Notes on Local Fields

Me

November 28, 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.

$\rightarrow$: 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 $\{\text{intermediate field of } L/K\}$ 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.

$$\begin{tikzcd}
& LM \arrow[dl, dash] \arrow[dr, dash] & \\
L \arrow[dr, dash, "\text{Galois}"'] & & M \arrow[dl, dash] \\
& K &
\end{tikzcd}$$

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
$$\begin{aligned} \mathrm{Gal}(LL'/K) &\hookrightarrow \mathrm{Gal}(L/K) \times \mathrm{Gal}(L'/K) \\ \sigma &\mapsto (\sigma|_L, \sigma|_{L'}). \end{aligned}$$

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.

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.

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

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*.

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

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

Proof. Let $R = A_0P + B_0Q$, 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 $\deg(A_0 - uQ) \le \deg Q - 1$. $\square$

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

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

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

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 $f = \sum_{i=0}^n a_i X^i$,

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

$K[X]$ is not complete w.r.t. Gauss norm, but on each subspace

$$K[X]_n := \{f \in K[X] \mid \deg f \leq n - 1\}$$

is complete, since it is a sup-norm on a f.d. K-vector space; see Theorem 4. Same if we replace K by $\mathcal{O}_K$.

Proof of Theorem 1. Let g resp. h be a lift of γ resp. η with degree m resp. n, so that $\deg f = m + n$. Consider

$$\theta : \mathcal{O}_K[X]_n \times \mathcal{O}_K[X]_m \to \mathcal{O}_K[X]_{n+m},\ (u, v) \mapsto gu + hv.$$

This is an $\mathcal{O}_K$-linear map, with determinant $\mathrm{res}(g, h) \in \mathcal{O}_K$. As $\overline{\mathrm{res}(g, h)} = \mathrm{res}(\gamma, \eta) \in k$ while γ and η are coprime, we have $\mathrm{res}(g, h) \in \mathcal{O}_K^\times$ and hence θ is invertible. Now let $V := \mathcal{O}_K[X]_n \times \mathcal{O}_K[X]_m$ and consider

$$\phi : V \to V, \quad \phi(u, v) := \theta^{-1}(f - gh - uv).$$

If ϕ has a fixed point (u, v), then

$$f - gh - uv = \theta(u, v) = gu + hv \implies f = (g + v)(h + u).$$

So we seek for such point in $B(0, 1) \subset V$. As

$$\begin{aligned} |\phi(u, v) - \phi(u', v')| &= |\theta^{-1}(uv - u'v')| \\ &\leq |\mathrm{res}(g, h)^{-1}||uv - u'v'| = |uv - u'v'| \\ &\leq \max\{|uv - u'v|, |u'v - u'v'|\} \leq \max\{|v|, |u'|\}|(u - u', v - v')|, \\ |\phi(u, v)| &\leq \max\{|f - gh|, |uv|\}, \end{aligned}$$

and $|f - gh| < 1$, we deduce that ϕ is a contracting map on $B(0, |f - gh|)$. Hence the fixed point theorem completes the proof. □

[3] Not a right notation, but anyway.

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**

$$
\begin{aligned}
&:= \text{they give the same topology} \\
&\iff (|x_n|_1 \to 0 \iff |x_n|_2 \to 0).
\end{aligned}
$$

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 be 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.

[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

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

Theorem 5. Let K be a local field, $L/K < \infty$. Then 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 lifts to a nontrivial decomposition of $\pi^n P$ in $K[X]$ via Hensel's lemma (Theorem 1). Therefore $r = 0$ or $r = d$. Now note 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 Proposition 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 $\sigma \in \operatorname{Hom}_K(L, L')$ preserves the norm; i.e., $|\sigma(x)|_{L'} = |x|_L$.

[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.

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

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

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 $p = \operatorname{char} k$ gives all finite unramified extensions of K.

Example 2.1. 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 $\operatorname{char} \mathbb{F}_q \nmid n$, 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 $\lambda =$ the length of $\mathrm{NP}(P)$ with slope $-\lambda$.

2.6 Ramification Groups

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

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

by giving filtrations on it.

Let val_L be the valuation on L normalized by $\mathrm{val}_L(L^\times) = \mathbb{Z}$. Assume $\mathrm{char}\, k_K = \mathrm{char}\, k_L = p > 0$ and k_L/k_K separable. The Galois group G acts on L/K, and its decomposition subgroup, by definition, acts on the integers $\mathcal{O}_L/\mathcal{O}_K$, and descends modulo π_L to k_L/k_K. We know that G acts by isometries, so the decomposition subgroup $= G$, giving a surjection $\mathrm{Gal}(L/K) \to \mathrm{Gal}(k_L/k_K)$, and the **inertia subgroup**

$$I(L/K) = \ker\left(\mathrm{Gal}(L/K) \to \mathrm{Gal}(k_L/k_K)\right) = \{g \in G \mid \mathrm{val}_L(ga - a) \geq 1,\ \forall a \in \mathcal{O}_L\}.$$

We develop this idea, giving a filtration of G by how "small" the effect of $g \in G$ is.

2.6.1 Lower Ramification Filtration

For $g \in \mathrm{Gal}(L/K)$, define

$$i_{L/K}(g) := \inf_{a \in \mathcal{O}_L} \mathrm{val}_L(ga - a).$$

- If $\mathcal{O}_L = \mathcal{O}_K[x]$, then $i_L(g) = \mathrm{val}_L(gx - x)$.

Proposition 2.4. Let $g, h \in G = \mathrm{Gal}(L/K)$.

(1) i_L is a class function: $i_L(ghg^{-1}) = i_L(h)$.

(2) i_L verifies the strong triangle inequality: $i_L(gh) \geq \min\{i_L(g), i_L(h)\}$, with "=" $\iff$ $i_L(g) \neq i_L(h)$.

(3) $i_L(g^{-1}) = i_L(g)$.

Proof. Since k_L/k_K is separable, we can write $\mathcal{O}_L = \mathcal{O}_K[x]$. Note that

$$\mathcal{O}_L = \mathcal{O}_K[x] \implies \mathcal{O}_L = \mathcal{O}_K[gx], \forall g \in G.$$

So:

$$i_L(ghg^{-1}) = \mathrm{val}(ghg^{-1}x - x) \underset{G \text{ preserves val}}{=} \mathrm{val}(hg^{-1}x - g^{-1}x) = i_L(h),$$
$$i_L(gh) = \mathrm{val}((ghx - hx) + (hx - x)) \geq \min i_L(g), i_L(h).$$

The last assertion is as trivial. □

Now for $G = \mathrm{Gal}(L/K)$, a real number $u \in \mathbb{R}_{\geq -1}$, we define[7] the lower ramification group

$$\begin{aligned} G_u &:= \{g \in G \mid i_L(g) \geq u + 1\} \\ &= \{g \in G \mid ga \equiv a \bmod \pi_L^{\lfloor u+1 \rfloor}, \forall a \in \mathcal{O}_L\}. \end{aligned}$$

- $G_u \lhd G$ by Proposition 2.4.
- $G_u = G_{\lfloor u \rfloor}$.
- $G_{-1} = G$, $G_0 = I(L/K)$.

[7] It is ok to put $G_u := G$ for $u < -1$.

- If $u \geq \max_{g \neq 1} i_L(g)$, then $G_u = 1$.

Let $L_0 := L^{G_0} = L^{I(L/K)}$. This is the maximal unramified subextension of L/K, hence $\mathcal{O}_L = \mathcal{O}_{L_0}[\pi_L]$. Therefore,

- if $g \in G_0$, then
$$i_L(g) = \mathrm{val}_L\left(\frac{g\pi_L}{\pi_L} - 1\right) + 1,$$
- if $u \geq 0$, then
$$\begin{aligned} G_u &= \left\{ g \in G_0 \,\middle|\, \mathrm{val}\left(\frac{g\pi_L}{\pi_L} - 1\right) \geq u \right\} \\ &= \left\{ g \in G_0 \,\middle|\, \frac{g\pi_L}{\pi_L} \equiv 1 \bmod \pi_L^{\lfloor u \rfloor} \right\}. \end{aligned}$$

Lemma 2.6. If $n \in \mathbb{Z}_{\geq 1}$, then $G_n^p \subset G_{n+1}$.

Proof. Take $g \in G_n$ and write
$$\frac{g\pi_L}{\pi_L} = 1 + \alpha, \;\; \alpha \in \mathfrak{m}_L^n.$$
Then[8]
$$\frac{g^p\pi_L}{\pi_L} = \frac{g\pi_L}{\pi_L}\frac{g^2\pi_L}{g\pi_L}\cdots\frac{g^p\pi_L}{g^{p-1}\pi_L} = (1+\alpha)(1+g\alpha)\cdots(1+g^{p-1}\alpha).$$
Note that $g\alpha \equiv \alpha \bmod \pi_L^{n+1}$, so the product
$$\equiv (1+\alpha)^p \equiv 1 \bmod \pi_L^{n+1}.$$
□

Proposition 2.5. G_1 is the unique Sylow p-group of G_0.

Proof. By the last lemma, $G_1^{p^n} \subset G_{1+n}$ for all n, $\implies G^{p^n} = 1$ for $n \gg 0$, $\implies G$ is a p-group.

We show that: if $g \in G_0$ and $g^p \in G_1$, then $g \in G_1$. This would imply that all elements of p-power order fall in G_1.

Take $g \in G_0$ and write $\dfrac{g\pi_L}{\pi_L} = \alpha \in \mathcal{O}_K^\times$.

- $g \in G_0 \implies g\alpha \equiv \alpha \bmod \pi_L \implies \dfrac{g^p\pi_L}{\pi_L} \equiv \alpha^p \bmod \pi_L$.
- $g^p \in G_1 \implies \dfrac{g^p\pi_L}{\pi_L} \equiv 1 \bmod \pi_L$.

$\implies \alpha \equiv \alpha^p \equiv 1 \bmod \pi_L \iff g \in G_1$. □

Write $[L : L_0] = p^k t$, $p \nmid t$. By Proposition 2.5, $L_1 := L^{G_1}$ has degree t over L_0, and L_1/K is the unique maximal tamely ramified subextension.

The next gaol is to investigate the subquotients G_n/G_{n+1} of the filtration $G \subset G_0 \subset G_1 \subset \cdots$.

Proposition 2.6. Let $n \in \mathbb{Z}_{\geq 0}$.

- $G/G_0 \simeq \mathrm{Gal}(k_L/k_K)$.

[8] More precisely,
$$\frac{g^2\pi_L}{g\pi_L} = \frac{g((1+\alpha)\pi_L)}{g\pi_L} = 1 + g\alpha.$$

- $G_0/G_1 \hookrightarrow \mathcal{O}_L^\times/(1+\mathfrak{m}_L) \simeq k_L^\times$ via $g \mapsto \dfrac{g\pi_L}{\pi_L}$.
- $G_n/G_{n+1} \hookrightarrow (1+\mathfrak{m}_L^n)/(1+\mathfrak{m}_L^{n+1}) \simeq \mathfrak{m}_L^n/\mathfrak{m}_L^{n+1} \simeq k_L$ via $g \mapsto \dfrac{g\pi_L}{\pi_L} \mapsto \dfrac{g\pi_L - \pi_L}{\pi_L^{n+1}}$.

In particular, all the quotients $G_n/G_{n+1}(n \geq 0)$ are finite abelian, and hence G_0 is solvable.

Proof. G/G_0 is known and G_0/G_1 is a sepcial case of G_n/G_{n+1}.

