Notes on Local Fields

November 8, 2024

1 Review: Galois theory

1.1 Field Extensions

Let L/K be an algebraic extension. It is called:

- ◇ **normal**, if every polynomial $f \in K[T]$ with a root in L splits in L, $\iff$ L is the splitting field of a bunch of polynomials over K;
- ◇ **separable**, if for every element in L, its minimal polynomial over K has no multiple roots in its splitting field, $\iff$ $\gcd(f, f') = 1$;
- ◇ **Galois**, if it is normal and separable, i.e., L is the splitting field of a bunch of *seperable* polynomials over K. We put $\mathrm{Gal}(L/K) := \mathrm{Aut}_K(L)$.

Remark.

1. For a finite *normal* extension L/K, $|\mathrm{Aut}_K(L)| \leq [L : K]$, where the equality holds $\iff$ L/K is separable, i.e. Galois. This is because a K-automorphism of $L = K[T]/(f)$ just permutes the roots of f.
2. Normality is NOT transitive. As an example, take $\mathbb{Q} \subset \mathbb{Q}(\sqrt{2}) \subset \mathbb{Q}(\sqrt[4]{2})$.

1.2 Galois theory

Now let L/K be a Galois extension. Equip $\mathrm{Gal}(L/K)$ with the following **Krull topology**: $\forall \sigma \in \mathrm{Gal}(L/K)$, a basis of nbhd around σ is given by

$$\sigma\,\mathrm{Gal}(L/F), \quad \text{where } L/F/K,\ F/K < \infty \text{ \& Galois.}$$

- Two elements $\sigma, \tau \in \mathrm{Gal}(L/K)$ are "close" to each other, if $\sigma|_F = \tau|_F$ for sufficiently large finite Galois subextensions F/K.
- Both multiplication and inverse on $\mathrm{Gal}(L/K)$ are continuous for Krull topology.
- The Krull topology is profinite for L/K infinite, whence

$$\mathrm{Gal}(L/K) \simeq \varprojlim_{F/K < \infty \text{ \& Galois}} \mathrm{Gal}(F/K).$$

When $L/K < \infty$, this is the discrete topology.

- If there is a tower
$$K \subset L_1 \subset L_2 \subset \cdots \subset L,$$
where all L_n/K's are Galois, and
$$L = \bigcup_n L_n,$$
then
$$\mathrm{Gal}(L/K) = \varprojlim_n \mathrm{Gal}(L_n/K).$$

Galois theory says that the intermediate fields of L/K corresponds to the closed subgroups of $\mathrm{Gal}(L/K)$ bijectively and $\mathrm{Gal}(L/K)$-equivariantly.

$\to$: For an intermediate field F, it gives $\mathrm{Gal}(L/F) \subset \mathrm{Gal}(L/K)$. Note that L/F is Glaois, but F/K is NOT always Galois. The Galois group acts on $\{$intermediate field of $L/K\}$ via $(\sigma, F) \mapsto \sigma F = \sigma(F)$.

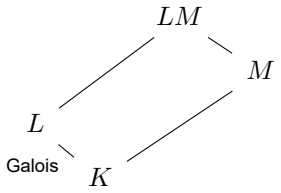
$\leftarrow$: For a closed subgroup $H < G$, it fixes a subfield $L^H \subset L$. The Galois group acts on $\{H : H < \mathrm{Gal}(L/K)\}$ by conjugation, i.e., $(\sigma, H) \mapsto \sigma H \sigma^{-1}$.

In particular,

- ◇ *Galois* extensions correspond to *normal closed* subgroups, and
- ◇ *finite* extensions correspond to *open* subgroups.

Base change

Proposition 1.1.



Let L/K be Galois. If M/K is any extension, and both L and M are subextensions of Ω/K, then LM/M is Galois, and
$$\begin{aligned} \mathrm{Gal}(LM/M) &\xrightarrow{\sim} \mathrm{Gal}(L/L \cap M) \\ \sigma &\longmapsto \sigma|_L. \end{aligned}$$

As a corollary, if L, L' are Galois subextensions of Ω/K, then LL'/K is also Galois, and
$$\begin{aligned} \mathrm{Gal}(LL'/K) &\hookrightarrow \mathrm{Gal}(L/K) \times \mathrm{Gal}(L'/K) \\ \sigma &\mapsto (\sigma|_L, \sigma|_{L'}) \square \end{aligned}$$

This embedding is an isomorphism if $L \cap L' = K$.

2 Extensions of Local Fields

2.1 Simple Extensions of DVRs

Let A be a local ring with $(\mathfrak{m},\ k)$, $f \in A[X]$ a monic polynomial of deg n. We consider the extension

$$A \to B_f := A[X]/f.$$

Let $\bar{f}$ be the image of f in $k[X] \simeq A[X]/\mathfrak{m}$ with decomposition

$$\bar{f} = \prod_i \bar{g}_i^{e_i},\ g_i \in A[X],\ \bar{g}_i \in k[X] \text{ irreducible.}$$

and

$$\bar{B}_f := B_f/\mathfrak{m}B_f \simeq A[X]/(\mathfrak{m}, f) \simeq k[X]/(\bar{f}).$$

Lemma 2.1. $\mathfrak{m}_i := (\mathfrak{m},\ g_i \bmod f) \subset B_f$ are all the distinct maximal ideals of B_f.

Proof. Denote $\pi : B_f \to \bar{B}_f$. We have $B_f/\mathfrak{m}_i \simeq \bar{B}_f/(\bar{g}_i)$, so $\mathfrak{m}_i$'s are maximal. Note that $\mathfrak{m}_i = \pi^{-1}(\bar{g}_i)$.

Take $\mathfrak{n} \in \operatorname{MaxSpec} B_f$. If $\mathfrak{n} \supset \mathfrak{m}$, then $\mathfrak{n} = \pi^{-1}\pi\mathfrak{n}$, and goes to a maximal ideal in $\bar{B}_f$ (because $\bar{B}_f/\pi\mathfrak{n} \simeq B_f/\mathfrak{n}$), so $\mathfrak{n} = \pi^{-1}(\bar{g}_i) = \mathfrak{m}_i$.

So assume that $\mathfrak{m} \not\subset \mathfrak{n}$, then $\mathfrak{n} + \mathfrak{m}B_f = B_f$.[1] Therefore

$$\frac{B_f}{\mathfrak{n}} = \frac{\mathfrak{n} + \mathfrak{m}B_f}{\mathfrak{n}} \simeq \frac{\mathfrak{m}B_f}{\mathfrak{n}}.$$

Since A is local and B_f is a f.g. A-mod, by Nakayama's lemma, we see $\mathfrak{n} = B_f$. Contradiction.

□

Now take A to be a DVR with $\mathfrak{m} = (\varpi)$ and $K = \operatorname{Frac} A$. Put $L := K[X]/(f)$. We give two cases where B_f is a DVR.

Unramified case

Let $\bar{f} \in k[X]$ be irreducible. Then B_f is a DVR with maximal ideal $\mathfrak{m}B_f$.

Corollary 2.1. $f \in A[X]$ is also irreducible, so L is a field. Moreover, B_f is the integral closure of A in L, and L/K is unramified if $\bar{f}$ is separable.

Proof. $L = K[X]/f \simeq (A[X]/f) \otimes_A K = B_f \otimes_A K$. As B_f is a domain, L is a field and $L = \operatorname{Frac} B_f$. Since A is integrally closed, B_f is also integrally closed, so B_f is the integral closure of A in L. □

Totally ramified case

Let $f \in A[X]$ be an **Eisenstein polynomial**, i.e.,

$$f = X^n + a_{n-1}X^{n-1} + \cdots + a_0,\ a_i \in \mathfrak{m},\ a_0 \notin \mathfrak{m}^2.$$

Proposition 2.1. B_f is a DVR, with maximal ideal generated by the image of X and residue field k.

[1] In this case $\mathfrak{n}/(\mathfrak{n} \cap \mathfrak{m}) \simeq \bar{B}_f$ as B_f-module, and thus $\pi^{-1}\pi\mathfrak{n} = B_f$.

