \in A\}$ hat in $\bigcup_{\alpha \in A} J_\alpha$ eine obere Schranke.
Also besitzt $M$ ein maximales Element. □

**Beweis von 14.6:** Wir konstruieren eine Körpererweiterung $K \subset K_1$, so dass jedes nicht-konstante Polynom aus $K[X]$ in $K_1$ eine Nullstelle hat. Für jedes nicht-konstante $p \in K[X]$ wählen wir eine Unbestimmte $X_p$ und betrachten

den Polynomring $R$ über $K$ in den Unbestimmten $X_p$. Sei $J \subset R$ das Ideal, das von den Polynomen $p(X_p)$ erzeugt wird.

**Behauptung:** $J \neq R$.

**Beweis:** Angenommen $J = R$, dann haben wir eine Darstellung der 1

$$q_1 \cdot p_1(X_{p_1}) + \ldots + q_n \cdot p_n(X_{p_n}) = 1, \qquad (*)$$

wobei $q_j$ ein Polynom in den Variablen $X_p$ ist. Nach 13.5 gibt es eine Körpererweiterung $K \subset E$, so dass jedes der Polynome $p_1(X), \ldots, p_n(X)$ in $E$ eine Nullstelle hat, etwa $\alpha_1, \ldots, \alpha_n$. Setzen wir $X_{p_i} = \alpha_i$ und alle anderen in $(*)$ auftretenden Variablen $X_p = 0$, erhalten wir in $E$ die Gleichung $0 = 1$, ein Widerspruch.

Da $J \neq R$, gibt es nach 14.9 ein maximales Ideal $U \subset R$ mit $J \subset U$. Dann ist $K_1 = R/U$ ein Körper und $K \subset R \to R/U = K_1$ ist injektiv, so dass $K_1$ Erweiterung von $K$ ist. Jedes Polynom $p(X) \in K[X]$ hat die Restklasse von $X_p$ als Nullstelle in $K_1$ (vergl. 13.4). Wir iterieren die Konstruktion und erhalten eine Sequenz von Körpererweiterungen.

$$K \subset K_1 \subset K_2 \subset \ldots$$

so dass jedes Polynom über $K_i$ eine Nullstelle in $K_{i+1}$ hat. Dann ist $F = \bigcup K_i$ ein Erweiterungskörper von $K$. Ein Polynom $f \in F[K]$ hat seine Koeffizienten in einem $K_i$, liegt also in $K_i[X]$ und hat damit eine Nullstelle in $K_{i+1}$, also auch in $E$. Folglich zerfällt $f$ über $F$. □

**14.10 Folgerung:** Zu jeder Teilmenge $\mathcal{F} \subset K[X]$ existiert ein Zerfällungskörper $\mathrm{Zer}(\mathcal{F})$.

**Beweis:** Sei $K \subset E$ Körpererweiterung mit algebraisch abgeschlossenen $E$. Die Polynome aus $\mathcal{F}$ zerfallen über $E$. Sei $A$ die Menge der Nullstellen dieser Polynome. Dann ist $K(A) \subset E$ ein Zerfällungskörper von $\mathcal{F}$. □

Der im Beweis von 14.6 konstruierte Körper braucht nicht der algebraische Abschluss von $K$ zu sein: Wir wissen nicht, dass $F/K$ algebraisch ist.

**14.11 Definition und Satz:** Sei $F/K$ Körpererweiterung. Dann ist

$$E = \{\alpha \in F;\ \alpha \text{ ist algebraisch über } K\}$$

ein Unterkörper von $F$, genannt *algebraischer Abschluss von $K$ in $F$*.

**Beweis:** Sind $\alpha, \beta$ algebraisch über $K$, dann ist $[K[\alpha, \beta] : K] < \infty$. Nach 13.13 und 13.18 ist $K[\alpha, \beta]$ ein Körper und $K \subset K[\alpha, \beta]$ ist nach 13.17 algebraisch. Also sind $\alpha \pm \beta$, $\alpha \cdot \beta$, $\alpha/\beta \in K[\alpha, \beta]$ algebraisch über $K$. □

**14.12 Satz:** Für eine Körpererweiterung $F/K$ sind äquivalent

(1) $\mathcal{F}$ ist ein algebraischer Abschluss von $K$.

(2) $\mathcal{F}/K$ ist algebraisch und jedes nicht-konstante Polynom $p \in K[X]$ zerfällt in $F$.

(3) $\mathcal{F}$ ist eine maximale algebraische Erweiterung von $K$, d.h. $K \subset F$ ist algebraisch und ist $F \subset E$ algebraisch, folgt $F = E$.

**Beweis:** (1) $\Rightarrow$ (2): folgt aus der Definition des algebraischen Abschusses.
(2) $\Rightarrow$ (3): Sei $F \subset E$ algebraisch und $\alpha \in E$. Dann gibt es ein $f \in F[X]$, $f \neq 0$, so dass $f(\alpha) = 0$ in $E$. Da aber $f$ bereits über $F$ zerfällt, ist $\alpha \in F$.
(3) $\Rightarrow$ (1): Sei $p \in F[X]$ und $E$ der Zerfällungskörper von $p$ über $F$. Dann ist $F \subset E$ algebraisch, also $E = F$. Damit zerfällt $p$ in $F$. □

**14.13 Satz:** Jeder Körper $K$ besitzt einen algebraischen Abschluss. Genauer gilt: Ist $F/K$ eine algebraische Körpererweiterung und $F$ algebraisch abgeschlossen, dann ist der algebraische Abschluss $E$ von $K$ in $F$, $K \subset E \subset F$, ebenfalls algebraisch abgeschlossen und damit ein algebraischer Abschluss von $K$.

**Beweis:** Nach Definition ist $E$ algebraisch über $K$. Sei nun $p \in E[X]$. Dann zerfällt $p$ über $F$. Sei $\alpha \in F$ Nullstelle von $p$ in $F$. Dann ist $E \subset E(\alpha)$ algebraische Erweiterung. Da $K \subset E$ ebenfalls algebraisch ist, ist $K \subset E(\alpha)$ algebraisch, also $\alpha$ algebraisch über $K$ und somit $\alpha \in E$. D.h. $E$ ist algebraisch abgeschlossen. □

Nachdem wir die Existenz von Zerfällungskörpern und algebraischen Abschlüssen gezeigt haben, beschäftigen wir uns mit deren Eindeutigkeit.

Wir erinnern daran, dass jeder Körperhomomorphismus injektiv ist.

**14.14 Definition:** Seien $E/K$ und $F/K$ Körpererweiterungen und $L$ ein Körper

(1) Sind $\sigma : K \to L$ und $\tau : E \to L$ Körperhomomorphismen, so dass $\tau|K = \sigma$, nennen wir $\tau$ eine *Erweiterung* von $\sigma$.

(2) Ist $p = \sum a_i \cdot X^i \in K[X]$, dann bezeichnen wir $\sum \sigma(a_i) \cdot X^i \in L[X]$ mit $\sigma p$ oder $p^\sigma$.

(3) Einen Körperhomomorphismus $\tau : E \to F$, für den $\tau(\alpha) = \alpha \ \forall \alpha \in K$ nennen wir *$K$-Homomorphismus* oder kürzer *$K$-Morphismus*.

**14.15 Aufgabe:** Sei $\sigma : K \to L$ ein Körperhomomorphismus

(1) Sei $p \in K[X]$. Dann ist $\alpha \in K$ genau dann Nullstelle von $p$, wenn $\sigma(\alpha)$ Nullstelle von $p^\sigma$ ist.

(2) Sei $\{E_i; i \in I\}$ eine Familie von Unterkörpern von $K$. Mit $\bigvee E_i$ bezeichnen wir den kleinsten Unterkörper von $K$, der jedes $E_i$ enthält.

Zeigen Sie: $\sigma(\bigvee E_i) = \bigvee \sigma(E_i)$

(3) Sei $E \subset K$ Unterkörper und $\alpha_1, \ldots, \alpha_n \in K$. Dann gilt

$$\sigma(E(\alpha_1, \ldots, \alpha_n)) = \sigma(E)(\sigma(\alpha_1), \ldots, \sigma(\alpha_n)) \subset L$$

(4) Sei $F/K$ Körpererweiterung, $p \in K[X]$ und $N$ die Nullstellenmenge von $p$ in $F$. Dann permutiert jeder $K$-Morphismus $\sigma : F \to F$ die Elemente von $N$.

**14.16 Satz:** Sei $F/K$ algebraisch und $\sigma : F \to F$ ein $K$-Homomorphismus. Dann ist $\sigma$ ein Automorphismus.

**Beweis:** Wir müssen zeigen, dass $\sigma$ surjektiv ist. Sei $\alpha \in F$ und $f$ das Minimalpolynom von $\alpha$ über $K$. Sei $N \subset F$ die Nullstellenmenge von $f$ in $F$. Nach 14.15.4 permutiert $\sigma$ die Elemente von $N$. Da $\alpha \in N$, gibt es ein $\beta \in N$, so dass $\sigma(\beta) = \alpha$. □

**14.17 Satz:** Sei $F/K$ algebraische Erweiterung. Sei $L$ algebraisch abgeschlossen und $\sigma : K \to L$ ein Körperhomomorphismus. Dann kann $\sigma$ zu einem Homomorphismus $\tau : F \to L$ erweitert werden. Ist $f \in K[X]$ das Minimalpolynom von $\alpha \in F$ und ist $\beta \in L$ Nullstelle von $f^\sigma$, kann $\tau$ so gewählt werden, dass $\tau(\alpha) = \beta$.

**Beweis:** Sei $\mathcal{A}$ die Menge aller Paare $(E, \tau)$, wobei $K \subset K(\alpha) \subset E \subset F$ eine Sequenz von Körpererweiterungen und $\tau : E \to L$ eine Erweiterung von $\sigma$ ist, so dass $\tau(\alpha) = \beta$. Nach 14.2 gibt es ein Paar $(K(\alpha), \tau)$ in $\mathcal{A}$, also ist $\mathcal{A} \neq \varnothing$. Wir definieren eine partielle Ordnung auf $\mathcal{A}$ durch

$$(E_1, \tau_1) \leq (E_2, \tau_2), \text{ falls } E_1 \subset E_2 \text{ und } \tau_2|E_1 = \tau_1.$$

Ist $\{E_i, \tau_i); i \in I\}$ eine total geordnete Kette in $\mathcal{A}$, dann ist $(\bigcup E_i, \tau)$ mit $\tau|E_i = \tau_i$ eine obere Schranke. Nach Zorn's Lemma besitzt $\mathcal{A}$ ein maximales Element $(E, \tau)$. Dann gilt $E = F$, denn sonst gibt es ein $\gamma \in F \backslash E$. Da $\gamma$ über $K$ und damit auch über $E$ algebraisch ist, können wir $\tau$ nach 14.2 auf $E(\gamma)$ erweitern, im Widerspruch zur Maximalität. □

**14.18 Folgerung:** Sind $E$ und $F$ algebraische Abschlüsse von $K$, dann gibt es einen $K$-Isomorphismus $\sigma : E \xrightarrow{\cong} F$.

**Beweis:** Nach 14.17 können wir die Inklusion $K \subset F$ zu einem $K$-Morphismus $\sigma : E \to F$ erweitern. Da $E$ algebraisch abgeschlossen ist, ist auch $\sigma(E)$ algebraisch abgeschlossen. Da $F$ algebraische Erweiterung von $K$ ist, ist $F$ auch algebraische Erweiterung von $\sigma(E)$. Es folgt $F = \sigma(E)$. □

Wenden wir uns jetzt wieder Zerfällungskörpern zu.

**14.19 Satz:** Sei $\mathcal{F} \subset K[X]$ und seien $Z_1$ und $Z_2$ Zerfällungskörper von $\mathcal{F}$ über $K$. Dann gibt es einen $K$-Isomorphismus $\sigma : Z_1 \to Z_2$. Ist $\tau : Z_1 \to \overline{Z_2}$ ein $K$-Morphismus in den algebraischen Abschluss von $Z_2$, dann ist $\tau = (Z_1) = Z_2$.

**Beweis:** Da $K \subset Z_1$ algebraisch ist, gibt es nach 14.17 einen $K$-Morphismus $\tau : Z_1 \to \overline{Z_2}$. Sei $p \in \mathcal{F}$ und seien $E_1(p) \subset Z_1$, $E_2(p) \subset Z_2$ die Zerfällungskörper von $p$ in $Z_1$ bzw. $Z_2$.
Ist $A \subset E_1(p)$ die Nullstellenmenge von $p$, dann folgt aus 14.15

$$\tau(E_1(p)) = \tau(K(A)) = \tau(K)(\tau(A)) = K(\tau(A)) = E_2(p),$$

da $p^\tau = p$ ist. Mit 14.15.2 erhalten wir

$$\tau(Z_1) = \tau(\bigvee_{p \in \mathcal{F}} E_1(p)) = \bigvee_{p \in \mathcal{F}} E_2(P)) = Z_2.$$

□

# 15 Normale Erweiterungen

Ist $K \subset F$ algebraisch und ist $F$ nach 14.12 genau dann algebraischer Abschluss von $K$, wenn jedes $f \in K[X]$ über $F$ zerfällt. Schwächen wir diese Bedingung ab, indem wir nur fordern, dass $f$ über $F$ zerfällt, falls es dort eine Nullstelle hat, erhalten wir Zerfällungskörper.

**15.1 Satz:** Sei $K \subset F$ algebraisch und $K \subset F \subset \overline{K}$. Dann sind äquivalent

(1) Es gibt eine Menge $\mathcal{F} \subset K[X]$, so dass $F = \mathrm{Zer}(\mathcal{F})$.

(2) Jeder $K$-Morphismus $F \to \overline{K}$ ist ein Automorphismus von $F$.

(3) Jedes irreduzible Polynom aus $K[X]$, das in $F$ eine Nullstelle hat, zerfällt über $F$.

**Beweis:** (1) $\Rightarrow$ (2): Da $\overline{K} = \overline{\mathrm{Zer}(\mathcal{F})}$, folgt das aus 14.19.

(2) $\Rightarrow$ (3): Sei $f \in K[X]$ irreduzibel und $\alpha \in F$ eine Nullstelle von $f$. Sei $\beta \in \overline{K}$ eine beliebige Nullstelle von $f$, dann kann nach 14.17 die Einbettung $K \subset \overline{K}$ zu einem $K$-Morphismus $\sigma : F \to \overline{K}$ erweitert werden, so dass $\sigma(\alpha) = \beta$. Nach (2) definiert $\sigma$ eine $K$-Automorphismus $F \to F$, so dass $\beta \in F$. Also zerfällt $f$ über $F$.

(3) $\Rightarrow$ (1): $F$ ist der Zerfällungskörper von $\mathcal{F} = \{f_\alpha \in K[X]; \alpha \in F,$ $f_\alpha$ ist Minimalpolynom von $\alpha\}$. □

**15.2 Definition:** Eine algebraische Erweiterung $K \subset F$, die die äquivalenten Aussagen von 15.1 erfüllt, heißt *normale Erweiterung*.

**15.3 Beispiel:** (1) Jede quadratische Erweiterung ist normal.

(2) Jede der Erweiterungen

$$\mathbb{Q} \subset \mathbb{Q}(\sqrt{2}) \subset \mathbb{Q}(\sqrt[4]{2})$$

ist normal, dagegen $\mathbb{Q} \subset \mathbb{Q}(\sqrt[4]{2})$ nicht, denn $\mathbb{Q}(\sqrt[4]{2})$ enthält nur die Nullstellen $\pm\sqrt[4]{2}$ des Minimalpolynoms $X^4 - 2$, aber nicht $\pm i \cdot \sqrt[4]{2}$.

**15.4 Satz:** Ist $F/K$ endliche normale Erweiterung, dann ist $F$ der Zerfällungskörper einer endlichen Familie irreduzibler Polynome in $K[X]$.

**Beweis:** Sei $F = K(\alpha_1, \ldots, \alpha_n)$ und $f_i$ das Minimalpolynom von $\alpha_i$. Da $F/K$ normal ist, zerfällt jedes $f_i$ über $F$, so dass $F = \mathrm{Zer}\{f_1, \ldots, f_n\}$. □

**15.5 Eigenschaften normaler Erweiterungen:**

(1) Ist $K \subset F$ normal und $K \subset E \subset F$, dann ist auch $E \subset F$ normal.

(2) Gegeben sei ein Diagramm von Körpern

$$\begin{array}{ccc} K & \subset & E \\ \cap & & \cap \\ F & \subset & L \end{array}$$

Ist $K \subset E$ normal, dann auch $F \subset F \vee E$

(3) Sei $\{E_i, i \in I\}$ eine Familie von Zwischenkörpern $K \subset E_i \subset \overline{K}$, so dass $K \subset E_i$, für alle $i \in I$ normal ist. Dann sind auch

$$K \subset \bigcap_{i \in I} E_i \quad \text{und} \quad K \subset \bigvee_{i \in I} E_i$$

normal.

**Beweis:** (1) Sei $\mathcal{F} \subset K[X]$, so dass $F = \mathrm{Zer}(\mathcal{F})$. Fassen wir $\mathcal{F}$ als Teilmenge von $E[X]$ auf, erhalten wir das Resultat.

(2) Sei $E = \mathrm{Zer}(\mathcal{F})$, $\mathcal{F} \subset K[X]$. Sei $N \subset E$ die Menge der Nullstellen der Polynome aus $\mathcal{F}$, so dass $E = K(N)$. Da $F \vee E$ der kleinste Unterkörper von $L$ ist, der $F$ und $E$ enthält, gilt $F \vee E = F(N)$. Damit ist $F \vee E$ der Zerfällungskörper von $\mathcal{F}$ über $F$, also $F \subset F \vee E$ normal.

(3) Sei $\sigma : \bigvee_i E_i \longrightarrow \overline{K}$ ein $K$-Morphismus. Dann ist auch

$$\sigma_i = \sigma | E_i : E_i \longrightarrow \overline{K}$$

ein $K$-Morphismus. Da $K \subset E_i$ normal ist, gilt $\sigma_i(E_i) = E_i$. Es folgt

$$\begin{array}{rcccl} \sigma(\bigvee_i E_i) & = & \bigvee_i \sigma_i(E_i) & = & \bigvee_i E_i \\ \sigma(\bigcap_i E_i) & = & \bigcap_i \sigma_i(E_i) & = & \bigcap_i E_i. \end{array}$$

Nach 15.1 sind $K \subset \bigvee_i E_i$ und $K \subset \bigcap_i E_i$ normal. □

**15.6 Definition:** Sei $K \subset F \subset \overline{K}$ eine algebraische Erweiterung. Der *normale Abschluss* $F^{nc}$ von $F$ in $\overline{K}$ ist der kleinste Unterkörper von $\overline{K}$, so dass

(a) $F \subset F^{nc}$

(b) $K \subset F^{nc}$ ist normal.

**15.7** $F^{nc}$ existiert: Es gilt

$$F^{nc} = \bigcap \{E;\ E \text{ Körper}, F \subset E \subset \overline{K}, K \subset E \text{ ist normal}\}.$$

**Beweis:** Da $K \subset \overline{K}$ normal ist, existiert der Schnitt. Der Rest ist klar.

□

**15.8 Aufgabe:** Sei $K \subset F \subset \overline{K}$ algebraisch mit normalem Abschluss $F^{nc}$.

Zeigen Sie:

(a) $F^{nc} = \bigvee \{\sigma(F);\ \sigma F \to \overline{K} \text{ ist } K\text{-Morphismus}\}$

(b) $F^{nc} = \mathrm{Zer}(\mathcal{F}) \subset \overline{K}$, wobei $\mathcal{F} = \{f_\alpha \in K[X];\ \alpha \in F, f_\alpha \text{ Minimalpolynom von } \alpha\}$.

(c) $F^{nc} = \mathrm{Zer}(\mathcal{F}) \subset \overline{K}$, wobei $\mathcal{F} = \{f_\alpha \in K[X];\ \alpha \in B, f_\alpha \text{ Minimalpolynom von } \alpha\}$ und $B$ eine Basis des $K$-Vektorraumes $F$ ist.

(d) Ist $K \subset F$ endlich, dann ist $K \subset F^{nc}$ endlich.

# 16 Separable Erweiterungen

Sei $F/K$ eine Körpererweiterung und seien $f, g \in K[X]$. Wir wollen nun untersuchen, ob sich der $\mathrm{ggT}(f,g)$ ändert, wenn wir $f$ und $g$ als Polynome von $F[X]$ auffassen.

**16.1 Lemma:** Seien $f, g \in K[X]$ und $d_K \in K[X]$, $d_F \in F[X]$ normierte Polynome, so dass $d_K = \mathrm{ggT}(f,g)$ in $K[X]$ und $d_F = \mathrm{ggT}(f,g)$ in $F[X]$. Dann gilt $d_K = d_F$.

**Beweis:** In $K[X]$ gilt $(d_K) = (f) + (g)$, also

$$K[X] \cdot d_K = K[X] \cdot f + K[X] \cdot g.$$

Es folgt

$$\begin{aligned} F[X] \cdot d_K &= F[X] \cdot K[X] \cdot d_K \\ &= F[X] \cdot K[X] \cdot f + F[X] \cdot K[X] \cdot g \\ &= F[X] \cdot f + F[K] \cdot g \end{aligned}$$

also $d_K = \mathrm{ggT}(f,g)$ in $F[X]$. □

**16.2 Folgerung:** Sind $f, g \in K[X]$ normiert und irreduzibel, $f \neq g$, dann haben $f$ und $g$ in jeder Erweiterung $F$ von $K$ keine gemeinsame Nullstelle.

**16.3 Definition:** Wir sagen, $f \in K[X]$ hat *einfache* bzw. *mehrfache Nullstellen*, wenn $f$ in einem Zerfällungskörper einfache bzw. mehrfache Nullstellen hat.

**16.4 Lemma:** Für ein normiertes irreduzibles $f$ aus $K[X]$ sind äquivalent

(1) $f$ hat mindestens eine mehrfache Nullstelle.

(2) $\mathrm{ggT}(f, f') \neq 1$.

(3) $\mathrm{char}\, K = p \neq 0$ und $f(X) = g(X^p)$ für ein $g \in K[X]$.

(4) $f$ hat nur mehrfache Nullstellen.

**Beweis:** Wir rechnen in einem algebraischen Abschluß $\overline{K}$ von $K$. Sei $f = \sum_{i=0}^{n} a_i X^i$.

(1) $\Rightarrow$ (2): Ist $a \in \overline{K}$ Mehrfachnullstelle, so ist $X - a$ nach 11.12 Teiler von $f$ und $f'$.

