9. Script zur Vorlesung: Algebra (B III)

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

WS 2016/2017: 25. November 2016

Satz 1

Sei $p(x) \in F[x]$ irreduzibel; $\deg p(x) = n, n \in \mathbb{N}$.
Es gilt $[K : F] = n$, wobei $K := F[x]/ < p(x) >$.

Beweis

Setze $\overline{x} := \theta$. Wir behaupten $O := \{1, \theta, \theta^2, \ldots, \theta^{n-1}\}$ ist eine F-Basis für K.

- Sei $a(x) \in F[x]$. Schreibe $a(x) = q(x)p(x) + r(x)$ mit $r(x) = 0$ oder $\deg r(x) < n$.
  Also $a(x)+ < p(x) >= r(x)+ < p(x) >$,

  $$\begin{array}{lccc} \text{d. h.} & \overline{a(x)} & = & \overline{r(x)} \\ & \shortparallel & & \\ \text{d. h.} & a(\overline{x}) & = & r(\overline{x}) \end{array}$$

  Schreibe $r(x) = \sum_{i=0}^{n-1} a_i x^i, a_i \in F$, i.e. $\overline{a(x)} =: r(\theta)$, also $K \ni \overline{a(x)} \in \operatorname{span} O$.

- O ist linear unabhängig über F: Seien $b_0, \ldots, b_{n-1} \in F$ mit $\sum b_i \theta^i = 0$.
  Setze $b(x) := \sum b_i x^i$. Es ist: $0 = b(\theta) = \overline{b(x)}$. Also $b(x) \in < p(x) >$ und $\deg b(x) < \deg p(x)$ und damit muss $b(x) = 0$ das Nullpolynom sein, i.e. $b_i = 0$ für alle $i = 0, \ldots, n-1$. $\square$

Bemerkung

$K = \{a(\theta), a(x) \in F[x], \deg a(x) < n\}$ mit $a(\theta) + b(\theta) = (a+b)(\theta)$ für alle $a(x), b(x) \in F[x]$ und $a(\theta)b(\theta) = r(\theta)$ (wobei $\deg r(x) < n; r(x) \in F[x]$ der Rest in E.A. ist; $a(x)b(x) = q(x)p(x) + r(x)$).

Definition

(1) Sei K/F eine Körpererweiterung; $S \subseteq K$.
Notation: $F(S)$ = der kleinste Unterkörper von K, der $F \bigcup S$ enthält $= \bigcap \{L \mid L \subseteq K$ Unterkörper $; L \supseteq F \bigcup S\}$.
$F(S)$ heißt der *Körper der von S über F erzeugt ist.*

(2) Wenn $S = \{\alpha_1, \ldots, \alpha_n\}$ endlich ist, schreiben wir $L = F(\alpha_1, \ldots, \alpha_n)$ und sagen: L ist *endlich erzeugt über F.*

(3) Wenn $S = \{a\}$ heißt $L = F(a)$ eine *einfache Erweiterung* und a heißt ein *primitives Element* für die Körpererweiterung L/F.

Satz 2

Sei $p(x) \in F[x]$ irreduzibel; $\alpha \in K/F$ eine Nullstelle. Es ist: $F(\alpha) \simeq F[x]/ < p(x) >$.

Beweis

Betrachte

$$\begin{array}{rccc} \varphi: & F[x]/ < p(x) > & \to & F(\alpha) \subseteq K \\ & a(x)+ < p(x) > & \mapsto & a(\alpha) \end{array}$$

- Es ist $\varphi \restriction_F = Id \restriction_F$ (i.e. $\varphi(r) = r$ für alle $r \in F$) und $\varphi(\overline{x}) = \alpha$.
- φ ist wohldefiniert: $a(x) \equiv b(x) \mod < p(x) > \Leftrightarrow a(x) - b(x) = p(x)q(x)$. Also $a(\alpha) - b(\alpha) = 0$ und damit $a(\alpha) = b(\alpha)$.
- $\varphi \neq 0$ (e.g. $\varphi \restriction_F = Id \restriction_F$), also φ ist ein injektiver Ringhomomorphismus und damit ist $\varphi : F[x]/ < p(x) > \simeq Bi(\varphi) \subseteq F(\alpha) \subseteq K$ ein Unterkörper. Also ist $Bi(\varphi)$ ein Unterkörper von K und enthält $F \bigcup \{\alpha\}$ und somit ist $F(\alpha) \subseteq Bi(\varphi)$. Also $Bi(\varphi) = F(\alpha)$. $\square$

Korollar 1

K/F ist eine Körpererweiterung; $\alpha \in K$ ist Nullstelle vom irreduziblen $p(x) \in F[x]; \deg p = n$.
Es ist $F(\alpha) = \{a(\alpha) \mid a(x) \in F[x]; \deg a(x) < n\}$.

Korollar 2

$\alpha, \beta \in K/F; p(x) \in F[x]$ ist irreduzibel mit $p(\alpha) = p(\beta) = 0$.
Es ist $F(\alpha) \simeq F[x]/ < p(x) > \simeq F(\beta)$.

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. $\varphi : F \xrightarrow{\sim} F'$ und $p(x) \in F[x]$ irreduzibel.
Setze $p(x) = \sum a_i x^i$ und $p'(x) := \sum \varphi(a_i)x^i$ (Anwendung von φ auf Koeffizienten). Dann ist $p'(x) \in F'[x]$ irreduzibel.
Sei $\alpha \in K/F$ mit $p(\alpha) = 0$ und $\beta \in K'/F'$ mit $p'(\beta) = 0$. Dann läßt sich φ zu einer Isomorphie φ' fortsetzen

$$\begin{array}{ccc} \varphi' : F(\alpha) & \to & F'(\beta) \\ \varphi' \restriction_F = \varphi & \text{und} & \varphi'(\alpha) = \beta \end{array}.$$

Beweis

(1) $p'(x)$ ist irreduzibel, weil eine Faktorisierung $p'(x) = a'(x)b'(x)$ 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 Koeffizienten) $p(x) = a''(x)b''(x)$ von $p(x)$ in $F[x]$ induziert, mit $\deg(a''(x)) \geq 1, \deg(b''(x)) \geq 1; a''(x), b''(x) \in F[x]$.

(2) $F[x] \simeq F'[x]$ und $< p(x) > \simeq < p'(x) >$ (durch Anwendung von φ auf Koeffizienten). Also $F(\alpha) \simeq F[x]/ < p(x) > \simeq F'[x]/ < p'(x) > \simeq F(\beta)$. □