Part III — Local Fields

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

What are local fields? Suppose we are interested in some basic number theoretic problem. Say we have a polynomial $f(x_1, \cdots, x_n) \in \mathbb{Z}[x_1, \cdots, x_n]$. We want to look for solutions $\mathbf{a} \in \mathbb{Z}^n$, or show that there are no solutions at all. We might try to view this polynomial as a real polynomial, look at its roots, and see if they are integers. In lucky cases, we might be able to show that there are no real solutions at all, and conclude that there cannot be any solutions at all.

On the other hand, we can try to look at it modulo some prime p. If there are no solutions mod p, then there cannot be any solution. But sometimes p is not enough. We might want to look at it mod p^2, or p^3, or .... One important application of local fields is that we can package all these information together. In this course, we are not going to study the number theoretic problems, but just look at the properties of the local fields for their own sake.

Throughout this course, all rings will be commutative with unity, unless otherwise specified.

1 Basic theory

We are going to start by making loads of definitions, which you may or may not have seen before.

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.

Example. The rationals, reals and complex numbers with the usual absolute values are absolute values.

Example (Trivial absolute value)**.** The *trivial absolute value* on a field K is the absolute value given by

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

The only reason why we mention the trivial absolute value here is that from now on, we will assume that the absolute values are *not* trivial, because trivial absolute values are boring and break things.

There are some familiar basic properties of the absolute value such as

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

An absolute value defines a metric $d(x, y) = |x - y|$ on K.

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.

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

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

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

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

Proof. Exercise □

Exercise. Let K be a valued field. Then equivalent absolute values induce the same the *completion* $\hat{K}$ of K, and $\hat{K}$ is a valued field with an absolute value extending $|\cdot|$.

In this course, we are not going to be interested in the usual absolute values. Instead, we are going to consider some really weird ones, namely *non-archimedean* ones.

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*.

Metrics satisfying $d(x,z) \leq \max(d(x,y), d(y,z))$ are often known as *ultrametrics*.

Example. $\mathbb{Q}$, $\mathbb{R}$ and $\mathbb{C}$ under the usual absolute values are archimedean.

In this course, we will only consider non-archimedean absolute values. Thus, from now on, unless otherwise mentioned, an absolute value is assumed to be non-archimedean. The metric is weird!

We start by proving some absurd properties of non-archimedean absolute values.

Recall that the closed balls are defined by

$$B(x,r) = \{y : |x-y| \leq r\}.$$

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

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

So closed balls do not have unique "centers". Every point can be viewed as the center.

Proof. Let $y \in B(z,r)$. Then

$$|x-y| = |(x-z)+(z-y)| \leq \max(|x-z|, |z-y|) \leq r.$$

So $y \in B(x,r)$. By symmetry, $y \in B(x,r)$ implies $y \in B(z,r)$. □

Corollary. Closed balls are open.

Proof. To show that $B(x,r)$ is open, we let $z \in B(x,r)$. Then we have

$$\{y : |y-z| < r\} \subseteq B(z,r) = B(x,r).$$

So we know the open ball of radius r around z is contained in $B(x,r)$. So $B(x,r)$ is open. □

Norms in non-archimedean valued fields are easy to compute:

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

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

Proof. On the one hand, we have $|x + y| \leq \max\{|x|, |y|\}$. On the other hand, we have

$$|x| = |(x + y) - y| \leq \max(|x + y|, |y|) = |x + y|,$$

since we know that we cannot have $|x| \leq |y|$. So we must have $|x| = |x + y|$. □

Convergence is also easy for valued fields.

Proposition. Let K be a valued field.

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

If we assume further that K is complete, then

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

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

The converses to all these are of course also true, with the usual proofs.

Proof.

(i) Pick $\varepsilon > 0$ and N such that $|x_n - x_{n+1}| < \varepsilon$ for all $n \geq N$. Then given $m \geq n \geq N$, we have

$$\begin{aligned} |x_m - x_n| &= |x_m - x_{m-1} + x_{m-1} - x_{m-2} + \cdots - x_n| \\ &\leq \max(|x_m - x_{m-1}|, \cdots, |x_{n+1} - x_n|) \\ &< \varepsilon. \end{aligned}$$

So the sequence is Cauchy.

(ii) Follows from (1) and the definition of completeness.

(iii) Follows from the definition of convergence of a series and (2).

□

The reason why we care about these weird non-archimedean fields is that they have very rich *algebraic* structure. In particular, there is this notion of the *valuation ring*.

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

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

We prove that it is actually a ring

Proposition. Let K be a valued field. Then

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

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

Note that this is very false for usual absolute values. For example, if we take $\mathbb{R}$ with the usual absolute value, we have $1 \in \mathcal{O}_\mathbb{R}$, but $1 + 1 \notin \mathcal{O}_R$.

Proof. We know that these sets are open since all balls are open.

To see $\mathcal{O}_K$ is a subring, we have $|1| = |-1| = 1$. So $1, -1 \in \mathcal{O}_K$. If $x, y \in \mathcal{O}_K$, then $|x + y| \leq \max(|x|, |y|) \leq 1$. So $x + y \in \mathcal{O}_K$. Also, $|xy| = |x||y| \leq 1 \cdot 1 = 1$. So $xy \in \mathcal{O}_K$.

That the other sets are ideals of $\mathcal{O}_K$ is checked in the same way.

To check the units, we have $x \in \mathcal{O}_K^\times \Leftrightarrow |x|, |x^{-1}| \leq 1 \Leftrightarrow |x| = |x|^{-1} = 1$. □

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 $f(s) = 0$.

Example. Any $r \in R$ is integral (take $f(x) = x - r$).

Example. Take $\mathbb{Z} \subseteq \mathbb{C}$. Then $z \in \mathbb{C}$ is integral over $\mathbb{Z}$ if it is an *algebraic integer* (by definition of algebraic integer). For example, $\sqrt{2}$ is an algebraic integer, but $\frac{1}{\sqrt{2}}$ is not.

We would like to prove the following characterization of integral elements:

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

Note that $R[s_1, \cdots, s_n]$ is by definition a finitely-generated R-algebra, but requiring it to be finitely-generated as a module is stronger.

Here one direction is easy. It is not hard to show that if $s_1, \cdots, s_n$ are all integral, then $R[s_1, \cdots, s_n]$ is finitely-generated. However to show the other direction, we need to find some clever trick to produce a *monic* polynomial that kills the s_i.

The trick we need is the adjugate matrix we know and love from IA Vectors and Matrices.

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.

As we know from IA, the following property holds for the adjugate matrix:

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

With this, we can prove our claim:

Proof of theorem. Note that we can construct $R[s_1, \cdots, s_n]$ by a sequence

$$R \subseteq R[s_1] \subseteq R[s_1, s_2] \subseteq \cdots \subseteq R[s_1, \cdots, s_n] \subseteq S,$$

and each s_i is integral over $R[s_1, \cdots, s_{n-1}]$. Since the finite extension of a finite extension is still finite, it suffices to prove it for the case $n = 1$, and we write s for s_1.

Suppose $f(x) \in R[x]$ is monic such that $f(s) = 0$. If $g(x) \in R[x]$, then there is some $q, r \in R[x]$ such that $g(x) = f(x)q(x) + r(x)$ with $\deg r < \deg f$. Then $g(s) = r(s)$. So any polynomial expression in s can be written as a polynomial expression with degree less than $\deg f$. So $R[s]$ is generated by $1, s, \cdots, s^{\deg f - 1}$.

In the other direction, let $t_1, \cdots, t_d$ be R-module generators of $R[s_1, \cdots, s_n]$. We show that in fact any element of $R[s_1, \cdots, s_n]$ is integral over R. Consider any element $b \in R[s_1, \cdots, s_n]$. Then there is some $a_{ij} \in R$ such that

$$bt_i = \sum_{j=1}^{d} a_{ij} t_j.$$

In matrix form, this says

$$(bI - A)t = 0.$$

We now multiply by $(bI - A)^*$ to obtain

$$\det(bI - A)t_j = 0$$

for all j. Now we know $1 \in R$. So $1 = \sum c_j t_j$ for some $c_j \in R$. Then we have

$$\det(bI - A) = \det(bI - A) \sum c_j t_j = \sum c_j (\det(bI - A)t_j) = 0.$$

Since $\det(bI - A)$ is a monic polynomial in b, it follows that b is integral. □

Using this characterization, the following result is obvious:

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

Proof. If s_1, s_2 are integral, then $R[s_1, s_2]$ is a finite extension over R. Since $s_1 + s_2$ and $s_1 s_2$ are elements of $R[s_1, s_2]$, they are also integral over R. □

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

Recall that we previously constructed the valuation ring $\mathcal{O}_K$. Since the valued field K itself has a topology, the valuation ring inherits a subspace topology. This is in fact a ring topology.

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*.

Example. $\mathbb{R}$ and $\mathbb{C}$ with the usual topologies and usual ring structures are topological rings.

Exercise. Let K be a valued field. Then K is a topological ring. We can see this from the fact that the product topology on $K \times K$ is induced by the metric $d((x_0, y_0), (x_1, y_1)) = \max(|x_0 - x_1|, |y_0 - y_1|)$.

Now if we are just randomly given a ring, there is a general way of constructing a ring topology. The idea is that we pick an ideal I and declare its elements to be small. For example, in a valued ring, we can pick $I = \{x \in \mathcal{O}_K : |x| < 1\}$. Now if you are not only in I, but I^2, then you are even smaller. So we have a hierarchy of small sets

$$I \supseteq I^2 \supseteq I^3 \supseteq I^4 \supseteq \cdots$$

Now to make this a topology on R, we say that a subset $U \subseteq R$ is open if every $x \in U$ is contained in some translation of I^n (for some n). In other words, we need some $y \in R$ such that

$$x \in y + I^n \subseteq U.$$

But since I^n is additively closed, this is equivalent to saying $x + I^n \subseteq U$. So we make the following definition:

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 $x + I^n \subseteq U$.

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

Note that the I-adic topology isn't really the kind of topology we are used to thinking about, just like the topology on a valued field is also very weird. Instead, it is a "filter" for telling us how small things are.

Proof. By definition, we have $\emptyset$ and R are open, and arbitrary unions are clearly open. If U, V are I-adically open, and $x \in U \cap V$, then there are n, m such that $x + I^n \subseteq U$ and $x + I^m \subseteq V$. Then $x + I^{\max(m,n)} \subseteq U \cap V$. □

Exercise. Check that the I-adic topology is a ring topology.

In the special case where $I = xR$, we often call the I-adic topology the *x-adic topology*.

Now we want to tackle the notion of completeness. We will consider the case of $I = xR$ for motivation, but the actual definition will be completely general.

If we pick the x-adic topology, then we are essentially declaring that we take x to be small. So intuitively, we would expect power series like

$$a_0 + a_1 x + a_2 x^2 + a_3 x^3 + \cdots$$

to "converge", at least if the a_i are "of bounded size". In general, the a_i are "not too big" if $a_i x^i$ is genuinely a member of $x^i R$, as opposed to some silly thing like x^{-i}.

As in the case of analysis, we would like to think of these infinite series as a sequence of partial sums

$$(a_0,\ a_0 + a_1 x,\ a_0 + a_1 x + a_2 x^2,\ \cdots)$$

Now if we denote the limit as L, then we can think of this sequence alternatively as

$$(L \bmod I,\ L \bmod I^2,\ L \bmod I^3,\ \cdots).$$

The key property of this sequence is that if we take $L \bmod I^k$ and reduce it mod I^{k-1}, then we obtain $L \bmod I^{k-1}$.

In general, suppose we have a sequence

$$(b_n \in R/I^n)_{n=1}^{\infty}.$$

such that $b_n \bmod I^{n-1} = b_{n-1}$. Then we want to say that the ring is *I-adically complete* if every sequence satisfying this property is actually of the form

$$(L \bmod I,\ L \bmod I^2,\ L \bmod I^3,\ \cdots)$$

for some L. Alternatively, we can take the *I-adic completion* to be the collection of all such sequences, and then a space is I-adically complete it is isomorphic to its I-adic completion.

To do this, we need to build up some technical machinery. The kind of sequences we've just mentioned is a special case of an inverse limit.

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*.

Proposition. The inverse limit topology is a ring topology.

Proof sketch. We can fit the addition and multiplication maps into diagrams

$$\begin{array}{ccc} \varprojlim R_n \times \varprojlim R_n & \longrightarrow & \varprojlim R_n \\ \uparrow & & \uparrow \\ \prod R_n \times \prod R_n & \longrightarrow & \prod R_n \end{array}$$

By the definition of the subspace topology, it suffices to show that the corresponding maps on $\prod R_n$ are continuous. By the universal property of the product, it suffices to show that the projects $\prod R_n \times \prod R_n \to R_m$ is continuous for all m. But this map can alternatively be obtained by first projecting to R_m, then doing multiplication in R_m, and projection is continuous. So the result follows. □

It is easy to see the following universal property of the inverse limit topology:

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

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

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.

Exercise. If ν is a bijection, then ν is in fact a homeomorphism.

1.4 The p-adic numbers

For the rest of this course, p is going to be a prime number.

We consider a particular case of valued fields, namely the p-adic numbers, and study some of its basic properties.

Let $x \in \mathbb{Q}$ be non-zero. Then by uniqueness of factorization, we can write x uniquely as

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

where $a, b, n \in \mathbb{Z}$, $b > 0$ and a, b, p are pairwise coprime.

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

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

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

Proof. It is clear that $|x|_p = 0$ iff $x = 0$.

Suppose we have

$$x = p^n \frac{a}{b}, \quad y = p^m \frac{c}{d}.$$

We wlog $m \geq n$. Then we have

$$|xy|_p = \left|p^{n+m} \frac{ac}{bd}\right| = p^{-m-n} = |x|_p |y|_p.$$

So this is multiplicative. Finally, we have

$$|x + y|_p = \left|p^n \frac{ab + p^{m-n} cb}{bd}\right| \leq p^{-n} = \max(|x|_p, |y|_p).$$

Note that we must have bd coprime to p, but $ab + p^{m-n} cb$ need not be. However, any extra powers of p could only decrease the absolute value, hence the above result. □

Note that if $x \in \mathbb{Z}$ is an integer, then $|x|_p = p^{-n}$ iff $p^n \mid\mid x$ (we say $p^n \mid\mid x$ if $p^n \mid x$ and $p^{n+1} \nmid x$).

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*.

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

Proof. If $x \in \mathbb{Z}$ is non-zero, then $x = p^n a$ with $n \geq 0$. So $|x|_p \leq 1$. So $\mathbb{Z} \subseteq \mathbb{Z}_p$.

We now want to show that $\mathbb{Z}$ is dense in $\mathbb{Z}_p$. We know the set

$$\mathbb{Z}_{(p)} = \{x \in \mathbb{Q} : |x|_p \leq 1\}$$

is dense inside $\mathbb{Z}_p$, essentially by definition. So it suffices to show that $\mathbb{Z}$ is dense in $\mathbb{Z}_{(p)}$. We let $x \in \mathbb{Z}_{(p)} \setminus \{0\}$, say

$$x = p^n \frac{a}{b}, \quad n \geq 0.$$

It suffices to find $x_i \in \mathbb{Z}$ such that $x_i \to \frac{1}{b}$. Then we have $p^n a x_i \to x$.

Since $(b, p) = 1$, we can find $x_i, y_i \in \mathbb{Z}$ such that $bx_i + p^i y_i = 1$ for all $i \geq 1$. So

$$\left|x_i - \frac{1}{b}\right|_p = \left|\frac{1}{b}\right|_p |bx_i - 1|_p = |p^i y_i|_p \leq p^{-i} \to 0.$$

So done. □

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

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

Proof. Let $0 \neq I \subseteq \mathbb{Z}_p$ be an ideal, and pick $x \in I$ such that $|x|_p$ is maximal. This supremum exists and is attained because the possible values of the absolute values are discrete and bounded above. If $y \in I$, then by maximality, we have $|y|_p \leq |x|_p$. So we have $|yx^{-1}|_p \leq 1$. So $yx^{-1} \in \mathbb{Z}_p$, and this implies that $y = (yx^{-1})x \in x\mathbb{Z}_p$. So $I \subseteq x\mathbb{Z}_p$, and we obviously have $x\mathbb{Z}_p \subseteq I$. So we have $I = x\mathbb{Z}_p$.

Now if $x = p^n \frac{a}{b}$, then since $\frac{a}{b}$ is invertible in $\mathbb{Z}_p$, we have $x\mathbb{Z}_p = p^n\mathbb{Z}_p$. So $I = p^n\mathbb{Z}_p$.

To show the second part, consider the map

$$f_n : \mathbb{Z} \to \frac{\mathbb{Z}_p}{p^n\mathbb{Z}_p}$$

given by the inclusion map followed by quotienting. Now $p^n\mathbb{Z}_p = \{x : |x|_p \leq p^{-n}$. So we have

$$\ker f_n = \{x \in \mathbb{Z} : |x|_p \leq p^{-n}\} = p^n\mathbb{Z}.$$

Now since $\mathbb{Z}$ is dense in $\mathbb{Z}_p$, we know the image of f_n is dense in $\mathbb{Z}_p/p^n\mathbb{Z}_p$. But $\mathbb{Z}_p/p^n\mathbb{Z}_p$ has the discrete topology. So f_n is surjective. So f_n induces an isomorphism $\mathbb{Z}/p^n Z \cong \mathbb{Z}_p/p^n\mathbb{Z}_p$. □

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

This is pretty much the point of the p-adic numbers — there are a lot of primes in $\mathbb{Z}$, and by passing on to $\mathbb{Z}_p$, we are left with just one of them.

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

Proof. Let $U \subseteq \mathbb{Z}$. By definition, U is open wrt $|\cdot|_p$ iff for all $x \in U$, there is an $n \in \mathbb{N}$ such that

$$\{y \in \mathbb{Z} : |y - x|_p \leq p^{-n}\} \subseteq U.$$

On the other hand, U is open in the p-adic topology iff for all $x \in U$, there is some $n \geq 0$ such that $x + p^n\mathbb{Z} \subseteq U$. But we have

$$\{y \in \mathbb{Z} : |y - x|_p \leq p^{-n}\} = x + p^n\mathbb{Z}.$$

So done. □

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

Proof. The second part follows from the first as follows: we have the maps

$$\mathbb{Z}_p \xrightarrow{\nu} \varprojlim \mathbb{Z}_p/(p^n\mathbb{Z}_p) \xleftarrow{(f_n)_n} \varprojlim \mathbb{Z}/(p^n\mathbb{Z})$$

We know the map induced by $(f_n)_n$ is an isomorphism. So we just have to show that ν is an isomorphism

To prove the first part, we have $x \in \ker \nu$ iff $x \in p^n\mathbb{Z}_p$ for all n iff $|x|_p \leq p^{-n}$ for all n iff $|x|_p = 0$ iff $x = 0$. So the map is injective.

To show surjectivity, we let

$$z_n \in \varprojlim \mathbb{Z}_p/p^n\mathbb{Z}_p.$$

We define $a_i \in \{0, 1, \cdots, p-1\}$ recursively such that

$$x_n = \sum_{i=0}^{n-1} a_i p^i$$

is the unique representative of z_n in the set of integers $\{0, 1, \cdots, p^n - 1\}$. Then

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

exists in $\mathbb{Z}_p$ and maps to $x \equiv x_n \equiv z_n \pmod{p^n}$ for all $n \geq 0$. So $\nu(x) = (z_n)$. So the map is surjective. So ν is bijective. □

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

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

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

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

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

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

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

Proof. The second part follows from the first part by multiplying a by p^{-n}. □

Example. We have

$$\frac{1}{1-p} = 1 + p + p^2 + p^3 + \cdots.$$

2 Valued fields

2.1 Hensel's lemma

We return to the discussion of general valued fields. We are now going to introduce an alternative to the absolute value that contains the same information, but is presented differently.

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

Here we use the conventions that $r + \infty = \infty$ and $r \leq \infty$ for all $r \in \infty$.

In some sense, this definition is sort-of pointless, since if v is a valuation, then the function

$$|x| = c^{-v(x)}$$

for any $c > 1$ is a (non-archimedean) absolute value. Conversely, if $|\cdot|$ is a valuation, then

$$v(x) = -\log_c |x|$$

is a valuation.

Despite this, sometimes people prefer to talk about the valuation rather than the absolute value, and often this is more natural. As we will later see, in certain cases, there is a canonical normalization of v, but there is no canonical choice for the absolute value.

Example. For $x \in \mathbb{Q}_p$, we define

$$v_p(x) = -\log_p |x|_p.$$

This is a valuation, and if $x \in \mathbb{Z}_p$, then $v_p(x) = n$ iff $p^n \mid\mid x$.

Example. Let K be a field, and define

$$k((T)) = \left\{ \sum_{i=n}^{\infty} a_i T^i : a_i \in k, n \in \mathbb{Z} \right\}.$$

This is the field of *formal Laurent series* over k. We define

$$v\left(\sum a_i T^i\right) = \min\{i : a_i \neq 0\}.$$

Then v is a valuation of $k((T))$.

Recall that for a valued field K, the *valuation ring* is given by

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

Since this is a subring of a field, and the absolute value is multiplicative, we notice that the units in $\mathcal{O}$ are exactly the elements of absolute value 1. The

remaining elements form an ideal (since the field is non-archimedean), and thus we have a *maximal ideal*

$$\mathfrak{m} = \mathfrak{m}_K = \{x \in K : |x| < 1\}$$

The quotient

$$k = k_K = \mathcal{O}_K/\mathfrak{m}_K$$

is known as the *residue field*.

