13 Script zur Vorlesung: Algebra 1 (WiSe2020-2021)

Prof. Dr. Salma Kuhlmann

In diesem Skript werden wir Kapitel 2 beenden. Im Abschnitt 14 werden wir LA II Skript 4 ergänzen, indem wir die Vielfachheit der Nullstellen in einem Grundkörper F ($Char(F) = 0$ oder $Char(F) = p$) untersuchen.

§14: Separable und inseparable Körpererweiterung

Definition 13.1.
Sei $f(x) \in F[x]$, mit $f(x) = a_n x^n + \cdots + a_0$, $\deg f \geq 1$, und sei K/F ein Zerfällungskörper für f. Dann ist

$$f(x) = (x - \alpha_1)^{n_1}(x - \alpha_2)^{n_2} \cdots (x - \alpha_k)^{n_k}$$

in $K[x]$; mit $n_i \geq 1$, $\alpha_i \neq \alpha_j$ für $i \neq j$.

- n_i ist die *Vielfachheit* der Nullstelle α_i.
- α_i ist eine *mehrfache* Nullstelle, wenn $n_i > 1$, sonst ist
- α_i eine *einfache* Nullstelle.

Definition 13.2. Sei $f(x) \in F[x]$ mit $\deg f \geq 1$.
(1) f ist *separabel*, wenn es nur einfache Nullstellen hat.
(2) f nicht separabel heißt *inseparabel*.

Definition 13.3. Sei $f(x) = a_n x^n + \cdots + a_0 \in F[x]$, die *Ableitung* Df von f ist
$Df(x) = D(a_n x^n + \cdots + a_0) = n a_n x^{n-1} + \cdots + a_1 \in F[x]$.
$D : F[x] \to F[x]$ ist *Ableitungsoperator* und erfüllt die Produktregel

$$Dfg = gDf + fDg.$$

Bemerkung 13.4.
Sei $f(x) \in F[x]$ mit $\deg f = n \geq 1$.

1. $Df = 0$ oder $\deg Df < \deg f$ gilt immer.
2. Sei Char $F = 0$, dann ist $Df \neq 0$, weil zum Beispiel $na_n \neq 0$, für den Hauptkoeffizient $a_n \neq 0$ von f.
3. Sei p eine Primzahl und Char $F = p$. Betrachte $f(x) = x^p \in F[x]$. Dann ist $\deg f(x) > 1$, jedoch ist $Df(x) = px^{p-1} = 0$.

Proposition 13.5.
Sei $f(x) \in F[x]$ mit $\deg f \geq 1$. Eine Nullstelle α für $f(x)$ ist eine mehrfache Nullstelle genau dann, wenn α auch eine Nullstelle für $Df(x)$ ist. Das heißt,

$$\{x; x \text{ ist eine mehrfache Nullstelle von } f\} = \{x; x \text{ ist eine gemeinsame Nullstelle von } f \text{ und } Df\}.$$

Beweis:

"⇒" Sei α eine mehrfache Nullstelle. Schreibe $f(x) = (x-\alpha)^n g(x)$ mit $n \geq 2$.
Berechne $Df(x) = n(x-\alpha)^{n-1}g(x) + (x-\alpha)^n Dg(x)$; $n-1 \geq 1 \Rightarrow \alpha$ ist Nullstelle von $Df(x)$.

"⇐" Sei α eine gemeinsame Nullstelle von $f(x)$ und $Df(x)$.
Schreibe $f(x) = (x-\alpha)h(x)$. $(*)$
Also ist $Df(x) = h(x) + (x-\alpha)Dh(x)$. Beim Einsetzen von α für x, ergibt das $h(\alpha) = 0$.
Zurück in $(*)$ ergibt es $f(x) = (x-\alpha)^2 h_1(x)$. □

Bemerkung 13.6. Sei $f(x) \in F[x]$ mit $\deg f \geq 1$; α eine Nullstelle, und $m_{\alpha,F} \in F[x]$ das minimal Polynom. Dann ist α auch Nullstelle von $Df(x) \Leftrightarrow m_{\alpha,F} \,/\, Df(x)$.

Lemma 13.7.
Die gemeinsamen Nullstellen von f und Df sind die Nullstellen von ggT (f, Df).

Beweis:

"⇐" α ist Nullstelle von ggT $(f, Df) \to \alpha$ ist Nullstelle von f und Df. Ist klar, ÜA.

"⇒" Sei α eine Nullstelle von f und Df. Da $m_{\alpha,F} \,/\, f$ und $m_{\alpha,F} \,/\, Df$, $m_{\alpha,F} /$ ggT (f, Df) auch.
Da α Nullstelle von $m_{\alpha,F}$ ist, folgt nun α ist Nullstelle von ggT (f, Df). □

Korollar 13.8.
Sei $f \in F[x]$ mit $\deg f \geq 1$ ein normiertes Polynom. Dann ist f separabel genau dann, wenn ggT $(f, Df) = 1$.

Beweis:

"⇐" Folgt aus Proposition 13.5 und Lemma 13.7.

