Vorlesung Algebra

SoSe'21, hhu
K. Halupczok

Teil III: KÖRPER

A18: Algebraische Erweiterungen

Stichworte: Charakteristik von K, Primkörper, Körpererweiterung $L|K$, Grad $[L:K]$, endliche Erweiterung, Multiplikativität des Körpergrades, der von $x_1,\dots,x_n$ über K erzeugte Körper $K(x_1,\dots,x_n)$, einfache Erweiterung, primitives El., algebraisches El., Minimalpolynom, alg. Erweiterung

---

18.1. Einleitung: Wir studieren Körpererweiterungen, etwa den von $x_1,\dots,x_n$ über K erzeugte Körper $K(x_1,\dots,x_n)$ in einer Körpererweiterung $L|K$. Wir nennen $x\in L$ algebraisch über K, falls x Wurzel (d.h. Nullstelle) eines Polynoms in $K[T]\setminus\{0\}$ ist. Ist jedes $x\in L$ alg. $|K$, heißt L alg. $/K$.

18.2. Def.: Sei K Körper, betr. Ringhom. $\varphi: \mathbb{Z}\to K$, $m\mapsto m_K := m\cdot 1_K$.
Dann: $\varphi(\mathbb{Z}) \cong \mathbb{Z}/\ker\varphi$ mit $\ker\varphi = (r)$, $r\in\mathbb{N}_0$.
Charakteristik von K: $\operatorname{Char} K := r$.

18.3. Lemma: (i) $r\neq 0$: $\varphi(\mathbb{Z})$ keine Nullteiler $\Rightarrow r=p$ prim.
Somit: $K_0 := \varphi(\mathbb{Z}) \cong \mathbb{F}_p$ ist Körper.

(ii) $r=0$: φ injektiv. $K_0 := \left\{\frac{\varphi(m)}{\varphi(n)};\ m,n\in\mathbb{Z},\ n\neq 0\right\}$ ist Quotientenkörper von $\varphi(\mathbb{Z})$.

Dann:
$$\begin{tikzcd} \mathbb{Z} \arrow[r, "\cong"', "\varphi"] \arrow[d] & \varphi(\mathbb{Z}) \subseteq K_0 \\ \mathbb{Q} \arrow[ur, dashed, "{\cong,\ \tilde\varphi}"'] & \end{tikzcd}$$
(Univ. Eig. von Quotientenkörpern)

Somit: φ lässt sich eind. erweitern zu Isom. $\mathbb{Q}\cong K_0$.

In beiden Fällen: K_0 ist kleinster Teilkörper von K.

18.4. Def.: K_0 heißt Primkörper von K.

18.5. Def.: L Körpererweiterung von K: $L|K :\Leftrightarrow L, K$ Körper, $K\subseteq L$

sprich: "L über K" für "$L|K$"

18.6. Def.: $[L:K] := \dim_K L$ heißt (Körper-) Grad von $L|K$.
L endl. Erweiterung von K: $\Leftrightarrow [L:K]$ endl.

Kurz: "Erw." für "Erweiterung"

18.7. Bsp.: $\mathbb{C}|\mathbb{R}$, $[\mathbb{C}:\mathbb{R}]=2$.

18.8. **Satz:** $E|L$ und $L|K$ endl. $\Rightarrow$ $E|K$ endl. und $[E:K] = [E:L]\cdot[L:K]$.
(Multiplikativität des Körpergrades)

Bew.: Sei $x_1, \dots, x_m$ L-Basis von E,
$y_1, \dots, y_n$ K-Basis von L.

Dann: $x_i y_j$ bilden K-Basis von E, denn

erzeugen: Sei $z \in E$, $z = \sum_{i=1}^{m} w_i x_i$, $w_i \in L$,
$w_i = \sum_j a_{ij} y_j$, $1 \leq i \leq m$ $\Rightarrow$ $z = \sum_{i,j} a_{ij} x_i y_j$.

lin. unabh.: Sei nun $\sum_{i,j} a_{ij} x_i y_j = 0$, die $a_{ij} \in K$.

