6.1 Transzendente Körpererweiterungen

Betrachte eine Körpererweiterung L/K.

6.1.1 Definition: Eine Kollektion paarweise verschiedener Elemente $A = \{a_\nu \mid \nu \in N\}$ von L heisst *algebraisch abhängig über K*, wenn ein Polynom $f \in K[(X_\nu)_{\nu \in N}] \smallsetminus \{0\}$ existiert mit $f((a_\nu)_\nu) = 0$. Andernfalls heisst sie *algebraisch unabhängig über K*.

6.1.2 Proposition: Für jede Teilmenge $A \subset L$ sind äquivalent:

(a) A ist algebraisch unabhängig über K, und $L/K(A)$ ist algebraisch.

(b) A ist eine maximale über K algebraisch unabhängige Teilmenge.

(c) A ist eine minimale Teilmenge von L, so dass $L/K(A)$ algebraisch ist.

6.1.3 Definition: Eine solche Teilmenge $A \subset L$ heisst *Transzendenzbasis von L/K*.

Beweis: (a) $\Rightarrow$ (b) Sei A wie in (a) und $A \subset A' \subset L$ und A' alg. unabh.
Für jedes $a' \in A' \smallsetminus A$ ist a' alg. über $K(A)$. D.h. $\exists f \in K(A)[X] \smallsetminus \{0\}$ mit $f(a') = 0$.
OBdA $f = g((a_\nu)_\nu, X)$ mit $g \in K[(X_\nu)_\nu, X]$. Dann ist $g \neq 0 \Rightarrow A'$ alg. abh.
Widerspruch. Also ist $A = A'$. qed

(b) $\Rightarrow$ (a) Ü.

(a) $\Rightarrow$ (c) Ü

(c) $\Rightarrow$ (a): Sei A wie in (c). Wäre A alg. abh., gäbe es $f \in K[(X_\nu)] \smallsetminus \{0\}$ mit $f((a_\nu)_\nu) = 0$.
Dann ist f nicht konstant z.B. in der Variablen a_μ. Setze $A' := A \smallsetminus \{a_\mu\}$
$\Rightarrow a_\mu$ alg. über $K(A') \Rightarrow K(A)/K(A')$ algebraisch
$\Rightarrow L/K(A')$ alg. $\Rightarrow$ Widerspruch! Also ist A alg. unabh. qed

A'

6.1.4 Proposition: *(Austauschsatz)* Für je zwei Transzendenzbasen A und B von L/K und jedes Element $b \in B \smallsetminus A$ existiert ein $a \in A \smallsetminus B$, so dass $(A \smallsetminus \{a\}) \cup \{b\}$ eine Transzendenzbasis von L/K ist.

Bew.: b algebraisch über $K(A)$. Wähle $f \in K[(X_\nu)_\nu, X] \setminus \{0\}$ mit $f((a_\nu)_\nu, b) = 0$.

Da b transzendent über K ist, ist f nichtkonstant in einem X_μ. Setze $a := a_\mu$.

Damit ist a algebraisch über $K(A') \Rightarrow K(A, b) = K(A', a)/K(A')$ alg.

$\Rightarrow L/K(A')$ alg. Wäre A' alg. abh., gäbe es $0 \neq g \in K[(X_\nu)_{\nu \neq \mu}, X]$ mit $g((a_\nu)_{\nu\neq\mu}, b) = 0$

$\Rightarrow \begin{cases} X \text{ kommt in } g \text{ vor} \Rightarrow b \text{ alg. über } K(A \setminus \{a\}) \Rightarrow K(A,b)/K(A\setminus\{a\}) \text{ alg.} \Rightarrow L/K(A \setminus \{a\}) \text{ alg.} \Rightarrow \text{Widerspruch zur Min. von } A \\ X \text{ kommt in } g \text{ nicht vor} \Rightarrow A \text{ alg. abh. Wid!} \end{cases}$ Also ist A' alg. unabh.

6.1.5 Satz: Es existiert eine Transzendenzbasis, und je zwei Transzendenzbasen von L/K haben dieselbe Kardinalität. gilt.

Zorns Lemma.

6.1.6 Definition: Diese Kardinalität heisst der *Transzendenzgrad von L/K* und wird bezeichnet mit $\mathrm{trdeg}_{L/K}$.