(2) $\Rightarrow$ (3): Da $f$ irreduzibel und $\operatorname{grad}(f') < \operatorname{grad}(f)$ ist, ist $\operatorname{ggT}(f, f') = 1$ oder $f' = 0$. Es folgt

$$0 = f' = \sum_{i=0}^{n} a_i \cdot i \cdot X^{i-1}, \qquad \text{d.h. } a_i \cdot i = 0 \text{ in } K \ \forall i = 0, \ldots, n.$$

Das erreicht man nur, wenn $\operatorname{char} K = p > 0$ und $p|i$, falls $a_i \neq 0$.

(3) $\Rightarrow$ (4): Da $\operatorname{char} K = p > 0$, gilt $(X - a)^p = X^p - a^p$. Sei $f = g(X^p)$ und $g = \prod (X - \alpha_i)^{r_i}$ in $\overline{K}[X]$. Dann gilt

$$f = \prod (X^p - \alpha_i)^{r_i} = \prod (X - b_i)^{p \cdot r_i},$$

wobei $b_i^p = \alpha_i$. Die $b_i$ existieren in $\overline{K}$, da $X^p - \alpha_i$ in Linearfaktoren zerfällt, d.h. die $p$-te Wurzel von $\alpha_i$ existiert. Damit hat jede Nullstelle von $f$ mindestens die Vielfachheit $p$.

(4) $\Rightarrow$ (1): Da $f$ normiert und irreduzible ist, ist $\operatorname{grad} f \geq 1$. Also hat $f$ Nullstellen und damit mindestens eine mehrfache Nullstelle. □

**16.5 Definition:** Ein Polynom $f \in K[X]$ heißt *separabel*, wenn seine irreduziblen Faktoren nur einfache Nullstellen haben. Ist $f$ nicht separabel, ist es *inseparable*.

**16.6 Folgerungen und Bezeichnung:**

(1) Ist $\operatorname{char} K = 0$, dann ist nach 16.4 jedes Polynom aus $K[X]$ separabel

(2) Ist $\operatorname{char} K = p > 0$ und $f \in K[X]$ normiert, irreduzibel und inseparabel, gibt es nach 16.4 ein $g_1 \in K[X]$, mit $f(X) = g_1(X^p)$. Da $f$ irreduzibel und normiert ist, ist auch $g_1$ irreduzibel und normiert. Ist $g_1$ inseparabel, gibt es ein $g_2 \in K[X]$, so dass $g_1(X) = g_2(X^p)$, also $f(X) = g_2(X^{p^2})$ ist. Wir fahren fort, bis wir ein separables $g_d \in K[X]$ erhalten:
Ist $f$ inseparabel, dann gibt es ein separables Polynom $g \in K[X]$ mit $f(X) = g(X^{p^d}),\ d > 0$. Wir nennen $d$ den *Radikalexponenten* von $f$.
Ist $f$ separabel, ist sein Radikalexponenten $d = 0$. In diesem Fall ist $f = g$.

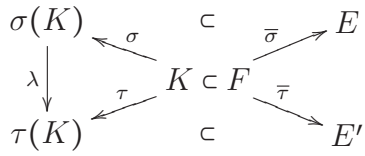
**16.7 Definition:** Sei $K \subset F$. Wir nennen $\alpha \in F$ *separabel über* $K$, falls $\alpha$ über $K$ algebraisch und sein Minimalpolynom separabel ist. $F/K$ ist *separable Erweiterung*, wenn jedes $\alpha \in F$ separabel über $K$ ist.

**16.8 Satz:** Sei $F/K$ algebraisch. Seien $\sigma : K \to E$, $\tau : K \to E'$ Körperhomomorphismen (und damit Einbettungen) in algebraisch abgeschlossene Körper $E$ und $E'$. Dann gilt

$$|\mathcal{E}_\sigma(F, K)| = |\mathcal{E}_\tau(F, K)|,$$

wobei $\mathcal{E}_\sigma(F,K)$ die Menge der Erweiterungen $F \to E$ von $\sigma$ ist.

**Beweis:** Ist $\overline{\sigma} : F \to E$ Erweiterung von $\sigma$, dann ist $\overline{\sigma}(F)$ algebraisch über $\overline{\sigma}(K) = \sigma(K)$, weil $F/K$ algebraisch ist. Also liegt $\overline{\sigma}(F)$ im algebraischen Abschluss von $\sigma(K)$ in $E$. Wir dürfen daher annehmen, dass $E$ und $E'$ algebraische Abschlüsse von $\sigma(K)$ bzw. $\tau(K)$ sind.




Der Isomorphismus $\lambda = \tau \circ \sigma^{-1} : \sigma(K) \to \tau(K)$. kann nach 14.17 zu einem Homomorphismus $\overline{\lambda} : E \to E'$ erweitert werden, der ein Isomorphismus ist nach der Argumentation im Beweis von 14.18. Damit ist die Abbildung

$$\mathcal{E}_\sigma(F,K) \to \mathcal{E}_\tau(F,K), \quad \overline{\sigma} \mapsto \overline{\lambda} \circ \overline{\sigma}$$

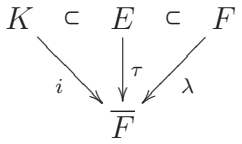
bijektiv. □

**16.9 Definition:** Sei $F/K$ algebraisch und $\sigma : K \to E$ eine Einbettung in einem algebraisch abgeschlossenen Körper. Dann heißt $|\mathcal{E}_\sigma(F,K)|$ *Separabilitätsgrad* von $F$ über $K$ und wird mit $[F:K]_{\text{sep}}$ bezeichnet.

**16.10 Satz:** Sind $K \subset E \subset F$ algebraisch, dann gilt

$$[F:K]_{\text{sep}} = [F:E]_{\text{sep}} \cdot [E:K]_{\text{sep}}.$$

**Beweis:** Sei $i : K \subset E \subset F \subset \overline{F}$ die Inklusion. Ist $\tau \in \mathcal{E}_\sigma(F,K)$ und $\lambda \in \mathcal{E}_\tau(F,E)$, dann ist $\lambda \in \mathcal{E}_i(F,K)$




Wir erhalten die Abbildung

$$\coprod_{\tau \in \mathcal{E}_i(E,K)} \mathcal{E}_\tau(F,E) \to \mathcal{E}_i(F,K)$$

Diese Abbildung ist injektiv, weil verschiedene $\tau$ zu verschiedenen $\lambda$ führen. Sie ist auch surjektiv, denn jede Erweiterung $\lambda$ von $i$ definert durch Einschränkung ein $\tau$. Da $|\mathcal{E}_{\tau_1}(F,E)| = |\mathcal{E}_{\tau_2}(F,E)|$, folgt der Satz. □

**16.11 Satz:** Sei $\operatorname{char} K = 0$ oder $\operatorname{char} K = p$ und $K \subset K(\alpha)$ eine einfache algebraische Erweiterung. Sei $f \in K[X]$ das Minimalpolynom von $\alpha$ und $d$ sein Radikalexponent. Dann gilt

(1) $p^d \cdot [K(\alpha) : K]_{\text{sep}} = [K(\alpha) : K]$

(2) Folgende Aussagen sind äquivalent:

(i) $\alpha$ ist separabel über $K$

(ii) $[K(\alpha) : K]_{\text{sep}} = [K(\alpha) : K]$

(iii) $K \subset K(\alpha)$ ist separabel.

(Zur Erinnerung: Ist $\operatorname{char} K = 0$, dann ist $f$ separabel und $d = 0$)

**Beweis:** (1) Nach 14.2 ist die Anzahl der Erweiterungen von $i : K \subset \overline{K}$ auf $K(\alpha)$ gleich der Anzahl der Nullstellen von $f$ in $\overline{K}$. Ist $f$ separabel, hat es $\operatorname{grad}(f)$ verschiedene Nullstellen. Es folgt

$$[K(\alpha) : K]_{\text{sep}} = |\mathcal{E}_i(K(\alpha), K)| = \operatorname{grad} f = [K(\alpha) : K].$$

Hat $f$ den Radikalexponenten $d$, folgt $f(X) = g(X^{p^d})$ für ein separables $g \in K[X]$. Damit hat jede Nullstelle von $f$ die Vielfachheit $p^d$. Es folgt

$$p^d \cdot [K(\alpha) : K]_{\text{sep}} = \operatorname{grad} f = [K(\alpha) : K].$$

(2) $f$ ist genau dann separabel, wenn $d = 0$ ist. Das beweist die Äquivalenz von (i) und (ii). Offensichtlich folgt (i) aus (iii). Wir zeigen noch:
(ii) $\Rightarrow$ (iii): Sei $\beta \in K(\alpha)$. Dann haben wir $K \subset K(\beta) \subset K(\alpha)$ und damit

$$[K(\alpha) : K(\beta)]_{\text{sep}} \cdot [K(\beta) : K]_{\text{sep}} = [K(\alpha) : K]_{\text{sep}} = [K(\alpha) : K(\beta)] \cdot [K(\beta) : K].$$

Da $K(\alpha) = K(\beta)(\alpha)$, folgt aus Teil (1):

$[K(\alpha) : K(\beta)]_{\text{sep}}$ teilt $[K(\alpha) : K(\beta)]$ und $[K(\beta) : K]_{\text{sep}}$ teilt $[K(\beta) : K]$

Es folgt $[K(\beta) : K]_{\text{sep}} = [K(\beta) : K]$. Also ist $\beta$ separabel über $K$.

□

Wir erweitern das Resultat auf endliche Erweiterungen.

**16.12 Satz:** Für eine endliche Erweiterung $F/K$ gilt

(1) $[F : K]_{\text{sep}}$ teilt $[F : K]$

(2) Äquivalent sind

(i) Es gibt eine Menge $S \subset F$ von über $K$ separablen Elementen, so dass $F = K(S)$.

(ii) $[F : K]_{\text{sep}} = [F : K]$

(iii) $F/K$ ist separabel.

**Beweis:** (1) Da $F/K$ endlich ist, gibt es über $K$ algebraische Elemente $\alpha_1, \ldots, \alpha_n$ aus $F$, so dass $F = K(\alpha_1, \ldots, \alpha_n)$. Für

$$K \subset K(\alpha_1) \subset K(\alpha_1, \alpha_2) \subset \ldots \subset K(\alpha_1, \ldots, \alpha_n) \qquad (*)$$

erhalten wir aus 16.10

$$[K(\alpha_1, \ldots, \alpha_n) : K]_{\text{sep}} = \prod_{i=1}^{n} [K(\alpha_1, \ldots, \alpha_i) : K(\alpha_1, \ldots, \alpha_{i-1})]_{\text{sep}}.$$

Damit folgt (1) aus 16.11.1.

(2) (i) $\Rightarrow$ (ii): Sei $S \subset F$ eine Menge von über $K$ separabelen Elementen, so dass $F = K(S)$. Da $F/K$ endlich ist, dürfen wir annehmen, dass $F = K(\alpha_1, \ldots, \alpha_n)$ mit $\alpha_1, \ldots, \alpha_n \in S$. Da $\alpha_i$ über $K$ separabel ist, ist es über $K(\alpha_1, \ldots, \alpha_{i-1})$ separabel. Aus 16.11 folgt

$$[K((\alpha_1, \ldots, \alpha_i) : K(\alpha_1, \ldots, \alpha_{i-1})]_{\text{sep}} = [K(\alpha_1, \ldots, \alpha_i) : K(\alpha_1, \ldots, \alpha_{i-1})]$$

und damit $[F : K]_{\text{sep}} = [F : K]$.

(ii) $\Rightarrow$ (iii): Für $\beta \in F$ betrachten wir $K \subset K(\beta) \subset F$. Aus

$$[F : K(\beta)]_{\text{sep}} \cdot [K(\beta) : K]_{\text{sep}} = [F : K]_{\text{sep}} = [F : K] = [F : K(\beta)] \cdot [K(\beta) : K]$$

und Teil (1) folgt $[K(\beta) : K]_{\text{sep}} = [K(\beta) : K]$. Nach 16.11 ist $\beta$ separabel über $K$.

(iii) $\Rightarrow$ (i): Nehme $S = F$. □

Für unser nächstes Ergebnis verwenden wir ein Resultat, das von eigenständigen Interesse ist.

**16.13 Satz:** Jede endliche Untergruppe $G$ der multiplikativen Gruppe $(K^*, \cdot)$ ist zyklisch.

**Beweis:** Sei $|G| = p_1^{r_1} \ldots p_k^{r_k}$ mit $p_1 < \ldots < p_k$ die Primfaktorzerlegung von $|G|$. Da $G$ abelsch ist, ist es das innere Produkt seiner Sylowuntergruppen, d.h. es gibt einen Isomorphismus

$$\alpha : G \cong S_1 \times \ldots \times S_k; \quad S_i \ \ p_i - \text{Sylowuntergruppe}.$$

Sei $x \in G$ das Urbild von $(z_1, \ldots, z_k)$, wobei $z_i \in S_i$ maximale Ordnung $t_i$ hat. Ist $y_i \in S_i$, gilt $\mathrm{ord}(y_i) | p_i^{r_i}$ und damit $\mathrm{ord}(y_i) | t_i$. Es folgt $\mathrm{ord}(x) = \mathrm{kgV}(\mathrm{ord}(z_1), \ldots, (z_k)) = t_1 \cdot \ldots \cdot t_k = q$, und für jedes $y \in G$ gilt $\mathrm{ord}(y) | q$. Da $x^q = 1$, sind die verschiedenen Elemente $1, x, x^2, \ldots, x^{q-1}$ Nullstellen des Polynoms $X^q - 1$. Weitere Nulllstellen kann das Polynom nach 11.7 nicht haben. Ist $y \in G$, so haben wir gesehen, dass $\mathrm{ord}(y) | q$, also $y$ Nullstelle von $X^q - 1$ ist. Es folgt $G = \langle x \rangle$. □

**16.14 Folgerung:** Ist $F/K$ Körpererweiterung und $F$ endlich, dann ist $F/K$ einfach (d.h. es gibt ein $\alpha \in F$, so dass $F = K(\alpha)$).

**Beweis:** Sei $\alpha \in F$ Erzeuger von $(F^*, \cdot)$, dann ist $F = K(\alpha)$. □

**16.15 Satz:** Sei $F = K[\alpha_1, \ldots, \alpha_r]$ eine endliche Erweiterung von $K$, und seien $\alpha_2, \ldots, \alpha_r$ (aber nicht notwendige $\alpha_1$) separabel über $K$. Dann gibt es ein primitives Element $\gamma \in F$, so dass $F = K[\gamma]$.

**Beweis:** Für endliche Körper haben wir das in 16.14 gezeigt. Sei also $K$ unendlich. Es genügt, den Satz für $r = 2$ zu zeigen, der Rest folgt durch Induktion. Sei also $F = K[\alpha, \beta]$ und $\beta$ separabel über $K$. Seien $f$ und $g$ aus $K[X]$ die Minimalpolynome von $\alpha$ und $\beta$. Seien weiterhin

$$\begin{array}{lll} \alpha_1 = \alpha, & \alpha_2, \ldots, \ \alpha_s & \text{die Nullstellen von } f \\ \beta_1 = \beta, & \beta_2, \ldots, \ \beta_t & \text{die Nullstellen von } g \end{array}$$

in einem algebraischen Abschluß $\overline{F}$ von $F$. Da $g$ separabel ist, sind die $\beta_i$ alle verschieden. Damit hat die Gleichung

$$\alpha_i + X\beta_j = \alpha_1 + X\beta_1 \quad j > 1$$

genau eine Lösung, nämlich $X = \frac{\alpha_i - \alpha_1}{\beta_1 - \beta_j}$. Da $K$ unendlich ist, gibt es ein $c \in K$, das von allen diesen Lösungen verschieden ist, d.h.

$$\alpha_i + c\beta_j \neq \alpha + c\beta \quad \text{für } j \neq 1.$$

**Behauptung:** $F = K(\gamma)$ mit $\gamma = \alpha + c\beta$.

**Beweis:** $K(\gamma) \subset F = K[\alpha, \beta]$.

Die Polynome $g$ und $f(\gamma - cX)$ aus $(K[\gamma])[X]$ haben $\beta$ als Nullstelle. $\beta$ ist ihre einzige gemeinsame Nullstelle in $\overline{F}$, denn für $j > 1$ gilt $\gamma - c\beta_j \neq \alpha_i$ für alle $i$, d.h. $\beta_j$ ist nicht Nullstelle von $f(\gamma - cX)$. Also gilt

$$X - \beta = \mathrm{ggT}(g, f(\gamma - cX)) \quad \text{in } \overline{F}[X]$$

und damit auch in $K[\gamma][X]$ nach 16.1. Es folgt, $\beta \in K[\gamma]$ und damit auch $\alpha = \gamma - c\beta \in K[\gamma]$, so dass $K[\alpha, \beta] \subset K[\gamma]$. □

**16.16** Der Beweis zeigt, dass wir im allgemeinen Fall $F = K[\alpha_1, \alpha_2, \ldots, \alpha_r]$ ein primitives Element $\gamma$ der Form

$$\gamma = \alpha_1 + c_2\alpha_2 + \ldots + c_r\alpha_r \quad c_i \in K$$

finden können.

**16.17 Folgerung:** Ist $\mathrm{char}(K) = 0$ oder $K$ endlich, dann ist jede endliche Erweiterung $K \subset F$ einfach.

**Beweis:** Ist $\mathrm{char}(K) = 0$, folgt das direkt aus 16.15, weil jedes $\alpha \in F$ separabel ist. Ist $K$ endlich und $K \subset F$ endliche Erweiterung, dann ist auch $F$ endlich, so dass wir 16.14 anwenden können. □

**16.18 Definition:** Sei $\alpha$ algebraisch über $K$ mit Minimalpolynom $f$. Wir nennen $\alpha$ *rein inseparabel* über $K$, wenn $f$ die Form $f = (X - \alpha)^n, n \geq 1$ über seinem Zerfällungskörper hat. Eine Erweiterung $F/K$ heißt *rein inseparabel*, wenn jedes $\alpha \in F$ rein inseparabel über $K$ ist.

**16.19 Beispiel:** Sei $\mathrm{char}(K) = 2$ und $\gamma$ tranzendent über $K$. Dann ist $\gamma$ über $K(\gamma^2)$ rein inseparabel, weil sein Minimalpolynom $X^2 - \gamma^2 = (X - \gamma)^2$ ist.

**16.20 Definition:** Der *Inseperabilitätsgrad* $[F : K]_i$ einer endlichen Erweiterung $K \subset F$ ist

$$[F : K]_i = \frac{[F : K]}{[F : K]_{\mathrm{sep}}}.$$

**16.21 Aufgabe:** Sei $K \subset F$ endliche Erweiterung. Zeigen Sie:

(1) Für $K \subset E \subset F$ gilt $[F : K]_i = [F : E]_i \cdot [E : K]_i$

(2) $K \subset F$ separabel $\iff [F : K]_i = 1$

(3) Sei $\alpha \in F$, $\mathrm{char}(F) = p > 0$, dann gilt $[K(\alpha) : K]_i = p^d$, wobei $d$ der Radikalexponent von $\alpha$ ist.

(4) Sei $\mathrm{char}(F) = p > 0$, dann ist $[F : K]_i$ eine Potenz von $p$.

Wir wollen nun die rein inseparablen Elemente charakterisieren. Da in Charakteristik 0 alle Polynome separabel sind, haben wir

**16.22 Satz:** Ist $\mathrm{char}(K) = 0$ und $\alpha$ über $K$ algebraisch, dann gilt: $\alpha$ rein inseparabel über $K \iff \alpha \in K$.

Ist $\mathrm{char}(K) = p > 0$, haben wir

**16.23 Satz:** Sei $\alpha$ über $K$ algebraisch mit Radikalexponent $d$ und Minimalpolynom $f$. Sei $p = \mathrm{char}(K) > 0$. Dann sind äquivalent:

(1) $\alpha$ ist rein inseparabel über $K$.

(2) Es gibt ein $n \geq 1$, so dass $(X - \alpha)^n \in K[X]$.

(3) $f = (X - \alpha)^{p^d} = X^{p^d} - \alpha^{p^d}$.

(4) Es gibt ein $\beta \in K$ und ein $k \geq 0$, so dass $\alpha$ Nullstelle von $X^{p^k} - \beta$ ist.

(5) $\alpha^{p^k} \in K$ für ein $k \geq 0$

(6) $d$ ist die kleinste Zahl in $\mathbb{N}$ mit $\alpha^{p^d} \in K$.

**Beweis:** Nach Definition gibt es ein separables Polynom $q \in K[X]$, so dass $f = q(X^{p^d})$

(1) $\Rightarrow$ (2): Nach Definition von rein inseparabel erfüllt $f$ die Bedingung.

(2) $\Rightarrow$ (3): Da $\alpha$ Nullstelle von $(X - \alpha)^n \in K[X]$ ist, folgt $f | (X - \alpha)^n$ in $K[X]$, also gibt es ein $r \leq n$, so dass $q(X^{p^d}) = (X - \alpha)^r$. Ist $\operatorname{grad} q = m$, folgt $r = m \cdot p^d$, so dass

$$q(X^{p^d}) = (X - \alpha)^{m \cdot p^d} = (X^{p^d} - \alpha^{p^d})^m.$$

Es folgt $q(X) = (X - \alpha^{p^d})^m$. Da $q$ separabel ist, folgt $m = 1$, so dass

$$f = q(X^{p^d}) = X^{p^d} - \alpha^{p^d}$$

(3) $\Rightarrow$ (4): Nehme $k = d$ und $\beta = \alpha^{p^d}$. Da $f \in K[X]$, ist $\beta \in K$.

(4) $\Rightarrow$ (5): Nach Voraussetzung ist $\alpha^{p^k} - \beta = 0$, also $\alpha^{p^k} \in K$.

(5) $\Rightarrow$ (6): $g(X) := X^{p^k} - \alpha^{p^k} = (X - \alpha)^{p^k}$ ist aus $K[X]$ nach Voraussetzung. Da $g(\alpha) = 0$, ist $q(X^{p^d})$ Teiler von $g$. Wie im Beweis ((2) $\Rightarrow$ (3)), folgt daraus

$$f = X^{p^d} - \alpha^{p^d},$$

so dass $\alpha^{p^d} \in K$. Außerdem folgt $d \leq k$. Also ist $d$ die kleinste Zahl $k$ in $\mathbb{N}$, so dass $\alpha^{p^k} \in K$.

(6) $\Rightarrow$ (1): $g = (X - \alpha)^{p^d} = X^{p^d} - \alpha^{p^d} \in K[X]$. Da $g(\alpha) = 0$, folgt $f | g$, d.h. $f$ hat die Form $(X - \alpha)^n$ für ein $n \geq 1$. Also ist $\alpha$ rein separabel. □

**16.24 Aufgabe:** Für eine algebraische Erweiterung $K \subset F$ sind äquivalent

(1) Es gibt eine Menge $S \subset F$ von inseparablen Elementen, so dass $F = K(S)$.

(2) $[F : K]_{\text{sep}} = 1$

(3) $K \subset F$ ist rein inseparabel.

