Algebra und Zahlentheorie SS 2019

Dozent: Prof. Dr. Arno Fehm

21. Juni 2019

Inhaltsverzeichnis

Vorwort

Motivation und Einführung

Kapitel I

Körper

1. Körpererweiterungen

Seien K, L, M Körper.

▶ **Bemerkung 1.1**

In diesem Kapitel bedeutet "Ring" immer kommutativer Ring mit Einselement, und ein Ringhomomorphismus bildet stets das Einselement auf das Einselement ab. Insbesondere gibt es für jeden Ring einen eindeutig bestimmten Ringhomomorphismus $: \mathbb{Z} \to R$.

▶ **Bemerkung 1.2**

(a) Ein Körper ist ein Ring R, in dem eine der folgenden äquivalenten Bedingungen gilt:

1) $0 \neq 1$ und jedes $0 \neq x \in R$ ist invertierbar
2) $R^\times = R \setminus \{0\}$
3) R hat genau zwei Hauptideale (nämlich (0) und (1))
4) (0) ist ein maximales Ideal von R
5) (0) ist das einzige echte Ideal von R
6) (0) ist das einzige Primideal von R

(b) Insbesondere sind Körper nullteilerfrei, weshalb $\mathrm{Ker}(\mathbb{Z} \to K)$ prim ist.

(c) Aus (5) folgt: Jeder Ringhomomorphismus $K \to L$ ist injektiv

(d) Der Durchschnitt einer Familie von Teilkörpern von K ist wieder ein Teilkörper von K.

Definition 1.3 (Charakteristik)

Die Charakteristik von K, $\mathrm{char}(K)$, ist das $p \in \{0, 2, 3, 5, 7, \dots\}$ mit $\mathrm{Ker}(\mathbb{Z} \to K) = (p)$.

■ **Beispiel 1.4**

(a) $\mathrm{char}(\mathbb{Q}) = 0$ und $\mathrm{char}(\mathbb{F}_p) = (p)$ ($p =$ Primzahl), wobei $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$

(b) Ist $K_0 \subseteq K$ Teilkörper, so ist $\mathrm{char}(K_0) = \mathrm{char}(K)$.

Definition 1.5 (Primkörper)

Der Primkörper von K ist der kleinste Teilkörper von K. (existiert nach Bemerkung 1.2 (d)).

Satz 1.6
Sei $\mathbb{F}$ der Primkörper von K.

(a) $\mathrm{char}(K) = 0 \Leftrightarrow \mathbb{F} \cong \mathbb{Q}$

(b) $\mathrm{char}(K) = p > 0 \Leftrightarrow \mathbb{F} \cong \mathbb{F}_p$

Beweis.
($\Leftarrow$) Beispiel 1.4

($\Rightarrow$) Es ist $\mathrm{Im}(\mathbb{Z} \to K) \subseteq \mathbb{F}$ und $\mathrm{Im}(\mathbb{Z} \to K) \cong \mathbb{Z}/\operatorname{Ker}(\mathbb{Z} \to K)$, sowie

(a) $\mathrm{Im}(\mathbb{Z} \to K) \cong Z/(0) \cong \mathbb{Z} \Rightarrow \mathbb{F} = \mathrm{Quot}(\mathrm{Im}(\mathbb{Z} \to K)) \cong \mathrm{Quot}(\mathbb{Z}) \cong \mathbb{Q}$

(b) $\mathrm{Im}(\mathbb{Z} \to K) \cong Z/(p) \cong \mathbb{F}_p$ ist Teilkörper von K $\Rightarrow \mathbb{F} = \mathrm{Im}(\mathbb{Z} \to K) \cong \mathbb{F}_p$ $\square$

Definition 1.7 (Körpererweiterung)
Ist K ein Teilkörper von L, so nennt man L eine Köpererweiterung von K, auch geschrieben $L \mid K$.

Definition 1.8 (K-Homomorphismus)
Seien $L_1 \mid K$ und $L_2 \mid K$ Körpererweiterungen.

(a) Ein Ringhomomorphismus $\varphi\colon L_1 \to L_2$ ist ein K-Homomorphismus, wenn $\varphi|_K = \mathrm{id}_K$ (i.Z. $\varphi\colon L_1 \to_K L_2$)

(b) $\mathrm{Hom}_K(L_1, L_2) = \{\varphi \mid \varphi : L_1 \to L_2 \text{ ist } K\text{-Homomorphismus}\}$

(c) L_1 und L_2 sind K-isomorph (i.Z. $L_1 \cong_K L_2$), wenn es einen Isomorphismus $\varphi \in \mathrm{Hom}_K(L_1, L_2)$ gibt.

▶ **Bemerkung 1.9**
Ist $L \mid K$ eine Körpererweiterung, so wird L durch Einschränkung der Multiplikation zu einem K-Vektorraum.

Definition 1.10 (Körpergrad)
Es ist $[L : K] := \dim_K(L) \in \mathbb{N} \cup \{\infty\}$ der Körpergrad der Körpererweiterungen $L \mid K$.

■ **Beispiel 1.11**

(a) $[K : K] = 1$

(b) $[\mathbb{C} : \mathbb{R}] = 2$ (Basis $(1, i)$) (aber $(\mathbb{C} : \mathbb{R}) = \infty$)

(c) $[\mathbb{R} : \mathbb{Q}] = \infty$ (mit Abzählarbarkeitsargument oder siehe §2)

(d) $[K(x) : K] = \infty$ ($K(x) = \mathrm{Quot}(K[x])$ (vgl. GEO II.8)

Satz 1.12
Für $K \subseteq L \subseteq M$ Körper ist $[M : K] = [M : L] \cdot [L : K]$ (“Körpergrad ist multiplikativ”)

Beweis. Für den Beweis betrachte folgende Aussage:
Behauptung: Sei $x_1, \ldots, x_n \in L$ K-linear unabhängig und $y_1, \ldots, y_m \in M$ L-linear unabhängig
$\Rightarrow \big\{x_i y_j \mid i \in \{1, \ldots, n\}, j \in \{1, \ldots, m\}\big\}$ K-linear unabhängig.

Beweis: Sei $\sum_{i,j} \lambda_{ij} x_i y_j = 0$ mit $\lambda_{ij} \in K$

$$\Rightarrow \sum_j \underbrace{\left[\sum_i \lambda_{ij} x_i\right]}_{\in L} y_j = 0 \quad \xRightarrow{y_j\, L\text{-l.u.}} \sum_i \lambda_{ij} x_i = 0 \quad \forall j \quad \xRightarrow{x_i\, K\text{-l.u.}} \lambda_{ij} = 0 \quad \forall i, \forall j$$

$\square$

Dann:

- $[L : K] = \infty$ oder $[M : L] = \infty \Rightarrow [M : K] = \infty$
- $[L : K] = n$, $[M : L] = m < \infty$:
  Sei $(x_1, \dots, x_n)$ Basis des K-Vektorraum L und $(y_1, \dots, y_m)$ Basis des L-Vektorraums M
  $\Rightarrow \{x_i y_j \mid i = 1, \dots, n;\ j = 1, \dots, m\}$ K-linear unabhängig und

$$\sum_{i,j} K x_i y_j = \sum_j \underbrace{\left[\sum_i \lambda_{ij} x_i\right]}_{=L} y_j = M,$$

also ist $\{x_i y_j \mid i = 1, \dots, n;\ j = 1, \dots, m\}$ Basis von M. $\square$

Definition 1.13 (Körpergrad endlich)
$L \mid K$ endlich $:\Leftrightarrow [L : K] < \infty$.

Definition 1.14 (Unterring, Teilkörper)
Sei $L \mid K$ eine Körpererweiterung $a_1, a_2, \dots, a_n \in L$.

(a) $K[a_1, \dots, a_n]$ ist kleinster Unterring von L, der $K \cup \{a_1, \dots, a_n\}$ enthält (“$a_1, \dots, a_n$ über K erzeugt”)

(b) $K(a_1, \dots, a_n)$ ist kleinster Teilkörper von L, der $K \cup \{a_1, \dots, a_n\}$ enthält (“von “$a_1, \dots, a_n$ über K erzeugte”, “$a_1, \dots, a_n$” zu K adjungieren)

(c) $L|K$ ist endlich erzeugt $:\Leftrightarrow a_1, \dots, a_n \in L$: $L = K(a_1, \dots, a_n)$

(d) $L|K$ ist einfach $:\Leftrightarrow$ existiert $a \in L$: $L = K(a)$

▶ Bemerkung 1.15

(a) $L \mid K$ endlich $\Rightarrow L \mid K$ endlich erzeugt.

(b) $K[a_1, \dots, a_n]$ ist das Bild des Homomorphismus

$$\begin{cases} K[x_1, \dots, x_n] & \to L \\ f & \mapsto f(a_1, \dots, a_n) \end{cases}$$

und $K(a_1, \dots, a_n) = \left\{\alpha\beta \mid \alpha, \beta \in K[a_1, \dots, a_n], \beta \neq 0\right\} \cong \text{Quot}\left(K[a_1, \dots, a_n]\right)$

2. Algebraische Körpererweiterungen

Sei $L \mid K$ eine Körpererweiterung.

Definition 2.1 (algebraisch, transzendent)
Sei $\alpha \in L$. Gibt es ein $0 \neq f \in K$ mit $f(\alpha) = 0$, so heißt α algebraisch über K, andernfalls transzendent über K.

■ **Beispiel 2.2**

(a) $\alpha \in K \Rightarrow \alpha$ ist algebraisch über K (denn $f(\alpha) = 0$ für $f = X - \alpha \in K[X]$)

(b) $\sqrt{-1} \in \mathbb{Q}(\sqrt{-1})$ ist algebraisch über $\mathbb{Q}$ (denn $f(\sqrt{-1}) = 0$ für $f = X^2 + 1 \in \mathbb{Q}[X]$)
$\sqrt{-1} \in \mathbb{C}$ ist algebraisch über $\mathbb{R}$

▶ **Bemerkung 2.3**
Sind $K \subseteq L \subseteq M$ Körper und $\alpha \in M$ algebraisch über K, so auch über L.

Lemma 2.4
Genau dann ist $\alpha \in L$ algebraisch über K, wenn $1, \alpha, \alpha^2, \ldots$ K-linear abhängig sind.

Beweis. Für $\lambda_0, \lambda_1, \ldots \in K$, fast alle gleich Null, so ist

$$\sum_{i=0}^{\infty} \lambda_i \alpha^i = 0 \quad \Leftrightarrow \quad f(\alpha) = 0 \text{ für } f = \sum_{i=0}^{\infty} \lambda_i X^i \in K[X] \qquad \square$$

Lemma 2.5
Betrachte den Epimorphismus

$$\varphi_\alpha : \begin{cases} K[X] & \to K[\alpha] \\ f & \mapsto f(\alpha). \end{cases}$$

Genau dann ist α algebraisch über K, wenn $\mathrm{Ker}(\varphi_\alpha) \neq (0)$. In diesem Fall ist $\mathrm{Ker}(\varphi_\alpha) = (f_\alpha)$ mit einem eindeutig bestimmten irreduziblen, normierten $f_\alpha \in K$.

Beweis. K Hauptidealring $\Rightarrow \mathrm{Ker}(\varphi_\alpha) = (f_\alpha)$, $f_\alpha \in K$, und o.E. sei f_α normiert. Aus $K[\alpha] \subseteq L$ nullteilerfrei folgt, dass $\mathrm{Ker}(\varphi_\alpha)$ prim ist. Somit ist f_α prim im Hauptidealring, also auch irreduzibel. $\square$

Definition 2.6 (Minimalpolynom, Grad)
Sei $\alpha \in L$ algebraisch über K, $\mathrm{Ker}(\varphi_\alpha) = (f_\alpha)$ mit $f_\alpha \in K$ normiert und irreduzibel.

(a) $\mathrm{MinPol}(\alpha \mid K) := f_\alpha$, das Minimalpolynom von α über K.

(b) $\deg(\alpha \mid K) :\Leftrightarrow \deg(f_\alpha)$, der Grad von α über K.

Satz 2.7
Sei $\alpha \in L$.

(a) α transzendent über K
$\Rightarrow K[\alpha] \cong K[X]$, $K(\alpha) \cong_K K(X)$, $[K(\alpha) : K] = \infty$.

(b) α algebraisch über K
$\Rightarrow K[\alpha] = K(\alpha) \cong K/\operatorname{MinPol}(\alpha \mid K)$, $[K(\alpha)\colon K)] = \deg(\alpha \mid K) < \infty$, und $1, \alpha, \ldots, \alpha^{\deg(\alpha|K)-1}$ ist K-Basis von $K(\alpha)$.

Beweis.
(a) $\operatorname{Ker}(\varphi_\alpha) = (0) \Rightarrow \varphi_\alpha$ ist Isomorphismus (da zusätzlich injektiv)
$\Rightarrow K(\alpha) \cong_K \operatorname{Quot}(K[\alpha]) \cong_K \operatorname{Quot}(K[X]) = K(X)$
$\Rightarrow [K(\alpha)\colon K] = [K(X)\colon K] = \infty$

(b) Sei $f = f_\alpha = \operatorname{MinPol}(\alpha \mid K)$, und $n = \deg(\alpha \mid K) = \deg(f)$.

- f irreduzibel $\Rightarrow (f) \neq (0)$ prim $\xRightarrow{\text{GEO II.4.7}} (f)$ ist maximal
  $\Rightarrow K[\alpha] \cong K[X]/(f)$ ist Körper $\Rightarrow K[\alpha] = K(\alpha)$
- $1, \alpha, \ldots, \alpha^{n-1}$ sind K-linear unabhängig:
  $$\sum_{i=0}^{n-1} \lambda_i \alpha^i = 0 \quad \Rightarrow \quad \sum_{i=0}^{n-1} \lambda_i X^i \in (f) \quad \xRightarrow{\deg f = n} \quad \lambda_i = 0 \ \forall i$$
- $1, \alpha, \ldots, \alpha^{n-1}$ ist Erzeugendensystem: Für $g \in K[X]$ ist
  $$g = qf + r$$
  mit q, $r \in K[X]$ und $\deg(r) < \deg(f) = n$ und
  $$g(\alpha) = q(\alpha) \underbrace{f(\alpha)}_{=0} + r(\alpha) = r(\alpha).$$
  Somit folgt:
  $$K[\alpha] = \operatorname{Im}(\varphi_\alpha) = \left\{ g(\alpha) \;\middle|\; g \in K \right\} = \left\{ r(\alpha) \;\middle|\; r \in K, \deg(r) < n \right\} = \sum_{i=0}^{n-1} K \cdot \alpha^i$$ □

■ Beispiel 2.8

(a) $p \in \mathbb{Z}$ prim $\Rightarrow \sqrt{p} \in \mathbb{C}$ ist algebraisch über $\mathbb{Q}$.
Da $f(X) = X^2 - p$ irreduzibel in $\mathbb{Q}$ ist (GEO II.7.3), ist $\operatorname{MinPol}(\sqrt{p} \mid \mathbb{Q}) = X^2 - p$, $[\mathbb{Q}(\sqrt{p}) : \mathbb{Q}] = 2$.

(b) Sei $\zeta_p = e^{\frac{2\pi i}{p}} \in \mathbb{C}$ ($p \in \mathbb{N}$ prim). Da $\Phi_p = \frac{X^p - 1}{X - 1} = X^{p-1} + X^{p-2} + \cdots + X + 1 \in \mathbb{Q}$ irreduzibel in $\mathbb{Q}$ ist (GEO II.7.9), ist $\operatorname{MinPol}(\zeta_p \mid \mathbb{Q}) = \Phi_p$, $[\mathbb{Q}(\zeta_p) : \mathbb{Q}] = p - 1$.

Daraus folgt schließlich $[\mathbb{C} : \mathbb{Q}] \geq [\mathbb{Q}(\zeta_p) : \mathbb{Q}] = p - 1 \ \forall p \Rightarrow [\mathbb{C} : \mathbb{Q}] = \infty \Rightarrow [R : \mathbb{Q}] = \infty$.

(c) e, $\pi \in \mathbb{R}$ sind transzendent über $\mathbb{Q}$ (Hermite 1873, Lindemann 1882).
Daraus folgt: $[R : \mathbb{Q}] \geq [\mathbb{Q}(\pi) : \mathbb{Q}] = \infty$. Jedoch ist unbekannt, ob z.B. $\pi + e$ transzendent ist.

Definition 2.9
$L \mid K$ ist algebraisch $:\Leftrightarrow$ jedes $\alpha \in L$ ist algebraisch über K.

Satz 2.10
$L \mid K$ endlich $\Rightarrow L \mid K$ algebraisch.

Beweis. Sei $\alpha \in L$, $[L : K] = n$. Dann ist $1, \alpha, \dots, \alpha^n$ K-linear abhängig $\stackrel{2.4}{\Longrightarrow}$ α algebraisch über K. □

Folgerung 2.11
Ist $L = K(\alpha_1, \dots, \alpha_n)$ mit $\alpha_1, \dots, \alpha_n$ algebraisch über K, so ist $L \mid K$ endlich, insbesondere algebraisch.

Beweis. Induktion nach n:

- $n = 0$: ✓
- $n > 0$: $K_1 := K(\alpha_1, \dots, \alpha_{n-1})$
  $\Rightarrow L = K_1(\alpha_n)$, α_n algebraisch über K_1 (Bemerkung 2.3)
  $\Rightarrow [L : K] = \underbrace{[K_1(\alpha_n) : K_1]}_{<\infty \text{ nach Satz } 2.7} \cdot \underbrace{[K_1 : K]}_{<\infty \text{ nach IH}}$ □

Folgerung 2.12
Es sind äquivalent:

(a) $L \mid K$ ist endlich.

(b) $L \mid K$ ist endlich erzeugt und algebraisch.

(c) $L = K(\alpha_1, \dots, \alpha_n)$ mit $\alpha_1, \dots, \alpha_n$ algebraisch über K.

Beweis.

