

## 3 Algebraische Körpererweiterungen

### 3.1 Algebraische und transzendente Elemente

#### Definition 3.1.1

Sei  $L$  ein Körper,  $K \subset L$  Teilkörper.

- (a) Dann heißt  $L$  Körpererweiterung von  $K$ . Schreibweise:  $L/K$  Körpererweiterung.
- (b)  $[L : K] = \dim_K L$  heißt **Grad** von  $L$  über  $K$
- (c)  $L/K$  heißt **endlich**, wenn  $[L : K] < \infty$
- (d)  $\alpha \in L$  heißt **algebraisch** über  $K$ , wenn es ein  $0 \neq f \in K[X]$  gibt mit  $f(\alpha) = 0$
- (e)  $\alpha \in L$  heißt **transzendent** über  $K$ , wenn  $\alpha$  nicht algebraisch über  $K$  ist.
- (f)  $L/K$  heißt **algebraische Körpererweiterung**, wenn jedes  $\alpha \in L$  algebraisch über  $K$  ist.

#### Beispiel:

- (1) Für  $a \in \mathbb{Q}$  und  $n \geq 2$  ist  $\sqrt[n]{a}$  algebraisch über  $\mathbb{Q}$ , da Nullstelle von  $X^n - a$   
Summe und Produkt von solchen Wurzeln sind auch algebraisch über  $\mathbb{Q}$   
z.B.:  $\sqrt{2} + \sqrt{3}$  ist Nullstelle von  $X^4 - 10X^2 + 1$ ,  $i$  ist Nullstelle von  $X^2 + 1$ .  
  
Klassische Frage: Hat jedes  $f \in \mathbb{Q}[X]$  eine Nullstelle, die ein „Wurzelausdruck“ ist?.
- (2) Sei  $L = K(X) = \text{Quot}(K[X])$ . Dann ist  $X$  transzendent über  $K$ . Das gleiche gilt für jedes  $f \in K(X) \setminus K$
- (3) In  $\mathbb{R}$  gibt es sehr viele über  $\mathbb{Q}$  transzendente Elemente. Da  $\mathbb{Q}$  abzählbar ist, ist auch  $\mathbb{Q}[X]$  abzählbar, da jedes  $f \in \mathbb{Q}[X]$  endlich viele Nullstellen hat. Das heißt, es gibt nur abzählbar viele Elemente in  $\mathbb{R}$ , die algebraisch über  $\mathbb{Q}$  sind.  $\mathbb{R}$  ist aber nicht abzählbar.

#### Definition + Bemerkung 3.1.2

Sei  $L/K$  Körpererweiterung,  $\alpha \in L$ ,  
 $\varphi_\alpha : K[X] \rightarrow L, f \mapsto f(\alpha)$  Einsetzungshomomorphismus.

- (a)  $\text{Kern}(\varphi_\alpha)$  ist Primideal in  $K[X]$

### 3 Algebraische Körpererweiterungen

**Beweis:**  $\text{Kern}(\varphi_\alpha)$  ist Ideal, da  $\varphi_\alpha$  Homomorphismus ist. Seien nun  $f, g \in K[X]$  mit  $f, g \in \text{Kern}(\varphi_\alpha) \Rightarrow (fg)(\alpha) = f(\alpha)g(\alpha) = 0 \xrightarrow{L \text{ Körper}} f(\alpha) = 0$  oder  $g(\alpha) = 0$  ■

- (b)  $\alpha$  algebraisch genau dann, wenn  $\varphi_\alpha$  nicht injektiv ist.
- (c) Ist  $\alpha$  algebraisch über  $K$ , so gibt es ein eindeutig bestimmtes, irreduzibles und normiertes Polynom  $f_\alpha \in K[X]$  mit  $f_\alpha(\alpha) = 0$  und  $\text{Kern}(\varphi_\alpha) = (f_\alpha)$ .  $f_\alpha$  heißt **Minimalpolynom** von  $\alpha$ .

**Beweis:**  $K[X]$  ist Hauptidealring  $\Rightarrow \exists \tilde{f}_\alpha$  mit  $\text{Kern}(\varphi_\alpha) = (\tilde{f}_\alpha)$ . Wegen (a) ist  $\tilde{f}_\alpha$  irreduzibel, eindeutig bis auf Einheit in  $K[X]$ , also ein Element aus  $K^\times \Rightarrow \exists! \lambda \in K^\times$ , so dass  $\lambda \tilde{f}_\alpha = f_\alpha$  normiert ist. ■

- (d)  $K[\alpha] := \text{Bild}(\varphi_\alpha) = \{f(\alpha) : f \in K[X]\} \subset L$  ist der kleinste Unterring von  $L$ , der  $K$  und  $\alpha$  enthält.
- (e)  $\alpha$  ist transzendent  $\Leftrightarrow K[\alpha] \cong K[X]$

**Beweis:**  $\alpha$  ist transzendent  $\Rightarrow \text{Kern}(\varphi_\alpha) = \{0\} \Rightarrow \varphi_\alpha$  injektiv ■

- (f) Ist  $\alpha$  algebraisch über  $K$ , so ist  $K[\alpha]$  ein Körper und  $[K[\alpha] : K] = \deg(f_\alpha)$

**Beweis:** Nach Homomorphiesatz ist  $K[\alpha] \cong K[X]/\text{Kern}(\varphi_\alpha)$ .  $\text{Kern}(\varphi_\alpha)$  ist maximales Ideal, da Primideal  $\neq (0)$  in  $K[X]$  (siehe Bew. Satz 8, Beh. 2)  $\Rightarrow K[\alpha]$  ist Körper.

$f_\alpha(\alpha) = 0$ , also  $\alpha^n + c_{n-1}\alpha^{n-1} + \dots + c_1\alpha + c_0 = 0$  mit  $c_i \in K$ ,  $c_0 \neq 0$  (da  $f_\alpha$  irreduzibel),  $\alpha(\alpha^{n-1} + \dots + c_1) = -c_0$ . Ebenso:  $1, \alpha, \alpha^2, \dots, \alpha^{n-1}$  ist  $K$ -Basis von  $K[\alpha]$ , denn ist  $\sum_{i=0}^{n-1} c_i \alpha^i = 0$  mit  $c_i \in K$ , so ist  $\sum_{i=0}^{n-1} c_i X^i \in \text{Kern} \varphi_\alpha$ , also sind alle  $c_i = 0$ , also sind  $1, \alpha, \dots, \alpha^{n-1}$  linear unabhängig. Sei  $g(\alpha) \in K[\alpha]$  für ein  $g \in K[X]$ , und schreibe  $g = q \cdot f_\alpha + r$  mit  $\text{Grad}(r) < n$ . Also ist  $g(\alpha) = r(\alpha)$  und  $r = \sum_{i=0}^{n-1} c_i X^i$ , also erzeugen  $1, \alpha, \dots, \alpha^{n-1}$  ganz  $R[\alpha]$ . ■

#### Definition 3.1.3

Sei  $L/K$  Körpererweiterung.

