Class Field Theory, L-Functions, Modular Curves, Eichler-Shimura and Taniyama-Shimura: motivating Langlands-type conjectures for undergraduates

An M3R project summary paper at Imperial College London

Student: Yourong Zang
CID: 01861742
Supervisor: Prof. David Helm

Plagiarism statement: This is my own work unless otherwise stated.

Abstract

In this paper I introduced class field theory, following which is a discussion of different L-functions. Two different formulations of Hecke L-functions were provided, featuring Tate's thesis and the adelization of Hecke characters. A very motivated and detailed section on Artin L-function was written, emphasizing on its motivation and origin. From the class field theory and Hecke L-functions, I concluded the first part by a Langlands-type correspondence.

In the second half of the paper, I introduced different properties of modular forms, elliptic curves and general algebraic curves. I also talked about Hecke operators in depth, giving their Fourier expansions. Modular curves were approached from three distinct viewpoints — complex, algebraic, and Katz-Mazur. I then proceed to proving the Eichler-Shimura relation, for which I gave a detailed proof and some very fine comments. The paper ends with some notes on how one could treat the two parts of this paper as special cases of the Langlands program, without providing any actual definition related to the modern formulation.

Acknowledgements

I want to thank my great supervisor Prof. David Helm for his kindness, patience and infinite support, as well as the wonderful topics he suggested. His lectures are the most inspiring, and nothing in the texts could compare.

I also want to thank the great people who have studied these topics before me. Without their succinct notes, my project could not be this smooth.

Contents

Chapter 1

Introduction

I will start this summary paper with several elementary but significant results in number theory. It is my belief that they perfectly foreshadow what comes next in the remaining fifty pages of the report. I have cut this introduction into several small sections according to the phenomena they demonstrate. One should not regard the content of this section as some sort of preliminary but as inspirations that can be taken less seriously.

A comment from the author after the completion of this report: the author uses "prime" and the notation $\mathfrak{p}$ for (possibly infinite) places in global fields. Indeed, finite places arise from nonzero prime ideals of $\mathfrak{o}_K$, but that's not true for some infinite places. The reason for this usage is that (1) sometimes places are referred to as primes and (2) I learned valuation theory with notations like $\mathfrak{p} \mid \infty$. Therefore, please accept my sincere apologies for the potential confusion. To avoid it, note that I only refer to prime ideals of rings of integers as "primes of the fields" in the case of ramifications of prime ideals where valuations are not involved. In other scenarios, I will specify whether a prime is finite or infinite so that the readers will realize I'm talking about places.

1.1 Ramification theory

We begin with a brief recollection of some ramification theory. Let L/K be a Galois extension (of some number field in this report) K and $\mathfrak{P}$ a prime ideal of $\mathfrak{o}_L$ lying above a fixed prime $\mathfrak{p}$ of K. Recall the **decomposition group**

$$D_{\mathfrak{P}} = \{\sigma \in \operatorname{Gal}(L/K) : \sigma(\mathfrak{P}) = \mathfrak{P}\}$$

and the **inertia subgroup**

$$I_{\mathfrak{P}} = \{\sigma \in D_{\mathfrak{P}} : \forall x \in \mathfrak{o}_L, \sigma(x) = x \bmod \mathfrak{P}\}$$

An element $\sigma \in D_{\mathfrak{P}}$ induces an automorphism $\tilde{\sigma} : a \mapsto \sigma(a)$ on $\mathfrak{o}_L/\mathfrak{P}$, as $\sigma(\mathfrak{o}_L) = \mathfrak{o}_L$ and $\sigma\mathfrak{P} = \mathfrak{P}$. The map $\sigma \mapsto \tilde{\sigma}$ is surjective (a nontrivial result) with kernel $I_{\mathfrak{P}}$. Note that the Galois group $G = \operatorname{Gal}(L/K)$ acts on the primes over $\mathfrak{p}$ transitively. To see this, fix some $\mathfrak{P}$ lying above $\mathfrak{p}$. Suppose $\mathfrak{P}'$ is a prime over $\mathfrak{p}$ and $\mathfrak{P}'$ is not $\sigma\mathfrak{P}$ for any $\sigma \in G$. Then by the Chinese remainder theorem there exists an element $x \in \mathfrak{o}_L$ such that $x \in \mathfrak{P}'$ but $x \notin \sigma\mathfrak{P}$ for any σ. Then $N_{L/K}(x) = \prod \sigma(x) \in \mathfrak{P}' \cap \mathfrak{o}_K = \mathfrak{p}$. But on the other hand we have $\sigma(x) \notin \mathfrak{P}$ for any σ, so $N_{L/K}(x) \notin \mathfrak{P} \cap \mathfrak{o}_K = \mathfrak{p}$, a contradiction. Then as σ varies over a set of representatives of the cosets $G/D_{\mathfrak{P}}$, the primes $\sigma\mathfrak{P}$ vary over all primes over $\mathfrak{p}$. In fact, we may apply this result to show that the ramification indices and inertia degrees of primes over $\mathfrak{p}$ are the same for Galois extensions.

It is worth the time to study the fixed fields $E_{\mathfrak{P}}$ and $F_{\mathfrak{P}} \subseteq L$ of $D_{\mathfrak{P}}$ and $I_{\mathfrak{P}}$. Denote by $\mathfrak{P}_1 = E_{\mathfrak{P}} \cap \mathfrak{P}$ the prime in $E_{\mathfrak{P}}$ below $\mathfrak{P}$. Then $\operatorname{Gal}(L/E_{\mathfrak{P}}) = D_{\mathfrak{P}}$ which acts transitively on the primes lying over $\mathfrak{P}_1$ (including $\mathfrak{P}$), which then suggests $\mathfrak{P}_1$ is just a power of $\mathfrak{P}$ in $\mathfrak{o}_L$. We may then deduce from the fundamental formula and the argument in the previous paragraph that $\#G = efg$ where e and f are the ramification index and inertia degree of $\mathfrak{P}$ over $E_{\mathfrak{P}}$, and $g = \#G/D_{\mathfrak{P}}$. Thus, $\#D_{\mathfrak{P}} = ef$. If e_1 and e_2 (f_1 and f_2) are the ramification indices (inertia degrees) of $\mathfrak{P}$ over $E_{\mathfrak{P}}$ and $\mathfrak{P}_1$ over K respectively, we have $e = e_1e_2$, $f = f_1f_2$, and $ef = \#D_{\mathfrak{P}} = [L : E_{\mathfrak{P}}] = e_1f_1$, meaning $e_2 = f_2 = 1$. Thus, $\mathfrak{P}_1$ splits completely over K. Similarly define $\mathfrak{P}_2 = \mathfrak{P} \cap F_{\mathfrak{P}}$.

Back to the map $\sigma \mapsto \tilde{\sigma}$ which induces an isomorphism $D_{\mathfrak{P}}/I_{\mathfrak{P}} \to \mathrm{Gal}(\kappa(\mathfrak{P})/\kappa(\mathfrak{p}))$ which suggests $\#D_{\mathfrak{P}}/I_{\mathfrak{P}} = [\kappa(\mathfrak{P}) : \kappa(\mathfrak{p})] = f$ and thus we get from $\#D_{\mathfrak{P}} = ef$ the equality $\#I_{\mathfrak{P}} = e$. Summarizing the above:

Lemma 1.1.1. *Let $\mathfrak{p} = \mathfrak{P} \cap \mathfrak{o}_K$. Then every element $\sigma \in D_{\mathfrak{P}}$ induces an automorphism $\tilde{\sigma}$ on $\kappa(\mathfrak{P})$ that fixes $\kappa(\mathfrak{p})$. The map $D_{\mathfrak{P}} \to \tilde{G} = \mathrm{Gal}(\kappa(\mathfrak{P})/\kappa(\mathfrak{p}))$ defined by $\sigma \mapsto \tilde{\sigma}$ is a surjective homomorphism with kernel $I_{\mathfrak{P}}$. Moreover, $\#I_{\mathfrak{P}} = e_{\mathfrak{P}|\mathfrak{p}}$, and $\#D_{\mathfrak{P}} = e_{\mathfrak{P}|\mathfrak{p}}f_{\mathfrak{P}|\mathfrak{p}}$. The prime $\mathfrak{P}$ has ramification index e and inertia degree 1 over $\mathfrak{P}_2$, which has ramification index 1 and inertia degree f over $\mathfrak{P}_1$, which has trivial ramification index and inertia degree over $\mathfrak{p}$.*

Corollary 1.1.1. *A prime $\mathfrak{p}$ is unramified if and only if for any $\mathfrak{P}$ lying above, $I_{\mathfrak{P}}$ is trivial. In this case $\mathrm{Gal}(\kappa(\mathfrak{P})/\kappa(\mathfrak{p}))$ is a subgroup of $\mathrm{Gal}(L/K)$.*

Proof. Apply $e = 1$ to the identity $\#I_{\mathfrak{P}}$. Then $I_{\mathfrak{P}}$ is trivial, from which we have

$$\mathrm{Gal}(\kappa(\mathfrak{P})/\kappa(\mathfrak{p})) \cong D_{\mathfrak{P}}/1 = D_{\mathfrak{P}} \leq \mathrm{Gal}(L/K).$$

□

1.2 The Local to Global Principle

Let K be a field and v a valuation on K. For each v we have the completion K_v and its algebraic closure $\bar{K}_v$. The valuation can be naturally extended to K_v and $\bar{K}_v$. Let L/K be an algebraic extension, we have a K-embedding $\tau : L \to \bar{K}_v$. We obtain a valuation $w = \bar{v} \circ \tau$. In the language of absolute values $|x|_w = |\tau x|_{\bar{v}}$.

Lemma 1.2.1 (product formula)**.** *If L/K is separable, then $L \otimes_K K_v \cong \prod_{w|v} L_w$.*

Proof. Let α be a primitive element of L/K with minimal polynomial f. For every $w \mid v$, there is an irreducible factor $f_w(X)$ of $K_v[X]$ such that, by L/K's separability, $f(X) = \prod_{w|v} f_w(X)$. Note that $L_w = K_v(\alpha_w)$ where α_w is the image of α in L_ω, and f_w is the minimal polynomial of α_w over K_w. By the Chinese remainder theorem, we get

$$K_v[X]/(f) \cong \prod_{w|v} K_v[X]/(f_w)$$

where $K_v[X]/(f) = K_v \otimes_K K[X](f) = L \otimes K_v$ and $K_v[X]/(f_w) = L_w$, completing the proof. □

Corollary 1.2.1. *We have, if L/K is separable,*

$$[L : K] = \sum_{w|v} [L_w : K_v]$$

and

$$N_{L/K} = \prod_{w|v} N_{L_w/K_v}, \quad Tr_{L/K} = \sum_{w|v} Tr_{L_w/K_v}$$

Proof. The dimension of L over K is the dimension of $L \otimes_K K_v$ over K_v, so with the product formula we get the desired result. □

Remark 1.2.1. We thus can prove the fundamental identity using a $\mathfrak{p}$-valuation for any prime ideal $\mathfrak{p}$ of K.

Now if L/K is Galois. The Galois group $\mathrm{Gal}(L/K)$ acts transitively on the set of places dividing v. We also define the **decomposition group** $D_{w|v} = \{\sigma \in \mathrm{Gal}(L/K) : \omega \circ \sigma = \omega\}$ and the inertia subgroup $I_{w|v}$ in the similar manner as that in ramification theory. Note that $D_{w|v}$ is closed in $\mathrm{Gal}(L/K)$. Given another Galois extension L'/K', a homomorphism $\tau : L \to L$ induces a homomorphism $\tau^* : \mathrm{Gal}(L'/K') \to \mathrm{Gal}(L/K)$ by conjugation. Let w' be a valuation lying over $v' = w'|_{K'}$ in L' and $w = w' \circ \tau$, $v = w|_K$. The map τ induces homomorphism of decomposition groups and in case v is nonarchimedean, the map induces homomorphisms of inertia subgroups.

Lemma 1.2.2. *The decomposition group $D_{w|v}$ is isomorphic tot* $\mathrm{Gal}(L_w/K_v)$.

Proof. The decomposition group consists of those automorphisms continuous with respect to the valuation w. The forward direction is obvious. For the converse, if $|x|_w < 1$, then for any continuous automorphism σ we have $|\sigma x|_w = |x|_{w\circ\sigma} < 1$ for arbitrary $x \in L$. This implies w and $w \circ \sigma$ are equivalent, so $w|_K = w \circ \sigma_K$ and $\sigma \in D_{w|v}$. Since L is dense in L_w, we may extend $\sigma \in D_{w|v}$ by continuity to $\mathrm{Gal}(L_w/K_v)$. □

1.3 A Master Moduli Problem

We try to find the moduli space of the moduli problem following the procedures in [Bou14]:

$$\mathcal{F} : S \mapsto \{(E, P) : E \text{ an elliptic curve over } S, P \in E(S) \text{ not of order } 1, 2, 3 \text{ in any fiber}\}$$

Write $E(\alpha, \beta)$ be the subscheme of $\mathfrak{P}^2_S$ defined by the Tate normal form

$$E(\alpha, \beta) : Y^2Z + \alpha XYZ + \beta YZ^2 = X^3 + \beta X^2Z$$

and its discriminant is

$$\Delta(\alpha, \beta) = \beta^3(\alpha^4 - \alpha^3 + 8\alpha^2\beta - 36\alpha\beta + 16\beta^2 + 27\beta)$$

Theorem 1.3.1. *The scheme* $\mathrm{Spec}\, \mathbb{Z}[A, B, \Delta(A, B)^{-1}]$ *is a moduli space for $\mathcal{F}$ with universal family $(E(A, B), (0, 0))$.*

Proof. We first prove a lemma for simplification.

Lemma 1.3.1. *For any scheme S, E/S an elliptic curve and P an S-point not of order $1, 2, 3$. Then there exist unique $\alpha, \beta \in \Gamma(S, \mathcal{O}_S)$ such that $\Delta(\alpha, \beta)$ is nonzero, and a unique isomorphism $E(\alpha, \beta) \cong E$ mapping $[0 : 0 : 1]$ to P.*

Proof. This is easy if E has a Weierstrass equation over S. In this case we may assume $P = (0, 0)$ by a linear transformation, and since $2P \neq 0$ then we can obtain the equation $Y^2 + a_1XY + a_3Y = X^3 + a_2X^2$ since the tangent line at P is not vertical. Since P does not have order 3, $(0, 0)$ is not an inflection point, meaning a_2 is a unit. Rescaling again, we may assume $a_2 = a_4$ and thus $E(a_1, a_2)$ is a Tate normal form. In general, there is an affine covering of S on which E has Weierstrass equations. Gluing their sheaves together we get the result. □

Now we may always assume the point $P = [0 : 0 : 1]$ sits inside $E(S)$. We can compute $-P = (0, -\beta)$, $2P = (-\beta, \beta(\alpha - 1))$, $-2P = (-\beta, 0)$, $3P = (1 - \alpha, \alpha - \beta - 1)$ and $-3P = (1 - \alpha, (\alpha - 1)^2)$. Then if $E(\alpha, \beta)$ is an elliptic curve, i.e., $\Delta(\alpha, \beta)$ is a unit, then P is a point not of order $1, 2, 3$. Thus, the scheme $\mathrm{Spec}\, \mathbb{Z}[A, B, \Delta(A, B)^{-1}]$ is a moduli space, and by the previous lemma, $(E(A, B), (0, 0))$ is a universal family. □

Example 1.3.1. We can use this master functor to classify other functors:

$$\mathcal{F} : S \mapsto \{(E, P) : E \text{ an elliptic curve over } S, P \in E(S) \text{ of exact order 5 in all fibers}\}$$

In this case we need $3P = -2P$ so $1 - A = -B$ meaning $A = 1 + B$. Thus the scheme became $\operatorname{Spec} \mathbb{Z}[B, \Delta(1 + B, B)]$ and the universal family is $(E(1 + B, B), (0, 0))$.

1.4 Tate Modules and the Frobenius

Fix a prime number p. Consider the l-adic Tate module of modular curves $T_l J$ for any prime $l \neq p$. On the Tate module we have the Frobenius map acting naturally. But note that $T_l J = \varprojlim J(\bar{\mathbb{Q}})[l^n]$ on which $\operatorname{Gal}(\overline{Q_p}/\mathbb{Q}_p)$ acts in the canonical way. The limit further reduces to $\varprojlim J(\overline{\mathbb{F}_p})[l^n]$ modulo a prime ideal of $\bar{\mathbb{Z}}$ lying over p. But in this case the Galois group is generated by a Frobenius element Frob_p. In the last chapter we will show that the Hecke operator (which also defines an action on the Jacobian, will be discussed later in the paper) $T_p = \operatorname{Frob}_p + p \operatorname{Frob}^{-1}$ on the reductions. This suggests $\operatorname{Frob}_p^2 - T_p \operatorname{Frob}_p + p = 0$ which gives us a characteristic polynomial of the Frobenius map on the Tate module.

Chapter 2

Class Field Theory

2.1 Classical Formulation

Before Chevalley introduced the modified ideals — idèles — mathematicians only had the ideal class groups to classify all abelian extensions of a number field. Heinrich Weber realized the normal ideal class group Cl_K and $\mathrm{Gal}(\mathbb{Q}(\mu_m)/\mathbb{Q})$ are just instances of ray class groups. In this section, we will introduce (with some proofs omitted) some basic notions and relevant results in global class field theory following the historical approach to special phenomena in algebraic number theory. The primary source for this section is [Cox14], with some of the histories taken from [Neu99].

2.1.1 Basic notions

Suppose K is a global field (i.e., a number field or a function field).

Definition 2.1.1. A **modulus** (or modulus) $\mathfrak{m}$ in K is a formal product

$$\mathfrak{m} = \prod_{\mathfrak{p}} \mathfrak{p}^{n_{\mathfrak{p}}}$$

where $\mathfrak{p}$ varies over all places of K; furthermore, the exponents satisfy:

(i) $n_{\mathfrak{p}} = 0$ for all but finitely many places,

(ii) $n_{\mathfrak{p}} = 0$ if $\mathfrak{p}$ is a complex infinite place,

(iii) $n_{\mathfrak{p}} \leqslant 1$ if $\mathfrak{p}$ is a real infinite place and K is a number field; if K is a function field then $n_{\mathfrak{p}} = 0$.

We will restrict our attention to number fields K. Rearranging the order, a modulus can be expressed as the product $\mathfrak{m}_0\mathfrak{m}_\infty$ where $\mathfrak{m}_0$ is an ideal in $\mathfrak{o}_K$ (by Ostrowski finite places corresponds to prime ideals of the ring of integers) and $\mathfrak{m}_\infty$ is the product of real infinite primes of K. Note that if K is totally imaginary, we simply see $\mathfrak{m}$ as an ideal of $\mathfrak{o}_K$.

Let $I_K(\mathfrak{m})$ be the group of all fractional ideals of K relatively prime to $\mathfrak{m}_0$, and $P_K(\mathfrak{m})$ the subgroup generated by the principal ideals $\alpha\mathfrak{o}_K$ where $\alpha \in K^\times$ and $\alpha \equiv 1 \pmod{\mathfrak{m}_0}$ and $\sigma(\alpha) > 0$ for all real infinite primes σ in $\mathfrak{m}_\infty$.

Remark 2.1.1. $P_K(\mathfrak{m})$ has finite index in $I_K(\mathfrak{m})$.

Definition 2.1.2. A subgroup H of $I_K(\mathfrak{m})$ containing $P_K(\mathfrak{m})$ is called a **congruence subgroup** and the quotient $I_K(\mathfrak{m})/H$ is a **ray class group** for $\mathfrak{m}$.

Remark 2.1.2. Here is a historical note on the term *ray*. Certainly ray is not a person. The concept of generalized ideal class groups was first studied by Weber, and later Hasse coined the term *ray class group* in 1926. Translated from the German word *Strahlklassengruppe* where *Strahl* means a ray or a beam, the terminology emphasizes our positivity condition on the principal ideals. Interestingly, according to [Lem12], the word "ray" was originally used by Rudolf Fueter in his text on complex multiplication, predating Hasse's usage by several years. It is also worth mentioning that Italian mathematicians refer to the ray class group as *gruppo delle classi modulo* $\mathfrak{m}$, so they never worried about the term ray!

We therefore could define the Artin symbol with respect to an unramified prime.

Lemma 2.1.1. *Let L/K be Galois and $\mathfrak{p}$ an unramified prime. Then if $\mathfrak{P}$ is a prime of L lying over $\mathfrak{p}$, there is a unique element $\sigma \in G = \mathrm{Gal}(L/K)$, up to conjugacy, such that for all $\alpha \in \mathfrak{o}_L$,*

$$\sigma(\alpha) = \alpha^{N(\mathfrak{p})} \bmod \mathfrak{P}$$

where $N(\mathfrak{p}) = |\mathfrak{o}_k/\mathfrak{p}|$.

Proof. The Galois group $\tilde{G}$ of $\kappa(\mathfrak{P})/\kappa(\mathfrak{p})$ where $q = |\mathfrak{o}_k/\mathfrak{p}|$ has a generator given by the Frobenius map $x \mapsto x^q$. Then since $\mathfrak{p}$ is unramified, by Corollary 1.1.1, $I_{\mathfrak{P}}$ is trivial, meaning there is a unique element $\sigma \in D_{\mathfrak{P}}$ which maps to the Frobenius morphism. By construction,

$$\sigma(\alpha) = \alpha^{N(\mathfrak{p})} \bmod \mathfrak{P}$$

for all $\alpha \in \mathfrak{o}_L$. The uniqueness of σ up to conjugacy in G simply follows from the fact that if $\tau \in G$ satisfies the same condition, it must lie in $D_{\mathfrak{P}}$. □

Definition 2.1.3. The unique element in the last lemma is called the **Frobenius element**, usually denoted by $\sigma_{\mathfrak{P}|\mathfrak{p}}$. We also call the map $\mathfrak{P} \mapsto \sigma_{\mathfrak{P}|\mathfrak{p}}$ the **Artin symbol**, defined by

$$\left(\frac{L/K}{\mathfrak{P}}\right) \text{ such that } \left(\frac{L/K}{\mathfrak{P}}\right)(\alpha) = \alpha^{N(\mathfrak{p})} \bmod \mathfrak{P}$$

Remark 2.1.3. If L/K is an abelian extension, we will show the symbol only depends on the prime $\mathfrak{p}$. In this case, we have a map on prime ideals $\left(\frac{L/K}{\cdot}\right)$.

Lemma 2.1.2. *The Artin symbol only depends on the prime $\mathfrak{p}$ of K if L/K is an abelian extension.*

Proof. Note that by the uniqueness of the Artin symbol, the symbol defined by $\sigma\mathfrak{P}$ is given by

$$\left(\frac{L/K}{\sigma\mathfrak{P}}\right) = \sigma\left(\frac{L/K}{\mathfrak{P}}\right)\sigma^{-1}.$$

We concluded in Section 1.1 that the Galois group G acts transitively on primes lying over $\mathfrak{p}$. Thus, for any two $\mathfrak{P}, \mathfrak{P}'$ lying over $\mathfrak{p}$, there is some $\sigma \in G$ such that $\sigma\mathfrak{P} = \mathfrak{P}'$. This means

$$\left(\frac{L/K}{\mathfrak{P}'}\right) = \sigma\left(\frac{L/K}{\mathfrak{P}}\right)\sigma^{-1} = \left(\frac{L/K}{\mathfrak{P}}\right)$$

since G is abelian. □

Example 2.1.1. The Frobenius element is unique up to conjugacy, and we must deal with this small problem in some particular cases. One exception is that when ρ is a representation of $\mathrm{Gal}(L/K)$, then $\det(I - \lambda\rho(\sigma_{\mathfrak{P}|\mathfrak{p}}))$ is well-defined since det is invariant under conjugacy. This fills a small gap in our definition of *Artin L-functions* later in Section 3.3.1.

Example 2.1.2. The Frobenius element can be used to derive common results in Galois theory. Keep in mind it is a much more powerful and general object than what it appears to be in the following application. In fact, one can deduce a special case of the Frobenius element on $\mathbb{Q}$ without using any sort of algebraic number theory.

Consider a monic polynomial of degree n and K/Q its splitting field. Suppose $p \in \mathbb{Z}$ is a prime such that the reduction of f to $\mathbb{Z}/p\mathbb{Z}$ has n distinct roots (i.e., $p \nmid \Delta f$) and factors into a product of irreducible factors of degree $n_1, \ldots, n_k$. Then $\text{Gal}(K/\mathbb{Q})$ contains a Frobenius element $\sigma_{\mathfrak{P}|p\mathbb{Z}}$ where $\mathfrak{P}$ is a prime of K lying above $p\mathbb{Z}$. Write the reduction of f, $f_p = \prod f_i$ where $\deg f_i = n_i$. Then the Frobenius morphism π of $\text{Gal}(\kappa(\mathfrak{P})/\kappa(p))$ acts transitively on the roots of each irreducible f_i. But in this case it acts on the orbit

$$\{x_{i1}, \pi(x_{i1}), \ldots, \pi^{n_i-1}(x_{i1})\} = \{\text{roots of } f_i\}$$

by the permutation $(12 \cdots n_i)$. Thus, π has a cycle decomposition $(n_1) \cdots (n_k)$, and so is the Frobenius element $\sigma_{\mathfrak{P}|p\mathbb{Z}} \in \text{Gal}(K/\mathbb{Q})$.

For instance, the splitting field of

$$f(x) = x^6 - 12x^4 - 15x^3 - 6x^2 + 15x + 12$$

over $\mathbb{Q}$ contains a permutation with cycle decomposition (5) (modulo 2) and a permutation (2) (modulo 5). Thus, by group theory, the Galois group of the splitting field of f contains S_6 and thus is S_6 (example taken directly from Prof. Alessio Corti's lecture notes on Galois theory at Imperial).

Let $\mathfrak{m}$ be the modulus of all ramified primes of L/K, and thus for primes relatively prime to $\mathfrak{m}$ one could define the Artin symbol. By the unique factorization of ideals in Dedekind domains, the Artin symbol can be extended to a homomorphism

$$\Phi_{\mathfrak{m}} : I_K(\mathfrak{m}) \to \text{Gal}(L/K)$$

since all fractional ideals in a Dedekind domain can be written as a product of integral prime ideals. We call this homomorphism the **Artin reciprocity map**.

2.1.2 Core theorems and the ray class field

We state the following important theorem without proof in terms of modulus.

Theorem 2.1.1 (Artin reciprocity law, with ray class groups)**.** *Let L/K be an abelian extension and let $\mathfrak{m}$ be a modulus divisible by all primes of K that ramify in L. Then*

(i) *The reciprocity map is surjective,*

(ii) *The kernel* $\ker \Phi_{\mathfrak{m}}$ *is a congruence subgroup given large enough the exponents of the finite primes in* $\mathfrak{m}$*,*

(iii) *Thus the isomorphism*

$$\Phi_{\mathfrak{m}} : I_K(\mathfrak{m})/\ker \Phi_{\mathfrak{m}} \xrightarrow{\sim} \text{Gal}(L/K)$$

turns $\text{Gal}(L/K)$ *into a ray class group of modulus* $\mathfrak{m}$*.*

Example 2.1.3. Consider the extension $\mathbb{Q}(\xi_m)/\mathbb{Q}$ where ξ_m is a primitive mth root of unity. Let $\mathfrak{m}$ be the modulus $m\infty$ (we need the place at infinity since it's ramified in $\mathbb{Q}(\xi_m)$) where m is the product of all ideals generated by primes dividing m and ∞ is the unique real infinite absolute value on $\mathbb{Q}$. The monic minimal polynomial $x^m - 1$ of ξ_m over $\mathbb{Q}$ is separable modulo

$\mathfrak{p}$ if and only if $\mathfrak{p}$ is a prime dividing $\mathfrak{m}_0$. Thus, $\mathfrak{m}$ contains all ramified primes, meaning the reciprocity map $\Phi_{m\infty}$ is defined. Thus, we have a map

$$\Phi_{m\infty} : I_{\mathbb{Q}}(\mathfrak{m}) \to \mathrm{Gal}(\mathbb{Q}(\xi_m)/\mathbb{Q}) \cong (\mathbb{Z}/m\mathbb{Z})^{\times}$$

Suppose $(a, m) = (b, m) = 1$ where $a/b > 0/$ Then $(a/b)\mathbb{Z}$ is a fractional ideal relatively prime to $\mathfrak{m}$. We claim that

$$\Phi_{m\infty}((a/b)\mathbb{Z}) = ab^{-1} \in (\mathbb{Z}/m\mathbb{Z})^{\times}$$

By multiplicativity, it suffices to show that

$$\Phi_{m\infty}(p\mathbb{Z}) = \left(\frac{\mathbb{Q}(\xi_m)/\mathbb{Q}}{p\mathbb{Z}}\right) = p \in (\mathbb{Z}/m\mathbb{Z})^{\times}$$

for a prime p not dividing m. By the Frobenius property of the Artin symbol, we get

$$\left(\frac{\mathbb{Q}(\xi_m)/\mathbb{Q}}{p\mathbb{Z}}\right)(\xi_m) = \xi_m^{N(p\mathbb{Z})} = \xi_m^p$$

which is the automorphism corresponding to p in $(\mathbb{Z}/m\mathbb{Z})^{\times}$. Therefore, given the condition $\alpha \equiv 1 \bmod \mathfrak{m}_0$ in $P_{\mathbb{Q}}(\mathfrak{m})$, the kernel of the reciprocity map is $P_{\mathbb{Q}}(\mathfrak{m})$ and thus in this case we have $I_{\mathbb{Q}}(m\infty)/P_{\mathbb{Q}}(m\infty) \cong (\mathbb{Z}/m\mathbb{Z})^{\times}$.

Example 2.1.4. Consider the subextension $\mathbb{Q}(\cos(2\pi/m))$ $(m > 2)$. Then the automorphisms on $\mathbb{Q}(\xi_m)/\mathbb{Q}(\cos(2\pi/m))/\mathbb{Q}$ restrict to $\mathbb{Q}(\cos(2\pi/m))$, which are simply $\cos(2\pi/m) \mapsto \cos(2\pi k/m)$. Thus,

$$\mathrm{Gal}(\mathbb{Q}(\cos(2\pi/m))/\mathbb{Q}) \cong (\mathbb{Z}/m\mathbb{Z})^{\times}/\{\pm 1\}.$$

For this example we take the modulus $\mathfrak{m} = m$. Then a similar equation holds for the Artin reciprocity map, and its kernel is still $P_{\mathbb{Q}}(m)$ which means

$$I_{\mathbb{Q}}(m)/P_{\mathbb{Q}}(m) \cong (\mathbb{Z}/m\mathbb{Z})^{\times}/\{\pm 1\}$$

for this case.

But the existence of modulus such that the kernel of the reciprocity map is a congruence subgroup is never guaranteed to be unique. Indeed, given any such modulus $\mathfrak{m}$, for every $\mathfrak{n}$ divisible by $\mathfrak{m}$, the kernel of $\Phi_{\mathfrak{n}}$ is a congruence subgroup. Thus, we must introduce a special modulus.

Theorem 2.1.2 (conductor theorem)**.** *Let L/K be an abelian extension. There is a modulus $\mathfrak{f}$ of L such that*

(i) *A prime of K ramifies in L if and only if it divides $\mathfrak{f}$,*

(ii) *Let $\mathfrak{m}$ be a modulus divisible by all primes of K which ramify in L. Then* $\ker \Phi_{\mathfrak{m}}$ *is a congruence subgroup if and only if* $\mathfrak{f} \mid \mathfrak{m}$ *(a refined version of the "large enough" condition).*

The proof is omitted here. The modulus is uniquely determined by the extension L/K and is called the **conductor** of the extension.

Of course, we must not forget the main goal of our theory, and the original motivation to develop the ray class group. That is, we want to classify the abelian extensions of a number field. The conductor theorem together with the following existence theorem, both due to Teiji Takagi, form a partial answer to that goal.

Theorem 2.1.3 (existence theorem)**.** *Let* $\mathfrak{m}$ *be a modulus of K and H a congruence subgroup. Then there is a unique abelian extension L/K whose ramified primes divide* $\mathfrak{m}$ *for which the Artin reciprocity map* $\Phi_{\mathfrak{m}}$ *has kernel H.*

Definition 2.1.4. By the previous theorem, we can construct abelian extensions of K with a given Galois group and limited ramified primes. If we take $H = P_K(\mathfrak{m})$, then we get an extension such that $\mathrm{Gal}(L/K)$ is the ray class group defined by $\mathfrak{m}$. This extension is called a **ray class field**, denoted by $K^{\mathfrak{m}}$.

2.1.3 Kronecker-Weber theorem and Hilbert class fields

We will use the following lemma to prove both Kronecker-Weber and the existence of the Hilbert class field.

Lemma 2.1.3. *Let L, M be abelian extensions of K. Then M/L if and only if there is a modulus $\mathfrak{m}$ divisible by all primes of K ramified in either L or M such that*

$$P_K(\mathfrak{m}) \subseteq \ker \Phi_{M/K,\mathfrak{m}} \subseteq \ker \Phi_{L/K,\mathfrak{m}}$$

Proof. Suppose M/L and r is the restriction map $\mathrm{Gal}(M/K) \to \mathrm{Gal}(L/K)$. By preceding remarks on the admissible modulus $\mathfrak{m}$, there is some $\mathfrak{m}$ for which both $\ker \Phi_{M/K,\mathfrak{m}}$ and $\ker \Phi_{L/K,\mathfrak{m}}$ are congruence subgroups for $\mathfrak{m}$ (the first inclusion). Given a prime $\mathfrak{p}$ of K, the prime ideals of $\mathfrak{o}_M$ lying over $\mathfrak{p}$ lie over the primes of L lying over $\mathfrak{p}$, the Frobenius property and the uniqueness of Artin symbols suggests $r \circ \Phi_{M/K,\mathfrak{m}} = \Phi_{L/K,\mathfrak{m}}$. Thus, the second inclusion.

Conversely, if there is a modulus $\mathfrak{m}$ such that the inclusions hold, then the kernel of $\Phi_{L/K,\mathfrak{m}}$ is mapped to a subgroup of $\mathrm{Gal}(M/K)$ by the map $\Phi_{M/K,\mathfrak{m}}$, which by Galois correspondence, there is an intermediate field $M/\tilde{L}/K$. In this case $H = \mathrm{Gal}(M/\tilde{L}) = \ker \Phi_{L/K,\mathfrak{m}} / \ker \Phi_{M/K,\mathfrak{m}}$ (to deduce this we must realize $\ker \Phi_{L/K,\mathfrak{m}}$ contains the kernel of $\Phi_{M/K,\mathfrak{m}}$, an application of the first part).

$$\mathrm{Gal}(M/K)/\mathrm{Gal}(M/\tilde{L}) = (I_K(\mathfrak{m})/\ker \Phi_{M/K,\mathfrak{m}})/H = I_L(\mathfrak{m})/Phi_{L/K,\mathfrak{m}}$$

The LHS is by Galois theory $\mathrm{Gal}(\tilde{L}/K)$ and the RHS is by the reciprocity law $\mathrm{Gal}(L/K)$. Therefore, $\mathrm{Gal}(L/K) = \mathrm{Gal}(\tilde{L}/K)$. From now we apply the first part, and see that both $\ker \Phi_{L/K,\mathfrak{m}}$ and $\ker \Phi_{\tilde{L}/K,\mathfrak{m}}$ contain $\ker \Phi_{M/K,\mathfrak{m}}$ so they must be the same. This implies L is an abelian extension whose reciprocity map has the same kernel as $\tilde{L}$. By the uniqueness part of Theorem 2.1.3, we get $L = \tilde{L}$, completing the proof. □

Utilizing this lemma, we can easily get Kronecker-Weber (of course this theorem is much older than class field theory).

