Juvitop CFT Notes

Niven Achenjang

February 23, 2021

Contents

Introduction

These are notes for my Juvitop talk. Our goal is to give an overview of class field theory, introducing the main statements and hopefully discussing enough results to understand the uses of CFT in this paper [FGV20] by Feng-Galatius-Venkatesh.

Since our primary motivation is understanding the paper of Feng-Galatius-Venkatesh, our main focus is arriving at the statements of the main theorems of (global) class field theory, and then seeing what these get us. To be safe, we begin by quickly recalling some background material[1] needed to understand the statements of the main results of class field theory. Afterwards, we give the main results, and then discuss how to think about them and how to derive some of their consequences.

The preliminaries section tries not to say much more than is needed. For more details, included proofs of statements only claimed here, see the last two chapters of [Mil20a] or the first two chapters of [Ser79]. Throughout these notes, K will denote a number field (and never a global function field).

1 Preliminaries

Fix a number field K, so $K/\mathbb{Q}$ is some finite extension. The goal of class field theory is to understand $\mathrm{Gal}(\overline{K}/K)^{\mathrm{ab}} = \mathrm{Gal}(K^{\mathrm{ab}}/K)$, the abelianization of the absolute Galois group of K. Here, $\overline{K}$ is a choice

[1] Section 1 is kinda unorganized. It's just a Hodge podge of stuff that seems like it may be useful for section 2

of algebraic closure of K, and

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

is the maximal abelian extension of K, the union of all finite, abelian intermediate extensions L of $\overline{K}/K$.

In order to understand $\mathrm{Gal}(K^{\mathrm{ab}}/K)$, a potentially good first step is being able to produce elements of Galois groups of number fields.

1.1 Frobenius and Ramification

Notation 1.1. We let $\mathscr{O}_K$ denote the ring of integers of K, the integral closure of $\mathbb{Z} \subset K$.

Remark 1.2. The ring $\mathscr{O}_K$ is a Dedekind domain, which, among other things, means that any ideal $I \subset \mathscr{O}_K$ uniquely factors

$$I = \prod_{i=1}^{g} \mathfrak{p}_i^{e_i}$$

as a finite product of prime ideals.

Fact. Let L/K be some finite extension, and fix a prime $\mathfrak{p} \subset \mathscr{O}_K$ of K. Then this factors upstairs as

$$\mathfrak{p}\mathscr{O}_L = \prod_{i=1}^{g} \mathfrak{P}_i^{e_i},$$

with $\mathfrak{P}_i$ a prime of L. Let $k_{\mathfrak{p}} = \mathscr{O}_K/\mathfrak{p}$, and let $\kappa_{\mathfrak{P}_i} = \mathscr{O}_L/\mathscr{P}_i$. Set $f_i := [\kappa_{\mathfrak{P}_i} : k_{\mathfrak{p}}]$. Then, one has $[L : K] = \sum_{i=1}^{g} e_i f_i$. We call e_i the **ramification degree** of $\mathfrak{P}_i$ over $\mathfrak{p}$, and f_i the **residue field degree** of $\mathfrak{P}_i$ over $\mathfrak{p}$. We say $\mathfrak{p}$ is

- **unramified** in L/K if $e_i = 1$ for all i.
- **totally ramified** in L/K if $e_1 = n$.
- **totally split** in L/K if $g = n$.
- **inert** in L/K if $f_1 = n$.

In the above situation, say L/K is a Galois extension. We still have $\mathfrak{p} \subset \mathscr{O}_K$ a prime downstairs, and a list $\{\mathfrak{P}_1, \mathfrak{P}_2, \ldots, \mathfrak{P}_g\}$ of primes above $\mathfrak{p}$. Let $G = \mathrm{Gal}(L/K)$ be the Galois group. Then, for any i and any $\sigma \in G$, $\sigma(\mathfrak{P}_i)$ is a prime above $\sigma(\mathfrak{p}) = \mathfrak{p}$, so $\sigma(\mathfrak{P}_i) = \mathfrak{P}_j$ for some j, and $G \curvearrowright \{\mathfrak{P}_i\}_{i=1}^{g}$. This action is in fact transitive, so all ramification and residue field degrees above $\mathfrak{p}$ are equal (say to e, f, respectively), and one writes $n := [L : K] = efg$.

In the same situation, choose some prime $\mathfrak{P} \in \{\mathfrak{P}_1, \ldots, \mathfrak{P}_g\}$ above $\mathfrak{p}$. We define its **decomposition group** to be

$$D(\mathfrak{P} \mid \mathfrak{p}) := \{\sigma \in G : \sigma(\mathfrak{P}) = \mathfrak{P}\}$$

the stabilizer of $\mathfrak{P}$ under the Galois action. Recall the notation $k_{\mathfrak{p}} = \mathscr{O}_K/\mathfrak{p}$ and $\kappa_{\mathfrak{P}} = \mathscr{O}_L/\mathfrak{P}$. There is a natural map $D(\mathfrak{P} \mid \mathfrak{p}) \to \mathrm{Gal}(\kappa_{\mathfrak{P}}/k_{\mathfrak{p}})$ sending $\sigma \in D(\mathfrak{P} \mid \mathfrak{p})$ to the automorphism $\overline{\sigma} : \overline{x} \mapsto \overline{\sigma(x)}$ for any $x \in \mathscr{O}_L$ with reduction $\overline{x} \in \kappa_{\mathfrak{P}}$.

Fact. The map $D(\mathfrak{P} \mid \mathfrak{p}) \to \mathrm{Gal}(\kappa_{\mathfrak{P}}/k_{\mathfrak{p}})$ is a surjection.

