Algebraische und transzendente Elemente

Definition (14.3)

Sei $L|K$ eine Körpererweiterung.

- Ein Element $\alpha \in L$ heißt algebraisch über K, wenn ein Polynom $f \neq 0$ in $K[x]$ mit der Eigenschaft existiert, dass α eine Nullstelle von f ist.
- Gibt es ein solches Polynom nicht, dann nennt man α transzendent über K.

Das Minimalpolynom eines algebraischen Elements

Definition (14.4)

Sei $L|K$ eine Körpererweiterung, und sei $\alpha \in L$ algebraisch über K. Dann gibt es ein eindeutig bestimmtes, normiertes Polynom $f \in K[x]$, $f \neq 0$ minimalen Grades mit $f(\alpha) = 0$. Man nennt f das Minimalpolynom von α über K. Wir bezeichnen es mit $\mu_{\alpha,K}$.

Grad einer einfachen algebraischen Erweiterung

Satz (14.6)

Sei $L|K$ eine Körpererweiterung, $\alpha \in L$ algebraisch über K, $f = \mu_{\alpha,K}$ und $n = \mathrm{grad}(f)$. Dann bilden die Elemente

$$1, \alpha, \alpha^2, ..., \alpha^{n-1}$$

eine Basis von $K(\alpha)$ als K-Vektorraum, es gilt also $[K(\alpha) : K] = n$.

Ausführung der arithmetischen Operationen in einer Erweiterung der Form $K(\alpha) \mid K$, wobei α algebraisch über K ist

geg.: $L \mid K$ Körpererweiterung. $\alpha \in L$ algebraisch über K. $f = \mu_{\alpha,K} \in K[x]$, $n = \operatorname{grad}(f)$

Satz 14.6 $\Rightarrow$ $K(\alpha) = \{ g(\alpha) \mid g \in K[x],\ g = 0_K$ oder $\operatorname{grad}(g) \leq n-1 \}$

Seien nun $\beta, \gamma \in K(\alpha)$, $\beta = g(\alpha)$, $h = h(\alpha)$ mit $g, h \in K[x]$, $g = 0_K$ oder $\operatorname{grad} g \leq n-1$, ebenso für h.

Addition: $\beta + \gamma = (g + h)(\alpha)$

Subtraktion: $\beta - \gamma = (g - h)(\alpha)$

Multiplikation: Bestimme mit dem Eukl. Alg.

Polynome $q, r \in K[x]$ mit $g \cdot h = qf + r$ und $\operatorname{grad}(r) \leq n-1$ oder $r = 0_K$. Dann gilt $\beta\gamma = r(\alpha)$.

Kehrwerte: Setze $\beta \neq 0_K$ voraus. (Dann gilt $\operatorname{ggT}(g, f) = 1_K$.)

Bestimme mit dem Eukl. Alg. $u, v \in K[x]$ mit $ug + vf = 1_K$ sowie $q, r \in K[x]$ mit $u = qf + r$, $r = 0_K$ oder $\operatorname{grad} r \leq n-1$.

Dann gilt $\beta^{-1} = r(\alpha)$.

Beispiel: ein Körper mit $125 = 5^3$ Elementen

(Achtung: Das ist nicht dasselbe wie $\mathbb{Z}/125\mathbb{Z}$.)

Sei $f = x^3 + x + \bar{1} \in \mathbb{F}_5[x]$. überprüfe

f hat in $\mathbb{F}_5$ keine Nullstellen und ist

wegen $\operatorname{grad}(f) = 3$ damit irreduzibel in

$\mathbb{F}_5[x]$. Sei L ein Erweiterungskörper

von $\mathbb{F}_5$ mit einer Nullstelle α von f.

Satz 14.6 $\Rightarrow \mathbb{F}_5(\alpha) = \{g(\alpha) \mid g \in \mathbb{F}_5[x],$

$\operatorname{grad}(g) \leq 2$ oder $g = \bar{0}\} =$

$\{a + b\alpha + c\alpha^2 \mid a, b, c \in \mathbb{F}_5\} =$

$\{\bar{0}, \bar{1}, \bar{2}, \bar{3}, \bar{4}, \alpha, \alpha+\bar{1}, \ldots, \alpha+\bar{4}, \bar{2}\alpha,$
$\bar{2}\alpha+\bar{1}, \ldots, \alpha^2, \alpha^2+\bar{1}, \ldots, \bar{4}\alpha^2+\bar{4}\alpha+\bar{4}\}$

Addition: Sei $\beta = \alpha^2 + \bar{3}\alpha + \bar{4}$, $\gamma = \bar{2}\alpha + \bar{3}$
$\Rightarrow \beta = g(\alpha)$, $\gamma = h(\alpha)$ mit $g = x^2 + \bar{3}x + \bar{4}$,
$h = \bar{2}x + \bar{3} \Rightarrow g + h = x^2 + \bar{5}x + \bar{7} =$
$x^2 + \bar{2} \Rightarrow \beta + \gamma = (g+h)(\alpha) = \alpha^2 + \bar{2}$
(direkte Rechnung: $\beta + \gamma = (\alpha^2 + \bar{3}\alpha + \bar{4}) +$
$(\bar{2}\alpha + \bar{3}) = \alpha^2 + \bar{5}\alpha + \bar{7} = \alpha^2 + \bar{2}$)
Subtraktion: $\beta - \gamma = (\alpha^2 + \bar{3}\alpha + \bar{4}) - (\bar{2}\alpha + \bar{3})$
$= \alpha^2 + (\bar{3}-\bar{2})\alpha + (\bar{4}-\bar{3}) = \alpha^2 + \alpha + \bar{1}$

