INTRODUCTION TO THE LOCAL LANGLANDS CORRESPONDENCE

MASAO OI

Contents

Date: March 2, 2025, 11:26pm.

1. Week 1: Course overview

1.1. **Class field theory.** Let us begin with the following very famous and classical theorem in elementary number theory.

Theorem 1.1. *The number of the solutions to the equation $x^2 - 2 = 0$ in $\mathbb{F}_p$ is given as follows:*

$$|\{x \in \mathbb{F}_p \mid x^2 - 2 = 0\}| = \begin{cases} 2 & \text{if } p \equiv 1, 7 \pmod 8, \\ 0 & \text{if } p \equiv 3, 5 \pmod 8, \\ 1 & \text{if } p = 2. \end{cases}$$

This theorem is called *the second supplement to the quadratic reciprocity law* (see, e.g., [Ser73, Chapter I, §3]). In fact, more generally, the general quadratic reciprocity law implies the following:

Theorem 1.2. *Let $a \in \mathbb{Z}$ be an integer. Then there exists a positive integer $N \in \mathbb{Z}_{>0}$ such that the number $|\{x \in \mathbb{F}_p \mid x^2 - a = 0\}|$ depends only on the modulo N of p.*

For example, Theorem 1.1 says that N can be taken to be 8 when $a = 2$.

Exercise 1.3. (1) Explain the statement of the quadratic reciprocity law.
(2) Determine the number N in Theorem 1.2 using the quadratic reciprocity law.

Next let us consider the equation $x^3 - 2 = 0$. Can we find a simple description of the numbers of the solutions to this equation in $\mathbb{F}_p$ like above? In fact, the answer is NO! More precisely, there does not exist a positive integer $N \in \mathbb{Z}_{>0}$ such that the number $\{x \in \mathbb{F}_p \mid x^3 - 2 = 0\}$ depends only on the modulo N of p.

What causes such a difference between the quadratic and the cubic cases? To explain it, let us think about how to prove Theorem 1.1 from a modern viewpoint based on algebraic number theory. (In the following, we appeal to some basics of algebraic number theory. But it's not a material necessary for this course. If you are not familiar with them, please try to feel just its flavor.)

Since the equality $|\{x \in \mathbb{F}_2 \mid x^2 - 2 = 0\}| = 1$ is obvious, let us suppose that p is an odd prime number. Then Theorem 1.1 is rephrased as follows:

$$\mathbb{F}_p \text{ has a square root of 2 if and only if } p \equiv \pm 1 \pmod 8.$$

Noting this, let us introduce the quadratic extension $K := \mathbb{Q}(\sqrt{2})$ of $\mathbb{Q}$ obtained by adding a square root $\sqrt{2}$ of 2. The ring of integer $\mathcal{O}_K$ in K is given by $\mathbb{Z}[\sqrt{2}]$. Because the quadratic extension $K/\mathbb{Q}$ is unramified outside 2, any odd prime number p has only the following two possibilities about the ideal $p\mathcal{O}_K$ of $\mathcal{O}_K$ generated by p:

- $p\mathcal{O}_K$ is a prime (maximal) ideal of $\mathcal{O}_K$ (p "inerts" in K), or
- $p\mathcal{O}_K$ is the product $\mathfrak{p}_1\mathfrak{p}_2$ of two different prime ideals $\mathfrak{p}_1$ and $\mathfrak{p}_2$ of $\mathcal{O}_K$ (p "splits completely" in K).

Let us look at the quotient ring $\mathcal{O}_K/p\mathcal{O}_K$. This ring is

- a field if p inerts in K, and
- the product of two fields ($\mathcal{O}_K/\mathfrak{p}_1$ and $\mathcal{O}_K/\mathfrak{p}_2$) if p splits completely in K.

On the other hand,

$$\begin{aligned} \mathcal{O}_K/p\mathcal{O}_K = \mathbb{Z}[\sqrt{2}]/p\mathbb{Z}[\sqrt{2}] &\cong \big(\mathbb{Z}[x]/(x^2-2)\big)/p\big(\mathbb{Z}[x]/(x^2-2)\big) \\ &\cong \mathbb{F}_p[x]/(x^2-2). \end{aligned}$$

The right-hand side is

- a field (a quadratic extension of $\mathbb{F}_p$) if $\mathbb{F}_p$ does not have a square root of 2, and
- the product of two fields (both $\mathbb{F}_p$) if $\mathbb{F}_p$ has a square root of 2.

Hence, in summary, we see that

$$\mathbb{F}_p \text{ has a square root of 2 if and only if } p \text{ splits completely in } K.$$

Recall that each odd prime number p gives rise to a special element Frob_p of $\mathrm{Gal}(K/\mathbb{Q})$, called *Frobenius element* (again note that $K/\mathbb{Q}$ is unramified outside 2). The important property of the Frobenius is that it knows whether p splits completely or not. More precisely,

$$p \text{ splits completely in } K \text{ if } \mathrm{Frob}_p = \mathrm{id}.$$

So, our task is now reduced to investigate when $\mathrm{Frob}_p = \mathrm{id}$.

In fact, the argument so far can be carried out in general (e.g., for $x^3 - 2 = 0$ by replacing K with the smallest factorization field of $x^3 - 2 = 0$) more or less. But here we reach the stage where a special nature of the equation $x^2 - 2 = 0$ comes into play. The point is that the quadratic extension $K/\mathbb{Q}$ is abelian, i.e., its Galois group $\mathrm{Gal}(K/\mathbb{Q})$ is abelian. In general, by the Kronecker–Weber theorem, any abelian extension of $\mathbb{Q}$ is contained in a cyclotomic field $\mathbb{Q}(\mu_N)$ (μ_N denotes the set of N-th roots of unity). The Galois group of $\mathbb{Q}(\mu_N)/\mathbb{Q}$ is given by $(\mathbb{Z}/N\mathbb{Z})^\times$; by choosing a primitive N-th root ζ_N of unity, it is described as follows:

$$\mathrm{Gal}(\mathbb{Q}(\mu_N)/\mathbb{Q}) \cong (\mathbb{Z}/N\mathbb{Z})^\times : \quad [\zeta_N \mapsto \zeta_N^i] \mapsto i.$$

Under this identification, the Frobenius element Frob_p on the left-hand side is mapped to $p \in (\mathbb{Z}/N\mathbb{Z})^\times$ on the right-hand side (as long as p is unramified, which is equivalent to that p does not divide N).

