

# MATH 223A: ALGEBRAIC NUMBER THEORY

MELANIE MATCHETT WOOD

## 1. MONDAY SEPTEMBER 11

Math 223a is a course on *local fields*. The main text will be Serre's *Local Fields*, but we will also rely on Neukirch's *Algebraic Number Theory*; in particular, the sections on local fields. The prerequisites for this course are a year-long algebra sequence (e.g., Math 122 and 123), an algebraic number theory course at the level of Marcus (e.g., Math 129), and topology (e.g., Math 131).

The course is evaluated based on homework and an in-person final. The weekly homework is due on Fridays. The in-person final is not problem-solving based. Rather, it will test one's ability to write main ideas from the course, give the main definitions from the course, give examples and nonexamples of these definitions, state the main theorems of the course, etc. The goal of the final is to reinforce the basic knowledge taught in the course. See the Canvas page and syllabus for more details about the final or other aspects of the course.

**1.1. Introduction.** The easiest way to motivate local fields is using global fields. Here are some examples of global fields.

**Example 1.1.** The first example of a global field is an algebraic number field, i.e., an extension  $K$  of  $\mathbb{Q}$  such that  $[K : \mathbb{Q}] < \infty$ .

**Example 1.2.** Another example of a global field is a function field over a finite field. Just as in number theory, where our interest is studying  $\mathbb{Z} \subset \mathbb{Q}$ , we can analogously study  $\mathbb{F}_q[t] \subset \mathbb{F}_q(t)$ , where  $\mathbb{F}_q$  is a finite field of order  $q$  and  $\mathbb{F}_q[t]$  is the polynomial ring over  $\mathbb{F}_q$ . Here,  $\mathbb{F}_q(t)$  denotes the field of rational functions over  $\mathbb{F}_q$ , i.e., quotients  $p(t)/q(t)$ , where  $p(t), q(t) \in \mathbb{F}_q[t]$  and  $q(t) \neq 0$ . There is a deep analogy between  $\mathbb{Z} \subset \mathbb{Q}$  and  $\mathbb{F}_q[t] \subset \mathbb{F}_q(t)$ . For example, recall that like  $\mathbb{Z}$ , we have that  $\mathbb{F}_q[t]$  is a unique factorization domain. Finite extensions  $F$  of  $\mathbb{F}_q(t)$  are analogous to number fields.

Moreover, function fields can be regarded as algebro-geometric objects, and we can use this algebro-geometric viewpoint to glean more information about these function fields. One can show that there is a bijection

$\{C \text{ smooth, geometrically irreducible projective curve over } \mathbb{F}_q\} / \simeq \longleftrightarrow \{F \mid [F : \mathbb{F}_q(t)] < \infty\} / \simeq$   
(the “ $\simeq$ ” denotes “up to isomorphism”) given by taking a curve  $C$  to the field of rational functions on the curve.

For example,  $\mathbb{F}_q(t)$  is the field of rational functions on  $\mathbb{P}_{\mathbb{F}_q}^1$ .

The above examples are in fact *all* of the global fields.

In the 1930s and 1940s, number theorists were interested in *class field theory*, i.e., classifying the Galois extensions of  $K$  with abelian Galois group. This was done for  $K$  a number field and  $K$  a function field over  $\mathbb{F}_q$ . In the 1940s, Artin and Whaples axiomatized what was special about these examples by giving a definition of global fields in terms of *valuations*. They used their results to prove Dirichlet's unit theorem and the finiteness of the class group from the abstract definition (which does not use ideals, Minkowski theory, and the geometry of numbers).

## 1.2. Valuations.

**Definition 1.3.** Let  $K$  be a field. A *valuation* (sometimes *absolute value*) on  $K$  is a function  $|\cdot| : K \rightarrow \mathbb{R}$  such that

- (1)  $|x| \geq 0$  with equality holding if and only if  $x = 0$ ;
- (2)  $|xy| = |x||y|$ ;
- (3)  $|x + y| \leq |x| + |y|$  (triangle inequality).

**Example 1.4.** Every field has a trivial valuation given by  $|x| = 1$  for  $x \neq 0$ .

**Example 1.5.** Here are some nontrivial examples of valuations.

- (1)  $K = \mathbb{R}$  with the usual absolute value;
- (2)  $K = \mathbb{Q}$  with the usual absolute value;
- (3)  $K = \mathbb{Q}(\sqrt{2})$  with the usual absolute value;
- (4)  $K = \mathbb{C}$  with modulus:  $|a + bi| = \sqrt{a^2 + b^2}$  for  $a, b \in \mathbb{R}$ ;
- (5)  $K = \mathbb{Q}(i)$

**Example 1.6.** If  $K$  is a finite extension of  $\mathbb{Q}$  with  $[K : \mathbb{Q}] = n$ , then there are  $n$  homomorphisms  $\phi_1, \dots, \phi_n : K \rightarrow \mathbb{C}$  (e.g., there are two maps  $\mathbb{Q}(i) \rightarrow \mathbb{C}$ , one given by  $i \mapsto i$ ; the other by  $i \mapsto -i$ ). This gives  $n$  potentially different absolute values, where we could take  $|x| = |\phi_i(x)|$  for  $i = 1, \dots, n$ .

**Example 1.7.** Let  $K$  be a field extension of  $\mathbb{Q}$  such that  $[K : \mathbb{Q}] < \infty$ . Let  $\mathcal{O}_K$  be its ring of algebraic integers, and let  $\mathfrak{p}$  be a prime ideal of  $\mathcal{O}_K$ . For any  $x \in K$ , the principal (fractional) ideal  $(x) \subset \mathcal{O}_K$  can be factored into prime ideals. Let  $v_{\mathfrak{p}}(x)$  denote the power of  $\mathfrak{p}$  in this factorization of  $(x)$ . For any  $c > 1$ , we define

$$|x| = c^{-v_{\mathfrak{p}}(x)}.$$

It is quick to verify that this valuation satisfies the first two valuation axioms. The triangle inequality is satisfied because  $c > 1$  and because we are taking  $c$  to a negative power. The moral of the story is: things are small when they are divisible by lots of powers of  $\mathfrak{p}$ .

For number fields, these are in some sense all examples of valuations. Note that most of these valuations rely on primes. In fact, the absolute values coming from embeddings into  $\mathbb{C}$  are sometimes called “infinite primes.” Moreover, note that in the definition of valuations we made no reference to rings or ideals. Thus, valuations give us a way of talking about “primes of a field.”

The definition of a global field is one with valuations that all together have some global coherence. We should think that the adjective “global” refers to seeing all the primes (all the valuations) at once. Likewise, we will use “local” to mean that we are seeing just one prime (valuation). Hence, *local fields* are fields that see one of the valuations of a global field. Here are some examples of local fields.

**Example 1.8.**  $\mathbb{R}$  and  $\mathbb{C}$  are both examples of local fields. Recall that  $\mathbb{R}$  is the completion of  $\mathbb{Q}$  with respect to the usual absolute value.

**Example 1.9.** Let  $K$  be a global field and  $|\cdot|$  a  $\mathfrak{p}$ -adic valuation on  $K$ . This valuation gives a metric on  $K$ , where  $d(x, y) = |x - y|$ , making  $K$  into a metric space. We get another field  $K_{\mathfrak{p}}$  by taking the *completion* (in the usual sense with Cauchy sequences) of  $K$  “at  $\mathfrak{p}$ ” for the metric from  $|\cdot|$ .

If  $K = \mathbb{Q}$ , then  $\mathbb{Q}_p$ —the  $p$ -adic rationals—are the completion of  $\mathbb{Q}$  with respect to the  $p$ -adic valuation on  $\mathbb{Q}$ . The  *$p$ -adic integers*  $\mathbb{Z}_p \subset \mathbb{Q}_p$  is the ring of integers inside  $\mathbb{Q}_p$ , and  $\mathbb{Q}_p$  is the field of fractions of  $\mathbb{Z}_p$ .

These are all the examples of local fields, and we'll see an axiomatic definition later. Here are some connections between local and global fields:

- (1) Sometimes statements about global fields are proven by reducing to proving a statement about local fields.
- (2) There are lots of beautiful local-to-global principles. For example, the Hasse-Minkowski theorem says a quadratic form over a number field has a nontrivial solution if and only if it has a root over every completion. Another example is class field theory (classification of abelian extensions). We'll cover local class field theory, and in Math 223b these results will be put together into global class field theory, which allows us to understand the abelian extensions of global fields in terms of the abelian extensions of local fields.

**1.3. Discrete Valuation Rings.** Chapter 1 of Serre is recommended to accompany the following material.

**Definition 1.10.** Let  $K$  be a field. A *discrete valuation*<sup>1</sup> on  $K$  is a surjective homomorphism  $v : K^* \rightarrow \mathbb{Z}$  such that  $v(x + y) \geq \min(v(x), v(y))$ . Conventionally,  $v(0) = \infty$ .

**Example 1.11.** If  $K$  denotes a number field, and  $\mathfrak{p}$  is a prime, then  $v(x) = v_{\mathfrak{p}}(x)$  (the power of  $\mathfrak{p}$  dividing  $x$ ) is a discrete valuation.

**Definition 1.12.** For a field  $K$  with a discrete valuation  $v$ ,

$$A = \{x \in K \mid v(x) \geq 0\}$$

is a *discrete valuation ring*.

**Remark 1.13.** If  $A$  is a DVR with fraction field  $K$ , then an element  $\pi$  with  $v(\pi) = 1$  is called a *uniformizer*. All  $x \in A \setminus \{0\}$  can be written  $x = \pi^n u$  for  $n = v(x) \in \mathbb{N}$  and  $u \in A^*$ . Let  $\mathfrak{m} = (\pi) = \pi A$  be an ideal of  $A$ . Note that  $\mathfrak{m} = \{x \in K \mid v(x) \geq 1\}$  and that  $\mathfrak{m}$  is a maximal ideal. Moreover, all ideals of  $A$  are  $\mathfrak{m}^n$  for some  $n \in \mathbb{N}$ . The *residue field* is defined to be  $A/\mathfrak{m}$ .

**Example 1.14.** For example  $K = \mathbb{Q}$  with the  $p$ -adic valuation, then  $\pi = p$ , or  $\pi = -p$ , or  $\pi = pq$  for some other prime  $q$  are all examples of uniformizers. If  $v = v_p$  is our discrete valuation, then our DVR is  $A = \mathbb{Z}_{(p)} \subset \mathbb{Q}$ ,<sup>2</sup> and we have  $A = \{r/s \in \mathbb{Q} \mid p \nmid s \text{ for } r, s \in \mathbb{Z}\}$ . Note that  $\mathbb{Z} \subset A \subset \mathbb{Q}$ .

**Example 1.15.** Let  $k$  be a field, and let  $k((T))$  be the formal Laurent series in  $T$  with coefficients in  $k$ . For  $a_{n_0} \neq 0$ ,

$$v\left(\sum_{n \geq n_0} a_n T^n\right) = n_0$$

is a discrete valuation. Here,  $A = k[[T]]$ , the ring of formal power series.

## 2. WEDNESDAY SEPTEMBER 13

**2.1. Discrete Valuation Rings continued.** Suggested reading: Serre Chapter 1. Recall that if  $A$  is an integral domain and  $B$  is another ring containing  $A$ , then  $x \in B$  is said to be *integral* over  $A$  if there are  $a_1, a_2, \dots \in A$  such that  $x^n + a_1 x^{n-1} + \dots + a_n = 0$ . We say that  $B$  is *integral* over  $A$  if all elements of  $B$  are integral over  $A$ . If all elements of the field of fractions of  $A$  that are integral over  $A$  are in  $A$ .

<sup>1</sup>Warning: these are not valuations in the sense of the previous subsection!!

<sup>2</sup>This is not  $\mathbb{Z}_p$ !! Note that  $\mathbb{Z}_{(p)}$  is countable whereas  $\mathbb{Z}_p$  is not.

**Example 2.1.** Recall that algebraic integers are the  $x$  integral over  $\mathbb{Z}$ . Moreover,  $\mathbb{Z}$  is integrally closed by (Gauss's Lemma). If  $K$  is a number field, then  $\mathcal{O}_K$  is integrally closed in  $K$ .

**Lemma 2.2.** *Let  $A$  be a DVR with fraction field  $K$ . Suppose  $x_i \in K$  are such that  $v(x_i) > v(x_1)$  for all  $i \geq 2$ . Then  $x_1 + x_2 + \cdots + x_n \neq 0$ .*

*Proof.* Recall that

$$v(x_2 + \cdots + x_n) \geq \min(v(x_2), \dots, v(x_n)).$$

By assumption, the right-hand side of the above is greater than  $v(x_1) = v(-x_1)$ .  $\square$

**Proposition 2.3.** *Discrete valuation rings are integrally closed.*

*Proof.* Let  $A$  be a DVR. Take  $x \in K = \text{Frac}(A)$  such that  $x^n + a_1x^{n-1} + \cdots = 0$  with  $a_i \in A$ . Suppose  $v(x) = -m$  for some  $(m \in \mathbb{Z}_+)$ . The leading term has valuation  $-mn$ , while the rest of the terms have valuation at least  $-(n-1)m$ . Applying Lemma 2.2 finishes the proof.  $\square$

**2.2. Dedekind Domains.** The suggested reading for this section is Sections 1, 2, 8, 11, and 12 in Chapter 1 of Neukirch's *Algebraic Number Theory*.

**Definition 2.4.** (Localization) Let  $A$  be a domain and  $K$  its field of fractions. Let  $S \subset A$  be a multiplicatively closed subset of  $A$  containing 1. The *localization away from  $S$* , denoted  $S^{-1}(A)$ , is defined to be

$$S^{-1}A = \left\{ x \in K \mid x = \frac{a}{b} \text{ for } a \in A, b \in S \right\}.$$

**Example 2.5.** If  $S = A \setminus 0$ , then we get  $S^{-1}A = K$ . If  $S = A^*$ , we get  $S^{-1}A = A$ .

**Proposition 2.6.** *For a domain  $A$  and multiplicatively closed subset  $S \subset A$  containing the unit, we have the following bijective correspondence:*

$$\{\text{prime ideals of } S^{-1}A\} \longleftrightarrow \{\text{prime ideals of } A \text{ not intersecting } S\}$$

*given by taking  $\wp \subset S^{-1}A$  to  $\wp \cap A$ . The inverse of the map we just described is given by  $\mathfrak{p} \mapsto \mathfrak{p}S^{-1} = \{q/s \mid q \in \mathfrak{p}, s \in S\}$ .*

**Example 2.7.** Let  $S = A \setminus \wp$  for  $\wp$  some prime ideal of  $A$ . In this case, we use  $A_\wp$  to denote  $S^{-1}A$ . Note that  $A_\wp$  has exactly the primes that are contained in  $\wp$ . So  $A_\wp$  has a unique maximal ideal, i.e.,  $A_\wp$  is a *local ring*. If  $I$  is an ideal of  $A$ , we use  $I_\wp$  to denote the ideal of  $A_\wp$  generated by  $I$ .

**Theorem 2.8.** *If  $A$  is a Noetherian integral domain, then the following are equivalent:*

- (1) *For every nonzero prime ideal  $\wp$  of  $A$ , we have  $A_\wp$  is a DVR.*
- (2) *The ring  $A$  is integrally closed and has Krull dimension at most 1.*<sup>3</sup>

A ring  $A$  satisfying either of the conditions in Theorem 2.8 is called a *Dedekind domain*.

**Example 2.9.** Here are some simple examples of Dedekind domains:

- (1)  $\mathbb{Z}$  and  $\mathcal{O}_K$  for  $K$  a number field;
- (2)  $\mathbb{F}_q[t]$ ;
- (3)  $\mathbb{C}[t]$  (recall that  $\mathbb{C}(t)$  is not a global field);
- (4) any PID (using that PID  $\implies$  UFD and a valuation from factoring);
- (5)  $S^{-1}A$ , where  $A$  is a Dedekind domain, is also a Dedekind domain.

<sup>3</sup>Recall that a ring has Krull dimension 1 if and only if every nonzero prime ideal is maximal.

**Lemma 2.10.** *For a commutative integral domain  $A$ , we have*

$$\bigcap_{\wp} A_{\wp} = A.$$

*Proof.* Suppose  $x \in \bigcap_{\wp} A_{\wp}$ , and write  $x = a/b$  for  $a, b \in A$ . Consider  $\mathfrak{a} = \{d \in A \mid dA \in bA\}$ , i.e., the “ideal of denominators” of  $a/b$ . In other words, if there exists  $x \in A$  such that  $da = bc$ , then  $a/b = c/d$ . For every  $\wp$ , note that  $\mathfrak{a} \not\subset \wp$ . But every proper ideal is contained in a maximal (and hence prime) ideal by Zorn’s lemma. This forces  $\mathfrak{a} = A$ .  $\square$

*Proof of Theorem 2.8.* We’ll start by showing that condition (1) implies condition (2). Let  $\wp$  be a prime ideal of  $A$  contained in some maximal ideal  $\mathfrak{m}$ . Then  $A_{\mathfrak{m}}$  contains a prime  $\wp A_{\mathfrak{m}}$ . Since  $A_{\mathfrak{m}}$  is a DVR, and since we know what the ideals of a DVR look like (they are generated by all powers of the uniformizer), we have that  $\wp = 0$  or  $\wp = \mathfrak{m}$ . Hence,  $A$  has Krull dimension at most 1.

For integral closure, let  $x \in K = \text{Frac}(A)$  be integral over  $A$ . Then  $x$  is integral over  $A_{\wp}$  for all primes  $\wp$ . Since DVRs are integrally closed, it follows that  $x \in A_{\wp}$  for all  $\wp$ . Apply Lemma 2.10.  $\square$

**Definition 2.11.** Given an integral domain  $A$  with field of fractions  $K$ , a *fractional ideal*  $I$  of  $A$  is a finitely generated sub- $A$ -module of  $K$ . We can multiply fractional ideals and get another fractional ideal:  $IJ = \{\sum_{i=1}^n a_i b_i \mid a_i \in I, b_i \in J\}$ . We say  $I$  is *invertible* if there exists a fractional ideal  $J$  such that  $IJ = A$ .

**Proposition 2.12.** *In a Dedekind domain, every nonzero fractional ideal is invertible.*

**Remark 2.13.** The above is equivalent to the other conditions defining a Dedekind domain from Theorem 2.8.

*Proof of Proposition 2.12.* In a DVR, all fractional ideals are  $(\pi^n)$  for some  $n \in \mathbb{Z}$ . Hence,  $(\pi^n)(\pi^{-n}) = (1)$ , so every fractional ideal is invertible.

For a general Dedekind domain  $A$  with fractional ideal  $I$ , let  $J = \{x \in K \mid xI \subset A\}$ . This is a good candidate for the inverse of  $I$ , since  $IJ \subset A$  and since when  $I$  is principal,  $J$  is the ideal of denominators. If  $IJ \neq A$ , then  $IJ \subset \wp$  for some prime ideal  $\wp$ . We can check that  $J_{\wp} = \{x \in K \mid xI_{\wp} \subset A_{\wp}\}$  and that  $(IJ)_{\wp} = I_{\wp}J_{\wp}$ . Since  $A_{\wp}$  is a DVR, we have that  $I_{\wp}J_{\wp} = A_{\wp}$ , contradicting the fact that  $IJ \subset \wp$ . Therefore  $IJ = A$ .  $\square$

**Theorem 2.14.** *For a Dedekind domain  $A$ , every fractional ideal can be written uniquely as*

$$\prod_{\wp} \wp^{a_{\wp}}$$

for some  $a_{\wp} \in \mathbb{Z}$ , where all but finitely many  $a_{\wp} = 0$ .

*Proof of uniqueness.* If  $I = \prod \wp^{a_{\wp}}$ , then at a prime  $\wp$ , we have  $I_{\wp}$  is an ideal in the DVR  $A_{\wp}$ . Moreover,  $a_{\wp}$  is the valuation of a generator of  $I_{\wp}$ . Uniqueness follows.  $\square$

### 3. MONDAY SEPTEMBER 18

**3.1. Integrality.** Reference: Neukirch Chapter 1 Section 2. The following equates the condition of integrality with that of being finitely generated as a module.

**Proposition 3.1.** *Given (commutative) rings  $A \subset B$ , and  $b_1, \dots, b_n \in B$ , the  $b_i$ ’s are integral over  $A$  if and only if  $A[b_1, \dots, b_n]$  is a finitely generated  $A$ -module.*

*Proof.* If  $b$  is integral, then  $A[b]$  is generated by  $1, \dots, b^{d-1}$  ( $d$  being the degree of the monic polynomial in  $A[x]$  that  $b$  is a root of) as an  $A$ -module. So  $A[b_1, \dots, b_n]$  is a finitely generated  $A$ -module by induction if  $b_1, \dots, b_n$  are integral over  $A$ .

For the converse, suppose  $A[b_1, \dots, b_n]$  is a finitely generated  $A$ -module generated by  $w_1, \dots, w_r$  as an  $A$ -module. For  $b \in A[b_1, \dots, b_n]$ , we have  $bw_i = \sum_{j=1}^n a_{ij}w_j$  for  $a_{ij} \in A$ . Given a matrix  $A \in M_n(A)$ , recall that its *adjugate*,  $\text{adj}(A)$ , has the property that  $\text{adj}(A)A = \det(A)I$ . Consider the matrix whose  $(i, j)$ -entry is given by  $b\delta_{ij} - a_{ij} \in B$ . Since applying  $M$  to  $(w_1, \dots, w_n)^t$  gives the 0 vector, we have  $\det(M)(w_1, \dots, w_n)^t = \det(M)I(w_1, \dots, w_n)^t = \text{adj}(M)M(w_1, \dots, w_n)^t = 0$ . Since we may write  $1 \in A[b_1, \dots, b_n]$  as a linear combination of the  $w_i$ 's, we must have  $\det(M) = 0$ . Thus, viewing  $\det(M)$  as a monic polynomial in  $b$  over  $A$ , we have that  $b$  is a root of this polynomial and is thus integral.  $\square$

The techniques used in the above allow us to prove the following result without any complicated constructions:

**Corollary 3.2.** *The elements of  $B$  integral over  $A$  form a subring of  $B$ .*

*Proof.* Because  $b_1 + b_2, b_1, b_2 \in A[b_1, b_2]$ , we have  $A[b_1, b_2] = A[b_1, b_2, b_1 + b_2]$ . Hence, if  $A[b_1, b_2]$  is finitely generated, then so is  $A[b_1, b_2, b_1 + b_2]$ . It follows that  $b_1 + b_2$  is integral. A similar argument applies for  $b_1b_2$ .  $\square$

**Corollary 3.3.** *Let  $A \subset B \subset C$  be rings such that  $C$  is integral over  $B$  and  $B$  is integral over  $A$ . Then  $C$  is integral over  $A$ .*

*Proof.* We adjoin elements one by one. For each  $c \in C$  that is integral over  $B$  (so that  $c^n + b_1c^{n-1} + \dots + b_n = 0$ ), we apply Proposition 3.1 to  $A, B' := A[b_1, \dots, b_n]$ , and  $C' = B[c]$ . More generally, if each is a module-finite extension where  $c_i$ 's generate  $C$  over  $B$  as a module and  $b_j$ 's generate  $B$  over  $A$ , then the set of  $c_i b_j$ 's generates  $C$  as an  $A$ -module.  $\square$

### 3.2. Extensions of Dedekind Domains: Construction and Examples.

**Definition 3.4.** Let  $A$  be a Dedekind domain with field of fractions denoted  $K$ . Let  $L$  be a finite extension of  $K$ , and let  $B$  be the integral closure of  $A$  in  $L$ . Then  $B$  is said to be an extension of  $A$ .

**Example 3.5.** Consider  $\mathbb{Z} \subset \mathbb{Q}$  as our Dedekind domain and  $\mathbb{Q}(\sqrt[3]{2})$  as our extension of fields. Note that  $\mathbb{Z}[\sqrt[3]{2}]$  is the ring of integers of  $\mathbb{Q}(\sqrt[3]{2})$ ; this is an extension of  $\mathbb{Z}$ .

**Example 3.6.** Here's another example. Let  $A = \mathbb{F}_q[t]$  with  $K = \mathbb{F}_q(t)$ . Let  $L$  be the field extension given by  $\mathbb{F}_q(t)[\sqrt{t^3 + t - 1}] = K[s]/(s^2 - (t^3 + t + 1))$ . This is a quadratic field extension since  $[L : K] = 2$ . We may interpret this geometrically as follows: regard  $K$  as the field of functions on  $\mathbb{P}_{\mathbb{F}_q}^1$  and  $L$  as the field of functions on the elliptic curve given by  $E : s^2 = t^3 + t + 1$ . The field extension  $L/K$  corresponds to the 2-to-1 map  $E \rightarrow \mathbb{P}^1$ . Assuming that  $\text{char}(\mathbb{F}_q) \neq 2$ , the integral closure of  $A$  in  $L$  is  $B = \mathbb{F}_q[t, \sqrt{t^3 + t + 1}]$ .

**Remark 3.7.** In the example given above, we could just as easily have taken  $A = \mathbb{F}_q[1/t]$  (with  $K$  and  $L$  the same). However, in this case,  $\sqrt{t^3 + t + 1}$  is *not* integral over  $A$ . Hence, it is very important to specify the Dedekind domain you start out with!

### 3.3. Various Properties of Extensions of Dedekind Domains.

**Proposition 3.8.** *Given an extension  $B$  in  $L$  of a Dedekind domain, we have that  $B$  is a ring with field of fractions  $L$ .*

*Proof.* The integral closure of a ring in a field is a ring. Thus, we only need to prove that  $L = \text{Frac}(B)$ . To do so, note that any element of  $L$  satisfies a monic polynomial over  $K$ ; we can clear denominators to get some  $A$ -multiple that is integral over  $A$ .  $\square$

**Theorem 3.9.** *Extensions of Dedekind domains are also Dedekind.*

**Proposition 3.10.** *Let  $B$  be an extension of a Dedekind domain  $A$  in a field extension  $L$  of  $K = \text{Frac}(A)$ . Then if  $L/K$  is separable, then  $B$  is a finitely generated  $A$ -module.<sup>4</sup>*

Before proving the above proposition, we review a few facts that will be imminently relevant. Let  $L/K$  be an extension of fields. Given  $x \in L$ , we have a  $K$ -linear map  $m_x : L \rightarrow L$  taking  $\alpha \mapsto x\alpha$ . The *trace* and *norm* of  $x$  are subsequently defined to by

$$\text{Tr}_{L/K}(x) = \text{tr}(m_x) \quad \text{and} \quad N_{L/K}(x) = \det(m_x).$$

If the extension  $L/K$  is Galois, then we have

$$\text{Tr}_{L/K}(x) = \sum_{i=1}^n \sigma_i(x) \quad \text{and} \quad N_{L/K}(x) = \prod_{i=1}^n \sigma_i(x),$$

where  $\sigma_1(x), \dots, \sigma_n(x)$  are the Galois conjugates of  $x$ . Recall that  $L/K$  is separable if and only if  $\langle x, y \rangle := \text{Tr}_{L/K}(xy)$  is a nondegenerate  $K$ -bilinear form on  $L$  (i.e.,  $\langle x, y \rangle = 0$  for all  $y$  implies  $x = 0$ ).

*Proof of Proposition 3.10.* If  $x \in B$ , then the conjugates of  $x$  over  $K$  are integral over  $A$ . Hence,  $\text{Tr}_{L/K}(x)$  is integral over  $A$ . Because  $A$  is integrally closed (recall that Dedekind domains are integrally closed), it follows that  $\text{Tr}_{L/K}(x) \in A$ .

Now, let  $e_1, \dots, e_d$  be a basis for  $L/K$  with  $e_i \in B$  for all  $i$ . Let  $V$  be the free  $A$ -module spanned by the  $e_i$ . For a sub- $A$ -module of  $L$ , let  $M^*$  be the set of  $x \in L$  such that  $\text{Tr}_{L/K}(xy) \in A$  for all  $y \in M$ . We have the following chain of inclusions:

$$V \subset B \subset B^* \subset V^*.$$

Since  $V^*$  is spanned by the basis dual to the  $e_i$ 's (using separability), it follows that  $B \subset V^*$  is finitely generated as an  $A$ -module.  $\square$

Before proving Theorem 3.9, we present the following helpful lemmas, the first of which shows that an extension of a Dedekind domain has Krull dimension at most 1.

**Lemma 3.11.** *Let  $B$  be an extension of the Dedekind domain  $A$ . If  $\wp \subset \wp'$  are prime ideals of  $B$ , and we have  $\wp \cap A = \wp' \cap A$ , then  $\wp = \wp'$ .*

*Proof.* Without loss of generality we may assume that  $\wp = 0$ , as otherwise we can work in  $B/\wp$ . If  $x \in \wp' \setminus \{0\}$ , let  $x^n + a_{n-1}x^{n-1} + \dots + a_0$  be the minimal polynomial of  $x$  with coefficients  $a_i \in A$ . This implies  $a_0 \neq 0$ , and  $x \in \wp'$  implies that  $a_0 \in \wp'$ . Hence,  $\wp' \neq 0$ . Therefore, if  $\wp_0 \subsetneq \wp_1 \subsetneq \wp_2$  are primes of  $B$ , then  $\wp_0 \cap A \subsetneq \wp_1 \cap A \subsetneq \wp_2 \cap A$ , contradicting the one-dimensionality of  $A$ .  $\square$

We also use the following, which is given as an exercise:

**Lemma 3.12.** *In a 0-dimensional Noetherian ring, a descending sequence of ideals stabilizes.*

<sup>4</sup>Serre calls this Hypothesis F in *Local Fields*.

*Proof of Theorem 3.9.* As usual, let  $A$  be our Dedekind domain with fraction field  $K$ , and let  $B$  denote our extension of  $A$  in the field extension  $L/K$ . Lemma 3.11 implies that  $B$  has Krull dimension at most 1.

Next, we show that extensions of Dedekind domains are Noetherian. Note that if  $L/K$  is separable, then Proposition 3.10 an extension  $B$  of a Dedekind domain  $A$  is a finitely generated  $A$ -module, which tells us that  $B$  is Noetherian. We use Lemma 3.12 to relate the condition of being Noetherian (one that has to do with ascending chains of ideals) to descending chains of ideals.

