

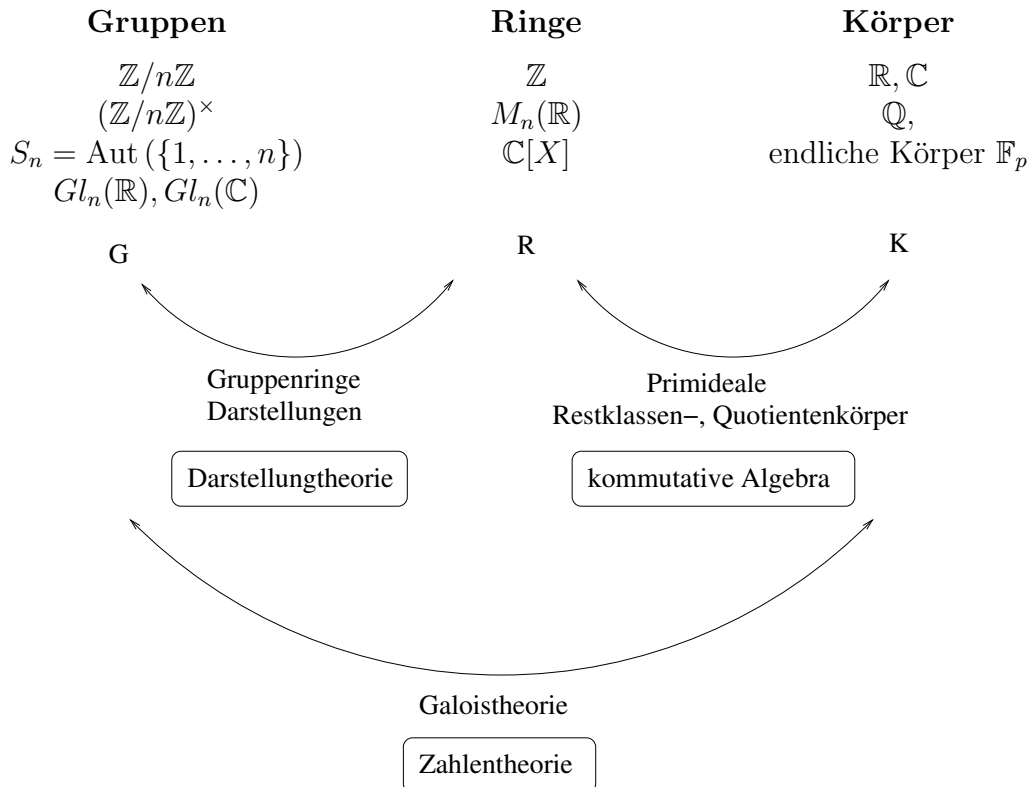
# Algebra

Prof. Dr. Uwe Jannsen Wintersemester 2006/2007

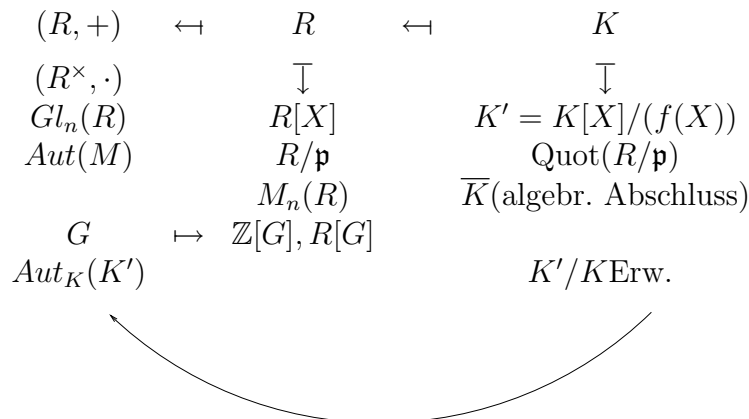
## §0 Einführung

### Überblick

Die zentralen Themen der Algebra sind



Wie angedeutet, gibt es unzählige Beziehungen zwischen diesen Objekten, und vor allem unzählige **Konstruktionen**, auf die man in ganz natürlicher Weise geführt wird.



Historisch entstanden die obigen Objekte und Beziehungen vor allem aus dem Studium der algebraischen Gleichungen

$$a_n X^n + a_{n-1} X^{n-1} + \dots + a_1 X + a_0 = 0$$

Beachte: Sind  $a_i \in \mathbb{Z}$ , so ist die Gleichung im allgemeinen nicht mit  $x \in \mathbb{Q}$  lösbar.

Kriterien? Beschreibung der Lösungen?

- Führt auf – Primelemente/- ideale in Polynomringen
- Erweiterungskörper
- Galoistheorie
- (algebraische) Zahlentheorie

$n = 2$

$$x^2 + pX + q = 0$$

$$x_{1,2} = -\frac{p}{2} \pm \sqrt{\frac{p^2}{4} - q}$$

Gibt es ähnliche (Wurzel-) Formeln für  $n \geq 3$ ? (“Auflösbarkeit von Gleichungen  $n$ -ten Grades”)

- $n = 3$  Cardano 1535 (gestohlen von Tartaglia)  $\rightarrow$  komplexe Zahlen
- $\uparrow$  Ferrari
- $n = 4$
- $n \geq 5$  Galois (1811-1832) Behandlungen durch endliche Gruppen
- Abel 1824 Gleichung i.a. nicht auflösbar ( $\Leftrightarrow S_n$  nicht auflösbar)

Weitere Anwendungen der Galoistheorie: die 3 klassischen Probleme des Altertums:

Quadratur des Kreises  
Trisektion des Winkels  
Verdopplung des Würfels

$\left( \begin{array}{c} \text{mit} \\ \text{Zirkel} \\ \text{und} \\ \text{Lineal} \end{array} \right)$  ist **nicht möglich**.

Positive Anwendungen: auf die Beschreibung aller Körpererweiterungen eines gegebenen Grundkörpers  $K$ .

### Ausblick

1) Beschreibung aller endlichen Körpererweiterungen von  $\mathbb{Q}$  (der sogenannten Zahlkörper) und der damit zusammenhängenden Arithmetik: Programm der **Algebraischen Zahlentheorie**.

abelsche Erweiterungen: Klassenkörpertheorie

beliebige Erweiterungen:

- Darstellungen: Langlandstheorie
- Struktur von  $Gal(\overline{\mathbb{Q}}/\mathbb{Q})$ : Galoiskohomologie, Isawatheorie

2) Betrachtet man Gleichungen in mehreren Variablen, z.B. die Fermat-Gleichung

$$X^n + Y^n = Z^n$$

oder die Gleichung einer elliptischen Kurve

$$y^2 = x^3 + 1,$$

so ist es nicht klar, wieviele Lösungen es im Körper  $K$  gibt (keine, endlich viele, unendlich viele?). In einem algebraisch abgeschlossenen Körper gibt es immer unendlich viele Lösungen; die Lösungen bilden die Punkte eines geometrischen Gebildes, wie zum Beispiel einer Kurve oder Fläche. Allgemein erhalten wir eine algebraische Varietät. Dies führt auf die **Algebraische Geometrie**.

3) Betrachtet man spezielle Grundkörper, so führt dies auf arithmetische Fragen.

Über  $\mathbb{Z}, \mathbb{Q}$ , bzw. Zahlkörpern:      diophantische Gleichungen  
mit Bewertungen, Abschätzungen      diophantische Geometrie

Allgemein erhält man durch die Verbindung von algebraischer Zahlentheorie und algebraischer Geometrie die **Arithmetische Geometrie**.

### Voraussetzungen:

Grundbegriffe aus der Linearen Algebra, insbesondere:

(i) Grundbegriffe über Mengen und Abbildungen  $M \cap N, M \cup N, M \times N$

Abbildung  $f : M \rightarrow N$ , Injektivität, Surjektivität, Bijektivität

Familien  $(a_i)_{i \in I}$

$\bigcup_{i \in I} M_i, \bigcap_{i \in I} M_i, \prod_{i \in I} M_i$

Äquivalenzrelationen  $\sim$  und Äquivalenzklassen  $\bar{a} = \{b \in M \mid b \sim a\}$

(ii) Gruppen  $(G, \circ)$ , Untergruppen  $U$ , Gruppenhomomorphismen  $\varphi : G \rightarrow G', \ker \varphi \subseteq G, \text{im } \varphi \subseteq G'$

(iii) Grundbegriffe über Ringe und Körper

(iv) Grundbegriffe über Vektorräume und lineare Abbildungen

### Vorbemerkungen:

1) Für eine Menge  $M$  sei  $|M|$  ihre Mächtigkeit (oder Kardinalität; dies ist eine natürliche Zahl  $n \in \mathbb{N}_0$  oder  $\infty$ ). Die folgende Sprechweise unterscheidet noch feiner: Wir sagen, dass zwei Mengen  $M$  und  $N$  gleichmächtig sind (Bezeichnung  $|M| = |N|$ ), wenn es eine Bijektion  $f : M \rightarrow N$  gibt. Dann gilt zum Beispiel

$$|\mathbb{N}| \neq |\mathbb{R}|;$$

dies ist der Unterschied zwischen abzählbarer unendlich ( $|\mathbb{N}|$ ) und überabzählbarer unendlich (z.B.  $|\mathbb{R}|$ ). Man definiert wie folgt Summe, Produkt und Potenz von solchen **Kardinalzahlen**:

$$\begin{aligned} |M| + |N| &= |M \cup N| \\ |M| \cdot |N| &= |M \times N| \\ |M|^{|N|} &= |M^N|, \end{aligned}$$

wobei  $M^N = \text{Abb}(N, M)$  die Menge der Abbildungen von  $N$  nach  $M$  ist (also der Familien in  $M$  über  $N$ ). Für endliche Mengen gibt dies die üblichen Rechenregeln.

2) Ist  $\sim$  eine Äquivalenzrelation auf der Menge  $M$ , so ist ein Repräsentantensystem für  $\sim$  (oder für  $M/\sim$ ) eine Familie  $(m_i)_{i \in I}$  in  $M$ , so dass es für jede Äquivalenzklasse  $\bar{m}$  bezüglich  $\sim$  genau ein  $i \in I$  gibt mit  $\bar{m}_i = \bar{m}$ . Mit anderen Worten: man hat eine Bijektion

$$\begin{aligned} \varphi: I &\rightarrow M/\sim \\ i &\mapsto \bar{m}_i \end{aligned}$$

(insbesondere gilt  $|I| = |M/\sim|$ ), und  $\varphi^{-1}$  liefert einen Schnitt von  $\pi: M \rightarrow M/\sim$ , d.h.,  $\pi\varphi^{-1} = \text{id}$ . Aus dem Auswahlaxiom (das wir annehmen wollen) folgt, dass es immer ein Repräsentantensystem gibt.

## §1 Normalteiler und Faktorgruppen

Für eine Teilmenge  $U$  einer Gruppe  $G$  schreiben wir auch  $U \leq G$ , wenn  $U$  eine Untergruppe ist.

**Definition 1.1** Sei  $G$  eine Gruppe und  $U \leq G$  eine Untergruppe. Für  $a \in G$  heißt die Menge

$$aU = \{au \mid u \in U\}$$

die Linksnebenklasse von  $a$  (bezüglich  $U$ ) und

$$Ua = \{ua \mid u \in U\}$$

die Rechtsnebenklasse.

**Satz 1.2** (a) Zwei Linksnebenklassen  $aU$  und  $bU$  sind entweder identisch oder disjunkt.

(b)  $G$  ist die disjunkte Vereinigung von Linksnebenklassen.

Dasselbe gilt für Rechtsnebenklassen.

Dies folgt aus den Eigenschaften von Äquivalenzrelationen und

**Lemma 1.3** Betrachte die folgende Relation  $\sim_U$  (bzw.  $U\sim$ )

$$a \sim_U b \quad :\Leftrightarrow \quad b^{-1}a \in U \quad \text{bzw.} \quad a U\sim b \quad :\Leftrightarrow \quad ab^{-1} \in U$$

Dies ist eine Äquivalenzrelation, und die Äquivalenzklasse von  $a \in G$  ist  $aU$  (bzw.  $Ua$ ).

**Beweis** für  $\sim = U\sim$ :  $a^{-1}a = e \in U \Rightarrow a \sim a$

$a \sim b \Rightarrow b^{-1}a \in U \Rightarrow a^{-1}b = (b^{-1}a)^{-1} \in U \Rightarrow b \sim a$

$a \sim b \sim c \Rightarrow b^{-1}a \in U, c^{-1}b \in U \Rightarrow c^{-1}a = c^{-1}bb^{-1}a \in U$

$\Rightarrow a \sim c$ .

Schließlich ist  $b \sim a \Leftrightarrow a^{-1}b \in U \Leftrightarrow b = au, u \in U \Leftrightarrow b \in aU$ .

Der Beweis für  $U\sim$  ist analog.

Es bezeichne  $G/U$  (bzw.  $U \setminus G$ ) die Menge der Linksnebenklassen (bzw. Rechtsnebenklassen), also die Menge  $G / \sim_U$  (bzw.  $G/U \sim$ ) der obigen Äquivalenzklassen.

**Lemma 1.4** Die Bijektion

$$i : G \rightarrow G \quad , \quad g \mapsto g^{-1}$$

induziert eine Bijektion

$$\bar{i} : G/U \rightarrow U \setminus G .$$

**Beweis** Expizit bildet  $\bar{i}$  die Restklasse  $aU$  ab auf

$$\begin{aligned} \bar{i}(aU) &= i(aU) = \{u^{-1}a^{-1} \mid u^{-1} \in U\} \\ &= \{ua^{-1} \mid u \in U\} = Ua^{-1} . \end{aligned}$$

Die inverse Abbildung ist die ebenfalls von  $i$  induzierte Abbildung

$$\begin{aligned} \bar{i} : U \setminus G &\rightarrow G/U \\ Ua &\mapsto i(Ua) = a^{-1}U . \end{aligned}$$

**Definition 1.5** Die Mächtigkeit  $|G|$  einer Gruppe  $G$  heißt die Ordnung von  $G$ . Für eine Untergruppe  $U \leq G$  heißt die Mächtigkeit  $|G/U| = |U \setminus G|$  der Index von  $U$  in  $G$ , Bez.  $(G : U)$ .

**Satz 1.6** (von Lagrange) ist  $U \leq G$  eine Untergruppe der Gruppe  $G$ , so ist

$$|G| = |U| \cdot (G : U) .$$

**Beweis** Sei  $(g_i)_{i \in I}$  ein Repräsentantensystem von  $G/U$  (so dass  $|I| = |G/U| = (G : U)$ ). Dann ist

$$\begin{aligned} \varphi : I \times U &\rightarrow G \\ (i, u) &\mapsto g_i u \end{aligned}$$

eine Bijektion nach Satz 1.2 und dem folgenden

**Lemma 1.7** Die Abbildung

$$\begin{aligned} U &\rightarrow aU \\ u &\mapsto au \end{aligned}$$

ist eine Bijektion.

**Beweis** Die Surjektivität ist trivial, und aus  $au = au'$  folgt  $u = u'$  durch Linksmultiplikation mit  $a^{-1}$ .

Sind zwei der drei Mächtigkeiten in 1.6 endlich, so auch die dritte, und die Gleichheit ist eine Gleichheit von natürlichen Zahlen. Insbesondere gilt:

**Corollar 1.8** ist  $G$  eine endliche Gruppe und  $U$  eine Untergruppe, so ist  $|U|$  ein Teiler von  $|G|$ .

**Lemma/Definition 1.9** Eine Untergruppe  $N \leq G$  einer Gruppe  $G$  heißt Normalteiler (Bez.  $N \trianglelefteq G$ ), wenn die folgenden äquivalenten Bedingungen erfüllt sind

- (i)  $gNg^{-1} \subset N$  für alle  $g \in G$ .
- (ii)  $gNg^{-1} = N$  für alle  $g \in G$ .
- (iii)  $gN = Ng$  für alle  $g \in G$ .

**Beweis** (i)  $\Rightarrow$  (ii): aus  $gNg^{-1} \subset N$  folgt durch Multiplikation mit  $g^{-1}$  von links und  $g$  von rechts

$$N \subset g^{-1}Ng \quad \forall g \in G.$$

Durch Betrachtung von  $g^{-1}$  folgt hieraus  $N \subset gNg^{-1}$ , also (ii).

$$\begin{aligned} \text{(ii)} \Rightarrow \text{(iii)}: \quad x \in gN &\Rightarrow g^{-1}x \in N = g^{-1}Ng \Rightarrow x \in Ng \\ x \in Ng &\Rightarrow xg^{-1} \in N = gNg^{-1} \Rightarrow x \in gN \end{aligned}$$

$$\text{(iii)} \Rightarrow \text{(i)}: \quad x \in gNg^{-1} \Rightarrow xg \in gN = Ng \Rightarrow x \in N.$$

**Beispiele 1.10** (a)  $\{1\}$  und  $G$  sind immer Normalteiler in  $G$ .

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

(c) Die Untergruppe  $U_i = \{\sigma \in S_n \mid \sigma(i) = i\}$  ist kein Normalteiler von  $S_n$  für  $n \geq 3$ . (Übungsaufgabe!)

**Lemma 1.11** Ist  $\varphi : G \rightarrow G'$  ein Gruppenhomomorphismus, so ist für jeden Normalteiler  $N'$  von  $G'$  die Menge  $\varphi^{-1}(N')$  ein Normalteiler in  $G$ .

**Beweis** Ist  $h \in \varphi^{-1}(N')$ , so gilt für  $g \in G$

$$\varphi(ghg^{-1}) = \varphi(g)\varphi(h)\varphi(g)^{-1} \in N',$$

also  $ghg^{-1} \in \varphi^{-1}(N')$ .

**Corollar 1.12**  $\text{Ker } \varphi$  ist ein Normalteiler.

Die folgende Konstruktion zeigt, dass jeder Normalteiler so entsteht.

**Satz/Definition 1.13** Sei  $G$  eine Gruppe und  $N \trianglelefteq G$  ein Normalteiler.

(a) Es gibt genau eine Verknüpfung  $\cdot$  auf  $G/N = N \backslash G$  derart, dass gilt:

- (i)  $(G/N, \cdot)$  ist eine Gruppe.
- (ii) Die kanonische Surjektion  $\pi : G \rightarrow G/N$  ist ein Homomorphismus.  
 $g \mapsto gN$

(b)  $G/N$  mit dieser Verknüpfung heißt die Faktorgruppe von  $G$  modulo (oder nach)  $N$ .

(c) Es ist  $N = \text{ker}(\pi)$ , und in der Gruppe  $G/N$  ist die Nebenklasse  $eN = N$  das neutrale Element und  $a^{-1}N$  das Inverse von  $aN$ .

**Beweis** Soll  $\pi$  ein Homomorphismus sein, so gilt notwendigerweise

$$aN \cdot bN = \pi(a)\pi(b) = \pi(ab) = abN.$$

Dies zeigt die Eindeutigkeit der Verknüpfung. Als nächstes haben wir zu zeigen, dass diese Definition wohldefiniert ist. Ist aber  $a'N = aN$  und  $b'N = bN$ , so ist  $a^{-1}a' = n_1 \in N$  und  $b^{-1}b' = n_2 \in N$ , also

$$(ab)^{-1}(a'b') = b^{-1}(a^{-1}a')b' = b^{-1}(a^{-1}a')bb^{-1}b' = (b^{-1}n_1b)n_2 \in N,$$

da  $N$  ein Normalteiler ist. Es folgt  $a'b'N = abN$ . Aus den Gruppeneigenschaften von  $G$  folgt nun sofort, dass  $G/N$  eine Gruppe ist, wobei  $eN \cdot aN = aN = aN \cdot eN$  und  $a^{-1}N \cdot aN = eN = aN \cdot a^{-1}N$ . Schließlich gilt:

$$g \in \ker(\pi) \Leftrightarrow gN = eN = N \Leftrightarrow g \in N.$$

**Beispiel 1.14** Für  $m \in \mathbb{Z}$  ist  $m\mathbb{Z}$  ein Normalteiler in  $\mathbb{Z}$ , und die Faktorgruppe  $\mathbb{Z}/m\mathbb{Z}$  heißt die Gruppe der Restklassen modulo  $m$  (diese Gruppe wird auch mit  $\mathbb{Z}/m$ ,  $\mathbb{Z}_m$  oder  $Z_m$  bezeichnet). Bezeichnet  $\bar{a} = a + m\mathbb{Z}$  die Nebenklasse von  $a$ , die hier auch als Restklasse von  $a$  (modulo  $m$ ) bezeichnet wird (wegen der Beziehung zum Teilen durch  $m$  mit Rest), so gilt nach 1.12 die einfache Regel

$$\bar{a} + \bar{b} = \overline{a + b},$$

weiter ist  $\bar{0}$  das Nullelement, und das Inverse von  $\bar{a}$  ist  $\overline{-a}$ . Man rechnet also wie in  $\mathbb{Z}$ , wobei man immer zu anderen Repräsentanten der Restklasse übergehen kann. Für  $m = 5$  gilt z.B.

$$\left. \begin{array}{l} \bar{1} + \bar{2} = \bar{3} \\ \bar{3} + \bar{3} = \bar{6} = \bar{1} \\ \bar{4} + \bar{4} = \bar{8} = \bar{3} \end{array} \right\} \text{ in } \mathbb{Z}/5\mathbb{Z}$$

Offenbar bilden für  $m > 0$  die ganzen Zahlen  $0, 1, 2, \dots, m-1$  ein Repräsentantensystem von  $\mathbb{Z}/m\mathbb{Z}$ ; also ist

$$\mathbb{Z}/m\mathbb{Z} = \{\bar{0}, \bar{1}, \bar{2}, \dots, \overline{m-1}\}.$$

Man beachte, dass  $\overline{m-i}$  das Inverse von  $\bar{i}$  ist. Für  $a, b \in \mathbb{Z}$  schreibt man

$$a \equiv b \pmod{m} \quad (\text{oder } a \equiv b \pmod{m}, \text{ oder } a \equiv b(m))$$

und spricht “ $a$  ist kongruent zu  $b$  modulo  $m$ ”, wenn

$$a + m\mathbb{Z} = b + m\mathbb{Z} \quad (\Leftrightarrow \bar{a} = \bar{b} \Leftrightarrow a - b \in m\mathbb{Z}).$$

Man schreibt auch oft  $a \bmod m\mathbb{Z}$  (oder ähnliches) für  $a + m\mathbb{Z}$ .

Wie man im obigen Beispiel sieht, kann man sich  $G/N$  als eine Gruppe vorstellen, in der man “wie in  $G$  rechnet”, wobei man die “Elemente in  $N$  gleich Eins (bzw. Null) setzt”. Dies kann präzisiert werden:

**Satz 1.15** (universelle Eigenschaft der Faktorgruppe) Sei  $N \trianglelefteq G$  ein Normalteiler einer Gruppe  $G$ . Ist  $\varphi : G \rightarrow G'$  ein Gruppenhomomorphismus mit  $\varphi(n) = 1$  für alle  $n \in N$ ,

so gibt es genau einen Homomorphismus  $\bar{\varphi} : G/N \rightarrow G'$ , der das folgende Diagramm kommutativ macht (d.h., es gilt  $\varphi = \bar{\varphi} \circ \pi$ )

$$\begin{array}{ccc} G & \xrightarrow{\pi} & G/N \\ & \searrow \varphi & \swarrow \exists! \bar{\varphi} \\ & & G' \end{array} .$$

**Beweis** Eindeutigkeit: Aus der Kommutativität des Diagramms folgt

$$\bar{\varphi}(aN) = \bar{\varphi}(\pi(a)) = \varphi(a) \text{ für } a \in G .$$

Wohldefiniertheit: Ist  $aN = bN$ , so ist  $a = bn$  mit  $n \in N$ , und somit  $\varphi(a) = \varphi(bn) = \varphi(b)\varphi(n) = \varphi(b)$ .

Homomorphieeigenschaft: für  $a, b \in G$  ist  $\bar{\varphi}(aN \cdot bN) = \bar{\varphi}(abN) = \varphi(ab) = \varphi(a)\varphi(b) = \bar{\varphi}(aN)\bar{\varphi}(bN)$ .

**Lemma 1.16** In der obigen Situation ist  $\ker(\bar{\varphi}) = \ker(\varphi)/N$ , und  $\bar{\varphi}$  ist ein Epimorphismus, falls  $\varphi$  dies ist.

**Beweis** Wir bemerken zunächst, dass nach Voraussetzung

$$N \subset \ker(\varphi) ,$$

und dass für jede Untergruppe  $U$  von  $G$  mit  $N \subset U$  die Menge

$$U/N = \{uN \mid u \in U\}$$

offenbar eine Untergruppe von  $G/N$  bildet. Es gilt nun  $\bar{\varphi}(aN) = 1 \Leftrightarrow \varphi(a) = 1 \Leftrightarrow a \in \ker \varphi$  und damit die erste Aussage. Die letzte Aussage ist trivial.

**Satz 1.17** (Homomorphiesatz) Ist  $\varphi : G \rightarrow G'$  ein Gruppenhomomorphismus, so induziert  $\varphi$  einen Monomorphismus

$$\bar{\varphi} : G/\ker(\varphi) \hookrightarrow G' .$$

und einen Isomorphismus

$$\bar{\varphi} : G/\ker(\varphi) \xrightarrow{\sim} \text{im}(\varphi) .$$

**Beweis** Dies ist einfach der Fall  $N = \ker(\varphi)$  von Satz 1.15: Nach 1.16 ist dann  $\ker(\bar{\varphi}) = \ker(\varphi)/\ker(\varphi) = \{\ker(\varphi)\}$  die triviale Gruppe und damit  $\bar{\varphi}$  injektiv. Schränkt man rechts auf  $\text{im}(\varphi) = \text{im}(\bar{\varphi})$  ein, so ist die Abbildung auch surjektiv, woraus die zweite Behauptung folgt.

**Corollar 1.18** (Erster Isomorphiesatz) Sei  $G$  eine Gruppe,  $N \trianglelefteq G$  ein Normalteiler und  $H \leq G$  eine Untergruppe.

- (a)  $HN := \{hn \mid h \in H, n \in N\} = NH$  ist eine Untergruppe von  $G$ .
- (b)  $N$  ist ein Normalteiler von  $HN$ .

(c)  $H \cap N$  ist Normalteiler von  $H$ , und man hat einen Isomorphismus

$$\begin{aligned} H/H \cap N &\xrightarrow{\sim} HN/N \\ h(H \cap N) = \bar{h} &\mapsto \bar{h} = hN. \end{aligned}$$

**Beweis** (a): Sind  $x = hn$  und  $x' = h'n' \in HN$  ( $h, h' \in H, n, n' \in N$ ), so ist  $xx'^{-1} = hn(h'n')^{-1} = hnn'^{-1}h'^{-1} = hh'^{-1}h'nn'^{-1}h'^{-1} \in HN$ , da  $h'(nn'^{-1})h'^{-1} \in h'Nh'^{-1} \subset N$ .

(b) Wegen  $1 \in H$  ist  $N \subset HN$ , und  $N$  ist Normalteiler von jeder Untergruppe  $U \leq G$  mit  $N \subset U$ .

(c) Betrachte die Komposition

$$H \hookrightarrow G \xrightarrow{\pi} G/N.$$

Dies ist ein Homomorphismus (als Komposition von Homomorphismen) mit Bild  $HN/N$  und Kern  $H \cap N$ . Die Behauptung folgt dann mit dem Homomorphiesatz 1.17.

**Corollar 1.19** (Zweiter Isomorphiesatz) Sind  $M$  und  $N$  Normalteiler einer Gruppe  $G$ , mit  $M \subset N$ , so gilt

(a)  $N/M$  ist Normalteiler von  $G/M$ .

(b) Man hat einen Isomorphismus

$$\begin{aligned} (G/M)/(N/M) &\xrightarrow{\sim} G/N \\ \bar{g} = gM(N/M) &\mapsto \bar{g} = gN. \end{aligned}$$

**Beweis** Für den Epimorphismus  $G \xrightarrow{\pi} G/N$  hat man  $M \subset N = \ker(\pi)$  und damit, nach 1.15, einen induzierten Epimorphismus

$$\bar{\pi} : G/M \rightarrow G/N.$$

Dieser hat den Kern  $\ker(\bar{\pi})/M = N/M$ , und mit dem Homomorphiesatz 1.17 folgt die Behauptung.

## §2 Zyklische Gruppen

**Definition 2.1** Sei  $G$  eine Gruppe. Für eine Teilmenge  $M \subseteq G$  sei  $\langle M \rangle$  die kleinste Untergruppe von  $G$ , die  $M$  enthält. Sie heißt die von  $M$  erzeugte Untergruppe.

**Bemerkungen 2.2** (a) Siehe Übungsaufgabe 1 für eine explizite Beschreibung von  $\langle M \rangle$ .

(b) Für  $g \in G$  sei  $\langle g \rangle := \langle \{g\} \rangle$ , also die kleinste Untergruppe die  $g$  enthält. Dann ist

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

wobei  $g^n := g \dots g$  ( $n$ -mal) für  $n \in \mathbb{N}$ ,  $g^0 = 1$  und  $g^n = (g^{-1})^{|n|}$  für  $n < 0$ .

Dies folgt aus Übungsaufgabe 1 oder so: Offenbar enthält  $\langle g \rangle$  alle  $g^n$  ( $n \in \mathbb{Z}$ ). Weiter zeigt man leicht

$$(2.2.1) \quad \begin{aligned} g^m g^n &= g^{m+n} && \text{für } m, n \in \mathbb{Z}. \\ (g^m)^n &= g^{m \cdot n} && \text{für } m, n \in \mathbb{Z}. \end{aligned}$$

Hieraus folgt, dass  $\{g^n \mid n \in \mathbb{Z}\}$  eine Untergruppe von  $G$  ist.

(c) Ist  $A$  eine abelsche Gruppe und schreiben wir die Verknüpfung als  $+$ , so schreiben wir eher  $na$  statt  $a^n$ , also  $na = a + \dots + a$  ( $n$ -mal) für  $n \in \mathbb{N}$ ,  $0a = 0$ ,  $(-n)a = -(na)$  für  $n \in \mathbb{N}$ .

**Definition 2.3** Eine Gruppe  $G$  heißt zyklisch, wenn sie von einem Element erzeugt wird, d.h., wenn es ein  $g \in G$  gibt mit  $G = \langle g \rangle$  (ein solches  $g$  heißt dann erzeugendes Element von  $G$ ).

**Satz 2.4** Sei  $G$  eine zyklische Gruppe.

(a) Hat  $G$  unendliche Ordnung, so ist  $G$  isomorph zu  $\mathbb{Z}$ .

(b) Hat  $G$  die Ordnung  $m$  mit  $m \in \mathbb{N}$ , so ist  $G$  isomorph zu  $\mathbb{Z}/m\mathbb{Z}$ .

Wir beginnen mit zwei Vorüberlegungen.

**Lemma 2.5** Sei  $G$  eine beliebige Gruppe und  $g \in G$  ein Element. Dann gibt es genau einen Homomorphismus

$$\psi_g : \mathbb{Z} \rightarrow G$$

mit  $\psi_g(1) = g$ . Das Bild von  $\psi_g$  ist die von  $g$  erzeugte Untergruppe  $\langle g \rangle$ .

**Beweis** Die Eindeutigkeit von  $\psi_g$  ist klar: es ist notwendigerweise für  $n \in \mathbb{Z}$

$$\psi_g(n) = g^n$$

wie man leicht durch Induktion beweist. Dies ergibt eine wohldefinierte Abbildung, und diese ist ein Homomorphismus wegen der Regel aus (2.2.1)

$$g^{a+b} = g^a g^b \quad \text{für } a, b \in \mathbb{Z}.$$

Schließlich ist nach Konstruktion  $\text{Im}(\psi_g) = \{g^n \mid n \in \mathbb{Z}\} = \langle g \rangle$ .

**Lemma 2.6** Alle Untergruppen von  $\mathbb{Z}$  sind von der Gestalt  $m\mathbb{Z}$  für ein  $m \in \mathbb{Z}$ .

**Beweis** Sei  $U$  eine Untergruppe von  $\mathbb{Z}$ . Ist  $U = \{0\}$ , so können wir  $m = 0$  nehmen. Andernfalls ist  $U \cap \mathbb{N} \neq \emptyset$ . Sei  $m$  die kleinste natürliche Zahl mit  $m \in U$ . Dann ist offenbar  $m\mathbb{Z} \subseteq U$ . Sei umgekehrt  $n \in U$ . Es gibt  $k, r \in \mathbb{Z}$  mit  $0 \leq r < m$  und

$$n = km + r.$$

Da  $U$  Untergruppe ist, folgt  $r = n - km \in U$ . Wegen der Minimalität von  $m$  muss  $r = 0$  sein, also  $n \in m\mathbb{Z}$ .

Damit kommen wir zum

**Beweis von Satz 2.4** Sei  $g \in G$  ein erzeugendes Element. Dann ist

$$\psi_g : \mathbb{Z} \rightarrow G$$

ein Epimorphismus. Sei  $m \in \mathbb{Z}$  mit  $\text{Ker}(\psi_g) = m\mathbb{Z}$ . Ist  $m = 0$ , so ist  $\psi_g$  ein Isomorphismus und  $G$  unendlich. Ist  $m \neq 0$ , ohne Einschränkung  $m \in \mathbb{N}$ , so induziert  $\psi_g$  nach dem Homomorphiesatz 1.17 einen Isomorphismus

$$\mathbb{Z}/m\mathbb{Z} \xrightarrow{\sim} G, \quad a + m\mathbb{Z} \mapsto g^a,$$

und es ist  $|G| = |\mathbb{Z}/m\mathbb{Z}| = m$ .

**Corollar 2.7** Zyklische Gruppen gleicher Ordnung sind isomorph.

**Definition 2.8** Sei  $G$  eine Gruppe. Für  $g \in G$  wird die Ordnung von  $g$  definiert als

$$\text{ord}(g) = \min\{n \in \mathbb{N} \mid g^n = 1\}.$$

(Dies ist  $\infty$ , falls es kein  $n \in \mathbb{N}$  gibt mit  $g^n = 1$ ).

**Lemma 2.9**  $\text{ord}(g) = |\langle g \rangle|$ .

**Beweis** Betrachte den Epimorphismus

$$\begin{aligned} \psi_g : \mathbb{Z} &\rightarrow \langle g \rangle \\ n &\mapsto g^n \end{aligned}$$

Gibt es kein  $n \in \mathbb{N}$  mit  $g^n = 1$ , so ist  $\psi_g$  ein Isomorphismus und  $|\langle g \rangle| = |\mathbb{Z}| = \infty$ . Gibt es ein  $n \in \mathbb{N}$  mit  $g^n = 1$ , also mit  $n \in \text{ker}(\psi_g)$ , und ist  $m$  das minimale solche  $n$ , so ist nach dem Beweis von Lemma 2.6  $\text{ker}(\psi_g) = m\mathbb{Z}$  und der Homomorphiesatz liefert einen Isomorphismus

$$\mathbb{Z}/m\mathbb{Z} \xrightarrow{\sim} \langle g \rangle.$$

Es folgt  $m = |\mathbb{Z}/m\mathbb{Z}| = |\langle g \rangle|$ .

**Corollar 2.10** Ist  $G$  eine endliche Gruppe und  $g \in G$ , so teilt  $\text{ord}(g)$  die Gruppenordnung  $|G|$ . Insbesondere gilt  $g^{|G|} = 1$  für alle  $g \in G$ .

**Beweis** Nach dem Satz von Lagrange teilt  $|\langle g \rangle|$  die Gruppenordnung.

**Bemerkung 2.11** Sei  $G$  eine endliche Gruppe der Ordnung  $n$ . Dann ist  $G$  genau dann zyklisch, wenn es ein Element der Ordnung  $n$  in  $G$  gibt. Ist nämlich  $g \in G$  ein beliebiges Element mit  $\text{ord}(g) = n$ , so ist  $g$  ein Erzeugendes von  $G$ : Aus  $|\langle g \rangle| = n = |G|$  folgt  $\langle g \rangle = G$ . Die umgekehrte Richtung ist klar.

**Beispiel 2.12** Sei  $n \in \mathbb{N}$ . Die Gruppe

$$\mu_n = \{\zeta \in \mathbb{C}^\times \mid \zeta^n = 1\} = \{e^{\frac{2\pi i}{n}k} \mid k = 0, \dots, n-1\}$$

der  $n$ -ten Einheitswurzeln in  $\mathbb{C}$  hat die Ordnung  $n$ . Jede primitive  $n$ -te Einheitswurzel  $\zeta$  (d.h.,  $\zeta \in \mu_n$  mit  $\text{ord}(\zeta) = n$ ) erzeugt  $\mu_n$ , und wir haben einen Isomorphismus

$$\begin{aligned} \mathbb{Z}/n\mathbb{Z} &\xrightarrow{\sim} \mu_n \\ a \bmod n\mathbb{Z} &\mapsto \zeta^a. \end{aligned}$$

**Corollar 2.13** Sei  $p$  eine Primzahl. Ist  $G$  eine Gruppe der Ordnung  $p$ , so ist  $G$  zyklisch (also insbesondere abelsch), und jedes nicht-triviale Element erzeugt  $G$ .

**Beweis** Ist  $1 \neq g \in G$ , so muss  $|\langle g \rangle|$  nach Lagrange die Ordnung von  $G$  teilen und ist nicht 1. Es folgt  $|\langle g \rangle| = p$  und damit  $\langle g \rangle = G$ .

**Satz 2.14** Untergruppen und homomorphe Bilder von zyklischen Gruppen sind wieder zyklisch.

**Beweis** Sei  $G$  zyklisch und  $U \leq G$  eine Untergruppe. Sei  $g \in G$  ein Erzeugendes und

$$\psi_g : \mathbb{Z} \rightarrow G, \quad 1 \mapsto g$$

der zugehörige Epimorphismus. Dann ist  $\psi_g^{-1}(U)$  eine Untergruppe von  $\mathbb{Z}$ , d.h., von der Form  $m\mathbb{Z}$  für ein  $m \in \mathbb{Z}$  (Lemma 2.6). Es folgt

$$U = \psi_g \psi_g^{-1}(U) = \psi_g(m\mathbb{Z}) = \langle g^m \rangle = G^m.$$

Insbesondere ist  $U$  zyklisch, erzeugt von  $g^m$ . Die Behauptung über homomorphe Bilder ist trivial.

### §3 Ringe, Ringhomomorphismen und Ideale

**Erinnerung 3.1** (a) Ein Ring ist eine Menge  $R$  mit zwei (inneren) Verknüpfungen  $+$  und  $\cdot$ , so dass gilt:

(i)  $(R, +)$  ist eine kommutative Gruppe.

(ii)  $\cdot$  ist assoziativ.

(iii) Es gelten die Distributivgesetze.

(b)  $R$  heißt Ring mit Eins, wenn es ein Element  $1 \in R$  gibt mit  $1x = x = x1$  für alle  $x \in R$ . Dieses Element 1 ist eindeutig.

(c)  $R$  heißt kommutativ, wenn  $\cdot$  kommutativ ist.

**Bemerkung 3.2** In einem Ring  $R$  mit Eins ist  $1 \neq 0$  genau dann wenn  $R \neq \{0\}$ : Ist  $R \neq \{0\}$  und  $x \in R \setminus \{0\}$ , so ist wegen  $1 \cdot x = x$  und  $0 \cdot x = 0$  (gilt in jedem Ring!)  $1 \neq 0$ .

**Definition 3.3** Sei  $R$  ein Ring mit Eins  $1 \neq 0$ . Ein Element  $a \in R$  heißt Einheit, wenn es ein  $b \in R$  gibt mit  $ab = 1 = ba$ . Die Menge der Einheiten in  $R$  wird mit  $R^\times$  bezeichnet.

**Lemma 3.4**  $(R^\times, \cdot)$  ist eine Gruppe.

**Beweis** Für  $a, b \in R^\times$  seien  $a', b' \in R$  mit  $aa' = 1 = a'a$  und  $bb' = 1 = b'b$ . Dann sind  $a'$  und  $b' \in R^\times$  und es gilt  $abb'a' = 1 = b'a'ab$ , also  $ab \in R^\times$ . Wegen  $1 \cdot 1 = 1$  ist auch  $1 \in R^\times$  und es folgt sofort, dass  $R^\times$  eine Gruppe ist.

**Corollar/Definition 3.5** Ist  $a \in R^\times$ , so gibt es genau ein  $b \in R$  mit  $ab = 1 = ba$ . Dieses wird mit  $a^{-1}$  bezeichnet.

**Beweis** Dies ist eine allgemeine Eigenschaft von Gruppen.

**Beispiele 3.6** (a) Ist  $R$  ein Ring, so ist die Menge  $M_n(R)$  der  $(n \times n)$ -Matrizen mit Koeffizienten aus  $R$  ein Ring mit der üblichen Matrixaddition  $((a_{ij}) + (b_{ij}) = (a_{ij} + b_{ij}))$  und Matrixmultiplikation  $((a_{ij})(b_{ij}) = (c_{ij})$  mit  $c_{ij} = \sum_{k=1}^n a_{ik}b_{kj}$ ). Selbst wenn  $R$  kommutativ ist, so ist  $M_n(R)$  nicht kommutativ für  $n \geq 2$ . Hat  $R$  eine Eins  $1$ , so hat  $M_n(R)$  die Eins  $\begin{pmatrix} 1 & & 0 \\ & \ddots & \\ 0 & & 1 \end{pmatrix}$ .

(b) Für einen Ring  $R$  mit Eins  $1 \neq 0$  ist per definitionem  $Gl_n(R)$  die Einheitengruppe von  $M_n(R)$ , nämlich die Gruppe der invertierbaren Matrizen.

Ist  $R$  kommutativ, so kann man Determinanten definieren (zum Beispiel mit der Leibniz-Formel) und es gilt die Cramersche Regel. Mit dieser folgt für  $A \in M_n(R)$ :

$$A \in Gl_n(R) \quad \Leftrightarrow \quad \det(A) \in R^\times.$$

(c) Die Einheitengruppe von  $\mathbb{Z}$  ist  $\{\pm 1\}$ , denn für eine natürliche Zahl  $m > 1$  und jede natürliche Zahl  $n$  ist  $m \cdot n > 1$ ,  $m \cdot (-n) = -m \cdot n < 0$ , und entsprechend  $(-m)n, (-m)(-n) \neq 1$ .

**Definition 3.7** (a) Eine Abbildung  $\varphi : R \rightarrow R'$  zwischen Ringen heißt (Ring-)Homomorphismus, wenn

$$\varphi(r_1 + r_2) = \varphi(r_1) + \varphi(r_2), \quad \varphi(r_1 \cdot r_2) = \varphi(r_1) \cdot \varphi(r_2)$$

für  $r_1, r_2 \in R$ . Haben  $R$  und  $R'$  Einselemente, so fordert man noch, dass  $\varphi(1) = 1$  ist.

(b)  $\varphi$  heißt Monomorphismus (bzw. Epimorphismus, bzw. Isomorphismus, bzw. Automorphismus), wenn  $\varphi$  injektiv (bzw. surjektiv, bzw. bijektiv, bzw. bijektiv und  $R = R'$  ist).

**Definition 3.8** Eine Teilmenge  $R' \subseteq R$  heißt Unterring, wenn  $R'$  eine Untergruppe von  $(R, +)$  ist, und wenn  $a \cdot b \in R'$  für alle  $a, b \in R'$  (Dann ist  $R'$  mit den Einschränkungen von  $+$  und  $\cdot$  ein Ring, und die Inklusion  $R' \subseteq R$  ist ein Ringhomomorphismus).