Proof. Let x be the image of X in B_f. We have $\bar{f} = X^n$, so B_f is a local ring with maximal ideal $(\mathfrak{m}, x)$. Because $a_0 \in \mathfrak{m} \setminus \mathfrak{m}^2$, a_0 must uniformise $\mathfrak{m} \subset A$, and

$$-a_0 \bmod f = x^n + \cdots + (a_1 \bmod f)\, x,$$

Therefore $(\mathfrak{m}, x) = (x)$. □

Similar to Corollary 2.1, f is irreducible and L is a field with B_f the integral closure of A in L.

2.2 Hensel's Lemma

Let K be a local field, or CDVF [2].

There are many versions of Hensel's lemma. A relatively complicated one is: the decomposition of a polynomial modulo $\mathfrak{m}_K$ into *coprime* factors can be lifted to K.

Theorem 1 (Hensel's lemma)**.** Let $f \in \mathcal{O}_K[X]$, $\gamma, \eta \in k[X]$ s.t.

$$\begin{cases} \bar{f} = \gamma\eta, \\ (\gamma, \eta) = 1 \end{cases} \quad \text{in } k[X].$$

Then there exists $g, h \in \mathcal{O}_K[X]$ s.t.

$$\begin{cases} f = gh, & \text{in } \mathcal{O}_K[X], \\ \bar{g} = \gamma, \bar{h} = \eta & \text{in } k[X]. \end{cases}$$

Also the most famous ones about lifting roots in residue fields.

Theorem 2. Let $f \in \mathcal{O}_K[X]$, $\pi \in \mathfrak{m}_K$, $\alpha_0 \in \mathcal{O}_K$ s.t.

$$\begin{cases} P(\alpha_0) \in \pi O_K, \\ P'(\alpha_0) \in \mathcal{O}_L^\times. \end{cases}$$

Then $\exists!\ \alpha \in \alpha_0 + \pi\mathcal{O}_K$ s.t.

$$P(\alpha) = 0.$$

Theorem 3. Let $f \in \mathcal{O}_K[X]$, $0 \le \lambda < 1$, $\alpha_0 \in \mathcal{O}_K$ s.t.

$$|P(\alpha_0)| \le \lambda |P'(\alpha)|^2.$$

Then $\exists!\ \alpha \in \mathcal{O}_K$ s.t.

$$\begin{cases} P(\alpha) = 0, \\ |\alpha - \alpha_0| \le \lambda |P'(\alpha_0)|. \end{cases}$$

Note that in both cases, the lift is *unique*.

[2] We define a **local field** to be a complete discretely valued field, without the assumption of residue field being finite.

Proof of Hensel's lemma

We propose two kind of proofs for them. Full proof is only given to Theorem 1.

The first one is the traditional π-adic approximation.

Lemma 2.2. If k is a field, $P, Q \in k[X]$ are coprime and $R \in k[X]$, then

$$\exists A, B \in k[X], \quad R = AP + BQ \text{ s.t. } \deg A \leq \deg Q - 1.$$

Proof. Let $R = A_0 P + B_0 Q$, then $R = (A_0 - uQ)P + (B_0 + uP)Q$ are all the possibilities. By Euclidean division, dividing A_0 by Q gives us $u \in k[X]$ with $\deg(A_0 - uQ) \leq \deg Q - 1$. □

Proof of Theorem 1. Let π be a uniformiser. Take a lift g_1 of γ with $\deg g_1 = \deg \gamma$, and a lift h_1 of η with $\deg h_1 = \deg \eta$. We seek for : $\{g_n\}_n, \{h_n\}_n \subset \mathcal{O}_K[X]$ s.t.

$$f \equiv g_n h_n \bmod \pi^n, \quad g_{n+1} = g_n + \pi^n y_n, \ h_{n+1} = h_n + \pi^n z_n.$$

In order $\lim_n g_n, \lim_n h_n \in \mathcal{O}_K[X]$, we require $\deg y_n \leq \deg \gamma$, $\deg z_n \leq \deg \eta$.

Assume we have found $g_n h_n \equiv f \bmod \pi^n$, then we need

$$\begin{aligned} f &\equiv (gn + \pi^n y_n)(h_n + \pi^n z_n) \equiv g_n h_n + \pi^n (g_n z_n + h_n y_n) && \bmod \pi^{n+1} \\ \implies \mathcal{O}_K[X] &\ni \frac{f - g_n h_n}{\pi^n} \equiv g_n z_n + h_n y_n \equiv \gamma z_n + \eta y_n && \bmod \pi. \end{aligned}$$

Via Lemma 2.2, we find $z_n, y_n \in \mathcal{O}_K[X]$ with

$$\deg y_n \leq \deg \gamma - 1, \implies \deg z_n \leq \deg f - \deg \eta.$$ □

Another proof uses the *fixed point theorem*

Lemma 2.3 (Fixed point theorem)**.** Let C be a complete metric space, $f : C \to C$ a **contracting map**, i.e,

$$\exists \alpha, 0 \leq \alpha < 1 \text{ s.t. } |f(x) - f(y)|^3 < \alpha |x - y|, \ \forall x, y \in C.$$

Then f has a *unique* fixed point in C.

Recall that the $K[X]$ is equipped with the **Gauss nrom**: for $f = \sum_{i=0}^n a_i X^i$,

$$|f| := \max\{a_0, \ldots, a_n\}.$$

(T.B.C.)

2.3 Extending the norm

Let K be a complete normed field[4]. Consider an algebraic extension L/K, we wonder if the norm extend to L.

Recall: two norms $|\cdot|_1$ and $|\cdot|_2$ on a K-vector space V are **equivalent**

[3] Not a right notation, but anyway.

[4] By a **complete normed field** K, we always require an *ultrametric / nonarchimedean* norm $|\cdot|_K$. The norm corresponds to a valuation $\mathrm{val} : K \to \mathbb{R} \cup \{\infty\}$ by $\mathrm{val}(x) = -\log_a |x|$ for any chosen $a \in \mathbb{R}_{\geq 1}$, which is not necessarily discrete. Then

$$K \text{ is a local field} \iff \mathfrak{m}_K \text{ is a principal ideal} \iff \mathrm{val}(K^\times) \text{ is a discrete subgroup of } \mathbb{R}.$$

$$:= \text{they give the same topology}$$

$$\iff (|x_n|_1 \to 0 \iff |x_n|_2 \to 0).$$

Proposition 2.2. If $|\cdot|_1$ and $|\cdot|_2$ are two equivalent norms on K, then

$$\exists \alpha > 0, \quad |\cdot|_1 = |\cdot|_2^\alpha$$

Proof. ($\Longleftarrow$) Assume $|\cdot|_1 \sim |\cdot|_2$.

- Let $y \in K$. $|y^n|_i \to 0 \iff |y|_i < 1$,

$$\implies (|y|_1 < 1 \iff |y|_2 < 1).$$

Fix $y \in K^\times$ with $|y|_1 \neq 1$. Then $|y|_2 \neq 1$.

- Let $x \in K$. By previous computation,

$$\begin{aligned}
&|x^m y^{-n}|_1 < 1 \iff |x^m y^{-n}|_2 < 1, && \forall m, n \in \mathbb{Z}, \\
\implies &|x|_1 < |y|_1^r \iff |x|_2 < |y|_2^r, && \forall r \in \mathbb{Q}, \\
\implies &|x|_1 < |y|_1^s \iff |x|_2 < |y|_2^s, && \forall s \in \mathbb{R} \\
\implies &|x|_2 = |x|_1^\alpha.
\end{aligned}$$

where $\alpha > 0$ is determined by $|y_2| = |y_1|^\alpha$. □

Theorem 4 (Artin)**.** Let K be complete normed field, V a f.d.K-vector space. Then all norms on V are equivalent, and V is complete for them.

Note that we don't require K to be locally compact; as a price, the norm on V need to be ultrametric too (which is our convention).

