Class Field Theory: Motivations and a Preview

Yujia Yin

Abstract

We summarize the number-theoretic and function-theoretic backgrounds needed for the later discussions of geometric inspirations of modern algebraic number theory. Along the way, we indicate some obstructions to upgrading these inspirations to literal translations with the current technology.

Contents

1 Introduction

The reciprocity problem is a central problem in algebraic number theory. It asks for descriptions of all finite Galois extensions of an arithmetically interesting field, which are considered to be “external” data, in terms of its “intrinsic” data.

The fields we consider are global fields [(1)], sometimes called A-fields following the terminology of Weil. Since our approach will be from local to global, we will study local fields[(2)] along the way.

Class field theory is a partial solution to the reciprocity problem for global fields in the case of abelian extensions. It characterizes the abelian extensions of both global and local fields using their congruence information(the class groups).

We will focus on local and global number fields to keep the exposition simple. Comments on function fields will only be made when separate treatments are absolutely necessary.

The purpose of this note is twofold. The first goal is dig out the function-theoretic roots of modern developments of algebraic number theory related

[(1)] These are number fields and function fields of one varibale over some finite field $\mathbb{F}_q$.

[(2)] These are completions of global fields with respect to metrics given by valuations.

to the reciprocity problem. To this end, we take steps towards formalizing the function field and number field analogy by geometrizing the number fields using scheme-theoretic machinery whenever possible while making the comparisons. The second goal is to substantiate the idea of geometrization of number fields by revisiting class field theory from a scheme-centric viewpoint.

It should be stressed that the transition to the scheme-theoretic framework is only a first-order approximation to a true geometric theory for number fields, whatever that might be, because the dictionary is far from being complete at this stage. We illustrate some of the challenges by specific examples.

Remarks about Notations and Terminology

Like many theories with long history and on-going developments, due to its diverse inputs and applications, notations and terminologies related to Class field theory in the literature may vary. Ours closely follow those used by [1], up to a point. For algebraic geometry, we stick with those in [10] and [17].

2 Motivations from Theory of Algebraic Curves in Classical Era

The number field-function field analogy suggests a dictionary to between arithmetics of number fields and geometries of curves. It was realized that they share many similar properties when interpreted properly. Attempts to make this analogy precise in towards the end of nineteenth century(the classical era) led to the introduction of valuations in algebraic number theory and the p-adic numbers.

The analogy can be made more precise by observing that the scheme $\operatorname{Spec}\mathbb{Z}_K$ is one-dimensional for the integer ring $\mathbb{Z}_K$[3] of a number field K and is therefore legitimately a curve. The function field K of $\operatorname{Spec}\mathbb{Z}_K$ and its rings of integers with respect to its discrete valuations share many similar and mostly commutative algebraic properties with their analogues of a smooth projective curve over a finite field. Some of these algebraic properties are listed in 3.1 of this note, for more details, we refer to Weil's "Basic Number Theory"([18]). Statements about function fields over finite fields by means of algebro-geometric methods often have arithmetic analogues by restating it in terms of algebraic language.

The world of compact Riemann surfaces and the world of function fields over finite fields are linked by algebraic geometry: replacing the finite con-

[3] Another commonly used notation is $\mathcal{O}_K$, we avoid it because $\mathcal{O}_X$ usually denotes the structural sheaf of a ringed space X.

stant fields by $\mathbb{C}$, we get complex smooth projective curves which are known to be equivalent[4] to compact Riemann surfaces, which are genuinely geometric. Many results about compact Riemann surfaces have counter-parts in function fields by transporting the algebro-geometric constructions.

Putting all of these together, we arrive at Weil's Rosetta stone([13]), expressed by the diagram

$$\begin{tikzcd} \mathbb{Z}_K \arrow[r, leftrightarrow, "\text{CA}"'] & X_{/\mathbb{F}_q} \arrow[r, leftrightarrow, "\text{AG}"'] & \Sigma_g \end{tikzcd} .$$[5]

The function field in the "number field-function field" analogy then has a different meaning: it refers to some compact Riemann surface. We can geometrize statements about number fields by walking through the two bridges.

Pushing the analogy further, Galois extensions of K should correspond to (possibly ramified [6]) normal covers of $\operatorname{Spec} \mathbb{Z}_K$, which should be literal covers after removing ramification points upstairs and branch points downstairs[7]. Formalizing this analogy requires the concept of an étale morphism. The morphism between the two punctured schemes induced by a finite Galois extension is an example of étale covers.

For a "nice" space X, such as a Riemann surface, there is an explicit correspondence between its covering spaces,which are intuitively external, and subgroups of its fundamental group $\pi_1(X, *)$, which can be computed intrinsically in principle, by analyzing its deck transformations. In fact, all covers of X, finite or not, can be constructed explicitly from its intrinsic data([11],section 1.3,p 63).

Reciprocity problem[8] is a challenge to generalize this correspondence to the arithmetic schemes $\operatorname{Spec} \mathbb{Z}_K$'s, which are easily verified to be terribly bad spaces from the point of view of a geometric topologist.

The reciprocity problem as stated is rather vague, in that it asserts no explicit falsifiable conjectures. A general trend of number theory is to bring order to chaos: without the benefit of hindsight, $\mathbb{Z}$ as is defined seemed

[4] More precisely, the category of compact Riemann surfaces is dual to the category of complex smooth projective curves.

