Local Fields

Dr. T. Dokchitser

Michaelmas 2007

LaTeXed by Sebastian Pancratz

These notes are based on a course of lectures given by Dr. T. Dokchitser in Part III of the Mathematical Tripos at the University of Cambridge in the academic year 2007–2008.

These notes have not been checked by Dr. T. Dokchitser and should not be regarded as official notes for the course. In particular, the responsibility for any errors is mine — please email Sebastian Pancratz (`sfp25`) with any comments or corrections.

Contents

1 Valued Fields 1

2 Non-Archimedean Absolute Values and Valuations 5

3 Completion 11

4 Local Fields 13

5 Discrete Valuation Rings and Completions 15

6 p-adic Numbers 17

7 Local Fields 25

8 Inverse Limits 27

9 Extensions of Complete Fields 31

10 Ramification and Inertia 35

11 Unramified Extensions 37

12 Totally Ramified Extensions 39

13 Inertia Group and Higher Ramification 41

Chapter 1

Valued Fields

An *absolute value* on a field K is a function $|\cdot|\colon K \to \mathbb{R}_{\geq 0}$ such that

(i) $|x| = 0$ if and only if $x = 0$;
(ii) $|xy| = |x||y|$;
(iii) $|x + y| \leq |x| + |y|$.

Example. Take $K = \mathbb{Q}$, $\mathbb{R}$, or $\mathbb{C}$ and let $|\cdot|$ be the usual absolute value, which we will denote $|\cdot|_\infty$.

Example. For any field K, let

$$|x| = \begin{cases} 0 & x = 0 \\ 1 & x \neq 0 \end{cases}$$

called the *trivial absolute value* on K.

From (i) and (ii) it follows that $|1| = |-1| = 1$. Generally, if $x \in K$ such that $x^n = 1$ then $|x| = 1$. In particular, if $K = \mathbb{F}_{p^n}$ is a finite field, or $K = \bar{\mathbb{F}}_p$, then K has only trivial absolute value. Also note that $|x/y| = |x|/|y|$ for $y \neq 0$ and $|x^n| = |x|^n$.

Example (p-adic Absolute Value on $\mathbb{Q}$)**.** Fix a prime p and $0 < \alpha < 1$. Write $x \in \mathbb{Q}^*$ as

$$x = p^n \frac{a}{b}$$

with $n \in \mathbb{Z}$ and a, b coprime to p. Then define $|x| = |p^n a/b| = \alpha^n$. This is called the *$p$-adic absolute value* on $\mathbb{Q}$. It is indeed an absolute value, for if $x = p^n a/b$, $y = p^m c/d$ then

$$\begin{aligned} |xy| &= |p^{n+m}\frac{ac}{bd}| = \alpha^{m+n} = |x||y| \\ |x + y| &= |p^{\min\{n,m\}}\frac{\star}{bd}| = |p^{\min\{n,m\}}||\frac{\star}{bd}| \\ &\leq \alpha^{\min\{n,m\}} = \max\{|x|, |y|\} \leq |x| + |y| \end{aligned}$$

So a rational number is small with respect to $|\cdot|$ if and only if it is divisible by a large power of p. To remove ambiguity in the choice of α, we make the following definition.

Definition. Two absolute values $|\cdot|$, $\|\cdot\|$ on K are *equivalent* if there exists $c > 0$ such that

$$|x| = \|x\|^c$$

for all $x \in K$. The *normalised p-adic absolute value* is the one with $\alpha = 1/p$ and it is denoted $|\cdot|_p$.

Example. Let $p = 5$. Then

$$|5^n|_5 = 5^{-n} \qquad |10|_5 = \frac{1}{5}$$

$$|\frac{1}{10}|_5 = 5 \qquad |\frac{2}{3}|_5 = 1$$

If an absolute value on K satisfies the following stronger condition (iii')

$$|x + y| \leq \max\{|x|, |y|\}$$

we call it *ultrametric* or *non-Archimedean*. Otherwise, we say it is *Archimedean*.

Theorem 1.1 (Ostrowski)**.** Any non-trivial absolute value $|\cdot|$ on $\mathbb{Q}$ is equivalent to either $|\cdot|_\infty$ or $|\cdot|_p$ for some p.

Proof. Let $a, b > 1$ be integers and write b^n in base a,

$$b^n = c_m a^m + c_{m-1} a^{m-1} + \cdots + c_0$$

with $c_i \in [0, a-1]$. Let $M = \max\{|1|, \ldots, |a-1|\}$. Then

$$\begin{aligned} |b^n| &\leq |c_m||a|^m + \cdots + |c_0| \\ &\leq (m+1)M \max\{|a|^m, \ldots, |1|\} \\ &\leq (n \log_a b + 1) M \max\{1, |a|^m\} \end{aligned}$$

Taking nth roots and letting $n \to \infty$,

$$|b| \leq \max\{1, |a|^{\log_a b}\} \tag{$*$}$$

Case 1. Assume $|b| > 1$ for some integer $b > 1$. By $(*)$,

$$|b| \leq \max\{1, |a|^{\log_a b}\} = |a|^{\log_a b}$$

so $|a| > 1$ for all $a > 1$. Interchanging a and b in $(*)$,

$$|a| \leq |b|^{\log_b a}$$

so

$$|b|^{\frac{1}{\log b}} = |a|^{\frac{1}{\log a}}$$

Equivalently, $|a| = a^\lambda$ for all $a \geq 1$ and some λ independent of a, so $|\cdot| \sim |\cdot|_\infty$.

Case 2. Suppose $|b| \leq 1$ for all integers $b \geq 1$. Then there is a $b > 1$ such that $|b| < 1$, otherwise $|\cdot|$ is trivial. Take such a b and write $b = p_1^{n_1} \cdots p_k^{n_k}$. Then

$$1 > |b| = |p_1|^{n_1} \cdots |p_k|^{n_k}$$

so there exists p such that $|p| < 1$. It suffices to show that $|q| = 1$ for all primes $q \neq p$, and it then follows that $|\cdot| \sim |\cdot|_p$.

Suppose $|p| < 1$ and $|q| < 1$ for some $p \neq q$. Take $n, m \geq 1$ such that $|p^n| < 1/2$, $|q^m| < 1/2$. As p^n, q^m are coprime, $1 = xp^n + yq^m$ for some $x, y \in \mathbb{Z}$, so

$$1 \leq |x||p^n| + |y||q^m| < \frac{1}{2} + \frac{1}{2} = 1$$

contradiction. $\square$

We do not need the following result, but there is a complete classification of Archimedean absolute values.

Theorem 1.2. If $|\cdot|$ is an Archimedean absolute value on a field K then there exists an injection $K \hookrightarrow \mathbb{C}$ such that $|\cdot| \sim |\cdot|_\infty$ on $\mathbb{C}$.

Chapter 2

Non-Archimedean Absolute Values and Valuations

From now on, $|\cdot| \colon K \to \mathbb{R}_{\geq 0}$ is non-Archimedean and non-trivial. We sometimes say K is non-Archimedean with a fixed $|\cdot|$ in mind.

Pick $0 < \alpha < 1$ and write $|x| = \alpha^{v(x)}$, i.e., let $v(x) = \log_\alpha |x|$.

$$K^* \to \mathbb{R}_{>0} \xrightarrow{\log_\alpha} (\mathbb{R}, +)$$

Then $v(x)$ is a *valuation*, an additive version of $|\cdot|$.

Definition. The map $v \colon K^* \to \mathbb{R}$ is a *valuation* if

(i) $v(K^*) \neq \{0\}$;
(ii) $v(xy) = v(x) + v(y)$;
(iii) $v(x+y) \geq \min\{v(x), v(y)\}$.

Valuations v and cv, for $c > 0$ a real constant, are called *equivalent*. A valuation determines a non-trivial non-Archimedean absolute value and vice versa.

We extend v to K formally by letting $v(0) = \infty$. The image $v(K^*)$ is an additive subgroup of $\mathbb{R}$, the *value group* of v. If it is discrete, i.e., isomorphic to $\mathbb{Z}$, we say v is a *discrete valuation*. If $v(K^*) = \mathbb{Z}$, we call v *normalised discrete valuation*.

We will only study discrete valuations.

Example. Let $K = \mathbb{Q}$ and p a prime. Then

$$v_p = \mathrm{ord}_p \colon \mathbb{Q}^* \ni p^n \frac{a}{b} \mapsto n \in \mathbb{Z}$$

is the p-adic valuation,

$$|x|_p = \left(\frac{1}{p}\right)^{v_p(x)}$$

Alternatively,

$$v_p(x) = \max_{r \in \mathbb{Z}} \{r : x \in p^r \mathbb{Z}\}$$

Generally, if K is a number field with $[K : \mathbb{Q}] < \infty$, let $\{0\} \leq P \subset \mathcal{O}_K$ be a prime ideal. Then define

$$v_P \colon K \to \mathbb{Z}, x \mapsto \max_{r \in \mathbb{Z}} \{r : x \in P^r \mathcal{O}_K\}$$

This is a normalised discrete valuation and every valuation on K is of this form, i.e., there is an analogue of Ostrowski's theorem for number fields.

Example. Let $K = k(t)$. Define

$$v_0\left(t^n \frac{p(t)}{q(t)}\right) = n$$

where $p(0), q(0) \neq 0$. This is a normalised discrete valuation, the order of zeros or poles at $t = 0$. In fact, for any $a \in K$ we may define

$$v_a\left((t-a)^n \frac{p(t)}{q(t)}\right) = n$$

where $p(a), q(a) \neq 0$. For instance, let $f(t) = t^2(t-1)/(t-2)^5$. Then

$$v_0(f) = 2 \qquad v_1(f) = 1 \qquad v_2(f) = -5 \qquad v_a(f) = 0$$

for all other $a \in k$. There is also

$$v_\infty\left(\frac{p(t)}{q(t)}\right) = \deg q(t) - \deg p(t) \in \mathbb{Z}$$

which again is a valuation, called the order at ∞.

If $X = \mathbb{C} \cup \{\infty\}$ is the Riemann sphere let $K = \mathbb{C}(z)$ be the field of meromorphic functions on X. The above valuation is

$$v_a(f) = \operatorname{ord}_{z=a} f(z)$$

for every $a \in X$, including ∞.

If $k = \mathbb{C}$, or in general, an algebraically closed field, then these are the only valuations on $K = k(t)$ with $v(k^*) = \{0\}$.

2.1 Aside on Algebraically Closed Fields

Definition. A field K is algebraically closed if the following equivalent conditions are satisfied.

(i) Every polynomial of degree n over K has precisely n roots, counted with multiplicity.
(ii) Every non-constant polynomial is a product of linear factors.
(iii) If $f \in K[X]$ is non-constant and irreducible then f is linear.
(iv) K has no non-trivial finite extensions.

Example. $\mathbb{C}$ is algebraically closed. $\mathbb{Q}, \mathbb{R}, \mathbb{F}_{p^n}$, $k(t)$ are not algebraically closed.

Theorem 2.1. Let K be any field. Then there exists an algebraically closed field $\bar{K}$ unique up to isomorphism such that $K \subset \bar{K}$ and every element of $\bar{K}$ is algebraic over K. $\bar{K}$ is called an *algebraic closure*.

Example. $\mathbb{C}$ is algebraically closed so $\bar{\mathbb{C}} = \mathbb{C}$. $\bar{\mathbb{R}} = \mathbb{C}$. $\bar{\mathbb{Q}}$ is the set of $\alpha \in \mathbb{C}$ satisfying polynomials with rational coefficients.

Exercise 1. Show that $\bar{\mathbb{Q}}$ as defined above is an algebraically closed field. Further show that there exists a sequence $(K_n)_{n\geq 1}$ of finite Galois extensions $Q \subset K_1 \subset K_2 \subset \cdots$ such that $\bar{\mathbb{Q}} = \bigcup_{n\geq 1} K_n$.

2.2 Algebraic Properties of Valuations

Let $v\colon K^* \to \mathbb{R}$ be a valuation corresponding to the absolute value $|\cdot|\colon K \to \mathbb{R}_{\geq 0}$. Then

$$\mathcal{O} = \mathcal{O}_v = \mathcal{O}_K = \{x \in K : v(x) \geq 0\} = \{x \in K : |x| \leq 1\}$$

is a ring, called the *valuation ring* of v. K is its field of fractions, and

$$x \in K \setminus \mathcal{O} \implies \frac{1}{x} \in \mathcal{O}$$

The set of units in $\mathcal{O}$ is

$$\mathcal{O}^\times = \{x \in K : v(x) = 0\} = \{x \in K : |x| = 1\}$$

and

$$M = \{x \in K : v(x) > 0\} = \{x \in K : |x| < 1\}$$

is an ideal in $\mathcal{O}$. Because $\mathcal{O} = \mathcal{O}^\times \cup M$, M is a unique maximal ideal, so $\mathcal{O}$ is *local*. $k = \mathcal{O}/M$ is a field, called the *residue field* of v or of K.

Suppose $v\colon K^* \twoheadrightarrow \mathbb{Z}$ is normalised discrete. Take $\pi \in M$ with $v(\pi) = 1$, called a *uniformiser*. Then every $x \in K^*$ can be written uniquely as

$$x = u\pi^n$$

for a unit $u \in \mathcal{O}^\times$ and $n \in \mathbb{Z}$. Every $x \in \mathcal{O}$ can be written uniquely as

$$x = u\pi^n$$

for a unit $u \in \mathcal{O}^\times$ and $n \in \mathbb{Z}_{\geq 0}$. Every $x \in M$ can be written uniquely as

$$x = u\pi^n$$

for a unit $u \in \mathcal{O}^\times$ and $n \geq 1$. In particular, $M = (\pi)$ is principal. Moreover, every ideal $I \subset \mathcal{O}$ is principal,

$$\mathcal{O} \supset I \neq (0) \implies I = (\pi^n)$$

where $n = \min\{v(x) : x \in I\}$, so $\mathcal{O}$ is a principal ideal domain (PID).

