Tutorium 13

1 Separable Körpererweiterungen

1 Definition. Sei L/K algebraische Körpererweiterung und $\bar{K}$ der algebraische Abschluss von K.

(a) $f \in K[X] \setminus K$ heißt *separabel*, falls f $\deg(f)$ verschiedene Nullstellen in $\bar{K}$ hat (d.h. genau dann, wenn f keine doppelten Nullstellen in $\bar{K}$ hat)

(b) $\alpha \in L$ heißt *separabel* über K, falls das Minimalpolynom $m_\alpha \in K[X]$ von α separabel ist

(c) L/K heißt *separabel*, falls alle $\alpha \in L$ separabel über K sind

2 Bemerkung. Sei $f \in K[X] \setminus K$. Dann gilt:

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

(f' ist die "formale" Ableitung.) Ist f zusätzlich irreduzibel, dann gilt sogar:

$$f \text{ separabel} \quad \Leftrightarrow \quad f' \neq 0$$

3 Definition. K heißt *vollkommen*, falls jede algebraische Erweiterung separabel ist.

4 Aufgabe. Zeige:

$$\operatorname{char}(K) = 0 \quad \Rightarrow \quad K \text{ vollkommen}$$

Beweis. Sei L/K algebraische Erweiterung, $\alpha \in L$ mit Minimalpolynom $m_\alpha = \sum_{i=0}^n a_i X^i \in K[X]$. Dann gilt:

$$\begin{aligned} & m'_\alpha = 0 \\ \Rightarrow\ & \forall i = 0, \ldots, n : i \cdot a_i = 0 \\ \Rightarrow\ & \forall i = 1, \ldots, n : a_i = 0 \\ \Rightarrow\ & \deg(m_\alpha) = 0 \end{aligned}$$

Widerspruch! Also $m'_\alpha \neq 0$, also ist das (irreduzible!) Minimalpolynom m_α separabel, d.h. α ist separabel über K. □

5 Definition. Sei L/K endliche Körpererweiterung und $\bar{K}$ der algebraische Abschluss von K.

$$[L : K]_s := \# \operatorname{Hom}_K(L, \bar{K})$$

heißt *Separabilitätsgrad* von L über K.

6 Satz. *(a)* $[L : K]_s \leq [L : K]$

(b) $[L : K]_s = [L : K] \Leftrightarrow L/K$ *separabel*

(c) M *Zwischenkörper* $\Rightarrow [L : K]_s = [L : M]_s \cdot [M : K]_s$

7 Aufgabe. Sei L/K algebraische Körpererweiterung, α, $\beta \in L$. Zeige:

(a) α separabel über $K \Rightarrow K(a)/K$ separabel

(b) α, β separabel über $K \Rightarrow \alpha + \beta$, $\alpha\beta$ separabel über K

Beweis. (a) Ist α separabel, so hat das Minimalpolynom $m_\alpha \in K[X]$ keine doppelten Nullstellen, d.h. $\deg(m_\alpha) = [K(a) : K]$ verschiedene.

Damit gibt es dann $[K(a) : K]$ viele K-Homomorphismen $K(\alpha) \to \bar{K}$, denn wir können α auf jede Nullstelle von m_α schicken, und durch die Wahl des Bilds von α ist jeder solche Homomorphismus bestimmt.

Es gilt also $[K(a) : K]_s = [K(a) : K]$, mit dem Satz folgt, dass $K(a)/K$ separabel ist.

(b) Sei $m_\beta^K \in K[X]$ das Minimalpolynom von β über K sowie $m_\beta^{K(\alpha)} \in K(\alpha)[X]$ das Minimalpolynom von β über $K(\alpha)$.

Wir wissen: m_β^K ist immer noch annullierend in $K(\alpha)[X]$, d.h. $m_\beta^{K(\alpha)} \mid m_\beta^K$. Nun ist β separabel über K, d.h. m_β^K hat keine doppelten Nullstellen. Dann kann aber auch $m_\beta^{K(\alpha)}$ keine doppelten Nullstellen haben! Folglich ist β auch separabel über $K(\alpha)$.

Mit (a) folgt, dass $K(\alpha)/K$ und $K(\alpha, \beta) = K(\alpha)(\beta)/K(\alpha)$ separabel sind, und dem Satz die Behauptung. □

8 Satz. *Sei* $\mathrm{char}(K) = p > 0$.

(a) Ist $f \in K[X]$ irreduzibel, so existiert ein $g \in K[X]$ irreduzibel und separabel mit

$$f = g(X^{p^k})$$

für ein $k \in \mathbb{N}_0$ und jede Nullstelle von f hat Vielfachheit p^k.