We define the **inertia group** $I(\mathfrak{P} \mid \mathfrak{p}) := \ker(D(\mathfrak{P} \mid \mathfrak{p}) \to \mathrm{Gal}(\kappa_{\mathfrak{P}}/k_{\mathfrak{p}}))$, so we have an exact sequence

$$1 \longrightarrow I(\mathfrak{P} \mid \mathfrak{p}) \longrightarrow D(\mathfrak{P} \mid \mathfrak{p}) \longrightarrow \mathrm{Gal}(\kappa_{\mathfrak{P}}/k_{\mathfrak{p}}) \longrightarrow 1.$$

Remark 1.3. Recall that $n = \#G = efg$, and G acts transitively on $\{\mathfrak{P}_1, \ldots, \mathfrak{P}_g\} \ni \mathfrak{P}$. By orbit-stabilizer, this means that $\#D(\mathfrak{P} \mid \mathfrak{p}) = \#\operatorname{Stab}_G(\mathfrak{P}) = \#G/g = ef$. Furthermore, by definition, $f = \#\mathrm{Gal}(\kappa_{\mathfrak{P}}/k_{\mathfrak{p}})$, so $e = \#I(\mathfrak{P} \mid \mathfrak{p})$.

Now suppose $\mathfrak{p}$ is unramified, so $e = 1$. By the above remark, in this case, $I(\mathfrak{P} \mid \mathfrak{p}) = 1$ is trivial, so $D(\mathfrak{P} \mid \mathfrak{p}) \xrightarrow{\sim} \mathrm{Gal}(\kappa_{\mathfrak{P}}/k_{\mathfrak{p}})$ is an isomorphism. The latter is a Galois group of an extension of finite fields, is isomorphic to $\mathbb{Z}/f\mathbb{Z}$ with canonical generator

$$\kappa_{\mathfrak{P}} \ni x \mapsto x^{\#k_{\mathfrak{p}}}.$$

The unique lift $\mathrm{Frob}_{\mathfrak{P}} \in D(\mathfrak{P} \mid \mathfrak{p}) \subset G$ of this generator to $D(\mathfrak{P} \mid \mathfrak{p})$ is called the **Frobenius** at $\mathfrak{P}$. This gives one way of producing Galois elements.

Remark 1.4. Still assuming $\mathfrak{p}$ is unramified, note that Frobenius $\mathrm{Frob}_{\mathfrak{P}} \in G$ generates the decomposition group $D(\mathfrak{P} \mid \mathfrak{p})$, so the splitting behavior of $\mathfrak{p}$ can be determined by knowing the order of Frobenius in the Galois group $G = \mathrm{Gal}(L/K)$. In particular, if $\mathrm{Frob}_{\mathfrak{P}} = 1$ is trivial, then $f = \#D(\mathfrak{P} \mid \mathfrak{p}) = 1$, so $n = efg = g$ which means $\mathfrak{p}$ splits completely.

Note that Frobenius $\mathrm{Frob}_{\mathfrak{P}}$ depends on a choice of prime $\mathfrak{P}$ above $\mathfrak{p}$. There is not natural choice of such a prime, so we would prefer if it Frobenius depended only of $\mathfrak{p}$. If $\sigma \in G$ is an arbitrary Galois element, then the Frobenius element associated to $\sigma(\mathfrak{P})$ is the canonical generator of $D(\sigma(\mathfrak{P}) \mid \mathfrak{p}) = \mathrm{Stab}_G(\sigma(\mathfrak{P})) = \sigma \operatorname{Stab}_G(\mathfrak{P})\sigma^{-1}$. By canonicity (or an easy by hands argument), we see that $\mathrm{Frob}_{\sigma(\mathfrak{P})} = \sigma \mathrm{Frob}_{\mathfrak{P}} \sigma^{-1}$, so choosing a different prime above $\mathfrak{p}$ conjugates Frobenius. In particular, there is a well-defined *conjugacy class* $\mathrm{Frob}_{\mathfrak{p}} \subset G$ associated to the prime $\mathfrak{p}$ downstairs. Finally, if G is abelian, then every conjugacy class is a singleton, so we get a well-defined *element* $\mathrm{Frob}_{\mathfrak{p}} \in G$. For some reason, people sometimes instead use the cumbersome notation

$$\mathrm{Frob}_{\mathfrak{p}} =: \left(\frac{L/K}{\mathfrak{p}}\right) \in G.$$

This has all been part of the "global" story. In order to talk about class field theory, we will also need to know some of the "local" theory, so we do that next. Everything I claimed without proof here can be found e.g. in the first chapter of Serre's 'Local Fields' [Ser79].

1.2 Places and Local Fields

Instead of studying a global field, it is often useful to complete it in order to study things "one prime[2] at a time," e.g. every prime of K has corresponding decomposition/inertia groups in $\mathrm{Gal}(K^{\mathrm{ab}}/K)$, so it may make sense to understand $\mathrm{Gal}(K^{\mathrm{ab}}/K)$ by understanding each of these subgroups. To study one prime at a time, think about the passage from $\mathbb{Z}$ to $\mathbb{Z}_p$, the p-adics.

As before, fix a number field K.

[2] really, place

Definition 1.5. An **absolute value** on K is a function $|\cdot| : K \to \mathbb{R}_{\geq 0}$ such that $|a| = 0 \iff a = 0$, $|ab| = |a|\,|b|$, and $|a+b| \leq |a| + |b|$. We say two absolute values $|\cdot|, |\cdot|'$ on K are **equivalent**, dented $|\cdot| \sim |\cdot|'$, if there exists some $t > 0$ such that $|\cdot|^t = |\cdot|'$. A **place** is an equivalence class of absolute values.

Definition 1.6. An absolute value $|\cdot|$ is called **non-archimedean** if $|a+b| \leq \max(a, b)$ (with equality if $|a| \neq |b|$), or equivalently, if $|\mathbb{Z}| \subset \mathbb{R}$ is bounded. It is called **archimedean** if it is not non-archimedean.