- (a) Für  $A \subset L$  sei  $K(A)$  der kleinste Teilkörper von  $L$ , der  $A$  und  $K$  umfaßt;  $K(A)$  heißt der **von A erzeugte Teilkörper** von  $L$ . Es ist

$$K(A) = \left\{ \frac{f(\alpha_1, \dots, \alpha_n)}{g(\alpha_1, \dots, \alpha_n)} : n \geq 1, \alpha_i \in A, f, g \in K[X_1, \dots, X_n], g \neq 0 \right\}$$

- (b)  $L/K$  heißt **einfach**, wenn es  $\alpha \in L$  gibt mit  $L = K(\alpha)$
- (c)  $L/K$  heißt **endlich erzeugt**, wenn es eine endliche Menge  $\{\alpha_1, \dots, \alpha_n\} \subset L$  gibt mit  $L = K(\alpha_1, \dots, \alpha_n)$

### Bemerkung 3.1.4

Sind  $M/L$  und  $L/K$  endlich, so auch  $M/K$  und es gilt  $[M : K] = [M : L] \cdot [L : K]$

**Beweis:** Sei  $b_1, \dots, b_m$   $K$ -Basis von  $L$  und  $e_1, \dots, e_n$   $L$ -Basis von  $M \Rightarrow B = \{e_i b_j : i = 1, \dots, n; j = 1, \dots, m\}$  ist  $K$ -Basis von  $M$ .

**denn:**  $B$  erzeugt  $M$ : Sei  $\alpha \in M$ ,  $\alpha = \sum_{i=1}^n \lambda_i e_i$  mit  $\lambda_i \in L$ ,  $\lambda_i = \sum_{j=1}^m \mu_{ij} b_j$  einsetzen  $\Rightarrow$

Behauptung.

$B$  linear unabhängig:

Ist  $\sum \mu_{ij} e_i b_j = 0$ , so ist für jedes feste  $i : \sum_{j=1}^m \mu_{ij} b_j = 0$ , da  $e_i$  über  $L$  linear unabhängig sind. Da die  $b_j$  linear unabhängig sind, sind die  $\mu_{ij} = 0$  ■

**Notation:**  $L/K$  Körpererweiterung,  $\alpha \in L$ ,  $K[\alpha] = \text{Bild}(\varphi_\alpha) = \dots$   
 $K(\alpha) = \text{Quot}(K[\alpha]) = K[\alpha]$ , falls  $\alpha$  algebraisch.

### Bemerkung 3.1.5

Für eine Körpererweiterung  $L/K$  sind äquivalent:

- (i)  $L/K$  ist endlich.
- (ii)  $L/K$  ist endlich erzeugt und algebraisch.
- (iii)  $L$  wird von endlich vielen über  $K$  algebraischen Elementen erzeugt.

**Beweis:**

**(i)  $\Rightarrow$  (ii)** Jede  $K$ -Basis in  $L$  ist auch Erzeugendensystem von  $L/K$ . Ist  $\alpha \in L$  transzendent über  $K$ , so ist  $K[\alpha] \cong K[X]$  ein unendlichdimensionaler  $K$ -Vektorraum in  $L$ , Widerspruch. Also sind alle Elemente in  $L$  algebraisch.

**(ii)  $\Rightarrow$  (iii)** ✓

**(iii)  $\Rightarrow$  (i)** Induktion über die Anzahl  $n$  der Erzeuger:

$n = 1$ :  $[K(\alpha) : K] = \text{Grad}(f_\alpha)$  nach 3.1.2 (f).

$n > 1$ :  $K(\alpha_1, \dots, \alpha_n) = K(\alpha_1, \dots, \alpha_{n-1})(\alpha_n)$ ,  $K' := K(\alpha_1, \dots, \alpha_{n-1})/K$  ist endlich nach Induktionsvoraussetzung und  $L/K'$  ist endlich nach Fall 1, also folgt aus 3.1.4  $L/K$  ist endlich.

**Beispiel:**  $\cos \frac{2\pi}{n}$  ist für jedes  $n \in \mathbb{Z} \setminus \{0\}$  algebraisch über  $\mathbb{Q}$ .

denn:

$$\cos \frac{2\pi}{n} = \Re \left( e^{\frac{2\pi i}{n}} \right) = \frac{1}{2} \left( e^{\frac{2\pi i}{n}} + \overline{e^{\frac{2\pi i}{n}}} \right) = \frac{1}{2} \left( e^{\frac{2\pi i}{n}} + e^{-\frac{2\pi i}{n}} \right)$$

$e^{\frac{2\pi i}{n}}$  ist Nullstelle von  $X^n - 1$ , also algebraisch (über  $\mathbb{Q}$ )  $\Rightarrow K = \mathbb{Q} \left( e^{\frac{2\pi i}{n}} \right)$  ist endliche Körpererweiterung von  $\mathbb{Q}$ ,  $\cos \frac{2\pi}{n} \in K \xrightarrow{3.5(i) \Rightarrow (ii)} \cos \frac{2\pi}{n}$  ist algebraisch.

$$\mathbb{Q} \subset \mathbb{Q} \left( \cos \frac{2\pi}{n} \right) \subsetneq K \quad (n \geq 3)$$

### Bemerkung 3.1.6

Seien  $K \subset L \subset M$  Körper. Sind  $M/L$  und  $L/K$  algebraisch, so auch  $M/K$

**Beweis:** Sei  $\alpha \in M$ ,  $f_\alpha = \sum_{i=0}^n c_i X^i \in L[X]$  mit  $f_\alpha(\alpha) = 0$ . Dann ist  $\alpha$  algebraisch über  $K(c_0, \dots, c_n) =: L' \subset L$ ,  $L'$  ist endlich erzeugt über  $K \xrightarrow{3.1.5} L'/K$  endlich. Außerdem ist  $L'(\alpha)/L'$  endlich.  $\xrightarrow{(b)} L'(\alpha)/K$  endlich  $\Rightarrow \alpha$  algebraisch über  $K$ . ■

## 3.2 Algebraischer Abschluss

### Proposition 3.2.1 (Kronecker)

Sei  $K$  Körper,  $f \in K[X]$ ,  $f$  nicht konstant.

Es gibt eine endliche Körpererweiterung  $L/K$ , so dass  $f$  in  $L$  eine Nullstelle hat. Genauer:  $[L : K] \leq \text{Grad } f$ .

**Beweis:**  $\mathbb{C}f$  irreduzibel. Setze  $L := K[X]/(f)$ .  $L$  ist Körper, da  $(f)$  maximales Ideal ist.  $\alpha = \bar{X} =$  Klasse von  $X$  in  $L$  ist Nullstelle von  $f$ . Genauer:  $f$  ist das Minimalpolynom von  $\alpha$ . ■

### Bemerkung 3.2.2

Ist  $f \in K[X] \setminus \{0\}$  und  $\alpha \in K$  mit  $f(\alpha) = 0$ , dann ist  $X - \alpha$  ein Teiler von  $f$ .

**Beweis:**  $\{f \in K[X] : f(\alpha) = 0\}$  ist ein Ideal im Hauptidealring  $K[X]$  und  $X - \alpha$  sein Erzeuger. ■

### Bemerkung + Definition 3.2.3

Sei  $K$  Körper,  $f \in K[X] \setminus K$

- (a) Es gibt eine endliche Körpererweiterung  $L/K$ , so dass  $f$  über  $L$  in Linearfaktoren zerfällt.

