Eidgenössische Technische Hochschule Zürich
Swiss Federal Institute of Technology Zurich

The Class Number Formula and Beyond

Semester Paper

Haoran Liang

liangha@student.ethz.ch

Department of Mathematics
ETH Zürich

Supervisors:
Prof. Dr. Burrin, Claire

June 07, 2022

Acknowledgements

I would like to express my deep gratitude to my supervisor, Prof. Dr. Claire Burrin, who guided me throughout this project. I have benefited so much from her valuable comments. I would also like to show my great appreciation to my mom, without whose love and support I would not have been able to complete this semester paper (or even study mathematics). Special thanks to Jeremy Feusi, Yuan Gao, Xuao, Li, Jiatong Nie, Zhiang Wu, Pengcheng Zhang, Cunyuan Zhao and everyone, I had a wonderful time with you guys and have grown a lot. Finally, I wish to thank Prof. Dr. Emmanuel Kowalski, for he kindly agreed to be my formal supervisor so I could get credits for this semester paper.

Abstract

The class number formula is a classical topic in algebraic number theory, which relates many important invariants of a number field K to the special value of its Dedekind zeta function $\zeta_K(s)$ at $s = 1$. In this semester paper, after a brief recap of relevant results on number fields, we present a proof of the class number formula via geometry of numbers and then derive an explicit formula of $\zeta_K(s)$ at $s = 1$ for Abelian number fields. This leads us to an analytic formulation of Gauss's Quadratic Reciprocity Law and the original proof of Dirichlet's theorem on arithmetic progressions by Dirichlet himself. To examine these themes further, we then summarize theorems of class field theory and use them to obtain general reciprocity laws and uniform distribution results of primes in number fields.

Contents

Chapter I

A Brief Recap on Number Fields

Let us begin our journey through the class number formula with a short recap on some relevant notions and facts about number fields.

We borrow heavily from the first five chapters of [M18], where one can find proofs of all[1] the results appeared in this chapter. Hence, all the statements in section 1.1 and 1.2 are stated without proofs. But section 1.3 (the geometry of numbers) is central to our main topic – the class number formula, so we kindly recall the proofs here.

1.1 Number fields and number rings

A **number field** K is a finite extension of the field of rational numbers $\mathbb{Q}$, so it is of the form $\mathbb{Q}(\alpha)$ for some algebraic number $\alpha \in \mathbb{C}$ (finite separable extensions are simple). The degree of the minimal polynomial $f \in \mathbb{Q}[x]$ of α is the degree of the field extension $K/\mathbb{Q}$, and we shall denote it by $n = [K : \mathbb{Q}]$.

Let $\mathcal{O}_K$ be the set of all *integral* elements in K over $\mathbb{Z}$, i.e., elements that are roots of monic integral polynomials in K, then $\mathcal{O}_K$ forms a subring of K (the integral closure of $\mathbb{Z}$ in K), called the **number ring of K**. We shall call elements in $\mathcal{O}_K$ *algebraic integers* to distinguish them from the case $K = \mathbb{Q}$, where $\mathcal{O}_K$ is nothing but the usual *rational integers* $\mathbb{Z}$.

An extension of number fields L/K of degree n has precisely n K-embeddings $\sigma_i : L \hookrightarrow \mathbb{C}$, so we define two K-valued functions $T = T_K^L$ (*trace*) and $N = N_K^L$ (*norm*) on L as follows: For each $\alpha \in L$, set

$$T_K^L(\alpha) = \sigma_1(\alpha) + \cdots + \sigma_n(\alpha),$$
$$N_K^L(\alpha) = \sigma_1(\alpha) \cdot \cdots \cdot \sigma_n(\alpha).$$

Note that if the minimal polynomial of $\alpha \in L$ is given by $f(x) = x^d + a_{d-1}x^{d-1} + \cdots + a_0 \in K[x]$ $(d \mid n)$, then $T_K^L = (n/d)a_0 \in K$ and $N_K^L(\alpha) = (a_{d-1})^{n/d} \in K$, so T_K^L and N_K^L are well-defined. In particular, if $K = \mathbb{Q}$, then the maps T, N send algebraic integers to rational integers. Clearly, T is additive and N is multiplicative by definition. Moreover, T and N satisfy the following transitive property for towers of number fields:

Proposition 1.1 *Let $L/F/K$ be extensions of number fields. Then, for all $\alpha \in L$,*

$$T_K^L(\alpha) = T_K^F(T_F^L(\alpha)),$$
$$N_K^L(\alpha) = N_K^F(N_F^L(\alpha)).$$

Let L/K be an extension of number fields of degree n. We now recall the notion of the *discriminant of an n-tuple* in L, which turns out to be quite helpful, for instance,

[1] Well... except for the Kronecker–Weber Theorem.

to deduce the additive structure of a number ring: For any n-tuple $(\alpha_1, \ldots, \alpha_n)$ in L, we define

$$d_{L/K}(\alpha_1, \ldots, \alpha_n) := \det(\sigma_i(\alpha_j))^2 = \det(T_K^L(\alpha_i\alpha_j)). \tag{1-1}$$

Observe that $d_{L/K}(\alpha_1, \ldots, \alpha_n) = 0$ iff $(\alpha_1, \ldots, \alpha_n)$ is K-linear. Also, the second equality tells us that when $K = \mathbb{Q}$, the discriminant of n algebraic integers is a rational integer.

Theorem 1.2 *Suppose K is a number field of degree n, then $(\mathcal{O}_K, +)$ is a free abelian group of rank n. i.e., there exists an n-tuple $(\omega_1, \ldots, \omega_n) \in \mathcal{O}_K$, such that*

$$\mathcal{O}_K = \omega_1\mathbb{Z} \oplus \cdots \oplus \omega_n\mathbb{Z}.$$

Corollary 1.3 *More generally, any ideal[1] $\mathfrak{a}$ of $\mathcal{O}_K$ has the additive structure of a free abelian group of rank n, and the quotient ring $\mathcal{O}_K/\mathfrak{a}$ is finite. Hence, prime ideals of $\mathcal{O}_K$ are maximal (finite integral domains are fields).*

Such an n-tuple in Theorem 1.2 is called an **integral basis of K**, its discriminant is invariant under change of bases, and hence is an invariant of K, called the **discriminant of K**. We shall denote the discriminant of K by $d(K)$.

For any ideal $\mathfrak{a}$ of $\mathcal{O}_K$, we define its **norm** to be the number of elements in the quotient ring $\mathcal{O}_K/\mathfrak{a}$, and denote it by $N_K(\mathfrak{a})$. Suppose $(\alpha_1, \ldots, \alpha_n)$ is a basis of $\mathfrak{a}$, then it follows from the fundamental theorem of finite abelian group that

$$d_{K/\mathbb{Q}}(\alpha_1, \ldots, \alpha_n) = N_K(\mathfrak{a})^2 d(K). \tag{1-2}$$

It is worth mentioning that norm is completely multiplicative with respect to ideals (Corollary 1.7).

Let us now work out two important special cases, which will be appear over and over again in our further discussions.

1) (Quadratic fields) If $K = \mathbb{Q}(\sqrt{d})$, d is square-free, then $\mathcal{O}_K = \mathbb{Z}[\omega]$, where

$$\omega = \begin{cases} \sqrt{d}, & d \equiv 2, 3 \pmod 4; \\ (1+\sqrt{d})/2, & d \equiv 1 \pmod 4. \end{cases} \tag{1-3}$$

And thus

$$d(K) = \begin{cases} 4d, & d \equiv 2, 3 \pmod 4; \\ d, & d \equiv 1 \pmod 4. \end{cases} \tag{1-4}$$

2) (Cyclotomic fields) If $K = \mathbb{Q}(\zeta_m)$, $\zeta_m = e^{2\pi i/m}$ is a m-th primitive root of unity, then $\mathcal{O}(K) = \mathbb{Z}[\zeta_m]$. In particular[2], if $m = p^t$ is a prime power, then one computes that $d(K) = d(\zeta_m) = (-1)^{k/2}p^{p^{t-1}(tp-t-1)}$, where $k = \varphi(p^t)$, φ is the Euler totient function. If $t = 1$ and p is odd, we get

$$d(K) = \begin{cases} p^{p-2}, & p \equiv 1 \pmod 4; \\ -p^{p-2}, & p \equiv 3 \pmod 4. \end{cases}$$

[1] Unless otherwise stated, by "ideal" we shall always mean "non-zero ideal".

[2] If m, n are coprime, then $\mathbb{Q}(\zeta_{mn}) = \mathbb{Q}(\zeta_m)\mathbb{Q}(\zeta_n)$ and $\mathbb{Z}[\zeta_{mn}] = \mathbb{Z}[\zeta_m]\mathbb{Z}[\zeta_n]$, so everything reduces to the case where $m = p^t$ is a prime power.

Note that $(1, \zeta_p, \ldots, \zeta_p^{p-1})$ is an integral basis of K, $d(K) = d(1, \zeta_p, \ldots, \zeta_p^{p-1})$, which is a perfect square in K by (1-1), we see $\mathbb{Q}(\sqrt{p}) \subset \mathbb{Q}(\zeta_p)$ if $p \equiv 1 \pmod 4$, $\mathbb{Q}(\sqrt{-p}) \subset \mathbb{Q}(\zeta_p)$ if $p \equiv 3 \pmod 4$. This is a special case of the Kronecker–Weber Theorem:

Theorem 1.4 (Kronecker–Weber) *Every* Abelian *number field (i.e., it is Galois over $\mathbb{Q}$ and the Galois group is abelian) is contained in a cyclotomic field.*

We will give a proof of this theorem in section 3.1.2, when we discuss first elements of class field theory.

1.2 Prime decomposition in number rings

1.2.1 Prime decomposition

Let K be a number field and let $\mathcal{O}_K$ be its number ring. Although elements in $\mathcal{O}_K$ may not be factorized uniquely, every ideal of $\mathcal{O}_K$ can be uniquely decomposed as a finite product of prime ideals, this is because number rings are *Dedekind domains* (noetherian, integrally closed domain of dimension 1). Indeed, one can show that $\mathcal{O}_K$ is a UFD iff it is a PID.

Theorem 1.5 *If A is a Dedekind domain, then every proper ideal of A can be written uniquely in the form*

$$\mathfrak{a} = \mathfrak{p}_1^{n_1} \cdots \mathfrak{p}_s^{n_s},$$

where $s \geq 1$, the $\mathfrak{p}_i$'s are pairwise distinct prime ideals and the n_i's are positive integers. By convention, A is the product of 0 prime ideal.

The key ingredient to prove the uniqueness of the prime decomposition of ideals in a Dedekind domain is the following lemma:

Lemma 1.6 *Let $\mathfrak{a}$ be an ideal of a Dedekind domain A, then there exists an ideal $\mathfrak{b}$ such that $\mathfrak{ab}$ is principal.*

Lemma 1.6 guarantees the *cancellation law* for ideals in a Dedekind domain, and also leads naturally to the definition of the ideal class group, where the class of principal ideals is the identity element. We will return to this in the next section.

By Theorem 1.5, addition and multiplication of ideals satisfy the *distributive law*, and thus it now makes sense to generalize the notions of factors, greatest common factions, least common multiples, etc. to ideals in a Dedekind domain.

Corollary 1.7 *Norm is completely multiplicative. More precisely, if*

$$\mathfrak{a} = \mathfrak{p}_1^{n_1} \cdots \mathfrak{p}_s^{n_s},$$

then

$$N_K(\mathfrak{a}) = N_K(\mathfrak{p}_1)^{n_1} \cdots N_K(\mathfrak{p}_s)^{n_s}.$$

Now, let L/K be an extension of number fields of degree n, then clearly $\mathcal{O}_K$ is a subring of $\mathcal{O}_L$. Given a prime ideal $\mathfrak{q} \in \mathcal{O}_L$, its contraction ideal $\mathfrak{p} := \mathfrak{q} \cap \mathcal{O}_K$ remains

prime, so we say that $\mathfrak{q}$ *lies over* $\mathfrak{p}$ and that $\mathfrak{p}$ *lies under* $\mathfrak{q}$. Conversely, given a prime ideal $\mathfrak{p} \subset \mathcal{O}_K$, its extension ideal $\mathfrak{p}\mathcal{O}_L$ may not be prime in S any more, and it has a prime decomposition

$$\mathfrak{p}\mathcal{O}_L = \mathfrak{q}_1^{e_1} \cdots \mathfrak{q}_g^{e_g}, \tag{1-5}$$

where the $\mathfrak{q}_i$'s are prime factors of $\mathfrak{p}\mathcal{O}_L$. We shall call the exponents e_i's *ramification indices* and denote $e_i = e(\mathfrak{q}_i|\mathfrak{p})$. Note that for each $\mathfrak{q}_i$, $\mathcal{O}_K/\mathfrak{p} \hookrightarrow \mathcal{O}_L/\mathfrak{q}_i$ is an extension of finite fields, we shall take its degree $f_i = f(\mathfrak{q}_i|\mathfrak{p})$ and call it the *inertial degree* of $\mathfrak{q}$ over $\mathfrak{p}$.

Surprisingly, there is a beautiful relation among these important numbers.

Theorem 1.8 *Keeping the same notations as above, we have*

$$e_1 f_1 + \cdots + e_g f_g = n. \tag{1-6}$$

Some important special cases are worth mentioning: If $\mathfrak{p}\mathcal{O}_L$ is not square-free, i.e., there exists some $1 \leq i \leq g$ such that $e_i > 1$, then we say that $\mathfrak{p}$ is *ramified*. Moreover, we say that $\mathfrak{p}$ is *totally ramified* in the extreme case $e = n, f = g = 1$; if $\mathfrak{p}\mathcal{O}_L$ remains to be prime, i.e., $f = n, e = g = 1$, then we say $\mathfrak{p}$ is *inert*; and if $g = n, e = f = 1$, then we say $\mathfrak{p}$ is *totally split*.

Ramification indices and inertial degrees are multiplicative in towers. Namely, let $L/F/K$ be extensions of number fields with their corresponding number rings $\mathcal{O}_L \supset \mathcal{O}_F \supset \mathcal{O}_K$, and suppose we have a chain of prime ideals $\mathfrak{r} \subset \mathcal{O}_L$ lying over $\mathfrak{q} \subset \mathcal{O}_F$ and $\mathfrak{q}$ lying over $\mathfrak{p} \subset \mathcal{O}_K$, then

$$e(\mathfrak{r}|\mathfrak{p}) = e(\mathfrak{r}|\mathfrak{q}) \cdot e(\mathfrak{q}|\mathfrak{p}), \quad f(\mathfrak{r}|\mathfrak{p}) = f(\mathfrak{r}|\mathfrak{q}) \cdot f(\mathfrak{q}|\mathfrak{p}).$$

1.2.2 Galois theory applied to prime decomposition

If L/K is a normal (and hence Galois) extension of number fields, then the Galois group $G = \mathrm{Gal}(L/K)$ acts transitively on the set of all prime ideals $\mathfrak{q} \subset \mathcal{O}_L$ lying over $\mathfrak{p}$. Hence, a prime $\mathfrak{q}$ of $\mathcal{O}_L$ splits into $(\mathfrak{p}_1 \cdots \mathfrak{p}_g)^e$, where the $\mathfrak{p}_i$'s are distinct primes, all having the same inertial degree f over $\mathfrak{p}$. Moreover, consider the following subgroups of G: the *decomposition group*

$$D_\mathfrak{q} := \{\sigma \in G \,:\, \sigma\mathfrak{q} = \mathfrak{q}\},$$

and the *inertia group*

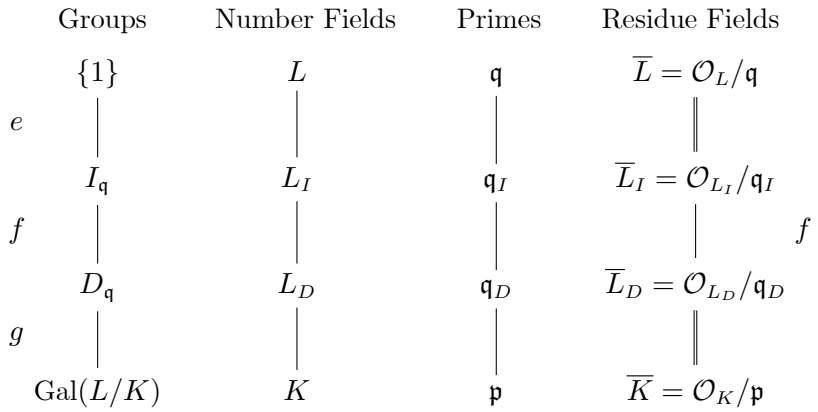
$$I_\mathfrak{q} := \{\sigma \in G \,:\, \sigma(\alpha) \equiv \alpha \pmod{\mathfrak{q}}, \forall\, \alpha \in \mathcal{O}_L\}.$$

Clearly, there is a chain of subgroups $I_\mathfrak{q} \leq D_\mathfrak{q} \leq G$. Any element σ of $D_\mathfrak{q}$ induces an automorphism of the *residue field* $\overline{L} := \mathcal{O}_L/\mathfrak{q}$ while fixing its subfield $\overline{K} := \mathcal{O}_K/\mathfrak{p}$ pointwise, and thus can be view as an element $\overline{\sigma}$ of the Galois group of residue fields $\overline{G} := \mathrm{Gal}(\overline{L}/\overline{K})$. In fact, this gives us a surjective group homomorphism

$$D_\mathfrak{q} \twoheadrightarrow \overline{G},\ \sigma \mapsto \overline{\sigma},$$

whose kernel is exactly $I_\mathfrak{q}$, so $D_\mathfrak{q}/I_\mathfrak{q} \cong \overline{G}$ canonically. More precisely, let L_D (resp. L_I) be the corresponding fixed field of $D_\mathfrak{q}$ (resp. $I_\mathfrak{q}$), called the *decomposition field* (resp.

inertia field), then we have the following diagram:



Where, $\mathfrak{q}_I = \mathfrak{q} \cap \mathcal{O}_{L_I}$, $\mathfrak{q}_D = \mathfrak{q}_I \cap \mathcal{O}_{L_D}$, and $e(\mathfrak{q}_I|\mathfrak{p}_D) = e(\mathfrak{q}_D|\mathfrak{p}) = 1$. Hence, $\mathfrak{p}_D$ is inert in $\mathcal{O}_{L_I}$ and $\mathfrak{p}_I$ is totally ramified in $\mathcal{O}_L$. If $D_\mathfrak{q} \trianglelefteq \mathrm{Gal}(L/K)$, then $\mathfrak{p}$ totally splits in to g primes in $\mathcal{O}_D$. If also $I_\mathfrak{q} \triangleleft \mathrm{Gal}(L/K)$, then these primes remain prime in $\mathcal{O}_I$, and each of them becomes an e-th power in $\mathcal{O}_L$.

1.2.3 The Frobenius automorphism

Let L/K be a Galois extension of number fields, and suppose a prime $\mathfrak{p} \subset \mathcal{O}_K$ is unramified in $\mathcal{O}_L$, i.e., $\mathfrak{p}\mathcal{O}_L = \mathfrak{q}_1 \cdots \mathfrak{q}_g$. Write $\mathfrak{q} = \mathfrak{q}_1$, then $I_\mathfrak{q}$ is trivial, so $D_\mathfrak{q} \cong \overline{G}$ is cyclic of order f. Note that $|\overline{K}| = |\mathcal{O}_K/\mathfrak{p}| = N_{K/\mathbb{Q}}(\mathfrak{p})$, $\overline{G}$ is generated by the map $\overline{\sigma} : x \mapsto x^{N_{K/\mathbb{Q}}(\mathfrak{p})}$. We shall denote by the **Artin symbol** $\left(\frac{L/K}{\mathfrak{q}}\right)$ its corresponding element σ in $D_\mathfrak{q}$ under the canonical isomorphism $\sigma \mapsto \overline{\sigma}$ above, and call it the **Frobenius automorphism** of $\mathfrak{q}$ over $\mathfrak{p}$. It is not hard to see that $\left(\frac{L/K}{\mathfrak{q}}\right)$ is characterized by

$$\left(\frac{L/K}{\mathfrak{q}}\right)\alpha \equiv \alpha^{N_{K/\mathbb{Q}}(\mathfrak{p})} \pmod{\mathfrak{q}}, \quad \forall\, \alpha \in \mathcal{O}_L. \tag{1-7}$$

Here are some first properties of the Frobenius automorphism:

1) For each $\sigma \in \mathrm{Gal}(L/K)$, we have

$$\left(\frac{L/K}{\sigma(\mathfrak{q})}\right) = \sigma\left(\frac{L/K}{\mathfrak{q}}\right)\sigma^{-1}; \tag{1-8}$$

2) For a tower $L/F/K$ of number fields (L/K is Galois), set $\mathfrak{q}_F = \mathfrak{q} \cap \mathcal{O}_F$, then

$$\left(\frac{L/F}{\sigma(\mathfrak{q})}\right) = \left(\frac{L/K}{\mathfrak{q}}\right)^{f(\mathfrak{q}_F|\mathfrak{p})}; \tag{1-9}$$

3) If in addition F/K is also Galois, then

$$\left(\frac{F/K}{\sigma(\mathfrak{q})}\right) = \left(\frac{L/K}{\mathfrak{q}}\right)\Big|_F. \tag{1-10}$$

One reason why the Frobenius automorphism is interesting can be seen in the fact that it is of order $f(\mathfrak{q}|\mathfrak{p})$, and hence indicates how $\mathfrak{p}$ splits in $\mathcal{O}_L$. The quadratic and cyclotomic fields provide us with perfect examples. So, let us now list how primes $p \in \mathbb{Z}$ split in these number fields, as follows:

1) $K = \mathbb{Q}(\sqrt{d})$, d square-free is a quadratic field. Then,

a) If $p \mid d(K)$, then p is ramified[1] in $\mathcal{O}_K$;

b) If $p \nmid d(K)$ is odd, then p totally splits in $\mathcal{O}_K$ when $d(K)$ is a quadratic residue of p and p is inert otherwise;

c) If $p \nmid d(K)$ and $p = 2$, then p totally splits in $\mathcal{O}_K$ when $p \equiv 1 \pmod 8$ and p is inert otherwise.