Injectivity is clear once we prove the multiplicity. For $g \in G_n$, let

$$\frac{g\pi_L}{\pi_L} = 1 + \alpha_g,\ \ \alpha_g \in \mathfrak{m}_L^n.$$

Note that $g \mapsto \dfrac{gx}{x}$ is a cocycle, and $g\alpha_h \equiv \alpha_h \bmod \pi^n$ for $g \in G_n$. So

$$\frac{gh\pi_L}{\pi_L} \equiv (1+g\alpha_h)(1+\alpha_g) \equiv (1+\alpha_h)(1+\alpha_g) \bmod \mathfrak{m}_L^{n+1}.$$

□

2.6.2 Upper Ramification Filtration and Ramification Groups of Infinite Extensions

The lower ramification filtration is compatible with *subgroups*:

Proposition 2.7. If $H < G$, then

$$H_u = G_u \cap H.$$

Namely, if $L \mid F \mid K$ is a tower of finite extensions, then

$$\mathrm{Gal}(L/F)_u = \mathrm{Gal}(L/K)_u \cap \mathrm{Gal}(L/F).$$

In practice, we usually fix the bottom K rather than the top L; we want a filtration compatible with quotients. This is given by Herbrand's theorem.

Define **Herbrand's** ϕ function

$$\phi_{L/K} : \mathbb{R}_{\geq -1} \to \mathbb{R}_{\geq -1},\ \phi_{L/K}(u) := \int_0^u \frac{1}{[G_0 : G_t]} dt.$$

- $\phi_{L/K}(0) = 0$, $\phi_{L/K}(-1) = -1$.
- $\phi_{L/K}$ is piece-wise affine, continuous, strictly increasing, concave, and a homeomorphism.

This gives

$$\psi_{L/K} : \mathbb{R}_{\geq -1} \to \mathbb{R}_{\geq -1} := \phi_{L/K}^{-1},$$

and we define

$$G^u := G_{\psi_{L/K}(u)}.$$

This upper ramification filtration is compatible with *quotients*.

Theorem 7. If $H \lhd G$, then

$$(G/H)^v = G^v H/H = \text{ image of } G^v \text{ in } G/H.$$

Namely, if $L \mid F \mid K$ is a tower of extensions, then

$$\mathrm{Gal}(F/K)^v = \mathrm{im}\left(\mathrm{Gal}(L/K)^v \hookrightarrow \mathrm{Gal}(L/K) \twoheadrightarrow \mathrm{Gal}(F/K)\right).$$

Since the upper ramification filtration is compatible with quotients, it can be defined for any infinite Galois extension L/K by

$$\mathrm{Gal}(L/K)^v := \varprojlim_F \left(\mathrm{Gal}(F/K)^v\right).$$

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

Fix an algebraic closure $\bar{\mathbb{Q}}_p = \mathbb{Q}_p^{\mathrm{alg}}$ 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 8 (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 $g\alpha, g \in \mathrm{Gal}(K/F)$ are all the conjugates of α over F. Now if $g \in \mathrm{Gal}(K/F(\beta))$, then

$$\begin{aligned} |g\alpha - \alpha| &= |(g\alpha - g\beta) + (\beta - \alpha)| \\ &\leq \min\{|g\alpha - g\beta|, |\alpha - \beta|\} \overset{[9]}{=} |\alpha - \beta| \end{aligned}$$

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

Theorem 9. 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 10 (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[10] 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 $\mathbb{C}_p$:

- $v_p(\mathbb{C}_p) = v_p(\bar{\mathbb{Q}}_p) = \mathbb{Q}$[11].

[9] Because embeddings of finite extensions of $\mathbb{Q}_p$ are isometries (the uniqueness of norm extension).
[10] Being **nowhere dense** means its closure has empty interior.
[11] 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 $v_p(\lim_n a_n) = v_p(a_m)$.

- $k_{\mathbb{C}_p} = \mathcal{O}_{\mathbb{C}_p}/\mathfrak{m}_{\mathbb{C}_p} \simeq \mathcal{O}_{\bar{\mathbb{Q}}_p}/\mathfrak{m}_{\bar{\mathbb{Q}}_p} \simeq \mathbb{F}_p^{\mathrm{alg}}$.[12]

Theorem 11. $\mathbb{C}_p$ 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 $P \in \mathcal{O}_{\mathbb{C}_p}[X]$.

(T.B.C.) □

2.8 Ax-Sen-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 12 (Ax-Sen-Tate)**.** $\mathbb{C}_p^{G_K} = \widehat{K}$.

Lemma 2.7. 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; multipliciy counted.
- $\dfrac{1}{q!}P^{(q)}(X) = \sum_{i=0}^{n-q} \binom{n-i}{q} a_{n-i} X^{n-i-q}$, so the product of roots of $P^{(q)} = \pm \dfrac{a_q}{\binom{n}{q}}$.

Hence, $\exists$ root β of $P^{(q)}$, s.y.

$$v_p(\beta) \geq \frac{1}{\deg P^{(q)}} v_p\left(\frac{a_q}{\binom{n}{q}}\right) \geq c - \frac{1}{n-q} v_p\left(\binom{n}{q}\right).$$

By looking at carries[13], one varifes that

$$v_p\left(\binom{n}{q}\right) = \begin{cases} 0, & n = qd = p^k d,\ p \nmid d, \\ 1, & n = qp = p^{k+1}. \end{cases}$$ □

For $\alpha \in \bar{\mathbb{Q}}_p$, we define

$$\Delta_K(\alpha) := \inf_{g \in G_K} v_p(g\alpha - \alpha).$$

Theorem 13 (Ax)**.** $\forall \alpha \in \bar{\mathbb{Q}}_p$, $\exists \delta \in K$, s.t.

$$v_p(\alpha - \delta) \geq \Delta_K(\alpha) - \frac{p}{(p-1)^2}.$$

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

[13] $v_p\left(\binom{a+b}{b}\right) = \#$ of carries when compute $a+b$ in base p.

Proof. We do induction on $n := [K(\alpha) : K]$ to show a stronger estimate: $\exists \delta \in K$ s.t.

$$v_p(\alpha - \delta) \geq \Delta_K(\alpha) - \sum_{k=1}^{m} \frac{1}{p^k(p-1)},$$

where $m \in \mathbb{Z}$ such that p^{m+1} is the largest p-power $\leq n$.

Let $Q(X) \in K[X]$ be the minimal polynomial of α over K, and set $P(X) := Q(X + \alpha) \in \bar{\mathbb{Q}}_p[X]$. The roots of P are $g\alpha - \alpha$, where $g \in G_K$.

Apply Lemma 2.7 to $v_p(g\alpha - \alpha) \geq \Delta_K(\alpha)$, we obtain a root $\beta \in \bar{\mathbb{Q}}_p$ of $P^{(q)}(X)$, where $q = p^k$, s.t.

$$\begin{cases} v_p(\beta) \geq \Delta_K(\alpha), & n \text{ is not a power of } p, q \parallel n \\ v_p(\beta) \geq \Delta_K(\alpha) - \dfrac{1}{p^m(p-1)}, & n = p^{m+1} = qp, k = m. \end{cases}$$

Consider $\alpha' := \alpha + \beta$, a root of $Q^{(q)}(X) \in K[X]$. We have

$$[K(\alpha') : K] \leq \deg Q^{(q)} < \deg Q = [K(\alpha) : K]$$

as $q > 0$, so by induction hypothesis, $\exists \delta \in K$ s.t.

$$v_p(\alpha - \delta) \geq \Delta_K(\alpha') - \sum_{i=1}^{r} \frac{1}{p^i(p-1)},$$

where p^{r+1} is the largest p-power $\leq n - q = \deg Q^{(q)}$. Now we estimate $\Delta_K(\alpha')$. Note that

$$g\alpha' - \alpha' = \underbrace{g\alpha' - g\alpha}_{=g\beta} + \underbrace{g\alpha - \alpha}_{v_p \geq \Delta_K(\alpha)} + \underbrace{\alpha - \alpha'}_{=-\beta}.$$

- If $n = qd$ with $p \nmid d$, then $\Delta_K(\alpha') \geq \Delta_K(\alpha)$, and the estimation holds for α.
- If $n = p^{m+1}$, then $\Delta_K(\alpha') \geq \Delta_K(\alpha) - \dfrac{1}{p^m(p-1)}$. Since $r < m$, the estimation of α still holds. □

Ax-Sen-Tate theorem is a direct corollary of Ax's theorem.

Proof of Ax-Sen-Tate. The inclusion $\widehat{K} \subset \mathbb{C}_p^{G_K}$ come from the fact that G_K acts on $\mathbb{C}_p$ continuously.

For the other inclusion, take $\alpha \in \mathbb{C}_p^{G_K}$ and write $\alpha = \lim_n \alpha_n$ with $\alpha_n \in \bar{\mathbb{Q}}_p$. Note that

$$\alpha \in \mathbb{C}_p^{G_K} \iff \Delta_K(\alpha_n) \to \Delta_K(\alpha) = +\infty.$$

So by Ax's theorem, there exists $\delta_n \in K$ with

$$v_p(\delta_n - \alpha_n) \geq \Delta_K(\alpha_n) - \frac{p}{(p-1)^2} \to +\infty,$$

and thus $\alpha = \lim_n \delta_n \in \widehat{K}$. □

Theorem 14. There is a bijection

$$\begin{aligned} \{\text{subfield of } \bar{\mathbb{Q}}_p\} &\longleftrightarrow \{\text{closed subfield of } \mathbb{C}_p\} \\ K &\longmapsto \widehat{K} \\ L \cap \bar{\mathbb{Q}}_p &\longleftarrow L. \end{aligned}$$

Proof.
- $K < \bar{\mathbb{Q}}_p \implies \widehat{K} \cap \bar{\mathbb{Q}}_p = \mathbb{C}_p^{G_K} \cap \bar{\mathbb{Q}}_p = \left(\mathbb{C}_p \cap \bar{\mathbb{Q}}_p\right)^{G_K} = K.$

- Show $L \overset{\text{closed}}{<} \mathbb{C}_p \implies \widehat{L \cap \bar{\mathbb{Q}}_p} = L$, i.e., $L \cap \bar{\mathbb{Q}}_p$ is dense in L.

  Take $z \in L$ and $c > 0$. Then there exists $\alpha \in \bar{\mathbb{Q}}_p$ s.t. $v_p(\alpha - z) \geq c$. Note that $K := L \cap \bar{\mathbb{Q}}_p$ is algebraically closed in L, so

  $$\text{the minimal polynomial of } \alpha \text{ over } K = \text{minimal polynomial of } \alpha \text{ over } L.$$

  This is because if $P = QR \in K[X]$ with $Q, R \in L[X]$, then the coefficients of Q and R are algebraic over K.

  Let $\alpha_1, \alpha_2, \ldots, \alpha_n$ be are all the conjugates of α over K (which are the same over L).
  $\implies \alpha_1 - z, \alpha_2 - z, \ldots, \alpha_n - z$ are all the conjugates of $\alpha - z$ over L.
  $\implies v_p(\alpha_i - \alpha) = v_p\left((\alpha_i - z) - (\alpha - z)\right) \geq \min\{c, c\} = c$ for all i,
  $\implies \Delta_K(\alpha) \geq c$. By Ax's theorem, $\exists \delta \in K$ s.t. $v_p(\alpha - \delta) \geq \Delta_K(\alpha) - \frac{p}{(p-1)^2} \geq c - \frac{p}{(p-1)^2}$. Apply this to all c, we see that $\alpha \in \widehat{K}$.

  □

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.
- $\rho(f(\alpha X)) = \rho(f) \cdot |\alpha|^{-1}$.

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

Example 3.2. $\log(1 + X) = \log_{\mathbb{G}_m}(X) = X - \dfrac{X^2}{2} + \dfrac{X^3}{3} - \cdots \in H_K \setminus K \otimes_{\mathcal{O}_K} \mathcal{O}_K[\![X]\!]$.

