

# ALGEBRA 21.5.

## 21. tělesná rozšíření $T \subseteq S$

$S_T \dots S$  jako v.p. nad tělesem  $T$ .

Stupeň rozšíření  $[S:T] = \dim S_T$ .

$[\mathbb{C}:\mathbb{R}] = 2 \dots$  báze  $1, i$ .

$[S:S] = 1 \dots$  báze  $1$ .

$[\mathbb{Q}(\sqrt{2}, \sqrt{3}):\mathbb{Q}] = 4 \dots$  báze  $1, \sqrt{2}, \sqrt{3}, \sqrt{6}$ .

•  $\xi_3 = e^{2\pi i/3}$    $x^3 - 1$ .  $[\mathbb{Q}(\xi_3):\mathbb{Q}] = 2!$   
 $\xi_3^3 = 1$   $\mathbb{Q}(\xi_3)$  má  $1, \xi_3, \xi_3^2$  jako gener. mož.

$$x^3 - 1 = (x-1)(x^2 + x + 1)$$

a platí  $\xi_3^2 = -\xi_3 - 1$ . báze je  $1, \xi_3$ .

Je lin. nez., protože  $a \cdot 1 + b \cdot \xi_3 \neq 0$ .

•  $v \in \mathbb{C}$  transcendent. (nepř.  $e, \pi$ )  $\Rightarrow [\mathbb{Q}(v):\mathbb{Q}] = \infty$  (spočítají)  
 nebo lin. nezáv. un. je nepř.  
 $1, v, v^2, \dots$

•  $[\mathbb{R}:\mathbb{Q}]$  je nespočetný.

Prvokruh.  $R$  okruh s 1.

$\dots$  nejmenší podokruh obsahující 1.

$\varphi: \mathbb{Z} \rightarrow R$  hom.

$$n \mapsto n \cdot 1 = 1 + \dots + 1$$

$\text{Im } \varphi = \text{prvokruh}$ .  $\text{Ker } \varphi =$  největší ideál v  $\mathbb{Z} = \mathbb{Z}$   
 $\mathbb{Z} \geq 0$ .

1. v-0 izom. :  $\mathbb{Z}/\text{ker } \varphi \cong \text{Im } \varphi = \text{prvokr.}$  [ $\mathbb{Z} \neq 1$ , protože  $1 \neq 0$ ]  
 $\cong \mathbb{Z}_r, \mathbb{Z}_{\dots} (r=0)$

Prvotěleso.  $T$  těleso  $\Rightarrow$  prvok  $\mathbb{Z}, \mathbb{Z}_n \subseteq T$ .

•  $\mathbb{Z}_n, n \geq 2 \Rightarrow n = \text{charistika } T$   
Dř. jme, že  $\text{char } T = \text{prvočíslo } p$ .

$\Rightarrow \mathbb{Z}_p$  těleso  $\cong$  prvokuhl.

Prvotěleso  $P =$  nejmenší podtěleso v  $T$ .

$\Rightarrow$  tedy je  $\boxed{P \cong \mathbb{Z}_p}$  prvotěleso.

• prvok  $\mathbb{Z}$  (čili  $\text{char} = 0$ ).  $P \supseteq \mathbb{Z}$

$P$  těleso  $\Rightarrow a b^{-1} \in P, a, b \in \mathbb{Z}, b \neq 0$ .

$\Rightarrow \mathbb{Q} \subseteq P$

Prvotěleso je nejv.  $\Rightarrow \boxed{P \cong \mathbb{Q}}$

•  $T$  je rozšíření svého prvot.  $P$ .

T.21.1 Počet prvků konečného tělesa je mocnina prvočíslo.

Dř.  $T$  kon. těleso,  $P$  prvot.  $P \cong \mathbb{Z}_p$ .

Tedy v. p.  $T_P$  je izom. v. p.  $(\mathbb{Z}_p)^\mathbb{Z}$ , kde  $\mathbb{Z} = [T: P]$ .

