NMMB538 - DÚ5

Jan Oupický

1

1. Použijeme lemma R.1. Využijeme předchozího úkolu, kde $F' = K(D)$. Pokud označíme $y_1 := \frac{x_2^2+(g)}{x_1^2+(g)} = t^2 = u \in K(D), y_2 := \frac{x_2(b-x_1^2)+(g)}{x_1^2+(g)} = st = v \in K(D)$. ϕ dle R.1 existuje pokud y_1 nebo y_2 je transcendentní nad K a $f(y_1, y_2) = 0$. Z předchozího úkolu zřejmě platí, že oba prvky jsou transcendentní nad K. Dále jsme v minulém úkolu také ukázali, že platí $f(y_1, y_2) = f(u, v) \in F' = K(D)$.

2. Dle R.7 platí $\phi = \sigma^*$, kde $\sigma = (\sigma_1, \sigma_2)$, kde $\sigma_1 = y_1, \sigma_2 = y_2$. Zvolíme reprezentanty (y_1, y_2) například jako $r_1 = \frac{x_2^2}{x_1^2}, r_2 = \frac{x_2(b-x_1^2)}{x_1^2}$.

3. Víme, že y_1, y_2 jsou trans. nad K, tedy $\deg(\sigma) < \infty$. Zároveň jsme ukázali, že $K(y_1, y_2) = K(u, v)$ a v minulých úkolech jsme ukázali, že $[F' : K(y_1, y_2)] = 2 \implies$ protože $F' = K(D) \implies [K(D) : K(y_1, y_2)] = 2 = \deg(\sigma)$.

4. Pro přehlednost označme P_∞ ze zadání jako $M_\infty \in \mathbb{P}_{K(C)/K}$. Místo $M_\infty \in \mathbb{P}_{K(C)/K}$ zřejmě obsahuje $x_1^{-2} + (f)$, jelikož $v_\infty(x_1 + (f)) = -2$. Tento prvek se nám pomocí σ^* zobrazí na $\frac{x_1^4+(g)}{x_2^4+(g)} = \frac{x_2^{-4}+(g)}{x_1^{-4}+(g)} = u^{-2} \in \mathrm{Im}(\sigma^*) = F \subset F'$. Z minulého úkolu víme, že jediné místo F/K, co obsahuje u^{-2} je $P_\infty \in \mathbb{P}_{F/K}$, tedy $\sigma^*(M_\infty) = P_\infty$. Dále jsme také ukázali, že pro $P_0' \in \mathbb{P}_{K(D)/K}$ platí $P_0' | P_\infty \implies P_0' | \sigma^*(M_\infty)$.

5. $\Rightarrow$:

   Opět použijeme značení M_α pro místo $K(C)/K$. Zvolme $\rho \in K(C)$. Víme, že platí $v_{M_\alpha}(\rho) > 0 \iff \rho(\alpha) = 0$. Z předpokladů platí obdobně, že $v_{P_\beta'}(\sigma^*(\rho)) > 0 \implies \sigma^*(\rho)(\beta) = 0$. Dle lemma R.8 pokud je $\rho(\sigma(\beta))$ definované, tak platí $\rho(\sigma(\beta)) = \sigma^*(\rho)(\beta) \implies \rho(\sigma(\beta)) = 0 \implies \rho \in M_{\sigma(\beta)}$, $\sigma(\beta) \in C$ tedy musí platit $M_{\sigma(\beta)} = M_\alpha \iff \sigma(\beta) = \alpha$.

   Pokud $\rho(\sigma(\beta))$ není def. tak musí platit $\beta \notin \mathrm{Dom}(\sigma) \implies \beta_1 = 0 \implies \beta_2 = 0$. Případ $\sigma(\beta) \notin \mathrm{Dom}(\rho)$ nenastane, jelikož ρ můžeme brat jako $\frac{x_1-\alpha_1+(f)}{1+(f)}$ nebo $\frac{x_2-\alpha_2+(f)}{1+(f)}$ tedy $\mathrm{Dom}(\rho) = C$. Tedy v případě $\beta = (0, 0)$ máme z 4) $P_0' | P_\infty$.

