

Algebra und Zahlentheorie SS 2019

Dozent: Prof. Dr. ARNO FEHM

13. Oktober 2019

Inhaltsverzeichnis

I	Körper	3
1	Körpererweiterungen	3
2	Algebraische Körpererweiterungen	6
3	Wurzelkörper und Zerfällungskörper	10
4	Der algebraische Abschluss	14
5	Die transzendente Erweiterung	18
6	Separable Polynome	21
7	Separable Erweiterungen	25
8	Norm und Spur	29
9	Einfache Erweiterung	33
II	Galoisttheorie	35
1	Normale Körpererweiterungen	35
2	Der Hauptsatz der Galoistheorie	40
3	Endliche Körper	44
4	Fundamentalsatz der Algebra	46
5	Das allgemeine Polynom	48
6	Kreisteilungskörper	52
7	Zyklische Erweiterungen	54
8	Auflösbarkeit von Gleichungen	57
	Anhang	59
	Index	59

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 $\mathbb{Z} \rightarrow R$.

► **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 $\text{Ker}(\mathbb{Z} \rightarrow K)$ prim ist.

(c) Aus (5) folgt: Jeder Ringhomomorphismus $K \rightarrow L$ 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 , $\text{char}(K)$, ist das $p \in \{0, 2, 3, 5, 7, \dots\}$ mit $\text{Ker}(\mathbb{Z} \rightarrow K) = (p)$.

■ **Beispiel 1.4**

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

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

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

Beweis.

(\Leftarrow) Beispiel 1.4

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

- (a) $\text{Im}(\mathbb{Z} \rightarrow K) \cong \mathbb{Z}/(0) \cong \mathbb{Z} \Rightarrow \mathbb{F} = \text{Quot}(\text{Im}(\mathbb{Z} \rightarrow K)) \cong \text{Quot}(\mathbb{Z}) \cong \mathbb{Q}$
- (b) $\text{Im}(\mathbb{Z} \rightarrow K) \cong \mathbb{Z}/(p) \cong \mathbb{F}_p$ ist Teilkörper von $K \Rightarrow \mathbb{F} = \text{Im}(\mathbb{Z} \rightarrow K) \cong \mathbb{F}_p$ □

Definition 1.7 (Körpererweiterung)

Ist K ein Teilkörper von L , so nennt man L eine Körpererweiterung von K , auch geschrieben $L | K$.

Definition 1.8 (K -Homomorphismus)

Seien $L_1 | K$ und $L_2 | K$ Körpererweiterungen.

- (a) Ein Ringhomomorphismus $\varphi: L_1 \rightarrow L_2$ ist ein K -Homomorphismus, wenn $\varphi|_K = \text{id}_K$ (i.Z. $\varphi: L_1 \rightarrow_K L_2$)
- (b) $\text{Hom}_K(L_1, L_2) = \{\varphi \mid \varphi: L_1 \rightarrow L_2 \text{ ist } K\text{-Homomorphismus}\}$
- (c) L_1 und L_2 sind K -isomorph (i.Z. $L_1 \cong_K L_2$), wenn es einen Isomorphismus $\varphi \in \text{Hom}_K(L_1, L_2)$ gibt.

► Bemerkung 1.9

Ist $L | K$ 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 $L | K$.

■ 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 Abzählbarkeitsargument oder siehe Abschnitt 2)
- (d) $[K(X) : K] = \infty$ ($K(X) = \text{Quot}(K[X])$) (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 $x_1, \dots, x_n \in L$ K -linear unabhängig und $y_1, \dots, y_m \in M$ L -linear unabhängig

$\Rightarrow \{x_i y_j \mid i \in \{1, \dots, n\}, j \in \{1, \dots, m\}\}$ K -linear unabhängig.

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

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

□

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 .

□

Definition 1.13 (Körpergrad endlich)

$L \mid K$ endlich $:\Leftrightarrow [L : K] < \infty$.

Definition 1.14 (Unterring, Teilkörper)

Sei $L \mid K$ eine Körpererweiterung $a_1, a_2, \dots, a_n \in L$.

- $K[a_1, \dots, a_n]$ ist kleinster Unterring von L , der $K \cup \{a_1, \dots, a_n\}$ enthält („ a_1, \dots, a_n über K erzeugt“)
- $K(a_1, \dots, a_n)$ 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)
- $L \mid K$ ist endlich erzeugt $:\Leftrightarrow a_1, \dots, a_n \in L: L = K(a_1, \dots, a_n)$
- $L \mid K$ ist einfach $:\Leftrightarrow$ existiert $a \in L: L = K(a)$

► Bemerkung 1.15

- $L \mid K$ endlich $\Rightarrow L \mid K$ endlich erzeugt.
- $K[a_1, \dots, a_n]$ ist das Bild des Homomorphismus

$$\begin{cases} K[X_1, \dots, X_n] \rightarrow L \\ f \mapsto f(a_1, \dots, a_n) \end{cases}$$

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

2. Algebraische Körpererweiterungen

Sei $L | K$ 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 $1, \alpha, \alpha^2, \dots$ K -linear abhängig sind.

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

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

Lemma 2.5

Betrachte den Epimorphismus

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

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

Beweis. K Hauptidealring $\Rightarrow \text{Ker}(\varphi_\alpha) = (f_\alpha)$, $f_\alpha \in K$, und o.E. sei f_α normiert. Aus $K[\alpha] \subseteq L$ nullteilerfrei folgt, dass $\text{Ker}(\varphi_\alpha)$ 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 , $\text{Ker}(\varphi_\alpha) = (f_\alpha)$ mit $f_\alpha \in K$ normiert und irreduzibel.

- (a) $\text{MinPol}(\alpha | K) := f_\alpha$, das Minimalpolynom von α über K .
- (b) $\deg(\alpha | K) := \deg(f_\alpha)$, der Grad von α über K .

Satz 2.7Sei $\alpha \in L$.(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

$$\Rightarrow K[\alpha] = K(\alpha) \cong K / \text{MinPol}(\alpha | K), [K(\alpha) : K] = \deg(\alpha | K) < \infty, \text{ und } 1, \alpha, \dots, \alpha^{\deg(\alpha|K)-1} \text{ ist } K\text{-Basis von } K(\alpha).$$

Beweis.(a) $\text{Ker}(\varphi_\alpha) = (0) \Rightarrow \varphi_\alpha$ ist Isomorphismus (da zusätzlich injektiv)

$$\Rightarrow K(\alpha) \cong_K \text{Quot}(K[\alpha]) \cong_K \text{Quot}(K[X]) = K(X)$$

$$\Rightarrow [K(\alpha) : K] = [K(X) : K] = \infty$$

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

- 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 $\Rightarrow K[\alpha] = K(\alpha)$
- $1, \alpha, \dots, \alpha^{n-1}$ sind K -linear unabhängig:

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

- $1, \alpha, \dots, \alpha^{n-1}$ 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:

$$K[\alpha] = \text{Im}(\varphi_\alpha) = \{g(\alpha) \mid g \in K[X]\} = \{r(\alpha) \mid r \in K, \deg(r) < n\} = \sum_{i=0}^{n-1} K \cdot \alpha^i \quad \square$$

■ 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 $\text{MinPol}(\sqrt{p} | \mathbb{Q}) = X^2 - p$, und $[\mathbb{Q}(\sqrt{p}) : \mathbb{Q}] = 2$.(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 $\text{MinPol}(\zeta_p | \mathbb{Q}) = \Phi_p$, $[\mathbb{Q}(\zeta_p) : \mathbb{Q}] = p - 1$.Daraus folgt schließlich $[\mathbb{C} : \mathbb{Q}] \geq [\mathbb{Q}(\zeta_p) : \mathbb{Q}] = p - 1 \quad \forall p \Rightarrow [\mathbb{C} : \mathbb{Q}] = \infty \Rightarrow [R : \mathbb{Q}] = \infty$.(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 $\xRightarrow{2.4} \alpha$ algebraisch über K . \square

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 :

- $n = 0$: \checkmark
- $n > 0$: $K_1 := K(\alpha_1, \dots, \alpha_{n-1})$ \square
 $\Rightarrow L = K_1(\alpha_n)$, 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 \square

► 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 $0 \neq f = \sum_{i=0}^n a_i X^i \in K[X]$.

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 $f = \text{MinPol}(\alpha | L) = \sum_{i=0}^n a_i x^i$, $L_0 := K(a_0, \dots, a_n)$

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

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

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

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

$$\stackrel{\alpha \text{ bel.}}{\Rightarrow} M | K \text{ algebraisch.}$$

□

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.

- $\alpha, \beta \in \tilde{K}$:
 $\Rightarrow K(\alpha, \beta) | K$ 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} :
 $\Rightarrow \tilde{K}(\alpha) | \tilde{K}$ algebraisch
 $\Rightarrow \tilde{K} | K$ algebraisch
 $\stackrel{2.14}{\Rightarrow} \tilde{K}(\alpha) | K$ 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 $L | K$ 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 $K[X]/(f) \xrightarrow{\cong} L$.

Beweis. Sei zunächst f irreduzibel, $f_\alpha = \text{MinPol}(\alpha | K)$. 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

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

Lemma 3.4

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

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

- K Körper $\Rightarrow \pi|_K$ injektiv
 \Rightarrow können K mit Teilkörper von L identifizieren, sodass $\pi|_K = \text{id}_K$
- (f) irreduzibel $\Rightarrow (f)$ prim $\xrightarrow{\text{GEO II.4.7}}$ (f) maximal $\Rightarrow L = K[X]/(f)$ ist Körper
- $f(\alpha) = f(\pi(X)) \stackrel{(*)}{=} \pi(f(X)) = 0 \Rightarrow f(X) \in \text{Ker}(\pi)$
(* gilt, da $f = \sum a_i X^i \Rightarrow \pi(f) = \sum \pi(a_i) \pi(X)^i = \sum a_i \pi(X)^i = f(\pi(X))$)
- $L = \pi(K[X]) = K[\pi(X)] = K[\alpha] \stackrel{\alpha \text{ alg.}}{=} K(\alpha)$ \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 $\varphi : L_1 \rightarrow L_2$ mit $\varphi(\alpha_1) = \alpha_2$.

Beweis.

- Existenz gibt Lemma 3.4
- Lemma 3.3 liefert Isomorphismus

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

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

Folgerung 3.6

f hat einen Wurzelkörper.

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

Folgerung 3.7

Es gibt eine Erweiterung $L \mid K$, über der f in Linearfaktoren zerfällt, also $f = c \prod_{i=1}^n (X - \alpha_i)$ mit $c \in K^\times$, $\alpha_1, \dots, \alpha_n \in L$.