[5] "CA" stands for commutative algebra."AG" stands for algebraic geometry. Σ_g is some compact Riemann surface with genus g.

[6] "Branched" is another commonly used-term in the literature.

[7] I am always confused which is which. Aren't they synonyms in English? Here I am using the definition of Vakil ([17],p588,21.6). It is not clear to me this is better than its conjugate.

[8] A schematic diagram of the reciprocity problem: $$\begin{tikzcd} X' \arrow[d, "p"] \\ X \arrow[u, dashed, bend right=60, "?"] \end{tikzcd}$$. The dotted arrow is not meant to be a lift of any sort. It just indicates some identification of external information from the bottom.

pretty chaotic and structureless[9]. It is no exaggeration that more than half of topics in an abstract algebra course were introduced while studying number-theoretic questions. It is expected that the reciprocity problem will provide directions for discoveries of new intrinsic structures and extrinsic structures and the relations among them.

Appendix A to 2: A Short List of Familiar Algebraic Concepts Motivated by Arithmetic

Recommended references:[6].

There were two impetuses for the developments of abstract algebra before the 20th century: i. the search for expressions of roots of polynomials over $\mathbb{Q}$(the only "numbers" known to the ancients), and ii. the Fermat's Last Theorem.

Some items related to i:

Groups

The concept of a permutation group was already in the air when Lagrange and Cauchy were studying the permutations of higher degree polynomials. Galois came up with his correspondence(duality) and solved the problem of solvability once for all. Incidentally, the study of Lie group was first motivated by the search of Galois theory for differential equations.

Finite fields

Some items related to ii:

Rings

Integral domains(P.I.D, U.F.D, Dedekind etc)

Ideals

Appendix B to 2: A Table from A Hypothetical Archaic Dictionary

The following is a table of items from each world in the analogy. All of them were essentially known to ancients like Kronecker and Hensel.

[9] It still is in view of the many open problems concerning the distribution of primes.

$\mathbb{Z}_K$	$X_{/\mathbb{F}_q}$	Σ_g
Prime ideals	Points	Points
One-dimensional as a commutative ring	One-dimensional as an algebraic variety	One-dimensional as a complex manifold
Ideals	Line bundles	Line bundles
$\mathfrak{p}$-adic Integers	Functions regular at a point p	Functions holomorphic at p
Fractions	Rational functions	Meromorphic functions
Prime ideal Q lying above a prime ideal $\mathfrak{p}$ in the base with ramification index ≥ 2	Branch points	Critical points
Factorizations of fractional ideals	Weil divisors of line bundles	Weil divisors of line bundles
Ramification index	Ramification index	Ramification index
Galois extensions	Smooth maps	Ramified covers

3 Algebraic Number Theory Background

We recall some basic algebraic number theory facts which are essential for later discussions. In particular, they are needed to state the main theorems of class field theory. It is hoped that the extra details will make them appear more geometric.

3.1 Ring-Theoretic Properties of $\mathbb{Z}_K$

Recommended reference: Andrew Sutherland's lecture notes for 18.785 - Number Theory I he taught in 2017([16]), especially the second and third notes.

An algebraic number α is said to be an algebraic integer if the ring $\mathbb{Z}[\alpha]$ is finitely generated as a $\mathbb{Z}$-module. $\mathbb{Z}_K$ is the set of algebraic integers contained in the number field K, which is a subring of K.

As a ring, $\mathbb{Z}_K$ is a Dedekind domain, which is a one-dimensional integrally closed Noetherian domain.More concretely:

1. Any non-zero prime ideal of $\mathbb{Z}_K$ is maximal, hence the domain is "one-dimensional".
2. Any fraction which is a root of a monic with coefficients in $\mathbb{Z}_K$ is already an element of $\mathbb{Z}_K$.

Existence and uniqueness of factorization hold for ideals in a general Dedekind domain.

3.2 Decompositions, Ramifications, and Inertia

Recommended reference: Chapter 3 and 4 of "Number Fields" by Daniel A. Marcus([14]).

For the purpose of class field theory, it is sufficient to consider Galois extensions.

Let L/K be a finite Galois extension, $\mathbb{Z}_K \to \mathbb{Z}_L$ is given by the inclusion map. Dually, this gives a morphism of scheme $(p, p^\sharp) : \operatorname{Spec} \mathbb{Z}_L \to \operatorname{Spec} \mathbb{Z}_K$.

Given a prime ideal $\mathfrak{p}$, taking $\mathfrak{p} \to \mathfrak{p}\mathbb{Z}_L$ corresponds to taking preimage $p^{-1}([\mathfrak{p}])$.

A consequence of the extension being Galois is that $\mathfrak{p}\mathbb{Z}_L = (Q_1...Q_r)^e$ for some positive integers r and e.

e is called the ramification index of $\mathfrak{p}$. $\mathfrak{p}$ is said to ramify in L if $e \geq 2$. Since a prime ideal ramifies in L iff it divides the discriminant ideal, the set of prime ideals ramified in L is finite.

The morphism $\mathbb{Z}_K \to \mathbb{Z}_L$ induces Galois extensions $\mathbb{Z}_L/Q_i$'s over $\mathbb{Z}_K/\mathfrak{p}$. The degree of extensions are all equal for a fixed $\mathfrak{p}$, denoted by f. To emphasize the roles of specific prime ideals, the notation $f(Q_i|\mathfrak{p})$ is sometimes used. This is the degree of inertia.

