CLASS FIELD THEORY
WEEK 1

JAVIER FRESÁN

1. Motivation

In a 1640 letter to Mersenne, Fermat proved the following:

Theorem 1.1 (Fermat)**.** A prime number p distinct from 2 is a sum of two squares if and only if $p \equiv 1 \bmod 4$.

Factorising the expression $x^2 + y^2$ as $(x + iy)(x - iy)$, this translates into a question about how prime numbers decompose in the ring of Gaussian integers $\mathbb{Z}[i]$. More generally, let K be a quadratic number field and $\mathcal{O}_K$ its ring of integers. For each prime number p, the ideal $p\mathcal{O}_K$ decomposes uniquely as a product of prime ideals. There are three posibilities:

- $p\mathcal{O}_K$ is a product of two distinct prime ideals $\mathfrak{p}_1$ and $\mathfrak{p}_2$ (p is *totally decomposed*),
- $p\mathcal{O}_K$ remains a prime ideal (p is *inert*),
- $p\mathcal{O}_K = \mathfrak{p}^2$ for some prime ideal $\mathfrak{p}$ (p is *ramified*).

Using this language, Fermat's theorem can be rephrased as follows: in the ring $\mathbb{Z}[i]$,

$$p \text{ is } \begin{cases} \text{totally decomposed} & p \equiv 1 \bmod 4, \\ \text{inert} & p \equiv 3 \bmod 4, \\ \text{ramified} & p = 2. \end{cases}$$

Similar phenomena arise for all quadratic fields. For example, in the ring of integers of the quadratic field $\mathbb{Q}(\sqrt{6})$, the ramified primes are $p = 2, 3$, and a prime is totally decomposed if and only if $p \equiv 1, 5, 19, 23 \bmod 24$. An inspection of the tables reveals the common features:

- There is a finite number of ramified primes and how p decomposes is determined mod N for an integer N which is a product of the ramified primes with some multiplicities.
- The totally decomposed primes form a subgroup of index 2 of $(\mathbb{Z}/N\mathbb{Z})^\times$. For instance,
$$(\mathbb{Z}/24\mathbb{Z})^\times = \{1, 5, 7, 11, 13, 17, 19, 23\}$$
and totally decomposed primes correspond to $\{1, 5, 19, 23\}$.

This is all explained by class field theory:

Theorem 1.2 (Kronecker-Weber)**.** A number field K is abelian if and only if it is embeddable into a cyclotomic field $\mathbb{Q}(\mu_N)$.

The smallest integer for which this holds is called the *conductor*.

Theorem 1.3. Let K be a number field.

(1) Assume that K is abelian. Then:

(a) A prime number p is ramified[1] in K if and only if p divides the conductor.
(b) If $K \subseteq \mathbb{Q}(\mu_N)$, then whether or not p is totally decomposed[2] in K depends on p modulo N.

(2) Conversely, if the conclusion of (b) holds, then $K \subseteq \mathbb{Q}(\mu_N)$ (so K is abelian).

In the particular case of quadratic fields, the conductor is given as follows: if $K = \mathbb{Q}(\sqrt{d})$ for a square-free integer d, then the conductor is

$$N = \begin{cases} |d| & d \equiv 1 \bmod 4, \\ 4|d| & d \equiv 2, 3 \bmod 4. \end{cases}$$

From this we get a group morphism

$$\chi_d \colon (\mathbb{Z}/N\mathbb{Z})^\times \simeq \mathrm{Gal}(\mathbb{Q}(\mu_N)/\mathbb{Q}) \longrightarrow \mathrm{Gal}(K/\mathbb{Q}) \simeq \{\pm 1\}$$

such that p is totally decomposed if and only if $\chi_d(p) = 1$. This map is given by

$$\chi_d(a) = \theta_d(a) \prod_{\substack{p \mid d \\ \text{odd prime}}} \left(\tfrac{a}{p}\right),$$

where $(\frac{\cdot}{p})$ is the Legendre symbol and $\theta_d(a)$ is defined as follows:

- if $d \equiv 1 \bmod 4$, then $\theta_d(a) = 1$ for all a,
- if $d \equiv 3 \bmod 4$, then $\theta_d(a) = 1$ if $a \equiv 1 \bmod 4$ and -1 otherwise,
- if d is even, then $\theta_d(a) = 1$ if $a \equiv \pm 1 \bmod 8$ and -1 otherwise,