Ale  $|\mathbb{Z}_p^\mathbb{Z}| = p^\mathbb{Z} = |T|$ .  $\ddot{\smile}$

---

## 22. ALGEBRA-PRVKY, ROZŠÍŘENÍ KON. STUPNĚ

### 22.1 Minim. polynom

Def.  $T \subseteq S$  rozšíření těles,  $\alpha \in S$ .

$\alpha$  je algebraický nad  $T$ , pokud  $\exists 0 \neq f \in T[x]; f(\alpha) = 0$ .

jinak je  $\alpha$  transcendentní nad  $T$ .

• Zřejmě soběčinnýje algebr. nad  $\mathbb{Q}$ .

• Např.  $\forall \alpha \in S$  je alg. nad  $S$ :  $\alpha$  je kořen  $f = x - \alpha \in S[x]$

Def.  $T \subseteq S$  rozš. těl.,  $\alpha \in S$  algebr. nad  $T$ .

Minimální polynom prvku  $\alpha$  nad tělesem  $T$  je  
irreducibilní monický polynom  $m_{\alpha, T} \in T[x]$ , kt. má  
kořen  $\alpha$ .

$m_{\alpha, T} \in T[x]$  irred., mon.,  $\alpha$  je kořen.

T. 22.1 (vlastnosti min. pol.)

- 1)  $m_{\alpha, T}$  existuje a je jednosm. mčej
- 2)  $\alpha$  je kořen  $f \in T[x] \Leftrightarrow m_{\alpha, T} \mid f$ .

Dř.  $I = \{ f \in T[x] \mid f(\alpha) = 0 \}$  je ideál v  $T[x]$ .

$T[x]$  OHI (obor hlavních ideálů)  $\Rightarrow I$  je hlavní.

Bud'  $m \in T[x]$  + 2.  $I = m T[x]$ .  
 moničj

Tedy:  $f(\alpha) = 0 \Leftrightarrow f \in I = m T[x] \Leftrightarrow m \mid f$ .

- $m = m_{\alpha, T}$  moničj  $\checkmark$  •  $m(\alpha) = 0 \checkmark$
- Kdyby  $m = fg$  nebyl irred., pak  $f(\alpha) \cdot g(\alpha) = 0 \Rightarrow f(\alpha) = 0$  nebo  $g(\alpha) = 0$ .  
 $\Rightarrow m \mid f$  nebo  $m \mid g$ , spor.
- $m$  tedy irred.  $\checkmark$

- jednosm.  $\tilde{m} \in T[x]$  irred., mon.,  $\tilde{m}(\alpha)$ .  
 $\Rightarrow m \mid \tilde{m}$ . Ale  $\tilde{m}$  irred.  $\Rightarrow m \parallel \tilde{m}$ , dle  $m = c \tilde{m}$   
 $\exists c \in T^*$
- Ale  $m, \tilde{m}$  moničj  $\Rightarrow c = 1$  a  $m = \tilde{m}$ .  $\square$

Př.  $m_{1, \mathbb{Q}} = x-1$ .

$m_{i, \mathbb{Q}} = x^2+1$

$m_{\sqrt[3]{2}, \mathbb{Q}} = x^3-2$  ... irreduc. d'le Eiristeinovi.

•  $m_{\xi_3, \mathbb{Q}} = x^2+x+1$  (uemi to  $x^3-1$ )

T. 22.2 (struktura jednoduchých rō. Bud'  $T \subseteq S$  kom. těles,  $\alpha \in S$ .

Pak  $T(\alpha) = T[\alpha] \Leftrightarrow \alpha$  je alg. nad  $T$ .

Dř.  $T(\alpha) = \{ f(\alpha) \mid f \in T[x] \}$

( $\Leftrightarrow$ ) hom. obzobn  $\varphi: T[x] \rightarrow T(\alpha)$   
 $f \mapsto f(\alpha)$

$\text{Im } \varphi = T(\alpha)$ ,  $\text{Ker } \varphi = \{ f \mid f(\alpha) = 0 \} = m_{\alpha, T} T[x]$ .