Theorem 2.1.4 (Kronecker-Weber)**.** *Every abelian extension of $\mathbb{Q}$ is a subfield of some cyclotomic field.*

Proof. Let L be an abelian extension of $\mathbb{Q}$. By the reciprocity theorem, there is a modulus $\mathfrak{m}$ with larger enough exponents such that $\ker \Phi_{L/\mathbb{Q},\mathfrak{m}}$ is a congruence subgroup. Of course, one can assume $\mathfrak{m} = m\infty$ for some integer m since we know $\mathfrak{m}$ contains finitely many finite primes, and $\mathfrak{m} \mid m\infty$ suggests $P(\mathfrak{m}) \subseteq \Phi_{L,\mathfrak{m}}$ implies $P(m\infty) \subseteq \Phi_{L,m\infty}$. In Example 2.1.3, we showed $P_{\mathbb{Q}}(m\infty) = \ker \Phi_{\mathbb{Q}(\xi_m)/\mathbb{Q},m\infty}$ and therefore

$$P_{\mathbb{Q}}(m\infty) = \ker \Phi_{\mathbb{Q}(\xi_m)/\mathbb{Q},m\infty} \subseteq \ker \Phi_{L/\mathbb{Q},\mathfrak{m}}$$

which means $L \subseteq \mathbb{Q}(\xi_m)$ by the previous lemma. □

The ideal class group of a number field K, $Cl(\mathfrak{o}_K)$ is clearly a ray class group defined by the modulus $\mathfrak{m} = 1$. By Theorem 2.1.3, there is a unique abelian extension L/K, unramified because $\mathfrak{m} = 1$, such that $\ker \Phi_{L/K,1} = P_K$.

Definition 2.1.5. The class field defined above corresponding to the ideal class group is called the **Hilbert class field**.

Theorem 2.1.5. *The Hilbert class field is the maximal unramified abelian extension of K.*

Proof. Suppose M is another unramified abelian extension of K. Then the Theorem 2.1.2 suggests the conductor $\mathfrak{f}(M/K) = 1$ since M is unramified. Furthermore, the kernel of $\Phi_{M/K,1}$ is a congruence subgroup. Yet notice that $P_K = \ker \Phi_{L/K,1}$ so we have

$$\ker \Phi_{L/K,1} \subseteq \ker \Phi_{M/K,1}$$

which means $M \subseteq L$. □

2.1.4 Some reciprocity theorems from ray class group

Let K be a number field containing a primitive nth root of unity ξ. Take any prime ideal $\mathfrak{p}$ of $\mathfrak{o}_K$ coprime to n. Then for any integer α coprime to $\mathfrak{p}$,

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

Since n is coprime to $\mathfrak{p}$, $x^n - 1$ is separable modulo $\mathfrak{p}$ as n does not divide $N(\mathfrak{p})$. Thus, $1, \xi, \dots, \xi^{n-1}$ are distinct modulo $\mathfrak{p}$. Thus, as ξ has order n in $\kappa(\mathfrak{p})$, $n \mid N(\mathfrak{p}) - 1$. We deduced that $\alpha^{N(\mathfrak{p})-1}$ is an nth root of unity modulo $\mathfrak{p}$, and the roots are distinct. Thus, $\alpha^{(N(\mathfrak{p})-1)/n}$ is a unique nth root of unity modulo $\mathfrak{p}$. This means we can define the **Legendre symbol**

$$\left(\frac{a}{\mathfrak{p}}\right)_n = \alpha^{(N(\mathfrak{p})-1)/n} \bmod \mathfrak{p}$$

We could further extend this symbol to $I_K(\mathfrak{m})$ where $\mathfrak{m}$ is a modulus of K such that every prime containing $n\alpha$ divides $\mathfrak{m}$. In this case the Legendre symbol gives a homomorphism

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

Take $L = K(\sqrt[n]{\alpha})$ for some $\alpha \in K$. For any $\sigma \in \operatorname{Gal}(L/K)$, $\sigma(\sqrt[n]{\alpha}) = \xi \sqrt[n]{\alpha}$ for some nth root of unity ξ. Thus the map $\sigma \mapsto \xi$ is an injective homomorphism $\iota : \operatorname{Gal}(L/K) \to \mu_n$. (The map is well-defined: if a, b are two nth roots of α, then a/b is an nth root of unity, which is fixed by σ.)

Theorem 2.1.6 (weak power reciprocity)**.** *Suppose K is a number field with a primitive nth root of unity, α nonzero, and $L = K(\sqrt[n]{\alpha})$. Let $\mathfrak{m}$ be a modulus divisible by all primes of K containing $n\alpha$, and $\ker \Phi_{L/K,\mathfrak{m}}$ is a congruence subgroup. Then we have $\iota \circ \Phi_{L/K,\mathfrak{m}} = (\alpha/\cdot)_n$. Namely, if G is the image of $\operatorname{Gal}(L/K)$, then*

$$\left(\frac{a}{\cdot}\right)_n : I_K(\mathfrak{m})/P_K(\mathfrak{m}) \to G$$

is a surjective homomorphism.

Proof. Take any $\mathfrak{p}$ coprime to $\mathfrak{m}$. Since $n\alpha$ is not in $\mathfrak{p}$, $x^n - \alpha$ is separable modulo $\mathfrak{p}$. Thus, $\mathfrak{p}$ is unramified in L. Furthermore, L is abelian, which means the Artin symbol can be defined. But note that

$$\left(\frac{L/K}{\mathfrak{p}}\right)(\sqrt[n]{\alpha}) = (\sqrt[n]{\alpha})^{N(\mathfrak{p})} = \alpha^{(N(\mathfrak{p})-1)/n} \sqrt[n]{\alpha} = \left(\frac{a}{\mathfrak{p}}\right)_n \sqrt[n]{\alpha} \bmod p$$

which proves the composition. Now since the kernel is a congruence subgroup, there is a surjective homomorphism $I_K(\mathfrak{m})/P_K(\mathfrak{m}) \to I_K(\mathfrak{m})/\ker \Phi_{L/K,\mathfrak{m}} = \operatorname{Gal}(L/K)$ induced by $\Phi_{L/K,\mathfrak{m}}$, which completes the proof. □

Example 2.1.5. We will prove the quadratic reciprocity. That is, if p, q are distinct odd primes, then

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

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

$$\left(\frac{(-1)^{(p-1)/2}p}{q}\right) = (-1)^{(p-1)(q-1)/4}\left(\frac{p}{q}\right)$$

So one can define $p^* = (-1)^{(p-1)/2}p$ and change the quadratic reciprocity to

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

The Galois group $\mathrm{Gal}(\mathbb{Q}(\xi_p)/\mathbb{Q})$ is a ray class group associated to the modulus $p\infty$. Cyclic of order $p-1$, the ray class group has a subgroup of index 2, which corresponds to a quadratic intermediate field $\mathbb{Q}(\xi_p)/K/\mathbb{Q}$. Note that the restriction of primes of $\mathbb{Q}(\xi_p)$ to the primes of K suggests $\mathrm{Gal}(K/\mathbb{Q})$ is also a ray class group for $p\infty$. With theories of quadratic extensions, $K = \mathbb{Q}(\sqrt{p^*})$ because p is the only prime that ramifies in K. Thus, $\ker \Phi_{\mathbb{Q}(\sqrt{p^*})/\mathbb{Q},p\infty}$ is a congruence class field. By Theorem 2.1.6, there is a surjective homomorphism, defined by $\left(\frac{p^*}{\cdot}\right)$,

$$I_{\mathbb{Q}}(p\infty)/P_{\mathbb{Q}}(p\infty) \to \{\pm 1\}$$

But the map sending $a \in (\mathbb{Z}/p\mathbb{Z})^\times$ to $a\mathbb{Z} \in I_{\mathbb{Q}}(p\infty)/P_{\mathbb{Q}}(p\infty)$ is an isomorphism. Composing the two maps, we have a surjective homomorphism from $(\mathbb{Z}/p\mathbb{Z})^\times$ to $\{\pm 1\}$. Yet $\left(\frac{\cdot}{p}\right)$ is a homomorphism of the same kind. Yet there is only one such homomorphism by group theory. Thus,

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

2.2 Cohomology-Free Class Field Theory

Main references: [Neu99] and [Mil20].

2.2.1 Abstract theory

In this section we will formulate some abstract theory of Galois groups, valuations and reciprocities. The term "abstract" is simply an indication of the style of the theory here, that is, not referring to the phenomena of some specific fields, but relying on a set of sophisticated axioms. Of course, the axioms can be found on the real objects of interests. Yet it is possible to develope a rich theory with these axioms.

Take a profinite group G. Denote by G_K its closed subgroups where the indices are called fields, and each K is called the fixed field of G_K. The field such that $G_k = G$ is the base field, and $\bar{k}$ is the field whose group is trivial. Given an element σ of G, the fixed field of $\overline{(\sigma)}$ is called the fixed field of σ. We write L/K if $G_L \le G_K$. If G_L is open, meaning it has finite index in G_K, the extension L/K is called finite with degree $[L : K] = (G_K : G_L)$. The extension is Galois if G_L is a normal subgroup of G_K, and in this case we write $G(L/K) = G_K/G_L$. If $N/L/K$ are Galois, then we could restrict automorphisms in $G(N/K)$ to $G(L/K)$ with kernel $G(N/L)$. An extension L/K is called cyclic, abelian or solvable if its Galois group has the same properties. If $G_{K'} = \sigma^{-1}G_K\sigma$, we write $K' = K^\sigma$.

Remark 2.2.1. The obscure constructions above are precisely those in Galois theory. That is, we write $G = G(\bar{k}/k)$ for some Galois extension $\bar{k}/k$, $G_K = G(\bar{k}/K)$. The normality and quotient construction are simply results of the Galois correspondence.

The next goal is to describe G-modules, which would become an important object in the statement of the reciprocity law.

Definition 2.2.1. We say A is a **continuous multiplicative G-module** if it is a multiplicative abelian group on which G acts on the right, furthermore, $A = \cup_{[K:k]<\infty} A_K$ where

$$A_K = \{a \in A : \forall \sigma \in A_K, a^\sigma = a\}$$

In other words, the map $(\sigma, a) \to a^\sigma$ is continuous when A is equipped with the discrete topology.

If L/K is finite, we have the norm map

$$N_{L/K} : A_L \to A_K, \quad N_{L/K} : a \mapsto \prod_{\sigma \in G_L \backslash G_K} a^\sigma.$$

If L/K is Galois, we clearly have

$$A_L^{G(L/K)} = A_K$$

Definition 2.2.2. The **norm residue group** is

$$H^0(G(L/K), A_L) = A_K / N_{L/K} A_L$$

Remark 2.2.2. The goal of this section is to present a cohomology-free approach, but some notations might be given in their cohomology form.

Also define

$$H^{-1}(G(L/K), A_L) = A_{L,1} / I_{G(L/K)} A_L$$

where $I_{G(L/K)} A_L$ is the subgroup of $A_{L,1} = \{a \in A_L : N_{L/K}(a) = 1\}$ generated by elements $a^{\sigma - 1} = a^\sigma a^{-1}$. If L/K is cyclic with generator σ,

$$a^{\sigma^k - 1} = \left(\prod_{i=0}^{k-1} a^{\sigma^i} \right)^{\sigma - 1}$$

which means $I_{G(L/K)} A_L = \{a^{\sigma - 1} : a \in A_L\}$. From now we assume the following axioms on G-modules A of prime interests (which will be proved later and properly named): for $i = 0, -1$,

$$H^i(G(L/K), A_L) = 1, \forall \text{ finite cyclic extensions } L/K$$

Example 2.2.1. Consider a G-equivariant homomorphism $\wp : A \to A$ with finite cyclic kernel $\mu_\wp$. The order of its kernel is called the **exponent** of $\wp$. Fix a field K with $\mu_\wp \subseteq A_K$ (which exists by the continuity condition on A). Then for every subset $B \subseteq A$, define $K(B)$ be the fixed field of

$$\{\sigma \in G_K : b^\sigma = b, \forall b \in B\} \leq G_K$$

Take some $\Delta \subseteq A_K$, the extension $K(\wp^{-1}(\Delta))/K$ is Galois (all elements of Δ is fixed by G_K and $\wp$ is G-equivariant, meaning its closed subgroup is normal). Such extensions are called **Kummer extensions**. The Galois group of a Kummer extension is abelian of exponent n. There is an injective homomorphism from $G(K(\wp^{-1}(a))/K) \to \mu_\wp$ given by $\sigma \mapsto \alpha^{\sigma - 1}$ for some $\alpha \in \wp^{-1}(a)$. Thus, as $K(\wp^{-1}(\Delta)) = \prod_{a \in \Delta} K(\wp^{-1}(a))$, there is an injective homomorphism from the Kummer extension to $\mu_\wp^\Delta$.

An important consequence of the construction above is that all abelian extensions of fixed exponent can be classified. In the theorem below we write $A_K^\wp$ for the image of A_K under $\wp$.

Theorem 2.2.1. *The map*

$$\Delta \mapsto L = K(\wp^{-1}(\Delta))$$

is a bijection from subgroups $A_K^\wp \subseteq \Delta \subseteq A_K$ and the abelian extensions of K of exponent n. Furthermore, if Δ corresponds to L, then $A_K^\wp \cap A_K = \Delta$, and we have an isomorphism

$$\Delta / A_K^\wp \cong \operatorname{Hom}(G(L/K), \mu_\wp), \quad a \mapsto \chi_a$$

where $\chi_a : \sigma \mapsto \alpha^{\sigma - 1}$ for some $\alpha \in \wp^{-1}(a)$.

The Kummer theory developed above has various applications, especially when G is the absolute Galois group of some actual field k with $A = \bar{k}^\times$ and $\wp : a \mapsto a^n$ for some n relatively prime to the characteristic of k. The axiom of the theory is satisfied because of the following theorem

Theorem 2.2.2 (Hilbert 90). *For a cyclic extension L/K one always has*

$$H^{-1}(G(L/K), L^\times) = 1$$

Proof. Let $n = [L : K]$ and $\alpha \in L^\times$. The automorphisms $1, \sigma, \dots, \sigma^{n-1}$ are linearly independent. Thus, there is an element $\gamma \in L^\times$ such that

$$\beta = \gamma + \alpha\gamma^\sigma + \cdots + \alpha^{1+\sigma+\cdots\sigma^{n-2}}\gamma^{\sigma^{n-1}} \neq 0$$

But $N_{L/K}(\alpha) = \prod_\sigma \alpha^\sigma = 1$, we have $\alpha\beta^\sigma = \beta$ meaning $\alpha = \beta^{1-\sigma}$, completing the proof. □

We thus can apply the main theorem of Kummer theory:

Corollary 2.2.1. *Let n be a natural number relatively prime to the characteristic of K, and suppose $\mu_n \subseteq K$. Then the abelian extensions of K of exponent n is in bijection to the subgroups of Δ of $K^\times$ that contain $K^{\times n}$:*

$$\Delta \mapsto L = K(\sqrt[n]{\Delta})$$

and $G(L/K) \cong \mathrm{Hom}(\Delta/K^{\times n}, \mu_n)$.

Let G be a finite group and A a multiplicative G-module. A 1-cocycle is a function $f : G \to A$ such that $f(\sigma\tau) = f(\sigma)^\tau f(\tau)$. They form an abelian group $Z^1(G, A)$. The 1-coboundaries are functions of the form $f_a(\sigma) = a^{\sigma-1}$ for every $a \in A$, forming a subgroup $B^1(G, A)$ of the 1-cocycles:

$$f_a(\sigma\tau) = a^{\sigma\tau-1} = a^{(\sigma-1)\tau+\tau-1} = f_a(\sigma)^\tau f_a(\tau)$$

We define $H^1(G, A) = Z^1(G, A)/B^1(G, A)$.

Lemma 2.2.1. *If G is cyclic then $H^1(G, A) \cong H^{-1}(G, A)$.*

Proof. Write $G = \langle\sigma\rangle$. If $f \in Z^1(G, A)$, then for $k \geqslant 1$, $f(\sigma^k) = f(\sigma^{k-1})^\sigma f(\sigma) = \cdots = \prod_{i=0}^{k-1} f(\sigma)^{\sigma^i}$. Note that $f(1) = 1$ since $f(1) = f(1 \cdot 1) = f(1)f(1)$. If n is the cardinality of G, then

$$N_G f(\sigma) = f(\sigma^n) = 1$$

meaning $f(\sigma) \in A_{G,1}$. Conversely, if $a \in A_{G,1}$, we may define a 1-cocycle $f(\sigma) = a$ and $f(\sigma^k) = \prod_{i=0}^{k-1} a^{\sigma^i}$. Then $f \mapsto f(\sigma)$ is an isomorphism between $Z^1(G, A)$ and $A_{G,1}$. Furthermore,

$$f \in B^1(G, A) \iff f(\sigma^k) = a^{\sigma^k-1} \iff f(\sigma) = a^{\sigma-1} \iff f(\sigma) \in I_G(A)$$

completing the proof. □

In fact, we have

Theorem 2.2.3. *For a finite Galois extension L/K one has*

$$H^1(G(L/K), L^\times) = 1$$

Proof. For any 1-cocycle $f : G \to L^\times$ and some $c \in L^\times$, we apply the same argument to

$$\alpha = \sum_{\sigma \in G(L/K)} f(\sigma)c^\sigma$$

to show that $f(\tau) = \beta^{\tau-1}$ with $\beta = \alpha^{-1}$. □

Recall that for a $\mathfrak{p}$-adic number field k and its absolute Galois group G, we have a surjective homomorphism $d : G \to \hat{\mathbb{Z}}$ induced by the isomorphism

$$G(\tilde{k}/k) \cong G(\overline{\mathbb{F}_q}/\mathbb{F}_q) \cong \hat{\mathbb{Z}}$$

where $\tilde{k}$ is the maximal unramified extension of k, which associates to the element $1 \in \hat{\mathbb{Z}}$ the Frobenius automorphism φ of $\tilde{k}$. The surjective homomorphism is then given as the composition

$$G \to G(\tilde{k}/k) \to \hat{\mathbb{Z}}$$

To build an abstract theory of valuation, we first fix some profinite group G and a surjective homomorphism $d : G \to \hat{\mathbb{Z}}$.

Remark 2.2.3. Neukirch's development of this theory is extremely obscure as it might seem superbly less natural than the Galois theory. The author will most definitely not include any of his proofs. Results will only be mentioned when it's needed.

For any field K (here we are still using the abstract notion of fields developed before), we denote by I_K the kernel of the restriction $d : G_K \to \hat{\mathbb{Z}}$, the **inertia subgroup** over K. If I is the kernel of d then

$$I_K = G_K \cap I = G_K \cap G_{\tilde{k}} = G_{\tilde{K}}$$

where the fixed field $\tilde{K}$ of I_K is the composite field of K and $\tilde{k}$. We call $\tilde{K}/K$ the **maximal unramified extension** of K and we define $f_K = (\hat{\mathbb{Z}} : d(G_K))$ and $e_K = (I : I_K)$ respectively. If f_K is finite, then we have a surjective homomorphism

$$d_K : \frac{1}{f_K} d : G \mapsto \hat{\mathbb{Z}}$$

with kernel I_K, and thus an isomorphism $d_K : G(\tilde{K}/K) \to \hat{\mathbb{Z}}$.

Definition 2.2.3. The element φ_K in $G(\tilde{K}/K)$ with $d_K(\varphi_K) = 1$ is the **Frobenius element** over K.

For an extension L/K, we define the inertia degree and ramification index by $f_{L/K} = (d(G_K) : d(G_L))$ and $e_{L/K} = (I_K : I_L)$ respectively. It is obvious to see that these definitions respect the tower law. We also have the fundamental identity

Lemma 2.2.2. *For every extension L/K we have*

$$[L : K] = f_{L/K} e_{L/K}$$

Proof. The exact commutative diagram

$$\begin{tikzcd}
1 \arrow[r] \arrow[d] & I_L \arrow[r] \arrow[d] & G_L \arrow[r] \arrow[d] & d(G_L) \arrow[r] \arrow[d] & 1 \arrow[d] \\
1 \arrow[r] & I_K \arrow[r] & G_K \arrow[r] & d(G_K) \arrow[r] & 1
\end{tikzcd}$$

By snake lemma, if L/K is Galois, we have an exact sequence

$$1 \to I_K/I_L \to G(L/K) \to d(G_K)/d(G_I) \to 1$$

If L/K is not Galois, take a Galois extension $M/L/K$. Then L/M is Galois so we have

$$[M : L][L : K] = e_{M/K} f_{M/K} = e_{M/L} e_{L/K} f M/L f_{L/K} = [M : L] f_{L/K} e_{L/K}$$

completing the proof. □

We can also define unramified, totally ramified extensions using the ramification index and the inertia degree. If L/K is unramified, and f_K is finite, there is a surjective homomorphism $G(\tilde{K}/K) \to G(L/K)$ and we call the image of φ_K the **Frobenius automorphism**. Consider the extension $\tilde{L}/K$ and the semigroup

$$\mathrm{Frob}(\tilde{L}/K) = \{\sigma \in G(\tilde{L}/K) : d_K(\sigma) \in \mathbb{N}\}$$

Lemma 2.2.3. *For a finite Galois extension L/K, the map*

$$\mathrm{Frob}(\tilde{L}/K) \to G(L/K), \quad \sigma \mapsto \sigma|_L$$

is surjective.

We also have

Lemma 2.2.4. *Let $\tilde{\sigma} \in \mathrm{Frob}(\tilde{L}/K)$ and let Σ be the fixed field of $\tilde{\sigma}$. Then $f_{\Sigma/K} = d_K(\tilde{\sigma})$, $[\Sigma, K] < \infty$, $\tilde{\Sigma} = \tilde{L}$ and $\tilde{\sigma} = \varphi_\Sigma$.*

Now add the data of the multiplicative G-module A. A **henselian valuation** of A_k with respect to d is a homomorphism $\nu : A_k \to \hat{\mathbb{Z}}$ such that $\nu(A_k) = Z$ contains $\mathbb{Z}$ and $Z/nZ \cong \mathbb{Z}/n\mathbb{Z}$ for all natural n; furthermore, $\nu(N_{K/k}A_K) = f_K Z$ for all finite extensions K/k. For every field K we can define $\nu_K = \frac{1}{f_K}\nu \circ N_{K/k}$. A **uniformizer** of A_K is an element $\pi_K \in A_K$ such that $\nu_K(\pi_K) = 1$. We write $U_K = \{u \in A_K : \nu_K(u) = 0\}$, the **unit subgroup**.

Suppose from now K is a finite extension of k. We assume the following axiom: for every unramified finite extension L/K, one has

$$H^i(G(L/K), U_L) = 1, \quad i = 0, -1$$

For an infinite extension L/K, we set

$$N_{L/K}A_L = \bigcap_M N_{M/K}A_M$$

over finite subextensions of L. We first work on the subgroup of Frobenius elements.

Definition 2.2.4. The **reciprocity map**

$$r_{\tilde{L}/K} : \mathrm{Frob}(\tilde{L}/K) \to A_K/N_{\tilde{L}/K}A_{\tilde{L}}$$

is defined by

$$r_{\tilde{L}/K}(\sigma) = N_{\Sigma/K}(\pi_\Sigma)$$

where Σ is the fixed field of σ and $\pi_\Sigma \in A_\Sigma$ is a uniformizer.

This definition is independent of the choice of the uniformizer. To wit this, any uniformizer π'_Σ differs from π_Σ by an element u in U_Σ. Then we claim $N_{\Sigma/K}(u) \in N_{\tilde{L}/K}A_{\tilde{L}}$. Since $H^0(G(\tilde{L}/K), U_{\tilde{L}}) = U_K/N_{\tilde{L}/K}U_{\tilde{L}} = 1$ by assumption,

$$N_{\Sigma/K}(u) \in U_K = N_{\tilde{L}/K}U_{\tilde{L}} \subseteq N_{\tilde{L}/K}A_{\tilde{L}}.$$

Indeed, $r_{\tilde{L}/K}$ is multiplicative. We consider for every $\sigma \in G(\tilde{L}/K)$ the endomorphisms

$$\sigma - 1 : a \mapsto a^{\sigma - 1}, \quad \sigma_n : a \mapsto \prod_{i=0}^{n-1} a^{\sigma^i}$$

For them we have $(\sigma - 1) \circ \sigma_n = \sigma_n \circ (\sigma - 1) = \sigma^n - 1$. We also define

$$N = N_{\tilde{L}/\tilde{K}} : A_{\tilde{L}} \to A_{\tilde{K}}$$

Lemma 2.2.5. *The reciprocity map*

$$r_{\tilde{L}/K} : \mathrm{Frob}(\tilde{L}/K) \to A_K/N_{\tilde{L}/K}A_{\tilde{L}}$$

is multiplicative.

Proof. Let $\sigma_1\sigma_2 = \sigma_3$ be elements in $\mathrm{Frob}(\tilde{L}/K)$ with $n_i = d_K(\sigma_i)$, Σ_i the fixed field of σ_i and π_i a uniformizer of Σ_i. We want to show that

$$N_{\Sigma_1/K}(\pi_1)N_{\Sigma_2/K}(\pi_2) \equiv N_{\Sigma_3/K}(\pi_3)$$

modulo $N_{\tilde{L}/K}A_{\tilde{L}}$. Take some φ in $G(\tilde{L}/K)$ with $d_K(\varphi) = 1$ and $\tau_i = \sigma_i^{-1}\varphi^{n_i}$. From our assumption, it is easy to see that

$$\tau_3 = \sigma_2^{-1}\varphi^{n_2}(\varphi^{-n_2}\sigma_1\varphi^{n_2})^{-1}\varphi^{n_1}$$

We could replace σ_1 with $\sigma_1' = \varphi^{-n_2}\sigma_1\varphi^{n_2}$. Then $d_K(s_1') = d_K(s_1) = n_1$, $\Sigma_1' = \Sigma_1^{\varphi^{n_2}}$, $pi_1' = \pi_1^{\varphi^{n_2}} \in A_{\Sigma_1'}$ and $\tau_1' = \sigma_1'^{-1}\varphi^{n_1}$. The valuation of π_1' is also one since $\nu_{\Sigma_1} = \nu_{\Sigma_1^{\varphi^{n_2}}} \circ \varphi^{n_2}$. Note that $N_{\Sigma_1'/K}(\pi_1') = N_{\Sigma_1/K}$. We thus rephrase the goal

$$N_{\Sigma_1'/K}(\pi_1')N_{\Sigma_2/K}(\pi_2) \equiv N_{\Sigma_3/K}(\pi_3)$$

using the new formula $\tau_3 = \tau_2\tau_1'$. In fact, we can explicitly spell out the formula of $N_{\Sigma_i/K}$.

Lemma 2.2.6. *Suppose $\varphi, \sigma \in \mathrm{Frob}(\tilde{L}/K)$ with $d_K(\varphi) = 1$ and $d_K(\sigma) = n$. If Σ is the fixed field of σ and $a \in A_\Sigma$, then*

$$N_{\Sigma/K}(a) = (N \circ \varphi_n)(a) = (\varphi_n \circ N)(a)$$

Proof. The core of this lemma is the fact that, if we put $U = \Sigma \cap \tilde{K}$ so that $N_{\Sigma/K} = N_{U/K} \circ N_{\Sigma/U}$, then $G(U/K)$ is generated by $\varphi|_U$ which has order n. □

Applying this lemma, $N_{\Sigma_i/K}(\pi_i) = N(\pi_i^{\varphi_{n_i}})$. In this case we write

$$u = \pi_3^{\varphi_{n_3}}\pi_2^{-\varphi_{n_2}}\pi_1'^{-\varphi_{n_1}}$$

Then the multiplicativity of $r_{\tilde{L}/K}$ amounts to the relation $N(u) \in N_{\tilde{L}/K}A_{\tilde{L}}$. Since $\varphi_{n_i}(\varphi - 1) = \varphi^{n_i} - 1$ and $\pi_i^{\varphi^{n_i}-1} = \pi_i^{\tau_i - 1}$ we see that

$$u^{\varphi-1} = \pi_3^{\tau_3-1}\pi_2^{1-\tau_2}\pi_1'^{1-\tau_1'}$$

Since $\tau_3 = \tau_2\tau_1'$, we see that $(\tau_3 - 1) + (1 - \tau_2) + (1 - \tau_1') = (1 - \tau_2)(1 - \tau_1')$. Putting $\pi_3 = u_3\pi_1'$, $\pi_2 = u_2^{-1}\pi_1'$ and $\pi_1'^{\tau_2} = u_1'\pi_1'$, we obtain

$$u^{\varphi-1} = \prod u_i^{\pi_i - 1} \in I_{G(\tilde{L}/\tilde{K})}U_L$$

which means that $u^{\varphi-1} = 1$ in $H_0(G(\tilde{L}/\tilde{K}), U_{\tilde{L}})$.

Lemma 2.2.7. *If $x \in H^0(G(\tilde{L}/\tilde{K}), U_{\tilde{L}})$ is an element fixed by some $\varphi \in G(\tilde{L}/K)$ with $d_K(\varphi) = 1$, then $N(x) \in N_{\tilde{L}/K}U_{\tilde{L}}$.*

Proof. This lemma is a consequence of the fact that

$$H^{-1}(G(\tilde{L}/\tilde{K}), U_{\tilde{L}}) = 1$$

and Lemma 2.2.6. A detailed proof can be found in [Ked23]. □

The lemma then follows from the lemma above. □

We have now proved that the reciprocity map is a homomorphism of semigroups. Given some Frobenius element σ, if $\sigma \in G(\tilde{L}/L)$, then the fixed field of σ contains L, meaning $N_{\Sigma/K}(\pi_\Sigma) = N_{L/K}N_{\Sigma/L}(\pi_\Sigma) \in N_{L/K}A_L$. We can make the observation $G(L/K) = G(\tilde{L}/K)/G(\tilde{L}/L)$, so that the reciprocity map induces a homomorphism as in the next lemma.

Lemma 2.2.8. *For every finite Galois extension L/K, there is a canonical homomorphism*

$$r_{L/K} : G(L/K) \to A_K/N_{L/K}A_L$$

given by

$$r_{L/K}(\sigma) = N_{\Sigma/K}(\pi_K) \bmod N_{L/K}A_L$$

where Σ is the fixed field of a preimage $\tilde{\sigma}$ of σ under the surjective map $\mathrm{Frob}(\tilde{L}/K) \to G(L/K)$*.*

Remark 2.2.4. We will instead call this new map the **reciprocity map**.

Proof. We just need to show that the reciprocity map is well-defined. Say $\tilde{\sigma}, \tilde{\sigma}'$ with fixed field Σ, Σ' are mapped to σ. If $d_K(\tilde{\sigma}) = d_K(\tilde{\sigma}')$ then $\tilde{\sigma}|_{\tilde{K}} = \tilde{\sigma}'|_{\tilde{K}}$ and $\tilde{\sigma}|_L = \tilde{\sigma}'|_L$, meaning $\tilde{\sigma} = \tilde{\sigma}'$ ($\tilde{L} = L\tilde{K}$) so we are done. However, if $d_K(\tilde{\sigma}) < d_K(\tilde{\sigma}')$, then $\tilde{\sigma}' = \tilde{\sigma}\tilde{\tau}$ for some Frobenius $\tilde{\tau}$ with $\tilde{\tau}|_L = 1$. The fixed field of $\tilde{\tau}$ contains L, so $r_{\tilde{L}/K}(\tilde{\tau}) = 1$ modulo $N_{L/K}A_L$, completing the proof. □

Remark 2.2.5. *Important:* Here is a very efficient, elegant and effective way to understand the reciprocity theorems in class field theory. The things we have in hand are fields and their extensions. It is one ultimate goal to classify all extensions, which is probably impossible to do. However, in class field theory we only focus on abelian extensions. To study the extensions there is Galois theory. Grothendieck in his [GR02] gave the axioms of a Galois category and a categorical interpretation of the Galois correspondence. However, it is still not enough for the classification of abelian extensions of a field solely in terms of the arithmetics of the base field (indeed, the Galois group still relies on a separable closure, which is not encoded in the base field). The reciprocity map then appears to be functorial, sending inclusions of Galois groups to norm maps between the G-module A attached to them.

The following lemma exhibits the functorial properties of the reciprocity map:

Lemma 2.2.9. *Let L/K and L'/K' be finite Galois extensions, so that K'/K and L'/L. Let σ be an element in G. Then the following diagrams commutative*

$$\begin{tikzcd}
G(L'/K') \arrow[r, "r_{L'/K'}"] \arrow[d] & A_{K'}/N_{L'/K'}A_{L'} \arrow[d, "N_{K'/K}"] \\
G(L/K) \arrow[r, "r_{L/K}"] & A_K/N_{L/K}A_L
\end{tikzcd}
\qquad
\begin{tikzcd}
G(L/K) \arrow[r, "r_{L/K}"] \arrow[d, "\sigma^*"] & A_K/N_{L/K}A_L \arrow[d, "\sigma"] \\
G(L^\sigma/K^\sigma) \arrow[r, "r_{L^\sigma/K^\sigma}"] & A_{K^\sigma}/N_{L^\sigma/K^\sigma}A_{L^\sigma}
\end{tikzcd}$$

where the vertical arrow are given by $\sigma' \mapsto \sigma'|_L$ and $\sigma^* : \tau \mapsto \sigma^{-1}\tau\sigma$.

For a subgroup of finite index H of G, we take a system of representations R. If $\sigma \in G$, we write for every $\rho \in R$, $\sigma\rho = \rho'\sigma_p$ for some $\sigma_\rho \in H$ and $\rho' \in R$. Then define the transfer map $V : G^{\mathsf{ab}} \to H^{\mathsf{ab}}$ given by $V(\sigma) = \prod_{\rho \in R} \sigma_\rho$.