Definition 1.7. Non-archimedean places are also called **finite places**, and we may denote that a place v is non-archimedean by writing $v \nmid \infty$. Archimedean places are also called **infinite places**, and we may denote that a place v is archimdean by writing $v \mid \infty$.

Theorem 1.8 (**Ostrowski**). *Let $|\cdot| : \mathbb{Q} \to \mathbb{R}_{\geq 0}$ be an absolute value. Then, one of the following holds,*

- *$|\cdot|$ is equivalent to the usual, archimedean absolute value $|\cdot|_\infty$ we all learned about long ago, i.e. $|a|_\infty = a$ if $a \geq 0$ and $|a|_\infty = -a$ if $a \leq 0$.; or*
- *There exists a (unique) prime p s.t. $|\cdot|$ is equivalent to the **p-adic absolute value** $|\cdot|_p$. This satisfies $|n|_p = p^{-\operatorname{ord}_p(n)}$ for any $n \in \mathbb{Z}$, where $\operatorname{ord}_p(n)$ is the largest e such that $p^e \mid n$.*

Notation 1.9. Given a place v of K, let $|\cdot|$ be some absolute value representing it. Then, $|\cdot|$ induce a metric $d(x, y) := |x - y|$ on K in the usual way, and we let K_v denote the completion of K with respect to this absolute value.

Example. Let v_∞ be the place of $\mathbb{Q}$ containing $|\cdot|_\infty$. Then $\mathbb{Q}_\infty = \mathbb{R}$. Let p be a prime, and let v_p be the place of $\mathbb{Q}$ containing $|\cdot|_p$. Then, $\mathbb{Q}_{v_p} = \mathbb{Q}_p$ is the p-adics.

In general, K_v will be some locally compact[3] field containing K as a dense subfield. Let u be the place on $\mathbb{Q}$ under v – i.e. pick a representative $|\cdot| : K \to \mathbb{R}_{\geq 0}$ of v and then let u be the place containing its restriction to $\mathbb{Q}$. Then, $K_v \supset \mathbb{Q}_u$ is a field extension. Furthermore, since K_v is locally compact, $[K_v : \mathbb{Q}_u] < \infty$. Hence, as a consequence of Ostrowski, we have the following partial classification

- Say v is an archimedean place. Then, $K_v = \mathbb{R}$ or $K_v = \mathbb{C}$. Indeed, v_∞ is the only archimedean place of $\mathbb{Q}$, so K_v must be some finite extension of $\mathbb{Q}_\infty = \mathbb{R}$.
- Say v is a non-archimedean place. Then, K_v is a finite extension of $\mathbb{Q}_p$ for some prime p.

In any case, we call K_v a **local field**. More intrinsically, a **local field** is a locally compact topological field which is complete with respect to some non-trivial absolute value.

Remark 1.10. Each place actually has a canonical choice of representative absolute value. Let v be a place of K. Since K_v is locally compact, it supports an additive Haar measure μ, unique up to scaling. For any $a \in K_v$, let μ_a be the measure defined by $\mu_a(S) := \mu(aS)$. Then, μ_a is easily seen to be a Haar measure, so there exists a unique scalar $c_a \in K^\times$ s.t. $\mu_a(S) = c_a\mu(S)$ for all $S \subset K_v$.[4] The assignment $|a|_v := c_a$ defines an absolute value $|\cdot|_v : K_v \to \mathbb{R}_{\geq 0}$. Both it and its restriction to K are called the **normalize absolute value** associated to v.

[3] Enough to show the closed unit ball is compact, and this follows from compactness of $[0, 1] \subset \mathbb{R}$ + completeness of K_v

[4] Technically, for all Borel subsets, but shhhhhh that doesn't matter

Exercise. The normalized absolute value on $\mathbb{R}$ is the usual one. However (since $\mathbb{C}$ is a 2-dimensional Euclidean space), the normalized absolute value on $\mathbb{C}$ is $|z| = z\overline{z}$, the square of the usual one.

Archimedean places are boring, so now fix a non-archimedean place v on K_v. We introduce the following heap of notation.

- $\mathscr{O}_v := \{a \in K_v : |a|_v \leq 1\}$ is called the **ring of integers** (or **valuation ring**) of K_v. This is a discrete valuation ring, i.e. a local PID.
- $\mathfrak{m}_v := \{a \in K_v : |a|_v < 1\}$ is the (unique) maximal ideal of $\mathscr{O}_v$. It is literally all the non-units in $\mathscr{O}_v$.
- $\kappa_v := \mathscr{O}_v/\mathfrak{m}_v$ is the residue field at v.

Let p be the rational prime such that $K_v \supset \mathbb{Q}_p$. Since K_v is a finite extension of $\mathbb{Q}_p$, it is not hard to show that $|K_v|_v \subset \mathbb{R}$ is a discrete subgroup. Choose some $\pi_v \in \mathfrak{m}_v$ with $|\pi_v|_v$ maximal. Then, $\mathfrak{m}_v = (\pi_v)$, and we call π_v a **uniformizer**. Any nonzero element of $a \in K_v^\times$ can be uniquely written in the form $a = u\pi_v^m$ for some $u \in \mathscr{O}_v^\times$ and $m \in \mathbb{Z}$. In particular, $|a|_v = |u|_v |\pi_v|_v^m = |\pi|_v^m$, so $|\cdot|_v$ is completely determined by its value on a uniformizer. Since $\pi_v\mathscr{O}_v = \mathfrak{m}_v$, letting μ be additive Haar measure on K_v, we see that

$$|\pi_v|_v \, \mu(\mathscr{O}_v) = \mu_{\pi_v}(\mathscr{O}_v) = \mu(\mathfrak{m}_v) \implies |\pi_v|_v = \mu(\mathfrak{m}_v)/\mu(\mathscr{O}_v).$$

