Ad §5.10: Irreduzible Polynome

Prop.: Für jedes L/K und $f \in K[X] \setminus \{0\}$ gilt:

f separabel über K $\iff$ f separabel über L.

Beweis: Sei $\bar{K}$ ein alg. Abschluss von K,
und sei $\bar{L}$ " " " " L.

$$\begin{tikzcd} & \bar{L} \arrow[d, dash] \\ \bar{K} \arrow[ur, hook] \arrow[d, dash] & L \\ K \arrow[ur, dash] & \end{tikzcd}$$

Nach §5.7 existiert eine Einbettung $\bar{K} \hookrightarrow \bar{L}$ über K. Via dieser fassen wir $\bar{K}$ als Unterkörper von $\bar{L}$ auf.

Da f schon über $\bar{K}$ in Linearfaktoren zerfällt, sehen wir dann, dass die Multiplizitäten der Faktoren dieselben sind, egal ob wir in $\bar{K}$ oder in $\bar{L}$ rechnen. qed.

allgemein: beliebiges L/K

Lemma: Für beliebige $f, g \in K[X]$ gilt:

f, g teilerfremd in $K[X]$ $\iff$ teilerfremd in $\bar{K}[X]$.

Beweis: f, g teilerfremd in $K[X]$ $\Longrightarrow$ $\exists\, u, v \in K[X]: 1 = uf + vg$

$\Downarrow$ teilerfremd in $\bar{K}[X]$.

Umgekehrt ist jeder Teiler $h \mid f, g$ in $K[X]$ auch ein gemeinsamer Teiler in $\bar{K}[X]$. qed.

Prop.: Ein Polynom $f \in K[X] \setminus \{0\}$ ist separabel genau dann, wenn f und f' teilerfremd in $K[X]$ sind.

Beweis: Nach dem Lemma genügt es zu zeigen ... $\iff$ teilerfremd in $\bar{K}[X]$
$\iff$ keine gemeinsame Nullstelle in $\bar{K}$.

Sei nun $a \in \bar{K}$ eine Nullstelle der Vielfachheit $\nu \geq 1$ von f.
Schreibe $f(X) = (X-a)^\nu \cdot g(X)$ für $g(X) \in \bar{K}[X]$ mit $g(a) \neq 0$.
Dann ist $f'(X) = \nu \cdot (X-a)^{\nu-1} \cdot g(X) + (X-a)^\nu \cdot g'(X)$

und somit $f'(a) = \begin{cases} 0 & \text{falls } \nu \geq 2. \\ g(a) \neq 0 & \text{falls } \nu = 1. \end{cases}$

Daraus folgt direkt die gesuchte Äquivalenz. qed.

Prop.: Ein irreduzibles $f \in K[X]$ ist separabel gdw $f' \neq 0$ ist.

Beweis: $f' = 0 \Rightarrow ggT(f, f') \sim f \not\sim 1 \Rightarrow f$ nicht separabel.

$f' \neq 0 \Rightarrow \deg(f') < \deg(f) \Rightarrow \deg(ggT(f,f')) < \deg(f)$

Also f irred $\Rightarrow ggT(f, f') \sim 1$. qed.

Lemma: Sei $f \in K[X]$ irreduzibel mit $f' = 0$. Dann gilt $p := \mathrm{char}(K) > 0$ und $f(X) = g(X^p)$ für ein irreduzibles $g \in K[X]$

Beweis: Schreibe $f(X) = \sum_{i=0}^{n} a_i X^i$ mit $n > 0$ und $a_n \neq 0$.

Dann ist $f'(X) = \sum_{i=0}^{n} a_i i X^{i-1} = 0$.

Also gilt: $\forall i \geq 0 : a_i \cdot i = 0$.

Insbesondere $\underset{\neq 0}{a_n} \cdot n = 0 \Rightarrow n = 0$ in $K \Rightarrow p > 0$ und $p \mid n$.

Es folgt: $\forall i \geq 0 : p \nmid i \Rightarrow a_i = 0$.

Setze $g(X) := \sum_{\substack{0 \leq i \leq n \\ p \mid i}} a_i X^{i/p}$. Dann folgt $g(X^p) = f(X)$.

Jedes $h \mid g$ würde dann einen Faktor $h(X^p)$ in $f(X)$ liefern,

also ist g selbst irreduzibel. qed.

Satz: (a) $\mathrm{char}(K) = 0 \Rightarrow$ Jedes irred. $f \in K[X]$ ist separabel.

(b) $\mathrm{char}(K) = p > 0 \Rightarrow$ Jedes irred. $f \in K[X]$ hat die Form

$f(X) = g(X^{p^r})$ für ein eindeutiges $r \geq 0$ und ein separables irred. $g(X) \in K[X]$.

Beweis: Benutze Lemma und Induktion über $\deg(f)$. qed.