Università degli Studi di Padova

DIPARTIMENTO DI MATEMATICA "TULLIO LEVI-CIVITA"

Corso di Laurea Magistrale in Matematica

Stark's Conjecture

Relatore:
Prof. Matteo Longo

Laureando:
Luca Lovato, 1176516

13 dicembre 2019

Contents

Chapter 1

Introduction

The *Riemann Zeta function*

$$\zeta(s) = \sum_{n=1}^{\infty} \frac{1}{n^s} \tag{1.1}$$

was introduced in the first half of the eighteenth century by Leonhard Euler as a function of a real variable, and extended to a complex variable by Riemann in 1859. $\zeta(s)$ is defined in the half-plane $\Re(s) > 1$ and it extends to the whole complex plane as a meromorphic function with only a simple pole at $s = 1$ by analytic continuation. The Riemann Zeta function is an important analytic object. For example, one of the main open problems in mathematics, the Riemann Hypothesis, concerns the Riemann Zeta function. On the other hand, thanks to its form as Euler product

$$\zeta(s) = \prod_{p \text{ prime}} \frac{1}{1 - p^{-s}},$$

$\zeta(s)$ gives us some important properties on the distribution of prime numbers.

A generalization of (1.1) is given by the *Dedekind Zeta function*, a complex-valued function of the form

$$\zeta_k(s) = \sum_{I} \frac{1}{\mathbf{N}I^s} = \prod_{P} \frac{1}{1 - \mathbf{N}P^{-s}} \tag{1.2}$$

defined in the half-plane $\Re(s) > 1$, where the sum is over all the nonzero ideals I of the ring of integers $\mathcal{O}_k$ of the number field k and the product runs over all the prime ideals P of $\mathcal{O}_k$. There is a relationship between certain algebraic invariants of the field k and (1.2). In fact, the analytic behavior of the function ζ_k allows us to prove purely algebraic facts about k. For example, Dirichlet used the fact that the Riemann Zeta function

$$\zeta_{\mathbb{Q}}(s) = \zeta(s)$$

has a simple pole at $s = 1$ in order to prove that there are infinitely many primes in every arithmetic progression of the form

$$\{a + nb : n \in \mathbb{N}\},$$

where a and b are positive coprime integers. To prove this theorem, Dirichlet also had to introduce a generalization of the Dedekind Zeta function for a general ideal class character χ, called *abelian L-function*. It is defined as

$$L(s,\chi) = \sum_I \frac{\chi(I)}{\mathbf{N}I^s} = \prod_P \frac{1}{1 - \chi(P)\mathbf{N}P^{-s}},$$

where the sum is over all the integral ideals I prime to the conductor $\mathfrak{m}_\chi$ associated to χ and the product is over the prime ideals P not dividing $\mathfrak{m}_\chi$.

In connection with his research into class field theory, in 1923 Emil Artin introduced the *Artin L-functions*. More precisely, let K/k be a finite Galois extension of number fields and let V be a complex representation of the Galois group $G = G_{K/k}$. For a finite place $v = P_v$ of k, set

$$L_v(s,V) = \frac{1}{\det(1 - \phi_w \mathbf{N}P_v^{-s} \mid {}_{V^{I_w}})},$$

where I_w is the inertia group of w, a places of K which lies above v, and

$$\begin{aligned} \phi_w : \mathbb{F}_w &\to \mathbb{F}_w \\ x &\mapsto x^{q_v} \end{aligned}$$

is the corresponding Frobenius automorphism. So, an Artin L-function is defined as

$$L(s,V) := \prod_v L_v(s,V), \tag{1.3}$$

where the product is over the finite places v of k. Since $L(s,V)$ depends only on the isomorphism class of the representation V, we can also denoted $L(s,V)$ by

$$L(s,\chi),$$

where

$$\chi : G \to \mathbb{C}$$

is the character corresponding to V. In particular, if G is abelian, we can observe that (1.3) is an abelian L-function.

The Dirichlet class number formula states that the Dedekind Zeta function $\zeta_K(s)$ has a simple pole at $s = 1$ with residue

$$\frac{2^{r_1}(2\pi)^{r_2}}{\sqrt{|d_K|}}\frac{h_K R_K}{w_K},$$

where

- r_1 and r_2 are the number of real and complex places of K respectively;
- h_K is the class number of K;
- R_K is the regulator of K;
- w_K is the number of roots of unity contained in K;
- d_K is the discriminant ideal of the extension $K/\mathbb{Q}$.

By the functional equation (3.31) for $\zeta_K(s)$, the Dirichlet class number formula can be reformulated to became true for $s = 0$. In this way, we have that the Taylor expansion of $\zeta_K(s)$ at $s = 0$ starts as

$$\zeta_K(s) = -\frac{h_K R_K}{w_K} s^{r_1+r_2-1} + \dots.$$

Note that, *Example 5* gives us a relation between the Dedekind Zeta function and the Artin L-functions, that is, the decompostion

$$\zeta_K(s) = \prod_i L(s, V_i)^{\mathrm{dim} V_i}, \tag{1.4}$$

where V_i runs through the irreducible complex representations of G. In particular,

$$-\frac{h_K R_K}{w_K} \tag{1.5}$$

is the ratio between the transcendental number R_K and the algebraic number

$$-\frac{h_K}{w_K}.$$

Stark Conjecture concerns the algebraicity of leading term of the Taylor expansions of Artin L-functions, divided by suitable complex numbers, called regulators. It has been inspired by the rationality of the result (1.5) and the factorization (1.4) for the Dedekind Zeta function.

More precisely, let S be a finite set of places of k containing S_∞, the set of infinite places of k. We define the *S-imprimitive Artin L-function* for $\Re(s) > 1$ as

$$L_S(s, V) \coloneqq \prod_{v \notin S} L_v(s, V).$$

We write

$$L_S(s, V) = c_S(\chi) s^{r_S(\chi)} + \dots,$$

where

$$r(\chi) = r_S(\chi)$$

is the order of vanishing of $L_S(s, V)$ at $s = 0$.

Let S_K be the set of places of K lying above the places of S. Let

$$Y = Y_{S_K}$$

be the free abelian group on S_K, and let

$$\eta : Y \to \mathbb{Z}$$

be the surjective homomorphism such that

$$\eta(w) = 1 \text{ for all } w \in S_K.$$

The kernel of η is denoted by

$$X = X_{S_K}.$$

Given an abelian group B and a subring A of $\mathbb{C}$, we set

$$AB \coloneqq A \otimes_{\mathbb{Z}} B.$$

Denote by

$$U = U_{K,S_K} = \{x \in K : \mathrm{ord}_{P_w}(x) = 0 \text{ for all } w \notin S_K\}$$

the group of S_K-units of K. Note that the logarithm map

$$\lambda : U \to \mathbb{R}Y$$

defined by

$$u \mapsto \sum_{w \in S_K} \log |u|_w \cdot w.$$

has image in $\mathbb{R}X$. By *Theorem 4.3.1*, tensoring λ with $\mathbb{R}$, we get the G-equivariant isomorphism

$$1 \otimes \lambda : \mathbb{R}U \to \mathbb{R}X,$$

which we denote with the same symbol λ. Moreover, tensoring λ with $\mathbb{C}$, we obtain an isomorphism of $\mathbb{C}[G]$-modules

$$\mathbb{C}U \to \mathbb{C}X,$$

also denoted by λ.

Let

$$f : \mathbb{Q}X \to \mathbb{Q}U$$

be a $\mathbb{Q}[G]$-isomorphism. f induces an isomorphism of $\mathbb{C}[G]$-modules

$$\mathbb{C}X \xrightarrow{\cong} \mathbb{C}U,$$

which we denote by the same symbol. Composing f with λ, we get the $\mathbb{C}[G]$-automorphism of $\mathbb{C}X$

$$\lambda \circ f : \mathbb{C}X \longrightarrow \mathbb{C}X,$$

which induces an automorphism

$$\begin{aligned}(\lambda \circ f)_V : \mathrm{Hom}_G(V^*, \mathbb{C}X) &\longrightarrow \mathrm{Hom}_G(V^*, \mathbb{C}X)\\ \varphi &\longmapsto \lambda \circ f \circ \varphi\end{aligned}$$

where

$$V^* = \mathrm{Hom}_{\mathbb{C}}(V, \mathbb{C})$$

is the dual representation to V.

Define the *Stark regulator* as the determinant

$$R(V, f) := R_S(V, f) = \det((\lambda \circ f)_V).$$

Since the definition of the Stark regulator does not depend on the choice of the representation V, we write

$$R(\chi, f)$$

instead of $R(V, f)$. Set

$$\mathbb{Q}(\chi) := \mathbb{Q}(\{\chi(\sigma) : \sigma \in G\}),$$

and

$$\Delta_\chi := \mathrm{Gal}(\mathbb{Q}(\chi)/\mathbb{Q}).$$

Define

$$A(\chi, f) = A_S(\chi, f) := \frac{R(\chi, f)}{c(\chi)}.$$

Then, the Stark basic's conjecture states that

- $A(\chi, f) \in \mathbb{Q}(\chi)$;
- $A(\chi, f)^\alpha = A(\chi^\alpha, f)$, for all $\alpha \in \Delta_\chi$.

In the case of rank 1, i.e. $r(\chi) = 1$, assuming Stark Conjecture, one can describe the leading term of the Taylor expansion of the Artin L-function, divided by the regulator term, by means of the logarithm of certain units in K, which are called *Stark units*. This can then be seen as a generalization of the formula for the leading coefficient of the Dedekind Zeta function in terms of the regulator, the class number and the number of roots of unity in K.

Chapter 2

Preliminaries

2.1 Number fields

Definition 2.1. A ***number field*** k is a finite extension of the field $\mathbb{Q}$ of rationals.

Definition 2.2. The ***ring of integers*** O_k of a number field k is the ring of all integral elements contained in k. In particular, if I is an ideal in O_k, we set

$$\mathbf{N}I = [\mathcal{O}_k : I],$$

where $[\mathcal{O}_k : I]$ is the number of residue classes of I.

Definition 2.3. Let k be a number field with $n = [k : \mathbb{Q}]$. Let $\alpha \in k$ and $f(X)$ be its minimal polynomial over $\mathbb{Q}$. If $\alpha_1 = \alpha, \dots, \alpha_m$ are the roots of f, then

$$\mathbf{Tr}_{k/\mathbb{Q}}(\alpha) = \frac{n}{m}(\alpha_1 + \cdots + \alpha_m)$$

is called the ***trace*** of α, and

$$\mathbf{N}_{k/\mathbb{Q}}(\alpha) = (\alpha_1 \cdot \ldots \cdot \alpha_m)^{\frac{n}{m}}$$

is called the ***norm*** of α.

Definition 2.4. A map

$$|-| : k \to \mathbb{R}_{\geq 0}$$

is an ***absolute value*** if for all $x, y \in k$

(1) $|x| = 0 \Leftrightarrow x = 0$;

(2) $|xy| = |x| \cdot |y|$;

(3) $|x+y| \le |x| + |y|$;

(4) $\exists\, x \in k$ with $|x| \notin \{0, 1\}$.

If (3) can be replaced by

$$(3') \ |x+y| \le \max(|x|, |y|),$$

then it is said to be a ***nonarchimedean*** absolute value. Otherwise, say it is ***archimedean***.

Proposition 2.1.1. *Let $|-|$ be an absolute value on k. Then the function*

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

is a metric on k, invariant under translation, for which the field operations are continuous. In particular, any absolute value on k makes k into a topological field.

Proof. Follows from the axioms. □

Definition 2.5. Two absolute values on k are ***equivalent*** if they induce the same metric topology on k.

Definition 2.6. A ***place*** of a field k is an equivalence class of non-trivial absolute values on k. There are three types of places:

- ***finite***, which correspond to a non-zero prime ideal in O_k;
- ***real***, which correspond to an embedding of k into $\mathbb{R}$;
- ***complex***, which correspond to a pair of distinct complex conjugate embeddings of k into $\mathbb{C}$.

Let v be an absolute value. We consider the following normalizations.

- If v is finite, with P_v the corresponding non-zero prime ideal in O_k, then
$$|x|_v = (\mathbf{N}P_v)^{-\mathrm{ord}_{P_v}(x)},$$
where $\mathrm{ord}_{P_v}(x)$ is the exponent of P_v in the prime factorization of (x).
- If v is real, then
$$|x|_v = |\sigma_v(x)|,$$
where σ_v is the corresponding real embedding.

- If v is complex, then

$$|x|_v = |\sigma_v(x)|^2 = \sigma_v(x)\bar{\sigma}_v(x),$$

where $\{\sigma_v, \bar{\sigma}_v\}$ is the corresponding pair of complex conjugate embeddings.

Theorem 2.1.2. *Let k be a field with an absolute value $|-|$. There exists a field $\hat{k}$ with an absolute value $|-|\hat{}$, together with an isometric embedding*

$$\iota : k \hookrightarrow \hat{k}$$

such that:

(i) $\hat{k}$ *is complete w.r.t. the metric given by* $|-|\hat{}$*;*

(ii) $\iota(k)$ *is dense in* $\hat{k}$*;*

(iii) any isometric embedding

$$\lambda : (k, |-|) \hookrightarrow (k', |-|')$$

of k into a complete field k' factors uniquely through ι.

Proof. Let

- $R \subset k^{\mathbb{N}}$ be the ring of Cauchy sequences in k;
- $I \subset R$ be the ideal of null sequences.

In particular, I is maximal. In fact, let

$$x = (x_n)_{n\in\mathbb{N}} \in R \setminus I.$$

Fix $N \in \mathbb{N}$. Since $x \notin I$, there exists $\varepsilon > 0$ such that

$$|x_n| \geq \varepsilon \text{ for each } n \geq N.$$

Set

$$y_n = \begin{cases} \frac{1}{x_n} & \text{if } n \geq N \\ 0 & \text{if } n < N \end{cases}.$$

Now, let $\varepsilon' > 0$. Since x is a Cauchy sequence, then there exists $N' = N'(\varepsilon'\varepsilon^2)$ such that for each $m, n \geq N'$

$$|x_n - x_m| < \varepsilon'\varepsilon^2.$$

Then, for each $m, n \geq \max\{N, N'\}$,

$$|y_n - y_m| = \frac{|x_m - x_n|}{|x_m x_n|} \leq \frac{|x_n - x_m|}{\varepsilon^2} < \frac{\varepsilon' \varepsilon^2}{\varepsilon^2} = \varepsilon'.$$

Hence, $y = (y_n)_{n\in\mathbb{N}}$ is a Cauchy sequence. In particular,

$$xy \in 1 + I.$$

So,

$$\hat{k} := R/I$$

is a field, i.e. $I \trianglelefteq R$ is maximal. Define the map

$$| - |^{\hat{}} : R \to \mathbb{R}_{\geq 0}$$

as

$$|(x_n)_{n\in\mathbb{N}}|^{\hat{}} = \lim_{n\to\infty} |x_n|,$$

with $(x_n)_{n\in\mathbb{N}} \in R$. Let $x = (x_n)_{n\in\mathbb{N}} \in R$. The inequality

$$-|x_m - x_n| \leq |x_m| - |x_n| \leq |x_m - x_n|$$

shows that $(|x_n|)_{n\in\mathbb{N}}$ is a Cauchy sequence in $[0, \infty)$, i.e. convergent in $[0, \infty)$. Moreover, if $(y_n)_{n\in\mathbb{N}}$ represents the same coset in $\hat{k}$ as $(x_n)_{n\in\mathbb{N}}$, then

$$\lim_{n\to\infty} |x_n - y_n| = 0.$$

Therefore

$$\lim_{n\to\infty} |x_n| = \lim_{n\to\infty} |y_n|.$$

This shows that $| - |^{\hat{}}$ is well defined on the field $\hat{k}$. Now, note that:

- $|x|^{\hat{}} = 0 \Leftrightarrow \lim_{n\to\infty} |x_n| = 0 \Leftrightarrow \lim_{n\to\infty} x_n = 0 \Leftrightarrow x \in I$;
- if $y = (y_n)_{n\in\mathbb{N}} \in R$, then
$$|xy|^{\hat{}} = \lim_{n\to\infty} |x_n y_n| = \lim_{n\to\infty} |x_n||y_n| = |x|^{\hat{}}|y|^{\hat{}};$$
- $|x + y|^{\hat{}} = \lim_{n\to\infty} |x_n + y_n| \leq \lim_{n\to\infty} (|x_n| + |y_n|) = |x|^{\hat{}} + |y|^{\hat{}}$;
- by definition of absolute value, there exists $z \in k$ with $|z| \notin \{0, 1\}$. Define the Cauchy sequence $(z_n)_n$ setting
$$z_n = z \text{ for each } n \in \mathbb{N}.$$
Since
$$\lim_{n\to\infty} |z_n| = \lim_{n\to\infty} |z| = |z|,$$
then
$$|(z_n)_n|^{\hat{}} \notin \{0, 1\}.$$

Therefore, $|-|^\wedge$ is an absolute value on $\hat{k}$.

Now, for each $a \in k$, let

$$\sigma^a : \mathbb{N} \to k$$

be a constant sequence defined by

$$\sigma^a_n := \sigma^a(n) = a \text{ for each } n \in \mathbb{N}.$$

This is a Cauchy sequence and so determines a coset in $\hat{k}$. Then, the map

$$\begin{aligned} \iota : k &\to \hat{k} \\ a &\mapsto \overline{(\sigma^a_n)_{n\in\mathbb{N}}} \end{aligned}$$

is an embedding. In particular, ι is an isometry with respect to the metrics induced by $|-|$ and $|-|^\wedge$ and its image is dense in $\hat{k}$. In fact, let $x \in \hat{k}$ be the equivalence class of $(x_n)_n \in R$. By the definition of Cauchy sequence, for any $\varepsilon > 0$, there exists $m \in \mathbb{N}$ such that

$$|x_n - x_m| < \varepsilon \text{ for all } n \geq m.$$

Then

$$|x - \iota(x_m)|^\wedge = \lim_{n\to\infty} |x_n - \sigma^{x_m}_n| < \varepsilon.$$

Let $(z_n)_n$ be a Cauchy sequence in k. Note that $(\iota(z_n))_n$ is a Cauchy sequence in $\hat{k}$. In fact, for any $\varepsilon > 0$, there exists $N \in \mathbb{N}$ such that

$$|z_n - z_m| < \varepsilon \text{ for all } n, m \geq N.$$

Hence,

$$|\iota(z_n) - \iota(z_m)|^\wedge = \lim_{k\to\infty} |\sigma^{z_n}_k - \sigma^{z_m}_k| = \lim_{k\to\infty} |z_n - z_m| < \varepsilon,$$

for all $n, m \geq N$. Let $z \in \hat{k}$ be the equivalence class of $(z_n)_n$. Since

$$|z - \iota(z_n)|^\wedge = \lim_{k\to\infty} |z_k - \sigma^{z_n}_k| < \varepsilon \text{ for all } n \geq N,$$

then $(\iota(z_n))_n$ coverges to z in $\hat{k}$. Thus, every Cauchy sequence in $\hat{k}$ that consists entirely of elements of k converges in $\hat{k}$.

Now, let $(z_n)_n$ be a Cauchy sequence in $\hat{k}$. Since k is dense in $\hat{k}$, for each z_n we may pick $x_n \in k$ so that

$$|z_n - \iota(x_n)|^\wedge < \frac{1}{n}. \tag{2.1}$$

In particular, for any $\varepsilon > 0$, there exists $N \in \mathbb{N}$ such that

- $|z_m - \iota(x_m)|^\wedge < \varepsilon/3$;
- $|z_n - \iota(x_n)|^\wedge < \varepsilon/3$;
- $|z_m - z_n|^\wedge < \varepsilon/3$,

for all $m, n \geq N$. Then, it follows from the triangle inequality that

$$\begin{aligned} |x_m - x_n| &= |\iota(x_m) - \iota(x_n)|^\wedge \\ &\leq |z_m - \iota(x_m)|^\wedge + |z_n - \iota(x_n)|^\wedge + |z_m - z_n|^\wedge \\ &< \varepsilon, \end{aligned}$$

for all $m, n \geq N$, i.e. $(x_n)_n \in R$. Hence, by (2.1), $(z_n)_n$ is equivalent to a Cauchy sequence in k. Then by above, $(z_n)_n$ converges in $\hat{k}$. Thus the pair $(\hat{k}, |-|^\wedge)$ satisfies the requirements of a completion.

Let λ as in the statement of the theorem. Define

$$\tau : \iota(k) \to \lambda(k)$$

by

$$\tau(x) = \lambda \circ \iota^{-1}(x), \text{ with } x \in \iota(k).$$

It follows that

$$\tau^{-1}(y) = \iota \circ \lambda^{-1}(y), \text{ with } y \in \lambda(k).$$

In particular, τ and τ^{-1} are both continuous. Since $\iota(k)$ and $\lambda(k)$ are dense in $\hat{k}$ and k', respectively, both τ and τ^{-1} have unique extensions to continuous maps

$$\tau : \hat{k} \to k' \text{ and } \tau^{-1} : k' \to \hat{k}.$$

So, by the continuity, the extended maps are isometric isomorphisms. □

Since the topology induced by an absolute value on k only depending on its place v, then we indicate by k_v the completion of k constructed in the proof of *Theorem 2.1.2*.