Sei $K \subset F$ und seien $\alpha, \beta \in F$ separabel über $K$ Dann ist nach $K \subset K(\alpha, \beta)$ nach 16.12.2 separable Erweiterung. Also sind auch $\alpha \pm \beta$, $\alpha \cdot \beta$ und für $\alpha \neq 0$ auch $\alpha^{-1}$ separabel über $K$. Die Menge $F^{sa}$ der über $K$ separablen Elemente bildt einen Unterkörper von $F$. Dasselbe gilt für die Menge $F^{ia}$ der über $K$ rein inseparablen Elemente von $F$ nach 16.24.

**16.25 Bezeichnung:** Die Zwischenkörper $K \subset F^{sa} \subset F$ und $K \subset F^{ia} \subset F$ nennt man den *separablen* bzw. *rein inseparablen Abschluss* von $K$ in $F$.

**16.26 Satz:** Sei $F/K$ algebraische Erweiterung. Dann gilt:

(1) In $K \subset F^{sa} \subset F$ ist $K \subset F^{sa}$ separabel und $F^{sa} \subset F$ rein inseparabel.

(2) $\alpha \in F \Rightarrow \alpha^{[F:K]_i} \in F^{sa}$.

(3) Jeder Körperhomomorphismus $\sigma : F \to \overline{F}$ ist durch $\sigma|F^{sa}$ bestimmt.

**Beweis:** In Charakteristik 0 gilt der Satz offensichtlich, weil $F^{sa} = F$. Sei also $\text{char}(K) = p > 0$.

(1) Nach Definition ist $K \subset F^{sa}$ separabel. $\alpha \in F$ habe Radikalexponent $d$ und Minimalpolynom $f = q(X^{p^d})$ mit separablem $q$. Dann ist $q$ Minimalpolynom von $\alpha^{p^d}$, also ist $\alpha^{p^d} \in F^{sa}$. Nach 16.23 ist $\alpha$ rein inserabel über $F^{sa}$.

(2) Sei $\alpha \in F$ wie in Beweis (1). Nach 16.21.3 gilt $p^d = [K(\alpha) : K]_i$, also $p^d | [F : K]_i$ nach 16.21.1. Wie wir im Beweis (1) gesehen haben, ist $\alpha^{p^d}$ und damit auch $\alpha^{[F:K]_i}$ in $F^{sa}$.

(3) Nach Definition des Separabilitätsgrades ist $[F : F^{sa}]_{\text{sep}}$ die Anzahl der Erweiterungen eines Körpermorphismuses $\sigma : F^{sa} \to \overline{F}$ auf $F$. Da $F^{sa} \subset F$ rein inseparabel ist, ist $[F : F^{sa}]_{\text{sep}} = 1$.

□

**16.27 Folgerung:** Ist $F/K$ endliche Erweiterung, dann gilt

$$[F : K]_{\text{sep}} = [F^{sa} : K] \quad \text{und} \quad [F : K]_i = [F : F^{sa}].$$

**Beweis:**

$$\begin{aligned}[F:K]_{\text{sep}} &= [F:F^{sa}]_{\text{sep}} \cdot [F^{sa}:K]_{\text{sep}} = [F^{sa}:K]_{\text{sep}} \\ [F:K]_i &= [F:F^{sa}]_i \cdot [F^{sa}:K]_i = [F:F^{sa}]_i\end{aligned}$$

□

# 17 Perfekte Körper

**17.1 Definition:** Ein Körper $K$ heißt *perfekt*, wenn jedes Polynom aus $K[X]$ separabel ist.

**17.2 Satz:** $K$ ist genau dann perfekt, wenn jede algebraische Erweiterung $K \subset F$ separabel ist.

**Beweis:** Sei $K \subset F$ algebraisch, $\alpha \in F$ und $f \in K[X]$ das Minimalpolynom von $\alpha$. Ist $K$ perfekt, so ist $f$, also auch $\alpha$ separabel.

Ist umgekehrt jede Körpererweiterung $K \subset F$ separabel und $f \in K[X]$ irreduzibel, dann gilt für jede Nullstelle $\alpha$ von $f$ in $\overline{K}$, dass $K \subset K(\alpha)$ separabel und damit $f$ separabel ist. □

**17.3 Bezeichnung:** (1) Wir setzen $K^r = \{\alpha^r; \alpha \in K\}$ für $r \geq 0$.

(2) Sei $\text{char}(K) = p > 0$. Dann nennen wir den Körperhomomorphismus

$$\phi : K \to K, \quad \phi(a) = a^p$$

*Frobeniusabbildung.*

**17.4 Satz:** Sei $\text{char}(K) = p > 0$. Dann sind äquivalent

(1) $K$ ist perfekt.

(2) $K = K^p$.

(3) Die Frobeniusabbildung ist ein Isomorphismus.

**Beweis:** (1) $\Rightarrow$ (2): Für $\alpha \in K$ betrachten wir $f = X^p - \alpha \in K[X]$. Für eine Nullstelle $\beta$ von $f$ in einem Zerfällungskörper gilt $\beta^p = \alpha$, so dass

$$f = X^p - \beta^p = (X - \beta)^p.$$

Also ist $\beta$ rein inseparabel über $K$. Da $K$ perfekt ist, ist $\beta$ auch separabel. Aus 16.11 und 16.24 folgt $[K(\beta):K] = [K(\beta):K]_{\text{sep}} = 1$, also $\beta \in K$. Damit ist $\alpha \in K^p$.

(2) $\Leftrightarrow$ (3): Als Körperhomomorphismus ist $\phi$ immer injektiv, und $\phi$ ist genau dann surjektiv, wenn $K = K^p$.

(2) $\Rightarrow$ (1): Sei $f \in K[X]$ irreduzibel, aber nicht separabel. Dann gibt es ein Polynom $g = \sum_{i=0}^{n} a_i X^i \in K[X]$, so dass $f(X) = g(X^p)$ nach 16.4. Da $K = K^p$, ist jedes $a_i$ von der Form $a_i = b_i^p$ mit $b_i \in K$. Es folgt

$$f(X) = \sum_{i=0}^{n} a_i (X^p)^i = \sum_{i=0}^{n} b_i^p (X^i)^p = \left( \sum_{i=0}^{n} b_i X^i \right)^p$$

im Widerspruch zur Irreduzibilität von $f$. □

**17.5 Folgerung:** Ist $K$ endlich oder $\operatorname{char} K = 0$, dann ist $K$ perfekt.

**Beweis:** Ist $\operatorname{char} K = 0$, dann ist $K$ nach 16.6 perfekt. Ist $K$ endlich, $\operatorname{char} K = p > 0$, dann ist die Frobeniusabbildung ein Automorphismus, weil sie injektiv ist. □

**17.6 Satz:** (1) Ist $K \subset F$ algebraisch und $K$ perfekt, dann ist $F$ perfekt.

(2) Ist $K \subset F$ endliche Erweiterung und $F$ perfekt, dann ist $K$ perfekt.

**Beweis:** (1) Sei $F \subset E$ eine algebraische Erweiterung, dann ist $K \subset E$ algebraische Erweiterung. Nach 17.2 ist $K \subset E$ separabel, also auch $F \subset E$. Nach 17.2 ist $F$ perfekt.

(2) Sei $\operatorname{char} K = p > 0$. Sei zunächst $F = K(\alpha)$ und $f = \sum_{i=0}^{n} a_i X^i \in K[X]$ das Minimalpolynom von $\alpha$. Dann gilt

$$0 = \left( \sum_{i=0}^{n} a_i \alpha^i \right)^p = \sum_{i=0}^{n} a_i^p \alpha^{p \cdot i}.$$

Also ist der Grad von $\alpha^p$ über $K^p$ höchstens der Grad von $\alpha$ über $K$:

$$[K^p(\alpha^p) : K^p] \leq [K(\alpha) : K].$$

Da $K^p(\alpha^p) = (K(\alpha))^p = K(\alpha)$, letzteres weil $K(\alpha)$ nach Voraussetzung perfekt ist, folgt

$$[K(\alpha) : K^p] \leq [K(\alpha) : K].$$

Da aber $K^p \subset K$, folgt aus der Gradschachtelungsformel, dass $K = K^p$.

Also ist $K$ perfekt.

Ist $K \subset F$ endliche Erweiterung, gibt es $\alpha_1, \ldots, \alpha_n \in F$, so dass $F = K(\alpha_1, \ldots, \alpha_n)$. Wiederholte Anwendung des vorausgegangenen Arguments liefert die Aussage. □

**17.7 Bemerkung:** Die Endlichkeitsbedingung in 17.6.2 ist notwendig, denn $K \subset \overline{K}$ ist algebraisch und $\overline{K}$ ist perfekt, selbst wenn $K$ nicht perfekt ist.

**17.8 Definition und Satz:** Sei $\operatorname{char} K = p > 0$ und $\overline{K}$ ein algebraischer Abschluss von $K$. Dann ist

$$K^{1/p^k} = \{\alpha \in \overline{K}; \alpha^{p^k} \in K\}$$

ein Unterkörper von $\overline{K}$. Weiter gilt

$$K \subset K^{1/p} \subset K^{1/p^2} \subset \dots$$

Der Unterkörper

$$\operatorname{perf}(K) = \bigcup_{k=1}^{\infty} K^{1/p^k} \subset \overline{K}$$

heißt *perfekter Abschluss* von $K$ in $\overline{K}$.

Der einfache Beweis ist dem Leser überlassen.

**17.9 Satz:** Sei $\operatorname{char} K = p > 0$. Dann ist $\operatorname{perf}(K)$ der kleinste perfekte Unterkörper von $\overline{K}$, der $K$ enthält.

**Beweis:** Sei $\alpha \in \operatorname{perf}(K)$; dann gibt es ein $k \geq 1$, so dass $\alpha^{p^k} \in K$. Sei $\beta \in \overline{K}$ Nullstelle des Polynoms $X^p - \alpha$, also $\beta^p = \alpha$. Dann gilt $\beta^{p^{k+1}} = \alpha^{p^k} \in K$, also ist $\beta \in \operatorname{perf}(K)$ und folglich $(\operatorname{perf}(K))^p = \operatorname{perf}(K)$. Damit ist $\operatorname{perf}(K)$ perfekt. Sei jetzt $K \subset F \subset \overline{K}$ und $F$ perfekt. Sei $\alpha \in \operatorname{perf}(K)$ wie eben, also $\alpha^{p^k} \in K \subset F$. Da $F = F^{p^k}$, gibt es ein $\beta \in F$ mit $\alpha^{p^k} = \beta^{p^k}$. Es folgt

$$0 = (\alpha^{p^k} - \beta^{p^k}) = (\alpha - \beta)^{p^k}.$$

Also $\alpha = \beta$ und somit $\alpha \in F$, so dass $\operatorname{perf}(K) \subset F$. □

# Teil III
# Galoistheorie

## 18 Die Galois-Korrespondenz

**18.1 Definition:** Die *Galois-Gruppe* einer Erweiterung $F/K$, bezeichnet $\mathrm{Gal}(F/K)$, ist die Gruppe der $K$-Automorphismen $F \to F$, d.h. der Automorphismen $\sigma : F \to F$ mit $\sigma(x) = x \ \forall \ x \in K$.

**18.2 Bezeichnung:** (1) $\mathcal{ZW} = \mathcal{ZW}(F/K)$ die Menge der Zwischenkörper $K \subset E \subset F$

(2) $\mathcal{U} = \mathcal{U}(F/K)$ die Menge der Untergruppen von $\mathrm{Gal}(F/K)$.

(3) Ist $L/K$ Erweiterung, dann ist $\mathrm{Hom}_K(F, L)$ die Menge der $K$-Morphismen $F \to L$.

**18.3** Ist $F/K$ algebraisch, dann ist $\mathrm{Gal}(F/K) = \mathrm{Hom}_K(F, E)$ nach 14.16.

Wir definieren die Abbildungen

$$\Pi : \mathcal{ZW} \rightleftarrows \mathcal{U} : \Omega$$

durch $\Pi(E) = \mathrm{Gal}(F/E)$ und $\Omega(H) = F^H$, wobei

$$F^H = \{x \in F; \sigma(x) = x \ \forall \sigma \in H\}$$

der *Fixkörper* von $H$ ist. Wir überlassen dem Leser den Nachweis, dass $F^H$ ein Zwischenkörper $K \subset F^H \subset F$ ist.

**18.4 Bezeichnung:** Das Paar $(\Pi, \Omega)$ heißt *Galois-Korrespondenz* der Erweiterung $F/K$.

Ziel dieses Abschnittes ist die Untersuchung der Galois-Korrespondenz.
Wir definieren partielle Ordnungen auf $\mathcal{ZW}$ bzw. $\mathcal{U}$ durch $A \leq B$, falls $A \subset B$.

**18.5 Satz:** $(\mathcal{ZW}, \leq)$ und $(\mathcal{U}, \leq)$ sind vollständige Verbände, d.h. jede Familie von Elementen hat ein Infinum, nämlich den Durchschnitt aller Elemente, und ein Maximum, nämlich den kleinsten Körper bzw. die kleinste Untergruppe, die jeden Körper bzw. jede Untergruppe der Familie enthält. □

**18.6 Aufgabe:** (1) $\Pi$ und $\Omega$ sind ordnungsumkehrende Abbildungen

(2) Für $E \in \mathcal{ZW}$ gilt

$$E \leq \Omega \circ \Pi(E) \quad \text{und} \quad \Pi(E) = \Pi \circ \Omega \circ \Pi(E)$$

(3) Für $U \in \mathcal{U}$ gilt

$$U \leq \Pi \circ \Omega(U) \quad \text{und} \quad \Omega(U) = \Omega \circ \Pi \circ \Omega(U)$$

**18.7** Die Abbildungen $\Omega \circ \Pi : \mathcal{ZW} \to \mathcal{ZW}$ und $\Pi \circ \Omega : \mathcal{U} \to \mathcal{U}$ sind *Abschlussoperationen*, d.h. ist $cl(E) = \Omega \circ \Pi(E)$ für $E \in \mathcal{ZW}$, dann gilt

(1) $E \leq cl(E)$

(2) $cl(cl(E)) = cl(E)$

(3) $E \leq L \Rightarrow cl(E) \leq cl(L)$

und entsprechend für $cl = \Pi \circ \Omega$.

**18.8 Definition:** $E \in \mathcal{ZW}$ und $U \in \mathcal{U}$ heißen *abgeschlossen*, wenn $cl(E) = \Omega \circ \Pi(E) = E$ bzw. $cl(U) = \Pi \circ \Omega(U) = U$. Die Mengen der abgeschlossenen Elemente werde $Cl(\mathcal{ZW})$ bzw. $Cl(\mathcal{U})$ bezeichnet.

**18.9 Aufgabe:** Zeigen Sie, dass $Cl(\mathcal{ZW})$ und $Cl(\mathcal{U})$ vollständige Verbände sind.

**18.10 Satz:** Sei $F/K$ algebraisch und $K \subset L \subset E \subset F$. Dann gilt

(1) $[\Pi(L) : \Pi(E)] = [\mathrm{Gal}(F/E) : \mathrm{Gal}(F/L)] \leq [E : L]_{\mathrm{sep}} \leq [E : L]$.

(2) Ist $F/K$ normal, gilt Gleichheit für die linke Ungleichung und

$$\psi : \frac{\mathrm{Gal}(F/L)}{\mathrm{Gal}(F/E)} \to \mathrm{Hom}_L(E, F), \quad \overline{\sigma} \mapsto \sigma|E$$

ist bijektiv.

(3) Ist $K \subset F$ normal und separabel, gilt in (1) überall Gleichheit.

**Beweis:** (1) Für $\sigma, \tau \in \mathrm{Gal}(F/L)$ gilt

$$\begin{aligned} \sigma|E = \tau|E \quad &\Longleftrightarrow \quad \tau^{-1} \circ \sigma(\alpha) = \alpha \quad \forall \alpha \in E \iff \tau^{-1} \circ \sigma \in \mathrm{Gal}(F/E) \\ &\Longleftrightarrow \quad \sigma \in \tau \circ \mathrm{Gal}(F/E). \end{aligned}$$

Also gilt $\psi(\sigma) = \psi(\tau)$ genau dann, wenn $\sigma$ und $\tau$ in derselben Linksnebenklasse von $\mathrm{Gal}(F/E)$ liegen. Damit induziert $\psi$ eine Bijektion der Linksnebenklassen von $\mathrm{Gal}(F/E)$ in $\mathrm{Gal}(F/L)$ und $\mathrm{Bild}(\psi)$. Da nun

$$\mathrm{Bild}(\psi) \subset \mathrm{Hom}_L(E,F) \subset \mathrm{Hom}_L(E,\overline{F}),$$

erhalten wir

$$[\mathrm{Gal}(F/L) : \mathrm{Gal}(F/E)] = |\mathrm{Bild}(\psi)| \leq |\mathrm{Hom}_L(E,\overline{F})| = [E:L]_{\mathrm{sep}}$$

(2) Sei jetzt $F/K$ normal. Dann ist nach 15.5 auch $F/L$ normal. Nach 14.17 kann jedes $\sigma \in \mathrm{Hom}_L(E,F)$ zu $\overline{\sigma} \in \mathrm{Hom}_L(E,\overline{F})$ erweitert werden. Nach 15.1 ist $\overline{\sigma} \in \mathrm{Gal}(F/L)$, da $F/L$ normal ist. Da $\sigma(E) \subset F$, ist $\sigma \in \mathrm{Hom}_L(E,F)$. Wir erhalten

$$\mathrm{Hom}_L(E,\overline{F}) = \mathrm{Hom}_L(E,F).$$

Da sich also jedes $\sigma \in \mathrm{Hom}_L(E,F)$ zu einem $\overline{\sigma} \in \mathrm{Gal}(F/L)$ erweitern lässt und $\sigma = \psi(\overline{\sigma})$ ist, folgt $\mathrm{Hom}_L(E,F) \subset \mathrm{Bild}(\psi)$. Es folgt

$$\mathrm{Bild}(\psi) = \mathrm{Hom}_L(E,F) = \mathrm{Hom}_L(E,\overline{F})$$

und damit $[\mathrm{Gal}(F/L) : \mathrm{Gal}(F/E)] = [E:L]_{\mathrm{sep}}$.

(3) folgt aus 16.12, da auch $E \subset L$ separabel ist (ist $E \subset L$ nicht endlich, gilt auch $[E:L]_{\mathrm{sep}} = \infty$, so dass nichts zu zeigen ist.). □

Wir wollen das entsprechende Resultat für $\Omega$ beweisen. Dazu benötigen wir noch

**18.11 Lemma von Artin:** Sei $H < \mathrm{Gal}(F/K)$ Untergruppe. Für $\alpha \in F$ sei

$$\widehat{\alpha} : H \to F, \quad \sigma \mapsto \sigma(\alpha).$$

Dann ist für $\alpha_1, \ldots, \alpha_n \in F$ äquivalent.

(1) $\alpha_1, \ldots, \alpha_n$ sind linear unabhängig über $F^H$.

(2) $\widehat{\alpha}_1, \ldots, \widehat{\alpha}_n$ sind linear unabhängig im $F$-Vektorraum $\mathrm{Abb}(H,F)$.

**Beweis:** (2) $\Rightarrow$ (1): Sei $\sum_{i=1}^n c_i\alpha_i = 0$ mit $c_1, \ldots, c_n \in F^H$. Dann gilt für $\sigma \in H$

$$0 = \sigma\left(\sum_i c_i\alpha_i\right) = \sum_i c_i \cdot \sigma(\alpha_i) = \sum_i c_i\widehat{\alpha}_i(\sigma)$$

Es folgt $\Sigma_i c_i\widehat{\alpha}_i = 0$ und somit $c_i = 0$ für $1 \leq i \leq n$.

(1) $\Rightarrow$ (2): Sei $\sum_i x_i \widehat{\alpha}_i = 0$ mit $x_i \in F$. Besitzt diese Gleichung eine nichttriviale Lösung, wählen wir unter diesen eine Lösung $(c_1, \ldots, c_n)$ mit maximaler Anzahl von Nullen. Durch Umordnen der $\alpha_i$ dürfen wir annehmen, dass $c_1 \neq 0$, und durch Multiplikation mit einer Konstanten, dass $c_1 = 1$. Wir erhalten die Gleichung

$$\widehat{\alpha}_1 + c_2 \cdot \widehat{\alpha}_2 + \ldots + c_n \cdot \widehat{\alpha}_n = 0 \qquad (A)$$

$$\sigma(\alpha_1) + c_2 \cdot \sigma(\alpha_2) + \ldots + c_n \cdot \sigma(\alpha_n) = 0 \quad \forall \sigma \in H \qquad (B)$$

Für $\sigma = \mathrm{id}$ gilt somit

$$\alpha_1 + c_2 \cdot \alpha_2 + \ldots + c_n \cdot \alpha_n = 0$$

Da $\alpha_1, \ldots, \alpha_n$ über $F^H$ linear unabhängig sind, gibt es ein $c_i \neq 0$, das nicht in $F^H$ liegt. Durch Umordnen dürfen wir annehmen, dass dies $c_n$ ist. Wenden wir $\tau \in H$ auf die Gleichung (B) an, erhalten wir

$$\tau\sigma(\alpha_1) + \tau(c_2) \cdot \tau\sigma(\alpha_2) + \ldots + \tau(c_n)\tau\sigma(\alpha_n) = 0 \quad \forall \sigma \in H$$

Da Linkstranslation mit $\tau$ bijektiv ist, folgt

$$\lambda(\alpha_1) + \tau(c_2) \cdot \lambda(c_2) + \ldots + \tau(c_n) \cdot \lambda(\alpha_n) = 0 \quad \forall \lambda \in H$$

und damit

$$\widehat{\alpha}_1 + \tau(c_2)\widehat{\alpha}_2 + \ldots + \tau(c_n) \cdot \widehat{\alpha}_n = 0 \qquad (C)$$

Da $c_n \notin F^H$, gibt es ein $\tau \in H$, so dass $\tau(c_n) \neq c_n$. Ziehen wir (B) von (C) ab, erhalten wir

$$(\tau(c_2) - c_2) \cdot \widehat{\alpha}_2 + \ldots + (\tau(c_n) - c_n) \cdot \widehat{\alpha}_n = 0.$$

Wir erhalten eine nicht trivale Lösung der Ausgangsgleichung mit mehr Nullen ($\tau$ erhält die 0) im Widerspruch zur Maximalität. □

**18.12 Satz:** Sei $F/K$ algebraisch und $G < H < \mathrm{Gal}(F/K)$ Untergruppen. Dann gilt $[\Omega(G) : \Omega(H)] = [F^G : F^H] \leq [H : G]$.

