Einführung in die Algebra

Vorlesung im
Wintersemester 2006-2007
Technische Universität Berlin

gehalten von
Prof. Dr. M. Pohst

Contents

CHAPTER 3

Körper

Bereits als bekannt werden die folgenden Aussagen vorausgesetzt:

Definition in (2.17): K kommutativer Ring mit 1 und $K^\times = K\backslash\{0\}$.

Charakteristik: Durchschnitt von Körpen ist wieder einer, der kleinste Teilkörper eines Körpers K heißt Primkörper $P(K)$ von K, für $\chi(K) = 0$ gilt $P(K) \cong \mathbb{Q}$, für $\chi(K) = p$ gilt $P(K) \cong \mathbb{Z}/p\mathbb{Z}$ (vgl. (2.21), (2.22)).

(Unter-) Teilkörper, (Ober-) Erweiterungskörper, Zwischenkörper: $K \subseteq L \subseteq M$ (mit $P(K) = P(L) = P(M)$); jeder Erweiterungskörper $L \supseteq K$ von K ist in natürlicher Weise ein K-Vektorraum, besitzt also speziell eine K-Basis B, damit ist die Konstruktion eines charakteristischen Polynoms für algebraische $x \in L$ mittels regulärer Darstellung möglich.

3.1. Definition

Als Grad einer Körpererweiterung L über K definiert man $[L : K] := \dim_K L$. L über K heißt endlich für $[L : K] < \infty$, andernfalls unendlich.

Beispiele:

(1) $[\mathbb{C} : \mathbb{R}] = 2$, $[\mathbb{R} : \mathbb{Q}] = \infty$, $[\mathbb{Q}(\sqrt[3]{2}) : \mathbb{Q}] = 3$ (vergleiche Bemerkung nach (3.2)).
(2) K endlich mit $\chi(K) = p \Rightarrow \sharp K = p^n$ für passendes $n \in \mathbb{N}$.
(3) $[L : K] = 1 \Leftrightarrow K = L$.
(4) Wie in der Ringtheorie unter Irreduzibilität gezeigt, hat das Minimalpolynom von $e^{2\pi i/p} (p \in \mathbb{P})$ über $\mathbb{Q}$ den Grad $p - 1$. Finden Sie den Grad von $\mathbb{Q}(e^{2\pi i/5})$ über $\mathbb{Q}$.

3.2. Satz (Gradsatz)

Es seien K, L, M drei Körper mit $K \subseteq L \subseteq M$. Dann gilt die Gradformel

$$[M : K] = [M : L]\,[L : K].$$

Beweis:
Ist $\{\alpha_i\}_{i\in I}$ eine Basis von M über L und $\{\beta_j\}_{j\in J}$ eine Basis von L über K, so ist $\{\alpha_i\beta_j\}_{i\in I,j\in J}$ eine Basis von M über K (vergleiche Übungen).

□

Bemerkung:
Ist L eine Zwischenkörper der endlichen Körpererweiterung M über K, so teilen $[L:K]$ und $[M:L]$ beide $[M:K]$. Ist speziell $[M:K]$ Primzahl, so folgt $L=K$ oder $L=M$.

3.3. Definition

Es seien L über K eine Körpererweiterung und A eine nicht leere Teilmenge von L. Dann bezeichnet $K(A)$ den kleinsten Teilkörper von L, der K und A enthält. (Schreibweise: $K(a)$ statt $K(\{a\})$.)

3.4. Hilfssatz

Es seien $K\subseteq L$ zwei Körper und $\emptyset\neq A\subseteq L$. Dann gilt:

$$K(A) = \left\{\tfrac{f(u_1,\ldots,u_r)}{g(u_1,\ldots,u_r)}\in L\,\middle|\, f,g\in K[t_1,\ldots,t_r], u_i\in A\ (1\leq i\leq r), r\in\mathbb{N}, g(u_1,\ldots,u_r)\neq 0\right\}.$$

Bemerkung:
Analog definiert man $K[A]$ als kleinsten Ring in L, der sowohl K als auch A enthält. $K[A]$ ist diejenige Teilmenge von $K(A)$, bei der stets $g\cong 1$ gewählt wird. Etwa: $K(t)=\mathfrak{Q}(K[t])$.

Beweis:
$K(A)$ ist in jedem Teilkörper M mit $K\subseteq M\subseteq L$ enthalten, der K und A umfasst. Ferner ist $K(A)$ selbst Körper.

□

3.5. Hilfssatz

Es sei K ein Körper, I ein Integritätsring mit $I\supseteq K$. Ist dann I ein endlich dimensionaler K-Vektorraum, so ist I bereits ein Körper.

Beweis: Übungen.

Bemerkung:
Besitzt $K[A]$ über K endliche Dimension, so gilt $K[A]=K(A)$. (Beachte: $A\subseteq L$, L Oberkörper von K.)

Die Definition von algebraischen und transzendenten Elementen erfolgte in (2.53).

3.6. Definition

Eine Körpererweiterung L über K (Schreibweise: L/K) heißt algebraisch (L algebraisch über K), falls jedes $x \in L$ algebraisch über K ist. Andernfalls heißt L/K transzendent.

3.7. Hilfssatz

Ist x über dem Körper K transzendent, so gilt:

(1) $(K(x) : K) = \infty$,
(2) x^k ($k \in \mathbb{N}$) ist transzendent über K mit $K(x^k) \subset K(x^l)$ für $l|k$, $l < k$, $l \in \mathbb{N}$.

Beweis:

(1) Die Potenzen x^k ($k \in \mathbb{Z}^{\geq 0}$) sind linear unabhängig über K.
(2) x^k transzendent folgt direkt aus (i); für $k = ml$ ($m \in \mathbb{Z}^{\geq 2}$) gilt offenbar $x^k = (x^l)^m$, also $K(x^k) \subseteq K(x^l)$. Bei Gleichheit existieren f, $g \in K[t]$ mit $g(x^k) \neq 0$ und

$$x^l = f(x^k)/g(x^k) \quad \Leftrightarrow \quad g(x^k)\, x^l = f(x^k).$$

"Gradvergleich (in x)" liefert

$$\begin{aligned} \deg\left(g(x^k)\, x^l\right) &\equiv l \bmod k, \\ \deg\left(f(x^k)\right) &\equiv 0 \bmod k. \end{aligned}$$

Widerspruch!

□

Bemerkung:

(1) Ist x über K transzendent, so besitzt $K(x)$ über K unendlich viele Zwischenkörper.
(2) Jede endliche Erweiterung L/K ist algebraisch.

3.8. Definition

Eine Erweiterung L/K heißt endlich erzeugbar, falls in L Elemente $\alpha_1, \ldots, \alpha_r$ existieren mit $L = K(\alpha_1, \ldots, \alpha_r)$. L/K heißt einfach, falls $L = K(\alpha)$ mit $\alpha \in L$ gilt. In diesem Fall heißt α primitiv.

Beispiele:
$\mathbb{C}/\mathbb{R}$ ist einfach mit primitivem Element i,
$K(t)/K$ ist einfach mit primitivem Element t,
$L = K(\alpha) \Rightarrow$ mit α ist auch $k\alpha$ primitives Element für alle $k \in K \setminus \{0\}$.
Einfache transzendente Erweiterungskörper über K sind isomorph zu $K(t)$.

3.9. Hilfssatz

(1) Jede endliche Untergruppe G von $K^\times$ ist zyklisch.
(2) Jede endliche Erweiterung L/K ist endlich erzeugbar.
(3) Jede endliche Erweiterung L/K mit $\sharp K < \infty$ ist einfach.

Beweis:

(1) Es sei $|G| = n$ und m minimaler Exponent für alle $x \in G$. Hierzu existiert $a \in G$ mit $\mathrm{ord}(a) = m$ (Übungen). Wegen $m|n$ folgt $m \leq n$. Alle $x \in G$ sind Nullstellen von $t^m - 1 \Rightarrow m \geq n$. Also gilt $m = n,\ G =< a >$.
(2) Ist etwa $w_1, \ldots, w_r$ eine K-Basis von L, so gilt $L = K(w_1, \ldots, w_r)$.
(3) L und K besitzen beide die gleiche Charakteristik p.
Gemäß (i) ist $L^\times$ zyklisch mit $L^\times =< x >$. Offenbar ist dann $L = K(x)$.

□

Ist x algebraisch über K, so bilden alle Polynome $f \in K[t]$ mit $f(x) = 0$ ein Ideal $\mathfrak{a}$ in $K[t]$. Dieses ist dann Hauptideal, wird also von einem Element m erzeugt, welches o.B.d.A. als normiert angenommen wird. Dann ist m irreduzibel und teilt alle $f \in \mathfrak{a}$. Ist andererseits $f \in \mathfrak{a}$ normiert und irreduzibel, so gilt $f = m$.

3.10. Definition

Ist α algebraisch über K, so heißt das normierte irreduzible Polynom $m_\alpha(t) \in K[t]$ mit $m_\alpha(\alpha) = 0$ Minimalpolynom von α über K.

Beispiele:

(1) $\alpha = i \Rightarrow m_\alpha(t) = t^2 + 1$ über $\mathbb{Q}$, $\mathbb{R}$;
$\alpha = \sqrt{2} \Rightarrow m_\alpha(t) = t^2 - 2$ über $\mathbb{Q}$ bzw. $m_\alpha(t) = t - \sqrt{2}$ über $\mathbb{R}$, $\mathbb{Q}(\sqrt{2})$.
(2) $\alpha = e^{2\pi i/p},\ p \in \mathbb{P} \Rightarrow m_\alpha(t) = \sum_{i=0}^{p-1} t^i$ über $\mathbb{Q}$.

3.11. Hilfssatz

Es sei α algebraisch über K. Dann gilt:

(1) $K(\alpha) = K[\alpha] \cong K[t]/m_\alpha(t)\,K[t]$,
(2) $[K(\alpha) : K] = \deg(m_\alpha)$,
(3) $1, \alpha, \ldots, \alpha^{\deg(m_\alpha)-1}$ ist eine K-Basis von $K(\alpha)$.

Beweis:

Der Einsetzungshomomorphismus $K[t] \to K[\alpha] : f(t) \mapsto f(\alpha)$ ist hier surjektiv, gemäß (2.14)(i) gilt also

$$K[\alpha] \cong K[t]/(m_\alpha).$$

Da $K[t]/(m_\alpha)$ Körper ist (m_α irreduzibel $\Rightarrow$ (m_α) maximal), ist auch $K[\alpha]$ Körper, also gilt $K[\alpha] = K(\alpha)$. Teil (ii) und (iii) folgen dann daraus, daß $1, x, \ldots, x^{\deg(m_\alpha)-1}$ für $x = t/(m_\alpha)$ eine Basis von $K[t]/(m_\alpha)$ bilden, und bei besagtem Isomorphismus wird α auf x abgebildet.