Proof. Let $e_1, \ldots, e_d$ be a K-basis of V, $\|\cdot\|_\infty$ the corresponding sup-norm. The sup-norm is complete. Then we do induction on d to show $\|\cdot\| \sim \|\cdot\|_\infty$ for any norm $\|\cdot\|$. Omitted. □

Corollary 2.2. Let K is a complete normed field, $L/K < \infty$. If the norm on K extends to a norm on L, then their is at most one way to do so, and L will be complete.

Proof. All such norm will be $|\cdot|^\alpha$ for a fixed norm $|\cdot|$. These norms coincide on K, so $\alpha = 1$. □

In case of complete *discretely valued* fields, there is indeed such an extension.

Theorem 5. Let K is a local field, $L/K < \infty$. Then there the norm on K extends uniquely to L, making L also a local field. The norm is given by

$$|x|_L = \left|N_{L/K}(x)\right|_K^{1/[L:K]},$$

and $\mathcal{O}_L =$ integral closure of $\mathcal{O}_K$ in L.

We give two proofs.

Proof (algebraic). Recall that:

Lemma 2.4. If A is a Dedekind, $L/\operatorname{Frac}(A) < \infty$, B is the integral closure of A in L, then: B is a Dedekind domain.

Apply this to $A = \mathcal{O}_K$, we see that $B :=$ integral closure of $\mathcal{O}_K$ in L is a Dedekind domain. Let

$$\mathfrak{m}_K B = \mathfrak{P}_1^{e_1} \cdots \mathfrak{P}_r^{e_r}$$

be the decomposition of $\mathfrak{m}_K$ in B. Define $v_i(x) :=$ exponent of $\mathfrak{P}_i$ in xB. One verifies that $v(\cdot)/e_i$ extends the valuation v_K on K with value group $\mathbb{Z}$. The uniqueness forces $r = 1$, and $\mathcal{O}_L = \{x \in L \mid v_i(x) > 0\} = B$. □

Another proof gives the explicit formula for the norm. We need a result on integrality.

Proposition 2.3. Let K be a local field, $P(X) = a_d X^d + a_{d-1} X^{d-1} + \cdots + a_0 \in K[X]$ an irreducible polynomial with $a_0 a_d \neq 0$. Then the Gauss norm of f is

$$|f| = \max\{|a_0|, |a_d|\}.$$

In particular, if f is monic and its constant term $a_0 \in \mathcal{O}_K$, then $P(X) \in \mathcal{O}_K[X]$.

Proof. Let $n \in \mathbb{Z}$ s.t. $\pi^n P \in \mathcal{O}_K[X]$ and $\overline{\pi^n P} \neq 0 \in k[X]$. Let r be the Weierstrass degree of $\pi^n P$,so that

$$\pi^n P(X) \bmod \pi = \pi^n X^r (a_r + a_{r+1} X + \cdots + a_d X^{d-r}).$$

If $0 < r < d$, then the decomposition lift to a nontrivial decomposition of $\pi^n P$ in $K[X]$ via Theorem 1. Therefore $r = 0$ or $r = d$. Now nate that $|f| = |a_r|$. □

Proof of Theorem 5 (analytic). Let $d := [L : K]$. We show that $|\cdot|_L := |N_{L/K}(\cdot)|_K^{1/d}$ is indeed a norm on L (it obviously extends $|\cdot|_K$). The only nontrivial step is to check the strong triangle inequality, which is equivalent to

$$|z|_L < 1 \implies |1 + z|_L < 1.$$

Let $P(X)$ be the minimal polynomial of z over K. Since $N_{L/K}(z) = (-1)^d P(0)^{[L:K(z)]}$[5], so by Section 2.3,

$$|z| \leq 1 \iff P(0) \in \mathcal{O}_K[X] \implies \text{minimal polynomial of } z + 1 \in \mathcal{O}_K[X] \implies |1 + z| \leq 1.$$ □

Corollary 2.3. Let K be a local field.

(1) The norm on K extends uniquely to its algebraic closure K^{alg}[6].

(2) If L and L' are two algebraic extension of K, then any K-embedding $\sigma \in \text{Hom}_K(L, L')$ preserves the norm; i.e., $|\sigma(x)|_{L'} = |x|_L$.

2.4 Unramified Extensions of Local Fields

Let K be a local field (i.e., CDVF). We assume further that both K and its residue field $k = \mathcal{O}_K/\mathfrak{m}$ are perfect.

The slogan is that unramified extensions are just extensions of residue fields. Using Hensel's lemma, an extension $k(a)/k$ can be lifted to a unique extension $K(\alpha)/K$ over K with

$$\text{Gal}(K(\alpha)/K) \simeq \text{Gal}(k(a)/k).$$

Moreover, given an extension L/K, there is a maximal unramified subextension K_0 in L containing every unramified extensions.

Now we assume k to be finite. Then adjoining roots of unities with order coprime to $p = \text{char}\, k$ gives all finite unramified extensions of K.

[5] Simple fact, see Lemma 4.5.

[6] Note that K^{alg} is not a local field and not complete. We'll see this later.

Example 1. Let $K/\mathbb{Q}_p < \infty$ and $k = \mathbb{F}_q$. Then the unique extension of k of degree n is the splitting field of $X^{q^n} - X$ over k, which equals $k(\mu_{q^n-1})$ once we fix an algebraic closure of k. So the unramified extension K_n/K of degree n is the splitting field of $X^{q^n} - X$ over K, i.e.,

$$K_n = K(\mu_{q^n-1}).$$

The Galois group $\mathrm{Gal}(K_n/K)$ is generated by Frob_K, which is determined by

$$\mathrm{Frob}_K\, \beta \equiv \beta^q \mod \varpi,\ \forall \beta \in \mathcal{O}_{K_n}$$

for any uniformiser ϖ (simultaneously of K and K_n).

What if we adjoin ζ_m to K where m is an arbitary integer prime to p? The answer is that $K(\mu_m)$ is unramified of degree the smallest positive integer f s.t. $m \mid p^f - 1$, by the following Lemma 2.5 on finite fields.

Lemma 2.5. Let ζ_n be a primitive n-th root of unity over $\mathbb{F}_q$ with q, n coprime. Then $[\mathbb{F}_q(\zeta_n) : \mathbb{F}_q]$ is the smallest integer $f > 0$ s.t. $n \mid q^f - 1$.

Proof. Because $\mathrm{char}\, \mathbb{F}_q \nmid n$, the primitive root ζ_n exists and $\mathbb{F}_q(\zeta_n)$ is the splitting field of $X^n - 1$ over $\mathbb{F}_q$. The degree $f = [\mathbb{F}_q(\zeta_n) : \mathbb{F}_q]$ is the order of Frob_q on $\mathbb{F}_q(\zeta_n)$, i.e., f is the smallest integer s.t.

$$\mathrm{Frob}_q^f(\zeta_n) = \zeta_n^{q^f} = \zeta_n.$$

The definition of primitive root of unity says that

$$\zeta_n^{q^f-1} = 1 \iff n \mid q^f - 1. \qquad \square$$

2.5 Newton Polygon

Let K be a local field with valuation val extended to K^{alg}.

For $P = a_0 + a_1 X + \cdots + a_d X^d \in K[X]$, the **Newton polygon** of $P := \mathrm{NP}(P) :=$ convex hull of points

$$(0, \mathrm{val}(a_0)), (1, \mathrm{val}(a_1)), \ldots, (d, \mathrm{val}(a_d)).$$

- $\mathrm{NP}(P)$ is a union of linked segments with increasing slopes.
- **length of a segment** := its length along x-axis.

Theorem 6. The number of roots of P in K^{alg} with valuation λ = the length of $\mathrm{NP}(P)$ with slope $-\lambda$.

2.6 Ramification Groups

Let K be a CDVF with perfect residue field k, $L/K < \infty$ Galois. We will study the Galois group

$$G := \mathrm{Gal}(L/K)$$

by giving filtrations on it.

