

H2ST1A4 geg:  $f = x^4 - 4x^2 + 2 \in \mathbb{Q}[x]$

reelle Nullstellen von  $f$ :  $\pm \alpha, \pm \beta$  mit  $\alpha = \sqrt{2 - \sqrt{2}}, \beta = \sqrt{2 + \sqrt{2}}, L = \mathbb{Q}(\alpha)$

bereits gezeigt:  $L$  ist Zerfällungskörper von  $f$  über  $\mathbb{Q}$ .  
 $L/\mathbb{Q}$  ist galois'sch,  $[L:\mathbb{Q}] = 4$

zu (d) Sei  $G = \text{Gal}(L/\mathbb{Q})$ . Zeigen Sie, dass ein eindeutig bestimmtes Element  $\sigma \in G$  mit  $\sigma(\alpha) = \beta$  existiert.  
Bestimmen Sie  $\sigma(\sqrt{2})$  und  $\sigma^2(\alpha)$ , und zeigen Sie, dass  $G$  eine zyklische Gruppe ist.

Wohl  $f$  in  $\mathbb{Q}[x]$  irreduzibel ist und  $\alpha, \beta$  Null-

stellen von  $f$  in  $L$ , existiert auf Grund des Fortsetzungssatzes ein  $\sigma \in G$  mit  $\sigma(\alpha) = \beta$ . Wegen  $L = \mathbb{Q}(\alpha)$  ist jedes Element  $\tau \in G$  durch  $\tau(\alpha)$  bereits eindeutig festgelegt. Daraus folgt die Eindeutigkeit von  $\sigma$ .

Bestimmung von  $\sigma(\sqrt{2})$  und  $\sigma^2(\alpha)$ :

$$\sigma(2 - \sqrt{2}) = \sigma(\alpha^2) = \sigma(\alpha)^2 = \beta^2 = 2 + \sqrt{2}$$

$$\xrightarrow{\text{Zu } \mathbb{Q}\text{-Hom.}} 2 - \sigma(\sqrt{2}) = 2 + \sqrt{2} \rightarrow -\sigma(\sqrt{2}) = \sqrt{2} \rightarrow$$

$$\sigma(\sqrt{2}) = -\sqrt{2}$$

$$\text{Erinnerung: } \alpha \beta = \sqrt{(2 - \sqrt{2})(2 + \sqrt{2})} =$$

$$\sqrt{2^2 - 2} = \sqrt{2} \Rightarrow \beta = \frac{\sqrt{2}}{\alpha} \Rightarrow \sigma^2(\alpha) = \sigma(\sigma(\alpha)) =$$

$$\sigma(\beta) = \sigma\left(\frac{\sqrt{2}}{\alpha}\right) = \frac{\sigma(\sqrt{2})}{\sigma(\alpha)} = \frac{-\sqrt{2}}{\beta} = \frac{(-\alpha\beta)}{\beta} = -\alpha$$

Da  $L/\mathbb{Q}$  galoissch ist, gilt  $|G| = [L:\mathbb{Q}] = 4$ .

Wenn  $G$  also ein Element der Ordnung 4 enthält, dann ist die Gruppe zyklisch. Beh:  $\text{ord}(\sigma) = 4$

zu überprüfen: (1)  $\sigma^4 = \text{id}_L$  (2)  $\sigma^2 \neq \text{id}_L$

zu (1) folgt aus  $\sigma \in G$  und  $|G| = 4$  (und dem Satz v. Lagrange)

zu (2) Ang.  $\sigma^2 = \text{id}_L \Rightarrow -x = \sigma^2(x) = \text{id}_L(x) = x$

$\Rightarrow 2x = 0 \Rightarrow x = 0 \quad \nmid$



H22T1A4 Sei  $f = x^4 + 5x^2 + 5 \in \mathbb{Q}[x]$ . Sei  $L$  der Zerfällungskörper von  $f$  über  $\mathbb{Q}$  in  $\mathbb{C}$  und  $\alpha \in \mathbb{C}$  eine Nullstelle von  $f$ .