Konstruktiver Aspekt: Ist $\frac{f(\alpha)}{g(\alpha)} \in K(\alpha)$, so ist $g(\alpha) \neq 0$ und damit $g(t)$ in $K[t]$ zu $m_\alpha(t)$ teilerfremd. Mit dem Euklidischen Algorithmus konstruiert man u, $v \in K[t]$ mit $1 = ug + vm_\alpha$ und erhält $1 = u(\alpha)\, g(\alpha)$ oder $1/g(\alpha) = u(\alpha) \in K[\alpha]$.

□

Aufgabe:
Wie sieht $K[\alpha]$ aus, falls $f(\alpha) = 0$ mit reduziblem Polynom f ist?

Bemerkung:
$[K(\alpha) : K] < \infty \;\Leftrightarrow\; \alpha$ algebraisch über K.

3.12. Hilfssatz

Eine Körpererweiterung L/K ist genau dann endlich, wenn $L = K(\alpha_1, \ldots, \alpha_r)$ mit über K algebraischen Elementen α_i ($1 \leq i \leq r$; $r \in \mathbb{N}$) ist.

Beweis:
"$\Rightarrow$" Es ist $L = Kw_1 + \ldots + Kw_r = K(w_1, \ldots, w_r)$ für jede K-Basis $w_1, \ldots, w_r$ von L. Hierbei sind dann alle w_i über K algebraisch gemäß der voranstehenden Bemerkung.

"$\Leftarrow$" Wegen $K(\alpha_1, \ldots, \alpha_i) = K(\alpha_1, \ldots, \alpha_{i-1})\,(\alpha_i)$ und (3.11), (3.2) folgt die Behauptung:

$$[L : K] = \prod_{i=1}^{r} [K(\alpha_1, \ldots, \alpha_i) : K(\alpha_1, \ldots, \alpha_{i-1})].$$

□

3.13. Hilfssatz

Sind $K \subseteq L \subseteq M$ drei Körper und M/L sowie L/K algebraisch, so ist auch M/K algebraisch.

Beweis:
Es sei $\alpha \in M$ algebraisch über L mit Minimalpolynom

$$m_\alpha(t) = t^n + a_1 t^{n-1} + \ldots + a_n \;\in L[t].$$

Hierbei sind $a_1, \ldots, a_n \in L$ algebraisch über K. Also ist $K_1 := K(a_1, \ldots, a_n)$ eine endliche Erweiterung von K gemäß (3.12), und α ist algebraisch über K_1. Also ist $K(a_1, \ldots, a_n, \alpha)$ endliche Erweiterung von K und folglich α algebraisch über K.

□

3.14. Korollar

Es sei L/K eine Körpererweiterung und $A(L)$ die Menge aller über K algebraischen Elemente aus L. Dann ist $A(L)$ ein algebraischer Erweiterungskörper von K.

Beweis:
Es bleibt "$A(L)$ ist Körper" zu zeigen. Sind aber $a, b \in A(L)$, so ist $K(a,b)$ algebraisch über K, also gilt $K(a,b) \subseteq A(L)$, d.h. $a \pm b$, ab, $ab^{-1} = \frac{a}{b}$ (für $b \neq 0$) sind über K algebraisch (gehören zu L), damit gehören sie auch zu $A(L)$.

□

Kennzeichnung einfacher algebraischer Erweiterungen:

3.15. Satz

Eine Körpererweiterung L/K ist genau dann einfach algebraisch, wenn es zwischen K und L nur endlich viele Zwischenkörper gibt.

Beweis:

(1) Es sei $L = K(\alpha)$. Wir zeigen, daß es eine surjektive Abbildung auf die Zwischenkörper von L/K von den Teilern des Minimalpolynoms $m_\alpha = m_{\alpha/K}$ (in $L[t]$) gibt. Ist etwa K_1 ein Zwischenkörper von L/K, so ist das Minimalpolynom m_{α/K_1} (von α über K_1) ein Teiler von $m_{\alpha/K}$ in $L[t]$. Sind $a_1, \ldots, a_m$ (über K algebraisch) die Koeffizienten von $m_{\alpha/K_1} \in K_1[t]$, so gilt $\tilde{K_1} := K(a_1, \ldots, a_m) \subseteq K_1 \subset L$ und

$$[K_1 : \tilde{K_1}] = [L : \tilde{K_1}]/[L : K_1] = 1 \quad ([L : K_1] = [L : \tilde{K_1}] = m)$$

(wegen (3.11)(ii)), und damit gilt: $K_1 = \tilde{K_1}$. Da $L[t]$ euklidischer Ring und folglich ZPE-Ring ist, besitzt $m_{\alpha/K}$ in $L[t]$ nur endlich viele Teiler. Also können für L/K nur endlich viele Zwischenkörper existieren.

(2) L/K muß algebraisch sein gemäß (3.7) und daran anschließende Bemerkung. Ferner ist L über K endlich erzeugbar, da man sonst eine nicht abbrechende Kette

$$K \subset K(\alpha_1) \subset K(\alpha_1, \alpha_2) \subset \ldots$$

erhielte. Wir können also $L = K(\alpha_1, \ldots, \alpha_r)$ mit über K algebraischen α_i $(1 \leq i \leq r)$ annehmen. Ferner sei r hierin minimal gewählt. Nach (3.12) ist dann speziell $[L : K] < \infty$ und die Behauptung für $\sharp K < \infty$ bereits wegen (3.9)(iii) bewiesen. Also sei $\sharp K = \infty$ und $r \geq 2$. Für $x \in K$ betrachten wir die Erweiterungskörper $K_x := K(\alpha_1 + x\alpha_2)$. Diese können nach Voraussetzung nicht alle verschieden sein; es existieren folglich $y, z \in K$, $y \neq z$, mit $K_y = K_z$. Dafür gilt speziell:

$$\alpha_1 + y\alpha_2 \in K_z, \text{ d.h. } \alpha_1 + y\alpha_2 - (\alpha_1 + z\alpha_2) \in K_z$$

und damit $\alpha_2 \in K_z,\ \alpha_1 = (\alpha_1 + y\alpha_2) - y\alpha_2 \in K_z$. Also ist

$$K_z \subseteq K(\alpha_1, \alpha_2) \subseteq K_z \quad \text{und} \quad K(\alpha_1, \ldots, \alpha_r) = K(\alpha_1 + z\alpha_2, \alpha_3, \ldots, \alpha_r)$$

im Widerspruch zur minimalen Wahl von r.

□

In (2.66) haben wir gezeigt, dass zu einem Körper K und einem Polynom $f \in K[t]$ mit $\deg(f) > 0$ stets ein Erweiterungskörper L von K existiert, über dem L in Linearfaktoren zerfällt.

3.16. Definition

Es sei K ein Körper und $f \in K[t]$ mit $\deg(f) > 0$. Ein Erweiterungskörper L von K heißt Zerfällungskörper von f, falls

$$f(t) = l(f) \prod_{i=1}^{\deg(f)} (t - x_i) \text{ in } L[t]$$

gilt und $L = K(x_1, \ldots, x_{\deg(f)})$ ist.

Bemerkung:
Die Bedingung $L = K(x_1, \ldots, x_{\deg(f)})$ bedeutet, dass es keinen echten Teilkörper von L gibt, über dem f in Linearfaktoren zerfällt. (L entsteht durch Adjunktion aller Wurzeln von f zu K.) Die Wurzeln brauchen i.a. nicht verschieden zu sein.

Beispiele:

(1) $\mathbb{C}$ ist Zerfällungskörper von $t^2+1 \in \mathbb{R}[t]$, ebenso $\mathbb{R}[t]/(t^2+1)$. $\mathbb{Q}(i)$ ist Zerfällungskörper von $t^2 + 1 \in \mathbb{Q}[t]$.

(2) Ist $K \subset L \subset M$ und M Zerfällungskörper von $f \in K[t]$, so ist M auch Zerfällungskörper von $f \in L[t]$.

(3) Es sei $f(t) = t^4 + t^2 + 1 = (t^2 + t + 1)(t^2 - t + 1) \in \mathbb{Q}[t]$. Dies hat in $\mathbb{C}$ die Wurzeln $\xi = \dfrac{-1 + \sqrt{-3}}{2},\ \xi^2,\ -\xi,\ -\xi^2$.
Also ist $L = \mathbb{Q}(\xi)$ Zerfällungskörper von f über $\mathbb{Q}$ mit $[L : \mathbb{Q}] = 2$, und es gilt $m_{\xi/\mathbb{Q}}(t) = t^2 + t + 1$.

(4) $t^3 - 2 \in \mathbb{Q}[t]$ hat Wurzeln $\sqrt[3]{2},\ \sqrt[3]{2}\ \underbrace{e^{\frac{2\pi i}{3}}}_{= \frac{-1+\sqrt{-3}}{2}},\ \sqrt[3]{2}\ \underbrace{e^{\frac{4\pi i}{3}}}_{= \frac{-1-\sqrt{-3}}{2}}$.
Über $\mathbb{Q}(\sqrt[3]{2})$ gilt

$$(t^3 - 2) : (t - \sqrt[3]{2}) = t^2 + \sqrt[3]{2}t + \sqrt[3]{4}.$$

Die Diskriminante des Quotientenpolynoms ist

$$\sqrt[3]{4} - 4\sqrt[3]{4} = -3\sqrt[3]{4} < 0.$$

Die beiden übrigen Nullstellen von $t^3 - 2$:

$$-\frac{\sqrt[3]{2}}{2} \pm \sqrt{\frac{-3\sqrt[3]{4}}{4}} = \sqrt[3]{2}\left(\frac{-1 \pm \sqrt{-3}}{2}\right)$$

sind demnach komplex.

$\mathbb{Q}(\sqrt[3]{2})$ ist kein Zerfällungskörper von $t^3 - 2 \in \mathbb{Q}[t]$, wohl aber

$$\mathbb{Q}\left(\sqrt[3]{2},\ \sqrt[3]{2}\,\frac{-1+\sqrt{-3}}{2},\ \sqrt[3]{2}\,\frac{-1-\sqrt{-3}}{2}\right) = \mathbb{Q}\left(\sqrt[3]{2},\ \frac{1+\sqrt{-3}}{2}\right).$$

(5) $\mathbb{Q}(\sqrt{m})$ ist Zerfällungskörper von $t^2 - m \in \mathbb{Q}[t]$.

Bemerkung:
Der Beweis zu (2.66) lehrt, dass für einen Zerfällungskörper L von $f \in K[t]$ stets $[L : K] \leq \deg(f)!$ gilt. Hierbei kann $<$ gelten, vergleiche Übungen.

Wir zeigen im folgenden, daß Zerfällungskörper bis auf Isomorphie eindeutig bestimmt sind.