   Dále by tedy P_0' obsahovalo místo P_α což je spor, protože pokud $\alpha_1 \neq 0$, tak $v_{P_\alpha}(u-\alpha_1+(w_D)) > 0$ a zároveň $v_{P_0'}(u-\alpha_1+(w_D)) = \min\{v_{P_0'}(u+(w_D)), v_{P_0'}(-\alpha_1+(w_D))\} = -2$.

   Pokud $\alpha_1 = 0$ tak $\alpha_2 = 0$ a v minulém úkolu, jsme ukázali, že P_0' neobsahuje P_0.

   $\Leftarrow$:

   Obdobně zvolme $\rho \in M_\alpha \implies \rho(\alpha) = 0$. Z předpokladu víme, že $\beta \in \mathrm{Dom}(\sigma)$, tedy je $\rho(\sigma(\beta))$ definováno, jelikož $\mathrm{Dom}(\rho) = C$. Platí tedy $0 = \rho(\alpha) = \rho(\sigma(\beta)) = \sigma^*(\rho)(\beta)$. Neboli $v_{P_\beta'}(\sigma^*(\rho)) > 0 \implies P_\beta' | \sigma^*(M_\alpha)$.

6. Vidíme, že $D \setminus \{(0, 0)\} = \mathrm{Dom}(r_1) \cap \mathrm{Dom}(r_2)$. Kdyby $\mathrm{Dom}(\sigma) \supset \{(0, 0)\}$, tak by dle 5) $P_0' | P_{(0,0)}$ což nejde. Takže $\mathrm{Dom}(r_1) \cap \mathrm{Dom}(r_2) = \mathrm{Dom}(\sigma)$.

2

Pokud α je kořen polynomu $x^3 + a_4x + a_6$, tak substitucí $x \mapsto x + \alpha$ dostaneme $x^3 + 3\alpha x^2 + (3\alpha^2 + a_4)x + \alpha^3 + a_4\alpha + b$, z definice α platí $\alpha^3 + a_4\alpha + b = 0$, máme tedy polynom $x^3 + 3\alpha x^2 + (3\alpha^2 + a_4)x$.

3

Označme $w_{\tilde{D}}(x, y) = y^2 - x^3 + x - 1$. Kořen $x^3 - x + 1$ v $\mathbb{Z}_5$ je 3. Máme tedy $w_D(x, y) = w_{\tilde{D}}(x + 3, y)$ neboli $w_D(x, y) = y^2 - x^3 - 4x^2 - x$.

Máme tedy $a = 4, b = 1 \implies w_C(x, y) = y^2 - x^3 - 2x^2 - 2x$ a následně $w_{\tilde{C}}(x, y) = w_C(x - \frac{-3}{3}, y) = w_C(x + 1, y) = y^2 - x^3 - 4x$. Dohromady:

$$
\begin{aligned}
w_{\tilde{D}}(x, y) &= y^2 - x^3 + x - 1 \\
w_D(x, y) &= y^2 - x^3 - 4x^2 - x \\
w_C(x, y) &= y^2 - x^3 - 2x^2 - 2x \\
w_{\tilde{C}}(x, y) &= y^2 - x^3 - 4x
\end{aligned}
$$

Z cvičení 1 známe K-rational map $\sigma' : D \to C$, $\deg(\sigma') = 2$. Sestrojíme σ jako složení $\sigma_2 \circ \sigma' \circ \sigma_1 : \tilde{D} \to D \to C \to \tilde{C}$.

Dle R.9 pokud σ_1, σ_2 budou konečného stupně, tak bude i σ. Z prvního cvičení víme, že $\sigma' = \left(\frac{x_2^2 + (w_D)}{x_1^2 + (w_D)}, \frac{x_2(1 - x_1^2) + (w_D)}{x_1^2 + (w_D)}\right)$.

Nyní popíšeme σ_1. Sestrojme $\sigma_1^* : K(D) \to K(\tilde{D})$. Z výše udělané substituce zřejmě:

$$\sigma_1^*(x + (w_D)) = x + 2 + (w_{\tilde{D}})$$

$$\sigma_1^*(y + (w_D)) = y + (w_{\tilde{D}})$$

A následně tedy $\sigma_1 = (x + 2 + (w_{\tilde{D}}), y + (w_{\tilde{D}}))$.

