NMMB538 - Zkouška

Jan Oupický

Lemma Q.1. *Proof:*

Denote $h = x_2^2 - f(x_1)$ and assume $h = u \cdot v$ where $u, v \in \bar{K}[x_1, x_2]$.

First assume $u, v \in \bar{K}[x_1, x_2] \backslash \bar{K}[x_1]$ i.e. $\deg_{x_2}(u) > 0, \deg_{x_2}(v) > 0$. Because $\deg_{x_2}(u) + \deg_{x_2}(v) = \deg_{x_2}(h) = 2 \implies \deg_{x_2}(u) = 1 = \deg_{x_2}(v)$. W.l.o.g assume $lc_{x_2}(u) = 1 = lc_{x_2}(v)$, we can do that since $lc_{x_2}(h) = 1$. Therefore we can write $u = x_2 - s_1$ and $v = x_2 - s_2$ where $s_1, s_2 \in \bar{K}[x_1]$. This gives us

$$x_2^2 - f(x_1) = h = (x_2 - s_1)(x_2 - s_2) = x_2^2 - (s_1 + s_2)x_2 + s_1 s_2$$

So it must hold that $s_1 = -s_2$ and then $h = x_2^2 + s_1(-s_1) \implies f(x_1) = s_1^2$.

Now assume w.l.o.g $u \in \bar{K}[x_1]$.We compare the leading coefficients.

$$1 = lc_{x_2}(h) = lc_{x_2}(u) \cdot lc_{x_2}(v) = u \cdot lc_{x_2}(v)$$

This shows that u must be invertible in $\bar{K}[x_1, x_2] \implies u \in \bar{K}^*$. In other words h is absolutely irreducible.

$\square$

Sublemma Q.3.5 *Let F/K be an algebraic function field, $char(K) \neq 2$, that is given by $y^2 = f(x)$, f being a quaternary polynomial that posseses a simple root. Let $P \in \mathbb{P}_{F/K}$. If $x \notin P$ or $y \notin P$, then $x, y \notin P$ and $2v_P(x) = v_P(y)$.*

Proof: In F it holds $y^2 = f(x)$ by definition which implies that for every $P \in \mathbb{P}_{F/K}$ $v_P(y^2) = 2v_P(y) = v_P(f(x))$.

Assume $v_P(x) < 0 \leq v_P(y)$. By properties of valution we have $\deg(f)v_P(x) = v_P(f(x)) = 2v_P(y) \implies 2v_P(x) = v_P(y)$ and by assumption $v_P(y) > v_P(x) \implies 2v_P(x) > v_P(x) \iff v_P(x) > 0$. That's a contradiction.

Now assume $v_P(x) \geq 0 > v_P(y)$. $v_P(x) \geq 0 \implies v_P(f(x)) \geq 0$ then $0 \leq v_P(f(x)) = 2v_P(y) < 0$ which is again a contradiction.

We have proven $v_P(x) < 0 \iff v_P(y) < 0$. Therefore we have the equality $4v_P(x) = 2v_P(y) \iff 2v_P(x) = v_P(y)$ assuming $v_P(x) < 0$ or $v_P(y) < 0$.

$\square$

Lemma Q.4. *Proof:* By sublemma Q.3.5 we know, that if $P \in \mathbb{P}_{F/K} : x^{-1} \in P \implies y^{-1} \in P$ and $2v_P(x) = v_P(y)$. This proves $(y)_- = 2(x)_-$ (x^{-1}, y^{-1} "share"places and the valuation is 2:1).

Let's first assume that f possesses a multiple root. Therefore $f(x_1) = (x_1 - \alpha)^2 g(x_1)$ where $\deg(g) = 2$ and g is not a square. By Q.3 F is given by $z^2 = g(x)$ i.e. $F = K(x, z)$. $[F : K(x)] = 2$ since $min_{z,K(x)}(T) = T^2 - g(x)$, that polynomial has z as a root in F and it is absolutely irreducible (as a polynomial in $K[x, T]$) since g is not a square. We can then assume $\bar{K} = K$ since $[F : \bar{K}(x)] = 2$ (same polynomial) and $[F : K(x)] = [F : \bar{K}(x)][\bar{K} : K] = 2 \implies [\bar{K} : K] = 1$.

Then we know $\deg((x)_-) = [F : K(x^{-1})] = [F : K(x)] = 2$ i.e. $\deg(D) = 2$.

