10. Script zur Vorlesung: Algebra (B III)

Prof. Dr. Salma Kuhlmann, Gabriel Lehéricy, Simon Müller

WS 2016/2017: 29. November 2016

Definition

(1) $\alpha \in K/F$ ist *algebraisch über* F (alg/F), wenn es ein Polynom $0 \neq f(x) \in F[x]$ gibt mit $f(\alpha) = 0$.

(2) Wenn α nicht algebraisch ist, dann heißt α *transzendent* über F.

(3) Die Körpererweiterung K/F heißt *algebraisch*, falls für alle $\alpha \in K$: α ist algebraisch über F.

Proposition 1

Sei α alg $/F$. Es gibt ein eindeutiges normiertes irreduzibles Polynom $m_{\alpha,F}(x) \in F[x]$, so dass

(i) $m_{\alpha,F}(\alpha) = 0$.

(ii) Ist $f(\alpha) = 0$ für ein $f \in F[x]$, dann teilt $m_{\alpha,F}(x)$ das Polynom $f(x)$ in $F[x]$.

Beweis

- Setze $m(x) := m_{\alpha,F}(x) :=$ normiertes Polynom vom minimalem deg, so dass $m(\alpha) = 0$. Sei $f(x) \in F[x]$, schreibe $f(x) = q(x)m(x) + r(x), \deg r(x) < \deg m(x)$ oder $r(x) = 0$. Wir sehen $0 = f(\alpha) \Leftrightarrow r(\alpha) = 0$. Die Minimalität vom $\deg m(x)$ impliziert $r(x) \equiv 0$, also $m(x)|f(x)$.

- Ist $m'(x)$ normiert vom minimalem deg mit $m'(\alpha) = 0$, dann gilt wie oben $m'(\alpha)|m(\alpha)$, aber auch $m(\alpha)|m'(\alpha), m(\alpha), m'(\alpha)$ normiert $\Rightarrow m'(x) = m(x)$. $\square$

Bemerkung

Vergleiche mit 13. Vorlesung "Lineare Algebra II" vom 1. Juni 2012:
Das Minimal-Polynom von T in $F[x]$ ist der eindeutige normierte Erzeuger vom Annihilator-Ideal von T

$$\mathcal{A}_T := \{f \in F[x] | f(T) = 0\}.$$

Definition

$m_{\alpha,F}(x)$ heißt das *Minimal-Polynom* von α über F. Wir schreiben $m(x)$, wenn klar.

Proposition 2

Sei $\alpha \in K/F$ algebraisch über F. Es ist $[F(\alpha) : F] = \deg m_{\alpha,F}(x)$.

Beweis

$F(\alpha) \simeq F[x]/ < m(x) >$ □

Terminologie

$\deg \alpha/F := \deg m_{\alpha,F}(x) = \deg F(\alpha)/F$.

Bemerkung

(1) $L \supseteq K \supseteq F, \alpha \in L,$ alg $/F \to \alpha$ alg $/K$ und es gilt

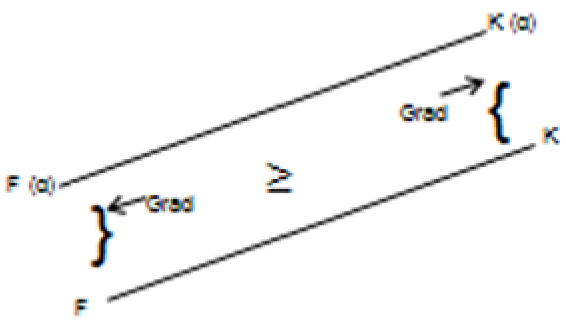
(2) $m_{\alpha,K}(x)$ teilt $m_{\alpha,F}(x)$ in $K[x]$, insbesondere

(3) $\deg m_{\alpha,K}(x) \leq \deg m_{\alpha,F}(x)$. Es gilt ferner

(4) $m_{\alpha,K}(x) = m_{\alpha,F}(x)$ genau dann, wenn $m_{\alpha,F}(x)$ irreduzibel bleibt in $K[x]$. Wir haben aus 3.:

(5) $[K(\alpha) : K] \leq [F(\alpha) : F]$

Für $\alpha \in L$ alg $/F \subseteq K \subseteq L$:



Wir zeigen nun die Umkehrung von Proposition 2.

(**Erinnerung:** K/F ist *endlich*, wenn $[K : F] < \infty$, sonst unendlich.)

Proposition 3
Sei $\alpha \in K/F$, so dass $[F(\alpha) : F] < \infty$. Dann ist α algebraisch über F.

Beweis
Sei $[F(\alpha) : F] = n$, dann sind $F(\alpha) \ni 1, \alpha, \alpha^2, \ldots, \alpha^n$ linear abhängig über F. Also existieren $b_i \in F$ *nicht alle gleich 0*, so dass $\sum_{i=0}^{n} b_i\alpha^i = 0$. Setze $f(x) := \sum b_i x^i \in F[x]; \neq 0$. Dann gilt $f(\alpha) = 0; \alpha$ alg $/F$. □

Bemerkung
$x \in F(x)$ ist transzendent über F (weil $f(x) = 0 \Leftrightarrow f = 0$ das Nullpolynom ist). Wir sehen, dass $F(x)/F$ eine endlich erzeugte (eigentlich eine einfache) Erweiterung ist, aber $[F(x) : F] = \infty$. Also i.a.: K/F endlich erzeugt $\not\Rightarrow K/F$ endlich.

