NMMB538 - DÚ4

Jan Oupický

1

Předpokládejme $a^2 \neq 4b, b \neq 0$ viz předchozí úkol. Definujme polynom $w(x,y) = y^2 - x^3 + 2ax^2 - x(a^2 - 4b)$ neboli máme dokázat, že F je dáno $w(u,v) = 0$. Tento polynom je Weirstrassův, tedy víme, že je ireducibilní. Chceme ověřit, že v F platí $w(u,v) = 0$.

Z minulého úkolu víme ($t = \frac{y}{x}, s = \frac{b-x^2}{x}$), že $K(t,s) = F' \supset F = K(t^2, st) = K(u,v)$. Dále víme, že platí rovnost $s^2 = t^4 - 2at^2 + (a^2 - 4b)$ v F'. Tedy $u = t^2, v = st \implies s = \frac{v}{t}$ v F'. Dosadíme-li $\frac{v^2}{t^2} = \frac{v^2}{u} = u^2 - 2au + (a^2 - 4b) \implies v^2 = u^3 - 2au^2 + u(a^2 - 4b)$. Daná rovnost platí v F', ale obsahuje jen prvky z F tedy platí i v F. Tudíž platí $w(u,v) = 0$ v F.

Ukážeme, že $w(x,y)$ je hladký, tedy genus F je 1.

$$\frac{\partial w}{\partial x}(x,y) = -3x^2 + 4ax - a^2 + 4b$$
$$\frac{\partial w}{\partial y}(x,y) = 2y$$

Spočteme řešení $-3x^2 + 4ax - a^2 + 4b = 0$. Máme řešení $x_{1,2} = \frac{1}{3}(2a \pm \sqrt{a^2 + 12b})$. Tedy pokud existuje singularita, tak je v bodě $(x_1, 0)$ nebo $(x_2, 0)$. Ověříme opět, zda pro tyto body platí také $w(x,y) = 0$.

Pro případ $w(x_1, 0) = 0$: zajímá tedy kdy $-x_1^3 + 2ax_1^2 - x_1(a^2 - 4b) = x_1(-x_1^2 + 2ax_1 - (a^2 - 4b)) = 0$. $x_1 = 0 \iff 2a - \sqrt{a^2 + 12b} = 0 \iff 4b = a^2$ což nejde z předpokladů. Zbývá tedy $-x_1^2 + 2ax_1 - (a^2 - 4b) = 0$. Pokud dosadíme za x_1, tak dostaneme $\frac{-2}{9}\left(a\sqrt{a^2 + 12b} + a^2 - 12b\right) = 0$, kde řešení musí splňovat $b = 0$ nebo $4b = a^2$. $w(x,y)$ je tedy smooth, tedy je F eliptické funkční těleso, tedy je rodu 1.

Víme, že F'/F je konečné jednoduché algebraické rozšíření. V předchozím úkolu jsme ukázali $K(t,s) \supset K(t^2, st)$ a $K(t,s) = K(t^2, st)(t)$ a že $m_{t,F}(T) = T^2 - t^2$. Tento polynom je ireducibilní nad F a jeho kořeny jsou $t, -t \in F'$. Tedy je t separabilní nad F a $F' = F(t)$, tedy F'/F je separabilní a zároveň $-t \in F'$ tedy je F'/F normální $\implies$ Galoisovo.