3.1 The Gauss Norm

Theorem 15. 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 3.3. 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.
- $\mathrm{wideg}(f) = \infty \iff f \in \mathfrak{m}_K[\![X]\!]$.
- $\mathrm{wideg}(f) = 0 \iff a_0 \in \mathcal{O}_K\times \iff f \in (\mathcal{O}_K[\![X]\!])^\times$.
- 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 $\mathrm{wideg}(f) < \infty$. Then: $\forall g \in \mathcal{O}_K[\![X]\!]$, $\exists! q \in \mathcal{O}_K[\![X]\!]$ & $r \in \mathcal{O}_K[X]$[14] s.t.

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

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

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 $\bmod \pi^n$. ☐

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 $\mathfrak{m}_{\mathbb{Q}_p^{\text{alg}}}$.

Theorem 16 (Weierstrass Preparation Theorem)**.** Let $f \in \mathcal{O}_K[\![X]\!]$ with $\operatorname{wideg} f < \infty$.
Then $\exists!$ distinguished polynomial $P \in \mathcal{O}_K[\![X]\!]$ with $\deg P = \operatorname{wideg} f$, s.t.

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

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, $u \in \left(\mathcal{O}_K[\![X]\!]\right)^\times$.
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 $\operatorname{wideg}(\pi^{-\mu} f) = \deg P$[15]. ☐

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 17. 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 $F = \mathbb{G}_{\mathrm{m}}$.

[15] I want to call this "the Weierstrass degree of f".

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 $B(0,\rho)$. $\square$

Now we can prove the converse of Corollary 3.1.

Theorem 18. 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. $\square$

3.3 p-adic Banach Spaces

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

4 Lubin-Tate Theory

4.1 Formal Groups

Let A be a commutative ring.

- If $f \in A[\![T]\!]$ and $g \in A[\![X_1, \ldots, X_n]\!]$, then

$$\begin{aligned}
f \circ g &:= f(g(X_1, \ldots, X_n)), \\
g \circ f &:= g(f(X_1), \ldots, f(X_n)).
\end{aligned}$$

- If $F \in A[\![X_1, \cdots, X_n]\!]$, we put $F_i :=$ the partial derivative of F w.r.t. the i-th variable X_i.

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

$$\exists g \in A[\![T]\!] \text{ s.t. } f \circ g = g \circ f = T \iff a_1 = f'(0) \in A^\times.$$

Such a power series is called **reversible**.

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

In this section, a **formal group** means a (commutative) formal group law of dimension one.

A **homomorphism** $h : F \to G$ between formal groups F and G over A

$$:= h \in XA[\![X]\!], \quad \text{s.t. } h \circ G = F \circ h,$$

that is $h(G(X,Y)) = F(h(X), h(Y))$.

- A homomorphism $h : F \to G$ is an isomorphism $\iff$ $h'(0) \in A^\times$.
- Every integer $n \in \mathbb{Z}$ gives rise to an endomorphism $[n] = nX + O(X^2) \in \mathrm{End}(F)$, yielding a ring homomorphism $\mathbb{Z} \to \mathrm{End}(F)$.

A **differential form** on F

$$:= \omega(X) = p(X)dX \in A[\![X]\!]dX, \quad \text{s.t.}$$

$$\omega(f(X)) = p(f(X))df(X) := p(f(X))f'(X)dX, \ \forall f(X).$$

We say $\omega(X)$ is **invariant**, if $\omega \circ F(-, Y) = \omega$; i.e,

$$p(F(X,Y))F_1(X,Y) = p(X).$$

Set $X = 0$, we see that

$$p(Y) = p(0)\frac{1}{F_1(0,Y)}.$$

Hence any invariant differential takes the form

$$\omega(X) = \frac{a \cdot dX}{F_1(0,X)}.$$

Conversely, we define

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

and call it **normalized invariant differential**. This name is verified as below.

Proposition 4.1. ω_F is invariant for F.

Proof. Take $\frac{d}{dZ}\big|_{Z=0}$ for

$$F(Z, F(X,Y)) = F(F(Z,X), Y),$$

we get

$$F_1(0, F(X,Y)) = F_1(X,Y)F_1(0,X).$$

□

- If $h \in \mathrm{Hom}(F,G)$, then

$$\omega_G \circ h = h'(0) \cdot \omega_F.$$

4.2 Formal Groups over local fields

Let K be an extension of $\mathbb{Q}_p$ inside $\mathbb{C}_p$.

4.2.1 The Logarithm

Let F be a formal group over K and ω_F the normalized invariant differential. We define

$$\log_F(X) := \int \omega_F \in K[\![X]\!], \quad \text{s.t. } \log_F(0) = 0.$$

- If $\omega(X) = (1 + p_1 X + p_2 X^2 + \cdots)dX$, then
$$\log_F(X) = X + \frac{p_1 X^2}{2} + \frac{p_2 X^3}{3} + \cdots \in XA[\![X]\!].$$
- $\log_F(X) \in H_K$ if F is defined over $\mathcal{O}_K$.

Proposition 4.2. $\log_F(X+Y) = \log_F(X) + \log_F(Y)$, so $\log_F : F \to_K \mathbb{G}_{\mathrm{a}}$ is an isomorphism *over* K.

Proof. Let $E(X) := \log_F(X+Y) - \log_F(X)$. Then $dE(X) = \omega_F \circ F - \omega_F = 0$, thus $E(X) = E(0) = \log_F(Y)$. $\square$

Example 4.1. $\log_{\mathbb{G}_{\mathrm{a}}}(X) = X$, $\log_{\mathbb{G}_{\mathrm{m}}}(X) = \log(1+X)$.

Example 4.2. $\mathbb{G}_{\mathrm{a}}$ and $\mathbb{G}_{\mathrm{m}}$ are *NOT* isomorphic over $\mathcal{O}_K$, because

$$(\mathfrak{m}_{\mathbb{C}_p}, +_{\mathbb{G}_{\mathrm{a}}}) = (\mathfrak{m}_{\mathbb{C}_p}, +) \not\simeq (1 + \mathfrak{m}_{\mathbb{C}_p}, \ \cdot) \simeq (\mathfrak{m}_{\mathbb{C}_p}, +_{\mathbb{G}_{\mathrm{a}}}),$$

as the former is torsion-free while the latter has many torsion.

Remark. Proposition 4.2 holds for any formal group over a $\mathbb{Q}$-algebra A. As the proof involves not the axiom of commutativity, it shows that any formal group (of dimension 1) over a $\mathbb{Q}$-algebra is necessarily commutative.

4.2.2 The Height

Let k be a ring of characteristic $p > 0$. If F, G are formal groups over k, and $f \in \mathrm{Hom}(F, G)$, we define the **height** of f to be

$$\mathrm{ht}(f) := \text{largest integer } h \in \mathbb{Z}, \text{ s.t. } f(X) = g\left(X^{p^h}\right) \text{ for some } g \in k[\![X]\!].$$

Proposition 4.3. If $f \in \mathrm{Hom}(F, G)$ and $f(X) = g\left(X^{p^h}\right)$ with $h = \mathrm{ht}(f)$, then $g'(0) \neq 0$.

Proof. Two steps.

- If $f \in \mathrm{Hom}(F, G)$ with $f'(0) = 0$, then $f(X) = g\left(X^{p^h}\right)$ for some g.

  This is because
$$0 = f'(0)\omega_F = \omega_G \circ f = \frac{f'(X)dX}{G_1(0, X)},$$
  So $f'(X) = 0$. As $\operatorname{char} k = p$, this leads to the result.
- If $F \in \mathrm{Hom}(F, G)$, $f(X) = g\left(X^{p^h}\right)$, then $g \in \mathrm{Hom}(F^{\mathrm{Frob}_{p^h}}, G)$.

  Write $F = \sum a_{ij} X^i Y^j$, so $F^{\mathrm{Frob}_{p^h}}(X) = \sum a_{ij}^{p^h} X^i Y^j$. As $\operatorname{char} k = p$, $F^{\mathrm{Frob}_{p^h}}$ is also a formal group over k. What left is obvious. $\square$

4.2.3 The Torsion of Formal Groups and the Tate Module

Let $K/\mathbb{Q}_p < \infty$, $k = \mathcal{O}_K/\pi$ the residue field, F a formal group over $\mathcal{O}_K$.

- Note that F can be regarded as a formal group over K, and $\bar{F} := F \bmod \pi \in k[\![X]\!]$ is a formal group over k.

We define the **height** of F to be

$$\operatorname{ht}(F) := \text{height of } [p] \in \operatorname{End}_k(\bar{F}).$$

Example 4.3. For $\mathbb{G}_{\mathrm{a}}$, $[p](X) = 0$ in $k[\![X]\!]$, so $\operatorname{ht}(\mathbb{G}_{\mathrm{a}/\mathcal{O}_K}) = \infty$.
For $\mathbb{G}_{\mathrm{m}}$, $[p](X) = (1+X)^p - 1 = X^p$ in $k[\![X]\!]$, so $\operatorname{ht}(\mathbb{G}_{\mathrm{m}/\mathcal{O}_K}) = 1$.

and consider the p^n-torsion points of F, namely

$$F[p^n] := \{z \in \mathfrak{m}_{\mathbb{C}_p} \mid [p^n]_F(x) = 0\}.$$

- $F[p^n]$ is a subgroup of $(\mathfrak{m}_{\mathbb{C}_p}, +_F)$ and a $\mathbb{Z}/p^n\mathbb{Z}$-module.
- $[p] : F[p^{n+1}] \hookrightarrow F[p^n]$ is a surjective homomorphism of $\mathbb{Z}/p^{n+1}\mathbb{Z}$-module

We look at the equation $[p](z) = y$ with $y \in \mathfrak{m}_{\bar{\mathbb{Q}}_p}$ first.

- If $h = \operatorname{ht}(F) < \infty$, then $[p](X) \in \mathcal{O}_K[\![X]\!]$ has Weierstrass degree p^h.
  $\implies$ $[p](z) = y$ has p^h solutions in $\mathfrak{m}_{\bar{\mathbb{Q}}_p}$.
- From $\omega_F \circ [p] = [p]'(0)\omega_F$, one deduce that $[p]'(X) = p(1 + O(X))$.
  $\implies$ all roots of $[p](z) = y$ are simple.

Therefore, if $\operatorname{ht}(F) < \infty$, then

$$\#F[p^n] = p^{hn}.$$

Now define

$$T_pF := \varprojlim_n F[p^n].$$

- T_pF is a $\mathbb{Z}_p$-module.
- If $z = (z_1, z_2, \dots) \in T_pF$, then $pz = (0, z_1, z_2, \dots)$.
  $\implies$ T_pF is torsion-free. In addition,

$$\bigcap_{n\geq 0} p^n T_pF = \{0\}.^{16}$$

- We have an isomorphism

$$\begin{aligned} T_pF/p^nT_pF &\simeq F[p^n] \\ \overline{(z_1, z_2, \dots)} &\mapsto z_n. \end{aligned}$$

Proposition 4.4. T_pF is a free $\mathbb{Z}_p$-module of rank $h = \operatorname{ht} F$.

[16] We say T_pF is seperated.

Proof. Let $m_1, \dots, m_h$ be a lift of a $\mathbb{F}_p$-basis of the dimension h vector space $T_pF/pT_pF \simeq F[p]$. We claim that $m_1, \dots, m_h$ is a $\mathbb{Z}_p$-basis for T_pF.

