L-functions in Number Theory

by

Yichao Zhang

A thesis submitted in conformity with the requirements
for the degree of Doctor of Philosophy
Graduate Department of Mathematics
University of Toronto

Abstract

L-functions in Number Theory

Yichao Zhang

Doctor of Philosophy

Graduate Department of Mathematics

University of Toronto

2010

As a generalization of the Riemann zeta function, L-function has become one of the central objects in Number Theory. The theory of L-functions, which produces a large family of consequences and conjectures in a unified way, concerns their zeros and poles, functional equations, special values and the connections between objects in different fields. Although most generalizations are largely conjectural, there are many existing results that provide us the evidence.

In this thesis, we shall consider some L-functions and look into some problems mentioned above. More explicitly, for the L-functions associated to newforms of fixed square-free level, we will consider an average version of the fourth moments problem. The final bound is proven by considering definite rational quaternion algebras and divisor functions in them, generalizing Maass Converse Theorem and one of Duke's result and eventually applying the solution to Basis Problem.

We then consider the problem of expressing the special value at $\frac{1}{2}$ of the Rankin-Selberg L-function associated to two newforms in terms of the Pertersson inner product, where one of the newforms is twisted by the derivative of some Eisenstein series.

Finally, we consider the Artin L-functions attached to irreducible 4-dimensional S_5-Galois representations and deal with the modularity problem. One sufficient condition on the modularity is given, which may help to find an affirmative example for Strong Artin Conjecture in this case.

Acknowledgements

The author is greatly indebted to his advisor, Professor Henry H. Kim, who suggested all the problems treated in this thesis. His constant guidance and support have been invaluable.

The author would also like to thank Professor Stephen Kudla for many valuable and inspiring conversations and comments and Professor James Arthur and Professor Valentin Blomer for the help during the work of this thesis.

The author is also grateful to Professor William Duke for agreeing to be the external examiner for this thesis.

The author thanks all of the faculty and the staff of the Department of Mathematics at University of Toronto for their wonderful help. Special thanks go to Ms. Ida Bulat, our graduate administrator, without whom the life at University of Toronto would never be easy and joyful for the author.

Lastly, the author would like to thank his wife, Hailing Liu, for all the sacrifices she has made these years. Without her company and support, this thesis could not have been completed.

List of Symbols

$\mathbb{C}$	the field of complex numbers
$\mathbb{R}$	the field of real numbers
$\mathbb{R}^+$	the field of complex numbers
$\mathbb{N}$	the set of non-negative rational integers
$\mathbb{Z}$	the ring of rational integers
$\mathbb{Z}^+$	the set of positive rational integers
$\mathbb{A}_F$	the ring of adeles of F
$\mathbb{A}_F^\times$	the group of ideles of F
$\mathcal{O}_F$	the ring of integers of F
F_v	the completion of F at v
$\mathcal{O}_{F,v}$	the completion of $\mathcal{O}_F$ at v
$R^\times$	the group of units in the ring R
$GL_2(R)$	the group of 2×2 matrices over the ring R with determinant in $R^\times$
$SL_2(R)$	the group of 2×2 matrices over the ring R of determinant one
$GL_2(\mathbb{R})^+$	elements of $GL_2(\mathbb{R})$ with positive determinant

