

# Klassische Algebra

Udo Hebisch

SS 2002

Dieses Skript enthält nur den “roten Faden”  
des zweiten Teils der Vorlesung. Zur selben Vorlesung  
gehört noch ein Teil zur Gruppentheorie.

Wesentliche Inhalte werden ausschließlich  
in der Vorlesung vermittelt. Daher ist dieses  
Skript nicht zum Selbststudium gedacht, sondern  
nur als “Erinnerungsstütze”.

# 1 Konstruierbarkeit mit Zirkel und Lineal

Es sei  $M \subseteq \mathbb{R}^2 = \mathbb{C}$  mit  $|M| \geq 2$  eine Menge von Punkten der Ebene.

$\mathcal{G}(M) =$  Menge der Geraden, die zwei verschiedene Punkte aus  $M$  enthalten

$\mathcal{K}(M) =$  Menge der Kreise, deren Mittelpunkt in  $M$  liegt und deren Radius gleich dem Abstand zweier Punkte aus  $M$  ist

$\langle M \rangle = \{P \in \mathbb{R}^2 \mid P \text{ ist mit Zirkel und Lineal aus } M \text{ konstruierbar}\}$

Dabei entstehen alle  $P \in \langle M \rangle$  rekursiv aus  $M$  durch endlich viele *elementare Konstruktionen* für “neue” Punkte aus  $\langle M \rangle$ :

1. Schnittpunkt von  $g_1 \neq g_2$  aus  $\mathcal{G}(\langle M \rangle)$
2. Schnittpunkt von  $g \in \mathcal{G}(\langle M \rangle)$  und  $k \in \mathcal{K}(\langle M \rangle)$
3. Schnittpunkt von  $k_1 \neq k_2$  aus  $\mathcal{K}(\langle M \rangle)$

## Vier Konstruktionsprobleme der Antike

a) *Quadratur des Kreises*

Zu einem gegebenen Kreis soll ein Quadrat gleichen Flächeninhalts konstruiert werden. Seien dazu  $P, Q, X$  Punkte auf einer Geraden mit  $\overline{PQ} = r$  und  $\overline{PX} = r\sqrt{\pi}$ .

Gilt dann  $X \in \langle \{P, Q\} \rangle$ ?

b) *Delisches Problem (Würfelverdopplung)*

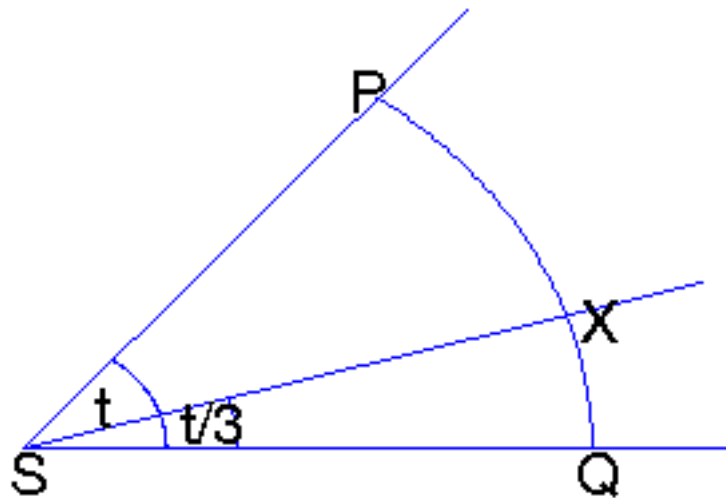
Zu einem gegebenen Würfel der Kantenlänge  $a$  ist ein Würfel mit doppeltem Volumen gesucht. Seien dazu  $P, Q, X$  Punkte auf einer Geraden mit  $\overline{PQ} = a$  und  $\overline{PX} = a\sqrt[3]{2}$ .

Gilt dann  $X \in \langle \{P, Q\} \rangle$ ?

c) *Winkeldreiteilung*

Zu einem (durch seinen Scheitelpunkt  $S$  und zwei Punkte  $P, Q$  auf seinen Schenkeln) gegebenen Winkel  $t$  soll der Winkel  $t/3$  (durch einen Punkt  $X$  auf seinem zweiten Schenkel) konstruiert werden.

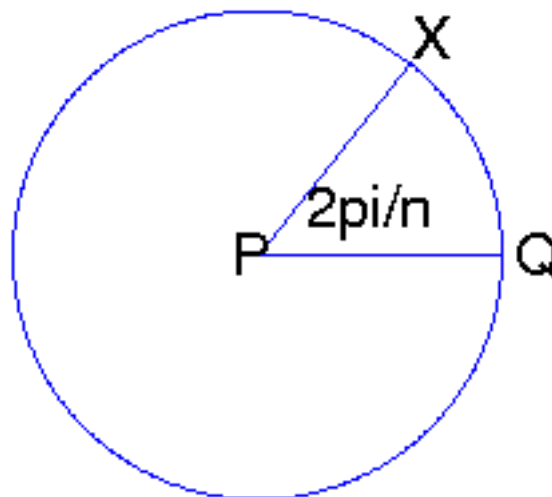
Gilt also  $X \in \langle \{S, P, Q\} \rangle$ ?



d) *Konstruktion des regelmäßigen  $n$ -Ecks*

Zu einem gegebenen Kreis mit Mittelpunkt  $P$  und einem Punkt  $Q$  auf dem Kreis sei  $X$  der Punkt auf dem Kreis mit  $\angle(X, P, Q) = 2\pi/n$ .

Für welche  $n \in \mathbb{N}$  gilt dann  $X \in \langle\{P, Q\}\rangle$ ?



Die Bedingung  $|M| \geq 2$  für  $M \subseteq \mathbb{R}^2 = \mathbb{C}$  läuft durch geeignete Wahl der reellen und imaginären Achse in  $\mathbb{C}$  und die Wahl eines Maßstabes auf die Bedingung  $0, 1 \in M \subseteq \mathbb{C}$  hinaus.

**Lemma 1.1** *Für  $M \subseteq \mathbb{C}$  mit  $0, 1 \in M$  gelten:*

[Vorherige Seite](#) [Nächste Seite](#) [Zurück](#) [Erste Seite](#) [Letzte Seite](#)

- (1)  $i \in \langle M \rangle$ ,
- (2)  $z \in \langle M \rangle \implies \operatorname{Re}(z), \operatorname{Im}(z) \in \langle M \rangle$ ,
- (3)  $z \in \langle M \rangle \implies -z \in \langle M \rangle$ ,
- (4)  $z_1, z_2 \in \langle M \rangle \implies z_1 + z_2 \in \langle M \rangle$ ,
- (5)  $z \in \langle M \rangle \implies \bar{z} \in \langle M \rangle$ ,
- (6)  $z_1, z_2 \in \langle M \rangle \implies z_1 \cdot z_2 \in \langle M \rangle$ ,
- (7)  $z \in \langle M \rangle, z \neq 0 \implies \frac{1}{z} \in \langle M \rangle$ .

Also ist  $\langle M \rangle$  ein Unterkörper von  $\mathbb{C}$ , der offensichtlich  $\mathbb{Q}$  enthält. Man nennt ihn den **Körper** der aus  $M$  konstruierbaren Zahlen.

**Beweis:**

(1) Wegen  $0, 1 \in M$  liegt die reelle Achse in  $\mathcal{G}(M)$  und der Einheitskreis in  $\mathcal{K}(M)$ . Also liegt der Schnittpunkt  $-1$  in  $\langle M \rangle$ . Eine elementare Konstruktion liefert die imaginäre Achse als Mittelsenkrechte auf der Strecke  $[-1, 1]$ . Einer ihrer Schnittpunkte mit dem Einheitskreis ist dann  $i \in \langle M \rangle$ .

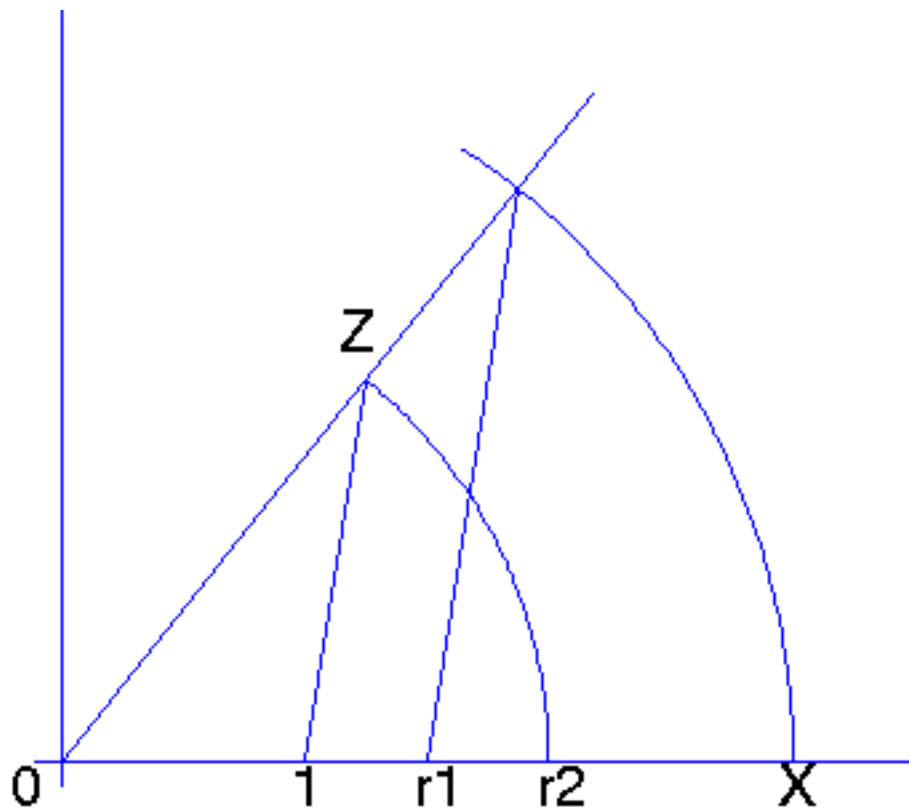
(2) Die Lote von  $z$  auf die reelle bzw. imaginäre Achse lassen sich durch elementare Konstruktionen bestimmen. Ihre Schnittpunkte mit den beiden Achsen liefern  $\operatorname{Re}(z), \operatorname{Im}(z)i \in \langle M \rangle$ . Der Kreis um  $0$  vom Radius  $|\operatorname{Im}(z)i|$  schneidet die reelle Achse in  $\operatorname{Im}(z)$ .