In our situation, actually we have $\mathbb{Q}(\sqrt{-2}) \subset \mathbb{Q}(\mu_8)$. More precisely, under the Galois theory, $\mathbb{Q}(\sqrt{-2})$ is the subfield of $\mathbb{Q}(\mu_8)$ corresponding to the subgroup $\{\pm 1\}$ of $\mathrm{Gal}(\mathbb{Q}(\mu_8)/\mathbb{Q}) \cong (\mathbb{Z}/8\mathbb{Z})^\times$. Hence the Galois group $\mathrm{Gal}(K/\mathbb{Q})$ is identified with the quotient of $(\mathbb{Z}/8\mathbb{Z})^\times$ by $\{\pm 1\}$. Thus we conclude that

$$\mathrm{Frob}_p = \mathrm{id} \text{ if and only if } p \equiv \pm 1 \pmod 8.$$

Hence this completes the proof of Theorem 1.1.

The classical class field theory enables us to do a similar thing for more general number fields (finite extensions of $\mathbb{Q}$).

Theorem 1.4 (class field theory)**.** *Let F be a number field. Let F^{ab} be the maximal abelian extension of F. Then there exists a natural surjective continuous homomorphism*

$$\mathrm{Art}_F \colon \mathbb{A}_F^\times \to \mathrm{Gal}(F^{\mathrm{ab}}/F),$$

which kernel is explicitly described.

Here, I do not explain the meaning of "natural" (it is formulated as the compatibility with the local class field theory, which will be explained later) nor even what "$\mathbb{A}_F$" on the source of the map is. But I just want to emphasize that this "$\mathbb{A}_F$" (which is called the adele ring of F) is defined only using the intrinsic data of the original object F. So, class field theory describes how the field F extends to a larger abelian field only by appealing to the internal data of F, which is much easier to grasp. For example, when $F = \mathbb{Q}$, the map Art_F exactly gives rise to the above-mentioned isomorphism $(\mathbb{Z}/N\mathbb{Z})^\times \cong \mathrm{Gal}(\mathbb{Q}(\mu_N)/\mathbb{Q})$ by taking an appropriate finite quotient.

If we try to imitate the above discussion in the case of the equation $x^3 - 2 = 0$, we immediately notice that the last part does not work because the smallest splitting field $\mathbb{Q}(\sqrt[3]{2}, \mu_3)$ of the equation $x^3 - 2 = 0$ is not abelian over $\mathbb{Q}$; its Galois group is given by $\mathfrak{S}_3$.

1.2. **What is the Langlands correspondence?** Then, is it impossible to find any beautiful law on the behavior of the number $|\{x \in \mathbb{F}_p \mid x^3 - 2 = 0\}|$ over prime numbers p? In fact, the following holds:

Theorem 1.5. *We let $\sum_{n=1}^{\infty} a_n q^n$ be the infinite series given by the following infinite product:*

$$q \cdot \prod_{n=1}^{\infty} (1 - q^{6n}) \cdot (1 - q^{18n}) = \sum_{n=1}^{\infty} a_n q^n.$$

Then, for any prime number $p \neq 2, 3$, we have

$$|\{x \in \mathbb{F}_p \mid x^3 - 2 = 0\}| = 1 + a_p.$$

(See, e.g., [DS05, Section 4.11] for the more general case of $x^3 - a = 0$.)

Let us also introduce a different, but similar, phenomenon. We consider the following equation:

$$E \colon y^2 + y = x^3 - x^2.$$

The set of solutions of this equation forms a curve, which is called an *elliptic curve*. Let us think about the solutions in $\mathbb{F}_p$:

$$E(\mathbb{F}_p) := \{(x, y) \in \mathbb{F}_p \times \mathbb{F}_p \mid y^2 + y = x^3 - x^2\}.$$

Note that, in this case, the equation is not one-variable. So we do not even have a simple interpretation of the set $E(\mathbb{F}_p)$ in terms of field extensions of $\mathbb{Q}$. (In the case of $x^3 - 2 = 0$, although we cannot apply the class field theory, we can still relate the number $|\{x \in \mathbb{F}_p \mid x^3 - 2 = 0\}|$ to how p decomposes into prime ideals in the smallest splitting field of $x^3 - 2 = 0$.) Nevertheless, we have the following:

Theorem 1.6. *We let $\sum_{n=1}^{\infty} a_n q^n$ be the infinite series given by the following infinite product:*

$$\sum_{n=1}^{\infty} a_n q^n = q \cdot \prod_{n=1}^{\infty} (1 - q^n)^2 \cdot (1 - q^{11n})^2.$$

Then, for any prime number $p \neq 11$, we have

$$|E(\mathbb{F}_p)| = 1 + p - a_p.$$

In Theorems 1.5 and 1.6, by putting $q := \exp(2\pi i z)$ (for $z \in \mathbb{C}$), we may regard the infinite serieses as functions on the complex upper-half plane. In fact, they are examples of so-called "modular forms", which is a holomorphic function on the complex upper-half plane equipped with a lot of symmetry. Both elliptic curves and modular forms have been investigated in the context of number theory for a long time. A priori, they are totally different objects; elliptic curves are purely-algebraic while modular forms are purely-analytic, at least from the above descriptions. However, they are actually related in a surprising way as above.

All the phenomena introduced so far (Theorems 1.1, 1.5, 1.6) can be thought of as special cases of the *Langlands correspondence*. The Langlands correspondence is a vast, but conjectural, framework which connects two completely different mathematical objects: on the one hand are *automorphic representations* and on the other hand are *Galois representations*:

$$\text{(automorphic representations)} \quad \overset{\text{Langlands correspondence}}{\leftsquigarrow} \quad \text{(Galois representations)}$$

Roughly speaking, an automorphic represenation is an irreducible representation of $\mathrm{GL}_n(\mathbb{A}_F)$ realized in the space of automorphic forms, which are generalization of modular forms, and

a Galois repersentaion is an n-dimensional continuous[1] representation of the absolute Galois group $\mathrm{Gal}(\overline{F}/F)$.