- (linear independence.) Suppose $\lambda_1 m_1 + \cdots + \lambda_h m_h = 0$ with $\lambda_i \in \mathbb{Z}_p \setminus \{0\}$. T_pF is torsion-free, so $\exists j$ s.t. $p \nmid \lambda_j$. Hecen it will give a nontrivial relation modulo p.
- (generate T_pF.) Use the standard method. Obtain

$$m = \sum_i \lambda_i^{(k)} m_i + p^k n^{(k)}$$

inductively for all $k \geq 1$ Take $\lambda_i := \lim_k \lambda_i^{(k)}$ by $\lambda_i^{(k+1)} \equiv \lambda_i^{(k)} \bmod p^k$. Then

$$m - \sum_i \lambda_i m_i \in \cap_{k \geq 1} p^k T_pF = 0.$$

□

4.2.4 Galois representation attached to a formal group

The Galois group $G_K = \mathrm{Gal}(\bar{\mathbb{Q}}_p/K)$ acts $\mathbb{Z}/p^n$-linearly on $F[p^n]$,
$\rightsquigarrow$ G_K acts $\mathbb{Z}_p$-linearly on T_pF.
$\rightsquigarrow$ continuous group homomorphism

$$\rho_F : G_K \to \mathrm{Aut}_{\mathbb{Z}_p}(T_pF) \underset{\text{choose basis}}{\xrightarrow{\sim}} \mathrm{GL}_h(\mathbb{Z}_p).$$

Example 4.4. For $K = \mathbb{Q}_p$ and $F = \mathbb{G}_{\mathrm{m}}$, ρ_F = cyclotomic charater χ_{cyc}.

4.3 Lubin-Tate formal groups

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

Choose a uniformiser ϖ of K. Define

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

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[17] 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.

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

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.

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

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

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

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

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 4.5. 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.

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

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

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

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 4.6. 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 $[a]_{g,f} \in \mathrm{Hom}(F_f, F_g)$, 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 $[a]_f := [a]_{f,f} \in \operatorname{End} F_f$. Note that

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

Proposition 4.7. 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, $\mathcal{O}_K \hookrightarrow \operatorname{End} F_f$ 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. □

4.4 Construction of K_ϖ

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

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

and

$$a \cdot \alpha := [a]_f(\alpha).$$

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 $\mathfrak{m}_{K^{\text{alg}}}$, 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: if M_1 having q elements, then $M_1 \simeq A/\varpi$. 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 4.8. The $\mathcal{O}_K$-module $\Lambda_{f,n}$ is isomorphic to $\mathcal{O}_K/\varpi^n$, and hence $\operatorname{End}(\Lambda_{f,n}) \simeq \mathcal{O}_K/\varpi^n$.

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. $\square$

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

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

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. $\square$

Theorem 19. Let $K_{\varpi,n} := K(\Lambda_{f,n}) \subset K^{\mathrm{alg}}$. These fields are independent to the choice of f.

(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

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

(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 $T^q + \dots + \varpi T$.

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 $\mathrm{Gal}(K_{\varpi,n}/K)$ embeds into the permutation group of the set $\Lambda_{f,n}$. By Lemma 4.4, the action of $\mathrm{Gal}(K_{\varpi,n}/K)$ on Λ_n preserves its $\mathcal{O}_K$-action, so

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

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 $f^{[n]} := (f/T) \circ f \circ \dots \circ f$. 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. $\square$

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

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

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

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

Moreover, if

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

then

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

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

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

□

Define

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

Then K_ϖ/K is totally ramified, Galois, and abelian. The isomorphisms in Theorem 19 (b) are

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

and clearly lift to an continuous isomorphism

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

We call

$$\chi_\varpi : G_K \to \mathrm{Gal}(K_\varpi/K) \xrightarrow{\sim} \mathcal{O}_K^\times, \quad g\alpha = [\chi_\varpi(g)]_f(\alpha), \forall \alpha \in \Lambda_f = F_f[\pi^\infty]$$

the **Lubin-Tate charater** attached to ϖ.

4.5 Local Class Field Theory: Statement

Let $K_\pi = K(F[\pi^\infty])$ be the Lubin-Tate extension. We have $\mathrm{Gal}(K_\pi/K) \simeq \mathcal{O}_K^\times$.

Recall that the maximal unramified extension K^{nr}/K has Galois group

$$\mathrm{Gal}(K^{\mathrm{nr}}/K) \simeq \mathrm{Gal}(\bar{k}/k) \simeq \widehat{\mathbb{Z}}.$$

If $q = \#k$, then $\mathrm{Frob}_q : x \mapsto x^q$ generates a dense subgroup of $\mathrm{Gal}(\bar{k}/k)$.

We define the **local Artin map** to be the group homomorphism

$$\mathrm{Art}_K : K^\times \simeq \pi^{\mathbb{Z}} \times \mathcal{O}_K^\times \to \mathrm{Gal}(K_\pi/K) \times \mathrm{Gal}(K^{\mathrm{nr}}/K) \simeq^{[18]} \mathrm{Gal}(K_\pi K^{\mathrm{nr}}/K)$$

s.t.

- $\pi \mapsto \mathrm{Frob}_q$,
- $\mathcal{O}_K^\times \ni u \mapsto g \in \mathrm{Gal}(K_\pi/K)$ s.t. $\chi_\pi(g) = \chi_\pi(\mathrm{Art}_K(u)) = u^{-1}$.

Theorem 20 (Local Class Field Theory). (1) $K^{\mathrm{ab}} := K_\pi K^{\mathrm{nr}}$ is the maximal abelian extension of K.

(2) $\mathrm{Art}_K : K^\times \to K^{\mathrm{ab}}$ is independent of all choices.

[18] K_π and K^{nr} are disjoint.

(3) If $L/K < \infty$, then the Artin map induces

$$K^\times / N_{L/K}(L^\times) \simeq \mathrm{Gal}(L/K),$$

which gives a bijection[19]

$$\{\text{open subgroup of } K^\times\} = \{\text{finite extension of } K\}.$$

(4) If $L/K < \infty$, then

$$\begin{array}{ccc} L^\times & \xrightarrow{\mathrm{Art}_K} & \mathrm{Gal}(L^{\mathrm{ab}}/L) \\ {\scriptstyle N_{L/K}}\downarrow & & \downarrow{\scriptstyle \mathrm{res}^{20}} \\ K^\times & \xrightarrow[\mathrm{Art}_L]{} & \mathrm{Gal}(K^{\mathrm{ab}}/K) \end{array}$$

commutes.

Corollary 4.1. $\exists$ unramified charater $\eta : G_K = \mathrm{Gal}(\bar{\mathbb{Q}}_p/K) \to \mathbb{Z}_p^\times$, s.t.

$$\forall g \in G_K,\ N_{K/\mathbb{Q}_p}(\chi_\pi(g)) = \chi_{\mathrm{cyc}}(g)\eta(g).$$

We say a charater η on G_K is **unramified**, if it restricts to the trivial charater on the inertia subgroup $I_K = I(\bar{\mathbb{Q}}_p/K)$. That is, η is lifted from a charater on $\mathrm{Gal}(K^{\mathrm{nr}}/K) \simeq \mathrm{Gal}(\bar{k}/k) \simeq G_K/I_K$.

Proof. We construct this charater η on the dense subgroup

$$\mathrm{im}(\mathrm{Art}_K) = \langle \mathrm{Frob}_q \rangle \times \mathrm{Gal}(K_\pi/K)$$

first. Let $g \in \mathrm{Gal}(\bar{\mathbb{Q}}_p/K)$ with

$$g|_{K^{\mathrm{nr}}} = \mathrm{Frob}_q^n$$

for $n(g) \in \mathbb{Z}$ so that $g \in \mathrm{im}(\mathrm{Art}_K)$. Write $q = p^f$, and note that

$$\mathrm{Frob}_q |_{\mathbb{Q}_p^{\mathrm{nr}}} = \mathrm{Frob}_p^f,$$

Then we have the commutative diagram

$$\begin{array}{ccc} \pi^{n(g)}\chi_\pi(g)^{-1} & \longleftarrow\!\!\!\!\!\!\longleftarrow\!\!\!\!| & g = \left(\mathrm{Frob}_q^{n(g)}, g\right) \\ \downarrow & & \downarrow \\ \left(N_{K/\mathbb{Q}_p}\pi\right)^{n(g)} N_{K/\mathbb{Q}_p}\left(\chi_\pi(g)^{-1}\right) = p^{fn(g)}\chi_{\mathrm{cyc}}(g)^{-1} & \longleftarrow\!\!\!\!| & g|_{\mathbb{Q}_p^{\mathrm{ab}}} = \left(\mathrm{Frob}_p^{fn(g)}, g\right) \end{array}$$

and we thereby find

$$N_{K/\mathbb{Q}_p}\left(\chi_\pi(g)\right) = \left(\frac{N_{K/\mathbb{Q}_p}\pi}{p^f}\right)^{n(g)} \chi_{\mathrm{cyc}}(g)$$

and $\eta(g) := N_{K/\mathbb{Q}_p}(\chi_\pi(g))/\chi_{\mathrm{cyc}}(g)$ indeed defines an unramified character on $\mathrm{im}(\mathrm{Art}_K)$. Hence it is unramified also on G_K. $\square$

[19] In particular, all open subgroups of $K^\times$ are norm of some $L^\times$.

[20] Here

$$\mathrm{res} : \mathrm{Gal}(L^{\mathrm{ab}}/L) \hookrightarrow \mathrm{Gal}(L^{\mathrm{ab}}/K) \twoheadrightarrow \mathrm{Gal}(K^{\mathrm{ab}}/K).$$

4.6 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

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

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

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

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

The field $(\mathbb{Q}_p)_p = \mathbb{Q}_p(\mu_{p^\infty})$

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

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

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 Lubin-Tate extension of $\mathbb{Q}_p$ given by uniformiser p is $(\mathbb{Q}_p)_p = \mathbb{Q}_p(\mu_{p^\infty})$, the cyclotomic extension.

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

It suffices to look at every

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

- 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 $\mathbb{Q}_p(\mu_{p^r}) \cap \mathbb{Q}_p(\mu_m) = \mathbb{Q}_p$.

5 Periods

Question: do we asssume all characters and G_K-action continuous?

5.1 Periods of Characters

Let K be an algebraic extension of $\mathbb{Q}_p$, $G_K = \mathrm{Gal}(\bar{\mathbb{Q}}_p/K)$. If $\eta : G_K \to \mathbb{Z}_p^\times$ is a character of G_K, then a **period in $\mathbb{C}_p$ for η**

$$:= \alpha \in \mathbb{C}_p \ \text{ s.t. } \eta(g) = \frac{g\alpha}{\alpha}, \ \forall g \in G_K.$$

Remark.

- Look at this "example": if we consider "$\chi_{\mathrm{cyc}} : G_K \to \mathbb{C}^\times$", then "$g(e^{2\pi i/n}) = e^{2\pi i/n}\chi_{\mathrm{cyc}}(g)$", so "$2\pi i$" is a "character for χ_{cyc} in $\mathbb{C}$". We are looking for this kind of "$2\pi i$" under p-adic setting.

- In general, for $\alpha \in \mathbb{C}_p$, $g \mapsto \dfrac{g\alpha}{\alpha}$ is a cocycle, but not a character.

So, what characters has periods in $\mathbb{C}_p$?

Theorem 21. If $\eta : G_K \to \mathbb{Z}_p^\times$ is unramified, then $\exists y \in \mathcal{O}^\times_{\widehat{K^{\mathrm{nr}}}}$, s.t. $\eta(g) = \dfrac{gy}{y}$.

Note that if $\alpha \in \mathbb{C}_p$ is a character for an unramified character, then $\alpha \in \mathbb{C}_p^{I_K} = \widehat{K^{\mathrm{nr}}}$.

Proof. Let K be a finite extension of $\mathbb{Q}_p$ with residue field $k = \mathbb{F}_q$, so that $\sigma = \mathrm{Frob}_q \in \mathrm{Gal}(K^{\mathrm{nr}}/K)$ is a generator.