Víme:  $m = m_{\alpha, T}$  je irred., tedy  $m T[x]$  je mex.

1. v. o isom.  
 $T(\alpha) \cong T[x] / m T[x]$   
 faktor podle mex. id.  
 $\Rightarrow T(\alpha)$  je těleso

$T[\alpha]$  těleso  $\Rightarrow$  nejmen. těleso  $\Rightarrow T[\alpha] = T(\alpha)$  ✓

[také jde o existence inverzů v  $T[\alpha]$  přímo z Be's.  
- viz skriptk]

$\Rightarrow$   $\alpha$  transc. Pro spor at'  $T[\alpha] = T(\alpha)$ .

Tedy  $\exists f(\alpha) \in T[\alpha] + \mathbb{Z}$ .  $f(\alpha) = \alpha^{-1}$ .

Ale pak  $\alpha$  je línou pol.  $x \cdot f - 1$ , spor.

T. 22.3 (stupně jednod. rozšíření).  $T \subseteq S$  rozš.,  $\alpha \in S$  alg. nad  $T$ .

$$[T(\alpha) : T] = \deg m_{\alpha, T}$$

Dl.  $n = \deg m_{\alpha, T}$ . Dokažem, že  $1, \alpha, \alpha^2, \dots, \alpha^{n-1}$  tvoří bázi.

v. p.  $T(\alpha)_T$ .

lin. nesolv. Kdyby  $\sum_{i=0}^{n-1} t_i \alpha^i = 0$  pro nějaké  $t_i \in T$ ,

pak  $f = \sum t_i x^i$  mě  $\alpha$  se línou  $\Rightarrow m_{\alpha, T} \mid f$   
 $\deg \uparrow = n$   $\deg \uparrow \leq n-1$

$\Rightarrow f=0$  a máme triv. lin. kombinaci.

Generování.  $f(\alpha) \in T[\alpha] = T(\alpha)$ , kde  $f \in T[x]$ .

At'  $f = m_{\alpha, T} \cdot q + r$ ,  $q, r \in T[x]$ ,  $\deg r < \deg m_{\alpha, T} = n$ .

$$\Rightarrow f(\alpha) = \underbrace{m_{\alpha, T}(\alpha)}_0 \cdot q(\alpha) + r(\alpha) = \sum_{i=0}^{n-1} r_i \alpha^i$$

$r = \sum_{i=0}^{n-1} r_i x^i$   
 $r_i \in T$ .

Tím jsem  $f(\alpha)$  vyjádřil v  $1, \alpha, \dots, \alpha^{n-1}$ .

Př. •  $[\mathbb{C} : \mathbb{R}] = [\mathbb{R}(i) : \mathbb{R}] = \deg m_{i, \mathbb{R}} = \deg x^2 + 1 = 2$ .

•  $[\mathbb{Q}(\sqrt[n]{p}) : \mathbb{Q}] = \deg m_{\sqrt[n]{p}, \mathbb{Q}} = \deg (x^n - p) = n$ .

$p$  prvoč.,  $n \in \mathbb{N}$

$\uparrow$   
je irred. díky  
Eisenst.

•  $[\mathbb{Q}(e^{2\pi i/n}) : \mathbb{Q}] = \varphi(n)$  ... všechno tělo dl. (viz TC).

"cyklot. rozš.". Pro  $n=p$  ... svedne',  $m = x^{p-1} + x^{p-2} + \dots + x + 1$

Důl. 22.4  $T \subseteq S, \alpha \in S.$

$\alpha$  je alg. nad  $T \Leftrightarrow [T(\alpha): T] < \infty.$

Důl.  $\alpha$  transc.  $\Rightarrow 1, \alpha, \alpha^2, \dots$  je lin. nezav. un.

