Part III — Local Fields

Definitions

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

Definition (Absolute value)**.** Let K be a field. An *absolute value* on K is a function $|\cdot| : K \to \mathbb{R}_{\geq 0}$ such that

(i) $|x| = 0$ iff $x = 0$;

(ii) $|xy| = |x||y|$ for all $x, y \in K$;

(iii) $|x + y| \leq |x| + |y|$.

Definition (Valued field)**.** A *valued field* is a field with an absolute value.

Definition (Equivalence of absolute values)**.** Let K be a field, and let $|\cdot|, |\cdot|'$ be absolute values. We say they are *equivalent* if they induce the same topology.

Definition (Non-archimedean absolute value)**.** An absolute value $|\cdot|$ on a field K is called *non-archimedean* if $|x + y| \leq \max(|x|, |y|)$. This condition is called the *strong triangle inequality*.

An absolute value which isn't non-archimedean is called *archimedean*.

Definition (Valuation ring)**.** Let K be a valued field. Then the *valuation ring of* K is the open subring

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

1.2 Rings

Definition (Integral element)**.** Let $R \subseteq S$ be rings and $s \in S$. We say s is *integral over* R if there is some monic $f \in R[x]$ such that $f(s) = 0$.

Definition (Adjoint/Adjugate matrix)**.** Let $A = (a_{ij})$ be an $n \times n$ matrix with coefficients in a ring R. The *adjugate matrix* or *adjoint matrix* $A^* = (a^*_{ij})$ of A is defined by

$$a^*_{ij} = (-1)^{i+j} \det(A_{ij}),$$

where A_{ij} is an $(n-1) \times (n-1)$ matrix obtained from A by deleting the ith column and the jth row.

Definition (Integrally closed)**.** Given a ring extension $R \subseteq S$, we say R is *integrally closed* in S if $\tilde{R} = R$.

1.3 Topological rings

Definition (Topological ring)**.** Let R be a ring. A topology on R is called a *ring topology* if addition and multiplication are continuous maps $R \times R \to R$. A ring with a ring topology is a *topological ring*.

Definition (I-adically open)**.** Let R be a ring and $I \subseteq R$ an ideal. A subset $U \subseteq R$ is called *I-adically open* if for all $x \in U$, there is some $n \geq 1$ such that $x + I^n \subseteq U$.

Definition (Inverse/projective limit)**.** Let $R_1, R_2, , \cdots$ be topological rings, with continuous homomorphisms $f_n : R_{n+1} \to R_n$.

$$R_1 \xleftarrow[f_1]{} R_2 \xleftarrow[f_2]{} R_3 \xleftarrow[f_3]{} R_4 \longleftarrow \cdots$$

The *inverse limit* or *projective limit* of the R_i is the ring

$$\varprojlim R_n = \left\{(x_n) \in \prod_n R_n : f_n(x_{n+1}) = x_n\right\},$$

with coordinate-wise addition and multiplication, together with the subspace topology coming from the product topology of $\prod R_n$. This topology is known as the *inverse limit topology*.

Definition (I-adic completion)**.** Let R be a ring and I be an ideal. The *I-adic completion* of R is the topological ring

$$\varprojlim R/I^n,$$

where R/I^n has the discrete topology, and $R/I^{n+1} \to R/I^n$ is the quotient map. There is an evident map

$$\begin{aligned}\nu : R &\to \varprojlim R/I^n \\ r &\mapsto (r \bmod I^n).\end{aligned}$$

This map is a continuous ring homomorphism if R is given the I-adic topology.

Definition (I-adically complete)**.** We say that R is *I-adically complete* if ν is a bijection.

1.4 The p-adic numbers

Definition (p-adic absolute value)**.** The *p-adic absolute value* on $\mathbb{Q}$ is the function $|\cdot|_p : \mathbb{Q} \to \mathbb{R}_{\geq 0}$ given by

$$|x|_p = \begin{cases} 0 & x = 0 \\ p^{-n} & x = p^n \frac{a}{b} \text{ as above} \end{cases}.$$

Definition (p-adic numbers)**.** The *p-adic numbers* $\mathbb{Q}_p$ is the completion of $\mathbb{Q}$ with respect to $|\cdot|_p$.