An unramified character η arose from a character

$$\eta : \mathrm{Gal}(K^{\mathrm{nr}}/K) = \langle \mathrm{Frob}_q \rangle \to \mathbb{Z}_p^\times.$$

Write $\sigma := \mathrm{Frob}_q \in G_K/I_K$. Assume that we have found y s.t. $\eta(\sigma) = \dfrac{\sigma y}{y}$. Note that $\eta(\sigma) \in \mathbb{Z}_p^\times \subset K$, so

$$\eta(\sigma^n) = \eta(\sigma)^n = \prod_{i=0}^{n-1} \sigma^i(\eta(\sigma)) = \prod_{i=0}^{n-1} \frac{\sigma^{i+1} y}{\sigma^i y} = \frac{\sigma^n y}{y}.$$

By continuity, $\eta(g) = \dfrac{gy}{y}$ for all $g \in G_K$.

We prove a stronger statement:

$$\forall x \in \mathcal{O}^\times_{\widehat{K^{\mathrm{nr}}}}, \exists y \in \mathcal{O}^\times_{\widehat{K^{\mathrm{nr}}}}, \text{ s.t. } x = \frac{\sigma(y)}{y}.$$

Take $x \in \mathcal{O}^\times_{\widehat{K^{\mathrm{nr}}}}$. We construct $y_i \in \mathcal{O}^\times_{K^{\mathrm{nr}}}$ s.t.

$$x \equiv \frac{\sigma(y_i)}{y_i} \bmod (1 + \pi^i \mathcal{O}_{K^{\mathrm{nr}}}),$$

where π is a uniformizer of K (and of K^{nr}), so that $y = \lim_i y_i \in \varprojlim_i \mathcal{O}^\times_{K^{\mathrm{nr}}}/(1+\pi^i \mathcal{O}_{K^{\mathrm{nr}}}) = \mathcal{O}^\times_{\widehat{K^{\mathrm{nr}}}}$ works[21].

For y_1, we need

$$0 \equiv \frac{x}{\sigma y_1 / y_1} - 1 \equiv \frac{x}{y_1^{q-1}} - 1 \mod \pi.$$

That is, $\bar{x} = \bar{y}_1^{q-1} \in \bar{\mathbb{F}}_q$. So choose any $(q-1)$-th root of $\bar{x}$ in the algebraically closed field $\bar{\mathbb{F}}_q$ then lift it to define y_1.

Assume that there is $y_i \in \mathcal{O}^\times_{K^{\mathrm{nr}}}$ s.t.

$$x = \frac{\sigma y_i}{y_i}(1 + \pi^i x_i),\ x_i \in \mathcal{O}_{\widehat{K^{\mathrm{nr}}}}.$$

We search for $y_{i+1} \equiv y_i \bmod (1 + \pi^i \mathcal{O}_{K^{\mathrm{nr}}})$, so write $y_{i+1} = y_i(1 + \pi^i z_i)$ with $z_i \in \mathcal{O}_{K^{\mathrm{nr}}}$. Then

$$\frac{\sigma y_{i+1}}{y_{i+1}} = \frac{\sigma y_i}{y_i} \frac{1 + \pi^i \sigma z_i}{1 + \pi^i z^i} = \frac{x(1 + \pi^i \sigma z_i)}{(1 + \pi^i x_i)(1 + \pi^i z_i)},$$

$$\implies \frac{\sigma y_{i+1}}{y_{i+1} x} - 1 = \frac{(1 + \pi^i \sigma z_i) - (1 + \pi^i x_i)(1 + \pi^i z_i)}{1 + \pi(\cdots)} \equiv \pi^i(\sigma z_i - z_i - x_i) \mod \pi^{i+1}.$$

We require that $\dfrac{\sigma y_{i+1}}{y_{i+1} x} - 1 \equiv 0 \bmod \pi^{i+1}$, so we need

$$0 \equiv \sigma z_i - z_i - x_i \equiv z_i^q - z_i - x_i \mod \pi.$$

So pick a root of $Z^q - Z - \bar{x}_i \in \bar{\mathbb{F}}_q[Z]$ and lift it to define z_i. $\square$

[21] We can alternatively use the additive approximation.

5.2 Periods of Lubin-Tate Characters - Not Exist

Let K be finite over $\mathbb{Q}_p$ and π a uniformizer of K. We study the Lubin-Tate character $\chi_\pi : G_K \to \mathcal{O}_K^\times$ attached to π. For simplicity, assume that $K/\mathbb{Q}_p$ is unramified of degree h. In particular, $K/\mathbb{Q}_p$ is Galois with $\mathrm{Gal}(K/\mathbb{Q}_p) = \langle \mathrm{Frob}_p \rangle \simeq \mathbb{Z}/h\mathbb{Z}$. Put $q := p^h$.

5.2.1 Periods of Twisted Lubin-Tate Characters

Observe that if $\eta : G_K \to \mathcal{O}_K^\times$ is a character, and $\tau : K \hookrightarrow \bar{\mathbb{Q}}_p$ is an embedding, then we can twist η by τ to obtain a character $\tau \circ \eta : G_K \to \bar{\mathbb{Q}}_p^\times$.

Theorem 22. If $1 \leq k \leq h-1$, then: $\exists x_k \in \mathbb{C}_p^\times$, s.t.

$$\left(\mathrm{Frob}_p^k \circ \chi_\pi\right)(g) = \frac{g(x_k)}{x_k}, \ \forall g \in G_K.$$

Remark. The proof of Theorem 22 works only for *nontrivial* twist; for $k=0$, it provides $x_0 = 0$. In particular, Theorem 22 is vacuous (say nothing) for $K = \mathbb{Q}_p$.

Remark. Theorem 22 holds for any $K/\mathbb{Q}_p < \infty$, which is stated as follows.

Theorem 22′. If $\mathrm{id} \neq \tau \in \mathrm{Hom}_{\mathbb{Q}_p}(K, \bar{\mathbb{Q}}_p)$, then $\exists x_\tau \in \mathbb{C}_p^\times$, s.t.

$$g(x_\tau) = \tau(\chi_\pi(g)) x_\tau, \quad \forall g \in \mathrm{Gal}\left(\bar{\mathbb{Q}}_p / K^{\mathrm{Gal}}\right),$$

where K^{Gal} is the Galois closure of K in $\bar{\mathbb{Q}}_p$.

In this Section 5.2.1, let $\sigma := \mathrm{Frob}_p \in \mathrm{Gal}(K/\mathbb{Q}_p)$. Let F be the Lubin-Tate group attached to π with

$$[\pi](X) = \pi X + X^q.$$

The Galois group $\mathrm{Gal}(K/\mathbb{Q}_p)$ acts on $K[\![X]\!]$ on the coefficients, namely for $f(X) = \sum_i f_i X^i \in [\![X]\!]$ and $\tau \in \mathrm{Gal}(K/\mathbb{Q}_p)$,

$$f^\tau(X) := \sum_i \tau(f_i) X^i.$$

Lemma 5.1. If $x, y \in \mathfrak{m}_{\mathbb{C}_p}$ and $x \equiv y \bmod p^n$, then $[\pi]^\tau(x) \equiv [\pi]^\tau(y) \bmod p^{n+1}$.

Proof. The series $[\pi](X) = \pi X + X^q$ has only two terms.

- $\tau(\pi) \in p\mathcal{O}_K$, because K is unramified over $\mathbb{Q}_p$, which implies $\pi \mathcal{O}_K = p\mathcal{O}_K$; and τ preserves valuation.
- If $y = x + p^n z$, then $y^q = (x + p^n z)^q \equiv x^q \bmod p^{n+1}$. □

Let $\{\pi_n\}_n \subset \mathfrak{m}_{\mathbb{C}_p}$ form a generator of the Tate module T_pF (simultaneously, a series of generators for the extensions $K_n = K(F[\pi^n])$ over K), i.e,

$$[\pi](z_1) = 0, \ z_1 \neq 0, \quad [\pi](z_{n+1}) = z_n.$$

Lemma 5.2. The sequence

$$\left\{ [\pi^n]^{\sigma^k} \left(z_n^{p^k} \right) \right\}_{n \geq 1}$$

converges in $\mathfrak{m}_{\mathbb{C}_p}$.

Proof. Note that
$$[\pi]^{\sigma^k}(z_{n+1}^{p^k}) \equiv z_{n+1}^{p^k q} \equiv ([\pi](z_{n+1}))^{p^k} = z_n^{p^k} \mod p,$$
because we have $[\pi](X) \equiv X^q \bmod \pi$, which implies $[\pi]^{\sigma^k}(X) \equiv X^q \bmod \pi$.

Since
$$(f \circ g)^\tau = f^\tau \circ g^\tau,$$
we apply the previous Lemma 5.1 n-times and get
$$\left[\pi^{n+1}\right]^{\sigma^k} \left(z_{n+1}^{p^k}\right) \equiv [\pi^n] \left(z_n^{p^k}\right) \mod p^{n+1}.$$
□

Let $y_k := \lim_{n\to\infty} [\pi^n]^{\sigma^k} \left(z_n^{p^k}\right)$, the limit of the sequence in the last lemma.

Lemma 5.3. $v_p(y_k) = 1 + \dfrac{p^k}{q-1}$.

Proof. We prove that
$$v_p\left([\pi^n]^{\sigma^k}\left(z_n^{p^k}\right)\right) = 1 + \frac{p^k}{q-1}$$
constantly.

$[\pi^n](X)$ is a monic polynomial of degree q^n, so
$$[\pi^n]^{\sigma^k}\left(z_n^{p^k}\right) = \prod_{[\pi^n]^{\sigma^k}(\omega)=0} \left(z_n^{p^k} - \omega\right).$$

(T.B.C.) □

Lemma 5.4. If $g \in G_K$, then $g(y_k) = [\chi_\pi(g)]^{\sigma^k}(y_k)$.

Proof. By the definition of Lubin-Tate character, $g(z_n) = [\chi_\pi(g)](z_n)$ because $z_n \in F[\pi^n]$. Hence
$$g(z_n^{p^k}) = ([\chi_\pi(g)](z_n))^{p^k} \equiv [\chi_\pi(g)]^{\sigma^k}(z_n^{p^k}) \mod p,$$
Apply $[\pi]^{\sigma^k}$ to this identity n-times via Lemma 5.1, then as we have all commutativity required, taking limits give the desired result. □

Proof of Theorem 22. Lemma 5.4 provides us a "multiplicative" result, while the period is an "additive" result. So, we use $\log_F : F \to_{/K} \mathbb{G}_{\mathrm{a}}$, with it also twisted.

Let $x_k := \log_F^{\sigma^k}(y_k) \in \mathfrak{m}_{\mathbb{C}_p}$, then
$$\begin{aligned} g(x_k) = \log_F^{\sigma^k}(g(y_k)) &= \log_F^{\sigma^k}\left([\chi_\pi(g)]^{\sigma^k}(y_k)\right) \\ &= (\log_F \circ [\chi_\pi(g)])^{\sigma^k}(y_k) \\ &= (\chi_\pi(g)\log_F)^{\sigma^k}(y_k) = \sigma^k(\chi_\pi(g))x_k. \end{aligned}$$
It remains (important!) to show that $x_k \neq 0$. Since
$$\log_F(X) = X + \sum_{j\geq 2} \frac{a_j}{j} X^j$$
for some $a_i \in \mathcal{O}_K$, and $v_p(y_k) > 1$ by Lemma 5.3, we have $v_p\left(\dfrac{\sigma^k a_j}{j} y_k^j\right) > v_p(y_k)$, thus $v_p(x_k) = v_p(y_k)$. □

5.2.2 Tate's Normalized Trace

Our next goal is to show that characters "too ramified", like cyclotomic and Lubin-Tate characters, have no period in $\mathbb{C}_p$.