(b) Ist L/K endliche Körpererweiterung, dann

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

für ein $l \in \mathbb{N}_0$.

Beweisidee. (von (a)) Der interessante Fall ist der, dass das irreduzible $f = \sum a_i X^i$ nicht separabel ist. Dann sagt die Bemerkung oben dass $f' = 0$ gilt, d.h. $a_i = 0$ für $p \nmid i$ und f ist ein Polynom in X^p. Induktiv folgt die Behauptung, d.h.

$$f = e(X^{p^k} - a_1) \cdot \dots \cdot (X^{p^k} - a_m)$$

(mit paarweise verschiedenen a_i, denn g ist separabel, und dem Faktor $e = a_{\deg(f)}$).

Ist nun a eine Nullstelle von f, also z.B. $a^{p^k} = a_1$, dann gilt

$$(X - a)^{p^k} = X^{p^k} - a^{p^k} = X^{p^k} - a_1 \mid f$$

und a hat Vielfachheit p^k. □

9 Aufgabe. Sei $\mathrm{char}(K) = p > 0$, $f \in K[X]$ normiert. Zeige:

(a) $f = X^{p^n} - c$ für ein $n \in \mathbb{N}_0$, $c \in K \;\Rightarrow\; f$ hat genau eine Nullstelle in $\bar{K}$,
und $\Leftarrow$ gilt zumindest wenn f irreduzibel ist

(b) Es gibt reduzible und irreduzible Polynome mit genau einer Nullstelle in $\bar{K}$

(c) Sei L/K Körpererweiterung, $\alpha \in L$ algebraisch über K und das Minimalpolynom $m_\alpha \in K[X]$ habe genau eine Nullstelle in $\bar{K}$. Berechne $\mathrm{Hom}_K(K(\alpha), \bar{K})$.

Beweis. (a) ($\Rightarrow$) Ist $a \in \bar{K}$ eine der Nullstellen von $f = X^{p^n} - c$, dann gilt

$$(X - a)^{p^n} = X^{p^n} - a^{p^n} = X^{p^n} - c = f$$

und f hat *genau eine* Nullstelle.

($\Leftarrow$) Gilt im allgemeinen nicht, z.B. für $f = (X - 1)^2 \in \mathcal{F}_3[X]$. Für irreduzible Polynome folgt das mit dem Satz, denn ist $f = g(X^{p^k})$ mit g separabel, dann hatte ja jede Nullstelle VF p^k. Wenn es nur eine gibt, dann folgt also $\deg(f) = p^k$ und $\deg(g) = 1$, und somit die gewünschte Form für f.

(b) Aus der Vorlesung bekannt: Betrachte $K = \mathcal{F}_p(t)$, wobei t transzendent über $\mathcal{F}_p$ ist (z.B. X!). Dann ist $X^p - t$ irreduzibel in $K[X]$ (im wesentlichen mit Eisenstein, wenn man erkennt dass t prim ist!).

Andererseits ist $X^{p^k} + 1 = (X + 1)^{p^k}$ (offenbar) reduzibel über $\mathcal{F}_p[X]$.

(c) Es gibt genau einen K-Homomorphismus $\phi : K(\alpha) \to \bar{K}$; er schickt α auf die einzige Nullstelle des Minimalpolynoms, also auf α!

Folglich $\phi = \mathrm{id}_{K(\alpha)}$, und $\mathrm{Hom}_K(K(\alpha), \bar{K})$ ist die triviale Gruppe. □

10 Aufgabe. Sei $\operatorname{char}(K) = p > 0$, L/K Körpererweiterung, $\alpha \in L$ algebraisch über K. Zeige:

$$\alpha \text{ separabel} \quad \Leftrightarrow \quad K(\alpha) = K(\alpha^p)$$

Beweis. ($\Leftarrow$) Ist α nicht separabel, so existiert ein separables, irreduzibles Polynom $g \in K[X]$ und $k \in \mathbb{N}_+$ mit

$$m_\alpha = g(X^{p^k})$$

und $g(X^{p^{k-1}})$ ist annullierendes Polynom von α^p!

$$\Rightarrow [K(\alpha^p) : K] \leq \deg(g(X^{p^{k-1}})) = p^{k-1}\deg(g) < p^k \deg(g) = \deg(m_\alpha) = [K(\alpha) : K]$$

Also gilt $K(\alpha^p) \subsetneq K(\alpha)$.