2.7 Krasner's lemma and the noncompleteness of $\bar{\mathbb{Q}}_p$

Fix an algebraic closure $\bar{\mathbb{Q}}_p = \mathbb{Q}_p^{\text{alg}}$ of $\mathbb{Q}_p$. Krasner's lemma states that if $\beta \in \bar{\mathbb{Q}}_p$ is closer to $\alpha \in \bar{\mathbb{Q}}_p$ than any other conjugate of α over F, then $\alpha \in F(\beta)$. Therefore, if two polynomials are "close enough", they will give the same extension.

Theorem 7 (Krasner's lemma)**.** Let $F/\mathbb{Q}_p < \infty$, $\alpha, \beta \in \bar{\mathbb{Q}}_p$. If

$$|\alpha - \beta| < |\alpha - \alpha_i|, \quad i = 2, \dots, n,$$

where $\alpha_1 = \alpha, \alpha_2, \dots, \alpha_n$ are all the conjugates of α over F, then

$$F(\alpha) \subset F(\beta).$$

Proof. Let K/F be finite Galois with $\alpha, \beta \in K$. Then $g\alpha, g \in \text{Gal}(K/F)$ are all the conjugates of α over F. Now if $g \in \text{Gal}(K/F(\beta))$, then

$$\begin{aligned} |g\alpha - \alpha| &= |(g\alpha - g\beta) + (\beta - \alpha)| \\ &\leq \min\{|g\alpha - g\beta|, |\alpha - \beta|\} = [7]|\alpha - \beta| \end{aligned}$$

So by the assumption, we have $\alpha = g\alpha$, i.e., $\alpha \in K^{\text{Gal}(K/F(\beta))} = F(\beta)$. □

Theorem 8. For every $d \geq 1$, $\mathbb{Q}_p$ has only finitely many extensions of degree d.

Proof. Every finite extension has a unique maximal unramified extension, so it suffices to show that: there is only finitely many unramified extensions of each $F/\mathbb{Q}_p < \infty$ of given degree e.

For $e \geq 1$, the set of Eisenstein polynomials over F is in bijection with

$$\Pi := (\mathfrak{m}_F \setminus \mathfrak{m}_F^2) \times \underbrace{\mathfrak{m}_F \times \cdots \times \mathfrak{m}_F}_{e-1},$$

which is compact. So we just need to show that for each Eisenstein polynomial P, its corresponding point in Π has a neighbourhood, in which all polynomials give the same extension.

(T.B.C.) □

Corollary 2.4. $\bar{\mathbb{Q}}_p$ is not complete.

Proof. Now we know $\bar{\mathbb{Q}}_p$ is a countable union of finite dimensional $\mathbb{Q}_p$-vector spaces. Recall what Baire's theorem says:

Theorem 9 (Baire category theorem)**.** A complete metric space is a Baire space; i.e, a countable intersection of open dense sets is dense.

As a corollary, a complete metric space is not a countable union of nowhere dense[8] sets.

A finite dimensional $\mathbb{Q}_p$-vector space is closed and nowhere dense, so the union is not complete. □

Let $\mathbb{C}_p := \widehat{\bar{\mathbb{Q}}_p}$ be the completion of $\bar{\mathbb{Q}}_p$. Note that neither reidue field nor value group are not extended from $\bar{\mathbb{Q}}_p$ to $\mathbb{C}_p$:

- $v_p(\mathbb{C}_p) = v_p(\bar{\mathbb{Q}}_p) = \mathbb{Q}$[9].

[7] Because embeddings of finite extensions of $\mathbb{Q}_p$ are isometries (the uniqueness of norm extension).

[8] Being **nowhere dense** means its closure has empty interior.

[9] Consider a Cauchy sequence $\{a_n\}_n$ in $\bar{\mathbb{Q}}_p$. The difference $a_m - a_{m+d}$ will eventually have valuation $> v_p(a_m)$, making $v_p(\lim_n a_n) = v_p(a_m)$.

- $k_{\mathbb{C}_p} = \mathcal{O}_{\mathbb{C}_p}/\mathfrak{m}_{\mathbb{C}_p} \simeq \mathcal{O}_{\bar{\mathbb{Q}}_p}/\mathfrak{m}_{\bar{\mathbb{Q}}_p} \simeq \mathbb{F}_p^{\mathrm{alg}}$.[10]

Theorem 10. $\mathbb{C}_p$ is algebraically closed.

Proof. The idea is simple: root of lim of polynomial = lim of root of polynomial. Let's make this clear.

Let $P \in \mathbb{C}_p[X]$ be monic of degree d. Replacing $P(X)$ by $p^{kd}P(p^{-k}X)$ for $k \gg 0$, we may assume $P \in \mathcal{O}_{\mathbb{C}_p}[X]$.

□

2.8 Ax-Sin-Tate theorem and closed subfields of $\mathbb{C}_p$

Let $\mathbb{Q}_p \subset K \subset \bar{\mathbb{Q}}_p$, $G_K := \mathrm{Gal}(\bar{\mathbb{Q}}_p/K)$ the absolute Galois group of K. Galois theory eastablishes a bijection

$$\{\text{subextension of } \bar{\mathbb{Q}}_p/\mathbb{Q}_p\} \longleftrightarrow \{\text{closed subgroup of } \mathrm{Gal}(\bar{\mathbb{Q}}_p/\mathbb{Q}_p)\}$$

via $K = \bar{\mathbb{Q}}_p^{G_K}$. We are going to expand this relation to (certain) subextensions of $\mathbb{C}_p/\mathbb{Q}_p$.

Any $g \in \mathrm{Gal}(\bar{\mathbb{Q}}_p/\mathbb{Q}_p)$ is an isometry, thus extends to an isometry and (continuous) field automorphism of $\mathbb{C}_p$, denoted still by g. So what is $\mathbb{C}_p^{G_K}$?

Theorem 11 (Ax-Sin-Tate)**.** $\mathbb{C}_p^{G_K} = \widehat{K}$.

Lemma 2.6. Let $P(X) \in \bar{\mathbb{Q}}_p[X]$ be monic of degree n, s.t. all the roots α of P have bounded valuation bounded from below; i.e., $v_p(\alpha) > c$ for some $c \in \mathbb{R}$. Let $n = p^k d$ with $p \nmid d$ or $p = d$. Then $P^{(p^k)}$ has a root β with

$$\begin{cases} v_p(\beta) \geq c, & n = p^k d, p \nmid d, \\ v_p(\beta) \geq c - \dfrac{1}{p^k(p-1)}, & n = p^{k+1}. \end{cases}$$

Proof. Write $P(X) = X^n + a_{n-1}X^n + \cdots + a_0$, and $q := p^k$.

- $v_p(a_i) \geq (n-i)c$, because $a_i = \pm$ sum of product of $n-i$ roots.
-

□

3 A Bit of p-adic Analysis

In this section, we consider some basic properties concerning powerseries over a closed subfield K of $\mathbb{C}_p$ as functions.

Let $f(X) = \sum_{i \geq 0} a_i X^i \in K[\![X]\!]$. We can evaluate f at $z \in \mathbb{C}_p$ iff $a_i z^i \to \infty$, so the **radius of convergence** is

$$\rho(f) := \sup\{\rho \in \mathbb{R} \mid a_i \rho^i \to \infty (i \to \infty)\}.$$

- If $|z| < \rho(f)$, then $f(z)$ converges in $\mathbb{C}_p$.
- If $|z| > \rho(f)$, then f diverges.
- $\rho(f(\alpha X)) = \rho(f) \cdot |\alpha|^{-1}$.

[10] In a sum $\sum_n a_n \in \mathbb{C}_p$, a.e. $a_n \in \mathfrak{m}_{\mathbb{C}_p}$.

We are mainly interested in the power series converging on the unit disk, i.e.,

$$\begin{aligned} H_K &:= \{f \in K[\![X]\!] \mid \rho(f) > 1\} \\ &= \{f \in K[\![X]\!] \mid a_i \rho^i \to 0, \forall \rho < 1\} \\ &= \{f \in K[\![X]\!] \mid f \text{ converges on the open unit disk } \mathfrak{m}_{\mathbb{C}_p} = B(0,1)\}. \end{aligned}$$

Example 2. $K \otimes_{\mathcal{O}_K} \mathcal{O}_K[\![X]\!]$ = power series over K with bounded coefficients $\subsetneq H_K$.

