3.5.12 Satz vom primitiven Element

Sei $K \subset L$ endlich und separabel. Dann ist $K \subset L$ einfach also es gibt ein primitives Element $\alpha \in L$, d.h. $L = K(\alpha)$.

Beweis 1. Fall: K endlich $\rightsquigarrow$ L endlich $\rightsquigarrow$ L^* endlich $\xrightarrow[\text{Blatt 11}]{}$ L^* zyklisch. Sei $L^* = \langle a \rangle \rightsquigarrow L = K(a)$

2. Fall: K unendlich. Sei $L = K(a_1, \dots, a_n)$. Wegen Induktion über n reicht den Fall $n = 2$ zu behandeln. Sei also $L = K(a,b)$, $m = [L:K]_s$ und $\mathrm{Hom}_K(L, \overline{K}) = \{\sigma_1, \dots, \sigma_m\}$. Definiere $P \in \overline{K}[X]$,

$$P = \prod_{i \neq j} \left[(\sigma_i(a) - \sigma_j(a)) + (\sigma_i(b) - \sigma_j(b))X \right] \neq 0$$

(jeweils mindestens eine Differenz $\neq 0$ (sonst $\sigma_i = \sigma_j$ ↯))

Wähle $c \in K$ mit $P(c) \neq 0$ (c existiert, da K unendlich)

$\rightsquigarrow \sigma_i(a) + c\,\sigma_i(b) \neq \sigma_j(a) + c\,\sigma_j(b)$ für $i \neq j$

Sei $f \in K[X]$ das Minpol. von $a + cb \in L$. (σ_i K-Homom.)

σ_i K-Homom $\rightsquigarrow f(\sigma_i(a) + c\,\sigma_i(b)) = f(\sigma_i(a+cb)) = \sigma_i(f(a+cb)) = 0$

$\rightsquigarrow \mathrm{grad}\, f \geq m = [L:K]_s$ Aber $\mathrm{grad}\, f = [K(a+cb):K] \leq [L:K]$

Voraussetzung: $K \subset L$ sep $\rightsquigarrow [L:K]_s = [L:K] \rightsquigarrow [K(a+cb):K] = [L:K]$

$\rightsquigarrow L = K(a+cb)$. ▨ Z.B. $\mathbb{Q}(\sqrt{2}, \sqrt{3}) = \mathbb{Q}(\sqrt{2} + \lambda\sqrt{3})$, $\lambda \in \mathbb{Q}^*$

4. Galois-Theorie

§4.1. Galois-Erweiterungen und Hauptsatz der Galois-Theorie

4.1.1 Def Eine endliche Körpererw. $K \subset L$ heißt Galois-Erweiterung (oder galois), wenn $K \subset L$ normal und separabel ist. Ist $K \subset L$ galois, so heißt $\mathrm{Gal}(L/K) := \mathrm{Aut}_K(L)$ die zugehörige Galois-Gruppe.

4.1.2. Bem Sei $K \subset L$ endlich. Äquivalent:

(i) $K \subset L$ galois (ii) L ist Zerfällungskörper eines sep. Pol. $f \in K[X]$

(iii) $\exists \alpha \in L$: $L = K(\alpha)$ und das Minpol von α über K zerfällt in Linearfakt. über L und hat paarweise versch. Nullstellen.

(iv) $\forall \beta \in L$: Minpol von β über K zerfällt in Linearfkt über L und hat paarweise versch. Nullstellen.

Beweis (i) $\Rightarrow$ (iv) folgt nach 3.4.6 (iii) und $K \subset L$ separabel

(iv) $\Rightarrow$ (iii): $K \subset L$ sep. nach Voraus. $\overset{3.5.12}{\rightsquigarrow} \exists \alpha \in L$: $L = K(\alpha)$

(iii) $\Rightarrow$ (ii) f = Minpol von α (ii) $\Rightarrow$ (i) z.z. $K \subset L$ sep. OK nach 3.5.10(ii) (nehme $\alpha_1, \dots, \alpha_n$ die Nst. von f). ▤

4.1.3 Bem. Seien $K \subset E \subset L$ Körpererw., $K \subset L$ galois. Dann:

(i) $E \subset L$ galois und $\mathrm{Aut}_E(L) < \mathrm{Aut}_K(L)$

(ii) Ist auch $K \subset E$ galois, so $\sigma(E) = E$ für alle $\sigma \in \mathrm{Aut}_K(L)$ und $\mathrm{Aut}_K(L) \ni \sigma \longmapsto \sigma|_E \in \mathrm{Aut}_K(E)$ ist surjektiv.

4.1.4 Bem. Sei $K \subset L$ endlich, normal. Dann $\mathrm{ord}\,\mathrm{Aut}_K(L) = [L:K]_s \leq [L:K]$. Es gilt $\mathrm{ord}\,\mathrm{Aut}_K(L) = [L:K] \Leftrightarrow K \subset L$ galois

Beweis $[L:K]_s := \mathrm{ord}\,\mathrm{Hom}_K(L, \overline{K}) = \mathrm{ord}\,\mathrm{Aut}_K(L)$ nach 3.4.6(i). Zweite Beh. folgt aus 3.5.10.