(3) Der Schnittpunkt des Kreises um  $0$  vom Radius  $|z|$  mit der Geraden durch  $0$  und  $z$  ist  $-z$ .

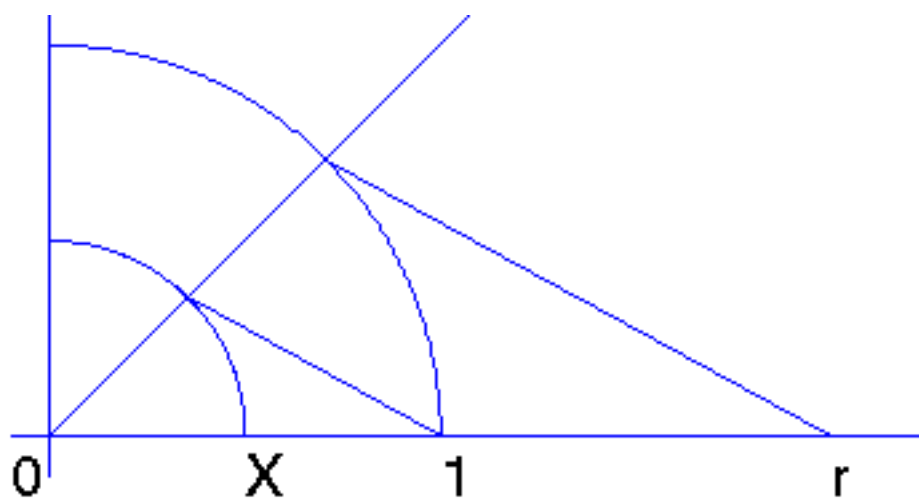
(4) Der vierte Eckpunkt des durch  $0, z_1$  und  $z_2$  bestimmten Parallelogramms ist  $z_1 + z_2$ .

(5) Wegen  $\bar{z} = \operatorname{Re}(z) - \operatorname{Im}(z)i$  folgt dies aus (2), (3) und (4).

(6) Wegen  $z_1 z_2 = (a_1 a_2 - b_1 b_2) + (a_1 b_2 + a_2 b_1)i$  und (1) - (5) genügt es, die Behauptung für alle positiven reellen Zahlen  $r_1$  und  $r_2$  zu zeigen. In der folgenden Konstruktion ist  $z$  der Schnittpunkt der Winkelhalbierenden (Gerade durch  $0$  und  $1 + i$  aus  $\langle M \rangle$ ) mit dem Kreis um  $0$  vom Radius  $r_2$ . Zu der Geraden durch  $1$  und  $z$  wird die Parallele durch  $r_1$  konstruiert und mit der Winkelhalbierenden geschnitten. Der Kreis um  $0$  durch diesen Schnittpunkt habe den Radius  $x$ . Dann gilt nach dem Strahlensatz  $x : r_2 = r_1 : 1$ , also  $x = r_1 r_2$ .



(7) Wegen  $\frac{1}{z} = \bar{z}/(z\bar{z})$  und (5), (6) genügt es, die Behauptung für positive reelle Zahlen  $r$  zu zeigen. In der folgenden Konstruktion gilt nach dem Strahlensatz  $1 : r = x : 1$ , also  $x = 1/r \in \langle M \rangle$ .

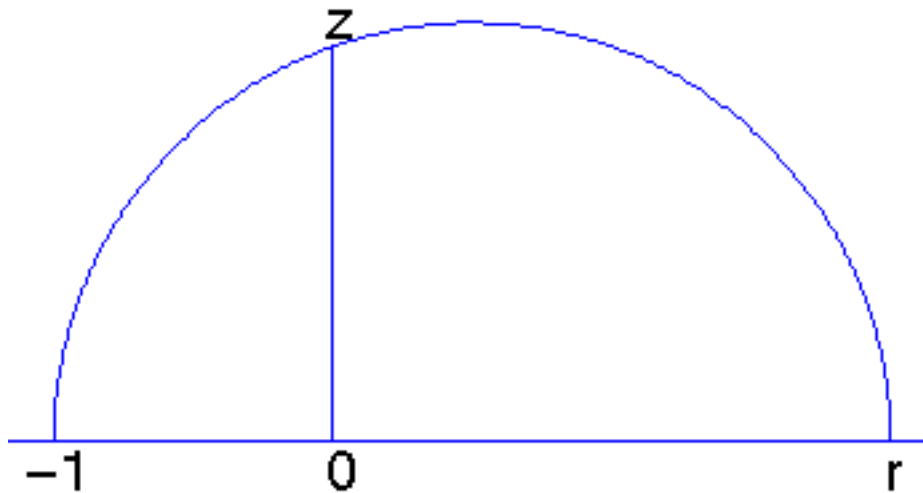


**Lemma 1.2** Der Körper  $\langle M \rangle$  ist quadratisch abgeschlossen, d. h. für alle  $z \in \mathbb{C}$  gilt

$$(8) \quad z \in \langle M \rangle \implies \sqrt{z} \in \langle M \rangle.$$

**Beweis:**

Gelte  $w^2 = z = re^{it}$ , also  $w = \pm\sqrt{r}e^{it/2}$ . Da die Winkelhalbierende durch elementare Konstruktionen gewonnen werden kann, bleibt (8) für positive reelle Zahlen  $r$  zu zeigen. Hierzu konstruiert man über der Strecke  $[-1, r]$  den Thaleskreis und auf ihm den Lotpunkt  $z$  über 0. Dann gilt  $x = |z| \in \langle M \rangle$ . In dem rechtwinkligen Dreieck  $-1, z, r$  liefert der Höhensatz  $x^2 = 1 \cdot r$ , also  $x = \sqrt{r}$ .



**Definition 1.3** Eine Körpererweiterung  $E : K$  besteht aus einem (Erweiterungs-)Körper  $E$  und einem Unterkörper  $K$  von  $E$ . Jeder Körper  $F$  mit  $K \subseteq F \subseteq E$  heißt ein *Zwischenkörper* von  $E : F$ . Für  $A \subseteq E$  sei

$$(9) \quad K(A) = \bigcap \{F \mid F \text{ Zwischenkörper von } E : K \text{ und } A \subseteq F\}$$

der kleinste Unterkörper von  $E$ , der  $K$  und  $A$  enthält. Dann heißt  $K(A)$  der *von  $A$  über  $K$  erzeugte Unterkörper* von  $E$ . Man sagt auch,  $K(A)$  entsteht aus  $K$  durch *Adjunktion der Elemente* von  $A$  zu  $K$ . Für  $A = \{\alpha_1, \dots, \alpha_n\}$  schreibt man auch  $K(A) = K(\alpha_1, \dots, \alpha_n)$ .

**Beispiel 1.4** Für  $E = \mathbb{C}$ ,  $K = \mathbb{Q}$  und  $A = \{i\}$  ist  $\mathbb{Q}(i) = \{a + bi \mid a, b \in \mathbb{Q}\}$ .

Für  $0, 1 \in M \subseteq \mathbb{C}$  sei  $\overline{M} = \{\bar{z} \mid z \in M\}$  und

$$(10) \quad K = \mathbb{Q}(M \cup \overline{M}).$$

Dann gilt offensichtlich

$$(11) \quad \langle M \rangle = \langle K \rangle,$$

d. h. man darf  $M$  in den obigen Fragestellungen durch den Körper (10) ersetzen. Für diesen Körper gilt

$$(12) \quad \overline{K} = K.$$

**Lemma 1.5** *Es sei  $K$  ein Unterkörper von  $\mathbb{C}$  mit  $K = \overline{K}$ .*

- a) *Ist  $z$  Schnittpunkt zweier Geraden aus  $\mathcal{G}(K)$ , so gilt bereits  $z \in K$ .*
- b) *Ist  $z$  Schnittpunkt einer Geraden aus  $\mathcal{G}(K)$  mit einem Kreis aus  $\mathcal{K}(K)$ , so gilt*  
 (\*) *Es gibt ein  $w \in \mathbb{C}$  mit  $w^2 \in K$  und  $z \in K(w)$ .*
- c) *Ist  $z$  Schnittpunkt zweier Kreise aus  $\mathcal{K}(K)$ , so gilt ebenfalls (\*).*

**Definition 1.6** Sei  $E : K$  eine **Körpererweiterung**.

- a)  *$E$  entsteht aus  $K$  durch Adjunktion einer Quadratwurzel, wenn es ein  $w \in E$  mit  $w^2 \in K$  und  $E = K(w)$  gibt. Dann heißt  $w$  eine Quadratwurzel von  $v = w^2$  aus  $K$ , in Zeichen  $w = \sqrt{v}$ .*
- b)  *$E$  entsteht aus  $K$  durch sukzessive Adjunktion von Quadratwurzeln, falls es eine endliche Kette  $K = K_0 \subseteq K_1 \subseteq \dots \subseteq K_m = E$  von Unterkörpern  $K_i$  von  $E$  gibt, in der jeweils  $K_i$  aus  $K_{i-1}$  durch Adjunktion einer Quadratwurzel entsteht.*