**Beweis:** Ist $[H : G] = \infty$, ist nichts zu zeigen. Sei also $[H : G] = r < \infty$. Seien $\sigma_1, \ldots, \sigma_r$ Repräsentanten der $r$ Linksnebenklassen von $G$ in $H$. Seien $\alpha_1, \ldots, \alpha_n \in F^G$ linear unabhängig über $F^H$, und wir wollen annehmen, dass $n > r$. Dann hat das Gleichungssystem

$$\begin{aligned} \sigma_1(\alpha_1) \cdot x_1 + \ldots + \sigma_1(\alpha_n) \cdot x_n &= 0 \\ &\vdots \\ \sigma_r(\alpha_1) \cdot x_1 + \ldots + \sigma_r(\alpha_n) \cdot x_n &= 0 \end{aligned}$$

eine nicht-triviale Lösung $(c_1, \ldots, c_n) \in F^n$, also

$$c_1 \cdot \sigma_i(\alpha_1) + \ldots + c_n \cdot \sigma_i(\alpha_n) = 0 \quad \text{für } 1 \leq i \leq r.$$

Jedes $\tau \in H$ ist von der Form $\sigma_i \circ \rho$ mit $\rho \in G$. Da $\alpha_i \in F^G$, gilt $\rho(\alpha_i) = \alpha_i$. Es folgt

$$\sum_{j=1}^{n} c_j \cdot \tau(\alpha_j) = \sum_{j=1}^{n} c_j \cdot (\sigma_i \circ \rho)(\alpha_j) = \sum_{j=1}^{n} c_j \cdot \sigma_i(\alpha_j) = 0$$

oder, in der Bezeichnungsweise von 18.11,

$$c_1 \cdot \widehat{\alpha}_1(\tau) + \ldots + c_n \cdot \widehat{\alpha}_n(\tau) = 0 \quad \forall \tau \in H.$$

Nach 18.11 sind aber $\widehat{\alpha}_1, \ldots, \widehat{\alpha}_n \in \mathrm{Abb}(H, F)$ linear unabhängig über $F$, ein Widerspruch! □

**18.13 Folgerung:** Sei $F/K$ algebraisch. Dann sind

$$\Pi : Cl(\mathcal{ZW}) \rightleftarrows Cl(\mathcal{U}) : \Omega$$

ordnungsumkehrende Bijektionen, die zueinander invers sind. Weiter gilt für $L \leq E$ in $Cl(\mathcal{ZW})$ und $G \leq H$ in $Cl(\mathcal{U})$

$$\begin{aligned} [\mathrm{Gal}(F/L) : \mathrm{Gal}(F/E)] &= [E : L] \\ [F^G : F^H] &= [H : G] \end{aligned}$$

**Beweis:** Nach Definition gilt $\Omega \circ \Pi(E) = E$ und $\Pi \circ \Omega(G) = G$ für abgeschlossenes $E$ und $G$. Für $L \leq E$ in $Cl(\mathcal{ZW})$ gilt nach 18.10 und 18.12

$$[E : L] = [\Omega \circ \Pi(E) : \Omega \circ \Pi(L)] \leq [\Pi(L) : \Pi(E)] \leq [E : L].$$

Also $[E : L] = [\Pi(L) : \Pi(E)] = [\mathrm{Gal}(F/L) : \mathrm{Gal}(F/E)]$. Genauso zeigt man die zweite Gleichung. □

**18.14 Aufgabe:** Zeigen Sie für $E, L \in Cl(\mathcal{ZW}(F/K))$ und $G, H \in Cl(\mathcal{U}(F, K))$

(1)
$$\begin{aligned} \mathrm{Gal}(F/E \cap L) &= \mathrm{Sup}(\mathrm{Gal}(F/E), \mathrm{Gal}(F/L)) \\ \mathrm{Gal}(F/\mathrm{Sup}(E, L)) &= \mathrm{Gal}(F/E) \cap \mathrm{Gal}(F/L) \end{aligned}$$

(2)
$$\begin{aligned} F^{G \cap H} &= \mathrm{Sup}(F^G, F^H) \\ F^{\mathrm{Sup}(G,H)} &= F^G \cap F^H \end{aligned}$$

wobei die Suprema in $Cl(\mathcal{ZW})$ bzw. $Cl(\mathcal{U})$ gebildet sind.

(3) Sei $L \subset L' \subset F$ und $L'/L$ endlich. Dann ist $L'$ abgeschlossen.
Sei $U < \mathrm{Gal}(F/K)$ eine endliche Untergruppe, dann ist $U$ abgeschlossen.

Folgerung 18.13 wirft die Frage auf, welche Zwischenkörper von $F/K$ und welche Untergruppen von $\mathrm{Gal}(F/K)$ abgeschlossen sind. Damit beschäftigen wir uns im nächsten Abschnitt.

# 19 Galois-Erweiterungen

**19.1 Definition:** Eine *Galois-Erweiterung* ist eine normale, separable Erweiterung.

Aus den Ergebnissen der Paragraphen 15 und 16 folgt

**19.2 Satz:** (1) Sei $K \subset E \subset F$. Ist $K \subset F$ Galois, dann auch $E \subset F$.

(2) Gegeben sei ein Diagramm von Körpern

$$\begin{array}{ccc} K & \subset & E \\ \cap & & \cap \\ F & \subset & L \end{array}$$

Ist $K \subset E$ Galois, dann auch $F \subset E \vee F$.

(3) Gegeben seien Zwichenkörper $K \subset E_i \subset F$, $i \in I$. Ist jedes $K \subset E_i$ Galois, dann sind auch $K \subset \bigvee_i E_i$ und $K \subset \bigcap_i E_i$ Galois (s. 15.5).

**19.3 Satz:** Sei $F/K$ algebraisch.

(1) Ein Zwischenkörper $E$ ist genau dann abgeschlossen, wenn $E \subset F$ Galois ist.

(2) Ist $L$ in $K \subset L \subset E \subset F$ abgeschlossen, dann ist auch $E$ abgeschlossen.

(3) Äquivalent sind

(i) $K$ ist abgeschlossen.

(ii) $K \subset F$ ist Galois.

(iii) $\mathcal{ZW}(F/K) = Cl(\mathcal{ZW}(F/K))$.

Für den Beweis von Teil (1) zeigen wir zunächst:

**19.4 Satz:** Sei $F/K$ normal und $G = \mathrm{Gal}(F/K)$. Dann gilt

(1) $F^G = K^{ia}$

(2) In $K \subset K^{ia} \subset F$ ist $K \subset K^{ia}$ rein inseparabel und $K^{ia} \subset F$ separabel.

**Beweis:** (1) Sei $\alpha \in F^G$ und $f \in K[X]$ sein Minimalpolynom. Sei $\beta \in \overline{K}$ eine Nullstelle von $f$. Nach 14.17 gibt es eine Erweiterung $\sigma : F \to \overline{K}$ der Inklusion $K \subset \overline{K}$, so dass $\sigma(\alpha) = \beta$. Wir dürfen annehmen, dass $F \subset \overline{K}$. Nach 15.1 ist $\sigma \in \mathrm{Gal}(F/K)$, so dass $\sigma(\alpha) = \alpha$, also $\alpha = \beta$. Damit hat $f$ nur eine Nullstelle, so dass $\alpha$ rein inseparabel ist. Es folgt $\alpha \in K^{ia}$.

Ist umgekehrt $\alpha \in K^{ia}$, dann gilt $\sigma(\alpha) = \alpha$ für $\sigma \in G$, da $\sigma$ die Nullstellen des Minimalpolynoms von $\alpha$ permutiert (14.15). Also ist $\alpha \in F^G$.

(2) Nach Definition ist $K \subset K^{ia}$ rein inseparabel. Sei $\alpha \in F$ und $f$ sei Minimalpolynom über $K^{ia} = F^G$. Seien $\beta_1, \ldots, \beta_n$ die **verschiedenen** Nullstellen von $f$ in $F$ und $g = \prod_{i=1}^{n}(X - \beta_i) \in F[X]$. Da $\sigma \in G$ die $\beta_i$ permutiert, folgt $g^\sigma = g$. Also liegen die Koeffizienten von $g$ in $F^G$. Da $\operatorname{grad} g \leq \operatorname{grad} f$ und $g(\alpha) = 0$, folgt $f = g$, d.h. $f$ ist separabel. □

**Beweis von 19.3:** Ist $E \subset F$ normal und separabel, gilt mit $G = \mathrm{Gal}(F/E)$ nach 19.4

$$\Omega \circ \Pi(E) = F^G = E^{ia} = E,$$

so dass $E$ abgeschlossen ist.

Sei umgekehrt $E$ abgeschlossen, sei $\alpha \in F$ mit Minimalpolynom $f \in E[X]$ vom Grad $n$. Da $E \subset E(\alpha)$ endlich und $E$ abgeschlossen ist, ist $E(\alpha)$ nach 18.14 abgeschlossen, so dass nach 18.13

$$n = [E(\alpha) : E] = [\mathrm{Gal}(F/E) : \mathrm{Gal}(F/E(\alpha))].$$

Seien $\sigma_1, \ldots, \sigma_n$ Repräsentanten der Linksnebenklassen von $\mathrm{Gal}(F/E(\alpha))$ in $\mathrm{Gal}(F/E)$.

**Behauptung:** $\tau \in \sigma_i \circ \mathrm{Gal}(F/E(\alpha)) \iff \tau(\alpha) = \sigma_i(\alpha)$.

**Beweis:** Sei $\tau = \sigma_i \circ \rho$ mit $\rho \in \mathrm{Gal}(F/E(\alpha))$. Dann gilt $\tau(\alpha) = \sigma_i(\rho(\alpha)) = \sigma_i(\alpha)$, weil $\alpha \in E(\alpha)$ und $E(\alpha)$ der Fixkörper von $\mathrm{Gal}(F/E(\alpha)$ ist.

Sei umgekehrt $\tau(\alpha) = \sigma_i(\alpha)$ und $\rho = \sigma_i^{-1} \circ \tau$, so dass $\rho(\alpha) = \alpha$. Jedes $x \in E(\alpha)$ ist von der Form $x = x_0 + x_1\alpha + \ldots + x_{n-1}\alpha^{n-1}$ mit $x_i \in E$.

Da $\rho \in \mathrm{Gal}(F/E)$ folgt

$$\rho(x) = \sum_{j=0}^{n-1} \rho(x_j) \cdot \rho(\alpha)^j = \sum_{j=0}^{n-1} x_j \cdot \alpha^j = x$$

Also ist $\rho \in \mathrm{Gal}(F/E(\alpha))$ und somit $\tau = \sigma_i \circ \rho \in \sigma_i \circ \mathrm{Gal}(F/E(\alpha))$.

Es folgt, die Bahn von $\alpha$ unter der Operation von $\mathrm{Gal}(F/E)$ hat genau $n$ Elemente. Da die Galoisgruppe die Nullstellen von $f$ permutiert, müssen das die Nullstellen von $f$ sein, die somit alle verschieden sind. Also ist $f$ separabel und hat alle Nullstellen in $F$. Es folgt $E \subset F$ ist separabel und normal.

Das beweist (1) und die Äquivalenz von (3(i)) und (3(ii)).

Die Äquivalenz aller Aussagen von (3) folgt, weil $K \subset F$ genau dann Galois ist, wenn $E \subset F$ Galois ist für alle $K \subset E \subset F$ nach 19.2.

Genauso folgt (2) aus (1).

**19.5 Bemerkung:** (1) Ist $F/K$ algebraisch, dann ist $F$ abgeschlossen, da $F = F^{\{\mathrm{id}\}}$ und $\mathrm{Gal}(F/F) = \{\mathrm{id}\}$.

(2) Ist $E$ ein abgeschlossener Zwischenkörper von $F/K$, so gilt

$$[F : E] = [\mathrm{Gal}(F/E) : \mathrm{Gal}(F/F)] = |\mathrm{Gal}(F/E)|.$$

Ist $F/K$ endlich, gilt auch die Umkehrung von 19.5.2: Wir zeigen

**19.6 Satz:** Für eine **endliche** Erweiterung $F/K$ gilt

(1) Ein Zwischenkörper $E$ ist genau dann abgeschlossen, wenn

$$[F : E] = |\mathrm{Gal}(F/E)|.$$

(2) Äquivalent sind

(i) $F/K$ ist Galois.

(ii) $K$ ist abgeschlossen.

(iii) Alle Zwischenkörper von $F/K$ sind abgeschlossen.

(iv) $[F : E] = |\mathrm{Gal}(F/E)|$ für alle Zwischenkörper $E$.

(v) $[F : K] = |\mathrm{Gal}(F/K)|$

**Beweis:** (1) Wir müssen die Umkehrung von 19.5.2 zeigen. Sei $G = \mathrm{Gal}(F/E)$. Aus $[F : E] = |\mathrm{Gal}(F/E)|$ folgt mit 18.10 und 18.12

$$\begin{aligned} [F : E] &= |\mathrm{Gal}(F/E)| = |\mathrm{Gal}(F/E) : \mathrm{Gal}(F/F)| \\ &\leq [F^{\{\mathrm{id}\}} : F^G] \leq [F : E], \end{aligned}$$

weil $\mathrm{Gal}(F/F) = \{\mathrm{id}\}$ und $E \subset F^G$. Da alles endlich ist, folgt $E = F^G$, d.h. $E$ ist abgeschlossen.

(2) folgt aus (1) und 19.3. □

**19.7 Folgerung:** Ist $F/K$ endlich, sind alle Untergruppen von $\mathrm{Gal}(F/K)$ abgeschlossen, und ein Zwischenkörper $E$ ist genau dann abgeschlossen, wenn $E \subset F$ Galois ist. Ist insbesondere $K \subset F$ Galois, sind alle Zwischenkörper abgeschlossen.

**Beweis:** Es bleibt nur der Gruppenteil zu zeigen,. $\{\mathrm{id}\} = \mathrm{Gal}(F/F)$ ist abgeschlossen. Da $\mathrm{Gal}(F/K)$ endlich ist, ist jede Untergruppe nach 18.14 abgeschlossen. □

**19.8 Bemerkung:** Ist $K \subset F$ beliebige Galois-Erweiterung, dann ist nicht jede Untergruppe von $\mathrm{Gal}(F/K)$ abgeschlossen.

**19.9 Aufgabe:** Sei $F$ ein Körper, $H$ eine Untergruppe von $\mathrm{Aut}(F)$. Zeigen Sie:

(1) $F^H \subset F$ ist Galois.

(2) Ist $H$ abgeschlossen bzgl. der Erweiterung $F^H \subset F$, dann gilt $H = \mathrm{Gal}(F/F^H)$.

Ist $K \subset E \subset F$ und $F/K$ normal, dann ist $F/E$ normal, aber $E/K$ braucht nicht normal zu sein. Die Galois-Gruppen geben Auskunft, wann auch $K \subset E$ normal ist.

**19.10 Satz:** Sei $K \subset E \subset F$ gegeben.

(1) $K \subset E$ normal $\Rightarrow \mathrm{Gal}(F/E) \lhd \mathrm{Gal}(F/K)$.

(2) Ist $K \subset F$ normal, $E \subset F$ Galois und $\mathrm{Gal}(F/E) \lhd \mathrm{Gal}(F/K)$, dann ist auch $K \subset E$ normal.

(3) Ist $F/K$ Galois, dann gilt

$$K \subset E \text{ normal} \iff \mathrm{Gal}(F/E) \lhd \mathrm{Gal}(F/K)$$

(4) Sind $E/K$ und $F/K$ normal, dann ist

$$\psi : \mathrm{Gal}(F/K) \to \mathrm{Gal}(E/K), \quad \sigma \mapsto \sigma|E$$

ein Epimorphismus mit Kern $\mathrm{Gal}(F/E)$, so dass

$$\mathrm{Gal}(E/K) \cong \frac{\mathrm{Gal}(F/K)}{\mathrm{Gal}(F/E)}.$$

**Beweis:** (1) Sei $\tau \in \mathrm{Gal}(F/K)$ und $\sigma \in \mathrm{Gal}(F/E)$. Nach 15.1 definiert $\tau$ eine Automorphismus von $E$, so dass $\tau(E) \subset E$. Es folgt $\tau^{-1} \circ \sigma \circ \tau(x) = x$ für alle $x \in E$, also $\tau^{-1} \circ \sigma \circ \tau \in \mathrm{Gal}(F/E)$, d.h. $\mathrm{Gal}(F/E) \lhd \mathrm{Gal}(F/K$.

(2) Sei $\alpha \in E$ und $f \in K[X]$ sein Minimalpolynom. Sei $\beta \in \overline{F}$ eine weitere Nullstelle von $f$. Nach 14.17 gibt es einen $K$-Morphismus $\sigma : F \to \overline{F}$ mit $\sigma(\alpha) = \beta$. Da $F/K$ normal ist, ist $\sigma \in \mathrm{Gal}(F/K)$ nach 15.1. Ist nun $\tau \in \mathrm{Gal}(F/E)$, gilt $\sigma^{-1} \circ \tau \circ \sigma = \tau' \in \mathrm{Gal}(F/E)$. Es folgt

$$\tau(\beta) = \tau \circ \sigma(\alpha) = \sigma \circ \tau'(\alpha) = \sigma(\alpha) = \beta.$$

Damit liegen die Nullstellen von $f$ im Fixkörper von $\mathrm{Gal}(F/E)$. Da $E \subset F$ Galois ist, ist $E$ abgeschlossen (19.3), also ist $E$ der Fixkörper von $\mathrm{Gal}(F/E)$, d.h. $f$ zerfällt in $E$. Damit ist $K \subset E$ normal.

(3) folgt aus (1) und (2), denn ist $F/K$ Galois, dann auch $F/E$ (19.2).

(4) Sei $\sigma \in \mathrm{Gal}(F/K)$. Da $E/K$ normal ist, ist $\sigma|E \in \mathrm{Gal}(E/K)$ nach 15.1, so dass $\psi$, wie angegeben, definiert ist. Offensichtlich ist $\psi$ ein Homomorphismus. $\psi$ ist surjektiv: Sei $\tau \in \mathrm{Gal}(E/K)$. Nach 14.17 kann

$$E \xrightarrow{\tau} E \hookrightarrow \overline{F}$$

zu einem $K$-Morphismus $\sigma : F \to \overline{F}$ erweitert werden. Da $F/K$ normal ist, ist $\sigma \in \mathrm{Gal}(F/K)$, und $\psi(\sigma) = \tau$. Weiter gilt

$$\sigma \in \mathrm{Kern}\,\psi \iff \sigma|E = \mathrm{id} \iff \sigma \in \mathrm{Gal}(F/E).$$

□

**19.11 Folgerung:** Sei $K \subset F$ endliche Galois-Erweiterung mit Galois-Gruppe $G$. Seien $U, V < G$ Untergruppen, so dass $U \lhd V$. Dann ist $F^V \subset F^U$ Galois und $\mathrm{Gal}(F^U/F^V) \cong V/U$.

**Beweis:** Nach 19.3 sind $F^U \subset F$ und $F^V \subset F$ Galois mit Galois-Gruppen $U$ bzw. $V$, weil $U$ und $V$ als endliche Untergruppen von $G$ abgeschlossen sind. Da $U \lhd V$, ist $F^V \subset F^U$ Galois mit Galois-Gruppe $\mathrm{Gal}(F^U/F^V) \cong V|U$. □

**19.12 Definition:** Sei $K \subset F$ Galois-Erweiterung und $K \subset E \subset F$ ein Zwischenkörper. Der *Galois-Abschluss* $\widetilde{E}$ von $E$ in $F$ ist der kleinste Unterkörper von $F$, der $E$ enthält und für den $K \subset \widetilde{E}$ Galois ist.

Da $K \subset F$ Galois ist, existiert $\widetilde{E}$ nach 19.2 immer:

$$\widetilde{E} = \bigcap \{L; E \subset L \subset F,\ K \subset L \text{ Galois}\}.$$

Nach 19.10 ist $K \subset L$ genau dann Galois, wenn $\mathrm{Gal}(F/L) \lhd \mathrm{Gal}(F/K)$. Sei $H = \mathrm{Gal}(F/E)$ und $G = \mathrm{Gal}(F/K)$. Nach Aufgabe 18.14 ist $\mathrm{Gal}(F/\widetilde{E})$ der größte abgeschlossene Normalteiler von $G$, der in $H$ enthalten ist.

**19.13 Aufgabe:** Sei $H$ Untergruppe der Gruppe $G$. Dann ist $\bigcap_{g\in G} gHg^{-1}$ der größte Normalteiler von $G$, der in $H$ enthalten ist.

Ist $K \subset F$ endlich, sind alle Untergruppen von $\mathrm{Gal}(F/K)$ abgeschlossen, und wir erhalten

**19.14 Satz:** Ist $K \subset F$ endliche Galois-Erweiterung mit Galois-Gruppe $G = \{\sigma_1, \sigma_2, \ldots, \sigma_n\}$ und ist $K \subset E \subset F$ ein Zwischenkörper, dann ist

$$\widetilde{E} = \bigvee_{i=1}^{n} \sigma_i(E) \subset F$$

der Galois-Abschluss von $E$ in $F$.
Ist insbesondere $E = K[\alpha_1, \ldots, \alpha_k]$, dann ist

$$\widetilde{E} = K[A]$$

mit $A = \{\sigma_i(\alpha_j);\ i = 1, \ldots, n;\ j = 1, \ldots, k\}$.

**Beweis:** Sei $H = \mathrm{Gal}(F/E)$. Dann gilt $F^H = E$. Weiter gilt $\mathrm{Gal}(F/\sigma(E)) = \sigma \cdot H \cdot \sigma^{-1}$, denn $\sigma \cdot H \cdot \sigma^{-1} \subset \mathrm{Gal}(F/\sigma(E))$ und

$$|\mathrm{Gal}(F/\sigma(E))| = [F : \sigma(E)] = [F : E] = |H| = |\sigma \cdot H \cdot \sigma^{-1}|.$$

Sei $N = \bigcap_{i=1}^{n} \sigma_i \cdot H \cdot \sigma_i^{-1}$, dann ist

$$\widetilde{E} = F^N = \bigvee_{i=1}^{n} F^{\sigma_i H \sigma_i^{-1}} = \bigvee_{i=1}^{n} \sigma_i(E),$$

weil im endlichen Fall alle Untergruppen von $G$ und alle Zwischenkörper abgeschlossen sind. □

# 20 Die Galois-Gruppe eines Polynoms

**20.1 Definition:** Sei $f \in K[X]$. Die *Galois-Gruppe* $\mathrm{Gal}_K(f)$ von $f$ ist definiert als

$$\mathrm{Gal}_K(f) = \mathrm{Gal}(\mathrm{Zer}(f)/K).$$

Sei

$$f = g_1^{r_1} \cdot \ldots \cdot g_n^{r_n}$$

eine Faktorisierung von $f$ in Potenzen verschiedener irreduzibler Polynome in $K[X]$, dann ist $\mathrm{Zer}(f)$ auch Zerfällungskörper von

$$g = g_1 \cdot g_2 \cdot \ldots \cdot g_n.$$

**20.2** $K \subset \mathrm{Zer}(f)$ ist genau dann separabel und damit Galois, wenn jedes $g_i$ separabel ist. Ist insbesondere $f$ separabel, dann ist $K \subset \mathrm{Zer}(f)$ endliche Galois-Erweiterung.