3.17. Hilfssatz

Es seien K, K' zwei Körper und $\varphi : K \to K'$ ein Isomorphismus. Dieser lässt sich kanonisch zu einem Isomorphismus von $K[t]$ auf $K'[t]$ fortsetzen, den wir wiederum mit φ bezeichnen. (vgl. Reduktionssatz im Kapitel Ringe). Ferner sei $f \in K[t]$ irreduzibel und $f' := \varphi(f)$. Sind dann α, α' Wurzeln von f bzw. f' in Erweiterungskörpern L bzw. L', so läßt sich φ fortsetzen zu einem Isomorphismus

$$\Phi : K(\alpha) \to K'(\alpha') : \sum_{i=0}^{r} k_i\,\alpha^i \mapsto \sum_{i=0}^{r} \varphi(k_i)\,\alpha'^i.$$

Bemerkung: Es ist $K(\alpha) = K[\alpha],\ K'(\alpha') = K'[\alpha']$.

Beweis:

Φ ist offensichtlich surjektiv. Φ ist wohldefiniert und injektiv wegen

$$\begin{aligned}
\sum_{i=0}^{n} k_i\alpha^i = \sum_{j=0}^{n} l_j\alpha^j \quad &\Leftrightarrow \quad \sum_{i=0}^{n}(k_i - l_i)\,\alpha^i = 0 \\
&\overset{\text{f irred.}}{\Leftrightarrow} \quad f(t) \left| \sum_{i=0}^{n}(k_i - l_i)\,t^i \right. \\
&\overset{\tilde{\varphi}\,\text{Isom.}}{\Leftrightarrow} \quad \varphi\, f(t) \left| \sum_{i=0}^{n} \varphi\,(k_i - l_i)\,t^i \right. \\
&\overset{\tilde{\varphi}\text{f irred.}}{\Leftrightarrow} \quad \sum_{i=0}^{n} \varphi\,(k_i - l_i)\,\alpha'^i = 0 \\
&\Leftrightarrow \quad \sum_{i=0}^{n} \varphi\,(k_i)\,\alpha'^i = \sum_{j=0}^{n} \varphi\,(l_j)\,\alpha'^j .
\end{aligned}$$

Φ ist zudem Homomorphismus, wie man leicht durch Nachrechnen erhält, da $\tilde{\varphi}$ Homomorphismus ist.

□

3.18. Korollar

Es seien $f \in K[t]$ irreduzibel und α, β Nullstellen von f in einem Erweiterungskörper L von K. Dann existiert ein K-Isomorphismus $K(\alpha) \to K(\beta)$ mittels $\alpha \mapsto \beta$ und $k \mapsto k\ \forall k \in K$.

Beweis: Wende (3.17) an mit $\varphi = \mathrm{id}_K,\ \alpha' = \beta$.

□

3.19. Satz

Es seien $\varphi : K \to K'$ ein Körperisomorphismus und $f \in K[t]$ mit $\deg(f) \geq 1$. Ist dann L ein Zerfällungskörper von f über K, L' ein Zerfällungskörper von $f' = \varphi(f)$ über K', so läßt sich φ zu einem Isomorphismus Φ von L auf L' fortsetzen.

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

$n = 1$: $\Phi = \varphi$ tut's wegen $L = K,\ L' = K'$.

$n - 1 \Rightarrow n$:

Es sei g ein irreduzibler Faktor von f in $K[t]$ mit $\deg(f) \geq 2$. Dann ist $g' := \varphi(g)$ irreduzibler Faktor von $f' = \varphi(f)$ in $K'[t]$. Ist L Zerfällungskörper von f über K, so besitzt g eine Wurzel α in L; das gleiche gilt für $\varphi(g)$ (mit $\alpha' \in L'$). Gemäß (3.17) existiert ein Isomorphismus Φ_1 von $K(\alpha)$ auf $K'(\alpha')$ mit $\Phi_1|_K = \varphi$ und $\Phi_1(\alpha) = \alpha'$.

Nach Induktionsvoraussetzung läßt sich daher Φ_1 wegen

$$[L : K(\alpha)] = \frac{[L : K]}{[K(\alpha) : K]} = \frac{n}{\deg(g)} < n$$

zu einem Homomorphismus Φ von L auf L' fortsetzen. (Falls kein solches g existiert, ist $L = K$ und die Beh. trivial.)

□

3.20. Korollar

Es sei $f \in K[t]$ mit $\deg(f) \geq 1$. Sind dann L, L' zwei Zerfällungskörper von f über K, so sind sie K-isomorph.

3.21. Definition

Es sei $f \in K[t]$ mit $\deg(f) \geq 1$. Ist dann α eine Wurzel von f (in einem Erweiterungskörper L von K), so heißt $k := k(\alpha)$ die Vielfachheit von α, falls $(t-\alpha)^k \mid f(t)$ in $L[t]$ und $(t-\alpha)^{k+1} \nmid f(t)$ in $L[t]$ gilt.

Bemerkungen:

(1) $f \in K[t]$ mit $\deg(f) \geq 1$ besitzt genau dann mehrfache Wurzeln (in einem Erweiterungskörper L), wenn $\gcd(f, f')$ positiven Grad besitzt.

Beweis:

"$\Rightarrow$" klar,

"$\Leftarrow$" Es sei $h(t) \in K[t]$ mit $\deg(h) > 0$ und $h \mid f$, $h \mid f'$ gegeben. Ferner sei α Nullstelle von h in einem Erweiterungskörper L/K.

Dann ist $f(t) = (t-\alpha) f_1(t)$ in $L[t]$ sowie $f'(t) = f_1(t) + (t-\alpha) f_1'(t)$.

Wegen $f'(\alpha) = 0$ folgt $f_1(\alpha) = 0$, d.h. $(t-\alpha) \mid f_1(t)$, also $f(t) = (t-\alpha)^2 \left(\frac{f_1(t)}{(t-\alpha)}\right)$ in $L[t]$.

(2) Ist $\chi(k) = p$ und $f \in k[t]$ irreduzibel mit mehrfachen Wurzeln, so gilt $f(t) = g(t^p)$ mit $g \in K[t]$.

Beweis:

Wegen $\gcd(f, f') \neq 1$ muß notwendig $\gcd(f, f') = f$ gelten, also wegen $\deg(f') < \deg(f)$ dann $f' = 0$ sein.

Für $f(t) = \sum_{i=0}^{n} a_i t^i$ bedingt dies $i a_i = 0 \;\; (0 \leq i \leq n)$, d.h. $a_i \neq 0$ höchstens für $p \mid i$.

Also gilt $f(t) = \sum_{i=0}^{\lfloor n/p \rfloor} a_{ip} (t^p)^i =: g(t^p)$.

□

(3) $\chi(K) = 0$, $f \in K[t]$ irreduzibel $\Rightarrow$ f besitzt nur einfache Nullstellen.

Zur Erinnerung an endliche Körper K

(a) $\chi(K)$ ist eine Primzahl p;
(b) K enthält $q = p^n$ Elemente ($n \in \mathbb{N}$), Bezeichnung $\mathbb{F}_q$;
(c) $\mathbb{F}_q^\times$ ist zyklisch von der Ordnung $q-1$,
$a^{q-1} = 1 \quad \forall\, a \in \mathbb{F}_q^\times \quad \Rightarrow a^q = a \quad \forall\, a \in \mathbb{F}_q$;
ist $\mathbb{F}_q^\times =< \xi >$, so gilt speziell $\mathbb{F}_q = \mathbb{F}_p(\xi) = \mathbb{F}_p[\xi]$.

Im folgenden seien stets p eine Primzahl, $n \in \mathbb{N}$, $q = p^n$.

3.22. Satz

(1) Der Zerfällungskörper von $t^q - t \in \mathbb{F}_p[t]$ besitzt p^n Elemente.
(2) Ist K ein Körper mit p^n Elementen, so ist K Zerfällungskörper von $t^q - t \in P(K)[t]$.
(3) Je zwei Körper mit p^n Elementen sind isomorph.

Beweis:

(1) Es sei L Zerfällungskörper von $t^q - t \in \mathbb{F}_p[t]$. Dieser enthält alle Wurzeln von $t^q - t$. Wir zeigen, daß L gerade aus allen solchen Wurzeln besteht. Zunächst gilt für $x \in \mathbb{F}_p$ stets $x^p = x$ und damit $x^{p\nu} = x \quad \forall \nu \in \mathbb{N}$, also $x^{p^n} = x$. Sind ferner x, y Wurzeln des besagten Polynoms, so gilt:

$$(x \pm y)^p = x^p \pm y^p, \text{ also } (x \pm y)^q = x \pm y; \; (xy^{-1})^p = x^p (y^{-1})^p, \text{ also } (xy^{-1})^q = xy^{-1}.$$

Also bilden die Wurzeln einen Teilkörper von L, der $\mathbb{F}_p$ enthält. Dieser muß folglich gleich L sein.

Besagtes Polynom besitzt aber in seinem Zerfällungskörper $q = p^n$ Wurzeln, die alle verschieden sind, da ja $\gcd(t^q - t,\, qt^{q-1} - 1) = \gcd(t^q - t,\, -1) = 1$ ist.

(2) Für $x \in \mathbb{F}_q$ gilt $x^q = x$, also ist x Nullstelle von $t^q - t \in \mathbb{F}_p[t]$. Besagtes Polynom zerfällt also in $\mathbb{F}_q$ in Linearfaktoren. $\mathbb{F}_q$ ist also der kleinste Erweiterungskörper, der alle Nullstellen des Polynoms enthält.
(3) Per (3.19), da die Primkörper jeweils isomorph zu $\mathbb{Z}/p\mathbb{Z}$ sind.

□

3.23. Satz

In $\mathbb{F}_q$ gibt es zu jedem Teiler m von n genau einen Unterkörper mit p^m Elementen, und alle Teilkörper von $\mathbb{F}_q$ sind von dieser Gestalt.

Beweis:

(1) Ist K ein Teilkörper von $\mathbb{F}_q$, so ist $[K : \mathbb{F}_p]$ Teiler von $[\mathbb{F}_q : \mathbb{F}_p] = n$. Also gilt $\#K = p^m$ mit $m \,|\, n$. K besteht dann

aus allen Elementen $y \in \mathbb{F}_q$ mit $y^{p^m} = y$ und ist hierdurch eindeutig bestimmt.

(2) Für $m \mid n$ folgt $(t^{p^m} - t) \mid (t^{p^n} - t)$, und die Wurzeln von $t^{p^m} - t$ (aus $\mathbb{F}_q$) bilden einen Unterkörper von $\mathbb{F}_q$ mit p^m Elementen.

□

Um irreduzible Polynome kleinen Grades über $\mathbb{F}_q$ zu bestimmen, lässt sich folgender Satz benutzen.

3.24. Satz

Über $\mathbb{F}_q$ ist $t^{q^m} - t$ das Produkt aller normierten irreduziblen Polynome aus $\mathbb{F}_q[t]$, deren Grad m teilt.

Beweis

(1) Es sei $f(t) \in \mathbb{F}_q[t]$ normiert, irreduzibel und vom Grad $d|m$. In einem Erweiterungskörper vom Grad d hat f eine Nullstelle α. Sie erfüllt dann $\alpha^{q^d} - \alpha = 0$ und ist wegen $d|m$ auch Nullstelle von $t^{q^m} - t$ (!). Hiernach ist $\gcd(f(t), t^{q^m} - t)$ in $\mathbb{F}_q[t]$ nicht konstant. Da $f(t)$ irreduzibel ist, muss jener gcd folglich mit $f(t)$ übereinstimmen und $f(t)$ daher $t^{q^m} - t$ teilen.