Definition (p-adic integers)**.** The valuation ring

$$\mathbb{Z}_p = \{x \in \mathbb{Q}_p : |x|_p \leq 1\}$$

is the *p-adic integers*.

2 Valued fields

2.1 Hensel's lemma

Definition (Valuation)**.** Let K be a field. A *valuation* on K is a function $v : K \to \mathbb{R} \cup \{\infty\}$ such that

(i) $v(x) = 0$ iff $x = 0$

(ii) $v(xy) = v(x) + v(y)$

(iii) $v(x + y) \geq \min\{v(x), v(y)\}$.

Definition (Primitive polynomial)**.** If K is a valued field and $f(x) = a_0 + a_1 x + \cdots + a_n x^n \in K[x]$ is a polynomial, we say that f is *primitive* if

$$\max_i |a_i| = 1.$$

In particular, we have $f \in \mathcal{O}[x]$.

2.2 Extension of norms

Definition (Norm on vector space)**.** Let K be a valued field and V a vector space over K. A *norm* on V is a function $\|\cdot\| : V \to \mathbb{R}_{\geq 0}$ such that

(i) $\|x\| = 0$ iff $x = 0$.

(ii) $\|\lambda\| = |\lambda| \|x\|$ for all $\lambda \in K$ and $x \in V$.

(iii) $\|x + y\| \leq \max\{\|x\|, \|y\|\}$.

Definition (Equivalence of norms)**.** Let $\|\cdot\|$ and $\|\cdot\|'$ be norms on V. Then two norms are equivalent if they induce the same topology on V, i.e. there are $C, D > 0$ such that

$$C \|x\| \leq \|x\|' \leq D \|x\|$$

for all $x \in V$.

2.3 Newton polygons

Definition (Lower convex set)**.** We say a set $S \subseteq \mathbb{R}^2$ is *lower convex* if

(i) Whenever $(x, y) \in S$, then $(x, z) \in S$ for all $z \geq y$.

(ii) S is convex.

Definition (Lower convex hull)**.** Given any set of points $T \subseteq \mathbb{R}^2$, there is a minimal lower convex set $S \supseteq T$ (by the intersection of all lower convex sets containing T – this is a non-empty definition because $\mathbb{R}^2$ satisfies the property). This is known as the *lower convex hull* of the points.

Definition (Newton polygon)**.** Let $f(x) = a_0 + a_1 x + \cdots + a_n x^n \in K[x]$, where (K, v) is a valued field. Then the *Newton polygon* of f is the lower convex hull of $\{(i, v(a_i)) : i = 0, \cdots, n, a_i \neq 0\}$.

Definition (Break points)**.** Given a polynomial, the points $(i, v(a_i))$ lying on the boundary of the Newton polygon are known as the *break points*.

Definition (Line segment)**.** Given a polynomial, the line segment between two adjacent break points is a *line segment*.

Definition (Multiplicity/length)**.** The *length* or *multiplicity* of a line segment is the horizontal length.

Definition (Slope)**.** The *slope* of a line segment is its slope.

3 Discretely valued fields

Definition (Discretely valued field)**.** Let K be a valued field with valuation v. We say K is a *discretely valued field* (DVF) if $v(k^\times) \subseteq \mathbb{R}$ is a discrete subgroup of $\mathbb{R}$, i.e. $v(k^\times)$ is infinite cyclic.

Definition (Normalized valuation)**.** Let K be a DVF. The *normalized valuation* V_K on K is the unique valuation on K in the given equivalence class of valuations whose image is $\mathbb{Z}$.

Definition (Uniformizer)**.** Let K be a discrete valued field. We say $\pi \in K$ is *uniformizer* if $v(\pi) > 0$ and $v(\pi)$ generates $v(k^\times)$ (iff $v(\pi)$ has minimal positive valuation).

