

ALGEBRA 28.5.

$S \geq T$ .  $\text{Gal}(S/T) = \{ \varphi : S \rightarrow S \mid \begin{array}{l} \text{$T$-autom.} \\ \varphi(t) = t \quad \forall t \in T. \end{array} \}$

$S = T(a_1, \dots, a_n)$ ,  $a_i$  alg. ned  $T$

$\Rightarrow \varphi \in \text{Gal}(S/T)$  jedu. méně hodn.  $\varphi(a_i)$ .

T.24.1  $T \leq S$ ,  $f \in T[x]$ ,  $A \subseteq S$  min. víclo břemí  $f$  v  $S/T$ .

$\forall \varphi \in \text{Gal}(S/T)$  je  $\varphi|A$  permutace ve  $A$  &

$\text{Gal}(S/T) \rightarrow S_A$  je grupový hom.

D8.  $f = \sum c_i x^i$ ,  $\alpha \in S$  kořen.

$$0 = f(\varphi(\alpha)) = \sum c_i \varphi(\alpha)^i \stackrel{T\text{-aut.}}{=} \sum \varphi(c_i) \varphi(\alpha)^i = \varphi\left(\sum c_i \alpha^i\right) = \varphi(f(\alpha)) = \varphi(0) = 0.$$

Tedy  $\varphi(\alpha)$  taky kořen.

Ale polud  $\alpha \in T$ , pak  $\varphi(\alpha) = \alpha \in T$ .

$\varphi$  je proti  $\Leftrightarrow$  Tedy jiný kořen  $\alpha'$  x mi ve  $\alpha$  neoblasti.

Tedy  $\varphi|A$  je proti' zobrazení na  $A$ .

$A$  je lom. množ.  $\Rightarrow \varphi|A$  je bijekce, t. i. permutace.

Grupový hom. ✓



Pi.  $\alpha \in R$ ,  $\alpha \neq 0$ .  $\text{Gal}(\mathbb{Q}(\sqrt{\alpha})/\mathbb{Q}) \ni \varphi$

$f = x^2 - \alpha \in \mathbb{Q}[x] \Rightarrow \varphi$  permutuje kořeny v  $\mathbb{Q}(\sqrt{\alpha}) \setminus \mathbb{Q}$ .

$A = \{\sqrt{\alpha}, -\sqrt{\alpha}\}$ . Tedy  $\varphi(\sqrt{\alpha}) = \begin{cases} \sqrt{\alpha} \\ -\sqrt{\alpha} \end{cases}$ .

Zároveň  $\varphi$  je jedn. méně hodnotou  $\varphi(\sqrt{\alpha})$ .

$\Rightarrow$  nejprve 2 možné prvky  $\text{Gal}(\mathbb{Q}(\sqrt{\alpha})/\mathbb{Q})$ , a zde

$$a + b\sqrt{\alpha} \mapsto \begin{cases} a + b\sqrt{\alpha} \\ a - b\sqrt{\alpha} \end{cases} \quad \text{Svedlo x očividně, že oba jsou } \mathbb{Q}\text{-autom.}$$

Pi.  $\alpha \in R$ ,  $\sqrt[3]{\alpha} \notin \mathbb{Q}$ .  $\text{Gal}(\mathbb{Q}(\sqrt[3]{\alpha})/\mathbb{Q}) \ni \varphi$

$f = x^3 - \alpha$  [notace: je to min. pol. pro  $\sqrt[3]{\alpha}$ ]

Ale kořeny  $f$  v  $\mathbb{C}$  jsou  $\sqrt[3]{\alpha}$ ,  $\xi_3 \sqrt[3]{\alpha}$ ,  $\xi_3^2 \sqrt[3]{\alpha}$ , kde  $\xi_3 = e^{\frac{2\pi i}{3}}$ .

$\Rightarrow A = \{\sqrt[3]{\alpha}\} \Rightarrow \varphi(\sqrt[3]{\alpha}) = \sqrt[3]{\alpha} \Rightarrow \varphi = \text{id}$  a Gal je 1-pruhová!