$\Rightarrow [T(\alpha): T]$  není konečný

$\alpha$  alg.  $\Rightarrow [T(\alpha): T] = \deg m_{\alpha, T} < \infty.$  (podle t. 22.3)

---

Př. (CV/zh.) Struktura kvadr. rozšíření (= rozš. stupně 2).

Pokud  $T \subseteq S \subseteq \mathbb{C}$  a  $[S: T] = 2$ , pak  $S = T[\sqrt{\alpha}]$   
pro nějaké  $\alpha \in T.$

22.2 Víceúrovňové rozšíření

$T \subseteq S \subseteq U.$

T. 22.5 (stupně úroveň rozš.) Bud'  $T \subseteq S \subseteq U$  rozš. těles.

Pak  $[U: T] = [U: S] \cdot [S: T].$

Důl.  $A =$  báze v.p.  $S_T$  Doložíme, že  $C = \{a \cdot b \mid a \in A, b \in B\}$   
 $B =$  báze v.p.  $U_S$  je báze  $U_T.$

Generování.  $C \subseteq U$ , tedy  $C$  generuje podprostor  $U_T$

$u \in U, B$  báze  $U_S \Rightarrow u = \sum_j s_j b_j, s_j \in S, b_j \in B.$

$A$  báze  $S_T \Rightarrow s_j = \sum_i t_{ij} a_i, t_{ij} \in T, a_i \in A.$

$\Rightarrow u = \sum_j \sum_i \underbrace{t_{ij}}_T \underbrace{(a_i b_j)}_C \Rightarrow u$  je vyjádření v  $C$   
s koef. z  $T.$

lin. nez. viz skriptu.

---

Pak  $[U: T] = |C| = |A| \cdot |B| = [S: T] \cdot [U: S]$

---

Úroveň víceúrovň. rozš.  $[T(\alpha_1, \alpha_2): T] = [T(\alpha_1, \alpha_2): T(\alpha_1)] \cdot$

$[T(\alpha_1): T] = \deg m_{\alpha_1, T} \cdot [T(\alpha_1): T]$

$[T(\alpha_1, \alpha_2): T(\alpha_1)] = [(T(\alpha_1)(\alpha_2): T(\alpha_1))] = \deg m_{\alpha_2, T(\alpha_1)} \leq \deg m_{\alpha_2, T}$

Def. 226  $T \subseteq S$ ,  $\alpha_1, \dots, \alpha_n \in S$  alg. nad  $T$ . Pak

$T(\alpha_1, \dots, \alpha_n)$  je normální těleso nad  $T$ .

Dk. viz výše + indukce.

Př.  $K = \mathbb{Q}(\sqrt{2} + \sqrt{3}) \stackrel{?}{=} \mathbb{Q}(\sqrt{2}, \sqrt{3})$  má stupeň 4 nad  $\mathbb{Q}$ .

•  $K \subseteq \mathbb{Q}(\sqrt{2}, \sqrt{3})$ , protože  $\sqrt{2} + \sqrt{3} \in \mathbb{Q}(\sqrt{2}, \sqrt{3})$ .

•  $\mathbb{Q} \subseteq \mathbb{Q}(\sqrt{2}) \subseteq \mathbb{Q}(\sqrt{2}, \sqrt{3}) = (\mathbb{Q}(\sqrt{2}))(\sqrt{3})$   
↑  
stupeň =  $\deg_{\mathbb{Q}} \sqrt{2} = 2$       stupeň =  $\deg_{\mathbb{Q}(\sqrt{2})} \sqrt{3} \stackrel{?}{=} 2$

•  $[\mathbb{Q}(\sqrt{2}, \sqrt{3}) : \mathbb{Q}] =$

$$[\mathbb{Q}(\sqrt{2}, \sqrt{3}) : \mathbb{Q}(\sqrt{2})] \cdot [\mathbb{Q}(\sqrt{2}) : \mathbb{Q}]$$

$$= 2 \cdot 2 = 4.$$

bo  $x^2 - 3$  je min. pol. pro  $\sqrt{3}$  nad  $\mathbb{Q}(\sqrt{2})$   
je totiž ired., protože nemá kořen.  
 $(a + b\sqrt{2})^2 - 3 \neq 0$ .