**Beweis:** Induktion über  $n = \deg(f)$ :

$n = 1$  ✓

$n \geq 1$   $L_1$  wie in Proposition 3.2.1. Dann ist  $f(X) = (X - \alpha) \cdot f_1(X)$  in  $L_1[X]$ ,  $\deg(f_1) = n - 1$ . Also gibt es  $L_2/L_1$ , so dass  $f_1(X) = \prod_{i=1}^{n-1} (X - \alpha_i)$  mit  $\alpha_i \in L_2$ . Dabei ist  $L_2/L_1$  endlich,  $L_1/K$  endlich, also  $L_2/K$  endlich. ■

- (b)  $L/K$  heißt **Zerfällungskörper** von  $f$ , wenn  $f$  über  $L$  in Linearfaktoren zerfällt, und  $L$  über  $K$  von den Nullstellen von  $f$  erzeugt wird.
- (c) Es gibt einen Zerfällungskörper  $Z(f)$ .

**Beweis:** Induktion über den Grad und die Anzahl über die irreduziblen Faktoren:

⊆ Sei  $f$  irreduzibel. Sei  $L_1 := K[X]/(f)$  und  $\alpha := \bar{X} \in L$ . Dann ist  $L_1 = K(\alpha)$  und  $f = (X - \alpha) \cdot g$  in  $L_1[X]$ . Nach Induktionsvoraussetzung gibt es einen Zerfällungskörper  $Z(g)$  von  $g$  über  $L_1$ , also wird  $Z(g)$  über  $K$  von  $\alpha$  und den Nullstellen von  $g$  erzeugt. ■

- (d) Ist  $f$  irreduzibel und  $n = \deg(f)$ , so ist  $[Z(f) : K] \leq n!$

**Beweis:** In Proposition 3.2.1 ist  $[L : K] = n = \deg(f)$  und  $f = (X - \alpha) \cdot f_1$  mit  $\deg(f_1) = n - 1$ . Mit Induktion folgt die Behauptung. ■

### Beispiel:

- (1)  $f \in K[X]$  irreduzibel vom Grad 2. Dann ist  $L = K[X]/(f)$  der Zerfällungskörper von  $f$ .  $f(X) = (X - \alpha)(X - \beta)$ ,  $\alpha, \beta \in L$ . Ist  $f(X) = X^2 + pX + q$ , so ist  $\alpha + \beta = -p$
- (2)  $f(X) = X^3 - 2 \in \mathbb{Q}[X]$ . Sei  $\alpha = \sqrt[3]{2} \in \mathbb{R}$  Nullstelle von  $f$ . In  $\mathbb{Q}(\alpha)$  liegt keine weitere Nullstelle von  $f$ , da  $\mathbb{Q}(\alpha) \subset \mathbb{R}$

$$X^3 - 2 = (X - \alpha) \underbrace{(X^2 + \alpha X + \alpha^2)}_{\text{irreduzibel über } \mathbb{Q}(\alpha)} \Rightarrow [Z(f) : \mathbb{Q}] = 6$$

$$(3) \ K = \mathbb{Q}, \ p \text{ Primzahl}, \ f(X) = X^p - 1 = (X - 1) \underbrace{(X^{p-1} + X^{p-2} + \dots + X + 1)}_{f_1}$$

$f_1$  irreduzibel (siehe 2.6.3).

$$L := \mathbb{Q}[X]/(f_1) =: \mathbb{Q}(\zeta_p); \ (\zeta_p^k)^p = \zeta_p^{pk} = 1; \ k = 1, \dots, p-1$$

$$\Rightarrow \mathbb{Q}(\zeta_p) = Z(f)$$

### Definition + Bemerkung 3.2.4

Sei  $K$  ein Körper.

- (a)  $K$  heißt **algebraisch abgeschlossen**, wenn jedes nichtkonstante Polynom  $f \in K[X]$  in  $K$  eine Nullstelle hat.
- (b) Die folgenden Aussagen sind äquivalent:
  - (i)  $K$  ist algebraisch abgeschlossen
  - (ii) Jedes  $f \in K[X] \setminus K$  zerfällt über  $K$  in Linearfaktoren
  - (iii)  $K$  besitzt keine echte algebraische Körpererweiterung.

**Beweis:**

(i)  $\Rightarrow$  (ii) Induktion über den Grad von  $f$ .

(ii)  $\Rightarrow$  (iii) Angenommen  $L/K$  algebraisch,  $\alpha \in L \setminus K$ . Dann sei  $f_\alpha \in K[X]$  das Minimalpolynom von  $\alpha$ ;  $f_\alpha$  ist irreduzibel und zerfällt in Linearfaktoren  $\Rightarrow \deg(f) = 1 \nmid$

(iii)  $\Rightarrow$  (ii) Sei  $f \in K[X]$  irreduzibel,  $L := K[X]/(f)$ , dann folgt aus der Voraussetzung  $L = K$  und damit  $\text{Grad } f = 1$ . ■

### Satz 11

Zu jedem Körper  $K$  gibt es eine algebraische Körpererweiterung  $\bar{K}/K$ , so dass  $\bar{K}$  algebraisch abgeschlossen ist.  $\bar{K}$  heißt **algebraischer Abschluss** von  $K$ .

**Beweis:**

**Hauptschritt:** Es gibt algebraische Körpererweiterung  $K'/K$ , so dass jedes nichtkonstante  $f \in K[X]$  in  $K'$  eine Nullstelle hat.

**Dann:** sei  $K'' := (K')'$  und weiter  $K^i := (K^{i-1})'$ ,  $i \geq 3$ ; Es ist  $K^i \subset K^{i+1}$ .

$L := \bigcup_{i \geq 1} K^i$ . Es gilt:

- (i)  $L$  ist Körper:  $a + b \in L$  für  $a \in K^i, b \in K^j$ , da  $\mathbb{E}: i \leq j \Rightarrow a$  auch in  $K^j$
- (ii)  $L$  ist algebraisch über  $K$ : jedes  $\alpha \in L$  liegt in einem  $K^i$ ,  $K^i$  ist algebraisch über  $K$ .
- (iii)  $L$  ist algebraisch abgeschlossen.  
**denn:** Sei  $f \in L[X]$ ,  $f = \sum_{i=0}^n c_i X^i$ ,  $c_i \in L$ . Also gibt es  $j$  mit  $c_i \in K^j$  für  $i = 0, \dots, n \Rightarrow f$  hat Nullstelle in  $(K^j)' = K^{j+1} \subset L \Rightarrow$  Behauptung

**Bew. (Hauptschritt):** Für jedes  $f \in K[X] \setminus K$  sei  $X_f$  ein Symbol.  $\mathcal{X} := \{X_f : f \in K[X] \setminus K\}$ ,  $R := K[\mathcal{X}]$ ,  $I$  sei das von allen  $f(X_f)$  in  $R$  erzeugte Ideal.

Behauptung:  $I \neq R$ .