## 24.2 Jednosměrnost řeš. a rozdil. nedt. [bez důležit.]

Tipoměr! T telos,  $f \in T[x]$ ,  $\deg f \geq 1$ .

• Korenové nedt. =  $S \geq T + \mathbb{Z}$ .  $\exists a \in S, f(a) = 0 \wedge S = T(a)$ .

• Rozkladové nedt. =  $S \geq T + \mathbb{Z}$ .  $\exists a_1, \dots, a_n \in S$ :

$$S = T(a_1, \dots, a_n) \quad \& \quad f \parallel (x-a_1) \cdots (x-a_n).$$

Př.  $T = \mathbb{Q}$ . Korenové': rozdil. množinu nejít jako podmnožinu ... díl. se' sledu' větě algebra.  $\Rightarrow f \in \mathbb{C}$  rozhledové' ne řeš. címitele. Pod def.  $S = \mathbb{Q}(a_1, \dots, a_n) \rightsquigarrow$  rozdil.

$$S = \mathbb{Q}(a_i) \rightsquigarrow \text{řeš.}$$

Př.  $x^2 + 1 \rightsquigarrow a_1 = i, a_2 = -i$ .

$$\text{Korenové'} \quad \mathbb{Q}(i) = \mathbb{Q}(-i)$$

$$\text{Rozkladové'} \quad \mathbb{Q}(i, -i))$$

•  $x^3 - 1 \rightsquigarrow$  řešený  $\vee \mathbb{C}$ :  $1, \xi_3, \xi_3^2$ .

$$\text{Korenové'} \quad \mathbb{Q}(1) = \mathbb{Q}, \quad \mathbb{Q}(\xi_3) = \mathbb{Q}(\xi_3^2).$$

Veta 24.2 (jednosměrnost řešených a rozdil. nedt.).

T telos,  $f \in T[x]$ ,  $\deg f \geq 1$ .

1) je-li  $f$  irreducibilní, pak kžde' dvě korenové' nedt.  $f$  nad  $T$  jsou  $T$ -isom.

2) kžde' dvě rozkladové' nedt.  $f$  nad  $T$  jsou  $T$ -isom.

Návaznost 1) Majme řeš. nedt.  $T(a), T(b)$ .

$a, b$  alg. nad  $T \Rightarrow T(a) = T[b] = \{g(a) \mid g \in T[x]\}$

Definujme  $T(a) \longrightarrow T(b)$ . Toto sobr. je kbledaný  
 $g(a) \longmapsto g(b)$   $+T$ -isom.

[napřed se ale musí dle, že to je dobré def.]

## 24.3 Galoisská grupa polynomu

Def.  $f \in T[x], \deg f \geq 1$ . Gal. sk. polynomu  $f$  nad  $T$  je

$\text{Gal}(f/T) = \text{Gal}(S/T)$  pro kždenou' rozkladové' nedt.

$S$  polynom  $f$  nad  $T$ .

• Dále' to smysl?  $S_1, S_2$  rozdil. nedt.  $\Rightarrow$  (V.24.2)

$S_1, S_2$  jsou  $T$ -isom.  $\stackrel{CV}{\longrightarrow} \text{Gal}(S_1/T) \cong \text{Gal}(S_2/T)$ .

Takže  $\text{Gal}(f/T)$  je dobré def. ( $\cong$  nejsou isom.)

Př.  $\alpha \neq 0$ .  $\mathbb{Q}(\sqrt{\alpha})$  je rozll. nedt.  $x^2 - \alpha$  a tedy  
 $\text{Gal}(\mathbb{Q}(\sqrt{\alpha})/\mathbb{Q}) = \text{Gal}(\mathbb{Q}(\sqrt{\alpha})/\mathbb{Q}) = \{\sqrt{\alpha} \mapsto \pm \sqrt{\alpha}\} + \mathbb{Z}_2$