Example 3. $\log(1+X) = \log_{\mathbb{G}_\mathfrak{m}}(X) = X - \dfrac{X^2}{2} + \dfrac{X^3}{3} - \cdots \in H_K \setminus K \otimes_{\mathcal{O}_K} \mathcal{O}_K[\![X]\!]$.

3.1 The Gauss Norm

Theorem 12. Let $f(X) = \sum_{i\geq 0} a_i X^i \in K[\![X]\!]$ with $\rho(f) > 0$, a real number $\rho < \rho(f)$ s.t. $\rho \in |\mathbb{C}_p^\times|$. Then $\sup_{i\geq 1} |a_i|\rho^i$ is a maximum (i.e., $\sup_{i\geq 1} |a_i|\rho^i = |a_j|\rho^j$ for some j), and

$$\sup_{i\geq 1} |a_i|\rho^i = \sup_{|z|=\rho} |f(z)| =: |f|_\rho.$$

Proof.

- $\rho < \rho(f) \implies |a_i|\rho^i \to 0 \implies \sup_{i\geq 0} |a_i|\rho^i$ is a maximum.
- $|f(z)| = \left|\sum_{i\geq 0} a_i z^i\right| \leq \sup_{i\geq 1} |a_i||z|^i$, so $|f|_\rho \leq \sup_{i\geq 1} |a_i|\rho^i$.
- Take $\alpha \in \mathbb{C}_p$ with $|\alpha| = \rho$, and $j \in \mathbb{Z}_{\geq 0}$ s.t. $\sup_{i\geq 1} |a_i|\rho^i = |a_j|\rho^j$. Let $\beta := a_j \alpha^j$. We aim to find $|z| = \rho$ s.t. $|f(z)| = |\beta|$. Consider
$$g(X) = \sum_{i\geq 0} g_i X^i := \frac{f(\alpha X)}{\beta} \in \mathcal{O}_{\mathbb{C}_p}[\![X]\!].$$
Moreover, the coefficients $g_i = \dfrac{a_i \alpha^i}{\beta} \to 0$ as $i \to \infty$, because $|g_i| = \beta^{-1}|a_i|\rho^i$. So $\bar{g}(X) \in k_{\mathbb{C}_p}[\![X]\!]$ is actually a polynomial, and it is nonzero since $|g_j| = 1$. Take $\bar{w} \in \bar{k}^\times$ s.t. $\bar{g}(\bar{w}) \neq 0$. Then a lift $w \in \mathcal{O}_{\mathbb{C}_p}^\times$ verifies $|g(w)| = 1$. Hence $|f(\alpha w)| = |\beta|$ and $|\alpha w| = |\alpha| = \rho$. □

Thus, the expression $|f|_\rho \in \mathbb{R} \cup \{+\infty\}$ is defined on $\rho \in \mathbb{R}$. In addition,

- $\rho \to |f|_\rho$ is continuous,
- $|f|_\sigma \leq |f|_\rho$ if $\sigma \leq \rho < \rho(f)$.

$\implies$ the **maximum modulus principle** holds: $|f|_\rho = \sup_{|z|\leq\rho} |f(z)| = \max_{|z|\leq\rho} |f(z)|$ for $\rho < \rho(f)$.

- $|\cdot|_\rho$ is multiplicative: $|fg|_\rho = |f|_\rho |g|_\rho$.

Example 4. If $f \in H_K$, then *as a function*:

- f is bounded on $\mathfrak{m}_{C_p} \iff f \in K \otimes_{\mathcal{O}_K} \mathcal{O}_K[\![X]\!]$,
- f is bounded by 1 on $\mathfrak{m}_{\mathbb{C}_p} \iff f \in \mathcal{O}_K[\![X]\!]$.

3.2 Weierstrass Preparation Theorem

For $f(X) = \sum_{i\geq 0} a_i X^i \in \mathcal{O}_K[\![X]\!]$, we define its **Weierstrass degree** := wideg(f) := smallest $i \in \mathbb{Z}_{\geq 0}$ s.t. $a_i \in \mathcal{O}_K^\times$.

- wideg is multiplicative.
- wideg$(f) = \infty \iff f \in \mathfrak{m}_K[\![X]\!]$.
- wideg$(f) = 0 \iff a_0 \in \mathcal{O}_K \times \iff f \in (\mathcal{O}_K[\![X]\!])^\times$.
- If $K/\mathbb{Q}_p < \infty$, then for $f \in K \otimes_{\mathcal{O}_K} \mathcal{O}_K[\![X]\!]$, $\exists! n \in \mathbb{Z}$ s.t. $\pi^n f$ has finite Weierstrass degree, which is the smallest degree of the term in f with minimum valuation (maximum norm).

Remark. The last statement fails if K is not finite over $\mathbb{Q}_p$, i.e., if there is no uniformiser. For example, $f(X) = \sum_{i\geq 1} \frac{1}{p^i} X^i$.

From now on, assume $K/\mathbb{Q}_p < \infty$ with uniformiser π.

Proposition 3.1 (Euclidean Division)**.** Let $f \in \mathcal{O}_K[\![X]\!]$ with wideg$(f) < \infty$. Then: $\forall g \in \mathcal{O}_K[\![X]\!]$, $\exists! q \in \mathcal{O}_K[\![X]\!]$ & $r \in \mathcal{O}_K[X]$[11] s.t.

$$g = q \cdot f + r, \ \deg(r) \leq \text{wideg}(f) - 1.$$

Proof. Idea is, again, π-adic approximation.

First we do "Euclidean division" in $k[\![X]\!]$. Write $\bar{f}(X) = X^n f_0(X)$ with $f_0(X) \in k[\![X]\!]^\times$. For $h = \sum_{i\geq 0} h_i X^i \in k[\![X]\!]$, it decomposes as

$$h = X^n s + r, \text{ with } r = h_0 + \cdots + h_{n-1} X^{n-1}$$

$$\implies h = q \cdot f + r, \text{ where } q = s \cdot f_0^{-1}.$$

Therefore,

$$\begin{aligned} g &= q_0 f + r_0 + \pi g_1 && \text{with } \deg r_0 \leq n-1, \\ &= (q_0 + \pi q_1) f + (r_0 + \pi r_1) + \pi^2 g_2 && \text{with } \deg r_1 \leq n-1 \\ &= \cdots \\ \implies g &= qf + r, && \text{with } q = \sum_{i\geq 0} \pi^i q_i, r = \sum_{i\geq 1} \pi^i r_i. \end{aligned}$$

Unicity. If $qf + r = 0$, then $\underbrace{\bar{q}\bar{f}}_{\text{divided by } X^n} + \underbrace{\bar{r}}_{\deg \leq n-1} = 0$, so $\bar{q}\bar{f} = \bar{r} = 0$. Deduce inductively mod π^n. □

Remark. Jiang Jiedong provided a proof for this theorem when K is not finite over $\mathbb{Q}_p$.

For a polynomial $P(X) \in \mathcal{O}_K[X]$, we say $P(X)$ is **distinguished**, if it is monic with other coefficients in $\mathfrak{m}_K$, i.e,

$$P(X) = X^n + a_{n-1} X^{n-1} + \cdots + a_0, \quad a_{n-1}, \ldots, a_0 \in \mathfrak{m}_K.$$

- The Newton polygon of a distinguished polynomial P will be above x-axis with only the end point on x-axis, and all slopes are < 0. So every root of P lies in $\mathfrak{m}_{\mathbb{Q}_p^{\text{alg}}}$.

[11] The residue $r(X)$ is a polynomial!

Theorem 13 (Weierstrass Preparation Theorem)**.** Let $f \in \mathcal{O}_K[\![X]\!]$ with wideg $f < \infty$.

Then $\exists!$ distinguished polynomial $P \in \mathcal{O}_K[\![X]\!]$ with $\deg P = \text{wideg } f$, s.t.

$$f(X) = P(X) \cdot u(X), \quad u \in (\mathcal{O}_K[\![X]\!])^\times.$$

So, power series over K with bounded coefficients would have finitely many zeros in the unit disk.