- (1) $\Rightarrow$ (2): Bemerkung 1.15 und Satz 2.10
- (2) $\Rightarrow$ (3): trivial
- (3) $\Rightarrow$ (1): Folgerung 2.11 □

▶ **Bemerkung 2.13**
Nach Satz 2.7 ist

$$\alpha \text{ algebraisch über } K :\Leftrightarrow K[\alpha] = K(\alpha).$$

Direkter Beweis für ($\Rightarrow$):
Sei $0 \neq \beta \in K[\alpha]$. Daraus folgt, dass $f(\beta) = 0$ für ein irreduzibles $0 \neq f = \sum_{i=0}^n a_i X^i \in K$. Durch Einsetzen von β und Division durch β erhält man

$$\xRightarrow{a_0 \neq 0} \beta^{-1} = -a_0^{-1}(a_1 + a_2\beta + \dots + a_n\beta^{n-1}) \in K[\beta] \subseteq K[\alpha]$$

Satz 2.14
Seien $K \subseteq L \subseteq M$ Körper. Dann gilt:

$$M \mid K \text{ algebraisch } \Leftrightarrow M \mid L \text{ algebraisch und } L \mid K \text{ algebraisch}$$

Beweis. ($\Rightarrow$) klar, siehe Bemerkung 2.3.

($\Leftarrow$) Sei $\alpha \in M$. Schreibe $f = \mathrm{MinPol}(\alpha \mid L) = \sum_{i=0}^n a_i x^i$, $L_0 := K(a_0, \dots, a_n)$

$$\Rightarrow \quad f \in L_0[X]$$

$$\Rightarrow \quad [L_0(\alpha) : L_0] \leq \deg(f) < \infty$$

$$\Rightarrow \quad [K(\alpha) : K] \leq [K(a_0, \dots, a_n, \alpha) : K] = \underbrace{[L_0(\alpha) : L_0]}_{<\infty} \underbrace{[L_0 : K]}_{< \text{ nach } 2.7}$$

$$\Rightarrow \quad \alpha \text{ algebraisch über } K$$

$$\overset{\alpha \text{ bel.}}{\Rightarrow} \quad M \mid K \text{ algebraisch.}$$ □

Folgerung 2.15
$\tilde{K} = \{\alpha \in L \mid \alpha \text{ algebraisch über } K\}$ ist ein Körper, und ist $\alpha \in L$ algebraisch über $\tilde{K}$, so ist schon $\alpha \in \tilde{K}$.

Beweis.

- α, $\beta \in \tilde{K}$:
  $\Rightarrow K(\alpha, \beta) \mid K$ endlich, insbesondere algebraisch
  $\Rightarrow \alpha + \beta$, $\alpha - \beta$, $\alpha \cdot \beta$, $\alpha^{-1} \in K(\alpha, \beta)$ alle algebraisch über K, also $K(\alpha, \beta) \subseteq \tilde{K}$.
- $\alpha \in L$ algebraisch über $\tilde{K}$:
  $\Rightarrow \tilde{K}(\alpha) \mid \tilde{K}$ algebraisch
  $\Rightarrow \tilde{K} \mid K$ algebraisch
  $\overset{2.14}{\Rightarrow} \tilde{K}(\alpha) \mid K$ algebraisch, insbesondere $\alpha \in \tilde{K}$. □

Definition 2.16 (relative algebraische Abschluss)
$\tilde{K} = \{\alpha \in L \mid \alpha \text{ algebraisch über } K\}$ heißt der relative algebraische Abschluss von K in L.

Beispiel 2.17
$\tilde{\mathbb{Q}} = \{\alpha \in \mathbb{C} \mid \alpha \text{ algebraisch über } \mathbb{Q}\}$ ist ein Körper, der Körper der algebraischen Zahlen. Es ist $[\tilde{\mathbb{Q}} : \mathbb{Q}] = \infty$, z.B. da $[\mathbb{Q}(\zeta_p) : \mathbb{Q}] = p - 1$ für jedes p prim. (algebraische Erweiterung die nicht endlich ist.)

3. Wurzelkörper und Zerfällungskörper

Sei K ein Körper, $f \in K[X]$ mit $n = \deg(f) > 0$.

Beispiel 3.1
Sei $K = \mathbb{Q}$. Dann hat f eine Nullstelle ("Wurzel") $\alpha \in \mathbb{C}$, und $L := K(\alpha) = K[\alpha]$ ist die kleinste Erweiterung von $\mathbb{Q}$ in $\mathbb{C}$, die diese Nullstelle enthält.

Definition 3.2 (Wurzelkörper)
Ein Wurzelkörper von f ist eine Körpererweiterung $L \mid K$ der Form $L = K(\alpha)$ mit $f(\alpha) = 0$.

Lemma 3.3
Sei $L = K(\alpha)$ mit $f(\alpha) = 0$ ein Wurzelkörper von f. Dann ist $[L : K] \leq n$. Ist f irreduzibel, so ist $[L : K] = n$ und $g \mapsto g(\alpha)$ induziert einen Isomorphismus $K[X]/(f) \xrightarrow{\cong}_K L$.

Beweis. Sei zunächst f irreduzibel, $f_\alpha = \mathrm{MinPol}(\alpha \mid K)$. Dann ist $f = cf_\alpha$, die Behauptung folgt somit aus Satz 2.7 (b). Für $f \in K[X]$ beliebig, schreibe $f = f_1 \cdots f_r$ mit $f_i \in K[X]$ irreduzibel und

$$f(\alpha) = 0 \quad \Rightarrow \quad \text{O.E. } f_1(\alpha) = 0 \quad \Rightarrow \quad [L : K] = \deg(f_1) \leq \deg(f) = n$$ □

Lemma 3.4
Sei f irreduzibel. Dann ist $L := K[X]/(f)$ ein Wurzelkörper von f.

Beweis. Betrachte den Epimorphismus $\pi = \pi_f : K[X] \to K[X]/(f) = L$, setze $\alpha = \pi(X)$

- K Körper $\Rightarrow \pi_{|K}$ injektiv
  $\Rightarrow$ können K mit Teilkörper von L identifizieren, sodass $\pi_{|K} = \mathrm{id}_K$
- (f) irreduzibel $\Rightarrow$ prim $\xRightarrow{\text{GEO II.4.7}}$ (f) maximal $\Rightarrow L = K[X]/(f)$ ist Körper
- $f(\alpha) = f(\pi(X)) \overset{(*)}{=} \pi(f(X)) = 0 \Rightarrow f(X) \in \mathrm{Ker}(\pi)$
  ($*$ gilt, da $f = \sum a_i x^i \Rightarrow \pi(f) = \sum \pi(a_i)\pi(x)^i = \sum a_i \pi(x)^i = f(\pi(x))$)
- $L = \pi(K[X]) = K[\pi(X)] = K[\alpha] \overset{\alpha \text{ alg.}}{=} K(\alpha)$ □

Satz 3.5
Sei f irreduzibel. Ein Wurzelkörper von f existiert und ist eindeutig in folgendem Sinn:
Sind $L_1 = K(\alpha_1), L_2 = K(\alpha_2)$ mit $f(\alpha_1) = 0 = f(\alpha_2)$, so existiert genau ein K-Isomorphismus $\varphi \colon L_1 \to L_2$ mit $\varphi(\alpha_1) = \alpha_2$.

Beweis.
- Existenz gibt Lemma 3.4
- Lemma 3.3 liefert Isomorphismus

$$\left.\begin{array}{ccc} L_1 \xleftarrow[\varphi_1]{\cong} & K[X]/(f) & \xrightarrow[\varphi_2]{\cong} L_2 \\ \alpha_1 \mapsfrom & X + (f) & \mapsto \alpha_2 \end{array}\right\} \quad \Rightarrow \quad \varphi_2 \circ \varphi_1 \colon L_1 \xrightarrow{\cong}_K L_2 \text{ mit } \alpha_1 \mapsto \alpha_2$$

Umgekehrt ist jeder K-Isomorphismus $\varphi \colon L_1 \to_K L_2$ wegen $L_1 = K(\alpha_1)$ schon durch $\varphi(\alpha_1)$ festgelegt. □

Folgerung 3.6
f hat einen Wurzelkörper.

Beweis. Schreibe $f = f_1 \cdots f_r, f_1, \ldots, f_r \in K[X]$ irreduzibel, nehme einen Wurzelkörper von f_1. □

Folgerung 3.7
Es gibt eine Erweiterung $L \mid K$, über der f in Linearfaktoren zerfällt, also $f = c\prod_{i=0}^{n}(x-\alpha_i)$ mit $c \in K^\times$, $\alpha, \ldots, \alpha_n \in L$.

Beweis. Schreibe $f = c \cdot f_0$ mit $c \in K^\times, f_0 \in K[X]$ normiert.
Induktion nach n:
$n = 1$: $f = x - a$, nehme $L = K$.

$n > 1$: Nach Folgerung 3.6 existiert $L_1 \mid K$, $\alpha_1 \in L_1$ mit $f_0(\alpha_1) = 0$

$\Rightarrow$ $f_0 = (x-\alpha_1) \cdot f_1$ mit $f_1 \in L_1[X]$ normiert

$\overset{\text{(IH)}}{\Longrightarrow}$ Es existiert $L \mid L_1$, $\alpha_1, \ldots, \alpha_n \in L$ mit $f_1 = \prod_{i=2}^{n}(x-\alpha_i)$

$\Rightarrow$ $f = c \cdot f_0 = c \cdot (x-\alpha_1) \cdot f_1 = c\prod_{i=1}^{n}(x-\alpha_i)$ □

Definition 3.8 (Zerfällungskörper)
Ein Zerfällungskörper von K ist eine Erweiterung $L \mid K$ der Form $L = K(\alpha_1, \ldots, \alpha_n)$ mit $f = c \cdot \prod_{i=1}^{n}(x-\alpha_i)$ und $c \in K^\times$.

Satz 3.9
Ein Zerfällungskörper von f existiert.

Beweis. Ist $L \mid K$ wie in Folgerung 3.7, ist $K(\alpha_1, \ldots, \alpha_n)$ ein Zerfällungskörper von f. □

Lemma 3.10
Ist $L \mid K$ ein Zerfällungskörper von f, so ist $[L : K] \leq n!$

Beweis. Sei $L = K(\alpha_1, \ldots, \alpha_n)$, $f = c\prod_{i=1}^{n}(x-\alpha_i)$.
Induktion nach n:
$n = 1$: $L = K$, $[K : K] = 1$

$n > 1$: $L_1 = K(\alpha_1)$ ist Wurzelkörper von f

$\overset{3.3}{\Longrightarrow}$ $[L_1 : K] \leq n$ und schreibe $f = c \cdot (x-\alpha_1) \cdot f_1, f_1 = \prod_{i=2}^{n}(x-\alpha_i) \in L_1[X]$

$\Rightarrow$ $L = K(\alpha_1, \ldots, \alpha_n) = L_1(\alpha_1, \ldots, \alpha_n)$ ist Zerfällungskörper von f_1 (über L_1)

$\overset{\text{IH}}{\Longrightarrow}$ $[L : L_1] \leq \deg(f_1)! = (n-1)!$

$\Rightarrow$ $[L : K] = [L : L_1][L_1 : K] = (n-1)!\,n = n!$ □

■ **Beispiel 3.11**

(a) Ist $n = 2$, so ist jeder Wurzelkörper L von f, schon ein Zerfällungskörper: $[L : K] \leq 2$.

(b) Ist $n = 3$, f irreduzibel. Schreibe $L_1 = K(\alpha), f = c(x-\alpha_1)f_1$ mit $f_1 \in L_1[X]$

- f_1 reduzibel: L_1 ist schon Zerfällungskörper von f, $[L_1 : K] = 3$
- f_1 irreduzibel: L_1 ist kein Zerfällungskörper von f. Ist L Wurzelkörper von f_1, so ist L

Zerfällungskörper von f, $[L : K] = 3! = 6$

■ **Beispiel**

Sei $f = x^3 - 2 \in \mathbb{Q}[X]$, dann sind die Nullstellen von f: $\sqrt[3]{2} \in \mathbb{R}$, $\zeta_3 \sqrt[2]{2}$, $\zeta_3^2 \sqrt[2]{2}$

- $\mathbb{Q}(\sqrt[2]{2})$ ist Wurzelkörper von f. $\mathbb{Q}(\sqrt[3]{2}) \subseteq \mathbb{R}$, $\zeta_3 \sqrt[3]{2}$, $\zeta_3^2 \sqrt[3]{2} \notin \mathbb{R}$, aber kein Zerfällungskörper. Der Zerfällungskörper von f ist

$$\mathbb{Q}(\sqrt[3]{2}, \zeta_3 \sqrt[3]{2}, \zeta_3^2 \sqrt[3]{2}) = \mathbb{Q}(\sqrt[3]{2}, \zeta_3 \sqrt[3]{2})$$

Mathematica/WolframAlpha-Befehle

Will man die Nullstellen von $f = X^3 - 2 \in \mathbb{Q}[X]$ finden, dann bietet Mathematica folgende Funktion:

```
Solve[f==0,x,Complexes],
```

der letzte Parameter lässt einem den Körper wählen, in dem Mathematica suchen soll. Es gibt zur Auswahl `Integers, Rationals, Reals, Complexes`. Für das Beispiel erhält man folgenden Output:

$$\left\{x \to -(-2)^{(1/3)}, x \to 2^{(1/3)}, x \to (-1)^{(2/3)} 2^{(1/3)}\right\}.$$

Dabei müsste man die Einheitswurzeln identifizieren:

$$\left\{x \to \zeta_3 \sqrt[3]{2}, x \to \sqrt[3]{2}, x \to \zeta_3^2 \sqrt[3]{2}\right\}$$

Anmerkung

Wenn f irreduzibel $\Rightarrow K[X]/(f)$ ist Wurzelkörper.

Lemma 3.12

Sei $f = \sum_{i=0}^n a_i X^i$ irreduzibel und sei $L = K(\alpha)$ mit $f(\alpha) = 0$ ein Wurzelkörper von f. Sei $L' \mid K'$ eine weitere Körpererweiterung und $\varphi \in \operatorname{Hom}(K, K')$. Ist $\sigma \in \operatorname{Hom}(L, L')$ eine Fortsetzung von φ (d.h. $\sigma_{|K} = \varphi$), so ist $\sigma(\alpha)$ eine Nullstelle von $f^\varphi = \sum_{i=0}^n \varphi(\alpha_i) X^i \in K[X]$.

Ist umgekehrt $\beta \in L'$ eine Nullstelle von f^φ, so gibt es genau eine Fortsetzung $\sigma \in \operatorname{Hom}(L, \tilde{L})$ von φ mit $\sigma(\alpha) = \beta$.

$$\begin{array}{ccc} L & \xrightarrow{\sigma} & L' \\ \uparrow & & \uparrow \\ K & \xrightarrow{\varphi} & K' \end{array}$$

Beweis (was für die Prüfung!).

- $f(\alpha) = 0 \Rightarrow 0 = \sigma(0) = \sigma\big(f(\alpha)\big) = \sigma\big(\sum_{i=0}^n a_i \alpha^i\big) = \sum_{i=0}^n \varphi(a_i) \sigma(\alpha)^i = f^\varphi\big(\sigma(\alpha)\big)$
- Eindeutigkeit klar, da $L = K(\alpha)$

- Existenz: Betrachte

$$\eta\colon \begin{cases} K[X] \to L \\ g \quad\ \mapsto g(\alpha) \end{cases} \qquad\qquad \psi\colon \begin{cases} K[X] \to L' \\ g \quad\ \mapsto g^{\varphi}(\beta) \end{cases}$$

Beide sind Homomorphismen nach der universellen Eigenschaft. (Bemerke: η surjektiv: $\eta_{|K} = \mathrm{id} \to K \subset \mathrm{Im}(\eta)$ mit $\eta(X) = \alpha \to \alpha \in \mathrm{Im}(\eta)$)
Aus $\mathrm{Ker}(\eta) = (f)$ folgt der Isomorphismus $\bar{\eta}\colon K[X]/(f) \xrightarrow{\cong} L$ und
$f \in \mathrm{Ker}(\psi) \Rightarrow \mathrm{Ker}(\psi) = (f)$ liefert Homomorphismus $\bar{\psi}\colon K[X]/(f) \to L'$
$\sigma := \bar{\psi} \circ \bar{\eta}^{-1}\colon L \to L'$ ist eine Fortsetzung von φ und

$$\sigma(\alpha) = \bar{\psi}(X + (f)) = \beta$$

□

Satz 3.13
Der Zerfällungskörper von f ist eindeutig bestimmt bis auf K-Isomorphie.

Beweis. Für den Beweis betrachte erst folgende Aussage.

Behauptung: Ist $\varphi\colon K \to K'$ ein Isomorphismus, L ein Zerfällungskörper und L' ein Zerfällungskörper von f^{φ}, so setzt sich φ zu einem Isomorphismus $L \to L'$ fort.

Beweis. Induktion nach $n = \deg(f)$:

$n = 1$: $L = K \underset{\varphi}{\xrightarrow{\cong}} K' = L'$ ✓

$n > 1$: Schreibe $f = cg_1 \cdots g_r$ mit $g_i \in K[X]$ normiert und irreduzibel, $c \in K^{\times}$
$\Rightarrow$ $f^{\varphi} = c^{\varphi} g_1^{\varphi} \cdots g_r^{\varphi}$ mit $c^{\varphi} \in (K')^{\varphi}$ und $g_i^{\varphi} \in K'[X]$ normiert und irreduzibel (weil φ Isomorphismus ist). Sei $\alpha_1 \in L$ mit $g_1(\alpha_1) = 0$, $\alpha_1' \in L'$ mit $g_1^{\varphi}(\alpha_1') = 0$

$\overset{3.12}{\Longrightarrow}$ φ setzt man zu einem Isomorphismus

$$\sigma\colon K_1 := K(\alpha_1) \to K'(\alpha_1') \quad \text{mit } \sigma(\alpha_1) = \alpha_1'$$

fort.