The important viewpoint here is not to look at the Galois group itself, but to consider representations of the Galois group. Recall that representation theory is a very strong tool (or even a modern "formulation") for studying non-abelian groups. For example, when $n = 1$, we have $\mathrm{GL}_1(\mathbb{A}_F) = \mathbb{A}_F^\times$; this implies an automorphic representation of $\mathrm{GL}_1(\mathbb{A}_F)$ is just a character of $\mathbb{A}_F^\times$. On the other hand, when the dimension of a Galois representation is 1, it must be a character, hence it necessarily factors through the maximal abelian quotient of $\mathrm{Gal}(\overline{F}/F)$, i.e., $\mathrm{Gal}(\overline{F}^{\mathrm{ab}}/F)$. Thus the Langlands correspondence in this case says that the characters of $\mathbb{A}_F^\times$ and $\mathrm{Gal}(\overline{F}^{\mathrm{ab}}/F)$ nicely correspond. This is exactly implied by the isomorphism $\mathbb{A}_F^\times \cong \mathrm{Gal}(\overline{F}^{\mathrm{ab}}/F)$ of class field theory.

When $n = 2$, the Shimura–Taniyama conjecture, which plays a crucial role in the proof of Fermart's conjecture, is also regarded as a special case of the Langlands correspondence. Theorem 1.6 is an example of the Shimura–Taniyama conjecture.

Other than these examples, It is known that various phenomena in number theory can be explained in a sophisticated way by appealing to the prediction of the Langlands correspondence. Therefore, one of the most important objectives in the modern number theory is to establish the Langlands correspondence.

Exercise 1.7. By looking at "LMFDB" (which is an online database of modular forms, elliptic curves, and so on), we can find a lot of examples of elliptic curves and modular forms which "correspond". For example, the elliptic curve and the modular form considered in Theorem 1.6 are labelled by "11.a3" and "11.2.a.a", respectively. I just randomly chose the following elliptic curve from this database: $y^2 + xy + y = x^3 - x$. Try to find the modular form corresponding to this elliptic curve using LMFDB (please explain how you arrive at it).

1.3. **Local-global principle in number theory.** Then, what is the "local" Langlands correspondence in the course title? To explain this, let us briefly talk about the philosophy of the local-global principle in number theory. Recall that the real number field $\mathbb{R}$ is the completion of the rational number field $\mathbb{Q}$ with respect to the normal metric on $\mathbb{Q}$. We note that $\mathbb{R}$ is not the only field obtained by such a procedure from $\mathbb{Q}$. Indeed, $\mathbb{Q}$ possesses non-trivial metrics other than the normal metric. For each fixed prime number p, if we put $|p^r \cdot \frac{n}{m}|_p := p^{-r}$ (here, n and m are integers prime to p), then $|\cdot|_p$ gives a well-defined metric on $\mathbb{Q}$ called the p-adic metric. If we complete $\mathbb{Q}$ with respect to the p-adic metric, we obtain a locally compact field different to $\mathbb{R}$, which is called the *p-adic number field* and denoted by $\mathbb{Q}_p$. The fundamental philosophy in number theory is that any problem on the rational number field $\mathbb{Q}$ should be able to be understood through its analog for $\mathbb{R}$ and $\mathbb{Q}_p$ for all prime numbers p; this is the idea of "local-global" in number theory.

$$\text{problem on } \mathbb{Q} \quad \overset{\text{local-global principle}}{\leftsquigarrow} \quad \text{problems on } \mathbb{R} \text{ and } \mathbb{Q}_p \text{ (for all } p)$$

For example, the local analog of the class field theory is the *local class field theory*, which says that, for any p-adic field F (i.e., a finite extension of $\mathbb{Q}_p$), we have a natural injective homomorphism

$$\mathrm{Art}_F \colon F^\times \to \mathrm{Gal}(F^{\mathrm{ab}}/F)$$

[1]It is very important which kind of coefficient field/topology we adopt when we consider a representation of $\mathrm{Gal}(\overline{F}/F)$. But let us just ignore this subtlety here.

with dense image.

Both automorphic representations and Galois representations are objects related to the rational number field $\mathbb{Q}$ (or, more generally, any number field F). Thus it is natural to think about the analog of the Langlands correspondence for $\mathbb{R}$ or $\mathbb{Q}_p$ (or, more generally, any local field of characteristic zero, which means a finite extension of $\mathbb{R}$ or $\mathbb{Q}_p$); this is what is called the *local Langlands correspondence (LLC)*. This also generalized the local class field theory.

1.4. **What is the local Langlands correspondence?** Let us explain the LLC a bit more precisely. In the following, we let F be any p-adic field, i.e., a finite extension of $\mathbb{Q}_p$. The LLC is a natural correspondence between the set of "irreducible admissible representations" of $\mathrm{GL}_n(F)$ and the set of "n-dimensional Weil–Deligne representations":

$$(\text{irred. adm. repns. of } \mathrm{GL}_n(F)) \quad \overset{\text{LLC}}{\leftsquigarrow\!\!\rightsquigarrow} \quad (n\text{-dim. WD repns.})$$

Here, roughly speaking,

- an *irreducible admissible representation* of $\mathrm{GL}_n(F)$ means an irreducible representation of the group $\mathrm{GL}_n(F)$ on a $\mathbb{C}$-vector space equipped with a certain finiteness condition (this can be thought of as the local version of an automorphic representation);
- a *Weil–Deligne representation* is a modified version of the notion of a continuous representation of $\mathrm{Gal}(\overline{F}/F)$.

Now recall that the starting point of our discussion was how to understand the absolute Galois group $\mathrm{Gal}(\overline{F}/F)$. The point of class field theory is that it can be understood through a much easier object $F^\times$. However, at this point, we notice the following:

- The automorphic side of LLC is not so obvious to understand as in the case of $F^\times$. So we may also think that LLC enables us to investigate irreducible admissible representations of $\mathrm{GL}_n(F)$ through the Galois side, which consists of arithmetic objects.
- The automorphic side of LLC makes sense even if we replace GL_n with more general groups.

