

0.1 Grundlagen

Definition (Körper). $K = (K, 0_K, 1_K, +, \cdot)$ ist Körper $\iff K$ ist ein kommutativer Ring und $(K \setminus \{0\}, 1_K, \cdot)$ ist eine Gruppe ($0_K \neq 1_K$).

Bemerkung. Im weiteren seien K, K' stets Körper.

Definition 0.1 (Unterkörper/Oberkörper). (i) $L \subseteq K$ heißt Unterkörper : $\iff L$ ist ein Unterring und L ist ein Körper.

(ii) $E \supseteq K$ heißt Oberkörper : $\iff E$ ist ein Körper und $K \subseteq E$ ist ein Unterkörper.

Bemerkung 0.2 (Übung). Sind $(K_i)_{i \in I}$ Unterkörper von K , so ist $\bigcap_{i \in I} K_i$ ein Unterkörper von K .

Definition 0.3 (Körperhomomorphismus). Eine Abbildung $\varphi : K \rightarrow K'$ heißt Körperhomomorphismus : $\iff \varphi$ ist ein Ringhomomorphismus (der Ringe $K \rightarrow K'$)

Bemerkung 0.4. Sei R ein Ring mit $0_R \neq 1_R$ und $\varphi : K \rightarrow R$ ein Ringhomomorphismus, dann:

(a) $\text{Kern}(\varphi) = \{0\}$ ($\implies \varphi$ ist injektiv)

(b) R ist ein K -Vektorraum (vermöge φ) durch

$$\cdot : K \times R \rightarrow R, (\alpha, r) \mapsto \varphi(\alpha) \cdot r, \quad + : R \times R \rightarrow R := +_R$$

Beweis. (a) Nur zu zeigen: $\text{Kern}(\varphi) \subsetneq K$. Dies ist klar wegen $\varphi(1_K) = 1_R \neq 0_R$. (einzige Ideale von K sind $\{0\}, K$)

(b) Übung. □

Proposition 0.5 (Primkörper). Jeder Körper K enthält einen kleinsten Unterkörper $K_0 \subseteq K$, der sogenannte **Primkörper** von K : es gilt:

$$K_0 \cong \begin{cases} \mathbb{Q}, & \text{char}(K) = 0, \\ \mathbb{F}_p, & \text{char}(K) = p > 0. \end{cases}$$

Beweis.

- Existenz: Nach Bemerkung 2 ist $K_0 := \bigcap_{L \subseteq K \text{ Unterkörper}} L$ ein Körper, sicher auch der kleinste.
- Isomorphietyp: betrachte $\varphi : \mathbb{Z} \rightarrow K, n \mapsto n \cdot 1_K$
 - Fall 1: $\text{Kern}(\varphi) \supsetneq \{0\}$: Hatten schon gesehen $\text{Kern}(\varphi) = p\mathbb{Z}$ für $p = \text{char}(K)$. Homomorphiesatz gibt Isomorphismus

$$\underbrace{\mathbb{Z}/p\mathbb{Z}}_{\text{Körper}} \xrightarrow{\cong} \text{Bild}(\varphi) \underbrace{\subseteq}_{\text{Unterring}} K \implies \text{Unterkörper}.$$

$\text{Bild}(\varphi) \subseteq K_0$, denn $1_K \in K_0$ und also $\mathbb{Z} \cdot 1_K \subseteq K_0 \implies \text{Bild}(\varphi) = K_0$ ist der kleinste $\implies K_0 \cong \mathbb{Z}/p\mathbb{Z} \cong \mathbb{F}_p$.

- Fall 2: $\text{Kern}(\varphi) = \{0\}$, d.h. φ ist injektiv, und es gilt $\text{char}(K) = 0$.
Beachte:

$$\underbrace{\varphi(\mathbb{Z} \setminus \{0\})}_S \subseteq_{\varphi \text{ inj. Hom.}} K_0 \setminus \{0\} \subseteq K \setminus \{0\}$$

universelle Eigenschaft der Lokalisierung (S multiplikativ abgeschlossen, $\varphi(S) \subseteq K^\times$) $\implies \exists!$ Ringhomomorphismus $\widehat{\varphi} : S^{-1}\mathbb{Z} = \mathbb{Q} \rightarrow K_0$,
der φ fortsetzt; und $\widehat{\varphi}\left(\frac{a}{b}\right) = \varphi(a)\varphi(b)^{-1}$, $a, b \in \mathbb{Z}, b \neq 0$. Erhalten:

$\widehat{\varphi}$ gibt Isomorphismus $\mathbb{Q} \xrightarrow{\cong} \widehat{\varphi}(\mathbb{Q}) \subseteq_{\text{Unterkörper}} K_0, K_0 \text{ minimal} \implies \widehat{\varphi}$
ist Isomorphismus $\mathbb{Q} \cong K_0$. \square

Definition 0.6. Sei $E \supseteq K$ ein Oberkörper. Der **Grad** von E über K ist die Vektorraumdimension.

$$[E : K] := \dim_K E \in \mathbb{N} \cup \{\infty\}$$

Satz 0.7. Sei $E \supseteq K$ ein Oberkörper und V ein E -Vektorraum, dann gilt:
 $\dim_K V = [E : K] \dim_E V$.

Beweis. Sei $B = (b_i)_{i \in I}$ eine Basis von E als K -Vektorraum, $C = (c_j)_{j \in J}$ eine Basis von V als E -Vektorraum.

- Behauptung: $D = (b_i c_j)_{(i,j) \in I \times J}$ ist eine Basis von V als K -Vektorraum
($\implies \dim_K V = \#(I \times J) = \#I \#J = [E : K] \dim_E V$).
- Dazu: D ist Erzeugendensystem (von V als K -Vektorraum) Sei $v \in V$,
schreibe $v = \sum_{j \in J} \lambda_j c_j$, ($\lambda_j \in E$). Für jedes j schreibe

$$\lambda_j = \sum_{i \in I} \mu_{ij} b_i \implies v = \sum_{j \in J} \left(\sum_{i \in I} \mu_{ij} b_i \right) c_j = \sum_{(i,j) \in I \times J} \mu_{ij} (b_i c_j).$$

