Homework

Lei Bichang

1 Composition of Ramified Extensions

Consider $X^p - pX \in \mathcal{L}_{-p}$. Let π be a root of the Eisenstein polynomial $f_\pi(X) = X^{p-1} - p \in \mathbb{Z}_p[X]$ in $\bar{\mathbb{Q}}_p$, and let $K := \mathbb{Q}_p(\pi)$, then $K/\mathbb{Q}_p$ is totally ramified. We claim that $K(\zeta_p)/\mathbb{Q}_p$ is not totally ramified.

$$\begin{tikzcd}[column sep=small]
 & \mathbb{Q}_p(\zeta_p, \pi) \arrow[dl, dash] \arrow[dr, dash] & \\
\mathbb{Q}_p(\zeta_p) \arrow[dr, dash] & & \mathbb{Q}_p(\pi) \arrow[dl, dash] \\
 & \mathbb{Q}_p &
\end{tikzcd}$$

Let $F := \mathbb{Q}_p(\zeta_p)$ and $\eta := \zeta_p - 1$ a uniformizer of F. Write $p = u\eta^{p-1}$ in F, where $u \in \mathcal{O}_F^\times$. Then π is a root of

$$X^{p-1} - p = X^{p-1} - u\eta^{p-1} \in \mathcal{O}_F[X],$$

so $z := \pi/\eta$ is a root of $X^{p-1} - u \in \mathcal{O}_F[X]$.

Next, we compute $u \bmod \eta$. For this we note that the following equation holds.

Lemma 1. $(\zeta_p - 1)(\zeta_p^2 - 1)\dots(\zeta_p^{p-1} - 1) = p$.

Proof. This is because the minimal polynomial of $\zeta_p - 1$ is

$$\frac{(1+X)^p - 1}{X} = X^{p-1} + \cdots + p,$$

whose roots are $\zeta_p^i - 1$, $1 \le i \le p-1$. □

From here we see that

$$\begin{aligned} u = \frac{p}{\eta^{p-1}} &= (\zeta_p + 1)(\zeta_p^2 + \zeta_p + 1)\dots(\zeta_p^{p-2} + \cdots + \zeta_p + 1) \\ &\equiv 1 \cdot 2 \cdots (p-1) \equiv -1 \pmod{\eta}. \end{aligned}$$

So as $p \ge 3$, the polynomial

$$\overline{X^{p-1} - u} = X^{p-1} + 1 \in \mathbb{F}_p[X]$$

is irreducible of degree ≥ 2. Therefore $K(\zeta_p) = \mathbb{Q}_p(\zeta_p, \pi) = \mathbb{Q}_p(\zeta_p, z)$ is a nontrivial unramified extension over $F = \mathbb{Q}_p(\zeta_p)$, and the inertia degree $f(K(\zeta_p)/\mathbb{Q}_p) = f(K(\zeta_p)/K) > 1$.

2 Multiplication by p

Write $[p](X) = \sum_{i\geq 1} a_i X^i$, so $[p]'(X) = \sum_{i\geq 1} i a_i X^{i-1}$. We know that $[p]'(0) = a_1 = p$. Consider the invariant differential

$$\omega_F(X) = \frac{dX}{F_1(0,X)}.$$

The endomorphism $[p](X)$ satisfies the equation

$$\omega_F \circ [p] = [p]'(0)\omega_F = p\omega_F,$$

i.e.,

$$\frac{[p]'(X)\,dX}{F_1(0,[p](X))} = p\frac{dX}{F_1(0,X)}.$$

Hence

$$[p]'(X) = p\frac{F_1(0,[p](X))}{F_1(0,X)}$$

Since $F_1(0,X) = 1 + X +$ terms of higher degree, it is invertible in $R[\![X]\!]$, and thus $F_1(0,[p](X))/F_1(0,X) \in R[\![X]\!]$. Therefore every coefficient of $[p]'(X)$ is divided by p, so

$$p \nmid i \implies p \mid a_i$$

for each integer $i \geq 1$. This shows that $[p](X) \in pR[\![X]\!] + R[\![X^p]\!]$.