Now assume f is separable. We can then use the same argument for $K = \bar{K}$ since $min_{y,K(x)}(T) = T^2 - f(x)$ and by Q.1 this one is also absolutely irreducible. $F = K(x, y) \implies [F : K(x)] = [F : \bar{K}(x)][\bar{K} : K] = 2 \implies [\bar{K} : K] = 1$. And again $\deg(D) = 2$.

Now let's prove that the genus is at most 1. Since $\deg(D) = 2 \implies \sum_{P:x^{-1}\in P} v_P(x)\deg(P) = 2$ means we have 2 possibilities (we are assuming $K = \bar{K}$ which implies $\forall P \in \mathbb{P}_{F/K}$: $\deg(P) = 1$:

1. There exists a unique place $P_\infty : v_{P_\infty}(x) = -2, v_{P_\infty}(y) = -4$ and $D = 2P_\infty$
2. There are 2 distinct places P, Q s.t. $v_P(x) = -1 = v_Q(x), v_P(y) = -2 = v_Q(y)$ and $D = P + Q$.

In both cases we can see that for $k \geq 2 : \{1, x, \ldots, x^k, y, yx, \ldots, yx^{k-2}\} \subset \mathcal{L}(kD)$ because $(x^k) + kD = k((x)_+ - (x)_-) + k(x)_- = k(x)_+ \geq 0$ and also $(y)_- = 2(x)_-$ so it holds if we substitute x^2 for y. This subset is linearly indepent over K because y cannot be expressed as a linear combination of x^i since f has one simple root (if $f(x) = g^2(x) \implies y = g(x)$). The set also contains $2k$ elements. Therefore $l(kD) \geq 2k$.

We know that for a sufficiently large k (if $l(kD) \geq 2g - 1$, g genus) we have $l(kD) = \deg(kD) - g + 1$ having $\deg(kD) = 2k, l(kD) \geq 2k \implies 0 \leq l(kD) - \deg(kD) = -g + 1 \iff g \leq 1$.

□

Proposition Q.5. *Proof:* Denote $ax^3 + bx^2 + cx + d = g(x) = f(x) - x^4$. First we will prove that for both $z \in Z = \{y + x^2, y - x^2\} : [F : K(z)] = 2$. Denote $z_1 = y + x^2, z_2 = y - x^2$ We have tower of field extensions $F \supseteq K(z_1, z_2) \supseteq K(z_1)$:

$$[F : K(z_1)] = [F : K(z_1, z_2)][K(z_1, z_2) : K(z_1)]$$

Clearly $K(x^2, y) \supseteq K(z_1, z_2)$ and conversely $x^2 = \frac{z_1 - z_2}{2}, y = \frac{z_1 + z_2}{2} \implies K(z_1, z_2) \supseteq K(x^2, y)$ therefore $K(z_1, z_2) = K(x^2, y)$.

Also $K(x^2, y) = F$ since $x = \frac{y^2 - x^4 - bx^2 - d}{ax^2 + c} \in K(x^2, y)$ if $a \neq 0$ and $c \neq 0$ ($F = K(x, y)$). If $a = 0 = c$ then F is given by $y^2 = g'(x^2)$ where $g'(x) = x^2 + a'x + b$ separable. Then $K(x^2, y) = F$ as well.

Choose $P \leq D$ a place. We will prove that for at least one $z \in Z : v_P(z) < v_P(x)$.

$$y^2 = f(x) \iff y^2 - x^4 = g(x), 0 \leq \deg(g) \leq 3 \implies$$
$$(y + x^2)(y - x^2) = g(x) \implies v_P(y + x^2) + v_P(y - x^2) = v_P(g(x)) = \deg(g)v_P(x)$$

Denote $z_1 = y + x^2, z_2 = y - x^2$. Assume to contrary $v_P(z_1) \geq v_P(x)$ and $v_P(z_2) \geq v_P(x)$. We will look at all possible cases.

$\deg(g) = 3$: $3v_P(x) = v_P(z_1) + v_P(z_2) \geq v_P(x) + v_P(x) \implies v_P(x) > 0$ which is a contradiction since $v_P(x) < 0$.

$\deg(g) = 2$: $2v_P(x) = v_P(z_1) + v_P(z_2)$.

First consider $v_P(x) = v_P(z_1) = v_P(z_2)$ and $v_P(x) = -2$, then $2P = (x)_- = (z_1)_- = (z_2)_-$. Then $z_1, z_2 \in \mathcal{L}(D)$ but then also $\frac{z_1 + z_2}{2} = y \in \mathcal{L}(D)$ which is a contradiction since $(y)_- = 2(x)_-$.