- D ist linear unabhängig (über K): Seien $\beta_{ij} \in K$ für alle $(i,j) \in I \times J$
(nur endlich viele $\neq 0$), sodass

$$0 = \sum_{(i,j) \in I \times J} \beta_{ij} b_i c_j = \sum_{j \in J} \underbrace{\left(\sum_{i \in I} \beta_{ij} b_i \right)}_{\in E} \cdot \underbrace{c_j}_{\text{bilden } E\text{-Basis von } V}$$

$$\implies \forall j \in J : \sum_{i \in I} \underbrace{\beta_{ij}}_{\in K} \cdot \underbrace{b_i}_{\text{bilden } K\text{-Basis von } E} = 0.$$

$$\implies \forall j \in J \forall i \in I : \beta_{ij} = 0. \quad \square$$

Korollar 0.8 (Gradformel für Körpertürme). Seien $L \supseteq E$ und $E \supseteq K$ Oberkörper. Dann ist $L \supseteq K$ ein Oberkörper und

$$[L : K] = [L : E] \cdot [E : K]$$

Beweis. (der Formel)

$$[L : K] = \dim_K L \stackrel{\text{Satz 7}}{=} [E : K] \cdot \dim_E L = [E : K] \cdot [L : E].$$

\square

Proposition 0.9 (Übung). Sei K ein Körper mit $\#K < \infty$ und seien p die Charakteristik, K_0 der Primkörper von K , dann gilt

$$\#K = p^n, \text{ für } n = \dim_{K_0} K$$

Bemerkung. Zu jeder Primpotenz $p^n \exists K$ Körper mit $\#K = p^n$

Definition 0.10. Sei $E \supseteq K$ ein Oberkörper und $S \subseteq E$ eine Teilmenge, dann:

(a) $K(S) :=$ der kleinste Oberkörper von K , der S enthält, d.h.

$$K(S) := \bigcap \{L \subseteq E \text{ Unterkörper} \mid K \cup S \subseteq L\}$$

(b) $K[S] :=$ der kleinste Oberring von K , der S enthält, d.h. (Übung)

$$K[S] := \bigcap \{L \subseteq E \text{ Unterring} \mid K \cup S \subseteq L\}$$

Falls $S = \{\alpha_1, \dots, \alpha_n\}$, schreibe auch $K(\alpha_1, \dots, \alpha_n)$ für $K(\{\alpha_1, \dots, \alpha_n\})$ und $K[\alpha_1, \dots, \alpha_n]$ für $K[\{\alpha_1, \dots, \alpha_n\}]$.

Bemerkung.

(a) $K[\alpha_1, \dots, \alpha_n] = \{f(\alpha_1, \dots, \alpha_n) \mid f \in K[X_1, \dots, X_n]\}$

(b) $K(S) = \text{Quot}(K[S]) = \{\frac{f}{g} \mid f, g \in K[S], g \neq 0\}$

(c) $K(S_1)(S_2) = K(S_1 \cup S_2)$ und $K[S_1][S_2] = K[S_1 \cup S_2]$

Beispiel.

(a) $E = \text{Quot}(K[X]) = K(X)$ rationaler Funktionenkörper über K in Variablen X . Hier gilt $K[X] \subsetneq K(X)$ und $[K[X] : K] = \infty$ ($\dim_K K[X] = \infty$)

(b) $\sqrt{3} \subseteq \mathbb{R} \subseteq \mathbb{C}$, dann

$$\mathbb{Q}[\sqrt{3}] = \{\alpha + \beta\sqrt{3} \mid \alpha, \beta \in \mathbb{Q}\} \subseteq \mathbb{R}$$

und

$$\mathbb{Q}(\sqrt{3}) \underset{\text{Übung}}{=} \mathbb{Q}[\sqrt{3}], ([\mathbb{Q}(\sqrt{3}) : \mathbb{Q}] = 2)$$

0.2 Algebraische und transzendente Elemente

Definition 0.11. Sei $E \supseteq K$ ein Oberkörper und seien $\alpha, \alpha_1, \dots, \alpha_n \in E$. Dann

(i) α heißt algebraisch über $K : \iff [K(\alpha) : K] < \infty$

(ii) α heißt transzendent über $K : \iff [K(\alpha) : K] = \infty$

Beispiele (ohne Beweis).

(a) $X \in K(X)$ ist transzendent über K .

(b) $\sqrt{3} \in \mathbb{R}$ ist algebraisch über \mathbb{Q} .

(c) $e = \sum_{n \geq 0} \frac{1}{n!} \in \mathbb{R}$ ist transzendent über \mathbb{Q}

(d) $\pi \in \mathbb{R}$ ist transzendent über \mathbb{Q}

Wiederholung 0.12. (Propositionen 3.49 und 3.50)

(a) $K[X]$ ist Hauptidealring.

(b) $f \in K[X]$ irreduzibel $\iff (f) \subseteq K[X]$ ist maximales Ideal.

(c) Ist $0 \neq P \subseteq K[X]$ Primideal, so $\exists f \in K[X]$ irred. $P = (f)$.

(d) (Übung, s. LA) für $f \in K[X] \setminus K$ von Grad $n > 0$, dann hat $K[X]/_{(f)}$ als K -Vektorraum die Basis $\{1, X, \dots, X^{n-1}\}$.

Definition. Die Auswertungsabbildung an $\alpha \in E$ ist der Ringhomomorphismus

$$\text{ev}_\alpha : K[X] \rightarrow E, f = \sum a_i X^i \mapsto f(\alpha) = \sum a_i \alpha^i$$

Satz 0.13. Für $\alpha \in E$ sind äquivalent:

(a) α ist algebraisch über K .

(b) $\exists n \in \mathbb{N} : 1, \alpha, \dots, \alpha^n$ sind linear unabhängig über K .

(c) $\exists g \in K[X] \setminus \{0\}$ mit $g(\alpha) = 0$.

(d) $\text{Kern}(\text{ev}_\alpha) \subseteq K[X]$ ist maximales Ideal.

(e) $K(\alpha) = K[\alpha]$.

Beweis.

(a) \implies (b): Sei $n := [K(\alpha) : K] = \dim_K K(\alpha) < \infty \implies 1, \alpha, \dots, \alpha^n$ sind l.u. über K .

