KAPITEL 5

Separable Körpererweiterungen

1. Differenzieren von Polynomen

In der Analysis kennt man Formeln für das Differenzieren von Polynomen mit Koeffizienten aus $\mathbb{R}$. Diese Formeln kann man benutzen, um „Differenzieren“ für Polynome mit Koeffizienten aus einem beliebigen Körper einzuführen.

DEFINITION. *Ist K ein Körper und $f \in K[x]$ ein Polynom mit*

$$f(x) = a_0 + a_1 x + a_2 x^2 + \cdots + a_n x^n = \sum_{i=0}^{n} a_i x^i,$$

so definiert man die **Ableitung** *f' von f durch*

$$f'(x) = a_2 + 2a_2 x + \cdots + (n-1)a_n x^{n-1} = \sum_{i=1}^{n} i a_i x^{i-1}.$$

Die bekannten Ableitungsregeln gelten auch hier:

SATZ. *Ist K ein Körper, sind $f, g \in K[x]$ und $a, b \in K$, so gilt:*

(1) *(Summenregel) $(af + bg)'(x) = af'(x) + bg'(x)$.*
(2) *(Produktregel) $(fg)'(x) = f'(x)g(x) + f(x)g'(x)$.*
(3) *(Kettenregel) Ist $h(x) = f(g(x))$, so gilt $h'(x) = f'(g(x))g'(x)$.*

Beweis: Sei $f = \sum_{i=0}^{n} a_i x^i$ und $g = \sum_{j=0}^{m} b_j x^j$. Bei Bedarf können wir auch $n = m$ annehmen, indem wir $a_{n+1} = a_{n+2} = \cdots = 0$ oder $b_{m+1} = b_{m+2} = \cdots = 0$ ergänzen.

(1) Es ist

$$\begin{aligned}(af(x) + b(x))' &= (a\sum_{i\geq 0} a_i x^i + b\sum_{i\geq 0} b_i x^i)' = (\sum_{i\geq 0}(aa_i + bb_i)x^i)' = \sum_{i\geq 1} i(aa_i + bb_i)x^{i-1} = \\ &= a\sum_{i\geq 1} i a_i x^{i-1} + b\sum_{i\geq 1} i b_i x^{i-1} = af'(x) + bg'(x).\end{aligned}$$

Dies beweist die Summenformel.

(2) Es gilt

$$f(x)g(x) = (\sum_{i\geq 0} a_i x^i)(\sum_{j\geq 0} b_j x^j) = \sum_{k\geq 0}(\sum_{\substack{k=i+j \\ i\geq 0 \\ j\geq 0}} a_i b_j)x^k.$$

Datei: kt_sep.tex. Version vom 5.6.2023

Damit erhalten wir

$$\begin{aligned}
f'(x)g(x)+f(x)g'(x) &= (\sum_{i\geq 1} ia_ix^{i-1})(\sum_{j\geq 0} b_jx^j)+(\sum_{i\geq 0} a_ix^i)(\sum_{j\geq 1} jb_jx^{j-1}) = \\
&= \sum_{i\geq 1}\sum_{j\geq 0} ia_ib_jx^{i+j-1}+\sum_{i\geq 0}\sum_{j\geq 1} ja_ib_jx^{i+j-1} = \\
&= \sum_{k\geq 1}(\sum_{\substack{k=i+j\\ i\geq 1\\ j\geq 0}} ia_ib_j)x^{k-1}+\sum_{k\geq 1}(\sum_{\substack{k=i+j\\ i\geq 0\\ j\geq 1}} ja_ib_j)x^{k-1} = \\
&= \sum_{k\geq 1}(\sum_{\substack{k=i+j\\ i\geq 0\\ j\geq 0}} ia_ib_j)x^{k-1}+\sum_{k\geq 1}(\sum_{\substack{k=i+j\\ i\geq 0\\ j\geq 0}} ja_ib_j)x^{k-1} = \\
&= \sum_{k\geq 1} k(\sum_{\substack{k=i+j\\ i\geq 0\\ j\geq 0}} a_ib_j)x^{k-1} = \Big(\sum_{k\geq 1}(\sum_{\substack{k=i+j\\ i\geq 0\\ j\geq 0}} a_ib_j)x^k\Big)' = \\
&= \Big(\sum_{k\geq 0}(\sum_{\substack{k=i+j\\ i\geq 0\\ j\geq 0}} a_ib_j)x^k\Big)' = \Big((\sum_{i\geq 0} a_ix^i)(\sum_{j\geq 0} b_jx^j)\Big)' = \Big(f(x)g(x)\Big)'.
\end{aligned}$$

Dies beweist die Produktformel.