Theorem 2.1.3. *Let k be a number field and Σ_k be the set of all places of k. Let $x \in k^*$. Then the product formula holds*

$$\prod_{v \in \Sigma_k} |x|_v = 1. \tag{2.2}$$

Proof. Note that the product is multiplicative in x. Then it suffices to check (2.2) when $x \in \mathcal{O}_k^*$.

If $x \in \mathcal{O}_k^\times$, then

$$\mathrm{ord}_{P_v}(x) = 0$$

for each finite place v of k, i.e.

$$|x|_v = 1$$

for each finite place v of k.

Let $x \in \mathcal{O}_k^* \smallsetminus \mathcal{O}_k^\times$. Consider the prime ideal factorization

$$x\mathcal{O}_k = P_{v_1}^{a_1} \cdots P_{v_r}^{a_r}, \tag{2.3}$$

for some finite places $v_1, \ldots, v_r$ of k and where

$$a_i = \mathrm{ord}_{P_{v_i}}(x) \in \mathbb{N}_{\geq 1},\ \ i = 1, \ldots, r.$$

The only terms in the factorization (2.3) which are not necessarily 1 come from the absolute values attached to these v_i's and to the real and complex absolute values.

The contribution to (2.2) from the finite places is

$$\prod_{i=1}^{r} |x|_{v_i} = \prod_{i=1}^{r} (\mathbf{N}P_{v_i})^{-\mathrm{ord}_{P_{v_i}}(x)} = \prod_{i=1}^{r} (\mathbf{N}P_{v_i})^{-a_i}.$$

On the other hand, the contribution to (2.2) from the real and complex absolute values is

$$\prod_{v \text{ real}} |x|_v \cdot \prod_{v \text{ complex}} |x|_v = \prod_{v \text{ real}} |\sigma_v(x)| \cdot \prod_{v \text{ complex}} |\sigma_v(x)|^2 = |\mathbf{N}_{k/\mathbb{Q}}(x)|.$$

From the compatibility of the norm on principal ideals and elements, we obtain

$$|\mathbf{N}_{k/\mathbb{Q}}(x)| = \mathbf{N}(x\mathcal{O}_k) = \prod_{i=1}^{r} (\mathbf{N}P_{v_i})^{a_i}.$$

Hence,

$$\prod_{v \in \Sigma_k} |x|_v = |\mathbf{N}_{k/\mathbb{Q}}(x)| \cdot \prod_{i=1}^{r} (\mathbf{N}P_{v_i})^{a_i} = 1.$$

□

We denote the number of real places by

$$r_1 = r_1(k),$$

and the number of complex places by

$$r_2 = r_2(k).$$

Moreover, for each finite place v, we denote the corresponding residue field by

$$\mathbb{F}_v = O_k/P_v,$$

and its cardinality by

$$q_v = \mathbf{N}P_v.$$

2.2 Representations of finite groups

Let G be a finite group.

Definition 2.7. A ***representation*** of G is a finite dimensional left $\mathbb{C}[G]$-module V where

$$\mathbb{C}[G] = \left\{ \sum_{g \in G} \lambda_g g, \lambda_g \in \mathbb{C} \right\}$$

is the group algebra. Equivalently, a representaion of G is a finite dimensional $\mathbb{C}$-vector space V together with a morphism

$$\rho : G \to GL(V)$$

giving the action of G on V.

Definition 2.8. Two representations V and W are said to be ***isomorphic*** if they are isomorphic as $\mathbb{C}[G]$-module.

In the following, we use the symbol $GL(V)$ to denote $\mathrm{Aut}(V)$ because a basis for V gives an isomorphism

$$\mathrm{Aut}(V) \xrightarrow{\sim} GL_n(\mathbb{C})$$

where $n = \dim(V)$. Moreover, we write

$$\sigma.x \text{ instead of } \rho(\sigma)(x)$$

for $x \in V$ and $\sigma \in G$, and define

$$V^G := \{x \in V : \sigma.x = x \text{ for each } \sigma \in G\}.$$

Definition 2.9. Given two representations

$$\rho : G \to GL(V) \text{ and } \nu : G \to GL(W),$$

a ***morphism***, or a ***G-equivariant map***, between V and W is a linear map

$$T : V \to W$$

such that the diagram

$$\begin{tikzcd} V \arrow[r, "T"] \arrow[d, "\rho(\sigma)"'] & W \arrow[d, "\nu(\sigma)"] \\ V \arrow[r, "T"] & W \end{tikzcd}$$

commutes for all $\sigma \in G$, i.e.

$$\nu(\sigma)T = T\rho(\sigma), \text{ for all } \sigma \in G.$$

Furthermore, if T is invertible, it is called an ***isomorphism***.

Example 1.

(1) The *trivial* representation is $V = \mathbb{C}$ where the action of G is given by

$$\sigma.x = x, \text{ for all } \sigma \in G, x \in \mathbb{C}.$$

(2) The *regular* representation is $V = \mathbb{C}[G]$ with the action of G given by left multiplication, i.e. if $\sigma \in G$ then

$$\sigma.g = \sigma g, \text{ for all } g \in G.$$

(3) If V and W are representations of G, then $V \oplus W$ is a representation, where the action is defined as

$$\sigma.(x \oplus y) \coloneqq \sigma.x \oplus \sigma.y,$$

for all $\sigma \in G, x \in V, y \in W$.

(4) If V and W are representations of G, then $V \otimes_{\mathbb{C}} W$ is a representation, where the action is defined as

$$\sigma.(x \otimes y) \coloneqq \sigma.x \otimes \sigma.y,$$

for all $\sigma \in G, x \in V, y \in W$.

(5) Let V and W be two representations of G. Then the space $\mathrm{Hom}_{\mathbb{C}}(V, W)$ of all linear maps $f : V \to W$ is a representation, where the action of G is given by

$$f^{\sigma}(x) = (\sigma.f)(x) = \sigma.(f(\sigma^{-1}.x)),$$

for all $\sigma \in G, f \in \mathrm{Hom}_{\mathbb{C}}(V, W), x \in V$. Note that

$$(f^{\sigma})^{\tau} = f^{\tau\sigma}.$$

Set

$$\mathrm{Hom}_G(V, W) \coloneqq \{T : V \to W \text{ such that } T \text{ is a } G\text{-equivariant map}\}.$$

Hence,

$$\begin{aligned}
\mathrm{Hom}_{\mathbb{C}}(V, W)^G &= \{F \in \mathrm{Hom}_{\mathbb{C}}(V, W) : F^{\sigma} = F \text{ for each } \sigma \in G\} \\
&= \{F \in \mathrm{Hom}_{\mathbb{C}}(V, W) : \sigma.F\sigma^{-1} = F \text{ for each } \sigma \in G\} \\
&= \mathrm{Hom}_G(V, W).
\end{aligned}$$

(6) Let V be a representation of G. Then $V^* = \mathrm{Hom}_{\mathbb{C}}(V, \mathbb{C})$ is the *dual* representation to V, where the action of G is defined as

$$(\sigma.f)(x) = f(\sigma^{-1}.x),$$

for all $\sigma \in G, f \in V^*, x \in V$. In particular, we have

$$(V^*)^* = V,$$

and

$$\mathrm{Hom}_{\mathbb{C}}(V^*, W^*) \xrightarrow{\sim} \mathrm{Hom}_{\mathbb{C}}(W, V).$$

Finally, we have an isomorphism

$$V^* \otimes_{\mathbb{C}} W \xrightarrow{\sim} \mathrm{Hom}_{\mathbb{C}}(V, W)$$

given by

$$\begin{aligned} f \otimes w \mapsto V &\to W \\ v &\mapsto f(v)w \end{aligned}$$

Definition 2.10. Given a representation V of G, a ***subrepresentation*** is a subspace $U \subset V$ such that

$$g.U \subset U \text{ for each } g \in G.$$

Definition 2.11. A representation V is called ***irreducible*** if it has no non-trivial subrepresentations.

Definition 2.12. The ***character*** of a representation V of G is the function

$$\chi_V : G \longrightarrow \mathbb{C}$$

defined by

$$\chi_V(\sigma) = \mathrm{Tr}(\sigma|V),$$

i.e. it is the trace of the map

$$\begin{aligned} V &\longrightarrow V \\ x &\longmapsto \sigma.x \end{aligned}$$

The ***degree*** of χ_V is

$$\chi_V(1) = \mathrm{dim} V.$$

Let $\sigma \in G$, and $n = |\sigma|$. Let $\rho : G \to GL(V)$ be a representation of G. Note that

$$(\rho(\sigma))^n = \rho(\sigma^n) = \rho(1) = 1,$$

i.e. the eigenvalues of $\rho(\sigma)$ are all complex n-th roots of 1. Let ζ be a primitive n-th root of 1. Then

$$\chi_V(\sigma) = \mathrm{Tr}(\rho(\sigma)) = \sum_{k=0}^{n-1} \zeta^k,$$

i.e. $\chi_V(\sigma)$ is a sum of complex n-th roots of 1.

Example 2.

(1) If $V = \mathbb{C}$ is the trivial representation, then

$$\chi_{\mathbb{C}}(\sigma) = 1, \text{ for all } \sigma \in G.$$

(2) If $V = \mathbb{C}[G]$ is the regular representation, then

$$\chi_{\mathbb{C}[G]}(\sigma) = \left\{ \begin{array}{cl} |G| & \text{if } \sigma = 1 \\ 0 & \text{if } \sigma \neq 1 \end{array} \right. .$$

(3) If V and W are representations of G, then

$$\chi_{V \oplus W}(\sigma) = \chi_V(\sigma) + \chi_W(\sigma), \text{ for all } \sigma \in G.$$

(4) If V is a representation of G, then

$$\chi_{V^*}(\sigma) = \chi_V(\sigma^{-1}) = \overline{\chi_V(\sigma)}, \text{ for all } \sigma \in G.$$

(5) If V and W are representations of G, then

$$\chi_{V \otimes_{\mathbb{C}} W}(\sigma) = \chi_V(\sigma) \cdot \chi_W(\sigma), \text{ for all } \sigma \in G.$$

By this,

$$\chi_{\mathrm{Hom}_{\mathbb{C}}(V,W)}(\sigma) = \chi_{V^* \otimes_{\mathbb{C}} W}(\sigma) = \overline{\chi_V(\sigma)} \cdot \chi_W(\sigma), \text{ for all } \sigma \in G.$$

Let

$$\begin{aligned} F_C(G, \mathbb{C}) &= \{f : G \to \mathbb{C} \text{ such that } f(\sigma) = f(\tau\sigma\tau^{-1}) \text{ for each } \sigma, \tau \in G\} \\ &= \{f : G \to \mathbb{C} \text{ such that } \textstyle\sum_{\sigma \in G} f(\sigma)\sigma \in \mathrm{Z}(\mathbb{C}[G])\} \end{aligned}$$

be the space of *central functions* on G. In particular, we can make this space into a Hilbert space by putting

$$\langle f, g\rangle_G = \frac{1}{|G|}\sum_{\sigma\in G} f(\sigma)\overline{g(\sigma)}.$$

Let $\sigma, \sigma' \in G$ sucht that $\sigma \sim \sigma'$, i.e. there exists $\tau \in G$ such that $\sigma = \tau\sigma'\tau^{-1}$. Then

$$\rho(\sigma) = \rho(\tau\sigma'\tau^{-1}) = \rho(\tau)\rho(\sigma')\rho(\tau)^{-1} = \rho(\sigma'),$$

i.e. $\chi_V \in F_C(G, \mathbb{C})$.

Proposition 2.2.1. *Let V be a representation of G. Then*

$$\frac{1}{|G|}\sum_{\sigma\in G}\sigma$$

is a projection of V onto V^G.

Proof. Set $P = \frac{1}{|G|}\sum_{\sigma\in G}\sigma$. Since $P \in \mathrm{Z}(\mathbb{C}[G])$, then

$$\sigma.(P.x) = P.(\sigma.x), \text{ for all } \sigma \in G, x \in V.$$

So the action of P on V lies in $\mathrm{End}_G(V)$. Note that

$$\tau P = P = P\tau, \text{ for all } \tau \in G.$$

Then

$$P^2 = \left(\frac{1}{|G|}\sum_{\sigma\in G}\sigma\right)P = \frac{1}{|G|}\sum_{\sigma\in G}\sigma P = \frac{1}{|G|}\sum_{\sigma\in G}P = \frac{1}{|G|}\cdot|G|P = P,$$

i.e. P is a projection onto $\mathrm{Im}P$. Now, let $x = P.y$ for some $y \in V$. Then

$$\sigma.x = \sigma.(P.y) = P.y = x, \text{ for all } \sigma \in G,$$

i.e. $\mathrm{Im}P \subset V^G$. Conversely, let $x \in V^G$. Then

$$P.x = \left(\frac{1}{|G|}\sum_{\sigma\in G}\sigma\right).x = \frac{1}{|G|}\sum_{\sigma\in G}\sigma.x = \frac{1}{|G|}\sum_{\sigma\in G}x = \frac{1}{|G|}\cdot|G|x = x,$$

i.e. $V^G \subset \mathrm{Im}P$. Then P is a projection of V onto V^G. $\square$

Theorem 2.2.2. *If V and W are representations of G, then*

$$\langle\chi_V, \chi_W\rangle_G = \dim(\mathrm{Hom}_G(V, W)).$$

Proof. By *Proposotion 2.2.1*, $\frac{1}{|G|}\sum_{\sigma\in G}\sigma$ is a projection of $\mathrm{Hom}_{\mathbb{C}}(V,W)$ onto $\mathrm{Hom}_{\mathbb{C}}(V,W)^G$. Since the trace of a projection is the dimension of its image, then

$$\begin{aligned}\dim(\mathrm{Hom}_{\mathbb{C}}(V,W)^G) &= \mathrm{Tr}\big(\tfrac{1}{|G|}\textstyle\sum_{\sigma\in G}\sigma|\mathrm{Hom}_{\mathbb{C}}(V,W)\big)\\ &= \tfrac{1}{|G|}\textstyle\sum_{\sigma\in G}\chi_{\mathrm{Hom}_{\mathbb{C}}(V,W)}(\sigma) = \tfrac{1}{|G|}\textstyle\sum_{\sigma\in G}\chi_{V^*\otimes_{\mathbb{C}}W}(\sigma)\\ &= \tfrac{1}{|G|}\textstyle\sum_{\sigma\in G}\overline{\chi_V(\sigma)}\cdot\chi_W(\sigma).\end{aligned}$$

In particular, since this is an integer, we have that

$$\dim(\mathrm{Hom}_{\mathbb{C}}(V,W)^G) = \overline{\dim(\mathrm{Hom}_{\mathbb{C}}(V,W)^G)} = \frac{1}{|G|}\sum_{\sigma\in G}\chi_V(\sigma)\overline{\chi_W(\sigma)}.$$

It follows that

$$\begin{aligned}\langle\chi_V,\chi_W\rangle_G &= \tfrac{1}{|G|}\textstyle\sum_{\sigma\in G}\chi_V(\sigma)\overline{\chi_W(\sigma)} = \dim(\mathrm{Hom}_{\mathbb{C}}(V,W)^G)\\ &= \dim(\mathrm{Hom}_G(V,W)).\end{aligned}$$

□

Let $\{V_i\}$ be a complete family of non-isomorphic irreducible representations of G, and χ_i be the corresponding characters. Consider the following

Theorem 2.2.3 (Schur's Lemma)**.** *Let V and W be representations of G.*

(1) *If $V \ncong W$, then*
$$\mathrm{Hom}_G(V,W) = 0.$$

(2) *If $V \cong W$, then*
$$\mathrm{Hom}_G(V,W) \cong \mathbb{C}.$$

Proof. See [12, Ch. 2, §2, Proposition 4]. □

So, by *Theorem 2.2.2*,

$$\langle\chi_i,\chi_j\rangle_G = \dim(\mathrm{Hom}_G(V_i,V_j)) = \begin{cases} 0 & \text{if } i\neq j\\ 1 & \text{if } i=j\end{cases},$$

i.e. the χ_i form an orthonormal system in $F_C(G,\mathbb{C})$. In particular, the χ_i span $F_C(G,\mathbb{C})$. To show this, it suffices to prove that if $f\in F_C(G,\mathbb{C})$ such that

$$\langle f,\chi_i\rangle_G = 0,\ \text{for each i},$$

then $f = 0$. Let $\tau = \sum_{\sigma \in G} f(\sigma)\sigma$. Since $\tau \in \mathbb{C}[G]$, then it acts G-linearly on every V_i. By *Theorem 2.2.2*, τ acts as a constant c_i on V_i^*. So, we have

$$\begin{aligned} \langle f, \chi_i \rangle_G &= \tfrac{1}{|G|} \cdot \textstyle\sum_{\sigma \in G} f(\sigma)\overline{\chi_i(\sigma)} = \tfrac{1}{|G|} \cdot \chi_{V_i^*}\left(\textstyle\sum_{\sigma \in G} f(\sigma)\sigma \right) \\ &= \tfrac{1}{|G|} \cdot \mathrm{Tr}(\tau | V_i^*) = \tfrac{1}{|G|} \cdot c_i \mathrm{dim} V_i. \end{aligned}$$

Thus

$$\langle f, \chi_i \rangle_G = 0 \Leftrightarrow c_i = 0 \Leftrightarrow \tau . V_i^* = \{0\},$$

i.e. τ annihilates every irreducible representation. Note that, $\mathbb{C}[G]$ is semisimple (see [12, Ch. 6, §1, Proposition 9]), i.e. every representation is a direct sum of irreducible representation. By this,

$$\tau . \mathbb{C}[G] = \{0\}.$$

We can conclude that

$$\sum_{\sigma \in G} f(\sigma)\sigma = \tau = 0,$$

that is $f \equiv 0$, by definition of $\mathbb{C}[G]$.
Consider

$$\{\delta_C, C \text{ conjugacy class in } G\}$$

where

$$\delta_C(\sigma) = \left\{ \begin{array}{ll} 1 & \text{if } \sigma \in C \\ 0 & \text{if } \sigma \notin C \end{array} \right. .$$

Note that this is a base for $F_C(G, \mathbb{C})$. So $\mathrm{dim} F_C(G, \mathbb{C})$ is equal to the number of conjugacy classes of G, hence to the number of isomorphism classes of the irreducible representations V_i, by the above result.

Let V be a representation of G. By semisemplicity,

$$V = \oplus_i V[i], \tag{2.4}$$

where $V[i] \cong V_i^{\oplus n_i}$ is called the *isotypical* component of V. So we obtain the decomposition,

$$\mathrm{Hom}_G(V_i, V) \simeq \mathrm{Hom}_G(V_i, V_i)^{\oplus n_i} \simeq \mathbb{C}^{\oplus n_i},$$

which is not at all unique. But, since

$$\chi_V = \sum_i n_i \chi_i,$$

then the number of copies of V_i in (2.4)

$$\dim(\mathrm{Hom}_G(V_i, V)) = \langle \chi_i, \chi_V \rangle_G = \sum_j n_j \langle \chi_i, \chi_j \rangle_G = n_i \tag{2.5}$$

is unique and it is called the *multiplicity* of V_i in V. In particular, we can denote the isotypical component of V corresponding to the trivial representation $\mathbb{C}$ by V^G.

Define

$$p_i := \frac{\dim V_i}{|G|} \sum_{\sigma \in G} \overline{\chi_i(\sigma)} \sigma.$$

Since $p_i \in \mathbb{C}[G]$, then

$$p_i|V_j \in \mathrm{End}_G(V_j) \simeq \mathbb{C}.$$

In particular,

$$p_i|V_j = \frac{1}{\dim V_j} \mathrm{Tr}(p_i|V_j),$$

where

$$\mathrm{Tr}(p_i|V_j) = \frac{\dim V_i}{|G|} \sum_{\sigma \in G} \overline{\chi_i(\sigma)} \chi_j(\sigma) = \dim V_i \cdot \langle \chi_j, \chi_i \rangle_G = \dim V_i \cdot \delta_{ij}.$$

Hence

$$p_i|V_j = \begin{cases} \mathrm{id}_{V_i} & \text{if } i = j \\ 0 & \text{if } i \neq j \end{cases},$$

that is p_i is the projection of V onto $V[i]$. So, if

$$x = \sum_i x_i \in V \text{ with } x_i \in V[i],$$

then

$$x_i = p_i(x) = \frac{\dim V_i}{|G|} \sum_{\sigma \in G} \overline{\chi_i(\sigma)} \sigma x.$$

Hence, the decomosition (2.4) is unique.

Let Rep_G denote the category of representations of G. Let $f : H \to G$ be a homomorphism of groups.