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

$\xRightarrow{\text{IH}}$ Es existiert $L \mid L_1$, $\alpha_1, \dots, \alpha_n \in L$ 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 $L = K(\alpha_1, \dots, \alpha_n)$ 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 $K(\alpha_1, \dots, \alpha_n)$ ein Zerfällungskörper von f . □

Lemma 3.10

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

Beweis. Sei $L = K(\alpha_1, \dots, \alpha_n)$, $f = c \prod_{i=1}^n (X - \alpha_i)$. 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 $f = c \cdot (X - \alpha_1) \cdot f_1$, $f_1 = \prod_{i=2}^n (X - \alpha_i) \in L_1[X]$

$\Rightarrow L = K(\alpha_1, \dots, \alpha_n) = L_1(\alpha_2, \dots, \alpha_n)$ ist Zerfällungskörper von f_1 (über L_1)

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

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

■ 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 $L_1 = K(\alpha)$, $f = c(X - \alpha)f_1$ 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 : $\sqrt[3]{2} \in \mathbb{R}$, $\zeta_3 \sqrt[3]{2}$, $\zeta_3^2 \sqrt[3]{2}$

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

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

Dabei müsste man die Einheitswurzeln identifizieren:

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

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 $\varphi \in \text{Hom}(K, K')$. Ist $\sigma \in \text{Hom}(L, L')$ eine Fortsetzung von φ (d.h. $\sigma|_K = \varphi$), so ist $\sigma(\alpha)$ eine Nullstelle von $f^\varphi = \sum_{i=0}^n \varphi(a_i) X^i \in K'[X]$.

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

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

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

Beide sind Homomorphismen nach der universellen Eigenschaft. (Bemerke: $\eta|_K = \text{id} \rightarrow K \subset \text{Im}(\eta)$ mit $\eta(X) = \alpha \rightarrow \alpha \in \text{Im}(\eta)$)

Aus $\text{Ker}(\eta) = (f)$ folgt der Isomorphismus $\bar{\eta}: K[X]/(f) \xrightarrow{\cong} L$ und

$f \in \text{Ker}(\psi) \Rightarrow \text{Ker}(\psi) = (f)$ liefert Homomorphismus $\bar{\psi}: K[X]/(f) \rightarrow L'$
 $\sigma := \bar{\psi} \circ \bar{\eta}^{-1}: L \rightarrow L'$ 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 $\varphi: K \rightarrow K'$ ein Isomorphismus, L ein Zerfällungskörper und L' ein Zerfällungskörper von f^φ , so setzt sich φ zu einem Isomorphismus $L \rightarrow L'$ fort.

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

$$n = 1: L = K \xrightarrow[\varphi]{\cong} K' = L' \quad \checkmark$$

$n > 1$: 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 $g_1^\varphi(\alpha'_1) = 0$

$\xRightarrow{3.12} \varphi$ setzt man zu einem Isomorphismus

$$\sigma: K_1 := K(\alpha_1) \rightarrow K'(\alpha'_1) \quad \text{mit } \sigma(\alpha_1) = \alpha'_1$$

fort.

Schreibe $f = (X - \alpha_1) \cdot f_1$ mit $f_1 \in K_1[X]$

$$\Rightarrow f^\varphi = (x - \underbrace{\sigma(\alpha_1)}_{\alpha'_1}) \cdot f_1^\sigma \quad \text{mit } f_1^\sigma \in K'_1[X].$$

L ist Zerfällungskörper von f_1 , L' ist Zerfällungskörper von f_1^σ

$\Rightarrow \sigma$ setzt sich fort zu einem Isomorphismus $L \rightarrow L'$

□

Die Behauptung im Fall $\varphi = \text{id}_K$ 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: $L = K(\alpha_1, \dots, \alpha_n)$, wobei $\alpha_1, \dots, \alpha_n$ 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 \iff 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 $f = \text{MinPol}(\alpha \mid K)$. 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 $L \stackrel{(*)}{=} K$ nach (c) hat f Nullstellen in K .
- (*) L ist Erweiterung \rightarrow die nach (c) trivial ist □

Definition 4.3 (algebraischer Abschluss)

L ist algebraischer Abschluss von K : $\iff L$ 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 $\tilde{K} \xrightarrow{2.15} \alpha \in \tilde{K}$. □

■ Beispiel 4.5

- (a) \mathbb{C} ist algebraisch abgeschlossen (Fundamentalsatz der Algebra, Theorem II.4.4)
- (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 die Halbordnung

$$\mathfrak{X} := \{(M, \sigma) \mid K \subseteq M \subseteq L \text{ Zwischenkörper}, \sigma \in \text{Hom}(M, E), \sigma|_K = \varphi\}$$

mit der Ordnung

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

Dann ist

- $\mathfrak{X} \neq \emptyset$: $(K, \varphi) \in \mathfrak{X}$
- Ist $(M, \sigma)_{i \in I}$ eine Kette in \mathfrak{X} , so definieren wir $M := \bigcup_{i \in I} M_i$ und $\sigma: M \rightarrow E$ 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 dem Lemma von ZORN existiert (M, σ) maximal. Es ist $M = L$: Sei $\alpha \in L$, $f = \text{MinPol}(\alpha \mid M)$. $f \in E[X]$ hat Nullstelle $\beta \in E$, da E algebraisch abgeschlossen ist [3.12](#) existiert Fortsetzung $\sigma' \in \text{Hom}(M(\alpha), E)$ von σ $(M, \sigma) \leq (M(\alpha), \sigma') \in \mathfrak{X} \xrightarrow{(M(\alpha), \sigma) \text{ max.}} M = M(\alpha)$, $\alpha \in M$. \square

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 $\xrightarrow{4.6}$ existiert $\sigma \in \text{Hom}(L_1, L_2)$

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

Somit ist $\sigma: L_1 \rightarrow L_2$ ein K -Isomorphismus.

- Existenz: Seien

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

Behauptung 1: Es gilt $I \trianglelefteq R$.

Beweis. Angenommen $I = R$. Dann existieren $f_1, \dots, f_n \in \mathcal{F}$ und $g_1, \dots, g_n \in R$ mit

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

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 $\varphi: R \rightarrow L$ der Einsetzungshomomorphismus gegeben durch

$$\varphi|_K = \text{id}_K, \quad \varphi(X_{f_i}) = \alpha_i, \quad \varphi(X_f) = 0 \text{ für } f \in \mathcal{F} / \{f_1, \dots, f_n\}$$

Dann folgt

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

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 $f \in \mathcal{F}$ 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 $L_{i+1} \subseteq L$ \square

Nach Lemma 4.4 ist somit

$$\bar{K} = \{\alpha \in L \mid \alpha \text{ algebraisch über } K\}$$

ein algebraischer Abschluss von K . \square

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)

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

► Bemerkung 4.10

$\text{Aut}(L \mid K)$ 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 $\varphi \in \text{Hom}_K(L, \bar{K})$ lässt sich zu einem $\sigma \in \text{Aut}(\bar{K} \mid K)$ fortsetzen.

Beweis. Sei $\bar{K} \mid K$ algebraisch abgeschlossen und \bar{K} algebraisch abgeschlossen

$\xRightarrow{4.6}$ existiert Fortsetzung $\sigma \in \text{Hom}_K(\bar{K}, \bar{K})$ von φ

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

somit ist $\sigma \in \text{Aut}(\bar{K}, K)$. \square

Definition 4.12 (konjugiert)

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

Beweis.

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

(\impliedby) $\text{MinPol}(\alpha \mid K) = \text{MinPol}(\beta \mid K)$

$\xRightarrow{3.5}$ existiert K -Isomorphismus $\varphi: K(\alpha) \rightarrow K(\beta)$ mit $\varphi(\alpha) = \beta$

$\xRightarrow{4.11}$ existiert Fortsetzung $\sigma \in \text{Aut}(\bar{K}, K)$ von φ . \square

■ **Beispiel 4.15**

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

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) $L = K(X_1, \dots, X_n) = \text{Quot}(K[X_1, \dots, X_n]) \implies X_1, \dots, X_n$ 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 $K \implies K(\mathfrak{X}) \cong_K K(X_i : i \in I) = \text{Quot}(K[X_i : i \in I])$.

Beweis. Betrachte K -Isomorphismus

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

Da \mathfrak{X} algebraisch unabhängig über K , ist $\text{Ker}(\varphi) = (0)$

$\implies K(\mathfrak{X}) = \text{Quot}(K[\mathfrak{X}]) \cong_K \text{Quot}(K[X_i : i \in I])$. □

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 $f = \text{MinPol}(\alpha \mid K)$.

f irreduzibel in $K[X] \xrightarrow{\text{GAUSS}} f$ irreduzibel in $K[X_1, \dots, X_n][X]$

$\xrightarrow{\text{GAUSS}} f$ irreduzibel in $K(X_1, \dots, X_n)[X]$

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

$$\implies \alpha \in K$$

□

► **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 $\sqrt{a_i} \in \tilde{L} \setminus L$.

Definition 5.7 (Transzendenzbasis)

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

Beweis.

$(\Leftarrow) a \in L \setminus K(\mathfrak{X}) \xrightarrow{\text{maximal}} \mathfrak{X} \cup \{a\}$ 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

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

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

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

O.E. (Problem: Nenner kann Koeffizienten in $K(\mathfrak{X})$ haben \rightarrow 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

$$\begin{array}{c} L \\ \downarrow \text{algebraisch} \\ K(\mathfrak{X}) \\ \downarrow \text{rein transzendent} \\ K \end{array}$$

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 $K(\mathfrak{X}')$

$\implies K(\mathfrak{X} \cup \mathcal{Y}) \mid K(\mathfrak{X}')$ algebraisch

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

Theorem 5.12 (Steinitz, 1910)

Je zwei Transzendenzbasen von $L \mid K$ besitzen die gleiche Mächtigkeit.

Beweis. Seien $\mathfrak{X} = (a_i)_{i \in I}$, $\mathcal{Y} = (b_j)_{j \in J}$ Transzendenzbasen 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 $\implies |I| = 0$

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

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 Transzendenzbasis 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 Transzendenzbasen 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

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

mit $f(a_{i_1}, \dots, a_{i_m}) = 0$.

O.E. ist $f \in K[a_1][X_1, \dots, X_m]$, d.h. es existiert $g \in K[X, X_1, \dots, X_m]$ mit

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

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

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

Definition 5.13 (Transzendenzgrad)

Der Transzendenzgrad von $L \mid K$ ist die Mächtigkeit $\text{tr. deg}(L \mid K)$ einer Transzendenzbasis von $L \mid K$.

Folgerung 5.14

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

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

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

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

$$L(\mathcal{Y}) = K(\mathfrak{X} \cup \mathcal{Y})(L)$$

$$\xrightarrow{L|K(\mathfrak{X}) \text{ alg.}} L(\mathcal{Y}) \mid K(\mathfrak{X} \cup \mathcal{Y}) \text{ algebraisch}$$

$$\Rightarrow M \mid K(\mathfrak{X} \cup \mathcal{Y}) \text{ algebraisch.} \quad \square$$

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

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

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

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

- (c) Aus (b) folgt insbesondere:

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

Definition 6.3

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

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

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 $\text{char}(K) \nmid \mu(f, a)$.