Dann gibt es ein maximales Ideal  $\mathfrak{m} \subset R$  mit  $I \subset \mathfrak{m}$ ,  $K' := R/\mathfrak{m}$ ,  $K'$  ist Körper,  $K'/K$  ist algebraisch,

**denn:**  $K'$  wird über  $K$  erzeugt von den  $\bar{X}_f \in \mathcal{X}$  und  $f(\bar{X}_f) = 0$  in  $K'$ , weil  $f(\bar{X}_f) \in I \subset \mathfrak{m}$ .  $f$  hat in  $K'$  die Nullstellen (Klasse von)  $\bar{X}_f$ .

**Beweis der Behauptung** Angenommen  $I = R$ , also  $1 \in I$ . Dann gibt es  $n \geq 1, f_1, \dots, f_n \in K[X] \setminus K$  und  $g_1, \dots, g_n \in R$  mit  $1 = \sum_{i=1}^n g_i f_i(X_{f_i})$ . Sei  $L/K$  Körpererweiterung, in der jedes  $f_i, i = 1, \dots, n$  Nullstelle  $\alpha_i$  hat (z.B. der Zerfällungskörper von  $f_1 \cdot \dots \cdot f_n$ ).

Setze nun  $\alpha_i$  für  $X_{f_i}$  ein ( $i = 1, \dots, n$ ) (und 42 für alle anderen  $X_f$ ). Dann ist  $1 = \sum_{i=1}^n g_i(\alpha_1, \dots, \alpha_n, 42, \dots) \cdot \underbrace{f_i(\alpha_i)}_{=0} = 0 \neq 1$  ■

### 3.3 Fortsetzung von Körperhomomorphismen

Sei  $f(x) = x^2 - 2$ ,  $K = \mathbb{Q}$ ,  $L = \mathbb{Q}[X]/(f)$  und  $\alpha = \bar{X}$ , also  $f(\alpha) = 0$ . Es gibt zwei Einbettungen von  $L$  in  $\mathbb{R}$ : Schreibe  $x \in L$  als  $x = a + b\alpha$  mit  $a, b \in \mathbb{Q}$  (dies ist eindeutig), dann sind  $\varphi_1(x) := a + b\sqrt{2}$  und  $\varphi_2(x) := a - b\sqrt{2}$  Homomorphismen  $L \rightarrow \mathbb{R}$ .

#### Proposition 3.3.1

Sei  $L = K(\alpha)$ ,  $K$  Körper (also einfache Körpererweiterung). Sei  $\alpha$  algebraisch über  $K$ ,  $f = f_\alpha \in K[X]$  das Minimalpolynom. Sei  $K'$  Körper und  $\sigma : K \rightarrow K'$  ein Körperhomomorphismus. Sei  $f^\sigma$  das Bild von  $f$  in  $K'[X]$  unter dem Homomorphismus  $K[X] \rightarrow K'[X]$ ,  $\sum a_i X^i \mapsto \sum \sigma(a_i) X^i$ . Dann gilt:

- (a) Ein Homomorphismus  $\tilde{\sigma} : L \rightarrow K'$  heißt **Fortsetzung** von  $\sigma$ , wenn  $\tilde{\sigma}(a) = \sigma(a)$  für alle  $a \in K$  gilt.





### 3.3 Fortsetzung von Körperhomomorphismen

Wohldefiniert: ist  $x \in L''$ , so ist  $\mathfrak{C}(L', \tau) \subseteq (L'', \tau'')$  und damit  $\tau''(x) = \tau(x)$ .  
 $\Rightarrow (\tilde{L}, \tilde{\tau})$  ist obere Schranke  $\xrightarrow{\text{Zorn}} \mathcal{M}$  hat maximales Element  $(\tilde{L}, \tilde{\sigma})$

**Zu zeigen:**  $\tilde{L} = L$ . Sonst sei  $\alpha \in L \setminus \tilde{L}$  und  $\sigma'$  Fortsetzung von  $\tilde{\sigma}$  auf  $\tilde{L}(\alpha)$  (nach 3.3.1)  
 $\Rightarrow (\tilde{L}(\alpha), \sigma') \in \mathcal{M}$  und  $(\tilde{L}, \tilde{\sigma}) \subsetneq (\tilde{L}(\alpha), \sigma') \nmid$  ■

#### Folgerung 3.3.4

Für jeden Körper  $K$  ist der algebraische Abschluss  $\bar{K}$  bis auf Isomorphie eindeutig bestimmt.

**Beweis:** Seien  $\bar{K}$  und  $C$  algebraische Abschlüsse von  $K$ . Nach Proposition 3.3.3 gibt es

Körperhomomorphismus  $\sigma : \bar{K} \rightarrow C$ , der  $\text{id}_K$  fortsetzt. Dann ist  $\sigma(\bar{K})$  auch algebraisch abgeschlossen: ist  $f = \sum_{i=0}^n a_i X^i \in \sigma(\bar{K})[X] \Rightarrow f^{\sigma^{-1}} = \sum_{i=0}^n \sigma^{-1}(a_i) X^i \in \bar{K}[X]$  hat Nullstelle  $\alpha \in \bar{K}$ .  
 $\Rightarrow \sigma(\alpha)$  ist Nullstelle von  $f$ :

$$\sum \sigma^{-1}(a_i) \alpha^i = 0 \Rightarrow 0 = \sigma(\sum \sigma^{-1}(a_i) \alpha^i) = \sum a_i \sigma(\alpha^i) = \sum a_i \sigma(\alpha)^i$$

$C$  ist algebraisch über  $K$ , also erst recht über  $\sigma(\bar{K}) \xrightarrow{3.2.4} \sigma(\bar{K}) = C$  ■

#### Definition + Bemerkung 3.3.5

Seien  $L/K, L'/K$  Körpererweiterungen von  $K$ .

(a)

$$\text{Hom}_K(L, L') := \{\sigma : L \rightarrow L' \text{ Körperhomomorphismus, } \sigma|_K = \text{id}_K\}$$

$$\text{Aut}_K(L) := \{\sigma : L \rightarrow L \text{ Körperautomorphismus, } \sigma|_K = \text{id}_K\}$$

(b) Ist  $L/K$  endlich,  $\bar{K}$  algebraischer Abschluss von  $K$ , so ist  $|\text{Hom}_K(L, \bar{K})| \leq [L : K]$ .

**Beweis:** Sei  $L = K(\alpha_1, \dots, \alpha_n)$ ,  $\alpha_i$  algebraisch über  $K$ . Induktion über  $n$ :

$n = 1$  Sei  $f \in K[X]$  das Minimalpolynom von  $\alpha_1$ . Für jedes  $\sigma \in \text{Hom}_K(L, \bar{K})$  ist  $\sigma(\alpha_1)$  Nullstelle von  $f^\sigma \in \bar{K}[X]$ . Durch  $\sigma|_K = \text{id}_K$  und  $\sigma(\alpha_1)$  ist  $\sigma$  eindeutig bestimmt.  $\Rightarrow |\text{Hom}_K(L, \bar{K})| = |\text{Nullstellen von } f^\sigma| \leq \deg(f^\sigma) = [L : K]$

$n > 1$  Sei  $L_1 = K(\alpha_1, \dots, \alpha_{n-1})$ ,  $f \in L_1[X]$  das Minimalpolynom von  $\alpha_n$  über  $L_1$ . Für  $\sigma \in \text{Hom}_K(L, \bar{K})$  ist  $\sigma(\alpha_n)$  Nullstelle von  $f^{\sigma_1} \in \bar{K}[X]$  mit  $\sigma_1 = \sigma|_{L_1} \Rightarrow |\text{Hom}_K(L, \bar{K})| \leq |\text{Hom}_K(L_1, \bar{K})| \cdot \deg(f) \stackrel{\text{IV}}{\leq} [L_1 : K] \cdot [L : L_1] \stackrel{3.1.6(b)}{=} [L : K]$  ■

### 3.4 Separable Körpererweiterungen

#### Definition + Bemerkung 3.4.1

Sei  $L/K$  algebraische Körpererweiterung und  $\bar{K}$  algebraischer Abschluss von  $K$ .

