Algebra und Zahlentheorie SS 2019

Dozent: Prof. Dr. Arno Fehm

26. April 2019

Inhaltsverzeichnis

Vorwort

Motivation und Einführung

Kapitel I

Körper

1. Körpererweiterungen

Sei 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 $p \in \{0, 2, 3, 5, 7, \ldots\}$ 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) $\operatorname{char}(K) = 0 \Leftrightarrow \mathbb{F} \cong \mathbb{Q}$

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

Beweis. "$\Leftarrow$": Beispiel 1.4
"$\Rightarrow$": $\operatorname{Im}(\mathbb{Z} \to K) \subseteq \mathbb{F}$ und $\operatorname{Im}(\mathbb{Z} \to K) \cong \mathbb{Z}/\operatorname{Ker}(\mathbb{Z} \to K)$

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

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

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. $\varphi : L_1 \to L_2$)

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

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

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

Definition 1.10 (Körpergrad)
$[L : K] := \dim_k(L) \in \mathbb{N} \cup \{\infty\}$, 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) $[K(x) : K] = \infty$ ($K(x) = \operatorname{Quot}(K[x])$) (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. Behauptung: Sei $x_1, \ldots, x_n \in L$ K-linear unabhängig und $y_1, \ldots, y_m \in M$ L-linear unabhängig
$\Rightarrow x_i y_j, i \in \{1, \ldots, n\}, j \in \{1, \ldots, m\}$ K-linear unabhängig.
Beweis: $\sum_{i,j} \lambda_{ij} x_i y_j = 0$ mit $\lambda_{ij} \in K$

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

- $[L : K] = \infty$ oder $[M : L] = \infty \Rightarrow [M : K] = \infty$
- $[L : K] = n, [M : L] = m < \infty$
  $(x_1, \dots, x_n)$ Basis des K-Vektorraum L und $(y_1, \dots, y_m)$ Basis des L-Vektorraums M
  $\Rightarrow \{x_i y_j : i = 1, \dots, n; j = 1, \dots, m\}$ K-linear unabhängig und
  $\sum_{i,j} K x_i y_j = \sum_j \left(\sum_i \lambda_{ij} x_i\right) y_j = M$, also ist
  $\{x_i y_j : i = 1, \dots, n; j = 1, \dots, m\}$ Basis von M □

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 $K(a_1, \dots, a_n) = \{\alpha\beta : \alpha, \beta \in K[a_1, \dots, a_n], \beta \neq 0\} \cong \mathrm{Quot}(K[a_1, \dots, a_n])$

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 $f = X - \alpha \in K$)

(b) $\sqrt{-1} \in \mathbb{Q}(\sqrt{-1})$ ist algebraisch über $\mathbb{Q}$ (denn $f(\sqrt{-1}) = 0$ für $f = X^2 + 1 \in \mathbb{Q}$)
$\sqrt{-1} \in \mathbb{C}$ 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 $1, \alpha, \alpha^2, \dots$ K-linear abhängig sind.

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

$$\sum_{i=0}^{\infty} \lambda_i \alpha^i :\Leftrightarrow f(\alpha) = 0 \text{ für } f = \sum_{i=0}^{\infty} \lambda_i X^i \in K$$ □

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 $\operatorname{Ker}(\varphi_\alpha) \neq (0)$. In diesem Fall ist $\operatorname{Ker}(\varphi_\alpha) = (f_\alpha)$ mit einem eindeutig bestimmten irreduziblen, normierten $f_\alpha \in K$.

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

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

(a) $\operatorname{MinPol}(\alpha \mid K) := f_\alpha$, 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
$\Rightarrow K[\alpha] \cong K$, $K(\alpha) \cong_K K(X)$, $[K(\alpha) : K] = \infty$.

(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
$1, \alpha, \dots, \alpha^{\deg(\alpha|K)-1}$ ist K-Basis von $K(\alpha)$.

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

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

- f irreduzibel $\Rightarrow (f) \neq (0)$ prim $\xRightarrow{\text{GEO II.4.7}}$ (f) ist maximal
  $\Rightarrow K[\alpha] \cong K/(f)$ ist Körper $\Rightarrow K[\alpha] = K(\alpha)$
- $1, \alpha, \dots, \alpha^{n-1}$ sind K-linear unabhängig:

$$\sum_{i=0}^{n-1} \lambda_i \alpha^i = 0 \Rightarrow \sum_{i=0}^{n-1} \lambda_i X^i \in (f) \quad \xRightarrow{\deg f = n} \quad \lambda_i = 0 \ \forall i$$

$1, \alpha, \dots, \alpha^{n-1}$ ist Erzeugendensystem: Für $g \in K$ ist

$$g = qf + r \text{ mit } q, r \in K \text{ und } \deg(r) < \deg(f) = n$$

und

$$g(\alpha) = q(\alpha) \underbrace{f(\alpha)}_{=0} + r(\alpha) = r(\alpha)$$

somit $K = \operatorname{Im}(\varphi_\alpha) = \{g(\alpha)\colon g \in K\} = \{r(\alpha)\colon r \in K, \deg(r) < n\} = \sum_{i=0}^{n-1} K \cdot \alpha^i$ □

■ **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 $\operatorname{MinPol}(\sqrt{p} : \mathbb{Q}) = X^2 - p$, $[\mathbb{Q}(\sqrt{p}) : \mathbb{Q}] = 2$.