Sind $\alpha_1, \ldots, \alpha_k \in \mathrm{Zer}(f)$ die Nullstellen von $f$, gilt $\mathrm{Zer}(f) = K(\alpha_1, \ldots, \alpha_k)$. Damit ist $\sigma \in \mathrm{Gal}_K(f)$ eindeutig seine Permutation der Nullstellen festgelegt. Wir erhalten

**20.3** Die Abbildung

$$\varphi : \mathrm{Gal}_K(f) \to \Sigma_k, \quad k = \text{Anzahl der verschiedenen Nullstellen von } f$$

die $\sigma \in \mathrm{Gal}_K(f)$ die Permutation der Nullstellen zuordnet, ist ein Monomorphismus von Gruppen ($\varphi$ hängt von der Anordnung der Nullstellen ab).

**20.4** Sei $f = p \cdot q \in K[X]$, $\operatorname{grad} p > 0$. Dann gilt $K \subset \mathrm{Zer}(p) \subset \mathrm{Zer}(f)$. Da $\mathrm{Zer}(f)/K$ und $\mathrm{Zer}(p)/K$ nach 15.1 normal sind, erhalten wir aus 19.10.4

$$\begin{aligned} \mathrm{Gal}_{\mathrm{Zer}(p)}(f) &\lhd \mathrm{Gal}_K(f) \\ \mathrm{Gal}_K(p) &\cong \frac{\mathrm{Gal}_K(f)}{\mathrm{Gal}_{\mathrm{Zer}(p)}(f)} \end{aligned}$$

Hat $f \in K[X]$ $n$ verschiedene Nullstellen, ist $\mathrm{Gal}_K(f)$ eine Untergruppe von $\Sigma_n$. Wir wollen jetzt untersuchen, wann $\mathrm{Gal}_K(f)$ bereits in $A_n$ liegt. Dabei hilft die Diskriminante.

$f \in K[X]$ habe die Nullstellen $\alpha_1, \ldots, \alpha_n$ in $\mathrm{Zer}(f)$, aufgelistet in ihrer Vielfachheit.

**20.5 Bezeichnung:** $\triangle(f) = \prod_{i<j}(\alpha_i - \alpha_j)$. Dann heißt

$$D(f) = \triangle(f)^2 = \prod_{i<j}(\alpha_i - \alpha_j)^2$$

*Diskriminante von* $f$.

**20.6**
$$\begin{aligned} D(f) \neq 0 &\iff f \text{ hat nur einfach Nullstellen} \\ &\iff f \text{ ist separabel und hat nur einfache Faktoren in seiner Primfaktorzerlegung} \\ &\Rightarrow K \subset \mathrm{Zer}(f) \text{ ist endliche Galois-Erweiterung} \end{aligned}$$

Wir wollen annehmen, dass $D(f) \neq 0$. Dann ist $f$ separabel und $K \subset \mathrm{Zer}(f)$ Galois. Da $\sigma \in \mathrm{Gal}_K(f)$ die Nullstellen von $f$ permutiert, erhalten wir

$$\sigma(\triangle(f)) = \operatorname{sign}\sigma \cdot \triangle(f).$$

Es folgt

$$\sigma(D(f)) = D(f),$$

so dass $D(f) \in K$. **1. Fall:** $\mathrm{char}(K) = 2$.

Dann ist $\sigma(\triangle(f)) = \triangle(f)$ für alle $\sigma \in \mathrm{Gal}_K(f)$, so dass $\triangle(f)$ im Fixkörper $K$ von $\mathrm{Gal}_K(f)$ liegt.

**2. Fall:** $\mathrm{char}(K) \neq 2$

(i) Falls $\triangle(f) \in K$, gilt $\sigma(\triangle(f)) = \triangle(f)$ für alle $\sigma \in \mathrm{Gal}_K(f)$. Damit muss $\sigma$ eine gerade Permutation sein.

(ii) Falls $\triangle(f) \notin K$, muss $\mathrm{Gal}_K(f)$ ungerade Permutationen enthalten. Aus der nächsten Aufgabe folgt, dass $|\mathrm{Gal}_K(f)|$ gerade ist und die Hälfte seiner Elemente gerade Permutationen sind. Wir identifizieren $\mathrm{Gal}_K(f)$ mit seinem Bild in $\Sigma_n$ unter $\varphi$. Ist $G = A_n \cap \mathrm{Gal}_K(f)$, dann ist $F^G \subset \mathrm{Zer}(f)$ Galois mit Galois-Gruppe $G$ nach 19.3 und 19.7. Wir erhalten nach 19.6

$$[\mathrm{Zer}(f) : F^G] = |G| = \frac{1}{2}|\mathrm{Gal}_K(f)| = \frac{1}{2}[\mathrm{Zer}(f) : K].$$

Es folgt $[F^G : K] = 2$. Da $D(f)$ im Fixkörper $K$ von $\mathrm{Gal}_K(f)$ ist, ist $X^2 - D(f) \in K[X]$ das Minimalpolynom von $\triangle(f)$, so dass $[K(\triangle(f)) : K] = 2$. Da $K(\triangle(f)) \subset F^G$, folgt $F^G = K(\triangle(f))$. Damit ist $K(\triangle(f))$ der Fixkörper der geraden Permutationen in $\mathrm{Gal}_K(f)$.

**20.7 Aufgabe:** Sei $U < \Sigma_n$ eine Untergruppe, die eine ungerade Permutation enthält. Dann ist $|U|$ gerade und $|U \cap A_n| = \frac{1}{2}|U|$.

Wir fassen zusammen

**20.8 Satz:** Für $f \in K[X]$ mit $\mathrm{grad}(f) = n$ gilt

(1) $D(f) = 0 \iff f$ hat Mehrfachnullstellen.

(2) $D(f) \neq 0$ und $\mathrm{char}(K) = 2 \Rightarrow \triangle(f) \in K$, aber $\mathrm{Gal}_K(f)$ braucht nicht Untergruppe von $A_n$ zu sein.

(3) $D(f) \neq 0$ und $\mathrm{char}(K) \neq 2$. Dann gilt

   (i) Hat $D(f)$ eine Quadratwurzel in $K$, dann ist $\mathrm{Gal}_K(f)$ vermöge $\varphi$ eine Untergruppe von $A_n$.

   (ii) Hat $D(f)$ keine Quadratwurzel in $K$, dann enthält $\mathrm{Gal}_K(f)$ je zur Hälfte gerade und ungerade Permutationen der Nullstellen von $f$. Weiterhin ist $K(\sqrt{D(f)})$ der Fixkörper von $\mathrm{Gal}_K(f) \cap A_n$.

**20.9 Bemerkung:** Sei $\operatorname{char} K = 2$ und seien $t_1, \ldots, t_n$ transzendent über $K$, so dass jedes $t_i$ transzendent über $K(t_1, \ldots, t_{i-1}, t_{i+1}, \ldots, t_n)$ ist. Sei

$$f = \prod_{i=1}^{n} (X - t_i).$$

Dann ist $\operatorname{Gal}_K(f) = \Sigma_n$.

Auf den Beweis verzichten wir aus Zeitgründen.

Zum Abschluss dieses Abschnitts wollen wir die Galois-Gruppen quadratischer Polynome bestimmen: Sei

$$f = X^2 + bX + c = (X - \alpha) \cdot (X - \beta).$$

Dann gilt

$$\begin{array}{rclcrcl} b & = & -\alpha - \beta & & c & = & \alpha \cdot \beta \\ D(f) & = & (\alpha - \beta)^2 & = & \alpha^2 - 2\alpha\beta + \beta^2 & = & b^2 - 4\alpha\beta = b^2 - 4c \end{array}$$

**Fall $\mathbf{D(f) = 0}$:** Dann ist $\alpha = \beta$ und

$$f = (X - \alpha)^2 = X^2 - 2\alpha X + \alpha^2 \in K[X],$$

also $2\alpha \in K$ und $\alpha^2 \in K$. Ist $\operatorname{char}(K) \neq 2$ oder $K$ perfekt, ist $\alpha \in K$ (für $\operatorname{char}(K) = 2$ folgt das aus 17.4).

Da wir nur eine Nullstelle haben, ist $\operatorname{Gal}_K(f) = \{id\}$.

**Fall $\mathbf{D(f) \neq 0}$:** Hier ist $\alpha \neq \beta$. Ist $\alpha \in K$, dann ist $f$ reduzibel und folglich auch $\beta \in K$. In diesem Fall $\operatorname{Gal}_K f = \{\mathrm{id}\}$.

Sind $\alpha, \beta \notin K$, dann ist $\operatorname{Gal}_K(f) \cong \mathbb{Z}/2$ erzeugt von $\sigma$ mit $\sigma(\alpha) = \beta$.

Ist $\operatorname{char}(K) \neq 2$, gilt

$$\alpha, \beta = \frac{-b \pm \sqrt{D(f)}}{2}.$$

Also liegen $\alpha, \beta$ genau dann in $K$, wenn $D(f)$ eine Quadratwurzel in $K$ besitzt.

**20.10 Satz:** Sei $f \in K[X]$, $\operatorname{grad}(f) = 2$

(1) Ist $D(f) = 0$, dann gilt

   (i) $\operatorname{Gal}_K(f) = \{\mathrm{id}\}$.

   (ii) $f$ hat eine doppelte Nullstelle $\alpha$.

   (iii) Ist $\operatorname{char}(K) \neq 2$ oder $K$ perfekt, dann ist $\alpha \in K$.

(2) Ist $D(f) \neq 0$, hat $f$ zwei verschiedene Nullstellen, die entweder beide in $K$ liegen oder beide nicht in $K$ liegen.

   (i) Liegen beide in $K$, ist $f$ reduzibel und $\mathrm{Gal}_K(f) = \{\mathrm{id}\}$.

   (ii) Liegen beide nicht in $K$, ist $f$ irreduzibel und $\mathrm{Gal}_K(f) \cong \mathbb{Z}/2$, erzeugt von $\sigma : \alpha \mapsto \beta$.

(3) Ist $\mathrm{char}(K) \neq 2$, hat jede quadratische Erweiterung $K \subset F$ die Form $F = K(\sqrt{\gamma})$ für ein $\gamma \in K$.

# 21 Zyklotomische Erweiterungen

**21.1 Definition:** Ein *primitive* $n$-te *Einheitswurzel* in einem Körper $K$ ist ein Element der Ordnung $n$ in $(K^*, \cdot)$. Eine $n$-te *Einheitswurzel* ist ein Element $a \in K$ mit $a^n = 1$. Man nennt $K \subset \mathrm{Zer}(X^n - 1)$ *zyklotomische Erweiterung* von $K$.

**21.2** Die Menge $\mu_n(K)$ der $n$-ten Einheitswurzel von $K$ ist eine endliche zyklische Untergruppe von $(K^*, \cdot)$ und $|\mu_n(K)|$ teilt $n$.

**Beweis:** $\mu_n(K)$ ist die Menge der Nullstellen von $X^n - 1$ in $K$ und daher endlich. $1 \in \mu_n(K)$ und mit $x, y$ ist auch $x^{-1}$ und $xy$ in $\mu_n(K)$. Also ist $\mu_n(K)$ eine Untergruppe von $(K^*, \cdot)$. Nach 16.13 ist $\mu_n(K)$ zyklisch. Ist $a$ ein Erzeuger, gilt $a^n = 1$, so dass $|\mu_n(K)| = \mathrm{ord}(a)$ Teiler von $n$ ist. □

**21.3 Satz:** Sei $K$ ein Körper der Charakteristik 0 oder $p$, wobei $p \nmid n$. Sei $F = \mathrm{Zer}(X^n - 1)$. Dann gilt

(1) $F$ enthält eine primitive $n$-te Einheitswurzel und $\mu_n(F) = \mathbb{Z}/n$.

(2) Ist $\zeta$ $n$-te primitive Einheitswurzel, so gilt $F = K[\zeta]$.

(3) $F/K$ ist Galois und die Abbildung

$$\begin{array}{rcl} \psi : \mathrm{Gal}(F/K) & \longrightarrow & ((\mathbb{Z}/n)^*, \cdot) \\ \sigma & \longmapsto & \bar{i}, \text{ falls } \sigma(\zeta) = \zeta^i \end{array}$$

ist ein Monomorphismus.

**Beweis:** (1) $f = X^n - 1$ hat nur einfache Nullstellen, weil $f' = nX^{n-1}$ und $n$ wegen $p \nmid n$ invertierbar ist. Also enthält $F$ genau $n$ verschiedene Einheitswurzeln. Nach 21.2 ist $\mu_n(F) \cong \mathbb{Z}/n$ und jeder Erzeuger von $\mathbb{Z}/n$ entspricht einer primitiven $n$-te Einheitswurzel.

(2) $K[\zeta]$ enthält ganz $\mu_n(F)$. Es folgt $K[\zeta] = F$.

(3) Sei $\zeta$ primitive $n$-te Einheitswurzel. Alle anderen primitiven $n$-ten Einheitswuzeln sind dann von der Form $\zeta^i$ mit $\mathrm{ggT}(i,n) = 1$, d.h. $\bar{i} \in (\mathbb{Z}/n)^*$.

Ein Automorphismus $\sigma \in \mathrm{Gal}(F/K)$ muss primitive $n$-te Einheitswurzeln auf primitive $n$-te Einheitswurzeln abbilden. Also ist $\sigma(\zeta) = \zeta^i$ mit $\bar{i} \in (\mathbb{Z}/n)^*$ und $\tau \circ \sigma(\zeta) = \tau(\zeta^i) = (\tau(\zeta))^i = \zeta^{j \cdot i}$, falls $\tau(\zeta) = \zeta^j$. Also ist $\psi$ ein Homomorphismus.

$$\psi(\sigma) = 1 \iff \sigma(\zeta) = \zeta \iff \sigma = \mathrm{id},$$

da auch $\sigma|K = \mathrm{id}$ und $F$ von $K$ und $\zeta$ erzeugt wird. □

**21.4 Beispiel:** (1) $K = \mathbb{C}$. Dann ist $F = K$, also $\mathrm{Gal}(F/K) = \{id\}$.

(2) $K = \mathbb{R}$ und $n > 2$. Dann ist $F = \mathbb{C}$, $|\mathrm{Gal}(\mathbb{C}/\mathbb{R})| = [\mathbb{C} : \mathbb{R}] = 2$, also $\mathrm{Gal}(\mathbb{C}/\mathbb{R}) = \mathbb{Z}/2$ erzeugt von $\sigma : \mathbb{C} \to \mathbb{C}$, $\sigma(x + iy) = x - iy$.

In beiden Fällen ist $\psi$ nicht surjektiv.

**21.5** $d|n \Rightarrow X^d - 1 | X^n - 1$.

Denn aus $n = k \cdot d$ folgt

$$X^n - 1 = (X^d)^k - 1 = (X^d - 1) \cdot (X^{d(k-1)} + X^{d(k-2)} + \ldots + X^d + 1).$$

Wir suchen nun nach dem Minimalpolynom einer primitiven Einheitswurzel. 21.5 legt nahe, folgende Polynome zu betrachten.

**21.6 Definition:** Die Polynome $\Phi_n = \prod(X - \zeta)$, das Produkt läuft über die $n$-ten primitiven Einheitswurzeln $\zeta$, heißen $n$-te *Kreisteilungspolynome*.

**21.7** (1) $\mathrm{grad}\, \Phi_n = \varphi(n) = |(\mathbb{Z}/n)^*|$

(2) $X^n - 1 = \prod_{d|n} \Phi_d$

(3) Der Leitkoeffizient von $\Phi_n$ ist 1.

**21.8 Beispiel:**
$$\begin{aligned} \Phi_1 &= X - 1 \\ \Phi_2 &= (X^2 - 1)/(X - 1) = X + 1 \\ \Phi_3 &= (X^3 - 1)/\Phi_1 = X^2 + X + 1 \\ \Phi_4 &= (X^4 - 1)/\Phi_1 \cdot \Phi_2 = (X^4 - 1)/(X^2 - 1) = X^2 + 1 \end{aligned}$$

Sei $F$ der Zerfällungskörper von $X^n - 1$. Nach Definition ist $\Phi_n \in F[X]$. Die Beispiele lassen aber vermuten, dass $\Phi_n \in \mathbb{Z}[X]$, falls $\mathrm{char}\, F = 0$, bzw. in $\mathbb{F}_p[X]$, falls $\mathrm{char}\, F = p$.

**21.9 Lemma:** $\Phi_n \in \begin{cases} \mathbb{Z}[X] & \text{in Charakteristik } 0 \\ \mathbb{F}_p[X] & p > 0 \end{cases}$

**Beweis:** Es genügt, Charakteristik 0 zu behandeln. Reduzieren wir mod $p$, erhalten wir den zweiten Teil. Den ersten Teil zeigen wir durch Induktion nach $n : \Phi_1 \in \mathbb{Z}[X]$ und hat Leitkoeffizient 1.

**Induktionsschritt:** Sei $g = \prod_{\substack{d|n \\ d \neq n}} \Phi_d$. Dann gilt $X^n - 1 = g \cdot \Phi_n$ nach 21.7.

Nach Induktion ist $g \in \mathbb{Z}[X]$ und hat Leitkoeffzient $1 \in \mathbb{Z}^*$. Daher können wir den Divisionalalgorithmus in $\mathbb{Z}[X]$ anwenden und erhalten $\Phi_n \in \mathbb{Z}[X]$ mit Leitkoeffzient 1. □

**21.10 Lemma:** Sei $K$ ein Körper der Charakteristik 0 oder $p$ mit $p \nmid n$. Sei $\zeta$ primitive $n$-te Einheitswurzel in einer Erweiterung $L$ von $K$. Dann sind äquivalent

(1) $\Phi_n$ ist irreduzibel in $K[X]$.

(2) $[K[\zeta] : K] = \varphi(n)$

(3) $\psi : \mathrm{Gal}(K[\zeta]/K) \to (\mathbb{Z}/n)^*$ aus 21.3 ist ein Isomorphismus.

**Beweis:** $\zeta$ ist Nullstelle von $\Phi_n$. Sei $f$ der normierte irreduzible Faktor von $\Phi_n$, der $\zeta$ als Nullstelle hat. Dann ist $f$ das Minimalpolynom von $\zeta$. Es gilt

$$\begin{aligned} [K[\zeta] : K] = \varphi(n) &\iff \operatorname{grad} f = \varphi(n) \iff f = \Phi_n \\ &\iff |\mathrm{Gal}(K[\zeta]/K)| = \varphi(n) \iff \psi \text{ ist bijektiv.} \end{aligned}$$

□

**21.11 Satz:** $\Phi_n$ ist irreduzibel in $\mathbb{Q}[X]$.

**Beweis:** Sei $f$ ein irreduzibler Faktor von $\Phi_n$. Wir zeigen

(1) $\zeta$ Nullstelle von $f \Rightarrow \zeta^i$ Nullstelle von $f$ $\forall i$ mit $\mathrm{ggT}(i, n) = 1$.

Das genügt, denn jede primitive $n$-te Einheitswurzel ist von der Form $\zeta^i$ mit $\mathrm{ggT}(i, n) = 1$. Wir erhalten also $f = \Phi_n$.

Um (1) zu zeigen, genügt der Nachweis von

(2) $\zeta$ Nullstelle von $f \Rightarrow \zeta^p$ Nullstelle von $f$, falls $p$ prim, $p \nmid n$. Denn $i$ aus (1) ist ein Produkt $i = p_1, \ldots, p_k$ solcher Primzahlen. Durch iteriertes Anwenden von (2) (ersetze $\zeta$ durch $\zeta^{p_1 \cdots p_k}$) erhält man (1).

Sei also $\Phi_n = f \cdot g$ mit $f, g \in \mathbb{Z}[X]$ und $\zeta$ Nullstelle von $f$. Angenommen $\zeta^p$ ist nicht Nullstelle von $f$, dann ist es Nullstelle von $g$, so dass $g(\zeta^p) = 0$.

Insbesondere ist $\zeta$ Nullstelle von $g(X^p)$. Da $f$ das Minimalpolynom von $\zeta$ ist, folgt $f|g(X^p)$, d.h.

$$g(X^p) = f \cdot h$$

in $\mathbb{Z}[X]$ (Der Leitkoeffizient von $f$ ist 1, so dass wir in $\mathbb{Z}[X]$ durch $f$ dividieren können). Die Gleichungen

$$\Phi_n = f \cdot g \qquad g(X^p) = f \cdot h$$

gelten auch über $\mathbb{F}_p$ nach Reduktion mod $p$. Sei $g = \sum_{i=0}^{p} a_i X^i$. Dann gilt mod $p$

$$g(X)^p = (\sum_{i=0}^{p} a_i X^i)^p = \sum_{i=0}^{r} a_i^p X^{ip} = \sum_{i=0}^{r} a_i (X^p)^i = g(X^p)$$

Es folgt

$$(g(X))^p = f \cdot h \qquad \text{in } \mathbb{F}_p[X].$$

Da $\mathbb{F}_p[X]$ euklidisch ist, können wir beide Seiten eindeutig in Primfaktoren zerlegen. Ist $u \in \mathbb{F}_p[X]$ ein Primfaktor von $f$, so ist $u$ auch Teiler von $g$. Es folgt $u^2|\Phi_n$ in $\mathbb{F}_p[X]$. Insbesondere hat $\Phi_n$ in seinem Zerfällungskörper über $\mathbb{F}_p[X]$ mehrfache Nullstellen. Wie wir aber im Beweis von 21.3 gesehen haben, hat $X^n - 1$ und damit auch $\Phi_n$ nur einfache Nullstellen. □

**21.12 Satz: Der Fall Charakteristik p $\nmid$ n:**

**21.13 Beispiel:** $\Phi_4$ ist reduzibel in $\mathbb{F}_5[X]$, denn in $\mathbb{F}_E[X]$ gilt

$$X^2 + 1 = (X + 3) \cdot (X + 2).$$

Das Beispiel zeigt, dass $\Phi_n$ über $\mathbb{F}_p$ reduzibel sein kann.

Sei $\zeta$ primitive $n$-te Einheitswurzel und $f \in \mathbb{F}_p[X]$ das Minimalpolynom von $\zeta$. Da $\Phi_n(\zeta) = 0$, folgt $f|\Phi_n$.