4.1.5 Bsp. (i) $\mathbb{Q} \subset \mathbb{Q}(\sqrt[3]{2})$ nicht galois, da nicht normal ($f = X^3 - 2$ ist irred/$\mathbb{Q}$, hat Nst. $\sqrt[3]{2}$ in $\mathbb{Q}(\sqrt[3]{2})$ aber zerfällt nicht in Linearfakt. über $\mathbb{Q}(\sqrt[3]{2})$).

(ii) $\mathbb{Q} \subset \mathbb{Q}(\sqrt[3]{2}, e^{\frac{2\pi i}{3}}) = L$ ist galois, da L ist Zerfällungskörper von $f = X^3 - 2 \in \mathbb{Q}[X]$. Außerdem $[L:\mathbb{Q}] = \underbrace{[L:\mathbb{Q}(\sqrt[3]{2})]}_{=2} \underbrace{[\mathbb{Q}(\sqrt[3]{2}):\mathbb{Q}]}_{=3}$ (Minpol. zu $e^{\frac{2\pi i}{3}}$ ist $X^2 + X + 1$)

$\overset{4.1.4}{\rightsquigarrow} \mathrm{ord}\,\mathrm{Gal}(L/\mathbb{Q}) = \mathrm{ord}\,\mathrm{Aut}_{\mathbb{Q}}(L) = 6$.

$\mathbb{Q} \subset L$ ist sep. da $\mathrm{char}\,\mathbb{Q} = 0$ (siehe 3.5.8(i), 3.5.10(iii)) oder direkt mit 4.1.2(ii).

4.1.6 Satz L Körper, $G < \mathrm{Aut}(L)$ endlich, $L^G := \{a \in L : \forall \sigma \in G,\ \sigma(a) = a\}$ (Fixkörper unter G). Dann $L^G \subset L$ galois, $[L:L^G] = \mathrm{ord}\,G$, $\mathrm{Gal}(L/L^G) = G$.

Beweis 1. Schritt: $L^G \subset L$ endlich. Sei $G = \{\sigma_1 = e, \dots, \sigma_m\}$ und $\alpha_1, \dots, \alpha_n \in L$ mit $n > m$. Wir zeigen, dass $\alpha_1, \dots, \alpha_n$ lin. abh. über L^G. Betrachte das Linearsystem

$$(*) \quad \begin{cases} \sigma_1(\alpha_1) X_1 + \dots + \sigma_1(\alpha_n) X_n = 0 \\ \vdots \\ \sigma_m(\alpha_1) X_1 + \dots + \sigma_m(\alpha_n) X_n = 0 \end{cases}$$

mit m Gl. und $n > m$ Unbekannten $\rightsquigarrow \exists$ nicht-triviale Lösung in L. Wähle eine Lösung $(c_1, \dots, c_n)$ mit maximalen Anzahl von Nullen. Nach Umnumerierung und Mult. mit einem Skalar kann man annehmen, dass $c_1 \in L^G \setminus \{0\}$. Betrachte die erste Gleichung ($\sigma_1 = e$): $\alpha_1 c_1 + \dots + \alpha_n c_n = 0$, eine lin. Kombination. Wir wollen alle $c_1, \dots, c_n$ aus L^G wählen. Gibt es $c_i \notin L^G$, so $\exists k$: $\sigma_k(c_i) \neq c_i$. Wende σ_k auf $(*)$ und benutze die Tatsache, dass $\{\sigma_k\sigma_1, \dots, \sigma_k\sigma_m\}$ eine Permutation von $\{\sigma_1, \dots, \sigma_m\}$ ist. $\rightsquigarrow (c_1, \sigma_k(c_2), \dots, \sigma_k(c_n))$ Lösung von $(*)$. Subtraktion $\rightsquigarrow$ $(0, \dots, c_i - \sigma_k(c_i), \dots)$ Lösung mit mehr Nullen als $(c_1, \dots, c_n)$ ↯ (nicht-triviale)

2. Schritt: $L^G \subset L$ separabel. Sei $a \in L$ und $\{\sigma_1, \dots, \sigma_r\} \subset G$ maximal mit $\sigma_i(a) \neq \sigma_j(a)$ für alle $i \neq j$. Jedes $\sigma \in G$ lässt $\{\sigma_1(a), \dots, \sigma_r(a)\}$ invariant (Maximalität von $\{\sigma_1, \dots, \sigma_r\}$). Setze $f := \prod_{i=1}^{r} (X - \sigma_i(a)) \in L^G[X]$. f ist separabel nach Konstr. und a ist Nst. von f ($a \in \{\sigma_1(a), \dots, \sigma_r(a)\}$ nach Wahl von $\{\sigma_1, \dots, \sigma_r\}$) $\rightsquigarrow a$ sep. $/L^G$.

3. Schritt: $L^G \subset L$ normal Wende 3.4.6(iii). Sei $g \in L^G[X]$ irred mit Nst $a \in L$. OBdA g normiert $\rightsquigarrow g$ Minpol. von a $\rightsquigarrow g \mid f \rightsquigarrow g$ zerfällt

4. Schritt: $[L : L^G] = \operatorname{ord} G$, $\operatorname{Gal}(L/L^G) = G$. Schritt 1 $\rightsquigarrow [L : L^G] \leq \operatorname{ord} G$
Aber $G < \operatorname{Aut}(L) = \operatorname{Aut}_{L^G}(L) \rightsquigarrow \operatorname{ord} G \leq \operatorname{ord} \operatorname{Aut}_{L^G}(L) \overset{4.1.4}{=} [L : L^G]$