We look at χ_{cyc} first. If $\alpha \in \mathbb{C}_p$ is a period for χ_{cyc}, then $x \in \mathbb{C}_p^{\mathrm{Gal}(\bar{\mathbb{Q}}_p/\mathbb{Q}_p(\mu_{p^\infty}))} = \widehat{\mathbb{Q}_p(\mu_{p^\infty})}$. That leads us to study the field $\widehat{\mathbb{Q}_p(\mu_{p^\infty})}$.

Let $F := \mathbb{Q}_p$, $F_n := \mathbb{Q}_p(\mu_{p^n}) \ni \pi_n := \zeta_{p^n} - 1$, $F_\infty := \mathbb{Q}_p(\mu_{p^\infty})$.

If $n \in \mathbb{Z}_{\geq 1}$ and $x \in F_\infty$, then for $k \gg 0$, $x \in F_{n+k}$; we thus define

$$R_n(x) := \frac{1}{p^k} \operatorname{Tr}_{F_{n+k}/F_n}(x) \in F.$$

- $R_n(x)$ is independent to k, bacause $[F_{n+k} : F_n] = p^k$.
- $R_n : F_\infty \to F_n$ is an F_n-linear projection[22], and it is G_F-equivariant.
- $R_n \circ R_m = R_{n+m}$.

Lemma 5.5. For $n \geq 1$ and $k \geq 0$,

$$R_n(\zeta_{p^{n+k}}^j) = \begin{cases} 1, & j = 0, \\ 0, & 1 \leq j \leq p^k - 1. \end{cases}$$

Proof. $\mathrm{Gal}(F_{n+k}/F_n)$ corresponds to the subgroup of $\left(\mathbb{Z}/p^{n+k}\mathbb{Z}\right)^\times$ defined by

$$\ker\left(\left(\mathbb{Z}/p^{n+k}\mathbb{Z}\right)^\times \to (\mathbb{Z}/p^n\mathbb{Z})^\times\right) = \left\{a \in \left(\mathbb{Z}/p^{n+k}\mathbb{Z}\right)^\times \middle| a \equiv 1 \bmod p^n\right\} = 1 + p^n\mathbb{Z}/p^{n+k}\mathbb{Z}.$$

So the conjugates of $\zeta \in \mu_{p^{n+k}}$ are

$$\zeta^{1+bp^n} = \zeta \cdot (\zeta^{p^n})^b, \quad b \in \mathbb{Z}/p^k\mathbb{Z}.$$

$$\Longrightarrow \operatorname{Tr}_{F_{n+k}/F_n}(\zeta_{p^{n+k}}^j) = \zeta_{p^{n+k}}^j \sum_{\eta \in \mu_{p^k}} \eta^j.$$

□

Therefore, since $\mathcal{O}_{F_{n+k}} = \mathcal{O}_{F_n}[\zeta_{p^{n+k}}]$, the map R_n sends $\mathcal{O}_{F_\infty}$ to $\mathcal{O}_{F_n}$, and in addition,

$$R_n(\pi_n^i \mathcal{O}_{F_\infty}) \subset \pi_n^i \mathcal{O}_{F_n}, \ \forall i \in \mathbb{Z}.$$

Corollary 5.1. $v_p(R_n(x)) > v_p(x) - v_p(\pi_n) = v_p(x) - \dfrac{1}{p^{n-1}(p-1)}$, $\forall x \in F_\infty$.

Proof. Let $x \in F_{n+k}$ s.t.

$$x = \pi_{n+k}^{j+p^k i} \cdot \text{unit} = \pi_{n+k}^j \pi_n^i u$$

for $0 \leq j \leq p^k - 1$ and $u \in \mathcal{O}_{F_{n+k}}^\times$. What is $R_n(xy)$? □

Hence, $R_n : F_\infty \to F_n$ is *uniformly continuous*, thereby extends to an F_n-linear G_F-equivariant continuous map

$$R_n : \widehat{F_\infty} \to F_n.$$

(T.B.C.)

Theorem 23. If $\psi : \mathrm{Gal}(F_\infty|F) \to \mathbb{Z}_p^\times$ is a character of infinite order, and $x \in \mathbb{C}_p$ s.t. $gx = \psi(g)x, \forall g \in G_F$, then $x = 0$.

[22] Here, projection = idempotent.

Corollary 5.2. There is no period for χ_{cyc} in $\mathbb{C}_p^\times$.

To study Lubin-Tate characters this way, we need to define R_n for cyclotomic extensions of K.

Corollary 5.3. If $\psi : \mathrm{Gal}(K_\infty|K) \to \mathbb{Z}_p^\times$ is a character of infinite order, and $x \in \mathbb{C}_p$ s.t. $gx = \psi(g)x, \forall g \in G_K$, then $x = 0$.

Corollary 5.4. The Lubin-Tate character χ_π has no period in $\mathbb{C}_p$: If $x \in \mathbb{C}_p$ s.t. $gx = \chi_\pi(g)x, \forall g \in G_K$, then $x = 0$.

5.3 Rings of Periods and Admissible Representations

Let V be a **p-adic representation** of G_K of dimension d, i.e, V is a $\mathbb{Q}_p$-vector space of dimension d with a $\mathbb{Q}_p$-linear G_K-action.

The $\mathbb{C}_p$-vector space $\mathbb{C}_p \otimes_{\mathbb{Q}_p} V$ is equipped with G_K-action on both $\mathbb{C}_p$ and V, called a **semi-linear $\mathbb{C}_p$-representation** of G_K of dimension d. Consider the K-vector space

$$D(V) := \left(\mathbb{C}_p \otimes_{\mathbb{Q}_p} V\right)^{G_K}$$

with the map

$$\begin{aligned} \alpha : \mathbb{C}_p \otimes_K D(V) &\to \mathbb{C}_p \otimes_{\mathbb{Q}_p} V \\ \lambda \otimes (\mu \otimes v) &\mapsto \lambda\mu \otimes v. \end{aligned}$$

Example 5.1. Let $\eta : G_K \to \mathbb{Z}_p^\times$ be a character. Define a 1-dimensional representation by

$$\mathbb{Q}_p(\eta) := \mathbb{Q}_p \cdot e_\eta, \quad \text{with } g(e_\eta) = \eta(g)e_\eta.$$

The G_K-action on

$$\mathbb{C}_p(\eta) := \mathbb{C}_p \otimes_{\mathbb{Q}_p} \mathbb{Q}_p(\eta) = \mathbb{C}_p \cdot e_\eta$$

is given by

$$g(\lambda e_\eta) = g(\lambda)\eta(g)e_\eta, \quad \lambda \in \mathbb{C}_p.$$

The space $\mathbb{C}_p(\eta)^{G_K}$ is a K-vector space of dimension 1 or 0, depending on if η has a period in $\mathbb{C}_p$.

Proof. For $y = xe_\eta \in \mathbb{C}_p(\eta)$, where $x \in \mathbb{C}_p$, □

Proposition 5.1. $\alpha : \mathbb{C}_p \otimes_K D(V) \to \mathbb{C}_p \otimes_{\mathbb{Q}_p} V$ is a $\mathbb{C}_p$-linear injection.

Corollary 5.5. $\dim_K D(V) \leq d$.

We say V is **$\mathbb{C}_p$-admissible**, if $\dim_K D(V) = \dim_{\mathbb{Q}_p} V$, whence

$$\alpha : \mathbb{C}_p \otimes_K D(V) \simeq \mathbb{C}_p \otimes_{\mathbb{Q}_p} V.$$

6 Group Cohomology

In this section we fix a commutative ring $\mathbb{K}$.

6.1 Cohomology

Let G be a group. A **G-module** with coefficients in $\mathbb{K}$ is a $\mathbb{K}$-module together with a $\mathbb{K}$-linear *left* G-action. Hence the category of G-modules with coefficients in $\mathbb{K}$ is isomorphic to the category of $\mathbb{K}[G]$-modules.

Remark. In particular, a G-module with coefficients in $\mathbb{Z}$ is an abelian group with additive left G-action.

Example 6.1. We list some important constructions of G-modules here.

(a) The **trivial G-module** is $\mathbb{K}$ with the trivial G-action.

(b) The group ring $\mathbb{K}[G]$ is a G-module with G acting by left-multiplication.

(c) Direct sum and product. Both direct sums and products for G-modules as $\mathbb{K}$-modules can be lifted to G-modules, by giving G-action diagonally, i.e,

$$g((m_i)_i) := ((gm_i)_i)\,.$$

(d) Tensor products. For $M, N \in \mathbf{Mod}_G$, define $M \otimes N \in \mathbf{Mod}_G$ to be $M \otimes_{\mathbb{K}} N$ with the diagonal G-action

$$g(x \otimes y) := gx \otimes gy, \quad x \in M, y \in N.$$

(e) Hom module. For $M, N \in \mathbf{Mod}_G$, define $\mathrm{Hom}(M, N) \in \mathbf{Mod}_G$ to be $\mathrm{Hom}_{\mathbb{K}}(M, N)$ with G acting "by conjugation":

$$(gf)(x) := gf(g^{-1}x), \quad f \in \mathrm{Hom}_{\mathbb{K}}(M, N), x \in M.$$

- We have

$$\mathrm{Hom}_G(M, N) = \mathrm{Hom}(M, N)^G$$

  as G-modules.

- The adjoint $L \otimes_{\mathbb{K}} (-) \dashv \mathrm{Hom}_{\mathbb{K}}(L, -)$ in $\mathbf{Mod}_{\mathbb{K}}$ holds in $\mathbf{Mod}_G$, i.e,

$$\begin{array}{ccc} \mathrm{Hom}(L \otimes M, N) & \overset{\sim}{\longleftrightarrow} & \mathrm{Hom}(L, \mathrm{Hom}(M, N)) \\ \varphi & \longmapsto & x \mapsto y \mapsto \varphi(x \otimes y) \\ (x \otimes y \mapsto \psi(x)(y)) & \longleftarrow\!\shortmid & \psi \end{array}$$

  are isomorphisms of G-modules.

  Remark. The K-modules $M \otimes_{\mathbb{K}} N$ and $\mathrm{Hom}_{\mathbb{K}}(M, N)$ with their G-module structures are *NOT* the tensor product or Hom-set in $\mathbb{K}[G]$-module.

(f) Induced module. Let $H < G$ be a subgroup, N a H-module. Then $\mathrm{Ind}_H^G N$ is the K-module of H-invariant functions $G \to N$, i.e.,

$$\mathrm{Ind}_H^G N := \{\varphi : G \to N \mid \varphi(hg) = h\varphi(g),\ \forall h \in H, g \in G\} \simeq \mathrm{Hom}_H(\mathbb{K}[G], N).$$

The group G acts on $\mathrm{Ind}_H^G N$ from the left by

$$(g\varphi)(x) := \varphi(xg).$$

We obtain a functor $\mathrm{Ind}_H^G : \mathbf{Mod}_H \to \mathbf{Mod}_G$ by sending $\alpha : N \to N'$ to

$$\alpha_* : \mathrm{Ind}_H^G N \to \mathrm{Ind}_H^G N' := \varphi \mapsto \alpha \circ \varphi.$$

- Ind_H^G is *right adjoint to the forgetful functor* $\mathbf{Mod}_G \to \mathbf{Mod}_H$. The isomorphism is given by

$$\begin{aligned}
\operatorname{Hom}_G\left(M, \operatorname{Ind}_H^G N\right) &\xleftrightarrow{\sim} \operatorname{Hom}_H(M,N) \\
\alpha &\longmapsto x \mapsto \alpha(x)(1_G) \\
[x \mapsto (g \mapsto \beta(gx)] &\longleftarrow\!\shortmid\ \beta
\end{aligned}$$

where $M \in \mathbf{Mod}_G$, $N \in \mathbf{Mod}_H$.