Example. Let $K = \mathbb{Q}_p$. Then $\mathcal{O} = \mathbb{Z}_p$, and $\mathfrak{m} = p\mathbb{Z}_p$. So

$$k = \mathcal{O}/\mathfrak{m} = \mathbb{Z}_p/p\mathbb{Z}_p \cong \mathbb{Z}/p\mathbb{Z}.$$

Definition (Primitive polynomial)**.** If K is a valued field and $F(x) = a_0 + a_1x + \cdots + a_nx^n \in K[x]$ is a polynomial, we say that F is *primitive* if

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

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

The point of a primitive polynomial is that such a polynomial is naturally, and non-trivially, an element of $k[x]$. Moreover, focusing on such polynomials is not that much of a restriction, since any polynomial is a constant multiple of a primitive polynomial.

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

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

with $(g, h) = 1$, then there is a factorization

$$F(x) = G(x)H(x)$$

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

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

with $\deg g = \deg G$.

Note that requiring $\deg g = \deg G$ is the best we can hope for — we cannot guarantee $\deg h = \deg H$, since we need not have $\deg f = \deg F$.

This is one of the most important results in the course. Unfortunately, the proof is not terribly enlightening.

Proof. Put $d = \deg F$ and $m = \deg g$. Then we have $\deg h \leq d - m$.

We pick lifts $G_0, H_0 \in \mathcal{O}[x]$ of g, h with $\deg G_0 = \deg g$, and $\deg H_0 \leq d - m$. Then we have

$$F = G_0H_0 \mod \mathfrak{m}.$$

Our strategy is to add some correction terms to G_0 and H_0 so that the corresponding equation holds mod $\mathfrak{m}^2$, then lift to a result mod $\mathfrak{m}^3$ etc, ... and hopefully eventually get something in the limit.

However, this doesn't really work, since there is no guarantee that the limit converges! The trick is to pick and element $\pi \in \mathfrak{m}$, and then work modulo π^k. This is not hard, since we notice that

$$\pi\mathcal{O} = \{x \in \mathcal{O} : |x| \leq |\pi|\}.$$

Since our equations only have finitely many coefficients, we can always replace $\mathrm{mod}\mathfrak{m}$ with $\mathrm{mod}\pi$ for large enough π.

If we do this, then the correction terms we add in each iteration will be bounded by $|\pi|^k$, and thus tends to 0. Now recall that a series converges iff the moduli of the terms tend to 0! So we are done if this works.

Before we begin, we use the given condition $(g, h) = 1$ to obtain some $A, B \in \mathcal{O}[x]$ such that

$$AG_0 + BH_0 \equiv 1 \mod \mathfrak{m}.$$

Then we know that

$$F - G_0H_0 \equiv AG_0 + BH_0 - 1 \equiv 0 \mod \mathfrak{m}.$$

Thus, since the polynomials involved have finitely many coefficients, we can pick pick a $\pi \in \mathfrak{m}$ with large enough modulus such that

$$F - G_0H_0 \equiv AG_0 + BH_0 - 1 \equiv 0 \mod \pi.$$

The idea is to find successive approximations

$$\begin{aligned} G_{n-1} &= G_0 + \pi P_1 + \cdots + \pi^{n-1}P_{n-1},\\ H_{n-1} &= H_0 + \pi Q_1 + \cdots + \pi^{n-1}Q_{n-1}. \end{aligned}$$

that satisfy

$$F \equiv G_{n-1}H_{n-1} \mod \pi^n.$$

We then set

$$\begin{aligned} G &= G_0 + \pi P_1 + \pi^2 P_2 + \cdots,\\ H &= H_0 + \pi Q_1 + \pi^2 Q_2 + \cdots. \end{aligned}$$

We then have $G \equiv G_i \mod \pi^{i+1}$, and similarly for H. So we have

$$F \equiv GH \mod \pi^n$$

for all n. As $|\pi^n| \to 0$ as $n \to \infty$, we must have $F = GH$.

We proceed by induction. Assume we already have G_{n-1}, H_{n-1}. We need to find P_n, Q_n such that

$$\begin{aligned} G_n &= G_{n-1} + \pi^n P_n\\ H_n &= H_{n-1} - \pi^n Q_n \end{aligned}$$

satisfy

$$F - G_nH_n = 0 \mod \pi^{n+1}.$$

Expanding G_n and H_n out, we get

$$F - G_{n-1}H_{n-1} \equiv \pi^n(G_{m-1}Q_n + H_{n-1}P_n) \mod \pi^{n+1}.$$

We rearrange and divide by π^n to obtain

$$G_{n-1}Q_n + H_{n-1}P_n \equiv \frac{1}{\pi^n}(F - G_{n-1}H_{n-1}) \mod \pi.$$

However, note that $G_{n-1} = G_0 \mod \pi$ (and similarly for H), so we have

$$G_0Q_n + H_0P_n \equiv \frac{1}{\pi^n}(F - G_{n-1}H_{n-1}) \mod \pi.$$

Note that this division makes sense since by assumption, $F - G_{n-1}H_{n-1}$ is a multiple of π^n.

We write

$$E_n = \frac{1}{\pi^n}(F - G_{n-1}H_{n-1}).$$

Now recall that there are A, B such that

$$AG_0 + BH_0 \equiv 1 \mod \pi.$$

Multiplying by E_n thus gives

$$E_n \equiv AG_0E_n + BH_0E_n \mod \pi.$$

We might be tempted to set Q_n and P_n to be just AE_n and BE_n respectively, but we must control the degree of P_n appropriately. Its degree must be less than $\deg g = \deg G_0$.

Fortunately, the division algorithm comes to the rescue. Recall that G_0 is the lift of g of the same degree, and thus its leading coefficient must be an element of $\mathcal{O} \setminus \mathfrak{m}$, i.e. a unit. So we can perform the division algorithm to write

$$BF_n = QG_0 + P_n.$$

with $\deg P_n < \deg G_0$. This gives the desired P_n. Then we have

$$G_0(AE_n + H_0Q) + H_0P_n \equiv E_n \mod \pi.$$

Finally, let $Q_n = AE_n + H_0Q$, where we drop all coefficients divisible by π. Then since $\deg E_n, \deg H_0P_n \leq \deg F = m$, we must have $\deg Q_n \leq m - \deg G_0 = m - d$. So this has the desired degree as well. So done. □

Corollary. Let $F(x) = a_0 + a_1x + \cdots + a_nx^n \in K[x]$ where K is complete and $a_0, a_n \neq 0$. If F is irreducible, then

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

for all ℓ.

Proof. By scaling, we can wlog F is primitive. Let r be minimal such that $|a_r| = 1$. Then we have

$$F(x) \equiv x^r(a_r + a_{r+1}x + \cdots + a_nx^{n-r}) \mod \mathfrak{m}.$$

We want to prove that $\max(|a_0|, |a_n|) = 1$. If not, then $0 < r < n$, and thus congruence lifts to a non-trivial factorization of F by Hensel's lemma. □

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

Example. Consider $x^{p-1} - 1 \in \mathbb{Z}_p[x]$. We know x^{p-1} splits into distinct linear factors over $\mathbb{F}_p[x]$. So all roots lift to $\mathbb{Z}_p$. So $x^{p-1} - 1$ splits completely in $\mathbb{Z}_p$. So $\mathbb{Z}_p$ contains all p roots of unity.

Example. Since 2 is a quadratic residue mod 7, we know $\sqrt{2} \in \mathbb{Q}_7$.

2.2 Extension of norms

The main goal of this section is to prove the following theorem:

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

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

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

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

This is since any algebraic extension is the union of finite extensions, and uniqueness means we can patch the absolute values together.

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

Proof. We check that $\alpha \mapsto |\sigma(\alpha)|_L$ is also an absolute value on L extending the absolute value on K. So the result follows from uniqueness. □

Before we can prove the theorem, we need some preliminaries. Given a finite extension L/K, we would like to consider something more general than a field norm on L. Instead, we will look at norms of L as a K-vector space. There are less axioms to check, so naturally there will be more choices for the norm. However, just as in the case of $\mathbb{R}$-vector spaces, we can show that all choices of norms are equivalent. So to prove things about the extended field norm, often we can just pick a convenient vector space norm, prove things about it, then apply equivalence.

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

Note that our norms are also non-Archimedean.

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 $x \in V$.

One of the most convenient norms we will work with is the max norm:

Example (Max norm)**.** Let K be a complete valued field, and V a finite-dimensional K-vector space. Let $x_1, \cdots, x_n$ be a basis of V. Then if

$$x = \sum a_i x_i,$$

then

$$\|x\|_{\max} = \max_i |a_i|$$

defines a norm on V.

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

Proof. Given a Cauchy sequence in V under the max norm, take the limit of each coordinate to get the limit of the sequence, using the fact that K is complete. □

That was remarkably easy. We can now immediately transfer this to all other norms we can think of by showing all norms are equivalent.

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

Corollary. V is complete with respect to any norm.

Proof. Let $\|\cdot\|$ be a norm. We need to find $C, D > 0$ such that

$$C\|x\|_{\max} \leq \|x\| \leq D\|x\|_{\max}.$$

We set $D = \max_i(\|x_i\|)$. Then we have

$$\|x\| = \left\|\sum a_i x_i\right\| \leq \max(|a_i|\,\|x_i\|) \leq (\max|a_i|)D = \|x\|_{\max} D.$$

We find C by induction on n. If $n = 1$, then $\|x\| = \|a_1 x_1\| = |a_1|\,\|x\| = \|x\|_{\max}\|x_1\|$. So $C = \|x_1\|$ works.

For $n \geq 2$, we let

$$\begin{aligned} V_i &= Kx_1 \oplus \cdots \oplus Kx_{i-1} \oplus Kx_{i+1} \oplus \cdots \oplus Kx_n \\ &= \operatorname{span}\{x_1, \cdots, x_{i-1}, x_{i+1}, \cdots, x_n\}. \end{aligned}$$

By the induction hypothesis, each V_i is complete with respect to (the restriction of) $\|\cdot\|$. So in particular V_i is closed in V. So we know that the union

$$\bigcup_{i=1}^{n} x_i + V_i$$

is also closed. By construction, this does not contain 0. So there is some $C > 0$ such that if $x \in \bigcup_{i=1}^n x_i + V_i$, then $\|x\| \geq C$. We claim that

$$C \|x\|_{\max} \leq \|x\|.$$

Indeed, take $x = \sum a_i x_i \in V$. Let r be such that

$$|a_r| = \max_i(|a_i|) = \|x\|_{\max}.$$

Then

$$\begin{aligned}\|x\|_{\max}^{-1} \|x\| &= \left\|a_r^{-1} x\right\| \\ &= \left\|\frac{a_1}{a_r}x_1 + \cdots + \frac{a_{r-1}}{a_r}x_{r-1} + x_r + \frac{a_{r+1}}{a_r}x_{r+1} + \cdots + \frac{a_n}{a_r}x_n\right\| \\ &\geq C,\end{aligned}$$

since the last vector is an element of $x_r + V_r$. □

Before we can prove our theorem, we note the following two easy lemmas:

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

Proof. Let $x \in K$ and $|x| > 1$. Suppose we have $a_{n-1}, \cdots, a_0 \in \mathcal{O}_K$. Then we have

$$|x^n| > |a_0 + a_1 x + \cdots + a_{n-1}x^{n-1}|.$$

So we know

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

has non-zero norm, and in particular is non-zero. So x is not integral over $\mathcal{O}_K$. So $\mathcal{O}_K$ is integrally closed. □

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

Proof. It is clear that if $|\cdot|$ is an absolute value, then $|\alpha| \leq 1$ implies $|\alpha+1| \leq 1$.

Conversely, if this holds, and $|x| \leq |y|$, then $|x/y| \leq 1$. So $|x/y + 1| \leq 1$. So $|x + y| \leq |y|$. So $|x + y| \leq \max\{|x|, |y|\}$. □

Finally, we get to prove our theorem.

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

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

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

Proof. For uniqueness and completeness, if $|\cdot|_L$ is an absolute value on L, then it is in particular a K-norm on L as a finite-dimensional vector space. So we know L is complete with respect to $|\cdot|_L$.

If $|\cdot|'_L$ is another absolute value extending $|\cdot|$, then we know $|\cdot|_L$ and $|\cdot|'_L$ is equivalent in the sense of inducing the same topology. But then from one of the early exercises, when *field* norms are equivalent, then we can find some $s > 0$ such that $|\cdot|_L^s = |\cdot|'_L$. But the two norms agree on K, and they are non-trivial. So we must have $s = 1$. So the norms are equal.

To show existence, we have to prove that

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

is a norm.

(i) If $|\alpha|_L = 0$, then $N_{L/K}(\alpha) = 0$. This is true iff $\alpha = 0$.

(ii) The multiplicativity of $|\alpha|$ and follows from the multiplicativity of $N_{L/K}$, $|\cdot|$ and $\sqrt[n]{\cdot}$.

To show the strong triangle inequality, it suffices to show that $|\alpha|_L \leq 1$ implies $|\alpha + 1|_L \leq 1$.

We know that

$$\{\alpha \in L : |\alpha|_L \leq 1\} = \{\alpha \in L : N_{L/K}(\alpha) \in \mathcal{O}_K\}.$$

The claim is that this is equal to the integral closure of $\mathcal{O}_K$ in L. This implies what we want, since the integral closure is closed under addition (and 1 is in the integral closure).

Let $|\alpha|_L \leq 1$. We wlog $\alpha \neq 0$, since that case is trivial. Let

$$f(x) = a_0 + a_1 x + \cdots + a_{n-1}x^{n-1} + x^n \in K[x]$$

be the minimal polynomial of α over K. We need to show that $a_i \in \mathcal{O}_K$ for all i.

By the corollary of Hensel's lemma, for each i, we have

$$|a_i| \leq \max(|a_0|, 1)$$

By general properties of the field norm, there is some $m \in \mathbb{Z}_{\geq 1}$ such that $N_{L/K}(\alpha) = \pm a_0^m$. So we have

$$|a_i| \leq \max\left(\left|N_{L/K}(\alpha)^{1/m}\right|, 1\right) = 1.$$

So $f \in \mathcal{O}_K[x]$. So α is integral over $\mathcal{O}_K$.

On the other hand, suppose α is integral over $\mathcal{O}_K$. Let $\bar{K}/K$ be an algebraic closure of K. Note that

$$N_{L/K}(\alpha) = \left(\prod_{\sigma: L \hookrightarrow \bar{K}} \sigma(\alpha)\right)^d,$$

for some $d \in \mathbb{Z}_{\geq 1}$, and each $\sigma(\alpha)$ is integral over $\mathcal{O}_K$, since α is (apply σ to the minimal polynomial). This implies that $N_{L/K}(\alpha)$ is integral over $\mathcal{O}_K$ (and lies in K). So $N_{L/K}(\alpha) \in \mathcal{O}_K$ since $\mathcal{O}_K$ is integrally closed in K. □

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

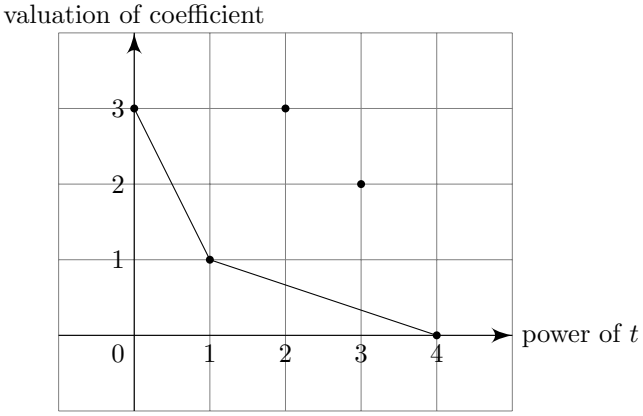
2.3 Newton polygons

We are going to have a small digression to Newton polygons. We will not make use of them in this course, but it is a cute visual devices that tell us about roots of polynomials. It is very annoying to write down a formal definition, so we first look at some examples. We will work with valuations rather than the absolute value.

Example. Consider the valued field $(\mathbb{Q}_p, v_p)$, and the polynomial

$$t^4 + p^2t^4 - p^3t^2 + pt + p^3.$$

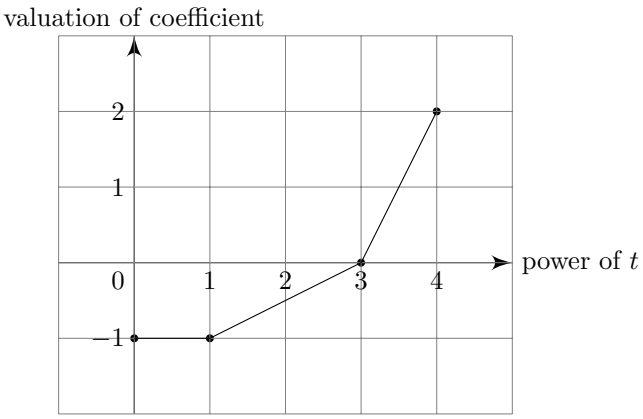
We then plot the coefficients for each power of t, and then draw a "convex polygon" so that all points lie on or above it:



Example. Consider $(\mathbb{Q}_2, v_2)$ with the polynomial

$$4t^4 + 5t^3 + \frac{7}{2}t + \frac{9}{2}.$$

Here there is no t^2 term, so we simply don't draw anything.



We now go to come up with a formal definition.

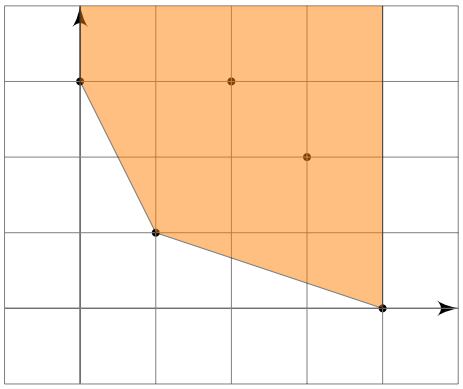
Definition (Lower convex set)**.** We say a set $S \subseteq \mathbb{R}^2$ is *lower convex* if

(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.

Example. The lower convex hull of the points $(0, 3), (1, 1), (2, 3), (3, 2), (4, 0)$ is given by the region denoted below:



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 $\{(i, v(a_i)) : i = 0, \cdots, n, a_i \neq 0\}$.

This is the formal definition, so in our first example, the Newton polygon really should be the shaded area shown above, but most of the time, we only care about the lower line.

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*.

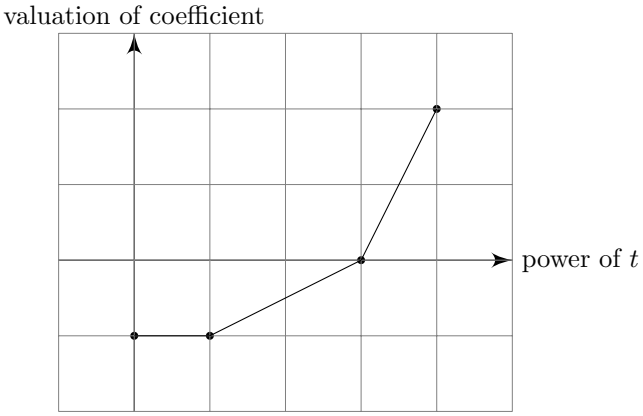
Definition (Line segment)**.** Given a polynomial, the line segment between two adjacent break points is a *line segment*.

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.

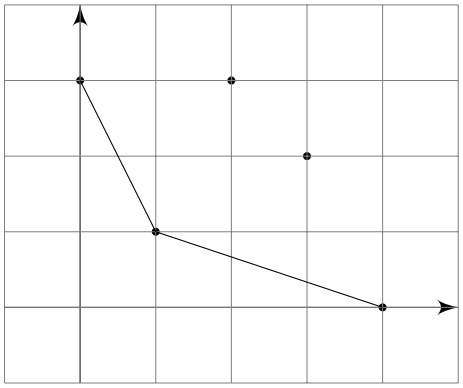
Example. Consider again $(\mathbb{Q}_2, v_2)$ with the polynomial

$$4t^4 + 5t^3 + \frac{7}{2}t + \frac{9}{2}.$$



The middle segment has length 2 and slope 1/2.

Example. In the following Newton polygon:



The second line segment has length 3 and slope $-\frac{1}{3}$.

It turns out the Newton polygon tells us something about the roots of the polynomial.

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

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

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

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

Note that by lower convexity, there can be at most one line segment for each slope. So this theorem makes sense.

Proof. Dividing by a_n only shifts the polygon vertically, so we may wlog $a_n = 1$.

We number the roots of f such that

$$\begin{aligned} w(\alpha_1) = \cdots = w(\alpha_{s_1}) &= w_1\\ w(\alpha_{s_1+1}) = \cdots = w(\alpha_{s_2}) &= w_2\\ &\vdots\\ w(\alpha_{s_t}) = \cdots = w(\alpha_n) &= w_{t+1}, \end{aligned}$$

where we have

$$w_1 < w_2 < \cdots < w_{t+1}.$$

Then we know

$$\begin{aligned} v(a_n) &= v(1) = 0\\ v(a_{n-1}) &= w\left(\sum \alpha_i\right) \geq \min_i w(\alpha_i) = w_1\\ v(a_{n-2}) &= w\left(\sum \alpha_i\alpha_j\right) \geq \min_{i\neq j} w(\alpha_i\alpha_j) = 2m_1\\ &\vdots\\ v(a_{n-s_1}) &= w\left(\sum_{i_1\neq\ldots\neq i_{s_1}} \alpha_{i_1\ldots\alpha_{i_{s_1}}}\right) = \min w(\alpha_{i_1}\cdots\alpha_{i_{s_1}}) = s_1m_1. \end{aligned}$$

It is important that in the last one, we have equality, not an inequality, because there is one term in the sum whose valuation is less than all the others.