---

$\sqrt[3]{\alpha} \notin \mathbb{Q}$ .  $\text{Gal}(\mathbb{Q}(\sqrt[3]{\alpha})/\mathbb{Q}) = \{1\}$ , ale totto není  $\text{Gal}(\mathbb{Q}(\sqrt[3]{\alpha})/\mathbb{Q})$   
 bo  $\mathbb{Q}(\sqrt[3]{\alpha})$  není rozll. nedt.  
 [ plati'  $\text{Gal}(\mathbb{Q}(\sqrt[3]{\alpha})/\mathbb{Q}) \cong \mathbb{Z}_3$  ]  
 $(\sqrt[3]{\alpha} \mapsto \zeta_3 \cdot \sqrt[3]{\alpha}) \mapsto j$

T. 24.5 (zákl. vlast. Gal. skup)  $T$  telos,  $f \in T[x]$ , def  $f \geq 1$ ,  $S =$  rozll. nedt.  
 $f$  ned  $T$ .

- 1)  $\text{Gal}(S/T)$  je izomorfí podskupiny symetr. skupiny  $S_m$ , kde  
 $m = \text{počet různých kořenů } f \in S \setminus T$ .
- 2)  $f$  irreducibilní  $\Rightarrow$   $\nexists$  kořeny  $a, b \in S \exists \varphi \in \text{Gal}(S/T)$ :  
 $\varphi(a) = b$ .
- 3)  $T \leq S \leq U$ , kde  $U$  je rozllad. nedt. nejakeho pol. ned  $T$ .  
 Pak  $\text{Gal}(U/S) \cong \text{Gal}(U/T)$  a  $\text{Gal}(U/T)/\text{Gal}(U/S) \cong \text{Gal}(S/T)$ .

[ zápisem jen dle 1) ]

Dl. 1)  $A = \{a_1, \dots, a_m\} =$  kořeny  $f \in S \setminus T$ .

T. 24.1  $\Rightarrow \forall \varphi \in \text{Gal}(S/T) \quad \varphi|_T$  je permutace  $A$ . a  
 $\psi: \text{Gal}(S/T) \rightarrow S_A$  je hom.

Dl. 2)  $\varphi$  je prostel:  $S$  rozllad. nedt.  $\Rightarrow S = T(a_1, \dots, a_m)$   
 Cili  $\forall \varphi$  je jednoz. určené hodnotami  $\varphi(a_1), \dots, \varphi(a_m)$ ,  
 iili  $\varphi|_T$  jednoz. určuje  $\varphi \Rightarrow \varphi$  je prostel.

Tedy podle 1. v. o izom.:  $\text{Gal}(S/T) \cong \text{Im } \varphi \leq S_A \cong S_m$ .

2) plývá  $=$  dle 2. jednoz. rozll. nedt.

3) Použij 1. v. o izom.

$\Phi: \text{Gal}(U/T) \rightarrow \text{Gal}(S/T) \quad \left\{ \begin{array}{l} \text{ověřte}, \\ \varphi \mapsto \varphi|_S \end{array} \right\}$  to funguje.

$\text{Im } \Phi = \text{Gal}(S/T) \dots$  zde užíváme jedn. rozll. nedt.

$\text{Ker } \Phi = \varphi \Leftrightarrow \varphi|_S = \text{id} \Leftrightarrow \varphi(s) = s \forall s \in S \quad \left\{ \begin{array}{l} \text{Ker } \Phi = \text{Gal}(U/S) \\ \Leftrightarrow \varphi \in \text{Gal}(U/S) \end{array} \right\} \quad \begin{array}{l} \text{Ker } \Phi = \text{Gal}(U/S) \\ \cong \text{Gal}(U/T) \end{array}$

Příklad:  $\text{Gal}(\mathbb{Q}(\sqrt{2}, \sqrt{3})/\mathbb{Q}) \cong \mathbb{Z}_2$ .