Lemma 2.2.10. *Let L/K be a finite Galois extensions and K' an intermediate field. Then we have the commutative diagram*

$$\begin{tikzcd}
G(L/K)^{\mathsf{ab}} \arrow[r, "r_{L/K}"] \arrow[d, "V"] & A_K/N_{L/K}A_L \arrow[d, "\iota"] \\
G(L/K')^{\mathsf{ab}} \arrow[r, "r_{L/K'}"] & A_{K'}/N_{L/K'}A_L
\end{tikzcd}$$

Our goal is to show the reciprocity map $r_{L/K} : G(L/K)^{\mathsf{ab}} \to A_K/N_{L/K}A_L$ is an isomorphism. The case of unramified extensions is easier.

Lemma 2.2.11. *If L/K is an unramified extension, then the reciprocity map*

$$r_{L/K} : G(L/K) \to A_K/N_{L/K}A_L$$

given by

$$r_{L/K}(\varphi_{L/K}) = \pi_K \bmod N_{L/K}A_L$$

is an isomorphism.

Proof. Since L is unramified, we have $L \subseteq \tilde{K}$ and thus $\tilde{L} = L\tilde{K} = \tilde{K}$. The Frobenius element over K, φ_K, is the preimage of $\varphi_{L/K}$ under the restriction map, and it has a fixed field K (since the Frobenius generates $G(\tilde{K}/K)$). Thus, by construction, $r_{L/K}(\varphi_{L/K}) = \pi_K$. Recall the henselian valuation $\nu_K : A_K \to Z$ such that $\nu_K(N_{L/K}A_K) \subseteq f_{L/K}Z$ and in this case the inertia degree $f_{L/K}$ is $[L : K]$. Thus, we have a map $A_K/N_{L/K}A_L \to Z/nZ \cong \mathbb{Z}/n\mathbb{Z}$. Indeed, it is an isomorphism. Take any $a \in A_K$ such that$\nu_K(a) = 0$. Then $a = u\pi_K^{dn}$ and since $u = N_{L/K}(\varepsilon)$ for some $\varepsilon \in U_L$, by the class field axiom, we have $a = N_{L/K}(\varepsilon\pi_K^d) = 1$ modulo $N_{L/K}A_L$. But we see that the generators of these three groups $\varphi_{L/K}$, the uniformizer, and 1 correspond to each other, so $r_{L/K}$ is an isomorphism. □

We proceed to the central part of this section — the general reciprocity law. We consider continuous G-module A satisfying:

Definition 2.2.5. The **class field axiom**: for every cyclic extensions L/K,

$$\#H^i(G(L/K), A_L) = \begin{cases} [L : K], & i = 0 \\ 1, & i = -1 \end{cases}$$

The class field axioms includes the assumptions we used in the previous lemma. That is

Lemma 2.2.12. *For every unramified extensions L/K, the cohomology group*

$$H^i(G(L/K), U_L) = 1$$

for $i = -1, 0$.

Proof. Since L/K is unramified, a uniformizer π_K is also a uniformizer of A_L. Since

$$H^{-1}(G(L/K), A_L) = 1,$$

every element of U_L has the form $a^{\sigma-1}$ for some $a \in A_L$ and $\sigma = \varphi_{L/K}$. Thus, if we write $a = \varepsilon\pi_L^m$, we see that $a = \varepsilon^{\sigma-1}$ and thus $H^{-1}(G(L/K), U_L) = 1$.

On the other hand, $\#A_K/N_{L/K}A_L = [L : K]$, the map $\nu_K : A_K/N_{L/K}A_L \to Z/nZ$ is bijective. If $u \in U_K$, then $u = N_{L/K}(a)$ for some $a \in A_L$ as $\nu_K(u) = 0$. But then $\nu_K(u) = \nu_K(N_{L/K}(a)) = n\nu_L(a)$ so $a \in U_L$, meaning $H^0(G(L/K), U_L) = 1$. □

In class field theory, we consider a profinite group G, a continuous G-module A, and two homomorphisms $d : G \to \hat{\mathbb{Z}}$ and $\nu : A \to \hat{\mathbb{Z}}$ where d is surjective, continuous and ν is a henselian valuation. One could then define the reciprocity map $r_{L/K} : G(L/K)^{\mathsf{ab}} \to A_K/N_{L/K}A_L$. With these constructions, we can state the main theorem of class field theory.

Theorem 2.2.4 (Artin reciprocity law, abstract)**.** *For every finite Galois extension L/K, the homomorphism*

$$r_{L/K} : G(L/K)^{\mathsf{ab}} \to A_K/N_{L/K}A_L$$

is an isomorphism.

Proof. If M/K is a Galois subextension of L/K, the functorial property of r gives the following commutative diagram (whose rows are exact).

$$\begin{tikzcd}
1 \arrow[r] & G(L/M) \arrow[r] \arrow[d, "r_{L/M}"] & G(L/K) \arrow[r] \arrow[d, "r_{L/K}"] & G(M/K) \arrow[r] \arrow[d, "r_{M/K}"] & 1 \\
& A_M/N_{L/M}A_L \arrow[r, "N_{M/K}"] & A_K/N_{L/K}A_L \arrow[r] & A_K/N_{M/K}A_M &
\end{tikzcd}$$

Based on this exact diagram, one can reduce the problem three times.

We can assume L/K is abelian. Let K^{ab} be the maximal abelian subextension of L/K. Observe that $G(K^{\mathsf{ab}}/K)$ is the abelianization of $G = G(L/K)$. Indeed, if M is the fixed field of $[G,G]$. Then $G(M/K) = G/[G,G]$ is abelian, namely $M \subseteq K^{\mathsf{ab}}$. This means $G(L/K^{\mathsf{ab}}) \subseteq G(L/M) = [G,G]$. Conversely, since $G(K^{\mathsf{ab}}/K) = G/G(L/K^{\mathsf{ab}})$ is abelian, $G(L/K^{\mathsf{ab}})$ must contain the commutator subgroup. Therefore, $G(L/K^{\mathsf{ab}}) = G(L/M)$ so $K^{\mathsf{ab}} = M$ and

$$G(K^{\mathsf{ab}}/K) = G/G(L/M) = G^{\mathsf{ab}}.$$

Thus $r_{L/K}$ is injective by the commutative exact diagram. we will not prove it's surjective.

We can further reduce to the case where L/K is cyclic. Suppose L/K is abelian. Let M varies over the cyclic subextensions of K. Then the kernel of $r_{L/K}$ lies in the kernel of the map $G(L/K) \mapsto \prod_M G(M/K)$. Since $G(L/K)$ is finite abelian, this map is injective and as a result $r_{L/K}$ is injective. Still we will not prove surjectivity.

Finally we show that it suffices to prove the statement when L/K is cyclic and totally ramified. Let M be the maximal unramified subextension of L/K. Then $f_{L/M} = 1$ and $r_{M/K}$ is an isomorphism by Lemma 2.2.11. The norm map $N_{M/K}$ must be injective because the class field axiom tells us the orders of the groups in the lower row are $[L : M]$, $[L : K]$ and $[M : K]$. Indeed, the map t on the right of $N_{M/K}$ is surjective, with an image of size $[M : K]$. The kernel of this map is the image of $N_{M/K}$, and $[L : K] = [M : K] \cdot \# \ker t$ so $\# \ker t = \operatorname{im} N_{M/K} = [L : M]$. By finiteness of the groups, $N_{M/K}$ has to be injective. Then by the short five lemma, $r_{L/K}$ is an isomorphism if $r_{L/M}$ is (and $r_{M/K}$ already is).

Now if L/K is cyclic and totally ramified. Let σ be a generator of $G(L/K)$. Then one may regard σ as an element of $G(\tilde{L}/\tilde{K}) \cong G(L/K)$ and let $\tilde{\sigma} = \sigma\varphi_L \in \mathrm{Frob}(\tilde{L}/K)$ which is a preimage of σ with $d_K(\tilde{\sigma}) = d_K(\varphi_L) = f_{L/K} = 1$. Therefore, the inertia degree of the fixed field Σ of σ is 1, meaning $\Sigma \cap tildeK = K$. Let M/K be a finite Galois subextension of $\tilde{L}/K$ containing Σ and L and let M^0 be the maximal unramified subextension of M. Take $N = N_{M/M^0}$. Since $f_{\Sigma/K} = f_{L/K} = 1$, we see that $N|_{A_\Sigma} = N_{\Sigma/K}$ and $N|_{A_L} = N_{L/K}$.

One may prove the injectivity of $r_{L/K}$ as follows. Suppose $r_{L/K}(\sigma^k) = 1$ where $0 \leqslant k < n = [L : K]$. Let π_Σ, π_L be the uniformizers of the corresponding modules. Write $\pi_\Sigma^k = u\pi_L^k$ where $u \in U_M$. We have

$$r_{L/K}(\sigma^k) = N(\pi_\Sigma^k) = N(u)N(\pi_L^k) = N(u)$$

It follows from $r_{L/K}(\sigma^k) = 1$ that $N(u) = N(v)$ for some $v \in U_L$. The class field axioms allow us to write $u^{-1}v = a^{\sigma-1}$ for some $a \in A_M$ and $x = \pi_L^k v a^{1-\sigma}$ is an element of A_{M^0}, which suggests $v_M(x) = k$. Thus, $k = 0$, so $r_{L/K}$ is injective. The surjectivity then follows from the injectivity of $r_{L/K}$ and the axiom that $H^0(G(L/K), A_L) = [L : K] = \mathrm{Gal}(L/K)$. □

We let $(\cdot, L/K) : A_K \to G(L/K)$ be the map with kernel $N_{L/K}A_L$ that induces the inverse of the reciprocity map.

We now derive a one-to-one correspondence between the abelian extensions of K and subgroups of A_K. For every field K, we can put a topology on A_K by defining $aN_{L/K}A_K$ to be a basis of neighborhoods of $a \in A_K$ where L/K varies over all finite Galois extensions of K. This topology is the **norm topology** of A_K. Some of its basic properties are presented below.

Lemma 2.2.13. (i) *The open subgroups of A_K are precisely the closed subgroups of finite index.*

(ii) *The valuation $\nu_K : A_K \to \hat{\mathbb{Z}}$ is continuous.*

(iii) *If L/K is a finite extension, then $N_{L/K}$ is continuos.*

(iv) *A_K is Hausdorff if and only if the group $A_K^0 = \cap_L N_{L/K} A_L$ is trivial.*

Proof. (i) If $\mathcal{N}$ is a subgroup of A_K, then

$$\mathcal{N} = A_K \backslash \bigcup_{a\mathcal{N} \neq \mathcal{N}} a\mathcal{N}$$

If $\mathcal{N}$ is open, then so are all $a\mathcal{N}$ (topological group A_K), and thus $\mathcal{N}$ is closed. Since $\mathcal{N}$ contains one neighborhood $N_{L/K}A_L$ of the basis of neighborhoods of 1, $\mathcal{N}$ has finite index. Conversely, if $\mathcal{N}$ is closed and of finite index, then the union (which is thus finite) is closed, and $\mathcal{N}$ is open.

(ii) The groups $f\hat{\mathbb{Z}}$ for $f \in \mathbb{N}$ form a basis of neighborhoods of 0. Now since $\nu_K(N_{L/K}A_L) \subseteq f\hat{\mathbb{Z}}$ where f is the inertia degree of L/K, the henselian valuation is continuous.

(iii) Let $N_{M/K}A_M$ be an open nbhd of 1. Then

$$N_{L/K}(N_{ML/L}A_{ML}) = N_{ML/K}A_{ML} \subseteq N_{M/K}A_M$$

which means $N_{L/K}$ is continuous. □

Theorem 2.2.5. *The map $L \mapsto \mathcal{N}_L = N_{L/K}A_L$ produces a one-to-one correspondence between finite abelian extensions L/K and the open subgroups $\mathcal{N}$ of A_K. Furthermore,*

$$L_1 \subseteq L_2 \iff \mathcal{N}_{L_2} \subseteq \mathcal{N}_{L_1}, \mathcal{N}_{L_1L_2} = \mathcal{N}_{L_1} \cap \mathcal{N}_{L_2}, \mathcal{N}_{L_1 \cap L_2} = \mathcal{N}_{L_1}\mathcal{N}_{L_2}$$

We call the field L corresponding to the subgroup $\mathcal{N}$ of A_K the **class field** associated with $\mathcal{N}$.

Proof. If L_1 and L_2 are abelian extensions of K, then the transitivity of norms implies $\mathcal{N}_{L_1L_2} \subseteq \mathcal{N}_{L_1} \cap \mathcal{N}_{L_2}$. If conversely $a \in \mathcal{N}_{L_1} \cap \mathcal{N}_{L_2}$, then $(a, L_1L_2/K) \in G(L_1L_2/K)$ projects to the trivial element in $G(L_i/K)$. Thus, $(a, L_1L_2/K) = 1$, meaning $a \in \mathcal{N}_{L_1L_2}$. It follows that

$$N_{L_2} \subseteq N_{L_1L_2} \cap N_{L_1} = N_{L_2} \iff [L_1L_2 : K] = [L_2 : K] \iff L_1 \subseteq L_2$$

which means the map in the theorem is injective.

If $\mathcal{N}$ is an open subgroup which contains some $\mathcal{L}$, we may assume L is abelian by the general reciprocity law. By Galois correspondence, the subgroup $(\mathcal{N}, L/K)$ corresponds to some intermediate field L' of L/K. Since $\mathcal{N}$ contains $\mathcal{N}_L$, the preimage of $G(L/L')$ is simply $\mathcal{N}$, meaning it's the kernel of $(\cdot, L'/K) : A_K \to G(L'/K)$. Hence, again by the general reciprocity law, $\mathcal{N} = \mathcal{N}_{L'}$ which suggests the map is surjective. The remaining relation can be proved easily using the previous two parts. □

An important tool which will be used to test the class field axioms in the other two sections of this chapter is the **Herbrand quotient**. Namely, the quotient

$$h(G, A) = \frac{\#H^0(G, A)}{\#H^{-1}(G, A)}$$

(of course, we are not using the standard cohomological definition). In fact, the Herbrand quotient is multiplicative on short exact sequences.

Lemma 2.2.14. *If $1 \to A \to B \to C \to 1$ is a short exact sequence of G-module, then one obtains*

$$h(G, B) = h(G, A)h(G, C)$$

For a finite G-module, $h(G, A) = 1$.

We will not give the proof of this noticeable property of Herbrand quotients here, as the actual idea fits the context of group cohomology better.

2.2.2 Local theory

The main theorems

In this section we apply the theory developed in the previous section to local fields, that is, finite extensions of $\mathbb{Q}_p$ or $\mathbb{F}_p((t))$ for primes $p \leqslant \infty$, depending on the characteristic of the field. The local fields can also be interpreted as fields complete against a given discrete valuation and with a finite residue class field.

Throughout the section, we keep the following objects in mind. ν_k the normalized discrete valuation on $K^\times$; $\mathfrak{o}_K$ the valuation ring; $\mathfrak{p}_K$ the maximal ideal of the ring; κ the residue class field; U_K the group of units; $U_K^{(}n) = 1 + \mathfrak{p}_K^n$ for $n = 1, 2, \dots, q = \#\kappa$; $|\cdot|_p$ the normalized $\mathfrak{p}$-adic absolute value; μ_n the group of nth roots of unity for which $\mu_n(K) = \mu_n \cap K^\times$; π_K the uniformizer $(\pi_K) = \mathfrak{p}_K$.

We let G be the absolute Galois group of k for some fixed local field k, and $A = \bar{k}^\times$, the G-module of units of the separable closure of k. If K/k is finite, $A_K = K^\times$. Indeed, we have the class field axiom:

Theorem 2.2.6. *For a cyclic extension L/K of local fields,*

$$\#H^i(G = G(L/K), L^\times) = \begin{cases} [L : K], & i = 0 \\ 1, & i = -1 \end{cases}$$

Proof. For $i = -1$, the axiom is simply Hilbert's 90, proved. It remains to show that $h(G, L^\times) = \#H^0(G(L/K), L^\times) = [L : K]$. The exact sequence

$$1 \to U_L \to L^\times \xrightarrow{\nu_L} \mathbb{Z} \to 0$$

where $\mathbb{Z}$ is regarded as a trivial G-module yields

$$h(G, L^\times) = h(G, \mathbb{Z})h(G, U_L) = [L : K]h(G, U_L)$$

It suffices to show that $h(G, U_L) = 1$. Choose (via the normal basis theorem) a normal basis $\{\alpha^\sigma\}$ of L/K where $\alpha \in \mathfrak{o}_L$. Consider the clopen G-module $M = \sum_{\sigma \in G}(\alpha^\sigma)$. Then the open sets $V^n = 1 + \pi_K^n(M)$ form a basis of open nhds of 1 in U_L. Since M is open, $(\pi_K^N) \subseteq \mathfrak{o}_L$ for some N. For $n \geqslant N$, V^n are subgroups of finite index in U_L since

$$(\pi_K^n M)(\pi_K^n M) = \pi_K^{2n} MM \subseteq \pi_K^{2n}\mathfrak{o}_L \subseteq \pi_K^{2n-N} M \subseteq \pi_K^{2n} M$$

which means $V^n V^n \subseteq V^n$. As $1 - \pi_K^n \mu \in V^n$ for any $\mu \in M$,

$$(1 - \pi_K^n \mu)^{-1} = 1 + \pi_K^n \sum_{i=1}^{\infty} \mu^i \pi_K^{n(i-1)} \in M$$

The map $1 + \pi_K^n \alpha \mapsto \alpha \bmod \pi_K M$ induces a G-isomorphism:

$$V^n/V^{n+1} \cong M/\pi_K M = \bigoplus_{\sigma \in G} (\mathfrak{o}_K/\mathfrak{p}_K)\alpha^\sigma = \mathrm{Ind}_G^{\{1\}}(\mathfrak{o}_K/\mathfrak{p}_K)$$

Shapiro's lemma extended to Tate cohomology groups implies

$$H^i(G, V^n/V^{n+1}) = H(\{1\}, \mathfrak{o}_K/\mathfrak{p}_K) = 1$$

for all i and $n \geqslant N$. Therefore, $H^i(G, V^n) = 1$. We now obtain, by the multiplicativity of h,

$$h(G, U_L) = h(G, U_L/V^n)h(G, V^n) = 1$$

where $h(G, U_L/V^n) = 1$ because U_L/V^n is finite. □

Since $\text{Gal}(\tilde{k}/k) \cong \text{Gal}(\bar{\kappa}/\kappa) \cong \hat{\mathbb{Z}}$, where $\tilde{k}$ is the maximal unramified extension of k, we have a surjective homomorphism $d : G = \text{Gal}(\bar{k}/k) \to \hat{\mathbb{Z}}$ being the composition of a restriction and the isomorphism above. Now if K/k is finite,

$$\frac{1}{e_K}\nu_K(K^*) = \frac{1}{[K:k]}\nu(N_{K/k}K^\times) = \frac{1}{e_K f_K}(N_{K/kK^\times})$$

which means ν_K is henselian. Thus, we have everything required for the reciprocity law. One may therefore obtain

Theorem 2.2.7 (Artin reciprocity law, local)**.** *For every finite Galois extension L/K of local fields, we have a canonical isomorphism*

$$r_{L/K} : \text{Gal}(L/K)^{\mathsf{ab}} \to K^\times/N_{L/K}L^\times$$

Proof. A combination of Theorem 2.2.4 and Theorem 2.2.6. □

The norm residue symbol of the field $\mathbb{C}$ can be defined as $(\cdot, \mathbb{C}/\mathbb{R}) : \mathbb{R}^\times \to \text{Gal}(\mathbb{C}/\mathbb{R})$

$$(a, \mathbb{C}/\mathbb{R})i = i^{\text{sign}(a)}$$

which clearly has kernel $\mathbb{R}_{>0} = N_{\mathbb{C}/\mathbb{R}}\mathbb{C}^\times$. Therefore, this is indeed the inverse of the reciprocity map.

Theorem 2.2.8. *The map*

$$L \mapsto \mathcal{N}_L = N_{L/K}L^\times$$

gives a one-to-one correspondence between finite abelian extensions of the local field K and the open subgroups of finite index in $K^\times$. Moreover, $E \subseteq F$ if and only if $\mathcal{N}_F \subseteq \mathcal{N}_F$, $\mathcal{N}_{EF} = \mathcal{N}_E \cap \mathcal{N}_F$ and $\mathcal{N}_{E\cap F} = \mathcal{N}_E\mathcal{N}_F$.

Proof. The last three statements are easy — simply use the correspondence and the fact that $N_{F/K} = N_{F/E}N_{E/K}$.

By Theorem 2.2.5, it suffices to show open subgroups of finite index in the norm topology are precisely the open subgroups of finite index in the p-adic topology. If $\mathcal{N}$ is open in the norm topology, then being a nbhd it contains some $N_{L/K}L^\times$ which has finite index in $K^\times$. The set is open in the valuation topology because it contains $N_{L/K}U_L$ which is open. To prove the converse we argue in two cases on the index of $\mathcal{N}$.

Suppose the characteristic of K is relatively prime to $n \in \mathbb{N}$. For any subgroup fo finite index $n = (K^\times : \mathcal{N})$, we have $K^{\times n} \subseteq \mathcal{N}$. If $K^\times$ does not contain the group of nth roots of unity, we take $K_1 = K(\mu_n)$. Now if $K_1^{\times n}$ contains a group of norms $N_{L_1/K_1}L_1^\times$ and L/K is a Galois extension containing L_1, then

$$N_{L/K}L^\times = N_{K_1/K}N_{L/K_1}L^\times \subseteq N_{K_1/K}N_{L_1/K_1}L_1^\times \subseteq K^{\times n}$$

Thus, assume $\mu_n \subseteq K$ and we claim that K contains a group of norms. Let $L = K(\sqrt[n]{K^\times})$ be the maximal abelian extension of exponent n. Then Kummer's theory suggests

$$\text{Hom}(\text{Gal}(L/K), \mu_n) \cong K^\times/K^{\times n}$$

which is finite. Since $K^\times/N_{L/K}L^\times$ is isomorphic to $\mathrm{Gal}(L/K)$, one may deduce $K^{\times n} \subseteq N_{L/K}L^\times$. But then

$$\#K^\times/K^{\times n} = \#\,\mathrm{Gal}(L/K) = \#K^\times/N_{L/K}L^\times$$

which means $K^{\times n} = N_{L/K}L^\times$ so that $\mathcal{N}$ is open.

The case where the characteristic of K divides n can be tackled via the Lubin-Tate theory. □

Definition 2.2.6. Let L/K be finite and n the smallest number such that $U_K^n \subseteq N_{L/K}L^\times$. Then the ideal $\mathfrak{f} = \mathfrak{p}_K^n$ is the **conductor** of L/K.

Lemma 2.2.15. *A finite abelian extension L/K is unramified if and only if its conductor is $\mathfrak{f} = 1$.*

We will use the local Artin reciprocity law to prove a local version of Kronecker-Weber. By the local property of the ring $\mathfrak{o}_K$, the groups $(\pi^f) \times U_K^{(n)}$ (where π is the prime element of $\mathfrak{o}_K$) form an open basis of the topological group $K^\times$. Therefore, every abelian extension L/K is contained in the class field of such an open subgroup. When $K = \mathbb{Q}_p$, the class field of the smallest such open subgroup $(p) \times U_K^{(n)}$ is just $\mathbb{Q}_p(\mu_{p^n})$. In particular we have,

Lemma 2.2.16. *The group $N_{L/K}L^\times$ of the extension $L = \mathbb{Q}_p(\mu_{p^n})/K = \mathbb{Q}_p$ is the group $(p) \times U_K^{(n)}$.*

The proof is quite sophisticated, so we omit it. But with the help of this observation, we can show the local Kronecker-Weber:

Theorem 2.2.9. *Every finite abelian extension L of $K = \mathbb{Q}_p$ is contained in a field $\mathbb{Q}_p(\zeta)$ where ζ is a root of unity. In particular, the maximal abelian extension of $\mathbb{Q}_p$ is the smallest extension containing all roots of unity.*

Proof. By the previous argument, we may assume $(p^f) \times U_K^{(n)}$ is contained in the open subgroup $N_{L/K}L^*$ for some n and some f. Then L is contained in the class field of the intersection of $(p^f) \times U_K$ and $(p) \times U_K^{(n)}$. Therefore L is contained in the compositum (following Theorem 2.2.8) of the class fields of the two groups. The first one is an unramified extension of inertia degree f, and $\mathbb{Q}_p(\mu_{p^n})$ (by Lemma 2.2.16), meaning it is contained in the generated by the $(p^f - 1)p^n$th roots of unity. □

2.2.3 Global theory

Adeles and ideles

Historically global fields are quite well-studied before local fields. In Section 2.1, we witnessed the development of the approach to global class field theory with modulus. But then, to understand the theory for local fields, Chevalley reformulated the statements using adeles. In [Tat67b], Tate outlines the reason behind the equivalence of the modulus construction and the adeles construction. The key is that an admissible (satisfying some topological properties) homomorphism from the idele group to the Galois group induces a unique admissible homomorphism from the generalized ideal group to the Galois group, and vice versa.

Definition 2.2.7. The **adele ring** of K is the restricted product

$$\mathbb{A}_K = \prod_{\mathfrak{p}}{}' K_{\mathfrak{p}}$$

with respect to the subrings $\mathfrak{o}_{\mathfrak{p}} \subseteq K_{\mathfrak{p}}$ where $\mathfrak{p}$ varies over the places of K and $K_{\mathfrak{p}}$ the completion of K at $\mathfrak{p}$. The adele has a ring structure with addition and multiplication defined componentwise.

By a restricted product, we mean for each element $(a_\mathfrak{p}) \in \mathbb{A}_K$, $a_\mathfrak{p} \in \mathfrak{o}_\mathfrak{p}$ for all but finitely many places $\mathfrak{p}$. Since each $K_\mathfrak{p}$ is locally compact, $\mathbb{A}_K$ is locally compact.

Remark 2.2.6. An equivalent definition of the adele ring is to set

$$\mathbb{A}_\mathbb{Z} = \widehat{\mathbb{Z}} \times \mathbb{R}, \quad \mathbb{A}_\mathbb{Q} = \mathbb{Q} \otimes_\mathbb{Z} \mathbb{A}_\mathbb{Z}$$

which makes sense as $\mathbb{Q}$ only has one infinite place. Note that This gives us a restricted product since

$$\mathbb{A}_\mathbb{Q} = (\mathbb{Q} \otimes_\mathbb{Z} \widehat{\mathbb{Z}}) \times (\mathbb{Q} \otimes_\mathbb{Z} \mathbb{R}) = \prod_p{}' \mathbb{Q}_p \times \mathbb{R}$$

but an element of the leftmost side $x/y \otimes (r, (a_p))$ is mapped to the element $(xr/y, (xa_p/y))$ on the rightmost side. Yet the element y is invertible in $\mathbb{Z}_p$ if p does not divide y. Thus, the product is in fact restricted.

Therefore we may naturally define $\mathbb{A}_K = \mathbb{A}_\mathbb{Q} \otimes_\mathbb{Q} K$, which is consistent with Definition 2.2.7.

Definition 2.2.8. The **idele group** of K is the restricted product

$$\mathbb{A}_K = \prod_\mathfrak{p}{}' K_\mathfrak{p}^\times$$

with respect to the subgroups $\mathfrak{o}_\mathfrak{p}^\times \subseteq K_\mathfrak{p}^\times$ where $\mathfrak{p}$ varies over the places of K and $K_\mathfrak{p}$ the completion of K at $\mathfrak{p}$.

Remark 2.2.7. It must be emphasized that the idele group does *not* inherit its topology from $\mathbb{A}_K$. Indeed, there is no reason for a unit group of some topological ring to be a topological group. For example, under the subspace topology of $\mathbb{A}_\mathbb{Q}$, we may define the sequence $(a_p) = (1, \dots, 1, p, 1, \dots)$ where p sits precisely in $\mathbb{Q}_p$. For each open nhds basis element U of 1, we notice that for some large enough p, $(a_p) \in U$. Thus, $\lim_{p\to\infty}(a_p) = 1$. But $1/p$ does not sit in $\mathbb{Z}_p$ for any p, so $\lim_{p\to\infty}(a_p)^{-1} \neq 1$. Therefore, the map $a \to a^{-1}$ is not continuous under the subspace topology so $I_\mathbb{Q}$ cannot be a topological group with that topology. It is fairly easy to solve this problem. We may embed I_K into $\mathbb{A}_K^2$ via the map $x \mapsto (x, x^{-1})$. Then we impose the subspace topology of I_K's image in $\mathbb{A}_K^2$ on I_K. In this case the inversion map is continuous since it's the composition of the projection to the first second and the map that defines the topology. It is therefore easy to see that each $a \in I_K$ lies in some product of open sets and thus $a, a^{-1} \in \mathfrak{o}_\mathfrak{p}$ or $a \in \mathfrak{o}_\mathfrak{p}$ for almost all $\mathfrak{p}$.

For every finite set of places S, I_K contains the subgroup

$$I_K^S = \prod_{\mathfrak{p}\in S} K_\mathfrak{p}^\times \times \prod_{\mathfrak{p}\notin S} U_\mathfrak{p}$$

of S**-ideles**. We may embed $K^\times$ into I_K by sending $a \in K^\times$ to (a) whose $\mathfrak{p}$th component is simply the image of a in $K_\mathfrak{p}$. We call $K^\times$ the **principal ideles** (and similarly the principal adeles) and write $K^S = K^\times \cap I_K^S$ consisting of elements called the S**-units**. This embedding is, according to Tate, essential to the adelic theory of characters, L-functions, etc. The principal ideles enjoy some very special topological properties.

Remark 2.2.8. The map sending $(a_\mathfrak{p})$ in I_K to $\prod_\mathfrak{o} \mathfrak{p}^{\nu_\mathfrak{p}(a_\mathfrak{p})}$ is a surjective morphism from I_K to the group of fractional ideals, with kernel I_K^S for S the set of infinite primes in K. Thus the adelic construction is actually equivalent to the ray class group construction (the image of $I_K^{S'}$ under the map above is precisely $I_K(\mathfrak{m})$ for $\mathfrak{m}$ divisible by all infinite primes and primes in S'), although the latter predates the former. But the adelic construction is more convenient in the sense that it provides an explicit way to switch between fields and their completions.

Definition 2.2.9. The quotient

$$C_K = K^\times \backslash I_K$$

is called the **idele class group** of K.

Remark 2.2.9. We let $K^\times$ act on I_K on the left to be consistent with the general case of $GL_n(K)$ acting on $GL_n(\mathbb{A}_K)$. In fact, one can easily wit that

$$C_K = K^\times \backslash \mathbb{A}_K^\times = GL_1(K)\backslash GL_1(\mathbb{A}_K)$$

Let L/K be a finite extension, one might wonder if there is a relation between $\mathbb{A}_L$ and $\mathbb{A}_K$. It is natural to define the L-vector space $\mathbb{A}_K \otimes L$, and in fact

Lemma 2.2.17. *If L/K is finite separable, there is a canonical isomorphism (of topological groups) $\mathbb{A}_L \cong \mathbb{A}_K \otimes_K L$ sending the principal adeles L to $K \otimes_K L$.*

Proof. The RHS contains elements of the form $(a_\mathfrak{p}) \otimes x$ which can be sent to $(a_\mathfrak{p} \otimes x)$, producing an isomorphism from $\mathbb{A}_K \otimes_K L$ to the restricted product of $K_\mathfrak{p} \otimes L$ with respect to $\mathfrak{o}_{K_\mathfrak{p}} \otimes_{\mathfrak{o}_K} \mathfrak{o}_L$. But $K_\mathfrak{p} \otimes L$ is isomorphic to $\prod_{\mathfrak{P}|\mathfrak{p}} L_\mathfrak{P}$ and $\mathfrak{o}_{K_\mathfrak{p}} \otimes_{\mathfrak{o}_K} \mathfrak{o}_L = \prod_{\mathfrak{P}|\mathfrak{p}} \mathfrak{o}_{L_\mathfrak{P}}$. Thus,

$$\mathbb{A}_K \otimes_K L \cong \prod (L_\mathfrak{P}, \mathfrak{o}_{L_\mathfrak{P}}) = \mathbb{A}_L$$

The image of $K \otimes_K L$ in $\mathbb{A}_K \otimes_K L$ is $\{(1, 1, \dots) \otimes x\}$ for $x \in L$, and via the isomorphism we get $\{(x, x, \dots)\} = L$ in $\mathbb{A}_L$. □

Since L is a $[L : K]$ dimensional K-vector space, the tensor product is therefore $\mathbb{A}_K \oplus \cdots \oplus \mathbb{A}_K = \mathbb{A}_L$, and $L = K \oplus \cdots \oplus K$. The embedding $K \hookrightarrow \mathbb{A}_K$, though seems trivial, is the crucial thing that makes adeles interesting. In fact, Tate says we can do nothing without this embedding.

Definition 2.2.10. On $\mathbb{A}$ we may define norms $|\cdot|_\mathfrak{p}$ by

$$|(a_\mathfrak{p})|_\mathfrak{p} = |a_\mathfrak{p}|_\mathfrak{p}$$

And naturally we can define the **adelic norm**

$$|a| = \prod_\mathfrak{p} |a|_\mathfrak{p}$$

which converges since the factors are less than or equal to 1 for all but finitely many $\mathfrak{p}$.

Lemma 2.2.18 (product formula). *Let L be a global field, embedded in $\mathbb{A}_L$. Then for all $x \neq 0 \in L$ we have $|x| = 1$*

Proof. Say L is a finite separable extension of $K = \mathbb{Q}$ or $\mathbb{F}_q(t)$. Note that for a prime $\mathfrak{p}$ of K

$$\prod_{\mathfrak{P}|\mathfrak{p}} |x|_\mathfrak{P} = \prod_{\mathfrak{P}|\mathfrak{p}} |N_{L_\mathfrak{P}/K_\mathfrak{p}}(x)|_\mathfrak{p} = |N_{L/K}(x)|_\mathfrak{p}$$

where the last equality is a consequence of the norms on products and $L \otimes K_\mathfrak{p} \cong \prod_{\mathfrak{P}|\mathfrak{p}} L_\mathfrak{P}$. Then

$$\prod_\mathfrak{p} |N_{L/K}(x)|_\mathfrak{p} = \prod_\mathfrak{P} |x|_\mathfrak{P}$$

where $|x|_\mathfrak{P}$ is just the $\mathfrak{P}$-norm of x in L by the embedding $x \mapsto (x, x, \dots)$ of L in $\mathbb{A}_L$. Therefore the product formula reduces to $\mathbb{Q}$ and $\mathbb{F}_q(t)$. The LHS is always one: for $\mathbb{Q}$ if we write $y = N_{L/K}(x) = \pm p_1^{k_1} \cdots p_n^{k_n}$ then $|y|_\infty = p_1^{k_1} \cdots p_n^{k_n}$, $|y|_{p_i} = p_i^{-k_i}$ and $|y|_q = 1$ for $q \nmid y$, so the LHS is one; for $\mathbb{F}_q(t)$, write $y = \pi_1^{k_1} \cdots \pi_n^{k_n}$. Then $|y|_\infty = q^{\deg y}$, $|y|_{\pi_i} = q^{-k_i \deg \pi_i}$ and $|y|_\pi = 1$ for all other $\mathfrak{p} \nmid y$. But the degree of y equals the sum of $k_i \deg \pi_i$, so the product of norms of y is also one, completing the proof. □

Theorem 2.2.10. *Let L be a global field. The principal adeles form a discrete subgroup and the quotient $\mathbb{A}_L/L$ is compact.*

Proof. We regard L as a finite separable extension of $\mathbb{Q}$ or $\mathbb{F}_q(t)$. If the statements hold for $K = \mathbb{Q}$ or $\mathbb{F}_q(t)$ then since $L = K \oplus \cdots \oplus K$, so are true for L. To show that K is discrete, we claim 0 is isolated. Consider the set $\{(a_\mathfrak{p})\}$ where $a_\mathfrak{p} \in \mathfrak{o}_{K_\mathfrak{p}}$ for all finite primes and $|a_\infty|_\infty < 1$ for the usual norm in $\mathbb{Q}$ or the absolute value of degree valuations in $\mathbb{F}_q(t)$. But note that $|a| = 1$ for all nonzero principal adeles, so the only principal adele in U is 0. Thus, K is discrete.