Let  $w_1, \dots, w_n$  be a basis of  $L/K$  contained in  $B$ . Then we have that  $B_0 = A[w_1, \dots, w_n]$  is a finitely generated  $A$ -module, implying that  $B_0$  is Noetherian. In order to prove that  $B$  is Noetherian, we will show that any ideal  $I$  of  $B$  is a finitely generated  $B$ -module. Let  $a \in I \cap A$  be some nonzero element.

We claim that  $B/aB$  is a finitely generated  $B_0$ -module. As an exercise, we show that  $B_0/aB_0$  is a 0-dimensional Noetherian ring. We have a descending chain of ideals in  $B$  given by  $(a^m B \cap B_0, aB_0)$  for  $m \in \mathbb{N}$ , which gives us a descending sequence of ideals  $(a^m B_0 \cap B_0)$  in  $B_0/aB_0$ . By Lemma 3.12, this stabilizes at some  $n$ . We now show that  $B \subset a^{-n}B_0 + aB$ . For  $\beta \in B$ , let  $\beta = b/c$  for  $b, c \in B_0$  (recall from its construction that the fraction field of  $B_0$  is  $L$ ). Now, consider the descending sequence of ideals in  $B_0/cB_0$  given by  $(\bar{a}^m)$ . This stabilizes at some  $h$ —i.e.,  $a^h = xa^{h+1}$  modulo  $cB_0$  for some  $x \in B_0$ . Therefore,  $(1 - xa)a^h \in cB_0$ , and we may write

$$\beta = \frac{b}{c}(1 - xa) + \beta xa = \frac{b(1 - xa)a^h}{a^h c} + \beta xa.$$

Note that  $(1 - xa)a^h/c \in B_0$ ; let  $h$  be minimal such that  $\beta \in a^{-h}B_0 + aB$ . To be continued...  $\square$

#### 4. WEDNESDAY SEPTEMBER 20

**4.1. Extensions of Dedekind Domains are Dedekind.** We recall some standard notation from last lecture. We are looking at extensions of Dedekind domains—let  $A$  be a Dedekind domain with fraction field  $K$  and  $L/K$  a finite extension with  $B$  the integral closure of  $A$  in  $L$ . We are trying to prove Theorem 3.9, i.e., that  $B$  is a Dedekind domain.

*Proof of Theorem 3.9 continued.* It remains to show that  $B$  is Noetherian. Recall that  $w_1, \dots, w_n \in B$  is a basis for  $L/K$  and that we showed that  $B_0 = A[w_1, \dots, w_n]$  is a finitely generated  $A$ -module.

We claim that  $B/aB$  is a finitely generated  $B_0$  module. The proof of this claim is as follows. We have ideals  $I_m = (a^m B \cap B_0, aB_0)$  of  $B_0$ , which stabilize for  $m \geq n$ . We take  $\beta \in B$  and aim to show that  $\beta \in a^{-n}B_0 + aB$ . Last class, we proved that there is a minimal  $h$  such that  $\beta \in a^{-h}B_0 + aB$ . If  $h \leq n$ , then we are done. Suppose for the sake of contradiction that  $h > n$ . Let  $\beta = u/a^h + a\tilde{u}$  for  $u \in B_0$  and  $\tilde{u} \in B$ . Then  $u = a^h(\beta - a\tilde{u}) \in a^h B \cap B_0 \subset I_h = I_{h-1}$ , since  $h > n$  and the  $I_m$ 's stabilize. Therefore  $u = a^{h-1}u' + a\tilde{u}'$  for  $u' \in B_0$  and  $\tilde{u}' \in B$ . Then  $\beta = u'/a^{h-1} + a(\tilde{u}' + u')$ , contradicting the minimality of  $h$ . Hence,  $\beta \in a^{-n}B_0 + aB$ , which tells us that  $B/aB \subset (a^{-n}B_0 + aB)/aB$ . Thus,  $B/aB$  is finitely generated as a  $B_0$ -module.

It follows that  $B/aB$  is a finitely generated  $A$ -module. For any ideal  $I \ni a$  of  $B$ , we have  $I/aB$  is a finitely generated  $A$ -module, since  $I/aB \subset B/aB$  and  $A$  is Noetherian. It follows that  $I$  is a finitely generated  $B$ -module, proving that  $B$  is Noetherian.  $\square$

**4.2. Primes in Extensions.** In an extension of a Dedekind domain, we would like to see how primes in  $A$  factor in  $B$ . Let  $\mathfrak{p}$  be a nonzero prime ideal of  $A$ . We write  $\mathfrak{p}B$  for the ideal of  $B$



generated by  $\mathfrak{p}$ , i.e.,

$$\mathfrak{p}B = \left\{ \sum_i a_i b_i \mid a_i \in \mathfrak{p}, b_i \in B \right\}.$$

We may factor

$$\mathfrak{p}B = \prod_{\varphi|\mathfrak{p}} \varphi^{e_\varphi}$$

into a product of primes  $\varphi$  of  $B$ . The exponent  $e_\varphi$  is called the *ramification index* of  $\varphi$  in  $L/K$ , and  $\varphi$  is said to *ramify* if  $e_\varphi > 1$ , and  $\mathfrak{p}$  ramifies if any  $e_\varphi > 1$  for  $\varphi|\mathfrak{p}$ .

**Proposition 4.1.** *With notation as above,  $\mathfrak{p} = \varphi \cap A$  (for  $\varphi|\mathfrak{p}$ ).*

*Proof.* We have  $A/(\varphi \cap A) \subset B/\varphi$ , which is a domain, so  $\varphi \cap A$  is prime. Moreover,  $\varphi \cap A \supset \mathfrak{p}B \cap A \supset \mathfrak{p}$ . Since  $\mathfrak{p} \neq 0$ , this forces  $\mathfrak{p} = \varphi \cap A$ .  $\square$

Also note that if  $\varphi$  is a prime of  $B$ , then  $\varphi \cap A$  is a prime of  $A$ .

The induced map  $A/\mathfrak{p} \rightarrow B/\varphi$  is a field homomorphism. The degree of this map (i.e., field extension), which we denote using  $f_\varphi = [B/\varphi : A/\mathfrak{p}]$ , is called the *inertia degree* of  $\varphi$  in  $L/K$ ;  $\mathfrak{p}$  is said to *split completely* if all  $e_\varphi = f_\varphi = 1$  for  $\varphi|\mathfrak{p}$ .

**Proposition 4.2.** *If  $B$  is a finitely generated  $A$ -module (proposition (F) in Serre) (e.g., if  $L/K$  is a separable field extension), then  $[L : K] = \sum_{\varphi|\mathfrak{p}} e_\varphi f_\varphi$ .*

*Proof.* As was the case with number fields, we analyze  $B/\varphi$  as an  $A/\mathfrak{p}$ -vector space and count the dimension in two ways using the fact that  $B$  is generated as an  $A$ -module from a basis of  $L/K$ .  $\square$

**Remark 4.3.** In general (without (F)), we have  $[L : K] \geq \sum_{\varphi|\mathfrak{p}} e_\varphi f_\varphi$ .

The notion of inertia degree allows us to define a *relative ideal norm*. Given a group of fractional ideals of  $A$ , denoted  $I_A$ , we have a map  $N_{B/A} : I_B \rightarrow I_A$  taking a prime  $\varphi \mapsto (\varphi \cap A)^{f_\varphi}$ .

**Proposition 4.4.** *If  $x \in L$ , then  $N_{B/A}(xB) = N_{L/K}(x)A$ .*

**4.3. The Galois Scenario.** Now assume  $L/K$  is Galois. Recall that  $\text{Gal}(L/K)$  acts on primes  $\varphi|\mathfrak{p}B$  for some nonzero prime  $\mathfrak{p}$  of  $A$ .

**Proposition 4.5.** *The action of  $\text{Gal}(L/K)$  on  $\varphi|\mathfrak{p}B$  is transitive.*

*Proof.* Assume that  $\varphi$  is not in the Galois orbit of  $\varphi'$  for  $\varphi, \varphi'|\mathfrak{p}B$ . Using the Chinese Remainder Theorem, we can find  $b \in \varphi$  such that  $b \notin \sigma\varphi'$  for any  $\sigma \in \text{Gal}(L/K)$ , i.e.,  $\sigma^{-1}b \notin \varphi'$ . Hence,  $N_{L/K}(b) \in \varphi$ , but  $N_{L/K}(b) = \prod_\sigma \sigma^{-1}b \notin \varphi'$  by the primality of  $\varphi'$ . Since  $N_{L/K}(b) \in A$ , we have a contradiction, since  $\varphi \cap A = \varphi' \cap A$ .  $\square$

**Corollary 4.6.** *For  $\varphi, \varphi'|\mathfrak{p}B$ , we have  $e_\varphi = e_{\varphi'} = e$  and  $f_\varphi = f_{\varphi'} = f$ .*

The *decomposition group* of some prime  $\varphi$  of  $B$  in  $L/K$  is the stabilizer of  $\varphi$  in the Galois group and is denoted  $D = D_\varphi(L/K) \subset \text{Gal}(L/K)$ . For  $\varphi, \varphi'|\mathfrak{p}B$ , we have that  $D_\varphi(L/K)$  and  $D_{\varphi'}(L/K)$  are conjugate. The order of  $D$  is  $|D| = ef = [L : K]/r$ , where  $r$  is the number of primes of  $B$  dividing  $\mathfrak{p}$ . Galois theory then gives us the *decomposition field* of  $\varphi$  for  $L/K$ , denoted  $K_D/K$ , which is the subfield of  $L$  fixed by  $D$ . Note that  $[K_D : K] = r$  and that  $[L : K_D] = ef$ . Colloquially, the decomposition field is “where the decomposition happens.”

Now, let’s assume  $A/\mathfrak{p}$  is finite (we do so because this holds in all of the cases we are interested in). Since  $D$  fixes  $\varphi|\mathfrak{p}$ , we get a  $D$ -action on  $B/\varphi$  fixing  $A/\mathfrak{p}$ . This action gives us a homomorphism

$\phi : D \rightarrow \text{Gal}((B/\wp)/(A/\mathfrak{p}))$ . The *inertia group* of  $\wp$  for  $L/K$  is defined to be  $T = T_\wp(L/K) = \ker(\phi)$ . In other words, elements of  $D$  that fix  $B/\wp$  pointwise, i.e., that the residue fields cannot see. Likewise, we define the *inertia field*  $K_T$  of  $\wp$  to be the fixed field of  $T$ .

**Proposition 4.7.** *The map  $\phi : D/T \rightarrow \text{Gal}((B/\wp)/(A/\mathfrak{p}))$  is an isomorphism.*

*Proof.* Idea: find a  $\sigma \in \text{Gal}(L/K)$  mapping an element to each conjugate by comparing minimal polynomials in  $B$  and  $B/\wp$ .  $\square$

It follows that  $|T| = e$ . The inertia group is “all about ramification” and is in fact the first of what are called *higher ramification groups*. Hence the inertia group should have been called the ramification group.

If  $L/K$  is *unramified* at  $\wp$ , we have  $D = \text{Gal}((B/\wp)/(A/\mathfrak{p}))$  is generated by the *Frobenius automorphism* which takes  $x \mapsto x^{|A/\mathfrak{p}|}$ . This element is often denoted as  $\text{Frob}_\wp \in D$ , as  $(\wp, L/K)$ , or as  $\left(\frac{\wp}{L/K}\right)$ .

**Example 4.8.** Let  $A = \mathbb{Z}$ ,  $K = \mathbb{Q}$ , and  $L = \mathbb{Q}(\zeta_n)$ , where  $\zeta_n$  is a primitive  $n$ th root of unity. There is an isomorphism  $(\mathbb{Z}/n\mathbb{Z})^* \simeq \text{Gal}(L/K)$  given by taking  $a \in (\mathbb{Z}/n\mathbb{Z})^*$  to the element of  $\text{Gal}(L/K)$  given by  $\zeta_n \mapsto \zeta_n^a$ . If  $p > 0$  is a prime element of  $\mathbb{Z}$  such that  $p \nmid n$  is unramified, then  $\text{Frob}_\wp = \left(\frac{\wp}{L/K}\right)$  corresponds to  $p$  under the map described above.

Since there are infinitely many  $p$  in each class of  $(\mathbb{Z}/n\mathbb{Z})^*$ , it follows that

**Remark 4.9.** When  $\wp$  is unramified, we have that  $D$  is cyclic and is generated by  $\text{Frob}_\wp$ .

In non-Galois separable extensions, we often will take the normal (Galois) closure and use these groups. Moreover, if we have two extended Dedekind domains, where  $A \subset B \subset C$  are the Dedekind domains with respective fields of fractions  $K \subset L \subset M$  with  $M/K$  Galois, then  $D(M/L) = D(M/K) \cap \text{Gal}(M/L)$  and  $T(M/L) = T(M/K) \cap \text{Gal}(M/L)$ . For  $\wp'$  a prime of  $M$ ,  $\wp$  a prime of  $L$ , and  $\mathfrak{p}$  a prime of  $K$ , we have  $\wp' | \wp C | \mathfrak{p} C$ .

**Remark 4.10.** Note that the order of  $\text{Frob}_\wp$  is  $f_\wp$ .

## 5. MONDAY SEPTEMBER 25

**5.1. Completions.** The recommended reading to supplement the following is Serre Chapter 2 and Neukirch Chapter 2 Sections 1-4 and 8-9. Let  $A$  be a Dedekind domain with  $\wp$  a prime. We have a local ring  $A_\wp$ , but  $A$  and  $A_\wp$  have the same field of fractions  $K$ . Note that  $K$  has all of the discrete valuations from primes of  $A$ . So in a sense we still have information about all of the other primes.

Let  $K$  be a field with discrete valuation  $v$  and discrete valuation ring  $A$ . Note that  $A$  has a *valuation*, or *absolute value* which is defined as follows. For  $0 < c < 1$ , define  $|x| = c^{v(x)}$  for  $x \neq 0$  and  $|0| = 0$ . Recall that a valuation has the following properties:

- (1)  $|x| = 0$  if and only if  $x = 0$ ;
- (2)  $|x||y| = |xy|$ ;
- (3)  $|x + y| \leq \max(|x|, |y|) \leq |x| + |y|$ .

An absolute value is called *nonarchimedian* (or, as Serre calls it, *ultrametric*) when (3) holds and *archimedian* otherwise.

For any field  $K$  with an absolute value  $|\cdot|$ , we have a completion  $\widehat{K}$  for the topology defined by the metric  $d(x, y) := |x - y|$ , i.e., equivalence classes of Cauchy sequences  $\{a_n\}_{n \in \mathbb{N}}$  with  $a_n \in K$  such that for all  $\epsilon > 0$ , there exists  $N$  such that for  $n, m \geq N$ , we have  $|a_n - a_m| < \epsilon$ . Note that

$\widehat{K}$  is a field: we have  $\{0\}$ ,  $\{1\}$ ,  $\{a_n\} + \{b_n\} = \{a_n + b_n\}$ , and  $\{a_n\}\{b_n\} = \{a_nb_n\}$ . Moreover,  $\widehat{K}$  is complete and  $\widehat{K}$  has an absolute value, where  $|\{a_n\}| = \lim_{n \rightarrow \infty} |a_n|$ .

**Example 5.1.** Take  $K = \mathbb{Q}$  with the usual absolute value. Then  $\widehat{K} = \mathbb{R}$ .

Let  $|\cdot|$  be an absolute value arising from a discrete valuation  $v$ . Define  $\widehat{v}(x)$  for  $x \in \widehat{K}$  to be such that  $|x| = c^{\widehat{v}(x)}$ . Since  $c^{\mathbb{Z}}$  is discrete, we have  $\widehat{v}(x) \in \mathbb{Z}$  and  $\widehat{v}$  is a discrete valuation on  $\widehat{K}$  with valuation ring  $\widehat{A}$ . Further,  $\widehat{A}$  is the topological closure of  $A$  in  $\widehat{K}$ . We call  $\widehat{A}$  a *complete discrete valuation ring*. Note that we can get all elements of  $\widehat{A}$  with Cauchy sequences  $\{a_n\}$  for  $a_n \in A$ .

Here are some other ways of viewing the elements of  $\widehat{A}$ . If  $\pi$  is a uniformizer, then  $\widehat{A}$  is the *inverse/projective limit* of  $A/\pi^n A$ :

$$\widehat{A} = \varprojlim_n A/\pi^n A.$$

The above is equal to the following

$$\{(r_n)_{n \in \mathbb{N}} \mid r_n \in A/\pi^n A \text{ such that } m > n \text{ implies } \overline{r_m} \equiv r_n \pmod{\pi^n}\}.$$

Note that  $\widehat{A}[1/\pi] = \widehat{K}$  and that  $\pi$  is also a uniformizer of  $\widehat{A} \subset \widehat{K}$ .

Let  $S$  be set of a choices of representatives of  $A/(\pi)$  in  $A$  (e.g.,  $0, 1, \dots, p-1$  for  $\mathbb{Z}/p\mathbb{Z}$ ).

**Proposition 5.2.** *Every element  $a \in \widehat{A}$  can be written uniquely as a convergent power series*

$$a = \sum_{n=0}^{\infty} s_n \pi^n$$

for  $s_n \in S$ . Similarly, every  $x \in \widehat{K}$  can be represented uniquely as a convergent Laurent series:

$$x = \sum_{n=-m}^{\infty} s_n \pi^n$$

for  $s_n \in S$ .

Note that  $A$  might be countable, but  $\widehat{A}$  is uncountable.

**Example 5.3.** Let  $K = \mathbb{Q}$ , and let  $v$  be the  $p$ -adic valuation for some prime  $p$ . Then  $\widehat{K} = \mathbb{Q}_p$  and  $\widehat{A} = \mathbb{Z}_p$ .

**Example 5.4.** Consider  $K = \mathbb{F}_q(t)$  with  $v$  the  $t$ -adic valuation for the prime  $(t) \in \mathbb{F}_q[t]$ . Here we have  $\widehat{K} = \mathbb{F}_q((t))$  and  $\widehat{A} = \mathbb{F}_q[[t]]$ .

What is special about the characterizations of  $\widehat{K}$  and  $\widehat{A}$  given in Proposition 5.2 is that we may choose  $S$  to be closed under addition and multiplication, which makes doing arithmetic in  $\widehat{K}$  much easier (we may do arithmetic with power series by multiplying and adding their coefficients).

Let  $A$  be a Dedekind domain with fraction field  $K$  and prime ideal  $\mathfrak{p}$ . Let  $v$  be the  $\mathfrak{p}$ -adic valuation. Here, we use  $K_{\mathfrak{p}}$  to denote  $\widehat{K}$ . Warning: we don't write  $A_{\mathfrak{p}}$  for  $\widehat{A}$  as otherwise we would confuse this notation with that of localization away from  $\mathfrak{p}$ . Note that  $A_{\mathfrak{p}} \subset K$  and that  $v(A_{\mathfrak{p}}) \geq 0$ . Moreover, note that  $A_{\mathfrak{p}} \subset \widehat{A}$  as constant Cauchy sequences; this should illustrate the extent to which  $\widehat{A}$  and  $\widehat{K}$  are much bigger than  $A_{\mathfrak{p}}$ .

Let  $K$  be a field with discrete valuation  $v$  with valuation ring  $A$ . Suppose  $K$  is complete with respect to the metric induced by  $v$ . Let  $L$  be a finite extension of  $K$ , and let  $B$  be the integral closure of  $A$  in  $L$ .

**Proposition 5.5.** *With notation as in the preceding paragraph, we have that  $B$  is a discrete valuation ring, a free  $A$ -module of rank  $[L : K]$ , and  $L$  is complete with respect to the metric given by  $B$ 's valuation.*

**Remark 5.6.** Contrast the above with  $A = A_\wp$ . If  $B$  is an extended Dedekind domain, then  $B$  contains all primes  $\wp_i | \wp B$ .

*Part of the proof of Proposition 5.5.* Let  $\wp_i$  be the primes of  $B$  ( $\wp_i \cap A = (\pi)$ ) with valuations  $w_i$ . By equivalence of norms on a vector space over a complete field, all the  $w_i$  give the same topology on  $L$ . Take  $x \in B$  with  $w_1(x) > 0$  and  $w_2(x) = 0$ . Then  $x^n \rightarrow 0$  in the topology induced by  $w_1$ , but  $x^n$  does not converge to 0 in the topology induced by  $w_2$ . Therefore, there can only be one nonzero prime of  $B$ .  $\square$

Even when  $L$  is not separable over  $K$ , we have proposition (F): that  $B$  is a finitely generated  $A$ -module. So  $\sum_i e_i f_i = L : K$ , but since there is only one prime in both  $L$  and  $K$ , this simplifies to  $ef = [L : K]$ . If  $w$  is the valuation on  $L$ , then

$$w(x) = \frac{v(N_{L/K}(x))}{f}$$

for  $x \in L$ . Here's how to remember this:

$$(N_{L/K}(\pi_L)) = N_{B/A}((\pi_L)) = (\pi_K)^f.$$

Now, let  $A$  be a discrete valuation ring with fraction field  $K$  and  $B$  an extension of  $A$  in  $L/K$  ( $K$  is not necessarily complete here). Suppose Proposition (F) holds so that  $B$  is a finitely generated  $A$ -module. Let  $\mathfrak{p}$  be some nonzero prime of  $A$ , and let  $\wp_i$  be the primes of  $B$  dividing  $\mathfrak{p}B$ . For  $x \in K$ , we have that

$$v_{\wp_i}(x) = e_{\wp_i} v_{\mathfrak{p}}(x)$$

for  $x \in K$ . We say that  $v_{\wp_i}$  *prolongs*  $v_{\mathfrak{p}}$  to  $L$  with index  $e_{\wp_i}$ .

**Proposition 5.7.** *Let  $w$  be a discrete valuation prolonging  $v_{\mathfrak{p}}$  to  $L$ . Then  $w = v_{\wp}$  for some  $\wp | \mathfrak{p}$ .*

*Proof.* Let  $W$  be the valuation ring for  $w$  with maximal ideal  $\mathfrak{m}$ . So  $W$  is integrally closed and has fraction field  $L$ . Moreover,  $A \subset W$ . Thus,  $B \subset W$ . Let  $\wp = \mathfrak{m} \cap B$ . We have  $\wp \cap A = \mathfrak{p}$ , implying  $B_\wp \subset W$ . If  $W$  contains an element with negative  $v_{\wp}$  valuation, then  $W = L$ , which is a contradiction. Hence,  $W = B_\wp$ .  $\square$

Let  $\widehat{K}$  be the completion of  $K$  with respect to the valuation  $v_{\mathfrak{p}}$ . This gives us several different completions of  $L$ , where we use  $\widehat{L}_i$  to denote the completion of  $\widehat{L}_i$  with respect to  $v_{\wp_i}$  for  $\wp_i | \mathfrak{p}B$ . Let  $\widehat{B}_i$  denote the corresponding valuation rings.

**Proposition 5.8.** *With notation as above, we have that the following hold:*

- (1)  $[\widehat{L}_i : \widehat{K}] = e_{\wp_i} f_{\wp_i}$ ;
- (2)  $L \otimes_K \widehat{K} = L \otimes_K K_{\mathfrak{p}} = \prod_i \widehat{L}_i$  as  $K_{\mathfrak{p}}$ -algebras;
- (3)  $B \otimes_A \widehat{A} = \prod_i \widehat{B}_i$ .

In (2) in the above, note that the splitting of the prime  $\mathfrak{p}$  into primes in  $L$  exactly corresponds to the splitting of the algebra  $L \otimes_K \widehat{K}$  into fields.

**Proposition 5.9.** *If  $L/K$  is Galois and  $D_i$  is the decomposition group of  $\wp_i$ , then  $\widehat{L}_i/\widehat{K}_i$  is Galois with Galois group  $D_i$ .*

*Proof.* The action of  $D_i$  extends by continuity to  $\widehat{L}_i$ , giving  $e_{\wp_i} f_{\wp_i} = [\widehat{L}_i : \widehat{K}]$  automorphisms.  $\square$

6. WEDNESDAY SEPTEMBER 27

**6.1. Hensel's Lemma.** Let  $K$  be a complete field for a discrete valuation  $v$ . Let  $A$  be its valuation ring ( $A$  is a *complete DVR*) with uniformizer  $\pi$ . For example, consider  $K = \mathbb{Q}_p$  or  $K = \mathbb{F}_q((t))$ .

**Theorem 6.1** (Hensel's Lemma 1). *Let  $f \in A[x]$  and  $a_0 \in A$  such that  $\bar{a}_0$  is a simple root of  $\bar{f}(x) \pmod{\pi}$  (the bars here denote reductions of elements in  $A$  modulo  $\pi$ ). Then there is a unique root  $a \in A$  of  $f(x)$  with  $\bar{a} = \bar{a}_0 \pmod{\pi}$ .*

*Proof.* We will construct a Cauchy sequence  $(a_n) \in A$  such that

$$(1) \quad f(a_n) \equiv 0 \pmod{\pi^{n+1}} \quad \text{and} \quad a_n \equiv a_0 \pmod{\pi}$$

whose limit will be  $a$ . We will also show that  $a_n$  is unique modulo  $\pi^{n+1}$  given Equation (1).<sup>5</sup> Proceed inductively. We have  $a_0$ . Let  $a_{n+1} = a_n - f(a_n)/f'(a_n)$ , where here  $f'$  denotes the formal derivative. The product rule implies the following: if  $\bar{f}'(a_0) \not\equiv 0 \pmod{\pi}$ , then  $\bar{a}_0$  is a double root of  $\bar{f}$ . So  $v(f'(a_0)) = 0$ , forcing  $f'(a_0) \in A$ . It follows that  $a_{n+1} \in A$ . We have

$$(x + y)^n \in x^n + nx^{n-1}y + y^2\mathbb{Z}[x, y],$$

so  $f(x + y) = f(x) + yf'(x) + y^2A[x, y]$  and

$$f(a_{n+1}) = f(a_n - f(a_n)/f'(a_n)) = f(a_n) - \frac{f(a_n)}{f'(a_n)}f'(a_n) + \left(\frac{f(a_n)}{f'(a_n)}\right)^2 X.$$

The last term in the sum on the right-hand side has valuation greater than or equal to  $2n+2 \geq n+2$ . Hence,  $f(a_{n+1}) \equiv 0 \pmod{\pi^{n+2}}$ . To see uniqueness, consider the following. We have that  $a_n$  is unique mod  $\pi^{n+1}$  if  $0 = f(a_n + h\pi^{n+1}) = f(a_n) + h\pi^{n+1}f'(a_n) + Y$  where  $Y$  has valuation greater than or equal to  $n + 2$ . This determines  $h \pmod{\pi}$  and implies the uniqueness of  $a_{n+1} \pmod{\pi^{n+2}}$ . The uniqueness of the  $a_n$ 's implies that  $(a_n)$  is Cauchy. Let  $a = \lim a_n$ . We note that  $f(a) = 0$  and that  $a$  is unique, as it is determined mod  $\pi^n$  for all  $n$ .  $\square$

**Theorem 6.2** (Hensel's Lemma 2). *Let  $a_0 \in A$  with  $v(f(a_0)) > 2v(f'(a_0))$ . Then there is a root  $a$  of  $f(x)$ .*

**Theorem 6.3** (Hensel's Lemma 3). *If  $f(x)$  is monic and  $\bar{f} = g_0h_0 \pmod{\pi}$ , where  $g_0, h_0 \in A/\pi[x]$  and relatively prime, then  $f = gh$  in  $A[x]$  with  $g, h$  monic and  $\bar{g} = g_0$  and  $\bar{h} = h_0 \pmod{\pi}$ .*

There is also a version of Hensel's Lemma that implies the previous two versions, and even a version where  $f$  does not have to be monic (see Neukirch Chapter 2 Section 4).

**Example 6.4.** Consider  $x^{p-1} - 1 \in \mathbb{Z}_p[x]$ . This polynomial factors into distinct linear factors over the residue field  $\mathbb{Z}_p/p\mathbb{Z}_p \simeq \mathbb{Z}/p\mathbb{Z}$ . Applying Hensel's Lemma  $p - 2$  times implies that  $x^{p-1} - 1$  factors over  $\mathbb{Z}_p$  into distinct linear factors. Hence,  $\mathbb{Z}_p$  contains  $p - 1$  ( $p - 1$ )st roots of unity. Note that this gives a multiplicatively closed set of representatives for the residue classes modulo  $p$ . This is one way of witnessing that  $\mathbb{Z}_p$  is much bigger than  $\mathbb{Z}_{(p)}$ , which lives in  $\mathbb{Q}$ . Moreover, if  $|A/\pi| = q$ , then  $K$  has all  $(q - 1)$ st roots of unity.

<sup>5</sup>Recall Newton's method: given some function  $f(x)$ , suppose we would like to approximate one of its roots. Say we have some approximation  $x_n$  of the root. Consider  $f(x_n)$  and the line tangent to the function at this point. In particular, let  $x_{n+1}$  be the zero of the tangent line; intuitively we should have  $x_{n+1} = x_n - f(x_n)/f'(x_n)$ . Continue inductively. Whether this algorithm actually gives us a sequence converging to the root of  $f$  is finicky, and this doesn't always work in the archimedean case. However, things are nicer when our absolute value is nonarchimedean.

## 6.2. Local Fields.

**Definition 6.5.** A *local field* is a field that is complete for a discrete valuation with finite residue field.

Let's try to classify the local fields. We'll first consider the *mixed characteristic case*. Let  $K$  be a local field with valuation ring  $A$  and  $\pi$  its uniformizer. Suppose that  $\text{char}(K) = 0$  and that  $\text{char}(A/\pi) = p$ . So  $\mathbb{Z} \subset A$  and  $p \in A$  with  $v(p) \geq 1$ . Let  $e := v(p)$ —this is called the *absolute ramification index* of  $K$  (or  $A$ ). We may write  $p = \pi^e u$  for some  $u \in A^*$ . Note that  $\mathbb{Z}_p \subset A$  as  $\mathbb{Z}_p$  is Cauchy sequences of integers for the  $p$ -adic metric. Let  $f = [A/\pi : \mathbb{Z}/p\mathbb{Z}]$ . Moreover,  $A$  is a free  $\mathbb{Z}_p$ -module of rank  $ef$  (prove this as an exercise; use the power series characterization). Hence,  $K/\mathbb{Q}_p$  is a field extension of degree  $ef$ . This is an extension of Dedekind domains, where  $e_{\pi/p} = e$ . (There is a unique canonical map  $\mathbb{Q}_p \rightarrow K$ .) If  $e = 1$ , we say that  $A$  is *absolutely unramified*.