2

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

Máme definováno, že $F' = K(x,y)$ kde $w'(x,y) = 0$ a $F' = K(u,v)$, kde $w(u,v) = 0$. Oba polynomy w', w jsou Weirstrassovy a pro funkční tělesa dáná těmito polynomy víme, že platí

$$P'_\infty \in \mathbb{P}_{F'/K} : v_{P'_\infty}(x) = -2, v_{P'_\infty}(y) = -3$$
$$P_\infty \in \mathbb{P}_{F/K} : v_{P_\infty}(u) = -2, v_{P_\infty}(v) = -3$$

Dále spočteme valuace pro x, y, u, v v místech $P'_{(0,0)}, P_{(0,0)}$. y, v nejsou tečny v $(0,0)$ a $(0,0) \in V_w \cap V_{w'}$, takže jejich valuace je 1. Pro x, u to vychází stejně, jelikož oba polynomy mají $mult_y = 2$.

$$P'_{(0,0)} \in \mathbb{P}_{F'/K} : v_{P'_{(0,0)}}(x) = 2, v_{P'_{(0,0)}}(y) = 1$$
$$P_{(0,0)} \in \mathbb{P}_{F/K} : v_{P_{(0,0)}}(u) = 2, v_{P_{(0,0)}}(v) = 1$$

(a) Dle definice $\mathrm{div}_{F'/K}(x) = \sum_{P \in \mathbb{P}_{F'/K}} v_P(x)P$. Víme, že jediná místa, kde $v_P(x) \neq 0$ jsou $P'_{(0,0)}$ a P'_∞. Takže $\mathrm{div}_{F'/K}(x) = v'_0(x)P'_{(0,0)} + v'_\infty(x)P'_\infty = 2P'_{(0,0)} - 2P'_\infty$.
Obdobně pro zbytek:

$$\mathrm{div}_{F'/K}(y) = v'_0(y)P'_{(0,0)} + v'_\infty(y)P'_\infty = 1P'_{(0,0)} - 3P'_\infty$$
$$\mathrm{div}_{F/K}(u) = v_0(u)P_{(0,0)} + v_\infty(u)P_\infty = 2P_{(0,0)} - 2P_\infty$$
$$\mathrm{div}_{F/K}(v) = v_0(v)P_{(0,0)} + v_\infty(v)P_\infty = 1P_{(0,0)} - 3P_\infty$$

(b) Použijeme The Fundamental Equality (F.7) a Proposition F.6. Uvažujme nejprve $P = P_\infty$. Víme, že $[F' : F] = 2$. Dále dle proposition F.6 pro taková místa P' platí $\deg_{F'/K}(P')[K : K] = f(P'|P)\deg_{F/K}(P)$. Víme ale že pro naše $P = P_\infty, P_{0,0}$: $\deg_{F/K}(P) = 1$. Tedy $f(P'|P) = \deg_{F'/K}(P')$. Dle F.7 tedy máme 3 možnosti:

(a) Existují právě 2 místa $P' \in \mathbb{P}_{F'/K} : P'|P, \deg_{F'/K}(P') = 1$ a platí $e(P'|P) = 1 = f(P'|P)$.
(b) Existuje jedno místo $P' \in \mathbb{P}_{F'/K} : P'|P, \deg_{F'/K}(P') = 1$ a platí $e(P'|P) = 2$ a $f(P'|P) = 1$.
(c) Existuje jedno místo $P' \in \mathbb{P}_{F'/K} : P'|P, \deg_{F'/K}(P') = 2$ a platí $e(P'|P) = 1$ a $f(P'|P) = 2$.

Uvažujme nyní případ $P = P_\infty$. Víme, že $v_P(u) = -2 \implies u^{-2} \in P$. Spočteme $v'_\infty(u) = v'_\infty(\frac{y^2}{x^2}) = 2v'_\infty(y) - 2v'_\infty(x) = 2 \cdot (-3) - 2 \cdot (-2) = -2 \implies u^{-2} \in P'_\infty$.

Víme, že $P'_\infty \cap F$ je místo F/K a toto místo obsahuje u^{-2}. P_∞ je jediné místo F/K co obsahuje u^{-2}. Nezbývá tedy než $P'_\infty \cap F = P_\infty \implies P'_\infty | P_\infty$.

Obdobně $v'_0(u) = v'_0(\frac{y^2}{x^2}) = 2v'_0(y) - 2v'_0(x) = 2 \cdot 1 - 2 \cdot 2 = -2 \implies u^{-2} \in P'_{(0,0)}$. Stejně jako výše tedy platí $P'_{(0,0)} \cap F = P_\infty \implies P'_{(0,0)} | P_\infty$.