($\Rightarrow$) Sei α separabel. Ist $\sigma \in \operatorname{Hom}_K(K(\alpha), \bar{K})$, dann gilt $\sigma|_{K(\alpha^p)} \in \operatorname{Hom}_K(K(\alpha^p), \bar{K})$.

Sei ferner $\tau \in \operatorname{Hom}_K(K(\alpha), \bar{K})$. Dann gilt:

$$\begin{aligned}
&\sigma|_{K(\alpha^p)} = \tau|_{K(\alpha^p)} \\
&\Rightarrow \sigma(\alpha^p) = \tau(\alpha^p) \\
&\Rightarrow 0 = \sigma(\alpha)^p - \tau(\alpha)^p = (\sigma(\alpha) - \tau(\alpha))^p \\
&\Rightarrow \sigma(\alpha) = \tau(\alpha) \\
&\Rightarrow \sigma = \tau
\end{aligned}$$

Also ist $\sigma \mapsto \sigma|_{K(\alpha^p)}$ eine Injektion, und

$$[K(\alpha) : K] = [K(\alpha) : K]_s \leq [K(\alpha^p) : K]_s \leq [K(\alpha^p) : K]$$

und wegen $K(\alpha^p) \subseteq K(\alpha)$ folgt $[K(\alpha) : K] = [K(\alpha^p) : K]$, d.h. $K(\alpha) = K(\alpha^p)$. □

11 Aufgabe (Trick für das ÜB)**.** Sei $\operatorname{char}(K) = p > 0$, $f = X^p - X - a \in K[X]$, $a \in K$, $x \in \bar{K}$ Zeige:

$$f(x) = 0 \quad \Rightarrow \quad f(x+1) = 0$$

Beweis.

$$f(x+1) = (x+1)^p - (x+1) - a = x^p - x - a + 1^p - 1 = f(x) = 0$$

□

12 Satz. *(vom primitiven Element) Sei L/K endlich und separabel. Dann ist L/K sogar einfach.*

Beweisidee. (nicht wirklich…) Ist L endlich, so ist L^x zyklisch und wir adjungieren einfach den Erzeuger.

Ist L unendlich, dann genügt es immerhin, die Behauptung für eine Erweiterung $L = K(\alpha_1, \alpha_2)$ zu zeigen, die allgemeine Behauptung für endliche Körpererweierungen folgt dann induktiv.

Vorlesung: Das primitive Element, d.h. das α mit $L = K(\alpha)$, hat die Form

$$\alpha = \alpha_1 + \lambda\alpha_2$$

für ein $\lambda \in K$. Ausprobieren klappt meistens, z.B. $\lambda = 1$! □

13 Aufgabe. Bestimme ein primitives Element von $\mathbb{Q}(\sqrt{2}, \sqrt{5})/\mathbb{Q}$.

Lösung. Rate $\alpha = \sqrt{2} + \sqrt{3} \in \mathbb{Q}(\sqrt{2}, \sqrt{5})$. Dann:

$$\begin{aligned}
\mathbb{Q}(\alpha) &\subseteq \mathbb{Q}(\sqrt{2}, \sqrt{5}) \\
\alpha^2 &= 7 + 2\sqrt{10} \\
\alpha^3 &= 17\sqrt{2} + 11\sqrt{5}
\end{aligned}$$

Aha! Damit gilt

$$\begin{aligned}
\sqrt{2} &= \frac{\alpha^3 - 11\alpha}{6} \in \mathbb{Q}(\alpha) \\
\Rightarrow &\sqrt{5} = \alpha - \sqrt{2} \in \mathbb{Q}(\alpha) \\
\Rightarrow &\mathbb{Q}(\sqrt{2}, \sqrt{5}) \subseteq \mathbb{Q}(\alpha)
\end{aligned}$$

□

2 Endliche Körper

14 Proposition. *Ist K Körper, so ist jede endliche Untergruppe von K^x zyklisch.*

15 Satz. *Sei $\mathcal{F}_{p^n}$ der Zerfällungskörper von $X^{p^n} - X \in \mathcal{F}_p[X]$, $n \in \mathbb{N}$. Dann gilt:*