**Definition 3.9** Eine Teilmenge  $\mathfrak{a}$  eines Ringes  $R$  heißt (zweiseitiges) Ideal von  $R$ , wenn gilt

- (i)  $\mathfrak{a}$  ist eine Untergruppe der additiven Gruppe von  $R$ ,
- (ii) Für jedes  $a \in \mathfrak{a}$  und  $x \in R$  gilt  $xa \in \mathfrak{a}$  und  $ax \in \mathfrak{a}$ .

**Beispiele 3.10** (a) Ist  $R$  ein Ring, so sind  $\{0\}$  und  $R$  immer Ideale von  $R$  und heißen die trivialen Ideale.

(b) Ist  $R$  ein kommutativer Ring, so ist für jedes  $a \in R$  die Menge  $Ra = \{ra \mid r \in R\}$  ein Ideal.

(c) Insbesondere ist in  $\mathbb{Z}$  jede Untergruppe (der additiven Gruppe  $\mathbb{Z}$ ) auch ein Ideal: die Untergruppen sind nach 2.6 von der Gestalt  $m\mathbb{Z}(= \mathbb{Z}m)$ , für  $m \in \mathbb{Z}$ , und dies ist ein Ideal nach (b).

(d) Jedes Ideal ist auch ein Unterring (i.a. ohne Eins, s.u.).

**Lemma 3.11** Sei  $\varphi : R \rightarrow R'$  ein Ringhomomorphismus.

(a) Ist  $\psi : R' \rightarrow R''$  ein zweiter Ringhomomorphismus, so ist  $\psi \circ \varphi : R \rightarrow R''$  ein Ringhomomorphismus.

(b) Ist  $\varphi$  ein Ringisomorphismus, so auch  $\varphi^{-1}$ .

(c) Das Bild von  $\varphi$  (Bez.  $\text{im}(\varphi)$ ) ist ein Unterring von  $R'$ .

(d) Ist  $\mathfrak{a}'$  ein Ideal (bzw. Unterring) von  $R'$ , so ist  $\varphi^{-1}(\mathfrak{a}')$  ein Ideal (bzw. Unterring) von  $R$ .

(e) Insbesondere ist der Kern von  $\varphi$ ,

$$\ker(\varphi) = \{a \in R \mid \varphi(a) = 0\},$$

ein Ideal von  $R$ .

**Beweis:** vollkommen analog zum Fall der Gruppen.

**Proposition 3.12** Sei  $R \neq \{0\}$  ein Ring mit Eins.

(a) Enthält ein Ideal  $\mathfrak{a}$  von  $R$  eine Einheit von  $R$ , so ist  $\mathfrak{a} = R$ .

(b) Ist  $R$  ein Schiefkörper, so besitzt  $R$  nur die trivialen Ideale  $\{0\}$  und  $R$ .

(c) Ist  $R$  kommutativ, so gilt auch die Umkehrung von (b).

**Beweis** (a): Ist  $a \in \mathfrak{a}$  eine Einheit, so gibt es ein  $a' \in R$  mit  $1 = a'a \in \mathfrak{a}$ . Es folgt  $x = x1 \in \mathfrak{a}$  für alle  $x \in R$ .

(b): Sei  $\mathfrak{a}$  ein Ideal von  $R$ . Ist  $\mathfrak{a} \neq 0$ , also etwa  $0 \neq a \in \mathfrak{a}$ , so ist nach Voraussetzung  $a$  eine Einheit, also  $\mathfrak{a} = R$  nach (a).

(c): Ist  $0 \neq r \in R$ , so ist  $Rr$  ein Ideal  $\neq 0$  (da  $r = 1r \in Rr$ ). Also ist  $Rr = R$ , d.h., es gibt ein  $r' \in R$  mit  $r'r = 1$ .

**Lemma/Definition 3.13** Sei  $R$  ein Ring.

(a) Ist  $(\mathfrak{a}_i)_{i \in I}$  eine nicht-leere Familie von Idealen von  $R$ , so ist  $\bigcap_{i \in I} \mathfrak{a}_i$  ein Ideal von  $R$ .

(b) Ist  $A \subseteq R$  eine Teilmenge von  $R$ , so ist

$$(A) = \bigcap_{\substack{\mathfrak{a} \text{ Ideal} \\ A \subseteq \mathfrak{a}}} \mathfrak{a}$$

das kleinste Ideal von  $R$ , welches  $A$  umfaßt und heißt das von  $A$  erzeugte Ideal. Ist  $A = \{a_1, \dots, a_n\}$  endlich, so schreibt man statt  $(A)$  meist  $(a_1, \dots, a_n)$ .

(c) Ist  $R$  kommutativ mit Eins, so ist

$$(A) = \left\{ \sum_{i=1}^n r_i a_i \mid n \in \mathbb{N} \cup \{0\}, a_1, \dots, a_n \in A, r_1, \dots, r_n \in R \right\}$$

(mit der üblichen Konvention, dass die leere Summe  $= 0$  ist).

**Beweis** (a) und (b) sind klar. Die in (c) rechts stehende Menge ist ein Ideal, enthält  $A$  (da  $a = 1a$  für  $a \in A$ ), und ist andererseits in jedem Ideal enthalten, welches  $A$  enthält, woraus (c) folgt.

**Lemma/Definition 3.14** Seien  $\mathfrak{a}, \mathfrak{b}$  Ideale eines Ringes  $R$ , so ist

$$\mathfrak{a} + \mathfrak{b} = \{a + b \mid a \in \mathfrak{a}, b \in \mathfrak{b}\}$$

ein Ideal von  $R$  und heißt die Summe von  $\mathfrak{a}$  und  $\mathfrak{b}$ . Es ist  $\mathfrak{a} + \mathfrak{b} = (\mathfrak{a} \cup \mathfrak{b})$ , d.h.,  $\mathfrak{a} + \mathfrak{b}$  das kleinste Ideal, welches  $\mathfrak{a}$  und  $\mathfrak{b}$  umfasst. Allgemeiner ist für eine Familie  $(\mathfrak{a}_i)_{i \in I}$  von Idealen in  $R$

$$\sum_{i \in I} \mathfrak{a}_i = \left\{ \sum_{\nu=1}^n a_\nu \mid n \in \mathbb{N}, a_\nu \in \mathfrak{a}_{i_\nu}, i_\nu \in I \right\} = \left( \bigcup_{i \in I} \mathfrak{a}_i \right)$$

das kleinste Ideal, welches alle  $\mathfrak{a}_i$  umfasst.

Der Beweis der Behauptungen in 3.14 ist klar.

Jedes Ideal  $\mathfrak{a}$  eines Ringes  $R$  ist insbesondere ein Normalteiler seiner additiven Gruppe (da letztere abelsch ist). Man kann daher die Faktorgruppe

$$R/\mathfrak{a} = \{x + \mathfrak{a} \mid x \in R\}$$

bilden. Diese ist abelsch, mit Verknüpfung

$$(x + \mathfrak{a}) + (y + \mathfrak{a}) = (x + y) + \mathfrak{a}.$$

**Satz 3.15** Es gibt genau eine Verknüpfung  $\cdot$  auf  $R/\mathfrak{a}$  derart, dass  $(R/\mathfrak{a}, +, \cdot)$  ein Ring und die kanonische Abbildung  $\pi : R \rightarrow R/\mathfrak{a}$  ein Ringhomomorphismus ist.

**Beweis** Es ist notwendigerweise

$$(x + \mathfrak{a}) \cdot (y + \mathfrak{a}) = \pi(x) \cdot \pi(y) = \pi(x \cdot y) = x \cdot y + \mathfrak{a}.$$

Dies ist wohldefiniert: ist  $x + \mathfrak{a} = x' + \mathfrak{a}$  und  $y + \mathfrak{a} = y' + \mathfrak{a}$ , so ist  $x' - x \in \mathfrak{a}$  und  $y' - y \in \mathfrak{a}$ , und damit

$$x'y' - xy = (x' - x)y' + x(y' - y) \in \mathfrak{a},$$

d.h.,  $x'y' + \mathfrak{a} = xy + \mathfrak{a}$ . Damit ist dann  $R/\mathfrak{a}$  ein Ring (das Assoziativgesetz der Multiplikation und die Distributivgesetze übertragen sich von  $R$  auf  $R/\mathfrak{a}$ ) und  $\pi$  ein Ringhomomorphismus (wir wissen schon, dass  $\pi(x + y) = \pi(x) + \pi(y)$  ist).

**Definition 3.16** (a) Der Ring  $R/\mathfrak{a}$  heißt Restklassenring von  $R$  modulo  $\mathfrak{a}$ .

(b) Für  $x - y \in \mathfrak{a}$  ( $\Leftrightarrow x + \mathfrak{a} = y + \mathfrak{a}$ ) schreibt man auch  $x \equiv y \pmod{\mathfrak{a}}$  ( $x$  kongruent zu  $y$  modulo  $\mathfrak{a}$ ), vergleiche 1.14.

**Lemma 3.17** (a) Ist  $R$  kommutativ, so auch  $R/\mathfrak{a}$ .

(b) Hat  $R$  eine Eins  $1$ , so ist  $1 + \mathfrak{a}$  Einselement von  $R/\mathfrak{a}$ , und  $\varphi : R \rightarrow R/\mathfrak{a}$  bildet die Einsen aufeinander ab.

(c) Eine Teilmenge  $\mathfrak{a}$  eines Ringes  $R$  ist genau dann ein Ideal, wenn es einen Ringhomomorphismus  $\varphi : R \rightarrow R'$  mit  $\mathfrak{a} = \ker(\varphi)$  gibt.

**Beweis** Dies ist alles klar. Für (c) beachte, dass der Kern von  $R \rightarrow R/\mathfrak{a}$  gleich  $\mathfrak{a}$  ist.

**Beispiel 3.18** Für jedes  $m \in \mathbb{Z}$  ist  $\mathbb{Z}/m\mathbb{Z}$  ein Ring, genannt der Restklassenring modulo  $m$ . Setzen wir  $\bar{a} = a + m\mathbb{Z}$ , so ist  $\bar{a} + \bar{b} = \overline{a+b}$  und  $\bar{a} \cdot \bar{b} = \overline{a \cdot b}$ . Zum Beispiel ist in  $\mathbb{Z}/5\mathbb{Z}$

$$\bar{3} + \bar{2} = \bar{5} = 0, \quad \bar{3} \cdot \bar{2} = \bar{6} = \bar{1}.$$

Sei  $(\mathbb{Z}/m\mathbb{Z})^\times$  die Gruppe der Einheiten in  $\mathbb{Z}/m\mathbb{Z}$ ; diese heißt die prime Restklassengruppe (oder Primrestklassengruppe) modulo  $m$ . Es gilt für  $a \in \mathbb{Z}$

$$\begin{aligned} a + m\mathbb{Z} &\in (\mathbb{Z}/m\mathbb{Z})^\times \\ \Leftrightarrow \exists b \in \mathbb{Z} \text{ mit } ab + m\mathbb{Z} &= 1 + m\mathbb{Z} \\ \Leftrightarrow \exists b \in \mathbb{Z} \text{ mit } ab - 1 &\in m\mathbb{Z} \\ \Leftrightarrow \exists b, r \in \mathbb{Z} \text{ mit } ab + mr &= 1 \\ \Leftrightarrow a \text{ und } m \text{ sind teilerfremd} &\text{ (nach dem Lemma unten).} \end{aligned}$$

Insbesondere ist  $(\mathbb{Z}/m\mathbb{Z})^\times$  die Menge der Erzeugenden der additiven Gruppe  $\mathbb{Z}/m\mathbb{Z}$ , und es gilt  $|(\mathbb{Z}/m\mathbb{Z})^\times| = \varphi(m)$ , wobei  $\varphi$  die Eulersche  $\varphi$ -Funktion ist.

**Lemma 3.19** Für ganze Zahlen  $m, n \in \mathbb{Z}$  gilt:  $m$  und  $n$  sind teilerfremd (d.h., die einzigen gemeinsamen Teiler sind  $+1$  und  $-1$ ) genau dann, wenn es  $r, s \in \mathbb{Z}$  gibt mit  $rm + sn = 1$ .

**Beweis:** Es genügt, dies für natürliche Zahlen  $m, n$  zu zeigen. Haben  $m$  und  $n$  einen gemeinsamen Teiler, so kann es offenbar keine Gleichung  $rm + sn = 1$  geben. Haben  $m$  und  $n$  keinen gemeinsamen Teiler  $d > 1$ , so zeigen wir durch Induktion über  $n$ , dass es  $r, s \in \mathbb{Z}$  mit  $rm + sn = 1$  gibt. Für  $n = 1$  ist nichts zu zeigen. Für  $n > 1$  gibt es  $q, c \in \mathbb{Z}$  mit  $0 < c < n$  mit

$$m = qn + c$$

( $c > 0$ , da  $m$  nicht durch  $n$  teilbar ist). Hieraus folgt, dass  $n$  und  $c$  keinen gemeinsamen Teiler  $d > 1$  haben (dieser würde auch  $m$  teilen). Nach Induktionsvoraussetzung gibt es  $a, b \in \mathbb{Z}$  mit  $an + bc = 1$ . Dann ist

$$1 = an + bc = an + b(m - qn) = bm + (a - bq)n.$$

Die in §1 gezeigten Homomorphie- und Isomorphiesätze haben Analoga für Ringe.

**Satz 3.20** Sei  $\varphi : R \rightarrow R'$  ein Ringhomomorphismus.

(a) Ist  $\mathfrak{a}$  ein Ideal von  $R$  mit  $\varphi(\mathfrak{a}) = \{0\}$  (d.h.,  $\mathfrak{a} \subseteq \ker(\varphi)$ ), so gibt es einen eindeutig bestimmten Ringhomomorphismus  $\bar{\varphi} : R/\mathfrak{a} \rightarrow R'$  der das Diagramm

$$\begin{array}{ccc} R & \xrightarrow{\pi} & R/\mathfrak{a} \\ & \searrow \varphi & \swarrow \bar{\varphi} \\ & & R' \end{array}$$

kommutativ macht.

(b) (Homomorphiesatz)  $\varphi$  induziert einen Ringhomomorphismus

$$\bar{\varphi} : R/\ker(\varphi) \hookrightarrow R'$$

und einen Isomorphismus von Ringen

$$\bar{\varphi} : R/\ker(\varphi) \xrightarrow{\sim} \text{im}(\varphi).$$

**Beweis** Der in 1.15 hergeleitete Gruppenhomomorphismus  $\bar{\varphi} : R/\mathfrak{a} \rightarrow R'$  der additiven Gruppen, mit  $\bar{\varphi}(r + \mathfrak{a}) = \varphi(r)$ , ist auch ein Ringhomomorphismus.

**Satz 3.21** Sei  $\varphi : R \rightarrow R'$  ein Ringhomomorphismus (Dann heißt  $R'$  auch homomorphes Bild von  $R$ ). Sei  $I'$  die Menge der Ideale von  $R'$  und  $I(\ker(\varphi)) = \{\mathfrak{a} \mid \mathfrak{a} \text{ Ideal von } R \text{ und } \ker(\varphi) \subseteq \mathfrak{a}\}$ . Dann ist

$$\begin{aligned} \varphi^{-1} : I' &\rightarrow I(\ker(\varphi)) \\ \mathfrak{a}' &\mapsto \varphi^{-1}(\mathfrak{a}') \end{aligned}$$

eine Bijektion mit Umkehrabbildung  $\mathfrak{a} \mapsto \varphi(\mathfrak{a})$ .

**Beweis:** Übungsaufgabe!

**Beispiel 3.22** Ist  $\mathfrak{a}$  ein Ideal eines Ringes  $R$ , so liefert

$$\mathfrak{b} \mapsto \mathfrak{b}/\mathfrak{a}$$

eine Bijektion zwischen den Idealen von  $R$  die  $\mathfrak{a}$  umfassen und den Idealen von  $R/\mathfrak{a}$  (betrachte  $R \rightarrow R/\mathfrak{a}$ ).

**Satz 3.23** (Zweiter Isomorphiesatz) seien  $\mathfrak{a} \subseteq \mathfrak{b}$  Ideale eines Ringes  $R$ . Dann ist die kanonische Bijektion (vergl. 1.19)

$$\varphi : (R/\mathfrak{a})/(\mathfrak{b}/\mathfrak{a}) \rightarrow R/\mathfrak{b}$$

ein Ringhomomorphismus.

**Beweis** Man beachte, dass  $\mathfrak{b}/\mathfrak{a}$  nach 3.22 ein Ideal von  $R/\mathfrak{a}$  ist. Die Multiplikativität von  $\varphi$  ist klar.

Es sei dem Leser als Übung überlassen, das ringtheoretische Analogon des ersten Isomorphiesatzes zu formulieren und zu beweisen.

**Satz 3.24** (Chinesischer Restsatz) Sei  $R$  ein kommutativer Ring mit Eins, und seien  $\mathfrak{a}_1, \dots, \mathfrak{a}_n$  Ideale von  $R$  derart, dass  $\mathfrak{a}_i + \mathfrak{a}_j = R$  für  $i \neq j$ . Dann hat man einen Isomorphismus

$$R / \bigcap_{i=1}^n \mathfrak{a}_i \xrightarrow{\sim} R / \mathfrak{a}_1 \times \dots \times R / \mathfrak{a}_n.$$

**Beweis** Definiere  $\varphi : R \rightarrow \prod_{i=1}^n R / \mathfrak{a}_i$  vermöge

$$\varphi(r) = (r + \mathfrak{a}_1, \dots, r + \mathfrak{a}_n).$$

Offenbar ist dies ein Ringhomomorphismus, und es ist  $\ker(\varphi) = \bigcap_{i=1}^n \mathfrak{a}_i$ . Es bleibt die Surjektivität von  $\varphi$  zu zeigen, dann folgt die Behauptung mit dem Homomorphiesatz. Seien  $r_1, \dots, r_n \in R$ ; wir müssen ein  $r \in R$  konstruieren mit  $r - r_i \in \mathfrak{a}_i$  für  $i = 1, \dots, n$ , wobei ohne Einschränkung  $n \geq 2$  ist.

Sei  $j \in \{1, \dots, n\}$ . Nach Voraussetzung gibt es für jedes  $i \neq j$  Elemente  $a_{ij} \in \mathfrak{a}_i$  und  $b_{ij} \in \mathfrak{a}_j$  mit

$$1 = a_{ij} + b_{ij}.$$

Setze  $s_j := \prod_{i \neq j} a_{ij}$ ; dann ist  $s_j \in \mathfrak{a}_i$  für jedes  $i \neq j$  und  $s_j = \prod_{i \neq j} (1 - b_{ij}) \in 1 + \mathfrak{a}_j := \{1 + a \mid a \in \mathfrak{a}_j\}$ . Mit anderen Worten ist

$$\begin{aligned} s_j &\equiv 1 \pmod{\mathfrak{a}_j} \\ s_j &\equiv 0 \pmod{\mathfrak{a}_i} \quad \text{für } i \neq j. \end{aligned}$$

Mit  $r := \sum_{j=1}^n r_j s_j$  ist dann  $r \equiv r_i s_i \equiv r_i \pmod{\mathfrak{a}_i}$ .

**Beispiel 3.25** (klassischer Chinesischer Restsatz) Sind  $m_1, \dots, m_n \in \mathbb{Z}$  paarweise teilerfremd, so ist

$$\mathbb{Z} / m_1 \dots m_n \mathbb{Z} \xrightarrow{\sim} \mathbb{Z} / m_1 \mathbb{Z} \times \dots \times \mathbb{Z} / m_n \mathbb{Z}.$$

Es ist nämlich  $m_i \mathbb{Z} + m_j \mathbb{Z} = \text{ggT}(m_i, m_j) \mathbb{Z} = \mathbb{Z}$  für  $i \neq j$  und  $\bigcap_{i=1}^n m_i \mathbb{Z} = \text{kgV}(m_1, \dots, m_n) \mathbb{Z} =$

$\prod_{i=1}^n m_i \mathbb{Z}$  (siehe auch §5). Explizit bedeutet der obige Isomorphismus: es gibt zu vorgegebenen  $a_1, \dots, a_n \in \mathbb{Z}$  ein  $x \in \mathbb{Z}$  mit

$$x \equiv a_i \pmod{m_i} \quad i = 1, \dots, n.$$

Ist  $x$  eine Lösung dieses Systems von Kongruenzen, so ist  $x + m_1 \dots m_n \mathbb{Z}$  die Menge aller Lösungen.

Im Hinblick auf dieses klassische Beispiel nennt man Ideale  $\mathfrak{a}$  und  $\mathfrak{b}$  in einem kommutativen Ring mit Eins teilerfremd, wenn  $\mathfrak{a} + \mathfrak{b} = R$ . Die Voraussetzung von 3.24 ist also, dass die  $\mathfrak{a}_i$  paarweise teilerfremd sind.

Wir kommen nun zu drei wichtigen Definitionen für Ringe und Ideale.

**Definition 3.26** (a) Ein Element  $r$  in einem Ring  $R$  heißt Nullteiler, wenn es ein Element  $s \in R \setminus \{0\}$  gibt mit  $r \cdot s = 0$  oder  $s \cdot r = 0$ .

(b) Ein Ring  $R$  heißt nullteilerfrei, wenn es außer der 0 keine Nullteiler gibt.

(c) Ein kommutativer Ring  $R$  mit Eins heißt Integritätsring (oder Integritätsbereich), wenn  $R \neq 0$  und nullteilerfrei ist.

**Beispiel 3.27** (a)  $\mathbb{Z}$  ist ein Integritätsring.

(b) Jeder (Schief-)Körper ist ein Integritätsring.

**Definition 3.28** Ein Ideal  $\mathfrak{p}$  in einem Ring  $R$  heißt Primideal (oder prim), wenn  $\mathfrak{p} \neq R$  ist und wenn für alle  $a, b \in R$  gilt

$$ab \in \mathfrak{p} \Rightarrow a \in \mathfrak{p} \text{ oder } b \in \mathfrak{p}.$$

**Beispiel 3.29** Ist  $p$  eine Primzahl, so ist  $p\mathbb{Z}$  ein Primideal in  $\mathbb{Z}$ . Denn es ist  $p\mathbb{Z} \neq \mathbb{Z}$ , und für  $a \in \mathbb{Z}$  gilt  $a \in p\mathbb{Z}$  genau dann wenn  $p \mid a$ . Für  $a, b \in \mathbb{Z}$  gilt aber

$$p \mid ab \Rightarrow p \mid a \text{ oder } p \mid b.$$

**Definition 3.30** Ein Ideal  $\mathfrak{m}$  in einem Ring heißt maximal, wenn  $\mathfrak{m} \neq R$  und wenn es kein Ideal  $\mathfrak{a} \subseteq R$  mit  $\mathfrak{m} \subsetneq \mathfrak{a} \subsetneq R$  gibt.

**Beispiel 3.31** Ist  $K$  ein (Schief-)Körper, so ist  $(0)$  ein maximales Ideal (siehe 3.12 (b)).

**Satz 3.32** Sei  $R$  ein kommutativer Ring mit Eins.

(a) Ein Ideal  $\mathfrak{p} \subseteq R$  ist genau dann ein Primideal, wenn  $R/\mathfrak{p}$  ein Integritätsring ist.

(b) Ein Ideal  $\mathfrak{p} \subseteq R$  ist genau dann maximal, wenn  $R/\mathfrak{p}$  ein Körper ist.

**Beweis** (a): Zunächst ist  $\mathfrak{p} \neq R$  genau dann, wenn  $R/\mathfrak{p} \neq 0$ . Weiter gilt für  $a \in R$  genau dann  $a \in \mathfrak{p}$  wenn  $\bar{a} = 0$  in  $R/\mathfrak{p}$ , wobei  $\bar{a}$  die Restklasse von  $a$  in  $R/\mathfrak{p}$  bezeichnet. Daher ist

$$ab \in \mathfrak{p} \Rightarrow a \in \mathfrak{p} \text{ oder } b \in \mathfrak{p}$$

äquivalent zu

$$\bar{a}\bar{b} = 0 \Rightarrow \bar{a} = 0 \text{ oder } \bar{b} = 0,$$

und Letzteres bedeutet die Nullteilerfreiheit von  $R/\mathfrak{p}$ .

(b): Da die Ideale in  $R/\mathfrak{m}$  gerade den Idealen  $\mathfrak{a} \subseteq R$  mit  $\mathfrak{m} \subseteq \mathfrak{a} \subseteq R$  entsprechen, folgt die Behauptung daraus, dass der kommutative Ring mit Eins  $R/\mathfrak{m}$  genau dann ein Körper ist, wenn er nur die trivialen Ideale hat (die in  $R$  den Idealen  $\mathfrak{m}$  und  $R$  entsprechen).

**Corollar 3.33** Sei  $R$  ein kommutativer Ring mit Eins.

(a)  $R$  ist Integritätsring genau dann, wenn  $(0)$  ein Primideal ist.

(b)  $R$  ist ein Körper genau dann, wenn  $(0)$  ein maximales Ideal ist.

(c) Jedes maximale Ideal ist auch ein Primideal.

**Beweis** (a) und (b) folgen aus der Isomorphie  $R/(0) \cong R$ , und (c) folgt aus 3.32 und Beispiel 3.27 (b).

**Satz 3.34** Für  $m \in \mathbb{N}$  sind die folgenden Aussagen äquivalent:

(a)  $m$  ist eine Primzahl.

(b)  $\mathbb{Z}/m\mathbb{Z}$  ist ein Integritätsring.

(c)  $\mathbb{Z}/m\mathbb{Z}$  ist ein Körper.

**Beweis:** (a)  $\Rightarrow$  (c): Ist  $m = p$  Primzahl, so besteht  $(\mathbb{Z}/p\mathbb{Z})^\times$  nach Beispiel 3.18 aus allen Elementen ungleich 0, nämlich  $\overline{1}, \overline{2}, \dots, \overline{p-1}$ .

(c)  $\Rightarrow$  (b): gilt allgemein.

(b)  $\Rightarrow$  (a): Ist  $m$  keine Primzahl, also etwa  $m = c \cdot d$  mit  $0 < c, d < m$ , so ist  $\overline{c} \neq 0, \overline{d} \neq 0$ , oder  $\overline{c}\overline{d} = \overline{cd} = \overline{m} = 0$ .

## §4 Polynomringe

In diesem Abschnitt seien alle Ringe kommutativ mit Eins und die Ringhomomorphismen sollen immer die Eins respektieren ( $\varphi(1) = 1$ ).

**4.1** Sei  $R$  ein kommutativer Ring mit Eins. Naiv ist ein Polynom in einer Unbestimmten  $X$  über  $R$  ein "formaler Ausdruck"

$$f(X) = a_0 + a_1X + \dots + a_nX^n$$

mit  $n \in \mathbb{N} \cup \{0\}$  und  $a_0, \dots, a_n \in R$ . Die  $a_i$  heißen die Koeffizienten von  $f(X)$ . Die Menge  $R[X]$  der Polynome bildet einen Ring, wenn man für ein zweites Polynom

$$g(X) = b_0 + b_1X + \dots + b_mX^m$$

die Summe von  $f(X)$  und  $g(X)$  definiert als

$$f(X) + g(X) = \sum_{i=0}^{\max(m,n)} (a_i + b_i)X^i,$$

wobei man  $a_i = 0$  für  $i > n$  und  $b_i = 0$  für  $i > m$  setzt, und das Produkt definiert als

$$f(X) \cdot g(X) = \sum_{k=0}^{m+n} \left( \sum_{i+j=k} a_i b_j \right) X^k.$$

Eine formal korrekte Definition, die auch für Polynomringe in beliebig vielen Variablen geeignet ist, erhalten wir wie folgt:

**Definition 4.2** Der Polynomring über  $R$  in einer Variablen ist die Menge

$$R^{(\mathbb{N}_0)} := \{(a_i)_{i \in \mathbb{N}_0} \mid a_i = 0 \text{ für fast alle } i \in \mathbb{N}_0\}$$

mit den Verknüpfungen

$$(a_i)_{i \in \mathbb{N}_0} + (b_i)_{i \in \mathbb{N}_0} = (a_i + b_i)_{i \in \mathbb{N}_0}$$

$$(a_i)_{i \in \mathbb{N}_0} \cdot (b_i)_{i \in \mathbb{N}_0} = (c_i)_{i \in \mathbb{N}_0} \quad \text{mit} \quad c_n = \sum_{i=0}^n a_i b_{n-i}.$$

Schreiben wir  $X$  für das Element  $(0, 1, 0, \dots)$ , so ist

$$X^i = (0, \dots, \underset{\substack{\uparrow \\ i\text{-te Stelle}}}{1}, 0, \dots) \quad \text{für } i \geq 0,$$

und jedes Element im Ring lässt sich schreiben als  $\sum_{i=0}^n a_i X^i$  mit  $n \in \mathbb{N}_0$  und  $a_0, \dots, a_n \in R$ .

Dies entspricht dem Element  $(a_0, \dots, a_n, 0, 0, \dots)$ . Umgekehrt können wir ein Element  $(a_0, a_1, \dots)$  schreiben als

$$\sum_{i=0}^{\infty} a_i X^i$$

wobei die Summe in Wirklichkeit endlich ist. Die Addition und Multiplikation ist dann wie in 4.1 beschrieben, und wir schreiben auch  $R[X]$  für den Polynomring, wenn wir das Element  $(0, 1, 0, \dots)$  mit  $X$  bezeichnen.

**Bemerkungen 4.3** (a) Ein Polynom ist also durch seine Koeffizienten festgelegt und nicht durch seine “Werte” (im Sinne des Einsetzens, siehe 4.5 unten).

(b) Wir haben einen kanonischen Monomorphismus von Ringen

$$\begin{aligned} R &\rightarrow R[X] \\ a &\mapsto a \quad (= aX^0 = (a, 0, \dots)). \end{aligned}$$

Hierüber fassen wir  $R$  immer als Unterring von  $R[X]$  auf.

**Satz 4.4** (Universelle Eigenschaft des Polynomrings) Sei  $R'$  ein Ring (mit Eins!) und  $\varphi : R \rightarrow R'$  ein Ringhomomorphismus (mit  $\varphi(1) = 1!$ ). Für jedes  $a \in R'$  gibt es genau einen Ringhomomorphismus

$$\varphi_a : R[X] \rightarrow R'$$

mit  $\varphi_a|_R = \varphi$  und  $\varphi_a(X) = a$ , nämlich

$$(4.4.1) \quad \varphi_a\left(\sum_{i=1}^n a_i X^i\right) = \sum_{i=1}^n \varphi(a_i) a^i.$$

**Beweis** Es ist klar, dass die Beziehung gelten muss, wenn  $\varphi_a$  ein Ringhomomorphismus mit den beiden vorgegebenen Eigenschaften sein soll. Diese Definition ist andererseits wohldefiniert, und macht  $\varphi_a$  zu einem Ringhomomorphismus mit den beiden gewünschten Eigenschaften.

**Bemerkung 4.5** Ist  $R \subseteq R'$  eine Ringerweiterung, also  $R$  ein Unterring von  $R'$ , so erhalten wir für  $a \in R'$  also die Abbildung

$$\begin{aligned} R[X] &\rightarrow R' \\ f(X) = \sum_{i=0}^n a_i X^i &\mapsto \sum_{i=0}^n a_i a^i =: f(a). \end{aligned}$$

Wir haben also einfach “die Variable  $X$  durch  $a$  ersetzt” und sprechen auch von dem Einsetzungsmorphismus. Betrachten wir nur  $R' = R$ , so wird ein Polynom im Allgemeinen nicht durch die Abbildung  $a \mapsto f(a)$  bestimmt: Für den Körper  $\mathbb{F}_2 = \mathbb{Z}/2\mathbb{Z} = \{0, 1\}$  gilt zum Beispiel immer  $a^2 - a = 0$ , aber das Polynom  $X^2 - X$  ist ungleich null.

**Definition 4.6** Sei  $R \subseteq R'$  eine Ringerweiterung und  $f = f(X) \in R[X]$ . Ein Element  $a \in R'$  heißt Nullstelle von  $f$ , wenn  $f(a) = 0$  (in  $R'$ ).

**Definition 4.7** Für  $f \in R[X]$  heißt

$$\deg(f) := \begin{cases} n & \text{falls } 0 \neq f = \sum_{i=0}^n a_i X^i \text{ mit } a_n \neq 0, \\ -\infty & \text{falls } f = 0, \end{cases}$$

der Grad von  $f$ . Ein Polynom  $0 \neq f \in R[X]$  heißt normiert, wenn sein Leitkoeffizient  $a_n = 1$  ist.

**Lemma 4.8** Wenn man mit  $-\infty$  wie üblich rechnet, gilt

- (a)  $\deg(fg) \leq \deg(f) + \deg(g)$ , mit Gleichheit, falls das Produkt der Leitkoeffizienten von 0 verschieden ist.
- (b)  $\deg(f + g) \leq \max(\deg(f), \deg(g))$  mit Gleichheit falls  $\deg(f) \neq \deg(g)$ .

**Beweis** selbst.

**Definition 4.9** Ist  $f(X) = \sum_{i=0}^n a_i X^i$  ein Polynom in  $R[X]$  und  $a_n \neq 0$ , so heißt  $a_n \in R$  der Leitkoeffizient von  $f$ .

**Satz 4.10** (Division mit Rest) Seien  $f, g \in R[X]$ , beide  $\neq 0$ .

- (a) Ist  $b$  der Leitkoeffizient von  $g$  und

$$k = \max\{0, \deg(f) - \deg(g) + 1\},$$

so gibt es Polynome  $q, r \in R[X]$  mit

$$b^k f = qg + r \quad \text{und} \quad \deg(r) < \deg(g).$$

- (b) Ist  $b$  keine Nullteiler von  $R$ , so sind  $q$  und  $r$  eindeutig bestimmt.
- (c) Ist  $b$  eine Einheit von  $R$ , so gibt es eindeutig bestimmte  $q, r \in R[X]$  mit

$$f = qg + r \quad \text{und} \quad \deg(r) < \deg(g).$$

**Beweis** (a): durch vollständige Induktion über  $m := \deg(f)$ . Setze  $n := \deg(g)$ .

Sei zunächst  $m = 0$ , also  $f \in R \setminus \{0\}$ . Ist  $n = 0$ , so ist  $g = b, k = 1$  und  $bf = fg + 0$  eine Zerlegung wie behauptet. Für  $n > 0$  ist  $k = 0$  und  $f = 0g + f$  eine Zerlegung wie benötigt.

Sei nun  $m > 0$ . Für  $n > m$  ist wieder  $k = 0$  und  $f = 0g + f$  eine Zerlegung wie gewünscht. Sei also  $n \leq m$  und  $a$  der Leitkoeffizient von  $f$ . Dann ist

$$m' := \deg(bf - aX^{m-n}g) \leq m - 1,$$

nach Induktionsvoraussetzung gibt es also  $q', r' \in R[X]$  mit

$$b^{m'-n+1}(bf - aX^{m-n}g) = q' \cdot g + r' \quad \text{und} \quad \deg(r') < \deg(g).$$

Es folgt durch Multiplikation mit  $b^{m-m'-1}$ , dass

$$b^{m-n+1}f = qg + r'$$

mit  $\deg(r') < \deg(g)$ , was zu zeigen war.

(b): Sei  $b$  kein Nullteiler und

$$\begin{aligned} q'g + r' &= qg + r, \\ \deg(r), \deg(r') &< \deg(g). \end{aligned}$$

Für  $q' \neq q$  folgt wegen  $(q - q')g = r - r'$

$$\begin{aligned} \deg(g) &> \max\{\deg(r), \deg(r')\} \\ &\geq \deg(r - r') = \deg(g) + \deg(q - q'), \end{aligned}$$

was ein Widerspruch ist. Also ist  $q = q'$  und damit auch  $r = r'$ .

(c) ist klar mit (a) und (b).

**Beispiel 4.11** (improvisiertes Teilen von Polynomen auf Zuruf)

**Lemma 4.12** Ein Element  $a \in R$  ist genau dann Nullstelle von  $f \in R[X]$ , wenn es ein  $g \in R[X]$  gibt mit  $f = g \cdot (X - a)$ .

**Beweis** Sei  $a \in R$  eine Nullstelle von  $f$ . Für  $f \neq 0$  gibt es  $g, r \in R[X]$  mit

$$f = g(X - a) + r,$$

wobei  $\deg(r) < \deg((X - a)) = 1$ , also  $r \in R$ . Es folgt  $0 = f(a) = r$ , also  $f = g(X - a)$ . Der Fall  $f = 0$  und die umgekehrte Richtung sind trivial.

**Satz 4.13** Ist  $R$  ein Integritätsring, so besitzt jedes  $0 \neq f \in R[X]$  höchstens  $\deg(f)$  viele Nullstellen in  $R$ .

**Beweis** durch vollständige Induktion über  $n := \deg(f)$ : Ist  $n = 0$ , so ist  $f$  konstant,  $\neq 0$ , hat also keine Nullstelle.

Sei nun  $n > 0$ . Hat  $f$  keine Nullstelle, so ist man fertig. Hat  $f$  eine Nullstelle in  $a \in R$ , so gibt es ein  $g \in R[X]$  mit  $f = (X - a)g$ . Da  $R$  ein Integritätsring ist, ist  $\deg(g) = n - 1$ , und jede von  $a$  verschiedene Nullstelle von  $f$  ist Nullstelle von  $g$ . Nach Induktionsvoraussetzung besitzt  $g$  höchstens  $n - 1$  Nullstellen, daher  $f$  höchstens  $n$  Nullstellen in  $R$ .

**Bespiele 4.14** (a) Das Polynom  $f = X^2 + 1 \in \mathbb{R}[X]$  besitzt keine Nullstelle in  $\mathbb{R}$ , da  $a^2 + 1 \geq 1$  für  $a \in \mathbb{R}$  ist, aber die zwei Nullstellen  $i, -i$  in  $\mathbb{C}$ .

(b) Sei  $R[\varepsilon] = R \oplus R\varepsilon$ , mit  $(r_1 + r_2\varepsilon)(r'_1 + r'_2\varepsilon) = r_1r'_1 + (r_1r'_2 + r_2r'_1)\varepsilon$ , der **Ring der dualen Zahlen über  $R$**  (Es ist  $R[\varepsilon] \cong R[X]/(X^2)$ ). Dann ist jedes  $r\varepsilon$  Nullstelle von  $f = X^2$ . Für  $R = \mathbb{Z}$  sind dies unendlich viele Nullstellen.

**Satz 4.15** Ein Ring  $R$  ist genau dann ein Integritätsring, wenn dies für  $R[X]$  gilt.

**Beweis:** Unterringe von Integritätsringen sind wieder solche. Ist umgekehrt  $R$  ein Integritätsring und sind  $f, g \in R[X] \setminus \{0\}$ , so ist nach Lemma 4.8  $\deg(f \cdot g) = \deg(f) + \deg(g) \neq -\infty$ , also  $f \cdot g \neq 0$ .

Wir diskutieren noch kurz Polynomringe in mehreren Variablen.

**Definition 4.16** Für  $n \in \mathbb{N}$  ist der Polynomring in  $n$  Variablen über dem Ring  $R$  definiert als die Menge

$$R^{(\mathbb{N}_0^n)} = \{(a_\alpha)_{\alpha \in \mathbb{N}_0^n} \in R^{\mathbb{N}_0^n} \mid a_\alpha = 0 \text{ für fast alle } \alpha \in \mathbb{N}_0^n\}$$

mit der Addition

$$(a_\alpha) + (b_\alpha) = (a_\alpha + b_\alpha)$$

und der Multiplikation

$$(a_\alpha) \cdot (b_\alpha) = (c_\alpha),$$

wobei

$$c_\alpha = \sum_{\beta + \gamma = \alpha} a_\beta \cdot b_\gamma.$$

Schreiben wir

$$X_i := (a_\alpha) \text{ mit } a_\alpha = \begin{cases} 1 & , \alpha = (0, \dots, 1, \dots, 0) \\ 0 & , \text{sonst,} \end{cases}$$

$i$ -te-Stelle  
↓

so können wir ein beliebiges Element  $(a_\alpha)$  schreiben als

$$\sum_{\alpha \in \mathbb{N}_0^n} a_\alpha X^\alpha = \sum_{(a_1, \dots, a_n) \in \mathbb{N}_0^n} a_{a_1, \dots, a_n} X_1^{a_1} \cdots X_n^{a_n}$$

wobei  $X^\alpha := X_1^{a_1} X_2^{a_2} \cdots X_n^{a_n}$  für  $\alpha = (a_1, \dots, a_n) \in \mathbb{N}_0^n$ , und wobei die Summe in Wirklichkeit endlich ist. Dies ist die übliche Schreibweise als Polynom. Wir bezeichnen den Polynomring dann auch mit  $R[X_1, \dots, X_n]$ .

**Bemerkung 4.17** Offenbar können wir identifizieren

$$R[X_1, \dots, X_n] = R[X_1, \dots, X_{n-1}][X_n].$$

Wir können den Polynomring in  $n$  Variablen auch induktiv so definieren.

**Beispiel 4.18** ( $n = 2$ ) Benennen wir die zwei Variablen  $X_1$  und  $X_2$  um in  $X$  und  $Y$ , so haben wir für die Elemente

$$\begin{aligned} f(X, Y) &= 1 + XY^2 + Y^2 = 1 + (1 + X)Y^2 \\ g(X, Y) &= X + X^2 + Y = (X + X^2) + Y \end{aligned}$$

in  $K[X, Y]$

$$\begin{aligned} f \cdot g &= X + X^2 + Y + X^2Y^2 + X^3Y^2 + XY^3 + XY^2 + X^2Y^2 + Y^3 \\ &= X + X^2 + Y + (X + 2X^2 + X^3)Y^2 + (1 + X)Y^3 \end{aligned}$$

## §5 Noethersche Ringe und Hauptidealringe

Sei  $R$  ein kommutativer Ring mit Eins.

**Definition 5.1** (a) Ein Ideal  $\mathfrak{a} \subset R$  heißt Hauptideal, wenn es von einem Element erzeugt wird:  $\mathfrak{a} = (a)$  für ein  $a \in R$ .  $R$  heißt Hauptidealring, wenn jedes Ideal Hauptideal ist.

(b) Ein Ideal  $\mathfrak{a} \subset R$  heißt endlich erzeugt, wenn es  $a_1, \dots, a_n \in R$  gibt mit  $\mathfrak{a} = (a_1, \dots, a_n)$ .  $R$  heißt noethersch, wenn jedes Ideal endlich erzeugt ist.

Wir betrachten zunächst Hauptidealringe.

**Definition 5.2** Ein Integritätsring  $R$  heißt euklidisch, wenn es eine Abbildung

$$d : R \setminus \{0\} \rightarrow \mathbb{N}_0$$

gibt mit der Eigenschaft: zu je zwei Elementen  $a, b \in R \setminus \{0\}$  gibt es  $q, r \in R$  mit

- (i)  $a = qb + r$ , wobei
- (ii)  $r = 0$  oder  $d(r) < d(b)$ .

**Bespiele 5.3** (a)  $\mathbb{Z}$  mit  $|| : \mathbb{Z} \setminus \{0\} \rightarrow \mathbb{N}_0, m \mapsto |m|$ , ist euklidisch – das ist das bekannte Teilen mit Rest.

(b) Nach 4.15 und 4.10 (c) ist für jeden Körper  $K$  der Polynomring in einer Variablen  $K[X]$  mit  $\deg : K[X] \setminus \{0\} \rightarrow \mathbb{N}_0, f \mapsto \deg(f)$ , euklidisch, denn jedes Element aus  $K \setminus \{0\}$  ist eine Einheit.