**Example 6.6.** If  $L/\mathbb{Q}$  is a finite extension that is unramified at  $p$  with  $\wp$  the prime of  $\mathcal{O}_L$  lying over  $p$ , then  $L_\wp$  (the completion of  $L$  at the  $\wp$ -adic valuation) is an absolutely unramified local field.

**Theorem 6.7.** For every finite field  $\mathbb{F}_q$  of characteristic  $p$ , there is a unique (up to isomorphism) complete local field of characteristic 0 that is absolutely unramified with residue field  $\mathbb{F}_q$ .

**Example 6.8.** Consider an extension  $L$  of  $\mathbb{Q}$  where  $p$  splits as  $\wp_1 \wp_2$  in  $\mathcal{O}_L$ . Here we have  $e_1 = f_1 = 1$  and  $e_2 = f_2 = 1$ , and  $L_{\wp_1} = \mathbb{Q}_p = L_{\wp_2}$ , since  $[L_{\wp_i} : \mathbb{Q}_p] = e_i f_i = 1$ .

*Proof of Theorem 6.7.* Let  $q = p^f$ , and let  $\bar{\theta}$  generate  $\mathbb{F}_q/(\mathbb{Z}/p\mathbb{Z})$  with minimal polynomial  $\bar{h} \in \mathbb{Z}/p\mathbb{Z}[x]$  of degree  $f$ . Uniqueness: Let  $A, A'$  denote discrete valuation rings of characteristic 0 that are absolutely unramified with  $A/\pi \simeq A'/\pi' \simeq \mathbb{F}_q$ . Letting  $K = \text{Frac}$  and  $K' = \text{Frac}(A')$ , we see that  $[K : \mathbb{Q}_p] = [K' : \mathbb{Q}_p] = f$ . Lift  $\bar{\theta}$  to  $\theta \in A$  with minimal polynomial  $g(x) \in \mathbb{Z}_p[x]$ . Then  $\bar{g}(\bar{\theta}) \equiv 0 \pmod{\pi}$ , so  $\bar{h}|\bar{g}$  implies that  $\deg(g) \geq \deg(\bar{h}) = f$ . Then  $[K : \mathbb{Q}_p] = f$  implies that  $f \geq \deg(g)$ . Thus,  $\deg(g) = f$  and  $\bar{h} = \bar{g}$ . Then  $K \simeq \mathbb{Q}_p[x]/g(x)$ .

Now, consider  $K'$ . We consider  $g(x) \in A'[x]$ , and  $g \pmod{\pi'}$  in  $\mathbb{F}_q[x]$  which splits into distinct linear factors (since it is a minimal polynomial over a finite field). Hensel's Lemma then implies that  $g$  factors into distinct linear factors over  $A'$ , and  $K'$  contains a root of  $g$  and  $[K' : \mathbb{Q}_p] = \deg(g)$ . Now,  $g$  is irreducible over  $\mathbb{Z}_p$ , which follows because  $\bar{g}$  is irreducible over  $\mathbb{Z}/p\mathbb{Z}$ . We conclude that  $K' \simeq \mathbb{Q}_p[x]/g(x)$ .

Existence is left as an exercise. □

## 7. MONDAY OCTOBER 2

We begin by stating a generalization of Theorem 6.7.

**Theorem 7.1.** Over a complete discrete valuation ring  $A$  with fraction field  $K$  and  $A/(\pi) \simeq \mathbb{F}_q$ , there is a unique unramified  $L/K$  with residue field  $\mathbb{F}_{q^f}$ . (Also,  $[L : K] = f_1$ .)

Last class, we gave a proof of the analogous theorem when  $K = \mathbb{Q}_p$  using Hensel's Lemma. Theorem 7.1 is proved analogously.

Recall that  $L$  and  $K$  each have exactly one prime ideal, since they are complete fields. So over a complete discrete valuation ring  $A$  with fraction field  $K$ , we have that

$$\{\text{unramified extensions}\} \longleftrightarrow \{\text{extensions of the residue field}\}.$$

This makes sense—because the extension is unramified, we have  $\text{Gal}(L/K) \rightarrow \text{Gal}(B/\pi_B/A/\pi_A)$  is an isomorphism, since  $\text{Gal}(L/K)$  is the decomposition group and the inertia group (the kernel of the aforementioned map) is trivial.

A complete discrete valuation ring in characteristic 0 is a finite extension of  $\mathbb{Q}_p$ . If  $e > 1$ , let  $T$  be the inertia group. We have the following commutative diagram, where  $K_T/\mathbb{Q}_p$  is an unramified extension of degree  $f$  and the extension  $K/K_T$  is some ramified extension.

$$\begin{array}{c} K \\ | \\ K_T \\ | \\ \mathbb{Q}_p \end{array}$$

By Krasner’s Lemma (left as a homework exercise), there are only finitely many extensions of  $K_T$  of a given degree.

### 7.1. Equal Characteristic Local fields.

**Theorem 7.2.** *If  $K$  is a local field of characteristic  $p > 0$ , then  $A \simeq A/\pi[[T]]$ , and  $K = A/\pi((T))$ .*

**Corollary 7.3.** *Any finite extension of  $\mathbb{F}_q((t))$  is isomorphic to  $\mathbb{F}_{q^r}((s))$  for some  $r$ .*

**Remark 7.4.** This is analogous to the fact that small analytic neighborhoods of a curve over  $\mathbb{C}$  are all isomorphic.

*Proof.* We’ll find a set  $S \subset A$  of representatives of  $A/\pi$  that is additively and multiplicatively closed. Then the theorem follows from our power series characterization. Let  $x \in A/\pi$ . Let  $\widetilde{x^{p^{-n}}}$  be a lift of  $x^{p^{-n}}$  to  $A$  (the map  $z \mapsto z^p$  in  $A/\pi$  is surjective, since  $|(A/\pi)^*|$  is relatively prime to  $p$ ). Note that any other lift  $\widetilde{x^{p^{-n}}} + \pi y$  has

$$\left(\widetilde{x^{p^{-n}}} + \pi y\right)^{p^n} = \widetilde{x^{p^{-n}p^n}} + (\pi y)^{p^n}.$$

Let  $\widehat{x} = \lim_{n \rightarrow \infty} \widetilde{x^{p^{-n}p^n}}$ . We can check that this limit exists and does not depend on the choices of lifts. Note that  $\widetilde{x^{p^{-n}}}\widetilde{y^{p^{-n}}}$  is a lift of  $(xy)^{p^{-n}}$ , implying that  $\widehat{xy} = \widehat{x}\widehat{y}$ . Moreover, since

$$\left(\widetilde{x^{p^{-n}}} + \widetilde{y^{p^{-n}}}\right)^{p^n} = \widetilde{x^{p^{-n}p^n}} + \widetilde{y^{p^{-n}p^n}} \equiv x + y \pmod{\pi},$$

so  $\widetilde{x^{p^{-n}}} + \widetilde{y^{p^{-n}}}$  lifts  $(x + y)^{p^{-n}}$ . Hence,  $\widehat{x + y} = \widehat{x} + \widehat{y}$ . □

Unlike  $\mathbb{Q}_p$ , where  $\mathbb{Q}_p$  maps into  $K$  canonically and uniquely, in the case with mixed characteristic, there are many morphisms in all degrees  $\mathbb{F}_q((t)) \rightarrow \mathbb{F}_{q^r}((s))$  (all have  $f = r$ ). For example, we could send  $t \mapsto s^k$  degree  $rk$  with  $e = k$ . We conclude that the local fields are  $\mathbb{F}_q(t)$  for some prime power  $q$  and the finite extensions of  $\mathbb{Q}_p$ .

**7.2. Multiplicative Groups of Local Fields.** Reading: Neukirch Chapter 2 Section 5. Let  $U^{(n)} = \{u \in A^* \mid u \equiv 1 \pmod{\pi^n}\} = 1 + \pi^n A$ . Note that the  $U^{(n)}$  are small neighborhoods of 1 and that the  $U^{(n)}$ ’s shrink as  $n$  grows.

**Proposition 7.5.** *The multiplicative group of a local field decomposes as*

$$K^* = \langle \pi \rangle \times \mu_{q-1} \times U^{(1)},$$

where  $\langle \pi \rangle$  denotes the group generated by the uniformizer  $\pi$  (i.e., powers of  $\pi$ ), where  $\mu_{q-1}$  denotes the  $q-1$  total  $(q-1)$ st roots of unity for  $q = |A/\pi|$ .

*Proof.* For  $\alpha \in K^*$ , then  $\alpha = \pi^n u$  uniquely for some  $n \in \mathbb{Z}$ ,  $u \in A^*$ . By Hensel's Lemma, there are  $q-1$  roots of unity  $\mu_{q-1} \in A^*$  and these are representatives of nonzero classes mod  $\pi$ . So we can uniquely write  $u = \zeta u'$  for some  $\zeta \in \mu_{q-1}$  and  $u' \in U^{(1)}$ .  $\square$

This filtration of our units gives us the following.

**Proposition 7.6.** *With notation as above, for  $n \geq 1$  we have that*

$$A^*/U^{(n)} \simeq (A/\pi^n)^* \quad \text{and} \quad U^{(n)}/U^{(n+1)} \simeq A/\pi$$

as groups.

*Proof.* The first claim is checked easily by verifying that the map sending  $u \in A^*/\pi^{(n)}$  to  $\bar{u} \in (A/\pi^n)^*$  is an isomorphism.

For the second claim, we have a map  $U^{(n)}/U^{(n+1)} \rightarrow A/\pi$  given by taking  $1 + \pi^n a \mapsto a$ . The most interesting thing to check is that  $(1 + \pi^n a)(1 + \pi^n b) = 1 + \pi^n(a + b) + \pi^{2n}ab \equiv 1 + \pi^n(a + b)$  in  $U^{(n+1)}$ . Verifying that this is an isomorphism is left to the reader.  $\square$

Note that the above implies that  $(U^{(n)})^p \subset U^{(n+1)}$ .

**7.3. Logarithms and Exponentials.** Let  $K$  be a local field of characteristic 0 with  $\text{char}(A/\pi) = p$ .

**Proposition 7.7.** *There is a unique continuous homomorphism  $\log : K^* \rightarrow K$  such that for  $1 + x \in U^{(1)}$ , we have  $\log(1 + x) = x - x^2/2 + x^3/3 - \dots$  and  $\log p = 0$ .*

*Proof.* We can check that this series converges for  $v(x) \geq 1$ . Since  $|x + y| \leq \max(|x|, |y|)$ , a series  $\sum_n a_n$  converges if and only if  $a_n \rightarrow 0$ . One can check that  $v(x^k) \geq k$  is enough to overcome the valuations of the denominators; therefore the series converges. The multiplicativity of  $\log((1 + x)(1 + y)) = \log(1 + y) + \log(1 + x)$  follows from the analogous fact for formal power series. Write  $p = \pi^e \cdot \zeta \cdot u_p$  for  $\zeta \in \mu_{q-1}$  and  $u_p \in U^{(1)}$ . Define  $\log(\pi) = -\log(u_p)/e$ .  $\square$

**Proposition 7.8.** *Let  $K$  as in the above and  $e$  the absolute ramification index. For  $n > e/(p-1)$ , then*

$$\exp(x) = 1 + x + \frac{x^2}{2!} + \dots$$

and  $\log$  give inverse continuous isomorphisms

$$\exp : \pi^n A \rightarrow U^{(n)} \quad \text{and} \quad \log : U^{(n)} \rightarrow \pi^n A.$$

Note that  $\pi^n A$  is additive whereas  $U^{(n)}$  is multiplicative.

*Proof.* We can calculate the values of each term, and  $n > e/(p-1)$  is what is necessary for convergence. Then  $\exp(\log) = \log(\exp) = \text{id}$  follows from the fact that this is true for formal power series.  $\square$

Next time, we will continue using  $\exp$  and  $\log$  to study  $U^{(n)}$ .



8. WEDNESDAY OCTOBER 4

**8.1. Multiplicative Groups of Local Fields continued.** Let  $K$  be a local field. Recall that  $K^* = \langle \pi \rangle \times \mu_{q-1} \times U^{(1)}$ . We would like to understand  $K^*$  better.

**Proposition 8.1.** *Let  $K$  have residue field  $\mathbb{F}_q$ , and let  $w_i \in A$  lift a basis of  $\mathbb{F}_q/\mathbb{F}_p$  as an  $\mathbb{F}_p$ -vector space. Then every element of  $U^{(1)}$  can be written uniquely as*

$$(2) \quad \prod_{k \geq 1} \prod_i (1 + w_i \pi^k)^{a_{k,i}}$$

with  $a_{k,i} \in \{0, \dots, p-1\}$ .<sup>6</sup>

*Proof.* We first prove that such expressions for the elements of  $U^{(1)}$  exist. To do so, we induct. Let  $x \in U^{(1)}$ . Suppose that for  $1 \leq k \leq n$  we have  $a_{k,i}$  such that

$$\prod_{k \geq 1} \prod_i (1 + w_i \pi^k)^{a_{k,i}} \equiv x \pmod{\pi^{n+1}}.$$

We'll find  $a_{n+1,i}$  such that (2) is congruent to  $x$  modulo  $\pi^{n+2}$ . Let

$$P = \prod_{k=1}^n \prod_i (1 + w_i \pi^k)^{a_{k,i}},$$

so

$$P \prod_i (1 + w_i \pi^{n+1})^{b_i} \equiv P + P \sum_i b_i \omega_i \pi^{n+1} \equiv P + \sum_i b_i \omega_i \pi^{n+1} \pmod{\pi^{n+2}}.$$

Let  $x = P + y\pi^{n+1}$  for  $y \in A$ , and choose  $a_{n+1,i} \in \{0, \dots, p-1\}$  such that  $\sum a_{n+1,i} w_i \equiv y$  modulo  $\pi$ .

As for uniqueness, suppose that

$$\prod_{k \geq 1} \prod_i (1 + u_i \pi^k)^{a_{k,i}} = \prod_{k \geq 1} \prod_i (1 + w_i \pi^k)^{a'_{k,i}}.$$

Without loss of generality, we have that  $a_{k,i} = 0$  for  $k < n$  and  $a_{n,i} \neq a'_{n,i}$  for some  $i$ . Modulo  $\pi^{n+1}$ , we have

$$\prod_i (1 + w_i \pi^n)^{a_{n,i}} = \prod_i (1 + w_i \pi^n)^{a'_{n,i}},$$

implying that  $\sum a_{n,i} w_i \equiv \sum a'_{n,i} w_i$  modulo  $\pi$ , which is a contradiction.  $\square$

Note that  $U^{(1)}$  is a  $\mathbb{Z}_p$ -module. In other words,  $(1 + x\pi)^z \in U^{(1)}$  makes sense for  $x \in A$  and  $z \in \mathbb{Z}_p$ . If  $\{z_i\}$  is a Cauchy sequence in  $\mathbb{Z}$  for  $z$ , we define  $(1 + x\pi)^z = \lim_{i \rightarrow \infty} (1 + x\pi)^{z_i}$ . It is not too difficult to check that this limit indeed exists (remember that  $(1 + x\pi)^{p^N}$  is close to 1).

**Remark 8.2.** Note that  $1/m \in \mathbb{Z}_p$  for  $p \nmid m$ ; this gives us additional  $m$ th roots of unity in  $\mathbb{Z}_p$ .

**Theorem 8.3.** *Let  $K$  be a local field with residue field  $\mathbb{F}_q$ , where  $q = p^f$ . Then the following hold:*

- (1) *if  $\text{char}(K) = 0$ , we have  $K^* \simeq \mathbb{Z} \times \mathbb{Z}/(q-1)\mathbb{Z} \times \mathbb{Z}/p^a\mathbb{Z} \times \mathbb{Z}_p^d$  (here,  $U^{(1)} \simeq \mathbb{Z}/p^a\mathbb{Z} \times \mathbb{Z}_p^d$ ) for some  $a \geq 0$  and  $d = [K : \mathbb{Q}_p]$ ;*

<sup>6</sup>Think of this as a ‘‘multiplicative power series,’’ where the  $a_{k,i}$  are the coefficients. Note that any such expression converges.

(2) if  $\text{char}(K) = p$ , then

$$K^* = \mathbb{Z} \times \mathbb{Z}/(q-1)\mathbb{Z} \times \mathbb{Z}_p^{\mathbb{N}}$$

(here  $U^{(1)} \simeq U^{(1)}$ ).

The isomorphisms in the above are isomorphisms of topological groups, where  $\mathbb{Z}$  is equipped with the discrete topology. Moreover, the isomorphisms relating certain components to  $U^{(1)}$  are  $\mathbb{Z}_p$ -modules isomorphism.

*Proof.* We begin by proving the case where the characteristic of  $K$  is 0. Recall that we have an isomorphism  $\log : U^{(n)} \rightarrow \pi^n A$  for some  $n$ . Hence,  $U^{(n)} \simeq \mathbb{Z}_p^d$ . Since  $[U^{(1)} : U^{(n)}] < \infty$  and since  $U^{(n)}$  is a finitely generated  $\mathbb{Z}_p$ -module, then  $U^{(1)}$  is a finitely generated  $\mathbb{Z}_p$ -module. So by the classification of finitely generated modules over a principle ideal domain, we have  $U^{(1)} \simeq \text{tors} \times \mathbb{Z}_p^d$ . We have that  $\text{tors} \simeq \mathbb{Z}_p/p^{k_1}\mathbb{Z}_p \times \cdots \times \mathbb{Z}_p/p^{k_r}\mathbb{Z}_p$ . Further, the torsion is cyclic because it is contained in  $U^{(1)}$  and hence consists of roots of unity. It follows that  $U^{(1)} \simeq \mu_{p^a} \times \mathbb{Z}_p^d$ .

Now, suppose that  $\text{char}(K) = p$ . We'll do the  $\mathbb{F}_q = \mathbb{F}_p$  case, since the general case is only slightly more complicated. Write  $x \in U^{(1)}$  uniquely as

$$x = \prod_{k \geq 1} (1 + \pi^k)^{a_k}$$

for  $a_k \in \{0, \dots, p-1\}$ . Note that  $(1 + \pi^\ell)^{mp^s} = (1 + \pi^{\ell p^s})^m$ . This allows us to move powers of  $p$  dividing  $k$  to the exponents:

$$x = \prod_{(\ell, p)=1} \prod_{s \geq 0} (1 + \pi^{\ell p^s})^{a_{\ell p^s}} = \prod_{(\ell, p)=1} \prod_{s \geq 0} (1 + \pi^\ell)^{a_{\ell p^s} p^s} = \prod_{(\ell, p)=1} (1 + \pi^\ell)^{\sum_s a_{\ell p^s} p^s}.$$

Note that the sum in the exponent is just an expression for some  $p$ -adic integer, since  $a_k$  was taken to be in  $\{0, \dots, p-1\}$ . Therefore  $U^{(1)}$  is a free  $\mathbb{Z}_p$  module with basis  $(1 + \pi^\ell)$  for  $(\ell, p) = 1$ .  $\square$

This theorem will be very useful later on, but we'll use it more immediately to answer the following question: what are the quadratic extensions of a local field  $K$  with characteristic other than 2?

**Proposition 8.4.** *Let  $K$  be any field, and suppose  $\text{char}(K) \neq 2$ . Then*

$$K^*/K^2 \setminus \{1\} \longleftrightarrow \{\text{quadratic extensions of } K\} / \simeq$$

(this is the first case of Kummer theory). The map from the left to the right is given by  $\alpha \mapsto K(\sqrt{\alpha})$ .

*Proof.* We get surjectivity by completing the square. As for injectivity, let  $\sigma$  be the automorphism generating the Galois group given by  $\sigma(\sqrt{\alpha}) = -\sqrt{\alpha}$ . If  $\alpha, \beta$  give the same extension, then  $\sigma(\alpha/\beta) = -\sqrt{\alpha}/-\sqrt{\beta} = \sqrt{\alpha}/\sqrt{\beta}$ . Hence,  $\sqrt{\alpha/\beta} \in K$ .  $\square$

For a local field  $K$  with characteristic other than 2, we have

$$K^*/K^2 \simeq \mathbb{Z}/2 \times \begin{cases} \mathbb{Z}/2\mathbb{Z} & \text{if } p \neq 2; \\ \mathbb{Z}/2\mathbb{Z} \times (\mathbb{Z}/2\mathbb{Z})^{[K:\mathbb{Q}_p]} & \text{if } p = 2. \end{cases}$$

Note that  $p = 2$  only in the characteristic 0 case. Thus, for example, if  $p \neq 2$ , then the quadratic extensions of  $K$  are  $K(\sqrt{\pi})$ ,  $K(\sqrt{u})$ , and  $K(\sqrt{u\pi})$  where  $u \in A^*$  is not a square (e.g., a primitive  $(q-1)$ st root of unity).

**8.2. The Different and the Discriminant.** The suggested readings for this section are Neukirch Chapter 3 Section 2 and Serre Chapter 3. Let  $A$  be a Dedekind domain with fraction field  $K$ , and let  $B$  be an extension of  $A$  in a separable field extension  $L/K$ . Suppose that the residue fields of  $A$  are finite, i.e., that  $|A/\wp| < \infty$  for  $\wp$  some nonzero prime ideal of  $A$ .

Recall that we have the following *trace form*:  $T : L \times L \rightarrow K$  taking  $(x, y) \mapsto \text{tr}_{L/K}(xy) = \text{tr}(M_{xy})$ , where  $M_{xy}$  is the multiplication matrix for  $xy$ . This is a nondegenerate, symmetric bilinear form.

*Proof of nondegeneracy.* Use the separability of  $L/K$  to write  $L = K(\theta)$  for some primitive element  $\theta$ , and consider the  $K$ -basis  $\theta, \theta^2, \dots, \theta^{n-1}$  for  $L$ . We'll use this basis to get a matrix for the trace form

$$M = (\text{tr}(\theta^{i-1}\theta^{j-1}))_{i,j} = (\sigma_k(\theta^{i-1}))_{i,k}^t (\sigma_k(\theta^{j-1}))_{j,k},$$

where the  $\sigma_k$  range over the Galois group of the normal closure of  $L/K$ . Then, we can easily compute the determinant of  $M$ , since we have written it as the product of Vandermonde matrices:

$$\det(M) = \prod_{a < b} (\sigma_a(\theta) - \sigma_b(\theta))^2,$$

and the above is nonzero by separability. □

For a fractional ideal  $I$  of  $L$ , we define the dual fractional ideal

$$I^* = \{x \in L \mid \text{tr}_{L/K}(xI) \in A\}.$$

As an exercise, check that  $I^*$  is a fractional ideal (the determinant of the trace form bounds the denominators). We claim that  $I$  and  $I^*$  are dual as  $B$ -modules: we have an isomorphism of  $B$ -modules  $I^* \simeq \text{Hom}_A(I, A)$  given by  $x \mapsto (y \mapsto \text{tr}(xy))$ .

**Definition 8.5.** The inverse *different* is  $B^*$ , and the *different* is  $(B^*)^{-1}$  (the inverse here is the inverse as a fractional ideal), which is often denoted  $\mathcal{D}_{L/K}$  (really it should be denoted  $\mathcal{D}_{B/A}$ , but we use the  $L/K$  notation when  $A$  and  $B$  are understood). Note that  $B \subset B^*$ , so  $(B^*)^{-1} \subset B$ , i.e.,  $\mathcal{D}_{L/K}$  is an integral ideal.

**Proposition 8.6.** *Differents have the following properties. Given  $K \subset L \subset M$ , we have*

- (1)  $\mathcal{D}_{M/K} = \mathcal{D}_{M/L}\mathcal{D}_{L/K}$ ;
- (2)  $\mathcal{D}_{S^{-1}A/S^{-1}B} = S^{-1}\mathcal{D}_{A/B}$  for  $S \subset A$ ;
- (3) for  $\wp \mid \mathfrak{p}$  with  $\wp$  a prime of  $B$  and  $\mathfrak{p} = \wp \cap A$ , then  $\mathcal{D}_{B/A}B_\wp = \mathcal{D}_{B_\wp/A_\wp}$ .

**Corollary 8.7.** *For  $L/K$  an extension of Dedekind domains, we have*

$$\mathcal{D}_{L/K} = \prod_{\wp \subset B} \mathcal{D}_{L_\wp/K_\wp},$$

where recall that  $L_\wp$  and  $K_\wp$  are completions of  $L$  and  $K$  at the primes  $\wp$  and  $\mathfrak{p}$ .

## 9. WEDNESDAY OCTOBER 11

**9.1. The Different.** Let  $A \subset K$  be a Dedekind domain and  $B$  an extended Dedekind domain in the separable field extension  $L/K$ . Suppose  $A$  has finite residue fields.

**Definition 9.1.** For  $\alpha \in B$  with minimal polynomial  $f(x) \in A[x]$ , the *different* of  $\alpha$  is

$$\delta_{L/K}(\alpha) = \begin{cases} f'(\alpha) & \text{if } L = K(\alpha) \\ 0 & \text{otherwise.} \end{cases}$$

**Proposition 9.2.** *If  $B = A[\alpha]$ , then  $\mathcal{D}_{L/K} = (\delta_{L/K}(\alpha))$ .*

*Proof.* Let  $f(x)$  be the minimal polynomial of  $\alpha$ ; let  $f(x)/(x-\alpha) = b_{n-1}x^{n-1} + \cdots + b_1x + b_0$ , where  $b_i \in L$ . We claim that the dual basis of  $1, \alpha, \dots, \alpha^{n-1}$  with respect to  $\text{Tr}_{L/K}(xy)$  is

$$\frac{b_0}{f'(\alpha)}, \dots, \frac{b_{n-1}}{f'(\alpha)}.$$

To see why the claim is true, let  $\alpha_1, \dots, \alpha_n$  be the conjugates of  $\alpha$  in the Galois closure. We have an equality of polynomials in  $X$  for each  $0 \leq r \leq n-1$

$$\sum_{i=1}^n \frac{f(x)}{(x-\alpha_i)} \frac{\alpha_i^r}{f'(\alpha_i)} = x^r,$$

since we have a polynomial of degree less than or equal to  $n-1$  with at least  $n$  roots for  $x \in \{\alpha_1, \dots, \alpha_n\}$  (use the product rule to see this). Hence,

$$\text{Tr}_{L/K} \left[ \frac{f(x)}{x-\alpha} \frac{\alpha^r}{f'(\alpha)} \right] = x^r,$$

where  $\text{Tr}_{L/K}$  above denotes taking the trace of the coefficients. Now, what is the coefficient of  $x^i$ ? We have

$$\text{Tr} \left( \frac{b_i \alpha^r}{f'(\alpha)} \right) = \delta_{ir},$$

where  $\delta_{ir}$  in the above is the Kronecker delta. This proves our claim.

It also follows that the inverse different

$$B^* = \frac{Ab_0 + \cdots + Ab_{n-1}}{f'(\alpha)}.$$

If  $f(x) = x^n + a_{n-1}x^{n-1} + \cdots + a_0$  for  $a_i \in A$ , applying long division implies that

$$b_{n-i} = \alpha^{i-1} + a_{n-1}\alpha^{i-2} + \cdots + a_{n-i+1},$$

so  $Ab_0 + \cdots + Ab_{n-1} = A[\alpha] = B$ . Therefore,  $B^* = (f'(\alpha))^{-1}$ , implying that  $\mathcal{D}_{L/K}(f'(\alpha))$ .  $\square$

**Remark 9.3.** Most of the time, in a global situation,  $B$  is not monogenic (i.e.,  $A[\alpha]$  for some  $\alpha$ ). This statement can in a sense be made precise using arithmetic statistics.

Let  $\mathfrak{p}$  be a nonzero prime of  $A$  and  $\wp$  a prime of  $B$  lying over  $\mathfrak{p}$ . Let  $\widehat{A}$  be the valuation ring of  $K_{\mathfrak{p}}$ , the completion of  $K$  at  $\mathfrak{p}$ . Similarly, let  $\widehat{B}$  be the valuation ring of  $L_{\wp}$ .

**Proposition 9.4.** *There exists  $\alpha \in L_{\wp}$  such that  $\widehat{B} = \widehat{A}[\alpha]$ .*

*Proof.* Let  $\bar{\alpha}$  be a primitive element of  $(B/\wp)/(A/\mathfrak{p})$ ; suppose  $\bar{f}$  is the minimal polynomial of  $\bar{\alpha}$ . Lift  $\bar{f}$  to a monic  $f \in \widehat{A}[x]$  (note that  $f$  is irreducible); likewise lift  $\bar{\alpha}$  to  $\alpha \in B$ . Note that  $v_L(f(\alpha)) > 0$ , since  $f(\alpha)$  is zero in the residue field. Moreover, we can choose lifts such that  $v_L(f(\alpha)) = 1$ . Note that

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

for  $b \in \widehat{B}$ . Because  $(B/\wp)/(A/\mathfrak{p})$  is separable, it follows that  $v_L(f'(\alpha)\pi_L) = 1$ . Hence, if  $v_L(f(\alpha)) \geq 2$ , then  $v_L(f(\alpha + \pi_L)) = 1$  and we can take  $\alpha + \pi_L$  as our lift of  $\bar{\alpha}$ .

We claim that  $\alpha^j f(\alpha)^i$  for  $0 \leq j \leq f_{\wp/\mathfrak{p}} - 1$  and  $0 \leq i \leq e_{\wp/\mathfrak{p}} - 1$  is an  $\widehat{A}$ -module basis of  $\widehat{B}$ . Note that this claim implies the proposition.

Let's prove the claim. Let  $M = \sum_{i=0}^{e-1} \sum_{j=0}^{f-1} A\alpha^j f(\alpha)^i$ , and let  $N = \sum_{j=0}^{f-1} A\alpha^j$ . By our choice of  $\alpha$ ,  $\widehat{B} = N + f(\alpha)\widehat{B}$ , since  $\bar{\alpha}$  generates the residue field. Recursively, this gives

$$\widehat{B} = N + f(\alpha)N + f(\alpha)^2N + \cdots + f(\alpha)^e\widehat{B} = M + p\widehat{B}$$

(as  $A$ -modules). Hence,  $\widehat{B} = M$  by Nakayama's Lemma.  $\square$

**Lemma 9.5** (Nakayama's Lemma). *Let  $R$  be a local ring with maximal ideal  $\mathfrak{m}$ . Let  $Q$  be a finitely generated  $R$ -module. If  $Q = M + \mathfrak{m}Q$ , then  $M = Q$ . Equivalently, if  $m_1, \dots, m_k$  generate  $Q/\mathfrak{m}Q$ , then they generate  $Q$ .*

**Remark 9.6.** If  $f_{\wp/p} = 1$ , then  $\widehat{B} = \widehat{A}[\pi_L]$  (take  $\bar{\alpha} = 0$  and  $f(x) = x$  in the previous lemma).