$\Gamma(N)$	$\{\gamma \in SL_2(\mathbb{Z}) : \ \gamma \equiv I_{2\times 2} \bmod N\}$
$\Gamma_1(N)$	$\{\gamma \in SL_2(\mathbb{Z}) : \ a_\gamma \equiv d_\gamma \equiv 1 \bmod N, c_\gamma \equiv 0 \bmod N\}$
$\Gamma_0(N)$	$\{\gamma \in SL_2(\mathbb{Z}) : \ c_\gamma \equiv 0 \bmod N\}$
$\mathbb{H}$	the upper half plane of $\mathbb{C}$
c_χ	the conductor of the character χ
f^d	$f^d(z) = f(dz)$
$f\|_k\gamma$	weight k action of $\gamma \in GL_2(\mathbb{R})^+$
q	$e(z) = \exp(2\pi i z)$
$\mathcal{M}_k(\Gamma)$	the space of modular forms of weight k for the group Γ
$\mathcal{M}_k(N,\chi)$	the subspace of $\mathcal{M}_k(\Gamma_1(N))$ that $\Gamma_0(N)$ acts by Dirichlet character χ
$\mathcal{S}_k(\Gamma)$	the space of cusp forms of weight k for the group Γ
$\mathcal{S}_k(N,\chi)$	$\mathcal{S}_k(\Gamma_1(N)) \cap \mathcal{M}_k(N,\chi)$
$\mathcal{S}_k^{new}(N,\chi)$	the subspace of newforms in $\mathcal{S}_k(N,\chi)$
$\mathcal{S}_k^{old}(N,\chi)$	the subspace of oldforms in $\mathcal{S}_k(N,\chi)$
$T_k(n)$	n-th Hecke operator of weight k
$\mathbb{T}, \mathbb{T}_k$	the Hecke algebra of fixed weight$k$
$\zeta(s)$	the Riemann zeta function
$\zeta_{\mathcal{O}}(s)$	the zeta function associated to an order $\mathcal{O}$
$\zeta_F(s)$	the zeta function associated to the number field F
$L(s,\chi)$	the L-function attached to χ
$L(s,f)$	the L-function attached to the modular form f
$L(s,\rho)$	the L-function attached to the Galois representation ρ

$L_v(s,\cdot)$	the local factor at v of the L-function $L(s,\cdot)$
$\mathfrak{A}_F$	a quaternion algebra over the field F
$(a,b)_F$	the quaternion algebra generated as a vector space by $\{1,i,j,k\}$, whose ring structure is given by $i^2=a, j^2=b, ij=-ji=k$
$\mathfrak{A}_v$	the localization of $\mathfrak{A}$ at v, that is $\mathfrak{A}\otimes_F F_v$
$\mathfrak{A}_{\mathbb{A}}$	the ring of adeles of $\mathfrak{A}$
$\mathfrak{A}_{\mathbb{A}}^{\times}$	the group of ideles of $\mathfrak{A}$
$\mathfrak{A}_{\mathbb{A},f}^{\times}$	the group of finite ideles of $\mathfrak{A}$
$\mathcal{O}_l(M)$	the left order of M
$\mathcal{O}_r(M)$	the right order of M
$\mathfrak{a}_v$	the localization of $\mathfrak{a}$ at v, that is $\mathfrak{a}\otimes_{\mathcal{O}_F}\mathcal{O}_{F,v}$
$\mathfrak{b}\mid_l\mathfrak{a}$	$\mathfrak{b}$ divides $\mathfrak{a}$ from the left
$\mathfrak{a}\sim_l\mathfrak{b}$	$\mathfrak{a}$ and $\mathfrak{b}$ are left-equivalent
$H, H(\mathfrak{A})$	the class number of $\mathfrak{A}$
$\overline{\alpha}$	the conjugate of α
$Tr, Tr_{\mathfrak{A}/F}$	the reduced trace of $\mathfrak{A}_F$
$N, N_{\mathfrak{A}/F}$	the reduced norm of $\mathfrak{A}_F$
$d(\mathfrak{a})$	$\lvert\{(\mathfrak{b},\mathfrak{c}):\mathfrak{a}=\mathfrak{b}\mathfrak{c}\}\rvert$, the divisor function
$a(\mathfrak{n})$	the number of integral ideals (of fixed left order) of norm $\mathfrak{n}$
$\mathfrak{C}_{n+1}$	the Clifford algebra generated by $\{i_1,\cdots,i_n\}$ subject to $i_h^2=-1$, and $i_hi_k=-i_ki_h(k\neq h)$
V^{n+1}	$\{x=x_0+x_1i_1+\cdots+x_ni_n : x_i\in\mathbb{R}\}\subset\mathfrak{C}_{n+1}$