Definition (Local field)**.** A *local field* is a complete discretely valued field with a finite residue field.

Definition (Discrete valuation ring)**.** A ring R is called a *discrete valuation ring* (DVR) if it is a PID with a unique prime element up to units.

Definition (Equal and mixed characteristic)**.** Let K be a valued field with residue field k_K. Then K has *equal characteristic* if

$$\operatorname{char} K = \operatorname{char} k_K.$$

Otherwise, we have K has *mixed characteristic*.

Definition (Perfect ring)**.** Let R be a ring of characteristic p. We say R is *perfect* if the Frobenius map $x \mapsto x^p$ is an automorphism of R, i.e. every element of R has a pth root.

3.1 Teichmüller lifts

Definition (Teichmüller map)**.** The map $[-] : R/xR \to R$ is called the *Teichm uller map*. $[x]$ is called the *Teichmüller lift* or *representative* of x.

3.2 Witt vectors*

Definition (Strict p-ring)**.** Let A be a ring. A is called a *strict p-ring* if it is p-torsion free, p-adically complete, and A/pA is a perfect ring.

Definition (Absolute ramification index)**.** Let R be a DVR with mixed characteristic p with normalized valuation v_R. The integer $v_R(p)$ is called the *absolute ramification index* of R.

4 Some p-adic analysis

Definition (Mahler coefficient)**.** Let $f \in C(\mathbb{Z}_p, \mathbb{Q}_p)$. Then nth-Mahler coefficient $a_n(f) \in \mathbb{Q}_p$ is defined by the formula

$$a_n(f) = \Delta^n(f)(0) = \sum_{i=0}^{n} (-1)^i \binom{n}{i} f(n-i).$$

5 Ramification theory for local fields

5.1 Ramification index and inertia degree

Definition (Inertia degree)**.** Let L/K be a finite extension of local fields. The *inertia degree* of L/K is

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

Definition (Ramification index)**.** Let L/K be a finite extension of local fields, and let v_L be the normalized valuation of L and π_K a uniformizer of K. The integer

$$e_{L/K} = v_L(\pi_K)$$

is the *ramification index* of L/K.

Definition (Unramified extension)**.** Let L/K be a finite extension of local fields. We say L/K is *unramified* if $e_{L/K} = 1$, i.e. $f_{L/K} = [L : K]$.

Definition (Totally ramified extension)**.** Let L/K be a finite extension of local fields. We say L/K is *totally ramified* if $f_{L/K} = 1$, i.e. $e_{L/K} = [L : K]$.

5.2 Unramified extensions

5.3 Totally ramified extensions

Definition (Eisenstein polynomial)**.** A polynomial $f(x) \in \mathcal{O}_K[x]$ satisfying the assumptions of Eisenstein's criterion is called an *Eisenstein polynomial*.

6 Further ramification theory

6.1 Some filtrations

Definition (Higher unit groups)**.** We define the *higher unit groups* to be

$$U_K^{(s)} = U^{(s)} = 1 + \pi_K^s \mathcal{O}_K.$$

We also put

$$U_K = U_K^{(0)} = U^{(0)} = \mathcal{O}_K^\times.$$

Definition (Higher ramification group)**.** Let L/K be a finite Galois extension of local fields, and v_L the normalized valuation of L.

Let $s \in \mathbb{R}_{\geq -1}$. We define the *sth ramification group* by

$$G_s(L/K) = \{\sigma \in \mathrm{Gal}(L/K) : v_L(\sigma(x) - x) \geq s + 1 \text{ for all } x \in \mathcal{O}_L\}.$$

Definition (Inertia group)**.** Let L/K be a finite Galois extension of local fields. Then the *inertia group* of L/K is the kernel of the natural homomorphism

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

given by reduction. We write this as

$$I(L/K) = G_0(L/K).$$

Definition (Wild inertia group and tame quotient)**.** $G_1(L/K)$ is called the *wild inertia group*, and the quotient $G_0(L/K)/G_1(L/K)$ is the *tame quotient*.