**Satz 5.4** Jeder euklidische Ring  $R$  ist ein Hauptidealring.

**Beweis** (vergleiche den Beweis von 2.6) Ist  $\mathfrak{a}$  ein Ideal von  $R$ , ohne Einschränkung  $\mathfrak{a} \neq \{0\}$ , so ist  $d(\mathfrak{a} \setminus \{0\})$  eine nichtleere Teilmenge von  $\mathbb{N}_0$ , hat also ein kleinstes Element  $k$ . Sei  $0 \neq a \in \mathfrak{a}$  mit  $d(a) = k$ ; dann ist  $\mathfrak{a} = (a)$ . Wäre nämlich  $b \in \mathfrak{a}$  mit  $b \notin (a)$ , so gäbe es  $q, r \in R$  mit  $b = qa + r$ , wobei  $r \neq 0$  und  $d(r) < d(a) = k$ . Da  $r = b - qa$  in  $\mathfrak{a}$  liegt, wäre dies ein Widerspruch zur Minimalität von  $k$ .

**Corollar 5.5** Ist  $K$  ein Körper und  $\mathfrak{a} \subseteq K[X]$  ein Ideal  $\neq \{0\}$ , so gibt es genau ein normiertes Polynom  $f \in K[X]$  mit  $\mathfrak{a} = (f)$ .

**Beweis** Nach 5.3 (b) und 5.4 ist  $K[X]$  ein Hauptidealring; es gibt daher ein  $f \in K[X]$  mit  $\mathfrak{a} = (f)$ . Ist  $a$  der Leitkoeffizient von  $f$ , so ist  $a \in K \setminus \{0\} = K^\times$ ,  $a^{-1}f$  normiert und  $(f) = (a^{-1}f)$ ; es kann also  $f$  als normiert vorausgesetzt werden. Ist  $(f) = (g)$ , so ist nach dem folgenden Lemma  $f = ug$  mit  $u \in K[X]^\times = K^\times$  (siehe Übungsaufgabe 7(i) für die letzte Gleichheit). Sind  $f$  und  $g$  normiert, so ist notwendigerweise  $u = 1$ , also  $f = g$ .

**Lemma 5.6** Ist  $R$  ein Integritätsring und sind  $a, b \in R$ , so gilt  $(a) = (b)$  genau dann wenn  $a = ub$  für eine Einheit  $u \in R^\times$ .

**Beweis** Gilt  $(a) = (b)$ , so ist  $a = ub$  und  $b = va$  mit  $u, v \in R$ , und damit  $a(1 - uv) = 0$ . Ist  $a \neq 0$ , so folgt  $uv = 1$ , d.h.,  $u, v \in R^\times$ .

Wir betrachten nun noethersche Ringe.

**Proposition 5.7** Die folgenden Aussagen sind äquivalent.

- (a)  $R$  ist noethersch.
- (b) Jede aufsteigende Kette  $\mathfrak{a}_0 \subset \mathfrak{a}_1 \subset \mathfrak{a}_2 \subset \dots$  von Idealen wird stationär, d.h., es gibt ein  $n \in \mathbb{N}$  mit  $\mathfrak{a}_n = \mathfrak{a}_{n+k}$  für alle  $k \geq 0$ .
- (c) Jede nichtleere Menge  $I$  von Idealen von  $R$  besitzt ein maximales Element, d.h., es existiert ein  $\mathfrak{b} \in I$  derart, dass kein  $\mathfrak{a} \in I$  existiert mit  $\mathfrak{b} \subsetneq \mathfrak{a}$ .

**Beweis** (a)  $\Rightarrow$  (b): Man zeigt leicht, dass  $\bigcup_{n \geq 0} \mathfrak{a}_n =: \mathfrak{a}$  ein Ideal ist (je endlich viele Elemente von  $\mathfrak{a}$  liegen in einem  $\mathfrak{a}_m$  für geeignetes  $m \in \mathbb{N}$ ). Ist  $\mathfrak{a} = (a_1, \dots, a_r)$ , so gibt es auch ein  $\mathfrak{a}_n$  mit  $a_1, \dots, a_r \in \mathfrak{a}_n$ . Die Inklusionen

$$(a_1, \dots, a_r) \subseteq \mathfrak{a}_n \subseteq \mathfrak{a}_{n+k} \subseteq \mathfrak{a} = (a_1, \dots, a_r)$$

sind dann alles Gleichheiten.

(b)  $\Rightarrow$  (c): Gäbe es in  $I$  kein maximales Element, so hätte man eine aufsteigende Kette  $\mathfrak{a}_0 \subsetneq \mathfrak{a}_1 \subsetneq \mathfrak{a}_2 \subsetneq \dots$ .

(c)  $\Rightarrow$  (a): Sei  $\mathfrak{a}$  ein Ideal von  $R$  und  $I$  die Menge aller in  $\mathfrak{a}$  enthaltenen endlich erzeugten Ideale. Wegen  $\{0\} \in I$  ist  $I$  nichtleer, nach (c) gibt es also ein maximales Element  $\mathfrak{c} = (c_1, \dots, c_r) \in I$ . Es ist nach Definition  $\mathfrak{c} \subseteq \mathfrak{a}$ . Ist  $a \in \mathfrak{a}$ , so ist  $\mathfrak{c}' = (c_1, \dots, c_r, a) \subseteq \mathfrak{a}$ ,  $\mathfrak{c} \subset \mathfrak{c}'$ , also  $\mathfrak{c} = \mathfrak{c}'$  wegen der Maximalität von  $\mathfrak{c}$ , d.h.,  $a \in \mathfrak{c}$ . Damit ist  $\mathfrak{a} = \mathfrak{c}$  endlich erzeugt.

**Beispiele 5.8** (a) Körper und Hauptidealringe sind trivialerweise noethersch; insbesondere ist  $\mathbb{Z}$  noethersch.

(b) Der Ring  $C([0, 1], \mathbb{R})$  der stetigen reellwertigen Funktionen auf dem Intervall  $[0, 1]$  ist nicht noethersch: für jedes  $n \in \mathbb{N}$  ist die Menge  $\mathfrak{a}_n = \{f \in C([0, 1], \mathbb{R}) \mid f|_{[0, \frac{1}{n}]} = 0\}$  ein Ideal, und es ist  $\mathfrak{a}_1 \subsetneq \mathfrak{a}_2 \subsetneq \mathfrak{a}_3 \subsetneq \dots$

(c) Ist  $R$  noethersch, so ist jedes epimorphe Bild  $R'$  von  $R$  wieder noethersch.

**Satz 5.9** (Hilbertscher Basissatz) Ist  $R$  noethersch, so auch  $R[X]$ .

**Beweis** (nach Heidrun Sarges) Angenommen  $\mathfrak{a} \neq \{0\}$  ist ein nicht endlich erzeugtes Ideal in  $R[X]$ . Dann sei  $f_1$  ein Polynom minimalen Grades in  $\mathfrak{a} \setminus \{0\}$ ,  $f_2$  minimalen Grades in  $\mathfrak{a} \setminus (f_1)$  usw., so dass man eine Folge  $f_1, f_2, f_3, \dots$  in  $\mathfrak{a}$  erhält mit  $f_k$  minimalen Grades in  $\mathfrak{a} \setminus (f_1, \dots, f_{k-1})$ . Sei  $n_k = \deg(f_k)$  und  $a_k$  der Leitkoeffizient von  $f_k$ . Dann ist  $n_{k+1} \geq n_k$  (nach Definition) und  $(a_1, \dots, a_k) \subsetneq (a_1, \dots, a_{k+1})$  für alle  $k$ , also  $R$  nicht noethersch. Wäre nämlich

$$a_{k+1} = \sum_{i=1}^k r_i a_i \quad \text{mit } r_i \in R,$$

so läge das Polynom

$$g = \sum_{i=1}^k r_i x^{n_{k+1}-n_i} f_i$$

in  $(f_1, \dots, f_k)$  und hätte den Leitkoeffizienten  $a_{k+1}$  und den Grad  $n_{k+1}$ . Dann wäre  $f_{k+1} - g \in \mathfrak{a} \setminus (f_1, \dots, f_k)$  und  $\deg(f_{k+1} - g) < n_{k+1} = \deg(f_{k+1})$ , im Widerspruch zur Wahl von  $f_{k+1}$ .

Durch vollständige Induktion folgt:

**Corollar 5.10** Ist  $R$  noethersch (z.B.  $R = \mathbb{Z}$  oder  $R =$  ein Körper  $K$ ), so ist  $R[X_1, \dots, X_n]$  noethersch.

## §6 Quotientenkörper und faktorielle Ringe

Sei  $R$  ein Integritätsring. Dann gibt es einen "kleinsten"  $R$  enthaltenden Körper, den sogenannten Quotientenkörper  $Q(R)$ . Dies verallgemeinert die Konstruktion der rationalen Zahlen aus den ganzen Zahlen.

**Konstruktion 6.1** Auf  $R \times R \setminus \{0\}$  ist die Relation

$$(a, b) \sim (c, d) \quad :\Leftrightarrow \quad ad = bc$$

eine Äquivalenzrelation. Die Äquivalenzklasse von  $(a, b)$  bezüglich  $\sim$  werde mit  $\frac{a}{b}$  bezeichnet und

$$\text{Quot}(R) = \left\{ \frac{a}{b} \mid a, b \in R, b \neq 0 \right\}$$

sei die Menge der Äquivalenzklassen. Durch die Addition

$$\frac{a}{b} + \frac{c}{d} = \frac{ad + bc}{bd}$$

und die Multiplikation

$$\frac{a}{b} \cdot \frac{c}{d} = \frac{ac}{bd}$$

wird  $\text{Quot}(R)$  zu einem Körper. Die Abbildung

$$\begin{aligned} \iota : R &\rightarrow \text{Quot}(R) \\ a &\mapsto \frac{a}{1} \end{aligned}$$

ist ein injektiver Ringhomomorphismus; wir fassen hiermit  $R$  als einen Unterring von  $\text{Quot}(R)$  auf.

**Beweis** der Behauptungen: selbst!

**Beispiele 6.2** (a) Es ist  $\text{Quot}(\mathbb{Z}) \cong \mathbb{Q}$ .

(b) Für einen Körper  $K$  ist  $\text{Quot}(K) = K$ .

**Satz 6.3** (universelle Eigenschaft) Ist  $\varphi : R \hookrightarrow K$  ein *injektiver* Ringhomomorphismus in einem Körper (mit  $\varphi(1) = 1!$ ), so gibt es einen eindeutig bestimmten Ringhomomorphismus  $\tilde{\varphi} : \text{Quot}(R) \rightarrow K$ , der  $\varphi$  fortsetzt, d.h., für den das Diagramm

$$\begin{array}{ccc} R & \xrightarrow{\quad} & \text{Quot}(R) \\ & \searrow \varphi & \swarrow \exists! \tilde{\varphi} \\ & & K \end{array}$$

kommutativ ist.

**Beweis** In  $\text{Quot}(R)$  ist

$$\frac{a}{b} = \frac{a}{1} \cdot \frac{1}{b} = \frac{a}{1} \left( \frac{b}{1} \right)^{-1} = a \cdot b^{-1}$$

wobei wir  $a \in R$  mit  $\frac{a}{1} \in \text{Quot}(R)$  identifizieren). Es muss also gelten

$$\tilde{\varphi} \left( \frac{a}{b} \right) = \tilde{\varphi}(ab^{-1}) = \varphi(a)\varphi(b)^{-1}.$$

Man rechnet leicht nach, dass diese Definition wohldefiniert ist und die damit definierte Abbildung  $\tilde{\varphi}$  ein Ringhomomorphismus ist. Per Definition ist  $\tilde{\varphi}|_R = \varphi$ .

**Bemerkungen 6.4** (a) Ist  $\varphi : R \rightarrow K$  ein nicht-trivialer Ringhomomorphismus, wobei  $K$  ein Körper ist, so ist  $\varphi$  injektiv. Denn es ist  $\ker(\varphi)$  ein Ideal ungleich  $K$ , also null. Dies gilt insbesondere, wenn  $R \neq 0$  ist und  $\varphi(1) = 1$  (da dann  $\varphi(1) = 1 \neq 0$ ).

(b) Insbesondere ist jeder (Ring-)Homomorphismus  $\varphi$  von Körpern injektiv (für diese setzen wir immer  $\varphi(1) = 1$  voraus).

(c) Insbesondere folgt, dass der Homomorphismus  $\tilde{\varphi}$  im obigen Satz injektiv ist. Wir können  $\text{Quot}(R)$  mit dem Teilkörper  $L = \text{im}(\tilde{\varphi})$  von  $K$  identifizieren. In diesem Sinne ist  $\text{Quot}(R)$  der kleinste Körper, der  $R$  enthält.

Wir kommen nun zur Teiler-Theorie in Integritätsringen. Sei  $R$  wieder ein Identitätsring.

**Definition 6.5** Für  $a, b \in R$  sagen wir  $a$  teilt  $b$  (Bez.  $a \mid b$  oder  $b \equiv 0 \pmod{a}$ ), wenn die folgenden äquivalenten Bedingungen gelten

- (i) Es existiert ein  $c \in R$  mit  $a \cdot c = b$ .
- (ii)  $b \in (a)$ .
- (iii)  $b \equiv 0 \pmod{a}$  (d.h.,  $\bar{b} = 0$  in  $R/(a)$ ).

(iv)  $(b) \subseteq (a)$ .

(v)  $\frac{b}{a} \in R \subseteq \text{Quot}(R)$ .

**Beweis** (i)  $\Leftrightarrow$  (ii) ist klar, da  $(a) = Ra$ . (ii)  $\Leftrightarrow$  (iii) gilt nach Definition. (ii)  $\Rightarrow$  (iv):  $b \in (a) \Rightarrow (b) = Rb \subseteq (a)$ , da  $(a)$  ein Ideal ist. (iv)  $\Rightarrow$  (ii) ist trivial.

(i)  $\Leftrightarrow$  (iv):  $\frac{b}{a} = \frac{c}{1}$  mit  $c \in R \Leftrightarrow b = ac$  mit  $c \in R$ .

**Corollar 6.6** Für  $a, b, c \in R$  gilt:

(a)  $a \mid a$  (reflexiv)

(b)  $a \mid b$  und  $b \mid c \Rightarrow a \mid c$  (transitiv)

(c)  $a \mid b$  und  $b \mid a \Leftrightarrow (a) = (b) \Leftrightarrow$  es existiert eine Einheit  $u \in R^\times$  mit  $a = ub$ . In diesem Fall sagen wir, dass  $a$  und  $b$  *assoziiert* sind. (Bez.:  $a \sim b$ ).

**Beweis** Alle Aussagen sind klar; die zweite Äquivalenz in (c) wurde in Lemma 5.6 bewiesen.

**Definition 6.7** Ein Element  $p \in R \setminus \{0\}$  heißt Primelement (oder prim), wenn die folgenden äquivalenten Bedingungen gelten:

(i)  $(p) \subseteq R$  ist ein Primideal.

(ii)  $R/(p)$  ist ein Integritätsring.

(iii)  $p \notin R^\times$  und es gilt:  $ab \equiv 0 \pmod{p} \Rightarrow a \equiv 0 \pmod{p}$  oder  $b \equiv 0 \pmod{p}$ .

(iv)  $p \notin R^\times$  und es gilt:  $p \mid ab \Rightarrow p \mid a$  oder  $p \mid b$ .

**Beweis** der Äquivalenzen: Dies ist klar nach Definition 3.28, Satz 3.32 und den Äquivalenzen in Definition 6.5. Beachte:  $p \notin R^\times \Leftrightarrow (p) \neq R$ .

**Bemerkungen 6.8** (a) Aus 6.7 (iv) folgt induktiv für ein Primelement  $p$ :

$$p \mid \prod_{i=1}^n a_i \quad \Rightarrow \quad \exists i : p \mid a_i.$$

(b) Ist  $p$  prim, so ist  $p$  keine Einheit (Dies folgt aus 6.7 (iii)).

(c) Aus 6.7 (i) folgt: Ist  $p$  prim und  $u$  Einheit, so ist auch  $up$  prim. Es gilt also für  $a \sim b$  :  $a$  prim  $\Leftrightarrow b$  prim.

(d) Sind  $p_1, \dots, p_n$  Primelemente, so ist  $\prod_{i=1}^n p_i$  keine Einheit, denn sonst wäre  $R = \left( \prod_{i=1}^n p_i \right) \subseteq (p_1)$  – Widerspruch!

**Definition 6.9** Ein Element  $a \in R \setminus \{0\}$  heißt irreduzibel (oder unzerlegbar), wenn  $a$  keine Einheit ist und wenn gilt:

$$a = bc \quad \Rightarrow \quad b \text{ oder } c \text{ Einheit.}$$

Sonst heißt  $a$  reduzibel (oder zerlegbar).

**Proposition 6.10** Ist  $p$  ein Primelement, so ist  $p$  irreduzibel.

**Beweis:** Sei  $a \in R$  prim. Ist  $a = bc$  mit  $b, c \in R$ , so gilt insbesondere  $a \mid bc$ , also  $a \mid b$  oder  $a \mid c$ , da  $a$  prim ist. Wenn (ohne Einschränkung)  $a \mid b$ , so gibt es ein  $d \in R$  mit  $ad = b$ . Es folgt  $a = bc = adc$ . Da  $R$  ein Integritätsring ist, folgt hieraus  $1 = dc$ . Damit ist  $c$  eine Einheit. Also ist  $a$  irreduzibel.

**Bemerkungen 6.11** Hier haben wir benutzt, dass in Integritätsringen gekürzt werden kann: Gilt  $ab = ac$  mit  $a \neq 0$ , so folgt  $a \cdot (b - c) = 0$ , also  $b - c = 0$  (da  $a \neq 0$  und  $R$  nullteilerfrei ist), also  $b = c$ .

**Bispiele 6.12** (a) Für jedes  $a > 0$  ist das Polynom  $x^2 + a$  in  $\mathbb{R}[X]$  irreduzibel. Gilt nämlich  $x^2 + a = f(x)g(x)$ , so kann  $f(x)$  nicht den Grad 1 haben, denn dann würde  $x^2 + a$  einen Linearfaktor  $x - b$  abspalten und hätte die Nullstelle  $b \in \mathbb{R}$ . Die Gleichung  $x^2 = -a$  ist aber in  $\mathbb{R}$  nicht lösbar. Also hat entweder  $f(x)$  oder  $g(x)$  den Grad 0, ist also eine Einheit.

(b) Im Allgemeinen ist die Umkehrung von Proposition 6.10 falsch. Betrachte zum Beispiel den Ring

$$\mathbb{Z}[\sqrt{-d}] = \{a + b\sqrt{-d} \mid a, b \in \mathbb{Z}\} \subseteq \mathbb{C},$$

wobei  $d \in \mathbb{N}$ ,  $d \geq 5$  und  $d \equiv 1 \pmod{4}$ . Das Element  $1 + \sqrt{-d}$  ist irreduzibel aber nicht prim (Übungsaufgabe!).

**Definition 6.13** Ein Integritätsring heißt faktoriell (oder ZPE-Ring), falls jedes Element  $\neq 0$  Produkt von Primelementen oder eine Einheit ist.

**Satz 6.14** In faktoriellen Ringen ist die Primzerlegung (Zerlegung in ein Produkt von Primelementen) bis auf Einheiten eindeutig.

**Beweis:** Dies folgt aus dem allgemeineren

**Lemma 6.15** Sei  $R$  ein Integritätsring. Für ein Element  $a \in R$  sei

$$a = up_1 \dots p_r = vq_1 \dots q_s,$$

wobei  $u, v$  Einheiten,  $p_1, \dots, p_r$  Primelemente und  $q_1, \dots, q_s$  irreduzibel sind. Dann gilt  $r = s$ , und nach möglicher Umm Nummerierung der  $q_j$  gilt, dass  $p_i$  und  $q_i$  assoziiert sind (d.h.,  $q_i = u_i p_i$  für eine Einheit  $u_i$ ).

**Beweis** Ist  $r < 1$  (also  $p_1 \dots p_r = 1$ ), so ist auch  $s < 1$ , da  $q_1, \dots, q_s$  keine Einheiten sind. Sei also  $r \geq 1$ . Da  $p_1$  Primelement ist, folgt aus  $p_1 \mid q_1, \dots, q_s$ , dass es ein  $i \in \{1, \dots, s\}$  gibt mit  $p_1 \mid q_i$  (siehe 6.8(a)). Durch Umm Nummerieren können wir annehmen, dass  $i = 1$  ist. Dann gibt es ein  $u_1 \in R$  mit  $p_1 \cdot u_1 = q_1$ . Da  $q_1$  irreduzibel ist und  $p_1$  keine Einheit ist (6.8 (b)), muss  $u_1$  eine Einheit sein. Wir erhalten die Gleichung

$$up_2 \dots p_r = u_1 v q_2 \dots q_s.$$

Da  $v' := u_1 v$  wieder eine Einheit ist, folgt per Induktion die Behauptung.

**Corollar 6.16** In einem faktoriellen Ring  $R$  ist jedes irreduzible Element auch prim.

**Beweis:** Sei  $a \in R$  irreduzibel und seien  $x, y \in R$  mit  $a \mid x \cdot y$ . Wir wollen zeigen  $a \mid x$  oder  $a \mid y$ . Seien

$$x = u x_1 \dots x_r \quad , \quad y = v y_1 \dots y_s$$

Primzerlegungen von  $x$  und  $y$  ( $u, v$  Einheiten,  $x_i$  und  $y_j$  Primelemente). Sei  $ab = xy$  mit  $b \in R$  und sei  $b = w b_1 \dots b_t$  eine Primzerlegung von  $b$  ( $w$  Einheit,  $b_1, \dots, b_t$  Primelemente). Dann gilt

$$w a b_1 \dots b_t = uv x_1 \dots x_r y_1 \dots y_s ,$$

und nach Lemma 6.15 ist  $a$  assoziiert zu einem  $x_i$  oder zu einem  $y_i$ . Damit gilt  $a \mid x$  oder  $a \mid y$ .

**Lemma 6.17** Sei  $R$  (ein Integritätsring und) ein Hauptidealring. Ist  $a \in R \setminus \{0\}$  irreduzibel, so ist  $(a)$  maximal.

**Beweis** Angenommen  $(a) \subsetneq (b) \subseteq R$ . Dann gibt es ein  $c \in R$  mit  $a = bc$ . Da  $a$  irreduzibel ist, ist entweder  $b$  oder  $c$  Einheit. Im ersten Fall ist  $(b) = R$ , im zweiten Fall ist  $(a) = (b)$  (Lemma 5.6).

**Satz 6.18** Sei  $R$  (ein Integritätsring und) ein Hauptidealring. Dann ist  $R$  faktoriell.

**Beweis** Sei  $a \in R \setminus R^\times$ ,  $a \neq 0$ .

1. *Schritt:*  $a$  besitzt einen irreduziblen Teiler.

Angenommen nicht. Dann ist  $a$  insbesondere reduzibel, also  $a = a_1 a'_1$  mit  $a_1, a'_1 \in R \setminus R^\times$ . Weiter ist dann  $a_1$  ohne irreduziblen Teiler, also  $a_1 = a_2 a'_2$  mit  $a_2, a'_2 \in R \setminus R^\times$ . Induktiv gibt dies eine unendliche echt aufsteigende Idealkette

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

Widerspruch dazu, dass  $R$  noethersch ist (als Hauptidealring)!

2. *Schritt:*  $a$  besitzt einen primen Teiler, da jedes irreduzible Element in  $R$  auch prim ist (nach Lemma 6.17; jedes maximale Ideal ist auch prim).

3. *Schritt:*  $a$  ist Produkt von (endlich vielen) Primelementen.

Denn nach dem 2. Schritt besitzt  $a$  einen Primteiler  $a_1$ , also  $a = a_1 b_1$ . Ist  $b_1$  keine Einheit, so besitzt  $b_1$  einen Primteiler  $a_2$ , so dass  $b_1 = a_2 b_2$ . Induktiv erhalten wir Primelemente  $a_i$  mit

$$(6.18.1) \quad a = a_1 \dots a_n b_n \quad , \quad b_i = a_{i+1} b_{i+1} .$$

Dies Verfahren bricht ab, wenn  $b_n$  eine Einheit ist; dann ist (6.18.1) eine Primzerlegung von  $a$ . Andernfalls bricht das Verfahren nicht ab, und wir erhalten eine echt aufsteigende Primidealkette

$$(b_1) \subsetneq (b_2) \subsetneq (b_3) \subsetneq \dots ,$$

da  $b_i = a_{i+1}b_{i+1}$  mit  $a_{i+1} \notin R^\times$ . Dies ist ein Widerspruch dazu, dass  $R$  noethersch ist.

**Corollar 6.19** Ist  $K$  ein Körper, so ist  $K[X]$  faktoriell.  $\mathbb{Z}$  ist faktoriell. Jeder euklidische Ring ist faktoriell.

**Definition 6.20** Sei  $R$  ein Integritätsring und seien  $a, b \in R \setminus \{0\}$ .

(a) Für ein Element  $d \in R$  sagen wir  $d$  ist ein größter gemeinsamer Teiler von  $a$  und  $b$  (Bez.  $d = ggT(a, b)$ ), wenn gilt:  $d \mid a$  und  $d \mid b$ , und falls  $t \mid a$  und  $t \mid b$  so gilt  $t \mid d$ .

(b) Für ein Element  $c \in R$  sagen wir  $c$  ist ein kleinstes gemeinsames Vielfaches von  $a$  und  $b$  (Bez.  $c = kgV(a, b)$ ), wenn gilt:  $a \mid c$  und  $b \mid c$ , und für  $a \mid s$  und  $b \mid s$  folgt  $c \mid s$ .

$ggT$  und  $kgV$  sind nur bis auf Einheiten wohlbestimmt.

**Lemma 6.21** In einem faktoriellen Ring  $R$  besitzen zwei Elemente  $\neq 0$  immer einen  $ggT$  und einen  $kgV$ .

**Beweis** Seien  $a, b \in R \setminus \{0\}$ . Dann gibt es eine endliche Menge  $P$  von Primelementen in  $R$  und Zahlen  $e_p, f_p \in \mathbb{N}_0$  mit

$$a \sim \prod_{p \in P} p^{e_p} \quad , \quad b \sim \prod_{p \in P} p^{f_p} .$$

Dann sieht man leicht, dass

$$\begin{aligned} ggT(a, b) &= \prod_{p \in P} p^{\min(e_p, f_p)} \\ kgV(a, b) &= \prod_{p \in P} p^{\max(e_p, f_p)} . \end{aligned}$$

**Bemerkungen 6.22** Sei  $R$  faktoriell.

(a) Auf  $R \setminus \{0\}$  ist die Assoziiertheit ( $x \sim y \Leftrightarrow x = uy$  für  $u \in R^\times \Leftrightarrow (x) = (y)$ ) eine Äquivalenzrelation. Die Menge der Äquivalenzklassen wird mit  $R \setminus \{0\}/R^\times$  bezeichnet. Die Teilrelation induziert eine Ordnungsrelation auf  $R \setminus \{0\}/R^\times$  (siehe Corollar 6.6). Bezüglich dieser Ordnungsrelation ist  $ggT(a, b)$  das Infimum und  $kgV$  das Supremum der Menge  $\{a \bmod \sim, b \bmod \sim\}$ . Es gibt eine Bijektion

$$(6.22.1) \quad \begin{aligned} R \setminus \{0\}/R^\times &\rightarrow \{\text{Hauptideale } (a)\} \\ a \bmod \sim &\mapsto (a) , \end{aligned}$$

bezüglich derer die Teilrelation  $\mid$  übergeht in die umgekehrte Inklusion (da  $a \mid b \Leftrightarrow (b) \subseteq (a)$ ).

(b) Auf  $R \setminus \{0\}/R^\times$  sind  $ggT$  und  $kgV$  assoziierte Operationen; daher machen für  $a_1, \dots, a_n \in R \setminus \{0\}$  die Bildungen

$$ggT(a_1, \dots, a_n) \quad \text{und} \quad kgV(a_1, \dots, a_n)$$

Sinn.

(c) In einem Hauptidealring  $R$  gilt für  $a_1, \dots, a_n \in R \setminus \{0\}$

$$\bigcap_{i=1}^n (a_i) = (kgV(a_1, \dots, a_n))$$

$$\sum_{i=1}^n (a_i) = (ggT(a_1, \dots, a_n)),$$

wegen der Identifikation (6.22.1) und der Tatsache, dass alle Ideale Hauptideale sind, also auch  $\bigcap (a_i)$  und  $\sum (a_i)$ . Vergleiche die Anwendung im klassischen chinesischen Restsatz (Beispiel 3.25)

## §7 Faktorisierung von Polynomen

Wir untersuchen in diesem Abschnitt, wie man Polynome in ein Produkt von irreduziblen Polynomen (= irreduziblen Elementen in Polynomringen) zerlegt beziehungsweise, wie man feststellt, ob ein Polynom irreduzibel ist.

Zur Erinnerung: Im Polynomring  $K[X]$  über einem Körper  $K$  ist ein Polynom genau dann irreduzibel, wenn es prim ist.

**Definition 7.1** Sei  $R$  ein faktorieller Ring und  $f = \sum_{i=0}^n a_i X^i \in R[X]$ . Dann heißt

$$I(f) := ggT\{a_i \mid a_i \neq 0\}$$

der *Inhalt* von  $f$ , und  $f$  heißt *primitiv*, wenn  $I(f) \sim 1$ .

**Bemerkung 7.2** Ist  $f$  normiert, so ist  $f$  primitiv; ebenso, falls ein Koeffizient eine Einheit ist.

**Beispiele 7.3** (a)  $3X^2 + 4X + 6$  ist primitiv in  $\mathbb{Z}[X]$ .

(b) In  $K[X]$ ,  $K$  Körper, ist jedes Polynom  $\neq 0$  primitiv.

**Lemma 7.4** (von Gauß) Sei  $R$  faktoriell. Sind  $f, g \in R[X]$  primitiv, so ist auch  $f \cdot g$  primitiv. Genauer gilt für  $f, g \in R[X]$ :

$$I(f \cdot g) \sim I(f) \cdot I(g).$$

**Beweis** 1) Seien  $f$  und  $g$  primitiv. Angenommen,  $f \cdot g$  ist nicht primitiv. Dann gibt es ein Primelement  $p \in R$  mit  $p \mid I(g)$ , also  $f \cdot g \equiv 0 \pmod{p}$ , d.h.,  $f \cdot g = 0$  in

$$R[X]/(p) = R[X]/pR[X] \cong (R/pR)[X].$$

Da  $R/pR = R/(p)$  ein Integritätsring ist, ist  $R/pR[X]$  auch ein Integritätsring (Satz 4.15). Es folgt also  $f = 0$  in  $R/pR[X]$  oder  $g = 0$  in  $R/pR[X]$ . Dies bedeutet aber  $p \mid I(f)$  oder  $p \mid I(g)$ .

2) Seien  $f, g \in R[X]$ . Dann ist  $f = I(f) \cdot f^*$  und  $g = I(g) \cdot g^*$  mit primitiven  $f^*, g^* \in R[X]$ . Es folgt

$$I(f \cdot g) = I(f) \cdot I(g) \cdot I(f^* \cdot g^*) \sim I(f) \cdot I(g),$$

da  $I(f^* \cdot g^*) \sim 1$  nach dem ersten Teil.

**Satz 7.5** (von Gauß) Sei  $R$  faktoriell und  $K = \text{Quot}(R)$ . Seien  $f, g \in R[X]$  mit  $g$  primitiv und  $g \mid f$  in  $K[X]$ . Dann  $g \mid f$  bereits in  $R[X]$ .

**Beweis** Sei  $f = g \cdot h$  mit  $h \in K[X]$ . Wähle  $b \in R \setminus \{0\}$  mit  $b \cdot h \in R[X]$  (Zum Beispiel sei  $b$  der Hauptnenner der Koeffizienten von  $h$ : für  $h := \sum_{i=0}^n \frac{a_i}{b_i} X^i$  mit  $a_i, b_i \in R$  können wir  $b := kgV(b_1, \dots, b_n)$  wählen). Dann gilt

$$bf = g \cdot (bh) \text{ in } R[X].$$

Es folgt

$$b \cdot I(f) = I(b \cdot f) = I(g) \cdot I(bh) = I(bh)$$

in  $R$ , da  $I(g) \sim 1$ , also  $b \mid I(bh)$ . Dann gilt bereits  $h = \frac{b \cdot h}{b} \in R[X]$ .

**Corollar 7.6** Sei  $R$  faktoriell,  $K = \text{Quot}(R)$  und  $f \in R[X]$  primitiv. Dann ist  $f(X)$  genau dann irreduzibel in  $R[X]$ , wenn  $f(X)$  irreduzibel in  $K[X]$  ist.

**Beweis** Sei  $f = g \cdot h$  in  $R[X]$  mit Nichteinheiten  $g, h$ . Wegen  $1 \sim I(f) = I(g) \cdot I(h)$  sind  $I(g)$  und  $I(h)$  Einheiten, also  $g$  und  $h$  primitiv. Daher haben  $g$  und  $h$  positiven Grad (sonst wäre  $g$  oder  $h$  in  $R^\times$ , also auch Einheit in  $R[X]$ ). Damit sind  $g$  und  $h$  auch Nicht-Einheiten in  $K[X]$ , also  $f$  reduzibel in  $K[X]$ .

Sei umgekehrt  $f$  reduzibel in  $K[X]$ , also  $f = g \cdot h$  mit  $g, h$  nicht konstant in  $K[X]$ . Wähle  $b \in K^\times$  mit  $bh \in R[X]$  primitiv (Wähle zum Beispiel  $b' \in R$  mit  $b'h \in R[X]$ ). Dann können wir

$$b = \frac{b'}{I(b'h)} \in K^\times$$

nehmen). Dann gilt

$$f = (b^{-1}g)(bh) \text{ in } K[X].$$

Mit Satz 7.5 folgt  $b^{-1}g \in R[X]$ ; wir erhalten also eine Zerlegung in Nicht-Einheiten in  $R[X]$ .

Durch die vorigen Sätze können wir für einen Körper  $K = \text{Quot}(R)$ , wobei  $R$  faktoriell ist (zum Beispiel für  $\mathbb{Q} = \text{Quot}(\mathbb{Z})$ ), die Irreduzibilität eines Polynoms  $f \in K[X]$  im Polynomring  $R[X]$  untersuchen (wähle  $a \in K^\times$  mit  $af \in R[X]$  und primitiv). Dies ist wegen der folgenden zwei Sätze nützlich.

**Satz 7.7** Sei  $R$  ein Integritätsring, sei  $p \in R$  ein Primideal und  $f \in R[X]$  ein primitives Polynom, dessen höchster Koeffizient nicht von  $p$  geteilt wird. Sei  $\bar{f} := f \pmod{p}$  das Bild von  $f$  in  $R/(p)[X]$ . Ist  $\bar{f}$  irreduzibel, so ist  $f$  irreduzibel in  $R[X]$ .

**Beweis** Angenommen  $f$  ist reduzibel, also  $f = g \cdot h$  in  $R[X]$  mit Nicht-Einheiten  $g, h$ , also  $\deg(g), \deg(h) > 0$  (vergleiche den Beweis von 7.6). Dann werden die Leitkoeffizienten von  $g$  und  $h$  nicht durch  $p$  geteilt, da sonst  $p$  den Leitkoeffizienten von  $f$  teilen würde. Damit ist

$$\bar{f} = \bar{g} \cdot \bar{h} \quad \text{in} \quad \mathbb{Z}/(p)[X]$$

eine Zerlegung in nicht-konstant Polynome, im Widerspruch zur Voraussetzung.

**Beispiel 7.8** Betrachte  $f(X) = X^3 + 3X^2 - 4X - 1 \in \mathbb{Q}[X]$ . Wir fassen  $f$  als ein primitives Polynom in  $\mathbb{Z}[X]$  auf und reduzieren die Koeffizienten modulo 3. Wir erhalten das Polynom

$$\bar{f}(X) = X^3 - X - \bar{1} \in \mathbb{Z}/3\mathbb{Z}[X].$$

Dieses ist irreduzibel: Falls nicht, so würde es einen Linearfaktor abspalten, hätte also eine Nullstelle in  $\mathbb{Z}/3\mathbb{Z}$ . Es ist aber

$$\bar{f}(0) = -\bar{1} \neq 0, \quad \bar{f}(1) = -\bar{1} \neq 0, \quad \bar{f}(2) = -\bar{1} \neq 0.$$

Nach 7.7 und 7.6 ist  $f(X)$  also irreduzibel in  $\mathbb{Q}[X]$ .

**Bemerkung 7.9** Sei  $K$  ein Körper. Ein Polynom  $f \in K[X]$  vom Grad 2 oder 3 ist genau dann reduzibel, wenn es eine Nullstelle in  $K$  hat.

**Satz 7.10** (Eisenstein-Kriterium) Sei  $R$  ein faktorieller Ring,  $p \in R$  ein Primelement und

$$f(X) = a_n X^n + a_{n-1} X^{n-1} + \dots + a_1 X + a_0 \in R[X]$$

mit

$$(7.10.1) \quad p \nmid a_n, \quad p \mid a_i \quad \text{für} \quad i < n, \quad p^2 \nmid a_0.$$

Dann ist  $f(X)$  irreduzibel in  $K[X]$  für  $K = \text{Quot}(R)$ .

**Beweis** Sei  $d = I(f)$  und  $f^* = f/d \in R[X]$ . Dann ist  $f^*$  primitiv und seine Koeffizienten  $a_i^*$  erfüllen wieder die Bedingungen (7.10.1), denn nach Voraussetzung ist  $a_i = a_i^* \cdot d$  und  $p \nmid d$  wegen  $p \nmid a_n$ . Also ist ohne Einschränkung  $f$  primitiv und dann genügt es (nach 7.6) zu zeigen, dass  $f(X)$  irreduzibel in  $R[X]$  ist.

Angenommen,  $f = gh$  in  $R[X]$  mit Nicht-Einheiten  $g, h \in R[X]$ , also  $\deg(f), \deg(h) > 0$  (vergleiche den Beweis von 7.6). Wegen  $p \nmid a_n$  werden die Leitkoeffizienten von  $g$  und  $h$  beide nicht durch  $p$  geteilt. Damit ist unter Reduktion modulo  $p$  und Berücksichtigung von (7.10.1)

$$\bar{f} = \bar{a}_n X^n = \bar{g} \cdot \bar{h} \quad \text{in} \quad R/(p)[X]$$

mit nicht-konstanten Polynomen  $\bar{g}, \bar{h}$ . Da  $X$  ein Primelement in  $\bar{R} := R/(p)[X]$  ist (denn offenbar ist  $R/(X) \cong R/(p)$  Integritätsring), folgt induktiv leicht  $\bar{g} = \alpha X^r, \bar{h} = \beta X^s$  mit  $\alpha, \beta \in R/(p)$  und  $0 < r, s < n, r + s = n$ . Daher ist

$$\begin{aligned} g &= b_r X^r + b_{r-1} X^{r-1} + \dots + b_1 X + b_0, \\ h &= c_s X^s + c_{s-1} X^{s-1} + \dots + c_1 X + c_0, \end{aligned}$$

mit  $p \nmid b_r, p \nmid c_s$  und

$$p \mid b_0, \dots, b_{r-1}, c_0, \dots, c_{s-1}.$$

Es folgt  $p^2 \mid b_0 \cdot c_0 = a_0$ , im Widerspruch zur Voraussetzung.  
(Siehe Bosch 'Algebra' 2.8 Satz 1 für einen anderen Beweis)

**Beispiele 7.11** (a)  $f(X) = X^4 + 15X^3 + 25X + 105$  ist irreduzibel in  $\mathbb{Q}[X]$ .

(b) Sei  $p$  eine Primzahl. Die Nullstellen des Polynoms  $X^p - 1$  in  $\mathbb{C}$  sind die  $p$ -ten Einheitswurzeln. Dieses Polynom ist über  $\mathbb{Q}$  nicht irreduzibel, denn es hat die Nullstelle 1. Betrachte

$$\Phi_p(X) = \frac{X^p - 1}{X - 1} = X^{p-1} + X^{p-2} + \dots + X + 1 \in \mathbb{Q}[X].$$

Dieses Polynom ist irreduzibel in  $(\mathbb{Z}[X])$  und  $\mathbb{Q}[X]$ : Das Eisenstein-Kriterium ist nicht direkt anwendbar, aber betrachte

$$\Phi_p(X+1) = \frac{(X+1)^p - 1}{(X+1) - 1} = X^{p-1} + \binom{p}{1} X^{p-2} + \dots + \binom{p}{i} X^{p-i-1} + \binom{p}{p-2} X + \binom{p}{p-1}.$$

Es ist

$$\binom{p}{i} = \frac{p(p-1)\dots(p-i+1)}{i(i-1)\dots 1} \equiv 0 \pmod{p} \text{ für } i < p$$

und

$$\binom{p}{p-1} = p \not\equiv 0 \pmod{p^2}.$$

Nach dem Eisenstein-Kriterium ist  $\Phi_p(X+1)$  irreduzibel in  $\mathbb{Q}[X]$ , also auch  $\Phi_p(X)$  (beachte:  $f(X) \mid \Phi_p(X) \Rightarrow f(X+1) \mid \Phi_p(X)$ ). Das Polynom  $\Phi_p(X)$  heißt das  $p$ -te Kreisteilungspolynom.

Wir zeigen nun noch einen Vererbungssatz für faktorielle Ringe.

**Satz 7.12** (Satz von Gauß) Ist  $R$  faktoriell, so auch der Polynomring  $R[X]$ .

**Beweis:** Sei  $K = \text{Quot}(R)$ . Dann ist  $K[X]$  faktoriell. Sei  $f \in R[X] \setminus \{0\}$ . Dann ist  $f = I(f) \cdot f^*$  mit  $I(f) \in R$  und  $f^* \in R[X]$  primitiv.  $I(f)$  ist Einheit in  $R$  oder Produkt von Primelementen in  $R$ , aber jedes Primelement  $p \in R$  ist auch Primelement in  $R[X]$ , denn

$$R[X]/(p) = R[X]/pR[X] \cong R/pR[X]$$

ist integer.

Also genügt es zu zeigen, dass  $f^*$  eine Einheit oder ein Produkt von Primelementen in  $R[X]$  ist. Ist  $\deg(f^*) = 0$ , so ist  $f^* \in R$ , also  $f^* \in R^\times$  (da  $f^*$  primitiv ist), also Einheit in  $R[X]$ . Ist  $\deg(f^*) > 0$ , so ist  $f^*$  keine Einheit in  $K[X]$ , also  $f^* = \prod_{i=1}^n f_i$  mit  $n \geq 1$  und Primelementen  $f_i \in K[X]$ . Wähle  $a_i \in K^\times$ , so dass für jedes  $i \in \{1, \dots, n\}$   $f_i^* := a_i f_i \in R[X]$  und primitiv ist. Dann ist  $f_i^*$  immer noch prim in  $K[X]$  ( $a_i$  Einheit in  $K$ ). Nach dem Satz von Gauß 7. ist  $f_i^*$  dann prim in  $R[X]$ . Wegen  $\prod_{i=1}^n a_i f^* = \prod_{i=1}^n f_i^*$  und der Primitivität

von  $f^*$  und  $\prod_{i=1}^n f_i^*$  ist  $\prod_{i=1}^n a_i$  eine Einheit in  $R$  (Lemma von Gauß 7.). Also besitzt  $f^* \sim \prod_{i=1}^n f_i^*$  eine Zerlegung in Primfaktoren.

**Corollar 7.13** Ist  $R$  faktoriell, so ist für jedes  $n \in \mathbb{N}$  der Polynomring  $R[X_1, \dots, X_n]$  faktoriell. Insbesondere ist  $\mathbb{Z}[X_1, \dots, X_n]$  faktoriell sowie  $K[X_1, \dots, X_n]$ , wenn  $K$  ein Körper ist.