Korollar
K/F ist endlich $\Rightarrow K/F$ algebraisch.

Beweis
Sei $\alpha \in K$. Es ist $[F(\alpha) : F] \leq [K : F] < \infty$, also ist α algebraisch über F. □

Satz 1
$F \subseteq K \subseteq L$. Es gilt $[L : F] = [L : K][K : F]$. (Also insbesondere ist L/F unendlich genau dann, wenn L/K oder K/F unendlich sind.)

Beweis
Zunächst nehmen wir an: $[L : K] = m$ mit $\{\alpha_1, \ldots, \alpha_m\}$ Basis für L/K; $[K : F] = n$ mit $\{\beta_1, \ldots, \beta_n\}$ Basis für K/F. Ein Element λ aus L ist also aus der Form $\lambda = \sum_i a_i\alpha_i$ mit $a_i \in K$. $(*)$
Schreibe $a_i = \sum_j b_{ij}\beta_j$ mit $b_{ij} \in F$ $(**)$

$\rightsquigarrow$ Einsetzen von $(**)$ in $(*)$ ergibt $\lambda = \sum_{i,j} b_{ij}\alpha_i\beta_j$. $(***)$

Also ist span ${}_F\{\alpha_i\beta_j \mid i = 1, \ldots, m, j = 1, \ldots, n\} = L$. Wir zeigen, dass diese Menge auch F-linear unabhängig ist.
Sei also $\sum_{i,j} b_{ij}\alpha_i\beta_j = 0$ für $b_{ij} \in F$. $(\dagger)$
Setze $a_i := \sum_j b_{ij}\beta_j \in K$ und schreibe $(\dagger)$, also $\sum_i a_i\alpha_i = 0$. Nun ist α_i linear unabhängig über $K \Rightarrow a_i = 0$ für alle i, also $\sum_j b_{ij}\beta_j = 0$ für alle i.
Nun ist β_j linear unabhängig über $F \Rightarrow b_{ij} = 0$ für alle j. □

Wir haben gezeigt: $[L : F] = \infty \Rightarrow [L : K] = \infty$ oder $[K : F] = \infty$.
Sei nun $[K : F]$ unendlich, dann ist auch $[L : F]$ unendlich, weil K ein F-Unterraum von L ist.
Sei nun $[L : K] = \infty$, dann ist *a* fortiori $[L : F] = \infty$ ($\lambda_1, \ldots, \lambda_s$ sind K linear unabhängig $\to \lambda_1, \ldots, \lambda_s$ sind F-linear unabhängig).

Korollar
Sei $L/K/F$ und L/F endlich. Es gilt $[K : F] | [L : F]$.

Wir haben bisher gezeigt, dass α algebraisch über F ist $\Leftrightarrow [F(\alpha) : F] < \infty$. Wir sind nun in der Lage dieses für $F(\alpha_1, \ldots, \alpha_n)$ zu verallgmeinern.

Bemerkung
$F(\alpha_1, \alpha_2) = F(\alpha_1)(\alpha_2) \subseteq K$ (folgt unmittelbar aus der Definition von $F(\alpha_1, \alpha_2)$).

Satz 2
K/F ist endlich $\Leftrightarrow K/F$ ist endlich erzeugt von alg $/F$-Elementen.

Beweis

"$\Rightarrow$" Setze $[K : F] = n$. Sei $\{\alpha_1, \ldots, \alpha_n\}$ die F-Basis von K. Jedes α_i ist algebraisch über F.
Außerdem ist $K = \text{span}_F\{\alpha_1, \ldots, \alpha_n\} \subseteq F(\alpha_1, \ldots, \alpha_n) \subseteq K$
und damit ist $K = F(\alpha_1, \ldots, \alpha_n)$.

"$\Leftarrow$" Sei $K = F(\alpha_1, \ldots, \alpha_k)$. Sei α_i algebraisch über F und $\deg \alpha_i = n_i$. Setze $F = F_0$ und $F_1 = F_0(\alpha_i)$. $F_{i+1} := F_i(\alpha_{i+1})$, so $K = F_{k-1}(\alpha_k)$.
Es ist:

$$\begin{tikzcd}
& F_i(\alpha_{i+1}) \arrow[d, dash] \\
F(\alpha_{i+1}) \arrow[ur, dash] \arrow[d, dash] & F_i \\
F \arrow[ur, dash] &
\end{tikzcd}$$

$$\begin{array}{c}
F_{k-1}(\alpha_k) = K \\
\vdots \\
F_{i+1} \\
F_i \\
\vdots \\
\vdots \\
F_1 \\
F_0 = F
\end{array}$$

Also $[F_{i+1} : F_i] \leq n_{i+1}$. Also (Satz 1) $[K : F] = [F_k : F_{k-1}] \cdots [F_1 : F_0] \leq n_1 \cdots n_k$ und damit ist K/F endlich. $\square$