We will not prove the compactness of the quotient. The proof is essentially an analysis of the Minkowski-theoretic subspace $U_\infty \otimes \prod_{\mathfrak{p}\nmid\infty} \mathfrak{o}_{K_\mathfrak{p}}$. □

Theorem 2.2.11 (strong approximation). *Let S be a finite set of primes in K. Fix any prime $\mathfrak{p} \notin S$ of K. Denote the T the primes not in S other than $\mathfrak{p}$. Given $a_\mathfrak{q} \in K$ and $\varepsilon_\mathfrak{q} \in \mathbb{R}_{>0}$ for each $\mathfrak{q} \in S$, there is an x such that $|x - a_\mathfrak{q}| \leqslant \varepsilon_\mathfrak{q}$ for all $\mathfrak{q} \in S$ and $|x|_\mathfrak{q} \leqslant 1$ for all $\mathfrak{q} \in T$.*

A more intuitive restatement of the result above is

Corollary 2.2.2. *Let $\mathfrak{p}$ be a prime in K. Then K is dense in the restricted product of $K_\mathfrak{q}$ with respect to $\mathfrak{o}_{K_\mathfrak{q}}$ for all primes $\mathfrak{q} \neq \mathfrak{p}$.*

The main result

Theorem 2.2.12 (global (adelic) reciprocity law). *For every Galois extension L/K of number fields, we have a canonical isomorphism*

$$r_{L/K} : \mathrm{Gal}(L/K)^{\mathsf{ab}} \to C_K/N_{L/K}C_K$$

We will not show the class field axiom for the global fields. They could be done via cohomologies of the Galois group, proving two inequalities the *first inequality* and the *second inequality* showing the size of the first cohomology group is $[L : K]$. The theorem then follows from the abstract class field theory, once the class field axiom is assumed.

But to understand the purpose of adeles and ideles here, we must construct some $s : C_K \to \mathrm{Gal}(L/K)$ explicitly. In fact, this map can be constructed from local class field theory — this is why the history of class field theory was global implied local, and local was used to prove global.

Let L/K be an abelian extension of number fields and v a place of K. Let G be the Galois group and G_v the decomposition group of v. Then $G_v \cong \mathrm{Gal}(L_w/K_v)$ where w is any place above v. Define $s_{K,v} : K_v^\times \to G_v$ as follows: if v is finite, then this is the inverse of the local reciprocity map; if v is real, then the sign map $\mathbb{R}^\times \to \{\pm 1\}$; if v is complex, then G_v is trivial and we are done. Then we have a well-defined map $\tilde{s}_K : I_K \to G$ given by $(a_v) \mapsto \prod_v s_{K,v}(\alpha_v)$.

Lemma 2.2.19 (local-global compatibility). *The map $s_{L/K}$ indeed induces the abstract reciprocity map.*

Chapter 3

L-functions

3.1 Euler, Dirichlet, Dedekind, Weber and Hecke

In this section I will go over three types of L-functions and some of their properties (analytic/meromorphic continuations, functional equations, etc.). The main references for this section are [Hei67], [Sny02] and [Cog06]. Prof. David Helm, the supervisor of this project, very kindly suggested [Sny02] to the author, who later found it a superbly rich and comprehensive source. Beyond the very shallow and short summary of some chosen information presented in this project, [Sny02] contains much more than what could be said here.

3.1.1 Dirichlet L-functions

L-functions play an important role in number theory. One of its special cases, the Riemann zeta function, has drawn great interest since Euler introduced it and wrote it as a product among primes. It was quite early that mathematicians realized certain analytic properties of L-function relate closely to those of prime numbers. The first great instance of L-functions besides the zeta function is Dirichlet L-functions with which Peter Gustav Lejeune Dirichlet proved his theorem on primes in arithmetic progressions.

It is unclear where the notation L came from. A thread on MathOverflow suggests three possibilities: (i) it was a natural alphabetical choice, (ii) the L is for Legendre or (iii) the L is for Lejeune. With any of them being the truth, we must first understand the significance of Dirichlet L-functions.

Definition 3.1.1. A **Dirichlet character of modulus** m is a completely multiplicative, m-periodic complex-valued function χ such that $\chi(a) \neq 0$ if and only if $(a, m) = 1$.

Therefore each homomorphism $(\mathbb{Z}/m\mathbb{Z})^\times \to \mathbb{C}^\times$ determines a Dirichlet character modulo m, and vice versa. Since $\chi(1) = 1$ and all elements of $(\mathbb{Z}/m\mathbb{Z})^\times$ have finite orders, we see that $|\chi(a)| = 1$ for all $(a, m) = 1$.

Definition 3.1.2. A **Dirichlet L-function** of the Dirichlet character χ is simply a function of complex numbers s defined by

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

Using his L-function, Dirichlet succeeded in proving the following theorem on the distribution of primes.

Theorem 3.1.1 (Dirichlet's theorem on arithmetic progressions)**.** *The series over primes congruent to a modulo m*

$$\sum_{p\equiv a \pmod m} \frac{1}{p}$$

diverges.

Proof. To prove this theorem we consider the following expansion of Dirichlet L-function.

$$\log L(s,\chi) = \sum_p -\log(1-\chi(p)p^{-s}) = \sum_{n=1}^{\infty} \frac{1}{n} \sum_p \frac{\chi(p)}{p^{ns}} = \sum_p \frac{\chi(p)}{p^s} + \sum_{n=2}^{\infty} \frac{1}{n} \sum_p \frac{\chi(p)}{p^{ns}}$$

where we use the Taylor expansion of the logarithm and the fact that the sums converge absolutely to interchange the summations. Furthermore,

$$\left|\sum_{n=2}^{\infty} \frac{1}{n} \sum_p \frac{\chi(p)}{p^{ns}}\right| \leqslant \int_2^{\infty} \int_2^{\infty} x^{-1}y^{-sx}dydx \leqslant x^{-2}s^{-1}2^{-sx}dx \leqslant \frac{1}{4s}\int_2^{\infty} 2^{-sx}dx < \frac{1}{32}$$

Write $G = (\mathbb{Z}/m\mathbb{Z})^\times$ for convenience. Then $|G| = \varphi(m)$. Thus, we may write $\log L(s,\chi) = \sum_p \chi(p)p^{-s} + O(1)$. If we define $f_a(s) = \sum_{p\equiv a} p^{-s}$ modulo m, then by the periodicity of χ, we have

$$\log L(s,\chi) = \sum_{a\in G} \chi(a) f_a(s) + O(1)$$

By the orthogonality of characters of finite groups, it is easy to see that

$$\frac{1}{\varphi(m)} \sum_{\chi\in\widehat{G}} \chi(g)\overline{\chi(h)} = \delta_{gh}$$

and thus

$$f_a(s) = \sum_{\chi\in\widehat{G}} \overline{\chi(a)} \log L(s,\chi) + O(1)$$

We aim to prove $f_a(1)$ diverges. It is known by Euler that $L(1,\chi_0)$ blows up where χ_0 is the trivial character. Also, if χ is nontrivial, then $\sum_{a\in G}\chi(a) = 0$ and $\sum_{a=1}^{\infty}\chi(a)$ is bounded, meaning $L(s,\chi)$ converges for $\mathrm{Re}(s) > 0$. Thus, it suffices to show $\log L(1,\chi) > -\infty$ or $L(1,\chi) \neq 0$ for any nontrivial character χ to show the divergence of $f_a(1)$.

This result of Dirichlet has many interesting proofs, and we just present an outline in this case. It can be shown that $L(1,\chi) = 0$ for at most one real primitive character χ. One then deduces that the character left is the Legendre symbol. Then using some heavy analysis one will deduce the L-function of the Legendre symbol at $s = 1$ is also nonzero, which completes the proof. □

After Riemann's great work on the zeta function (for which the zeta function got its name), people realized functional equations bear great technical significance. Indeed, L-functions also have analytic continuations and a functional equation. We call the smallest period of a Dirichlet character its **conductor** and a character is **primitive** if its conductor equals its modulus.

Theorem 3.1.2 (functional equation of Dirichlet L-functions)**.** *Let χ be a primitive DIrichlet character with conductor N and let ε be* 0 *or* 1 *such that $\chi(-1) = (-1)^\varepsilon$. Define*

$$\Lambda(s,\chi) = \pi^{-(s+\varepsilon)/2}\Gamma\left(\frac{s+\varepsilon}{2}\right) L(s,\chi)$$

Then $\Lambda(s,\chi)$ has a meromorphic continuation to all s. In particular, if χ is nontrivial, it has an analytic continuation; if χ is trivial, then Λ is analytic for all $s \neq 0, 1$. We have the functional equation

$$\Lambda(s,\chi) = (-i)^{\varepsilon}\tau(\chi)N^{-s}\Lambda(1-s,\bar{\chi})$$

where τ is the Gauss sum

Proof. If χ is trivial, then $L(s,\chi)$ is just the Riemann zeta function, $N = 1$ and $\varepsilon = 0$. In this case, the Gauss sum is just 1. Then, by Riemann's functional equation,

$$\Lambda(s,\chi) = \pi^{-s/2}\Gamma\left(\frac{s}{2}\right)\zeta(s) = \pi^{-(1-s)/2}\Gamma\left(\frac{1-s}{2}\right)\zeta(1-s) = \Lambda(1-s,\chi)$$

Thus, it suffices to show the theorem for nontrivial χ. We define the theta function of χ by

$$\theta_{\chi}(t) = \frac{1}{2}\chi(0) + \sum_{n=1}^{\infty}\chi(n)e^{-\pi n^2 t}$$

Then as a consequence of the Poisson summation formula, we see

$$\theta_{\chi}(t) = \frac{(-i)^{\varepsilon}\tau(\chi)}{N^{1+\varepsilon}t^{\varepsilon+1/2}}\theta_{\bar{\chi}}\left(\frac{1}{N^2 t}\right)$$

Note that for all $\mathrm{Re}(s) > 1$,

$$\int_0^{\infty} e^{-\pi t n^2}t^{(s+\varepsilon)/2}t^{-1}dt = \pi^{-(s+\varepsilon)/2}\Gamma\left(\frac{s+\varepsilon}{2}\right)n^{-(s+\varepsilon)}$$

So

$$\int_0^{\infty}\theta_{\chi}(t)t^{(s+\varepsilon)/2}t^{-1}dt = \Lambda(s,\chi)$$

Both sides are analytic for all s. Take the change of variables $t = 1/N^2 t$ and use the functional equation of θ_{χ}, we get the desired result. □

One may obverse that the use of θ_{χ} in the previous proof is quite dry. Indeed, the essence of the functional equation is the Poisson summation formula. We will later see that, with a suitable way of defining L-functions and Fourier analysis, Tate was able to deduce the functional equation of a special class of L-functions using only the Poisson summation formula.

3.1.2 Hecke L-functions

Following Dirichlet's effort to compute the class number of cyclotomic fields, Kummer defined a form of zeta functions on cyclotomic fields in Chapter VIII of his [Kum51]. It was then generalized by Dedekind in [DD13] to all number fields.

Take K a number field, $\mathfrak{o}_K$ its ring of integers, and N the absolute norm of ideals. Define

Definition 3.1.3. The **Dedekind zeta function** for K is

$$\zeta_K(s) = \sum_{\mathfrak{a}}\frac{1}{N(\mathfrak{a})^s}$$

summing over all ideals of $\mathfrak{o}_K$.

Lemma 3.1.1. *The Dedekind zeta function converges for* $\mathrm{Re}(s) > 1$ *and*

$$\zeta_K(s) = \prod_{\mathfrak{p}}\frac{1}{1-N(\mathfrak{p})^{-s}}$$

where $\mathfrak{p}$ varies over the nonzero prime ideals of $\mathfrak{o}_K$.

Proof. We will prove the equality and deduce the first statement using the convergence of the product. It is obvious that there are at most $[K:\mathbb{Q}] = n$ prime ideals lying above a rational prime p. Write $(p) = \mathfrak{p}_1 \cdots \mathfrak{p}_l$, then as $1 < N(\mathfrak{p}_i) | N(p) = p^n$, $p^n = N(p) = \prod N(\mathfrak{p}_i) \geqslant p^l$. This suggests

$$\prod_{\mathfrak{p}|(p)} \frac{1}{1 - N(\mathfrak{p})^{-s}} < \frac{1}{(1-p^{-s})^n}$$

The new Euler product

$$\prod_{\mathfrak{p}} \frac{1}{1 - N(\mathfrak{p})^{-s}} = \prod_p \prod_{\mathfrak{p}|(p)} \frac{1}{1 - N(\mathfrak{p})^{-s}} < \zeta(s)^n$$

which converges for $\mathrm{Re}(s) > 1$. We also see, from the unique factorization of ideals, that

$$\sum_{N(\mathfrak{a})<n} N(\mathfrak{a})^{-s} \leqslant \prod_{N(\mathfrak{p})<n} \frac{1}{1 - N(\mathfrak{p})^{-s}}.$$

By the monotone convergence theorem, the LHS converges to the RHS for $\mathrm{Re}(s) > 1$, completing the proof. □

Before Weber generalized Dirichlet L-functions to characters of ray class groups, Ramanujan proved his significant result on coefficients of the cuspidal modular form Δ, which inspired a lot in the study of L-functions of modular forms.

As Cogdell stated in [Cog06], analogous to Dirichlet's definition of L-functions on characters of the finite group $(\mathbb{Z}/m\mathbb{Z})^\times$, Weber defined a generalized version on characters of ray class groups (which were proven finite). Hecke then proved many analytic properties of this function, which we now call the Hecke L-function.

Let K be a number field and $\mathfrak{m}$ be some modulus. Take K^∞ to be the direct product of completions of K at infinite places.

Definition 3.1.4. Let $\{\mathfrak{a}_1, \ldots, \mathfrak{a}_r\}$ be a set of representatives of the ideal class group I_K/P_K of K. A **Grossencharacter modulo** $\mathfrak{m}$ is a character χ of $I_K(\mathfrak{m})$ such that $\chi(\mathfrak{a}_i(a)) = \chi'(\mathfrak{a}_i)\chi_f(a)\chi_\infty(a)$ where χ' is a character of I_K/P_K, χ_f a character of $(\mathfrak{o}_K/\mathfrak{m})^\times$ and χ_∞ a character of K^∞.

In Section 3.2.3, I will show that the definition here corresponds to Tate's adelic definition of Grossencharacters.

The **conductor** of a Grossencharacter χ is the smallest modulus $\mathfrak{n}$ such that χ is a Grossencharacter modulo $\mathfrak{n}$. A Grossencharacter modulo $\mathfrak{m}$ is **primitive** if its conductor is $\mathfrak{m}$. This is equivalent to saying that χ_f does not factor through $\mathfrak{o}_k/\mathfrak{m}'$ for any $\mathfrak{m}'$ dividing $\mathfrak{m}$.

Definition 3.1.5. If χ is a Grossencharacters modulo $\mathfrak{m}$, then define the **Hecke L-function** to be

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

Hecke spent a lot of time proving the following functional equation of Hecke L-functions. His proof requires much effort and also a very complicated theta function. However, in the next section, we will see an elegant proof of Tate which reformulates the Grossencharacters in terms of ideles.

Theorem 3.1.3 (functional equation of Hecke L-functions)**.** *Take χ a primitive Grossencharacter of K modulo $\mathfrak{m}$. Define the* **completed L-function**

$$\Lambda(s,\chi) = (|d_K| N(\mathfrak{m}))^{s/2} L(s,\chi) L_\infty(s,\chi)$$

where

$$L_\infty(s,\chi) = \prod_{v\mid\infty} L_v(s,\chi)$$

and

$$L_v(s,\chi) = \begin{cases} \Gamma_{\mathbb{R}}(s) = \pi^{-s/2}\Gamma\left(\frac{s}{2}\right), & v \text{ real dividing } \mathfrak{m} \\ \Gamma_{\mathbb{R}}(s+1), & v \text{ real not dividing } \mathfrak{m} \\ \Gamma_{\mathbb{C}}(s) = \Gamma_{\mathbb{R}}(s)\Gamma_{\mathbb{R}}(s+1), & v \text{ complex} \end{cases}.$$

Then Λ has a meromorphic continuation to all complex numbers. It satisfies the functional equation

$$\Lambda(s,\chi) = \varepsilon(\chi)\Lambda(1-s,\bar{\chi})$$

where $|\varepsilon(\chi)| = 1$.

It is then a natural thing to consider the relations of L-functions of field extensions. Indeed, Weber proved the following theorem as a fantastic result of Theorem 2.2.12.

Theorem 3.1.4 (Weber)**.** *Let L/K be an abelian extension of number fields, and $\widehat{G}$ the Pontryagin dual of the ray class group $G = I_K(\mathfrak{m})/H$ of L/K where H is a congruence subgroup. Then*

$$\zeta_L(s) = \prod_{\chi\in\widehat{G}} L(s,\chi) = L(s,1)\prod_{\chi\neq 1} L(s,\chi) = \zeta_K(s)\prod_{\chi\neq 1} L(s,\chi)$$

Proof. First we expand the zeta function over L by its definition.

$$\zeta_L(s) = \prod_{\mathfrak{P}} \frac{1}{1-N(\mathfrak{P})^{-s}}$$

Say $\mathfrak{p}$ is an unramified prime. Then suppose there are g numbers of primes $\mathfrak{P}$ lying above $\mathfrak{p}$, all of inertia degree f. Then $N(\mathfrak{P}) = N(\mathfrak{p})^f$ and $[L:K] = fg$. In this case we have

$$\prod_{\mathfrak{P}\mid\mathfrak{p}} \frac{1}{1-N(\mathfrak{P})^{-s}} = \frac{1}{[1-N(\mathfrak{p})^{-sf}]^g} = \left[\prod_{\omega_f^f=1} \frac{1}{1-\omega_f N(\mathfrak{p})^{-s}}\right]^g$$

where ω_f varies over the fth roots of unity. The Frobenius element over $\mathfrak{p}$ has order f, so the prime $\mathfrak{p}$ also has order f. Thus, $\chi(\mathfrak{p})$ is an fth root of unity. But since the ray class group is finite abelian, it has a cyclic decomposition, meaning the roots of unity occur equally often for characters of the ray class group. Then by the fundamental identity $\#G = \#\operatorname{Gal}(L/K) = gf$ where the first equality is class field theory and the second is the fundamental identity. Then

$$\prod_{\chi\in\widehat{G}} \frac{1}{1-\chi(\mathfrak{p})N(\mathfrak{p})^{-s}} = \left[\prod_{\omega_f^f=1} \frac{1}{1-\omega_f N(\mathfrak{p})^{-s}}\right]^g = \prod_{\mathfrak{P}\mid\mathfrak{p}} \frac{1}{1-N(\mathfrak{P})^{-s}}$$

The case of ramified primes can be easily reduced to unramified primes using a maximal unramified subextension of L/K. Therefore, we have

$$\zeta_L(s) = \prod_{\mathfrak{P}} \frac{1}{1-N(\mathfrak{P})^{-s}} = \prod_{\mathfrak{p}}\prod_{\chi\in\widehat{G}} \frac{1}{1-\chi(\mathfrak{p})N(\mathfrak{p})^{-s}} = \prod_{\chi\in\widehat{G}} L(s,\chi)$$

The holomorphic property of $\zeta_L(s)/\zeta_K(s)$ follows immediately from the analytic continuation of $L(s,\chi)$ for χ nontrivial. □

In fact, this theorem is true for the completed Hecke L-functions:

Theorem 3.1.5 (Hecke)**.** *Let L/K be an abelian extension of number fields, and $\widehat{G}$ the Pontryagin dual of the ray class group $G = I_K(\mathfrak{m})/H$ of L/K where H is a congruence subgroup. Then*

$$\zeta_L(s) = \prod_{\chi \in \widehat{G}} \Lambda(s, \chi) = \Lambda(s, 1) \prod_{\chi \neq 1} \Lambda(s, \chi) = \zeta_K(s) \prod_{\chi \neq 1} \Lambda(s, \chi)$$

3.2 Tate's thesis

In this section we will introduce the renowned result of Tate. Tate's 1950 Ph.D. thesis, known as *Tate's thesis* for its significance in the history of mathematics, is regarded as the foundation of adelic analysis. Although idele class groups are perfect improvements of ray class groups in the theory of class fields, adeles had little applications before Tate. However, in his thesis, Tate presented beautiful results related to adeles (which were called "groups of valuation vectors") and Hecke's zeta function. Tate's method (or at least the structure of his argument) was then adapted by many mathematicians when generalizing L-functions (for instance, Hasse-Weil, Jacquet-Langlands, etc). We will follow the unaltered reprint of Tate's thesis [Tat67a] in [FC67] and Bjorn Poonen's notes [Poo15].

3.2.1 A short preparation

Before we start the main theme of this section, here are some crucial preparations. Take G to be a locally compact (and Hausdorff) abelian topological group. Although the objects of interest are locally profinite, being totally disconnected is unnecessary for the general theory. All such groups are unimodular, that is, Haar measures on them both are left and right invariant.

Recall that quasicharacters on G are continuous homomorphisms from G to $\mathbb{C}^\times$, and characters are those onto S^1. We have the Pontryagin dual $\hat{G} = \mathrm{Hom}(G, S^1)$ with the topology generated by $\{\chi : \chi(K) \subseteq U\}$ for every compact K in G and open U in S^1. The Pontryagin dual is also a locally compact abelian group and it is in fact an exact contravariant functor from the category of abelian locally compact groups to itself.

The group G and its Pontryagin double dual $\hat{\hat{G}}$ bear the following duality:

Theorem 3.2.1. *The homomorphism: $\varphi : G \to \hat{\hat{G}}$ defined by*

$$g \mapsto (\chi \to \chi(g))$$

is an isomorphism.

In the case of $G = \mathbb{R}$, whose Pontryagin dual is just $\mathbb{R}$ itself, Fourier transforms of Schwartz functions are functions defined on $\mathbb{R}$. But for general G, the Fourier transform would be defined on the Pontryagin dual.

Definition 3.2.1. Given a locally compact group G and a fixed Haar measure, suppose f is an absolutely integrable complex-valued function on G. Then define the **Fourier transform** of f to be

$$\hat{f}(\chi) = \int_G f(g)\overline{\chi(g)}dg$$

for each $\chi \in \hat{G}$.

Remark 3.2.1. The Fourier transform is well-defined as

$$|\hat{f}(\chi)| \leqslant \int_G |f(g)||\chi(g)|dg = \int_G |f(g)|dg < \infty$$

since f is absolutely integrable. Therefore, $\hat{f}$ is continuous and absolutely integrable.

As usual, the inversion formula for Fourier transforms holds. We quote the theorem directly without proof,

Theorem 3.2.2 (Fourier inversion formula)**.** *Fix G and dg. There exists a unique Haar measure $d\chi$ on $\hat{G}$, the **dual measure** of dg, such that if $f \in L^1(G)$ then*

$$f(g) = \int_{\hat{G}} \hat{f}(\chi)\chi(g)d\chi$$

almost everywhere (except on a set of measure zero). Moreover, if f is continuous, the null set is empty.

Note that this is the same as saying $\hat{\hat{f}} = f(-g)$ due to the fact that $\chi(-g) = \overline{\chi(g)}$ for an additive character χ.

3.2.2 Local Theory

Following Tate we first start from local fields. Not only is the local theory much easier, but it also sets up the base of global cases.

Additive theory

Take a local field K, then as an additive group it's locally compact and abelian. We take the Pontryagin dual of the additive group $\hat{K}$. An **additive character** is a nontrivial element of $\hat{K}$.

Lemma 3.2.1. *Let ψ be an additive character of the local field F. The map $\Psi : K \to \hat{K}$ sending η to*

$$\psi_\eta : \xi \mapsto \psi(\eta\xi)$$

is an isomorphism.

The proof of this lemma is omitted, as it's mostly a topological argument. Note that the lemma strictly relies on the nontriviality of ψ. Therefore, it is necessary to construct a nontrivial character on all local fields.

We consider the following special local fields F. On $F = \mathbb{R}$, we simply define $\psi(x) = e^{-2\pi i x}$; If $F = \mathbb{Q}_p$, let ψ be the map $\mathbb{Q}_p \twoheadrightarrow \mathbb{Q}_p/\mathbb{Z}_p \cong \mathbb{Z}[1/p]/\mathbb{Z} \hookrightarrow S^1$, namely $\psi|_{\mathbb{Z}_p} = 1$ and $\psi(1/p^n) = e^{2\pi i/p^n}$; if $F = \mathbb{F}_p((t))$ let $\psi(\sum a_i t^i) = e^{2\pi i a_{-1}/p}$. Since a local field K is a finite extension of one of the fields above, we may define $\psi_K = \mathrm{tr}_{K/F} \circ \psi_F$.

In what remains, we will focus on the class of Schwartz-Bruhat functions, namely Schwartz functions on archimedean fields and locally constant functions with compact support on nonarchimedean fields.

In a local field K, the **different** of F is defined to be the inverse of the fractional ideal

$$\mathfrak{D}_K^{-1} = \{x \in K : \forall y \in \mathfrak{o}_K, \mathrm{tr}_{K/Q}(xy) \in \mathbb{Z}\}$$

Then clearly $\mathfrak{D}_K = (\pi_K^d)$ for some integer d where π_K is the prime of K.

Take a Schwartz-Bruhat function f, define its Fourier transform as

$$\bar{f}(\eta) = \int_K f(\xi)\psi(\xi\eta)d\xi$$

then

Lemma 3.2.2. *The unique Haar measure that makes $\hat{\hat{f}}(\xi) = f(-\xi)$ (the Fourier inversion formula) hold is*

(i) *If $K = \mathbb{R}$, the usual Lebesgue measure.*

(ii) *If $K = \mathbb{C}$, twice the Lebesgue measure.*

(iii) *If K is nonarchimedean, then the Haar measure such that $\mathfrak{o}_K$ has measure $N(\mathfrak{K})^{-1/2}$.*

Proof. It suffices to evaluate the Fourier transform on some functions to prove this lemma. For K real we can take $f(\xi) = e^{-\pi\xi^2}$, and K complex take $f(\xi) = e^{-2\pi|\xi|}$. When K is nonarchimedean, take $f = 1_{\mathfrak{o}_K}$. □

Remark 3.2.2. Since Schwartz-Bruhat functions are continuous, the Fourier inversion formula holds for all $\xi \in F$, with no exceptions.

Multiplicative theory

Consider the multiplicative group $K^\times$ and its subgroup $U^{(1)}$ of absolute value 1 which is the kernel of the continuous homomorphism $\alpha \to |\alpha|$ on $K^\times$.

In this setting, we are interested in the quasicharacters on $K^\times$. We say a quasicharacter is **unramified** if it's trivial on $U^{(1)}$. Following Tate, we classify the unramified quasicharacters.

Lemma 3.2.3. *Unramified quasicharacters on $K^\times$ are maps of the form $c(\alpha) = |\alpha|^s$ for some complex number s.*

Proof. Here is only a sketch. Quasicharacters are unramified if and only if they factor through the image of $K^\times$ under the absolute value. If K is nonarchimedean, we can choose some s such that $q^s = \chi(q)$ since the image is just $q^{\mathbb{Z}}$ (q is the cardinality of the residue field, as normal). If the image is the positive reals, then every quasicharacter from the image of $K^\times$ (which is isomorphic to $\mathbb{R}$) factor through the exponential map on $\mathbb{C}$. But note that continuous homomorphisms $\mathbb{R} \to \mathbb{C}$ are just left multiplications by some $s \in \mathbb{C}$. This s, after the exponential map, is the desired one. □

With the help of unramified ones, we can classify call quasicharacters on $K^\times$.

Lemma 3.2.4. *Every quasicharacter is of the form $\tilde{c}|\cdot|^s$ for some character $\tilde{c}$ and $s \in \mathbb{C}$.*

Proof. Write $c = \frac{c}{|c|} \cdot |c|$. The factor $\frac{c}{|c|}$ is clearly a character and $|c|$ is unramified since $c|_U$ is a character. □

From this lemma, we see that $|c| = |\cdot|^\sigma$ for $\sigma = \mathrm{Re}(s)$. We call σ the **exponent** of c.

In Tate's original paper, Hecke L-functions were not explicitly discussed. However, being the main theme of this chapter, these L-functions should be presented along the lines.

Example 3.2.1. The ζ-function can be expressed as an Euler product

$$\zeta(s) = \prod_p \frac{1}{1 - p^{-s}}$$

Consider the easy case $K = \mathbb{Q}_p$. Then given the prime element π_K and the unramified character $c = |\cdot|^s$, we have $c(\pi_K) = p^{-s}$.

It is thus natural to define the local factors of L-functions as

Definition 3.2.2. Let K be a local field and c a quasicharacter of $K^\times$ with $s \in \mathbb{C}$.

(i) If K is real, define

$$L(c) = \Gamma_{\mathbb{R}}(s) = \pi^{-s/2}\Gamma\left(\frac{s}{2}\right)$$

(ii) If K is complex, define

$$L(c) = \Gamma_{\mathbb{C}}(s) = \Gamma_{\mathbb{R}}(s)\Gamma_{\mathbb{R}}(s+1)$$

(iii) If K is nonarchimedean, define

$$L(c) = \begin{cases} \frac{1}{1-c(\pi_K)}, & c \text{ unramified} \\ 1, & \text{otherwise} \end{cases}$$

Fix some Haar measure $d\alpha$ of $K^\times$. Take $\mathscr{F}$ to be the family of Schwartz-Bruhat functions f on K such that $f|\cdot|^s$ and $\hat{f}|\cdot|^s$ are absolutely integrable functions on $K^\times$ for all $\sigma > 0$.

Definition 3.2.3. For each $f \in \mathscr{F}$, we define the **local ζ-function** of K to be

$$\zeta(f, c) - \int_{K^\times} f(\alpha)c(\alpha)d\alpha$$

as a function of all quasicharacters.

We say two quasicharacters are equivalent if their quotient is an unramified quasicharacter. Then an equivalence class of quasicharacters consists of those of the form $c = c_0|\cdot|^s$ for some fixed representative c_0 of the class. Thus, we can see an equivalence class of quasicharacters as a Riemann surface. When K is real or complex, the number s is uniquely determined by c and the surface is just $\mathbb{C}$. When K is nonarchimedean, s is determined up to $\frac{2\pi i}{\log N(\mathfrak{p}_K)}\mathbb{Z}$, and thus the Riemann surface is just $\mathbb{C}/\frac{2\pi i}{\log N(\mathfrak{p}_K)}\mathbb{Z}$. Thus when we say the analytic continuations of certain functions on quasicharacters, we actually refer to that of the function separately on the Riemann surface corresponding to each equivalence class of quasicharacters.

Lemma 3.2.5. *The functions $\zeta(f, c)$ and $\zeta(f, c)/L(c)$ are holomorphic for c with a positive component.*

Proof. By absolute convergence, we can exchange the integral and any derivative with respect to s. Then as $\text{Re}(s) > 0$, the derivative of $\zeta(f, c)$ exists. In addition, since L has no zeros, $\zeta(f, c)/L(c)$ is holomorphic. □

In fact,

Lemma 3.2.6 (Meromorphic continuation)**.** *The zeta function $\zeta(f, c)$ extends to all quasicharacters of $K^\times$ meromorphically.*

We then present a stronger version (improved by Deligne, according to Bjorn Poonen's notes [Poo15]) of Tate's result on the meromorphic continuation and functional equation of local zeta functions. The proof is omitted since it's quite lengthy, tedious and irrelevant. For any quasicharacter c, we define $c^\vee$ to be its dual given by $c^\vee(\alpha) = |\alpha|c^{-1}(\alpha)$.

Theorem 3.2.3 (Tate's main theorem, local version)**.** *The followings are true:*

(i) *For each equivalence class, there exists some $f \in \mathscr{F}$ such that $\zeta(f, c)/L(c)$ has no zeros. Moreover, if K is nonarchimedean, then $\zeta(1_{\mathfrak{o}_K}, |\cdot|^s)/L(|\cdot|^s)$ is 1.*

(ii) *Fix a nontrivial character ψ and a Haar measure μ on K for Fourier transforms. There exists a nonvanishing holomorphic function $\varepsilon(c, \psi, \mu)$ such that*

$$\frac{\zeta(\hat{f}, c^\vee)}{L(c^\vee)} = \varepsilon(c, \psi, \mu)\frac{\zeta(f, c)}{L(c)}$$

for all $f \in \mathscr{F}$. If c varies over an equivalence class, then $\varepsilon(c, \psi, \mu) = Ae^{Bs}$ for some $A, B \in \mathbb{C}$.

3.2.3 Global Theory

Let K be a global field. For any place v we denote by K_v its completion at v. Similarly for $\mathfrak{o}_v$, $\mathfrak{p}_v$ and k_v. Let $\mathbb{A}_K$ be the adele ring and I_K the idele group of K. The adelic part of the global theory is extremely elegant. It decomposes analytic properties of Hecke L-functions into local cases, for which we have seen a beautiful functional equation. Conducting analysis on the adeles, Tate was able to replace Hecke's complicated proof of his functional equation for Hecke L-functions.

Setups

The quasicharacters on the adele of a global field can be easily linked to those on the local completions of K.

Lemma 3.2.7. *The map $\psi \mapsto (\psi_v)$ where*

$$\psi_v(\alpha_v) = \psi(1, \dots, \alpha_v, \dots, 1)$$

with inverse $(\psi_v) \mapsto \prod \psi_v$ is an isomorphism

$$\widehat{\mathbb{A}}_K \to \{\prod_v\}'(\hat{K}_v, \mathfrak{o}_v^*)$$

where $\mathfrak{o}_v^*$ is the subgroup of quasicharacters vanishing on $\mathfrak{o}_v$.