At the same time, $\mathscr{O}_v = \bigsqcup_{\overline{a} \in \kappa_v} (a + \mathfrak{m}_v)$ is a disjoint union of $\#\kappa_v$ cosets of $\mathfrak{m}_v$, so

$$\mu(\mathscr{O}_v) = \sum_{\overline{a} \in \kappa_v} \mu(a + \mathfrak{m}_v) = \sum_{\overline{a} \in \kappa_v} \mu(\mathfrak{m}_v) = (\#\kappa_v)\mu(\mathfrak{m}_v) \implies |\pi_v|_v = (\#\kappa_v)^{-1}.$$

Now, note that $\mathfrak{p}_v := \mathfrak{m}_v \cap \mathscr{O}_K$ is a nonzero (e.g. it contains p fixed earlier) prime of $\mathscr{O}_K$. Furthermore, $(\mathscr{O}_K/\mathfrak{p}_v) \xrightarrow{\sim} \kappa_v$. In this way, associated to any non-archimedean place v of K is a nonzero prime $\mathfrak{p}_v$ of $\mathscr{O}_K$.

Remark 1.11. In the reverse direction, if $\mathfrak{p}$ is a nonzero prime of $\mathscr{O}_K$, then the localization $\mathscr{O}_{K,\mathfrak{p}} = (\mathscr{O}_K \setminus \mathfrak{p})^{-1}\mathscr{O}_K$ is a dvr. Hence, for any $a \in \mathscr{O}_K$, there is a unique $n \in \mathbb{Z}_{\geq 0}$, denote $\mathrm{ord}_\mathfrak{p}(a)$, such that $a\mathscr{O}_{K,\mathfrak{p}} = (\mathfrak{p}\mathscr{O}_{K,\mathfrak{p}})^n$. Thus, we get a $\mathfrak{p}$-adic absolute value defined by $|a|_\mathfrak{p} := (\#\mathscr{O}_K/\mathfrak{p})^{-\mathrm{ord}_\mathfrak{p}(a)}$.

Remark 1.12. The previous remark shows that non-archimedean places of K are in bijection with maximal ideals of $\mathscr{O}_K$. Archimedean places of K are in bijection with embeddings $\iota : K \hookrightarrow \mathbb{C}$, up to conjugation. On the one hand, such an embedding gives rise to an absolute value $|x|_\iota = |\iota(x)|$ where the latter is the usual Euclidean absolute value on $\mathbb{C}$. On the other hand, an archimedean place v gives an embedding $K \hookrightarrow K_v$, but $K_v = \mathbb{R}$ or $\mathbb{C}$, so we get an embedding $K \hookrightarrow K_v \hookrightarrow \mathbb{C}$.

Notation 1.13. Let L/K be an extension of number fields, and let w be a place of L. Let $v = w|_K$ be the place of K obtained by restricting w. In this situation, we say "w lies above v," and write $w \mid v$.

Remark 1.14. If L/K is a Galois extension of number fields, and v is a place on K, then there exists a (non-unique) place w of L above v. The **Decomposition group** $D(w \mid v) := \mathrm{Gal}(L_w/K_v)$, and this agrees with our earlier definition in the case that v is a non-archimedean place.[5] When v is non-

[5]Any Galois element $\sigma \in \mathrm{Gal}(L/K)$ fixing $\mathfrak{P}_w$ acts continuous w.r.t to the $|\cdot|_w$ absolute value, and so extends to an automorphism of the completion L_w, fixing K_v. Conversely, any $\tau \in \mathrm{Gal}(L_w/K_v)$ restricts to an automorphism of L (recall, L/K normal) which fixes $\mathfrak{P}_w \subset \mathscr{O}_L$. This is because one can show $|\sigma(\cdot)|_w = |\cdot|_w$ e.g. by showing there is a unique absolute value on L_w extending the one on K_v.

archimedean, we define the inertia group $I(w \mid v)$ as before. When v is archimedean, we define the **inertia group** $I(w \mid v) := D(w \mid v)$ to be equal to the decomposition group. That is, $I(w \mid v) = D(w \mid v) = \mathrm{Gal}(\mathbb{C}/\mathbb{R}), \mathrm{Gal}(\mathbb{C}/\mathbb{C})$, or $\mathrm{Gal}(\mathbb{R}/\mathbb{R})$ depending on if v, w are real or complex.

Definition 1.15. We say an archimedean place v of a number field K **ramifies** in L if it has non-trivial inertia group, i.e. if it is a real place with a complex place lying above it.

2 Global Class Field Theory

2.1 idèles

In order to state the main results of global class field theory, we need to introduce one more concept. This is that of ideles.

Definition 2.1. Fix a collection of locally compact Hausdorff abelian groups $\{G_i\}_{i \in I}$. Let $S \subset I$ be some finite set, and for each $i \in I \setminus S$ choose a compact, open subgroup $K_i \leq G_i$. We define the **restricted direct product**[6]

$$\prod_{i \in I}{}' (G_i, K_i) := \left\{ (g_i) \in \prod_{i \in I} G_i : g_i \in K_i \text{ for all but finitely many } i \in I \setminus S \right\}.$$

We topologize this by giving it a basis of opens of the form

$$\prod_{i \in I} A_i \text{ with } A_i \overset{\text{open}}{\subset} G_i \text{ and } A_i = K_i \text{ for all but finitely many } i \in I.$$

Fact. Restricted direct products are themselves locally compact, Hausdorff abelian groups.

Definition 2.2. Let K be a number field. We define the **finite ideles** are the restricted direct product

$$\mathbb{I}_K^{fin} := \prod_{v \nmid \infty}{}' (K_v^\times, \mathscr{O}_v^\times),$$

while the **ideles** are

$$\mathbb{I}_K := \prod_{v}{}' (K_v^\times, \mathscr{O}_v^\times) = \mathbb{I}_K^{fin} \times \prod_{v \mid \infty} K_v^\times.$$

Fact. There is a diagonal embedding $K^\times \hookrightarrow \mathbb{I}_K$ given by $x \mapsto (\dots, x, x, x, \dots)$ whose image is discrete.