H^{n+1}	$\{x \in V^{n+1} : x_n > 0\}$
Δ_{n+1}	$x_n^{n+1} \sum_{h=0}^{n} \frac{\partial}{\partial x_h}(x_n^{1-n} \frac{\partial}{\partial x_h})$
$\mathcal{P}_m$	the space of spherical harmonics of degree m (in n variables)
$\sum_{\mathcal{P}_m}^{*}$	the summation over any orthonormal basis of $\mathcal{P}_m$

The following symbols are used in limiting process, say, as $x \to a$:

$f \ll g$	when x is close enough to a, $f(x) \leq A\|g(x)\|$ for some positive constant A
$f = O(g)$	$f \ll g$
$f = o(g)$	$\lim_{x \to a} \frac{f(x)}{g(x)} = 0$
$f \asymp g$	when x is close enough to a, $A_1\|g(x)\| \leq f(x) \leq A_2\|g(x)\|$ for some positive constants A_1 and A_2
$f \sim g$	$f - g = o(g)$

Contents

Chapter 1

Introduction

1.1 Generalized Lindelöf Hypothesis and Moments Problem

Conjecture 1.1.1 (Generalized Lindelöf Hypothesis) *Assume $L(s)$ is an L-function (over $\mathbb{Q}$) which admits meromorphic continuation to the whole s-plane and a functional equation under $s \leftrightarrow 1-s$. Then for any $\epsilon > 0$,*

$$L(\frac{1}{2} + it) = O(t^{\epsilon}).$$

Lindelöf conjectured this for the Riemann zeta function, namely, $\zeta(\frac{1}{2} + it) = O(t^{\epsilon})$. Note that the Riemann Hypothesis, which asserts that all of the non-trivial zeros of $\zeta(s)$ lie on the vertical line $Re(s) = \frac{1}{2}$, implies the Lindelöf Hypothesis. Actually the former is much stronger. Define

$$\mu(\sigma) = \inf\{a > 0 : \zeta(\sigma + it) = O(t^{a})\},$$

and Lindelöf Hypothesis states $\mu(\frac{1}{2}) = 0$. In 1908, Lindelöf proved that μ is convex and it follows that $\mu(\frac{1}{2}) \leq \frac{1}{4}$, which is called the convexity bound.

On the other hand, one can show that the Lindelöf Hypothesis for Riemann zeta

function is equivalent to the statement that the $2k$-th integral moment

$$\int_0^T |\zeta(\frac{1}{2}+it)|^{2k}dt = O(T^{1+\epsilon}), \text{ as } T \to \infty,$$

for all positive integers k and all positive real numbers ϵ. The latter is known for $k = 1, 2$, but for $k \geq 3$, it is still open.

For a general L-function $L(s)$, moments problems are the problems of providing non-trivial bounds for the moments of $L(s)$, namely, a result would take the form

$$\int_0^T |L(\frac{1}{2}+it)|^{2k}dt = O(T^a).$$

In Chapter 3 and 4, we will consider an average version of fourth moments problem for L-functions attached to newforms. This is first done by Duke [7] in the case of level $N = 2$, then generalized by Kim and the author [13] to general prime level $N = p$. In this thesis, we further generalize this result to general square-free level N.

Let us review Duke's idea briefly. Take a maximal order $\mathcal{O}$ in the Hamiltonian quaternion algebra $\mathfrak{A} = (-1, -1)_{\mathbb{Q}}$, and construct its zeta function $\zeta_{\mathcal{O}}(s)$. From this he obtained a Dirichlet series ϕ, which is essentially $\zeta_{\mathcal{O}}^2(s)$. This ϕ, as Duke proved, is a Dirichlet series of specific signature in the sense of Maass [17], that is, there is an automorphic function f associated to ϕ. With an asymptotic assumption on the summatory function of ϕ, he was able to give a (sharp) bound, as $T \to \infty$, for

$$\sum_{0<m\leq T} \sum_{\mathcal{P}_m}^* \int_{-T}^T |\phi(1+it)|^2 dt,$$

where $\sum_{\mathcal{P}_m}^*$ is over an orthogonal basis of the space $\mathcal{P}_m$ of spherical harmonics of degree m. This is Theorem 2 in [7], which is a generalization of Potter's result(see [27]).

