Artin's L-series and Stark's Conjecture

Yusheng Luo
Advisor: Professor Gross, Benedict

Minor Thesis

Department of Mathematics
Harvard University

December 25, 2015

Contents

1 Introduction

It is well-known that every abelian extension of $\mathbb{Q}$ is contained in some cyclotomic extension of $\mathbb{Q}$ (Kronecker-Weber theorem). Every cyclotomic extension is of the form $\mathbb{Q}(\zeta_m)$, where $\zeta_m = \exp(\frac{2\pi i}{m})$ is some special value of the exponential function. In 1900, David Hilbert asked if one can generalize the role that exponential function plays for $\mathbb{Q}$ to a general number field k (Hilbert's Twelfth Problem). In other words, can we find some special functions such that the maximal abelian extension of k can be obtained by adjoining special values of those functions. The problem remains still largely open, the only two cases we know are $\mathbb{Q}$ and quadratic imaginary field. For the quadratic imaginary field, using complex multiplication for elliptic curve associated to the field, we can show that the special functions are j-invariant and Weierstrass $\wp$-function.

In 1970s, Harold Stark made a sequence of conjectures about the first non-zero coefficients at $s = 0$ of the Artin's L-series associated to a field extension K/k. In the case of abelian extension and the order of vanishing at 0 is 1, the conjecture is equivalent to the existence of the so-called Stark's unit, whose roots generates a Kummer extension of K, which is abelian over k. The use of these conjectures to provide explicit generators of ray class fields, and thus to answer Hilbert's Twelfth Problem was one of the original motivations for their formulation. The Stark's conjecture has been proved in many special cases, in particular, for abelian extensions over $\mathbb{Q}$ and any quadratic imaginary field.

In this paper, we will start by reviewing class field theory and L-series in section 2 and 3. We will introduce the Stark's conjecture in the most general form in section 4, then we will focus on rank 1 abelian case in section 5. We will compute the Stark's units for the case $\mathbb{Q}$ and quadratic imaginary field in section 6 and 7.

2 Class Field Theory

The notion of *class field* is generally attributed to Hilbert in his fundamental paper *Zahlbericht* (number report). In truth, the origins of the concept may be dated back to the quadratic reciprocity law proved by Gauss. Generally speaking, the class filed theory studies abelian extension of a *global field*, i.e. a number filed or a function field of an algebraic curve. In this section, we will focus on the number field, and summarize some important theorems in class field theory.

Recall that a valuation of $|\cdot|_v$ on a field k is a function defined on k with values in the non-negative real numbers satisfying

1. $|\alpha|_v = 0$ if and only if $\alpha = 0$.
2. $|\alpha\beta|_v = |\alpha|_v|\beta|_v$
3. There is a constant C such that $|1+\alpha| \leqslant C$ if $|\alpha| \leqslant 1$

Two valuations are called *equivalent* if there is a constant $c > 0$ such that $|\alpha|_v = |\alpha|_w^c$ for every $\alpha \in k$. A field with topology induced by a valuation is a *topological field*, i.e. the operation sum, product and reciprocal are continuous. It is readily checked that two valuations on k are equivalent if and only if the topologies induced are the same.

A valuation is called *discrete* if the image $|\alpha|_v$ for $\alpha \in k^*$ forms a discrete subgroup of $\mathbb{R}_+$, and is called *non-archimedean* (or *non-arch.* for short) if we can take $C = 1$ in the axiom 3, i.e. the valuation satisfies the strong triangle inequality $|\alpha+\beta|_v \leqslant \max\{|\alpha|_v, |\beta|_v\}$. It is called *archimedean* (or *arch.* for short) otherwise. Note that using the classification of valuation on $\mathbb{Q}$ (which we will state later), we can easily show that if k is a number field, every non-arch. valuation is discrete. A field with a valuation is called *complete* if it is complete as a metric with respect to the metric induced by the valuation. Every field can be embedded in a unique complete field, and we will denote this by k_v, and call this the *completion* of k. A field with complete valuation is called a *local field*. For non-arch. valuations, the elements with $|\alpha|_v \leqslant 1$ clearly form a ring, the ring $\mathfrak{o}_v$ of *v-integers*. The elements with $|\alpha|_v < 1$ form a maximal ideal of $\mathfrak{o}_v$, and is denoted by $\mathfrak{p}_v$. It can be checked directly that two non-arch. valuations v, w are equivalent if and only if the rings $\mathfrak{o}_v = \mathfrak{o}_w$. The elements $\epsilon \in k$ with $|\epsilon|_v = 1$ form a group U_v under multiplication, and is called *group of v-units*. If the valuation v is discrete, then $\mathfrak{p}_v$ is a principal ideal (π), and every element $\alpha \in k^*$ is of the form $\pi^\nu\epsilon$ where ϵ is a v-unit. ν is called the *order* of α, and we will denote it by $\operatorname{ord}_v \alpha$. The *residue field* in our case $\mathfrak{o}_v/\mathfrak{p}_v$ is always finite, say with p elements, so we can define the *normalized valuation* to be $|\alpha|_v = p^{-\operatorname{ord}_v(\alpha)}$, if the valuation is non-arch.. If the valuation is arch., then Gelfand-Tornheim theorem tells us that the field k is isomorphic to a subfield of $\mathbb{C}$, with the valuation being equivalent to that induced by the *absolute valuation* on $\mathbb{C}$. Hence, we can define the *normalized valuation* to be the usual absolute value if $k \subset \mathbb{R}$, and the square of the absolute value if k is complex. We define a *finite prime* (or a *finite place*) to be an equivalent class of non-arch. valuation, (or equivalently a normalized non-arch. valuation), and an *infinite prime* (or an *infinite place*) to be an equivalent class of arch. valuation, (or equivalently a normalized arch. valuation). By a *prime* (or a *place*), we simply mean either a finite or infinite prime. Note if we let $\mathfrak{o} = \bigcap_v \mathfrak{o}_v$ be the ring of integers of k, then the equivalent classes of non-arch. valuations have one to one correspondence to prime ideals in $\mathfrak{o}$, via the map $v \mapsto \mathfrak{p}_v \cap \mathfrak{o}$. We will use $\mathfrak{M}_k$ to denote the set of primes for k.

For rational number $\mathbb{Q}$, we define the p-adic valuation to be $|p^a u/v|_p = p^{-a}$, where p is a prime, $a, u, v \in \mathbb{Z}$ and $p \nmid u$, $p \nmid v$. It can be checked directly that the ideal $\mathfrak{p}_p = (p)$. In fact, Ostrowski classifies all valuation on $\mathbb{Q}$: every non-trivial valuation on $\mathbb{Q}$ is either equivalent to $|\cdot|_p$ or the absolute valuation $|\cdot|_\infty$.

Let $a = p_1^{a_1} p_2^{a_2} ... p_k^{a_k}$ be a prime decomposition of a rational number, then clearly $|a|_p = 1$ if $p \neq p_j$, and $\prod_{p \text{ prime or } \infty} |a|_p = 1$. In fact, this still holds for general number field: if $\alpha \in k^*$, then $|\alpha|_v = 1$ for almost every $v \in \mathfrak{M}_k$ and $\prod_v |\alpha|_v = 1$.

Let Ω_λ with $\lambda \in \Lambda$ be a family of topological spaces, and Θ_λ be an open set of Ω_λ, the *restricted topological product* Ω to be the subspace of usual product $\prod_\lambda \Omega_\lambda$ consisting of elements $\boldsymbol{\alpha} = (\alpha_\lambda)_{\lambda \in \Lambda}$ with $\alpha_\lambda \in \Theta_\lambda$ for almost every $\lambda \in \Lambda$.

Let k be a number field, we can define the *Adele ring* V_k of k to be the restricted topological product of k_v the completion of a prime with respect to the ring $\mathfrak{o}_{k_v}$ of v-integers in k_v if v is a finite prime, and k_v if v is an infinite prime. The addition and multiplication are defined point-wise, and it can be easily check that this makes the V_k a topological ring. The *Idele group* J_k is defined to be the group of units V_k^* with the topology given by the subspace topology of $V_k \times V_k$ under the embedding $x \mapsto (x, x^{-1})$. It can be shown that the Idele group J_k is just the restricted topological product of k_v with respect to U_v the group of v-units if v is a finite prime, and k_v if v is an infinite prime. For $\boldsymbol{\alpha} = (\alpha_v) \in J_k$, we define the *content* of $\boldsymbol{\alpha}$ as $c(\boldsymbol{\alpha}) = \prod_v |\alpha_v|_v$. This is clearly a continuous group homomorphism, we denote J_k^1 to be the kernel of this map. Note k naturally embeds into V_k by the map $\alpha \mapsto (\alpha)_v$, and image of k^* lies in $J_k^1 \subset J_k \subset V_k$ as $|\alpha|_v = 1$ for almost every v and $\prod_v |\alpha|_v = 1$. The following theorems concerns the image of k under this natural embedding. The proof can be found in

Chapter II of [1, Chapter II, Section 15, 16].

Theorem 2.1. *Let k be a number field, V_k, J_k be its Adele ring and Idele group respectively, and let J_k^1 be defined as before, then*

1. *The image of k in V_k is discrete.*
2. *If v_0 be a prime, and $\mathcal{V}$ be the restricted topological product of k_v with respect to $\mathfrak{o}_{k_v}$ if v is finite, and k_v if v is infinite where $v \in \mathfrak{M}_k - \{v_0\}$, then the image of k is dense in $\mathcal{V}$.*
3. *The quotient space J_k^1/k^* is compact.*

The second part of the theorem stated above is usually referred as *Strong Approximation Theorem.* The third part of the theorem has many important applications, it is usually used together with discreteness to prove certain objects of interest are finite.

Let k be a number field, we define the *ideal class* I_k to be the free abelian group generated by finite primes, i.e., formal sums of $\sum_{v \text{ finite prime}} n_v v$, where only finitely many n_v's are non-zero. We call an element in I_k *integral* if every $n_v \geqslant 0$. Note that the $\mathfrak{o} := \bigcap_{v \text{ finite}} \mathfrak{o}_v$ is a Dedekind domain. If we identify any finite prime v with the prime ideal $\mathfrak{p}_v \cap \mathfrak{o}$, we can identify I_k with the group of fractional ideals in $\mathfrak{o}$, and the definition of integral elements agrees with the definition of integral ideals. We have a natural homomorphism from J_k to I_k defined by $\boldsymbol{\alpha} = (\alpha_v) \mapsto \mathrm{ord}_v(\alpha_v)v$ The image of $k*$ (viewed as a subset of J_k) is the group of *principal ideals.* The following theorem [1, Chapter II, Section 17] is a direct application of the previous theorem:

Theorem 2.2. *The* ideal class group*, i.e., I_k modulo the group of principal ideals, is finite.*

Proof. For the map $J_k^1 \longrightarrow I_k$ is the surjective, so the ideal group class is the continuous image of the compact group J_k^1/k^*, hence it is compact. But it is also discrete, so it is finite. $\square$

The cardinality of the ideal class group is called *class number*, and usually denoted by $h(k)$. The class number measures how far the ring of integers of certain field is away from principal ideal domain. In later sections, we will see how the class number is related to some special values of the Dedekind Zeta function of the field. For now, we will discuss the structure of units in a field.