We can then continue to get

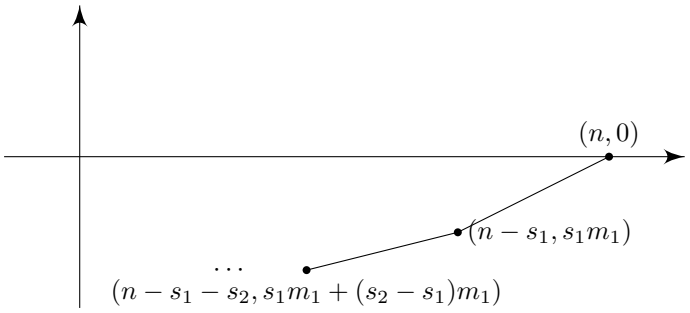
$$v(\alpha_{n-s_1-1}) \geq \min w(\alpha_{i_1}\cdots\alpha_{i_{s_1+1}}) = s_1m_1 + m_2,$$

until we reach

$$v(\alpha_{n-s_1-s_2}) = s_1m_1 + (s_2 - s_1)m_2.$$

We keep going on.

We draw the Newton polygon.



We don't know where exactly the other points are, but the inequalities imply that the $(i, v(a_i))$ are above the lines drawn. So this is the Newton polygon.

Counting from the right, the first line segment has length $n - (n - s_1) = s_1$ and slope

$$\frac{0 - s_1m_1}{n - (n - s_1)} = -m_1.$$

In general, the kth segment has length $(n - s_{k-1}) - (n - s_k) = s_k - s_{k-1}$, and slope

$$\frac{\left(s_1 m_1 + \sum_{i=1}^{k-2}(s_{i+1} - s_i)m_{i+1}\right) - \left(s_1 m_1 + \sum_{i=1}^{k-1}(s_{i+1} - s_i)m_{i+1}\right)}{s_k - s_{k-1}}$$
$$= \frac{-(s_k - s_{k-1})m_k}{s_k - s_{k-1}} = -m_k.$$

and the others follow similarly. □

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

Proof. We need to show that all roots have the same valuation. Let α, β be in the splitting field L. Then there is some $\sigma \in \mathrm{Aut}(L/K)$ such that $\sigma(\alpha) = \beta$. Then $w(\alpha) = w(\sigma(\alpha)) = \beta$. So done. □

Note that Eisenstein's criterion is a (partial) converse to this!

3 Discretely valued fields

We are now going to further specialize. While a valued field already has some nice properties, we can't really say much more about them without knowing much about their valuations.

Recall our previous two examples of valued fields: $\mathbb{Q}_p$ and $\mathbb{F}_p((T))$. The valuations had the special property that they take values in $\mathbb{Z}$. Such fields are known as *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.

Note that we do not require the image to be exactly $\mathbb{Z} \subseteq \mathbb{R}$. So we allow scaled versions of the valuation. This is useful because the property of mapping to $\mathbb{Z}$ is not preserved under field extensions in general, as we will later see. We will call those that do land in $\mathbb{Z}$ *normalized valuations*.

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 $\mathbb{Z}$.

Note that the normalized valuation does not give us a preferred choice of absolute value, since to obtain an absolute value, we still have to arbitrarily pick the base $c > 1$ to define $|x| = c^{-v(x)}$.

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).

So with a normalized valuation, we have $v_K(\pi)$.

Example. The usual valuation on $\mathbb{Q}_p$ is normalized, and so is the usual valuation on $k((T))$. p is a uniformizer for $\mathbb{Q}_p$ and t is a uniformizer for $k((T))$.

The kinds of fields we will be interested are *local fields*. The definition we have here might seem rather ad hoc. This is just one of the many equivalent characterizations of a local field, and the one we pick here is the easiest to state.

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

Example. $\mathbb{Q}$ and $\mathbb{Q}_p$ with v_p are both discretely valued fields, and $\mathbb{Q}_p$ is a local field. p is a uniformizer.

Example. The Laurent series field $k((T))$ with valuation

$$v\left(\sum a_n T^n\right) = \inf\{n : a_n \neq 0\}$$

is a discrete valued field, and is a local field if and only if k is finite field, as the residue field is exactly k. We have

$$\mathcal{O}_{k((T))} = k[[T]] = \left\{\sum_{n=0}^{\infty} a_n T^n : a_n \in k\right\}.$$

Here T is a uniformizer.

These discretely valued field are pretty much like the p-adic numbers.

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

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

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

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

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

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

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

where $a_n \in S$, and

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

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

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

is an isomorphism.

Proof. The same as for $\mathbb{Q}_p$ and $\mathbb{Z}_p$, with π instead of p. □

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

Proof. If $\mathcal{O}_K$ is compact, then $\pi^{-n}\mathcal{O}_K$ is compact for all $n \geq 0$ (where π is the uniformizer), and in particular complete. So

$$K = \bigcup_{n \geq 0}^{\infty} \pi^{-n}\mathcal{O}_K$$

is complete, as this is an increasing union, and Cauchy sequences are bounded. Also, we know the quotient map $\mathcal{O}_K \to k_K$ is continuous when k_K is given the discrete topology, by definition of the π-adic topology. So k_K is compact and discrete, hence finite.

In the other direction, if K is local, then we know $\mathcal{O}_K/\pi^n\mathcal{O}_K$ is finite for all $n \geq 0$ (by induction and finiteness of k_K). We let (x_i) be a sequence in $\mathcal{O}_K$. Then by finiteness of $\mathcal{O}_K/\pi\mathcal{O}_K$, there is a subsequence $(x_{1,i})$ which is constant modulo π. We keep going, choosing a subsequence $(x_{n+1,i})$ of (x_{n_i}) such that $(x_{n+1,i})$ is constant modulo π^{n+1}. Then $(x_{i,i})_{i=1}^{\infty}$ converges, since it is Cauchy as

$$|x_{ii} - x_{jj}| \leq |\pi|^j$$

for $j \leq i$. So $\mathcal{O}_K$ is sequentially compact, hence compact. □

Now the valuation ring $\mathcal{O}_K$ inherits a valuation from K, and this gives it a structure of a *discrete valuation ring*. We will define a discrete valuation ring in a funny way, but there are many equivalent definitions that we will not list.

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.

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

Proof. We have already seen that valuation rings of discrete valuation fields are DVRs. In the other direction, let R be a DVR, and π a prime. Let $x \in \mathbb{R} \setminus \{0\}$. Then we can find a unique unit $u \in R^\times$ and $n \in \mathbb{Z}_{\geq 0}$ such that $x = \pi^n u$ (say, by unique factorization of PIDs). We define

$$v(x) = \begin{cases} n & x \neq 0 \\ \infty & x = 0 \end{cases}$$

This is then a discrete valuation of R. This extends uniquely to the field of fractions K. It remains to show that $R = \mathcal{O}_K$. First note that

$$K = R\left[\frac{1}{\pi}\right].$$

This is since any non-zero element in $R\left[\frac{1}{\pi}\right]$ looks like $\pi^n u, u \in R^\times, n \in \mathbb{Z}$, and is already invertible. So it must be the field of fractions. Then we have

$$v(\pi^n u) = n \in \mathbb{Z}_{\geq 0} \iff \pi^n u \in R.$$

So we have $R = \mathcal{O}_K$. □

Now recall our two "standard" examples of valued fields — $\mathbb{F}_p((T))$ and $\mathbb{Q}_p$. Both of their residue fields are $\mathbb{F}_p$, and in particular has characteristic p. However, $\mathbb{F}_p((T))$ itself is *also* of characteristic p, while $\mathbb{Q}_p$ has characteristic 0. It would thus be helpful to split these into two different cases:

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*.

If K has mixed characteristic, then necessarily $\operatorname{char} K = 0$, and $\operatorname{char} k_K > 0$.

Example. $\mathbb{Q}_p$ has mixed characteristic, since $\operatorname{char} \mathbb{Q}_p = 0$ but $\operatorname{char} k_{\mathbb{Q}_p} = \mathbb{Z}/p\mathbb{Z} = p$.

We will also need the following definition:

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.

Fact. Let F be a field of characteristic p. Then F is perfect if and only if every finite extension of F is separable.

Example. $\mathbb{F}_q$ is perfect for every $q = p^n$.

3.1 Teichmüller lifts

Take our favorite discretely valued ring $\mathbb{Z}_p$. This is p-adically complete, so we can write each element as

$$x = a_0 + a_1 p + a_2 p^2 + \cdots,$$

where each a_i is in $\{0, 1, \cdots, p-1\}$. The reason this works is that $0, 1, \cdots, p-1$ are coset representatives of the ring $\mathbb{Z}_p/p\mathbb{Z}_p \cong \mathbb{Z}/p\mathbb{Z}$. While these coset representatives might feel like a "natural" thing to do in this context, this is because we have implicitly identified with $\mathbb{Z}_p/p\mathbb{Z}_p \cong \mathbb{Z}/p\mathbb{Z}$ as a particular subset of $\mathbb{Z} \subseteq \mathbb{Z}_p$. However, this identification respects effectively no algebraic structure at all. For example, we cannot multiplying the cosets simply by multiplying the representatives as elements of $\mathbb{Z}_p$, because, say, $(p-1)^2 = p^2 - 2p + 1$, which is not 1. So this is actually quite bad, at least theoretically.

It turns out that we can actually construct "natural" lifts in a very general scenario.

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

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

and

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

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

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.

The idea of the proof is as follows: suppose we have an $a \in R/xR$. If we randomly picked a lift α, then chances are it would be a pretty "bad" choice, since any two such choices can differ by a multiple of x.

Suppose we instead lifted a pth root of a to R, and then take the pth power of it. We claim that this is a better way of picking a lift. Suppose we have picked two lifts of $a^{p^{-1}}$, say, α_1 and α_1'. Then $\alpha_1' = xc + \alpha_1$ for some c. So we have

$$(\alpha_1')^p - \alpha_1^p = \alpha_1^p + pxc + O(x^2) - \alpha_1^p = pxc + O(x^2),$$

where we abuse notation and write $O(x^2)$ to mean terms that are multiples of x^2.

We now recall that R/xR has characteristic p, so $p \in xR$. Thus in fact $pxc = O(x^2)$. So we have

$$(\alpha_1')^p - \alpha_1^p = O(x^2).$$

So while the lift is still arbitrary, any two arbitrary choices can differ by at most x^2. Alternatively, our lift is now a well-defined element of R/x^2R.

We can, of course, do better. We can lift the p^2th root of a to R, then take the p^2th power of it. Now any two lifts can differ by at most $O(x^3)$. More generally, we can try to lift the p^nth root of a, then take the p^nth power of

it. We keep picking a higher and higher n, take the limit, and hopefully get something useful out!

Unfortunately, to prove this result, we will need the following messy lemma:

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

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

Then we have

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

Proof. It is left as an exercise to modify the proof to work for $p = 2$ (it is actually easier). So suppose p is odd. We take the pth power of † to obtain

$$\alpha^p - \beta^p + \sum_{i=1}^{p-1} \binom{p}{i} \alpha^{p-i}\beta^i \in x^{p(k+1)}R.$$

We can now write

$$\begin{aligned}\sum_{i=1}^{p-1}(-1)^i \binom{p}{i} \alpha^{p-i}\beta^i &= \sum_{i=1}^{\frac{p-1}{2}}(-1)^i \binom{p}{i} (\alpha\beta)^i \left(\alpha^{p-2i} - \beta^{p-2i}\right)\\ &= p(\alpha - \beta)(\text{something}).\end{aligned}$$

Now since R/xR has characteristic p, we know $p \in xR$. By assumption, we know $\alpha - \beta \in x^{k+1}R$. So this whole mess is in $x^{k+2}R$, and we are done. □

Proof of theorem. Let $a \in R/xR$. For each n, there is a unique $a^{p^{-n}} \in R/xR$. We lift this arbitrarily to some $\alpha_n \in R$ such that

$$\alpha_n \equiv a^{p^{-n}} \mod x.$$

We define

$$\beta_n = \alpha_n^{p^n}.$$

The claim is that

$$[a] = \lim_{n\to\infty} \beta_n$$

exists and is independent of the choices.

Note that if the limit exists no matter how we choose the α_n, then it must be independent of the choices. Indeed, if we had choices β_n and β_n', then $\beta_1, \beta_2', \beta_3, \beta_4', \beta_5, \beta_6', \cdots$ is also a respectable choice of lifts, and thus must converge. So β_n and β_n' must have the same limit.

Since the ring is x-adically complete and is discretely valued, to show the limit exists, it suffices to show that $\beta_{n+1} - \beta_n \to 0$ x-adically. Indeed, we have

$$\beta_{n+1} - \beta_n = (\alpha_{n+1}^p)^{p^n} - \alpha_n^{p^n}.$$

We now notice that

$$\alpha_{n+1}^p \equiv (a^{p^{-n-1}})^p = a^{p^{-n}} \equiv \alpha_n \mod x.$$

So by applying the previous the lemma many times, we obtain

$$(\alpha_{n+1}^p)^{p^n} \equiv \alpha_n^{p^n} \mod x^{n+1}.$$

So $\beta_{n+1} - \beta_n \in x^{n+1}R$. So $\lim \beta_n$ exists.

To see $[a] = a \mod x$, we just have to note that

$$\lim_{n\to\infty} \alpha_n^{p^n} \equiv \lim_{n\to\infty} (a^{p^{-n}})^{p^n} = \lim a = a \mod x.$$

(here we are using the fact that the map $R \to R/xR$ is continuous when R is given the x-adic topology and R/xR is given the discrete topology)

The remaining properties then follow trivially from the uniqueness of the above limit.

For multiplicativity, if we have another element $b \in R/xR$, with $\gamma_n \in R$ lifting $b^{p^{-n}}$ for all n, then $\alpha_n\gamma_n$ lifts $(ab)^{p^{-n}}$. So

$$[ab] = \lim \alpha_n^{p^n}\gamma_n^{p^n} = \lim \alpha_n^{p^n} \lim \gamma_n^{p^n} = [a][b].$$

If R has characteristic p, then $\alpha_n + \gamma_n$ lifts $a^{p^{-n}} + b^{p^{-n}} = (a+b)^{p^{-n}}$. So

$$[a+b] = \lim(\alpha_n + \gamma_n)^{p^n} = \lim \alpha_n^{p^n} + \lim \gamma_n^{p^n} = [a] + [b].$$

Since 1 is a lift of 1 and 0 is a lift of 0, it follows that this is a ring homomorphism.

Finally, to show uniqueness, suppose $\phi : R/xR \to R$ is a map with these properties. Then we note that $\phi(a^{p^{-n}}) \equiv a^{p^{-n}} \mod x$, and is thus a valid choice of α_n. So we have

$$[a] = \lim_{n\to\infty} \phi(a^{p^{-n}})^{p^n} = \lim \phi(a) = \phi(a).$$

□

Example. Let $R = \mathbb{Z}_p$ and $x = p$. Then $[-] : \mathbb{F}_p \to \mathbb{Z}_p$ satisfies

$$[x]^{p-1} = [x^{p-1}] = [1] = 1.$$

So the image of $[x]$ must be the unique $p-1$th root of unity lifting x (recall we proved their existence via Hensel's lemma).

When proving theorems about these rings, the Teichmüller lifts would be very handy and natural things to use. However, when we want to do actual computations, there is absolutely no reason why these would be easier!

As an application, we can prove the following characterization of equal characteristic complete DVF's.

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

Proof. Let K be a complete DVF. Since every DVF the field of fractions of its valuation ring, it suffices to prove that $\mathcal{O}_K \cong k_K[[T]]$. We know $\mathcal{O}_K$ has characteristic p. So $[-] : k_K \to \mathcal{O}_K$ is an injective ring homomorphism. We choose a uniformizer $\pi \in \mathcal{O}_K$, and define

$$k_K[[T]] \to \mathcal{O}_K$$

by

$$\sum_{n=0}^{\infty} a_n T^n \mapsto \sum_{n=0}^{\infty} [a_n]\pi^n.$$

Then this is a ring homomorphism since $[-]$ is. The bijectivity follows from property (v) in our list of properties of complete DVF's. □

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

3.2 Witt vectors*

We are now going to look at the mixed characteristic analogue of this result. We want something that allows us to go from characteristic p to characteristic 0. This is known as *Witt vectors*, which is non-examinable.

We start with the notion of a *strict p-ring*. Roughly this is a ring that satisfies all the good properties whose name has the word "p" in it.

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.

Note that a strict p-ring in particular satisfies the conditions for the Teichmüller lift to exist, for $x = p$.

Example. $\mathbb{Z}_p$ is a strict p-ring.

The next example we are going to construct is more complicated. This is in some sense a generalization of the usual polynomial rings $\mathbb{Z}[x_1, \cdots, x_n]$, or more generally,

$$\mathbb{Z}[x_i \mid i \in I],$$

for I possibly infinite. To construct the "free" strict p-ring, after adding all these variables x_i, to make it a strict p-ring, we also need to add their pth roots, and the p^2th roots etc, and then take the p-adic completion, and hope for the best.

Example. Let $X = \{x_i : i \in I\}$ be a set. Let

$$B = \mathbb{Z}[x_i^{p^{-\infty}} \mid i \in I] = \bigcup_{n=0}^{\infty} \mathbb{Z}[x_i^{p^{-n}} \mid i \in I].$$

Here the union on the right is taken by treating

$$\mathbb{Z}[x_i \mid i \in I] \subseteq \mathbb{Z}[x_i^{p^{-1}} \mid i \in I] \subseteq \cdots$$

in the natural way.

We let A be the p-adic completion of B. We claim that A is a strict p-ring and $A/pA \cong \mathbb{F}_p[x_i^{p^{-\infty}} \mid i \in I]$.

Indeed, we see that B is p-torsion free. By Exercise 13 on Sheet 1, we know A is p-adically complete and torsion free. Moreover,

$$A/pA \cong B/pB \cong \mathbb{F}_p[x_i^{p^{-\infty}} \mid i \in I],$$

which is perfect since every element has a p-th root.

If A is a strict p-ring, then we know that we have a Teichmüller map

$$[-] : A/pA \to A,$$

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

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

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

Proof. We recursively construct the a_n by

$$\begin{aligned} a_0 &= a \pmod p \\ a_1 &\equiv p^{-1}(a - [a_0]) \pmod p \\ &\vdots \end{aligned}$$

□

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

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

Proof sketch. We define F by the given formula and check that it works. First of all, by the formula, F is continuous is p-adically continuous, and the key thing is to check that it is additive (which is slightly messy). Multiplicativity then follows formally from the continuity and additivity.

To show uniqueness, suppose that we have some ψ lifting f. Then $\psi(p) = p$. So ψ is p-adically continuous. So it suffices to show that $\psi([a]) = [\psi(a)]$.

We take $\alpha_n \in A$ lifting $a^{p^{-n}} \in A/pA$. Then $\psi(\alpha_n)$ lifts $f(a)^{p^{-n}}$. So

$$\psi([a]) = \lim \psi(\alpha_n^{p^{-n}}) = \lim \psi(\alpha_n)^{p^n} = [f(a)].$$

So done. □

There is a generalization of this result which we shall not prove:

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

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

We can now state the main theorem about strict p-rings.

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

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

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

Proof sketch. If $W(R)$ and $W(R')$ are such strict p-rings, then the second part follows from the previous lemma. Indeed, if C is a strict p-ring with $C/pC \cong R \cong W(R)/pW(R)$, then the isomorphism $\bar{\alpha} : W(R)/pW(R) \to C/pC$ and its inverse $\bar{\alpha}^{-1}$ have unique lifts $\gamma : W(R) \to C$ and $\gamma^{-1} : C \to W(R)$, and these are inverses by uniqueness of lifts.

To show existence, let R be a perfect ring. We form

$$\begin{aligned}\mathbb{F}_p[x_r^{p^{-\infty}} \mid r \in R] &\to R\\ x_r &\mapsto r\end{aligned}$$

Then we know that the p-adic completion of $\mathbb{Z}[x_r^{p^{-\infty}} \mid r \in R]$, written A, is a strict p-ring with

$$A/pA \cong \mathbb{F}_p[x_r^{p^{-\infty}} \mid r \in R].$$

We write

$$I = \ker(\mathbb{F}_p[x_r^{p^{-\infty}} \mid r \in R] \to R).$$

Then define

$$J = \left\{\sum_{n=0}^{\infty}[a_k]p^n \in A : a_n \in I \text{ for all } n\right\}.$$

This turns out to be an ideal.

We put $W(R) = A/J$. We can then painfully check that this has all the required properties. For example, if

$$x = \sum_{n=0}^{\infty}[a_n]p^n \in A,$$

and

$$px = \sum_{n=0}^{\infty}[a_n]p^{n+1} \in J,$$

then by definition of J, we know $[a_n] \in I$. So $x \in J$. So $W(R)/J$ is p-torsion free. By a similar calculation, one checks that

$$\bigcap_{n=0}^{\infty} p^n W(R) = \{0\}.$$

This implies that $W(R)$ injects to its p-adic completion. Using that A is p-adically complete, one checks the surjectivity by hand.

Also, we have

$$\frac{W(R)}{pW(R)} \cong \frac{A}{J + pA}.$$

But we know

$$J + pA = \left\{\sum_n [a_n]p^n \mid a_0 \in I\right\}.$$

So we have

$$\frac{W(R)}{pW(R)} \cong \frac{\mathbb{F}_p[x_r^{p^{-\infty}} \mid r \in R]}{I} \cong R.$$

So we know that $W(R)$ is a strict p-ring. □

Example. $W(\mathbb{F}_p) = \mathbb{Z}_p$, since $\mathbb{Z}_p$ satisfies all the properties $W(\mathbb{F}_p)$ is supposed to satisfy.