On the other hand, since $\mathfrak{A}$ is definite, there is a two-by-two complex matrix representation of $\mathfrak{A}$, denoted by X_1. Let X_m be the symmetric m-th power of X_1 and the construction of Brandt matrices applies, so does that of theta (matrix) series (see [8] or [24]). It is known that the entries of $\sqrt{m+1}X_m$, considered as a function of the coordinate variables of $(-1, -1)_{\mathbb{R}}$ with respect to the canonical basis, constitute an orthonormal

basis of $\mathcal{P}_m$. Moreover, by analyzing the divisor function d of $\mathfrak{A}$, he obtained an identity, which is a quaternion prototype of the classical famous identity

$$\sum_{n=1}^{\infty} d(n)^2 n^{-s} = \frac{\zeta^4(s)}{\zeta(2s)}.$$

Such an identity provides the asymptotic assumption on the summatory function in Theorem 2 of [7]. The solution to Basis Problem given by Eichler [8] for square-free level and Theorem 2 mentioned above are applied to prove that, as $T \to \infty$,

$$\sum_{2<k\leq T} \sum_{f\in\mathcal{S}_k^{\mathrm{new}}(2)} \int_{-T}^{T} |L(\frac{k}{2}+it, f)|^4 dt \ll T^3 \log^4 T.$$

In the case of general square-free level N or even the case of prime level $N = p$, the class number of a maximal order $\mathcal{O}$ in the definite quaternion algebra $\mathfrak{A}$ that ramifies precisely at ∞ and all prime divisors of N is bigger than 1 in general.

We need first generalize the Maass Correspondence Theorem to a family of Dirichlet series and a family of automorphic functions, and then Duke's Theorem 2. This is done in [13] and we include this part in Chapter 4 for completeness.

Secondly, we need to verify a similar asymptotic assumption as in Theorem 2 above. This is done by redefining the divisor function using ideals and working out the exact expression and hence an analogous identity as before, namely,

$$\sum_{\mathfrak{a}} d(\mathfrak{a})^2 N(\mathfrak{a})^{-s} = \frac{\zeta_{\mathcal{O}}^4(s)}{\zeta_{\mathcal{O}}(2s)}.$$

Note that such an identity is true in general and we include this result for any maximal order in general quaternion algebras over general number fields in Chapter 3.

Finally, we need a result on the exact modular forms that appear in the diagonal after diagonalization. Although Eichler and others did not use general definite quaternion algebras to solve the Basis Problem, they did calculate the traces of the Hecke operators and Brandt matrices in general. By comparing the traces of Hecke operators and Brandt matrices in the case of square-free level, we are able to see that the non-zero diagonal entries (after diagonalization) form precisely the set of newforms of level N.

Therefore, these efforts generalize Duke's result to square-free level N. Please see Chapter 3 for the consideration of quaternion algebras, divisor functions and the derivation of the identity mentioned above. Chapter 4 contains the generalization of Maass Correspondence Theorem, that of Duke's Theorem 2 and eventually the application to fourth moment problem associated to newforms of square-free level N.

1.2 Special Values and Non-vanishing Properties

It turns out that much arithmetic information is encoded in the values or behavior of L-functions at points where their series representations do not converge and also in the distribution of zeros and poles, provided that they can be meromorphically continued.

For example, Deligne conjectured that the special value of an automorphic L-function at a critical point is algebraic up to a specified transcendental number. In particular, for the Riemann zeta function $\zeta(s)$, it is a well known fact that $\zeta(2k)/\pi^{2k}$ is a rational number for any $k \in \mathbb{Z}^+$.

On the other hand, that $\zeta(s)$ is non-vanishing on the line $Re(s) = 1$ implies the Prime Number Theorem. Recall that Prime Number Theorem says

$$\pi(x) \sim \frac{x}{\log(x)}, \text{ as } x \to \infty,$$

where $\pi(x)$ is the number of rational primes less than or equal to x.

Another conjectural example is the Birch and Swinnerton-Dyer conjecture, one of the Millennium Prize Problems. It predicts that the rank of the abelian group of rational points of an elliptic curve E is equal to the order of the zero of the associated L-function $L(s, E)$ as $s = 1$. ($L(s, E)$ has a functional equation under $s \leftrightarrow 2 - s$.) In particular, if $L(1, E) \neq 0$, there would be only finitely many rational points.