2. The maximal abelian extension

2.1. **Infinite Galois theory.** Let K be a field. A (possibly infinite) field extension L/K is *Galois* if it is the union of all the finite Galois extensions of K contained in L. The Galois group $\mathrm{Gal}(L/K)$ is the group of field automorphisms of L restricting to the identity on K. It can be written as an inverse limit of usual Galois groups

$$\mathrm{Gal}(L/K) = \varprojlim \mathrm{Gal}(M/K)$$

indexed by the directed set of finite Galois extensions M of K. Groups of this shape are called *profinite groups* and come together with a topology for which the group operations are continuous. A new feature of infinite Galois theory is that the topology plays a role. For example, the Galois correspondence reads:

Theorem 2.1 (Galois correspondence)**.** Let L/K be a Galois extension of Galois group G. There is a one-to-one correspondence

$$\{\text{subfields } K \subseteq M \subseteq L\} \overset{1:1}{\longleftrightarrow} \{\textit{closed} \text{ subgroups } H \text{ of } G\}$$

given by sending a field M to $\mathrm{Gal}(L/M)$ and a subgroup H to $M = L^H$. Moreover,

- M is a finite extension if and only if H is an open subgroup.
- M is a Galois extension if and only if $\mathrm{Gal}(L/M)$ is a normal subgroup of G.

(As you will prove in the exercises, an open subgroup is always closed!)

[1] for a general number field, this means that $p\mathcal{O}_K$ decomposes as a product of distinct prime ideals.
[2] now this means that $p\mathcal{O}_K$ decomposes as a product of $[K \colon \mathbb{Q}]$ distinct prime ideals

Example 2.2.

(1) Let K^{sep} be a separable closure of K. Then K^{sep} is a Galois extension and the group $\mathrm{Gal}(K^{\mathrm{sep}}/K)$ is called the *absolute Galois group* of K.

(2) Let K be a field and K^{sep} a separable closure. The *maximal abelian extension of* K is the union of all finite abelian extensions $K \subseteq L \subseteq K^{\mathrm{sep}}$. It will be denoted by:

$$K^{\mathrm{ab}} = \bigcup_{\substack{L/K \\ \text{finite abelian}}} L.$$

It is a Galois extension and the group $\mathrm{Gal}(K^{\mathrm{ab}}/K)$ is the abelianization of the absolute Galois group of K. Class field theory aims at describing $\mathrm{Gal}(K^{\mathrm{ab}}/K)$ for various K.

2.2. **The case of finite fields.** Let $K = \mathbb{F}_q$ be the finite field with q elements. For each integer $n \geq 1$, there is a unique degree n extension of $\mathbb{F}_q$, namely $\mathbb{F}_{q^n}$. It is a Galois extension. If σ_q denotes the Frobenius automorphism $x \mapsto x^q$, then

$$\mathrm{Gal}(\mathbb{F}_{q^n}/\mathbb{F}_q) = \langle \sigma_q \rangle \simeq \mathbb{Z}/n\mathbb{Z}.$$

It follows that the absolute Galois group of $\mathbb{F}_q$ is isomorphic to

$$\mathrm{Gal}(\overline{\mathbb{F}}_q/\mathbb{F}_q) = \varprojlim_n \mathbb{Z}/n\mathbb{Z} \stackrel{\mathrm{def}}{=} \widehat{\mathbb{Z}}. \tag{1}$$

The assignment $1 \mapsto \sigma_q$ yields a continuous group morphism

$$\rho_{\mathbb{F}_q} \colon \mathbb{Z} \longrightarrow \mathrm{Gal}(\overline{\mathbb{F}}_q/\mathbb{F}_q)$$

whose composition with (1) is the map sending an integer r to the collection of residues $(r \bmod n)_n$. Class field theory for finite fields is the following "toy" statement:

Proposition 2.3. There is a one-to-one correspondence

$$\{\text{finite abelian extensions of } \mathbb{F}_q\} \stackrel{1:1}{\longleftrightarrow} \{\text{open subgroups of finite index in } \mathbb{Z}\}$$

given by sending the open subgroup $U \subset \mathrm{Gal}(\overline{\mathbb{F}}_q/\mathbb{F}_q)$ associated to a finite abelian extension by the Galois correspondence to $\rho_{\mathbb{F}_q}^{-1}(U)$.

2.3. **The case of cyclotomic fields.** Assuming the Kronecker-Weber theorem, the maximal abelian extension of $K = \mathbb{Q}$ is the union of all cyclotomic fields $\mathbb{Q}(\mu_N)$. Therefore,

$$\begin{aligned} \mathrm{Gal}(\mathbb{Q}^{\mathrm{ab}}/\mathbb{Q}) &= \varprojlim_n \mathrm{Gal}(\mathbb{Q}(\mu_n)/\mathbb{Q}) \\ &= \varprojlim_n (\mathbb{Z}/n\mathbb{Z})^\times \\ &\stackrel{\mathrm{def}}{=} \widehat{\mathbb{Z}}^\times. \end{aligned}$$

But we want to proceed the other way around, that is, to understand the structure of $\mathrm{Gal}(\mathbb{Q}^{\mathrm{ab}}/\mathbb{Q})$ to prove the Kronecker-Weber theorem!