3 The Zeroes of the Logarithm

3.1

Let

$$\omega(X) = (1 + a_1 X + a_2 X^2 + \dots)\,dX = \frac{dX}{F_1(0,X)}$$

be the normalized invariant differential of F, so

$$\log_F(X) = X + \frac{a_1}{2}X^2 + \frac{a_3}{3}X^3 + \dots.$$

As F is defined over $\mathcal{O}_K$, $F_1(0,X) \in \mathcal{O}_K[\![X]\!]^\times$ and the numbers $a_i \in \mathcal{O}_K$. Let $z \in \mathfrak{m}_{\mathbb{C}_p}$, then $v_p(z) > 0$, and thus

$$v_p\left(\frac{a_i z^i}{i}\right) = v_p(a_i) + iv_p(z) - v_p(i) \geq iv_p(z) - v_p(i) \to +\infty$$

as $i \to \infty$, because $v_p(i)$ grows in the speed of $\log(i)$. So $\log_F \in \mathrm{H}_K$.

3.2

By Exercise 2, there eixst $f, g \in \mathcal{O}_K[\![X]\!]$ s.t.

$$[p](X) = pf(X) + g(X^p),$$

so

$$|[p](z)|_p \leq \max\{p^{-1}|f(z)|_p, |g(z^p)|_p\}.$$

Because $[p](X) = pX + \text{terms of higher order}$, $f(0) = g(0) = 0$ and $f = X + \text{terms of higher order}$. Write $f(X) = Xf_1(X)$ and $g(X) = Xg_1(X)$, where $f_1 = 1 + \text{terms of higher order}$. As $0 < |z|_p < 1$, we have $|f_1(z)|_p = 1$ and $|g_1(z^p)|_p \le 1$. Hence

$$p^{-1}|f(z)|_p = p^{-1}|z|_p < |z|_p,$$

and

$$|g(z^p)|_p \le |z|_p^p < |z|_p.$$

So $|[p](z)|_p < |z|_p$.

3.3

Assume that $z \in \mathfrak{m}_{\mathbb{C}_p}$ is a zero of $\log_F$. Since $\log_F$ is an isomorphism $F \to \mathbb{G}_\mathrm{a}$ over K, we have

$$\log_F([p](z)) = p\log_F(z) = 0.$$

From here we can prove that $z \in \mathrm{Tors}(F)$.

- If $z \notin \mathrm{Tors}(F)$, then $z \neq 0$. Using the previous computation inductively, we see that $[p^n](z) \neq 0$ is a zero of $\log_F$ for each $n \geq 1$. Exercise 3.2 tells us that

  $$1 > |z|_p > |[p](z)|_p > |[p^2](z)|_p > \cdots > 0,$$

  so these $[p^n](z)$'s are disjoint and $\log_F$ has infinitely many zeroes in the ball $B(0, |z|_p)$. But a function in H_K can have only finitely many zeroes in $B(0, |z|_p)$, so this contradicts the fact that $\log_F \in \mathrm{H}_K$.

Conversely, if $z \in \mathrm{Tors}(F)$, then $[p^n](z) = 0$ for some $n \geq 1$. So

$$p^n \log_F(z) = \log_F([p^n](z)) = \log_F(0) = 0,$$

and thus $\log_F(z) = 0$.

4 Torsion of some formal group

4.1

It suffices to check the associativity and the commutativity. For associativity,

$$\begin{aligned} F_\alpha(X, F_\alpha(Y, Z)) &= X + (Y + Z + \alpha YZ) + \alpha X(Y + Z + \alpha YZ) \\ &= X + Y + \alpha XY + Z + \alpha(X + Y + XY)Z \\ &= F_\alpha(F_\alpha(X, Y), Z). \end{aligned}$$

Commutativity is clear.