Schreibe $f = (x - \alpha_1) \cdot f_1$ mit $f_1 \in K_1[X]$
$\Rightarrow$ $f^{\varphi} = \big(x - \underbrace{\sigma(\alpha_1)}_{\alpha_1'}\big) \cdot f_1^{\sigma}$ mit $f_1^{\sigma} \in K_1'[X]$.
L ist Zerfällungskörper von f_1, L' ist Zerfällungskörper von f_1^{σ}
$\Rightarrow$ σ setzt sich fort zu einem Isomorphismus $L \to L'$ □

Die Behauptung im Fall $\varphi = \mathrm{id}_K$ ist genau die Aussage von Satz 3.13. □

▶ Bemerkung 3.14
Ist $M \mid K$ eine Erweiterung, die einem Zerfällungskörper L von f enthält, dann ist dieser nicht nur bis auf die Isomorphie sondern als Teilkörper eindeutig bestimmt: $L = K(\alpha_1, \ldots, \alpha_n)$, wobei $\alpha_1, \ldots, \alpha_n$ genau die n Nullstellen von f in M sind.

4. Der algebraische Abschluss

Sei $L \mid K$ eine Körpererweiterung.

Definition 4.1 (algebraisch abgeschlossen)
K ist algebraisch abgeschlossen $\Longleftrightarrow$ jedes $f \in K[X]$ mit $\deg(f) > 0$ hat eine Nullstelle in K.

Lemma 4.2
Es ist äquivalent:

(a) K ist algebraisch abgeschlossen.

(b) Jedes $0 \neq f \in K[X]$ zerfällt über K in Linearfaktoren.

(c) K hat keine echte algebraische Erweiterung.

Beweis.

(a) $\Rightarrow$ (b): Induktion nach $\deg(f)$ (siehe LAAG)

(b) $\Rightarrow$ (c): Sei $L \mid K$ algebraisch, $\alpha \in L$. Schreibe $f = \mathrm{MinPol}(\alpha \mid K)$. Nach (b) zerfällt f in Linearfaktoren über $K \Rightarrow \alpha \in K$

(c) $\Rightarrow$ (a): Sei $f \in K[X]$, $\deg(f) > 0$. Nach Satz 3.9 existiert ein Zerfällungskörper L von f. Da $L \overset{(*)}{=} K$ nach (c) hat f Nullstellen in K.
(($*$) L ist Erweiterung $\to$ die nach (c) trivial ist) □

Definition 4.3 (algebraischer Abschluss)
L ist algebraischer Abschluss von K $:\Longleftrightarrow$ L ist algebraisch abgeschlossen und $L \mid K$ algebraisch.

Lemma 4.4
Ist L algebraischer Abschluss, so ist der relative algebraische Abschluss $\tilde{K}$ ein algebraischer Abschluss von K.

Beweis.

- $\tilde{K}$ ist Körper: Folgerung 2.15
- $\tilde{K} \mid K$ ist algebraisch: Definition
- $\tilde{K}$ ist algebraisch abgeschlossen: Sei $f \in \tilde{K}[X]$ mit $\deg(f) > 0$.
  L algebraisch abgeschlossen $\Rightarrow$ existiert $\alpha \in L$ mit $f(\alpha) = 0 \Rightarrow \alpha$ algebraisch über $\tilde{K} \overset{2.15}{\Longrightarrow} \alpha \in \tilde{K}$. □

■ **Beispiel 4.5**

(a) $\mathbb{C}$ ist algebraisch abgeschlossen (Fundamentalsatz der Algebra, $\nearrow$ II.)

(b) $\mathbb{C}$ ist algebraischer Abschluss von $\mathbb{R}$.

(c) $\tilde{\mathbb{Q}} := \{\alpha \in \mathbb{C} \mid \alpha \text{ algebraisch über } \mathbb{Q}\}$ ist nach Lemma 4.4 ein algebraischer Abschluss von $\mathbb{Q}$.

Lemma 4.6
Sei $L \mid K$ algebraisch, E ein algebraisch abgeschlossener Körper und $\varphi \in \mathrm{Hom}(K, E)$. Dann existiert eine Fortsetzung von φ auf L, d.h. ein $\sigma \in \mathrm{Hom}(L, E)$ mit $\sigma_{|K} = \varphi$.

Beweis. Definiere die Halbordnung

$$\mathfrak{X} := \left\{(M,\sigma) \;\middle|\; K \subseteq M \subseteq L \text{ Zwischenkörper}, \; \sigma \in \operatorname{Hom}(M,E), \; \sigma_{|K} = \varphi\right\}$$

mit der Ordnung

$$(M,\sigma) \subseteq (M',\sigma') :\Longleftrightarrow M \subset M' \text{ und } \sigma'_{|M} = \sigma$$

- $\mathfrak{X} \neq \varnothing$: $(K,\varphi) \in \mathfrak{X}$
- Ist $(M,\sigma)_{i\in I}$ eine Kette in $\mathfrak{X}$, so definieren wir $M := \bigcup_{i\in I} M_i$ und $\sigma\colon M \to E$ durch $\sigma(x) = \sigma_i(x)$ falls $x \in M_i$.

  Dann ist $(M,\sigma) \in \mathfrak{X}$ eine obere Schranke der Kette $(M_i,\sigma_i)_{i\in I}$. Nach Lemma von Zorn existiert (M,σ) maximal. Es ist $M = L$: Sei $\alpha \in L$, $f = \operatorname{MinPol}(\alpha \mid M)$. $f \in E[X]$ hat Nullstelle $\beta \in E$, da E algebraisch abgeschlossen ist $\overset{3.12}{\Longrightarrow}$ existiert Fortsetzung $\sigma' \in \operatorname{Hom}(M(\alpha),E)$ von σ
  $(M,\sigma) \leq (M(\alpha),\sigma') \in \mathfrak{X} \xrightarrow{(M(\alpha),\sigma) \text{ max.}} M = M(\alpha)$, $\alpha \in M$. □

Theorem 4.7 (Steinitz, 1910)
Jeder Körper K besitzt einen bis auf K-Isomorphie eindeutig bestimmten algebraischen Abschluss.

Beweis.
- Eindeutigkeit:
  Seien L_1, L_2 algebraische Abschlüsse von K
  $L_1 \mid K$, L_2 algebraisch abgeschlossen $\overset{4.6}{\Longrightarrow}$ existiert $\sigma \in \operatorname{Hom}(L_1,L_2)$

$$\left.\begin{array}{l} L_1 \text{ algebraisch abgeschlossen } \Rightarrow \sigma(L_1) \cong L_1 \text{ algebraisch abgeschlossen} \\ L_2 \mid K \text{ algebraisch } \Rightarrow L_2 \mid \sigma(L_1) \text{ algebraisch} \end{array}\right\} \overset{4.2}{\Longrightarrow} L_2 = \sigma(L_1).$$

  Somit ist $\sigma\colon L_1 \to L_2$ ein K-Isomorphismus.

- Existenz: Seien
  - $\mathscr{F} = \{f \in K[X] \mid \deg(f) > 0\}$
  - $\mathfrak{X} = (X_f)_{f\in\mathscr{F}}$ Familie von Variablen
  - $R := K[\mathfrak{X}]$ Polynomring in den Variablen X_f $(f \in \mathscr{F})$
  - $I := (f(X_f)\colon f \in \mathscr{F}) \trianglelefteq R$

  Behauptung 1: Es gilt $I \ntrianglelefteq R$.
  Beweis. Angenommen $I = R$. Dann existieren $f_1, \ldots, f_n \in \mathscr{F}$ und $g_1, \ldots, g_n \in R$ mit

$$\sum_{i=1}^{n} g_i \cdot f_i(X_f f_i) = 1.$$

  Sei L ein Zerfällungskörper von $f_1, \ldots, f_n$. Dann existieren $\alpha_1, \ldots, \alpha_n \in L$ mit $f_i(\alpha_i) = 0$ für alle i. Sei $\varphi : R \to L$ der Einsetzungshomomorphismus gegeben durch

$$\varphi_{|K} = \mathrm{id}_K, \quad \varphi(X_{f_i}) = \alpha_i, \quad \varphi(X_f) = 0 \text{ für } f \in \mathscr{F}/\{f_1,\ldots,f_n\}$$

  Dann folgt

$$1 = \varphi(1) = \sum_{i=1}^{n} \varphi(g_i)\cdot\varphi(f_i(X_f)) = \sum_{i=1}^{n} \varphi(g_i)\cdot f_i(\underbrace{\varphi(X_f)}_{=\alpha_i}) = \sum_{i=1}^{n} \varphi(g_i)\cdot \underbrace{f_i(\alpha_i)}_{=0} = 0$$ □

Jedes echte Ideal ist in einem maximalen Ideal von R enthalten (GEO II 2.13)
$\implies$ existiert maximales Ideal $m \trianglelefteq R$ mit $I \subseteq m$. $L_1 := R/m$ ist Körpererweiterung von K, und jedes $f \in \mathscr{F}$ hat eine Nullstelle in L_1, nämlich $f(X_f + m) = f(X_f) + m = 0 + m$. Iteriere dies und

$$K := L_0 \subseteq L_1 \subseteq L_2 \subseteq \cdots,$$

wobei jedes $f \in L_i[X]$, $\deg(f) > 0$ eine Nullstelle in L_{i+1} hat. Setze nun $L = \bigcup_{i=1}^{\infty} L_i$.

Behauptung 2: L ist algebraisch abgeschlossen.

Beweis. Sei $f \in L[X]$, $\deg(f) > 0 \implies f \in L_i[X]$ für ein $i \implies f$ hat eine Nullstelle in $L_{i+1} \subseteq L$ □

Nach Lemma 4.4 ist somit

$$\tilde{K} = \left\{\alpha \in L \,\middle|\, \alpha \text{ algebraisch über } K\right\}$$

ein algebraischer Abschluss von K. □

Definition 4.8 (algebraischer Abschluss)
Mit $\bar{K}$ bezeichnen wir den (bis auf K-Isomorphie eindeutig bestimmten) algebraischen Abschluss von K.

Definition 4.9 (Automorphismengruppe)
$\operatorname{Aut}(L \mid K) := \{\sigma \in \operatorname{Hom}_K(L, L) \mid \sigma \text{ Isomorphismus}\}$, die Automorphismengruppe von $L \mid K$.

▶ Bemerkung 4.10
$\operatorname{Aut}(L \mid K)$ ist Gruppe unter $\sigma \cdot \sigma' = \sigma' \circ \sigma$ und wirkt auf L durch $x^\sigma := \sigma(x)$.

Satz 4.11
Sei $K \subseteq L \subseteq \bar{K}$ ein Zwischenkörper. Jedes $\varphi \in \operatorname{Hom}_K(L, \bar{K})$ lässt sich zu einem $\sigma \in \operatorname{Aut}(\bar{K} \mid K)$ fortsetzen.

Beweis. Sei $\bar{K} \mid K$ algebraisch abgeschlossen und $\bar{K}$ algebraisch abgeschlossen
$\overset{4.6}{\implies}$ existiert Fortsetzung $\sigma \in \operatorname{Hom}_K(\bar{K}, \bar{K})$ von φ

$$\left.\begin{array}{lll} \bar{K} \text{ algebraisch abgeschlossen} & \implies & \sigma(\bar{K}) \text{ algebraisch abgeschlossen} \\ \bar{K} \mid K \text{ algebraisch ist} & \implies & \bar{K} \mid \sigma(\bar{K}) \text{ algebraisch} \end{array}\right\} \bar{K} = \sigma(\bar{K})$$

somit ist $\sigma \in \operatorname{Aut}(\bar{K}, K)$. □

Definition 4.12 (konjugiert)
$\alpha, \beta \in \bar{K}$ sind K-konjugiert $\iff$ existiert $\sigma \in \operatorname{Aut}(\bar{K}, K)$ mit $\sigma(\alpha) = \beta$.

▶ Bemerkung 4.13
K-Konjugiertheit ist eine Äquivalenzrelation auf $\bar{K}$.

Folgerung 4.14
$\alpha, \beta \in \bar{K}$ sind K-konjugiert $\iff \operatorname{MinPol}(\alpha \mid K) = \operatorname{MinPol}(\beta \mid K)$.

Beweis.
($\Rightarrow$) $\sigma(\alpha) = \beta$ mit $\sigma \in \operatorname{Aut}(\bar{K} \mid K)$, $f \in K[X]$, $f(\alpha) = 0 \implies 0 = \sigma(0) = \sigma(f(\alpha)) = f(\sigma(\alpha)) = f(\beta)$

($\Leftarrow$) $\operatorname{MinPol}(\alpha \mid K) = \operatorname{MinPol}(\beta \mid K)$
$\overset{3.5}{\implies}$ existiert K-Isomorphismus $\varphi\colon K(\alpha) \to K(\beta)$ mit $\varphi(\alpha) = \beta$
$\overset{4.11}{\implies}$ existiert Fortsetzung $\sigma \in \operatorname{Aut}(\bar{K}, K)$ von φ. □

■ **Beispiel 4.15**

- $\mathrm{i}, -\mathrm{i} \in \tilde{\mathbb{Q}}$ sind $\mathbb{Q}$-konjugiert: komplex Konjugation (eingeschränkt auf $\tilde{\mathbb{Q}}$)
- $\sqrt{2}$, $-\sqrt{2} \in \tilde{\mathbb{Q}}$ sind $\mathbb{Q}$-konjugiert: $\mathrm{MinPol}(\sqrt{2} \mid \mathbb{Q}) = x^2 - 2 = \mathrm{MinPol}(-\sqrt{2} \mid \mathbb{Q})$

5. Die transzendente Erweiterung

Sei $L \mid K$ eine Körpererweiterung.

Definition 5.1 (algebraisch abhängig)

(a) $a_1, \dots, a_n \in L$ sind algebraisch abhängig über K, wenn ein $0 \neq f \in K(X_1, \dots, X_n)$ existiert mit $f(a_1, \dots, a_n) = 0$.

(b) $(a_i)_{i \in I}$ ist algebraisch abhängig über K, wenn ein endliches $J \subseteq I$ existiert und $(a_i)_{i \in J}$ ist algebraisch abhängig über K.

■ **Beispiel (nicht aus VL, sondern ergänzt!)**

Betrachte die reellen Zahlen $\sqrt{\pi}$ und $2\pi + 1$, beide sind transzendent über $\mathbb{Q}$. Die Singletons $\{\sqrt{\pi}\}$ und $\{2\pi + 1\}$ sind algebraisch unabhängig über $\mathbb{Q}$. Aber die Vereinigung $\{\sqrt{\pi}, 2\pi + 1\}$ ist nicht algebraisch unabhängig in $\mathbb{Q}$, da

$$P(x, y) = 2x^2 - y + 1 = 0$$

ist, wenn $x = \sqrt{\pi}$ und $y = 2\pi + 1$ gesetzt sind.

▶ **Bemerkung 5.2**

(a) (a) ist algebraisch abhängig über $K \iff a$ ist algebraisch über K

(b) $L = K(X_1, \dots, X_n) = \mathrm{Quot}(K[X_1, \dots, X_n]) \implies X_1, \dots, X_n$ sind algebraisch unabhängig über K

(c) Sind π, e unabhängig über $\mathbb{Q}$? Falls "Ja", wäre z.B. $\pi + e$ transzendent über $\mathbb{Q}$

Definition 5.3 (rein transzendent)

$L \mid K$ rein transzendent $:\iff L = K(\mathfrak{X})$ mit $\mathfrak{X} = (a_i)_{i \in I}$ algebraisch unabhängig über K.

Lemma 5.4

$\mathfrak{X} = (a_i)_{i \in I}$ algebraisch unabhängig über $K \implies K(\mathfrak{X}) \cong_K K(X_i : i \in I) = \mathrm{Quot}(K[X_i : i \in I])$.

Beweis. Betrachte K-Isomorphismus

$$\varphi = \begin{cases} K[X_i : I \in I] \to K[a_i : i \in I] \\ f \qquad\qquad\quad \mapsto f(\mathfrak{X}) \end{cases}$$

Da $\mathfrak{X}$ algebraisch unabhängig über K, ist $\mathrm{Ker}(\varphi) = (0)$
$\implies K(\mathfrak{X}) = \mathrm{Quot}(K[\mathfrak{X}]) \cong_K \mathrm{Quot}(K[X_i : i \in I])$. □

Satz 5.5

$L \mid K$ rein transzendent $\implies \tilde{K} = K$.

Beweis. Nach Lemma 5.4 sei o.E. $L = K(X_i : i \in I)$. Weiter o. E. $I = \{1, \dots, n\}$ endlich. Sei $\alpha \in L$ algebraisch über K. Definiere $f = \mathrm{MinPol}(\alpha \mid K)$.
f irreduzibel in $K[X] \overset{\text{Gauss}}{\implies} f$ irreduzibel in $K[X_1, \dots, X_n][X]$
$\overset{\text{Gauss}}{\implies} f$ irreduzibel in $K(X_1, \dots, X_n)[X]$

$\overset{\alpha \in L}{\Longrightarrow}$ $\deg(f) = 1$

$\Longrightarrow$ $\alpha \in K$ □

▶ **Bemerkung 5.6**

Die Umkehrung gilt nicht, da z.B. $L = \mathbb{C}$. Sei $K = \tilde{\mathbb{Q}}$, dann $\tilde{K} = K$, aber $L \mid K$ nicht rein transzendent. Ist $L = K[\mathfrak{X}]$, $\mathfrak{X} = (a_i)_{i \in I}$ algebraisch unabhängig, so wäre $a_i \in L$ aber $\sqrt{a_i} \in \bar{L} \setminus L$.

Definition 5.7 (Transzendentbasis)

$\mathfrak{X} = (a_i)_{i \in I}$ ist eine Transzendentbasis von $L \mid K$ $:\Longleftrightarrow$ $\mathfrak{X}$ ist algebraisch unabhängig über K und $L \mid K(\mathfrak{X})$ algebraisch.

Lemma 5.8

$\mathfrak{X} = (a_i)_{i \in I} \subseteq L$ ist genau dann eine Transzendentbasis von $L \mid K$, wenn $\mathfrak{X}$ maximal algebraisch unabhängig über K ist.

Beweis.