3. Local fields

The next case to study is local fields. Let us give a few definitions:

Definition 3.1. Let K be a field. An *absolute value* $|\cdot|$ on K is a map $|\cdot|\colon K \to \mathbb{R}_{\geq 0}$ satisfying the following three properties:

- $|0| = 0$ and $|1| = 1$,
- $|xy| = |x||y|$ for all $x, y \in K$;
- $|x + y| \leq |x| + |y|$ for all $x, y \in K$.

A field together with an absolute value will be called a *valued field*. We say that a valued field is *non-archimedean*[3] whenever the stronger inequality $|x + y| \leq \max(|x|, |y|)$ holds.

A valued field is equipped with the metric topology associated to the distance

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

Example 3.2.

(1) Let $K = \mathbb{Q}$ and p a prime number. Every non-zero rational number x can be written as $x = p^u \frac{m}{n}$ for $u \in \mathbb{Z}$ and $m, n \in \mathbb{Z}$ not divisible by p. Then $|x|_p = p^{-u}$ is a non-archimedean absolute value on $\mathbb{Q}$.

(2) Let k be a field and $K = k((t))$ the field of *Laurent series* with coefficients in k, *i.e.* formal power series $f = \sum_{n \in \mathbb{Z}} a_n t^n$ such that, for negative n, only finitely many a_n are non-zero. Fix a real number $q > 1$ and define $|f| = q^{-n}$, where n is the smallest integer such that $a_n \neq 0$. This is a non-archimedean absolute value on K.

Definition 3.3. Let K be a valued field.

(1) K is *complete* if the metric topology is complete, *i.e.* all Cauchy sequences converge.

(2) K is a *local field* if the absolute value is non-trivial and K is locally compact for the metric topology.

Recall that *locally compact* means that every point has a compact neighborhood. All fields are locally compact when endowed with the trivial absolute value $|x| = 1$ for all $x \in K^\times$, this is why one needs to exclude it. It is easy to see that local fields are complete.

Example 3.4.

(1) The valued field $(\mathbb{Q}, |\cdot|_p)$ is *not* complete. The completion is the field $\mathbb{Q}_p$ of p-adic numbers, and there is a unique absolute value extending $|\cdot|_p$. It is a local field.

(2) The field of Laurent series $k((t))$, together with the above absolute value, is a complete field. It is locally compact if and only if k is finite.

These are essentially all local fields. Precisely:

Proposition 3.5. Local fields fall into three classes:

- the fields $\mathbb{R}$ and $\mathbb{C}$ of real and complex numbers (*archimedean local fields*),
- finite extensions of $\mathbb{Q}_p$ (*p-adic fields*),
- finite extensions of the field of Laurent series $\mathbb{F}_p((t))$.

[3] also called *ultrametric*.

The second two families of local fields share the property that K is a discrete valuation field whose residue field is finite. This means that K comes together with a surjective group morphism $\nu\colon K^\times \to \mathbb{Z}$ such that, setting $\nu(0) = +\infty$, the inequality

$$\nu(x+y) \geq \min(\nu(x), \nu(y))$$

holds for all $x, y \in K$. Then the subring[4] $\mathcal{O}_K \subset K$ consisting of those elements with $\nu(x) \geq 0$ has a unique maximal ideal $\mathfrak{m}$. The quotient $\kappa = \mathcal{O}_K/\mathfrak{m}$ is called the *residue field*.

Example 3.6.

(1) For $K = \mathbb{Q}_p$, the valuation ring is $\mathcal{O}_{\mathbb{Q}_p} = \mathbb{Z}_p$, the maximal ideal $\mathfrak{m} = p\mathbb{Z}_p$ and the residue field is $\kappa = \mathbb{F}_p$.
(2) For $K = k((t))$, the valuation ring is $\mathcal{O}_{k((t))} = k[[t]]$, the maximal ideal $\mathfrak{m} = tk[[t]]$ and the residue field is $\kappa = k$.

3.1. **Ramification.** Let K be a complete discrete valuation field with finite residue field.

Lemma 3.7. Let L be a finite extension of K. There exists a unique discrete valuation ν_L on L and an integer $e > 0$ such that $\nu_L(x) = e \cdot \nu_K(x)$ for all $x \in K$.

Definition 3.8. An extension L/K is called *unramified* if $e = 1$. The *maximal unramified extension* K^{ur} of K is the union of all finite unramified extensions $K \subseteq L \subseteq K^{\mathrm{sep}}$.