Now let's assume $v_P(x) = -1$ and then there also exist a different place Q s.t. $v_Q(x) = v_Q(z_1) = v_Q(z_2) = -1$. Since $\deg((z)_-) = 2$ then again $P + Q = (x)_- = (z_1)_- = (z_2)_-$ and we have the same contradiction.

We have proven that $v_P(x) = v_P(z_1) = v_P(z_2)$ is impossible therefore for one z it must hold $v_P(z) < v_P(x)$.

$\deg(g) = 1$: $v_P(x) = v_P(z_1) + v_P(z_2)$. First assume $v_P(x) = -2$. And also $v_P(z_1) = v_P(z_2) = -1$. This is impossible since $\deg((z)_-) = 2$ but for every other place $Q \neq P : 0 =$

$v_Q(z_1) + v_Q(z_2) \implies v_Q(z_1) = -v_Q(z_2)$. If there was $Q_1 : v_{Q_1}(z_1) = -1 \implies v_{Q_1}(z_2) = 1$ and $Q_2 : v_{Q_2}(z_2) = -1 \implies v_{Q_2}(z_1) = 1$. Then for some P_1, P_2 places of degree 1: $(z_1) = (P_1 + Q_2) - (P + Q_1), (z_2) = (P_2 + Q_1) - (P + Q_2)$. Set $D' = P + Q_1 + Q_2$ then $z_1, z_2 \in \mathcal{L}(D')$ and as before this means that $y \in \mathcal{L}(D')$ which is a contradiction.

Now if $v_P(x) = -1$ then either $v_P(z) < v_P(x)$ for a $z \in Z$ or w.l.o.g $v_P(z_1) = -1$ and $v_P(z_2) = 0$. Then also assume first $v_Q(z_1) = -1 \implies v_Q(z_2) = 0$. But since $\deg((z)_+) = 2$ there must be a place P' s.t. $v_{P'}(z_2) > 0$ and $v_{P'}(x) = 0$ since $P' \neq P, Q$ but it must be $v_{P'}(z_1) < 0$. This again contradicts the degree of the divisor.

If $v_Q(z_1) = 0$ and $v_Q(z_2) = -1$. Then again there must be a place P_1 s.t. $v_{P_1}(z_1) = -1$ and $v_{P_1}(z_2) = 1$ and a place $v_{P_2}(z_2) = 1 \implies v_{P_2}(z_1) = -1$. This also contradicts divisor degree.

The last case is $\deg(g) = 0$: $v_P(z_1) = -v_P(z_2) \implies (z_1) = -(z_2)$. First assume $v_P(z_1) = 0 \implies v_P(z_2) = 0$ and same for v_Q (Q not necessary different from P). Then there exist places $P_1, P_2, Q_1, Q_2 \neq P, Q$ s.t. $(z_1) = P_1 + P_2 - (Q_1 + Q_2), (z_2) = -(z_1)$. Set $D' = P_1 + P_2 + Q_1 + Q_2$ then $z_1, z_2 \in \mathcal{L}(D')$ but also $y \in \mathcal{L}(D')$ which is again contradiction since $(y)_- = 2(x)_-$.

If $v_P(z_1) = 1 \implies v_P(z_2) = -1$. There exists another place P' s.t. $v_{P'}(z_1) = 1 \implies v_{P'}(z_2) = -1$. There must be again two places Q_1, Q_2 s.t. $(z_1) = P + P' - (Q_1 + Q_2), (z_2) = -(z_1)$. Put $D' = P + P' + Q_1 + Q_2$ then again $y \in \mathcal{L}(D')$ which is a contradiction.

We have proven that for each place $P \leq D$ at least one $z \in Z$ must have $v_P(z) < v_P(x)$. This shows also that $(x)_- = P + Q$ for distinct P, Q. If $P = Q$ then $v_P(x) = -2 \implies v_P(z) \leq -3$ which contradicts $[F : K(z)] = 2$. Since $\deg((z)_-) = 2$ and $v_P(z) < -1$ it must be that $(z)_- = 2P, (z')_- = 2Q$ for $z, z' \in Z$. Since we have not distinguished P and Q we can say $(z_1)_- = 2P$ and $(z_2)_- = 2Q$.

$\square$

Theorem Q.6. *Proof:* Assume genus 0. There exists $t \in F$ s.t. $(t) = P - Q$ and also $(t^{-1}) = -(t) = Q - P$. Also $l(D) = \deg(D) + 1 = 3$.