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

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

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

$$\mu(f', a) \geq k \iff (X - a)^k \mid k(X - a)^{k-1} \cdot g$$

$$\iff X - a \mid k \cdot g$$

$$\iff X - a \mid k$$

$$\iff k = 0 \text{ in } K$$

$$\iff \text{char}(K) \mid k$$

□

Satz 6.6

Sei $f \neq 0$. Dann gilt:

$$f \text{ separabel} \iff \text{ggT}(f, f') = 1$$

Beweis.

(\Rightarrow) f separabel

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

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

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

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

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

□

Lemma 6.7

$f' = 0 \iff \exists g \in K[X]$ mit $f(X) = g(X^p)$ und $p = \text{char}(K)$.

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

$$f' = 0 \iff i a_i = 0 \text{ in } K \forall i$$

$$\iff \forall i: i = 0 \text{ in } K \text{ oder } a_i = 0$$

□

$$\iff f = a_0 + a_p X^p + \dots + a_{pm} X^{pm} = g(X^p) \text{ mit } g = a_0 + a_p X + \dots + a_{pm} X^m$$

Folgerung 6.8

Sei f irreduzibel

- (a) Ist $\text{char}(K) = 0$, so ist f separabel
- (b) Ist $\text{char}(K) = p > 0$, 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 $\implies \underbrace{\text{ggT}(f, f') \sim 1}_{\substack{\text{6.6} \\ \iff f \text{ sep}}} \text{ oder } \underbrace{\text{ggT}(f, f') \sim f}_{\substack{\text{6.6} \\ \iff f \text{ sep}}}.$

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

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

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

Definition 6.9 (vollkommen)

K ist vollkommen \iff jedes irreduzibel $f \in K[X]$ ist separabel.

■ Beispiel 6.10

- (a) $\text{char}(K) = 0 \implies K$ ist vollkommen
- (b) $K = \bar{K} \implies K$ ist vollkommen
- (c) $K = \mathbb{F}_p(t)$ ist nicht vollkommen:

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

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

Definition 6.11

Sei $\text{char}(K) = p > 0$.

- (1) Der FROBENIUS-Endomorphismus von K ist

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

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

Satz 6.12

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

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 $\Phi_p \in \text{End}(K)$ 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 $\text{char}(K) = p > 0$, $a \in K \setminus K^p$. Dann ist $f = X^p - a$ irreduzibel und inseparabel

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

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

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

$$a \notin K^p$$

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

$$\implies g \text{ ist inseparabel}$$

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

$$\implies k = p \implies f = g \text{ irreduzibel}$$

□

Satz 6.15

Genau dann ist K vollkommen, wenn

- (i) $\text{char}(K) = 0$ oder
- (ii) $\text{char}(K) = p > 0$ und $K^p = K$

Beweis.

- $\text{char}(K) = 0$: klar (Beispiel 6.10 (a))
- $\text{char}(K) = p > 0$:
 (\implies) Es existiert ein $a \in K \setminus K^p$, so ist K nicht vollkommen nach Lemma 6.14.
 (\impliedby) 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

$$f(X) = g(X^p) = \sum_{i=0}^n a_i (X^i)^p \stackrel{=}{=} \sum_{\substack{i \in \bar{K}^0 \\ \text{da } K^p = K}}^n \underbrace{a_i^{1/p}}_{\in K} X^i \Bigg)^p,$$

folglich ein Widerspruch.

□

■ **Beispiel 6.16**

K endlich $\implies K$ 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 $f = \text{MinPol}(\alpha \mid K)$ ist

$$[L : K] = \deg(f) \geq |\{\beta \in \bar{K} \mid f(\beta) = 0\}| \stackrel{3.12}{=} |\text{Hom}_{\mathbb{K}}(L, \bar{K})|$$

mit Gleichheit genau dann wenn f separabel.

Definition 7.2

Sei $\alpha \in L$.

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

$$[L : K]_S = |\text{Hom}_{\mathbb{K}}(L, \bar{K})|$$

Lemma 7.3

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

$$|\{\psi \in \text{Hom}(L, E) \mid \psi|_K = \varphi\}| = [L : K]_S$$

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

$$\left\{ \begin{array}{ll} \text{Hom}_{\mathbb{K}}(L, \bar{K}) & \Rightarrow \{\psi \in \text{Hom}(L, E) \mid \psi|_K = \varphi\} \\ \sigma & \mapsto g \circ \sigma \end{array} \right.$$

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

Satz 7.4

Sind $K \subset L \subset M$ Körper mit $M \mid K$ algebraisch, so ist

$$[M : K]_S = [M : L]_S [L : K]_S$$

Insbesondere ist $[L : K]_S \leq [M : K]_S$.

Beweis. Betrachte die Abbildung

$$f: \left\{ \begin{array}{ll} \text{Hom}(M, \bar{K}) & \rightarrow \text{Hom}_{\mathbb{K}}(L, \bar{K}) \\ \sigma & \mapsto \sigma|_L \end{array} \right.$$

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

$$f^{-1}(\{\tau\}) = \left| \left\{ \sigma \in \text{Hom}_{\mathbb{K}}(M, \bar{K}) \mid \sigma|_L = \tau \right\} \right| = [M : L]_S$$

Daher gilt $[M : K]_S = [M : L]_S [L : K]_S$. □

Lemma 7.5

Sei $L \mid K$ endlich und $p = \text{char}(K) > 0$. Dann ist

$$[L : K] = p^l [L : K]_S$$

für ein $l \in \mathbb{N}$. Insbesondere ist $[L : K]_S \leq [L : K]$.

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

$$[L : K]_S \stackrel{7.1, 7.2}{=} \left| \left\{ x \in \bar{K} \mid f(x) = 0 \right\} \right| = \left| \left\{ x \in \bar{K} \mid g(x) = 0 \right\} \right| = \deg(g) = \frac{\deg(f)}{p^l} = \frac{[L : K]}{p^l},$$

sodass $[L : K] = p^l [L : K]_S$. □

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) $[L : K]_S = [L : K]$.

Beweis.

(1) \Rightarrow (2) klar nach Definition 7.2

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

$$[K(\alpha_1, \dots, \alpha_i) : K(\alpha_1, \dots, \alpha_{i-1})]_S \stackrel{7.1}{=} [K(\alpha_1, \dots, \alpha_i) : K(\alpha_1, \dots, \alpha_{i-1})]$$

Nach Sätze 1.12 und 7.4 gilt dann

$$[L : K]_S = [L : K]$$

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

$$[L : K] \stackrel{1.12}{=} [L : K(\alpha)][K(\alpha) : K] \stackrel{7.5}{\geq} [L : K(\alpha)]_S \cdot p^l [K(\alpha) : K]_S \stackrel{7.4}{=} [L : K]_S p^l \stackrel{(3)}{=} [L : K] p^l,$$

daher $l = 0$, d.h. $[K(\alpha) : K] = [K(\alpha) : K]_S$. 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). \square

Folgerung 7.8

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

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

Beweis.

(\Rightarrow) klar

(\Leftarrow) Sei $\alpha \in M$, setze $f = \text{MinPol}(\alpha \mid L) = \sum_{i=0}^n a_i X^i$ und $L_0 = K(a_0, \dots, a_n)$. 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

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

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

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 $L_1 \cdot L_2 := K(L_1, L_2)$.

Beweis. Es sei $\alpha \in L_1 L_2$. Dann gibt es $x_1, \dots, x_n \in L_1$ und $y_1, \dots, y_m \in L_2$ mit $\alpha \in K(x_1, \dots, x_n, y_1, \dots, y_m) =: L_0$. 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 . \square

Definition 7.10

Die Erweiterung $L \mid K$ ist rein separabel $:\Leftrightarrow$ jedes $\alpha \in L \setminus K$ ist inseparabel über K .

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

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

(2) \Rightarrow (3) Sei $\varphi \in \text{Hom}_K(L, \bar{K})$ 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 $\sigma|_L = \text{id}_L$ und daher $[L : K]_S = 1$.

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

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

also ist α inseparabel über K nach Satz 7.6. \square

■ 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

$$[L : K]_S \stackrel{7.4}{=} [L : L_S]_S [L_S : K] \stackrel[7.6]{7.11}{=} 1 \cdot [L_S : K] = [L_S : K]$$

8. Norm und Spur

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

► Bemerkung 8.1

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

Definition 8.2 (Spur, Norm)

- (a) $\mu_\alpha: \begin{cases} L \rightarrow L \\ x \mapsto \alpha x \end{cases} \in \text{End}_K(L)$
- (b) $N_{L|K}(\alpha) := \det(\mu_\alpha)$, die $(L \mid K)$ - Norm von α
 $\text{Tr}_{L|K}(\alpha) := \text{Tr}(\mu_\alpha)$, 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) $f_\alpha = \text{MinPol}(\alpha \mid K)$
 (b) $\chi_\alpha = f_\alpha^m$ für $m = [L : K(\alpha)]$

Beweis.

- (a) Die Abbildung

$$\mu: \begin{cases} L \rightarrow \text{End}_K(L) \\ \beta \mapsto \mu_\beta \end{cases} \quad (\star)$$

ist K -linearer Ringhomomorphismus: ✓

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

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

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

V n -dimensionaler K -VR, $\varphi \in \text{End}_K(V)$, \mathcal{B} Basis von $V \rightsquigarrow A = M_{\mathcal{B}}(\varphi)$. $\chi_\varphi = \chi_A \in K[X]$ 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.