(2) Es sei $f(t) \in \mathbb{F}_q[t]$ ein normierter irreduzibler Teiler von $t^{q^m} - t$ vom Grad d. In einem Erweiterungskörper $\mathbb{F}_{q^d}$ hat dann f eine Nullstelle α. Wegen $f(t)|(t^{q^m} - t)$ ist $\mathbb{F}_{q^d}$ Teilkörper von $\mathbb{F}_{q^m}$, und wir erhalten mit dem Gradsatz:

$$m = [\mathbb{F}_{q^m} : \mathbb{F}_q] = [\mathbb{F}_{q^m} : \mathbb{F}_{q^d}][\mathbb{F}_{q^d} : \mathbb{F}_q] = [\mathbb{F}_{q^m} : \mathbb{F}_{q^d}]\, d,$$

also $d|m$.

(3) Wegen $\gcd(t^{q^m} - t, (t^{q^m} - t)') = \gcd(t^{q^m} - t, q^m t^{q^m - 1} - 1) = \gcd(t^{q^m} - t, -1) = 1$ besitzt $t^{q^m} - t$ keine mehrfachen Teiler.

□

Wir benutzen dieses Resultat, um alle normierten ireduziblen Polynome von Grad ≤ 4 über $\mathbb{F}_2$ zu erhalten.

d	1	2	3	4
$f(t)$	$t, t+1$	t^2+t+1	t^3+t+1, t^3+t^2+1	t^4+t+1 t^4+t^3+1 $t^4+t^3+t^2+t+1.$

Außerdem ist es damit einfach zu zeigen, daß über $\mathbb{F}_q$ zu vorgegebenem Grad d stets normierte irreduzible Polynome vom Grad d existieren.

3.25. Definition

(Möbius Funktion) Wir setzen

$$\mu : \mathbb{N} \longrightarrow \{0,1,-1\} : n \mapsto \begin{cases} 1 & \text{für} \quad n = 1 \\ (-1)^r & \text{für} \quad n = p_1 \cdots p_r \ (p_i \in \mathbb{P}). \\ 0 & \text{falls} \quad p \in \mathbb{P} \text{ mit } p^2 | n \text{ existiert.} \end{cases}$$

3.26. Hilfssatz

Für $n \in \mathbb{N}$ gilt

$$\sum_{d|n} \mu(d) = \begin{cases} 1 & \text{für } n = 1 \\ 0 & \text{sonst.} \end{cases}$$

Beweis Es sei $n = p_1^{m_1} \cdots p_r^{m_r}$. Dann wird

$$\begin{aligned} \sum_{d|n} \mu(d) &= \mu(1) + \sum_{i=1}^{n} \mu(p_i) + \sum_{1 \le i < j \le r} \mu(p_i p_j) + \ldots \\ &= \binom{r}{0} 1 + \binom{r}{1} (-1) + \binom{r}{2} 1 + \ldots \\ &= (1-1)^r. \qquad \square \end{aligned}$$

3.27. Satz

(Möbuissche Umkehrformeln) Es seien $f,\ g : \mathbb{N} \longrightarrow R$, R kommutativer Ring. Dann gilt:

$$\sum_{d|n} f(d) = g(n) \ \forall n \in \mathbb{N} \Longleftrightarrow \sum_{d|n} \mu(d) g\left(\frac{n}{d}\right) = f(n) \ \forall n \in \mathbb{N}.$$

Beweis

Wir haben

$$\begin{aligned} \sum_{d|n} \mu(d) g\left(\tfrac{n}{d}\right) &= \sum_{d\,\tilde{d} = n} \mu(d) g(\tilde{d}) \\ &= \sum_{d\,\tilde{d} = n} \mu(d) \sum_{d_3 | \tilde{d}} f(d_3) \\ &= \sum_{d_3 | n} f(d_3) \sum_{d_4 | \frac{n}{d_3}} \mu(d_1) \\ &= f(n), \end{aligned}$$

und andererseits

$$\begin{aligned} \sum_{d|n} f(d) &= \sum_{d_1\,d_2\,d_3 = n} \sum_{d_2} \mu(d_2) g(d_3) \\ &= \sum_{d_3 | n} g(d_3) \sum_{d_2 | \frac{n}{d_3}} \mu(d_2) \\ &= g(n). \qquad \square \end{aligned}$$

Dies wird angewandt auf: $f(m) = A_{q,m}m = (\#$ norm. irr. Pol. vom Grad $m)*$ Grad, $g(m) = q^m$. Wir erhalten gemäß obigem Satz

$$\begin{aligned}
\sum_{d|m} A_{q,d}d = q^m, \text{ also } mA_{q,m} &= \sum_{d|m} \mu(d) q^{\frac{m}{d}} \\
\text{bzw. } A_{q,m} &\geq \tfrac{1}{m}(q^m - \sum_{1<d|m} q^{m/d}) \\
&\geq \tfrac{1}{m}(q^m - \sum_{d=0}^{m-1} q^d) \\
&= \tfrac{1}{m}(q^m - \tfrac{q^m-1}{q-1}) \\
&\geq \tfrac{1}{m}(q^m - (q^m - 1)) \\
&= \tfrac{1}{m} > 0.
\end{aligned}$$

Was noch fehlt, ist ein Irreduzibilitätstest. Vorgelegt sei ein (normiertes) Polynom aus $\mathbb{F}_q[t]$ vom Grad $d > 1$.

1. Schritt: Berechne $\gcd(f, f')$. Falls dieser von 1 verschieden ist, ist f reduzibel. (Für $f' = 0$ liegt dies daran, daß die injektive Frobeniusabbildung $x \mapsto x^q$ auf endlichen Körpern $\mathbb{F}_q$ surjektiv ist. Vgl. dazu die Ausführungen nach der Definition von Separabilität.) Man kann dann f in Faktoren kleineren Grades aufspalten.

2. Schritt: Wir können jetzt voraussetzen, dass das vorgelegte Polynom $f(t) \in \mathbb{F}_q[t]$ vom Grad $n > 1$ in $\mathbb{F}_q[t]$ in r irreduzible, paarweise verschiedene Polynome zerfällt:

$$f(t) = f_1(t) \cdot \ldots \cdot f_r(t).$$

Nach dem Chinesischen Restsatz erhalten wir

$$R := \mathbb{F}[t]/(f) \cong \bigoplus_{i=1}^{r} R_i \text{ mit } R_i := \mathbb{F}_q[t]/(f_i).$$

Beide Seiten sind $\mathbb{F}_q$-Vektorräume, die Frobenius Abbildung $\varphi_q : x \mapsto x^q$ ist auf ihnen jeweils ein Endomorphismus. Ist dann $g(t) + (f)$ ein Ele-ment auf R, welches von φ_q reproduziert wird, so gilt für den Vertreter $g(t)$ offenbar $f(t) \mid (g(t)^q - g(t))$ und wegen $g(t)^q - g(t) = \prod_{x \in \mathbb{F}_q} (g(t) - x)$ sodann, dass der irreduzible Teiler $f_i(t)$ von $f(t)$ $(i \in \{1, \ldots, r\})$ das Polynom $g(t) - x_i$ für passendes $x_i \in \mathbb{F}_q$ teilt.

Hiervon gilt auch die Umkehrung: Ist $g(t) \in \mathbb{F}_q[t]$ vom Grad $\deg(g) < n$ mit $g(t) \equiv x_i \bmod f_i(t)$ mit $x_i \in \mathbb{F}_q$ $(1 \leq i \leq r)$, so folgt $g(t)^q \equiv g(t) \bmod f_1(t)$ und weiter $f(t) \mid (g(t)^q - g(t))$.

Es gibt folglich genau q^r Kandidaten für solche Polynome $g(t)$.

Zu ihrer Berechnung bestimmt man zunächst eine Matrix der linearen Abbildung φ_q auf R bezüglich der Basis $t^i + (f)$ $(0 \leq i < n)$.

Man erhält so $A \in \mathbb{F}_q^{n\times n}$ mit

$$A(1+(f),\ldots,t^{n-1}+(f))^{tr} = (1+(f),t^q+(f),\ldots,t^{(n-1)q}+(f)).$$

Dann entsprechen die $g(t)$ mit $f(t) \mid (g(t)^q - g(t))$ gerade den Elementen aus

$$\ker(A - I_n).$$

Dieser Kern hat die Dimension $r \geq 1$. Für $r = 1$ ist $f(t)$ in $\mathbb{F}_q[t]$ irreduzibel. Für $r > 1$ spaltet $f(t)$ in r irreduzible Faktoren $f_i(t)$ $(1 \leq i \leq r)$ auf. Wegen $g(t) \equiv x_i \bmod f_i(t)$ für passendes $x_i \in \mathbb{F}_q$ gewinnt man eine Aufspaltung von $f(t)$ über die Berechnung von $\gcd(g(t) - x, f(t))$ für $x \in \mathbb{F}_q$.

Algorithmus (Berlekamp)

Eingabe: $f(t) \in \mathbb{F}_q[t]$ quadratfrei mit $\deg(f) = n > 1$.
Ausgabe: "f irreduzibel" oder echter Faktor von f.

1. Schritt: Berechne zur Frobenius Abbildung φ_q die Darstellungsmatrix $A \in \mathbb{F}_q^{n\times n}$ bzgl. der $\mathbb{F}_q$-Basis $t^{i-1}+(f)$ $(1 \leq i \leq n)$ von R.

2. Schritt: Berechne eine Basis $\underline{b}_1, \ldots, \underline{b}_r$ von $\ker(A - I_n)$.

3. Schritt: Für $r = 1$ return "f irreduzibel" und terminiere. Für $r > 1$ wähle $0 \neq \underline{b} \in \ker(A - I_n)$ und berechne für $x \in \mathbb{F}_q$ jeweils $h(t) := \gcd\left(\sum_{i=1}^{n} b_i t^{i-1} - x, f(t)\right)$ bis $\deg(h) \geq 1$ wird. Return $h(t)$ und terminiere.

Beispiel zum Berlekamp Algorithmus.
Es sei $f(t) = t^4 + 1 \in \mathbb{F}_5[t]$.
Wegen $t^5 = t(t^4+1) - t$ folgt $t^5 + (f) = -t + (f)$ in R.
Wir erhalten die Darstellungsmatrix

$$A = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & -1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & -1 \end{pmatrix} \quad \text{sowie} \quad A - I = \begin{pmatrix} 0 & 0 & 0 & 0 \\ 0 & -2 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & -2 \end{pmatrix}.$$

Es gilt $\operatorname{rg}(A - I) = 4 - \dim(\ker(A - I)) = 2$. Die Elemente aus dem Kern entsprechen Polynomen der Gestalt $g(t) = g_0 + g_2 t^2$.

