Algebra B III

- Kahlmann -

14. Vorlesung

Am 13. 12. 2012.

Erinnerung: $f(x) \in F[x]$; α ist eine mehrfache NS
$\deg f \geq 1$
$\Leftrightarrow$ α ist NS von $Df(x)$ $\Leftrightarrow$

$m_{\alpha, F} \mid f(x)$ und $m_{\alpha, F} \mid Df(x)$.

Korollar 1. Sei $f(x)$ irreduzibel.
$\deg f \geq 1$
Es gilt: f ist inseparable genau dann wenn $Df \equiv 0$
(Das heißt f hat mehrfache NS $\Leftrightarrow$ $Df \equiv 0$).

Bew. α ist mehrfache NS $\Leftrightarrow$ $m_{\alpha, F}$ g.T von f und Df.

Nun f irred $\Rightarrow$ $\deg m_{\alpha, F} = \deg f > \deg Df$,

also $m_{\alpha, F} \mid Df \Rightarrow Df \equiv 0$. ∎

Beisp. (1) $f(x) = x^{p^m} - x \in \mathbb{F}_p[x]$
$Df(x) = p^m x^{p^m - 1} - 1 = -1$
Df hat gar keine NS;
also f ist separable.

(2) $f(x) = x^n - 1$ Annahme:

$Df(x) = n x^{n-1}$ Char $F = 0$ oder

Char $F = p \nmid n$

Dann ist $Df \neq 0$ und hat 0 als

einzige NS; 0 ist aber keine NS von f,

also f ist separable, und die Gleichung

$$x^n - 1 = 0$$

hat n paarweise verschiedene NS;

(die heißen die n n^{te} Einheitswurzel).

(3) $f(x) = x^n - 1$ char $F = p \mid n$

$Df(x) = n x^{n-1} \equiv 0$

$\Rightarrow$ f ist inseparable. ∎

Korollar 2. Sei Char $F = 0$.

(i) Sei $f \in F[X]$ irreduzible (mit $\deg f \geq 1$).

Dann ist f separable.

allgemeiner (ii) $f(x)$ ist separable gdw $f = c \prod p_i(x)$; $p_i \neq p_j$; p_i irreduzibl

$0 \neq c \in F$ für $i \neq j$ normiert

Bew.

(i) $f \neq 0 \Rightarrow Df \neq 0$ (weil Char $F = 0$).

(ii) verschiedene irreduzible (normierte) können keine

gemeinsame NS wegen Eindeutigkeit der

Min Pols. In der Primfaktorisierung

$$f = c \prod_{i=1}^{k} p_i(x) \qquad p_i \neq p_j$$

haben außerdem keine der Faktoren mehrfache NS

(folgt aus (i)). Also hat f keine " " ∎

Bsp. (4) $f = x^2 - t \in \mathbb{F}_2(t)[x]$

f ist irreduzible weil $\sqrt{t} \notin \mathbb{F}_2(t)$.

$Df \equiv 0$; also f irreduzible aber inseparable !

Bem. Sei $f(x) = g(x^p) \in F[x]$ Char $F = p > 0$
deg $f \geq 1$

i.e. $f(x) = \gamma_m (x^p)^m + \dots + \gamma_1 x^p + \gamma_0$ ⊛

Also $Df(x) \equiv 0$ und f ist inseparable.

Umgekehrt: $f(x) \in F[x]$ mit $Df \equiv 0$ muss
deg $f \geq 1$

die Gestalt ⊛ haben i.e. $f(x) = g(x^p)$ mit $g(X) \in F[x]$.

Proposition 1. (ü B) Sei $\mathrm{char}\, F = p > 0$

Es gelten: $(a+b)^p = a^p + b^p$ $\quad \forall a, b \in F$

$(ab)^p = a^p b^p$

und $\varphi : F \longrightarrow F$, $a \longmapsto a^p$

ist ein injektiver Körper Homomorphismus (Frobenius). ∎

Korollar 3 $\mathbb{F}$ endlich $\Rightarrow$ $\varphi : \mathbb{F} \longrightarrow \mathbb{F}$, $a \longmapsto a^p$

ist auch surjektiv, also ein Automorphismus.

D.h: $\mathbb{F} = \mathbb{F}^p := \{ a^p ; a \in \mathbb{F} \}$.

Bew. $\mathbb{F}$ ist endlich also endlich dimensional über den Primkörper $\mathbb{F}_p$; und kann also nicht Isomorph sein zu einem echten Unterraum.

(LA I Kor. 4 13. Vor 02. 12. 2011). ∎

Proposition 2 Jedes irreduzibles Polynome über ein endlicher $\mathbb{F}$ Körper ist separable.

Ein Polynom $f(x) \in \mathbb{F}[X]$ $(\deg f \geq 1)$ ist separable $\Leftrightarrow$ Produkt von paarweise verschieden irreduzible Polynome.

↑ Korollar 2 also gilt auch für endliche Körper!

Bew. Sei $f \in \mathbb{F}[x]$; $\operatorname{Char} \mathbb{F} =: p > 0$

$\deg f \geq 1$; f irreduzible.

f insep. $\Leftrightarrow Df \equiv 0 \Leftrightarrow f(x) = g(x^p)$.

Berechne:

$$f(x) = g(x^p) = a_m (x^p)^m + \dots + a_1 x^p + a_0$$

$$= b_m^p (x^m)^p + \dots + b_1^p x^p + b_0^p$$

$$= (b_m x^m)^p + \dots + (b_1 x)^p + b_0^p$$

$$= (b_m x^m + \dots + b_1 x + b_0)^p . \quad \lightning \quad \blacksquare$$

Bem. Wichtig war: $\mathbb{F}^p = \mathbb{F}$.

Definition Ein Körper F heißt perfekt,

falls $\operatorname{Char} F = 0$ oder $\operatorname{Char} F = p > 0$ und $F = F^p$.

Proposition 3: Proposition 2 gilt für F perfekt (anstatt $\mathbb{F}$ endlich) $\blacksquare$

Kapitel 3. (Endliche) Gruppen.

Definition. Sei G eine Gruppe; $H \subseteq G$ ist eine Untergruppe falls

H eine Gruppe ist (mit der Verknüpfung von G);

d.h $H \neq \emptyset$; $x, y \in H \Rightarrow xy \in H$, $x^{-1} \in H$.

Definition 2 (i) Seien G, H gruppen, eine Abbildung

$\varphi : G \longrightarrow H$ ist ein **Gruppenhomomorphismus**

wenn $\varphi(xy) = \varphi(x)\varphi(y)$ $\forall x, y \in G$

(ii) ein bijektiver Homomorph. heißt

Isomorphismus.

Notation: $|G| := \begin{cases} \#\text{ der Elementen in } G & \text{falls } G \text{ endlich} \\ \infty & \text{Sonst.} \end{cases}$