Keeping these observations in mind, let us present a naive formulation of LLC in general:

Conjecture 1.8 (local Langlands conjecture, naive form)**.** *Let G be a reductive group defined over F. Then there exists a natural map from the set of irreducible admissible representations of $G(F)$ to the set of "L-parameters" of G.*

For general G, we can no longer say that one of the automorphic or Galois sides is particularly easier than the other side. Therefore the local Langlands correspondence is very important not only from number-theoretic viewpoint, but also representation-theoretic viewpoint (representation theory of p-adic reductive groups).

At present, LLC is still conjectural in general, but has been constructed for several specific groups. For example,

- GL_n by Harris–Taylor [HT01], Henniart [Hen00],
- SO_n and Sp_{2n} (quasi-split) by Arthur [Art13],
- U_n (quasi-split) by Mok [Mok15],
- and so on...

On the other hand, there are also approaches for specific classes of irreducible admissible representations. For example,

- the classical construction by Satake for unramified representations,

- regular depth-zero supercuspidal representations by DeBacker–Reeder [DR09],
- regular (positive-depth) supercuspidal representations by Kaletha [Kal19],
- and so on...

The aims of this course to understand the following:

- A naive formulation of LLC in general. For this, I will explain some basics of representation theory of p-adic reductive groups (such as the notion of admissible representations) and also representations theory of local Galois groups (especially, Weil–Deligne representations etc).
- The precise formulation (characterization) of LLC for GL_n given by [HT01] and [Hen00]. For this, I will explain more details of representaiton theory of p-adic reductive groups by focusing on the case of GL_n (so-called "Bernstein–Zelevinsky classification"). It is far beyond my ability to explain the construction of LLC, so I'm not going to touch it.
- The precise formulation (characterization) of LLC for quasi-split classical groups given by [Art13] and [Mok15]. For this, I will explain basics about harmonic analysis on p-adic reductive groups including the Harish–Chandra characters of representaitons etc.
- Recent developments on explicit construction of LLC for certain supercuspidal representations by [DR09], [Kal19], etc.

Of course, this plan must be too ambitious. Let's see how much I can achieve...

2. Week 2: Overview of local class field theory

2.1. **Local fields and CDVR.** We briefly review some basic facts about local fields (see, e.g., [Ser79, Chapters 1, 2] or [Wei74, Chapter I]).

We first introduce the *p-adic number field* $\mathbb{Q}_p$. Recall that the real number field $\mathbb{R}$ is the completion of the rational number field $\mathbb{Q}$ with respect to the normal metric on $\mathbb{Q}$. In fact, there is a different way of completing $\mathbb{Q}$; for each prime number p, we put

$$|p^r \cdot \tfrac{n}{m}|_p := p^{-r}$$

(here, n and m are integers prime to p). Then $|\cdot|_p$ gives a well-defined metric on $\mathbb{Q}$ called the *p-adic metric*. If we complete $\mathbb{Q}$ with respect to the p-adic metric, we obtain a locally compact field different to $\mathbb{R}$, which is called the *p-adic number field* and denoted by $\mathbb{Q}_p$.

Local fields are generalizations of these fields.

Definition 2.1 (local field)**.** We say that a field F is a *local field* if it is a nondiscrete locally compact topological field.

Fact 2.2. *Any local field is isomorphic to one of the following:*

- $\mathbb{R}$ *or* $\mathbb{C}$ *(archimedean);*
- *a finite extension of* $\mathbb{Q}_p$ *(nonarchimedean, characteristic* 0*);*
- *a finite extension of* $\mathbb{F}_p((t))$ *(nonarchimedean, characteristic* p*).*

One notable characterization of a local field is that it is the completion of a *global field* (i.e., a finite extension of $\mathbb{Q}$ or $\mathbb{F}_p(t)$) with respect to a nontrivial metric. Thus, from the viewpoint of "global" number theory, both archimedean and nonarchimedean local fields have equal importance. However, in this course, we focus only on nonarhimedean local fields (and often assume even that characteristic is zero).

Let us introduce more ring-theoretic description of nonarchimedean local fields.

Definition 2.3 (DVR (discrete valuation ring))**.** Let F be a field. We say that a group homomorphism $v\colon F^\times \to \mathbb{Z}^\times$ is a *discrete valuation* of F if it is surjective and satisfies the following condition:

$$\text{For any } x, y \in F, \text{ we have } v(x+y) \geq \min\{v(x), v(y)\},$$

where we put $v(0) := \infty$. When F is equipped with a discrete valuation v, the set

$$\{x \in F \mid v(x) \geq 0\}$$

forms a subring of F, called the *valuation ring F (with respect to v)*. If a ring $\mathcal{O}$ is obtained as the valuation ring of a field with respect to its discrete valuation, we call it a *discrete valuation ring (DVR)*.

Fact 2.4. *Let $\mathcal{O}$ be a ring. Then $\mathcal{O}$ is a DVR if and only if it is a PID with unique nonzero prime (hence maximal) ideal.*

When $\mathcal{O}$ is a DVR with discrete valuation v, its subset

$$\{x \in F \mid v(x) = 0\}$$

forms the multiplicative group of units $\mathcal{O}^\times$. The maximal ideal of $\mathcal{O}$ is given by

$$\mathfrak{p} = \{x \in F \mid v(x) \geq 1\}.$$

Any generator of the maximal ideal $\mathfrak{p}$ is often referred to as a *uniformizer* of $\mathfrak{p}$. If we fix a uniformizer ϖ of $\mathfrak{p}$, then any nonzero ideal of $\mathcal{O}$ is expressed as [2]

$$\mathfrak{p}^n = \{x \in F \mid v(x) \geq n\} = \varpi^n \mathcal{O}.$$

We call $\mathcal{O}/\mathfrak{p}$ the *residue field* of $\mathcal{O}$.

Now let F be a fractional field of a DVR $\mathcal{O}$ with discrete valuation v. Then we can equip F with a metric $|x| := r^{v(x)}$ ($|0| := 0$) by choosing any real number $r \in (0, 1)$. If we let $\hat{F}$ be the completion of F with respect to this metric, $\hat{F}$ naturally has a structure of a topological field. Moreover, we can equip $\hat{F}$ with a discrete valuation which extends v; the valuation ring of $\hat{F}$ is given by the closure of $\mathcal{O}$ in $\hat{F}$. By noting that $\{\mathfrak{p}^n\}_{n \in \mathbb{Z}_{\geq 0}}$ forms a fundamental system of open neighborhoods of 0 in $\mathcal{O}$, we can see that the closure of $\mathcal{O}$ in $\hat{F}$ is nothing but

$$\hat{\mathcal{O}} := \varprojlim_n \mathcal{O}/\mathfrak{p}^n,$$

where the transition map $\mathcal{O}/\mathfrak{p}^{n+1} \twoheadrightarrow \mathcal{O}/\mathfrak{p}^n$ is given by the natural surjection.