(b) \implies (c): Voraussetzung in (b) $\implies \exists (c_0, \dots, c_n) \in K^{n+1} \setminus \{0\}$ mit $\sum_{0 \leq i \leq n} c_i \alpha^i = 0$, dann ist

$$\implies g(X) = \sum_{0 \leq i \leq n} c_i X^i \in K[X] \setminus \{0\}. \text{ und } g(\alpha) = 0$$

(c) \implies (d): Homomorphiesatz gibt und den Isomorphismus

$$K[X]/_{\text{Kern}(\text{ev}_\alpha)} \xrightarrow{\cong} \text{Bild}(\text{ev}_\alpha) \underset{\text{Unterring}}{\subseteq} E$$

$\text{Bild}(\text{ev}_\alpha)$ ist Integritätsbereich $\implies \text{Kern}(\text{ev}_\alpha)$ ist Primideal. Da $0 \neq g \in \text{Kern}(\text{ev}_\alpha)$ (g aus (c)) folgt: $\text{Kern}(\text{ev}_\alpha)$ ist Primideal $\neq 0$ also ein maximales Ideal.

(d) \implies (a): Voraussetzung: $\mathfrak{m}_\alpha := \text{Kern}(\text{ev}_\alpha) \subseteq K[X]$ ist maximales Ideal.

$$\xrightarrow{\text{Homomorphiesatz}} \underbrace{K[X]/_{\mathfrak{m}_\alpha}}_{\text{Körper, da } \mathfrak{m}_\alpha \text{ max.}} \xrightarrow{\cong} \text{Bild}(\text{ev}_\alpha) \subseteq E$$

$\implies \text{Bild}(\text{ev}_\alpha)$ ist ein Körper. Aber: $\text{Bild}(\text{ev}_\alpha) = K[\alpha]$, also $K[\alpha] = K(\alpha)$ (*), und sei $f \in K[X]$ irreduzibler Erzeuger von \mathfrak{m}_α , dann:

$$\dim_K K[X]/_{(f)} = \text{Grad } f < \infty \implies \dim_K K(\alpha) = \text{Grad } f < \infty.$$

(d) \implies (e): gezeigt wegen (*).

(e) \implies (a): Zu zeigen: $K[\alpha] = K(\alpha) \implies [K(\alpha) : K] < \infty$, wir zeigen (b).
o.E. $\alpha \neq 0$, wesentliche Beobachtung: $\alpha^{-1} \in K[\alpha]$. d.h. $\exists c_0, \dots, c_n \in K$ mit $\alpha^{-1} = c_0 + c_1\alpha + \dots + c_n\alpha^n$

$$\implies 0 = -1 + c_0\alpha + c_1\alpha^2 + \dots + c_n\alpha^{n+1}$$

d.h. $1, \alpha, \dots, \alpha^{n+1}$ sind linear abhängig über K . □

Definition 0.14. Sei $\alpha \in E$ algebraisch über K . Das Minimalpolynom μ_α (oder $\mu_{\alpha, K}$) von α über K ist das normierte Polynom in $K[X] \setminus \{0\}$ kleinsten Grades mit $\mu_\alpha(\alpha) = 0$.

Proposition 0.15. Sei $\alpha \in E$ algebraisch über K , dann:

(a) $(\mu_\alpha) = K[X] \cdot \mu_\alpha = \text{Kern}(\text{ev}_\alpha)$.

(b) μ_α ist irred. und $K[X]/(\mu_\alpha)$ ist ein Körper.

(c) $[K(\alpha) : K] = \text{Grad } \mu_\alpha$

Beweis.

- (a) • “ \subseteq ”: Klar, da $\mu_\alpha = 0$ also $\text{ev}_\alpha(\mu_\alpha) = 0$
 • “ \supseteq ”: $K[X]$ ist Hauptidealring $\implies \exists g \in K[X] : (g) = \text{Kern}(\text{ev}_\alpha)$ mit $g \neq 0, g \mid \mu_\alpha$ und $\text{Kern}(\text{ev}_\alpha)$ ist ein maximales Ideal ($\neq 0$) folgt aus 13. μ_α hat den kleinsten Grad unter allen solchen $f \neq 0$ mit $f(\alpha) = 0 \implies g \simeq \mu_\alpha \implies (g) = (\mu_\alpha)$.

(b) $\text{Kern}(\text{ev}_\alpha)$ maximal $\neq 0 \implies$ Erzeuger μ_α von $\text{Kern}(\text{ev}_\alpha)$ ist irred. und $K[X]/(\mu_\alpha)$ ist ein Körper, da (μ_α) maximal.

(c) Im Beweis von Satz 13: $K(\alpha) \cong K[X]/(\mu_\alpha)$

$$\implies [K(\alpha) : K] = \dim_K K[X]/(\mu_\alpha) \stackrel{\text{Whg. 12}}{=} \text{Grad } \mu_\alpha. \quad \square$$

Korollar 0.16. Sei $f \in K[X]$ irred. normiert und $\alpha \in E$ eine Nullstelle von f , dann ist α algebraisch über K und $\mu_\alpha = f$ und $[K(\alpha) : K] = \text{Grad } f$

Beispiel. $X^2 - 3 \in \mathbb{Q}[X]$ ist irreduzibel (Eisenstein mit $p = 3$)

$$\implies \mu_{\sqrt{3}, \mathbb{Q}} = X^2 - 3$$

analog: $\alpha = \sqrt[3]{2}$ algebraisch über \mathbb{Q} mit $\mu_\alpha = X^3 - 2$ und

$$\mathbb{Q}[\alpha] = \mathbb{Q}(\alpha) = \{a + b\alpha + c\alpha^2 \mid a, b, c \in \mathbb{Q}\}$$

Korollar 0.17. Für $\alpha \in E$ sind äquivalent:

(a) α ist transzendent über K

(b) $K[\alpha] \subsetneq K(\alpha)$

(c) $\text{ev}_\alpha : K[X] \rightarrow K[\alpha]$ ist ein Isomorphismus.

Beweis.

$\neg(a) \iff \neg(b)$, folgt aus Satz 13 $(a) \iff (e)$.

Beachte weiter: $(c) \iff \text{Kern}(\text{ev}_\alpha) = \{0\}$, also: $\neg(c) \iff \exists g \in K[X] \setminus \{0\} : g(\alpha) = a \iff \alpha \text{ ist algebraisch} \iff \neg(a)$. \square

Bemerkung. Ist $\alpha \in E$ transzendent über K , so setzt sich $\text{ev}_\alpha : K[X] \xrightarrow{\cong} K[\alpha]$ fort zu einem Körperisomorphismus $K(X) = \text{Quot}(K[X]) \rightarrow K(\alpha)$.

Definition 0.18 (Algebraischer Oberkörper). Ein Oberkörper $E \supseteq K$ heißt algebraisch über K : \iff jedes $\alpha \in E$ ist algebraisch über K .