Example. Let $K = \mathbb{Q}$, $v = v_p$. Then

$$\mathcal{O} = \left\{\frac{x}{y} : (y, p) = 1\right\}$$
$$M = \left\{\frac{x}{y} : (y, p) = 1, p \mid x\right\} = (p)\mathcal{O}$$
$$\mathcal{O}/M = k \cong \mathbb{F}_p, \frac{x}{y} \mapsto \frac{x \mod p}{y \mod p}$$

Example. Let $K = k(T)$ and consider v_a for some $a \in k$. Then

$$\mathcal{O} = \left\{\frac{f}{g} : g(a) \neq 0\right\}$$
$$M = \left\{\frac{f}{g} : g(a) \neq 0, f(a) = 0\right\}$$
$$\mathcal{O}/M \xrightarrow{\sim} k, f \mapsto f(a)$$

the evaluation map.

Definition. A *discrete valuation ring* (DVR) is a local integral PID, which is not a field.

Theorem 2.2. (i) Suppose $v\colon K^* \twoheadrightarrow \mathbb{Z}$ is a valuation. Then $\mathcal{O}_v$ is a DVR.

(ii) If R is a DVR then there exists a unique valuation v on its field of fractions K such that $R = \mathcal{O}_v$.

Proof. (i) $\mathcal{O}_v \subset K$ is a subring, hence is an integral domain; we have already shown it is local and a PID. $\pi^{-1} \in K \setminus \mathcal{O}$, so $\mathcal{O}$ is not a field.

(ii) Let R be a DVR. R is local so has a unique maximal ideal M, and R is a PID so $M = (\pi)$ for some $\pi \in R$. (Recall that if R is a PID then R is also a UFD.) If π' is another irreducible element then (π') is maximal, hence $(\pi) = (\pi')$ so π' is associate to π. As R is a UFD, every element is uniquely of the form $u\pi^n$, $u \in R$ a unit.

Now define v on R by letting $v(u\pi^n) = n$, and extend to K by $v(x/y) = v(x) - v(y)$. Check it is a valuation.

□

Definition. Let $R \subset S$ be rings. Then $x \in S$ is *integral* over R if

$$x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0 = 0$$

for some $a_i \in R$. The *integral closure* of R in S is

$$\{x \in S : x \text{ integral over } R\}$$

This is a ring, contained in S and containing R.

Example. Let $R = \mathbb{Z}$, $S = \mathbb{C}$. Then the integral closure is the ring of algebraic integers.

A domain R is *integrally closed* if R is its integral closure in its field of fractions. Equivalently, for all $y \in \mathrm{Frac}(R)$, y is integral over R if and only if $y \in R$.

Theorem 2.3. Let R be a domain. Then R is a DVR if and only if R is Noetherian, integrally closed, and has a unique non-zero prime ideal.

Proof. Suppose R is a DVR. We know every ideal is principal and hence finitely generated, so R is Noetherian.

Now take $x \in \mathrm{Frac}(R) = K$, $x \notin R$, i.e., $v(x) = m < 0$, but satisfying

$$x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0 = 0$$

Then

$$mn = v(x^n) = v(-x^n) = v(a_{n-1}x^{n-1} + \cdots + a_1 x + a_0) \geq m(n-1)$$

a contradiction.

Every ideal $(0) \neq I \subset R$ is of the form $I = (\pi^k)$, and (π^m) is prime if and only if $m = 1$. Thus (π) is the unique non-zero prime ideal. This completes one direction of the proof.

Lemma 2.4 (Poor Man's Factorisation)**.** Let R be Noetherian and $I \subset R$ an ideal. Then there exists prime ideals $P_1, \ldots, P_n$ such that

$$I \subset P_i, \qquad \prod_{i=1}^{n} P_i \subset I$$

Proof. Let $\mathcal{S}$ be the set of ideals I not having this property. Assume $\mathcal{S} \neq \emptyset$ and take $I \in \mathcal{S}$ to be a maximal element, which is possible as R is Noetherian. Prime ideals are not in $\mathcal{S}$, so I is not prime, i.e., there exist $a, b \in R$ such that $a, b \notin I$ and $ab \in I$. As I is maximal,

$$I \subsetneq I + (a), I \subsetneq I + (b) \implies I + (a), I + (b) \notin \mathcal{S}$$

Thus there exist P_i, Q_j such that

$$\begin{aligned} &\prod_i P_i \subset I + (a) \qquad && P_i \supset I + (a) \supset I \\ &\prod_j Q_j \subset I + (b) \qquad && Q_j \supset I + (b) \supset I \end{aligned}$$

Now

$$\left(\prod_i P_i\right)\left(\prod_j Q_j\right) \subset (I + (a))(I + (b)) \subset I$$

a contradiction. □

Proof (of Theorem 2.3). Conversely, let M be the unique non-zero prime ideal. Then R is maximal and local. It is now enough to show that M is principal since then every ideal is principal.

Let $y \in M$, $y \neq 0$. Poor man's factorisation gives

$$M^n \subset (y) \subset M$$

for some n. Let n be the smallest such. Then

$$M^n \subset (y), M^{n-1} \not\subset (y)$$

Let $x \in M^{n-1} \setminus (y)$. Set $z = x/y \in \mathrm{Frac}(R)$, $z \notin R$. (At this stage, morally, $z = \pi^{-1}$.) Then

$$xM \subset M^n \subset (y) \implies zM \subset R$$

so zM is an ideal in R. Either $zM = R$, so $M = (z^{-1})R$ and hence M is principal. Or zM is a proper ideal, $zM \subset M$. As R is Noetherian, M is finitely generated. Let $M = (x_1, \ldots, x_n)$, say. Multiplying by z,

$$\begin{pmatrix} zx_1 \\ \vdots \\ zx_n \end{pmatrix} = \begin{pmatrix} a_{11}x_1 + \cdots + a_{1n}x_n \\ \vdots \\ a_{n1}x_1 + \cdots + a_{nn}a_n \end{pmatrix}$$

with $a_{ij} \in R$, i.e.,

$$A(x_i) = z(x_i)$$

working over $\mathrm{Frac}(R)$. This means $\det(A - zI) = 0$. Note $\det(A - zI)$ is a monic polynomial in z with coefficients in R. Since R is integrally closed, $z \in R$. □

Exercise 2. Show that if M is principal then every ideal is principal.

Example. (i) $R = \{m/n \in \mathbb{Q} : (n, p) = 1\}$;
(ii) $R = \{f/q \in k(t) : g(a) \neq 0\}$.

Example. (i) Let $R = \mathbb{Z}$, or $R = \mathcal{O}_K$ where K is a number field. This is Noetherian and integrally closed, but has many non-zero prime ideals.
(ii) Let $v\colon K^* \to \mathbb{R}$ be a non-discrete valuation. Then $\mathcal{O}_K$ is integrally closed and has a unique non-zero prime ideal, but is not Noetherian.
(iii) Let $v\colon \mathbb{Q}^* \to \mathbb{Z}$ be the 2-adic valuation and $\mathcal{O}_v$ be its valuation ring. Then $R = \mathcal{O}_v[2i]$ is local, Noetherian and has a unique non-zero prime ideal, but is not integrally closed.

Chapter 3

Completion

Suppose $K, |\cdot|$ is any valued field. Then K is a metric and topological space, with metric

$$d(x,y) = |x-y|$$

and the topology defined by the open balls

$$B_{a,r} = \{x \in K : |x-a| < r\}$$

We say $x_n \to x$ if $|x_n - x| \to 0$ as $n \to \infty$ and $\sum_{n=1}^{\infty} a_n = A$ if $\sum_{n=1}^{N} a_n \to A$ as $N \to \infty$.

Properties of the absolute value imply that if $x_n \to x, y_n \to x$ then $x_n \pm y_n \to x \pm y$, $x_n y_n \to xy$, and $1/x_n \to 1/x$ provided $x \neq 0$. Hence $+, \times \colon K \times K \to K$ and $(\cdot)^{-1} \colon K^* \to K^*$ are continuous maps.

Definition. $\{x_n\}_{n\in\mathbb{N}}$ is a *Cauchy sequence* if $|x_n - x_m| \to 0$ as $n, m \to \infty$, i.e.,

$$\forall \varepsilon > 0 \quad \exists N \in \mathbb{N} \quad \forall m, n > N \quad |x_n - x_m| < \varepsilon$$

K is *complete* with respect to $|\cdot|$ is every Cauchy sequence converges.

Example. $\mathbb{R}, |\cdot|_\infty$ and $\mathbb{C}, |\cdot|_\infty$ are the only two Archimedean complete fields. $\mathbb{Q}, |\cdot|_\infty$ is non complete, $\mathbb{R}, |\cdot|_\infty$ is its completion. $\mathbb{Q}, |\cdot|_p$ is not complete.

Exercise 3. Argue by countability that $\mathbb{Q}, |\cdot|_\infty$ and $\mathbb{Q}, |\cdot|_p$ are not complete since there are uncountably many Cauchy sequences.

The topological completion of K with respect to $|\cdot|$ can be made into a field, called the *completion* $\hat{K}$ of K with respect to $|\cdot|$. This is constructed as follows.

Let C be the set of Cauchy sequences in K, and note this is a ring containing the ideal I of Cauchy sequences tending to 0. Define $\hat{K} = C/I$, which is a ring.

Then $(x_k) \in \hat{K}^*$ is a Cauchy sequence with $x_k \not\to 0$. Thus for some $\varepsilon > 0$ and sufficiently large k, $|x_k| > \varepsilon$. Hence $(1/x_k)$ is a Cauchy sequence in $\hat{K}^*$ and so $\hat{K}$ is a field.

Note there is a natural injection $K \hookrightarrow \hat{K}$ by $x \mapsto (x, \dots)$. We can extend $|\cdot|$ from K to $\hat{K}$ by

$$|(x_n)| = \lim_{n\to\infty} |x_n|$$

3.1 Properties

(i) $\hat{K}$ is a complete valued field, $|\cdot|_{\hat{K}}$ extends $|\cdot|_K$;
(ii) $K \hookrightarrow \hat{K}$ is dense;
(iii) $K = \hat{K}$ if and only if K is complete;
(iv) K is non-Archimedean if and only if $\hat{K}$ is non-Archimedean;
(v) Equivalent absolute values on K give rise to isomorphic completions (as fields and vector spaces);
(vi) If $\phi\colon K \hookrightarrow L$ is an inclusion of valued fields then there exists a unique $\hat{\phi}\colon \hat{K} \hookrightarrow \hat{L}$ extending ϕ, and this is defined by $\hat{\phi}((x_n)_n) = (\phi(x_n))_n$.

Exercise 4. Check the above statements.

Example. Let K, $|\cdot|$ be non-Archimedean. Theorem 1.2 gives

$$\mathbb{Q}, |\cdot|_\infty \hookrightarrow K, |\cdot| \hookrightarrow \mathbb{C}, |\cdot|_\infty$$

Taking completions, $\mathbb{R} \subset \hat{K} \subset \mathbb{C}$ so $\hat{K} \cong \mathbb{R}$ or $\mathbb{C}$. In particular, $\mathbb{R}$ and $\mathbb{C}$ are the only complete Archimedean fields.

Chapter 4

Local Fields

From now on, we assume every absolute value is non-trivial.

Definition. Let $K, |\cdot|$ be a valued field. $K, |\cdot|$ is a *local field* if it is locally compact as a topological space.

We recall the following properties of topological spaces.

(i) A topological space X is *compact* if every open cover of X has a finite subcover.
(ii) A topological space X is *locally compact* if for every open set $U \subset X$ and $x \in U$ there is an open set U_0 such that $x \in U_0 \subset U$ and U_0 has compact closure.
(iii) A metric space X is locally compact if and only if for every $x \in X$ there exists $R > 0$ such that for all $0 < r < R$ the ball $B_r(x)$ is compact.

Lemma 4.1. The following statements are equivalent.

(i) K is local.
(ii) There exists a compact disc $B_{a,\leq r}$.
(iii) All discs $B_{a,\leq r}$ are compact.

Proof. (iii) $\implies$ (i) $\implies$ (ii) is clear.

We now show (ii) $\implies$ (iii). Take a compact disc $B_{a,\leq r}$. The translation $x \mapsto x + a$ is a homomorphism. Thus $B_{0,\leq r}$ is compact, so $B_{0,\leq s}$ is compact for all $0 < s \leq r$ as a closed subset of a compact set. Now $|\cdot|$ is non-trivial so there exists $\alpha \in K$ such that $|\alpha| > 1$. The map $K \to K, x \mapsto \alpha x$ is continuous so $B_{0,\leq |\alpha|^n r}$ is compact for all $n \in \mathbb{N}$. Hence $B_{0,\leq s}$ is compact for all $0 < s$ and again by translation we are done. $\square$

Proposition 4.2. A local field $K, |\cdot|$ is complete.

Proof. Assume not. Pick $x \in \hat{K} \setminus K$ and a sequence $(x_n)_n$ in K with $x_n \to x$.

Let B be any closed disc that contains all x_n for $n \geq N$ and some $N \in \mathbb{N}$. (For example, there exists $N \in \mathbb{N}$ such that $|x_n - x| < 1$ for all $n \geq N$; now take $B = B_{x_N,\leq 2}$.) B is compact by the above lemma.

Let $U_n = \{y \in K : |y - x| > 1/n\}$. These are open sets and give an open cover of B,

$$B = \bigcup_{n \geq 1} (U_n \cap B)$$

but it has no finite subcover. $\square$

Corollary 4.3. $\mathbb{R}$ and $\mathbb{C}$ are the only Archimedean local fields.

Now suppose $K, |\cdot|$ is non-Archimedean. The following are consequences of the condition $|x+y| \leq \max\{|x|, |y|\}$.