6.2 Multiple extensions

Definition ($i_{L/K}$)**.** We define

$$i_{L/K}(\sigma) = \min_{x \in \mathcal{O}_L} v_L(\sigma(x) - x).$$

Notation.

$$\psi_{L/K} = \eta_{L/K}^{-1}.$$

Definition (Upper numbering)**.** Let L/K be a Galois extension of local fields. Then the *upper numbering* of the ramification groups of L/K is defined by

$$G^t(L/K) = G_{\psi_{L/K}(t)}(L/K)$$

for $t \in [-1, \infty)$. The original number is called the *lower numbering*.

7 Local class field theory

7.1 Infinite Galois theory

Definition (Separable and normal extensions)**.** Let L/K be an algebraic extension of fields. We say that L/K is *separable* if, for every $\alpha \in L$, the minimal polynomial $f_\alpha \in K[\alpha]$ is separable. We say L/K is *normal* if f_α splits in L for every $\alpha \in L$.

Definition (Galois extension)**.** Let L/K be an algebraic extension of fields. Then it is *Galois* if it is normal and separable. If so, we write

$$\mathrm{Gal}(L/K) = \mathrm{Aut}_K(L).$$

Definition (Krull topology)**.** Let M/K be a Galois extension. We define the *Krull topology* on M/K by the basis

$$\{\mathrm{Gal}(M/L) : L/K \text{ is finite}\}.$$

More explicitly, we say that $U \subseteq \mathrm{Gal}(M/K)$ is open if for every $\sigma \in U$, we can find a finite subextension L/K of M/K such that $\sigma\,\mathrm{Gal}(M/L) \subseteq U$.

Definition (Directed system)**.** Let I be a set with a partial order. We say that I is a *directed system* if for all $i, j \in I$, there is some $k \in I$ such that $i \le k$ and $j \le k$.

Definition (Inverse limit)**.** Let I be a directed system. An *inverse system* (of topological groups) indexed by I is a collection of topological groups G_i for each $i \in I$ and continuous homomorphisms

$$f_{ij} : G_j \to G_i$$

for all $i, j \in I$ such that $i \le j$, such that

$$f_{ii} = \mathrm{id}_{G_i}$$

and

$$f_{ik} = f_{ij} \circ f_{jk}$$

whenever $i \le j \le k$.

We define the *inverse limit* on the system (G_i, f_{ij}) to be

$$\varprojlim_{i \in I} G_i = \left\{ (g_i) \in \prod_{i \in I} G_i : f_{ij}(g_j) = g_i \text{ for all } i \le j \right\} \subseteq \prod_{i \in I} g_i,$$

which is a group under coordinate-wise multiplication and a topological space under the subspace topology of the product topology on $\prod_{i \in I} G_i$. This makes $\varprojlim_{i \in I} G_i$ into a topological group.

7.2 Unramified extensions and Weil group

Definition (Unramified extension)**.** Let K be a local field, and M/K be algebraic. Then M/K is unramified if L/K is unramified for every finite subextension L/K of M/K.

Definition (Totally ramified extension)**.** Let K be a local field, and M/K be algebraic. Then M/K is totally ramified if L/K is totally ramified for every finite subextension L/K of M/K.

Definition (Arithmetic Frobenius)**.** Let L/K be a finite unramified extension of local fields, the *(arithmetic) Frobenius* of L/K is the lift of $\mathrm{Frob}_{L/K} \in \mathrm{Gal}(k_L/k_K)$ under the isomorphism $\mathrm{Gal}(L/K) \cong \mathrm{Gal}(k_L/k_K)$.