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

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

■ **Beispiel 8.4**

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

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

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

$$\Rightarrow N_{\mathbb{C}|\mathbb{R}}(\alpha) = \det(M_{\mathcal{B}}(\mu_\alpha)) = x^2 + y^2 = |\alpha|^2 = \alpha\bar{\alpha},$$

$$\mathrm{Sp}_{\mathbb{C}|\mathbb{R}}(\alpha) = \mathrm{Sp}(M_{\mathcal{B}}(\mu_\alpha)) = 2\alpha = \alpha + \bar{\alpha}$$

$$\begin{aligned} \chi_\alpha(t) &= \det(\mathbb{1} - A) = (t - x)^2 + y^2 = t^2 - 2xt + x^2 + y^2 = t^2 - 2\mathrm{Sp}_{\mathbb{C}|\mathbb{R}}(\alpha)t + N_{\mathbb{C}|\mathbb{R}}(\alpha) \\ &= (t - \alpha)(t - \bar{\alpha}), \end{aligned}$$

$$f_\alpha(t) = \begin{cases} t - \alpha, & \alpha \in \mathbb{R}, \\ (t - \alpha)(t - \bar{\alpha}), & \alpha \notin \mathbb{R} \end{cases}$$

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) $\chi_\alpha = X^n + b_{n-1}X^{n-1} + \cdots + b_0$

$$\Rightarrow \det \mu_\alpha = (-1)^n \chi_\alpha(0) = (-1)^n b_0, \quad \mathrm{Sp}_{\mu_\alpha} = -b_{n-1}$$

$$\chi_\alpha = (f_\alpha)^m$$

$$\Rightarrow N_{L|K}(\alpha) = \det(\mu_\alpha) = (-1)^n a_0^m, \quad \mathrm{Sp}_{L|K}(\alpha) = \mathrm{Sp} \mu_\alpha = -b_{n-1} = -m \cdot a_{r-1}$$

□

► **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

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

(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 $\mathrm{hom}_K(L, \bar{K}) = \{\sigma_1, \dots, \sigma_r\}$, so gilt

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

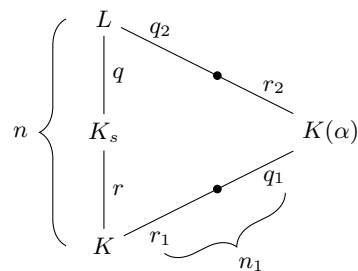
Beweis.

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

Schreibe

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

$$g(X) = \prod_{i=1}^{r_1} (X - \tau_i^{q_1}(\alpha))$$



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

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

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

□

Lemma 8.8

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

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

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

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

denn $\# \operatorname{Hom}(M, \bar{K}) = [M : K]_{\mathbb{S}} = r_1 \cdot r_2$ und

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

Analog für die Spur. \square

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 χ_1, \dots, χ_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 $\chi_1 \neq \chi_n \Rightarrow \exists g \in G$ 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

$$\begin{aligned}
 \Rightarrow \forall h \in G: & \begin{cases} \sum_{i=1}^n a_i \cdot \underbrace{\chi_i(hg)}_{\chi_i(h) \cdot \chi_i(g)} = 0 \\ \sum_{i=1}^n a_i \cdot \chi_i(h) \cdot \chi_i(g) = 0 \end{cases} \\
 \Rightarrow 0 &= \sum_{i=1}^n a_i \cdot \chi_i(h) (\chi_i(g) - \chi_n(g)) = \sum_{i=1}^{n-1} a_i (\chi_i(g) - \chi_n(g)) \cdot \chi_i(h) \\
 \Rightarrow \sum_{i=1}^{n-1} a_i \cdot (\chi_i(g) - \chi_n(g)) \cdot \chi_i &= 0
 \end{aligned}$$

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

Folgerung 8.10

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

Beweis.

(\Rightarrow) Bemerkung 8.6

(\Leftarrow) Sei $\operatorname{Hom}_K(L, \bar{K}) = \{\sigma_1, \dots, \sigma_n\}$. $\sigma_i|_{L^\times} \in \operatorname{Hom}_K(L^\times, K^\times)$

$\stackrel{8.7}{\Rightarrow} \sigma_1, \dots, \sigma_n$ sind \bar{K} -linear unabhängig. Insbesondere ist $\operatorname{Tr}_{L|K} = \sum_{i=1}^n \sigma_i \neq 0$. \square

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

Beweis.

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

$$g := \text{MinPol}(\alpha \mid M) = \sum_{i=0}^n a_i X^i,$$

$$M_0 := K(a_0, \dots, a_n).$$

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

$$\implies M \mid K \text{ endlich und einfach}$$

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

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

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

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

Sei $\gamma := \alpha + c\beta$ und $f = \text{MinPol}(\alpha | K)$ sowie $g := \text{MinPol}(\beta | K)$.

Behauptung: $g(X)$ und $f(\gamma - cX)$ haben genau eine gemeinsame Nullstelle β .

Beweis.

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

□

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

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

$\xrightarrow{\beta \text{ sep.}} g$ 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

$\mathbb{Q}(\sqrt{2}, \sqrt{3}) | \mathbb{Q}$ 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

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

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 $L = \mathbb{F}_p(t, s) = \text{Quot}(\mathbb{F}_p[t, s])$, $K = L^p$. Dann ist $[L : K] = p^2$ (↗ P41) aber $L | K$ 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

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

Satz 1.2

Ist $L | K$ endlich, so sind äquivalent

- (a) $L | K$ 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 $\sigma \in \text{Aut}(\bar{K} | K)$ ist $\sigma(L) = L$
- (e) Jedes $\sigma \in \text{Aut}(\bar{K} | K)$ ist $\sigma(L) \subseteq L$

Beweis.

(1) \Rightarrow (2) klar nach Folgerung 1.4.14

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

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

ist L der Zerfällungskörper von f .

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

$$f = \prod_{i=1}^n (X - X_i),$$

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

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

(4) \Rightarrow (5) trivial

(5) \Rightarrow (1) trivial □

■ Beispiel 1.3

- a) $K | K$ ist normal
- b) $\bar{K} | K$ ist normal

- c) $\bar{K}_S \mid K$ ist normal (Folgerung 1.7.7)
- d) $[L : K] = 2 \Rightarrow L \mid K$ ist normal
 $(\deg(f) = 2, f \text{ hat Nullstelle} \Rightarrow f \text{ zerfällt in Linearfaktoren})$
- e) $L = \mathbb{Q}(\sqrt[3]{2}), [L : \mathbb{Q}] = 3 \mid \mathbb{Q}$ 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 1.3.11 (b))
- f) $Sei \alpha = \sqrt[4]{2} \in \mathbb{R}_{\geq 0}$ und $f = \text{MinPol}(\alpha \mid \mathbb{Q}) = X^4 - 2$. 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

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

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) • $L_1 \cap L_2$: klar aus Definition
- $L_1 L_2$: Sei $\sigma \in \text{Aut}(\bar{K} \mid K) \Rightarrow \sigma(L_1 L_2) = \sigma(L_1) \sigma(L_2) = L_1 L_2$
- b) klar, da $\text{Aut}(\bar{L}_1 \mid L_1) \subseteq \text{Aut}(\bar{K} \mid K)$ □

Satz 1.5

Sei $L \mid K$ endlich. Es ist

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

mit Gleichheit, wenn die Erweiterung normal ist.

Beweis. Es ist

$$\text{Aut}(L \mid K) = \text{Hom}_K(L, L) = \{ \sigma \in \text{Hom}_K(L, \bar{K}) \mid \sigma(L) \subseteq L \} \subseteq \text{Hom}_K(L, \bar{K}),$$

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

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

$$\Leftrightarrow \forall \sigma \in \text{Hom}_K(L \mid \bar{K}): \sigma(L) \subseteq L$$

$$\xLeftrightarrow{1.4.11} \forall \sigma \in \text{Aut}(\bar{K} \mid K): \sigma(L) \subseteq L$$

$$\xLeftrightarrow{1.2} L \mid K \text{ normal.} \quad \square$$

► **Bemerkung 1.6**

Es ist also

$$\text{Aut}(L | K) \stackrel{\textcircled{1}}{\leq} [L : K]_s \stackrel{\textcircled{2}}{\leq} [L : K],$$

wobei gilt:

① ist Gleichheit : $\stackrel{1.5}{\iff} L | K$ normal

② ist Gleichheit : $\stackrel{1.7.6}{\iff} L | K$ separabel

Definition 1.7

$L | K$ ist galoissch (oder Galoiserweiterung) $\iff L | K$ ist normal und separabel

Satz 1.8

Ist $L | K$ endlich, so sind äquivalent

- (1) $L | K$ ist galoissch
- (2) Jedes $\alpha \in L$ hat $\deg(\alpha | L)$ 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) $\# \text{Aut}(L | K) = [L : K]$

Beweis.

(1) \iff (5) Bemerkung 1.6

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

(1) \Rightarrow (3) $L | K$ separabel $\stackrel{1.9.4}{\implies} L = K(\alpha)$ einfach.
 $L | K$ normal $\Rightarrow L$ ist Zerfällungskörper von $\text{MinPol}(\alpha | K)$

(3) \Rightarrow (4) trivial

(4) \Rightarrow (1) Satz 1.2 und Satz 1.7.6 □

Folgerung 1.9

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

- (a) Sind $L_1 | K$ und $L_2 | K$ galoissch, so auch $L_1 \cap L_2 | K$ und $L_1 L_2 | K$
- (b) Ist $L | K$ galoissch, so auch $L | L_1$

Beweis. Folgerung 1.4, Folgerung 1.7.8 und Folgerung 1.7.9. □

Definition 1.10

Ist $L | K$ galoissch, so heißt

$$\text{Aut}(L | K) = \text{Gal}(L | K)$$

die Galoisgruppe von $L | K$.

► **Bemerkung 1.11**

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

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

Definition 1.12

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

$$L^G := \{ \alpha \in L \mid \forall \sigma \in G: \alpha^\sigma = \alpha \}$$

der Fixkörper von G .

► **Bemerkung 1.13**

L^G ist ein Teilkörper von L .

Satz 1.14 (Artin)

Sei $G \leq \text{Aut}(L)$ endlich, so ist $L \mid L^G$ galoissch und $\text{Gal}(L \mid L^G) = G$.

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

$$G_\alpha = \{ \sigma \in G \mid \alpha^\sigma = \alpha \} \leq G$$

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

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

Dann 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

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

und

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

$L \mid L^G$ ist also nach Definition 1.7.2 separabel.

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

$$[L : K] \stackrel{1.9.4}{\leq} \#G \leq \# \operatorname{Aut}(L | K) \stackrel{1.6}{\leq} [L : K].$$

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

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

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

Folgerung 1.15

Sei $L | K$ endlich. Es gilt

$$L | K \text{ galoissch} \Leftrightarrow L^{\operatorname{Aut}(L|K)} = K$$

Beweis.

(\Rightarrow) $L | K$ galoissch

$$\stackrel{1.8}{\Rightarrow} \operatorname{Aut}(L | K) = [L : K]$$

$$K \subset L^{\operatorname{Aut}(L|K)} \subset L$$

$$\Rightarrow [L : L^{\operatorname{Aut}(L|K)}] \stackrel{1.14}{=} \# \operatorname{Aut}(L | K)$$

$$\Rightarrow K = L^{\operatorname{Aut}(L|K)}$$

(\Leftarrow) $L | K$ endlich

$$\stackrel{1.5}{\Rightarrow} \operatorname{Aut}(L | K) \text{ endlich}$$

$$\stackrel{1.14}{\Rightarrow} L | L^{\operatorname{Aut}(L|K)} = K \text{ ist galoissch} \quad \square$$

Lemma 1.16

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

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

ein Epimorphismus.