Let S be a finite set containing infinite primes, we call an element α is a S-unit if $|\alpha|_v = 1$ for all $v \notin S$, and denote the set of S-unit by U_S, i.e. $U_S = \bigcap_{v \notin S} U_v$. Note that given $0 < c \leqslant C < \infty$, the set of S-units with $c \leqslant |\alpha|_v \leqslant C$ for all $v \in S$ is finite, as this set is precisely the intersection of the compact set

$$W = \{\boldsymbol{\alpha} : |\alpha|_v = 1, \text{ if } v \notin S, |\alpha|_v \in [c, C], \text{ if } v \in S\} \subset J_k$$

with the discrete set $k^* \subset J_k$.

If we put $c = C = 1$, we can easily see that the set with $|\alpha|_v = 1$ for all v is finite, and it is the group of roots of unity. Now we can prove the structure theorem of units [1, Chapter II, Section 18]:

Theorem 2.3 (Dirichlet Unit Theorem)**.** *U_S is the direct sum of a finite cyclic group (group of roots of unity) and a free abelian group of rank $s - 1$, where $s = |S|$.*

Proof. Let J_S consist of the $\boldsymbol{\alpha} = (\alpha_v)$ with $|\alpha_v|_v = 1$ for $v \notin S$, and let $J_S^1 = J_S \cap J_k^1$. Then clearly, the group $J_S^1/U_S = J_S^1/(J_S^1 \cap k^*)$ is compact in J_k^1/k^*.

Let r denote that number of infinite primes in S, and consider the map

$$\lambda : J_S \longrightarrow \mathbb{R}^r \oplus \mathbb{Z}^{s-r}$$

given by the map

$$\boldsymbol{\alpha} \mapsto (\log |\alpha_1|_1, ..., \log |\alpha_s|_s)$$

where $1, ..., s$ are primes in S, with the first r being infinite primes. The logarithm for the finite primes are assumed to be taken with base $|\mathfrak{o}_v/\mathfrak{p}_v|$. The map is clearly continuous and surjective, with kernel the group of roots of unity. By the previous observation, the group $\Lambda = \lambda(U_S)$ is discrete. Further, $T = \lambda(J_S^1)$ is just the set of $(x_1, ..., x_s)$ with $x_1 + ... + x_s = 0$. Finally, begin a continuous image of J_S^1/U_S, we know T/Λ is compact, so Λ is free with rank $s - 1$ as asserted. □

If we choose S to be the set of infinite primes, then the theorem above is called *Dirichlet Unit Theorem.*

We will now focus on the a finite Galois extension K of a number field k, with Galois group

$G = \mathrm{Gal}(K/k)$. If $\sigma \in G$ and $a \in K$, we will use either σa or a^σ to denote the natural action of G on K. Note that in the second form, we need to switch the order when we compose the two group actions. Let w be a prime of K, and v is a prime of k, we say w is *over* v, or v is *under* w if the restriction of w on k is v. Let $\mathfrak{M}_v \subset \mathfrak{M}_K$ be the set of primes above v, then G naturally acts on $\mathfrak{M}_v$ by $|a|_{\sigma w} = |\sigma^{-1}a|_w$, and this action is transitive. Using Cauchy sequence, we can easily check σ gives a field isomorphism of the completion K_w to $K_{\sigma w}$. The *decomposition group* G_w of w is the subgroup $G_w = \{\sigma : \sigma w = w\}$ of G. Note the $G_{\tau w} = \tau G_w \tau^{-1}$. Let w be a prime over v and $\sigma \in G_w$, we have a field automorphism on K_w preserving k_v, i.e., we have a group homomorphism from G_w to $\mathrm{Gal}(K_w/k_v)$. It can be proved that this homomorphism is actually a group isomorphism.

Note the above definition has a more algebraic interpretation: if we have w is a prime over v, then $\mathfrak{p}_{k_v} = \mathfrak{p}_{K_w} \cap \mathfrak{o}_{k_v}$. The residue field of $k(v) = \mathfrak{o}_{k_v}/\mathfrak{p}_{k_v}$ naturally embeds in the residue field $k(w) = \mathfrak{o}_{K_w}/\mathfrak{p}_{K_w}$, and its degree is called *residue class degree*, denoted by $f(K_w/k_v)$. Let I be a fractional ideal of k_v, we can define the *valuation* of a fractional ideal I as $v(I) = \inf_{x \in I}(-\mathrm{ord}_v(x))$. The *ramification index* is defined as $w(\mathfrak{p}_{k_v}\mathfrak{o}_{K_w})$, denoted by $e(K_w/k_v)$. A prime w over v is called *unramified* if $e(K_w/k_v)$ is 1, and v is called *unramified* if for every $w \in \mathfrak{M}_v$, w over v is unramified. If the extension is Galois, then the ramification indices are equal for every $w \in \mathfrak{M}_v$. Using local field theory, one can prove if K/k if a finite separable field extension of a number field, then a prime v is ramified if and only if $\mathfrak{p}_v \cap \mathfrak{o}_k$ divides the discriminant $\mathfrak{d}$ of K/k. Hence, almost every prime is unramified.

For unramified local field extension, the Galois group $\mathrm{Gal}(K_w/k_v)$ is isomorphic to the Galois group $\mathrm{Gal}(k(w)/k(v))$ of the residue field extension. The later is a finite field extension of a finite field, so the Galois group is cyclic and generated by the Frobenius element $x \mapsto x^{Nv}$, where $Nv = |k(v)|$. Therefore, if v is unramified, and w is over v, we can associate w a special element $\sigma_w \in G_w$ which maps to the Frobenius element under the composition of two group isomorphisms defined above. This element can also be characterized by the property

$$a^{\sigma_w} \equiv a^{Nv} \mod \mathfrak{p}_w$$

for all $a \in \mathfrak{o}_w$. This element σ_w is called *Frobenius automorphism* associated with w. A direct computation shows that $\sigma_{\tau w} = \tau^{-1}\sigma_w\tau$. Hence, we can define $F_{K/k}(v)$ to be the conjugacy class of σ_w for any w over v.

Let S be a finite of primes containing all infinite primes, and define $I^S \subset I_k$ to be the free abelian group on $\mathfrak{M}_k - S$. Assume K/k be an abelian Galois extension, and assume that S contains all ramified primes, then $FK/k(v)$ is well defined for every $v \notin S$ as there is only one element in every conjugacy class. Extend this map linearly, we have a homomorphism $F_{K/k} : I^S \longrightarrow \mathrm{Gal}(K/k)$. If $a \in k^*$, we define $(a)^S = \sum_{v \notin S} \mathrm{ord}_v(a)v$, then there is a constant $\epsilon > 0$ such that if $|a-1|_v < \epsilon$ for all $v \in S$, $F_{K/k}((a)^S) = 1$. This above is the crudest form of Artin's reciprocity law, which we will state the full theorem later.

Motivated by this, we are particularly interested in the following special type of group homomorphism on I^S:

Definition 2.1. Let k be a number field, S is a finite set of primes of k containing all infinite primes, and G is a abelian topological group, a homomorphism $\phi : I^S \longrightarrow G$ is said to be *admissible* if for each neighborhood N of 1 in G, there is a constant $\epsilon > 0$ such that $\phi((a)^S) \in N$ for all $a \in k^*$ with $|a-1|_v < \epsilon$ for all $v \in S$.

Hence, the Artin's reciprocity law in crudest form says $F_{K/k}$ is admissible.

Let J_k be the Idele group of k, we can associate $x \in J_k$ with $(x)^S = \sum_{v \notin S} \mathrm{ord}_v(x_v)v$. We denote $J_k^S \subset J_k$ to be the set of element which have value 1 at all v-th components for $v \in S$.

If $\phi : I^S \longrightarrow G$ is an admissible homomorphism, then there is a unique extension of

$$\psi : J_k^S \longrightarrow G$$

given by $x \mapsto \phi((x)^S)$ to a continuous homomorphism from J_k^S to G with $\psi(k^*) = 1$. Conversely, every continuous homomorphism with $\psi(k^*) = 1$ comes in this way (if the only subgroup of G in a sufficiently small neighborhood of 1 is the trivial subgroup). Hence, we can identify admissible homomorphisms from I^S to G with continuous homomorphism from J_k/k^* to G.

If K/k is an abelian extension, we will call $\psi : J_k \longrightarrow \mathrm{Gal}(K/k)$ satisfying the following three conditions, if exists, the *Artin map* associated with the extension K/k

1. ψ is continuous.

2. $\psi(k^*) = 1$.

3. $\psi(x) = F_{K/k}((x)^S)$ for all $x \in J_k^S$, where S consists of all infinite primes and ramified primes.

We are now ready to state the full version of Artin's reciprocity law, whose proof can be found in Chapter VII in [1, Chapter VII, Section 5]:

Theorem 2.4 (Artin's Reciprocity Law). *1. Given any abelian extension K/k, the Artin map exists.*

2. The Artin map $\psi_{K/k}$ is surjective with kernel $k^* N_{K/k}(J_K)$, where $N_{K/k}$ is the norm map. Hence, the Galois group is isomorphic to $C_k/N_{K/k}C_K$, where $C_k = J_k/k^*$ is the Idele class group.

3. For every open subgroup N of finite index in C_k, therer is a unique abelian extension K/k with $N_{K/k}C_K = N$.

The subgroups N are called *norm* groups, and the abelian extension K such that $N_{K/k}C_K = N$ is called the *class field* belonging to N. The reciprocity law allows us to translate the problems about abelian extensions of the field k to the problems about the group structure of C_k.

We will now see some examples of special class field.

The *Hilbert class field* of a field k is the maximal abelian unramified extension of k. It is the unique class field with norm group the kernel of the homomorphism $C_k \longrightarrow I_k/k^*$. Hence, the Galois group is canonically isomorphic to the ideal class group of k using Frobenius elements for the prime ideals in k. A generalization of the Hilbert class field is the *ray class field*, which is the class field associated with the *ray class group*, which is the quotient of C_k with the norm group defined as follows. Given an ideal $\mathfrak{m}$ in $\mathfrak{o}_k$ and a set S of real places, the norm group associated with $\mathfrak{m}$ and S is the product $\prod W_v$ where W_v is given by:

- k^* if v is a complex infinite prime, or v is real and $v \notin S$.
- k_+ if v is a real infinite prime and $v \in S$.
- All units if v is finite and $\mathfrak{p}_v$ does not divide $\mathfrak{m}\mathfrak{o}_v$.
- Units congruent to 1 mod $\mathfrak{p}_v^n$ if n is the maximal power of $\mathfrak{p}_v$ dividing $\mathfrak{m}\mathfrak{o}_v$.