**Satz 1.7** *Sei  $0, 1 \in M \subseteq \mathbb{C}$  und  $K = \mathbb{Q}(M \cup \overline{M})$ . Dann sind für alle  $z \in \mathbb{C}$  äquivalent:*

- (i)  $z \in \langle M \rangle$ .
- (ii) *Es existiert ein Unterkörper  $E$  von  $\mathbb{C}$ , der aus  $K$  durch sukzessive Adjunktion von Quadratwurzeln entsteht, mit  $z \in E$ .*

### Algebraische Formulierung der Konstruktionsprobleme

- a) **Quadratur des Kreises**: Ist  $\pi$  in einem Unterkörper  $E$  von  $\mathbb{C}$  enthalten, der aus  $K = \mathbb{Q}$  durch sukzessive Adjunktion von Quadratwurzeln entsteht?
- b) **Delisches Problem**: Ist  $\sqrt[3]{2}$  in einem Unterkörper  $E$  von  $\mathbb{C}$  enthalten, der aus  $K = \mathbb{Q}$  durch sukzessive Adjunktion von Quadratwurzeln entsteht?
- c) **Winkeldreiteilung**: Ist für  $t \in \mathbb{R}$  stets  $e^{it/3}$  in einem Unterkörper  $E$  von  $\mathbb{C}$  enthalten, der aus  $K = \mathbb{Q}(e^{it})$  durch sukzessive Adjunktion von Quadratwurzeln entsteht?
- d) **Konstruktion des regelmäßigen  $n$ -Ecks**: Für welche  $n \in \mathbb{N}$  ist  $e^{2\pi i/n}$  in einem Unterkörper  $E$  von  $\mathbb{C}$  enthalten, der aus  $K = \mathbb{Q}$  durch sukzessive Adjunktion von Quadratwurzeln entsteht?

**Lemma 1.8 (Dedekind)** Für jede Körpererweiterung  $E : K$  ist  $E$  eine  $K$ -Algebra, also insbesondere ein  $K$ -Vektorraum.

**Definition 1.9** Für eine Körpererweiterung  $E : K$  nennt man die Dimension  $[E : K]$  des  $K$ -Vektorraums  $E$  den *Grad von  $E$  über  $K$* .

**Beispiel 1.10** 1)  $[\mathbb{C} : \mathbb{R}] = 2$ .

2)  $[\mathbb{Q}(i) : \mathbb{Q}] = 2$ .

3)  $[\mathbb{Q}(\sqrt[3]{2}) : \mathbb{Q}] = 3$ . (Beweis später!)

4)  $[\mathbb{R} : \mathbb{Q}] = \infty$ .

**Lemma 1.11** Es sei  $E : K$  eine Körpererweiterung mit  $\text{char}(K) \neq 2$ . Dann sind äquivalent:

(i)  $[E : K] = 2$ .

(ii)  $E$  entsteht aus  $K$  durch Adjunktion einer Quadratwurzel, die nicht schon in  $K$  liegt.

**Satz 1.12** Mit den Bezeichnungen aus Satz 1.7 sind äquivalent

- (i)  $z \in \langle M \rangle$ .
- (ii) Es gibt eine endliche Kette  $K = K_0 \subseteq K_1 \subseteq \dots \subseteq K_m$  von Unterkörpern von  $\mathbb{C}$  mit  $[K_i : K_{i-1}] = 2$  für  $i = 1, \dots, m$  und  $z \in K_m$ .

**Satz 1.13** Es sei  $F$  Zwischenkörper einer Körpererweiterung  $E : K$ . Dann gilt die Gradformel

$$(13) \quad [E : K] = [E : F][F : K].$$

**Folgerung 1.14** Entsteht  $E$  durch sukzessive Adjunktion von Quadratwurzeln aus  $K$ , so gilt  $[E : K] = 2^m$  für ein  $m \in \mathbb{N}_0$ .

**Folgerung 1.15** Sei  $K$  Unterkörper von  $\mathbb{C}$  mit  $K = \overline{K}$ . Ist dann  $z \in \mathbb{C}$  konstruierbar aus  $K$ , so gilt

$$(14) \quad [K(z) : K] = 2^m \text{ für ein } m \in \mathbb{N}_0.$$

**Bemerkung 1.16** Für die Beantwortung der klassischen Konstruktionsprobleme sind daher folgende Zahlen zu bestimmen:

- a)  $[\mathbb{Q}(\pi) : \mathbb{Q}] (= \infty)$
- b)  $[\mathbb{Q}(\sqrt[3]{2}) : \mathbb{Q}] (= 3)$
- c)  $[\mathbb{Q}(e^{it/3}) : \mathbb{Q}(e^{it})] (= 3 \text{ außer in speziellen Fällen!})$
- d)  $[\mathbb{Q}(e^{2\pi i/n}) : \mathbb{Q}] (= 2^m \text{ nur für } n = \dots)$

**Aufgabe 1.17** Es sei  $k \in \mathbb{Z}$ . Zeigen Sie  $\mathbb{Q}(\sqrt{k}) = \{a + b\sqrt{k} \mid a, b \in \mathbb{Q}\}$  und folgern Sie hieraus  $[\mathbb{Q}(\sqrt{k}) : \mathbb{Q}] = 2$  für alle  $k < 0$ . Für welche  $k > 0$  gilt dasselbe?

**Aufgabe 1.18** Zeigen Sie  $\mathbb{Q}(\sqrt[3]{2}) = \{a + b\sqrt[3]{2} + c(\sqrt[3]{2})^2 \mid a, b, c \in \mathbb{Q}\}$ .

**Aufgabe 1.19** Beweisen Sie die Gradformel (13) für jeden Zwischenkörper  $F$  einer Körpererweiterung  $E : K$ .

## 2 Algebraische und transzendente Körpererweiterungen

**Definition 2.1** Es sei  $E : K$  eine **Körpererweiterung**. Ein Element  $\alpha \in E$  heißt *algebraisch über  $K$* , wenn  $\alpha$  Nullstelle eines Polynoms  $f(x) \neq 0$  aus  $K[x]$  ist, wenn also  $f(\alpha) = 0$  gilt. Ist  $\alpha$  nicht algebraisch über  $K$ , so nennt man  $\alpha$  *transzendent über  $K$* . Die Körpererweiterung  $E : K$  heißt *algebraisch*, wenn jedes  $\alpha \in E$  algebraisch über  $K$  ist, andernfalls spricht man von einer *transzendenten* Körpererweiterung. Schließlich heißt  $E : K$  *endlich*, wenn der **Grad**  $[E : K]$  endlich ist.

**Bemerkung 2.2** a) Die über  $K = \mathbb{Q}$  algebraischen Elemente von  $E = \mathbb{C}$  nennt man auch (*absolut-*)*algebraische Zahlen*, die über  $K = \mathbb{Q}$  transzendenten Elemente von  $E = \mathbb{C}$  auch *transzendente Zahlen*.

b) Es ist  $\alpha = \sqrt[3]{2}$  eine algebraische Zahl, da  $\alpha$  Nullstelle von  $f(x) = x^3 - 2$  aus  $\mathbb{Q}[x]$  ist. Ebenso ist  $\alpha = i$  als Nullstelle von  $x^2 + 1 \in \mathbb{Q}[x]$  eine algebraische Zahl.

c) Die Menge der algebraischen Zahlen ist abzählbar, da  $\mathbb{Q}[x]$  abzählbar ist und jedes  $f(x) \neq 0$  aus  $\mathbb{Q}[x]$  nur endlich viele Nullstellen in  $\mathbb{C}$  hat. Daher gibt es überabzählbar viele transzendente Zahlen.

**Satz 2.3 (Lindemann, 1882)** Die Zahl  $\pi$  ist transzendent.

**Beweis:** Hier ohne!

**Lemma 2.4** Es sei  $(R, +, \cdot)$  ein *Integritätsbereich*, der einen Körper  $K$  enthält. Ist dann die Dimension von  $R$  als  *$K$ -Vektorraum* endlich, so ist  $R$  bereits ein *Körper*.

**Satz 2.5** Es sei  $E : K$  eine Körpererweiterung. Ist  $\alpha \in E$  algebraisch über  $E$ , so ist  $[K(\alpha) : K]$  endlich.

**Definition 2.6** Es sei  $E : K$  eine Körpererweiterung und  $\alpha \in E$  sei algebraisch über  $K$ . Weiterhin sei  $\varphi : K(\alpha) \rightarrow K(\alpha)$  der durch  $\varphi_\alpha(v) = \alpha v$  für alle  $v \in K(\alpha)$  gegebene Endomorphismus des  $K$ -Vektorraums  $K(\alpha)$ . Das Minimalpolynom  $m_{\varphi_\alpha}(x)$  von  $\varphi_\alpha$  heißt dann *Minimalpolynom von  $\alpha$  über  $K$* . Den Grad des Minimalpolynoms nennt man auch den *Grad von  $\alpha$  über  $K$* , in Zeichen:  $[\alpha : K]$ .

## 2 ALGEBRAISCHE UND TRANSZENDENTE KÖRPERERWEITERUNGEN

---

**Bemerkung 2.7** Es ist offensichtlich  $m_{\varphi_\alpha}(x)$  das normierte Polynom kleinsten Grades aus  $K[x]$ , das  $\alpha$  als Nullstelle hat.

**Satz 2.8** Es sei  $E : K$  eine Körpererweiterung und  $\alpha \in E$  sei algebraisch über  $K$  vom Grad  $n = [\alpha : K]$ . Dann ist  $\{1, \alpha, \alpha^2, \dots, \alpha^{n-1}\}$  eine Basis von  $K(\alpha)$  über  $K$ . Insbesondere gilt  $[K(\alpha) : K] = [\alpha : K]$ .