(b) Sei $\zeta_p = e^{\frac{2\pi i}{p}} \in \mathbb{C}$ ($p \in \mathbb{N}$ prim). Da $\Phi_p = \frac{X^p - 1}{X - 1} = X^{p-1} + X^{p-2} + \dots + X + 1 \in \mathbb{Q}$ 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) $e \in \mathbb{R}$ ist transzendent über $\mathbb{Q}$ (Hermite 1873), $\pi \in \mathbb{R}$ ist transzendent über $\mathbb{Q}$ (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. $\alpha \in L$, $[L:K] = n \Rightarrow 1, \alpha, \dots, \alpha^n$ K-linear abhängig $\overset{2.4}{\Longrightarrow} \alpha$ 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 (auch wegen der aus der Irreduzibilität

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

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 $f = \mathrm{MinPol}(\alpha \mid L) = \sum_{i=0}^{n} a_i x^i$, $\quad L_0 := K(a_0, \dots, a_n)$
$\Rightarrow f \in L_0[x]$

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

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

$\Rightarrow \alpha$ algebraisch über K

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

Folgerung 2.15

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

Beweis.
- $\alpha, \beta \in \tilde{K}$:
  $\Rightarrow K(\alpha, \beta) \mid K$ 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)

$\tilde{K} = \{\alpha \in L \colon \alpha$ algebraisch über $K\}$ heißt der relative algebraische Abschluss von K in L.

Beispiel 2.17

$\tilde{\mathbb{Q}} = \{\alpha \in \mathbb{C} \colon \alpha$ algebraisch über $K\}$ 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 2.7b). Für $f \in K[X]$ beliebig, schreibe $f = f_1 \cdots f_r$ mit $f_i \in K[X]$ irreduzibel

$$f(\alpha) = 0 \Rightarrow \text{ OE } f_1(\alpha) = 0 \Rightarrow [L : K] = \deg(f_1) \leq \deg(f) = n \qquad \square$$

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
- $f(\alpha) = f(\pi(X)) \overset{(*)}{=} \pi(f(X)) = 0 \quad f(X) \in \mathrm{Ker}(\pi)$
  ($*$ gilt, da $f = \sum a_i x^i = \pi(f) = \sum \pi(a_i)\pi(x)^i = \sum a_i \pi(x)^i = f(\pi(x))$)
- $L = \pi(K[X]) = K[\pi(X)] = k[\alpha] \overset{\alpha \text{ alg.}}{=} K(\alpha)$ $\square$

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 $\varphi : L_1 \to L_2$ mit $\varphi(\alpha_1) = \alpha_2$.

Beweis.

- Existenz gibt Lemma 3.4
- Lemma 3.3 liefert Isomorphismus

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

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

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
  $\xRightarrow{\text{(IH)}}$ 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 $f = c \cdot \prod_{i=1}^{n}(x-\alpha_i)$ mit $c \in K^\times$.

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 vpn 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 $f \xRightarrow{3.3} [L_1 : K] \leq n$ 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)
  $\xRightarrow{\text{IH}} [L : L_1] \leq \deg(f_1)! = (n-1)!$
  $\Rightarrow [L : K] = [L : L_1][L_1 : K] = (n-1)!n = n!$ □

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: $\sqrt[2]{2} \in \mathbb{R}, \zeta_3 \sqrt[2]{2}, \zeta_3^2 \sqrt[2]{2}$

- $\mathbb{Q}(\sqrt[2]{2})$ 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

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

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 $f(\alpha)$ ein Wurzelkörper von f. Sei $\tilde{L} \mid \tilde{K}$ eine weitere Körpererweiterung und $\varphi \in \operatorname{Hom}(K, \tilde{K})$. Ist $\sigma \in \operatorname{Hom}(L, \tilde{L})$ 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 $\sigma(\alpha) = \beta$.

$$\begin{tikzcd} L \arrow[r, "\sigma"] & L' \\ K \arrow[u] \arrow[r, "\varphi"] & K' \arrow[u] \end{tikzcd}$$

Beweis (was für die Prüfung!).