The ray class field is the maximal abelian extension unramified outside the primes dividing the modulus and satisfying a particular ramification condition at the primes dividing the modulus. The Hilbert class field corresponds to the ray class field with unit ideal and empty set of real places.

For $\mathbb{Q}$, the ray class field associated to the ideal (m) is the cyclotomic extension adjoining m-th roots of unity to $\mathbb{Q}$. The Kronecker-Weber theorem says that every abelian extension of $\mathbb{Q}$ is contained in some cyclotomic field. We have a generalization of this result for ray class field: every abelian extension of k is contained in some ray class field of k.

3 Zeta Function and L-Series

In this section, we are going to discuss the some analytic function associated with the number field, namely, zeta function and L-functions. These function are usually used to prove 'density theorems', and its values at special points usually give algebraic information about the number field.

We start with a continuous homomorphism from $\psi : J_k \longrightarrow S^1 \subset \mathbb{C}$ with $\psi(k^*) = 1$. By continuity, there is a finite set S of primes containing all infinite primes such that $\psi(x) = 1$ if $x_v = 1$ for $v \in S$, and $|x_v|_v = 1$ for $v \notin S$. S is sometimes referred to as the *exceptional* set. Clearly, ψ generates a character of the ideal group I^S by

$$\chi(\mathfrak{a}) = \chi(\sum_v n_v v) = \psi(x^{\mathfrak{a}})$$

where $(x^{\mathfrak{a}})_v$ is 1 if $v \in S$, and $\pi_v^{n_v}$, where π_v is any generator of $\mathfrak{p}_v$. If S and S' are two exceptional sets, and χ, χ' are two characters of I^S and $I^{S'}$, they are called *co-trained* if $\chi(\mathfrak{a}) = \chi'(\mathfrak{a}')$ whenever they are both defined. This is clearly an equivalent definition, and we will call the character with least possible exceptional set the *primitive* character.

For each element $x \in J_k$, we can write $x = \prod_v x(v)$, where $(x(v))_v = x_v$ and $(x(v))_w = 1$ if $w \neq v$, and we define $\psi_v(x) = \psi(x(v))$, and is referred as a *local component* of ψ. By continuity, there exists μ_v a least positive integer such that $\psi_v(1 + \mathfrak{p}_v^{\mu_v}) = 1$ for v finite and in the exceptional set of the primitive character. We will call

$$\mathfrak{f}_\chi = \sum_{v \text{ finite}, v \in S} \mu_v v = \prod_{v \text{ finite}, v \in S} (\mathfrak{p}_v \cap \mathfrak{o})^{\mu_v} \in I_k$$

the *conductor* of the character.

Now let $\mathfrak{m}$ be an ideal such that $\mathfrak{f}_\chi | \mathfrak{m}$. If $\mathfrak{a} = (\alpha)$ where $\alpha \equiv 1(\mathfrak{m})$, then a simple computation shows that

$$\chi(\mathfrak{a}) = \prod_{v \in S_0} \psi_v(\alpha^{-1})$$

where S_0 is the set of infinite primes.

If a character χ with $\psi_v(J_k)$ being discrete subset of S^1 for all $v \in S_0$, then $\psi_v(x) = 1$ if v is complex, and $\psi_v(x) = 1$ or $\psi_v(x) = \begin{cases} 1 & \text{if } x_v > 0 \\ -1 & \text{if } x_v < 0 \end{cases}$ if v is real. If $x_v > 0$ for all real $v \in S_0$, then x is said to be totally positive and we write $x \gg 0$. Thus, if ψ has discrete infinite components, $\chi \equiv 1$ on the subgroup of totally positive principal ideals $\equiv 1(\mathfrak{m})$. Such a character is called a *Dirichlet character modulo* $\mathfrak{m}$, and if $\mathfrak{m} = 1$, χ is called a *Hilbert character.*

Conversely, any character of the ideal group I^S which is 1 on the subgroup of totally positive principal ideals $\equiv 1(\mathfrak{m})$ (where S consists of the archimedean primes and all primes dividing $\mathfrak{m}$) arrises in this way.

Note for $\mathbb{Q}$, we can define a Dirichlet character modulo m to be a character χ satisfying

- $\chi(n+m) = \chi(n)$ for all n.
- If $(n,m) > 1$, then $\chi(n) = 0$, otherwise, $\chi(n) \neq 0$.
- $\chi(n_1 n_2) = \chi(n_1)\chi(n_2)$.

One can easily check that this definition agrees with the our more general definition.

Now let $\mathfrak{a}$ be an integral ideal (one can also think of $\mathfrak{a}$ as an integral element in the ideal group), with absolute norm $N(\mathfrak{a}) = N_{k/\mathbb{Q}}(\mathfrak{a})$. The Dedekind zeta-function $\zeta_j = k(s)$ is defined by

$$\zeta_k(s) = \sum_{\mathfrak{a} \neq 0} \frac{1}{N(\mathfrak{a})^s} = \prod_{\mathfrak{p}} (1 - \frac{1}{N(\mathfrak{p})^s})^{-1}$$

We'll write $s = \sigma + it$, then the infinite sum and product converge for $\sigma > 1$. Complete the zeta function using Γ-functions (associated to infinite primes), and using Merlin transformation of certain θ-functions, one can show that ζ_k is meromorphic on $\mathbb{C}$, having a simple pole only at $s = 1$. If we let

$$\Lambda_s(s) = |\mathfrak{D}_k|^{s/2}\Gamma_{\mathbb{R}}(s)^{r_1}\Gamma_{\mathbb{C}}(s)^{r_2}\zeta_k(s)$$

where $\mathfrak{D}$ is the discriminant of $k/\mathbb{Q}$, r_1 is the number of infinite real primes, and r_2 is the number of infinite complex primes, and

$$\Gamma_{\mathbb{R}}(s) = \pi^{-s/2}\Gamma(s/2)$$

and

$$\Gamma_{\mathbb{C}}(s) = 2(2\pi)^{-s}\Gamma(s)$$

then Λ_k satisfies the functional equation:

$$\Lambda_k(s) = \Lambda_k(1-s)$$

Now if we have a Dirichlet character χ, we can associate a Dirichlet L-seires

$$L(s,\chi) = \sum_{\mathfrak{a}\neq 0}\frac{\chi(\mathfrak{a})}{N(\mathfrak{a})} = \prod_{\mathfrak{p}}(1-\frac{\chi(\mathfrak{p})}{N(\mathfrak{p})^s})^{-1}$$

Clearly, $L(s,\chi)$ is defined for $\sigma > 1$. Almost identical proof as in the case for ζ_k, $L(s,\chi)$ has an analytic continuation to a meromorphic function on $\mathbb{C}$, and if we complete the Dirichlet L-series by

$$\Lambda_{k,\chi}(s) = (|\mathfrak{D}_k|N(\mathfrak{f}_\chi))^{s/2}(\prod_{v \text{ real}}\Gamma_{\mathbb{R}}(s+a_v)^{r_1})\Gamma_{\mathbb{C}}(s)^{r_2}L(s,\chi)$$

where $a_v = 0$ or 1 according as the value of χ in the domain of all principal ideals congruent to 1 mod $\mathfrak{f}_\chi$ does or does not depend on the sign of the v real conjugation, then we have the following functional equation:

$$\Lambda_{k,\chi}(s) = W(\chi)\Lambda_{k,\chi}(1-s,\bar{\chi})$$

where W has absolute value 1, and can be determined explicitly.

If χ is trivial, then we recover the Dedekind zeta-function $\zeta_k(s)$. One can prove that the Dirichlet L-series is actually holomorphic if χ is not trivial. This is closely related to the Artin's conjecture, which asserts analyticity of a more general L-series (which we will define in a moment) on the whole plane $\mathbb{C}$.

In the previous section, we have introduced Artin's reciprocity law. Now let K be an abelian extension of k whose Galois group is canonically identified with I^S/H_S via Frobenius element, where S is the exceptional set, and H_S is identified with kernel of the Artin's map. Then the zeta function for K and k is related by the Dirichlet L-series:

$$\zeta_K(s) = \prod_{\chi} L_k(s, \chi)$$

where χ run through all primitive (Dirichlet) characters co-trained with the characters of the class group I^S/H_S. For unramified primes of k, $\mathfrak{p} = \mathfrak{P}_1 ... \mathfrak{P}_l$ where $\mathfrak{P}_j$'s are distinct primes of K. Then the absolute norm of $\mathfrak{P}_j$ and $\mathfrak{p}$ are related by $N(\mathfrak{P}_j) = N(\mathfrak{p})^f$ where f is the residue class degree defined in earlier. So the local factor are related via

$$\prod_j (1 - N(\mathfrak{P}_j)^{-s})^{-1} = (1 - N(\mathfrak{p})^{fs})^{-n/f}$$

where $lf = [K : k] = n$. Since f is the least positive integer such that $\chi(\mathfrak{p}^f) = 1$ for all χ, we know the righthand side actually equals

$$(1 - N(\mathfrak{p})^{fs})^{-n/f} = \prod_{\chi} (1 - \chi(\mathfrak{p}) N(\mathfrak{p})^{-s})^{-1}$$

which proves the local factors are equal for unramified primes. For ramified primes, the situation is more complicated, but again, their local factors are equal.

Recall if χ is the trivial character, we recover the zeta function of k, so we can rewrite the above equality by

$$\frac{\zeta_K(s)}{\zeta_k(s)} = \prod_{\chi \not\equiv 1} L_k(s, \chi)$$

Since the L-series is entire for $\chi \not\equiv 1$, for abelian extension K/k, the zeta function $\zeta_k | \zeta_K$. We'll see we have a similar result for more general extension if Artin's conjecture is true.

There are a slight generalization of zeta function and Dirichlet L-series. Let K/k be an abelian extension. Let S be a finite set containing all infinite primes, we define the *partial zeta functions* to be

$$\zeta_{K/k,S}(s,\sigma) = \sum_{\mathfrak{n}\in\mathfrak{o}_k,(n,S)=1,F_{K/k}(\mathfrak{n})=\sigma} \frac{1}{N(\mathfrak{n})^s}$$

where $\sigma \in \mathrm{Gal}(K/k)$. We define *relative L-series* with respect to S to be:

$$L_S(s,\chi) = \sum_{(\mathfrak{a},S)=1} \frac{\chi(\mathfrak{a})}{N(\mathfrak{a})} = \prod_{\mathfrak{p}\notin S}(1-\frac{\chi(\mathfrak{p})}{N(\mathfrak{p})^s})^{-1}$$

It can be checked easily that if χ is a character of the Galois group $\mathrm{Gal}(K/k)$, $\chi \circ F_{K/k}$ is a Dirichlet character. We abuse the notation to denote both character as χ, then we have the following equality:

$$L_S(s,\chi) = \sum_{\sigma\in G} \chi(\sigma)\zeta_{K/k,S}(s,\sigma)$$

So far, we have only dealt with one dimensional representations, which are associated to abelian extensions. Now we are going to discuss the L-series in non-abelian case: the Artin L-series.