($\Leftarrow$) $a \in L \backslash K(\mathfrak{X}) \xRightarrow{\text{maximal}} \mathfrak{X} \cup \{a\}$ algebraisch abhängig, d.h. existieren $i_1, \dots, i_n \in I$, $0 \neq f \in K[X_1, \dots, X_n, X]$ mit $f(a_{i_1}, \dots, a_{i_n}, a) = 0$

$a_{i_1}, \dots, a_{i_n}$ algebraisch unabhängig über K

$\Longrightarrow \underbrace{f(a_{i_1}, \dots, a_{i_n}, X)}_{\in K(a_{i_1}, \dots, a_{i_n})[X] \subseteq K(\mathfrak{X})[X]} \neq 0$

$\Longrightarrow$ a ist algebraisch über $K(\mathfrak{X})$

($\Rightarrow$) $a \in L \setminus K(\mathfrak{X}) \xRightarrow{L \backslash K(\mathfrak{X}) \text{ alg.}}$ existiert $0 \neq f \in K(\mathfrak{X})[X]$ mit $f(a) = 0$

O.E. (Problem: Nenner kann Koeffizienten in $K(\mathfrak{X})$ haben $\to$ Multiplikation mit Nenner, weil $f(a) = 0$) $f \in K[\mathfrak{X}][X]$, d.h. es existiert $g \in K[X_1, \dots, X_n][X]$ und $i_1, \dots, i_n \in I$ mit $f(X) = g(a_{i_1}, \dots, a_{i_n}, X)$ und $\mathfrak{X} \cup \{a\}$ ist algebraisch abhängig. □

Satz 5.9

Es gibt eine Transzendenzbasis von $L \mid K$.

Beweis. Nach Lemma von Zorn gibt es eine Familie $\mathfrak{X}$ in L, die maximal algebraisch unabhängig über K ist. □

Folgerung 5.10

Jede Erweiterung $L \mid K$ lässt sich zerlegen als

$$\begin{tikzcd} L \arrow[d, "\text{algebraisch}"] \\ K(\mathfrak{X}) \arrow[d, "\text{rein transzendent}"] \\ K \end{tikzcd}$$

Lemma 5.11

Ist $\mathcal{Y} = (b_j)_{j \in J}$ mit $L \mid K(\mathcal{Y})$ algebraisch und $\mathfrak{X} = (a_i)_{i \in I}$ algebraisch unabhängig über K, so existiert $J_0 \subseteq J$ mit $\mathfrak{X} \cup (b_j)_{j \in J_0}$ eine Transzendenzbasis von $L \mid K$.

Beweis. Nach dem Lemma von Zorn existiert $J_0 \subseteq J$ maximal mit $\mathfrak{X}' = \mathfrak{X} \cup (b_j)_{j \in J_0}$ algebraisch unabhängig über K. Für jedes $j \in J$ ist $\mathfrak{X}' \cup \{b_j\}$ algebraisch abhängig über K, somit b_j algebraisch über $K(\mathfrak{X}')$

$\Longrightarrow K(\mathfrak{X} \cup \mathcal{Y}) \mid K(\mathfrak{X}')$ algebraisch
$L \mid K(\mathcal{Y})$ algebraisch $\Longrightarrow L \mid K(\mathfrak{X} \cup \mathcal{Y})$ algebraisch $\xrightarrow{\text{alg. transitiv}} L \mid K(\mathfrak{X}')$ algebraisch. Somit ist $\mathfrak{X}'$ eine Transzendenzbasis. □

Theorem 5.12 (Steinitz, 1910)
Je zwei Transzendenzbasen von $L \mid K$ besitzen die gleiche Mächtigkeit.

Beweis. Seien $\mathfrak{X} = (a_i)_{i \in I}$, $\mathcal{Y} = (b_j)_{j \in J}$ Transzendenzbasis von $L \mid K$.
Beweisen hier nur für J endlich:
Wegen Symmetrie genügt es zu zeigen, dass $|I| \leq |J|$.
Induktion nach $n = |J|$:

$n = 0$: $L \mid K$ algebraisch $\Longrightarrow |I| = 0$

$n > 0$: $L \mid K$ nicht algebraisch $\Longrightarrow |I| > 0$.

O.E. $1 \in I$. Nach Lemma 5.11 existiert ein $J_0 \subset J$ mit $\{a_i\} \cup (b_j)_{j \in J_0}$ eine Transzendentenbasis von $L \mid K$. Da $\mathcal{Y}$ maximal algebraisch unabhängig über K ist, ist $|J_0| \leq |J| - 1$.

Sowohl $\mathfrak{X}' = (a_i)_{i \in I \setminus \{1\}}$ als auch $(b_j)_{j \in J_0}$ sind Transzendentenbasen von $L \mid K(a_1)$:

$K(a_1)(\mathfrak{X}') = K(\mathfrak{X}) \Rightarrow L \mid K(a_1)(\mathfrak{X}')$ algebraisch, analog $L \mid K(a_1)(b_j)_{j \in J_0}$ algebraisch.

Wäre $\mathfrak{X}'$ algebraisch abhängig über $K(a_1)$, so existierte ein

$$0 \neq f \in K(a_1)[X_1, \ldots, X_m], \quad i_1, \ldots, i_m \in I \setminus \{1\}$$

mit $f(a_{i_1}, \ldots, a_{i_m}) = 0$.
O.E. ist $f \in K[a_1][X_1, \ldots, X_m]$, d.h. es existiert $g \in K[X, X_1, \ldots, X_m]$ mit

$$f(X_1, \ldots, X_m) = g(a_1, X_1, \ldots, X_m)$$

im Widerspruch zur algebraischen Unabhängigkeit von $\mathfrak{X}$.

$\xrightarrow{\text{(IH)}} |I| - 1 \leq |J_0| \Rightarrow |I| - 1 \leq |J| - 1 \Rightarrow |I| \leq |J|$. □

Definition 5.13 (Transzendenzgrad)
Der Transzendenzgrad von $L \mid K$ ist die Mächtigkeit $\operatorname{tr.deg}(L \mid K)$ einer Tarnszendenzbasis von $L \mid K$.

Folgerung 5.14
Sind $L \subseteq L \subseteq M$ Körper, so ist

$$\operatorname{tr.deg}(M \mid K) = \operatorname{tr.deg}(M \mid L) + \operatorname{tr.deg}(L \mid K).$$

Beweis. Ist $\mathfrak{X}$ eine Transzendentenbasis von $L \mid K$, $\mathcal{Y}$ eine Transzendentenbasis von $M \mid L$, so ist $\mathfrak{X} \cup \mathcal{Y}$ eine Transzendentenbasis von $M \mid K$.

- $\mathfrak{X} \cup \mathcal{Y}$ ist algebraisch unabhängig über K. Denn ist $f(a_{i_1}, \ldots, a_{i_n}, b_{j_1}, \ldots, b_{j_m}) = 0$ mit $i_1, \ldots, i_n \in I$ und $j_1, \ldots, j_m \in J$ sowie $0 \neq f \in K[X_1, \ldots, X_n, Y_1, \ldots, Y_m]$, so gälte:
  - $f \in K[X_1, \ldots, X_n]$: im Widerspruch zur algebraischen Unabhängigkeit von $\mathfrak{X}$ über K
  - $f \notin K[X_1, \ldots, X_n]$: $0 \neq f(a_{i_1}, \ldots, a_{i_n}, Y_1, \ldots, Y_m) \in L[Y_1, \ldots, Y_m]$ im Widerspruch zur algebraischen Unabhängigkeit von $\mathcal{Y}$ über L.
- $M \mid K(\mathfrak{X} \cup \mathcal{Y})$ algebraisch:

$$\begin{aligned} & L(\mathcal{Y}) = K(\mathfrak{X} \cup \mathcal{Y})(L) \\ \xrightarrow{L \mid K(\mathfrak{X}) \text{ alg.}} \; & L(\mathcal{Y}) \mid K(\mathfrak{X} \cup \mathcal{Y}) \text{ algebraisch} \\ \Rightarrow \; & M \mid K(\mathfrak{X} \cup \mathcal{Y}) \text{ algebraisch.} \end{aligned}$$

□

6. Separable Polynome

Sei K ein Körper, $f \in K[X]$, $n = \deg(f)$.

Definition 6.1
Sei $a \in K$.

(1) $\mu(f, a) := v_{x-a}(f) := \sup\{k \in \mathbb{N}_0 : (x-a)^k \mid f\} \in \mathbb{N}_0 \cup \{\infty\}$ die Vielfachheit der Nullstelle a von f

(2) Nullstelle a von f ist einfach $:\Leftrightarrow \mu(f, a) = 1$

(3) f ist separabel $:\Leftrightarrow$ jede Nullstelle $a \in \bar{K}$ von $f \in \bar{K}[X]$ ist einfach.

▶ **Bemerkung 6.2**

(a) Ist $L \mid K$ eine Körpererweiterung und $g \in K[X]$, so gilt

$$f \mid g \text{ in } K[X] \quad \Leftrightarrow \quad f \mid g \text{ in } L[X]$$

Insbesondere ist die Nullstelle $\mu_K(f, a) = \mu_L(f, a)$. Wir können deshalb von der Vielfachheit der Nullstelle von f sprechen.

(b) $\#\{a \in K \mid f(a) = 0\} \leq \sum_{a \in K} \mu(f, a) \leq \sum_{a \in \bar{K}} \mu(f, a) = \deg(f)$, falls $(f \neq 0)$

(c) Aus (b) folgt insbesondere:

f ist separabel $\Leftrightarrow$ f hat genau $\deg(f)$ paarweise verschiedene Nullstellen in $\bar{K}$

Definition 6.3
Die formale Ableitung von $f = \sum_{i=1}^n a_i X^{i-1}$ ist

$$f' := \frac{\mathrm{d}}{\mathrm{d}x} f(x) := \sum_{i=1} i a_i X^{i-1}$$

Lemma 6.4
Für $f, g \in K[X], a, b \in K$ gelten

(a) $(af + bg)' = af' + bg'$ (Linearität)

(b) $(fg)' = f'g + fg'$ (Produktregel)

(c) $(f(g(x)))' = f'(g(x)) \cdot g'(x)$ (Kettenregel)

Beweis. Übung. □

Lemma 6.5
Sei $f \neq 0$. Für $a \in K$ gilt

$$\mu(f', a) \geq \mu(f, a) - 1$$

mit Gleichheit genau dann, wenn $\operatorname{char}(K) \nmid \mu(f, a)$.

Beweis. Schreibe $f = (X-a)^k \cdot g$, $k = \mu(f, a)$

$k = 0$: $\mu(f', a) \geq 0 > -1$ und $\operatorname{char}(K) \mid 0$

$k > 0$: $f' = k(X-a)^{k-1} g + (X-a)^k \cdot g' \implies \mu(f', a) \geq k$, sowie

$$\begin{aligned} \mu(f', a) \geq k \quad &\Leftrightarrow \quad (X-a)^k \mid k(X-a)^{k-1} \cdot g \\ &\Leftrightarrow \quad X - a \mid k \cdot g \\ &\Leftrightarrow \quad X - a \mid k \\ &\Leftrightarrow \quad k = 0 \text{ in } K \\ &\Leftrightarrow \quad \operatorname{char}(K) \mid k \end{aligned}$$

□

Satz 6.6
Sei $f \neq 0$. Dann gilt:

$$f \text{ separabel} \quad \Leftrightarrow \quad \operatorname{ggT}(f, f') = 1$$

Beweis.
($\Rightarrow$) f separabel

$\Rightarrow f = c \cdot \prod_{i=1}^n (X - a_i)$ mit $c \in K$, $a_1, \dots, a_n \in \bar{K}$ paarweise verschieden und $\mu(f, a_i) = 1$

$\xRightarrow[\operatorname{char}(K)\nmid 1]{6.5} \mu(f', a_i) = 0 \ \forall i$

$$\Rightarrow \operatorname{ggT}(f, f') = \prod_{a \in \bar{K}} (X-a)^{\min\{\mu(f,a), \mu(f',a)\}} = 1$$

($\Leftarrow$) f nicht separabel $\Rightarrow \exists a \in \bar{K}$ mit $\mu(f, a) \geq 2 \overset{6.5}{\Longrightarrow} \mu(f', a) \geq 1$.

Mit $g = \operatorname{MinPol}(a \mid K)$ gilt: $g \mid f \Rightarrow \operatorname{ggT}(f, f') \neq 1$ □

Lemma 6.7
$f' = 0 \Leftrightarrow \exists g \in K[X]$ mit $f(X) = g(X^p)$ und $p = \operatorname{char}(K)$.

Beweis. Ist $f = \sum_{i=1}^n a_i X^i \Rightarrow f' = \sum_{i=1}^n i a_{i-1} X^{i-1}$ und

$$\begin{aligned} f' = 0 \quad &\Leftrightarrow \quad i a_i = 0 \text{ in } K \ \forall i \\ &\Leftrightarrow \quad \forall i\colon i = 0 \text{ in } K \text{ oder } a_i = 0 \\ &\Leftrightarrow \quad f = a_0 + a_p X^p + \dots + a_{pm} X^{pm} = g(X^p) \text{ mit } g = a_0 + a_p X + \dots + a_{pm} X^m \end{aligned}$$

□

Folgerung 6.8
Sei f irreduzibel

(a) Ist $\operatorname{char}(K) = 0$, so ist f separabel

(b) Ist $\operatorname{char}(K) = p > 0$, so sind äquivalent

  (1) f ist inseparabel

  (2) $f' = 0$

  (3) $f(X) = g(X^p)$ für ein $g \in K[X]$

Beweis. f irreduzibel $\implies \underbrace{\operatorname{ggT}(f, f') \sim 1}_{\overset{6.6}{\iff} f \text{ sep}}$ oder $\underbrace{\operatorname{ggT}(f, f') \sim f}_{\overset{6.6}{\iff} f \text{ sep.}}$.

Da $\deg(f') = \deg(f)$ ist

$$f \mid f' \quad \iff \quad f' = 0 \quad \iff \quad f(X) = g(X^p) \text{ für ein } g$$

Im Fall $\operatorname{char}(K) = 0$ tritt dieser Fall nicht ein. □

Definition 6.9 (vollkommen)
K ist <u>vollkommen</u> $\iff$ jedes irreduzibel $f \in K[X]$ ist separabel.

■ **Beispiel 6.10**

(a) $\operatorname{char}(K) = 0 \implies K$ ist vollkommen

(b) $K = \bar{K} \implies K$ ist vollkommen

(c) $K = \mathbb{F}_p(t)$ ist nicht vollkommen:

$$\begin{aligned} f &= X^p - t \in K[X] \text{ ist irreduzibel} \\ f' &= pX^{p-1} = 0 \implies f \text{ nicht seperabel.} \end{aligned}$$

Tatsächlich hat f nur eine Nullstelle in $\bar{K}$: $f = X^p - t \overset{\text{V1}}{=} (X - t^{\frac{1}{p}})^p$.

Definition 6.11
Sei $\operatorname{char}(K) = p > 0$.

(1) Der Frobenius-Endomorphismus von K ist

$$\Phi_p : \begin{cases} K \to K \\ X \mapsto X^p \end{cases}$$

(2) $K^p = \operatorname{Im}(\Phi_p) = \{a^p \mid a \in K\}$

Satz 6.12
Sei $\operatorname{char}(K) = p > 0$. Dann ist $\Phi_p \in \operatorname{End}(K) := \operatorname{Hom}(K, K)$

Beweis. Für $a, b \in K$ ist

- $\Phi_p = (ab)^p = a^p \cdot b^p = \Phi_p(a) \cdot \Phi_p(b)$
- $\Phi_p(a + b) = (a + b)^p = \sum_{i=0}^{p} \binom{p}{i} a^i b^{p-i} = b^p + a^p = \Phi_p(a) + \Phi_p(b)$, da $p \mid \binom{p}{i}$ für $i = 1, \dots, p-1$ (V1).
- $\Phi_p(1) = 1^p = 1$ □

▶ Bemerkung 6.13

(a) Da $\Phi_p \in \mathrm{End}(K)$ ist K^p ein Teilkörper von K und Φ_p ist injektiv.

(b) Insbesondere gibt es zu jedem $a \in K$ ein eindeutig bestimmtes $a^{\frac{1}{p}} \in \bar{K}$ mit

$$\Phi_p(a^{\frac{1}{p}}) = (a^{\frac{1}{p}})^p = a$$

(c) Für $a \in \mathbb{F} \cong \mathbb{F}_p$ ist $\Phi_p(a) = a$. (z.B. $\Phi_p(1) = 1$ oder kleiner Satz von Fermat)

> **Lemma 6.14**
> Sei $\mathrm{char}(K) = p > 0$, $a \in K \setminus K^p$. Dann ist $f = X^p - a$ irreduzibel und inseparabel

Beweis. Sei $\alpha \in \bar{K}$ mit $f(\alpha) = 0$, $g = \mathrm{MinPol}(\alpha \mid K)$

$\implies g \mid f = X^p - \alpha = (X - \alpha)^p$

$\implies g \equiv (X - \alpha)^k$ mit $k \leq p$.

$a \notin K^p$

$\implies \alpha \notin K \implies k > 1$

$\implies g$ ist inseperabel

$\xRightarrow{g \text{ irred.}} g(X) = h(X^p)$ für ein h

$\implies k = p \implies f = g$ irreduzibel ☐

> **Satz 6.15**
> Genau dann ist K vollkommen, wenn
>
> (i) $\mathrm{char}(K) = 0$ oder
>
> (ii) $\mathrm{char}(K) = ß > 0$ und $K^P = K$

Beweis.

- $\mathrm{char}(K) = 0$: klar (Beispiel 6.10 (a))
- $\mathrm{char}(K) = p > 0$:
  (⇒) Es existiert ein $a \in K \setminus K^p$, so ist K nicht vollkommen nach Lemma 6.14.
  (⇐) Sei $f(X) \in K[X]$ irreduzibel und inseparabel. Nach Folgerung 6.8 existiert ein $g(X) \in K[X]$ mit

  $$f(X) = g(X^p)$$

  Setze $g(X) = \sum_{i=0}^n a_i X^i \in K[X]$. Dann ist

  $$f(X) = g(X^p) = \sum_{i=0}^n a_i \left(X^i\right)^p \overset{=}{\mathrm{V}}1 \left(\sum_{i=0}^n \underbrace{a_i^{1/n}}_{\in K \text{ da } K^p = K} X^i \right)^p,$$

  folglich ein Widerspruch. ☐

■ Beispiel 6.16

K endlich $\Rightarrow$ K vollkommen (Bemerkung 6.13 (a), Satz 6.15).