**Proposition 9.7.** *The different  $\mathcal{D}_{L/K}$  is the ideal generated by all  $\delta_{L/K}(\alpha)$  for  $\alpha \in B$ .*

*Proof.* If  $\beta \in L$  with  $\text{Tr}(\beta B) \subset A$ , then  $\text{Tr}(\beta A[\alpha]) \subset A$ , implying that  $\beta = \sum_i A \frac{b_i}{f'(\alpha)}$  (recall that the  $b_i$ 's are the coefficients of  $f(x)/(x - \alpha)$ ). Hence,  $B^* | (f'(\alpha)^{-1})$ , implying that  $f'(\alpha) \in \mathcal{D}_{L/K}$ .

For the other direction, we give a sketch of the proof. For each nonzero prime  $\wp$  of  $B$ , we check there is some  $\alpha \in B$  with  $\delta_{L/K}(\alpha)$  gives the right power of  $\wp$ , i.e.,  $v_{\wp}(\delta_{L/K}(\alpha)) = v_{\wp}(\mathcal{D}_{L/K})$ . Reduce to the complete local case that we had before with  $\widehat{A}$  (respectively  $\widehat{B}$ ) is the valuation ring of  $K_{\mathfrak{p}}$  (respectively  $L_{\wp}$ ), where  $\widehat{B} = \widehat{A}[\lambda]$ . Now,  $\lambda$  has some minimal polynomial over  $\widehat{A}$ . By Krasner's lemma, a sufficiently close polynomial over  $A$  will have a root  $\alpha$  such that  $\widehat{B} = \widehat{A}[\alpha]$  and  $v_{\wp}(\delta_{L_{\wp}/K_{\mathfrak{p}}}(\lambda)) = v_{\wp}(\delta_{L_{\wp}/K_{\mathfrak{p}}}(\alpha))$ .  $\square$

## 9.2. Ramification.

**Definition 9.8.** For a prime  $\wp$  of  $B$  with  $\mathfrak{p} = \wp \cap A$ , we say that  $\wp$  is *tamely ramified* if  $e_{\wp/p} > 1$  but  $\text{char}(B/\wp) \nmid e_{\wp/p}$ . Otherwise, we say that  $\wp$  is *wildly ramified*.

Let  $s = v_{\wp}(\mathcal{D}_{L/K})$  and  $e = e_{\wp/p}$ . Then  $s = e - 1$  if  $\wp$  tamely ramifies (or unramified). If  $\wp$  is wildly ramified, then  $e \leq s \leq e - 1 + v_{\wp}(e)$ .

**Theorem 9.9.** *A prime ideal  $\wp$  of  $B$  is ramified over  $A$  if and only if  $\wp | \mathcal{D}_{L/K}$ .*

*Proof sketch.* Reduce to the complete local case where  $A$  is a complete discrete valuation ring with maximal ideal  $\mathfrak{p} = \wp \cap A$ . We may do this because the powers of  $\wp$  are unchanged in the completion. So  $B = A[\alpha]$  for some  $\alpha \in B$ . If our extension is unramified, then  $\bar{\alpha}$  is a simple root, implying that  $f'(\alpha) \in B^*$  is a unit. Hence,  $s = 0 = e - 1$ .

Now, we reduce to the totally ramified case; we may do so because everything is multiplicative in towers. Thus, by the above,  $B = A[\pi_L]$ . We can compute  $v_{\wp}(\mathcal{D}_{L/K}) = s$  using a minimal polynomial  $f$  of  $\pi_L$ . Suppose  $f(x) = x^e + a_1x^{e-1} + \cdots + a_e$ . We see that  $f'(\pi_L) = e\pi_L^{e-1} + (e-1)a_1\pi_L^{e-2} + \cdots$  for  $a_i \in A$ , so  $e | v_{\wp}(a_i)$ . We can check that all the terms in the sum have different valuations because they all have different valuations modulo  $e$ . It follows that  $s = \min_i (v_{\wp}(e - i)a_i\pi_L^{e-i-1})$ .  $\square$

## 10. MONDAY OCTOBER 16

**10.1. The Discriminant.** Let  $A$  be a Dedekind domain with field of fractions  $K$ , and let  $B \subset L$  be an extended Dedekind domain. Suppose that  $L/K$  is separable and that  $A$  has finite residue fields.

**Definition 10.1.** Let  $\alpha_1, \dots, \alpha_n$  be a basis of  $L$  over  $K$ . We define the *discriminant* of  $\alpha_1, \dots, \alpha_n$  to be

$$\text{disc}(\alpha_1, \dots, \alpha_n) = \det(\text{Tr}_{L/K}(\alpha_i \alpha_j))_{i,j}$$

**Remark 10.2.** Changing  $\alpha_1, \dots, \alpha_n$  by  $M \in M_n(K)$  changes the discriminant by  $\det(M)^2$ .

If  $A = \mathbb{Z}$ , choose  $\alpha_1, \dots, \alpha_n$  to be a  $\mathbb{Z}$ -basis of  $B$ . Then  $\text{disc}(\alpha_1, \dots, \alpha_n)$  is well-defined in  $\mathbb{Z}$  (not depending on  $\alpha_1, \dots, \alpha_n$ ). We define  $\text{Disc}_{B/A}$  to be the *ideal* of  $A$  generated by  $\text{disc}(\alpha_1, \dots, \alpha_n)$  for all  $\alpha_1, \dots, \alpha_n \in B$ . We often write  $\text{Disc}_{L/K}$  when  $A$  and  $B$  are understood. If  $\alpha_1, \dots, \alpha_n$  is an  $A$ -module basis of  $B$ , then

$$\text{Disc}_{B/A} = (\text{disc}(\alpha_1, \dots, \alpha_n))$$

(since all other  $\alpha'_1, \dots, \alpha'_n$  are  $A$ -linear combinations,  $\text{disc}(\alpha'_1, \dots, \alpha'_n)$  is an  $A$ -multiple of  $\text{disc}(\alpha_1, \dots, \alpha_n)$ ).

**Lemma 10.3.** *With notation as above,*

$$\text{disc}(\alpha_1, \dots, \alpha_n) = \det(\sigma_i(\alpha_j))_{i,j}^2,$$

where the  $\sigma_i$  range over  $\sigma_i \in \text{Hom}_K(L, \overline{K})$ .

**Theorem 10.4.** *With notation as above, we have*

$$\text{Disc}_{L/K} = N_{L/K}(\mathcal{D}_{L/K}).$$

*Proof.* We reduce to the case where  $A$  is a discrete valuation ring. We show that the two ideals in question have the same factorization (recall we are working in a Dedekind domain). Then  $B$  is a free  $A$ -module; suppose  $\alpha_1, \dots, \alpha_n$  is a basis of  $B$  over  $A$ . We have

$$\text{Disc}_{L/K} = (\text{disc}(\alpha_1, \dots, \alpha_n)).$$

Moreover,  $B^*$  has  $\alpha'_1, \dots, \alpha'_n$  as an  $A$ -basis, where

$$\text{Tr}_{L/K}(\alpha_i \alpha'_j) = \delta_{ij}.$$

Since  $B$  has finitely many primes, it is a principal ideal domain. Let  $\beta \in L$  be such that  $B^* = (\beta)$ . Note that  $B^*$  has an  $A$ -basis  $\beta\alpha_1, \dots, \beta\alpha_n$ . Moreover,

$$\text{disc}(\beta\alpha_1, \dots, \beta\alpha_n) = \det(M_\beta)^2 \text{disc}(\alpha_1, \dots, \alpha_n) = N_{L/K}(\beta)^2 \text{disc}(\alpha_1, \dots, \alpha_n),$$

where  $M_\beta$  is the matrix corresponding to the linear transformation given by multiplication by  $\beta$ . We have

$$N_{L/K}(\beta) = N_{L/K}(B^*) = N_{L/K}(\mathcal{D}_{L/K})^{-1},$$

and

$$\text{disc}(\alpha'_1, \dots, \alpha'_n) = \det(\sigma_i \alpha'_j)_{i,j}^2.$$

We also have

$$(\sigma_i \alpha_j)_{ij}^t (\sigma_i \alpha'_j)_{ij} = \left( \sum_i \sigma_i \alpha'_j \alpha_k \right)_{jk} = \left( \text{Tr}_{L/K}(\alpha'_j \alpha_k) \right)_{jk} = I,$$

implying that

$$\text{disc}(\alpha_1, \dots, \alpha_n) = \text{disc}(\alpha_1, \dots, \alpha_n)^{-1}.$$

Further,

$$\text{Disc}_{L/K}^{-1} = \text{disc}(\alpha'_1, \dots, \alpha'_n) = \text{disc}(\beta\alpha_1, \dots, \beta\alpha_n) = N_{L/K}(\mathcal{D}_{L/K})^{-2} \text{Disc}_{L/K}.$$

It follows that the prime factorizations of  $\text{Disc}_{L/K}$  and  $N_{L/K}(\mathcal{D}_{L/K})$  are the same.  $\square$

**Corollary 10.5.** For a tower  $K \subset L \subset M$ , we have

$$\text{Disc}_{M/K} = \text{Disc}_{L/K}^{[M:L]} N_{L/K}(\text{Disc}_{M/L}).$$

*Proof.* This follows from the corresponding fact about differentials:

$$\mathcal{D}_{M/K} = \mathcal{D}_{M/L} \mathcal{D}_{L/K};$$

we are done. □

**Corollary 10.6.** A prime ideal  $\mathfrak{p}$  of  $A$  is unramified if and only if  $\mathfrak{p} \nmid \text{Disc}_{L/K}$ .

**10.2. Ramification Groups.** Reading for this section: Serre Chapter 4 and Neukirch Chapter 2 Section 10. Suppose  $A$  is a complete discrete valuation ring with  $K = \text{Frac}(A)$ . Let  $v_K$  denote the corresponding valuation with  $\pi_K$  its uniformizer. Again, consider the extension of Dedekind domains given by  $L/K$  with integral closure  $B$  in  $L$ . Suppose that  $L/K$  is separable that that  $A/\pi_K$  is finite. Let  $v_L$  and  $\pi_L$  be the valuation and uniformizer of the extension, respectively.

**Definition 10.7.** When  $L/K$  is Galois, we have  $B = A[x]$  ( $B$  is always monogenic over  $A$  for a complete discrete valuation ring). For  $\sigma \in \text{Gal}(L/K)$ , the following are equivalent:

- (1)  $\sigma$  is trivial on  $B/(\pi_L)^{i+1}$ ;
- (2)  $v_L(\sigma(b) - b) \geq i + 1$  for all  $b \in B$ ;
- (3)  $v_L(\sigma(x) - x) \geq i + 1$ .

For  $i \in \mathbb{Z}_{\geq -1}$ , the  $i$ th ramification group is defined to be

$$G_i = \{\sigma \in \text{Gal}(L/K) \mid \sigma \text{ is trivial on } B/(\pi_L)^{i+1}\}.$$

This gives us the following filtration  $\text{Gal}(L/K)$ :

$$\{1\} = G_m \trianglelefteq \cdots \trianglelefteq G_2 \trianglelefteq G_1 \trianglelefteq G_0 \trianglelefteq G_{-1} = \text{Gal}(L/K).$$

We note that  $G_0$  is the inertia subgroup and that each  $G_i$  is a normal subgroup. Moreover if  $\sigma \neq 1$ , we have  $\sigma(x) = y$ . If we let  $G = \text{Gal}(L/K)$  and consider the function  $i_G : G \rightarrow \mathbb{Z}$  given by

$$i_G(\sigma) := v_L(\sigma(x) - x),$$

we see that  $i_G$  is equivalent to the data of the filtration.

If  $H \leq G$  is a subgroup of  $G$ , where  $H = \text{Gal}(L/K^H)$ , then  $i_H(\sigma) = i_G(\sigma)$  implies that  $H_i = G_i \cap H$  (here,  $H_i$  denotes the ramification groups of  $\text{Gal}(L/K^H)$ ).

**Proposition 10.8.** If  $H$  is normal, then  $G/H = \text{Gal}(K^H/K)$ . Moreover, for  $\sigma \in G/H$ , we have

$$i_{G/H}(\sigma) = \frac{1}{e_{L/K^H}} \sum_{g \in \sigma H} i_G(g).$$

*Proof.* The proof is given in Serre; we refer the reader there. □

**Corollary 10.9.** If  $H = G_j$  for some  $j \geq 0$ , then we have

$$(G/H)_i = G_i/H$$

for  $i \leq j$ , where  $(G/H)_i$  denotes the  $i$ th ramification group of  $\text{Gal}(K^H/K)$ . We also have  $(G/H)_i = \{1\}$  for  $i \geq j$ .

*Proof.* If  $\sigma \in G/H \setminus \{1\}$ , there is a unique  $i < j$  such that  $\sigma \in G_i/H$  and  $\sigma \notin G_{i+1}/H$ . If  $g \in \sigma H$  with  $g \in G_i$  and  $g \notin G_{i+1}$ , then  $i_G(g) = i + 1$ . Also,  $H \leq G_0$ , implying that  $L/K^H$  is totally ramified. Hence,  $e_{L/K^H} = |H|$ , and  $i_{G/H}(\sigma) = i + 1$ , implying that the filtrations agree. □

**Remark 10.10.** If  $H \neq G_j$ , one can still use the formula, but the numbers are more complicated.

**Proposition 10.11.** *We have*

$$v_L(\mathcal{D}_{L/K}) = \sum_{\sigma \neq 1} i_G(\sigma) = \sum_{i=0}^{\infty} |G_i| - 1.$$

*Proof.* Write  $B = A[\alpha]$  with  $f$  the minimal polynomial of  $\alpha$ . We have

$$f(\alpha) = \prod_{g \in G} (x - g(\alpha)) \quad \text{and} \quad f'(\alpha) = \prod_{g \in G \setminus \{1\}} (\alpha - g(\alpha)).$$

Hence,

$$v_L(\mathcal{D}_{L/K}) = v_L(f'(\alpha)) = \sum_{g \neq 1} i_G(s),$$

as desired.  $\square$

**Corollary 10.12.** *If  $K^H$  is a general separable extension, we have*

$$v_{K^H}(\mathcal{D}_{K^H/K}) = \frac{1}{e_{L/K^H}} \sum_{s \notin H} i_G(s).$$

*Proof.* Use

$$\mathcal{D}_{L/K} = \mathcal{D}_{L/K^H} \mathcal{D}_{K^H/K}$$

to prove the corollary.  $\square$

## 11. WEDNESDAY OCTOBER 18

**11.1. More on Ramification Groups.** Recall the setting:  $A$  is a complete discrete valuation ring with field of fractions  $K$ . Let  $v_K$  be the valuation on  $K$  and  $\pi_K$  the uniformizer so that  $v_K(\pi_K) = 1$ . Suppose that  $A/(\pi_K)$  is finite. Let  $L/K$  be a Galois extension, and let  $B$  be the integral closure of  $A$  in  $L$ . Let  $v_L$  be its valuation with uniformizer  $\pi_L$ .

Let  $G_i \subset \text{Gal}(L/K)$  be the subgroup of elements of  $\text{Gal}(L/K)$  acting trivially on  $B/\pi_L^{i+1}$ . In other words,  $G_i = \{g \in \text{Gal}(L/K) \mid g(x) = x \pmod{\pi_L^{i+1}} \text{ for all } x \in B\}$ . If  $g \in \text{Gal}(L/K)$ , we let  $i_G(g) = 1 + \max\{i \mid g \in G_i\}$ . This gives us a filtration

$$\text{Gal}(L/K) = G_{-1} \supset G_0 \supset G_1 \supset \cdots.$$

**Proposition 11.1.** *Let  $i \geq 0$  and let  $g \in G_0$ . Then  $g \in G_i$  if and only if  $g(\pi_L)/\pi_L \equiv 1 \pmod{\pi_L^i}$ .*

*Proof.* If we replace  $K$  by  $L^{G_0}$  (the maximally unramified extension of  $K$ ), we can assume  $K \subset L$  is totally ramified. This allows us to assume  $B = A[\pi_L]$ . Thus,  $i_G(g) = v_L(g(\pi_L) - \pi_L) = 1 + v_L(g(\pi_L)/\pi_L - 1)$ .  $\square$

The proposition above is useful for the following reason. Consider the map  $G_i \rightarrow U_L^{(i)} = 1 + \pi_L^i B$  taking  $g \mapsto g(\pi_L)/\pi_L$ . We can further quotient, giving a map  $G_i \rightarrow U_L^{(i)}/U_L^{(i+1)}$ . The kernel of this map is  $G_{i+1}$ , and hence we have an injective group homomorphism  $\Theta_i : G_i/G_{i+1} \rightarrow U_L^{(i)}/U_L^{(i+1)}$ . Recall that for  $i \geq 1$ , we have  $U_L^{(i)}/U_L^{(i+1)} \simeq B/\pi_L$  where the isomorphism is given by  $1 + \pi_L^i a \mapsto a$ . Also note that  $\Theta_i$  does not depend on  $\pi_L$ . For  $u \in B^*$ , we have

$$\frac{g(u\pi_L)}{u\pi_L} = \frac{g(u)}{u} \cdot \frac{g(\pi_L)}{\pi_L} \equiv \frac{g(\pi_L)}{\pi_L} \pmod{\pi_L^{i+1}}$$



where the last congruence follows because  $g \in G_i$  implies  $g(u)/u \equiv 1 \pmod{\pi_L^{i+1}}$ . Hence, we have that  $G_0/G_1$  injects into  $(B/\pi_L)^*$ ; recall that  $B/\pi_L$  is a finite field of characteristic  $p > 0$ .

**Corollary 11.2.** *We have that  $G_0/G_1$  is cyclic of order coprime to  $p$ .*

**Corollary 11.3.** *For  $i \geq 1$ , we have that  $G_i/G_{i+1}$  is abelian of exponent  $p$ , since  $G_i/G_{i+1}$  injects into  $B/\pi_L$ .*

**Corollary 11.4.** *We have that  $G_0 = G_1 \rtimes C_m$ , where  $G_1$  is a  $p$ -group and  $C_m$  is a cyclic group of order coprime to  $p$ .*

*Proof.* We have the following exact sequence

$$1 \longrightarrow G_1 \longrightarrow G_0 \longrightarrow G_0/G_1 \longrightarrow 1,$$

where we recall that  $G_0/G_1$  is cyclic of order coprime to  $p$ . Hence  $G_1$  is the Sylow  $p$ -subgroup of  $G_0$ . Hall's theorem tells us that a normal subgroup whose order is coprime to the index has a complement, or, in simpler terms, the above exact sequence splits, telling us that  $G_0 = G_1 \rtimes G_0/G_1$ .  $\square$

**Corollary 11.5.** *We have that  $G_{-1} = \text{Gal}(L/K)$  is solvable. We have the following exact sequence:*

$$1 \longrightarrow G_0 \longrightarrow G_{-1} \longrightarrow G_{-1}/G_0 \longrightarrow 1$$

*Recall that  $G_0$  is solvable and that  $\text{Gal}(B/\pi_L/A/\pi_K) = G_{-1}$  is abelian. The result follows.*

**Corollary 11.6.** *We have that  $L/K$  is wildly ramified if and only if  $G_1 \neq \{1\}$ .*

*Proof.* Recall that an extension  $L/K$  is wildly ramified if and only if  $e(L/K)$  is divisible by  $p$ . If  $p|e = \#G_0 = \#G_1 \cdot \#(G_0/G_1)$ , then  $p|\#G_1$ , since  $\#(G_0/G_1)$  is coprime to  $p$ . Conversely, if  $\#G_1 > 1$ , then  $p|\#G_1$ , and  $\#G_1|\#G_0 = e$ , so  $p|e$ .  $\square$

**Example 11.7.** Consider the cyclotomic extensions of  $\mathbb{Q}_p$ . Let  $n \geq 1$  and let  $\zeta_n$  be a primitive  $n$ th root of unity. Write  $n = p^k m$  for  $(p, m) = 1$ . Consider the following tower of extensions

$$\begin{array}{c} K = \mathbb{Q}_p(\zeta_n) \\ | \\ \widehat{K} = \mathbb{Q}_p(\zeta_m) \\ | \\ \mathbb{Q}_p \end{array}$$

where  $\zeta_m = \zeta_n^{p^k}$ .

**Proposition 11.8.** *Assume  $(n, p) = 1$ . Let  $K$  be as above,  $k = A/\pi_K$ , and  $p$  the characteristic of  $k$ . Let  $q = |k|$ . Let  $K_n$  be the splitting field of  $x^n - 1$  over  $K$ , i.e., let  $K = K(\zeta_n)$ . Likewise, let  $k_n$  be the splitting field of  $x^n - 1$  over  $k$ . Then*

- (1)  $K_n/K$  is unramified;
- (2) the residue field of  $K_n$  is  $k_n$ ;
- (3)  $A_{K_n} = A_K[\zeta_n]$ ;
- (4)  $\text{Gal}(K_n/K) \simeq \text{Gal}(k_n/k)$ ;
- (5)  $\text{Gal}(K_n/K)$  is generated by the Frobenius element  $\zeta_n \mapsto \zeta_n^q$ .

*Proof.* Let  $L$  be the unramified extension of  $K$  whose residue field is  $k_n$ . Let  $S \subset L$  the multiplicatively closed set of representatives of the residue field  $k_n$  in  $L$ . Let  $\overline{\alpha}_n$  be a primitive  $n$ th root of unity in  $k_n$ . Let  $\alpha_n$  denote the corresponding element of  $S$ , and note that  $\alpha_n$  is a “primitive”  $n$ th root of unity. By Nakayama’s Lemma,  $B = A[\alpha_n]$ ; therefore  $L = K_n$ .  $\square$

**Corollary 11.9.** *It follows that  $[K_n : K]$  is the order of  $q$  modulo  $n$ .*

**Corollary 11.10.** *The maximal unramified extension of  $K$ , denoted  $K^{unr}$ , is given by  $K(\zeta_n, (n, p) = 1)$ . Moreover,  $\text{Gal}(K^{unr}/K)$  is generated by the Frobenius element  $\sigma(\zeta) = \zeta^q$ .*

**Proposition 11.11.** *Assume that  $K = \mathbb{Q}_p$ ,  $K_n = \mathbb{Q}_p(\zeta_n)$ , and  $n = p^m$  for  $m \geq 1$ . Then*

- (1)  $[K_n : K] = \varphi(n) = (p-1)p^{m-1}$ ;
- (2)  $\text{Gal}(K_n/K) \simeq (\mathbb{Z}/n\mathbb{Z})^*$ ;
- (3)  $K_n/K$  is totally ramified and  $\pi = \zeta_n - 1$  is a uniformizer. (If  $B$  is the integral closure of  $\mathbb{Z}_p$  in  $K$ , then  $B = \mathbb{Z}_p[\zeta_n]$ .)

*Proof.* Any  $\sigma \in \text{Gal}(K_n/K)$  has the form  $\sigma(\zeta_n) = \zeta_n^a$  for  $a \in (\mathbb{Z}/n\mathbb{Z})^*$ . So  $\text{Gal}(K_n/K)$  injects into  $(\mathbb{Z}/n\mathbb{Z})^*$ . Hence (1) and (2) are equivalent. Let  $\mu = \zeta_n^{p^{m-1}}$ . Note that  $\mu$  is a primitive  $p$ th root of unity. Hence,  $\mu^{p-1} + \dots + 1 = 0$ . Let

$$F(x) = x^{(p-1)p^{m-1}} + \dots + 1,$$

and note that  $F(\zeta_n) = 0$ . It follows that  $\pi$  is a root of  $F(1+x) = G(x)$ . Since  $G(0) = p$  and  $G(x) \equiv x^{(p-1)p^{m-1}} \pmod{p}$ , Eisenstein’s criterion implies that  $G$  is irreducible. Because  $\#(\mathbb{Z}/n\mathbb{Z})^* = (p-1)p^{m-1}$ , we have shown (1) and (2).

Now, note that

$$p = F(1) = \prod_{a \in (\mathbb{Z}/p^m\mathbb{Z})^*} (1 - \zeta_n^a) = \prod_{\sigma \in \text{Gal}(K_n/K)} \sigma(1 - \zeta_n).$$

Hence,

$$v_{K_n}(1 - \zeta_n) = \frac{v_{K_n}(p)}{[K_n : K]},$$

but since the above is an integer, it follows that  $v_{K_n}(1 - \zeta) = 1$ ; thus  $1 - \zeta$  is a uniformizer.  $\square$

Now, we would like to compute the ramification groups of  $K_n/\mathbb{Q}_p$  for  $n = p^m$ . We have that  $\text{Gal}(K_n/\mathbb{Q}_p) \simeq (\mathbb{Z}/n\mathbb{Z})^*$  by the above proposition. For  $0 \leq v \leq m$ , let  $G(n)^v$  be the subgroup of  $(\mathbb{Z}/n\mathbb{Z})^*$  of  $a$  such that  $a \equiv 1 \pmod{p^v}$ .

**Proposition 11.12.** *With notation as above, we have  $G_0 = \text{Gal}(K_n/\mathbb{Q}_p)$ ,*

$$G_1 = G_2 = \dots = G_{p-1} = G(n)^1 = \{a \mid a \equiv 1 \pmod{p}\},$$

$$G_p = \dots = G_{p^2-1} = G(n)^2,$$

*etc., until we have  $G_{p^{m-1}} = G(n)^m = \{1\}$ .*

*Proof.* Let  $a \in (\mathbb{Z}/n\mathbb{Z})^*$ . Let  $\sigma_a \in \text{Gal}(K_n/\mathbb{Q}_p)$  be the corresponding element  $\sigma_a(\zeta) = \zeta^a$ . Let  $v$  be the largest integer such that  $a \equiv 1 \pmod{p^v}$  (i.e.,  $a \in G(n)^v$ ) but  $a \notin G(n)^{v+1}$ . We have

$$i_G(\sigma_a) = v_{K_n}(\sigma_a(\zeta) - \zeta) = v_{K_n}(\zeta^a - \zeta) = v_{K_n}(\zeta^{a-1} - 1).$$

Since  $\zeta^{a-1}$  is a primitive  $p^{m-v}$ th root of unity, we have that  $\zeta^{a-1}$  is a uniformizer for  $K_{p^{m-v}}$ . Then  $i_G(\sigma_a) = [K_n : K_{p^{m-v}}] = \#G(n)^{m-v} = p^v$ . So if  $p^{k-1} \leq u \leq p^k - 1$ , then  $\sigma_a \in G_u$  if and only if  $v \geq k$ .  $\square$

12. MONDAY OCTOBER 23

Algebraic number theory is motivated by studying  $\text{Gal}(\overline{\mathbb{Q}}, \mathbb{Q})$  and its finite index subgroups  $\text{Gal}(\overline{\mathbb{Q}}, K) = \text{Gal}(\overline{K}, K)$  for number fields  $K$ . Class field theory is motivated by understanding  $\text{Gal}(\overline{K}, K)^{ab}$  for both global and local fields, but it turns out that understanding class field theory in the global case is intimately connected to the local one.

**12.1. Infinite Galois Theory.** Galois theory does not extend word for word to infinite-degree extensions of fields.

**Proposition 12.1.** *Let  $L$  be an algebraic extension of a field  $K$  (i.e., each  $\alpha \in L$  is algebraic over  $K$ ). Then the following are equivalent:*

- (1)  $L = \bigcup_i L_i$  for  $L_i/K$  finite Galois subextensions
- (2)  $L^{\text{Aut}(L/K)} = K$
- (3)  $L/K$  is separable and normal (i.e., every irreducible polynomial in  $K[x]$  with a root in  $L$  splits into linear factors in  $L[x]$ ).

We call these  $L/K$  Galois and let  $\text{Gal}(L/K) = \text{Aut}(L/K)$ .

**Example 12.2.** Consider  $K = \mathbb{Q}(\sqrt{-1}, \sqrt{2}, \sqrt{3}, \sqrt{5}, \dots)/\mathbb{Q}$ . We see that  $\text{Gal}(K/\mathbb{Q}) \simeq \{\pm 1\}^{\mathbb{N}}$ , where each component corresponds to switching the sign of the corresponding square root. The Galois group has uncountably many index 2 subgroups (i.e., kernels of surjective homomorphisms  $\{\pm 1\}^{\mathbb{N}} \rightarrow \{\pm 1\}$ ), but countably many degree 2  $L/K$  subextensions.

**Definition 12.3.** For a field  $K$ , we let  $\overline{K}$  denote the *separable closure* of  $K$ . We see that  $\overline{K}$  is a field where every separable polynomial over  $K$  has a root and where every  $\alpha \in \overline{K}$  has a separable minimal polynomial over  $K$  (i.e., adjoin the roots of every separable minimal polynomial). Moreover,  $\overline{K}$  is the unique (up to isomorphism separable extension of  $K$  containing all separable extensions of  $K$ ).

**Proposition 12.4.** *For a field  $K$ , the separable closure  $\overline{K}$  exists.*

*Proof.* The proof uses Zorn's lemma; it is exactly the same as the proof of the existence of the algebraic closure of a field. □

Note that  $\overline{K}/K$  is Galois, and we call  $G_K = \text{Gal}(\overline{K}/K)$  the *absolute Galois group* of  $K$ .

**Proposition 12.5.** *Let  $M/K$  be a Galois extensions with intermediate Galois extension  $L/K$ , then  $\text{Gal}(M/K) \rightarrow \text{Gal}(L/K)$  is surjective.*

*Proof.* The argument also requires Zorn's Lemma. □

Infinite Galois groups  $G = \text{Gal}(M/K)$  are *topological groups* with a basis of neighborhoods given by cosets  $\sigma\text{Gal}(M/L)$  for  $L/K$  a finite Galois extension. The multiplication and inverse maps are continuous. For example, we may check that multiplication  $G \times G \rightarrow G$  is continuous: Consider  $(\sigma, \tau) \in G \times G$ . A basis open in  $G$  around its image is  $\sigma\tau\text{Gal}(M/L)$ , which has preimage containing  $\sigma\text{Gal}(M/L) \times \tau\text{Gal}(M/L)$  (note here that we are using the fact that  $\text{Gal}(M/L)$  is continuous).