(i) If $|y| < |x|$ then $|x \pm y| = |x|$;
(ii) If $x_1 + \cdots + x_n = 0$ then the two largest absolute values are equal.
(iii) $(x_n)_n$ is Cauchy if and only if $x_n - x_{n-1} \to 0$.
(iv) In a complete field, $\sum_{n=1}^{\infty} x_n$ converges if and only if $x_n \to 0$.

4.1 Topological Properties

(i) If $x \in B_{a,<r}$ then $B_{x,<r} = B_{a,<r}$, so every point in the disc is a centre.
(ii) If B, B' are open discs with $B \cap B' \neq \emptyset$ then $B \subset B'$ or $B' \subset B$.
(iii) Every open disc is also closed.

Proof. Let $K = \bigcup_{a \in K} B_{a,<r}$, a disjoint union of open discs. Then one is the complement of the union of all others (on choosing the radius appropriately small), so every one is closed. □

Theorem 4.4. Suppose $K, |\cdot|$ is non-Archimedean and has the corresponding valuation v. Then the following are equivalent.

(i) K is a local field.
(ii) The valuation ring $\mathcal{O} = \mathcal{O}_v$ is compact.
(iii) K is complete, v is discrete and the residue field $k = \mathcal{O}/M$ is finite.

Proof. (i) $\iff$ (ii): $\mathcal{O} = \{x \in K : |x| \leq 1\} = B_{0,\leq 1}$, and now apply the lemma.

(i),(ii) $\implies$ (iii): K is complete by Proposition 4.2. Write

$$\mathcal{O} = \bigcup_{x \in \mathcal{O}} x + M = \bigcup_{x \in \mathcal{O}} B_{x,<1}$$

a disjoint union of open discs. $\mathcal{O}$ is compact so there exists a finite subcover, hence $\mathcal{O}/M$ is finite. Now take $y \in M \setminus \{0\}$ and write

$$\mathcal{O} = \bigcup_{x \in \mathcal{O}} x + y\mathcal{O}$$

This is a finite union, so the valuation is discrete.

(iii) $\implies$ (ii): Exercise. □

Chapter 5

Discrete Valuation Rings and Completions

Lemma 5.1. Let $\mathcal{O}$ be a DVR and v a valuation of it. Let $K = \mathrm{Frac}(\mathcal{O})$, $M = (\pi)$ for a uniformiser π, and $\mathcal{O}/M = k$ the residue field.

Let $A = \{a_i\}$ be any set of representatives of $\mathcal{O}/M$, $a_i \in \mathcal{O}$, say $0 \in A$. Then every $x \in K^*$ can be written as

$$x = \pi^{v(x)} \sum_{n=0}^{\infty} a_n \pi^n$$

with $a_n \in A$ and $a_0 \neq 0$. We say that a_i are the *digits* in the π-adic expansion of x.

Proof. Write $x = \pi^{v(x)} u$ for some unit $u \in \mathcal{O}^\times$. Reducing mod π,

$$\begin{aligned} \mathcal{O}/M &\xrightarrow{\sim} k \\ u &\mapsto \bar{u} \end{aligned}$$

There exists a unique $a_0 \in A$ such that $\bar{a}_0 = \bar{u}$, so $a_0 - u \in M$. Now write $u = a_0 + \pi u_1$ and reduce u_1 mod π. Then there exists a unique $a_1 \in A$ such that $\bar{a}_1 = \bar{u}_1$. Now write $u = a_0 + \pi a_1 + \pi^2 u_2$ and proceed. We obtain partial sums

$$S_N = \sum_{n=0}^{N} a_n \pi^n \to u$$

in the topology defined by v, because $v(S_n - u) \geq N$ implies $S_N \to u$. Clearly the a_n are unique. □

Remark.
(i) The open balls in K are of the form $x + \pi^n \mathcal{O}$, which is the set of elements of K whose digits coincide with those of x up to a_{n-1}.
(ii) A sequence $(x_k)_k$ in K is Cauchy if and only if the digits of x_k eventually stabilise.
(iii) K is complete with respect to $|\cdot|$ if and only if every Cauchy sequence converges if and only if the inclusion given by the lemma,

$$K \hookrightarrow \left\{ \text{power series } \sum_{n=n_0}^{\infty} a_n \pi^n,\ a_n \in A \right\}$$

is an equality. In general, the RHS is equal to $\hat{K}$.

(iv) $K, \mathcal{O}, M, v$ induce $\hat{K}, \hat{\mathcal{O}}, \hat{M}, \hat{v}$. From the description above, the valuation on $\hat{K}$ is still discrete.

$$\begin{tikzcd} K^* \arrow[r, "v"'] \arrow[d, hook] & \mathbb{Z} \arrow[d, "\iota"] \\ \hat{K}^* \arrow[r, "\hat{v}"'] & \mathbb{Z} \end{tikzcd}$$

Exercise 5. $\mathcal{O}/M^n \to \hat{\mathcal{O}}/\hat{M}^n$ is an isomorphism. In particular, the residue fields are the same and uniformisers stay uniformisers.

Chapter 6

p-adic Numbers

Consider $\mathbb{Q}$ with the p-adic absolute value $|\cdot|_p$ and the p-adic valuation v_p. Then the valuation ring is $\mathcal{O} = \{a/b : p \nmid b\}$, the maximal ideal is $M = (p)$ and the residue field is

$$\mathcal{O}/M \xrightarrow[\text{mod } p]{\sim} \mathbb{F}_p$$

Definition. The *field of p-adic numbers* $\mathbb{Q}_p$ is the completion of $\mathbb{Q}$ with respect to $|\cdot|_p$. The *ring of p-adic integers* $\mathbb{Z}_p$ is its valuation ring. Let $\pi = p$ and $A = \{0, 1, \ldots, p-1\}$ and apply Lemma 5.1.

$$\mathbb{Q} \hookrightarrow \left\{ \sum_{n=n_0}^{\infty} a_n p^n : a_n \in \{0, 1, \ldots, p-1\} \right\} = \mathbb{Q}_p$$

$$\mathbb{Z} \hookrightarrow \mathcal{O} \hookrightarrow \left\{ \sum_{n=0}^{\infty} a_n p^n : a_i \in \{0, 1, \ldots, p-1\} \right\} = \mathbb{Z}_p$$

$$M_{\mathbb{Z}_p} = (p) = \left\{ \sum_{n=1}^{\infty} a_n p^n : a_i \in \{0, 1, \ldots, p-1\} \right\}$$

$$\mathbb{Z}_p / M_{\mathbb{Z}_p} = \mathbb{F}_p$$

Example. Let $p = 3$ and take $A = \{0, 1, 2\}$.

(i) $x = 106 = 1 + 2 \times 3 + 2 \times 3^2 + 3^4$. In general, if $x \in \mathbb{Z}_p$ with $x = \sum_{n=0}^{\infty} a_n p^n$ then $x \in \mathbb{Z}_{\geq 0}$ if and only if this expansion termintates.

(ii) $x = 1/2 \in \mathbb{Z}_3$. Then

$$\frac{1}{2} \mod 3 = \frac{\bar{1}}{\bar{2}} = \bar{2} \in \mathbb{F}_3$$

and this lifts to $2 \in A$, giving the 0th digit.

$$\frac{1}{2} = 2 + \frac{-3}{2} = 2 + 3\frac{-1}{2}$$

Now

$$\frac{-1}{2} \mod 3 = \frac{\overline{-1}}{\bar{2}} = \bar{1} \in \mathbb{F}_3$$

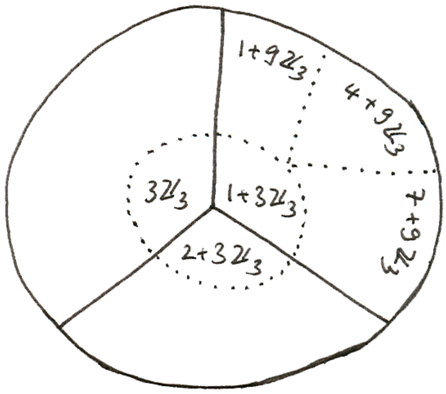
which lifts to $1 \in A$, giving the 1st digit. Continuing this process,

$$\frac{1}{2} = 2 + 1 \cdot 3 + \frac{-9}{2} = 2 + 1 \cdot 3 + 3^2\frac{-1}{2} = 2 + 1 \cdot 3 + 1 \cdot 3^2 + 1 \cdot 3^3 + \cdots$$

Exercise 6. Suppose $x \in \mathbb{Q}_p$. Then $x \in \mathbb{Q}$ if and only if its p-adic expansion is eventually periodic.

Adddition and multiplication work as for decimal expansion, for example,

$$\begin{aligned} \frac{1}{2} &= 2 + 3 + 3^2 + 3^3 + \cdots \\ +\frac{1}{2} &= 2 + 3 + 3^2 + 3^3 + \cdots \\ \frac{1}{2} + \frac{1}{2} &= 4 + 2 \cdot 3 + 2 \cdot 3^2 + 2 \cdot 3^3 + \cdots \\ &= (1+3) + 2 \cdot 3 + 2 \cdot 3^2 + 2 \cdot 3^3 + \cdots = 1 \end{aligned}$$



where the first circle distinguishes the first digit, the second circle distinguishes the first two digits, etc.

$\mathbb{Z}_p$ is topologically homeomorphic to a Cantor set.

6.1 Power Series in $\mathbb{Z}_p$

(i) The geometric series
$$\frac{1}{1-x} = 1 + x + x^2 + \cdots$$
converges (in any complete DVR) if and only $|x| < 1$ if and only if $x \in p\mathbb{Z}_p$. For example, in $\mathbb{Z}_3$,
$$\frac{1}{2} + 1 + \frac{1}{1-3} = 1 + (1 + 3 + 3^2 + \cdots) = 2 + 3 + 3^2 + 3^3 + \cdots$$

(ii) The p-adic logarithm has expansion
$$\log_p(1+x) = x - \frac{x^2}{2} + \frac{x^3}{3} - \cdots$$
It is left as an exercise to show this converges for $x \in \mathbb{Q}_p$ if and only if $|x| < 1$ if and only if $x \in p\mathbb{Z}_p$.

(iii) The exponential function
$$\exp(x) = \sum_{n=0}^{\infty} \frac{x^n}{n!}$$
This converges on $p\mathbb{Z}_p$ for $p > 2$ and on $4\mathbb{Z}_2$ for $p = 2$.

6.2 Additive Structure of $\mathbb{Z}_p$

$\mathbb{Z}_p \subset \mathbb{Q}_p$ is a subgroup of a field of characteristic 0, hence it is a torsion-free abelian group.

We have the following filtration by open and closed subgroups

$$\mathbb{Z}_p \supset p\mathbb{Z}_p \supset p^2\mathbb{Z}_p \supset \cdots$$

where

$$\begin{aligned} p^n\mathbb{Z}_p/p^{n+1}\mathbb{Z}_p &\cong \mathbb{Z}/p\mathbb{Z} \\ x &\mapsto n\text{th } p\text{-adic digit} \end{aligned}$$

6.3 Multiplicative Structure

We know

$$x = \sum_{n=0}^{\infty} a_n p^n$$

is a unit, i.e., in $\mathbb{Z}_p^*$ if and only if $a_0 \neq 0$. $\mathbb{Z}_p^*$ the multiplicative group of units. We have a filtration of subsets

$$\mathbb{Z}_p^* \supset 1 + p\mathbb{Z}_p \supset 1 + p^2\mathbb{Z}_p \supset \cdots$$

and upon writing $U_0 = \mathbb{Z}_p^*$, $U_1 = 1 + p\mathbb{Z}_p$, $U_2 = 1 + p^2\mathbb{Z}_p$, etc. we have, for $n \geq 1$,

$$U_n = \ker\bigl(\mathbb{Z}_p^* \to (\mathbb{Z}/p^n\mathbb{Z})^*, x \mapsto x \mod p^n\bigr)$$

hence this is a subgroup.

$$\begin{aligned} U_0/U_1 &\xrightarrow[\text{mod } p]{\sim} (\mathbb{Z}/p\mathbb{Z})^* && n = 0 \\ U_n/U_{n+1} &\xrightarrow{\sim} (\mathbb{Z}/p\mathbb{Z}, +) && n \geq 1 \end{aligned}$$

These are even isomorphisms of topological groups, under the convention that finite groups are equipped with the discrete topology.

Theorem 6.1. The following are isomorphisms of topological groups

$$\begin{aligned} \mathbb{Z}_p^* &\cong U_1 \times (\mathbb{Z}/p\mathbb{Z})^* \cong \mathbb{Z}_p \times (\mathbb{Z}/p\mathbb{Z})^* && p > 2 \\ \mathbb{Z}_p^* &\cong U_2 \times (\mathbb{Z}/4\mathbb{Z})^* \cong \mathbb{Z}_p \times \{\pm 1\} && p = 2 \end{aligned}$$

Proof. In the cases $p > 2$ and $p = 2$, respectively, consider the maps

$$\begin{aligned} &\exp\colon p\mathbb{Z}_p \to 1 + p\mathbb{Z}_p = U_1 && \log\colon 1 + p\mathbb{Z}_p \to p\mathbb{Z}_p \quad p > 2 \\ &\exp\colon p^2\mathbb{Z}_2 \to 1 + p^2\mathbb{Z}_p = U_2 && \log\colon 1 + p^2\mathbb{Z}_p \to p^2\mathbb{Z}_p \quad p = 2 \end{aligned}$$

These are continuous homomorphisms of groups, and they are inverses to each other. Thus

$$\begin{aligned} U_1 &\cong \mathbb{Z}_p \quad p > 2 \\ U_2 &\cong \mathbb{Z}_p \quad p = 2 \end{aligned}$$

[To prove that the these are indeed inverses and homomorphisms, we need to check that

$$\exp(\log(1+z)) = 1+z$$
$$\log(\exp(z)) = z$$
$$\exp(z+w) = \exp(z)\exp(w)$$

formally as power series, e.g.,

$$\exp(\log(1+z)) = \sum_{m\geq 0} \frac{1}{m!}\left(\sum_{n\geq 1} \frac{(-z)^n}{n}\right)^m = 1+z$$

This is true on $\mathbb{R}$, and now we can use uniqueness of Taylor series.]