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

Proof. Let A be a complete DVR such that p is a uniformizer and A/pA is perfect. Then A is p-torsion free, as A is an integral domain of characteristic 0. Since it is also p-adically complete, it is a strict p-ring.

Conversely, if A is a strict p-ring, and A/pA is a field, then we have $A^\times \subseteq A \setminus pA$, and we claim that $A^\times = A \setminus pA$. Let

$$x = \sum_{n=0}^{\infty} [x_n] p^n$$

with $x_0 \neq 0$, i.e. $x \notin pA$. We want to show that x is a unit. Since A/pA is a field, we can multiply by $[x_0^{-1}]$, so we may wlog $x_0 = 1$. Then $x = 1 - py$ for some $y \in A$. So we can invert this with a geometric series

$$x^{-1} = \sum_{n=0}^{\infty} p^n y^n.$$

So x is a unit. Now, looking at Teichmüller expansions and factoring out multiple of p, any non-zero element z can be written as $p^n u$ for a unique $n \geq \mathbb{Z}_{\geq 0}$ and $u \in A^\times$. Then we have

$$v(z) = \begin{cases} n & z \neq 0 \\ \infty & z = 0 \end{cases}$$

is a discrete valuation on A. □

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.

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

Proof. Having absolute ramification index 1 is the same as saying p is a uniformizer. So R is a strict p-ring with $R/pR \cong k$. By uniqueness of the Witt vector, we know $R \cong W(k)$. □

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

Proof. We need to first exhibit $W(k)$ as a subring of R. We know that $\mathrm{id} : k \to k$ lifts to a homomorphism $W(k) \to R$. The kernel is a prime ideal because R is an integral domain. So it is either 0 or $pW(k)$. But R has characteristic 0. So it can't be $pW(k)$. So this must be an injection.

Let e be the absolute ramification index of R. We want to prove that

$$R = \bigoplus_{i=0}^{e-1} \pi^i W(k).$$

Looking at valuations, one sees that $1, \pi, \pi, \cdots, \pi^{e-1}$ are linearly independent over $W(k)$. So we can form

$$M = \bigoplus_{i=0}^{e-1} \pi^i W(k) \subseteq R.$$

We consider R/pR. Looking at Teichmüller expansions

$$\sum_{n=0}^{\infty} [x_n]\pi^n \equiv \sum_{n=0}^{e-1} [x_n]\pi^n \mod pR,$$

we see that $1, \pi, \cdots, \pi^{e-1}$ generate R/pR as $W(k)$-modules (all the Teichmüller lifts live in $W(k)$). Therefore $R = M + pR$. We iterate to get

$$R = M + p(M + pR) = M + p^2 r = \cdots = M + p^m R$$

for all $m \geq 1$. So M is dense in R. But M is also p-adically complete, hence closed in R. So $M = R$. □

The important statement to take away is

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

Proof. Let $\mathbb{F}_q$ be the residue field of K. Then $\mathcal{O}_K$ is finite over $W(\mathbb{F}_q)$ by the previous theorem. So it suffices to show that $W(\mathbb{F}_q)$ is finite over $W(\mathbb{F}_p) = \mathbb{Z}_p$. Again the inclusion $\mathbb{F}_p \subseteq \mathbb{F}_q$ gives an injection $W(\mathbb{F}_p) \hookrightarrow W(\mathbb{F}_q)$. Write $q = p^d$, and let $x_1, \cdots, x_d \in W(F_q)$ be lifts of an $\mathbb{F}_p$-bases of $\mathbb{F}_q$.. Then we have

$$W(\mathbb{F}_q) = \bigoplus_{i=1}^{d} x_d \mathbb{Z}_p + pW(\mathbb{F}_q),$$

and then argue as in the end of the previous theorem to get

$$W(\mathbb{F}_q) = \bigoplus_{i=1}^{d} x_d \mathbb{Z}_p.$$ □

4 Some p-adic analysis

We are now going to do some fun things that is not really related to the course. In "normal" analysis, the applied mathematicians hold the belief that every function can be written as a power series

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

When we move on to p-adic numbers, we do not get such a power series expansion. However, we obtain an analogous result using binomial coefficients.

Before that, we have a quick look at our familiar functions exp and log, which we shall continue to define as a power series:

$$\exp(x) = \sum_{n=0}^{\infty} \frac{x^n}{n!}, \quad \log(1+x) = \sum_{n=1}^{\infty} (-1)^{n-1} \frac{x^n}{n}$$

The domain will no longer be all of the field. Instead, we have the following result:

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

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

Proof. We let $v = -\log_p |\cdot|$ be a valuation extending v_p. Then we have the dumb estimate

$$v(n) \leq \log_p n.$$

Then we have

$$v\left(\frac{x^n}{n}\right) \geq n \cdot v(x) - \log_p n \to \infty$$

if $v(x) > 0$. So log converges.

For exp, we have

$$v(n!) = \frac{n - s_p(n)}{p-1},$$

where $s_p(n)$ is the sum of the p-adic digits of n. Then we have

$$v\left(\frac{x^n}{n!}\right) \geq n \cdot v(x) - \frac{n}{p-1} = n \cdot \left(v(x) - \frac{1}{p-1}\right) \to \infty$$

if $v(x) > 1/(p-1)$. Since $v\left(\frac{x^n}{n!}\right) \geq 0$, this lands in $\mathcal{O}_K$.

For the continuity, we just use uniform convergence as in the real case. □

What we really want to talk about is binomial coefficients. Let $n \geq 1$. Then we know that

$$\binom{x}{n} = \frac{x(x-1)\cdots(x-n+1)}{n!}$$

is a polynomial in x, and so defines a continuous function $\mathbb{Z}_p \to \mathbb{Q}_p$ by $x \mapsto \binom{x}{n}$. When $n = 0$, we set $\binom{x}{n} = 1$ for all $x \in \mathbb{Z}_p$.

We know $\binom{x}{n} \in \mathbb{Z}$ if $x \in \mathbb{Z}_{\geq 0}$. So by density of $\mathbb{Z}_{\geq 0} \subseteq \mathbb{Z}_p$, we must have $\binom{x}{n} \in \mathbb{Z}_p$ for all $x \in \mathbb{Z}_p$.

We will eventually want to prove the following result:

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

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

and moreover

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

We write $C(\mathbb{Z}_p, \mathbb{Q}_p)$ for the set of continuous functions $\mathbb{Z}_p \to \mathbb{Q}_p$ as usual. This is a $\mathbb{Q}_p$ vector space as usual, with

$$(\lambda f + \mu g)(x) = \lambda f(x) + \mu g(x)$$

for all $\lambda, \mu \in \mathbb{Q}_p$ and $f, g \in C(\mathbb{Z}_p, \mathbb{Q}_p)$ and $x \in \mathbb{Z}_p$.

If $f \in C(\mathbb{Z}_p, \mathbb{Q}_p)$, we set

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

Since $\mathbb{Z}_p$ is compact, we know that f is bounded. So the supremum exists and is attained.

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

Let c_0 denote the set of sequences $(a_n)_{n=0}^{\infty}$ in $\mathbb{Q}_p$ such that $a_n \to 0$. This is a $\mathbb{Q}_p$-vector space with a norm

$$\|(a_n)\| = \max_{n\in\mathbb{N}} |a_n|_p,$$

and c_0 is complete. So what Mahler's theorem gives us is an isometric isomorphism between c_0 and $C(\mathbb{Z}_p, \mathbb{Q}_p)$.

We define

$$\Delta : C(\mathbb{Z}_p, \mathbb{Q}_p) \to C(\mathbb{Z}_p, \mathbb{Q}_p)$$

by

$$\Delta f(x) = f(x + 1) - f(x).$$

By induction, we have

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

Note that Δ is a linear operator on $C(\mathbb{Z}_p, \mathbb{Q}_p)$, and moreover

$$|\Delta f(x)|_p = |f(x + 1) - f(x)|_p \leq \|f\|.$$

So we have

$$\|\Delta f\| \leq \|f\|.$$

In other words, we have

$$\|\Delta\| \leq 1.$$

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

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

We will eventually show that these are the a_n's that appear in Mahler's theorem. The first thing to prove is that these coefficients do tend to 0. We already know that they don't go up, so we just have to show that they always eventually go down.

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

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

Proof. If $f = 0$, there is nothing to prove. So we will wlog $\|f\| = 1$ by scaling (this is possible since the norm is attained at some x_0, so we can just divide by $f(x_0)$). We want to find some k such that

$$\Delta^{p^k} f(x) \equiv 0 \mod p$$

for all x. To do so, we use the explicit formula

$$\Delta^{p^k} f(x) = \sum_{i=0}^{p^k} (-1)^i \binom{p^k}{i} f(x + p^k - i) \equiv f(x + p^k) - f(x) \pmod{p}$$

because the binomial coefficients $\binom{p^k}{i}$ are divisible by p for $i \neq 0, p^k$. Note that we do have a negative sign in front of $f(x)$ because $(-1)^{p^k}$ is -1 as long as p is odd, and $1 = -1$ if $p = 2$.

Now $\mathbb{Z}_p$ is compact. So f is uniformly continuous. So there is some k such that $|x - y|_p \leq p^{-k}$ implies $|f(x) - f(y)|_p \leq p^{-1}$ for all $x, y \in \mathbb{Z}_p$. So take this k, and we're done. □

We can now prove that the Mahler's coefficients tend to 0.

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

Proof. First we prove that $a_n(f) \to 0$. We know that

$$\|a_n(f)\|_p \leq \|\Delta^n f\|.$$

So it suffices to show that $\|\Delta^n f\| \to 0$. Since $\|\Delta\| \leq 1$, we know $\|\Delta^n f\|$ is monotonically decreasing. So it suffices to find a subsequence that tends to 0. To do so, we simply apply the lemma repeatedly to get $k_1, k_2, \cdots$ such that

$$\left\| \Delta^{p^{k_1 + \cdots + k_n}} \right\| \leq \frac{1}{p^n}\|f\|.$$

This gives the desired sequence.

Note that

$$|a_n(f)|_p \leq \|\Delta^n\| \leq \|f\|.$$

So we know

$$\|(a_n(f))_n\| = \max |a_n(f)|_p \leq \|f\|.$$

So the map is norm-decreasing. Linearity follows from linearity of Δ. To finish, we have to prove injectivity.

Suppose $a_n(f) = 0$ for all $n \geq 0$. Then

$$a_0(f) = f(0) = 0,$$

and by induction,we have that

$$f(n) = \Delta^k f(0) = a_n(f) = 0.$$

for all $n \geq 0$. So f is constantly zero on $\mathbb{Z}_{\geq 0}$. By continuity, it must be zero everywhere on $\mathbb{Z}_p$. □

We are almost at Mahler's theorem. We have found some coefficients already, and we want to see that it works. We start by proving a small, familiar, lemma.

Lemma. We have

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

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

Proof. It is well known that this is true when $x \in \mathbb{Z}_{\geq n}$. Since the expressions are polynomials in x, them agreeing on infinitely many values implies that they are indeed the same. □

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

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

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

Proof. Linearity is clear. Norm-decreasing follows from

$$|f_a(x)| = \left|\sum a_n \binom{x}{n}\right| \leq \sup_n |a_n|_p \left|\binom{x}{n}\right|_p \leq \sup_n |a_n|_p = \|a_n\|,$$

where we used the fact that $\binom{x}{n} \in \mathbb{Z}_p$, hence $\left|\binom{x}{n}\right|_p \leq 1$.

Taking the supremum, we know that

$$\|f_a\| \leq \|a\|.$$

For the last statement, for all $k \in \mathbb{Z}_{\geq 0}$, we define

$$a^{(k)} = (a_k, a_{k+1}, a_{k+1}, \cdots).$$

Then we have

$$\begin{aligned}\Delta f_a(x) &= f_a(x+1) - f_a(x)\\ &= \sum_{n=1}^{\infty} a_n \left(\binom{x+1}{n} - \binom{x}{n}\right)\\ &= \sum_{n=1}^{\infty} a_n \binom{x}{n-1}\\ &= \sum_{n=0}^{\infty} a_{n+1}\binom{x}{n}\\ &= f_{a^{(1)}}(x)\end{aligned}$$

Iterating, we have

$$\Delta^k f_a = f_{a^{(k)}}.$$

So we have

$$a_n(f_a) = \Delta^n f_a(0) = f_{a^{(n)}}(0) = a_n.$$

□

Summing up, we now have maps

$$C(\mathbb{Z}_p, \mathbb{Q}_p) \underset{G}{\overset{F}{\rightleftarrows}} c_0$$

with

$$\begin{aligned}F(f) &= (a_n(f))\\ G(a) &= f_a.\end{aligned}$$

We now that F is injective and norm-decreasing, and G is norm-decreasing and $FG = \mathrm{id}$. It then follows formally that $GF = \mathrm{id}$ and the maps are norm-preserving.

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

Proof. Let $v \in V$. Then

$$F(v - GFv) = Fv - FGFv = (F - F)v = 0.$$

Since F is injective, we have

$$v = GFv.$$

Also, we have

$$\|v\| \geq \|Fv\| \geq \|GFv\| = \|v\|.$$

So we have equality throughout. Similarly, we have $\|v\| = \|Gv\|$. □

This finishes the proof Mahler's theorem, and also finishes this section on p-adic analysis.

5 Ramification theory for local fields

From now on, the characteristic of the residue field of any local field will be denoted p, unless stated otherwise.

5.1 Ramification index and inertia degree

Suppose we have an extension L/K of local fields. Then since $\mathfrak{m}_K \subseteq \mathfrak{m}_L$, and $\mathcal{O}_L \subseteq \mathcal{O}_L$, we obtain an injection

$$k_K = \frac{\mathcal{O}_K}{\mathfrak{m}_k} \hookrightarrow \frac{\mathcal{O}_L}{\mathfrak{m}_L} = k_L.$$

So we also get an extension of residue fields k_L/k_K. The question we want to ask is how much of the extension is "due to" the extension of residue fields k_L/k_K, and how much is "due to" other things happening.

It turns out these are characterized by the following two numbers:

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.

The goal of the section is to show the following result:

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

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

We then have two extreme cases of ramification:

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

In the next section we will, amongst many things, show that every extension of local fields can be written as an unramified extension followed by a totally ramified extension.

Recall the following: let R be a PID and M a finitely-generated R-module. Assume that M is torsion-free. Then there is a unique integer $n \geq 0$ such that $M \cong R^n$. We say n has *rank* n. Moreover, if $N \subseteq M$ is a submodule, then N is finitely-generated, so $N \cong R^m$ for some $m \leq n$.

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

Moreover, L is also a local field.

Proof. Choose a K-basis $\alpha_1, \cdots, \alpha_n$ of L. Let $\|\cdot\|$ denote the maximum norm on L.

$$\left\|\sum_{i=1}^n x_i\alpha_i\right\| = \max_{i=1,\dots,n}|x_i|$$

as before. Again, we know that $\|\cdot\|$ is equivalent to the extended norm $|\cdot|$ on L as K-norms. So we can find $r > s > 0$ such that

$$M = \{x \in L : \|x\| \leq s\} \subseteq \mathcal{O}_L \subseteq N = \{x \in L : \|x\| \leq r\}.$$

Increasing r and decreasing s if necessary, we wlog $r = |a|$ and $s = |b|$ for some $a, b \in K$.

Then we can write

$$M = \bigoplus_{i=1}^n \mathcal{O}_k b\alpha_i \subseteq \mathcal{O}_L \subseteq N = \bigoplus_{i=1}^n \mathcal{O}_K a\alpha_i.$$

We know that N is finitely generated and free of rank n over $\mathcal{O}_K$, and so is M. So $\mathcal{O}_L$ must be finitely generated and free of rank n over $\mathcal{O}_K$.

Since $\mathfrak{m}_k = \mathfrak{m}_k \cap \mathcal{O}_K$, we have a natural injection

$$\frac{\mathcal{O}_K}{\mathfrak{m}_k} \hookrightarrow \frac{\mathcal{O}_L}{\mathfrak{m}_L} = k_L.$$

Since $\mathcal{O}_L$ is generated over $\mathcal{O}_K$ by n elements, we know that k_K is generated by n elements over k_K, so it has rank at most n.

To see that L is a local field, we know that k_L/k_K is finite and k_K is finite, so k_L is finite. It is complete under the norm because it is a finite-dimensional vector space over a complete field.

Finally, to see that the valuation is discrete, suppose we have a normalized valuation on K, and w the unique extension of v_K to L. Then we have

$$w(\alpha) = \frac{1}{n} v_K(N_{L/K}(\alpha)).$$

So we have

$$w(L^\times) \subseteq \frac{1}{n} v(K^\times) = \frac{1}{n}\mathbb{Z}.$$

So it is discrete. □

Note that we cannot just pick an arbitrary basis of L/K and scale it to give a basis of $\mathcal{O}_L/\mathcal{O}_K$. For example, $\mathbb{Q}_2(\sqrt{2})/\mathbb{Q}_2$ has basis $1, \sqrt{2}$, but $|\sqrt{2}| = \frac{1}{\sqrt{2}}$ and cannot be scaled to 1 by an element in $\mathbb{Q}_2$.

Even if such a scaled basis exists, it doesn't necessarily give a basis of the integral rings. For example, $\mathbb{Q}_3(\sqrt{-1})/\mathbb{Q}_3$ has a $\mathbb{Q}_3$-basis $1, 1 + 3\sqrt{-1}$ and $|1 + 3\sqrt{-1}| = 1$, but

$$\sqrt{-1} \notin \mathbb{Z}_3 + \mathbb{Z}_3(1 + 3\sqrt{-1}).$$

So this is not a basis of $\mathcal{O}_{\mathbb{Q}_3(\sqrt{-1})}$ over $\mathbb{Z}_3$.

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

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

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

Proof. We will be lazy and write $e = e_{L/K}$ and $f = f_{L/K}$. We first note that k_L/k_K is separable, so there is some $\bar{\alpha} \in k_L$ such that $k_L = k_K(\bar{\alpha})$ by the primitive element theorem. Let

$$\bar{f}(x) \in k_K[x]$$

be the minimal polynomial of $\bar{\alpha}$ over k_K and let $f \in \mathcal{O}_L[x]$ be a monic lift of $\bar{f}$ with $\deg f = \deg \bar{f}$.

We first claim that there is some $\alpha \in \mathcal{O}_L$ lifting $\bar{\alpha}$ such that $v_L(f(\alpha)) = 1$ (note that it is always ≥ 1). To see this, we just take any lift β. If $v_L(f(\beta)) = 1$, then we are happy and set $\alpha = \beta$. If it doesn't work, we set $\alpha = \beta + \pi_L$, where π_L is the uniformizer of L.

Then we have

$$f(\alpha) = f(\beta + \pi_L) = f(\beta) + f'(\beta)\pi_L + b\pi_L^2$$

for some $b \in \mathcal{O}_L$, by Taylor expansion around β. Since $v_L(f(\beta)) \geq 2$ and $v_L(f'(\beta)) = 0$ (since $\bar{f}$ is separable, we know $f'(\beta)$ does not vanish when we reduce mod $\mathfrak{m}$), we know $v_L(f(\alpha)) = 1$. So $f(\alpha)$ is a uniformizer of L.

We now claim that the elements $\alpha^i\pi^j$ for $i = 0, \cdots, f-1$ and $j = 0, \cdots, e-1$ are an $\mathcal{O}_K$-basis of $\mathcal{O}_L$. Suppose we have

$$\sum_{i,j} a_{ij}\alpha^i\pi^j = 0$$

for some $a_{ij} \in K$ not all 0. We put

$$s_j = \sum_{i=0}^{f-1} a_{ij}\alpha^i.$$

We know that $1, \alpha, \cdots, \alpha^{f-1}$ are linearly independent over K since their reductions are linearly independent over k_K. So there must be some j such that $s_j \neq 0$.

The next claim is that if $s_j \neq 0$, then $e \mid v_L(s_j)$. We let k be an index for which $|a_{kj}|$ is maximal. Then we have

$$a_{kj}^{-1}s_j = \sum_{i=0}^{f-1} a_{kj}^{-1}a_{ij}\alpha^i.$$

Now note that by assumption, the coefficients on the right have absolute value ≤ 1, and is 1 when $i = k$. So we know that

$$a_{kj}^{-1}s_j \not\equiv 0 \mod \pi_L,$$

because $1, \bar{\alpha}, \cdots, \bar{\alpha}^{f-1}$ are linearly independent. So we have

$$v_L(a_{kj}^{-1}s_j) = 0.$$

So we must have

$$v_L(s_j) = v_L(a_{kj}) + v_L(a_{kj}^{-1}s_j) \in v_L(K^\times) = ev_L(L^\times) = e\mathbb{Z}.$$

Now we write

$$\sum a_{ij}\alpha^i\pi^j = \sum_{j=0}^{e-1} s_j\pi^j = 0.$$

If $s_j \neq 0$, then we have $v_L(s_j\pi^j) = v_L(s_j) + j \in j + e\mathbb{Z}$. So no two non-zero terms in $\sum_{j=0}^{e-1} s_j\pi^j$ have the same valuation. This implies that $\sum_{j=0}^{e-1} s_j\pi^j \neq 0$, which is a contradiction.