Beweis. Nach Satz 1.4.11 sind $\operatorname{res}_{\bar{K}|M}$ und $\operatorname{res}_{\bar{K}|L}$ surjektiv. Dann

- $\sigma|_L \in \operatorname{Aut}(L | K)$: 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

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

Definition 2.1

Es sind

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

Theorem 2.2 (Galoiskorrespondenz)

Es sind

$$\left\{ \begin{array}{ll} \text{Zwk}(L | K) \rightarrow & \text{Ugr}(G) \\ F & \mapsto F^\circ := \text{Gal}(L | F) \end{array} \right. \quad \left\{ \begin{array}{ll} \text{Ugr}(G) \rightarrow & \text{Zwk}(L | K) \\ H & \mapsto H^\circ := L^H \end{array} \right.$$

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

i) die Bijektion 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:

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

In diesem Fall gilt:

$$\text{Gal}(F | K) \cong G/H = \text{Gal}(L | K) / \text{Gal}(L | F)$$

Beweis.

- $F \in \text{Zwk}(L | K) \xrightarrow{1.9} F \text{ galoissch} \xrightarrow{1.15} (F^\circ)^\circ = L^{F^\circ} = F$

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

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) • $F_1 \cap F_2 \subset F_1 F_2 \Rightarrow (F_1 \cap F_2)^\circ \supset \langle H_1, H_2 \rangle$,

$$H_1, H_2 \subset \langle H_1, H_2 \rangle \Rightarrow F_1 \cap F_2 \supset (\langle H_1, H_2 \rangle)^\circ \Rightarrow (F_1 \cap F_2)^\circ \subset ((\langle H_1, H_2 \rangle)^\circ)^\circ = \langle H_1, H_2 \rangle$$

- $F_1, F_2 \subset F_1 F_2 \Rightarrow H_1 \cap H_2 \supset (F_1 F_2)^\circ$

$$H_1 \cap H_2 \subset H_1, H_2 \Rightarrow (H_1 \cap H_2)^\circ \supset F_1 F_2 \Rightarrow (F_1 F_2)^\circ \supset ((H_1 \cap H_2)^\circ)^\circ = H_1 \cap H_2$$

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

v) $F \mid K$ normal

$$\xLeftrightarrow{1.2} F^\sigma = F \forall \sigma \in \text{Aut}(\bar{K} \mid K)$$

$$\xLeftrightarrow{1.16} F^\sigma = F \forall \sigma \in G$$

$$\xLeftrightarrow{\text{iv)}} H^\sigma = H \forall \sigma \in G$$

$$\Leftrightarrow H \trianglelefteq G$$

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

$$\text{res: } \begin{cases} \text{Gal}(L \mid K) \rightarrow \text{Gal}(F \mid K) \\ \sigma \mapsto \sigma|_F \end{cases}$$

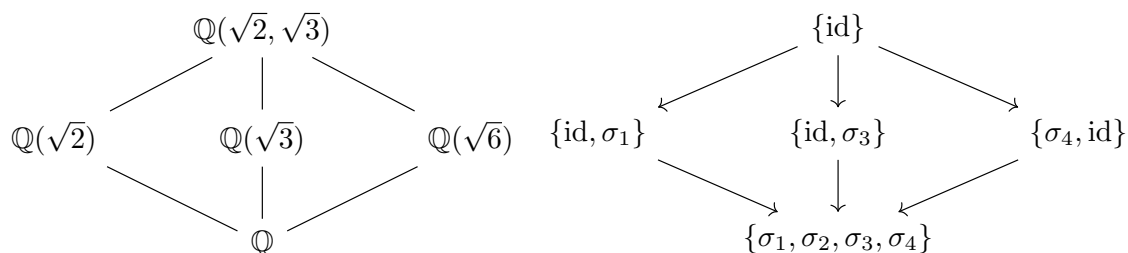
ist ein Epimorphismus.

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

□

■ Beispiel 2.3

Betrachte $\mathbb{Q}(\sqrt{2}, \sqrt{3}) \mid \mathbb{Q}$:



mit den Automorphismen

$$\begin{array}{cccc} \sigma_1: & \sqrt{2} \rightarrow \sqrt{2} & , & \sigma_2: \sqrt{2} \rightarrow \sqrt{2} & , & \sigma_3: \sqrt{2} \rightarrow -\sqrt{2} & , & \sigma_4: \sqrt{2} \rightarrow -\sqrt{2} . \\ & \sqrt{3} \rightarrow \sqrt{3} & & \sqrt{3} \rightarrow -\sqrt{3} & & \sqrt{3} \rightarrow \sqrt{3} & & \sqrt{3} \rightarrow -\sqrt{3} \end{array}$$

► **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 $\text{Ugr}(G)$ und $\text{Zwk}(L | K)$.
- (b) Die Bijektivität gilt nicht für unendliche Galoiserweiterungen (siehe Übung)
- (c) Mit Theorem 2.2 erhalten wir einen neuen Beweis der Aussage

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

was schon aus Satz 1.9.2 folgt.

Satz 2.5

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

$$G \rightarrow \text{Sym}(X) \cong S_n$$

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

Beweis. Sei $\sigma \in G$.

- treu: $\alpha_i^\sigma = \alpha_i \ \forall i \Rightarrow \sigma = \text{id}$, denn $L = K(\alpha_1, \dots, \alpha_n)$ und $\sigma|_K = \text{id}_K$.
- Einbettung: GEO I.6.8
- transitiv $\Leftrightarrow \forall i, j: \exists \sigma \in G: \sigma(\alpha_i) = \alpha_j$ □
 $\Leftrightarrow \forall i, j: \exists \sigma \in \text{Aut}(\bar{K} | K): \sigma(\alpha_i) = \alpha_j$
 $\Leftrightarrow \alpha_1, \dots, \alpha_n$ sind paarweise k -konjugiert
 $\Leftrightarrow f = c \cdot \text{MinPol}(\alpha_1 | K), c \in K^\times$
 $\Leftrightarrow f$ irreduzibel

Definition 2.6

In der Situation von Satz 2.5 heißt

$$\text{Gal}(f | K) := \text{Im}(G \rightarrow \text{Sym}(\alpha_1, \dots, \alpha_n))$$

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

$$\text{Gal}(L | K) \cong \text{Gal}(f | K) \leq \text{Sym}(\{\alpha_1, \dots, \alpha_n\}) \cong S_n.$$

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

■ **Beispiel 2.8**

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

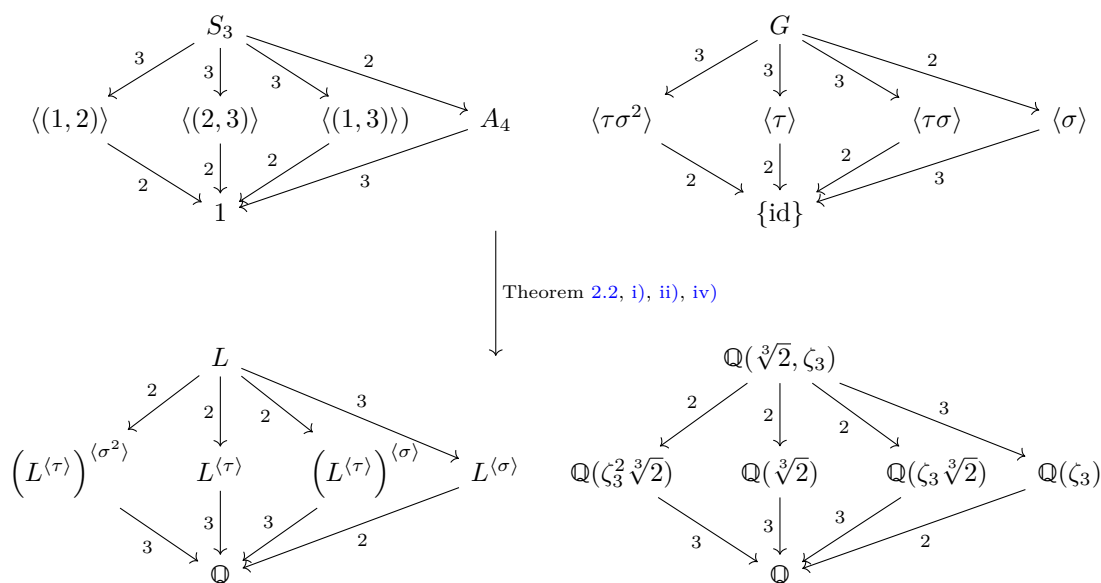
$$\begin{aligned}\alpha_1 &= \sqrt[3]{2}, \\ \alpha_2 &= \sqrt[3]{2}\zeta_3, \\ \alpha_3 &= \sqrt[3]{2}\zeta_3^2.\end{aligned}$$

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

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

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

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



3. Endliche Körper

Sei K ein endlicher Körper mit $\text{char}(K) = p$ 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) $K \cong \mathbb{F}_p^{[K:\mathbb{F}_p]}$ 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:

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

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

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

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

Beweis.

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

Lemma 3.6

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

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

Beweis.

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

$$(\Leftarrow) \quad \text{Gal}(L_2 | \mathbb{F}_q) \xrightarrow{3.5} C_{m_2}.$$

$$m_1 \mid m_2$$

$$\Rightarrow \text{ex. } H \leq C_{m_2} \text{ mit } \#H = \frac{m_2}{m_1}$$

$$\Rightarrow [L_2^H : \mathbb{F}_q] = (C_{m_2} : H) = m_1$$

$$\Rightarrow \#L_2^H = q^{m_1} = \#L_1$$

$$\xrightarrow{3.3} L_1 = L_2^H \subseteq L_2. \quad \square$$

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: $\mathbb{F}_q \subseteq \mathbb{F}_{q^m}$ 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 folgenden 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 $\hat{L} = K(\cup_{\sigma \in \text{Aut}(\bar{K}|K)} L^\sigma)$. Für $\tau \in \text{Aut}(\bar{K}, K)$ ist dann $\hat{L}^\tau = K(\cup_{\sigma} L^{\sigma\tau}) = K(\cup_{\sigma} L^\sigma) = \hat{L}$.

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

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

- separabel: $L \mid K$ separabel $\Rightarrow L^\sigma \mid K$ separabel $\xrightarrow{1.7.6} K(\cup_{\sigma} L^\sigma) \mid K$ 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 $z = a + bi \in \mathbb{C}$ hat eine Quadratwurzel in \mathbb{C} ($a, b \in \mathbb{R}$)

Beweis. $z = a + bi = (x + yi)^2 = x^2 + y^2 + 2xyi$ ($x, y \in \mathbb{R}$)

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

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

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

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

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

nach Bemerkung 4.1 (b).

