11. Script zur Vorlesung: Algebra (B III)

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

WS 2016/2017: 2. Dezember 2016

Erinnerung: Eine Erweiterung K/F ist genau dann endlich, wenn es endlich erzeugt von algebraischen Elementen ist.

Korollar 1
α, β sind algebraisch über $F \to \alpha \pm \beta, \alpha\beta, \alpha/\beta (\beta \neq 0)$ sind auch algebraisch über F.

Beweis
$F(\alpha, \beta)/F$ ist endlich und $\alpha \pm \beta, \alpha\beta, \alpha/\beta \in F(\alpha, \beta)$ für $\beta \neq 0$. □

Korollar 2
Sei L/F eine beliebige Körpererweiterung. Die Menge $\{\alpha \in L \mid \alpha \text{ alg } /F\}$ ist ein Unterkörper von L (und enthält F).

Definition 1
Dieser Unterkörper heißt der *relative algebraische Abschluss von F in L.*

Beispiele

(1) $\mathbb{C}/\mathbb{Q}$. $\tilde{\mathbb{Q}} := \{z \in \mathbb{C} \mid z \text{ alg } /\mathbb{Q}\}$ ist der *Körper der algebraischen Zahlen.*

(2) $\mathbb{R}/\mathbb{Q}$. $\tilde{\mathbb{Q}}^r := \{r \in \mathbb{R} \mid r \text{ alg } /\mathbb{Q}\}$ ist der *Körper der reellen algebraischen Zahlen.*

Es gilt $\tilde{\mathbb{Q}} \subsetneq \mathbb{C}$ und $\tilde{\mathbb{Q}}^r \subsetneq \mathbb{R}$ (z.B: $\pi, e \in \mathbb{R} \backslash \tilde{\mathbb{Q}}^r$) . Eigentlich gilt es ferner $|\tilde{\mathbb{Q}}| = |\tilde{\mathbb{Q}}^r| = \aleph_0$ und $|\mathbb{C} \setminus \tilde{Q}| = |\mathbb{R} \setminus \tilde{\mathbb{Q}}^r| = 2^{\aleph_0}$.

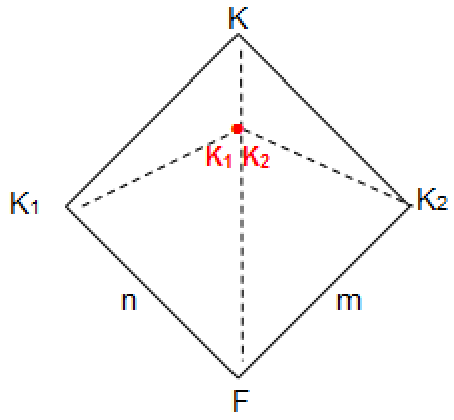
Satz 1

$$\underset{\text{alg}}{L/K} \quad \text{und} \quad \underset{\text{alg}}{K/F} \quad \Rightarrow \quad \underset{\text{alg}}{L/F}$$

Beweis
Sei $\alpha \in L, k(x) \in K[x]; k(\alpha) = 0$. Setze $k(x) := \sum_{i=0}^{n} a_i x^i$ mit $a_i \in K$ nicht alle Null. Betrachte $F_1 := F(a_0, \ldots, a_n)$ und $F_1(\alpha), F_1 \subseteq K, F_1(\alpha) \subseteq L; a_i$ alg $/F$ und α alg $/F_1$.
Also $[F_1 : F] < \infty$ und $[F_1(\alpha) : F_1] < \infty \Rightarrow [F_1(\alpha) : F] = [F_1(\alpha) : F_1][F_1 : F] < \infty$.
Insbesondere $F_1(\alpha)/F$ algebraisch und damit α algebraisch über F.

Definition 2
Sei K/K_1 und K/K_2 eine Körpererweiterung. $K_1K_2 := K_1(K_2) = K_2(K_1) \subseteq K$ heißt *das Kompositum von K_1 und K_2 in K.*

Lemma
Sei



$\{\alpha_1, \ldots, \alpha_n\}$ eine F-Basis von K_1 und $\{\beta_1, \ldots, \beta_m\}$ eine F-Basis von K_2 (ohne Einschränkung mit $\alpha_1 = \beta_1 = 1$). Es ist $\operatorname{span}_F\{\alpha_i\beta_j/i,j\} = K_1K_2$.

Beweis
Es ist klar, dass $\operatorname{span}_F\{\alpha_i\beta_j/i,j\} \subseteq K_1K_2$. Bemerke, dass $K_1K_2 = F(\alpha_1, \ldots, \alpha_n, \beta_1, \ldots \beta_m)$. Weil $\alpha_1, \ldots, \alpha_n, \beta_1, \ldots \beta_m$ algebraisch über F sind, gilt außerdem $F(\alpha_1, \ldots, \alpha_n, \beta_1, \ldots \beta_m) = \operatorname{span}_F(\alpha_1, \ldots, \alpha_n, \beta_1, \ldots \beta_m)$. Es gilt also:
$K_1K_2 = \operatorname{span}_F(\alpha_1, \ldots, \alpha_n, \beta_1, \ldots \beta_m) \subseteq \operatorname{span}_F\{\alpha_i\beta_j/i,j\} \subseteq K_1K_2$ $\square$

Korollar 3
Seien $F \subseteq K_1, K_2 \subseteq K; [K_1 : F] := n; [K_2 : F] := m$. Es gilt $[K_1K_2 : F] \leq nm$ und $[K_1K_2 : F] := mn$, falls β_j linear unabhängig über K_1 bleiben (oder α_i linear unabhängig über K_2 bleiben).

