

## 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:

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

zasubstituuje 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  $[2] : D \rightarrow D$ , kde  $[2] = (\gamma_1 + (w), \gamma_2 + (w))$ . Sestrojíme nyní projektivní reprezentaci zobrazení  $[2]$  jako v předchozím úkolu pomocí lemma M.3.

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

$$A'_1 = \widehat{a}_1 X_3^2 = (X_1^4 - 2bX_1^2X_3^2 + b^2X_3^4)X_3^2$$

$$A'_2 = \widehat{a}_2 X_3^3 = (X_1^6 + 2aX_1^5X_3 + 5bX_1^4X_3^2 - 5b^2X_1^2X_3^4 - 2ab^2X_1X_3^5 - b^3X_3^6)X_3^3$$

$$B'_1 = 4X_2^2X_3^4$$

$$B'_2 = 8X_2^3X_3^6$$

$\implies$

$$(A_1 : A_2 : A_3) = (A'_1B'_2 : A'_2B'_1 : B'_1B'_2)$$

dosazení a zkrácení:

$$(A_1 : A_2 : A_3) = (2(X_1^4 - 2bX_1^2X_3^2 + b^2X_3^4)X_2X_3 : \widehat{a}_2 : 8X_2^3X_3^3)$$

## 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:

$$(A'_1 : A'_2 : A'_3) = (2(X_1^4 - 2bX_1^2X_3^2 + b^2X_3^4)X_2X_3 : \widehat{a}_2 : 8X_2X_3^2(X_1^3 + aX_1^2X_3 + bX_1X_3^2))$$

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:

$$\begin{aligned} B_2 &= -X_3^2(-X_2^4 + X_2^2X_3f_1(X_1, X_2, X_3) + X_3^2f_2(X_1, X_2, X_3)), \deg_{X_1}(f_i) = i \text{ kde} \\ f_1(X_1, X_2, X_3) &= a^2X_1 + a^3(-X_3) + 5abX_3 - 3bX_1 \\ f_2(X_1, X_2, X_3) &= -6a^2bX_1^2 + a^3bX_1X_3 + a^4X_1^2 - 3ab^2X_1X_3 + b^2(bX_3^2 + 9X_1^2) \end{aligned}$$

### 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  $B'_2(\infty) = 1$ .

Pro zbylé body nyní můžeme uvažovat  $X_3 = 1$ . Pokud 2. souřadnice bodu z  $D$  není 0, tak  $A'_3(\alpha) \neq 0$  pro každý takový bod  $\alpha \in D$  (protože  $X_2 \neq 0$  a  $X_3 = 1$ ).

Zbývají 3 body  $D$  tvaru  $\alpha = (\alpha_1, 0) \in D$ . Možná  $\alpha_1$  jsou  $\{0, r_1, r_2\}$ , kde  $r_i, i = 1, 2$  jsou kořeny  $x^2 + ax + b$ . Jelikož  $X_2 = 0$ , tak jsou relevantní jen polynomy  $A'_2$  a  $B_2$  (ostatní jsou 0).

Pro bod  $(0, 0)$  se to redukuje na zda  $f_2(0, 0, 1) = 0$ ? Po dosazení platí  $f_2(0, 0, 1) = b^3$  neboli  $B'_2(\alpha) \neq 0$ .

Polynom  $f_2(x, 0, 1) = x^2(a^4 - 6a^2 + 9b^2) + x(a^3b - 3ab^2) + b^3$ . Tento polynom nemá žádné společné kořeny s polynomem  $x^2 + ax + b$ . Takže  $f_2(r_i, 0, 1) \neq 0, i = 1, 2 \implies B'_2((r_i : 0 : 1)) \neq 0, i = 1, 2$ .

### 4

Označme

$$\begin{aligned} \rho_1 &= \left( \frac{x_1^2 - b}{2x_2} \right)^2 \\ \rho_2 &= \frac{x_1^6 + 2ax_1^5 + 5bx_1^4 - 5b^2x_1^2 - 2ab^2x_1 - b^3}{8x_2^3} \end{aligned}$$

Všimneme si, že platí:

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

Kde  $u = t^2, v = st, t = \frac{x_2}{x_1}, s = \frac{b-x_1^2}{x_1}$  z minulých úloh. Poněkud nepřesně zde ztotožňujeme  $x_1 + (w) = x_1, x_2 = x_2 + (w)$ . Obdobně také  $\rho_2$  jde vyjádřit pomocí  $u, v$ .

