$\sigma|_K = \text{Inkl. } K \hookrightarrow \overline{L}$, und $\sigma(\alpha) = \beta$ (wegen 3.3.10(ii)). Nach 3.3.11 es gibt eine Fortsetzung $\sigma' : L \to \overline{L}$ von $\sigma \overset{(ii)}{\leadsto} \sigma'(L) = L$ $\leadsto \beta \in L$. Also zerfällt g über L in Linearfaktoren.

(iii) $\Rightarrow$ (i): Seien $\alpha_1, \dots, \alpha_n \in L$ mit $L = K(\alpha_1, \dots, \alpha_n)$. Seien $f_1, \dots, f_n$ Minimalpolynome zu $\alpha_1, \dots, \alpha_n$. Aus (iii) folgt, dass $f_1, \dots, f_n$ zerfallen im $L[X]$ in Linearfaktoren $\leadsto$ L ist Zerfällungskörper zu $f = f_1 \cdot \dots \cdot f_n$. $\blacksquare$

3.4.7 Bem. (i) Jede Körpererw. von Grad 2 ist Zerfällungskörper.

Beweis: Sei $[L:K] = 2$, $\alpha \in K \setminus L$, $f \in K[X]$ Minimalpol. zu α.
Dann gilt $1 \leq [K(\alpha):K] \leq 2$. Da $K(\alpha) \neq K$, bleibt $[K(\alpha):K] = 2$.
Aber $[K(\alpha):K] = \text{grad} f$ (Satz 3.2.8) $\leadsto$ $\text{grad} f = 2$.
In $L[X]$ gilt $f = (X - \alpha) g$, mit $g \in L[X]$, $\text{grad}\, g = 1 \leadsto g$ zerfällt vollständig in $L[X]$.

(ii) $K \subset L$, $L \subset M$ endliche Körpererw, $K \subset M$ normal $\overset{3.4.6(i)}{\leadsto}$ $L \subset M$ normal.

3.4.8 Bsp. $\mathbb{Q} \subset \mathbb{Q}(\sqrt{2})$ hat Grad 2 ($X^2 - 2$ Minpol zu $\sqrt{2}$), normal
$\mathbb{Q}(\sqrt{2}) \subset \mathbb{Q}(\sqrt[4]{2})$ hat Grad 2 ($X^2 - \sqrt{2}$ Minimalpol. zu $\sqrt[4]{2}$; in der Tat $X^2 - \sqrt{2}$ ist irred. in $\mathbb{Q}(\sqrt{2})[X]$, da es keine Nullstelle in $\mathbb{Q}(\sqrt{2})$ hat: für $a, b \in \mathbb{Q}$ gilt $(a + b\sqrt{2})^2 = a^2 + 2b^2 + 2\sqrt{2}ab \neq \sqrt{2}$; sonst $a^2 + 2b^2 = 0$, $2ab = 1$ $\lightning$) $\leadsto$ $\mathbb{Q}(\sqrt{2}) \subset \mathbb{Q}(\sqrt[4]{2})$ normal
Aber $\mathbb{Q} \subset \mathbb{Q}(\sqrt[4]{2})$ nicht normal: $X^4 - 2$ hat die Nullstelle $\sqrt[4]{2}$ in $\mathbb{Q}(\sqrt[4]{2})$ aber zerfällt nicht vollständig in Linearfaktoren:

$$X^4 - 2 = (X^2 - \sqrt{2})(X^2 + \sqrt{2}) = (X - \sqrt[4]{2})(X + \sqrt[4]{2})\underbrace{(X^2 + \sqrt{2})}_{\text{zerfällt nich in } \mathbb{R}[X]}$$

Fazit: die Normalität ist nicht tranzitiv.

3.4.9 Bem. $K \subset L$ endliche Körpererw. $\leadsto$ $\exists L \subset L'$ endlich, so dass $K \subset L'$ normal. (Sei $L = K(\alpha_1, \dots, \alpha_n)$, f_i Minpol. zu α_i, $f = f_1 \cdots f_n$, $\alpha_1, \dots, \alpha_n, \dots \alpha_N$ Nst von f in $\overline{L}$ $\leadsto$ $L' = K(\alpha_1, \dots, \alpha_N) \supset L$ normal)

3.4.10 Bsp. $\mathbb{Q} \subset \mathbb{Q}(\sqrt[4]{2})$ nicht normal, aber $\mathbb{Q} \subset \mathbb{Q}(\sqrt[4]{2}, i\sqrt[4]{2})$ normal, als Zerfällungskörper von $X^4 - 2$

§3.5 Separable Körpererweiterungen

<u>3.5.1 Def</u> Sei $f = \sum_{i=0}^{n} a_i X^i \in K[X]$. Die formale Ableitung von f ist $f' := \sum_{i=1}^{n} i a_i X^{i-1} \in K[X]$ (falls $n=0$, $f'=0$).

Wenn $K=\mathbb{R}$ dies ist die übliche Ableitung. Ist char $K=p$, so $(X^p)'=0$!

<u>3.5.2 Lemma</u> (i) Sei $K\subset L$ Körpererw., $f,g\in K[X]$, $h=ggT(f,g)$ in $K[X]$. Dann $h=ggT(f,g)$ in $L[X]$.

(ii) $\alpha\in\overline{K}$ ist mehrfache Nullstelle von f (d.h. Vielfachkeit von α ist ≥ 2, d.h. $(X-\alpha)^2 \mid f$) $\Longleftrightarrow f(\alpha)=f'(\alpha)=0 \Longleftrightarrow \alpha$ Nullstelle von $ggT(f,f')$.

