18. Normale und separable Körpererweiterungen

Def. Eine Körpererweiterung $L:K$ heisst <u>normal</u>, falls jedes irred. Polynom $f \in K[X]$, welches in L eine Nullstelle besitzt, über L vollständig in Linearfaktoren zerfällt.

Bsp. $\mathbb{C}:\mathbb{R}$ ist normal; $\mathbb{Q}(\sqrt[3]{2}):\mathbb{Q}$ ist nicht normal; $\sqrt[3]{2}\cdot e^{i\frac{2\pi}{3}} \notin \mathbb{Q}(\sqrt[3]{2})$.

Satz 18.1 Eine Körpererweiterung $L:K$ ist genau dann endlich und normal, wenn ein Polynom $f \in K[X]$ existiert, so dass L Zerfällungskörper von f über K ist.

Beweis: ($\Rightarrow$) $L:K$ ist endlich, also algebraisch und $L = K(\alpha_1, \dots, \alpha_s)$ mit α_i alg. über K. Für $1 \leq i \leq s$ sei $h_i \in K[X]$ das Minimalpolynom von α_i. Da jedes Polynom h_i in L eine Nullstelle besitzt, zerfällt (nach Vorraussetzung) jedes h_i (h_i irred.) über L in Linearfaktoren. Damit zerfällt auch $f := \prod_{i=1}^{s} h_i \in K[X]$ über L in Linearfaktoren. Andererseits ist L erzeugt durch $\alpha_1, \dots, \alpha_s$, sodass L der Zerfällungskörper von $f \in K[X]$ ist.

($\Leftarrow$) Sei L der Zerfällungskörper von $f \in K[X]$. Dann ist $[L:K]$ endlich. Es bleibt zu zeigen, dass $L:K$ normal ist:

- Sei $g \in K[X]$ ein über K irred. Polynom, welches in L die Nullstelle $\alpha \in L$ besitzt. Wir zeigen, dass g in L in Linearfaktoren zerfällt.
- Wir betrachten den Zerfällungskörper M von $f \cdot g \in K[X]$. Es gilt $K \subseteq L \subseteq M$ und es seien $\beta_1, \beta_2 \in M$ Nullstellen von $g \in K[X]$.

Beh. $[L(\beta_1):L] = [L(\beta_2):L]$

Bew. Wir betrachten folgende Körpererweiterungen:

$$\begin{array}{ccccc} M & = & M & = & M \\ \cup\!\mid & & \cup\!\mid & & \cup\!\mid \\ L(\beta_1) & \supseteq & L & \subseteq & L(\beta_2) \\ \cup\!\mid & & \cup\!\mid & & \cup\!\mid \\ K(\beta_1) & \supseteq & K & \subseteq & K(\beta_2) \end{array}$$

Für $j=1,2$ gilt mit Gradsatz 14.1:

$$[L(\beta_j):L]\cdot[L:K] = [L(\beta_j):K] = [L(\beta_j):K(\beta_j)]\cdot[K(\beta_j):K].$$

- Da g über K irred. ist, gilt $[K(\beta_1):K] = \operatorname{grad}(g) = [K(\beta_2):K]$.
  Mit Folgerung 14.5 (β_1,β_2 besitzen dasselbe Min.-Poly.) ex. Isom. $\varphi: K(\beta_1) \xrightarrow{\sim} K(\beta_2)$ mit $\varphi|_K = \mathrm{id.}$ und $\varphi(\beta_1) = \beta_2$.
- Nun ist $L(\beta_j)$ ein Zerfällungskörper von $f \in K[X]$ über $K(\beta_j)$, da in M der Körper $L(\beta_j)$ erzeugt wird von β_j und den Nullstellen $\alpha_1, \dots, \alpha_s$ von f (weil L ein Zerfällungskörper von f ist).
- Mit Satz 15.2 (Isom. zw. Zerf.-Körpern) lässt sich φ zu einem Isom. $\tilde{\varphi}: L(\beta_1) \xrightarrow{\sim} L(\beta_2)$ mit $\tilde{\varphi}|_{K(\beta_1)} = \varphi$ erweitern.
- Somit gilt $[L(\beta_1):K(\beta_1)] = [L(\beta_2):K(\beta_2)]$ und mit $[K(\beta_1):K] = [K(\beta_2):K]$ erhalten wir $[L(\beta_1):L] = [L(\beta_2):L]$.

$\dashv$ Beh.