$$\begin{aligned}\rho_2 &= \rho_2 \frac{x_1^2}{x_1^2} = \frac{(b - x_1^2)(-1)(x_1^6 + 2ax_1^5 + 6bx_1^4 + 2abx_1^3 + b^2x_1^2)}{8x_1^2x_2^3} = \\ &= \frac{v - (x_1^6 + 2ax_1^5 + 6bx_1^4 + 2abx_1^3 + b^2x_1^2) \frac{x_2}{x_2}}{8 \frac{x_2^3}{x_2^2}} = \frac{v - ((x_1^3 + ax_1^2 + bx_1)^2 - a^2x_1^4 + 4bx_1^4)}{8 \frac{x_2^4}{x_2^4}} = \\ &= \frac{v(-x_2^4 + a^2x_1^4 - 4bx_1^4) \frac{x_1^4}{x_1^4}}{8 \frac{x_2^4}{x_2^4} \frac{x_1^4}{x_1^4}} = \frac{v(a^2 - 4b - \frac{x_2^4}{x_1^4})}{8 \frac{x_2^4}{x_1^4}} = \frac{v(a^2 - 4b - u^2)}{8u^2}\end{aligned}$$

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

Zvolme  $d = \sqrt{\frac{v^2}{u^2}} = \frac{v}{u}$ . Ukažeme, že  $K(\rho_1, \rho_2, d) = K(u, v)$ . Poté zřejmě  $\min_{d, K(\rho_1, \rho_2)}(T) = T^2 - 4\rho_1$ , což je ireducibilní a separabilní polynom nad  $K(\rho_1, \rho_2)$  (kořeny  $\pm d$ ).

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

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

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

Z definice isogeny víme, že  $[2](\infty) = \infty$ . 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 musí  $\alpha_2 = 0$ .  $D$  je smooth, tedy máme 3 různé body  $P_0, P_1, P_2 = (0, 0), (r_1, 0), (r_2, 0) \in D$ , kde 2. souřadnice je 0.

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

Přesně jsme neukázali, že  $d \notin K(\rho_1, \rho_2)$ . Pokud by to platilo, tak  $\deg([2]) = 2$  a  $[2]$  separabilní. Nalezli jsme ale 4 různé body, které jsou prvky  $\text{Ker}([2])$ , tedy spor s T.15.

## 5

Zadání splňuje předpoklady T.17, tedy  $\text{Gal}(K(D)|\text{Im}([2]^*)) = \{t_\alpha^* | \alpha \in \{\infty, P_1, P_2, P_3\}\}$ . Z definice  $t_\infty(\alpha) = \infty \oplus \alpha = \alpha$ , neboli  $t_\infty = [1] \iff t_\infty^* = (x, y), (X : Y : Z)$ .

Dále  $P_1 = (0, 0) \implies t_{(0,0)}(\alpha) = (0, 0) \oplus \alpha$ .

Spočteme tedy afinní reprezentanty  $t_{(0,0)}^*$ , které jsou  $t_{(0,0)}^* = \left(\frac{-b}{x_1}, \frac{-bx_2}{x_1^2}\right)$ . Z toho dostaneme klasickým způsobem projektivní reprezentanty:

$$(-bX_1X_3 : -bX_2X_3 : X_1^2)$$

Zbylé 2 translace korespondují s body  $P_2, P_3$ , kde  $P_2 = (r_1, 0), P_3 = (r_2, 0)$  pro  $r_1, r_2$  platí  $r_i^2 + ar_i + b = 0$  (jsou to kořeny  $x^2 + ax + b$ ). Opět z definice  $t_{(r_1, 0)}(\alpha) = (r_1, 0) \oplus \alpha$ . Pak jsou afinní reprezentanti  $t_{(r_1, 0)}^*$ :

$$\left( \frac{r_1(a + r_1 + x_1)}{x_1 - r_1}, \frac{x_1^2 x_2 - 2r_1 x_1 x_2 + b x_2}{(x_1 - r_1)^2} \right)$$

a projektivní:

$$(r_1((a + r_1)X_3 + X_1)(X_1 - r_1 X_3)X_3 : X_1^2 X_2 - 2r_1 X_1 X_2 X_3 + b X_2 X_3^2 : (X_1 - r_1 X_3)^2 X_3)$$

Při úpravě 2. afinního reprezentanta jsme použili  $x_2^2 = x_1^3 + ax_1^2 + bx_1$  a  $r_1^2 + ar_1 = -b$ .

Pro  $P_3 = (r_2, 0)$ ,  $t_{(r_2, 0)}(\alpha) = (r_2, 0) \oplus \alpha$  můžeme provést stejný postup. Reprezentanti  $t_{(r_2, 0)}^*$  jsou tedy:

$$\left( \frac{r_2(a + r_2 + x_1)}{x_1 - r_2}, \frac{x_1^2 x_2 - 2r_2 x_1 x_2 + b x_2}{(x_1 - r_2)^2} \right)$$

a projektivní:

$$(r_2((a + r_2)X_3 + X_1)(X_1 - r_2 X_3)X_3 : X_1^2 X_2 - 2r_2 X_1 X_2 X_3 + b X_2 X_3^2 : (X_1 - r_2 X_3)^2 X_3)$$