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 $K \subseteq R$ 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 $\varphi : K \to K'$ heißt Körperhomomorphismus : $\iff$ φ ist ein Ringhomomorphismus (der Ringe $K \to K'$)

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

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

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

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

Beweis. (a) Nur zu zeigen: $\mathrm{Kern}(\varphi) \subsetneq K$. 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:*

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

Beweis.

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

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

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

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

$$\varphi(\underbrace{\mathbb{Z} \setminus \{0\}}_{S}) \underset{\varphi \text{ inj. Hom.}}{\subseteq} K_0 \setminus \{0\} \subseteq K \setminus \{0\}$$

universelle Eigenschaft der Lokalisierung (S multiplikativ abgeschlossen, $\varphi(S) \subseteq K^\times$) $\implies$ $\exists!$ Ringhomomorphismus $\widehat{\varphi} : S^{-1}\mathbb{Z} = \mathbb{Q} \to K_0$, der φ fortsetzt; und $\widehat{\varphi}\left(\frac{a}{b}\right) = \varphi(a)\varphi(b)^{-1}, z, b \in \mathbb{Z}, b \neq 0$. Erhalten: $\widehat{\varphi}$ gibt Isomorphismus $\mathbb{Q} \xrightarrow{\cong} \widehat{\varphi}(\mathbb{Q}) \underset{\text{Unterkörper}}{\subseteq} K_0, K_0$ minimal $\implies$ $\widehat{\varphi}$ ist Isomorphismus $\mathbb{Q} \cong K_0$. □

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

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

- 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

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

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

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

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)

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

□

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

Bemerkung.

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

(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 $\alpha, \alpha_1, \ldots, \alpha_n \in E$. 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 $\{1, X, \ldots, X^{n-1}\}$.

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

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

Satz 0.13. *Für $\alpha \in E$ sind äquivalen:*

(a) α ist algebraisch über K.

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

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

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

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

Beweis.

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

(b) $\implies$ (c): Voraussetzung in (b) $\implies \exists (c_0, \ldots, c_n) \in K^{n+1} \setminus \{0\}$ 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

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

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

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

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

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

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

(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. $\exists c_0, \ldots, c_n \in K$ mit $\alpha^{-1} = c_0 + c_1\alpha + \cdots + c_n\alpha^n$

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

d.h. $1, \alpha, \ldots, \alpha^{n+1}$ 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) $(\mu_\alpha) = K[X] \cdot \mu_\alpha = \mathrm{Kern}(\mathrm{ev}_\alpha)$.

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

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

Beweis.

(a)
- "$\subseteq$": Klar, da $\mu_\alpha = 0$ also $\mathrm{ev}_\alpha(\mu_\alpha) = 0$
- "$\supseteq$": $K[X]$ ist Hauptidealring $\implies \exists g \in K[X] : (g) = \mathrm{Kern}(\mathrm{ev}_\alpha)$ mit $g \neq 0, g \mid \mu_\alpha$ und $\mathrm{Kern}(\mathrm{ev}_\alpha)$ 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) $\mathrm{Kern}(\mathrm{ev}_\alpha)$ maximal $\neq 0 \implies$ Erzeuger μ_α von $\mathrm{Kern}(\mathrm{ev}_\alpha)$ ist irred. und $K[X]/(\mu_\alpha)$ ist ein Körper, da (μ_α) maximal.

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

$$\implies [K[\alpha] : K] = \dim_K K[X]/(\mu_\alpha) \underset{\text{Whg. } 12}{=} \mathrm{Grad}\,\mu_\alpha.$$ □

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 $[K(\alpha) : K] = \mathrm{Grad}\, f$*

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) $\mathrm{ev}_\alpha : K[X] \to K[\alpha]$ *ist ein Isomorphismus.*

Beweis.