(3)
- Wir beweisen zunächst durch Induktion, dass für $i \geq 1$

$$\big(g(x)^i\big)' = ig(x)^{i-1}g'(x)$$

gilt.
Für $i = 1$ folgt die Aussage mit der üblichen Konvention $g(x)^0 = 1$.
Sei nun $i \geq 1$ und die Aussage bereits für $g(x)^i$ bezeigt. Mit der Produktregel folgt:

$$\begin{aligned}
\big(g(x)^{i+1}\big)' &= \big(g(x)^i\big)'g(x)+g(x)^ig'(x) = ig(x)^{i-1}g'(x)g(x)+g(x)^ig'(x) = \\
&= (i+1)g(x)^ig'(x).
\end{aligned}$$

Dies beweist die Behauptung.
- Sei nun $f(x) = \sum_{i=0}^n a_ix^i$. Mit $f'(x) = \sum_{i=1}^n ia_ix^{i-1}$ und der Summenregel ergibt sich dann

$$\begin{aligned}
(f(g(x)))' &= \left(\sum_{i=0}^n a_ig(x)^i\right)' = \sum_{i=1}^n a_i\big(g(x)^i\big)' = \sum_{i=1}^n a_i\cdot ig(x)^{i-1}g'(x) = \\
&= \left(\sum_{i=1}^n ia_ig(x)^{i-1}\right)g'(x) = f'(g(x))g'(x),
\end{aligned}$$

wie behauptet. ■

Der folgende Satz zeigt einen wichtigen Unterschied zwischen Körpern der Charakteristik 0 und der Charakteristik p.

Satz. *Sei K ein Körper und $f \in K[x]$. Dann gilt:*

(1) *Ist* $\mathrm{char}(K) = 0$, *so gilt*

$$f' = 0 \quad \Longleftrightarrow \quad f \in K, \text{ d.h. } f \text{ ist konstant.}$$

(2) *Ist* $\mathrm{char}(K) = p$, *so gilt*

$$f' = 0 \quad \Longleftrightarrow \quad f(x) = g(x^p) \text{ für ein Polynom } g \in K[x].$$

Beweis: Sei $f = \sum_{i=0}^{n} a_i x^i$, wobei wir o.E. $n \geq 1$ annehmen können. Dann ist

$$f' = \sum_{i=1}^{n} i a_i x^{i-1} = a_1 + 2a_2 x + 3a_3 x^2 + 4a_4 x^3 + n a_n x^{n-1}.$$

(1) Im Fall $\mathrm{char}(K) = 0$ gilt:

$$f' = 0 \iff ia_i = 0 \text{ für alle } i \in \{1, \ldots, n\} \iff a_i = 0 \text{ für alle } i \in \{1, \ldots, n\} \iff$$
$$\iff f \in K.$$

(2) Im Fall $\mathrm{char}(K) = p$ gilt:

$$\begin{aligned} f' = 0 &\iff ia_i = 0 \text{ für alle } i \in \{1, \ldots, n\} \iff \\ &\iff ia_i = 0 \text{ für alle } i \in \{1, \ldots, n\} \text{ mit } p \nmid i \iff \\ &\iff a_i = 0 \text{ für alle } i \in \{1, \ldots, n\} \text{ mit } p \nmid i \iff \\ &\iff f = \sum_{j \geq 0} a_{pj} x^{pj} = \sum_{j \geq 0} a_{pj} (x^p)^j \iff \\ &\iff f(x) = g(x^p) \text{ mit } g(x) = \sum_{j \geq 0} a_{pj} x^j. \end{aligned}$$

2. Separable Polynome

DEFINITION. *Sei K ein Körper mit algebraischem Abschluss $\overline{K}$ und $f \in K[x]$ ein Polynom vom Grad ≥ 1. Über $\overline{K}$ erhalten wir dann eine Zerlegung*

$$f = c(x - \alpha_1)^{e_1} \ldots (x - \alpha_r)^{e_r}$$

mit paarweise verschiedenen Zahlen $\alpha_1, \ldots, \alpha_r \in \overline{K}$ und $e_1, \ldots, e_r \in \mathbb{N}$ und $c \in K^*$.

(1) *Man sagt, die Nullstelle α_i ist* **einfach**, *wenn $e_i = 1$ gilt.*
(2) *Man sagt, α_i ist eine* **mehrfache Nullstelle** *von f, wenn $e_i \geq 2$ gilt.*
(3) *Sind alle Nullstellen von f einfach, so nennt man f* **separabel**.
(4) *Ein Polynom mit mehrfachen Nullstellen nennt man auch* **inseparabel**.

Beispiel: Das Polynom $f = x^2 - x = x(x-1)$ ist separabel, das Polynom $g = x^3 - x^2 = x^2(x-1)$ ist nicht separabel.

Man kann einem Polynom schon über dem Grundkörper „ansehen“, ob es separabel ist oder nicht.

SATZ. *Sei $f \in K[x]$ ein Polynom vom Grad ≥ 1. Dann gilt:*

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

Beweis:

- $\Longrightarrow$ Sei f separabel. Dann gibt es paarweise verschiedene $\alpha_1, \ldots, \alpha_n \in \overline{K}$ mit

$$f = c(x - \alpha_1) \ldots (x - \alpha_n) = c \prod_{i=1}^{n} (x - \alpha_i).$$

Es folgt

$$f' = c \sum_{i=1}^{n} \prod_{\substack{1 \leq j \leq n \\ j \neq i}} (x - \alpha_j),$$

und damit

$$f'(\alpha_k) = c \sum_{i=1}^{n} \prod_{\substack{1 \leq j \leq n \\ j \neq i}} (\alpha_k - \alpha_j) = c \prod_{\substack{1 \leq j \leq n \\ j \neq k}} (\alpha_k - \alpha_j) \neq 0.$$