Obdobně pro σ_2: $\sigma_2^* : K(\tilde{C}) \to K(C), w_C(x, y) = w_{\tilde{C}}(x + 4, y) \implies$

$$\sigma_2^*(x + (w_{\tilde{C}})) = x + 4 + (w_C)$$

$$\sigma_2^*(y + (w_{\tilde{C}})) = y + (w_C)$$

$\sigma_2 = (x + 4 + (w_C), y + (w_C))$.

Zřejmě jsou $x + 2 + (w_{\tilde{D}}), y + (w_{\tilde{D}}), x + 4 + (w_C), y + (w_C)$ transcendentní nad K, tedy σ_1, σ_2 jsou konečného stupně. To, že σ' je konečného stupně jsme ukázali v 1). Následně tedy σ je také konečného stupně dle R.9.

Zřejmě $\mathrm{Dom}(\sigma_1) = \tilde{D}$, $\mathrm{Dom}(\sigma_2) = C$.

Z prvního cvičení víme, že $\mathrm{Dom}(\sigma') = D \setminus \{(0, 0)\}$.

Neboli pro $\alpha = (\alpha_1, \alpha_2) \in \mathrm{Dom}(\sigma)$:

$$\sigma(\alpha) = \sigma_2(\sigma'(\sigma_1(\alpha))) = \left(\frac{\alpha_2^2}{(\alpha_1 + 2)^2} + 4, \frac{\alpha_2(1 - (\alpha_1 + 2)^2)}{(\alpha_1 + 2)^2}\right)$$

4

$\mathbb{Z}_5$-racionální body $\tilde{D}$ jsou:

$$(0,1),(0,4),(1,1),(1,4),(3,0),(4,1),(4,4)$$

$\mathbb{Z}_5$-racionální body $\tilde{C}$ jsou:

$$(0,0),(1,0),(2,1),(2,4),(3,2),(3,3),(4,0)$$

Jelikož ve cvičení 3 jsme určili, že $\mathrm{Dom}(\sigma_1) = \tilde{D}$, $\mathrm{Dom}(\sigma_2) = \tilde{C}$ a $\mathrm{Dom}(\sigma') = D \setminus \{(0,0)\}$. Prvek $\tilde{D}$, který nebude prvkem $\mathrm{Dom}(\sigma)$ je ten, co se pomocí σ_1 zobrazí na $(0,0)$. Z definice to je pouze bod $(3,0)$, jelikož $\sigma_1((3,0)) = (3+2,0) = (0,0)$. Jiný takový bod není.

Zřejmě $\tilde{D} \supset \mathrm{Dom}(\sigma) \implies \tilde{D} \cap \mathrm{Dom}(\sigma) = \mathrm{Dom}(\sigma)$ a $\mathrm{Dom}(\sigma) = \tilde{D} \setminus \{(3,0)\}$.

Spočteme tedy obrazy prvků $\{(0,1),(0,4),(1,1),(1,4),(4,1),(4,4)\}$:

$$\begin{aligned}
\sigma((0,1)) &= \left(\frac{1^2}{(0+2)^2}+4, \frac{1(1-(0+2)^2)}{(0+2)^2}\right) = (3,3)\\
\sigma((0,4)) &= \left(\frac{4^2}{(0+2)^2}+4, \frac{4(1-(0+2)^2)}{(0+2)^2}\right) = (3,2)\\
\sigma((1,1)) &= \left(\frac{1^2}{(1+2)^2}+4, \frac{1(1-(1+2)^2)}{(1+2)^2}\right) = (3,3)\\
\sigma((1,4)) &= \left(\frac{4^2}{(1+2)^2}+4, \frac{4(1-(1+2)^2)}{(1+2)^2}\right) = (3,2)\\
\sigma((4,1)) &= \left(\frac{1^2}{(4+2)^2}+4, \frac{1(1-(4+2)^2)}{(4+2)^2}\right) = (0,0)\\
\sigma((4,4)) &= \left(\frac{4^2}{(4+2)^2}+4, \frac{4(1-(4+2)^2)}{(4+2)^2}\right) = (0,0)
\end{aligned}$$