(a) Teilen Sie  $f$  im Polynomring  $\mathbb{Q}(\alpha)[x]$  durch  $x^2 - \alpha^2$ , ohne  $\alpha$  zu berechnen.

$$f - x^2 \cdot (x^2 - \alpha^2) = (x^4 + 5x^2 + 5) - x^4 + \alpha^2 x^2 = (5 + \alpha^2)x^2 + 5$$

$$(5 + \alpha^2)x^2 + 5 - (5 + \alpha^2) \cdot (x^2 - \alpha^2) = (5 + \alpha^2)x^2 + 5$$

$$- (5x^2 + \alpha^2 x^2 - 5\alpha^2 - \alpha^4) = 5 + 5\alpha^2 + \alpha^4 = f(\alpha) = 0$$

$$\text{Ergebnis: } f = (x^2 + 5 + \alpha^2) \cdot (x^2 - \alpha^2)$$

(g) Zeigen Sie:  $(x^3 + 3x)^2 = -(5 + x^2)$

$$f(x) = 0 \Rightarrow x^4 + 5x^2 + 5 = 0 \Rightarrow x^4 = -5x^2 - 5$$

$$x^5 = x \cdot x^4 = x(-5x^2 - 5) = -5x^3 - 5x$$

$$\begin{aligned} x^6 &= x \cdot x^5 = x(-5x^3 - 5x) = -5x^4 - 5x^2 \\ &= -5(-5x^2 - 5) - 5x^2 = 20x^2 + 25 \end{aligned}$$

$$\begin{aligned} \Rightarrow (x^3 + 3x)^2 &= x^6 + 6x^4 + 9x^2 = (20x^2 + 25) \\ &+ 6(-5x^2 - 5) + 9x^2 = 20x^2 + 25 - 30x^2 - 30 \\ &+ 9x^2 = -x^2 - 5 = -(5 + x^2) \end{aligned}$$

(c) Sei  $G = \text{Gal}(L|\mathbb{Q})$ . Zeigen Sie, dass  $[L:\mathbb{Q}] = 4$  und  $G \cong \mathbb{Z}/4\mathbb{Z}$  gilt.

Es gilt  $f(x) = 0$ , das Polynom ist normiert und

in  $\mathbb{Q}[x]$  irreduzibel nach dem Eisenstein-Krit.  
 $\Rightarrow f = \text{Mx. } \mathbb{Q} \Rightarrow [\mathbb{Q}(x): \mathbb{Q}] = \text{grad}(f) = 4$ .

Sei  $\beta = x^3 + 3x$ . Beh.: Durch  $\pm x, \pm \beta$  sind vier verschiedene Nullstellen von  $f$  in  $\mathbb{C}$  gegeben.

Laut Angabe ist  $x$  eine Nullstelle von  $f$ . Ist  $x \in \mathbb{C}$  eine Nullstelle von  $f$ , dann auch  $-x$ , wegen  
 $f(-x) = (-x)^4 + 5(-x)^2 + 5 = x^4 + 5x^2 + 5 = f(x) = 0$ .  
 $\Rightarrow -x$  ist Nullstelle von  $f$ .

$$f(\beta) \stackrel{(\text{a})}{=} (\beta^2 + 5 + \alpha^2) \cdot (\beta^2 - \alpha^2) \stackrel{(\text{b})}{=} (-5 - \alpha^2 + 5 + \alpha^2) \cdot (\beta^2 - \alpha^2) = 0 \cdot (\beta^2 - \alpha^2) = 0. \text{ Mit } \beta \text{ ist auch } -\beta \text{ eine Nullstelle von } f.$$

Ang.  $x = -x \Rightarrow 2x = 0 \Rightarrow x = 0$   $\nmid$  da 0 keine Nullstelle von  $f$  ist. Genauso sieht man  $\beta \neq -\beta$ .

