NMMB538 - DÚ3

Jan Oupický

1

(a) $x \in P \subset O_P$. Z definice O_P víme, že $K \subset O_P \implies K[x] \subset O_P$. Zřejmě $x \notin O_P$, protože jinak by $O_P = F$. Označme $I \coloneqq P \cap K[x]$. I je prvoideál v $K[x]$, tedy je tvaru $I = (f), f \in K[x], f$ ireducibilní. Označme $R \coloneqq K[x]_{(f)} = \{\frac{a}{b} | a \in K[x], b \in K[x] \setminus (f)\}$.

$R \subseteq O_P$, protoze $O_P = \{a \in F | v_P(a) \geq 0\}, P = \{a \in F | v_P(a) \geq 1\} \implies \frac{a}{b} \in R : v_P(\frac{a}{b}) = v_P(a) - v_P(b)$ z definice $v_P(b) = 0$, protože $b \notin (f) \subset P$ a $a \in K[x] \in O_P \implies v_P(a) \geq 0 \implies v_P(\frac{a}{b} \geq 0$.

Zároveň je R také valuační okruh F. Protože $\frac{a}{b} \in F \iff a \in K[x], b \in K[x] \setminus 0$. Buď $b \notin (f) \implies \frac{a}{b} \in R, a \notin (f), b \in (f) \implies \frac{b}{a} \in R$ a nebo $a, b \in (f)$ a to se dá vydělit na jeden z přechozích případů. Nechť Q je daný jediný maximální ideál R. Máme tedy $Q \subset R \subseteq O_P$. Z maximality P tedy plyne, že $Q = P$ a tedy musí platit $R = O_P$.

(b) $\Rightarrow$: $P' \subset P \implies a \in F : v_{P'}(a) = e(P'|P) \cdot v_P(a)$ kde $e(P'|P) \geq 1$. $x \in P$ z definice P, tedy $v_P(x) > 0 \implies v_{P'} > 0$ z předchozí rovnosti.

$\Leftarrow$: Označme $Q \coloneqq P' \cap F$. $v_{P'}(x) \geq 0, x \in F \implies v_Q(x) \geq 0$. Tedy Q je místo $K(x)$ obsahující x. Víme, že existuje jediné takové místo F/K, protože
$1 = [F : K(x)] \geq \sum_{P: x \in P} v_P(x) \deg(P)$. Takže $P' \subset Q = P \implies P'|P$.

(c) Z předchozího bodu víme, že $v_P(x) = 1$ a $\deg_{F/K}(P) = 1$. Tudíž $e(P'|P) = v_{P'}(x)$. Stejně tak dle prop F.6, kde $K' = K, \deg_{F/K}(P) = 1 \implies f(P'|P) = \deg_{F'/K}(P')$.

(d) Označíme-li $n = [F' : F]$, rozšíření je konečné, jelikož F' je algebraické funkční těleso nad K a $F = K(x)$ a x je transcendentní nad K.

Použijeme-li značení a předpoklady věty F.7 pro naše P obsahující x a předchozí bod. Dostaneme tedy
$[F' : F] = \sum_i v_{P_i}(x) \cdot \deg_{F'/K}(P_i)$

2

Označme $w(x, y) = y^2 - x^3 - ax - b$.

(a) Z předchozího úkolu víme, že pokud w je smooth, tak $F/K(x)$ je separabilní. Také víme, že $F/K(x)$ je konečné. Dále F je jednoduché rozšíření jelikož $F = \{\frac{a+(w)}{b+(w)} | a \in K[x, y], b \in K[x, y] \setminus 0\} \supset \{\frac{a+(w)}{b+(w)} | a \in K[x], b \in K[x] \setminus 0\} \cong K(x)$. Tedy lehce nepřesně můžeme napsat, že $K(x) = K(x + (w)) \implies F = K(x + (w))(y + (w))$. Budeme ale používat zjednodušené značení, jako v předchozím úkolu.

Tedy $[F : K(x)] = 2$, $m_{y,K(x)}(T) = T^2 - x^3 - ax - b$. Kořeny tohoto polynomu jsou $y, -y \in F$. Víme, že y je separabilní nad $K(x)$ tedy $|\mathrm{Hom}(F, \overline{K(x)})| = [F :$

$K(x)] = 2$. Oba tyto homomorfismy permutují kořeny $m_{y,K(x)}$ a oba tyto kořeny jsou v F. Takze je $F/K(x)$ normální a Galoisovo.

(b) Pokud $t = y+\lambda x+\mu$, protíná $C = V_w$ právě ve 2 různých bodech, tak pro dané (x, y) platí $y = -\lambda x-\mu, w(x, y) = 0 \implies w(x, -\lambda x-\mu) = 0$, kde $g(x) = w(x, -\lambda x-\mu) = -x^3+x^2\lambda^2+x(2\lambda\mu-a)+\mu^2-b \in K[x]$. Tento polynom je stupně 3 a dle zadání má jen 2 různé kořeny tedy má násobný kořen $\implies g(x) = -(x - c_1)^2(x - c_2) \in K[x]$.

Dále nevím.