We now want to prove that

$$\mathcal{O}_L = \bigoplus_{i,j} \mathcal{O}_K\alpha^i\pi^j.$$

We let

$$M = \bigoplus_{i,j} \mathcal{O}_K\alpha^i\pi^j,$$

and put

$$N = \bigoplus_{i=0}^{f-1} \mathcal{O}_L\alpha^i.$$

Then we have

$$M = N + \pi N + \pi^2 N + \cdots + \pi^{e-1}N.$$

We are now going to use the fact that $1, \bar{\alpha}, \cdots, \bar{\alpha}^{f-1}$ span k_L over k_K. So we must have that $\mathcal{O}_L = N + \pi\mathcal{O}_L$. We iterate this to obtain

$$\begin{aligned}
\mathcal{O}_L &= N + \pi(N + \mathcal{O}_L)\\
&= N + \pi N + \pi^2\mathcal{O}_L\\
&= \cdots\\
&= N + \pi N + \pi^2 N + \cdots + \pi^{e-1}N + \pi^n\mathcal{O}_L\\
&= M + \pi_K\mathcal{O}_L,
\end{aligned}$$

using the fact that π_K and π^e have the same valuation, and thus they differ by a unit in $\mathcal{O}_L$. Iterating this again, we have

$$\mathcal{O}_L = M + \pi_k^n\mathcal{O}_L$$

for all $n \geq 1$. So M is dense in $\mathcal{O}_L$. But M is the closed unit ball in the subspace

$$\bigoplus_{i,j} K\alpha^i\pi^j \subseteq l$$

with respect to the maximum norm with respect to the given basis. So it must be complete, and thus $M = \mathcal{O}_L$.

Finally, since $\alpha^i\pi^j = \alpha^i f(\alpha)^j$ is a polynomial in α, we know that $\mathcal{O}_L = \mathcal{O}_K[\alpha]$. □

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

$$\begin{aligned}
f_{M/K} &= f_{L/K}f_{M/L}\\
e_{M/K} &= e_{L/K}e_{M/L}
\end{aligned}$$

Proof. The multiplicativity of $f_{M/K}$ follows from the tower law for the residue fields, and the multiplicativity of $e_{M/K}$ follows from the tower law for the local fields and that $f_{M/K}e_{M/K} = [M : K]$. □

5.2 Unramified extensions

Unramified extensions are easy to classify, since they just correspond to extensions of the residue field.

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

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

Proof. We start with existence. Let $\bar{\alpha}$ be a primitive element of ℓ/k_K with minimal polynomial $\bar{f} \in k_K[x]$. Take a monic lift $f \in \mathcal{O}_K[x]$ of $\bar{f}$ such that $\deg f = \deg \bar{f}$. Note that since $\bar{f}$ is irreducible, we know f is irreducible. So we can take $L = K(\alpha)$, where α is a root of f (i.e. $L = K[x]/f$). Then we have

$$[L : K] = \deg f = \deg(\bar{f}) = [\ell : k_K].$$

Moreover, k_L contains a root of $\bar{f}$, namely the reduction α. So there is an embedding $\ell \hookrightarrow k_L$, sending $\bar{\alpha}$ to the reduction of α. So we have

$$[k_L : k_K] \geq [\ell : k_L] = [L : K].$$

So L/K must be unramified and $k_L \cong \ell$ over k_K.

Uniqueness and the Galois property follow from the following lemma: □

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

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

given in one direction by restriction followed by reduction.

Proof. By the uniqueness of extended absolute values, any K-algebra homomorphism $\varphi : L \hookrightarrow M$ is an isometry for the extended absolute values. In particular, we have $\varphi(\mathcal{O}_L) \subseteq \mathcal{O}_M$ and $\varphi(\mathfrak{m}_L) \subseteq \mathfrak{m}_M$. So we get an induced k_K-algebra homomorphism $\bar{\varphi} : k_L \to k_M$.

So we obtain a map

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

To see this is bijective, we take a primitive element $\bar{\alpha} \in k_L$ over k_K, and take a minimal polynomial $\bar{f} \in k_K[x]$. We take a monic lift of $\bar{f}$ to $\mathcal{O}_k[x]$, and $\alpha \in \mathcal{O}_L$ the unique root of f which lifts $\bar{\alpha}$, which exists by Hensel's lemma. Then by counting dimensions, the fact that the extension is unramified tells us that

$$k_L = k_K(\bar{\alpha}), \quad L = K(\alpha).$$

So we can construct the following diagram:

$$\begin{array}{ccccc} \varphi & & \mathrm{Hom}_{K\text{-}\mathrm{Alg}} & \xrightarrow{\text{reduction}} & \mathrm{Hom}_{k_K\text{-}\mathrm{Alg}}(k_L, k_M) & & \bar{\varphi} \\ \big\downarrow & & \big\downarrow \cong & & \big\downarrow \cong & & \big\downarrow \\ \varphi(\alpha) & & \{x \in M : f(x) = 0\} & \xrightarrow{\text{reduction}} & \{\bar{x} \in k_M : \bar{f}(\bar{x})\} & & \bar{\varphi}(\bar{\alpha}) \end{array}$$

But the bottom map is a bijection by Hensel's lemma. So done. □

Alternatively, given a map $\bar{\varphi} : k_L \to k_M$, we can lift it to the map $\varphi : L \to M$ given by

$$\varphi\left(\sum [a_n]\pi_k^n\right) = \sum [\bar{\varphi}(a_n)]\pi_k^n,$$

using the fact that π_k^n is a uniformizer in L since the extension is unramified. So we get an explicit inverse.

Proof of theorem (continued). To finish off the proof of the theorem, we just note that an isomorphism $\bar{\varphi} : k_L \cong k_M$ over k_K between unramified extensions. Then $\bar{\varphi}$ lifts to a K-embedding $\varphi : L \hookrightarrow M$ and $[L : K] = [M : K]$ implies that φ is an isomorphism.

To see that the extension is Galois, we just notice that

$$|\operatorname{Aut}_K(L)| = |\operatorname{Aut}_{k_K}(k_L)| = [k_L : k_K] = [L : K].$$

So L/K is Galois. Moreover, the map $\operatorname{Aut}_K(L) \to \operatorname{Aut}_{k_K}(k_L)$ is really a homomorphism, hence an isomorphism. □

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

Proof. Let $\bar{\alpha}$ be a primitive element of k_K/k_L, and $\bar{f} \in k_K[x]$ a minimal polynomial of $\bar{\alpha}$, and $f \in \mathcal{O}_k[x]$ a monic lift of $\bar{f}$, and $\alpha \in \mathcal{O}_L$ a unique lift of f lifting $\bar{\alpha}$. Then $L = K(\alpha)$. So $LM = M(\alpha)$.

Let $\bar{g}$ be the minimal polynomial of $\bar{\alpha}$ over k_M. Then $\bar{g} \mid \bar{f}$. By Hensel's lemma, we can factorize $f = gh$ in $\mathcal{O}_M[x]$, where g is monic and lifts $\bar{g}$. Then $g(\alpha) = 0$ and g is irreducible in $M[x]$. So g is the minimal polynomial of α over M. So we know that

$$[LM : M] = \deg g = \deg \bar{g} \leq [k_{LM} : k_M] \leq [LM : M].$$

So we have equality throughout and LM/M is unramified.

The second assertion follows from the multiplicativity of $f_{L/K}$, as does the third. □

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

Proof. Let T/K be the unique unramified extension with residue field extension k_L/k_K. Then $\mathrm{id} : k_T = k_L \to k_L$ lifts to a K-embedding $T \hookrightarrow L$. Identifying T with its image, we know

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

Now if T' is any other unramified extension, then $T'T$ is an unramified extension over K, so

$$[T : K] \leq [TT' : K] \leq f_{L/K} = [T : K].$$

So we have equality throughout, and $T' \subseteq T$. So this is maximal. □

5.3 Totally ramified extensions

We now quickly look at totally ramified extensions. Recall the following irreducibility criterion:

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

Proof. Left as an exercise. You've probably seen this already in a much more general context, but in this case there is a neat proof using Newton polygons. □

We will need to use the following characterization of the ramification index:

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

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

Proof. We know w and v_L differ by a constant. To figure out what this is, we have

$$1 = w(\pi_K) = e_{L/K}^{-1} v_L(\pi_K).$$

So for any $x \in L$, we have

$$w(x) = e_{L/K}^{-1} v_L(x).$$

In particular, putting $x = \pi_L$, we have

$$w(\pi_L) = e_{L/K}^{-1} v_L(\pi_L) = e_{L/K}^{-1}.$$

The equality

$$w(\pi_L) = \min\{w(x) : x \in \mathfrak{m}_L\},$$

is trivially true because the minimum is attained by π_L. □

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

We can now state the proposition:

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

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

Proof. Let $n = [L : K]$, v_K be the valuation of K, and w the unique extension to L. Then

$$[K(\pi_L) : K]^{-1} \leq e_{K(\pi_L)/K}^{-1} = \min_{x \in \mathfrak{m}_{K(\pi_L)}} w(c) \leq \frac{1}{n},$$

where the last inequality follows from the fact that $\pi_L \in \mathfrak{m}_{L(\pi_L)}$.

But we also know that

$$[K(\pi_L) : K] \leq [L : K].$$

So we know that $L = K(\pi_L)$.

Now let $f(x) = x^n + a_{n-1}x^{n-1} + \cdots + a_0 \in \mathcal{O}_K[x]$ be the minimal polynomial of π_L/K. Then we have

$$\pi_L^n = -(a_0 + a_1\pi_L + \cdots + a_{n-1}\pi_L^{n-1}).$$

So we have

$$1 = w(\pi_L^n) = w(a_0 + a_1\pi_L + \cdots + a_{n-1}\pi_L^{n-1}) = \min_{i=0,\ldots,n-1}\left(v_k(a_i) + \frac{i}{n}\right).$$

This implies that $v_K(a_i) \geq 1$ for all i, and $v_K(x_0) = 1$. So it is Eisenstein.

For the converse, if $K = K(\alpha)$ and $n = [L : K]$, take

$$g(x) = x^n + b_{n-1}x^{n-1} + .. + b_0 \in \mathcal{O}_K[x]$$

be the minimal polynomial of α. So all roots have the same valuation. So we have

$$1 = w(b_0) = n \cdot w(\alpha).$$

So we have $w(\alpha) = \frac{1}{n}$. So we have

$$e_{L/K}^{-1} = \min_{x \in \mathfrak{m}_L} w(x) \leq \frac{1}{n} = [L : K]^{-1}.$$

So $[L : K] = e_{L/K} = n$. So L/K is totally ramified and α is a uniformizer. □

In fact, more is true. We have $\mathcal{O}_L = \mathcal{O}_K[\pi_L]$.

6 Further ramification theory

6.1 Some filtrations

If we have a field K, then we have a unit group $U_K = \mathcal{O}_K^\times$. We would like to come up with a *filtration* of subgroups of the unit group, namely a sequence

$$\cdots \subseteq U_K^{(2)} \subseteq U_K^{(1)} \subseteq U_K^{(0)} = U_K$$

of subgroups that tells us how close a unit is to being 1. The further down we are in the chain, the closer we are to being 1.

Similarly, given a field extension L/K, we want a filtration on the Galois group (the indexing is conventional)

$$\cdots \subseteq G_2(L/K) \subseteq G_1(L/K) \subseteq G_0(L/K) \subseteq G_{-1}(L/K) = \mathrm{Gal}(L/K).$$

This time, the filtration tells us how close the automorphisms are to being the identity map.

The key thing about these filtrations is that we can figure out information about the quotients $U_K^{(s)}/U_K^{(s+1)}$ and $G_s(L/K)/G_{s+1}(L/K)$, which is often easier. Later, we might be able to patch these up to get more useful information about U_K and $\mathrm{Gal}(L/K)$.

We start with the filtration of the unit group.

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

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

The quotients of these units groups are surprisingly simple:

Proposition. We have

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

for $s \geq 1$.

Proof. We have a surjective homomorphism $\mathcal{O}_K^\times \to k_K^\times$ which is just reduction mod π_K, and the kernel is just things that are 1 modulo π_K, i.e. $U_K^{(1)}$. So this gives the first part.

For the second part, we define a surjection $U_K^{(s)} \to k_K$ given by

$$1 + \pi_K^s x \mapsto x \mod \pi_k.$$

This is a group homomorphism because

$$(1 + \pi_K^s x)(1 + \pi_K^s y) = 1 + \pi^S(x + y + \pi^s xy),$$

and this gets mapped to

$$x + y + \pi^s x + y \cong x + y \mod \pi_K.$$

Then almost by definition, the kernel is $U_K^{(s+1)}$. □

The next thing to consider is a filtration of the Galois group.

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

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

So if you belong to G_s for a large s, then you move things less. Note that we could have defined these only for $s \in \mathbb{Z}_{\geq -1}$, but allowing fractional indices will be helpful in the future.

Now since $\sigma(x) - x \in \mathcal{O}_L$ for all $x \in \mathcal{O}_L$, we know

$$G_{-1}(L/K) = \mathrm{Gal}(L/K).$$

We next consider the case of $G_0(L/K)$. This is, by definition

$$\begin{aligned} G_0(L/K) &= \{\sigma \in \mathrm{Gal}(L/K) : v_L(\sigma(x) - x) \geq 1 \text{ for all } x \in \mathcal{O}_L\} \\ &= \{\sigma \in \mathrm{Gal}(L/K) : \sigma(x) \equiv x \bmod \mathfrak{m} \text{ for all } x \in \mathcal{O}_L\}. \end{aligned}$$

In other words, these are all the automorphisms that reduce to the identity when we reduce it to $\mathrm{Gal}(k_L/k_K)$.

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

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

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

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

given by reduction is surjective.

Proof. Let T/K be maximal unramified subextension. Then by Galois theory, the map $\mathrm{Gal}(L/K) \to \mathrm{Gal}(T/K)$ is a surjection. Moreover, we know that $k_T = k_L$. So we have a commutative diagram

$$\begin{array}{ccc} \mathrm{Gal}(L/K) & \longrightarrow & \mathrm{Gal}(k_L/k_K) \\ \big\downarrow & & \big\| \\ \mathrm{Gal}(T/K) & \xrightarrow{\sim} & \mathrm{Gal}(k_T/k_K). \end{array}$$

So the map $\mathrm{Gal}(L/K) \to \mathrm{Gal}(k_L/k_K)$ is surjective. □

Then the inertia group is trivial iff L/K is unramified. The field T is sometimes called the *inertia field*.

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

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

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

Proof. Consider the map $k_L \to \mathcal{O}_L$ given by

$$f : x \mapsto \sigma^{-1}([\bar{\sigma}(x)]).$$

This is multiplicative, because every term is multiplicative, and

$$\sigma^{-1}([\bar{\sigma}(x)]) \equiv x \mod \pi_L.$$

So this map f has to be the Teichmüller lift by uniqueness. □

That's all we're going to say about the inertia group. We now consider the general properties of this filtration.

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

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

given by

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

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

Proof. We define the map

$$\begin{aligned} \phi : G_s(L/K) &\to \frac{U_L^{(s)}}{U_L^{(s+1)}} \\ \sigma &\mapsto \sigma(\pi_L)/\pi_L. \end{aligned}$$

We want to show that this has kernel $G_{s+1}(L/K)$.

First we show it is well-defined. If $\sigma \in G_s(L/K)$, we know

$$\sigma(\pi_L) = \pi_L + \pi_L^{s+1} x$$

for some $x \in \mathcal{O}_L$. So we know

$$\frac{\sigma(\pi_L)}{\pi_L} = 1 + \pi_L^s x \in U_L^{(s)}.$$

So it has the right image. To see this is independent of the choice of π_L, we let $u \in \mathcal{O}_L^\times$. Then $\sigma(u) = u + \pi_L^{s+1} y$ for some $y \in \mathcal{O}_L$.

Since any other uniformizer must be of the form $\pi_L u$, we can compute

$$\begin{aligned} \frac{\sigma(\pi_L u)}{\pi_L u} &= \frac{(\pi_L + \pi_L^{s+1})(u + \pi_L^{s+1} y)}{\pi_L u} \\ &= (1 + \pi_L^s x)(1 + \pi_L^{s+1} u^{-1} y) \\ &\equiv 1 \pi_L^s x \pmod{U_L^{s+1}}. \end{aligned}$$

So they represent the same element in in $U_L^{(s)}/U_L^{(s+1)}$.

To see this is a group homomorphism, we know

$$\phi(\sigma\tau) = \frac{\sigma(\tau(\pi_L))}{\pi_L} = \frac{\sigma(\tau(\pi_L))}{\tau(\pi_L)}\frac{\tau(\pi_L)}{\pi_L} = \phi(\sigma)\phi(t),$$

using the fact that $\tau(\pi_L)$ is also a uniformizer.

Finally, we have to show that $\ker\phi = G_{s+1}(L/K)$. We write down

$$\ker\phi = \{\sigma \in G_s(L/K) : v_L(\sigma(\pi_L) - \pi_L) \geq s+2\}.$$

On the other hand, we have

$$G_{s+1}(L/K) = \{\sigma \in G_s(L/K) : v_L(\sigma(z) - z) \geq s+2 \text{ for all } z \in \mathcal{O}_L\}.$$

So we trivially have $G_{s+1}(L/K) \subseteq \ker\phi$. To show the converse, let $x \in \mathcal{O}_L$ and write

$$x = \sum_{n=0}^{\infty} [x_n]\pi_L^n.$$

Take $\sigma \in \ker\phi \subseteq G_s(L/K) \subseteq I(L/K)$. Then we have

$$\sigma(\pi_L) = \pi_L + \pi_L^{s+2}y, \quad y \in \mathcal{O}_L.$$

Then by the previous lemma, we know

$$\begin{aligned}\sigma(x) - x &= \sum_{n=1}^{\infty}[x_n]\left((\sigma(\pi_L))^n - \pi_L^n\right)\\ &= \sum_{n=1}^{\infty}[x_n]\left((\pi_L + \pi_L^{s+2}y)^n - \pi_L^n\right)\\ &= \pi_L^{s+2}(\text{things}).\end{aligned}$$

So we know $v_L(\sigma(x) - x) \geq s+2$. □

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

Proof. Note that

$$\bigcap_s G_s(L/K) = \{\mathrm{id}\}.$$

So $(G_s(L/K))_{s\in\mathbb{Z}_{\geq -1}}$ is a subnormal series of $\mathrm{Gal}(L/K)$, and all quotients are abelian, because they embed into $\frac{U_L^{(s)}}{U_L^{(s+1)}} \cong (k_K, +)$ (and $s = -1$ can be checked separately). □

Thus if L/K is a finite extension of local fields, then we have, for $s \geq 1$, injections

$$\frac{G_s(L/K)}{G_{s+1}(L/K)} \hookrightarrow k_L.$$

Since k_L is a p-group, it follows that

$$\frac{|G_s(L/K)|}{|G_{s+1}(L/K)|}$$

is a pth power. So it follows that for any t, the quotient

$$\frac{|G_1(L/K)|}{|G_t(L/K)|}$$

is also a pth power. However, we know that the intersection of all $G_s(L/K)$ is $\{\mathrm{id}\}$, and also $\mathrm{Gal}(L/K)$ is finite. So for sufficiently large t, we know that $|G_t(L/K)| = 1$. So we conclude that

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

We now use the injection

$$\frac{G_0(L/K)}{G_1(L/K)} \hookrightarrow k_L^\times,$$

and the fact that $k_L^\times$ has order prime to p. So $G_1(L/K)$ must be the Sylow p-subgroup of $G_0(L/K)$. Since it is normal, it must be the unique p-subgroup.

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

Suppose we have tower $M/L/K$ of finite extensions of local fields. How do the ramification groups of the different extensions relate? We first do the easy case.

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

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

Proof. We have

$$G_s(M/K) = \{\sigma \in \mathrm{Gal}(M/L) : v_M(\sigma x - x) \geq s + 1\} = G_s(M/K) \cap \mathrm{Gal}(M/L).$$

□

This is trivial, because the definition uses the valuation v_M of the bigger field all the time. What's more difficult and interesting is quotients, namely going from M/K to L/K.

We want to prove the following theorem:

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

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

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

To better understand the situation, it helps to provide an alternative characterization of the Galois group.

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

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

It is then immediate that

$$G_s(L/K) = \{\sigma \in \mathrm{Gal}(L/K) : i_{L/K}(\sigma) \geq s + 1\}.$$

This is not very helpful. We now claim that we can compute $i_{L/K}$ using the following formula:

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

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

Proof. Fix a σ. It is clear that $i_{L/K}(\sigma) \leq v_L(\sigma(\alpha) - \alpha)$. Conversely, for any $x \in \mathcal{O}_L$, we can find a polynomial $g \in \mathcal{O}_K[t]$ such that

$$x = g(\alpha) = \sum b_i \alpha^i,$$

where $b_i \in \mathcal{O}_K$. In particular, b_i is fixed by σ.

Then we have

$$\begin{aligned} v_L(\sigma(x) - x) &= v_L(\sigma g(\alpha) - g(\alpha)) \\ &= v_L\left(\sum_{i=1}^{n} b_i(\sigma(\alpha)^i - \alpha^i)\right) \\ &\geq v_L(\sigma(\alpha) - \alpha), \end{aligned}$$

using the fact that $\sigma(\alpha) - \alpha \mid \sigma(\alpha)^i - \alpha^i$ for all i. So done. □

Now if $M/L/K$ are finite Galois extensions of local fields, then $\mathcal{O}_M = \mathcal{O}_K[\alpha]$ implies $\mathcal{O}_M = \mathcal{O}_L[\alpha]$. So for $\sigma \in \mathrm{Gal}(M/L)$, we have

$$i_{M/L}(\sigma) = i_{M/K}(\sigma).$$

Going in the other direction is more complicated.

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

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

Here $e_{M/L}$ is just to account for the difference between v_L and v_M. So the real content is that the value of $i_{L/K}(\sigma)$ is the sum of the values of $i_{M/K}(\tau)$ for all τ that restrict to σ.