Zum Schluss besprechen wir noch das konstruktive Verfahren von Kronecker zur Bestimmung der irreduziblen Faktoren von Polynomen  $f(X) \in \mathbb{Z}[X]$ .

**Vorbemerkung 7.14** Sei  $K$  ein Körper der Charakteristik 0 (also z.B.  $K = \mathbb{Q}, \mathbb{R}$  oder  $\mathbb{C}$ ). Seien  $x_0, \dots, x_n \in K$  paarweise verschieden und  $y_0, \dots, y_n \in K$  beliebig. Dann gibt es genau ein Polynom

$$g(X) = a_0 + a_1X + \dots + a_nX^n \in K[X]$$

$n$ -ten Grades mit

$$g(x_i) = y_i \quad (i = 0, \dots, n).$$

**Beweis:** Wir haben das lineare Gleichungssystem

$$\begin{pmatrix} 1 & x_0 & x_0^2 & \dots & x_0^n \\ 1 & x_1 & x_1^2 & \dots & x_1^n \\ \vdots & \vdots & \vdots & & \vdots \\ 1 & x_n & x_n^2 & \dots & x_n^n \end{pmatrix} \begin{pmatrix} a_0 \\ a_1 \\ \vdots \\ a_n \end{pmatrix} = \begin{pmatrix} y_0 \\ y_1 \\ \vdots \\ y_n \end{pmatrix}$$

zu lösen. Die Determinante der Matrix ist die Vandermonde'sche Determinante, nämlich

$$\prod_{i < j} (x_j - x_i) \neq 0$$

(da die  $x_i$  paarweise verschieden sind). Daher gibt es eine eindeutige Lösung  $a_0, \dots, a_n$ .

**Bemerkung 7.15** Explizit kann man  $g(X)$  auch durch die Interpolationspolynome von Lagrange bzw. Newton bestimmen (siehe Numerik, Approximationstheorie).

**Kronecker-Verfahren 7.16:** Sei  $f \in \mathbb{Z}[X]$  und sei  $g \in \mathbb{Z}[X]$  ein Polynom vom Grad  $m$ , welches  $f$  teilt. Dann gibt es nur endlich viele Möglichkeiten für  $g$ . Für jedes  $r \in \mathbb{Z}$  gilt nämlich  $g(r) \mid f(r) \in \mathbb{Z}$ , also gibt es nur endlich viele Möglichkeiten für  $g(r)$ . Sind  $x_0, \dots, x_m \in \mathbb{Z}$  paarweise verschieden, so gibt es also nur endlich viele Möglichkeiten für  $(g(x_0), \dots, g(x_m))$  und nach 7.14 genau soviele Möglichkeiten für  $g$ .

**Beispiele 7.17:** Betrachte  $f(X) = X^4 - X + 1$ . Eisenstein-Kriterium – schwierig! Linearfaktor: Falls  $aX - b \mid X^4 - X + 1$  ( $a, b \in \mathbb{Z}$ ), so  $a \mid 1$  und  $b$  teilt 1, also  $a, b \in \{\pm 1\}$ . Aber 1 und  $-1$  sind keine Nullstellen von  $f(X)$ . Bleiben quadratische Faktoren zu überprüfen: Betrachte (ohne Einschränkung)  $g(X) = X^2 + aX + b$ . Gilt  $g \mid f$ , so folgt

$$\begin{aligned} b &= g(0) \mid f(0) = 1 \Rightarrow b = \pm 1 \\ 1 + a + b &= g(1) \mid f(1) = 1 \Rightarrow a = \pm 1 - 1 + b \end{aligned}$$

Die möglichen Teiler sind also

$$g(X) = \begin{cases} X^2 - X + 1 \\ X^2 + X - 1 \\ X^2 - 3X + 1 \\ X^2 - X - 1 \end{cases} .$$

Polynomdivision zeigt: Keins dieser Polynome teilt  $f$ . Also ist  $f$  irreduzibel in  $\mathbb{Z}[X]$ , also auch in  $\mathbb{Q}[X]$ , da  $f$  primitiv ist.

## §8 Körper und Körpererweiterungen; grundlegende Definitionen

Ist  $R$  ein Ring mit Eins, so gibt es einen eindeutig bestimmten Homomorphismus von Ringen mit Eins

$$\varphi : \mathbb{Z} \rightarrow R,$$

nämlich  $\varphi(n) = n \cdot 1$ .

**Definition 8.1** Sei  $K$  ein Körper. Die Charakteristik von  $K$  (Bez.  $\text{char}(K)$ ) ist die eindeutig bestimmte Zahl  $n \in \mathbb{N}_0$  mit  $\ker(\varphi) = n\mathbb{Z}$ .

**Lemma 8.2** (a)  $\text{char}(K) = 0 \Leftrightarrow n \cdot 1 \neq 0$  für alle  $n \in \mathbb{N} \Leftrightarrow n \cdot x \neq 0$  für alle  $x \in K \setminus \{0\}$ .

(b) Ist  $\text{char}(K) \neq 0$ , so ist  $\text{char}(K) = p$  eine Primzahl und die kleinste Zahl  $n \in \mathbb{N}$  mit  $n \cdot 1 = 0$ . Es ist dann  $px = 0$  für alle  $x \in K$ .

**Beweis** (a) ist klar, da  $n \cdot x = (n \cdot 1)x$  und  $K$  nullteilerfrei ist.

(b) Sei  $m = \text{char}(K)$ , dann ist nach dem Homomorphiesatz  $\mathbb{Z}/m\mathbb{Z}$  isomorph zu einem Unterring von  $K$ , also ein Integritätsring. Es folgt, dass  $m$  eine Primzahl ist (Satz 3.34). Die anderen Aussagen sind klar (vergleiche auch den Beweis von Lemma 2.6).

**Beispiele 8.3** (a)  $\mathbb{Q}, \mathbb{R}$  und  $\mathbb{C}$  sind Körper der Charakteristik 0.

(b) Für jede Primzahl  $p$  ist der Ring  $\mathbb{Z}/p\mathbb{Z}$  ein Körper der Charakteristik  $p$ .

**Definition 8.4** (a) Eine Teilmenge  $k$  eines Körpers  $K$  heißt Teilkörper, wenn gilt:

(i) Mit  $a, b \in k$  liegen auch  $a + b$  und  $a \cdot b$  in  $k$ ,

(ii)  $k$  ist mit den Einschränkungen der Verknüpfungen  $+$  und  $\cdot$  ein Körper.

(b)  $K$  heißt dann Erweiterungskörper von  $k$ , und das Paar  $(K, k)$  (man schreibt meist  $K/k$ ) heißt Körpererweiterung.

(c) Ein Teilkörper  $L$  von  $K$  mit  $k \subseteq L \subseteq K$  heißt Zwischenkörper der Körpererweiterung.

**Bemerkung 8.5** Ist  $K/k$  eine Körpererweiterung, so ist  $\text{char}(k) = \text{char}(K)$ , da bereits  $1 \in k$ .

**Definition 8.6** Sei  $K$  ein Körper. Dann ist

$$P = \bigcap_{k \subset K \text{ Teilkörper}} k$$

offenbar der kleinste Teilkörper von  $K$  und heißt der Primkörper von  $K$ .

**Lemma 8.7** Sei  $K$  ein Körper.

(a)  $\text{char}(K) = 0 \Leftrightarrow P \cong \mathbb{Q}$ .

(b)  $\text{char}(K) = p > 0 \Leftrightarrow P \cong \mathbb{Z}/p\mathbb{Z}$ .

Insbesondere sind die Körper  $\mathbb{Q}$  und  $\mathbb{Z}/p\mathbb{Z}$  ( $p$  prim) bis auf kanonische Isomorphie die einzigen Primkörper. Man schreibt auch oft  $\mathbb{F}_p$  für den eindeutig bestimmten Körper mit  $p$  Elementen  $\mathbb{Z}/p\mathbb{Z}$ .

**Beweis** Die Implikationen “ $\Leftarrow$ ” folgen aus 8.5. Ist umgekehrt  $\text{char}(K) = 0$ , so ist  $\varphi : \mathbb{Z} \rightarrow K$  ein Monomorphismus und induziert nach der universellen Eigenschaft des Quotientenkörpers einen Monomorphismus von Körpern  $\phi : \mathbb{Q} \hookrightarrow K$ . Nach der Minimalität von  $P$  ist  $P = \text{im}(\phi)$ , also  $\mathbb{Q} \xrightarrow{\sim} P$ . Ist  $\text{char}(K) = p > 0$ , so hat man  $\ker(\varphi) = p\mathbb{Z}$  und entsprechend nach dem Homomorphiesatz einen Isomorphismus  $\mathbb{Z}/p\mathbb{Z} \xrightarrow{\sim} \text{Im}(\varphi) = P$ .

Ist  $K/k$  eine Körpererweiterung, so wird  $K$  zu einem  $k$ -Vektorraum durch die Addition  $+$  in  $K$  und die Skalarmultiplikation  $rs = r \cdot s$  (Multiplikation in  $K$ ) für  $r \in k, s \in K$ .

**Definition 8.8** Die (Kardinal-)Zahl  $\dim_k K$  (=Mächtigkeit einer Basis von  $K$  über  $k$ ) heißt der Grad von  $K$  über  $k$  (Bez.:  $[K : k]$ ).

**Satz 8.9** (Gradsatz) Ist  $K/k$  eine Körpererweiterung und  $L$  ein Zwischenkörper, so ist

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

**Beweis** Sei  $(x_i)_{i \in I}$  eine Basis von  $L$  über  $k$  und  $(y_j)_{j \in J}$  eine Basis von  $K$  über  $L$ , so bildet die Familie  $(x_i y_j)_{(i,j) \in I \times J}$  eine Basis von  $K$  über  $k$ :

*Lineare Unabhängigkeit:* Ist  $\sum_{i,j} \alpha_{ij} x_i y_j = 0$ , mit  $\alpha_{ij} \in k$ , fast alle null, so ist  $\sum_i \alpha_{ij} x_i = 0$  für alle  $j \in J$ , wegen der linearen Unabhängigkeit der  $y_j$ , also  $\alpha_{ij} = 0$  für alle  $i \in I$  und  $j \in J$ , wegen der linearen Unabhängigkeit der  $x_i$ .

*Erzeugendensystem:* Ist  $y \in K$ , so gibt es nach Voraussetzung  $j_1, \dots, j_n \in J$  und  $b_1, \dots, b_n \in L$  mit

$$y = \sum_{\nu=1}^n b_\nu y_{j_\nu}.$$

Weiter gibt es  $i_1, \dots, i_m \in I$  und  $a_{\mu,\nu} \in k$ ,  $\nu = 1, \dots, n$ ,  $\mu = 1, \dots, m$ , mit

$$b_\nu = \sum_{\mu=1}^m a_{\mu,\nu} x_{i_\mu}.$$

Es folgt

$$y = \sum_{\nu=1}^n b_\nu y_{j_\nu} = \sum_{\nu=1}^n \sum_{\mu=1}^m a_{\mu,\nu} x_{i_\mu} y_{j_\nu}.$$

Zusammen ergibt sich nun:  $[K : k] = |I \times J| = |I| \cdot |J| = [L : k] \cdot [K : L]$ .

**Bemerkung 8.10**  $[K : k] = 1 \Leftrightarrow K = k$ .

**Lemma/Definition 8.11** Sei  $K/k$  eine Körpererweiterung und  $A \subset K$  eine Teilmenge. Dann ist

$$k[A] := \bigcap_{\substack{R \subset K \text{ Unterring} \\ k \subset R, A \subset R}} R$$

der kleinste Unterring von  $K$ , der  $k$  und  $A$  enthält, und heißt der von  $A$  über  $k$  erzeugte Unterring von  $K$ . Weiter ist

$$k(A) := \bigcap_{\substack{L \subset K \text{ Teilkörper} \\ k \subset L, A \subset L}} L$$

der kleinste Zwischenkörper von  $K/k$ , der  $A$  enthält, und heißt der von  $A$  über  $k$  erzeugte Teilkörper von  $K$ . Man sagt auch, dass  $k[A]$  (bzw.  $k(A)$ ) durch Adjunktion der Elemente in  $A$  entsteht. Für  $A = \{a_1, \dots, a_n\}$  schreibt man meist  $k[a_1, \dots, a_n]$  bzw.  $k(a_1, \dots, a_n)$ .

Der Beweis der Behauptungen ist klar.

**Lemma 8.12** (a) Für endliches  $A$  ist  $k[A]$  das Bild des Einsetzungshomomorphismus

$$\phi : k[X_a \mid a \in A] \rightarrow K \quad X_a \mapsto a.$$

Insbesondere ist

$$k[a_1, \dots, a_n] = \{f(a_1, \dots, a_n) \mid f(X_1, \dots, X_n) \in k[X_1, \dots, X_n]\}.$$

(Hierbei seien  $k[X_a \mid a \in A]$  bzw.  $k[X_1, \dots, X_n]$  die Polynomringe in den Variablen  $X_a$  bzw.  $X_i$ ).

(b) Es ist  $k(A)$  der Quotientenkörper von  $k[A]$ .

(c) Für Teilmengen  $A, B$  von  $K$  gilt  $k(A \cup B) = (k(A))(B)$ .

**Beweis** (a) Für jeden Ring  $R \subseteq K$  mit  $k \subset R$  und  $A \subset R$  hat man  $\text{im}(\phi) \subseteq R$ , und  $\text{im}(\phi)$  ist selbst so ein Ring.

(b) Offenbar ist  $k[A] \subset k(A)$ , und nach der universellen Eigenschaft des Quotientenkörpers  $Q(k[A])$  gibt es einen Monomorphismus  $\varphi : Q(k[A]) \hookrightarrow k(A)$ , der die Inklusion fortsetzt. Wegen der Minimalität von  $k(A)$  ist  $\text{im}(\varphi) = k(A)$ , also  $\varphi$  ein Isomorphismus.

(c) Für jeden Teilkörper  $L$  von  $K$  gilt

$$k \cup A \cup B \subset L \Leftrightarrow k(A) \cup B \subset L.$$

**Bemerkungen 8.13** (a) In 8.12 (b) und (c) haben wir nicht vorausgesetzt, dass  $A$  und  $B$  endlich sind.

(b) 8.12 (a) gilt auch für unendliches  $A$ , wenn  $k[X_a \mid a \in A]$  der Polynomring in den unendlich vielen Variablen  $X_a (a \in A)$  ist (siehe später).

**Definition 8.14** Eine Körpererweiterung  $K/k$  heißt einfach, wenn es ein Element  $a \in K$  gibt mit  $K = k(a)$ , und  $a$  heißt dann primitives Element für  $K/k$ .

**Beispiel 8.15** Es ist  $[\mathbb{C} : \mathbb{R}] = 2$  ( $\{1, i\}$  ist eine  $\mathbb{R}$ -Basis von  $\mathbb{C}$ ). Insbesondere hat die Erweiterung  $\mathbb{C}/\mathbb{R}$  nach dem Gradsatz 8.9 keine echten Zwischenkörper. Offenbar ist  $\mathbb{R}[i] = \mathbb{C}$ , und dies ist gleich  $\mathbb{R}(i)$ , da  $\mathbb{C}$  ein Körper ist. Daher ist  $i$  ein primitives Element für  $\mathbb{C}/\mathbb{R}$ .

## §9 Algebraische und transzendente Elemente

Sei  $K/k$  eine Körpererweiterung.

**Definition 9.1** Ein Element  $a \in K$  heißt algebraisch über  $k$ , wenn es ein Polynom  $f \in k[X] \setminus \{0\}$  gibt mit  $f(a) = 0$ . Andernfalls heißt  $a$  transzendent über  $k$ .

Sei  $\varphi_a : k[X] \rightarrow K$  mit  $f(X) \mapsto f(a)$  der Einsetzungshomomorphismus. Dann ist  $a$  offenbar genau dann algebraisch über  $k$ , wenn  $\ker(\varphi_a) \neq \{0\}$  ist. In diesem Fall gibt es nach Corollar 5.5 genau ein normiertes Polynom  $f_a \in k[X]$  mit  $\ker(\varphi_a) = (f_a) \subset k[X]$ .

**Definition 9.2** Ist  $a \in K$  algebraisch über  $k$ , so heißt das Polynom  $f_a$  das Minimalpolynom von  $a$  über  $k$ .

**Proposition 9.3** Sei  $a \in K$  algebraisch über  $k$ . Für ein normiertes Polynom  $g \in k[X]$  sind dann äquivalent:

- (a)  $g$  ist das Minimalpolynom von  $a$ .
- (b)  $g(a) = 0$ , und für jedes  $0 \neq h \in k[X]$  mit  $h(a) = 0$  gilt  $\deg(g) \leq \deg(h)$ .
- (c)  $g(a) = 0$ , und für jedes  $0 \neq h \in k[X]$  mit  $h(a) = 0$  gilt  $g \mid h$ .
- (d)  $g(a) = 0$ , und  $g$  ist irreduzibel.

**Beweis** (a)  $\Rightarrow$  (c): Wegen  $\ker(\varphi_a) = (f_a)$  gilt für jedes  $h \in \ker(\varphi_a) : h = f_a \cdot h'$  für ein  $h' \in k[X]$ , also  $f_a \mid h$  für  $h \neq 0$ .

(c)  $\Rightarrow$  (b) ist trivial ( $g \mid h \Rightarrow \deg(g) \leq \deg(h)$  für  $h \neq 0$ ).

(b)  $\Rightarrow$  (d): Aus  $g = g' \cdot g''$  mit  $g', g'' \in k[X]$  folgt  $0 = g(a) = g'(a) \cdot g''(a)$ . Ist (ohne Einschränkung)  $g'(a) = 0$ , so ist nach (b)  $\deg(g) \leq \deg(g')$ . Wegen  $\deg(g) = \deg(g') + \deg(g'')$  ist dann  $\deg(g'') = 0$ , also  $g'' \in k^\times$ .

(d)  $\Rightarrow$  (a) Ist  $g \in \ker(\varphi_a)$ , so folgt  $g = f_a g'$  mit  $g' \in k[X]$ . Ist  $g$  irreduzibel, so ist  $g' \in k^\times$  (da  $f_a$  wegen  $f_a(a) = 0$  keine Einheit ist) und damit  $g = f_a$  wegen der Normiertheit beider Polynome.

**Beispiel 9.4** Ist  $m \in \mathbb{Z}$  kein Quadrat (in  $\mathbb{Z}$ ) – also z.B. eine Primzahl – so ist  $\sqrt{m} \in \mathbb{C} \setminus \mathbb{Q}$  und  $X^2 - m$  das Minimalpolynom von  $\sqrt{m}$  über  $\mathbb{Q}$  (es kommt nicht darauf an, welche Wurzel wir in  $\mathbb{C}$  wählen).

**Satz 9.5** Sei  $a \in K$  algebraisch mit Minimalpolynom  $f_a \in k[X]$ . Dann gilt:

(a)  $k[a] = k(a) \cong k[X]/(f_a)$ .

(b)  $[k(a) : k] = \deg(f_a)$ . Genauer gilt: Ist  $m = \deg(f_a)$ , so bilden  $1, a, \dots, a^{m-1}$  eine  $k$ -Basis von  $k(a)$ .

**Beweis** (a) Nach dem Homomorphiesatz und 8.12 (a) ist

$$k[X]/(f_a) = k[X]/\ker(\varphi_a) \xrightarrow{\sim} k[a].$$

Andererseits ist  $f_a$  nach 9.3 (d) irreduzibel und daher  $(f_a)$  ein maximales Ideal (Lemma 6.17). Damit ist  $k[a] \cong k[X]/(f_a)$  ein Körper und es folgt  $k[a] = k(a)$ .

(b) Ist  $b \in k[a]$ , so gibt es nach 8.12 (a) ein  $g \in k[X]$  mit  $b = g(a)$ . Ist  $g \neq 0$ , so gibt es  $q, r \in k[X]$  mit  $\deg(r) < m$  und  $g = q \cdot f_a + r$ . Es folgt  $g(a) = r(a) = \sum_{i=0}^{m-1} c_i a^i$  mit  $c_i \in k$ ; d.h.,  $1, a, \dots, a^{m-1}$  bildet ein Erzeugendensystem des  $k$ -Vektorraums  $k[a]$ . Diese Elemente sind linear unabhängig: wäre

$$\sum_{i=0}^{m-1} c_i a^i = 0, \quad c_i \in k, \quad \text{nicht alle null,}$$

so wäre  $\sum_{i=0}^{m-1} c_i X^i \in \ker(\varphi_a)$  und vom Grad  $< m$  im Widerspruch zu 9.3(b).

Für transzendente Elemente haben wir:

**Satz 9.6** Die folgenden Aussagen sind äquivalent für  $a \in K$ :

(a)  $a$  ist transzendent über  $k$ .

(b)  $\varphi_a : k[X] \xrightarrow{\sim} k[a]$  ist ein Isomorphismus.

(c)  $k[a] \neq k(a)$ .

(d)  $[k(a) : k] = \infty$ .

**Beweis** (a)  $\Leftrightarrow \ker(\varphi_a) = 0 \Leftrightarrow$  (b) ist klar. Gilt (b), so ist  $[k(a) : k] \geq \dim_k k[a] = \dim_k k[X] = \infty$ , da die Monome  $1, X, X^2, \dots$  linear unabhängig über  $k$  sind, und es ist  $k[a] \neq k(a)$ , da  $k[X]$  kein Körper ist (z.B. besitzt  $X$  kein Inverses in  $k[X]$ ). Umgekehrt kann für (c) oder (d) das Element  $a$  nach 9.5 nicht algebraisch sein.

**Bemerkungen 9.7** Die Zahlen  $\pi$  bzw.  $e \in \mathbb{R}$  sind transzendent (d.h., transzendent über  $\mathbb{Q}$ ), nach tiefliegenden Sätzen von Lindemann und Hermite.

**Definition 9.8** Eine Körpererweiterung  $K/k$  heißt algebraisch, wenn jedes  $a \in K$  algebraisch über  $k$  ist, und andernfalls transzendent.

**Satz 9.9** Für  $K/k$  sind äquivalent:

(a)  $K/k$  ist endlich.

(b)  $K$  ist endlich erzeugt über  $k$  (d.h., es gibt  $a_1, \dots, a_n \in K$  mit  $K = k(a_1, \dots, a_n)$ ) und  $K/k$  ist algebraisch.

(c) Es gibt über  $k$  algebraische Elemente  $a_1, \dots, a_n \in K$  mit  $K = k(a_1, \dots, a_n)$ .

**Beweis** (a)  $\Rightarrow$  (b): Ist  $m = [K : k] < \infty$ , so sind für jedes  $a \in K$  die  $m + 1$  Potenzen  $1, a, a^2, \dots, a^m$  linear abhängig über  $k$ ,  $a$  also die Nullstelle eines nicht-trivialen Polynoms  $m$ -ten Grades in  $k[X]$ . Ist  $a_1, \dots, a_n$  eine  $k$ -Basis von  $K$ , so ist offenbar  $K = k[a_1, \dots, a_n] = k(a_1, \dots, a_n)$ .

(b)  $\Rightarrow$  (c): ist trivial.

(c)  $\Rightarrow$  (a): Wegen  $K = k(a_1, \dots, a_{n-1})(a_n)$  folgt dies durch Induktion aus 9.5 und dem Gradsatz 8.9: ist  $a_n$  algebraisch über  $k$ , so erst recht über  $K' := k(a_1, \dots, a_{n-1})$ , und damit  $[K : K'] = [K'(a_n) : K'] < \infty$ .

**Corollar 9.10** Ist  $K/k$  eine Körpererweiterung und  $L$  ein Zwischenkörper, so ist äquivalent:

(a)  $K/k$  algebraisch.

(b)  $K/L$  und  $L/k$  algebraisch.

**Beweis** (a)  $\Rightarrow$  (b) ist trivial.

(b)  $\Rightarrow$  (a): Ist  $a \in K$ , so gibt es nach (b) ein Polynom

$$f = \sum_{i=0}^n b_i X^i \in L[X]$$

mit  $f(a) = 0$ , und wiederum sind  $b_0, \dots, b_n$  algebraisch über  $k$ . Ist  $k' = k(b_0, \dots, b_n)$ , so folgt mit 9.9  $[k(a) : k] \leq [k'(a) : k] = [k'(a) : k'] \cdot [k' : k] < \infty$ , da  $a$  algebraisch über  $k'$  ist. Damit ist wiederum  $a$  algebraisch über  $k$ .

## §10 Zerfällungskörper und normale Körpererweiterungen

Ist  $f \in \mathbb{Q}[X]$ , so kann es passieren, dass  $f$  keine Nullstelle in  $\mathbb{Q}$  hat. Aber nach dem ‘Fundamentalsatz der Algebra’ zerfällt  $f$  in  $\mathbb{C}[x]$  in Linearfaktoren. Wir zeigen in diesem Abschnitt für einen beliebigen Körper  $k$  und  $f(X) \in k[X]$ , dass es eine endliche Körpererweiterung  $L/k$  gibt, so dass  $f$  in  $L[X]$  in Linearfaktoren zerfällt.

**Satz 10.1** Sei  $k$  ein Körper und  $f \in k[X]$  nicht konstant. Dann gibt es einen Erweiterungskörper  $K/k$  und ein  $a \in K$  mit  $f(a) = 0$ .

**Beweis** Sei  $f = p \cdot f'$  mit einem irreduziblen Polynom  $p$ . Dann ist  $K := k[X]/(p)$  nach Lemma 6.17 ein Körper und die Komposition  $k \rightarrow k[X] \rightarrow K$  injektiv (wie jeder Körperhomomorphismus, siehe 6.4 (b)). Wir können also  $k$  als Teilkörper von  $K$  auffassen. Für  $g(x) \in k[X]$  sei  $\overline{g(X)} := g(x) \bmod (p)$  das Bild von  $g(X)$  in  $K = k[X]/(p)$ . Das Element  $a = \overline{X} \in K$  ist dann eine Nullstelle von  $p$  über  $K$ , denn es ist  $p(a) = p(\overline{X}) = \overline{p(X)} = 0$ . Daher ist auch  $f(a) = 0$ .

**Definition 10.2** Eine Körpererweiterung  $K/k$  heißt Zerfällungskörper eines nicht-konstanten Polynoms  $f \in k[X]$ , wenn gilt:

(i)  $f$  zerfällt über  $K$  in Linearfaktoren, d.h., es gibt  $b, a_1, \dots, a_n \in K$  mit

$$f = b(X - a_1) \cdot (X - a_2) \dots (X - a_n) \quad \text{in } K[X].$$

(ii)  $K/k$  ist minimal mit dieser Eigenschaft, d.h.,  $f$  zerfällt über keinem echten Zwischenkörper  $K'$  von  $K/k$  in Linearfaktoren.

**Beispiel 10.3**  $\mathbb{Q}(\sqrt{2}) = \mathbb{Q}[\sqrt{2}]$  ist Zerfällungskörper von  $f = X^2 - 2$  über  $\mathbb{Q}$ .

**Satz 10.4** Sei  $k$  ein Körper und  $f \in k[X]$  nicht konstant.

(a) Es gibt einen Zerfällungskörper von  $f$  über  $k$ .

(b) Ist  $K$  eine Körpererweiterung von  $k$  und zerfällt  $f$  über  $K$  in Linearfaktoren  $X - a_1, \dots, X - a_n$ , so ist  $k(a_1, \dots, a_n) \subseteq K$  ein Zerfällungskörper von  $f$  über  $k$ .

**Beweis** Nach 10.1 erhält man einen Erweiterungskörper  $K_1$  von  $k$ , in dem  $f$  eine Nullstelle  $a_1$  hat. In  $K_1[X]$  erhalten wir dann durch Polynomdivision durch  $X - a_1$  ein Polynom  $f_1$  kleineren Grades mit  $f(X) = (X - a_1)f_1(X)$ . Nun können wir das Verfahren auf  $K_1$  und  $f_1(X)$  anwenden und weiter iterieren und bekommen so in endlich vielen Schritten einen Erweiterungskörper  $K$  von  $k$  und Elemente  $a_1, \dots, a_n \in K$  und  $b \in K$  mit  $f = b(X - a_1)(X - a_2) \dots (X - a_n)$  in  $K[X]$ . Es genügt also, (b) zu zeigen.

Offenbar zerfällt  $f$  über  $K' = k(a_1, \dots, a_n)$  in Linearfaktoren. Ist dies schon über einem Zwischenkörper  $L$  von  $K'/k$  der Fall, so gibt es  $b_1, \dots, b_n \in L$  mit  $f = b(X - b_1) \dots (X - b_2) \dots (X - b_n)$  in  $L[X]$ . Da  $K'[X]$  ein faktorieller Ring ist, gilt dann  $\{b_1, \dots, b_n\} = \{a_1, \dots, a_n\}$  und damit  $L = K'$ , wegen  $k(b_1, \dots, b_n) \subseteq L \subseteq k(a_1, \dots, a_n) = K'$ .

Die folgenden Untersuchungen zeigen, dass der Zerfällungskörper bis auf Isomorphie eindeutig ist. In den nächsten drei Sätzen betrachten wir die folgende Situation:

Seien  $K/k$  und  $\tilde{K}/\tilde{k}$  Körpererweiterungen,  $\varphi : k \rightarrow \tilde{k}$  ein Körperhomomorphismus, und sei mit  $\varphi : k[X] \rightarrow \tilde{k}[X]$  auch der zugehörige Homomorphismus der Polynomringe bezeichnet (bestimmt durch  $\varphi \left( \sum_{i=0}^n a_i X^i \right) = \sum_{i=0}^n \varphi(a_i) X^i$ ). Ferner sei  $f \in k[X]$  ein nicht konstantes Polynom und  $\tilde{f} = \varphi(f) \in \tilde{k}[X]$ .

**Satz 10.5** Sei  $f$  irreduzibel,  $a$  eine Nullstelle von  $f$  in  $K$  und  $\tilde{a}$  eine Nullstelle von  $\tilde{f}$  in  $\tilde{K}$ . Dann gibt es genau einen Homomorphismus

$$\tilde{\varphi} = \tilde{\varphi}_{a, \tilde{a}} : k(a) \rightarrow \tilde{k}(\tilde{a})$$

mit  $\tilde{\varphi}|_k = \varphi$  und  $\tilde{\varphi}(a) = \tilde{a}$ . Ist  $\varphi$  ein Isomorphismus, so auch  $\tilde{\varphi}$ .

**Beweis** Notwendigerweise gilt

$$\tilde{\varphi}(g(a)) = \varphi(g)(\tilde{a}) \quad \text{für jedes } g \in k[X],$$

d.h., das Diagramm

$$\begin{array}{ccccccc}
 g(X) & X & k[X] & \xrightarrow{\varphi} & \tilde{k}[X] & X & h(X) \\
 \downarrow & \downarrow & \varphi_a \downarrow & & \downarrow \varphi_{\tilde{a}} & \downarrow & \downarrow \\
 g(a) & a & k(a) & \xrightarrow{\tilde{\varphi}} & \tilde{k}(\tilde{a}) & \tilde{a} & h(\tilde{a})
 \end{array}$$

ist kommutativ. Dies zeigt die Eindeutigkeit von  $\tilde{\varphi}$ . Zur Wohldefiniertheit: Da  $f$  irreduzibel ist, gilt  $f = bf_a$ , wobei  $b \in k^\times$  und  $f_a$  das Minimalpolynom von  $a$  über  $k$  ist (9.3). Daher ist  $(f) = \ker(\varphi_a)$ . Ist also  $g_1(a) = g_2(a)$  für  $g_1, g_2 \in k[X]$ , so ist  $g_1 - g_2 \in (f)$ , und damit  $\varphi(g_1) - \varphi(g_2) = \varphi(g_1 - g_2) \in (\tilde{f})$ , d.h.,  $\varphi(g_1)(\tilde{a}) - \varphi(g_2)(\tilde{a}) = 0$  wegen  $\tilde{f}(\tilde{a}) = 0$ .

Ist  $\varphi$  ein Isomorphismus, so liefert die Anwendung auf  $\varphi^{-1}$ ,  $\varphi^{-1}\varphi = id_k$ , einen Homomorphismus  $\widetilde{\varphi^{-1}}: \tilde{k}(\tilde{a}) \rightarrow k(a)$ , wobei wegen der Eindeutigkeit gilt  $\widetilde{\varphi^{-1}}\tilde{\varphi} = \varphi^{-1}\varphi = id_k = id_{k(a)}$ ; ebenso folgt  $\tilde{\varphi}\varphi^{-1} = id_{\tilde{k}(\tilde{a})}$ .

**Corollar 10.6** Die Fortsetzungen

$$\psi : k(a) \rightarrow \tilde{K}$$

von  $\varphi : k \rightarrow \tilde{k}$  entsprechen gerade bijektiv den Nullstellen von  $\tilde{f}$  in  $\tilde{K}$ , vermöge  $\psi \mapsto \psi(a)$ .

**Beweis** Nach 10.5 erhalten wir für jede Nullstelle  $\tilde{a}$  von  $\tilde{f}$  in  $\tilde{K}$  genau eine Fortsetzung

$$(10.6.1) \quad \psi : k(a) \xrightarrow{\tilde{\varphi}} \tilde{k}(\tilde{a}) \subseteq K$$

mit  $\psi(a) = \tilde{a}$ . Ist umgekehrt  $\psi : k \rightarrow \tilde{K}$  eine Fortsetzung von  $\varphi$ , so ist  $\tilde{a} := \psi(a) \in K$  eine Nullstelle von  $\tilde{f}$ , da für  $f = \sum_{i=1}^n a_i X^i$  gilt  $\tilde{f}(\tilde{a}) = \sum_{i=1}^n \varphi(a_i)\psi(a)^i = \psi(\sum_{i=1}^n a_i a^i) = \psi(0) = 0$ .

Weiter ist  $\psi(k(a)) = \psi(k[a]) \subseteq \tilde{k}[\tilde{a}] = \tilde{k}(\tilde{a})$ , also  $im(\psi) \subseteq \tilde{k}(\tilde{a})$  und  $\psi$  von der Form (10.6.1) mit  $\tilde{\varphi} = \tilde{\varphi}_{a, \tilde{a}}$ .

**Satz 10.7** (a) Ist  $K$  (bzw.  $\tilde{K}$ ) ein Zerfällungskörper von  $f$  über  $k$  (bzw.  $\tilde{f}$  über  $\tilde{k}$ ), so gibt es einen Homomorphismus  $\psi : K \rightarrow \tilde{K}$  mit den Eigenschaften

(i)  $\psi|_k = \varphi$ .

(ii)  $\psi$  bildet die Nullstellen von  $f$  auf Nullstellen von  $\tilde{f}$  ab.

(b) Sind  $\psi, \psi'$  zwei solche Homomorphismen mit  $\psi(a) = \psi'(a)$  für jede Nullstelle  $a$  von  $f$  in  $K$ , so gilt  $\psi = \psi'$ .

(c) Ist  $a \in K$  die Nullstelle eines irreduziblen Faktors  $g$  von  $f$ , und ist  $\tilde{a} \in \tilde{K}$  eine Nullstelle von  $\tilde{g} = \varphi(g)$ , dann gibt es ein  $\psi$  wie in (a) mit  $\psi(a) = \tilde{a}$ .

(d) Ist  $\varphi$  ein Isomorphismus, so auch jede der Fortsetzungen wie in (a).

**Beweis** von (a): durch vollständige Induktion über die Anzahl  $r$  der Nullstellen von  $f$  in  $K \setminus k$ . Für  $r = 0$  zerfallen  $f$  und  $\tilde{f}$  in Linearfaktoren, und  $\psi = \varphi : K = k \rightarrow \tilde{k} = \tilde{K}$  hat die gewünschten Eigenschaften. Sei nun  $r \geq 1$  und seien  $a_1, \dots, a_r$  die Nullstellen von  $f$  in  $K \setminus k$ . Es gibt einen irreduziblen Faktor  $g$  von  $f$ , der  $a_1$  als Nullstelle hat

(z.B. das Minimalpolynom  $f_{a_1}$  von  $a_1$  über  $k$ ). Dann ist  $\tilde{g} = \varphi(g)$  ein Faktor von  $\tilde{f}$ . Da  $\tilde{f}$  über  $\tilde{K}$  in Linearfaktoren zerfällt, hat  $\tilde{g}$  eine Nullstelle  $\tilde{a}_1$  in  $\tilde{K}$ . Nach 10.5 gibt es einen Homomorphismus  $\tilde{\varphi} : k(a_1) \rightarrow \tilde{k}(\tilde{a}_1)$  mit  $\tilde{\varphi}|_k = \varphi$  und  $\tilde{\varphi}(a_1) = \tilde{a}_1$ . Nun ist  $K$  (bzw.  $\tilde{K}$ ) auch ein Zerfällungskörper von  $f$  über  $k(a_1)$  (bzw.  $\tilde{f}$  über  $\tilde{k}(\tilde{a}_1)$ ). Nach Induktionsvoraussetzung gibt es also eine Fortsetzung  $\psi : K \rightarrow \tilde{K}$  von  $\tilde{\varphi}$ , welche wegen  $\psi(f) = \varphi(f) = \tilde{f}$  die Nullstellen von  $f$  in die Menge der Nullstellen von  $\tilde{f}$  abbildet. Dies zeigt (a).

(b) Aus der Voraussetzung folgt insbesondere  $\psi(a_1) = \psi'(a_1)$  und wegen der Eindeutigkeitsaussage in 10.5 gilt  $\psi|_{k(a_1)} = \psi'|_{k(a_1)}$ . Mit Induktion über  $r$  folgt dann  $\psi = \psi'$ .

(c) Für  $a \in k$  ist die Aussage klar. Für  $a \in K \setminus k$  wurde die Aussage oben bewiesen.

(d) Ist  $\tilde{a}_1 = \tilde{\varphi}(a_1)$ , so ist  $\psi|_{k(a_1)} = \tilde{\varphi} : k(a_1) \rightarrow \tilde{k}(\tilde{a}_1)$  ein Isomorphismus nach 10.5, und mit Induktion über  $r$  folgt, dass auch  $\psi$  ein Isomorphismus ist.

**Corollar 10.8** Sei  $K/k$  ein Zerfällungskörper des nichtkonstanten Polynoms  $f \in k[X]$ . Ist  $\tilde{K}/k$  ein anderer Zerfällungskörper von  $f$ , so gibt es einen Isomorphismus  $\psi : K \xrightarrow{\sim} \tilde{K}$  über  $k$ , d.h., mit  $\psi|_k = id$ . Insbesondere ist jeder Zerfällungskörper endlich über  $k$ .

**Beweis** Die erste Aussage ist der Fall  $k = \tilde{k}$  und  $\varphi = id$  von 10.7 (a). Da  $\psi$  insbesondere ein Isomorphismus von  $k$ -Vektorräumen ist, folgt die zweite Behauptung aus 10.4: Es gibt einen Zerfällungskörper der Form  $k(a_1, \dots, a_n)$  mit algebraischen  $a_i$ . Dies ist endlich über  $k$  nach 9.9.

**Definition 10.9** Eine algebraische Körpererweiterung  $K/k$  heißt *normal*, wenn jedes irreduzible Polynom  $f \in k[X]$ , das in  $K$  eine Nullstelle hat, über  $K$  in Linearfaktoren zerfällt ( $\Leftrightarrow$  für jedes  $a \in K$  gilt: das Minimalpolynom  $f_a$  von  $a$  über  $k$  zerfällt über  $K$  in Linearfaktoren).

Wir haben die folgende wichtige Charakterisierung.

**Satz 10.10** Für eine *endliche* Körpererweiterung  $K/k$  sind äquivalent:

(a)  $K/k$  ist normal.

(b)  $K$  ist Zerfällungskörper über  $k$  eines Polynoms  $f \in k[X]$ .

(c) Ist  $\tilde{K}/K$  eine Körpererweiterung und ist  $\psi : K \rightarrow \tilde{K}$  ein Homomorphismus mit  $\psi|_k = id_k$ , so gilt  $\psi(K) \subset \tilde{K}$ .

**Beweis** (a)  $\Rightarrow$  (b): Sei  $K = k(a_1, \dots, a_n)$ . Für jedes  $i = 1, \dots, n$  zerfällt das Minimalpolynom  $f_{a_i}$  von  $a_i$  über  $k$  nach Voraussetzung über  $K$  in Linearfaktoren. Wegen  $K = k(a_1, \dots, a_n)$  ist dann  $K$  der Zerfällungskörper von  $f_{a_1} \cdot f_{a_2} \cdot \dots \cdot f_{a_n}$  (vergleiche 10.4).

(b)  $\Rightarrow$  (c) Nach (b) und 10.4 gibt es ein  $f \in k[X]$  und  $b, a_1, \dots, a_n \in K$  mit  $f = b(X - a_1) \cdot \dots \cdot (X - a_n)$  und  $K = k(a_1, \dots, a_n)$ . Für  $\psi$  wie in (c) gilt dann offenbar  $\psi(\{a_1, \dots, a_n\}) \subset \{a_1, \dots, a_n\}$  und damit  $\psi(K) \subseteq K$ .

(c)  $\Rightarrow$  (a) Als endliche Körpererweiterung ist  $K/k$  algebraisch (vergleiche 9.9). Sei  $f \in k[X]$  irreduzibel mit einer Nullstelle  $a$  in  $K$ . Seien  $a_1, \dots, a_n \in K$  mit  $K = k(a, a_1, \dots, a_n)$ , und sei  $f_{a_i}$  das Minimalpolynom von  $a_i$  über  $k$ ,  $i = 1, \dots, n$ . Ist  $\tilde{K}$  ein Zerfällungskörper

von  $g := f_{a_1} \dots f_{a_n} \in k[X]$  über  $K$ , so ist  $\tilde{K}$  auch ein Zerfällungskörper von  $f$  über  $k$ , wegen  $K = k(a_1, \dots, a_n)$  und 10.4 (b). Nach Definition zerfällt  $f$  über  $\tilde{K}$  in Linearfaktoren. Ist nun  $b \in \tilde{K}$  eine Nullstelle von  $f$ , so gibt es nach 10.7 (c) und (d) einen Automorphismus  $\psi$  von  $\tilde{K}$  mit  $\psi|_k = id$  und  $\psi(a) = b$ . Nach (c), angewendet auf  $\psi|_K: K \rightarrow \tilde{K}$ , gilt  $\psi(K) \subseteq K$  und damit  $b = \psi(a) \in K$ ;  $f$  zerfällt also schon über  $K$  in Linearfaktoren.

**Lemma 10.11** Sei  $K/k$  normal und  $k \subseteq L \subseteq K$  ein Zwischenkörper. Dann ist  $K/L$  normal.

**Beweis:** Sei  $a \in K$ , sei  $f_a$  das Minimalpolynom von  $a$  über  $k$  und sei  $g_a$  das Minimalpolynom von  $a$  über  $L$ . Dann gilt  $g_a \mid f_a$  in  $L[X]$  (da  $f_a \in L[X]$  und  $f_a(a) = 0$ ). Mit  $f_a$  zerfällt also auch  $g_a$  über  $K$  in Linearfaktoren.

$L/K$  muss nicht normal sein; weiter folgt aus der Normalität von  $K/L$  und  $L/K$  nicht die von  $K/k$ :

**Beispiele 10.12** (a) Das Polynom  $f(X) = X^3 - 2 \in \mathbb{Q}[X]$  ist irreduzibel (Eisenstein-Kriterium für  $p = 2$ ) und sein Zerfällungskörper in  $\mathbb{C}$  ist  $K = \mathbb{Q}(\sqrt[3]{2}, \zeta)$ , wobei  $\zeta = e^{\frac{2\pi i}{3}}$  eine primitive dritte Einheitswurzel ist, denn  $f$  hat die Nullstellen  $\sqrt[3]{2}, \zeta\sqrt[3]{2}, \zeta^2\sqrt[3]{2}$  in  $\mathbb{C}$ . Aber der Zwischenkörper  $L = \mathbb{Q}(\sqrt[3]{2})$  ist nicht normal über  $\mathbb{Q}$ , da er reell ist und die Nullstellen  $\zeta\sqrt[3]{2}, \zeta^2\sqrt[3]{2}$  nicht enthält.