In Chapter 5, following Moreno ([20]), we will show that the value $L(\frac{1}{2}, \rho_1 \otimes \overline{\rho_2})$ for two-dimensional irreducible modular Galois representation ρ_1 and ρ_2 with the same determinant character is related to the Petersson inner product. Specifically, there exists

some constant $c \neq 0$,

$$\langle f^* f, h\rangle = cL(\frac{1}{2}, \rho_1 \otimes \overline{\rho_2}),$$

where f, h are the newforms corresponding to ρ_1 and ρ_2 respectively, via Strong Artin Conjecture and f^* is the derivative of an Eisenstein series. By further decomposing $\rho_1 \otimes \overline{\rho_2}$ in concrete cases, we may get information of the resulting L-functions.

There are two cases; ρ_1 and ρ_2 both are odd or both are even. In either case the proof is carried out by calculating one integral in two ways. The integral is essentially equal to the Rankin-Selberg L-function of f and h.

Finally, at the end of Chapter 5, we give an easy application of this type of equalities in the case of image being $\widetilde{S}_4$.

1.3 Strong Artin Conjecture

Conjecture 1.3.1 (Strong Artin Conjecture) *Let $\rho : Gal(\overline{F}/F) \to GL_n(\mathbb{C})$ be a (continuous) Galois representation. Then there exists an automorphic representation $\pi(\rho)$ of GL_n over F such that for almost all $\mathfrak{p}$, $L_{\mathfrak{p}}(s, \rho) = L_{\mathfrak{p}}(s, \pi(\rho))$.*

We call ρ **modular** if the above conjecture is true. This conjecture is a special case of a much more general conjecture of Langlands, known as the Langlands functoriality conjecture. If $n = 2$ and $F = \mathbb{Q}$, this conjecture can be reformulated using classical language. In particular, for odd Galois representations, it takes the following form.

Conjecture 1.3.2 (Strong Artin Conjecture) *If $\rho : Gal(\overline{\mathbb{Q}}/\mathbb{Q}) \to GL_2(\mathbb{C})$ is an odd Galois representation with determinant character ϵ and conductor N, then there exists a newform f_ρ of weight 1,level N and central character ϵ such that $L(s, f_\rho) = L(s, \rho)$.*

Note that the converse of this conjecture is a theorem of Deligne and Serre (cf. [6]).

Finite groups in $PGL_2(\mathbb{C})$ are classified by Klein into 5 classes, cyclic, dihedral (D_{2n}), tetrahedral (A_4), octahedral (S_4) and icosahedral (A_5) (see [15]). We call ρ the same name

if its image in $PGL_2(\mathbb{C})$ falls into the corresponding class. All the cases are proved except the icosahedral one; the cyclic and dihedral case was proved by Artin as part of the class field theory, Langlands [16] proved the tetrahedral case and Tunnell [34] finished the octahedral case.

In this thesis, we shall consider a class of 4-dimensional Galois representations with image isomorphic to S_5 and provide a sufficient condition on their modularity.

Given such a Galois representation ρ, let K be the number field fixed by $ker(\rho)$ and $\mathrm{Gal}(K/\mathbb{Q}) \simeq S_5$. Let $\widetilde{S}_5$ be one of the two nontrivial central extensions by C_2, say, the one where a transposition in S_5 has preimages of order 2. Assume that $K/\mathbb{Q}$ has a double cover $\widetilde{K}/\mathbb{Q}$, that is, $\widetilde{K}/K$ is quadratic and $\mathrm{Gal}(\widetilde{K}/\mathbb{Q}) \simeq \widetilde{S}_5$.

Let $E/\mathbb{Q}$ be the quadratic subextension of $K/\mathbb{Q}$ determined by A_5; hence $\mathrm{Gal}(\widetilde{K}/E) \simeq \widetilde{A}_5$, providing an 2-dimensional icosahedral Galois representation σ of G_E. Our main theorem in Chapter 6 tells us that the modularity of σ implies that of ρ.