We say that a DVR $\mathcal{O}$ is *complete* (and say $\mathcal{O}$ is a *CDVR*) if $\hat{\mathcal{O}} = \mathcal{O}$.

Fact 2.5. *Let F be a field. Then F is a nonarchimedean local field if and only if F is a fractional field of CDVR ("CDVF") with finite residue field.*

Remark 2.6. When F is a nonarchimedean local field with valuation ring $\mathcal{O}$ and maximal ideal $\mathfrak{p}$, the characteristics of $(F, \mathcal{O}/\mathfrak{p})$ must be either $(0, p)$ (called *mixed characteristic*) or (p, p) (called *equal characteristic*). According to a classification result mentioned above, F is mixed characteristic if and only if it is a finite extension of $\mathbb{Q}_p$. In this case, we often say that F is a *p-adic field* (but this terminology depends on people).

Let F be a nonarcimedean local field. Recall that the absolute Galois group of F is, by definition, the Galois group $\Gamma_F := \mathrm{Gal}(F^{\mathrm{sep}}/F)$ of the separable closure F^{sep} of F. [3] The separable closure F^{sep} is given by the direct limit (union) of all finite separable (Galois) extensions of F. We define F^{ab} to be the *maximal abelian extension* of F in F^{sep}, i.e., the direct limit (union) of all finite abelian extensions of F. (Note that this makes sense since the composite field of any two finite abelian extensions is again a finite abelian extension.) Then the Galois group $\mathrm{Gal}(F^{\mathrm{ab}}/F)$ is identified with the maximal abelian quotient of Γ_F, i.e., $\Gamma_F/\overline{[\Gamma_F, \Gamma_F]}$.

2.2. **Extension of local fields.**

Fact 2.7. *Let $\mathcal{O}_F$ be a CDVR with fractional field F. Let E/F be a finite separable extension of rank n. Then the integral closure of $\mathcal{O}_F$ in E (write $\mathcal{O}_E$) is a CDVR. Moreover, $\mathcal{O}_E$ is a free $\mathcal{O}_F$-module of rank $[E : F]$.*

By this fact, it makes sense to refer to $\mathcal{O}_F$ as the *ring of integers in F*.

Let E/F be a finite separable extension of non-archimedean local fields of degree n. Let $\mathcal{O}_F$ be the ring of integers in F, $\mathfrak{p}_F$ the maximal ideal of $\mathcal{O}_F$, $k_F := \mathcal{O}_F/\mathfrak{p}_F$ the residue field. Also for E, we define $\mathcal{O}_E$, $\mathfrak{p}_E$, and k_E in a similar way. We introduce two invariants of the extension E/F:

[2] Another popular symbol for a uniformizer is π, but we often use ϖ in our area (representation theory of p-adic groups) in order to reserve π to denote a representation.

[3] Another standard symbol for the absolute Galois group is "G_F", but we avoid it because we want to use "G" for a reductive group over F.

- The ideal $\mathfrak{p}_F\mathcal{O}_E$ of $\mathcal{O}_E$ is of the form $\mathfrak{p}_E^e$, where $e \in \mathbb{Z}_{>0}$. We call e the *ramification index* of E/F.
- Noting that $k_F = \mathcal{O}_F/\mathfrak{p}_F$ is regarded as a subfield $k_E = \mathcal{O}_E/\mathfrak{p}_E$, we let f be the degree of the finite extension k_E/k_F. We call f the *residue degree* of E/F.

Note that these invariants satisfies the chain rule: if E/F is a finite separable extension with ramification index e and residue degree f and L/E is a finite separable extension with ramification index e' and residue degree f', then L/F is a finite separable extension with ramification index ee' and residue degree ff',

Fact 2.8. *We have $n = ef$.*

Definition 2.9. (1) We say that E/F is *unramified* if $e = 1$ and (so, equivalently, $n = f$) and the residual extension k_E/k_F is separable.
(2) We say that E/F is *ramified* if it is not unramified.
(3) We say that E/F is *totally ramified* if $e = n$ (so, equivalently, $f = 1$).

Note we don't have to be worried about the second condition of the unramifiedness (separability of k_E/k_F) for local field since k_F is finite, hence perfect. Also, in this case, the ramifiedness is equivalen to that $e > 1$.

Example 2.10. Let p be an odd prime number such that $p \equiv -1 \pmod 4$. Note that this condition is equivalent to that $\sqrt{-1} \notin \mathbb{F}_p$, which is furthermore equivalent to that $\sqrt{-1} \notin \mathbb{Q}_p$ by Hensel's lemma (explained later). We put $F_0 := \mathbb{Q}_p(\sqrt{-1})$ and $F_1 := \mathbb{Q}_p(\sqrt{p})$.

- The quadratic extension $F_0/\mathbb{Q}_p$ is unramified since the residue field of F_0 must contain $\sqrt{-1}$, hence be a quadratic extension of $\mathbb{F}_p$.
- The quadratic extension $F_1/\mathbb{Q}_p$ is ramified since the ring of integers $\mathcal{O}_{F_1}$ contains $\sqrt{p}$ and the ideal $\mathfrak{p}_{E_1}$ generate by $\sqrt{p}$ satisfies $\mathfrak{p}_{E_1}^2 = p\mathcal{O}_{F_1}$ (so $\mathfrak{p}_{E_1}$ must be the maximal ideal).