Example. To make things more concrete, let's see that the ideles of $\mathbb{Q}$ are a familiar object. Fix some $x = (x_v)_v \in \mathbb{I}_\mathbb{Q}$ (so $x_v \in \mathbb{Q}_v$). There are only finitely many primes p s.t. $x_p \in \mathbb{Q}_p \setminus \mathbb{Z}_p$; call them $p_1, p_2, \dots, p_k$. Let $q = \pm \prod_{i=1}^k p_i^{-\operatorname{ord}_{p_i}(x_{p_i})} \in \mathbb{Q}$ with sign chosen so that $qx \in \mathbb{R}_{>0}^\times \times \prod_p \mathbb{Z}_p^\times \subset \mathbb{I}_\mathbb{Q}$. Thus, the natural map

$$\mathbb{Q}^\times \times \mathbb{R}_{>0}^\times \times \prod_p \mathbb{Z}_p^\times \longrightarrow \mathbb{I}_\mathbb{Q}$$

[6] If you want, you can imagine $K_s = G_s$ when $s \in S$, even though G_s is not compact

is a surjection. This map is easily seen to be injective, so it is in fact a bijection. Secretly, it is actually an iso of topological groups (with $\mathbb{Q}^\times$ given the discrete topology). You get a similar idelic decomposition for any number field with trivial class group.[7]

Now, consider some extension L/K of number fields. There is unsurprisingly a natural map $\mathbb{I}_K \to \mathbb{I}_L$, but there is even a map $\mathbb{I}_L \to \mathbb{I}_K$ in the other direction! We like this map more.

Recall 2.3. For any extension E/F of fields, there is a norm map $\mathrm{Nm}_{E/F} : E \to F$ given by $\alpha \mapsto \det(m_\alpha)$, where $m_\alpha : E \to E$ is the F-linear "multiplication by α" map $m_\alpha(\beta) := \alpha\beta$.

We want to construct a norm map $\mathrm{Nm} = \mathrm{Nm}_{\mathbb{I}_L/\mathbb{I}_K} : \mathbb{I}_L \to \mathbb{I}_K$. Let Σ_K denote the set of places of K, and similarly for L. We begin by writing

$$\mathbb{I}_L = \prod_{w\in\Sigma_L}{}' L_w^\times = \prod_{v\in\Sigma_K}{}' \left(\prod_{w|v} L_w^\times\right).$$

The norm map is induced by the coordinatewise maps

$$\prod_{w|v} \mathrm{Nm}_{L_w/K_v} : \prod_{w|v} L_w^\times \to K_v^\times$$

for $v \in \Sigma_K$.

2.2 Statements of Main Results

This brings us to the good stuff. A good reference for this section is [Mil20b], especially sections I.1 and V.5.

Fix a number field K.

Theorem 2.4 (**Main Theorem of Global CFT**). *There exists a unique homomorphism, called the* ***(global) Artin map***

$$\varphi_K : \mathbb{I}_K \to \mathrm{Gal}(K^{\mathrm{ab}}/K)$$

satisfying

(1) $\varphi(K^\times) = 1$ *where, as always,* $K^\times \hookrightarrow \mathbb{I}_K$ *diagonally. That is, we really have a map*

$$\varphi_K : K^\times\backslash\mathbb{I}_K \to \mathrm{Gal}(K^{\mathrm{ab}}/K).$$

This is sometimes referred to as ***reciprocity****.*

(2) *Fix a finite place v of K, and let L/K be an extension unramified at v. For any uniformizer π_v of $\mathcal{O}_v \subset K_v$, one has*

$$\varphi_K(\pi_v)|_L = \mathrm{Frob}_v \in \mathrm{Gal}(L/K),$$

i.e. any uniformizer of a finite, unramified place acts by Frobenius.

[7] Eh trivial class group + arbitrarily signed units.

(3) For every finite abelian extension L/K, φ descends to an isomorphism[8]

$$\varphi_{L/K} : K^\times \backslash \mathbb{I}_K / \operatorname{Nm}(\mathbb{I}_L) \xrightarrow{\sim} \operatorname{Gal}(L/K).$$

Remark 2.5. Motivated by reciprocity, we define the **idele class group** $C_K = \mathbb{I}_K/K^\times$. Let L/K be finite, abelian. Note that the norm map $\operatorname{Nm} : \mathbb{I}_L \to \mathbb{I}_K$ descends to a map $C_L \to C_K$, and one can phrase **(3)** above as saying that

$$\varphi_{L/K} : C_K / \operatorname{Nm}(C_L) \xrightarrow{\sim} \operatorname{Gal}(L/K).$$

Motivated by **(3)**, we define a **norm group** of K to be a group of the form $\operatorname{Nm}(C_L) \subset C_K$, where L/K is finite, abelian.

Fact. A norm group of K is precisely an open, finite-index subgroup of C_K. Hence, CFT gives a bijection

$$\left\{ \begin{matrix} \text{finite abelian} \\ L/K \end{matrix} \right\} \leftrightarrow \left\{ \begin{matrix} \text{open, finite index} \\ \text{subgroups of } C_K \end{matrix} \right\}.$$

Corollary 2.6. *Let G be an abelian, finite (hence, discrete) group. The data of a G-extension of K is equivalent to that of a continuous, surjection $C_K \twoheadrightarrow G$.*

Notation 2.7. The Artin map $\varphi_K : C_K \to \operatorname{Gal}(K^{\mathrm{ab}}/K)$ is sometime also denoted

$$\operatorname{Art} = \operatorname{Art}_K : C_K \to \operatorname{Gal}(K^{\mathrm{ab}}/K)$$

instead.