Theorem 3.9. Let K be a complete discrete valuation field with finite residue field $\mathbb{F}_q$. The maximal unramified extension K^{ur} is obtained by adjoining to K all roots of unity of orders prime to p. In particular, $K^{\mathrm{ur}} \subseteq K^{\mathrm{ab}}$ and

$$\mathrm{Gal}(K^{\mathrm{ur}}/K) \simeq \mathrm{Gal}(\bar{\mathbb{F}}_q/\mathbb{F}_q). \tag{2}$$

(This is the part of the Galois group which is the easiest to understand).

4. Local class field theory

Our first main goal in this course will be to prove the following:

Theorem 4.1 (Main theorem of local class field theory)**.** Let K be a local field.

(1) There exists a unique continuous group morphism

$$\rho_K\colon K^\times \longrightarrow \mathrm{Gal}(K^{\mathrm{ab}}/K) \tag{3}$$

satisfying the following two conditions:

(a) For each finite abelian extension L of K, ρ_K induces an isomorphism of the quotient groups

$$\begin{array}{ccc} K^\times & \xrightarrow{\rho_K} & \mathrm{Gal}(K^{\mathrm{ab}}/K) \\ \downarrow & & \downarrow \\ K^\times/N_{L/K}(L^\times) & \xrightarrow{\sim} & \mathrm{Gal}(L/K), \end{array}$$

where $N_{L/K}\colon L \to K$ denotes the norm, given by $N_{L/K}(x) = \prod_{\mathrm{Gal}(L/K)} \sigma(\alpha)$.

[4] called the *valuation ring*

(b) If K is a complete discrete valuation field with finite residue field $\mathbb{F}_q$, then the following diagram commutes

$$\begin{array}{ccc} K^\times & \xrightarrow{\rho_K} & \mathrm{Gal}(K^{\mathrm{ab}}/K) \\ \downarrow{\scriptstyle \nu_K} & & \downarrow \\ \mathbb{Z} & \xrightarrow{\rho_{\mathbb{F}_q}} & \mathrm{Gal}(\overline{\mathbb{F}}_q/\mathbb{F}_q). \end{array}$$

Here, ν_K is the discrete valuation of K and the right vertical arrow is the composition $\mathrm{Gal}(K^{\mathrm{ab}}/K) \to \mathrm{Gal}(K^{\mathrm{ur}}/K)$ with the isomorphism (2).

(2) There is a one-to-one correspondence between open subgroups of $\mathrm{Gal}(K^{\mathrm{ab}}/K)$ and open subgroups of finite index of $K^\times$ given by

$$U \mapsto \rho_K^{-1}(U).$$

An immediate corollary is the following:

Corollary 4.2. Let K be a local field. There is a one-to-one correspondence

$$\{\text{finite abelian extensions of K}\} \overset{1:1}{\longleftrightarrow} \{\text{open subgroups of finite index of } K^\times\}$$

which maps L/K to the subgroup $N_{L/K}(L^\times)$ of $K^\times$.

We will give two proofs, one based on group cohomology and the Brauer group, the other through Lubin-Tate theory. For number fields, the main theorem of global class field theory looks very similar, but $K^\times$ is replaced by something more complicated, the group of *ideles*. It is a quotient $C_K = \mathbb{A}_K^\times/K^\times$ of the group of invertible elements in the ring of adeles

$$\mathbb{A}_K = \{(x_v)_v \in \prod_v K_v \mid \text{all but finitely many } a_v \text{ belong to } \mathcal{O}_{K_v}\}.$$

Example 4.3.

(1) When $K = \mathbb{R}$, the only open subgroups of finite index of $\mathbb{R}^\times$ are $\mathbb{R}^\times_{>0}$ and $\mathbb{R}^\times$. They correspond to the extensions $\mathbb{C}$ and $\mathbb{R}$ respectively. The map

$$\rho_{\mathbb{R}} \colon \mathbb{R}^\times \longrightarrow \mathrm{Gal}(\mathbb{C}/\mathbb{R})$$

sends positive real numbers to 1 and negative real numbers to complex conjugation.

(2) Let p be a prime number different from 2. The theorem implies that there are exactly $p+1$ abelian extensions of $\mathbb{Q}_p$ of degree p.

References

[1] K. Kato, N. Kurokawa, T. Saito. *Number theory. 2. Introduction to class field theory.* Translations of Mathematical Monographs **240**, American Mathematical Society, 2011.

ETH Zürich, D-MATH, Rämistrasse 101, CH-8092 Zürich, Switzerland

E-mail address: javier.fresan@math.ethz.ch