Falls eine endlich ist, wie die Basis eines VR s.o.

6.1.7 Proposition: Es ist L/K algebraisch genau dann, wenn $\mathrm{trdeg}_{L/K} = 0$ ist.

$\Updownarrow$

$\emptyset$ Transzendenzbasis

6.1.8 Proposition: Für jede endlich erzeugte Körpererweiterung $L = K(a_1, \ldots, a_n)/K$ gilt

$$\mathrm{trdeg}_{L/K} \leqslant n < \infty.$$

6.1.9 Beispiel: Es ist $\mathrm{trdeg}_{\mathbb{R}/\mathbb{Q}} = \mathrm{card}(\mathbb{R})$.

6.1.10 Proposition: Für jeden Körperturm $M/L/K$ gilt $\mathrm{trdeg}_{M/K} = \mathrm{trdeg}_{M/L} + \mathrm{trdeg}_{L/K}$.

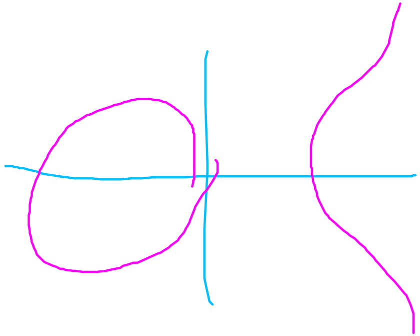
6.1.11 Definition: Eine Körpererweiterung L/K, welche von einer Transzendenzbasis erzeugt ist, heisst *rein transzendent.*

6.1.12 Beispiel: Der rationale Funktionenkörper $K(X_1, \ldots, X_n)$ ist rein transzendent über K vom Transzendenzgrad n.

$X_1, \ldots, X_n$ alg. unabh. über K. $\Rightarrow$ Transzendenzbasis.

6.1.13 Beispiel: Der *elliptische Funktionenkörper* $\mathbb{C}(x, y)$ für über $\mathbb{C}$ transzendente Elemente x und y mit $y^2 = x^3 - x$ ist nicht rein transzendent über $\mathbb{C}$.

$$\mathbb{C}(x,y) = \mathbb{C}(x, \sqrt{x^3 - x}), \qquad [\mathbb{C}(x, \sqrt{x^3 - x}) / \mathbb{C}(x)] = 2.$$



7.3 Symmetrische Funktionen

$\underline{X}^{\underline{i}} = \prod_{\nu=1}^{n} X_\nu^{i_\nu}$.

$\underline{i} = (i_1, \ldots, i_n)$

Wir betrachten Polynome in $\underline{X} = (X_1, \ldots, X_n)$ über einem beliebigen Ring R.

7.3.1 Definition: Ein Polynom der Form $f(\underline{X}) = \sum_{\underline{i}}' a_{\underline{i}} \underline{X}^{\underline{i}}$, bei der die Summe sich nur über Multiindizes $\underline{i}$ mit $\sum_\nu i_\nu = d$ erstreckt, heisst *homogen vom Grad d.*

$\Rightarrow f(tX_1, \ldots, tX_n) = t^d \cdot f(X_1, \ldots, X_n)$

7.3.2 Proposition: Jedes Polynom ist eine eindeutige Summe $f = \sum_{d \geqslant 0}' f_d$ mit f_d homogen vom Grad d.

7.3.3 Definition: Der *Totalgrad* $\deg(f)$ eines Polynoms $f \in R[\underline{X}] \setminus \{0\}$ ist das grösste d mit $f_d \neq 0$.

7.3.4 Proposition: Für alle $f, g \in R[\underline{X}] \setminus \{0\}$ gilt $\deg(fg) \leqslant \deg(f) + \deg(g)$, mit Gleichheit wenn R ein Integritätsbereich ist.

Bew.: $f = \sum_{d \le d_0} f_d$, $g = \sum_{e \le e_0} g_e \Rightarrow f \cdot g = \sum_{d,e} f_d \cdot g_e = \sum_k \underbrace{\Big(\sum_{\substack{d,e \\ d+e=k}} f_d g_e \Big)}_{\text{homogen vom Grad } k}$

$f_{d_0}, g_{e_0} \neq 0 \Rightarrow f \cdot g = \overbrace{f_{d_0} \cdot g_{e_0}}^{\neq 0 \text{ falls } R \text{ Int.ber.}} + \text{Terme kleineren Grades}$. $\underline{\text{qed}}$.