Corollary 3.1. Let $f(X) \in K \otimes_{\mathcal{O}_K} \mathcal{O}_K[\![X]\!]$.

1. $f(X) = \pi^\mu P(X)u(X)$ uniquely, where $\mu \in \mathbb{Z}$, P a distinguished polynomial, $u \in (\mathcal{O}_K[\![X]\!])^\times$.
2. f has finitely many zeros in $\mathfrak{m}_{\mathbb{C}_p}$, and they are actually in $\mathfrak{m}_{\mathbb{Q}_p^{\text{alg}}}$. The number of zeros is $\text{wideg}(\pi^{-\mu} f) = \deg P$[12]. □

Corollary 3.2. $K \otimes_{\mathcal{O}_K} \mathcal{O}_K[\![X]\!]$ is a PID.

Proof. For $I = (\{f_i\}_i)$, write $f_i = \pi^{\mu_i} P_i u_i$, then $I = (\gcd_i(P_i))$. □

Theorem 14. Let $f \in H_K$, $\rho < 1$. Then f has finitely many zeros in $B(0, \rho)$, all of which are in $\mathfrak{m}_{\mathbb{Q}_p^{\text{alg}}}$.

Remark. $f \in H_K$ *could* have infinitely many zeros in $\mathfrak{m}_{\mathbb{C}_p} = B(0, 1)$. For example, we saw in the homework that the zeros of $\log_F$ in $\mathfrak{m}_{\mathbb{C}_p}$ are $F[p^\infty]$, which is infinite in many cases, such as $F = \mathbb{G}_{\mathfrak{m}}$.

Proof. We may assume $\rho \in |\mathbb{C}_p|$.

Take $L/\mathbb{Q}_p < \infty$ and $\alpha \in \mathfrak{m}_L$ with $|\alpha| = \rho$. Then $f(\alpha X) \in L \otimes_{\mathcal{O}_L} \mathcal{O}_L[\![X]\!]$, because $|a_i|\rho^i \to 0$ for $f = \sum a_i X^i \in H_K$. Hence $f(\alpha X)$ has finitely many zeros in $\mathfrak{m}_{\mathbb{C}_p} = B(0, 1)$ and they are algebraic over $\mathbb{Q}_p$. These zeros are in bijection with zeros of $f(X)$ in $B(0, \rho)$. □

Now we can prove the converse of Corollary 3.1.

Theorem 15. If $f \in H_K$, then

$$f \in K \otimes_{\mathcal{O}_K} \mathcal{O}_K[\![X]\!] \iff f \text{ has finitely many zeros in } \mathfrak{m}_{\mathbb{C}_p}.$$

Proof. ($\Longleftarrow$) Assume that $f = \sum_{i \geq 0} f_i X^i$ has n zeros in $\mathfrak{m}_{\mathbb{C}_p}$.

Take $\rho \in \mathfrak{m}_{\mathbb{C}_p}$ and $\alpha \in \mathfrak{m}_{\mathbb{Q}_p}$ with $|\alpha| = \rho$. By previous results,

$$\begin{aligned} \#\{\text{zero of } f \text{ in } B(0,\rho)\} &= \text{“Weierstrass degree” of } f(\alpha X) \\ &= \min\left\{ j \in \mathbb{Z}_{\geq 0} \,\middle|\, \rho^j |f_j| = \max_{i \in \mathbb{Z}_{\geq 0}} \rho^i |f_i| \right\}. \end{aligned}$$

Hence

$$\begin{aligned} &\min\left\{ j \in \mathbb{Z}_{\geq 0} \,\middle|\, \rho^j |f_j| = \max_{i \in \mathbb{Z}_{\geq 0}} \rho^i |f_i| \right\} \leq n, \\ \iff &\rho^i |f_i| \leq \max\left\{ |f_0|, \rho|f_1|, \ldots, \rho^n |f|_n \right\}, \ \forall i \geq 0. \end{aligned}$$

Letting $i \to \infty$ tells us that the coefficients of f are bounded. □

3.3 p-adic Banach Spaces

Let $K/\mathbb{Q}_p < \infty$ with uniformiser π, $k := \mathcal{O}_K/\pi$.

[12] I want to call this “the Weierstrass degree of f”.

4 Lubin-Tate Theory

4.1 Formal Groups

In this section, a formal group means a commutative formal group law of dimension one. If $f \in A[\![T]\!]$ and $g \in A[\![X_1, \dots, X_n]\!]$, then

$$f \circ g := f(g(X_1, \dots, X_n)),$$
$$g \circ f := g(f(X_1), \dots, f(X_n)).$$

Lemma 4.1. Let $f = \sum_{i \geq 1} a_i T^i \in A[\![T]\!]$. Then

$$\exists g \in A[\![T]\!] \text{ s.t. } f \circ g = g \circ f = T \iff a_1 \in A^\times.$$

Proof. Use $A[\![T]\!] = \varprojlim A[T]/T^n$. For details, see the proof of Lemma 4.2. □

4.2 Lubin-Tate formal groups

From now on, we write $A := \mathcal{O}_K$.

Choose a uniformiser ϖ of K. Define

$$\mathcal{F}_\varpi := \left\{ f \in \mathcal{O}_K[\![T]\!] \;\middle|\; \begin{array}{ll} f(T) \equiv \varpi T & \text{mod } T^2 \\ f(T) \equiv T^q & \text{mod } \varpi \end{array} \right\}.$$

For example, $f(T) = T^q + \varpi T \in \mathcal{F}_\varpi$. The following lemma is a fundamental property of $\mathcal{F}_\varpi$.

Lemma 4.2. Let $f, g \in \mathcal{F}_\varpi$, Φ_1 be a linear form[13] over $\mathcal{O}_K$. Then there is a **unique** $\Phi \in \mathcal{O}_K[\![X_1, \dots, X_n]\!]$, s.t.

$$\begin{cases} \Phi \equiv \Phi_1 \mod (X_1, \dots, X_n)^2, \\ f(\Phi(X_1, \dots, X_n)) = \Phi(g(X_1), \dots, g(X_n)). \end{cases}$$

Proof. We use a standard method. Finding Φ is equivalent to finding $\Phi_r \in A[X_1, \dots, X_n]$ s.t.

$$\begin{cases} \Phi_{r+1} \equiv \Phi_r & \text{mod } (\deg \geq r+1), \\ f(\Phi_r) \equiv \Phi_r(g(X_1), \dots, g(X_n)) & \text{mod } (\deg \geq r+1). \end{cases}$$

The second condition is guaranteed because $X \mapsto h(X)$ is X-adically continuous for any power series h.

Suppose we have found Φ_r. We look for Φ_{r+1} of the form $\Phi_{r+1} = \Phi_r + Q$, where Q is homogeneous of degree $r+1$, s.t.

$$f(\Phi_{r+1}) \equiv \Phi_{r+1}(g(X_1), \dots, g(X_n)) \mod \deg \geq r+2.$$

The LHS is

$$f(\Phi_r) + f(Q) \equiv f(\Phi_r) + \varpi Q \mod \deg \geq r+2,$$

while the RHS is

$$\Phi_r \circ g + Q(\varpi X_1, \dots, \varpi X_n) \equiv \Phi_r \circ g + \varpi^{r+1} Q,$$

so if such a $Q \in A[X_1, \dots]$ exists, it must satisfy

$$\varpi(\varpi^r - 1)Q \equiv f \circ \Phi_r - \Phi_r \circ g \mod \deg \geq r+2$$

[13] A **linear form** is a homogeneous polynomial of degree 1.

and thus being unique. This procedure also shows that all Φ_r's are unique if we require $\Phi_{r+1} - \Phi_r$ to be homogeneous.

Because $\varpi^r - 1 \in A^\times$, it suffices to show

$$f(\Phi_r) \equiv \Phi_r \circ g \mod \varpi,$$

which is clear. □

By Lemma 4.2, one may define the **Lubin-Tate formal groups**. They are exactly the formal group laws admitting an endomorphism

- that has derivative at the origin equal to a uniformiser of K, and
- reduces mod $\mathfrak{m}$ to the Frobenius map $T \mapsto T_q$.