2) $K = \mathbb{Q}(\zeta_m)$, $\zeta_m = e^{2\pi i/m}$ is a cyclotomic field. Suppose $m = p^k n$, $p \nmid n$, then

$$p\mathcal{O}_K = (\mathfrak{q}_1 \cdots \mathfrak{q}_g)^e,$$

where $e = \varphi\left(p^k\right)$ and f is the smallest positive integer such that $p^f \equiv 1 \pmod m$.

The Frobenius automorphism will be very important for our discussions of class field theory in chapter 3.

1.3 The ideal class group and the unit group

In this section, we recall two important groups associated to a number ring $\mathcal{O}_K$: the ideal class group and the unit group, mainly from a geometric point of view. This section follows much of chapter 6-9 of [ST16].

1.3.1 The ideal class group

Let A be an integral domain, and $F = \mathrm{Frac}(A)$ be its field of fractions. Then, the set S of all (non-zero, as usual) ideals of A forms a commutative *monoid*[2] w.r.t. the product $\cdot$ of ideals. If $(S, \cdot)$ satisfies the cancellation law, then we can extend S to an abelian group G by taking fractions. In addition, if A is a Dedekind domain, then explicitly, G is just the group of fractional ideals of A (thanks to Lemma 1.6), and it has a subgroup H of principal fractional ideals. We define the **ideal class group of** $\boldsymbol{A}$ to be the quotient group $\mathcal{C} := G/H$.

Equivalently, here is a down-to-earth way of viewing $\mathcal{C}$: For an integral domain A, we define an equivalence relation $\sim$ on S by setting

$$\mathfrak{a} \sim \mathfrak{b} \text{ iff } \exists\, \alpha, \beta \in A, s.t. \beta\mathfrak{a} = \alpha\mathfrak{b},$$

then $\widetilde{\mathcal{C}} := S/\sim$ inherits the product operation $\cdot$ from the product of ideals. We shall call an equivalence class of S under $\sim$ an *ideal class*, and write $C = [\mathfrak{a}]$ the ideal class of $\mathfrak{a}$. One can check that

1) $\mathfrak{a} \sim \mathfrak{b}$ iff they are isomorphic as A-modules;

2) The set of all principal ideals forms an ideal class;

3) $(\widetilde{\mathcal{C}}, \cdot)$ forms an (abelian) group iff for any ideal $\mathfrak{a}$, there exists an ideal $\mathfrak{b}$ such that $\mathfrak{ab}$ is principal. In particular, if A is a Dedekind domain, $\widetilde{\mathcal{C}} = \mathcal{C}$. In this case, the class of principal ideals is the identity of $\mathcal{C}$ and $[\mathfrak{b}]$ is the inverse of $[\mathfrak{a}]$.

Let us go back to number fields. Let K be a number field, then the discussion above shows that the set of ideal classes of $\mathcal{O}_K$ can indeed be given an abelian group structure, which we shall denote by $\mathcal{C}_K$. Formally, $\mathcal{C}_K := \mathcal{I}_K/\mathcal{P}_K$ is the quotient group

[1] In fact, for any number field K, p is ramified in $\mathcal{O}_K$ iff $p \mid d(K)$.

[2] Monoids are semigroups with identity.

of fractional ideals $\mathcal{I}_K$ by the subgroup of principal fractional ideals $\mathcal{P}_K$.

Although both $\mathcal{I}_K$ and $\mathcal{P}_K$ are huge, their quotient turns out to be rather small.

Theorem 1.9 *For any number field K, $\mathcal{C}_K$ is a finite abelian group.*

The idea of the proof is to first show that there exists some constant $\lambda = \lambda(K) > 0$, such that every ideal $\mathfrak{a}$ of $\mathcal{O}_K$ contains a non-zero element α with the property

$$|N_K(\alpha)| \leq \lambda N_K(\mathfrak{a}), \tag{1-11}$$

and then deduce that every ideal class contains some ideal of norm no greater than λ, so the finiteness of $\mathcal{C}_K$ follows from the fact that there exists finitely many ideals of a given norm. To see this, note that for any ideal $\mathfrak{a}$, $N_K(\mathfrak{a}) \in \mathfrak{a}$ since by definition $N_K(\mathfrak{a}) = |\mathcal{O}_K/\mathfrak{a}|$, so $\mathfrak{a}$ is divisible the ideal generated by $N_K(\mathfrak{a})$. But there exists finitely many factors of $(N_K(\mathfrak{a}))$, so we are done.

Although one can deduce (1-11) by algebraic tricks, a more enlightening way to achieve this is to use the geometry of numbers, which also gives us a better bound for λ. So, let us now move to the geometry of numbers.

Suppose the *signature* of K is (s, t), i.e., K has s real and t complex embeddings $(n = s + 2t)$, and let σ_i, $1 \leq i \leq n$ be these embeddings, arranged in such a way

$$\sigma_1, \ldots, \sigma_s; \sigma_{s+1}, \overline{\sigma}_{s+1}, \ldots, \sigma_{s+t}, \overline{\sigma}_{s+t}$$

that the first s ones are real and the rest are complex, and that $\overline{\sigma}_i(\alpha) := \overline{\sigma_i(\alpha)}$. Consider the real vector space $\mathbb{L}^{s,t} := \mathbb{R}^s \times \mathbb{C}^t$ with a *norm*[1]

$$N(\boldsymbol{x}) := x_1 \cdots x_s |x_{s+1}|^2 \cdots |x_{s+t}|^2 \in \mathbb{R},$$

where $\boldsymbol{x} = (x_1, \ldots, x_s; x_{s+1}, \ldots, x_{s+t}) \in \mathbb{L}^{s,t}$. The map

$$\sigma : K \to \mathbb{L}^{s,t}, \quad \alpha \mapsto (\sigma_1(\alpha), \ldots, \sigma_s(\alpha); \sigma_{s+1}(\alpha), \ldots, \sigma_{s+t}(\alpha)), \tag{1-12}$$

σ is a norm preserving $\mathbb{Q}$-algebra homomorphism. Furthermore, σ maps $\mathbb{Q}$-bases of K to $\mathbb{R}$-bases of $\mathbb{L}^{s,t}$, and thus maps additive subgroups of K to lattices of $\mathbb{L}^{s,t}$. Indeed, for any n-tuple $(\alpha_1, \ldots, \alpha_n)$ in K, put

$$\sigma(\alpha_k) = (x_1^{(k)}, \ldots, x_s^{(k)}; y_1^{(k)} + iz_1^{(k)}, \ldots, y_t^{(k)} + iz_t^{(k)}),$$

and let A be the coordinate matrix of these $\sigma(\alpha_j)$'s (view $\mathbb{L}^{s,t}$ as an n-dimensional real vector space with the standard basis)

$$A = \begin{pmatrix} x_1^{(1)} & \cdots & x_s^{(1)} & y_1^{(1)} & z_1^{(1)} & \cdots & y_t^{(1)} & z_t^{(1)} \\ \vdots & & \vdots & \vdots & \vdots & & \vdots & \vdots \\ x_1^{(n)} & \cdots & x_s^{(n)} & y_1^{(n)} & z_1^{(n)} & \cdots & y_t^{(n)} & z_t^{(n)} \end{pmatrix},$$

then a direct computation yields

$$d_K(\alpha_1, \ldots, \alpha_n) = \det(\sigma_i(\alpha_j))^2 = 4^t (\det A)^2.$$

Hence, by Corollary 1.3 we see that the image of any ideal $\mathfrak{a}$ of $\mathcal{O}_K$ is a n-dimensional

[1]Here, the word "norm" is not the same as the usual meaning of the norm of a vector space!

lattice $\sigma(\mathfrak{a})$ of $\mathbb{L}^{s,t}$. Suppose $(\alpha_1, \ldots, \alpha_n)$ is an integral basis of $\mathfrak{a}$, then $\sigma(\mathfrak{a})$ is generated by $(\sigma(\alpha_1), \ldots, \sigma(\alpha_n))$ and has a fundamental domain

$$P = \left\{ \sum_{i=1}^{n} m_i \sigma(\alpha_i) \ : \ 0 \leq m_i < 1, \ i = 1, \ldots, n \right\}.$$

Combining with (1-2), one computes the volume of a fundamental domain P (invariant under change of bases) of $\sigma(\mathfrak{a})$ to be

$$V(P) = \det A = 2^{-t} N_K(\mathfrak{a}) \sqrt{|d(K)|}, \tag{1-13}$$

where $V(\cdot)$ shall always denote the volume of a set $\cdot$ in $\mathbb{R}^n$, and A is as above.

The power of the geometry of numbers lies on the following result, which seems innocent at the first glance:

Theorem 1.10 (Minkowski) *Let L be an n-dimensional lattice in $\mathbb{R}^n$ with fundamental domain P, and let $X \subset \mathbb{R}^n$ be a bounded symmetric (w.r.t. the origin) convex set. If*

$$V(X) > 2^n V(P),$$

then X contains a non-zero element of L. If in addition X is compact, then the result holds if $V(X) \geq 2^n V(P)$.

The proof of this theorem is based on the observation that "if an injective map is locally volume-preserving, then it is globally volume-preserving", which we now state as a lemma. For convenience, let π be the natural map $\mathbb{R}^n \to \mathbb{T}^n$ with kernel L, then it induces a bijection $\varphi : P \to \mathbb{T}^n$. We define the *volume* of a subset $Y \subset \mathbb{T}^n$ by

$$v(Y) = V(\varphi^{-1}(Y)),$$

where $v(Y)$ exists iff $\varphi^{-1}(Y)$ has a volume in $\mathbb{R}^n$.

Lemma 1.11 *Keep notations as above. Suppose X be a bounded set in $\mathbb{R}^n$ and suppose $V(X)$ exists. If $v(\varphi(X)) \neq V(X)$, then $\pi|_X$ is not injective.*

Proof: Since X is bounded, there are only finitely many elements l's in L such that $X_l := X \cap (P + l) \neq \emptyset$. Namely, $X = \sqcup_{i=1}^{m} X_{l_i}$ for some distinct $l_1, \ldots, l_m \in L$. For each i, put $Y_{l_i} = X_{l_i} - l_i \subset T$. Suppose $\varphi|_X$ is injective, then $Y_{l_i} \cap Y_{l_j} = \emptyset$ whenever $i \neq j$. Hence, $V(X_{l_i}) = V(Y_{l_i})$ and $\pi(X_{l_i}) = \pi(Y_{l_i})$, for all $i = 1, \ldots, m$. But

$$v(\pi(X)) = v\left(\pi\left(\bigsqcup_{i=1}^{m} X_{l_i}\right)\right) = V\left(\bigsqcup_{i=1}^{m} Y_{l_i}\right) = \sum_{i=1}^{m} V(Y_{l_i}) = \sum_{i=1}^{m} V(X_{l_i}) = V(X),$$

contradiction! □

We are now ready to prove the Minkowski theorem.

Proof of Theorem 1.10: Double the size of L, we get a lattice $2L$ with a fundamental domain $2P$, and $V(2P) = 2^n V(P)$. We now apply Lemma 1.11 to our new lattice $2L$.

Since $V(X) > 2^n V(P) = v(\mathbb{T}^n)$, by Lemma 1.11 the map $\pi|_X$ cannot be injective,

so there exist $x_1 \neq x_2$, $x_1, x_2 \in X$, such that $\pi(x_1) = \pi(x_2)$. Namely, $0 \neq x_1 - x_2 \in 2L$ and thus $0 \neq (x_1 - x_2)/2 \in L \cap X$ by symmetry and convexity of X.

If X is compact, then the same argument shows that for any $m \in \mathbb{N}^*$, $(1+1/m)X$ contains a non-zero element of L. Let A_m be the set of all such elements, then all A_m's are finite, non-empty, and $A_m \subseteq A_k$ whenever $m \geq k$. Hence, $A := \cap_{m \geq 1} A_m \neq \emptyset$. Pick any $x \in A$, $x \in \cap_{m \geq 1}(1 + 1/m)X = \overline{X} = X$, as desired. □

Intuitively, the Minkowski theorem merely states that if the volume of a "nice" set X is large enough, then it must contains some non-zero lattice point, but this leads to many non-trivial and important consequence, such as an elegant proof of the two- and four-squares theorem. (See for instance [ST16] p. 142-144, Theorem 7.2 and 7.3.)

Here, given a lattice L with fundamental domain P of volume V in $\mathbb{L}^{s,t}$, if we pick some positive real numbers $c_1, \ldots, c_{s+t}$ such that

$$c_1 \cdot \cdots c_{s+t} \geq \left(\frac{4}{\pi}\right)^t V,$$

then the set $X := \{(\boldsymbol{x} \in \mathbb{L}^{s,t} \ : \ |x_i| \leq c_i, 1 \leq i \leq s, \ |x_{s+j}|^2 \leq c_{s+j}\}$ contains a non-zero lattice point. So, interpreting this observation to ideals of $\mathcal{O}_K$, and combining with (1-13), we deduce that every ideal $\mathfrak{a}$ of $\mathcal{O}_K$ contains some $\alpha \neq 0 \in \mathfrak{a}$ with

$$|N_K(\alpha)| \leq \left(\frac{2}{\pi}\right)^t N_K(\mathfrak{a})\sqrt{|d(K)|}. \tag{1-14}$$

Thanks to our discussions above, the proof of Theorem 1.9 is now not so hard.

Proof of Theorem 1.9: Let C be an ideal class, and let $\mathfrak{a}$ be an ideal in its inverse class C^{-1}. Then, there exists some $0 \neq \alpha \in \mathfrak{a}$ such that (1-14) holds. Since $(\alpha) \subseteq \mathfrak{a}$, there exists an ideal $\mathfrak{b}$ such that $\mathfrak{a}\mathfrak{b} = (\alpha)$, so $\mathfrak{b} \in C$ and

$$N_K(\mathfrak{b}) \leq \left(\frac{2}{\pi}\right)^t \sqrt{|d(K)|}^{[1]}$$

Hence, every ideal class contains some ideal whose norm is bounded by a constant. So, it suffices to show that there are only finitely many ideals of a given norm. To see this, note that for any ideal $\mathfrak{c}$, $m := N_K(\mathfrak{c}) \in \mathfrak{c}$ since by definition $m = |\mathcal{O}_K/\mathfrak{c}|$, so $(m) \subseteq \mathfrak{c}$ and by Theorem 1.5 (m) has only finitely many factors. □

In conclusion, the group $\mathcal{C}_K$ is indeed finite, and we shall denote its order by h_K, or simply by h if the number field K is clear.

1.3.2 The unit group

Let us now determine the structure of the multiplicative subgroup U_K of all units in our number ring $\mathcal{O}_K$ in the spirit of the geometry of numbers. It is clear that U_K contains a finite torsion subgroup W_K consisting of all the roots of unity in K. W_K is cyclic since any finite multiplicative subgroup of a field is cyclic. Moreover,

[1] In fact, we can do better. A clever choice of X will give us a stronger bound $(n^n/n!) \cdot (2/\pi)^t \sqrt{|d(K)|}$, which is called the *Minkowski constant*. This is really a nice result since it is helpful for computations and it gets small quickly as n increases.

Theorem 1.12 (Dirichlet unit theorem) *Keeping notations as above, we have*

$$U_K = W_K \times V_K,$$

where V_K is a free abelian group of rank $s+t-1$.

In particular, this theorem tells us that except for the cases of $\mathbb{Q}$ (where $s=1, t=0$) and imaginary quadratic fields (where $s=0, t=1$), the unit group U_K is always *infinite*.

To prove the theorem, we define a *logarithm map*[1]

$$L : K \setminus \{0\} =: K^* \xrightarrow{\sigma} \mathbb{L}^{s,t} \xrightarrow{l} \mathbb{R}^{s+t}, \quad \alpha \mapsto \sigma(\alpha) \mapsto \begin{cases} \log|\sigma_i(\alpha)|, & 1 \le i \le s \\ 2\log|\sigma_{s+j}(\alpha)|, & 1 \le j \le t \end{cases}, \tag{1-15}$$

which induces a group homomorphism $U_K \to \mathbb{R}^{s+t}$ (with a slight abuse of notations, we shall denote this also by L) with the following properties:

1) $\mathrm{Ker}(L) = W_K$;

2) $\mathrm{Im}(L)$ is an additive subgroup contained in a hyper-surface H in $\mathbb{R}^{s+t}$, given by

$$H = \{(x_1, \dots, x_{s+t}) \in \mathbb{R}^{s+t} \ : \ x_1 + \cdots + x_{s+t} = 0\};$$

3) $\mathrm{Im}(L)$ is discrete, and hence a lattice of dimension $r \le s+t-1$. In particular, $U = W_K \times V_K$, where V_K is a free abelian group of rank r;

4) $r = s+t-1$.

So we now prove these properties, and Theorem 1.12 follows.

Proof: 1). We claim that $\alpha \in W_K$ iff $|\sigma_k(\alpha)| = 1, \forall\, 1 \le k \le n$. Clearly, $\alpha \in W_K$ implies all the $\sigma_k(\alpha)$'s have absolute value 1; Conversely, if all the $\sigma_k(\alpha)$'s have absolute value 1, then the same is true for every α^m, $m \ge 1$. But the coefficient of the minimal polynomials (over $\mathbb{Q}$) of the α^m's are integral and bounded, so there are only finitely many options. Hence, the set $\{\alpha^m\}_{m \ge 1}$ cannot be pairwise distinct, so $\alpha \in W_K$.

2). Note that for any $\alpha \in K^*$, the sum of all coordinates of $L(\alpha)$ is $\log|N_K(\alpha)|$. So it suffices to show that $\alpha \in U_K$ iff $|N_K(\alpha)| = 1$, which is clear since $N_K(\alpha)$ has to be an invertible rational integer.

3). Given any bounded subset B of $\mathbb{R}^{s+t}$, if $L(\alpha) \in B$, then each $|\sigma_k(\alpha)|$ is bounded, so a similar argument as in 1) shows again that there exist finitely many such α's, so $\mathrm{Im}(L)$ is discrete.

4). The proof accomplishes in three steps.

a) We first claim that fixing any $1 \le k \le s+t$, for each $0 \ne \alpha \in \mathcal{O}_K$ there exists $0 \ne \beta \in \mathcal{O}_K$ with

$$|N_K(\beta)| \le \left(\frac{2}{\pi}\right)^t \sqrt{|d(K)|} =: M,$$

and such that if we write $L(\alpha) = (a_1, \dots, a_{s+t})$, $L(\beta) = (b_1, \dots, b_{s+t})$, then $b_i < a_i$ for all $i \ne k$.

[1]The map l is actually defined for any $\boldsymbol{x} = (x_1, \dots, x_{s+t}) \in \mathbb{L}^{s,t}$ with $N(\boldsymbol{x}) \ne 0$, which sends x_i to $\log|x_i|$ for $1 \le i \le s$, and x_{s+j} to $2\log|x_{s+j}|$ for $1 \le j \le t$.

To see this, we apply Theorem 1.10 to the lattice $L = \sigma(\mathcal{O}_K)$ and a special choice of a compact, symmetric and convex set X. For instance, if $k = 1$, put

$$X = \left\{(x_1 \dots, x_n) \in \mathbb{R}^n \,:\, |x_i| \leq c_i, 1 \leq i \leq s, x_j^2 + x_{j+t}^2 \leq |c_j|, s+1 \leq j \leq s+t\right\},$$

where $0 \leq c_i \leq e^{a_i}, 2 \leq i \leq s+t$ and $c_1 = (c_2 \cdots c_{s+t})^{-1} M$. Note that $V(X) = 2^n M$, by Theorem 1.10 and (1-13) we see that X contains a non-zero element of $\sigma(\mathcal{O}_K)$, which gives us some $0 \neq \beta \in \mathcal{O}_K$, as desired.

b) By a), fixing any $1 \leq k \leq s+t$, we can now find a special unit u_k such that if we write

$$L(u_k) = (y_{k1}, \dots, y_{k(s+t)}),$$

then $y_{ik} < 0$ whenever $i \neq k$.