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

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

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

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) $\alpha_1, \ldots, \alpha_n \in E$ *mit* α_i *algebraisch über* $K, \forall i \implies K(\alpha_1, \ldots, \alpha_n) \supseteq K$ *algebraisch.*

(c) $F \supseteq K$ *ist algebraisch* $\iff F \supseteq E$ *und* $E \supseteq K$ *sind algebraisch.*

(d) Ist $K = K_0 \subseteq K_1 \subseteq \cdots$ *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 $K_i = K(\alpha_1, \ldots, \alpha_i), i \in \{1, \ldots, n\}$, 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}

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

$$\underset{(a)}{\implies} K_n = K(\alpha_1, \ldots, \alpha_n) \supseteq K \text{ algebraisch.}$$

(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 $\mu_{\alpha,E} = a_0 + a_1 X + \cdots + a_{n-1}X^{n-1} + X^n$ mit $a_i \in E$ algebraisch über $K \implies E' = K[a_0, \ldots, a_{n-1}]$ 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 $K = K_0 \subseteq K_1 \subseteq \cdots K_n \subseteq \cdots$, $K_\infty = \bigcup K_n$ 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 $\alpha_n := \sqrt[2^n]{2} \in R$ 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. $\widetilde{\mathbb{Q}} := \{\alpha \in \mathbb{C} \mid \alpha \text{ ist algebraisch über } \mathbb{Q}\} \implies [\widetilde{\mathbb{Q}} : \mathbb{Q}] = \infty$ und $\widetilde{\mathbb{Q}} \supseteq \mathbb{Q}$ 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 $f(\alpha) = 0 \iff \mathrm{ev}_\alpha(f) = 0 \iff \mu_{\alpha,K} \mid f$.

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

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 $\overline{g}$ für die Klasse zu $g \in K[X]$).*

(b) $K \to E, \alpha \to \overline{\alpha}$ *ist ein Ringhomomorphismus, also Körperhomomorphismus. (Betrachte K als Unterkörper von E, schreibe α für $\overline{\alpha}$)*

(c) Es gilt $f(\overline{X}) = 0$, d.h. f hat keine Nullstelle in E.

(d) Es gilt $E = K[\overline{X}]$ 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 $f_1, \ldots, f_t \in K[X]$ irred. Dann $\exists$ Oberkörper $E \supseteq K$ mit $\beta_1, \ldots, \beta_t \in E$, so dass $f_i(\beta_i) = 0, \forall i \in \{1, \ldots, t\}$ und $E = K(\beta_1, \ldots \beta_t)$.*

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

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 $\widetilde{K}$.*

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. $\overline{K}$ sei immer ein algebraischer Abschluss von K.

Bemerkung (zu Satz 28)**.** $\widetilde{K}$ 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 $\overline{E} \supseteq E$ ein algebraischer Abschluss. Dann ist $\overline{E} \supseteq K$ ein algebraischer Abschluss.

(c) Ist $E \supseteq K$ algebraisch abgeschlossen, so ist $F := \{\alpha \in E \mid \alpha$ algebraisch über $K\}$ ein algebraischer Abschluss von K.

Beweis.

(a)
- " $\Longrightarrow$ ": Sei $\alpha \in E$, z.z. $\alpha \in K$. Betrachte $\mu_{\alpha,K} \in K[X]$, K algebraisch abgeschlossen $\Longrightarrow$ irred. Polynome haben Grad $\Longrightarrow$ Grad $\mu_{\alpha,K} = 1 \Longrightarrow \mu_{\alpha,K} = X - \alpha \in K[X]$ also $\alpha \in K$.
- " $\Longleftarrow$ ": Sei $f \in K[X]$ irred. normiert. Sei E sein Stammkörper $\Longrightarrow$ $\exists \alpha \in E$ mit $f(\alpha) = 0 \underset{E \supseteq K \text{ alg.}}{\Longrightarrow} E = K$ und also $\alpha \in K \Longrightarrow f = X - \alpha$.

(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 $\Longrightarrow$ f linear. f faktorisiert in $E[X]$ also $f = \prod_{1 \leq i \leq n}(X - \alpha_i)$ ($n = \operatorname{Grad} f, \alpha_i \in E$). Nun sind die α_i algebraisch über F, also auch über $K \Longrightarrow \alpha_1, \ldots, \alpha_n \in F \underset{f \text{ irr.}}{\Longrightarrow} n = 1$. □

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 $\varphi_i : K \to K'$ ein Körperhomomorphismus.