Proof. If $\sigma = 1$, then both sides are infinite by convention, and equality holds. So we assume $\sigma \neq 1$. Let $\mathcal{O}_M = \mathcal{O}_L[\alpha]$ and $\mathcal{O}_L = \mathcal{O}_K[\beta]$, where $\alpha \in \mathcal{O}_M$ and $\beta \in \mathcal{O}_L$. Then we have

$$e_{M/L} i_{L/K}(\sigma) = e_{M/L} v_L(\sigma\beta - \beta) = v_M(\sigma\beta - \beta).$$

Now if $\tau \in \mathrm{Gal}(M/K)$, then

$$i_{M/K}(\tau) = v_M(\tau\alpha - \alpha)$$

Now fix a τ such that $\tau|_L = \sigma$. We set $H = \mathrm{Gal}(M/L)$. Then we have

$$\sum_{\tau' \in \mathrm{Gal}(M/K), \tau'|_L = \sigma} i_{M/K}(\tau') = \sum_{g \in H} v_M(\tau g(\alpha) - \alpha) = v_M\left(\prod_{g \in H} (\tau g(\alpha) - \alpha)\right).$$

We let

$$b = \sigma(\beta) - \beta = \tau(\beta) - \beta$$

and

$$a = \prod_{g \in H} (\tau g(\alpha) - \alpha).$$

We want to prove that $v_M(b) = v_M(a)$. We will prove that $a \mid b$ and $b \mid a$.

We start with a general observation about elements in $\mathcal{O}_L$. Given $z \in \mathcal{O}_L$, we can write

$$z = \sum_{i=1}^{n} z_i \beta^i, \quad z_i \in \mathcal{O}_K.$$

Then we know

$$\tau(z) - z = \sum_{i=1}^{n} z_i(\tau(\beta)^i - \beta^i)$$

is divisible by $\tau(\beta) - \beta = b$.

Now let $F(x) \in \mathcal{O}_L[x]$ be the minimal polynomial of α over L. Then explicitly, we have

$$F(x) = \prod_{g \in H} (x - g(\alpha)).$$

Then we have

$$(\tau F)(x) = \prod_{g \in H} (x - \tau g(\alpha)),$$

where τF is obtained from F by applying τ to all coefficients of F. Then all coefficients of $\tau F - F$ are of the form $\tau(z) - z$ for some $z \in \mathcal{O}_L$. So it is divisible by b. So b divides every value of this polynomial, and in particular

$$b \mid (\tau F - F)(\alpha) = \prod_{g \in H} (\alpha - g(\alpha)) = \pm a,$$

So $b \mid a$.

In other direction, we pick $f \in \mathcal{O}_K[x]$ such that $f(\alpha) = \beta$. Then $f(\alpha) - \beta = 0$. This implies that the polynomial $f(x) - \beta$ divides the minimal polynomial of α in $\mathcal{O}_L[x]$. So we have

$$f(x) - \beta = F(x)h(x)$$

for some $h \in \mathcal{O}_L[x]$.

Then noting that f has coefficients in $\mathcal{O}_K$, we have

$$(f - \tau\beta)(x) = (\tau f - \tau b)(x) = (\tau F)(x)(\tau h)(x).$$

Finally, set $x = \alpha$. Then

$$-b = \beta - \tau\beta = \pm a(\tau h)(\alpha).$$

So $a \mid b$. □

Now that we understand how the $i_{L/K}$ behave when we take field extensions, we should be able to understand how the ramification groups behave!

We now write down the right choice of $\eta_{L/K} : [-1, \infty) \to [-1, \infty)$:

$$\eta_{L/K}(s) = \left(e_{L/K}^{-1} \sum_{\sigma \in G} \min(i_{L/K}(\sigma), s+1) \right) - 1.$$

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

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

Then we have

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

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

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

Proof. Let $G = \mathrm{Gal}(M/K)$. Fix a $\sigma \in \mathrm{Gal}(L/K)$. We let $\tau \in \mathrm{Gal}(M/K)$ be an extension of σ to M that maximizes $i_{M/K}$, i.e.

$$i_{M/K}(\tau) \geq i_{M/K}(\tau g)$$

for all $g \in H$. This is possible since H is finite.

We claim that

$$i_{L/K}(\sigma) - 1 = \eta_{M/L}(i_{M/K}(\tau) - 1).$$

If this were true, then we would have

$$\begin{aligned} \sigma \in \frac{G_s(M/K)H}{H} &\Leftrightarrow \tau \in G_s(M/K) \\ &\Leftrightarrow i_{M/K}(\tau) - 1 \geq s \end{aligned}$$

Since $\eta_{M/L}$ is strictly increasing, we have

$$\begin{aligned} &\Leftrightarrow \eta_{M/L}(i_{M/K}(\tau) - 1) \geq \eta_{M/L}(s) = t \\ &\Leftrightarrow i_{L/K}(\sigma) - 1 \geq t \\ &\Leftrightarrow \sigma \in G_t(L/K), \end{aligned}$$

and we are done.

To prove the claim, we now use our known expressions for $i_{L/K}(\sigma)$ and $\eta_{M/L}(i_{M/K}(\tau) - 1)$ to rewrite it as

$$e_{M/L}^{-1} \sum_{g \in H} i_{M/K}(\tau g) = e_{M/L}^{-1} \sum_{g \in H} \min(i_{M/L}(g), i_{M/K}(\tau)).$$

We then make the *stronger* claim

$$i_{M/K}(\tau g) = \min(i_{M/L}(g), i_{M/K}(\tau)).$$

We first note that

$$\begin{aligned} i_{M/K}(\tau g) &= v_M(\tau g(\alpha) - \alpha) \\ &= v_M(\tau g(\alpha) - g(\alpha) + g(\alpha) - \alpha) \\ &\geq \min(v_M(\tau g(\alpha) - g(\alpha)), v_M(g(\alpha) - \alpha)) \\ &= \min(i_{M/K}(\tau), i_{M/K}(g)) \end{aligned}$$

We cannot conclude our (stronger) claim yet, since we have a $\geq$ in the middle. We now have to split into two cases.

(i) If $i_{M/K}(g) \geq i_{M/K}(\tau)$, then the above shows that $i_{M/K}(\tau g) \geq i_{M/K}(\tau)$. But we also know that it is bounded above by m. So $i_{M/K}(\tau g) = i_{M/K}(\tau)$. So our claim holds.

(ii) If $i_{M/K}(g) < i_{M/K}(\tau)$, then the above inequality is in fact an equality as the two terms have different valuations. So our claim also holds.

So done. □

We now prove an alternative characterization of the function $\eta_{L/K}$, using a funny integral.

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

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

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

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

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

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

Proof. We denote the RHS by $\theta(s)$. It is clear that both $\eta_{L/K}(s)$ and $\theta(s)$ are piecewise linear and the break points are integers (since $i_{L/K}(\sigma)$ is always an integer). So to see they are the same, we see that they agree at a point, and that they have equal derivatives. We have

$$\eta_{L/K}(0) = \frac{|\{\sigma \in G : i_{L/K}(\sigma) \geq 1\}|}{e_{L/K}} - 1 = 0 = \theta(0),$$

since the numerator is the size of the inertia group.

If $s \in [-1, \infty) \setminus \mathbb{Z}$, then

$$\begin{aligned} \eta'_{L/K}(s) &= e_{L/K}^{-1}(|\{\sigma \in G : i_{L/K}(\sigma) \geq s + 1\}|) \\ &= \frac{|G_s(L/K)|}{|G_0(L/K)|} \\ &= \frac{1}{(G_0(L/K) : G_s(L/K))} \\ &= \theta'(s). \end{aligned}$$

So done. □

We now tidy up the proof by inventing a different numbering of the ramification groups. Recall that

$$\eta_{L/K} : [-1, \infty) \to [-1, \infty)$$

is continuous, strictly increasing, and

$$\eta_{L/K}(-1) = -1, \quad \eta_{L/K}(s) \to \infty \text{ as } s \to \infty.$$

So this is invertible. We set

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*.

To rephrase our previous theorem using the upper numbering, we need a little lemma:

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

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

Hence

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

Proof. Let $s \in [-1, \infty)$, and let $t = \eta_{M/L}(s)$, and $H = \mathrm{Gal}(M/L)$. By Herbrand's theorem, we know

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

Thus by multiplicativity of the inertia degree, we have

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

By the fundamental theorem of calculus, we know that whenever the derivatives make sense, we have

$$\eta'_{M/K}(s) = \frac{|G_s(M/K)|}{e_{M/K}}.$$

So putting this in, we know

$$\eta'_{M/K}(s) = \eta'_{L/K}(t)\eta'_{M/L}(s) = (\eta_{L/K} \circ \eta_{M/L})'(s).$$

Since $\eta_{M/K}$ and $\eta_{L/K} \circ \eta_{M/L}$ agree at 0 (they both take value 0), we know that the functions must agree everywhere. So done. □

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

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

Proof. Put $s = \eta_{L/K}(t)$. Then by Herbrand's theorem, we have

$$\begin{aligned}\frac{G^t(M/K)H}{H} &= \frac{G_{\psi_{M/K}(t)}(M/K)H}{H}\\ &\cong G_{\eta_{M/L}(\psi_{M/K}(t))}(L/K)\\ &= G_s(L/K)\\ &= G^t(L/K).\end{aligned}$$

□

This upper numbering might seem like an unwieldy beast that was invented just so that our theorem looks nice. However, it turns out that often the upper numberings are rather natural, as we could see in the example below:

Example. Consider ζ_{p^n} a primitive p^nth root of unity, and $K = \mathbb{Q}_p(\zeta_{p^n})$. The minimal polynomial of ζ_{p^n} is the p^nth cyclotomic polynomial

$$\Phi_{p^n}(x) = x^{p^{n-1}(p-1)} + x^{p^{n-1}(p-2)} + \cdots + 1.$$

It is an exercise on the example sheet to show that this is indeed irreducible. So $K/\mathbb{Q}_p$ is a Galois extension of degree $p^{n-1}(p-1)$. Moreover, it is totally ramified by question 6 on example sheet 2, with uniformizer

$$\pi = \zeta_{p^n} - 1$$

is a uniformizer. So we know

$$\mathcal{O}_K = \mathbb{Z}_p[\zeta_{p^n} - 1] = \mathbb{Z}_p[\zeta_{p^n}].$$

We then have an isomorphism

$$\left(\frac{\mathbb{Z}}{p^n\mathbb{Z}}\right)^\times \to \mathrm{Gal}(L/\mathbb{Q}_p)$$

obtained by sending $m \to \sigma_m$, where

$$\sigma_m(\zeta_{p^n}) = \zeta_{p^n}^m.$$

We have

$$\begin{aligned}i_{K/\mathbb{Q}_p}(\sigma_m) &= v_K(\sigma_m(\zeta_{p^n}) - \zeta_{p^n})\\ &= v_K(\zeta_{p^n}^m - \zeta_{p^n})\\ &= v_K(\zeta_{p^n}^{m-1} - 1)\end{aligned}$$

since ζ_{p^n} is a unit. If $m = 1$, then this thing is infinity. If it is not 1, then $\zeta_{p^n}^{m-1}$ is a primitive p^{n-k}th root of unity for the maximal k such that $p^k \mid m-1$. So by Q6 on example sheet 2, we have

$$v_K(\zeta_{p^n}^{m-1} - 1) = \frac{p^{n-1}(p-1)}{p^{n-k-1}(p-1)} = p^k.$$

Thus we have

$$v_K(\zeta_{p^n}^{m-1} - 1) \geq p^k \Leftrightarrow m \equiv 1 \bmod p^k.$$

It then follows that for

$$p^k \geq s + 1 \geq p^{k-1} + 1,$$

we have

$$G_s(K/\mathbb{Q}_p) \cong \{m \in (\mathbb{Z}/p^n)^\times : m \equiv 1 \bmod p^k\}.$$

Now $m \equiv 1 \bmod p^k$ iff $\sigma_m(\zeta_{p^k}) = \zeta_{p^k}$. So in fact

$$G_s(K/\mathbb{Q}_p) \cong \mathrm{Gal}(K/\mathbb{Q}_p(\zeta_{p^k})).$$

Finally, when $s \geq p^n - 1$, we have

$$G_s(K/\mathbb{Q}_p) = 1.$$

We claim that

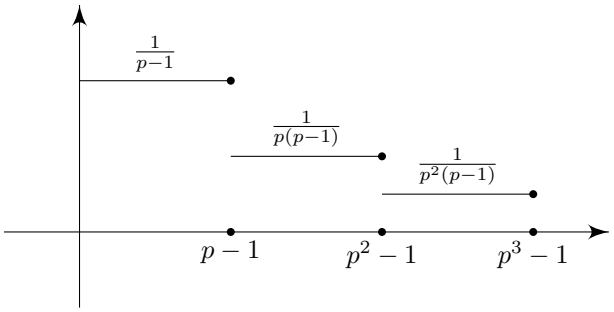
$$\eta_{K/\mathbb{Q}_p}(p^k - 1) = k.$$

So we have

$$G^k(K/\mathbb{Q}_p) = \mathrm{Gal}(K/\mathbb{Q}_p(\zeta_{p^k})).$$

This actually looks much nicer!

To actually compute $\eta_{K/\mathbb{Q}_p}$, we have notice that the function we integrate to get η looks something like this (not to scale):



The jumps in the lower numbering are at $p^k - 1$ for $k = 1, \cdots, n-1$. So we have

$$\begin{aligned}\eta_{K/\mathbb{Q}_p}(p^k - 1) &= (p-1)\frac{1}{p-1} + ((p^2-1) - (p-1))\frac{1}{p(p-1)} \\ &\quad + \cdots + ((p^k - 1) - (p^{k-1} - 1))\frac{1}{p^{k-1}(p-1)} \\ &= k.\end{aligned}$$

7 Local class field theory

Local class field theory is the study of abelian extensions of local fields, i.e. a Galois extension whose Galois group is abelian.

7.1 Infinite Galois theory

It turns out that the best way of formulating this theory is to not only use finite extensions, but infinite extensions as well. So we need to begin with some infinite Galois theory. We will mostly just state the relevant results instead of proving them, because this is not a course on Galois theory.

In this section, we will work with any field.

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

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

These are all the same definitions as in the finite case.

In finite Galois theory, the subgroups of $\mathrm{Gal}(L/K)$ match up with the intermediate extensions, but this is no longer true in the infinite case. The Galois group has too many subgroups. To fix this, we need to give $\mathrm{Gal}(L/K)$ a topology, and talk about closed subgroups.

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 $\sigma\,\mathrm{Gal}(M/L) \subseteq U$.

Note that any open subgroup of a topological group is automatically closed, but the converse does not hold.

Note that when M/K is finite, then the Krull topology is discrete, since we can just take the finite subextension to be M itself.

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

Groups with properties in this proposition are known as *profinite groups*.

Proof. We will not prove the first part.

For the last part, note that by definition, there is a finite subextension of M/K such that $\mathrm{Gal}(M/L) \subseteq U$. We then let L' be the Galois closure of L over K. Then $\mathrm{Gal}(M/L') \subseteq \mathrm{Gal}(M/L) \subseteq U$, and $\mathrm{Gal}(M/L')$ is open and normal. □

Recall that we previously defined the inverse limit of a sequence rings. More generally, we can define such an inverse limit for any sufficiently nice poset of things. Here we are going to do it for topological groups (for those doing Category Theory, this is the filtered limit of topological groups).

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 $i \leq k$ and $j \leq k$.

Example. Any total order is a directed system.

Example. $\mathbb{N}$ with divisibility $|$ as the partial order is a directed system.

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 $i \leq j$, such that

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

and

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

whenever $i \leq j \leq k$.

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

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

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.

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

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

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

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

is an isomorphism of topological groups.

We now state the main theorem of Galois theory.

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

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

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

is an isomorphism of topological groups.

Proof. This follows easily from the fundamental theorem for finite field extensions. We will only show that $\mathrm{Gal}(M/L)$ is closed and leave the rest as an exercise. We can write

$$L = \bigcup_{\substack{L' \subseteq L \\ L'/K \text{ finite}}} L'.$$

Then we have

$$\mathrm{Gal}(M/L) = \bigcap_{\substack{L' \subseteq L \\ L'/K \text{ finite}}} \mathrm{Gal}(M/L'),$$

and each $\mathrm{Gal}(M/L')$ is open, hence closed. So the whole thing is closed. □

7.2 Unramified extensions and Weil group

We first define what it means for an infinite extension to be unramified or totally ramified. To do so, we unexcitingly patch up the definitions for finite cases.

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.

Note that since the extension is not necessarily finite, in general M will not be a local field, since chances are its residue field would be infinite.

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.

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

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

via the reduction map.

Proof. Every finite subextension of M/K is unramified, so in particular is Galois. So M/K is Galois (because normality and separability is checked for each element). Then we have a commutative diagram

$$\begin{array}{ccc} \mathrm{Gal}(M/K) & \xrightarrow{\text{reduction}} & \mathrm{Gal}(k_M/k_K) \\ \downarrow\sim & & \downarrow\sim \\ \varprojlim_{L/K} \mathrm{Gal}(L/K) & \xrightarrow[\sim]{\text{reduction}} & \varprojlim_{L/K} \mathrm{Gal}(k_L/k_K) \end{array}$$

The left hand map is an isomorphism by (infinite) Galois theory, and since all finite subextensions of k_M/k_K are of the form k_L/k_K by our finite theory, we know the right-hand map is an isomorphism. The bottom map is an isomorphism since it is an isomorphism in each component. So the top map must be an isomorphism. □

Since the compositor of unramified extensions is unramified, it follows that any algebraic extension M/K has a maximal unramified subextension

$$T = T_{M/K}/K.$$

We now try to understand unramified extensions. For a finite unramified extension L/K, we have an isomorphism

$$\mathrm{Gal}(L/K) \xrightarrow{\sim} \mathrm{Gal}(k_L/k_K) \ ,$$

By general field theory, we know that $\mathrm{Gal}(k_L/k_K)$ is a cyclic group generated by

$$\mathrm{Frob}_{L/K} : x \mapsto x^q,$$

where $q = |k_K|$ is the size of k_K. So by the isomorphism, we obtain a generator of $\mathrm{Gal}(L/K)$.

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

There is also a geometric Frobenius, which is its inverse, but we will not use that in this course.

We know Frob is compatible in towers, i.e. if $M/L/K$ is a tower of finite unramified extension of local fields, then $\mathrm{Frob}_{M/K}|_L = \mathrm{Frob}_{L/K}$, since they both reduce to the map $x \mapsto x^{|k_K|}$ in $\mathrm{Gal}(k_L/k_K)$, and the map between $\mathrm{Gal}(k_L/k_K)$ and $\mathrm{Gal}(L/K)$ is a bijection.

So if M/K is an arbitrary unramified extension, then we have an element

$$(\mathrm{Frob}_{L/K}) \in \varprojlim_{L/K} \mathrm{Gal}(L/K) \cong \mathrm{Gal}(M/K).$$

So we get an element $\mathrm{Frob}_{M/K} \in \mathrm{Gal}(M/K)$. By tracing through the proof of $\mathrm{Gal}(M/K) \cong \mathrm{Gal}(k_M/k_K)$, we see that this is the unique lift of $x \mapsto x^{|k_K|}$.

Note that the Galois group $\mathrm{Gal}(M/K)$ need not be generated by the Frobenius in the case of an infinite extension. We are now going to restrict to the subgroup of $\mathrm{Gal}(M/K)$ that consists of things generated by the Frobenius.

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 $\sigma\,\mathrm{Gal}(L/T) \subseteq U$.

In particular, if M/K is unramified, then $W(M/K) = \mathrm{Frob}_{T/K}^{\mathbb{Z}}$.

It is helpful to put these groups into a diagram of topological groups to see what is going on.

$$\begin{array}{ccccc} \mathrm{Gal}(M/T) & \hookrightarrow & W(M/K) & \twoheadrightarrow & \mathrm{Frob}_{T/K}^{\mathbb{Z}} \\ \| & & \downarrow & & \downarrow \\ \mathrm{Gal}(M/T) & \hookrightarrow & \mathrm{Gal}(M/K) & \twoheadrightarrow & \mathrm{Gal}(T/K) \end{array}$$

Here we put the discrete topology on the subgroup generated by the Frobenius. The topology of $W(M/K)$ is then chosen so that all these maps are continuous homomorphisms of groups.

In many ways, the Weil group works rather like the Galois group.

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

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

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

If L/K is also Galois, then

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

via restriction.

Proof. We first prove density. To see that density is equivalent to $W(M/K) \to \mathrm{Gal}(L/K)$ being surjective for all finite subextension L/K, note that by the topology on $\mathrm{Gal}(M/K)$, we know density is equivalent to saying that $W(M/K)$ hits every coset of $\mathrm{Gal}(M/L)$, which means that $W(M/K) \to \mathrm{Gal}(L/K)$ is surjective.

Let L/K be a subextension. We let $T = T_{M/K}$. Then $T_{L/K} = T \cap L$. Then we have a diagram

$$\begin{array}{ccccc} \mathrm{Gal}(M/T) & \longrightarrow & W(M/K) & \longrightarrow & \mathrm{Frob}_{T/K}^{\mathbb{Z}} \\ \downarrow & & \downarrow & & \downarrow \\ \mathrm{Gal}(L/T \cap L) & \longrightarrow & \mathrm{Gal}(L/K) & \longrightarrow & \mathrm{Gal}(T \cap L/K) \end{array}$$

Here the surjectivity of the left vertical arrow comes from field theory, and the right hand vertical map is surjective because $T \cap L/K$ is finite and hence the Galois group is generated by the Frobenius. Since the top and bottom rows are short exact sequences (top by definition, bottom by Galois theory), by diagram chasing (half of the five lemma), we get surjectivity in the middle.