**Remark 12.6.** Our basic opens  $\sigma\text{Gal}(M/L)$  are closed, since  $\sigma\text{Gal}(M/L)^c$  is the open set given by the union of the other cosets.

**Lemma 12.7.** *Any open subgroup is closed.*

*Proof.* All of the nontrivial cosets of the subgroup are open by the continuity of multiplication. Hence, the complement of an open subgroup is open.  $\square$

**Proposition 12.8.** *We have  $\text{Gal}(M/K)$  is compact and Hausdorff.*

*Proof.* First show that the image of  $\text{Gal}(M/K)$  is closed in

$$\prod_{\substack{L/K \\ \text{finite Galois}}} \text{Gal}(L/K),$$

where  $\text{Gal}(L/K)$  is equipped with the discrete topology; use Tychonoff's theorem.  $\square$

**Theorem 12.9** (Galois Theory for infinite extensions). *For  $M/K$  Galois, the map  $L \mapsto \text{Gal}(M/L)$  is a bijective correspondence between subextensions  $M/L/K$  and closed subgroups of  $\text{Gal}(M/L)$ . The open subgroups correspond exactly to finite  $L/K$ .*

*Proof.* If  $L/K$  is finite (not necessarily Galois), with Galois closure  $N/K$ , then  $\text{Gal}(M/L)$  is open, and so  $\text{Gal}(M/L)$  is open as any  $\sigma \in \text{Gal}(M/L)$  has  $\sigma \in \sigma\text{Gal}(M/N) \subset \text{Gal}(M/L)$ . If  $L/K$  is an arbitrary subextension, then

$$\text{Gal}(M/L) = \bigcap_{\substack{L_i \text{ finite} \\ \text{subextension of } L/K}} \text{Gal}(M/L_i),$$

implying that  $\text{Gal}(M/L)$  is closed.

To see that the map is injective, we first show that  $L$  is the field fixed by  $\text{Gal}(M/L)$ . Suppose  $\alpha \notin L$  is fixed by  $\text{Gal}(M/L)$ . Then recall that  $\text{Gal}(M/L)$  surjects onto  $\text{Gal}(\overline{L(\alpha)}/L)$ , where  $\overline{L(\alpha)}$  is the Galois closure of  $L(\alpha)$ , and moreover, there exists  $\sigma \in \text{Gal}(\overline{L(\alpha)}/L)$  such that  $\sigma(\alpha) \neq \alpha$  by finite Galois theory. This is a contradiction; this proves our claim and the injectivity of the map.

To see that the map is surjective, consider a closed subgroup  $H$  and let  $L = M^H$ . Clearly,  $H \subset \text{Gal}(M/L)$ . Moreover, let  $\sigma \in \text{Gal}(M/L)$ . If  $N/L$  is a finite Galois subextension, then  $\sigma \in \text{Gal}(M/N)$  is a basic open around  $\sigma$ . We have  $H \rightarrow \text{Gal}(N/L)$  is surjective, since the image of  $\overline{H}$  has fixed field  $L$ . Hence, there exists  $\tau \in H$  such that  $\tau \in H \cap \sigma\text{Gal}(M/N)$ . So every basic open around  $\sigma$  intersects  $H$ , implying that  $\sigma$  is in the closure of  $H$ . Thus,  $\sigma \in H$ , which proves surjectivity.

If  $H$  is an open subgroup, then  $\text{Gal}(M/L) \subset H$  for some finite Galois extension  $L/K$ . Set  $E = M^H$ , and let  $H = \text{Gal}(M/E)$ . Then  $E \subset L$ , so  $E/K$  is finite by Galois theory.  $\square$

**Example 12.10.** Consider  $M = \mathbb{Q}(\sqrt{-1}, \sqrt{2}, \sqrt{3}, \sqrt{5}, \dots)/\mathbb{Q}$ . The open subgroups of  $\text{Gal}(M/\mathbb{Q})$  correspond to finite extensions which correspond to subgroups of  $\{\pm 1\}^{\mathbb{N}}$  of the form  $S \times \{\pm 1\}^{\mathbb{N}-n}$  where  $S \subset \{\pm 1\}^n$ . Note that there are countably many of these!

**12.2. Projective Limits.** The material in this subsection corresponds to Neukirch Chapter 4 Section 2.

**Definition 12.11.** Suppose we are working in some category  $\mathcal{C}$ . A *directed system*  $I$  is a partially ordered set such that for all  $i, j \in I$  there exists  $k \in I$  with  $i, j \leq k$ . A *projective system* over  $I$  is a family of objects in  $\mathcal{C}$   $X_i$  for  $i \in I$  and morphisms  $f_{ij} : X_j \rightarrow X_i$  for all  $i \leq j$  such that  $f_{ii} = \text{id}$  and  $f_{ik} = f_{ij} \circ f_{jk}$  when  $i \leq j \leq k$ .

The *projective limit* is

$$X = \varprojlim_{i \in I} X_i = \left\{ (x_i)_{i \in I} \in \prod_{i \in I} X_i \mid f_{ij}(x_j) = x_i \text{ for } i \leq j \right\}.$$

**Example 12.12.** A complete discrete valuation ring  $A$  can be realized as the projective limit of

$$\cdots \longrightarrow A/\pi^3 A \longrightarrow A/\pi^2 A \longrightarrow A/\pi A$$

**Example 12.13.** We have  $\widehat{\mathbb{Z}} = \lim_{n \in \mathbb{N}} \mathbb{Z}/n\mathbb{Z}$  as topological rings. Here we say  $m \leq n$  when  $m|n$  and the map  $\mathbb{Z}/n\mathbb{Z} \rightarrow \mathbb{Z}/m\mathbb{Z}$  is given by reduction modulo  $m$ . The Chinese Remainder Theorem implies that  $\widehat{\mathbb{Z}} = \prod_p \mathbb{Z}_p$ .

**Remark 12.14.** We have that  $\lim X_i$  is an object in  $\mathcal{C}$  since the  $X_i$  are. If we are working in a category of topological objects, then  $\lim X_i$  is equipped with subspace topology of the product topology on  $\prod X_i$ .

### 13. WEDNESDAY OCTOBER 25

#### 13.1. More on Projective Limits.

**Proposition 13.1.** A projective limit of nonempty compact spaces is nonempty and compact.

**Proposition 13.2.** Suppose  $\{G_i\}_i$  is a projective system with maps  $g_{ij} : G_i \rightarrow G_j$  for  $i \leq j$ . If  $H$  is a topological group and  $h_i : H \rightarrow G_i$  is a family of continuous homomorphisms such that  $h_i = g_{ij} \circ h_j$  for  $i \leq j$ , then there exists a unique continuous homomorphism  $h : H \rightarrow \lim_{\leftarrow} G_i$  such that  $h$  gives  $h_i$  when composed with the projection to  $G_i$  for all  $i$ .

**Proposition 13.3.** If  $M/K$  is Galois, then as topological groups, we have

$$\text{Gal}(M/K) = \varprojlim_{\substack{L/K \text{ finite Galois} \\ \text{subextensions}}} \text{Gal}(L/K).$$

Here the ordering is containment and the maps are restrictions.

**Example 13.4.** Recalling that  $\text{Gal}(\mathbb{F}_{q^n}/\mathbb{F}_q) = \mathbb{Z}/n\mathbb{Z}$  and  $\text{Gal}(\overline{\mathbb{F}_q}/\mathbb{F}_q) \simeq \widehat{\mathbb{Z}} = \lim_n \mathbb{Z}/n\mathbb{Z}$ .

**Example 13.5.** Recall that  $\text{Gal}(\mathbb{Q}(\mu_n)/\mathbb{Q}) \simeq (\mathbb{Z}/n\mathbb{Z})^*$ . We have that  $\text{Gal}(\mathbb{Q}(\mu_n)_n/\mathbb{Q}) \simeq \widehat{\mathbb{Z}}^* = \lim_n (\mathbb{Z}/n\mathbb{Z})^*$ .

**Example 13.6.** If  $G$  is any group and  $N$  varies over normal subgroup of finite index, then

$$\widehat{G} := \varprojlim_N G/N$$

is called the *profinite completion* of  $G$ .

#### 13.2. Galois Actions.

The companion reading for this subsection is Neukirch Chapter 4 Section 3.

Let  $K$  be a field and  $G = G_K = \text{Gal}(\overline{K}/K)$ . Let  $A$  be a continuous (the action  $G \times A \rightarrow A$  taking  $(\sigma, a) \mapsto \sigma(a)$  is continuous) discrete (A is equipped with the discrete topology) multiplicative (we write the group operation on  $A$  multiplicatively)  $G$ -module ( $G$ -module is shorthand for  $\mathbb{Z}[G]$ -module). By the continuity of the  $G$ -action, there exists a finite  $L/K$  such that  $\sigma \text{Gal}(\overline{K}/L)a = \sigma(a)$ , i.e.,  $\text{Gal}(\overline{K}/L) \subset \text{Stab}(a)$ . Hence, such a  $G$ -action is continuous if and only if every element  $a \in A$  is stabilized by  $\text{Gal}(\overline{K}/L)$  for some finite  $L \subset \overline{K}$ . This is equivalent to  $\text{Stab}(a)$  being open for all  $a \in A$ . Write  $G_L = \text{Gal}(\overline{K}/L) \subset G_K$ .

**Example 13.7.** Our main example will be  $A = K^*$ .

**Definition 13.8.** For  $L/K$  finite ( $L \subset \overline{K}$ ), we have  $A_L := A^{G_L} = \{a \in A \mid \sigma(a) = a, \sigma \in \text{Gal}(\overline{K}/L)\}$ .

**Example 13.9.** In the case  $A = \overline{K}^*$ , we have  $A_L = L^*$

**Definition 13.10.** We define a norm  $N_{L/K} : A_L \rightarrow A_K$  taking

$$a \mapsto \prod_{\substack{\text{representatives} \\ \sigma \text{ of } G_K/G_L}} \sigma(a)$$

**13.3. The Norm Residue Group.** For  $L/K$  Galois, define

$$H^0(\text{Gal}(L/K), A_L) = A_K / (N_{L/K} A_L).$$

**Remark 13.11.** This is not the usual group cohomology. Rather, this is Tate cohomology; in a setting in which one is working with both group cohomology and Tate cohomology, it is usual to let  $\widehat{H}^0$  denote the group defined above.

Also define

$$H^{-1}(\text{Gal}(L/K), A_L) = \frac{\{a \in A_L \mid N_{L/K}(a) = 1\}}{\langle \sigma(b)b^{-1} \mid b \in A_L, \sigma \in \text{Gal}(L/K) \rangle}.$$

Note that  $H^{-1}(\text{Gal}(L/K), A_L)$  measures the extent to which  $\sigma(b)b^{-1}$  gives all of the norm 1 elements.

**Example 13.12.** Here is another common example. Let  $K$  be a local field and  $A \subset \overline{K}^*$  the subgroup of elements of valuation 0.

**Theorem 13.13** (Hilbert 90). *For a finite cyclic extension (i.e., the extension is Galois with cyclic Galois group)  $L/K$ , any  $\alpha \in L^*$  with  $N_{L/K}(\alpha) = 1$  is of the form  $\alpha = \sigma(\beta)\beta^{-1}$  for some  $\beta \in L^* + \sigma \in \text{Gal}(L/K)$ . In particular, we have  $H^{-1}(\text{Gal}(L/K), L^*) = 1$ .*

*Proof.* Let  $n = [L : K]$ . By the linear independence of elements of  $\langle \sigma \rangle = \text{Gal}(L/K)$ , the map

$$\gamma \mapsto \gamma + \alpha\sigma(\gamma) + \alpha\sigma\alpha\sigma^2(\gamma) + \cdots + \alpha\sigma\alpha \cdots \sigma^{n-1}(\alpha)\sigma^{n-1}(\gamma)$$

is not 0. In other words, there is some nonzero  $\beta$  in the image of the map described above such that  $\alpha\sigma(\beta) = \alpha\sigma(\gamma) + \alpha\sigma(\alpha)\sigma^2(\gamma) + \cdots + \alpha\sigma(\alpha) \cdots \sigma^{n-1}(\alpha)\sigma^n(\gamma)$ . Since  $\alpha$  has norm 1, we have  $\alpha\sigma(\alpha) \cdots \sigma^{n-1}(\alpha) = 1$ , and since  $\sigma$  has order  $n$ , we have  $\sigma^n(\gamma) = \gamma$ . Hence,  $\alpha\sigma(\beta) = \beta$ , as desired.  $\square$

**13.4. Kummer Theory.** Neukirch begins his presentation of Kummer theory in the following way: “Assume  $H^{-1}(G(L/K), A_L) = 1$  for all finite cyclic extensions  $L/K$ ...” However, our approach will not be so general. Let  $n$  be an integer such that  $\text{char}(K) \nmid n$ . Consider the  $n$ th power map  $n : \overline{K}^* \rightarrow \overline{K}^*$  taking  $a \mapsto a^n$ . We get the following exact sequence

$$1 \longrightarrow \mu_n \longrightarrow \overline{K}^* \xrightarrow{n} \overline{K}^* \longrightarrow 1$$

**Proposition 13.14.** *Assume  $\mu_n \subset K$  and that the characteristic of  $K$  does not divide  $n$ . For  $\Delta \subset K^*$ , we have that*

$$\text{Gal}(K(\sqrt[n]{\Delta})/K)$$

*is abelian of exponent  $n$ .*

*Proof.* We have a map  $\text{Gal}(K(\sqrt[n]{\Delta})/K) \rightarrow \mu_n$  taking  $\sigma \mapsto \sigma(\alpha)/\alpha$  for  $\alpha = \sqrt[n]{a}$ ,  $a \in \Delta$ . Since  $\mu_n \subset K$ , this map only depends on  $a$  (not  $\alpha$ ). Together, we have

$$\text{Gal}(K(\sqrt[n]{\Delta})/K) \rightarrow \prod_{a \in \Delta} \text{Gal}(K(\sqrt[n]{a})/K) \rightarrow (\mu_n)^\Delta,$$

where the first map is injective, as is each component of the second map. □

**Proposition 13.15.** *Assume  $\mu_n \subset K$  and that the characteristic of  $K$  does not divide  $n$ . If  $L/K$  is an abelian extension of exponent  $n$ , then  $L = K(\sqrt[n]{\Delta})$  with  $\Delta = (L^*)^n \cap K^*$*

14. MONDAY OCTOBER 30

**14.1. Kummer Theory Continued.** For those interested in more general group cohomology, we refer the reader to Sharifi's notes on general group cohomology and Brown's *Cohomology of Groups*.

**Theorem 14.1** (Kummer Theory). *If  $K$  is a field and  $n$  a natural number relatively prime to  $\text{char}(K)$  with  $\mu_n \subset K$ . Then finite abelian extensions  $L/K$  of exponent dividing  $n$  correspond bijectively with finite subgroups  $\Delta \subset K^*/(K^*)^n$ .<sup>7</sup> The map is given by  $\Delta \mapsto L = K(\sqrt[n]{\Delta})$ ; its inverse takes  $L \mapsto (L^*)^n K^*$ . Moreover, in this correspondence, we have  $\text{Gal}(L/K) \simeq \text{Hom}(\Delta, \mu_n)$  (so the Galois group is the Pontryagin dual of  $\Delta$ ).*

*Proof.* We begin with some field  $L$ ; let  $\Delta = (L^*)^n \cap K^*$ . We have  $\sqrt[n]{\Delta} \subset L^*$ , so  $K(\sqrt[n]{\Delta}) \subset L$ . Now,  $L/K$  is the compositum of finite cyclic extensions. Let  $M/K$  be a finite cyclic subextension. Let  $\text{Gal}(M/K) = \langle \sigma \rangle$  and  $\mu_n = \langle \zeta \rangle$  and  $d = [M : K]$ . Also let  $d' = n/d$ , and let  $\xi = \zeta^{d'}$ ; note that this is a  $d$ th root of unity. Since  $N_{M/K}(\xi) = \xi^d = 1$ , by Theorem 13.13, we have  $\xi = \sigma(\alpha)\alpha^{-1}$  for some  $\alpha \in M^*$ . Hence, we have  $K \subset K(\alpha) \subset M$ . But  $\sigma^i(\alpha) = \xi^i \alpha$ , so  $\sigma^i(\alpha) = \alpha$  if and only if  $i = 0 \pmod d$ . Thus,  $K(\alpha) = M$ . Also,  $\sigma(\alpha^n) = \alpha^{-n} = \xi^n - 1$ , implying  $\alpha^n \in K$ , so  $\alpha \in \sqrt[n]{\Delta}$ . It follows that  $M \subset K(\sqrt[n]{\Delta})$  and  $L = K(\sqrt[n]{\Delta})$ .

Now, consider  $\Delta \rightarrow \text{Hom}(\text{Gal}(L/K), \mu_n)$  taking  $a \mapsto \chi_a$ , where  $\chi_a \in \text{hom}(\text{Gal}(L/K), \mu_n)$  is given by  $\chi_a(\sigma) = \sigma(\sqrt[n]{a})/\sqrt[n]{a}$ . Since  $\chi_a = 1$  if and only if  $a \in (K^*)^n$ , the map described above is injective. To show surjective, take  $\chi \in \text{Hom}(\text{Gal}(L/K), \mu_n)$ . So  $\chi$  defines a cyclic subextension  $M/K$  and  $\chi$  is the composite

$$\text{Gal}(L/K) \longrightarrow \text{Gal}(M/K) \xrightarrow{\bar{\chi}} \mu_d \subset \mu_n.$$

Let notation be as above, and take  $\xi = \bar{\chi}(\sigma)$ . So  $\bar{\chi}(\sigma) = \xi = \sigma(\alpha)\alpha^{-1}$  and  $\sigma^i(\alpha) = \xi^i \alpha$  and  $\bar{\chi}(\sigma^i) = \xi^i = \sigma^i(\alpha)\alpha^{-1}$ . For  $\tau \in \text{Gal}(L/K)$ , we have

$$\chi(\tau) = \bar{\chi}(\tau|_M) = \tau(\alpha)\alpha^{-1} = \chi_{\alpha^n},$$

so  $\Delta \simeq \text{Hom}(\text{Gal}(L/K), \mu_n)$ . It follows that  $\text{Gal}(L/K) \simeq \text{Hom}(\Delta, \mu_n)$ .

Conversely, starting with any  $\Delta$  and  $L = K(\sqrt[n]{\Delta})$ , let  $\Delta' = (L^*)^n \cap K^*$ . Now,  $\Delta \subset \Delta'$ , and we have

$$\Delta' \simeq \text{Hom}(\text{Gal}(L/K), \mu_n) \quad \text{and} \quad \Delta \simeq \text{Hom}(\text{Gal}(L/K)/H, \mu_n)$$

for some subgroup  $H$ . The inclusion  $\Delta \subset \Delta'$  induces a map

$$\text{Hom}(\text{Gal}(L/K)/H, \mu_n) \rightarrow \text{Hom}(\text{Gal}(L/K), \mu_n).$$

We see that elements of  $H$  fix everything in  $\sqrt[n]{\Delta}$ , i.e., that  $H$  fixes  $L$ , so  $H$  is trivial. Thus,  $\Delta = \Delta'$ . □

<sup>7</sup>Recall that the exponent of a finite abelian group  $A$  is the smallest  $n$  such that  $nA = 0$ .

**14.2. Local Class Field Theory.** Goal: classify the abelian extensions of a local field  $k$ . Let  $G_k = \text{Gal}(\bar{k}/k)$ . We have

$$\begin{aligned} G_k &= \varprojlim_{\substack{K/k \text{ finite} \\ \text{Galois}}} \text{Gal}(K/k) \longrightarrow \varprojlim_{\substack{K/k \text{ unramified} \\ \text{finite Galois}}} \text{Gal}(K/k) \simeq \varprojlim_{\substack{K/k \text{ unramified} \\ \text{finite Galois}}} \text{Gal}(\kappa_K/\kappa_k) \\ &\simeq \varprojlim_r \text{Gal}(\mathbb{F}_{q^r}/\mathbb{F}_q) \simeq \hat{\mathbb{Z}}, \end{aligned}$$

where  $\kappa_K$  and  $\kappa_k$  denote the residue fields of  $K$  and  $k$  respectively.

This gives a surjective continuous homomorphism

$$(3) \quad d : G_k \rightarrow \hat{\mathbb{Z}}$$

(surjectivity follows from the fact that a projective limit of nonempty compact sets is nonempty). Note that (3) is one input into abstract class field theory. Let  $\ker(d) = \text{Gal}(\bar{k}/\tilde{k})$ ; one can check that  $\tilde{k}$  is the union of all unramified extensions of  $k$ —the “maximal unramified extension of  $k$ .”

For any finite Galois  $K/k$ , we have a map  $G_k \rightarrow \text{Gal}(K/k)$ , and under this map we see that  $\ker(d)$  maps to the inertia group isomorphically. We call  $\ker(d)$  the *inertia group*  $I_k$  of  $G_k$ .

For any finite separable  $K/k$ , we have  $G_K = \text{Gal}(\bar{k}/K) \subset \text{Gal}(\bar{k}/k) = G_k$ . We let  $I_K = G_K \cap I_k = \ker(d|_{G_K}) = G_K \cap G_{\tilde{k}} = G_{K\tilde{k}}$ . The takeaway is that  $K\tilde{k}$  is the maximal unramified extension of  $K$ . We also see that  $[\hat{\mathbb{Z}} : d(G_K)] = f_{K/k}$ , and  $[I_k : I_K] = e_{K/k}$ . We have

$$d_K = \frac{1}{f_{K/k}} d : G_K \rightarrow \hat{\mathbb{Z}}$$

is a continuous surjective map. Furthermore,  $\text{Frob}_K \in \text{Gal}(\tilde{k}/k)$  such that  $d_K(\text{Frob}_K) = 1$ .

Consider the isomorphism  $d_K : \text{Gal}(\tilde{K}/K) \rightarrow \hat{\mathbb{Z}}$  under which  $\text{Frob}_K \mapsto 1$ . Let  $L/K$  be a finite Galois extension. We take  $\text{Frob}(\tilde{L}/K)$  to be  $\{\sigma \in \text{Gal}(\tilde{L}/K) \mid d_K(\sigma) \in \mathbb{Z}_{\geq 1}\}$ . While this seems like an artificial set to consider, it is the easiest to understand at first. Moreover, we have the following proposition:

**Proposition 14.2.** *For  $L/K$  finite and Galois, we have*

$$\text{Frob}(\tilde{L}/K) \rightarrow \text{Gal}(L/K)$$

*is surjective, where the map is given by taking  $\sigma \in \text{Gal}(\tilde{L}/K)$  to its restriction to  $L$ .*

*Proof.* Let  $\sigma \in \text{Gal}(L/K)$  and  $\varphi \in \text{Gal}(\tilde{L}/K)$  such that  $d_K(\varphi) = 1$ , then  $\varphi|_{\tilde{k}} = \text{Frob}_K$ . Restricting  $\sigma$  to the maximal unramified subextension  $L \cap \tilde{K}/K$  of  $L/K$ , we get that  $\sigma|_{L \cap \tilde{K}} = \text{Frob}_K^n|_{L \cap \tilde{K}}$  for  $n \in \mathbb{Z}_{\geq 1}$ . One can check using Galois theory that  $\text{Gal}(\tilde{L}/\tilde{K}) \simeq \text{Gal}(L/L \cap \tilde{K})$ , so if  $\tau \in \text{Gal}(\tilde{L}/\tilde{K})$  is sent to  $\sigma\varphi^{-n}|_L$  under this map, then  $\tau\varphi^n|_L = \sigma$  and  $\tau\varphi^n|_{\tilde{k}} = \varphi^n|_{\tilde{k}} = \text{Frob}_K^n$ .  $\square$

## 15. WEDNESDAY NOVEMBER 1

**15.1. More Local Class Field Theory.** The companion reading is Neukirch Chapter IV Section 4. Recall that  $k$  is some local field with  $L/K/k$  finite extensions. We let  $\tilde{L}$  be the maximal unramified extension of  $L$ , i.e.,  $\tilde{L} = L\tilde{k}$ . Recall that there is a map

$$d_K : \text{Gal}(\tilde{k}/K) \twoheadrightarrow \text{Gal}(\tilde{K}/K) \leftrightarrow \widehat{\mathbb{Z}},$$

where the last map is an isomorphism under which  $\text{Frob}_K \mapsto 1 \in \widehat{\mathbb{Z}}$ . If  $L/K$  is Galois, then we can consider the semigroup  $\text{Frob}(\tilde{L}/K) = \{\sigma \in \text{Gal}(\tilde{L}/K) \mid d_K(\sigma) \in \mathbb{Z}_{\geq 1}\}$ .



**Proposition 15.1.** *Let  $\sigma \in \text{Frob}(\tilde{L}/K)$ , and let  $\Sigma$  be the fixed field of  $\sigma$ . Then*

- (1)  $[\Sigma : K] < \infty$ ;
- (2)  $f_{\Sigma/K} = d_K(\sigma)$ ;
- (3)  $\tilde{\Sigma} = \tilde{L}$ ;
- (4)  $\sigma|_{\tilde{\Sigma}} = \text{Frob}_{\tilde{\Sigma}}$ .

*Proof.* Recall that  $d_K$  gives an isomorphism  $\text{Gal}(\tilde{K}/K) \rightarrow \widehat{\mathbb{Z}}$ . Galois theory then implies that  $\text{Gal}(\Sigma \cap \tilde{K}/K) \simeq \widehat{\mathbb{Z}}/\langle d_K(\sigma) \rangle$ , where  $\langle d_K(\sigma) \rangle$  is the closed subgroup generated by  $d_K(\sigma)$ . Since  $d_K(\sigma) \in \mathbb{Z}_{\geq 1}$ , it follows that  $\widehat{\mathbb{Z}}/\langle d_K(\sigma) \rangle \simeq \mathbb{Z}/d_K(\sigma)\mathbb{Z}$ . Thus,  $[\Sigma \cap \tilde{K} : K] < \infty$ . On the other hand,  $\tilde{K} \subset \Sigma\tilde{K} = \tilde{\Sigma} \subset \tilde{L}$ , so

$$[\text{Gal}(\tilde{k}/\tilde{K}) = I_K : \text{Gal}(\bar{k}/\tilde{\Sigma}) = I_{\Sigma}] = \#\text{Gal}(\tilde{\Sigma}/\tilde{K}) \leq \#\text{Gal}(\tilde{L}/\tilde{K}) \leq \#\text{Gal}(L/K).$$

Now, considering the following diagram, we see that

$$\begin{array}{ccccccc} 1 & \longrightarrow & I_{\Sigma} & \longrightarrow & G_{\Sigma} & \longrightarrow & \text{Gal}(\tilde{\Sigma}/\Sigma) \longrightarrow 1 \\ & & \downarrow & & \downarrow & & \downarrow \\ 1 & \longrightarrow & I_K & \longrightarrow & G_K & \longrightarrow & \text{Gal}(\tilde{K}/K) \longrightarrow 1 \end{array}$$

$\Sigma/K$  is finite because  $I_K$  has finite index since its image is  $\text{Gal}(\tilde{K}/\Sigma \cap \tilde{K})$ .

For (2), recall that  $f_{\Sigma/K}$  is the degree of the maximal unramified subextension of  $\Sigma/K$ , which is just  $[\Sigma \cap \tilde{K} : K] = d_K(\sigma)$ .

For (3), we have a surjection

$$\langle \sigma \rangle = \text{Gal}(\tilde{L}/\Sigma) \twoheadrightarrow \text{Gal}(\tilde{\Sigma}/\Sigma) \simeq \widehat{\mathbb{Z}},$$

where again  $\langle \sigma \rangle$  is the closed subgroup generated by  $\sigma$ . This forces the above map to be an isomorphism, so  $\tilde{L} = \tilde{\Sigma}$ .

For (4), we have  $f_{\Sigma/K}d_{\Sigma}(\sigma) = D_K(\sigma) = f_{\Sigma/K}$ , implying  $d_{\Sigma}(\sigma) = 1$ .  $\square$

For any subextension  $M$  of  $\bar{k}/k$ , we let  $O_M^*$  denote the elements of  $M^*$  with valuation 0.

**Lemma 15.2** (Input 1). *Let  $L/K/k$  be finite and let  $L/K$  be Galois and unramified. Then we have that  $H^i(\text{Gal}(L/K), O_L^*) = 1$  for  $i = 0, -1$ .*

Our goal is to, for all  $L/K$  finite and Galois, define canonical

$$r_{L/K} : \text{Gal}(L/K) \rightarrow K^*/N_{L/K}(L^*).$$

Since the codomain is abelian, such maps will tell us about the abelianization of  $\text{Gal}(L/K)$ .

**Definition 15.3.** Assuming Input 1 (Lemma 15.2), we define the *reciprocity map* to be

$$r_{\tilde{L}/K} : \text{Frob}(\tilde{L}/K) \rightarrow K^*/N_{\tilde{L}/K}\tilde{L}^*$$

taking  $\sigma \mapsto [N_{\Sigma/K}(\pi_{\Sigma})]$  where  $\Sigma$  is the fixed field of  $\sigma$ .

We need to check that  $r_{\tilde{L}}(\sigma)$  does not depend on  $\pi_{\Sigma}$ . In other words, we need to show that  $u \in O_{\Sigma}^*$  has  $N_{\Sigma/K}(u) \in N_{M/K}M^*$  for all  $M/K$  finite subextensions of  $\tilde{L}/K$ . Since a norm from  $M$  is a norm from any subfield, we can assume  $\Sigma \subset M$  and  $M/\Sigma$  is Galois. Moreover, since  $\tilde{\Sigma} = \tilde{L}$ , we have  $M/\Sigma$  is unramified. Applying Input 1 (Lemma 15.2) for  $H^0$ , it follows that  $O_{\Sigma}^*/N_{M/\Sigma}O_M^* = 1$ . So  $u \in N_{M/\Sigma}(u')$ , implying  $N_{\Sigma/K}(u) \in N_{M/K}M^*$ .