For K a number field K, it is easy to choose a standard ψ_v for each K_v and then their product is the standard ψ on K. For a function field K the standard quasicharacter is a little bit more difficult to choose, so I will just assume its existence. Note that the standard quasicharacter is trivial on K (embedded into $\mathbb{A}_K$).

After characters, we now want to construct measures on the adelic ring from measures on the completions of K. This construction is the **Tamagawa measure**. Namely, for the normalized Haar measure μ_v on K_v, we define μ to be the measure on $\mathbb{A}_K$ such that for each basis element $\prod U_v$,

$$\mu\left(\prod U_v\right) = \prod \mu(U_v)$$

The resulting measure has unit volume on $\mathbb{A}_K/K$.

Adelic Fourier analysis

A Schwartz-Bruhat function on $\mathbb{A}$ is a linear combination of functions $\prod f_v$ where each f_v is a Schwartz-Bruhat function that's trivial on $\mathfrak{o}_v$. We can define the Fourier transform of a Schwartz-Bruhat function on $\mathbb{A}$ in the same manner:

$$\hat{f} = \int_{\mathbb{A}} f(x)\psi(xy)dx$$

Lemma 3.2.8. *On compact sets, the sum $\sum_{k \in K} f(x+k)$ converges absolutely and uniformly to a K-periodic function.*

From this we may deduce the Poisson summation formula for K.

Theorem 3.2.4 (Poisson summation formula)**.** *If f is a Schwartz-Bruhat function on $\mathbb{A}_K$. Then*

$$\sum_{k \in K} f(k) = \sum_{k \in K} \hat{f}(k)$$

From this point we will skip a huge chunk of proofs, lemmas and results. They are either too irrelevant to the main theme of this report, or too long/complicated/tedious to reproduce. In this section I do not intend to prove any main result — that would be another project.

Grossencharacters

The protagonist in the story of Hecke L-functions is

Definition 3.2.4. A **Grossencharacter** is a continuous character of I_K that is trivial on $K^\times$ (embedded in I_K), namely, a character of C_K.

As promised in Section 3.1.2, we will show the adelic version of Grossencharacters corresponds to the classical ideal-theoretic ones.

Lemma 3.2.9. *Under Tate's reinterpretation, Grossencharacters are in one-to-one correspondence to those under the classical definition.*

Proof. We will summarize the proof in [Neu99]. But first let us observe a simple result. Given a Grossencharacter χ, the subgroup

$$V = \chi^{-1}(U) \cap \prod_{v \nmid \infty} \mathfrak{o}_v^\times$$

is an open nhds of 1 where $U = \{e^{i\theta} : |\theta| < \pi\}$ is an open subset of S^1. Then the open basis of the adele gives us a finite set S of primes such that V contains an open subset of the form

$$\prod_{v \in S} U_v \times \prod_{v \notin S} \mathfrak{o}_v^\times$$

where U_v is an open set of $\mathfrak{o}_v^\times$. Again by the basis of topology on $\mathfrak{o}_v$, we get one $n_v \geqslant 1$ for each place $v \in S$ such that

$$V \supseteq W = \prod_{v \in S} (1 + \pi_v^{n_v} \mathfrak{o}_v) \times \prod_{v \notin S} \mathfrak{o}_v^\times$$

But then $\chi(W)$ is an open subgroup of U in S^1, which must be trivial. Thus, $W \subseteq \ker \chi$. Therefore, the restriction of χ at some place v is unramified (i.e., trivial on $\mathfrak{o}_v^\times$) for all but finitely many nonarchimedean v.

Let $\mathfrak{m} = \prod_v \mathfrak{p}_v^{n_v}$ be an ideal of K with no infinite primes with n_v defined in the previous paragraph. Define $\bar{I}_K^{\mathfrak{m}}$ to be the product of

$$I_f^{\mathfrak{m}} = \prod_{v \nmid \infty} U_v^{(n_v)}, \quad I_\infty = \prod_{v \mid \infty} K_v^\times$$

We say $\mathfrak{m}$ is a modulus of χ if $\chi(I_f^{\mathfrak{m}}) = 1$. Let $C_K(\mathfrak{m}) = I_K / I_f^{\mathfrak{m}} K^\times$, then χ induces a character of $C_K(\mathfrak{m})$. From now we denote by $\mathfrak{m}$ the modulus of χ.

For each finite prime v of K, fix a prime element π_v of K_v. We may define a homomorphism

$$c : I_K(\mathfrak{m}) \to C_K(\mathfrak{m}), \quad \mathfrak{p}_v \mapsto (..., 1, 1, \pi_v, 1, 1, ...)$$

Take the composition $\chi \circ c$, we get a classical Grossencharacter. In fact, this relation is a one-to-one correspondence.

To wit this, we will use the following exact sequence without proof.

Lemma 3.2.10. *We have a short exact sequence*

$$1 \to K^{\mathfrak{m}} / \mathfrak{o}_K^{\mathfrak{m}} \xrightarrow{\delta} I_K(\mathfrak{m}) \times (\mathfrak{o}_K / \mathfrak{m})^\times \times K^\infty \to C_K(\mathfrak{m}) \to 1$$

where δ sends a to $((a)^{-1}, a, a)$.

Then the characters of $C_K(\mathfrak{m})$ corresponds to the characters of $I_K(\mathfrak{m}) \times (\mathfrak{o}_K/\mathfrak{m})^\times \times K^\infty$ that vanish on the image of δ, which precisely correspond to the classical Grossencharacters: χ, χ_f and χ_∞ such that

$$\chi((a)^{-1})\chi_f(a)\chi_\infty(a) = 1$$

□

Example 3.2.2. Let K be the field of rationals, and χ a Dirichlet character. Recall the idele of $\mathbb{Q}$ is

$$I_\mathbb{Q} = \mathbb{Q}^\times \times \mathbb{R}^\times_{>0} \times \hat{\mathbb{Z}}^\times$$

and since the Prüfer ring $\hat{\mathbb{Z}} = \varprojlim \mathbb{Z}/n\mathbb{Z}$, we have the composition

$$I_\mathbb{Q} \twoheadrightarrow \hat{\mathbb{Z}}^\times \twoheadrightarrow (\mathbb{Z}/n\mathbb{Z})^\times \xrightarrow{\chi} \mathbb{C}^\times$$

which is a Grossencharacter of $\mathbb{Q}$. Indeed every Grossencharacter of finite order is such a composition.

Example 3.2.3. When $K = \mathbb{Q}(i)$. Then $\mathbb{Z}[i]$ is a PID. In particular, the unique prime ideal lying above 2 is $(1+i)$. Note that in any other prime ideal, there is a unique generator π such that $\pi \equiv 1 \pmod{(1+i)^3}$. Then

$$\chi : (\pi) \to \frac{\pi}{\sqrt{N(\pi)}}$$

defines a Grossencharacter of modulus (in fact, of conductor) $(1+i)^3$.

Example 3.2.4. In class field theory we've shown (Theorem 2.2.12) that there is a canonical map $\tilde{r}_K : C_K \to \mathrm{Gal}(K^{\mathsf{ab}}/K)$ where K^{ab} is the maximal abelian extension of K. Any continuous quasicharacter on the absolute Galois group of K factors through $\mathrm{Gal}(K^{\mathsf{ab}}/K)$. It therefore induces a map by composing $\rho : \mathrm{Gal}(K^{\mathsf{ab}}/K) \to \mathbb{C}^\times$ with $I_K \twoheadrightarrow C_K \xrightarrow{r_K} \mathrm{Gal}(K^{\mathsf{ab}}/K)$.

Note that r_K is not an isomorphism, and therefore not all Grossencharacters of K arise from the continuous quasicharacters of the absolute Galois group. However, if we use continuous quasicharacters on the *Weil group* W_K of K, then all Grossencharacters could be found in the way above.

Global ζ-functions

Definition 3.2.5. Given a Schwartz-Bruhat f, we may define the **global ζ-function** of K by

$$\zeta(f, \chi) = \int_{I_K} f(x)\chi(x)dx$$

It is a pity that, due to length, time and relevance, I have to omit the proof of the most important theorem in Tate's thesis. However, I am confident that it is a pleasure for the readers to simply admire the results, even if one does not understand its true nature.

Theorem 3.2.5 (Tate's main theorem, global version)**.** *Given an $f \in \mathscr{A}$,*

(i) *The function $\zeta(f, \chi)$ converges for Grossencharacters of exponents larger than* 1*.*

(ii) *The function extends meromorphically to all Grossencharacters, with simple poles at $|\cdot|^0$ and $|\cdot|^1$.*

(iii) *As meromorphic functions of χ,*

$$\zeta(f, \chi) = \zeta(\hat{f}, \chi^\vee)$$

3.2.4 Hecke L-functions, again

We have finally arrived (by skipping a lot of things) at one of the main characters of this chapter.

Definition 3.2.6. Define the global ε- and L-factors as $\varepsilon(\chi) = \prod_v \varepsilon(\chi_v)$ and $L(\chi) = \prod_v L(\chi_v)$.

Remark 3.2.3. In the definition of the ε-factor we are implicitly using a standard quasicharacter and the Tamagawa measure.

Theorem 3.2.6. *The followings are true:*

(i) *The ε-factor is a nonvanishing holomorphic function.*

(ii) *The L-factor is holomorphic for Grossencharacters of exponents larger than* 1*, and extends to a meromorphic function on all Grossencharacters.*

(iii) *As meromorphic functions,*

$$L(\chi) = \varepsilon(\chi)L(\chi^\vee)$$

Proof. The first two statements are just consequences of the local statements and the factors equal to one for all but finitely many places.

Now from the functional equation of the local ζ-function

$$\frac{\zeta(\hat{f}_v, \chi_v^\vee)}{L(\chi_v^\vee)} = \varepsilon(\chi_v)\frac{\zeta(f_v, \chi_v)}{L(\chi_v)}$$

Let $f = \prod_v f_v$. Then we have

$$\frac{\zeta(\hat{f}, \chi^\vee)}{L(\chi^\vee)} = \varepsilon(\chi)\frac{\zeta(f, \chi)}{L(\chi)}$$

and dividing both sides by the global functional equation in Theorem 3.2.5, we get

$$L(\chi) = \varepsilon(\chi)L(\chi^\vee)$$

which completes the proof. □

The **Hecke L-function**, under this interpretation, is therefore

$$L(s, \chi) = L(\chi|\cdot|^s), \quad \varepsilon(s, \chi) = \varepsilon(\chi|\cdot|^s)$$

and thus

$$L(s, \chi) = \varepsilon(s, \chi)L(1 - s, \chi^{-1})$$

3.3 Artin L-functions

3.3.1 Nonabelian L-functions

In this section I will talk briefly about Artin L-functions. Class field theory was partly solved before Emil Artin by Kronecker, Hilbert and Takagi. Using the ray class group, Takagi successfully described the Galois group of abelian extensions of number fields. He also raised the question of nonabelian extensions. Weber and Hecke proved a decomposition of Dedekind zeta functions on abelian extensions into a product of Hecke L-functions of nontrivial characters of the abelian class group of L/K. Emil Artin was trying to generalize this result to nonabelian extensions. In this case he could no longer rely on the L-functions of abelian characters. Thus, in [Art24], he made the following definition.

Definition 3.3.1. Say L/K is a (possibly nonabelian) Galois extension of the number field K and ρ a continuous representation of $\mathrm{Gal}(L/K)$. The **Artin L-function** is defined to be

$$L(s,\rho) = \prod_{\mathfrak{p}} \frac{1}{\det\left[\mathrm{id} - N(\mathfrak{p})^{-s}\rho\left(\sigma_{\mathfrak{P}|\mathfrak{p}}\right)\right]}$$

where $\mathfrak{p}$ varies over the unramified primes of K, $\mathfrak{P}$ any prime of L lying over $\mathfrak{p}$ and $\sigma_{\mathfrak{P}|\mathfrak{p}}$ the Frobenius element.

Remark 3.3.1. The motivation for this definition can be roughly summarized in the following paragraph. let χ be a Grossencharacter. We may thus consider the Hecke L-function

$$L(s,\chi) = \prod_{\mathfrak{p}} \frac{1}{1-\chi(\mathfrak{p})N(\mathfrak{p})^{-s}}.$$

Taking the logarithm of one local L-factor we get

$$\log L_{\mathfrak{p}}(s,\chi) = -\sum_{l=1}^{\infty} \frac{\chi(\mathfrak{p})^l}{lN(\mathfrak{p})^{ls}} = -\sum_{l=1}^{\infty} \frac{\chi(\mathfrak{p}^l)}{lN(\mathfrak{p})^{ls}}$$

The last equality is quite important since we will later work with characters of representations, which are not homomorphisms. Now given a representation ρ of the Galois extension L/K, the character attached to it is denoted by χ_ρ. Then we may take its value on the Frobenius element $\sigma_{\mathfrak{P}|\mathfrak{p}}$ corresponding to $\mathfrak{p}$ for primes $\mathfrak{p}$ with trivial inertia subgroups. In this case it is natural to define, mimicking Hecke L-functions,

$$\log L_{\mathfrak{p}}(s,\chi) = -\sum_{l=1}^{\infty} \frac{\chi_\rho(\sigma_{\mathfrak{P}|\mathfrak{p}}^l)}{lN(\mathfrak{p})^{ls}}$$

But note that $\operatorname{tr}\log X = \log\det X$ for all matrices X and the trace of a representation defines its character, we have

$$L_{\mathfrak{p}}(s,\chi) = \frac{1}{\det\left[\mathrm{id} - N(\mathfrak{p})^{-s}\rho\left(\sigma_{\mathfrak{P}|\mathfrak{p}}\right)\right]}$$

which leads to Artin's elegant definition.

Indeed, Weber's theorem on Dedekind's zeta function Theorem 3.1.4

$$\zeta_L(s) = \prod_{\chi\in\widehat{G}} L(s,\chi)$$

resembles some core properties of the regular representation $(\rho_{\mathrm{reg}}, \mathbb{C}[G])$ of G:

$$\rho = \bigoplus_{V_i\in\mathrm{Irr}(G)} V_i^{\dim V_i}$$

Then if the π sign of L-functions corresponds to the $\oplus$ sign of representations. We should expect the following:

Lemma 3.3.1. *If ρ_1 and ρ_2 are two representations of* $\mathrm{Gal}(L/K)$. *Then*

$$L(s,\rho_1\oplus\rho_2) = L(s,\rho_1)L(s,\rho_2)$$

In particular,

$$L(s,\rho_{reg}) = \prod_{\rho\in\widehat{G}} L(s,\rho)^{\dim\rho}.$$

Proof. This is quite obvious from Remark 3.3.1. Indeed, $\chi_1 + \chi_2$ is the character of $\rho_1 + \rho_2$ where χ_i is the character of ρ_i. Then

$$\log L_{\mathfrak{p}}(s, \chi_1 + \chi_2) = -\sum_{l=1}^{\infty} \frac{(\chi_1 + \chi_2)(\sigma_{\mathfrak{P}|\mathfrak{p}}^l)}{lN(\mathfrak{p})^{ls}} = -\sum_{l=1}^{\infty} \frac{\chi_1(\sigma_{\mathfrak{P}|\mathfrak{p}}^l)}{lN(\mathfrak{p})^{ls}} - \sum_{l=1}^{\infty} \frac{\chi_2(\sigma_{\mathfrak{P}|\mathfrak{p}}^l)}{lN(\mathfrak{p})^{ls}}$$

which after exponential becomes $L_{\mathfrak{p}}(s, \chi_1)L_{\mathfrak{p}}(s, \chi_2)$, completing the proof. □

Now for the Hecke L-function, we have $L(s, 1) = \zeta_L(s)$. For Artin L-function this also holds. If the trivial representation of $\mathrm{Gal}(L/K)$ is ρ_{triv}, then we should have $L(s, \rho_{\mathrm{triv}}) = \zeta_K(s)$ as in Weber's decomposition. But $\zeta_K(s)$ is in fact the L-series of the trivial representation of $\mathrm{Gal}(K/K)$. We actually have something a lot more powerful than this small observation.

Lemma 3.3.2. *If H is a normal subgroup of* $\mathrm{Gal}(L/K)$*, let M be the fixed field of H, ρ a representation of* $\mathrm{Gal}(M/K)$*, then*

$$L(s, \rho) = L(s, \tilde{\rho})$$

where $\tilde{\rho}$ is the canonical extension of ρ to $\mathrm{Gal}(L/K)$ *with kernel H.*

Proof. Fix a prime $\mathfrak{p}$ of K. Say $\mathfrak{P}'$ is a prime of M above $\mathfrak{p}$, and $\mathfrak{P}$ a prime above $\mathfrak{p}$ in L. Then $\sigma_{\mathfrak{P}|\mathfrak{p}}$ restricted to M is just $\sigma_{\mathfrak{P}'|\mathfrak{p}}$ by its uniqueness. Therefore, $\rho(\sigma_{\mathfrak{P}'|\mathfrak{p}}) = \tilde{\rho}(\sigma_{\mathfrak{P}|\mathfrak{p}})$. □

The previous two lemmas combine to

$$L(s, \rho_{\mathrm{reg}}) = \zeta_K(s) \prod_{\rho \neq \rho_{\mathrm{triv}}} L(s, \rho)^{\dim \rho},$$

so we want

$$L(s, \rho_{\mathrm{reg}}) = \zeta_L(s) = L(s, \rho'_{\mathrm{triv}})$$

for the trivial representation ρ'_{triv} of $\mathrm{Gal}(L/L)$. Note that in representation theory, we have $(\mathbb{C}[G], \rho_{\mathrm{reg}}) = \mathrm{Ind}_1^G(\rho_{\mathrm{triv}})$, so still Artin proved a stronger relation on the L-functions:

Lemma 3.3.3. *Let $L/M/K$ be number fields with* $\mathrm{Gal}(L/K) = G$ *and* $\mathrm{Gal}(L/M) = H$*. Then if ρ is a representation of H, we have*

$$L(s, \rho) = L(s, \mathrm{Ind}_H^G \rho)$$

Proof. We follow the proof in [Neu99]. Fix a prime $\mathfrak{p}$ of K. Let $\mathfrak{q}_1, \ldots, q_r$ be the full list of primes in M above $\mathfrak{p}$ and $\mathfrak{P}_1, \ldots, \mathfrak{P}_r$ a list of primes in L above $\mathfrak{q}_i$. Let D_i and I_i be the decomposition and inertia groups of $\mathfrak{P}_i$ over $\mathfrak{p}$. Then $H_i = D_i \cap H$ and $I_i' = I_i \cap H$ are the decomposition and inertia groups of $\mathfrak{q}_i$ over $\mathfrak{p}$. The inertia degree of $\mathfrak{q}_i$ over $\mathfrak{p}$ is simply $f_i = \#H_i/I_i' = \#D_i/H_iI_i$, which means we have $N(\mathfrak{q}_i) = N(\mathfrak{p})_i^f$.

Since G acts on primes above $\mathfrak{p}$ transitively, we may select τ_i such that $\mathfrak{P}_i = \tau_i\mathfrak{P}_1$. Let $\varphi \in D_1$ be the Frobenius element of $\mathfrak{P}_1|\mathfrak{p}$, then $\varphi_i = \tau_i^{-1}\varphi\tau_i$ is the Frobenius element $\mathfrak{P}_i|\mathfrak{p}$ and $\varphi_i^{f_i}$ are the Frobenius elements for $\mathfrak{P}_i|\mathfrak{q}_i$.

Let ρ be a representation of H. In this case

$$L_{\mathfrak{p}}(s, \mathrm{Ind}_H^G \rho) = \frac{1}{\det[\mathrm{id} - \mathrm{Ind}_H^G \rho(\varphi)N(\mathfrak{p})^{-s}]} = L_{\mathfrak{p}}(s, \mathrm{Res}_{D_1}^G \mathrm{Ind}_H^G \rho)$$

as $\varphi \in D_1$. By Mackey's theorem,

$$\mathrm{Res}_{D_1}^G \mathrm{Ind}_H^G \rho = \bigoplus_{\tau} \mathrm{Ind}_{D_1 \cap \tau H \tau^{-1}}^{D_1} \rho_\tau$$

where $\rho_\tau(g) = \rho(\tau^{-1}g\tau)$. Then by Lemma 3.3.1,

$$L_\mathfrak{p}(s, \operatorname{Ind}_H^G \rho) = L_\mathfrak{p}(s, \operatorname{Res}_{D_1}^G \operatorname{Ind}_H^G \rho) = \prod_{i=1}^r \frac{1}{\det\left[\mathrm{id} - \operatorname{Ind}_{D_1 \cap \tau H \tau^{-1}}^{D_1} \rho(\varphi) N(\mathfrak{p})^{-s}\right]}$$

We may apply a conjugation by τ_i to the determinant, and get

$$L_\mathfrak{p}(s, \operatorname{Ind}_H^G \rho) = \prod \frac{1}{\det\left[\mathrm{id} - \operatorname{Ind}_{H_i}^{D_i} \rho(\varphi_i) N(\mathfrak{p})^{-s}\right]}$$

Since φ_i generates D_i, the induced representation is

$$\operatorname{Ind}_{H_i}^{D_i} \rho = \rho \oplus \varphi_i \rho \oplus \cdots \oplus \varphi_i^{f_i - 1} \rho$$

Then the matrix of $\rho(\varphi_i)$ with respect to this basis is

$$\begin{bmatrix} 0 & E & \cdots & 0 \\ & & & \\ 0 & 0 & \cdots & E \\ A & 0 & \cdots & 0 \end{bmatrix}$$

w here A is the matrix of $\varphi_i^{f_i}$ with respect to a basis of ρ and E the identity matrix. Therefore

$$\det \begin{bmatrix} E & -N(\mathfrak{p})^{-s}E & \cdots & 0 \\ & & & \\ 0 & 0 & \cdots & -N(\mathfrak{p})^{-s}E \\ A & 0 & \cdots & E \end{bmatrix}^{-1} = \det\left[\mathrm{id} - \rho(\varphi_i^{f_i}) N(\mathfrak{p})^{-f_i s}\right]^{-1}$$

whose product is precisely $L_\mathfrak{p}(s, \rho)$. □

Summarizing what we have shown:

Theorem 3.3.1 (Artin L-functions). *Let L/K be two number fields, ρ, ρ' two representations of the Galois group. Then the Artin L-function $L(s, \rho)$ converges for all* $\mathrm{Re}(s) > 1$. *Furthermore,*

(i) $L(s, \rho \oplus \rho') = L(s, \rho) L(s, \rho')$

(ii) *If H is a normal subgroup of G, then*

$$L(s, \rho) = L(s, \rho|_H)$$

(iii) *If H is a subgroup of G,and ρ a representation of H then*

$$L(s, \rho) = L(s, \operatorname{Ind}_H^G \rho)$$

In particular, the Dedekind zeta functions of L and K satisfy the relation

$$\zeta_L(s) = \zeta_K(s) \prod_{\rho \neq \rho_{triv}} L(s, \rho).$$

Theorem 3.3.2 (functional equation of Artin L-functions). *Define the completed Artin L-functions:*

$$\Lambda(s, \rho) = c(\rho)^{s/2} \prod_\mathfrak{p} L_\mathfrak{p}(s, \rho)$$

where c is a factor analogous to that in the completed Hecke L-functions. Then

$$\Lambda(s, \rho) = \varepsilon(s, \rho) \Lambda(1 - s, \rho^*)$$

I won't bother with the factor c and ε in this theorem, as they are not the theme of my report.

3.3.2 The reciprocity law: an overture

We have witnessed that (1) characters of the Galois group define Artin L-functions, and Grossencharacters of the ray class groups define Hecke L-functions, (2) they all help decompose Dedekind zeta functions and (3) the two L-functions satisfy the same functional equation. So one might wonder: is there a one-to-one correspondence

$$\Phi : \{\chi_\rho : \mathrm{Gal}(L/K) \to \mathbb{C}^\times = GL_1(\mathbb{C})\} \to \{\chi : C_K \to \mathbb{C}^\times\}$$

such that $L(s, \chi_\rho) = L(s, \Phi(\chi_\rho))$? The answer is: no but yes. Although class field theory, namely the (abelian) Artin reciprocity law: Theorem 2.2.12, gives us a map $C_K \to \mathrm{Gal}(L/K)$, but this map is not bijective. Indeed, via this map every character of the Galois group induces a Grossencharacter, but the converse is not true. However, all Grossencharacters of finite order can be acquired in this way. Indeed, every finite order Grossencharacter factors through $C_K/N_{L/K}C_L$ for some finite abelian extension L/K, so we have a correspondence:

$$\Phi : \{\chi_\rho : \mathrm{Gal}(L/K) \to GL_1(\mathbb{C})\} \to \{\chi : C_K/N \to S^1\}$$

The characters of $\mathrm{Gal}(L/K)$ are one dimensional Galois representations, where a Galois representation is defined by

Definition 3.3.2. A **Galois representation** is a continuous representation of $\mathrm{Gal}(\bar{K}/K) \to GL_n(\mathbb{C})$.

Indeed, if a Galois representation is one dimensional, then its image is abelian, meaning it factors through the abelianization $\mathrm{Gal}(\bar{K}/K)^{\mathsf{ab}} = \mathrm{Gal}(K^{\mathsf{ab}}/K)$. Moreover, it has finite image and thus factors through the Galois group of some finite abelian extension L/K. In particular, one concludes a correspondence equivalent to the abelian class field theory:

$$\{\text{1-dimensional Galois representations}\} \longleftrightarrow \{\text{Grossencharacters of finite orders}\}$$

But what will happen in higher dimensions? Even if a similar correspondence exists for higher dimensions, we don't know what to put on the right side! It is true that $C_K = GL_1(K)\backslash GL_1(\mathbb{A}_K)$ can be replaced by $GL_n(K)\backslash GL_n(\mathbb{A}_K)$, but we still need something to fill in the blank:

$$\{n\text{-dimensional Galois representations}\} \longleftrightarrow \{\text{??? representations of } GL_n(K)\backslash GL_n(\mathbb{A}_K)\}$$

Note that $GL_n(K)\backslash GL_n(\mathbb{A}_K)$ is not even a group, so we should expect the things on the RHS to be sophisticated! The case of $n = 2$ and $K = \mathbb{Q}$ will be lightly touched in the next two chapters.

Chapter 4

Modular Forms

4.1 Basic Theory

The study of modular forms dated back to Gauss (as well as most things in mathematics). But the objects were pretty analytic at that time. It was later during the study of new problems that modular forms gradually associated with geometry, number theory and ultimately became a significant part of modern mathematics. The most notable of them is probably the proof of Fermat's last theorem, or more generally Fermat's last theorem. The main references for this chapter are [DS05] and [Bum04].

4.1.1 The modular group

The modular group refers to $SL_2(\mathbb{Z})$, generated by the matrices

$$S = \begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix}, T = \begin{bmatrix} 0 & -1 \\ 1 & 0 \end{bmatrix}$$

The modular group naturally acts on the upper half plane $\mathbb{H} = \{\tau \in \mathbb{C} : \operatorname{Im}(\tau) > 0\}$ via the Möbius transformation:

$$\gamma = \begin{bmatrix} a & b \\ c & d \end{bmatrix} : z \mapsto \frac{az+b}{cz+d}.$$

Indeed, $\operatorname{Im}(\gamma(z)) = |cz+d|^{-2} \operatorname{Im}(z)$. It can also be checked as an easy exercise that $\gamma_1(\gamma_1\gamma_2)(z) = \gamma_1(\gamma_2(z))$ which confirms the group action. We further define the subgroups

$$\Gamma(N) = \{\gamma \in SL_2(\mathbb{Z}) : \gamma \equiv I \pmod N\}$$

which are precisely the kernel of $SL_2(\mathbb{Z}) \to SL_2(\mathbb{Z}/n\mathbb{Z})$.

Definition 4.1.1. A **congruence subgroup of level** N is a subgroup of $\Gamma(1)$ containing some $\Gamma(N)$.

The action of $\Gamma(1)$ on $\mathbb{H}$ is relatively simple:

Lemma 4.1.1. *The group action of* $\Gamma(1)$ *on* $\mathbb{H}$ *is discontinuous.*

Proof. Tedious. □

Definition 4.1.2. A **fundamental domain** of a subgroup Γ of $SL_2(\mathbb{R})$ acting discontinuously on $\mathbb{H}$ is an open subset $D \subseteq \mathbb{H}$ such that for every $z \in \mathbb{H}$, there is some $\gamma \in \Gamma$ such that $\gamma(z) \in \bar{D}$ and for any $z_1, z_2 \in D$, $\gamma(z_1) = z_2$ if and only if $\gamma = \pm I$.

Lemma 4.1.2. *The open set* $D = \{z \in \mathbb{H} : |\operatorname{Re}(z)| < 1/2, |z| > 1\}$ *is a fundamental domain of the modular group.*

Proof. Still quite tedious. Use the generators S and T. □

If we put $\mathbb{H}$ inside the Riemann sphere $\hat{\mathbb{C}}$, the boundary of $\mathbb{H}$ would be $\mathbb{R} \cup \{\infty\}$. The modular group $SL_2(\mathbb{Z})$ acts transitively on the set $\mathbb{Q} \cup \{\infty\}$ and therefore a subgroup of finite index in $\Gamma(1)$ acts on $\mathbb{Q} \cup \{\infty\}$ with finite orbits. Let Γ be a congruence subgroup of level N. Since $SL_2(\mathbb{Z})/\Gamma(N) = SL_2(\mathbb{Z}/n\mathbb{Z})$, the congruence subgroup has finite index.

Definition 4.1.3. The **cusps** of the congruence subgroup Γ are the orbits of Γ in $\mathbb{Q} \cup \{\infty\}$.

On the space $\mathbb{H}^* = \mathbb{H} \cup \mathbb{Q} \cup \{\infty\}$, we define a special topology. On $\mathbb{H}$, we impose the standard topology. For ∞, we let the open nhds be $\{z \in \mathbb{H} : \mathrm{Im}(z) > C\} \cup \{\infty\}$ for nonnegative real C. For $r \in \mathbb{Q}$, we define the nhds $\{r\} \cup U$ where U is the interior of a disk in $\mathbb{H}$ tangent to $\mathbb{R}$ at r.

We then want to make $\Gamma\backslash\mathbb{H}^*$ into a complex manifold. Around $z \in \Gamma\backslash\mathbb{H}$, a standard chart of $\mathbb{H}$ would work if z is not stabilized by a nontrivial subgroup of $\Gamma/\{\pm I\}$. The exceptions are called **elliptic points**. Apply the transform $\tau \mapsto \frac{\tau - z}{\tau - \bar{z}}$ which maps $\mathbb{H}$ to the unit disk. The stabilizer of z then becomes the group of rotations by $2\pi/n$ where n is the order of the stabilizer. Then $\tau \mapsto w^n$ where w is the standard coordinate on the disk maps a nhds of a in $\Gamma\backslash\mathbb{H}^*$ to a nhds of the origin in the unit disk, and thus provides a complex chart. If $z \in \mathbb{Q} \cup \{\infty\}$ let ρ be the matrix sending z to ∞. Then $\rho\Gamma\rho^{-1}$ is a subgroup of finite index in $\Gamma(1)$ and the stabilizer of ∞ is $\rho\Gamma_z\rho^{-1}$, and thus it is an infinite cyclic subgroup generated by T^n for some n. Thus, $\tau \mapsto e^{2\pi i\rho(\tau)/n}$ gives us a chart around the origin which can be taken to z. The quotient $\Gamma\backslash\mathbb{H}^*$ has thus been made into a compact Riemann surface.

4.1.2 Modular forms

Definition 4.1.4. A **modular form of weight** k is a holomorphic function $f : \mathbb{H} \to \mathbb{C}$ such that

$$f\left(\frac{az+b}{cz+d}\right) = (cz+d)^k f(z)$$

and f is holomorphic at the cusp ∞, meaning if we define $g(e^{2\pi iz}) = f(z)$ then g can be extended analytically to 0.

Proof. Indeed, the definition of f allows us to write f in its Fourier expansion:

$$f(z) = \sum_{n=-\infty}^{\infty} a_n q^n, \quad q = e^{2\pi iz}$$

and the condition on g is equivalent to $a_n = 0$ for all $n < 0$. □

Definition 4.1.5. A modular form f is **cuspidal** or a **cusp form** if $a_0 = 0$ in its Fourier expansion.

Denote by $\mathcal{M}_k(\Gamma(1))$ the space of modular forms of weight k. Denote by $\mathcal{S}_k(\Gamma(1))$ the subspace of cusp forms. Let $\mathcal{M}(\Gamma(1))$ be the direct sum of $\mathcal{M}_k(\Gamma(1))$ for $k \in \mathbb{Z}$. Then $\mathcal{M}(\Gamma(1))$ has a ring structure and a natural grading since if f has weight k and f' has weight l then ff' has weight $k + l$.

Lemma 4.1.3. *The space $\mathcal{M}_k(\Gamma(1))$ is finite dimensional.*

Proof. If f_0 is a nontrivial modular form of weight k. Let $X = \Gamma(1)\backslash\mathbb{H}^*$. Let $p_1, \ldots, p_m$ the zeros of f_0 with orders $r_1, \ldots, r_m$. Then $f \mapsto f/f_0$ is an isomorphism of $\mathcal{M}_k(\Gamma(1))$ to the space of automorphic functions with poles $p_1, \ldots, p_m$ of order $r_1, \ldots, r_m$. Then a theorem in complex analysis suggests $\mathcal{M}_k(\Gamma(1))$ has at most dimension $\sum r_i + 1$. □

Definition 4.1.6. The **Eisenstein series of weight** k for an even integer $k > 2$ is

$$G_k(z) = \sum_{(c,d)\neq(0,0)} \frac{1}{(cz+d)^k}.$$

The **normalized Eisenstein series** $G_k(z)/(2\zeta(k))$ is denoted by $E_k(z)$.

Since

$$\frac{1}{z} + \sum_{d=1}^{\infty}\left(\frac{1}{z-d} + \frac{1}{z+d}\right) = \pi i - 2\pi i \sum_{m=0}^{\infty} q^m$$

which after $k-1$ times of differentiation gives

$$\sum_{d\in\mathbb{Z}} \frac{1}{(z+d)^k} = \frac{(-2\pi i)^k}{(k-1)!}\sum_{m=1}^{\infty} m^{k-1}q^m$$

Therefore, we have

$$G_k(z) = 2\zeta(k) + 2\frac{(2\pi i)^k}{(k-1)!}\sum_{n=1}^{\infty}\sigma_{k-1}(n)q^n$$

where $\sigma_{k-1}(n) = \sum_{m|n} m^{k-1}$.

