18.786. Separability of f_m

Recall that (π, f) is as usual:

(i) π is a uniformizer of a complete unramified extension L over K,

(ii) $f \in \mathcal{O}_L[X]$ is a monic polynomial such that $f \equiv \pi X \mod X^2$ and $f \equiv X^q \mod \pi$. (In particular f has degree q.)

We defined

- $\pi_m := \pi^{\varphi^{m-1}} \pi^{\varphi^{m-2}} \cdots \pi^{\varphi} \pi = \pi^{(m-1)} \cdots \pi^{(1)} \pi$,
- $f_m := f^{\varphi^{m-1}} \circ \cdots \circ f^{\varphi} \circ f = f^{(m)} \circ \cdots \circ f^{(1)} \circ f$.

I should have proved the following at the very beginning of the section on Lubin-Tate extensions.

Proposition 0.1. *f_m is a separable polynomial, i.e. the roots of f_m are mutually distinct.*

Proof. Recall that every $\alpha \in \mu_{f,m}$ satisfies

$$v(\alpha) > 0$$

since $0 = f_m(\alpha) \equiv \alpha^{q^m} \mod \pi$.

Let's start with the $m = 0$ case. Since $f_m(X) = \pi X + X^q + \pi g(x)$ for some $g(X) \in X^2 \mathcal{O}_L[X]$. The derivative $f'(X)$ has the form

$$f'(X) = \pi(1 + (q/\pi) X^{q-1} + g'(X)).$$

From this it's clear that any α such that $v(\alpha) > 0$ cannot be a root. (For such an α, $v((q/\pi)\alpha^{q-1} + \pi g'(\alpha)) > 0$.) Thus $f(X)$ and $f'(X)$ have no common factor.

Now proceed by induction on m. Suppose the assertion is true up to $m - 1$. Note

$$f_m(X) = f^{(m-1)}(f_{m-1}(X)), \quad f'_m(X) = (f^{(m-1)})'(f_{m-1}(X)) \cdot f'_{m-1}(X).$$

For any root α of $f_m(X)$ it suffices to show that

$$f'_m(\alpha) \neq 0. \tag{0.1}$$

By the way α is chosen, $f_{m-1}(\alpha)$ is a root of $f^{(m-1)}$. Thus $f_{m-1}(\alpha)$ cannot be a root of $(f^{(m)})'$ by the $m = 0$ case applied to $f^{(m-1)}$. On the other hand, $f'_{m-1}(\alpha) \neq 0$ by the induction hypothesis. Hence (0.1) is verified. □

Recall that $\mu_{f,m}$ is the set of roots of f_m and that $f_m^{\times} := f_m / f_{m-1}$.

Corollary 0.2. *$|\mu_{f,m}| = q^m$ and $f_m^{\times} \in \mathcal{O}_L[X]$.*

Proof. The former is immediate from the proposition. For the latter, obviously $f_m^{\times}$ is monic and belongs to $L[X]$ by the proposition. Since its roots are all integral, the coefficients are in $\mathcal{O}_L$. □