Part III — Local Fields

Theorems

Based on lectures by H. C. Johansson

Notes taken by Dexter Chua

Michaelmas 2016

The p-adic numbers $\mathbb{Q}_p$ (where p is any prime) were invented by Hensel in the late 19th century, with a view to introduce function-theoretic methods into number theory. They are formed by completing $\mathbb{Q}$ with respect to the p-adic absolute value $|-|_p$, defined for non-zero $x \in \mathbb{Q}$ by $|x|_p = p^{-n}$, where $x = p^n a/b$ with $a, b, n \in \mathbb{Z}$ and a and b are coprime to p. The p-adic absolute value allows one to study congruences modulo all powers of p simultaneously, using analytic methods. The concept of a local field is an abstraction of the field $\mathbb{Q}_p$, and the theory involves an interesting blend of algebra and analysis. Local fields provide a natural tool to attack many number-theoretic problems, and they are ubiquitous in modern algebraic number theory and arithmetic geometry.

Topics likely to be covered include:

> The p-adic numbers. Local fields and their structure.
>
> Finite extensions, Galois theory and basic ramification theory.
>
> Polynomial equations; Hensel's Lemma, Newton polygons.
>
> Continuous functions on the p-adic integers, Mahler's Theorem.
>
> Local class field theory (time permitting).

Pre-requisites

Basic algebra, including Galois theory, and basic concepts from point set topology and metric spaces. Some prior exposure to number fields might be useful, but is not essential.

Contents

0 Introduction

1 Basic theory

1.1 Fields

Proposition. $||x| - |y|| \leq |x - y|$. Here the outer absolute value on the left hand side is the usual absolute value of $\mathbb{R}$, while the others are the absolute values of the relevant field.

Proposition. Let K be a field, and $|\cdot|, |\cdot|'$ be absolute values on K. Then the following are equivalent.

(i) $|\cdot|$ and $|\cdot|'$ are equivalent

(ii) $|x| < 1$ implies $|x|' < 1$ for all $x \in K$

(iii) There is some $s \in \mathbb{R}_{>0}$ such that $|x|^s = |x|'$ for all $x \in K$.

Proposition. Let $(K, |\cdot|)$ be a non-archimedean valued field, and let $x \in K$ and $r \in \mathbb{R}_{>0}$. Let $z \in B(x, r)$. Then

$$B(x, r) = B(z, r).$$

Corollary. Closed balls are open.

Proposition. Let K be a non-archimedean valued field, and $x, y \in K$. If $|x| > |y|$, then $|x + y| = |x|$.

More generally, if $x = \sum_{c=0}^{\infty} x_i$ and the non-zero $|x_i|$ are distinct, then $|x| = \max |x_i|$.

Proposition. Let K be a valued field.

(i) Let (x_n) be a sequence in K. If $x_n - x_{n+1} \to 0$, then x_n is Cauchy.

If we assume further that K is complete, then

(ii) Let (x_n) be a sequence in K. If $x_n - x_{n+1} \to 0$, then a sequence (x_n) in K converges.

(iii) Let $\sum_{n=0}^{\infty} y_n$ be a series in K. If $y_n \to 0$, then $\sum_{n=0}^{\infty} y_n$ converges.

Proposition. Let K be a valued field. Then

$$\mathcal{O}_K = \{x : |x| \leq 1\}$$

is an open subring of K. Moreover, for each $r \in (0, 1]$, the subsets $\{x : |x| < r\}$ and $\{x : |x| \leq r\}$ are open ideals of $\mathcal{O}_K$. Moreover, $\mathcal{O}_K^\times = \{x : |x| = 1\}$.

1.2 Rings

Theorem. Let $R \subseteq S$ be rings. Then $s_1, \cdots, s_n \in S$ are all integral iff $R[s_1, \cdots, s_n] \subseteq S$ is a finitely-generated R-module.

Proposition. For any A, we have $A^*A = AA^* = \det(A)I$, where I is the identity matrix.

Corollary. Let $R \subseteq S$ be rings. If $s_1, s_2 \in S$ are integral over R, then $s_1 + s_2$ and $s_1 s_2$ are integral over R. In particular, the set $\tilde{R} \subseteq S$ of all elements in S integral over R is a ring, known as the integral closure of R in S.

1.3 Topological rings

Proposition. The set of all I-adically open sets form a topology on R, called the *I-adic topology*.

Proposition. The inverse limit topology is a ring topology.

Proposition. Giving a continuous ring homomorphism $g : S \to \varprojlim R_n$ is the same as giving a continuous ring homomorphism $g_n : S \to R_n$ for each n, such that each of the following diagram commutes:

$$\begin{array}{ccc} S & \xrightarrow{g_n} & R_n \\ & \searrow^{g_{n-1}} & \downarrow{\scriptstyle f_{n-1}} \\ & & R_{n-1} \end{array}$$

1.4 The p-adic numbers

Proposition. The p-adic absolute value is an absolute value.

Proposition. $\mathbb{Z}_p$ is the closure of $\mathbb{Z}$ inside $\mathbb{Q}_p$.