Lemma 0.19. Seien $F \supseteq E \supseteq K$ Oberkörper, dann:

- (a) $[E : K] < \infty \implies E$ ist algebraisch über K .
- (b) $\alpha_1, \dots, \alpha_n \in E$ mit α_i algebraisch über $K, \forall i \implies K(\alpha_1, \dots, \alpha_n) \supseteq K$ algebraisch.
- (c) $F \supseteq K$ ist algebraisch $\iff F \supseteq E$ und $E \supseteq K$ sind algebraisch.
- (d) Ist $K = K_0 \subseteq K_1 \subseteq \dots$ eine Kette (indiziert über \mathbb{N}) von Oberkörpern, so ist $K_\infty = \bigcup_n K_n$ ein Oberkörper von K , und sind alle $K_{i+1} \supseteq K_i$ algebraisch, so ist $K_\infty \supseteq K$ algebraisch.
- (e) Ist $S \subseteq E$ eine beliebige Teilmenge, so dass alle $\alpha \in S$ algebraisch über K sind, so gilt $K(S) = K[S]$ und $K(S)$ ist algebraisch über K .

Beweis. (a) Für $\alpha \in E$ gilt: $K \subseteq K(\alpha) \subseteq E$ und wegen Gradformel folgt $[K(\alpha) : K] \leq [E : K] < \infty \implies \alpha$ algebraisch über K .

- (b) Definiere $K_i = K(\alpha_1, \dots, \alpha_i), i \in \{1, \dots, n\}$, wir wissen α_i algebraisch über K , d.h. $\exists g \in K[X] \setminus \{0\} = g(\alpha_i) = 0 \implies g \in K_{i-1}[X] \setminus \{0\}$ ($K_{i-1} \supseteq K$), $\exists g \in K_{i-1} \setminus \{0\} : g(\alpha_i) = 0 \implies \alpha_i$ algebraisch über K_{i-1}

$$\implies [K_i : K_{i-1}] = [K_{i-1}(\alpha) : K_{i-1}] < \infty \xrightarrow{\text{Ind.} + \text{Gradformel}} [K_n : K] < \infty$$

$$\xrightarrow{(a)} K_n = K(\alpha_1, \dots, \alpha_n) \supseteq K \text{ algebraisch.}$$

- (c) • “ \implies ”: Sei $F \supseteq K$ algebraisch, sei $\alpha \in E \implies \alpha \in F \implies \alpha$ algebraisch über K . Und sei $\alpha \in F$. Dann argumentiere wie in (b) um α algebraisch über E zu folgen $\implies F \supseteq E$ algebraisch.
- “ \impliedby ”: (Problem: $[E : K]$ könnte unendlich sein.) Es gelte: $F \supseteq E$ und $E \supseteq K$ sind algebraisch. $\alpha \in F$ (zz: $[K(\alpha) : K] < \infty$). Wir wissen α algebraisch über $E \implies$ haben $\mu_{\alpha, E} \in E[X] \setminus E$ schreibe $\mu_{\alpha, E} = a_0 + a_1 X + \dots + a_{n-1} X^{n-1} + X^n$ mit $a_i \in E$ algebraisch über $K \implies E' = K[a_0, \dots, a_{n-1}]$ hat endlichen Grad über K (nach (b)) und α ist algebraisch über E' , da $\mu_{\alpha, E} \in E'[X] \implies [E'[\alpha] : E'] < \infty$. Nach Definition von algebraisch und Gradformel $[E'[\alpha] : K] < \infty \implies \alpha$ algebraisch über K .
- Gegeben eine Körperkette $K = K_0 \subseteq K_1 \subseteq \dots \subseteq K_n \subseteq \dots, K_\infty = \bigcup K_n$ ist Oberkörper von K (Übung). Gilt zusätzlich $K_{i+1} \supseteq K_i$ algebraisch $\forall i$, so folgt mit Induktion und (c): $K_i \supseteq K$ algebraisch $\forall i$. Sei $\alpha \in K_\infty \implies \exists n : \alpha \in K_n \implies \alpha$ ist algebraisch über K .

- Übung.

□

Korollar 0.20. Sei $E \supseteq K$ ein Oberkörper und

$$F := \{\alpha \in E \mid \alpha \text{ algebraisch über } K\}$$

Dann gilt:

(a) $F \subseteq E$ Unterkörper.

(b) $F \supseteq K$ algebraisch.

(c) $K[F] = F$.

Beweis. 19(e) $\implies K[F] \supseteq K$ ist algebraischer Oberkörper und $K[F] \subseteq E \implies K[F] = F$, d.h. (c) gilt. Und (a), (b) folgen. ((a),(b) gelten für $K[F]$ nach 19(e)). □

Beispiel 0.21 (Übung). Sei $\alpha_n := \sqrt[n]{2} \in R$ für $n \geq 0$, dann: $[\mathbb{Q}(\alpha_n) : \mathbb{Q}] = 2^n$.
 $\implies \mathbb{Q}_\infty = \bigcup_n \mathbb{Q}(\alpha_n)$ ist algebraisch über \mathbb{Q} , aber $[\mathbb{Q}_\infty : \mathbb{Q}] = \infty$.

Beispiel. $\tilde{\mathbb{Q}} := \{\alpha \in \mathbb{C} \mid \alpha \text{ ist algebraisch über } \mathbb{Q}\} \implies [\tilde{\mathbb{Q}} : \mathbb{Q}] = \infty$ und $\tilde{\mathbb{Q}} \supseteq \mathbb{Q}$ ist algebraisch.

Leitfragen. (a) Gegeben $f \in K[X]$ irred. Finde Oberkörper E und $\alpha \in E$ mit $f(\alpha) = 0$.

(b) Finde Oberkörper $E \supseteq K$ in dem alle irred. $f \in K[X]$ eine Nullstelle (alle Nullstellen) haben.

Sei $f = \sum_{0 \leq i \leq n} a_i X^i \in K[X] \setminus K$, sei $E \supseteq K$ Oberkörper, hatten schon gesehen $f(\alpha) = 0 \iff \text{ev}_\alpha(f) = 0 \iff \mu_{\alpha, K} \mid f$.

Proposition 0.22. $\#\{\alpha \in E \mid f(\alpha) = 0\} \leq \text{Grad } f$.

Beweis. TODO □

Definition 0.23. (a) $f \in K[X] \setminus K$ zerfällt in Linearfaktoren über $K : \iff$ jeder irred. normierte Faktor von f ist der Form $X - \alpha$ für ein $\alpha \in K$.