Let K be a Galois extension of k, with Galois group G. Let ρ be a representation of G, with character χ. Note the representation is uniquely determined by its character. Let $\mathfrak{p}$ be an unramified prime in k, we define the local factor to be the characteristic polynomial $|I - \rho(F_{K/k}(\mathfrak{p}))N(\mathfrak{p})^{-s}|^{-1}$, where $F_{K/k}(\mathfrak{p})$ is the conjugacy class of Frobenius element associated to any $\mathfrak{P}$ over $\mathfrak{p}$. Note this is well defined as the characteristic polynomial is invariant under conjugation. We collect up the local factors corresponding to non-ramified $\mathfrak{p}$ and defined the Atin L-series by

$$L(s,\chi,K/k) = \prod_{\mathfrak{p}\text{ non-ramified}} |I - \rho(F_{K/k}(\mathfrak{p}))N(\mathfrak{p})^{-s}|^{-1}$$

If G is abelian, and assume χ is irreducible, then apart from the factors corresponding to the ramified primes, the definition coincides with the Dirichlet L-series. It can also be checked directly that $L(s,\chi,K/k)$ is holomorphic for $\sigma > 1$ where σ is the real part of s as usual.

Here we list some properties of the Artin's L-series [1, Chapter VIII, Section 3]:

Theorem 3.1. *1. If $\chi = \chi_1 + \chi_2$, then $L(s, \chi, K/k) = L(s, \chi_1, K/k)L(s, \chi_2, K/k)$.*

2. Let Ω is a intermediate field between K and k, Galois over k, then $H = Gal(K/\Omega)$ is a normal subgroup of G, and $G/H = Gal(\Omega/k)$. If χ is a character of G/H, it can be viewed as a character of G, then we have

$$L(s, \chi, K/k) = L(s, \chi, \Omega/k)$$

3. Let Ω is a intermediate field between K and k, not necessarily Galois over k, and $H = Gal(K/\Omega)$ is a subgroup of G. Given a character χ of H, we can associate the induced character $\mathrm{Ind}_H^G \chi$ of G, then we have

$$L(s, Ind_H^G \chi, K/k) = L(s, \chi, K/\Omega)$$

Proof. 1. If we choose a basis, and write $\rho(F_{K/k}(\mathfrak{P}))$ (choose any $\mathfrak{P}$ over $\mathfrak{p}$) in Jordan canonical form, with diagonal entries $d_1, ..., d_n$, then the local factor

$$\begin{aligned}
|I - \rho(F_{K/k}(\mathfrak{p}))N(\mathfrak{p})^{-s}|^{-1} &= \prod_{i=1}^{n}(1 - d_i N(\mathfrak{p})^{-s})^{-1} \\
&= \exp(\sum_{i=1}^{n}\sum_{m=1}^{\infty} \frac{1}{m} d_i^m N(\mathfrak{p})^{-ms}) \\
&= \exp(\sum_{m=1}^{\infty} \frac{1}{m} \chi(F_{K/k}(\mathfrak{P})^m) N(\mathfrak{p})^{-ms})
\end{aligned}$$

The first statement follows from this.

2. Using the characterization of the Frobenius element, i.e. the unique element in G satisfying

$$a^{F_{K/k}(\mathfrak{P})} \equiv a^{N(\mathfrak{p})} (\mathfrak{P}),$$

one can show directly that $F_{\Omega/k}(\mathfrak{P} \cap \Omega) = F_{K/k}(\mathfrak{P})H$. Using this, the local factor satisfies

$$\begin{aligned}
|I - \rho'(F_{K/k}(\mathfrak{p}))N(\mathfrak{p})^{-s}|^{-1} &= |I - \rho(F_{K/k}(\mathfrak{p})H)N(\mathfrak{p})^{-s}|^{-1} \\
&= |I - \rho(F_{\Omega/k}(\mathfrak{p}))N(\mathfrak{p})^{-s}|^{-1}
\end{aligned}$$

The second statement follows from this.

3. Let $\mathfrak{p}$ be an unramified prime in k, decomposes into $\mathfrak{p} = \prod_{i=1}^{r} \mathfrak{q}_i$, with $N(\mathfrak{q}_i) = (N(\mathfrak{p}))^{f_i}$. Choose a prime $\mathfrak{P}$ over $\mathfrak{p}$, to simplify the notation, we will denote $\mu = F_{K/k}(\mathfrak{P})$. Choose $\tau_i \in G$ such that $\mathfrak{q}_i$ lies under $\tau_i\mathfrak{P}$. It can be shown that we have a complete system of representatives for G/H of $\tau_i\mu^j$ where i ranges from 1 to r and j ranges from 0 to $f_i - 1$. By definition of induced representation, we have

$$\begin{aligned}\operatorname{Ind}_H^G \chi(\mu^m) &= \sum_{i=1}^{r} \sum_{j=0,H}^{f_i-1} \chi(\tau_i\mu^j\mu^m\mu^{-j}\tau_i^{-1}) \\ &= \sum_{i=1,H}^{r} f_i\chi(\tau_i\mu^m\tau_i^{-1}) \\ &= \sum_{i=1,f_i|m}^{r} f_i\chi(\tau_i\mu^m\tau_i^{-1})\end{aligned}$$

here H indicates that we only take the sum of the elements which lie in H, and the last equality holds as $\tau_i\mu^m\tau_i^{-1} \in H$ if and only if $f_i|m$. Using this, the logarithm of local factor satisfies

$$\begin{aligned}\sum_{m=1}^{\infty} \frac{1}{m} \operatorname{Ind}_H^G \chi(\mu^m) N(\mathfrak{p})^{-ms} &= \sum_{m=1}^{\infty} \frac{1}{m} N(\mathfrak{p})^{-ms} \sum_{i=1,f_i|m}^{r} f_i\chi(\tau_i\mu^m\tau_i^{-1}) \\ &= \sum_{i=1}^{r} \sum_{m=1,f_i|m}^{\infty} \frac{f_i}{m} \chi(\tau_i\mu^m\tau_i^{-1}) N(\mathfrak{p})^{-ms} \\ &= \sum_{i=1}^{r} \sum_{k=1}^{\infty} \frac{1}{k} \chi((\tau_i\mu^{f_i}\tau_i^{-1})^k) N(\mathfrak{q}_i)^{-ks}\end{aligned}$$

where the last equality follows from substitute $m, f_i|m$ by $m = f_i k$.

Note from the characterization of Frobenius element, we have clearly $\tau_i\mu^{f_i}\tau_i^{-1}$ is the Frobenius element associated to $\mathfrak{P}$ over $\mathfrak{q}_i$ for the extension K/Ω, so the the sum on the right of the above equality is precisely the sum of the logarithm of local components associated to $\mathfrak{q}_i$. The statement three now follows from this.

□

We have the following corollary from the third statement, which is a generalization of a theorem for Dirichlet L-series.

Corollary 3.2. *Let K/k be a Galois extension, then*

- $\zeta_k(s) = L(s, 1, K/k) = L(s, 1, k/k)$
- $\zeta_K(s) = \prod_{i=1}^{n} L(s, \psi_i, K/k)^{\psi_i(1)}$ *where ψ_i ranges over all characters for irreducible representations of G.*

Proof. Note if we choose $\Omega = k$, and by second statement of the previous theorem, we get $\zeta_k(s) = L(s, 1, K/k) = L(s, 1, k/k)$.

For the second equality, we choose $\Omega = K$, then $H = \mathrm{Gal}(K/\Omega) = (1)$. The third statement says $L(s, Ind_{(1)}^{G} 1, K/k) = L(s, 1, K/K)$. From representation theory of finite groups, we have $Ind_{(1)}^{G} 1 = \sum_{i=1}^{n} \psi_i(1)\psi_i$. The equality follows immediately from this and first statement of the previous theorem. □

In representation theory of finite group, we have the following Artin-Brauer theorem, whose proof can be found in [3, Chapter 10, Theorem 19]:

Theorem 3.3. *Every character χ of G can be written with integral coefficients of characters of representation induced from cyclic subgroups, (more precisely, elementary subgroups).*

Using this, we can immediately prove the following theorem [1, Chapter VIII, Theorem 7]:

Theorem 3.4. *For any character χ of G, $L(s, \chi, K/k)$ is given by*

$$L(s, \chi, K/k) = \prod_{l} \prod_{j} L(s, \xi_{l,j}, K/\Omega_l)^{n_{l,j}}$$

where Ω_l run though all intermediate field between K and k with cyclic Galois group $Gal(K/\Omega_l)$, $\xi_{l,j}$ run though all characters of irreducible representation of $Gal(K/\Omega_l)$, and $n_{l,j}$ are some integers.

An immediate consequence of this is that if K/k is a Galois extension and χ is not trivial, the Artin L-series is holomorphic, as it can be represented as a finite product of Dirichlet L-series with non-trivial characters. Artin conjectures this holds for any field extension. A functional equation for the Artin L-series also follows immediately from this.

Similarly, we can define *relative Artin L-series* with respect to S, a finite set of primes containing all infinite primes and all ramified primes, as

$$L_S(s,\chi,K/k)=\prod_{\mathfrak{p}\notin S}|I-\rho(F_{K/k}(\mathfrak{p}))N(\mathfrak{p})^{-s}|^{-1}$$

The relative Artin L-series satisfies all the properties we listed earlier, as the the proof only considers the local components.

4 Stark's Conjecture

The Stark's conjecture concerns the derivatives of the Artin's L-series at point $s=0$. This serves as a generalization of the well-known Dirichlet class number theorem for Dedekind zeta functions.

Let k be a number field, denote r_1 and r_2 be the number of infinite real and complex primes respectively. Note $[k:\mathbb{Q}]=r_1+2r_2$. Let h_k is the class number as defined in section 2; e_k is the number of roots of unity in k, which we have shown to be finite in section 2; $\mathfrak{D}_k$ is the discriminant of the field extension $k/\mathbb{Q}$. We can define the *regulator* which measures the density of the units as follows:

Definition 4.1. Let $u_1,...,u_r$ be a set of generators for unit group modulo roots of unity, and $v_1,...,v_{r+1}$ be infinite real and complex primes. We can construct an r by $r+1$ matrix with ij-th entry being $\log|u_i|_{v_j}$ where $|\cdot|_{v_j}$ is the normalized valuation associated to v_j. The *regulator* R_k of k is (any) $r\times r$ minor.

More generally, if S is a finite set of primes containing all infinite primes, let $u_1,...,u_r$ be a set of generators for S-unit group modulo roots of unity, and $v_1,...,v_{r+1}$ be primes in S. The *relative regulator* R_S is (any) $r\times r$ minor of the matrix $(\log|u_i|_{v_j})_{ij}$.