7.3.5 Variante: Für jede Variable X_ν sei ein Gewicht $\mu_\nu \in \mathbb{R}$ gegeben. Ein Polynom der Form $f(\underline{X}) = \sum_{\underline{i}}' a_{\underline{i}} \underline{X}^{\underline{i}}$, bei der die Summe sich nur über Multiindizes $\underline{i}$ mit $\sum_\nu i_\nu \mu_\nu = \lambda$ erstreckt, heisst dann *isobar vom Gewicht* λ. Jedes Polynom ist eine eindeutige Summe $f = \sum_\lambda' f_\lambda$ mit f_λ isobar vom Gewicht λ.

7.3.6 Definition: Ein Polynom $f \in R[X_1, \ldots, X_n]$ heisst *symmetrisch*, wenn gilt

$$\forall \sigma \in S_n: \; f(X_{\sigma 1}, \ldots, X_{\sigma n}) = f(X_1, \ldots, X_n).$$

Bsp.
$S_1 = X_1 + \ldots + X_n$
$S_n = X_1 \cdot \ldots \cdot X_n$.

7.3.7 Definition: Für jedes $1 \leqslant m \leqslant n$ ist das *m-te elementarsymmetrische Polynom in* $X_1, \ldots, X_n$ das homogene symmetrische Polynom vom Grad m

$$\boxed{S_m := \sum_{1 \leqslant \nu_1 < \ldots < \nu_m \leqslant n} X_{\nu_1} \cdots X_{\nu_m} \in \mathbb{Z}[X_1, \ldots, X_n].}$$

$S_2 = X_1X_2 + X_1X_3 + \ldots + X_1X_n$
$+ X_2X_3 + \ldots + X_2X_n$
$+ \ldots$
$+ X_{n-1}X_n$.

Eine äquivalente Charakterisierung ist die Identität

$$\begin{aligned} \boxed{\prod_{i=1}^{n} (X - X_i)} &= X^n + \sum_{m=1}^{n} (-1)^m S_m X^{n-m} \\ &= X^n - S_1 X^{n-1} + - \ldots + (-1)^n S_n \in \mathbb{Z}[X, X_1, \ldots, X_n]. \end{aligned}$$

Betrachte nun weitere Variablen $U_1, \ldots, U_n$.

7.3.8 Hauptsatz: Für jedes symmetrische Polynom $f \in R[X_1, \ldots, X_n]$ existiert ein eindeutiges Polynom $g \in R[U_1, \ldots, U_n]$ mit $f = g(S_1, \ldots, S_n)$.

Beweis später

$$= \sum_{I \subset \{1 \ldots n\}} X^{n-|I|} \cdot \prod_{i \in I} (-X_i) =$$

$$= \sum_{k=0}^{n} X^{n-k} \cdot \Big(\sum_{\substack{I \subset \{1 \ldots n\} \\ |I| = k}} \prod_{i \in I} X_i \Big) (-1)^k$$

7.3.9 Zusatz: Ist f symmetrisch und homogen vom Grad d, so ist g isobar vom Gewicht d, wobei jedes U_ν mit dem Gewicht ν versehen wird.

Beweis später

7.3.10 Beispiel: Für jedes $d \geqslant 1$ ist $\sum_{\nu=1}^n X_\nu^d$ ein symmetrisches Polynom. Zum Beispiel sind

$$\begin{aligned}
\textstyle\sum_{\nu=1}^n X_\nu &= S_1, \\
\textstyle\sum_{\nu=1}^n X_\nu^2 &= S_1^2 - 2S_2, \\
\textstyle\sum_{\nu=1}^n X_\nu^3 &= S_1^3 - 3S_1S_2 + 3S_3.
\end{aligned}$$

$\sum X_\nu^2$ = Linearkombination von S_1^2 und S_2.

$$S_1^2 = \left(\sum X_\nu\right)^2 = \sum_{\nu,\mu} X_\nu \cdot X_\mu = \sum_\nu X_\nu^2 + 2 \cdot \sum_{\nu<\mu} X_\nu \cdot X_\mu = \sum X_\nu^2 + 2S_2$$

$$\Rightarrow \sum X_\nu^2 = S_1^2 - 2S_2.$$

7.3.11 Bemerkung: Aus dem Hauptsatz folgt, dass für jedes von Null verschiedene Polynom $g \in R[U_1, \ldots, U_n]$ auch das Polynom $g(S_1, \ldots, S_n)$ ungleich Null ist.