Also gilt $x - \alpha_k \nmid f'$ für alle k, und damit

$$\mathrm{ggT}(f, f') = 1.$$

- $\Longleftarrow$ Wir nehmen an, f wäre nicht separabel. Dann hätte f eine mehrfache Nullstelle α im algebraischen Abschluss. Wir können dann zerlegen $f(x) = (x-\alpha)^2 g(x)$ mit einem Polynom $g \in \overline{K}[x]$. Es folgt

$$f'(x) = 2(x-\alpha)g(x) + (x-\alpha)^2 g'(x) = (x-\alpha)\cdot(2g(x) + (x-\alpha)g'(x))\,,$$

also $x-\alpha \mid f$ und $x-\alpha \mid f'$, was insbesondere

$$\mathrm{ggT}(f, f') \neq 1$$

liefert, ein Widerspruch zu Voraussetzung $\mathrm{ggT}(f,f') = 1$. Die Annahme war also falsch, d.h. f ist separabel. ■

Beispiele: Für $f = x^2 - x = x(x-1)$ gilt $f' = 2x - 1 = 2(x - \frac{1}{2})$, also ist $\mathrm{ggT}(f,f') = 1$. Für $g = x^3 - x^2 = x^2(x-1)$ gilt $g' = 3x^2 - 2x = 3x(x - \frac{2}{3})$, also ist $\mathrm{ggT}(f,f') = x \neq 1$.

Die Situation wird noch einfacher, wenn man irreduzible Polynome anschaut:

Satz. *Sei $f \in K[x]$ ein irreduzibles Polynom. Dann gilt:*

$$f \text{ separabel} \quad \Longleftrightarrow \quad f' \neq 0.$$

Beweis: Wir unterscheiden zwei Fälle:

- **Fall $f' = 0$:** Dann gilt $\mathrm{ggT}(f,f') = f \neq 1$. Nach dem letzten Satz ist dann f nicht separabel.
- **Fall $f' \neq 0$:** Dann ist $0 \leq \mathrm{grad}(f') \leq \mathrm{grad}(f) - 1$. Da f als normierte Teiler nur 1 und f hat, bleibt nur die Möglichkeit $\mathrm{ggT}(f,f') = 1$. Nach dem letzten Satz ist f separabel.

Es folgt die Behauptung. ■

Satz. *Hat K Charakteristik 0, so ist jedes irreduzible Polynom separabel.*

Beweis: Sei $f = a_n x^n + a_{n-1}x^{n-1} + \cdots \in K[x]$ mit $n \geq 1$ und $a_n \neq 0$. Dann gilt

$$f' = n a_n x^{n-1} + \ldots$$

Wegen $\mathbb{Q} \subseteq K$ ist $n \neq 0$ in K, also auch $n a_n \neq 0$, was $f' \neq 0$ und damit nach dem vorangegangenen Satz die Separabilität von f liefert. ■

Satz. *Ist K ein endlicher Körper, so ist jedes irreduzible Polynom separabel.*

Beweis: Sei $f \in K[x]$ irreduzibel und normiert. Sei $\alpha \in \overline{K}$ eine Nullstelle von f, sodass f das Minimalpolynom von α über K ist. Sei $p^d = |K(\alpha)|$. Dann gilt $\alpha^{p^d} = \alpha$, d.h. α ist Nullstelle des Polynoms $x^{p^d} - x$. Es folgt

$$f(x) \mid x^{p^d} - x.$$

Nun ist aber $x^{p^d} - x$ separabel wegen

$$\left(x^{p^d} - x\right)' = -1 \neq 0.$$

Daher ist auch f separabel, was gezeigt werden sollte. ■

Bemerkung: Im letzten Beweis haben wir die offensichtliche Aussage benutzt, dass Teiler separabler Polynome separabel sind.

Definition. *Ein Körper K heißt* **vollkommen**, *wenn jedes irreduzible Polynom aus $K[x]$ separabel ist.*

Beispiel: Körper der Charakteristik 0 und endliche Körper sind vollkommen.

Beispiel: Der Quotientenkörper $\mathbb{F}_p(t)$ des Polynomrings $\mathbb{F}_p[t]$ ist nicht vollkommen. Da t ein Primelement in $\mathbb{F}_p[t]$ ist, ist $x^p - t \in \mathbb{F}_p(t)[x]$ nach Eisenstein irreduzibel. Das Polynom hat aber Ableitung 0, ist also nicht separabel.

Man kann die Vollkommenheit eines Körpers der Charakteristik p auch noch anders charakterisieren:

SATZ. *Sei K ein Körper der Charakteristik p. Dann gilt:*

$$K \text{ ist vollkommen} \quad \Longleftrightarrow \quad K^p = K,$$

wobei $K^p = \{a^p : a \in K\}$.