**21.14 Satz:** Sei $p$ prim, $p \nmid n$ und sei $e = \mathrm{ord}(\overline{p})$ in $(\mathbb{Z}/n)^*$. Dann hat jeder irreduzible Faktor $f$ von $\Phi_n$ in $\mathbb{F}_p[X]$ den Grad $e$. Also hat $\Phi_n$ genau $\frac{\varphi(n)}{e}$ irreduzibel Faktoren und

$$[\mathbb{F}_p[\zeta] : \mathbb{F}_p] = e.$$

**Beweis:** Sei $\zeta$ primitive $n$-Einheitswurzel, $F = \mathbb{F}_p[\zeta]$ ist der Zerfällungskörper von $\Phi_n$ nach 21.3. Sei $f$ das Minimalpolynom von $\zeta$, $\mathrm{grad}\, f = m$. Dann gilt $\dim_{\mathbb{F}_p}(F) = \mathrm{grad}\, f = m$, also

$$|F| = p^m.$$

Damit ist $\zeta$ Nullstelle von $X^{p^m} - X$ (s. Einführung in die Algebra), so dass $\zeta^{p^m-1} = 1$. Da $\mathrm{ord}(\zeta) = n$ in $F^*$, folgt $n | p^m - 1$, also

$$p^m \equiv 1 \mod n.$$

Da $p \nmid n$, ist $p \in (\mathbb{Z}/n)^*$. Sei $e = \mathrm{ord}(p)$ in $(\mathbb{Z}/n)^*$. Dann folgt

$$e|m, \quad p^e \equiv 1 \mod n, \quad \zeta^{p^e} = \zeta \qquad (*)$$

letzteres, weil $p^e \equiv 1 \mod n$ und $\zeta^n = 1$.
Nach 13.15 ist $\{1, \zeta, \zeta^2, \ldots \zeta^{m-1}\}$ eine Basis von $F$. Sei $y \in F^* \cong \mathbb{Z}/p^m - 1$ ein Erzeuger und

$$y = \sum_{i=0}^{m-1} c_i \zeta^i \quad c_i \in \mathbb{F}_p.$$

seine Darstellung als Linearkombination der Basiselemente. Dann gilt

$$y^{p^e} = \left( \sum_{i=0}^{m-1} c_i \cdot \zeta^i \right)^{p^e} = \sum_{i=0}^{m-1} c_i^{p^e} \cdot \zeta^{ip^e} = \sum_{i=0}^{m-1} c_i \cdot \zeta^i = y$$

weil $c^p = c$ in $\mathbb{F}_p$ nach dem kleinen Fermat'schen Satz und $\zeta^{p^e} = \zeta$. Es folgt

$$\mathrm{ord}\, y = p^m - 1 | p^e - 1, \qquad \text{also } e = m \text{ wegen } (*)$$

Also hat $f$ den Grad $e$. □

**21.15 Beispiel:** $\mathrm{ord}\, \overline{5}$ in $(\mathbb{Z}/4)^*$ ist 1 und $\varphi(4) = 2$. Also zerfällt $\Phi_4$ in zwei irreduzible Faktoren über $\mathbb{F}_5$.

# 22 Zyklische Erweiterungen

**22.1 Definition:** Eine *zyklische Erweiterung* ist eine Galois-Erweiterung $K \subset F$, so dass $\mathrm{Gal}(F/K)$ zyklisch ist.

Sei $b \in K$. Wir wollen den Zerfällungskörper $Z$ von $X^n - b$ studieren.

**22.2 Konvention:** Ist $\mathrm{char}(K) = p > 0$, setzen wir stets voraus, dass $\mathrm{ggT}(p, n) = 1$.

Nach 21.3 ist $X^n - 1$ separabel. Ist $\alpha$ Nullstelle von $X^n - b$ und $\zeta$ eine primitive $n$-te Einheitswurzel, dann sind

**22.3** $\alpha,\ \zeta\cdot\alpha,\ \zeta^2\cdot\alpha,\ \ldots,\ \zeta^{n-1}\cdot\alpha$
die Nullstellen von $X^n = b$, denn

$$(\zeta^k\cdot\alpha)^n - b = \zeta^{n\cdot k}\cdot\alpha^n - b = \alpha^n - b = 0.$$

Es folgt

$$Z = \mathrm{Zer}(X^n - b) = K(\alpha,\zeta).$$

Wir haben Körpererweiterungen

$$K \subset K(\zeta) \subset K(\alpha,\zeta) = \mathrm{Zer}(X^n - b).$$

Die erste Erweiterung ist zyklotomisch. Wir wollen die zweite Erweiterung studieren.
Wir nehmen daher ab jetzt an, dass $K$ eine primitive $n$-te Einheitswurzel $\zeta$ enthält. Dann ist

$$K \subset K(\alpha) = \mathrm{Zer}(X^n - b) = Z$$

Galois, und $\sigma \in \mathrm{Gal}(Z/K)$ ist eindeutig durch $\sigma(\alpha)$ festgelegt. Da $\sigma$ die Nullstellen von $X^n - b$ permutiert, gilt

$$\sigma(\alpha) = \zeta^{k(\sigma)}\cdot\alpha \qquad \text{mit } k(\sigma) \in \mathbb{Z}/n.$$

Da $\zeta \in K$, gilt für $\sigma,\tau \in \mathrm{Gal}(Z/K)$

$$(\sigma\circ\tau)(\alpha) = \sigma(\tau(\alpha)) = \sigma(\zeta^{k(\tau)}\cdot\alpha) = \zeta^{k(\tau)}\cdot\sigma(\alpha) = \zeta^{k(\tau)}\cdot\zeta^{k(\sigma)}\cdot\alpha$$

Damit definiert $\sigma \mapsto \zeta^{k(\sigma)}$ einen Monomorphismus

$$\mathrm{Gal}(Z/K) \to \mu_n.$$

Da $\mu_n$ zyklisch ist, ist $\mathrm{Gal}(Z/K)$ zyklisch und

$$|\mathrm{Gal}(Z/K)| = [K(\alpha):K] \text{ teilt } n.$$

Wir erhalten

**22.4 Satz:** Enthält $K$ eine primitive $n$-te Einheitswurzel und ist $b \in K$, dann ist die Galoisgruppe $G = G_K(X^n - b)$ zyklisch und $|G|$ teilt $n$.

Ziel der Restes dieses Abschnitts ist der Beweis des folgenden Klassifikationssatzes.

**22.5 Satz:** Sei $K$ ein Körper, der eine $n$-te primitive Einheitswurzel $\zeta$ enthält. Dann sind äquivalent

(1) $K \subset F$ ist zyklisch vom Grad $d|n$.

(2) $F = K(\alpha)$, und das Minimalpolynom von $\alpha$ ist $X^d - c$ mit $c \in K$ und $d|n$.

(3) $F$ ist Zerfällungskörper eines irreduziblen Polynoms $X^d - c$ mit $c \in K$ und $d|n$.

(4) $F = K(\alpha)$, wobei $\alpha$ Nullstelle eines Polynoms $X^n - b$ mit $b \in K$ ist.

(5) $F$ ist der Zerfällungskörper eines Polynoms $X^n - b$ mit $b \in K$.

**Beweis:** Nach Voraussetzung enthält $K$ die primitive $d$-te Einheitswurzel $\zeta^k$, wobei $n = k \cdot d$. Das impliziert (2) $\iff$ (3) und (4) $\iff$ (5):
Denn ist $\alpha \in F$ Nullstelle von $X^d - c$ und $\eta = \zeta^k$, dann sind

$$\alpha,\ \eta \cdot \alpha,\ \ldots,\ \eta^{d-1} \cdot \alpha \text{ aus } F$$

nach 22.3 alle Nullstellen von $X^d - c$, und entsprechendes gilt für die Äquivalenz (4) $\iff$ (5).
(2) $\Longrightarrow$ (4): Sei $F = K(\alpha)$ mit $\alpha$ wie in (2), dann gilt $\alpha^d = c \in K$. Da $d|n$, gibt es ein $k \in \mathbb{N}$ mit $n = k \cdot d$. Es folgt $b := c^k \in K$ und $\alpha^n = c^k = b$. Also ist $\alpha$ Nullstelle von $X^n - b \in K[X]$.
(4) $\Longrightarrow$ (2): Nach 22.3 ist

$$\alpha,\ \zeta \cdot \alpha, \ldots,\ \zeta^{n-1} \cdot \alpha \quad \text{ aus } F$$

die Liste aller Nullstellen von $X^n - b$. Sei $f$ das Minimalpolynom von $\alpha$. Dann ist $f$ Teiler von $X^n - b$ und $d = \operatorname{grad} f$ teilt $n$. Die $d$ Nullstellen von $f$ sind in der Liste enthalten. Ihr Produkt hat die Form $\zeta^l \cdot \alpha^d$. Da dieses Produkt der konstante Term von $f$ ist, ist $\alpha^d \in K$. Es folgt $f = X^d - \alpha^d$.
(5) $\Longrightarrow$ (1) folgt aus 22.4
(1) $\Longrightarrow$ (2): Sei $F/K$ zyklisch vom Grad $d|n$. Sei $G = \langle\sigma\rangle = \operatorname{Gal}(F/K)$. Da $F/K$ Galois ist, ist $\operatorname{ord}(\sigma) = d$. Für $\alpha \in F$ gilt

$$\alpha^d \in K = F^G \iff \alpha^d = \sigma(\alpha^d) = (\sigma(\alpha))^d \iff \left(\frac{\alpha}{\sigma(\alpha)}\right)^d = 1 \qquad (*)$$

Sei $n = k \cdot d$. Dann ist $\eta = \zeta^k \in K$ eine primitive $d$-te Einheitswurzel. Finden wir ein $\alpha \in F$, so das $\frac{\alpha}{\sigma(\alpha)} = \eta$, dann ist $(*)$ erfüllt, also $\alpha^d \in K$. Es folgt, dass $\alpha$ Nullstelle von $X^d - \alpha^d \in K[X]$ ist. Das Minimalpolynom $f$ teilt $X^d - \alpha^d$. Die Elemente

$$\alpha,\ \sigma(\alpha), \ldots,\ \sigma^{d-1}(\alpha)$$

sind Nullstellen von $f$, da $G$ die Nullstellen von $f$ permutiert. Nun gilt $\sigma(\alpha) = \eta^{-1} \cdot \alpha$, also $\sigma^k(\alpha) = \eta^{-k} \cdot \alpha$, so dass diese Nullstellen alle verschieden sind. Damit hat $f$ den Grad $d$, so dass $f = X^d - \alpha^d$. Wir erhalten (2) mit $c = \alpha^d$.

Es bleibt also, $\alpha \in F$ zu finden, so dass $\frac{\alpha}{\sigma(\alpha)} = \eta$.

Da $\eta \in K$, gilt $\sigma^k(\eta) = \eta$, also

$$\prod_{\tau \in G} \tau(\eta) = \eta^{|G|} = \eta^d = 1.$$

Damit gibt es nach dem folgenden Satz mit $\beta = \eta$ ein solches $\alpha$. □

**22.6 Hilbert Theorem 90:** Sei $F/K$ eine endliche zyklische Erweiterung mit Galois-Gruppe $G = \langle \sigma \rangle$. Dann gilt für $\beta \in F$

$$\exists \alpha \in F^* \text{ mit } \beta = \frac{\alpha}{\sigma(\alpha)} \iff \prod_{\tau \in G} \tau(\beta) = 1.$$

Der Beweis bedarf einiger Vorbereitungen.

**22.7 Definition:** Sei $F/K$ eine endliche Galois-Erweiterung mit Galois-Gruppe $G$. Die *Norm-Abbildung* der Erweiterung ist definiert durch

$$N_{F/K} : F \to K, \quad \alpha \mapsto \prod_{\tau \in G} \tau(\alpha).$$

**22.8** (1) $N_{F/K}(\alpha) \in K$ für alle $\alpha \in F$.

(2) $N_{F/K}(\alpha) = \alpha^{|G|}$ für alle $\alpha \in K$.

(3) $N_{F/K} : (F^*, \cdot) \to (K^*, \cdot)$ ist ein Homomorphismus.

**Beweis:** Sei $\alpha \in F^*$, dann gilt für $\sigma \in G = \mathrm{Gal}(F/K)$

$$\sigma(N_{F/K}(\alpha)) = \prod_{\tau \in G} \sigma \circ \tau(\alpha) = \prod_{\tau \in G} \tau(\alpha) = N_{F/K}(\alpha).$$

Also ist $N_{F/K}(\alpha) \in F^G = K$. Da $\tau(\alpha) \neq 0$ für $\alpha \in F^*$, folgt $N_{F/K}(\alpha) \in K^*$.

$$N_{F/K}(\alpha \cdot \beta) = \prod_{\tau \in G} \tau(\alpha) \cdot \tau(\beta) = \prod_{\tau \in G} \tau(\alpha) \cdot \prod_{\tau \in G} \tau(\beta) = N_{F/K}(\alpha) \cdot N_{F/K}(\beta).$$

Ist $\alpha \in K$, gilt $\tau(\alpha) = \alpha$ für $\tau \in G$, so dass $N_{F/K}(\alpha) = \alpha^{|G|}$. □

**Beweis von 22.6 $\Rightarrow$:** Sei $\alpha = \beta \cdot \sigma(\alpha)$. Dann gilt

$$\begin{aligned} \prod_{\tau \in G} \tau(\alpha) = N_{F/K}(\alpha) &= N_{F/K}(\beta) \cdot N_{F/K}(\sigma(\alpha)) \\ &= N_{F/K}(\beta) \cdot \prod_{\tau \in G} \tau(\sigma(\alpha)) = N_{F/K}(\beta) \cdot N_{F/K}(\alpha). \end{aligned}$$

Es folgt $N_{F/K}(\beta) = 1$. □

Die andere Richtung bedarf auch einiger Vorbereitung.

**22.9 Satz:** (Artin, vergl. 18.11) Sei $M$ ein Monoid und $K$ ein Körper. Sei $\mathcal{F}$ eine Menge von verschiedenen Homomorphismen $f : M \to K^*$. Dann ist $\mathcal{F}$ linear unabhängig im $K$-Vektorraum $\mathrm{Abb}(M, K)$.

**Beweis:** Seien $f_1, \ldots, f_n \in \mathcal{F}$ verschiedenen. Wir wollen annehmen, wir haben eine nicht-triviale Gleichung

$$\alpha_1 \cdot f_1 + \ldots + \alpha_n \cdot f_n = 0 \qquad (A)$$

mit $\alpha_i \in K$. Unter allen diesen Gleichungen wählen wir eine mit der minimalen Anzahl von $\alpha_i \neq 0$. Indem wir die Summanden mit $\alpha_i = 0$ weglassen, dürfen wir annehmen, dass $(A)$ eine solche Gleichung ist mit $\alpha_i \neq 0$ für $i = 1, \ldots, n$. Da $f_1 \neq f_n$, gibt es eine $x \in M$ mit $f_1(x) \neq f_n(x)$. Für $y \in M$ haben wir

$$\alpha_1 \cdot f_1(x \cdot y) + \ldots + \alpha_n \cdot f_n(x \cdot y) = 0$$

$$\alpha_1 \cdot f_1(x) \cdot f_1(y) + \ldots + \alpha_n \cdot f_n(x) \cdot f_n(y) = 0 \qquad (B)$$

Aus (A) erhalten wir durch Multiplikation mit $f_1(x)$

$$\alpha_1 \cdot f_1(x) \cdot f_1(y) + \ldots + \alpha_n \cdot f_n(x) \cdot f_n(y) = 0 \qquad (C)$$

(B)-(C) ergibt

$$\alpha_2 \cdot (f_2(x) - f_1(x)) \cdot f_2(y) + \ldots + \alpha_n \cdot (f_n(x) - f_1(x)) \cdot f_n(y) = 0.$$

Da dies für alle $y \in M$ gilt und da $\alpha_n \cdot (f_n(x) - f_1(x)) \neq 0$, erhalten wir eine nicht-triviale Gleichung kürzerer Länge

$$\alpha_2 \cdot (f_2(x) - f_1(x)) \cdot f_2 + \ldots + \alpha_n (f_n(x) - f_1(x)) \cdot f_n = 0$$

ein Widerspruch. □

**Beweis von 22.6 $\Leftarrow$:** Sei $[F; K] = d$ und $N_{F/K}(\beta) = 1$. Wir suchen ein $\alpha \in F^*$ mit $\beta \cdot \sigma(\alpha) = \alpha$. Dazu betrachten wir die Homomorphismen

$$\tau_k : F \to F, \qquad 0 \leq k \leq d$$

$\tau_0 = \mathrm{id}$ und $\tau_k = \beta \cdot \sigma(\beta) \cdot \sigma^2(\beta) \cdot \ldots \cdot \sigma^{k-1}(\beta) \cdot \sigma^k$ für $0 < k \leq d$.
Dann gilt

$$\tau_{k+1} = \beta \cdot (\sigma \cdot \tau_k) \qquad \text{für } 0 \leq k \leq d-1.$$

Da $\sigma^0, \sigma^1, \ldots, \sigma^{d-1}$ verschiedene Homomorphismen $F^* \to F^*$ sind und

$$\tau = \tau_0 + \tau_1 + \ldots + \tau_{d-1}$$

eine $F$-Linearkombination von $\sigma^0, \sigma^1, \ldots, \sigma^{d-1}$ ist, ist $\tau \neq 0$ nach 22.9.
Da $\tau_d = N_{F/K}(\beta) \cdot \sigma^d = 1 \cdot \mathrm{id} = \tau_0$, folgt

$$\beta \cdot (\sigma \circ \tau) = \tau_1, +\tau_2 + \ldots + \tau_d = \tau.$$

Da $\tau$ als Abbildung $\tau : F^* \to F$ von 0 verschieden ist, gibt es ein $\gamma \in F^*$, so dass $\alpha := \tau(\gamma) \neq 0$. Für dieses $\alpha$ gilt

$$\beta \cdot \sigma(\alpha) = \beta \cdot \sigma(\tau(\gamma)) = \tau(\gamma) = \alpha.$$

# Teil IV
# Anwendungen

## 23 Lösbarkeit polynomialer Gleichungen

Sei $f \in K[X]$ ein Polynom. Wir fragen uns, ob es eine „Formel“ für die Lösungen der polynomialen Gleichung

$$f(x) = 0$$

gibt, so dass die Lösungen durch iteriertes Wurzelziehen berechnet werden können. Das bekannteste Beispiel ist die Lösungsformel für

$$x^2 + px + q = 0,$$

nämlich

$$x_{1/2} = -\frac{p}{2} \pm \sqrt{\frac{p^2}{4} - q}.$$

**23.1 Definition:** Die Gleichung $f(x) = 0$ heißt *auflösbar* und $f$ ein *auflösbares Polynom*, wenn es einen Turm von Körpern

$$K = K_0 \subset K_1 \subset \ldots \subset K_m$$

gibt, so dass

(i) $K_i = K_{i-1}[\alpha_i]$ mit $\alpha_i^{m_i} \in K_{i-1}$ für ein $m_i \in \mathbb{N}$

(ii) $f$ zerfällt über $K_m$.

**23.2 Erläuterung:** $K_i$ entsteht aus $K_{i-1}$ durch Adjunktion einer $m_i$-ten Wurzel wegen (i). Wegen (ii) liegen die Nullstellen von $f$ in $K_m$, lassen sich daher als Ausdrücke darstellen, in denen nur Elemente aus $K$ und iterierte Wurzeln der $\alpha_i$ auftreten.

**23.3 Theorem:** (Galois 1832) Sei $\operatorname{char} K = 0$ und $f \in K[X]$. Dann gilt: $f$ ist genau dann auflösbar, wenn die Galoisgruppe $\mathrm{Gal}_K(f)$ von $f$ auflösbar ist. (Daher der Begriff “auflösbare Gruppe“).

Wir benötigen zwei Hilfssätze.

**23.4 Lemma:** Sei $F/K$ eine Körpererweiterung und $f \in K[X] \subset F[X]$. Dann ist $\mathrm{Gal}_F(f)$ Untergruppe von $\mathrm{Gal}_K(f)$.

**Beweis:** Sei $Z'$ der Zerfällungskörper von $f$ über $F$, so dass $\mathrm{Gal}_F(f) = \mathrm{Gal}(Z'/F)$. Seien $\alpha_1, \ldots, \alpha_n$ die Nullstellen von $f$ in $Z'$. Dann ist $Z = K[\alpha_1, \ldots, \alpha_n]$ der Zerfällungskörper von $f$ über $K$. Ein Element $\sigma \in \mathrm{Gal}_F(f)$ permutiert die $\alpha_i$ und lässt $F$ fest. Es folgt $\sigma(Z) \subset Z$. Die Abbildung

$$\psi : \mathrm{Gal}_F(f) \longrightarrow \mathrm{Gal}_K(f) \qquad \sigma \mapsto \sigma|Z$$

ist ein Monomorphismus, denn $\psi(\sigma) = \mathrm{id}$ genau dann, wenn $\sigma|Z$, also auch $\sigma$ die $\alpha_i$ fest lässt. Aber dann ist $\sigma = \mathrm{id}$. □

**23.5 Lemma:** Ist $G$ eine endliche auflösbare Gruppe, dann besitzt $G$ eine Subnormalreihe

$$G = G_0 \rhd G_1 \rhd \ldots \rhd G_k = \{e\}$$

mit zyklischen Faktoren $G_i/G_{i+1}$.

**Beweis:** $G$ besitzt eine Subnormalreihe

$$G = H_0 \rhd H_1 \rhd \ldots \rhd H_r = \{e\}$$

mit abelschen Faktoren $H_i/H_{i+1}$. Es genügt zu zeigen, dass wir

$$H_i \rhd H_{i+1}$$

zu einer Subnormalreihe

$$H_i = K_q \rhd K_1 \rhd \ldots \rhd K_0 = H_{i+1}$$

mit zyklischen Faktoren verfeinern können. Als endliche abelsche Gruppe ist $H_i/H_{i+1} \cong Z_1 \times \ldots \times Z_q$, wobei jedes $Z_i$ zyklisch ist

$$\{e\} \lhd Z_1 \lhd Z_1 \times Z_2 \lhd Z_1 \times Z_2 \times Z_3 \lhd \ldots \lhd Z_1 \times \ldots \times Z_q$$

ist eine Normalreihe mit zyklischen Faktoren. Sei

$$p : H_i \longrightarrow H_i/H_{i+1} \cong Z_1 \times \ldots \times Z_q.$$

Sei $K_j = p^{-1}(Z_1 \times \ldots \times Z_j)$. Da $Z_1 \times \ldots \times Z_j \lhd Z_1 \times \ldots \times Z_q$, ist $K_j \lhd H_i$. Wir erhalten eine Subnormalreihe der gewünschten Form, denn

$$K_j/K_{j-1} \cong K_j/H_{i+1} \Big/ K_{j-1}/H_{i+1} \cong \frac{Z_1 \times \ldots \times Z_j}{Z_1 \times \ldots \times Z_{j-1}} \cong Z_j.$$

□

**Beweis 23.3:** Sei $G = \mathrm{Gal}_K(f)$ auflösbar. Wir wollen zeigen, dass $f$ auflösbar ist.

Sei $n = |G|$ und $\zeta$ eine primitive $n$-te Einheitswurzel. Sei $F = K[\zeta]$. Nach 23.4 ist $H = \mathrm{Gal}_F(f)$ Untergruppe von $G$ und daher nach 8.9 ebenfalls auflösbar. Nach 23.5 gibt es eine Subnormalreihe

$$H = G_m \rhd G_{m-1} \rhd \ldots \rhd G_0 = \{e\}$$

mit zyklischen Faktoren $G_i/G_{i-1}$. Sei $Z$ der Zerfällungskörper von $f$ über $F$ und sei $F_i = Z^{G_i}$. Wir erhalten einen Turm von Körpern

$$K \subset F = F_m \subset F_{m-1} \subset \ldots \subset F_0 = Z. \qquad (*)$$

Nach 19.11 ist $F_{i+1} \subset F_i$ Galois mit zyklischer Galois-Gruppe $G_{i+1}/G_i$, also eine zyklische Erweiterung. Da nach der Gradschachtelungsformel $d = [F_i : F_{i+1}]$ ein Teiler von $[Z : F] = |H|$ und $|H|$ Teiler von $|G| = n$ ist, ist $d = [F_i : F_{i+1}]$ ein Teiler $n$. Aus 22.5 folgt, dass $F_i = F_{i+1}(\alpha)$ mit $\alpha^d \in F_{i+1}$ ist. Da $F = K[\zeta]$ und $\zeta^n = 1$, ist $(*)$ der gesuchte Turm von Körpern.

