

## Hauptsatz der Galois-theorie

$L|K$  endliche Galoiserweiterung

$G = \text{Gal}(L|K)$ ,  $\mathcal{U}$  = Menge der Untergr. von  $G$

$\mathcal{Z}$  = Menge der Zwischenkörper

Dann sind die beiden Abbildungen

$$\phi: \mathcal{U} \rightarrow \mathcal{Z}, \quad U \mapsto L^U = \{x \in L \mid \sigma(x) = x \forall \sigma \in U\}$$

(Fixkörper von  $U$ )

$$\psi: \mathcal{Z} \rightarrow \mathcal{U}, \quad M \mapsto \text{Gal}(L|M)$$

bijektiv und zueinander invers.

( $\Rightarrow |\mathcal{U}| = |\mathcal{Z}|$ , beide Mengen sind endlich)

## Ergänzungssätze

(1)  $\phi$  und  $\psi$  sind antiton, d.h. es gilt

$$U_1 \subseteq U_2 \iff L^{U_1} \supseteq L^{U_2} \quad \forall U_1, U_2 \in \mathcal{U}$$

$$M_1 \subseteq M_2 \iff \text{Gal}(L/M_1) \supseteq \text{Gal}(L/M_2)$$

für alle  $M_1, M_2 \in \mathcal{Z}$

(2)  $L^G = K$ ,  $L^{\text{id}} = L$ ,  $\text{Gal}(L/K) = G$ ,  $\text{Gal}(L/L) = \{\text{id}\}$

(3) Für jedes  $U \in \mathcal{U}$  gilt  $|U| = [L : L^U]$  und  
 $(G, U) = [L^U : K]$ . Entsprechend gilt für jedes  
 $M \in \mathcal{Z}$  jeweils  $[L : M] = |\text{Gal}(L/M)|$  und  
 $[M : K] = (G, \text{Gal}(L/M))$

Untergr.  $U$  mit  $10 \nmid \#U \nmid 2/4\mathbb{Z}$  hat. Also hat auch  $G$   
nur eine Untergr.  $V$  mit  $10 \nmid \#V \nmid G$ . Nach dem Hauptsatz

(4) Sei  $U \in \mathcal{U}$  und  $M = L^U \in \mathcal{Z}$ . Dann gilt die  
Äquivalenz  $U \trianglelefteq G \iff M/K \text{ normal} \iff M/K$   
galois'sch. Sind die drei Aussagen erfüllt, dann  
gilt auch  $G/U \cong \text{Gal}(M/K)$ .

F26T1A2 geg:  $f = x^4 - 6x^2 - 3 \in \mathbb{Q}[x]$

bereits bekannt: Menge der komplexen Nullstellen ist

$N = \{\pm\alpha, \pm\beta\}$  mit  $\alpha = \sqrt{3+2\sqrt{3}}$ ,  $\beta = \sqrt{3-2\sqrt{3}}$  ( $\alpha \in \mathbb{R}$ ,  $\beta \in \mathbb{C} \setminus \mathbb{R}$ )

$\nmid$  irreduzibel über  $\mathbb{Q}$ ,  $\mathbb{Q}(\alpha) \neq \mathbb{Q}(\beta)$ ,  $\mathbb{Q}(\alpha) \cap \mathbb{Q}(\beta) =$

$\mathbb{Q}(\sqrt{3})$ ,  $\mathbb{Q}(\alpha, \beta) | \mathbb{Q}(\sqrt{3})$  ist galois'sch, und  $G =$

$\text{Gal}(\mathbb{Q}(\alpha, \beta) | \mathbb{Q}(\sqrt{3}))$  ist isomorph zu  $\mathbb{Z}/4\mathbb{Z}$  oder  $(\mathbb{Z}/2\mathbb{Z})^2$

Ang.  $G \cong \mathbb{Z}/4\mathbb{Z}$ . Die Gruppe  $\mathbb{Z}/4\mathbb{Z}$  hat als zyklische Gruppe der Ordnung 4 wg. 2|4 genau eine Untergruppe der Ordnung 2. Weil 2 der einzige Teiler von 4 in  $\mathbb{N}$  ungleich 1 und 4 ist, folgt daraus, dass  $\mathbb{Z}/4\mathbb{Z}$  nur eine Untergr.  $U$  mit  $\{0\} \subsetneq U \subsetneq \mathbb{Z}/4\mathbb{Z}$  hat. Also hat auch  $G$  nur eine Untergr.  $V$  mit  $\{1\} \subsetneq V \subsetneq G$ . Nach dem Hauptsatz der Galois-theorie hat  $\mathbb{Q}(\alpha, \beta) | \mathbb{Q}(\sqrt{3})$  somit nur einen echten Zwischenkörper.