To prove the second part, we again let L/K be a finite subextension. Then $L \cdot T_{M/K} \subseteq T_{M/L}$. We then have maps

$$\begin{array}{ccccc} \mathrm{Frob}_{T_{M/K}/K}^{\mathbb{Z}} & \hookrightarrow & \mathrm{Gal}(T_{M/K}/K) & \xrightarrow{\cong} & \mathrm{Gal}(k_M/k_K) \\ \uparrow & & \uparrow & & \uparrow \\ \mathrm{Frob}_{T_{M/L}/L}^{\mathbb{Z}} & \hookrightarrow & \mathrm{Gal}(T_{M/L}/L) & \xrightarrow{\cong} & \mathrm{Gal}(k_M/k_L) \end{array}$$

So the left hand vertical map is an inclusion. So we know

$$\mathrm{Frob}^{\mathbb{Z}}_{T_{M/L}/L} = \mathrm{Frob}^{\mathbb{Z}}_{T_{M/K}/K} \cap \mathrm{Gal}(T_{M/L}/L).$$

Now if $\sigma \in \mathrm{Gal}(M/L)$, then we have

$$\begin{aligned}\sigma \in W(M/L) &\Leftrightarrow \sigma|_{T_{M/L}/L} \in \mathrm{Frob}^{\mathbb{Z}}_{T_{M/L}/L}\\ &\Leftrightarrow \sigma|_{T_{M/K}/K} \in \mathrm{Frob}^{\mathbb{Z}}_{T_{M/K}/K}\\ &\Leftrightarrow \sigma \in W(M/K).\end{aligned}$$

So this gives the second part.

Now L/K is Galois as well. Then $\mathrm{Gal}(M/L)$ is normal in $\mathrm{Gal}(M/K)$. So $W(M/L)$ is normal in $W(M/K)$ by the second part. Then we can compute

$$\begin{aligned}\frac{W(M/K)}{W(M/L)} &= \frac{W(M/K)}{W(M/K) \cap \mathrm{Gal}(M/L)}\\ &\cong \frac{W(M/K)\,\mathrm{Gal}(M/L)}{\mathrm{Gal}(M/L)}\\ &= \frac{\mathrm{Gal}(M/K)}{\mathrm{Gal}(M/L)}\\ &\cong \mathrm{Gal}(L/K).\end{aligned}$$

The only non-trivial part in this chain is the assertion that $W(M/K)\,\mathrm{Gal}(M/L) = \mathrm{Gal}(M/K)$, i.e. that $W(M/K)$ hits every coset of $\mathrm{Gal}(M/L)$, which is what density tells us. □

7.3 Main theorems of local class field theory

We now come to the 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.

We will fix an algebraic closure $\bar{K}$ of K, and all algebraic extensions we will consider will be taken to be subextensions of $\bar{K}/K$. We let K^{sep} be the separable closure of K inside $\bar{K}$.

If M/K and M/K are Galois extensions, then LM/K is Galois, and the map given by restriction

$$\mathrm{Gal}(LM/K) \hookrightarrow \mathrm{Gal}(L/K) \times \mathrm{Gal}(M/K).$$

is an injection. In particular, if L/K and M/K are both abelian, then so is LM/K. This implies that there is a maximal abelian extension K^{ab}.

Finally, note that we know an example of an abelian extension, namely the maximal unramified extension $K^{\mathrm{ur}} = T_{K^{\mathrm{sep}}/K} \subseteq K^{\mathrm{ab}}$, and we put $\mathrm{Frob}_K = \mathrm{Frob}_{K^{\mathrm{ur}}/K}$.

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

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

characterized by the properties

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

(ii) We have
$$\mathrm{Art}_K(N_{L/K}(x))|_L = \mathrm{id}_L$$
for all L/K finite abelian and $x \in L^\times$.

Moreover, if M/K is finite, then for all $x \in M^\times$, we know $\mathrm{Art}_M(x)$ is an automorphism of M^{ab}/M, and restricts to an automorphisms of K^{ab}/K. Then we have
$$\mathrm{Art}_M(x)|_K^{K^{\mathrm{ab}}} = \mathrm{Art}_K(N_{M/K}(x)).$$
Moreover, Art_K induces an isomorphism
$$\frac{K^\times}{N_{M/K}(M^\times)} \to \mathrm{Gal}\left(\frac{M \cap K^{\mathrm{ab}}}{K}\right).$$

To simplify this, we will write $N(L/K) = N_{L/K}(L^\times)$ for L/K finite. From this theorem, we can deduce a lot of more precise statements.

Corollary. Let L/K be finite. Then $N(L/K) = N((L \cap K^{ab})/K)$, and
$$(K^\times : N(L/K)) \leq [L : K]$$
with equality iff L/K is abelian.

Proof. To see this, we let $M = L \cap K^{\mathrm{ab}}$. Applying the isomorphism twice gives
$$\frac{K^\times}{N(L/K)} \cong \mathrm{Gal}(M/K) \cong \frac{K^\times}{N(M/K)}.$$
Since $N(L/K) \subseteq N(M/K)$, and $[L : K] \geq [M : K] = |\mathrm{Gal}(M/K)|$, we are done. □

Now the really important result is the Galois correspondence between subgroups of the unit group and finite abelian extensions:

Theorem. Let K be a local field. Then there is an isomorphism of posets
$$\begin{array}{ccc} \left\{\begin{array}{c}\text{open finite index}\\ \text{subgroups of } K^\times\end{array}\right\} & \longleftrightarrow & \left\{\begin{array}{c}\text{finite abelian}\\ \text{extensions of } L/K\end{array}\right\} \\ H & \longmapsto & (K^{\mathrm{ab}})^{\mathrm{Art}_K(H)} \\ N(L/K) & \longmapsto & L/K \end{array}.$$

In particular, for L/K and M/K finite abelian extensions, we have
$$\begin{aligned} N(LM/K) &= N(L/K) \cap N(M/K), \\ N(L \cap M/K) &= N(L/K)N(M/K). \end{aligned}$$

We will only prove part of it. The remaining are left as an exercise on the example sheet.

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

Proof. By the previous theorem, we may wlog L/K abelian by replacing with $L \cap K^{\mathrm{ab}}$. The $\Leftarrow$ direction is clear by the last part of Artin reciprocity.

For the other direction, we assume that we have $N(L/K) \subseteq N(M/K)$, and let $\sigma \in \mathrm{Gal}(K^{\mathrm{ab}}/L)$. We want to show that $\sigma|_M = \mathrm{id}_M$. This would then imply that M is a subfield of L by Galois theory.

We know $W(K^{\mathrm{ab}}/L)$ is dense in $\mathrm{Gal}(K^{\mathrm{ab}}/L)$. So it suffices to show this for $\sigma \in W(K^{\mathrm{ab}}/L)$. Then we have

$$W(K^{\mathrm{ab}}/L) \cong \mathrm{Art}_K(N(L/K)) \subseteq \mathrm{Art}_K(N(M/K)).$$

So we can find $x \in M^\times$ such that $\sigma = \mathrm{Art}_K(N_{M/K}(x))$. So $\sigma|_M = \mathrm{id}_M$ by local Artin reciprocity. □

Side note: Why is this called "class field theory"? Usually, we call the field corresponding to the subgroup H the *class field* of H. Historically, the first type of theorems like this are proved for number fields. The groups that appear on the left would be different, but in some cases, they are the class group of the number field.

8 Lubin-Tate theory

For the rest of the course, we will indicate how one can explicitly construct the field K^{ab} and the map Art_K.

There are many ways we can approach local class field theory. The approach we use, using Lubin-Tate theory, is the most accessible one. Another possible approach is via Galois cohomology. This, however, relies on more advanced machinery, namely Galois cohomology.

8.1 Motivating example

We will work out the details of local Artin reciprocity in the case of $\mathbb{Q}_p$ as a motivating example for the proof we are going to come up with later. Here we will need the results of local class field theory to justify our claims, but this is not circular since this is not really part of the proof.

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

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

Proof. Pick $x \in L^\times$, and w the valuation on L extending v_K, and $n = [L : K]$. Then by construction of w, we know

$$v_K(N_{L/K}(x)) = nw(x) = f_{L/K} v_L(x).$$

So we have a surjection

$$\frac{K^\times}{N(L/K)} \xrightarrow{v_K} \frac{\mathbb{Z}}{f_{L/K}\mathbb{Z}}.$$

The kernel of this map is equal to

$$\frac{\mathcal{O}_K^\times N(L/K)}{N(L/K)} \cong \frac{\mathcal{O}_K^\times}{\mathcal{O}_K^\times \cap N(L/K)} = \frac{\mathcal{O}_K^\times}{N_{L/K}(\mathcal{O}_L^\times)}.$$

So by local class field theory, we know

$$n = (K^\times : N(L/K)) = f_{L/K}(\mathcal{O}_K^\times : N_{L/K}(\mathcal{O}_L^\times)),$$

and this implies what we want. □

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

Now we fix a uniformizer π_K. Then we have a topological group isomorphism

$$K^\times \cong \langle \pi_K \rangle \times \mathcal{O}_K^\times.$$

Since we know that the finite abelian extensions correspond exactly to finite index subgroups of $K^\times$ by taking the norm groups, we want to understand subgroups of $K^\times$. Now consider the subgroups of $K^\times$ of the form

$$\langle \pi_K^m \rangle \times U_K^{(n)}.$$

We know these form a basis of the topology of $K^\times$, so it follows that finite-index open subgroups must contain one of these guys. So we can find the maximal abelian extension as the union of all fields corresponding to these guys.

Since we know that $N(LM/K) = N(L/K) \cap N(M/K)$, it suffices to further specialize to the cases

$$\langle \pi_K \rangle \times U_K^{(n)}$$

and

$$\langle \pi_K^m \rangle \times \mathcal{O}_K$$

separately. The second case is easy, because this corresponds to an unramified extension by the above corollary, and unramified extensions are completely characterized by the extension of the residue field. Note that the norm group and the extension are both independent of the choice of uniformizer. The extensions corresponding to the first case are much more difficult to construct, and they depend on the choice of π_K. We will get them from Lubin-Tate theory.

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

$$L = \bigcup_m L_m.$$

Then we have

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

Lemma. We have isomorphisms

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

Proof. The first isomorphism follows from the previous lemma. The second follows from the fact that $K^{\mathrm{ur}} \cap L = K$ as L is totally ramified. The last isomorphism follows from the fact that $T_{K^{\mathrm{ur}}/K} = K^{\mathrm{ur}}$ trivially, and then by definition $W(K^{\mathrm{ur}/K}) \cong \mathrm{Frob}_K^{\mathbb{Z}}$. □

Example. We consider the special case of $K = \mathbb{Q}_p$ and $\pi_K = p$. We let

$$L_n = \mathbb{Q}_p(\zeta_{p^n}),$$

where ζ_{p^n} is the primitive p^nth root of unity. Then by question 6 on example sheet 2, we know this is a field with norm group

$$N(\mathbb{Q}_p(\zeta_{p^n})/\mathbb{Q}_p) = \langle p \rangle \times (1 + p^n \mathbb{Z}_p) = \langle p \rangle \times U_{\mathbb{Q}_p}^{(n)},$$

and thus this is a totally ramified extension of $\mathbb{Q}_p$.

We put

$$\mathbb{Q}_p(\zeta_{p^\infty}) = \bigcup_{n=1}^{\infty} \mathbb{Q}_p(\zeta_{p^n}).$$

Then again this is totally ramified extension, since it is the nested union of totally ramified extensions.

Then we have

$$\begin{aligned}\mathrm{Gal}(\mathbb{Q}_p(\zeta_{p^\infty})/\mathbb{Q}_p) &\cong \varprojlim_n \mathrm{Gal}(\mathbb{Q}_p(\zeta_{p^n})/\mathbb{Q}_p)\\ &= \varprojlim_n (\mathbb{Z}/p^n\mathbb{Z})^\times\\ &= \mathbb{Z}_p^\times.\end{aligned}$$

Note that we are a bit sloppy in this deduction. While we know that it is true that $\mathbb{Z}_p^\times \cong \varprojlim_n (\mathbb{Z}/p^n\mathbb{Z})^\times$, the inverse limit depends not only on the groups $(\mathbb{Z}/p^n\mathbb{Z})^\times$ themselves, but also on the maps we use to connect the groups together. Fortunately, from the discussion below, we will see that the maps

$$\mathrm{Gal}(\mathbb{Q}_p(\zeta_{p^n})/\mathbb{Q}_p) \to \mathrm{Gal}(\mathbb{Q}_p(\zeta_{p^{n-1}})/\mathbb{Q}_p)$$

indeed correspond to the usual restriction maps

$$(\mathbb{Z}/p^n\mathbb{Z})^\times \to (\mathbb{Z}/p^{n-1}\mathbb{Z})^\times.$$

It is a fact that this is the *inverse* of the Artin map of $\mathbb{Q}_p$ restricted to $\mathbb{Z}_p^\times$. Note that we have $W(\mathbb{Q}_p(\zeta_{p^\infty})/\mathbb{Q}_p) = \mathrm{Gal}(\mathbb{Q}_p(\zeta_{p^\infty})/\mathbb{Q}_p)$ because its maximal unramified subextension is trivial.

We can trace through the above chains of isomorphisms to figure out what the Artin map does. Let $m = \mathbb{Z}_p^\times$. Then we can write

$$m = a_0 + a_1 p + \cdots,$$

where $a_i \in \{0, \cdots, p-1\}$ and $a_0 \neq 0$. Now for each n, we know

$$m \equiv a_0 + a_1 p + \cdots + a_{n-1}p^{n-1} \mod p^n.$$

By the usual isomorphism $\mathrm{Gal}(\mathbb{Q}_p(\zeta_{p^n})/\mathbb{Q}_p) \cong \mathbb{Z}/p^n\mathbb{Z}$, we know m acts as

$$\zeta_{p^n} \mapsto \zeta_{p^n}^{a_0+a_1p+\ldots+a_{n-1}p^{n-1}} \text{ “}=\text{”} \zeta_{p^n}^m$$

on $\mathbb{Q}_p(\zeta_{p^n})$, where we abuse notation because taking ζ_{p^n} to powers of p greater than n gives 1. It can also be interpreted as $(1+\lambda_{p_n})^m$, where $\lambda_{p_n} = \zeta_{p_n} - 1$ is a uniformizer, which makes sense using binomial expansion.

So the above isomorphisms tells us that $\mathrm{Art}_{\mathbb{Q}_p}$ restricted to $\mathbb{Z}_p^\times$ acts on $\mathbb{Q}_p(\zeta_{p^\infty})$ as

$$\mathrm{Art}_{\mathbb{Q}_p}(m)(\zeta_{p^n}) \equiv \sigma_{m^{-1}}(\zeta_{p^n}) = \zeta_{p^n}^{m^{-1}}.$$

The full Artin map can then be read off from the following diagram:

$$\begin{array}{ccc}\mathbb{Q}_p^\times & \xrightarrow{\quad\mathrm{Art}_{\mathbb{Q}_p}\quad} & W(\mathbb{Q}_p^{\mathrm{ab}}/\mathbb{Q}_p)\\ \downarrow\cong & & \sim\downarrow\text{restriction}\\ \langle p\rangle \times \mathbb{Z}_p^\times & \longrightarrow & W(\mathbb{Q}_p^{\mathrm{ur}}/\mathbb{Q}_p) \times \mathrm{Gal}(\mathbb{Q}_p(\zeta_{p^\infty})/\mathbb{Q}_p)\end{array}$$

where the bottom map sends

$$\langle p^n, m\rangle \mapsto (\mathrm{Frob}_{\mathbb{Q}_p}^n, \sigma_{m^{-1}}).$$

In fact, we have

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

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

Not a proof. We will comment on the proof of the generalized version later. □

Remark. There is another normalization of the Artin map which sends a uniformizer to the *geometric Frobenius*, defined to be the inverse of the arithmetic Frobenius. With this convention, $\mathrm{Art}_{\mathbb{Q}_p}(m)|_{\mathbb{Q}_p(\zeta_{p^\infty})}$ is σ_m.

We can define higher ramification groups for general Galois extensions.

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

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

This definition makes sense, because the upper number behaves well when we take quotients. This is one of the advantages of upper numbering. Note that we can write the ramification group as the inverse limit

$$G^s(M/K) \cong \varprojlim_{L/K} G^s(L/K),$$

as in the case of the Galois group.

Example. Going back to the case of $K = \mathbb{Q}_p$. We write $\mathbb{Q}_{p^n}$ for the unramified extension of degree n of $\mathbb{Q}_p$. By question 11 of example sheet 3, we know that

$$G^s(\mathbb{Q}_{p^n}(\zeta_{p^m})/\mathbb{Q}_p) = \begin{cases} \mathrm{Gal}(\mathbb{Q}_{p^n}(\zeta_{p^m})/\mathbb{Q}_p) & s = -1 \\ \mathrm{Gal}(\mathbb{Q}_{p^n}(\zeta_{p^m})/\mathbb{Q}_{p^n}) & -1 < s \leq 0 \\ \mathrm{Gal}(\mathbb{Q}_{p^n}(\zeta_{p^m})/\zeta_{p^k}) & k-1 < s \leq k \leq m-1 \\ 1 & s > m-1 \end{cases},$$

which corresponds to

$$\begin{cases} \dfrac{\langle p\rangle \times U^{(0)}}{\langle p^n\rangle \times U^{(m)}} & s = -1 \\ \dfrac{\langle p^n\rangle \times U^{(0)}}{\langle p^n\rangle \times U^{(m)}} & -1 < s \leq 0 \\ \dfrac{\langle p^n\rangle \times U^{(k)}}{\langle p^n\rangle \times U^{(m)}} & k-1 < s \leq k \leq m-1 \\ 1 & s > m-1 \end{cases}$$

under the Artin map.

By taking the limit as $n, m \to \infty$, we get

Theorem. We have

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

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

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

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

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

Here $\mathrm{Art}_{\mathbb{Q}_p}$ induces an isomorphism

$$\frac{\mathbb{Q}_p^\times}{N(L/\mathbb{Q}_p)} \to \mathrm{Gal}(L/\mathbb{Q}_p).$$

So it follows that $L \subseteq \mathbb{Q}_{p^n}(\zeta_{p^m})$ for some n if and only if $G^s(L/\mathbb{Q}_p) = 1$ for all $s > m - 1$.

8.2 Formal groups

The proof of local Artin reciprocity will be done by constructing the analogous versions of L_n for an arbitrary local field, and then proving that it works. To do so, we will need the notion of a *formal group*. The idea of a formal group is that a formal group is a rule that specifies how we should multiply two elements via a power series over a ring R. Then if we have a complete R-module, then the formal group will turn the R-module into an actual group. There is then a natural notion of a formal module, which is a formal group F with an R-action.

At the end, we will pick $R = \mathcal{O}_K$. The idea is then that we can fix an algebraic closure $\bar{K}$, and then a formal $\mathcal{O}_K$-module will turn $\mathfrak{m}_{\bar{K}}$ into an actual $\mathcal{O}_K$-module. Then if we adjoin the right elements of $\mathfrak{m}_{\bar{K}}$ to K, then we obtain an extension of K with a natural $\mathcal{O}_K$ action, and we can hope that this restricts to field automorphisms when we restrict to the unit group.

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

In algebraic geometry, this is used as the generalization of the Lie algebra over a Lie group, where instead of talking about the tangent space of a group, we talk about its infinitesimal neighbourhood, which contains all higher-order information. A lot of the seemingly-arbitrary compatibility conditions we later impose have such geometric motivation that we unfortunately cannot go into.

Example. If F is a formal group over $\mathcal{O}_K$, where K is a complete valued field, then $F(x, y)$ converges for all $x, y \in \mathfrak{m}_K$. So $\mathfrak{m}_K$ becomes a (semi)group under the multiplication

$$(x, y) \mapsto F(x, y) \in \mathfrak{m}_k$$

Example. We can define

$$\hat{\mathbb{G}}_a(X, Y) = X + Y.$$

This is called the *formal additive group*.

Similarly, we can have

$$\hat{\mathbb{G}}_m(X, Y) = X + Y + XY.$$

This is called the *formal multiplicative group*. Note that

$$X + Y + XY = (1 + X)(1 + Y) - 1.$$

So if K is a complete valued field, then $\mathfrak{m}_K$ bijects with $1 + \mathfrak{m}_k$ by sending $x \mapsto 1 + x$, and the rule sending $(x, y) \in \mathfrak{m}_K^2 \mapsto x + y + xy \in \mathfrak{m}_K$ is just the usual multiplication in $1 + \mathfrak{m}_K$ transported to $\mathfrak{m}_K$ via the bijection above.

We can think of this as looking at the group in a neighbourhood of the identity 1.

Note that we called this a formal *group*, rather than a formal semi-group. It turns out that the existence of identity and inverses is automatic.

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

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

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

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

Proof. See example sheet 4. □

The next thing to do is to define homomorphisms of formal groups.

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.

We can now define a formal module in the usual way, plus some compatibility conditions.

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

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

Those were all general definitions. We now restrict to the case we really care about. Let K be a local field, and $q = |k_K|$. We let $\pi \in \mathcal{O}_K$ be a uniformizer.

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

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

We can think of this condition of saying "uniformizer corresponds to the Frobenius".

Example. The formal group $\hat{\mathbb{G}}_m$ is a Lubin-Tate $\mathbb{Z}_p$ module with respect to p given by the following formula: if $a \in \mathbb{Z}_p$, then we define

$$[a]_{\hat{\mathbb{G}}_m}(X) = (1+X)^a - 1 = \sum_{n=1}^{\infty} \binom{a}{n} X^n.$$

The conditions

$$(1+X)^a - 1 \equiv aX \mod X^2$$

and

$$(1+X)^p - 1 \equiv X^p \mod p$$

are clear.

We also have to check that $a \mapsto [a]_F$ is a ring homomorphism. This follows from the identities

$$((1+X)^a)^b = (1+X)^{ab}, \quad (1+X)^a(1+X)^b = (1+X)^{ab},$$

which are on the second example sheet.