7. Separable Erweiterungen

Sei K ein Körper und $L \mid K$ algebraische Körpererweiterung.

▶ Bemerkung 7.1
Für $L = K(\alpha)$ mit $f = \operatorname{MinPol}(\alpha \mid K$ ist

$$[L : K] = \deg(f) \geq \left|\left\{\beta \in \bar{K} \;\middle|\; f(\beta) = 0\right\}\right| \overset{3.12}{=} |\operatorname{Hom}_{\mathbb{K}}(L, \bar{K})|$$

mit Gleichheit genau dann wenn f separabel.

Definition 7.2
Sei $\alpha \in L$.

1. α ist separabel über K :⇔ $\operatorname{MinPol}(\alpha \mid K)$ ist separabel.
2. $L \mid K$ ist separabel :⇔ jedes $\alpha \in L$ ist separabel über K.
3. Der Separabilitätsgrad von $L \mid K$ ist

$$[L : K]_{\mathrm{S}} = |\operatorname{Hom}_{\mathbb{K}}(L, \bar{K})|$$

Lemma 7.3
Sei E algebraisch abgeschlossen, $\varphi \in \operatorname{Hom}(K, E)$. Dann ist

$$\left|\left\{\psi \in \operatorname{Hom}(L, E) \;\middle|\; \psi_{\mathbb{K}} = \varphi\right\}\right| = [L : K]_{\mathrm{S}}$$

Beweis. Nach Lemma 4.6 existiert ein $g \in \operatorname{Hom}(\bar{K}, E)$ mit $g_{|K} = \varphi$. Ohne Einschränkung ist $E = \widetilde{\varphi(K)} = g(\bar{K})$, d.h. g ist Isomorphismus. Dann ist die Abbildung

$$\begin{cases} \operatorname{Hom}_{\mathbb{K}}(L, \bar{K}) \Rightarrow \left\{\psi \in \operatorname{Hom}(L, E) \;\middle|\; \psi_{|K} = \varphi\right\} \\ \sigma \qquad\qquad \mapsto g \circ \sigma \end{cases}.$$

Diese ist bijektiv mit Umkehrabbildung $\psi \mapsto g^{-1} \circ \psi$. □

Satz 7.4
Sind $K \subset L \subset M$ Körer mit $M \mid K$ algebraisch, so ist

$$[M : K]_{\mathrm{S}} = [M : L]_{\mathrm{S}}[L : K]_{\mathrm{S}}$$

Insbesondere ist $[L : K]_{\mathrm{S}} \leq [M : K]_{\mathrm{S}}$.

Beweis. Betrachte die Abbildung

$$f\colon \begin{cases} \operatorname{Hom}(M, \bar{K}) \to \operatorname{Hom}_{\mathbb{K}}(L, \bar{K}) \\ \sigma \qquad\qquad\quad \mapsto \sigma_{|L} \end{cases}.$$

Für $\tau \in \mathrm{Hom}_{\mathbb{K}}(L, \bar{K})$ ist

$$f^{-1}(\{\tau\}) = \left|\left\{\sigma \in \mathrm{Hom}_{\mathbb{K}}(M, \bar{K}) \;\middle|\; \sigma_{|L} = \tau\right\}\right| = [M : L]_{\mathrm{S}}$$

Daher gilt $[M : K]_{\mathrm{S}} = [M : L]_{\mathrm{S}}[L : K]_{\mathrm{S}}$. □

Lemma 7.5
Sei $L \mid K$ endlch und $p = \mathrm{char}(K) > 0$. Dann ist

$$[L : K] = p^l [L : K]_{\mathrm{S}}$$

für ein $L \in \mathbb{N}$. Insbesondere ist $[L : K]_{\mathrm{S}} \leq [L : K]$.

Beweis. Schreibe $L = K(\alpha_1, \dots, \alpha_n)$, ohne Einschränkung ist $n = 1$ (nach Sätze 1.12 und 7.4). Sei $f = \mathrm{MinPol}(\alpha_1 \mid K)$ und $l \in \mathbb{N}$ die größte Zähl mit

$$f(X) = g(X^{lp}), \quad g(X) \in K[X].$$

Dann ist $g(X)$ irreduzibel und separabel nach Folgerung 6.8. Daher gilt

$$[L : K]_{\mathrm{S}} \overset{7.1,7.2}{=} \left|\left\{x \in \bar{K} \;\middle|\; f(x) = 0\right\}\right| = \left|\left\{x \in \bar{K} \;\middle|\; g(x) = 0\right\}\right| = \deg(g) = \frac{\deg(f)}{p^l} = \frac{[L : K]}{p^l},$$

sodass $[L : K] = p^l [L : K]_{\mathrm{S}}$. □

Satz 7.6
Für $L \mid K$ endlich sind äquivalent

(1) $L \mid K$ ist separabel.

(2) $L = K(\alpha_1, \dots, \alpha_n)$ mit $\alpha_1, \dots, \alpha_n$ separabel über K

(3) $[L : K]_{\mathrm{S}} = [L : K]$.

Beweis.
(1) ⇒ (2) klar nach Definition 7.2

(2) ⇒ (3) Da α_i separabel über K ist α_i separabel über $K(\alpha_1, \dots, \alpha_{n-1})$. Daher ist

$$[K(\alpha_1, \dots, \alpha_i) : K(\alpha_1, \dots, \alpha_{i-1})]_{\mathrm{S}} \overset{7.1}{=} [K(\alpha_1, \dots, \alpha_i) : K(\alpha_1, \dots, \alpha_{i-1})]$$

Nach Sätze 1.12 und 7.4 gilt dann

$$[L : K]_{\mathrm{S}} = [L : K]$$

(3) ⇒ (1) Für $\alpha \in L$ ist mit $l \in \mathbb{N}$

$$[L : K] \overset{1.12}{=} [L : K(\alpha)][K(\alpha) : K] \overset{7.5}{\geq} [L : K(\alpha)]_{\mathrm{S}} \cdot p^l [K(\alpha) : K]_{\mathrm{S}} \overset{7.4}{=} [L : K]_{\mathrm{S}} p^l \overset{(3)}{=} [L : K] p^l,$$

daher $l = 0$, d.h. $[K(\alpha) : K] = [K(\alpha) : K]_{\mathrm{S}}$. Nach Bemerkung 7.1 ist α separabel über K, d.h. (1) gilt. □

Folgerung 7.7
Der relative, separable Abschluss

$$L_S = \{\alpha \in L \mid \alpha \text{ separabel über } K\}$$

von K in L ist Teilkörper in L.

Beweis. Folgt aus Satz 7.6 (vergleiche Folgerung 2.15). □

Folgerung 7.8
Seien $K \subset L \subset M$ mit $M \mid K$ algebraisch. Dann gilt:

$$M \mid K \text{ separabel} \quad \Leftrightarrow \quad M \mid L \text{ separabel und } L \mid K \text{ separabel}$$

Beweis.

($\Rightarrow$) klar

($\Leftarrow$) Sei $\alpha \in M$, setzte $f = \mathrm{MinPol}(\alpha \mid L) = \sum_{i=0}^{n} a_i X^i$ und $L_0 = K(a_0, \ldots, a_n)$. Da $M \mid L$ separabel ist f separabel. Daher ist α separabel über L_0, d.h $L_0(\alpha) \mid L_0$ ist separabel (siehe Satz 7.6). Da $L \mid K$ separabel ist, ist auch $L_0 \mid K$ separabel und es gilt

$$[L_0(\alpha) \mid K]_S \overset{7.4}{=} [L_0(\alpha) : L_0]_S [L_0 : K]_S \overset{7.5}{=} [L_0(\alpha) \mid L_0][L_0 : K] \overset{1.2}{=} [L_0(\alpha) \mid K]$$

Deswegen ist $L_0(\alpha) \mid K$ separabel (siehe Satz 7.6). Insbesondere ist α separabel über K. □

Folgerung 7.9
Sei $K \subset L_1$, $L_2 \subset M$ Körper mit $M \mid K$ algebraisch. Sind $L_1 \mid K$ und $L_2 \mid K$ separabel,so auch die Komposition $L1 \cdot_2 := K(L_1, L_2)$.

Beweis. Es sei $\alpha \in L_1 L_2$. Dann gibt es $x_1, \ldots, x_n \in L_1$ und $y_1, \ldots, y_m \in L_2$ mit $\alpha \in K(x_1, \ldots, x_n, y_1, \ldots, y_n) =: L_0$. Da x_i, y_i separabel über K, so ist $L_0 \mid K$ separabel. Nach Satz 7.6. Insbesondere ist α separabel über K.□

Definition 7.10
Die Erweiterung $L \mid K$ ist <u>rein separabel</u> $:\Leftrightarrow$ jedes $\alpha \in L \setminus K$ ist inseparabel über K.

Beweis. Ist $p = \mathrm{char}(K) > 0$, so sind äquivalent

(1) $\Rightarrow$ (2) Sei $\alpha \in L$, $f = \mathrm{MinPol}(\alpha \mid K) = g(X^{p^l})$ mit l maximal und $g \in K[X]$ (wie in Lemma 7.5). Dann ist α^{pl} separabel über K. Da $L \mid K$ rein inseparabel ist, folgt $\alpha^{p^l} \in K$.

(2) $\Rightarrow$ (3) Sei $\varphi \in \mathrm{Hom}_{\mathbb{K}}(L, \bar{K})$ Für $\sigma \in L$ ist

$$\sigma(\alpha) = \sigma(\underbrace{\alpha^{p^l}}_{\in K})^{1/p\,l} = (\alpha^{p^l})^{1/p\,l} = \alpha,$$

also $\sigma_{|L} = \mathrm{id}_L$ und daher $[L : K]_S = 1$.

(3) $\Rightarrow$ (1) Es sei $\alpha \in L \setminus K$. Es ist

$$[K(\alpha) : K] > 1 \overset{(3)}{=} [L : K]_S \overset{7.4}{\geq} [K(\alpha) : K]_S,$$

also ist α inseparabel über α nach Satz 7.6. □

■ **Beispiel 7.11**

Die Erweiterung $\mathbb{F}_p(t) \mid \mathbb{F}_p(t)^p = \mathbb{F}_p(t)$ ist rein inseparabel vom Grad p.

▶ **Bemerkung 7.12**

Jede algebraische Erweiterung $L \mid K$ hat also eine Unterteilung in eine separablen und inseparablen Teil. Es gilt

$$[L:K]_{\mathrm{S}} \overset{7.4}{=} [L:L_{\mathrm{S}}]_{\mathrm{S}}[L_{\mathrm{S}}:K] \underset{7.6}{\overset{7.11}{=}} 1 \cdot [L_{\mathrm{S}}:K] = [L_{\mathrm{S}}:K]$$

8. Norm und Spur

Sei $L \mid K$ endliche Körpererweiterung und $\alpha \in L$.

▶ **Bemerkung 8.1**

L ist ein K-Vektorraum $\implies$ $\mathrm{End}_K(L)$ ist ein K-Vektorraum und ein (nicht kommutativer) Ring unter Komposition.

Definition 8.2 (Spur, Norm)

(a)
$$\mu_\alpha\colon \begin{cases} L & \to L \\ x & \mapsto \alpha x \end{cases} \in \mathrm{End}_K(L)$$

(b) $N_{L|K}(\alpha) := \det(\mu_\alpha$, die $(L \mid K)$- Norm von α

$\mathrm{Tr}_{L|K}(\alpha) := \mathrm{Tr}(\mu_\alpha)$, die $(L \mid K)$-Spur von α

(c) $\chi_\alpha :=$ charakteristisches Polynom von μ_α

$f_\alpha :=$ Minimalpolynom von μ_α

Lemma 8.3

(a) $f_\alpha = \mathrm{MinPol}(\alpha \mid K)$

(b) $\chi_\alpha = f_\alpha^m$ für $m = [L : K(\alpha)]$

Beweis.

(a) Die Abbildung

$$\mu\colon \begin{cases} L \to \mathrm{End}_K(L) \\ \beta \mapsto \mu_\beta \end{cases} \tag{$\star$}$$

ist K-linearer Ringhomomorphismus: ✓

Sei $g := \mathrm{MinPol}(\alpha \mid K)$. Dann

$$\left.\begin{array}{llll} g(\mu_\alpha) \overset{(\star)}{=} \mu_{g(\alpha)} & = 0 \in \mathrm{End}_K(L) & & \implies f_\alpha \mid g \\ \mu_{f_\alpha(\alpha)} \overset{(\star)}{=} f_\alpha(\mu_\alpha) & = 0 \in \mathrm{End}_K(L) & \overset{\mu \text{ inj.}}{\implies} f_\alpha(\alpha) = 0 & \implies g \mid f_\alpha \end{array}\right\} \implies f_\alpha = g$$

(b) Charakteristisches Polynom und Minimalpolynom haben die gleichen irreduziblen Faktoren: ↗ LAAG VIII.7.6 oder direkt:

V n-dimensionaler K-VR, $\varphi \in \mathrm{End}_K(V)$, $\mathscr{B}$ Basis von $V \rightsquigarrow A = M_{\mathscr{B}}(f)$. $\chi_\varphi = \chi_A \in K[X]$ zerfällt in Linearfaktoren in $\bar{K}[X]$

$\implies$ lese $\chi_\varphi = \chi_A$ und $P_\varphi = P_A$ aus der Jordan-Normalform von A ab.

$f_\alpha = \mathrm{MinPol}(\alpha \mid K)$ irreduzibel $\implies$ $\chi_\alpha = f_\alpha^m$ für ein m und

$$\left.\begin{array}{ll} \deg(f_\alpha) = \deg(\alpha \mid K) & = [K(\alpha) : K] \\ \deg(\chi_\alpha) = \dim_K L & = [L : K] \end{array}\right\} \implies m = \frac{\deg(\chi_\alpha)}{\deg(f_\alpha)} = \frac{[L : K]}{[K(\alpha) : K]} = [L : K(\alpha)]$$

□

■ **Beispiel 8.4**

Sei $\mathbb{C} = \mathbb{R} + \mathbb{R}\mathrm{i}$, $\alpha = x + y\mathrm{i} \in \mathbb{C}$.

$\Rightarrow$ μ_α bezüglich Basis $(1, i) = \mathcal{B}$ ist

$$M_{\mathcal{B}}(\mu_\alpha) = \begin{pmatrix} x & -y \\ y & x \end{pmatrix}$$

$$\begin{aligned}
\Rightarrow\ N_{\mathbb{C}|\mathbb{R}}(\alpha) &= \det\big(M_{\mathcal{B}}(\mu_\alpha)\big) = x^2 + y^2 = |\alpha|^2 = \alpha\bar{\alpha}, \\
\mathrm{Sp}_{\mathbb{C}|\mathbb{R}}(\alpha) &= \mathrm{Sp}\big(M_{\mathcal{B}}(\mu_\alpha)\big) = 2\alpha = \alpha + \bar{\alpha} \\
\chi_\alpha(t) &= \det(\mathbb{1} - A) = (t - x)^2 + y^2 = t^2 - 2xt + x^2 + y^2 = t^2 - 2\mathrm{Sp}_{\mathbb{C}|\mathbb{R}}(\alpha)t + N_{\mathbb{C}|\mathbb{R}}(\alpha) \\
&= (t - \alpha)(x - \bar{\alpha}), \\
f_\alpha(t) &= \begin{cases} t - \alpha, & \alpha \in \mathbb{R}, \\ (t - \alpha)(t - \bar{\alpha}), & \alpha \notin \mathbb{R} \end{cases}
\end{aligned}$$

Lemma 8.5

Seien $n = [L : K]$ und $\alpha,\beta \in L$, $\lambda \in K$.

(a) $N_{L|K}(\alpha\beta) = N_{L|K}(\alpha) \cdot N_{L|K}(\beta)$,

(b) $\mathrm{Sp}_{L|K}(\lambda\alpha + \beta) = \lambda\,\mathrm{Sp}_{L|K}(\alpha) + \mathrm{Sp}_{L|K}(\beta)$,

(c) $N_{L|K}(\lambda) = \lambda^n$, $\mathrm{Sp}_{L|K}(\lambda) = n \cdot \lambda$,

(d) Ist $f_\alpha = X^r + a_{r-1}X^{r-1} + \cdots + a_0$ und $m = [L : K(\alpha)] = n/r$, so ist

$$N_{L|K}(\alpha) = (-1)^n a_0^m, \quad \mathrm{Sp}_{L|K}(\alpha) = -ma_{r-1}$$

Beweis.

(a), (b) klar: Multiplikativität der Determinante und Linearität der Spur

(c) $M_{\mathcal{B}}(\mu_\lambda) = \lambda\mathbb{1}$ für alle Basen $\mathcal{B}$ von L.