Moreover, these formal groups admit $\mathcal{O}_K$-actions and are isomorphic as formal $\mathcal{O}_K$-modules.

Proposition 4.1. For each $f \in \mathcal{F}_\varpi$, there is a unique formal group F_f over $\mathcal{O}_K$ admitting f as an endomorphism.

Proof. Lemma 4.2 gives $F_f \in A[\![X, Y]\!]$ s.t.

$$\begin{cases} F_f = X + Y + \text{deg} \geq 2, \\ f(F_f(X + Y)) = F_f(f(X), f(Y)). \end{cases}$$

The associativity is proved by showing that both $G_1 = F_f(X, F_f(Y, Z))$ and $G_2 = F_f(F_f(X, Y), Z)$ satisfies

$$\begin{cases} G = X + Y + Z + \text{deg} \geq 2, \\ f(G) = G(f(X), f(Y), f(Z)). \end{cases}$$

This is a direct application of Lemma 4.2 and will be used many times. □

So Lubin-Tate formal groups exist. Now we investigate their homomorphisms.

Proposition 4.2. For each $f, g \in \mathcal{F}_\varpi$ and $a \in \mathcal{O}_K$, there is a unique $[a]_{g,f} \in \mathcal{O}_K[\![T]\!]$ s.t.

$$\begin{cases} [a]_{g,f} = aT + \dots, \\ g \circ [a]_{g,f} = [a]_{g,f} \circ f, \end{cases}$$

and $[a]_{g,f} \in \text{Hom}(F_f, F_g)$, i.e.

$$F_g \circ [a]_{g,f} = [a]_{g,f} \circ F_f.$$

As a corollary of Lemma 4.1, each $u \in A^\times$ gives an isomorphism $[u]_{g,f} : F_f \xrightarrow{\sim} F_g$, and there is a unique isomorphism $F_f \simeq F_g$ of the form $T + \cdots$. □

We write $[a]_f := [a]_{f,f} \in \text{End}\, F_f$. Note that

$$[\varpi]_f = f.$$

Proposition 4.3. For any $a, b \in \mathcal{O}_K$,

$$[a + b]_{g,f} = [a]_{g,f} + [b]_{g,f},$$

and

$$[ab]_{h,f} = [a]_{h,g} \circ [b]_{g,f}.$$

In particular, $\mathcal{O}_K \hookrightarrow \text{End}\, F_f$ as a ring by $a \mapsto [a]_f$, making F_f a formal $\mathcal{O}_K$-module. The canonical isomorphism $[1]_{g,f}$ is an isomorphism of $\mathcal{O}_K$-modules. □

4.3 Construction of K_ϖ

Fix an algebraic closure K^{alg} of K. Each $f \in \mathcal{F}_\varpi$ associates to $\mathfrak{m}_{K^{\mathrm{alg}}}$ an $\mathcal{O}_K$-module structure via

$$\alpha +_{F_f} \beta := F_f(\alpha, \beta)$$

and

$$a \cdot \alpha := [a]_f(\alpha)^{14}.$$

for $|\alpha| < 1, |\beta| < 1$ and $a \in \mathcal{O}_K$. We denote this $\mathcal{O}_K$-module by Λ_f. If $g \in \mathcal{F}_\pi$, then the canonical isomorphism $[1] : F_f \to F_g$ yields an isomorphism of $\mathcal{O}_K$-modules $\Lambda_f \xrightarrow{\sim} \Lambda_g$.

The ϖ^n-torsion part of Λ_f is denoted by $\Lambda_{f,n}$ or $F_f[n]$, i.e.,

$$\Lambda_{f,n} = F_f[n] := \Lambda_f[[\varpi]_f^n].$$

Because $[\varpi]_f = f$, $\Lambda_{f,n}$ is the $\mathcal{O}_K$-module consisting of the roots of $f^{(n)} := f \circ \cdots \circ f$. If one takes f to be an Eisenstein polynomial, then all the roots of $f^{(n)}$ lie in $\mathfrak{m}_{K^{\mathrm{alg}}}$, so $\Lambda_{f,n}$ is precisely the set of roots of $f^{(n)}$ equipped with the $\mathcal{O}_K$-module structure from F_f.

Lemma 4.3. Let M an $\mathcal{O}_K$-module, $M_n = M[\varpi^n]$. If

- M_1 has $q = [\mathcal{O}_K : \varpi]$ elements, and
- $\varpi : M \to M$ is surjective,

then $M_n \simeq \mathcal{O}_K/\varpi^n$.

Proof. Do induction on n. The structure theorem of f.g. modules over a PID shows that M_1 having q elements implies that $M_1 \simeq A/\varpi$. Now assume it true for $n-1$. Look at the sequence

$$0 \to M_1 \to M_n \xrightarrow{\varpi} M_{n-1} \to 0.$$

Surjectivity of ϖ implies the exactness of this sequence, and thus M_n has q^n elements. In addition, M_n must be cyclic, otherwise $M_1 = M_n[\varpi^n]$ is not cyclic. □

Proposition 4.4. The $\mathcal{O}_K$-module $\Lambda_{f,n}$ is isomorphic to $\mathcal{O}_K/\varpi^n$, and hence $\mathrm{End}(\Lambda_{f,n}) \simeq \mathcal{O}_K/\varpi^n$.

Proof. It suffices to show for a chosen f, so let's take $f = \varpi T + \cdots + T^q$, an Eisenstein polynomial. We use the above Lemma 4.3 by the following observations.

- All roots of an Eisenstein polynomial have valuation > 0.
- If $|\alpha| < 1$, then the Newton polygon of $f(T) - \alpha$ shows that its roots have valuation > 0, and thus $[\varpi] = f(T)$ is surjective on Λ_f. □

Lemma 4.4. Let L be a finite Galois extension of K. Then for every $F \in \mathcal{O}_K[\![X_1, \ldots, X_n]\!]$, $\alpha_1, \ldots, \alpha_n \in \mathfrak{m}_L$ and $\tau \in \mathrm{Gal}(L/K)$,

$$\tau F(\alpha_1, \ldots, \alpha_n) = F(\tau\alpha_1, \ldots, \alpha_n).$$

Proof. Note that τ acts continuously on L, because the extension of valuation for local fields is unique. Therefore writing $F = \lim_{m\to\infty} F_m$ gives the desired result. □

Theorem 16. Let $K_{\varpi,n} := K(\Lambda_{f,n}) \subset K^{\mathrm{alg}}$. These fields are independent to the choice of f.

[14] These power serieses converges because they actually falls in a finite extension of K.

(a) $K_{\varpi,n}/K$ is totally ramified of degree $q^{n-1}(q-1)$.

(b) The action of $\mathcal{O}_K$ on $\Lambda_{f,n}$ defines an isomorphism

$$(\mathcal{O}_K/\mathfrak{m}_K^n)^\times \simeq \mathsf{Gal}(K_{\varpi,n}/K). \tag{1}$$

(c) For all n, ϖ is a norm from $K_{\varpi,n}$, i.e., $\exists \alpha_n \in K_{\varpi,n}$ with $N_{K_{\varpi,n}/K}(\alpha_n) = \varpi$.

Proof. Since $F_f[n] \simeq_{\mathcal{O}_K} F_g[n]$, the extesnions over K given by them equal. Let f be a polynomial $T^q + \cdots + \varpi T$.

Choose a nonzero root ϖ_1 of $f(T)$ and, inductively, a root ϖ_n of $f(T) - \varpi_{n-1}$. So $\varpi_n \in \Lambda_{f,n}$, and we obtain a tower of extensions

$$K_{\varpi,n} \supset K(\varpi_n) \overset{q}{\supset} K(\varpi_{n-1}) \overset{q}{\supset} \dots \overset{q}{\supset} K(\varpi_1) \overset{q-1}{\supset} K.$$

All the extensions with indicated degrees are given by Eisenstein polynomials, and thus Galois and totally ramified.