(b) K heißt algebraisch abgeschlossen \iff jedes $f \in K[X] \setminus K$ zerfällt in Linearfaktoren über K .

Bemerkung 0.24. K ist algebraisch abgeschlossen \iff jedes $f \in K[X] \setminus K$ hat eine Nullstelle $\alpha \in K$.

Beweis.

- “ \implies ”: Klar
- “ \impliedby ”: Sei $f \in K[X] \setminus K$ irred. normiert, nach Voraussetzung hat f eine Nullstelle $\alpha \in K \implies f = X - \alpha$ (alle irred. Polynome sind linear).

□

Beispiel.

\mathbb{C} ist algebraisch abgeschlossen.

TODO

Definition 0.25. Sei $f \in K[X]$ irred. Ein Oberkörper $E \supseteq K$ heißt Stammkörper zu $f \iff \exists \alpha \in E$ mit $f(\alpha) = 0$ und $E = K(\alpha)$.

Satz 0.26. Sei $f \in K[X]$ irred. von Grad n , dann:

- (a) $E := K[X]_{(f)}$ ist ein Körper (schreibe \bar{g} für die Klasse zu $g \in K[X]$).
- (b) $K \rightarrow E, \alpha \rightarrow \bar{\alpha}$ ist ein Ringhomomorphismus, also Körperhomomorphismus. (Betrachte K als Unterkörper von E , schreibe α für $\bar{\alpha}$)
- (c) Es gilt $f(\bar{X}) = 0$, d.h. f hat keine Nullstelle in E .
- (d) Es gilt $E = K[\bar{X}]$ und $[E : K] = n$
- (e) Ist F ein Oberkörper von K mit Nullstelle $\beta \in F$ von f , so gilt $n \mid [F : K]$, falls $[F : K] < \infty$.

Beweis. TODO □

Korollar 0.27. Seien $f_1, \dots, f_t \in K[X]$ irred. Dann \exists Oberkörper $E \supseteq K$ mit $\beta_1, \dots, \beta_t \in E$, so dass $f_i(\beta_i) = 0, \forall i \in \{1, \dots, t\}$ und $E = K(\beta_1, \dots, \beta_t)$.

Bemerkung. Es gilt nur $[E : K] \leq \prod_{1 \leq i \leq t} \text{Grad } f_i$.

Beispiel. Seien $f_1, f_2 \in \mathbb{R}[X]$ irred. quadr. Polynome $\implies E = \mathbb{C}$ und $[E : \mathbb{R}] = 2 < 2 \cdot 2$. z.B. $f_1 = X^2 + 1$ und $f_2 = X^2 + \pi$.

Satz 0.28. Jeder Körper K hat einen (inj.) Körperhomomorphismus in einen algebraisch abgeschlossen Körper \tilde{K} .

Definition 0.29 (Algebraischer Abschluss). Ein Oberkörper $E \supseteq K$ heißt algebraischer Abschluss, wenn

- (a) E ist algebraisch abgeschlossen.
- (b) $E \supseteq K$ ist algebraisch.

Bezeichnung. \bar{K} sei immer ein algebraischer Abschluss von K .

Bemerkung (zu Satz 28). \tilde{K} ist ein algebraischer Abschluss.

Beweis. (von Satz 28) TODO. □

Proposition 0.30.

- (a) K ist algebraisch abgeschlossen $\iff \forall$ algebraischer Oberkörper $E \supseteq K$ gilt $E = K$
- (b) Ist $E \supseteq K$ algebraischer Oberkörper und $\bar{E} \supseteq E$ ein algebraischer Abschluss. Dann ist $\bar{E} \supseteq K$ ein algebraischer Abschluss.
- (c) Ist $E \supseteq K$ algebraisch abgeschlossen, so ist $F := \{\alpha \in E \mid \alpha \text{ algebraisch über } K\}$ ein algebraischer Abschluss von K .

Beweis.

- (a) • “ \implies ”: Sei $\alpha \in E$, z.z. $\alpha \in K$. Betrachte $\mu_{\alpha,K} \in K[X]$, K algebraisch abgeschlossen \implies irred. Polynome haben Grad \implies $\text{Grad } \mu_{\alpha,K} = 1 \implies \mu_{\alpha,K} = X - \alpha \in K[X]$ also $\alpha \in K$.
- “ \impliedby ”: Sei $f \in K[X]$ irred. normiert. Sei E sein Stammkörper $\implies \exists \alpha \in E$ mit $f(\alpha) = 0 \xRightarrow{E \supseteq K \text{ alg.}} E = K$ und also $\alpha \in K \implies f = X - \alpha$.
- (b) Folgt aus Proposition 19.
- (c) Nach Korollar 20 ist F ein alg. Oberkörper von K . Noch z.z: $f \in F[X]$ irred. normiert $\implies f$ linear. f faktorisiert in $E[X]$ also $f = \prod_{1 \leq i \leq n} (X - \alpha_i)$ ($n = \text{Grad } f, \alpha_i \in E$). Nun sind die α_i algebraisch über F , also auch über $K \implies \alpha_1, \dots, \alpha_n \in F \xRightarrow{f \text{ irr.}} n = 1$. \square

Beispiel 0.31. $\overline{\mathbb{Q}} := \{\alpha \in \mathbb{C} \mid \alpha \text{ ist alg. über } \mathbb{Q}\}$ ist ein algebraischer Abschluss von \mathbb{Q} . Es gilt $\overline{\mathbb{Q}} \subsetneq \mathbb{C}$, denn $\overline{\mathbb{Q}}$ ist abzählbar, \mathbb{C} aber nicht.

Bemerkung. Nächste Ziele:

- (a) \overline{K} ist eindeutig bis auf Isomorphie.
- (b) “Verstehe” Körperautomorphismen von \overline{K} über K .

Bezeichnungen 0.32. Sei $\varphi_i : K \rightarrow K'$ ein Körperhomomorphismus.