- Ind_H^G is an exact funtor.
- For any $\mathbb{K}$-module M, we define

$$\operatorname{Ind}^G M := \operatorname{Ind}_{\{1\}}^G M = \{\varphi : G \to M\}.$$

An **induced module** is a G-module of the form $\operatorname{Ind}^G M$ for some $\mathbb{K}$-module M.

- Let M be a G-module. Define $M_* := \operatorname{Ind}^G M$, then we have an embedding

$$M \hookrightarrow M_* := x \mapsto [g \mapsto gx]$$

of G-modules. The exact sequence

$$0 \to M \to M_* \to M_\dagger \to 0 \tag{2}$$

in $\mathbf{Mod}_G$, where $M_\dagger := M_*/M$, will be used many times in “dimensional shifting”.

Let M be a G-module, $r \geq 0$ a natural number. We define the **r-th cohomology groups of G with coefficients in M** to be the value of the r-th right derived functor of the left-exact functor

$$(-)^G \simeq \operatorname{Hom}_G(\mathbb{K}, -) : \mathbf{Mod}_G \to \mathbf{Mod}_K$$

at M. But for this definition to make sense, we need to show that:

Lemma 6.1. The category $\mathbf{Mod}_G$ has enough injectives.

Proof. The category $\mathbf{Ab}$ has enough injectives. Let $M \in \mathbf{Mod}_G$, $I \in \mathbf{Ab}$ injective with $M \hookrightarrow I$. Applying the exact functor Ind^G gives

$$M \hookrightarrow M_* := \operatorname{Ind}^G M \hookrightarrow \operatorname{Ind}^G I.$$

So it remains to show that

- the functor Ind^G preserves injectives,

which follows from $\operatorname{Hom}_G(-, \operatorname{Ind}^G I) \simeq \operatorname{Hom}_{\mathbb{Z}}(-, I)$. □

Proposition 6.1 (Shapiro's lemma)**.** Let $H < G$ be a subgroup. The isomorphism

$$(-)^H \simeq \operatorname{Hom}_H(\mathbb{Z}, -) \simeq \operatorname{Hom}_G\left(\mathbb{Z}, \operatorname{Ind}_H^G(-)\right) \simeq \left(\operatorname{Ind}_H^G(-)\right)^G$$

induces a canonical isomorphism

$$H^\bullet\left(G, \operatorname{Ind}_H^G(-)\right) \simeq H^\bullet(H, -),$$

which is compatible with the long exact sequence.

Proof. □

Corollary 6.1. If M is an induced G-module, then $H^r(G, M) = 0$ for all $r \geq 1$. □

6.2 Compute Cohomology via cochains

Homological algebra tells us that

$$H^r(G, M) = R^r \operatorname{Hom}_G(\mathbb{Z}, -)(M) = \operatorname{Ext}^r(\mathbb{Z}, M) = R^r \operatorname{Hom}_G(-, M)(\mathbb{Z}),$$

so we can use the projective resolution of $\mathbb{Z} \in \mathbf{Mod}_G$ to compute $H^\bullet(G, M)$.

Denote by P_r the free $\mathbb{Z}$-module with basis $G^{r+1} = G \times \cdots \times G$ and endow P_r with the G-action

$$g(g_0, g_1, \ldots, g_r) := (gg_0, gg_1, \ldots, gg_r).$$

Define $d_r : P_r \to P_{r-1}$ by

$$d_r(g_0, \ldots, g_r) := \sum_{i=0}^{r} (-1)^i (g_0, \ldots, \hat{g}_i, \ldots, g_r).$$

Then

$$\cdots \to P_1 \xrightarrow{d_1} P_0 \xrightarrow{d_0} \mathbb{Z}$$

is exact, i.e., a projective resolution of $\mathbb{Z}$.

Note that $\varphi \in \operatorname{Hom}_G(P_r, M)$ is equivalent to a function $\varphi : G^{r+1} \to M$ s.t.

$$\varphi(gg_0, \ldots, gg_r) = g\varphi(g_0, \ldots, g_r),$$

which is thus determined by its value on the set $\{(1, g_1, \ldots, g_r) : g_i \in G\}$. Therefore we consider the abelian group[23] $C^r(G^r, M) := \{\varphi : G \to M\}$. Note that $G^0 = 1$ and thus $C^0(G, M) = M$. Define a homomorphism

$$d^r : C^r(G, M) \to C^{r+1}(G, M)$$

by $(d^r\varphi)(g_1, \ldots, g_{r+1})$

$$:= g_1\varphi(g_2, \ldots, g_{r+1}) + \sum_{j=1}^{r} (-1)^j \varphi(g_1, \ldots, \hat{g}_j, \ldots, g_r) + (-1)^{r+1}\varphi(g_1, \ldots, g_r). \tag{3}$$

Let

$$Z^r(G, M) := \ker d^r, \;\; B^r(G, M) := \operatorname{im} d^{r-1}.$$

One can prove that $d^r \circ d^{r-1} = 0$, and

$$H^r(G, M) = Z^r(G, M)/B^r(G, M).$$

Example 6.2 (H^1)**.** An 1-cocycle $c : G \to M$ is called a **crossed homomorphism**. We have

$$H^1(G, M) = \frac{Z^1(G, M)}{B^1(G, M)} = \frac{\{c : G \to M \mid c(gh) = c(g) + gc(h)\}}{\{g \mapsto gm - m \mid m \in M\}}.$$

Now fix a G-module M and let E be an **extension of** $\mathbb{K}$ **by** M, meaning that E is a G-module with an exact sequence

$$0 \to M \to E \xrightarrow{\pi} \mathbb{K} \to 0.$$

Take $e \in E$ with $\pi(e) = 1$. Then $ge - e \in \ker \pi = M$ for $g \in G$, and the map

$$G \to M, \quad g \mapsto ge - e$$

is a cocycle. Moreover, different choices of the lift e are cohomologous. Hence, the extension E of $\mathbb{K}$ by M defines $[E] \in H^1(G, M)$, and $[E] = 1 \iff E \simeq M \oplus \mathbb{K}$.

[23] The group structure on $C^r(G, M)$ is point-wise addition.

Example 6.3. If G acts trivially on M, then a crossed homomorphism is a homomorphism, and $H^1(G, M) = \mathrm{Hom}_{\mathrm{Grp}}(G, M)$.

Example 6.4 (H^1 for finite cyclic groups)**.** Let G be a finite cyclic group generated by σ. Then

$$I_G = \langle \sigma^n m - m \mid m \in M, n \in \mathbb{Z} \rangle = \langle \sigma m - m \mid m \in M \rangle ,$$

$$\hat{H}^{-1}(G, M) = \ker(N_G)/(\sigma - 1)M.$$

In this case, choosing a generator σ of G defines an explicit isomorphism

$$\begin{aligned} \hat{H}^1(G, M) &\to \hat{H}^{-1}(G, M) \\ \varphi &\mapsto \varphi(\sigma). \end{aligned}$$

Indeed, crossed homomorphisms $G \to M$ are defined by their value on generators of G, and for $\varphi : G \to M$ a crossed homomorphism,

$$\varphi(\sigma^n) = \sigma^{n-1}\varphi(\sigma) + \sigma^{n-2}\varphi(\sigma) + \cdots + \sigma\varphi(\sigma) + \varphi(\sigma), \ \forall \sigma \in G.$$

Therefore, if $G \simeq \mathbb{Z}/n\mathbb{Z}$ is generated by σ of order n, then

$$\varphi \text{ is a crossed homomorphism } \iff x := \varphi(\sigma) \text{ verifies } N_G x = \sum_{g \in G} gx = x + \sigma x + \cdots + \sigma^{n-1}x = 0.$$

$$\varphi \text{ is principal } \iff \varphi(\sigma) \in (\sigma - 1)\, M.$$

As $Z^1(G, M) \to M, \ \varphi \to \varphi(\sigma)$ is a group homomorphism, we get the isomorphism.

Example 6.5 (H^1 for infinite cyclic groups with value in finite G-modules)**.** Let G be infinite and topologically generated by σ, and M be a *finite* G-module. Then

$$H^1(G, M) \simeq M/(\sigma - 1)M.$$

6.3 The Inflation-Restriction Exact Sequence

6.4 Homology

For $M \in \mathbf{Mod}_G$, define its **coinvariant** to be the quotient

$$M_G := M/\langle gm - m \mid g \in G, m \in M \rangle = M/(G - \mathrm{id})M \in \mathbf{Ab}.$$

Lemma 6.2. The assignment $M \mapsto M_G$ defines a right-exact functor

$$(-)_G \simeq \mathbb{Z} \otimes_{\mathbb{Z}[G]} (-) : \mathbf{Mod}_{\mathbb{Z}[G]} \to \mathbf{Ab}$$

Proof. Consider the augmentation map $\mathbb{Z}[G] \to \mathbb{Z}$ which is an additive homomorphism sending all $g \in G$ to $1 \in \mathbb{Z}$. Its kernel I_G is called the **augmentation ideal**. Note that:

- $I_G \subset \mathbb{Z}[G]$ is the free abelian subgroup with basis $\{g - 1 \mid g \in G, g \neq 1\}$.

Therefore

$$M_G = M/I_G M \simeq \mathbb{Z}[G]/I_G \otimes_{\mathbb{Z}[G]} M \simeq \mathbb{Z} \otimes_{\mathbb{Z}[G]} M. \qquad \square$$

We define the **r-th homology groups of G with coefficients in** $M \in \mathbf{Mod}_G$ to be the value of the r-th left derived functor of the right-exact functor $(-)_G$.

6.5 The Tate cohomology groups

In this subsection, let G be a *finite* group.

Recall that the norm $N_G : M \to M$ for a G-module M is defined by

$$N_G(x) := \sum_{g \in G} gx, \quad x \in G.$$

One observes that

$$\operatorname{im} N_G \subset M^G, \quad I_G M \subset \ker N_G.$$

Therefore N_G factors as

$$M \twoheadrightarrow M/I_G M = M_G \to M^G \hookrightarrow M,$$

and we got an exact sequence

$$0 \to \ker N_G / I_G M \to M_G \to M^G \to M^G / \operatorname{im} N_G \to 0.$$

The map $H_0(G, M) \to H^0(G, M)$ induced by the norm map on M connects homologies and cohomologies. We define the **Tate cohomology groups** by

$$\hat{H}^r(G, M) := \begin{cases} H^r(G, M), & r \geq 1, \\ M^G / N_G(M), & r = 0, \\ \ker(N_G : M \to M)/I_G M, & r = -1, \\ H_{-r-1}(G, M), & r \leq -2. \end{cases}$$

Proposition 6.2. If M is induced, then $\hat{H}^\bullet(G, -) = 0$.

(connecting H^r to H^{r+2}.)

6.6 Non-commutative Cohomology

Let G be a topological group, and M be a topological (not necessarily commutative) group with a *continuous* left G-action compatible with the group structure on M, namely a continuous map

$$G \times M \to M, \quad (g, m) \mapsto gm,$$

s.t. $(g_1 g_2)m = g_1(g_2 m),\ 1m = m; \quad g(m_1 m_2) = gm_1 \cdot gm_2,\ g1 = 1.$

Remark. Assume that G is profinite, and M is discrete. Then TFAE:

- $G \times M \to M$ is continuous.
- $M = \bigcup_K M^K$, where K goes through all *normal open* subgroups of G.
- For all $m \in M$, its stabiliser $\operatorname{Stab}_G(m)$ in G is open.

We look at only H^0 and H^1 now. Define

$$H^0(G, M) := M^G = \{m \in M \mid gm = m, \forall g \in G\},$$

which is a group.

A (1-)cocycle on G is a continuous map $c : G \to M$ s.t.

$$c(gh) = c(g) \cdot gc(h).$$

- $c : G \to M$ is a cocycle $\implies c(1) = 1$.
- $m \in M \rightsquigarrow g \mapsto m^{-1}gm$ is a cocycle.

