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 $R = O_P$.

Díky charakterizaci valuací na $K(x)$ víme, že místo, které obsahuje P je definováno valuací v_x, pro kterou platí $v_x(a/b) = mult(a) - mult(b), \frac{a}{b} \in K(x)$. Pokud tedy použijeme definici $O_P = \{a \in F : v_x(a) \geq 0\}$. Pak O_P můžeme definovat alternativně jako $O_P = \{\frac{a}{b} | a, b \in K[x], b \neq 0, mult(a) \geq mult(b)\}$

(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 $v_P(x) > 0 \implies v_{P'}(a) > 0$ 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 $P' \supset Q = P \implies P'|P$.

(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
$[F' : F] = \sum_i v_{P_i}(x) \cdot \deg_{F'/K}(P_i)$.

Všimneme si, že prvek $(x)_+ \in \mathrm{Div}(F'/K)$, který je definován jako
$(x)_+ = \sum\limits_{P \in \mathbb{P}_{F'/K} : x \in P} v_P(x) \deg(P)$, odpovídá $[F' : F]$.

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 $|\mathrm{Hom}_K(F, \bar{K}(x))| = [F : K(x)] = 2$. Oba tyto homomorfismy permutují kořeny $m_{y,K(x)}$ a oba tyto kořeny jsou v F. Takže je $F/K(x)$ normální a tedy Galoisovo.

(b) Z minulého semestru víme, že pokud $t = y + \lambda x + \mu$, $\gamma \in V_w(K) \cap V_t(K)$ a $|V_w \cap V_t| > 1$, tak existují body $\delta_1, \delta_2 \in V_w(K) : V_w \cap V_t = \{\gamma, \delta_1, \delta_2\}$ a t je tečnou w v bodě γ právě když pokud $\gamma \in \{\delta_1, \delta_2\}$. V našem případě jsou průsečíky pouze 2, tedy $\delta := \delta_1 = \delta_2$. A máme $V_w \cap V_t = \{\gamma, \delta\}$ a t je tečnou pouze v jednom bodě.

Označme místa příslušná těmto průsečíkům $P_1', P_2' \in \mathbb{P}_{F/K}$. Nechť P_1' je místo příslušné průsečíku, kde je t tečnou. Poté platí $v_{P_1'}(t) \geq 2$ a $v_{P_2'}(t) = 1$.

Označme nyní $P_1 = P_1' \cap K(t), P_2 = P_2' \cap K(t)$. P_1, P_2 jsou prvky $\mathbb{P}_{K(t)/K}$. Ze stejného důvodu, proč existuje jediné místo $K(x)/K$ obsahující x existuje jediné místo $P \in \mathbb{P}_{K(t)/K}$ obsahující t. P_1, P_2 zřejmě z definice obsahují t jelikož P_1', P_2' obsahují t. Tedy $P := P_1 = P_2 \implies P_1' | P$ a $P_2' | P$.

Nyní předpokládejme pro spor, že $F/K(t)$ je Galoisovo. Dle proposition F.15 existuje $\sigma \in \mathrm{Gal}(F|K(t))$ takové, že $\sigma(P_1') = P_2'$. Z definice σ platí $\sigma^{-1}(t) = t$, tedy dle F.9 platí $v_{\sigma(P_1')}(t) = v_{P_2'}(t) = v_{P_1'}(\sigma^{-1}(t)) = v_{P_1'}(t)$ což je spor s valuacemi spočtenými výše. Tedy $F/K(t)$ není Galoisovo.

(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) Víme, že F' lze vyjádřit jako $K(z)$ pro nějaké $z \in F'$ právě když genus F' je roven 0. Zároveň F' je eliptické funkční těleso právě když w je hladké. Eliptické funkční těleso má genus 1. Chceme tedy dokázat, že w je hladké.

$$\frac{\partial w}{\partial x}(x,y) = -3x^2 - 2ax - b$$
$$\frac{\partial w}{\partial y}(x,y) = 2y$$

Spočteme kořeny polynomu $\frac{\partial w}{\partial x}(x,y)$, které jsou $x_{1,2} = \frac{-a \pm \sqrt{a^2-3b}}{3}$. Kanditáti na singularitu jsou tedy body $(x_1, 0), (x_2, 0)$. Ověříme, zda leží na křivce neboli $w(x_1, 0) = x_1(-x_1^2 - ax_1 - b) = 0$ nebo $w(x_2, 0) = 0$. Spočteme to pro případ x_1, pro x_2 to jde obdobně.

Kdy te jedy $x_1 = 0$ nebo $-x_1^2 - ax_1 - b = 0$

$$x_1 = 0 \iff \frac{-a + \sqrt{a^2 - 3b}}{3} = 0 \iff \sqrt{a^2 - 3b} = a \iff b = 0$$
$$-x_1^2 - ax_1 - b = 0 \iff a^2 + a\sqrt{a^2 - 3b} - 6b = 0 \iff$$
$$a^2 - 6b = a\sqrt{a^2 - 3b} \iff a^4 - 12a^2b + 36b^2 = a^4 - 3a^2b \iff$$
$$36b^2 = 8a^2b \iff b = \frac{a^2}{4}$$

Což dle předpokládů nejde. Tedy je w hladké a tedy i F má genus 1 tedy to není jednoduché rozšíření.

(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 $z \in K(t^2, st) : z = f + g \cdot st, f, g \in K(t^2)$ neboli existují $u, v, w, z \in K[x]$: $f = \frac{u(t^2)}{v(t^2)}, g = \frac{w(t^2)}{z(t^2)} \implies z = \frac{u(t^2)}{v(t^2)} + \frac{w(t^2) \cdot st}{z(t^2)}$. Převedeme na společný jmenovatel: $z = \frac{u \cdot z(t^2) + v \cdot w(t^2) \cdot st}{v \cdot z(t^2)}$. Tedy máme požadovaný tvar, jelikož $u \cdot z \in K[x]$ a stejně tak zbylé 2 polynomy.

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

$$t \cdot h\left(\frac{y^2}{x^2}\right) = \frac{y}{x} \cdot h\left(\frac{y^2}{x^2}\right) = f\left(\frac{y^2}{x^2}\right) + \frac{yb - yx^2}{x^2} \cdot g\left(\frac{y^2}{x^2}\right) =$$

$$f\left(\frac{y^2}{x^2}\right) + \frac{yb}{x^2} \cdot g\left(\frac{y^2}{x^2}\right) - y \cdot g\left(\frac{y^2}{x^2}\right)$$

Na levé strance se y vyskytuje v liché mocnině, ale na pravé v liché i sudé, takže musí $f = 0$. Poté máme

$$\frac{y}{x} \cdot h\left(\frac{y^2}{x^2}\right) = \frac{yb}{x^2} \cdot g\left(\frac{y^2}{x^2}\right) - y \cdot g\left(\frac{y^2}{x^2}\right)$$

Obdobně můžeme argumentovat, že na levé straně se nenachází zlomky tvaru $\frac{y^i}{x^j}$: $i \neq j$. t tedy nejde takto vyjádřit.

(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 $[F' : K(t^2, st)] = \deg m_{t,K(t^2,st)} = 2$.