- (a) Schreibe φ_* für den induzierten Ringhomomorphismus

$$\varphi_* : K[X] \rightarrow K'[X], \sum a_i X^i \mapsto \sum \varphi(a_i) X^i$$

- (b) Sei $L \supseteq K$ ein Oberkörper, Nenne einen Körperhomomorphismus $\psi : L \rightarrow K'$ eine Ausdehnung von φ , falls $\psi|_K = \varphi$, also wenn

$$\begin{array}{ccc} L & \xrightarrow{\psi} & K' \\ \uparrow i & \nearrow \varphi & \\ K & & \end{array}$$

Lemma 0.33. Sei $L \supseteq K$ ein Stammkörper zu $f \in K[X]$ irred. und sei $\alpha \in L$ eine Nullstelle von f , sei $\varphi : K \rightarrow E$ ein Körperhomomorphismus, dann gilt: Die Abbildung

$$\begin{array}{ccc} \left\{ \begin{array}{l} \psi : L \rightarrow E \text{ eine} \\ \text{Ausdehnung von } \varphi \end{array} \right\} & \longrightarrow & \left\{ \beta \in E \mid \begin{array}{l} \beta \text{ ist eine} \\ \text{Nst. von } \varphi_*(f) \end{array} \right\} \\ \psi \longmapsto & & \psi(\alpha) \end{array}$$

ist wohl-definiert und bijektiv, insbesondere:

$$\# \left\{ \begin{array}{l} \psi : L \rightarrow E \text{ eine} \\ \text{Ausdehnung von } \varphi \end{array} \right\} = \# \left\{ \beta \in E \mid \begin{array}{l} \beta \text{ ist eine} \\ \text{Nst. von } \varphi_*(f) \end{array} \right\} \leq \text{Grad } f = [L : K]$$

Beweis. • Abbildung ist wohl-definiert: Sei $f = \sum a_i X^i$

$$\begin{aligned} \varphi_*(f)(\psi(\alpha)) &= \sum_i \underbrace{\varphi(a_i)}_{\psi(a_i)} \psi(\alpha)^i \\ &\stackrel{\psi \text{ Körperhom.}}{=} \psi\left(\sum_i a_i \alpha^i\right) = \psi(f(\alpha)) = \psi(0) = 0 \end{aligned}$$

- Abbildung ist injektiv: $L = K[\alpha] \implies$ Ausdehnungen $\psi : L \rightarrow E$ sind eindeutig bestimmt durch $\psi|_K = \varphi$ und Angabe von $\psi(\alpha)$. D.h. unterschiedliche Ausdehnungen führen auf verschiedene Nullstellen von $\varphi_*(f)$.
- Abbildung ist surjektiv: Sei $\beta \in E$ Nullstelle von $\varphi_*(f)$. Betrachte den Ringhomomorphismus:

$$\xi : K[X] \rightarrow E, \sum \alpha_i X^i \mapsto \sum \varphi(\alpha_i) \beta^i$$

Beachte: $f \in \text{Kern}(\xi)$, nach der Wahl von β , nach dem Homomorphiesatz erhalten wir einen Ringhomomorphismus

$$\bar{\xi} : K[X]_{/(f)} \rightarrow E, [g] \mapsto \varphi_*(g)(\beta)$$

Wir erinnern uns, dass L konstruiert wurde als $K[X]_{/(f)}$, d.h. wir haben einen Isomorphismus

$$\bar{\rho} : K[X]_{/(f)} \rightarrow L, [g] \mapsto g(\alpha)$$

Erhalten $\psi : L \rightarrow E$ als $\psi = \bar{\xi} \circ \bar{\rho}^{-1}$ (prüfe $\psi|_K = \varphi$ und $\psi(\alpha) = \bar{\xi}(\bar{\rho}^{-1}(\alpha)) = \bar{\xi}(\bar{X}) = \beta$). \square

Lemma 0.34. Sei $L \supseteq K$ ein Oberkörper mit $[L : K] < \infty$, dann \exists Oberkörper $F \supseteq K$ mit $L \supsetneq F$ und $f \in F[X]$ irred., sodass $L \supseteq F$ Stammkörper von f ist.

Beweis. TODO. \square

Korollar 0.35. Sei $L \supseteq K$ ein Oberkörper mit $[L : K] < \infty$ und sei $\varphi : K \rightarrow E$ ein Körperhomomorphismus, dann gilt:

$$\#\{\psi : L \rightarrow E \text{ Ausdehnung von } \varphi\} \leq [L : K]$$

Satz 0.36. Sei E algebraisch abgeschlossener Körper, $\varphi : K \rightarrow E$ ein Körperhom. Sei $L \supseteq K$ ein algebraischer Oberkörper, dann \exists Ausdehnung $\psi : L \rightarrow E$ von φ .

Beweis. TODO. \square

Definition 0.37. Seien E_1, E_2 Oberkörper von K . Ein Körperhomomorphismus $\varphi : E_1 \rightarrow E_2$ heißt

- (a) K -Homomorphismus : $\iff \varphi|_K = \text{id}_K$
- (b) K -Isomorphismus : $\iff \varphi$ ist bij. und $\varphi|_K = \text{id}_K$

(c) K -Automorphismus : $\iff E_1 = E_2$ und φ ist K -Isomorphismus.

Notation.

(a) $\text{Hom}_K(E_1, E_2) := \{\varphi : E_1 \rightarrow E_2 \mid \varphi \text{ ist } K\text{-Hom.}\}$

(b) $\text{Isom}_K(E_1, E_2) := \{\varphi : E_1 \rightarrow E_2 \mid \varphi \text{ ist } K\text{-Isom.}\}$

(c) $\text{Aut}_K(E_1) := \text{Isom}_K(E_1, E_1)$

Korollar 0.38. Sei $E \supseteq K$ ein algebraischer Oberkörper und $\overline{K} \supseteq K$ ein algebraischer Abschluss von K , dann:

(a) $\text{Hom}_K(E, \overline{K}) \neq \emptyset$ (Satz 36). Ist $[E : K] < \infty$, so gilt $\# \text{Hom}_K(E, \overline{K}) \leq [E : K]$ (Kor 35). Ist E Stammkörper zu $f \in K[X]$ irred, so gilt

$$\# \text{Hom}_K(E, \overline{K}) = \#\{\alpha \in E \mid f(\alpha) = 0\}$$

(Lemma 33)

(b) Ist E algebraisch abgeschlossen, so gilt $\text{Hom}_K(E, \overline{K}) = \text{Isom}(K)(E, \overline{K}) (\neq \emptyset$ wegen (a))

(c) Ist \overline{E} ein algebraischer Abschluss von E und $\varphi : E \rightarrow \overline{K}$ ein K -Homomorphismus, so $\exists K$ -Isomorphismus $\psi : \overline{E} \rightarrow \overline{K}$, der φ ausdehnt. ((b) und Satz 36)

Beweis. TODO

□

0.3 Normale Erweiterungen und Zerfällungskörper

Bezeichnung. Nenne Oberkörper $E \supseteq K$ auch Erweiterungskörper oder Erweiterung.