(b)  $\mathbb{Q}(\sqrt{2})/\mathbb{Q}$  ist normal (vergleiche 10.3). Genauso ist  $\mathbb{Q}(\sqrt[4]{2})/\mathbb{Q}(\sqrt{2})$  normal, als Zerfällungskörper des Polynoms  $X^2 - \sqrt{2} \in \mathbb{Q}(\sqrt{2})[X]$ . Aber  $\mathbb{Q}(\sqrt[4]{2})$  ist nicht normal über  $\mathbb{Q}$ , denn das Polynom

$$X^4 - 2 \quad (= (X - \sqrt[4]{2})(X + \sqrt[4]{2})(X - i\sqrt[4]{2})(X + i\sqrt[4]{2}) \text{ in } \mathbb{C}[X])$$

ist irreduzibel in  $\mathbb{Q}[X]$  (Eisenstein-Kriterium), hat in  $\mathbb{Q}(\sqrt[4]{2})$  die Nullstelle  $\sqrt[4]{2}$ , zerfällt aber nicht in Linearfaktoren über  $\mathbb{Q}(\sqrt[4]{2})$ , da die Nullstellen  $\pm i\sqrt[4]{2}$  nicht in  $\mathbb{Q}(\sqrt[4]{2}) \subseteq \mathbb{R}$  liegen.

**Lemma 10.13** Ist  $K/k$  eine endliche Körpererweiterung, so gibt es eine Körpererweiterung  $K'/K$  derart, dass  $K'/k$  normal ist.

**Beweis** Ist  $K = k(a_1, \dots, a_n)$ ,  $f_{a_i}$  das Minimalpolynom von  $a_i$  über  $k$  und  $K'$  der Zerfällungskörper von  $f = f_{a_1} \dots f_{a_n}$  über  $K$ , so ist  $K'$  auch der Zerfällungskörper von  $f$  über  $k$  (da dieser alle Nullstellen von  $f$  in  $K'$ , also auch  $a_1, \dots, a_n$  und damit  $K$  enthalten muß). Nach 10.10 ist  $K'/k$  normal.

## §11 Separable Körpererweiterungen

Wir beschäftigen uns in diesem Paragraphen mit dem Unterschied zwischen einfachen und mehrfachen Nullstellen. Sei  $k$  ein Körper.

**Definition 11.1** Sei  $f \in k[X]$  ein nicht-konstantes Polynom und  $Z/k$  der Zerfällungskörper von  $f$  über  $k$  (dieser ist nach 10.8 bis auf Isomorphie eindeutig). Sei  $a$  ein Element von  $Z$ .

(a) Die Zahl

$$v_a(f) = \max \{n \in \mathbb{N}_0 \mid (X - a)^n \text{ teilt } f \text{ in } Z[X]\}$$

heißt die Vielfachheit von  $f$  in  $a$ . Ist  $a$  eine Nullstelle von  $f$  ( $\Leftrightarrow v_a(f) \geq 1$ , vergleiche 4.12), so heißt  $v_a(f)$  auch die Vielfachheit (oder Ordnung) der Nullstelle  $a$  von  $f$ . Insbesondere heißt  $a$  eine einfache Nullstelle, wenn  $v_a(f) = 1$ , und eine mehrfache Nullstelle, wenn  $v_a(f) \geq 2$ .

(b)  $f$  heißt separabel, wenn  $f$  nur einfache Nullstellen in  $Z$  hat.

**Definition 11.2** Die Abbildung

$$D : k[X] \rightarrow k[X], \quad D \left( \sum_{i=0}^n a_i X^i \right) = \sum_{i=0}^n i a_i X^{i-1}$$

heißt (formale) Differentiation in  $k[X]$ . Für  $f \in k[X]$  heißt  $Df$  die Ableitung von  $f$  und wird auch mit  $f'$  bezeichnet.

**Lemma 11.3**  $D$  ist eine  $k$ -Derivation von  $k[X]$ , d.h., eine  $k$ -lineare Abbildung von  $k[X]$  in sich mit

$$D(fg) = (Df)g + f(Dg).$$

Jede  $k$ -Derivation  $\sigma : k[X] \rightarrow k[X]$  ist von der Form  $\sigma(f) = p \cdot f'$  für ein eindeutig bestimmtes  $p \in k[X]$ .

**Beweis:** Übungsaufgabe!

**Beispiele 11.4** (a) Aus 11.3 folgt leicht durch Induktion

$$((X - a)^n)' = n(X - a)^{n-1}$$

für  $a \in k$  und  $n \in \mathbb{N}_0$ .

(b) Allgemeiner gilt für Polynome  $f(X), g(X) \in k[X]$  die übliche Kettenregel

$$(f(g(X)))' = f'(g(X)) \cdot g'(X).$$

**Lemma 11.5** Sei  $f \in k[X]$  nicht-konstant, und  $Z/k$  ein Zerfällungskörper von  $f$ .

(a) Für  $a \in Z$  gilt

$$\begin{aligned} v_a(f) = 1 &\Leftrightarrow f(a) = 0 \quad \text{und} \quad f'(a) \neq 0 \\ v_a(f) > 1 &\Leftrightarrow f(a) = 0 \quad \text{und} \quad f'(a) = 0. \end{aligned}$$

(b)  $f$  hat genau dann mehrfache Nullstellen in  $Z$ , wenn  $f$  und  $f'$  einen nicht-konstanten gemeinsamen Teiler in  $k[X]$  haben.

**Beweis** (a) Sei  $r = v_a(f)$ . Dann gibt es ein  $g \in Z[X]$  mit  $f = (X - a)^r g$  und  $g(a) \neq 0$ . Es folgt mit 11.3 und 11.4 (a), dass

$$\begin{aligned} f' &= r(X - a)^{r-1}g + (X - a)^r g' \\ &= (X - a)^{r-1}(rg + (X - a)g'). \end{aligned}$$

Ist  $r = 1$ , so ist danach  $f'(a) = g(a) \neq 0$ ; ist  $r > 1$ , so ist  $f'(a) = 0$ .

(b) Ist  $a$  eine mehrfache Nullstelle von  $f$ , so ist das Minimalpolynom  $f_a$  wegen  $f(a) = 0 = f'(a)$  ein Teiler sowohl von  $f$  als auch von  $f'$ . Ist umgekehrt  $g$  ein nicht-konstanter gemeinsamer Teiler von  $f$  und  $f'$ , so gilt für jede Nullstelle  $a$  von  $g$  in  $Z$ :  $f(a) = 0 = f'(a)$ ; nach (a) ist also  $a$  eine mehrfache Nullstelle von  $f$ .

**Satz 11.6** Ein irreduzibles Polynom  $f \in k[X]$  ist genau dann separabel, wenn  $f' \neq 0$  ist.

**Beweis** Sei  $Z$  der Zerfällungskörper von  $f$  über  $k$ . Ist  $f' = 0$ , so ist jede Nullstelle von  $f$  in  $Z$  mehrfach nach 11.5. Ist  $f' \neq 0$ , so haben  $f$  und  $f'$  keinen nicht-konstanten gemeinsamen Teiler: da  $f$  irreduzibel ist, würde dies bedeuten, dass  $f'$  von  $f$  geteilt wird, im Widerspruch zur Ungleichung  $\deg(f') < \deg(f)$ .

Wir untersuchen nun, wann  $f' = 0$  (identisch 0) sein kann.

**Lemma 11.7** Sei  $f \in k[X]$ .

(a) Ist  $\text{char}(k) = 0$ , so gilt:

$$f' = 0 \Leftrightarrow f \text{ ist konstant.}$$

(b) Ist  $\text{char}(k) = p > 0$ , so gilt:

$$f' = 0 \Leftrightarrow \text{es gibt ein } g \in k[X] \text{ mit } f(X) = g(X^p).$$

**Beweis** Sei  $f = \sum_{i=0}^n a_i X^i$  und  $f' = \sum_{i=0}^n i a_i X^{i-1} = 0$ . Ist  $\text{char}(k) = 0$ , so folgt aus  $i a_i = 0$  auch  $a_i = 0$  für  $i \geq 1$ , d.h.,  $f$  ist konstant. Ist  $\text{char}(k) = p > 0$ , so folgt nur  $a_i = 0$  für  $p \nmid i$ , da dann  $i$  invertierbar in  $k$  ist. Damit ist

$$\begin{aligned} f &= a_0 + a_p X^p + a_{2p} X^{2p} + \dots + a_{mp} X^{mp} \\ &= g(X^p) \end{aligned}$$

für  $g = \sum_{i=0}^m a_{p_i} X^i$  wie behauptet. Die Rückrichtungen sind klar.

**Corollar 11.8** Ist  $\text{char}(k) = 0$ , so ist jedes irreduzible Polynom  $f \in k[X]$  separabel.

**Definition 11.9** Sei  $K/k$  eine algebraische Körpererweiterung.

(a) Ein Element  $a \in K$  heißt separabel über  $k$ , wenn das Minimalpolynom  $f_a$  von  $a$  über  $k$  separabel ist ( $\Leftrightarrow a$  ist die Nullstelle eines separablen Polynoms  $f \in k[X]$ ).

(b)  $K/k$  heißt separabel, wenn jedes Element  $a \in K$  separabel über  $k$  ist ( $\Rightarrow K/k$  ist algebraisch).

(c) Der Körper  $k$  heißt vollkommen (oder perfekt), wenn jede algebraische Erweiterung  $K/k$  separabel ist ( $\Leftrightarrow$  jedes irreduzible Polynom aus  $k[X]$  ist separabel).

(d) Für "nicht separabel" sagt man meist "inseparabel".

**Corollar 11.10** Jeder Körper der Charakteristik Null ist vollkommen.

Wir kommen nun zu einer Kennzeichnung von separablen Erweiterungen.

**Definition 11.11** Für Körpererweiterungen  $K$  und  $K'$  von  $k$  sei  $\text{Hom}_k(K, K')$  die Menge der  $k$ -Morphismen  $\psi : K \rightarrow K'$ , d.h., der Körperhomomorphismen mit  $\psi(x) = x$  für alle  $x \in k$ .

**Satz 11.12** Sei  $K/k$  eine endliche Körpererweiterung und  $K'$  ein beliebiger Erweiterungskörper von  $K$ , der normal über  $k$  ist.

(a) Es ist  $|\text{Hom}_k(K, K')| \leq [K : k]$ .

(b) Es ist  $|\text{Hom}_k(K, K')| = [K : k]$  genau dann, wenn  $K/k$  separabel ist.

**Beweis** Sei  $K = k(a_1, \dots, a_r)$ . Wir zeigen die Aussagen durch Induktion über  $r$ , wobei der Induktionsanfang mit  $r = 0$  (d.h.,  $K = k$ ) trivial ist. Sei  $L = K(a_1, \dots, a_{r-1})$ , so dass  $K = L(a_r)$ , und seien

$$\varphi_1, \dots, \varphi_m : L \rightarrow K'$$

die verschiedenen  $k$ -Homomorphismen von  $L$  nach  $K'$ . Dann ist nach Induktionsvoraussetzung  $m \leq [L : k]$ . Weiter ist  $M := \text{Hom}_k(K, K')$  die disjunkte Vereinigung der Mengen  $M(\varphi_i) = \{\psi : K \rightarrow K' \mid \psi|_L = \varphi_i\}$  für  $i = 1, \dots, m$ .

Für (a) genügt es zu zeigen, dass  $|M(\varphi_i)| \leq [K : L]$  gilt für alle  $i$ ; dann folgt nämlich

$$|M| = \sum_{i=1}^m |M(\varphi_i)| \leq m[K : L] \leq [L : K] \cdot [K : L] = [K : k].$$

Sei also  $i$  beliebig, aber fest. Sei  $g$  das Minimalpolynom von  $a_r$  über  $L$ . Dann zerfällt  $\varphi_i(g)$  über  $K'$  in Linearfaktoren:  $g$  teilt nämlich das Minimalpolynom  $f$  von  $a_r$  über  $k$  (wegen  $f(a_r) = 0$ ), daher teilt  $\varphi_i(g)$  das Polynom  $\varphi_i(f) = f$ , welches die Nullstelle  $a_r$  in  $K'$  hat und also wegen der Normalität von  $K'/k$  über  $K'$  in Linearfaktoren zerfällt. Nach Corollar 10.6 entsprechen die Fortsetzungen

$$\psi : K = L(a_r) \rightarrow K'$$

von  $\varphi_i$  gerade den verschiedenen Nullstellen von  $\varphi_i(g)$ , und dies sind höchstens  $\deg(\varphi_i(g)) = \deg(g) = [L(a_r) : L] = [K : L]$  viele.

Wir zeigen nun (b). Ist  $K/k$  separabel, so hat  $f = f_{a_r}$  in  $K'$  lauter verschiedene Nullstellen und dasselbe gilt auch für den Faktor  $\varphi_i(g)$ . Nach Corollar 10.6 gibt es dann genau  $\deg(\varphi_i(g)) = [K : L]$  viele verschiedene Fortsetzungen

$$\psi : K = L(\alpha_i) \rightarrow K'$$

von  $\varphi_i : L \rightarrow K'$  (nämlich zu jeder Nullstelle von  $\varphi_i(g)$  eine). Weiter ist  $L/k$  auch separabel, nach Induktionsvoraussetzung also  $m = [L : k]$ . Es folgt  $|M| = m \cdot [K : L] = [K : k]$ . Ist dagegen  $K/k$  inseparabel, so gibt es ein Element  $a \in K$ , welches inseparabel über  $k$  ist. Durch etwaige Hinzunahme zum Erzeugendensystem können wir annehmen, dass  $a_1 = a$  ist. Ist  $r = 1$ , so ist  $L = k$ , und nach 10.6 gibt es höchstens so viele  $k$ -Homomorphismen  $\psi : K = k(a_1) \rightarrow K'$ , wie es verschiedene Nullstellen von  $f_{a_1}$  gibt, und

dies sind wegen der Inseparabilität von  $f_{a_1}$  echt weniger als  $\deg(f_{a_1}) = [K : k]$ . Ist  $r \geq 2$ , so ist  $L/k$  inseparabel, und es gilt nach Induktionsvoraussetzung  $m < [L : k]$ . Zusammen mit (a) folgt  $|M| \leq m \cdot [K : L] < [K : k]$ .

**Corollar 11.13** Ist  $K = k(a_1, \dots, a_n)$  mit  $a_1, \dots, a_n$  separabel über  $k$ , so ist  $K/k$  separabel.

**Beweis** mit Induktion über  $n$ , wobei der Fall  $n = 0$  wieder trivial ist. Sei  $K'/K$  ein Erweiterungskörper, der über  $k$  normal ist (ein solcher existiert nach 10.13 immer). Sei  $n \geq 1$  und  $L = k(a_1, \dots, a_{n-1})$ , so dass  $K = L(a_n)$ . Nach Induktionsvoraussetzung gibt es  $m = [L : k]$  viele  $k$ -Homomorphismen  $\varphi_1, \dots, \varphi_m : L \rightarrow K'$ . Weiter ist nach dem Argument im Beweis von 11.12 (b) die Anzahl der Fortsetzungen  $\psi : K = L(a_n) \rightarrow K'$  von  $\varphi_i$  gleich  $[L(a_n) : L]$ . Es folgt  $|\text{Hom}_k(K, K')| = [L : k] \cdot [K : L] = [K : k]$ , und nach 11.12 (b) ist  $K/k$  separabel.

Als weitere Anwendung erhalten wir:

**Satz 11.14** (Satz vom primitiven Element) Sei  $K/k$  eine endliche separable Körpererweiterung. Dann gibt es ein  $\alpha \in K$  mit  $K = k(\alpha)$ .

**Beweis** für endliches  $k$  (den Fall endlicher Körper behandeln wir später): Da es Elemente  $a_1, \dots, a_n \in K$  gibt mit  $K = k(a_1, \dots, a_n) = k(a_1, \dots, a_{n-1})(a_n)$ , können wir per Induktion die Frage auf den Fall zurückführen, dass  $K = k(a, b)$  mit  $a, b \in K$  ist. Sei  $K'/K$  ein über  $k$  normaler Erweiterungskörper. Sind  $\sigma_1, \dots, \sigma_n$  die verschiedenen  $k$ -Homomorphismen von  $K$  in  $K'$ , so gilt wegen 11.12 und der Separabilität von  $K/k$  die Gleichheit  $n = [K : k]$ . Das Polynom

$$p(X) = \prod_{i \neq j} (\sigma_i a + X \sigma_i b - \sigma_j a - X \sigma_j b)$$

ist nicht das Nullpolynom; wegen der Unendlichkeit von  $k$  gibt es daher ein  $c \in k$  mit  $P(c) \neq 0$ . Dann sind die Elemente  $\sigma_i(a + cb)$  für  $i = 1, \dots, n$  alle verschieden, also die Einbettungen

$$\sigma_i|_{k(a+cb)} : k(a+cb) \hookrightarrow K'$$

paarweise verschieden. Mit 11.12 folgt, dass  $[k(a+cb) : k] \geq n = [K : k]$ , also  $k(a+cb) = K$ .

Wir bemerken noch:

**Lemma 11.15** Sei  $K/k$  eine Körpererweiterung und  $k \subseteq L \subseteq K$  ein Zwischenkörper.

(a) Ist  $K/k$  separabel, so auch  $K/L$  und  $L/k$ .

(b) Sind  $K/L$  und  $L/k$  separabel so auch  $K/k$ .

**Beweis** (a) Sei  $K/k$  separabel. Dann ist  $L/k$  trivialerweise separabel. Weiter sei  $a \in K$ ,  $f_a \in k[X]$  das Minimalpolynom von  $a$  über  $k$  und  $g_a \in L[X]$  das Minimalpolynom von  $a$  über  $L$ . Wegen  $f_a(a) = 0$  gilt dann  $g_a \mid f_a$  in  $L[X]$ , also  $f_a = g_a \cdot h$  mit  $h \in L[X]$ . Dann

ist

$$f'_a = g'_a \cdot h + g_a \cdot h'$$

also  $g'_a \neq 0$  wegen  $f'_a(a) \neq 0$  und  $g_a(a) = 0$ . Also ist  $g_a$  separabel und damit  $a$  separabel über  $L$ .

(b): Übungsaufgabe!

## §12 Der Hauptsatz der Galoistheorie

**Definition 12.1** Für eine Körpererweiterung  $K/k$  sei  $\text{Aut}_k(K)$  die Gruppe der  $k$ -Automorphismen von  $K$ , d.h., die Gruppe der Körperautomorphismen  $\sigma : K \rightarrow K$  mit  $\sigma(x) = x$  für alle  $x \in k$ .

**Definition 12.2** Eine Körpererweiterung  $K/k$  heißt galoissch, wenn sie normal und separabel ist.  $\text{Aut}_k(K)$  heißt dann die Galoisgruppe von  $K$  über  $k$  (Bez.  $\text{Gal}(K/k)$ ).

**Satz 12.3** Sei  $K/k$  eine *endliche* galoissche Körpererweiterung mit Galoisgruppe  $G = \text{Gal}(K/k)$ .

(a) Ist  $U$  eine Untergruppe von  $G$ , so ist

$$K^U := \{x \in K \mid u(x) = x \text{ für alle } u \in U\}$$

ein Körper und heißt der Fixkörper von  $U$  in  $K$ .

(b) Ist  $L$  ein Zwischenkörper von  $K/k$ , so ist  $K/L$  galoissch.

(c) (Galoiskorrespondenz) Sei  $U(G)$  die Menge der Untergruppen von  $G$  und  $Z(K/k)$  die Menge der Zwischenkörper von  $K/k$ . Die Abbildungen

$$\begin{array}{ccc} U(G) & \xrightleftharpoons{\psi} & Z(K/k) \\ & \phi & \\ U & \mapsto & K^U \\ \text{Gal}(K/L) & \leftrightarrow & L \end{array}$$

sind zueinander inverse Bijektionen.

(d) Es gilt unter diesen Bijektionen

- (i)  $U \subseteq U' \Leftrightarrow K^{U'} \subseteq K^U$
- (ii)  $L \subseteq L' \Leftrightarrow \text{Gal}(K/L') \subseteq \text{Gal}(K/L)$

(e)  $G$  ist endlich, und für jeden Zwischenkörper  $L$  von  $K/k$  gilt

- (i)  $[K : L] = (\text{Gal}(K/L) : 1)$
- (ii)  $[L : k] = (G : \text{Gal}(K/L))$ .

(f) Ist  $L$  ein Zwischenkörper von  $K/k$ , so ist  $L/k$  genau dann galoissch, wenn  $\text{Gal}(K/L)$  ein Normalteiler in  $G$  ist. Es ist dann  $\sigma(L) = L$  für jedes  $\sigma \in G$ , und der Homomorphismus

$$G = \text{Gal}(K/k) \rightarrow \text{Gal}(L/k), \quad \sigma \mapsto \sigma|_L$$

induziert einen Gruppenisomorphismus

$$\text{Gal}(K/k)/\text{Gal}(K/L) \xrightarrow{\sim} \text{Gal}(L/k).$$

**Beweis** (a) ist klar, und (b) folgt aus 10.11 und 11.15. Die Beziehungen

$$\begin{aligned} U \subseteq U' &\Rightarrow K^{U'} \subseteq K^U \\ L \subseteq L' &\Rightarrow \text{Gal}(K/L') \subseteq \text{Gal}(K/L) \end{aligned}$$

in (d) sind trivial. Hat man (c) gezeigt, so gilt

$$\begin{aligned} \text{Gal}(K/K^U) &= \phi(\psi(U)) = U \\ K^{\text{Gal}(K/L)} &= \psi(\phi(L)) = L, \end{aligned}$$

und wir erhalten auch die Implikationen in die andere Richtung (z.B.:  $K^{U'} \subseteq K^U \Rightarrow \text{Gal}(K/K^U) \subseteq \text{Gal}(K/K^{U'}) \Leftrightarrow U \subseteq U'$ ).

In (e) ist nur (i) zu zeigen; dann folgt (ii) aus der Gradgleichung  $[K : k] = [L : k] \cdot [K : L]$  und dem Satz von Lagrange:  $(G : 1) = (G : \text{Gal}(K/L)) \cdot (\text{Gal}(K/L) : 1)$ .

Weiter folgt (e) (i) aus

**Lemma 12.4** Ist  $K/k$  endlich und normal, so gilt

(a)  $\# \text{Aut}_k(K) \leq [K : k]$

(b)  $\# \text{Aut}_k(K) = [K : k]$  genau dann, wenn  $K/k$  separabel ist.

Dies ist der Fall  $K' = K$  von 11.12. Wir zeigen nun eine Hälfte von 12.3 (c), nämlich  $\psi\phi(L) = L$ . Da  $K/L$  wieder galoissch ist, genügt es zu zeigen:

**Proposition 12.5** Ist  $K/k$  eine endliche galoissche Körpererweiterung, so gilt

$$K^{\text{Gal}(K/k)} = k.$$

**Beweis** Trivialerweise ist  $k \subseteq K^{\text{Gal}(K/k)}$ . Umgekehrt sei  $\alpha \in K^{\text{Gal}(K/k)}$  und sei  $\sigma : k(\alpha) \rightarrow K$  ein  $k$ -Homomorphismus. Nach dem Beweis von 11.12 gibt es eine Fortsetzung  $\tilde{\sigma} : K \rightarrow K$  von  $\sigma$ . Nach Voraussetzung wird  $\alpha$  von  $\tilde{\sigma} \in \text{Gal}(K/k)$  festgelassen, also auch von  $\sigma$ . Es folgt mit 11.12, dass  $[k(\alpha) : k] = 1$  ist, also  $\alpha \in k$ .

Für die andere Hälfte von (c) benötigen wir einige Vorbereitungen.

Das folgende Lemma gibt zusammen mit dem nachfolgenden Satz eine Beschreibung von Minimalpolynomen bei galoisschen Körpererweiterungen.

**Lemma 12.6** Sei  $K$  ein Körper,  $G \leq \text{Aut}(K)$  eine endliche Untergruppe und  $k = K^G$  der Fixkörper. Sei  $\alpha \in K$  und  $N := N(\alpha) := \{\sigma\alpha \mid \sigma \in G\}$ . Dann ist

$$f(X) = \prod_{\beta \in N} (X - \beta)$$

das Minimalpolynom von  $\alpha$  über  $k$ .

**Beweis** Für jedes  $\sigma \in G$  gilt

$$\sigma(f)(X) = \prod_{\beta \in N} (X - \sigma\beta) = f(X),$$

d.h.,  $\sigma$  lässt die Koeffizienten von  $f$  fest, d.h., es ist  $f(X) \in k[X]$ . Da  $f$  normiert ist und  $f(x) = 0$  gilt, ist nur noch zu zeigen, dass  $f$  irreduzibel in  $k[X]$  ist. Seien also  $g, h \in k[X]$  mit  $f = g \cdot h$ , und sei ohne Einschränkung  $g(\alpha) = 0$ . Ist  $\beta \in N$ , etwa  $\beta = \sigma(\alpha)$  mit  $\sigma \in G$ , so ist  $g(\beta) = g(\sigma(\alpha)) = \sigma(g(\alpha)) = 0$ . Da die  $\beta \in N$  alle verschieden sind, folgt  $f \mid g$  und damit  $h \in k^\times$ .

Wir erhalten hiermit die folgende Charakterisierung von endlichen Galoiserweiterungen.

**Satz 12.7** Sei  $K/k$  eine Körpererweiterung. Dann sind äquivalent:

- (a) Es gibt eine endliche Untergruppe  $G \subseteq \text{Aut}(K)$  mit  $k = K^G$ .
- (b)  $K/k$  ist endlich und galoissch.
- (c)  $K/k$  ist Zerfällungskörper eines separablen Polynoms  $f \in k[X]$ .

**Beweis** (a)  $\Rightarrow$  (b): Ist  $\alpha \in K$ , so ist  $\alpha$  nach 12.6 algebraisch über  $k$ , und das Minimalpolynom zerfällt über  $K$  in verschiedene Linearfaktoren.  $K/k$  ist also normal und separabel. Für jedes  $\alpha \in K$  gilt weiter nach 12.6:  $[k(\alpha) : k] = |N(\alpha)| \leq |G|$ . Sei  $\beta \in K$  mit  $[k(\alpha) : k]$  maximal. Wäre  $k(\beta) \neq K$ , so gäbe es ein  $\alpha \in K$  mit  $k(\alpha, \beta) \supsetneq k(\beta)$  und nach dem Satz vom primitiven Element ist  $k(\alpha, \beta) = k(\gamma)$  für ein  $\gamma \in K$ , im Widerspruch zur Maximalität von  $\beta$ . Es ist also  $K = k(\beta)$  endlich über  $k$ .

(b)  $\Rightarrow$  (c): Nach 10.10 ist  $K/k$  Zerfällungskörper eines Polynoms  $f \in k[X]$ . Ist  $g$  ein irreduzibler Faktor von  $f$  und  $a \in K$  eine Nullstelle von  $g$ , so ist  $g$  bis auf einen konstanten Faktor gleich dem Minimalpolynom von  $a$ . Da  $a$  separabel über  $k$  ist, ist  $g$  separabel. Sind  $g_1, \dots, g_m$  die verschiedenen irreduziblen Faktoren von  $f$ , so ist  $\tilde{f} = g_1 \dots g_m$  separabel und  $K$  auch Zerfällungskörper von  $\tilde{f}$ .

(c)  $\Rightarrow$  (b): Ist  $K/k$  Zerfällungskörper eines separablen Polynoms  $f \in k[X]$ , so ist  $K/k$  normal nach 10.10, und nach 10.4 ist  $K = k(a_1, \dots, a_n)$ , wobei  $a_1, \dots, a_n$  die Nullstellen von  $f$  sind. Nach Corollar 11.13 ist  $K/k$  separabel.

(b)  $\Rightarrow$  (a): Nach 12.5 ist  $k = K^{\text{Gal}(K/k)}$ .

Wir zeigen nun die andere Hälfte von 12.3 (c), nämlich  $\phi\psi U = U$ .

**Proposition 12.8** Sei  $K/k$  eine endliche Galoiserweiterung und sei  $U$  eine Untergruppe von  $\text{Gal}(K/k)$ . Dann ist

$$\text{Gal}(K/K^U) = U.$$

**Beweis** Offenbar ist  $U \subseteq \text{Gal}(K/K^U)$ , und mit 12.4 also

$$|U| \leq |\text{Gal}(K/K^U)| = [K : K^U].$$

Umgekehrt sei  $\alpha$  ein primitives Element von  $K/K^U$ , also  $K = K^U(\alpha)$ . Dann folgt wie im Beweis von 12.7

$$[K : K^U] = [K^U(\alpha) : K^U] \leq |U|,$$

und wir erhalten  $|U| = |\text{Gal}(K/K^U)|$ , also die Behauptung.

Wir beweisen nun den letzten Teil von 12.3, nämlich (f).

**Proposition 12.9** Sei  $K/k$  endlich galoissch und  $L$  ein Zwischenkörper. Dann ist äquivalent:

- (a)  $L/k$  ist galoissch.
- (b) Für alle  $\sigma \in \text{Gal}(K/k)$  gilt  $\sigma(L) = L$ .
- (c)  $\text{Gal}(K/L)$  ist Normalteiler in  $\text{Gal}(K/k)$ .

**Beweis** (a)  $\Rightarrow$  (b): Nach 10.10 (c) (für  $(K, \tilde{K}) = (L, K)$ ) gilt  $\sigma(L) \subseteq L$ . Andererseits ist  $\sigma : L \xrightarrow{\sim} \sigma(L)$  ein Isomorphismus von  $k$ -Vektorräumen (da  $\sigma$  ein  $k$ -Homomorphismus ist), also  $[L : k] = [\sigma(L) : k]$ . Damit ist die Inklusion  $\sigma(L) \subseteq L$  eine Gleichheit.

(b)  $\Leftrightarrow$  (c): Ist  $L$  ein Zwischenkörper und  $\sigma \in \text{Gal}(K/k)$ , so ist  $\sigma(L)$  ebenfalls ein Zwischenkörper von  $K/k$  und es gilt

$$\begin{aligned} \text{Gal}(K/\sigma(L)) &= \{\tau \in G \mid \tau\sigma x = \sigma x \quad \forall x \in L\} \\ &= \{\tau \in G \mid \sigma^{-1}\tau\sigma x = x \quad \forall x \in L\} \\ &= \sigma \text{Gal}(K/L)\sigma^{-1}. \end{aligned}$$

Die Äquivalenz von (b) und (c) folgt also aus der Galois-Korrespondenz, denn diese besagt:  $\sigma(L) = L \Leftrightarrow \text{Gal}(K/\sigma(L)) = \text{Gal}(K/L)$ .

(b)  $\Rightarrow$  (a): Nach (b) hat man einen kanonischen Homomorphismus

$$\text{Gal}(K/k) \rightarrow \text{Aut}_k(L), \quad \sigma \mapsto \sigma|_L.$$

Es folgt  $k \subseteq L^{\text{Aut}_k(L)} \subseteq K^{\text{Gal}(K/k)} = k$  und damit Gleichheit;  $L/k$  ist also galoissch nach 12.7.

Für den Rest von 12.3 (f) genügt es zu zeigen, dass für galoissches  $L/k$  die Restriktion

$$\text{Gal}(K/k) \rightarrow \text{Gal}(L/k), \quad \sigma \mapsto \sigma|_L$$

surjektiv ist, denn der Kern ist per definitionem  $\text{Gal}(K/L)$ . Diese Surjektivität folgt aber zum Beispiel aus dem Homomorphiesatz und der Gleichheit

$$(\text{Gal}(K/k) : \text{Gal}(K/L)) = [L : k] = \text{Gal}(L/k).$$

**Beispiel 12.10** Sei  $K = \mathbb{Q}(\sqrt[3]{2}, \zeta)$ , wobei  $\zeta = e^{\frac{2\pi i}{3}} \in \mathbb{C}$  eine primitive dritte Einheitswurzel ist. Dann ist  $K/\mathbb{Q}$  galoissch, denn  $K$  ist der Zerfällungskörper von  $f(X) = X^3 - 2 \in \mathbb{Q}[X]$  (siehe Beispiel 10.12 (a)), also normal über  $\mathbb{Q}$  und weiter ist  $\mathbb{Q}$  als Körper der Charakteristik 0 vollkommen, also jede algebraische Erweiterung separabel (Wir können auch sofort sehen, dass  $f(X)$  nach 10.12 (a) paarweise verschiedene Nullstellen in  $K$

hat, also separabel ist, und dann 12.7 (c) benutzen). Es ist  $[\mathbb{Q}(\sqrt[3]{2}) : \mathbb{Q}] = 3$ , da  $f$  das Minimalpolynom von  $\sqrt[3]{2}$  über  $\mathbb{Q}$  ist und  $\deg(f) = 3$ . Das Minimalpolynom von  $\zeta$  über  $\mathbb{Q}$  ist das Kreisteilungspolynom  $\phi_3(X) = X^2 + X + 1$  (siehe 7.11 (b)); also ist  $[\mathbb{Q}(\zeta) : \mathbb{Q}] = 2$ . Aber  $\phi_3(X)$  ist auch das Minimalpolynom von  $\zeta$  über  $\mathbb{Q}(\sqrt[3]{2})$ , da die Nullstellen  $\zeta$  und  $\zeta^{-1}$  nicht  $\mathbb{Q}(\sqrt[3]{2}) \subseteq \mathbb{R}$  liegen. Also ist  $[\mathbb{Q}(\sqrt[3]{2}, \zeta) : \mathbb{Q}(\sqrt[3]{2})] = 2$ . Es folgt  $[K : \mathbb{Q}] = [K : \mathbb{Q}(\sqrt[3]{2})] \cdot [\mathbb{Q}(\sqrt[3]{2}) : \mathbb{Q}] = 2 \cdot 3 = 6$ . Welche Gruppe mit 6 Elementen ist  $\text{Gal}(K/\mathbb{Q})$ ?

### §13 Bestimmung von Galoisgruppen

Sei  $K/k$  eine endliche Galoiserweiterung. Da  $K/k$  separabel ist, gibt es ein Element  $\alpha \in K$  mit  $K = k(\alpha)$  (Satz von primitiven Element). Da  $K/k$  auch normal ist, zerfällt das Minimalpolynom  $f_\alpha$  von  $\alpha$  über  $k$  über  $K$  in Linearfaktoren. Zusammen folgt, dass  $K$  der Zerfällungskörper von  $f_\alpha$  ist (die weiteren Nullstellen von  $f_\alpha$  sind bereits in  $k(\alpha)$  enthalten). Es genügt also, die Galoisgruppen von irreduziblen separablen Polynomen zu bestimmen, wobei wir definieren:

**Definition 13.1** Sei  $k$  ein Körper und  $f \in k[x]$  ein irreduzibles separables Polynom. Die Galoisgruppe von  $f$  ist definiert als die Galoisgruppe von  $K/k$ , wobei  $K$  der Zerfällungskörper von  $f$  über  $k$  ist.

Wir bemerken, dass  $K/k$  als Zerfällungskörper von  $f$  normal ist. Weiter ist  $K/k$  separabel, denn es gilt  $K = k(\alpha)$ , wobei  $\alpha \in K$  eine Nullstelle von  $f$  ist. Da  $\alpha$  separabel ist (das Minimalpolynom von  $\alpha$  über  $k$  entsteht durch Normierung von  $f$ , ist also nach Voraussetzung separabel), erhalten wir die Behauptung mit 11.13.

**Definition 13.2** Sei  $K/k$  normal. Zwei Elemente  $\alpha, \beta \in K$  heißen konjugiert über  $k$ , wenn sie dasselbe Minimalpolynom über  $k$  haben.

Für  $\alpha \in K$  sind also die Konjugierten von  $\alpha$  über  $k$  (in  $K$ ) die Nullstellen des Minimalpolynoms  $f_\alpha$  von  $\alpha$  über  $k$  (welches in  $K$  in Linearfaktoren zerfällt).

**Beispiel 13.3** Die Zahlen  $\sqrt[3]{2}, \zeta\sqrt[3]{2}, \zeta^2\sqrt[3]{2}$ , mit  $\zeta = e^{\frac{2\pi i}{3}} \in \mathbb{C}$  (siehe Beispiel 12.10), sind also zueinander konjugiert über  $\mathbb{Q}$  (in  $K = \mathbb{Q}(\sqrt[3]{2}, \zeta)$ ).

**Lemma 13.4** Sei  $K/k$  endlich und normal. Zwei Elemente  $\alpha, \beta \in K$  sind genau dann konjugiert über  $k$ , wenn es ein  $\sigma \in \text{Aut}_k(K)$  gibt mit  $\sigma(\alpha) = \beta$ .

**Beweis** Seien  $\alpha$  und  $\beta$  konjugiert über  $k$  und sei  $g$  das (gemeinsame) Minimalpolynom von  $\alpha$  und  $\beta$ . Nach 10.10 gibt es ein Polynom  $h \in k[X]$ , so dass  $K$  der Zerfällungskörper von  $h$  über  $k$  ist. Dann ist  $K$  auch der Zerfällungskörper von  $f := g \cdot h$  über  $k$  (da  $g$  über  $K$  zerfällt). Nach Satz 10.7 (c) (mit  $k = \tilde{k}$  und  $K = \tilde{K}$ ) gibt es also ein  $\sigma \in \text{Hom}_k(K, K) = \text{Aut}_k(K)$  mit  $\sigma(\alpha) = \beta$  ( $g$  ist ein irreduzibler Faktor von  $f$  und  $\alpha, \beta$  sind Nullstellen von  $g = \tilde{g}$ ).

Sei umgekehrt  $\sigma \in \text{Aut}_k(K)$  mit  $\sigma(\alpha) = \beta$ , und sei  $f_\alpha$  das Minimalpolynom von  $\alpha$  über

$k$ . Dann gilt in  $K : f_\alpha(\beta) = f_\alpha(\sigma(\alpha)) = \sigma(f_\alpha(\alpha)) = \sigma(0) = 0$ , da  $\sigma(f_\alpha) = f_\alpha$  wegen  $f_\alpha \in k[X]$ .

**Bemerkung 13.5** Es folgt, dass für  $K/k$  endlich normal und  $\alpha \in K$

$$N(\alpha) = \{\sigma(\alpha) \mid \sigma \in \text{Aut}_k(K)\}$$

die Menge der Konjugierten von  $\alpha$  über  $k$  ist und

$$f(X) = \prod_{\beta \in N(\alpha)} (X - \beta)$$

das Minimalpolynom von  $\alpha$  über  $k$  ist (vergleiche mit Lemma 12.6).

**Lemma/Definition 13.6** Sei  $M$  eine Menge. Dann ist die Menge

$$S(M) = \{\varphi : M \rightarrow M \mid \varphi \text{ bijektiv}\}$$

der bijektiven Selbstabbildungen von  $M$  eine Gruppe mit der Komposition als Verknüpfung und heißt die symmetrische Gruppe von  $M$ .

Dass  $S(M)$  mit der Komposition eine Gruppe bildet ist klar (Assoziativität ist klar,  $id_M$  ist das neutrale Element, und das Inverse von  $\varphi$  ist die Umkehrabbildung  $\varphi^{-1}$ ).

**Bemerkung 13.7** Für  $M = \{1, \dots, n\}$  ist  $S(M) = S_n$ , die symmetrische Gruppe  $n$ -ten Grades. Allgemeiner ist für endliches  $M$ ,  $|M| = n$ , die Gruppe  $S(M)$  isomorph zu  $S_n$ : Schreiben wir  $M = \{m_1, \dots, m_n\}$ , so ist jedes  $\varphi \in S(M)$  von der Form  $\varphi_\sigma$  mit

$$\varphi_\sigma(m_i) = m_{\sigma(i)} \quad (i = 1, \dots, n)$$

für ein eindeutiges  $\sigma \in S_n$ , und  $\sigma \mapsto \varphi_\sigma$  liefert einen Isomorphismus  $S_n \xrightarrow{\sim} S(M)$ .

**Satz 13.8** Sei  $K/k$  der Zerfällungskörper des irreduziblen Polynoms  $f(X) \in k[X]$ . Sei  $N$  die Menge der Nullstellen von  $f$  in  $K$ . Dann ist die Abbildung

$$\begin{aligned} \nu : \text{Aut}_k(K) &\hookrightarrow S(N) \\ \sigma &\mapsto \sigma|_N \end{aligned}$$

ein injektiver Gruppenhomomorphismus.

**Beweis** Zunächst ist die Abbildung wohldefiniert, denn es ist  $\sigma(N) \subseteq N$  wegen  $\sigma|_k = id_k : f(a) = 0 \Rightarrow 0 = \sigma(f(a)) = \sigma(f)(\sigma(a)) = f(\sigma(a))$ . Weiter ist die Restriktionsabbildung offenbar ein Gruppenhomomorphismus. Schließlich ist dieser nach Satz 10.7 (b) (Fall  $k = \tilde{k}$ ,  $K = \tilde{K}$ ,  $\varphi = id_k$ ) injektiv.

**Corollar 13.9** Ist  $f$  separabel, so ist

$$\nu : G \longrightarrow S(N)$$

injektiv, wobei  $G = \text{Gal}(K/k)$  die Galoisgruppe von  $f$  ist.

**Beispiel 13.10** Wir können nun leicht die Galoisgruppe von  $K = \mathbb{Q}(\sqrt[3]{2}, \zeta)$  über  $\mathbb{Q}$  bestimmen ( $\zeta = e^{\frac{2\pi i}{3}}$ , siehe Beispiel 12.10):  $K$  ist der Zerfällungskörper von  $X^3 - 2 \in \mathbb{Q}[X]$ ; also haben wir einen injektiven Homomorphismus

$$G = \text{Gal}(K/\mathbb{Q}) \xrightarrow{\nu} S(\{\sqrt[3]{2}, \zeta\sqrt[3]{2}, \zeta^2\sqrt[3]{2}\}) \cong S_3.$$

Nach 12.10 gilt  $|G| = [K : \mathbb{Q}] = 6 = |S_3|$ . Daher ist  $\nu$  ein Isomorphismus und  $G \cong S_3$ .

**Bemerkung 13.11** Allgemein hat man für die Galoisgruppe  $G$  eines irreduziblen separablen Polynoms  $f \in k[X]$  vom Grad  $\deg(f) = n$  nach 13.9 und 13.7 einen Monomorphismus

$$\nu : G \hookrightarrow S_n.$$

Das Polynom  $f$  heißt ohne Defekt, wenn dies ein Isomorphismus ist, also  $G \cong S_n$  isomorph zur vollen Permutationsgruppe der Nullstellen von  $f$  ist.

## §14 Endliche abelsche Gruppen und endliche Körper

Der folgende Struktursatz für endliche abelsche Gruppen ist ein Vorläufer der sogenannten Sylowsätze für beliebige endliche Gruppen.

**Satz 14.1** Sei  $(A, +)$  eine endliche abelsche Gruppe. Für jede Primzahl  $p$  ist die  $p$ -primäre Komponente von  $A$  definiert als

$$A(p) = \{a \in A \mid \text{es existiert ein } \ell \in \mathbb{N} \text{ mit } p^\ell a = 0\}.$$

Dies ist eine Untergruppe von  $A$ . Gilt  $|A| = \prod_{i=1}^r p_i^{n_i}$ , mit verschiedenen Primzahlen  $p_1, \dots, p_r$ , so ist

$$A = A(p_1) \times \dots \times A(p_r),$$

und  $|A(p_i)| = p^{n_i}$ .