aber:  $\mathbb{Q}(\alpha), \mathbb{Q}(\beta)$  sind offenbar beides Zwischenkörper von  $\mathbb{Q}(\alpha, \beta) | \mathbb{Q}(\sqrt{3})$  bereits bekannt:  $\mathbb{Q}(\alpha), \mathbb{Q}(\beta) \neq \mathbb{Q}(\sqrt{3})$

Weiter gilt  $\mathbb{Q}(\alpha) \neq \mathbb{Q}(\alpha, \beta)$  wegen  $\mathbb{Q}(\alpha) \subseteq \mathbb{R}$  und  $\beta \notin \mathbb{R}$ . Ang.  $\mathbb{Q}(\beta) = \mathbb{Q}(\alpha, \beta)$ .  
 $\Rightarrow \mathbb{Q}(\alpha) \subseteq \mathbb{Q}(\beta) \Rightarrow \mathbb{Q}(\alpha) = \mathbb{Q}(\alpha) \cap \mathbb{Q}(\beta)$   
 $= \mathbb{Q}(\sqrt{3}) \uparrow [\mathbb{Q}(\alpha) : \mathbb{Q}] = 4, [\mathbb{Q}(\sqrt{3}) : \mathbb{Q}]$   
 $= 2$ . Insgesamt sind  $\mathbb{Q}(\alpha), \mathbb{Q}(\beta)$  also  
zwei verschiedene echte Zwischenkörper  
der Erweiterung  $L | \mathbb{Q}(\sqrt{3})$ , im Widerspruch  
zur Feststellung von oben  $\Rightarrow G \cong (Z/2Z)^2$ .  $\square$

Frage: Lassen sich alle echten Zwischenkörper der Erweiterung  $L | \mathbb{Q}(\sqrt{3})$  angeben?

Wegen  $|(Z/2Z)^2| = 4$ , und weil 1, 2, 4 die einzigen Teiler von 4 sind, ist jede Untergr.  $U$  von  $(Z/2Z)^2$  mit  $\{(0,0)\} \subsetneq U \subsetneq (Z/2Z)^2$  von Ordnung 2. 2 Primzahl  $\Rightarrow$  jede <sup>solche</sup> Untergr. ist zyklisch und wird also von einem Element der Ordnung 2 erzeugt  $\Rightarrow U_1 = \langle (1,0) \rangle$ ,  $U_2 = \langle (0,1) \rangle$ ,  $U_3 = \langle (1,1) \rangle$  sind die drei Untergr. der Ordnung 2.

Wegen  $G \cong (Z/2Z)^2$  und dem Hauptsatz der Galois-theorie hat  $\mathbb{Q}(\alpha, \beta) | \mathbb{Q}(\sqrt{3})$  also genau drei echte Zwischenkörper. Zwei davon sind  $\mathbb{Q}(\alpha)$  und  $\mathbb{Q}(\beta)$ .  $(\alpha\beta)^2 = \alpha^2\beta^2 = (3+2\sqrt{3})(3-2\sqrt{3}) = 9-12 = -3 \Rightarrow \alpha\beta \in \{\pm\sqrt{-3}\} \Rightarrow \mathbb{Q}(\alpha\beta) = \mathbb{Q}(\sqrt{-3})$

$\Rightarrow \mathbb{Q}(\sqrt{3}, \sqrt{-3})$  ist ein Zwischenkörper von  $\mathbb{Q}(\alpha, \beta) \mid \mathbb{Q}(\sqrt{3})$ . Offenbar ist  $\mathbb{Q}(\sqrt{3}) \subsetneq \mathbb{Q}(\sqrt{3}, \sqrt{-3})$  wg.  $\mathbb{Q}(\sqrt{3}) \subseteq \mathbb{R}$ ,  $\sqrt{-3} \notin \mathbb{R}$ .

Weiter gilt  $[\mathbb{Q}(\sqrt{3}, \sqrt{-3}) : \mathbb{Q}] = 4$  (Übung.)  
andereits aber  $[\mathbb{Q}(\alpha, \beta) : \mathbb{Q}] =$   
$$\underbrace{[\mathbb{Q}(\alpha, \beta) : \mathbb{Q}(\alpha)]}_{> 1, \text{ da } \beta \notin \mathbb{Q}(\alpha)} \cdot \underbrace{[\mathbb{Q}(\alpha) : \mathbb{Q}]}_{= 4} > 4$$