"⇒" f separabel $\Rightarrow$ f hat keine gemeinsame Nullstelle mit Df (s. Proposition 13.5)
$\Rightarrow$ ggT $(f, Df) = 1$ (ÜA). □

Korollar 13.9.
Sei $f(x)$ mit $\deg f \geq 1$ ein irreduzibles Polynom. Es gilt: f ist inseparabel genau dann, wenn $Df = 0$.

Beweis:
α ist eine mehrfache Nullstelle von $f \Leftrightarrow m_{\alpha,F}$ ist gT von f und Df (s. Bemerkung 13.6). Nun f irreduzibel $\Rightarrow \deg m_{\alpha,F} = \deg f$. Also $m_{\alpha,F} \,/\, Df \Leftrightarrow Df = 0$ (s. Bemerkung 13.4 (1)). □

Beispiel 13.10.

(1) Sei $f(x) = x^{p^n} - x \in \mathbb{F}_p[x]$.
Berechne $Df(x) = p^n x^{p^n-1} - 1 = -1$.
Df hat gar keine Nullstelle, also ist f separabel.

(2) Sei F so dass Char $F = 0$ oder Char $F := p \nmid n$. Sei $f(x) = x^n - 1$, berechne $Df(x) = nx^{n-1}$.
Dann ist $Df \neq 0$ 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. Diese Nullstellen heißen die $n$te *Einheitswurzel*.

(3) Sei nun F so dass Char $F = p | n$. Für $f(x) = x^n - 1$, $Df(x) = nx^{n-1} = 0 \Rightarrow f$ ist inseparabel.

Korollar 13.11.
Sei Char $F = 0$, und $f \in F[x]$ mit $\deg f \geq 1$.

1. Wenn f irreduzibel, dann ist f separable.
2. Allgemeiner gilt: $f(x)$ ist separabel genau dann, wenn die Primfaktorisierung von f in $F[x]$ diese Gestalt hat:

   $f = c\prod_{i=1}^{k} p_i(x)$; $0 \neq c \in F$, $p_i \in F[x]$ sind irreduzibel und normiert, **und** $p_i \neq p_j$ für $i \neq j$.

Beweis:

1. $f \neq 0 \Rightarrow Df \neq 0$ (weil Char $F = 0$).
2. "$\Leftarrow$" Wegen Eindeutigkeit des minimal Polynoms, können verschiedene irreduzible, normierte Polynome in $F[x]$ keine gemeinsame Nullstelle in K haben (ÜA). In der Primfaktorisierung
   $$f = c\prod_{i=1}^{k} p_i(x) \qquad p_i \neq p_j$$
   haben außerdem keiner der Faktoren eine mehrfache Nullstelle (folgt aus 1.). Also hat f keine mehrfache Nullstelle, f ist separabel.

"$\Rightarrow$": Analog (ÜA). □

Beispiel 13.12.
$f = x^2 - t \in \mathbb{F}_2(t)[x]$. f ist irreduzibel, weil $\sqrt{t} \notin \mathbb{F}_2(t)$ (ÜA).
$Df = 0$, also ist f irreduzibel, aber inseparabel.

Bemerkung 13.13.
Sei Char $F = p > 0$; $g \in F[x]$, $\deg g \geq 1$. Setze $f(x) := g(x^p)$, schreibe

$$f(x) = \gamma_m(x^p)^m + \cdots + \gamma_1 x^p + \gamma_0 \qquad (*) .$$

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

Proposition 13.14. Sei 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 $\varphi : F \to F$

$a \mapsto a^p$

ist ein injektiver Körper-Homomorphismus (Frobenius).

Beweis: (ÜB).

Korollar 13.15.
$\mathbb{F}$ ist endlich $\Rightarrow \varphi : \mathbb{F} \to \mathbb{F}$
$a \mapsto a^p$
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 (vgl. LA I Skript 13). □

Korollar 13.11. gilt also auch für endliche Körper.

Proposition 13.16. Sei $\mathbb{F}$ ein endlicher Körper.

1. Jedes irreduzible Polynom $f \in \mathbb{F}[x]\,(\deg f \geq 1)$ ist separabel.
2. Ein Polynom $f(x) \in \mathbb{F}[x]\,(\deg f \geq 1)$ ist separabel $\Leftrightarrow$ die Primfaktorisierung von f in $F[x]$ diese Gestalt hat:

   $f = c\prod_{i=1}^{k} p_i(x)$; $0 \neq c \in F$, $p_i \in F[x]$ sind irreduzibel und normiert, **und** $p_i \neq p_j$ für $i \neq j$.

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

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

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

Widerspruch.
(2) Analog zum Beweis vom Korollar 13.11. (ÜA). □

Bemerkung 13.17.
Im Beweis von Proposition 13.16 haben wir die wichtige Eingenschaft $\mathbb{F}^p = \mathbb{F}$ benutzt (s.Korollar 13.15).

Definition 13.18.
Ein Körper F heißt *perfekt*, falls Char $F = 0$ oder Char $F = p > 0$ und $F = F^p$.

Bemerkung 13.19.
Proposition 13.16. gilt allgemeiner für F perfekt (anstatt $\mathbb{F}$ endlich).

Beweis: (ÜB).