In fact, unramified extensions are much easier to understand than ramified extensions. The fundamental reason for this lies in the following theorem:

Fact 2.11 (Hensel's lemma)**.** *Let $\mathcal{O}$ be a CDVR with maximal ideal $\mathfrak{p}$ and residue field k. Let $f(X) \in \mathcal{O}[X]$ be a polynomial with mod $\mathfrak{p}$ reduction $\bar{f}(X) \in k[X]$. If $\bar{\alpha} \in k$ is a simple root of $\bar{f}(X)$, then there uniquely exists a root $\alpha \in \mathcal{O}$ of $f(X)$ such that $\alpha \equiv \bar{\alpha} \pmod{\mathfrak{p}}$.*

Example 2.12. Let p be an odd prime number. Then $\mathbb{Q}_p$ contains $\sqrt{-1}$ if and only if $p \equiv 1 \pmod 4$. Indeed, note that the monic $X^2 + 1$ has a root in $\mathbb{Q}_p$ is and only if it has a root in $\mathbb{Z}_p$ since $\mathbb{Z}_p$ is integrally closed. By Hensel's lemma, the latter condition is equivalent to that $X^2 + 1$ has a root in $\mathbb{F}_p$. Since $\sqrt{-1}$ is a primitive 4th root of unity (this is nothing but the definition of the symbol "$\sqrt{-1}$") and $\mathbb{F}_p^\times$ is cyclic of order $p-1$, we have $\sqrt{-1} \in \mathbb{F}_p^\times$ if and only if $4 \mid (p-1)$, which means that $p \equiv 1 \pmod 4$.

Proposition 2.13. *Let F be a CDVF with residue field k_F. The association $E \mapsto k_E$ for any finite unramified extension E/F gives a bijective map between the set of finite unramified extensions of F (in $\overline{F}$) and the set of finite separable extensions of k_F (in $\overline{k}_F$). Moreover, E/F is Galois if and only if so is k_E/k_F; in this case the Galois groups are identified.*

Proof. We just give a sketch here. For checking the surjectivity, we take a finite separable extension k' of k_F. We write $k' = k_f[X]/(\bar{f}(X))$ with $\bar{f}(X) \in k[X]$ and choose a lift $f(X) \in \mathcal{O}_F[X]$ of $\bar{f}(X)$. Then we can show that $F[X]/(f(X))$ is a finite unramified extension whose residue field is isomorphic to k'.

To show the remaining part, we take a finite unramified extension E of F. For the residual extension k_E/k_F, we choose $\bar{f}(X) \in k_F[X]$ as in the previous paragraph and lift it to $f(X) \in \mathcal{O}_F[X]$. Then, for any finite unramified extension E', we have

$$\mathrm{Hom}_F(E, E') \overset{1:1}{\longleftrightarrow} \mathrm{Hom}_{\mathcal{O}_F}(\mathcal{O}_E, \mathcal{O}_{E'}) \overset{1:1}{\longleftrightarrow} \{\text{roots of } f(X) \text{ in } \mathcal{O}_{E'}\}$$

(if $\alpha' \in \mathcal{O}_{E'}$ is a root of $f(X)$, then the corresponding $\mathcal{O}_F$-algebra homomorphism is determined by $\alpha \mapsto \alpha'$). On the other hand, we also have

$$\mathrm{Hom}_{k_F}(k_E, k_{E'}) \overset{1:1}{\longleftrightarrow} \{\text{roots of } \bar{f}(X) \text{ in } k_{E'}\}$$

By Hensel's lemma, the right-hand sides of these are naturally bijective. Thus we get a natural bijection $\mathrm{Hom}_F(E, E') \cong \mathrm{Hom}_{k_F}(k_E, k_{E'})$. This shows the injection of the map in the assertion. Also, being Galois is preserved between E/F and k_E/k_F. □

Note that, in particular, when E and E' are finite unramified extensions of F, their composite field EE' is also a finite unramified extension of F; this is the field corresponding to $k_E k_{E'}$ in the above proposition. Hence it makes sense to think about the *maximal unramified extension* of F, which is the direct limit (union) of all finite unramified extensions of F and denoted by F^{ur}. Then F^{ur} is a Galois extension of F whose Galois group $\mathrm{Gal}(F^{\mathrm{ur}}/F)$ is isomorphic to $\mathrm{Gal}(k_F^{\mathrm{sep}}/k_F)$. We remark that, for any finite extension E/F, the intersection $E \cap F^{\mathrm{ur}}$ gives the maximal unramified (over F) subextension of F in E; in other words, $E/E \cap F^{\mathrm{ur}}$ is totally ramified and $E \cap F^{\mathrm{ur}}/F$ is unramified.

Let us apply this to the case of nonarchimedean local field. Let F be a nonarchimedean local field, hence k_F is a finite field, say $\mathbb{F}_q$ (a field of q elements). As long as we fix an algebraic closure $\overline{\mathbb{F}}_q$ of $\mathbb{F}_q$, there uniquely exists a degree n extension of $\mathbb{F}_q$ in $\overline{\mathbb{F}}_q$ for each $n \in \mathbb{Z}_{>0}$; it is $\mathbb{F}_{q^n}$, which is realized as the set of solutions of $x^{q^n} - x = 0$. This degree n extension $\mathbb{F}_{q^n}/\mathbb{F}_q$ is cyclic; $\mathrm{Gal}(\mathbb{F}_{q^n}/\mathbb{F}_q)$ has a natural generator called the *arithmetic Frobenius* element[4]

$$\mathrm{Frob}_{\mathbb{F}_q} : \mathbb{F}_{q^n} \overset{\cong}{\longrightarrow} \mathbb{F}_{q^n}; \quad x \mapsto x^q.$$

Therefore, the Galois group of the infinite Galois extension $\overline{\mathbb{F}}_q/\mathbb{F}_q$ is isomorphic to the profinite completion $\hat{\mathbb{Z}}$ of $\mathbb{Z}$:

$$\mathrm{Gal}(\overline{\mathbb{F}}_q/\mathbb{F}_q) \cong \varprojlim_n \mathrm{Gal}(\mathbb{F}_{q^n}/\mathbb{F}_q) \cong \varprojlim_n \mathbb{Z}/n\mathbb{Z} =: \hat{\mathbb{Z}}.$$

Here, the topological generator 1 of $\hat{\mathbb{Z}}$ on the right-hand side corresponds to the arithmetic Frobenius element $\overline{\mathbb{F}}_q \overset{\cong}{\longrightarrow} \overline{\mathbb{F}}_q : x \mapsto x^q$ (again denoted by $\mathrm{Frob}_{\mathbb{F}_q}$) on the left-hand side.