**Beispiel 2.9** Für  $\alpha = \sqrt[3]{2} \notin \mathbb{Q}$  ist  $m_{\varphi_\alpha}(x) = x^3 - 2$ . Hieraus erhält man  $[\mathbb{Q}(\sqrt[3]{2}) : \mathbb{Q}] = [\sqrt[3]{2} : \mathbb{Q}] = 3$ .

**Satz 2.10** Das *Delische Problem* ist unlösbar, da  $\sqrt[3]{2}$  nicht in  $\langle\{0, 1\}\rangle$  liegt.

**Lemma 2.11** Jede *endliche* Körpererweiterung  $E : K$  ist auch *algebraisch*. Für jedes  $\alpha \in E$  ist dann  $[\alpha : K]$  ein Teiler von  $[E : K]$ .

**Folgerung 2.12** Es sei  $E : K$  eine Körpererweiterung und  $\alpha \in E$ . Genau dann ist  $\alpha$  algebraisch über  $K$ , wenn  $K(\alpha) : K$  endlich ist. In diesem Falle ist  $K(\alpha) : K$  algebraisch.

**Satz 2.13** Es sei  $M \subseteq \mathbb{C}$  mit  $0, 1 \in M$  und  $K = \mathbb{Q}(M \cup \overline{M})$ . Dann ist  $\langle M \rangle : K$  algebraisch, also jedes  $z \in \langle M \rangle$  algebraisch über  $K$ .

**Satz 2.14** Das Problem der *Quadratur des Kreises* ist unlösbar, da  $\pi$  transzendent ist.

**Bemerkung 2.15** Die Umkehrung von Lemma 2.11 ist nicht richtig, denn es gibt algebraische Körpererweiterungen, die nicht endlich sind. So sind zum Beispiel für den Körper  $E = \langle\{0, 1\}\rangle$  oder den Körper  $\mathbb{Q}^c$  aller algebraischen Zahlen (vgl. Satz 2.17) die Körpererweiterungen  $E : \mathbb{Q}$  und  $\mathbb{Q}^c : \mathbb{Q}$  algebraisch, aber nicht endlich.

## 2 ALGEBRAISCHE UND TRANSZENDENTE KÖRPERERWEITERUNGEN

---

**Lemma 2.16** Für jede Körpererweiterung  $E : K$  sind äquivalent:

a)  $E : K$  ist endlich.

b) Es gibt endlich viele über  $K$  algebraische Elemente  $\alpha_1, \dots, \alpha_n$  von  $E$  mit  $E = K(\alpha_1, \dots, \alpha_n)$ .

**Satz 2.17** Es sei  $E : K$  eine Körpererweiterung. Dann ist die Teilmenge

$$(1) \quad K^c = \{\alpha \in E \mid \alpha \text{ ist algebraisch über } K\}$$

ein *Zwischenkörper* von  $E : K$ . Insbesondere ist  $\mathbb{Q}^c$  ein Unterkörper von  $\mathbb{C}$ .

**Folgerung 2.18** Es sei  $E : K$  eine Körpererweiterung und  $A \subseteq E$ . Besteht  $A$  nur aus über  $K$  algebraischen Elementen, so ist  $K(A) : K$  algebraisch.

**Satz 2.19** Es sei  $K \subseteq L \subseteq E$  eine Kette von Körpern. Genau dann ist  $E : K$  algebraisch, wenn  $E : L$  und  $L : K$  algebraisch sind.

**Aufgabe 2.20** Jeder endliche *Integritätsbereich* ist ein *Körper*.

### 3 Elementare Ringtheorie

**Definition 3.1** Ein *Ring* ist eine **universelle Algebra**  $(R, +, -, o, \cdot)$  vom Typ  $(2, 1, 0, 2)$ , in der folgende Axiome gelten:

- (2)  $(R, +, -, o)$  ist eine abelsche **Gruppe**.
- (3)  $(R, \cdot)$  ist eine **Halbgruppe**.
- (4) Die Multiplikation  $\cdot$  ist distributiv gegenüber der Addition  $+$ .

Ist auch  $(R, \cdot)$  kommutativ (bzw. ein **Monoid**  $(R, \cdot, e)$ ), so heißt  $(R, +, -, o, \cdot)$  ein *kommutativer Ring* bzw. ein *Ring mit Einselement*  $(R, +, -, o, \cdot, e)$ .

**Satz 3.2** Zu jedem Ring  $(R, +, -, o, \cdot)$  existiert ein Oberring  $(R', +, -, o, \cdot)$ , der ein Einselement besitzt.

**Definition 3.3** Elemente  $a \neq o \neq b$  eines Ringes  $(R, +, -, o, \cdot)$  heißen *Nullteiler* (genauer:  $a$  heißt linker und  $b$  rechter Nullteiler), wenn  $a \cdot b = o$  gilt. Einen kommutativen Ring mit Einselement  $e \neq o$  ohne Nullteiler nennt man *Integritätsbereich*. Ein (kommutativer) Ring  $(R, +, -, o, \cdot)$ , für den  $(R \setminus \{o\}, \cdot)$  eine Gruppe ist heißt (*Körper*) *Schiefkörper*.

**Lemma 3.4** Jeder Körper ist ein Integritätsbereich, jeder endliche Integritätsbereich ist ein Körper.

**Lemma 3.5** Jeder Körper  $E$  besitzt einen kleinsten Unterkörper  $K$ , den Primkörper von  $E$ . Für  $\text{char}(E) = 0$  ist  $K$  isomorph zu  $\mathbb{Q}$ , für endliche Charakteristik  $\text{char}(E) = n$  ist  $n$  eine Primzahl und  $K$  ist isomorph zum Restklassenring  $\mathbb{Z}/(n)$ . In jedem Fall gilt  $\text{char}(E) = \text{char}(K)$ , woraus diese Beziehung für jede Körpererweiterung  $E : K$  folgt.

**Beispiel 3.6** Im Restklassenring  $\mathbb{Z}/(n)$  sind genau die Elemente  $\bar{x} \neq \bar{0}$  Nullteiler, für die  $\text{ggT}(x, n) \neq 1$  gilt. Also ist  $\mathbb{Z}/(n)$  genau dann ein Integritätsbereich und damit ein Körper, wenn  $n$  eine Primzahl ist. Es gibt aber weitere endliche Körper, z. B. auf  $E = \{0, 1, \alpha, \alpha + 1\}$  über dem Primkörper  $K = \mathbb{Z}/(2) = \{0, 1\}$  mit folgenden Strukturtafeln:

$+$	0	1	$\alpha$	$\alpha + 1$	$\cdot$	0	1	$\alpha$	$\alpha + 1$
0	0	1	$\alpha$	$\alpha + 1$	0	0	0	0	0
1	1	0	$\alpha + 1$	$\alpha$	1	0	1	$\alpha$	$\alpha + 1$
$\alpha$	$\alpha$	$\alpha + 1$	0	1	$\alpha$	0	$\alpha$	$\alpha + 1$	1
$\alpha + 1$	$\alpha + 1$	$\alpha$	1	0	$\alpha + 1$	0	$\alpha + 1$	1	$\alpha$

**Satz 3.7 (Wedderburn)** *Jeder endliche Schiefkörper ist ein Körper.*

**Satz 3.8 (Homomorphiesatz)** *Ist  $\varphi : R \rightarrow R'$  ein surjektiver Ringhomomorphismus, dann gibt es eine Kongruenzrelation  $\kappa$  auf  $(R, +, -, o, \cdot)$ , so daß  $R'$  zum Faktorring  $R/\kappa$  isomorph ist. Dabei gilt  $x\kappa y \iff \varphi(x) = \varphi(y) \iff \varphi(x - y) = o \iff x - y \in \text{Kern}(\varphi) = \{a \in R \mid \varphi(a) = o\}$  für alle  $x, y \in R$ .*

**Definition 3.9** Eine nichtleere Teilmenge  $I$  eines Ringes  $(R, +, -, o, \cdot)$  heißt ein *Ideal* von  $R$ , wenn gelten

$$(5) \quad a, b \in I \implies a - b \in I, \text{ d. h. } (I, +) \text{ ist Untergruppe von } (R, +),$$

$$(6) \quad a \in I, x \in R \implies ax, xa \in I.$$

**Lemma 3.10** *Für jedes Ideal  $I$  eines Ringes  $(R, +, -, o, \cdot)$  wird durch*

$$(7) \quad x \equiv y \pmod{I} \iff x - y \in I$$

für alle  $x, y \in R$  eine Kongruenzrelation  $\equiv \pmod{I}$  auf  $(R, +, -, o, \cdot)$  definiert. Umgekehrt bestimmt jede Kongruenz  $\kappa$  von  $(R, +, -, o, \cdot)$  ein Ideal  $I = [o]_\kappa$ . Hierbei gilt für alle  $x, y \in R$

$$(8) \quad x \kappa y \iff x \equiv y \pmod{I}.$$

**Bemerkung 3.11** a) Die Ideale eines Ringes  $(R, +, -, o, \cdot)$  bilden ebenso wie seine Kongruenzen einen vollständigen Verband. Zu jeder Teilmenge  $A$  von  $R$  existiert daher  $(A) = \bigcap \{I \mid I \text{ Ideal von } R \text{ mit } A \subseteq I\}$ , das *von  $A$  in  $R$  erzeugte Ideal*. Speziell für  $A = \{a\}$  schreibt man  $(a)$  für dieses Ideal und nennt  $(a)$  ein *Hauptideal* von  $R$ .

b) Jeder Ring  $(R, +, -, o, \cdot)$  besitzt die *trivialen Ideale*  $R$  und  $\{o\} = (o)$ . Ein Ring ist folglich genau dann einfach, wenn er nur diese trivialen Ideale besitzt. Insbesondere besitzt jeder Schiefkörper nur die trivialen Ideale.

c) Ist  $I$  Ideal eines Ringes  $R$  und  $\kappa$  die Kongruenzrelation  $\equiv \text{ mod } I$ , dann schreibt man auch  $R/I$  für den Faktorring  $R/\kappa$ . Die Elemente von  $R/I$  sind also die Kongruenzklassen von  $R$  modulo  $I$  und lassen sich in der Form  $a + I$  für  $a \in R$  schreiben. Dabei gilt  $a + I = b + I \iff a - b \in I$ .

d) Ist  $\varphi : R \rightarrow R'$  ein Ringhomomorphismus, dann ist  $I = \text{Kern}(\varphi) = \{a \in R \mid \varphi(a) = o\}$  ein Ideal von  $(R, +, -, o, \cdot)$  und  $R/I$  ist isomorph zum homomorphen Bild  $\varphi(R)$ .