Sei nun umgekehrt $f$ auflösbar. Wir wollen zeigen, dass $G$ auflösbar ist. Nach 8.9 genügt es zu zeigen, dass $G$ Faktorgruppe einer auflösbaren Gruppe ist. Nach 19.10 reicht es, eine Galois-Erweiterung $K \subset E$ mit auflösbarer Galois-Gruppe $\mathrm{Gal}(E/K)$ zu finden, so dass $f$ über $E$ zerfällt, denn dann enthält $E$ einen Zerfällungskörper $Z$ von $f$, so dass $K \subset Z \subset E$, und nach 19.10 ist

$$\mathrm{Gal}_K(f) = \mathrm{Gal}(Z/K) \cong \frac{\mathrm{Gal}(E/K)}{\mathrm{Gal}(E/Z)}.$$

Da $f$ auflösbar ist, zerfällt $f$ in einer Erweiterung $K \subset K_m$ von $K$ mit folgenden Eigenschaften

(1) $K_m = K[\alpha_1, \ldots, \alpha_m]$

(2) Zu jedem $\alpha_i$ gibt es ein $r_i \in \mathbb{N}$, so dass $\alpha_i^{r_i} \in K[\alpha_1, \ldots, \alpha_{i-1}]$

Nach 16.17 ist $K \subset K_m$ einfach, d.h. es gibt ein $\gamma \in K_m$, so dass $K_m = K[\gamma]$. Sei $g \in K[X]$ das Minimalpolynom von $\gamma$ und sei $F$ ein Zerfällungskörper von $g \cdot (X^n - 1)$, wobei $n = r_1 \cdot r_2 \cdot \ldots \cdot r_m$. Wir dürfen annehmen, dass $K_m = K[\gamma] \subset F$. Sei $G = \{\sigma_1 = \mathrm{id}, \sigma_2, \ldots, \sigma_k\} = \mathrm{Gal}(F/K)$ und $\zeta \in F$ eine primitive $n$-te Einheitswurzel. Wir wählen $E$ als Galois-Abschluss von $K_m[\zeta]$ in $F$. Dann gilt nach 19.14

$$E = K[\zeta, \alpha_1, \ldots, \alpha_m, \sigma_2(\alpha_1), \ldots, \sigma_2(\alpha_m), \ldots, \sigma_k(\alpha_1), \ldots, \sigma_k(\alpha_m)]$$

Wir adjungieren diese Elemente nacheinander an $K$ und erhalten so einen Turm

$$K \subset K[\zeta] \subset K[\zeta, \alpha_1] \subset \ldots \subset K' \subset K'' \subset \ldots \subset E \qquad (**)$$

Dabei entsteht $K''$ aus $K'$ durch Adjunktion eines $\sigma_i(\alpha_j)$. Da

$$\sigma_i(\alpha_j)^{r_j} = \sigma_i(\alpha_j^{r_j}) \in \sigma_i(K[\alpha_1, \ldots, \alpha_{j-1}]) = K[\sigma_i(\alpha_1), \ldots, \sigma_i(\alpha_{j-1})] \subset K',$$

adjungieren wir die $r_j$-te Wurzel eines Elementes aus $K'$.

Da $n = r_1 \cdot r_2 \cdot \ldots \cdot r_m$, enthält $K'$ eine $r_j$-te primitive Einheitswurzel $w$.

$K''$ ist der Zerfällungskörper von $X^{r_i} - (\sigma_i(\alpha_j))^{r_j}$, denn $\sigma_i(\alpha_j)$ ist eine Nullstelle in $K''$, die übrigen sind von der Form $w^t\sigma_i(\alpha_j) \in K''$. Damit ist $K' \subset K''$ Galoiserweiterung. Nach 22.4 ist die Galoisgruppe zyklisch. Auch $K \subset K[\zeta]$ ist Galois mit Galoisgruppe $(\mathcal{Z}/n)^*$ nach 21.10. Die Galois-Korrespondenz überträgt $(**)$ in einem Turm von Untergruppen

$$\mathrm{Gal}(E/K) = G_0 > G_1 > \ldots > G' > G'' > \ldots > \{id\}.$$

Da $K \subset K[\zeta]$ und $K' \subset K''$ Galois sind, folgt aus 19.10, dass $G_0 \rhd G_1$ und $G' \rhd G''$ mit $G_0/G_1 \cong \mathrm{Gal}(K[\zeta]/K)$ abelsch und $G'/G'' \cong \mathrm{Gal}(K''/K')$ zyklisch. Also ist $\mathrm{Gal}(F/K)$ auflösbar. □

**23.6 Folgerung:** Sei $\mathrm{char}\, K = 0$ und $f \in K[X]$ von Grad $\leq 4$. Dann ist $f$ auflösbar.

**Beweis:** Sei $\mathrm{grad}\, f = n$ und seien $\alpha_1, \ldots, \alpha_k$ die verschiedenen Nullstellen von $f$ in seinem Zerfällungskörper. Dann gilt $k \leq n$. Nach 20.3 ist $\mathrm{Gal}_K(f)$ Untergruppe von $\Sigma_k$. Nach 8.3 ist $\Sigma_k$ und damit $\mathrm{Gal}_K(f)$ für $k \leq 4$ auflösbar. □

**23.7 Satz:** Für $n \geq 5$ gibt es Polynome $f \in \mathbb{Q}[X]$, die nicht auflösbar sind.

Es genügt, ein nicht auflösbares Polynom $f$ vom Grad 5 zu finden. Denn multiplizieren wir $f$ mit einem beliebigen Polynom $g$ vom Grad $n > 0$, erhalten wir ein Polynom vom Grad $n + 5$, und es gilt nach 20.4

$$\mathrm{Gal}_{\mathbb{Q}}(f) = \frac{\mathrm{Gal}_{\mathbb{Q}}(f \cdot g)}{\mathrm{Gal}_Z(f \cdot g)},$$

wobei $Z$ der Zerfällungskörper von $f$ über $\mathbb{Q}$ ist. Nach 8.5 ist dann auch $f \cdot g$ nicht auflösbar.

**23.8 Satz:** Sei $p$ prim und $f \in \mathbb{Q}[X]$ irreduzibel vom Grad $p$. Hat $f$ in $\mathbb{C}$ genau zwei nicht-reelle Nullstellen, dann ist $\mathrm{Gal}_{\mathbb{Q}}(f) \cong \Sigma_p$. Insbesondere ist $f$ für $p \geq 5$ nicht auflösbar.

Für den Beweis benötigen wir

**23.9 Lemma:** Sei $p$ prim. Dann wird $\Sigma_p$ von einer beliebigen Transposition $\tau = (i, j)$ und einem beliebigen $p$-Zykel $\sigma = (i_1, \ldots, i_p)$ erzeugt.

**Beweis:** Indem wir gegebenfalls umnummerieren, dürfen wir annehmen dass $\tau = (1, 2)$. Weiter schreiben wir $\sigma$ so, dass 1 an der ersten Stelle steht $\sigma = (1, i_2, \ldots, i_p)$. Da $p$ prim ist, ist $\langle \sigma^k \rangle = \langle \sigma \rangle$ für $1 \leq k \leq p-1$. Für ein geeignetes $k$ gilt $\sigma^k(1) = 2$. Es genügt zu zeigen, dass $\sigma' = \sigma^k$ und $\tau$ ganz $\Sigma_p$ erzeugen. Aber $\sigma' = (1, 2, j_3, \ldots, j_p)$. Indem wir $j_3, \ldots, j_p$ umnummerieren, genügt es zu zeigen, dass $(1, 2)$ und $\rho = (1, 2, 3, \ldots, p)$ ganz $\Sigma_p$ erzeugen. Nun gilt

$$\rho \circ \tau \circ \rho^{-1} = (2, 3),\ \rho^2 \circ \tau \circ \rho^{-2} = (3, 4), \ldots, \rho^k \circ \tau \circ \rho^{-k} = (k+1, k+2)$$

Aber die Elemente $(i, i+1), i = 1, \ldots, p-1$ erzeugen $\Sigma_p$ nach 7.7. □

**Beweis 23.8:** Sei $Z \subset \mathbb{C}$ der Zerfällungskörper von $f$ und $G = \mathrm{Gal}_{\mathbb{Q}}(f)$. Sei $\alpha \in Z$ eine Nullstelle von $f$. Da $f$ irreduzibel ist, ist $[\mathbb{Q}[\alpha] : \mathbb{Q}] = p$. Da $\mathbb{Q} \subset \mathbb{Q}[\alpha] \subset Z$, folgt $p$ teilt $[Z : \mathbb{Q}] = |G|$. Nach den Sylowsätzen enthält $G$ ein Element der Ordnung $p$. Fassen wir $G$ als Untergruppe von $\Sigma_p$ auf, enthält $G$ somit einen $p$-Zykel.

Ist $\sigma$ die komplexe Konjugation, dann vertauscht $\sigma$ die beiden nicht-reellen Nullstellen von $f$ und lässt die übrigen Nullstellen fest. Also ist $\sigma$ ein Automorphismus $\sigma : Z \to Z$ und liegt in $G$. Damit enthält $G$ ein Element der Ordnung 2, d.h. eine Transposition.

Aus dem Lemma folgt, dass $G = \Sigma_p$. □

**23.10 Beispiel:** $f = X^5 - 6X + 3$

3 teilt 6 und 3 und $3^2$ teilt nicht 3. Damit ist $f$ nach Eisensteins Kriterium irreduzibel. Die Ableitung $f' = 5X^4 - 6$ hat die reellen Nullstellen $\pm \sqrt[4]{\frac{6}{5}}$. Damit hat $f$ höchstens zwei lokale Extrema. Da

$$f(-2) = -17 \qquad f(0) = 3 \qquad f(1) = -2 \qquad f(2) = 23$$

hat $f$ genau 3 reelle Nullstellen und damit genau 2 nicht-reelle ($f$ hat als irreduzibles Polynom aus $\mathbb{Q}[X]$ nur einfache Nullstellen). Es folgt: $\mathrm{Gal}_{\mathbb{Q}}(f) \cong \Sigma_5$.

# 24 Konstruktion mit Zirkel und Lineal

**24.1 Definition:** Gegeben sei eine Punktmenge $M$ der Ebene $E$. Wir sagen $M'$ entsteht aus $M$ durch einen *Elementarschritt*, wenn $M' = M \sqcup \{a\}$, wobei $a$ der Schnittpunkt

(1) zweier verschiedener Geraden durch jeweils zwei Punkte aus $M$

(2) einer Geraden durch zwei Punkte von $M$ mit einem Kreis um einen Punkt von $M$ mit dem Abstand zweier Punkte aus $M$ als Radius

(3) zweier solcher Kreis

ist.

$z \in E$ heißt aus $M$ *mit Zirkel und Lineal konstruierbar*, wenn es eine endliche Kette von Mengen $M = M_1 \subset M_2 \subset \ldots \subset M_r$ gibt mit $z \in M_r$ und $M_{i+1}$ aus $M_i$ durch einen Elementarschritt entsteht.

Wir betrachten nur Mengen $M$ mit mindestens zwei Elementen. Wir nennen eines der Elemente 0 und ein anderes 1 und identifizieren dadurch $E$ mit dem Körper $\mathbb{C}$ der komplexen Zahlen, also $M \subset \mathbb{C}$.

In der Einführung in die Algebra wurde bereits gezeigt.

**24.2 Satz:** Für die Menge $K_M$ der aus $M$ konstruierbaren Elemente aus $\mathbb{C}$ gilt:

(1) $K_M$ ist Unterkörper von $\mathbb{C}$

(2) $z \in K_M \Rightarrow \overline{z} \in K_M$

(3) $z \in K_M \Rightarrow \sqrt{z} \in K_M$

**24.3 Bezeichnung:** Für $M \subset \mathbb{C}$ ist $\overline{M} = \{\overline{z}; z \in M\}$.

Die folgenden beiden Ergebnisse wurden ebenfalls in der Einführung in die Algebra gezeigt:

**24.4 Satz:** Sei $M \subset \mathbb{C}$, $0, 1 \in M$. Sei $K = \mathbb{Q}(M \cup \overline{M}) \subset \mathbb{C}$. Dann gilt: $z \in \mathbb{C}$ ist genau dann mit Zirkel und Lineal aus $M$ konstruierbar, wenn es Körper

$$K = L_0 \subset L_1 \subset L_2 \subset \ldots \subset L_m \subset \mathbb{C}$$

gibt, so dass $z \in L_m$ und $[L_i : L_{i-1}] \leq 2$ für $i = 1, \ldots, m$. □

**24.5 Satz:** Seien $M$ und $K$ wie in 24.4. Ist $z \in \mathbb{C}$ aus $M$ konstruierbar, dann gilt $[K(z) : K] = 2^t$ für ein $t \in \mathbb{N}$.

Als Anwendungen wurde gezeigt (z.T. in Übungsaufgaben)

**24.6 Satz:** (1) Die Quadratur des Kreises mit Zirkel und Lineal ist nicht möglich.

(2) Die Würfelverdopplung ist mit Zirkel und Lineal nicht möglich, d.h. die Kantenlänge eines Würfel von doppeltem Volumen lässt sich nicht aus der Kantenlänge des gegebenen Würfels konstruieren.

(3) Der Winkel von $60^\circ$ lässt sich nicht mit Zirkel und Lineal dritteln.

(4) Enthält die Primfaktorzerlegung von $n$ eine Primzahl, die keine Fermat'sche Primzahl ist, dann lässt sich das reguläre $n$-Eck nicht mit Zirkel und Lineal konstruieren.

(Zur Erinnerung: Die Zahl $F_n = 2^{2^n} + 1$ heißt *$n$-te Fermat'sche Zahl*. Ist $F_n$ prim, heißt $F_n$ *Fermat'sche Primzahl*.)

In diesem Paragraphen wollen wir auf die Winkeldrittelung und die Konstruktion des regulären $n$-Ecks näher eingehen. Wir beginnen mit der Drittelung *rationaler Winkel* $\alpha = \frac{m}{n} \cdot 2\pi$ mit $m \in \mathbb{Z}$ und $n \in \mathbb{N}\backslash\{0\}$ .

In unseren Überlegungen spielt die Euler'sche $\varphi$-Funktion eine große Rolle

$$\varphi : \mathbb{N} \to \mathbb{N}, \quad \varphi(n) = |\{k \in \mathbb{N}\backslash\{0\}; k \leq n, \mathrm{ggT}(k,n) = 1\}|.$$

Insbesondere gilt

$$\varphi(n) = |(\mathbb{Z}/n)^*|.$$

Ist $n = p_1^{r_1} \cdot p_2^{r_2} \cdot \ldots \cdot p_k^{p_k}$ die Primfaktorzerlegung von $n$ mit $p_1 < p_2 < \ldots < p_k$, dann ist nach dem chinesischen Restsatz

$$\mathbb{Z}/n \cong \mathbb{Z}/p_1^{r_1} \times \ldots \times \mathbb{Z}/p_k^{r_k}$$

als Ring, und damit

$$(\mathbb{Z}/n)^* \cong (\mathbb{Z}/p_1^{r_1})^* \times \ldots \times (\mathbb{Z}/p_k^{r_k})^*.$$

Es folgt

$$\varphi(n) = \varphi(p_1^{r_1}) \cdot \ldots \cdot \varphi(p_k^{r_k}).$$

Nun ist für $p$ prim

$$\varphi(p^r) = |\{k \in \mathbb{N}\backslash\{0\}; k \leq p^r, p \nmid k\}|.$$

Sei $0 < k \leq p^r$. Dann ist $k$ genau dann durch $p$ teilbar, wenn

$$k \in \{p, 2p, 3p, \ldots, p^{r-1} \cdot p\}.$$

Es folgt

$$\varphi(p^r) = p^r - p^{r-1} = (p-1) \cdot p^{r-1}.$$

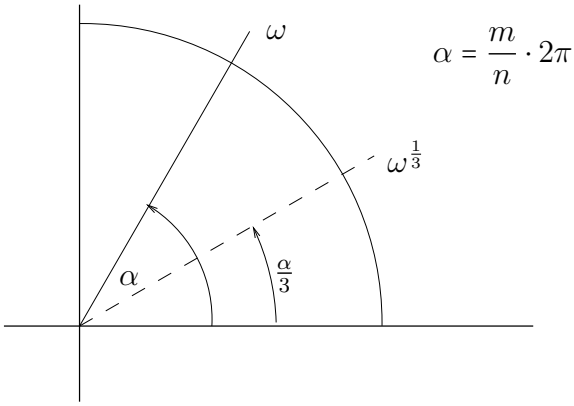
Wir erhalten

**24.7** Sei $n = p_1^{r_1} \cdot \ldots \cdot p_k^{r_k}$ die Primfaktorzerlegung von $n$. Dann gilt

$$\varphi(n) = \prod_{i=1}^{k}(p_i - 1) \cdot p^{r_i - 1} = n \cdot \prod_{i=1}^{k}(1 - \frac{1}{p_i}).$$

**24.8 Satz:** Ein rationaler Winkel $\frac{m}{n} \cdot 2\pi$ kann genau dann mit Zirkel und Lineal gedrittelt werden, wenn $3 \nmid n$ ist.

**Beweis:**: Sei $\omega = \cos(\frac{m}{n}2\pi) + i\sin(\frac{m}{n}2\pi)$ und $\zeta = \cos(\frac{2\pi}{n}) + i\sin(\frac{2\pi}{n})$, also $\omega = \zeta^m$. Wir müssen $\omega^{\frac{1}{3}}$ aus $M = \{0, 1, \omega\}$ konstruieren.




Da $ggT(m, n) = 1$ ist, ist $\omega$ primitive $n$-te Einheitswurzel. Es folgt $\mathbb{Q}(M) = \mathbb{Q}(\omega) = \mathbb{Q}(\zeta)$. Da $\overline{\zeta} = \zeta^{n-1} \in \mathbb{Q}(\zeta)$, ist $\mathbb{Q}(M) = \mathbb{Q}(M \cup \overline{M})$. Ist $3|m$, so ist $\omega^{\frac{1}{3}} = \zeta^{\frac{m}{3}}$ aus $\mathbb{Q}(M)$ konstruierbar.

Ist $3 \nmid m$, so ist $ggT(m, 3n) = 1$. Da $\zeta^{\frac{1}{3}}$ primitive $(3n)$-te Einheitswurzel ist, ist auch $\omega^{\frac{1}{3}}$ eine primitive $(3n)$-te Einheitswurzel. Also ist $\omega^{\frac{1}{3}}$ genau dann aus $\mathbb{Q}(M)$ konstruierbar, wenn $\zeta^{\frac{1}{3}}$ aus $\mathbb{Q}(\zeta)$ konstruierbar ist. Aus

$$\mathbb{Q} \subset \mathbb{Q}(M) = \mathbb{Q}(\zeta) \subset \mathbb{Q}(\zeta^{\frac{1}{3}})$$

erhalten wir

$$[\mathbb{Q}(\zeta^{\frac{1}{3}}) : \mathbb{Q}] = [\mathbb{Q}(\zeta^{\frac{1}{3}}) : \mathbb{Q}(\zeta)] \cdot [\mathbb{Q}(\zeta) : \mathbb{Q}].$$

Ist $\varphi$ die Euler'sche Phi-Funktion, übersetzt sich diese Gleichung in

$$k := [\mathbb{Q}(\zeta^{\frac{1}{3}}) : \mathbb{Q}(\zeta)] = \frac{\varphi(3n)}{\varphi(n)}.$$

Sei $n = 3^r \cdot l$ und $3 \nmid l$. Dann gilt $\varphi(n) = \varphi(3^r) \cdot \varphi(l)$ und $\varphi(3n) = \varphi(3^{r+1}) \cdot \varphi(l)$, so dass

$$k = \frac{\varphi(3^{r+1})}{\varphi(3^r)} = \begin{cases} 2 & r = 0 \\ 3 & r > 0, \end{cases}$$

denn $\varphi(p^r) = (p-1)\cdot p^{r-1}$ für jede Primzahl $p$.

Da $\mathbb{Q}(\zeta) = \mathbb{Q}(M \cup \overline{M})$ ist, folgt aus 24.4, dass $\omega^{\frac{1}{3}}$ genau dann aus $\{0,1,\omega\}$ konstruiert werden kann, wenn $r = 0$ ist. □

Wenden wir uns jetzt der Konstruktion regulärer $n$-Ecke zu.

**24.9 Bemerkung:** Es gilt folgende Verallgemeinerung von Satz 24.8: Sei $p$ prim. Dann kann ein rationaler Winkel $\frac{m}{n}\cdot 2\pi$ genau dann mit Zirkel und Lineal durch $p$ geteilt werden, wenn $p$ eine Fermat'sche Primzahl ist und $p \nmid n$.

Die Notwendigkeit dieser Bedingung folgt wie im Beweis von 24.8. Beim Beweis, dass diese Bedingung auch hinreichend ist, kann man wie im Beweis von 24.12 vorgehen.

Wenden wir uns jetzt der Konstruktion regulärer $n$-Ecke zu.

**24.10 Aufgabe:** (1) Ist das reguläre $n$-Eck konstruierbar, dann ist auch das reguläre $(2^s\cdot n)$-Eck mit $s \in \mathbb{N}$ konstruierbar.