4.2

(1) *Compute* $\mathrm{Tors}(F)$. Following the hint, we compute

$$1 + \alpha F_\alpha(X, Y) = 1 + \alpha X + \alpha Y + \alpha^2 XY = 1 + \mathbb{G}_\mathrm{m}(\alpha X, \alpha Y).$$

Hence $\alpha X \in \mathcal{O}_K[\![X]\!]$ is a homomorphism $F_\alpha \to \mathbb{G}_{\mathrm{m}}$, and

$$\alpha[n]_{F_\alpha}(X) = [n]_{\mathbb{G}_{\mathrm{m}}}(\alpha X) = (1+\alpha X)^n - 1, \quad \forall n \in \mathbb{Z}.$$

Since $(1+\alpha X)^n - 1 \in \alpha\mathcal{O}_K[\![X]\!]$, the multiply-by-$n$ endomorphism for F_α is

$$[n]_{F_\alpha} = \frac{(1+\alpha X)^n - 1}{\alpha}$$

if $\alpha \neq 0$. In case $\alpha = 0$, $F_\alpha = \mathbb{G}_{\mathrm{a}}$ and $[n]_{F_\alpha}(X) = nX$. Therefore,

$$\mathrm{Tors}(F_\alpha) = \begin{cases} \{z \in \mathfrak{m}_{\mathbb{C}_p} | 1+\alpha z \in \mu_{p^\infty}\}, & \alpha \neq 0, \\ \{0\}, & \alpha = 0. \end{cases}$$

(2) *Compute the height of F_α.* We divide the problem into two cases.

- $\alpha \in \mathfrak{m}_K$. In this case $\bar{F}_\alpha = X + Y = \bar{\mathbb{G}}_{\mathrm{a}}$, so the height of F_α is infinity.
- $\alpha \in \mathcal{O}_K^\times = \mathcal{O}_K \setminus \mathfrak{m}_K$. By the computation above,

$$[p]_{\bar{F}_\alpha} = \frac{(1+\bar{\alpha}X)^p - 1}{\bar{\alpha}} = \bar{\alpha}^{p-1}X^p.$$

  So the height of F_α is 1.

4.3

Choose a uniformizer π of K. Then $[p](X) \in \pi\mathcal{O}_K[\![X]\!]$ because $\overline{[p]}(X) = 0$, and $[p^n](X) = [p]([p^{n-1}](X)) \in \pi\mathcal{O}_K[\![X]\!]$ for every integer $n \geq 1$. In fact, we have a better control for $[p^n]$.

Lemma 2. For every $n \in \mathbb{Z}_{\geq 1}$, $[p^n](X) \in \pi^n\mathcal{O}_K[\![X]\!]$.

Proof. The case of $n = 1$ is known. Suppose that $[p^n](X) \in \pi^n\mathcal{O}_K[\![X]\!]$, then every coefficient of $[p^{n+1}](X) = [p]([p^n(X)])$ is a finite sum of the form $\sum ab_1 \cdots b_r$, where a is a coefficient of $[p](X)$ and $b_1, \ldots, b_r$ are coefficients of $[p^n](X)$. So $\pi^{n+1} \mid ab_1 \cdots b_r$, and thus π^{n+1} divides all coefficients of $[p^{n+1}](X)$. □

Now we look at $\mathrm{Tors}(F) = \bigcup_{n\geq 1} F[p^n]$. Since $F[p^n] \subset F[p^{n+1}]$, $\mathrm{Tors}(F)$ is finite if and only if $\#F[p^n]$ is finite and constant for n sufficiently large. For simplicity, we introduce the following definition.

Definition 1. For $f(X) = \sum_{i\geq 0} a_i X^i \in K \otimes_{\mathcal{O}_K} \mathcal{O}_K[\![X]\!]$, let $w(f)$ be the index of the lowest term whose coefficient has minimum valuation, i.e.,

$$w(f) := \min\{i \in \mathbb{Z}_{\geq 0} \mid v_p(a_i) \leq v_p(a_j), \forall j \in \mathbb{Z}_{\geq 0}\}.$$

By definition, if d is the integer s.t. $\pi^d f(X)$ has finite Weierstrass degree w, then $w = w(f)$. So by Weierstrass preparation theorem, $\#F[p^n] = w([p^n]) < \infty$.