Proposition. The non-zero ideals of $\mathbb{Z}_p$ are $p^n\mathbb{Z}_p$ for $n \geq 0$. Moreover,

$$\frac{\mathbb{Z}}{p^n\mathbb{Z}} \cong \frac{\mathbb{Z}_p}{p^n\mathbb{Z}_p}.$$

Corollary. $\mathbb{Z}_p$ is a PID with a unique prime element p (up to units).

Proposition. The topology on $\mathbb{Z}$ induced by $|\cdot|_p$ is the p-adic topology (i.e. the $p\mathbb{Z}$-adic topology).

Proposition. $\mathbb{Z}_p$ is p-adically complete and is (isomorphic to) the p-adic completion of $\mathbb{Z}$.

Corollary. Every $a \in \mathbb{Z}_p$ has a unique expansion

$$a = \sum_{i=0}^{\infty} a_i p^i.$$

with $a_i \in \{0, \cdots, p-1\}$.

More generally, for any $a \in \mathbb{Q}^\times$, there is a unique expansion

$$a = \sum_{i=n}^{\infty} a_i p^i$$

for $a_i \in \{0, \cdots, p-1\}$, $a_n \neq 0$ and

$$n = -\log_p |a|_p \in \mathbb{Z}.$$

2 Valued fields

2.1 Hensel's lemma

Theorem (Hensel's lemma)**.** Let K be a complete valued field, and let $f \in K[x]$ be primitive. Put $\bar{f} = f \bmod \mathfrak{m} \in k[x]$. If there is a factorization

$$\bar{f}(x) = \bar{g}(x)\bar{h}(x)$$

with $(\bar{g}, \bar{h}) = 1$, then there is a factorization

$$f(x) = g(x)h(x)$$

in $\mathcal{O}[x]$ with

$$\bar{g} = g, \quad \bar{h} = h \mod \mathfrak{m},$$

with $\deg g = \deg \bar{g}$.

Corollary. Let $f(x) = a_0 + a_1 x + \cdots + a_n x^n \in K[x]$ where K is complete and $a_0, a_n \neq 0$. If f is irreducible, then

$$|a_\ell| \leq \max(|a_0|, |a_n|)$$

for all ℓ.

Corollary (of Hensel's lemma)**.** Let $f \in \mathcal{O}[x]$ be monic, and K complete. If $f \bmod \mathfrak{m}$ has a simple root $\bar{\alpha} \in k$, then f has a (unique) simple root $\alpha \in \mathcal{O}$ lifting $\bar{\alpha}$.

2.2 Extension of norms

Theorem. Let K be a complete valued field, and let L/K be a finite extension. Then the absolute value on K has a unique extension to an absolute value on L, given by

$$|\alpha|_L = \sqrt[n]{|N_{L/K}(\alpha)|},$$

where $n = [L : K]$ and $N_{L/K}$ is the field norm. Moreover, L is complete with respect to this absolute value.

Corollary. Let K be complete and M/K be an algebraic extension of K. Then $|\cdot|$ extends uniquely to an absolute value on M.

Corollary. Let K be a complete valued field and L/K a finite extension. If $\sigma \in \mathrm{Aut}(L/K)$, then $|\sigma(\alpha)|_L = |\alpha|_L$.

Proposition. Let K be a complete valued field, and V a finite-dimensional K-vector space. Then V is complete under the max norm.

Proposition. Let K be a complete valued field, and V a finite-dimensional K-vector space. Then any norm $\|\cdot\|$ on V is equivalent to $\|\cdot\|_{\max}$.

Corollary. V is complete with respect to any norm.

Lemma. Let K be a valued field. Then the valuation ring $\mathcal{O}_K$ is integrally closed in K.

Lemma. Let L be a field and $|\cdot|$ a function that satisfies all axioms of an absolute value but the strong triangle inequality. Then $|\cdot|$ is an absolute value iff $|\alpha| \leq 1$ implies $|\alpha + 1| \leq 1$.

Theorem. Let K be a complete valued field, and let L/K be a finite extension. Then the absolute value on K has a unique extension to an absolute value on L, given by

$$|\alpha|_L = \sqrt[n]{|N_{L/K}(\alpha)|},$$

where $n = [L : K]$ and $N_{L/K}$ is the field norm. Moreover, L is complete with respect to this absolute value.

Corollary (of the proof)**.** Let K be a complete valued field, and L/K a finite extension. We equip L with $|\cdot|_L$ extending $|\cdot|$ on K. Then $\mathcal{O}_L$ is the integral closure of $\mathcal{O}_K$ in L.

2.3 Newton polygons

Theorem. Let K be complete valued field, and v the valuation on K. We let

$$f(x) = a_0 + a_1 x + \cdots + a_n x^n \in K[x].$$

Let L be the splitting field of f over K, equipped with the unique extension w of v.

If $(r, v(a_r)) \to (s, v(a_s))$ is a line segment of the Newton polygon of f with slope $-m \in \mathbb{R}$, then f has precisely $s - r$ roots of valuation m.

Corollary. If f is irreducible, then the Newton polygon has a single line segment.

