# NMMB538 - DÚ7

Jan Oupický

## 1

Z definice [2] víme, že $\forall \alpha \in D : [2](\alpha) = \alpha \oplus \alpha$. Vyjádříme tedy vzorec pro výpočet bodu $\alpha \oplus \alpha \in D$ křivky $V_w$.

Nejprve vyjádříme racionální funkci. Použijeme vzorec pro součet bodů a to, že pro body $(\alpha_1, \alpha_2) \in D$ platí $\alpha_2^2 = \alpha_1^3 + a\alpha_1^2 + b\alpha$. $\gamma$ bude značit reprezentanta rac. zobrazení $\gamma(\alpha) = [2](\alpha), \gamma = (\gamma_1, \gamma_2), \gamma_i \in K(x_1, x_2)$.

Vyjádříme nejprve $\gamma_1(x_1, x_2)$. Ze vzorců pro součet stejného bodu vyjde, že:

$$\gamma_1(x_1, x_2) = \frac{-8x_1x_2^2 - 4ax_2^2 + 9x_1^4 + 12ax_1^3 + 6bx_1^2 + 4a^2x_1^2 + 4abx_1 + b^2}{4x_2^2}$$

zasubstituujeme za $x_2^2$ v čitateli a vyjde:

$$\gamma_1(x_1, x_2) = \frac{x_1^4 - 2bx_1^2 + b^2}{4x_2^2} = \left(\frac{x_1^2 - b}{2x_2}\right)^2$$

Nyní spočteme $\gamma_2(x_1, x_2)$:

$$\gamma_2(x_1, x_2) = \frac{3x_1^3 + 2ax_1^2 + bx_1}{2x_2} - \frac{3x_1^2 + 2ax_1 + b}{2x_2} \cdot \frac{x_1^4 - 2bx_1^2 + b^2}{4x_2^2} - x_2$$

Převedení na společného jmenovatele a použití substituce za $x_2^2$ v čitateli:

$$\gamma_2(x_1, x_2) = \frac{x_1^6 + 2ax_1^5 + 5bx_1^4 - 5b^2x_1^2 - 2ab^2x_1 - b^3}{8x_2^3}$$

Máme tedy reprezentanty $K-$racionálního zobrazení $[2] : D \to D$, kde
$[2] = (\gamma_1 + (w), \gamma_2 + (w))$. Sestrojíme nyní projektivní reprezentaci zobrazení [2] jako v předchozím úkolu pomocí lemma M.3.

$$\gamma_i = \frac{a_i}{b_i}, a_i, b_i \in K[x_1, x_2], b_i \neq 0$$

$$A_1' = \widehat{a_1}X_3^2 = (X_1^4 - 2bX_1^2X_3^2 + b^2X_3^4)X_3^2$$

$$A_2' = \widehat{a_2}X_3^3 = (X_1^6 + 2aX_1^5X_3 + 5bX_1^4X_3^2 - 5b^2X_1^2X_3^4 - 2ab^2X_1X_3^5 - b^3X_3^6)X_3^3$$

$$B_1' = 4X_2^2X_3^4$$

$$B_2' = 8X_2^3X_3^6$$

$$\Longrightarrow$$

$$(A_1 : A_2 : A_3) = (A_1'B_2' : A_2'B_1' : B_1'B_2')$$

dosazení a zkrácení:

$$(A_1 : A_2 : A_3) = (2(X_1^4 - 2bX_1^2X_3^2 + b^2X_3^4)X_2X_3 : \widehat{a_2} : 4X_2^3X_3^3)$$

## 2

Pro reprezentaci $[2] = (A_1 : A_2 : A_3)$ výše platí $\deg_{X_2}(A_1) = 1, \deg_{X_2}(A_2) = 0$. V posledním členu $A_3$ nahradíme $X_2^2X_3$ za $X_1^3 + aX_1^2X_3 + bX_1X_3^2$. Máme tedy novou

reprezentaci, která splňuje podmínky:

$$(A_1' : A_2' : A_3') = (2(X_1^4 - 2bX_1^2X_3^2 + b^2X_3^4)X_2X_3 : \widehat{a_2} : 4X_2X_3^2(X_1^3 + aX_1^2X_3 + bX_1X_3^2))$$

Pro reprezentaci $[2] = (B_1 : B_2 : B_3), \deg_{X_1}(B_i) \leq 2$ využijeme substituci $X_1^3 = X_2^2X_3 - aX_1^2X_3 - bX_1X_3^2$. Každá substituce sníží stupeň (v $X_1$) polynomu o 1. Zřejmě se dostaneme do tvaru, kde $\deg_{X_1}(B_i) \leq 2$. Substituce do 1. členu:

$$B_1 = 2X_2X_3^2((a^2 - 3b)X_1^2X_3 + X_1X_2^2 + abX_1X_3^2 - aX_2^2X_3 + b^2X_3^3)$$

$B_2$ získáme opakovanou substitucí za $X_1^3$. Polynom je tvaru:

$$B_2 = -X_3^2(-X_2^4 + X_2^2X_3f_1(X_1, X_2, X_3) + X_3^2f_2(X_1, X_2, X_3)), \deg_{X_1}(f_i) = i$$

# 3

Bod $\infty = (0 : 1 : 0) \in D$. Zřejmě $A_1', A_3'(\infty) = 0$ (násobky $X_3$) a $A_2'(\infty) = 0$ (jsou tam jen monočleny $X_1^iX_3^j$). Obdobně $B_i(\infty) = 0$ (všechno to jsou násobky $X_3$).