We are now able to state the Dirichlet class number formula:

Theorem 4.1. *ζ_k has a simple pole at $s=1$, with residue*

$$\frac{2^{r_1}(2\pi)^{r_2}h_kR_k}{e_k\sqrt{|\mathfrak{D}_k|}}$$

Using the functional equation for Dedekind zeta function, we can relate the poles at $s = 1$ with the zeros at $s = 0$. We immediately get the following Dirichlet class number formula at $s = 0$:

Theorem 4.2. *ζ_k has a zero of order $r = r_1 + r_2 - 1$ at $s = 0$, with first non-zero coefficient in Taylor series expansion at 0*

$$-\frac{h_k R_k}{e_k}$$

Note that the form of Dirichlet class number formula is much clearer at $s = 0$.

Recall in section 3, we defined the partial zeta function with respect to a field extension K/k, a finite set of primes containing all infinite primes S, and a element $\sigma \in G$:

$$\zeta_{K/k,S}(s,\sigma) = \sum_{\mathfrak{n} \in \mathfrak{o}_k, (n,S)=1, F_{K/k}(\mathfrak{n})=\sigma} \frac{1}{N(\mathfrak{n})^s}$$

Indeed, we also have the Dirichlet class number formula for partial zeta function of field extension k/k with little modification:

Theorem 4.3. *Let $r = |S| - 1$, then the partial zeta function $\zeta_{k/k,S}(s,1)$ has a zero of order r at $s = 0$, with first non-zero coefficient in Taylor series expansion at 0*

$$-\frac{h_S R_S}{e_k}$$

where h_S is the relative class number, and R_S is the relative regulator.

The Stark's conjecture aim to generalize the above formula for arbitrary L-function. Let $L_S(s,\chi,K/k)$ be an Artin L-series, we define the *rank* to be the degree of the first non-zero term in the Laurent expansion of $L_S(s,\chi,K/k)$ at $s = 0$, and denoted as $r_S(\chi,K/k)$. We will drop some or all parameters if there is no confusion in the situation. To start with, we would like to get a formula for $r_S(\chi,K/k)$.

We will start with one dimensional representation [2]:

Lemma 4.4. *If χ is a 1-dimensional character of G of a Galois extension K/k, then*

$$r_S(\chi,K/k) = \sum_{v \in S} \dim V^{G_v} - \dim V^G = \begin{cases} |S| - 1, & \text{if } \chi = 1 \\ |\{\mathfrak{p} \in S : \chi(G_v) = 1\}|, & \text{otherwise} \end{cases}$$

where V is the 1*-dimensional representation of* χ*, and* $V^H = \{v \in V : v^\sigma = v \text{ for all } \sigma \in H\}$*.*

Proof. The second equality is an easy computation using representation theory, hence, we only need to show $r_S(\chi, K/k)$ equals the right most expression.

If $\chi = 1$, then this is the first part of Dirichlet class number formula. If $\chi \neq 1$, it can be shown using functional equation for L-series that the full L-series has a zero of order $|\{v \text{ prime or ramified} : \chi(G_v) = 1\}|$. Start from this, we note that

$$L_S(s, \chi, K/k) = \prod_{v \in S, \text{ finite, unramified}} |I - \rho(F_{K/k}(v))N(v)^{-s}| L(s, \chi, K/k)$$

Hence, the order of zero increase by 1 exactly at those primes with $\chi(G_{\mathfrak{p}}) = 1$, and the result follows. □

Let S_K be the set of primes of K over primes in S_k, and denote Y to be the free abelian group with generators S_K, and let

$$X = \{\sum_{w \in S_K} n_w w \in Y : \sum_{w \in S_K} n_w = 0\}$$

Note we have a short exact sequence as G-modules:

$$0 \longrightarrow X \longrightarrow Y \longrightarrow \mathbb{Z} \longrightarrow 0$$

If we let χ_X and χ_Y be the characters of representation $\mathbb{C}X$ and $\mathbb{C}Y$ of G respectively, $\chi_X = \chi_Y - 1$. We also clearly have $\chi_Y = \sum_{v \in S} \operatorname{Ind}_{G_w}^G 1_{G_w}$

Using this, and Artin-Brauer theory, we can prove the general case [2]:

Theorem 4.5. *If χ is the character of a representation V, then*

$$r_S(\chi, K/k) = \sum_{v \in S} \dim V^{G_v} - \dim V^G = \langle \chi, \chi_X \rangle = \dim_{\mathbb{C}} \operatorname{Hom}_G(V^*, \mathbb{C}X)$$

Proof. Note $\mathrm{Hom}_{\mathbb{C}}(V^*, \mathbb{C}X) = V^* * \otimes_{\mathbb{C}} \mathbb{C}X$, so by orthogonality of the characters, we have

$$\begin{aligned}\dim_C \mathrm{Hom}_{\mathbb{C}}(V^*, \mathbb{C}X) &= \dim_{\mathbb{C}}(V) \times \dim_{\mathbb{C}} \mathbb{C}X \\ &= \langle \chi \cdot \chi_X, 1\rangle \\ &= \langle \chi, \overline{\chi_X}\rangle \\ &= \langle \chi, \chi_X\rangle\end{aligned}$$

as $\chi_X = \overline{\chi_X}$. So the last equality follows.

For the second equality, we note

$$\begin{aligned}\langle \chi, \chi_X\rangle &= \sum_{v\in S}\langle \chi, \mathrm{Ind}_{G_v}^G 1_{G_v}\rangle_G - \langle \chi, 1_G\rangle_G \\ &= \sum_{v\in S}\langle \mathrm{Res}_{G_v} \chi, 1_{G_v}\rangle_{G_v} - \langle \chi, 1_G\rangle_G \\ &= \sum_{v\in S} \dim V^{G_v} - \dim V^G\end{aligned}$$

where we used the Frobenius reciprocity theorem.

Hence, it remains to prove $r_S(\chi, K/k)$ equals any of them. Using Artin-Brauer theory,

$$\chi = \sum_\theta n_\theta \mathrm{Ind}_{H_\theta}^G \theta$$

where θ is 1-dimensional representation of some cyclic subgroup H_θ of G. As show in section 3, the L-series can be written as a product of L-series associated to representations θ, and

$$\langle \chi, \chi_X\rangle = \langle \sum_\theta n_\theta \mathrm{Ind}_{H_\theta}^G \theta, \chi_X\rangle_G = \sum_\theta n_\theta \langle \theta, \mathrm{Res}\, \chi_X\rangle_{H_\theta}$$

so it is enough to prove the equality for 1-dimensional representations, which follows from the previous lemma. □

Now we want to introduce a new type of regulator attached to a character χ. Let S_K

defined as above, and let U denote the S_K-units in K, and we consider the the following map

$$\begin{aligned} \lambda : U &\longrightarrow \mathbb{R}X \\ u &\mapsto \sum_{w \in S_K} \log |u|_w w \end{aligned}$$

An easy application of the Unit theorem in section 2, we see λ induces an isomorphism (we still call it λ) $\mathbb{R}U \xrightarrow{\sim} \mathbb{R}X$ and $\mathbb{C}U \xrightarrow{\sim} \mathbb{C}X$. Since the characters take value in $\mathbb{Q}$, they are isomorphic as $\mathbb{Q}[G]$-modules. Let

$$f : \mathbb{Q}X \xrightarrow{\sim} \mathbb{Q}U$$

be an isomorphism, and use the same symbol f to denote the complexification of the isomorphism. Composing λ, we get an automorphism

$$\lambda \circ f : \mathbb{C}X \xrightarrow{\sim} \mathbb{C}X$$

which induces an automorphism

$$(\lambda \circ f)_V : \mathrm{Hom}_G(V^*, \mathbb{C}X) \xrightarrow{\sim} \mathrm{Hom}_G(V^*, \mathbb{C}X)$$

Recall from the previous computation of the rank, $\dim_{\mathbb{C}} \mathrm{Hom}_G(V^*, \mathbb{C}X)$ is exactly equal to $r_S(\chi, K/k)$.

We define the *Stark's regulator* associated to f and χ to be

$$R(\chi, f) = \det((\lambda \circ f)_V)$$

We are now able to state the Stark's conjecture:

Conjecture 4.6 (Stark's Conjecture)**.** *Let $c(\chi)$ be the first non-zero coefficient in Artin's L-series at $s = 0$, and let $A(\chi, f) = \frac{R(\chi,f)}{c(\chi)} \in \mathbb{C}$, then for any automorphism σ of $\mathbb{C}$,*

$$A(\chi, f)^\sigma = A(\chi^\sigma, f)$$

where $\chi^\sigma = \sigma \circ \chi : G \longrightarrow \mathbb{C}$.

It is clear that the conjecture is equivalent to the following two statement:

- $A(\chi, f) \in \mathbb{Q}(\chi)$
- $A(\chi, f)^\sigma = A(\chi^\sigma, f)$ for all $\sigma \in \mathrm{Gal}(\mathbb{Q}(\chi)/\mathbb{Q})$

Here $\mathbb{Q}(\chi) = \mathbb{Q}(\chi(g) : g \in G)$.

There is another formulation of the Stark's conjecture due to Deligne. Suppose E is a field of characteristic 0 and $\chi : G \to E$ be the character of the representation, and $\sigma \in \mathrm{Hom}_{\mathbb{Q}}(E, \mathbb{C})$, we can define the character $\chi^\sigma = \sigma \circ \chi$ of G and its realization as a complex representation: $V^\sigma = V \otimes_{E,\sigma} \mathbb{C}$. Moreover, if $f : X \to EU$ is some G-homomorphism which induces an isomorphism of $f^\sigma = (\sigma \otimes 1) \circ f : \mathbb{C}X \to \mathbb{C}U$, we can similarly construct an automorphism $(\lambda \circ f^\sigma)_{V^\sigma}$ of $\mathrm{Hom}_G((V^\sigma)^*, \mathbb{C}X)$. We define $R(\chi^\sigma, f^\sigma) = \det((\lambda \circ f^\sigma)_{V^\sigma})$. We are now stating the second formulation of Stark's conjecture:

Conjecture 4.7 (Stark's Conjecture (Second Formulation))**.** *Let E be a field containing $\mathbb{Q}(\chi)$, then there exists an element $A(\chi, f) \in E$ such that for any $\sigma \in \mathrm{Hom}_{\mathbb{Q}}(E, \mathbb{C})$ we have,*

$$R(\chi^\sigma, f^\sigma) = A(\chi, f)^\sigma \cdot c(\chi^\sigma)$$

Note if we let $E = \mathbb{C}$, and $f : \mathbb{Q}X \to \mathbb{Q}U$ is an isomorphism, then $f^\sigma = f$ for any automorphism of $\mathbb{C}$. Hence, the conjecture 4.6 follows directly from conjecture 4.7.