- $f(\alpha) = 0 \Rightarrow 0 = \sigma(0) = \sigma(f(\alpha)) = \sigma\left(\sum_{i=0}^n a_i \alpha_i\right) = \sum_{i=0}^n \varphi(a_i) \sigma(\alpha)^i = f^\varphi(\sigma(\alpha))$
- Eindeutigkeit klar, da $L = K(\alpha)$
- Existenz: Betrachte

$$\eta : \begin{cases} K[X] & \to L \\ g & \mapsto g(\alpha) \end{cases} \qquad \psi : \begin{cases} K[X] & \to L' \\ g & \to g^\varphi(\beta) \end{cases} \qquad \to \text{ sind Homomorphismen nach univer. Eigenschaft}$$

(Bemerke: η surjektiv: $\eta_{|K} = \mathrm{id} \to K \in \operatorname{Im}(\eta)$ mit $\eta(x) = \alpha \to \alpha \in \operatorname{Im}(\eta)$)

$Ker(\eta) = (f)$ ist Isomorphismus und $\bar{\eta} : K[X]/(f) \xrightarrow{\cong} L$ und
$f \in \mathrm{Ker}(\psi) \Rightarrow \mathrm{Ker}(\psi) = (f)$ ist Homomorphismus $\bar{\psi} : K[X]/(f) \to L'$
$\sigma := \bar{\psi} \circ \bar{\eta}^{-1} : L \to L'$ ist eine Fortsetzung von ψ und

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

□

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

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

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

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

(IS) $n > 1$: 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

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

fort. Schreibe $f = (x - \alpha_1) \cdot f_1^\sigma$ mit $f_1 \in K_1[X]$
$\Rightarrow f^\varphi = (x - \underbrace{\sigma(\alpha_1)}_{\alpha_1'}) \cdot f_1^\sigma$ mit $f_1^\sigma \in K_1'[X]$. L ist Zerfällungskörper von f_1, L' ist Zerfällungskörper von f_1^σ
$\Rightarrow \sigma$ 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) (a) $\Rightarrow$ (b): Induktion nach $\deg(f)$ (siehe LAAG)

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

(c) (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 (algebraisch Abgeschlossen)
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 $f(\alpha) = 0$ und $f(\alpha) = 0 \Rightarrow \alpha$ algebraisch über $\tilde{K} \overset{2.15}{\Longrightarrow}$ $\alpha \in \tilde{K}$. □

Beispiel 4.5

(a) $\mathbb{C}$ ist algebraisch abgeschlossen (Fundamentalsatz der Algebra, ↗ 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 $\varphi \in \text{Hom}(K, E)$. Dann existiert eine Fortsetzung von φ auf L, d.h. ein $\sigma \in \text{Hom}(L, E)$ mit $\sigma_{|K} = \varphi$.

Beweis. Definiere Halbordnung.

$$\mathfrak{X} := \left\{(M,\sigma) : K \subseteq M \subseteq L \text{ Zwischenkörper}, \sigma \in \mathrm{Hom}(M,E), \sigma_{|K} = \varphi\right\}$$
$$(M,\sigma) \subseteq (M',\sigma') :\Leftrightarrow m \subset M' \text{ und } \sigma'_{|M} = \sigma$$

- $\mathfrak{X} \neq \varnothing$: $(K,\varphi) \in \mathfrak{X}$
- Ist $(M,\sigma)_{i\in I}$ eine Kette in $\mathfrak{X}$, so definieren wir $M := \bigcup_{i\in I} M_i$ und $\sigma : M \to E$ 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 $\alpha \in L, f = \mathrm{MinPol}(\alpha \mid M)$. $f \in E[X]$ hat Nullstelle $\beta \in E$, da E algebraisch abgeschlossen ist. $\overset{3.12}{\Longrightarrow}$ existiert Fortsetzung $\sigma' \in \mathrm{Hom}(M(\alpha),E)$ 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 $\sigma \in \mathrm{Hom}(L_1,L_2)$

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

  Somit ist $\sigma : L_1 \to L_2$ ein K-Isomorphismus.
- Existenz: Seien
  (a) $\mathscr{F} = \{f \in K[X] \colon \deg(f) > 0\}$
  (b) $\mathfrak{X} = (X_f)_{f\in\mathscr{F}}$ Familie von Variablen
  (c) $R := K[\mathfrak{X}]$ Polynomring in den Variablen X_f $(f \in mathscrF)$
  (d) $I := (f(X_f) \colon f \in \mathscr{F}) \trianglelefteq R$
  (a) Behauptung 1: Es gilt $I \ntrianglelefteq R$.