The objective of the remainder of the section is to show that all Lubin-Tate modules are isomorphic.

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 $\mathcal{E}_\pi$.

Now by definition, if F is a Lubin-Tate $\mathcal{O}_K$ module for π, then $[\pi]_F$ is a Lubin-Tate series for π.

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.

Example. $X^q + \pi X$ is a Lubin-Tate polynomial.

Example. If $K = \mathbb{Q}_p$ and $\pi = p$, then $(1+X)^p - 1$ is a Lubin-Tate polynomial.

The result that allows us to prove that all Lubin-Tate modules are isomorphic is the following general result:

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

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

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

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

and

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

For reasons of time, we will not prove this. We just build F by successive approximation, which is not terribly enlightening.

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

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

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

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

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

We now state the theorem that classifies all Lubin-Tate modules in terms of Lubin-Tate series.

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

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

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

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

So in some sense, there is only one Lubin-Tate module.

Proof sketch. If F is a Lubin-Tate $\mathcal{O}_K$-module for π, then $e = [\pi]_F \in \mathcal{E}_\pi$ by definition, and F satisfies the properties that characterize the series F_e. So $F = F_e$ by uniqueness.

For the remaining parts, one has to verify the following for all $e, e_1, e_2, e_3 \in \mathcal{E}_\pi$ and $a, b \in \mathcal{O}_K$.

(i) $F_e(X,Y) = F_e(Y,X)$.

(ii) $F_e(X, F_e(Y,Z)) = F_e(F_e(X,Y), Z)$.

(iii) $[a]_{e_1,e_2}(F_e(X,Y)) = F_{e_1}([a]_{e_1,e_2}(X), [a]_{e_1,e_2}(Y))$.

(iv) $[ab]_{e_1,e_3}(X) = [a]_{e_1,e_2}([b]_{e_2,e_3}(X))$.

(v) $[a+b]_{e_1,e_2}(X) = [a]_{e_1,e_2}(X) + [b]_{e_1,e_2}(X)$.

(vi) $[\pi]_e(X) = e(X)$.

The proof is just repeating the word "uniqueness" ten times. □

8.3 Lubin-Tate extensions

We now use the Lubin-Tate modules to do things. As before, we fixed an algebraic closure $\bar{K}$ of K. We let $\bar{\mathfrak{m}} = \mathfrak{m}_{\bar{K}}$ be the maximal ideal in $\mathcal{O}_{\bar{K}}$.

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

$$x +_F = F(x,y)$$
$$a \cdot x = [a]_F(x)$$

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

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

This isn't exactly immediate, because $\bar{K}$ need not be complete. However, this is not a problem as each multiplication given by F only involves finitely many things (namely two of them).

Proof. If $x, y \in \bar{\mathfrak{m}}$, then $F(x,y)$ is a series in $K(x,y) \subseteq \bar{K}$. Since $K(x,y)$ is a finite extension, we know it is complete. Since the terms in the sum have absolute value < 1 and $\to 0$, we know it converges to an element in $\mathfrak{m}_{K(x,y)} \subseteq \bar{\mathfrak{m}}$. The rest then essentially follows from definition. □

To prove local class field theory, we want to find elements with an $U_K/U_K^{(n)}$ action for each n, or equivalently elements with an $\mathcal{O}_K/\mathcal{O}_K^{(n)}$ action. Note that the first quotient is a quotient of groups, while the second quotient is a quotient of a ring by an ideal. So it is natural to consider the following elements:

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.

Example. Let $F = \hat{\mathbb{G}}_m, K = \mathbb{Q}_p$ and $\pi = p$. Then for $x \in \bar{\mathfrak{m}}_{\hat{\mathbb{G}}_m}$, we have

$$p^n \cdot x = (1+x)^{p^n} - 1.$$

So we know

$$\hat{\mathbb{G}}_m(n) = \{\zeta_{p^n}^i - 1 \mid i = 0, 1, \cdots, p^n - 1\},$$

where $\zeta_{p^n} \in \bar{\mathbb{Q}}_p$ is the primitive p^nth root of unity.

So $\hat{\mathbb{G}}_m(n)$ generates $\mathbb{Q}_p(\zeta_{p^n})$.

To prove this does what we want, we need the following lemma:

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

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

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

Proof. Let $x \in \bar{K}$. We claim that if $|f_i(x)| < 1$ for $i = 0, \cdots, n-1$, then $f_n'(X) \neq 0$.

We proceed by induction on n.

(i) When $n = 1$, we assume $|x| < 1$. Then

$$f_1'(x) = e'(x) = qx^{q-1} + \pi = \pi\left(1 + \frac{q}{\pi}x^{q-1}\right) \neq 0,$$

since we know $\frac{q}{\pi}$ has absolute value ≤ 1 (q vanishes in k_K, so q/π lives in $\mathcal{O}_K$), and x^{q-1} has absolute value < 1.

(ii) in the induction step, we have

$$f_{n+1}'(x) = (qf_n(x)^{q-1} + \pi)f_n'(x) = \pi\left(1 + \frac{q}{\pi}f_n(x)^{q-1}\right)f_n'(x).$$

By induction hypothesis, we know $f_n'(x) \neq 0$, and by assumption $|f_n(x)| < 1$. So the same argument works.

We now prove the lemma. We assume that $f_n(x) = 0$. We want to show that $|f_i(x)| < 1$ for all $i = 0, \cdots, n-1$. By induction, we have

$$f_n(x) = x^{q^n} + \pi g_n(x)$$

for some $g_n(x) \in \mathcal{O}_K[x]$. It follows that if $f_n(x) = 0$, then $|x| < 1$. So $|f_i(x)| < 1$ for all i. So $f_n'(x) \neq 0$. □

The point of the lemma is to prove the following proposition:

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

Proof. By definition, we know

$$\pi^n \cdot F(n) = 0.$$

So $F(n)$ is indeed an $\mathcal{O}_K/\pi^n\mathcal{O}_K$-module.

To prove that it is free of rank 1, we note that all Lubin-Tate modules for π are isomorphic. This implies that all the honest $\mathcal{O}_K$ modules $F(n)$ are isomorphic. We choose $F = F_e$, where $e = X^q + \pi X$. Then $F(n)$ consists of the roots of the polynomial $f_n = e^n(X)$, which is of degree q^n and has no repeated roots. So $|F(n)| = q^n$. To show that it is actually the right thing, if $\lambda_n \in F(n) \setminus F(n-1)$, then we have a homomorphism

$$\mathcal{O}_K \to F(n)$$

given by $A \mapsto a \cdot \lambda_n$. Its kernel is $\pi^n \mathcal{O}_K$ by our choice of λ_n. By counting, we get an $\mathcal{O}_K$-module isomorphism

$$\frac{\mathcal{O}_K}{\pi^n \mathcal{O}_K} \to F(n)$$

as desired. □

Corollary. We have isomorphisms

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

Given a Lubin-Tate $\mathcal{O}_K$-module F for π, we consider

$$L_{n,\pi} = L_n = K(F(n)),$$

which is the field of π^n division points of F. From the inclusions $F(n) \subseteq F(n+1)$ for all n, we obtain a corresponding inclusion of fields

$$L_n \subseteq L_{n+1}.$$

The field L_n depends only in π, and not on F. To see this, we let G be another Lubin-Tate $\mathcal{O}_K$-module, and let $f : F \to G$ be an isomorphism. Then

$$G(n) = f(F(n)) \subseteq K(F(n))$$

since the coefficients of f lie in K. So we know

$$K(G(n)) \subseteq K(F(n)).$$

By symmetry, we must have equality.

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

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

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

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

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

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

Moreover, if $F = F_e$, where

$$e(X) = X^q + \pi(a_{q-1}\pi^{q-1} + \cdots + a_2 X^2) + \pi X,$$

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

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

is the minimal polynomial of λ_n. In particular,

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

Proof. Consider a Lubin-Tate polynomial

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

We set $F = F_e$. Then

$$\phi_n(X) = \frac{e^n(X)}{e^{n-1}(X)} = (e^{n-1}(X))^{q-1} + \pi(a_{q_1}e^{n-1}(X)^{q-2} + \cdots + a_2e^{n-1}(X)) + \pi$$

is an Eisenstein polynomial of degree $q^{n-1}(q-1)$ by starting at it long enough. So if $\lambda_n \in F(n) \setminus F(n-1)$, then λ_n is a root of $\phi_n(x)$, so $K(\lambda_n)/K$ is totally ramified of degree $q^{n-1}(q-1)$, and λ_n is a uniformizer, and

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

as the norm is just the constant coefficient of the minimal polynomial.

Now let $\sigma \in \mathrm{Gal}(L_n/K)$. Then σ induces a permutation of $F(n)$, as these are the roots of $e^n(X)$, which is in fact $\mathcal{O}_K$-linear, i.e.

$$\sigma(x) +_F \sigma(y) = F(\sigma(x), \sigma(y)) = \sigma(F(x,y)) = \sigma(x +_F y)$$
$$\sigma(a \cdot x) = \sigma([a]_F(x)) = [a]_F(\sigma(x)) = a \cdot \sigma(x)$$

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

So we have an injection of groups

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

But we know

$$\left|\frac{U_K}{U_K^{(n)}}\right| = q^{n-1}(q-1) = [K(\lambda_n) : K] \leq [L_n : K] = |\mathrm{Gal}(L_n/K)|.$$

So we must have equality throughout, the above map is an isomorphism, and $K(\lambda_n) = L_n$.

It is clear from the construction of the isomorphism that for $m \geq n$, the diagram

$$\begin{array}{ccc} \mathrm{Gal}(L_m/K) & \xrightarrow{\sim} & U_K/U_K^{(m)} \\ \big\downarrow{\scriptstyle \text{restriction}} & & \big\downarrow{\scriptstyle \text{quotient}} \\ \mathrm{Gal}(L_n/K) & \xrightarrow{\sim} & U_K/U_K^{(n)} \end{array}$$

commutes. So the isomorphism

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

follows by looking at the kernels. □

Example. In the case where $K = \mathbb{Q}_p$ and $\pi = p$, recall that

$$\hat{\mathbb{G}}_m(n) = \{\zeta_{p^n}^i - 1 \mid i = 0, \cdots, p^{n-1} - 1\},$$

where ζ_{p^n} is the principal p^nth root of unity. The theorem then gives

$$\mathrm{Gal}(\mathbb{Q}_p(\zeta_{p^n})/\mathbb{Q}_p) \cong (\mathbb{Z}/p^n)^\times$$

given by if $a \in \mathbb{Z}_{\geq 0}$ and $(a, p) = 1$, then

$$\sigma_a(\zeta_{p^n}^i - 1) = [a]_{\hat{\mathbb{G}}_m(n)}(\zeta_{p^n}^i - 1) = (1 + (\zeta_{p^n}^i - 1))^a - 1 = \zeta_{p^n}^{ai} - 1.$$

This agrees with the isomorphism we previously constructed.

Back to the general situation, setting

$$L_\infty = \bigcup_{n=1}^{\infty} L_n,$$

we know L_∞/K is Galois, and we have isomorphisms

$$\begin{aligned} \mathrm{Gal}(L_\infty/K) &\xrightarrow{\sim} \varprojlim \mathrm{Gal}(L_n/K) \xrightarrow{\sim} \varprojlim_n U_K/U_K^{(n)} \cong U_K \\ \sigma &\longmapsto (\sigma|_{L_n})_n \end{aligned}$$

This map will be the inverse of the Artin map restricted to L_∞.

To complete the proof of Artin reciprocity, we need to use the following theorem without proof:

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

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

(for any π).

Comments on the proof. One can prove this from the *Hasse-Arf theorem*, which states that in an abelian extension, the jumps in the upper ramification groups occur only at integer values. This, together with the calculation of ramification groups done later, easily implies the theorem. Essentially, L_∞ maxed out all possible jumps of the upper ramification groups. However, the Hasse-Arf theorem is difficult to prove.

Another approach is to prove the existence of the Artin map using other techniques (e.g. Galois cohomology). Consideration of the norm group (cf. the next theorem) then implies the theorem. The content of this section then becomes an explicit construction of a certain family of abelian extensions. □

We can characterize the norm group by

Theorem. We have

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

Comments on the proof. This can be done by defining *Coleman operators*, which are power series representations of the norm. Alternatively, assuming the description of the local Artin map given below and local Artin reciprocity, $U_k^{(n)}$ is in the kernel of $\mathrm{Art}|_{L_n}$, so $\langle \pi \rangle \times U_k^{(n)} \subseteq N(L_n/K)$. The result follows by comparing order. □

We can then construct the Artin map as follows:

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

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

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

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

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

The inverse shows up in the proof to make sure the map defined above is independent of the choice of uniformizer. We will not prove this, nor that the map obtained has the desired properties. Instead, we will end the course by computing the higher ramification groups of these extensions.

Theorem. We have

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

Proof. The case for $-1 \le s \le 0$ is clear.

For $0 \le s \le 1$ (which we may wlog is actually 1), we know that

$$\mathrm{Gal}(L_n/L_k) \cong U_K^{(k)}/U_K^{(n)}$$

under the isomorphism $\mathrm{Gal}(L_n/K) \cong U_K/U_K^{(n)}$. On the other hand, we know $G_1(L_n/K)$ is the Sylow p-subgroup of $\mathrm{Gal}(L_n/K)$. So we must have

$$G_1(L_n/K) \cong U_K^{(1)}/U_K^{(n)}.$$

So we know that $G_1(L_n/K) = \mathrm{Gal}(L_n/L_1)$. Thus we know that $G_s(L_n/K) = \mathrm{Gal}(L_n/K)$ for $0 < s \le 1$.

We now let $\sigma = \sigma_u \in G_1(L_n/K)$ and $u \in U_K^{(1)}/U_K^{(n)}$. We write

$$u = 1 + \varepsilon\pi^k$$

for some $\varepsilon \in U_K$ and some $k = k(u) \ge 1$. Since σ is not the identity, we know $k < n$. We claim that

$$i_{L_n/K}(\sigma) = v_{L_n}(\sigma(\lambda) - \lambda) = q^k.$$

Indeed, we let $\lambda \in F(n) \setminus F(n-1)$, where F is a choice of Lubin-Tate module for π. Then λ is a uniformizer of L_n and $\mathcal{O}_{L_n} = \mathcal{O}_K[\lambda]$. We can compute

$$\begin{aligned} \sigma_u(\lambda) &= [u]_F(\lambda) \\ &= [1 + \varepsilon\pi^k]_F(\lambda) \\ &= F(\lambda, [\varepsilon\pi^k]_F(\lambda)) \end{aligned}$$

Now we can write

$$[\varepsilon\pi^k]_F(\lambda) = [\varepsilon]_F([\pi^k]_F(\lambda)) \in F(n-k) \setminus F(n-k-1),$$

since $[\varepsilon]_F$ is invertible, and applying $[\pi^{n-k}]_F$ to $[\pi^k]_F(\lambda)$ kills it, but applying $[\pi^{n-k-1}]_F$ gives $[\pi^{n-1}]_F$, which does not kill.

So we know $[\varepsilon\pi^k]_F(\lambda)$ is a uniformizer of L_{n-k}. Since L_n/L_{n-k} is totally ramified of degree q^k, we can find $\varepsilon_0 \in \mathcal{O}_{L_n}^\times$ such that

$$[\varepsilon\pi^k]_F(\lambda) = \varepsilon_0\lambda^{q^k}$$

Recall that $F(X,0) = X$ and $F(0,Y) = Y$. So we can write

$$F(X,Y) = X + Y + XYG(X,Y),$$

where $G(X,Y) \in \mathcal{O}_K[[X,Y]]$. So we have

$$\begin{aligned}\sigma(\lambda) - \lambda &= F(\lambda, [\varepsilon\pi^k]_F(\lambda)) - \lambda\\ &= F(\lambda, \varepsilon_0\lambda^{q^k}) - \lambda\\ &= \lambda + \varepsilon_0\lambda^{q^k} + \varepsilon_0\lambda^{q^k+1}G(\lambda, \varepsilon_0\lambda^{q^k}) - \lambda\\ &= \varepsilon_0\lambda^{q^k} + \varepsilon_0\lambda^{q^k+1}G(\lambda, \varepsilon_0\lambda^{q^k}).\end{aligned}$$

In terms of valuation, the first term is the dominating term, and

$$i_{L_n/K}(\sigma) = v_{L_n}(\sigma(\lambda) - \lambda) = q^k$$

So we know

$$i_{L_n/K}(\sigma_k) \geq s+1 \Leftrightarrow q^{k(u)} - 1 \geq s.$$

So we know

$$G_s(L_n/K) = \{\sigma_K \in G_1(L_n/K) : q^{k(u)} - 1 \geq s\} = \mathrm{Gal}(L_n/L_k),$$

where $q^{k-1} - 1 < s \leq q^k - 1$ for $k = 1, \cdots, n-1$, and 1 if $s > q^{n-1} = 1$. □

Corollary. We have

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

In other words, we have

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

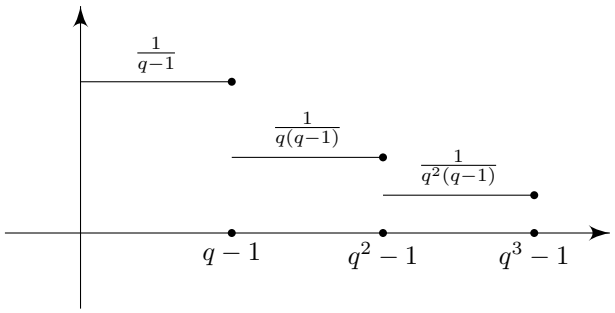
where we set $L_0 = K$.

Once again, the numbering is a bit more civilized in the upper numbering.

Proof. We have to compute the integral of

$$\frac{1}{(G_0(L_n/K) : G_x(L_n/K)}.$$

We again plot this out



So by the same computation as the ones we did last time, we find that

$$\eta_{L_n/K}(s) = \begin{cases} s & -1 \le s \le 0 \\ (k-1) + \frac{s-(q^{k-1}-1)}{q^{k-1}(q-1)} & q^{k-1} - 1 \le s \le q^k - 1, \quad k = 1, \cdots, n-1 \\ (n-1) + \frac{s-(q^{n-1}-1)}{q^{n-1}(q-1)} & s > q^{n-1} - 1. \end{cases}$$

Inverting this, we find that

$$\psi_{L_n/K} = \begin{cases} t & -1 \le t \le 0 \\ q^{\lceil t \rceil - 1}(q-1)(t - (\lceil t \rceil - 1)) + q^{\lceil t \rceil - 1} - 1 & 1 < t \le n-1 \\ q^{n-1}(q-1)(t-(n-1)) + q^{n-1} - 1 & t > n-1 \end{cases}.$$

Then we have

$$G^t(L_n/K) = G_{\psi(L_n/K)(t)}(L_n/K),$$

which gives the desired by the previous theorem. □

So we know that

$$\mathrm{Art}_K^{-1}(G^t(L_n/K)) = \begin{cases} U_K^{\lceil t \rceil}/U_K^{(n)} & -1 \le t \le n \\ 1 & t \ge n \end{cases}.$$

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

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

and

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

Proof. Recall the following fact from the examples class: If L/K is finite unramified and M/K is finite totally ramified, then LM/L is totally ramified, and $\mathrm{Gal}(LM/L) \cong \mathrm{Gal}(M/K)$ by restriction, and

$$G^t(LM/K) \cong G^t(M/K).$$

via this isomorphism (for $t > -1$).

Now let K_m/K be the unramified extension of degree m. By the lemma and the previous corollary, we have

$$\begin{aligned} G^t(K_m L_n/K) \cong G^t(L_n/K) &= \begin{cases} \mathrm{Gal}(L_n/L_{\lceil t \rceil}) & -1 < t \le n \\ 1 & t \ge n \end{cases} \\ &= \begin{cases} \mathrm{Gal}(K_m L_n/K_m L_{\lceil t \rceil}) & -1 < t \le n \\ 1 & t \ge n \end{cases} \end{aligned}$$

So we have

$$\begin{aligned} G^t(K^{\mathrm{ab}}/K) &= G^t(K^{\mathrm{ur}}L_\infty/K) \\ &= \varprojlim_{m,n} G^t(K_mL_n/K) \\ &= \varprojlim_{\substack{m,n \\ n\geq \lceil t\rceil}} \mathrm{Gal}(K_mL_n/K_mL_{\lceil t\rceil}) \\ &= \mathrm{Gal}(K^{\mathrm{ur}}L_\infty/K^{\mathrm{ur}}L_{\lceil t\rceil}) \\ &= \mathrm{Gal}(K^{\mathrm{ab}}/K^{\mathrm{ur}}L_{\lceil t\rceil}), \end{aligned}$$

and

$$\begin{aligned} \mathrm{Art}_K^{-1}(\mathrm{Gal}(K^{\mathrm{ab}}/K^{\mathrm{ur}}L_{\lceil t\rceil})) &= \mathrm{Art}_K^{-1}\left(\varprojlim_{\substack{m,n \\ n\geq \lceil t\rceil}} \mathrm{Gal}(K_mL_n/K_mL_{\lceil t\rceil})\right) \\ &= \varprojlim_{\substack{m,n \\ n\geq \lceil t\rceil}} \mathrm{Art}_K^{-1}\left(\mathrm{Gal}(K_mL_n/K_mL_{\lceil t\rceil})\right) \\ &= \varprojlim_{\substack{m,n \\ n\geq \lceil t\rceil}} \frac{U_K^{(\lceil t\rceil)}}{U_K^{(n)}} \\ &= U^{\lceil t\rceil}. \end{aligned}$$

□

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

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

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

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

Proof. We have

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

Index