Beweis
Dass $[K_1K_2 : F] \leq nm$ folgt direkt aus dem Lemma. Wir nehmen an, dass $\alpha_1, \ldots, \alpha_n$ linear unabhängig über K_2 sind und wir zeigen, dass die Familie $\{\alpha_i\beta_j \mid 1 \leq i \leq n, 1 \leq j \leq m\}$ linear unabhängig über F ist. Seien $(\nu_{ij})_{ij} \subseteq F$ so, dass $\sum_{i,j} \nu_{ij}\alpha_i\beta_j = 0$. Man kann diese Summe umschreiben: $\sum_{i=1}^n \alpha_i(\sum_{j=1}^m \nu_{ij}\beta_j) = 0$. Für alle $i \in \{1, \ldots, n\}$ ist $\sum_{j=1}^m \nu_{ij}\beta_j \in K_2$. Nach annahme muss dann $\sum_{j=1}^m \nu_{ij}\beta_j = 0$ gelten für alle $i \in \{1, \ldots, n\}$. Weil $\beta_1, \ldots, \beta_m$ linear unabhängig über F sind, muss dann $\nu_{ij} = 0$ gelten für alle i, j. $\square$

Korollar 4
Seien $F \subseteq K_1, K_2 \subseteq K$ mit $[K_1 : F] = n, [K_2 : F] = m$ und ggT $(n, m) = 1$.
Es gilt $[K_1K_2 : F] = mn$.

Beweis

$$\left.\begin{array}{ccc} n & | & [K_1K_2 : F] \\ m & | & [K_1K_2 : F] \end{array}\right\} \Rightarrow kgV(n,m) | [K_1K_2 : F]$$

$kgV(n, m) = \frac{nm}{ggT(n,m)} = mn$. Also $mn \leq [K_1K_2 : F] \leq mn$. □

Zerfällungskörper

Definition 3
Sei $\mathcal{E} \subseteq F[X]$. Ein Zerfällungskörper von $\mathcal{E}$ ist eine Körpererweiterung K/F, so dass folgendes gilt:

1. Jedes $f \in \mathcal{E}$ zerfällt vollständig in lineare Faktoren in $K[X]$
2. K wird von den Nullstellen der Polynome in $\mathcal{E}$ erzeugt, also

   $K = F(\{\alpha \in K \mid \exists f \in \mathcal{E} \text{ mit } f(\alpha) = 0\})$

Definition 4
Sei $f \in F[X]$. Ein Zerfällungskörper von f ist ein Zerfällungskörper der Familie $\{f\}$.

Bemerkung
K ist genau dann ein Zerfällungskörper von f, wenn folgendes gilt:

1. f zerfällt vollständig in lineare Faktoren in $K[X]$
2. Für alle Körper L mit $F \subseteq L \subsetneq K$ zerfällt f in $L[X]$ **nicht**.

Satz 2
Es gibt einen Zerfällungskörper K/F für $f(x)$ über F.

Beweis
Per Induktion zeigen wir zunächst, dass es eine Körpererweiterung E/F gibt, in der $f(x)$ vollständig zerfällt.
Setze $n = \deg f(x)$. $n = 1, E = F$✓ Induktionsanfang $n > 1$.
Sei $p(x)$ ein irreduzibler Faktor von $f(x)$ in $F[x]$ mit $\deg p \geq 2$ (sonst ist wieder $E = F$).
Sei $\alpha \in E_1/F$ eine Nullstelle von $p(x)$, über E_1 haben wir also

(*) $$f(x) = (x - \alpha)f_1(x)$$

$f_1(x) \in E_1[x]; \deg f_1 \leq n - 1$.

Induktionsanfang für f_1 und E_1 ergibt eine E/E_1 und f_1 zerfällt vollständig in $E[x]$. Nun ist auch $\alpha \in E$. Also zerfällt f wie in $(*)$ vollständig über E.
Setze nun $K := \bigcap\{L/F \subseteq L \subseteq E; f \text{ zerfällt vollständig in } L[x]\}$ □

Definition 5
K/F ist *normal*, falls
- (i) K/F algebraisch ist
- (ii) und K ein Zerfällungskörper über F

einer Familie von Polynomen $f(x) \in F[x]$.

