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.

□

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 $v_P(y) < 0$.

□

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 $k \geq 2 : \{1, x, \dots, x^k, y, yx, \dots, yx^{k-2}\} \subset \mathcal{L}(kD)$ 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:* In the proof of lemma Q.4 we have established there are 2 possibilities for the structure of $(x)_-$ either $(x)_- = 2P_\infty$ or $(x)_- = P + Q$, P, Q distinct.

□

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.

□