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 $S = \{\alpha_1, \dots, \alpha_n\}$, 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) $K(S) = \mathrm{Quot}(K[S]) = \{\frac{f}{g} \mid f, g \in K[S], g \neq 0\}$

(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) $E = \mathrm{Quot}(K[X]) = K(X)$ 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 $\{1, X, \ldots, X^{n-1}\}$.

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. $\exists c_0, \dots, c_n \in K$ 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. $\square$

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: $K(\alpha) \cong {K[X]}/{(\mu_\alpha)}$

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

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

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: $(c) \iff \text{Kern}(\text{ev}_\alpha) = \{0\}$, 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 $\text{ev}_\alpha : K[X] \xrightarrow{\cong} K[\alpha]$ fort zu einem Körperisomorphismus $K(X) = \text{Quot}(K[X]) \to K(\alpha)$.

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.

$\square$

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)). $\square$

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 $\square$

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).

$\square$

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.

□