- (a)  $f \in K[X]$  heißt **separabel**, wenn  $f$  in  $\bar{K}$  keine mehrfache Nullstelle hat (also  $\deg(f)$  verschiedene Nullstellen).
- (b)  $\alpha \in L$  heißt separabel, wenn das Minimalpolynom von  $\alpha$  über  $K$  separabel ist.
- (c)  $L/K$  heißt separabel, wenn jedes  $\alpha \in L$  separabel ist.
- (d)  $f \in K[X] \setminus K$  ist genau dann separabel, wenn  $\text{ggT}(f, f') = 1$ . Dabei ist für  $f = \sum_{i=0}^n a_i X^i$  die **Ableitung** definiert durch  $f' := \sum_{i=1}^n i a_i X^{i-1}$

**Beweis:** Sei  $f(X) = \prod_{i=1}^n (X - \alpha_i)$ ,  $\alpha_i \in \bar{K} \Rightarrow f'(X) = \sum_{i=1}^n \prod_{j \neq i} (X - \alpha_j)$  nach Definition ist  $f$  separabel  $\Leftrightarrow \alpha_i \neq \alpha_j$  für  $i \neq j$ .

**Beh.:**  $\alpha_1 = \alpha_i$  für ein  $i \geq 2 \Leftrightarrow (X - \alpha_1) \mid f'$

Aus der Behauptung folgt:  $f$  separabel  $\Leftrightarrow f$  und  $f'$  teilerfremd in  $\bar{K}[X]$ . Ist das so, dann ist  $\text{ggT}(f, f') = 1$  (teilerfremd in  $K[X]$ ). Ist umgekehrt  $\text{ggT}(f, f') = 1$ , so gibt es  $g, h \in K[X]$  mit  $1 = gf + hf'$ .

Das stimmt dann auch in  $\bar{K}[X]$ , also sind  $f$  und  $f'$  in  $\bar{K}[X]$  teilerfremd.

**Bew. der Beh.:**  $(X - \alpha_1)$  teilt  $\prod_{j \neq 1} (X - \alpha_j)$ , falls  $i \neq 1$ . Also gilt  $X - \alpha_1$  teilt  $f' \Leftrightarrow X - \alpha_1$  Teiler von  $\prod_{j \neq 1} (X - \alpha_j) \Leftrightarrow \alpha_1 = \alpha_j$  für ein  $j \neq 1$ . ■

- (e) Ist  $f \in K[X]$  irreduzibel, so ist  $f$  separabel genau dann, wenn  $f' \neq 0$  (Nullpolynom) ist.

**Beweis:** Ist  $f' = 0$ , so ist  $\text{ggT}(f, f') = f \neq 1$

Ist  $f' \neq 0$ , so ist  $\deg f' < \deg f$ ; ist  $f$  irreduzibel und  $\alpha \in \bar{K}$  Nullstelle von  $f$ , so ist  $f$  das Minimalpolynom von  $\alpha \xrightarrow{f' \neq 0} \alpha$  nicht Nullstelle von  $f' \Rightarrow \text{ggT}(f, f') = 1$  ■

#### Folgerung 3.4.2

Ist  $\text{char}(K) = 0$ , so ist jede algebraische Körpererweiterung separabel.

### Beispiele 3.4.3

Sei  $p$  Primzahl,  $K = \mathbb{F}_p(t) = \text{Quot}(\mathbb{F}_p[t])$ . Sei  $f(X) = X^p - t \in K[X]$ .

$f'(X) = pX^{p-1} = 0$ ,  $t \in \mathbb{F}_p[t]$  ist Primelement  $\xRightarrow{\text{Eisenstein}} f$  irreduzibel in  $(\mathbb{F}_p[t])[X] \xrightarrow{??} f$  irreduzibel in  $K[X]$

$f(X) = X^p - a \in \mathbb{F}_p \Rightarrow f' = 0$ ,  $f$  ist nicht irreduzibel, da  $f$  Nullstelle in  $\mathbb{F}_p$  hat, dh. es gibt ein  $b \in \mathbb{F}_p$  mit  $b^p = a$ .

Denn:  $\varphi : \mathbb{F}_p \rightarrow \mathbb{F}_p, b \mapsto b^p$  ist Körperhomomorphismus! (denn  $(a+b)^p = a^p + b^p$ )

### Proposition 3.4.4

Sei  $\text{char}(K) = p > 0$ ,  $f \in K[X]$  irreduzibel,  $\bar{K}$  ein algebraischer Abschluss von  $K$ .

- (a) Es gibt ein separables irreduzibles Polynom  $g \in K[X]$ , so dass  $f(X) = g(X^{p^r})$  für ein  $r \geq 0$ .
- (b) Jede Nullstelle von  $f$  in  $\bar{K}$  hat Vielfachheit  $p^r$ .

**Beweis:** Sei  $f$  nicht separabel,  $f = \sum_{i=0}^n a_i X^i$ ,  $f' = \sum_{i=1}^n i a_i X^{i-1} = 0 \Rightarrow i a_i = 0$  für  $i = 1, \dots, n \Rightarrow a_i = 0$ , falls  $i$  nicht durch  $p$  teilbar  $\Rightarrow f$  ist Polynom in  $X^p$ , dh.  $f = g_1(X^p)$ . Mit Induktion folgt die Behauptung. ■

### Proposition + Definition 3.4.5

Sei  $L/K$  endliche Körpererweiterung,  $\bar{K}$  algebraischer Abschluss von  $L$ .

- (a)  $[L : K]_s := |\text{Hom}_K(L, \bar{K})|$  heißt **Separabilitätsgrad** von  $L$  über  $K$ .
- (b) Ist  $L'$  Zwischenkörper von  $L/K$ , so ist  $[L : K]_s = [L : L']_s \cdot [L' : K]_s$
- (c)  $L/K$  ist separabel  $\Leftrightarrow [L : K] = [L : K]_s$
- (d) Ist  $\text{char}(K) = p > 0$ , so gibt es ein  $r \in \mathbb{N}$  mit  $[L : K] = p^r \cdot [L : K]_s$

#### Beweis:

- (b) Sei  $\text{Hom}_K(L', \bar{K}) = \{\sigma_1, \dots, \sigma_n\}$ ,  $\text{Hom}_{L'}(L, \bar{K}) = \{\tau_1, \dots, \tau_m\}$ . Sei  $\tilde{\sigma}_i : \bar{K} \rightarrow \bar{K}$  Fortsetzung von  $\sigma_i$ ,  $i = 1, \dots, n$ . Dann ist  $\tilde{\sigma}_i \in \text{Aut}_K(\bar{K})$ .