Lemma 3. If $[p^n](X) \in p\mathcal{O}_K[\![X]\!]$, then $w([p^{n+1}]) = w([p^n])$.

Proof. Write $[p](X) = pX + \pi X^2 f(X)$ with $f(X) \in \mathcal{O}_K[\![X]\!]$, and $[p^n](X) = \sum_{i\geq 1} a_i X^i$ with $v_p(a_i) \geq v_p(p)$. Then

$$\begin{aligned} [p^{n+1}](X) &= [p]([p^n](X)) \\ &= p[p^n](X) + \pi([p^n](X))^2 f([p^n](X)) \\ &= \sum_{i\geq 1} pa_i X^i + \left(\sum_{k\geq 2}\left(\sum_{i+j=k} \pi a_i a_j\right) X^k\right) f([p^n](X)). \end{aligned}$$

Let $d := w([p^n])$, so $v_p(a_i) > v_p(a_d) \geq v_p(p)$ for $1 \leq i \leq d-1$. From here we deduce that all the terms appeared in $G(X) := \pi([p^n](X))^2 f([p^n](X))$ will

- either have coefficient with valuation strictly greater than $v_p(pa_d)$,
- or have order strictly greater than d.

More precisely, we look at the sum $S(X) := \sum_{k\geq 2} \left(\sum_{i+j=k} \pi a_i a_j\right) X^k$. For $i+j=k \leq d$ with $i,j \in \mathbb{Z}_{\geq 1}$, $v_p(\pi a_i a_j) > v_p(a_i a_j) > v_p(pa_d)$. As $S(X) \mid G(X)$, every term of G of degree $< d$ is a sum of elements divided by some $\left(\sum_{i+j=k} \pi a_i a_j\right) X^k$ with $k < d$, so the statement holds.

Therefore $w([p^{n+1}]) = d = w([p^n])$. $\square$

By Lemma 2, if $e \in \mathbb{Z}_{\geq 1}$ is the ramification index of $K/\mathbb{Q}_p$, then $[p^n] \in \pi^n \mathcal{O}_K[\![X]\!] \subset p\mathcal{O}_K[\![X]\!]$ for all $n \geq e$. So Lemma 3 indicates that $F[p^n] = F[p^e]$ for all $n \geq e$, and $\mathrm{Tors}(F) = F[p^e]$ is finite.

4.4

By Exercise 3, the only zero of $\log_F$ in $\mathfrak{m}_{\mathbb{C}_p}$ is 0 as $\mathrm{Tors}(F) = \{0\}$. Particularly, $\log_F$ has finitely many zeros in $\mathfrak{m}_{\mathbb{C}_p}$, so $\log_F \in K \otimes_{\mathcal{O}_K} \mathcal{O}_K[\![X]\!]$. Thus there exists $d \in \mathbb{Z}$ s.t. $\pi^d \log_F \in \mathcal{O}_K[\![X]\!]$ and the Weierstrass degree of $\pi^d \log_F$ equals the number of zeros of $\log_F$ in $\mathfrak{m}_{\mathbb{C}_p}$, which is 1. Since $\log_F(X) = X +$ higher terms, we must have $d = 0$ and hence $\log_F \in \mathcal{O}_K[\![X]\!]$. Then $\log_F$ gives an isomorphism $F \xrightarrow{\sim} \mathbb{G}_\mathrm{a}$ over $\mathcal{O}_K$.

4.5

Since $K/\mathbb{Q}_p$ is unramified and F is of infinite height, $[p](X) = pX + \cdots \in p\mathcal{O}_K[\![X]\!]$. In particular, $[p](X)/p \in \mathcal{O}_K[\![X]\!]$ has Weierstrass degree 1, and the only zero of $[p](X)$ in $\mathfrak{m}_{\mathbb{C}_p}$ is 0.

For $n \geq 2$ and $z \in \mathfrak{m}_{\mathbb{C}_p}$,

$$[p^n](z) = 0 \iff [p^{n-1}](z) \in F[p] = \{0\}.$$

We can then deduce inductively that $F[p^n] = 0$ for all positive integer n. So $\mathrm{Tors}(F) = \{0\}$.