Also

$$\begin{aligned} &\mathbb{Z}_p^*/U_1 \cong (\mathbb{Z}/p\mathbb{Z})^* && p>2 \\ &\mathbb{Z}_p^*/U_2 \cong (\mathbb{Z}/p^2\mathbb{Z})^* = (\mathbb{Z}/4\mathbb{Z})^* \cong \{\pm 1\} && p=2 \end{aligned}$$

That is, we have an exact sequence of groups

$$0 \to \mathbb{Z}_p \to \mathbb{Z}_p^* \to (\mathbb{Z}/p\mathbb{Z})^* \to 0$$

and we want to show that is *splits*.

[The sequence

$$0 \to A \xrightarrow{\alpha} B \xrightarrow{\beta} C \to 0$$

of abelian groups is *exact* if $A \xrightarrow{\alpha} B$ is injective and

$$B/A \xrightarrow[\beta]{\sim} C$$

An exact sequence *splits* if there exists a map $\gamma\colon C \to B$ such that $\beta \circ \gamma = \iota$, or equivalently, if $A \times C \xrightarrow{\sim} B$ via $(a, c) \mapsto \alpha(a) + \gamma(c)$.

For example,

$$0 \to \mathbb{Z} \xrightarrow{i_1} \mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \xrightarrow{p_2} \mathbb{Z}/2\mathbb{Z} \to 0$$

splits but

$$0 \to \mathbb{Z} \xrightarrow{\times 2} \mathbb{Z} \xrightarrow{\text{mod } 2} \mathbb{Z}/2\mathbb{Z} \to 0$$

does not split.]

Consider first the case $p = 2$. $\{\pm 1\} \hookrightarrow \mathbb{Z}_p^*$. It is clear that

$$\{\pm 1\} \subset \mathbb{Z}^* \subset \mathbb{Z}_p^*, \{\pm 1\} \hookrightarrow \mathbb{Z}_2^* \xrightarrow{\text{mod } 4} \{\pm 1\}$$

is the identity.

Now assume $p > 2$. We want $(\mathbb{Z}/p\mathbb{Z})^* \hookrightarrow \mathbb{Z}_p^* \hookrightarrow \mathbb{Q}_p^*$, i.e., what we want is the group of $(p-1)$th roots of unity inside $\mathbb{Q}_p$. Let $1 \leq a \leq p-1$. The details of the following argument are left as an exercise.

Suppose $(a^{p^n})_{n\geq 1}$ is a Cauchy sequence. Then, as $\mathbb{Q}_p$ is complete, $a^{p^n} \to x \in \mathbb{Q}_p$; in fact $x \in \mathbb{Z}_p$ as $\mathbb{Z}_p \subset \mathbb{Q}_p$ is closed. From $x \equiv a \pmod p$ and by continuity, we see that there are at least $p-1$ $(p-1)$th roots of unity in $\mathbb{Q}_p$, namely one for each a. Now use that $\mathbb{Q}_p$ is a field to deduce there are precisely $p-1$ of them. They form a group μ_{p-1} under multiplication.

This gives maps

$$(\mathbb{Z}/p\mathbb{Z})^* \xrightarrow{a \mapsto \lim a^{p^n}} \mathbb{Z}_p^* \qquad\qquad \mathbb{Z}_p^* \xrightarrow{\bmod p} (\mathbb{Z}/p\mathbb{Z})^*$$

and the composition is the identity. □

Corollary 6.2.

$$\mathbb{Q}_p^* \cong \mathbb{Z} \times \mathbb{Z}_p^* \cong \begin{cases} \mathbb{Z} \times \mathbb{Z}_p \times (\mathbb{Z}/p\mathbb{Z})^* & p > 2 \\ \mathbb{Z} \times \mathbb{Z}_p \times \{\pm 1\} & p = 2 \end{cases}$$

Corollary 6.3. There are exactly $p-1$ roots of unity in $\mathbb{Q}_p$ for $p > 2$, and 2 in $\mathbb{Q}_2$.

Proof. Note that $\mathbb{Z}$ and $\mathbb{Z}_p$ are torsion-free. □

Corollary 6.4. For $p > 2$,

$$\mathbb{Q}_p^*/\mathbb{Q}_p^{*2} \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}_p/2\mathbb{Z}_p \times (\mathbb{Z}/p\mathbb{Z})^*/(\mathbb{Z}/p\mathbb{Z})^{*2} \cong \{1, p, \eta, \eta p\}$$

for a non-residue η, upon writing $\mathbb{Z}/2\mathbb{Z} \cong \{1, p\}$, $\mathbb{Z}_p/2\mathbb{Z}_p \cong \{1\}$ as 2 is a unit in $\mathbb{Z}_p^*$, and $(\mathbb{Z}/p\mathbb{Z})^*/(\mathbb{Z}/p\mathbb{Z})^{*2} \cong \mathbb{Z}/2\mathbb{Z} \cong \{1, \eta\}$.

For $p = 2$,

$$\mathbb{Q}_p^*/\mathbb{Q}_p^{*2} \cong \{\pm 1, \pm 2, \pm 5, \pm 10\}$$

Corollary 6.5. $\mathbb{Q}_p$ has three quadratic extensions $\mathbb{Q}_p(\sqrt{p})$, $\mathbb{Q}_p(\sqrt{\eta})$, and $\mathbb{Q}_p(\sqrt{\eta p})$ for $p > 2$. For $p = 2$, $\mathbb{Q}_p$ has seven quadratic extensions.

Remark. Compare the last corollary with the following. $\mathbb{R}^*/\mathbb{R}^{*2} = \{\pm 1\}$, $\mathbb{R}$ has one quadratic extension $\mathbb{R}(i) = \mathbb{C}$, and $\mathbb{Q}^*/\mathbb{Q}^{*2}$ is infinite.

Note 1. Suppose K is a field with $\mathrm{char}(K) \neq 2$. Then quadratic extensions of K are in one-to-one correspondence with non-trivial elements of K^*/K^{*2} via

$$K(\sqrt{d}) \mapsto d$$
$$K[X]/(X^2 + aX + b) \hookleftarrow a^2 - nb$$

Note 2. Suppose $p \neq 2$. Under the logarithm map,

$$U_1 = 1 + p\mathbb{Z}_p \to p\mathbb{Z}_p$$
$$U_n = 1 + p^n\mathbb{Z}_p \to p^n\mathbb{Z}_p$$

and $p\mathbb{Z}_p \supset p^n\mathbb{Z}_p$ is the unique subgroup of index p^{n-1} as this is true on the LHS.

Corollary 6.6. Suppose $p \neq 2$. Then

$$(\mathbb{Z}/p^n\mathbb{Z})^* \cong \mathbb{Z}_p^*/U_n \cong (\mathbb{Z}/p\mathbb{Z})^* \times (\mathbb{Z}/p^{n-1}\mathbb{Z})$$

where for the last group on the RHS, $U_1/U_n \cong p\mathbb{Z}_p/p^n\mathbb{Z}_p$. The RHS is a product of cyclic groups of coprime order, so $(\mathbb{Z}/p^n\mathbb{Z})^*$ is cyclic, which is important in basic number theory.

Corollary 6.7. Suppose $p = 2$. Then

$$(\mathbb{Z}/2^n\mathbb{Z})^* \cong (\mathbb{Z}/2\mathbb{Z}) \times (\mathbb{Z}/2^{n-2}\mathbb{Z})$$

generated by -1 and 5.

Note 3. Let $u \in \mathbb{Z}_p^*$. The following are equivalent.

(i) u is a square.
(ii) $u \mod p^n$ is a square in $(\mathbb{Z}/p^n\mathbb{Z})^*$ for all $n \geq 1$.
(iii) If $p > 2$, $u \mod p$ is a square in $(\mathbb{Z}/p\mathbb{Z})^*$. Otherwise, if $p = 2$, $u \mod 8$ is a square in $(\mathbb{Z}/8\mathbb{Z})^*$.

Lemma 6.8. Consider the following system of polynomial equations in $\mathbb{Z}$ or $\mathbb{Z}_p$,

$$V\colon \begin{cases} f_1(x_1, \ldots, x_k) = 0 \\ \vdots \\ f_r(x_1, \ldots, x_k) = 0 \end{cases}$$

Then V has p-adic solution $x \in \mathbb{Z}_p^k$ if and only if V has a solution modulo p^n for all $n \geq 1$. In different notation, $V(\mathbb{Z}_p) \neq \emptyset$ if and only if $V(\mathbb{Z}/p^n\mathbb{Z}) \neq \emptyset$ for all $n \geq 1$.

Proof. The 'if' direction is obvious. For the 'only if' direction, take $x^{(n)} \in \mathbb{Z}_p^k$ with $f_i(x^{(n)}) \equiv 0 \pmod{p^n}$ for all $i = 1, \ldots, r$. As $\mathbb{Z}_p^k$ is compact, there exists a convergent subsequence $x^{(n_i)} \to x \in \mathbb{Z}_p^k$, and by continuity $f_i(x) = 0$ for $i = 1, \ldots, r$. $\square$

We now consider the following setting. Let K be complete with respect to the non-Archimedean absolute value $|\cdot|$ and let $\mathcal{O} = \{x \in K : |x| \leq 1\}$ be its valuation ring.

Theorem 6.9 (Hensel's Lemma, Version 1)**.** Let $f(X) \in \mathcal{O}[X]$ be monic and suppose there exists $x_1 \in \mathcal{O}$ such that

$$\begin{aligned} &|f(x_1)| < 1 && (\iff f(x_1) \in M) \\ &|f'(x_1)| = 1 && (\iff f'(x_1) \in \mathcal{O}^\times = \mathcal{O} \setminus M) \end{aligned}$$

Then there exists a unique $x \in \mathcal{O}$ such that $f(x) = 0$ and $|x - x_1| \leq |f(x_1)|$.

Proof. Choose any $\pi \in M \setminus \{0\}$, not necessarily a uniformiser, such that $\pi \mid f(x_1)$ in $\mathcal{O}$. We proceed by induction on n. Given x_n such that $|x_n - x_1| < |f(x_1)|$ and $f(x_n) \equiv 0 \pmod{\pi^n}$, we want a unique $x_{n+1} \equiv x_n \pmod{\pi^n}$ such that $|x_{n+1} - x_1| < |f(x_1)|$ and $f(x_{n+1}) \equiv 0 \pmod{\pi^{n+1}}$. Then, as $(x_n)_n$ is Cauchy, we take $x = \lim_{n\to\infty} x_n$ and by continuity have $f(x) = 0$. Consider

$$\begin{aligned} \mathcal{O}_K[T] \ni f(x_n + \pi^n T) &= \sum_{j=0}^{\deg(f)} \frac{f^{(j)}(x_n)}{j!} \pi^{nj} T^j \\ &\equiv f(x_n) + f'(x_n)\pi^n T \pmod{\pi^{n+1}} \end{aligned}$$

and recall $f(x_n) \equiv 0 \pmod{\pi^n}$ and $f'(x_n)$ is a unit, as $|f'(x_1)| = 1$ and x_1 is close to x_n. In order to force this to be 0 mod π^{n+1} set $T = -f(x_n)/(f'(x_n)\pi^n) \in \mathcal{O}$, and this is a unique choice modulo T. In other words, if we let

$$x_{n+1} = x_n - \frac{f(x_n)}{f'(x_n)}$$

then $f(x_{n+1}) \equiv 0 \pmod{\pi^{n+1}}$. $\square$

This is essentially the Newton–Raphson method.

Theorem 6.10 (Hensel's Lemma, Version 2)**.** Let $f_1, \dots, f_r \in \mathcal{O}[x_1, \dots, x_d]$, $r \leq d$. Suppose $x_1 \in \mathcal{O}^d$ is such that

$$\begin{aligned} f_i(x_1) &\equiv 0 \pmod{M} \\ |\frac{\partial f_i}{\partial x_j}(x_1) &\mod M| = r \end{aligned}$$

where $\partial f_i / \partial x_j \in M_{r \times d}(k)$, $k = \mathcal{O}/M$, for every i, j. Then there exists $x \in \mathcal{O}^d$, not in general unique, such that $x \equiv x_1 \pmod{M}$ and $f_i(x) = 0$ for all $i = 1, \dots, r$.

Proof. Similar. □

Theorem 6.11 (Hensel's Lemma, Version 3)**.** Suppose $f \in \mathcal{O}[X]$ is monic and $x_1 \in \mathcal{O}$ is such that $|f(x_1)| < |f'(x_1)|^2$. Then there exists a unique $x \in \mathcal{O}$ such that $f(x) = 0$ and $|x - x_1| < |f(x_1)|/|f'(x_1)|$.

Proof. Similar. □

Example (Square Roots of Unity)**.** This gives an alternative proof that for $u \in \mathbb{Z}_p^*$, if $u \mod p \in \mathbb{F}_p^{*2}$ then $u \in \mathbb{Z}_p^{*2}$.