$\Rightarrow 0 = \sum_i \underbrace{\Big(\sum_j a_{ij} y_j\Big)}_{\in L} x_i$

$\Rightarrow \forall i: \sum_j a_{ij} y_j = 0 \Rightarrow \forall i\, \forall j: a_{ij} = 0$. □

18.9. **Def.:** Sei $L|K$, $x_1, \dots, x_n \in L$. Dann:

$K(x_1, \dots, x_n) := \bigcap \{K';\ K \subseteq K' \subseteq L,\ K' \text{ Körper},\ x_1, \dots, x_n \in K'\}$

heißt der von $x_1, \dots, x_n$ über K erzeugte Körper. (sprich: "K adjungiert x_1 bis x_n")
$\rightsquigarrow$ "Körper-Adjunktion"

18.10. **Lemma:** $K(x_1, \dots, x_n)$ ist der Quotientenkörper von $K[x_1, \dots, x_n]$,
d.h. $\forall z \in L$: $z \in K(x_1, \dots, x_n) \Leftrightarrow \exists u, v \in K[x_1, \dots, x_n]: (v \neq 0 \wedge z = \frac{u}{v})$.

Bew.:

$$\begin{tikzcd} K[x_1, \dots, x_n] \arrow[r, hook] \arrow[d] & K(x_1, \dots, x_n) \\ Q \arrow[ur, hook, dashed, "\varphi \text{ inj.}"'] & \end{tikzcd}$$

Sei Q der Quot. Körper von $K[x_1, \dots, x_n]$.
Univ. Eig. von Quot. Körpern
$\Rightarrow \exists \varphi: Q \hookrightarrow K(x_1, \dots, x_n)$.

Nun enthält Q sicher $x_1, \dots, x_n$ sowie K, d.h. $K(x_1, \dots, x_n) \subseteq Q$.

Insgesamt also: $Q = K(x_1, \dots, x_n)$. □

18.11. **Def.:** $L|K$ einfache Erw. von K $:\Leftrightarrow \exists x \in L: L = K(x)$.

Dann: x primitives El. für $L|K$.

18.12. **Def.:** $L|K$. Dann $x \in L$ algebraisch über K $:\Leftrightarrow \exists f \in K[T]: (f \neq 0 \wedge f(x) = 0)$.

Dann: x Wurzel von f. [bzw. Nullstelle von f]

Kurz: x alg. $|K$.

18.13 Bsp.: $\mathbb{R}|\mathbb{Q}$. $\mathbb{R} \ni x = \sqrt[5]{7}$ ist alg.$|\mathbb{Q}$, da Wurzel von $T^5 - 7 \in \mathbb{Q}[T]$.
$\pi \in \mathbb{R}$ ist nicht algebraisch über $\mathbb{Q}$. [Lindemann im Jahr 1882]

18.14 Bsp.: Jedes $x \in \mathbb{R}$ ist alg.$|\mathbb{R}$, da Wurzel von $T - x \in \mathbb{R}[T]$.

18.15 Satz: Das normierte $f \in K[T]$ (d.h. $f \neq 0$, höchster Koeff. $= 1$) von minimalem Grad mit $f(x) = 0$ ist eind. best. und irreduzibel.

Bew.: Eind.: $f_1 - f_2$ hat strikt kleineren Grad, $(f_1 - f_2)(x) = 0 \Rightarrow f_1 - f_2 = 0$.
Irred.: Sei $f = g \cdot h$ mit $g, h \in K[T]$. Dann: $0 = f(x) = g(x) \cdot h(x)$,
OE $g(x) = 0$. Also: $\deg(g) = \deg(f) \Rightarrow h \in K^\times$ (da f normiert). □

18.16 Def.: f (wie in 18.15) heißt Minimalpolynom von x über K, Grad von x über $K := \deg(f)$.
Kurz: $f = \mathrm{Mipo}_K(x)$, $\deg(x) = \deg(f)$.

18.17 Satz: Sei $L|K$, $x \in L$ alg., $f \in K[T]$ das Mipo von $x|K$. Dann:
(i) $K(x) = K[x] \cong K[T]/(f)$ (Körperiso über K, d.h. Körperiso und K-linear)
vermöge: $g(x) \longleftrightarrow g + (f)$
(ii) $[K(x):K] = \deg(f) =: n$,
und $1, x, x^2, \dots, x^{n-1}$ ist K-Basis von $K(x)$.
(iii) Ist $g \in K[T]$ irreduzibel, normiert, mit $g(x) = 0 \Rightarrow g = f$.