(d) $\chi_\alpha = X^n + b_{n-1}X^{n-1} + \cdots + b_0$
$\Rightarrow$ $\det \mu_\alpha = (-1)^n\chi_\alpha(0) = (-1)^n b_0$, $\mathrm{Sp}_{\mu_\alpha} = -b_{n-1}$
$\chi_\alpha = \big(f_\alpha\big)^m$
$\Rightarrow$ $N_{L|K}(\alpha) = \det(\mu_\alpha) = (-1)^n a_0^m$, $\mathrm{Sp}_{L|K}(\alpha) = \mathrm{Sp}\,\mu_\alpha = -b_{n-1} = -m \cdot a_{n-1}$ □

▶ **Bemerkung 8.6**

(a) Ist α inseparabel über K, so ist $f_\alpha(X) = g(X^r)$ für ein $g \in K[X]$, und somit ist

$$\mathrm{Sp}_{L|K}(\alpha) = -m \cdot \underbrace{a_{r-1}}_{=0} = 0$$

(b) Ist $L \mid K(\alpha)$ inseparabel, so ist $m = p^d \cdot [L : K(\alpha)]_S$, somit ist ist

$$\mathrm{Sp}_{L|K}(\alpha) = \underbrace{m}_{=0} \cdot a_{r-1} = 0$$

(c) Aus (a) und (b) folgt:

$$L \mid K \text{ inseparabel} \quad \Leftrightarrow \quad \mathrm{Sp}_{L|K} = 0$$

Satz 8.7
Ist $\alpha \in L$, $n = [L : K] = q \cdot r$ und $r = [L : K]_S$ sowie $\hom_K(L, \bar{K}) = \{\sigma_1, \dots, \sigma_r\}$, so gilt

$$N_{L|K}(\alpha) = \left(\prod_{r=1}^{n} \sigma_j(\alpha) \right)^q, \qquad \mathrm{Sp}\,(\alpha) = q \sum_{i=1}^{r} \sigma_i(\alpha)$$

Beweis. Sei $n_1 = [K(\alpha) : K] = r_1 q_1$ und $n_2 = [L : K(\alpha)] = r_2 q_2$. Schreibe

$$f_\alpha = X^{r_1} + a_{n_1-1} X^{n_1-1} + \dots + a_0 = \prod_{i=1}^{r_1} \big(X - \tau_i(\alpha)\big)^{q_1} = g\big(X^{q_1}\big), \quad g(X) = \prod_{i=1}^{r_1} \big(X - \tau_i^{q_1}(\alpha)\big)$$

Jedes τ_i hat genau r_2 viele Fortsetzungen zu einem $\sigma_j \in \hom_K(L \mid \bar{K})$ (Lemma 7.3), sodass

$$\left(\prod_{j=1}^{r} \sigma_j(\alpha) \right)^q = \left(\prod_{i=1}^{r_1} \tau_i(\alpha)^{r_2} \right)^q = \big((-1)^{r_1} a_0\big)^{r_2 q_2} = (-1)^n a_0^{r_2} \overset{8.5}{=} N_{L|K}(\alpha),$$

$$q \sum_{i=1}^{r} \sigma_j(\alpha) = q r_2 \sum_{i=1}^{r_1} \tau_j(\alpha) = -q_2 r_1 a_{n_1-1} = \mathrm{Sp}_{L|K}(\alpha)$$ □

Lemma 8.8
Seien $K \subseteq L \subseteq M$ Körper mit $M \mid K$ endlich und sei $\alpha \in M$. Dann ist

- $N_{M|K}(\alpha) = N_{L|K}\big(N_{M|L}(\alpha)\big)$
- $\mathrm{Tr}_{M|K}(\alpha) = \mathrm{Tr}_{L|K}\left(\mathrm{Tr}_{M|L}(\alpha)\right)$

Beweis. Sei $[L : K] = q_1 \cdot r_1$, $[M : L] = q_2 \cdot r_2$; $\mathrm{Hom}(M, \bar{L}) = \{\sigma_1, \dots, \sigma_{r_2}\}$. Fixiere die Einbettung $L \subseteq \bar{K}$ und setze τ_i fort zu $\tilde{\tau}_i \in \mathrm{Aut}(\bar{K} \mid K)$(Satz 4.11) Dann ist

$$\mathrm{Hom}_K(M, \bar{K}) = \left\{ \tilde{\tau}_i \circ \sigma_j \,\middle|\, i = 1, \dots, r_1,\ j = 1, \dots, r_2 \right\},$$

denn $\#\,\mathrm{Hom}(M, \bar{K}) = [M : K]_S = r_1 \cdot r_2$ und

$$\begin{aligned}
&\tilde{\tau}_i \circ \sigma_j = \tilde{\tau}_{i'} \circ \sigma_{j'} \\
\Rightarrow\ & \sigma_j = \left(\tilde{\tau}_i^{-1} \circ \tilde{\tau}_{i'}\right) \circ \sigma_{j'} \\
\Rightarrow\ & \tilde{\tau}_i^{-1} \circ \tilde{\tau}_i\big|_L = \mathrm{id}_L \\
\Rightarrow\ & \tau_i = \tau_{k'} \quad \Rightarrow i = i' \quad \Rightarrow \sigma_j = \sigma_{j'} \quad \Rightarrow j = j' \\
\Rightarrow\ & N_{L|K}\big(N_{M|L}(\alpha)\big) \overset{8.7}{=} N_{L|K} \left(\prod_{j=1}^{r_2} \sigma_i(\alpha) \right)^{q_2} \overset{8.7}{=} \prod_{i=1}^{r_1} \tilde{\tau}_i \left(\prod_{j=1}^{r_2} \sigma_j(\alpha) \right)^{q_1 q_2} = \left(\prod_{i,j} \big(\tilde{\tau}_i \circ \sigma_j\big)(\alpha) \right)^{q_1 q_2} \overset{8.7}{=} N_{M|K}(\alpha)
\end{aligned}$$

Analog für die Spur. □

Theorem 8.9 (Unabhängigkeit der Charaktere, Artin)
Sei G eine Gruppe. Sind $\chi_1, \dots, \chi_n \in \operatorname{Hom}(G, K^\times)$ paarweise verschieden, so sind sie linear unabhängig im K-Vektorraum $\operatorname{Abb}(G, K)$.

Beweis. Seien $\chi_1, \dots, \chi_n$ linear abhängig, oE $n \geq 2$ minimal, d.h.

$$\sum_{i=1}^n a_i \chi_i = 0 \quad \text{mit } a_1, \dots, a_n \in K^\times.$$

Sind $\chi_1 \neq \chi_n \implies \exists g \in G$ mit $\chi_1(g) \neq \chi_n(g)$. Ist die Summe $\sum a_i \chi_i = 0$, so folgt, dass $\forall h \in G$ ist $\sum_{i=1}^n a_i \chi_i(h) = 0$ und

$$\implies \forall h \in G\colon \begin{cases} \sum_{i=1}^n a_i \cdot \underbrace{\chi_i(hg)}_{\chi_i(h)\cdot\chi_i(g)} = 0 \\ \sum_{i=1}^n a_i \cdot \chi_i(h) \cdot \chi_i(g) = 0 \end{cases}$$

$$\implies 0 = \sum_{i=1}^n a_i \cdot \chi_i(h)\big(\chi_i(g) - \chi_n(g)\big) = \sum_{i=1}^{n-1} a_i\big(\chi_i(g) - \chi_n(g)\big) \cdot \chi_i(h)$$

$$\implies \sum_{i=1}^{n-1} a_i \cdot \big(\chi_i(g) - \chi_n(g)\big) \cdot \chi_i = 0$$

$a_n(\chi_1(g) - \chi_n(g)) \neq 0$, was ist ein Widerspruch zur Minimalität von n. □

Folgerung 8.10
Genau dann ist $\operatorname{Tr}_{L|K} \neq 0$, wenn $L \mid K$ separabel.

Beweis.

($\Rightarrow$) Bemerkung 8.6

($\Leftarrow$) Sei $\operatorname{Hom}_K(L, \bar{K}) = \{\sigma_1, \dots, \sigma_n\}$. $\sigma_i|_{L^\times} \in \operatorname{Hom}_K(L^\times, K^\times)$
$\overset{8.7}{\implies} \sigma_1, \dots, \sigma_n$ sind $\bar{K}$-linear unabhängig. Insbesondere ist $\operatorname{Tr}_{L|K} = \sum_{i=1}^n \sigma_i \neq 0$. □

9. Einfache Erweiterung

Sei K unendlich, $L \mid K$ endliche Erweiterung.

▶ Bemerkung 9.1

$L \mid K$ einfach $\iff L = K(\alpha)$ für ein $\alpha \in L$. Ein solches α heißt ein primitives Element von $L \mid K$.

Satz 9.2

$L \mid K$ einfach $\quad\Leftrightarrow\quad$ Die Menge der Zwischenkörper von $\mathcal{M} = \{M \mid K \subseteq M \subseteq L\}$ ist endlich.

Beweis.

($\Rightarrow$) Sei $L = K(\alpha)$, $f = \mathrm{MinPol}(\alpha \mid K)$. Für $M \in \mathcal{M}$ setze

$$g := \mathrm{MinPol}(\alpha \mid M) = \sum_{i=0}^{n} a_i X^i,$$
$$M_0 := K(a_0, \dots, a_n).$$

Dann gilt $g \mid f$ in $L[X]$, es gibt also nur endlich viele solche g. Da $K \subseteq M_0 \subseteq M \subseteq L$ und

$$[L : M_0] = [M_(\alpha) : M_0] = \deg(g) = [M(\alpha) : M] = [L : M]$$

ist $M = M_0$ durch g bestimmt.

($\Leftarrow$) Sei $L = K(\alpha_1, \dots, \alpha_r)$. Es genügt, die Behauptung für $r = 2$ zu zeigen. Sei also $L = K(\alpha, \beta)$, oE $\beta \neq 0$. Da $|K| = \infty$ ist $|\{\alpha + c\beta \mid c \in K\}| = \infty$. Ist $|\mathcal{M}| < \infty$, so existiert somit c, $c' \in K$ mit $c \neq c'$ und $K(\alpha + c\beta) = K(\alpha + c'\beta) =: M \in \mathcal{M}$

$\implies M \ni (\alpha + c\beta) \cdot (\alpha + c'\beta) = (\underbrace{c - c'}_{\in K^\times})\beta$

$\implies \beta \in M \implies \alpha \in M$

$\implies L = K(\alpha, \beta) \subseteq M \subseteq L$

$\implies L = M = K(\alpha + c\beta)$. □

▶ Bemerkung 9.3

(a) Insbesondere gilt: $K \subseteq M \subseteq L$, $L \mid K$ endlich und einfach
$\implies M \mid K$ endlich und einfach

(b) Dies gilt auch für transzendente einfache Erweiterungen. $K \subseteq M \subseteq L = K(X) \implies M = K(f)$ für ein $f \in K(X)$. (↗ Satz von Lüroth)

Theorem 9.4 (Satz vom primitiven Element, Abel)

Sei $L = K(\alpha_1, \dots, \alpha_r)$ eine endliche Erweiterung von K. Ist höchstens eines der α_i inseparabel über K, so ist die $L \mid K$ einfach.

Beweis. Es genügt, den Fall $r = 2$ zu betrachten (Satz 7.6). Sei also $L = K(\alpha, \beta)$ und β sei separabel über K. Seien

$$\alpha = \alpha_1, \dots, \alpha_n, \ \beta = \beta_1, \dots, \beta_l$$

die zu α bzw. β K-Konjugierten. Da $|K| = \infty$ existiert ein $c \in K$ mit

$$c \neq \frac{\alpha_i - \alpha}{\beta - \beta_j}, \quad i = 1, \dots, n, \; j = 2, \dots, l$$

Sei $\gamma := \alpha + c\beta$ und $f = \mathrm{MinPol}(\alpha \mid K)$ sowie $g := \mathrm{MinPol}(\beta \mid K)$.
Behauptung: $g(X)$ und $f(\gamma - cX)$ haben genau eine gemeinsame Nullstelle β.

Beweis.

- $g(\beta) = 0$, $f(\gamma - c\beta) = f(\alpha) = 0$)
- $f(\gamma - c\beta_j) = 0$
  $\Rightarrow \exists i\colon\; \alpha + c(\beta - \beta_j) = \alpha_i$
  $\Rightarrow c = \dfrac{\alpha_i - \alpha}{\beta - \beta_j}$
  $\Rightarrow$ Entweder ein Widerspruch oder $j = 1$ □

Sei $h := \mathrm{MinPol}(\beta \mid K(\gamma))$. Dann gilt $h \mid g$, $h \mid f(\gamma - cX)$

$\overset{\text{Beh.}}{\Longrightarrow}$ h hat nur eine Nullstelle in $\bar{K}$

$\overset{\beta\text{ sep.}}{\Longrightarrow}$ g separabel

$\Rightarrow \deg(h) = 1$

$\Rightarrow \beta \in K(\gamma) \Rightarrow \alpha \in K(\gamma)$

$\Rightarrow L = K(\alpha, \beta) = K(\gamma)$ □

Folgerung 9.5
Jede endliche separable Erweiterung von K ist einfach und besitzt nur endliche viele Zwischenkörper. Dies gilt insbesondere für jede endliche Erweiterung in Charakteristik 0.

Beweis. Folgt aus Satz 9.2, Theorem 9.4 und Satz 6.15. □

■ **Beispiel 9.6**
$\mathbb{Q}(\sqrt{2}, \sqrt{3}) \mid \mathbb{Q}$ besitzt ein primitives Element, z.B. $\sqrt{2} + \sqrt{3}$ (↗ Übung 21). Tatsächlich ist $\mathbb{Q}(\sqrt{2}, \sqrt{3}) = \mathbb{Q}(\sqrt{2} + c\sqrt{3})$ für jedes $c \in \mathbb{Q}^\times$.

K-Konjugierte zu $\sqrt{2}$: $\pm\sqrt{2}$
$\sqrt{3}$: $\pm\sqrt{3}$

Folglich ist

$$\left\{ \frac{\alpha_i - \alpha}{\beta - \beta_j} \;\middle|\; i = 1, 2, \; j = 2 \right\} = \left\{ 0, \frac{-2\sqrt{3}}{2\sqrt{3}} \right\}$$

die Menge der nicht-zugelassenen Proportionalitätsfaktoren und $\alpha + c\beta$ ist primitives Element für alle $c \in \mathbb{Q} \setminus \{0, -\sqrt{2}/\sqrt{3}\} = \mathbb{Q}^\times$

■ **Beispiel 9.7**
Sei $L = \mathbb{F}_p(t, s) = \mathrm{Quot}(\mathbb{F}_p[t, s])$, $K = L^p$. Dann ist $[L : K] = p^2$ (↗ P41) aber $L \mid K$ ist nicht einfach und besitzt unendliche viele Zwischenkörper. (Nach Satz 9.2) (↗ Übung)

▶ **Bemerkung 9.8**
Das Theorem 9.4 gilt auch für K endlich, siehe II.3.

Kapitel II

Galoistheorie

1. Normale Körpererweiterungen

Sei K Körper, $\bar{K}$ ein fixierter algebraischer Abschluss von K und L ein Zwischenkörper $K \subseteq L \subseteq \bar{K}$.

Definition 1.1
$L \mid K$ ist Normal $:\Leftrightarrow$ Ist $\alpha \in L$ und $\beta \in \bar{K}$ K-konjugiert, so ist $\beta \in L$.

Satz 1.2
Ist $L \mid K$ endlich, so sind äquivalent

(a) $L \mid K$ ist normal

(b) Jedes irreduzible $f \in K[X]$, das eine Nullstelle in L hat, zerfällt über L in Linearfaktoren

(c) L ist der Zerfällungskörper von $f \in K[X]$

(d) Für jedes $\sigma \in \mathrm{Aut}(\bar{K} \mid K)$ ist $\sigma(L) = L$

(e) Jedes $\sigma \in \mathrm{Aut}(\bar{K} \mid K)$ ist $\sigma(L) \subseteq L$

Beweis.

(1) $\Rightarrow$ (2) klar nach Folgerung I.4.14

(2) $\Rightarrow$ (3) Sei $L = K(\alpha_1, \dots, \alpha_n)$. Mit

$$f = \prod_{i=1}^{n} \mathrm{MinPol}(\alpha_i \mid K)$$

ist L der Zerfällungskörper von f.

(3) $\Rightarrow$ (4) Ist f der Zerfällungskörper von

$$f = |_{i=1}^{n}(X - X_i),$$

und $\sigma \in \mathrm{Aut}(\bar{K} \mid K)$, so permutiert σ die Nullstellen $\{\alpha_1, \dots, \alpha_n\}$ von f, folglich

$$\sigma(L) = \sigma\big(K(\alpha_1, \dots, \alpha_n)\big) = K\big(\sigma(\alpha_1), \dots, \sigma(\alpha_n)\big) = K(\alpha_1, \dots, \alpha_n) = L.$$

(4) $\Rightarrow$ (5) trivial

(5) $\Rightarrow$ (1) trivial □

■ **Beispiel 1.3**

a) $K \mid K$ ist normal

b) $\bar{K} \mid K$ ist normal

c) $\bar{K}_S \mid K$ ist normal (Folgerung I.7.7)

d) $[L : K] = 2 \Rightarrow L \mid K$ ist normal

(deg$(f) = 2$, f hat Nullstelle $\Rightarrow f$ zerfällt in Linearfaktoren)

e) $L = \mathbb{Q}(\sqrt[3]{2})$, $[L : \mathbb{Q}] = 3$ $L \mid Q$ ist nicht normal, die zu $\sqrt[3]{2}$ $\mathbb{Q}$-konjugierte Elemente $\zeta_3 \sqrt[3]{2}$ und $\zeta_3^2 \sqrt[3]{2}$ liegen nicht in L (Beispiel I.3.11 (b))

f) $Sei \alpha = \sqrt[4]{2} \in \mathbb{R}_{\geq 0}$ und $f = \mathrm{MinPol}(\alpha \mid \mathbb{Q}) = X^4 - 2$. Dann sind die $\mathbb{Q}$-konjugierten $\pm\sqrt[4]{2}$ und $i\sqrt[4]{2}$. Da $i\sqrt[4]{2} \notin \mathbb{R}$ ist $\mathbb{Q}(\alpha) \mid \mathbb{Q}$ nicht normal und

$$\underbrace{\mathbb{Q}(\sqrt[4]{2}) \underset{\text{normal}}{\overset{2}{\text{———}}} \mathbb{Q}(\sqrt{2}) \underset{\text{normal}}{\overset{2}{\text{———}}} \mathbb{Q}}_{\text{nicht normal}},$$

also ist Normalität nicht transitiv.

Folgerung 1.4
Sei $L \mid K$ endlich und seien $K \subseteq L_1,\ L_2 \subseteq L$ Zwischenkörper. Dann

(a) Sind $L_1 \mid K$ und $L_2 \mid K$ normal, so auch $L_1 \cap L_2 \mid K$ und $L_1 L_2 \mid K$

(b) Ist $L \mid K$ normal, so auch $L \mid L_1$

Beweis.
a) • $L1 \cap L_2$: klar aus Definition
  • $L_1 L_2$: Sei $\sigma \in \mathrm{Aut}(\bar{K} \mid K) \Rightarrow \sigma(L_1 L_2) = \sigma(L_1)\sigma(L_2) = L_1 L_2$

b) klar, da $\mathrm{Aut}(\bar{L}_1 \mid L_1) \subseteq \mathrm{Aut}(\bar{K} \mid K)$ □

Satz 1.5
Sei $L \mid K$ endlich. Es ist

$$\#\,\mathrm{Aut}(L \mid K) \leq [L : K]_S$$

mit Gleichheit, wenn die Erweiterung normal ist.