The field $K_{\varpi,n} = K(\Lambda_{f,n})$ is the splitting field of $f^{(n)}$ over K, hence $\mathsf{Gal}(K_{\varpi,n}/K)$ embeds into the permutation group of the set $\Lambda_{f,n}$. By Lemma 4.4, the action of $\mathsf{Gal}(K_{\varpi,n}/K)$ on Λ_n preserves its $\mathcal{O}_K$-action, so

$$\mathsf{Gal}(K_{\varpi_n}/K) \hookrightarrow \mathsf{Aut}(\Lambda_{f,n}) \simeq (\mathcal{O}_K/\varpi^n)^\times.$$

So $[K_{\varpi,n} : K] \le (q-1)q^{n-1}$. Comparing the degree gives $K_{\varpi,n} = K(\varpi_n)$.

Now we prove (c). Let $f^{[n]} := (f/T) \circ f \circ \cdots \circ f$. Then $f^{[n]}$ is monic with degree $q^{n-1}(q-1)$ and $f^{[n]}(\varpi_n) = 0$, and thus $f^{[n]}$ is the minimal polynomial of ϖ_n over K. So we have

$$N_{K_{\varpi,n}/K}(\varpi_n) = (-1)^{q^{n-1}(q-1)}$$

by the following Lemma 4.5. □

Lemma 4.5. Let L/K be a finite extension in an algebraic closure K^{alg}, and $\alpha \in L$ has minimal polynomial f over K of degree d. Suppose

$$f(X) = (X - \alpha_1) \cdots (X - \alpha_d) \in K^{\mathsf{alg}}[X],$$

and let $e = [L : K(\alpha)]$ then

$$N_{L/K}(\alpha) = \left(\prod_{i=1}^{d} \alpha_i \right)^e, \qquad \mathsf{Tr}_{L/K}(\alpha) = e \sum_{i=1}^{d} \alpha_i.$$

Moreover, if

$$f(X) = a_d X^d + a_{d-1} X^{d-1} + \cdots + a_0,$$

then

$$N_{L/K}(\alpha) = (-1)^{de} a_0^e, \qquad \mathsf{Tr}_{L/K}(\alpha) = -e a_{d-1}.$$

Remark. This follows directly from $N_{L/K} = N_{K(\alpha)/K} \circ N_{L/K(\alpha)}$ and $\mathsf{Tr}_{L/K} = \mathsf{Tr}_{L/K(\alpha)} \circ \mathsf{Tr}_{K(\alpha)/K}$. For example,

$$\begin{aligned} N_{L/K}(\alpha) &= N_{L/K(\alpha)} \left(N_{K(\alpha)/K} \alpha \right) \\ &= \left(\prod_{\sigma \in \mathsf{Hom}_K(K(\alpha), \bar{K})} \sigma\alpha \right)^{[L:K(\alpha)]} = \left(\prod_{i=1}^{d} \alpha_i \right)^{[L:K(\alpha)]}. \end{aligned}$$

Define

$$K_\varpi := \bigcup_n K_{\varpi,n}.$$

The isomorphisms in Theorem 16 (b) are

$$(\mathcal{O}_K/\varpi^n)^\times \to \mathsf{Gal}(K_{\varpi,n}/K) \quad \bar{u} \mapsto (\Lambda_{f,n} \ni \alpha \mapsto [u]_f(\alpha)),$$

and clearly lift to an isomorphism

$$\mathcal{O}_K^\times \simeq \mathsf{Gal}(K_\varpi/K).$$

The local Artin map

The **local Artin map** is a homomorphism

$$\phi_\varpi : K^\times \to \mathsf{Gal}(K_\varpi K^{\mathsf{nr}}/K) = \mathsf{Gal}(K^{\mathsf{nr}}/K) \times \mathsf{Gal}(K_\varpi/K)$$

defined as follows. Let $a = u\varpi^m \in K^\times$, then

- $\phi_\varpi(a)|_{K^{\mathsf{nr}}} := \mathsf{Frob}^m$;
- $\phi_\varpi(a)(\lambda) := [u^{-1}]_f(\lambda)$, $\forall \lambda \in \bigcup_n \Lambda_n$.

Theorem 17. The field $K_\varpi K^{\mathsf{nr}}$ is independent of the choice of ϖ.

4.4 The Local Kronecker-Weber theorem

4.5 The Case of $\mathbb{Q}_p$

Let $K = \mathbb{Q}_p$ and $\varpi = p$. Then $f(T) := (1+T)^p - 1 \in \mathcal{F}_p$. Note that f is an endomorphism of

$$\mathbb{G}_{\mathsf{m}}(X,Y) = X + Y + XY,$$

so $F_f = \mathbb{G}_{\mathsf{m}/\mathbb{Z}_p}$. Under the isomorphism

$$(\mathfrak{m}, +_{\mathbb{G}_{\mathsf{m}}}) \simeq (1+\mathfrak{m}, \ \cdot\ ),$$

the endomorphism $f : a \mapsto (1+a)^p - 1$ is converted to the Frobenius map $a \mapsto a^p$.

The field $(\mathbb{Q}_p)_p$

For each $r \geq 1$, the p^r-torsion part of Λ_f is

$$\Lambda_{f,r} = \left\{ \alpha \in \mathbb{Q}_p^{\mathsf{alg}} \,\middle|\, (1+\alpha)^{p^r} = 1 \right\} \simeq \left\{ \zeta \in (\mathbb{Q}_p^{\mathsf{alg}})^\times \,\middle|\, \zeta^{p^r} = 1 \right\} = \mu_{p^r}.$$

The isomorphism is for $\mathcal{O}_K$-modules. So choose primitive p^r-th roots of unity ζ_{p^r} s.t. $\zeta_{p^r}^p = \zeta_{p^{r-1}}$, then $\varpi_r := \zeta_{p^r} - 1$ forms a sequence of compatible generators of $\Lambda_{f,r}$. Therefore

$$(\mathbb{Q}_p)_{p,r} = \mathbb{Q}_p(\varpi_r) = \mathbb{Q}_p(\mu_{p^r}),$$

and the "maximal totally ramified abelian extension"[15] of $\mathbb{Q}_p$ is $(\mathbb{Q}_p)_p = \mathbb{Q}_p(\mu_{p^\infty})$.

[15] Not sure if this terminology is correct ...?

The local Artin map $\phi_p : \mathbb{Q}_p^\times \to \mathsf{Gal}(\mathbb{Q}_p^{\mathsf{ab}}/\mathbb{Q}_p)$

It suffices to look at every

$$\phi_p : \mathbb{Q}_p^\times \to \mathsf{Gal}(\mathbb{Q}_p(\mu_n)/\mathbb{Q}_p).$$

- If n is prime to p, then $\mathbb{Q}_p(\mu_n)/\mathbb{Q}_p$ is unramified of degree f, where f is the minimum natural number s.t. $m \mid p^f - 1$. The map ϕ_p sends up^t to the t-th power of Frobenius-p^f on $\mathbb{Q}_p(\mu_n) = \mathbb{Q}_p(\mu_{p^f-1})$, and $\ker \phi_p = (p^f)^{\mathbb{Z}} \times \mathbb{Z}_p^\times$.
- If $n = p^r$, then $\mathbb{Q}_p(\mu_{p^r})/\mathbb{Q}_p$ is totally ramified. The map ϕ_p sends up^t to the element sending a root of unity ζ to $\zeta^{\bar{u}^{-1}}$, where $\bar{u} \in \mathbb{Z}$ has the same residue modulo p^r as u. The kernel is $p^{\mathbb{Z}} \times (1 + p^r\mathbb{Z}_p)$.
- In general, let $n = p^r \cdot m$ with $p \nmid m$. Then $\mathbb{Q}_p(\mu_n) = \mathbb{Q}_p(\mu_{p^r})\mathbb{Q}_p(\mu_m)$, and $\mathbb{Q}_p(\mu_{p^r}) \cap \mathbb{Q}_p(\mu_m) = \mathbb{Q}_p$.