Beweis:

- $\Longrightarrow$ Da $K^p \subseteq K$ gilt, müssen wir noch die umgekehrte Inklusion zeigen. Sei also $a \in K$. Wir wollen zeigen, dass $a \in K^p$ gilt. Sei $\alpha \in \overline{K}$ mit $\alpha^p = a$. Sei $f \in K[x]$ das Minimalpolynom von α über K. Nach Voraussetzung ist f irreduzibel und separabel. α ist auch Nullstelle des Polynoms $g = x^p - a \in K[x]$. Also gilt $f \mid g$. Nun ist aber $g = x^p - \alpha^p = (x - \alpha)^p$. Da $f \mid g$ gilt und f separabel ist, folgt $f = x - \alpha$, also $\alpha \in K$. Es folgt $a \in K^p$, was wir zeigen wollten.
- $\Longleftarrow$ Sei $f \in K[x]$ ein irreduzibles Polynom. Wir müssen zeigen, dass f separabel ist. Angenommen, f ist nicht separabel. Dann ist $f' = 0$, es gibt also ein Polynom $g \in K[x]$ mit $f(x) = g(x^p)$. Sei $g = \sum_i a_i x^i$. Wegen $a_i \in K = K^p$ gibt es $b_i \in K$ mit $a_i = b_i^p$. Es folgt

  $$f(x) = g(x^p) = \sum_{i \geq 0} a_i x^{pi} = \sum_{i \geq 0} b_i^p x^{pi} = \sum_{i \geq 0} (b_i x^i)^p = \Big(\sum_{i \geq 0} b_i x^i \Big)^p.$$

  Also ist f reduzibel, im Widerspruch zur Voraussetzung. Die Annahme war also falsch, d.h. f ist separabel. ■

3. Separable Körpererweiterungen

DEFINITION. *Sei $L|K$ eine algebraische Körpererweiterung.*

(1) *Ein Element $\alpha \in L$ heißt* **separabel über** *K, wenn das Minimalpolynom $m_{\alpha,K} \in K[x]$ separabel ist.*
(2) *L heißt* **separabel über** *K, wenn jedes Element $\alpha \in L$ separabel über K ist.*

Der folgende Satz ergibt sich direkt aus den vorangegangenen Überlegungen:

SATZ. *Ist K vollkommen, so ist jede algebraische Erweiterung L separabel über K. Insbesondere ist dies der Fall, wenn K Charakteristik 0 hat oder ein endlicher Körper ist.*

Der folgende Satz gibt es einfaches Kriterium für eine separable Körpererweiterung in Charakteristik p.

SATZ. *Sei $L|K$ eine endliche Körpererweiterung und* $\mathrm{char}(K) = p$. *Dann gilt:*

$$p \nmid [L : K] \quad \Longrightarrow \quad L|K \text{ separabel.}$$

Beweis: Angenommen, $L|K$ ist nicht separabel. Dann gibt es ein $\alpha \in L$, sodass α über K nicht separabel ist. Ist also $f \in K[x]$ das Minimalpolynom von α, so ist f nicht separabel. Daher ist $f' = 0$. Also gibt es ein Polynom $g \in K[x]$ mit $f(x) = g(x^p)$. Es folgt

$$[K(\alpha) : K] = \mathrm{grad}(f) = p \cdot \mathrm{grad}(g),$$

woraus natürlich sofort $p \mid [L : K]$ folgt, im Widerspruch zur Voraussetzung. Die Annahme ist also falsch, die Behauptung also richtig. ■

4. Der Satz vom primitiven Element II

Wir haben einen „Satz vom primitiven Element“ in folgender Form kennengelernt: Ist $L|K$ eine endliche Körpererweiterung mit nur endlich vielen Zwischenkörpern E, so gibt es ein $\alpha \in L$ mit $L = K(\alpha)$. Wir werden jetzt eine andere Variante kennenlernen, die praktisch bedeutsamer ist.

LEMMA. *Sei $L|K$ eine algebraische Erweiterung und $\alpha, \beta \in L$ separable Elemente mit Minimalpolynomen $f = m_{\alpha,K} \in K[x]$ und $g = m_{\beta,K} \in K[x]$. Sei M ein Oberkörper von L, über dem f und g in Linearfaktoren zerfallen:*

$$f(x) = (x-\alpha)(x-\alpha_2)\dots(x-\alpha_m) \quad \text{und} \quad g(x) = (x-\beta)(x-\beta_2)\dots(x-\beta_n),$$

also $\alpha_2, \dots, \alpha_m, \beta_2, \dots, \beta_n \in M$. (Da α und β separabel über K sind, sind die Elemente $\alpha, \alpha_2, \dots, \alpha_m$ paarweise verschieden, ebenso die Elemente $\beta, \beta_2, \dots, \beta_n$.) Sei

$$A = \{\frac{\alpha - \alpha_i}{\beta_j - \beta} : 2 \le i \le m, 2 \le j \le n\} \cup \{0\}.$$

Dann gilt für jedes Element $c \in K \setminus A$

$$K(\alpha, \beta) = K(\alpha + c\beta).$$

Beweis:

(1) Für $c \in K$ betrachten wir

$$\gamma_c = \alpha + c\beta \quad \text{und} \quad h_c(x) = f(\gamma_c - cx) \in M[x].$$

Natürlich gilt $K(\gamma_c) \subseteq K(\alpha, \beta)$. Außerdem gilt $h_c(x) \in K(\gamma_c)[x]$.