Beweis. Es ist

$$\mathrm{Aut}(L \mid K) = \mathrm{Hom}_K(L, L) = \left\{\sigma \in \mathrm{Hom}_K(L, \bar{K}) \;\middle|\; \sigma(L) \subseteq L\right\} \subseteq \mathrm{Hom}_K(L, \bar{K}),$$

sodass $\#\,\mathrm{Aut}(L \mid K) \leq \#\,\mathrm{Hom}_K(L, \bar{K}) = [L : K]_S$.

Es gilt: $\mathrm{Aut}(L \mid K) = \mathrm{Hom}_K(L \mid \bar{K})$

$$\begin{aligned}
&\Leftrightarrow \forall \sigma \in \mathrm{Hom}_K(L \mid \bar{K})\colon \sigma(L) \subseteq L \\
&\overset{\text{I.4.11}}{\Longleftrightarrow} \forall \sigma \in \mathrm{Aut}(\bar{K} \mid K)\colon \sigma(L) \subseteq L \\
&\overset{1.2}{\Leftrightarrow} L \mid K \text{ normal.}
\end{aligned}$$

□

▶ Bemerkung 1.6

Es ist also

$$\mathrm{Aut}(L \mid K) \overset{1}{\leq} [L : K]_S \overset{2}{\leq} [L : K],$$

wobei gilt:

1 ist Gleichheit $:\overset{1.5}{\Longleftrightarrow} L \mid K$ normal

2 ist Gleichheit $:\overset{\text{I.7.6}}{\Longleftrightarrow} L \mid K$ separabel

Definition 1.7

$L \mid K$ ist galoissch (oder Galoiserweiterung) $\Leftrightarrow L \mid K$ ist normal und separabel

Satz 1.8

Ist $L \mid K$ endlich, so sind äquivalent

(1) $L \mid K$ ist galoissch

(2) Jedes $\alpha \in L$ hat $\deg(\alpha \mid L)$ viele K-konjugierte in L

(3) L ist Zerfällungskörper eines irreduziblen, separablen Polynoms $f \in K[X]$

(4) L ist Zerfällungskörper eines separablen Polynoms $f \in K[X]$

(5) $\#\,\mathrm{Aut}(L \mid K) = [L : K]$

Beweis.

(1) $\Leftrightarrow$ (5) Bemerkung 1.6

(1) $\Leftrightarrow$ (2) $L \mid K$ separabel $\Leftrightarrow$ jdes $\alpha \in L$ hat $\deg(\alpha \mid K)$ viele K-konjugierte in $\bar{K}$.
$L \mid K$ normal $\Leftrightarrow$ alle K-konjugierte von $\alpha \in L$ liegen in L.

(1) $\Rightarrow$ (3) $L \mid K$ separabel $\overset{\text{I.9.4}}{\Longrightarrow} L = K(\alpha)$ einfach.
$L \mid K$ normal $\Rightarrow L$ ist Zerfällungskörper von $\mathrm{MinPol}(\alpha \mid K)$

(3) $\Rightarrow$ (4) trivial

(4) $\Rightarrow$ (1) Satz 1.2 und Satz I.7.6 □

Folgerung 1.9

Sei $L \mid K$ endlich und seien $K \subseteq L_1, L_2 \subseteq L$ Zwischenkörper.

(a) Sind $L_1 \mid K$ und $L_2 \mid K$ galoissch, so auch $L_1 \cap L_2 \mid K$ und $L_1L_2 \mid K$

(b) Ist $L \mid K$ galoissch, so auch $L \mid L_1$

Beweis. Folgerung 1.4, Folgerung I.7.8 und Folgerung I.7.9. □

Definition 1.10

Ist $L \mid K$ galoissch, so heißt

$$\mathrm{Aut}(L \mid K) = \mathrm{Gal}(L \mid K)$$

die Galoisgruppe von $L \mid K$.

▶ Bemerkung 1.11
Ist $L \mid K$ endlich und galoissch, so gilt nach Satz 1.8

$$\#\operatorname{Gal}(L \mid K) = [L : K].$$

Definition 1.12
Sei $G \leq \operatorname{Aut}(L \mid K)$ Untergruppe. Dann ist

$$L^{\mathrm{G}} := \left\{\alpha \in L \;\middle|\; \forall \sigma \in G\colon\; \alpha^\sigma = \alpha\right\}$$

der Fixkörper von G.

▶ Bemerkung 1.13
L^{G} ist ein Teilkörper von L.

Satz 1.14 (Artin)
Sei $G \leq \operatorname{Aut}(L)$ endlich, so ist $L \mid L^{\mathrm{G}}$ galoissch und $\operatorname{Gal}(L \mid L^{\mathrm{G}}) = G$.

Beweis. Sei $\alpha \in K = L^{\mathrm{G}}$. Dann ist

$$G_\alpha = \left\{\sigma \in G \;\middle|\; \alpha^\sigma = \alpha\right\} \leq G$$

und die G_α partitionieren G:

$$G = \bigcup_{i=1}^{m} G_\alpha \sigma_i,$$

wobei $m = [G : G_\alpha]$ und σ_i ein Repräsentantensystem ist.

Betrachte

$$f(X) = \prod_{i=1}^{m} (X - \alpha^{\sigma_i}) \in L[X].$$

Dannn gilt

- f ist unabhängig von der Wahl der σ_i,
- $f(\alpha) = 0$,
- f ist separabel, da $\alpha^{\sigma_i} = \alpha^{\sigma_j} \Rightarrow G_\alpha\sigma_i = G_\alpha\sigma_j \Rightarrow i = j$,
- $f \in K[X]$, da

$$\forall \tau \in G\colon\; G = G_\tau = \bigcup_{i=1}^{m} G_\alpha \sigma_i^\tau$$

und

$$f^\tau(X) = \prod_{i=1}^{m} (X - \alpha^{\sigma_i \tau}) = f(X).$$

$L \mid L^{\mathrm{G}}$ ist also nach Definition I.7.2 separabel.

Für jedes $\alpha \in L$ gilt, dass $\deg(\alpha \mid K) \leq \#G$ und

$$[L : K] \overset{\text{I.9.4}}{\leq} \#G \leq \#\operatorname{Aut}(L \mid K) \overset{1.6}{\leq} [L : K].$$

Daher: $G = \operatorname{Aut}(L \mid K)$ und aus

$$\#\operatorname{Aut}(L \mid K) = [L : K]$$

folgt, dass die Erweiterung $L \mid K$ galoissch ist. □

Folgerung 1.15
Sei $L \mid K$ endlich. Es gilt

$$L \mid K \text{ galoisch} \quad \Leftrightarrow \quad L^{\operatorname{Aut}(L|K)} = K$$

Beweis.
($\Rightarrow$) $L \mid K$ galoissch
$\overset{1.8}{\Longrightarrow}$ $\operatorname{Aut}(L \mid K) = [L : K]$
$K \subset L^{\operatorname{Aut}(L|K)} \subset L$
$\Rightarrow$ $[L : L^{\operatorname{Aut}(L|K)}] \overset{1.14}{=} \#\operatorname{Aut}(L \mid K)$
$\Rightarrow$ $K = L^{\operatorname{Aut}(L|K)}$

($\Leftarrow$) $L \mid K$ endlich
$\overset{1.5}{\Longrightarrow}$ $\operatorname{Aut}(L \mid K)$ endlich
$\overset{1.14}{\Longrightarrow}$ $L \mid L^{\operatorname{Aut}(L|K)} = K$ ist galoissch □

Lemma 1.16
Sind $K \subset L \subset M \subset \bar{K}$ Körper mit $L \mid K$ und $M \mid K$ normal, dann ist

$$\operatorname{res}_{M|L} : \begin{cases} \operatorname{Aut}(M \mid K) \to \operatorname{Aut}(L \mid K) \\ \quad \sigma \quad \mapsto \quad \sigma|_L \end{cases}$$

ein Epimorphismus.

Beweis. Nach Satz I.4.11 sind $\operatorname{res}_{\bar{K}|M}$ und $\operatorname{res}_{\bar{K}|L}$ surjektiv. Dann

- $\sigma|_L \in \operatorname{Aut}(L \mid K)$: Schreibe $\sigma = \operatorname{res}_{\bar{K}|M}(\tilde{\sigma})$. Es gilt wegen Satz 1.2 (d): $\sigma(L) = \tilde{\sigma}(L) = L$.
- $\operatorname{res}_{M|L}$ ist Homomorphismus: klar
- $\operatorname{res}_{M|L}$ ist surjektiv: $\operatorname{res}_{\bar{K}|L} = \operatorname{res}_{M|L} \circ \operatorname{res}_{\bar{K}|M}$. Als zweiter Teil einer surjektiven Verkettung ist dieser selbst surjektiv. □

2. Der Hauptsatz der Galoistheorie

$L \mid K$ ist endliche Galoiserweiterung mit $G = \mathrm{Gal}(L \mid K)$.

Definition 2.1
Es sind

- $\mathrm{Zwk}(L \mid K) = \{F \mid K \subset F \subset L,\ F\,\text{Zwischenkörper}\}$ die Menge der Zwischenkörper und
- $\mathrm{Ugr}(G) = \{H \mid H \leq G\}$ die Menge der Untergruppen.

Theorem 2.2 (Galoiskorrespondenz)
Es sind

$$\begin{cases} \mathrm{Zwk}(L \mid K) \to & \mathrm{Ugr}(G) \\ \quad F & \mapsto F^\circ := \mathrm{Gal}(L \mid F) \end{cases} \qquad \begin{cases} \mathrm{Ugr}(G) \to \mathrm{Zwk}(L \mid K) \\ \quad H \quad \mapsto \ H^\circ := L^H \end{cases}$$

zueinander inverse Bijektionen. Weiterhin gilt für F, F_1, $F_2 \in \mathrm{Zwk}(L \mid K)$ mit $H = F^\circ$, $H_1 = F_1^\circ$ und $H_2 = F_2^\circ$

i) die Bijketion ist antiton

$$F_1 \subset F_2 \quad \Leftrightarrow \quad H_1 \supset H_2$$

ii) die Bijektion ist indextreu, d.h.

$$[F_2 : F_1] = (H_1 : H_2), \quad \text{wenn } F_1 \subset F_2$$

iii) die Bijektion vertauscht Erzeugnis und Durchschnitt

$$(F_1 \cap F_2)^\circ = \langle H_1, H_2 \rangle \quad \text{und} \quad (F_1 F_2)^\circ = H_1 \cap H_2$$

iv) die Bijektion ist mit Konjugation verträglich: $\forall \sigma \in G$

$$(F^\sigma)^\circ = (F^\circ)^\sigma$$

v) die Bijektion erhält Normalität:

$$F \mid K \text{ normal} \quad \Leftrightarrow \quad H \trianglelefteq G$$

In disem Fall gilt:

$$\mathrm{Gal}(F \mid K) \cong G/H = \mathrm{Gal}(L \mid K)/\,\mathrm{Gal}(L \mid F)$$

Beweis.

- $F \in \mathrm{Zwk}(L \mid K) \overset{1.9}{\Longrightarrow} F$ galoissch $\overset{1.15}{\Longrightarrow} (F^\circ)^\circ = L^{F^\circ} = F$

- $H \in \mathrm{Ugr}(G) \overset{1.14}{\Longrightarrow} L \mid H^\circ$ galoissch mit $(H^\circ)^\circ = \mathrm{Gal}(L \mid H^\circ) = H$

i) $(\Leftarrow)$ klar, da $F_1 = H_1^\circ$, $F_2 = H_2^\circ$
   $(\Rightarrow)$ klarer

ii) $L \mid F_i$ ist galoissch, daher folgt aus Bemerkung 1.11 $[L : F_i] = \#H_i$ für $i = 1{,}2$ und

$$[F_2 : F_1] = \frac{[L : F_1]}{[L : F_2]} = \frac{\#H_1}{\#H_2} = (H_1 : H_2)$$

iii)
- $F_1 \cap F_2 \subset F_1F_2 \Rightarrow (F_1 \cap F_2)^\circ \overset{\text{i)}}{\supset} \langle H_1, H_2\rangle$,
  $H_1,\, H_2 \subset \langle H_1, H_2\rangle \Rightarrow F_1 \cap F_2 \supset (\langle H_1, H_2\rangle)^\circ \Rightarrow (F_1 \cap F_2)^\circ \subset \big((\langle H_1, H_2\rangle)^\circ\big)^\circ = \langle H_1, H_2\rangle$
- $F_1,\, F_2 \subset F_1F_2 \Rightarrow H_1 \cap H_2 \supset (F_1F_2)^\circ$
  $H_1 \cap H_2 \subset H_1,\, H_2 \Rightarrow (H_1 \cap H_2)^\circ \supset F_1F_2 \Rightarrow (F_1F_2)^\circ \supset \big((H_1 \cap H_2)^\circ\big)^\circ = H_1 \cap H_2$

iv) $(F^\sigma)^\circ = \{\tau \in G \mid \tau|_{F^\sigma} = \mathrm{id}\} = \{\tau \in G \mid \tau(x) = x\ \forall x \in F^\sigma\} = \{\tau \in G \mid \tau(x^\sigma) = x^\sigma\ \forall x \in F\} = \{\tau \in G \mid \tau^{\sigma^{-1}} \in F^\circ\} = (F^\circ)^\sigma$

v) $F \mid K$ normal
$\overset{1.2}{\Longleftrightarrow} F^\sigma = F\ \forall \sigma \in \mathrm{Aut}(\bar{K} \mid K)$
$\overset{1.16}{\Longleftrightarrow} F^\sigma = F\ \forall \sigma \in G$
$\overset{\text{iv)}}{\Longleftrightarrow} H^\sigma = H\ \forall \sigma \in G$
$\Leftrightarrow H \trianglelefteq G$

Sei $F \mid K$ normal. Nach Lemma 1.16 gilt

$$\mathrm{res}\colon \begin{cases} \mathrm{Gal}(L \mid K) \to \mathrm{Gal}(F \mid K) \\ \qquad \sigma \quad \mapsto \quad \sigma|_F \end{cases}$$

ist ein Epimorphismus.

$\Rightarrow\ \mathrm{Gal}(F \mid K) \cong \mathfrak{Im}(\mathrm{res}) \cong \mathrm{Gal}(L \mid K)/\ker(\mathrm{res}) \cong \mathrm{Gal}(L \mid K)/\,\mathrm{Gal}(L \mid F) = G/H$ □

■ **Beispiel 2.3**
Betrachte $\mathbb{Q}(\sqrt{2}, \sqrt{3}) \mid \mathbb{Q}$:

$$\begin{tikzcd}[column sep=small]
 & \mathbb{Q}(\sqrt{2},\sqrt{3}) \arrow[dl, dash] \arrow[d, dash] \arrow[dr, dash] & \\
\mathbb{Q}(\sqrt{2}) \arrow[dr, dash] & \mathbb{Q}(\sqrt{3}) \arrow[d, dash] & \mathbb{Q}(\sqrt{6}) \arrow[dl, dash] \\
 & \mathbb{Q} &
\end{tikzcd}
\qquad
\begin{tikzcd}[column sep=small]
 & \{\mathrm{id}\} \arrow[dl] \arrow[d] \arrow[dr] & \\
\{\mathrm{id}, \sigma_1\} \arrow[dr] & \{\mathrm{id}, \sigma_3\} \arrow[d] & \{\sigma_4, \mathrm{id}\} \arrow[dl] \\
 & \{\sigma_1, \sigma_2, \sigma_3, \sigma_4\} &
\end{tikzcd}$$

mit den Automorphismen

$$\sigma_1\colon \begin{array}{ccc} \sqrt{2} & \to & \sqrt{2} \\ \sqrt{3} & \to & \sqrt{3} \end{array},\quad \sigma_2\colon \begin{array}{ccc} \sqrt{2} & \to & \sqrt{2} \\ \sqrt{3} & \to & -\sqrt{3} \end{array},\quad \sigma_3\colon \begin{array}{ccc} \sqrt{2} & \to & -\sqrt{2} \\ \sqrt{3} & \to & \sqrt{3} \end{array},\quad \sigma_4\colon \begin{array}{ccc} \sqrt{2} & \to & -\sqrt{2} \\ \sqrt{3} & \to & -\sqrt{3} \end{array}.$$

▶ **Bemerkung 2.4**

(a) Die Bijektivität in Theorem 2.2 lässt sich mit i) und iii) auch so ausdrücken: Das Bilden von Fixkörpern ist ein Verbandisomorphismus zwischen $\mathrm{Ugr}(G)$ und $\mathrm{Zwk}(L \mid K)$.

(b) Die Bijektivität gilt nicht für unendliche Galoiserweiterungen (siehe Übung)

(c) Mit Theorem 2.2 erhalten wir einen neuen Beweis der Aussage

$$L \mid K \text{ endlich galoissch} \quad \Leftrightarrow \quad \mathrm{Zwk}(L \mid K) \text{ endlich},$$

was schon aus Satz I.9.2 folgt.

Satz 2.5
Sei $f \in K[X]$ separabel mit Nullstellen $\alpha_1, \ldots, \alpha_n \in \bar{K}$ und sei $L = K(\alpha_1, \ldots, \alpha_n)$ der Zerfällungskörper von f. Dann wirkt $G = \mathrm{Gal}(L \mid K)$ treu auf $X := \{\alpha_1, \ldots, \alpha_n\}$; der Homomorphismus

$$G \to \mathrm{Sym}(X) \cong S_n$$

ist also eine Einbettung. Die Wirkung von G auf X ist genau dann transitiv, wenn f irreduzibel ist.

Beweis. Sei $\sigma \in G$.