(a) Schreibe φ_* für den induzierten Ringhomomorphismus

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

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

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

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 $\varphi : K \to E$ ein Körperhomomorphismus, dann gilt: Die Abbildung*

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

ist wohl-definiert und bijektiv, insbesondere:

$$\# \left\{ \begin{array}{c} \psi : L \to E \text{ eine} \\ \text{Ausdehnung von } \varphi \end{array} \right\} = \# \left\{ \beta \in E \;\middle|\; \begin{array}{c} \beta \text{ ist eine} \\ \text{Nst. von } \varphi_*(f) \end{array} \right\} \leq \operatorname{Grad} f = [L : K]$$

Beweis.

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

$$\varphi_*(f)(\psi(\alpha)) = \sum_i \underbrace{\varphi(a_i)}_{\psi(a_i)} \psi(\alpha)^i$$

$$\underset{\psi \text{ Körperhom.}}{=} \psi(\sum_i a_i \alpha^i) = \psi(f(\alpha)) = \psi(0) = 0$$

- Abbildung ist injektiv: $L = K[\alpha] \implies$ Ausdehnungen $\psi : L \to E$ sind eindeutig bestimmt durch $\psi \mid_K = \varphi$ 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:

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

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

$$\overline{\xi} : {}^{K[X]}\!/_{(f)} \to E, [g] \mapsto \varphi_*(g)(\beta)$$

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

$$\overline{\rho} : {}^{K[X]}\!/_{(f)} \to L, [g] \to g(\alpha)$$

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

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. □

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

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

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

Beweis. TODO. □

Definition 0.37. Seien E_1, E_2 Oberkörper von K. Ein Körperhomomorphismus $\varphi : E_1 \to E_2$ 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) $\mathrm{Hom}_K(E_1, E_2) := \{\varphi : E_1 \to E_2 \mid \varphi \text{ ist } K\text{-Hom.}\}$

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

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

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

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

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

(Lemma 33)

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

(c) Ist $\overline{E}$ ein algebraischer Abschluss von E und $\varphi : E \to \overline{K}$ ein K-Homomorphismus, so $\exists K$-Isomorphismus $\psi : \overline{E} \to \overline{K}$, 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 $E[X] \underset{\text{Übung}}{\iff} \forall f \in K[X]$ irred. mit Nullstellen $\alpha_1, \ldots, \alpha_n$ in $\overline{K}$ gilt: liegt ein α_i in E, so folgt $\{\alpha_1, \ldots, \alpha_n\} \subseteq E$.

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

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

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

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

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

(b) Ist E ein Zerfällungskörper von f, und $\varphi : E \to F$ 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) $\forall \psi, \psi' \in \mathrm{Hom}_K(E, \overline{K})$ *gilt* $\psi(E) = \psi'(E)$

(i') $\forall \psi \in \mathrm{Hom}_K(E, \overline{K})$ *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.

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

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

Hierbei steht i für $i \cdot 1 = 1 + \cdots + 1 \in K$ 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* $\frac{d}{dX}(g^n) = n g^{n-1}$.

Beweis. Übung. □

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

(a) $p \not| \mathrm{Grad}\, f \implies \mathrm{Grad}\, \frac{d}{dX} f = \mathrm{Grad}\, f - 1$.

(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* $g := \mathrm{ggT}(f, f') \in K[X]$. *Dann: f hat mehrfache Nullstellen in* $\overline{K} \iff \mathrm{Grad}\, g = 0$.

Beweis. TODO. □

Korollar 0.51. *Sei* $p = \mathrm{char}\, K$ *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* $\exists > 0$ *sodass* $f = g(X^{p^m})$ *und g irred.*

Insbesondere gelten für g, m *aus (iii):*

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

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

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

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

Beweis. TODO. □

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

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

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

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

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

(e) Ist f irred., so heißt f rein inseperabel $\iff$ 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 $\operatorname{char} K = p > 0$, 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. $K = \mathbb{F}_p(Y) = \operatorname{Quot}(\mathbb{F}_p[Y])$, 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) $\operatorname{char} K = 0$.

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

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

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

Beispiel.

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

und $\mathbb{F}_p$ ist perfekt.