(c) Zjistíme, kdy je $F/K(y)$ normální. $m_{x,K(y)}(T) = -T^3 - aT - b - y^2 \in K(y)[T]$. Víme, že kořen v F je x, polynom tedy vydělíme v F $\frac{m_{x,K(y)}(T)}{T-x} = -T^2-Tx-x^2-a$. Z toho nám vyjde, že další kořeny $m_{x,K(y)}(T)$ tedy jsou $x_{1,2} = \frac{1}{2}(-x\pm\sqrt{-3x^2 - 4a})$. Pokud $x_{1,2} \in F$ tak je $F/K(y)$ Galoisovo.

Zajímá nás tedy kdy $x_{1,2} \notin F$. Speciálně $\sqrt{-3x^2 - 4a} \notin F$. Pokud tedy například $a = 0$, tak $\sqrt{-3x^2 - 4a} = \sqrt{-3}x = \sqrt{2}x$ když $K = \mathbb{Z}_5$. V $\mathbb{Z}_5$ neexistuje $\sqrt{2}$ tedy kořen není v F, takže pokud $a = 0$, tak $F/K(y)$ není normální tedy ani Galoisovo.

3

Označme $w(x, y) = y^2 - x^3 - ax^2 - bx \in K[x, y], a^2 - 4b \neq 0, b \neq 0$.

(a) Takové z nemůže být algebraické nad K. Jelikož $[F' : K] = \infty$. Předpokládejme tedy, že existuje $z \in F' : F' = K(z), z$ transcendentní nad K, tedy $K(z) \cong K(x)$. Víme ale, že $[F' : K(x)] = 2$, tedy $F' \neq K(x) \cong K(z)$.

(b) $s = \frac{b-x^2}{x} = \frac{bx-x^3}{x^2}$ použijme rovnost v F' $x^3 = y^2 - ax^2 - bx \implies$

$$s = \frac{bx - (y^2 - ax^2 - bx)}{x^2} = \frac{-y^2 + ax^2 + 2bx}{x^2} = -\frac{y^2}{x^2} + a + \frac{2b}{x} \implies$$

$$s = -t^2 + a + \frac{2b}{x} \implies s + t^2 - a = \frac{2b}{x} \iff x = \frac{2b}{s + t^2 - a}$$

$$y = t \cdot \frac{2b}{s + t^2 - a} = \frac{y}{x}x$$

Umíme vyjádřit x, y pomocí s, t tedy $K(s, t) = K(x, y)$ kde $w(x, y) = 0$

(c) Porovnáme strany a využijeme rovnosti $y^2 = x^3 + ax^2 + bx$, která platí v F':

$$s^2 = \left(\frac{b - x^2}{x}\right)^2 = \frac{b^2 - 2bx^2 + x^4}{x^2} = x^2 - 2b + \frac{b^2}{x^2}$$

$$t^4 - 2at^2 + a^2 - 4b = \frac{y^4}{x^4} - 2a\frac{y^2}{x^2} + a^2 - 4b = \frac{y^4 - 2ax^2y^2 + a^2x^4 - 4bx^4}{x^4} \implies$$
$$\frac{(x^3 + ax^2 + bx)^2 - 2ax^2(x^3 + ax^2 + bx) + a^2x^2 - 4bx^4}{x^4} = \frac{x^6 - 2bx^4 + b^2x^2}{x^4} = s^2$$

(d) $K(t^2, st) = K(t^2)(st)$. $st \notin K(t^2)$ protože $st = \frac{yb - x^2y}{x^2}$ a monočlen x^2y nemůžeme dostat jako prvek $K(\frac{y^2}{x^2})$. Zároveň $m_{st,K(t^2)}(T) = T^2 - (st)^2$. Je to opravdu min. poly nad $K(t)$ protože výše jsme ukázali, že $s^2 \in K(t^2) \implies (st)^2 = s^2t^2 \in K(t^2)$.

Tedy $z \in K(t^2, st) : z = \frac{f + g \cdot st}{h + j \cdot st}, f, g, h, j \in K(t^2)(\iff f = f'(t^2), \ldots, f' \in K[x]) \implies z = \frac{f'(t^2) + g'(t^2)st}{h'(t^2) + j'(t^2)st} \cdot \frac{h'(t^2) - j'(t^2)st}{h'(t^2) - j'(t^2)st} = \frac{a(t^2) + b(t^2)st}{c(t^2)}$

Pokud tedy existují $f, g, h \in K[x] : t = \frac{f(t^2) + s \cdot g(t^2)}{h(t^2)} \implies$

$$th\left(\frac{y^2}{x^2}\right) = \frac{y}{x}h\left(\frac{y^2}{x^2}\right) = f\left(\frac{y^2}{x^2}\right) + \frac{b - x^2}{x}g\left(\frac{y^2}{x^2}\right)$$

Na levé strance se y vyskytuje v liché mocnině, ale na pravé vždy v sudé, tudíž rovnost nemůže platit.

(e) Víme, že $t \notin K(t^2, st)$. Zároveň ale $F' = K(s, t) = K(t^2, st)(t)$, protože $s = st \cdot t^{-1}$. $m_{t,K(t^2,st)}(T) = T^2 - t^2$, tento polynom má za kořeny $t, -t$ a je ireducibilní v $K(t^2, st)$ protože $t, -t \notin K(t^2, st)$. Tedy $F'/K(t^2, st)$ je tedy jednoduché algebraické rozšíření konečného stupně $[F' : K(t^2, st)] = \deg m_{t,K(t^2,st)} = 2$.