If there exists a noncuspidal form f of weight k, then we subtract a constant multiple of f from each modular form of weight k to get a cusp form of weight k. Therefore, $\dim \mathcal{M}_k(\Gamma(1)) = \dim \mathcal{S}_k(\Gamma(1)) + 1$ for even $k > 2$ by the existence of Eisenstein series. It remains to construct some cusp forms. The **discriminant function** $\Delta(z) = (g_2(z))^3 - 27(g_3(z))^2$ for $g_2 = 60G_4$ and $g_3 = 140G_6$ is an example. It is cuspidal of weight 12 ($a_0 = 0$, $a_1 = (2\pi)^{12}$). We can also define

Definition 4.1.7. The j**-invariant** $j : \mathbb{H} \to \mathbb{C}$ is given by $1728\frac{(g_2(z))^3}{\Delta(z)}$.

which is a modular function with a simple pole at infinity.

Lemma 4.1.4. *The space $\mathcal{S}_{12}(\Gamma(1))$ is one dimensional.*

Proof. If f is a cusp form of weight 12, then f/Δ is an automorphic function with no poles in $\mathbb{H}$ and further at ∞ since Δ has a first-order zero at ∞. Thus, f/Δ is constant. □

4.1.3 L-functions attached to modular forms

Petersson inner product

Say f and g are two cuspidal forms of weight k. Then the map $z = x + yi \mapsto f(z)\overline{g(z)}y^k$ is invariant under $\Gamma(1)$ since $\gamma(y)^k = |cz+d|^{-2k}y^k$.

Lemma 4.1.5. *The measure $|y|^{-2}dxdy$ is invariant under the left action of $SL_2(\mathbb{R})$*

Proof. The Bruhat decomposition of $SL_2(\mathbb{R})$ can be stated as follows. If B is the Borel subgroup consisting of upper triangular matrices, and S one of the generators of $SL_2(\mathbb{Z})$, then

$$SL_2(\mathbb{R}) = B \sqcup BSB$$

meaning $SL_2(\mathbb{R})$ is generated by

$$A = \begin{bmatrix} a & 0 \\ 0 & a^{-1} \end{bmatrix}, \quad B = \begin{bmatrix} 1 & b \\ 0 & 1 \end{bmatrix}, \quad S$$

Then $Az = a^2 z$, $Bz = z + b$ and $Sz = -z^{-1}$. In particular, $\text{Re}(Az)$, $\text{Im}(Az)$ are multiplication by a^2; $\text{Re}(Bz) = x+b$, $\text{Im}(Bz) = y$; and $\text{Re}(Sz) = \frac{-x}{x^2+y^2}$, $\text{Im}(Sz) = \frac{y}{x^2+y^2}$. Clearly the measure $|y|^{-2}dxdy$ is invariant under the actions of A, B. For S, we have

$$|Sy|^{-2}d(Sx)d(Sy) = \frac{(x^2+y^2)^2}{|y|^2}\left[\frac{(x^2-y^2)^2}{(x^2+y^2)^4} + \frac{4x^2y^2}{(x^2+y^2)^4}\right]dxdy = |y|^{-2}dxdy$$

which completes the proof. □

Remark 4.1.1. The groups we are studying are in fact discontinuous subgroups of $GL_2(\mathbb{R})_+$ such that $\Gamma\backslash\mathbb{H}$ has finite volume with respect to the measure $|y|^{-2}dxdy$. We say a nontrivial element γ of the matrix group is **parabolic** if the absolute value of its trace is 2. The cusps of such a group Γ can be defined as points a in $\mathbb{R} \cup \{\infty\}$ for which there is a parabolic $\gamma \in \Gamma$ such that $\gamma(a) = a$ and the orbits of those points.

Using the previous lemma, one can define

Definition 4.1.8. The **Petersson inner product** is the natural inner product on $\mathcal{S}_k(\Gamma(1))$ given by

$$(f, g) = \int_{\Gamma(1)\backslash\mathbb{H}} f(z)\overline{g(z)}y^k \frac{dxdy}{y^2}$$

The inner product is well-defined. Furthermore, since $f(z)$ decays rapidly when $y \to \infty$ as it's cuspidal, the integral converges near the cusp ∞. It is easy to see the inner product is positive definite from its definition, and Hermitian from the conjugation.

L-functions

Definition 4.1.9. Given a modular form f of weight k, then one can define **the L-function attached to f** by

$$L(s, f) = \sum_{n=1}^{\infty} \frac{a_n}{n^s}$$

where a_n are the Fourier coefficients of f.

Here is a well-known lemma on the bound of the Fourier coefficients of f:

Lemma 4.1.6. *If f is a cups form, its Fourier coefficients are bounded by $Cn^{k/2}$ for some constant C.*

Theorem 4.1.1 (functional equation of L-functions attached to modular forms)**.** *The L-function has meromorphic continuation to all s. Let the completed L-function attached to f be*

$$\Lambda(s, f) = (2\pi)^{-s}\Gamma(s)L(s, f)$$

then Λ has an analytic continuation if f is cuspidal; otherwise it has simple poles at $s = 0$ and $s = k$. Moreover,

$$\Lambda(s, f) = (-1)^{k/2}\Lambda(k - s, f)$$

Proof. If f is cuspidal, $f(iy) \to 0$ for $y \to \infty$. Because

$$f(i/y) = f(S(iy)) = (-1)^{k/2}y^{-k}f(iy),$$

$f(iy)$ approaches zero when $y \to 0$. Thus,

$$\int_0^\infty f(iy)y^s \frac{dy}{y}$$

converges for all s. But

$$\int_0^\infty e^{-2\pi ny} y^s \frac{dy}{y} = (2\pi)^{-s}\Gamma(s)n^{-s},$$

so

$$\int_0^\infty f(iy)y^s \frac{dy}{y} = \Lambda(s,f)$$

This gives us an analytic continuation of $\Lambda(s,f)$. Plugging in the equation of $f(i/y)$ and replacing $1/y$ by y, we see that

$$\int_0^\infty f(iy)y^s \frac{dy}{y} = (-1)^{k/2} \int_0^\infty f(iy)y^{k-s} \frac{dy}{y} = (-1)^{k/2}\Lambda(k-s,f)$$

The case when f is not cuspidal is similar: we just need to separate the cases of $s=0$ and $s=k$ for the convergence of the integral used in the previous paragraph. □

4.2 Hecke operators

4.2.1 More about congruence subgroups

In the last section, we defined modular forms with respect to the modular group. In this section we need modular forms with respect to congruence subgroups. Besides the principal congruence subgroups $\Gamma(N)$, there are two common congruence subgroups of level N.

$$\Gamma_0(N) = \left\{\gamma \equiv \begin{bmatrix} * & * \\ 0 & * \end{bmatrix} \pmod N\right\}, \quad \Gamma_1(N) = \left\{\gamma \equiv \begin{bmatrix} 1 & * \\ 0 & 1 \end{bmatrix} \pmod N\right\} \subseteq \Gamma(1)$$

Let γ be a matrix in $\Gamma(1)$. We denote by

$$(f|\gamma)(z) = (cz+d)^{-k} f(\gamma z)$$

the right action of $\Gamma(1)$ on holomorphic functions on $\mathbb{H}$.

Remark 4.2.1. For the general case in Remark 4.1.1, we multiply the right side by an extra factor of $(\det\gamma)^{k-1}$.

Definition 4.2.1. Given a congruence subgroup Γ, a **modular form of weight k with respect to Γ** is a holomorphic function f such that $f|\gamma = f$ for all $\gamma \in \Gamma$, and holomorphic at the cusps of Γ. a **cusp form with respect to** Γ is one that vanishes at all cusps.

Remark 4.2.2. The holomorphy at cusps can be easily verified by the holomorphy of $f|\alpha$ at infinity for all $\alpha \in \Gamma(1)$. Indeed, this is equivalent to inspecting $f|\alpha$ at infinity for the finitely many representatives α of $\Gamma\backslash\Gamma(1)$.

This definition can easily be generalized to the discontinuous subgroup of $SL_2(\mathbb{R})$ such that $\Gamma\backslash\mathbb{H}$ has finite volume.

We use the same notation $\mathcal{M}_k(\Gamma)$, $\mathcal{S}_k(\Gamma)$, $\mathcal{M}(\Gamma)$ and $\mathcal{S}(\Gamma)$ to denote the spaces of modular forms with respect to Γ. Denote by $\mathcal{E}_k(\Gamma) = \mathcal{M}_k(\Gamma)/\mathcal{S}_k(\Gamma)$, the space of **Eisenstein forms**. An immediate observation is when $-I \in \Gamma$, there is no nontrivial modular form of weight k with respect to Γ for odd k. Otherwise we get $f(z) = -f(z)$ for all $z \in \mathbb{H}$.

It is therefore an immediate task to construct some nontrivial modular forms with respect to known congruence subgroups. For $\Gamma(1)$ we already defined Eisenstein series. We now define Eisenstein series for the principal congruence subgroups $\Gamma(N)$.

Definition 4.2.2. Let v be a row vector in $(\mathbb{Z}/n\mathbb{Z})^2$, and $\varepsilon_N = 1/2$ if $N \leqslant 2$ or 1 otherwise. Then define the **Eisenstein series for** $\Gamma(N)$ as

$$E_k^v(z) = \varepsilon_N \sum_{(c,d)\equiv v} \frac{1}{(cz+d)^{-k}}$$

where we require the gcd of (c,d) to be 1.

The definition follows from the fact that

$$G_k(z) = \sum_{(c,d)\neq(0,0)} \frac{1}{(cz+d)^k} = \sum_{n=1}^{\infty} \frac{1}{n^k} \sum_{(c,d)=1} \frac{1}{(cz+d)^k} = \zeta(k) \sum_{(c,d)=1} \frac{1}{(cz+d)^k}$$

Then $E_k = \frac{1}{2}\sum_{(c,d)=1}(cz+d)^{-k}$. If γ lives in $SL_2(\mathbb{Z})$, its bottom row automatically has gcd 1. But the upper rows must have the form $a+nc$ and $b+nd$ for $ad-bc=1$. In this case one $(cz+d)$ term corresponds to a representative of $P^+\backslash SL_2(\mathbb{Z})$ where P^+ is the positive parabolic subgroup consisting of parabolic elements of trace 2. Then

$$E_k^v(z) = \sum_{\gamma\in(P^+\cap\Gamma(N))\backslash\Gamma(N)\delta} \frac{1}{(cz+d)^k}$$

for some δ with bottom row congruent to v modulo N. It is therefore easy to show that $E_k^v(\gamma z) = (cz+d)^k E_k^{v\gamma}(z)$. But note that $\gamma \equiv I \bmod N$ for *gamma* $\in \Gamma(N)$, so

Lemma 4.2.1. *The Eisenstein series E_k^v is a modular form of weight k with respect to $\Gamma(N)$.*

Let α be a matrix in $GL_2(\mathbb{Q})$ with positive determinant. We consider the double coset $\Gamma_1\alpha\Gamma_2$ for congruence subgroups Γ_1, Γ_2.

Lemma 4.2.2. *Let Γ_1, Γ_2 be congruence subgroups of $SL_2(\mathbb{Z})$ and let $\alpha \in GL_2(\mathbb{Q})_+$. Let $\Gamma_3 = \alpha^{-1}\Gamma_1\alpha \cap \Gamma_2$. Then the left multiplication by α induces a natural bijection from $\Gamma_3\backslash\Gamma_2$ to the space $\Gamma_1\backslash\Gamma_1\alpha\Gamma_2$.*

An immediate consequence of this lemma is that $\Gamma_1\backslash\Gamma_1\alpha\Gamma_2$ is finite, by the finiteness of $\Gamma_3\backslash\Gamma_2$. We may then define, for a modular form $f \in M_k(\Gamma_1)$,

$$f|\Gamma_1\alpha\Gamma_2 = \sum_j f|\beta_j$$

for a set of representatives $\{\beta_j\}$ of $\Gamma_1\backslash\Gamma_1\alpha\Gamma_2$. This definition is independent of the choice of representatives (quite obvious from the Γ_1-invariance of f). Note that for any $\gamma \in \Gamma_2$, $\{\beta_j\gamma\}$ is another set of representatives of the orbit space. Therefore,

$$(f|\Gamma_1\alpha\Gamma_2)|\Gamma = \sum_j f|(\beta_j\gamma) = f|\Gamma_1\alpha\Gamma_2$$

Thus, the operator $(\cdot)|\Gamma_1\alpha\Gamma_2$ is a linear map $\mathcal{M}_k(\Gamma_1) \to \mathcal{M}_k(\Gamma_2)$. Furthermore, it restricts to a linear map $\mathcal{S}_k(\Gamma_1) \to \mathcal{S}_k(\Gamma_2)$. Indeed, if $f \in \mathcal{S}_k(\Gamma_1)$ then for any $\gamma \in GL_2(\mathbb{Q})_+$, $f|\gamma$ vanishes at infinity. Therefore, $f|\Gamma_1\alpha\Gamma_2$ being a sum of holomorphic functions vanishes at infinity vanishes at all cusps.

Definition 4.2.3. The linear map $(\cdot)|\Gamma_1\alpha\Gamma_2$ is called the **double coset operator**.

4.2.2 Two Hecke operators

The case of prime numbers

Definition 4.2.4. The **diamond operator** $\langle d\rangle$ sends a modular form f of weight k with respect to $\Gamma_1(N)$ to

$$\langle d\rangle f = f|\alpha, \quad \alpha = \begin{bmatrix} a & b \\ c & e \end{bmatrix} \in \Gamma_0(N), e \equiv d \pmod N$$

Remark 4.2.3. In this special case, we see that $\alpha^{-1}\Gamma_1(N)\alpha = \Gamma_1(N)$, which means α is the only representative of $\Gamma_1(N)\backslash\Gamma_1(N)$. Thus, $f = f|\alpha = f|\Gamma_1(N)\alpha\Gamma_1(N)$. The action of α is determined solely by the element at the lower right corner.

Note that if $\chi : (\mathbb{Z}/N\mathbb{Z})^\times \to \mathbb{C}^\times$ is a Dirichlet character, then we can define the χ-eigenspace of $\mathcal{M}_k(\Gamma_1(N))$:

$$\mathcal{M}_k(N,\chi) = \{f \in \mathcal{M}_k(\Gamma_1(N)) : f|\gamma = \chi(d_\gamma)f, \forall\gamma \in \Gamma_0(N)\}$$

where d_γ is the lower right entry of γ. The space $\mathcal{M}_k(\Gamma_1(N))$ decomposes into $\bigoplus_\chi \mathcal{M}_k(N,\chi)$ (a standard result in the theory of representations over $\mathbb{C}$). Since the actions of $\Gamma_0(N)$ on the right preserve cuspidal forms, we may also decompose $\mathcal{S}_k(\Gamma_1(N))$ and $\mathcal{E}_k(\Gamma_1(N))$ in the same manner.

Therefore we have a homomorphism $(\mathbb{Z}/N\mathbb{Z})^\times \to GL(\mathcal{M}_k(\Gamma_1(N)))$ given by $d \mapsto \langle d\rangle$. Since the action of a matrix in $\Gamma_0(N)$ on modular forms with respect to $\Gamma_1(N)$ is completely determined by $\langle d\rangle$, we have the decomposition

$$\mathcal{M}_k(\Gamma_1(N)) = \bigoplus_\chi \mathcal{M}_k(N,\chi) = \bigoplus_\chi \{f \in \mathcal{M}_k(\Gamma_1(N)) : \langle d\rangle f = \chi(d)f, \forall d \in (\mathbb{Z}/N\mathbb{Z})^\times\}$$

Definition 4.2.5. The Hecke operator T_p is defined by

$$T_p f = f|\Gamma_1(N)\alpha_p\Gamma_1(N)$$

for a prime p and $\alpha_p = \operatorname{diag}(1,p)$.

We proceed to some basic properties of the two operators.

Lemma 4.2.3. *The two operators commute, i.e.,*

$$\langle d\rangle T_p = T_p\langle d\rangle.$$

Proof. The first two statements are easy: they follow from the double coset operator's multiplicativity. For the last one, if $\{\beta_j\}$ is a set of representatives for $\Gamma_1(N)\backslash\Gamma_1(N)\alpha_p\Gamma_1(N)$ then for any $\gamma \in \Gamma_0(N)$, $\{\beta_j\gamma\}$ and $\{\gamma\beta_j\}$ are two other set of representatives. Observe if $f \in \mathcal{M}_k(\Gamma_1(N))$,

$$\langle d\rangle T_p f = \sum_j (f|\beta_j)|\gamma = \sum_j (f|\gamma)|\beta_j = T_p\langle d\rangle f$$

where γ is any matrix that defines $\langle d\rangle$. □

Easily one may see that, by the commutativity and the decomposition with respect to the roots of $\langle d\rangle$, T_p also preserves the root spaces $\mathcal{M}_k(N,\chi)$.

Lemma 4.2.4. *The operator T_p satisfies*

$$T_p f = \begin{cases} \sum_{j=1}^{p-1} f|\begin{bmatrix} 1 & j \\ 0 & p \end{bmatrix}, & p \mid N \\ f|\begin{bmatrix} m & n \\ N & p \end{bmatrix}\begin{bmatrix} p & 0 \\ 0 & 1 \end{bmatrix} + \sum_{j=1}^{p-1} f|\begin{bmatrix} 1 & j \\ 0 & p \end{bmatrix}, & p \nmid N \end{cases}$$

where $mp - nN = 1$.

Proof. Very tedious. □

As an immediate corollary,

Corollary 4.2.1. *Suppose $f \in \mathcal{M}_k(\Gamma_1(N))$ has Fourier coefficients a_n and $\langle p\rangle f$ has Fourier coefficients b_n. Then the Fourier coefficients of $T_p f$ are*

$$t_n = a_{np} + \varepsilon_{Np} p^{k-1} b_{n/p}$$

where $\varepsilon_{Np} = 1$ if $p \mid N$ and 0 otherwise. In particular, if $f \in \mathcal{M}_k(N,\chi)$ then $t_n = a_{np} + \chi(p)p^{k-1}a_{n/p}$.

Proof. The element T sits inside $\Gamma_1(N)$ and thus f has period 1, meaning f has a Fourier expansion $\sum a_n e^{2\pi i n z}$. Then by Lemma 4.2.4,

$$\left(f| \begin{bmatrix} 1 & j \\ 0 & p \end{bmatrix}\right)(z) = p^{k-1}p^{-k} f\left(\frac{z+j}{p}\right) = \frac{1}{p}\sum a_n e^{2\pi i n(z+j)/p} = \frac{1}{p}\sum a_n q_p^n \mu_p^{nj}$$

where $q_p = e^{2\pi i z/p}$ and $\mu_p = e^{2\pi i/p}$. Note that $\sum_j \mu_p^{nj} = 0$ if $p \nmid n$ and p if $p \mid n$. Thus,

$$\sum_{j=0}^{p-1} \left(f| \begin{bmatrix} 1 & j \\ 0 & p \end{bmatrix}\right)(z) = \sum_{n=0}^{\infty} a_{np} q^n$$

Similarly

$$f| \begin{bmatrix} m & n \\ N & p \end{bmatrix} \begin{bmatrix} p & 0 \\ 0 & 1 \end{bmatrix} = \langle p\rangle f| \begin{bmatrix} p & 0 \\ 0 & 1 \end{bmatrix} = p^{k-1}\sum_{n=0}^{\infty} b_n q^{np}$$

which completes the proof of the first part. The second statement is immediate as $\langle d\rangle f = \chi(d) f$ in this case. □

Lemma 4.2.5. *Let $d, d' \in (\mathbb{Z}/N\mathbb{Z})^\times$ then*

$$\langle d\rangle\langle d'\rangle = \langle d'\rangle\langle d\rangle = \langle dd'\rangle$$

Let p, q be distinct primes, then

$$T_p T_q = T_q T_p$$

Proof. The first statement is immediate if we check it for each $\mathcal{M}_k(N,\chi)$. The second statement follows from the Fourier coefficients. □

Generalizing Hecke operators

We want to define $\langle n\rangle$ and T_n for arbitrary positive n. The diamond operator is rather easy to define. If $(n, N) = 1$ then $\langle n\rangle$ is just the standard diamond operator; otherwise we define $\langle n\rangle = 0$. This extends the homomorphism on $(\mathbb{Z}/N\mathbb{Z})^\times$ to $n \mapsto \langle n\rangle$ — a multiplicative arithmetic function on $\mathbb{Z}$.

The definition of T_n is not obvious, but it closely relates to the content in chapter 5. Let $T_1 = 1$. For prime p, we define

$$T_{p^r} = T_p T_{p^{r-1}} - p^{k-1}\langle p\rangle T_{p^{r-2}}$$

Then $T_{p^r} T_{q^s} = T_{q^s} T_{p^r}$ by induction for distinct primes. Then define

$$T_n = \prod T_{p_i^{r_i}}$$

with respect to the prime factorization $n = \prod p_i^{r_i}$.

4.2.3 A basis for $S_k(\Gamma)$

Petersson inner product

We've defined a Petersson inner product for $\Gamma(1)$, and now we extend the definition to other congruence subgroups. This is actually quite easy.

Definition 4.2.6. Let Γ be a congruence subgroup and V_Γ the volume of $\Gamma\backslash\mathbb{H}^*$ with respect to the hyperbolic measure. Then the **Petersson inner product on $\mathcal{S}_k(\Gamma)$** is

$$(f,g)_\Gamma = \frac{1}{V_\Gamma}\int_{\Gamma\backslash\mathbb{H}^*} f(z)\overline{g(z)}y^k\frac{dxdy}{y^2}$$

Nothing in the integrand changed except for the normalizing factor $1/V_\Gamma$. So it is still a positive-definite Hermitian inner product. Note that we include the cusps in this definition, but they don't matter. The measure is zero at those points (certainly at ∞, and since the measure is invariant under the action of $GL_2(\mathbb{R})_+$, we may transform any cusp to infinity).

Adjoints of Hecke operators

Now we have linear maps $\langle d\rangle$ and T_p and a positive-definite inner product on the space of cuspidal forms. It is natural to think about the existence of an orthogonal basis. The most efficient tool we have is probably the spectral theorem for finite dimensional vector spaces, so we should focus on the adjoints of Hecke operators. In fact, we have (without its long but nontrivial proof)

Lemma 4.2.6. *If $p \nmid N$, the Adjoints of $\langle p\rangle$ and T_p are $\langle p\rangle^{-1}$ and $\langle p\rangle^{-1}T_p$ resp. under the Petersson inner product on $\mathcal{S}_k(\Gamma_1(N))$.*

Theorem 4.2.1. *The space of cuspidal forms $\mathcal{S}_k(\Gamma_1(N))$ has an orthogonal basis of simultaneous eigenforms of $\langle n\rangle$ and T_n with $(n,N)=1$.*

Proof. A direct application of the spectral theorem on commuting normal (by the previous lemma) linear operators on finite dimensional vector spaces. □

4.3 Eigenforms

4.3.1 Oldforms and newforms

In the previous sections, we defined linear maps on the space of modular forms and cuspidal forms with respect to the same congruence subgroup. We now attempt to pass modular forms to other levels.

Say M and N are two integers such that $M \mid N$. If f is a modular form of level M of weight k, then we can easily pass it to level N via the inclusion map. If $d|N/M$, then we can pass some $f \in \mathcal{S}_k(\Gamma_1(M))$ to $S_k(\Gamma_1(N))$ by

$$f \mapsto f|\alpha_d = d^{k-1}f(dz), \quad \alpha_d = \begin{bmatrix} d & 0 \\ 0 & 1 \end{bmatrix}$$

This map is injective. We can therefore define maps for each divisor d of N

$$i_d : (\mathcal{S}_k(\Gamma_1(N/d)))^2 \to \mathcal{S}_k(\Gamma_1(N)), (f,g) \mapsto f + g|\alpha_d$$

Definition 4.3.1. The **oldforms at level** N of weight k are

$$\mathcal{S}_k(\Gamma_1(N))^{\text{old}} = \sum_{p|N \text{ prime}} (\mathcal{S}_k(\Gamma_1(N/p)))^2$$

The **newforms at level** N is

$$\mathcal{S}_k(\Gamma_1(N))^{\text{new}} = \left[\mathcal{S}_k(\Gamma_1(N))^{\text{old}}\right]^{\perp}$$

Remark 4.3.1. The term old and new simply refers to whether a form of level N can be obtained by lifting an old modular form at level M dividing N or not.

Lemma 4.3.1. *The space of oldforms and newforms are T_n and $\langle n\rangle$ invariant for all positive n.*

Corollary 4.3.1. *The space of oldforms and newforms have orthogonal bases of eigenforms of the Hecke operators.*

4.3.2 The main lemma

Like i_d, we can define another lifting map $\iota_d : f(z) \mapsto f(dz) = d^{1-k} f|\alpha_d$. Then the Fourier expansion of $\iota_d f$ is just

$$\iota_d f = \sum_{n=1}^{\infty} a_n q^{dn}$$

In particular, if a cusp form f with respect to $\Gamma_1(N)$ takes the form $f = \sum_{p|N} \iota_p f_p$, then the Fourier coefficients of f satisfies $a_n = 0$ for all $(n, N) = 1$. The main lemma is precisely its converse:

Theorem 4.3.1 (main lemma)**.** *If $f \in \mathcal{S}_k(\Gamma_1(N))$ has Fourier coefficients a_n with $a_n = 0$ for all n coprime to N, then f has the shape*

$$\sum_{p|N} \iota_p f_p$$

for $f_p \in \mathcal{S}_k(\Gamma_1(N/p))$.

4.3.3 Linear independence of newforms

Definition 4.3.2. We say a nonzero modular form in $\mathcal{M}_k(\Gamma_1(N))$ is a **Hecke eigenform** if it's an eigenform for all $T_n, \langle n\rangle$ and $n \in \mathbb{Z}_{>0}$. An eigenform is normalized if the second Fourier coefficient is 1. A **newform** is a normalized eigenform in $\mathcal{S}_k(\Gamma_1(N))$.

Theorem 4.3.2. *Let $f \in \mathcal{S}_k(\Gamma_1(N))^{new}$ be a nonzero eigenform for the Hecke operators T_n and $\langle n\rangle$ for all n coprime to N. Then*

(i) *It is a Hecke eigenform.*

(ii) *If f' satisfies the same conditions, $f' = cf$ for some constant c.*

The set of newforms is an orthogonal basis of $\mathcal{S}_k(\Gamma_1(N))^{new}$, and their Fourier coefficients are their T_n-eigenvalues.

Proof. Clearly such a form is an eigenform for all $\langle n\rangle$: the operator is zero if $(n, N) > 1$. We first show that f can be normalized such that $a_1 = 1$. Suppose g (not necessarily in $\mathcal{S}_k(\Gamma_1(N))^{\text{new}}$) is an eigenform for the Hecke operators T_n and $\langle n\rangle$ for all n coprime to N. Let c_n and d_n be the corresponding eigenvalues. The map $\chi : n \mapsto d_n$ is therefore a Dirichlet character modulo N and $f \in \mathcal{S}_k(N, \chi)$. Moreover, the Fourier expansion of $T_n f$ in Corollary 4.2.1 suggests $a_1(T_n f) = a_n f$ which equals to $c_n a_1(f)$ for n coprime to N. Thus, $a_n = c_n a_1$. In this case if $a_1(f) = 0$, then $a_n(f) = 0$ for all $(n, N) = 1$. By the main lemma, f is an oldform.

However, since f is a newform at level N, we must have $a_1 \neq 0$. Thus, we may normalize this coefficient. For all natural number m, we may define the cuspidal newform $g_m = T_m f - a_m f$, which is clearly an eigenform for T_n and $\langle n \rangle$ for all n coprime to N. But then its second Fourier coefficient is $a_m - a_1 a_m = a_m - a_m = 0$, thus g_m is also an oldform. Thus, $g_m = 0$ and $T_m f = a_m f$ for all natural number m. This proves the statements (i), (ii) and the last sentence.

It remains to show the linear independence of newforms. Suppose there is a linear dependence of newforms with minimal number of terms

$$\sum_{i=1}^{n} c_i f_i = 0$$

Its image under the map $a_p(f_1) - T_p$ is zero for any prime p. This means

$$\sum_{i=2}^{n} c_i (a_p(f_1) - a_p(f_i)) f_i = 0$$

which by the minimality of n implies $a_p(f_1) - a_p(f_i) = 0$ for all i. But as p is arbitrary, $f_i = f_1$ for all i, a contradiction. Thus, the newforms are linearly independent, and they span $\mathcal{S}_k(\Gamma_1(N))^{\text{new}}$. □

4.3.4 L-functions attached to eigenforms

For a modular form $f \in \mathcal{M}_k(\Gamma_1(N))$, we associate the L-function $L(s, f) = \sum a_n n^{-s}$ as before.

Lemma 4.3.2. *The L-function of f converges absolutely for all s with real part larger than $k/2 + 1$, if f is a cuspidal form. Otherwise, the L-function converges for all $\operatorname{Re}(s) > k$.*

Proof. An immediate result of the bound $|a_n| \leqslant C n^{k/2}$. □

The reader might notice that although we have discussed the functional equation of the L-function, we haven't even mentioned its Euler product! This is because not all L-functions attached to a modular form can be written in the form of an Euler product.

Lemma 4.3.3. *A modular form f in $\mathcal{M}_k(N, \chi)$ is a normalized eigenform if and only if its Fourier coefficients satisfy $a_1 = 1$, for any prime p*

$$a_{p^r} = a_p a_{p^{r-1}} - \chi(p) p^{k-1} a_{p^{r-2}} f,$$

and $a_{mn} = a_m a_n$ for m, n coprime.

Proof. We only need to prove the backward direction as the forward implication is immediate from the definition of $T_n f$. Clearly f is normalized. We need to show $a_m(T_p f) = a_p a_m$. If $p \nmid m$, then $a_m(T_p f) = a_{pm} = a_p a_m$ by Corollary 4.2.1. If $p \mid m$ write $m = p^r m'$ for $p \nmid m'$. Then

$$\begin{aligned} a_m(T_p f) &= a_{p^{r+1} m'} + \chi(p) p^{k-1} a_{p^{r-1} m'} \\ &= (a_{p^{r+1}} + \chi(p) p^{k-1} a_{p^{r-1}}) a_{m'} \\ &= a_p a_{p^r} a_{m'} \\ &= a_p a_m \end{aligned}$$

w where we used Corollary 4.2.1 in the first equality and the assumptions in the other equalities. □

Theorem 4.3.3. *A modular form f in $\mathcal{M}_k(N,\chi)$ is a normalized eigenform if and only if*

$$L(s,f) = \prod_p \frac{1}{1 - a_p p^{-s} + \chi(p)p^{k-1-2s}}$$

taking over all primes.

Proof. By the previous lemma, the modular form is normalized if and only if $a_1 = 1$, for any prime p

$$a_{p^r} = a_p a_{p^{r-1}} - \chi(p)p^{k-1}a_{p^{r-2}}f,$$

and $a_{mn} = a_m a_n$ for m, n coprime. Now multiply the second equality by p^{-rs} and sum over r. We obtain

$$\sum_{r=0}^{\infty} a_{p^r} p^{-rs}(1 - a_p p^{-s} + \chi(p)p^{k-1-2s}) = a_1 + (1 - a_1)a_p p^{-s}$$

which suggests

$$\sum_{r=0}^{\infty} a_{p^r} p^{-rs}(1 - a_p p^{-s} + \chi(p)p^{k-1-2s}) = 1$$

If the equation holds, then letting $s \to \infty$ we get $a_1 = 1$, and we can consequently get the second condition. Therefore, the first and second conditions are equivalent to

$$\sum_{r=0}^{\infty} a_{p^r} p^{-rs} = \frac{1}{1 - a_p p^{-s} + \chi(p)p^{k-1-2s}}$$

A similar argument shows that the third condition holds if and only if

$$L(s,f) = \sum_{n=1}^{\infty} a_n n^{-s} = \sum_{n=1}^{\infty} \prod_{n=p^r n'} a_{p^r} p^{-rs} = \prod_p \sum_{r=0}^{\infty} a_{p^r} p^{-rs} = \prod_p \frac{1}{1 - a_p p^{-s} + \chi(p)p^{k-1-2s}}$$

where the second equality is equivalent to the third condition. □

Chapter 5

Elliptic Curves and Modular Curves

In this chapter, we prepare things required for the celebrated Eichler-Shimura relation. I will omit many proofs, especially those of pure facts in algebraic curves, algebraic geometry or elliptic curves. The reason for this is simple: the proofs are too long. Thus, I will freely quote a result when necessary and only demonstrate those closely related to the theme of this chapter. The main references for this section are [DS05], [Sil94] and [Mil86].

5.1 Elliptic Curves

In this section we briefly study the elliptic curves over different fields. They have some very nice properties that make them easy to understand. They also have a close relation to modular forms.

5.1.1 Complex tori

Take an abelian variety A, i.e., a complete, connected algebraic group. Then $A(\mathbb{C})$ is a connected, compact, complex Lie group. Let T be an arbitrary such Lie group. Consider the adjoint representation of T on $\mathrm{Lie}(T)$. writing the representation in a matrix form with respect to a basis of the Lie algebra, we see that each entry is a holomorphic function of T. Then since T is compact, the adjoint representation is trivial. Therefore the exponential maps $\mathrm{Lie}(T)$ to a subgroup of the center of T. As T is connected, the image of $\mathrm{Lie}(T)$ generates T, meaning T is commutative.

Indeed, T is a complex torus. That is, the kernel of the exponential map is a discrete subgroup Λ. Then since the exponential map is surjective (standard result from the theory of Lie groups, given that T is connected and compact), $T = \mathrm{Lie}(T)/\Lambda$, a complex torus.

We now focus on one dimensional complex torus. Suppose Λ is a lattice in $\mathbb{C}$, namely, a discrete subgroup of $\mathbb{C}$ that spans $\mathbb{C}$. Then a complex torus is the quotient space $\mathbb{C}/\Lambda$. Say Λ has a $\mathbb{Z}$-basis $\{\omega_1, \omega_2\}$ with $\omega_1/\omega_2 \in \mathbb{H}$, then let $\tau = \omega_1/\omega_2$, and $\Lambda_\tau = \mathbb{Z} \oplus \tau\mathbb{Z}$, we have an isomorphism $\mathbb{C}/\Lambda \to \mathbb{C}/\Lambda_\tau$ given by $z \mapsto z/\omega_2$. In fact, this τ is unique up to actions of $SL_2(\mathbb{Z})$ on $\mathbb{H}$. The standard theory of complex elliptic curves shows that we have a map

$$z \mapsto (\wp(z), \wp'(z))$$

where $\wp$ is the Weierstrass $\wp$-function:

$$\wp(z) = \frac{1}{z^2} + \sum_{\omega \neq 0 \in \Lambda} \left(\frac{1}{(z-\omega)^2} - \frac{1}{\omega^2} \right)$$

which is an example of elliptic functions namely functions with lattice periods. We may also generalize the Eisenstein series to a function of the lattice

$$G_k(\Lambda) = \sum_{\omega = \neq \in \Lambda} \frac{1}{\omega^k}$$

In particular $G_k(\Lambda_\tau)$ are the modular forms Eisenstein series $G_k(\tau)$. It can be shown quite easily that

Lemma 5.1.1. *The functions $\wp$ and $\wp'$ satisfy the relation*

$$\wp'^2 = 4\wp^3 - g_2(\Lambda)\wp - g_3(\Lambda)$$

where $g_2(\Lambda) = 60G_4(\Lambda)$ and $g_3(\Lambda) = 140G_6(\Lambda)$ and the RHS splits into

$$y^2 = 4(x - e_1)(x - e_2)(x - e_3)$$

where $e_i = \wp(\omega_i/2)$ with $\Lambda = \omega_1\mathbb{Z} \oplus \omega_2\mathbb{Z}$ and $\omega_3 = \omega_1 + \omega_2$.