It turns out that the converse is also true: i.e. conjecture 4.6 also implies conjecture 4.7, and the conjecture does not depend on the choice of the isomorphism f.

The relationship between the Stark's conjecture and the Dirichlet class number formula will become more apparent in the case of rank 1, which we will discuss in more details in the next section.

5 Rank 1 Stark's Conjecture

Let χ be a irreducible character with $r(\chi) = 1$. Let $E = \mathbb{Q}(\chi)$, then χ can be realized as the character of a representation over E. We define $\psi = \sum_{\sigma \in \mathrm{Gal}(\mathbb{Q}(\chi)/\mathbb{Q})}$, then ψ can be realized over $\mathbb{Q}$, and let W be its realization, i.e., W is a $\mathbb{Q}[G]$-module with character ψ. Also denote X_W and U_W be the unique $\mathbb{Q}[G]$-submodule of $\mathbb{Q}X$ and $\mathbb{Q}U$ which are isomorphic to W (where

X and U are defined as earlier). We will now state an equivalent version of Stark's conjecture for rank 1 explicitly using $\mathbb{Q}$ subspace $\lambda(U_V)$ of $\mathbb{C}X$ and the value of $L'_S(0, \chi^\sigma, K/k)$.

Associate to χ, we have a idempotent central element of $\mathbb{C}[G]$

$$e_\chi = \frac{\chi(1)}{|G|} \sum_{\sigma \in G} \chi(\sigma^{-1})\sigma$$

This element acts as the projection to the χ-component in the canonical decomposition as a $\mathbb{C}[G]$ module.

Denote $\Gamma = \mathrm{Gal}(E/\mathbb{Q})$, we also define

$$\pi(a, \chi) = \sum_{\alpha \in \Gamma} a^\alpha L'_S(0, \chi^\alpha, K/k) e_{\bar{\chi}^\alpha} \in \mathbb{C}[G]$$

for $a \in E$.

Let ψ be a character of G, such that $r(\psi) \neq 1$, then $\pi(a, \psi)\mathbb{Q}X = 0$ as $L'_S(0, \psi^\alpha, K/k) = 0$ if $r(\psi) > 1$, $e_{\bar{\psi}^\alpha}\mathbb{Q}X = 0$ if $r(\psi) = 0$, since $\mathbb{Q}X$ contains no sub-representation of χ, as $0 = r(\psi) = \langle \chi_X, \psi \rangle$.

We now state the equivalent version of Stark's conjecture:

Proposition 5.1. *Let $a \in E^*$, and χ is a character of G with $r(\chi) = 1$, then the following assertions are equivalent:*

1. $\pi(a, \chi)\mathbb{Q}X \cap \lambda(\mathbb{Q}U) \neq \{0\}$
2. $\pi(a, \chi)\mathbb{Q}X = \lambda U_W$
3. *Stark's conjecture is true.*

The proof of the proposition can be found in [2]. With the above proposition, we can reformulate Stark's conjecture by introducing the Stark's unit. Let ψ be a finite set of irreducible characters such

- $1_G \notin \psi$.
- $\forall \chi \in \psi$, $\forall \alpha \in \mathrm{Aut}\,\mathbb{C}$, $\chi^\alpha \in \psi$.
- $\forall \chi \in \psi$, $r(\chi) = 1$.

Note that this is consistent with $\psi = \sum_{\sigma \in \mathrm{Gal}(\mathbb{Q}(\chi)/\mathbb{Q})}$ by viewing ψ as a collection of irreducible representations. By previous proposition, if the Stark's conjecture is true,

$$(\sum_{\chi \in \psi} a_\chi L'_S(0, \chi, K/k) e_{\bar{\chi}}).X \subset \mathbb{Q}\lambda(U)$$

for all family $(a_\chi)_{\chi \in \psi} \in \mathbb{C}$ such that $a_{\chi^\alpha} = (a_\chi)^\alpha$.

Since $1_G \notin \psi$, we can replace X by Y. So the above inclusion can be rephrased as fro all prime $v \in S$, and prime w above v, there is a positive integer m and an S-unit ϵ of K such that

$$m \sum_{\chi \in \psi} a_\chi L'_S(0, \chi, K/k) e_{\bar{\chi}} w = \lambda(\epsilon)$$

The unit ϵ is called the *Stark's unit.* It's easy to check that once m is fixed, ϵ is well defined up to roots of unity. Now substituting the definition of λ and e_χ, we have the following

- $|\epsilon|_w = 1$, if $w \nmid v$,
- $\log|\epsilon|_{\sigma w} = \log|\epsilon^{\sigma^{-1}}|_w = \frac{m}{|G|} \sum_{\chi \in \psi} a_\chi L'_S(0, \chi, K/k) \chi(1) \sum_{\tau \in G_w} \chi(\sigma\tau)$, if $w \mid v$

Conversely, if $\log|\epsilon^{\sigma^{-1}}|_w = \frac{m}{|G|} \sum_{\chi \in \psi} a_\chi L'_S(0, \chi, K/k) \chi(1) \sum_{\tau \in G_w} \chi(\sigma\tau)$ for some w over v and positive integer m, then $\pi(a, \chi)\mathbb{Q}X \cap \lambda(\mathbb{Q}U) \neq \{0\}$. So it follows that Stark's conjecture is equivalent to the existence of Stark's unit some $w \mid v$.

Note this formula states that the derivative of Artin's L-series can be written as a linear combination of valuations of the Stark unit ϵ.

Let S be a finite set of primes such that

- S contains all finite primes and ramified primes.
- S contains at least 1 completely splitting prime v.
- $|S| \geqslant 2$.

Assume that χ is 1-dimensional, and $r(\chi) = 1$, then the Stark's conjecture in this case is equivalent as saying there exists positive integer m and a Stark's unit ϵ such that

$$\log|\epsilon^{\sigma^{-1}}|_w = \frac{m}{|G|} \sum_{\chi \in \psi} L'_S(0, \chi, K/k) \chi(\sigma)$$

In the case of abelian extension K/k, Stark made a refined conjecture by asserting that m to be the number of roots of unity e_K in K, and $K(\epsilon^{1/e_K})/k$ being an abelian extension.

Fix a completely splitting prime $v \in S$, and w over v. Define $U^v = \{u \in U_{S_K} : |u|_{w'} = 1 \text{ for all } w \nmid v\}$ if $|S| \geqslant 3$, and $U^v = \{u \in U_{S_K} : |u|_{w'} = |u|_{\sigma u} \text{ for all } \sigma \in G\}$ if $S = \{v, v'\}$ and w' is over v', and $U^{\mathrm{ab}}_{K/k} = \{u \in U_{S_K} : K(u^{1/e_K}) \text{ is an abelian extension of } k\}$.

Conjecture 5.2 (Refined Abelian Stark's Conjecture)**.** *Suppose S satisfies the above three conditions, and v, w as above, then there exists a unit $\epsilon \in U^{\mathrm{ab}}_{K/k} \cap U^v$ such that*

$$\log |\epsilon^\sigma|_w = -e\zeta'_{k,S}(0, \sigma)$$

for all $\sigma \in G$. Or equivalently,

$$L'_S(0, \chi, K/k) = -\frac{1}{e} \sum_{\sigma} \chi(\sigma) \log |\epsilon^\sigma|_w$$

for all $\chi \in \hat{G}$, where $e = e_K$ is the number of roots of unity in K.

The equivalence between the two statements can be easily checked using the equation relating partial zeta function and L-series. It can be verified that the truth of the conjecture does not depend on the choice of completely splitting prime v. Hence, for convenience, we will use $\mathrm{St}(K/k, S)$ to denote the refined abelian Stark's conjecture for abelian field extension K/k and exceptional set S.

We are now going to prove some special cases when the conjecture $\mathrm{St}(K/k, S)$ is true [2]:

Theorem 5.3. *If S contains at least 2 completely splitting primes, then $\mathrm{St}(K/k, S)$ is true.*

Proof. If $|S| \geqslant 3$, by Lemma 4.4, $r(\chi) \geqslant 2$ for all $\chi \in \hat{G}$, so $L'_S(0, \chi, K/k) = 0$ for all χ. We may choose $\epsilon = 1$, and $\mathrm{St}(K/k, S)$ is true.

If $S = \{v, v'\}$ be a set of two completely splitting primes, by Dirichlet class number formula, we know

$$L'_S(0, 1_G, K/k) = \zeta'_S(0, k) = -\frac{h_S R_S}{e_k}$$

where $R_S = \log |\eta|_v$ for some S-unit η with $|\eta|_v > 1$. Let $m = \frac{e_K}{e_k} \cdot \frac{h_S}{[K:k]}$. Note that m is an integer as $e_k \mid e_K$, and $[K : k] \mid h_S$ because the Galois group $\mathrm{Gal} K/k$ is a quotient group of the S-ideal class group I^S/k^*. Let $\epsilon = \eta^m$, then clearly, $\epsilon \in U^v$. Moreover, $K(\epsilon^{1/e_K})$ is a subfield of $K(\eta^{1/e_k})$ which is abelian over k by Kummer theory. Hence

$$\epsilon \in U^{\mathrm{ab}}_{K/k} \cap U^v$$

Moreover,

$$\begin{aligned} L'_S(0, 1_G, K/k) &= -\frac{h_S R_S}{e_k} \\ &= -\frac{[K:k]}{e_K} \log|\epsilon|_w \\ &= -\frac{1}{e_K} \sum_{\sigma \in G} 1_G(\sigma) \log|\epsilon^\sigma|_w \end{aligned}$$

and

$$\begin{aligned} L'_S(0, \chi, K/k) = 0 &= -\frac{\log|\epsilon|_w}{e_K} \langle \chi, 1_G \rangle \\ &= -\frac{\log|\epsilon|_w}{e_K} \sum_{\sigma \in G} \chi(\sigma) \\ &= -\frac{1}{e_K} \sum_{\sigma \in G} \chi(\sigma) \log|\epsilon^\sigma|_w \end{aligned}$$

if $\chi \neq 1_G$ and χ is irreducible. Note that the first equality holds as $r(\chi) = 2$ if $\chi \neq 1_G$ by Lemma 4.4.

Hence, we proved $\mathrm{St}(K/k, S)$ in this case. □

We immediately get the following two corollaries as we assume S containing all infinite primes and $|S| \geqslant 2$:

Corollary 5.4. *The conjecture* $\mathrm{St}(k/k, S)$ *is true.*

Corollary 5.5. *If k has at least two complex infinite primes, then* $\mathrm{St}(K/k, S)$ *is true for any abelian extension K/k.*

Note that Corollary 5.4 is essentially Dirichlet class number formula.

Theorem 5.6. *If* $\mathrm{St}(K/k, S)$ *is true, then* $\mathrm{St}(K/k, S')$ *is true for all* $S' \supseteq S$.