The goal of class field theory is to understand $\operatorname{Gal}(K^{\mathrm{ab}}/K)$. How well does Theorem 2.4 achieve this goal? The Artin map $\varphi_K : C_K \to \operatorname{Gal}(K^{\mathrm{ab}}/K)$ is not an isomorphism (e.g. because the source is not compact but the target is), but clearly it captures much information about $\operatorname{Gal}(K^{\mathrm{ab}}/K)$ in terms of ideles. Here are a few ways in which φ_K answers the goal of class field theory

- **(3)** says that the composition

  $$C_K \xrightarrow{\varphi_K} \operatorname{Gal}(K^{\mathrm{ab}}/K) \twoheadrightarrow \operatorname{Gal}(L/K)$$

  is a surjection for any finite, abelian L/K. Hence, φ_K has dense image in $\operatorname{Gal}(K^{\mathrm{ab}}/K)$. In fact, again by **(3)** (+ the fact after Theorem 2.4), φ_K induces an isomorphism

  $$\widehat{\varphi}_K : \widehat{C}_K \xrightarrow{\sim} \operatorname{Gal}(K^{\mathrm{ab}}/K),$$

  from the profinite completion $\widehat{C}_K = \varprojlim_{L/K} C_K / \operatorname{Nm}(C_L)$ of C_K to $\operatorname{Gal}(K^{\mathrm{ab}}/K)$.

- We can actually do one better, and compute this profinite completion. In particular, we have the following (only true when K is a number field).

  Fact. $\varphi_K : C_K \to \operatorname{Gal}(K^{\mathrm{ab}}/K)$ is surjective with kernel C_K^0, the connected component of the identity.[9]

[8] This double coset space is really just $\mathbb{I}_K/(K^\times \cdot \operatorname{Nm}(\mathbb{I}_L))$ since everything abelian

[9] Note that non-archimedean local fields are totally disconnected, so this is really $\prod_{v \text{ real}} \mathbb{R}^\times_{>0} \times \prod_{v \text{ complex}} \mathbb{C}^\times$

- Number theorists care about $\mathrm{Gal}(K^{\mathrm{ab}}/K)$ as more than just a topological group. We also care about e.g. understanding its inertia subgroups. Fix a finite place v of K. Let $K^{ab,ur-v}/K$ be the maximal abelian extension of K which is unramified at v. We then have an exact sequence

$$1 \longrightarrow I(v) \longrightarrow \mathrm{Gal}(K^{\mathrm{ab}}/K) \longrightarrow \mathrm{Gal}(K^{ab,ur-v}/K) \longrightarrow 1,$$

whose kernel is inertia at v. By **(2)**, $\varphi_K(\mathscr{O}_v^\times) \in \mathrm{Gal}(K^{\mathrm{ab}}/K)$ lies in the kernel of the above map, and so lands in $I(v)$.

Fact. The top map is the below commutative square is an isomorphism.

$$\begin{array}{ccc} \mathscr{O}_v^\times & \xrightarrow{\sim} & I(v) \\ \downarrow & & \downarrow \\ C_K & \xrightarrow{\varphi_K} & \mathrm{Gal}(K^{\mathrm{ab}}/K), \end{array}$$

i.e. $\mathscr{O}_v^\times$ is inertia at v.

I am not sure if the above fact is explicitly in [Mil20b], but it can be found e.g. in section 3.8 of [Ser67].[10]

What about infinite places? When v is infinite, inertia at v is given by $K_v^\times/(K_v^\times)^0$. In particular, $K_v^\times$ surjects onto inertia under the Artin map.

Inspired by the third bullet point above, we introduce the following (non-standard) notation.

Notation 2.8. For v a place of K, let $I(v)$ denote the following

- if v is non-archimedean, then $I(v) = \mathscr{O}_v^\times$
- if v is archimedean, then $I(v) = K_v^\times$

Hence, $I(v)$ essentially denotes inertia at v. This is not literally true when v is archimedean. What is always true, though, is that $I(v) = \varphi_K^{-1}(\text{inertia at } v)$.

Example. Let's pause and see what things say in the case of $K = \mathbb{Q}$. Recall that

$$I_{\mathbb{Q}} \xrightarrow{\sim} \mathbb{Q}^\times \times \mathbb{R}_{>0}^\times \times \prod_p \mathbb{Z}_p^\times.$$

Thus $\mathbb{Q}$'s idele class group is

$$C_{\mathbb{Q}} = I_{\mathbb{Q}}/\mathbb{Q}^\times \simeq \mathbb{R}_{>0}^\times \times \prod_p \mathbb{Z}_p^\times.$$

Recall the Artin map gives an iso $\varphi_{\mathbb{Q}} : C_{\mathbb{Q}}/C_{\mathbb{Q}}^0 \xrightarrow{\sim} \mathrm{Gal}(\mathbb{Q}^{\mathrm{ab}}/\mathbb{Q})$, so

$$\prod_p \mathbb{Z}_p^\times \xrightarrow{\sim} \mathrm{Gal}(\mathbb{Q}^{\mathrm{ab}}/\mathbb{Q})$$

[10] This is (one of) Serre's chapter(s) in Cassels-Fröhlich

(product taken over rational primes[11]) and $\mathbb{Z}_p^\times$ is inertia at p. As an unimportant (to us) consequence, we see that class field theory gives an (overpowered) proof that $\mathrm{Gal}(L/\mathbb{Q})$ is generated by inertia (at finite primes) for all Galois number fields L.

2.3 Various Flavors of Class Groups

As far as I can tell, the main use of class field theory in [FGV20] is asserting the existence of various flavors of Hilbert class fields, so we should probably talk about this.

As always, fix a number field K.

(ideal) Class group We will show the existence of a number field whose Galois group is the ideal class group of K.