Für eine Faktorisierung von f können wir oBdA $g_2 = 1$ wählen. Wegen $f(0) \neq 0$ starten wir mit $g(t) = t^2 + 1$ und erhalten $\gcd(t^2 + 1, t^4 + 1) = 1$, jedoch dann $\gcd(t^2 + 2, t^4 + 1) = t^2 + 2$ und damit die vollständige (!) Zerlegung $t^4 + 1 = (t^2 + 2)(t^2 - 2)$ in $\mathbb{F}_5[t]$.

3.28. Definition

Ein Polynom $f \in K[t]$ heißt separabel, falls für jeden irreduziblen Faktor g von f der gcd von g und g' Eins ist. Ein über K algebraisches Element x heißt separabel über K, falls sein Minimalpolynom $m_{x/K}$ separabel ist. Schließlich heißt eine algebraische Körpererweiterung L/K separabel, falls jedes $x \in L$ separabel über K ist. Ist L/K algebraisch und nicht separabel, so heißt L/K inseparabel. Ein Körper K heißt vollkommen, falls er keine inseparablen Erweiterungskörper besitzt.

Bemerkung. Sind $K \subseteq L \subseteq M$ drei Körper und ist M/K separabel, so ist auch M/L separabel.

3.29. Satz

Genau die Körper K mit $\chi(K) = p$ und $K^p = K$ und die Körper der Charakteristik 0 sind vollkommen.

Beweis:
Es sei $\chi(K) = 0$ und L eine algebraische Erweiterung von K.

Ist dann $x \in L$, so folgt $\gcd(m_x, m_{x'}) = 1$, also $m'_x(x) \neq 0$, x ist über K separabel.

Andererseits sei $\chi(K) = p$. Wir unterscheiden zwei Fälle.

(1) $K^p := \{x^p \mid x \in K\} = K$.
Wir nehmen an, daß $x \in L$ inseparabel über K ist. Dann folgt $m'_x = 0$ und $m_x(t) = \sum_{i=0}^{n} a_i t^{pi}$. Wegen $a_i = \tilde{a}_i^p \quad (0 \leq i \leq n)$ folgt $m_x(t) = \sum_{i=0}^{n} \left(\tilde{a}_i\, t^i\right)^p = \left(\sum_{i=0}^{n} \tilde{a}_i\, t^i\right)^p$ im Widerspruch zur Irreduzibilität von m_x.
Also ist in diesem Fall L/K separabel.

(2) Es sei K vollkommen.
Zu $a \in K$ betrachten wir das Polynom $t^p - a \in K[t]$.
Wir nehmen an, daß es keine Wurzel in K besitzt. Ist nun $g \in K[t]$ ein irreduzibler Teiler von $t^p - a$, so bilden wir eine Erweiterung L/K, in der g eine Nullstelle b besitzt. In $L[t]$ ist dann $t^p - a = t^p - b^p = (t-b)^p$, d.h. $g(t) = (t-b)^m$ für einen Exponenten $m \in \mathbb{Z}^{\geq 2}$. Dann ist jedoch b eine mehrfache Nullstelle des irreduziblen Polynoms $g \in K[t]$ im Widerspruch zur Vollkommenheit von K. Also muß $K^p = K$ gelten.

□

3.30. Korollar

Alle endlichen Körper sind vollkommen.

Beweis:

Die Frobenius-Abbildung $x \mapsto x^p$ ist dort wegen der Endlichkeit notwendig surjektiv.

□

Beispiel eines nicht vollkommenen Körpers: $\mathbb{F}_q(t),\ t \neq \left(\frac{f(t)}{g(t)}\right)^p$.

Bemerkung:
Algebraische Erweiterungen vollkommener Körper sind separabel.

3.31. Definition

Es sei L ein Erweiterungskörper von K. Ein algebraisches Element $\alpha\ \varepsilon\ L$ heißt **rein inseparabel** über K, wenn sein Minimalpolynom $f_{\alpha/K}(t) \in K[t]$ in $L[t]$ die Form $f(t) = (t-\alpha)^m$ hat. L ist eine **rein inseparable Erweiterung** von K, wenn jedes Element von L rein inseparabel über K ist.

3.32. Theorem

Es sei L ein Erweiterungskörper von K. $\alpha \in L$ ist sowohl separabel als auch rein inseparabel über K genau dann, wenn $\alpha \in K$ gilt und $\alpha \in L$ über K algebraisch ist.

Beweis: Es ist definitionsgemäß $m_{\alpha/K}(t) = (t-\alpha)^m$. Dieses ist genau für $m = 1$ separabel. Jedes $\alpha \in K$ hat andererseits $m_{\alpha/K}(t) = t - \alpha$. □

3.33. Lemma

Es sei L ein Erweiterungskörper von K mit $\chi(K) = p \neq 0$. Wenn $\alpha \in L$ algebraisch über K ist, dann ist α^{p^e} separabel über K für einen geeigneten Exponenten $e \geq 0$.

Beweis:
Es sei $\alpha \in L$ über K inseparabel mit $m_\alpha(t) \in K[t]$. Es folgt $m_\alpha(t) = f_1(t^p)$ mit $f_1(t) \in K[t]$. Hierbei ist $f_1(t)$ natürlich irreduzibel, es ist $f_1(t) = m_{\alpha^p}(t)$.
Ist α^p nicht separabel über K, folgt $f_1(t) = f_2(t^p)$ mit $f_2(t) \in K[t],\ f_2(t) = m_{\alpha^{p^2}}(t)$.
Nach endlich vielen Schritten ($\deg(m_\alpha) < \infty$) erhalten wir $f_e(t) = m_{\alpha^{p^e}}(t) \in K[t]$ mit α^{p^e}/K separabel. □

3.34. Theorem

Wenn L ein algebraischer Erweiterungskörper von K vom Charakter $p \neq 0$ ist, dann sind die folgenden Behauptungen äquivalent:

(1) L ist rein inseparabel über K;

(2) das irreduzible Polynom von $\alpha \in L$ ist von der Gestalt $t^{p^e} - a \in K[t]$;
(3) für $\alpha \in L$ ist $\alpha^{p^e} \in K$ für ein $e \geq 0$;
(4) die einzigen Elemente von L, die separabel über K sind, sind die Elemente von K selbst;
(5) L wird über K durch eine Menge rein inseparabler Elemente erzeugt.

Beweis:

$(i) \Longrightarrow (ii)$ Es ist $m_{\alpha/K}(t) = (t-\alpha)^m$ in $L[t]$ über K irreduzibel. Es sei $m = p^e r$ mit $p \not| r$. Dann folgt

$$(t-a)^m = (t^{p^e} - \alpha^{p^e})^r = t^{p^e r} - r\alpha^{p^e} t^{p^e(r-1)} \pm \cdots$$

in $K[t]$, also ist wegen $p \not| r$ bereits α^{p^e} in K. Damit ist auch $t^{p^e} - \alpha^{p^e} \in K[t]$ und wegen der Irreduzibilität von $m_{\alpha/K}$ notwendig $r = 1$.
$(ii) \Longrightarrow (iii)$ Trivial.
$(iii) \Longrightarrow (i)$ Es ist α Nullstelle von $(t-\alpha)^{p^e} = t^{p^e} - \alpha^{p^e}$ in $L[t]$.
Also ist $m_{\alpha/K}(t) = (t-\alpha)^m$ mit $1 \leq m \leq p^n$, das heißt α/K rein inseparabel.
$(i) \Longrightarrow (iv)$ Gemäß Satz 3.32.
$(iv) \Longrightarrow (iii)$ Gemäß Lemma 3.33.
$(i) \Longrightarrow (v)$ Trivial.
$(v) \Longrightarrow (iii)$ Es ist $L = K(S)$ mit einer Menge S von über K rein inseparablen Elementen.
Für $\alpha \in L$ existieren dann $f, g \in K[t_1, \ldots, t_r]$ und $x_1, \ldots, x_r \in S$ mit $g(x_1, \ldots, x_r) \neq 0$ und $\alpha = \frac{f(x_1,\ldots,x_r)}{g(x_1,\ldots,x_r)}$. Nach Voraussetzung existieren $n_i \in \mathbb{Z}^{\geq 0}$ mit $x_i^{p^{ni}} \in K$ $(1 \leq i \leq r)$. Für $e := \max_{1 \leq i \leq r} n_i$ ist dann $\alpha^{p^e} \in K$ (Frobenius-Isomorphismus!). □

3.35. Korollar

Ist L/K endlich und L/K rein inseparabel $\Rightarrow [L : K]$ ist p-Potenz.

Beweis:
L/K endlich impliziert $L = K(\alpha_1, \ldots, \alpha_r)$ mit algebraischen Elementen α_i.

Setze $K_i := K(\alpha_1, \ldots, \alpha_i)$, $K_0 = K, K_r = L$.

α_1 ist rein inseparabel über K, also gilt $[K_1 : K_0] = \deg(m_{\alpha_1}) = p^{e_1}$.

Ist α_i rein inseparabel über K, so folgt $m_{\alpha_i}(t) = (t-\alpha_i)^{p^{e_i}} \in K[t]$, also ist das Minimalpolynom von α_i/K_{i-1} eine Potenz von $t - \alpha_i$, α_i/K_{i-1} rein inseparabel, $[K_i : K_{i-1}]$ p-Potenz.

Also folgt die Behauptung nach dem Gradsatz.

□

3.36. Satz

L/K separabel impliziert $KL^p = L$.
L/K endlich mit $KL^p = L$ impliziert L/K separabel.

Beweis:
Zunächst sei L/K separabel.
Wegen $L^p \subseteq KL^p \subseteq L$ ist $\alpha^p \in KL^p$ für alle $\alpha \in L$, also ist jedes solche α nach 3.34 rein inseparabel über KL^p.
Daher ist L/KL^p separabel und rein inseparabel, es folgt $L = KL^p$ mittels 3.32.

Es sei nunmehr L/K endlich mit $L = KL^p$.
Wir nehmen an, dass $\alpha \in L$ mit $m_\alpha(t) \in K[t]$ existiert, welches über K nicht separabel ist.
Es muß notwendig $m_\alpha(t) = \sum_{i=0}^{m} a_{ip}\, t^{ip}$ $(a_{mp} = 1)$ gelten!

Dies bedeutet, dass $1, \alpha^p, \ldots, \alpha^{mp} \in L$ K-linear abhängig sind.
Ferner sind $1, \alpha, \ldots, \alpha^m \in L$ K-linear unabhängig wegen $\deg(m_\alpha) = mp > m$.

Es sei nun $\omega_1, \ldots, \omega_n$ eine Basis von L/K. Wir erhalten für $\beta \in L$:

$$\begin{aligned} \beta &= b_1\,\omega_1 + \ldots + b_n\,\omega_n \in K\omega_1 + \ldots + K\omega_n = L, \\ \beta^p &= b_1^p\,\omega_1^p + \ldots + b_n^p\,\omega_n^p, \end{aligned}$$

also ist $\omega_1^p, \ldots, \omega_n^p$ ein Erzeugendensystem von L^p/K^p.
Nach Voraussetzung gilt:

$$\begin{aligned} L = KL^p &= K(K^p\omega_1^p + \ldots + K^p\omega_n^p) \\ &\subseteq K\omega_1^p + \ldots + K\omega_n^p \subseteq L, \end{aligned}$$

folglich ist auch $\omega_1^p, \ldots, \omega_n^p$ eine Basis von L/K.