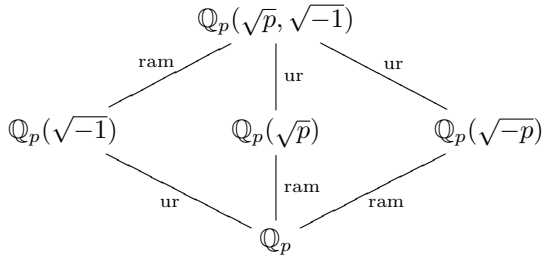
Now, by Proposition 2.13, for each $n \in \mathbb{Z}_{>0}$, there uniquely exists a degree n unramified extension F_n of F; it is generated by the solutions to the equation $x^{q^n} - x = 0$. In other words, F_n is obtained by adjoining all $(q^n - 1)$-th roots of unity to F.

Exercise 2.14. Let F be a nonarchimedean local field with residue field k_F of characteristic p. Prove that the maximal unramified extension F^{ur} is generated over F by roots of unity whose orders are prime-to-p.

We next consider ramified extensions. As mentioned before, ramified extensions are not so easy compared with unramified extension. For example, totally ramified extensions are not closed under the composition. Thus it does not make sense to think about something like "maximal totally ramified extension". Related to this, there is also no canonical way of associating a "maximal totally ramified subextension" to a given extension E/F.

[4]The inverse to the arithmetic Frobenius element is called the *geometric Frobenius* element.

Example 2.15. Let p, $F_0 = \mathbb{Q}_p(\sqrt{-1})$, and $F_1 := \mathbb{Q}_p(\sqrt{p})$ be as in Example 2.10. We furthermore introduce another quadratic extension $F_2 := \mathbb{Q}_p(\sqrt{-p})$, which is ramified for the same reason as F_1. If we let E be the quartic extension $\mathbb{Q}_p(\sqrt{p}, \sqrt{-1})$ of $\mathbb{Q}_p$, then we have $E = F_0F_1 = F_0F_2 = F_1F_2$. The situation is summarized as follows:



In particular, note that the composite of two totally ramified extensions F_1 and F_2 contains an unramified extension.

Definition 2.16. Let $\mathcal{O}$ be a CDVR with discrete valuation v. Let $f(X) \in \mathcal{O}[X]$ be a monic polynomial $f(X) = X^n + a_{n-1}X^{n-1} + \cdots + a_0$. We say that $f(X)$ is an *Eisenstein polynomial* if $v(a_i) \geq 1$ for any $1 \leq i \leq n-1$ and $v(a_0) = 1$.

Fact 2.17. *Let $\mathcal{O}$ be a CDVR with fractional field F. Let $f(X) \in \mathcal{O}[X]$ be an Eisenstein polynomial of degree n. Then $f(X)$ is irreducible and the field $F[X]/(f(X))$ is a totally ramified extension of F of degree n.*

Exercise 2.18. Let $M_n(\mathbb{Q}_p)$ be the $\mathbb{Q}_p$-algebra of n-by-n matrices whose entries are in $\mathbb{Q}_p$. We consider the following element

$$\varphi := \begin{pmatrix} 0 & 1 & & \\ & \ddots & \ddots & \\ & & \ddots & 1 \\ p & & & 0 \end{pmatrix} \in M_n(\mathbb{Q}_p).$$

More precisely, $(i, i+1)$-entry of φ is 1 for $1 \leq i \leq n-1$, $(n, 1)$-entry of φ is p, and all the other entries are 0. We consider the $\mathbb{Q}_p$-subalgebra $\mathbb{Q}_p[\varphi]$ of $M_n(\mathbb{Q}_p)$ generated by φ. Prove that $\mathbb{Q}_p[\varphi]$ is a finite extension of $\mathbb{Q}_p$ (in particular, $\mathbb{Q}_p[\varphi]$ is a field). Also, determine the extension degree, the ramification index, and the residue degree of $\mathbb{Q}_p[\varphi]/\mathbb{Q}_p$.

2.3. **Galois groups and Weil groups of local fields.** Let E/F be a finite Galois extension of nonarchmedean local fields. Then, any element of $\mathrm{Gal}(E/F)$ induces an element of the extension of residue fields k_E/k_F. In other words, we have a natural surjection $\mathrm{Gal}(E/F) \twoheadrightarrow \mathrm{Gal}(k_E/k_F)$. By letting E run over all finite Galois extensions of F, we also get a natural surjection $\Gamma_F := \mathrm{Gal}(F^{\mathrm{sep}}/F) \twoheadrightarrow \mathrm{Gal}(\overline{k}_F/k_F)$.

Definition 2.19. We let I_F be the kernel of the map $\Gamma_F \twoheadrightarrow \mathrm{Gal}(\overline{k}_F/k_F)$ and call it the *inertia subgroup* of Γ_F.

Recall that we have $\mathrm{Gal}(F^{\mathrm{ur}}/F) \cong \mathrm{Gal}(\overline{k}_F/k_F)$. Hence the inertia subgroup I_F is nothing but the closed subgroup of Γ_F corresponding to the subextension F^{ur}, i.e., $I_F = \mathrm{Gal}(F^{\mathrm{sep}}/F^{\mathrm{ur}})$.

Definition 2.20. We define a subgroup W_F of Γ_F to be the preimage of $\langle \mathrm{Frob}_{k_F} \rangle$ under the map $\Gamma_F \twoheadrightarrow \mathrm{Gal}(\bar{k}_F/k_F)$ and call it the *Weil group* of F.

$$\begin{array}{ccccccccc} 1 & \longrightarrow & I_F & \longrightarrow & \Gamma_F & \longrightarrow & \mathrm{Gal}(\bar{k}_F/k_F) \cong \hat{\mathbb{Z}} & \longrightarrow & 1 \\ & & \| & & \cup & & \cup & & \\ 1 & \longrightarrow & I_F & \longrightarrow & W_F & \longrightarrow & \langle \mathrm{Frob}_{k_F} \rangle \cong \mathbb{Z} & \longrightarrow & 1 \end{array}$$

Note that the Weil group is not the Galois group for any Galois extension, hence there is no intrinsic topology on W_F. We equip W_F with the topology such that I_F is open in W_F and the induced topology on I_F coincides with the natural topology of I_F (as the Galois group of $F^{\mathrm{sep}}/F^{\mathrm{ur}}$). The natural inclusion $W_F \hookrightarrow \Gamma_F$ induces an inclusion between their maximal abelian quotients $W_F^{\mathrm{ab}} \hookrightarrow \Gamma_F^{\mathrm{ab}}$.