$\Rightarrow \mathbb{Q}(\sqrt{3}, \sqrt{-3}) \subsetneq \mathbb{Q}(\alpha, \beta) \Rightarrow \mathbb{Q}(\sqrt{3}, \sqrt{-3})$  ist  
echter Zwischenkörper von  $\mathbb{Q}(\alpha, \beta) \mid \mathbb{Q}(\sqrt{3})$   
 $\mathbb{Q}(\alpha) \neq \mathbb{Q}(\sqrt{3}, \sqrt{-3})$ , da  $\mathbb{Q}(\alpha) \subseteq \mathbb{R}$ ,  $\sqrt{-3} \notin \mathbb{R}$ .  
Ang.  $\mathbb{Q}(\beta) = \mathbb{Q}(\sqrt{3}, \sqrt{-3}) \Rightarrow \alpha \beta \in \mathbb{Q}(\beta)$

$\mathbb{Q}(\alpha) \subseteq \mathbb{Q}(\beta) \Rightarrow \alpha = (\alpha\beta) \cdot \beta^{-1} \in \mathbb{Q}(\beta) \Rightarrow \mathbb{Q}(\alpha) \subseteq \mathbb{Q}(\beta) \quad \checkmark$   
 also:  $\mathbb{Q}(\alpha, \beta) / \mathbb{Q}(\sqrt{3})$  hat drei echte Zwischenkörper, dies sind  $\mathbb{Q}(\alpha)$ ,  $\mathbb{Q}(\beta)$  und  $\mathbb{Q}(\sqrt{3}, \sqrt{-3})$   $\square$

Übung: F22T2A5, H25T2A3  
 (vgl. Bsp  $\mathbb{Q}(\sqrt{2}, \sqrt{3}) / \mathbb{Q}$  im Skript)

F14T3A4 Sei  $L \subseteq \mathbb{C}$  der Zerfällungskörper von  $f = x^3 - \pi$  über  $K = \mathbb{Q}(\pi)$

Es darf verwendet werden, dass  $\pi$  transzendent über  $\mathbb{Q}$  ist.

(a) Bestimmen Sie den Erweiterungsgrad  $[L : K]$ .

Sei  $\alpha = \sqrt[3]{\pi}$  und  $\zeta = -\frac{1}{2} + \frac{1}{2}\sqrt{-3}$ .

Beh.:  $L = K(\alpha, \zeta)$

$\zeta$  ist primitive dritte Einheitswurzel  $\Rightarrow 1, \zeta, \zeta^2$   
sind paarw. verschieden  $\alpha \neq 0$  (da  $\pi \neq 0$ )  $\Rightarrow$

$\alpha, \zeta\alpha, \zeta^2\alpha$  sind paarw. verschieden

Für  $j \in \{0, 1, 2\}$  ist  $\zeta^j\alpha$  jeweils eine Nullstelle

von  $f$  wg.  $f(\zeta^j\alpha) = (\zeta^j\alpha)^3 - \pi = (\zeta^3)^j \alpha^3 - \pi$

$= 1^j \cdot \pi - \pi = 0 \Rightarrow N = \{\alpha, \zeta\alpha, \zeta^2\alpha\}$  ist die

Menge der komplexen Nullst. von  $f \Rightarrow$

$L = \mathbb{Q}(N)$  z.zg. also:  $\mathbb{Q}(N) = \mathbb{Q}(\alpha, \zeta)$

genügt:  $N \subseteq \mathbb{Q}(\alpha, \beta)$ ,  $\{\alpha, \beta\} \subseteq \mathbb{Q}(N)$

Die erste Inkl. gilt, da für  $j \in \{0, 1, 2\}$  aus  $\{\alpha, \beta\} \subseteq \mathbb{Q}(\alpha, \beta)$  auch  $\beta^j \alpha \in \mathbb{Q}(\alpha, \beta)$  folgt. Die zweite erhält man wg.  $N \subseteq \mathbb{Q}(N)$  aus  $\alpha \in N$  und  $\beta = \frac{\beta \alpha}{\alpha}$ ,  $\alpha, \beta \alpha \in N$  ( $\Rightarrow$  Beh.)

$$\text{Gradformel} \Rightarrow [L:K] = [K(\alpha, \beta):K(\alpha)] \cdot [K(\alpha):K]$$

Das Element  $\beta$  ist Nullst. von  $g = x^2 + x + 1 \in K(\alpha)[x]$

Ang.  $g$  ist reduzibel.  $\text{grad}(g) = 2 \Rightarrow$  Die Nullstel-

len  $\beta, \beta^2 = -\frac{1}{2} - \frac{1}{2}\sqrt{-3}$  liegen in  $K(\alpha)$   $\wedge$  da  $K(\alpha) =$

$\mathbb{Q}(\pi, \alpha) \subseteq \mathbb{R}$  wg.  $\pi, \alpha \in \mathbb{R}$ , andererseits aber  $\beta \notin \mathbb{R}$

Da also  $g$  irred. in  $K(x)[x]$ , außerdem normiert, folgt  
 $g = \mu_{g, K(x)}$  und  $[K(x, \sqrt[3]{x}) : K(x)] = \text{grad}(g) = 2$