Pokud ale definujeme $B_i' = \frac{B_i}{X_3^2}$. Poté $B_2'(\infty) = 1$.

# 4

Označme

$$\rho_1 = \left(\frac{x_1^2 - b}{2x_2}\right)^2$$

$$\rho_2 = \frac{x_1^6 + 2ax_1^5 + 5bx_1^4 - 5b^2x_1^2 - 2ab^2x_1 - b^3}{8x_2^3}$$

Všimneme si, že platí:

$$\rho_1 = \frac{v^2}{4u^2} = \left(\frac{v}{2u}\right)^2$$

Kde $u = t^2, v = st$ z minulých úloh. Obdobně také $\rho_2$ jde vyjádřit pomocí $u, v$.

$$\rho_2 = \rho_2\frac{x_1^2}{x_1^2} = \frac{(b - x_1^2)(-1)(x_1^6 + 2ax_1^5 + 6bx_1^4 + 2abx_1^3 + b^2x_1^2)}{8x_1^2x_2^3} =$$

$$\frac{v}{8}\frac{-(x_1^6 + 2ax_1^5 + 6bx_1^4 + 2abx_1^3 + b^2x_1^2)}{x_2^3}\frac{x_2}{x_2} = \frac{v}{8}\frac{-((x_1^3 + ax_1^2 + bx_1)^2 - a^2x_1^4 + 4bx_1^4)}{x_2^4} =$$

$$\frac{v}{8}\frac{(-x_2^4 + a^2x_1^4 - 4bx_1^4)}{x_2^4}\frac{x_1^4}{x_1^4} = \frac{v}{8}\frac{a^2 - 4b - \frac{x_2^4}{x_1^4}}{\frac{x_2^4}{x_1^4}} = \frac{v(a^2 - 4b - u^2)}{u^2}$$

Neboli $\mathrm{Im}([2]^*) = K(\frac{v^2}{4u^2}, \frac{v(a^2-4b-u^2)}{u^2})$. Ukažeme, že $[K(u, v) : \mathrm{Im}([2]^*)] = 2$.

Zvolme $d = \sqrt{\frac{v^2}{u^2}} = \frac{v}{u}$. Ukážeme, že $K(\rho_1, \rho_2, d) = K(u, v)$. Poté zřejmě $min_{d,K(\rho_1,\rho_2)}(T) = T^2 - \rho_1$, což je ireducibilní a separabilní polynom nad $K(\rho_1, \rho_2)$ (kořeny $\pm\rho_1$).

$$\rho_2 d^{-1} = \frac{v(a^2-4b-u^2)}{u^2}\frac{u}{v} = \frac{a^2u-4bu-u^3}{u^2} = \frac{a^2u-4bu-(v^2+2au^2-a^2u+4bu)}{u^2} =$$
$$\frac{-v^2-2au^2+2a^2u-8bu}{u^2} = -\frac{v^2}{u^2} - 2a + \frac{2a^2-8b}{u} \implies$$
$$\rho_2 d^{-1} + d^2 + 2a = \frac{2a^2-8b}{u} \implies u = \frac{2a^2-8b}{\rho_2 d^{-1} + d^2 + 2a} \in K(\rho_1, \rho_2, d)$$
$$d = \frac{v}{u} \implies du = v \implies v \in K(\rho_1, \rho_2, d)$$

V úpravách jsme použili rovnost $v^2 = u^3 - 2au^2 + u(a^2 - 4b)$, kterou jsme dokázali v úkolu 4.

Tedy $K(u,v)/\mathrm{Im}([2]^*)$ je separabilní a stupně 2. Z minulých úkolů víme, že $K(D)/K(u,v)$ je galoisovo a stupně 2. Z toho vyplývá, že $K(D)/\mathrm{Im}([2]^*)$ je stupně $2 \cdot 2$ a je separabilní. Ekvivalentně [2] je separabilní isogeny a $\deg([2]) = 4$.

V minulých úlohách jsme dokázali, že $D$ je smooth, tedy dle X.13 $\mathrm{Im}[2] = D$.

Z definice isogeny víme, že $[2](\infty_D) = \infty_D$. Pro zjištění jádra chceme vědět, jaké body $\alpha \in D$ se zobrazí [2] na $\infty$ neboli pro jaké body platí $\rho_1 = \frac{a_1}{b_1}, \rho_2 = \frac{a_2}{b_2}$ platí $b_i(\alpha) = 0$. Vidíme, že $\alpha_2 = 0$. $D$ je smooth, tedy máme 3 různé body $P_0, P_1, P_2 = (0,0), (\alpha_1, 0), (\beta_1, 0) \in D$, kde 2. souřadnice je 0.

Dle T.15 ($K(D)/\mathrm{Im}([2]^*)$ je separabilní, tedy $[K(D)/\mathrm{Im}([2]^*)]_s = [K(D)/\mathrm{Im}([2]^*)] = 4$), tedy $|\mathrm{Ker}([2])| = 4$. Našli jsme 4 různé body a tedy $\mathrm{Ker}([2]) = \{\infty_D, P_0, P_1, P_2\}$.

# 5

Zadání splňuje předpoklady T.17, tedy $\mathrm{Gal}(K(D)|\mathrm{Im}([2]^*)) = \{t^*_\alpha | \alpha \in \{\infty, P_1, P_2, P_3\}\}$.