2.4. **Local class field theory.**

Theorem 2.21 (local class field theory)**.** *Let F be a non-archimedean local field with residue field k. Then there uniquely exists an isomorphism*

$$\mathrm{Art}_F \colon F^\times \xrightarrow{\cong} W_F^{\mathrm{ab}}$$

as topological groups satisfying the following properties:

1. *For any uniformizer $\varpi \in F^\times$, its image $\mathrm{Art}_F(\varpi) \in W_F^{\mathrm{ab}}$ is a lift of the arithmetic Frobenius $\mathrm{Frob}_k \in \mathrm{Gal}(\bar{k}/k)$.*
2. *For any finite separable extension E/F, the following diagram commutes:*

$$\begin{array}{ccc} E^\times & \xrightarrow{\mathrm{Art}_E} & W_E^{\mathrm{ab}} \\ {\scriptstyle \mathrm{Nr}_{E/F}}\downarrow & & \downarrow{\scriptstyle \mathrm{res}} \\ F^\times & \xrightarrow{\mathrm{Art}_F} & W_F^{\mathrm{ab}} \end{array}$$

3. *For any finite abelian extension E/F, Art_F induces an isomorphism*

$$F^\times / \mathrm{Nr}_{E/F}(E^\times) \xrightarrow{\cong} \mathrm{Gal}(E/F).$$

Because of this theorem, it is important to know the structure of $F^\times$. So let us explain how $F^\times$ can be understood.

We first note the exact sequence

$$1 \to \mathcal{O}_F^\times \to F^\times \xrightarrow{v} \mathbb{Z} \to 1.$$

This splits by choosing a uniformizer $\varpi \in F^\times$, i.e., we have $F^\times \cong \mathcal{O}_F \times \langle \varpi \rangle$. Secondly, we have the exact sequence

$$1 \to (1 + \mathfrak{p}_F) \to \mathcal{O}_F^\times \to k_F^\times \to 1.$$

This splits by Hensel's lemma; elements of $k_F^\times$ are identified with $(q-1)$-roots of unity, where $q = |k_F|$. Finally, we consider the exponential/logarithm map between F and $F^\times$. Here, for simplicity, we suppose that $F = \mathbb{Q}_p$:

$$\exp \colon \mathbb{Q}_p \to \mathbb{Q}_p^\times; \quad x \mapsto \sum_{n=0}^{\infty} \frac{1}{n!} x^n,$$

$$\log \colon \mathbb{Q}_p^\times \to \mathbb{Q}_p; \quad x \mapsto \sum_{n=1}^{\infty} \frac{(-1)^{n-1}}{n} (x-1)^n.$$

These maps do not converge on the whole domain, but gives group isomorphisms between

$$\begin{cases} p\mathbb{Z}_p \text{ and } 1+p\mathbb{Z}_p & \text{if } p \neq 2, \\ 4\mathbb{Z}_2 \text{ and } 1+4\mathbb{Z}_2 & \text{if } p = 2. \end{cases}$$

In the case where $p = 2$, we have $(1 + 2\mathbb{Z}_2) \cong \{\pm 1\} \times (1 + 4\mathbb{Z}_2)$. Thus, in conclusion, we have

$$\mathbb{Q}_p^\times \cong \begin{cases} \mathbb{Z} \times \mathbb{Z}/(p-1)\mathbb{Z} \times \mathbb{Z}_p & \text{if } p \neq 2, \\ \mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}_2 & \text{if } p = 2. \end{cases}$$

Exercise 2.22. Count the number of (isomorphism classes of) quadratic extensions of $\mathbb{Q}_p$.

Exercise 2.23. For any finite abelian group G, can we always find a finite abelian extension of nonarchimedean local fields E/F whose Galois group is isomorphic to G?

References

[Art13] J. Arthur, *The endoscopic classification of representations: Orthogonal and symplectic groups*, American Mathematical Society Colloquium Publications, vol. 61, American Mathematical Society, Providence, RI, 2013.

[DR09] S. DeBacker and M. Reeder, *Depth-zero supercuspidal L-packets and their stability*, Ann. of Math. (2) **169** (2009), no. 3, 795–901.

[DS05] F. Diamond and J. Shurman, *A first course in modular forms*, Graduate Texts in Mathematics, vol. 228, Springer-Verlag, New York, 2005.

[Hen00] G. Henniart, *Une preuve simple des conjectures de Langlands pour* GL(n) *sur un corps p-adique*, Invent. Math. **139** (2000), no. 2, 439–455.

[HT01] M. Harris and R. Taylor, *The geometry and cohomology of some simple Shimura varieties*, Annals of Mathematics Studies, vol. 151, Princeton University Press, Princeton, NJ, 2001, With an appendix by Vladimir G. Berkovich.

[Kal19] T. Kaletha, *Regular supercuspidal representations*, J. Amer. Math. Soc. **32** (2019), no. 4, 1071–1170.

[Mok15] C. P. Mok, *Endoscopic classification of representations of quasi-split unitary groups*, Mem. Amer. Math. Soc. **235** (2015), no. 1108, vi+248.

[Ser73] J.-P. Serre, *A course in arithmetic*, Graduate Texts in Mathematics, vol. No. 7, Springer-Verlag, New York-Heidelberg, 1973, Translated from the French.

[Ser79] ———, *Local fields*, Graduate Texts in Mathematics, vol. 67, Springer-Verlag, New York-Berlin, 1979, Translated from the French by Marvin Jay Greenberg.

[Wei74] A. Weil, *Basic number theory*, third ed., Die Grundlehren der mathematischen Wissenschaften, vol. Band 144, Springer-Verlag, New York-Berlin, 1974.

Department of Mathematics, National Taiwan University, Astronomy Mathematics Building 5F, No. 1, Sec. 4, Roosevelt Rd., Taipei 10617, Taiwan

Email address: masaooi@ntu.edu.tw