Beh.  $f$  ist über  $K$  irreduzibel

Ang.,  $f$  ist über  $K$  reduzibel. Wegen  $\text{grad}(f) = 3$   
ist dann eine der drei komplexen Nullstellen in  $K$  ent-  
halten.  $\exists x \in K$  und  $f^2 \in K$  ist ausgeschlossen,  
da  $\pi \in \mathbb{R}$ , somit  $K = \mathbb{Q}(\pi) \subseteq \mathbb{R}$ , aber  $\exists x, f^2 x \notin \mathbb{R}$   
 $\Rightarrow$  einzige Möglichkeit:  $x = \sqrt[3]{\pi} \in \mathbb{Q}(\pi) \Rightarrow$   
 $\exists u, v \in \mathbb{Q}[x] \setminus \{0\}$  mit  $x = \frac{u(\pi)}{v(\pi)}$ , wobei  $\text{ggT}(u, v) = 1$   
( $v(\pi) \neq 0$ , da  $\pi$  transzendent)

$$\Rightarrow \pi = \frac{u(\pi)^3}{v(\pi)^3} \Rightarrow \pi v(\pi)^3 - u(\pi)^3 = 0$$

$\Rightarrow \pi$  ist Nullstelle von  $W = x v^3 - u^3$ , und  $W \neq 0$ ,

da  $3 \nmid \text{grad}(x v^3)$  (wg.  $\text{grad}(x v^3) = 1 + 3 \text{grad}(v)$ )

und  $3 \mid \text{grad}(u^3) \quad \Downarrow$  da  $\pi$  transzendent ( $\Rightarrow$  Beh.)

[Alternative: Das Auswertungschem. an der Stelle  $\pi$  liefert

einen Isom.  $\mathbb{Q}[x] \cong \mathbb{Q}[\pi]$  von Ringen. Da  $x$  in  $\mathbb{Q}[x]$

ein Primalelement ist, ist  $\pi$  ein Primalelement in  $\mathbb{Q}[\pi]$ .

Man kann nun mit dem Eisenstein-Kriterium zeigen,

dass  $f$  in  $\mathbb{Q}[\pi][x]$  und damit auch in  $K[x] =$

$\mathbb{Q}(\pi)[x]$  irreduzibel.]

außerdem:  $f$  normiert,  $f(x) = 0 \Rightarrow f = \mu_{\alpha, K}$   
 $\Rightarrow [K(x):K] = \text{grad}(f) = 3$   
 $\Rightarrow [L:K] = 2 \cdot 3 = 6$

(b) Bestimmen Sie alle Zwischenkörper von  $L|K$ , indem Sie für jeden Zwischenkörper ein primitives Element angeben.

Die Erweiterung  $L|K$  ist galois'sch, denn  $L$  ist als Zerf.-korp eines Pol.  $f \in K[X]$  über  $K$  normal über  $K$ , damit auch algebraisch, und wegen  $\text{char}(K) = 0$  damit auch separabel.

Sei  $G = \text{Gal}(L|K)$ . Dann gilt  $|G| = [L:K] = 6$ . Bekanntlich sind  $\mathbb{Z}/6\mathbb{Z}$  und  $S_3$

$\mu_{x,K}$

bis auf Isomorphie die einzigen Gruppen der  
Ordnung 6  $\Rightarrow G \cong \mathbb{Z}/6\mathbb{Z}$  oder  $G \cong S_3$ .

Ang.  $G = \mathbb{Z}/6\mathbb{Z}$  Dann besitzt  $G$  genau  
eine Untergr.  $U$  mit  $|U| = 2$  (weil eine zykl.  
Gruppe zu jedem Teiler  $d$  der Gruppenordn. genau  
eine Untergr. der Ordnung  $d$  besitzt). Aus  $|U| = 2$   
und  $|G| = 6$  folgt  $(G:U) = \frac{|G|}{|U|} = \frac{6}{2} = 3$ .

Laut Galois-Theorie besitzt  $L|K$  dann genau einen  
Zwischenkörper  $M$  mit  $[M:K] = 3$ .  $\hookrightarrow$

$[K(x):K] = 3 \Rightarrow M = K(x)$  also: Auch  $Sx$   
ist Nullst. von  $f \Rightarrow [K(Sx):K] = \deg(f) = 3$   
 $\Rightarrow K(Sx) = M = K(x)$   $\forall$  da  $K(x) \subseteq \mathbb{R}$  und  $Sx \notin \mathbb{R}$ .

von  $L|K$ ,  
ein primi-

dann  $L$   
über  $K$   
trisch, und  
parabel.

$|G| =$   
 $\mathbb{Z}/6\mathbb{Z}$  und  $S_3$