**Lemma 3.12** Für Elemente  $a$  eines kommutativen Ringes  $(R, +, -, o, \cdot, e)$  mit Einselement gilt  $(a) = Ra = \{ra \mid r \in R\}$ .

**Definition 3.13** Ein Ideal  $I$  eines Ringes  $(R, +, -, o, \cdot)$  heißt *maximal*, wenn  $I \neq R$  gilt und es kein Ideal  $J \supset I$  von  $(R, +, -, o, \cdot)$  mit  $J \neq R$  gibt.

**Definition 3.14** Ein Ideal  $I \neq R$  eines kommutativen Ringes  $(R, +, -, o, \cdot)$  heißt *Primideal*, wenn für alle  $a, b \in R$  aus  $a \cdot b \in I$  stets  $a \in I$  oder  $b \in I$  folgt.

**Satz 3.15** Es sei  $(R, +, -, o, \cdot, e)$  ein kommutativer Ring mit Einselement und  $I \neq R$  ein Ideal von  $R$ . Genau dann ist  $R/I$  ein Körper (Integritätsbereich), wenn  $I$  ein maximales Ideal (Primideal) ist.

**Folgerung 3.16** a) Ein kommutativer Ring mit Einselement ist genau dann ein Körper, wenn er nur die trivialen Ideale besitzt.

b) In einem kommutativen Ring mit Einselement ist jedes maximale Ideal auch ein Primideal.

**Satz 3.17** Ist  $(R, +, -, o, \cdot, e)$  ein kommutativer Ring mit Einselement, dann gibt es einen Oberring  $Q = Q(R)$  von  $R$  mit Einselement, der  $Q(R) = \{p \cdot q^{-1} \mid p \in R, q \in N\}$  mit  $N = \{q \in R \mid q \neq o \text{ ist kein Nullteiler von } R\}$  erfüllt.

**Bemerkung 3.18** Der Oberring  $Q(R)$  von  $R$  ist bis auf Isomorphie eindeutig bestimmt. Man nennt ihn auch den (vollen) *Quotientenring* von  $R$ . Offensichtlich ist dieser genau dann ein Körper, der *Quotientenkörper* von  $R$ , wenn  $R$  ein Integritätsbereich ist.

**Beispiel 3.19** Bekanntlich ist der Polynomring  $K[x]$  für jeden Körper  $K$  ein Integritätsbereich. Folglich existiert der Quotientenkörper  $Q(K[x])$  und es gilt  $Q(K[x]) = \{\frac{f(x)}{g(x)} \mid f(x), g(x) \in K[x], g(x) \neq 0\} = K(x)$ . Dieser Körper heißt *rationaler Funktionenkörper in einer Unbestimmten über  $K$* . Für  $K = \mathbb{Z}/(p)$  erhält man so unendliche Körper der Charakteristik  $p$ .

**Definition 3.20** Ein Polynom  $f(x) \in K[x]$  mit  $\text{Grad}(f(x)) \geq 1$  heißt *irreduzibel* oder ein *Primpolynom*, wenn für jede Zerlegung  $f(x) = g(x)h(x)$  mit  $g(x), h(x) \in K[x]$  bereits  $g(x) \in K$  oder  $h(x) \in K$  folgt.

**Lemma 3.21** Ist  $f(x) \in K[x]$  irreduzibel, so folgt aus  $f(x) \mid g(x)h(x)$  in  $K[x]$  bereits  $f(x) \mid g(x)$  oder  $f(x) \mid h(x)$ .

**Satz 3.22** Es sei  $(f(x))$  das von  $f(x) \in K[x]$  erzeugte Hauptideal. Der Faktoring  $K[x]/(f(x))$  ist genau dann ein Körper, wenn  $f(x)$  irreduzibel in  $K[x]$  ist.

**Bemerkung 3.23** Zur Konstruktion von Körpererweiterungen über einem Körper  $K$  ist es also nützlich, irreduzible Polynome aus  $K[x]$  zu kennen. ■

**Satz 3.24 (Kronecker)** Jedes nicht-konstante Polynom mit Koeffizienten aus einem Körper  $K$  besitzt in einem geeigneten Erweiterungskörper von  $K$  eine Nullstelle.

**Aufgabe 3.25** Beweisen Sie Lemma 3.4.

**Aufgabe 3.26** Beweisen Sie Lemma 3.9.

**Aufgabe 3.27** Beweisen Sie Lemma 3.11.

**Aufgabe 3.28** Es sei  $\varphi : R \rightarrow R'$  ein surjektiver Ringhomomorphismus. Zeigen Sie, daß für jedes Ideal  $I$  von  $R$  das homomorphe Bild  $\varphi(I)$  ein Ideal von  $R'$  ist. Umgekehrt ist das vollständige Original  $\varphi^{-1}(I')$  ein Ideal von  $R$  für jedes Ideal  $I'$  von  $R'$ .

## 4 Einfache Körpererweiterungen

**Definition 4.1** Eine Körpererweiterung  $E : K$  heißt *einfach*, wenn es ein  $\alpha \in E$  mit  $E = K(\alpha)$  gibt. Jedes solche  $\alpha \in E$  nennt man ein *primitives Element* von  $E : K$ .

**Beispiel 4.2** Für  $E = \mathbb{Q}(\sqrt{2}, \sqrt{3})$  ist etwa  $\alpha = \sqrt{2} + \sqrt{3} \in E$  ein solches primitives Element.

**Satz 4.3** Für eine Körpererweiterung  $E : K$  und  $\alpha \in E$  sind äquivalent:

- a)  $\alpha$  ist algebraisch über  $K$ .
- b)  $K(\alpha) = K[\alpha]$ .
- c)  $K[\alpha]$  ist ein Körper.

**Satz 4.4** Für eine Körpererweiterung  $E : K$  und  $\alpha \in E$  sind äquivalent:

- a)  $\alpha$  genügt keiner algebraischen Relation, d. h. aus  $f(\alpha) = 0$  für  $f(x) \in K[x]$  folgt  $f(x) = 0$ .
- b)  $\alpha$  ist transzendent über  $K$ .
- c)  $K[\alpha] \cong K[x]$  als  $K$ -Algebren.
- d)  $K[\alpha]$  ist kein Körper.

**Satz 4.5** Es sei  $K(\alpha) : K$  eine einfache algebraische Körpererweiterung mit dem primitiven Element  $\alpha$  und  $f(x) = m_{\varphi_{\alpha}}(x)$  das Minimalpolynom von  $\alpha$ . Dann vermittelt der Einsetzungshomomorphismus  $K[x] \rightarrow K[\alpha] = K(\alpha)$  einen Isomorphismus von  $K$ -Algebren  $K[x]/(f(x)) \rightarrow K(\alpha)$ . Insbesondere gilt für alle  $g(x) \in K[x]$

$$(9) \quad g(\alpha) = 0 \iff f(x) | g(x).$$

**Lemma 4.6** *Es sei  $E : K$  eine Körpererweiterung und  $\alpha \in E$  sei algebraisch über  $K$ . Dann ist das Minimalpolynom  $f(x) = m_{\varphi_{\alpha}}(x) \in K[x]$  von  $\alpha$  irreduzibel. Ist umgekehrt  $g(x)$  ein normiertes irreduzibles Polynom aus  $K[x]$  mit  $g(\alpha) = 0$ , so gilt  $g(x) = m_{\varphi_{\alpha}}(x)$ .*

**Satz 4.7** *Es sei  $K(\alpha) : K$  eine einfache Körpererweiterung mit dem über  $K$  transzendenten Element  $\alpha$ . Dann vermittelt der Einsetzungshomomorphismus  $K[x] \rightarrow K[\alpha]$  einen Isomorphismus von  $K$ -Algebren  $K(x) \rightarrow K(\alpha)$ . Gilt umgekehrt  $K(x) \cong K(\alpha)$ , so ist  $\alpha$  transzendent über  $K$ . ■*

**Lemma 4.8** *Es sei  $K(\alpha) : K$  eine einfache algebraische Körpererweiterung. Weiterhin sei  $L$  ein Zwischenkörper und  $g(x) = x^m + \beta_{m-1}x^{m-1} + \dots + \beta_1x + \beta_0 \in L[x]$  das Minimalpolynom von  $\alpha$  über  $L$ . Dann gilt  $L = K(\beta_0, \dots, \beta_{m-1})$ .*

Ohne Beweis sei noch angemerkt:

**Satz 4.9** *Eine algebraische Körpererweiterung  $E : K$  ist genau dann einfach, wenn sie nur endlich viele Zwischenkörper besitzt.*

## 5 Teilbarkeitslehre

In diesem Abschnitt bezeichne  $R$  stets einen kommutativen Ring mit Einselement  $e \neq o$ .