To begin with, pick an arbitrary $0 \neq \gamma_1 \in \mathcal{O}_K$, then by a) we can find a sequence $\gamma_2, \gamma_3, \cdots$ of non-zero elements in $\mathcal{O}_K$ such that whenever $i \neq k$, the i-th coordinate of $L(\gamma_{j+1})$ is strictly smaller than that of $L(\gamma_j)$ and that each has norm $|N_K(\gamma_j)| \leq M$. Notice that there are only finitely many ideals of a bounded norm, the principal ideals generated by the γ_i's cannot be pairwise distinct. So, fixing some pair $h > j$ such that $(\gamma_j) = (\gamma_h)$, we get $\gamma_h = u_k \gamma_j$ for some u_k, and this u_k is what we required.

c) For our special units $u_1, \dots, u_k$, the coordinate matrix (y_{jk}) of $L(u_1), \dots, L(u_{s+t})$ has rank $s+t-1$, which implies 4).

More generally, we will prove the following lemma and c) follows immediately.

Lemma 1.13 *Given a matrix $A = (a_{ij}) \in M_l(\mathbb{R})$, all of whose diagonal elements are positive while others are negative, if each row-sum of A is 0, then rank$(A) = l - 1$.*

Proof of Lemma 1.13: On the one hand, we know that $\det(A) = 0$ since each row-sum is 0, so $\operatorname{rank}(A) \leq l-1$; On the other hand, the first $(l-1)$ columns v_i's of A are linearly independent so $\operatorname{rank}(A) \geq l-1$. Otherwise, there exist some non-trivial $t_1, \dots, t_{l-1}$ such that $\sum_{i=1}^{l-1} t_i v_i = 0$, and we may assume $t_k = 1$ for some k and all other $t_i \leq 1$. Then, by looking at the k-th row we get

$$0 = \sum_{i=1}^{l-1} t_i a_{ki} \geq \sum_{i=1}^{l-1} a_{ki} > \sum_{i=1}^{l} a_{ki} = 0,$$

contradiction! □

Finally, our proof is now complete. □

Remark 1.14 *Equivalently, Theorem 1.12 states that there exist $u_1, \dots, u_r \in U_K$, such that every unit $u \in U_K$ can be uniquely represented as*

$$u = w u_1^{n_1} u_2^{n_2} \cdots u_r^{n_r},$$

*where $r = s+t-1$, $w \in W_K$ and $n_i \in \mathbb{Z}$, $\forall\, 1 \leq i \leq r$. Such an r-tuple $(u_1, \dots, u_r)$ is called a **system of fundamental units of K**. Suppose $L(u_i) = (x_{i1}, \dots, x_{i(r+1)})$, we then put*

$$r(u_1, \dots, u_r) := |det(x_{ij})_{1 \leq i,j \leq r}|.$$

One can check that $r(u_1, \ldots, u_r)$ is independent of the choice of a system of fundamental units, so we call this constant the ***regulator of K****, and denote it by $r(K)$ instead.*

Chapter II

When Zeta Functions Meet Number Fields

In the first chapter, we recalled some algebraic and geometric aspects of number fields. It turns out that analytic methods, which were first introduced by Dirichlet and Riemann, also play an important role in many essential problems related to number fields, and they provide a natural entry to the class field theory.

Let us now step along this direction by introducing the Dedekind zeta function $\zeta_K(s)$ of a given number field K and discussing its analytic properties. We shall follow much of section 5.1 and 5.2 of [BS86] and chapter 7 of [M18].

2.1 Introduction

2.1.1 The Dedekind zeta function $\zeta_K(s)$

Analogous to the Riemann zeta function

$$\zeta(s) = \sum_{n\geq 1} \frac{1}{n^s}, \quad \mathrm{Re}(s) > 1,$$

one can associate a zeta function to an arbitrary number field K of degree n by summing over all the ideals $\mathfrak{a}$ of $\mathcal{O}_K$ and replacing n by the norm of $\mathfrak{a}$, which is

$$\zeta_K(s) := \sum_{\mathfrak{a}} \frac{1}{N(\mathfrak{a})^s}, \tag{2-1}$$

where we omit K from notations and simply write $N(\mathfrak{a})$ to denote the norm of $\mathfrak{a}$. This is called the **Dedekind zeta function of K**. Similar to the Euler product

$$\zeta(s) = \prod_{p} \left(1 - \frac{1}{p^s}\right)^{-1}, \quad \mathrm{Re}(s) > 1,$$

where p runs through all prime numbers, by Theorem 1.5 the Dedekind zeta function $\zeta_k(s)$ can also be seen as an infinite product of all prime ideals of $\mathcal{O}_K$, i.e., formally we can write[1]

$$\zeta_K(s) = \prod_{\mathfrak{p}} \left(1 - \frac{1}{N(\mathfrak{p})^s}\right)^{-1}. \tag{2-2}$$

It is not hard to see that this product converges absolutely if $\mathrm{Re}(s) > 1$, since every prime ideal lies over at most n primes (Theorem 1.8). To be precise,

$$\sum_{N(\mathfrak{a})\leq x} \frac{1}{N(\mathfrak{a})^\sigma} \leq \sum_{p\leq x} \sum_{\mathfrak{a}|p\mathcal{O}_K} \frac{1}{N(\mathfrak{a})^\sigma} \leq n \sum_{p\leq x} p^{-\sigma} \leq n \sum_{m\leq x} m^{-\sigma},$$

[1]The Euler product can be understood as an infinite product of all (non-Archimedean) valuations on K as well, which is (by Ostrowski's theorem) in one-to-one correspondence between all prime ideals of $\mathcal{O}_K$.

the last expression converges as $x \to \infty$ when $\sigma > 1$. Where, by convention we write $s = \sigma + i\tau$. In this case, the Euler product is indeed valid, and the proof is exactly the same as that of the Riemann zeta function $\zeta(s)$. Moreover, $\zeta_K(s)$ has many analytic properties similar to those of $\zeta(s)$:

1) $\zeta_K(s)$ admits an analytic continuation to the right half-plane $\mathrm{Re}(s) > (1-1/n)$ that is holomorphic except for a simple pole at $s = 1$;

2) Suppose K has signature (s, t)[1], then the residue of $\zeta_K(s)$ at $s = 1$ is given by

$$\mathrm{Res}_{s=1}\zeta_K(s) = h\kappa, \tag{2-3}$$

where $h = |\mathcal{C}_K|$ is the class number of K and

$$\kappa = \frac{2^{s+t}\pi^t r(K)}{m\sqrt{|d(K)|}} \tag{2-4}$$

is a constant which depends on many invariants of the field K, namely, the number m of roots of unity in K, the discriminant $d(K)$ and the regulator $r(K)$.

3) * With notations as above, the "completed Dedekind zeta function" of K

$$\xi_K(s) = \left(\frac{|d(K)|}{2^{2q}\pi^n}\right)^{s/2} \Gamma(s/2)^p \Gamma(s/2)^q \zeta_K(s), \tag{2-5}$$

where $\Gamma(s)$ is the complex Gamma function, satisfies a functional equation

$$\xi_K(s) = C \cdot \xi_K(1-s) \tag{2-6}$$

for some constant $C = C(K) \in \mathbb{C}$ with $|C| = 1$. In particular, $\xi_K(s)$ admits further an analytic continuation to the whole complex plane that is holomorphic except for a simple pole at $s = 1$.

We shall only prove 1) and 2) here via techniques from the geometry of numbers, while omit the heavy computations of 3). To motivate our proof, let us now consider the simplest imaginary quadratic field $\mathbb{Q}(i)$ as a first example.

2.1.2 A baby case: $K = \mathbb{Q}(i)$

The field $K = \mathbb{Q}(i)$ has no real but two complex embeddings; its discriminant is $d(K) = -4$; its number ring is the ring of Gaussian integers $\mathbb{Z}[i]$, which is a PID and hence $h = 1$; its group of units U_K has exactly 4 elements $\pm 1, \pm i$, i.e., $U_K = W_K \cong \mathbb{Z}/4\mathbb{Z}$, so its regulator $r(K) = 1$.

Now, compute that

$$\begin{aligned}
\zeta_K(s) &= \sum_{\mathfrak{a}} \frac{1}{N(\mathfrak{a})^s} \\
&= \sum_{(m+ni)/U_K} \frac{1}{(m^2+n^2)^s} \qquad (2\text{-}7) \\
&= \frac{1}{4} \sum_{\mathbf{0} \neq (m,n) \in \mathbb{Z}^2} \frac{1}{(m^2+n^2)^s}, \qquad (2\text{-}8)
\end{aligned}$$

[1]Warning! I hope this notation is not too confusing, since s also stands for the complex variable in this chapter. After all, it should be clear what we mean.

so from (2-8) we also see $\zeta_K(s)$ converges (absolutely) iff $\mathrm{Re}(s) > 1$ by Cauchy's integral test. On the other hand, set

$$D = \{(x, y) \in \mathbb{R}^2 \,:\, x \geq 0, y > 0, \text{ and } (x, y) \neq \mathbf{0}\},$$

then we can also view (2-7) as a summation over points on the lattice $\Lambda = \mathbb{Z}+\mathbb{Z}i \subset \mathbb{L}^{01}$ (see section 1.3.1) and in the cone D, i.e.,

$$\zeta_K(s) = \sum_{\boldsymbol{x}\in\Lambda\cap D} \frac{1}{N(\boldsymbol{x})^s}. \tag{2-9}$$

To show that $\zeta_K(s)$ admits an analytic continuation to $\mathrm{Re}(s) > 1/2$ and compute its residue of at $s = 1$, we put $D_n := \#\{(\boldsymbol{x} \in \Lambda \cap D \,:\, N(\boldsymbol{x}) = n\}$, so (2-9) becomes

$$\zeta_K(s) = \sum_{n\geq 1} \frac{D_n}{n^s}. \tag{2-10}$$

Hence, we need to estimate symptotically the sum $A_n = \sum_{k=1}^{n} D_n$, which is the number of integral points in the quarter-circle region $T_n = \{\boldsymbol{x} \in D \,:\, N(\boldsymbol{x}) \leq n\}$.

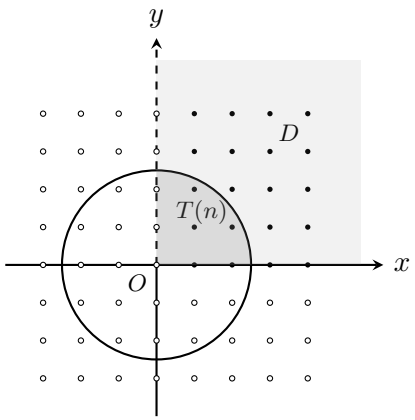


Figure 2.1.1

Fortunately, this is closely related to the *Gauss circle problem*:

Theorem 2.1 (Gauss) *Let $C(r)$ be the number of integral points in the circle centered at the origin with radius r, then*

$$C(r) = \pi r^2 + E(r), \tag{2-11}$$

where $|E(r)| \leq 4\sqrt{2}\pi r$.

Proof: Since the maximum distance between any two points in the unit square is $\sqrt{2}$, all the unit squares intersecting the boundary of the circle are contained in the annulus $A(r)$ of width $2\sqrt{2}$ with radii $r + \sqrt{2}$ and $r - \sqrt{2}$ So for any $r > \sqrt{2}$,

$$|E(r)| = |C(r) - \pi r^2| \leq S(A(r)) = \pi\left(\left(r + \sqrt{2}\right)^2 - \left(r - \sqrt{2}\right)^2\right) = 4\sqrt{2}\pi r,$$

where $S(\cdot)$ is the area of $\cdot$. □

Remark 2.2 *If we write $E(r) = O(r^t)$, then clearly $t \leq 1$ by Theorem 2.1. Hardy and*

Landau independently found a lower bound of $|E(r)|$ *in 1915 by showing that*

$$|E(r)| \neq o\left(r^{1/2}(\log r)^{1/4}\right),$$

so $t > 1/2$. *It is conjectured that the correct bound should be*

$$|E(r)| = O(r^{1/2+\epsilon})$$

for any $\epsilon > 0$. *Currently, the best bounds on* t *are*

$$\frac{1}{2} < t \leq \frac{517}{824} \approx 0.6274,$$

where the the upper bound was proved by Bourgain and Watt in 2017 [BW17].

Theorem 2.1 yields $A_n = (\pi/4)n + O(n^{1/2})$, so $\zeta_K(s)$ can be written as

$$\begin{aligned}\zeta_K(s) &= \sum_{n\geq 1} \frac{\pi/4}{n^s} + \sum_{n\geq 1} \frac{D_n - \pi/4}{n^s} \\ &= \frac{\pi}{4}\zeta(s) + f(s), \end{aligned} \tag{2-12}$$

where $f(s)$ is a Dirichlet series with coefficients $a_n = D_n - \pi/4$, $\sum_{i=1}^{n} a_i = O(n^{1/2})$, and from general theory of Dirichlet series we know its abscissa of convergence is $1/2$. In particular, $\zeta_K(s)$ admits an analytic continuation to $\mathrm{Re}(s) > 1/2$ and has a simple pole that $s = 1$, of residue $\pi/4$.

We wish to generalize our argument for the case of $\mathbb{Q}(i)$ to any number field K. However, there are two challenges: ideals of $\mathcal{O}_K$ may not always be principal, so (2-7) fails, and the unit group U_K may be infinite, so (2-8) fails. We will see how to overcome these difficulties in the next section, but the general strategy is as follows:

1) Break the Dedekind zeta function $\zeta_K(s)$ into several series (according to ideal classes), so that each of them can be written in the form of (2-7).

2) Find a region D with "nice" properties, so that each series in 1) can be further simplified into the form of (2-9).

3) Derive an asymptotic formula for the number of lattice points in D with norm $\leq x$ as $x \to \infty$;

4) Combine the results and play the same trick as that of (2-12).

We will make these ideas precise via the geometry of numbers in the next section to prove 1) and 2) simultaneously.

2.2 The analytic class number formula

Let K be a number field of degree n, and suppose it has signature (s, t). By Theorem 1.12, the group U_K of units in $\mathcal{O}_K$ is a direct product $W_K \times V_K$, where W_K is a finite cyclic group and V_K is free abelian of order $s + t - 1$. If we denote the order of W_K by m, then $W_K = \langle \zeta_m \rangle$, where $\zeta_m = e^{2\pi i/m}$ is an m-th root of unity.

As promised, we now prove that $\zeta_K(s)$ can be analytic continued to the right half-plane $\mathrm{Re}(s) > (1 - 1/n)$ that is holomorphic except for a simple pole at $s = 1$, and deduce an explicit formula for its residue formula at $s = 1$.

The first step is to put $\zeta_K(s)$ in a form we can handle.

2.2.1 A more convenient form of $f_C(s)$

In general, the class number h of K may not be 1 ($h = 1$ iff $\mathcal{O}_K$ is a PID[1]), so one cannot expect to write $\zeta_K(s)$ directly in the form (2-7). To simplify the situation, we break the series (2-1) into the sum of h series

$$\zeta_K(s) = \sum_{C \in \mathcal{C}_K} \sum_{\mathfrak{a} \in C} \frac{1}{N(\mathfrak{a})^s}, \tag{2-13}$$

and consider

$$f_C(s) := \sum_{\mathfrak{a} \in C} \frac{1}{N(\mathfrak{a})^s}$$

for each ideal class C. If all the $f_C(s)$'s have our desired properties, then so does $\zeta_K(s)$. Now, by Lemma 1.6 and Theorem 1.9 we fix an ideal $\mathfrak{b}$ in C^{-1}, then $\mathfrak{ab} = (\alpha)$ is principal for any $\mathfrak{a}$ in C. In other words, the mapping $\mathfrak{a} \mapsto (\alpha)$ establishes a one-to-one correspondence between ideals in C and principal ideals divisible by $\mathfrak{b}$. Since norm is completely multiplicative (Corollary 1.7), we obtain that

$$f_C(s) = N(\mathfrak{b})^s \sum_{\mathfrak{b} \mid (\alpha)} \frac{1}{|N(\alpha)|^s}. \tag{2-14}$$

Further note that elements $\alpha \in \mathcal{O}_K$ with $\mathfrak{b} \mid (\alpha)$ are exactly those elements in $\mathfrak{b}$ (in Dedekind domains, ideals $\mathfrak{a} \mid \mathfrak{b}$ iff $\mathfrak{b} \subseteq \mathfrak{a}$), (2-14) becomes

$$f_C(s) = N(\mathfrak{b})^s \sum_{\substack{(\alpha)/U_K \\ \alpha \in \mathfrak{b}}} \frac{1}{|N(\alpha)|^s}, \tag{2-15}$$

where $(\alpha)/U_K$ represents the class of associate numbers of α.

Now, we use the geometry of numbers to transfer (2-15) into a more convenient form. Namely, under the map $\sigma : K \mapsto \mathbb{L}^{s,t}$ (see (1-12)), $\mathfrak{b}$ is a n-dimensional lattice Λ in $\mathbb{L}^{s,t}$, and we would like to find a *fundamental domain*[2] of the quotient space $\sigma(U_K)\backslash\mathbb{L}^{s,t}$ (like the cone D we constructed for $\mathbb{Q}(i)$), which is characterized by following property: For every class of non-zero associate numbers of the field K, there exists precisely one number whose geometric representation in $\mathbb{L}^{s,t}$ lies in the fundamental domain. Given such a fundamental domain (still denoted by D), (2-15) can now be written as

$$f_C(s) = N(\mathfrak{b})^s \sum_{\boldsymbol{x} \in \Lambda \cap D} \frac{1}{|N(\boldsymbol{x})|^s}, \tag{2-16}$$

which allows us to study the analytic properties of $f_C(s)$ via the asymptotic behavior of $\#\{\boldsymbol{x} \in \Lambda \cap D \,:\, N(\boldsymbol{x}) \leq x\}$ as $x \to \infty$.

Hence, our next step is to construct explicitly a "canonical" fundamental domain D, which turns out to always be a cone.

---

[1] In fact, $\mathcal{O}_K$ is a PID iff it is a UFD, and one can check that $\mathbb{Q}(\zeta_{23})$ is not a UFD, where $\zeta_{23} = e^{2\pi i/23}$.

[2] Pedantically, this is not exactly the fundamental domain of $\sigma(U_K)\backslash\mathbb{L}^{p,q}$ in the usual sense, since we will remove all the points in $\mathbb{L}^{s,t}$ of norm 0.

2.2.2 The fundamental domain D

Recall that the logarithm map $L : K^* \to \mathbb{R}^{s+t}$ (see (1-15)) induces a group homomorphism $U_K \to \mathbb{R}^{s+t}$ such that $\mathrm{Ker}(L) = W_k$ and $\mathrm{Im}(L) \cong V_K$ such that is a lattice of dimension $r = s+t-1$. In addition, let $(u_1, \ldots, u_r)$ be a system of fundamental units of K, then the vectors $L(u_i) = l(\sigma(u_i))$, $1 \le i \le r$ form a basis for the hyper-surface

$$H = \{(x_1, \ldots, x_{s+t}) \in \mathbb{R}^{s+t} \,:\, x_1 + \cdots + x_{s+t} = 0\}.$$

Hence, if we put $l^* = (\underbrace{1, \ldots, 1}_{s}; \underbrace{2, \ldots, 2}_{t})$ and write $l_i = l(\sigma(u_i))$, then $(l^*, l_1, \ldots, l_r)$ forms a basis of $\mathbb{R}^{s+t}$. In particular, for any $\boldsymbol{x} \in \mathbb{L}^{s,t}$ with $N(\boldsymbol{x}) \neq 0$, the vector $l(\boldsymbol{x}) \in \mathbb{R}^{s+t}$ can be written uniquely in the form

$$l(\boldsymbol{x}) = y + y_1 l_1 + \cdots + y_r l_r \tag{2-17}$$

for some real numbers $y, y_1, \ldots, y_r$.

Theorem 2.3 *The subset $D \subset \mathbb{L}^{s,t}$ consisting of all points $\boldsymbol{x} = (x_1, \ldots, x_{s+t})$ which satisfy the following conditions*

1) $N(\boldsymbol{x}) \neq 0$;

2) $0 \le \arg x_1 < 2\pi/m$;

3) In the representation (2-17) above, $0 \le y_i < 1$ for all $i = 1, \ldots, r$,

forms a fundamental domain of $\sigma(U_K)\backslash\mathbb{L}^{s,t}$.

In particular, if $s \ge 1$ then K has a real embedding and thus $m = 2$, so condition 2) is nothing but $x_1 \ge 0$.

Lemma 2.4 *For any $\boldsymbol{x} \in \mathbb{L}^{s,t}$ with $N(\boldsymbol{x}) \neq 0$, $\boldsymbol{x}$ has a unique representation in the form*

$$\boldsymbol{x} = \boldsymbol{x}'\sigma(u) \tag{2-18}$$

for some $\boldsymbol{x}' \in D$ and $u \in U_K$.