Multiplikation:

$$gh = (x^2 + \bar{3}x + \bar{4})(\bar{2}x + \bar{3}) =$$

$$\bar{2}x^3 + \bar{4}x^2 + \bar{2}x + \bar{2}$$

Division mit Rest: Bestimme $q, r \in \mathbb{F}_5[x]$ mit $gh = qf + r$, $r = \bar{0}$ oder $\operatorname{grad}(r) \leq 2$

$$\bar{2}x^3 + \bar{4}x^2 + \bar{2}x + \bar{2} - \bar{2}(x^3 + x + \bar{1})$$

$$= \bar{4}x^2 \quad (\Rightarrow q = \bar{2},\ r = \bar{4}x^2) \rightarrow$$

$\beta\gamma = r(\alpha) = \bar{4}\alpha^2 = -\alpha^2$

direkte Rechnung: $f(\alpha) = \bar{0}$

$\Rightarrow \alpha^3 + \alpha + \bar{1} = \bar{0} \Rightarrow \alpha^3 = -\alpha - \bar{1}$

Ebenso Multiplikation:

$$\beta \cdot \gamma = (\alpha^2 + \bar{3}\alpha + \bar{4})(\bar{2}\alpha + \bar{3}) =$$

$$\bar{2}\alpha^3 + \bar{4}\alpha^2 + \bar{2}\alpha + \bar{2} =$$

$$\bar{2}(-\alpha - \bar{1}) + \bar{4}\alpha^2 + \bar{2}\alpha + \bar{2} =$$

$$-\bar{2}\alpha - \bar{2} + \bar{4}\alpha^2 + \bar{2}\alpha + \bar{2} = \bar{4}\alpha^2$$

Kehrwertbildung:

Bestimme $u, v \in \mathbb{F}_5[x]$ mit $u \cdot g + v \cdot f = \bar{1}$.

	q	a_n	x_n	y_n
f		$x^3 + x + \bar{1}$	$\bar{1}$	0
g	$x + \bar{2}$	$x^2 + \bar{3}x + \bar{4}$	0	$\bar{1}$
r	$x + \bar{3}$	$\bar{1}$	$-x - \bar{2}$	
	x	$\bar{4}$	$-x$	$x^2 + 2x + \bar{1}$

(*)

$$\Rightarrow \bar{4} = (-x) \cdot f + (x^2 + 2x + \bar{1}) \cdot g$$

$\Rightarrow \bar{1} = x \cdot f + (\bar{4}x^2 + \bar{3}x + \bar{4}) \cdot g$

$\Rightarrow u = \bar{4}x^2 + \bar{3}x + \bar{4}, \quad v = x$

$\Rightarrow \beta^{-1} = u(\alpha) = \bar{4}\alpha^2 + \bar{3}\alpha + \bar{4}$

(*) Polynomdivision ergibt

$$x^3 + x + \bar{1} = (x + \bar{2})(x^2 + \bar{3}x + \bar{4}) + x + \bar{3}$$

Algebraische Erweiterungen als Faktorringe

Satz (14.7)

Sei $L|K$ eine Körpererweiterung, $\alpha \in L$ algebraisch über K und $f = \mu_{\alpha,K}$. Dann gibt es einen Isomorphismus

$$\bar{\phi} : K[x]/(f) \longrightarrow K(\alpha)$$

mit

$$\phi(g + (f)) = g(\alpha) \text{ für alle } g \in K[x].$$

Dabei bezeichnet $K(\alpha)$ den von α erzeugten Zwischenkörper der Erweiterung $L|K$.

Beweis von Satz 14.7

geg. $L|K$ Körpererw., $\alpha \in L$ alg. über K.

$f = M_{\alpha,K}$ Beh: $K[x]/(f) \cong K(\alpha)$

Definiere $\phi: K[x] \to L$ durch $g \mapsto g(\alpha)$.

(Dies ist der Einsetzhomomorphismus.)

Überprüfe: i) $\operatorname{im}(\phi) = K(\alpha)$ (d.h. als Hom $K[x] \to K(\alpha)$ ist ϕ surjektiv)

ii) $\ker(\phi) = (f)$

Wenn (i), (ii) erfüllt sind, dann liefert der Hom.-satz für Ringe ein $\bar{\phi}: K[x]/(f) \to K(\alpha)$ mit

$\Phi(g + (f)) = \phi(g) = g(\alpha) \quad \forall g \in K[x]$

zu (i) „$\subseteq$" Da $K(\alpha)$ als Körper abgeschlossen unter Addition und Multiplikation ist, ist $\phi(g) = g(\alpha)$ für jedes $g \in K[x]$ in $K(\alpha)$ enthalten.