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

□

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

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

$$\begin{aligned} &\xrightarrow{\text{Ü20}} \text{o.E. } \alpha^2 \in \mathbb{C} \\ &\xrightarrow{\text{Beh. 1}} \alpha \in \mathbb{C}. \end{aligned}$$

□

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

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

$$\xrightarrow{1.9.5} L = \mathbb{R}(\alpha) \text{ für ein } \alpha$$

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

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

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

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

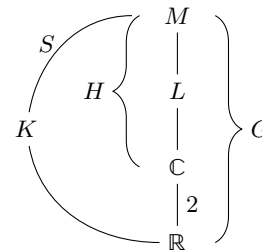
$$\Rightarrow [K : \mathbb{R}] = (G : S) \text{ ungerade}$$

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

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

$$\xrightarrow{\text{GEO 1.7.9}} \text{ex. } U \leq H \text{ mit } (H : U) = 2$$

$$\Rightarrow [M^U : \underbrace{M^H}_{=\mathbb{C}}] = (H : U) \not\equiv 1 \text{ zu Beh. 2}$$



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.

5. Das allgemeine Polynom

Sei K ein Körper, $R = K[x_1, \dots, x_n]$ Polynomring in n Variablen, $F = \text{Quot}(R) = K(x_1, \dots, x_n)$.

Definition 5.1

Das allgemeine Polynom vom Grad n ist

$$f_{\text{allg}} = \prod_{i=1}^n (X - X_i) = X^n + \sum_{k=1}^n s_k(X_1, \dots, X_n) X^{n-k} \in R[X],$$

wobei

$$s_k(X_1, \dots, X_n) = \sum_{1 \leq i_1 \leq \dots \leq i_k \leq n} X_{i_1} \dots X_{i_k} \in R$$

das k -te elementarsymmetrische Polynom in X_1, \dots, X_n ist (vgl. GEO II.10).

■ Beispiel 5.2

$n = 2 \Rightarrow s_1 = X_1 + X_2, s_2 = X_1 X_2$ und

$$(X - X_1)(X - X_2) = X^2 - (X_1 + X_2)X + X_1 X_2$$

Lemma 5.3

S_n wirkt auf R durch Permutation der Variablen

$$f(X_1, \dots, X_n)^\sigma = f(X_{1^\sigma}, \dots, X_{n^\sigma}) \quad (f \in R, \sigma \in S_n).$$

Diese setzt sich fort auf F durch

$$\left(\frac{f}{g}\right)^\sigma = \frac{f^\sigma}{g^\sigma} \quad (f, g \in R, \sigma \in S_n).$$

Beweis. Klar, siehe GEO. □

Definition 5.4

Sei $f \in F$. f ist symmetrisch $:\Leftrightarrow f^\sigma = f \ \forall \sigma \in S_n$ und $F_{\text{sym}} := \{f \in F \mid f \text{ ist symmetrisch}\}$.

Satz 5.5

F_{sym} ist Teilkörper von F , $F \mid F_{\text{sym}}$ ist galoissch mit

$$\text{Gal}(F \mid F_{\text{sym}}) \cong \text{Gal}(f_{\text{allg}} \mid F_{\text{sym}}) \cong S_n$$

und

$$F_{\text{sym}} = K(s_1, \dots, s_n).$$

Beweis. S_n wirkt auf F treu durch Automorphismen, d.h. $S_n \rightarrow \text{Sym}(F)$ ist Einbettung $S_n \hookrightarrow \text{Aut}(F)$.

$F_{\text{Sym}} = F^{S_n} \Rightarrow F_{\text{Sym}}$ ist Körper, $F \mid F_{\text{Sym}}$ galoissch mit $\text{Gal}(F \mid F_{\text{Sym}}) = S_n$ (Satz 1.14).

$$s_1, \dots, s_n \in F_{\text{Sym}}$$

$$\Rightarrow f_{\text{allg}} \in K(s_1, \dots, s_n)[X] \subseteq F_{\text{Sym}}[X]$$

$\Rightarrow F$ ist Zerfällungskörper von f_{allg} über $K(s_1, \dots, s_n)$ und über F_{Sym} , insbesondere ist

$$\text{Gal}(f_{\text{allg}} \mid F_{\text{Sym}}) = S_n.$$

$$\Rightarrow [F : K(s_1, \dots, s_n)] \leq (\deg(f_{\text{allg}}))! = n! = \#S_n = [F : F_{\text{Sym}}].$$

Damit folgt $K(s_1, \dots, s_n) = F_{\text{Sym}}$. □

Folgerung 5.6

Für jede endliche Gruppe existiert eine Galoiserweiterung $M \mid L$ mit $\text{Gal}(M \mid L) \cong G$.

Beweis. Nach GEO I.6.9 sei o.E. $G \leq S_n$ für ein n . Dann ist

$$\text{Gal}(F \mid F^G) = G. \quad \square$$

Folgerung 5.7

s_1, \dots, s_n sind algebraisch unabhängig über K , insbesondere $F_{\text{Sym}} \cong K(Y_1, \dots, Y_n)$.

Beweis. Da $F \mid F_{\text{Sym}}$ algebraisch ist, ist $\text{tr. deg}(F \mid F_{\text{Sym}}) = 0$, somit

$$\text{tr. deg}(F_{\text{Sym}} \mid K) = \text{tr. deg}(F \mid K) = n.$$

Aus $F_{\text{Sym}} \mid K(s_1, \dots, s_n)$ algebraisch folgt dann mit Lemma I.5.11 (Satz von Steinitz), dass s_1, \dots, s_n eine Transzendenzbasis von $F_{\text{Sym}} \mid K$ ist. □

► Bemerkung 5.8

Somit hat f_{allg} „variable“ Koeffizienten: für $f = X^n + \sum_{i=1}^n Y_i X^{n-i}$ ist

$$\text{Gal}(f \mid K(Y_1, \dots, Y_n)) \cong S_n$$

mit dem Isomorphismus

$$\begin{cases} K(Y_1, \dots, Y_n) \rightarrow K(s_1, \dots, s_n) = F_{\text{Sym}} \\ g(Y_1, \dots, Y_n) \mapsto g(s_1, \dots, s_n) \end{cases}.$$

Folgerung 5.9

Ist $f \in K(X_1, \dots, X_n)$ symmetrisch, so ist

$$f(X_1, \dots, X_n) = g(s_1(\underline{X}), \dots, s_n(\underline{X}))$$

für ein eindeutig bestimmtes $g \in K(Y_1, \dots, Y_n)$.

Beweis. Existenz: Satz 5.5, Eindeutigkeit: $f = g(s_1, \dots, s_n) = \tilde{g}(s_1, \dots, s_n) \Rightarrow (g - \tilde{g})(s_1, \dots, s_n) = 0$ (da die s_i algebraisch unabhängig sind) $\xRightarrow{5.7} g - \tilde{g} = 0$. □

► Bemerkung 5.10

Vergleiche mit dem Hauptsatz über symmetrische Polynome (GEO II.10.9). Ist $f \in K[X_1, \dots, X_n]$

symmetrisch, so ist

$$f(X_1, \dots, X_n) = g(s_1(\underline{X}), \dots, s_n(\underline{X}))$$

für ein eindeutig bestimmtes $g \in K[Y_1, \dots, Y_n]$.

Definition 5.11

Schreibe $f \in K[X]$ als $f = c \cdot \prod_{i=1}^n (X - \alpha_i)$, $\alpha_1, \dots, \alpha_n$, $c \in K^\times$. Die Diskriminante von f ist

$$\text{discr}(f) = \prod_{i < j} (\alpha_i - \alpha_j)^2$$

► **Bemerkung 5.12**

f separabel $\Leftrightarrow \text{discr}(f) \neq 0$.

■ **Beispiel 5.13**

Für $f = X^2 + bX + c$ ist

$$\text{discr}(f) = (\alpha_1 - \alpha_2)^2 = \alpha_1^2 + \alpha_2^2 - 2\alpha_1\alpha_2 = \alpha_1^2 + 2\alpha_1\alpha_2 + \alpha_2^2 - 4\alpha_1\alpha_2 = b^2 - 4c$$

Satz 5.14

Für $f \in K[X]$ ist $\text{discr}(f) \in K$.

Beweis. O.E. sei f separabel. Sei L der Zerfällungskörper von f , $G = \text{Gal}(L | K)$, $d = \text{discr}(f) \in L$. Für $\sigma \in G$ ist $d^\sigma = d$, da $(\alpha_i - \alpha_j)^2 = (\alpha_j - \alpha_i)^2$, und somit $d \in L^G = K$. \square

Satz 5.15

Es gibt $d_n \in K[Y_1, \dots, Y_n]$ mit $\text{discr}(f) = d_n(a_1, \dots, a_n)$ für jedes

$$f = X^n + \sum_{i=1}^n a_i X^{n-i} \in K[X]$$

Beweis. $D = \prod_{i < j} (X_i - X_j)^2 \in K[X_1, \dots, X_n]$ ist symmetrisch $\xrightarrow{5.10} D(\underline{X}) = d(s(\underline{X}))$ für ein $d \in K[X_1, \dots, X_n]$.

Für $f = \prod_{i=1}^n (X - \alpha_i) = X^n + \sum_{i=1}^n a_i X^{n-i} \in K[X]$ ist

$$d(a_1, \dots, a_n) = d(s_1(\underline{a}), \dots, s_n(\underline{a})) = D(\alpha_1, \dots, \alpha_n) = \text{discr}(f). \quad \square$$

■ **Beispiel 5.16**

Man kann zeigen (Übung): Für $f = X^3 + aX + b$ ist

$$\text{discr}(f) = -4a^3 - 27b.$$

Satz 5.17

Sei $f \in K[X]$ separabel, $\deg(f) = n \geq 2$. Dann gilt

$$\text{Gal}(f \mid K) \leq A_n \quad \Leftrightarrow \quad \text{discr}(f) \in (K^\times)^2$$

Beweis. Sei $f = c \prod_{i=1}^n (X - \alpha_i)$, $c \in K^\times$, $\alpha_i \in \bar{K}$, L der Zerfällungskörper von f über K .
 $\Rightarrow \text{discr}(f) = \delta^2$, $\delta = \prod_{i < j} (\alpha_i - \alpha_j) \in L^\times$ (da f separabel)

Für $\sigma \in \text{Gal}(L \mid K)$ ist

$$\delta^\sigma = \prod_{i < j} (\alpha_i^\sigma - \alpha_j^\sigma) = (-1)^{\#\text{Fehlstände von } \sigma} \delta = \text{sgn}(\delta) \delta.$$

Somit gilt: $\text{discr}(f) \in (K^\times)^2$

$$\Leftrightarrow \delta^\sigma = \delta \quad \forall \sigma \in \text{Gal}(L \mid K)$$

$$\Leftrightarrow \text{sgn}(\delta) = 1 \quad \forall \sigma \in \text{Gal}(L \mid K)$$

$$\Leftrightarrow \text{Gal}(L \mid K) \leq A_n$$

□

■ Beispiel 5.18

$d = \text{discr}(f)$, $G = \text{Gal}(f \mid K) \leq S_n$.

$$n = 2: \quad d \in (K^\times)^2 \Leftrightarrow G = 1 \Leftrightarrow f \text{ reduzibel}$$

$$d \notin (K^\times)^2 \Leftrightarrow G = S_2 \Leftrightarrow f \text{ irreduzibel}$$

$$n = 3: \quad \begin{array}{ccc} G & f \text{ irreduzibel} & f \text{ reduzibel} \\ \hline \end{array}$$

$$d \in (K^\times)^2 \quad = A_3 \quad = 1$$

$$d \notin (K^\times)^2 \quad = S_3 \quad \cong C_2$$

6. Kreisteilungskörper

Sei K ein Körper, $\text{char}(K) = p \geq 0$, $n \in \mathbb{N}$ mit $p \nmid n$.