Proposition
Sei $\deg f = n$ K/F ein Zerfällungskörper von f über F. Es gilt $[K : F] \leq n!$

Beweis
Sei $\alpha_1 \in F_1/F$, α_1 ist Nullstelle von f. Dann ist $[F_1 : F] \leq n$ und $f(x) = (x - \alpha_1)f_1(x)$, $f_1(x) \in F[x]$, $\deg f_1 \leq n - 1$.
Wiederholung: $\alpha_2 \in F_2/F_1, \alpha_2$ ist Nullstelle von f_1.
Dann ist $[F_2 : F_1] \leq n - 1$ und damit $[F_2 : F] \leq n(n - 1)$ usw. □

Satz 3 (Eindeutigkeit bis auf Isomorphie)
Sei $\varphi : F \xrightarrow{\sim} F'$ eine Isomorphie.
$f(x) \in F[x] \rightsquigarrow f'(x) \in F'[x]$ $(\deg f \geq 1)$.
E ist Zerfällungskörper für f über F - E' ist Zerfällungskörper für f' über F'.
Dann läßt sich φ fortsetzen:

$$\begin{tikzcd} E \arrow[r, "\overset{\sigma}{\sim}"] \arrow[d, dash] & E' \arrow[d, dash] \\ F \arrow[r, "\sim", "\varphi"'] & F' \end{tikzcd}$$

Beweis
Sei $\deg f := n$. Induktion nach n. Wenn f über F erfällt, dann zerfällt f' über F' und $\sigma = \varphi$. Sei also $p(x)$ ein irreduzibler Faktor von $f(x)$ in $F[x]$ mit $\deg p \geq 2$ und $p' = \varphi(p)$ der entsprechende Faktor von $f'(x)$ in $F'[x]$.
$\alpha \in E$ ist Nullstelle für $p(x)$ und $\beta \in E'$ ist Nullstelle für $p'(x)$. Setze $F_1 := F(\alpha)$ und $F_1' := F'(\beta)$.
Aus Satz 3 der 9. Vorlesung folgt, dass ein σ_1 existiert, so dass

$$\begin{tikzcd} F_1 \arrow[r, "\sim", "\sigma_1"'] \arrow[d, dash] & F_1' \arrow[d, dash] \\ F \arrow[r, "\sim", "\varphi"'] & F' \end{tikzcd}$$

Wir haben also den folgenden Ansatz:

$$\sigma_1 : F_1 \xrightarrow{\sim} F_1'$$

$f(x) = (x - \alpha) f_1(x)$ über F_1, $\deg f_1 \leq n - 1$ und E ist ein Zerfällungskörper von f_1 über F_1, weil $E \supseteq F_1$ und alle Nullstellen von f_1 und für $E \supsetneq L \supseteq F_1$ ist es unmöglich, dass L alle Nullstellen von f_1 enthält (sonst enthält L α und alle Nullstellen von f_1, also alle Nullstellen von f - Widerspruch. Minimalität von E als ein Zerfällungskörper von f über F).
$f'(x) = (x - \beta) f_1'(x)$ über F_1', $\deg f_1 \leq n - 1$ und E' ist ein Zerfällungskörper von f_1' über F_1'. Also haben wir nun den Ansatz f_1, F_1, σ_1 mit $\deg f_1 \leq n - 1$.

Die Induktionsannahme liefert ein σ, so dass

$$\begin{tikzcd}
E \arrow[r, "\sim", "\sigma"'] \arrow[d, dash] & E' \arrow[d, dash] \\
F_1 \arrow[r, "\sim", "\sigma_1"'] & F_1'
\end{tikzcd}$$

Also

$$\begin{tikzcd}
E \arrow[r, "\sim", "\sigma"'] \arrow[d, dash] & E' \arrow[d, dash] \\
F_1 \arrow[r, "\sim", "\sigma_1"'] \arrow[d, dash] & F_1' \arrow[d, dash] \\
F \arrow[r, "\sim", "\varphi"'] & F'
\end{tikzcd}$$

Korollar
Ein Zerfällungskörper von $f \in F[x]$ über F ist bis Isomorphie auf F eindeutig.

Beweis
Seien K und K' Zerfällungskörper von f über F. Es gilt

$$\begin{tikzcd}
K \arrow[r, "\sim", "\sigma"'] \arrow[d, dash] & K' \arrow[d, dash] \\
F \arrow[r, "Id"] & F
\end{tikzcd}$$

$\sigma \restriction F = Id$ $\square$

Definition

(a) $\tilde{F}/F$ ist ein *algebraischer Abschluss* von F, falls

   (a) $\tilde{F}/F$ algebraisch ist;

   (b) $f(x) \in F[x]$ vollständig in lineare Faktoren über $\tilde{F}$ zerfällt für alle $f \in F[x]$.

(b) K heißt *algebraisch abgeschlossen*, falls jedes $f \in K[x]$ $(\deg f \geq 1)$ eine Nullstelle in K hat.

Bemerkung

K ist algebraisch abgeschlossen $\Leftrightarrow$ $f \in K[x]$ $(\deg f \geq 1)$ zerfällt vollständig in linearen Faktoren über $K \Leftrightarrow K = \tilde{K}$.