„$\supseteq$" Nach Satz 14.6 gibt es für jedes $\beta \in K(\alpha)$ ein Polynom $g \in K[x]$ mit $\beta = g(\alpha) \Rightarrow \beta = \phi(\alpha) \Rightarrow \beta \in \text{im}(\phi)$

zu (ii) „$\supseteq$" Da $\ker(\phi)$ ein Ideal in $K[x]$ ist, genügt es, $f \in \ker(\phi)$ zu überprüfen. Es gilt $\phi(f) = f(\alpha) = 0_K$.
$\Rightarrow f \in \ker(\phi)$ „$\subseteq$" Sei $g \in \ker(\phi) \Rightarrow \phi(g) = 0_K \rightarrow g(\alpha) = 0_K$
Division mit Rest $\Rightarrow \exists q, r \in K[x]$ mit $g = q \cdot f + r$,

wobei $\operatorname{grad}(r) \leq n-1 < n = \operatorname{grad}(f)$ oder

$r = 0_K$. Ang. $r \neq 0_K$. $r = g - qf$

$\Rightarrow r(\alpha) = g(\alpha) - q(\alpha) \cdot f(\alpha) = 0_K - q(\alpha) \cdot 0_K$

$= 0_K$ $\lightning$ zu Minimalität von $\operatorname{grad}(f)$

$\Rightarrow g = q \cdot f \in (f)$ $\square$

Existenz algebraischer Erweiterungen

Satz (14.8)

Sei K ein Körper und $f \in K[x]$ ein irreduzibles Polynom. Dann gibt es eine Körpererweiterung $L|K$ und ein Element $\alpha \in L$ mit $f(\alpha) = 0$.

Beweis von Satz 14.8

Erinnerung Satz 6.3: Ist $\phi : R \to S$ ein Monomorphismus von Ringen, dann gibt es eine Ringerweiterung $\hat{R} \mid R$ und einen Isomorphismus $\hat{\phi} : \hat{R} \to S$ mit $\hat{\phi}_{|R} = \phi$.

geg: K Körper, $f \in K[x]$ irreduzibel

z.zg: Es gibt einen Erweiterungskörper $L \mid K$ und ein $\alpha \in L$ mit $f(\alpha) = 0_K$.

Sei $S = K[x]/(f)$, und sei $\phi : K \to S$ geg. durch $a \mapsto a + (f)$. Dies ist ein Monomorphismus von Ringen, da er durch

Einschränkung des kanonischen Epimorphismus
$K[x] \to K[x]/(f)$, $g \mapsto g + (f)$ auf $K \subseteq K[x]$
zu Stande kommt. Beh.: ϕ ist injektiv

Sei $a \in \ker(\phi) \Rightarrow \phi(a) = 0_S = (f) \Rightarrow$
$a + (f) = (f) \Rightarrow a \in (f) \Rightarrow f \mid a$
$\operatorname{grad}(a) = 0$ (oder $a = 0_K$)
$\Rightarrow \operatorname{grad}(f) \geq 1$, da f irred. $a = 0_K$ ($\Rightarrow$ Beh.)

Nach Satz 6.3 gibt es einen Erweiterungsring L von K und einen Ringisom.
$\hat{\phi} : L \to S$ mit $\hat{\phi}|_K = \phi$

noch zu zeigen: i) L ist ein Körper

ii) $\exists \alpha \in L$ mit $f(\alpha) = 0_K$

zu i) $K[x]$ ist Hauptidealring (da Polynomring über einem Körper), $f \in K[x]$ ist irreduzibel $\Rightarrow$ (f) ist ein maximales Ideal in $K[x] \Rightarrow$ $K[x]/(f)$ ist ein Körper

zu ii) Sei $\alpha = \hat{\phi}^{-1}(\underbrace{x + (f)}_{\in K[x]/(f) = S}) \in L$.

Beh: $\hat{\phi}(f(\alpha)) = 0_S$

Sei $f = \sum_{k=0}^{n} a_k x^k$ mit $n \in \mathbb{N}_0$, $a_0, \dots, a_n \in K$.

$\hat{\phi}(f(\alpha)) = \hat{\phi}\left(\sum_{k=0}^{n} a_k \alpha^k\right) \overset{\hat{\phi} \text{ Ringhom.}}{=}$

$$\sum_{k=0}^{n} \hat{\phi}(a_k)\,\hat{\phi}(x)^k = \sum_{k=0}^{n} \phi(a_k)\cdot(x+(f))^k$$

$\hat{\phi}|_K = \phi$

$\hat{\phi}(x) = x + (f)$

$$= \sum_{k=0}^{n} (a_k + (f))\cdot(x+(f))^k = \sum_{k=0}^{n} a_k x^k + (f)$$

$= f + (f) = (f) = 0_S$ $(\Rightarrow$ Beh$)$

Da $\hat{\phi}$ injektiv ist, folgt aus der Beh $f(a) = 0_K$. $\square$