**Definition 5.1** Gilt  $b = ca$  für Elemente  $a, b, c \in R$ , so sagt man  $a$  teilt  $b$  oder  $a$  ist ein Teiler von  $b$ , in Zeichen:  $a \mid b$ . Gilt  $a \mid b$  und  $b \mid a$ , so heißen  $a$  und  $b$  assoziiert zueinander, in Zeichen:  $a \sim b$ . Unter einer *Einheit*  $\varepsilon$  von  $R$  versteht man ein in  $(R, \cdot, e)$  invertierbares Element. Man bezeichnet die Menge aller Einheiten von  $R$  auch mit  $R^*$ . Ein Teiler  $a$  von  $b$  heißt *echter Teiler* von  $b$ , wenn  $a$  weder Einheit von  $R$  noch zu  $b$  assoziiert ist.

**Lemma 5.2** a) Für Elemente  $a, b, c, d \in R$  gelten:

- (10)  $a \mid b \iff (b) \subseteq (a)$ ,
- (11)  $a \mid a$ ,
- (12)  $a \mid b$  und  $b \mid c \implies a \mid c$ ,
- (13)  $e \mid a$  und  $a \mid o$ ,
- (14)  $a \mid b$  und  $c \mid d \implies ac \mid bd$ ,
- (15)  $a \mid b$  und  $a \mid c \implies a \mid b + c$ ,
- (16)  $\varepsilon \mid e \iff \varepsilon$  ist Einheit,
- (17)  $a \sim b \iff (a) = (b)$ .

Die Assoziiertheit  $\sim$  ist also eine Äquivalenzrelation auf  $R$ .

b) Ist  $R$  sogar ein Integritätsbereich, so gilt außerdem für alle  $c \neq o$

$$(18) \quad ac \mid bc \implies a \mid b,$$

und  $a \sim b$  gilt genau dann, wenn es ein  $\varepsilon \in R^*$  mit  $b = \varepsilon a$  gibt.

**Beispiel 5.3** a) Für jeden Körper  $K$  ist  $K^* = K \setminus \{o\}$ .

b) Für den Ring  $R = \mathbb{Z} + \mathbb{Z}i \subseteq \mathbb{C}$  der ganzen Gaußschen Zahlen ist  $R^* = \{\pm 1, \pm i\}$ .

c) Ist  $R$  ein Integritätsbereich, so gilt  $(R[x])^* = R^*$ .

d) Für  $R = \mathbb{Z} + \mathbb{Z}\sqrt{2}$  gilt  $R^* = \{\pm(1 + \sqrt{2})^n \mid n \in \mathbb{Z}\}$ . (Dies ist nicht ganz einfach zu zeigen!)

**Definition 5.4** Es sei  $A$  eine nichtleere Teilmenge von  $R$ . Ein Element  $d \in R$  heißt *ein größter gemeinsamer Teiler (der Elemente) von  $A$* , wenn folgende zwei Bedingungen erfüllt sind:

- (i)  $d$  ist gemeinsamer Teiler (der Elemente) von  $A$ , d. h.  $d \mid a$  für alle  $a \in A$ ,
- (ii) für jeden gemeinsamen Teiler  $t$  von  $A$  gilt  $t \mid d$ .

Man schreibt dafür auch  $d = \text{ggT}(A)$  und nennt  $A$  *teilerfremd*, wenn  $e = \text{ggT}(A)$  gilt. Analog wird das *kleinste gemeinsame Vielfache*  $k = \text{kgV}(A)$  von  $A$  definiert.

**Lemma 5.5** Es sei  $d \in R$  ein größter gemeinsamer Teiler von  $A$ . Genau dann ist auch  $d' \in R$  ein größter gemeinsamer Teiler von  $A$ , wenn  $d \sim d'$  gilt. Entsprechendes gilt für kleinste gemeinsame Vielfache von  $A$ .

**Lemma 5.6** Für endlich viele Ideale  $I_1, \dots, I_n$  von  $R$  ist auch  $I_1 + \dots + I_n = \{a_1 + \dots + a_n \mid a_\nu \in I_\nu\}$  ein Ideal von  $R$  und zwar das kleinste Ideal von  $R$ , welches jedes  $I_\nu$  enthält.

**Bemerkung 5.7** Im Falle von Hauptidealen  $I_\nu = (a_\nu)$  schreibt man kurz  $(a_1, \dots, a_n) = (a_1) + \dots + (a_n)$ . ■

**Definition 5.8** Ein Integritätsbereich  $R$  heißt *Hauptidealring*, wenn jedes Ideal von  $R$  ein Hauptideal ist.

**Lemma 5.9** In einem Hauptidealring  $R$  existiert zu beliebigen Elementen  $a_1, \dots, a_n$  von  $R$  stets ein größter gemeinsamer Teiler. Ist  $d$  ein solcher größter gemeinsamer Teiler, so gibt es  $x_1, \dots, x_n \in R$  mit

$$(19) \quad d = x_1 a_1 + \dots + x_n a_n.$$

**Satz 5.10** Jeder euklidische Ring ist ein Hauptidealring, also speziell der Ring der ganzen Zahlen  $\mathbb{Z}$  und jeder Polynomring  $K[x]$  über einem Körper  $K$ .

**Definition 5.11** Ein Element  $p \neq o$  von  $R$ , das keine Einheit von  $R$  ist, heißt *irreduzibel* oder *unzerlegbar*, wenn

$$(20) \quad p = ab \implies a \in R^* \text{ oder } b \in R^*$$

gilt. Dagegen nennt man  $p$  *prim* oder ein *Primelement* von  $R$ , wenn gilt

$$(21) \quad p \mid ab \implies p \mid a \text{ oder } p \mid b.$$

**Bemerkung 5.12** In einem Integritätsbereich  $R$  ist  $p \neq o$  also genau dann irreduzibel, wenn  $p$  keine Einheit ist und keine echten Teiler besitzt. Insbesondere ist also jedes prime Element auch irreduzibel. Die Umkehrung hiervon gilt nicht, denn in dem Integritätsbereich  $R = \mathbb{Z} + \mathbb{Z}\sqrt{-5} \subseteq \mathbb{C}$  gilt  $2 \cdot 3 = 6 = (1 + \sqrt{-5}) \cdot (1 - \sqrt{-5})$ , aber das auch in  $R$  irreduzible Element 2 ist weder Teiler von  $1 + \sqrt{-5}$  noch von  $1 - \sqrt{-5}$ .

**Folgerung 5.13** Genau dann ist  $p \neq o$  aus  $R$  prim, wenn das Hauptideal  $(p)$  ein Primideal ist.

**Folgerung 5.14** Ist  $p$  irreduzibles Element eines Hauptidealringes  $R$ , so ist  $R/(p)$  ein Körper. Insbesondere ist  $p$  also prim. ■

**Folgerung 5.15** Der Polynomring  $R[x]$  ist genau dann ein Hauptidealring, wenn  $R$  ein Körper ist.

**Definition 5.16** Ein Element  $a \in R$  besitzt eine *Zerlegung in irreduzible Faktoren*, wenn  $a$  eine Darstellung der Form

$$(22) \quad a = \varepsilon p_1 \cdots p_n \text{ mit } \varepsilon \in R^* \text{ und irreduziblen } p_\nu$$

besitzt. Man sagt  $a$  besitzt eine *eindeutige Zerlegung in irreduzible Faktoren*, wenn  $a$  eine Zerlegung gemäß (22) besitzt und für jede andere derartige Zerlegung

$$(23) \quad a = \varepsilon' p'_1 \cdots p'_m$$

bereits  $n = m$  und nach geeigneter Ummumerierung  $p_\nu \sim p'_\nu$  für  $\nu = 1, \dots, n$  gilt. Ein Integritätsbereich, in dem jedes  $a \neq o$  eine eindeutige Zerlegung in irreduzible Faktoren besitzt, heißt *faktoriell* oder *ZPE-Ring* oder *Gaußscher Ring*.

**Lemma 5.17** *Es sei  $R$  ein Integritätsbereich, in dem jedes  $a \neq 0$  eine Zerlegung in irreduzible Faktoren besitzt. Dann sind äquivalent:*

- a)  *$R$  ist faktoriell.*
- b) *Jedes irreduzible Element von  $R$  ist prim.*

**Definition 5.18** Der Ring  $R$  erfüllt die *Teilerkettenbedingung* oder *aufsteigende Kettenbedingung für Hauptideale*, wenn jede Kette  $(a_1) \subseteq (a_2) \subseteq \dots \subseteq (a_n) \subseteq (a_{n+1}) \subseteq \dots$  von Hauptidealen stationär ist, d. h. es gibt ein  $n \in \mathbb{N}$  mit  $(a_j) = (a_n)$  für alle  $j \geq n$ .

**Satz 5.19** *Ein Integritätsbereich  $R$  ist genau dann faktoriell, wenn er die Teilerkettenbedingung erfüllt und jedes irreduzible Element von  $R$  prim ist.*

**Folgerung 5.20** *Jeder Hauptidealring ist faktoriell.*

## 6 Faktorielle Ringe

In diesem Abschnitt bezeichne  $R$  stets einen Integritätsbereich.

**Lemma 6.1** Für  $a \in R$  sei  $R/(a) = \bar{R}$  der Faktorring von  $R$  nach dem Hauptideal  $(a)$ . Dann läßt sich der natürliche Homomorphismus  $R \rightarrow \bar{R}$  zu einem Homomorphismus der Polynomringe  $\varphi : R[x] \rightarrow \bar{R}[x]$  fortsetzen. Hieraus ergibt sich die Isomorphie der Ringe  $R[x]/(a)$  und  $(R/(a))[x]$ . Dabei ist  $a$  genau dann prim in  $R$ , wenn  $a$  prim in  $R[x]$  ist.