**Beh.:**

(1)  $\text{Hom}_K(L, \bar{K}) = \{\tilde{\sigma}_i \circ \tau_j : i = 1, \dots, n, j = 1, \dots, m\}$

(2)  $\tilde{\sigma}_i \circ \tau_j = \tilde{\sigma}_{i'} \circ \tau_{j'} \Leftrightarrow i = i' \text{ und } j = j'$ .

Aus (1) und (2) folgt (b).

**Bew.(1):** " $\supseteq$ " ✓ " $\subseteq$ ": Sei  $\sigma \in \text{Hom}_K(L, \bar{K})$ . Dann gibt es ein  $i$  mit  $\sigma|_{L'} = \sigma_i \Rightarrow \tilde{\sigma}_i^{-1} \circ \sigma|_{L'} = \text{id}_{L'} \Rightarrow \exists j$  mit  $\tilde{\sigma}_i^{-1} \circ \sigma = \tau_j \Rightarrow \sigma = \tilde{\sigma}_i \circ \tau_j$ .

**Bew.(2):** Sei  $\tilde{\sigma}_i \circ \tau_j = \tilde{\sigma}_{i'} \circ \tau_{j'} \Rightarrow \underbrace{\tilde{\sigma}_i|_{L'}}_{=\sigma_i} = \underbrace{\tilde{\sigma}_{i'}|_{L'}}_{=\sigma_{i'}} \Rightarrow i = i' \Rightarrow \tau_j = \tau_{j'} \Rightarrow j = j'$ .

(c) " $\Rightarrow$ ": Sei  $L = K(\alpha_1, \dots, \alpha_n)$ . Induktion über  $n$ :

**n=1**  $L = K(\alpha)$ ,  $f = f_\alpha \in K[X]$  das Minimalpolynom von  $\alpha$  über  $K \Rightarrow [L : K]_s \stackrel{3.3.5}{=} |\{\text{Nullstellen von } f \text{ in } \bar{K}\}| = \deg f = [L : K]$ .

**n>1**  $L_1 := K(\alpha_1, \dots, \alpha_{n-1})$ ,  $f \in L_1[X]$  das Minimalpolynom von  $\alpha_n$ . Zu jedem  $\sigma_1 \in \text{Hom}_K(L_1, \bar{K})$  und jeder Nullstelle von  $f$  in  $\bar{K}$  gibt es genau eine Fortsetzung  $\tilde{\sigma}_1 : L \rightarrow \bar{K}$ .

$$\begin{aligned} \xRightarrow{f \text{ separabel}} [L : K]_s &= |\text{Hom}_K(L, \bar{K})| = \deg(f) \cdot |\text{Hom}_K(L_1, \bar{K})| = [L : L_1] \cdot \\ &[L_1 : K]_s \stackrel{\text{IV}}{=} [L : L_1] \cdot [L_1 : K] = [L : K]. \end{aligned}$$

" $\Leftarrow$ ": Ist  $\text{char}(K) = 0$ , so ist  $L/K$  separabel. Sei also  $\text{char}(K) = p > 0$  und  $\alpha \in L$ ;  $f \in K[X]$  das Minimalpolynom von  $\alpha$ . Nach 3.4.4 gibt es  $r \geq 0$  und ein separables, irreduzibles Polynom  $g \in K[X]$  mit  $f(X) = g(X^{p^r}) \Rightarrow [K(\alpha) : K]_s = |\{\text{Nullstellen von } g \text{ in } \bar{K}\}| \stackrel{g \text{ separabel}}{=} \deg(g) \cdot (*) \Rightarrow [K(\alpha) : K] = \deg(f) = p^r \cdot \deg(g) = p^r \cdot [K(\alpha) : K]_s \Rightarrow [L : K] = [L : K(\alpha)] \cdot [K(\alpha) : K] \geq [L : K(\alpha)]_s \cdot p^r [K(\alpha) : K]_s \stackrel{(b)}{=} [L : K]_s \stackrel{\text{Voraussetzung}}{\Rightarrow} p^r = 1 \Rightarrow g = f \Rightarrow \alpha \text{ separabel.}$

(d) folgt aus (\*) ■

## Satz 12 (Satz vom primitiven Element)

Jede endliche separable Körpererweiterung  $L/K$  ist einfach, also gibt es  $\alpha \in L$  mit  $L = K(\alpha)$ .  $\alpha$  heißt **primitives Element**.

**Beweis:** Ist  $K$  endlich, so folgt aus 3.5.1, dass  $L^\times$  zyklische Gruppe ist. Ist  $L^\times = \langle \alpha \rangle$ , so ist  $L = K[\alpha]$ .

Sei also  $K$  unendlich,  $L = K(\alpha_1, \dots, \alpha_r)$ .  $\exists$ :  $r = 2$ , also  $L = K(\alpha, \beta)$ . Sei  $\bar{K}$  algebraischer Abschluss von  $K$ ,  $[L : K] = n$ . Sei  $\text{Hom}_K(L, \bar{K}) = \{\sigma_1, \dots, \sigma_n\}$  (3.4.5(c)).

Sei  $g(X) := \prod_{1 \leq i < j \leq n} (\sigma_i(\alpha) - \sigma_j(\alpha)) + (\sigma_i(\beta) - \sigma_j(\beta))X \in \bar{K}[X]$ ,  $g \neq 0$ , denn aus  $\sigma_i(\alpha) = \sigma_j(\alpha)$  und  $\sigma_i(\beta) = \sigma_j(\beta)$  folgt  $\sigma_i = \sigma_j$ . Da  $K$  unendlich ist, gibt es  $\lambda \in K$  mit  $g(\lambda) \neq 0$ .

**Beh.:**  $\gamma := \alpha + \lambda\beta \in L$  erzeugt  $L$  über  $K$ .

**denn:** Sei  $f \in K[X]$  das Minimalpolynom von  $\gamma$  über  $K$ . Für jedes  $i$  ist  $f(\sigma_i(\gamma)) \stackrel{\sigma_i|_K = \text{id}_K}{=} \sigma_i(f(\gamma))$ . Angenommen,  $\sigma_i(\gamma) = \sigma_j(\gamma)$  für ein  $i \neq j$ . Dann wäre  $(\sigma_i(\alpha) + \sigma_i(\beta)\lambda) - (\sigma_j(\alpha) + \sigma_j(\beta)\lambda) = 0 \Rightarrow g(\lambda) = 0 \nmid \Rightarrow f$  hat mindestens  $n$  Nullstellen  $\Rightarrow \deg(f) = [K(\gamma) : K] \geq n = [L : K]$ , da  $\gamma \in L$ , folgt  $K(\gamma) = L$ . ■

### 3.5 Endliche Körper

#### Proposition 3.5.1

Ist  $K$  ein Körper, so ist jede endliche Untergruppe von  $(K^\times, \cdot)$  zyklisch.

**Beweis:** Sei  $G \subseteq K^\times$  endliche Untergruppe,  $a \in G$  ein Element maximaler Ordnung. Sei  $n = \text{ord}(a)$ ,  $G_n := \{b \in G : \text{ord}(b) \mid n\}$ .