(2) Ist $n = k\cdot l$ mit $k,l > 2$ und ist das reguläre $n$-Eck konstruierbar, dann ist auch das reguläre $k$-Eck und $l$-Eck konstruierbar.

(3) Sind das reguläre $k$-Eck und das reguläre $l$-Eck konstruierbar, und ist $\mathrm{ggT}(k,l) = 1$, dann ist das reguläre $(k\cdot l)$-Eck konstruierbar.

Also genügt zu untersuchen, wann das reguläre $p^k$-Eck konstruiert werden kann, wobei $p > 2$ eine Primzahl ist.

**24.11 Aufgabe:** Ist $p$ eine Primzahl der Form $p = 2^s + 1$, dann ist $p$ eine Fermat'sche Primzahl.

**24.12 Satz:** (Carl Friedrich Gauß, 1777-1855) Das reguläre $n$-Eck ist genau dann mit Zirkel und Lineal konstruierbar, wenn $n = 2^s\cdot p_1\cdot\ldots\cdot p_k$, wobei $p_i$ **verschiedene** Fermat'sche Primzahlen sind.

**Beweis:** Sei $n = p_1^{k_1}\cdot\ldots\cdot p_t^{k_t}$ die Primfaktorzerlegung von $n$. Das reguläre $n$-Eck ist genau dann konstruierbar, wenn jedes reguläre $(p_i^{k_i})$-Eck konstruierbar ist. Wir fragen uns also:

Wann ist das reguläre $p^k$-Eck, $p$ prim, konstruierbar?

Sei $\zeta = \cos\left(\frac{2\pi}{p^k}\right) + i\sin\left(\frac{2\pi}{p^k}\right)$. Wir müssen $\zeta$ aus $\mathbb{Q}$ konstruieren. Da

$$[\mathbb{Q}(\zeta):\mathbb{Q}] = \varphi(p^k) = (p-1)\cdot p^{k-1}$$

nach 21.10 und 21.11 muss $(p-1)\cdot p^{k-1}$ eine Potenz von 2 sein nach 24.5. Wir erhalten

**Notwendige Bedingung:**

(i) $p = 2$ oder

(ii) $p > 2,\ k = 1,\ p-1 = 2^s$, d.h. $p = 2^s + 1$.

Dies ist nach 24.11 die Bedingung des Satzes.

**Die Bedingung ist auch hinreichend:** Nach 21.3 ist $\mathbb{Q}(\zeta)/\mathbb{Q}$ Galois-Erweiterung. Die Galoisgruppe $G$ ist eine 2-Gruppe, da

$$|G| = [\mathbb{Q}(\zeta) : \mathbb{Q}] = 2^s.$$

Nach den Sylowsätzen gibt es einen Turm von Untergruppen

$$\{\mathrm{id}\} = U_0 < U_1 < \ldots < U_s = G$$

mit $|U_i| = 2^i$. Damit erhalten wir Zwischenkörper

$$\mathbb{Q} = \mathbb{Q}(\zeta)^G \subset \mathbb{Q}(\zeta)^{U_{s-1}} \subset \ldots \subset \mathbb{Q}(\zeta)^{U_0} = \mathbb{Q}(\zeta),$$

und nach 18.13 und 19.6 gilt

$$[\mathbb{Q}(\zeta)^{U_i} : \mathbb{Q}^{U_{i+1}}] = [U_{i+1} : U_i] = 2.$$

Nach 24.4 ist $\zeta$ aus $\mathbb{Q}$ konstruierbar. □

Fermat vermutete 1650, dass alle Fermat'schen Zahlen prim sind. Das ist richtig für $F_0 = 3$, $F_1 = 5$, $F_2 = 17$, $F_3 = 257$, $F_4 = 65537$, aber $F_5 = 641 \cdot 6700417$, wie Euler 1732 zeigte.

Außer $F_0, \ldots, F_4$ sind keine weiteren Fermat'schen Primzahlen bekannt.

**24.13** Kurze Geschichte der Konstruktionen:

Euklid (~325-265 v.Chr.) kannte die Konstruktionen von Dreieck, Quadrat und regulärem 5-Eck.

Erchinger konstruierte auf der Basis der Ergebnisse von Gauß um 1800 herum das reguläre 17-Eck.

Richelot und unabhängig davon Schwendenwein konstruierten gegen 1890 das 257-Eck.

Hermes beschäftigte sich um 1900 ganze 10 Jahre lang mit der Konstruktion des 65537-Ecks, führte sie aber nicht durch.

Bishop hat 1978 die Konstruktion computerisiert.

# 25 Einfache Erweiterungen

In 16.15 und dessen Beweis (s. 16.16) haben wir gezeigt

**25.1 Satz:** Ist $F = K[\alpha_1, \alpha_2, \ldots, \alpha_r]$ endliche Erweiterung von $K$ und sind $\alpha_2, \ldots, \alpha_r$ separabel über $K$, dann gibt es ein

$$\gamma = \alpha_1 + c_2\alpha_2 + \ldots + c_r\alpha_r \text{ mit } c_i \in K,$$

so dass $F = K[\gamma]$.

Wie findet man ein solches primitives Element $\gamma$? Wir zeigen

**25.2 Satz:** Sei $K \subset F = K[\alpha_1, \alpha_2, \ldots, \alpha_r]$ eine endliche Galois-Erweiterung (insbesondere sind alle $\alpha_i$ separabel über $K$), und sei

$$\gamma = \alpha_1 + c_2\alpha_2 + \ldots + c_r\alpha_r \text{ mit } c_i \in K.$$

Gilt für alle $\sigma \neq \mathrm{id}$ aus $\mathrm{Gal}(F/K)$, dass $\sigma(\gamma) \neq \gamma$, dann ist $\gamma$ primitiv, d.h. $F = K[\gamma]$.

**Beweis:** $K \subset K(\gamma) \subset F$. Nach 19.6 ist $K(\gamma)$ Fixkörper einer Untergruppe von $\mathrm{Gal}(F/K)$. Da aber id der einzige $K$-Automorphismus ist, der $\gamma$ festlässt, folgt $K(\gamma) = F^{\{\mathrm{id}\}} = F$. □

**25.3 Beispiel:** $\mathbb{Q} \subset \mathbb{Q}[\sqrt{2}, \sqrt{3}]$.
$\dim_{\mathbb{Q}} \mathbb{Q}[\sqrt{2}, \sqrt{3}] = 4$, denn $X^2 - 2$ ist das Minimalpolynom von $\sqrt{2}$ über $\mathbb{Q}$, und $X^2 - 3$ das Minimalpolynom von $\sqrt{3}$ über $\mathbb{Q}[\sqrt{2}]$ (warum?). Da beide Polynome in $\mathbb{Q}[\sqrt{2}, \sqrt{3}]$ zerfallen und separabel sind, ist $\mathbb{Q} \subset \mathbb{Q}[\sqrt{2}, \sqrt{3}]$ Galois. Die Galoisgruppe $G$ ist

$$G = \langle\sigma\rangle \times \langle\tau\rangle \cong \mathbb{Z}/2 \times \mathbb{Z}/2$$

mit $\sigma(\sqrt{2}) = -\sqrt{2}$ $\qquad$ $\tau(\sqrt{2}) = \sqrt{2}$
$\sigma(\sqrt{3}) = \sqrt{3}$ $\qquad$ $\tau(\sqrt{3}) = -\sqrt{3}$

$\gamma = \sqrt{2} + \sqrt{3}$ ist primitiv, denn

$$\begin{aligned} \sigma(\gamma) &= -\sqrt{2} + \sqrt{3} \neq \gamma \\ \tau(\gamma) &= \sqrt{2} - \sqrt{3} \neq \gamma \\ \sigma \circ \tau(\gamma) &= -\sqrt{2} - \sqrt{3} \neq \gamma. \end{aligned}$$

□

# 26 Der Fundamentalsatz der Algebra

Wir wollen in diesem Abschnitt den Fundamentalsatz der Algebra beweisen. Bis heute ist kein rein algebraischer Beweis bekannt. In unserem Beweis machen wir Anleihen aus der Analysis, die aber von sehr elementarem Charakter sind: Sie folgen direkt aus dem Zwischenwertsatz, der allerdings das Vollständigkeitsaxiom voraussetzt.

**26.1 Anleihen aus der Analysis:**

(1) Zu $a \geq 0$ aus $\mathbb{R}$ existiert $\sqrt{a} \in \mathbb{R}$.

(2) Jedes Polynom $f$ von ungeradem Grad hat eine reelle Nullstelle.

**26.2 Theorem:** $\mathbb{C}$ ist algebraisch abgeschlossen.

**Beweis:** $\mathbb{C}$ ist der Zerfällungskörper von $X^2+1 \in \mathbb{R}[X]$. Sei $i$ Nullstelle von $X^2+1$, so dass $\mathbb{C} = \mathbb{R}[i]$. Nach 14.12 genügt es zu zeigen, dass jedes $f \in \mathbb{R}[X]$ über $\mathbb{C}$ in Linearfaktoren zerfällt.

**Behauptung:** Sei $z = a + bi \in \mathbb{C}$, $a, b \in \mathbb{R}$. Dann existiert $\sqrt{z}$ in $\mathbb{C}$.

**Beweis:** Nach Anleihe 26.1 existieren

$$c = \pm\sqrt{\frac{a+\sqrt{a^2+b^2}}{2}} \qquad d = \pm\sqrt{\frac{-a+\sqrt{a^2+b^2}}{2}}$$

$c^2 - d^2 = a$, $(2cd)^2 = b^2$. Wir wählen die Vorzeichen von $c$ und $d$ so, dass $cd$ und $b$ dasselbe Vorzeichen haben. Dann gilt

$$(c+di)^2 = c^2 - d^2 + 2cdi = a + bi = z.$$

Sei nun $f \in \mathbb{R}[X]$ und $Z$ der Zerfällungskörper von $f \cdot (X^2+1)$. Wir müssen zeigen, dass $Z \subset \mathbb{C}$. Da $\operatorname{char}\mathbb{R} = 0$, ist $f \cdot (X^2+1)$ separabel. Also ist $\mathbb{R} \subset Z$ eine Galoiserweiterung. Sei $G$ die Galoisgruppe und $H < G$ eine 2-Sylowgruppe.

Sei $L = Z^H$. Dann gilt nach Theorem 19.6

$$[G : H] = [Z^H : Z^G] = [L : \mathbb{R}].$$

Also ist $\dim_R L$ ungerade. Nach 16.15 gibt es ein $\alpha \in L$ mit $L = \mathbb{R}[\alpha]$.

Der Grad des Minimalpolynoms $g$ von $\alpha$ ist ungerade; damit hat das Minimalpolynom eine reelle Nullstelle. Da $g$ irreduzibel ist, ist es linear. Es folgt $L = \mathbb{R}$ und damit $G = H$.

Da $\mathbb{R} \subset \mathbb{C} \subset Z$, ist $\mathrm{Gal}(Z/\mathbb{C})$ eine 2-Gruppe. Angenommen $\mathrm{Gal}(Z/\mathbb{C}) \neq \{\mathrm{id}\}$, dann besitzt $\mathrm{Gal}(Z/\mathbb{C})$ nach den Sylowsätzen eine Untergruppe $N$ vom Index

2. Der Körper $Z^N$ hat damit den Grad 2 über $\mathbb{C}$, d.h. $Z^N = \mathbb{C}[\beta]$, wobei $\beta$ Nullstelle eines quadratischen Polynoms in $\mathbb{C}[X]$ ist. Nach Behauptung 1 liegen diese Nullstellen bereits in $\mathbb{C}$, so dass $Z^N = \mathbb{C}$, ein Widerspruch zu $\dim_{\mathbb{C}} Z^N = 2$. Es folgt $\mathrm{Gal}(Z/\mathbb{C}) = \{\mathrm{id}\}$ und damit $Z = \mathbb{C}$. □

**26.3 Folgerung:** (1) $\mathbb{C}$ ist der algebraische Abschluss von $\mathbb{R}$

(2) Der Körper $\mathbb{A}$ der algebraischen Zahlen ist ein algebraischer Abschluss von $\mathbb{Q}$.

**Beweis:** (1) folgt direkt aus der Definition des algebraischen Abhschlusses.
(2) folgt aus 14.11 und 14.12. □

# Teil V
# Anhang

## 27 Der Basissatz für abelsche Gruppen

Ziel des Anhangs ist der Beweis des folgenden Satzes:

**27.1 Basissatz für abelsche Gruppen:** Eine endlich erzeugte abelsche Gruppe ist ein Produkt zyklischer Gruppen. Genauer gibt es ein $r \in \mathbb{N}$ und Zahlen $\tau_1, \ldots, \tau_k \in \mathbb{N}\backslash\{0\}$, so dass

$$G \cong \mathbb{Z}^r \times \mathbb{Z}/\tau_1 \times \mathbb{Z}/\tau_2 \times \ldots \times \mathbb{Z}/\tau_k,$$

wobei $\tau_1|\tau_2|\ldots|\tau_k$.

**27.2 Lemma:** Ist $\varphi : G \to H$ ein Epimorphismus von Gruppen mit Kern $K$ und sind $K$ und $H$ endlich erzeugt, dann ist auch $G$ endlich erzeugt.

**Beweis:** Sei $K = \langle A \rangle$ und $H = \langle B \rangle$. Zu jedem $b \in B$ wählen wir ein $c \in G$ mit $\varphi(c) = b$.
$G$ zerfällt in Äquivalenzklassen $\overline{x} = x \cdot K$. Drücke $\overline{x}$ als Produkt von $b$'s aus $B$ aus; sei $y \in G$ das entsprechende Produkt der $c$. Dann ist $y \cdot K = x \cdot K$, weil $\overline{x} = \overline{y}$. Also ist jedes Element aus $g$ als Produkt von Elementen aus $C$ und aus $A$ (und deren Inversen) darstellbar, d.h.

$$G = \langle A \cup B \rangle \quad \text{mit } |A \cup B| = |A| + |B|.$$

□

**27.3 Lemma:** Jede Untergruppe $U$ von $\mathbb{Z}^n$ hat ein Erzeugendensystem mit höchstens $n$ Elementen.

**Beweis:** Induktion nach $n$.

Jede Untergruppe von $\mathbb{Z}$ wird von einem Element erzeugt.

Induktionsschritt: Sei $U$ Untergruppe von $\mathbb{Z}^n$. Betrachte

$$\begin{array}{ccccc} \mathbb{Z} & \longrightarrow & \mathbb{Z}^n & \xrightarrow{p} & \mathbb{Z}^{n-1} \\ & & \cup & & \cup \\ & & U & \xrightarrow{\overline{p}} & V \end{array}$$

$p(x_1, \ldots, x_n) = (x_2, \ldots, x_n)$ hat Kern $\mathbb{Z}$. Sei $V = p(U)$ und $\overline{p} = p|U|$. Dann ist Kern $\overline{p} = \mathbb{Z} \cap U$. Da $V$ von höchstens $n-1$ und $\mathbb{Z} \cap U$ von höchstens einem Elemente erzeugt wird, wird $U$ nach 27.2 von höchstens $n-1+1 = n$ Elementen erzeugt. □

Sei nun $G$ eine abelsche Gruppe, erzeugt von $g_1, \ldots, g_n \in G$. Dann ist

$$\mathbb{Z}^n \xrightarrow{\varphi} G,$$

definiert durch $\varphi(e_i) = g_i$, surjektiv, wobei $e_i = (0, 0, \ldots, 1, 0, \ldots, 0)$. Dann wird Kern $\varphi = K \subset \mathbb{Z}^n$ nach 27.3 von $m$ Elementen $k_1, \ldots, k_m$ mit $m \leq n$ erzeugt.

Sei

$$d : \mathbb{Z}^m \longrightarrow \mathbb{Z}^n$$

definiert durch $e_i \mapsto k_i \in K \subset \mathbb{Z}^n$. Wir erhalten eine sog. **exakte** Sequenz.

$$\mathbb{Z}^m \xrightarrow{d} \mathbb{Z}^n \xrightarrow{\varphi} G \longrightarrow 0$$

$d$ ist bzgl. der Standardbasen durch eine $(n \times m)$-Matrix $M(d)$ mit Koeffizienten aus $\mathbb{Z}$ gegeben. Wir wollen $M(d)$ durch Zeilen- und Spaltentransformationen diagonalisieren: Sei

(1) Sei $F_{ij}^n$ die Matrix, die aus der Einheitsmatrix $E_n$ durch Vertauschen der $i$-ten mit der $j$-ten Zeile entsteht.

(2) $G_i^n$ die Matrix, die aus $E_n$ durch Multiplikation der $i$-ten Zeile mit -1 entsteht.

(3) $E_{ij}^n(r)$, die Matrix, die aus $E_n$ dadurch entsteht, dass auf Position $(i, j)$, $i \neq j$, die 0 durch $r \in \mathbb{Z}$ ersetzt wird.

Da $\det(F_{ij}^n) = -1$, $\det(G_i^n) = -1$ und $\det(E_{ij}(r)) = 1$, haben diese Matrizen ganzzahlige Inverse und definieren Isomorphismen

$$\mathbb{Z}^n \longrightarrow \mathbb{Z}^n.$$

**27.4 Lemma:** Sei $M$ eine $(n \times m)$-Matrix. Dann gilt

(1) $M \cdot F_{ij}^m$ entsteht aus $M$ durch Vertauschen von $i$-ter und $j$-ter Spalte

(2) $F_{ij}^n \cdot M$ entsteht aus $M$ durch Vertauschen von $i$-ter und $j$-ter Zeile

(3) $M \cdot G_i^m$ entsteht aus $M$ durch Multiplikation der $i$-ten Spalte mit -1.

(4) $G_i^n \cdot M$ entsteht aus $M$ durch Multiplikation der $i$-ten Zeile mit -1.

(5) $M \cdot E_{ij}^m(r)$ entsteht aus $M$ durch Addition der $r$-fachen der $i$-ten Spalte zur $j$-ten

(6) $E_{ij}^n(r) \cdot M$ entsteht aus $M$ durch Addition der $r$-fachen der $j$-ten Zeile zur $i$-ten

**Beweis von 27.1:** Wir bringen durch Zeilen- und Spaltenoperationen unsere Matrix $M(d) = (a_{ij})$ auf die Form

$$\begin{pmatrix} \tau_1 & & & \\ & \ddots & & \\ & & \tau_k & \\ & & & \\ 0 & \cdots & 0 & \end{pmatrix} \qquad \text{mit} \tau_1 | \tau_2 | \ldots | \tau_k$$

Ist $M(d) = (0)$ sind wir fertig. Sonst bringen wir sie in die Form

$$C = \left(\begin{array}{c|ccc} \tau_1 & 0 & \cdots & 0 \\ \hline 0 & & & \\ \vdots & & (d_{ij}) & \\ 0 & & & \end{array}\right), \quad \text{so dass } \tau_1 | d_{ij} \ \forall i, j$$

und iterieren.

Durch Zeilen- und Spaltenvertauschen erreichen wir, dass $a_{11} \neq 0$ und von minimalem positiven Betrag ist.

Gibt ein $a_{1j}$, so dass $a_{11} \nmid a_{1j}$, teilen wir mit Rest

$$a_{1j} = q \cdot a_{11} + r_1$$

Dann ziehen wir das $a_{11}$-fache der ersten Spalte von der $j$-ten ab und tauschen die erste mit der $j$-ten Spalte. Wir erhalten eine neue Matrix $(b_{ij})$ mit $0 < |b_{11}| = |r_1| < |a_{11}|$.

Wir führen den entsprechenden Prozess für die erste Zeile durch und iterieren solange, bis das neue $a_{11}$ alle anderen $a_{1j}$ teilt.

Dann ziehen wir geeignete Vielfache der ersten Spalte von den übrigen ab um in der ersten Zeile, außer an Position $(1,1)$ Nullen zu erzeugen.Entsprechend verfahren wir mit der ersten Spalte.

Wir erhalten eine Matrix der Form $C$ ohne die Zusatzbedingung. Gibt es ein $d_{ij}$, so dass $c_{11} \nmid d_{ij}$ addieren wir die $i$-te Zeile zur ersten und beginnen wieder wie oben.

Wir fahren fort, bis wir die gewünschte Form $D$ haben.

$$D = A \cdot M \cdot B \qquad A \in M_{n,n}(\mathbb{Z}),\ B \in M_{m,m}(\mathbb{Z})$$

Wir erhalten

$$\begin{array}{ccccc} \mathbb{Z}^m & \xrightarrow{M} & \mathbb{Z}^n & \xrightarrow{\varphi} & G \\ \cong\downarrow B^{-1} & \curvearrowright & \cong\downarrow A & & \downarrow\psi \\ \mathbb{Z}^m & \xrightarrow{D} & \mathbb{Z}^n & \xrightarrow{p} & \mathbb{Z}^n/\operatorname{Bild} D = H \end{array}$$

wobei $\psi(g) = \overline{A(z)}$ mit $\varphi(z) = g$.

$\psi$ ist wohldefiniert: Denn sei $\varphi(z_1) = \varphi(z_2)$, also $z_1 = z_2 + k$mit $k \in \operatorname{Kern}\varphi$, folgt

$$\overline{A(z_1)} = \overline{A(z_2 + k)} = \overline{A(z_2)} + \overline{A(k)}$$

Dann $\exists\, w \in Z^m$ mit $M(w) = k$. Es folgt $A \cdot M(w) = D \cdot B^{-1}(w)$ also

$$\overline{A(k)} = \overline{D \cdot B^{-1}(w)} = \overline{0}.$$

Da $A$ und $B^{-1}$ Isomorphismen sind, ist $\psi$ ein Isomorphismus. Es folgt

$$G \cong \mathbb{Z}/\tau_1 \oplus \mathbb{Z}/\tau_2 \oplus \ldots \oplus \mathbb{Z}/\tau_m \oplus \mathbb{Z}^{n-m}.$$

(Es kann sein, dass einige der $\tau_i = 0$ sind.)

**27.5 Bemerkung:** Der Beweis des Basissatzes macht nur vom euklidischen Restesatz Gebrauch und lässt sich daher verbatim auf Moduln über euklidischen Ringen übertragen. Die einzige Änderung ist, dass man Matrizen $G_i^n(c)$ zulässt, die aus $E_n$ durch Multiplikation der $i$-ten Zeile mit einer Einheit $c$ entsteht.

Wir erhalten dann folgenden Satz:

**27.6 Satz:** Sei $R$ ein euklidischer Ring und $M$ ein endlich erzeugter $R$-Modul. Dann gibt es ein $r \in \mathbb{N}$ und Elemente $q_1, \ldots q_k$ in $R$, so dass $q_1 | \, q_2 | \ldots | q_k$, sowie einen $R$-linearen Isomorphismus

$$M \cong R^r \oplus R/(q_1) \oplus \ldots \oplus R/(q_k)$$

**27.7 Bemerkung:** Satz 27.6 gilt auch für Hauptidealringe, der Beweis ist aber komplizierter.