3 Discretely valued fields

Proposition. Let K be a discretely valued field with uniformizer π. Let $S \subseteq \mathcal{O}_K$ be a set of coset representatives of $\mathcal{O}_k/\mathfrak{m}_k = k_K$ containing 0. Then

(i) The non-zero ideals of $\mathcal{O}_K$ are $\pi^n\mathcal{O}_K$ for $n \geq 0$.

(ii) The ring $\mathcal{O}_K$ is a PID with unique prime π (up to units), and $\mathfrak{m}_K = \pi\mathcal{O}_K$.

(iii) The topology on $\mathcal{O}_K$ induced by the absolute value is the π-adic topology.

(iv) If K is complete, then $\mathcal{O}_K$ is π-adically complete.

(v) If K is complete, then any $x \in K$ can be written uniquely as

$$x = \sum_{n \gg -\infty}^{\infty} a_n \pi^n,$$

where $a_n \in S$, and

$$|x| = |\pi|^{-\inf\{n : a_n \neq 0\}}.$$

(vi) The completion $\hat{K}$ is also discretely valued and π is a uniformizer, and moreover the natural map

$$\frac{\mathcal{O}_k}{\pi^n\mathcal{O}_k} \xrightarrow{\sim} \frac{\mathcal{O}_{\hat{K}}}{\pi^n\mathcal{O}_{\hat{K}}}$$

is an isomorphism.

Proposition. Let K be a discretely valued field. Then K is a local field iff $\mathcal{O}_K$ is compact.

Proposition. R is a DVR iff $R \cong \mathcal{O}_K$ for some DVF K.

3.1 Teichmüller lifts

Theorem. Let R be a ring, and let $x \in R$. Assume that R is x-adically complete and that R/xR is perfect of characteristic p. Then there is a unique map $[-] : R/xR \to R$ such that

$$[a] \equiv a \mod x$$

and

$$[ab] = [a][b].$$

for all $a, b \in R/xR$. Moreover, if R has characteristic p, then $[-]$ is a ring homomorphism.

Lemma. Let R be a ring with $x \in R$ such that R/xR has characteristic p. Let $\alpha, \beta \in R$ be such that

$$\alpha = \beta \mod x^k \tag{$\dagger$}$$

Then we have

$$\alpha^p = \beta^p \mod x^{k+1}.$$

Theorem. Let K be a complete discretely valued field of equal characteristic p, and assume that k_K is perfect. Then $K \cong k_K((T))$.

Corollary. Let K be a local field of equal characteristic p. Then $k_K \cong \mathbb{F}_q$ for some q a power of p, and $K \cong F_q((T))$.

3.2 Witt vectors*

Lemma. Let A be a strict p-ring. Then any element of A can be written uniquely as

$$a = \sum_{n=0}^{\infty} [a_n] p^n,$$

for a *unique* $a_n \in A/pA$.

Lemma. Let A and B be strict p-rings and let $f : A/pA \to B/pB$ be a ring homomorphism. Then there is a unique homomorphism $F : A \to B$ such that $f = F \bmod p$, given by

$$F\left(\sum [a_n] p^n\right) = \sum [f(a_n)] p^n.$$

Proposition. Let A be a strict p-ring and B be a ring with an element x such that B is x-adically complete and B/xB is perfect of characteristic p. If $f : A/pA \to B/xB$ is a ring homomorphism. Then there exists a unique ring homomorphism $F : A \to B$ with $f = F \mod x$, i.e. the following diagram commutes:

$$\begin{array}{ccc} A & \xrightarrow{F} & B \\ \downarrow & & \downarrow \\ A/pA & \xrightarrow{f} & B/xB \end{array} .$$

Theorem. Let R be a perfect ring. Then there is a unique (up to isomorphism) strict p-ring $W(B)$ called the *Witt vectors* of R such that $W(R)/pW(R) \cong R$.

Moreover, for any other perfect ring R, the reduction mod p map gives a bijection

$$\mathrm{Hom}_{\mathrm{Ring}}(W(R), W(R')) \xrightarrow{\sim} \mathrm{Hom}_{\mathrm{Ring}}(R, R') \ .$$

Proposition. A complete DVR A of mixed characteristic with perfect residue field and such that p is a uniformizer is the same as a strict p-ring A such that A/pA is a field.

Corollary. Let R be a complete DVR of mixed characteristic with absolute ramification index 1 and perfect residue field k. Then $R \cong W(k)$.

Theorem. Let R be a complete DVR of mixed characteristic p with a perfect residue field k and uniformizer π. Then R is finite over $W(k)$.

Corollary. Let K be a mixed characteristic local field. Then K is a finite extension of $\mathbb{Q}_p$.