We have $[L : K] = n = efr^{(10)}$. The prime is said to ramify completely if $g = f = 1$, and to split completely if $e = f = 1$.

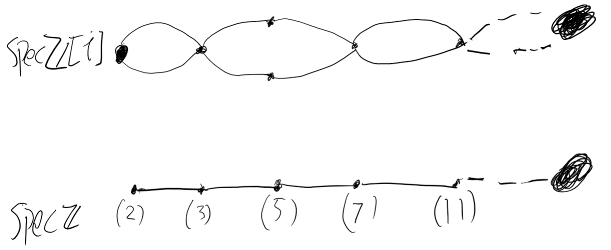


Figure 1: An example:$\operatorname{Spec} \mathbb{Z}[i] \to \operatorname{Spec} \mathbb{Z}$

In the above sketch, the large dots are the generic points [(0)]'s. The medium dot indicates the ramification point above the branch point [(2)]. The small dots represent the ordinary points.

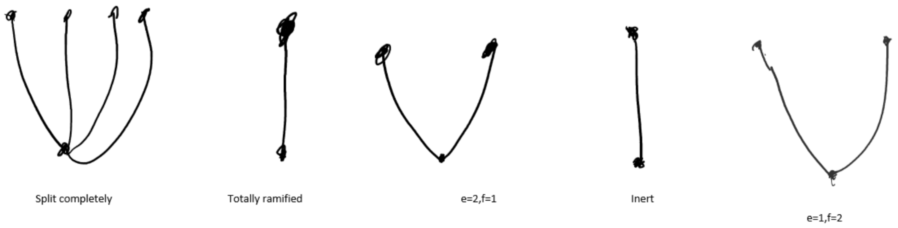
From the picture, it appears that points like [(3)],[(7)] and [(11)] are also branch points. One might then be tempted to conclude the arithmetic definition disagrees with geometric intuition. This discrepancy is rectified by considering the situation at the level of schemes.

Indeed, any one of these points $\mathfrak{p}$ has the one point set of preimage $\mathfrak{p}\mathbb{Z}[i] = Q$. The inertia degree is therefore 2. There is then a non-identity automorphism of the point $\operatorname{Spec} \mathbb{F}_Q$ commuting with the morphism between

[10] The notations e,f and r are due to Hilbert([12], part II, section 10), which don't seem to have special meanings. A competing notation is to replace r by g, which is a natural continuation of e and f.

closed points $\operatorname{Spec}\mathbb{F}_Q \to \operatorname{Spec}\mathbb{F}_{\mathfrak{p}}$, so there are enough lifts. Such an extra automorphism is unavailable for $p^{-1}([(2)]) = [(1+i)]$.

In a sense which can be made precise, the prime lying above an inert prime is a refinement of its image, whereas a branch point can be thought of as a thickening of a ramification point above it.



All possible splittings in a degree 4 Galois extension

We can also discuss ramifications of Archimedean places. A real place v ramifies in L if it admits an extension to an imaginary Archimedan valuation of L. The imaginary places never ramify.

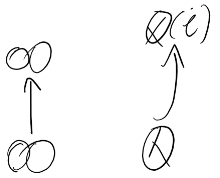
Here is a possible nonsensical question: Does it make sense to say real places all have degree of inertia 1? What does that even mean?

Example 3.1 (A Ramified Real Place)**.** Consider the Galois extension $\mathbb{Q}(i)/\mathbb{Q}$. $\mathbb{Q}$ only has one Archimedean place, given by the unique complex embedding, which is real. We denote this prime place by ∞. $\mathbb{Q}(i)$ also has only one Archimedean place, because the only two complex embeddings it possesses induce the same absolute value. Moreover, this Archimedean place of $\mathbb{Q}(i)$ is imaginary, which we also denote by ∞.

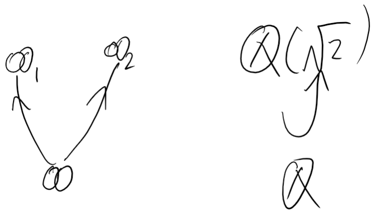
Since the only extension of the real ∞ from below is the imaginary ∞ of $\mathbb{Q}(i)$, ∞ of $\mathbb{Q}$ necessarily ramifies in $\mathbb{Q}(i)$.

Example 3.2 (An Unramified Real Place)**.** Consider this time the Galois extension $\mathbb{Q}(\sqrt{2})/\mathbb{Q}$. $\mathbb{Q}(\sqrt{2})$ has only two Archimedean places, both real, given by $a_0 + a_1\alpha \to |a_0 + a_1\sqrt{2}|$ and $a_0 + a_1\alpha \to |a_0 - a_1\sqrt{2}|$, where α is a root of the polynomial $x^2 - 2$.

Since both of them are extensions of ∞ of $\mathbb{Q}$, it is unramified in $\mathbb{Q}(\sqrt{2})$.



An example of ramified real place



An Example of unramified real place

It is actually a bad habit to choose a fixed complex embedding like $\mathbb{Q}(i)$ and $\mathbb{Q}(\sqrt{2})$, because they are non-canonical. I hereby confess my sin but promise I will definitely do similar things in the future whenever convenient.