(2) Es ist

$$\begin{aligned} h_c(x) &= f(\gamma_c - cx) = f(\alpha + c\beta - cx) = \\ &= ((\alpha + c\beta - cx) - \alpha) \cdot \prod_{i=2}^{m}((\alpha + c\beta - cx) - \alpha_i) = \\ &= c(\beta - x) \cdot \prod_{i=2}^{m}((\alpha - \alpha_i) - c(x - \beta)), \end{aligned}$$

also

$$h_c(\beta) = 0$$

und für $2 \le j \le n$

$$\begin{aligned} h_c(\beta_j) &= c(\beta - \beta_j) \prod_{i=2}^{m}((\alpha - \alpha_i) - c(\beta_j - \beta)) = \\ &= c(\beta - \beta_j)(\beta_j - \beta)^{m-1} \prod_{i=2}^{m}(\frac{\alpha - \alpha_i}{\beta_j - \beta} - c) = \\ &= -c(\beta_j - \beta)^m \prod_{i=2}^{m}(\frac{\alpha - \alpha_i}{\beta_j - \beta} - c). \end{aligned}$$

Ist also $c \notin A$, so gilt

$$h_c(\beta_j) \neq 0 \text{ für } 2 \le j \le n.$$

(3) Sei $c \in K \setminus A$. Dann ist

$$g(x) = (x-\beta)(x-\beta_2)\dots(x-\beta_n), \quad h_c(\beta) = 0 \quad \text{und} \quad h_c(\beta_j) \neq 0 \text{ für } 2 \le j \le n,$$

und somit in $M[x]$

$$\mathrm{ggT}(g(x), h_c(x)) = x - \beta.$$

Nun sind $g(x), h_c(x) \in K(\gamma_c)[x]$. Da die ggT-Berechnung in dem Körper bleibt, über dem die Polynome definiert sind, folgt

$$x - \beta \in K(\gamma_c)[x], \quad \text{also} \quad \beta \in K(\gamma_c).$$

Aus $\alpha = \gamma_c - c\beta$ folgt dann auch $\alpha \in K(\gamma_c)$, und damit $K(\alpha, \beta) \subseteq K(\gamma_c)$. Da wir zuvor schon $K(\gamma_c) \subseteq K(\alpha, \beta)$ bemerkt haben, folgt

$$K(\alpha, \beta) = K(\gamma_c).$$

Dies wollten wir zeigen. ■

Beispiel: Seien $m, n \in \mathbb{Q}^* \setminus \mathbb{Q}^{*2}$, sodass gilt $mn \notin \mathbb{Q}^{*2}$. Seien $\alpha, \beta \in \mathbb{C}$ mit

$$\alpha^2 = m, \quad \beta^2 = n.$$

Dann ist

$$\alpha_2 = -\alpha \quad \text{und} \quad \beta_2 = -\beta$$

und

$$\frac{\alpha - \alpha_2}{\beta_2 - \beta} = \frac{\alpha + \alpha}{-\beta - \beta} = -\frac{\alpha}{\beta},$$

also

$$A = \{-\frac{\alpha}{\beta}, 0\}.$$

Wäre $-\frac{\alpha}{\beta} \in \mathbb{Q}$, so wäre $\frac{m}{n} = (-\frac{\alpha}{\beta})^2 \in \mathbb{Q}^{*2}$, also auch $mn = \frac{m}{n} \cdot n^2 \in \mathbb{Q}^{*2}$, was wir ausgeschlossen hatten. Daher gilt

$$A \cap \mathbb{Q} = \{0\}.$$

Daher gilt

$$\mathbb{Q}(\alpha, \beta) = \mathbb{Q}(\alpha + c\beta) \text{ für alle } c \in \mathbb{Q} \setminus \{0\}.$$

Schreiben wir $\sqrt{m}$ für α und $\sqrt{n}$ für β, so gilt also

$$\mathbb{Q}(\sqrt{m}, \sqrt{n}) = \mathbb{Q}(\sqrt{m} + c\sqrt{n}) \text{ für alle } c \in \mathbb{Q} \setminus \{0\}.$$

Wie zuvor bei der ersten Version des Satzes vom primitiven Element ergibt sich folgender Satz:

Satz (Satz vom primitiven Element II). *Sei $L|K$ eine endliche separable Körpererweiterung.*

(1) *Dann gibt es ein $\alpha \in L$ mit*
$$L = K(\alpha).$$

(2) *Sind $\alpha_1, \ldots, \alpha_n \in L$ mit*
$$L = K(\alpha_1, \ldots, \alpha_n),$$
so gibt es $c_2, \ldots, c_n \in K$ mit
$$L = K(\alpha_1 + c_2\alpha_2 + \cdots + c_n\alpha_n).$$

Folgerung. *Ist $L|K$ eine endliche Körpererweiterung und*

- *K vollkommen oder*
- *K endlich oder*
- *$\mathrm{char}(K) = 0$,*

so gibt es ein $\alpha \in L$ mit

$$L = K(\alpha).$$

Wir geben noch eine weitere Folgerung an.