If $c \in Z^1(G, M)$ and $m \in M$, then $g \mapsto m^{-1}c(g)gm$ is a cocycle. This defines a right M-action on $Z^1(G, M)$, and thereby defines an equivalence relation $\sim$, called **cohomologous**, allowing us to define

$$H^1(G, M) := Z^1(G, M)/\sim .$$

Note that $H^1(G, M)$ is only a **pointed set**, in which the special point is

$$1 = [g \mapsto 1] = [g \mapsto m^{-1}gm].$$

Example 6.6 (Classify semli-linear representations)**.** Let R be a *commutative* topological ring with a continuous G-action compatible with the ring structure on R, X be a free R-module of rank d with a semi-linear G-action. By choosing a basis $e = \{e_1, \dots, e_d\}$ of X, we write for each $g \in G$ the matrix $M_e(g)$ in the basis e, and thus define a cocyle

$$G \to \mathrm{GL}_d(R), \quad g \mapsto M_e(g).$$

- Indeed, G acts on $\mathrm{GL}_d(R)$ "element-wisely", i.e,

  $$gA = g(a_{ij})_{i,j} := (ga_{ij})_{i,j}.$$

  Write $\boldsymbol{e} = (e_1 \ \cdots \ e_d)$. Recall that the i-th column $(g_{1i} \ \cdots \ g_{di})^{\mathrm{t}}$ of $M_e(g)$ is defined by

  $$ge_i = g_{1i}e_1 + \cdots + g_{di}e_d = \boldsymbol{e} \cdot \begin{pmatrix} g_{1i} \\ \vdots \\ g_{di} \end{pmatrix}.$$

  Or $g\boldsymbol{e} = e \cdot M_e(g)$. If

  $$x = \boldsymbol{e} \begin{pmatrix} x_1 \\ \vdots \\ x_d \end{pmatrix}, \quad g \in G,$$

  then

  $$gx = \boldsymbol{e} \cdot M_e(g) \cdot \begin{pmatrix} gx_1 \\ \vdots \\ gx_d \end{pmatrix}.$$

  Hence

  $$ghx = \boldsymbol{e} \cdot M_e(g) \cdot gM_e(h) \cdot \begin{pmatrix} ghx_1 \\ \vdots \\ ghx_d \end{pmatrix},$$

  i.e., $M_e(gh) = M_e(g) \cdot gM_e(h)$.

[Classify extensions] Let M be a R-module.

If $f = \{f_1, \dots, f_d\}$ is another basis of X, and P is the matrix of f in e, i.e.,

$$f_i = \boldsymbol{e} \cdot i\text{-th column of } P.$$

Then

$$M_f(g) = P^{-1} \cdot M_e(g) \cdot gP.$$

- Write $\boldsymbol{f} = \boldsymbol{e} \cdot P$, then

$$\boldsymbol{e}PM_f(g) = \boldsymbol{f}M_f(g) = g\boldsymbol{f} = g(\boldsymbol{e}P) = g\boldsymbol{e} \cdot gP = \boldsymbol{e}M_e(g)g(P).$$

Therefore, we assign to each R-semi-linear G-representation X a class $[X] \in H^1(G, \mathrm{GL}_d(R))$.

6.7 The First Applications in Galois Cohomology

In this subsection, let L/K be a *finite* Galois extension, $G := \mathrm{Gal}(L/K)$. Then both L and $L^\times$ have natural G-module structures.

6.7.1 Hilbert's Theorem 90 and $H^1(G, \mathrm{GL}_d(L))$

Theorem 24 (Dedekind-Artin)**.** Let Γ be a monoid, E be a integral domain, and $\mathrm{Hom}_\times(\Gamma, E)$ the set of monoid homomorphisms $\Gamma \to E$. [24] Then $\mathrm{Hom}_\times(\Gamma, E)$ is a linearly independent set over E; i.e, for $a_\chi \in E$,

$$\sum_{\chi \in \mathrm{Hom}_\times(\Gamma, E)} a_\chi \chi(\cdot) = 0 \text{ on } E \implies a_\chi = 0, \forall \chi.$$

Proof. Suppose that $J := \{\chi \in \mathrm{Hom}_\times(\Gamma, E) \mid a_\chi \neq 0\} \neq \varnothing$. The idea is to take $(a_\chi)_\chi$ s.t. $J = J((a_\chi)_\chi)$ is nonempty but minimal.

Since $\chi(1) = 1 \neq 0 \in E$, we have $\#J > 1$. Let ξ, η be two different characters $\Gamma \to E$. Then $\exists g \in \Gamma$ s.t. $\xi(g) \neq \eta(g)$. Note that

$$\sum_{\chi \in J} a_\chi \chi(g)\chi(\cdot) = \sum_{\chi \in J} a_\chi \chi(g\,\cdot) = 0,$$

$$\sum_{\chi \in J} a_\chi \xi(g)\chi(\cdot) = \xi(g) \sum_{\chi \in J} a_\chi \chi(\cdot) = 0,$$

and subtracting these two identities yields

$$\sum_{\chi \in J \smallsetminus \{\xi\}} a_\chi(\chi(g) - \xi(g))\chi(\cdot) = 0.$$

This new identity is nontrivial sicne $\eta(g) - \chi(g) \neq 0$, but concerns strictly lesser characters than J. Contradiction. ∎

Proposition 6.3. $H^1(\mathrm{Gal}(L/K), L^\times) = 0$.

In other words, if $\varphi : G \to L^\times$ is a crossed homomorphism, i.e.,

$$\varphi(gh) = g\varphi(h)\varphi(g),\ \forall g, h \in G,$$

then $\exists b_\varphi \in L^\times$ s.t.

$$\varphi(g) = \frac{gb_\varphi}{b_\varphi},\ \forall g \in G.$$

Proof. Take $a \in L^\times$ and define

$$b := \sum_{g \in G} \varphi(g) \cdot ga \in L.$$

[24] The set $\mathrm{Hom}_\times(\Gamma, E)$ admits a E-module structure defined point-wisely. The elements in $\mathrm{Hom}_\times(\Gamma, E)$ are sometimes called characters.

Then

$$hb = \sum_{g \in G} h\varphi(g) \cdot hga = \sum_{g \in G} \frac{\varphi(hg)}{\varphi(h)} hga = \frac{b}{\varphi(h)}.$$

Hence if $b \neq 0$, we would have $\varphi(g) = b/gb = g(b^{-1})/b^{-1}$. By Theorem 24, $\mathrm{Gal}(L/K) \subset \mathrm{Hom}_\times(L, L)$ is linearly independent over L, so $\sum_{g \in G} \varphi(g)g(\cdot) : L \to L$ is a non-zero function, and thus can we find $a \in L$ with $b \neq 0$. ◻

Corollary 6.2. Let L/K be a finite cyclic extension, σ a generator of $G = \mathrm{Gal}(L/K)$, and $a \in L$. If $N_{L/K} a = 1$, then $\exists b \in L^\times$ s.t. $a = \sigma b/b$.

Proof. For the G-module $L^\times$, the norm map

$$N_G = N_{L/K} : x \mapsto \prod_{g \in G} gx.$$

So

$$\frac{\ker(N_{L/K})}{(\sigma(\cdot)/\,\mathrm{id}(\cdot))L^\times} = \hat{H}^{-1}(G, L^\times) \simeq H^1(G, L^\times) = 0.$$ ◻

Note that $L^\times = \mathrm{GL}_1(L)$. The result above extends to higher $\mathrm{GL}_d(L)$.

Theorem 25 (Artin)**.** If L is an infinite field, G is a finite subgroup of field automorphisms $\mathrm{Aut}(L)$ of L, then the elements of G are algebraically independent over L.

Theorem 26 (Hilbert 90)**.** If L/K is finite Galois, then $H^1(\mathrm{Gal}(L/K), \mathrm{GL}_d(L)) = 0$ for all $d \in \mathbb{Z}_{\geq 1}$.

Proof. Let $\varphi : G \to \mathrm{GL}_d(L)$ be a cocycle. Similarly, take $a \in L^\times$ and consider

$$P(a) := \sum_{g \in G} ga \cdot \varphi(g).$$

Then

$$hP(a) = \sum_{g \in G} hga \cdot h\varphi(g) = \sum_{g \in G} hga \cdot \varphi(h)^{-1}\varphi(hg) = \varphi(h)^{-1}P(a),$$

so once $P(a) \in \mathrm{GL}_d(L)$, we would have $\varphi(g) = P(a)\,(hP(a))^{-1} = \left(P(a)^{-1}\right)^{-1} h(P(a)^{-1})$.

(1) *K is infinite.* Let $\boldsymbol{X} = \{X_g\}_{g \in G}$ be a set of variables. Consider

$$Q(\boldsymbol{X}) := \det\left(\sum_{g \in G} X_g \varphi(g)\right) \in L[\boldsymbol{X}].$$

Note that $Q(\{g(\cdot)\}_{g \in G}) : L \to L$ is a polynomial in automorphisms of L, and $Q(\{ga\}_{g \in G}) = \det P(a)$. The polynomial $Q \neq 0$, because, for instance, Q evaluated at $X_g = 0$ for all $g \neq 1$ and $X_1 = 1$ is $\det \varphi(1) = 1$. By Artin's Theorem 25, $Q(\{g(\cdot)\}_{g \in G}) \neq 0$, hence $\exists a \in L$ s.t. $\det P(a) \neq 0$.

(2) *G is cyclic.* Pick a generator σ of $G \simeq \mathbb{Z}/n\mathbb{Z}$. Then

$$P(a) = \sum_{i=1}^{n} \sigma^i a \cdot \frac{\sigma^i - 1}{\sigma - 1} \varphi(\sigma)$$

(T.B.C.)

◻

6.7.2 Normal Basis and $H^r(G, L)$

Theorem 27 (Normal basis theorem)**.** Any finite Galois extension L/K admits a normal basis; i.e, $\exists x \in L$ s.t. $\{\sigma x \mid \sigma \in \mathrm{Gal}(L/K)\}$ forms a K-basis of L.

We prove this in two cases: 1) K is infinite and 2) L/K is finite cyclic.

Proof in case K infinite. (T.B.C.) ☐

Proof in case G cyclic. (T.B.C.) ☐

Proposition 6.4. L is an induced $G = \mathrm{Gal}(L/K)$-module, hence $H^r(G, L) = 0$ for all $r \geq 1$.

Proof. By Theorem 27, we choose $x \in L$ with $L = \bigoplus_{g \in G} Kgx$, giving an isomorphism

$$K[G] \to L, \quad \sum_{g \in G} a_g g \to \sum_{g \in G} a_g gx$$

as G-modules. Hence as a G-module, $L \simeq K[G] \simeq K \otimes_{\mathbb{Z}} \mathbb{Z}[G] \simeq \mathrm{Ind}^G(K)$. ☐

Remark. We can use $H^1(G, \mathrm{GL}_2(L)) = 0$ to deduce that $H^1(G, L) = 0$ via the following trick: a cocycle $c : G \to L$ defines a cocycle

$$\begin{pmatrix} 1 & c \\ & 1 \end{pmatrix} : G \to \mathrm{GL}_2(L).$$

Hence,

Corollary 6.3. Let L/K be a finite cyclic extension, σ a generator of G, and $a \in L$. If $\mathrm{Tr}_{L/K}\, a = 0$, then $\exists b \in L$ s.t. $a = \sigma b - b$.

Proof. For the G-module L, the norm map

$$N_G = \mathrm{Tr}_{L/K} : x \mapsto \sum_{g \in G} gx.$$

Now use $H^1(G, L) \simeq \hat{H}^{-1}(G, L)$. ☐

6.7.3 Kummer Theory