3.3 Valuations and Absolute Values

There is a complete classification of valuations for global fields. For number fields, these are the Archimedean valuations given by the complex embeddings and the non-Archimedean ones given by the non-zero prime ideals(the so-called $\mathfrak{p}$-adic valuations). This result is due to Ostrowski(See chapter 4 of [2] for more details.). On the other hand, function fields do not have Archimedean valuations. This is an important difference which in many instances prevents the number field-function field analogy from being a literal dictionary.

Let K be a global field, denote by $\mathrm{Val}(K)$ the set of equivalent classes of valuations of K. The elements of $\mathrm{Val}(K)$ are sometimes called prime places. It is sometimes convenient to distinguish the two terminologies by introducing the set of prime places $\mathrm{Pl}(K)$ whose elements are in bijection with $\mathrm{Val}(K)$ via $v \leftrightarrow \mathfrak{p}_v$.

Let K_v be the completion of K with respect to $|\cdot|_v$. For v non-Archimedean(which can be any of the valuations when K is a function field), $\mathbb{Z}_v$ is defined to be the closed unit disc of K_v. The group of units U_v consists of elements with norm exactly 1.

It can be verified that $\mathbb{Z}_v$ is a local ring, i.e., it has a unique maximal ideal m_v. This is why p-adic fields are also called local number fields. In addition to being local, the ring of integers of a local field is a discrete valuation ring(DVR), with the discrete valuation given by v. This in particular implies they are PIDs(*Consult 11.1 of [9] for more details. We will refer to that section when studying local fields.*). Any generator of the unique maximal ideal of a DVR is called an uniformizer. For a positive integer n, the n-th (higher) unit group $U_v^{(n)}$ is the subgroup $1 + m_v^n$ of U_v.

3.4 Adeles and Ideles

The ring of finite adeles[11] $\mathbb{A}_{K,\text{fin}}$ is obtained by taking restricted direct product[12] of $\{(K_v, \mathbb{Z}_v)\}_{v<\infty}$. The unit group of $\mathbb{A}_{K,\text{fin}}$ is the group of finite ideles [13] $J_{K,\text{fin}}$[14] which is obtained by taking restricted direct product of $\{(K_v^\times, U_v)\}_{v<\infty}$. $\mathbb{A}_{K,\text{fin}}$ and $J_{K,\text{fin}}$ are equipped with the restricted direct product topology. While the latter is a subset of the former, its topology is NOT the same as the one given by the subspace topology. *Verify, for example, $J_{K,fin}$ is not a topological group with the subspace topology.*

Now, suppose K has $r_1 + 2r_2$ complex embeddings, where r_1 is the number of totally real embeddings, and $2r_2$ is the number of imaginary embeddings(which come in pairs). The infinite components $\mathbb{A}_{K,\infty}$ and $J_{K,\infty}$ are $\mathbb{R}^{r_1} \times \mathbb{C}^{r_2}$ and $(\mathbb{R}^\times)^{r_1} \times (\mathbb{C}^\times)^{r_2}$ respectively.

$\mathbb{A}_K = \mathbb{A}_{K,\infty} \times \mathbb{A}_{K,\text{fin}}$ and $J_K = J_{K,\infty} \times J_{K,\text{fin}}$ equipped with direct product topology.

Given a modulus $\mathfrak{M}$, we define a collection of neighbourhoods $L_{\mathfrak{M}}(v(\mathfrak{p}))$[15] of 1 in $K_{v(\mathfrak{p})}$ for each $\mathfrak{p}|\mathfrak{M}$:

$$L_{\mathfrak{M}}(v(\mathfrak{p})) = \begin{cases} 1 + (\pi_{\mathfrak{p}})^{v_{\mathfrak{p}}(\mathfrak{M})} & \text{if } \mathfrak{p} < \infty, \\ \mathbb{R}_+^\times & \text{if } \mathfrak{p} \text{ is real.} \end{cases}$$

Collectively, we can define a neighbourhood $L_{\mathfrak{M}}$ of 1 in J_K componentwise:

$$a = (..., a_{\mathfrak{p}}...) \in L_{\mathfrak{M}} \iff a_{\mathfrak{p}} \in \begin{cases} L_{\mathfrak{M}}(v(\mathfrak{p})) \text{ if } \mathfrak{p} \mid \mathfrak{M}, \\ U_{\mathfrak{p}} \text{ if } \mathfrak{p} \nmid \mathfrak{M}. \end{cases}$$

In many ways, $\mathbb{A}_K$ and J_K contain all relevant arithmetic information of the number field K. The former sums up the additive information, while the latter amalgamates the multiplicative information.

Class field theory was initially proven in the ideal-theoretic language, and was (much) later rewritten in the adelic language. We hope to demonstrate that the two approaches are not as different as commonly perceived after all.

At the moment, the most visible advantage of the adelic language is that it provides compact descriptions for many local-to-global operations.

3.5 Class Groups

A number of class groups were first introduced while developing class field theory. Arithmetically, they are collections of congruence information

[11] Adele stands for additive idele.

[12] Recall the restricted direct product of family of pairs $\{(A_i, B_i)\}_{i \in I}$ with $B_i \subset A_i$ for each i in an index set I is the subset of $\Pi_{i \in I} A_i$ whose elements have all but finitely many entries in B_i.

[13] Idele stands for Ideal element.

[14] J probably stands for Jacobian which is closely related to its geometric counter-part.

