Model solution exercises week 11

(Presentation: Nils Donselaar)

Exercise 1

a) Give a proof of Lemma 2, i.e. prove that if $F$ is a field of characteristic $p \geq 3$, then for all $x \in F(t)$ the expression $u = \frac{x^{p+1}}{x^p - t}$ has only simple zeroes and poles. (3 pts.)

b) Using Lemma 2, complete the proof of Lemma 3 discussed during the presentation by proving the right-to-left direction for the case where $s > 0$ and $y$ is not a $p$-th power of any function $z \in F(t)$. (4 pts.)

a) Write $x = \frac{a}{b}$ in its unique way. Now $u = \frac{(\frac{x}{x^{p-1}})^{p+1}}{x^p - t} = \frac{a^{p+1}}{b^{p+1} - t b^p}$. Let $q$ be a prime of $F[t]$ such that $q^2 \mid a^p + tb^p$. Then $q$ divides $\frac{d}{dt}(a^p + tb^p) = b^p$; hence also $q \mid a^p$. This would mean that $q \mid a$ and $q \mid b$, but this cannot occur since $a, b$ coprime, so $u$ only has simple zeroes. The case for poles is entirely symmetrical: if $q^2 \mid a^p - tb^p$, then $q$ divides $\frac{d}{dt}(a^p - tb^p) = -b^p$, and so $q \mid a^p$ by that fact that $q \mid a^p - tb^p$ is also true. This would again mean that $q \mid a$ and $q \mid b$ are both true, which is impossible, so $u$ also has only simple poles. Points awarded: 1 for rewriting $u$ by taking $x$ as a unique fraction; 1 for showing how we get a contradiction from assuming that we have a zero/pole of higher multiplicity; $\frac{1}{2}$ for pointing out how the argument can be extended to poles/zeroes.

b) Assume $s > 0$ and $y$ is not a $p$-th power of any function $z \in F(t)$. If $v = w^p$ for some $w \in F(t)$, then $v = \frac{y^p + t^p}{y - t^p} = w^p$. From this we obtain $y + t^p = w^p(y - t^p)$, which in turn gives $y(1 - w^p) = -t^p(w^p + 1)$ which because of characteristic $p$ is equal to $y(1 - w)^p = -(t^{p-1}(w + 1))^p$. Since char($F$) $\neq 2$, $w = 1$ is impossible (for this would lead to $y + t^p = y - t^p$), but now $y = (t^{p-1}(w + 1))^p$ which contradicts our assumption that $y$ is not a $p$-th power, hence $v$ is not a $p$-th power. Suppose $q \neq t$ is a prime in $F[t]$ such that $\text{ord}_q v < 0, p \nmid \text{ord}_q v$. Now if $\text{ord}_q (\sigma^p - \sigma) < 0$, then $p \mid \text{ord}_q (\sigma^p - \sigma)$. By Lemma 2, $\text{ord}_q u^2 \in \{0, \pm 2\}$, so by (1) we know that $\text{ord}_q u^2 = \text{ord}_q v^2 = -2$ has to hold for $\text{ord}_q (v^2 - u^2) \geq 0$ to occur (for $p \mid \text{ord}_q (v^2 - u^2)$ cannot hold if it is negative). Since $q \neq t$, this now also gives us $\text{ord}_q u^2 t^p = \text{ord}_q u^2 t = -2$.
and \( \text{ord}_q(v^2 t^{p^s} - u^2 t) = \text{ord}_q(\mu^p - \mu) \geq 0 \). Now since \( \mu^p - \mu - t(\sigma^p - \sigma) = v^2 t^{p^s} - u^2 t - v^2 t + u^2 t = v^2(t^{p^s} - t) \) and \( \text{ord}_q(\mu^p - \mu - t(\sigma^p - \sigma)) \geq 0 \), we have \( \text{ord}_q(v^2(t^{p^s} - t)) \geq 0 \), and therefore \( \text{ord}_q(t^{p^s} - t) \geq 2 \). Because \( s > 0 \) we have \( \text{ord}_q(t^{p^s} - t) \in \{0, 1\} \) which gives a contradiction, so there cannot be such primes \( q \), hence \( v = w^pt^i \) for some \( w \in \overline{F}(t), \ i \in \mathbb{Z} \). Write \( x = zt^j \) with \( j \in \mathbb{Z} \) and \( z,t \) coprime, so that \( u = \frac{z^pt^i t^j + 1}{2^{p^s} - 2^j} \). If \( j < 0 \), then \( u = \frac{z^pt^i t^j + 1}{2^{p^s} - 2^j} \); if \( j = 0 \), then \( u = \frac{z^pt^i + 1}{2^{p^s} - 2^j} \); if \( j > 0 \), then \( u = \frac{z^pt^i t^j + 1}{2^{p^s} - 2^j} \), so in all cases \( \text{ord}_q u = 0 \). This means that if \( j \neq 0 \) then either (1) or (2) gives \( p \mid j \), so \( p \mid j \) must hold, but now \( v \) is a \( p \)-th power again which shows that this case cannot occur.

Points awarded: 1 for showing why \( v \) cannot be a \( p \)-th power by using the characteristic \( p \neq 2 \); 1 for using Lemma 2 to reason why \( \text{ord}_q(v^2 - u^2) \geq 0 \) has to hold; 1 for demonstrating using \( \text{ord}_q(t^{p^s} - t) \) why such primes \( q \) cannot exist; 1 for providing an argument which shows that \( v \) must then be a \( p \)-th power giving our final contradiction.

**Exercise 2**

Prove the Proposition used in the proof of Lemma 4: If \( z \in F[t] \) has only simple roots and \( t \nmid z \), then \( \exists s \in \mathbb{N}_{>0} \ z \mid t^{p^s-1} - 1 \). (3 pts.)

Suppose \( z \in F[t] \) has only simple roots and \( t \nmid z \); also suppose \( z \) is not a constant in \( F \) (for then the result follows immediately since \( z \) is now a unit). Because \( F[t]/z \) is finite (the finiteness of \( F \) is part of the assumptions of Lemma 4) and \( t \) is not 0 here since \( t \nmid z \), there are \( m,n \in \mathbb{N} \) with \( m \neq n \) such that \( z \mid t^m - t^n \). Take \( m > n \) without loss of generality, so that \( z \mid t^{m-n} - 1 \) because \( t \nmid z \). If \( m-n = kp, k \in \mathbb{N}_{>0} \), then \( z \mid (t^k - 1)^p \) by characteristic \( p \), but then \( z \mid t^k - 1 \) since \( z \) has only simple roots, so we may assume \( p \nmid m-n \). This means that \( m-n, p \) are coprime, so \( \exists s \in \mathbb{N}_{>0} \ (m-n) \mid p^s-1 \), hence \( t^{m-n} - 1 \mid t^{p^s-1} - 1 \) and therefore \( z \mid t^{p^s-1} - 1 \) as we needed to prove.

Points awarded: 1 for reasoning that we have such \( m,n \) using \( t \nmid z \) and the finiteness of \( F \); 1 for showing how we get to \( z \mid t^k - 1 \) where \( p \nmid k \) by using that \( z \) has only simple roots; 1 for providing an argument how this leads to an \( s \) such that \( z \mid t^{p^s-1} - 1 \).