Definition 0.39. (a) Eine algebraische Erweiterung $E \supseteq K$ heißt normal :
 $\iff \forall \alpha \in E : \mu_{\alpha, K}$ zerfällt in Linearfaktoren über $E[X]$ $\iff \forall f \in K[X]$ irred. mit Nullstellen $\alpha_1, \dots, \alpha_n$ in \overline{K} gilt: liegt ein α_i in E , so folgt $\{\alpha_1, \dots, \alpha_n\} \subseteq E$.
Übung

(b) Eine Erweiterung $E \supseteq K$ heißt Zerfällungskörper (ZK) über K von $f \in K[X] \setminus K$ normiert : \iff

(i) $\exists \alpha_1, \dots, \alpha_n \in E : f = \prod_{1 \leq i \leq n} (X - \alpha_i)$

(ii) Kein echter Unterkörper von E enthält $\alpha_1, \dots, \alpha_n$.

Proposition 0.40. Sei $f \in K[X] \setminus K$ normiert, dann gilt:

(a) f besitzt einen eindeutigen Zerfällungskörper in \overline{K} , nämlich $E = K(\alpha_1, \dots, \alpha_n)$ mit $\alpha_1, \dots, \alpha_n$ die Nst. von f in \overline{K} . (so dass $f = \prod_{1 \leq i \leq n} (X - \alpha_i)$, $n = \text{Grad } f$)

(b) Ist E ein Zerfällungskörper von f , und $\varphi : E \rightarrow F$ ein Körperhomomorphismus, so ist $\varphi(E)$ der Zerfällungskörper über $\varphi(K)$ von $\varphi_*(f)$

(c) Je zwei Zerfällungskörper E, E' zu f (über K) sind K -isomorph.

Beweis. TODO. □

Beispiel 0.41.

$$f = X^4 - 5 \underset{\text{Übung}}{=} (X - \sqrt[4]{5})(X - i\sqrt[4]{5})(X + \sqrt[4]{5})(X + i\sqrt[4]{5}) \in \mathbb{Q}[X]$$

Zerfällungskörper von f über \mathbb{Q} ist (Übung)

$$E = \mathbb{Q}(i, \sqrt[4]{5})$$

und es gilt (Übung) $[E : \mathbb{Q}] = 8$.

Wiederholung. $E \supseteq K$ algebraische Erweiterung heißt normal $\iff \forall \alpha \in E$ zerfällt $\mu_{\alpha, K}$ in $E[X]$ über Linearfaktoren.

Satz 0.42. Für eine algebraische Erweiterung $E \supseteq K$ sind äquivalent:

(i) $\forall \psi, \psi' \in \text{Hom}_K(E, \overline{K})$ gilt $\psi(E) = \psi'(E)$

(i') $\forall \psi \in \text{Hom}_K(E, \overline{K})$ gilt $\psi(E) = E$

(ii) $E \supseteq K$ ist normale Erweiterung.

Gilt $[E : K] < \infty$, so sind (i), (ii) äquivalent zu

(iii) E ist der Zerfällungskörper eines Polynoms in $K[X]$.

Beweis. TODO. □

Korollar 0.43. Sei E ein Oberkörper von K in \overline{K} mit $[E : K] < \infty$, dann \exists kleinster Oberkörper $F \supseteq E$ in \overline{K} , sodass $F \supseteq K$ normal ist, für diesen gilt $[F : K] < \infty$.

Beweis. TODO. □

Definition 0.44. Der Körper $F \supseteq \overline{K}$ aus Korollar 43 heißt normale Hülle von $E \supseteq K$.

0.4 Seperabilität

Sei \overline{K} ein algebraischer Abschluss von K .

Vorbereitung. "Formale Ableitung."

Definition 0.45.

$$\frac{d}{dX} : K[X] \rightarrow K[X],$$

$$f = \sum_{0 \leq i \leq n} a_i X^i \mapsto f' := \frac{d}{dX} f = \sum_{0 \leq i \leq n} i a_i X^{i-1}$$

Hierbei steht i für $i \cdot 1 = 1 + \dots + 1 \in K$ i -fache Summe.

Proposition 0.46 (Rechenregeln).

(a) $\frac{d}{dX}$ ist K -linear.

(b) $\frac{d}{dX}(f \cdot g) = \frac{df}{dX} \cdot g + f \cdot \frac{dg}{dX}$.

(c) $\frac{d}{dX} f(g(X)) = \frac{df}{dX}(g(X)) \cdot \frac{d}{dX} g$. Insbesondere $\frac{d}{dX}(g^n) = ng^{n-1}$.

Beweis. Übung. □

Lemma 0.47. Sei $p = \text{char}(K)$, sei $f \in K[X] \setminus \{0\}$, dann gilt

(a) $p \nmid \text{Grad } f \implies \text{Grad } \frac{d}{dX} f = \text{Grad } f - 1$.

(b) $f' = 0 \iff f \in K[X^p]$ mit der Konvention $X^0 = 1$

Beweis. TODO. □

Definition 0.48. $f \in K[X]$ hat mehrfache Nullstelle in $\overline{K} \iff \exists \alpha \in \overline{K}$ mit $f(\alpha) = 0$ und $(X - \alpha)^2$ teilt f in \overline{K} .

Bemerkung 0.49 (Übung). $\alpha \in \overline{K}$ ist mehrfache Nullstelle von $f \iff f(\alpha) = f'(\alpha) = 0$.

Proposition 0.50. Sei $f \in K[X] \setminus \{0\}$ und $g := \text{ggT}(f, f') \in K[X]$. Dann: f hat mehrfache Nullstellen in $\overline{K} \iff \text{Grad } g = 0$.

Beweis. TODO. □

Korollar 0.51. Sei $p = \text{char } K$ und $f \in K[X]$ irred. Dann sind äquivalent:

(i) f hat mehrfache Nullstelle in \overline{K} .

(ii) $p > 0$ und $f' = 0$.

(iii) $p > 0$ und $\exists g \in K[X]$ ohne mehrfache Nst. und $\exists m > 0$ sodass $f = g(X^{p^m})$ und g irred.