Pro $P = P_\infty$ tedy máme 2 různá místa F'/K co ho obsahují $(P'_\infty, P'_{(0,0)})$. Platí možnost a) $\implies e(P'_\infty|P) = e(P'_{(0,0)}|P) = 1$ a $f(P'_\infty|P) = f(P'_{(0,0)}|P) = 1$

Uvažujme nyní $P = P_{(0,0)}$. Víme, že místo $P' \in \mathbb{P}_{F'/K} : P'|P$ nemůže už být P'_∞ ani $P'_{(0,0)}$ jinak by $P_{(0,0)} = P' \cap F = P_\infty \implies P_\infty = P_{(0,0)} \implies$ spor.

Chceme místo P', pro které platí $v_{P'}(u) \geq 2$, protože $P'|P \implies v_{P'}(u) \geq v_P(u) = 2$. Platí $v_{P'}(u) = v'_P(\frac{y^2}{x^2}) = 2(v_{P'}(y) - v_{P'}(x)) \geq 2 \iff v_{P'}(y) - v_{P'}(x) \geq 1$. Rozebereme možné hodnoty $v_{P'}(\cdot)$.

Pokud $v_{P'}(x) < 0 \implies P' = P'_\infty \implies$ spor. Pokud $v_{P'}(x) > 0, v_{P'}(y) > 0 \implies P' = P'_{(0,0)} \implies$ spor. Zbývá tedy $v_{P'}(x) = 0$ nebo $v_{P'}(y) = 0$. Druhá možnost nemůže nastat jelikož by neplatilo $v_{P'}(y) - v_{P'}(x) \geq 1$. Hledáme tedy místo F'/K, kde $v_{P'}(x) = 0, v_{P'}(y) \geq 1$.

Chceme tedy najít body $(x', 0) \in V_{w'} \implies x(x^2 + ax + b) = 0$. Pokud $x = 0$, tak máme místo $P'_{(0,0)}$, které nemůžeme použít. Chceme tedy místa příslušná zbylým kořenům. Řešení kvadratické rovnice jsou $x_{1,2} = \frac{1}{2}(-a \pm \sqrt{a^2 - 4b})$. Z přepokladů to pod odmocninou není 0, tedy máme vždy 2 kořeny za předpokladu že existuje daná odmocnina v K.

Označme místa příslušná těmto bodům $(x_1, 0), (x_2, 0) \in V_{w'}$ jako P'_1, P'_2. Máme tedy 2 různá místa stupně 1 t.ž. $v_{P'}(y) \geq 1, v_{P'}(x) = 0 \implies v_{P'}(u) \geq 2$ (jelikož dále $e(P'|P) = 1 \implies v_{P'}(u) = 2$). Tedy daná místa obsahují $P_{(0,0)}$ a platí $e(P'|P) = f(P'|P) = 1$.

Pokud neexistuje $\sqrt{a^2 - 4b}$. Tak neexistuje jiné místo stupně 1 obsahující y. Tedy zbývá možnost P' je jediné místo obsahující $P_{(0,0)}$, P' je stupně 2. Dále se nebudeme tímto případem zabývat.

(c) Pro přehlednost označme $P'_0 \coloneqq P'_{(0,0)}, P_0 \coloneqq P_{(0,0)}$. Dle b) tedy $P'_0, P'_\infty | P_\infty$ a $P'_1, P'_2 | P_0$. Víme, že $\mathrm{div}_{F/K}(u) = 2P_0 - 2P_\infty$. Dále jsme zjistili, že jediná místa $P' \in \mathbb{P}_{F'/K}$, kde $v_{P'}(u) < 0$ jsou P'_0 a P'_∞. Kdyby totiž existovalo jiné místo F'/K t.ž. $v_{P'}(u) < 0 \implies P' \cap F = P \in \mathbb{P}_{F/K}$ neboli místo t.ž. $v_P(u) < 0$ což musí být P_∞ a jiná místa co ho dělí už nejsou, tedy spor. Stejně tak jiná místa $P' \in \mathbb{P}_{F'/K} : v_{P'}(u) > 0$ než P'_1, P'_2 nejsou.