Ang.  $\beta = \alpha \Rightarrow \alpha = \alpha^3 + 5\alpha \Rightarrow \alpha^3 + 2\alpha = 0$   
 $\Rightarrow \alpha$  ist Nullstelle von  $g = x^3 + 2x \nmid$  da  $\text{grad}(g) <$   
 $\text{grad}(f)$  und  $f = \mu_{\alpha, \mathbb{Q}}$

Ang.  $\beta = -\alpha \Rightarrow -\alpha = \alpha^3 + 3\alpha \Rightarrow \alpha^3 + 4\alpha = 0$   
 $\Rightarrow \alpha$  ist Nullstelle von  $h = x^3 + 4x \nmid$  da  $\text{grad}(h)$   
 $< \text{grad}(f)$  und  $f = \mu_{\alpha, \mathbb{Q}}$

Aus  $\beta \neq \pm \alpha$  folgt  $-\beta \neq \pm \alpha$ . ( $\Rightarrow$  Beh.)

Aus der Beh. folgt  $L = \mathbb{Q}(S)$  mit  $S = \{\pm \alpha, \pm \beta\}$ .

Es gilt  $\mathbb{Q}(S) = \mathbb{Q}(\alpha)$ , denn: „ $\supseteq$ “  $\alpha \in S$   
 $\Rightarrow \alpha \in \mathbb{Q}(S)$  „ $\subseteq$ “  $\alpha \in \mathbb{Q}(\alpha) \Rightarrow \beta = \alpha^3 + 3\alpha$   
 $\in \mathbb{Q}(\alpha) \Rightarrow \{\pm \alpha, \pm \beta\} \subseteq \mathbb{Q}(\alpha) \Rightarrow S \subseteq \mathbb{Q}(\alpha)$

Insgesamt erhalten wir  $L = \mathbb{Q}(S) = \mathbb{Q}(\alpha)$

und  $[L:\mathbb{Q}] = [\mathbb{Q}(\alpha):\mathbb{Q}] = 4$

Die Erweiterung  $L|\mathbb{Q}$  ist galois'sch, denn

- Als Zerfällungskörper eines Polynoms  $f \in \mathbb{Q}[x]$  über  $\mathbb{Q}$  ist  $L|\mathbb{Q}$  normal.

- Als normale Erweiterung ist  $L|\mathbb{Q}$  insb. algebraisch und wegen  $\text{char}(\mathbb{Q}) = 0$  damit auch separabel.

Da  $L|\mathbb{Q}$  galois'sch ist, gilt  $|G| = |\text{Gal}(L|\mathbb{Q})| = [L:\mathbb{Q}] = 4$ . Wenn  $G$  ein Element der Ordnung 4 enthält, dann ist  $G$  also isomorph zu  $\mathbb{Z}/4\mathbb{Z}$ .

Da  $f$  in  $\mathbb{Q}[x]$  irreduzibel ist, und  $\alpha, \beta$  Nullstellen von  $f$  in  $L$  sind, gibt es auf Grund des Fortsetzungssatzes ein Element  $\sigma \in G$  mit  $\sigma(\alpha) = \beta$ .

Beh.  $\text{ord}(\sigma) = 4$  zu überprüfen: (1)  $\sigma^4 = \text{id}_L$  (2)  $\sigma^2 \neq \text{id}_L$

zu (1) Wegen  $|G| = 4$  gilt  $\text{ord}(\sigma) \mid 4$ , also  $\sigma^4 = \text{id}_L$ .