(i) $\#\mathcal{F}_{p^n} = p^n$

(i) K *endlicher Körper* $\Rightarrow K \cong \mathcal{F}_{p^n}$ *für ein* $n \in \mathbb{N}$, $p = \mathrm{char}(K)$

16 Satz. *Jede algebraische Erweiterung eines endlichen Körpers ist separabel.*

17 Aufgabe. Zeige:

$$\mathcal{F}_{p^n} \subseteq \mathcal{F}_{p^m} \quad \Leftrightarrow \quad n \mid m$$

Beweis. ($\Rightarrow$) $\mathcal{F}_{p^m}$ ist dann $\mathcal{F}_{p^n}$-Vektorraum, also

$$\begin{aligned} p^m &= \#\mathcal{F}_{p^m} = (\#\mathcal{F}_{p^n})^{\dim_{\mathcal{F}_{p^n}}(\mathcal{F}_{p^m})} = (p^n)^{\dim_{\mathcal{F}_{p^n}}(\mathcal{F}_{p^m})} \\ \Rightarrow m &= n \cdot \dim_{\mathcal{F}_{p^n}}(\mathcal{F}_{p^m}) \\ \Rightarrow n &\mid m \end{aligned}$$

($\Leftarrow$) Wir wollen zeigen:

$$X^{p^n} - X \mid X^{p^m} - X$$

Dann wäre jede Nullstelle des linken auch Nullstelle des rechten Polynoms, d.h. $\mathcal{F}_{p^m}$ würde $\mathcal{F}_{p^n}$ enthalten (denn letztere sind ja gerade die jeweiligen Zerfällungskörper).

Sei also $n \cdot k = m$. Bekanntlich gilt in jedem kommutativen Ring, dass $x - 1 \mid x^k - 1$ (*)

$$\begin{aligned} &\overset{(*)}{\Rightarrow} p^n - 1 \mid (p^n)^k - 1 = p^m - 1 \\ &\Rightarrow \exists l \in \mathbb{N} : (p^n - 1) \cdot l = p^m - 1 \\ &\Rightarrow (X^{p^n - 1})^l = X^{p^m - 1} \\ &\overset{(*)}{\Rightarrow} X^{p^n - 1} - 1 \mid (X^{p^n - 1})^l - 1 = X^{p^m - 1} - 1 \\ &\Rightarrow X^{p^n} - X \mid X^{p^m} - X \end{aligned}$$

□

18 Aufgabe. Verstehe $\mathcal{F}_4$.

Beweis. $\mathcal{F}_4$ ist nach Definition der Zerfällungskörper des Polynoms

$$X^4 - X = X(X-1) \underbrace{(X^2 + X + 1)}_{\text{irreduzibel, keine NST!}} \in \mathcal{F}_2[X]$$

Adjungiere Nullstelle α von $X^2 + X + 1$ (Kronecker-Konstruktion)

$$\begin{aligned} &[\mathcal{F}_2(\alpha) : \mathcal{F}_2] = \deg(X^2 + X + 1) = 2 \\ \Rightarrow &\#\mathcal{F}_2(\alpha) = 2^2 = 4 \\ \Rightarrow &\mathcal{F}_2(\alpha) \cong \mathcal{F}_4 \end{aligned}$$

Wir wissen auch, dass $\{1, \alpha\}$ eine $\mathcal{F}_2$-Basis von $\mathcal{F}_4$ ist.

Man stellt dann unter Ausnutzung von $\alpha^2 + \alpha + 1 = 0$ und $-x = x$ in $\mathcal{F}_2$ leicht folgende Additions- und Multiplikationstabelle auf:

$+$	0	1	α	$\alpha+1$
0	0	1	α	$\alpha+1$
1	1	0	$\alpha+1$	α
α	α	$\alpha+1$	0	1
$\alpha+1$	$\alpha+1$	α	1	0

Die additive Gruppe von $\mathcal{F}_4$ ist also isomorph zu $\mathcal{F}_2^2$, was zu erwarten war — $\mathcal{F}_4$ ist ja $\mathcal{F}_2$-Vektorraum der Dimension 2!

$\cdot$	1	α	$\alpha+1$
1	1	α	$\alpha+1$
α	α	$\alpha+1$	1
$\alpha+1$	$\alpha+1$	1	α

Und die Einheitengruppe $\mathcal{F}_4^x$ ist zyklisch; das bestätigt die Proposition von oben. $\square$