Folgerung. *Ist $L|K$ eine (nicht notwendig endliche) separable algebraische Körpererweiterung, sodass ein $n \in \mathbb{N}$ existiert mit*

$$[K(\beta) : K] \leq n \text{ für alle } \beta \in L,$$

so gilt $[L : K] \leq n$ und es existiert ein $\alpha \in L$ mit $L = K(\alpha)$.

Beweis: Wir können o.E. n minimal wählen mit der angegebenen Eigenschaft, d.h.

$$n = \max\{[K(\beta) : K] : \beta \in L\}.$$

Sei $\alpha \in L$ mit $[K(\alpha) : K] = n$. Sei nun $\beta \in L$ beliebig. Wäre $\beta \notin K(\alpha)$, so wäre $[K(\alpha, \beta) : K] > n$, andererseites gäbe es nach dem Satz vom primitiven Element ein $\gamma \in L$ mit $K(\alpha, \beta) = K(\gamma)$. Dann wäre aber $[K(\gamma) : K] = [K(\alpha, \beta) : K] > n$, im Widerspruch zur Definition von n. Also gilt $\beta \in L$, und damit $L \subseteq K(\alpha)$, also $L = K(\alpha)$. ■

Bemerkung: Verzichtet man auf die Voraussetzung „separabel“, so muss die Aussage nicht mehr stimmen. Sind beispielsweise x, y Unbestimmte über $\mathbb{F}_p$, setzt man $K = \mathbb{F}_p(x^p, y^p)$ und $L = \mathbb{F}_p(x, y)$, so gilt $[L : K] = p^2$, aber $[K(\beta) : K] \in \{1, p\}$ für alle $\beta \in L$.

5. Separabilitätsgrad

Vorbemerkung: Ist α separabel über einem Körper K, so ist zunächst nicht klar, warum alle Elemente von $K(\alpha)$ separabel über K sind. Um dies zu zeigen, werden wir wieder Körperhomomorphismen betrachten.

DEFINITION. *Für eine algebraische Körpererweiterung $L|K$ werde definiert*

$$\mathrm{Hom}_K(L, \overline{K}) = \{\sigma : L \to \overline{K} \text{ ist } K\text{-Homomorphismus}\}.$$

Der **Separabilitätsgrad** $[L : K]_s$ *wird definiert als*

$$[L : K]_s = |\mathrm{Hom}_K(L, \overline{K})|.$$

SATZ. *Sei K ein Körper und α algebraisch über K mit Minimalpolynom $f \in K[x]$. Seien $\alpha_1, \ldots, \alpha_r \in \overline{K}$ die paarweise verschiedenen Nullstellen von f im algebraischen Abschluss $\overline{K}$.*

(1) *Dann ist*
$$\mathrm{Hom}_K(K(\alpha), \overline{K}) = \{\sigma_1, \ldots, \sigma_r\},$$
wobei σ_i durch $\sigma_i(\alpha) = \alpha_i$ gegeben ist. Es ist also
$$[K(\alpha) : K]_s = r.$$
(2) *Es gilt $[K(\alpha) : K]_s \leq [K(\alpha) : K]$.*
(3) *Es gilt*
$$\alpha \text{ separabel über } K \quad \Longleftrightarrow \quad [K(\alpha) : K]_s = [K(\alpha) : K].$$

Beweis:

(1) Dies haben wir bereits gesehen, als wir die K-Homomomorphismen $K(\alpha) \to \overline{K}$ beschrieben haben.
(2) Da f höchstens soviele verschiedenen Nullstellen hat, wie der Grad angibt, gilt $r \leq n$, also $[K(\alpha) : K]_s \leq [K(\alpha) : K]$.
(3) α ist genau dann separabel, wenn das Minimalpolynom separabel ist, wenn also $r = n$ gilt. Dies ist aber äquivalent mit $[K(\alpha) : K]_s = [K(\alpha) : K]$. ■

Sind $K \subseteq L \subseteq M$ Körpererweiterungen, so kennen wir die Dimensionsformel/Gradformel

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

Wir werden zeigen, dass eine entsprechende Formel auch für den Separabilitätsgrad gilt.

SATZ. *Seien $K \subseteq L \subseteq M \subseteq \overline{K}$ algebraische Körpererweiterungen und*

$$\mathrm{Hom}_K(L, \overline{K}) = \{\sigma_i : i \in I\}, \quad \mathrm{Hom}_L(M, \overline{K}) = \{\tau_j : j \in J\}.$$

Wir setzen die K-Homomorphismen $\sigma_i : L \to \overline{K}$ irgendwie zu K-Homomorphismen $\widetilde{\sigma}_i : \overline{K} \to \overline{K}$ fort. Dann gilt

$$\mathrm{Hom}_K(M, \overline{K}) = \{\widetilde{\sigma}_i \circ \tau_j : i \in I, j \in J\},$$

wobei die Elemente $\widetilde{\sigma}_i \circ \tau_j$ paarweise verschieden sind.