Definition 2.13. If $V \in \mathrm{Rep}_G$, then the adjoint functor

$$f^* : \mathrm{Rep}_G \to \mathrm{Rep}_H$$

gives a representation f^*V of H with the same underlying vector space as V and where H acts through f, that is,

$$\tau.x = f(\tau).x \text{ for } \tau \in H, x \in V.$$

The adjoint functor

$$f_* : \mathrm{Rep}_H \to \mathrm{Rep}_G$$

comes with the canonical elements

$$\iota_W \in \mathrm{Hom}_H(W, f^* f_* W) \text{ for } W \in \mathrm{Rep}_H,$$

and is characterized by the fact that for every $W \in \mathrm{Rep}_H$ and $V \in \mathrm{Rep}_G$, the map

$$\begin{aligned} \mathrm{Hom}_G(f_*W, V) &\to \mathrm{Hom}_H(W, f^*V) \\ \phi &\mapsto (f^*\phi) \circ \iota_W \end{aligned} \tag{2.6}$$

is bijective. Since we can decompose f as follows

$$\begin{tikzcd} H \arrow[r, two heads] \arrow[d, "f"'] & H/\mathrm{ker} f \arrow[d, "\simeq"] \\ G & \mathrm{Im} f \arrow[l, hook'] \end{tikzcd}$$

to describe f_* explicity, it suffices to treat the two following cases:

(a) $\pi : H \twoheadrightarrow H/N$, for some $N \trianglelefteq H$.

(b) $i : H \hookrightarrow G$.

Let $W \in \mathrm{Rep}_H$. In (a),

$$\pi_* W = W^N,$$

where the action of H/N is given by

$$hN.x = h.x \text{ for all } h \in H, x \in W^N.$$

Moreover, ι_W is the projection of W onto W^N defined as in the *Proposition 2.2.1.* In (b),

$$\iota_W : W \hookrightarrow i_* W$$

is an inclusion and

$$i_* W = \oplus_j \sigma_j W,$$

where the σ_j are representatives of the left cosets $\sigma_j H$ of H in G. Given $\sigma \in G$, the action of G on i_*W is defined by

$$\sigma.\left(\sum_j \sigma_j y_j\right) = \sum_j \sigma_{\sigma(j)} \tau_{\sigma,j}.y_j, \text{ for } y_j \in W,$$

where the subscript $\sigma(j)$ and $\tau_{\sigma,j} \in H$ are uniquely determined by

$$\sigma\sigma_j = \sigma_{\sigma(j)}\tau_{\sigma,j}.$$

In particular we have that:

- if χ_V is the character of a representation V of G, then

$$f^*\chi_V(\tau) \coloneqq \chi_V(f(\tau)), \text{ for } \tau \in H,$$

  is the character of f^*V;

- if ψ_W is the character of a representation W of H, then

$$f_*\psi_W(\sigma) \coloneqq \frac{1}{|H|}\sum_{\eta\in G}\ \sum_{\tau\in H:\ f(\tau)=\eta\sigma\eta^{-1}} \psi_W(\tau), \text{ for } \sigma \in G, \tag{2.7}$$

  is the character of f_*W (see [11, p. 14]).

Definition 2.14. Let H be a subgroup of G and let

$$f : H \hookrightarrow G$$

be the relative inslusion map.

- $\mathrm{res}^G_H V \coloneqq f^*V$ is called the ***restriction*** to H of the representation V of G.

- $\mathrm{Ind}^G_H W \coloneqq f_*W$ is called the representation of G ***induced by*** the representation W of H.

Let V be a representation of G. Equating the dimensions of the spaces on each side of the isomorphism (2.6), we obtain the relation

$$\langle f_*\psi_W, \chi_V\rangle_G = \langle \psi_W, f^*\chi_V\rangle_H, \tag{2.8}$$

called *Frobenius reciprocity* (see [10, Ch. 7, 10.2]).

Definition 2.15. A representation V of a group G and its character χ_V are called ***monomial*** if there exist a 1-dimensional representation W of a subgroup H of G such that

$$V = \mathrm{Ind}_H^G W,$$

or, equivalently, if V is a direct sum of 1-dimensional subspaces which are permutated transitevely by G.

Theorem 2.2.4 (Brauer)**.** *Every character χ of a finite group G is a linear combination with integral coefficients of monomial characters.*

Proof. See [12, Ch. 10, §5, Theorem 20]. □

Definition 2.16. The character

$$\chi_V : G \to \mathbb{C}^\times$$

of a 1-dimensional representation V of G is a group homomorphism called ***abelian character***.

The abelian characters form an abelian group $\mathrm{Hom}(G, \mathbb{C}^\times)$ under multiplication. Moreover, if G is abelian, they are the only irreducible characters. In fact, if

$$\rho : G \to GL(V)$$

be an irreducible complex representation, for any fixed $g \in G$, then

$$\rho(g)\rho(g') = \rho(gg') = \rho(g'g) = \rho(g')\rho(g), \text{ for each } g' \in G,$$

i.e.

$$\rho(g) : V \to V$$

is a G-equivariant map. Since V is irreducible, by *Theorem 2.2.3*,

$$\rho(g) = \lambda_g \mathrm{id}_V, \text{ for some } \lambda_g \in \mathbb{C}.$$

Therefore, every subspace of V is invariant under G. Due to irreducibility, V must be 1-dimensional.

Definition 2.17. If G is an abelian group, then

$$\hat{G} := \mathrm{Hom}(G, \mathbb{C}^\times)$$

is called the ***character group*** of G.

Consider the map

$$G \xrightarrow{\varphi} \hat{\hat{G}}$$

defined by

$$\begin{aligned}\varphi(g) : \hat{G} &\to \mathbb{C}^\times \\ \chi &\mapsto \chi(g)\end{aligned}$$

First, note that φ is injective. In fact, let $g \in G$ sucht that

$$\chi(g) = \varphi(g)(\chi) = \chi_{\mathbb{C}}(g) = 1 \text{ for all } \chi \in \hat{G}.$$

Assume $g \neq 1$. Consider

$$|G| = p_1^{e_1} \cdot \ldots \cdot p_r^{e_r},$$

where $p_1, \ldots, p_r$ are primes and $e_1, \ldots, e_r \in \mathbb{N}_{\geq 1}$. Then

$$G \cong C_{p_1^{e_1}} \times \ldots \times C_{p_r^{e_r}}$$

with

$$C_{p_i^{e_i}} = \langle g_i \rangle \text{ for each } i = 1, \ldots, r.$$

So, we can write

$$g = (g_1^{\alpha_1}, \ldots, g_r^{\alpha_r}),$$

for some $\alpha_1, \ldots, \alpha_r \in \mathbb{N}$. Since $g \neq 1$, we can find $N \in \{1, \ldots, r\}$ sucht that

$$g_N^{\alpha_N} \neq 1.$$

Thus, if for each $i = 1, \ldots, r$ we choose a $p_i^{e_i}$-th root of unity $\zeta_i \in \mathbb{C}$, we can define a character of χ of G as

$$\chi(1, \ldots, 1, g_i, 1, \ldots, 1) = \zeta_i$$

for all $i = 1, \ldots, r$. Then, we have that

$$\chi(g) = \chi(g_1^{\alpha_1}, \ldots, g_r^{\alpha_r}) = \prod_{i=1}^{r} \zeta_i^{\alpha_i} \neq 1.$$

Now, let $\chi \in \hat{G}$. Note that, χ is completely determined by

$$\chi(g_i) = \zeta_i \text{ for each } i = 1, \ldots, r,$$

where ζ_i are $p_i^{e_i}$-th root of unity. Then we have the bijective correspondence

$$\hat{G} \overset{1:1}{\longleftrightarrow} \{(\zeta_1, \ldots, \zeta_r) : \zeta_i^{p_i^{e_i}} = 1,\ i = 1, \ldots, r\}. \tag{2.9}$$

By (2.9), we have

$$|\hat{G}| = p_1^{e_1} \cdot \ldots \cdot p_r^{e_r} = |G|.$$

It follows that

$$|G| = |\hat{G}| = |\hat{\hat{G}}|. \tag{2.10}$$

Then, by the injectivity of φ, (2.10) implies

$$G \cong \hat{\hat{G}}. \tag{2.11}$$

Moreover, the map

$$\mathrm{Hom}(G_1, G_2) \xrightarrow{\psi} \mathrm{Hom}(\hat{G}_2, \hat{G}_1)$$

defined by

$$\begin{aligned} \psi(f) : \hat{G}_2 &\to \hat{G}_1 \\ h &\mapsto h \circ f \end{aligned}$$

is also an isomorphism. In fact, let $f, g \in \mathrm{Hom}(G_1, G_2)$ such that

$$\psi(f) = \psi(g). \tag{2.12}$$

By (2.12), for all $h \in \hat{G}_2$,

$$h \circ f = \psi(f)(h) = \psi(g)(h) = h \circ g.$$

In particular, if h is the trivial representation of G_2, then

$$f(\sigma) = g(\sigma) \text{ for all } \sigma \in G_2.$$

Thus, ψ is injective.

Now, by the isomorphism (2.11), we have that

$$\mathrm{Hom}(G_1, G_2) \cong \mathrm{Hom}(\hat{\hat{G}}_1, \hat{\hat{G}}_2).$$

In particular,

$$|\mathrm{Hom}(G_1, G_2)| = |\mathrm{Hom}(\hat{\hat{G}}_1, \hat{\hat{G}}_2)|. \tag{2.13}$$

Moreover, by the injectivity of ψ, we obtain the composition of embeddings

$$\mathrm{Hom}(G_1, G_2) \hookrightarrow \mathrm{Hom}(\hat{G}_2, \hat{G}_1) \hookrightarrow \mathrm{Hom}(\hat{\hat{G}}_1, \hat{\hat{G}}_2).$$

Then, by (2.13), we obtain

$$|\mathrm{Hom}(G_1, G_2)| = |\mathrm{Hom}(\hat{G}_2, \hat{G}_1)|.$$

Finally, by the injectivity of ψ, we can conclude that

$$\mathrm{Hom}(G_1, G_2) \cong \mathrm{Hom}(\hat{G}_2, \hat{G}_1).$$

Chapter 3

L-functions

3.1 Ideal class characters

Definition 3.1. A ***level*** is a pair $\mathfrak{m} = (\mathfrak{m}_f, \mathfrak{m}_\infty)$ where

- $\mathfrak{m}_f$ is an ideal in $\mathcal{O}_k$;
- $\mathfrak{m}_\infty$ is a set of real places of k.

In particular,

$$\mathfrak{m}_f = \prod_{P_v | \mathfrak{m}_f} P_v^{\mathfrak{m}_v},$$

where the P_v are finite places of k and $\mathfrak{m}_v \in \mathbb{N}$.

Definition 3.2. For $a, b \in \mathcal{O}_k$, we write

$$a \equiv b \bmod^\times \mathfrak{m}$$

if

- a and b are prime to $\mathfrak{m}$;
- $a \equiv b \bmod \mathfrak{m}_f$, i.e. $a - b \in \mathfrak{m}_f$;
- $\sigma_v(a/b) > 0$ for each place $v \in \mathfrak{m}_\infty$.

Definition 3.3. A ***fractional ideal*** of $\mathcal{O}_k$ is a $\mathcal{O}_k$-submodule I of k such that $aI \subset \mathcal{O}_k$ for some $a \in \mathcal{O}_k \setminus \{0\}$.

Denote with $\mathcal{I}_k$ the group of fractional ideal in k. Let

$$k_{m,1} = \{c \in k^\times : \ c = a/b \text{ for some } a, b \in \mathcal{O}_k \text{ with } a \equiv b \bmod^\times \mathfrak{m}\}.$$

Let $\mathcal{I}_\mathfrak{m}$ denote the group of fractional ideals prime to the level $\mathfrak{m} = (\mathfrak{m}_f, \mathfrak{m}_\infty)$, i.e. generated by prime ideals not dividing $\mathfrak{m}_f$. Since, for any $c \in k_{m,1}$, the ideal (c) lies in $\mathcal{I}_\mathfrak{m}$, then the map

$$\begin{aligned} i : k_{m,1} &\to \mathcal{I}_\mathfrak{m} \\ c &\mapsto (c) \end{aligned}$$

is well defined. Set

$$\mathcal{P}_m := i(k_{m,1}).$$

Definition 3.4. The quotient group

$$\mathcal{C}_\mathfrak{m} := \mathcal{I}_\mathfrak{m}/\mathcal{P}_\mathfrak{m}$$

is called the ***ray class group modulo*** $\mathfrak{m}$.

Lemma 3.1.1. *Every pair of homomorphisms*

$$A \xrightarrow{f} B \xrightarrow{g} C$$

of abelian groups gives rise to an exact sequence

$$0 \to \mathrm{Ker}\ f \to \mathrm{Ker}\ g \circ f \to \mathrm{Ker}\ g \to \mathrm{Coker}\ f \to \mathrm{Coker}\ g \circ f \to \mathrm{Coker}\ g \to 0.$$

Proof. See [9, Lemma A.2]. □

Theorem 3.1.2. *Let k be a field and let*

$$| - |_1, ..., | - |_n$$

be pairwise inequivalent nontrivial absolute values on k. Let $a_1, ..., a_n \in k$ and let $\varepsilon_1, ..., \varepsilon_n$ be positive real numbers. Then there exists $x \in k$ such that

$$|x - a_i|_i < \varepsilon_i \text{ for } 1 \leq i \leq n.$$

Proof. See [10, Ch. 2, Theorem 3.4]. □

Theorem 3.1.3. *For every level $\mathfrak{m} = (\mathfrak{m}_f, \mathfrak{m}_\infty)$ of k, there is an exact sequence*

$$\mathcal{O}_k^\times \to (\mathcal{O}_k/\mathfrak{m}_f)^\times \times \{\pm 1\}^{\mathfrak{m}_\infty} \to \mathcal{C}_\mathfrak{m} \to \mathcal{C}_k \to 0,$$

where

- $\mathcal{C}_k = \mathcal{C}_1$ *is the usual ideal class group;*

- $\{\pm 1\}^{\mathfrak{m}_\infty}$ *denotes the product of* $|\mathfrak{m}_\infty|$ *groups of order two, representing the possible choices of signs at the real places* $v \in \mathfrak{m}_\infty$.

Proof. Define the map

$$\begin{aligned} g : k_{\mathfrak{m}} &\to \mathcal{I}_{\mathfrak{m}} \\ c &\mapsto (c) \end{aligned}$$

where

$$k_{\mathfrak{m}} = \{a \in k^\times : \ a \text{ is prime to } \mathfrak{m}\}.$$

Then the sequence

$$0 \to \mathcal{O}_k^\times \to k_{\mathfrak{m}} \xrightarrow{g} \mathcal{I}_{\mathfrak{m}} \to \mathcal{C}_k \to 0 \tag{3.1}$$

is exact. In fact, let $I \in \mathcal{I}_k$. Since k is a Dedekind domain, I admits a unique prime ideal factorization

$$I = \prod_{\mathfrak{p}} \mathfrak{p}^{n_{\mathfrak{p}}}.$$

In particular, we may write

$$I = I_1 I_2,$$

where

$$I_1 := \prod_{\mathfrak{p} \nmid \mathfrak{m}_f} \mathfrak{p}^{n_{\mathfrak{p}}} \text{ and } I_2 := \prod_{\mathfrak{p} | \mathfrak{m}_f} \mathfrak{p}^{n_{\mathfrak{p}}}$$

are coprime. If we hoose a uniformizer $\pi_{\mathfrak{p}}$ for each $\mathfrak{p}|\mathfrak{m}_f$ and set

$$\alpha := \prod_{\mathfrak{p}|\mathfrak{m}_f} \pi_{\mathfrak{p}}^{-n_{\mathfrak{p}}},$$

then αI and I represent the same ideal class in $\mathcal{C}_k$. Therefore, since $\alpha I \in \mathcal{I}_{\mathfrak{m}}$, we can conclude that the cokernel of g is $\mathcal{C}_k$.

Consider the composition of maps

$$k_{\mathfrak{m},1} \overset{f}{\hookrightarrow} k_{\mathfrak{m}} \xrightarrow{g} \mathcal{I}_{\mathfrak{m}}. \tag{3.2}$$

By (3.1), the kernel of (3.2) is

$$k_{\mathfrak{m},1} \cap \mathcal{O}_k^\times,$$

and its cokernel is

$$\mathcal{I}_{\mathfrak{m}}/g(k_{\mathfrak{m},1}) = \mathcal{I}_{\mathfrak{m}}/\mathcal{P}_{\mathfrak{m}} = \mathcal{C}_{\mathfrak{m}}.$$

Hence, by *Lemma 3.1.1*, we obtain the exact sequence

$$0 \to k_{\mathfrak{m},1} \cap \mathcal{O}_k^\times \to \mathcal{O}_k^\times \to k_\mathfrak{m}/k_{\mathfrak{m},1} \to \mathcal{C}_\mathfrak{m} \to \mathcal{C}_k \to 0.$$

Note that we can write each $c \in k_\mathfrak{m}$ as $c = a/b$ for some $a, b \in \mathcal{O}_k$ such that (a) and (b) are coprime to $\mathfrak{m}_f$ and to each other. In particular, the ideals (a) and (b) are uniquely determined by c, even though a and b are not. In fact, if we assume

$$a/b = a'/b',$$

then

$$ab' = a'b.$$

Hence, we obtain

$$(a)(b') = (a')(b).$$

Since (a) and (b) are coprime to each other, we must have

$$(a) = (a') \text{ and } (b) = (b'),$$

by unique factorization of ideals. We now define the homomorphism

$$\begin{aligned} \varphi : k_\mathfrak{m} &\to (\mathcal{O}_k/\mathfrak{m}_f)^\times \times \{\pm 1\}^{\mathfrak{m}_\infty} \\ c &\mapsto \bar{c} \times \prod_{v \in \mathfrak{m}_\infty} \operatorname{sgn}(\sigma_v(c)) \end{aligned}$$

where

$$\bar{c} = \bar{a}\bar{b}^{-1} \in (\mathcal{O}_k/\mathfrak{m}_f)^\times,$$

because $\bar{a}, \bar{b} \in (\mathcal{O}_k/\mathfrak{m}_f)^\times$, since (a) and (b) are coprime to $\mathfrak{m}_f$. In particular, φ is a canonical homomorphism, because $\bar{c}$ depends only on the uniquely determined ideals (a) and (b). In fact, if we replace a with $a' = au$ for some $u \in \mathcal{O}_k$, we must replace b with $b' = bu$.

Now, we want to prove that φ is surjective. So, let

$$\overline{a} \times \prod_{v \in \mathfrak{m}_\infty} (-1)^{m_v} \in (\mathcal{O}_k/\mathfrak{m}_f)^\times \times \{\pm 1\}^{\mathfrak{m}_\infty},$$

where $a \in \mathcal{O}_k$ and $m_v \in \{0, 1\}$. First, note that, by the Chinese remainder theorem,

$$(\mathcal{O}_k/\mathfrak{m}_f)^\times \cong \prod_{P_v | \mathfrak{m}_f} (\mathcal{O}_k/P_v^{n_v})^\times.$$

For each finite absolute value v of k such that $P_v | \mathfrak{m}_f$, let $a_v \in \mathcal{O}_k$ with $\overline{a_v} \in (\mathcal{O}_k/P_v^{n_v})^\times$ such that

$$a \equiv a_v \bmod P_v^{n_v}. \tag{3.3}$$

Thus, by *Theorem 3.1.2*, there exists $c \in k$ such that

$$(\mathbf{N}P_v)^{-\mathrm{ord}_{P_v}(c-a_v)} = |c - a_v|_v < (\mathbf{N}P_v)^{-n_v},$$

for each finite absolute value v of k such that $P_v|\mathfrak{m}_f$, and

$$|\sigma_v(c - (-1)^{m_v})| = |c - (-1)^{m_v}|_v < \frac{1}{2},$$

for all $v \in \mathfrak{m}_\infty$. Equivalently,

$$c \equiv a \bmod \mathfrak{m}_f,$$

and

$$\mathrm{sgn}(\sigma_v(c)) = (-1)^{m_v},$$

for all $v \in \mathfrak{m}_\infty$.

It remains to check that $c \in k_\mathfrak{m}$. By contradiction, assume that

$$((c), \mathfrak{m}_f) \neq 1.$$

Then, there exists a finite absolute value v_0 of k such that

$$P_{v_0}|(c) \text{ and } P_{v_0}|\mathfrak{m}_f.$$

This means that

$$c \notin (\mathcal{O}_k/P_{v_0}^{n_{v_0}})^\times,$$

which is a contradiction by (3.3).