$t \in \mathcal{L}(D)$ since $(t) + D = P - Q + P + Q = 2P \geq 0$. Also $t^{-1} \in \mathcal{L}(D) : (t^{-1}) + D = Q - P + P + Q = 2Q \geq 0$. t and t^{-1} are linearly independent since $t \notin K$. This means $\{1, t, t^{-1}\}$ is a basis of $\mathcal{L}(D)$.

$x \in \mathcal{L}(D) \implies x = c_0 + c_1 t + c_2 t^{-1}$ for some $c_i \in K$. This is equivalent to saying $tx = u(t), u(t) \in K[t], \deg(u) = 2$.

In the same way we see $\{1, t, t^{-1}, t^2, t^{-2}\}$ for a basis of $\mathcal{L}(2D)$. Again $y \in \mathcal{L}(2D)$: $(y) + 2D = (y)_+ - (y)_- + 2(x)_- = (y)_+ \geq 0$. This means $t^2 y = v(t)$ where $v(t) \in K[t], \deg(v) = 4$.

$y^2 = f(x) \iff t^4 y^2 = t^4 f(x)$. Substitute $yt = v(t)$ and $xt^2 = u(t)$ then we have equality $v^2(t) = t^4 f(\frac{u(t)}{t})$. f is a polynomial of degree 4 therefore it has up to 4 different roots $1 \leq i \leq 4 : \alpha_i \implies v^2(t) = t^4(\frac{u(t)}{t} - \alpha_1)(\frac{u(t)}{t} - \alpha_2)(\frac{u(t)}{t} - \alpha_3)(\frac{u(t)}{t} - \alpha_4)$ we can rewrite this as

$$v^2(t) = (u(t) - t\alpha_1)(u(t) - t\alpha_2)(u(t) - t\alpha_3)(u(t) - t\alpha_4)$$

$v^2(t) = v(t)v(t)$ is a polynomial of degree 8, which has at most 4 different roots. Also $u(t) - t\alpha_i$ is a polynomial of degree 2. There exist at most two $\alpha \in K$ s.t. $u(t) - t\alpha$ has a root of multiplicity 2. This is because the root of a quadratic polynomial has multiplicity 2 when the discriminant D is 0. If $g(x) - \alpha x = ax^2 + (b - \alpha)x + c \implies 0 = \mathrm{D} = (b - \alpha)^2 - 4ac \iff \alpha = \pm 2\sqrt{ac} + b$.

Also if $i \neq j : \alpha_i \neq \alpha_j$ the polynomials $u(t) - t\alpha_i$ and $u(t) - t\alpha_j$ do not have common roots. This means that if $1 \leq i \leq 4 : \alpha_i$ are all different then $v^2(t)$ has at least $6 = 2+2+1+1$ different roots. This a contradiction.

Therefore if genus is 0 then f cannot be separable. We have shown that genus of F is 0 or 1, this means that for f separable we must have genus 1.

Denote $w = x_2^2 - f(x_1)$.

$$\frac{\partial w}{\partial x_1} = -f'(x_1), \frac{\partial w}{\partial x_1} = 2x_2 \tag{1}$$

For a singularity $\alpha = (\alpha_1, \alpha_2), \alpha_2$ must be 0 and α_1 must be a root of $f(x_1)$ and also of $f'(x_1)$ this is true iff $f(x_1)$ is separable. If $f(x_1)$ is not separable then it shares a common root α_1 with $f'(x_1)$ and this gives us singularity at $(\alpha_1, 0)$. This proves the rest of the theorem.

$\square$

Theorem Q.7. *Proof:* Denote $D = P + Q$ a divisor. Due to genus being 1 $\forall k \geq 1 : l(kD) = 2k$. $l(D) = 2$ and that means there exists $x \notin K$ s.t. $\{1, x\}$ is a basis of $\mathcal{L}(D)$ and also $(x)_- \leq P + Q$. Then $(x)^2 = 2(x) = 2(x)_+ - 2(x)_- \implies x^2 \in \mathcal{L}(2D), \{1, x, x^2\}$ is linearly independent in $\mathcal{L}(2D)$ but $l(2D) = 4$ that means there exists $y \in \mathcal{L}(2D) \setminus \mathcal{L}(D)$ such that $\{1, x, x^2, y\}$ is a basis of $\mathcal{L}(2D)$.