The roots of the cubic are distinct, so we have a bijection $(\wp, \wp')$ from the set of complex tori to the set of elliptic curves over $\mathbb{C}$. In fact, the field of meromorphic functions $\mathcal{M}(\mathbb{C}/\Lambda)$ is generated by $\wp$ and $\wp'$.

5.1.2 Divisors and algebraic curves

Throughout this section I use the notation Pic instead of Pic^0 for convenience. Elliptic curves over a field k of characteristic zero are easy to deal with because they can all be transformed into a Weierstrass normal form

$$E : y^2 = 4x^2 + ax + b, \quad a, b \in k$$

In the case of characteristic zero, the curve being nonsingular is equivalent to requiring three distinct roots of $g(x) = 4x^2 + ax + b$. It is also easier to define the group law on $\bar{k}$-points of the elliptic curve in this form. We say $P + Q + R = \mathcal{O}$ if and only if P, Q, R is colinear, where $\mathcal{O}$ is the point at infinity $[0 : 1 : 0]$.

Since the elliptic curve is defined over k, for all algebraic extensions K/k the K-points $E(K)$ form an abelian group on its own. The n-torsion subgroup of E, $E[n]$ is isomorphic to $(\mathbb{Z}/n\mathbb{Z})^2$.

Consider the function field of some nonsingular algebraic curve C over $\bar{k}$, denoted by $\bar{k}(C)$. On this function field we can define a valuation at each point $P \in C$, given by

$$\nu_P : \bar{k}[C] \to \mathbb{N} \cup \{\infty\}, f \mapsto \begin{cases} \infty, & f = 0 \\ e, & f = t^e u \end{cases}$$

where t is a uniformizer of the localization $\bar{k}[C]_{\mathfrak{m}_P}$ and u a unit. Then we can extend ν_P to the whole field $\bar{k}(C)$ by $\nu_P(f/g) = \nu_P(f) - \nu_P(g)$. It is easy to show that ν_P is a nonarchimedean valuation.

We also have Weil divisors on C. Define the **principal divisor** of some f in the function field to be

$$\mathrm{div}(f) = \sum_{P \in C} \nu_P(f)(P)$$

The ramification degree is $e_P(f) = \nu_P(f^*t)$ for a uniformizer t at $f(P)$. In fact we have

$$\sum_{P \in f^{-1}(Q)} e_P(f) = \deg f = [\bar{k}(C) : f^*\bar{k}(C)]$$

and

$$\operatorname{div}(f) = \sum_{f(P)=0} e_P(f)(P) - \sum_{f(P)=\mathcal{O}} e_P(f)(P)$$

Thus, $\sum \nu_P(f) = 0$ and $\operatorname{div}(f)$ is an element of

$$\operatorname{Div}^0(C) = \left\{D = \sum n_P(P) : \deg D = \sum n_P = 0\right\}$$

a subgroup of the divisor group for formal sums

$$\operatorname{Div}(C) = \left\{\sum n_P(P) : n_P = 0 \text{ for all but finitely many } P\right\}$$

The Picard group of C is then

$$\operatorname{Pic}(C) = \operatorname{Div}^0(C)/\operatorname{div}(C)$$

A nonconstant morphism of elliptic curves $\varphi : C \to C'$ induces pushforwards and pullbacks of divisors

$$\varphi^* : \operatorname{Div}(C') \to \operatorname{Div}(C), \quad \varphi^*(Q) = \sum_{P \in \varphi^{-1}(Q)} e_\varphi(P)(P)$$

and

$$\varphi_* : \operatorname{Div}(C) \to \operatorname{Div}(C'), \quad \varphi_*(P) \mapsto (\varphi(P)),$$

and extend them by linearity.

Given a curve C and a divisor D on C, we say D is **positive** if all $n_P \geqslant 0$. We denote this by $D \geqslant 0$. Given two divisors we write $D_1 \geqslant D_2$ if $D_1 - D_2 \geqslant 0$.

Definition 5.1.1. For a divisor D, define a K-vector space:

$$\mathcal{L}(D) = \{f \neq 0 \in K(C) : \operatorname{div}(f) \geqslant -D\} \cup \{0\}$$

This vector space is actually finite-dimensional and we write

$$l(D) = \dim_K \mathcal{L}(D).$$

Lemma 5.1.2. *For any $D \in \operatorname{Div}(C)$,*

(i) *If $\deg D < 0$ then $\mathcal{L}(D) = 0$.*

(ii) *For another $D' \in \operatorname{Div}(C)$, if $D \equiv D'$ in $\operatorname{Pic}(C)$, then $\mathcal{L}(D) \cong \mathcal{L}(D')$ and as a consequence $l(D) = l(D')$.*

Let K_C be a canonical divisor of C (meaning it corresponds to the canonical line bundle $\Omega_C^{\wedge n}$ of C). The dimension $l(K_C)$ is independent of the choice of canonical divisors.

Theorem 5.1.1 (Riemann-Roch)**.** *Let C be a curve and K_C the canonical divisor on C. There is an integer $g \geqslant 0$ called the* genus of C *such that for any $D \in \operatorname{Div}(C)$,*

$$l(D) - l(K_C - D) = \deg D - g + 1$$

Remark 5.1.1. The term $l(K_C - D)$ is sometimes called the correction term. Since $l(K_C - D) \geqslant 0$ for any D, we have

$$l(D) \geqslant \deg D - g + 1$$

which is called Riemann's inequality.

Corollary 5.1.1. *The followings hold:*

(i) $l(K_C) = g$.

(ii) $\deg K_C = 2g - 2$ *(which is $-\chi$ where χ is the Euler characteristic of C).*

(iii) *If* $\deg D > 2g - 2$*, then* $l(D) = \deg D - g + 1$

Lemma 5.1.3. *Suppose E is an elliptic curve. Then for any two points $P, Q \in E$, $(P) \sim (Q)$ if and only if $P = Q$.*

Proof. Let $f \neq 0 \in K(C)$ such that $\operatorname{div}(f) = (P) - (Q)$. Clearly $\operatorname{div}(f) \geqslant -(Q)$ so $\operatorname{div}(f) \in \mathcal{L}((Q))$. But since the genus of E is $g = 1$, $\deg(Q) = 1 > 2g - 2$. Thus, by Corollary 5.1.1 (iii), $l((Q)) = \deg(Q) = 1$. Therefore, as $1 \in \mathcal{L}((Q))$, $f \in K$ and $\operatorname{div}(f) = 0$. This means $P = Q$ (otherwise the formal sum cannot cancel). □

Consider any divisor $D \in \operatorname{Div}^0(E)$ of degree 0. We have $l(D + (\mathcal{O})) = \deg(D + (\mathcal{O})) = 1$ by Corollary 5.1.1 (iii). Let f be a nonzero element of $K(E)$ that spans $\mathcal{L}(D + (\mathcal{O}))$. Then we have $\operatorname{div}(f) \geqslant -D - (\mathcal{O})$. But $\deg \operatorname{div}(f) = 0$, we have some $P \in E$ such that $\operatorname{div}(f) = -D - (\mathcal{O}) + (P)$ To deduce the last statement, We must think about the formal sum. The inequality above tells us that the coefficients in $\operatorname{div} f$ before (Q) and each term in D must be larger than -1 and the coefficient of each term in $-D$; but the coefficient before $\mathcal{O}$ in $\operatorname{div}(f)$ cannot be positive, otherwise we cannot cancel it in the degree, as the other coefficients must be nonnegative. Thus the degree of $\operatorname{div}(f) = 0$ suggests that there is one single point (or else the degree of the part other than $-D - (\mathcal{O})$ would be larger than 1, which is impossible to cancel in $\deg \operatorname{div}(f)$) such that $\operatorname{div}(f) = -D - (\mathcal{O}) + (P)$ (it could be $\mathcal{O}$ of course). Then if P' is another such point, we have $(P') \sim D + (\mathcal{O}) \sim (P)$ which by Lemma 5.1.3 gives $P = P'$.

Let $\sigma : \operatorname{Div}^0(E) \to E$ be the map sending D to the unique point P found above.

Theorem 5.1.2. *The map σ induces a bijection $\sigma : \operatorname{Pic}(E) \to E$, with its inverse being $\kappa : E \to \operatorname{Pic}(E)$ defined by $P \mapsto [(P) - (\mathcal{O})]$. Therefore we can impose E with a group structure by defining*

$$P + Q = \kappa^{-1}(\kappa(P) + \kappa(Q)).$$

The theorem implies the two ways of defining the group law in elliptic curves, using lines or a bijection to the Picard group, are the same in the sense of the isomorphism above. I used the Picard group method in our M2R project on elliptic curves.

5.2 The Geometry of Modular Curves

5.2.1 As Riemann surfaces

Given a congruence subgroup Γ, the space $\Gamma\backslash\mathbb{H}$ is a Riemann surface and $\Gamma\backslash\mathbb{H}^*$ its compactification (Section 4.1.1). Denote by $Y(\Gamma) = \Gamma\backslash\mathbb{H}$ and $X(\Gamma)$ the compactified one. These are called **modular curves**. For convenience we write $Y(N), Y_0(N)$, $Y_1(N)$, $X(N)$, $X_0(N)$ and $X_1(N)$ for the modular curves and their compactifications of the common congruence subgroups $\Gamma(N), \Gamma_0(N)$ and $\Gamma_1(N)$. I do not intend to prove any results on the modular curves as complex manifolds — they are all consequences of Riemann-Roch and the Riemann-Hurwitz formula. Instead, I will simply list some formulas for the dimensions.

To compute the genus of $X(\Gamma)$, consider the elliptic points of period $2, 3$, $\Gamma(1)i$ and $\Gamma(1)e^{2\pi i/3}$. Their image in $X(\Gamma)$ is finite. Let $\varepsilon_2, \varepsilon_3$ denote the number of elliptic points of period 2 and 3 respectively, and ε_∞ the number of cusps of Γ. Then

Theorem 5.2.1. *The genus of $X(\Gamma)$ is*

$$g = 1 + \frac{d}{12} - \frac{\varepsilon_2}{4} - \frac{\varepsilon_3}{3} - \frac{\varepsilon_\infty}{2}$$

where d is the degree of the projection map $f : X(\Gamma) \to X(1)$ which equals to $[\Gamma(1) : \Gamma]$.

Example 5.2.1. When $\Gamma = \Gamma(1)$, $d = \varepsilon_2 = \varepsilon_3 = \varepsilon_\infty = 1$ from their definition. Therefore, $g = 0$ is the genus of $X(\Gamma(1))$.

Theorem 5.2.2. *Let k be an even integer. Then*

$$\dim \mathcal{M}_k(\Gamma) = \begin{cases} (k-1)(g-1) + \left\lfloor \frac{k}{4} \right\rfloor \varepsilon_2 + \left\lfloor \frac{k}{3} \right\rfloor \varepsilon_3 + \frac{k}{2} ve_\infty, & k \geqslant 2 \\ 1, & k = 0 \\ 0, & k < 0 \end{cases}$$

and

$$\dim \mathcal{S}_k(\Gamma) = \begin{cases} (k-1)(g-1) + \left\lfloor \frac{k}{4} \right\rfloor \varepsilon_2 + \left\lfloor \frac{k}{3} \right\rfloor \varepsilon_3 + \left(\frac{k}{2} - 1\right) ve_\infty, & k \geqslant 4 \\ g, & k = 2 \\ 0, & k < 2 \end{cases}$$

Example 5.2.2. Since $g = 0$ and $\varepsilon_2 = \varepsilon_3 = \varepsilon_\infty$ for $\Gamma = \Gamma(1)$, we actually have $\dim \mathcal{M}_k(\Gamma(1)) = \dim \mathcal{S}_k(\Gamma(1)) + 1$ for $k \geqslant 4$, which suggests

$$\mathcal{M}_k(\Gamma(1)) = \mathcal{S}_k(\Gamma(1)) \oplus \mathbb{C}E_k$$

and

$$\dim \mathcal{S}_k(\Gamma(1)) = \begin{cases} \left\lfloor \frac{k}{12} \right\rfloor - 1, & k \equiv 2 \pmod{12} \\ \left\lfloor \frac{k}{12} \right\rfloor, & \text{otherwise} \end{cases}$$

Similar formula exists for odd k, but we need to separate the regular and irregular cusps in this case. Still since $-I \in \Gamma(1)$ there are no modular forms of odd weights. An easy analysis of the dimension shows that $\mathcal{M}(\Gamma(1)) = \mathbb{C}[E_4, E_6]$ and $\mathcal{S}(\Gamma(1)) = \Delta \cdot \mathcal{M}(\Gamma(1))$. To see this, note that $1, 0, E_4, E_6$, $E_4^2, E_4E_6, \{E_4^3, E_6^2\}$ are the bases for $\mathcal{M}_k(\Gamma(1))$, $k = 0, 2, \ldots, 12$ respectively. The multiplying by E_4^3 and E_6^2, we get bases for $k = 12, \ldots, 24$. Repeating this process, $\mathcal{M}(\Gamma(1)) = \mathbb{C}[E_4, E_6]$. The map $f \mapsto \Delta \cdot f$ gives an isomorphism $\mathcal{M}_k(\Gamma(1)) \to \mathcal{S}_{k+12}(\Gamma(1))$, so the second statement holds.

5.2.2 As algebraic curves

On the modular curve $X(\Gamma)$ as a Riemann surface, we may define the sheaf

$$\omega_k : U \mapsto \{\text{modular forms of weight } k \text{ on } \tilde{U}\}$$

where $\tilde{U}$ is the preimage of U in $\mathbb{H}$. Clearly if a is a holomorphic function on U and $f \in \Gamma(\omega_k, U)$, then af is a modular form on U of weight k. Thus, ω_k is a sheaf of $\mathcal{O}_{X(\Gamma)}$-modules.

Lemma 5.2.1. *The sheaf ω_k is invertible.*

Proof. For p a point in $X(\Gamma)$ not a cusp or elliptic point, we can find a nhds V around p such that its preimage $\pi^{-1}(V)$ is simply the disjoint union $\pi^{-1}(V) = \bigcup_{\gamma \in \Gamma} \gamma U$ and $\omega_k(V) = \mathcal{O}_{\mathbb{H}}(U) = \mathcal{O}_{X_\Gamma}(U)$, that is, the value of the modular form is determined by a holomorphic function on U and pasting its values to other cosets. For the other cases, consider the charts around p and spell out the definitions of these items, obtaining $\omega_k(V) = \mathcal{O}_{X(\Gamma)}(V)b$ for some $b \in \omega_k(V)$. Thus, ω_k is an invertible sheaf. □

By GAGA the modular curves associates to unique algebraic varieties $X(\Gamma)_{\mathbb{C}}$ whose $\mathbb{C}$-points are the modular curves $X(\Gamma)$, and also corresponding to the analytic sheaf ω_k there is a sheaf ω_k on $X(\Gamma)_{\mathbb{C}}$ such that $\mathcal{M}_k(\Gamma) = \Gamma(X(\Gamma)_{\mathbb{C}}, \omega_k)$. In fact,

$$X(\Gamma)_{\mathbb{C}} = \operatorname{Proj}\left(\bigoplus_k \mathcal{M}_k(\Gamma)\right).$$

Recall the j-**invariant** is a meromorphic function $j : \mathbb{H} \to \mathbb{C}^*$ invariant under the action of $\Gamma(1)$, defined by $\frac{1}{1728}\frac{g_2^3}{\Delta}$. Its numerator and denominator are both holomorphic modular forms of weight 12, so j is a meromorphic modular function.

Remark 5.2.1. I will not use the term "automorphic" for meromorphic modular forms because apparently it means different things for different people.

It turns out that the (meromorphic since we are working with the analytic structure sheaf) function field of $X(\Gamma(1))_{\mathbb{C}}$ over $\mathbb{C}$ is precisely the algebra generated by j. Obviously $\mathbb{C}(X(\Gamma(1))_{\mathbb{C}})$ is the field of meromorphic modular functions as they are invariant under the actions of $\Gamma(1)$. The inclusion $\mathbb{C}(j) \subseteq \mathbb{C}(X(\Gamma(1))_{\mathbb{C}})$ is evident. For the opposite we use the usual Liouville trick. That is, take f a meromorphic modular function with finite zeros $z_1, \ldots, z_n$ and poles $w_1, \ldots, w_m$ counted by multiplicities. Define

$$g(z) = \frac{\prod_i [j(z) - j(z_i)]}{\prod_i [j(z) - j(w_i)]}$$

Then g has the same zeros and poles as f for non-cusp points. At the cusp ∞, g thus vanishes to the same order as f as the number of zeros equals to the number of poles. Therefore f/g is a holomorphic function on $X(\Gamma(1))$, so it's constant. Therefore $\mathbb{C}(j) = \mathbb{C}(X(\Gamma(1))_{\mathbb{C}})$.

Define the invariant for $\Gamma(N)$

$$f_0^v(z) = \frac{g_2(z)}{g_3(z)} \wp_z \left(\frac{c_v z + d_v}{N} \right)$$

where v is a nonzero vector in $(\mathbb{Z}/N\mathbb{Z})^2$ and $(c, d) \equiv v \pmod{N}$. To see its invariance, note that if $\gamma = \left[\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right]$ and $m = (cz + d)^{-1}$ then $m\Lambda_z = \Lambda_{\gamma(z)}$. Then

$$\begin{aligned} \wp_{\Lambda_{\gamma(z)}} \left(\frac{c_v \gamma(z) + d_v}{N} \right) &= \wp_{m\Lambda_z} \left(m \frac{c_v az + bc_v + d_v cz + d_v d}{N} \right) \\ &= m^{-2} \wp_z \left(\frac{c_v z + d_v}{N} \right) \end{aligned}$$

where the last equality follows from $\wp_{mz}(mw) = m^{-2}\wp_z(w)$ and $\gamma \equiv I \pmod{N}$. Since g_2/g_3 has weight -2, $f_0^v(z)$ is thus $\Gamma(N)$-invariant. We won't check for the meromorphic property. Let $f_0^d = f_0^{(0,d)}$ ($\Gamma_1(N)$-invariant via a similar argument) and $f_0 = \sum_{d=1}^{N-1} f_0^d$ ($\Gamma_0(N)$-invariant). Let $f_{1,0} = f_0^{(1,0)}$ and $f_{0,1} = f_1 = f_0^{0,1}$. Denote by j_N the function $z \mapsto j(Nz)$.

Lemma 5.2.2. *The function fields on $X(N)$, $X_1(N)$ and $X_0(N)$ are*

(i) $\mathbb{C}(X(N)) = \mathbb{C}(j, f_{1,0}, f_{0,1})$,

(ii) $\mathbb{C}(X_1(N)) = \mathbb{C}(j, f_1)$,

(iii) $\mathbb{C}(X_0(N)) = \mathbb{C}(j, f_0) = \mathbb{C}(j, j_N)$.

Proof. For $\Gamma(N)$, $\wp_z(w) = \wp_z(w')$ if and only if $w = \pm w' \pmod{\Lambda_z}$. Therefore, the pairs f_0^v, f_0^{-v} are equal and distinct from all other equal pairs. The action of $\Gamma(1)$ on $X(N)$ induces field automorphisms on $\mathbb{C}(X(N))$. Because pullbacks respect compositions, the map $\theta : \gamma \mapsto \gamma^*$ is a homomorphism. Its kernel is precisely $\pm\Gamma(N)$ since $f_0^v \circ \gamma = f_0^{v\gamma}$ and $v\gamma \equiv \pm v$ if and only if $\gamma \in \pm\Gamma(N)$. Then $\operatorname{im}\theta = \Gamma(1)/\pm\Gamma(N)$. The fixed field of $\operatorname{im}\theta$ is $\mathbb{C}(X(1))$ so $\operatorname{Gal}(\mathbb{C}(X(N))/\mathbb{C}(X(1))) = \operatorname{im}\theta$. Take the set $S = \{f_0^w : w \in (\mathbb{Z}/N\mathbb{Z})^{2\times}/\pm 1\}$ of distinct functions, the field $\mathbb{C}(j, S)$ is fixed by the trivial subgroup, and similarly for $\mathbb{C}(j, f_{1,0}, f_{0,1})$. By Galois theory we have $\mathbb{C}(j, f_{1,0}, f_{0,1}) = \mathbb{C}(j, S) = \mathbb{C}(X(N))$.

For $\Gamma_1(N)$, we have fields

$$\mathbb{C}(X(1)) \subseteq \mathbb{C}(j, \{f_0^d\}) \subseteq \mathbb{C}(X_1(N)) \subseteq \mathbb{C}(X(N))$$

Note that $\pm\Gamma_1(N)/\pm\Gamma(N)$ fixes the second subfield, so a Galois-theoretic argument gives us $\mathbb{C}(X_1(N)) = \mathbb{C}(j, \{f_0^d\}) = \mathbb{C}(j, f_1)$. I won't prove the last statement. □

Remark 5.2.2. Note that given some $\tau \in \mathbb{H}$ such that $j(\tau) \notin \{0, 1728\}$, the complex torus $\mathbb{C}/\Lambda_\tau$ can be sent to the elliptic curve $E_j : y^2 = 4x^3 - \frac{g_2^3}{g_3^2}x - \frac{g_2^3}{g_3^2}$ via the map $(u^2\wp_\tau, u^3\wp'_\tau)$ where $u = (g_2^3/g_3^2)^{1/2}$. Since $\frac{g_2^3}{g_3^2} = \frac{27j}{j-1728}$, we have the **universal elliptic curve**

$$E_j : y^2 = 4x^3 - \left(\frac{27j}{j-1728}\right)x - \left(\frac{27j}{j-1728}\right)$$

The universal elliptic curve has j-invariant j by some simple algebra. This can be regarded as an elliptic curve over $\mathbb{C}(j)$ if we assume j is transcendental over $\mathbb{C}$. Then the distinct x-coordinates are precisely $x(E_j[N]) = \{f_0^v\}$ for a set of representatives $\{v\}$ of $(\mathbb{Z}/N\mathbb{Z})^{2\times}$. They are distinct because for z with $j(z) \neq 0, 1728$, $f_0^v(z)$ are distinct. To summarize, we have

Lemma 5.2.3.

$$\mathrm{Gal}(\mathbb{C}(j, E_j[N])/\mathbb{C}(j)) = SL_2(\mathbb{Z}/N\mathbb{Z})$$

Proof. First from Lemma 5.2.2 we see

$$\mathrm{Gal}(\mathbb{C}(j, x(E_j[N]))/\mathbb{C}(j)) = \mathrm{Gal}(\mathbb{C}(j, f_{0,1}, f_{1,0})/\mathbb{C}(j)) = \Gamma(1)/\pm\Gamma(N) = SL_2(\mathbb{Z}/N\mathbb{Z})/\pm 1$$

Let $\sigma \in \mathrm{Gal}(\mathbb{C}(j, E_j[N])/\mathbb{C}(j))$. Then we get an invariance of the Weil pairing (induced by the injective representation $\rho : G \to GL_2(\mathbb{Z}/N\mathbb{Z})$)

$$e_N(P, Q)^\sigma = e_N(P, Q)^{\det \rho\sigma}$$

where P, Q is a basis of $E_j[N]$. But σ fixes $e_N(P, Q)$ as the latter is an Nth root of unity in $\mathbb{C}$. Thus,

$$e_N(P, Q) = e_N(P, Q)^{\det \rho\sigma}$$

Furthermore the pairing is a primitive root, so $\det \rho(\sigma) = 1$, meaning $\operatorname{im}\rho$ lies in $SL_2(\mathbb{Z}/N\mathbb{Z})$.

Let K be the subgroup fixing $\mathbb{C}(j, x(E_j[N]))$. Then by the Weierstrass normal form, two points with the same x-coordinates have y-coordinates y or $-y$. Thus, $P^\sigma = \pm P$, $Q^\sigma = \pm Q$. Thus, $\rho(\sigma) \in \{\pm I\}$, and vice versa. One may then count $\#K = \rho^{-1}(\pm I) \leqslant 2$, meaning $[SL_2(\mathbb{Z}/N\mathbb{Z}) : \operatorname{im}\rho] \leqslant 2$. But if the index is 2, then K is trivial, meaning $-I$ doesn't lie in $\operatorname{im}\rho$ (injectivity). Hence $\pm \operatorname{im}\rho$ is the whole group $SL_2(\mathbb{Z}/N\mathbb{Z})$, suggesting one of $\pm S$ is in $\operatorname{im}\rho$. This means $-I = (-S)^2 \in \operatorname{im}\rho$, a contradiction. □

We will use the following result without proving it — this is quite nontrivial.

Theorem 5.2.3. *The function fields $\mathbb{Q}(j, f_0)$ and $\mathbb{Q}(j, f_1)$ define projective nonsingular curves $X_0(N)$ and $X_1(N)$ whose $\mathbb{C}$-points are isomorphic to the complex modular curves.*

Proof. One must argue about the action of Galois groups of the two fields in the theorem. Indeed, there is an injective representation ρ on their Galois group with surjective determinant. This means the fields are function fields of some projective nonsingular curves. □

One of the most amazing results in modern mathematics is the proof of Fermat's last theorem due to Andrew Wiles and Kenneth Ribet. Ribet's theorem suggests Taniyama-Shimura implies Fermat's last theorem. Following this path, Wiles proved an equivalent of the modularity theorem (which was known as the Taniyama-Shimura conjecture):

Theorem 5.2.4 (modularity theorem)**.** *Let E be an elliptic curve over $\mathbb{Q}$. Then for some positive N there is a surjective morphism of algebraic curves over $\mathbb{Q}$:*

$$X_0(N) \to E$$

Definition 5.2.1. We call the smallest N in the previous theorem the **analytic conductor of** E.

The theorem above has a complexified version:

Theorem 5.2.5 (modularity theorem)**.** *Let E be a complex elliptic curve with rational j-invariant. Then for some positive integer N there is a surjective holomorphic map of Riemann surfaces:*

$$X_0(N) \to E$$

Remark 5.2.3. This version can be deduced from the rational version, as E can be considered as the $\mathbb{C}$-points of the universal elliptic curve $E_{j(E)}$ which has the same j-invariant and is defined over $\mathbb{Q}$. Then a surjective morphism of algebraic curves easily induces a surjective holomorphic map of complex manifolds. The converse is hard.

5.2.3 As moduli spaces

The main reference for this section is [KM85], although I will only take a few statements from this text to motivate some discussions in the following sections. The text follows the Grothendieck fashion of putting everything in the language of schemes, making some of the notations crazily sophisticated or lacking explanation. This also made it so hard for the readers to follow the text. If one gets confused with any term not properly defined in this text, and is uncertain what the term truly means, the rest of the paragraph becomes incomprehensible. Thanks to the great notes of [Par03], I was able to get a general view of what's going on. In this section $Y(N)$, $Y_0(N)$ and $Y_1(N)$ no longer refer to the modular curves but only three moduli spaces.

In this section we will also see one (probably a priori) reason why the three types of congruence subgroups $\Gamma(N)$, $\Gamma_0(N)$ and $\Gamma_1(N)$ are so important, and how they are related to elliptic curves.

Given any ring R, we consider the **category of elliptic curves over** R, Ell/R. An elliptic curve in this category is a proper smooth curve E over an R-scheme S (that is, we have a proper smooth morphism from the algebraic curve $E \to S$), with geometric fibers are smooth curves of genus 1, given with a section $\mathcal{O} : S \to E$. By geometric fibers we mean the pullbacks $E_x = E \times_S \operatorname{Spec} R$ via a geometric point $\operatorname{Spec} R \to S$. Vaguely speaking, this definition does nothing else but parametrizing a family of elliptic curves with the scheme S. Elliptic curves over S also have group laws:

Theorem 5.2.6. *Each $\pi : E \to S$ is a commutative group scheme such that for any S-scheme T and any three T-points P, Q, R of the base change $\pi_T : E_T \to S$, we have*

$$P + Q = R$$

if and only if there is some invertible sheaf $\mathcal{L}$ on T such that

$$\mathcal{I}^{-1}(P) \otimes \mathcal{I}^{-1}(P) \otimes \mathcal{I}(\mathcal{O}) \cong \mathcal{I}^{-1}(R)\mathcal{I}(P) \otimes \pi_T^*(\mathcal{L})$$

where $\mathcal{I}^{-1}(P)$ is the inverse of the invertible ideal sheaf $\mathcal{I}(P)$ of P.

Indeed, the proof of this group law is similar to the classical case; one only needs to replace the Picard group of divisors with its scheme-theoretic variety version.

Let N be a positive integer, then we can define the map $[N] : E \to E$.

Theorem 5.2.7. *The S-morphism $[N] : E/S \to E/S$ is finite locally free of rank N^2, and its kernel is locally isomorphic to $(\mathbb{Z}/N\mathbb{Z})^2$ if N is invertible in the affine rings of S.*

Theorem 5.2.8. *If $f : E_1 \to E_2$ an S-homomorphism of elliptic curves over S, then locally $f = \mathcal{O}$ or f is an isogeny.*

A **moduli problem** for elliptic curves is defined in the usual way, that is, a contravariant functor $\mathcal{F} : \operatorname{Ell}/R \to \operatorname{Set}$. The goal is to find a scheme representing the functor.

The case of $\Gamma_1(N)$

Consider the moduli problem

$$S_1(N) : S \mapsto \{(E, P) : E \in \mathrm{Ell}/S, P \in E(S) \text{ has order } N \text{ in all geometric fibers}\}/\sim$$

where the equivalence relation is given by isogenies preserving the order N point.

We need to specify the base scheme of this moduli problem. Suppose $S = \operatorname{Spec} K$ for some number fields K and $\mathfrak{p}$ a finite prime of K such that $\mathfrak{p} \nmid N$. Although we are talking about schemes, I actually think about the reductions of classical curves to get a good understanding of what's going on. In fact the phenomenon is quite easy to understand. Suppose E has good reduction modulo $\mathfrak{p}$, then the reduction of P has exact order N in $E/\mathfrak{o}_{K_\mathfrak{p}}$. But for primes $\mathfrak{p} \mid N$, E might have bad reductions or the reduction of P no longer has order N in $E(K_\mathfrak{p})$. But the scheme $\operatorname{Spec} \mathbb{Z}[1/N]$ consists of, naively, all prime ideals $p\mathbb{Z}[1/N]$ for $p \nmid \mathbb{Z}[1/N]$. Therefore, when we perform the reduction over $\mathbb{Z}[1/N]$, no prime divisors of N would be considered. Thus, the moduli problem $S_1(N)$ is a functor on $\mathbb{Z}[1/N]$-schemes.

Theorem 5.2.9. *For any $N \geqslant 4$, the moduli problem $S_1(N)$ has a fine moduli space $Y_1(N)$.*

Proof. We won't prove this. But we will illustrate a classic result that derives this theorem.

Theorem 5.2.10. *The functor*

$$\mathcal{F} : S \mapsto \{(E, P) : P \textit{ is not of order } 1, 2, 3\}/\sim$$

is represented by Y : $\operatorname{Spec}(\mathbb{Z}[B, C, \Delta(B, C)^{-1}])$ with the universal family $(E(B, C), (0, 0))$.

Here $E(B, C)$ is the curve define by $y^2 + (1 - C)xy - By = x^3 - Bx^2$ and $\Delta(B, C)$ its discriminant.

We pullback Y of the diagonal of $E(B, C) \times_Y E(B, C)$ along the map $\mathcal{O} \times [N](0, 0)$, obtaining a scheme Y_N. Intuitively the S-points of this schemes classify pairs (E, P) such that E is an elliptic curve over S and P an S-point not of order 1, 2, or 3 but $[N]P = \mathcal{O}$. Then taking the complements of the subschemes Y_d for all $d < N$ dividing N, we get $Y_1(N)$. □

Theorem 5.2.11. *The complex points of $Y_1(N)$ is precisely the modular curve $\Gamma_1(N)\backslash\mathbb{H}$.*

The case of $\Gamma_0(N)$

We also wish to represent the functor $S \mapsto \{(E/S, C)\}/\sim$ where C/S is a subgroup scheme of E/S étale locally isomorphic to the constant scheme $\mathbb{Z}/N\mathbb{Z}$. But it turns out the functor is not representable, and thus we can only look for coarse moduli spaces. Coarse moduli spaces are enough for this report — they can be used to parametrize the geometric points of the functor and they are the best approximation of the functor we can obtain!

The diamond operator acts on $Y_1(N)$ by $d : (E, P) \mapsto (E, [d]P)$. Since P has order N, the orbit of P is a cyclic subgroup scheme of order N. Thus, we have $Y_0(N) = Y_1(N)/(\mathbb{Z}/N\mathbb{Z})^\times$, a coarse moduli space by geometric invariant theory. The $\mathbb{C}$-points of $Y_0(N)$ coincides with $\Gamma_0\backslash\mathbb{H}$.

The case of $\Gamma(N)$

The functor

$$S \mapsto \{(E, (P, Q)) : P, Q \text{ generate } E[N] \text{with Weil pairing } \varepsilon_N(P, Q) = e^{2\pi i N}\}/\sim$$

is representable by scheme $Y(N)$ whose complex points are $\Gamma(N)\backslash\mathbb{H}$.

Complex points

I now provide a full summary of $\mathbb{C}$-points of the moduli spaces. I will also verify they are isomorphic to the said quotients. The $\mathbb{C}$-points of $Y(N)$, $Y_1(N)$ and $Y_0(N)$ corresponds respectively to the sets

$$\begin{aligned}
S(N) &= \{(E,(P,Q)) : P, Q \text{ generate } E[N] \text{with Weil pairing } \varepsilon_N(P,Q) = e^{2\pi i N}\}/\sim \\
S_0(N) &= \{(E,C) : C \text{ a cyclic subgroup of } E[N] \text{ of order } N\}/\sim \\
S_1(N) &= \{(E,P) : P \in E \text{ a point of exact order } N\}/\sim
\end{aligned}$$

where the equivalence relations are defined by isomorphisms of elliptic curves that preserve the object in the second entry. Let $E_\tau = \mathbb{C}/\Lambda_\tau$.

Lemma 5.2.4. (i) $S(N) = \{[E_\tau, (\tau/N, 1/N)]\}$. *Two points are equal if and only if* $\Gamma(N)\tau = \Gamma(N)\tau'$. *There is a bijection from* $S(N)$ *to* $\Gamma(N)\backslash\mathbb{H}$ *sending* $[E_\tau, (1/N, \tau/N)]$ *to* $\Gamma(N)\tau$.