Finally, since the kernel of φ is $k_{\mathfrak{m},1}$, thus φ induces the isomorphism

$$k_\mathfrak{m}/k_{\mathfrak{m},1} \cong (\mathcal{O}_k/\mathfrak{m}_f)^\times \times \{\pm 1\}^{\mathfrak{m}_\infty}.$$

Hence we obtain the exact sequence

$$\mathcal{O}_k^\times \to (\mathcal{O}_k/\mathfrak{m}_f)^\times \times \{\pm 1\}^{\mathfrak{m}_\infty} \to \mathcal{C}_\mathfrak{m} \to \mathcal{C}_k \to 0.$$

□

Corollary 3.1.4. *The group $\mathcal{C}_\mathfrak{m}$ is finite.*

Proof. By *Theorem 3.1.3*, we have the exact sequence

$$\mathcal{O}_k^\times \to (\mathcal{O}_k/\mathfrak{m}_f)^\times \times \{\pm 1\}^{\mathfrak{m}_\infty} \to \mathcal{C}_\mathfrak{m} \to \mathcal{C}_k \to 0.$$

By the finiteness of $\mathcal{C}_k$ (see [10, Ch. 1, Theorem 6.3]), we can conclude. □

Definition 3.5. Let $\mathfrak{m}$ be a level for a number field k. A ***(generalized) ideal class character*** mod $\mathfrak{m}$ is a group homomorphism

$$\chi : \mathcal{I}_{\mathfrak{m}} \to \mathbb{C}^*$$

which is trivial on $\mathcal{P}_{\mathfrak{m}}$. In particular, χ is the same as a character of the group $\mathcal{C}_{\mathfrak{m}}$.

Note that, for each $a \in \mathcal{C}_{\mathfrak{m}}$,

$$\chi(a)^{|a|} = \chi(a^{|a|}) = \chi(1) = 1,$$

i.e. the values of an ideal class character χ are complex roots of 1. In particular, they have absolute value 1.

Example 3. A function

$$f : \mathbb{Z} \to \mathbb{C}$$

is called an *arithmetic function*. We say that f is *multiplicative* if

$$f(mn) = f(m)f(n)$$

holds for all relatively prime $m, n \in \mathbb{Z}$, and *totally multiplicative* (or *completely multiplicative*) if this holds for all $m, n \in \mathbb{Z}$. For $m \in \mathbb{Z}_{\geq 1}$, we say that f is *m-periodic* if

$$f(n + m) = f(n)$$

for all $n \in \mathbb{Z}$, and call m the *period* of f if it is the least m for which this holds.

A *Dirichlet character* is an arithmetic function

$$\chi : \mathbb{Z} \to \mathbb{C}$$

that is both totally multiplicative and periodic.

Note that each m-periodic Dirichlet character χ restricts to a group character χ on $(\mathbb{Z}/m\mathbb{Z})^\times$. Conversely, every group character χ of $(\mathbb{Z}/m\mathbb{Z})^\times$ can be extended to a Dirichlet character χ by defining

$$\chi(n) = 0 \text{ for } n \notin (\mathbb{Z}/m\mathbb{Z})^\times.$$

A *Dirichlet character mod m* is an m-periodic Dirichlet character χ that is the zero-extension of a group character on $(\mathbb{Z}/m\mathbb{Z})^\times$. Equivalently, a character for which

$$n \in (\mathbb{Z}/m\mathbb{Z})^\times \Leftrightarrow \chi(n) \neq 0.$$

Let $k = \mathbb{Q}$. If we identify ideals prime to $m \in \mathbb{Z}$ with their positive integer generators, then an ideal class character mod $(m\mathbb{Z}, \{\infty\})$ is the same as a Dirichlet character mod m (see [11, p. 10]).

Note that the set of levels of a number field is partially ordered under the relation

$$\mathfrak{m}_1 \leq \mathfrak{m}_2 \Leftrightarrow (\mathfrak{m}_1)_f | (\mathfrak{m}_2)_f \text{ and } (\mathfrak{m}_1)_\infty \subset (\mathfrak{m}_2)_\infty. \tag{3.4}$$

In particular, if $\mathfrak{m}_1 \leq \mathfrak{m}_2$, the identity map on ideals induces a surjective homomorphism

$$\mathcal{C}_{\mathfrak{m}_2} \to \mathcal{C}_{\mathfrak{m}_1}. \tag{3.5}$$

This allows us to identify characters mod $\mathfrak{m}_1$ with certain characters mod $\mathfrak{m}_2$.

Definition 3.6. Let k be a number field and let $\mathfrak{m}$ be a level of k. A ***congruence subgroup*** for the level $\mathfrak{m}$ is a subgroup $\mathcal{C}$ of $\mathcal{I}_\mathfrak{m}$ that contains $\mathcal{P}_\mathfrak{m}$.

Example 4. Let $\mathfrak{m}$ be a level for a number field k. The kernel of an ideal class character mod $\mathfrak{m}$ is a congruence subgroup.

Definition 3.7. Let $\mathfrak{m}_1$ and $\mathfrak{m}_2$ be two level of a number field k. If $\mathcal{C}_1$ is a congruence subgroup for $\mathfrak{m}_1$ and $\mathcal{C}_2$ is a congruence subgroup for $\mathfrak{m}_2$, then we say that $\mathcal{C}_1$ and $\mathcal{C}_2$ are ***equivalent*** and write $\mathcal{C}_1 \sim \mathcal{C}_2$ whenever

$$\mathcal{I}_{\mathfrak{m}_1} \cap \mathcal{C}_2 = \mathcal{I}_{\mathfrak{m}_2} \cap \mathcal{C}_1,$$

as subgroups of $\mathcal{I}_k$.

If $\mathcal{C}_1$ and $\mathcal{C}_2$ have the same level $\mathfrak{m}_1 = \mathfrak{m}_2$, then

$$\mathcal{C}_1 \sim \mathcal{C}_2 \Leftrightarrow \mathcal{C}_1 = \mathcal{C}_2.$$

In fact, if $\mathcal{C}_1$ and $\mathcal{C}_2$ are equivalent, then

$$\mathcal{C}_1 = \mathcal{I}_{\mathfrak{m}_1} \cap \mathcal{C}_1 = \mathcal{I}_{\mathfrak{m}_2} \cap \mathcal{C}_1 = \mathcal{I}_{\mathfrak{m}_1} \cap \mathcal{C}_2 = \mathcal{I}_{\mathfrak{m}_2} \cap \mathcal{C}_2 = \mathcal{C}_2.$$

On the other hand, if $\mathcal{C}_1 = \mathcal{C}_2$, then

$$\mathcal{I}_{\mathfrak{m}_1} \cap \mathcal{C}_2 = \mathcal{I}_{\mathfrak{m}_2} \cap \mathcal{C}_2 = \mathcal{I}_{\mathfrak{m}_2} \cap \mathcal{C}_1.$$

By this, within an equivalence class of congruence subgroups there can be at most one congruence subgroup for each level. Thus the partial ordering of levels (3.4) induces a partial ordering of the congruence subgroups within an equivalence class.

Lemma 3.1.5. *Let $\mathcal{C}_1$ be a congruence subgroup of level $\mathfrak{m}_1$ for a number field k. There exists a congruence subgroup $\mathcal{C}_2$ of level $\mathfrak{m}_2|\mathfrak{m}_1$ equivalent to $\mathcal{C}_1$ if and only if*

$$\mathcal{I}_{\mathfrak{m}_1} \cap \mathcal{P}_{\mathfrak{m}_2} \subset \mathcal{C}_1.$$

In which case

$$\mathcal{C}_2 = \mathcal{C}_1\mathcal{P}_{\mathfrak{m}_2}.$$

Proof. Let $\mathfrak{m}_2$ be a level of k such that $\mathfrak{m}_2|\mathfrak{m}_1$. This implies

$$\mathcal{C}_1 \subset \mathcal{I}_{\mathfrak{m}_1} \subset \mathcal{I}_{\mathfrak{m}_2}.$$

Now, suppose there exists a congruence subgroup $\mathcal{C}_2 \sim \mathcal{C}_1$ of level $\mathfrak{m}_2$. Then

$$\mathcal{I}_{\mathfrak{m}_1} \cap \mathcal{P}_{\mathfrak{m}_2} \subset \mathcal{I}_{\mathfrak{m}_1} \cap \mathcal{C}_2 = \mathcal{I}_{\mathfrak{m}_2} \cap \mathcal{C}_1 = \mathcal{C}_1,$$

because $\mathcal{P}_{\mathfrak{m}_2} \subset \mathcal{C}_2$. On the other hand, assume

$$\mathcal{I}_{\mathfrak{m}_1} \cap \mathcal{P}_{\mathfrak{m}_2} \subset \mathcal{C}_1.$$

Define the congruence subgroup of level $\mathfrak{m}_2$

$$\mathcal{C}_2 \coloneqq \mathcal{C}_1\mathcal{P}_{\mathfrak{m}_2}.$$

Since

$$\mathcal{C}_1(\mathcal{I}_{\mathfrak{m}_1} \cap \mathcal{P}_{\mathfrak{m}_2}) = \mathcal{I}_{\mathfrak{m}_1} \cap \mathcal{C}_1\mathcal{P}_{\mathfrak{m}_2} = \mathcal{I}_{\mathfrak{m}_1} \cap \mathcal{C}_2,$$

and

$$\mathcal{C}_1(\mathcal{I}_{\mathfrak{m}_1} \cap \mathcal{P}_{\mathfrak{m}_2}) \subset \mathcal{C}_1\mathcal{C}_1 = \mathcal{C}_1,$$

then

$$\mathcal{I}_{\mathfrak{m}_1} \cap \mathcal{C}_2 \subset \mathcal{C}_1.$$

In particular,

$$\mathcal{I}_{\mathfrak{m}_1} \cap \mathcal{C}_2 = \mathcal{C}_1,$$

because

$$\mathcal{C}_1 \subset \mathcal{I}_{\mathfrak{m}_1} \text{ and } \mathcal{C}_1 \subset \mathcal{C}_2.$$

Therefore,

$$\mathcal{I}_{\mathfrak{m}_1} \cap \mathcal{C}_2 = \mathcal{C}_1 = \mathcal{I}_{\mathfrak{m}_2} \cap \mathcal{C}_1.$$

Finally, since the equivalence class of $\mathcal{C}_1$ contains at most one congruence subgroup of level $\mathfrak{m}_2$, if one exists it must be

$$\mathcal{C}_2 = \mathcal{C}_1\mathcal{P}_{\mathfrak{m}_2}.$$

$\square$

Proposition 3.1.6. *Let $\mathcal{C}_1$ and $\mathcal{C}_2$ be equivalent congruence subgroups of level $\mathfrak{m}_1$ and $\mathfrak{m}_2$, respectively. There exists a congruence subgroup $\mathcal{C}$ equivalent to $\mathcal{C}_1$ and $\mathcal{C}_2$ of level $\mathfrak{n} := \gcd(\mathfrak{m}_1, \mathfrak{m}_2)$.*

Proof. Put

$$\mathfrak{m} := \operatorname{lcm}(\mathfrak{m}_1, \mathfrak{m}_2),$$

and

$$\mathcal{D} := \mathcal{I}_{\mathfrak{m}_1} \cap \mathcal{C}_2 = \mathcal{I}_{\mathfrak{m}_2} \cap \mathcal{C}_1.$$

Then

$$\mathcal{P}_{\mathfrak{m}} = \mathcal{P}_{\mathfrak{m}_1} \cap \mathcal{P}_{\mathfrak{m}_2} \subset \mathcal{D} \subset \mathcal{I}_{\mathfrak{m}_1} \cap \mathcal{I}_{\mathfrak{m}_2} = \mathcal{I}_{\mathfrak{m}},$$

i.e. $\mathcal{D}$ is a congruence subgroup of level $\mathfrak{m}$. In particular,

$$\mathcal{I}_{\mathfrak{m}} \cap \mathcal{P}_{\mathfrak{m}_1} = \mathcal{I}_{\mathfrak{m}_2} \cap \mathcal{P}_{\mathfrak{m}_1} \subset \mathcal{I}_{\mathfrak{m}_2} \cap \mathcal{C}_1 = \mathcal{D},$$

and similarly

$$\mathcal{I}_{\mathfrak{m}} \cap \mathcal{P}_{\mathfrak{m}_2} \subset \mathcal{D}.$$

Thus, by *Lemma 3.1.5*,

$$\mathcal{D} \sim \mathcal{C}_1 \sim \mathcal{C}_2.$$

Now, let

$$\mathfrak{a} := (\alpha) \in \mathcal{I}_{\mathfrak{m}} \cap \mathcal{P}_{\mathfrak{n}}.$$

By *Theorem 3.1.2*, we can choose $\beta \in k_{\mathfrak{m}} \cap k_{\mathfrak{m}_2,1}$ such that

$$\alpha\beta \in k_{\mathfrak{m}_1,1}.$$

Since

$$(\beta) \in \mathcal{I}_{\mathfrak{m}} \cap \mathcal{P}_{\mathfrak{m}_2} \subset \mathcal{D},$$

and

$$\beta\mathfrak{a} = (\alpha\beta) \in \mathcal{I}_{\mathfrak{m}} \cap \mathcal{P}_{\mathfrak{m}_1} \subset \mathcal{D},$$

then

$$\mathfrak{a} = \beta^{-1}\beta\mathfrak{a} \in \mathcal{D}.$$

By this,

$$\mathcal{I}_{\mathfrak{m}} \cap \mathcal{P}_{\mathfrak{n}} \subset \mathcal{D}.$$

Therefore, by *Lemma 3.1.5*,

$$\mathcal{C} := \mathcal{D}\mathcal{P}_{\mathfrak{n}}$$

is a congruence subgroup of level $\mathfrak{n}$ equivalent to $\mathcal{D} \sim \mathcal{C}_1 \sim \mathcal{C}_2$. □

Corollary 3.1.7. *Let $\mathcal{C}$ be a congruence subgroup of level $\mathfrak{m}$ for a number field k. There exists a unique congruence subgroup in the equivalence class of $\mathcal{C}$ whose level $\mathfrak{c}$ divides the level of every congruence subgroup equivalent to $\mathcal{C}$.*

Definition 3.8. Let $\mathcal{C}$ be a congruence subgroup of level $\mathfrak{m}$ for a number field k. The unique level given by *Corollary 3.1.7* is called the ***conductor*** of $\mathcal{C}$, denoted $\mathfrak{c}(\mathcal{C})$. If the conductor of $\mathcal{C}$ is equal to its level, then we say that $\mathcal{C}$ is ***primitive***.

Definition 3.9. Let $\mathfrak{m}$ be a level for a number field k. Let χ be an ideal class character mod $\mathfrak{m}$. The ***conductor*** $\mathfrak{m}_\chi$ of χ is the conductor of its kernel. We say that χ is ***primitive*** mod $\mathfrak{m}_\chi$ and ***imprimitive*** mod $\mathfrak{m}$ for all $\mathfrak{m} > \mathfrak{m}_\chi$.

3.2 Classical abelian L-functions

Definition 3.10. Let χ be an ideal class character of conductor $\mathfrak{m}_\chi$. A ***classical abelian L-function***

$$L(s,\chi) := \prod_P \frac{1}{1-\chi(P)\mathbf{N}P^{-s}}$$

is a function of complex variable s, defined in the right half-plane $\Re(s) > 1$ and where the product is over the prime ideals P not dividing $\mathfrak{m}_\chi$.

Proposition 3.2.1. *Let χ be an ideal class character of conductor $\mathfrak{m}_\chi$. Then*

$$L(s,\chi) = \sum_I \chi(I)\mathbf{N}I^{-s},$$

where the sum is over all the integral ideals I prime to $\mathfrak{m}_\chi$.

Proof. Consider the multiplicative function

$$X(I) := \chi(I)\mathbf{N}I^{-s}.$$

For $x > 0$ define

$$A_x = \{P \subset O_k : P \text{ prime ideal not dividing } \mathfrak{m}_\chi \text{ with } \mathbf{N}P \le x\}.$$

So

$$\begin{aligned}
\prod_{P\in A_x}(1-X(P))^{-1} &= \prod_{P\in A_x}\sum_{n=0}^{\infty} X(P)^n \\
&= \sum_{(\ldots,n_P,\ldots)}\prod_{P\in A_x} X(P)^{n_P} \\
&= \sum_{(\ldots,n_P,\ldots)} X\left(\prod_{P\in A_x} P^{n_P}\right) \\
&= \sum_{I} X(I),
\end{aligned}$$

where the last sum is over all the integral ideals I prime to $\mathfrak{m}_\chi$ whose prime factorization involves only prime ideals of the set A_x. Now, consider

$$\begin{aligned}
\log\left(\prod_{P}(1-X(P))^{-1}\right) &= \sum_{P}\log\left((1-X(P))^{-1}\right) = \sum_{P} -\log\left(1-X(P)\right) \\
&= \sum_{P} -\left(\sum_{n=1}^{\infty}(-1)^{n+1}\frac{(-X(P))^n}{n}\right) \\
&= \sum_{P}\sum_{n=1}^{\infty}(-1)^{2(n+1)}\frac{(X(P))^n}{n} \\
&= \sum_{P}\sum_{n=1}^{\infty}\frac{(X(P))^n}{n},
\end{aligned}$$

where the sum is over the prime ideals P not dividing $\mathfrak{m}_\chi$. Note that it converges absolutely for $\Re(s)=\sigma>1$. In fact, since

$$|X(P)| = |\mathbf{N}P^{-s}| = \mathbf{N}P^{-\sigma},$$

then

$$\sum_{P}\sum_{n=1}^{\infty}\frac{|X(P)|^n}{n} < \sum_{P}\sum_{n=1}^{\infty}\left(\frac{1}{\mathbf{N}P^{\sigma}}\right)^n = \sum_{P}\frac{\mathbf{N}P^{-\sigma}}{1-\mathbf{N}P^{-\sigma}} = \sum_{P}\frac{1}{\mathbf{N}P^{\sigma}-1}.$$

Since

$$\mathbf{N}P \geq p,$$

for all prime ideal P of $\mathcal{O}_k$ over a prime $p\in\mathbb{Z}$, then

$$\frac{\mathbf{N}P^{\sigma}}{2} > \frac{\mathbf{N}P}{2} \geq 1,$$

that is
$$\frac{1}{\mathbf{N}P^\sigma - 1} < \frac{2}{\mathbf{N}P^\sigma}.$$
So we obtain the inequality
$$\sum_P \sum_{n=1}^{\infty} \frac{|X(P)|^n}{n} < 2\sum_P \frac{1}{\mathbf{N}P^\sigma} = 2\sum_P |X(P)|.$$
Now, since
$$|\{P : P \text{ is a prime ideal over the prime } p \in \mathbb{Z}\}| \leq [k : \mathbb{Q}],$$
we have that
$$\sum_P |X(P)| \leq \sum_P \mathbf{N}P^{-\sigma} \leq [k : \mathbb{Q}] \cdot \sum_p p^{-\sigma}.$$
Moreover, if we compare the sum
$$\sum_p p^{-\sigma}$$
with the integral
$$\int_1^\infty x^{-\sigma} dx = \lim_{n\to\infty} \int_1^n x^{-\sigma} dx = \lim_{n\to\infty} \left[\frac{x^{1-\sigma}}{1-\sigma}\right]_1^n = \lim_{n\to\infty} \frac{n^{1-\sigma} - 1}{1-\sigma} = \frac{1}{\sigma - 1},$$
we can conclude that
$$\sum_P \sum_{n=1}^{\infty} \frac{|X(P)|^n}{n} < 2\sum_P |X(P)| \leq \frac{2[k : \mathbb{Q}]}{\sigma - 1}.$$
This implies the absolute convergence of
$$\log\left(\prod_P (1 - X(P))^{-1}\right)$$
for $\Re(s) = \sigma > 1$. Finally, since
$$\prod_P (1 - X(P))^{-1} = \exp\left(\sum_P \sum_{n=1}^{\infty} \frac{(X(P))^n}{n}\right),$$
then
$$\prod_{P \in A_x} (1 - X(P))^{-1}$$
converges absolutely and uniformly in $\Re(s) = \sigma > 1$ as $x \to \infty$. □

For $\chi = 1$, the zeta function

$$\zeta_k(s) := L(s, 1)$$

is analytic in the whole plane except for a simple pole in $s = 1$ (see [10, Ch. 7, Corollary 1.7]).

If $\chi \neq 1$, Hecke proved that $L(s, \chi)$ has an analytic continuation to the whole s-plane. Moreover, he gives a functional equation relating $L(1 - s, \chi)$ and $L(s, \bar{\chi})$ (see [10, Ch. 7, §2]). To express it, we need the gamma function

$$\Gamma(z) = \int_0^\infty x^{z-1} e^{-x} dx, \ \Re(z) > 0.$$

Consider some of its properties.

1. It is a meromorphic function on the complex plane.
2. It satisfies
$$\Gamma(s + 1) = s\Gamma(s) \text{ and } \Gamma(1) = 1.$$
Hence
$$\Gamma(n + 1) = n! \text{ for } n = 1, 2, ...$$
3. It is nowhere zero and has simple poles only at
$$s = -n \text{ where } n = 0, 1, 2, ...,$$
with residue
$$\frac{(-1)^n}{n!}.$$
4. It satisfies the Legendre duplication formula
$$\Gamma\Big(\frac{s}{2}\Big)\Gamma\Big(\frac{s+1}{2}\Big) = 2^{1-s}\pi^{\frac{1}{2}}\Gamma(s).$$
Hence
$$\Gamma\Big(\frac{1}{2}\Big) = \sqrt{\pi}.$$

For a proof of these facts see [10, Ch. 7, Proposition 1.2]. So, for each infinite place v of k, define

$$\gamma_v(s, \chi) = \begin{cases} \Gamma(\frac{s}{2}) & \text{if } v \text{ is real and } v \notin (\mathfrak{m}_\chi)_\infty \\ \Gamma(\frac{s+1}{2}) & \text{if } v \text{ is real and } v \in (\mathfrak{m}_\chi)_\infty \\ \Gamma(\frac{s}{2})\Gamma(\frac{s+1}{2}) & \text{if } v \text{ is complex} \end{cases}.$$

Then there exist constants $B_\chi > 0$ and $C_\chi \in \mathbb{C}^*$ such that the functions

$$\Lambda(s,\chi) := \prod_{v|\infty} \gamma_v(s,\chi) L(s,\chi)$$

satisfy

$$\Lambda(1-s,\chi) = C_\chi B_\chi^s \Lambda(s,\bar{\chi}).$$

3.3 Artin L-functions

Let K/k be a finite Galois extension of number fields and $G = G_{K/k}$ its Galois group.