(Eindeutigkeit von g).

$$(s_1^2-2s_2)\cdot s_1 = \sum_\nu x_\nu^2 \cdot \sum_\mu x_\mu = \sum_\nu x_\nu^3 + \sum_{\nu\neq\mu} x_\nu^2 x_\mu .$$

$$s_2 \cdot s_1 = \Big(\sum_{\mu<\nu} x_\mu x_\nu\Big)\cdot\Big(\sum_\lambda x_\lambda\Big) = \underbrace{\sum_{\mu<\nu} x_\mu^2 x_\nu + \sum_{\mu<\nu} x_\mu x_\nu^2}_{=\ \sum_{\mu\neq\nu} x_\mu^2 x_\nu} + \underbrace{\sum_{\substack{\mu<\nu\\ \lambda\neq\mu,\nu}} x_\mu x_\nu x_\lambda}_{=\ 3\cdot s_3}$$

$$\Rightarrow \sum_\nu x_\nu^3 = (s_1^2-2s_2)\cdot s_1 - (s_2 s_1 - 3s_3) = s_1^3 - 3s_1 s_2 + 3s_3$$

<u>Vorsicht</u>: Der Hauptsatz gilt nicht für die Polynome $\sum_\nu x_\nu^d$ anstelle der s_d, weil z.B. $\sum x_\nu^2 = s_1^2 - 2s_2$ nicht nach s_2 aufgelöst werden kann über jedem Ring:

$$s_2 = \frac{s_1^2 - \sum x_\nu^2}{2} \quad ?$$

7.3.12 Variante: Sei K ein Körper. Eine rationale Funktion $f \in K(X_1, \dots, X_n)$ heisst *symmetrisch*, wenn gilt

$$\forall \sigma \in S_n\colon\ f(X_{\sigma 1}, \dots, X_{\sigma n}) = f(X_1, \dots, X_n).$$

7.3.13 Satz: Für jede symmetrische rationale Funktion $f \in K(X_1, \dots, X_n)$ existiert eine eindeutige rationale Funktion $g \in K(U_1, \dots, U_n)$ mit $f = g(S_1, \dots, S_n)$.

Beweis: Sei $f = \frac{\varphi}{\psi}$ für $\varphi, \psi \in K[\underline{X}]$.

$$\Rightarrow f = \frac{\overbrace{\varphi \cdot \prod_{\sigma \neq id} \sigma(\psi)}^{\text{symmetrisch in } K[\underline{X}]}}{\underbrace{\prod_{\sigma \in S_n} \sigma(\psi)}_{\text{symmetrisch in } K[\underline{X}]}} = \frac{\varphi'(S_1, \dots, S_n)}{\psi'(S_1, \dots, S_n)}$$

für gewisse $\varphi', \psi' \in K[\underline{U}]$.
Also $f = g(S_1, \dots, S_n)$ für $g := \frac{\varphi'}{\psi'}$.
Eindeutigkeit, da $S_1, \dots, S_n$ algebraisch unabhängig über K. qed.

7.3.14 Folge: Die Körpererweiterung $K(X_1, \dots, X_n)/K(S_1, \dots, S_n)$ ist endlich galoissch mit Galoisgruppe S_n. Die Erweiterung $K(S_1, \dots, S_n)/K$ ist rein transzendent mit der Transzendenzbasis $S_1, \dots, S_n$.

algebraisch unabhängig wegen 7.3.11.

Beweis: $K(S_1, \dots, S_n) = K(X_1, \dots, X_n)^{S_n}$, verwende Satz 7.1.5.

$K(X_1, \dots, X_n)^{S_n} = K(S_1, \dots, S_n)$ nach 7.3.13. qed.