4 Some p-adic analysis

Proposition. Let K be a complete valued field with an absolute value $|\cdot|$ and assume that $K \supseteq \mathbb{Q}_p$ and $|\cdot|$ restricts to the usual p-adic norm on $\mathbb{Q}_p$. Then $\exp(x)$ converges for $|x| < p^{-1/(p-1)}$ and $\log(1+x)$ converges for $|x| < 1$, and then define continuous maps

$$\exp : \{x \in K : |x| < p^{-1/(p-1)}\} \to \mathcal{O}_K$$
$$\log : \{1 + x \in K : |x| < 1\} \to K.$$

Theorem (Mahler's theorem)**.** Let $f : \mathbb{Z}_p \to \mathbb{Q}_p$ be any continuous function. Then there is a unique sequence $(a_n)_{n\geq 0}$ with $a_n \in \mathbb{Q}_p$ and $a_n \to 0$ such that

$$f(x) = \sum_{n=0}^{\infty} a_n \binom{x}{n},$$

and moreover

$$\sup_{x\in\mathbb{Z}_p} |f(x)| = \max_{k\in\mathbb{N}} |a_k|.$$

Proposition. The norm $\|\cdot\|$ defined above is in fact a (non-archimedean) norm, and that $C(\mathbb{Z}_p, \mathbb{Q}_p)$ is complete under this norm.

Lemma. Let $f \in C(\mathbb{Z}_p, \mathbb{Q}_p)$. Then there exists some $k \geq 1$ such that

$$\|\Delta^{p^k} f\| \leq \frac{1}{p}\|f\|.$$

Proposition. The map $f \mapsto (a_n(f))_{n=0}^{\infty}$ defines an injective norm-decreasing linear map $C(\mathbb{Z}_p, \mathbb{Q}_p) \to c_0$.

Lemma. We have

$$\binom{x}{n} + \binom{x}{n-1} = \binom{x+1}{n}$$

for all $n \in \mathbb{Z}_{\geq 1}$ and $x \in \mathbb{Z}_p$.

Proposition. Let $a = (a_n)_{n=0}^{\infty} \in c_0$. We define $f_a : \mathbb{Z}_p \to \mathbb{Q}_p$ by

$$f_a(x) = \sum_{n=0}^{\infty} a_n \binom{x}{n}.$$

This defines a norm-decreasing linear map $c_0 \to C(\mathbb{Z}_p, \mathbb{Q}_p)$. Moreover $a_n(f_a) = a_n$ for all $n \geq 0$.

Lemma. Suppose V, W are normed spaces, and $F : V \to W$, $G : W \to V$ are maps such that F is injective and norm-decreasing, and G is norm-decreasing and $FG = \mathrm{id}_W$. Then $GF = \mathrm{id}_V$ and F and G are norm-preserving.

5 Ramification theory for local fields

5.1 Ramification index and inertia degree

Theorem. Let L/K be a finite extension. Then

$$[L : K] = e_{L/K} f_{L/K}.$$

Proposition. Let K be a local field, and L/K a finite extension of degree n. Then $\mathcal{O}_L$ is a finitely-generated and free $\mathcal{O}_K$ module of rank n, and k_L/k_K is an extension of degree $\leq n$.

Moreover, L is also a local field.

Theorem. Let L/K be a finite extension. Then

$$[L : K] = e_{L/K} f_{L/K},$$

and there is some $\alpha \in \mathcal{O}_L$ such that $\mathcal{O}_L = \mathcal{O}_K[\alpha]$.

Corollary. If $M/L/K$ is a tower of finite extensions of local fields, then

$$f_{M/K} = f_{L/K} f_{M/L}$$
$$e_{M/K} = e_{L/K} e_{M/L}$$

5.2 Unramified extensions

Theorem. Let K be a local field. For every finite extension ℓ/k_K, there is a *unique* (up to isomorphism) finite unramified extension L/K with $k_L \cong \ell$ over k_K. Moreover, L/K is Galois with

$$\mathrm{Gal}(L/K) \cong \mathrm{Gal}(\ell/k_K).$$

Lemma. Let L/K be a finite unramified extension of local fields and let M/K be a finite extension. Then there is a natural bijection

$$\mathrm{Hom}_{K\text{-}\mathrm{Alg}}(L, M) \longleftrightarrow \mathrm{Hom}_{k_K\text{-}\mathrm{Alg}}(k_L, k_M)$$

given in one direction by restriction followed by reduction.

Proposition. Let K be a local field, and L/K a finite unramified extension, and M/K finite. Say L, M are subfields of some fixed algebraic closure $\bar{K}$ of K. Then LM/M is unramified. Moreover, any subextension of L/K is unramified over K. If M/K is unramified as well, then LM/K is unramified.

Corollary. Let K be a local field, and L/K finite. Then there is a unique maximal subfield $K \subseteq T \subseteq L$ such that T/K is unramified. Moreover, $[T : K] = f_{L/K}$.

5.3 Totally ramified extensions

Theorem (Eisenstein criterion)**.** Let K be a local field, and $f(x) = x^n + a_{n-1}x^{n-1} + \cdots + a_0 \in \mathcal{O}_K[x]$. Let π_K be the uniformizer of K. If $\pi_K \mid a_{n-1}, \cdots, a_0$ and $\pi_K^2 \nmid a_0$, then f is irreducible.

Proposition. Let L/K be an extension of local fields, and v_K be the normalized valuation. Let w be the unique extension of v_K to L. Then the ramification index $e_{L/K}$ is given by

$$e_{L/K}^{-1} = w(\pi_L) = \min\{w(x) : x \in \mathfrak{m}_L\},$$

Proposition. Let L/K be a totally ramified extension of local fields. Then $L = K(\pi_L)$ and the minimal polynomial of π_L over K is Eisenstein.