Proof. If S satisfying the three conditions for the conjecture, then S' clearly also satisfies the three conditions. We can prove by induction on the size $|S' - S|$, so it is suffice to prove the case when $S' = S \cup \{\mathfrak{p}\}$. Note that $\mathfrak{p}$ must be unramified finite prime, so we let $\sigma_{\mathfrak{p}}$ to be the Frobenius element associated to the prime $\mathfrak{p}$. Let ϵ be the Stark unit for $\mathrm{St}(K/k, S)$, define $\epsilon' = \epsilon^{1-\sigma_{\mathfrak{p}}^{-1}} = \frac{\epsilon}{\sigma_{\mathfrak{p}}^{-1}(\epsilon)}$. It's easy to verify that $\epsilon' \in U^{\mathrm{ab}}_{K/k} \cap U^v$. Moreover,

$$\begin{aligned}
L'_{S'}(0, \chi, K/k) &= (1 - \chi(\sigma_{\mathfrak{p}}))L'_S(0, \chi, K/k) \\
&= -\frac{1 - \chi(\sigma_{\mathfrak{p}})}{e_K} \sum_{\sigma \in G} \chi(\sigma) \log |\epsilon^\sigma|_w \\
&= -\frac{1}{e_K} \sum_{\sigma \in G} \chi(\sigma) \log |\epsilon^\sigma|_w + \frac{\chi(\sigma_{\mathfrak{p}})}{e_K} \sum_{\sigma \in G} \chi(\sigma) \log |\epsilon^\sigma|_w \\
&= -\frac{1}{e_K} \sum_{\sigma \in G} \chi(\sigma) \log |\frac{\epsilon^\sigma}{\epsilon^{\sigma\sigma_{\mathfrak{p}}^{-1}}}|_w \\
&= -\frac{1}{e_K} \sum_{\sigma \in G} \chi(\sigma) \log |\epsilon'^\sigma|_w
\end{aligned}$$

Hence, we have proved the assertion. □

Theorem 5.7. *If* $\mathrm{St}(K/k, S)$ *is true, then* $\mathrm{St}(\Omega/k, S)$ *is true for all intermediate field* Ω.

Proof. Let ϵ be the Stark's unit for $\mathrm{St}(K/k, S)$. We will assume that there exists $\epsilon_\Omega \in U^{\mathrm{ab}}_{\Omega/k}$ such that

$$\epsilon_\Omega^{e_K/e_\Omega} = \zeta N_{K/\Omega}\epsilon$$

where ζ is some roots of unity in Ω. Note that $\epsilon_\Omega \in U^{\mathrm{ab}}_{\Omega/k} \cap U^v$, and we will show this is the Stark's unit for $\mathrm{St}(\Omega/k, S')$.

Let $G = \mathrm{Gal}(K/k)$, $H = \mathrm{Gal}(K/\Omega)$ so $G/H = \mathrm{Gal}(\Omega/k)$. Let χ be a character of G/H, it can be viewed naturally as a character of G which we will still denote as χ. By the property of L-series proved in section 3, we have

$$\begin{aligned} L'_S(0,\chi,\Omega/k) &= L'_S(0,\chi,K/k) \\ &= -\frac{1}{e_K}\sum_{\sigma\in G}\chi(\sigma)\log|\epsilon^{\sigma}|_w \\ &= -\frac{1}{e_K}\sum_{\sigma\in G/H}\chi(\sigma)\sum_{\tau\in H}\log|\epsilon^{\sigma\tau}|_w \\ &= -\frac{1}{e_K}\sum_{\sigma\in G/H}\chi(\sigma)\log|(N_{K/\Omega}\epsilon)^{\sigma}|_{w'} \\ &= -\frac{1}{e_\Omega}\sum_{\sigma\in G/H}\chi(\sigma)\log|\epsilon_\Omega^{\sigma}|_{w'} \end{aligned}$$

which proves the assertion. □

If $e_\Omega = e_K$, we may simply pose $\epsilon_\Omega = N_{K/\Omega}\epsilon$ to be the Stark's unit for $\mathrm{St}(\Omega/k,S)$. In particular, if the prime v which splits completely is real infinite, then $e_K = e_\Omega = 2$ (as ± 1 are the only roots of unity). In this case, the Stark's unit

$$\epsilon = \exp(-2\zeta'_{k,S}(0,1))$$

is an algebraic number generated by a transcendental function (here $1 \in G$ is the identity). Moreover, the field $K(\epsilon)$ is an abelian extension of k. Finding such a generator of an abelian extension of a number field is closely related to the Hilbert's 12-th question, and Stark's conjecture provides an important contribution to this problem.

The Stark's conjecture still remains open after 40 years when Stark made the first conjecture. There are only two cases the conjecture is entirely proved, when the base field is $\mathbb{Q}$ or a quadratic imaginary field. We will discuss these two cases in the next few sections.

6 Stark's Conjecture for Abelian Extension of $\mathbb{Q}$

In this section, we will compute the Stark's unit for $\mathrm{St}(K/\mathbb{Q},S)$. We will use the powerful theorem of Kronecker and Weber [1, Chapter III] to reduce the problem to calculating the

Stark's unit for cyclotomic extensions of $\mathbb{Q}$.

Theorem 6.1 (Kronecker-Weber Theorem)**.** *Any abelian extension $K/\mathbb{Q}$ is contained in some cyclotomic extension $\mathbb{Q}(\zeta_n)$.*

Using Theorem 5.7 from the last section, we only need to prove the conjecture for cyclotomic extensions.

For simplicity of demonstration, we will only consider the case of totally real extension of $\mathbb{Q}$. Let ζ_m be a primitive m-th roots of unity in $\mathbb{C}$, let $K = \mathbb{Q}(\zeta_m)^+$ be the maximal real subgroup of $\mathbb{Q}(\zeta_m)$, and $S = \{\infty, p : p \mid m\}$, and $v = \infty$ be the completely splitting infinite prime. The group $G = \mathrm{Gal}(K/\mathbb{Q})$ is canonically isomorphic to $(\mathbb{Z}/m\mathbb{Z})^*/\{\pm 1\}$. Let $\sigma_a \in G$ be the restriction to K of the automorphism on $\mathbb{Q}(\zeta_m)$, $\zeta \mapsto \zeta^a$. Note that $\sigma_a = \sigma_{-a}$. We can write the partial zeta function with respect to σ_a as

$$\zeta_{K/\mathbb{Q},S}(s,\sigma_a) = \sum_{n \equiv \pm a\,(m), n>0} n^{-s} = \sum_{n \equiv a\,(m)} |n|^{-s}$$

Let $\zeta_H(s,x) := \sum_{n=0}^{\infty} \frac{1}{(x+n)^s}$ be the Hurwitz zeta function. It can be checked directly that

$$\zeta_{K/\mathbb{Q},S}(s,\sigma_a) = m^{-s}(\zeta_H(s,\frac{a}{m}) + \zeta_H(s, 1-\frac{a}{m}))$$

Using the classical identity

$$\frac{\partial}{\partial s}\zeta_H(s,x)|_{s=0} = \log\Gamma(x) - \frac{1}{2}\log(2\pi),$$

we can compute the derivative of the partial zeta function:

$$\begin{aligned}\zeta'_{K/\mathbb{Q},S}(0,\sigma_a) &= \log\frac{\Gamma(\frac{a}{m})\Gamma(1-\frac{a}{m})}{2\pi} \\ &= -\log(2\sin(\frac{a\pi}{m})) \\ &= -\frac{1}{2}\log(2-2\cos(\frac{2a\pi}{m}))\end{aligned}$$

Now we define the Stark's unit $\epsilon := (1-\zeta_m)(1-\zeta_m^{-1}) = 2 - 2\cos(\frac{2\pi}{m}) \in K$, then it is well-known that ϵ is a unit of K if $|S| \geqslant 3$, and it is a S-unit if $|S| = 2$. Note that

$\epsilon^{\sigma_a} = (1-\zeta_m^a)(1-\zeta_m^{-a}) = 2 - 2\cos(\frac{2a\pi}{m})$, so we have

$$\zeta'_{K/\mathbb{Q},S}(0,\sigma_a) = -\frac{1}{2}\log\epsilon^{\sigma_a} = -\frac{1}{e}\log|\epsilon^{\sigma_a}|$$

Hence, to prove the refined abelian Stark's conjecture for $\mathbb{Q}$, we only need to show $K(\epsilon^{1/2})$ is an abelian extension of $\mathbb{Q}$. Note that

$$\epsilon = 2 - \zeta_m - \zeta_m^{-1} = (\zeta_4(\zeta_{2m} - \zeta_{2m}^{-1}))^2$$

so $K(\sqrt{\epsilon}) \subset \mathbb{Q}(\zeta_{4m})$ is abelian. This proves the Stark's conjecture for abelian extension of $\mathbb{Q}$.

7 Stark's Conjecture for Abelian Extension of Quadratic Imaginary Field

For abelian extension of rational numbers $\mathbb{Q}$, Kronecker-Weber theorem tells us that it is enough to study cyclotomic extensions. For quadratic imaginary field, complex multiplication does essentially the same.

Let E be an elliptic curve over $\mathbb{C}$. We will write it in Weierstrass normal form: $y^2 = 4x^3 - g_2x - g_3$. We know that as a complex manifold, $E = \mathbb{C}/\Gamma$, where Γ is a lattice in $\mathbb{C}$. An endomorphism of E can be viewed as an element $z \in \mathbb{C}$ such that $z\Gamma \subset \Gamma$. Generically, $\mathrm{End}(E) = \mathbb{Z}$, but there are some special curves with larger endomorphism. If this is the case, $\mathrm{End}(E) \otimes \mathbb{Q}$ must be some quadratic imaginary field k, and we will call the elliptic curve to have *complex multiplication.* Note $\mathrm{End}(E)$ must be a subring of finite index (sometimes called an *order*) of the ring of integers $\mathfrak{o}_k$. Such ring are of the form $\mathbb{Z} + f\mathfrak{o}_k$ where f is some positive integer, called the *conductor.* Hence, if E has complex multiplication, there is a quadratic imaginary field k and a positive integer f associated to it. Conversely, every order of a quadratic imaginary field corresponds to the endomorphism ring of some elliptic curve. In fact, according to Chapter XIII of [1, Chapter XIII], we have:

Lemma 7.1. *The elliptic curves with a given endomorphism ring $R_f = \mathbb{Z} + fR$ (where R is the ring of integers of some quadratic imaginary field k) correspond one-to-one with the class group* $\mathrm{Cl}(R_f)$.

Note that R_f may not be a Dedekind domain, we need to consider *proper fractional ideals*, i.e. fractional ideal $\mathfrak{a} \subset R_f$ such that $\{\beta \in k : \beta_{\mathfrak{a}} \subset \mathfrak{a}\} = R_F$, and the class group $\mathrm{Cl}(R_f)$ is defined to be the proper fractional ideals quotient principal proper fractional ideals.