(iii) Sei $f\in K[X]$ irreduzibel. f eine mehrfache Nullstelle in $\overline{K} \Longleftrightarrow f'=0$

<u>Beweis</u> (i) Sei $h_K = ggT(f,g)$ in $K[X]$, $h_L = ggT(f,g)$ in $L[X]$.
h_K Teiler von f,g und $h_K\in K[X]\subset L[X] \rightsquigarrow h_K \mid h_L$ in $L[X]$
$K[X]$ Hauptidealring $\overset{2.4.18}{\rightsquigarrow} \exists \alpha,\beta\in K[X]: \alpha f+\beta g = h_K$
$\rightsquigarrow h_L \mid h_K$ in $L[X] \rightsquigarrow h_K = h_L$ (bis zur Assoziiertheit).

(ii) Sei α Nullstelle von f in $\overline{K}$ von Vielfachkeit r, d.h. $(X-\alpha)^r \mid f$ und $(X-\alpha)^{r+1}\nmid f$ in $\overline{K}[X]$. Also $f=(X-\alpha)^r g$ mit $g(\alpha)\neq 0$.
Also $f' = r(X-\alpha)^{r-1} g + (X-\alpha)^r g'$. Daher

$$r\geq 2 \Longleftrightarrow f'(\alpha)=0 \Longleftrightarrow \alpha \text{ Nullstelle von } f \text{ und } f'$$

$$\Longleftrightarrow X-\alpha \mid f, f' \Longleftrightarrow X-\alpha \mid ggT(f,f') \Longleftrightarrow \alpha \text{ Nullstelle von } ggT(f,f').$$

(iii) OBdA f normiert. Sei $\alpha\in\overline{K}$, $f(\alpha)=0 \rightsquigarrow$
f Minimalpol. von $\alpha \rightsquigarrow Ker(\varphi_\alpha)=(f)$ mit $\varphi_\alpha: K[X]\to K$, $g\mapsto g(\alpha)$
α mehrfach $\rightsquigarrow f'(\alpha)=0 \rightsquigarrow f'\in(f) \Longleftrightarrow f'=0$
(da grad f' < grad f) ▤

3.5.3 Def. (i) $f \in K[X]$ heißt <u>separabel</u>, wenn f keine mehrfache Nullstellen in $\overline{K}$ hat

(ii) $K \subset L$ Körpererw, $\alpha \in L$ alg $/K$ heißt <u>separabel</u> über K, falls sein Minimalpolynom separabel ist

(iii) Eine alg. Körpererw. heißt <u>separabel</u>, falls alle $\alpha \in L$ sep.$/K$

(iv) K heißt <u>vollkommen</u>, wenn jedes irred. $f \in K[X]$ separabel ($\Leftrightarrow$ jede alg. Körpererw. $K \subset L$ separabel)

3.5.4 Satz (i) $\operatorname{char} K = 0 \Rightarrow K$ vollkommen

(ii) K endlich $\Rightarrow K$ vollkommen.

<u>Beweis</u> (i) Sei $f \in K[X]$ irred, also $\operatorname{grad} f = n \geq 1$. Sei $f = a_n X^n + \dots$

also $f' = \underbrace{n a_n}_{\neq 0} X^{n-1} + \dots$ also $f' \neq 0 \underset{3.5.2(iii)}{\rightsquigarrow} f$ separabel.

(ii) Sei $\operatorname{char} K = p$, $f \in K[X]$ irred. Angenommen f nicht sep.

$\underset{3.5.2(iii)}{\rightsquigarrow} f' = 0 \rightsquigarrow f = \sum_{k=0}^{n} a_{kp} X^{kp}$

Betrachte $K \ni a \longmapsto a^p \in K$ den Frobenius-Homom.

($(x+y)^p = x^p + y^p$, da $p \mid \binom{p}{k}$ für $1 \leq k \leq p-1$, weil p prim)

Der Frobenius-Homom ist inj. also surjektiv, da K endlich.

Wähle $b_0, \dots, b_n \in K$ mit $a_{kp} = b_k^p \rightsquigarrow f = \sum_{k=0}^{n} (b_k X^k)^p = \left(\sum_{k=0}^{n} b_k X^k\right)^p$

$\rightsquigarrow f$ reduzibel $\lightning$ ▨

Ein Beispiel für ein irred. nicht separables Polynom findet man also nur in unendliche Körper von Charakteristik $p > 0$.

Bezeichne $\mathbb{F}_p := \mathbb{Z}/p\mathbb{Z}$; sei $K = \mathbb{F}_p(X)$, $f = Y^p - X \in K[Y]$

Eigentlich $f \in \mathbb{F}_p[X][Y]$; $X \in \mathbb{F}_p[X]$ ist prim. Eisenstein $\rightsquigarrow f$ irred. in $\mathbb{F}_p[X][Y] \rightsquigarrow$ irred in $Q(\mathbb{F}_p[X])[Y]$ $= \mathbb{F}_p(X)[Y] = K[Y]$. Sei L ein Zerfällungskörper von f, $\alpha \in L$ mit $0 = f(\alpha) = \alpha^p - X$. Also $f = Y^p - \alpha^p = (Y-\alpha)^p$

$\rightsquigarrow \alpha$ ist p-fache Nullstelle von f in $L[X]$. Eigentlich $f' = 0$.