Proof: To find such a representation, we write

$$l(\boldsymbol{x}) = y + y_1 l_1 + \cdots + y_r l_r$$

for some real numbers $y, y_1, \ldots, y_r$, and set $k_i = \lfloor y_i \rfloor$, $y_i' = y_i - k_i \in [0, 1)$. Then,

$$\begin{aligned} l(\boldsymbol{x}) &= y l^* + y_1' l_1 + \cdots + y_r' l_r + (k_1 l_1 + \cdots k_r l_r) \\ &= y l^* + y_1' l_1 + \cdots + y_r' l_r + l(\sigma(\underbrace{u_1^{k_1} \cdots u_r^{k_r}}_{:=\widetilde{u}})), \end{aligned}$$

and thus $l(\boldsymbol{x}\sigma(\widetilde{u}^{-1})) = y l^* + y_1' l_1 + \cdots + y_r' l_r$ for some $0 \le y_i \le 1$, $i = 1, \ldots, r$. Let $\widetilde{\boldsymbol{x}} := \boldsymbol{x}\sigma(\widetilde{u}^{-1})$, then it is left to rotate $\widetilde{\boldsymbol{x}}$ such that its first coordinate x_1 has argument $0 \le \arg < (2\pi/m)$, which can be done by multiplying ζ_m^{-k} ($\zeta_m \in W_K$) for some k. Hence, setting $\boldsymbol{x}' := \boldsymbol{x}\sigma(\widetilde{u}^{-1}\zeta_m^{-k}) \in D$, then $\boldsymbol{x} = \boldsymbol{x}'\sigma(u\zeta_m^k)$ is in the desired form.

If $\boldsymbol{x}$ allows two such representations $\boldsymbol{x} = \boldsymbol{x}_1'\sigma(u_1) = \boldsymbol{x}_2'\sigma(u_2)$, then

$$l(\boldsymbol{x}_1') - l(\boldsymbol{x}_2') = l(\sigma(u_2)) - l(\sigma(u_1)).$$

Since the $\sigma(u_i)$'s are integral linear combinations of the vectors $(l_1, \ldots, l_r)$, this equality is possible only when $l(\boldsymbol{x}'_1) = l(\boldsymbol{x}'_2)$ and hence $\boldsymbol{x}'_1 = \zeta \boldsymbol{x}'_2$ for some m-th root of unity ζ, but both $\boldsymbol{x}'_1$ and $\boldsymbol{x}'_2$ are in D, so $\zeta = 1$ and the result follows. □

Proof of Theorem 2.3: For any $\alpha \in K^*$, $\sigma(\alpha) = \boldsymbol{x} \in \mathbb{L}^{s,t}$ has norm $N(\boldsymbol{x}) = N(\alpha) \neq 0$, so by Lemma 2.4 it has a unique representation in the form $\boldsymbol{x}'\sigma(u)$ for some $\boldsymbol{x}' \in D$ and $u \in U_K$, so the number $\beta = \alpha u^{-1}$ is associate with α, whose geometric representation is $\boldsymbol{x}' \in D$. The uniqueness of β follows from the uniqueness of (2-18). □

Remark 2.5 *Note that for any $k > 0$,*

$$l(k\boldsymbol{x}) = (\log k, \ldots, \log k; 2\log k, \ldots, 2\log k) + l(\boldsymbol{x}) = (\log k)l^* + l(\boldsymbol{x}),$$

$N(k\boldsymbol{x}) = k^n N(\boldsymbol{x})$, and that $\arg(k\boldsymbol{x}) = \arg \boldsymbol{x}$, if $\boldsymbol{x} \in D$ then so does $k\boldsymbol{x}$. Hence, D is a cone in $\mathbb{L}^{s,t}$.

As an example, let us find the fundamental domain D for quadratic fields explicitly. For imaginary quadratic fields, $s = 0, t = 1$ so D is relatively simple, given by

$$D = \{\boldsymbol{x} = x + yi \in \mathbb{C}^* \ : \ 0 \leq \arg \boldsymbol{x} < 2\pi/m\},$$

which looks like figure 2.1.1 (the case $K = \mathbb{Q}(i)$); For real quadratic fields, $s = 2, t = 0$, $\sigma_1 = \mathrm{id}$, $\sigma_2 = -\mathrm{id}$ and $r = s + t - 1 = 1$. Let u be a fundamental unit, then we may assume $u > 1$ since $-u, 1/u, -1/u$ are also fundamental units. If $\boldsymbol{x} = (x_1, x_2) \in \mathbb{L}^{2,0} = \mathbb{R}^2$, $N(\boldsymbol{x}) = x_1 x_2 \neq 0$, then $l(\boldsymbol{x}) = (\log|x_1|, \log|x_2|)$. (2-17) now becomes

$$l(\boldsymbol{x}) = y(1, 1) + y_1(\log u, -\log u).$$

Namely,

$$\begin{cases} \log|x_1| = y + y_1 \log u, \\ \log|x_2| = y - y_1 \log u. \end{cases}$$

Hence, $\log|x_1| = \log|x_2| + 2y_1 \log u \Leftrightarrow |x_1| = |x_2|u^{2y_1} \Leftrightarrow |x_2/x_1| = u^{2y_1}$. The fundamental domain D is shown in the following figure:

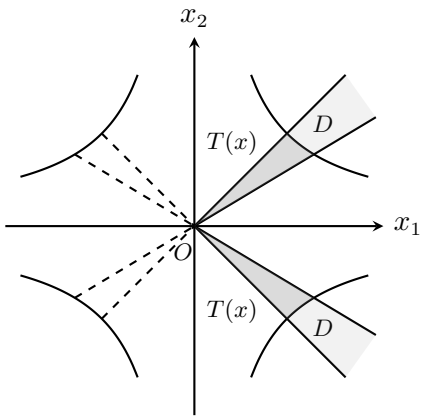


Figure 2.2.2

Let $T_x := \{\boldsymbol{x} \in \Lambda \cap D \ : \ N(\boldsymbol{x}) \leq x\}$, our third step now is to derive an asymptotic

formula for the number $D(x)$ of Λ-lattice points in T_x as $x \to \infty$. In fact, we will show that

$$D(x) = \frac{2^{s+t}\pi^t r(K)}{mN(\mathfrak{b})\sqrt{|d(K)|}}x + O(x^{1-\frac{1}{n}}),$$

and hence deduce 1) and 2).

2.2.3 Asymptotic behavior of $D(x)$

Observe that Λ-lattice points are in one-to-one correspondence with $(x^{-1/n}\Lambda) =: \Lambda_x$-lattice points in T_1 (we shall denote just by T below), and that if P is a fundamental domain of Λ, then so is $P_x := x^{-1/n}P$ of Λ_x. Then, the number $D(x)$ of Λ_x-lattice points in T is roughly the volume of T divided by the volume of the fundamental domain P_x of Λ_x, but with an error term of order[1]

$$O(1/S(P_x)) = O((x^{\frac{1}{n}})^{n-1}) = O(x^{1-\frac{1}{n}}),$$

where $S(P(x))$ is the surface area of P_x. Namely,

$$D(x) = \frac{V(T_1)}{V(P_x)} + O(x^{1-\frac{1}{n}}). \tag{2-19}$$

Since we have seen in (1-13) that

$$V(P_x) = x^{-1}2^{-t}N(\mathfrak{b})\sqrt{|d(K)|}, \tag{2-20}$$

it suffices to compute the volume of T_1. We will first show that T_1 is bounded, and then replace it with another set defined by simpler conditions to show its volume exists and actually compute it.

To see that T_1 is bounded, first note that in every ray contained in the cone X, there exists precisely one point $\boldsymbol{x}$ with $N(\boldsymbol{x}) = 1$. Denote the set of all such points by S, then

$$T_1 = \{tx \,:\, x \in S, 0 \le t \le 1\}.$$

Now, for any $\boldsymbol{x} \in \mathbb{L}^{s,t}$ with non-zero norm, on the left hand side of (2-17), the sum of components of this vector is $\log|N(\boldsymbol{x})|$, while on the right hand side it is $(s+2t)y = ny$ since the norm of a unit is ± 1. Hence, $ny = \log|N(\boldsymbol{x})|$ and (2-17) becomes

$$l(\boldsymbol{x}) = \frac{\log|N(\boldsymbol{x})|}{n}l^* + y_1 l_1 + \cdots + y_r l_r. \tag{2-21}$$

If $\boldsymbol{x} \in S$, then $\log|N(\boldsymbol{x})| = 0$, so $l(\boldsymbol{x}) = y_1 l_1 + \cdots + y_r l_r$ for some y_i's with $0 \le y_i < 1$, $i = 1, \ldots, r$. In particular, the components of $l(\boldsymbol{x})$ are bounded, and by the definition of l (1-15) we conclude that T_1 is bounded.

Notice that for any unit $u \in U_K$, the linear map on $\mathbb{L}^{s,t}$ given by $\boldsymbol{x} \mapsto \sigma(u)\boldsymbol{x}$ is order preserving because the determinant of this transformation (w.r.t. the standard basis) is $N(\sigma(u)) = \pm 1$. It follows that for each $0 \le k \le m-1$, the set $\zeta_m^k T_1$ has the same volume as that of T_1 (provided it exists). These $\zeta_m^k T_1$'s are pairwise disjoint, and

[1] Think of approximating the volume (assume it exists) of T_1 via the Riemann sum $D(x)V(P_x)$ as $x \to \infty$, then $D(x)$ is roughly $V(P_x)/V(T_1)$, and the error comes from Λ_x-lattice points on the surface of T_1.

their union $\cup_{k=0}^{m-1}\zeta_m^k T_1$ consists of all points $\boldsymbol{x}\in\mathbb{L}^{s,t}$ for which

1) $0<N(\boldsymbol{x})\leq 1$;
2) the coefficients of $l(\boldsymbol{x})$ in (2-21) satisfy $0\leq y_i<1$ for all $i=1,\ldots,r$.

For instance, if K is an imaginary quadratic field, then the set $\cup_{k=0}^{m-1}\zeta_m^k T_1$ consists of all the four curved triangles shown in figure 2.2.2. Let

$$\overline{T}=\{\boldsymbol{x}=(x_1,\ldots,x_{s+t})\in\cup_{k=0}^{m-1}\zeta_m^k T_1\ :\ x_i>0, 1\leq i\leq s\},$$

we now show that $\overline{T}$ has non-zero volume v, and thus T has a well-defined volume, given by $2^s v/m$. To do this, we introduce a "polar coordinate system" in $\mathbb{L}^{s,t}$.

Denote the i-th coordinate of $l(\boldsymbol{x})$ by $l_i(\boldsymbol{x})$, then (2-21) yields a system of equations

$$l_i(\boldsymbol{x})=\frac{e_i}{n}\log|N(\boldsymbol{x})|+\sum_{j=1}^{r}y_j l_i(u_j),\quad 1\leq i\leq s+t,$$

where $e_i=1$ if $1\leq i\leq s$ and $e_i=2$ if $s+1\leq i\leq t$. Write

$$\begin{cases}x_j=\rho_j, & 1\leq j\leq s,\\ x_{s+k}=\rho_{s+k}e^{i\varphi_k}, & 1\leq k\leq t\end{cases},$$

i.e, for each $1\leq k\leq t$, we set $x_{s+k}=z_k+w_k i$, where $z_k=\rho_{s+k}\cos\varphi_k$, $w_k=\rho_{s+k}\sin\varphi_k$. Then, the Jacobian of this change of variables is given by $\rho_{s+1}\cdots\rho_{s+t}$, and the set $\overline{T}$ is given by the conditions

1) $\rho_i>0, 1\leq i\leq s+t$, and $0<\prod_{i=1}^{s+t}\rho_i^{e_i}\leq 1$;
2) In the equations

$$\log\rho_i^{e_i}=\frac{e_i}{n}\log\left(\prod_{i=1}^{s+t}\rho_i^{e_i}\right)+\sum_{j=1}^{n}y_j l_i(u_j),$$

the coefficients satisfy $0\leq y_j<1$, for all $j=1,\ldots,r$.

To further simplify 1) and 2) above, we replace the ρ_i's by another set of variables $\eta,\ \eta_1,\ldots,\eta_r$ via the following formulas.

$$\log\rho_i^{e_i}=\frac{e_i}{n}\log\eta+\sum_{j=1}^{r}\eta_j l_i(u_j),\quad 1\leq i\leq s+t.$$

Note that $\sum_{i=1}^{s+t}e_i=n$ and $\sum_{i=1}^{s+t}l_i(u_j)=0$ for all j, adding these equations up yields

$$\eta=\sum_{i=1}^{s+t}\rho_i^{e_i}.$$

The conditions on $\overline{T}$ now reduce to

$$0<\eta\leq 1,\quad 0\leq\eta_i<1,\quad 1\leq i\leq r,$$

and there is no doubt that the volume v of $\overline{T}$ exists. Compute that

$$\frac{\partial\rho_i}{\partial\eta}=\frac{\rho_i}{n\eta},\quad \frac{\partial\rho_i}{\partial\eta_j}=\frac{\rho_i}{e_i}l_i(u_j),$$

one can compute the absolute value of the Jacobian of this transformation to be

$$|J| = \frac{r(K)}{2^t \rho_{s+1} \cdots \rho_{s+t}},$$

where $r(K)$ is the regulator of K. Finally, we are ready to compute v:

$$\begin{aligned} v &= \int_{\overline{T}} dx_1 \dots dx_s dz_1 dw_1 \cdots dz_t dw_t \\ &= \int_{\overline{T}} \rho_{s+1} \cdots \rho_{s+t} d\rho_1 \dots d\rho_{s+t} d\varphi_1 \cdots \varphi_t \\ &= (2\pi)^t \int \cdots \int \rho_{s+1} \cdots \rho_{s+t} d\rho_1 \dots d\rho_{s+t} \\ &= (2\pi)^t \int \cdots \int |J| \rho_{s+1} \cdots \rho_{s+t} d\eta d\eta_1 \dots d\eta_r \\ &= (2\pi)^t \int_0^1 d\eta \int_0^1 d\eta_1 \cdots \int_0^1 d\eta_r \\ &= \pi^t r(K). \end{aligned}$$

Putting everything together, we obtain that:

Theorem 2.6 *With notations as above,*

$$D(x) = \frac{\kappa}{N(\mathfrak{b})} x + O(x^{1-\frac{1}{n}}),$$

where

$$\kappa = \frac{2^{s+t} \pi^t r(K)}{m\sqrt{|d(K)|}}.$$

By (2-16), we can write

$$f_C(s) = N(\mathfrak{b})^s \sum_{k \geq 1} \frac{D_k}{k^s} \quad \mathrm{Re}(s) > 1,$$

where $D_k = \{\boldsymbol{x} \in \Lambda \cap D \,:\, N(\boldsymbol{x}) = t\}$ satisfies $A_k = \sum_{l=1}^{k} D_l = \kappa t / N(\mathfrak{b}) + O(k^{1-1/n})$.

Hence, by the same trick as that of (2-12), we see that $f_C(s)$ allows an analytic continuation to $\mathrm{Re}(s) > 1 - 1/n$, it is holomorphic except for a simple pole at $s = 1$. Moreover, the residue of $f_C(s)$ at $s = 1$ is given by $\mathrm{res}_{s=1} f_C(s) = \kappa$. Recall (2-13), we finally obtain 1) and 2).

In the next section, we shall take a further look at our favorite cases – the quadratic and cyclotomic fields, to obtain an explicit expression of the residue of $\zeta_K(s)$ at $s = 1$, which is the so-called *Dirichlet Class Number Formula*. More generally, we would expect an explicit expression of $\zeta_K(s)$ for Abelian number fields since they are always contained in cyclotomic fields by the Kronecker–Weber Theorem (Theorem 1.4).

2.3 Abelian number fields

So far, we have shown that for a number field K of signature (s, t) $(n = s + 2t)$, its Dedekind zeta function $\zeta_K(s)$ admits an analytic continuation to the right half-plane

$\mathrm{Re}(s) > (1 - 1/n)$ that is holomorphic except for a simple pole at $s = 1$, and that we have the following residue formula

$$\mathrm{Res}_{s=1}\zeta_K(s) = h\frac{2^{s+t}\pi^t r(K)}{m\sqrt{|d(K)|}}.$$

In the right hand side, the signature (s, t), the discriminant $d(K)$, and the number m of roots of unity in K are (usually) relatively easy to compute, while the same is not true for the regulator $r(K)$. Hence, we would expect a better expression for the left hand side. Gauss derived a simple formula of $\zeta_K(s)$ for quadratic fields, and later Kummer for cyclotomic fields, when he studied Fermat's Last Theorem. After 1930s, Hasse generalized these result to Abelian number fields, and studied elaborately many related problems in his book *On the Class Number of Abelian Number Fields*.

In this section, we shall proceed in a different order from these historical developments: We start with cyclotomic fields and analogize the result to derive a nice formula for quadratic fields. After that, we sketch the idea for general Abelian number fields.

2.3.1 Cyclotomic fields

Let $K = \mathbb{Q}(\zeta_m)$, $\zeta_m = e^{2\pi i/m}$ $(m \geq 3)$, be a cyclotomic field, then $[K : \mathbb{Q}] = \varphi(m)$, and $\mathrm{Gal}(K/\mathbb{Q}) \cong \mathbb{Z}_m^\times$. In particular, K is Abelian. From 2) in the end of section 1.1, one computes that

$$d(K) = (-1)^{\varphi(m)/2} m^{\varphi(m)} / \prod_{p|m} p^{\varphi(m)/p-1},$$

so primes of $\mathbb{Z}$ which are ramified in K are exactly the prime factors of m. Also, recall how each prime $p \in \mathbb{Z}$ splits in K from 2) in section 1.2, let r_p denote the number of prime ideals lying over p and f_p be the inertial degree of p, then f_p is the order of p in the multiplicative group $\mathbb{Z}_m^\times$, so

$$\zeta_K(s) = \prod_p \left(1 - \frac{1}{p^{f_p s}}\right)^{-r_p}, \quad \mathrm{Re}(s) > 1. \tag{2-22}$$

These facts hint us that $\zeta_K(s)$ might be expressed as a product of Dirichlet L-function $L(s, \chi)$'s with perhaps some extra factors, where χ runs through all *Dirichlet characters* mod m (group homomorphisms from[1] $\mathbb{Z}_m^\times$ to S^1). The key observation is as follows:

Lemma 2.7 *For each $p \nmid m$, we have*

$$\prod_{\chi \in \widehat{\mathbb{Z}_m^\times}} \left(1 - \frac{\chi(p)}{p^s}\right) = \left(1 - \frac{1}{p^{f_p s}}\right)^{r_p}, \tag{2-23}$$

where $\widehat{\mathbb{Z}_m^\times}$ is the dual group of $\mathbb{Z}_m^\times$, consisting of all Dirichlet characters mod m.

Proof: Consider the map $v_p : \chi \mapsto \chi(p)$, which induces a group homomorphism $\varphi_p : \widehat{\mathbb{Z}_m^\times} \to S^1$. The kernel of φ_p is given by $\{\chi \in \widehat{\mathbb{Z}_m^\times} : \chi(p) = 1\} = \widehat{\mathbb{Z}_m^\times/\langle\overline{p}\rangle}$, where $\bar{\cdot}$ denotes the image of $\cdot$ under the reduction mod m map, so $|\mathrm{Ker}(\varphi_p)| = \varphi(m)/f_p = r_p$, and

[1] Given a Dirichlet character χ mod m, we can extended it naturally to a function $\mathbb{Z} \to \mathbb{C}$ by setting $\chi(a) = 0$ whenever $(a, m) > 1$. We shall not bother to distinguish these two.

hence $|\mathrm{Im}(\varphi_p)| = f_p$. In particular, $\chi(p)$ runs through all the f_p-th roots of unity, and takes each value of them exactly r_p times since φ_p is a homomorphism.

Now, note that the roots of the polynomial $x^{f_p} - (1/p^{f_p s})$ are precisely the $\chi(p)/p^s$'s, where $\chi(p)$ runs through all the f_p-th roots of unity. Hence, factoring this polynomial into linear factors, setting $x = 1$, and then raising both sides to the r_p's power gives the desired result. □

Lemma 2.7 and (2-22) yields

$$\zeta_K(s) = \prod_{p|m} \left(1 - \frac{1}{p^{f_p s}}\right)^{-r_p} \prod_{\chi \in \widehat{\mathbb{Z}_m^\times}} L(s, \chi), \quad \mathrm{Re}(s) > 1, \tag{2-24}$$

where

$$L(s, \chi) = \sum_{n \geq 1} \frac{\chi(n)}{n^s} = \prod_p \left(1 - \frac{\chi(p)}{p^s}\right)^{-1}$$

is called a *Dirichlet L-function*. It has an Euler product as above since χ is completely multiplicative.