Definition 3.11. Let v be a place of k and let w be a place of K.

- If v is finite, then w ***lies above*** v if $w = P_w$ for some prime ideal P_w s.t. $P_w | P_v$.
- If v is infinite, then w ***lies above*** v if $w = \sigma'_v$ or $w = \{\sigma'_v, \bar{\sigma}'_v\}$ for some

$$\sigma'_v : K \to \mathbb{C}$$

  extending σ_v. In particular, if v is real, then w could be real or complex. If v is complex, then w must also be complex.

Let w be a place of K. G acts on w as follows:

- if w is finite, then

$$g.w = gP_w \text{ for each } g \in G;$$

- if w is real, then

$$g.w = \sigma_w \circ g \text{ for each } g \in G;$$

- if w is complex, then

$$g.w = \{\sigma_w \circ g, \bar{\sigma}_w \circ g\} \text{ for each } g \in G.$$

Proposition 3.3.1. *Let $v = P_v$ be a finite place of k. Then G acts transitively on the set*

$$\{w : \ w \text{ lies over } v\}.$$

Proof. Let w and w' be places of K lying over v. By contradiction, assume

$$\sigma.w \neq w' \text{ for all } \sigma \in G.$$

By the Chinese remainder theroem, we may choose $b \in w'$ such that

$$b \equiv 1 \bmod \sigma^{-1}.w \text{ for all } \sigma \in G.$$

Then

$$a := \mathbf{N}_{K/k}(b) = \prod_{\sigma \in G} \sigma(b) \equiv 1 \bmod w.$$

Thus

$$a \notin w, \text{ i.e. } a \notin k \cap w = v.$$

But

$$a = \mathbf{N}_{K/k}(b) \in \mathbf{N}_{K/k}(w') = P_v^{f_{\mathbb{F}_{w'}/\mathbb{F}_v}} \subset P_v = v,$$

where $f_{\mathbb{F}_{w'}/\mathbb{F}_v} = [\mathbb{F}_{w'} : \mathbb{F}_v]$, a contradiction. □

Definition 3.12. If w is a place of K which lies above a place v of k, its stabilizer

$$G_w := \{g \in G : g.w = w\}$$

is a subgroup of G called the ***decomposition group*** of w.

Proposition 3.3.2. *Let w be a place of K which lies above a place v of k. Then*

$$G_w \cong G_{K_w/k_v}$$

Proof. First note that the decomposition group G_w consists precisely of those automorphisms $\sigma \in G$ which are continuous with respect to the valuation w. Indeed, let $x \in K$ such that

$$|x|_w < 1. \tag{3.6}$$

If we consider $\sigma \in G_w$, then

$$|\sigma(x)|_w = |x|_{\sigma^{-1}.w} = |x|_w < 1.$$

On the other hand, consider an arbitrary continuous automorphism $\sigma \in G$. By (3.6), we have that $(x^n)_{n\in\mathbb{N}}$ is a w-nullsequence. By the continuity of σ, then

$$\lim_{n\to\infty} \sigma(x^n) = \sigma\left(\lim_{n\to\infty} x^n\right) = 0,$$

i.e.

$$((\sigma(x))^n)_{n\in\mathbb{N}} = ((\sigma(x^n))_{n\in\mathbb{N}}$$

is a w- nullsequence. Thus,

$$|x|_{\sigma.w} = |\sigma(x)|_w < 1. \tag{3.7}$$

The fact that (3.6) implies (3.7), is equivalent to the fact that w and $\sigma.w$ are equivalent, as we can view in [10, p. 117]. Moreover, since

$$w|_k = v = (\sigma.w)|_k,$$

then

$$w = \sigma.w, \text{ i.e. } \sigma \in G_w.$$

Now, since K is dense in K_w, then every automorphism $\sigma \in G_w$ extends to a continuous k_v-automorphism $\hat{\sigma}$ of K_w defined as

$$\hat{\sigma}(x) = \hat{\sigma}\left(\lim_{n\to\infty} x_n\right) = \lim_{n\to\infty} \hat{\sigma}(x_n) = \lim_{n\to\infty} \sigma(x_n),$$

for all $x \in K_w$ and for a suitable sequence $(x_n)_{n\in\mathbb{N}}$ in K. In particular, $\hat{\sigma}$ is unique. In fact, assume there exists another continuous k_v-automorphism $\hat{\sigma}'$ of K_w which extends σ. If $\hat{\sigma}'$ is different from $\hat{\sigma}$, then there exists $x \in K_w$ such that

$$\hat{\sigma}'(x) \neq \hat{\sigma}(x).$$

Since K is dense in K_w, then

$$x = \lim_{n\to\infty} x_n$$

for a suitable sequence $(x_n)_{n\in\mathbb{N}}$ in K. Thus,

$$\hat{\sigma}'(x) = \hat{\sigma}'\left(\lim_{n\to\infty} x_n\right) = \lim_{n\to\infty} \hat{\sigma}'(x_n) = \lim_{n\to\infty} \hat{\sigma}(x_n) = \hat{\sigma}\left(\lim_{n\to\infty} x_n\right) = \hat{\sigma}(x),$$

which is a contradiction. Hence, we obtain the well defined isomorphism

$$\begin{aligned} G_w &\to G_{K_w/k_v} \\ \sigma &\mapsto \hat{\sigma} \end{aligned}$$

□

If v is finite, an element $\sigma \in G_w$ induces an automorphism

$$\begin{aligned} \bar{\sigma} : \mathbb{F}_w &\to \mathbb{F}_w \\ \bar{y} &\mapsto \overline{\sigma(y)} \end{aligned}$$

where $\mathbb{F}_w = O_K/P_w$ is the residue field of w.

Proposition 3.3.3. *The map*

$$\pi_w : G_w \to \mathrm{Gal}(\mathbb{F}_w/\mathbb{F}_v)$$
$$\sigma \mapsto \bar{\sigma}$$

is a surjective group homomorphism.

Proof. First, note that π_w preserves the identity element. Moreover, for any $\sigma, \tau \in G_w$, we have

$$\overline{\sigma\tau}(\bar{y}) = \overline{\sigma\tau(y)} = \overline{\sigma(y)\tau(y)} = \overline{\sigma(y)}\,\overline{\tau(y)} = \bar{\sigma}(\bar{y})\bar{\tau}(\bar{y}),$$

because the action of G_w on O_K fixes w and commutes with quotienting by w. Thus, π_w is an homomorphism.

Since $\mathbb{F}_w/\mathbb{F}_v$ is a cyclic Galois extension, it is generated by some $\alpha \in \mathbb{F}_w^\times$. By the Chinese remainder theorem, we can pick $a \in O_K$ such that

$$a \equiv \alpha \bmod w,$$

and

$$a \equiv 0 \bmod \sigma^{-1}.w \text{ for all } \sigma \in G \setminus G_w. \tag{3.8}$$

Now, define

$$g(X) := \prod_{\sigma \in G} (X - \sigma(a)) \in O_k[X].$$

Let $\overline{g}$ denote the image of g in $\mathbb{F}_v[X]$. By (3.8), the image of $\sigma(a)$ in $\mathbb{F}_w$ is 0 for each $\sigma \in G \setminus G_w$. So 0 is a root of $\overline{g}$ with multiplicity $m = \#(G \setminus G_w)$. The remaining roots are $\overline{\sigma}(\alpha)$ for $\sigma \in G_w$, which are Galois conjugates of α. It follows that

$$\frac{\overline{g}(X)}{X^m} \tag{3.9}$$

divides the minimal polynomial of α, which is irreducible in $\mathbb{F}_v[X]$. Then (3.9) is the minimal polynomial of α. In particular, every conjugate of α is of the form

$$\overline{\sigma}(\alpha) \text{ for some } \sigma \in G_w.$$

Thus π_w is surjective. □

Definition 3.13. The kernel of π_w is called the ***inertia group*** of w and is detoned by I_w.

The order of I_w is the ramification index $e_{\mathbb{F}_w/\mathbb{F}_v}$. It is 1 for all but a finite number of places v, those dividing the relative discriminant ideal $d_{K/k}$. By π_w, we can view the quotient group G_w/I_w as the Galois group of the finite field extension $\mathbb{F}_w/\mathbb{F}_v$. Hence, G_w/I_w is cyclic and it has as generator the Frobenius automorphism

$$\begin{aligned} \phi_w : \mathbb{F}_w &\to \mathbb{F}_w \\ x &\mapsto x^{q_v} \end{aligned}$$

where $q_v = \mathbf{N}P_v$.

Definition 3.14. The inverse image of the Frobenius automorphism ϕ_v of $\mathrm{Gal}(\mathbb{F}_w/\mathbb{F}_v)$ under the surjective group homomorphism

$$\pi_w : G_w \to \mathrm{Gal}(\mathbb{F}_w/\mathbb{F}_v),$$

defined in the *Proposition 3.3.3*, is called the ***Frobenius substitution*** of w, and it is denoted by $\tilde{\phi}_w$.

Let V be a representation of G. For a finite place v of k let

$$F_v(T, V) = \det(1 - \phi_w T \mid_{V^{I_w}})$$

be the characteristic polynomial of the action on V^{I_w} of a Frobenius automorphism ϕ_w attached to a place w of K above v. Although ϕ_w is determined only up to multiplication by an element of I_w, its action on V^{I_w} is independent of which element of a coset $\phi_w I_w$ we chose. The polynomial $F_v(T, V)$ depends only on the isomorphism class of V. Moreover, it also depends only on v and not on the choice of w above v, because the places w above v are all conjugate. Note that for v unramified in K, we have

$$I_w = \{1\}, \text{ i.e. } V^{I_w} = V.$$

By this, $F_v(T, V)$ is of degree $\dim V$. Finaly, $F_v(T, V)$ depends only on V as G_w-module, not as G-module.

Definition 3.15. An ***Artin L-function*** is an Euler product

$$L(s, V) := \prod_v L_v(s, V)$$

over the finite places v of k where

$$L_v(s, V) := F_v(\mathrm{N}P_v^{-s}, V)^{-1} = \frac{1}{\det(1 - \phi_w q_v^{-s} \mid_{V^{I_w}})}$$

is called ***local L-function***.

Note that $L(s, V)$ depends only on the isomorphism class of the representation V. By this, we can also denoted $L(s, V)$ by

$$L(s, \chi_V),$$

where

$$\chi_V : G \to \mathbb{C}$$

is the character of V.

Proposition 3.3.4. *$L(s, \chi_V)$ converges absolutely and defines an analytic function in the half plane $\Re(s) > 1$.*

Proof. Consider

$$\log\left(L(s, \chi_V)\right) = \log\left(\prod_v L_v(s, \chi_V)\right) = \sum_v \log(L_v(s, \chi_V)), \tag{3.10}$$

where the sum is over the finite places v of k. Note that

$$\det(1 - \phi_w q_v^{-s}|_{V^{I_w}}) = \exp(\mathrm{Tr}(\log(1 - \phi_w q_v^{-s}|_{V^{I_w}}))).$$

Thus, for each finite place v of k, we obtain

$$\begin{aligned}
\log(L_v(s, \chi_V)) &= -\log(\det(1 - \phi_w q_v^{-s}|_{V^{I_w}})) \\
&= -\mathrm{Tr}(\log(1 - \phi_w q_v^{-s}|_{V^{I_w}})) \\
&= -\mathrm{Tr}\left(\sum_{n=1}^{\infty}(-1)^{n+1}\frac{(-\phi_w|_{V^{I_w}} q_v^{-s})^n}{n}\right) \\
&= \sum_{n=1}^{\infty}(-1)^{2(n+1)}\mathrm{Tr}\left(\frac{\phi_w^n|_{V^{I_w}}}{n q_v^{ns}}\right) \\
&= \sum_{n=1}^{\infty}\frac{\mathrm{Tr}(\phi_w^n|_{V^{I_w}})}{n q_v^{ns}}.
\end{aligned}$$

Now, consider on G_w the restriction representation

$$W = \mathrm{res}_{G_w}^{G} V.$$

By definition

$$\chi_W(\sigma) = \chi_V(\sigma), \text{ for all } \sigma \in G_w.$$

Let

$$\pi_w : G_w \to G_w/I_w$$

be the canonical projection. So

$$(\pi_w)_* W = W^{I_w}$$

is the representation of G_w/I_w defined as

$$\pi_w(\sigma).x = \sigma.x, \text{ for all } \sigma \in G_w, x \in W^{I_w}.$$

Then

$$\mathrm{Tr}(\phi_w^n|_{V^{I_w}}) = \mathrm{Tr}(\phi_w^n|_{W^{I_w}}) = \chi_W(\tilde{\phi}_w^n) = \chi_V(\tilde{\phi}_w^n),$$

where

$$\begin{aligned}
\mathrm{Tr}(\phi_w^n|_{V^{I_w}}) &= \frac{1}{|G_w|} \sum_{\eta \in G_w/I_w} \sum_{\tau \in G_w:\ \pi_w(\tau) = \eta\phi_w^n\eta^{-1}} \chi_W(\tau) \\
&= \frac{1}{|G_w|} \sum_{\eta \in G_w/I_w} \sum_{\tau \in G_w:\ \pi_w(\tau) = \phi_w^n} \chi_V(\tau) \\
&= \frac{1}{|G_w|} \frac{|G_w|}{|I_w|} \sum_{\tau \in G_w:\ \pi_w(\tau) = \phi_w^n} \chi_V(\tau) \\
&= \frac{1}{|I_w|} \sum_{\tau \in G_w:\ \pi_w(\tau) = \phi_w^n} \chi_V(\tau)
\end{aligned}$$

is the average value of χ_V on the coset $\phi_w^n I_w$ of I_w by (2.7). So,

$$\log(L_v(s, \chi_V)) = \sum_{n=1}^{\infty} \frac{\mathrm{Tr}(\phi_w^n|_{V^{I_w}})}{n q_v^{ns}} = \sum_{n=1}^{\infty} \frac{\chi_V(\tilde{\phi}_w^n)}{n q_v^{ns}}.$$

By (3.10), we obtain

$$\log\left(L(s, \chi_V)\right) = \sum_v \left(\sum_{n=1}^{\infty} \frac{\chi_V(\tilde{\phi}_w^n)}{n q_v^{ns}} \right).$$

Let $\sigma = \Re(s)$. Now, note that

$$\sum_v \left(\sum_{n=1}^{\infty} \left| \frac{\chi_V(\tilde{\phi}_w^n)}{n q_v^{ns}} \right| \right) < M \sum_v \sum_{n=1}^{\infty} \left(\frac{1}{q_v^{\sigma}} \right)^n = M \sum_v \frac{q_v^{-\sigma}}{1 - q_v^{-\sigma}} = M \sum_v \frac{1}{q_v^{\sigma} - 1}$$

for some $M \in \mathbb{N}$ such that

$$|\chi_V(\tilde{\phi}_w^n)| \leq M.$$

Since

$$q_v \geq p,$$

for all finite place v of k such that P_v is over a prime $p \in \mathbb{Z}$, then

$$\frac{q_v^\sigma}{2} > \frac{q_v}{2} \geq 1,$$

that is

$$\frac{1}{q_v^\sigma - 1} < \frac{2}{q_v^\sigma}.$$

Since

$$|\{P : P \text{ is a prime ideal over the prime } p \in \mathbb{Z}\}| \leq [k : \mathbb{Q}],$$

we have that

$$\sum_v q_v^{-\sigma} \leq [k : \mathbb{Q}] \cdot \sum_p p^{-\sigma}.$$

Now, by the proof of *Proposition 3.2.1*, we have that

$$\int_1^\infty x^{-\sigma} dx = \frac{1}{\sigma - 1}. \tag{3.11}$$

So, if we compare the sum

$$\sum_p p^{-\sigma}$$

with the integral (3.11), we can conclude that

$$\sum_v \left(\sum_{n=1}^\infty \left| \frac{\chi_V(\tilde{\phi}_w^n)}{n q_v^{ns}} \right| \right) < 2M \sum_v \frac{1}{q_v^\sigma} \leq \frac{2M[k : \mathbb{Q}]}{\sigma - 1}.$$

This implies the absolute convergence of

$$L(s, \chi_V) = \exp \left(\sum_v \left(\sum_{n=1}^\infty \frac{\chi_V(\tilde{\phi}_w^n)}{n q_v^{ns}} \right) \right) \tag{3.12}$$

for $\sigma = \Re(s) > 1$. □

Proposition 3.3.5. *Let V, W be two representations of G. Then*

$$L(s, \chi_{V \oplus W}) = L(s, \chi_V) L(s, \chi_W). \tag{3.13}$$

Proof. Note that

$$\sum_v \left(\sum_{n=1}^{\infty} \frac{\chi_{V\oplus W}(\tilde{\phi}_w^n)}{nq_v^{ns}} \right) = \sum_v \left(\sum_{n=1}^{\infty} \frac{\chi_V(\tilde{\phi}_w^n) + \chi_W(\tilde{\phi}_w^n)}{nq_v^{ns}} \right)$$
$$= \sum_v \left(\sum_{n=1}^{\infty} \frac{\tilde{\phi}_V(\phi_w^n)}{nq_v^{ns}} \right) + \sum_v \left(\sum_{n=1}^{\infty} \frac{\chi_W(\tilde{\phi}_w^n)}{nq_v^{ns}} \right).$$

By the equation (3.12) in the proof of *Proposition 3.3.4*, we obtain

$$L(s, \chi_{V\oplus W}) = L(s, \chi_V)L(s, \chi_W).$$

□

As a conseguence of *Proposition 3.3.5*, it is enough to consider irreducible representations.

Assume that K is contained in a larger Galois extension K' of k, i.e. $k \subset K \subset K'$. By the Galois theory,

$$G \simeq G'/G_{K'/K} \tag{3.14}$$

where $G' \coloneqq G_{K'/k}$. Let

$$\pi : G' \to G'/G_{K'/K}$$

be the canonical projection.

Definition 3.16. Let V be a representation of G. The ***inflation*** of V is the G'-module

$$V' \coloneqq \pi^* V$$

having the same underlying vector space as V, with G' acting through G as follows

$$\tau.x \coloneqq \bar{\tau}.x \text{ for } \tau \in G', x \in V.$$

Proposition 3.3.6. *Let V be a representation of G. Then*

$$L(s, V') = L(s, V).$$

Proof. Let w' be a place of K' above w, which is a place of K above v. Thanks to the isomorphism (3.14), we have

$$\phi_w = \phi_{w'} G_{K'/K} \text{ and } I_w = I'_{w'} G_{K'/K},$$

By the action of G' in *Definition 3.16*, then

$$(V')^{I'_{w'}} = V^{I_w}.$$

So

$$L(s, V') = L(s, V).$$

□

Definition 3.17. The ***absolute Galois group*** of k is the Galois group

$$G_k := \mathrm{Gal}(\bar{k}/k)$$

where $\bar{k}$ is the algebraic closure of k.

Proposition 3.3.6 shows that $L(s, V)$ really depends only on V viewed as module $\overline{V}$ for G_k. Note that the isomorphism class of $\overline{V}$ as G_k-module is independent of how we view K/k as subextension of $\bar{k}/k$. Moreover, the representations of the form $\overline{V}$ are, up to isomorphism, simply the $\mathbb{C}[G_k]$-modules X of finite dimension over $\mathbb{C}$ for which the action map

$$G_k \times X \to X$$

is continuous for the Krull topology in G_k and the discrete topology in X.