Conversely, if $L = K(\alpha)$ and the minimal polynomial of α over K is Eisenstein, then L/K is totally ramified and α is a uniformizer of L.

6 Further ramification theory

6.1 Some filtrations

Proposition. We have

$$U_K/U_K^{(1)} \cong (k_K^\times, \cdot),$$
$$U_K^{(s)}/U_K^{(s+1)} \cong (k_K, +).$$

for $s \geq 1$.

Proposition. Let L/K be a finite Galois extension of local fields. Then the homomorphism

$$\mathrm{Gal}(L/K) \to \mathrm{Gal}(k_L/k_K)$$

given by reduction is surjective.

Lemma. Let L/K be a finite Galois extension of local fields, and let $\sigma \in I(L/K)$. Then $\sigma([x]) = [x]$ for all x.

More generally, let $x \in k_L$ and $\sigma \in \mathrm{Gal}(L/K)$ with image $\bar{\sigma} \in \mathrm{Gal}(k_L/k_K)$. Then we have

$$[\bar{\sigma}(x)] = \sigma([x]).$$

Proposition. Let L/K be a finite Galois extension of local fields, and v_L the normalized valuation of L. Let π_L be the uniformizer of L. Then $G_{s+1}(L/K)$ is a normal subgroup of $G_s(L/K)$ for $s \in \mathbb{Z}_{\geq 0}$, and the map

$$\frac{G_s(L/K)}{G_{s+1}(L/K)} \to \frac{U_L^{(s)}}{U_L^{(s+1)}}$$

given by

$$\sigma \mapsto \frac{\sigma(\pi_L)}{\pi_L}$$

is a well-defined injective group homomorphism, independent of the choice of π_L.

Corollary. $\mathrm{Gal}(L/K)$ is solvable.

Proposition. $G_1(L/K)$ is always a p-group.

6.2 Multiple extensions

Proposition. Let $M/L/K$ be finite extensions of local fields, and M/K Galois. Then

$$G_s(M/K) \cap \mathrm{Gal}(M/L) = G_s(M/L).$$

Theorem (Herbrand's theorem)**.** Let $M/L/K$ be finite extensions of local fields with M/K and L/K Galois. Then there is some function $\eta_{M/L}$ such that

$$G_t(L/K) \cong \frac{G_s(M/K)}{G_s(M/L)}$$

for all s, where $t = \eta_{M/L}(s)$.

Proposition. Let L/K be a finite Galois extension of local fields, and pick $\alpha \in \mathcal{O}_L$ such that $\mathcal{O}_L = \mathcal{O}_K[\alpha]$. Then

$$i_{L/K}(\sigma) = v_L(\sigma(\alpha) - \alpha).$$

Proposition. Let $M/L/K$ be a finite extension of local fields, such that M/K and L/K are Galois. Then for $\sigma \in \mathrm{Gal}(L/K)$, we have

$$i_{L/K}(\sigma) = e_{M/L}^{-1} \sum_{\substack{\tau \in \mathrm{Gal}(M/K) \\ \tau|_L = \sigma}} i_{M/K}(\tau).$$

Theorem (Herbrand's theorem)**.** Let $M/L/K$ be a finite extension of local fields with M/K and L/K Galois. We set

$$H = \mathrm{Gal}(M/L), \quad t = \eta_{M/L}(s).$$

Then we have

$$\frac{G_s(M/K)H}{H} = G_t(L/K).$$

By some isomorphism theorem, and the fact that $H \cap G_s(M/K) = G_s(M/L)$, this is equivalent to saying

$$G_t(L/K) \cong \frac{G_s(M/K)}{G_s(M/L)}.$$

Proposition. Write $G = \mathrm{Gal}(L/K)$. Then

$$\eta_{L/K}(s) = \int_0^s \frac{\mathrm{d}x}{(G_0(L/K) : G_x(L/K))}.$$

When $-1 \leq x < 0$, our convention is that

$$\frac{1}{(G_0(L/K) : G_x(L/K))} = (G_x(L/K) : G_0(L/K)),$$

which is just equal to 1 when $-1 < x < 0$. So

$$\eta_{L/K}(s) = s \text{ if } -1 \leq s \leq 0.$$

Lemma. Let $M/L/K$ be a finite extension of local fields, and M/K and L/K be Galois. Then

$$\eta_{M/K} = \eta_{L/K} \circ \eta_{M/L}.$$

Hence

$$\psi_{M/K} = \psi_{M/L} \circ \psi_{L/K}.$$

Corollary. Let $M/L/K$ be finite Galois extensions of local fields, and $H = \mathrm{Gal}(M/L)$. Let $t \in [-1, \infty)$. Then

$$\frac{G^t(M/K)H}{H} = G^t(L/K).$$

7 Local class field theory

7.1 Infinite Galois theory

Proposition. Let M/K be a Galois extension. Then $\mathrm{Gal}(M/K)$ is compact and Hausdorff, and if $U \subseteq \mathrm{Gal}(M/K)$ is an open subset such that $1 \in U$, then there is an open normal subgroup $N \subseteq \mathrm{Gal}(M/K)$ such that $N \subseteq U$.