Note that for the *principal character* $\chi = \chi_0$ (the trivial group homomorphism),

$$L(s, \chi_0) = \prod_{p|m} \left(1 - \frac{1}{p^s}\right) \zeta(s),$$

we obtain that

$$\frac{\zeta_K(s)}{\zeta(s)} = \prod_{p|m} \left(1 - \frac{1}{p^s}\right) \left(1 - \frac{1}{p^{f_p s}}\right)^{-r_p} \prod_{\substack{\chi \in \widehat{\mathbb{Z}_m^\times} \\ \chi \neq \chi_0}} L(s, \chi), \quad \mathrm{Re}(s) > 1. \tag{2-25}$$

For non-principal characters, $L(s, \chi)$ converges to a holomorphic function on the right half-plane $\mathrm{Re}(s) > 0$ since $\sum_{k=1}^{n} \chi(k) = O(1)$, so taking the limit at $s = 1$ yields:

Theorem 2.8 *Keeping notations as above,*

$$h\kappa = \prod_{p|m} \left(1 - \frac{1}{p}\right) \left(1 - \frac{1}{p^{f_p}}\right)^{-r_p} \prod_{\substack{\chi \in \widehat{\mathbb{Z}_m^\times} \\ \chi \neq \chi_0}} L(1, \chi). \tag{2-26}$$

Hence, the problem now is reduced to derive an explicit formula for $L(1, \chi)$ for non-principal characters mod m.

Theorem 2.9 *Let χ be a non-principal character mod m (so $m \geq 3$), then*

$$L(1, \chi) = -\frac{1}{m} \sum_{k=1}^{m-1} \tau_k(\chi) \log\left(1 - \zeta_m^{-k}\right), \tag{2-27}$$

where $\tau_k(\chi)$ is the Gauss sum

$$\tau_k(\chi) = \sum_{a \in \mathbb{Z}_m^\times} \chi(a) \zeta_m^{ak}.$$

Proof: Let s be in the right half-plane $\mathrm{Re}(s) > 1$. Since $L(s,\chi)$ converges absolutely here, we are free to interchange the order of summation. Compute that

$$\begin{aligned} L(s,\chi) &= \sum_{a\in\mathbb{Z}_m^\times} \chi(a) \sum_{\substack{n\geq 1\\ \overline{n}=a}} \frac{1}{n^s} \\ &= \sum_{a\in\mathbb{Z}_m^\times} \chi(a) \sum_{n\geq 1} \left(\frac{1}{m} \sum_{k=1}^{m} \zeta_m^{(a-n)k} \right) \frac{1}{n^s} \\ &= \frac{1}{m} \sum_{k=1}^{m} \tau_k(\chi) \sum_{n\geq 1} \frac{\zeta_m^{-nk}}{n^s}, \end{aligned}$$

and note that $\tau_m(\chi) = \sum_{a\in\mathbb{Z}_m^\times} \chi(a) = 0$ since χ is non-principal, it suffices to deal with the Dirichlet series

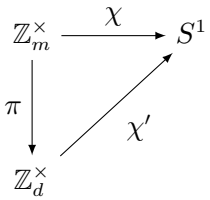
$$f_k(s) := \sum_{n\geq 1} \frac{\zeta_m^{-nk}}{n^s},$$

where $1 \leq k \leq m-1$. Since $\sum_{i=1}^{n} \zeta_m^{-nk} = O(1)$, each $f_k(s)$ converges to a holomorphic function on the right half-plane $\mathrm{Re}(s) > 0$. In particular, at $s = 1$ we see

$$\sum_{n\geq 1} \frac{\zeta^{-nk}}{n} = -\log\left(1-\zeta_m^k\right),$$

from which the theorem follows by taking the limit as $s \to 1^+$ □

We can simplify the expression of $L(1,\chi)$ in (2-27) further. Indeed, if χ is *induced* by some character χ' mod d for some $d \mid m$ $(d < m)$, i.e., the following diagram



commutes, where π is the reduction mod d map, then

$$L(1,\chi) = \prod_{\substack{p\mid m\\ p\nmid d}} \left(1 - \frac{\chi'(p)}{p}\right) L(1,\chi').$$

Otherwise, we say that χ is a *primitive* character. Note that every Dirichlet character is induced by a unique primitive character, it suffices to calculate $L(1,\chi)$ for primitive characters, or equivalently, to understand $\tau_k(\chi)$.

Lemma 2.10 *Let χ be a primitive character mod m, then the Gauss sum*

$$\tau_k(\chi) = \begin{cases} \overline{\chi}(k)\tau(\chi), & (k,m) = 1; \\ 0, & (k,m) > 1. \end{cases}$$

Where, $\tau(\chi) = \tau_1(\chi)$ and $\bar{\cdot}$ is the complex conjugation of $\cdot$.

Proof: If $(k,m)=1$, then

$$\tau_1(\chi)=\sum_{a\in\mathbb{Z}_m^\times}\chi(a)\zeta_m^a=\sum_{a\in\mathbb{Z}_m^\times}\chi(ak)\zeta_m^{ak}=\chi(k)\sum_{a\in\mathbb{Z}_m^\times}\chi(a)\zeta_m^{ak},$$

so $\tau_k(\chi)=\overline{\chi(k)}\tau_1(\chi)$.

If $(k,m)>1$, then $d:=m/(k,m)<m$. We first claim that there exists some $b\in\mathbb{Z}$ such that $(b,m)=1$, $b\equiv 1 \pmod d$ and $\chi(b)\neq 1$, and then play the same trick as in the previous case:

$$\tau_k(\chi)=\sum_{a\in\mathbb{Z}_m^\times}\chi(a)\zeta_m^{ak}=\sum_{a\in\mathbb{Z}_m^\times}\chi(ab)\zeta_m^{abk}=\chi(b)\sum_{a\in\mathbb{Z}_m^\times}\chi(a)\zeta_m^{ak}=\chi(b)\tau_k(\chi),$$

so $\tau_k(\chi)=0$. Where, the third equality follows from the fact that $b\equiv 1 \pmod d$.

To prove the claim, note that χ is not induced by any character mod d, so there exist integers p,q such that $(pq,m)=1$, $p\equiv q \pmod d$ but $\chi(p)\neq\chi(q)$. Now, pick some $b\in\mathbb{Z}$ such that $(b,m)=1$ and $bp\equiv q \pmod m$, then

$$\chi(q)=\chi(bp)=\chi(b)\chi(p),$$

so $\chi(b)\neq 1$, as desired. □

Lemma 2.11 *With notations as above,*

$$|\tau(\chi)|=\sqrt{m}.$$

Proof: Compute that

$$\begin{aligned}\tau(\chi)\overline{\tau}(\chi)&=\sum_{a\in\mathbb{Z}_m^\times}\chi(a)\zeta_m^a\sum_{b\in\mathbb{Z}_m^\times}\overline{\chi}(b)\zeta_m^{-b}\\&=\sum_{a\in\mathbb{Z}_m^\times}\sum_{b\in\mathbb{Z}_m^\times}\chi(ab^{-1})\zeta_m^{a-b}\\&=\sum_{c\in\mathbb{Z}_m^\times}\chi(c)\sum_{b\in\mathbb{Z}_m^\times}\zeta_m^{(c-1)b}.\quad(\star)\end{aligned}$$

By Lemma 2.10 we see that for any $(b,m)>1$,

$$\sum_{c\in\mathbb{Z}_m^\times}\chi(c)\zeta_m^{(c-1)b}=\zeta_m^{-b}\tau_b(\chi)=0.$$

Hence,

$$(\star)=\sum_{c\in\mathbb{Z}_m^\times}\chi(c)\sum_{b\in\mathbb{Z}_m}\zeta_m^{(c-1)b}=\sum_{b\in\mathbb{Z}_m}1=m$$

because the inner sum vanishes whenever $c\neq 1$. We thus obtain that $|\tau(\chi)|=\sqrt{m}$. □

Now, we are ready to simplify (2-27) for primitive characters mod m, $m\geq 3$: By Lemma 2.10, compute that

$$L(1,\chi)=-\frac{\tau(\chi)}{m}\sum_{k\in\mathbb{Z}_m^\times}\overline{\chi}(k)\log\left(1-\zeta_m^{-k}\right)$$

$$= -\frac{\chi(-1)\tau(\chi)}{m} \sum_{k\in\mathbb{Z}_m^\times} \overline{\chi}(k) \log\left(1-\zeta_m^k\right)$$
$$= -\frac{\chi(-1)\tau(\chi)}{m} \sum_{k\in\mathbb{Z}_m^\times} \overline{\chi}(k) \left[\log 2 + \log\sin\frac{k\pi}{m} + \left(\frac{k}{m}-\frac{1}{2}\right)\pi i\right]$$
$$= -\frac{\chi(-1)\tau(\chi)}{m} \sum_{k\in\mathbb{Z}_m^\times} \overline{\chi}(k) \left(\log\sin\frac{k\pi}{m} + \frac{k\pi i}{m}\right) \quad (\star\star).$$

Replacing k by $(m-k)$, we see that when χ is *even* (i.e., $\chi(-1)=1$),

$$\sum_{k\in\mathbb{Z}_m^\times} \overline{\chi}(k)k = 0;$$

and when χ is *odd* (i.e., $\chi(-1)=-1$),

$$\sum_{k\in\mathbb{Z}_m^\times} \overline{\chi}(k) \log\sin\frac{k\pi}{m} = 0.$$

so by Lemma 2.11 and after lengthy computations to simplify the sum $\sum_{k\in\mathbb{Z}_m^\times}\overline{\chi}(k)k$, we finally obtain:

Theorem 2.12 *For non-principal, primitive characters χ mod m,*

$$|L(1,\chi)| = \begin{cases} \dfrac{2}{\sqrt{m}} \left| \displaystyle\sum_{\substack{k\in\mathbb{Z}_m^\times \\ k<m/2}} \overline{\chi}(k)\log\sin\frac{k\pi}{m}\right|, & \text{if } \chi \text{ is even;} \\ \dfrac{\pi}{|2-\chi(2)|\sqrt{m}} \left| \displaystyle\sum_{\substack{k\in\mathbb{Z}_m^\times \\ k<m/2}} \overline{\chi}(k)\right|, & \text{if } \chi \text{ is odd.} \end{cases}$$

Remark 2.13 *We now have an explicit expression of the value of $L(1,\chi)$ for all primitive, non-principal characters χ. Theorem 2.8 implies that all of these $L(1,\chi)$'s are non-zero, which is the key ingredient of the proof of Dirichlet's theorem on arithmetic progressions:*

Theorem 2.14 (Dirichlet) *For any two positive coprime integers a and m, the arithmetic progression*

$$a, \quad a+m, \quad a+2m, \cdots$$

contains infinitely many primes.

In fact, the real challenge there is to show that $L(1,\chi)\neq 0$ for all primitive, quadratic characters χ, and this can be done using only the Quadratic Class Number Formula, *which is the topic of our next subsection.*

2.3.2 Quadratic fields

Let $K=\mathbb{Q}(\sqrt{d})$, d square-free, be a quadratic field, then clearly K is Abelian. Set $m=|d(K)|$, then $m=|d|$ if $d\equiv 1 \pmod 4$ and $m=|4d|$ if $d\equiv 2,3 \pmod 4$. We

have seen that a prime $p \in \mathbb{Z}$ is ramified iff $p \mid m$, and that otherwise, if p is odd, then p totally splits iff $\left(\frac{d}{p}\right) = 1$, where $\left(\frac{\cdot}{\cdot}\right)$ is the Legendre symbol, and if $p = 2$, then p totally splits iff $d \equiv 1 \pmod 8$.

Similar to cyclotomic fields (2-24), we would also expect to express $\zeta_K(s)$ in terms of Dirichlet L-functions. And note that $K \subset \mathbb{Q}(\zeta_m)$ by 2) in section 1.1, there should be a close relation between these two zeta functions. So, we start by mimicking (2-23), but this time there can only be two different characters appearing (since $r_p f_p = 2$ in (2-22)), one is the principal character χ_0. We now figure out what is the other desired character χ, and in fact (2-23) leaves us with precisely one choice:

Extending the Legendre symbol multiplicatively[1], we define

$$\chi(n) := \left(\frac{d}{n}\right)$$

for odd positive integers n, and (if $2 \nmid m$)

$$\chi(2) := \left(\frac{2}{d}\right).$$

χ can indeed be seen as a character mod m by the Quadratic Reciprocity Law, if we set $\chi(n) = 0$ whenever $(m, n) > 1$ and extend its definition multiplicatively. We shall call χ the *character of the quadratic field* K[2]. Thus, parallel to Lemma 2.7, we have

Lemma 2.7′ *For each $p \nmid m$,*

$$\left(1 - \frac{\chi_0(p)}{p^s}\right)\left(1 - \frac{\chi(p)}{p^s}\right) = \left(1 - \frac{1}{p^{f_p s}}\right)^{r_p}, \tag{2-28}$$

where χ_0 is the principal character mod m, χ is the character of K, r_p is the number of prime ideals lying over p, and f_p is the inertial degree of p.

Therefore, (2-25) now reduces to

$$\zeta_K(s) = \zeta(s)L(s, \chi), \tag{2-29}$$

since p is ramified when $p = m$, so $r_p = f_p = 1$.

Remark 2.15 *Just like the Euler product of $\zeta_K(s)$ being an analytic formulation of the uniqueness of prime decomposition of ideals in $\mathcal{O}_K$, (2-29) turns out to be equivalent to the Quadratic Reciprocity Law of Gauss.*

Proof: We have shown that the Quadratic Reciprocity Law implies (2-29). Conversely, suppose (2-29) holds for all quadratic fields K, where χ is some Dirichlet character mod m. Let p, q be odd primes, and set $p' = (-1)^{(p-1)/2}p$. We now consider the quadratic field $K = \mathbb{Q}(p')$:

Note that $p' \equiv 1 \pmod 4$, $m = |d(K)| = p$. On the one hand, following the spirit of (2-22), (2-29) yields

$$\chi(q) = \left(\frac{p'}{q}\right) = \left(\frac{(-1)^{(p-1)/2}p}{q}\right);$$

[1] This is called the *Jacobi symbol*, written also $\left(\frac{\cdot}{\cdot}\right)$. $\left(\frac{a}{b}\right)$ is defined for all $a \in \mathbb{Z}$ and for all $b > 0$ odd.
[2] This χ also has a special name – the *Kronecker symbol*.

On the other hand, there is exactly one non-trivial *quadratic character* χ mod m (i.e., $\chi^2 = \mathrm{id}$, or equivalently, χ is a group homomorphism $\mathbb{Z}_m^\times \twoheadrightarrow \{\pm 1\}$), given by

$$\chi(n) := \left(\frac{n}{m}\right),$$

since $m = p$ is a prime and thus $\mathbb{Z}_m^\times$ is cyclic. Hence,

$$\left(\frac{q}{p}\right) = \left(\frac{(-1)^{(p-1)/2}p}{q}\right),$$

which is equivalent to the Quadratic Reciprocity Law. □

Lemma 2.16 *The character χ defined above is primitive.*

Proof: It suffices to show that for each prime $p \mid m$, there exists some $n \in \mathbb{Z}_m^\times$ such that $n \equiv 1 \pmod{m/p}$ and $\chi(n) = -1$. We now verify this case by case. For convenience, write $|d| = 2^r k$, k odd, square-free and $r = 0$ or 1.

1) Let $p \mid m$ be an odd prime, then $(p, k/p) = 1$. Let a be a quadratic non-residue mod p, then by the Chinese Remainder Theorem we can find some positive integer n such that

$$\begin{cases} n \equiv 1 \pmod 8 \\ n \equiv 1 \pmod{k/p} \\ n \equiv a \pmod p \end{cases},$$

so noting that $\left(\frac{-1}{b}\right) = 1$ iff $b \equiv 1 \pmod 4$, the Quadratic Reciprocity Law yields

$$\chi(n) = \left(\frac{d}{n}\right) = \left(\frac{m}{n}\right) = \left(\frac{n}{m}\right) = \left(\frac{n}{p}\right)\left(\frac{n}{m/p}\right) = \left(\frac{a}{p}\right)\left(\frac{1}{m/p}\right) = -1,$$

as desired.

2) For $p = 2$, then necessarily $d \equiv 2 \text{ or } 3 \pmod 4$, and $m = 4|d|$.

a) If $d \equiv 2 \pmod 4$, then $r = 1$ and for any positive integer n satisfying

$$\begin{cases} n \equiv 1 \pmod k \\ n \equiv 5 \pmod 8 \end{cases},$$

we have

$$\chi(n) = \left(\frac{d}{n}\right) = \left(\frac{|d|}{n}\right) = \left(\frac{2k}{n}\right) = \left(\frac{2}{n}\right)\left(\frac{k}{n}\right) = (-1)\cdot 1 = -1$$

since $\left(\frac{2}{b}\right) = 1$ iff $b \equiv \pm 1 \pmod 8$.

b) If $d \equiv 3 \pmod 4$, then $r = 0$ and similarly, for any positive integer n satisfying

$$\begin{cases} n \equiv 1 \pmod k \\ n \equiv 3 \pmod 4 \end{cases},$$

$\chi(n) = -1$ since when $d > 0$, then

$$\chi(n) = \left(\frac{d}{n}\right) = \left(\frac{k}{n}\right) = (-1)\left(\frac{n}{k}\right) = -1;$$

and when $d < 0$, then

$$\chi(n) = \left(\frac{d}{n}\right) = \left(\frac{-1}{n}\right)\left(\frac{k}{n}\right) = (-1)\cdot 1 \cdot \left(\frac{n}{k}\right) = -1.$$

In each case, we have constructed our desired n, so χ must be primitive. □

Thanks to Lemma 2.16, we can now mimic Theorem 2.8 and 2.12 to establish the Quadratic Class Number Formula. Thanks to our hard work for cyclotomic fields, this is not terribly hard any more.

Theorem 2.17 *Keeping the notations as above, The number of ideal classes in $\mathcal{O}_K$ is given by*[1]

$$h = \begin{cases} \dfrac{1}{\log(u)}\left|\displaystyle\sum_{\substack{k\in\mathbb{Z}_m^\times \\ k<m/2}} \overline{\chi}(k)\log\sin\frac{k\pi}{m}\right|, & \text{if } d>0; \\ \dfrac{1}{2-\chi(2)}\left|\displaystyle\sum_{\substack{k\in\mathbb{Z}_m^\times \\ k<m/2}} \overline{\chi}(k)\right|, & \text{if } d<0, d\neq -1,-3. \end{cases}$$

Where, u is the unique fundamental unit of $\mathcal{O}_K$ which is strictly larger than 1.

Proof: Note that

$$\kappa = \begin{cases} 2\log(u)/\sqrt{m}, & \text{if } d>0; \\ \pi/\sqrt{m}, & \text{if } d<0, d\neq -1,-3 \end{cases},$$

it suffices to show that χ is even when $d > 0$ and odd when $d < 0$, which can be checked directly case by case. □

Remark 2.18 *From the discussions above, we have attached a special quadratic character χ to each quadratic field, which is primitive. Conversely, it turns out that* every *primitive, quadratic character χ is uniquely given in this way. In particular, Theorem 2.17 actually tells us that $L(1,\chi) \neq 0$ for every such χ, and from which Theorem 2.14 can be proved without much difficulty. This is Dirichlet's original proof!*

As an application, let us compute the class numbers of some quadratic fields:

1) When $d = -2$,

$$h = \frac{1}{2}|\chi(1)+\chi(3)| = 1;$$

2) When $d = -5$,

$$h = \frac{1}{2}|\chi(1)+\chi(3)+\chi(7)+\chi(9)| = 2;$$

3) When $d = 2$,

$$h = \frac{1}{\log(1+\sqrt{2})}\left|\chi(1)\log\sin\frac{\pi}{8} + \chi(3)\log\sin\frac{3\pi}{8}\right|$$

[1] When $d = -1$ (resp. -3), there is an extra factor of 2 (resp. 3) in the denominator of the expression above, since in this case $W_K = \{\pm 1, \pm i\}$ (resp. $\{\pm 1, \pm\zeta_3, \pm\zeta_3^2\}$), while $W_K = \{\pm 1\}$ whenever $d < -4$.

$$= \frac{\log\left(\sin\frac{3\pi}{8}/\sin\frac{\pi}{8}\right)}{\log(1+\sqrt{2})}$$
$$< \frac{\log 3}{\log(1+\sqrt{2})} < 2,$$

so h must be 1.