Proposition 3.3.7. *Let H be a subgroup of G and consider the intermediate field*

$$k' := K^H,$$

i.e. $k \subset k' \subset K$. Let W be a representation of H and set

$$V = \mathrm{Ind}_H^G W.$$

Then

$$L(s, W) = L(s, V).$$

Proof. Let v be a finite place of k and w be a place of K above v. Let

$$G = \coprod_{i=1}^{r} G_w \rho_i H$$

be the expression of G as disjoint union of double cosets of G_w and H. Set

$$w_i = \rho_i^{-1}.w$$

and let v_i' be the place of k' below w_i. Since $v_1', v_2', ..., v_r'$ are places of k' above v, then it suffices to show that

$$L_v(s, V) = \prod_{i=1}^{r} L_{v_i'}(s, W). \tag{3.15}$$

For each i, let

$$G_w = \coprod_{j=1}^{m_i} \tau_{ij}(G_w \cap H^{\rho_i}),$$

where $H^{\rho_i} = \rho_i H \rho_i^{-1}$. Then

$$G = \coprod_{i=1}^{r} \coprod_{j=1}^{m_i} \tau_{ij} \rho_i H.$$

By definition of induced representation, V contains W as an H-submodule. Hence

$$V = \oplus_{i=1}^{r} V_i, \tag{3.16}$$

where

$$V_i = \oplus_{j=1}^{m_i} \tau_{ij} \rho_i W \simeq \mathrm{Ind}_{G_w \cap H^{\rho_i}}^{G_w} \rho_i W$$

is a G_w-module for each i. Applying the automorphism ρ_i to our situation, we obtain by transport of structure,

$$L_{v_i'}(s, W) = L_{v_i}(s, \rho_i W), \tag{3.17}$$

where v_i is the place of $\rho_i k$ below w. If we put (3.16) and (3.17) in (3.15), by (3.13), we have

$$\prod_{i=1}^{r} L_v(s, V_i) = \prod_{i=1}^{r} L_{v_i}(s, \rho_i W).$$

By this, we can reduced to the local case $G = G_w$.

Let $I = I_w$ and $J = H \cap I$ be the inertia subgroups of G and H, respectively. Consider the homomorphism

$$f : H \to G/I.$$

Since we can factor f as

$$H \hookrightarrow G \to G/I,$$

then

$$f_* W = (\mathrm{Ind}_H^G W)^I = V^I.$$

Moreover, we can factor f as

$$H \to H/J \hookrightarrow G/I,$$

because

$$H/J \simeq HI/I \leq G/I.$$

So,

$$f_* W = \mathrm{Ind}_{H/J}^{G/I}(W^J),$$

i.e.

$$V^I \simeq \mathrm{Ind}_{H/J}^{G/I}(W^J). \tag{3.18}$$

Thanks to (3.18), we can reduced to the local unramified case $G = G/I$ where $V = V^I$ and $W = W^J$.

In this case, G is cyclic and generated by the v-Frobenius automorphism ϕ_v. Moreover, H is the subgroup generated by the v'-Frobenius automorphism $\phi_{v'} = \phi_v^k$, where $k = (G : H)$. Then

$$V = \mathrm{Ind}_H^G W = \oplus_{i=0}^{k-1} \phi_v^i W.$$

So we can assume W is 1-dimensional with basis x. Let

$$\phi_{v'} x = \eta x.$$

For each solution ζ to $X^k = \eta$, the element

$$\sum_{i=0}^{k-1} \zeta^{-i} \phi_v^i x \in V$$

is an eigenvector for ϕ_v with eigenvalue ζ. In fact,

$$\phi_v \left(\sum_{i=0}^{k-1} \zeta^{-i} \phi_v^i x \right) = \sum_{i=0}^{k-1} \zeta^{-i} \phi_v^{i+1} x = \zeta^{-k+1} \phi_v^k x + \sum_{i=0}^{k-2} \zeta^{-i} \phi_v^{i+1} x,$$

where

$$\zeta^{-k+1} \phi_v^k x = \eta^{-1} \zeta \phi_{v'} x = \zeta \eta^{-1} \eta x = \zeta x.$$

Then

$$\begin{aligned} \zeta x + \sum_{i=0}^{k-2} \zeta^{-i} \phi_v^{i+1} x &= \zeta \left(x + \sum_{i=0}^{k-2} \zeta^{-(i+1)} \phi_v^{i+1} x \right) = \zeta \left(x + \sum_{j=1}^{k-1} \zeta^{-j} \phi_v^j x \right) \\ &= \zeta \cdot \sum_{j=0}^{k-1} \zeta^{-j} \phi_v^j x, \end{aligned}$$

that is,

$$\phi_v \left(\sum_{i=0}^{k-1} \zeta^{-i} \phi_v^i x \right) = \zeta \cdot \sum_{i=0}^{k-1} \zeta^{-i} \phi_v^i x.$$

Hence

$$L_v(s, V) = \frac{1}{\det(1 - \sigma_v q_v^{-s}|_V)} = \prod_{\zeta \text{ s.t. } \zeta^k = \eta} \frac{1}{1 - \zeta q_v^{-s}}.$$

Now, let ζ_0 be such that

$$\zeta_0^k = \eta,$$

and ξ be a k-th root of unity. Since

$$X^k - 1 = \prod_{i=0}^{k-1}(X - \xi^i),$$

then

$$\frac{q_v^{sk}}{\zeta_0^k}\left(1 - \zeta_0^k q_v^{-sk}\right) = \left(\frac{q_v^s}{\zeta_0}\right)^k - 1 = \prod_{i=0}^{k-1}\left(\frac{q_v^s}{\zeta_0} - \xi^i\right) = \frac{q_v^{sk}}{\zeta_0^k} \cdot \prod_{i=0}^{k-1}(1 - \zeta_0 \xi^i q_v^{-s}),$$

that is,

$$1 - \eta(q_v^{-s})^k = \prod_{i=0}^{k-1}(1 - \zeta_0 \xi^i q_v^{-s}) = \prod_{\zeta \text{ s.t. } \zeta^k = \eta}(1 - \zeta q_v^{-s}).$$

So

$$L_v(s, V) = \frac{1}{1 - \eta(q_v^{-s})^k} = \frac{1}{1 - \eta(q_v^k)^{-s}} = \frac{1}{\det(1 - \eta(q_v^k)^{-s}|_W)} = L_{v'}(s, W).$$

□

Example 5. If in *Proposition 3.3.7* we choose $H = 1_G$ and $W = \mathbb{C}$ is the trivial representation, then $V = \mathbb{C}[G]$ is the regular representation of G. Since

$$\langle \chi_i, \chi_{\mathbb{C}[G]} \rangle_G = \frac{1}{|G|}\sum_{\sigma \in G} \chi_i(\sigma)\overline{\chi_{\mathbb{C}[G]}(\sigma)} = \frac{1}{|G|} \cdot \chi_i(1) \cdot |G| = \dim V_i,$$

by (2.5), we obtain

$$\mathbb{C}[G] \simeq \oplus_i V_i^{\dim V_i},$$

where the V_i are the irreducible representations of G. So, by (3.13), we have

$$\zeta_K(s) = L(s, \mathbb{C}) = L(s, \mathbb{C}[G]) = \prod_i L(s, V_i)^{\dim V_i}.$$

In particular, if we number the V_i so that V_1 is the trivial representation of G, then

$$L(s, V_1) = \zeta_k(s),$$

by definition of Artin L-function. So, we obtain

$$\zeta_K(s) = \zeta_k(s) \prod_{i \neq 1} L(s, V_i)^{\dim V_i}. \tag{3.19}$$

More generally, if k' is any intermediate field, and W the trivial representation of H, then $V = \mathbb{C}[G/H]$ is the permutation representation of G acting on the set G/H of cosets of H. By Frobenius reciprocity, we have

$$\langle \chi_V, \chi_i \rangle_G = \langle \chi_W, \chi_i|_H \rangle_H$$

Since the isotypical component of V_i corresponding to the trivial representation W is V_i^H, then

$$m_i := \langle \chi_i, \chi_V \rangle_G = \dim V_i^H,$$

i.e.

$$V \simeq \oplus_i V_i^{m_i}.$$

Since $m_1 = 1$, we obtain

$$\zeta_{k'}(s) = \zeta_k(s) \prod_{i \neq 1} L(s, V_i)^{m_i}.$$

3.4 Reciprocity and the relation between the two kind of L-functions

Consider the following Takagi-Artin existence theorem

Theorem 3.4.1. *For each level $\mathfrak{m}$, there is an abelian extension $K_\mathfrak{m}$ of k with Galois group $G_{K_\mathfrak{m}/k}$ having the same invariants as, hence isomorphic to, the generalized ideal class group $\mathcal{C}_\mathfrak{m} = \mathcal{I}_\mathfrak{m}/\mathcal{P}_\mathfrak{m}$. In particular, the way in which a prime ideal P of k decomposes in $K_\mathfrak{m}$ is determined by the class of P in $\mathcal{C}_\mathfrak{m}$. Conversely, for each finite abelian extension K of k, there exists a level $\mathfrak{m}$ of k such that*

$$G_{K/k} \cong \mathcal{C}_\mathfrak{m}.$$

Proof. See [2, Ch. 7, Theorem 5.1]. □

Let $a \in O_k$ such that $a \equiv 1 \bmod^\times \mathfrak{m}$. The reciprocity law

$$(a) = \prod_v P_v^{m_v} \Rightarrow \prod_v \tilde{\phi}_w^{m_v} = 1 \tag{3.20}$$

by Artin (see [2, Ch. 7, §3.3]) allows us to prove the existence of the canonical isomorphism

$$\mathcal{C}_\mathfrak{m} \xrightarrow{\sim} G_{K_\mathfrak{m}/k} \tag{3.21}$$

which, for each finite place v of k unramified in K, associates to the class of the prime ideal P_v the Frobenius substitution $\tilde{\phi}_w$. From Takagi's decomposition law, it follows that

$$\zeta_K(s) = \prod_{\chi} L(s, \chi) = \zeta_k(s) \prod_{\chi \neq 1} L(s, \chi), \tag{3.22}$$

where the first product is over all characters χ of $\mathcal{C}_{\mathfrak{m}}$ and the $L(s, \chi)$ are the classical abelian L-functions. Thanks to the isomorphism (3.21), the factorizations (3.19) and (3.22) coincide.

Example 6. Let q be a prime such that $q \equiv 1 \bmod 4$. Then, for the extension $\mathbb{Q}(\sqrt{q})/\mathbb{Q}$, (3.20) implies that there is a non-trivial character χ with

$$\chi(1) \equiv 2 \bmod q$$

such that

$$\chi(p) = \left(\frac{q}{p}\right) \text{ for primes } p \neq q.$$

Since the only such character is

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

then

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

(See [11, p. 18]).

3.5 Application of Brauer's theorem

Theorem 3.5.1. *Every Artin L-function is meromorphic in the whole complex plane.*

Proof. Let V be a representation of a Galois group G, with χ_V its character. By *Theorem 2.2.4*, there exist W_i, 1-dimensional representations of some subgroups H_i of G, such that

$$\chi_V = \sum_i n_i \mathrm{Ind}_{H_i}^G \psi_i,$$

where ψ_i is the character of H_i. For each i, let

$$k_i = K^{H_i}$$

be the fixed field of H_i. So, by the Galois correspondence we have that

$$H_i = \mathrm{Gal}(K/k_i).$$

Let k_i^{ab} be the maximal abelian extension of k_i contained in K. Set

$$H_i^{ab} := \mathrm{Gal}(k_i^{ab}/k_i).$$

By the Galois theory,

$$H_i^{ab} \cong H_i/G_{K/k_i^{ab}}.$$

So, we can consider the canonical projection

$$\pi_i : H_i \to H_i^{ab}.$$

Thus, it is uniquely determined a character

$$\psi_i' : H_i^{ab} \to \mathbb{C}^\times$$

of H_i^{ab} which makes the diagram

$$\begin{tikzcd} H_i \arrow[rr, "\psi_i"] \arrow[dr, "\pi_i"'] & & \mathbb{C}^\times \\ & H_i^{ab} \arrow[ur, "\psi_i'"'] & \end{tikzcd}$$

commutative. Let W_i' be the corresponding representation. Consider the inflation of W_i'

$$V_i := \mathrm{Infl}(W_i') = (\pi_i)^* W_i',$$

where

$$\chi_i : H_i \to \mathbb{C}^\times$$

is the corresponding character. Since

$$\chi_i(\sigma) = \psi_i'(\pi_i\sigma) = \psi_i(\sigma)$$

for all $\sigma \in G$, by *Theorem 3.3.6*, we have that

$$L(s, \psi_i) = L(s, \chi_i) = L(s, \psi_i').$$

Now, since k_i^{ab}/k_i is an abelian extension, by *Theorem 3.4.1*, there exist a level $\mathfrak{m}_i$ of k_i such that

$$H_i^{ab} \cong \mathcal{C}_{\mathfrak{m}_i}.$$

Hence

$$L(s,\psi_i')=\prod_v \frac{1}{\det(1-\phi_w q_v^{-s}|_{(W_i^{ab})^{I_w}})}=\prod_v \frac{1}{1-\phi_w q_v^{-s}|_{(W_i^{ab})^{I_w}}},$$

where the product is over the finite places v of k_i. Since W_i^{ab} is a 1-dimensional representation, then

$$(W_i^{ab})^{I_w}=0 \text{ or } (W_i^{ab})^{I_w}=W_i^{ab}.$$

Since each finite place v of k_i such that

$$P_v|m_i$$

is ramified in k_i^{ab}, we must have that

$$(W_i^{ab})^{I_w}=0.$$

Moreover,

$$\phi_w.x=\psi_i'(\phi_w)x=\psi_i'(P_v)x, \tag{3.23}$$

because W_i^{ab} is 1-dimensional (see [17, Appendix, §3, Theorem 1-4]). Hence

$$L(s,\psi_i')=\prod_v \frac{1}{1-\psi_i'(P_v)\mathbf{N}P_v{}^{-s}},$$

where the product is over the finite places v of k_i such that P_v not dividing $\mathfrak{m}_i$. So, $L(s,\psi_i')$ is a classical abelian L-function, hence meromorphic on $\mathbb{C}$, and even entire for $\psi_i\neq 1$. Since

$$\begin{aligned}L(s,\chi_V)&=L(s,V_{\sum_i n_i \mathrm{Ind}_{H_i}^G\psi_i})=L(s,\sum_i n_i\mathrm{Ind}_{H_i}^G W_i)\\&=\prod_i L(s,\mathrm{Ind}_{H_i}^G W_i)^{n_i}=\prod_i L(s,W_i)^{n_i}=\prod_i L(s,\psi_i)^{n_i},\end{aligned} \tag{3.24}$$

we can conclude. □

Note that, if the trivial representation does not occur in χ, then one can cancel on the right side of (3.24) all the terms in which ψ_i is the trivial character of H_i. In fact, by Frobenius reciprocity, we have

$$\langle\chi,1_G\rangle_G=\sum_i n_i\langle\mathrm{Ind}_{H_i}^G\psi_i,1_G\rangle_G=\sum_i n_i\langle\psi_i,1_{H_i}\rangle_{H_i}=\sum_{i\in J}n_i,$$

where $J=\{j:\psi_j=1_{H_j}\}$. Since

$$\langle\chi,1_G\rangle_G=0,$$

then

$$L(s,\chi) = L(s,1_H)^{\sum_{i\in J} n_i} \cdot \prod_{i\notin J} L(s,\psi_i)^{n_i} = \prod_{i\notin J} L(s,\psi_i)^{n_i}.$$

If in (3.24) $n_i \geq 0$ and $\psi_i \neq 1$ for all i, then $L(s,\chi)$ is entire. However, for most character χ such an expression does not exist. Artin's conjecture that $L(s,\chi)$ is holomorphic for irreducible $\chi \neq 1$ is much deeper (see [10, p. 525]). In particular, it implies the cancellation of the zeroes of the $L(s,\psi_i)$ with $n_i < 0$ with those of $L(s,\psi_i)$ with $n_i > 0$ in (3.24).

3.6 Functional equation

Let v be an infinite place of k. Since the decomposition group G_w of a place w of K above v is of order 1 or 2, then it has a unique generator, which we denote by σ_w.

Definition 3.18. If v is a real place, we set

$$L_v(s,\chi) = \left(\Gamma\left(\frac{s}{2}\right)\Gamma\left(\frac{s+1}{2}\right)\right)^{\chi(1)} = (2^{1-s}\sqrt{\pi}\Gamma(s))^{\chi(1)}.$$

If v is a complex place, we set

$$L_v(s,\chi) = \Gamma\left(\frac{s}{2}\right)^{\frac{\chi(1)+\chi(\sigma_w)}{2}} \Gamma\left(\frac{s+1}{2}\right)^{\frac{\chi(1)-\chi(\sigma_w)}{2}}.$$

Note that the local L-functions in the *Definition 3.18* depend only on the action of σ_w on V, i.e. only on V as G_w-module. Moreover,

$$\frac{\chi(1)+\chi(\sigma_w)}{2} = \langle \chi|_{G_w}, 1_{G_w}\rangle_{G_w} = \mathrm{dim} V^{G_w},$$

and

$$\frac{\chi(1)-\chi(\sigma_w)}{2} = \chi(1) - \frac{\chi(1)+\chi(\sigma_w)}{2} = \mathrm{dim} V - \mathrm{dim} V^{G_w} = \mathrm{codim} V^{G_w}.$$

Let

$$\Lambda(s,V) := \prod_v L_s(s,V) = \Gamma\left(\frac{s}{2}\right)^a \Gamma\left(\frac{s+1}{2}\right)^b L(s,V), \tag{3.25}$$

where the product is over all the places of k, and where

$$a = a_1 + r_2 \mathrm{dim} V,$$
$$b = a_2 + r_2 \mathrm{dim} V,$$

with

$$a_1 = \sum_{v \text{ real}} \dim V^{G_w},$$
$$a_2 = \sum_{v \text{ real}} \operatorname{codim} V^{G_w}.$$

Note that, if V and W are two representations of G then

$$\Lambda(s, V \oplus W) = \Lambda(s, V) L_S(s, W). \tag{3.26}$$

Moreover, let V' be the inflation of V. Then

$$\Lambda(s, V') = \Lambda(s, V). \tag{3.27}$$

Finally, let H be a subgroup of G and consider the intermediate field

$$k' := K^H,$$

i.e. $k \subset k' \subset K$. Let W be a representation of H and set

$$V = \mathrm{Ind}_H^G W.$$

Then
$$\Lambda(s, W) = \Lambda(s, V). \tag{3.28}$$

The properties (3.26), (3.27) and (3.28) verified by the fact that (3.15) holds for infinite v as well (see [11, p. 19]).

Consider an Artin L-function $L(s, \chi)$. By *Theorem 2.2.4*, there exist ψ_i, 1-dimensional characters of some subgroups H_i of G, such that

$$L(s, \chi) = \prod_i L(s, \psi_i)^{n_i}.$$

In particular, our definition of $\Lambda(s, \psi_i)$ is consistent with *Definition 3.10.* So, we know that there exist constants $B_{\psi_i} > 0$ and $C_{\psi_i} \in \mathbb{C}^*$ such that

$$\Lambda(1 - s, \psi_i) = C_{\psi_i} B_{\psi_i}^s \Lambda(s, \bar{\psi}_i).$$

Thus, by (3.26), we have that

$$\begin{aligned} \Lambda(1 - s, \chi) &= \prod_i \Lambda(1 - s, \psi_i)^{n_i} = \prod_i C_{\psi_i}^{n_i} B_{\psi_i}^{s n_i} \Lambda(s, \bar{\psi}_i)^{n_i} \\ &= C_\chi B_\chi^s \Lambda(s, \bar{\chi}), \end{aligned} \tag{3.29}$$

where

$$B_\chi = \prod_i B_{\psi_i}^{s_i} > 0 \text{ and } C_\chi = \prod_i C_{\psi_i}^{n_i}.$$

In particular, B_χ and C_χ are uniquely determined by (3.29), independent of the choice of the expression

$$\chi = \sum_i n_i \mathrm{Ind}_{H_i}^G \psi_i.$$

Moreover, there exist unique constants $A_\chi > 0$ with

$$A_\chi = A_{\bar{\chi}},$$

and $W_\chi \in \mathbb{C}^*$, called an *Artin root number*, with

$$|W_\chi| = 1 \text{ and } W_{\bar{\chi}} = \overline{W}_\chi,$$

such that the functions

$$\xi(s,\chi) := A_\chi^{s/2}\Lambda(s,\chi) = A_\chi^{s/2}\Gamma\left(\frac{s}{2}\right)^a \Gamma\left(\frac{s+1}{2}\right)^b L(s,\chi) \tag{3.30}$$

satisfy

$$\xi(1-s,\chi) = W_\chi \xi(s,\bar{\chi}).$$

(see [2, p. 225]). In particular, Artin showed that

$$A_\chi = \frac{|d_k|^{\chi(1)}\mathbf{N}\mathfrak{f}(\chi)}{\pi^{[k:\mathbb{Q}]\chi(1)}},$$

where d_k is the discriminant ideal of the extension $k/\mathbb{Q}$ and $\mathfrak{f}(\chi)$ is an integral ideal of $\mathcal{O}_k$ involving only primes ramified in K called the *conductor* of χ (see [10, Ch. 7, Theorem 12.6]).