Bew.: (i):
$$\begin{tikzcd} K[T] \arrow[r, two heads, "\varphi"] \arrow[d] & K[x] \subseteq L \\ K[T]/\ker\varphi \arrow[ur, dashed, "\bar\varphi\ (\mathrm{Iso})"'] & \end{tikzcd}$$
$\varphi : g \mapsto g(x)$, $\quad \bar\varphi : g + (f) \mapsto g(x)$

Es ist $\ker\varphi = (f)$, denn: $\ker\varphi = \underbrace{(g)}_{\text{Hauptideal}} \Rightarrow f = g \cdot h \Rightarrow h \in K^\times \Rightarrow (g) = (f)$.

Da f irreduzibel, ist (f) maximales Ideal.
(Sonst: $(f) \subsetneq (g) \subsetneq K[T] \Rightarrow f = g \cdot h$ ↯)
$\Rightarrow K[x] \cong K[T]/(f)$ ist Körper, also $K(x) = K[x]$.

(ii): $[K(x):K] = [K[T]/(f) : K] = \deg(f) = n$
und $1, x, x^2, \dots, x^{n-1}$ K-Basis von $K(x)$ nach A14.12.

(iii): $g(x) = 0 \Rightarrow (g) \subseteq (f)$,
g irred. $\Rightarrow (g) = (f) \Rightarrow f = g \cdot h,\ h \in K^\times \xRightarrow{f, g \text{ norm.}} f = g$. □

18.18. Bsp.: Sei $n \in \mathbb{Z}$ kein Quadrat $\Rightarrow x := \sqrt{n} \notin \mathbb{Q}$.
Nun $T^2 - n \in \mathbb{Q}[T]$ irreduzibel.
$\Rightarrow T^2 - n$ ist Mipo von $x|\mathbb{Q}$.
Somit: $[\mathbb{Q}(\sqrt{n}):\mathbb{Q}] = 2$, $\mathbb{Q}(\sqrt{n}) = \{a + b\sqrt{n};\ a,b \in \mathbb{Q}\}$ Körper.

18.19. Bsp.: Sei p prim, $k \geq 1$, $x := \sqrt[k]{p} \in \mathbb{R}$, $\mathbb{Q}(x)|\mathbb{Q}$.
Dann $T^k - p$ irreduzibel nach Eisenstein, also Mipo von $x|\mathbb{Q}$.
Somit: $[\mathbb{Q}(x):\mathbb{Q}] = k$, $\mathbb{Q}(x) = \{a_0 + a_1 x + \ldots + a_{k-1} x^{k-1};\ a_i \in \mathbb{Q}\}$.

18.20 Lemma: Sei $L|K$. Für $x \in L$ sind äquivalent:
(i) x alg. $|K$, (ii) $K(x)|K$ endl.

Bew.: (i)$\Rightarrow$(ii): ✓ nach 18.17, da $[K(x):K] =$ Grad von $x|K$.
(ii)$\Rightarrow$(i): Sei $n := [K(x):K]$. Dann sind $1, x, \ldots, x^n$ K-lin. abh.,
d.h. $\exists a_0, \ldots, a_n \in K$, nicht alle $a_i = 0$: $a_0 + a_1 x + \ldots + a_n x^n = 0$
$\Rightarrow x$ ist Wurzel von $f := \sum_{i=0}^{n} a_i T^i \neq 0$. □

18.21. Def.: $L|K$ heißt algebraisch $:\Leftrightarrow \forall x \in L:\ x$ alg. $|K$.

18.22. Satz: Sei $L = K(x_1, \ldots, x_n)$ eine endl. erz. Erw. Dann sind äquivalent:
(1) $x_1, \ldots, x_n$ alg. $|K$, (2) $L|K$ alg., (3) $L|K$ endl.

Bew.: (3)$\Rightarrow$(2): Sei $x \in L$. Dann: $K(x)$ ist K-Unterraum von L,
also endl. dim. $\underset{18.20}{\Rightarrow}$ x alg. $|K$. Somit $L|K$ alg.
(2)$\Rightarrow$(1): trivial, (1)$\Rightarrow$(3):

Betr.

$$\begin{array}{c} K_n = K(x_1, \ldots, x_n) = L \\ | \\ \vdots \\ | \\ K_2 = K(x_1, x_2) \\ | \\ K_1 = K(x_1) \\ | \\ K_0 = K \end{array}$$

„Körperturm"

$\forall i$: x_i ist alg. $|K$
$\Rightarrow x_i$ ist alg. $|K_{i-1}$
$\underset{18.20}{\Rightarrow} K_i = K_{i-1}(x_i)|K_{i-1}$ endl.
Somit $L|K$ endl. nach 18.8,
und $[L:K] = \prod_{i=1}^{n} [K_i : K_{i-1}]$.

□