- treu: $\alpha_i^\sigma = \alpha_i \ \forall i \Rightarrow \sigma = \mathrm{id}$, denn $L = K(\alpha_1, \ldots, \alpha_n)$ und $\sigma|_K = \mathrm{id}_K$.
- Einbettung: GEO I.6.8
- transitiv $\Leftrightarrow$ $\forall i, j$: $\exists \sigma \in G$: $\sigma(\alpha_i) = \alpha_j$ □

$$\Leftrightarrow \forall i, j\colon \exists \sigma \in \mathrm{Aut}(\bar{K} \mid K)\colon \sigma(\alpha_i) = \alpha_j$$

$$\Leftrightarrow \alpha_1, \ldots, \alpha_n \text{ sind paarweise } k\text{-konjugiert}$$

$$\Leftrightarrow f = c \cdot \mathrm{MinPol}(\alpha_1 \mid K),\ c \in K^\times$$

$$\Leftrightarrow f \text{ irreduzibel}$$

Definition 2.6
In der Situation von Satz 2.5 heißt

$$\mathrm{Gal}(f \mid K) := \mathrm{Im}(G \to \mathrm{Sym}(\alpha_1, \ldots, \alpha_n))$$

die Galoisgruppe von f. Man nennt f galoissch, wenn f irreduzibel ist und ein Wurzelkörper von f schon ein Zerfällungskörper von f ist.

▶ **Bemerkung 2.7**

(a) Ist L ein Zerfällungskörper von $f = \prod_{i=1}^n (X - \alpha_i) \in K[X]$, so gilt also

$$\mathrm{Gal}(L \mid K) \cong \mathrm{Gal}(f \mid K) \leq \mathrm{Sym}(\{\alpha_1, \ldots, \alpha_n\}) \cong S_n.$$

(b) Genau dann ist f galoissch, wenn $G := \mathrm{Gal}(f \mid K) \leq S_n$ transitiv und $\#G = n$.

■ **Beispiel 2.8**

Sei $f = X^3 - 2 \in \mathbb{Q}[X]$. Die Nullstellen von f sind

$$
\begin{aligned}
\alpha_1 &= \sqrt[3]{2},\\
\alpha_2 &= \sqrt[3]{2}\zeta_3,\\
\alpha_3 &= \sqrt[3]{2}\zeta_3^2.
\end{aligned}
$$

Der Zerfällungskörper ist $L := \mathbb{Q}(\alpha_1, \alpha_2, \alpha_3) = \mathbb{Q}(\alpha_1, \alpha_2) = \mathbb{Q}(\sqrt[3]{2}, \zeta_3)$. Weiterhin ist

$$
G = \mathrm{Gal}(f \mid \mathbb{Q}) \leq S_3; \quad \#G = [L : K] = 6 \quad \Rightarrow \quad \mathrm{Gal}(L \mid K) \cong \mathrm{Gal}(f \mid K) = S_3 = \langle (1\,2\,3), (2\,3) \rangle
$$

Sei $\sigma \in G \leftrightsquigarrow (1\,2\,3)$, also $(\sqrt[3]{2})^\sigma = \zeta_3 \sqrt[3]{2}$, $(\zeta_3 \sqrt[3]{2})^\sigma = \zeta_3^2 \sqrt[3]{2}$, $(\zeta_3^2 \sqrt[3]{2})^\sigma = \sqrt[3]{2}$, $\zeta_3^\sigma = (\frac{\alpha_2}{\alpha_1})^\sigma = \zeta_3$.

$G \ni \tau \leftrightsquigarrow (2\,3)$, also $(\sqrt[3]{2})^\tau = \sqrt[3]{2}$, $(\zeta_3 \sqrt[3]{2})^\tau = \zeta_3^2 \sqrt[3]{2}$, $(\zeta_3^2 \sqrt[3]{2})^\tau = \zeta_3 \sqrt[3]{2}$, $\zeta_3^\tau = (\frac{\alpha_2}{\alpha_1})^\tau = \zeta_3^2 = \zeta_3^{-1} = \bar{\zeta}_3$.

$$
\begin{tikzcd}
& S_3 \arrow[dl, "3"'] \arrow[d, "3"] \arrow[dr, "3"] \arrow[drr, "2"] & & \\
\langle (1,2) \rangle \arrow[dr, "2"'] & \langle (2,3) \rangle \arrow[d, "2"] & \langle (1,3) \rangle \arrow[dl, "2"] & A_4 \arrow[dll, "3"] \\
& 1 & &
\end{tikzcd}
\qquad
\begin{tikzcd}
& G \arrow[dl, "3"'] \arrow[d, "3"] \arrow[dr, "3"] \arrow[drr, "2"] & & \\
\langle \tau\sigma^2 \rangle \arrow[dr, "2"'] & \langle \tau \rangle \arrow[d, "2"] & \langle \tau\sigma \rangle \arrow[dl, "2"] & \langle \sigma \rangle \arrow[dll, "3"] \\
& \{\mathrm{id}\} & &
\end{tikzcd}
$$

$$
\begin{tikzcd}
{} \arrow[d, "\text{Theorem 2.2, i), ii), iv)}"] \\ {}
\end{tikzcd}
$$

$$
\begin{tikzcd}
& L \arrow[dl, "2"'] \arrow[d, "2"] \arrow[dr, "2"] \arrow[drr, "3"] & & \\
\left(L^{\langle \tau \rangle}\right)^{\langle \sigma^2 \rangle} \arrow[dr, "3"'] & L^{\langle \tau \rangle} \arrow[d, "3"] & \left(L^{\langle \tau \rangle}\right)^{\langle \sigma \rangle} \arrow[dl, "3"] & L^{\langle \sigma \rangle} \arrow[dll, "2"] \\
& \mathbb{Q} & &
\end{tikzcd}
\qquad
\begin{tikzcd}
& \mathbb{Q}(\sqrt[3]{2}, \zeta_3) \arrow[dl, "2"'] \arrow[d, "2"] \arrow[dr, "2"] \arrow[drr, "3"] & & \\
\mathbb{Q}(\zeta_3^2 \sqrt[3]{2}) \arrow[dr, "3"'] & \mathbb{Q}(\sqrt[3]{2}) \arrow[d, "3"] & \mathbb{Q}(\zeta_3 \sqrt[3]{2}) \arrow[dl, "3"] & \mathbb{Q}(\zeta_3) \arrow[dll, "2"] \\
& \mathbb{Q} & &
\end{tikzcd}
$$

3. Endliche Körper

Sei K ein endlicher Körper mit $\mathrm{char}(K) = p$ und Primkörper $\mathbb{F}_p$.

▶ **Bemerkung 3.1**

$K \mid \mathbb{F}_p$ ist endlich, insbesondere algebraisch, also o.E. $K \subset \bar{\mathbb{F}_p}$.

Lemma 3.2

(a) $\#K = p^n$ für ein $n \in \mathbb{N}$.

(b) K ist vollkommen.

(c) $K^\times \cong C_{p^n-1}$

(d) K ist Zerfällungskörper von $X^{p^n} - X = \prod_{\alpha \in K}(X_\alpha)$ über $\mathbb{F}_p$.

Beweis.

(1) $K \cong \mathbb{F}_p^{[K:\bar{\mathbb{F}_p}]}$ als $\mathbb{F}_p$-Vektorraum

(2) Beispiel I.6.16

(3) GEO I.4.13.

(4) $\alpha^{p^n-1} = 1 \ \forall \alpha \in K^\times$

$\Rightarrow$ jedes $\alpha \in K$ ist Nullstelle von $X(X^{p^n-1} - 1) = X^{p^n} - X$

$\Rightarrow$ $X^{p^n} - X = \prod_{\alpha \in K}(X - \alpha)$ zerfällt über K in Linearfaktoren. □

Satz 3.3

Zu jeder Primpotenz $q = p^n$ gibt es bis auf Isomorphie genau einen Körper mit $\#K = q$. Ein gegebener Körper E besitzt höchstens einen Teilkörper mit $\#K = q$.

Beweis.

- Eindeutigkeit: Lemma 3.2 (d) + Satz I.3.13 + Bemerkung I.3.14
- Existenz: $f = X^q - X \in \mathbb{F}_p[X]$
  - $f' = -1 \Rightarrow f$ separabel $\Rightarrow f$ hat genau q viele Nullstellen in $\bar{\mathbb{F}_p}$
  - Die Nullstellen von f bilden einen Körper: Für $\alpha \in \bar{\mathbb{F}_p}$ gilt:

$$f(\alpha) = 0 \quad \Leftrightarrow \quad \alpha^{p^n} = \alpha \quad \Leftrightarrow \quad \Phi_p^n(\alpha) = \alpha \quad \Leftrightarrow \quad \alpha \in \bar{\mathbb{F}_p}^{\langle \Phi_p^n \rangle}$$

□

Definition 3.4

Man bezeichnet den eindeutig bestimmten Körper $K \subseteq \bar{\mathbb{F}_p}$ mit $q = p^n$ Elementen mit $\mathbb{F}_q$.

Satz 3.5

Sei $L \mid \mathbb{F}_q$ endlich mit $[L : \mathbb{F}_q] = m$, $q = p^n$. Dann ist $L \mid \mathbb{F}_q$ einfach und galoissch mit

$$\mathrm{Gal}(L \mid \mathbb{F}_q) = \langle \Phi_p|_L{}^n \rangle \cong C_m$$

mit $\Phi_p \colon \bar{\mathbb{F}_p} \to \bar{\mathbb{F}_p}$, $x \mapsto x^p$.

Beweis.

- einfach: Lemma 3.2 (c)
- $\Phi_p|_L \in \mathrm{End}(L) = \mathrm{Aut}(L) = \mathrm{Aut}(L \mid \mathbb{F}_p) \Rightarrow \Phi_p|_L{}^n \in \mathrm{Aut}(L \mid \mathbb{F}_q)$
- $\Phi_p|_L{}^n \in \mathrm{Aut}(L \mid \mathbb{F}_q)$, $L^{\langle \Phi_p|_L{}^n \rangle} = \mathbb{F}_q$
  $\overset{1.14}{\Longrightarrow}$ $L \mid \mathbb{F}_q$ galoissch mit $\mathrm{Gal}(L \mid \mathbb{F}_q) = \mathrm{Gal}(L \mid L^{\langle \Phi_p|_L{}^n \rangle}) = \langle \Phi_p|_L{}^n \rangle$
  $\#\,\mathrm{Gal}(L \mid \mathbb{F}_q) = [L : \mathbb{F}_q] = m \Rightarrow \mathrm{Gal}(L \mid \mathbb{F}_q) \cong C_m$. □

Lemma 3.6
Für $\mathbb{F}_q \subseteq L_1, L_2 \subseteq \bar{\mathbb{F}}_p$ mit $m_i := [L_i : \mathbb{F}_q] < \infty$ gilt:

$$L_1 \subseteq L_2 \quad \Leftrightarrow \quad m_1 \mid m_2.$$

Beweis.

($\Rightarrow$) $m_2 = [L_2 : \mathbb{F}_q] = [L_2 : L_1][L_1 : \mathbb{F}_q] = [L_2 : L_1] \cdot m_1$

($\Leftarrow$) $\mathrm{Gal}(L_2 \mid \mathbb{F}_q) \overset{3.5}{\cong} C_{m_2}$.

$m_1 \mid m_2$
$\Rightarrow$ ex. $H \leq C_{m_2}$ mit $\#H = \frac{m_2}{m_1}$
$\Rightarrow$ $[L_2^H : \mathbb{F}_q] = (C_{m_2} : H) = m_1$
$\Rightarrow$ $\#L_2^H = q^{m_1} = \#L_1$
$\overset{3.3}{\Longrightarrow}$ $L_1 = L_2^H \subseteq L_2$. □

Satz 3.7
Zu jedem $m \in \mathbb{N}$ besitzt $\mathbb{F}_q$ genau eine Erweiterung $L \subseteq \bar{\mathbb{F}}_p$ vom Grad $[L : \mathbb{F}_q] = m$.

Beweis.

- Eindeutigkeit: $L = \mathbb{F}_{q^m}$ nach Satz 3.3
- Existenz: $\mathbb{F}_q \subseteq F_{q^m}$ nach Lemma 3.6 ($[\mathbb{F}_q : \mathbb{F}_p] = n \mid nm = [\mathbb{F}_{q^m} : \mathbb{F}_p]$) □

▶ **Bemerkung 3.8**
Wir sehen, dass $\bar{\mathbb{F}}_p = \cup_{n \in \mathbb{N}} \mathbb{F}_{p^n}$ eine unendliche algebraische Erweiterung von $\mathbb{F}_p$ ist, vgl. H88.

4. Fundamentalsatz der Algebra

▶ **Bemerkung 4.1**

Wir werden die folgende Eigenschaften der Körper $\mathbb{R}$ und $\mathbb{C}$ benutzen:

(a) $\mathbb{C} = \mathbb{R}(i)$ mit $i^2 = -1$,

(b) $a \in \mathbb{R}$, $a > 0 \Rightarrow \sqrt{a} \in \mathbb{R}$

(c) $f \in \mathbb{R}[X]$, $\deg(f)$ ungerade $\Rightarrow f$ hat Nullstelle in $\mathbb{R}$

Lemma 4.2

Sei $K \subseteq L \subseteq \bar{K}$ eine Erweiterung von K. Dann gibt es eine kleinste Erweiterung $K \subseteq \hat{L} \subseteq \bar{K}$ mit $\hat{L} \mid K$ normal.

Ist $L \mid K$ endlich, so ist auch $\hat{L} \mid K$ endlich.

Ist $L \mid K$ separabel, so auch $\hat{L} \mid K$.

Beweis. klar, da $\hat{L} = K\big(\cup_{\sigma \in \mathrm{Aut}(\bar{K}|K)} L^\sigma\big)$. Für $\tau \in \mathrm{Aut}(\bar{K}, K)$ ist dann $\hat{L}^\tau = K\big(\cup_\sigma L^{\sigma\tau}\big) = K\big(\cup_\sigma L^\sigma\big) = \hat{L}$.

- endlich: Ist $L = K(\alpha_1, \ldots, \alpha_n)$, so ist $\hat{L}$ der Zerfällungskörper von

$$f := \prod_{i=1}^{n} \mathrm{MinPol}(\alpha_i \mid K)$$

- separabel: $L \mid K$ separabel $\Rightarrow L^\sigma \mid K$ separabel $\overset{1.7.6}{\Longrightarrow} K\big(\cup_\sigma L^\sigma\big) \mid K$ separabel □

Definition 4.3

$\hat{L}$ ist die normale Hülle von $L \mid K$.

Theorem 4.4

$\mathbb{C} = \bar{\mathbb{C}}$.

Beweis. Unter Benutzung Bemerkungen 4.1 (a) bis 4.1 (c).

Beh. 1: Jedes $z = a + b\imath \in \mathbb{C}$ hat eine Quadratwurzel in $\mathbb{C}$ $(a, b \in \mathbb{R})$

Beweis. $z = a + b\imath = (x + y\imath)^2 = x^2 + y^2 + 2xy\imath$ $(x, y \in \mathbb{R})$

$\Rightarrow a = x^2 - y^2, b = 2xy$

$\Rightarrow a = x^2 - \left(\frac{b}{2x}\right)^2$

$\Rightarrow x^4 - ax^2 - \frac{1}{4}b^2 = 0$

$w^2 - aw - \frac{1}{4}b^2 = 0$ hat die Lösung

$$w = \frac{a \pm \sqrt{a^2 + b^2}}{2} \in \mathbb{R},$$

nach Bemerkung 4.1 (b).

Wähle $w > 0 \overset{4.1\ (b)}{\Longrightarrow}$ ex. $x \in \mathbb{R}$ mit $x^4 - ax^2 - \frac{1}{4}b^2 = 0$ □

Beh. 2: $\mathbb{C}$ hat keine Erweiterung vom Grad 2.

Beweis. $L = \mathbb{C}(\alpha)$, $[L : \mathbb{C}] = 2$

$\overset{\text{Ü20}}{\Longrightarrow}$ o.E. $\alpha^2 \in \mathbb{C}$

$\overset{\text{Beh. 1}}{\Longrightarrow}$ $\alpha \in \mathbb{C}$. □

Beh. 3: $\mathbb{R}$ hat keine Erweiterung ungeraden Grades.

Beweis. $[L \mid \mathbb{R}] = n$ ungerade

$\overset{\text{I.9.5}}{\Longrightarrow}$ $L = \mathbb{R}(\alpha)$ für ein α

$\Rightarrow$ $f := \mathrm{MinPol}(\alpha \mid \mathbb{R})$ hat Grad $\deg(f) = \deg(\alpha \mid \mathbb{R}) = [\mathbb{R}(\alpha) : \mathbb{R}] = n$ ungerade

$$\left.\begin{array}{l} f \text{ ist irreduzibel} \\ f \text{ hat Nullstelle in } \mathbb{R} \text{ nach Bemerkung 4.1 (c)} \end{array}\right\} \Rightarrow \deg(f) = 1 \Rightarrow L = \mathbb{R}$$ □

Beh. 4: $\mathbb{C}$ hat keine echten endlichen Erweiterungen.

Beweis. Sei $L \mid \mathbb{C}$ endlich. Sei M die normale Hülle $L \mid \mathbb{R}$, $G := \mathrm{Gal}(M \mid \mathbb{R})$, $H := \mathrm{Gal}(M \mid \mathbb{C})$, $S := \mathrm{Syl}_2(G)$, $K = M^S$

$\Rightarrow$ $[K : \mathbb{R}] = (G : S)$ ungerade

$\overset{\text{Beh. 3}}{\Longrightarrow}$ $K = \mathbb{R}$, $G = S$ ist 2-Gruppe.

Angenommen $\#G = 2^k$, $k \geq 2$

$\overset{\text{GEO I.7.9}}{\Longrightarrow}$ ex. $U \leq H$ mit $(H : U) = 2$

$\Rightarrow$ $[M^U : \underbrace{M^H}_{=\mathbb{C}}] = (H : U)$ ↯ zu Beh. 2

Somit ist $\#G = 2$, $\#H = 1$, $M = \mathbb{C} \Rightarrow L = \mathbb{C}$. □

Ein Körper ist genau dann abgeschlossen, wenn er keine echte algebraische Erweiterung besitzt. □

▶ Bemerkung 4.5

Körper, die eine Anordnung $<$ besitzen und Bemerkungen 4.1 (b) und 4.1 (c) erfüllen, nennt man reell abgeschlossen.

■ Beispiel 4.6

$\mathbb{R} \cap \bar{\mathbb{Q}}$ ist reell abgeschlossen.

Anhang

Index