Z toho plyne $\mathrm{div}_{F'/K}(u) = 2P'_1 + 2P'_2 - 2P'_0 - 2P'_\infty$.

Spočteme $\mathrm{Con}_{F'/F}(\mathrm{div}_{F/K}(u)) = 2(\sum\limits_{P'|P_0} 1 \cdot P') - 2(\sum\limits_{P'|P_\infty} 1 \cdot P') = 2(P'_1 + P'_2) - 2(P'_0 + P'_\infty)$.

Rovnost tedy platí.

(d) Máme $\mathrm{Con}_{F'/F}(P_\infty) = \sum\limits_{P'|P} 1 \cdot P' = P'_0 + P'_\infty$. Potom $\deg_{F'/K}(P'_0 + P'_\infty) = \deg_{F'/K}(P'_0) + \deg_{F'/K}(P'_\infty) = 1 + 1 = 2$. První deg značí stupeň divisoru a druhý deg je stupeň místa.

Na druhé straně $\deg_{F/K} P_\infty = 1$ a $[F' : F] = 2$ tedy rovnost platí.

(e) $\mathrm{div}_{F'/K}(x) = 2P'_0 - 2P'_\infty$. $P'_0 \cap F = P_\infty = P'_\infty \cap F$ a $f(P'_\infty|P_\infty) = 1 = f(P'_0|P_\infty)$ jak jsme zjistili výše. Hodnota $\mathrm{N}_{F'/F}(\mathrm{div}_{F'/K}(x)) = \mathrm{N}_{F'/F}(2P'_0 - 2P'_\infty) = 2(1P_\infty) - 2(1P_\infty) = 0$.

$[F' : F] = 2$ a F'/F je Galoisovo rozšíření, tedy $|\mathrm{Gal}(F'|F)| = 2$. Zřejmě jeden automorfismus je identita, tedy $\sigma_1(x) = x$.

V minulém úkolu, jsme dokázali, že $F' = K(s, t) = F(t)$ a že $min_{t,F}(T) = T^2 - t^2$. Tedy prvky $\mathrm{Gal}(F'|F)$ permutují kořeny zmíněného minimálního polynomu $(t, -t)$. Víme, že $\sigma_1 = id \implies \sigma_2(t) = -t$.

Nyní vyjádříme $x \in F'$ v bázi $(1, t)$ nad F. Použijeme vzorec z minulého úkolu pro výpočet x pomocí t a s. Výsledkem je:

$$x = \frac{2bt^6 - 2abt^4}{(t^4 - at^2)^2 - (st)^2 t^2} + t \cdot \frac{-2bst^3}{(t^4 - at^2)^2 - (st)^2 t^2}$$

Díky tomu můžeme spočítat tedy $\sigma_2(x)$:

$$\sigma_2(x) = \frac{2bt^6 - 2abt^4}{(t^4 - at^2)^2 - (st)^2t^2} + \sigma_2(t) \cdot \frac{-2bst^3}{(t^4 - at^2)^2 - (st)^2t^2} =$$
$$\frac{2bt^6 - 2abt^4}{(t^4 - at^2)^2 - (st)^2t^2} + (-t) \cdot \frac{-2bst^3}{(t^4 - at^2)^2 - (st)^2t^2}$$

Po dosazení za t, s vyjde, že $\sigma_2(x) = bx^{-1}$

Dle S.12 tedy $N_{F'/F}(x) = \sigma_1(x) \cdot \sigma_2(x) = x \cdot bx^{-1} = b$ a zřejmě $\mathrm{div}_{F/K}(b) = 0$, jelikož $b \in K$. Rovnost tedy platí.