**Beweis** Ist  $p^\ell a = 0$  und  $p^m b = 0$ , so ist  $p^{\ell+m}(a - b) = 0$ , also ist  $A(p)$  eine Untergruppe. Definiere nun

$$\varphi : \prod_{i=1}^r A(p_i) \rightarrow A$$

durch  $\varphi(a_1, \dots, a_r) = \sum_{i=1}^r a_i$ . Dies ist ein Homomorphismus, da  $A$  abelsch ist.

$\varphi$  ist injektiv: Ist  $\sum_{i=1}^r a_i = 0$ , mit  $p_i^{\ell_i} a_i = 0$ , so ist wegen  $a_i = -\sum_{j \neq i} a_j$  auch  $\left(\prod_{j \neq i} p_j^{\ell_j}\right) a_i = 0$ .

Wegen  $\text{ord}(a_i) \mid p_i^{\ell_i}$  und  $\text{ord}(a_i) \mid \prod_{j \neq i} p_j^{\ell_j}$  folgt dann  $\text{ord}(a_i) = 1$  (die Zahlen rechts sind teilerfremd), also  $a_i = 0$ , für alle  $i$ .

$\varphi$  ist surjektiv: Wir zeigen durch Induktion über  $s$ : Ist  $\prod_{i=1}^s p_i^{n_i} a = 0$ , so liegt  $a$  im Bild von  $\prod_{i=1}^s A(p_i)$  (Beachte, dass  $|A| \cdot a = 0$  für jedes  $a \in A$ ). Dies ist klar für  $s = 1$ ; sei also  $s > 1$ .

Da  $m = p_s^{n_s}$  und  $n = \prod_{j=1}^{s-1} p_j^{n_j}$  teilerfremd sind, gibt es  $u, v \in \mathbb{Z}$  mit

$$mu + nv = 1.$$

Dann gilt

$$a = uma + vna,$$

und für  $mna = 0$  folgt  $n(uma) = 0$ , also  $uma = \sum_{i=1}^{s-1} a_i$  mit  $a_i \in A(p_i)$  nach Induktionsvoraussetzung, und  $m(vna) = 0$ , also  $vna \in A(p_s)$  nach Definition.

Wir zeigen nun noch  $|A(p_i)| = p_i^{n_i}$  für alle  $i$ . Sei  $p$  eine Primzahl. Wegen der Endlichkeit von  $A(p)$  gibt es eine  $p$ -Potenz  $p^L$  mit  $p^L a = 0$  für alle  $a \in A(p)$ , zum Beispiel

$$L = \sum_{a \in A(p)} \ell_a \quad , \quad \text{falls } p^{\ell_a} a = 0.$$

Nach dem nachfolgenden Lemma ist also  $|A(p)|$  eine  $p$ -Potenz. Wegen

$$|A| = \prod_{i=1}^r |A(p_i)|$$

und der Eindeutigkeit der Primfaktorzerlegung folgt hieraus die Behauptung.

**Lemma 14.2** Ist  $B$  eine endliche abelsche Gruppe und  $n$  eine natürliche Zahl mit  $nb = 0$  für alle  $b \in B$ , so gilt für jede Primzahl  $p$

$$p \mid |B| \Rightarrow p \mid n.$$

**Beweis:** Übungsaufgabe!

Aus Satz 14.1 folgern wir:

**Corollar 14.3** Eine endliche abelsche Gruppe  $A$  ist genau dann zyklisch, wenn alle  $p$ -primären Komponenten  $A(p)$  zyklisch sind.

**Beweis** Untergruppen von zyklischen Gruppen sind zyklisch. Gilt umgekehrt, dass für alle Primteiler  $p_1, \dots, p_r$  von  $|A|$  die zugehörigen Komponenten  $A(p_i)$  zyklisch sind, so gilt nach 14.1 und dem chinesischen Restsatz

$$A \cong \prod_{i=1}^r A(p_i) \cong \prod_{i=1}^r \mathbb{Z}/p_i^{n_i} \mathbb{Z} \cong \mathbb{Z}/m\mathbb{Z},$$

mit  $m = \prod_{i=1}^r p_i^{n_i}$ .

Wir wenden uns wieder der Körpertheorie zu. Der folgende Satz gilt für beliebige Körper.

**Lemma 14.4** Ist  $K$  ein Körper, so ist jede endliche Untergruppe von  $K^\times$  zyklisch.

**Beweis** Sei  $G \leq K^\times$  eine endliche Untergruppe. Da  $G$  abelsch ist, genügt es nach 14.3 zu zeigen, dass für jede Primzahl  $p$  die  $p$ -primäre Komponente  $G(p)$  zyklisch ist. Da  $G$  endlich ist, gibt es ein  $y \in G(p)$  maximaler Ordnung  $p^m$ . Dann ist  $x^{p^m} = 1$  für alle  $x \in G(p)$ , d.h., jedes  $x \in G(p)$  ist eine Nullstelle des Polynoms  $X^{p^m} - 1$ . Da dieses höchstens  $p^m$  Nullstellen hat (siehe 4.13), folgt  $|G(p)| \leq p^m$ . Andererseits hat  $\langle y \rangle$  schon die Ordnung  $p^m$ ; es folgt  $G(p) = \langle y \rangle$ .

Für endliche Körper liefert dies:

**Corollar 14.5** Ist  $k$  ein endlicher Körper mit  $q$  Elementen, so ist  $k^\times$  zyklisch von der Ordnung  $q - 1$ , und es gibt ein  $y \in k$  mit

$$k = \{0, 1, y, y^2, \dots, y^{q-2}\}.$$

**Corollar 14.6** Ist  $K/k$  eine Erweiterung endlicher Körper, so gibt es ein  $y \in K$  mit  $K = k(y)$  (also ein primitives Element für  $K/k$ ).

Dies beweist den Satz 11.14 (vom primitiven Element) auch im Fall endlicher Körper.

**Bemerkung 14.7** Ist  $k$  ein endlicher Körper mit  $q$  Elementen, so ist  $\text{char}(k) = p > 0$  (da  $\mathbb{Z} \rightarrow k$  nicht injektiv sein kann), der Primkörper von  $k$  also gleich  $\mathbb{F}_p$  (vergleiche 8.7), und damit  $q = p^m$  mit  $m = [k : \mathbb{F}_p] < \infty$ .

**Lemma 14.8** Ist  $K$  ein Körper der Charakteristik  $p > 0$ , so ist die Abbildung

$$F : K \rightarrow K \quad , \quad x \mapsto x^p ,$$

ein Körperhomomorphismus und heißt der (absolute) Frobenius-Homomorphismus von  $K$ .

**Beweis** Trivialerweise gilt  $(xy)^p = x^p y^p$  für  $x, y \in K$ . Weiter ist

$$(x + y)^p = \sum_{i=0}^p \binom{p}{i} x^i y^{p-i} = x^p + y^p ,$$

da  $\binom{p}{i} = \frac{p!}{i!(p-i)!} \equiv 0 \pmod{p}$  für  $0 < i < p$ .

**Bemerkung 14.9** Ist  $K$  endlich, so ist  $F : K \rightarrow K$  nicht nur injektiv, sondern auch surjektiv aus Mächtigkeitsgründen. Dagegen ist  $F : \mathbb{F}_p(X) \rightarrow \mathbb{F}_p(X)$  nicht surjektiv.

**Satz 14.10** Ein Körper der Charakteristik  $p > 0$  ist genau dann vollkommen, wenn  $F : K \rightarrow K$  surjektiv (und damit ein Isomorphismus) ist.

**Beweis** Sei  $F$  surjektiv und  $f \in K[X]$  irreduzibel. Ist  $f$  inseparabel, so gibt es nach 11.6 und 11.7  $a_0, a_1, \dots, a_m \in K$  mit  $f(X) = a_0 + a_1 X^p + \dots + a_m (X^p)^m$ . Seien  $b_0, \dots, b_m \in K$  mit  $b_i^p = a_i$  ( $i = 0, \dots, m$ ). Dann folgt

$$\begin{aligned} f(X) &= b_0^p + b_1^p X^p + \dots + b_m^p (X^p)^m \\ &= (b_0 + b_1 X + \dots + b_m X^m)^p \end{aligned}$$

im Widerspruch zur Irreduzibilität von  $f$ .

Sei umgekehrt  $K$  vollkommen und  $a \in K$ . Sei  $f(X) := X^p - a \in K[X], g \in K[X]$  ein irreduzibler Faktor von  $f$ ,  $L$  der Zerfällungskörper von  $g$  über  $K$  und  $b \in L$  eine Nullstelle von  $g$ . Dann ist  $b^p = a$  und damit  $f = X^p - b^p = (X - b)^p$ . Es gibt also ein  $n \in \{1, \dots, p\}$  mit  $g = (x - b)^n$ . Da  $g$  wegen der Vollkommenheit von  $K$  nur einfache Nullstellen in  $L$  hat, gilt  $n = 1$ , d.h.,  $b \in K$  (mit  $F(b) = b^p = a$  wie gewünscht).

**Corollar 14.11** Jeder endliche Körper ist vollkommen.

**Satz 14.12** Sei  $p$  eine Primzahl und  $n \in \mathbb{N}$ .

- (a) Ist  $K$  der Zerfällungskörper des Polynoms  $X^{p^n} - X \in \mathbb{F}_p[X]$ , so hat  $K$   $p^n$  Elemente.
- (b) Ist  $K$  ein Körper mit  $p^n$  Elementen, so ist  $K/k$  Zerfällungskörper des Polynoms  $X^{p^n} - X$ .

**Beweis** (a) Sei  $N$  die Menge der Nullstellen von  $f(X) = X^{p^n} - X$  in  $K$ , d.h., der Elemente  $a \in K$  mit  $a^{p^n} = a$ . Wegen  $f' = -1$  ist  $ggT(f, f') = 1$ , also  $f$  separabel (Lemma 11.5), also  $|N| = \deg(f) = p^n$ . Wegen

$$F^n(x) = \underbrace{((x^p)^p) \dots}_n = x^{p^n}$$

$n$ -mal

ist  $N = K^{\langle F^n \rangle}$ , wobei  $\langle F^n \rangle \subseteq \text{Aut}(K)$  die von  $F^n$  erzeugte Untergruppe ist. Also ist  $N$  ein Körper. Wegen der Minimalität von  $K$  ist  $N = K$ , d.h.,  $|K| = p^n$ .

(b) Wegen  $|K^\times| = p^n - 1$  gilt  $a^{p^n-1} = 1$  für alle  $a \in K^\times$ , und also  $a^{p^n} = a$  für alle  $a \in K$ . Da  $f = X^{p^n} - X$  höchstens  $p^n$  Nullstellen hat, ist  $K$  gleich der Menge der Nullstellen von  $f$  in einem Zerfällungskörper von  $f$ , also gleich dem Zerfällungskörper (vergleiche 10.4).

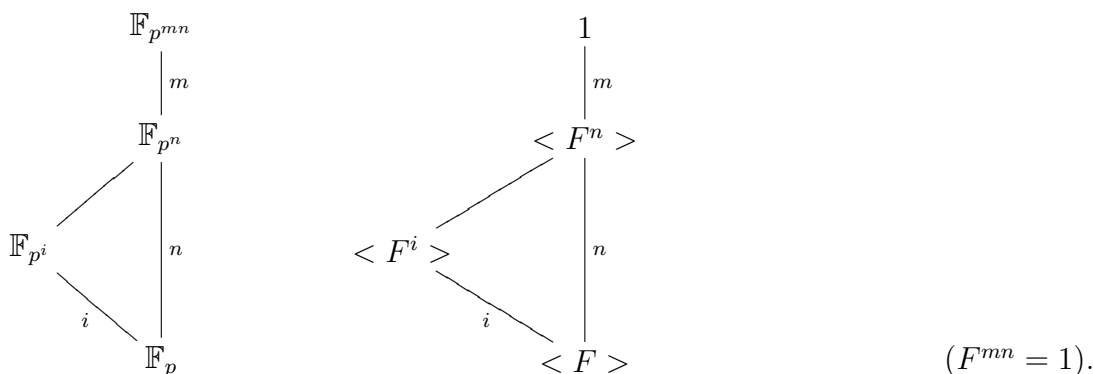
**Corollar 14.13** Es gibt bis auf Isomorphie genau einen Körper mit  $p^n$  Elementen (Bez.:  $\mathbb{F}_{p^n}$ ).

Dies folgt aus der Eindeutigkeit von Zerfällungskörpern, siehe 10.8.

**Corollar 14.14** Sei  $k$  ein endlicher Körper mit  $p^n$  Elementen ( $p$  Primzahl).

- (a) Jede algebraische Erweiterung  $K/k$  ist galoissch.
- (b) Ist  $m \in \mathbb{N}$ , so gibt es bis auf  $k$ -Isomorphie genau eine Erweiterung  $K/k$  mit  $[K : k] = m$ .  $\text{Gal}(K/k)$  ist zyklisch und wird von  $F^n$  erzeugt.

(c)  $\text{Aut}(k)$  wird von  $F$  erzeugt, und die Teilkörper von  $k$  sind die Körper  $\mathbb{F}_{p^i} = k^{\langle F^i \rangle}$  für  $i \mid n$ .



**Beweis** (a)  $K/\mathbb{F}_p$  ist separabel (nach 14.11) und normal (nach 14.12 (b)), daher auch  $K/k$ .

(c) Es ist  $\text{Aut}(k) = \text{Gal}(k/\mathbb{F}_p)$ , da der Primkörper von jedem Automorphismus festgelassen wird. Nach dem Hauptsatz der Galoistheorie ist  $|\text{Gal}(k/\mathbb{F}_p)| = [k : \mathbb{F}_p] = n$ . Andererseits ist die Ordnung von  $\langle F \rangle \subset \text{Gal}(k/\mathbb{F}_p)$  gleich  $n$ , da es ein Element  $y \in k^\times$  der Ordnung  $p^n - 1$  gibt, also mit  $F^m(y) = y^{p^m} \neq y$  für  $m < n$ . Es folgt  $\text{Gal}(k/\mathbb{F}_p) = \langle F \rangle$ . Nach der Theorie der zyklischen Gruppen (siehe Beweis von 2.14) sind die Untergruppen von  $\langle F \rangle$  von der Form  $\langle F^i \rangle$  mit  $i \mid n$ , nach Galoistheorie also die Zwischenkörper von  $k/\mathbb{F}_p$  von der Form  $k^{\langle F^i \rangle}$  mit  $i \mid n$ . Weiter gilt

$$a \in k^{\langle F^i \rangle} \Leftrightarrow a^{p^i} = a \Leftrightarrow a \in \mathbb{F}_{p^i}.$$

(b) Wegen  $[K : \mathbb{F}_p] = m \cdot n$  hat  $K$   $p^{mn}$  Elemente, ist also Zerfällungskörper von  $X^{p^{mn}} - X$  über  $\mathbb{F}_p$ , also auch über  $k$ . Dies zeigt die Eindeutigkeit (nach 10.8). Es ist  $K^{\langle F^n \rangle} \supseteq k$ , und nach (c) gilt Gleichheit. Nach Galoistheorie folgt  $\text{Gal}(K/k) = \langle F^n \rangle$ .

## §15 Einheitswurzeln

**Erinnerung 15.1** (siehe Beispiel 3.18) Für  $m \in \mathbb{N}$  ist  $\bar{a} \in \mathbb{Z}/m\mathbb{Z}$  genau dann Erzeugendes, wenn  $\bar{a}$  in  $(\mathbb{Z}/m\mathbb{Z})^\times$  liegt. Weiter gilt

$$(\mathbb{Z}/m\mathbb{Z})^\times = \{\bar{a} \in \mathbb{Z}/m\mathbb{Z} \mid a \in \mathbb{Z} \text{ mit } \text{ggT}(a, m) = 1\}$$

und daher

$$(15.1.1) \quad |(\mathbb{Z}/m\mathbb{Z})^\times| = \varphi(m),$$

wobei

$$\varphi(m) := |\{a \in \mathbb{N} \mid 0 \leq a < m, \text{ggT}(a, m) = 1\}|.$$

Die Funktion

$$\begin{aligned} \varphi &: \mathbb{N} \rightarrow \mathbb{N} \\ m &\mapsto \varphi(m) \end{aligned}$$

heißt die Eulersche  $\varphi$ -Funktion.

**Lemma 15.2** (a) Für  $ggT(m, n) = 1$  gilt

$$\varphi(m \cdot n) = \varphi(m) \cdot \varphi(n).$$

(b) Ist  $p$  eine Primzahl und  $r \in \mathbb{N}$ , so gilt

$$\varphi(p^r) = (p - 1)p^{r-1}.$$

**Beweis:** (a) Falls  $ggT(m, n) = 1$ , so hat man nach dem chinesischen Restsatz einen Ringisomorphismus

$$\mathbb{Z}/m \cdot n\mathbb{Z} \xrightarrow{\sim} \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}.$$

Dieser induziert natürlich einen Isomorphismus

$$(\mathbb{Z}/m \cdot n\mathbb{Z})^\times \xrightarrow{\sim} (\mathbb{Z}/m\mathbb{Z})^\times \times (\mathbb{Z}/n\mathbb{Z})^\times$$

für die zugehörigen Einheitengruppen. Mit (15.1.1) folgt die Behauptung.

(b): Die natürlichen Zahlen  $a \in \{0, 1, \dots, p^r - 1\}$ , die *nicht* teilerfremd zu  $m = p^r$  sind, sind offenbar gerade die Vielfachen von  $p$

$$0 \cdot p, 1 \cdot p, 2 \cdot p, \dots, (p^{r-1} - 1) \cdot p.$$

Dies sind  $p^{r-1}$  Zahlen. Daher ist

$$\varphi(p^r) = p^r - p^{r-1} = (p - 1)p^{r-1}.$$

**Corollar 15.3** Ist  $m = \prod_{i=1}^{\nu} p_i^{r_i}$  die Primfaktorzerlegung von  $m$  (mit verschiedenen Primzahlen  $p_1, \dots, p_\nu$  und  $r_i \in \mathbb{N}$ ), so gilt

$$\varphi(m) = \prod_{i=1}^{\nu} (p_i - 1)p_i^{r_i-1}.$$

**Beispiel 15.4**  $\varphi(100) = \varphi(4 \cdot 25) = 2 \cdot 20 = 40$ .

Sei nun  $K$  ein Körper und  $n$  eine natürliche Zahl.

**Definition 15.5** Ein Element  $\zeta \in K$  heißt  $n$ -te Einheitswurzel, wenn  $\zeta^n = 1$ , also wenn  $\zeta$  eine Nullstelle des Polynoms  $X^n - 1$  ist. Nenne  $\zeta$  eine primitive  $n$ -te Einheitswurzel, wenn  $\zeta$  die Ordnung  $n$  in  $K^\times$  hat. Die Gruppe der  $n$ -ten Einheitswurzeln sei mit  $\mu_n(K)$  bezeichnet.

Sei  $K_n$  der Zerfällungskörper von  $X^n - 1$  über  $K$ .

**Lemma 15.6** (a)  $\mu_n(K)$  ist zyklisch und die Ordnung von  $\mu_n(K)$  teilt  $n$ .

- (b) Ist  $\zeta \in \mu_n(K_n)$  ein Erzeugendes, so ist  $K_n = K(\zeta)$ .  
(c)  $K_n/K$  ist galoissch.  
(d) Ist  $\text{char}(K) = p > 0$ , so ist  $\mu_{n \cdot p}(K) = \mu_n(K)$  und  $K_{n \cdot p} = K_n$ . Insbesondere ist  $\mu_{p^\nu}(K) = \{1\}$  und  $K_{p^\nu} = K$ .  
(e) Gilt  $\text{char}(K) \nmid n$ , so hat  $\mu_n(K_n)$  die Ordnung  $n$ .

**Beweis:** (a) folgt aus 14.4 (jede endliche Untergruppe von  $K^\times$  ist zyklisch). Beachte, dass  $|\mu_n(K)| = \text{ord}(\zeta) \mid n$  für ein Erzeugendes  $\zeta$  von  $\mu_n(K)$ .

(b):  $K(\zeta)$  enthält alle Potenzen  $\zeta^i$ , also auch alle Elemente von  $\mu_n(K_n)$ , d.h., alle Nullstellen von  $X^n - 1$ . Also ist  $K(\zeta)$  der Zerfällungskörper dieses Polynoms, d.h., gleich  $K_n$ .

(d) folgt wegen  $X^{n \cdot p} - 1 = (X^n - 1)^p$  für  $\text{char}(K) = p$ .

(e): Für  $\text{char}(K) \nmid n$  sind  $X^n - 1$  und  $(X^n - 1)' = n \cdot X^{n-1}$  teilerfremd. Also ist  $X^n - 1$  separabel und hat  $n$  verschiedene Nullstellen in  $K_n$ .

(c): Nach (d) können wir annehmen, dass  $\text{char}(K) \nmid n$ . Dann ist  $K_n/K$  galoissch als Zerfällungskörper des separablen Polynoms  $X^n - 1$ .

Im Folgenden sei angenommen, dass  $n$  nicht von  $\text{char}(K)$  geteilt wird.

**Bemerkung 15.7** Dann ist die Anzahl der primitiven  $n$ -ten Einheitswurzeln in  $K_n$  gleich  $\varphi(n)$ . Denn nach 15.6 (e) ist  $\mu_n(K_n)$  zyklisch von der Ordnung  $n$ . Also ist  $\zeta \in \mu_n(K_n)$  genau dann primitive  $n$ -te Einheitswurzel, wenn  $\zeta$  Erzeugendes dieser Gruppe ist, und nach 15.1 gibt es  $\varphi(n)$  Erzeugende.

**Definition 15.8** Sind  $\zeta_1, \dots, \zeta_{\varphi(n)}$  die primitiven  $n$ -ten Einheitswurzeln in  $K_n$ , so heißt

$$\Phi_n(X) = \Phi_{n,K}(X) = (X - \zeta_1)(X - \zeta_2) \cdots (X - \zeta_{\varphi(n)})$$

das  $n$ -te Kreisteilungspolynom über  $K$ .

**Satz 15.9** (a)  $\Phi_n(X)$  liegt in  $K[X]$ , ist normiert und separabel und hat den Grad  $\varphi(n)$ .

(b) In  $K[X]$  gilt

$$X^n - 1 = \prod_{d \mid n} \Phi_d(X).$$

**Beweis:** (a): Nach Definition gilt  $\Phi_n \in K_n[X]$ . Sei  $G = \text{Gal}(K_n/K)$  (beachte 15.6 (c)!). Ist  $\sigma \in G$  und  $\zeta \in K_n$  eine primitive  $n$ -te Einheitswurzel, so gilt dies auch für  $\sigma(\zeta)$ . Daher permutiert  $\sigma$  die primitiven  $n$ -ten Einheitswurzeln  $\zeta_1, \dots, \zeta_{\varphi(n)}$  und lässt damit  $\Phi_n(X)$  fest. Da dies für alle  $\sigma \in G$  gilt, liegen alle Koeffizienten von  $\Phi_n(X)$  in  $K_n^G = K$ , also  $\Phi_n$  in  $K[X]$ . Der Rest von (a) ist klar.

(b): Dies ergibt sich durch Zusammenfassung der Faktoren in der Zerlegung

$$X^n - 1 = \prod_{\zeta \in \mu_n(K_n)} (X - \zeta).$$

Die Gruppe  $\mu_n(K_n)$  ist nämlich die disjunkte Vereinigung der  $P_d$  für  $d \mid n$ , wobei  $P_d$  die Menge der Elemente der Ordnung  $d$  in  $\mu_n(K_n)$  bezeichnet, also der primitiven  $d$ -ten Einheitswurzeln in  $K_n$ . Es ist also

$$X^n - 1 = \prod_{d \mid n} \prod_{\zeta \in P_d} (X - \zeta) = \prod_{d \mid n} \Phi_d(X).$$

Diese Zerlegung gilt zunächst in  $K_n[X]$ , aber alle Faktoren sind nach (a) in  $K[X]$ .

**Bemerkung 15.10** Mit der Gleichung aus 15.9 (b)

$$X^n - 1 = \prod_{d \mid n} \Phi_d(X) = \Phi_n \cdot \prod_{d \mid n, d < n} \Phi_d$$

kann man die  $\Phi_n$  rekursiv ausrechnen: Kennt man alle  $\Phi_d$  für  $d \mid n$  und  $d < n$ , so erhält man  $\Phi_n$  durch Polynomdivision.

**Beispiele 15.11** (a) Für  $n = 1$  ist  $\Phi_1(X) = X - 1$ .

(b) Für eine Primzahl  $p$  ist

$$X^p - 1 = \Phi_p(X) \cdot (X - 1),$$

also

$$\Phi_p(X) = \frac{X^p - 1}{X - 1} = X^{p-1} + X^{p-2} + \dots + X + 1.$$

Dies zeigt Übereinstimmung mit der Definition in Beispiel 7.11 (b).

(c) Die ersten Kreisteilungspolynome über  $\mathbb{Q}$  sind

$$\begin{aligned} \Phi_1(X) &= X - 1 \\ \Phi_2(X) &= X + 1 \\ \Phi_3(X) &= X^2 + X + 1 \\ \Phi_4(X) &= \frac{X^4 - 1}{(X+1)(X-1)} = \frac{X^4 - 1}{X^2 - 1} = X^2 + 1 \\ \Phi_5(X) &= X^4 + X^3 + X^2 + X + 1 \\ \Phi_6(X) &= \frac{X^6 - 1}{(X^2 + X + 1)(X^2 - 1)} = X^2 - X + 1. \end{aligned}$$

**Satz 15.12** (a) Für  $K = \mathbb{Q}$  ist  $\Phi_n = \Phi_{n, \mathbb{Q}} \in \mathbb{Z}[X]$  und irreduzibel in  $\mathbb{Z}[X]$  und  $\mathbb{Q}[X]$ .

(b) Für beliebiges  $K$  erhält man  $\Phi_{n, K}$  durch Anwendung des kanonischen Homomorphismus  $\mathbb{Z} \rightarrow K$  auf die Koeffizienten von  $\Phi_{n, \mathbb{Q}}$ .

**Beweis:** (a) Sei  $\zeta \in \mathbb{Q}_n$  eine primitive  $n$ -te Einheitswurzel, und sei  $f \in \mathbb{Q}[X]$  das Minimalpolynom von  $\zeta$  über  $\mathbb{Q}$ . Für jede Nullstelle  $\alpha$  von  $f$  in  $\mathbb{Q}_n$  gibt es nach 10.7 (c) ein  $\sigma \in G = \text{Gal}(\mathbb{Q}_n/\mathbb{Q})$  mit  $\sigma(\zeta) = \alpha$ . Also ist  $\alpha$  eine primitive  $n$ -te Einheitswurzel. Wir zeigen, dass umgekehrt jede primitive  $n$ -te Einheitswurzel  $\zeta'$  in  $\mathbb{Q}_n$  Nullstelle von  $f$  ist. Dann folgt  $f = \Phi_n$  nach Definition von  $\Phi_n$  und damit die Irreduzibilität von  $\Phi_n$ .

Als Minimalpolynom von  $\zeta$  ist  $f$  ein Teiler von  $X^n - 1$ , also

$$X^n - 1 = f \cdot h$$

mit  $h \in \mathbb{Q}[X]$ . Nach dem folgenden Lemma sind dann  $f, h \in \mathbb{Z}[X]$  und normiert.

Es ist  $\zeta' = \zeta^m$  mit einem  $m$ , welches teilerfremd zu  $n$  ist.

1. Fall:  $m = p$  Primzahl. Annahme  $f(\zeta^p) \neq 0$ . Dann ist also  $h(\zeta^p) = 0$ , d.h.,  $\zeta$  Nullstelle von  $h(X^p)$ . Hieraus folgt wiederum  $f \mid h(X^p)$ , also

$$h(X^p) = f \cdot g,$$

wobei wie oben folgt, dass  $g \in \mathbb{Z}[X]$  und normiert ist. Betrachte nun die Bilder  $\bar{h}, \bar{f}$  und  $\bar{g}$  in  $\mathbb{F}_p[X]$ . Für diese gilt

$$\bar{h}^p = \bar{h}(X^p) = \bar{f} \cdot \bar{g}.$$

Also sind  $\bar{h}$  und  $\bar{f}$  nicht teilerfremd in  $\mathbb{F}_p[X]$ , also hat das Polynom

$$X^n - 1 = \bar{f} \cdot \bar{h} \in \mathbb{F}_p[X]$$

mehrfache Nullstellen in dem Zerfällungskörper von  $X^n - 1$  über  $\mathbb{F}_p$ . Das ist ein Widerspruch zur Separabilität von  $X^n - 1$  für  $p \neq n$  (Beweis von 15.6(e)).

2. Fall:  $m$  beliebig. Wir führen Induktion über die Anzahl  $r$  der Primfaktoren von  $m$ , wobei der 1. Fall der Induktionsanfang ist. Ist  $m$  zusammengesetzt, so ist  $m = p \cdot q$  für eine Primzahl  $p$ , und nach Induktionsvoraussetzung ist  $\zeta'' = \zeta^q$  Nullstelle von  $f$ . Dann ist  $f$  auch das Minimalpolynom von  $\zeta''$  und nach dem Argument vom 1. Fall ist  $(\zeta'')^p = \zeta^{q \cdot p} = \zeta^m = \zeta'$  Nullstelle von  $f$ .

Da  $f \in \mathbb{Z}[X]$  und normiert ist, folgen wegen  $\Phi_n = f$  nun auch die restlichen Aussagen von (a).

(b): Sei  $\tau : \mathbb{Z}[X] \rightarrow K[X]$  der kanonische Homomorphismus und  $\Phi_n = \Phi_{n, \mathbb{Q}}$ . Wir zeigen durch Induktion über  $n$ , dass  $\tau(\Phi_n) = \Phi_{n, K}$ . Für  $n = 1$  ist

$$\tau(\Phi_1) = X - 1 = \Phi_{1, K}.$$

Für  $n > 1$  gilt

$$\begin{aligned} X^n - 1 &= \Phi_n \cdot \prod_{\substack{d|n \\ d < n}} \Phi_d && \text{in } \mathbb{Z}[X], \\ X^n - 1 &= \Phi_{n, K} \cdot \prod_{\substack{d|n \\ d < n}} \Phi_{d, K} && \text{in } K[X]. \end{aligned}$$

Durch Induktion und Nullteilerfreiheit von  $K[X]$  folgt hieraus  $\tau(\Phi_n) = \Phi_{n, K}$ .

**Lemma 15.12** Sei  $R$  ein faktorieller Ring mit Quotientenkörper  $Q = \text{Quot}(R)$ . Sei  $f \in R[X]$  normiert (bzw. primitiv) und

$$f = g \cdot h \quad \text{in } K[X],$$

wobei  $g$  normiert (bzw. primitiv) ist. Dann sind  $g$  und  $h$  beide in  $R[X]$  und normiert (bzw. primitiv).

**Beweis:** Sei  $b \in Q^\times$  derart, dass  $bh \in R[X]$  und primitiv ist. Nach dem Beweis von Corollar 7.6 ist dann  $b^{-1}g \in R[X]$ . Weiter ist  $b^{-1}g$  nach Lemma 7.4 primitiv. Ist nun  $g$  primitiv, so folgt  $b \in R^\times$  und die Behauptung. Der Fall "normiert" folgt genauso.

**Corollar 15.13** (a) Es gibt einen kanonischen Monomorphismus von Gruppen

$$(15.13.1) \quad \text{Gal}(K_n/K) \hookrightarrow (\mathbb{Z}/n\mathbb{Z})^\times.$$

Insbesondere ist  $\text{Gal}(K_n/K)$  kommutativ und  $[K_n : K]$  ein Teiler von  $\varphi(n)$ .

(b) Für  $K = \mathbb{Q}$  ist (15.3.1) ein Isomorphismus. Für die primitive  $n$ -te Einheitswurzel  $\zeta_n = e^{\frac{2\pi i}{n}} \in \mathbb{C}$  und  $\mathbb{Q}_n = \mathbb{Q}(\zeta_n)$  gilt also

$$(15.13.2) \quad \text{Gal}(\mathbb{Q}(\zeta_n)/\mathbb{Q}) \xrightarrow{\sim} (\mathbb{Z}/n\mathbb{Z})^\times$$

und  $[\mathbb{Q}(\zeta_n) : \mathbb{Q}] = \varphi(n)$ .

**Beweis** (a): Nach 15.6 (c) ist  $K_n/K$  galoissch, und nach 15.6 (b) ist  $K_n = K(\zeta)$ , wobei  $\zeta$  eine primitive  $n$ -te Einheitswurzel in  $K_n$  ist. Für  $\sigma \in \text{Gal}(K_n/K)$  ist  $\sigma(\zeta)$  wieder eine primitive  $n$ -te Einheitswurzel; es gibt also ein  $a' \in \mathbb{Z}$  mit  $ggT(a', n) = 1$ , so dass

$$\sigma(\zeta) = \zeta^{a'}.$$

Die Zahl  $a'$  ist nicht eindeutig, aber für  $a'' \in \mathbb{Z}$  mit  $\zeta^{a'} = \zeta^{a''}$  gilt  $\zeta^{a'-a''} = 1$ , also  $a' - a'' \in n\mathbb{Z}$ . Daher ist

$$a(\sigma) := \bar{a}' := a' \pmod{n\mathbb{Z}} \in (\mathbb{Z}/n\mathbb{Z})^\times \subseteq \mathbb{Z}/n\mathbb{Z}$$

wohldefiniert. Allgemein ist für  $x = \bar{m} \in \mathbb{Z}/n\mathbb{Z}$  mit  $m \in \mathbb{Z}$  die Potenz

$$\zeta^x = \zeta^{\bar{m}} := \zeta^m$$

wohldefiniert, denn für  $m' \in \mathbb{Z}$  mit  $\bar{m} = \bar{m}'$  ist  $t = m' - m \in n\mathbb{Z}$  und damit

$$\zeta^{m'} = \zeta^{m+t} = \zeta^m \cdot \zeta^t = \zeta^m.$$

Die Abbildung

$$\begin{aligned} \varphi : \text{Gal}(K_n/K) &\rightarrow (\mathbb{Z}/n\mathbb{Z})^\times \\ \sigma &\mapsto a(\sigma) \text{ mit } \sigma(\zeta) = \zeta^{a(\sigma)} \end{aligned}$$

ist ein Homomorphismus, denn für  $\sigma, \tau \in \text{Gal}(K_n/K)$  gilt

$$(\sigma\tau)(\zeta) = \sigma(\tau(\zeta)) = \sigma(\zeta^{a(\tau)}) = \zeta^{a(\tau)a(\sigma)},$$

wegen  $(\sigma\tau)(\zeta) = \zeta^{a(\sigma\tau)}$  also  $a(\sigma\tau) = a(\sigma) \cdot a(\tau)$ . Für  $m, r \in \mathbb{Z}$  gilt nämlich

$$\zeta^{\bar{m}} = \zeta^{\bar{r}} \Leftrightarrow \zeta^m = \zeta^r \Leftrightarrow \zeta^{m-r} = 1 \Leftrightarrow m - r \in n\mathbb{Z} \Leftrightarrow \bar{m} = \bar{r} \text{ in } \mathbb{Z}/n\mathbb{Z}.$$

Weiter ist  $\ker(\varphi)$  trivial, also  $\varphi$  injektiv, denn für  $\sigma \in \text{Gal}(K_n/K)$  mit  $\sigma(\zeta) = \zeta^1 = \zeta$  operiert  $\sigma$  trivial auf  $K_n = K(\zeta)$ ; es ist also  $\sigma = id$  das neutrale Element in  $G$ .

Die zweite Aussage in (a) ist dann klar, da  $\text{Gal}(K_n/K) \cong im(\varphi)$  und  $im(\varphi)$  eine Untergruppe von  $(\mathbb{Z}/n\mathbb{Z})^\times$  ist, so dass  $[K_n : K] = |\text{Gal}(K_n/K)| = |im(\varphi)|$  die Ordnung von  $(\mathbb{Z}/n\mathbb{Z})^\times$ , also  $\varphi(n)$  teilt.

(b): Für  $K = \mathbb{Q}$  ist  $\Phi_n$  nach 15.12(a) irreduzibel und damit das Minimalpolynom von  $\zeta_n$  (denn  $\zeta_n$  ist als primitive  $n$ -te Einheitswurzel per Definition eine Nullstelle von  $\Phi_n$  in  $\mathbb{Q}_n$ ). Es folgt  $[\mathbb{Q}_n : \mathbb{Q}] = [\mathbb{Q}(\zeta_n) : \mathbb{Q}] = \deg(\Phi_n) = \varphi(n)$ . Damit muss der Monomorphismus (15.3.1) für  $K = \mathbb{Q}$  ein Isomorphismus sein.  $\square$

**Beispiel 15.14** Für jede Primzahl  $p$  ist  $[\mathbb{Q}(\zeta_p) : \mathbb{Q}] = p-1$  und  $Gal(\mathbb{Q}(\zeta_p) : \mathbb{Q}) \cong (\mathbb{Z}/p\mathbb{Z})^\times$  zyklisch. Zum Beispiel ist  $[\mathbb{Q}(\zeta_3) : \mathbb{Q}] = 2$  und  $Gal(\mathbb{Q}(\zeta_3)/\mathbb{Q}) \cong (\mathbb{Z}/3\mathbb{Z})^\times = \{\pm 1\}$ .

**Bemerkung 15.15** Für allgemeines  $n \in \mathbb{Z}$  ist  $(\mathbb{Z}/n\mathbb{Z})^\times$  nicht immer zyklisch. Für  $n = 15 = 3 \cdot 5$  ist zum Beispiel

$$\begin{aligned} (\mathbb{Z}/15\mathbb{Z})^\times &\cong (\mathbb{Z}/3\mathbb{Z})^\times \times (\mathbb{Z}/5\mathbb{Z})^\times \text{ (Beweis von 15.2)} \\ &\cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z}, \end{aligned}$$

was nicht zyklisch ist, wie man leicht überprüft ( $(0, a)$  und  $(1, a)$  sind beides keine Erzeugenden).

## §16 Der algebraische Abschluss eines Körpers

**Lemma/Definition 16.1** Ein Körper  $K$  heißt algebraisch abgeschlossen, wenn er die folgenden äquivalenten Bedingungen erfüllt:

- (a) In  $K[X]$  zerfällt jedes Polynom in Linearfaktoren.
- (b) Jede algebraische Erweiterung  $L$  von  $K$  ist trivial, d.h., gleich  $K$ .

**Beweis** der Äquivalenz: Gilt (a) und ist  $L/K$  algebraisch, so ist für jedes  $\alpha \in L$  das Minimalpolynom von  $\alpha$  über  $K$  vom Grad 1, also  $\alpha \in K$ . Also ist  $L = K$ . Sei umgekehrt  $f \in K[X]$  nicht konstant und  $L/K$  der Zerfällungskörper von  $f$  über  $K$ . Gilt (b), so ist  $L = K$  und  $f$  zerfällt schon über  $K$ .

Erstes Ziel dieses Abschnitts ist der Beweis von:

**Satz 16.2** Sei  $K$  ein Körper. Dann gibt es eine algebraische Körpererweiterung  $L/K$ , für die  $L$  algebraisch abgeschlossen ist.  $L$  ist bis auf  $K$ -Isomorphie eindeutig und heißt der algebraische Abschluss von  $K$ . (Bez:  $\overline{K}$  oder  $K^{\text{alg}}$ ).

Hierzu brauchen wir Polynomringe in unendlich vielen Variablen.

**Definition 16.3** Sei  $R$  ein kommutativer Ring mit Eins. Eine  $R$ -Algebra ist ein Ring mit Eins  $S$  zusammen mit einem Homomorphismus  $\varphi : R \rightarrow S$  von Ringen mit Eins.

Für  $r \in R$  und  $s \in S$  schreibe auch

$$(16.3.1) \quad r \cdot s := \varphi(r) \cdot s.$$

Ein Homomorphismus  $\phi : S \rightarrow S'$  von  $R$ -Algebren ist ein Ringhomomorphismus für den

$$\begin{array}{ccc} S & \xrightarrow{\phi} & S' \\ & \swarrow \varphi & \nearrow \varphi' \\ & R & \end{array}$$

kommutativ ist.

**Beispiel 16.4** Der Polynomring  $R[X]$  in einer Variablen ist eine  $R$ -Algebra vermöge

$$\begin{array}{ll} R & \rightarrow R[X] \\ a & \mapsto a \quad (\text{konstantes Polynom}). \end{array}$$

**Definition 16.5** Sei  $I$  eine Menge. Der Polynomring über  $R$  mit Indexmenge  $I$  ist eine  $R$ -Algebra  $R[I]$  zusammen mit einer Familie  $(X_i)_{i \in I}$  in  $R[I]$ , so dass die folgende universelle Eigenschaft gilt: Ist  $S$  eine  $R$ -Algebra und ist  $(s_i)_{i \in I}$  eine mit  $I$  indizierte Familie in  $S$ , so gibt es genau einen  $R$ -Algebren-Homomorphismus

$$\phi : R[I] \rightarrow S$$

mit  $\phi(X_i) = s_i$  für alle  $i \in I$ .

**Satz 16.6** Es gibt einen Polynomring  $(R[I], (X_i)_{i \in I})$  und dieser ist bis auf Isomorphie von  $R$ -Algebren eindeutig. Genauer gilt: Hat  $(\tilde{S}, (\tilde{X}_i)_{i \in I})$  dieselbe universelle Eigenschaft, so gibt es genau einen  $R$ -Algebren-Isomorphismus  $\tilde{\phi} : R[I] \rightarrow \tilde{S}$  mit  $\tilde{\phi}(X_i) = \tilde{X}_i$  für alle  $i \in I$ .  $R[I]$  wird auch mit  $R[(X_i)_{i \in I}]$  oder  $R[X_i \mid i \in I]$  bezeichnet.

**Beweis** Die *Eindeutigkeitsaussage* ist klar:  $\tilde{\phi}$  existiert nach der universellen Eigenschaft von  $(R[I], (X_i)_{i \in I})$ , und nach der universellen Eigenschaft von  $(\tilde{S}, (\tilde{X}_i)_{i \in I})$  gibt es (genau) einen  $R$ -Algebren Homomorphismus  $\tilde{\phi} : \tilde{S} \rightarrow R[I]$  mit  $\tilde{\phi}(\tilde{X}_i) = X_i$  für alle  $i \in I$ . Wiederrum mit den universellen Eigenschaften folgt  $\tilde{\phi} \tilde{\phi} = id_{S[I]}$  und  $\tilde{\phi} \tilde{\phi} = id_{\tilde{S}}$ . Daher ist  $\tilde{\phi}$  ein Isomorphismus.