**Beh.:**  $G_n = \langle a \rangle$

**denn:** jedes  $b \in G_n$  ist Nullstelle von  $X^n - 1$ . Diese sind  $1, a, a^2, \dots, a^{n-1} \Rightarrow |G_n| = |\langle a \rangle| = n$ .

Nach Folgerung 1.4.5 ist  $G \cong \bigoplus_{i=1}^r \mathbb{Z}/a_i\mathbb{Z}$  mit  $a_i \mid a_{i+1} \Rightarrow$  Für jedes  $b \in G$  ist  $\text{ord}(b)$  Teiler von  $a_r = n$ . ■

#### Definition + Bemerkung 3.5.2

Sei  $K$  Körper mit Charakteristik  $p > 0$ .

- (a) Dann ist die Abbildung  $\varphi : K \rightarrow K, x \mapsto x^p$  ein Homomorphismus. Er heißt **Frobenius**-Homomorphismus.
- (b) Es ist  $\varphi(x) = x \iff x \in \mathbb{F}_p$  (als Primkörper in  $K$ ).

#### Satz 13

Sei  $p$  Primzahl,  $n \geq 1, q = p^n$ . Sei  $\mathbb{F}_q$  der Zerfällungskörper von  $X^q - X \in \mathbb{F}_p[X]$ .

Dann gilt:

- (a)  $\mathbb{F}_q$  hat  $q$  Elemente.
- (b) Zu jedem endlichen Körper  $K$  gibt es ein  $q = p^n$  mit  $K \cong \mathbb{F}_q$

**Beweis:**

- (a)  $f(X) = X^q - X$  ist separabel, da  $f'(X) = -1 \Rightarrow \text{ggT}(f, f') = 1 \Rightarrow f$  hat  $q$  verschiedene Nullstellen in  $\mathbb{F}_q \Rightarrow |\mathbb{F}_q| \geq q$ .

Umgekehrt: Jedes  $a \in \mathbb{F}_q$  ist Nullstelle von  $f$ .

**denn:**  $\mathbb{F}_q$  wird erzeugt von den Nullstellen von  $f$ . Sind also  $a, b$  Nullstellen von  $f$ , so ist  $a^q = a, b^q = b$ , also auch  $(ab)^q = ab, (a+b)^q = a^q + b^q = a + b$ .

- (b)  $(K^\times, \cdot)$  ist Gruppe der Ordnung  $q - 1 \Rightarrow$  Für jedes  $a \in K$  gilt  $a^q = a \Rightarrow$  Jedes  $a \in K$  ist Nullstelle von  $X^q - X \Rightarrow K$  liegt im Zerfällungskörper von  $X^q - X \Rightarrow K$  enthält  $\mathbb{F}_q$  (bis auf Isomorphie).

$$|K| = |\mathbb{F}_q| = q \Rightarrow K \cong \mathbb{F}_q$$

### Folgerung 3.5.3

Jede algebraische Erweiterung eines endlichen Körpers ist separabel.

**Beweis:**  $\mathbb{F}_q/\mathbb{F}_p$  separabel, da  $X^q - X$  separables Polynom ist. Ist  $K$  endlich, also  $K = \mathbb{F}_q$ ,  $L/K$  algebraisch,  $\alpha \in L$ , so ist  $K(\alpha)/K$  endlich, also separabel (da  $K(\alpha) = \mathbb{F}_{q^r}$  für ein  $r \geq 1$ )

**Definition:** Ein Körper  $K$  heißt **vollkommen** (oder perfekt), wenn jede algebraische Körpererweiterung  $L/K$  separabel ist.

## 3.6 Konstruktion mit Zirkel und Lineal

**Aufgabe:** Sei  $M \subset \mathbb{C} = \mathbb{R}^2$ , z.B.:  $M = \{0, 1\}$ .

Linien:  $\mathcal{L}(M) := \{L \subset \mathbb{R}^2 \text{ Gerade: } |L \cap M| \geq 2\} \cup \{K_{z_1-z_2}(z_3) : z_1, z_2, z_3 \in M\}$

$(K_r(z) = \{y \in \mathbb{R}^2 : |z - y| = r\})$

$K_1(M) := \{z \in \mathbb{C} : z \text{ liegt auf zwei verschiedenen Linien in } \mathcal{L}(M)\}$

$K_n(M) := K_1(K_{n-1}(M))$  für  $n \geq 2$

$K(M) := \bigcup_{n=1}^{\infty} K_n(M)$

### Satz 14

Sei  $M \subseteq \mathbb{R}^2$  mit  $0, 1 \in M$  und  $K(M)$  die Menge der mit Zirkel und Lineal konstruierbaren Punkte.

- (a)  $K(M)$  ist ein Teilkörper von  $\mathbb{C}$ .
- (b)  $K(M)/\mathbb{Q}(M)$  ist eine algebraische Körpererweiterung, dabei sei  $\mathbb{Q}(M)$  der kleinste Teilkörper von  $\mathbb{C}$ , der  $\mathbb{Q}$  und  $M$  umfasst und mit  $a$  auch  $\bar{a}$  enthält.
- (c) Eine komplexe Zahl  $a \in \mathbb{C}$  liegt genau dann in  $K(M)$ , wenn es eine Kette

$$\mathbb{Q}(M) = L_0 \subset L_1 \subset \cdots \subset L_n$$

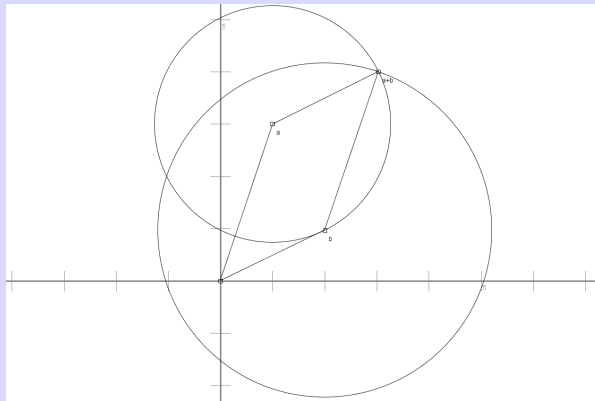
gibt mit  $a \in L_n$  und  $[L_i : L_{i-1}] = 2$  für  $i = 1, \dots, n$ .

**Beweis:**

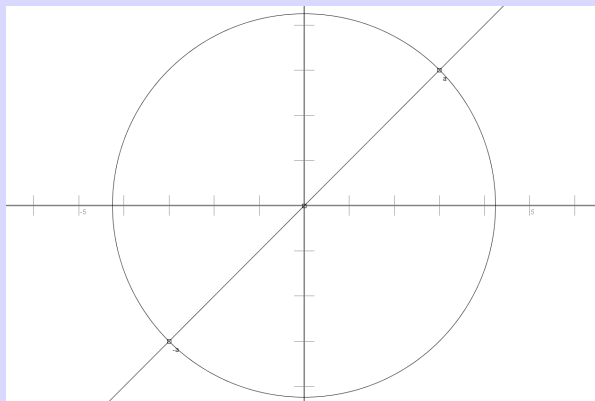
- (a) Seien  $a, b \in K(M)$ . Zu zeigen:  $a + b, -a, a \cdot b, \frac{1}{a} \in K(M)$ .