**Lemma 6.2** Mit  $R[x]$  ist auch  $R$  faktoriell.

**Satz 6.3 (Gauß)** Mit  $R$  ist auch  $R[x]$  faktoriell.

**Definition 6.4** Es sei  $R$  ein faktorieller Ring. Unter einem *Vertretersystem*  $P$  für die Klassen assoziierter Primelemente versteht man eine Menge  $P$  von Primelementen von  $R$ , so daß jedes Primelement von  $R$  zu genau einem Primelement von  $P$  assoziiert ist. (Ein solches System muß nach dem Auswahlaxiom existieren!)

**Lemma 6.5** Es sei  $R$  ein faktorieller Ring und  $P$  ein Vertretersystem für die Klassen assoziierter Elemente von  $R$ . Dann besitzt jedes  $a \neq 0$  aus  $R$  eine eindeutige Darstellung der Form

$$(24) \quad a = \varepsilon \prod_{p \in P} p^{e_p}$$

mit  $\varepsilon \in R^*$  und ganzen Zahlen  $e_p \geq 0$  mit  $e_p = 0$  für fast alle  $p \in P$ .

**Bemerkung 6.6** In manchen faktoriellen Ringen  $R$  gibt es "natürliche" Vertretersysteme, etwa in  $R = \mathbb{Z}$  die Menge der natürlichen Primzahlen und in  $R = K[x]$  die Menge der normierten Primpolynome.

**Definition 6.7** Es sei  $R$  ein faktorieller Ring und  $K = Q(R)$  sein Quotientenkörper. Weiterhin sei  $p \in R$  ein Primelement von  $R$ . Für jedes  $a \neq o$  aus  $R$  sei dann  $w_p(a) \in \mathbb{N}_0$  der höchste Exponent, "mit dem  $p$  in  $a$  aufgeht", also

$$(25) \quad a = p^{w_p(a)} a' \text{ mit } p \nmid a'.$$

Setzt man noch  $w_p(o) = \infty$ , dann hat man eine Abbildung  $w_p : R \rightarrow \mathbb{Z} \cup \{\infty\}$ . Diese läßt sich durch

$$(26) \quad w_p\left(\frac{a}{b}\right) = w_p(a) - w_p(b) \text{ für alle } \frac{a}{b} \in K$$

zu einer (wohldefinierten!) Abbildung  $w_p : K \rightarrow \mathbb{Z} \cup \{\infty\}$  fortsetzen. Man nennt sie die zu  $p$  gehörende *Exponentenbewertung von  $K$* .

**Lemma 6.8** *Es sei  $R$  ein faktorieller Ring,  $K = Q(R)$  sein Quotientenkörper und  $P$  ein Vertretersystem für die Klassen assoziierter Primelemente von  $R$ .*

a) *Für jedes Primelement  $p \in P$  erfüllt die Exponentenbewertung  $w_p$  die Bedingungen*

$$(27) \quad w_p(ab) = w_p(a) + w_p(b)$$

$$(28) \quad w_p(a + b) \geq \min(w_p(a), w_p(b))$$

*für alle  $a, b \in K$ .*

b) *Jedes Element  $a \neq o$  aus  $K$  besitzt die Darstellung*

$$(29) \quad a = \varepsilon \prod_{p \in P} p^{w_p(a)} \text{ mit } \varepsilon \in R^*,$$

*wobei  $w_p(a) = 0$  für fast alle  $p \in P$  gilt.*

c) *Ein Element  $a \in K$  liegt genau dann in  $R$ , wenn  $w_p(a) \geq 0$  für alle  $p \in P$  gilt.*

d) *Für  $a, b \in R$  ist  $a \mid b$  gleichwertig mit  $w_p(a) \leq w_p(b)$  für alle  $p \in P$ .*

e) *Zu beliebigen  $a_1, \dots, a_n \in R$  existieren  $d = \text{ggT}(a_1, \dots, a_n)$  und  $k = \text{kgV}(a_1, \dots, a_n)$  gemäß* ■

$$(30) \quad d = \prod_{p \in P} p^{\min(w_p(a_1), \dots, w_p(a_n))} \text{ und } k = \prod_{p \in P} p^{\max(w_p(a_1), \dots, w_p(a_n))},$$

*wobei gegebenenfalls  $p^\infty = o$  zu interpretieren ist.*

**Lemma 6.9** *Es sei  $R$  ein faktorieller Ring,  $K = Q(R)$  sein Quotientenkörper und  $p$  ein Primelement von  $R$ . Die zugehörige Exponentenbewertung  $w_p : K \rightarrow \mathbb{Z} \cup \{\infty\}$  werde durch*

$$(31) \quad w_p(a_n x^n + \cdots + a_1 x + a_0) = \min(w_p(a_n), \dots, w_p(a_0))$$

*zu einer Abbildung  $w_p : K[x] \rightarrow \mathbb{Z} \cup \{\infty\}$  fortgesetzt. Dann gilt*

$$(32) \quad w_p(g(x)h(x)) = w_p(g(x)) + w_p(h(x))$$

*für alle  $g(x), h(x) \in K[x]$ .*

**Definition 6.10** *Es sei  $f(x) \in R[x]$  mit  $\text{Grad}(f(x)) \geq 1$ . Der größte gemeinsame Teiler der Koeffizienten von  $f(x)$  heißt *Inhalt* von  $f(x)$ , in Zeichen:  $\text{Inh}(f(x))$ , und man nennt  $f(x)$  *primitiv*, wenn  $e = \text{Inh}(f(x))$  ist.*

Nun kann man eine etwas genauere Version von Satz 6.3 beweisen:

**Satz 6.11** *Es sei  $R$  ein faktorieller Ring mit dem Quotientenkörper  $K = Q(R)$ . Ist  $P_1$  ein Vertretersystem für die Klassen assoziierter Primelemente von  $R$  und  $P_2$  ein Vertretersystem für die Klassen assoziierter Primelemente von  $K[x]$ , das aus primitiven Polynomen aus  $R[x]$  besteht, dann ist  $R[x]$  faktoriell und  $P_1 \cup P_2$  ist ein Vertretersystem für die Klassen assoziierter Primelemente von  $R[x]$ .*

**Lemma 6.12** *Es sei  $R$  faktoriell mit dem Quotientenkörper  $K = Q(R)$  und für  $g(x) \in R[x]$  gelte  $\text{Grad}(g(x)) \geq 1$ . Ist dann  $g(x)$  irreduzibel in  $R[x]$ , so auch in  $K[x]$ .*

**Lemma 6.13 (Lemma von Gauß)** *Es sei  $R$  faktoriell mit dem Quotientenkörper  $K = Q(R)$  und  $f(x) \in R[x]$ . Gilt dann  $f(x) = g(x)h(x)$  für normierte Polynome  $g(x), h(x) \in K[x]$ , so liegen  $g(x)$  und  $h(x)$  bereits in  $R[x]$ .*

**Lemma 6.14** *Es sei  $R$  faktoriell mit dem Quotientenkörper  $K = Q(R)$  und  $f(x) \in R[x]$  sei normiert. Ist dann  $\alpha \in K$  Nullstelle von  $f(x)$ , so liegt  $\alpha$  bereits in  $R$  und teilt das Absolutglied von  $f(x)$ .*

**Satz 6.15** *Es seien  $R$  und  $\overline{R}$  Integritätsbereiche und  $\varphi : R \rightarrow \overline{R}$  ein Homomorphismus, der in natürlicher Weise zu einem Homomorphismus  $f(x) = \sum_{\nu=0}^n a_\nu x^\nu \mapsto \varphi(f(x)) = \overline{f}(x) = \sum_{\nu=0}^n \overline{a}_\nu x^\nu$  der Polynomringe fortgesetzt werde. Weiterhin sei  $f(x) = \sum_{\nu=0}^n a_\nu x^\nu \in R[x]$  ein primitives Polynom mit  $\overline{a}_n \neq 0$ . Ist dann  $\overline{f}(x)$  irreduzibel in  $\overline{R}[x]$ , so ist  $f(x)$  irreduzibel in  $R[x]$ .*

**Satz 6.16 (Irreduzibilitätskriterium von Eisenstein)** *Es sei  $f(x) = ax^n + a_{n-1}x^{n-1} + \dots + a_1x + a_0 \in R[x]$  ein primitives Polynom und  $p \in R$  prim mit*

- (i)  $p \nmid a$ , (ii)  $p \mid a_\nu$  für  $0 \leq \nu \leq n-1$  und (iii)  $p^2 \nmid a_0$ ,

*so ist  $f(x)$  irreduzibel in  $R[x]$ . Im Falle eines faktoriellen Ringes  $R$  ist  $f(x)$  dann auch irreduzibel in  $Q(R)[x]$ .*

**Beispiel 6.17** *Ist  $a \in \mathbb{Z} \setminus \{-1, 0, 1\}$  quadratfrei, so ist  $f(x) = x^n - a$  für alle  $n \in \mathbb{N}$  irreduzibel in  $\mathbb{Z}[x]$  und  $\mathbb{Q}[x]$ .*

**Satz 6.18** *Für alle  $\varphi$  mit  $0 \leq \varphi < 2\pi$ , für die  $e^{i\varphi}$  transzendent ist, ist die Dreiteilung des Winkels  $\varphi$  mit Zirkel und Lineal nicht möglich.*

**Bemerkung 6.19** a) Die Bedingung “ $e^{i\varphi}$  ist transzendent” ist für überabzählbar viele  $\varphi$  erfüllt. Die Abbildung  $\varphi \mapsto e^{i\varphi}$  ist nämlich eine Bijektion von  $[0, 2\pi)$  auf den Einheitskreis in  $\mathbb{C}$  und dort liegen nur abzählbar viele algebraische Elemente.

b) Auch wenn  $e^{i\varphi}$  algebraisch ist, ist die Dreiteilung von  $\varphi$  mit Zirkel und Lineal nicht immer möglich, etwa für  $\varphi = 2\pi i/3$ . Denn hierfür läuft die Dreiteilung des Winkels auf die Konstruktion des regelmäßigen 9-Ecks hinaus, was nach den folgenden Überlegungen unmöglich ist.

c) Viele Beispiele für “ $e^{i\varphi}$  ist transzendent” liefert der berühmte **Satz von Hermite-Lindemann**: *Für algebraisches  $z \neq 0$  aus  $\mathbb{C}$  ist  $e^z$  stets transzendent.* Wegen  $e^{i\pi} = -1$  folgt daraus insbesondere die Transzendenz von  $\pi$ .