Recall 2.9. The **class group** of K, is the group

$$\mathrm{Cl}_K := \frac{\{\text{fractional ideals}\}}{\{\text{principal fractional ideas}\}}.$$

This is sometimes denote $\operatorname{Pic}\mathscr{O}_K$ since it coincides with the Picard group of $\operatorname{spec}\mathscr{O}_K$.[12] This group is finite for any number field.

Recall also the finite ideles $\mathbb{I}_K^{fin}$. Note that there is a natural map

$$\begin{array}{ccc} \mathbb{I}_K^{fin} & \longrightarrow & \{\text{fractional ideals}\} \\ (x_v)_{v\nmid\infty} & \longmapsto & \prod_{v\nmid\infty} \mathfrak{p}_v^{\mathrm{ord}_v(x_v)} \end{array}$$

This map is visibly surjective, and visibly not injective (because units). However, the quotient map

$$\mathbb{I}_K^{fin} \Big/ \prod_{v\nmid\infty} \mathscr{O}_v^\times \xrightarrow{\sim} \{\text{fractional ideals}\}$$

is now an isomorphism. It is probably not a surprise that the principal fractional ideals on the right hand side exactly correspond to $K^\times$ (diagonally embedded) on the left hand side, so we get an isomorphism

$$C_K \Big/ \left(\prod_{v\nmid\infty} \mathscr{O}_v^\times \times \prod_{v\mid\infty} K_v^\times \right) = K^\times \backslash \mathbb{I}_K \Big/ \left(\prod_{v\nmid\infty} \mathscr{O}_v^\times \times \prod_{v\mid\infty} K_v^\times \right) = K^\times \backslash \mathbb{I}_K^{fin} \Big/ \prod_{v\nmid\infty} \mathscr{O}_v^\times = \mathrm{Cl}_K\,.$$

We express this perhaps more digestibly as the exact sequence

$$1 \longrightarrow \mathscr{O}_K^\times \longrightarrow \prod_v I(v) \longrightarrow C_K \longrightarrow \mathrm{Cl}_K \longrightarrow 1.$$

That is, we have a continuous surjection $C_K \twoheadrightarrow \mathrm{Cl}_K$ with kernel $\left(\prod_{v\nmid\infty} \mathscr{O}_v^\times \times \prod_{v\mid\infty} K_v^\times\right)$! This is exciting for two reasons. First, class field theory tells us that this surjection $C_K \twoheadrightarrow \mathrm{Cl}_K$ corresponds to

[11] finite places of $\mathbb{Q}$

[12] [FGV20] uses $\operatorname{Pic}\mathscr{O}_K$ to denote the Picard groupoid of $\operatorname{spec}\mathscr{O}_K$ (category of f.g. projective $\mathscr{O}_K$-modules with morphisms given by $\mathscr{O}_K$-linear isomorphisms), and so uses $\pi_0 \operatorname{Pic}\mathscr{O}_K$ to denote the class group, the iso classes of $\operatorname{Pic}\mathscr{O}_K$

some number field H_K, called the **Hilbert class field** of K, and an isomorphism $\mathrm{Gal}(H_K/K) \xrightarrow{\sim} \mathrm{Cl}_K$. Secondly, the kernel of this map is precisely $\prod_v I(v) \subset C_K$; that is, we kill inertia at all places of K and nothing more. Thus, we get the following characterization of H_K.

Proposition 2.10. *The Hilbert class field H_K of K is the maximal abelian, unramified extension of K.*

Remark 2.11. H_K is unramified at *all* places, including the infinite ones.

Fact. Assume $K/\mathbb{Q}$ is Galois. Then, we get an exact sequence

$$1 \longrightarrow \mathrm{Gal}(H_K/K) \longrightarrow \mathrm{Gal}(H_K/\mathbb{Q}) \longrightarrow \mathrm{Gal}(K/\mathbb{Q}) \longrightarrow 1.$$

This induces the usual "lift-and-conjugate" action of $\mathrm{Gal}(K/\mathbb{Q}) \curvearrowright \mathrm{Gal}(H_K/K) = \mathrm{Cl}_K$, i.e. given $\sigma \in \mathrm{Gal}(K/\mathbb{Q})$ and $\tau \in \mathrm{Gal}(H_K/K)$, we set[13]

$$\sigma \cdot \tau = \widetilde{\sigma}\tau\widetilde{\sigma}^{-1} \in \mathrm{Gal}(H_K/K)$$

for any lift $\widetilde{\sigma} \in \mathrm{Gal}(H_K/\mathbb{Q})$ of σ. Under the identification $\mathrm{Gal}(H_K/K) = \mathrm{Cl}_K$, this becomes the natural action $\mathrm{Gal}(K/\mathbb{Q}) \curvearrowright \mathrm{Cl}_K$ given by $\sigma(I) = \{\sigma(a) : a \in I\}$ for any fractional ideal.

So far, we've defined class groups and idele class groups. Why stop there? Note that the Hilbert class field is unramified everywhere, but it's easy to forget ramification at infinite places is a thing, so what if we only wanted a field unramified at finite places?

Narrow class group The **narrow class group** of K is

$$\mathrm{Cl}_K^+ := C_K \Bigg/ \left(\prod_{v \nmid \infty} \mathscr{O}_v^\times \right),$$

i.e. it is the Galois group of the maximal abelian extension H_K^+ of K which is unramified at all finite places. This H_K^+ is called the **narrow Hilbert class field**.

If one wants to, they can give an equivalent definition in terms of fractional ideals. This can be done either by expanding definitions and thinking things through carefully, or just looking at the Wikipedia page.

Ray class groups At this point, it is maybe not a surprise what comes next. You can impose whatever ramification conditions you want, and get a corresponding class group and Hilbert class field.