zu (2)  $\sigma^2(\alpha) = \sigma(\sigma(\alpha)) = \sigma(\beta) = \sigma(\alpha^3 + 3\alpha) =$   
 $\sigma(\alpha^3) + \sigma(3\alpha) = \sigma(\alpha)^3 + \sigma(3)\sigma(\alpha) = \sigma(\alpha)^3 + 3\sigma(\alpha) =$   
 $\beta^3 + 3\beta = (\alpha^3 + 3\alpha)^3 + 3(\alpha^3 + 3\alpha) = (\alpha^3 + 3\alpha)^2(\alpha^3 + 3\alpha)$   
 $+ 3(\alpha^3 + 3\alpha) = -(5 + \alpha^2)(\alpha^3 + 3\alpha) + 3(\alpha^3 + 3\alpha) =$   
 $(-5 - \alpha^2 + 3)(\alpha^3 + 3\alpha) = -(2 + \alpha^2)(\alpha^3 + 3\alpha) = -(2\alpha^3 + \alpha^5$   
 $+ 3\alpha^3 + 6\alpha) = -(2\alpha^3 + (-5\alpha^3 - 5\alpha) + 3\alpha^3 + 6\alpha)$   
 $= -\alpha \quad \text{Ang. } \sigma^2 = \text{id}_L \Rightarrow -\alpha = \sigma^2(\alpha) = \alpha \quad \nmid \quad \square$

Erinnerung: Sei  $K$  ein Körper,  $f \in K[x]$  ein Polynom ist separabel irreduziblen Faktoren. Sei  $L$  ein Zerfällungskörper von  $f$  über  $K$ . Dann ist  $L|K$  eine Galois-erweiterung.

- Die Galoisgruppe  $\text{Gal}(L|K)$  wird dann auch als Galoisgruppe  $\text{Gal}(f|K)$  des Polynoms  $f$  über  $K$  bezeichnet.

- Seien  $\alpha_1, \dots, \alpha_n$  die verschiedenen Nullstellen von  $f$  in  $L$ . Dann existiert ein injektiver Homomorphismus  $\phi: \text{Gal}(f|K) \rightarrow S_n$  mit  $\sigma(\alpha_k) = \alpha_{\phi(\sigma)(k)}$  für  $1 \leq k \leq n$ ,  $\sigma \in \text{Gal}(f|K)$ .

Bsp:  $f = (x^2 - 2)(x^2 - 3) \in \mathbb{Q}[x]$

Nullstellen:  $\alpha_1 = \sqrt{2}, \alpha_2 = -\sqrt{2}, \alpha_3 = \sqrt{3}, \alpha_4 = -\sqrt{3}$

$K = \mathbb{Q}, L = \mathbb{Q}(\alpha_1, \alpha_2, \alpha_3, \alpha_4) = \mathbb{Q}(\sqrt{2}, \sqrt{3})$

Sei  $\phi: \text{Gal}(f/\mathbb{Q}) \rightarrow S_4$  wie oben.

letzte Stunde:  $G = \text{Gal}(f/\mathbb{Q})$  besteht aus den Elementen  $\{ \text{id}, \sigma, \tau, \sigma\tau \}$ , wobei  $\sigma(\sqrt{2}) = -\sqrt{2}, \sigma(\sqrt{3}) = \sqrt{3}, \tau(\sqrt{2}) = \sqrt{2}, \tau(\sqrt{3}) = -\sqrt{3}$

$\sigma(\alpha_1) = -\sqrt{2} = \alpha_2, \sigma(\alpha_2) = \sigma(-\sqrt{2}) = -\sigma(\sqrt{2}) = -(-\sqrt{2}) = \sqrt{2} = \alpha_1, \sigma(\alpha_3) = \alpha_3, \sigma(\alpha_4) = \alpha_4$

$\Rightarrow \phi(\sigma) = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 1 & 3 & 4 \end{pmatrix} = (12)$

Ebenso erhält man  $\phi(\tau) = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 2 & 4 & 3 \end{pmatrix} = (3\ 4)$   
und  $\phi(\sigma\tau) = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 1 & 4 & 3 \end{pmatrix} = (1\ 2)(3\ 4)$