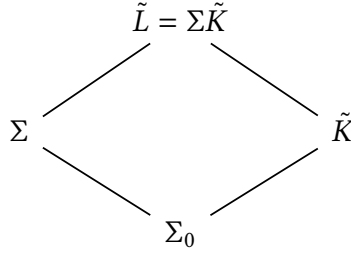
For an infinite extension  $M/K$ , we have

$$N_{M/K}M^* = \bigcap_{\substack{L/K \text{ finite} \\ \text{subextensions}}} N_{L/K}L^*.$$

Next, we will work towards showing that  $r_{\tilde{L}/K}$  is multiplicative. For  $\sigma \in \text{Gal}(\tilde{L}/K)$  and  $n \in \mathbb{Z}_{\geq 1}$ , let  $\sigma_n : \tilde{L}^* \rightarrow \tilde{L}^*$  be the map taking  $a \mapsto a\sigma(a)\sigma^2(a) \cdots \sigma^{n-1}(a)$ . In the group algebra we would use additive notation and write this as  $1 + \sigma + \cdots + \sigma^{n-1} = (\sigma^n - 1)/(\sigma - 1)$ .

**Lemma 15.4.** *Let  $\varphi, \sigma \in \text{Frob}(\tilde{L}/K)$  with  $d_K(\varphi) = 1$ . Let  $d_K(\sigma) = n$ . If  $\Sigma$  is the fixed field of  $\sigma$  and  $a \in \Sigma^*$ , then  $N_{\Sigma/K}(a) = N_{\tilde{L}/\tilde{K}}(\varphi_n(a))$ .*

*Proof.* The maximal unramified subextension  $\Sigma^0 = \Sigma \cap \tilde{K}$  of  $\Sigma/K$  has  $\text{Gal}(\Sigma^0/K)$  generated by  $\text{Frob}_K = \varphi|_{\Sigma^0}$ . So,  $N_{\Sigma^0/K} = \varphi_n$ . Also,  $\Sigma\tilde{K} = \tilde{L}$ , so



implies that  $N_{\Sigma/\Sigma_0} = N_{\tilde{L}/\tilde{K}}|_{\Sigma}$ . □

**Lemma 15.5.** *Given Input 1 (Lemma 15.2), if*

$$x \in \mathcal{O}_{\tilde{L}}^* / \langle \sigma(\alpha)\alpha^{-1} \mid \alpha \in \mathcal{O}_{\tilde{L}}^*, \sigma \in \text{Gal}(\tilde{L}/\tilde{K}) \rangle$$

*is fixed by an element  $\varphi \in \text{Gal}(\tilde{L}/K)$  such that  $d_K(\varphi) = 1$ , then  $N_{\tilde{L}/\tilde{K}}(x) \in N_{\tilde{L}/K}\mathcal{O}_{\tilde{L}}^*$ . By  $N_{\tilde{L}/K}\mathcal{O}_{\tilde{L}}^*$  we mean*

$$\bigcap_{\substack{\text{finite } M/K \\ \text{subextensions}}} N_{M/K}\mathcal{O}_M^*.$$

*Remarks on the proof.* To prove the above, one needs to show a norm from every sufficiently large finite extension; the proof is computational and uses Input 1 for  $H^0$  and  $H^{-1}$ . □

Next time, we will put all of this together to see that  $r_{\tilde{L}/K}$  is multiplicative and then define  $r_{L/K}$ .

## 16. MONDAY NOVEMBER 6

**16.1. Reciprocity.** Let  $k$  be a local field, and let  $K, L$  be finite extensions of  $k$  contained in the separable closure  $\bar{k}$  of  $k$ . Recall that  $\bar{K} = K\bar{k}$  is the maximal unramified extension of  $K$ ; moreover, we have a map

$$d_K : G_K = \text{Gal}(\bar{k}/k) \rightarrow \text{Gal}(\tilde{K}/K) \simeq \widehat{\mathbb{Z}}$$

which sees the action on the residue fields. We also have  $\text{Frob}(\tilde{L}/K) = \{\sigma \in \text{Gal}(\tilde{L}/K) \mid d_K(\sigma) \in \mathbb{Z}_{\geq 1}\}$ , and a map  $r_{\tilde{L}/K} : \text{Frob}(\tilde{L}/K) \rightarrow K^*/N_{\tilde{L}/K}(\tilde{L}^*)$  taking  $\sigma \mapsto [N_{\Sigma/K}(\pi_{\Sigma})]$ , where  $\Sigma$  is the field fixed by  $\sigma$ .

**Proposition 16.1.** *Assuming Lemma 15.2, which states that  $H^i(\mathcal{O}_L^*) = 0$  for unramified extensions, then  $r_{\tilde{L}/K}$  is multiplicative.<sup>8</sup>*

*Proof.* Take  $\sigma_1, \sigma_2, \sigma_3 \in \text{Frob}(\tilde{L}/K)$  be such that  $\sigma_1\sigma_2 = \sigma_3$ . Let  $n_i = d_K(\sigma_i)$ , let  $\Sigma_i$  be the fixed field of  $\sigma_i$ , and let  $\pi_i$  be a uniformizer of  $\Sigma_i$ . Our goal is to show that

$$N_{\Sigma_1/K}(\pi_1)N_{\Sigma_2/K}(\pi_2) \equiv N_{\Sigma_3/K}(\pi_3) \pmod{N_{\tilde{L}/K}(\tilde{L}^*)}.$$

Choose  $\varphi \in \text{Gal}(\tilde{L}/K)$  such that  $d_K(\varphi) = 1$ , and let  $\tau_i = \varphi^{n_i}\sigma_i^{-1} \in \text{Gal}(\tilde{L}/\tilde{K})$  (note that  $\tau_i$  fixes  $\tilde{K}$  since  $d_K(\tau_i) = 0$ ). So

$$\tau_3 = \varphi^{n_3}\sigma_3^{-1} = \varphi^{n_1+n_2}\sigma_2^{-1}\sigma_1^{-1} = \varphi^{n_2}(\varphi^{n_1}\sigma_2^{-1}\varphi^{-n_1})\varphi^{n_1}\sigma_1^{-1}.$$

Let  $\sigma_4 = \varphi^{n_1}\sigma_2^{-1}\varphi^{-n_1}$ ; note that  $d_K(\sigma_4) = n_2$ . The fixed field  $\Sigma_4$  of  $\sigma_4$  is  $\varphi^{n_1}(\Sigma_2)$ , and we can take the corresponding uniformizer to be  $\pi_4 = \varphi^{n_1}(\pi_2)$ . Then  $\tau_4 = \varphi^{n_2}\sigma_4^{-1}$ , so  $\tau_3 = \tau_4\tau_1$ . Also,  $N_{\Sigma_4/K}(\pi_4) = N_{\Sigma_2/K}(\pi_2)$ . By the lemma we proved last class, we have that

$$N_{\Sigma_i/K}(\pi_i) = N_{\tilde{L}/\tilde{K}}(\varphi_{n_i}(\pi_i)),$$

where we recall that  $\varphi_{n_i} = (\varphi^{n_i} - 1)/(\varphi - 1)$ . Hence, it suffices to show that

$$N_{\tilde{L}/\tilde{K}}(\varphi_{n_3}(\pi_3)\varphi_{n_4}(\pi_4)^{-1}\varphi_{n_1}(\pi_1)^{-1}) \in N_{\tilde{L}/K}(\tilde{L}^*).$$

Letting

$$u = \varphi_{n_3}(\pi_3)\varphi_{n_4}(\pi_4)^{-1}\varphi_{n_1}(\pi_1)^{-1},$$

we have

$$\varphi(u)u^{-1} = \tau_3(\pi_3)\pi_3^{-1}\pi_4\tau_4(\pi_4)^{-1}\pi_1\tau_1(\pi_1)^{-1};$$

this follows from the fact that  $\sigma_i(\pi_i) = \pi_i$ . Let  $u_3 = \pi_3\pi_4^{-1}$ ,  $u_1 = \pi_4\pi_1^{-1}$ , and  $u_4 = \tau_1(\pi_4)\pi_4^{-1}$ .

We claim that the  $u_i$ 's have valuation 0.<sup>9</sup> We have  $\varphi(u)u^{-1} = \prod_{i \in \{1,3,4\}} \tau_i(u_i)u_i^{-1}$  using the fact that  $\tau_3 = \tau_4\tau_1$ . By Lemma 15.5, we have  $N_{\tilde{L}/\tilde{K}}(u) \in N_{\tilde{L}/K}(\tilde{L}^*)$ .  $\square$

For any finite Galois  $L/K$ , we have the *reciprocity homomorphism*  $r_{L/K} : \text{Gal}(L/K) \rightarrow K^*/N_{L/K}(L^*)$ . Given  $\sigma \in \text{Gal}(L/K)$ , we lift  $\sigma$  to  $\tilde{\sigma} \in \text{Frob}(\tilde{L}/K)$  and apply  $r_{\tilde{L}/K}$  to get the element  $[N_{\Sigma/K}\pi_\Sigma] \in K^*/N_{L/K}L^*$ , where  $\Sigma$  is the fixed field of  $\tilde{\sigma}$ . This map is well-defined, since  $N_{\tilde{L}/\tilde{K}}\tilde{L}^* \subset N_{L/K}L^*$ ; moreover the map is independent of our choice of  $\tilde{\sigma}$ . To see this, let  $\tilde{\sigma}, \tilde{\sigma}'$  be preimages of  $\sigma$  with corresponding fixed fields  $\Sigma, \Sigma'$ , respectively. If  $d_K(\tilde{\sigma}) = d_K(\tilde{\sigma}')$ , then  $\tilde{\sigma}, \tilde{\sigma}'$  are the same on  $\tilde{K}$  and  $L$ , so they are the same on  $\tilde{K}L = \tilde{L}$ . Therefore  $\tilde{\sigma} = \tilde{\sigma}'$ . If  $d_K(\tilde{\sigma}) < d_K(\tilde{\sigma}')$ , then  $\tilde{\sigma}' = \tilde{\sigma}\tau$  for some  $\tau \in \text{Frob}(\tilde{L}/K)$  with  $\tau|_L = 1$ . Let  $\Sigma''$  be the fixed field of  $\tau$ . So

$$r_{\tilde{L}/K}(\tau) = N_{\Sigma''/K}(\pi_{\Sigma''}) \equiv 1 \pmod{N_{L/K}(L^*)},$$

since  $L \subset \Sigma''$ . Thus,

$$r_{\tilde{L}/K}(\tilde{\sigma}') = r_{\tilde{L}/K}(\tilde{\sigma})r_{\tilde{L}/K}(\tau) \equiv r_{\tilde{L}/K}(\tilde{\sigma}) \pmod{N_{L/K}(L^*)},$$

implying  $r_{L/K}$  does not depend on our choice of lift. Finally, the multiplicativity of  $r_{L/K}$  follows from that of  $r_{\tilde{L}/K}$ .

**Proposition 16.2.** *Assume Lemma 15.2. Then for an unramified finite extension  $L/K$ , the map  $r_{L/K} : \text{Gal}(L/K) \rightarrow K^*/N_{L/K}L^*$  takes  $\text{Frob}_K \mapsto \pi_K$  and is an isomorphism.*

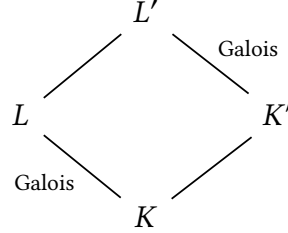
<sup>8</sup>Warning: in the corresponding section of Neukirch, the Galois action is presented as a right action. However, in what follows our Galois action shall always be a left action.

<sup>9</sup>Prove this as an exercise.

*Proof.* Note that  $\text{Frob}_K$  has fixed field  $K$  and that  $\text{Gal}(L/K)$  is cyclic of order  $f_{L/K}$  generated by  $\text{Frob}_K$ . Likewise,  $K^*/N_{L/K}(L^*)$  is cyclic of order  $f_{L/K}$  generated by  $\pi_K$ .

By Lemma 15.2,  $H^0$  is trivial, so all units in  $\mathcal{O}_K^*$  are norms. And  $v(N_{L/K}L^*) = f_{L/K}\mathbb{Z}$ .  $\square$

Functoriality of the reciprocity homomorphism: given the following diagram



we have that the following diagram commutes

$$\begin{array}{ccc}
 \text{Gal}(L'/K') & \xrightarrow{r_{L'/K'}} & (K')^*/N_{L'/K'}(L')^* \\
 \downarrow & & \downarrow N_{K'/K} \\
 \text{Gal}(L/K) & \xrightarrow{r_{L/K}} & K^*/N_{L/K}L^*
 \end{array}$$

**Example 16.3.** For  $\sigma \in \text{Frob}(\tilde{L}/K)$  with fixed field  $\Sigma$ , the above diagram becomes

$$\begin{array}{ccc}
 \sigma \in \text{Gal}(L\Sigma/\Sigma) & \xrightarrow{r_{L\Sigma/\Sigma}} & \pi_\Sigma \in \Sigma^*/N_{L\Sigma/\Sigma}(L\Sigma)^* \\
 \downarrow & & \downarrow N_{\Sigma/K} \\
 \sigma \in \text{Gal}(L/K) & \xrightarrow{r_{L/K}} & N_{\Sigma/K}(\pi_\Sigma) \in K^*/N_{L/K}L^*.
 \end{array}$$

For  $\sigma \in G_k = \text{Gal}(\bar{k}/k)$ , the following diagram commutes:

$$\begin{array}{ccc}
 \text{Gal}(L/K) & \xrightarrow{r_{L/K}} & K^*/N_{L/K}L^* \\
 \downarrow & & \downarrow N_{K/\sigma(K)} \\
 \text{Gal}(\sigma(L)/\sigma(K)) & \xrightarrow{r_{\sigma(L)/\sigma(K)}} & \sigma(K)^*/N_{\sigma(L)/\sigma(K)}\sigma(L)^*
 \end{array}$$

To summarize what we've done so far, recall that we have basically only used Lemma 15.2 to construct the reciprocity homomorphism  $r_{L/K}$ . Next, we will use the *Class Field Axiom*, which implies Lemma 15.2, to show that  $r_{L/K} : \text{Gal}(L/K)^{ab} \rightarrow K^*/N_{L/K}(L^*)$  is an isomorphism.

## 17. WEDNESDAY NOVEMBER 8

**17.1. The Class Field Axiom.** The companion reading for this section is Neukirch Chapter IV Section 6. Let  $k$  be a local field with  $L/K/k$  finite extensions such that  $L, K \subset \bar{k}$ .

**Theorem 17.1** (Class Field Axiom). *For every finite cyclic  $L/K$ , we have*

$$|H^i(\text{Gal}(L/K), L^*)| = \begin{cases} [L : K] & \text{if } i = 0; \\ 1 & \text{otherwise.} \end{cases}$$

**Proposition 17.2.** *Theorem 17.1 implies Lemma 15.2.*

*Proof.* Let  $L/K$  be unramified. Then  $\pi_K$  is a uniformizer of  $L$ . Since  $H^{-1}(\text{Gal}(L/K), L^*) = 0$ , every  $u \in \mathcal{O}_L^*$  such that  $N_{L/K}(u) = 1$  is of the form  $u = \sigma(a)a^{-1}$  for some  $a \in L^*$  and  $\sigma$  a generator of  $\text{Gal}(L/K)$ . If  $a = \epsilon\pi_K^m$  for  $\epsilon \in \mathcal{O}_L^*$ , then  $\sigma(\epsilon)\epsilon^{-1} = u$  since  $\sigma(\pi_K) = \pi_K$ . It follows that  $H^{-1}(\text{Gal}(L/K), \mathcal{O}_L^*) = 0$ .

The valuation gives a surjection

$$\bar{v} : k^*/N_{K/L}L^* \twoheadrightarrow \mathbb{Z}/f_{L/K}.$$

Since  $[L : K] = f_{L/K}$ , so  $\bar{v}$  is an isomorphism. So  $u \in \mathcal{O}_K^*$ , implying that  $\bar{v}(u) = 0$ . Therefore  $u \in N_{L/K}L^*$ . By valuations,  $u \in N_{L/K}\mathcal{O}_L^*$  implies  $H^0(\text{Gal}(L/K), \mathcal{O}_L^*) = 0$ .  $\square$

**Theorem 17.3** (General Reciprocity Law). *Assume Theorem 17.1 (the Class Field Axiom). Then for all finite Galois extensions  $L/K$ , the reciprocity map*

$$r_{L/K} : \text{Gal}(L/K)^{ab} \rightarrow K^*/N_{L/K}L^*$$

*is an isomorphism.*

*Proof.* Case 1: Suppose  $L/K$  is cyclic and totally ramified. Then  $L \cap \tilde{K} = K$ . Let  $\sigma$  generate  $\text{Gal}(\tilde{L}/\tilde{K}) \simeq \text{Gal}(L/K)$ . Let  $\tilde{\sigma} = \sigma \text{Frob}_L \in \text{Frob}(\tilde{L}/\tilde{K})$  and  $d_K(\tilde{\sigma}) = f_{L/K} = 1$ . Let  $\Sigma$  be a fixed field of  $\tilde{\sigma}$ , so  $f_{\Sigma/K} = 1$  and  $\Sigma \cap \tilde{K} = K$ . Let  $M/K$  be a finite Galois subextension of  $\tilde{L}/K$  containing  $L$  and  $\Sigma$ . Let  $M_0 = M \cap \tilde{K}$  be the maximal unramified subextension. Let  $N = N_{M/M_0}$ . In the homework, we showed that  $N|_{\Sigma} = N_{\Sigma/K}$ ,  $N|_L = N_{L/K}$ ,  $\text{Gal}(M/M_0) = \text{Gal}(L/K)$ , and  $\text{Gal}(M/K) \simeq \text{Gal}(M/L) \times \text{Gal}(L/K)$ . To show that  $r_{L/K}$  is injective, suppose that  $r_{L/K}(\sigma^k) = 1$  with  $0 \leq k < [L : K]$ . Note that  $\pi_{\Sigma}, \pi_L$  are both uniformizers of  $M$ , since  $M \subset \tilde{L} = \tilde{\Sigma}$ , so  $M/L$  and  $M/\Sigma$  are unramified. Let  $\pi_{\Sigma}^k = u\pi_L^k$  for  $u \in \mathcal{O}_M^*$ . So

$$1 = r_{L/K}(\sigma^k) \equiv N(\pi_{\Sigma}^k) \equiv N(u)N(\pi_L^k) \equiv N(u) \pmod{N_{L/K}L^*}.$$

Hence,  $N(u) = N(v)$  for some  $v \in \mathcal{O}_L^*$ . By the Class Field Axiom applied to  $M/M_0$ ,  $u^{-1}v = \sigma(a)a^{-1}$  for some  $a \in M^*$ . A computation shows that  $x = \pi_L^k v a \tilde{\sigma}(a)^{-1}$  is fixed by  $\sigma$ . Thus,  $x \in M_0$ . Further, we have that  $[L : K]v_{M_0}(x) = [M : M_0]v_{M_0}(x) = v_M(x) = k$  implies  $k = 0$ . It follows that  $r_{L/K}$  is injective. Now  $r_{L/K}$  is surjective by the Class Field Axiom for  $L/K$  and counting.

Case 2: Suppose  $L/K$  is cyclic. Let  $M = L \cap \tilde{K}$  be the maximal unramified subextension of  $L/K$ . So  $f_{L/M} = 1$  and  $r_{M/K}$  is an isomorphism since  $M/K$  is unramified. We know that  $r_{L/M}$  is an isomorphism since it is a cyclic, totally ramified extension. Now, we have an exact sequence

$$M^*/N_{L/M}L^* \xrightarrow{N_{M/K}} K^*/N_{L/K}L^* \longrightarrow K^*/N_{M/K} \longrightarrow 1.$$

The Class Field Axiom implies that the orders of the groups are  $[L : M]$ ,  $[L : K]$ ,  $[M : K]$ , which implies by counting that the map  $N_{M/K}$  in the above is injective, giving us a short exact sequence:

$$1 \longrightarrow M^*/N_{L/M}L^* \xrightarrow{N_{M/K}} K^*/N_{L/K}L^* \longrightarrow K^*/N_{M/K} \longrightarrow 1.$$

We also have an exact sequence of Galois groups

$$1 \longrightarrow \text{Gal}(L/M) \longrightarrow \text{Gal}(L/K) \longrightarrow \text{Gal}(M/K) \longrightarrow 1.$$

Putting these two exact sequences together using the reciprocity maps, we have the following commutative diagram

$$\begin{array}{ccccccc}
1 & \longrightarrow & \text{Gal}(L/M) & \longrightarrow & \text{Gal}(L/K) & \longrightarrow & \text{Gal}(M/K) \longrightarrow 1 \\
& & \downarrow r_{L/M} & & \downarrow r_{L/K} & & \downarrow r_{M/K} \\
1 & \longrightarrow & M^*/N_{L/M}L^* & \xrightarrow{N_{M/K}} & K^*/N_{L/K}L^* & \longrightarrow & K^*/N_{M/K}L^* \longrightarrow 1,
\end{array}$$

where  $r_{L/M}$  and  $r_{M/K}$  are isomorphisms. The Snake Lemma then implies that  $r_{L/K}$  is an isomorphism.

**Third Case:** Suppose  $L/K$  is abelian. If  $M/K$  varies over cyclic subextensions of  $L/K$ , the functoriality of the reciprocity maps imply

$$\ker_{r_{L/K}} \subset \ker \left( \text{Gal}(L/K) \rightarrow \prod_M \text{Gal}(M/K) \right).$$

However, the right-hand side is just 0, since  $L$  is the composite of the  $M$ 's. Surjectivity follows by functoriality and induction on the degree.

**Final Case:** Suppose  $L/K$  is a general extension. Let  $M = L^{ab}$ , so  $\text{Gal}(L/K)^{ab} = \text{Gal}(M/K)$ . Hence,  $\ker(r_{L/K}|_{\text{Gal}(L/K)}) \subset \ker(\text{Gal}(L/K) \rightarrow \text{Gal}(M/K))$ . It follows that  $r_{L/K}$  is injective on  $\text{Gal}(L/K)^{ab}$ . To see surjectivity, we induct on the degree and use functoriality. Since  $r_{M/K}$  is surjective ( $M/K$  is abelian), so if  $[L : M] < [L : K]$  the surjectivity of  $r_{L/M}$  follows from induction. Therefore,  $r_{L/K}$  is surjective. And if  $M = K$ , i.e., if  $\text{Gal}(L/K)^{ab} = 1$ , let  $M_p$  be the fixed field of a Sylow  $p$ -subgroup of  $\text{Gal}(L/K)$  for  $p \nmid \#\text{Gal}(L/K)$ . It follows that  $[L : M_p] < [L : K]$ , so by induction we can assume  $r_{L/M_p}$  is surjective. We will show that  $\text{im}(N_{M_p/K}M_p^*)$  is the Sylow  $p$ -subgroup  $S_p$  of  $K^*/N_{L/K}L^*$ . For  $k \in S_p$ ,  $\alpha = k^{1/[M_p:K]}$  exists in  $S_p$  since  $p \nmid [M_p : K]$ . Then  $N_{M_p/K}(\alpha) = \alpha^{[M_p:K]} = k$ . So  $\text{im}(r_{L/K})$  contains a Sylow  $p$ -subgroup of  $K^*/N_{L/K}L^*$  for all  $p$ , implying that  $r_{L/K}$  is surjective.  $\square$

## 18. MONDAY NOVEMBER 13

Let  $K$  be a local field. On  $K^*$ , define the *norm topology*, where a basis of open neighborhoods is given by cosets of  $N_{L/K}L^*$  for  $L/K$  finite Galois.

**Theorem 18.1.** *Assuming Theorem 17.1, associating  $L \mapsto N_{L/K}L^*$  gives a bijective correspondence between finite abelian extensions of  $K$  and norm-topology-open subgroups of  $K^*$ .*

*Proof.* The proof is formal using Galois theory.  $\square$

**Remark 18.2.** We remark that  $L$  is called the *class field* of  $N_{L/K}L^*$  with  $\text{Gal}(L/K) \simeq K^*/N_{L/K}L^*$ . For a subgroup  $N$  of  $K^*$ , we say that  $L$  is the class field of  $N$  if  $N = N_{L/K}L^*$ .

**Proposition 18.3.** *The open subgroups in the norm topology are exactly the open subgroups of finite index in the usual topology on  $K^*$ .*

*Proof of the hard direction for  $\text{char}(K) \nmid n$ .* The difficult direction is showing that an open finite index subgroup  $N \leq K^*$  contains a norm group. If  $N$  has finite index, then  $n = [K^* : N]$  implies that  $(K^*)^n \subset N$ . Thus, we will show that  $(K^*)^n$  contains a norm group when  $\text{char}(K) \nmid n$ . If  $\text{char}(K) \nmid n$ , then we can assume  $K$  contains  $\mu_n$ , since if  $(K(\mu_n)^*)^n$  contains a norm group then so does  $(K^*)^n$  by taking further norms. We have  $K^*/(K^*)^n$  is finite by the structure of  $K^*$  and the fact that  $\text{char}(K) \nmid n$ . So  $L = K(\sqrt[n]{K^*})/K$  has Galois group  $\text{Gal}(L/K) \simeq \text{Hom}(K^*/(K^*)^n, \mu_n)$  by Kummer theory. Also,  $\text{Gal}(L/K) \simeq K^*/N_{L/K}L^*$ , so because  $\text{Gal}(L/K)$  has exponent dividing  $n$ , we have that  $(K^*)^n \subset N_{L/K}L^*$ . However,  $[K^* : N_{L/K}L^*] = |\text{Gal}(L/K)| = [K^* : (K^*)^n]$ , so  $(K^*)^n = N_{L/K}L^*$ , as desired.  $\square$

**Remark 18.4.** When  $K \supset \mu_n$  and  $\text{char}(K) \nmid n$ , then  $K(\sqrt[n]{K^*})$  is the class field  $(K^*)^n$

These results fit together into an isomorphism

$$r_K : \text{Gal}(K^{ab}/K) \rightarrow \widehat{K^*} := \varprojlim_{\substack{N \leq K^* \text{ open,} \\ \text{finite-index subgroups}}} K^*/N$$

( $K^{ab}$  is the maximal abelian extension, i.e., the composite of all abelian extensions of  $K$ ; the projective limit in the above ranges over continuous finite quotients of  $K^*$ ). Recall that  $K^* \simeq \mathcal{O}_K \times \langle \pi_K \rangle \simeq \mathcal{O}_K^* \times \mathbb{Z}$ . As an exercise, prove that  $\widehat{K^*} \simeq \mathcal{O}_K^* \times \widehat{\mathbb{Z}}$ ; recall that we know the group structure of  $\mathcal{O}_K^*$  in detail. This allows us to “find” all abelian extensions of  $K^*$ .

**18.1. The Herbrand Quotient.** The companion reading for this section is Neukirch Chapter IV Section 7. Let  $G$  be a cyclic group of order  $n$  generated by  $\sigma$ . Recall that

$$H^0(G, A) = A^G / \{Na = a\sigma(a) \cdots \sigma^{n-1}(a)\};$$

$$H^{-1}(G, A) = \{a \in A \mid Na = 1\} / \{\sigma(a)a^{-1} \mid a \in A\}.$$

**Proposition 18.5.** *If*

$$1 \longrightarrow A \longrightarrow B \longrightarrow C \longrightarrow 1$$

*is an exact sequence of  $G$ -modules, then we obtain an exact hexagon*

$$\begin{array}{ccccc}
 & & H^0(G, A) & \xrightarrow{f_1} & H^0(G, B) & & \\
 & \nearrow f_6 & & & & \searrow f_2 & \\
 H^{-1}(G, C) & & & & & & H^0(G, C) \\
 & \nwarrow f_5 & & & & \swarrow f_3 & \\
 & & H^{-1}(G, B) & \xleftarrow{f_4} & H^{-1}(G, A) & & 
 \end{array}$$

*Proof.* The maps  $f_1, f_2, f_4, f_5$  are induced by the maps  $A \rightarrow B \rightarrow C$ . For  $f_3$ , take  $c \in C^G$ , and let  $b$  be a lift of  $c$  to  $B$ . Then  $\sigma(b)b^{-1}$  has image 1 in  $C$ , so  $\sigma(b)b^{-1} \in A$ . Note  $N(\sigma(b)b^{-1}) = 1$ , so  $\sigma(b)b^{-1}$  is a norm 1 element of  $A$ , so  $f_3([c]) = [a]$ . It is not difficult to see that  $f_3$  is well-defined. For  $f_6$ , let  $c \in C$  with  $N(c) = 1$ . Lift  $c$  to  $b \in B$ . Then  $N(b) \in A$ . Let  $f_6([c]) = [N(b)]$ , and we can check that this is well-defined.

Checking exactness is straightforward; we show this (partially) at  $H^{-1}(G, A)$ . If  $a \in A$  with  $N(a) = 1$  and  $f_4([a]) = 0$ , then  $a = \sigma(b)b^{-1}$  for some  $b \in B$  (uses  $G$  is cyclic). Let  $c$  be the image of  $b$ , then  $f_3([c]) = [a]$ . □

**Definition 18.6.** The *Herbrand quotient* of  $A$  is

$$h(G, A) = \frac{|H^0(G, A)|}{|H^{-1}(G, A)|}$$

(if it is understood we may suppress the group from our notation and simply write  $h(A)$ ).

As an exercise, show that if

$$1 \longrightarrow A \longrightarrow B \longrightarrow C \longrightarrow 1$$

is exact, then  $h(B) = h(A)h(C)$  (Hint: this follows from the exact hexagon).

**Lemma 18.7.** *If  $A$  is finite, then  $h(A) = 1$ .*

*Proof.* This follows from the exact sequence

$$1 \longrightarrow A^G \longrightarrow A \longrightarrow \{\sigma(a)a^{-1} \mid a \in A\} \longrightarrow 1 ,$$

where the center map takes  $a \mapsto \sigma(a)a^{-1}$ , and the exact sequence

$$1 \longrightarrow \{a \mid N(a) = 1\} \longrightarrow A \longrightarrow NA \longrightarrow 1 .$$

The details are left to the reader. □

For a group  $G$  and an abelian group  $B$ , we have an induced  $G$ -module

$$A = \text{Ind}_G(B) = \prod_{\sigma \in G} \sigma B,$$

where the action of  $\sigma$  on  $B$  is purely formal. We can express elements as  $\sum_{\sigma} \sigma b_{\sigma}$  for  $b_{\sigma} \in B$ . For  $g \in G$ , we have

$$g \left( \sum_{\sigma} \sigma b_{\sigma} \right) = \sum_{\sigma} g \sigma b_{\sigma}.$$

**Proposition 18.8.** *Let  $G$  be a finite cyclic group. Then*

$$H^i(G, \text{Ind}_G(B)) = 0$$

for  $i \in \{0, -1\}$ .