2.3.3 The general case

Let K now be an arbitrary Abelian number field, then by the Kronecker–Weber Theorem (Theorem 1.4) we see that K is always contained in a cyclotomic field $\mathbb{Q}(\zeta_m)$. Moreover, we may assume that primes of $\mathbb{Z}$ which are ramified in K are precisely the prime divisors of m[1]. Note that

$$G := \mathrm{Gal}(K/\mathbb{Q}) \leq \mathrm{Gal}(\mathbb{Q}(\zeta_m)/\mathbb{Q}) \cong \mathbb{Z}_m^\times,$$

the discussions above for cyclotomic and quadratic fields suggest us to view the dual group $\widehat{G}$ (the group of all group homomorphisms from G to S^1) as a subgroup of $\widehat{\mathbb{Z}_m^\times}$, and write

$$\prod_{\chi\in\widehat{G}}\left(1-\frac{\chi(p)}{p^s}\right) = \left(1-\frac{1}{p^{f_p s}}\right)^{r_p}. \tag{2-30}$$

The proof is similar to that of Lemma 2.7. In particular, if K is a quadratic field then there are exactly two elements in $\widehat{G}$. The identity element corresponds to the principal character χ_0, and the other one is the character χ of K we constructed just now.

Once we have obtained (2-30), everything else is the same as what we did for cyclotomic fields, except that we are only concerned with characters in the subgroup $\widehat{G}$ instead of the whole group $\widehat{\mathbb{Z}_m^\times}$.

[1]This follows from the maximal and minimal conditions for decomposition and inertia fields.

Chapter III

Some Hints at Class Field Theory

Different themes in number theory are leading us to class field theory, such as distribution and density theorems for primes, reciprocity laws, and relations between abelian extensions and ideal class groups. We have encountered with a bit of the first two in the previous chapter, and we shall explore more of them under the help of the third theme.

So, let us now take a first glimpse of this beautiful theory and see how analytic methods contribute to it. Our discussions here owe much to section 5.C., 8.A. and 8.B. of chapter 2 of [C11], and chapter 8 of [M18].

3.1 Theorems of class field theory

Class field theory describes the abelian extensions of a number field in terms of the arithmetic of the field itself. But before stating the general theorems of class field theory, let us first study the special case of the Hilbert class field.

3.1.1 The Hilbert class field

The Hilbert class field of K is defined in terms of the unramified Abelian extensions of K. We have seen the notion of *Abelian* extensions (L/K is Abelian if it is Galois and $\mathrm{Gal}(L/K)$ is Abelian). To define unramified extensions, we first need to discuss the ramification of infinite primes.

Given a number field K, we shall (sometimes) call prime ideals of $\mathcal{O}_K$ *finite primes* to distinguish them from the *infinite primes*, which are determined by the embeddings of K into $\mathbb{C}$. A *real infinite prime* is identified with a real embedding $\sigma : K \hookrightarrow \mathbb{R}$, while a *complex infinite prime* is identified with a pair of complex conjugate embeddings $\sigma, \overline{\sigma} : K \hookrightarrow \mathbb{C}$. For instance, the infinite prime of $\mathbb{Q}$ ($\sigma = \mathrm{id}$) is unramified in $\mathbb{Q}(\sqrt{2})$ but ramified in $\mathbb{Q}(i)$.

Suppose L/K is an extension of number fields, we shall say an infinite prime σ of K is *ramified* in L if σ is real but it has a complex extension to L, and that L/K is *unramified* if it is unramified at all primes, finite or infinite.

While some number fields may allow unramified extensions of them of arbitrarily high degree, the situation for unramified Abelian extensions is much nicer:

Theorem 3.1 *Given a number field K, there is a finite Galois extension L of K such that*

1) L/K is an unramified Abelian extension;

2) Any unramified Abelian extension of K is contained in L.

This number field L is called **the Hilbert class field of K**, denoted by H_K. We shall prove its existence by class field theory later in section 3.1.2. Clearly, it is unique

and the *maximal* unramified Abelian extension of K.

To see the power of the Hilbert class field H_K of K, recall the Artin symbol that we introduced in section 1.2.3: Let L/K be a Galois extension of number fields, suppose a prime $\mathfrak{p}$ in $\mathcal{O}_K$ is unramified in $\mathcal{O}_L$, and let $\mathfrak{q}$ be a prime in $\mathcal{O}_L$ lying over $\mathfrak{p}$, then we set $\left(\frac{L/K}{\mathfrak{q}}\right)$ to be the Frobenius automorphism of $\mathfrak{q}$ over $\mathfrak{p}$. When L/K is Abelian, the Artin symbol $\left(\frac{L/K}{\mathfrak{q}}\right)$ depends only on the underlying prime $\mathfrak{p}$, so we can write $\left(\frac{L/K}{\mathfrak{p}}\right)$ instead. Furthermore, if L/K is also unramified, then $\left(\frac{L/K}{\mathfrak{q}}\right)$ is defined for *all* primes $\mathfrak{p}$ of $\mathcal{O}_K$. To exploit this, let us extend the Artin symbol multiplicatively: note that any fractional ideal $\mathfrak{a} \in \mathcal{I}_K$ has a unique prime decomposition

$$\mathfrak{a} = \prod_{i=1}^{s} \mathfrak{p}_i^{n_i}, \quad n_i \in \mathbb{Z},$$

we set

$$\left(\frac{L/K}{\mathfrak{a}}\right) := \prod_{i=1}^{s} \left(\frac{L/K}{\mathfrak{p}_i}\right)^{n_i}.$$

Then, the Artin symbol induces a homomorphism

$$\left(\frac{L/K}{\cdot}\right) : \mathcal{I}_K \to \mathrm{Gal}(L/K) \tag{3-1}$$

called the **Artin map**, which relates the Hilbert class field and the ideal class group $\mathcal{C}_K$ by the *Artin Reciprocity Theorem for the Hilbert Class Field*:

Theorem 3.2 *Let H_K be the Hilbert class field of a number field K, then the Artin map $\left(\frac{H_K/K}{\cdot}\right)$ is surjective, and its kernel is precisely the subgroup $\mathcal{P}_K$ of principal fractional ideals. Hence, the Artin map induces an isomorphism*

$$\mathcal{C}_K \xrightarrow{\sim} \mathrm{Gal}(H_K/K). \tag{3-2}$$

This theorem will follow from general results in section 3.1.2.

Applying Galois theory to Theorem 3.1 and 3.2, we obtain the *Class Field Theory for Unramified Abelian Extensions*[1], which illustrates that unramified Abelian extensions of a number field K can be classified via intrinsic data of K.

Corollary 3.3 *Given a number field K, there is a one-to-one correspondence between unramified Abelian extensions L/K and subgroups H of the ideal class group $\mathcal{C}_K$. Moreover, the Artin induces an isomorphism*

$$\mathcal{C}_K/H \xrightarrow{\sim} \mathrm{Gal}(L/K). \tag{3-3}$$

Theorem 3.2 allows us to characterize the primes of K which split completely in the Hilbert class field:

Corollary 3.4 *Let H_K be the Hilbert class field of a number field K, then a prime ideal $\mathfrak{p}$ of $\mathcal{O}_K$ splits completely in L iff $\mathfrak{p}$ is a principal ideal.*

[1] If L/K is ramified, then the Artin map is not defined on all of $\mathcal{I}_K$, and this is one reason why general theorems of class field theory are complicated to state.

Proof: The prime $\mathfrak{p}$ splits completely in L iff its Artin symbol $\left(\frac{H_K/K}{\mathfrak{p}}\right) = 1$, which is equivalent to $\mathfrak{p}$ being principal by Theorem 3.2. □

Let us now work out a concrete example to get a taste of how the Artin symbol is related to reciprocity laws. Consider $K = \mathbb{Q}(\sqrt{-3}) = \mathbb{Q}(\zeta_3)$, where $\zeta_n = e^{2\pi i/n}$ as usual, and $L = K(\sqrt[3]{2})$. L/K is Abelian since $\mathrm{Gal}(L/K) \cong \mathbb{Z}_3$. Notice that $\mathcal{O}_K = \mathbb{Z}[\zeta_3]$ is a PID, every prime ideal $\mathfrak{p}$ is of the form (π) for some prime π in $\mathcal{O}_K$. If $\pi \nmid 6$, then π is unramified in L. In this case, $\left(\frac{L/K}{\pi}\right)$ is defined. To see explicitly which automorphism it is, let $\mathfrak{q}$ be a prime of $\mathcal{O}_L$ lying over (π), compute that

$$\begin{aligned}\left(\frac{L/K}{\pi}\right)(\sqrt[3]{2}) &\equiv \sqrt[3]{2}^{N(\pi)} \pmod{\mathfrak{q}} \\ &\equiv 2^{(N(\pi)-1)/3}\sqrt[3]{2} \pmod{\mathfrak{q}} \\ &\equiv \left(\frac{2}{\pi}\right)_3 \sqrt[3]{2} \pmod{\mathfrak{q}}. \end{aligned} \tag{3-4}$$

Where, we omit K from our notations of the norm $N = N_{K/\mathbb{Q}}$ again, and $\left(\frac{2}{\pi}\right)_3$ is the *3-rd power Legendre symbol*, defined as the unique cube root of unity such that

$$2^{(N(\pi)-1)/3} \equiv \left(\frac{2}{\pi}\right)_3 \pmod{\pi}. \tag{3-5}$$

It is worth mentioning that

$$\begin{aligned}\left(\frac{\alpha}{\pi}\right)_3 &\Leftrightarrow \alpha^{N(\pi)-1)/3} \equiv 1 \pmod{\pi} \\ &\Leftrightarrow x^3 \equiv \alpha \pmod{\pi} \text{ has a solution in } \mathcal{O}_K\end{aligned}$$

since the unit group of any finite field is cyclic. This establishes the link between the Legendre symbol and cubic residues. Moreover, we have:

Theorem 3.5 (Cubic Reciprocity Law) *If π and θ are primary[1] primes in $\mathbb{Z}[\zeta_3]$ of unequal norm, then*

$$\left(\frac{\theta}{\pi}\right)_3 = \left(\frac{\pi}{\theta}\right)_3. \tag{3-6}$$

We will generalize the Legendre symbol to exploit more about reciprocity laws after we state main theorems of class field theory, in section 3.1.3.

3.1.2 Class field theory: a classical formulation

We now present a classical formulation of class field theory. To begin with, we introduce the notion of a modulus. Given a number field K, a *modulus* in K is a formal product

$$\mathfrak{m} = \prod_{\mathfrak{p}} \mathfrak{p}^{n_{\mathfrak{p}}} \tag{3-7}$$

over all primes $\mathfrak{p}$ of K, finite or infinite, and such that

[1] A prime α is called *primary* if $\alpha \equiv \pm 1 \pmod 3$. This restriction is a normalization analogous to that of $p > 0$ for ordinary primes.

1) $n_{\mathfrak{p}} \geq 0$, and only finitely many of them are non-zero;
2) $n_{\mathfrak{p}} = 0$ whenever $\mathfrak{p}$ is a complex infinite prime;
3) $n_{\mathfrak{p}} \leq 1$ whenever $\mathfrak{p}$ is a real infinite prime.

We shall write $\mathfrak{m} = \mathfrak{m}_0\mathfrak{m}_\infty$, where $\mathfrak{m}_0$ is an ideal of $\mathcal{O}_K$ and $\mathfrak{m}_\infty$ is a product of distinct real infinite primes of K. When all the $n_{\mathfrak{p}}$'s are zero, we simply set $\mathfrak{m} = 1$.

Given a modulus $\mathfrak{m} = \mathfrak{m}_0\mathfrak{m}_\infty$, the set $\mathcal{I}_K(\mathfrak{m})$ of all fractional ideals of $\mathcal{O}_K$ relatively prime to $\mathfrak{m}_0$ forms a group. Let $\mathcal{P}_{K,1}(\mathfrak{m})$ be its subgroup generated by principal ideals (α), where $\alpha \in \mathcal{O}_K$ satisfies

$$\alpha \equiv 1 \pmod{\mathfrak{m}_0}$$

and $\sigma(\alpha) > 0$ for every real infinite prime σ dividing $\mathfrak{m}_\infty$. One can show that $\mathcal{P}_{K,1}(\mathfrak{m})$ has *finite* index in $\mathcal{I}_K(\mathfrak{m})$. A subgroup $H \leq \mathcal{I}_K(\mathfrak{m})$ is called a *congruence subgroup* if it contains $\mathcal{P}_{K,1}(\mathfrak{m})$, and in this case, the quotient

$$\mathcal{I}_K(\mathfrak{m})/H$$

is called a *generalized ideal class group* for $\mathfrak{m}$. For instance, when $\mathfrak{m} = 1$, we see that $\mathcal{P}_{K,1}(1) = \mathcal{P}_K$ is a congruence subgroup and thus $\mathcal{C}_K = \mathcal{I}_K/\mathcal{P}_K$ is a generalized ideal class group.

Similar to the case of Hilbert class field (Theorem 3.2), the idea of class field theory is that generalized ideal class groups are the Galois groups of all Abelian extensions of K, and the Artin map builds up a bridge between these two. To make this precise, we now define the Artin map of an Abelian extension of K.

Suppose L/K is an Abelian extension of number field, and let $\mathfrak{m}$ be a modulus divisible by all primes ramified in L. Note that for any given a prime $\mathfrak{p}$ not dividing $\mathfrak{m}$, the Artin symbol $\left(\frac{L/K}{\mathfrak{p}}\right) \in \mathrm{Gal}(L/K)$ is defined. Extending it by multiplicativity gives us a group homomorphism

$$\Phi_{L/K,\mathfrak{m}} : \mathcal{I}_K(\mathfrak{m}) \to \mathrm{Gal}(L/K). \tag{3-8}$$

We shall call $\Phi_{L/K,\mathfrak{m}}$ the *Artin map for* L/K *and* $\mathfrak{m}$, and denote it simply by $\Phi_{\mathfrak{m}}$ when L/K is clear.

Theorem 3.6 (Artin Reciprocity Theorem) *Let L/K be an Abelian extension of number fields, and let $\mathfrak{m}$ be a modulus divisible by all primes of K ramified in L, finite or infinite. Then:*

1) The Artin map $\Phi_{\mathfrak{m}}$ is surjective;

2) If the exponents of the finite primes in $\mathfrak{m}$ are sufficiently large, then $\mathrm{Ker}(\Phi_{\mathfrak{m}})$ is a congruence subgroup, and the isomorphism

$$\mathcal{I}_K(\mathfrak{m})/\mathrm{Ker}(\Phi_{\mathfrak{m}}) \cong \mathrm{Gal}(L/K)$$

shows that $\mathrm{Gal}(L/K)$ is a generalized ideal class group for the modulus $\mathfrak{m}$.

As an example, consider $K = \mathbb{Q}$ and $L = \mathbb{Q}(\zeta_m)$, and let $\mathfrak{m}$ be the modulus $m\infty$, where ∞ stands for the real infinite prime of $\mathbb{Q}$. A direct computation shows that the

Artin map

$$\Phi_{\mathfrak{m}} : \mathcal{I}_K(\mathfrak{m}) \twoheadrightarrow \mathrm{Gal}(\mathbb{Q}(\zeta_m)/\mathbb{Q}) \cong \mathbb{Z}_m^\times$$

can be described as follows: for any $(a/b) \in \mathcal{I}_{\mathbb{Q}}(\mathfrak{m})$, where $(a/b) > 0$ and $(ab, m) = 1$,

$$\Phi_{\mathfrak{m}}\left(\frac{a}{b}\right) = \bar{a}\bar{b}^{-1} \in \mathbb{Z}_m^\times, \tag{3-9}$$

where $\bar{\cdot}$ denotes the image of $\cdot$ under the reduction mod m map. In particular, we get

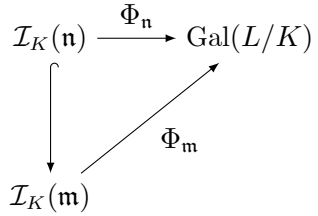
$$\mathrm{Ker}(\Phi_{\mathfrak{m}}) = \mathcal{P}_{\mathbb{Q},1}(\mathfrak{m}), \tag{3-10}$$

which is an important observation for our treatment of the Kronecker–Weber Theorem and the Quadratic Reciprocity Law later.

Remark 3.7 *The modulus* $\mathfrak{m}$ *for which* $\mathrm{Ker}(\Phi_{\mathfrak{m}})$ *is a congruence subgroup for* $\mathfrak{m}$ *is* not *unique. Indeed, if* $\mathcal{P}_{K,1}(\mathfrak{m}) \subseteq \mathrm{Ker}(\Phi_{\mathfrak{m}})$*, then for any* $\mathfrak{m} \mid \mathfrak{n}$*, it is not hard to see*

$$\mathcal{P}_{K,1}(\mathfrak{n}) \subseteq \mathrm{Ker}(\Phi_{\mathfrak{n}})$$

from the following commutative diagram:



Hence, $\mathrm{Gal}(L/K)$ *is a generalized ideal class group for infinitely many moduli.*

However, there is a canonical modulus that we would prefer:

Theorem 3.8 (Conductor Theorem) *With notations as above, there is a modulus* $\mathfrak{f} = \mathfrak{f}(L/K)$ *such that*

1) a prime (finite or infinite) of K *is ramified in* L *iff it divides* $\mathfrak{f}$*, and*

2) for any such a modulus $\mathfrak{m}$*,* $\mathrm{Ker}(\Phi_{\mathfrak{m}})$ *is a congruence subgroup for* $\mathfrak{m}$ *iff* $\mathfrak{f} \mid \mathfrak{m}$*.*

This modulus $\mathfrak{f}$, determined uniquely by L/K, is called the *conductor* of the extension L/K. For instance, the conductor for $\mathbb{Q}(\zeta_m)/\mathbb{Q}$, $m \geq 3$ is given by

$$\mathfrak{f} = \begin{cases} (m/2)\infty, & \text{if } 2 \parallel m, \\ m\infty, & \text{otherwise.} \end{cases}$$

Finally, we state the Existence Theorem, which asserts that every generalized ideal class group is the Galois group of some Abelian extension L/K.

Theorem 3.9 (Existence Theorem) *Given a number field* K*, let* $\mathfrak{m}$ *be a modulus of* K*, and let* H *be a congruence subgroup for* $\mathfrak{m}$*. Then, there exists a unique Abelian extension* L *of* K*, all of whose ramified primes divide* $\mathfrak{m}$*, finite or infinite, such that the Artin map*

$$\Phi_{\mathfrak{m}} : \mathcal{I}_K(\mathfrak{m}) \to \mathrm{Gal}(L/K)$$

has kernel precisely H.

As promised, we now indicate two applications of class field theory, the Kronecker–Weber Theorem and the existence of the Hilbert class field. A key ingredient in both proofs is the following:

Corollary 3.10 *Suppose L and M are Abelian extensions of K. Then $L \subseteq M$ iff there is a modulus $\mathfrak{m}$, divisibly by all primes of K ramified in either L or M, such that*

$$\mathcal{P}_{K,1}(\mathfrak{m}) \subseteq \mathrm{Ker}(\Phi_{M/K,\mathfrak{m}}) \subseteq \mathrm{Ker}(\Phi_{L/K,\mathfrak{m}}).$$

Proof: Assume first that $L \subseteq M$, and let $\pi : \mathrm{Gal}(M/K) \to \mathrm{Gal}(L/K)$ be the restriction map. Then, Theorem 3.6 and Remark 3.7 imply that there exists a modulus $\mathfrak{m}$ such that both $\mathrm{Ker}(\Phi_{L/K,\mathfrak{m}})$ and $\mathrm{Ker}(\Phi_{M/K,\mathfrak{m}})$ are congruence subgroups for $\mathfrak{m}$. Note that $\Phi_{L/K,\mathfrak{m}} = \pi \circ \Phi_{M/K,\mathfrak{m}}$, it is then clear that $\mathrm{Ker}(\Phi_{M/K,\mathfrak{m}}) \subseteq \mathrm{Ker}(\Phi_{L/K,\mathfrak{m}})$.