Consider some "**modulus**"

$$N = \prod_{v \nmid \infty} \mathfrak{p}_v^{m_v} \text{ with } m_v \geq 0$$

which is an integral ideal (so we require the product to be finite). We can define

$$\left(1 + N\widehat{\mathscr{O}}\right)^\times := \prod_{v \nmid \infty} (1 + \pi_v^{m_v}),$$

[13] This is well-defined since $\mathrm{Gal}(H_K/K)$ is abelian.

where $\pi_v \in \mathscr{O}_v$ is a uniformizer and we set $(1+\pi_v^0) := \mathscr{O}_v^\times$. Note that the products above are only taken over *finite places* of K (since no infinite places appear in N). We define the **Ray class group of modulus** N to be

$$\mathrm{Cl}_{K,N} := C_K \Big/ \prod_{v|\infty} K_v^\times \cdot \left(1 + N\widehat{\mathscr{O}}\right)^\times.$$

Again, one can interpret this as certain isomorphism classes of ideals, and Wikipedia will tell you how. One can also impose conditions on the infinite places if they want. The notion of ray class group subsumes both the usual (ideal) class group as well as the narrow class group. As before, class field theory gives a corresponding **ray class field** $H_{K,N}$ which, in the present case, is the maximal abelian extension of K which is unramified outside of N (i.e. at v for which $m_v = 0$) and whose inertia at $v \mid N$ (i.e. at v for which $m_v > 0$) is at worst $\mathscr{O}_v^\times/(1+\pi_v^{m_v})$ (i.e. is a quotient of this).[14]

2.4 Chebotarev

The last thing we do is state Chebotarev density since this comes up in [FGV20] at some point.

Let L/K be some Galois extension of number fields, and let $S \subset \Sigma_K$ be the (finite) set of archimedean or ramified (in L/K) places of K. Recall that for any place $v \in \Sigma_K \setminus S$ we get a well-defined *conjugacy class* $\mathrm{Frob}_v \subset \mathrm{Gal}(L/K)$. Thus, we have a map

$$F : \left\{ \begin{array}{c} \text{unram primes} \\ \text{in } \mathscr{O}_K \end{array} \right\} \longrightarrow \left\{ \begin{array}{c} \text{conj. classes} \\ \text{in } \mathrm{Gal}(L/K) \end{array} \right\}.$$

Chebotarev says that the fibers of this map have the "size" you might naively expect.

Theorem 2.12 (**Chebotarev density**). *In the above situation, let $C \subset \mathrm{Gal}(L/K)$ be a fixed conjugacy class. Then, $F^{-1}(C)$ has natural density*

$$\delta(F^{-1}(C)) = \lim_{X\to\infty} \frac{\#\left\{\mathfrak{p} : \mathrm{Frob}_\mathfrak{p} \in C, \mathrm{Nm}\,\mathfrak{p} < X\right\}}{\#\left\{\mathfrak{p} : \mathrm{Nm}\,\mathfrak{p} < X\right\}} = \frac{\#C}{\#G}.$$

Above, $\mathfrak{p}$ ranges over (nonzero) prime ideals of $\mathscr{O}_K$, and $\mathrm{Nm}\,\mathfrak{p} := \#(\mathscr{O}_K/\mathfrak{p})$. In particular, there are infinitely many primes with Frobenius in any given conjugacy class.

Corollary 2.13 (**Dirichlet's Theorem on Primes in Arithmetic Progressions**). *Fix $a, n \in \mathbb{N}$ with $\gcd(a,n) = 1$. Then, there are infinitely many rational primes p such that $p \equiv a \pmod{n}$.*

We don't need this corollary for anything, but I figured these notes should have at least one proof block.

Proof. Let $K = \mathbb{Q}(\zeta_n)$, where ζ_n is some primitive nth root of unity. Then, $\mathrm{Gal}(K/\mathbb{Q}) \simeq (\mathbb{Z}/n\mathbb{Z})^\times$ with natural isomorphism $a : \mathrm{Gal}(K/\mathbb{Q}) \xrightarrow{\sim} (\mathbb{Z}/n\mathbb{Z})^\times$ satisfying $\sigma(\zeta_n) = \zeta_n^{a(\sigma)}$ for all $\sigma \in \mathrm{Gal}(K/\mathbb{Q})$. It is a fact from algebraic number theory that a rational prime p is unramified in K iff $p \nmid n$. For such a p, we get a well-defined $\mathrm{Frob}_p \in \mathrm{Gal}(K/\mathbb{Q}) \simeq (\mathbb{Z}/n\mathbb{Z})^\times$ which is uniquely characterized by the fact that

$$\mathrm{Frob}_p(x) \equiv x^p \pmod{\mathfrak{p}},$$

[14] Assuming I haven't confused myself, this is requiring your extension to have conductor at v of value at most m_v.

where $\mathfrak{p}$ is any prime of K above p. Considering the case $x = \zeta$, it is clear that Frob_p corresponds to $p \bmod n \in (\mathbb{Z}/n\mathbb{Z})^\times$. Thus, Chebotarev says that there are infinitely many primes p such that $\mathrm{Frob}_b = a \bmod n \in (\mathbb{Z}/n\mathbb{Z})^\times$, i.e. that there are infinitely primes such that $p \equiv a \pmod{n}$. ■

Milne proves Chebotarev in chapter VIII of his notes [Mil20b].

References

[FGV20] Tony Feng, Soren Galatius, and Akshay Venkatesh. The galois action on symplectic k-theory, 2020.

[Mil20a] J.S. Milne. Algebraic number theory. `https://www.jmilne.org/math/CourseNotes/ant.html`, 2020. Course notes.

[Mil20b] J.S. Milne. Class field theory. `https://www.jmilne.org/math/CourseNotes/cft.html`, 2020. Course notes.

[Ser67] J.-P. Serre. Local class field theory. In *Algebraic Number Theory (Proc. Instructional Conf., Brighton, 1965)*, pages 128–161. Thompson, Washington, D.C., 1967.

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