Proof. Let E be an elliptic curve, then $E = \mathbb{C}/\Gamma$, where Γ is a lattice in $\mathbb{C}$. We can view Γ as a fractional ideal $\mathfrak{a}$ of $\mathbb{R}_f$. Note that $\mathbb{R}_f = \mathrm{End}(\mathbb{C}/\mathfrak{a})$, so Γ is a proper fractional ideal.

If $\mathfrak{a}'$ is another proper fractional ideal, then $\mathbb{C}/\mathfrak{a} \cong \mathbb{C}/\mathfrak{a}'$ if and only if $\mathfrak{a} = a\mathfrak{a}'$ for some $a \in k*$. Hence, $\mathfrak{a}$ and $\mathfrak{a}'$ are same as ideal class.

Conversely, if $\mathfrak{a}$ is a proper fractional ideal, then define $E = \mathbb{C}/\mathfrak{a}$ is the elliptic curve corresponding to $[\mathfrak{a}]$. □

The j-invariant or j-function is the *modular function* (of weight zero), i.e., a holomorphic function on upper half plane $\mathbb{H}$ which is invariant under $\mathrm{SL}(2, \mathbb{Z})$ action, normalized to

$$j(\exp(\frac{2}{3}\pi i) = 0, \ j(i) = 1728.$$

For a elliptic curve $E = \mathbb{C}/\Gamma$, we can normalize the lattice so that $\Gamma \cap \mathbb{R} = \mathbb{Z}$, we define $j(E) := j(a)$ where a is any point in $\mathbb{H} \cap \Gamma$. We have the following theorem [1, Chapter XIII]

Theorem 7.2 (Weber-Fueter)**.** *Let E be an elliptic curve with endomorphism ring $\mathfrak{o}_k$, then*

1. *$\alpha = j(E)$ are algebraic integers.*
2. *$k(\alpha)$ is the Hilbert class field of k.*
3. *Gal($k(\alpha)/k$) permutes the $j(E)$' associated to $\mathfrak{o}_k$ transitively.*

The proof uses reduction on primes, and it is very technical. We will not present the proof here.

Recall that in Section 2, we have defined a generalization of Hilbert class field: ray class field. For $\mathbb{Q}$, the ray class field corresponds to the cyclotomic extension of $\mathbb{Q}$, and every cyclotomic extension can be written as $\mathbb{Q}(\zeta_m)$ where $\zeta_m = \exp(\frac{2\pi i}{m})$ is a special value of the exponential function. We are trying to generalize this construction to quadratic imaginary field k. According to the above theorem, it seems that the j-invariant seems a good candidate, however, we will see it soon that j-invariant alone does not generate the ray class field. We will need to define some special elliptic functions.

We will start by defining 4 classical Weierstrass elliptic functions:

Definition 7.1. Let $\Lambda \subset \mathbb{C}$ be a lattice in $\mathbb{C}$, we define

1. The *Weierstrass σ-function* to be

$$\sigma(z;\Lambda) = z \prod_{w \in \Lambda - \{0\}} (1 - \frac{z}{w}) \exp(\frac{z}{w} + \frac{1}{2}(\frac{z}{w})^2).$$

2. The *Weierstrass ζ-function* to be

$$\zeta(z;\Lambda) = \frac{\sigma'(z;\Lambda)}{\sigma(z;\Lambda)}.$$

3. The *Weierstrass η-function* to be

$$\eta(w;\Lambda) = \zeta(z+w;\Lambda) = \zeta(z;\Lambda)$$

   for any $z \in C$.

4. The *Weierstrass $\wp$-function* to be

$$\wp(z,\Lambda) = -\zeta'(z;\Lambda)$$

Note that Weierstrass $\wp$-function is doubly periodic with periods Λ and satisfies

$$[\wp'(z;\Lambda)]^2 = 4[\wp(z;\Lambda)]^2 - g_2\wp(z;\Lambda) - g_3$$

where $y^2 = 4x^3 - g_2x - g_3$ is the function defining $E \cong \mathbb{C}/\Lambda$. In other words, the map $f : \mathbb{C}/\Lambda \xrightarrow{\sim} E \subset \mathbb{P}^2$ by $z \mapsto (\wp(z,\Lambda), [\wp(z,\Lambda)]')$ is an isomorphism as complex manifold.

We now define the Weber τ-function:

Definition 7.2. The Weber τ-function $\tau : E \longrightarrow \mathbb{P}^1$ is defined to be

$$\tau(f(z))) = \begin{cases} \frac{g_2(\Lambda)g_3(\Lambda)}{\Delta(\Lambda)}\wp(z,\Lambda) & \text{if } j(E) \neq 0, 1728 \\ \frac{g_2(\Lambda)^2}{\Delta(\Lambda)}\wp(z,\Lambda)^2 & \text{if } j(E) = 1728 \\ \frac{g_3(\Lambda)}{\Delta(\Lambda)}\wp(z,\Lambda)^3 & \text{if } j(E) = 0 \end{cases}$$

where $\Delta(\Lambda) = g_2(\Lambda)^3 - 27g_3(\Lambda)^2$ is the discriminant.

We also define the group of torsions points of E

Definition 7.3. Let $\mathfrak{a}$ be an integral ideal of $\mathfrak{o}_k$, we define the group of $\mathfrak{a}$-torsions points of E to be

$$E[\mathfrak{a}] = \{P \in E : \gamma(P) = 0 \text{ for all } \gamma \in \mathfrak{a}\}$$

We are now able to state the theorem as an analogue of the cyclotomic field for quadratic imaginary field [4, Chapter II, Theorem 5.6]:

Theorem 7.3. *Let k be a quadratic imaginary field, and E be an elliptic curve with complex multiplication by $\mathfrak{o}_k$, and $\mathfrak{a}$ be an integral ideal of $\mathfrak{o}_k$, then*

$$k(j(E), \tau(E[\mathfrak{a}]))$$

is the ray class field of k associated to $\mathfrak{a}$.

Since every abelian extension is contained in some ray class field, we can immediately derive the following corollary:

Corollary 7.4. *With the notation above, let k^{ab} denotes the maximal abelian extension of k, then*

$$k^{\mathrm{ab}} = k(j(E), \tau(E_{tors}))$$

Since every abelian extension is contained in some ray class field, by Theorem 5.7, we only need to prove the Stark's conjecture for ray class field. In order to do this, we will construct Stark's unit using some special functions.

We define

$$G(z;\Lambda) = \exp(-6z \cdot \eta(z;\Lambda))\sigma(z;\Lambda)^{12}\Delta(\Lambda)$$

where η and σ are classical Weierstrass elliptic functions defined earlier.

Let $\mathfrak{m} \neq (1)$ be an integral ideal of $\mathfrak{o}_k$, and $\mathrm{Cl}(\mathfrak{m})$ be the ray class group associated to $\mathfrak{m}$. Denote f to be the smallest positive integer in $\mathfrak{m} \cap \mathbb{Z}$. For each $c \in \mathrm{Cl}(\mathfrak{m})$, we define *Siegel-Ramachandra* invariant

$$g_{\mathfrak{m}}(c) = G(1, \mathfrak{m}\mathfrak{a}^{-1})^f$$

where $\mathfrak{a}$ is an integral ideal in the class c. This invariant has some nice properties [2]:

Proposition 7.5. *The Siegel-Ramachandra invariant defined above satisfies:*

1. $g_{\mathfrak{m}}(c)$ *does not depend on the choice* $\mathfrak{a}$ *in* c.
2. $g_{\mathfrak{m}}(c)$ *is contained in the ray class field* $k_{\mathfrak{m}}$ *associated to* $\mathfrak{m}$.
3. *If* $\sigma_c \in Gal(k_{\mathfrak{m}}/k)$ *is the automorphism of* $k_{\mathfrak{m}}$ *associated to the class* c *with Artin's map, then*
$$g_{\mathfrak{m}}(c) = g_{\mathfrak{m}}(1)^{\sigma_c}$$
4. $g_{\mathfrak{m}}(c)$ *is a unit if* $\mathfrak{m}$ *has at least* 2 *distinct prime divisors. Otherwise,* $g_{\mathfrak{m}}(c)$ *is a* $\{\infty, \mathfrak{p}\}$*-unit, where* $\mathfrak{p}$ *is the unique prime dividing* $\mathfrak{m}$*, and for all* $\sigma \in Gal(k_{\mathfrak{m}}/k)$, $g_{\mathfrak{m}}(c)^{1-\sigma}$ *is a unit.*
5. *The field* $k(g_{\mathfrak{m}}(c)^{1/(12f)})$ *is an abelian extension of* k.
6. *Using 'Second Kronecker Limit Formula', we can show*
$$\zeta'_{k_{\mathfrak{m}}/k,S}(0,\sigma) = \frac{1}{12f \cdot w(\mathfrak{m})} \log |g_{\mathfrak{m}}(1)^{\sigma}|$$
for all $\sigma \in Gal(k_{\mathfrak{m}}/k)$*. Here* $S = \{\infty, \mathfrak{p} : \mathfrak{p} \mid \mathfrak{m}\}$, $w(\mathfrak{m}) = |\{\zeta \in \mu(k) : \zeta \equiv 1\,(\mathfrak{m})\}|$*, and* $\mu(k)$ *is the set of roots of unity in* k.

Note by passing to a larger ray class field, we can always get that $w(\mathfrak{m}) = 1$. So every abelian extension of k is contained in some ray class field $k_{\mathfrak{m}}$ with $u(\mathfrak{m}) = 1$. Now similar as in the proof of Theorem 5.7, there exists $\epsilon \in U^{\text{ab}}_{k_{\mathfrak{m}}/k}$ such that

$$\epsilon^{12f} = \zeta g_{\mathfrak{m}}(1)^{e}$$

where ζ is some roots of unity in $k_{\mathfrak{m}}$ and $e = e_{k_{\mathfrak{m}}}$ is the number of roots of unity in $k_{\mathfrak{m}}$.

Now Property 6 from the previous Proposition tells us that

$$\zeta'_{k_{\mathfrak{m}}/k,S}(0,\sigma) = -\frac{1}{e} \log |\epsilon^{\sigma}|$$

where we choose our completely splitting prime to be the infinite prime. The Property 4 shows that $|\epsilon|_w = 1$ if $|S| \geqslant 3$, and $|\epsilon|_{\sigma w} = |\epsilon|_w$ for all $\sigma \in G$ if $S = \{\infty, \mathfrak{p}\}$. This proves the Stark's conjecture for abelian extension of quadratic imaginary field k.

Bibliography

[1] J.W.S. Cassels, A. Frohlich *Algebraic Number Theory,* London Mathematical Society, (2010)

[2] J. Tate, *Les Conjectures de Stark sur les Fonction L d'Artin en* $s = 0$*,* Birkhauser Boston, Inc., (1984)

[3] J. Serre *Linear Representations of finite groups,* Springer-Verlag New York, Inc., (1977)

[4] J. Silverman, *Advanced topics in the arithmetic of elliptic curves,* Springer-Verlag New York, Inc., (1994)