**18.2. Proof of the Class Field Axiom.** The corresponding reading is Neukich Chapter V Section 1.

**Theorem 18.9** (Class Field Axiom for Local Fields). *For a cyclic extension  $L/K$  of local fields,*

$$\#H^i(\text{Gal}(L/K), L^*) = \begin{cases} [L : K] & \text{if } i = 0 \\ 1 & \text{if } i = -1. \end{cases}$$

*Proof.* We have that  $i = -1$  statement from Hilbert 90. Thus, we need to show  $h(L^*) = [L : K]$ . We use the exact sequence

$$1 \longrightarrow \mathcal{O}_L^* \longrightarrow L^* \xrightarrow{v} \mathbb{Z} \longrightarrow 1 ,$$

which tells us that  $h(L^*) = h(\mathbb{Z})h(\mathcal{O}_L^*)$  (note that  $\mathbb{Z}$  is a trivial  $G = \text{Gal}(L/K)$ -module), as long as each Herbrand quotient is well defined. As an exercise, show that  $h(\mathbb{Z}) = |G| = [L : K]$ . Thus, we need to show that  $h(\mathcal{O}_L^*) = 1$ . Choose a normal basis  $\{\sigma^i(\alpha)\}$  of  $L/K$  with  $\alpha \in \mathcal{O}_L$ . Let

$$M = \sum_{i=1}^{|G|} \sigma^i(\alpha) \mathcal{O}_K \subset \mathcal{O}_L.$$

As an exercise, show that  $M$  is open in  $\mathcal{O}_L$ , i.e.,  $\pi_K^N \mathcal{O}_L \subset M$  for some  $N \in \mathbb{N}$ . Moreover, the opens  $V^n = 1 + \pi_K^n M$  form a basis of open neighborhoods of 1 in  $\mathcal{O}_L^*$ . For  $n \geq N$ , the  $v^n$  are finite index subgroups of  $\mathcal{O}_L^*$ :

$$(\pi_K^n M)(\pi_K^n M) = \pi_K^{2n} M \cdot M \subset \pi_K^{2n} \mathcal{O}_L \subset \pi_K^{2n-N} M \subset \pi_K^n M$$



(can also check inverses). For  $n \geq N$ , we have an isomorphism

$$V^n/V^{n+1} \rightarrow M/\pi_K M = \bigoplus_{\sigma \in G} \mathcal{O}_K/\pi_K$$

by  $1 + \pi_K^n a \mapsto a$ . This  $M/\pi_K M$  is  $\text{Ind}_G(\mathcal{O}_K/\pi_K)$ , so  $H^i(G, V^n/V^{n+1}) = 0$  for  $n \geq N$ . To be continued...  $\square$

19. WEDNESDAY NOVEMBER 15

**19.1. Proof of the Class Field Axiom, continued.** Recall that our goal is to show that the Herbrand quotient  $h(\mathcal{O}_L^*) = 1$ . We have subgroups

$$\dots \subset V^{N+1} \subset V^N \subset \mathcal{O}_L^*$$

such that  $H^i(G, V^n/V^{n+1}) = 0$  for  $i \in \{0, -1\}$  and  $n \geq N$ . Next, we show that  $H^0(G, V^n) = 0$  for all  $n \geq N$ . Take  $a \in (V^n)^G$ ; we have  $a = (Nb_0)a_1$  for  $b_0 \in V^n$  and  $a_1 \in (V^{n+1})^G$ . Then we have  $a_1 = (Nb_1)a_2$  for  $b_1 \in V^{n+1}$  and  $a_2 \in (V^{n+2})^G$ , and so on, this process yields a sequence of  $b_i$ . Let

$$b = \prod_{i=0}^{\infty} b_i,$$

where the product converges because the  $V^n$ 's are a basis of open neighborhoods of 1. Moreover, we have  $a = Nb$ . So  $H^0(G, V^n) = 0$ . Similarly, for  $H^{-1}(G, V^n) = 0$ : given  $a \in V^n$  such that  $Na = 1$ , we get  $a = \sigma(b_0)b_0^{-1}a_1$  for  $b_0 \in V^n$ ,  $a_1 \in V^{n+1}$  with  $Na_1 = 1$ . Then  $a_1 = \sigma(b_1)b_1^{-1}a_2$  for  $b_1 \in V^{n+1}$  and  $a_2 \in V^{n+2}$  with  $Na_2 = 1$ . Continuing this process, we get  $a = \sigma(b)b^{-1}$  where  $b = \prod_{i=1}^{\infty} b_i$ . Hence,  $H^{-1}(G, V^n) = 0$ . We have an exact sequence

$$1 \longrightarrow V^n \longrightarrow \mathcal{O}_L^* \longrightarrow \mathcal{O}_L^*/V^n \longrightarrow 1,$$

where recall that  $\mathcal{O}_L^*/V^n$  is finite. Hence,  $h(\mathcal{O}_L^*) = h(V^n)h(\mathcal{O}_L^*/V^n) = 1 \cdot 1$ .

**19.2. Abstract Class Field Theory.** For abstract class field theory, we only need the following ingredients:

- (1) a field  $k$ , with associated group  $G = \text{Gal}(\bar{k}/k)$ ;
- (2)  $d : G \rightarrow \widehat{\mathbb{Z}}$  a surjective continuous homomorphism (for us, this was the action on residue fields) where we set  $f_{K/k} = [\widehat{\mathbb{Z}} : d(\text{Gal}(\bar{k}/k))]$ ;
- (3) a  $G$ -module  $A$ , with  $A_K = A^G$  (for us  $A = \bar{k}^*$  and  $A_K = K^*$ );
- (4)  $v : A_k \rightarrow \widehat{\mathbb{Z}}$  (for us, this was a valuation) such that  $\mathbb{Z} \subset v(A_k)$ ,  $v(A_k)/n \simeq \mathbb{Z}/n\mathbb{Z}$ , and  $v(N_{K/k}A_k) = f_{K/k}v(A_k)$ .

This allows us to define some familiar objects in the following way:  $\tilde{K}$  is the fixed field of  $\text{Gal}(\bar{k}/k) \cap \ker(d)$ ;  $\pi_K$  is any element of  $A_K$  with  $v(N_{K/k}\pi_K) = f_{K/k}$ ;  $U_K$  is the set of elements  $u \in A_K$  with  $v(u) = 0$  (this was our  $\mathcal{O}_K^*$ ).

**Theorem 19.1.** *If for all cyclic  $L/K$  (with  $L/K/k$  finite) one has*

$$|H^i(\text{Gal}(L/K), A_L)| = \begin{cases} [L : K] & \text{if } i = 0 \\ 1 & \text{if } i = -1, \end{cases}$$

*then, for all finite Galois  $L/K$ , we have an isomorphism*

$$\text{Gal}(L/K)^{ab} \rightarrow A_K/N_{L/K}A_L$$

given by  $L \mapsto N_{L/K}A_K$ . The isomorphism in the above gives a correspondence between finite abelian extensions and open subgroups of  $A_K$  in the norm topology.

**19.3. Back to the Local Class Field Theory.** For  $K$  a local field, recall that we have shown that

$$\mathrm{Gal}(K^{ab}/K) \simeq \widehat{K}^*.$$

Recall:  $U_K^{(n)} = 1 + \pi_K^n \mathcal{O}_K$  for  $n \geq 1$  and that  $U_K^{(0)} = \mathcal{O}_K^*$ .

**Definition 19.2.** Let  $L/K$  be a finite abelian extension of local fields and  $n$  the smallest non-negative number such that  $U_K^{(n)} \subset N_{L/K}L^*$ . Then  $(\pi_K)^n$  is the (class field theory) *conductor* of  $L/K$ .

**Proposition 19.3.** A finite abelian extension  $L/K$  of local fields is unramified if and only if the conductor is 1.

*Proof.* If  $L/K$  is unramified, Lemma 15.2 (which is implied by the Class Field Axiom) tells us that  $H^i(\mathrm{Gal}(L/K), \mathcal{O}_L^*) = 1$  for  $i \in \{0, -1\}$ . Thus,  $\mathcal{O}_K^* \subset N_{L/K}\mathcal{O}_L^*$  implies the conductor is 1. Conversely, if the conductor is 1, then we have  $\mathcal{O}_K^* \subset N_{L/K}L^*$ , and  $\pi_K^m \in N_{L/K}L^*$  for  $m = [K^* : N_{L/K}L^*]$ . If  $M/K$  is the unramified extension of degree  $m$ , then  $N_{M/K}(M^*) = \langle \pi_K^m \rangle \times \mathcal{O}_K^* \subset N_{L/K}L^*$ . This implies  $M \supset L$ , so  $L/K$  is unramified.  $\square$

**Corollary 19.4.** In the reciprocity map,  $\mathrm{Gal}(L/K) \simeq K^*/N_{L/K}K^*$  or  $\mathrm{Gal}(K^{ab}/K) \simeq \widehat{K}^*$ , where the inertia group  $I$  corresponds to  $\mathcal{O}_K^*$ .

We have a filtration

$$G_{i+1} \subset G_i \subset \cdots \subset I$$

of higher ramification groups and a filtration

$$U^{(n)} \subset U^{(n-1)} \subset \cdots \subset \mathcal{O}_K^*$$

of units. Given the above proposition, it is natural to ask whether they are the same. The answer is yes, but only after renumbering. The reading for this section is Neukirch Chapter V Section 6. Recall that

$$G_i = \{\sigma \in \mathrm{Gal}(L/K) \mid v_L(\sigma(a) - a) \geq i + 1 \text{ for all } a \in \mathcal{O}_L\}$$

and that  $G_{-1} = \mathrm{Gal}(L/K)$  and  $G_0 = I$ . We have a strictly increasing function  $\eta_{L/K} : \mathbb{R}_{\geq 0} \rightarrow \mathbb{R}_{\geq 0}$  given by

$$\eta_{L/K}(s) = \int_0^s \frac{dx}{[G_0 : G_{\lceil x \rceil}]} = \frac{1}{[G_0 : G_1]} + \frac{1}{[G_0 : G_2]} + \cdots + \frac{s - \lfloor s \rfloor}{[G_0 : G_{\lfloor s \rfloor + 1}]}.$$

Note that  $y = \eta_{L/K}(s)$  is piecewise linear. We define

$$G^i(L/K) = G_{\lceil \eta_{L/K}^{-1}(i) \rceil}(L/K).$$

**Theorem 19.5.** Let  $L/K$  be a finite abelian extension of local fields. Then the reciprocity map gives an isomorphism between  $r_{L/K} : \mathrm{Gal}(L/K) \rightarrow K^*/N_{L/K}L^*$  under which  $G^n(L/K)$  is sent to  $U_K^{(n)}$ .

**Remark 19.6.** Why this numbering? This has the correct functoriality—recall that comparing  $G_i$  in  $L/K$  versus  $L'/K$  involved a complicated formula.

**Proposition 19.7.** The group of norms of the extension  $\mathbb{Q}_p(\mu_{p^n})/\mathbb{Q}_p$  is the group  $\langle p \rangle \times U_{\mathbb{Q}_p}^{(n)}$ .

*Proof for  $p$  odd.* Let  $K = \mathbb{Q}_p$  and  $L = \mathbb{Q}_p(\mu_{p^n})$ . We have  $L/K$  is totally ramified of degree  $p^{n-1}(p-1)$  and if  $\zeta$  is a primitive  $p^n$ th root of unity,  $1 - \zeta = \pi_L$ , and  $N_{L/K}(\pi_L) = p$ . Since  $p$  is odd, we have isomorphisms

$$\exp : (\pi_K)^v \rightarrow U_K^{(v)}$$

for  $v \geq 1$ ,  $(\pi_K)^v \rightarrow (\pi_K)^{v+s-1}$  given by  $a \mapsto p^{s-1}(p-1)a$ , and  $U_K^{(v)} \rightarrow U_K^{(v+s-1)}$  given by  $u \mapsto u^{p^{s-1}(p-1)}$  (here we are using that  $\pi_K = p$ ). Because  $\exp$  is an isomorphism, we have that  $\exp : (\pi_K)^{v+s-1} \rightarrow U_K^{(v+s-1)}$  is an isomorphism. Therefore,  $(U_K^{(1)})^{p^{n-1}(p-1)} = U_K^{(n)}$ , and it follows that  $U_K^{(n)} \subset N_{L/K}L^*$  because any  $[L : K]$  power is a norm (of an element of  $K$ ). Also  $p \in N_{L/K}L^*$ , so  $\langle p \rangle \times U_K^{(n)} \subset N_{L/K}L^*$  and both groups have index  $p^{n-1}(p-1)$  in  $K^*$  (recall that we worked out the group structure of  $U^{(n)}/U^{(n+1)}$ ; in particular, we know its size).  $\square$

20. MONDAY NOVEMBER 20

**20.1. Local Kronecker–Weber.** The companion reading for this section is Neukirch Chapter V Section 1.

**Theorem 20.1** (Local Kronecker–Weber). *Every finite abelian extension  $L/\mathbb{Q}_p$  is contained in a field  $\mathbb{Q}_p(\zeta)$ , where  $\zeta$  is a root of unity.*

*Proof.* For some  $k, n$ , we have  $\langle p^k \rangle \times U_{\mathbb{Q}_p}^{(n)} \subset N_{L/K}L^*$ . Since  $\langle p^k \rangle \times U_{\mathbb{Q}_p}^{(n)}$  is open and of finite index, it has class field  $M$  with  $L \subset M$ . Let  $S$  denote  $\langle p^k \rangle \times U_{\mathbb{Q}_p}^{(n)}$ , let  $S_1 = \langle p^k \rangle \times U_{\mathbb{Q}_p}$ , and let  $S_2 = \langle p \rangle \times U_{\mathbb{Q}_p}^{(n)}$ . Note that  $S_1$  has class field  $M_1 = \mathbb{Q}_p(\mu_{p^{k-1}})$ —the unramified extension of degree  $k$ —and that  $S_2$  has class field  $M_2 = \mathbb{Q}_p(\mu_{p^n})$ . We have  $S = S_1 \cap S_2$ . Now, the diagram

$$\begin{array}{ccc} \text{Gal}(M/K) & \longleftrightarrow & K^*/S_1 \cap S_2 \\ \downarrow & & \downarrow \\ \text{Gal}(M_1/K) \times \text{Gal}(M_2/K) & \longleftrightarrow & K^*/S_1 \times K^*/S_2 \end{array}$$

is commutative by functoriality, where the left injection implies that  $M \subset M_1M_2 = \mathbb{Q}_p(\mu_{(p^{k-1})p^n})$ .  $\square$

**Theorem 20.2** (Kronecker–Weber). *Every finite abelian extension  $L/\mathbb{Q}$  is contained in a field  $\mathbb{Q}(\zeta)$  for a root of unity  $\zeta$ .*

*Proof.* Let  $L/\mathbb{Q}$  be finite and abelian, and let  $S$  be the set of primes ramifies at  $L$ . Also let  $L_p$  be a completion of  $L$  at a prime of  $L$  dividing  $p$ . Then  $L_p/\mathbb{Q}_p$  is abelian (recall that  $\text{Gal}(L_p/\mathbb{Q}_p) \hookrightarrow \text{Gal}(L/\mathbb{Q})$ ), so  $L_p \subset \mathbb{Q}_p(\mu_{n_p})$  for some  $n_p$ . Let  $e_p = v_p(n_p)$ , and let  $n = \prod_{p \in S} p^{e_p}$ . We will show  $L = \mathbb{Q}(\mu_n)$ . Let  $M = L(\mu_n)$ , and note that  $M/\mathbb{Q}$  is abelian. If  $p$  ramifies in  $M/\mathbb{Q}$ , then  $p \in S$ . Let  $M_p$  be a completion at a prime of  $M$  dividing the prime we used for  $L_p$ . We have that

$$M_p = L_p(\mu_n) = \mathbb{Q}_p(\mu_p^{e_p} n') = \mathbb{Q}_p(\mu_p^{e_p})\mathbb{Q}_p(\mu_{n'}),$$

where  $(n', p) = 1$ . Here,  $\mathbb{Q}_p(\mu_{n'})/\mathbb{Q}_p$  is the maximal unramified subextension, so the inertia group  $I_p$  of  $M_p/\mathbb{Q}_p$  is isomorphic to  $\text{Gal}(\mathbb{Q}_p(\mu_{p^{e_p}})/\mathbb{Q})$  and hence has order  $\varphi(p^{e_p})$ . Let  $I$  be the subgroup of  $\text{Gal}(M/\mathbb{Q})$  generated by all  $I_p$  for  $p \in S$ . The fixed field of  $I$  is unramified over  $\mathbb{Q}$ , implying that  $\mathbb{Q}$  is the fixed field of  $I$  (since  $\mathbb{Q}$  has no nontrivial unramified extensions). Also

$$|\text{Gal}(M/\mathbb{Q})| = |I| \leq \prod_{p \in S} |I_p| = \prod_{p \in S} \varphi(p^{e_p}) = \varphi(n) = [\mathbb{Q}(\mu_n) : \mathbb{Q}].$$

So  $[M : \mathbb{Q}] \leq [\mathbb{Q}(\mu_n) : \mathbb{Q}]$ , so  $M = \mathbb{Q}(\mu_n)$ , and  $L \subset \mathbb{Q}(\mu_n)$ .  $\square$

**Remark 20.3.** Note that the above result does not hold for more general number fields.

**20.2. The Hilbert Symbol.** The corresponding section in Neukirch is Chapter V Section 3. Let  $K$  be a local field with  $\mu_n \subset K$  such that  $\text{char}(K) \nmid n$ . By Kummer theory, we have that  $L = K(\sqrt[n]{K^*})$  is the maximal abelian extension of  $K$ . By Class Field Theory, we have  $\text{Gal}(L/K) \simeq K^*/K^n$ , and Kummer theory implies that  $\text{Hom}(\text{Gal}(L/K), \mu_n) \simeq K^*/K^n$ . Thus, we have a tautological (perfect) pairing

$$\text{Gal}(L/K) \otimes \text{Hom}(\text{Gal}(L/K), \mu_n) \rightarrow \mu_n.$$

This pairing, which may be written as a map  $K^*/K^n \otimes K^*/K^n \rightarrow \mu_n$  (via first the reciprocity map and then the Kummer pairing), takes

$$a \otimes b \mapsto \left( \frac{a, b}{\wp} \right),$$

where  $\wp$  is a prime of  $K$ . The expression on the right-hand side of the above is called the *Hilbert symbol*.

**Proposition 20.4.** *The Hilbert symbol has the following properties:*

- (1)  $\left( \frac{aa', b}{\wp} \right) = \left( \frac{a, b}{\wp} \right) \left( \frac{a', b}{\wp} \right)$
- (2)  $\left( \frac{a, b}{\wp} \right) = 1$  if and only if  $a$  is a norm from  $K(\sqrt[\wp]{b})/K$
- (3)  $\left( \frac{a, b}{\wp} \right) = \left( \frac{b, a}{\wp} \right)^{-1}$
- (4)  $\left( \frac{a, 1-a}{\wp} \right) = 1$  and  $\left( \frac{a, -a}{\wp} \right) = 1$ .

*Proof.* (2): Suppose  $[a] = r_{L/K}(\sigma)$  for  $\sigma \in \text{Gal}(L/K)$ , and then

$$\left( \frac{a, b}{\wp} \right) = \frac{\sigma(\sqrt[\wp]{b})}{\sqrt[\wp]{b}}.$$

Also  $[a] = r_{K(\sqrt[\wp]{b})/K}(\bar{\sigma})$ , where  $\bar{\sigma}$  is the image of  $\sigma$  in  $\text{Gal}(\sqrt[\wp]{b}/K)$ . Here,  $\bar{\sigma} = 1$  if and only if  $a \in N_{K(\sqrt[\wp]{b})/K} K(\sqrt[\wp]{b})^*$ . So

$$\left( \frac{a, b}{\wp} \right) = \frac{\bar{\sigma}(\sqrt[\wp]{b})}{\sqrt[\wp]{b}} = 1$$

if and only if  $a$  is a norm from  $K(\sqrt[\wp]{b})$ .

(4): For  $b \in K^*$  and  $x \in K$  such that  $x^n - b \neq 0$ , then  $x^n - b = \prod_{i=0}^{n-1} (x - \zeta^i \beta)$  for  $\beta^n = b$  and  $\zeta$  a primitive  $n$ th root of unity. Let  $d$  be the greatest divisor of  $n$  such that  $x^d = b$  has a solution in  $K$ , and let  $n = dm$ . Then  $K(\beta)/K$  is cyclic of degree  $m$  and conjugates of  $x - \zeta^i \beta$  are  $x - \zeta^j \beta$  such that  $j \equiv i \pmod{d}$ . So

$$x^n - b = \prod_{i=0}^{d-1} N_{K(\beta)/K}(x - \zeta^i \beta)$$

is a norm from  $K(\sqrt[\wp]{b})^*$ . Letting  $x = 1$ ,  $b = 1 - a$  and  $x = 0$ ,  $b = -a$  implies (4).

(3): We have

$$\left( \frac{a, b}{\wp} \right) \left( \frac{b, a}{\wp} \right) = \left( \frac{a, -a}{\wp} \right) \left( \frac{a, b}{\wp} \right) \left( \frac{b, a}{\wp} \right) \left( \frac{b, -b}{\wp} \right) = \left( \frac{a, -ab}{\wp} \right) \left( \frac{b, -ab}{\wp} \right) = \left( \frac{ab, -ab}{\wp} \right) = 1,$$

as desired. □

When the residue characteristic of  $K$  does not divide  $d$ , it turns out that  $\left(\frac{\pi_K u}{\wp}\right)$  does not depend on the choice of  $\pi_K$  for  $u \in \mathcal{O}_K^*$ . We define the *Legendre symbol* to be

$$\left(\frac{u}{\wp}\right) = \left(\frac{\pi_K u}{\wp}\right) \equiv u^{(q-1)/n} \pmod{\wp},$$

where  $q = |\mathcal{O}_K/\wp|$ . The  $n$ th roots of unity are distinct in  $\mathcal{O}_K/\wp$  (since  $x^n - 1$  is separable), so  $n|(q-1)$ , and  $u^{(q-1)/n} \pmod{\wp}$  determines  $\left(\frac{u}{\wp}\right)$ . Also,  $\left(\frac{u}{\wp}\right) = 1$  if and only if  $u$  is an  $n$ th power mod  $\wp$ . In a number field  $K$ , for  $a, b \in \mathcal{O}_K \setminus \{0\}$  with  $(a, n) = (b, n) = (a, b) = 1$ , we define

$$\left(\frac{a}{b}\right) = \prod_{\substack{\wp|n \\ \text{prime of } K}} \left(\frac{a}{\wp}\right)^{v_\wp(b)}.$$

**Theorem 20.5** (General Reciprocity Law for  $n$ th powers). *Let  $K$  be a number field with  $a, b \in \mathcal{O}_K \setminus \{0\}$  such that  $(a, n) = (b, n) = (a, b) = 1$ . Then*

$$\left(\frac{a}{b}\right) \left(\frac{b}{a}\right)^{-1} = \prod_{\wp|n\infty} \left(\frac{a, b}{\wp}\right).$$

## 21. MONDAY NOVEMBER 27

**21.1. Artin Conductors.** See Neukich Chapter VII Section 2. Let  $L/K$  be a finite Galois extension of local fields with Galois group  $G = \text{Gal}(L/K)$ . Let  $\chi$  be the character of a finite-dimensional  $\mathbb{C}$ -representation of  $G$  (i.e., a  $\mathbb{C}$ -vector space  $V$  and homomorphism  $\rho : G \rightarrow GL(V)$ ). The *Artin conductor* of  $(L/K, \chi)$  is  $(\pi_K)^{f(\chi)}$ , where

$$f_{L/K}(\chi) = f(\chi) = \sum_{i \geq 0} \frac{|G_i|}{|G_0|} \text{codim}(V^{G_i}).$$

Here  $G_i = \{\sigma \in G \mid v_L(\sigma x - x) \geq i + 1\}$  and for  $\mathcal{O}_L = \mathcal{O}_K[x]$ . Artin conductors arise in many places, e.g., the functional equation for Artin  $L$ -functions (generalize  $\zeta(s)$ ). Recall from basic representation theory that

$$\dim(V^{G_i}) = \frac{1}{|G_i|} \sum_{g \in G_i} \chi(g),$$

so

$$\text{codim}(V^{G_i}) = \chi(1) - \frac{1}{|G_i|} \sum_{g \in G_i} \chi(g).$$

Hence, we may write

$$\begin{aligned} f(\chi) &= \sum_{i \geq 0} \left( \frac{|G_i|}{|G_0|} \chi(1) - \frac{1}{|G_0|} \sum_{g \in G_i} \chi(g) \right) \\ &= \frac{1}{|G_0|} \sum_{i \geq 0} \sum_{g \in G_i} \chi(1) - \chi(g) \\ &= \frac{1}{|G_0|} \sum_{g \in G} (\chi(1) - \chi(g)) \#\{i \geq 0 \mid g \in G_i\}. \end{aligned}$$

The term  $\#\{i \geq 0 \mid g \in G_i\}$  is a class function, and thus the above looks like an inner product of characters. To realize it as such, let

$$i_G(g) = \#\{i \geq 0 \mid g \in G_i\} = v_L(g(x) - x),$$

and define a class function

$$a_G(g) = \begin{cases} -\frac{|G|}{|G_0|} i_G(g) & \text{if } g \neq 1; \\ \frac{|G|}{|G_0|} \sum_{g \neq 1} i_G(g) & \text{if } g = 1. \end{cases}$$

We see immediately that

$$\langle 1, a_G \rangle = \frac{1}{|G|} \sum_{g \in G} a_G(g) = 0.$$

For  $\chi$ , we have

$$\langle \chi, a_G \rangle = \frac{1}{|G|} \sum_{g \in G} a_G(g) \chi(g) = \frac{1}{|G_0|} \left( \sum_{g \neq 1} \chi(1) i_G(g) - \sum_{g \neq 1} \chi(g) i_G(g) \right) = f(\chi).$$

If  $\chi$  is irreducible,  $f(\chi)$  is the number of copies of  $\chi$  in  $a_G$ .

For  $L/L'/K$  with  $G = \text{Gal}(L/K)$  and  $H = \text{Gal}(L/L')$  a normal subgroup, if  $\pi$  denotes the projection  $G \rightarrow G/H$ , then

$$i_{G/H}(\bar{g}) = \frac{1}{|G_0 \cap H|} \sum_{g \in \pi^{-1}(\bar{g})} i_G(g).$$

Hence,

$$a_{G/H}(\bar{g}) = \frac{1}{|H|} \sum_{g \in \pi^{-1}(\bar{g})} a_G(g).$$

Let  $W$  be the representation of  $a_G$ , then  $W' = \mathbb{C}[G/H] \otimes_{\mathbb{C}[G]} W$  is the representation of  $a_{G/H}$ . For  $\phi$  a character on  $G/H$  (and hence a character on  $G$  by pullback), then

$$\langle \phi, a_{G/H} \rangle_{G/H} = \langle \phi, a_G \rangle_G$$

(this follows from Frobenius reciprocity). It follows that  $f_{L'/K}(\phi) = f_{L/K}(\phi)$ .

**Remark 21.1.** The above lets us see these Artin conductors are really about representations of  $G_K = \text{Gal}(\bar{K}/K)$  on  $V$ .

**Theorem 21.2.** *With notation as above, we have  $f(\chi) \in \mathbb{Z}_{\geq 0}$ . Hence,  $a_G$  is the character of a representation.*

*Proof.* This follows from the Hasse–Arf Theorem, which tells us where the jumps in the upper-numbering are.  $\square$

Recall that for  $L/K$  abelian, the class-field-theoretic conductor is  $(\pi_K)^n$  where  $n$  is the smallest integer such that  $U^{(n)} \subset N_{L/K} L^*$ . By reciprocity, this is equivalent to the smallest  $n$  such that  $G^n(L/K) = 1$  and  $G^i(L/K) = G_j(L/K)$ , where  $i = \eta_{L/K}(j)$  for

$$\eta_{L/K}(s) = \sum_{i=1}^{\lfloor s \rfloor} \frac{|G_i|}{|G_0|} + \frac{(s - \lfloor s \rfloor) |G_{\lfloor s \rfloor + 1}|}{|G_0|}.$$

**Proposition 21.3.** *For  $\chi$  a character of degree 1 (i.e.,  $\dim(V) = 1$ ) and  $j$  the largest integer such that  $\chi|_{G_j}$  is nontrivial, then  $f(\chi) = \eta_{L/K}(j) + 1$ .*

*Proof.* If  $\chi|_{G_{j+1}}$  is trivial and

$$f(\chi) = \sum_{k=0}^j \frac{|G_k|}{|G_0|},$$

since  $V$  1-dimensional implies that

$$\text{codim}(V^{G_k}) = \begin{cases} 0 & \text{if } G_k \text{ acts on } V \text{ trivially;} \\ 1 & \text{otherwise.} \end{cases}$$

The  $k = 0$  term gives the additional 1. □

**Proposition 21.4.** *For  $\chi$  a character of degree 1, let  $L_\chi$  be the fixed field of  $\ker(\chi)$  (i.e.,  $\ker \rho : G \rightarrow GL(V)$ ). This is an abelian extension, and the class-field-theoretic conductor of  $L_\chi/K$  is equal to  $(\pi_K)^{f(\chi)}$ .*

*Proof.* We have that  $f(\chi) = \eta_{L/K}(j) + 1$ , where  $j$  is the largest integer such that  $G_j(L/K) \not\subset \text{Gal}(L/L_\chi) = \ker(\chi)$ . The class-field-theoretic conductor of  $L_\chi/K$  is  $(\pi_K)^i$  for the minimal integer  $i$  such that  $G^i(L_\chi/K) = 1$ . Hence,  $G^i(L_\chi/K) = G^i(L/K) \ker(\chi) / \ker(\chi)$ , so  $i$  is the minimal integer such that  $G^i(L/K) \subset \ker(\chi)$ . So  $G^{\eta_{L/K}(j)}(L/K) = G_j(L/K) \not\subset \ker(\chi)$ . However,  $G^{\eta_{L/K}(j)+1}(L/K) = G_m(L/K) \subset \ker(\chi)$ , since  $m > j$ . Using that  $f(\chi) \in \mathbb{N}$ , we can conclude the proposition. □

For a finite Galois extension  $L/K$  of global fields,

$$\mathfrak{f}(\chi) = \prod_{\mathfrak{p} \text{ prime of } L} \mathfrak{p}^{f_{L_\mathfrak{p}/K_\mathfrak{p}}(\chi)},$$

where  $\mathfrak{p} = \mathfrak{p} \cap \mathcal{O}_K$ . Note that  $f_{L_\mathfrak{p}/K_\mathfrak{p}} = 0$  if  $L_\mathfrak{p}/K_\mathfrak{p}$  is unramified (recall that then  $G_0$  is the inertia group, so  $G_0 = 1$  implies that  $\text{codim}(V^{G_i}) = 0$  for all  $i \geq 0$ ).