*Existenz* von  $(R[I], (X_i)_{i \in I})$  (vergleiche 4.16):

Setze

$$A := \mathbb{N}_0^{(I)} := \{(\alpha_i)_{i \in I} \in \mathbb{N}^I \mid \alpha_i = 0 \text{ für fast alle } i \in I\}$$

und

$$R[I] := R^{(A)} := \{(a_\alpha)_{\alpha \in A} \mid a_\alpha = 0 \text{ für fast alle } \alpha \in A\}.$$

mit der Addition

$$(a_\alpha) + (b_\alpha) := (a_\alpha + b_\alpha)$$

und der Multiplikation

$$(16.6.1) \quad (a_\alpha) \cdot (b_\alpha) := (c_\alpha) \quad \text{wobei} \quad c_\alpha = \sum_{\beta+\gamma=\alpha} a_\beta b_\gamma.$$

Hierbei ist

$$(\beta_i)_{i \in I} + (\gamma_i)_{i \in I} = (\beta_i + \gamma_i)_{i \in I}$$

für  $\beta = (\beta_i), \gamma = (\gamma_i) \in A$ . Beachte, dass die Summe in (16.6.1) endlich ist. Dann ist  $(R[I], +, \cdot)$  ein kommutativer Ring mit Eins und eine  $R$ -Algebra mittels des Ringhomomorphismus

$$R \rightarrow R[I]$$

$$a \mapsto a \text{ mit } a_\alpha = \begin{cases} a & , \alpha = 0 \\ 0 & , \alpha \neq 0 \end{cases} .$$

Setzen wir

$$X_i := (a_\alpha) \text{ mit } a_\alpha := \begin{cases} 1 & , \alpha = (\delta_{ji})_{j \in I} \\ 0 & , \text{sonst} \end{cases} ,$$

so lässt sich jedes  $f = (a_\alpha)_{\alpha \in A}$  schreiben als

$$(16.6.2) \quad f = \sum_{\alpha \in A} a_\alpha \cdot X^\alpha ,$$

wobei

$$(16.6.3) \quad X^\alpha := \prod_{i \in I} X_i^{\alpha_i} \text{ für } \alpha \in A = \mathbb{N}_0^{(I)} ,$$

und wobei die Summe in (16.6.2) und die Produkte in (16.6.3) endlich sind. In dieser Schreibweise ist klar, dass jedes  $f$  eine endliche Summe von *Monomen*

$$a_\alpha X^\alpha$$

sind, wobei  $a_\alpha \in R$  und  $X^\alpha$  ein endliches Produkt von  $X_i$ 's ist (wobei ein  $X_i$  mehrfach, nämlich in der Potenz  $X_i^{\alpha_i}$  ( $\alpha_i \in \mathbb{N}_0$ ) vorkommen kann und  $X_i^{\alpha_i}$  weggelassen wird für  $\alpha_i = 0$  – was für fast alle  $i \in I$  der Fall ist).

Die universelle Eigenschaft für  $(k[I], (X_i)_{i \in I})$  ist nun einfach: Ist eine  $R$ -Algebra  $S$  und eine Familie  $s = (s_i)_{i \in I}$  in  $S$  gegeben, so definiere

$$\phi : R[I] \rightarrow S$$

durch

$$(16.6.4) \quad \phi\left(\sum_{\alpha \in A} a_\alpha X^\alpha\right) := \sum_{\alpha \in A} a_\alpha s^\alpha \in S$$

(beachte die Konvention (16.3.1)!), wobei

$$s^\alpha := \prod_{i \in I} s_i^{\alpha_i} \quad (\alpha \in A)$$

gesetzt wird und wieder Summe und Produkte endlich sind ( $s_i^{\alpha_i} = 1$  für  $\alpha_i = 0$  wird im Produkt weggelassen,  $a_\alpha s^\alpha = 0$  für  $a_\alpha = 0$  wird in der Summe weggelassen). Offenbar gilt  $\phi(X_i) = s_i$  und man zeigt leicht mit (16.6.2) und (16.6.3), dass  $\Phi$  ein Homomorphismus von  $R$ -Algebren ist. Schließlich ist  $\Phi$  der einzige Homomorphismus von  $R$ -Algebren mit  $\Phi(X_i) = s_i$  für alle  $i \in I$ , denn hieraus folgt sofort (16.6.4).

**Beispiel 16.7** Der Polynomring  $\mathbb{Z}[X_i \mid i \in \mathbb{N}]$  enthält zum Beispiel alle Polynome

$$f_{m,n}(X) = X_1^n + \dots + X_m^n$$

für alle  $m$  und  $n$  in  $\mathbb{N}$ .

Als nächstes benötigen wir:

**Satz 16.8** Sei  $R$  ein Ring (kommutativ, mit Eins) und sei  $\mathfrak{a} \subsetneq R$  ein echtes Ideal. Dann besitzt  $R$  ein maximales Ideal  $\mathfrak{m}$  mit  $\mathfrak{a} \subseteq \mathfrak{m}$ . Insbesondere besitzt also jeder Ring  $R \neq 0$  ein maximales Ideal.

**Beweis** mit Zorns Lemma (Lineare Algebra II, Lemma 11.13): Sei  $M$  die Menge der echten Ideale  $\mathfrak{b} \subseteq R$  die  $\mathfrak{a}$  enthalten. Dann ist die Inklusion  $\subseteq$  eine Ordnung auf  $M$  und wegen  $\mathfrak{a} \in M$  nicht leer. Weiter besitzt jede Kette (=total geordnete Teilmenge)  $N \subseteq M$  eine obere Schranke in  $M$ : Für  $N = \emptyset$  ist nichts zu zeigen. Für  $N \neq \emptyset$  ist

$$\mathfrak{c} = \bigcup_{\mathfrak{b} \in N} \mathfrak{b}$$

ein echtes Ideal in  $R$ . Denn für  $\alpha_1, \alpha_2 \in \mathfrak{c}$  gibt es  $\mathfrak{b}_1, \mathfrak{b}_2 \in N$  mit  $\alpha_1 \in \mathfrak{b}_1, \alpha_2 \in \mathfrak{b}_2$  und es gibt  $\mathfrak{b}_1 \subseteq \mathfrak{b}_2$  oder  $\mathfrak{b}_2 \subseteq \mathfrak{b}_1$ . Gilt (ohne Einschränkung)  $\mathfrak{b}_1 \subseteq \mathfrak{b}_2$ , so liegen  $\alpha_1, \alpha_2$  in  $\mathfrak{b}_2$ , also  $\alpha_1 + \alpha_2 \in \mathfrak{b} \subseteq \mathfrak{c}$ . Weiter ist für  $\alpha \in \mathfrak{c}$  und  $\lambda \in R$  offenbar  $\lambda\alpha \in \mathfrak{c}$ .

Also ist  $\mathfrak{c} \in M$  und offenbar eine obere Schranke für  $N$  bezüglich  $\subseteq$ .

Nach Zorns Lemma besitzt nun  $M$  ein maximales Element  $\mathfrak{m}$ , dies ist ein maximales Ideal  $\mathfrak{m} \supseteq \mathfrak{a}$  wie gewünscht.

Nun kommen wir zum **Beweis von Satz 16.2**:

Sei  $K$  der gegebene Körper und

$$I = \{f \in K[X] \mid \deg f \neq 0\}$$

die Menge der nicht-konstanten Polynome über  $K$ . Sei

$$R = K[X_f \mid f \in I]$$

der mit  $f \in I$  indizierte Polynomring über  $K$ . Dann ist das Ideal

$$\mathfrak{a} = (f(X_f) \mid f \in I)$$

ein echtes Ideal in  $R$ . Andernfalls wäre nämlich  $1 \in \mathfrak{a}$  und es gäbe eine Gleichung

$$1 = \sum_{i=1}^n g_i(X) f_i(X_{f_i})$$

in  $R$  mit  $f_1, \dots, f_n \in I$  und  $g_1, \dots, g_n \in R$ . Sei  $K_1/K$  ein Zerfällungskörper von  $f_1 \cdots f_n$  und  $\alpha_i \in K_1$  eine Nullstelle von  $f_i$  in  $K_1$  ( $i = 1, \dots, n$ ). Wählen wir nun die Familie  $\alpha = (\alpha_f)_{f \in I}$  mit  $\alpha_{f_i} = \alpha_i$  ( $i = 1, \dots, n$ ) und  $\alpha_f = 0$  für  $f \notin \{f_1, \dots, f_n\}$  (zum Beispiel) so folgt

$$1 = \sum_{i=1}^n g_i(\alpha) f_i(\alpha_i) = 0,$$

Widerspruch! Also ist  $\mathfrak{a} \neq R$ , und nach 16.8 gibt es ein maximales Ideal  $\mathfrak{m} \subseteq R$  mit  $\mathfrak{a} \subseteq \mathfrak{m}$ . Dann ist

$$L_1 := R/\mathfrak{m}$$

ein Körper, der mittels des Körperhomomorphismus

$$K \hookrightarrow K[X_f \mid f \in I] = R \twoheadrightarrow R/\mathfrak{m} = L_1$$

eine Körpererweiterung von  $K$  ist. In dieser hat jedes nicht-konstante Polynom  $f \in K[X]$  eine Nullstelle: Ist nämlich  $\alpha_f := \overline{X_f}$  die Restklasse von  $X_f$  in  $R/\mathfrak{a}$ , so ist  $f(\alpha_f) = \overline{f(X_f)} = 0$  in  $R/\mathfrak{a}$ , also für das Bild  $\beta_f$  von  $\alpha_f$  in  $L_1$  ebenfalls  $f(\beta_f) = 0$ .

Iterieren wir die Konstruktion, so erhalten wir Körpererweiterungen

$$K = L_0 \subseteq L_1 \subseteq L_2 \subseteq \dots \quad ,$$

so dass für jedes  $n \geq 0$  gilt: Jedes nicht-konstante Polynom  $f \in L_n[X]$  hat eine Nullstelle in  $L_{n+1}$ . Dann ist

$$L = \bigcup_{n=0}^{\infty} L_n$$

wieder ein Körper (ähnlicher Schluss wie im Beweis von 16.8), also eine Körpererweiterung von  $K$ .

*Behauptung:*  $L$  ist ein algebraischer Abschluss von  $K$ .

*Beweis* 1)  $L$  ist algebraisch abgeschlossen: Sei  $f \in L[X]$  nicht konstant. Dann gibt es ein  $n \geq 0$  mit  $f \in L_n[X]$ ; dieses hat in  $L_{n+1}$  eine Nullstelle, also auch in  $L$ . Jedes nicht-konstante Polynom  $f \in L[X]$  hat also eine Nullstelle in  $L$  und spaltet daher einen Linearfaktor ab. Durch Polynomdivision folgt, dass  $f$  über  $L$  in Linearfaktoren zerfällt.

2)  $L/L_n$  ist algebraisch:  $L_1/K$  ist algebraisch, denn jedes  $\alpha \in L_1$  liegt in  $K(\beta_1, \dots, \beta_n)$ , wobei  $\beta_i = \text{Bild von } X_{f_i} \text{ in } L_1$ , für gewisse  $f_i \in I$  ( $i = 1, \dots, n$ ). Aber  $f_i(\beta_i) = 0$ , also ist jedes  $\beta_i$  algebraisch über  $K$ . Damit ist  $K(\beta_1, \dots, \beta_n)/K$  algebraisch (Satz 9.9), also  $\alpha$  algebraisch über  $K$ . Entsprechend ist  $L_n/L_{n-1}$  algebraisch für alle  $n \geq 1$  und damit  $L_n/K$  algebraisch für alle  $n \geq 0$  (Corollar 9.10). Es folgt, dass jedes  $\alpha \in L$  algebraisch über  $K$  ist.

Es bleibt noch die Eindeutigkeit in Satz 16.2 zu zeigen.

**Lemma 16.9** (a) Sei  $L/K$  eine algebraische Körpererweiterung und  $\varphi : K \rightarrow \Omega$  ein Homomorphismus in einem algebraisch abgeschlossenen Körper  $\Omega$ . Dann gibt es eine Fortsetzung  $\psi : L \rightarrow \Omega$  von  $\varphi$ .

(b) Ist  $L$  algebraisch abgeschlossen und  $\Omega$  algebraisch über  $\varphi(K)$ , so ist  $\psi$  ein Isomorphismus.

**Beweis** (a) mit dem Lemma von Zorn: Sei  $M$  die Menge aller Paare  $(E, \tau)$ , wobei  $K \subseteq E \subseteq L$  ein Zwischenkörper ist und  $\tau : E \rightarrow \Omega$  eine Fortsetzung von  $\varphi$ . Definiere eine (Teil-)Ordnung  $\preceq$  auf  $M$  durch

$$(E, \tau) \preceq (E', \tau') \Leftrightarrow E \subseteq E' \text{ und } \tau'|_E = \tau.$$

Da  $(K, \varphi) \in M$ , ist  $M$  nicht leer. Weiter ist  $M$  induktiv geordnet: Ist  $N \subseteq M$  totalgeordnet, so zeigt das übliche Vereinigungselement, dass  $N$  eine obere Schranke in  $M$  besitzt. Nach Zorns Lemma besitzt  $M$  also ein maximales Element

$$(F, \psi : F \rightarrow \Omega).$$

Angenommen  $F \subsetneq L$ . Dann gibt es ein  $\alpha \in L \setminus F$ . Nach Corollar 10.6 gibt es dann eine Fortsetzung  $\tau : F(\alpha) \rightarrow \Omega$  von  $\psi$  (Ist  $f$  das Minimalpolynom von  $\alpha$  über  $F$ , so hat  $\tilde{f} = \varphi(f)$  eine Nullstelle  $\tilde{\alpha}$  in  $\Omega$ , da  $\Omega$  algebraisch abgeschlossen ist; es gibt also nach 10.6 eine Fortsetzung  $\tau$  von  $\psi$  mit  $\tau(\alpha) = \tilde{\alpha}$ ). Dies ist aber ein Widerspruch zur Maximalität von  $(F, \psi)$ . Also ist  $F = L$  und (a) gezeigt.

(b): Ist  $L$  algebraisch abgeschlossen, so gilt dies auch für  $\psi(L)$ . Da  $\Omega$  algebraisch über  $\varphi(K)$  ist und  $\varphi(K) \subseteq \psi(L) \subseteq \Omega$ , ist  $\Omega$  auch algebraisch über  $\psi(L)$ . Nach 16.1 ist also  $\psi(L) = \Omega$ . Daher ist  $\psi$  surjektiv und, als Körperhomomorphismus, auch injektiv.  $\square$

**Corollar 16.10** Sind  $\Omega_1, \Omega_2$  zwei algebraische Körpererweiterungen von  $K$ , die algebraisch abgeschlossen sind, so gibt es einen  $K$ -Isomorphismus

$$\varphi : \Omega_1 \xrightarrow{\sim} \Omega_2.$$

Damit ist Satz 16.2 vollständig bewiesen.

**Beispiele 16.11** (a) Sei  $K/\mathbb{Q}$  eine endliche Körpererweiterung (man nennt dann  $K$  einen Zahlkörper). Dann gibt es nach 16.9 eine  $(\mathbb{Q})$ -Einbettung  $\varphi : K \hookrightarrow \mathbb{C}$ . Ist  $\overline{\mathbb{Q}}$  ein algebraischer Abschluss von  $\mathbb{Q}$ , so können wir diesen mit dem Teilkörper  $\Omega$  aller über  $\mathbb{Q}$  algebraischen Zahlen in  $\mathbb{C}$  identifizieren (vergleiche Übungsaufgabe 29 ii)).

(b) Sei  $p$  eine Primzahl und  $\overline{\mathbb{F}}_p$  ein algebraischer Abschluss von  $\mathbb{F}_p$ . Sei  $F : \overline{\mathbb{F}}_p \rightarrow \overline{\mathbb{F}}_p$  der Frobenius-Homomorphismus. Dieser ist surjektiv (also ein Automorphismus): Für  $a \in \overline{\mathbb{F}}_p$  liegt  $a$  nämlich im endlichen Körper  $\mathbb{F}_p(a)$ , und es ist schon  $F : \mathbb{F}_p(a) \rightarrow \mathbb{F}_p(a)$  surjektiv. Für  $n \in \mathbb{N}$  sei

$$\overline{\mathbb{F}}_p^{\langle F^n \rangle} = \{\alpha \in \overline{\mathbb{F}}_p \mid F^n(\alpha) = \alpha\}$$

der Fixkörper von  $F^n$ , also auch der von  $F^n$  erzeugten Untergruppe von  $\text{Aut}(\overline{\mathbb{F}}_p)$ . Dann ist

$$\overline{\mathbb{F}}_p^{\langle F^n \rangle} = \mathbb{F}_{p^n},$$

denn es ist

$$\overline{\mathbb{F}}_p^{\langle F^n \rangle} = \{\alpha \in \overline{\mathbb{F}}_p \mid \alpha^{p^n} - \alpha = 0\}$$

die Nullstellenmenge des separablen Polynoms  $X^{p^n} - X$ , hat also  $p^n$  Elemente.

**Bemerkungen 16.12** (a) Sei  $k$  ein Körper. Offenbar ist der algebraische Abschluss  $\overline{k}$  normal über  $k$  (Jedes Polynom  $f \in k[X]$  zerfällt über  $\overline{k}$  in Linearfaktoren).

(b)  $k$  ist genau dann vollkommen, wenn  $\overline{k}/k$  separabel (und damit auch galoissch) ist. Also sind  $\overline{\mathbb{Q}}/\mathbb{Q}$  und  $\overline{\mathbb{F}}_p/\mathbb{F}_p$  galoissch. Die Untersuchung von  $\text{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$  ist ein wichtiges Thema der Algebraischen Zahlentheorie.

Aus Satz 11.12 folgt sofort:

**Corollar 16.13** Sei  $K/k$  eine endliche Körpererweiterung. Dann ist  $|\text{Hom}_k(K, \bar{k})| \leq [K : k]$  und  $|\text{Hom}_k(K, \bar{k})| = [K : k]$  genau dann, wenn  $K/k$  separabel ist.

**Bemerkung 16.14** Es gilt sogar, dass  $|\text{Hom}_k(K, \bar{k})|$  den Grad  $[K : k]$  teilt (siehe Übungsaufgabe 46). Man nennt  $|\text{Hom}_k(K, \bar{k})|$  auch den *Separabilitätsgrad* von  $K/k$  (Bez.:  $[K : k]_s$ ) und  $[K : k]_i := [K : k]/[K : k]_s$  den *Inseparabilitätsgrad* von  $K/k$ , so dass

$$[K : k] = [K : k]_s \cdot [K : k]_i.$$

Viele Aussagen, die wir für Zerfällungskörper formuliert haben, lassen sich auch mit den algebraischen Abschluss formulieren. Ein Beispiel war 16.12, ein anderes ist (vergleiche Satz 10.7):

**Satz 16.15** Sei  $L/k$  eine algebraische Körpererweiterung und  $\varphi : k \rightarrow \Omega$  ein Homomorphismus in einen algebraisch abgeschlossenen Körper (z.B.  $\Omega = \bar{k}$ ). Sei  $\alpha \in L$ ,  $f$  das Minimalpolynom von  $\alpha$  über  $k$  und  $\tilde{\alpha}$  eine Nullstelle von  $f$  in  $\Omega$ . Dann gibt es eine Fortsetzung  $\psi : L \rightarrow \Omega$  von  $\varphi$  mit  $\psi(\alpha) = \tilde{\alpha}$ .

**Beweis** Übungsaufgabe!

## §17 Gruppenoperationen

Gruppen werden eigentlich erst dadurch interessant, dass (und wie) sie auf anderen Objekten (Mengen, Vektorräumen, ...) operieren. Dies ist auch für viele Anwendungen wichtig.

**Definition 17.1** Sei  $G$  eine Gruppe und  $M$  eine Menge. Eine (Links-)Operation von  $G$  auf  $M$  ist eine Verknüpfung

$$\begin{aligned} \psi &: G \times M \rightarrow M \\ (g, m) &\mapsto gm := \psi(g, m) \end{aligned}$$

für die gilt:

$$\begin{aligned} g_1(g_2m) &= (g_1g_2)m \\ 1m &= m \end{aligned}$$

für  $g_1, g_2 \in G, m \in M$  und das neutrale Element  $1 \in G$ .  $M$  mit dieser Verknüpfung heißt dann auch eine (Links-)  $G$ -Menge.

**Bemerkungen 17.2** Es gibt auch Rechts-Operationen; für diese verlangt man  $g_2(g_1m) = (g_1g_2)m$ . Schreibt man die Operation "von rechts", als  $mg$ , so liest sich diese Regel einleuchtender als  $(mg_1)g_2 = m(g_1g_2)$ . Man schreibt dann auch meist die Verknüpfung als  $\psi : M \times G \rightarrow M, (m, g) \mapsto mg$ .

**Beispiele 17.3** (a) Ist  $L/K$  eine galoissche Körpererweiterung mit Galoisgruppe  $G = \text{Gal}(L/K)$ , so operiert  $G$  auf  $L$  vermöge  $\sigma\alpha := \sigma(\alpha)$  für  $\sigma \in G$  und  $\alpha \in L$ .

(b)  $Gl_n(\mathbb{R})$  operiert auf  $\mathbb{R}^n$  vermöge

$$(A, x) \mapsto Ax$$

(übliche Anwendung der Matrix  $A \in Gl_n(\mathbb{R})$  auf den Vektor  $x \in \mathbb{R}^n$ ).

(c) Sei  $(G, \cdot)$  eine Gruppe. Die Assoziativität der Verküpfung

$$\psi : G \times G \rightarrow G \quad , \quad (g, h) \mapsto g \cdot h$$

besagt gerade, dass  $\mu$  eine Links- und eine Rechts-Operation von  $G$  auf sich selbst (also auf  $M = G$ ) definiert.

**Definition 17.4** Die Gruppe  $G$  operiere auf der Menge  $M$ .

(a) Ist  $m \in M$ , so heißt

$$Gm := \{gm \mid g \in G\} \subseteq M$$

die Bahn (oder der Orbit) von  $m$  unter  $G$  und

$$St(m) := St_G(m) := \{g \in G \mid gm = m\} \subseteq G$$

die Standgruppe (oder der Stabilisator) von  $m$  in  $G$ .

(b)  $G \setminus M$  sei die Menge der Bahnen.

(c) Man sagt, dass  $G$  transitiv auf  $M$  operiert, wenn es nur einen Orbit gibt ( $\Leftrightarrow$  Sind  $m_1, m_2 \in M$ , so gibt es ein  $g \in G$  mit  $m_2 = gm_1$ ).

**Satz 17.5** Sei  $m \in M$ . Dann ist die Standgruppe  $St(m)$  eine Untergruppe von  $G$  und die Abbildung

$$\begin{aligned} \varphi_m : G/St(m) &\rightarrow Gm \\ gSt(m) &\mapsto gm \end{aligned}$$

eine wohldefinierte Bijektion (Hier ist  $G/St(m)$  die Menge der Linksnebenklassen von  $G$  nach der Untergruppe  $St(m)$ , siehe §1).

**Beweis** Sind  $g, h \in St(m)$ , also  $gm = m = hm$ , so folgt  $(gh^{-1})m = (gh^{-1})hm = gh^{-1}hm = gm = m$ , d.h.,  $gh^{-1} \in St(m)$ . Also ist  $St(m)$  nach dem Untergruppenkriterium eine Untergruppe. Weiter gilt für  $u \in St(m)$

$$(gu)m = g(um) = gm;$$

dies zeigt die Wohldefiniiertheit von  $\varphi_m$ . Die Surjektivität ist klar. Ist weiter  $gm = hm$  für  $g, h \in G$ , so folgt  $g^{-1}hm = g^{-1}gm = m$ , also  $g^{-1}h \in St(m)$  und damit  $gSt(m) = hSt(m)$ . Dies zeigt die Injektivität von  $\varphi_m$ .

**Lemma 17.6** Ist  $m \in M$  und  $g \in G$ , so gilt

$$St(gm) = gSt(m)g^{-1}.$$

**Beweis**  $g' \in St(gm) \Leftrightarrow g'(gm) = gm \Leftrightarrow g^{-1}g'gm = m \Leftrightarrow g^{-1}g'g \in St(m)$ . Es folgt  $g^{-1}St(gm)g = St(m)$  und damit die Behauptung.

**Proposition 17.7** Die Relation

$$m_1 \sim m_2 \Leftrightarrow \exists g \in G \text{ mit } m_2 = gm_1$$

ist eine Äquivalenzrelation auf  $M$ , und die Äquivalenzklassen sind die Bahnen unter  $G$ . Insbesondere sind zwei Bahnen entweder gleich oder disjunkt und  $M$  ist die disjunkte Vereinigung der Bahnen:

$$M = \bigcup_{b \in G \backslash M} b.$$

**Beweis** Reflexivität:  $m = 1m$ . Transitivität:  $m_2 = gm_1, m_3 = hm_2 \Rightarrow m_3 = hm_2 = hgm_1$ . Symmetrie:  $m_2 = gm_1 \Rightarrow m_1 = g^{-1}m_2$ . Die zweite Aussage ist klar: Die Äquivalenzklasse von  $m_1$  ist  $\{m_2 \in M \mid m_1 \sim m_2\} = \{m_2 \in M \mid \exists g \in G \text{ mit } m_2 = gm_1\} = Gm_1$ . Die dritte Aussage folgt daraus, dass Äquivalenzklassen immer eine Partition der unterliegenden Menge liefern (Lineare Algebra II, Satz 9.6).

**Beispiele 17.8** (a) Die symmetrische Gruppe  $S_n$  operiert transitiv auf der Menge  $\{1, \dots, n\}$ . Für  $i \in \{1, \dots, n\}$  ist

$$U_i := \{\sigma \in S_n \mid \sigma(i) = i\}$$

die Standgruppe von  $i$ . Aus Satz 17.6 folgt

$$(S_n : U_i) = n.$$

(b) Sei  $U \leq G$  eine Untergruppe der Gruppe  $G$ . Dann operiert  $U$  von links auf  $G$  durch die Gruppen-Verknüpfung  $((u, g) \mapsto ug$  für  $u \in U, g \in G$ ). Per definitionem ist hierbei die Rechtsnebenklasse  $Ug$  die Bahn von  $G$  unter  $U$ . Der Stabilisator jedes Elements ist trivial, denn aus  $ug = g$  folgt  $u = 1$ .

(c) Für  $U \leq G$  operiert  $G$  transitiv von links auf  $G/U$ ; und der Stabilisator der Nebenklasse  $U \in G/U$  ist  $U$ . Insbesondere ist jede Untergruppe ein Stabilisator für eine geeignete Operation.

**Satz 17.9** (Bahnengleichung) Sei  $G$  eine endliche Gruppe und  $M$  eine endliche  $G$ -Menge. Sei

$$M^G := \{m \in M \mid gm = m \quad \forall g \in G\}$$

die *Fixmenge* von  $G$  in  $M$ . Dann gilt

$$|M| = \sum_{b \in G \backslash M} |b| = |M^G| + \sum_{x \in R'} |Gx|,$$

wobei  $R' \subseteq M$  ein Repräsentantensystem für diejenigen Bahnen in  $G \backslash M$  ist, die nicht nur aus einem Element bestehen (d.h., die Zuordnung  $x \mapsto Gx$  liefert eine Bijektion zwischen  $R'$  und der Menge der Bahnen, die mehr als ein Element enthalten).

**Beweis** Die erste Gleichung gilt nach Proposition 17.7. Die zweite folgt, da  $M^G$  die Vereinigung der Bahnen ist, die nur aus einem Element bestehen.

Wir erhalten die folgende nützliche Anwendung auf die Gruppentheorie:

**Definition 17.10** Sei  $G$  eine Gruppe.

(a) Für  $g, h \in G$  heißt  $h$  konjugiert zu  $g$ , wenn es ein  $a \in G$  gibt mit  $h = aga^{-1}$ .

(b) Sei  $g \in G$ . Die *Konjugationsklasse* von  $g$  (in  $G$ ) ist die Menge

$$C(g) := C_G(g) := \{aga^{-1} \mid a \in G\}$$

aller Elemente in  $G$ , die konjugiert zu  $g$  sind.

(c) Der *Zentralisator* von  $g \in G$  ist die Menge

$$Z(g) := Z_G(g) := \{a \in G \mid ag = ga\}$$

der mit  $g$  vertauschbaren Elemente in  $G$ .

**Proposition 17.11** (a) Konjugation ist eine Äquivalenzrelation. Die zugehörigen Äquivalenzklassen sind die Konjugationsklassen.

(b) Zwei Konjugationsklassen sind entweder gleich oder disjunkt, und  $G$  ist die disjunkte Vereinigung der Konjugationsklassen.

(c) Für  $g \in G$  ist  $Z(g)$  eine Untergruppe von  $G$ , und es gibt eine Bijektion

$$\begin{aligned} G/Z(g) &\rightarrow C(g) \\ aZ(g) &\mapsto aga^{-1}. \end{aligned}$$

Insbesondere ist  $|C(g)| = (G : Z(g))$ .

**Beweis** Durch die Konjugation, d.h., die Abbildung

$$(17.11.1) \quad \begin{aligned} G \times G &\rightarrow G \\ (a, g) &\mapsto aga^{-1} \end{aligned}$$

ist eine Operation von  $G$  auf sich selbst erklärt: Es ist  $(ab)g(ab)^{-1} = abgb^{-1}a^{-1} = a(bgb^{-1})a$  für  $a, b, g \in G$ . Dabei ist offenbar  $C(g)$  die Bahn von  $g$  und  $Z(g)$  die Standgruppe von  $g$ . Die Behauptungen folgen daher mit 17.5 und 17.7.

**Corollar 17.12** (Klassengleichung) Sei  $G$  eine endliche Gruppe und

$$Z(G) := \{g \in G \mid ag = ga \forall a \in G\}$$

das *Zentrum* von  $G$ . Dann ist  $Z(G)$  eine Untergruppe von  $G$  und

$$(G : 1) = (Z(G) : 1) + \sum_{g \in R'} (G : Z(g)),$$

wobei  $R' \subseteq G$  ein Repräsentatensystem für die Konjugationsklassen ist, die nicht nur aus einem Element bestehen.

**Beweis** Dass  $Z(G)$  eine Untergruppe ist, rechnet man leicht mittels der Definition nach. Die anderen Aussagen folgen sofort aus der Bahnengleichung 17.8 für die Konjugationsoperation (17.11.1): Die Fixmenge ist gerade  $Z(G)$ , denn es gilt  $ag = ga$  genau dann,

wenn  $aga^{-1} = g$ . Weiter ist nach 17.11 der Orbit von  $g$  unter dieser Operation gerade  $C(g)$  und  $|C(g)| = (G : Z(g))$ .

## §18 p-Gruppen und Sylowsätze

Sei  $p$  eine Primzahl.

**Definition 18.1** Eine  $p$ -Gruppe ist eine endliche Gruppe, deren Ordnung eine  $p$ -Potenz ist.

**Definition 18.2** Sei  $G$  eine endliche Gruppe und  $H \leq G$  eine Untergruppe.

- (a)  $H$  heißt  $p$ -Untergruppe, wenn  $H$  eine  $p$ -Gruppe ist.
- (b)  $H$  heißt  $p$ -Sylowgruppe, wenn die Ordnung von  $H$  die höchste  $p$ -Potenz ist, die  $(G : 1)$  teilt (d.h., wenn  $H$  eine  $p$ -Untergruppe und  $(G : H)$  prim zu  $p$  ist).

**Satz 18.3** (Sylow) Ist  $G$  eine endliche Gruppe, so besitzt  $G$  eine  $p$ -Sylowgruppe.

**Beweis** Durch Induktion über die Ordnung  $(G : 1)$ . Ist  $(0 : 1)$  prim, so ist die Aussage trivial. Sei nun  $G$  eine endliche Gruppe, und die Behauptung bewiesen für alle Gruppen kleinerer Ordnung. Existiert eine echte Untergruppe  $H \leq G$ , deren Index prim zu  $p$  ist, so ist eine  $p$ -Sylowgruppe  $P$  von  $H$  auch eine von  $G$ , denn aus dem Satz von Lagrange folgt  $(G : P)(P : 1) = (G : 1) = (G : H)(H : 1) = (G : H)(H : P)(P : 1)$ , also  $(G : P) = (G : H)(H : P)$ . Wir können also annehmen, dass alle echten Untergruppen einen Index in  $G$  haben, der von  $p$  geteilt wird.

Nach der Klassengleichung gilt

$$(G : 1) = (Z(G) : 1) + \sum_{g \in R'} (G : Z(g)),$$

wobei  $R'$  ein Repräsentantensystem für die Konjugationsklassen ist, die nicht nur aus einem Element bestehen,  $Z(G)$  das Zentrum von  $G$  und  $Z(g)$  der Zentralisator von  $g$  in  $G$  ist. Nach Voraussetzung ist  $Z(g) \neq G$  für  $g \in R'$ , also werden die Indizes  $(G : Z(g))$  und  $(G : 1)$  von  $p$  geteilt. Folglich wird auch  $(Z(G) : 1)$  von  $p$  geteilt.

Es ist damit die  $p$ -primäre Komponente  $Z(G)(p)$  (siehe §14) der abelschen Gruppe  $Z(G)$  nicht-trivial; somit gibt es ein nicht-triviales  $a \in Z(G)$ , dessen Ordnung eine  $p$ -Potenz ist. Durch Übergang zu einer Potenz können wir annehmen, dass  $\text{ord}(a) = p$ . Sei  $H = \langle a \rangle$  die von  $a$  erzeugte zyklische Untergruppe; wegen  $H \subseteq Z(G)$  ist dies ein Normalteiler in  $G$ . Sei  $p^n$  die höchste Potenz von  $p$ , die  $(G : 1)$  teilt. Dann teilt  $p^{n-1}$  (und nicht  $p^n$ ) die Ordnung von  $G/H$ . Nach Induktionsvoraussetzung existiert eine  $p$ -Sylowgruppe  $P'$  von  $G/H$ . Ist  $P$  das Urbild von  $P'$  unter dem Epimorphismus  $G \rightarrow G/H$ , so ist  $H \trianglelefteq P$  und  $P/H \xrightarrow{\sim} P'$ . Damit hat  $P$  die Ordnung  $(P : H)(H : 1) = (P' : 1)(H : 1) = p^{n-1}p = p^n$  und ist eine  $p$ -Sylowgruppe von  $G$ .

**Satz 18.4** (Sylow) Sei  $G$  eine endliche Gruppe.

- (a) Ist  $H$  eine  $p$ -Untergruppe von  $G$ , so ist  $H$  in einer  $p$ -Sylowgruppe enthalten.  
 (b) Alle  $p$ -Sylowgruppen sind konjugiert.

**Beweis** Sei  $S$  die Menge aller  $p$ -Sylowgruppen von  $G$ . Dann operiert  $G$  auf  $S$  durch Konjugation, d.h., vermöge

$$\begin{aligned} G \times S &\rightarrow S \\ (g, P) &\mapsto gPg^{-1}. \end{aligned}$$

Denn wegen des Gruppenisomorphismus  $P \xrightarrow{\sim} gPg^{-1}$ ,  $a \mapsto gag^{-1}$ , ist  $(gPg^{-1} : 1) = (P : 1)$ , also  $gPg^{-1}$  wieder eine  $p$ -Sylowgruppe für jedes  $g \in G$ . Weiter gilt  $g(hPh^{-1})g^{-1} = (gh)P(gh)^{-1}$ ; es handelt sich also um eine Gruppenoperation.

(a): Sei  $P_0$  eine  $p$ -Sylowgruppe. Die Standgruppe  $St(P_0)$  von  $P_0 \in S$  in  $G$  enthält  $P_0$ , der Index  $(G : St(P_0))$  ist also prim zu  $p$ , als Teiler von  $(G : P_0)$ . Nach 17.5 ist  $(G : St(P_0))$  gleich der Mächtigkeit des Orbits  $S_0 \subset S$  von  $P_0$ .  $H$  operiert auf diesem Orbit, und  $S_0$  ist die disjunkte Vereinigung von Orbits unter  $H$ . Da  $H$  eine  $p$ -Gruppe ist, ist die Mächtigkeit jedes dieser  $H$ -Orbits entweder 1 oder eine nicht-triviale  $p$ -Potenz (die Standgruppen haben Index 1 oder eine  $p$ -Potenz). Da  $|S_0|$  prim zu  $p$  ist, gibt es also einen  $H$ -Orbit, der nur aus einem Element besteht, etwa aus der  $p$ -Sylowgruppe  $P_1$ . Nach Definition ist dann  $H$  im Normalisator  $N = N(P_1)$  von  $P_1$  enthalten: Für eine beliebige Gruppe  $G$  und eine Untergruppe  $U \leq G$  ist der *Normalisator* von  $U$  in  $G$  definiert als

$$N(U) := N_G(U) := \{g \in G \mid gUg^{-1} = U\}.$$

Es ist klar, dass dies die größte Untergruppe von  $G$  ist, in der  $U$  ein Normalteiler ist.

Es ist also  $P_1$  normal in  $N$  und nach dem ersten Isomorphiesatz ist  $HP_1$  eine Untergruppe von  $N$ ,  $P_1$  normal hierin, und

$$H/H \cap P_1 \xrightarrow{\sim} HP_1/P_1.$$

Die linksstehende Gruppe ist (als Faktorgruppe von  $H$ ) eine  $p$ -Gruppe, die Ordnung der rechtsstehenden Gruppe ist (als Teiler von  $(G : P_1)$ ) prim zu  $p$ . Daher sind beide Gruppen trivial, d.h.,  $HP_1 = P_1$ , d.h.  $H \subseteq P_1$ . Da  $P_1 \in S_0$ , ist  $P_1 = gP_0g^{-1}$  für ein  $g \in G$ .

(b): Sei insbesondere  $H$  eine  $p$ -Sylowgruppe von  $G$ . Wir haben eben gesehen, dass  $H$  in einem konjugierten  $P_1$  von  $P_0$  liegt. Es folgt  $H = P_1$ , da diese Gruppen dieselbe Ordnung haben (nämlich die maximale  $p$ -Potenz, die  $(G : 1)$  teilt).

**Beispiel 18.5**  $A_3 = \langle (123) \rangle$  ist die eindeutig bestimmte 3-Sylowgruppe von  $S_3$ . Die 2-Sylowgruppen von  $S_3$  sind  $\langle (12) \rangle$ ,  $\langle (13) \rangle$  und  $\langle (23) \rangle$ .

**Satz 18.6** (Sylow) Sei  $G$  eine endliche Gruppe.

(a) Ist  $P$  eine  $p$ -Sylowgruppe von  $G$  und  $H \leq G$  eine  $p$ -Untergruppe, die im Normalisator von  $P$  enthalten ist, so gilt  $H \subseteq P$ .

(b) Für die Anzahl  $s_p$  der  $p$ -Sylowgruppen von  $G$  gilt  $s_p \equiv 1 \pmod{p}$ .

**Beweis** (a) haben wir in Beweis von Satz 18.4 bewiesen (dort die Überlegungen für  $H$  und  $P_1$ ).

(b) Sei  $S(p)$  die Menge der  $p$ -Sylowgruppen von  $G$  und  $P_0$  eine feste  $p$ -Sylowgruppe von  $G$ . Dann operiert  $P_0$  auf  $S(p)$  durch Konjugation:

$$\begin{aligned} P_0 \times S(p) &\rightarrow S(p) \\ (h, U) &\mapsto hUh^{-1}. \end{aligned}$$

Der Orbit von  $P_0$  besteht nur aus einem Element, nämlich  $P_0$ . Für eine  $p$ -Sylowgruppe  $P \neq P_0$  dagegen wird  $P$  nicht von  $P_0$  festgelassen, denn sonst wäre nach (a)  $P_0 \subseteq P$ , also  $P_0 = P$ , weil diese Gruppen gleiche Ordnung haben – Widerspruch! Also ist die Mächtigkeit des Orbits eine nicht-triviale  $p$ -Potenz ( $P_0 : St(P)$ ). Aus der Bahnengleichung folgt die Behauptung: Es ist

$$\begin{aligned} s_p = |S(p)| &= |\{P_0\}| + \sum_{\substack{b \in P_0 \setminus P(p) \\ |b| \neq 1}} |b| \\ &\equiv 1 \pmod{p}. \end{aligned}$$

**Satz 18.7** Eine nicht-triviale endliche  $p$ -Gruppe hat ein nicht-triviales Zentrum.

**Beweis** Wir benutzen wieder die Klassengleichung

$$(G : 1) = (Z(G) : 1) + \sum_{g \in R'} (G : Z(g)).$$

Da  $G$  eine  $p$ -Gruppe ist, werden  $(G : 1)$  und auch alle Indizes  $(G : Z(g))$  durch  $p$  geteilt: nach Definition von  $R'$  ist  $(G : Z(g)) \neq 1$  für  $g \in R'$ , andererseits muss  $(G : Z(g))$  eine  $p$ -Potenz sein. Es folgt  $p \mid (Z(G) : 1)$ , also  $Z(G) \neq 1$ .

**Corollar 18.8** Sei  $G$  eine nicht-triviale  $p$ -Gruppe. Dann existiert eine Folge von Normalteilern in  $G$

$$1 = G_0 \subseteq G_1 \subseteq \dots \subseteq G_n = G$$

derart, dass  $G_i/G_{i-1}$  zyklisch von der Ordnung  $p$  ist.

**Beweis** Da  $Z(G)$  nicht-trivial ist, gibt es ein Element  $a$  der Ordnung  $p$  in  $Z(G)$ . Dann ist  $H = \langle a \rangle$  ein Normalteiler in  $G$  (wegen  $gag^{-1} = a$  für alle  $g \in G$ ). Ist  $G \neq H$ , so gibt es nach Induktion eine Folge

$$1 = G'_1 \subseteq G'_2 \subseteq \dots \subseteq G'_n \subseteq G/H$$

von Normalteilern wie oben in der Gruppe  $G/H$ , und die Urbilder  $G_i = \pi^{-1}(G'_i)$  unter  $\pi : G \rightarrow G/H$  zusammen mit  $G_0 := 1$  bilden eine Folge wie gewünscht in  $G$  (wegen  $G_i/G_{i-1} \cong G'_i/G'_{i-1}$  für  $i \geq 1$  und  $G_1 = H$ ).

## §19 Symmetrische Gruppen

Sei  $n \in \mathbb{N}$  und  $S_n$  die zugehörige Gruppe der Permutationen (bijektive Selbstabbildungen) der Menge  $\{1, \dots, n\}$ .

**Definition 19.1** (vergleiche Lineare Algebra, Beispiel 14.6 (b)) (a) Ein Element  $\sigma \in S_n$  heißt Zyklus der Länge  $m$ , wenn es paarweise verschiedene  $x_1, \dots, x_m \in \{1, \dots, n\}$  gibt mit

$$\begin{aligned}\sigma(x_i) &= x_{i+1} & \text{für } i = 1, \dots, m-1, \\ \sigma(x_m) &= x_1 \\ \sigma(x) &= x & \text{für } x \notin \{x_1, \dots, x_m\}.\end{aligned}$$

Wir schreiben dann  $\sigma = (x_1 \cdots x_m)$ .

(b) Ein Zyklus der Länge 2 heißt Transposition.

**Beispiel 19.2** Das Element

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

aus  $S_4$  kann geschrieben werden als  $(243)$ . Die Elemente von  $S_3$  sind  $(1), (12), (13), (23), (123), (13, 2)$ .

**Satz 19.3** (a) Zwei Zyklen  $(x_1 \dots x_k)$  und  $(y_1 \dots y_\ell)$  in  $S_n$  sind genau dann gleich, wenn  $k = \ell$  ist und wenn die Tupel  $(x_1, \dots, x_k)$  und  $(y_1, \dots, y_k)$  durch zyklische Permutation auseinander hervorgehen, d.h., es gibt ein  $i \in \{1, \dots, k\}$  mit  $\{y_1, \dots, y_k\} = (x_1, x_{i+1}, \dots, x_k, x_1, x_2, \dots, x_{i-1}) (\Leftrightarrow y_j = x_{\varphi^i(j)} \text{ für } \varphi = (123 \dots k) \in S_k)$ .