Suppose $p \neq 2$ and let $u \in \mathbb{Z}_p^*$. Suppose

$$u \equiv \bar{u} = y^2 \pmod{p}$$

in $\mathbb{F}_p^*$. Look at $f(x) = x^2 - u$ and reduce modulo $M = (p)$,

$$\bar{f}(x) = x^2 - \bar{u} = (x - y)(x + y)$$

This has roots $y, -y$ in $\mathbb{F}_p$. Lift y to any element $Y \in \mathbb{Z}_p$ such that $Y \mod p = y$. Then

$$\begin{aligned} f(Y) &= Y^2 - u \equiv 0 \pmod{p} \\ f'(Y) &= 2Y \not\equiv 0 \pmod{p} \end{aligned}$$

so as u is a unit, Y is a unit and $2Y$ is a unit. By Hensel's Lemma, there exists $X \in \mathbb{Z}_p$ such that $X^2 = u$ so $f(x) = x^2 - u = (x - X)(x + X)$ factorises over $\mathbb{Z}_p$.

This does not work for $p = 2$ as 2 is not a unit in $\mathbb{Z}_2$, but Hensel's Lemma (Version 3) still applies.

Exercise 7. A solution modulo 8 lifts to a solution in $\mathbb{Z}_2$.

In general, let K be a complete non-Archimedean field with $\mathcal{O}$, M and $k = \mathcal{O}/M$. Suppose $f(X) \in \mathcal{O}[X]$ is monic and $\bar{f} = f \mod M$ is separable, i.e., $\bar{f}$ has no repeated roots in $\bar{k}$, or equivalently, $\gcd(\bar{f}, \bar{f}') = 1$ in $k[X]$. Then, as $\mathcal{O}$ is integrally closed,

$$\begin{aligned} \{\text{roots of } f(X) \text{ in } K\} &= \{\text{roots of } f(X) \text{ in } \mathcal{O}\} \\ &\leftrightarrow \{\text{roots of } \bar{f} \text{ in } k\} \end{aligned}$$

where the two maps are reduction modulo M and Hensel lifting.

Example (($p-1$)th Roots of Unity in $\mathbb{Z}_p^*$)**.** Let $f(X) = X^p - X$ so $\bar{f}(X) = X(X-1)\cdots(X-(p-1))$. By Hensel's Lemma, $X^p - X$ has p distinct roots $[0], [1], \ldots, [p-1]$ and

$$[\cdot]\colon \mathbb{F}_p^* \to \mathbb{Z}_p^*$$

is a group homomorphism, called *Teichmüller lift.*

Example. Consider $p = 5$, $\mathbb{Q}_5$, $\mathbb{Z}_5$, $k = \mathbb{F}_5$. Then

$$\begin{aligned} &[0] = 0 \qquad [1] = 1 \qquad [-1] = 2 \\ &[2] = 2 + 1 \cdot 5 + 2 \cdot 5^2 + 1 \cdot 5^3 + 3 \cdot 5^4 + \cdots \\ &[3] = 3 + 3 \cdot 5 + 2 \cdot 5^2 + 3 \cdot 5^3 + 1 \cdot 5^4 + \cdots \end{aligned}$$

In general, let K be a complete non-Archimedean field with $\mathcal{O}$, M and suppose $k = \mathcal{O}/M$ is finite (or injects into $\bar{F}_p$). Then there exists a unique group homomorphism

$$[\cdot]\colon k^* \to K^*$$

such that $[x] \mod M = x$, called the Teichmüller lift. To see this, apply Hensel's Lemma to $X^{|k|} - X$.

Chapter 7

Local Fields

Suppose K is a local, non-Archimedean field with $\mathcal{O}$, M, $|\cdot|$ and discrete valuation v, uniformiser π, and $\mathcal{O}/M = k \cong \mathbb{F}_{p^n}$.

By considering Teichmüller lifts, $\{[a] : a \in k\}$ is a set of representatives for $\mathcal{O}/M$, so

$$K = \left\{ \sum_{n=n_0}^{\infty} [a_n]\pi^n : a_n \in k \right\}$$

where $[a_n]$ are called *Teichmüller digits.*

Now suppose $\mathrm{char}(K) = q > 0$. Then since $\mathrm{char}(K) = \mathrm{char}(k)$, we have $q = p$. Then $\mathbb{F}_p \hookrightarrow K$ and, by Hensel's Lemma, K contains the roots of $X^{p^n} - X$. Thus K contains $\mathbb{F}_p(\text{roots of } X^{p^n} - X) = \mathbb{F}_{p^n}$, that is,

$$[\cdot]\colon \mathbb{F}_{p^n} \hookrightarrow K$$

in this case is a field inclusion.

Calling $t = \pi$,

$$K = \left\{ \sum_{m=m_0}^{\infty} a_m t^m : a_m \in \mathbb{F}_{p^n} \right\} = \mathbb{F}_{p^n}((t))$$

$$\mathcal{O} = \left\{ \sum_{m=1}^{\infty} a_m t^m : a_m \in \mathbb{F}_{p^n} \right\} = \mathbb{F}_{p^n}[[t]]$$

So we have a unique local field of positive characteristic, with given residue field $\mathbb{F}_{p^n}$, namely $\mathbb{F}_{p^n}((t))$.

Theorem 7.1. Suppose K is a local field. Then one of the following three cases applies.

(i) $K \cong \mathbb{R}$ or $\mathbb{C}$ (Archimedean);
(ii) $K \cong \mathbb{F}_q((t))$ for a unique $q = p^n$ (Equal Characteristic);
(iii) $[K : \mathbb{Q}_p] < \infty$ for a unique p (Mixed Characteristic).

Proof. We have already seen the two cases K is Archimedean and K is non-Archimedean with $\mathrm{char}(K) > 0$.

So suppose K is local, non-Archimedean and $\mathrm{char}(K) = 0$. Then $\mathbb{Q} \hookrightarrow K$, and so $|\cdot|$ restricts to $\mathbb{Q} \subset K$. Note $|\cdot|_{\mathbb{Q}}$ is non-Archimedean and non-trivial, for otherwise $\mathbb{Z} \hookrightarrow \mathcal{O}$

is an infinite discrete set, hence closed, contradicting that $\mathcal{O}$ is compact. By Ostrowski's Theorem, $|\cdot|_{\mathbb{Q}}$ is $|\cdot|_p$ for some p, so

$$\mathbb{Q}, |\cdot|_p \hookrightarrow K, |\cdot|$$

Taking completions, $\mathbb{Q}_p \hookrightarrow K$, and it suffices to show $[K : \mathbb{Q}_p] < \infty$. Let $k = \mathcal{O}/M$, $k \supset \mathbb{F}_p$, and call $[k : \mathbb{F}_p] = f$. Say k has $\mathbb{F}_p$-basis $\bar{v}_1, \ldots, \bar{v}_f$ and lift these to arbitrary $v_1, \ldots, v_f \in \mathcal{O}$.

The valuation is discrete, and we may assume it is normalised so $v(\pi) = 1$.

$$\begin{tikzcd} K^* \arrow[r, two heads, "v"] & \mathbb{Z} \\ \mathbb{Q}_p^* \ni p \arrow[u, hook] \arrow[r, mapsto] & e > 0 \end{tikzcd}$$

for some integer $e > 0$, because $p \in M_{\mathbb{Q}_p} \subset M_K$ so $v(p) > 0$.

We claim that $[K : \mathbb{Q}_p] \leq ef$ (in fact, it is equal to ef), and $v_i \pi^j$ generate K over $\mathbb{Q}_p$.

Multiplying by a suitable power of p, it is enough to show that, for every $x \in \mathcal{O}$,

$$x = \sum_{\substack{1 \leq i \leq f \\ 1 \leq j \leq e}} A_{ij} v_i \pi^j$$

for some $A_{ij} \in \mathbb{Z}_p$. Clearly,

$$x = \sum_{\substack{1 \leq i \leq f \\ 1 \leq j \leq e}} a_{ij} v_i \pi^j + p \cdot \mathcal{O}$$

for unique $a_{ij} \in \{0, 1, \ldots, p-1\}$, and

$$= \sum_{\substack{1 \leq i \leq f \\ 1 \leq j \leq e}} a_{ij} v_i \pi^j + p \sum_{\substack{1 \leq i \leq f \\ 1 \leq j \leq e}} a'_{ij} v_i \pi^j + \cdots$$

which is a combination of $v_i \pi^j$ with $\mathbb{Z}_p$-coeffients. $\square$

We know that if K is local, non-Archimedean and $\operatorname{char}(K) = 0$ then

$$[K : \mathbb{Q}_p] < \infty$$

Conversely, we will show that every finite extension K of $\mathbb{Q}_p$ has a *unique* structure as a local field, i.e., $|\cdot|_p$ extends to a unique absolute value on K, and K is complete with respect to it.

Chapter 8

Inverse Limits

Instead of considering

$$\mathbb{Q}, |\cdot|_p \xrightarrow{\widehat{\ }} \mathbb{Q}_p \xrightarrow{\text{valutation ring}} \mathbb{Z}_p$$

we consider, given $\mathbb{Z}$ and (p) the quotients $\mathbb{Z}/p^i\mathbb{Z}$ for $i \in \mathbb{N}$ and the projections $\mathbb{Z}/p^i\mathbb{Z} \twoheadrightarrow \mathbb{Z}/p^j\mathbb{Z}$ for $j \leq i$.

We call I a *directed set* if I is a set equipped with a partial order $\leq$. Let $(A_i)_{i\in I}$ be a sequence of groups (resp. rings). Let $\pi_{ij} : A_i \to A_j$ be group homomorphism (resp. ring homomorphisms) for $j \leq i$ such that $\pi_{ii} = \iota$ and $\pi_{jk} \circ \pi_{ij} = \pi_{ik}$ for $k \leq j \leq i$.

Definition. The inverse limit is defined as

$$A = \varprojlim_{i\in I}(A_i, \pi_{ij}) = \varprojlim_{i\in I} A_i = \{(a_i)_{i\in I} : \pi_{ij}(a_i) = a_j \ \forall j \leq i\}$$

This is a group (resp. ring).

Example. $\mathbb{N}$ can be made a directed set via $(\mathbb{N}, \leq)$ or $(\mathbb{N}, |)$.

Example. Let $I = (\mathbb{N}, \leq)$, $(A_i)_{i\in\mathbb{N}} = (\mathbb{Z}/p^i\mathbb{Z})_{i\in\mathbb{N}}$ for some prime p, and let

$$\pi_{ij} \colon \mathbb{Z}/p^i\mathbb{Z} \to \mathbb{Z}/p^j\mathbb{Z}$$

for $j \leq i$. Then

$$\mathbb{Z}_p = \varprojlim_{i\in\mathbb{N}} \mathbb{Z}/p^i\mathbb{Z}$$

Similarly,

$$k[[t]] = \varprojlim_{i\in\mathbb{N}} k[t]/(t^i)$$

where π_{ij} is truncation modulo t^j.

Example. Let $I = (\mathbb{N}, |)$, $A_i = \mathbb{Z}/i\mathbb{Z}$, and

$$\pi_{ij} \colon \mathbb{Z}/i\mathbb{Z} \xrightarrow{\text{mod } j} \mathbb{Z}/j\mathbb{Z}$$

for $j \mid i$. Then

$$\varprojlim_{i\in\mathbb{N}} \mathbb{Z}/i\mathbb{Z} = \hat{\mathbb{Z}}$$

is a ring. It is left as an exercise to also show

$$\hat{\mathbb{Z}} = \prod_{p \text{ prime}} \mathbb{Z}_p$$

Remark. (i) $A = \varprojlim_{i\in I}(A_i, \pi_{ij})$. This has the universal property that we have projections $A \xrightarrow{p_i} A_i$ such that $p_i\pi_{ij} = p_j$. For any B with such maps $B \xrightarrow{q_i} A_i$, $q_i\pi_{ij} = q_j$ there exists a unique $\phi\colon B \to A$

$$\begin{tikzcd} A \arrow[dr, "p_i"] & \\ B \arrow[u, "\phi"] \arrow[r, "q_i"'] & A_i \end{tikzcd}$$

(ii) If the A_i have a topology, the *inverse limit topology* on $A = \varprojlim_{i\in I} A_i$ is the weakest topology that makes all $A \xrightarrow{p_i} A_i$ continuous.

Example. On $\mathbb{Z}_p$ the inverse limit topology coincides with the p-adic topology. The LHS is generated by preimages of points under $\mathbb{Z}_p \to \mathbb{Z}/p^i\mathbb{Z}$, and the RHS is generated by open balls $a + p^i\mathbb{Z}_p$.

Let $K, |\cdot|$ be non-Archimedean with $\mathcal{O}$, M, and corresponding valuation v. Choose $\pi \in M \setminus \{0\}$ and normalise such that $v(\pi) = 1$.

Proposition 8.1. *K is complete with respect to $|\cdot|$ if and only if*

$$\mathcal{O} \to \varprojlim_{i\in\mathbb{N}} \mathcal{O}/\pi^i\mathcal{O}, x \mapsto (x \mod \pi^i)_{i\in\mathbb{N}} \tag{$*$}$$

is an isomorphism.

Note 4. $\varprojlim_{i\in\mathbb{N}} \mathcal{O}/\pi^i\mathcal{O}$ is the completion of the ring $\mathcal{O}$ with respect to the ideal (π).

Note 5. If $(*)$ is an isomorphism, we say $\mathcal{O}$ is (π)-adically complete (cf. surjective) and separated (cf. injective).

Proof. Write $K = \bigcup_x x + \mathcal{O}$ as a disjoint union of open and closed sets, where x runs over coset representatives of $\mathcal{O}$ in K. Note that K is complete with respect to $|\cdot|$ if and only if each $x+\mathcal{O}$ is complete with respect to $|\cdot|$ if and only if $\mathcal{O}$ is complete with respect to $|\cdot|$. Equivalently,

$$\forall (x_n)_n \text{ in } \mathcal{O} \text{ with } |x_n - x_{n+1}| \to 0 \quad \exists x \in \mathcal{O} \quad |x_n - x| \to 0 \tag{A}$$

and such an x is necessarily unique.