[15] These are called the local groups in the geometric setting.

of the integer ring $\mathbb{Z}_K$. Geometrically, they are moduli spaces of certain restricted classes of line bundles over $\operatorname{Spec}\mathbb{Z}_K$ [16].

To fix notations,we quickly recall some definitions.

3.5.1 The Ideal-Theoretic Viewpoint

Definition 3.1 (Fractional Ideals)**.** $\mathcal{I}_K$ denotes the set of fractional ideals, which are formal quotients of non-zero ideals of $\mathbb{Z}_K$.

Definition 3.2 (Principal Fractional Ideals)**.** $\mathcal{P}_K$ denotes the set of principal non-zero fractional ideals, which are fractional ideals of the form (α) where $\alpha \in K^\times$. (α) is obtained by first writing $\alpha = \frac{x}{y}$, where x and y are in $\mathbb{Z}_K$, then $(\alpha) := \frac{(x)}{(y)} \in \mathcal{I}_K$.

Exercise:Check this definition is independent of the choices of x and y.

Definition 3.3 (Norm Ideal of A L-Fractional Ideal)**.** Suppose L/K is a finite extension, and $\mathfrak{a}$ is a L-fractional ideal, the norm ideal $N_{L/K}(\mathfrak{a})$ is the K-fractional ideal generated by the norms of elements in $\mathfrak{a}$.

More generally, if $\mathcal{I}$ is a subgroup of $\mathcal{I}_L$, the norm group of $\mathcal{I}$ is the subgroup of $\mathcal{I}_K$ generated by the norms of elements in $\mathcal{I}$.

Definition 3.4 (Modulus of K)**.** A modulus[17] $\mathfrak{m}$ is formal product $\prod_{\mathfrak{p}\in \mathrm{Pl}(K)} \mathfrak{p}^{v_\mathfrak{p}(\mathfrak{m})}$ with the following properties:

1. $v_\mathfrak{p}(\mathfrak{m}) \geq 0$ for all prime place $\mathfrak{p}$, and is 0 for all but finitely many of them.

2. $v_\mathfrak{p}(\mathfrak{m}) = 0$ when $\mathfrak{p}$ is imaginary Archimedean.

3. $v_\mathfrak{p}(\mathfrak{m})$ is at most 1 at a real Archimedean $\mathfrak{p}$.

It is often convenient to factor $\mathfrak{m} = \mathfrak{m}_\infty \mathfrak{m}_{\text{fin}}$, where $\mathfrak{m}_\infty$ is the infinite component and $\mathfrak{m}_{\text{fin}}$ is the finite component.

The support $\operatorname{supp}\mathfrak{m}$ of $\mathfrak{m}$ is the set of prime places with positive multiplicities, which can be represented by the divisor given by their formal product each with multiplicity 1.

Notation 3.1. $\mathcal{I}_{K,\mathfrak{m}}$ denotes the group of fractional ideals whose reduced fractions do not contain any factors of $\mathfrak{m}$.

Notation 3.2. Write $\mathfrak{p}_\sigma$ for the prime place associated to the valuation σ, and $\mathfrak{p}_{K,\mathbb{R}} := \prod_{\sigma \text{ is real}} \mathfrak{p}_\sigma$.

[16] Actually, it is not so straightforward to make this precise.

[17] Sometimes the term effective divisor is used, but the condition on the Archimedean places are stronger than just being non-negative. Another geometrically suggestive name is cycle.

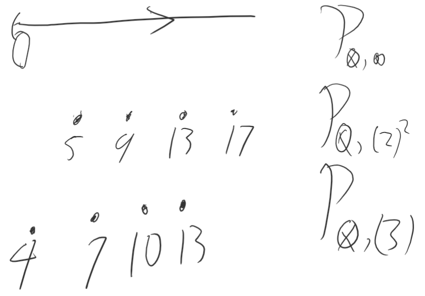
Notation 3.3. For $\alpha \in K$,by $\alpha \equiv 1 \bmod \mathfrak{m}$, we mean $\alpha \equiv 1 \bmod \mathfrak{p}^{v_{\mathfrak{p}}(\mathfrak{m})}$. For σ real, $\alpha \equiv 1 \bmod \mathfrak{p}_\sigma :\iff \sigma(\alpha) > 0$. We say α is totally positive if $\alpha \equiv 1 \bmod \mathfrak{p}_{K,\mathbb{R}}$.

Notation 3.4. $\mathcal{P}_{K,\mathfrak{m}} = \{(\alpha) : \alpha \in K, \alpha \equiv 1 \bmod \mathfrak{m}\}$ and $\mathcal{P}^+_{K,\mathfrak{m}} = \{(\alpha) : \alpha \in K, \alpha \equiv 1 \bmod \mathfrak{p}_{\mathbb{R}}\mathfrak{m}_{\text{fin}}\}$.

Definition 3.5. The norm group $N_{L/K}(\mathfrak{M})$ given by a modulus $\mathfrak{M}$ is the subgroup generated by the norms of L-fractional ideals prime to the extensions of divisors of $\mathfrak{M}$ in $\mathcal{I}_L$.

Definition 3.6. $\mathrm{Cl}_{K,\mathfrak{m}} = \mathcal{I}_{K,\mathfrak{m}}/\mathcal{P}_{K,\mathfrak{m}}$ and $\mathrm{Cl}^+_{K,\mathfrak{m}} = \mathcal{I}_{K,\mathfrak{m}}/\mathcal{P}^+_{K,\mathfrak{m}}$. The former is called the ray class group associated to $\mathfrak{m}$, and the latter is called the restricted ray class group associated to $\mathfrak{m}$.