T. 24.1 Pro polynomy  $x^2 - 2$ ,  $x^2 - 3$ .  
 $\Rightarrow \varphi(\sqrt{2}) = v\sqrt{2}$  pro  $v = \pm 1$ . } jednosložné mění  $\varphi$ .  
 $\varphi(\sqrt{3}) = v\sqrt{3}$  pro  $v = \pm 1$ .

$$\mathbb{Q}(\sqrt{2}, \sqrt{3}) = \mathbb{Q}[\sqrt{2}, \sqrt{3}] = \{ a + b\sqrt{2} + c\sqrt{3} + d\sqrt{6} \mid a, b, c, d \in \mathbb{Q} \}$$

$\downarrow \varphi_{v,v}$

$$a + b v \sqrt{2} + c v \sqrt{3} + d v v \sqrt{6}$$

Je tyto třídy ověřit, že když volba  $v, v$  funguje.  
 třídy  $\varphi_{v,v} \in G$ .

Na rovnou:  $\varphi_{v,v}$ .

- Zatím náleží, že  $|G| \leq 4$ .
- Zároveň:  $\mathbb{Q}(\sqrt{2}, \sqrt{3}) = \mathbb{Q}(\sqrt{2} + \sqrt{3})$ , kde  $\alpha = \sqrt{2} + \sqrt{3}$ ,  $\alpha^4 = x^4 - 10x^2 + 1$ .  
 Tedy máme 4 různých  $\alpha$  podle T. 24.5(2)  $\exists \varphi_i \in G$ :  
 $\varphi_i(\alpha_i) = \alpha_i$

$$\Rightarrow |G| \geq 4$$

- Dohromady  $|G|=4$  &  $G = \{\varphi_{v,v} \mid v, v = \pm 1\} \cong \mathbb{Z}_2 \times \mathbb{Z}_2$

$$\begin{aligned} \varphi_{1,1} &\mapsto (0, 0) \\ \varphi_{1,-1} &\mapsto (0, 1) \\ \varphi_{-1,1} &\mapsto (1, 0) \\ \varphi_{-1,-1} &\mapsto (1, 1) \end{aligned}$$

Posl. V čer. O pro rozsl. ned. S plati':  $[S:T] = |\text{Gal}(S/T)|$

$$\xi_n = e^{\frac{2\pi i}{n}}$$

L. 24.6 Ufa  $a \in \mathbb{Q}$ . Rozkladové násil. polynomu  $f = x^n - a$  nad  $\mathbb{Q}$   
 je  $\mathbb{Q}(\xi_n, b)$ , kde  $b$  je libovolný komplexní kořen  $f$ .

Dl. kompl. řešení  $x^n - a$  jsou právě  $b \cdot \xi_n^\ell$ ,  $\ell = 0, -1, \dots, n-1$ :

$$\text{Bo} \quad f(b \cdot \xi_n^\ell) = b^n \cdot \underbrace{\left(e^{\frac{2\pi i}{n} \cdot \ell}\right)^n}_{=} -a = b^n - a = 0.$$

$\Rightarrow$  melem u řešení polynomu  $-tupné u \Rightarrow$  melem už všechny.

Rozsl. ned.  $S = \mathbb{Q}(b, b\xi_n, b\xi_n^2, \dots, b\xi_n^{n-1}) = ? \mathbb{Q}(b, \xi_n) = S'$

$$\Leftrightarrow b \in S \vee \xi_n = e^{-1} \cdot (b\xi_n) \in S \quad \Leftrightarrow b\xi_n^\ell \in S'$$

T. 24-7 (Galoisový základ pro odmocniny).  $\mathbb{Q} \leq T \leq \mathbb{C}$  těleso,  $n \in \mathbb{N}$ ,  $a \in T$ . Pak

1)  $\text{Gal}(x^{n-1}/T)$  je abelovské

2)  $\text{Gal}(x^{n-a}/T(\xi_n))$  je abelovské

3)  $\text{Gal}(x^{n-a}/+)$  je řešitelné' grupa stupně'  $\leq 2$ .

Dl.  $S = T(\xi_n)$ ,  $U = T(\xi_n, b)$ , kde  $b \in \mathbb{C}$  je nejednoduchější kořen  $x^{n-a}$ .

1) Dl., že je izom. podgrupe  $\mathbb{Z}_n^*$ .

$S = \text{rozdil. nedl. pol. } x^{n-1}$  (bo kořeny jsou  $1 = \xi_n^0, \xi_n^1, \xi_n^2, \dots, \xi_n^{n-1}$ )

$\forall \varphi \in \text{Gal}(S/T)$  permutuje kořeny  $x^{n-1}$ , tedy  $\varphi(\xi_n) = \xi_n^{\varrho}$  pro nejale'  $\varrho$ .