Now, if we consider the case $\chi = 1$ and assuming $W_1 = 1$, we have that the Dedekind zeta function $\zeta_k(s)$ satisfies the functional equation

$$\xi(1-s) = \xi(s), \tag{3.31}$$

where

$$\xi(s) = \left(\frac{|d_k|^{\chi(1)}}{\pi^{[k:\mathbb{Q}]}}\right)^{s/2} \Gamma\left(\frac{s}{2}\right)^{r_1+r_2} \Gamma\left(\frac{s+1}{2}\right)^{r_2} \zeta_k(s).$$

Chapter 4

Basic Stark Conjecture

4.1 Class number formula

Theorem 4.1.1. *Let k be a number field. The Dedekind zeta function $\zeta_k(s)$ has a simple pole at $s = 1$ with residue*

$$\frac{2^{r_1}(2\pi)^{r_2}}{\sqrt{|d_k|}}\frac{h_k R_k}{w_k},$$

where

- *h_k is the class number of k;*
- *R_k is the regulator of k;*
- *w_k is the number of roots of unity contained in k.*

Proof. See [10, Ch. 7, Corollary 5.11]. □

By means of the functional equation (3.31) of $\zeta_k(s)$, the *Theorem 4.1.1* can be reformulated to became true for $s = 0$.

Corollary 4.1.2. *The Taylor expansion of $\zeta_k(s)$ at $s = 0$ starts as follows*

$$\zeta_k(s) = -\frac{h_k R_k}{w_k} s^{r_1+r_2-1} + \ldots$$

Therefore, by *Corollary 4.1.2*, the first non-vanishing Taylor coefficient of $\zeta_k(s)$ at $s = 0$ is the product of a rational number $-h_k/w_k$ with the regulator R_k, which is the determinant of a matrix whose entries involve logarithms of absolute values of units and whose size

$$r_1 + r_2 - 1$$

is the order of vanishing of $\zeta_k(s)$ at $s = 0$.

4.2 S-imprimitive L-functions

Let S be a finite set of places of k containing S_∞, the set of infinite places of k, and let V be a representation of the Galois group $G = G_{K/k}$ of a Galois extension K/k of number fields.

Definition 4.1. The ***S-imprimitive Artin L-function*** is defined for $\Re(s) > 1$ as

$$L_S(s, V) := \prod_{v \notin S} L_v(s, V).$$

Note that, if V and W are two representations of G then

$$L_S(s, V \oplus W) = L_S(s, V) L_S(s, W). \tag{4.1}$$

Moreover, let V' be the inflation of V. Then

$$L_S(s, V') = L_S(s, V). \tag{4.2}$$

Finally, let H be a subgroup of G and consider the intermediate field

$$k' := K^H,$$

i.e. $k \subset k' \subset K$. Let W be a representation of H and set $V = \mathrm{Ind}_H^G W$. Then

$$L_S(s, W) = L_S(s, V). \tag{4.3}$$

The properties (4.1), (4.2) and (4.3) are satisfy by the S-imprimitive Artin L-functions since all of them hold place by place for the local L-functions $L_v(s, V)$ (see [11, p. 21]).

Definition 4.2. We define the *S-Dedekind zeta function* of the field k as

$$\zeta_{k,S}(s) := L_S(s, 1) = \prod_{P \notin S} \frac{1}{1 - \mathbf{N}P^{-s}}.$$

We can view $\zeta_{k,S}(s)$ as the zeta function associated with the Dedekind domain

$$\mathcal{O}_{k,S} = \{x \in k : |x|_v = (\mathbf{N}P_v)^{-\mathrm{ord}_{P_v}(x)} \leq 1 \text{ for all } v \notin S\},$$

consisting of the S-integers of k. Moreover, we denote the S-class number by $h_{k,S}$ and the S-regulator by $R_{k,S}$.

Lemma 4.2.1. *Let v be a place of k which is not contained in S and let*

$$S' = S \cup \{v\}.$$

Let m be the order of v in the S-class group of k, which is the ideal class group of $\mathcal{O}_{k,S}$. Then

$$h_{k,S'} = \frac{h_{k,S}}{m},$$

and

$$R_{k,S'} = m(\log \mathbf{N}v) R_{k,S}.$$

Corollary 4.2.2. *The Taylor expansion of $\zeta_{k,S}(s)$ at $s = 0$ starts as follows*

$$\zeta_{k,S}(s) = -\frac{h_{k,S} R_{k,S}}{w_k} s^{|S|-1} + \dots$$

(See [11, p. 21]).

Given an S-imprimitive Artin L-function, we write

$$L_S(s, \chi) = c_S(\chi) s^{r_S(\chi)} + \dots,$$

where

$$r(\chi) = r_S(\chi)$$

is the order of vanishing of $L_S(s, \chi)$ at $s = 0$. In order to compute it, we introduce some notation. Let S_K be the set of places of K lying above the places of S. Let

$$Y = Y_{S_K}$$

be the free abelian group on S_K, and let

$$\eta : Y \to \mathbb{Z}$$

be the surjective homomorphism such that

$$\eta(w) = 1 \text{ for all } w \in S_K.$$

The kernel of η is denoted by

$$X = X_{S_K}.$$

Thus we obtain the short exact sequence of G-modules

$$0 \longrightarrow X \longrightarrow Y \xrightarrow{\eta} \mathbb{Z} \longrightarrow 0. \tag{4.4}$$

Now, given an abelian group B and a subring A of $\mathbb{C}$, we set

$$AB \coloneqq A \otimes_{\mathbb{Z}} B.$$

By *Proposition 3.3.1*, G acts on $\mathbb{C}Y$ by permuting the places of S_K, that is,

$$\sigma.\left(a \otimes \left(\sum_{w \in S_K} n_w w\right)\right) = a \otimes \left(\sum_{w \in S_K} n_w \cdot \sigma.w\right),$$

for all $\sigma \in G$ and $a \otimes \left(\sum_{w \in S_K} n_w w\right) \in \mathbb{C}Y$. Since $\mathbb{C}Y$ is a permutation representation of G, then its character

$$\chi_Y \coloneqq \chi_{\mathbb{C}Y}$$

is integer valued (see [13, Proposition 7.2.5]). Similarly, we define the permutation representation $\mathbb{C}X$ of G and the corresponding character

$$\chi_X \coloneqq \chi_{\mathbb{C}X}.$$

In particular, tensoring the exact sequence (4.4) with $\mathbb{C}$, we obtain the exact sequence of $\mathbb{C}[G]$-modules

$$0 \to \mathbb{C}X \to \mathbb{C}Y \to \mathbb{C} \to 0. \tag{4.5}$$

By semisemplicity, the exactness of (4.5) implies that

$$\mathbb{C}Y \cong \mathbb{C}X \oplus \mathbb{C}$$

as $\mathbb{C}[G]$-modules. By *Example 2*, we have

$$\chi_Y = \chi_X + \chi_{\mathbb{C}}, \tag{4.6}$$

where $\chi_{\mathbb{C}}$ is the trivial representation defined in *Example 1*.

Lemma 4.2.3. *For each $v \in S$, let us choose a place w of K lying above v. Then we have the formula*

$$r_S(\chi) = \sum_{v \in S} \dim V^{G_w} - \dim V^G = \langle \chi_V, \chi_X \rangle_G = \dim(\mathrm{Hom}_G(V^*, \mathbb{C}X)),$$

where

$$V^* = \mathrm{Hom}_{\mathbb{C}}(V, \mathbb{C})$$

is the dual representation to V.

Proof. By *Theorem 2.2.2*,

$$\langle \chi_V, \chi_X \rangle_G = \langle \chi_X, \chi_V^* \rangle_G = \langle \chi_V^*, \chi_X \rangle_G = \dim(\mathrm{Hom}_G(V^*, \mathbb{C}X)),$$

where the first equality follows by the fact that χ_X is integer valued, as we can see from (4.6).

Now, if we choose for each $v \in S$ a fixed place $w \in S_K$ lying above v, we have an isomorphism of $\mathbb{Z}[G]$-modules

$$Y \cong \bigoplus_{v \in S} \mathrm{Ind}_{G_w}^G \mathbb{Z} = \bigoplus_{v \in S} \mathbb{Z}[G] \otimes_{\mathbb{Z}[G]} \mathbb{Z}.$$

Tensoring with $\mathbb{C}$, we obtain

$$\mathbb{C}X \oplus \mathbb{C} \cong \mathbb{C}Y \cong \bigoplus_{v \in S} \mathrm{Ind}_{G_w}^G \mathbb{C}.$$

Thus

$$\langle \chi_V, \chi_X \rangle_G = \langle \chi_V, \chi_Y - \chi_{\mathbb{C}} \rangle_G = \langle \chi_V, \chi_Y \rangle_G - \langle \chi_V, \chi_{\mathbb{C}} \rangle_G,$$

where

$$\langle \chi_V, \chi_Y \rangle_G = \sum_{v \in S} \langle \chi_V, \mathrm{Ind}_{G_w}^G \chi_{\mathbb{C}} \rangle_G = \sum_{v \in S} \langle \mathrm{res}_{G_w}^G \chi_V, \chi_{\mathbb{C}} \rangle_H = \sum_{v \in S} \dim V^{G_w},$$

by (2.8), and

$$\langle \chi_V, \chi_{\mathbb{C}} \rangle_G = \dim V^G.$$

Finally, by *Theorem 2.2.4*, there exist W_i, 1-dimensional representations of some subgroups H_i of G, such that

$$\chi_V = \sum_i n_i \mathrm{Ind}_{H_i}^G \psi_i, \tag{4.7}$$

where ψ_i is the character of H_i. Since

$$L_S(s, \chi_V) = \prod_i L_S(s, \psi_i)^{n_i},$$

then

$$r(\chi) = \sum_i n_i r(\psi_i). \tag{4.8}$$

On the other hand, (4.7) and (2.8) imply that

$$\langle \chi_V, \chi_X \rangle_G = \sum_i n_i \langle \mathrm{Ind}_{H_i}^G \psi_i, \chi_X \rangle_G = \sum_i n_i \langle \psi_i, \mathrm{res}_H^G \chi_X \rangle_H. \tag{4.9}$$

Comparing (4.8) and (4.9), it suffices to study the ψ_i's instead of χ_V, that is, we can reduced to prove

$$r(\psi_i) = \sum_{v\in S} \mathrm{dim} W_i^{(H_i)_w} - \mathrm{dim} W_i^{H_i}$$

for all i.

If $\psi_i = 1$, then

$$L_S(s, \psi_i) = \zeta_{k,S}(s).$$

By *Corollary 4.2.2*, we have that

$$r(\psi_i) = |S| - 1 = \sum_{v\in S} \mathrm{dim} W_i^{(H_i)_w} - \mathrm{dim} W_i^{H_i}.$$

If $\psi_i \neq 1$, then

$$W_i^{H_i} = 0.$$

Note that

$$L_{S_\infty}(s, \psi_i) = L(s, \psi).$$

Moreover, by *Definition 3.15*, for each finite place v, the Euler factor $L_v(s, \psi_i)$ has neither a zero nor a pole at $s = 1$. The same holds for each real, or complex, place v, by *Definition 3.18*. So, equating the orders at $s = 0$ in the functional equation

$$\xi(s, \psi_i) = W_{\psi_i} \xi(1 - s, \overline{\psi_i}),$$

where

$$\xi(s, \psi_i) \coloneqq A_{\psi_i}^{s/2} \Lambda(s, \psi_i) = A_{\psi_i}^{s/2} \Gamma\left(\frac{s}{2}\right)^a \Gamma\left(\frac{s+1}{2}\right)^b L(s, \psi_i),$$

by (3.30), we obtain

$$-a + r_{S_\infty}(\chi_i) = 0.$$

Since

$$a = a_1 + r_2 \mathrm{dim} W_i = a_1 + r_2,$$

with

$$a_1 = \sum_{v \text{ real}} \mathrm{dim} W_i^{(H_i)_w},$$

we have that

$$r_{S_\infty}(\chi_i) = a = \sum_{v\in S_\infty} \mathrm{dim} W_i^{(H_i)_w}.$$

Since

$$L_S(s, V) \coloneqq \prod_{v\notin S} L_v(s, V),$$

we obtain

$$\begin{aligned} r(\psi_i) &= |\{v \in S \smallsetminus S_\infty : \psi_i((H_i)_w) = 1\}| + r_{S_\infty}(\psi_i) \\ &= \sum_{v \in S \smallsetminus S_\infty} \dim W_i^{(H_i)_w} + r_{S_\infty}(\psi_i) \\ &= \sum_{v \in S} \dim W_i^{(H_i)_w}, \end{aligned}$$

which is what we want. □

Corollary 4.2.4. *If V is a 1-dimensional representation of G, then*

$$r_S(\chi) = \begin{cases} |\{v \in S : G_w \subset \mathrm{Ker}(\chi)\}| & \text{if } \chi \neq 1 \\ |S| - 1 & \text{if } \chi = 1 \end{cases}.$$

4.3 Stark regulator

Given a character χ, we will now introduce a regulator attached to χ which will appear in the formulation of the conjecture.

We denote by

$$U = U_{K,S_K} = \{x \in K : \mathrm{ord}_{P_w}(x) = 0 \text{ for all } w \notin S_K\}$$

the group of S_K-units of K, and we consider the logarithm map

$$\lambda : U \to \mathbb{R}Y$$

defined by

$$u \mapsto \sum_{w \in S_K} \log |u|_w \cdot w.$$

The image of λ is in $\mathbb{R}X$. In fact, for each $u \in U$,

$$\eta\left(\sum_{w \in S_K} \log |u|_w \cdot w\right) = \sum_{w \in S_K} \log |u|_w \cdot \eta(w) = \log\left(\prod_{w \in S_K} |u|_w\right) = 0$$

because, by *Theorem 2.1.3*,

$$\prod_{w \in S_K} |u|_w = \prod_{w \in \Sigma_K} |u|_w = 1,$$

where Σ_K is set of all places of K.

Theorem 4.3.1. *The image of λ is a lattice of full rank $|S| - 1$ in $\mathbb{R}X$.*

Proof. See [6, Ch. 5, §1, Unit Theorem]. □

We denote by μ_K the kernel of λ, which consists of roots of unity in K.

Corollary 4.3.2. *U/μ_K is a free abelian group on $|S|-1$ generators.*

Proof. See [6, Ch. 5, §1, Corollary]. □

By *Theorem 4.3.1*, tensoring λ with $\mathbb{R}$, we get the G-equivariant isomorphism

$$1 \otimes \lambda : \mathbb{R}U \to \mathbb{R}X, \tag{4.10}$$

which we denote with the same symbol λ. Moreover, tensoring (4.10) with $\mathbb{C}$, we obtain an isomorphism of $\mathbb{C}[G]$-modules

$$\mathbb{C}U \to \mathbb{C}X,$$

also denoted by λ. This implies that $\mathbb{Q}X$ and $\mathbb{Q}U$ are isomorphic as $\mathbb{Q}[G]$-modules, but not canonically so (see [12, p. 91]).

Definition 4.3. A set of units ε_w, one for each place $w \in S_K$, such that

$$\varepsilon_w^\sigma = \varepsilon_{w^\sigma} \text{ for all } \sigma \in G,$$

and such that the only relation among them is

$$\prod_{w \in S_K} \varepsilon_w = 1,$$

is called an ***Artin system of units***.

For a proof of the existence of an Artin system of units, see [1, Ch.5, §3].

Note that an Artin system of units gives the $\mathbb{Z}[G]$-module morphism

$$Y \to U \tag{4.11}$$

which sends w to ε_w for each $w \in S_K$. By definition of X, (4.11) induces an injective $\mathbb{Z}[G]$-module morphism

$$X \hookrightarrow U. \tag{4.12}$$

Now, if we tensor the exact sequence (4.4) with $\mathbb{Q}$, we obtain the exact sequence

$$0 \to \mathbb{Q}X \to \mathbb{Q}Y \to \mathbb{Q} \to 0.$$

It follows that

$$\dim_{\mathbb{Q}}(\mathbb{Q}X) = \dim_{\mathbb{Q}}(\mathbb{Q}Y) - 1 = |S_K| - 1.$$

Since

$$\dim_{\mathbb{Z}}(U) = |S_K| - 1$$

(see [10, Ch. 1, Corollary 11.7]), after tensoring (4.12) with $\mathbb{Q}$, we get a $\mathbb{Q}[G]$-isomorphism

$$\mathbb{Q}X \to \mathbb{Q}U.$$

Let

$$f : \mathbb{Q}X \to \mathbb{Q}U$$

be a $\mathbb{Q}[G]$-isomorphism. f induces an isomorphism of $\mathbb{C}[G]$-modules

$$\mathbb{C}X \xrightarrow{\cong} \mathbb{C}U,$$

which we denote by the same symbol. Composing with λ, we get a $\mathbb{C}[G]$-automorphism of $\mathbb{C}X$

$$\lambda \circ f : \mathbb{C}X \longrightarrow \mathbb{C}X. \tag{4.13}$$

Moreover, given any representation V of G, (4.13) induces an automorphism

$$\begin{aligned} (\lambda \circ f)_V : \mathrm{Hom}_G(V^*, \mathbb{C}X) &\longrightarrow \mathrm{Hom}_G(V^*, \mathbb{C}X) \\ \varphi &\longmapsto \lambda \circ f \circ \varphi \end{aligned}$$

Definition 4.4. The determinant

$$R(V, f) := R_S(V, f) = \det((\lambda \circ f)_V) \tag{4.14}$$

is called the ***Stark regulator***.

Since the definition (4.14) does not depend on the choice of the representation V, we write $R(\chi, f)$ instead of $R(V, f)$.

4.4 Stark's Basic Conjecture

Given a representation V of a finite group G with character $\chi = \chi_V$, we define

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

Let $|G| = n$ for some $n \in \mathbb{N}$. Since $\chi(\sigma)$ is a sum of n-roots of 1 for all $\sigma \in G$, then $\mathbb{Q}(\chi)$ is contained in a cyclotomic field, which is abelian. So, $\mathbb{Q}(\chi)$ is an abelian extension of $\mathbb{Q}$. Set

$$\Delta_\chi := \mathrm{Gal}(\mathbb{Q}(\chi)/\mathbb{Q}).$$

Lemma 4.4.1. *Let K be a Galois extension of $\mathbb{Q}$ contained in $\mathbb{C}$. The map*

$$\begin{aligned} \mathrm{Aut}(\mathbb{C}) &\to \mathrm{Gal}(K/\mathbb{Q}) \\ \alpha &\mapsto \alpha|_K \end{aligned}$$

is a surjective homomorphism, and K is the fixed field of its kernel.

(See [11, p. 23]).

Viewing $\alpha \in \mathrm{Aut}(\mathbb{C})$ as a base extension, we can define the functor

$$\begin{aligned} \mathrm{Rep}_G &\to \mathrm{Rep}_G \\ V &\mapsto \mathbb{C} \otimes_\alpha V \end{aligned}$$

where the action of G on $\mathbb{C} \otimes_\alpha V$ is given by

$$\sigma.(a \otimes x) = \alpha(a) \otimes \sigma.x,$$

for all $\sigma \in G, a \in \mathbb{C}$ and $x \in V$. The map

$$\begin{aligned} V &\to V^\alpha \\ x &\mapsto x^\alpha := 1 \otimes x \end{aligned} \tag{4.15}$$

is an isomorphism of $\mathbb{Q}[G]$-modules. In particular, (4.15) is an "α-linear" map of $\mathbb{C}[G]$-modules, since

$$(ax)^\alpha = 1 \otimes ax = \alpha(a) \otimes x = \alpha(a)(1 \otimes x) = a^\alpha x^\alpha,$$

for all $a \in \mathbb{C}$ and $x \in V$.

Now, fix $\sigma \in G$. Let x be an eigenvector for the action of σ on V of eigenvalue μ_x, that is,

$$\sigma.x = \mu_x x.$$

Then

$$\sigma.(1 \otimes x) = \alpha(1) \otimes \sigma.x = 1 \otimes \mu_x = \alpha(\mu_x) \otimes x = \mu_x^\alpha(1 \otimes x),$$

i.e. $1 \otimes x$ is an eigenvector for the action of σ on V^α of eigenvalue μ_x^α. By the isomorphism (4.15), we have that

$$\{1 \otimes v : v \text{ is in the eigenbasis for the action of } \sigma \text{ on } V\}$$

is an eigenbasis for the action of σ on V^α. Then the character of V^α is given by

$$\chi^\alpha(\sigma) := \mathrm{Tr}(\sigma|_{V^\alpha}) = \alpha(\chi(\sigma)), \text{ for all } \sigma \in G.$$

By this, the character χ^α, and hence the isomorphism class of V^α, depend only on the image $\alpha|_{\mathbb{Q}(\chi)}$ of α in Δ_χ.