• Tedy dk., že  $K = \mathbb{Q}(\sqrt{2} + \sqrt{3}) = \mathbb{Q}(\sqrt{2}, \sqrt{3})$ , takže  $\sqrt{2}, \sqrt{3} \in K$ .

$$(\sqrt{2} + \sqrt{3})^2 = 5 + 2\sqrt{6} \Rightarrow \sqrt{6} \in K$$

$$K \ni (\sqrt{2} + \sqrt{3} + \sqrt{6})^2 = 11 + 2\sqrt{2} \cdot \sqrt{3} + 2 \cdot \sqrt{2} \cdot \sqrt{6} + 2 \cdot \sqrt{3} \cdot \sqrt{6} = \\ = \underbrace{11 + 2\sqrt{6}}_{\in K} + \underbrace{4\sqrt{3} + 6\sqrt{2}}_{\in K}$$

$$\Rightarrow 3\sqrt{2} + 2\sqrt{3} \in K. \text{ Zároveň } \sqrt{2} + \sqrt{3} \in K \Rightarrow \sqrt{2}, \sqrt{3} \in K.$$

• Tedy  $[\mathbb{Q}(\sqrt{2} + \sqrt{3}) : \mathbb{Q}] = 4$

$\Rightarrow$  min. pol. pro  $\sqrt{2} + \sqrt{3} = \alpha$  nad  $\mathbb{Q}$  má stupeň 4.

Spočítáme  $(\sqrt{2} + \sqrt{3})^2$ ,  $(\sqrt{2} + \sqrt{3})^4$  a vidíme, že  $\alpha^4 - 10\alpha^2 + 1 = 0$

•  $x^4 - 10x^2 + 1$  je pol. stupně 4, kt. má  $\alpha$  za kořen.

min. pol. má stupeň 4  $\Rightarrow x^4 - 10x^2 + 1 = m_{\alpha, \mathbb{Q}}$   
(speciálně je ired.)

---

Def.  $T \subseteq S$  norm. těleso je algebraické, pokud  $\forall \alpha \in S$  je alg. prvěk nad  $T$ .

T.22.7. Každé rozšíření kon. stupně je algebraické!

Dl.  $u = [S:T]$ . Bud'  $\alpha \in S$ .

$\alpha$  je alg.  $(\Leftrightarrow) [T(\alpha):T] < \infty$ .

$\parallel$

$$\frac{[S:T]}{[S:T(\alpha)]} \leq u$$

} tedy  $[T(\alpha):T] \leq u$   
 $\Rightarrow \alpha$  alg. nad  $T$ .

---

Opačné impl. neplatí! Ex. alg. roz. nekou. stupně  
(nepř. alg. uzávení  $\mathbb{Q}$ )

V.22.8  $T \subseteq S$ . Proby  $S$ , jest' jsou alg. nad  $T$ , trou' podteleso  $S$ .

Dl.  $\alpha, \beta \in S$  alg. nad  $T$ . Ukaz:  $\alpha + \beta, -\alpha, \alpha \cdot \beta, \alpha^{-1}$  jsou  
alg. nad  $T$ .

$$T \subseteq T(\alpha + \beta) \subseteq T(\alpha, \beta)$$

$$\forall u, \text{ je } [T(\alpha, \beta):T] < \infty \Rightarrow [T(\alpha + \beta):T] < \infty$$

$$\Rightarrow \alpha + \beta \text{ je alg.}$$

Úplně stejně pro  $-\alpha, \alpha \cdot \beta, \alpha^{-1}$ .