  Beweis (Behauptung 1). Angenommen $I = R$. Dann existieren $f_1, \dots, f_n \in \mathscr{F}$ und $g_1, \dots, g_n \in R$ mit $\sum_{i=1}^n g_i \cdot f_i(X_f f_i) = 1$. Sei L ein Zerfällungskörper von $f_1, \dots, f_n$. Dann existieren $\alpha_1, \dots, \alpha_n \in L$ mit $f_i(\alpha_i) = 0$ für alle i. Sei $\varphi : R \to L$ der Einsetzungshomomorphismus gegeben durch

$$\varphi_{|K} = \mathrm{id}_K \quad \varphi(X_{f_i}) = \alpha_i \quad \varphi(X_f) = 0 \text{ für } f \in \mathscr{F}/\{f_1,\dots,f_n\}$$
$$\Longrightarrow \ 1 = \varphi(1) = \sum_{i=1}^n \varphi(g_i) \cdot \varphi(f_i(X_f))$$
$$= \sum_{i=1}^n \varphi(g_i) \cdot f_i(\underbrace{\varphi(X_f)}_{=\alpha_i}) = \sum_{i=1}^n \varphi(g_i) \cdot \underbrace{f_i(\alpha_i)}_{=0} = 0$$ □

  Jedes echte Ideal ist in einem maximalen Ideal von R enthalten (GEO II 2.13) $\Longrightarrow$ 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 erhalte eine Kette von Körpern

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

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

(a) Behauptung 2: L ist algebraisch abgeschlossen.

Beweis (Behauptung 2). 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 $\tilde{K} = \{\alpha \in L \colon \alpha \text{ algebraisch über } K\}$ ein abgeschlossener 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)
$\mathrm{Aut}(L \mid K) := \{\sigma \in \mathrm{Hom}_K(L, L) \colon \sigma \text{ Isomorphismus}\}$, die Automorphismengruppe von $L \mid K$.

▶ Bemerkung 4.10
$\mathrm{Aut}(L \mid K)$ 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 $\varphi \in Hom_K(L, \bar{K})$ lässt sich zu einem $\sigma \in \mathrm{Aut}(\bar{K} \mid K)$ fortsetzen.

Beweis. Sei $\bar{K} \mid K$ algebraisch abgeschlossen und $\bar{K}$ algebraisch abgeschlossen
$\overset{4.6}{\implies}$ existiert Fortsetzung $\sigma \in \mathrm{Hom}_K(\bar{K}, \bar{K})$ von ϖ
$\bar{K}$ algebraisch abgeschlossen $\implies \sigma(\bar{K})$ algebraisch abgeschlossen
$\bar{K} \mid K$ algebraisch ist $\implies \bar{K} \mid \sigma(\bar{K})$ algebraisch $(\bar{K} = \sigma(\bar{K}))$ somsit ist $\sigma \in \mathrm{Aut}(\bar{K}, K)$. □

Definition 4.12 (konjugiert)
$\alpha, \beta \in \bar{K}$ sind K-konjugiert $\iff$ existiert $\sigma \in \mathrm{Aut}(\bar{K}, K)$ 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 $\Leftrightarrow \mathrm{MinPol}(\alpha \mid K) = \mathrm{MinPol}(\beta \mid K)$.

Beweis.

- $\Rightarrow$: $\sigma(\alpha) = \beta$ mit $\sigma \in \mathrm{Aut}(\bar{K} \mid K), f \in K[X],\ f(\alpha) = 0 \implies 0 = \sigma(0) = \sigma(f(\alpha)) = f(\sigma(\alpha)) = f(\beta)$
- $\Leftarrow$: $\mathrm{MinPol}(\alpha \mid K) = \mathrm{MinPol}(\beta \mid K)$
$\overset{3.5}{\implies}$ existiert K-Isomorphismus $\varphi : K(\alpha) \to K(\beta)$ mit $\varphi(\alpha) = \beta$
$\overset{4.11}{\implies}$ existiert Fortsetzung $\sigma \in \mathrm{Aut}(\bar{K}, K)$ 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) $a_1, \dots, a_n \in L$ algebraisch abhängig über K :⇔ existiert $0 \neq f \in K(X_1, \dots, X_n)\colon f(a_1, \dots, a_n) = 0$

(b) $(a_i)_{i \in I}$ ist algebraisch abhängig über K :⇔ existiert $J \subseteq I$ endlich: $(a_i)_{i \in I}$ algebraisch abhängig über K

■ **Beispiel**

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 ⇔ 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 :⇔ $L = K(\mathfrak{X})$ 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 $K \implies K(\mathfrak{X}) \cong_K K(X_i\colon i \in I) = \mathrm{Quot}(K[X_i\colon i \in I])$.

Beweis. Betrachte K-Isomorphismus

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

(a_i für x_i einsetzen.) 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 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 $K[X] \overset{\text{Gauss}}{\Longrightarrow} f$ irreduzibel in $K[X_1, \dots, X_n][X]$
$\overset{\text{Gauss}}{\Longrightarrow} f$ irreduzibel $K(X_1, \dots, X_n)[X]$

$\implies \deg(f) = 1$
$\implies \alpha \in K.$ $\square$

6. Die separable Erweiterung

Anhang

Index