Definition 6.1

- (1) $\mu_n := \{\zeta \in \bar{K} \mid \zeta^n = 1\} \leq \bar{K}^\times$, die Gruppe der n -ten Einheitswurzeln,
- (2) $\zeta \in \mu_n$ ist eine primitive n -te Einheitswurzel $\Leftrightarrow \text{ord}(\mu_n(\zeta)) = n$,
- (3) $K_n := K(\mu_n)$, der n -te Kreisteilungskörper.

Satz 6.2

$\mu_n \cong C_n$ und für $\zeta \in \bar{K}^\times$ gilt: $\mu_n = \langle \zeta \rangle \Leftrightarrow \zeta$ ist primitive n -te Einheitswurzel

Beweis.

- μ_n zyklisch: Jede endliche Untergruppe der multiplikativen Gruppe eines Körpers ist zyklisch.
- $\#\mu_n = n$: $f = X^n - 1 \in K[X]$ ist separabel, $f' = nX^{n-1} \stackrel{p \nmid n}{\neq} 0 \Rightarrow \text{ggT}(f, f') = 1$ □

Satz 6.3

$K_n \mid K$ ist galoissch und es gibt eine eindeutig bestimmte Einbettung

$$\chi_n: \text{Gal}(K_n \mid K) \hookrightarrow (\mathbb{Z}/n\mathbb{Z})^\times$$

mit

$$\zeta^\sigma = \zeta^{\chi_n(\sigma)} \quad \text{für alle } \zeta \in \mu_n, \sigma \in \text{Gal}(K_n \mid K). \quad (\star)$$

Beweis. K ist Zerfällungskörper des separablen Polynoms $f = X^n - 1 \in K[X]$ und somit ist $K_n \mid K$ endlich galoissch. Fixiere $\zeta_n \in \mu_n$ primitiv. Für ein $\sigma \in \text{Gal}(K_n \mid K)$ ist $\zeta_n^\sigma \in \mu_n$ wieder primitiv. Somit

$$\zeta_n^\sigma = \zeta_n^{\chi_n(\sigma)} \quad \text{für ein } \chi_n(\sigma) \in (\mathbb{Z}/n\mathbb{Z})^\times \text{ (oder teilerfremd zur Gruppenordnung)}$$

- χ_n erfüllt Gleichung (\star) : für $\zeta \in \mu_n$, $\sigma \in \text{Gal}(K_n \mid K)$ ist $\zeta^\sigma = \left(\zeta_n^m\right)^\sigma = \left(\zeta_n^{\chi_n(\sigma)}\right)^m = \zeta^{\chi_n(\sigma)}$
- χ_n ist Homomorphismus: $\zeta_n^{\sigma\tau} = \left(\zeta_n^{\chi_n(\sigma)}\right)^\tau = \zeta_n^{\chi_n(\tau)\chi_n(\sigma)}$
- χ_n ist injektiv: $\chi_n(0) = 1 \Rightarrow \zeta^\chi = \zeta \forall \zeta \in \mu_n$. Da $K_n = K(\zeta : \zeta \in \mu_n)$ folgt $\sigma = \text{id}_{K_n}$. □

Folgerung 6.4

$\text{Gal}(K_n \mid K)$ ist abelsch und $[\text{Gal}(K_n \mid K)] \leq (\mathbb{Z}/n\mathbb{Z})^\times = \Phi(n)$.

Definition 6.5

$\Phi_n := \prod_{\substack{\zeta \in \mu_n \\ \zeta \text{ primitiv}}} (X - \zeta) \in K_n[X]$ ist das n -te Kreisteilungspolynom.

Lemma 6.6

$\Phi_n \in K[X]$ und K_n ist Zerfällungskörper von Φ_n über K .

Beweis. Für $\sigma \in \text{Gal}(K_n | K)$ ist

$$\Phi_n^\sigma = \prod_{\substack{\zeta \in \mu_n \\ \zeta \text{ primitiv}}} (X - \zeta^\sigma) = \prod (X - \zeta) = \Phi_n,$$

somit $\Phi_n \in K^{\text{Gal}(K_n | K)}[X] = K[X]$. \square

► **Bemerkung 6.7**

Für $n = l$ prim ist $\Phi_n = \frac{X^l - 1}{X - 1} = X^{l-1} + X^{l-2} + \dots + X + 1$. Da $X^n - 1 = \prod_{d|n} \Phi_d$, lässt sich daraus Φ_n für ein allgemeines n bestimmen, z.B.

$$\Phi_6 = \frac{X^6 - 1}{\Phi_1 \Phi_2 \Phi_3} = \frac{X^6 - 1}{(X - 1)(X + 1)(X^2 + X + 1)} = X^2 - X + 1$$

Theorem 6.8

Sei $K = \mathbb{Q}$. Dann ist $\Phi_n \in \mathbb{Z}[X]$ irreduzibel.

Beweis. Da Φ_n normiert ist, und $\Phi_n | X^n - 1$ ist $\Phi_n \in \mathbb{Z}[X]$ nach dem Satz von Gauß.

Sei $\zeta \in \mu_n$ primitiv, $f = \text{MinPol}(\zeta | \mathbb{Q})$. Aus $\Phi_n(\zeta) = 0$ folgt, dass $f | \Phi_n$, also $\Phi_n = f \cdot g$, $g \in \mathbb{Q}[X]$. Nach dem Satz von Gauß sind $f, g \in \mathbb{Z}[X]$.

Behauptung: Für $l \nmid n$ prim ist $f(\zeta^l) = 0$.

Beweis. Da ζ^l wieder primitiv ist, ist $\Phi_n(\zeta^l) = 0$. Wäre $f(\zeta^l) \neq 0$, so folge $g(\zeta^l) = 0$. Dann ist ζ Nullstelle von $g(X^l)$, also $f | g(X^l)$ bzw.

$$g(X^l) = f(X) \cdot n(X) \in \mathbb{Z}[X].$$

Reduktion modulo l : $\bar{\cdot}: \mathbb{Z}[X] \rightarrow (\mathbb{Z}/l\mathbb{Z})[X]$.

$$\begin{aligned} \overline{g(X^l)} &= \bar{g}(X^l) = (\bar{g}(X))^l \\ \Rightarrow \bar{g}^l &= \bar{f} \cdot \bar{n} = \bar{f} \cdot \bar{n} \end{aligned}$$

\Rightarrow Jede Nullstelle von \bar{f} in $\bar{\mathbb{F}}_l$ ist Nullstelle von \bar{g}^l , somit auch von \bar{g} , somit eine doppelte Nullstelle von $\bar{f} \cdot \bar{g} = \bar{\Phi}_n$ im Widerspruch zu $\bar{\Phi}_n | X^n - 1$ separabel (in $\bar{\mathbb{F}}_l[X]$). \square

\Rightarrow Für m mit $\text{ggT}(m, n) = 1$ ist $f(\zeta^m) = 0$, d.h. jede Nullstelle von Φ_n ist auch Nullstelle von f

$\Rightarrow \Phi_n = f$ ist irreduzibel. \square

Folgerung 6.9

Ist $\zeta_n \in \mathbb{C}$ eine primitive n -te Einheitswurzel, so ist $\mathbb{Q}(\zeta_n) | \mathbb{Q}$ galoissch mit

$$\text{Gal}(\mathbb{Q}(\zeta_n) | \mathbb{Q}) \cong (\mathbb{Z}/n\mathbb{Z})^\times.$$

Beweis. Satz 6.3, Theorem 6.8, da $\deg(\Phi_n) = \varphi(n) = \#(\mathbb{Z}/n\mathbb{Z})^\times$. \square

7. Zyklische Erweiterungen

Sei $L | K$ eine endliche Galoiserweiterung.

Definition 7.1

$L | K$ ist zyklisch (abelsch, auflösbar) $\Leftrightarrow \text{Gal}(L | K)$ ist zyklisch (bzw. abelsch, auflösbar).

► Bemerkung 7.2 (Erinnerung)

Sei $\text{Hom}_K(L, \bar{K}) = \{\sigma_1, \dots, \sigma_n\}$

- $N_{L|K}(\alpha) = \det(\mu_\alpha) = \prod_{i=1}^n \sigma_i(\alpha)$
- $\text{Tr}_{L|K}(\alpha) = \text{Tr}(\mu_\alpha) = \sum_{i=1}^n \sigma_i(\alpha)$
- $L | K$ galoissch $\implies \text{Hom}_K(L, \bar{K}) = \text{Gal}(L | K)$ (wie üblich nehmen wir hier an, dass $L \subseteq \bar{K}$)

Satz 7.3 (Hilbert 90, multiplikativ)

Sei $L | K$ endlich zyklisch mit $\text{Gal}(L | K) = \langle \sigma \rangle$. Für $b \in L$ gilt:

$$N_{L|K}(b) = 1 \quad \Leftrightarrow \quad b = \frac{a}{\sigma(a)} \text{ für ein } a \in L^\times.$$

Beweis. Sei $n = [L : K]$.

(\Leftarrow) Ist $b = \frac{a}{\sigma(a)}$, so folgt

$$N_{L|K}(b) = \prod_{\sigma \in \text{Gal}(L|K)} \sigma(b) = \prod_{i=0}^{n-1} \sigma^i(b) = \frac{a}{\sigma(a)} \cdot \sigma\left(\frac{a}{\sigma(a)}\right) \cdots \sigma^{n-1}\left(\frac{a}{\sigma(a)}\right) = \frac{a}{\sigma^n(a)} = \frac{a}{a} = 1.$$

(\Rightarrow) Sei $1 = N_{L|K}(b) = \prod_{i=0}^{n-1} \sigma^i(b)$. Nach Theorem 1.8.9 sind $\sigma^0, \dots, \sigma^{n-1}$ linear unabhängig in $\text{Abb}(L^\times, L)$, insbesondere existiert $c \in L$ mit

$$a := \sigma^0(c) + b\sigma^1(c) + b\sigma(b)\sigma^2(c) + \cdots + b\sigma(b) \cdots \sigma^{n-2}(b)\sigma^{n-1}(c) \neq 0$$

Es gilt $b\sigma(a) = a$, da $\sigma^n(c) = \sigma^0(c)$ und $b\sigma(b) \cdots \sigma^{n-1}(b) = N_{L|K}(b) = 1$. Also folgt $b = \frac{a}{\sigma(a)}$. \square

Satz 7.4 (Kummer)

Sei $p = \text{char}(K) \geq 0$ und $n \in \mathbb{N}$ mit $p \nmid n$. Sei $\mu_n \subseteq K$.