Proposition. Let M/K be a Galois extension. The set I of finite Galois subextensions L/K is a directed system under inclusion. If $L, L' \in I$ and $L \subseteq L'$, then we have a restriction map

$$\cdot|_L^{L'} : \mathrm{Gal}(L'/K) \to \mathrm{Gal}(L/K).$$

Then $(\mathrm{Gal}(L/K), \cdot|_L^{L'})$ is an inverse system, and the map

$$\begin{aligned} \mathrm{Gal}(M/K) &\to \varprojlim_{i \in I} \mathrm{Gal}(L/K) \\ \sigma &\mapsto (\sigma|_L)_{i \in I} \end{aligned}$$

is an isomorphism of topological groups.

Theorem (Fundamental theorem of Galois theory)**.** Let M/K be a Galois extension. Then the map $L \mapsto \mathrm{Gal}(M/L)$ defines a bijection between subextensions L/K of M/K and closed subgroups of $\mathrm{Gal}(M/K)$, with inverse given by sending $H \mapsto M^H$, the fixed field of H.

Moreover, L/K is finite if and only if $\mathrm{Gal}(M/L)$ is open, and L/K is Galois iff $\mathrm{Gal}(M/L)$ is normal, and then

$$\frac{\mathrm{Gal}(L/K)}{\mathrm{Gal}(M/L)} \to \mathrm{Gal}(L/K)$$

is an isomorphism of topological groups.

7.2 Unramified extensions and Weil group

Proposition. Let M/K be an unramified extension of local fields. Then M/K is Galois, and

$$\mathrm{Gal}(M/K) \cong \mathrm{Gal}(k_M/k_K)$$

via the reduction map.

Proposition. Let K be a local field, and M/K Galois. Then $W(M/K)$ is dense in $\mathrm{Gal}(M/K)$. Equivalently, for any finite Galois subextension L/K of M/K, the restriction map $W(M/K) \to \mathrm{Gal}(L/K)$ is surjective.

If L/K is a finite subextension of M/K, then

$$W(M/L) = W(M/K) \cap \mathrm{Gal}(M/L).$$

If L/K is also Galois, then

$$\frac{W(M/K)}{W(M/L)} \cong \mathrm{Gal}(L/K)$$

via restriction.

7.3 Main theorems of local class field theory

Theorem (Local Artin reciprocity)**.** There exists a unique topological isomorphism

$$\mathrm{Art}_K : K^\times \to W(K^{\mathrm{ab}}/K)$$

characterized by the properties

(i) $\mathrm{Art}_K(\pi_K)|_{K^{\mathrm{ur}}} = \mathrm{Frob}_K$, where π_K is *any* uniformizer.

(ii) We have

$$\mathrm{Art}_K(N_{L/K}(x))|_L = \mathrm{id}_L$$

for all L/K finite abelian and $x \in L^\times$.

Moreover, if M/K is finite, then for all $x \in M^\times$, we know $\mathrm{Art}_M(x)$ is an automorphism of M^{ab}/M, and restricts to an automorphisms of K^{ab}/K. Then we have

$$\mathrm{Art}_M(x)|_K^{K^{\mathrm{ab}}} = \mathrm{Art}_K(N_{M/K}(x)).$$

Moreover, Art_K induces an isomorphism

$$\frac{K^\times}{N_{M/K}(M^\times)} \to \mathrm{Gal}\left(\frac{M \cap K^{\mathrm{ab}}}{K}\right).$$

Corollary. Let L/K be finite. Then $N(L/K) = N((L \cap K^{ab})/K)$, and

$$(K^\times : N(L/K)) \leq [L : K]$$

with equality iff L/K is abelian.

Theorem. Let K be a local field. Then there is an isomorphism of posets

$$\left\{\begin{array}{c}\text{open finite index}\\ \text{subgroups of } K^\times\end{array}\right\} \longleftrightarrow \left\{\begin{array}{c}\text{finite abelian}\\ \text{extensions of } L/K\end{array}\right\}$$

$$H \longmapsto (K^{\mathrm{ab}})^{\mathrm{Art}_K(H)}$$

$$N(L/K) \longmapsfrom L/K$$

.

In particular, for L/K and M/K finite abelian extensions, we have

$$N(LM/K) = N(L/K) \cap N(M/K),$$
$$N(L \cap M/K) = N(L/K)N(M/K).$$

Theorem. Let L/K be a finite extension, and M/K abelian. Then $N(L/K) \subseteq N(M/K)$ iff $M \subseteq L$.

8 Lubin–Tate theory

8.1 Motivating example

Lemma. Let L/K be a finite abelian extension. Then we have

$$e_{L/K} = (\mathcal{O}_K^\times : N_{L/K}(\mathcal{O}_L^\times)).$$

Corollary. Let L/K be a finite abelian extension. Then L/K is unramified if and only if $N_{L/K}(\mathcal{O}_L^\times) = \mathcal{O}_K^\times$.