Co můžu učinit o  $\varrho$ ?  $\varphi$  je autom. tělesa  $S \Rightarrow \varphi$  je taky autom. grupy  $S^*$

$\Rightarrow \varphi$  zachovává' řády prvků  $\sim S^*$

$\text{ord}(\xi_n) = n \Rightarrow \text{ord}(\xi_n^{\varrho}) = 1 \Leftrightarrow \varrho \text{ je v. d. } \text{NSD}(\varrho, n) = 1$ .

Tedy mám zobrazení  $\Phi: \text{Gal}(S/T) \rightarrow \mathbb{Z}_n^*$

$$\varphi(\xi_n) = \xi_n^{\varrho} \mapsto \varrho$$

To to zobrazení je prosté', bo  $\varphi(\xi_n)$  jednoznačně určuje  $\varphi$  na  $S = T(\xi_n)$

$\Phi$  se grupovým hodn.:  $\varphi(\xi_n) = \xi_n^{\varrho}, \psi(\xi_n) = \xi_n^{\varphi}$

$$\begin{aligned} & (\varphi \circ \psi)(\xi_n) = \varphi(\psi(\xi_n)) = \varphi(\xi_n^{\varphi}) = \xi_n^{\varphi \varrho} \\ & \text{Tedy } \underbrace{\Phi(\varphi \circ \psi)}_{\text{ře}} = \underbrace{\Phi(\varphi)}_{\varrho} \cdot \underbrace{\Phi(\psi)}_{\varphi} \quad \therefore \end{aligned}$$

1. v. o izom.:  $\text{Gal}(S/T) \cong \text{Im } \Phi \leq \mathbb{Z}_n^*$ .

2) Na'vsej, neoboušíme:  $\text{Gal}(x^{n-a}/S) = \text{Gal}(U/S) \ni \varphi$ .

Dl., že  $\text{Gal}(U/S)$  je izom. podgrupe  $\mathbb{Z}_n^*$ .

Kořeny  $x^{n-a}$  jsou  $b \cdot \xi_n^{\varrho} \Rightarrow \varphi(b) = b \cdot \xi_n^{\varrho}$ ,

a to mi dělá' hodn.

$$\text{Gal}(U/S) \rightarrow \mathbb{Z}_n^*$$

$$\varphi(b) = b \cdot \xi_n^{\varrho} \mapsto \varrho \quad - \text{Ověřte si, že vše OK.}$$

3)

$$3) \text{Gal}(x^n - a/\tau) = \text{Gal}(\mathbb{Q}/\tau)$$

$U = \tau(\xi_n, b)$  -- rovník. neděl. pro  $x^n - a$  (podle č. 24.6)

$$S = \tau(\xi_n)$$

Rozšíření  $\tau \leq S \leq U$ .

$$\text{Č. 24.5(3): } \text{Gal}(U/S) \trianglelefteq \text{Gal}(\mathbb{Q}/\tau)$$

K řešitelnosti potřebujeme řetězec podgrup

$$\{\text{id}\} \leq \text{Gal}(U/S) \leq \text{Gal}(\mathbb{Q}/\tau),$$

$$\text{Kde } \text{Gal}(\mathbb{Q}/S)/_{\{\text{id}\}} \text{ a } \text{Gal}(\mathbb{Q}/\tau)/_{\text{Gal}(\mathbb{Q}/S)} \text{ jsou abeliovské}$$

$$\text{Gal}(\mathbb{Q}/S)$$

abel. podle 2)

$$\text{Gal}(S/\tau)$$

abel. podle 1).

Stupeň řešitelnosti = délka nejkratšího řetězce, když řetězec

má v řetězci délku 2  $\Rightarrow$  stupeň řeš.  $\leq 2$ .

(ale mohlo by být, že  $\text{Gal}(\mathbb{Q}/\tau)$  je abel., tedy stupeň řeš. = 1)