Note that the restricted ray class group is bigger than the ray class group for a general modulus $\mathfrak{m}$.


0
$\mathcal{P}_{\mathbb{Q},\infty}$
5 9 13 17
$\mathcal{P}_{\mathbb{Q},(2)^2}$
4 7 10 13
$\mathcal{P}_{\mathbb{Q},(3)}$

Here are points on several "rays" of $\mathbb{Q}$. More generally, any $\mathcal{P}_{K,\mathfrak{m}}$ is an intersection of rays.

The term "class field theory" probably refers to the fact that it is a theory relating these ray class groups of a number field K with abelian overfields of K.

3.5.2 The Adelic Viewpoint

Let J_K be the group of ideles of the field K, then the multiplicative group $K^\times$ can be embedded in J_K diagonally. We can then define the idele class group.

Definition 3.7 (The idele class group C_K)**.** The idele class group C_K of a global field K is defined to be the quotient $J_K/K^\times$.

3.6 The Frobenius Maps

Suppose now L/K is a finite Galois extension, and $\mathfrak{p}$ does not ramify in L. For each prime ideal Q lying above $\mathfrak{p}$, we can define $\mathrm{Frob}(Q|\mathfrak{p}) \in \mathrm{Gal}(L/K)$ associated to the pair $(Q, \mathfrak{p})$.

Start with the following diagram of embeddings:

$$\begin{tikzcd}
 & L_Q \\
L \arrow[ur] & K_{\mathfrak{p}} \arrow[u] \\
K \arrow[u] \arrow[ur] &
\end{tikzcd}$$

Fix a choice of uniformizers π_Q and $\pi_{\mathfrak{p}}$ of $\mathbb{Z}_Q$ and $\mathbb{Z}_{\mathfrak{p}}$ respectively,we can lift the Frobenius endomorphism[18] of the residue field $\mathbb{Z}_Q/\pi_Q$ over $\mathbb{Z}_{\mathfrak{p}}/\pi_{\mathfrak{p}}$ to a ring automorphism of $\mathbb{Z}_Q$ over $\mathbb{Z}_{\mathfrak{p}}$ and then extend to a field automorphism of L_Q over $K_{\mathfrak{p}}$, which restricts to a field automorphism of L over K.

Concretely, the lift to L_Q is given by the corresponding action on the coefficients(which we identify with the residual field $\mathbb{Z}_Q/\pi_Q$) of the Laurent series. Since it fixes $K_{\mathfrak{p}}$(hence K), it restricts to an automorphism of L over K.

Definition 3.8 ($\mathrm{Frob}(Q|\mathfrak{p})$)**.** $\mathrm{Frob}(Q|\mathfrak{p})$ is defined to be this lift.

Question:What goes wrong with the argument if the prime $\mathfrak{p}$ ramifies?

Remark 3.1. *It is immediate that Frob$(Q|\mathfrak{p})$ is trivial iff $\mathfrak{p}$ splits completely.*

If Q_1 and Q_2 are prime ideals lying above an unramified prime ideal $\mathfrak{p}$, then Q_1 and Q_2 are conjugate to each other: $\exists \sigma \in \mathrm{Gal}(L/K)$ such that $\sigma(Q_1) = Q_2$. For the corresponding Frobenius maps, $\mathrm{Frob}(\sigma(Q_1)|\mathfrak{p}) = \sigma \mathrm{Frob}(Q_1|\mathfrak{p})\sigma^{-1}$.

An easy but important observation is that $\mathrm{Frob}(Q|\mathfrak{p})$ is independent of the choice of prime ideal Q lying above $\mathfrak{p}$ when the extension is abelian. Therefore, suppressing Q and denote it using $\mathrm{Frob}_{\mathfrak{p}}$ will not cause confusion.

When the extension L/K is non-abelian, the notation $\mathrm{Frob}_{\mathfrak{p}}$ refers to the conjugacy class of any one of the $\mathrm{Frob}(Q|\mathfrak{p})$'s in $\mathrm{Gal}(L/K)$.

Example 3.3 ($\mathrm{Frob}_{(3)}$ for $\mathbb{Q}(i)/\mathbb{Q}$)**.** We know (3) inerts in $\mathbb{Q}(i)$. Therefore, $\mathbb{Z}[i]/3\mathbb{Z}[i]$ is the degree two extension of $\mathbb{Z}/(3)$.

$\mathrm{Frob}_{(3)}$ is given by cubing $3\mathbb{Z}[i]$-units. Note that i is a $3\mathbb{Z}[i]$-unit. So $i \to i^3 = -i$ under the action of $\mathrm{Frob}_{(3)}$.

Since the image of the primitive element i determines a Galois action in $\mathrm{Gal}(\mathbb{Q}(i)/\mathbb{Q})$ completely, we see $\mathrm{Frob}_{(3)}$ is the complex conjugation.

[18] Recall the Frobenius endomorphism of $\mathbb{F}_{q^f}/\mathbb{F}_q$ is given by $x \to x^q$.