Ergänzen wir also $1, \alpha, \ldots, \alpha^m$ zu einer Basis $1, \alpha, \ldots, \alpha^m, \beta_{m+1}, \ldots, \beta_{n-1}$ von L/K, so ist $1, \alpha^p, \ldots, \alpha^{mp}, \beta_{m+1}^p, \ldots, \beta_{n-1}^p$ wieder eine, und speziell sind $1, \alpha^p, \ldots, \alpha^{mp}$ K-linear unabhängig. Widerspruch!

□

3.37. Korollar

(1) Die folgenden Aussagen für $\alpha \in L/K$ algebraisch sind äquivalent:
   (a) $K(\alpha) = K(\alpha^p)$,
   (b) $K(\alpha)/K$ ist separabel,
   (c) α/K ist separabel.
(2) M/L und L/K endlich separabel $\Rightarrow$ M/K endlich separabel.
(3) $\alpha_1, \ldots, \alpha_r \in L$ über K separabel $\Rightarrow$ $K(\alpha_1, \ldots, \alpha_r)/K$ separabel.
(4) M/L und L/K separabel $\Rightarrow$ M/K separabel.

(5) Für L/K beliebige Erweiterung ist

$$\begin{aligned} L_{sep} &= \{\alpha \in L \mid \alpha/K \text{ separabel}\} \\ &= L_{sep/K} \end{aligned}$$

ein Teilkörper von L, der K enthält. L/L_{sep} ist rein inseparabel.

Beweis:

(1) (a) $\rightarrow$ (b)
Es ist $K(\alpha) = K(\alpha^p)$ und $K(\alpha)/K$ endlich.
Wegen $K(\alpha) = K(\alpha^p) \subseteq KK(\alpha)^p \subseteq K(\alpha)$ gilt $KK(\alpha)^p = K(\alpha)$, und die Behauptung folgt mittels 3.36.

(b) $\Rightarrow$ (c) trivial.

(c) $\Rightarrow$ (a) $\alpha \in L$ ist über K separabel, also über $K(\alpha^p)$.
Wegen $\alpha^p \in K(\alpha^p)$ ist $\alpha/K(\alpha^p)$ rein inseparabel.
Folglich ist $\alpha \in K(\alpha^p)$ und $K(\alpha) \subseteq K(\alpha^p) \subseteq K(\alpha)$.

(2) Wir haben $LM^p = M$, $KL^p = L$, folglich $KM^p = KL^pM^p = LM^p = M$ und M/K ist nach 3.36 separabel.

(3) Setze $K_0 = K$, $K_i = K(\alpha_1, \ldots, \alpha_i)$ mit $K_r = L$. Nach (i) ist K_1/K_0 separabel. Ferner ist α_i/K_0 und damit über K_{i-1} separabel, also K_i/K_{i-1}. Damit folgt die Behauptung nach (ii).

(4) Es sei $\alpha \in M$. α/L ist separabel mit Minimalpolynom $m_{\alpha/L}(t) = \sum_{i=0}^{m} a_i\, t^i$.
Hierbei sind $a_0, \ldots, a_m$ über K separabel.
Also ist $\hat{L} := K(a_0, \ldots, a_m)$ über K nach (iii) separabel.
Ferner ist $m_{\alpha/\hat{L}}(t) = m_{\alpha/L}(t)$, also $\alpha/\hat{L}$ separabel.

Demnach ist nach (i) $\hat{L}(\alpha)/\hat{L}$ und somit $\hat{L}(\alpha)$ nach (iii) über K separabel, also ist α/K separabel.

(5) Sind $\alpha, \beta \in L$ über K separabel, so ist $K(\alpha, \beta)/K$ separabel nach (iii), also sind $\alpha \overset{\pm}{\bullet} \beta$, $\alpha\, \beta^{-1}$ (für $\beta \neq 0$) separabel über K. L_{sep} ist somit Körper. $K \subseteq L_{sep}$ folgt nach (3.32). Gemäß 3.33 ist für $\alpha \in L$ stets $\alpha^{p^e} \in L_{sep}$ für geeignetes $e \in \mathbb{Z}^{\geq 0}$. Nach 3.34 (i) und (iii) (L_{sep} in der Rolle von K) ist demnach L/L_{sep} rein inseparabel.

□

Bemerkungen:

(1) $L_{sep} = L_{sep/K}$ heißt separabler Abschluss (separable Hülle) von K in L.

(2) Ist L/K algebraisch, so ist L/L_{sep} rein inseparabel. (Für $x \in L$ ist eine geeignete p–Potenz über K separabel gemäß Lemma

3.35, also ist etwa $x^{p^e} \in L_{sep}$ und x demnach über L_{sep} rein inseparabel.)

(3) $[L : K]_{sep} := [L_{sep} : K]$ heißt **Separabilitätsgrad** von L/K. Entsprechend heißt $[L : K]_i := [L : L_{sep}]$ **Inseparabilitätsgrad** der Erweiterung L/K.

(4) Ist $[L : K]_i < \infty$, so ist es eine Potenz der Charakteristik. Ist $[L : K] < \infty$ mit $p \nmid [L : K]$, so ist L/K separabel.

3.38. Definition

Eine Körpererweiterung L/K heißt normal, falls L/K algebraisch ist und jedes irreduzible Polynom $f \in K[t]$, welches in L eine Wurzel besitzt, in $L[t]$ in Linearfaktoren zerfällt.

3.39. Satz

Es sei L/K algebraisch. Dann sind äquivalent:

(1) L/K ist endlich und normal,
(2) L ist Zerfällungskörper eines Polynoms $f \in K[t]$.

Beweis:
(i) $\Rightarrow$ (ii)
Es sei $L = K(\alpha_1, \ldots, \alpha_n)$ und $f_i = m_{\alpha_i} \in K[t] \quad (1 \leq i \leq n)$.
Da L/K normal ist, zerfällt jedes Minimalpolynom m_{α_i} in $L[t]$. Also zerfällt auch $f := \prod_{i=1}^{n} f_i$ in $L[t]$ in Linearfaktoren, und L ist dann definitionsgemäß Zerfällungskörper von f über K.

(ii) $\Rightarrow$ (i)
Es seien $\alpha_1, \ldots, \alpha_n$ die Wurzeln von f, d.h. $L = K(\alpha_1, \ldots, \alpha_n)$. Ferner sei $g \in K[t]$ irreduzibel mit $g(\beta) = 0$, $\beta \in L$. Es sei M Zerfällungskörper von g über K und γ eine Wurzel von g in M.
Gemäß 3.18 existiert dann ein K-Isomorphismus ϕ von $K(\beta)$ auf $K(\gamma)$ mit $\phi(\beta) = \gamma$.
Nun ist $L = L(\beta)$ ein Zerfällungskörper von $f \in K(\beta)[t]$ und $L(\gamma) := K(\alpha_1, \ldots, \alpha_n, \gamma)$ ein Zerfällungskörper von $\phi f = f$ über $K(\gamma)[t]$.
Nach 3.19 existiert dann ein K-Isomorphismus Φ von L auf $L(\gamma)$, der ϕ fortsetzt. Wegen $L \subseteq L(\gamma)$ und $\dim_K L = \dim_K L(\gamma)$ (Φ Isom.!) folgt also $L = L(\gamma)$, d.h. $\gamma \in L$. Also zerfällt g in $L[t]$ in Linearfaktoren. Ferner war $[L : K] < \infty$, damit L/K algebraisch, also normal.

$$\begin{array}{ccc} L & \xrightarrow{\Phi} & L(\gamma) = K(\alpha_1, \ldots, \alpha_n, \gamma) \\ | & & | \\ K(\beta) & \xrightarrow{\varphi} & K(\gamma) \\ | & & | \\ K & \xrightarrow{id} & K \end{array}$$

□

Beispiele:
Kreiskörper, quadratische Körpererweiterungen.

3.40. Lemma

Es sei L/K eine endliche normale Erweiterung.

Ferner seien E, F K-isomorphe Zwischenkörper dieser Erweiterung. Ist dann $\phi : E \to F$ ein K- Isomorphismus, so läßt er sich zu einem K-Automorphismus von L fortsetzen.

Beweis:
Es sei L Zerfällungskörper von $f \in K[t]$.

Dann ist L auch Zerfällungskörper für $f \in E[t]$ bzw. $f \in F[t]$, und die Behauptung folgt wie im Beweis von 3.19.

□

Ist L/K eine endliche normale Erweiterung, so bilden die K-Automorphismen von L bezüglich Hintereinanderausführung eine Gruppe $G = G(L/K)$. Diese Gruppe ist endlich. Denn ist etwa L Zerfällungskörper von $f \in K[t]$, so permutiert jedes $\phi \in G$ die Wurzeln von f, man erhält unmittelbar $\#G \leq \deg(f)!$

3.41. Lemma

Es sei L/K eine endliche Körpererweiterung. Dann existiert hierzu eine minimale normale (endliche) Erweiterung M/K mit $M \supseteq L$, d.h. ist E eine normale Erweiterung über K, die L enthält, so existiert ein K-Monomorphismus von M in E.

Beweis:

Es sei $L = K(\alpha_1, \ldots, \alpha_n)$ und $f = \prod_{i=1}^{n} m_{\alpha_i}$.

Es sei M der Zerfällungskörper von f über K. M ist dann gemäß (3.28) normal über K.

Ist dann $E \supseteq L$ eine normale Erweiterung über K, so zerfällt jedes $m_{\alpha i}$ und damit f in $E[t]$ in Linearfaktoren, d.h. E enthält einen Zerfällungskörper von f als Teilkörper E_1.

Gemäß (3.19) existiert ein K-Isomorphismus zwischen M und E_1.

□

3.42. Satz

Es sei L eine endliche separable Erweiterung über K und M/K normal mit $K \subseteq L \subseteq M$.

Dann existieren genau $n := [L : K]$ verschiedene K- Isomorphismen von L auf Teilkörper von M.

Beweis:

Wegen 3.41 können wir auch $[M : K] < \infty$ annehmen.

Der Beweis erfolgt mittels Induktion über n.

$n = 1$: $L = K$, die Identität ist die einzig mögliche Abbildung.

$n > 1$: Sei zunächst L/K einfach, d.h. $L = K(\alpha)$ und $n = \deg(m_\alpha)$.

Wegen L/K separabel besitzt m_α gerade n verschiedene Nullstellen. Jeder K-Isomorphismus ϕ von L bildet notwendig α auf eine der Nullstellen von m_α ab, und ϕ ist durch $\phi(\alpha)$ eindeutig bestimmt. Also existieren genau $n = [L : K]$ Isomorphismen.

Man beachte, daß alle Nullstellen von m_α in M liegen!