Mit unserer Annahme ist $\alpha \in L$ eine Nullstelle von $g \in K[X]$, also auch von $f\cdot g$. Setzen wir $\beta_1 := \alpha$ und sei β_2 eine weitere Nullstelle von g, so ist $\underbrace{[L(\alpha):L]}_{=1} = [L(\beta_2):L] = 1$, also ist $\beta_2 \in L$ und somit liegen mit $\alpha \in L$ alle Nullstellen von $g \in K[X]$ (im Zerf.-Körper von g) ebenfalls in L. D.h. g zerfällt in L vollständig in Linearfaktoren und $L:K$ ist normal. $\dashv$

Def. Die <u>formale Ableitung</u> eines Polynoms $f = a_0 + \ldots + a_n X^n$ in $K[X]$ ist definiert durch
$$Df := a_1 + 2a_2 X + \ldots + n \cdot a_n \cdot X^{n-1}.$$

Bem. Diese Ableitung genügt den Ableitungsregeln wie z.B.
$$D(f \cdot g) = (Df) \cdot g + f \cdot (Dg).$$

<u>Proposition 18.2</u> Ein Polynom $f \in K[X]$ besitzt genau dann eine mehrfache Nullstelle in einer Körpererw. $L \supseteq K$, wenn f und Df einen gemeinsamen Faktor $h \in K[X]$ mit $\mathrm{grad}(h) \geq 1$ besitzen.

<u>Beweis:</u> ($\Rightarrow$) Es sei a eine mehrfache Nullstelle von f in L. Dann gilt in $K(a) \subseteq L$ die Gleichung $(X-a)^2 \cdot g = f$ für ein $g \in K(a)[X]$. Es folgt
$$Df = 2(X-a) \cdot g + (X-a)^2 \cdot Dg$$
und somit ist a auch Nullstelle von Df. D.h. das Min.-Poly. $h \in K[X]$ von a teilt sowohl f wie auch Df.

($\Leftarrow$) Sei das Polynom $h \in K[X]$ ein gemeinsamer Faktor von f und Df, und sei a eine Nullstelle von h (in L). Dann ist a auch eine Nullstelle von f und Df.
- Wir zeigen, dass a eine mehrfache Nullstelle von f ist:
- In $K(a)$ gilt $f = (X-a) \cdot g$ und $Df = g + (X-a) \cdot Dg$.
- Weil a eine Nullstelle von Df ist, ist a auch eine Nullstelle von g, also $g = (X-a) \cdot \tilde{g}$, und somit ist $f = (X-a) \cdot g = (X-a)^2 \cdot \tilde{g}$, d.h. a ist eine mehrfache Nullstelle von f.

$\dashv$

Def. Ein Polynom $h \in K[X]$ heisst <u>separabel</u> über K, wenn jeder irred. Faktor von h in $K[X]$, in einem Zerf.-Körper von h über K nur einfache Nullstellen besitzt; andernfalls heisst h <u>inseparabel</u> über K.

[Bsp. für ein irred. und insep. Polynom, siehe Afg. 105]

Def. Ein Körper K heisst <u>perfekt</u>, wenn jedes irred. Polynom $f \in K[X]$ über K separabel ist.

<u>Proposition 18.3</u> $\mathbb{F}_p$ ist perfekt für alle Primzahlen p.

<u>Beweis:</u> Mit Satz 16.5.(a) ist jedes irred. Polynom $f \in \mathbb{F}_p[X]$ separabel. $\dashv$

<u>Proposition 18.4</u> Jeder Körper mit Charakteristik 0 ist perfekt.

<u>Beweis:</u> Sei $f = a_0 + a_1 X + \ldots + a_n X^n \in K[X]$ irred. mit $a_n \neq 0$.

- Dann ist $Df = a_1 + 2a_2 X + \ldots + n \cdot a_n X^{n-1}$, und weil $\operatorname{char}(K) = 0$ gilt für $n \neq 0$, $n \cdot a_n \neq 0$. Damit ist $Df \neq 0$ und $\operatorname{grad}(Df) < \operatorname{grad}(f)$.
- Da f irred. ist, ex. kein nicht-trivialer Faktor von f und Df, und damit hat mit Prp. 18.2 das Polynom f im Zerf.-Körper von f über K keine mehrfachen Nullstellen. $\dashv$

Def.
- Sei $L:K$ eine Körpererweiterung. Ist $\alpha \in L$ alg. über K, so heisst <u>α separabel über K</u>, wenn dass Min.-Poly. von α über K separabel ist.
- Ist $L:K$ alg. und ist jedes $\alpha \in L$ separabel über K, so heisst die <u>Körpererweiterung</u> $L:K$ <u>separabel</u>.