(ii) $S_0(N) = \{[E_\tau, \langle 1/N\rangle]\}$. *Two points are equal if and only if* $\Gamma_0(N)\tau = \Gamma_0(N)\tau'$. *There is a bijection from* $S_0(N)$ *to* $\Gamma_0(N)\backslash\mathbb{H}$ *sending* $[E_\tau, \langle 1/N\rangle]$ *to* $\Gamma(N)_0\tau$.

(iii) $S_1(N) = \{[E_\tau, 1/N]\}$. *Two points are equal if and only if* $\Gamma_1(N)\tau = \Gamma_1(N)\tau'$. *There is a bijection from* $S_1(N)$ *to* $\Gamma_1(N)\backslash\mathbb{H}$ *sending* $[E_\tau, 1/N]$ *to* $\Gamma_1(N)\tau$.

Proof. WLOG we only prove the lemma for $\Gamma_1(N)$. Fix some (E,Q). Then E is isomorphic to some $\mathbb{C}/\Lambda_{\tau'}$ and $Q = (c\tau' + d)/N$ for some $(c,d,N) = 1$ as Q has exact order N. Then we get some a, b, k such that $ad - bc - kN = 1$. Thus $\gamma = \left[\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right]$ sits in $SL_2(\mathbb{Z}/N\mathbb{Z})$ so we can lift it to $SL_2(\mathbb{Z})$. Let $\tau = \gamma(\tau')$. Then $z \mapsto (c\tau' + d)^{-1}z$ is an isomorphism from $\mathbb{C}/\Lambda_{\tau'}$ to $\mathbb{C}/\Lambda_\tau$ sending Q to $1/N$. It's easy to show the condition on equivalence of points in $S_1(N)$. □

5.2.4 Hecke operators on modular curves

Denote by α a matrix in $\Gamma_1(N)$ with its lower right corner congruent to d, and β_j (where β_∞ is the matrix in the expression of T_p for $p \nmid N$) the matrices in the explicit expression of T_p. We define $T_p : \Gamma_1(N)\tau \mapsto \sum_j \Gamma_1(N)\beta_j(\tau)$ and $\langle d\rangle : \Gamma_1(N)\tau \mapsto \Gamma_1(N)\alpha(\tau)$. The Hecke operators are therefore maps on $X_1(N)$ (although T_p lands on the divisor group).

This definition is completely natural. The Picard group of a compact Riemann surface is the Jacobian of that surface, and the Jacobian of modular curves are quotients of the dual of weight two cusps forms of level N. Therefore, the operators on cusps forms induces maps on the modular curves.

Hecke operators act on $\mathrm{Div}(X_1(N))$ in the following way. Consider the lattice Λ_τ. To each β_j associate a subgroup $C_j = c_j\Lambda_{\beta_j\tau}$ of Λ_τ where $c_j = 1$ if $j \neq \infty$ and $(N\tau + 1)$ otherwise. Then $\Lambda_{\beta_j\tau} = \frac{\tau+j}{p}\mathbb{Z} + \mathbb{Z}$ which clearly equals to $\left\langle \frac{\tau+j}{p} \right\rangle + \Lambda_\tau$; similarly

$$\Lambda_{\beta_\infty\tau} = \frac{pm\tau + n}{p}\mathbb{Z} + \mathbb{Z} = \frac{n}{p}\mathbb{Z} + \tau\mathbb{Z} + \mathbb{Z}$$

which is $\left\langle \frac{1}{p} \right\rangle + \Lambda_\tau$. Then $C_j \cong \mathbb{Z}/p\mathbb{Z}$ and $C_j \cap \langle 1/N\rangle = 0$. The groups are pairwise disjoint except for 0 and they sum up to a total of $1 + (p+1)(p-1) = p^2 = \#E_\tau[p]$ elements. Therefore, any cyclic subgroup of order p is one of C_j. Thus, the Hecke operator induces a map on the divisor group of $S_1(N)$ (map the points of $Y_1(N)$ to $S_1(N)$ via $\Gamma_1(N)\tau \mapsto [E_\tau, 1/N]$):

$$T_p : \mathrm{Div}(S_1(N)) \to \mathrm{Div}(S_1(N)), \quad [E,Q] \mapsto \sum_{C \cong \mathbb{Z}/p\mathbb{Z}, C \cap \langle Q\rangle = 0} [E/C, Q + C]$$

For $\langle d\rangle$, the lattice $\Lambda_{\alpha\tau}$ is isomorphic to Λ_τ via the map $z \mapsto mz$ where $m = c\tau + d$. Under this isomorphism the point $1/N$ is sent to $(c\tau + d)/N \equiv d/N \pmod{\Lambda_\tau}$ since $c \equiv 0 \pmod{N}$. Thus,

$$\langle d\rangle_* : \mathrm{Div}(S_1(N)) \to \mathrm{Div}(S_1(N)), \quad [E,Q] \mapsto [E,[d]Q]$$

Is the pushforward of the map $\langle d\rangle$ that sends $[E, Q]$ to $[E, [d]Q]$ and $\Gamma_1(N)\tau$ to $\Gamma_1(N)\alpha(\tau)$. Note that T_p is not the pushforward of some map on the moduli spaces since it sends a point to a formal sum of points, so its image does not lie in the moduli spaces.

From now we start working with the algebraic curves $X_1(N)$ over $\mathbb{Q}$. The descriptions above for Hecke operators are specifically for the complex points of $X_1(N)$. We claim that T_p is defined over $\mathbb{Q}$, so we may restrict T_p to the $\mathbb{Q}$-points and get an endomorphism from the divisor group of the curve $X_1(N)$ over $\mathbb{Q}$. To wit this, it suffices to show $\langle d\rangle^*$ and T_p^* are both defined over $\mathbb{Q}$. Say α_d is a matrix defining $\langle d\rangle$. Note $\alpha_d^* j = j$ so we won't worry about this generator. But for f_1, we have $\alpha_d^* f_1 = f_0^{\pm(0,d)}$, the x-coordinate of $[\pm d]Q$. So $\alpha_d^* f_1(\tau)$ is an element of $\mathbb{Q}(j(\tau), E_{j(\tau)}[N])$. The Galois group of $\mathbb{Q}(X_1(N))$ has images $\{\pm \left[\begin{smallmatrix} a & b \\ 0 & 1 \end{smallmatrix}\right]\}$ in $GL_2(\mathbb{Z}/N\mathbb{Z})$ which preserve $[\pm d]Q$. Thus, $\alpha_d^* f_1$ sits inside $\mathbb{Q}(j, f_1)$. Furthermore, the Hecke operators on the complex $S_1(N)$ and the map $[\mathbb{C}/\Lambda_\tau, 1/N] \mapsto \Gamma_1(N)\tau$ preserve divisors of degree 0. The double coset operator is a composition of reverse and forward maps, so it induces a map on the Picard group. We finally arrive at the following commutative diagrams.

$$\begin{tikzcd}
\mathrm{Div}^0(S_1(N)) \arrow[r, "T"] \arrow[d, "\varphi"'] & \mathrm{Div}^0(S_1(N)) \arrow[d, "\varphi"] \\
\mathrm{Pic}^0(X_1(N)) \arrow[r, "T"] & \mathrm{Pic}^0(X_1(N))
\end{tikzcd}$$

where T is either T_p or $\langle d\rangle_*$.

5.3 Eichler-Shimura

The last section of this chapter is dedicated to the Eichler-Shimura relation, detailing the relation between Hecke operators and Frobenius morphisms.

5.3.1 Reduction of curves

Recall on an algebraic curve C over an $\mathbb{F}_p$-scheme S (or more generally, an S-scheme), there is a Frobenius morphism $\mathrm{Frob}_p : C \to C$ induced by the algebra homomorphism (because of the characteristic p) $x \mapsto x^p$ on the defining algebras of C. This morphism actually factors through $C^{(p)}$ where $C^{(p)}$ is the pullback $C \times_S S$ along the map $C \to S$ and the $\mathrm{Frob}_p : S \to S$ on S. In the affine or projective case, if $C = \operatorname{Spec} B$ and $S = \operatorname{Spec} A$ where B is the A-algebra defined by some (homogeneous in case of projective curves) ideal $(f_1, \dots, f_n)$ of $A[X_1, \dots, X_n]$, then $C^{(p)}$ is the scheme defined by $(f_1^p, \dots, f_n^p)$. The Frobenius map from $C \to C^{(p)}$ is therefore given by $(x_1, \dots, x_n) \mapsto (x_1^p, \dots, x_n^p)$ (we factorize the Frobenius endomorphism on C, and abuse the name "Frobenius map" a little). If C is itself defined over $\mathbb{F}_p$, then the defining ideals of C and $C^{(p)}$ would be the same, meaning $C = C^{(p)}$ in this case. Let V denote the dual isogeny of the Frobenius map on elliptic curves, called the **Verschiebung**.

I will also recall some facts from algebraic curves. Given a surjective morphism $h : C \to C'$ of nonsingular projective curves over $\overline{\mathbb{F}_p}$, we may decompose h as h_{sep} and h_{insep} using the pullback $h*$ which factors through the maximal separable extension of the function field of C'. Note that h_{insep} is Frob_p^e for the inseparable degree $p^e = [\overline{\mathbb{F}_p}(C) : \overline{\mathbb{F}_p}(C')_{\text{sep}}]$. The Frobenius map is purely inseparable of degree p. Also note that the separable degree of an isogeny of elliptic curves is the size of its kernel. The p-torsion group of an elliptic curve E is either trivial or isomorphic to $\mathbb{Z}/p\mathbb{Z}$, so the map $[p]$ is not separable. If E is instead an elliptic curve over $\mathbb{F}_p$, the Frobenius map naturally acts on the Picard group of E by

$$\mathrm{Frob}_{p,*} : (P) \mapsto (\mathrm{Frob}_p(P)), \quad \mathrm{Frob}_p^* : (P) \mapsto p(\sigma_p^{-1}(P))$$

since the map is bijective and ramified everywhere with ramification degree p.

Definition 5.3.1. Let E be an elliptic curve over $\mathbb{Q}$ in reduced form. Let p be a prime and $\bar{E}$ the reduction of E modulo p. Then

$$a_p(E) = p + 1 - \#\bar{E}(\mathbb{F}_p).$$

Lemma 5.3.1. *Suppose E has good reduction modulo p. Then*

$$[a_p(E)] = \mathrm{Frob}_{p,*} + \mathrm{Frob}_p^*$$

on the Picard group of $\bar{E}$.

Proof. The $\mathbb{F}_p$-points of $\bar{E}$ is precisely the fixed group of Frob_p. Therefore,

$$\bar{E}(\mathbb{F}_p) = \ker(\mathrm{Frob}_p - \mathrm{id}).$$

Since $\mathrm{Frob}_p - 1$ is separable (otherwise there is some morphism f such that $\mathrm{Frob}_p - 1 = f \circ \mathrm{Frob}_p$ which means Frob_p is an isomorphism, a contradiction), its degree is the separable degree which is the size of its kernel. Thus,

$$[\#\bar{E}(\mathbb{F}_p)] = (\mathrm{Frob}_{p,*} - \mathrm{id})(\mathrm{Frob}_p^* - \mathrm{id}) = p + 1 - \mathrm{Frob}_{p,*} - \mathrm{Frob}_p^*$$

□

Let C be a nonsingular affine curve over $\mathbb{Q}$ defined by a homogeneous ideal I in $\mathbb{Z}_{(p)}[X]$. We say

Definition 5.3.2. C has a **good reduction at** p if I is prime and the reduction of I in $\mathbb{F}_p[X]$ defines a smooth affine curve $\bar{C}$, called **the reduction of** C **at** p.

For projective cases we require the affine open of C to be empty modulo p or to have a good reduction at p. For curves over $\bar{\mathbb{Q}}$, simply replace $\mathbb{Z}$ by $\bar{\mathbb{Z}}$, $\mathbb{F}_p$ by $\overline{\mathbb{F}_p}$ and p by an ideal $\mathfrak{p}$ of $\bar{\mathbb{Z}}$ lying above p. We say an elliptic curve has an **ordinary** good reduction at $\mathfrak{p}$ if $\bar{E}[p] \cong \mathbb{Z}/p\mathbb{Z}$ and a **supersingular reduction** if $\bar{E}[p] = 0$ (by the structure theorem of torsion subgroups of elliptic curves, $\bar{E}[p]$ is either trivial or $\mathbb{Z}/p\mathbb{Z}$); in case of bad reductions, the reduction is **multiplicative** if the singular point in the reduction is a node in which case the reduction **split** if the tangent slopes at the node lie in $\mathbb{F}_p^\times$, and the reduction is **additive** if the singular point is a cusp. We will not prove the following very important theorem.

Theorem 5.3.1. *Let C be a nonsingular projective algebraic curve over $\mathbb{Q}$ with good reduction at p. The map on degree zero divisors induced by reduction sends principal divisors to principal divisors and thus it defines a surjection of Picard groups. Let C' be another curve of the same type with positive genus, and $h : C \to C'$ a morphism over $\mathbb{Q}$. Then the following diagram commutes:*

$$\begin{tikzcd}
\mathrm{Pic}(C) \arrow[r, "h_*"] \arrow[d] & \mathrm{Pic}(C') \arrow[d] \\
\mathrm{Pic}(\bar{C}) \arrow[r, "\bar{h}_*"] & \mathrm{Pic}(\overline{C'})
\end{tikzcd}$$

Let $S_1(N)'_g$ be the family $\{[E, Q] : E \text{ has good reduction at } \mathfrak{p}, j(E) \neq 0, 1728 \pmod{\mathfrak{p}}\}$, $\overline{S_1(N)}'$ be the moduli problems of elliptic curves over $\mathbb{F}_p$ with j-invariant not equal to $0, 1728$. Then

Theorem 5.3.2 (Igusa). *The modular curves $X_1(N)$ has good reduction at $p \nmid N$, and the diagram*

$$\begin{tikzcd}
S_1(N)'_g \arrow[r] \arrow[d] & X_1(N) \arrow[d] \\
\overline{S_1(N)}' \arrow[r] & \overline{X_1(N)}
\end{tikzcd}$$

where the vertical map on the left is the reduction map $[E, Q] \mapsto [\bar{E}, \bar{Q}]$.

5.3.2 The Eichler-Shimura congruence

By Theorem 5.3.1, we obtain a commutative diagram

$$\begin{tikzcd}
\mathrm{Pic}(X_1(N)) \arrow[r, "\langle d\rangle_*"] \arrow[d] & \mathrm{Pic}(X_1(N)') \arrow[d] \\
\mathrm{Pic}(\overline{X_1(N)}) \arrow[r, "\overline{\langle d\rangle}_*"] & \mathrm{Pic}(\overline{X_1(N)'})
\end{tikzcd}$$

The aim is to find a similar diagram for the Hecke operator. We already know the two vertical maps and the map on top which is the protagonist T_p.

Let E be an elliptic curve over $\bar{\mathbb{Q}}$ with ordinary reduction at $\mathfrak{p}$, a prime lying above p and Q a point of order N. Let C_0 be the kernel of the reduction $E[p] \mapsto \bar{E}[p]$, which is a group of order p since the map is surjective, $E[p] = (\mathbb{Z}/p\mathbb{Z})^2$ and $\bar{E}[p] = \mathbb{Z}/p\mathbb{Z}$. We proceed to prove this extremely important lemma.

Lemma 5.3.2. *For any subgroup C of order p,*

$$[\overline{E/C}, \overline{Q+C}] = \begin{cases} [\bar{E}^{(p)}, \mathrm{Frob}_p(\bar{Q})], & C = C_0 \\ [\bar{E}^{(-p)}, [p]\,\mathrm{Frob}_p^{-1}(\bar{Q})], & C \neq C_0 \end{cases}$$

Proof. The proof reduces to one *superbly crucial* fact: an isogeny of elliptic curves over $\mathbb{F}_p$ is either the Frobenius map or the Verschiebung. Suppose $C = C_0$. Let $E' = E/C$, $Q' = Q + C$ and φ the quotient isogeny with dual ψ. Then since E has ordinary reduction at $\mathfrak{p}$, its isogenous image E' also has. The kernel of ψ has p elements as $\deg\psi = \deg\varphi = \#\ker\varphi = p$. Therefore, together with the fact that $E[p] = (\mathbb{Z}/p\mathbb{Z})^2$, the image of $E'[p]$ under ψ has order p. We also obverse $\varphi(\psi(E'[p])) = [p]E'[p] = 0$ so $C = \psi(E'[p]) = C_0$. The map $\bar{\psi}$ is zero on $\overline{E'}[p]$ since the reduction $E'[p] \to \overline{E'}[p]$ surjects. One can deduce $\overline{E'}[p] = \ker\bar{\psi}$.

Good reductions preserve degrees of isogenies, so $\deg\bar{\psi} = \deg\bar{\varphi} = p$, and $\deg[p] = p^2$ on $\bar{E}'$. The kernel of $[p]$, $\overline{E'}[p]$, coincides with the kernel of $\bar{\psi}$ so $[p]$ has separable and inseparable degree of p. Similarly, $\bar{\psi}$ has separable degree p and inseparable degree 1. Therefore, $\bar{\varphi}$ is purely inseparable of degree p, meaning it's the composition of Frob_p on $\overline{E'}$ and the isomorphism $\bar{E}^{(p)} \xrightarrow{\sim} \overline{E'}$ taking $\mathrm{Frob}_p(\bar{Q})$ to $\overline{Q}$, completing the proof.

Now if $C \neq C_0$, with the same notation we consider the map φ and its reduction $\bar{\varphi}$. Let $C' = \ker\psi$ and C_0' the kernel of the reduction map $E'[p] \to \overline{E'}[p]$. With the exact same argument, we may show $C' = C_0'$ and furthermore that $\bar{\psi}$ is the composition of the Frobenius and an isomorphism from $\overline{E'}^{(p)}$ to $\bar{E}$ taking $\mathrm{Frob}_p(\overline{Q'})$ to $[p]\bar{Q}$ applying Frob_p to the curve and the point we get the desired isomorphism. □

Recall what I said at the beginning of the proof: an isogeny of elliptic curves over $\mathbb{F}_p$ is either the Frobenius map or the Verschiebung. Let's make another *important observation*: there are $p+1$ degree p isogenies on E, all but one, which reduces to the Frobenius map, reduce to the Verschiebung, meaning there are p numbers of such map on the reduction. In the language of subgroups of E, there $p+1$ subgroups of E of order p, one of which is C_0. Thus, we have

$$\sum_{C \cong \mathbb{Z}/p\mathbb{Z}} [\overline{E/C}, \overline{Q+C}] = \left(\mathrm{Frob}_p + p\overline{\langle p\rangle}\,\mathrm{Frob}_p^{-1}\right)[\bar{E}, \bar{Q}]$$

We are summing over all subgroups of order p because Q has order N so $\langle Q\rangle \cap C$ is trivial for all C of order $p \nmid N$.

When the good reduction of E at $\mathfrak{p}$ is supersingular, it is also easy to find out

$$[\overline{E/C}, \overline{Q+C}] = [\bar{E}^{(p)}, \mathrm{Frob}_p(\bar{Q})] = [\bar{E}^{(-p)}, [p]\,\mathrm{Frob}_p^{-1}(\bar{Q})]$$

in this case, using the same argument. We thus have a commutative diagram:

$$\begin{tikzcd}
\mathrm{Div}^0(S_1(N)'_g) \arrow[r, "T_p"] \arrow[d] & \mathrm{Div}^0(S_1(N)'_g) \arrow[d] \\
\mathrm{Div}^0(\overline{S_1(N)}') \arrow[r, "\mathrm{Frob}_p + p\overline{\langle p\rangle}\,\mathrm{Frob}_p^{-1}"] & \mathrm{Div}^0(\overline{S_1(N)}')
\end{tikzcd}$$

On the other hand, we have another commutative diagram:

$$\begin{tikzcd}
\mathrm{Div}^0(\overline{S_1(N)}') \arrow[r, "\mathrm{Frob}_p + p\overline{\langle p\rangle}\,\mathrm{Frob}_p^{-1}"] \arrow[d] & \mathrm{Div}^0(\overline{S_1(N)}') \arrow[d] \\
\mathrm{Pic}(\overline{X_1(N)}) \arrow[r, "\mathrm{Frob}_{p,*} + \overline{\langle p\rangle}_*\,\mathrm{Frob}_p^*"] & \mathrm{Pic}(\overline{X_1(N)})
\end{tikzcd}$$

For an explicit proof of this diagram, we may use the planar model of the modular curve $X_1(N)$ given by pairs (j,x) where j is the j-invariant of E and x the x-coordinate of Q in the class $[E,Q]$. This planar model is birational to the actual modular curve over $\mathbb{Q}$, and thus proving the diagram for the planar model is the same as proving the diagram above. The only subtlety is that Frob_p^* sends a point (j,x) in the planar model to $p(\mathrm{Frob}_p^{-1}(j), \mathrm{Frob}_p^{-1}(x))$.

Theorem 5.3.3 (Eichler-Shimura)**.** *Let $p \nmid N$. Then the following diagram commutes:*

$$\begin{tikzcd}
\mathrm{Pic}(X_1(N)) \arrow[r, "T_p"] \arrow[d] & \mathrm{Pic}(X_1(N)) \arrow[d] \\
\mathrm{Pic}(\overline{X_1(N)}) \arrow[r, "\mathrm{Frob}_{p,*} + \overline{\langle p\rangle}_*\,\mathrm{Frob}_p^*"] & \mathrm{Pic}(\overline{X_1(N)})
\end{tikzcd}$$

Restricted to $\bar{X}_0(N)$ on which $\overline{\langle p\rangle}$ is trivial, we have

$$\begin{tikzcd}
\mathrm{Pic}(X_1(N)) \arrow[r, "T_p"] \arrow[d] & \mathrm{Pic}(X_1(N)) \arrow[d] \\
\mathrm{Pic}(\overline{X_1(N)}) \arrow[r, "\mathrm{Frob}_{p,*} + \mathrm{Frob}_p^*"] & \mathrm{Pic}(\overline{X_1(N)})
\end{tikzcd}$$

Proof.

$$\begin{tikzcd}
 & \mathrm{Pic}(X_1) \arrow[rr, magenta, "T_p"] \arrow[dd, teal] & & \mathrm{Pic}(X_1) \arrow[dd, lime] \\
\mathrm{Div}^0(S'_{1,g}) \arrow[ur, green] \arrow[rr, red, "T_p"] \arrow[dd, blue] & & \mathrm{Div}^0(S'_{1,g}) \arrow[ur, orange] \arrow[dd, pink] & \\
 & \mathrm{Pic}(\bar{X}_1) \arrow[rr, "\mathrm{Frob}_{p,*} + \overline{\langle p\rangle}_*\,\mathrm{Frob}_p^*"] & & \mathrm{Pic}(\bar{X}_1) \\
\mathrm{Div}^0(\bar{S}'_1) \arrow[ur, yellow] \arrow[rr, purple, "\mathrm{Frob}_p + p\overline{\langle p\rangle}\,\mathrm{Frob}_p^{-1}"] & & \mathrm{Div}^0(\bar{S}'_1) \arrow[ur, olive] &
\end{tikzcd}$$

It remains to show the back square of this diagram commutes, since the top and bottom were just proved. The two sides are Igusa Theorem 5.3.2.

We have

$$\text{Green} + \text{Magenta} + \text{Lime} = \text{Blue} + \text{Yellow} + \text{Black} = \text{Green} + \text{Teal} + \text{Black}$$

and assuming there is some $\overline{T_p}$ on the black arrow that could make the diagram commute (nontrivial, without proof),

$$\text{Green} + \text{Magenta} + \text{Lime} = \text{Green} + \text{Teal} + \overline{T_p}.$$

Then as $\overline{\text{Green} + \text{Teal}}$ is surjective, we must have the reduction of T_p equal to Black $= \text{Frob}_{p,*} + \overline{\langle p \rangle}_* \text{Frob}_p^*$. □

5.3.3 The Taniyama-Shimura conjecture

We claim, without proof, the following version of the modularity theorem:

Theorem 5.3.4 (modularity theorem). *Let E be an elliptic curve over $\mathbb{Q}$ with analytic conductor N_E. Then for some newform $f \in S_2(\Gamma_0(M_f))$ where $M_f \mid N$, $a_p(f) = a_p(E)$ for all $p \nmid N_E N$.*

Proof. The proof is rather difficult, but we will summarize the main idea. Let N be a positive integer and α nonzero morphism of curves over $\mathbb{Q}$ from $X_0(N)$ to E which exists b Theorem 5.2.4. Let f be a weight 2 newform of level M_f. Then its Fourier coefficient $a_p(f)$ is T_p. We pass the form and T_p to the abelian variety associated to f. The sum of all such abelian varieties is isogenous to $\text{Pic}^0(X_0(N))$, and then the Hecke operator acts and reduces to $\text{Frob}_{p,*} + \text{Frob}_p^*$. But the reduction of α_* commutes with the map, and thus T_p is the map $\text{Frob}_{p,*} + \text{Frob}_p^*$ on $\text{Pic}(\bar{E})$, which simply equals to $a_p(E)$. I won't prove the existence. □

We define the local zeta factor of E to be

$$Z_p(p^{-s}, E) = \frac{1}{1 - a_p(E)p^{-s} + 1_E(p)p^{1-2s}}$$

where 1_E equals 1 at good reductions and 0 at bad reductions.

Definition 5.3.3. The **Hasse-Weil L-function** of E is

$$L(s, E) = \prod_p Z_p(p^{-s}, E) = \prod_p \frac{1}{1 - a_p(E)p^{-s} + 1_E(p)p^{1-2s}}$$

Now given a newform f of in $\mathcal{S}_2(\Gamma_0(N_E))$ where E is the conductor of E, by Theorem 4.3.3, its L-function is

$$L(s, f) = \prod_p \frac{1}{1 - a_p p^{-s} + \chi(p)p^{k-1-2s}}$$

But since $f \in \mathcal{S}_2(\Gamma_0(N_E))$ $(k = 2)$, $\langle p \rangle$ acts trivially on f, so it lives in $\mathcal{M}_k(N, 1_{N_E})$. The character 1_{N_E} is precisely the character 1_E. Therefore,

Theorem 5.3.5 (modularity theorem). *Let E be an elliptic curve over $\mathbb{Q}$ with analytic conductor N_E. Then for some newform $f \in S_2(\Gamma_0(N_E))$*

$$L(s, f) = L(s, E).$$

This was called the Taniyama-Shimura conjecture (which was proved by Wiles and generalized in a joint paper of Breuil, Conrad, Diamond and Taylor). We say an elliptic curve over $\mathbb{Q}$ is **modular** if its L-function arises from a cusp form of weight 2 level N.

Theorem 5.3.6 (Taniyama-Shimura). *Every elliptic curve over $\mathbb{Q}$ is modular.*

5.4 What's more?

We have shown: (1) L-functions of finite order Hecke characters equal the L-functions of one dimensional Galois representations by class field theory and (2) L-functions of elliptic curves arise from newforms of weight 2 by Eichler-Shimura and the modularity theorem. Robert Langlands, in a letter [Lan67] to Weil, outlined one of the greatest ideas in modern mathematics. He listed a collection of conjectures of which this is the most relevant one: if K is a number field, there is a one-to-one correspondence

$$\{\text{automorphic representations of } GL_n(\mathbb{A}_K)\} \leftrightarrow \{n\text{-dimensional Galois representations } \rho \text{ of } K\}$$

such that the L-function attached to each side is the same.

Note that we may attach Galois representations to elliptic curves (beyond the scope of this paper), and Taniyama-Shimura would give a partial correspondence between automorphic representations and Galois representations when $n = 2$ and $K = \mathbb{Q}$. We say it's partial because not all automorphic representations of $GL_2(\mathbb{A}_\mathbb{Q})$ arise from modular form — there are those arising from *Mass forms*, a generalized version of modular forms that are eigenforms of a hyperbolic Laplacian.

Note that $PSL_2(\mathbb{R})$ acts on $\mathbb{H}$ transitively, and the stabilizer of i is $S = SO(2)/\{\pm I\}$. Thus, $\mathbb{H} \cong PSL_2(\mathbb{R})/S$. Then modular forms with respect to a congruence subgroup Γ are functions on $\Gamma\backslash PSL_2(\mathbb{R})$ (which is $\Gamma\backslash SL_2(\mathbb{R})$ when $-I \in \Gamma$, an usual assumption). As a consequence of the strong approximation Theorem 2.2.11 for algebraic groups, one has

$$\Gamma_0(N)\backslash SL_2(\mathbb{R}) \cong Z(\mathbb{A}_\mathbb{Q})GL_2(\mathbb{Q})\backslash GL_2(\mathbb{A}_\mathbb{Q})/K_0(N)$$

for $Z(\mathbb{A}_\mathbb{Q})$ the group of scalar matrices, $K_0(N)$ is the compact subgroup of $GL_2(\mathbb{Z}_p)$ if $p \mid N$ and the intersection of $GL_2(\mathbb{Z}_p)$ and $\Gamma_0(N)$ otherwise. We therefore relate modular form to functions on the adelic group (although very informally). This process, like what Tate did to Hecke characters Section 3.2, will be used to **adelize** classical modular forms along with some sophisticated constructions.

The theory of automorphic representations is extremely involved and technically demanding, so we can only use some of the terms to illustrate how this paper relates to Langlands' ideas while not knowing what they mean at all.

Bibliography

[Art24] E. Artin. “Über eine neue art von L-Reihen”. In: *Abhandlungen aus dem Mathematischen Seminar der Universität Hamburg* 3.1 (Dec. 1924), pp. 89–108. DOI: `10.1007/bf02954618`. URL: `https://doi.org/10.1007/bf02954618`.

[Bou14] Florian Bouyer. *Modular Curves.* 2014. URL: `https://warwick.ac.uk/fac/sci/maths/people/staff/fbouyer/modular_curves.pdf`.

[Bum04] Daniel Bump. *Automorphic Forms and Representations.* Cambridge Univ. Press, 2004.

[Cog06] James Cogdell. *On Artin L-Functions.* `https://people.math.osu.edu/cogdell.1/artin-www.pdf`. 2006.

[Con09] Keith Conrad. “History of Class Field Theory”. In: 2009.

[Cox14] David Cox. *Primes of the Form $x^2 + ny^2$.* John Wiley & Sons, Aug. 2014.

[DD13] Richard Dedekind and Peter Gustav Lejeune Dirichlet. “Über die Theorie der ganzen algebraischen Zahlen”. In: *Vorlesungen über Zahlentheorie.* Ed. by Richard Dedekind. Cambridge Library Collection - Mathematics. Cambridge University Press, 2013, pp. 434–627. DOI: `10.1017/CBO9781139237321.017`.

[DS05] Fred Diamond and Jerry Shurman. *A First Course in Modular Forms.* Springer, 2005.

[FC67] Albrecht Fröhlich and J. W. S. Cassels, eds. Thompson Book Company, Inc., 1967.

[Gau65] Carl Friedrich Gauss. *Disquisitiones Arithmeticae.* Trans. by Arthur A. Clarke. Yale University Press, 1965.

[GR02] Alexander Grothendieck and Michele Raynaud. *Revêtements étales et groupe fondamental (SGA 1).* 2002. DOI: `10.48550/ARXIV.MATH/0206203`. URL: `https://arxiv.org/abs/math/0206203`.

[Hei67] Hans Heilbronn. “Zeta-Functions and L-Functions”. In: *Algebraic Number Theory: Proceedings of an Instructional Conference Organized by the London Mathematical Society.* Ed. by Albrecht Fröhlich and J. W. S. Cassels. Thompson Book Company, Inc., 1967, pp. 204–230.

[Hil97] David Hilbert. “Die Theorie der algebraischen Zahlkörper”. In: *Jahresbericht der Deutschen Mathematiker-Vereinigung* 4 (1897), pp. 175–546.

[Ked23] Kiran Kedlaya. *Notes on Class Field Theory.* `https://kskedlaya.org/cft/book-1.html`. [Accessed Feburary 13th, 2023]. 2023.

[KM85] Nicholas M. Katz and Barry Mazur. *Arithmetic Moduli of Elliptic Curves.* Princeton University Press, 1985.

[Kum51] Ernst Kummer. “Mémoire sur la théorie des nombres complexes composés de racines de l’unité et de nombres entiers.” fre. In: *Journal de Mathématiques Pures et Appliquées* (1851), pp. 377–498. URL: `http://eudml.org/doc/235621`.

[Lan67] Robert Langlands. *Letter to André Weil.* 1967.

[Lem12] Franz Lemmermeyer. *What is the "ray" in ray class group?* MathOverflow, July 2012. URL: https://mathoverflow.net/q/101778 (visited on 01/27/2023).

[Mil20] J.S. Milne. *Class Field Theory (v4.03).* www.jmilne.org/math/. 2020.

[Mil86] J.S. Milne. "Jacobian Varieties". In: ed. by Gary Cornell and Joseph Silverman. Arithmetic Geometry. Springer New York, 1986. DOI: 10.1007-978-1-4613-8655-1. URL: https://doi.org/10.1007/978-1-4613-8655-1_7.

[Neu99] Jürgen Neukirch. *Algebraic Number Theory.* 1st ed. Springer Berlin, 1999. DOI: 10.1007-978-3-662-03983-0.

[Par03] James Parson. *Moduli of Elliptic Curves.* 2003. URL: https://math.stanford.edu/~conrad/vigregroup/vigre03/moduli.pdf.

[Poo15] Bjorn Poonenm. *Tate's Thesis.* https://math.mit.edu/~poonen/786/notes.pdf. 2015.

[Ser67] Jean-Pierre Serre. "Local Class Field Theory". In: *Algebraic Number Theory: Proceedings of an Instructional Conference Organized by the London Mathematical Society.* Ed. by Albrecht Fröhlich and J. W. S. Cassels. Thompson Book Company, Inc., 1967, pp. 129–160.

[Ser97] Jean-Pierre Serre. *Galois Cohomology.* Springer Berlin, Heidelberg, 1997.

[Sil94] Joseph Silverman. *Advanced Topics in the Arithmetic of Elliptic Curves.* Springer New York, 1994.

[Sny02] Noah Snyder. *Artin's L-functions: A Historical Approach.* 2002.

[Tat67a] John Tate. "Fourier Analysis in Number Fields and Hecke's Zeta-Functions". In: *Algebraic Number Theory: Proceedings of an Instructional Conference Organized by the London Mathematical Society.* Ed. by Albrecht Fröhlich and J. W. S. Cassels. Thompson Book Company, Inc., 1967, pp. 305–347.

[Tat67b] John Tate. "Global Class Field Theory". In: *Algebraic Number Theory: Proceedings of an Instructional Conference Organized by the London Mathematical Society.* Ed. by Albrecht Fröhlich and J. W. S. Cassels. Thompson Book Company, Inc., 1967, pp. 163–203.