Now $(*)$ is an isomorphism if and only if

$$\forall (x_i)_i \text{ in } \mathcal{O} \text{ with } v(x_{i+1} - x_i) \geq i \quad \exists! x \in \mathcal{O} \quad v(x - x_i) \geq i \tag{B}$$

But every sequence in (A) has a subsequence as in (B), so they are equivalent. □

8.1 Profinite Groups

Let I be a directed set and $\pi_{ij}\colon G_i \to G_j$ group homomorphisms. Suppose $(G_i)_{i\in I}$ be a directed system of finite groups, all with the discrete topology. Then

$$G = \varprojlim_{i\in I} G_i$$

is a *profinite group* with the inverse limit topology, called the profinite topology.

Note 6. If the G_i are compact (e.g. finite) then $G \subset \prod_{i \in I} G_i$ is compact and so G is compact in the profinite topology.

Example. $(\mathbb{Z}_p, +)$, $(\mathbb{Z}_p^*, \times)$, $(\mathbb{F}_{p^n}[[t]], +)$, $(\hat{\mathbb{Z}}, +)$.

8.2 Main Example

Let L/K be an extension of fields, possibly infinite, but the union of finite Galois extensions k/K. For example, $\bar{\mathbb{Q}}/\mathbb{Q}$, $\bar{\mathbb{F}}_p/\mathbb{F}_p$, recalling $\bar{\mathbb{F}}_p = \bigcup_{n \geq 1} \mathbb{F}_{p^n}$. Then

$$G = \mathrm{Gal}(L/K) = \mathrm{Aut}(L/K) = \varprojlim_k \mathrm{Gal}(k/K)$$

is a profinite group.

By the Fundamental Theorem of Galois Theory, extensions of K in L are in one-to-one correspondence with closed subgroups of G, and finite extensions of K in L are in one-to-one correspondence with open subgroups of G.

Exercise 8. Show the following

$$\mathrm{Gal}(\bar{\mathbb{F}}_q/\mathbb{F}_q) \cong (\hat{Z}, +)$$
$$\mathrm{Frob}_q \colon x \mapsto x^q \leftrightarrow 1$$
$$\mathrm{Gal}(\mathbb{Q}\Big(\bigcup_{n \geq 1} \mu_{p^n}\Big)/\mathbb{Q}) \cong \mathbb{Z}_p^*$$
$$\mathrm{Gal}(\mathbb{Q}\Big(\bigcup_{n \geq 1} \mu_n\Big)/\mathbb{Q}) \cong \hat{Z}^*$$

Note $\mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q})$ is presently still unknown.

Chapter 9

Extensions of Complete Fields

Example.

$$\begin{tikzcd}
\mathbb{Z}[i] & P \arrow[l, hook'] \arrow[d] & 1+i \arrow[d, dash] & 3 \arrow[d, dash] & 2+i \arrow[d, dash] & 2-i \arrow[dl, dash] & 7 \arrow[d, dash] \\
\mathbb{Z} \arrow[u, hook] & P \cap \mathbb{Z} & 2 & 3 & 5 & & 7
\end{tikzcd}$$

$|\cdot|_5$ on $\mathbb{Q}$ has two extensions to $\mathbb{Q}(i)$, $|\cdot|_{2+i}$ and $|\cdot|_{2-i}$. This cannot happen for complete fields. “Primes do not split”.

Theorem 9.1. Suppose $K, |\cdot|$ is complete non-Archimedean and L/K is finite with $[L : K] = d$. Then

(i) There is a unique absolute value $|\cdot|_L$ on L extending $|\cdot|$ on K, and L is complete with respect to this.
(ii) $|x|_L = |N_{L/K}(x)|^{1/d}$.
(iii) $\mathcal{O}_L$ is the integral closure of $\mathcal{O}_K$ in L.

Proof. **Uniqueness.** We do more. Given $K, |\cdot|$ and a vector space V over K, a *norm* on V is a map $\|\cdot\| \colon V \to \mathbb{R}$ such that

- $\|v\| = 0$ if and only if $v = 0$;
- $\|\alpha v\| = |\alpha| \|v\|$;
- $\|v + w\| \leq \max\{\|v\|, \|w\|\}$.

For example, $V = K^d$, $\|v\|_{\text{sup}} = \max_i |v_i|$ for $v = (v_1, \ldots, v_d)$. We say two norms are *equivalent*, denoted $\|\cdot\|_1 \sim \|\cdot\|_2$, if there exists $c, C \in \mathbb{R}_{>0}$ such that

$$c\|\cdot\|_1 \leq \|\cdot\|_2 \leq C\|\cdot\|_1$$

A norm defines a metric on V, and equivalent norms induce the same topology.

Proposition 9.2. Let $K, |\cdot|$ be complete non-Archimedean and V be a finite-dimensional K-vector space. Then any two norms on V are equivalent, and V is complete with respect to any of them.

Proof. By induction on $d = \dim V$. If $d = 1$ then $V = K \cdot e$, $\|\alpha e\| = |\alpha| \|e\|$, so any two norms on V are multiples of each other.

Suppose $d > 1$, let $V = K^d$ with norm $\|\cdot\|$. We show that $\|\cdot\| \sim \|\cdot\|_{\text{sup}}$. This also proves that V is complete. Let $e_1, \dots, e_d$ be a basis of V, let $C = \max_i \|e_i\|$. Then

$$v = \sum_{i=1}^{d} v_i e_i \implies \|v\| \le \max_i \|v_i e_i\| \le C\|v\|_{\text{sup}}$$

It suffices to prove $c\|v\|_{\text{sup}} \le \|v\|$ for some $0 < c$. Suppose not and take a sequence $v^{(n)}$ in $V \setminus \{0\}$ such that

$$\frac{\|v^{(n)}\|}{\|v^{(n)}\|_{\text{sup}}} \to 0$$

as $n \to \infty$. Then, for some $i \in \{1, \dots, d\}$,

$$\|v^{(n)}\|_{\text{sup}} = |v_i^{(n)}|$$

for infinitely many $n \in \mathbb{N}$. Without loss of generality assume $i = d$, replace $v^{(n)}$ by this subsequence and rescale

$$v^{(n)} \mapsto \frac{1}{v_d^{(n)}} v^{(n)}$$

so that

(i) $v_d^{(n)} = 1$ for all $n \in \mathbb{N}$;
(ii) $v^{(n)}$ is in $\mathcal{O}_K^d \subset K^d$, i.e., $\|v^{(n)}\|_{\text{sup}} = 1$;
(iii) $\|v^{(n)}\| \to 0$ as $n \to \infty$.

Let $u^{(n)} = v^{(n)} - e_d \in \mathcal{O}_k^{d-1} \subset \mathcal{O}_K^d$. Then

$$\|u^{(n+1)} - u^{(n)}\| = \|v^{(n+1)} - v^{(n)}\| \le \max\{\|v^{(n+1)}\|, \|v^{(n)}\|\} \to 0$$

as $n \to \infty$. By induction, $(K^{d-1}, \|\cdot\|)$ is complete, so

$$u^{(n)} \to u \in K^{d-1}$$

and

$$\|e_d + u\| = \lim_{n\to\infty} \|e_d + u^{(n)}\| = \lim \|v^{(n)}\| = 0$$

so $e_d + u = 0$ but $u \in K^{d-1}$, $e_d \notin K^{d-1}$, contradiction. □

Now suppose $|\cdot|_1$, $|\cdot|_2$ are absolute values on L extending $|\cdot|$ on K. They are norms on L, hence equivalent, i.e.,

$$c|x|_1 \le |x|_2 \le C|x|_1$$

But $|x^n|_1 = |x|_1^n$ and $|x^n|_2 = |x|_2^n$, so

$$c^{1/n}|x|_1 \le |x|_2 \le C^{1/n}|x|_1$$

As $c^{1/n}, C^{1/n} \to 1$ as $n \to \infty$,

$$|x|_1 = |x|_2$$

Existence. Let $|x|_L = |N_{L/K}(x)|^{1/d}$. We want to prove this is an absolute value on L. Clearly

(i) $|x|_L$ extends $|\cdot|$ on K;

(ii) $|x|_L = 0$ if and only if $x = 0$;
(iii) $|xy|_L = |x|_L |y|_L$.

It suffices to prove $|x+y|_L \leq \max\{|x|_L, |y|_L\}$. Without loss of generality $|y|_L \leq |x|_L$, so $z = y/x$ has $|z|_L \leq 1$, and

$$|x+y|_L \leq |x|_L \iff |1+z|_L \leq 1$$

so we claim

$$N_{L/K}(z) \in \mathcal{O}_K \implies N_{L/K}(1+z) \in \mathcal{O}_K$$

Let f be the minimal polynomial of z over K. Then

$$N_{L/K}(z) = \pm f(0)^m$$

where $m = [L : K]/\deg(f)$. Then, as f is monic irreducible in $K[X]$ and $f(0)^m \in \mathcal{O}_K$ hence $f(0) \in \mathcal{O}$ (as $\mathcal{O}_K$ is integrally closed), we deduce $f(z) \in \mathcal{O}_K[z]$ (see Question 23). Therefore,

$$N_{L/K}(1+z) \in \mathcal{O}_K$$

Finally, $\mathcal{O}_L$ is the integral closure of $\mathcal{O}_K$ in L, because we know that $N_{L/K}(z) \in \mathcal{O}_K$ if and only if z is integral over K. □

9.1 Consequences

Suppose $K, |\cdot|$ is complete non-Archimedean. Then $|\cdot|$ extends uniquely to $\bar{K}$,

$$\alpha \in \bar{K} \implies |\alpha| = |N_{K(\alpha)/K}(\alpha)|^{1/[K(\alpha):K]}$$

Note that, in general, $\bar{K}$ is not complete, e.g., $\bar{\mathbb{Q}}_p$ is not. Its completion is $\mathbb{C}_p = \hat{\bar{\mathbb{Q}}}_p$, which is complete and algebraically closed.

If $\alpha, \alpha' \in \bar{K}$ are Galois conjugates over K then $|\alpha| = |\alpha'|$. To see this, note that α, α' are Galois conjugates if and only if α, α' are roots of the same irreducible polynomials $f \in K[X]$, and then α, α' have the same norm.

Lemma 9.3 (Krasner's Lemma)**.** Let $f(X) \in K[X]$ be irreducible and monic, say

$$f(x) = \prod_{i=1}^{d}(X - \alpha_i)$$

over $\bar{K}$. Suppose $\beta \in \bar{K}$ is such that $|\beta - \alpha_1| < |\beta - \alpha_i|$ for all $i > 1$. Then $\alpha_1 \in K(\beta)$.

Proof. $\alpha_1 \neq \alpha_2, \ldots, \alpha_d$, so α_1 is a simple root of f, so f is separable. Let $L = K(\beta)$, and note $L' = L(\alpha_1, \ldots, \alpha_d)$ is a Galois extension of L. For $\sigma \in \mathrm{Gal}(L'/L)$,

$$|\beta - \sigma(\alpha_1)| = |\sigma(\beta - \alpha_1)| = |\beta - \alpha_1| \neq |\beta - \alpha_i|$$

for all $i > 1$. Thus $\sigma(\alpha_1) \neq \alpha_2, \ldots, \alpha_d$, so $\sigma(\alpha_1) = \alpha_1$. Hence the minimal polynomial of α_1 over L has degree 1, so $\alpha_1 \in K(\beta)$. □

As a consequence of this, $\mathbb{Q}_p$ has only finitely many extensions of a given degree.

Now suppose L/K is finite. We have

$$\begin{aligned} K, |\cdot| &\hookrightarrow L, |\cdot| \\ \mathcal{O}_K &\hookrightarrow \mathcal{O}_L \\ M_K &\hookrightarrow M_L \\ k_K &\hookrightarrow k_L \end{aligned}$$

Proposition 9.4. Suppose $[L : K] = d$, L/K is separable and the valuations are discrete. Then

$$\mathcal{O}_L \cong \mathcal{O}_K^d$$

as $\mathcal{O}_K$-modules.

Remark. All conditions are necessary, and the result does not hold for general number fields.

Proof. We want to show that $\mathcal{O}_L$ injects into a free $\mathcal{O}_K$-module of finite rank. Then, as $\mathcal{O}_K$ is a PID, $\mathcal{O}_L$ is free of finite rank, and since $\mathrm{Frac}(\mathcal{O}_K) = K$, $\mathrm{Frac}(\mathcal{O}_L) = L$ we conclude $\mathcal{O}_L$ has rank $[L : K] = d$.

Let $B(x, y) = \mathrm{Tr}_{L/K}(xy)$, $L \times L \to K$. It is a non-degenerate K-bilinear form, where the non-degeneracy of this form is equivalent to the separability of L/K.

Pick $e_1, \dots, e_d \in \mathcal{O}_L$ a basis for L/K, and let $e_1^\checkmark, \dots, e_d^\checkmark \in L$ be the dual basis with respect to B, i.e., $B(e_i, e_j^\checkmark) = \delta_{ij}$. Then

$$\mathcal{O}_L \subset \{x \in L : B(x, y) \in \mathcal{O}_K \ \forall y \in \mathcal{O}_L\} =: \mathcal{O}_L^\checkmark$$

as $\mathrm{Tr}_{L/K}(\mathcal{O}_L) \subset \mathcal{O}_K$, because $\mathcal{O}_L/\mathcal{O}_K$ is integral. Further,

$$\mathcal{O}_L^\checkmark \subset \bigoplus_{i=1}^{d} \mathcal{O}_k \cdot e_i^\checkmark$$

a finitely generated free $\mathcal{O}_K$-module. $\square$

Chapter 10

Ramification and Inertia

Consider the following setting. Suppose we have K, $|\cdot|$, v_k, $\mathcal{O}_K$, M_K, k_K and L, $|\cdot|$, v_L, $\mathcal{O}_L$, M_L, k_L, where $[L:K]=d$, all with their usual meaning.