Example 3.4 (Frob$_{(5)}$ for $\mathbb{Q}(i)/\mathbb{Q}$)**.** The prime ideal (5) splits in $\mathbb{Z}[i]$: $5\mathbb{Z}[i] = (1 + 2i)(1 - 2i)$.

We check $\mathbb{Z}[i]/(1 + 2i) \cong \mathbb{Z}/(5)$, which will imply the field extension of the residue field is trivial. The Frobenius map is then necessarily the identity, so is its lift Frob$_{(5)}$ to Gal$(\mathbb{Q}(i)/\mathbb{Q})$.

Let j be the mod-$(1 + 2i)$ image of i. Then, the relation $1 + 2j = 0$ in $\mathbb{Z}[i]/(1+2i)$ implies that $j = 2$. So all elements in $\mathbb{Z}[i]/(1+2i)$ have integral representatives. We see from this that the image of $\mathbb{Z}$ under mod-$(1 + 2i)$ reduction is exactly $\mathbb{F}_5 \cong \mathbb{Z}/(5)$, as claimed.

4 Chebotarev's Density Theorem

Recommended reference: chapter VII, section 13 of [15], section 2 of [5].

Solving the reciprocity problem is often described as finding splitting laws of prime ideals in terms of intrinsic arithmetic. This is justified by the Chebotarev's density theorem. More precisely, it is one of its corollaries we will need.

Theorem 4.1 (A corollary of the Chebotarev's density theorem)**.** *A finite Galois extension L/K is uniquely determined by the set Spl(L/K) of prime ideals in Z_K which split completely in L.*

Therefore, an intrinsic description of splitting laws of primes of K is literally a solution to the reciprocity problem.

A different kind of splittings which is frequently mentioned in literature is the splitting of the mod-$\mathfrak{p}$ reductions of irreducible integral monics in $\mathbb{Z}_K[x]$, where $\mathfrak{p}$ ranges over all prime ideals of $\mathbb{Z}_K$.

The splittings of prime ideals and splittings of integral monics are related as follows:

Suppose $f(x) \in \mathbb{Z}_K[x]$ is an integral monic, and L is the splitting field of f. L/K is finite Galois. For any prime ideal $\mathfrak{p}$ of K outside of a finite set of exceptional prime ideals, the splitting of mod-$\mathfrak{p}$ reduction of f and the splitting of of $\mathfrak{p}$ in $\mathbb{Z}_L$ determine each other.

For more details about this correspondence, see appendix.

5 Main Theorems of Class Field Theory in Ideal-Theoretic Language

We now state the main theorems of class field theory. The goal is to describe all finite abelian extensions of a number field K in terms of its congruence information.

There is not an universal agreement on what the fundamental theorems are, because the results can be organized differently. Nevertheless, it is hard to refute the claim that the existence and isomorphy theorems are the essence of Class field theory, which together describe all abelian extensions of a number field.

Let L/K be an abelian extension, and $\mathfrak{M}$ be the product of all prime places of K ramifying in L, The Artin reciprocity map $\mathcal{A} : \mathcal{I}_{K,\mathfrak{M}} \to \mathrm{Gal}(L/K)$ is defined by extending $\mathfrak{p} \to \mathrm{Frob}_{\mathfrak{p}}$ multiplicatively. Another commonly used notation for the reciprocity map is the Artin symbol $(-, L/K)$ named after Emil Artin.

5.1 Isomorphy

For an abelian extension L/K, the Artin reciprocity map $(-, L/K) : \mathcal{I}_{K,\mathfrak{M}} \to \mathrm{Gal}(L/K)$ is surjective. This result is already highly non-trivial and requires a lot of efforts to prove: it asserts that the Galois data of the extension L/K is contained in $\mathcal{I}_{K,\mathfrak{M}}$, a group which is completely determined by the arithmetic of K [19].

Moreover, the kernel of this map can be described by a unique modulus $\mathfrak{f}(L/K) = \mathfrak{f}$ of K, called the conductor of L/K, with the following properties:

1. $\ker(-, L/K) = \mathcal{P}_{K,\mathfrak{f}} N_{L/K}(\mathfrak{f}) \bigcap \mathcal{I}_{K,\mathfrak{M}} = \mathcal{P}_{K,\mathfrak{M}} N_{L/K}(\mathfrak{M})$.
2. For any admissible modulus $\mathfrak{M}$ of K with respect to the extension L/K, that is, a modulus $\mathfrak{M}$ such that $W_{\mathfrak{M}}(v) \subset N_{L_w/K_v}(L_w^\times)$ for every extension w of $v = v(\mathfrak{p})$ with $\mathfrak{p} \mid \mathfrak{M}$, we have $I_{K,\mathfrak{M}}/\mathcal{P}_{K,\mathfrak{M}} N_{L/K}(\mathfrak{M}) \cong I_{K,\mathfrak{f}}/\mathcal{P}_{\mathfrak{f}} N_{L/K}(\mathfrak{f})$.

The term “isomorphy” refers to the isomorphism between the Galois group $\mathrm{Gal}(L/K)$ and and the quotient group $I_{K,\mathfrak{f}}/\mathcal{P}_{\mathfrak{f}} N_{L/K}(\mathfrak{f})$.

5.2 Ramification

There is also a simple and intrinsic description of the prime places ramified in L in terms of the conductor $\mathfrak{f}(L/K)$: a prime place $\mathfrak{p}$ ramifies in L iff $\mathfrak{p} \mid \mathfrak{f}$.

