Algebra B III

– Kuhlmann –

9. Vorlesung am 22. 11. 2012.

Satz 1. Sei $p(x) \in F[x]$ irreduzibel, $\deg p(x) = n$.

Es gilt $[K : F] = n$ wobei $K := F[x]/_{\langle p(x) \rangle}$

Bew. Setze $\bar{x} := \theta$

Wir behaupten: $\Theta := \{1, \theta, \theta^2, \dots, \theta^{n-1}\}$ ist eine F-Basis

für K.

- Sei $a(x) \in F[x]$; schreibe

$$a(x) = q(x)\,p(x) + r(x) \qquad r(x) = 0 \text{ oder } \deg r(x) < n$$

also $a(x) + \langle p(x) \rangle = r(x) + \langle p(x) \rangle$

d.h. $\overline{a(x)} = \overline{r(x)}$ $\qquad$ schreibe $r(x) = \sum_{i=0}^{n-1} a_i x^i$

$\qquad \| $

d.h. $a(\bar{x}) = r(\bar{x})$ $\qquad$ $a_i \in F$

i.e $\overline{a(x)} = r(\theta)$ also $K \ni \overline{a(x)} \in \operatorname{span} \Theta$

- Θ ist l. unabh. über F: seien $b_0, \dots, b_{n-1} \in F$ mit $\sum b_i \theta^i = 0$. Setze $b(x) := \sum b_i x^i$. Es ist:

$0 = b(\theta) = \overline{b(x)}$; also $b(x) \in \langle p(x) \rangle$

und $\deg b(x) < \deg p(x)$; und damit

muss $b(x) = 0$ das Nullpolynom sein ;

i.e. $b_i = 0 \quad \forall i = 0, \dots, n-1.$ $\blacksquare$

<u>Bem:</u> $K = \{ a(\theta) ; \; a(x) \in F[x], \deg a(x) < n \}$

mit $a(\theta) + b(\theta) = (a+b)(\theta) \qquad \forall a(x), b(x) \in F[x]$

und $a(\theta) b(\theta) = r(\theta)$ wobei

$\deg r(x) < n$; $r(x) \in F[x]$ ist der

Rest in E.A:

$$a(x) b(x) = q(x) p(x) + r(x).$$ $\blacksquare$

<u>Definition:</u> 1. Sei $K|F$ KE ; $S \subseteq K$.
<u>Notation</u>

$F(S) :=$ der kleinste Unterkörper von K der $F \cup S$ enthält
$= \bigcap \{ L \mid L \subseteq K$ unterkörper; $L \supseteq F \cup S \}$

$F(S)$ heißt: der <u>Körper der von S über F erzeugt ist.</u>

2. Wenn $S = \{\alpha_1, \dots, \alpha_s\}$ endlich ist, schreiben wir $L = F(\alpha_1, \dots, \alpha_n)$ und sagen: L ist <u>endlich erzeugt über F.</u>

3. Wenn $S = \{\alpha\}$ heißt $L = F(\alpha)$ eine <u>einfache Erweiterung</u>; und α heißt ein <u>primitives Element</u> für die KE $L|F$.

<u>Satz 2.</u> Sei $p(x) \in F[x]$ irreduzible; $\alpha \in K|F$ eine NS.

Es ist : $F(\alpha) \simeq F[x]/\langle p(x)\rangle$.

<u>Bew.</u> Betrachte $\varphi : F[x]/_{\langle p(x)\rangle} \longrightarrow F(\alpha) \leq K$

$$a(x) + \langle p(x)\rangle \longmapsto a(\alpha)$$

- Es ist : $\varphi|_F = Id|_F$ (i.e $\varphi(r) = r \quad \forall r \in F$)

  und $\varphi(x) = \alpha$

- φ ist wohldefiniert : $a(x) \equiv b(x) \bmod \langle p(x)\rangle$

  $\Leftrightarrow a(x) - b(x) = p(x)q(x)$

  also $a(\alpha) - b(\alpha) = 0$ und damit

  $a(\alpha) = b(\alpha)$

- $\varphi \neq 0$ (e.g $\varphi|_F = Id|_F$) also φ ist ein injektiver Ringhom- und damit ist

$$\varphi : F[x]/_{\langle p(x)\rangle} \simeq Bi(\varphi) \underset{\text{Unterkörper}}{\subseteq} F(\alpha) \leq K$$

Also ist $Bi(\varphi)$ ein Unterkörper von K; und

enthält $F \cup \{\alpha\}$, und somit ist $F(\alpha) \subseteq Bi(\varphi)$.

Also $Bi(\varphi) = F(\alpha)$. $\square$

Korollar 1 $K | F$ KE; $\alpha \in K$ NS

vom irreduziblem $p(x) \in F[x]$, $\deg p = n$.

Es ist: $F(\alpha) = \{ a(\alpha) \mid a(x) \in F[x];\ \deg a(x) < n \}$ $\square$

Korollar 2. $\alpha, \beta \in K|F$, $p(x) \in F[x]$ irred; mit
$p(\alpha) = p(\beta) = 0$

Es ist: $F(\alpha) \simeq F[x]/_{\langle p(x) \rangle} \simeq F(\beta)$. $\square$

Allgemeiner betrachten wir folgenden Ansatz:

$$\begin{tikzcd} F(\alpha) \arrow[r, dashed, "?"] \arrow[d, dash] & F'(\beta) \arrow[d, dash] \\ F \arrow[r, "\sim", "\varphi"'] & F' \end{tikzcd}$$

Satz 3. Seien: F, F' Körper

$$\varphi : F \xrightarrow{\sim} F'$$

$p(x) \in F[x]$
irreduzible.

Setze $p(x) = \sum a_i x^i$ und $p'(x) := \sum \varphi(a_i)\, x^i$ (Anwendung von φ auf Koeffiz.)

Dann ist $p'(x) \in F'[x]$ irreduzible.

Sei $\alpha \in K|F$ und $\beta \in K'|F'$
mit $p(\alpha) = 0$ mit $p'(\beta) = 0$.

Dann läßt sich φ zu einer Isomorphie φ' fortsetzen

$$\varphi' : F(\alpha) \longrightarrow F'(\beta)$$

$$\varphi'\restriction_F = \varphi \quad \text{und} \quad \varphi'(\alpha) = \beta.$$

Bew 1. $p'(x)$ ist irreduzible weil eine Faktorisierung

$$p'(x) = a'(x)\, b'(x) \qquad \text{mit } \deg a'(x) \geq 1$$
$$\deg b'(x) \geq 1$$
$$a'(x),\ b'(x) \in F'[x]$$

eine Faktorisierung (durch Anwendung von φ^{-1} auf Koeffiz.)

$$p(x) = a''(x)\, b''(x) \quad \text{von } p(x) \text{ in } F[x]$$
induziert

$\deg(a''(x)) \geq 1$; $\deg(b''(x)) \geq 1$; $a''(x), b''(x) \in F[x]$.

2. $F[x] \simeq F'[x]$ und $\langle p(x) \rangle \simeq \langle p'(x) \rangle$

(durch Anwendung von φ auf Koeffiz.)

Also $F(\alpha) \simeq F[x]/_{\langle p(x) \rangle} \simeq F'[x]/_{\langle p'(x) \rangle} \simeq F(\beta)$. ∎