Ist schließlich $L = K(\alpha_1, \ldots, \alpha_n)$, so bilden wir $L_1 := K(\alpha_1)$, und L ist über L_1 separabel mit $K \subset L_1 \subset L$. Ferner ist M normal über L_1. Wegen $[L : L_1] < [L : K]$ existieren genau $m = [L : L_1]$ L_1-Isomorphismen von L auf Teilkörper von M, die sich zu L_1-Automorphismen $\sigma_1, \ldots, \sigma_m$ von M fortsetzen lassen. Ferner existieren genau $r = [L_1 : K]$ K-Isomorphismen von L_1 auf Teilkörper von M.

Diese lassen sich ebenfalls zu K-Automorphismen $\phi_1, \ldots, \phi_r$ von M fortsetzen.

Setze $\tau_{ij} := \phi_j \, \sigma_i \qquad (1 \le i \le m,\ 1 \le j \le r)$.

Ist nun ρ ein K-Isomorphismus von L, so gilt $\rho \,|\, L_1 = \phi_\nu \,|_{L_1}$ mit $\nu = \nu(\rho) \in \{1, \ldots, r\}$ und $\phi_\nu^{-1} \, \rho$ läßt L_1 invariant, also ist $\phi_\nu^{-1} \, \rho \,|_L$ gleich einem $\sigma_\mu \,|_L$ mit $\mu = \mu(\rho, \nu) \in \{1, \ldots, m\}$. Es bleibt zu zeigen, daß alle $\tau_{ij} \,|_L$ verschieden sind. Wäre etwa $\tau_{ij} \,|_L = \tau_{\mu\nu} \,|_L$, also $\phi_j \, \sigma_i \,|_L = \phi_\nu \, \sigma_\mu \,|_L$, so folgte $\phi_j \,|_{L_1} = \phi_\nu \,|_{L_1}$, also $\nu = j$ und damit $\sigma_i \,|_L = \sigma_\mu \,|_L$.

□

3.43. Korollar

(2. Satz vom primitiven Element) Jede endliche separable Erweierung L/K besitzt ein primitives Element.

Beweis:

Gemäß 3.15 genügt es zu zeigen, daß nur endlich viele Zwischenkörper existieren. Gemäß 3.41 sei M/K eine minimale normale K-Erweiterung, die L enthält. Diese ist dann über K separabel (vgl. 3.37(iii))) Die Gruppe $G(M/K)$ ist endlich von der Ordnung $n = [M : K]$. Ist nun E ein Zwischenkörper $K \subset E \subset M$, so ist M/E normal und separabel, und die Gruppe $G(M/E)$ ist eine Untergruppe von $G(M/K)$.

Wir zeigen, daß verschiedene Zwischenkörper verschiedene Automorphismengruppen besitzen. Da $G(M/K)$ nur endlich viele Untergruppen hat, beendet dies den Beweis.

Seien also E, F zwei Zwischenkörper $K \subset \begin{matrix} E \\ F \end{matrix} \subset M$ und $E \neq F$. Sei $oBdA \quad x \in E \backslash F$. Da M/F separabel ist, exisiert $\sigma \in G(M/F)$ mit $\sigma(x) \neq x$ (!). Dies beweist $G(M/F) \neq G(M/E)$.

□

3.44. Korollar

Es sei L/K endlich mit $n_0 := [L : K]_{sep}$. Ferner sei M/K normal mit $M \supseteq L \supseteq K$. Dann existieren genau n_0 verschiedene K-Isomorphismen von L auf Teilkörper von M.

Beweis: Wie im Beweis des Satzes können wir $[M : K] < \infty$ annehmen. Die Erweiterung L/K spalten wir auf in L_{sep}/K und L/L_{sep}. Es ist dann L_{sep}/K endlich und separabel, also nach dem vorangehenden Korollar einfach. Wir haben $L_{sep} = K(\alpha)$ für ein passendes $\alpha \in L$. Nach dem letzten Satz existieren genau n_0 verschiedene K-Isomorphismen von L_{sep}, etwa $\sigma_1, \ldots, \sigma_{n_0}$, die sich zu K-Automorphismen $\tilde{\sigma_1}, \ldots, \tilde{\sigma_{n_0}}$ von M fortsetzen lassen. Wir zeigen, dass $\tilde{\sigma_j}|_L$ $(1 \leq j \leq n_0)$ alle K-Isomorphismen von L auf Teilkörper von M sind.
Es ist L/L_{sep} endlich, also gilt $L = L_{sep}(\alpha_1, \ldots, \alpha_r)$. Es seien $m_{\alpha_i/L_{sep}}(t)$ die zugehörigen Minimalpolynome aus $L_{sep}[t]$ $(1 \leq i \leq r)$. Wegen α_i/L_{sep} rein inseparabel ist $m_{\alpha_i/L_{sep}}(t) = t^{p^{e_i}} - a_i$, und diese Polynome zerfallen in $M[t]$ in der Form $(t - \alpha_i)^{p^{e_i}}$ mit $\alpha_i \in M, \alpha_i^{p^{e_i}} = a_i$. Jeder K-Isomorphismus σ von L auf einen Teilkörper von M lässt $m_{\alpha_i/L_{sep}}$ invariant, seine Fortsetzung $\tilde{\sigma}$ zu einem K-Automorphismus von M erfüllt notwendig $\tilde{\sigma}(\alpha_i) = \alpha_i$, also $\tilde{\sigma}|_L(\alpha_i) = \sigma(\alpha_i) = \alpha_i$. Damit ist $\tilde{\sigma}$ bereits durch seine Bilder auf L_{sep} eindeutig festgelegt, es folgt $\tilde{\sigma}|_L = \tilde{\sigma_j}|_L$ für passendes $j \in \{1, \ldots, n_0\}$.

□

Bemerkungen:

(1) M/K normal und $K \subset L \subset M$ impliziert M/L normal. (Das Minimalpolynom $m_{\alpha/L}$ eines Elements $\alpha \in M$ ist ein Teiler von $m_{\alpha/K}$. Da $m_{\alpha/K}$ in $M[t]$ in Linearfaktoren zerfällt, leistet dies auch $m_{\alpha/L}$.)
(2) Für M/K endlich und normal gilt $\#G(M/K) = [M : K]_{sep}$.
(3) Es sei M/K endlich und normal. Gilt für ein $\alpha \in M$ dann $\sigma(\alpha) = \alpha$ für alle $\sigma \in G(M/K)$, ist α/K notwendig rein inseparabel. Ist also zusätzlich M/K separabel, so folgt bereits $\alpha \in K$. In jedem Fall ist $L := \{\alpha \in M | \sigma(\alpha) = \alpha \quad \forall\ \sigma \in G/(M/K)\}$ ein Körper, sowie L/K rein inseparabel.

Normen und Spuren

Im folgenden sei L/K endlich mit $[L:K]_{sep} = n_0$ und Γ/K endlich und normal mit $\Gamma \supseteq L$. Gemäß 3.43 existieren gerade n_0 K-Isomorphismen $\sigma_1, \ldots, \sigma_{n_0}$ von L auf Teilkörper von Γ, die K enthalten.

3.45. Definition

Für Elemente $\alpha \in L$ definieren wir

Norm $\qquad N_{L/K}(\alpha) = \left(\prod_{j=1}^{n_0} \sigma_j(\alpha)\right)^{[L:K]_i}$ und

Spur $\qquad Tr_{L/K}(\alpha) = [L:K]_i \sum_{j=1}^{n_0} \sigma_j(\alpha).$

3.46. Hilfssatz

Ist $m_{\alpha/K}(t) = t^r + c_1\, t^{r-1} + \ldots + c_r \in K[t]$, so gilt

$$\begin{aligned} N_{L/K}(\alpha) &= \left((-1)^r\, c_r\right)^{[L:K(\alpha)]}, \\ Tr_{L/K}(\alpha) &= -[L:K(\alpha)]c_1. \end{aligned}$$

Beweis:

Es sei $m_0 = [K(\alpha):K]_{sep}$. Also existieren gerade $\tau_1, \ldots, \tau_{m_0}$ K- Isomorphismen von $K(\alpha)$ in Teilkörper von F. Deren Fortsetzungen (fixiert!) zu Γ-Automorphismen seien $T_1, \ldots, T_{m_0}$. Ist $r_0 = [L:K(\alpha)]_{sep}$, so existieren genau r_0 $K(\alpha)$-Isomorphismen κ_j von L auf Teilkörper von Γ, und wie im Beweis zu (3.46) sind dann $\rho_{ij} := T_i\,\kappa_j$ alle K-Isomorphismen von L. Also erhalten wir:

$$\begin{aligned} N_{L/K}(\alpha) &= \left(\prod_{i=1}^{m_0}\prod_{j=1}^{r_0} T_i\,\kappa_j(\alpha)\right)^{[L:K]_i} = \left(\prod_{j=1}^{m_0} \tau_j(\alpha)\right)^{r_0[L:K]_i}, \\ Tr_{L/K}(\alpha) &= [L:K]_i \sum_{i=1}^{m_0}\sum_{j=1}^{r_0} T_i\,\kappa_j(\alpha) = r_0[L:K]_i \sum_{i=1}^{m_0} \tau_i(\alpha) \\ &= [L:K(\alpha)]_{sep}\,[L:K(\alpha)]_i\,[K(\alpha):K]_i \textstyle\sum_{i=1}^{m_0} \tau_i(\end{aligned}$$

Andererseits ist in $\Gamma[t]$:

$$m_{\alpha/K}(t) = \left(\prod_{i=1}^{m_0}\Big(t-\tau_i(\alpha)\Big)\right)^{[K(\alpha):K]_i}, \text{ also}$$

$$c_r = \left((-1)^{m_0}\left(\prod_{i=1}^{m_0}\tau_i(\alpha)\right)\right)^{[K(\alpha):K]_i}, \qquad c_1 = -\,[K(\alpha):K]_i\sum_{i=1}^{m_0}\tau_i(\alpha),$$

$$(-1)^r\,c_r = \left(\prod_{i=1}^{m_0}\tau_i(\alpha)\right)^{[K(\alpha):K]_i}.$$

□

Bemerkungen:

(a) Norm und Spur sind Elemente des Grundkörpers K.
(b) Norm und Spur sind unabhängig von der Wahl von Γ.

Eigenschaften von Norm und Spur

3.47. Hilfssatz

Es seien $M/L/K$ endlich, $a \in K$, $\alpha, \beta \in L$, $x \in M$.
Dann gilt:

(1) $N_{L/K}(\alpha\,\beta) = N_{L/K}(\alpha)\,N_{L/K}(\beta)$, $Tr_{L/K}(\alpha+\beta) = Tr_{L/K}(\alpha) + Tr_{L/K}(\beta)$;
(2) $N_{L/K}(a) = a^{[L:K]}$, $Tr_{L/K}(a) = [L:K]a$;
(3) $N_{M/K}(x) = N_{L/K}\Big(N_{M/L}(x)\Big)$, $Tr_{M/K}(x) = Tr_{L/K}\Big(Tr_{M/L}(x)\Big)$.