$a + b \in K(M)$  :

### 3.6 Konstruktion mit Zirkel und Lineal



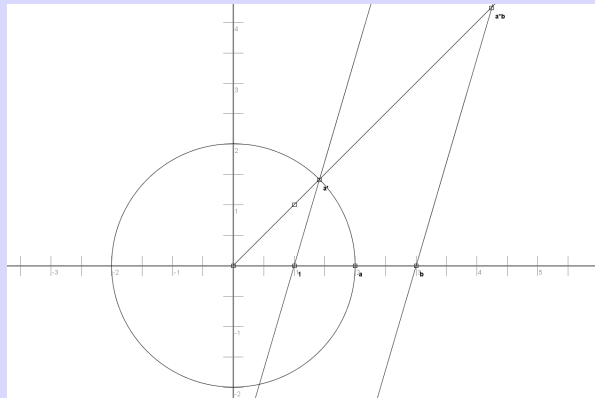
$-a \in K(M)$  :



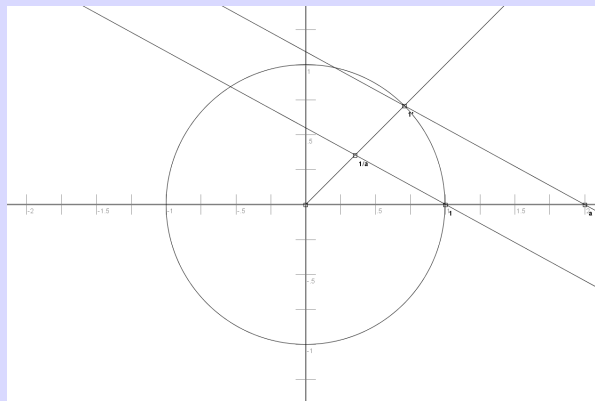
$a \cdot b \in K(M)$  :

Strahlensatz:  $\frac{1}{a} = \frac{b}{x}$ , also  $x = a \cdot b$ . Winkel addieren ✓  $\Rightarrow a \cdot b$  allgemein ✓

### 3 Algebraische Körpererweiterungen



$$\frac{1}{a} \in K(M) : \exists a \in \mathbb{R}$$



(b) folgt aus (a)

(c) Zeige mit Induktion über  $n$ : Jedes  $a \in K_n(M)$  ist algebraisch über  $\mathbb{Q}(M)$ . Wegen  $K_n(M) = K_1(\mathcal{L}_n(M))$  genügt es, die Behauptung für  $n = 1$  zu zeigen. Sei also  $z \in K_1(M)$ .

Vorüberlegung: Für  $z \in M$  ist  $\Re(z) = \frac{1}{2}(z + \bar{z}) \in \mathbb{Q}(M)$  und  $\Im(z) = \frac{1}{2}(z - \bar{z}) \in \mathbb{Q}(M)$ .

- a)  $z$  ist Schnittpunkt zweier Geraden in  $\mathcal{L}(M) \Rightarrow z$  ist Lösung zweier linearer Gleichungen  $z_1 + \lambda z_2 = z'_1 + \mu z'_2$
- b)  $z$  ist Schnittpunkt einer Geraden und eines Kreises:  $\Rightarrow$  quadratische Gleichung mit Koeffizienten in  $\mathbb{Q}(M)$



c)  $z$  ist Schnittpunkt zweier Kreise  $K_{r_1}(m_1)$  und  $K_{r_2}(m_2)$  mit Mittelpunkten  $m_1, m_2 \in M$ . Radien:  $r_1 = |z_1 - z'_1|$ ,  $r_2 = \dots$  also  $r_1^2 = (z_1 - z'_1)(\overline{z_1 - z'_1}) \in \mathbb{Q}(M)$ .

Dann ist  $|z - m_1|^2 = r_1^2$ .

$$\Rightarrow z\bar{z} - (z\bar{m}_1 + \bar{z}m_1) = r_1^2 - m_1\bar{m}_1 \text{ und } z\bar{z} - (z\bar{m}_2 + \bar{z}m_2) = r_2^2 - m_2\bar{m}_2 \Rightarrow 2\Re[z(\bar{m}_1 - \bar{m}_2)] = r_1^2 - r_2^2 - (m_1\bar{m}_1 - m_2\bar{m}_2)$$

Das ist eine lineare Gleichung, die  $\Re(z)$  und  $\Im(z)$  enthält. Einsetzen in (1) ergibt quadratische Gleichung für  $\Re(z)$  (mit Koeffizienten in  $\mathbb{Q}(M)$ ).

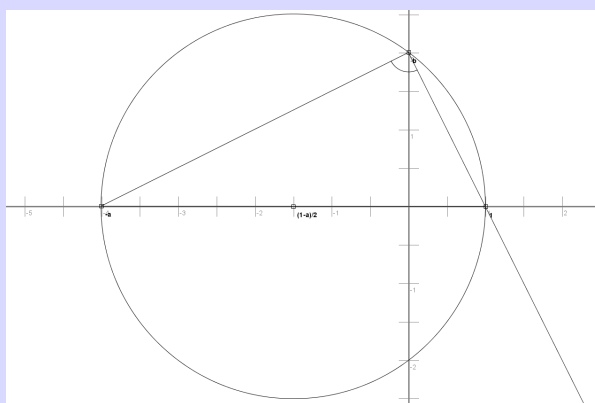
Noch zu zeigen: Ist  $a \in \mathbb{C}$  und gibt es eine Kette

$$\mathbb{Q}(M) = L_0 \subset L_1 \subset \dots \subset L_n$$

von Körpererweiterungen mit  $[L_i : L_{i-1}] = 2$  und  $a \in L_n$ , so ist  $a \in K(M)$ .

Sei also  $L/K$  quadratische Erweiterung von Körpern (mit Charakteristik ungleich 2). Dann gibt es  $\alpha \in L$  und  $a \in K$ , so dass  $L = K(\alpha)$  und  $\alpha^2 = a$ , das heißt  $L = K(\sqrt{a})$ . Zu zeigen ist also: Ist  $K \subset K(M)$ , so ist  $\sqrt{a} \in K(M)$ :

Wurzelziehen:  $a \in \mathbb{R}$



$\xRightarrow{\text{Thales}}$  Winkel ist rechtwinklig  $\xRightarrow{\text{Höhensatz}} b^2 = |-a| \cdot 1 = a$  ■

**Beispiel:** Das regelmäßige Fünfeck ist aus 0 und 1 konstruierbar. Ziel: Konstruiere Nullstellen von  $X^5 - 1 = (X - 1) \cdot f$ ,  $f := X^4 + X^3 + X^2 + X + 1$ . Trick von Lagrange:  $f(X) = X^2(X^2 + \frac{1}{X^2} + X + \frac{1}{X} + 1)$ . Mit  $Y := X + \frac{1}{X}$  ist dann  $\frac{1}{X^2} \cdot f(X) = Y^2 + Y - 1 =: g(Y)$ . Ist  $y$  Nullstelle von  $g$  und  $\xi$  Nullstelle von  $f$ , so ist  $\mathbb{Q} \subset \mathbb{Q}(y) \subset \mathbb{Q}(\xi)$  eine Kette wie im Satz.