(b) Für  $\sigma \in S_n$  und einen Zyklus  $(x_1 \dots x_k) \in S_n$  ist

$$\sigma(x_1 \dots x_k) \sigma^{-1} = (\sigma(x_1) \sigma(x_2) \dots \sigma(x_k)).$$

(c) Sei  $\tau = (x_1 x_2 \dots x_k)$  ein  $k$ -Zyklus. Die Konjugationsklasse  $C(\tau)$  von  $\tau$  in  $S_n$  besteht genau aus allen  $k$ -Zyklen. Der Zentralisator  $Z(\tau)$  von  $\tau$  ist die Untergruppe

$$\{\tau^i \sigma \mid i = 0, \dots, k-1, \sigma \in U_{\{x_1, \dots, x_k\}}\}$$

wobei  $U_{\{x_1, \dots, x_k\}} = \{\sigma \in S_n \mid \sigma(x_i) = x_i \forall i = 1, \dots, k\}$ . Es gilt

$$|C(\tau)| = \frac{n!}{(n-k)!k}, \quad (Z(\tau) : 1) = (n-k)!k.$$

**Beweis** (a): Die Menge  $\{x_1, \dots, x_k\}$  ist durch  $\tau = (x_1, \dots, x_k)$  festgelegt, da  $\tau(x) = x$  für  $x \notin \{x_1, \dots, x_k\}$  und  $\tau(x) \neq x$  für  $x \in \{x_1, \dots, x_k\}$ . Aus  $(x_1 \dots x_k) = (y_1 \dots y_\ell)$  folgt somit  $\{x_1, \dots, x_k\} = \{y_1, \dots, y_\ell\}$  und insbesondere  $k = \ell$ . Ist  $y_1 = x_i, i \in \{1, \dots, k\}$ , so sind alle anderen  $y_j$  wie beschrieben festgelegt. Umgekehrt sind die angegebenen Bedingungen hinreichend für die Gleichheit  $(x_1 \dots x_m) = (y_1 \dots y_\ell)$ .

(b): Dies folgt unmittelbar aus den Definitionen.

(c): Übungsaufgabe!

**Definition 19.4** Zwei Zyklen  $(x_1 \dots x_m)$  und  $(y_1 \dots y_n)$  heißen elementfremd, wenn  $\{x_1, \dots, x_m\} \cap \{y_1, \dots, y_n\} = \emptyset$  ist.

**Satz 19.5** (a) Zwei elementfremde Zyklen  $\tau_1, \tau_2 \in S_n$  sind vertauschbar, d.h., es ist  $\tau_1 \tau_2 = \tau_2 \tau_1$ .

(b) Jedes  $\sigma \in S_n$  ist Produkt von paarweise elementfremden Zyklen; in diesem Produkt sind die Zyklen der Länge  $\geq 2$  eindeutig bestimmt.

(c) Jedes  $\sigma \in S_n$  ist Produkt von Transpositionen (d.h.,  $S$  wird von den Transpositionen erzeugt).

**Beweis** Da ein Zyklus  $\tau = (x_1 \dots x_m)$  die Menge  $\{x_1, \dots, x_m\}$  in sich überführt und alle  $x \notin \{x_1, \dots, x_m\}$  festlässt, ist (a) klar. Für  $\sigma \in S_n$  sei  $H = \langle \sigma \rangle$  die von  $\sigma$  erzeugte zyklische Untergruppe, und seien  $Ha_1 \dots Ha_r$  die verschiedenen Bahnen unter der Operation von  $H$  auf  $M = \{1, \dots, n\}$ . Ist  $m_i = (H : St(a_i))$  der Index des Stabilisators  $St(a_i)$  von  $a_i$ , so besteht  $Ha_i$  aus den verschiedenen Elementen

$$a_i, \sigma a_i, \sigma^2 a_i, \dots, \sigma^{m_i-1} a_i,$$

und es ist  $\sigma(\sigma^{m_i-1} a_i) = \sigma^{m_i} a_i = a_i$  (es ist  $H/St(a_i) \cong \mathbb{Z}/m_i\mathbb{Z}$ ). Damit ist klar, dass  $\sigma = \tau_1 \dots \tau_r$ , mit den Zyklen

$$\tau_i = (a_i \sigma a_i \dots \sigma^{m_i-1} a_i).$$

Hierbei kann man Zyklen der Länge 1 weglassen ( $(x) = id$  für jedes  $x \in \{1, \dots, n\}$ ). Ist umgekehrt  $\sigma = \tau'_1 \dots \tau'_s$  mit paarweise elementfremden Zyklen  $\tau'_i$ , ohne Einschränkung alle der Länge  $\geq 2$ , so lässt  $\sigma$  genau die  $x \in M$  fest, die in keinem der Zyklen  $\tau'_i$  auftauchen, und die verschiedenen Bahnen der Länge  $\geq 2$  sind die Mengen  $\{x_1^i, \dots, x_{m_i}^i\}$  für  $\tau'_i = (x_1^i \dots x_{m_i}^i)$ . Hieraus folgt die Übereinstimmung mit dem zuerst erhaltenen Produkt der  $\tau_i$  bis auf die 1-Zyklen unter den  $\tau_i$ .

Die Behauptung (c) wurde schon in der Linearen Algebra bewiesen; sie folgt auch aus (b) und der Beziehung

$$(x_1 \dots x_m) = (x_1 x_m)(x_1 x_{m-1}) \dots (x_1 x_2)$$

für einen Zyklus der Länge  $m \geq 3$  (Beweis: Induktion).

In Linearer Algebra I wurde eingeführt und bewiesen:

**Proposition/Definition 19.6** (a) Es gibt einen eindeutig bestimmten Homomorphismus.

$$sign : S_n \rightarrow \{\pm 1, -1\} = \mu_2$$

mit  $sign(\tau) = -1$  für jede Transposition  $\tau$ .

(b) Der Wert  $sign(\sigma)$  heißt das Signum (oder auch die Parität) von  $\sigma \in S_n$ . Das Element  $\sigma$  heißt gerade (bzw. ungerade), wenn  $sign(\sigma) = 1$  (bzw.  $sign(\sigma) = -1$ ).

(c) Die alternierende Gruppe  $A_n \leq S_n$  wird definiert als der Kern von  $sign$ .

(d)  $A_n$  ist ein Normalteiler in  $S_n$ , es ist  $(A_n : 1) = \frac{n!}{2}$  und  $(S_n : A_n) = 2$ .

Für (d) beachte man, dass der Homomorphiesatz einen Isomorphismus  $S_n/A_n \xrightarrow{\sim} \{\pm 1\}$  liefert.

**Lemma 19.7** (a) Ein Element  $\sigma \in S_n$  liegt genau dann in  $A_n$ , wenn es Produkt von Dreierzyklen (d.h., Zyklen der Länge 3) ist.

(b) Für  $n \geq 3$  wird  $A_n$  von den Dreierzyklen  $(123), (124), \dots, (12n-1), (12n)$  erzeugt.

**Beweis** Für  $n \leq 2$  ist (a) trivialerweise richtig (das triviale Produkt ist das Einselement). Ist nun  $(ijk)$  ein Dreierzykel, so sind  $i, j, k$  paarweise verschieden, und man hat

$$(19.7.1) \quad (ijk) = (ik)(ij),$$

welches nach 19.6 (a) in  $A_n$  liegt. Da  $A_n$  eine Untergruppe ist, enthält es auch alle Produkte von Dreierzykeln. Umgekehrt ist nach 19.5 (c) und 19.6 (a) jedes  $\sigma \in A_n$  Produkt einer geraden Anzahl von Transpositionen. Es reicht daher, das Produkt von zwei Transpositionen  $\tau_1 = (ij)$  und  $\tau_2 = (k\ell)$  zu betrachten. Sind  $\tau_1, \tau_2$  elementfremd, also  $i, j, k, \ell$  paarweise verschieden, so ist

$$(k\ell)(ij) = (ilk)(kij).$$

Andernfalls ist entweder  $\tau_1 = \tau_2$  und damit  $\tau_1\tau_2 = \tau_1^2 = 1$ , oder  $\tau_1, \tau_2$  stimmen in genau einer Stelle überein, und das Produkt ist ein Dreierzyklus nach (19.7.1)

(b): Übungsaufgabe.

**Definition 19.8** Eine Gruppe  $G$  heißt einfach, wenn sie keine Normalteiler außer den trivialen (d.h., 1 und  $G$ ) hat.

**Satz 19.9** Für  $n \geq 5$  ist  $A_n$  einfach.

**Beweis** Sei  $N \trianglelefteq A_n$  ein Normalteiler. Es genügt zu zeigen, dass  $N$  einen Dreierzyklus  $(x_1x_2x_3)$  enthält. Dann enthält nämlich  $N$  das Quadrat  $(x_1x_2x_3)^2 = (x_2x_1x_3)$  und alle Konjugierten  $\sigma(x_2x_1x_3)\sigma^{-1}$ , für  $\sigma \in A_n$ . Ist  $x_k \notin \{x_1, x_2, x_3\}$  und  $\sigma = (x_1x_2)(x_3x_k)$ , so ist

$$\sigma(x_2x_1x_3)\sigma^{-1} = (x_1x_2x_k),$$

und diese Dreierzyklen erzeugen zusammen mit  $(x_1x_2x_3)$  die Gruppe  $A_n$  nach 19.7 (b) (und Umnummerierung, d.h., Konjugation).

Sei nun  $1 \neq \sigma \in N$  ein Element, welches minimal viele Zahlen  $i \in \{1, \dots, n\}$  verrückt (d.h., nicht festlässt). Verrückt  $\sigma$  genau 3 Zahlen, so ist  $\sigma$  ein Dreierzyklus. Verrückt  $\sigma$  genau 4 Zahlen, so ist wegen  $\sigma \in A_n$

$$\sigma = (x_1x_2)(x_3x_4)$$

mit paarweise verschiedenen  $x_1, \dots, x_4$ . Nach Voraussetzung gibt es ein  $x_5 \notin \{x_1, \dots, x_4\}$ , und mit  $\tau = (x_3x_4x_5) \in A_n$  liegt

$$\sigma_1 = \tau\sigma\tau^{-1} = (x_1x_2)(x_4x_5)$$

in  $N$ . Daher ist auch

$$\sigma\sigma_1 = (x_1x_2)^2(x_3x_4x_5) = (x_3x_4x_5)$$

in  $N$ , welches nur 3 Zahlen verrückt: Widerspruch!

Verrückt  $\sigma$  mehr als 4 Zahlen, so schreiben wir

$$\sigma = \tau_1 \dots \tau_r$$

mit paarweise elementfremden, nicht-trivialen Zyklen, die nach der Länge geordnet sind, wobei  $\tau_1$  die maximale Länge  $k$  hat.

Ist  $k = 2$ , so schreibe

$$\text{Fall 1:} \quad \sigma = (x_1x_2)(x_3x_4)\sigma'$$

(alle  $\tau_i$  sind dann Transpositionen und  $r$  muss gerade sein). Ist  $k = 3$ , so schreibe

$$\text{Fall 2:} \quad \sigma = (x_1x_2x_3)(x_4x_5)\sigma', \quad \text{oder}$$

$$\text{Fall 3:} \quad \sigma = (x_1x_2x_3)(x_4x_5x_6)\sigma',$$

und ist  $k \geq 4$ , so schreibe

$$\text{Fall 4:} \quad \sigma = (x_1x_2x_3x_4\dots)\sigma'.$$

Im zweiten Fall ist  $\sigma^2 = (x_2x_1x_3)$  ein nicht-trivialer Dreierzyklus in  $N$ : Widerspruch! In den anderen Fällen benutzen wir, dass  $\sigma_1 = \tau\sigma\tau^{-1} \in N$ , für  $\tau = (x_2x_3x_4) \in A_n$ . In den Fällen 1,3 und 4 ist jeweils

$$\begin{aligned} \sigma_1 &= (x_1x_3)(x_4x_2)\sigma' \\ \sigma_1 &= (x_1x_3x_4)(x_2x_5x_6)\sigma' \\ \sigma_1 &= (x_1x_3x_4x_2\dots)\sigma'. \end{aligned}$$

Da  $N$  eine Untergruppe ist, liegt  $\sigma_2 = \sigma^{-1}\sigma_1 \in N$ . Im ersten und letzten Fall verrückt  $\sigma_2$  nur 4 Zahlen, da  $\sigma x = \sigma_1 x$  für  $x \notin \{x_1, x_2, x_3, x_4\}$ : Widerspruch. Im mittleren Fall ist

$$\sigma_2 = (x_1x_2x_4x_3x_6),$$

welches 5 Zahlen, also weniger als  $\sigma$  verrückt. Widerspruch!

## §20 Kummer-Theorie

Die folgenden Aussagen sind fundamental für viele Anwendungen der Körpertheorie und insbesondere für die Behandlung abelscher Erweiterungen, d.h., von Galoiserweiterungen mit abelscher Galoisgruppe.

**Definition 20.1** Ist  $G$  eine Gruppe und  $K$  ein Körper, so heißt ein Gruppenhomomorphismus

$$\chi : G \rightarrow K^\times$$

ein Charakter von  $G$  mit Werten in  $K$ .

**Satz 20.2** (von Artin, über die lineare Unabhängigkeit von Charakteren) Sei  $G$  eine Gruppe und  $K$  ein Körper. Verschiedene Charaktere  $\chi_1, \dots, \chi_n$  von  $G$  mit Werten in  $K$  sind linear unabhängig im  $K$ -Vektorraum  $\text{Abb}(G, K)$  aller Abbildungen von  $G$  nach  $K$ .

**Beweis** Angenommen der Satz ist falsch. Dann gibt es ein minimales  $n \in \mathbb{N}$ , so dass es paarweise verschiedene Charaktere  $\chi_1, \dots, \chi_n : G \rightarrow K^\times$  gibt mit einer nicht-trivialen Linearkombination

$$(20.2.1) \quad a_1\chi_1 + a_2\chi_2 + \dots + a_n\chi_n = 0,$$

mit  $a_1, \dots, a_n \in K$ . Wegen der Minimalität sind alle  $a_i \neq 0$  und es ist  $n \geq 2$  wegen  $\chi_1 \neq 0$ . Für alle  $g, h \in G$  gilt dann

$$a_1\chi_1(gh) + \dots + a_n\chi_n(gh) = 0.$$

Wegen  $\chi_1 \neq \chi_2$  gibt es ein  $g_0 \in G$  mit  $\chi_1(g_0) \neq \chi_2(g_0)$ . Da  $h$  beliebig war, und wegen  $\chi_i(g_0h) = \chi_i(g_0)\chi_i(h)$  für alle  $i$ , gilt

$$(20.2.2) \quad a_1\chi_1(g_0)\chi_1 + a_2\chi_2(g_0)\chi_2 + \dots + a_n\chi_n(g_0)\chi_n = 0$$

in  $\text{Abb}(G, K)$ . Multiplizieren wir (20.2.1) mit  $\chi_1(g_0)$  und ziehen wir (20.2.2) ab, so erhalten wir

$$a_1(\chi_1(g_0) - \chi_2(g_0))\chi_2 + \dots + a_n(\chi_1(g_0) - \chi_n(g_0))\chi_n = 0.$$

Diese Linearkombination ist nicht trivial (wegen  $\chi_1(g_0) - \chi_2(g_0) \neq 0$ ) und von kleinerer Länge als  $n$  – Widerspruch!

**Corollar 20.3** Sind  $L$  und  $M$  Körper und  $\varphi_1, \dots, \varphi_n : L \rightarrow M$  paarweise verschiedene Körper-Homomorphismen, so sind  $\varphi_1, \dots, \varphi_n$  linear unabhängig über  $M$ .

**Beweis** Wir können die  $\varphi_i$  als Charaktere  $\varphi : L^\times \rightarrow M^\times$  auffassen.

Wir studieren nun die Galoistheorie von Wurzelenerweiterungen. Sei  $K$  ein Körper und  $n$  eine natürliche Zahl, die nicht von  $\text{char}(K)$  geteilt wird (dies gilt immer, wenn  $\text{char}(K) = 0$ ).

**Definition 20.4** Sei  $a \in K^\times$  und  $b$  eine Nullstelle des Polynoms

$$X^n - a$$

in einem Erweiterungskörper  $K'$  von  $K$  (zum Beispiel  $K'$  der Zerfällungskörper von  $X^n - a$  oder  $K' = \overline{K}$  der algebraische Abschluss von  $K$ ). Dann heißt  $b$  eine  $n$ -te Wurzel von  $a$  (Bezeichnung:  $b = \sqrt[n]{a}$ ) (in  $L$ ).

**Satz 20.5**  $K$  enthalte eine primitive  $n$ -te Einheitswurzel, d.h., die Gruppe  $\mu_n$  alle  $n$ -ten Einheitswurzeln in  $\overline{K}$  sei in  $K$  enthalten. Sei  $\sqrt[n]{a}$  ein  $n$ -te Wurzel von  $a \in K^\times$  in einer Erweiterung  $K'/K$ . Dann ist  $K(\sqrt[n]{a})/K$  zyklisch (d.h., galoissch mit zyklischer Galoisgruppe) und  $[K(\sqrt[n]{a}) : K] = (\text{Gal}(K(\sqrt[n]{a})/K) : 1)$  ist ein Teiler von  $n$ . Genauer gilt: Die Abbildung

$$\begin{aligned} \chi : \text{Gal}(K(\sqrt[n]{a})/K) &\rightarrow \mu_n \\ \sigma &\mapsto \frac{\sigma(\sqrt[n]{a})}{\sqrt[n]{a}} \end{aligned}$$

ist ein injektiver Gruppenhomomorphismus.

**Beweis** Sei  $\beta = \sqrt[n]{a}$ . Jede weitere Nullstelle  $\beta'$  von  $X^n - a$  in  $\overline{K}$  ist von der Form  $\beta' = \beta \cdot \zeta$  mit  $\zeta \in \mu_n$ , denn es gilt  $(\beta')^n = a = \beta^n$ , also  $(\beta'/\beta)^n = 1$ , d.h.,  $\beta'/\beta \in \mu_n$ . Wegen  $\mu_n \subseteq K$  ist also  $K(\beta)$  bereits der Zerfällungskörper von  $f(X) = X^n - a$  über  $K$ . Weiter ist  $f$  wegen  $\text{char}(K) \nmid n$  separabel, da  $f$  und  $f' = nX^{n-1}$  teilerfremd sind. Dies zeigt, dass  $K(\beta)$  galoissch über  $K$  ist (als Zerfällungskörper eines separablen Polynoms). Betrachte die obige Abbildung

$$\begin{aligned} \chi : G := \text{Gal}(K(\beta)/K) &\rightarrow \mu_n \\ \sigma &\mapsto \sigma(\beta)/\beta. \end{aligned}$$

$\chi$  ist wohldefiniert, denn es ist  $(\sigma(\beta))^n = \sigma(\beta^n) = \sigma(a) = a$ , also  $\sigma(\beta)$  auch eine  $n$ -te Wurzel aus  $a$ , also  $\sigma(\beta)/\beta \in \mu_n$  (siehe oben). Weiter ist  $\chi$  ein Homomorphismus: Für  $\sigma, \tau \in G$  gilt

$$\chi(\sigma\tau) = \frac{(\sigma\tau)(\beta)}{\beta} = \frac{\sigma(\beta)}{\beta} \cdot \frac{\sigma(\tau(\beta))}{\sigma(\beta)} = \frac{\sigma(\beta)}{\beta} \cdot \sigma\left(\frac{\tau(\beta)}{\beta}\right) = \frac{\sigma(\beta)}{\beta} \cdot \frac{\tau(\beta)}{\beta} = \chi(\sigma)\chi(\tau)$$

denn es ist  $\zeta = \frac{\tau(\beta)}{\beta} \in \mu_n \subseteq K$  nach Voraussetzung, also  $\sigma(\zeta) = \zeta$ . Schließlich ist  $\chi$  injektiv, denn für  $\sigma(\beta) = \beta$  operiert  $\sigma$  trivial auf  $K(\beta)$ , ist also gleich  $1 \in G$ .

**Bemerkungen 20.6** (a) Ist  $\beta'$  eine andere  $n$ -te Wurzel von  $a$  (in  $\overline{K}$ ), so ist der Homomorphismus

$$\begin{aligned} \tilde{\chi} : G &\rightarrow \mu_n \\ \sigma &\mapsto \sigma(\beta')/\beta' \end{aligned}$$

gleich  $\chi$ , denn es ist  $\beta' = \beta \cdot \zeta$  für ein  $\zeta \in \mu_n \subseteq K$ , also  $\sigma(\beta') = \sigma(\beta \cdot \zeta) = \sigma(\beta) \cdot \zeta$ , d.h.,

$$\frac{\sigma(\beta')}{\beta'} = \frac{\sigma(\beta)}{\beta}.$$

Der Homomorphismus

$$\begin{aligned} \chi : G &\rightarrow \mu_n \\ \sigma &\mapsto \frac{\sigma(\sqrt[n]{a})}{\sqrt[n]{a}} \end{aligned}$$

hängt also nur von  $a$  (und nicht von der Wahl von  $\sqrt[n]{a}$ ) ab und wird auch als der Kummer-Charakter zu  $a$  (Bez.  $\chi_a$ ) bezeichnet. Beachte: Wir können  $\chi_a$  vermöge der Inklusion  $\mu_n \subseteq K^\times$  auch als Charakter von  $G$  mit Werten in  $K$  auffassen.

(b) Da die Ordnung von  $G$  die Zahl  $n$  teilt, hat jeder Charakter  $\chi : G \rightarrow K^\times$  Bild in  $\mu_n$  (für  $\sigma \in G$  ist  $(\chi(\sigma))^n = \chi(\sigma^n) = \chi(1) = 1$ , also  $\chi(\sigma) \in \mu_n$ ).

Wir zeigen nun, dass umgekehrt jede zyklische Erweiterung  $L/K$  mit  $[L : K] = n$  auf die obige Weise, d.h., durch Ziehen einer  $n$ -ten Wurzel entsteht, falls  $\mu_n \in K$ .

**Satz 20.7** Sei  $K$  ein Körper und  $n \in \mathbb{N}$  mit  $\text{char}(K) \nmid n$ . Weiter enthalte  $K$  eine primitive  $n$ -te Einheitswurzel. Ist dann  $L/K$  eine Galoiserweiterung vom Grad  $n$  mit zyklischer Galoisgruppe  $G$ , so gibt es ein  $b \in L^\times$  mit  $a := b^n \in K^\times$  und  $L = K(b)$  (so dass also  $L = K(\sqrt[n]{a})$  für die  $n$ -te Wurzel  $\sqrt[n]{a} = b$ ).

**Beweis** Sei  $\zeta \in K$  eine primitive Einheitswurzel und  $\sigma \in G$  ein Erzeugendes. Dann sind  $1, \sigma, \sigma^2, \dots, \sigma^{n-1} : L \rightarrow L$  paarweise verschieden, nach Corollar 20.3 also linear unabhängig über  $L$ . Es ist also insbesondere

$$id + \zeta\sigma + \zeta^2\sigma^2 + \dots + \zeta^{n-1}\sigma^{n-1} \neq 0,$$

d.h., es gibt ein  $x \in L$  mit

$$b := x + \zeta\sigma(x) + \zeta^2\sigma^2(x) + \dots + \zeta^{n-1}\sigma^{n-1}(x) \neq 0.$$

Es folgt

$$0 \neq \sigma(b) = \sigma(x) + \zeta\sigma^2(x) + \dots + \zeta^{n-1}x = \zeta^{-1} \cdot b$$

(beachte  $\sigma(\zeta) = \zeta$ ,  $\sigma^n = id$  und  $\zeta^n = 1$ ). Damit ist

$$\sigma(b^n) = \sigma(b)^n = (\zeta^{-1}b)^n = b^n,$$

also  $a := b^n \in L^G = K$  nach Galoistheorie. Es bleibt noch zu zeigen:

*Behauptung:*  $L = K(b)$ .

*Beweis:* Wegen  $\sigma^i(b) = \zeta^{-i} \cdot b$  sind die Einschränkungen von  $id, \sigma, \sigma^2, \dots, \sigma^{n-1}$  auf  $K(b)$  paarweise verschieden, also  $(Gal(K(b)/K) : 1) = [K(b) : K] \geq n$ . Andererseits ist  $[K(b) : K] \leq [L : K] = n$ . Es folgt  $L = K(b)$  wie behauptet.

## §21 Auflösungen von Gleichungen durch Wurzeln

(in der Vorlesung nur skizziert)

Sei  $K$  ein Körper der Charakteristik 0. Eine quadratische Gleichung

$$X^2 + pX + q = 0$$

lässt sich im algebraischen Abschluss  $\overline{K}$  von  $K$  durch die quadratische Lösungsformel lösen:

$$X = -\frac{p}{2} \pm \frac{\sqrt{p^2 - 4q}}{2},$$

also durch Adjunktion von geeigneten Quadratwurzeln. Nach S. del Ferro (Tartaglia)/G. Cardano sowie L. Ferrari kann man auch kubische Gleichungen

$$X^3 + bX^2 + cX + d = 0$$

und Gleichungen 4. Grades

$$X^4 + bX^3 + cX^2 + dX + e = 0$$

durch sukzessives Ziehen von Wurzeln (2. und 3. Ordnung) lösen, mit expliziten (aber komplizierten) Lösungsformeln.

Es wurde lange versucht, auch Gleichungen höheren Grades durch iteratives Wurzelziehen zu lösen, bis dann durch Galoistheorie bewiesen wurde, dass dies im Allgemeinen nicht geht. Dies beruht auf den folgenden Resultaten.

**Definition 21.1** Eine Erweiterung  $L/K$  heißt Radikalerweiterung, wenn es Zwischenkörper

$$K = L_0 \subseteq L_1 \subseteq L_2 \subseteq \dots \subseteq L_r = L$$

gibt, so dass  $L_i = L_{i-1}(\sqrt[n_i]{a_i})$  für  $i = 1, \dots, r$ , wobei  $n_i \in \mathbb{N}$  und  $a_i \in L_{i-1}$ .

Offenbar erhält man für eine Polynomgleichung  $f(X) = 0$  genau dann alle Lösungen durch wiederholtes Wurzelziehen, wenn der Zerfällungskörper in einer Radikalerweiterung liegt.

**Beispiel 21.2** In der Lösungsformel für die Gleichung

$$x^3 + 3pX + 2q = 0$$

(auf die man eine kubische Gleichung immer transformieren kann) kommen zum Beispiel primitive dritte Einheitswurzeln  $\zeta$  und Ausdrücke wie

$$\sqrt[3]{-q + \sqrt{q^2 + p^3}}$$

vor. Diese liegen in der Radikalerweiterung

$$L_0 = K \subseteq L_1 = K(\zeta) \subseteq L_2 = L_1(\sqrt{q^2 + p^3}) \subseteq L_3 = L_2(\sqrt[3]{\alpha}),$$

mit  $\alpha = -q + \sqrt{q^2 + p^3} \in L_2$ .

**Lemma 21.3** Ist  $L/K$  eine Radikalerweiterung, so gibt es eine Radikalerweiterung  $M/L$  so dass  $M/K$  galoissch ist. (Beachte: Insbesondere ist  $M/K$  Radikalerweiterung).

**Beweis** Alle Körper seien in einem festen algebraischen Abschluss betrachtet. Sei

$$K = L_0 \subseteq L_1 \subseteq \dots \subseteq L_{n-1} \subseteq L_n = L$$

so dass  $L_i = L_{i-1}(\sqrt[n_i]{a_i})$  mit  $n_i \in \mathbb{N}$  und  $a_i \in L_{i-1}$ . Wir führen Induktion über  $n$ , wobei der Induktionsanfang mit  $n = 0$  trivial ist. Ist  $n > 0$  und die Aussage schon für  $n - 1$  bewiesen, so gibt es eine Radikalerweiterung  $M_1/L_{n-1}$ , so dass  $M_1/K$  galoissch ist. Wir erhalten Inklusionen

$$\begin{array}{ccccccc} M_1 & \subseteq & M_2 & = & M_1(\sqrt[m]{a}) \\ \cup & & \cup & & \\ K = L_0 & \subseteq & L_{n-1} & \subseteq & L_n & = & L_{n-1}(\sqrt[m]{a}), \end{array}$$

wobei  $m := m_n$  und  $a = a_n \in L_{n-1}$  und wobei  $M_2$  sowohl  $M_1$  als auch  $L_n$  enthält und eine Radikalerweiterung von  $M_1$  ist. Weiter können wir annehmen, dass  $M_1$  eine primitive  $m$ -te Einheitswurzel  $\zeta$  enthält, denn sonst können wir  $M_1$  durch  $M_1(\zeta)$  ersetzen; dieser Körper ist dann als Kompositum der galoisschen Erweiterungen  $M_1/K$  und  $K(\zeta)/K$  wieder galoissch über  $K$  (siehe folgendes Lemma). Betrachte nun das Polynom

$$g(x) = \prod_{\sigma \in \text{Gal}(M_1/K)} (X^m - \sigma(a))$$

Man sieht, dass für alle  $\tau \in \text{Gal}(M_1/K)$  gilt  $\tau(g) = g$ , also ist  $g \in K[X]$ . Da  $M_1/K$  galoissch ist, gibt es ein Polynom  $f \in K[X]$ , so dass  $M_1$  der Zerfällungskörper von  $f$

über  $K$  ist. Sei  $M$  der Zerfällungskörper von  $f \cdot g$  über  $K$ . Dann ist  $M/K$  galoissch und enthält offenbar  $M_2$  und  $M_1$ . Weiter ist  $M$  der Zerfällungskörper von  $g$  über  $M_1$  (da  $f$  über  $M_1$  schon in Linearfaktoren zerfällt), also auch von  $g$  über  $M_2$ . Wegen der Form von  $g$  sehen wir, dass  $M/M_2$  Radikalerweiterung ist. Da dies auch für  $M_2/L_n$  gilt, ist  $M/L_n$  Radikalerweiterung.

**Lemma 21.4** Seien  $E/K$  und  $E'/K$  endliche Galoisweiterungen.

(a) Dann ist  $E \cdot E'/K$  endlich galoissch und der Homomorphismus

$$\begin{aligned} \varphi : Gal(E \cdot E'/E) &\rightarrow Gal(E'/E \cap E') \\ \sigma &\mapsto \sigma|_{E'} \end{aligned}$$

ein Isomorphismus.

(b) Der Homomorphismus

$$\begin{aligned} \psi : Gal(E \cdot E'/K) &\rightarrow Gal(E/K) \times Gal(E'/K) \\ \sigma &\mapsto (\sigma|_E, \sigma|_{E'}) \end{aligned}$$

ist injektiv.

**Beweis** (a): Ist  $E$  (bzw.  $E'$ ) Zerfällungskörper des separablen Polynoms  $f$  (bzw.  $f'$ ), so ist  $E \cdot E'$  Zerfällungskörper des Polynoms  $f \cdot f'$  über  $K$ , also normal über  $K$ , und Zerfällungskörper des Polynoms  $f'$  über  $E$ , also separabel über  $E$ , also auch über  $K$ , da  $E/K$  separabel ist. Damit ist  $E \cdot E'/K$  endlich galoissch. Weiter ist  $\varphi$  injektiv, denn für  $\sigma \in Gal(E \cdot E'/E)$  gilt  $\sigma|_E = id$  und für  $\sigma \in \ker(\varphi)$  gilt zusätzlich  $\sigma|_{E'} = id$ , so dass  $\sigma$  trivial auf allen Elementen in  $E \cdot E'$  operiert, also  $\sigma = id$ . Für die Surjektivität von  $\varphi$  betrachte die offensichtliche Beziehung

$$(E')^{im(\varphi)} = (E \cdot E')^{Gal(E \cdot E'/E)} \cap E' = E \cap E',$$

woraus nach Galoistheorie  $im(\varphi) = Gal(E'/E \cap E')$  folgt.

(b): Die Injektivität von  $\psi$  folgt wie im Beweis von (a).

**Definition 21.5** Sei  $G$  eine Gruppe.

(a) Eine Kette von Untergruppen

$$G_n = 1 \subseteq G_{n-1} \subseteq \dots \subseteq G_0 = G$$

heißt *Normalreihe* von  $G$ , wenn jeweils  $G_{i+1}$  Normalteiler in  $G_i$  ist. Die Faktorgruppen  $G_i/G_{i+1}$  heißen die Faktoren der Normalreihe.

(b) Eine Gruppe heißt *auflösbar*, wenn sie eine Normalreihe mit abelschen Faktoren besitzt.

**Lemma 21.6** Ist eine endliche Gruppe  $G$  auflösbar, so besitzt sie eine Normalreihe, deren Faktoren zyklisch von Primzahlordnung sind.

**Beweis** Durch Induktion über die Länge  $n$  der Kompositionsreihe.

1. *Schritt:* Ist  $G$  abelsch, so führen wir Induktion über die Gruppenordnung. Ist  $G$  zyklisch von Primzahlordnung, so sind wir fertig. Andernfalls gibt es eine zyklische Untergruppe  $\langle a \rangle \subseteq G$  und darin eine zyklische Untergruppe  $C$  von Primzahlordnung (Theorie der zyklischen Gruppen). Da  $G$  abelsch ist, ist  $C$  ein Normalteiler. Nach Voraussetzung ist  $C \neq G$ , also  $G/C$  von kleinerer Ordnung als  $G$ . Nach Induktionsvoraussetzung gibt es dann eine Normalreihe

$$1 = \overline{G}_r \subseteq \overline{G}_{r-1} \subseteq \dots \subseteq \overline{G}_0 = G/C$$

mit zyklischen Faktoren von Primzahlordnung. Dann ist

$$1 = G_{r+1} \subseteq C = G_r \subseteq G_{r-1} \subseteq \dots \subseteq G_0 = G,$$

mit  $G_i = \pi^{-1}(\overline{G}_i)$  für  $\pi : G \rightarrow G/C$  und  $i = 0, \dots, r$  eine Normalreihe wie gewünscht für  $G$ , weil  $G_i/G_{i+1} \cong \overline{G}_i/\overline{G}_{i+1}$  nach dem zweiten Isomorphiesatz.

2. *Schritt:* Sei nun  $G$  nicht abelsch und

$$1 = G_n \subsetneq G_{n-1} \subsetneq \dots \subsetneq G_0 = G$$

eine Normalreihe mit abelschen Faktoren. Nach dem ersten Schritt besitzt  $G/G_1$  eine Normalreihe

$$1 = \overline{G}_r \subseteq \overline{G}_{r-1} \subseteq \dots \subseteq \overline{G}_0 = G/G_1$$

deren Faktoren zyklisch von Primzahlordnungen sind. Nach Induktionsvoraussetzung besitzt weiter  $G_1$  eine Normalreihe

$$1 = G'_s \subseteq G'_{s-1} \subseteq \dots \subseteq G'_r = G_1$$

mit primzyklischen Faktoren. Für  $\pi : G \rightarrow G/G_1$  und  $G'_i = \pi^{-1}(\overline{G}_i)$  für  $i = 0, \dots, r$  ist dann

$$1 = G'_s \subseteq \dots \subseteq G'_r \subseteq \dots \subseteq G'_0 = G_0 = G$$

eine Normalreihe wie gewünscht.

**Lemma 21.7** (a) Sei  $G$  eine Gruppe und  $H \leq G$  eine Untergruppe. Ist  $G$  auflösbar, so auch  $H$ .

(b) Ist  $H$  ein Normalteiler, so ist  $G$  genau dann auflösbar, wenn  $H$  und  $G/H$  auflösbar sind.

**Beweis** (a): Ist  $\{G_i\}$  eine Normalreihe von  $G$  mit abelschen Faktoren, so  $\{G_i \cap H\}$  eine solche Normalreihe für  $H$ , denn es ist  $G_{i+1} \cap H$  normal in  $G_i \cap H$ , und der Homomorphismus

$$G_i \cap H / G_{i+1} \cap H \rightarrow G_i / G_{i+1}$$

ist injektiv; mit  $G_i/G_{i+1}$  ist also auch der linke Quotient abelsch.

(b) Sei nun  $H$  ein Normalteiler. Für  $G/H$  ist dann  $\{G_i H / H\}$  eine Normalreihe und die Isomorphie/Surjektion

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

zeigt, dass die zugehörigen Faktoren abelsch sind.

Sind umgekehrt  $H$  und  $G/H$  auflösbar und

$$\begin{aligned} 1 = H_m &\subseteq \dots \subseteq H_0 = H \\ 1 = \overline{G}_n &\subseteq \dots \subseteq \overline{G}_0 = G/H \end{aligned}$$

Normalreihen mit abelschen Faktoren, so gilt für die Urbilder  $G'_i$  der  $\overline{G}_i$  in  $G$ , dass

$$1 = Hm \subseteq \dots \subseteq H_0 = H = G'n \subseteq \dots \subseteq G'_0 = G$$

eine Normalreihe mit abelschen Faktoren für  $G$  ist.

**Satz 21.8** Sei  $L/K$  eine endliche Galoiserweiterung. Dann ist  $L/K$  genau dann in einer Radikalerweiterung enthalten, wenn die Galoisgruppe  $G = Gal(L/K)$  auflösbar ist.

**Beweis** Sei  $L/K$  in einer Radikalerweiterung enthalten. Nach 21.3 gibt es dann eine Erweiterung  $M/L$ , so dass  $M/K$  eine galoissche Radikalerweiterung ist. Seien

$$K = M_0 \subseteq M_1 \subseteq \dots \subseteq M_n = M$$

Körper, so dass  $M_i = M_{i-1}(\sqrt[m_i]{a_i})$  mit  $m_i \in \mathbb{N}$  und  $a_i \in M_{i-1}$ . Sei  $m = \prod_{i=1}^n m_i \in \mathbb{N}$  und  $\zeta$  eine primitive  $m$ -te Einheitswurzel. Wir erhalten Körper

$$\begin{array}{ccccccc} M'_0 & \subseteq & M'_1 & \subseteq & \dots & \subseteq & M'_n =: M' \\ \cup & & \cup & & & & \cup \\ K & = & M_0 & \subseteq & M_1 & \subseteq & \dots & \subseteq & M_n = M, \end{array}$$

wobei  $M'_i = M_i(\zeta)$ . Dann ist  $M'/K$  wieder galoissch (Lemma 21.4, als Kompositum von  $M/K$  und  $M'_0/K$ ) und eine Radikalerweiterung. Sei  $i \geq 1$ . Wegen  $\zeta \in M'_{i-1}$  enthält  $M'_{i-1}$  eine primitive  $m_{i-1}$ -te Einheitswurzel, und nach Kummertheorie ist die Erweiterung  $M'_i/M'_{i-1} = M'_{i-1}(\sqrt[m_i]{a_i})/M'_{i-1}$  galoissch mit zyklischer Galoisgruppe. Setzen wir  $G'_i = Gal(M'/M'_{i-1})$ , mit  $M'_{-1} := K$ , so erhalten wir Untergruppen

$$1 = G'_{n+1} \subseteq G'_n \subseteq \dots \subseteq G'_1 \subseteq G'_0 = G' = Gal(M'/K)$$

wobei nach dem Hauptsatz der Galoistheorie 12.3, Teil (f) (angewendet auf den Zwischenkörper  $M'_i$  von  $M/M'_{i-1}$ )  $G'_{i+1}$  normal in  $G'_i$  ist mit zyklischem Quotienten, da  $M'_i/M'_{i-1}$  galoissch zyklisch ist. Also ist  $G'$  auflösbar, also nach Lemma 21.7 auch die Faktorgruppe  $G = Gal(L/K) = G'/Gal(M'/L)$  ( $Gal(M'/L)$  ist Normalteiler, da  $L/K$  galoissch ist).

Sei umgekehrt  $G$  auflösbar und  $n = [L : K]$ . Sei  $K' = K(\zeta_n)$  für eine primitive  $n$ -te Einheitswurzel  $\zeta_n$ , und es sei  $L' = K' \cdot L = L(\zeta)$ . Dann ist

$$(21.8.1) \quad G' := Gal(L'/K') \xrightarrow{\sim} Gal(L/L \cap K) \hookrightarrow Gal(L/K) = G$$

nach 21.4 (a). Nach 21.7 (a) ist  $G'$  dann wieder auflösbar, besitzt also nach 21.6 eine Normalreihe

$$1 = G'_m \subseteq G'_{m-1} \subseteq \dots \subseteq G'_0 = G'$$

mit zyklischen Quotienten  $G'_{i-1}/G'_i$ . Sei  $L'_i = L'^{G'_i}$ , so dass  $L'_m = L'$  und  $L'_0 = K'$ . Nach Galoistheorie ist dann  $G'_i = \text{Gal}(L'/L'_i)$  und  $L'_i/L'_{i-1}$  galoissch mit zyklischer Galoisgruppe  $G'_{i-1}/G'_i$ . Weiter teilt  $m_i = [L'_i : L'_{i-1}]$  den Grad  $[L' : K']$ , also auch  $[L : K] = n$  nach (21.8.1). Wegen  $\zeta_n \in K'$  folgt nach Kummertheorie, dass  $L'_i = L'_{i-1}(\sqrt[m_i]{a_i})$  für ein  $a_i \in L'_{i-1}$  ist. Damit ist  $L'/K'$  offenbar eine Radikalerweiterung und  $L'/K$  in der Radikalerweiterung  $L'/K$  enthalten.

Mit der Bemerkung nach Definition 21.1 folgt:

**Corollar 21.9** Eine Polynomgleichung  $f(X) = 0$  über  $K$  ist genau dann durch Radikale (d.h., durch sukzessives Wurzelziehen) lösbar, wenn die Galoisgruppe von  $f$  auflösbar ist.

Denn nach Definition ist die Galoisgruppe von  $f$  die Galoisgruppe des Zerfällungskörpers von  $f$  über  $K$ .

**Satz 21.10** Es gibt für  $n \geq 5$  Gleichungen  $n$ -ten Grades, die nicht durch Radikale (d.h., sukzessives Wurzelziehen) auflösbar sind.

**Beweis** Sei  $k$  ein Körper der Charakteristik 0 und  $L = k(X_1, \dots, X_n)$  der rationale Funktionenkörper in  $n$  Variablen. Dann operiert die symmetrische Gruppe  $S_n$  auf  $L$  durch Permutation der  $X_i$ . Insbesondere operiert auch die Untergruppe  $A_n \leq S_n$  auf  $L$ . Sei  $K = L^{A_n}$  der Fixkörper. Nach 12.7 ist dann  $L/K$  galoissch mit Galoisgruppe  $A_n$ . Das Polynom  $n$ -ten Grades

$$f(X) = \prod_{i=1}^n (X - X_i)$$

hat Koeffizienten in  $K$ , da  $\sigma f = f$  für alle  $\sigma \in A_n$  (sogar alle  $\sigma \in S_n$ ). Genauer ist

$$f(X) = \sum_{i=0}^n (-1)^i s_i(X_1, \dots, X_n) X^{n-i}$$

wobei  $s_i \in K$  die *elementarsymmetrischen* Polynome in  $X_1, \dots, X_n$  sind ( $s_0 = 1, s_1 = X_1 + \dots + X_n, \dots$ ).

$L$  ist der Zerfällungskörper von  $f(X)$  und die Galoisgruppe von  $f(X)$  ist  $\text{Gal}(L/K) = A_n$ . Nach Satz 19.9 ist  $A_n$  für  $n \geq 5$  einfach und nicht-abelsch, also nicht auflösbar. Daher ist die Gleichung  $f(X) = 0$  nicht durch Radikale auflösbar.

**Bemerkungen 21.11** (a) Das obige Polynom nennt man auch das “allgemeine Polynom  $n$ -ten Grades”, da man die Nullstellen als freie Variablen gewählt hat (Jedes Polynom  $n$ -ten Grades über einen Körper  $K$  erhält man, indem man bestimmte Werte in algebraischen Abschluss  $\bar{K}$  für die  $X_i$  einsetzt – nämlich die Nullstellen von  $f$ ). Man kann also sagen, dass für  $n \geq 5$  das allgemeine Polynom  $n$ -ten Grades nicht durch Radikale auflösbar ist. Dies schliesst ein solches Lösungsverfahren ganz allgemein aus.

(b) Es gibt auch Polynome  $f$   $n$ -ten Grades über  $\mathbb{Q}$  für  $n \geq 5$ , deren Galoisgruppe  $S_n$  oder auch  $A_n$  ist. Dann ist  $f(X) = 0$  auch nicht durch Radikale auflösbar.