

14. Script zur Vorlesung: Algebra (B III)

Prof. Dr. Salma Kuhlmann, Dr. Lorna Gregory, Katharina Dupont

WS 2012/2013: 13. Dezember 2012

(WS 2015/2016: Korrekturen vom 28. Januar 2016)

Erinnerung

$f(x) \in F[x]$ ($\deg f \geq 1$); α ist eine mehrfache Nullstelle $\Leftrightarrow \alpha$ ist Nullstelle von $Df(x) \Leftrightarrow m_{\alpha,F} | f(x)$ und $m_{\alpha,F} | Df(x)$.

Korollar 1

Sei $f(x)$ ($\deg f \geq 1$) irreduzibel. Es gilt: f ist inseparabel genau dann, wenn $Df = 0$. (Das heißt, dass f eine mehrfache Nullstelle hat $\Leftrightarrow Df = 0$).

Beweis

α ist eine mehrfache Nullstelle $\Leftrightarrow m_{\alpha,F}$ ggT von f und Df .

Nun ist f irreduzibel $\Rightarrow \deg m_{\alpha,F} = \deg f > \deg Df$. Also $m_{\alpha,F} | Df \Rightarrow Df \equiv 0$. □

Beispiel

$$(1) f(x) = x^{p^n} - x \in \mathbb{F}_p[x]$$

$$Df(x) = p^n x^{p^n-1} - 1 = -1$$

Df hat gar keine Nullstelle, also ist f separabel.

$$(2) f(x) = x^n - 1; Df(x) = nx^{n-1}$$

Annahme: $\text{Char } F = 0$ oder $\text{Char } F := p \nmid n$. Dann ist $Df \not\equiv 0$ und hat 0 als einzige Nullstelle. 0 ist aber keine Nullstelle von f , also ist f separabel und die Gleichung

$$x^n - 1 = 0$$

hat n paarweise verschiedene Nullstellen. (Sie heißen die n te Einheitswurzel.)

$$(3) f(x) = x^n - 1; \text{Char } F = p | n; Df(x) = nx^n - 1 \equiv 0 \Rightarrow f \text{ ist inseparabel.} \quad \square$$

Korollar 2

Sei $\text{Char } F = 0$.

(i) Sei $f \in F[x]$ irreduzibel (mit $\deg f \geq 1$). Dann ist f separabel. Allgemeiner

(ii) $f(x)$ ist separabel genau dann, wenn $f = c \prod p_i(x); 0 \neq c \in F; p_i \neq p_j$ für $i \neq j$ p_i ist irreduzibel normiert.

Beweis

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

(ii) Verschiedene Irreduzible (normierte) können keine gemeinsame Nullstelle wegen Eindeutigkeit des Minimal-Polynoms in der Primfaktorisation

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

haben. Außerdem hat keiner der Faktoren eine mehrfache Nullstelle (folgt aus (i)). Also hat f keine mehrfache Nullstelle. \square

Beispiel

(4) $f = x^2 - t \in \mathbb{F}_2(t)[x]$. f ist irreduzibel, weil $\sqrt{t} \notin \mathbb{F}_2(t)$.

$Df \equiv 0$, also ist f irreduzibel, aber inseparabel.

Bemerkung

Sei $f(x) = g(x^p) \in F[x]$ $\text{Char } F = p > 0$; $\deg f \geq 1$

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

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

Umgekehrt: $f(x) \in F[x]$ ($\deg f \geq 1$) mit $Df \equiv 0$ muss die Gestalt (*) haben, i.e. $f(x) = g(x^p)$ mit $g(x) \in F[x]$.

Proposition 1 (Übungsaufgabe)

Sei $\text{Char } F = p > 0$.

Es gelten $(a+b)^p = a^p + b^p$ für alle $a, b \in F$

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

und $\varphi : F \rightarrow F$

$$a \mapsto a^p$$

ist ein injektiver Körper-Homomorphismus (Frobenius).

Korollar 3

\mathbb{F} ist endlich $\Rightarrow \varphi : \mathbb{F} \rightarrow \mathbb{F}$

$$a \mapsto a^p$$

ist auch surjektiv, also ein Automorphismus. Das heißt $\mathbb{F} = \mathbb{F}^p := \{a^p; a \in \mathbb{F}\}$.

Beweis

\mathbb{F} ist endlich, also endlich dimensional über den Primkörper \mathbb{F}_p und kann also nicht isomorph sein zu einem echten Unterraum (siehe Korollar 4 aus "Lineare Algebra I", 13. Vorlesung vom 2.12.2011).

Proposition 2

Jedes irreduzible Polynom über einen endlichen Körper \mathbb{F} ist separabel. Ein Polynom $f(x) \in \mathbb{F}[x]$ ($\deg f \geq 1$) ist separabel \Leftrightarrow Produkt von paarweise verschiedenen irreduziblen Polynomen. (Korollar 2 gilt also auch für endliche Körper.)

Beweis

Sei $f \in \mathbb{F}[x]$ ($\deg f \geq 1$); Char $\mathbb{F} := p > 0$, f irreduzibel.

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

Berechne:

$$\begin{aligned} f(x) = g(x^p) &= a_m(x^p)^m + \cdots + a_1x^p + a_0 \\ &= b_m^p(x^m)^p + \cdots + b_1^p x^p + b_0^p \\ &= (b_mx^m)^p + \cdots + (b_1x)^p + b_0^p \\ &= (b_mx^m + \cdots + b_1x + b_0)^p \end{aligned}$$

Widerspruch. □

Bemerkung

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

Definition

Ein Körper F heißt *perfekt*, falls Char $F = 0$ oder Char $F = p > 0$ und $F = F^p$.

Proposition 3

Proposition 2 gilt für F perfekt (anstatt \mathbb{F} endlich).

Kapitel 3: (Endliche Gruppen)**Definition 1**

Sei G eine Gruppe. $H \subseteq G$ ist eine *Untergruppe*, falls H eine Gruppe ist (mit der Verknüpfung von G), das heißt $H \neq \emptyset; x, y \in H \Rightarrow xy \in H, x^{-1} \in H$.

Definition 2

(i) Seien G, H Gruppen. Eine Abbildung $\varphi : G \rightarrow H$ ist ein *Gruppenhomomorphismus*, wenn $\varphi(xy) = \varphi(x)\varphi(y)$ ist für alle $x, y \in G$.

(ii) Ein bijektiver Homomorphismus heißt *Isomorphismus*.

Notation: $|G| := \begin{cases} \# & \text{der Elemente in } G, \text{ falls } G \text{ endlich} \\ \infty & \text{sonst} \end{cases}$