Beweis:

- Sei $\widetilde{\sigma} : \overline{K} \to \overline{K}$ und $\tau_j : M \to \overline{K}$ gegeben. Dann ist $\widetilde{\sigma}_i \circ \tau_j : M \to \overline{K}$ und für $a \in K$ gilt
$$(\widetilde{\sigma}_i \circ \tau_j)(a) = \widetilde{\sigma}_i(\tau_j(a)) = \widetilde{\sigma}_i(a) = \sigma_i(a) = a,$$
also gilt
$$\widetilde{\sigma}_i \circ \tau_j \in \mathrm{Hom}_K(M, \overline{K}).$$
- Sei $\rho \in \mathrm{Hom}_K(M, \overline{K})$ gegeben. Dann gilt natürlich $\rho|_L \in \mathrm{Hom}_K(L, \overline{K})$, also gibt es ein σ_i mit $\rho|_L = \sigma_i = \widetilde{\sigma}_i|_L$. Daher ist $\widetilde{\sigma}_i^{-1} \circ \rho$ die Identität auf L. Wir können $\widetilde{\sigma}_i^{-1} \circ \rho$ also als Element von $\mathrm{Hom}_L(M, \overline{K})$ auffassen. Es gibt daher ein τ_j mit $\widetilde{\sigma}_i^{-1} \circ \rho = \tau_j$. Es folgt
$$\rho = \widetilde{\sigma}_i \circ \tau_j.$$
- Es gelte
$$\widetilde{\sigma}_{i_1} \circ \tau_{j_1} = \widetilde{\sigma}_{i_2} \circ \tau_{j_2}.$$
Für alle $\alpha \in L$ folgt wegen $\tau_{j_1}(\alpha) = \alpha$ und $\tau_{j_2}(\alpha) = \alpha$
$$\sigma_{i_1}(\alpha) = \widetilde{\sigma}_{i_1}(\alpha) = (\widetilde{\sigma}_{i_1} \circ \tau_{j_1})(\alpha) = (\widetilde{\sigma}_{i_2} \circ \tau_{j_2})(\alpha) = \widetilde{\sigma}_{i_2}(\alpha) = \sigma_{i_2}(\alpha),$$
also $\sigma_{i_1} = \sigma_{i_2}$. Daraus folgt $\widetilde{\sigma}_{i_1} = \widetilde{\sigma}_{i_2}$ und daraus sofort $\tau_{j_1} = \tau_{j_2}$. ■

Aus dem letzten Satz folgt sofort:

SATZ. *Seien $K \subseteq L \subseteq M \subseteq \overline{K}$ algebraische Körpererweiterungen. Dann gilt für die Separabilitätsgrade*
$$[M : K]_s = [M : L]_s \cdot [L : K]_s.$$

Damit können wir nun separable Körpererweiterungen gut charakterisieren.

SATZ. *Sei $L|K$ eine endliche Körpererweiterung. Dann sind äquivalent:*

(1) *$L|K$ ist separabel.*
(2) *Es gibt ein über K separables Element $\alpha \in L$ mit $L = K(\alpha)$.*
(3) $[L : K]_s = [L : K]$.

Beweis:

- (1)$\Longrightarrow$(2) Das folgt aus dem Satz vom primitiven Element.
- (2)$\Longrightarrow$(3) Dies wurde im letzten Satz gezeigt:
$$[L : K]_s = [K(\alpha) : K]_s = [K(\alpha) : K] = [L : K].$$
- (3)$\Longrightarrow$(1) Sei $\beta \in L$ ein beliebiges Element. Wir müssen zeigen, dass β separabel über K ist. Es ist
$$[K(\beta) : K]_s \leq [K(\beta) : K], \quad [L : K(\beta)]_s \leq [L : K(\beta)]$$
und
$$[L : K] = [L : K]_s = [L : K(\beta)]_s \cdot [K(\beta) : K]_s \leq [L : K(\beta)] \cdot [K(\beta) : K] = [L : K],$$
woraus sofort
$$[L : K(\beta)]_s = [L : K(\beta)] \quad \text{und} \quad [K(\beta) : K]_s = [K(\beta) : K]$$
folgt. Daher ist β separabel über K, wie behauptet. ■

SATZ. *Seien $K \subseteq L \subseteq M$ algebraische Körpererweiterungen. Dann gilt:*
$$M|K \text{ ist separabel} \quad \Longleftrightarrow \quad M|L \text{ und } L|K \text{ sind separabel.}$$

Beweis:

- $\Longrightarrow$ Dies folgt schnell aus der Tatsache, dass Teiler separabler Polynome wieder separabel sind.
- $\Longleftarrow$ Ist $M|K$ endlich, so folgt aus $[M : L]_s = [M : L]$ und $[L : K]_s = [L : K]$ sofort $[M : K]_s = [M : K]$, was zeigt, dass $M|K$ separabel ist. Auf den Beweis der allgemeinen Aussage verzichten wir hier. ■

Bemerkung: Ist $L|K$ eine algebraische Körpererweiterung, so kann man nun einfach zeigen, dass

$$L_{\text{sep}} = \{\alpha \in L : \alpha \text{ separabel über } K\}$$

ein Unterkörper von L ist, der sogenannte **separable Abschluss** von K in L.