Denote $B = \{1, x, x^2, x^3, x^4, y, yx, yx^2, y^2\}$, clearly $B \subseteq \mathcal{L}(4D), l(4D) = 8$ and $|B| = 8 \implies 1 \leq i \leq 8 : \exists a_i \in K :$

$$y^2 = a_1 y + a_2 yx + a_3 yx^2 + a_4 x^4 + a_5 x^3 + a_6 x^2 + a_7 x + a_8$$

Denote $C = \{1, x, x^2, x^3, y, yx\}$. C is a basis of $\mathcal{L}(3D)$, $C \cup \{yx^2, y^2\}$ is also a basis of $\mathcal{L}(4D)$. If $a_4 = 0$ that would be a contradiction to $C \cup \{yx^2, y^2\}$ being a basis of $\mathcal{L}(4D)$ since y^2 would be a linear combination of 7 elements.

Now we make a substitution $y \to y - \frac{a_1 + a_2 x + a_3 x^2}{2}$. This gives us form:

$$y^2 = b_1 x^4 + b_2 x^3 + b_3 x^2 + b_4 x + b_5$$

where $b_1 = a_4 + \frac{a_3^2}{4}$. If $b_1 = 0$ then y^2 would be a linear combination of elements in $\mathcal{L}(3D)$ but

$\square$

Theorem Q.8. *Proof:* Denote $f(x) = g(x^2)$. F is EFF therefore genus is 1 and there exists a place of degree 1. Also K can be assumed algebraically closed.

If $g(x)$ has a multiple root α, then $f(x) = g(x^2)$ has also a multiple root because $g(x) = (x - \alpha)^2 \implies g(x^2) = (x - \sqrt{\alpha})^2 (x + \sqrt{\alpha})^2$. Set $z = \frac{y}{x - \sqrt{\alpha}}$. Then F is given by $z^2 = (x + \sqrt{\alpha})^2$. This means $x \in K(z)$ and from the definition of y also $y \in K(z)$ which means F has genus 0, a contradiction.

From now on we can assume $g(x)$ has 2 distinct roots. If $f(x) = g(x^2)$ would have a multiple root then it's genus would not be 1 by Q.6. So we can assume $g(x^2)$ separable.

First we will prove the second part of the theorem. We have shown that $g(x^2)$ must be separable. Therefore by Q.5 we have places of degree 1 ($P \neq Q$), $(x)_- = P + Q$ and $(y + x^2)_- = 2Q, (y - x^2)_- = 2P$.

$$y^2 = g(x^2) = x^4 + 2bx^2 + c \iff y^2 - (x^4 - 2bx^2 - b^2) = c - b^2 \implies$$
$$(y - (x^2 + b))(y + (x^2 + b)) = c - b^2$$

Since $g(x^2)$ is separable $g(x)$ must have simple roots. If $g(x)$ has a multiple root then it's discriminant is 0 and that happens iff $c - b^2 = 0$. So we know $0 \neq c - b^2 \in K$.

$$0 = v_P(c - b^2) = v_P(y - (x^2 + b)) + v_P(y + (x^2 + b))$$
$$v_P(y - (x^2 + b)) = v_P(y - x^2) = -2 \implies v_P(y + (x^2 + b)) = 2$$

Similarly we can show $v_Q(y - (x^2 + b)) = 2$ and $v_Q(y + x^2 + b) = -2$.

Since $\deg((y+x^2+b)_+) = \deg((y+x^2+b)_-) = \deg((y+x^2)_-) = 2 \implies \operatorname{div}(y+x^2+b) = 2P - 2Q$ and similarly $\operatorname{div}(y + x^2 + b) = 2Q - 2P$.

We have proven the last part of the theorem. Now let's prove the equivalence.

As we have shown before. We can assume $g(x^2)$ separable and then we have involution $P-Q$ as shown above since $2P-2Q = (t)$ for $t \in F$. We only have to show that $P-Q \neq (t)$ for some $t \in F$.

If $t \in F$ s.t. $(t) = P - Q \implies \deg((t)_+) = 1 = [F : K(t)]$ and that would be contradiction with F being EFF.

Now we assume we have involution. We can always find $t \in F \setminus K$ s.t. $(t) = 2P - 2Q$ where P, Q distinct places of degree 1 and $P - Q$ is involution.

Then $l(2P) = 2 = l(2Q) \implies \{1, t\}$ is a basis of $\mathcal{L}(2P)$ and $\{1, t^{-1}\}$ is a basis of $\mathcal{L}(2Q)$.