5.3 Splitting

By remark 3.1, we see that a prime ideal $\mathfrak{p}$ splits completely in L iff it is contained in $\mathcal{P}_{K,\mathfrak{f}} N_{L/K}(\mathfrak{f}) \subset \mathcal{I}_{K,\mathfrak{f}} \subset \mathcal{I}_K$. This is clearly a piece of K-data.

By the Chebotarev's density theorem, $\mathcal{P}_{K,\mathfrak{f}} N_{L/K}(\mathfrak{f})$ alone already determines the abelian extension L/K. The isomorphy theorem complements the splitting theorem by describing the group $\mathrm{Gal}(L/K)$.

[19] While it is true that the determination of $\mathfrak{M}$ requires knowledge of ramification data of L/K, the modulus $\mathfrak{M}$ by itself is a congruence data of K and has no a priori connection to the extension L.

5.4 Existence

For any modulus $\mathfrak{M}$ of K, and any subgroup H lying in the (not necessarily strictly) descending tower $\mathcal{I}_{K,\mathfrak{M}} \supset H \supset \mathcal{P}_{K,\mathfrak{M}}$, there is a unique abelian extension $L(H)/K$ corresponding to H.

Moreover, the kernel of the Artin reciprocity map $(, L(H)/K)$ is $\mathcal{P}_{\mathfrak{M}} N_{L(H)/K}(\mathfrak{M})$, so that $\mathrm{Gal}(L(H)/K) \cong \mathcal{I}_{K,\mathfrak{M}}/H$ and $\mathfrak{M}$ is an admissible modulus.

5.5 Principalization

Let $\mathfrak{m} = 0$, by the existence theorem, we have a unique abelian extension L/K in which none of the prime places ramifies. L is called the Hilbert class field of K.

Theorem 5.1 (Principalization)**.** *All ideals of K become principal after pulling back to its Hilbert class field L. Geometrically, this means all line bundles over* $\operatorname{Spec}\mathbb{Z}_K$ *become untwisted after pulling them back along* $\operatorname{Spec}\mathbb{Z}_L \to \operatorname{Spec}\mathbb{Z}_K$.

5.6 Functoriality

6 Main Theorems of Class Field Theory in Adelic Language

7 Fundamental Groups and Galois Groups

There is a way to further geometrize the arithmetic side instead of appealing to imperfect analogy. The result will be a theorem rather than a heuristic that Galois groups are related to fundamental groups(20).

8 The Strategy

Motivated by $\pi_1^{ab} \cong H_1$ for nice(e.g. cellular) spaces, and $H_1 \cong H^1$ for complex curves, we expect a cohomological approach to class field theory.

(20) Or the other way around, depending on your background.

8.1 Local Class Field Theory

8.2 From Local to Global

9 Scheme-Theoretic Geometrizations of the Main Theorems of (Local) Class Field Theory

10 Twentieth-Century Developments Inspired by Function Theory

11 Appendix

11.1 Background of Complex Curves

Recommended references:[4],[7],[8].

In order to solidify the number field-function field analogy with real mathematics, we study the analogous basic notions in the setting of complex algebraic curves.

11.2 Valuation-Theoretic Approach to Function Fields

11.3 Splittings of Prime Ideals in Terms of Reductions of Polynomials

Recommended reference:[3].

References

[1] Nancy Childress. *Class field theory.* Springer Science & Business Media, 2008.

[2] Henri Cohen. *Number theory: Volume I: Tools and diophantine equations*, volume 239. Springer Science & Business Media, 2008.

[3] Henri Cohen. *A course in computational algebraic number theory*, volume 138. Springer Science & Business Media, 2013.

[4] Harvey Cohn. *Introduction to the construction of class fields.* Courier Corporation, 1994.

[5] Keith Conrad. History of class field theory. *This unpublished essay is available online as a PDF file at www. math. uconn. edu/˜ kconrad/blurbs/gradnumthy/cfthistory. pdf*, 2001.

[6] Al Cuoco and Joseph Rotman. *Learning Modern Algebra*, volume 23. MAA, 2013.

[7] Simon Donaldson. *Riemann surfaces.* Oxford University Press, 2011.

[8] Régine Douady and Adrien Douady. *Algebra and Galois Theories.* Springer, 2020.

[9] David Eisenbud. *Commutative Algebra: with a view toward algebraic geometry*, volume 150. Springer Science & Business Media, 2013.

[10] Robin Hartshorne. *Algebraic geometry*, volume 52. Springer Science & Business Media, 2013.

[11] Allen Hatcher. *Algebraic Topology.* Cambridge University Press, 2002.

[12] David Hilbert. Die theorie der algebraischen zahlkörper. In *Gesammelte Abhandlungen*, pages 63–363. Springer, 1932.

[13] Martin H Krieger. A 1940 letter of andré weil on analogy in mathematics. *Notices of the AMS*, 52(3), 2005.

[14] Daniel A Marcus. *Number Fields.* Springer, 2018.

[15] Jürgen Neukirch. *Algebraic number theory.* Springer, 1999.

[16] Andrew Sutherland. 18.785 algebraic number theory i. URL: `https://math.mit.edu/classes/18.785/2017fa/index.html`.

[17] Ravi Vakil. The rising sea: foundations of algebraic geometry. *preprint*, 2017.

[18] André Weil. *Basic number theory.* Springer, 1973.