6. Spur und Norm bei separablen Körperweiterungen

Für eine endliche Körpererweiterung $L|K$ hatten wir Spur $\mathrm{Sp}_{L|K} : L \to K$ und Norm $\mathrm{N}_{L|K} : L \to K$ wie folgt definiert: Ist $\omega_1, \ldots, \omega_n$ eine K-Basis von L, so gibt es für jedes $\alpha \in L$ eine Matrix $A(\alpha) \in \mathrm{M}_n(K)$ mit

$$\alpha \begin{pmatrix} \omega_1 \\ \vdots \\ \omega_n \end{pmatrix} = A(\alpha) \begin{pmatrix} \omega_1 \\ \vdots \\ \omega_n \end{pmatrix}.$$

Dann ist

$$\mathrm{Sp}_{L|K}(\alpha) = \mathrm{sp}(A(\alpha)) \quad \text{und} \quad \mathrm{N}_{L|K}(\alpha) = \det(A(\alpha)).$$

(Bei Basiswechsel wird aus der Matrix $A(\alpha)$ eine Matrix $S^{-1}A(\alpha)S$ mit $S \in \mathrm{Gl}_n(K)$.) Die Zuordnung $\alpha \mapsto A(\alpha)$ ist ein K-linearer Ringhomomorphismus $K \to \mathrm{M}_n(K)$. Im Fall einer separablen Körpererweiterung können wir Spur und Norm auch anders beschreiben.

Satz. *Sei $L|K$ eine endliche, separable Körpererweiterung vom Grad n und*

$$\sigma_i : L \to \overline{K}, \quad i = 1, \ldots, n,$$

die K-Homomorphismen von L in einen algebraischen Abschluss $\overline{K}$. Dann gilt:

$$\mathrm{Sp}_{L|K}(\alpha) = \sum_{i=1}^{n} \sigma_i(\alpha) = \sigma_1(\alpha) + \cdots + \sigma_n(\alpha) \quad \textit{und} \quad \mathrm{N}_{L|K}(\alpha) = \prod_{i=1}^{n} \sigma_i(\alpha) = \sigma_1(\alpha) \ldots \sigma_n(\alpha).$$

Beweis:

(1) Sei $L|K$ eine endliche, separable Körpererweiterung. Wir können $K \subseteq L \subseteq \overline{K}$ annehmen. Nach dem Satz vom primitiven Element gibt es ein $\beta \in L$ mit $L = K(\beta)$. Sei $f \in K[x]$ das Minimalpolynom von β über K. Seien $\beta_1, \ldots, \beta_n$ die Nullstellen von f in $\overline{K}$. Dann ist

$$f = (x - \beta_1) \ldots (x - \beta_n).$$

Da f separabel ist, sind die Element $\beta_1, \ldots, \beta_n$ paarweise verschieden. Die K-Körperhomomorphismen $L \to \overline{K}$ werden dann durch

$$\sigma_i(\beta) = \beta_i$$

definiert.

(2) Sei $\omega_1, \ldots, \omega_n \in L$ eine K-Basis von L. Wir betrachten die rationale Darstellung:

$$\alpha \begin{pmatrix} \omega_1 \\ \vdots \\ \omega_n \end{pmatrix} = A(\alpha) \begin{pmatrix} \omega_1 \\ \vdots \\ \omega_n \end{pmatrix} \text{ mit } A(\alpha) \in \mathrm{M}_n(K).$$

(3) Das charakteristische Polynom von $A(\beta)$ ist das Minimalpolynom von β, also $f = (x-\beta_1) \ldots (x-\beta_n)$. Da die Elemente $\beta_1, \ldots, \beta_n$ paarweise verschieden sind, ist $A(\beta)$ über $\overline{K}$ diagonalisierbar, d.h. es gibt eine Matrix $S \in \mathrm{GL}_n(\overline{K})$ mit

$$S^{-1}A(\beta)S = \begin{pmatrix} \beta_1 & & \\ & \ddots & \\ & & \beta_n \end{pmatrix} = \begin{pmatrix} \sigma_1(\beta) & & \\ & \ddots & \\ & & \sigma_n(\beta) \end{pmatrix}.$$

(4) Sei nun $\alpha \in L$ ein beliebiges Element. Wegen $L = K(\beta)$ können wir schreiben $\alpha = \sum_j c_j \beta^j$ mit $c_j \in K$. Dann gilt

$$\begin{aligned} S^{-1}A(\alpha)S &= S^{-1}A(\sum_j c_j\beta^j)S = \sum_j c_j (S^{-1}A(\beta)S)^j = \\ &= \sum_j c_j \begin{pmatrix} \sigma_1(\beta) & & \\ & \ddots & \\ & & \sigma_n(\beta) \end{pmatrix}^j = \begin{pmatrix} \sum_j c_j\sigma_1(\beta)^j & & \\ & \ddots & \\ & & \sum_j c_j\sigma_n(\beta)^j \end{pmatrix} = \\ &= \begin{pmatrix} \sigma_1(\alpha) & & \\ & \ddots & \\ & & \sigma_n(\alpha) \end{pmatrix}. \end{aligned}$$

Durch Spur- und Normbildung folgt aus der letzten Darstellung die Behauptung. ■