Lemma. Let K be a local field, and let L_m/K be the extension corresponding to $\langle \pi_K^m \rangle \times \mathcal{O}_K$. Let

$$L = \bigcup_m L_m.$$

Then we have

$$K^{\mathrm{ab}} = K^{\mathrm{ur}} L,$$

Lemma. We have isomorphisms

$$\begin{aligned} W(K^{\mathrm{ab}}/K) &\cong W(K^{\mathrm{ur}}L/K) \\ &\cong W(K^{\mathrm{ur}}/K) \times \mathrm{Gal}(L/K) \\ &\cong \mathrm{Frob}_K^{\mathbb{Z}} \times \mathrm{Gal}(L/K) \end{aligned}$$

Theorem (Local Kronecker-Weber theorem)**.**

$$\begin{aligned} \mathbb{Q}_p^{\mathrm{ab}} &= \bigcup_{n \in \mathbb{Z}_{\geq 1}} \mathbb{Q}_p(\zeta_n), \\ \mathbb{Q}_p^{\mathrm{ur}} &= \bigcup_{\substack{n \in \mathbb{Z}_{\geq 1} \\ (n,p)=1}} \mathbb{Q}_p(\zeta_n). \end{aligned}$$

Theorem. We have

$$G^s(\mathbb{Q}_p^{\mathrm{ab}}/\mathbb{Q}_p) = \mathrm{Art}_{\mathbb{Q}_p}(1 + p^k\mathbb{Z}_p) = \mathrm{Art}_{\mathbb{Q}_p}(U^{(k)}),$$

where k is chosen such that $k - 1 < s \leq k$, $k \in \mathbb{Z}_{\geq 0}$.

Corollary. If $L/\mathbb{Q}_p$ is a finite abelian extension, then

$$G^s(L/\mathbb{Q}_p) = \mathrm{Art}_{\mathbb{Q}_p}\left(\frac{N(L/\mathbb{Q}_p)(1 + p^n\mathbb{Z}_p)}{N(L/\mathbb{Q}_p)}\right),$$

where $n - 1 < s \leq n$.

8.2 Formal groups

Lemma. Let R be a ring and F a formal group over R. Then

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

Also, there exists a power series $i(X) \in X \cdot R[[X]]$ such that

$$F(X, i(X)) = 0.$$

Lemma. Let $e_1, e_2 \in \mathcal{E}_\pi$ and take a linear form

$$L(x_1, \cdots, x_n) = \sum_{i=1}^n a_i X_i, \quad a_i \in \mathcal{O}_K.$$

Then there is a unique power series $F(x_1, \cdots, x_n) \in \mathcal{O}_K[[x_1, \cdots, x_n]]$ such that

$$F(x_1, \cdots, x_n) \equiv L(x_1, \cdots, x_n) \mod (x_1, \cdots, x_n)^2,$$

and

$$e_1(F(x_1, \cdots, x_n)) = F(e_2(x_1), e_2(x_2), \cdots, e_2(x_n)).$$

Corollary. Let $e \in \mathcal{E}_\pi$ be a Lubin–Tate series. Then there are unique power series $F_e(X, Y) \in \mathcal{O}_K[[X, Y]]$ such that

$$\begin{aligned} F_e(X, Y) &\equiv X + Y \mod (X + Y)^2 \\ e(F_e(X, Y)) &= F_e(e(X), e(Y)) \end{aligned}$$

Corollary. Let $e_1, e_2 \in \mathcal{E}_\pi$ be Lubin–Tate series and $a \in \mathcal{O}_K$. Then there exists a unique power series $[a]_{e_1,e_2} \in \mathcal{O}_K[[X]]$ such that

$$\begin{aligned} [a]_{e_1,e_2}(X) &\equiv aX \mod X^2 \\ e_1([a]_{e_1,e_2}(X)) &= [a]_{e_1,e_2}(e_2(X)). \end{aligned}$$

To simplify notation, if $e_1 = e_2 = e$, we just write $[a]_e = [a]_{e,e}$.

Theorem. The Lubin–Tate $\mathcal{O}_K$ modules for π are precisely the series F_e for $e \in \mathcal{E}_\pi$ with formal $\mathcal{O}_K$-module structure given by

$$a \mapsto [a]_e.$$

Moreover, if $e_1, e_2 \in \mathcal{E}_\pi$ and $a \in \mathcal{O}_K$, then $[a]_{e_1,e_2}$ is a homomorphism from $F_{e_2} \to F_{e_1}$.

If $a \in \mathcal{O}_K^\times$, then it is an isomorphism with inverse $[a^{-1}]_{e_2,e_1}$.

8.3 Lubin–Tate extensions

Proposition. If F is a formal $\mathcal{O}_K$-module, then $\bar{\mathfrak{m}}$ becomes a (genuine) $\mathcal{O}_K$ module under the operations $+_F$ and $\cdot$

$$\begin{aligned} x +_F y &= F(x, y) \\ a \cdot x &= [a]_F(x) \end{aligned}$$

for all $x, y \in \bar{\mathfrak{m}}$ and $a \in \mathcal{O}_K$.