Definition (Weil group)**.** Let K be a local field and M/K be Galois. Let $T = T_{M/K}$ be the maximal unramified subextension of M/K. The *Weil group* of M/K is

$$W(M/K) = \{\sigma \in \mathrm{Gal}(M/K) : \sigma|_T = \mathrm{Frob}_{T/K}^n \text{ for some } n \in \mathbb{Z}\}.$$

We define a topology on $W(M/K)$ by saying that U is open iff there is a finite extension L/T such that $\sigma\,\mathrm{Gal}(L/T) \subseteq U$.

7.3 Main theorems of local class field theory

Definition (Abelian extension)**.** Let K be a local field. A Galois extension L/K is *abelian* if $\mathrm{Gal}(L/K)$ is abelian.

8 Lubin–Tate theory

8.1 Motivating example

Definition (Higher ramification groups)**.** Let K be a local field and L/K Galois. We define, for $s \in \mathbb{R}_{\geq -1}$

$$G^s(M/K) = \{\sigma \in \mathrm{Gal}(M/K) : \sigma|_L \in G^s(L/K) \text{ for all finite Galois subextension } M/K\}.$$

8.2 Formal groups

Notation. Let R be a ring. We write

$$\mathbb{R}[[x_1, \cdots, x_n]] = \left\{ \sum_{k_1,\ldots,k_n \in \mathbb{Z}_{\geq 0}} a_{k_1,\ldots,k_n} x_1^{k_1} \cdots x_n^{k_n} : a_{k_1,\ldots,k_n} \in R \right\}$$

for the ring of formal power series in n variables over R.

Definition (Formal group)**.** A (one-dimensional, commutative) *formal group* over R is a power series $F(X, Y) \in R[X, Y]$ such that

(i) $F(X, Y) \equiv X + Y \mod (X^2, XY, Y^2)$

(ii) Commutativity: $F(X, Y) = F(Y, X)$

(iii) Associativity: $F(X, F(Y, Z)) = F(F(X, Y), Z)$.

Definition (Homomorphism of formal groups)**.** Let R be a ring, and F, G be formal groups over R. A *homomorphism* $f : F \to G$ is an element $f \in R[[X]]$ such that $f(X) \equiv 0 \mod X$ and

$$f(F(X, Y)) = G(f(X), f(Y)).$$

The endomorphisms $f : F \to F$ form a ring $\mathrm{End}_R(F)$ with addition $+_F$ given by

$$(f +_F g)(x) = F(f(x), g(x)).$$

and multiplication is given by composition.

Definition (Formal module)**.** Let R be a ring. A *formal R-module* is a formal group F over R with a ring homomorphism $R \to \mathrm{End}_R(F)$, written, $a \mapsto [a]_F$, such that

$$[a]_F(X) = aX \mod X^2.$$

Definition (Lubin–Tate module)**.** A *Lubin–Tate module* over $\mathcal{O}_K$ with respect to π is a formal $\mathcal{O}_K$-module F such that

$$[\pi]_F(X) \equiv X^q \mod \pi.$$

Definition (Lubin–Tate series)**.** A *Lubin–Tate series* for π is a power series $e(X) \in \mathcal{O}_K[[X]]$ such that

$$e(X) \equiv \pi X \mod X^2, \quad e(X) \equiv X^q \mod \pi.$$

We denote the set of Lubin–Tate series for π by $\mathcal{E}_\pi$.

Definition (Lubin–Tate polynomial)**.** A *Lubin–Tate polynomial* is a polynomial of the form

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

with $u \in U_K^{(1)}$, and $a_{q-1}, \cdots, a_2 \in \mathcal{O}_K$.

In particular, these are Lubin–Tate series.

8.3 Lubin–Tate extensions

Definition (π^n-division points)**.** Let F be a Lubin–Tate $\mathcal{O}_K$-module for π. Let $n \geq 1$. The group $F(n)$ of *π^n-division points of F* is defined to be

$$F(n) = \{x \in \bar{\mathfrak{m}}_F \mid [\pi^n]_F x = 0\} = \ker([\pi^n]_F).$$

This is a group under the operation given by F, and is indeed an $\mathcal{O}_K$ module.