Beweis: Übungen.

Sind L/K endlich vom Grad n und $\alpha_1, \ldots, \alpha_n$ eine K-Basis von L, so heißt $d(\alpha_1, \ldots, \alpha_n) := det\Big(Tr_{L/K}(\alpha_i\,\alpha_j)\Big)$ Diskriminante der Basis.

Sind $\alpha_1, \ldots, \alpha_n$ sowie $\beta_1, \ldots, \beta_n$ zwei Basen von L/K, so ist $d(\alpha_1, \ldots, \alpha_n) = d(\beta_1, \ldots, \beta_n)\,a^2$
mit $a \in K$, $a \neq 0$.

Man kann also als Diskriminante $d(L/K)$ von L/K die Quadratklasse $d(\alpha_1, \ldots, \alpha_n)\,(K^\times)^2$ erklären.

3.48. Satz

$d(L/K) = 0 \Leftrightarrow Tr_{L/K}(\alpha) = 0\ \forall\ \alpha \in L$.

Beweis: " $\Leftarrow$ " trivial.
" $\Rightarrow$ " Die Spalten der Matrix $\Big(Tr_{L/K}(\alpha_i\,\alpha_j)\Big)$ sind linear abhängig.
Also existieren $b_1, \ldots, b_n \in K$, nicht alle gleich 0, mit

$$\sum_{j=1} b_j \, Tr_{L/K}(\alpha_i \, \alpha_j) = 0 \qquad (1 \leq i \leq n).$$

Folglich ist $\beta := \sum_{j=1}^{n} b_j \, \alpha_j \neq 0$. Für $\alpha \in L$ existiert demnach $\gamma = \sum_{i=1}^{n} c_i \, \alpha_i \in L$ mit $\alpha = \beta \, \gamma$.

Es folgt:

$$Tr_{L/K}(\alpha) = Tr_{L/K}\left(\sum_{i=1}^{n} c_i \, \alpha_i \sum_{j=1}^{n} b_j \, \alpha_j\right) = \sum_{i=1}^{n} c_i \, Tr_{L/K}\left(\sum_{j=1}^{n} b_j \, \alpha_i \, \alpha_j\right) = 0.$$

□

3.49. Satz

$d(L/K) \neq 0 \Leftrightarrow L/K$ ist separabel.

Beweis:

(1) L/K inseparabel $\Rightarrow Tr_{L/K}(\alpha) = 0 \ \forall \ \alpha \in L \ \Rightarrow_{(3.51)} d(L/K) = 0$

(2) L/K separabel $\Rightarrow_{(3.32)} L = K(\alpha)$, $m_{\alpha/K}(t)$ hat keine mehrfachen Wurzeln.

Es ist $1, \alpha, \ldots, \alpha^{n-1}$ $(n = deg(m_{\alpha/K}))$ eine Basis von L/K. Hierfür ist $d(1, \alpha, \ldots, \alpha^{n-1})$ Quadrat einer Vandermonde Determinante, also von 0 verschieden.

□

Beispiel:
$K = \mathbb{Q}$, $L = \mathbb{Q}(\sqrt{m})$, $[L : K] = 2$, L/K separabel.
Eine Basis ist $1, \sqrt{m}$.
Für $\alpha = a + b\sqrt{m}$ ist

$$\begin{array}{rcl} Tr(\alpha) & = & 2a, \ N(\alpha) \qquad\qquad = \ a^2 - m\,b^2 \\ d(1,\,\alpha) & = & \begin{pmatrix} Tr(1) & Tr(\alpha) \\ Tr(\alpha) & Tr(\alpha^2) \end{pmatrix} \ = \ \begin{pmatrix} 2 & 2a \\ 2a & 2(a^2 + mb^2) \end{pmatrix} \\ & = & 4m\,b^2. \end{array}$$

Es ist $m_{\alpha/\mathbb{Q}}(t) = \begin{cases} t - a \text{ für } b = 0 \\ t^2 - Tr(\alpha)t + N(\alpha) \text{ sonst.} \end{cases}$

3.50. Definition

Ein Körper K heißt algebraisch abgeschlossen, falls für jede algebraische Erweiterung L/K

bereits $L = K$ gilt. $\bar{K}$ heißt algebraischer Abschluß des Körpers K, falls $\bar{K}/K$ algebraisch und $\bar{K}$ algebraisch abgeschlossen ist.

3.51. Satz

Ein Körper K besitzt einen algebraischen Abschluß $\bar{K}$, und je zwei algebraische Abschlüsse von K sind K-isomorph.

Beweis:

(1) Existenz
Wir konstruieren zunächst eine Körpererweiterung L_1/K, in der jedes Polynom f aus $K[t]$ mit $\deg(f) \geq 1$ eine Nullstelle besitzt. Dazu bilden wir eine Indexmenge $I = \{f \in K[t] | \deg(f) \geq 1\}$ und betrachten dazu ein unendliches System $S = (x_f)_{f \in I}$ von Variablen nebst Polynomring $K[S]$, (Konstruktion als Halbgruppenring wie in Kapitel 2.) $K[S]$ enthält das Ideal $A = \langle f(x_f) | f \in I \rangle$, wobei die Variable t jeweils durch x_f ersetzt wird.
Es gilt $A \subset K[S]$. (Denn für $1 \in A$ existieren Polynome $g_i \in K[S]$ sowie $f_i \in A$ $(1 \leq i \leq r)$ mit

$$1 = \sum_{i=1}^{r} g_i \; f_i \; (x_{f_i}). \tag{1}$$

Es existiert nun ein Erweiterungskörper $\tilde{K}$ von K, indem jedes der f_i eine Nullstelle α_i besitzt. Einsetzen von α_i für (x_{f_i}) in Gleichung 1 liefert den Widerspruch $1 = 0$.)
Also ist A in einem maximalen Ideal M von $K[S]$ enthalten. Hierfür ist $L_1 := K[S]/M$ ein Körper. Mittels der Einbettung $K \hookrightarrow K[S]$ und dem kanonischen Epimorphismus $K[S] \longrightarrow K[S]/M$ lässt sich L_1 als Erweiterungskörper von K auffassen. Für $f \in A$ ist dann $x_f + M$ eine Nullstelle in L_1.
Diese Konstruktion iterieren wir, falls L_1 noch nicht algebraisch abgeschlossen ist, und erhalten so eine echt aufsteigende Kette von Körpern $K = L_0 \subset L_1 \subset L_2 \subset \ldots$, wobei jedes Polynom $f \in L_n[t]$ mit $\deg(f) \geq 1$ in L_{n+1} eine Nullstelle hat. Wir bilden dann $L := \bigcup_{n=0}^{\infty} L_n$. Es ist L Körper (!), und wir zeigen, dass L algebraisch abgeschlossen ist. Ist dazu $f \in L[t]$ mit $k := \deg(f) \geq 1$, so liegen die $k+1$ Koeffizienten von f in Teilkörpern, etwa $L_{i_1}, \ldots, L_{i_{k+1}}$. Ist $i_0 := \max\{i_\nu | 1 \leq \nu \leq k+1\}$, so gilt bereits $f \in L_{i_0}[t]$, und f hat nach Konstruktion eine Nullstelle in $L_{i_0+1} \subseteq L$. Folglich ist L algebraisch abgeschlossen.

(2) Eindeutigkeit bis auf Isomorphie.
Wir nehmen an, daß $\bar{K}$ und $\hat{K}$ beides algebraische Abschlüsse von K sind.
Es bezeichne $\mathfrak{M}$ die Menge aller geordneten Tripel $(L, \tilde{L}, \psi)$ mit $K \subseteq L \subseteq \bar{K}$,

$K \subseteq \tilde{L} \subseteq \hat{K},\ \psi : L \to \tilde{L}$ Isomorphismus.

Es ist $\emptyset \neq \mathfrak{M}$ wegen $(K,\ K,\ id) \in \mathfrak{M}$.

Wir ordnen $\mathfrak{M}$ partiell gemäß $(L,\ \tilde{L},\ \psi) \leq (L_1,\ \tilde{L_1},\ \psi_1)$ für $L \subseteq L_1,\ \tilde{L} \subseteq \tilde{L_1},\ \psi_1 \,|\, \tilde{L} = \psi$.

Es sei $(F,\ \tilde{F},\ \Phi)$ maximales Element in $\mathfrak{M}$ gemäß Zorn's Lemma (!).

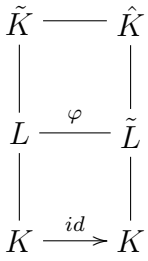
Ist $F = \bar{K}$, so ist notwendig $\tilde{F} = \Phi(F)$ algebraisch abgeschlossen, also $\tilde{F} = \hat{K}$.

Existiert jedoch $x \in \bar{K} \backslash F$, so besitzt x ein Minimalpolynom $m_{x/F}(t)$.

Hierfür ist $\Phi(m_{x/F}(t)) \in \tilde{F}[t]$ irreduzibel, und Φ läßt sich fortsetzen zu einem Isomorphismus $\tilde{\Phi} : F(x) \to \tilde{F}(\tilde{x})$ (für eine Nullstelle $\tilde{x}$ von $\phi(m_{x/F}(t))$) im Widerspruch zur Maximalität von $(F,\ \tilde{F},\ \Phi)$.

Also muß $F = \bar{K},\ \tilde{F} = \hat{K}$ gelten.

□



Bibliography

[1] Bewersdorff, Jörg, *Algebra für Einsteiger*,Vieweg, 2002.
[2] Birkhoff, Bartee, *Modern Applied Algebra*.
[3] S. Bosch, *Algebra*, Springer, 1993.
[4] N. Bourbaki, *Algebre*, Hermann, Paris 1962.
[5] J. H. Davenport, Y. Siret, E. Tournier, *Computer algebra*, Acad. Press, 1989.
[6] I. N. Herstein, *Topics in Algebra*, Xerox Coll. Pub., 1964.
[7] Th. W. Hungerford, *Algebra*, 1974.
[8] N. Jacobson, *Lectures in Abstract Algebra*, Springer GTM, 1974.
[9] R. Kochendörffer, *Einführung in die Algebra*, Dt.Verl.d. Wissenschaften, 1974.
[10] S. Lang, *Algebra*, Addison-Wesley, 1971.
[11] A. Leutbecher, *Zahlentheorie*, Springer, 1996.
[12] F. Lorenz, *Algebra I, II*, BI Wissenschaftsverlag, 1987/90.
[13] K. Meyberg, *Algebra I, II*, Carl Hanser Verlag, 1975.
[14] Mignotte, *Mathematics for Computer Algebra*, Springer, 1992.
[15] E. Scholz, *Geschichte der Algebra*, BI Wissenschaftsverlag, 1990.
[16] G. Stroth, *Algebra*, de Gruyter, 1998.
[17] B. L. van der Waerden, *Algebra I, II*, Springer, 1966/87.
[18] Weber, *Lehrbuch der Algebra*, Vieweg, 1895.