We denote this $\bar{\mathfrak{m}}_F$.

Lemma. Let $e(X) = X^q + \pi X$. We let

$$f_n(X) = \underbrace{(e \circ \cdots \circ e)}_{n \text{ times}}(X).$$

Then f_n has no repeated roots. Here we take f_0 to be the identity function.

Proposition. $F(n)$ is a free $\mathcal{O}_K/\pi^n\mathcal{O}_K$ module of rank 1. In particular, it has q^n elements.

Corollary. We have isomorphisms

$$\frac{\mathcal{O}_K}{\pi^n\mathcal{O}_K} \cong \mathrm{End}_{\mathcal{O}_K}(F(n))$$
$$\frac{U_K}{U_K^{(n)}} \cong \mathrm{Aut}_{\mathcal{O}_K}(F(n)).$$

Theorem. L_n/K is a totally ramified abelian extension of degree $q^{n-1}(q-1)$ with Galois group

$$\mathrm{Gal}(L_n/K) \cong \mathrm{Aut}_{\mathcal{O}_K}(F(n)) \cong \frac{U_K}{U_K^{(n)}}.$$

Explicitly, for any $\sigma \in \mathrm{Gal}(L_n/K)$, there is a unique $u \in U_K/U_K^{(n)}$ such that

$$\sigma(\lambda) = [u]_F(\lambda)$$

for all $\lambda \in F(n)$. Under this isomorphism, for $m \geq n$, we have

$$\mathrm{Gal}(L_m/L_n) \cong \frac{U_K^{(n)}}{U_K^{(m)}}.$$

Moreover, if $F = F_e$, where

$$e(X) = X^q + \pi(a_{q-1}\pi^{q-1} + \cdots + a_2X^2) + \pi X,$$

and $\lambda_n \in F(n) \setminus F(n-1)$, then λ_n is a uniformizer of L_n and

$$\phi_n(X) = \frac{e^n(X)}{e^{n-1}(X)} = X^{q^{n-1}(q-1)} + \cdots + \pi$$

is the minimal polynomial of λ_n. In particular,

$$N_{L_n/K}(-\lambda_n) = \pi.$$

Theorem (Generalized local Kronecker-Weber theorem)**.** We have

$$K^{\mathrm{ab}} = K^{\mathrm{ur}}L_\infty$$

(for any π).

Theorem. We have

$$N(L_n/K) = \langle\pi\rangle \times U_k^{(n)}.$$

Theorem. Let K be a local field. Then we have an isomorphism $\mathrm{Art} : K^\times \to W(K^{\mathrm{ab}}/K)$ given by the composition

$$\begin{array}{ccc} K^\times & \overset{\mathrm{Art}}{\dashrightarrow} & W(K^{\mathrm{ab}}/K) \\ \downarrow\sim & & \downarrow\sim \\ \langle\pi\rangle \times U_K & \longrightarrow & \mathrm{Frob}_K^{\mathbb{Z}} \times \mathrm{Gal}(L_\infty/K) \end{array}$$

where the bottom map is given by $(\pi^m, u) \mapsto (\mathrm{Frob}_K^m, \sigma_{u^{-1}})$, where

$$\sigma_u(\lambda) = [u]_F(\lambda)$$

for all $\lambda \in \bigcup_{n=1}^\infty F(n)$.

Theorem. We have

$$G_s(L_n/K) = \begin{cases} \mathrm{Gal}(L_n/K) & -1 \le s \le 0 \\ \mathrm{Gal}(L_n/L_k) & q^{k-1} - 1 < s \le q^k - 1,\ 1 \le k \le n-1 \\ 1 & s > q^{n-1} \end{cases}$$

Corollary. We have

$$G^t(L_n/K) = \begin{cases} \mathrm{Gal}(L_n/K) & -1 \le t \le 0 \\ \mathrm{Gal}(L_n/L_k) & k-1 < t \le k, \quad k = 1, \cdots, n-1 \\ 1 & t > n-1 \end{cases}$$

In other words, we have

$$G^t(L_n/K) = \begin{cases} \mathrm{Gal}(L_n/L_{\lceil t \rceil}) & -1 \le t \le n-1 \\ 1 & t > n-1 \end{cases},$$

where we set $L_0 = K$.

Corollary. When $t > -1$, we have

$$G^t(K^{\mathrm{ab}/K}) = \mathrm{Gal}(K^{\mathrm{ab}}/K^{\mathrm{ur}}L_{\lceil t \rceil}),$$

and

$$\mathrm{Art}_K^{-1}(G^t(K^{\mathrm{ab}}/K)) = U^{(\lceil t \rceil)}.$$

Corollary. Let M/K be a finite abelian extension. Then we have an isomorphism

$$\mathrm{Art}_K : \frac{K^\times}{N(M/K)} \cong \mathrm{Gal}(M/K).$$

Moreover, for $t > -1$, we have

$$G^t(M/K) = \mathrm{Art}_K\left(\frac{U_K^{(\lceil t \rceil)} N(M/K)}{N(M/K)}\right).$$