(f) Máme $F' \supset F \supset K(v), [F' : F] = 2$. Dále platí $[F : K(v)] = 3$, jelikož polynom $w(x, y)$ z 1) dává minimální polynom u nad $K(v)$. $F/K(v)$ je tedy algebraické konečného stupně.

Dle lemma F.9 je tedy $\mathrm{N}_{F'/K(v)}(\mathrm{div}_{F'/K}(x)) = 0$, protože dle e) $\mathrm{N}_{F'/F}(\mathrm{div}_{F'/K}(x)) = 0$ a zřejmě $\mathrm{N}_{F/K(v)}(0) = 0$.

Obdobně použitím proposition S.13 platí $N_{F'/K(v)}(x) = b$, jelikož dle e) $N_{F'/F}(x) = b$ a $N_{F/K(v)}(b) = b$. Poté $\mathrm{div}_{K(v)/K}(b) = 0$

3

Proposition F.13 říká v našem případě:

$$\deg_{F'/K}(\mathrm{Con}_{F'/F}(P)) = \frac{[F' : F]}{[K' : K]} \cdot \deg_{F/K}(P) = \frac{2}{1} \cdot 1 = 2 \implies$$
$$\mathrm{Con}_{F'/F}(P) = \sum_{P'|P} e(P'|P)P' \implies \deg_{F'/K}(\mathrm{Con}_{F'/F}(P)) = \sum_{P'|P} e(P'|P) \deg_{F'/K}(P') \implies$$
$$\sum_{P'|P} e(P'|P) \deg_{F'/K}(P') = 2$$

Máme tedy 3 možnosti:

1. Máme $P_1 \neq P_2 : P_1, P_2|P$. Poté už musí platit $\deg_{F'/K}(P_1) = 1 = \deg_{F'/K}(P_2)$ a $e(P_1|P) = 1 = e(P_2|P)$.
2. Nebo jediné $P'|P$, pro které buď $e(P'|P) = 2$ a následně musí být $\deg_{F'/K}(P') = 1$,
3. nebo $e(P'|P) = 1$ a následně musí $\deg_{F'/K}(P') = 2$.

Dle proposition F.6 platí (v našem případě $K' = K$), že pokud $P'|P$, pak $\deg_{F'/K}(P') = f(P'|P) \cdot \deg_{F/K}(P)$. Jelikož $f(P'|P) \geq 1$ a předpokládáme, že $\deg_{F'/K}(P') = 1$, nezbývá nic jiného, než $\deg_{F/K}(P) = 1$.

V předpokladech proposition F.6 je pouze, že F'/F je algebraické rozšíření. Podíváme-li se ale na důkaz podtvrzení $\deg_{F'/K}(P')[K' : K] = f(P'|P) \deg_{F/K}(P)$, tak se v důkazu nikde algebraičnost nepoužívá. Jediný bod, kde se využívá znalost tvrzení dokázaných pro algebraická, je $O_P \cap P' = P$. Toto ale platí obecně pro $P'|P$:

$$O_P \cap P' = (P \cup O_P^*) \cap P' = (P \cap P') \cup (O_P^* \cap P')$$

Zřejmě $P \cap P' = P$. Chceme tedy zjistit jestli $O_P^* \cap P' = \emptyset$. Uvažujme pro spor $x \in O_P^* \cap P' \implies x \in F, v_{P'}(x) > 0$. Zvolme uniformující element P označme ho t. Poté $x = ut^k, u \in O_P^*, k \in Z$. Ale $0 < v_{P'}(x) = v_{P'}(ut^k) = v_{P'}(u)v_{P'}(t^k)$, ale zřejmě $k = 0$ tedy $0 < v_{P'}(x) = v_{P'}(u)v_{P'}(1) = 0$, což je spor. Tedy je průnik prázdný.