**Folgerung 6.20** *Ist  $p \in \mathbb{N}$  eine Primzahl, dann ist das Polynom  $F_p(x) = x^{p-1} + x^{p-2} + \dots + x + 1$  irreduzibel in  $\mathbb{Q}[x]$ .*

**Satz 6.21** *Es sei  $n = p$  eine Primzahl. Dann ist die Konstruktion des regelmäßigen  $n$ -Ecks mit Zirkel und Lineal nicht möglich, wenn  $p - 1$  keine Potenz von 2 ist.*

**Bemerkung 6.22** Also ist das regelmäßige 7-Eck (11-Eck, 13-Eck, 14-Eck, 19-Eck, ...) nicht mit Zirkel und Lineal konstruierbar. Eine Konstruktion des regelmäßigen 17-Ecks gab der 18jährige Gauß an. Daß auch die Konstruktion des regelmäßigen 9-Ecks unmöglich ist, ergibt sich aus der folgenden Verallgemeinerung von Folgerung 6.20.

**Folgerung 6.23** *Ist  $p \in \mathbb{N}$  eine Primzahl und  $n = p^k$  für ein  $k \in \mathbb{N}$ , dann ist  $F_{p^k}(x) = x^{(p-1)p^{k-1}} + \dots + x^{2p^{k-1}} + x^{p^{k-1}} + 1 = F_p(x^{p^{k-1}})$  das Minimalpolynom von  $\alpha = e^{2\pi i/n}$  über  $\mathbb{Q}$ . Insbesondere gilt  $[\mathbb{Q}(\alpha) : \mathbb{Q}] = p^{k-1}(p - 1)$ .*

**Bemerkung 6.24** Das regelmäßige  $n$ -Eck ist genau dann mit Zirkel und Lineal konstruierbar, wenn

$$(33) \quad n = 2^m p_1 \cdots p_\ell, \quad m, \ell \in \mathbb{N}_0$$

gilt mit verschiedenen Fermatschen Primzahlen  $p_i$ . Dabei heißt eine Primzahl  $p$  *Fermatsche Primzahl*, wenn sie von der Gestalt  $p = 2^{2^k} + 1$  für ein  $k \in \mathbb{N}_0$  ist. Fermat hatte angenommen, daß alle Zahlen  $p$  dieser Form Primzahlen sind. Dies ist richtig für  $k = 0, 1, 2, 3, 4$  und liefert die Primzahlen 3, 5, 17, 257 und 65537. Für  $k = 5, \dots, 16$  und viele größere Werte von  $k$  liefert diese Formel jedoch keine Primzahl. Der Fall  $k = 17$  ist noch offen. Man kennt überhaupt keine weitere Fermatsche Primzahl.

Eng verwandt mit den Fermatschen Primzahlen sind die *Mersenneschen Zahlen* der Form  $n = 2^k - 1$  und unter ihnen insbesondere die Primzahlen. Sie sind die beliebtesten Kandidaten bei der Jagd nach der größten bekannten Primzahl. (Zur Zeit liegt dieser Rekord bei  $k = 1398269$ , vgl. <http://www.utm.edu/research/primes/mersenne.shtml>)

## 7 Endliche Körper

**Lemma 7.1** *Für jeden Schiefkörper  $K$  ist das Zentrum*

$$(34) \quad Z(K) = \{a \in K \mid ab = ba \text{ für alle } b \in K\}$$

*ein kommutativer Unterkörper von  $K$ , der somit den Primkörper  $P(K)$  von  $K$  enthält.*

**Bemerkung 7.2** a) Der Beweis des Satzes von Wedderburn, wonach jeder endliche Schiefkörper  $K$  bereits kommutativer Körper ist, beruht auf dem Nachweis, daß  $K$  eindimensionaler  $Z(K)$ -Vektorraum ist.

b) Ist  $K$  endlicher Körper, dann ist die Charakteristik  $\text{char}(K)$  eine Primzahl  $p$  und der Primkörper  $P(K)$  ist isomorph zu  $\mathbb{Z}/(p)$ . Mit  $n = [K : P(K)]$  gilt daher  $|K| = q = p^n$ .

**Lemma 7.3** *Ist  $(G, \cdot, e)$  eine endliche Gruppe mit  $|G| = n$ , so gilt  $x^n = e$  für alle  $x \in G$ .*

**Folgerung 7.4** *Sind  $K$  und  $K'$  endliche Körper mit  $q$  Elementen, so sind sie isomorph.*

**Satz 7.5** *Ist  $p \in \mathbb{N}$  eine Primzahl,  $n \in \mathbb{N}$  und  $q = p^n$ , dann gibt es einen Körper  $K$  mit  $q$  Elementen.*

**Definition 7.6** Es sei  $p \in \mathbb{N}$  eine Primzahl,  $n \in \mathbb{N}$  und  $q = p^n$ . Der bis auf Isomorphie eindeutig bestimmte endliche Körper  $K$  mit  $q$  Elementen heißt das *Galois-Feld*  $GF(q)$ .

**Bemerkung 7.7** Man könnte einen solchen Körper  $K$  konstruieren, indem man ein irreduzibles Polynom  $f(x) \in \mathbb{Z}/(p)$  mit  $\text{Grad}(f(x)) = n$  nimmt und den Körper  $K = \mathbb{Z}/(p)[x]/(f(x))$  bildet (vgl. Beispiel 3.5). Die Existenz eines solchen Körpers ist daher äquivalent mit der Existenz eines derartigen irreduziblen Polynoms. Üblicherweise konstruiert man  $K$  aber als Zerfällungskörper des Polynoms  $f(x) = x^q - x \in \mathbb{Z}/(p)[x]$  wie im folgenden erläutert.

**Definition 7.8** Erweiterungskörper  $E$  und  $E'$  eines Grundkörpers heißen *K-isomorph*, wenn es einen Isomorphismus  $\varphi : E \rightarrow E'$  mit  $\varphi(k) = k$  für alle  $k \in K$  gibt.

**Folgerung 7.9** Ist  $K$  ein endlicher Körper, so gibt es für jedes  $m \in \mathbb{N}$  bis auf  $K$ -Isomorphie genau einen Erweiterungskörper  $E$  von  $K$  mit  $[E : K] = m$ .

**Definition 7.10** Es sei  $K$  ein Körper und  $f(x) \in K[x]$  ein nicht-konstantes Polynom. Ein Erweiterungskörper  $E$  von  $K$  heißt *Zerfällungskörper von  $f(x)$  über  $K$* , wenn es  $\alpha_1, \dots, \alpha_n \in E$  gibt mit  $E = K(\alpha_1, \dots, \alpha_n)$  und  $f(x) = k(x - \alpha_1) \cdots (x - \alpha_n)$ , d. h.  $f(x)$  zerfällt über  $E$  vollständig in Linearfaktoren.

**Beispiel 7.11** Für das *Kreisteilungspolynom*  $f(x) = x^n - 1 \in \mathbb{Q}[x]$  ist  $E = \mathbb{Q}(\zeta)$  mit  $\zeta = e^{2i\pi/n}$  Zerfällungskörper, denn es gilt  $x^n - 1 = \prod_{j=1}^n (x - \zeta^j)$  mit den paarweise verschiedenen komplexen Zahlen  $\zeta, \zeta^2, \dots, \zeta^n = 1$ .

**Folgerung 7.12** Es sei  $K$  ein Körper und  $f(x) \in K[x]$  nicht konstant. Dann existiert ein Zerfällungskörper von  $f(x)$  über  $K$ .

**Definition 7.13** Ein Körper  $C$  heißt *algebraisch abgeschlossen*, wenn jedes Polynom  $f(x) \in C[x]$  mit  $\text{Grad}(f(x)) \geq 1$  eine Nullstelle in  $C$  besitzt.

**Beispiel 7.14** Der Körper  $\mathbb{C}$  der komplexen Zahlen ist algebraisch abgeschlossen. Die Körper  $\mathbb{Q}$  und  $\mathbb{R}$  sind nicht algebraisch abgeschlossen.

**Lemma 7.15** Für jeden Körper  $C$  sind äquivalent:

- a)  $C$  ist algebraisch abgeschlossen.
- b) Jedes irreduzible Polynom in  $C[x]$  ist linear.
- c) Jedes nicht-konstante Polynom aus  $C[x]$  zerfällt über  $C$  vollständig in Linearfaktoren.
- d) Ist  $E : C$  eine algebraische Körpererweiterung, so gilt  $E = C$ .

**Satz 7.16 (Steinitz)** *Zu jedem Körper  $K$  existiert ein Erweiterungskörper  $C$  von  $K$  mit den folgenden Eigenschaften:*

(i)  *$C$  ist algebraisch abgeschlossen.*

(ii)  *$C : K$  ist algebraisch.*

*Ist  $C'$  ein weiterer Körper mit diesen beiden Eigenschaften, so sind  $C$  und  $C'$   $K$ -isomorph.*

**Definition 7.17** Den Erweiterungskörper  $C$  von  $K$  mit den Eigenschaften (i) und (ii) nennt man den *algebraischen Abschluß* oder die *algebraische Hülle* von  $K$ .

**Folgerung 7.18** *Der Zerfällungskörper eines nicht-konstanten Polynoms  $f(x) \in K[x]$  ist bis auf  $K$ -Isomorphie eindeutig bestimmt.*