Suppose v_K is discrete and normalised. Assume k_K is *perfect*, i.e., every finite extension of k_K is separable. This is the case, e.g., for $\mathbb{F}_q$, $\bar{\mathbb{F}}_p$, fields of characteristic 0, or algebraically closed fields. It is not true for $\mathbb{F}_p(t)$.

Definition. The *residue degree*, or *inertial degree*, is $f = f_{L/K} = [k_L : k_K]$.

Let the valuations on K^* and L^* be given by $\log_\alpha |\cdot| \colon K^* \twoheadrightarrow \mathbb{Z}$ and $\log_\alpha |N_{L/K}(\cdot)|^{1/d} \colon L^* \to \mathbb{R}$ with image in $(1/d)\mathbb{Z}$, respectively. Then the image is a discrete subgroup, so v_L is discrete.

Definition. The index $[v_L(L^*) : v_L(K^*)]$ is called the *ramification index* of L/K, denoted $e = e_{L/K}$. Equivalently, $(\pi_K) = (\pi_L^e)$ in $\mathcal{O}_L$.

Remark. There are two possible conventions.

(i) Normalise $v_L, |\cdot|_L$, but then $v_L|_{K^*} \neq v_K$ but $v_L|_{K^*} = e v_K$.
(ii) Let $v_L \colon L^* \to (1/e)\mathbb{Z}$, then v_L is not normalised but $v_L|_{K^*} = v_K$.

Both are used.

Proposition 10.1.
$$e_{L/K} f_{L/K} = [L:K]$$

Proof. We know $\mathcal{O}_L \cong \mathcal{O}_K^d$ as $\mathcal{O}_K$-modules where $d = [L:K]$. Thus
$$\mathcal{O}_L/\pi_K \mathcal{O}_L \cong \mathcal{O}_K^d / \pi_K \mathcal{O}_K^d \cong (\mathcal{O}_K/\pi_K \mathcal{O})^d \cong k_K^d$$
as $\mathcal{O}_K$-modules. But
$$\mathcal{O}_L \supset \pi_L \mathcal{O}_L \supset \pi_L^2 \mathcal{O}_L \supset \cdots \supset \pi_L^e \mathcal{O}_L = \pi_K \mathcal{O}_L$$
and
$$\pi_L^i \mathcal{O}_L / \pi_L^{i+1} \mathcal{O}_L \cong \mathcal{O}_L / \pi_L \mathcal{O}_L, \quad x \mapsto x \mod \pi_L^i$$
as $\mathcal{O}_K$-modules, so these are also isomorphic to $k_L \cong k_K^f$ as $\mathcal{O}_K$-modules. Comparing dimensions, $d = ef$. □

Definition. L/K is *unramified* if $e_{L/K} = 1$, or equivalently, $[L:K] = f_{L/K}$. L/K is *totally ramified* if $e_{L/K} = [L:K]$, or equivalently, $f_{L/K} = 1$, that is, $k_L \cong k_K$.

Note 7. Given extensions $M/L/K$,

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

by the tower law for $k_M/k_L/k_K$, and

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

by the tower law for $M/L/K$.

Example. Suppose $[L : \mathbb{Q}_p] = 2$ for some $p \neq 2$. Then

$$L = \mathbb{Q}_p(\sqrt{d})$$

for some $d \in \{p, \eta p, \eta\}$ with $\bar{\eta} = \eta \mod p \in \mathbb{F}_p^*$ a non-residue.

- $L = \mathbb{Q}_p(\sqrt{p})$, $\mathbb{Q}_p(\sqrt{\eta p})$ have $e_{L/\mathbb{Q}_p} \geq 2$ as $p = \sqrt{\eta p}^2 u$ for some unit u, so $v(\sqrt{\eta p}) = 1/2$ in L. So $e = 2$, $f = 1$, and this is a totally ramified extension.
- $L = \mathbb{Q}_p(\sqrt{\eta})$ has $f_{L/\mathbb{Q}_p} \geq 2$. L contains the roots of $X^2 - \eta$, so

$$k_L \supset \mathbb{F}_p(\text{roots of } X^2 - \bar{\eta}) = \mathbb{F}_{p^2}$$

as $X^2 - \bar{\eta}$ is irreducible over $\mathbb{F}_p$. So $e = 1$, $f = 2$ and this is an unramified extension.

Exercise 9. For $L/\mathbb{Q}_2$, the extension $L = \mathbb{Q}_2(\mu_3) = \mathbb{Q}_2(\sqrt{-3}) = \mathbb{Q}_2(\sqrt{5})$ is unramified, but the other six quadratic extensions are ramified.

Chapter 11

Unramified Extensions

Note that these are in one-to-one correspondence with extensions of the residue fields.

Theorem 11.1. (i) Suppose L/K is a finite, unramified extension. Then $\mathcal{O}_L = \mathcal{O}_K[\alpha]$ (and so $L = K(\alpha)$) for any $\alpha \in \mathcal{O}_L$ with $k_L = k_K(\bar{\alpha})$.

(ii) Suppose ℓ/k_K is finite. There exists an unramified extension L/K with $k_L \cong \ell$ over k_K.

(iii) Suppose L/K is a finite, unramified extension and let L'/K be any finite extension. Then

$$\mathrm{Hom}_K(L, L') \to \mathrm{Hom}_{k_K}(k_L, k_{L'})$$

is a bijection.

Proof. (i) We know $\mathcal{O}_L \cong \mathcal{O}_K^d$ as $\mathcal{O}_K$-modules, where $d = [L : K]$. As the extension L/K is unramified, $\pi_L = \pi_K$. Now $k_L = k_K(\bar{\alpha})$ implies $1, \bar{\alpha}, \ldots, \bar{\alpha}^{d-1}$ generate $\mathcal{O}_L/\pi_L\mathcal{O}_L$. Therefore, by Nakayama's lemma, as $\mathcal{O}_L$ is local, $1, \alpha, \ldots, \alpha^{d-1}$ generate $\mathcal{O}_L$ as an $\mathcal{O}_K$-module.

(ii) Write $\ell = k_K(\bar{\alpha})$. We can do this since k_K is perfect and so ℓ/k_K is separable, hence there exists a primitive element.
Lift the minimal polynomial $\bar{g}(X) \in k_K[X]$ of $\bar{\alpha}$ to any monic polynomial $g(X) \in \mathcal{O}_K[X]$, so $g(X)$ is irreducible. Now let $L = K(\text{roots of } g) = K[X]/(g(X))$.

(iii) Write $L = K(\alpha)$ as in (ii); so $k_L = k_K(\bar{\alpha})$. Let $g(X)$ be the minimal polynomial of α over K and let $\bar{g}(X)$ be its reduction over k_K.
Given $\tilde{\phi}\colon k_L \to k_{L'}$, we find a root $\tilde{\phi}(\bar{\alpha})$ of $\bar{g}(X)$ in $k_{L'}$. By Hensel's Lemma, there exists a unique root of $g(X)$ in L lifting to it, and hence there exists a unique $\phi\colon L \to L'$ lifting $\tilde{\phi}$.

□

Remark. Part (iii) implies the field L in (ii) is unique up to isomorphism.

Corollary 11.2. Suppose L/K is a finite, unramified extension. Then L/K is Galois if and only if k_L/k_K is Galois, and if this is the case then $\mathrm{Gal}(L/K) \cong \mathrm{Gal}(k_L/k_K)$.

Proof. K-automorphisms $\sigma\colon L \to L$ and k_K-automorphisms $\bar{\sigma}\colon k_L \to k_L$ are in one-to-one correspondence under the maps reduction modulo M_K and its inverse by part (iii) of Theorem 11.1. So

$$\mathrm{Aut}(L/K) \cong \mathrm{Aut}(k_L/k_K)$$

In particular, L/K is Galois if and only if $|\mathrm{Aut}(L/K)| = [L : K]$ if and only if $|\mathrm{Aut}(k_L : k_K)| = [k_L : k_K] = [L : K]$ if and only if k_L/k_K is Galois. □

Example. Suppose $K = \mathbb{Q}_p$. (The situation is similar for any local field K.) $\mathbb{Q}_p$ has a unique ramified extension of degree $n \geq 1$,

$$L_n = \mathbb{Q}_p(\mu_{p^n-1})$$

$L_n/\mathbb{Q}_p$ is Galois with $\mathrm{Gal}(L_n/\mathbb{Q}_p) \cong \mathbb{Z}/n\mathbb{Z}$.

This is because $\mathbb{F}_p$ has a unique extension of degree n,

$$\mathbb{F}_{p^n} = \mathbb{F}_p(\text{roots of } X^{p^n} - X) = \mathbb{F}_p(\mu_{p^n-1})$$

and $\mathbb{F}_{p^n}/\mathbb{F}_p$ is Galois with Galois group $\mathbb{Z}/n\mathbb{Z}$.

Corollary 11.3. Suppose L/K is finite. There exists a unique maximal unramified extension K' of K in L, so

$$\begin{tikzcd} L \\ K' \arrow[u, "\text{totally ramified}"] \\ K \arrow[u, "\text{unramified}"] \end{tikzcd}$$

and every unramified extension of K in L is contained in K'.

Proof.

$$\begin{tikzcd} L & k_L \\ K \arrow[u] & k_K \arrow[u] \end{tikzcd}$$

By part (iii) of Theorem 11.1, there exists an unramified extension K' of K with $k_{K'} \cong k_L$ over k_K. By part (ii) of Theorem 11.1, $K' \hookrightarrow L$ over K.

L/K' is totally ramified, i.e., $f_{L/K'} = 1$, and part (iii) of Theorem 11.1 gives the last claim. ☐

Note 8. If L/K is Galois then K'/K is Galois.

Example. Suppose $p \neq 2$ is a prime and let $K = \mathbb{Q}_p$. Then

$$\begin{tikzcd} L = \mathbb{Q}_p(\sqrt{p}, \sqrt{\eta}) & \\ & \mathbb{Q}_p(\sqrt{\eta}) \arrow[ul, "2"'] \\ \mathbb{Q}_p \arrow[uu, "e=f=2"] \arrow[ur, "2"'] & \end{tikzcd}$$

$\mathbb{Q}_p(\sqrt{\eta})$ is the maximal unramified extension of $\mathbb{Q}_p$ in L.

Chapter 12

Totally Ramified Extensions

Proposition 12.1. Suppose L/K is totally ramified of degree e, $\pi = \pi_L$ is a uniformiser and v_L is a normalised valuation, i.e., $v_L(\pi) = 1$. Then

(i) π satisfies an Eisenstein polynomial of degree e over $\mathcal{O}_K$.
(ii) $\mathcal{O}_L = \mathcal{O}_K[\pi]$.

Conversely, if $g \in \mathcal{O}_K[X]$ is Eisenstein then $L = K[X]/g(X)$ is totally ramified over K and $v_L(\text{root of } g) = 1$.

Recall that $g(X)$ is *Eisenstein* if and only if

$$g(X) = X^n + a_{n-1}X^{n-1} + \cdots + a_0$$

with $v(a_i) \geq 1$, $v(a_0) = 1$. Then $g(X)$ is irreducible by Eisenstein's criterion.

Proof. (i) Consider the minimal polynomial of π over K,

$$\pi^n + a_{n-1}\pi^{n-1} + \cdots + a_0 = 0$$

irreducible over K and $n \leq e = [L : K]$. π is integral over $\mathcal{O}_K$, so $a_i \in \mathcal{O}_K$ for all $i = 0, \ldots, n-1$. Now consider the valuation of the LHS. The sum is 0 so two terms have the same smallest valuation.

$$v_L(a_i\pi^i) = i + ev_K(a_i) \equiv i \pmod{e}$$

So these are all distinct for $i < e$. Hence $n = e$, $v_L(a_0) = v_L(\pi^n) = n = e$, in other words, $v_K(a_0) = 1$, and $v_K(a_i) > 0$ because $v_K(a_0)$ and $v_K(a_n)$ are smallest. Thus $g(X)$ is Eisenstein, irreducible, and $L = K(\pi)$.

(ii) For $x \in L$ write $x = \sum_{i=0}^{e-1} b_i\pi^i$ with $b_i \in K$. Then

$$v_L(x) = \min_i\{i + ev_K(b_i)\}$$

as the elements $i + ev_K(b_i)$ all have distinct valuations. Now $x \in \mathcal{O}_L$ if and only if $v_L(x) \geq 0$ if and only if $v_K(b_i) \geq 0$ for all $i = 0, \ldots, e-1$. So $\mathcal{O}_L = \mathcal{O}_K[\pi]$.

Conversely, if $g(X) \in \mathcal{O}_K[X]$ is Eisenstein, let

$$L = K[X]/g(X) \cong K(\text{root of } g) = K(\alpha)$$

for some $\alpha \in L$. Then

$$\alpha \in L \implies \alpha \in \mathcal{O}_L$$

as $\mathcal{O}_L$ is integrally closed, and as $g \mod M = X^n$,

$$\alpha \in M_L$$

so $v_L(\alpha) > 0$. Consider

$$\alpha^n + \underbrace{a_{n-1}\alpha^{n-1} + \cdots + a_1\alpha}_{v_L(\cdot) > e_{L/K}} + \underbrace{a_0}_{v_L(\cdot) = e_{L/K}} = 0$$

so $v_L(\alpha^n) = e_{L/K}$, so $n = [L : K] \mid e_{L/K}$, but $e_{L/K} \mid n$. Thus $n = e_{L/K}$, L/K is totally ramified, and $v_L(\alpha) = 1$. $\square$

Chapter 13

Inertia Group and Higher Ramification

Suppose L/K is Galois, $G = \mathrm{Gal}(L/K)$. Let K' be the maximal unramified extension of K in L and recall K'/K is also Galois.

$$\begin{tikzcd}
L \arrow[d, dash, "\text{totally ramified}"'] \arrow[dd, dash, bend left=60, "G"] \\
K' \arrow[d, dash, "\text{unramified}"'] \\
K
\end{tikzcd}$$

We also have $\mathrm{Gal}(K'/K) = \mathrm{Gal}(k_L/k_K)$.