Conversely, assume $\mathfrak{m}$ is a modulus with above properties. Then, the Artin map $\Phi_{M/K,\mathfrak{m}} : \mathcal{I}_K(\mathfrak{m}) \to \mathrm{Gal}(M/K)$ sends the subgroup $\mathrm{Ker}(\Phi_{L/K,\mathfrak{m}}) \leq \mathcal{I}_K(\mathfrak{m})$ to a subgroup $H \leq \mathrm{Gal}(M/K)$. H corresponds to an intermediate field $K \subseteq \widetilde{L} \subseteq M$ by Galois theory. Applying the first part of our proof shows that $\mathrm{Ker}(\Phi_{\widetilde{L}/K,\mathfrak{m}}) = \mathrm{Ker}(\Phi_{L/K,\mathfrak{m}})$, which is possible only if $L = \widetilde{L} \subseteq M$ by the uniqueness part of Theorem 3.9. □

We are now ready to prove the Kronecker-Weber Theorem (Theorem 1.4).
Proof of Theorem 1.4: Suppose K is an Abelian number field. By the Artin reciprocity theorem (Theorem 3.6), there is a modulus $\mathfrak{m}$ such that $\mathcal{P}_{\mathbb{Q},1}(\mathfrak{m}) \subseteq \mathrm{Ker}(\Phi_{K/\mathbb{Q}})(\mathfrak{m})$. We may assume w.l.o.g. that $\mathfrak{m} = m\infty$. From (3-10), we see that

$$\mathcal{P}_{\mathbb{Q},1}(\mathfrak{m}) = \mathrm{Ker}(\Phi_{\mathbb{Q}(\zeta_m)/\mathbb{Q},\mathfrak{m}}) \subseteq \mathrm{Ker}(\Phi_{K/\mathbb{Q},\mathfrak{m}}),$$

and thus $K \subseteq \mathbb{Q}(\zeta_m)$ follows from Corollary 3.10. □

Next, let us discuss the Hilbert class field. Apply the Existence Theorem (Theorem 3.9) to the modulus $\mathfrak{m} = 1$ and the subgroup $\mathcal{P}_K = \mathcal{P}_{K,1}(\mathfrak{m})$, we see that there exists a unique unramified Abelian extension L of K, such that the Artin map induces an isomorphism

$$\mathcal{C}_K = \mathcal{I}_K/\mathcal{P}_K \xrightarrow{\sim} \mathrm{Gal}(L/K).$$

L is the Hilbert class field of K. Indeed,

Theorem 3.11 *The Hilbert class field L is the maximal unramified Abelian extension of K.*

Proof: Let M be any unramified Abelian extension of K. Then, 1) of the Conductor Theorem (Theorem 3.8) tells us that the conductor $\mathfrak{f}$ of M/K must be 1, and 2) implies that $\mathrm{Ker}(\Phi_{M/K,1})$ is a congruence subgroup for the modulus 1. Hence,

$$\mathcal{P}_K = \mathrm{Ker}(\Phi_{L/K,1}) \subseteq \mathrm{Ker}(\Phi_{M/K,1})$$

and by Corollary 3.10 we see that $M \subseteq L$. □

In particular, Theorem 3.1, 3.2 and Corollary 3.3 now follows immediately.

Remark 3.12 *By the Existence Theorem (Theorem 3.9), given any modulus $\mathfrak{m}$, there exists a unique Abelian extension $K_\mathfrak{m}$ of K such that*

$$\mathcal{P}_{K,1}(\mathfrak{m}) = \mathrm{Ker}(\Phi_{K_{\mathfrak{m}/K},\mathfrak{m}}).$$

$K_\mathfrak{m}$ is called the ray class field for the modulus $\mathfrak{m}$. *This is a generalization of the Hilbert class field since when $\mathfrak{m} = 1$, we see that $K_\mathfrak{m}$ is reduced to the Hilbert class field H_K. The computation in (3-9) (3-10) gives us another example: the cyclotomic field $\mathbb{Q}(\zeta_m)$ is the ray class field of $\mathbb{Q}$ for the modulus $m\infty$.*

In terms of ray class fields, the conduct $\mathfrak{f}$ of an Abelian extension L/K of number fields can be interpreted as the smallest modulus $\mathfrak{m}$ for which L is contained in $K_\mathfrak{m}$.

3.1.3 Reciprocity laws

Class field theory is the source of many reciprocity theorems. But let us focus on some of them for the n-th power Legendre symbol $\left(\frac{\alpha}{\mathfrak{p}}\right)_n$, as promised. To define this symbol, let K be a number field containing the n-th root of unity ζ_n, and let $\mathfrak{p}$ be a prime of $\mathcal{O}_K$. Then, for any $\alpha \in \mathcal{O}_K$ coprime to $\mathfrak{p}$,

$$\alpha^{N(\mathfrak{p})-1} \equiv 1 \pmod{\mathfrak{p}},$$

which is a fancy version of Fermat's Little Theorem. Suppose in addition that $\mathfrak{p}$ is coprime to n, then one can show (by general theory of finite fields) that $n \mid N(\mathfrak{p}) - 1$. Hence, $x = \alpha^{(N(\mathfrak{p})-1)/n}$ is a solution to the congruence equation $x^n \equiv 1 \pmod{\mathfrak{p}}$, and thus ($\zeta_n \in \mathcal{O}_K$)

$$\alpha^{(N(\mathfrak{p})-1)/n} \equiv 1, \zeta_n, \ldots, \zeta_n^{n-1} \pmod{\mathfrak{p}}$$

since the ζ_n^i's are pairwise distinct modulo $\mathfrak{p}$. We then set $\left(\frac{\alpha}{\mathfrak{p}}\right)_n$ to be the unique n-th root of unity such that

$$\alpha^{(N(\mathfrak{p})-1)/n} \equiv \left(\frac{\alpha}{\mathfrak{p}}\right)_n \pmod{\mathfrak{p}}. \tag{3-11}$$

This is a generalization of all the Legendre symbols we have seen so far (the ordinary one, and $\left(\frac{\alpha}{\pi}\right)_3$ in (3-5))! We can also extend $\left(\frac{\alpha}{\cdot}\right)_n$ to ideals $\mathfrak{a}$ of $\mathcal{O}_K$ which are coprime to n and α by multiplicativity, which induces a group homomorphism

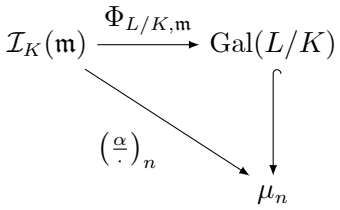
$$\left(\frac{\alpha}{\cdot}\right)_n : I_K(\mathfrak{m}) \to \mu_n,$$

where $\mathfrak{m}$ is a modulus divisible by every prime containing $n\alpha$, and μ_n is the group of n-th roots of unity.

Before proving two reciprocity theorems for the n-th power of Legendre symbol, let us recap a fact from Galois theory: If K contains the n-th root of unity ζ_n, then for any $\alpha \in K$, the extension $L = K(\sqrt[n]{\alpha})/K$ is Galois. Moreover, if $\sigma \in \mathrm{Gal}(L/K)$, then $\sigma(\sqrt[n]{\alpha}) = \zeta(\sqrt[n]{\alpha})$ for some n-th root of unity ζ, so $\mathrm{Gal}(L/K) \hookrightarrow \mu_n$.

Theorem 3.13 (Weak Reciprocity Law) *Let K be a number field containing ζ_n, and let $L = K(\sqrt[n]{\alpha})$ for some $0 \neq \alpha \in \mathcal{O}_K$. Suppose that $\mathfrak{m}$ is a modulus divisible by all primes of K containing $n\alpha$, and that $\mathrm{Ker}(\Phi_{L/K,\mathfrak{m}})$ is a congruence subgroup for $\mathfrak{m}$.*

Then, the following diagram



commutes.

Proof: It suffices to show that

$$\left(\frac{L/K}{\mathfrak{p}}\right)\left(\sqrt[n]{\alpha}\right)=\left(\frac{\alpha}{\mathfrak{p}}\right)_n\left(\sqrt[n]{\alpha}\right),$$

which is the same as our computation for the case $n=3$ in the end of section 3.1.1. □

Let G be the image of the natural injection $\mathrm{Gal}(L/K)\hookrightarrow\mu_n$, then the n-th power Legendre symbol induces a surjective homomorphism

$$\left(\frac{\alpha}{\cdot}\right)_n:\mathcal{I}_K(\mathfrak{m})/\mathcal{P}_{K,1}(\mathfrak{m})\twoheadrightarrow G\leq\mu_n.$$

Though the Weak Reciprocity Law merely asserts that $\left(\frac{\alpha}{\cdot}\right)_n$ is a homomorphism, rather than giving explicit formulas for computation (that is why it is called "weak"), it is still powerful. For instance, let us use it to prove the Quadratic Reciprocity Law:

Let p,q be distinct odd primes, and set $p'=(-1)^{(p-1)/2}p$. Note that the quadratic reciprocity law is equivalent to saying that (as we have used once in section 2.3.2)

$$\left(\frac{p'}{q}\right)=\left(\frac{p}{q}\right),$$

our first step would be to study $\mathbb{Q}(\sqrt{p'})/\mathbb{Q}$. We have seen that $\mathbb{Q}(\sqrt{p'})\subseteq\mathbb{Q}(\zeta_p)$ (see 2) of section 1.1), but let us give a different proof here:

Recall (3-10), $\mathrm{Gal}(\mathbb{Q}(\zeta_p)/\mathbb{Q})$ is a generalized ideal class group for the modulus $p\infty$, and thus the same is true for any subfield of $\mathbb{Q}(\zeta_p)$ (by Corollary 3.10). In particular, since $\mathrm{Gal}(\mathbb{Q}(\zeta_p)/\mathbb{Q})\cong\mathbb{Z}_p^\times$ is cyclic, there exists a unique quadratic subfield $K\subseteq\mathbb{Q}(\zeta_p)$, and $\mathrm{Gal}(K/\mathbb{Q})$ is a general ideal class group for $p\infty$. Hence, p is the only finite prime of $\mathbb{Q}$ that is ramified in K, so $K=\mathbb{Q}(\sqrt{p'})$.

It follows that $\mathrm{Ker}\left(\Phi_{\mathbb{Q}(\sqrt{p'})/\mathbb{Q},p\infty}\right)$ is a congruence subgroup for $p\infty$, so the Weak Reciprocity Law offers us a surjective homomorphism

$$\left(\frac{p'}{\cdot}\right):\mathcal{I}_{\mathbb{Q}}(p\infty)/\mathcal{P}_{\mathbb{Q},1}(p\infty)\twoheadrightarrow\{\pm1\}.$$

However, the Artin map

$$\Phi_{\mathbb{Q}(\zeta_p)/\mathbb{Q},p\infty}:\mathcal{I}_{\mathbb{Q}}(p\infty)\to\mathrm{Gal}(\mathbb{Q}(\zeta_p)/\mathbb{Q}),\quad(a)\mapsto\overline{a}$$

induces an isomorphism

$$\mathcal{I}_{\mathbb{Q}}(p\infty)/\mathcal{P}_{\mathbb{Q},1}(p\infty)\xrightarrow{\sim}\mathbb{Z}_p^\times,$$

so the Legendre symbol $\left(\frac{p'}{\cdot}\right)$ can be viewed as a non-trivial quadratic character, which must coincide with $\left(\frac{\cdot}{p}\right)$.

We now state the Strong Reciprocity Law for n-th power Legendre symbol. For simplicity, if $\alpha, \beta \in \mathcal{O}_K$, then we write $\left(\frac{\alpha}{\beta}\right)_n$ to denote $\left(\frac{\alpha}{\cdot}\right)_n$ valued at the ideal (β), when defined.

Theorem 3.14 (Strong reciprocity law) *Let K be a number field containing ζ_n, and let $\alpha, \beta \in \mathbb{O}_K$ be coprime to each other and both to n. Then*

$$\left(\frac{\alpha}{\beta}\right)_n \left(\frac{\beta}{\alpha}\right)_n^{-1} = \prod_{\mathfrak{p}|n\infty} \left(\frac{\alpha, \beta}{\mathfrak{p}}\right)_n, \tag{3-12}$$

where $\left(\frac{\alpha,\beta}{\mathfrak{p}}\right)_n$ is the n-th power Hilbert symbol *and ∞ is the product of the real infinite primes of K.*

The n-th power Hilbert symbol $\left(\frac{\alpha,\beta}{\mathfrak{p}}\right)_n$ is defined using local class field theory of the completion $K_\mathfrak{p}$ of K at the prime $\mathfrak{p}$, so the precise definition is kindly omitted here, since we did not develop any local methods. But let us apply the Strong Reciprocity Law to the Cubic Reciprocity Law (Theorem 3.5) to get a feel of what is going on: Consider $K = \mathbb{Q}(\sqrt{-3}) = \mathbb{Q}(\zeta_3)$, and hence $n = 3$. The only prime of $\mathbb{O}_K$ dividing 3 is $(1 - \zeta_3)$ and thus

$$\left(\frac{\pi}{\theta}\right)_3 \left(\frac{\theta}{\pi}\right)_3^{-1} = \left(\frac{\pi, \theta}{1 - \zeta_3}\right)_3.$$

Therefore, the proof of the cubic reciprocity law is reduced to a purely local computation, which is not hard after establishing the properties of the Hilbert symbol.

3.2 The distribution of primes and its friends

We have met with several situations in which the primes of a number field are mapped naturally into a finite abelian group. And it turns out that, in each case, they are distributed uniformly (in a certain sense) among the members of the group. The study of this problem by Kronecker, Frobenius, Čebotarev, et. al. set off another path to class field theory. We will see how they are related and give some brief historical notes on the developments of class field theory along this direction.

Our main references here are chapter 8 of [M18], section 8.B. of chapter 2 of [C11], and Conrad's notes on history of class field theory [C01].

3.2.1 Uniform distribution results in Abelian number fields

Consider the following maps:

1) Fix $m \in \mathbb{N}^+$, and send the primes $p \in \mathbb{Z}$, $p \nmid m$ into $\mathbb{Z}_m^\times$ by taking its congruence class mod m;

2) Let K be a number field, send the (finite) primes of K into the ideal class group $\mathcal{C}_K$ by taking its ideal class;

3) Let L/K be an abelian extension of number fields, send the primes of K which are unramified in L into the Galois group $\mathrm{Gal}(L/K)$ via the Artin map.

We have computed in (3-9) that 1) can be regarded as a special case of 3), in which we take $K=\mathbb{Q}$ and $L=\mathbb{Q}(\zeta_m)$. Moreover, Class field theory tells us that 2) is also a special case of 3). Indeed, let H_K be the Hilbert class field of K, then the Artin map induces an isomorphism

$$\left(\frac{H_K/K}{\cdot}\right):\mathcal{C}_K\xrightarrow{\sim}\mathrm{Gal}(H_K/K),$$

so take $L=H_K$ in 3) reduces to 2), which is far from obvious at first.

For convenience, we will first put 1) - 3) into a more abstract context and establish general sufficient conditions of uniform distribution in finite abelian groups, and then check that these conditions are satisfied case by case.

Let X be a countably infinite set and let G be a finite abelian group. Suppose we are given a function $\Phi: X\to G$, and for each $P\in X$ (we shall call it a "prime") we have assigned it a "norm" $N(P)>1$. Let Π be the free abelian semigroup generated by X, then we can extend $\Phi(\cdot)$ and $N(\cdot)$ to Π multiplicatively.

It is clear what X, G, Π and $N(\cdot), \Phi(\cdot)$ should be in 1) - 3). For instance, in 3), X is the set of primes of which are unramified in L, $G=\mathrm{Gal}(L/K)$ and Π consists of all moduli $\mathfrak{m}$ not divisible by finite primes ramified in L and infinite primes, $N(\cdot)=N_{K/\mathbb{Q}}(\cdot)$ and $\Phi(\cdot)$ is the Artin map.

Our next step is to form some Dirichlet-type series. We shall make a technical assumption that

$$\sum_{P\in X}\frac{1}{N(P)^s}<\infty,\quad \forall s>1 \tag{3-13}$$

which assures that the series

$$\sum_{I\in\Pi}\frac{1}{N(I)^s}$$

converges in the right half-plane $\mathrm{Re}(s)>1$. Moreover, it is not hard to see that

$$\sum_{I\in\Pi}\frac{1}{N(I)^s}=\prod_{P\in X}\left(1-\frac{1}{N(P)^s}\right)^{-1}$$

when $\mathrm{Re}(s)>1$. Note that (3-13) is indeed valid in our three concrete examples since for any number field K,

$$\log\zeta_K(s)=\sum_{\mathfrak{p}}-\log\left(1-\frac{1}{N(\mathfrak{p})^s}\right)\sim\sum_{\mathfrak{p}}\frac{1}{N(\mathfrak{p})^s} \tag{3-14}$$

and our set X are always subsets of finite ideals of K.

Let χ be any character of G (i.e., group homomorphism $G\to S^1$[1]), we define the

[1]Equivalently, χ is an *irreducible representation* of G. This point of view is important for Weber L-functions and Artin L-functions.

L-series of χ to be

$$L(s,\chi)=\sum_{I\in\Pi}\frac{\chi(I)}{N(I)^s},\quad \mathrm{Re}(s)>1,$$

where $\chi(I)$ is defined as $\chi(\Phi(I))$. Again, it allows a product expression

$$L(s,\chi)=\prod_{P\in X}\left(1-\frac{\chi(P)}{N(P)^s}\right)^{-1},\mathrm{Re}(s)>1.$$

For instance, in 1) the $L(s,\chi)$'s are ordinary Dirichlet L-functions, in 2) $L(s,1)$ is the Dedekind zeta function ζ_K and in 3) $L(s,1)$ is close to ζ_K.

Theorem 3.15 (Abstract Distribution Theorem) *With notations as above, under assumption (3-13), and assume further that all $L(s,\chi)$'s have meromorphic extensions in a neighborhood of $s=1$ such that $L(s,1)$ has a pole at $s=1$ which other $L(s,\chi)$ have finite non-zero values at $s=1$. Then, for each $a\in G$,*

$$\sum_{\Phi(P)=a}\frac{1}{N(P)^s}-\frac{1}{|G|}\sum_{P\in X}\frac{1}{N(P)^s} \tag{3-15}$$

has a finite limit as $s\to 1^+$.

Remark 3.16 *From the conditions of the Abstract Distribution Theorem, (3-15) implies that*

$$\lim_{s\to 1^+}\frac{\sum_{\Phi(P)=a}N(P)^{-s}}{\sum_{P\in X}N(P)^{-s}}=\frac{1}{|G|}. \tag{3-16}$$

We say that the set $S:=\{X\in P:\Phi(P)=a\}$ has Dirichlet density $1/|G|$. *In our examples 1) - 3) here, (3-16) has the following equivalent formulation that*

$$\lim_{s\to 1^+}\frac{\sum_{P\in S}N(P)^{-s}}{-\log(s-1)}=\frac{1}{|G|}, \tag{3-17}$$

since $\sum_{P\in X}1/N(P)^s\sim\log\zeta_K(s)\sim(-\log(s-1))$.

Proof of Theorem 3.15: Our proof is analogous to that of Theorem 2.9 in the sense that similar stratgies are applied here. Fixing $a\in G$, and for $\mathrm{Re}(s)>1$, we have

$$\begin{aligned}\sum_{\chi\in\hat{G}}\chi\left(a^{-1}\right)\sum_{P\in X}\frac{\chi(P)}{N(P)^s}&=\sum_{P\in X}\frac{\sum_{\chi\in\hat{G}}\chi(a^{-1}\Phi(P))}{N(P)^s}\\&=|G|\sum_{\Phi(P)=a}\frac{1}{N(P)^s}.\end{aligned}$$

Where, the first equality is justified by absolute convergence, and the second equality follows from the orthogonal relations of characters (this can be also seen as a direct corollary of the proof of Lemma 2.7). Hence,

$$\sum_{P\in X}\frac{1}{N(P)^s}+\sum_{\chi\neq 1}\chi(a^{-1})\sum_{P\in X}\frac{\chi(P)}{N(P)^s}=|G|\sum_{\phi(P)=a}\frac{1}{N(P)^s}.$$

To complete the proof, we need to show that each of the series

$$M(s,\chi) := \sum_{P\in X} \frac{\chi(P)}{N(P)^s}, \quad \chi \neq 1,$$

has a finite limit as $s \to 1^+$, which we proceed via exponential functions:

For any $\chi \neq 1$, we know $M(s,\chi)$ is holomorphic on the right half-plane $\mathrm{Re}(s) > 1$ by complex analysis[1], so in particular, $M(s,\chi)$ is continuous to the right of $s = 1$. Moreover, if f is any continuous complex-valued function defined on an interval $(1, 1+\varepsilon)$, then $f(x)$ has a finite limit at $s = 1$ iff so is $e^{f(x)}$. Thus, it suffices to show that

$$e^{M(s,\chi)}$$

has a finite, non-zero limit as $s \to 1^+$ for each $\chi \neq 1$.

For $\mathrm{Re}(s) > 1$, we have

$$e^{M(s,\chi)} = \prod_{P\in X} e^{z(s,P)} = L(s,\chi) \prod_{P\in X} \left((1 - z(s,P))e^{z(s,P)}\right)$$

where

$$z(s,P) = \frac{\chi(P)}{N(P)^s}.$$

By assumption, $L(s,\chi)$ has a finite, non-zero limit at $s = 1$, so it remains to prove the same is true for the product at the right. If we write the product as

$$\prod_{P\in X} (1 - w(s,P))$$

where

$$w(s,P) = 1 - (1 - z(s,P))e^{z(s,P)},$$

then it is equivalent[2] to show that the sum

$$\sum_P |w(s,P)|$$

converges uniformly in a neighborhood of $s = 1$. Claim: for each $P \in X$,

$$|w(s,P)| \leqslant B|z(s,P)|^2$$

for all $\mathrm{Re}(s) > 0$, where B is a constant independent of s and P. Our result will follow from the claim since $|z(s,P)| = N(P)^{-\sigma}$ $(s = \sigma + i\tau)$, and by assumption

$$\sum_P \frac{1}{N(P)^{2\sigma}}$$

converges uniformly for $\sigma \geqslant 1/2 + \delta$, $\forall\, \delta > 0$.