Now, consider a Galois extension of number fields K/k. Let V be a representation of the Galois group $G = G_{K/k}$ with character $\chi = \chi_V$. By *Lemma 4.2.3*, we have

$$r(\chi) = \langle \chi, \chi_X \rangle_G = \frac{1}{|G|} \sum_{\sigma \in G} \chi(\sigma)\chi_X(\sigma) = \dim(\mathrm{Hom}_G(V^*, \mathbb{C}X)) \in \mathbb{N},$$

since χ_X is integer valued. We thus have

$$\begin{aligned} r(\chi^\alpha) = \langle \chi^\alpha, \chi_X \rangle_G &= \frac{1}{|G|} \sum_{\sigma \in G} \chi^\alpha(\sigma)\chi_X(\sigma) = \frac{1}{|G|} \sum_{\sigma \in G} \alpha(\chi(\sigma))\chi_X(\sigma) \\ &= \frac{1}{|G|} \sum_{\sigma \in G} \alpha(\chi(\sigma)\chi_X(\sigma)) = \alpha\left(\frac{1}{|G|} \sum_{\sigma \in G} \chi(\sigma)\chi_X(\sigma)\right) \\ &= \frac{1}{|G|} \sum_{\sigma \in G} \chi(\sigma)\chi_X(\sigma) = r(\chi), \end{aligned}$$

for all $\alpha \in \Delta_\chi$. Define

$$A(\chi, f) = A_S(\chi, f) := \frac{R(\chi, f)}{c(\chi)}.$$

Given any representation V of $G_{K/k}$ with character χ, the Stark basic's conjecture states that

- $A(\chi, f) \in \mathbb{Q}(\chi)$;
- $A(\chi, f)^\alpha = A(\chi^\alpha, f)$, for all $\alpha \in \Delta_\chi$.

4.5 The case $r(\chi) = 1$

Let χ be an irreducible character of $G = G_{K/k}$ for which

$$r(\chi) = r_S(\chi) = 1 \tag{4.16}$$

for some S. This means that χ has multiplicity 1 in $\mathbb{C}X$. Moreover,

$$r(\chi^\alpha) = r(\chi) = 1$$

for all $\alpha \in \Delta = \Delta_\chi = \mathrm{Gal}(\mathbb{Q}(\chi)/\mathbb{Q})$. By (4.16),

$$V^\alpha = \mathbb{C} \otimes_\alpha V$$

denotes the unique irreducible constituent of $\mathbb{C}X$ with character χ^α. Let

$$\bar{V} := V^\beta$$

such that

$$\chi^\beta = \bar{\chi}$$

for some $\beta \in \Delta$. In particular,

$$\bar{V} \cong V^*.$$

The central idempotent

$$\begin{aligned} e_\chi^\alpha := e_{\chi^\alpha} &= \frac{\chi^\alpha(1)}{|G|} \sum_{\sigma \in G} \overline{\chi^\alpha(\sigma)} \sigma = \frac{\chi(1)}{|G|} \sum_{\sigma \in G} \chi^\alpha(\sigma^{-1}) \sigma \\ &= \frac{\chi(1)}{|G|} \sum_{\sigma \in G} (\chi(\sigma^{-1}))^\alpha \sigma \in \mathbb{C}[G] \end{aligned}$$

projects $\mathbb{C}X$ onto V^α, and kills all the other irreducible constituents of $\mathbb{C}X$. Consider the sum

$$\pi := \sum_{\alpha \in \Delta} e_\chi^\alpha \in \mathbb{Q}[G].$$

Note that π projects $\mathbb{Q}X$ onto a $\mathbb{Q}[G]$-submodule W of $\mathbb{Q}X$ such that

$$\mathbb{C}W = \sum_{\alpha \in \Delta} V^\alpha.$$

In particular,

$$\chi_W = \chi_{\mathbb{C}} \cdot \chi_W = \chi_{\mathbb{C} \otimes W} = \chi_{\mathbb{C}W} = \sum_{\alpha \in \Delta} \chi^\alpha.$$

For each $\mathbb{C}$-valued function

$$h : \Delta \to \mathbb{C},$$

let

$$\begin{aligned} \mathbb{C}W &\to \mathbb{C}W \\ \sum_{\alpha \in \Delta} v_\alpha &\mapsto \sum_{\alpha \in \Delta} h(\alpha) v_\alpha \end{aligned} \tag{4.17}$$

be the endomorphism of $\mathbb{C}W$ which acts on V^α as a scalar multiplication by $h(\alpha)$. Note that (4.17) is induced by the action of the element

$$\theta_h := \sum_{\alpha \in \Delta} h(\alpha) e_\chi^\alpha.$$

These operators θ_h form a commutative ring which is canonically isomorphic to $\mathbb{C} \otimes_{\mathbb{Q}} \mathbb{Q}(\chi)$ via the map

$$a \otimes z \mapsto a\theta_{h_z},$$

with $a \in \mathbb{C}, z \in \mathbb{Q}(\chi)$, and where

$$h_z(\alpha) \coloneqq z^\alpha \text{ for all } \alpha \in \Delta.$$

Moreover, consider the isomorphism

$$\begin{aligned} \mathbb{C} \otimes_{\mathbb{Q}} \mathbb{Q}(\chi) &\to \mathbb{C}^{|\Delta|} \\ a \otimes z &\mapsto (a \cdot h_z(\alpha))_{\alpha \in \Delta} \end{aligned}$$

So, we have an isomorphism between the commutative ring formed by the operators θ_h and $\mathbb{C}^{|\Delta|}$.

Lemma 4.5.1. *Let*

$$h : \Delta \to \mathbb{C}$$

be a $\mathbb{C}$-valued function. The following are equivalent conditions on h:

(1) $h(1) \in \mathbb{Q}(\chi)$ and $h(\alpha) = h(1)^\alpha$ for all $\alpha \in \Delta$.

(2) $\theta_h \in \mathbb{Q}[G]$.

(3) $\theta_h W \subset W$.

Proof. Denote with H_i the set of $\mathbb{C}$-valued functions

$$h : \Delta \to \mathbb{C}$$

satisfying the condition (i). Let $h \in H_1$. If $\sigma \in G$, the coefficient of σ in θ_h is

$$\frac{\chi(1)}{|G|} \sum_{\alpha \in \Delta} h(\alpha)\chi(\sigma^{-1})^\alpha = \frac{\chi(1)}{|G|} \sum_{\alpha \in \Delta} h(1)^\alpha \chi(\sigma^{-1})^\alpha = \frac{\chi(1)}{|G|} \sum_{\alpha \in \Delta} (h(1)\chi(\sigma^{-1}))^\alpha.$$

By (1),

$$h(1)\chi(\sigma^{-1}) \in \mathbb{Q}(\chi).$$

Then

$$\sum_{\alpha \in \Delta} (h(1)\chi(\sigma^{-1}))^\alpha \in \mathbb{Q}$$

because it is the trace from $\mathbb{Q}(\chi)$ to $\mathbb{Q}$ of $h(1)\chi(\sigma^{-1})$. Thus

$$\theta_h \in \mathbb{Q}[G].$$

Now, let $h \in H_2$. Since W is a $\mathbb{Q}[G]$-submodule of $\mathbb{Q}X$, then

$$\theta_h W \subset W,$$

i.e. $h \in H_3$.

So, we know that

$$H_1 \subset H_2 \subset H_3.$$

Then, if we prove that

$$\dim_{\mathbb{Q}} H_3 \leq \dim_{\mathbb{Q}} H_1, \tag{4.18}$$

we obtain

$$H_1 = H_3, \text{ i.e. } H_3 \subset H_1.$$

Consider the map

$$\begin{aligned} H_1 &\to \mathbb{Q}(\chi) \\ h &\mapsto h(1) \end{aligned} \tag{4.19}$$

Note that (4.19) is a bijection with inverse

$$\begin{aligned} \mathbb{Q}(\chi) &\to H_1 \\ z &\mapsto h_z \end{aligned}$$

In fact, for all $h \in H_1$, we have

$$h_{h(1)}(\alpha) = h(1)^{\alpha} = h(\alpha).$$

On the other hand, for all $z \in \mathbb{Q}(\chi)$, we obtain

$$h_z(1) = z^1 = z.$$

So, we have to show that

$$\dim_{\mathbb{Q}} H_3 \leq |\Delta|,$$

since

$$|\Delta| = [\mathbb{Q}(\chi) : \mathbb{Q}] = \dim_{\mathbb{Q}} H_1$$

by the bijection (4.19). Now, the maps

$$\begin{aligned} H_3 &\to \operatorname{End}_{\mathbb{Q}[G]}(W) \\ h &\mapsto \theta_h \end{aligned}$$

and

$$\mathbb{C} \otimes_{\mathbb{Q}} \operatorname{End}_{\mathbb{Q}[G]}(W) \to \operatorname{End}_{\mathbb{C}[G]}(\mathbb{C}W)$$

defined as

$$\begin{aligned} \mathbb{C}W &\to \mathbb{C}W \\ b \otimes x &\mapsto (ab) \otimes f(x) \end{aligned}$$

are injective. Hence

$$\begin{aligned} \dim_{\mathbb{Q}} H_3 &\le \dim_{\mathbb{Q}} \operatorname{End}_{\mathbb{Q}[G]}(W) = \dim_{\mathbb{C}}(\mathbb{C} \otimes_{\mathbb{Q}} \operatorname{End}_{\mathbb{Q}[G]}(W)) \\ &\le \dim_{\mathbb{C}} \operatorname{End}_{\mathbb{C}[G]}(\mathbb{C}W) = \dim_{\mathbb{C}} \operatorname{End}_{\mathbb{C}[G]} \left(\sum_{\alpha \in \Delta} V^{\alpha} \right) \\ &= \dim_{\mathbb{C}} \left(\prod_{\alpha \in \Delta} \operatorname{End}_{\mathbb{C}[G]}(V^{\alpha}) \right) = |\Delta|. \end{aligned}$$

□

Now let

$$f : \mathbb{Q}X \to \mathbb{Q}U$$

be a $\mathbb{Q}[G]$-homomorphism and put:

- $A \coloneqq \sum_{\alpha \in \Delta} A(\chi^{\alpha}, f) e_{\bar{\chi}^{\alpha}}$.
- $c \coloneqq \sum_{\alpha \in \Delta} c(\chi^{\alpha}) e_{\bar{\chi}^{\alpha}} = \sum_{\alpha \in \Delta} \partial_s L_S(0, \chi^{\alpha}) e_{\bar{\chi}^{\alpha}}$.
- $R \coloneqq \sum_{\alpha \in \Delta} R(\chi^{\alpha}, f) e_{\bar{\chi}^{\alpha}}$.

Theorem 4.5.2. *Let χ be an irreducible character of G such that*

$$r(\chi) = 1.$$

Let

$$W_U \coloneqq f(W) = \pi \mathbb{Q}U.$$

The following assertions are equivalent:

(1) Stark's Basic Conjecture is true for χ.

(2) $cW = \lambda(W_U)$.

(3) For all $z \in \mathbb{Q}(\chi)^*$,

$$\gamma(z, \chi)\mathbb{Q}X \subset \lambda(\mathbb{Q}U),$$

where

$$\gamma(z, \chi) \coloneqq \sum_{\alpha \in \Delta} h_z(\alpha) \cdot \partial_s L_S(0, \chi^{\alpha}) e_{\bar{\chi}^{\alpha}}.$$

Proof. We start proving the equivalence between the conditions (1) and (2). If we apply *Lemma 4.5.1* with

$$h(\alpha) = A(\chi^\alpha, f),$$

we have that Stark's Basic Conjecture holds for χ if, and only if,

$$AW \subset W.$$

Note that each of the three operators A, c and R act injectively on $\mathbb{C}W$. By definition of W, we have that

$$W \subset AW.$$

Thus we have

$$AW \subset W \Leftrightarrow W = AW \Leftrightarrow cW = cAW. \tag{4.20}$$

By definition of $A(\chi, f)$, we have that

$$cA = R,$$

because

$$\begin{cases} e_{\bar{\chi}^\alpha} e_{\bar{\chi}^\beta} = 0 & \text{if } \alpha \neq \beta \\ e_{\bar{\chi}^\alpha} e_{\bar{\chi}^\beta} = e_{\bar{\chi}^\alpha} & \text{if } \alpha = \beta \end{cases}.$$

So,

$$AW \subset W \Leftrightarrow cW = RW. \tag{4.21}$$

It remains to prove that

$$RW = \lambda(W_U).$$

For each $\alpha \in \Delta$, R acts on $\bar{V}^\alpha$ by the scalar $R(\chi^\alpha, f)$. By definition, the Stark regulator $R(\chi^\alpha, f)$ is the determinant of the endomorphism

$$(\lambda \circ f)_{V^\alpha} : \mathrm{Hom}_{\mathbb{C}[G]}(\bar{V}^\alpha, \mathbb{C}X) \longrightarrow \mathrm{Hom}_{\mathbb{C}[G]}(\bar{V}^\alpha, \mathbb{C}X),$$

where

$$\mathrm{Hom}_{\mathbb{C}[G]}(\bar{V}^\alpha, \mathbb{C}X) = \mathrm{Hom}_{\mathbb{C}[G]}(\bar{V}^\alpha, \bar{V}^\alpha).$$

Since, by *Lemma 4.2.3*,

$$\dim \mathrm{Hom}_{\mathbb{C}[G]}(\bar{V}^\alpha, \bar{V}^\alpha) = r(\chi) = 1,$$

then $R(\chi^\alpha, f)$ is the same as the scalar by which $\lambda \circ f$ acts on $\bar{V}^\alpha$. Hence

$$RW = (\lambda \circ f)(W) = \lambda(f(W)) = \lambda(W_U).$$

Thus, by (4.21), we can conclude that

$$AW \subset W \Leftrightarrow cW = \lambda(W_U),$$

that is, the conditions (1) and (2) are equivalent.

Now, assume

$$cW = \lambda(W_U).$$

If $z = 0$, we have that the condition (3) holds. If $z \neq 0$, then

$$\theta_{h_z}\mathbb{Q}X = W,$$

since θ_{h_z} maps $\mathbb{Q}X$ isomorphically in W. Hence

$$\gamma(z, \chi)\mathbb{Q}X = c\theta_{h_z}\mathbb{Q}X = cW.$$

Since

$$W = \pi U \subset \mathbb{Q}U,$$

we can conclude that

$$\gamma(z, \chi)\mathbb{Q}X = \lambda(W_U) \subset \lambda(\mathbb{Q}U).$$

On the other hand, applying π to (3) with $z = 1$, we obtain

$$\pi(c\mathbb{Q}X) \subset \pi(\lambda(\mathbb{Q}U)), \tag{4.22}$$

where

$$\pi(c\mathbb{Q}X) = c\pi(\mathbb{Q}X) = cW,$$

and

$$\pi(\lambda(\mathbb{Q}U)) = \lambda(\pi(\mathbb{Q}U)) = \lambda(W_U)$$

with

$$\lambda(W_U) = \lambda(\pi\mathbb{Q}U)) \cong \lambda(\pi\mathbb{Q}X)) = \lambda(W) \cong W.$$

Since

$$\dim_{\mathbb{Q}}(cW) = \dim_{\mathbb{Q}}(W) = \dim_{\mathbb{Q}}(\lambda(W_U)),$$

by (4.22) we can conclude that

$$cW = \lambda(W_U).$$

□

4.6 Stark units

Let Ψ be a set of irreducible characters of G such that

(1) The trivial character is not contained in Ψ.

(2) For all $\chi \in \Psi$, we have

$$\chi^\alpha \in \Psi \text{ for all } \alpha \in \mathrm{Aut}(\mathbb{C}).$$

Let $(z_\chi)_{\chi\in\Psi}$ be a family of complex numbers satisfying

$$z_{\chi^\alpha} = z_\chi^\alpha$$

for all $\chi \in \Psi$ and for all $\alpha \in \mathrm{Aut}(\mathbb{C})$. Assuming Stark's Basic Conjecture, *Theorem 4.5.2* implies that

$$\left(\sum_{\chi\in\Psi} z_\chi \partial_s L_S(0,\chi) e_{\bar{\chi}}\right) \cdot X \subset \lambda(\mathbb{Q}U), \tag{4.23}$$

Since the trivial character is not in Ψ, we can replace X by Y in (4.23). For each $w \in S_K$, then there exists a $m \in \mathbb{N}_{>0}$ and a S_K-unit ε of K such that

$$\lambda(\varepsilon) = m \sum_{\chi\in\Psi} z_\chi \partial_s L_S(0,\chi) e_{\bar{\chi}} \cdot w. \tag{4.24}$$

Suppose for simplicity that there is a $v \in S$ which splits completely, and fix a place w of K lying above v. Since

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

we can rewrite (4.24) as

$$\lambda(\varepsilon) = \sum_{\sigma\in G} \left(\frac{m}{|G|} \sum_{\chi\in\Psi} \chi(1) z_\chi \partial_s L_S(0,\chi)\chi(\sigma)\right) \cdot \sigma w,$$

where

$$\lambda(\varepsilon) = \sum_{u\in S_K} \log|\varepsilon|_u \cdot u = \sum_{w'\nmid v} \log|\varepsilon|_{w'} \cdot w' + \sum_{\sigma\in G} \log|\varepsilon|_{\sigma w} \cdot \sigma w.$$

Then the equation (4.24) is equivalent to the conditions

$$\begin{cases} |\varepsilon|_{w'} = 1 & \text{if } w' \nmid v \\ \log|\varepsilon|_{\sigma w} = \frac{m}{|G|} \sum_{\chi\in\Psi} \chi(1) z_\chi \partial_s L_S(0,\chi)\chi(\sigma) & \text{for all } \sigma \in G \end{cases}. \tag{4.25}$$

Definition 4.5. A S_K-unit ε which solves the system of equations (4.25) is called a ***Stark unit***.

Note that, if a Stark unit exists, it is determined up to a root of unity in K.

Example 7. Suppose v is a real place which splits completely in K. Let w be a place of K which lies above v given by the embedding

$$\sigma_w : K \hookrightarrow \mathbb{R}.$$

Note that

$$\varepsilon = \pm|\sigma_w(\varepsilon)| = \pm|\varepsilon|_w = \pm e^{\log|\varepsilon|_w}.$$

Since for all $\sigma \in G$

$$|\varepsilon|_{\sigma w} = |\varepsilon^{\sigma^{-1}}|_w,$$

we find

$$\varepsilon^{\sigma^{-1}} = \pm e^{\log|\varepsilon^{\sigma^{-1}}|_w} = \pm e^{\log|\varepsilon|_{\sigma w}} = \pm e^{\frac{m}{|G|}\sum_{\chi\in\Psi}\chi(1)z_\chi\partial_s L_S(0,\chi)\chi(\sigma)}.$$

If K/k is abelian and S contains the places v ramified in K, Stark has conjectured that, if $\mu(K)$ is the group of unity in K, then

$$m = |\mu(K)|,$$

will do for the case

$$z_\chi = 1 \text{ for all } \chi.$$

The non-abelian case is unclear instead. So, in general one supposes m is small, at least in the case K is totally real.

If we found a valid m and double it, we obtain for all $\sigma \in G$ that

$$\varepsilon^{2\sigma^{-1}} = e^{\frac{2m}{|G|}\sum_{\chi\in\Psi}\chi(1)z_\chi\partial_s L_S(0,\chi)\chi(\sigma)}.$$

So we can calculate real numbers close to the conjugates of ε at a real place w. We can then compute approximations to the coefficients of the polynomial

$$f(X) = \prod_{\sigma\in G}(X - \varepsilon^\sigma) \in k[X],$$

and try to find the small integers in k which are those coefficients. Finally, we can check that the roots of the polynomial $f(X)$ generate the starting extension of number fields K/k.

Example 8. Another special case in which the conjecture is a classical result is when

$$k = \mathbb{Q}$$

and K is the real subfield of the group of n-th roots of 1. In fact, we have that the Stark unit is

$$2 - 2\cos(\frac{2\pi}{n}).$$

Bibliography

[1] E. Artin & J. Tate, *Class Field Theory*, AMS Chelsea, 2008.

[2] J.W.S. Cassels & A. Fröhlich, *Algebraic Number Theory*, Thompson Book Company Inc., 1967

[3] K. Conrad, *Ostrowski for Number Field*, `https://kconrad.math.uconn.edu/blurbs/gradnumthy/ostrowskinumbfield.pdf`.

[4] S. Dasgupta, *Stark's Conjectures*, `https://services.math.duke.edu/~dasgupta/papers/Dasguptaseniorthesis.pdf`.

[5] S. Lang, *Algebra*, Springer, 2002.

[6] S. Lang, *Algebraic Number Theory*, Springer, 1994.

[7] D.A. Marcus, *Number Fields*, Springer.

[8] J.S. Milne, *Algebraic Number Theory*, `https://www.jmilne.org/math/CourseNotes/ANT.pdf`.

[9] J.S. Milne, *Class Field Theory*, `https://www.jmilne.org/math/CourseNotes/CFT.pdf`.

[10] J. Neukirch, *Algebraic Number Theory*, Springer, 1999.

[11] C. Popescu, K. Rubin & A. Silverberg, *Arithmetic of L-functions*, AMS, 2011.

[12] J.-P. Serre, *Linear Representations of Finite Groups*, Springer-Verlag, 1977.

[13] B. Steinberg, *Representation Theory of Finite Groups. An Introductory Approach*, Springer, 2012.

[14] A.V. Sutherland, *Number Theory 1*, `http://math.mit.edu/classes/18.785/2015fa/LectureNotes21.pdf`.

[15] A.V. Sutherland, *Number Theory 1*, http://math.mit.edu/classes/18.785/2016fa/LectureNotes21.pdf.

[16] J. Tate, *Les Conjectures de Stark sur les Fonctions L d'Artin en s = 0*, Birkhäuser, 1984.

[17] L.C. Washington, *Introduction to Cyclotomic Fields*, Springer, 1997.