Definition. The *inertia group* $I = I_{L/K}$ is $\mathrm{Gal}(L/K')$. Equivalently,

$$\begin{aligned} I &= \{\sigma \in G : \sigma \text{ maps to } \iota \text{ in } \mathrm{Gal}(k_L/k_K)\} \\ &= \{\sigma \in G : \sigma x \equiv x \pmod{M}\ \forall x \in \mathcal{O}_L\} \end{aligned}$$

Note 9. $I \triangleleft G_{L/K}$, $e = |I|$.

Example. Let $K = \mathbb{Q}_2$, let $L = \mathbb{Q}_2(\sqrt[3]{2}, \zeta\sqrt[3]{2}, \zeta^2\sqrt[3]{2})$ be the splitting field of $X^3 - 2$, where $\{1, \zeta, \zeta^2\} = \mu_3$.

We have $[L : K] \le 3! = 6$. $\mu_3 \subset L$ so $k_L \supset \mathbb{F}_2(\mu_3) = \mathbb{F}_4$, so $f_{L/K} \ge 2$ and $2 \mid f_{L/K}$. $\sqrt[3]{2} \in L$ so $e_{L/K} \ge 3$ and $3 \mid e_{L/K}$. But now $[L : K] = f_{L/K} e_{L/K}$, so these are in fact equalities.

$$\begin{tikzcd}
L \arrow[d, dash, "3"'] \arrow[d, dash, bend right=60, "I=C_3"'] \arrow[dd, dash, bend left=60, "G=S_3"] \\
\mathbb{Q}_2(\mu_3) \arrow[d, dash, "2"'] \arrow[d, dash, bend right=60, "\mathrm{Gal}\,\mathbb{F}_4/\mathbb{F}_2 \cong C_2"'] \\
\mathbb{Q}_2
\end{tikzcd}$$

Note 10. $\sqrt[3]{2}$ is a uniformiser of L. $0, 1, \zeta, \zeta^2$ are representatives for $\mathcal{O}_L/M_L$.

$$\mathcal{O}_L = \{a_0 + a_1\sqrt[3]{2} + a_2\sqrt[3]{2}^2 + a_3 \cdot 2 + \cdots : a_i \in \{0, 1, \zeta, \zeta^2\}\}$$

is a free $\mathbb{Z}_2$-modulo of rank 6 with basis $1, \zeta, \sqrt[3]{2}, \zeta\sqrt[3]{2}, \sqrt[3]{2}^2, \zeta\sqrt[3]{2}^2$, and $\mathrm{Gal}(L/K)$ permutes the elements — this is not true in general.

$G = S_3$ is the set of permutations of $\{\sqrt[3]{2}, \zeta\sqrt[3]{2}, \zeta^2\sqrt[3]{2}\}$, i.e., the maps

$$\begin{aligned} \sqrt[3]{2} &\mapsto \{\sqrt[3]{2}, \zeta\sqrt[3]{2}, \zeta^2\sqrt[3]{2}\} \\ \zeta &\mapsto \{\zeta, \zeta^2\} \end{aligned}$$

$I = C_3$ is the set of even permutation, i.e., the maps

$$\begin{aligned} \sqrt[3]{2} &\mapsto \{\sqrt[3]{2}, \zeta\sqrt[3]{2}, \zeta^2\sqrt[3]{2}\} \\ \zeta &\mapsto \zeta \end{aligned}$$

Note 11. $\mathrm{Gal}(L/K) \to \mathrm{Gal}(k_L/k_K) = \mathrm{Gal}(\mathbb{F}_4/\mathbb{F}_2) = \{\iota, (\zeta \leftrightarrow \zeta^2)\}$. On

$$\mathcal{O}_L = \{a_0 + a_1\sqrt[3]{2} + a_2\sqrt[3]{2}^2 + a_3 \cdot 2 + \cdots : a_i \in \{0, 1, \zeta, \zeta^2\}\}$$

elements of $G \setminus I \cong S_3 \setminus C_3$ act non-trivially on a_0, and non-identity elements of C_3 act non-trivially on $\mathcal{O}_L/M_L^2$.

More generally, we let

$$G_i = \{\sigma \in G : \sigma x \equiv x \mod M_L^{i+1}\ \forall x \in \mathcal{O}_L\}$$

be the ith *ramification group*. Then

$$G \supset G_0 \supset G_1 \supset \cdots$$

and $G_0 = I_{L/K}$. In the example above,

$$S_3 = G \supset G_0 = C_3 \supset G_1 = \{\iota\} \supset G_2 = \{\iota\} \supset \cdots$$

Note that

$$G_i = \ker\bigl(G \hookrightarrow \mathrm{Aut}\,\mathcal{O}_L \to \mathrm{Aut}\,\mathcal{O}_L/(\pi_L)^{i+1}\bigr)$$

so that G_i is normal in G for all $i \geq 0$.

Theorem 13.1. Let L/K be Galois, $\pi = \pi_L$ be a uniformiser, $v = v_L$ be normalised and $G = \mathrm{Gal}(L/K)$.

(i) For $\sigma \in I$, $\sigma \in G_n$ if and only if $v(\pi - \sigma\pi) > n$.
(ii) $\bigcap_{n \geq 0} G_n = \{\iota\}$.
(iii) If we write, for $\sigma \in G_n$,

$$\begin{aligned} \sigma\pi &= \alpha_\sigma \pi && n = 0 \\ \sigma\pi &= \pi + \alpha_\sigma \pi^{n+1} && n \geq 1 \end{aligned}$$

then $\sigma \mapsto \bar{\alpha}_\sigma = \alpha_\sigma \mod M$ defines an embedding

$$\begin{aligned} G_0/G_1 &\hookrightarrow k_L^* && n = 0 \\ G_n/G_{n+1} &\hookrightarrow (k_L, +) && n \geq 1 \end{aligned}$$

(iv) If $\mathrm{char}(k_K) = p$ then G is the unique p-Sylow subgroup of $I = G_0$. If $\mathrm{char}(k_K) = 0$ then $G_1 = \{\iota\}$.

Proof. Replacing K by K', the maximal unramified extension in L, we may assume that L/K is totally ramified and $I = G$.

(i) The 'if' direction is clear by definition. For the 'only if' direction, recall that $\mathcal{O}_L = \mathcal{O}_K[\pi]$.

(ii) If $\sigma \neq \iota$ then $\sigma\pi \neq \pi$ because $L = K(\pi)$, hence $\sigma \notin G_n$ for sufficiently large n.

(iii) Let $n = 0$ and take $\sigma, \tau \in G_0 = I = G$. Writing

$$\sigma\pi = \alpha_\sigma \pi, \tau\pi = \alpha_\tau \pi$$

we see that

$$(\sigma\tau)\pi = \sigma\tau\pi = \sigma\alpha_\tau\pi = (\sigma\alpha_\tau)\alpha_\sigma\pi \equiv \alpha_\sigma\alpha_\tau\pi \pmod{\pi^2}$$

as $\sigma\alpha_\tau \equiv \alpha_\tau \pmod{\pi}$ for $\sigma \in I$. So $\sigma \mapsto \bar{\alpha}_\sigma$ is a group homomorphism $G_0 \to k_L^*$. Clearly, $\ker(\sigma \mapsto \bar{\alpha}_\sigma) = G_1$ by part (i).
Now let $n \geq 1$. Similarly,

$$\begin{aligned}
(\sigma\tau)\pi &= \sigma(\pi + \alpha_\tau \pi^{n+1}) \\
&= \sigma(\pi(1 + \alpha_\tau\pi^n)) \\
&= (\pi + \alpha_\sigma\pi^{n+1})(1 + \underbrace{\sigma(\alpha_\tau\pi^n)}_{\equiv \alpha_\tau\pi^n \mod \pi^{n+1}}) \\
&\equiv (\pi + \alpha_\sigma\pi^{n+1})(1 + \alpha_\tau\pi^n) \pmod{\pi^{n+2}} \\
&\equiv \pi + (\alpha_\sigma + \alpha_\tau)\pi^{n+1} \pmod{\pi^{n+2}}
\end{aligned}$$

so here $G_n \to (k_L, +)$ via $\sigma \mapsto \bar{\alpha}_\sigma$ and by part (i) the kernel is G_{n+1}.

(iv) If $\mathrm{char}(k_L) = 0$ then $(k_L, +)$ has no finite subgroup, so for all $n > 0$, $G_n/G_{n+1} = \{\iota\}$, and hence $G_1 = \{\iota\}$.
If $\mathrm{char}(k_L) = p$ then

$$G_n/G_{n+1} \hookrightarrow (k_L, +)$$

is a $\mathbb{F}_p$-vector space. Thus G_1 is a p-group.
$G_1 \triangleleft G_0 = G$, G_1 is a p-group. By part (iii),

$$G_0/G_1 \hookrightarrow k_L^*$$

But k_L is a field of characteristic p so has no elements of order p, so G_0/G_1 has order coprime to p. It follows that $G_1 \triangleleft G_0$ is its p-Sylow subgroup, and $G_1 \triangleleft G_0$ is normal hence unique. $\square$

Definition. G_1 is the *wild interia group.* G_0/G_1 is the *tame inertia group.* L/K is *tamely ramified* if $G_1 = \{\iota\}$ and *wildly ramified* otherwise.

We have the following picture for $\mathrm{char}(k_K) = p$.

$$
\begin{array}{ccc}
\{\iota\} & & L \\
| & & | \\
\vdots & & \vdots \\
| & & | \\
G_2 & & K''' \\
| & & | \\
G_1 & & K'' \\
| & & | \\
I = G_0 & & K' \\
| & & | \\
G & & K
\end{array}
$$

where

- K/K' is maximal unramified, $\mathrm{Gal}(K'/K) = G/G_0 = \mathrm{Gal}(k_L/k_K)$ and this is cyclic if K is local.
- Further, K'/K'' is totally tamely ramified, $\mathrm{Gal}(K''/K') \hookrightarrow k_L^*$, which is the tame inertia group, cyclic of order coprime to p.
- Finally, L/K'' is totally widly ramified, $\mathrm{Gal}(L/K'')$ is the wild inertia group; it is a p-group and quite complicated in general.

Corollary 13.2. G_n/G_{n+1} is abelian for all $n \geq 0$.

Corollary 13.3. I is soluble. If L/K is local then $\mathrm{Gal}(L/K)$ is soluble.

Corollary 13.4. If $\mathrm{char}(k_K) = 0$, e.g., $K = \mathbb{Q}((t))$ or $\mathbb{C}((t))$, then every extension of K is tamely ramified.

13.1 Structure of Tamely Ramified Extensions

Lemma 13.5. Let L/K be Galois, totally and tamely ramified of degree n. Then

(i) $\mu_n \subset K$ since $C_n \cong \mathrm{Gal}(L/K) \hookrightarrow k_K^*$;
(ii) there exists a uniformiser π of K such that $L = K(\sqrt[n]{\pi})$, which follows from Kummer's theorem.

Proof. Exercise. □

Example (S_3-Extensions of $\mathbb{Q}((t))$)**.** Let $K = \mathbb{Q}((t))$. We describe all Galois extensions L of K with $\mathrm{Gal}(L/K) \cong S_3$. Let $\pi_K = t$, a uniformiser of K, and $k_K = \mathbb{Q}$. Recall that this is perfect as it has characteristic 0. Let $k_L = F$, some number field.

Case 1. Suppose L/K is unramified. Then $L = F((t))$ for some S_3-extensions $F/\mathbb{Q}$.

Case 2. Suppose L/K is ramified. $I \triangleleft S_3$, $I \neq \{\iota\}$ and I is cyclic (cf. tame inertia). Thus $I = C_3$ and

$$G/I \cong C_2 \cong \mathrm{Gal}(F/\mathbb{Q})$$

and

$$\begin{tikzcd} L \arrow[d, dash, "3"', "\text{totally ramified}"] \\ K' = F((t)) \arrow[d, dash, "2"', "\text{unramified}"] \\ K = \mathbb{Q}((t)) \end{tikzcd}$$

with $[F : \mathbb{Q}] = 2$.

L/K' is Galois, totally and tamely ramified so, by the previous lemma, $\mu_3 \subset \mathbb{F}^*$ and hence $F = \mathbb{Q}(\mu_3) = \mathbb{Q}(\sqrt{-3})$ as this is the only quadratic extension of $\mathbb{Q}$ containing the cube roots of unity.

By the lemma,

$$L = K'(\sqrt[3]{f})$$

for some $f \in \mathbb{Q}(\mu_3)[[t]]$ of the form $f = ct + O(t^2) = ct(1 + \cdots)$. $1 + O(t)$ is a cube in K'. To see this, either apply Hensel's Lemma or write $(1 + \cdots)^{1/3} := \sum_{n=0}^{\infty} \binom{1/3}{n} (\cdots)^n$. So in fact

$$L = \mathbb{Q}(\mu_3)((t))(\sqrt[3]{ct})$$

for some $c \in \mathbb{Q}(\mu_3)$.

Exercise 10. By considering $\sqrt[3]{\tilde{c}t} \in L$, $c = \alpha + \beta\sqrt{-3}$, $\tilde{c} = \alpha - \beta\sqrt{-3}$ prove that in fact $L = K'(\sqrt[3]{ct})$ with $c \in \mathbb{Q}$.

This gives as the final answer that the S_3-extensions of $K = \mathbb{Q}((t))$ are

(i) $F((t))$ with $F/\mathbb{Q}$ an S_3-extension;
(ii) $\mathbb{Q}(\mu_3)((t))(\sqrt[3]{ct})$, $c \in \mathbb{Q}$, i.e., splitting fields for $X^3 - ct$ over K.