Finally, we prove the claim as follows: Fix s and P, and write $w = w(s,P), z =$

[1] Let $\{f_n\}$ be a sequence of holomorphic functions on a region $\Omega \subset \mathbb{C}$. Suppose f is a complex function on $\mathbb{C}$ such that f_n converges uniformly to f on compact subsets of Ω, then f is holomorphic on Ω.

[2] The infinite product $\prod_{k\geq 1} z_k$ of complex numbers converges absolutely iff $\sum_{k\geq 1} \|z_k - 1\| < \infty$.

$z(s,P)$. Then, $|z|<1$ and

$$w = 1-(1-z)e^z.$$

To show that $|w| \leq B|z|^2$, consider the meromorphic function

$$g(z) = \frac{1-(1-z)e^z}{z^2},$$

which is holomorphic on $\mathbb{C}$ since the numerator has a double zero at $z=0$. In particular, $g(z)$ is continuous, and thus bounded on compact sets of $\mathbb{C}$, so our claim follows. □

Now, we are left to check that the conditions of the Abstract Distribution Theorem (Theorem 3.15) are satisfied in 1) - 3).

The case 1) is what we have done to obtain the Dirichlet Class Number Formula for cyclotomic fields (the proof of 2) of section 2.1.1, Theorem 2.8 and 2.12). Hence, we now have a strong version of Dirichlet's theorem on arithmetic progressions:

Theorem 2.14′ (Dirichlet) *For any two positive coprime integers a and m, the set*

$$\{p \in \mathbb{Z} \text{ prime} : p \equiv a \pmod{m}\}$$

has Dirichlet density $1/\varphi(m)$, where φ is the Euler totient function.

As aforementioned, the crucial step in the proof was showing that $L(1,\chi) \neq 0$ for non-principal characters, so we now examine this more closely. Instead of applying the Class Number Formula, it is important to go back to Lemma 2.7. Taking the product over all the primes $p \nmid m$ in (2-23) yields

$$\prod_{\chi \in \widehat{\mathbb{Z}_m^\times}} L(s,\chi) = \prod_{p \nmid m} \left(1 - \frac{1}{p^{f_p s}}\right)^{-r_p}, \quad \mathrm{Re}(s) > 1, \tag{3-18}$$

where we recall that f_p is the order of $\overline{p}$ in $\mathbb{Z}_m^\times$, and $r_p = \varphi(m)/f_p$. If $L(s,\chi)$ vanishes at $s=1$ for some $\chi \neq 1$, then the left hand side of (3-18) would allow a holomorphic continuation to the right half-plane $\mathrm{Re}(s) > 0$, since that zero would cancel out the simple pole of $L(s,1)$ at $s=1$. Hence, the product on the right hand side would have a finite limit as $s \to 1^+$, s real. In particular, removing all factors with $p \not\equiv 1 \pmod{m}$ (this is legal since when $s>1$, all factors in the product are real numbers greater than 1), we see that

$$\lim_{s \to 1^+} \prod_{p \equiv 1 \pmod{m}} \left(1 - \frac{1}{p^s}\right)^{-\varphi(m)} < \infty. \tag{3-19}$$

This contradicts with the following fact:

Theorem 3.17 *Let L/K be a Galois extension of number fields. Then, the set of primes of K which split completely in L, denoted by $\mathrm{Spl}(L/K)$, has Dirichlet density $1/[L:K]$.*

Proof: Write $A = \mathrm{Spl}(L/K)$, and let B be the set of primes of L which lie over primes in

A. Then, for each $\mathfrak{p} \in A$, there are $[L:K]$ primes $\mathfrak{q} \in B$ lying over $\mathfrak{p}$, and $N(\mathfrak{q}) = N(\mathfrak{p})$ whenever $\mathfrak{q} \in B$, $\mathfrak{p} \in A$. Hence,

$$\zeta_{L,B}(s) = \zeta_{K,A}^{[L:K]}(s),$$

where we set $[A]$ to be the semigroup generated by A and define

$$\zeta_{K,A}(s) := \sum_{\mathfrak{a} \in [A]} \frac{1}{N(\mathfrak{a})^{-s}} = \prod_{\mathfrak{p} \in A} \left(1 - \frac{1}{N(\mathfrak{p})^{-s}}\right)^{-1}, \quad \text{Re(s)>1},$$

and similar for $\zeta_{L,B}(s)$. Note that B contains every prime $\mathfrak{q}$ of L for which $N(\mathfrak{q})$ is prime, except possibly for finitely many which are ramified over K,

$$\zeta_{L,B}(s) \sim \zeta_L(s)$$

and thus B has Dirichlet density 1. It follows immediately that A has Dirichlet density $1/[L:K]$. □

In particular, if we take $K = \mathbb{Q}$ and $L = \mathbb{Q}(\zeta_m)$, then the set

$$\{p \in \mathbb{Z} \text{ prime} : p \equiv 1 \pmod{m}\}$$

has Dirichlet density $1/\varphi(m)$, contradicting (3-19).

We now generalize our alternative argument of 1) to 2) as well. Mimicking the argument above, we are led to consider the product

$$\prod_{\chi \in \widehat{G}} L(s,\chi) = \prod_{\mathfrak{p}} \left(1 - \frac{1}{N(\mathfrak{p})^{f_p s}}\right)^{-r_p}. \tag{3-20}$$

From 2) of section 2.1.1, it is clear that $L(s,1) = \zeta_K(s)$ has a simple pole at $s = 1$, and each $L(s,\chi)$ $(\chi \neq 1)$ converges to a holomorphic function on the right half-plane $\mathrm{Re}(s) > 1/[K:\mathbb{Q}]$. Thus, it suffices to show that $L(1,\chi) \neq 0$ for $\chi \neq 1$, which we prove by contradiction analogously:

If any $L(s,\chi)$ vanishes at $s = 1$, then the product in the left hand side of (3-20) extends to a holomorphic function on the right half-plane $\mathrm{Re}(s) > 1/[K:\mathbb{Q}]$, and similarly we would get

$$\lim_{s \to 1^+} \prod_{\mathfrak{p} \text{ principal}} \left(1 - \frac{1}{N(\mathfrak{p})^s}\right)^{-|G|} < \infty.$$

Intuitively, this implies that there are very few principal primes. In particular, the set of principal primes cannot have positive Dirichlet density. However, Theorem 3.17 tells us that the set of primes of K which split completely have positive Dirichlet density, so we would have enough principal primes to reach a contradiction if we can find an extension of K in which every prime splits completely is principal. But this is what the Hilbert class field H_K of K offers us for free (Corollary 3.4)! Moreover, the isomorphism induced by the Artin map $\left(\frac{H_K/K}{\cdot}\right)$ leads us to the special case of 3) (when $L = H_K$) as well.

How to generalize our argument work to all cases of 3)? This is where class field theory comes to rescue! Indeed, note that any abelian extension L of K is contained in some ray class field $K_{\mathfrak{m}}$ of K for some modulus $\mathfrak{m}$ (this follows from Remark 3.12), it suffices to deal with the case where $L = K_{\mathfrak{m}}$. This is not terribly hard since $\mathcal{P}_{K,1}(\mathfrak{m})$ is the identity class of the *ray class group* $\mathcal{C}_K(\mathfrak{m})$ for the modulus $\mathfrak{m}$, which contains enough primes in $K_{\mathfrak{m}}$.

3.2.2 Some historical notes

In the last section, let us go for a hiking along the historical path of the motivations and developments of class field theory. Our discussions here mainly follow section 1-6 of [C01]. Though far from complete, this will still be an exciting trip. As Grothendieck once said[1]:

"*And every science, when we understand it not as an instrument of power and domination but as an adventure in knowledge pursued by our species across the ages, is nothing but this harmony, more or less vast, more or less rich from one epoch to another, which unfurls over the course of generations and centuries, by the delicate counterpoint of all the themes appearing in turn, as if summoned from the void.*"

How can one not get thrilled when he/she sees how these greatest minds, Kronecker, Weber, Hilbert, Takagi, Artin, et. al. built up the whole beautiful class field theory, little by little from concrete problems?

In 1853, Kronecker announced that *every Abelian number field lies in a cyclotomic field*, now known as the Kronecker–Weber Theorem (Theorem 1.4). However, his own proof had difficulties with extensions of 2-power degree. The first accepted proof was by Weber in 1886, but it also had an error at 2, which went not noticed until about 90 years later. Hilbert gave the first correct proof in 1896, in which he succeeded partly because $\mathbb{Q}$ does not admit proper unramified Abelian extensions. This might lead his interests to unramified extensions later.

Extending Abel's work on Abelian extensions of $\mathbb{Q}(i)$ (1829), Kronecker was able to construct abelian extensions of imaginary quadratic fields via special values of elliptic and modular functions. In a letter to Dedekind in 1880, he described his "Jugendtraum" as the hope that *every finite abelian extension of an imaginary quadratic field is contained in one of the extensions he had found*, which was proved later by T. Takagi in his 1903 thesis.

An important case of Kronecker's work uses the j-function: Let K be an imaginary quadratic field, and write $\mathbb{O}_K = \mathbb{Z} + \mathbb{Z}\tau$, where $\tau \in \mathbb{H}$ (the upper half-plane). Then, Kronecker proved that $j(\tau)$ is algebraic over K, $K(j(\tau))/K$ is Galois whose Galois group is isomorphic to the ideal class group of K. Moreover, he observed that $K(j(\tau))$ is unramified over K and every ideal of K becomes principal in it. Hilbert included these properties into his general conjectures on Hilbert class fields.

In an 1880 paper, Kronecker set off another path to class field theory by studying densities of primes and factorization of polynomials. Given a monic polynomial $f \in \mathbb{Z}[x]$, Kronecker considered the number n_p of roots of the reduction mod p of f (denoted

[1]Translated from his autobiography *Récoltes et semailles: Réflexions et témoignage sur un passé de mathématicien.*

by f_p) as p varies:

Theorem 3.18 (Kronecker) *If f has r irreducible factors in $\mathbb{Z}[x]$, then the average value of n_p is r. More precisely,*

$$\lim_{s\to 1^+} \frac{\sum_p n_p p^{-s}}{\sum_p p^{-s}} = r.$$

As a corollary, we obtained a special case of Theorem 3.17:

Corollary 3.19 *Let $K/\mathbb{Q}$ be a Galois extension. Then, the set of primes which split completely in K has Dirichlet density $1/[K:\mathbb{Q}]$.*

Proof: Write $K = \mathbb{Q}(\alpha)$ for some algebraic integer α, and let $f(x) \in \mathbb{Z}[x]$ be its minimal polynomial. Note that the roots of f are polynomials in α with rational coefficients ($K/\mathbb{Q}$ is Galois), if f_p has a root, then it splits completely for all but at most finitely many primes. In this case, $n_p = \deg f = [K:\mathbb{Q}]$. Let A be the set of primes p such that $n_p = [K:\mathbb{Q}]$, then by Theorem 3.18 we see that

$$\lim_{s\to 1^+} \frac{\sum_{p\in A} 1 p^{-s}}{\sum_p p^{-s}} = \frac{1}{[K:\mathbb{Q}]}.$$

Hence, the result follows from the fact that expect for finitely many primes, f_p splits completely iff p splits completely in K[1]. □

Kronecker's paper contained two influential conjectures on sets of primes. The first one was about the density of the set of primes p such that f_p has a fixed number of roots n_p in $\mathbb{F}_p$. In particular, if $n_p = \deg f$ then f splits completely and it reduces to Theorem 3.19. Though he did not managed to prove the existence of these densities in general, he conjectured that they exist and described some properties they should have. The existence of these densities was first established by Frobenius:

Theorem 3.20 (Frobenius Density Theorem) *Let L/K be a Galois extension of number fields, and let $\sigma \in G = \mathrm{Gal}(L/K)$. Suppose σ has t elements in its* division *(the collection of all elements of G which are conjugate to some σ^m with $(m, |G|) = 1$), then the set S of primes of K which are divisible by a prime of L having Frobenius automorphism in the division of σ has Dirichlet density $t/|G|$.*

Proof: See for instance [J96] Chapter V, Theorem 5.2, p. 162-164. □

Corollary 3.21 *Let $f \in \mathbb{Z}[x]$ be a monic and irreducible, then the set of primes p such that f_p has a given decomposition type $n_1, n_2, \ldots, n_r$ has Dirichlet density $t/|\mathrm{Gal}(f)|$, where $\mathrm{Gal}(f)$ is the Galois group of f (i.e., the Galois group of the splitting field of f), and*

$$t = \#\{\sigma \in \mathrm{Gal}(f) : \sigma \text{ has the cycle pattern } n_1, \ldots, n_r\}.$$

Proof: Note that a permutation τ is in the division of σ iff it has the same cycle type as σ, apply Theorem 3.20 to the case where $K = \mathbb{Q}$ and L is the splitting field of f. □

[1] This follows from the Dedekind–Kummer Theorem, which we use extensively in this subsection.

Corollary 3.21 solves Kronecker's first conjecture since the number of roots of f_p is measured by the number of 1's appearing in the decomposition typer of f_p. In Frobenius's work on this problem, he introduced the Frobenius element of a prime ideal and conjectured what later became the Čebotarev density theorem:

Theorem 3.22 (Čebotarev Density Theorem) *Let L be a Galois extension of K, and let $\langle\sigma\rangle$ be the conjugate class of an element $\sigma \in \mathrm{Gal}(L/K)$. Then, the set*

$$S = \left\{ \mathfrak{p} \in \mathcal{O}_K \text{ prime} : \mathfrak{p} \text{ is unramified in } L \text{ and } \left(\frac{L/K}{\mathfrak{p}}\right) = \langle\sigma\rangle \right\}$$

has Dirichlet density $|\langle\sigma\rangle|/|\mathrm{Gal}(L/K)| = |\langle\sigma\rangle|/[L:K]$.

Proof: See for instance [J96] Chapter V, Theorem 10.4, p. 217-218. □

Kronecker's second conjecture was that a Galois extension K of $\mathbb{Q}$ is characterized by the set of primes in $\mathbb{Q}$ which split completely in K, which was proved by Bauer (1903) for any Galois extensions of number fields.

Theorem 3.23 (Bauer) *Let K be a number field, and suppose L_1 and L_2 are finite Galois extensions of K. Then $L_1 \subseteq L_2$ iff $\mathrm{Spl}(L_2/K) \subseteq \mathrm{Spl}(L_1/K)$. In particular, $L_1 = L_2$ iff $\mathrm{Spl}(L_1/K) = \mathrm{Spl}(L_2/K)$.*

Though Bauer's theorem tells that a Galois extension L/K of number fields is determined by the set $\mathrm{Spl}(L/K)$ of primes in K which split completely in L, it does not give us a way of describing the $\mathrm{Spl}(L/K)$. When L/K is Abelian, class field theory give a simple criterion of finding $\mathrm{Spl}(L/K)$ in terms of generalized congruence subgroups. ($\mathfrak{p} \in \mathrm{Spl}(L/K)$ iff $\mathfrak{p}$ is in the Kernel of the Artin map!)

In 1897, Weber extended the concept of ideal class group to what we saw[1] in the beginning of section 3.1.2. For instance, when $K = \mathbb{Q}$ and $\mathfrak{m} = m$, then $\mathcal{I}_K(\mathfrak{m})/\mathcal{P}_{K,1}(\mathfrak{m}) \cong \mathbb{Z}_m^\times$. Regarding the generalized ideal class group $\mathcal{I}_K(\mathfrak{m})/H$ (where $H \geq \mathcal{P}_{K,1}(\mathfrak{m})$ is a congruence subgroup) as a generalization of $\mathbb{Z}_m^\times$, Weber considered the following question analogous to Dirichlet's theorem on arithmetic progressions (Theorem 2.14): Does each coset of $\mathcal{I}_K(\mathfrak{m})/H$ contain infinitely many prime ideals? He adapted Dirichlet's method and formed the following L-function for characters $\psi : \mathcal{I}_K(\mathfrak{m})/H \to S^1$

$$L(s,\psi) := \sum_{(\mathfrak{a},\mathfrak{m})=1} \frac{\psi(\mathfrak{a})}{N(\mathfrak{a})^s} = \prod_{\mathfrak{p}\nmid\mathfrak{m}} \frac{1}{1-\psi(\mathfrak{p})N(\mathfrak{p})^{-s})}, \quad \mathrm{Re}(s) > 1.$$

It turns out that if ψ is non-trivial, then the series converges for $\mathrm{Re}(s) > 1 - [K:\mathbb{Q}]$, so again it makes sense to talk about $L(1,\psi)$. Based on the fact that $L(1,\psi) \neq 0$, Weber proved that:

Theorem 3.24 (Weber) *Let $\mathfrak{m}$ be a modulus of K, and let H be a congruence subgroup with modulus $\mathfrak{m}$. Assume that there is a Galois extension L/K such that $\mathrm{Spl}(L/K) \subseteq H$ with at most finitely many exceptions. Then,*

$$[\mathcal{I}_K(\mathfrak{m}) : H] \leq [L:K].$$

[1] In fact, it is a slightly special case of our definition.

If $\mathrm{Spl}(L/K) = H$ *except for at most finitely many exceptions, then* $[\mathcal{I}_K(\mathfrak{m}) : H] = [L : K]$ *and there are infinitely many primes in each coset of* $\mathcal{I}_K(\mathfrak{m})/H$.

To complete Weber's extension of Dirichlet's theorem on arithmetic progressions, the existence of class fields was needed. And based on analogies between number fields and Riemann surfaces, Hilbert made conjectured that *given a number field* K*, there is a unique finite Galois extension* H_K *of* K *such that*

1) $Gal(H_K) \cong \mathcal{C}_K$ *(in particular,* H_K *is Abelian);*

2) H_K/K *is unramified, and every unramified Abelian extension of* K *is a subfield of* H_K*;*

3) for any prime $\mathfrak{p}$ *of* K*, its inertial degree is the same as its order in* $\mathcal{C}_K$*;*

4) every ideal of K *is principal in* H_K.

As we have seen 1) and 2) is the statement of Theorem 3.1, and the rest follows from the Artin Reciprocity Theorem (3.2).

Hilbert proved the existence of Hilbert class field when $h(K) = 2$ and $[K : \mathbb{Q}] = 2$. Hilbert's student Furtwängler proved 1) and 2) in general in 1907, and 3) in 1911. After Artin reduced the last part to a group-theoretic statement related to the iterated Hilbert class field H_{H_K}, he finally managed to prove 4) in 1930.

During the World War I, working in isolation, Takagi combined the work of Furtwängler on the Hilbert class field and Fueter on abelian extensions of imaginary quadratic fields to prove the existence of class fields in full generality. Takagi did not prove the isomorphism

$$\mathcal{I}_K(\mathfrak{m})/H \to Gal(L/K)$$

by constructing an explicit isomorphism, but only obtained it indirectly.

It was Artin who established this canonical isomorphism (1927), the Artin map (3-8). He proved the Artin Reciprocity Theorem (Theorem 3.6), which leads to many applications, and we discussed some of them in section 3.1.2 and 3.1.3.

All of these had made our hiking along the path of class field theory a fascinating journey!

Reference

[M18] Daniel A. Marcus. *Number fields*, 2nd ed. Springer International Publishing AG, 2018.

[ST16] Ian Stewart, and David Tall. *Algebraic number theory and Fermat's last theorem*, 4th ed. CRC Press, 2016.

[BS86] Zenon I. Borevich, and Igor R. Shafarevich. *Number theory*. Academic press, 1986.

[BW17] Jean Bourgain and Nigel Watt. "Mean square of zeta function, circle problem and divisor problem revisited." *arXiv preprint*. arXiv:1709.04340 (2017).

[C11] David A. Cox. *Primes of the form x2+ ny2: Fermat, class field theory, and complex multiplication.* Vol. 34. John Wiley & Sons, 2011.

[C01] 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).

[J96] Gerald J. Janusz. *Algebraic number fields.* Vol. 7. American Mathematical Soc., 1996.

Eidgenössische Technische Hochschule Zürich
Swiss Federal Institute of Technology Zurich

Declaration of originality

The signed declaration of originality is a component of every semester paper, Bachelor's thesis, Master's thesis and any other degree paper undertaken during the course of studies, including the respective electronic versions.

Lecturers may also require a declaration of originality for other written papers compiled for their courses.

I hereby confirm that I am the sole author of the written work here enclosed and that I have compiled it in my own words. Parts excepted are corrections of form and content by the supervisor.

Title of work (in block letters):

THE CLASS NUMBER FORMUA AND BEYOND

Authored by (in block letters):

For papers written by groups the names of all authors are required.

Name(s):	**First name(s):**
LIANG	HAORAN

With my signature I confirm that

- I have committed none of the forms of plagiarism described in the 'Citation etiquette' information sheet.
- I have documented all methods, data and processes truthfully.
- I have not manipulated any data.
- I have mentioned all persons who were significant facilitators of the work.

I am aware that the work may be screened electronically for plagiarism.

Place, date	**Signature(s)**
Zurich, 08.06.2022	Haoran Liang

For papers written by groups the names of all authors are required. Their signatures collectively guarantee the entire content of the written paper.