**Remark 21.5.** Note that  $f(\chi + \chi') = f(\chi) + f(\chi')$ , since  $\text{codim}((V \oplus V')^{G_i}) = \text{codim}(V^{G_i}) + \text{codim}((V')^{G_i})$ .

**Proposition 21.6.** *If  $G = \text{Gal}(L/K)$ , and if  $H$  is a subgroup of  $G$ , then*

$$\text{Disc}_{K^H/K} = \mathfrak{f}(\text{Ind}_H^G \mathbb{C}).$$

*In particular, taking  $H$  to be the trivial group, we see that*

$$\text{Disc}_{L/K} = \mathfrak{f}(\chi_{\text{reg}}),$$

*where  $\chi_{\text{reg}}$  denotes the character of the regular representation of  $G$ .*

*Proof.* Recall, locally, that

$$v_{K^H}(\mathcal{D}_{K^H/K}) = \frac{1}{|G_0 \cap H|} \sum_{s \notin H} i_G(s).$$

The proposition follows from the above combined with the fact that  $\text{Disc} = \mathbb{N}\mathcal{D}$  and that  $\mathcal{D}_{L/K} = \mathcal{D}_{L/K^H} \mathcal{D}_{K^H/K}$ . □

**Remark 21.7.** The above proposition is very useful for computing discriminants when you get  $L/K$  from some Galois representation.

## 22. WEDNESDAY NOVEMBER 29

Let  $K$  be a local field with separable closure  $\overline{K}$ . Let  $G_K = \text{Gal}(\overline{K}/K)$ . Let  $K^{ab}$  be the composite of all abelian extensions, and recall that  $\text{Gal}(K^{ab}/K) = \text{Gal}(\overline{K}/K)^{ab}$ . We also let  $K^{un}$  be the composite of all unramified extensions and  $K^t$  the composite of all tamely ramified and unramified extensions. Note that  $\text{Gal}(K^{un}/K) \simeq \widehat{\mathbb{Z}}$ . We let  $G_K^t$  denote  $\text{Gal}(K^t/K)$ .

Now, recall that we showed a finite tamely ramified extension  $L/K$  has cyclic inertia group  $T(L/K)$  (for any  $L/K$ , we have  $G_0/G_1 \hookrightarrow (\mathcal{O}_L/\pi_L)^*$  by  $\sigma \mapsto \sigma(\pi_L)/\pi_L$ ;  $L$  is tamely ramified if and only if  $G_1 = 1$ ).

**Lemma 22.1.** *With notation as above,  $\text{Gal}(K^t/K)$  has an element  $\tau$  which generates the inertia group in every finite quotient.*

*Proof.* We have

$$\text{Gal}(K^t/K) = \varprojlim_{L/K \text{ tame}} \text{Gal}(L/K).$$

Consider

$$\varprojlim_{L/K \text{ tame}} \{\text{generators of inertia in } \text{Gal}(L/K)\}.$$

This is an inverse system of nonempty finite sets, so the inverse limit is nonempty.  $\square$

We have the following exact sequence

$$1 \longrightarrow \text{Gal}(K^t/K^{un}) = \overline{\langle \tau \rangle} \longrightarrow \text{Gal}(K^t/K) \longrightarrow \text{Gal}(K^{un}/K) \simeq \widehat{\mathbb{Z}} \longrightarrow 1.$$

Note that  $\langle \tau \rangle$  has to be some quotient of  $\widehat{\mathbb{Z}} = \prod_{\ell} \mathbb{Z}_{\ell}$ . Let  $p$  be the characteristic of the residue field.

**Lemma 22.2.** *With notation as above,  $\langle \tau \rangle$  has no finite quotients of order divisible by  $p$ .*

*Proof.* Let  $K^t/L/K^{un}$  with  $L/K^{un}$  finite. Then  $L = K^{un}(\alpha)$ , and the coefficients of  $\alpha$ 's minimal polynomial only involve finitely many elements of  $K^{un}$ ; let these elements be contained in a finite extension of  $K$ , say  $K'$ . Then  $\text{Gal}(L/K^{un}) \hookrightarrow \text{Gal}(K'(\alpha)/K)$ , and its image fixes the maximal unramified subextension of  $K'(\alpha)/K$ . In other words, its image lands in the inertia group which is of order prime to  $p$  since  $K'(\alpha) \subset K^t$ .  $\square$


So  $\langle \tau \rangle$  is a quotient of  $\widehat{\mathbb{Z}}' = \prod_{\ell \neq p} \mathbb{Z}_{\ell} = \varprojlim_{p \nmid n} \mathbb{Z}/n\mathbb{Z}$ .

**Proposition 22.3.** *The group  $\langle \tau \rangle$  has a quotient of order  $m$  for all  $m$  in with  $p \nmid m$ , and hence is  $\widehat{\mathbb{Z}}'$ .*

*Proof.* For  $m$  with  $p \nmid m$ , we have  $K^{un}(\sqrt[m]{\pi_K})/K^{un}$ . This extension has order  $m$  by Kummer Theory, since  $\pi_K$  has order  $m$  in  $(K^{un})^*/((K^{un})^*)^m$ . Also,  $K^{un}(\sqrt[m]{\pi_K}) \subset K^t$ , since  $K(\sqrt[m]{\pi_K}, \mu_m)/K(\mu_m)$  is tame, since it is totally ramified of degree  $m$ .  $\square$

We have the following exact sequence

$$1 \longrightarrow \widehat{\mathbb{Z}}' \longrightarrow \text{Gal}(K^t/K) \longrightarrow \widehat{\mathbb{Z}} \longrightarrow 1,$$

$\nwarrow$  

and the exact sequence splits, because  $\widehat{\mathbb{Z}}$  is a “free profinite group.” We take any lift  $F$  of 1, and  $F^{\widehat{\mathbb{Z}}}$  are all distinct and the splitting takes  $a \in \widehat{\mathbb{Z}}$  to  $F^a$ . So  $G_K^t = \widehat{\mathbb{Z}}' \rtimes \widehat{\mathbb{Z}}$ . Now how does  $\widehat{\mathbb{Z}}$  act on



$\widehat{\mathbb{Z}}'$ ? For  $p \nmid m$ , if  $d$  is the order of  $q \bmod m$ , then  $m \mid (q^d - 1)$  and  $\mu_m \subset K_d$ , the degree  $d$  unramified extension of  $K$ . We have  $K_d(\sqrt[q]{\pi_K})/K$ . The elements  $\tau, F \in \text{Gal}(K^t/K)$  act in the following way:

$$\begin{aligned}\tau(\sqrt[q]{\pi_K}) &= \zeta \sqrt[q]{\pi_K}, \\ \tau(\zeta) &= \zeta, \\ F(\sqrt[q]{\pi_K}) &= \zeta^a \sqrt[q]{\pi_K}, \\ F(\zeta) &= \zeta^q\end{aligned}$$

where  $\zeta$  is a primitive  $m$ th root of unity, where  $a$  is some integer (we don't necessarily know what  $a$  is because the splitting is noncanonical), and where  $q = |O_K/\pi_K|$ . So  $F^{-1}(\zeta) = \zeta^{q^{-1}}$  and  $F^{-1}(\sqrt[q]{\pi_K}) = \zeta^{-aq^{-1}} \sqrt[q]{\pi_K}$ . Hence,

$$F\tau F^{-1}(\sqrt[q]{\pi_K}) = F\tau(\zeta^{-aq^{-1}} \sqrt[q]{\pi_K}) = F(\zeta^{-aq^{-1}+1} \sqrt[q]{\pi_K}) = \zeta^{-a+q+a} \sqrt[q]{\pi_K},$$

and  $F\tau F^{-1}(\zeta) = \zeta$ , implying that  $F\tau F^{-1} = \tau^q$  in  $\text{Gal}(K_d(\sqrt[q]{\pi_K})/K)$ . This is true for all  $d$  and  $m$ , and these fields generate  $K^t$ .

Therefore, we may conclude that  $\text{Gal}(K^t/K)$  is the profinite group generated by  $F, \tau$  such that

- (1)  $\tau$  has order prime to  $p$ ;
- (2)  $F\tau F^{-1} = \tau^q$ .

Concretely, we have

$$\text{Gal}(K^t/K) = \varprojlim_{\substack{G, F, \tau; |G| < \infty; \\ G = \langle F, \tau \rangle \\ F\tau F^{-1} = \tau^q; p \nmid \text{ord}(\tau)}} G,$$

where the maps  $G \rightarrow G'$  in the inverse system must take  $F \mapsto F'$  and  $\tau \mapsto \tau'$ .

**Remark 22.4.** Note that  $\widehat{\mathbb{Z}} = \varprojlim_{n \neq 3} \mathbb{Z}/n\mathbb{Z}$ , but these are all the finite quotients of  $G_K^t$ .

In fact,  $\text{Gal}(\overline{K}/K)$  is known, but finding this is much more difficult. For the statements, we refer the reader to Chapter VII Section 5 of *Cohomology of Number Fields* by Neukirch, Schmidt, and Wingberg, which, despite being thicker and more densely written than *Algebraic Number Fields*, does not contain the proofs.

**Theorem 22.5** (Koch). *Let  $K$  be a local field of characteristic  $p$  with finite residue field  $\mathbb{F}_q$ . We have*

$$\text{Gal}(\overline{K}/K) = \mathcal{F}_{G_K^t \mathbb{N}} \rtimes G_K^t.$$

The group  $\mathcal{F}_{G_K^t \mathbb{N}}$  is the free pro- $p$  group on the generators  $\sigma x_i$ , where  $\sigma \in G_K^t, i \in \mathbb{N}$ . The action is given by  $\sigma'(\sigma x_i) = (\sigma' \sigma) x_i$ , so

$$\text{Gal}(\overline{K}/K) = \varprojlim_{\substack{G \text{ a finite } p\text{-group} \\ (G, x_1, \dots) \\ x_i \in G \\ \text{a } G_K^t \text{ action on } G}} G \rtimes G_K^t,$$

where the maps  $G \rightarrow G'$  in the inverse system take  $x_i \mapsto x'_i$  and respect the  $G_K^t$  action.

Comparing this to the abelian case, we see that  $\text{Gal}(\overline{K}/K)^{ab} = (\mathcal{F}_{G_K^t \mathbb{N}})_{G_K^t}^{ab} \times (G_K^t)^{ab}$ , where  $(\mathcal{F}_{G_K^t \mathbb{N}})_{G_K^t}^{ab}$  is the maximal quotient where  $G_K^t$  acts trivially (i.e.,  $[x_i] = [\sigma x_i]$ ). We have that  $(\mathcal{F}_{G_K^t \mathbb{N}})_{G_K^t}^{ab} = \mathbb{Z}_p^{\mathbb{N}}$  and  $(G_K^t)^{ab} = \mathbb{Z}/(q-1)\mathbb{Z} \times \widehat{\mathbb{Z}}$ . By Class Field Theory, we have  $\widehat{K}^* = \mathbb{Z}_p^{\mathbb{N}} \times \mathbb{Z}/(q-1)\mathbb{Z} \times \widehat{\mathbb{Z}}$ .

**Remark 22.6.** We can have infinitely many  $G$ -extensions of a characteristic  $p$  local field for  $G$  finite when  $p|G$ .

**Theorem 22.7** (Jannsen-Wingberg). *Let  $K$  be a characteristic 0 local field of odd residue characteristic (characteristic 2 is much harder) and  $N = [K : \mathbb{Q}_p]$  even (the odd case is slightly more complicated). Then  $\text{Gal}(\overline{K}/K)$  is a profinite group generated by  $F, \tau, x_0, \dots, x_N$  such that*

- (1) *the closed normal subgroup generated by the  $x_0, \dots, x_N$  is pro- $p$*
- (2)  *$F\tau F^{-1} = \tau^q$  (where  $q = |\mathcal{O}_K/\pi_K|$ )*
- (3) *there is a relation  $Fx_0 F^{-1} = (x_0 \cdots) \cdots$ .*

## 23. MONDAY DECEMBER 4

### 23.1. Course Review.

23.1.1. *Discrete Valuation Rings.* Some examples of discrete valuation rings are valuations on global/local fields, e.g.,  $v_\varphi(\alpha) = \#\{\varphi \text{ in the factorization of } (\alpha)\}$ . Discrete valuation rings have uniformizers  $\pi$ , i.e., elements  $\pi$  with  $v(\pi) = 1$ . The ideals of a discrete valuation ring are of the form  $(\pi^n)$  for a uniformizer  $\pi$ , and the units are  $\{\alpha \mid v(\alpha) = 0\}$ . There is one maximal ideal  $(\pi)$  (i.e., the ring is local).

23.1.2. *Dedekind Domains.* Recall that a Dedekind domain is an integrally closed Noetherian ring with Krull dimension 1. Some examples include

- (1)  $\mathcal{O}_K$  for  $K$  a number field
- (2) the valuation ring of a local field
- (3) a discrete valuation ring
- (4)  $\mathbb{F}_q[t]$ .

The most important property of Dedekind domains is the unique factorization of ideals into products of prime ideals.

23.1.3. *Extensions of Dedekind Domains.* Recall that we always begin with the following setup. Let  $A$  be a Dedekind domain with field of fractions  $K$ . Let  $L/K$  be a finite extension, and let  $B$  be the integral closure of  $A$  in  $L$ . Then  $B$  is said to be an extension of the Dedekind domain  $A$ , and we have the following theorem.

**Theorem 23.1.** *With notation as above,  $B$  is a Dedekind domain.*

Extensions of Dedekind domains have the following properties:

- (1) for  $\mathfrak{p}$  a prime of  $A$ , we have  $\mathfrak{p}B = \prod_i \varphi^{e_i}$ ;
- (2) for  $L/K$  separable or  $B$  a finitely generated  $A$ -module, we have  $[L : K] = \sum_i e_i f_i$ .

23.1.4. *Decomposition and Inertia Groups.* For some prime  $\varphi$ , we have  $D_\varphi \subset \text{Gal}(L/K)$ , the *decomposition group*, which is the stabilizer of  $\varphi$  of  $L$ . For  $L/K$  an extension of global fields and  $L_\varphi/K_\mathfrak{p}$  completions at primes, we have  $\text{Gal}(L_\varphi/K_\mathfrak{p}) \simeq D_\varphi \subset \text{Gal}(L/K)$ . Moreover,  $|D_\varphi| = e_{\varphi/\mathfrak{p}} f_{\varphi/f(\cdot)}$ .

The inertia group is defined to be the subgroup  $T_\varphi \subset D_\varphi$  fixing  $\mathcal{O}_L/\varphi$  pointwise. We have that  $D_\varphi/T_\varphi \simeq \text{Gal}(\mathcal{O}_L/\varphi/\mathcal{O}_K/\mathfrak{p})$ , so  $|T_\varphi| = e_{\varphi/\mathfrak{p}}$ . Its fixed field  $L^{T_\varphi}$  (for  $L/K$  Galois) is unramified. Recall that  $\text{Frob}_K$  is (an) element of the Galois group that acts like  $x \mapsto x^q$  on residue fields, where  $q = |\mathcal{O}_K/\mathfrak{p}|$ . We use this often when  $\mu_n \subset \mathcal{O}_L/\varphi$ .

23.1.5. *Completions of (Fraction Fields of) Discrete Valuation Rings.* We have a topology on  $K$  defined by valuation, and complete using equivalence classes of Cauchy sequences for this topology. Unlike localization, which changes  $A$  but keeps  $K$  fixed, completion enlarges  $K$  to  $\widehat{K}$ , so now more polynomials have roots over  $\widehat{K}$  than  $K$ . Alternatively, we may think of  $\widehat{A}$  (for  $A$  a discrete valuation ring) as the inverse limit of  $A/\mathfrak{p}^n$ .

23.1.6. *Extensions of Complete Discrete Valuation Rings.* If  $L/\widehat{K}$  is a finite extension of a complete discrete valuation ring  $\widehat{K}$ , then  $L$  is a complete discrete valuation. So  $L$  only has one prime. In other words,  $B$ , the integral closure of  $\widehat{A}$  in  $L$  is a discrete valuation ring.

If  $L/K$  is an extension of global fields, we can complete  $K$  at  $\mathfrak{p}$ , to get  $K_{\mathfrak{p}} = \widehat{K}$ . Then  $L \otimes_K K_{\mathfrak{p}} = \prod_{\mathfrak{p}|\mathfrak{p}} L_{\mathfrak{p}}$  (which is not a field, but we can consider each  $L_{\mathfrak{p}}$  separately). If  $L = K[\theta]/f(\theta)$  for some primitive element  $\theta$ , then

$$K[\theta]/f(\theta) \otimes_{K_{\mathfrak{p}}} K_{\mathfrak{p}} \simeq K_{\mathfrak{p}}[\theta]/f(\theta) \simeq \prod_i K_{\mathfrak{p}}[\theta]/f_i(\theta)^{a_i}$$

by the Chinese Remainder Theorem. Note that the product in the above runs over factors of  $f$  over  $K_{\mathfrak{p}}$ . Recall that the factorization of  $f$  in  $K_{\mathfrak{p}}$  corresponds to the factorization of  $\mathfrak{p}$  in  $L$ .

23.1.7. *Hensel's Lemma.* If  $K$  is a local field and  $a_0$  a simple root of  $f$  over the residue field, then  $K$  has a unique root of  $f$  lifting  $a_0$ . This tells us about the structure of unramified extensions: for each positive integer  $d$ , there is a *unique* degree  $d$  unramified extension of a local field. This extension is Galois, cyclic, and it is generated by Frobenius, and is given by  $K_d = K(\mu_{q^d-1})$ .

23.1.8. *Local Fields Classification.*

**Definition 23.2.** Abstractly, a local field is a complete field with discrete valuation ring and finite residue fields.

All of the local fields are given by

- (1) finite extensions  $K/\mathbb{Q}_p$
- (2)  $\mathbb{F}_q((t))$  for  $q$  a prime power.

23.1.9. *Multiplicative Group of a Local Field (and the Unit Filtration).* Recall that  $K^* = \mathcal{O}_K^* \times \langle \pi \rangle$ . Moreover, recall  $U^{(n)} = \{x \in \mathcal{O}_K^* \mid x \equiv 1 \pmod{\pi_K^n}\}$ . Then

$$\mathcal{O}_K^* = (\mathcal{O}_K/\pi_K)^* \times U^{(1)},$$

where  $(\mathcal{O}_K/\pi_K)^*$  are lifts of roots of unity. We have that  $(\mathcal{O}_K/\pi_K)^* \simeq \mathbb{Z}/(q-1)\mathbb{Z}$  for  $q = |\mathcal{O}_K/\pi_K|$ . Moreover, we saw that  $U^{(n)}/U^{(n+1)} \simeq \mathcal{O}_K/\pi$  are abelian of exponent  $p$ . Hence,

$$U^{(1)} \simeq \mathbb{Z}/p^a\mathbb{Z} \times \mathbb{Z}_p^d,$$

where  $p$  is the characteristic of the residue field  $\mathcal{O}_K/\pi_K$  and the  $\mathbb{Z}/p^a\mathbb{Z}$  are the  $p^a$ th roots of unity. We have  $d = [K : \mathbb{Q}_p]$  in characteristic 0; otherwise  $d = \mathbb{N}$ . This theorem is used to apply class field theory.

23.1.10. *Different and Discriminant.* Let  $L/K$  be an extension of Dedekind domains. The inverse different is the ideal

$$\mathcal{D}_{L/K}^{-1} = \{x \in L \mid \text{Tr}(x\mathcal{O}_L) \subset \mathcal{O}_K\},$$

making  $\mathcal{D}_{L/K}$  an integral ideal of  $L$ . We also have

$$\mathcal{D}_{L/K} = (f'(\alpha)),$$

where  $f$  is a minimal polynomial of  $\alpha$  for  $L = K(\alpha)$ . For a tower of extensions  $M/L/K$ , we have  $\mathcal{D}_{M/K} = \mathcal{D}_{M/L}\mathcal{D}_{L/K}$ . Under completion, we have  $\mathcal{D}_{B/A}\widehat{B} = \mathcal{D}_{\widehat{B}/\widehat{A}}$ . We also have  $v_\varphi(\mathcal{D}_{L/K}) = e_{\varphi/\mathfrak{p}} - 1$  if  $\varphi$  is tamely ramified. In the wild case, we have an upper and lower bound:  $e \leq v_\varphi(\mathcal{D}_{L/K}) \leq e - 1 + v_\varphi(e)$ .

We have  $\text{Disc}_{L/K} = N_{L/K}\mathcal{D}_{L/K}$ , or, alternatively,  $\text{Disc}_{L/K}$  is generated by determinants of the trace form on bases of  $L/K$  in  $\mathcal{O}_L$ . Both  $\text{Disc}_{L/K}$  and  $\mathcal{D}_{L/K}$  are both products of powers of ramified primes. For example, if  $\mathfrak{p} = \varphi_1\varphi_2^2$ , then  $\mathfrak{p}|\text{Disc}$  while  $\varphi_2|\mathcal{D}_{L/K}$  and  $\varphi_1 \nmid \mathcal{D}_{L/K}$ .

23.1.11. *Higher Ramification Groups.* Recall that

$$G_i = \{\sigma \in \text{Gal}(L/K) \mid \sigma \text{ is trivial on } \mathcal{O}_L/(\pi_L)^{i+1}\}.$$

Note that  $v_\varphi(\mathcal{D}_{L/K})$  can be given explicitly from the  $G_i$ . Moreover,  $G_0/G_1$  is cyclic of order prime to  $\mathfrak{p}$ , and  $G_i/G_{i+1}$  for  $i \geq 1$  is abelian of exponent  $\mathfrak{p}$ . Motto: tame inertia is cyclic.

23.1.12. *Final Exam Format:* Part 1: Pick 8 out of 10 definitions/theorems (e.g., definition of the inertia group, higher ramification groups). Statements of big theorems (e.g., class field theory).

Part 2: Write about the main statements/topics. Main takeaways of the course, it's okay if you only get to 2/3 of the topics.

## 24. WEDNESDAY DECEMBER 6

### 24.1. More Course Review.

24.1.1. *Infinite Galois Theory.* There are several ways to define infinite Galois extensions:

- (1) normal and separable
- (2)  $L = \bigcup_{L_i/K \text{ finite Galois subextensions}} L_i$

Main Theorem of Infinite Galois Theory: take the Fundamental Theorem and Galois theory and add the word “closed” before subgroups.

The topology on  $\text{Gal}(L/K)$  has a basis of neighborhoods consisting of cosets of  $\text{Gal}(L/L_i)$  for  $L_i$  a finite Galois subextension. Moreover, Galois theory tells us that finite subextensions correspond to open subgroups of  $\text{Gal}(L/K)$ .

We can also think of  $\text{Gal}(L/K)$  as an inverse limit:

$$\text{Gal}(L/K) = \varprojlim_{\substack{L_i/K \text{ finite} \\ \text{Galois subextension}}} \text{Gal}(L_i/K).$$

24.1.2. *Kummer Theory.* Let  $K$  be a field with  $\mu_n \subset K$ , and suppose that the characteristic of  $K$  does not divide  $n$ . There is a correspondence

$$\{L/K \text{ abelian extensions}\} \longleftrightarrow \{\Delta \subset K^*/K^n\},$$

where  $\Delta \subset K^*/K^n$  corresponds to  $L = K(\sqrt[n]{\Delta})$ . Moreover, we have a perfect pairing

$$\text{Gal}(L/K) \otimes \Delta \rightarrow \mu_n$$

given by taking  $\sigma \otimes \alpha \mapsto \sigma(\sqrt[n]{\alpha})/\sqrt[n]{\alpha}$ . We used this in the proof of class field theory, and we also used Kummer Theory in conjunction with class field theory to get the Hilbert symbol.

24.1.3. *Local Class Field Theory.* (Abstract Class Field Theory) We have a field  $k$ , a group  $G = \text{Gal}(\bar{k}/k)$ , and a surjective homomorphism  $d : G \rightarrow \widehat{\mathbb{Z}}$ . We also have a  $G$ -module  $A$  and a  $v : A^{\text{Gal}(\bar{k}/k)} \rightarrow \widehat{\mathbb{Z}}$ , along with a condition tying  $d$  and  $v$  together. The Class Field Axiom on  $H^0(\text{Gal}(L/K \text{ cyclic}), A^{\text{Gal}(\bar{k}/k)})$  and  $H^{-1}(\text{Gal}(L/K \text{ cyclic}), A^{\text{Gal}(\bar{k}/k)})$  imply that the reciprocity map

$$r : \text{Gal}(L/K)^{ab} \rightarrow A^{\text{Gal}(\bar{k}/k)} / N_{L/K} A^{\text{Gal}(\bar{k}/k)}$$

is an isomorphism, and  $L \longleftrightarrow N_{L/K} A^{\text{Gal}(\bar{k}/L)}$  gives a one-to-one correspondence between finite abelian  $L/K$  and open subgroups of  $A^{\text{Gal}(\bar{k}/k)}$  in the norm topology.

Local Class Field Theory: The Class Field axiom is true for  $A = \bar{k}^*$ , and  $d$  is the map  $d : G \rightarrow \text{Gal}(k^{un}/k) \simeq \text{Gal}(\overline{\mathbb{F}}_q/\mathbb{F}_q)$  and  $v$  is just the usual valuation. The norm topology is simply the usual topology on  $K^*$ , and the reciprocity map is

$$r : \text{Gal}(K^{ab}/K) \rightarrow \widehat{K}^* \simeq \mathcal{O}_K^* \times \widehat{\mathbb{Z}},$$

where we note that  $\mathcal{O}_K^*$  is the inertia group. Here, the Frobenius  $\text{Frob}$  is mapped to the uniformizer. The reciprocity map is functorial in that the following diagram is commutative

$$\begin{array}{ccc} \text{Gal}(L/\Sigma) & \xrightarrow{r} & \Sigma^*/N_{L/\Sigma}L^* \\ \downarrow & & \downarrow N_{\Sigma/K} \\ \text{Gal}(L/K) & \xrightarrow{r} & K^*/N_{L/K}L^* \end{array}$$

for  $L/\Sigma$  unramified and  $\sigma = \text{Frob}_\Sigma$ .

To prove the Class Field Axiom, we used *Herbrand quotients*:

$$h(A) = \frac{|H^0(G, A)|}{|H^{-1}(G, A)|}$$

for cyclic groups. Recall that Herbrand quotients are multiplicative in exact sequences.

Moreover, the reciprocity map sends

$$G^i \longleftrightarrow U^{(i)},$$

and  $G^i$  is preserved by  $\text{Gal}(M/K) \rightarrow \text{Gal}(L/K)$  for  $M/L/K$ .

The *conductor* of  $L/K$  is  $(\pi_L^i)$  for the minimum  $i$  such that  $G_i(L/K) = 1$ , or equivalently,  $U^{(i)} \subset N_{L/K}L^*$ .

24.1.4. *Local and Global Kronecker–Weber.* Local Class Field Theory implies that  $\mathbb{Q}_p^{ab} = \mathbb{Q}_p(\mu_\infty)$ , and we also have that  $\mathbb{Q}^{ab} = \mathbb{Q}(\mu_\infty)$ .

24.1.5. *Hilbert Symbol.* Combined, Kummer Theory and Class Field Theory give us the following. Let  $K$  be a local field containing  $\mu_n$  with  $\text{char}(K) \nmid n$ . Then we have a pairing

$$(K^*/K^n \simeq \text{Gal}) \otimes (K^*/K^n \simeq \text{Hom}(\text{Gal}, \mu_n)) \rightarrow \mu_n,$$

where the first isomorphism follows from Class Field Theory and the second from Kummer Theory. The image of  $a \otimes b$  under the pairing is the Hilbert symbol  $\left(\frac{a,b}{\wp}\right)$ , where  $\wp$  is a prime of  $K$ .

There are several rules that simplify things and make Hilbert symbols easier to compute. The Legendre symbol

$$\left(\frac{u}{\wp}\right) = \left(\frac{\pi, u}{\wp}\right) = u^{(q-1)/n} \pmod{\wp}$$

for  $u \in \mathcal{O}_K^*$  and  $q = |\mathcal{O}_K/\wp|$  tests  $n$ th powers mod  $\wp$ .

There is a General Reciprocity Law for  $n$ th powers given by

$$\left(\frac{a}{b}\right) = \left(\frac{b}{a}\right)^*,$$

where the  $*$  only depends on  $a, b$  “at”  $n$  and  $\infty$  and  $*$  can be given explicitly by the Hilbert symbol.

24.1.6. *Artin Conductors.* Input Data: a representation of  $\text{Gal}(L/K)$  and exponent to put on ramified primes, using higher ramification groups contained in  $G_0 = T$ , the inertia group. Artin conductors are related to discriminants: the discriminant of the fixed field of  $H$  is the Artin conductor of  $\text{Ind}_H^G \mathbb{C}$ , the permutation representation of  $G$  on  $G/H$ .

In the tame case, the exponent of the Artin conductor is  $\text{codim} V^{G_0}$  and

$$\text{Disc} = \pi^{[G:H] - \#\{\text{cycles in the action of } G_0 = \langle \tau \rangle \text{ on } G/H\}}.$$

Recall: tame inertia is cyclic.

24.1.7. *Tame and Absolute Galois Groups.* We have that

$$\text{Gal}(K^{\text{tame}}/K) = \langle F, \tau \mid F\tau F^{-1} = \tau^q \rangle,$$

where  $F$  is a lift of Frob,  $\tau$  is a generator of the tame inertia, and  $q = |\mathcal{O}_K/\pi_K|$ . In proving this, we used our knowledge of  $\text{Gal}(K^{\text{un}}/K)$  and we used our understanding of the  $G_i$ 's and their quotients to see that tame inertia is cyclic. There are explicit descriptions of the absolute Galois groups.