- Ist $\alpha \in \bar{K}$ mit $\alpha^n = a \in K$, so ist $K(\alpha) | K$ eine zyklische Galoiserweiterung vom Grad $d | n$.
- Ist $L | K$ zyklisch vom Grad n , so ist $L = K(\alpha)$ mit $\alpha^n \in K$.

Beweis. O.E. $\alpha \neq 0$.

(a) α ist Nullstelle von $f = X^n - a = \prod_{\zeta \in \mu_n} (X - \zeta\alpha)$

$\xrightarrow{\mu_n \subseteq K} K(\alpha) = K(\zeta\alpha : \zeta \in \mu_n)$ ist Zerfällungskörper von f und f ist separabel, also ist $K(\alpha) | K$ galoissch.

Betrachte $\chi: G = \text{Gal}(K(\alpha) | K) \rightarrow \mu_n, \sigma \mapsto \frac{\sigma(\alpha)}{\alpha}$

- χ ist unabhängig von der Wahl von α : $\alpha' = \zeta\alpha$ mit $\zeta \in \mu_n \subseteq K$
 $\implies \frac{\sigma(\alpha')}{\alpha'} = \frac{\sigma(\zeta\alpha)}{\zeta\alpha} = \frac{\zeta \cdot \sigma(\alpha)}{\zeta\alpha} = \frac{\sigma(\alpha)}{\alpha}$

- χ ist Homomorphismus: Für $\sigma, \tau \in G$ ist

$$\chi(\sigma\tau) = \frac{\sigma\tau(\alpha)}{\alpha} = \frac{\sigma\tau(\alpha)}{\tau(\alpha)} \cdot \frac{\tau(\alpha)}{\alpha} = \chi(\sigma) \cdot \chi(\tau)$$

- χ ist injektiv:

$$1 = \chi(\sigma) = \frac{\sigma(\alpha)}{\alpha} \implies \sigma(\alpha) = \alpha \implies \sigma = \text{id}_{K(\alpha)}$$

Haben somit Einbettung

$$G \hookrightarrow \mu_n \cong C_n$$

und damit $G \cong C_d$ für ein $d \mid n$.

(b) Sei $\text{Gal}(L \mid K) = \langle \sigma \rangle$. Dann

- $N_{L|K}(\zeta_n) = \zeta_n^n = 1 \xrightarrow{7.3} \zeta_n = \frac{\alpha}{\sigma(\alpha)}$ für ein $\alpha \in L^\times$
- $\sigma(\alpha^n) = \sigma(\alpha)^n = \left(\frac{\alpha}{\zeta_n}\right)^n = \alpha^n \implies \alpha^n \in L^{\text{Gal}(L|K)} = K$
- $\alpha, \sigma(\alpha) = \zeta_n^{-1}(\alpha), \dots, \sigma^{n-1}(\alpha) = \zeta_n^{-(n-1)}(\alpha)$ sind paarweise verschieden
 $\implies \deg(\alpha \mid K) \geq n \implies L = K(\alpha)$

□

Satz 7.5 (Hilbert 90, additiv)

Sei $L \mid K$ endlich zyklisch mit $\text{Gal}(L \mid K) = \langle \sigma \rangle$. Für $b \in L$ gilt

$$\text{Tr}_{L|K}(b) = 0 \iff b = a - \sigma(a) \text{ für ein } a \in L.$$

Beweis. Sei $n = [L : K]$.

(\Leftarrow) Ist $b = a - \sigma(a)$, so folgt

$$\begin{aligned} \text{Tr}_{L|K}(b) &= \sum_{i=0}^{n-1} \sigma^i(b) \\ &= a - \sigma(a) + \sigma(a - \sigma(a)) + \dots + \sigma^{n-1}(a - \sigma(a)) \\ &= a - \sigma^n(a) = a - a = 0 \end{aligned}$$

(\Rightarrow) Sei $0 = \text{Tr}_{L|K}(b) = \sum_{i=0}^{n-1} \sigma^i(b)$. Nach Folgerung 1.8.10 ist $\text{Tr}_{L|K} \neq 0$, insbesondere existiert $c \in L$ mit $\text{Tr}_{L|K}(c) \neq 0$. Setze

$$a := \text{Tr}_{L|K}(c)^{-1} \left(b\sigma(c) + (b + \sigma(b))\sigma^2(c) + \dots + (b + \sigma(b) + \dots + \sigma^{n-2}(b))\sigma^{n-1}(c) \right),$$

und es folgt

$$\begin{aligned} a - \sigma(a) &= \left(b\sigma(c) + b\sigma^2(c) + \dots + b\sigma^{n-1}(c) - \underbrace{(\sigma(b) + \sigma^2(b) + \dots + \sigma^{n-1}(b))}_{\text{Tr}_{L|K}(b) - b} \underbrace{\sigma^n(c)}_{=c} \right) \cdot \text{Tr}_{L|K}(c)^{-1} \\ &= b \cdot \text{Tr}_{L|K}(c)^{-1} (\sigma(c) + \sigma^2(c) + \dots + \sigma^{n-1}(c) + c) = b. \end{aligned}$$

□

Satz 7.6 (Artin-Schreier)

Sei $p = \text{char}(K) > 0$.

- (a) Ist $\alpha \in \overline{K}$ eine Nullstelle von $f = X^p - X - a \in K[X]$, so ist entweder $\alpha \in K$ oder f ist irreduzibel und $K(\alpha) | K$ ist zyklisch vom Grad p .
- (b) Ist $L | K$ zyklisch vom Grad p , so ist $L = K(\alpha)$ mit $\alpha^p - \alpha = a \in K$.

Beweis.

- (a) α ist Nullstelle von $f = X^p - X - a = \prod_{i=1}^{p-1} (X - (\alpha + i))$
 $\implies K(\alpha) = K(\alpha + i, i = 0, \dots, p-1)$ ist Zerfällungskörper von f und mit f separabel folgt: $K(\alpha) | K$ galoissch.

Betrachte $\chi: G = \text{Gal}(K(\alpha) | K) \rightarrow \mathbb{F}_p, \sigma \mapsto \alpha - \sigma(\alpha)$.

- χ ist unabhängig von der Wahl von α :
 $\alpha' = \alpha + i, i \in \mathbb{F}_p \subseteq K \implies \sigma(\alpha') = \sigma(\alpha) + i$
 $\alpha' - \sigma(\alpha') = \alpha + i - (\sigma(\alpha) + i) = \alpha - \sigma(\alpha)$
- χ ist Hom.:

$$\chi(\sigma\tau) = \alpha - \sigma\tau(\alpha) = \alpha - \tau(\alpha) + \tau(\alpha) - \sigma(\tau(\alpha)) = \chi(\tau) + \chi(\sigma)$$

- χ ist injektiv: $\chi(\sigma) = 0 \implies \sigma(\alpha) = \alpha \implies \sigma = \text{id}_{K(\alpha)}$.

Dies liefert Einbettung $\chi: \text{Gal}(K(\alpha) | K) \hookrightarrow \mathbb{F}_p \cong C_p$, sodass $G \cong C_p$ (f irreduzibel) oder $G = 1$ ($\alpha \in K$).

- (b) Sei $G = \text{Gal}(L | K) = \langle \sigma \rangle$ und $\#G = p$. Einerseits gilt

$$\text{Tr}_{L|K}(-1) = p(-1) = 0 \xrightarrow{7.5} -1 = \alpha - \sigma(\alpha) \text{ für ein } \alpha \in L,$$

andererseits ergibt sich

$$\sigma(\alpha^p - \alpha) = \sigma(\alpha)^p - \sigma(\alpha) = (\alpha + 1)^p - (\alpha + 1) = \alpha^p + 1^p - \alpha - 1 = \alpha^p - \alpha,$$

sodass $a := \alpha^p - \alpha \in L^G = K$.

$\alpha, \sigma(\alpha) = \alpha + 1, \sigma^2(\alpha) = \alpha + 2, \dots, \sigma^{p-1}(\alpha) = \alpha + p - 1$ sind paarweise verschieden und damit folgt $\deg(\alpha | K) \geq p \implies L = K(\alpha)$. \square

Lemma 7.7

Sei $F | K$ eine weitere Körpererweiterung. Dann: Ist $L | K$ zyklisch (abelsch, auflösbar), so auch $LF | F$.

Beweis. $FL | L$ ist galoissch und

$$\text{Gal}(FL | L) \cong \text{Gal}(L | L \cap F) \leq \text{Gal}(L | K)$$

Untergruppen zyklischer (abelscher, auflösbarer) Gruppen sind wieder zyklisch (abelsch, auflösbar). (\nearrow Abschnitt 8). \square

8. Auflösbarkeit von Gleichungen

Anhang

Index

A

abelsch, [54](#)
algebraisch, [6](#), [8](#)
algebraisch abhängig, [18](#)
algebraischen Abschluss, [16](#)
algebraischer Abschluss, [14](#)
auflösbar, [54](#)
Automorphismengruppe, [16](#)

C

Charakteristik, [3](#)

D

Diskriminante, [50](#)

E

einfach, [5](#), [21](#)
endlich erzeugt, [5](#)

F

Fixkörper, [38](#)
formale Ableitung, [21](#)

G

Galoisgruppe, [37](#)
galoissch, [37](#)
Grad, [6](#)

K

konjugiert, [16](#)
Körpererweiterung, [4](#)
Körpergrad, [4](#)
Kreisteilungskörper, [52](#)

M

Minimalpolynom, [6](#)

N

Normal, [35](#)
normale Hülle, [46](#)

P

primitives Element, [33](#)
Primkörper, [3](#)

R

rein separabel, [27](#)
rein transzendent, [18](#)
relative algebraische Abschluss, [9](#)

S

separabel, [21](#), [25](#)
Separabilitätsgrad, [25](#)
symmetrisch, [48](#)

T

Teilkörper, [5](#)
transzendent, [6](#)
Transzendentbasis, [19](#)
Transzendenzgrad, [20](#)

U

Unterring, [5](#)

V

Vielfachheit, [21](#)
vollkommen, [23](#)

W

Wurzelkörper, [10](#)

Z

Zerfällungskörper, [11](#)
zyklisch, [54](#)