Insbesondere gelten für g, m aus (iii):

(a) $p^m \mid \text{Grad } f$

(b) $\#\{\beta \in \overline{K} \mid f(\beta) = 0\} = \text{Grad } g$

(c) Ist $\xi : K \rightarrow K'$ ein Körperhomomorphismus, so gilt $\xi_* f = (\xi_* g)(X^{p^m})$ und

$$\#\{\beta \in \overline{K}' \mid \xi_* f(\beta) = 0\} = \text{Grad } g = \text{Grad}(\xi_*(g))$$

Beweis. TODO. □

Definition 0.52. Sei $f \in K[X] \setminus K$, und $E \supseteq K$ Oberkörper.

(a) f heißt separabel \iff Kein irred. Faktor von f hat mehrfache Nst.

(b) $\alpha \in E$ heißt separabel über $K \iff \mu_{\alpha, K}$ ist separabel.

(c) $E \supseteq K$ heißt separabel \iff alle $\alpha \in E$ sind separabel über K .

(d) K heißt perfekt \iff alle $g \in K[X] \setminus K$ sind separabel (\iff alle algebraische Erweiterungen $E \supseteq K$ sind separabel.)

(e) Ist f irred., so heißt f rein inseparabel $\iff f$ besitzt genau eine Nst. in \overline{K} .

(f) $E \supseteq K$ ist rein inseperabel $\iff \forall \alpha \in E : \mu_{\alpha,K}$ ist rein inseperabel.

Beispiel (zu 52(e)). in 54 geg. $X^p - Y$

Beispiel 0.53. Gelte $\text{char } K = p > 0$, sei $f = X^p - a \in K[X]$ und sei $b \in \overline{K}$ eine Nst. von f , dann:

(a) $(X - b)^p = f(X)$ in $\overline{K}[X]$

(b) f ist irred. $\iff b \in \overline{K} \setminus K$.

Beweis. Übung. □

Beispiel 0.54. $K = \mathbb{F}_p(Y) = \text{Quot}(\mathbb{F}_p[Y])$, sei $f(X) = X^p - Y \in (\mathbb{F}_p[Y])[X] \subseteq K[X]$ irred. nach Existenz ($Y \in \mathbb{F}_p[Y]$ prim). Haben TODO.

Satz 0.55. K ist perfekt \iff es gelten (i) oder (ii).

(i) $\text{char } K = 0$.

(ii) $\text{char } K = p > 0$ und der Frobeniushomomorphismus

$$\varphi_K : K \rightarrow K, \alpha \mapsto \alpha^p$$

ist surjektiv. (φ_K ist Ringhomomorphismus, da $\text{char } K = p$, also ein Körperhomomorphismus)

Beispiel.

$$\varphi_K : \mathbb{F}_p \rightarrow \mathbb{F}_p(Y) = K, \quad \text{Bild}(\varphi_K) \stackrel{\text{Übung}}{=} \mathbb{F}_p(Y^p)$$

und \mathbb{F}_p ist perfekt.

Korollar 0.56. K endlicher Körper $\implies K$ ist perfekt.

Beweis. TODO. □

Beispiel 0.57. K algebraisch abgeschlossen $\implies K$ perfekt, denn jede algebraische Erweiterung E ist seperabel, da $E = K$.

Definition 0.58. Sei $E \supseteq K$ ein Oberkörper mit $[E : K] < \infty$, der seperable Grad von $E \supseteq K$ ist

$$[E : K]_s := \# \text{Hom}_K(E, \overline{K}) \quad (= \text{Hom}_K(E, \overline{E}))$$

Facts 0.59. (a) $[E : K]_s \leq [E : K]$

(b) Ist E Stammkörper über K zu $\alpha \in E \implies [E : K]_s \stackrel{38a}{=} \#\{\beta \in \overline{K} \mid \mu_{\alpha,K}(\beta) = 0\}$

(c) Seien E, α wie in (b), dann ist $\text{Grad } \mu_{\alpha,K} = [E : K] = [E : K]_s \iff \mu_{\alpha,K}$ ist seperabel $\iff \#\{\beta \in \overline{K} \mid \mu_{\alpha,K}(\beta) = 0\} = \text{Grad } \mu_{\alpha,K}$

Lemma 0.60. Seien $K \subseteq E \subseteq F$ Oberkörper mit $[F : K] < \infty$, dann

$$[F : K]_s = [F : E]_s \cdot [E : K]_s \quad (*)$$

Beweis. TODO. □

Satz 0.61. Für Oberkörper $E \supseteq K$ mit $[E : K] < \infty$ sind äquivalent:

(i) $E \supseteq K$ separabel.

(ii) Für $\alpha_1, \dots, \alpha_n \in E : E = K[\alpha_1, \dots, \alpha_n]$, gilt $f = \prod_i \mu_{\alpha_i, K}$ ist separabel.

(iii) $[E : K]_s = [E : K]$

Korollar 0.62. Seien $F \supseteq E \supseteq K$ Oberkörper mit $[F : K] < \infty$, dann: $F \supseteq K$ separabel $\iff F \supseteq E$ und $E \supseteq K$ sind separabel.

Korollar 0.63 (Übung). Sei $E \supseteq K$ algebraischer Oberkörper, dann ist $E_0 = \{\alpha \in E \mid \alpha \text{ separabel über } K\}$ der größte Unterkörper von E , der separabel über K ist.

Bemerkung. Der Beweis verwendet, dass Kor. 62 auch dann gilt, wenn $F \supseteq K$ eine beliebige algebraische Erweiterung ist und $F \supseteq E \supseteq K$ Erweiterungen sind.

Korollar 0.64. Sei $E \subseteq \overline{K}$ Oberkörper von K mit $[E : K] < \infty$, ist $E \supseteq K$ separabel, so ist auch die normale Hülle F von E über K separabel.

Beweis. Gelte $E = K[\alpha_1, \dots, \alpha_n]$ für $\alpha_1, \dots, \alpha_n \in E$, dann ist F der ZK in \overline{K} von $\mu_{\alpha_1, K} \cdot \dots \cdot \mu_{\alpha_n, K}$, es folgt, dass F separabel über K ist, wegen Satz 61, Formulierung in (ii) (Die $\mu_{\alpha_i, K}$ sind separabel, da α_i über K separabel.) \square

Satz 0.65 (Satz von primitiven Elementen). Sei $E \supseteq K$ Oberkörper mit $[E : K] < \infty$, ist $E \supseteq K$ separabel, so $\exists \alpha \in E$ mit $E = K(\alpha)$