The proof given there is elementary. By using character tables, we can show that ρ is a (degree-one) character twist of $As(\sigma)$, the Asai lift of σ. Then a result of Ramakrishnan [28] applies to show that $As(\sigma)$ is modular, so is ρ.

In the last section of Chapter 6, we shall state an open problem which asks for an affirmative example of modular 4-dimensional S_5-Galois representation. The above result may help to attack this problem.

Chapter 2

L-functions

In this chapter, we will provide some necessary background for the subsequent chapters. As well as to list some basic facts in corresponding theories, this chapter also serves to fix the notation to be used in the sequel. More specifically, we will give the notion of L-functions, sketch the theory of modular forms and their L-functions and then summarize some basic facts on Galois representations and Artin L-functions. Readers who are acquainted with these subjects are urged to skip this chapter.

2.1 L-functions

The theory of L-functions started with the consideration of the Riemann zeta function and then of the Dirichlet series attached to Dirichlet characters.

Let $N \in \mathbb{Z}^+$. Recall that a **Dirichlet character mod** N is a mapping $\chi : \mathbb{Z} \to \mathbb{C}$ induced from a homomorphism $\chi' : (\mathbb{Z}/N\mathbb{Z})^\times \to \mathbb{C}^\times$ by lifting first to integers relative prime to N and then to $\mathbb{Z}$ by filling with 0's elsewhere. We call N the **modulus** of χ. Note that the correspondence $\chi' \to \chi$ is bijective.

Suppose $M \in \mathbb{Z}^+$, $M \mid N$ and χ is a Dirichlet character mod M induced from χ'. By composing with the projection $(\mathbb{Z}/N\mathbb{Z})^\times \to (\mathbb{Z}/M\mathbb{Z})^\times$, we can obtain a character ψ', hence a Dirichlet character ψ mod N. Define the **conductor** c_χ of χ to be the smallest

positive integer m such that some Dirichlet character mod m induces χ. If a Dirichlet character χ mod N has conductor N, we say that χ is **primitive**.

Definition 2.1.1 *The **Riemann zeta function** is defined to be*

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

*and for a Dirichlet character χ, the associated **Dirichlet L-function** is defined similarly as*

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

Both series defining them converge absolutely for $Re(s) > 1$ and they both have Euler products

$$\zeta(s) = \prod_p (1 - p^{-s})^{-1}, \quad L(s, \chi) = \prod_p (1 - \chi(p)p^{-s})^{-1}.$$

Moreover, they also have meromorphic continuations to the s-complex plane and functional equations.

We follow Iwaniec and Sarnak [10] on the definition of general L-functions. Fix a number field F, denote its prime ideals by $\mathfrak{p}$ and let $N(\mathfrak{a})$ be the absolute norm of $\mathfrak{a}$, for a general ideal $\mathfrak{a}$.

Definition 2.1.2 *An **L-function** takes the form of a product of degree $m \geq 1$ over all prime ideals $\mathfrak{p}$ of F*

$$L(s) = \prod_{\mathfrak{p}} L_{\mathfrak{p}}(s),$$

where for almost all $\mathfrak{p}$ the local factors are

$$L_{\mathfrak{p}}(s) = \prod_{i=1}^{m} (1 - \alpha_i(\mathfrak{p})(N\mathfrak{p})^{-s})^{-1},$$

for some complex numbers $\alpha_i(\mathfrak{p})$, such that as a function of s, the product converges absolutely for $Re(s) > 1$.

Note that if we multiply out the product, we can get the series of the form

$$L(s) = \sum_{\mathfrak{a} \neq 0} c(\mathfrak{a}) N(\mathfrak{a})^{-s},$$

where the sum is over integral ideals $\mathfrak{a}$.

The Riemann zeta function and Dirichlet L-functions are degree one L-functions over $\mathbb{Q}$. Other examples can be constructed from many mathematical objects. For example, given a number field F, its Dedekind zeta function $\zeta_F(s)$ is an L-function. Recall that

$$\zeta_F(s) = \sum_{\mathfrak{a}}{}' N(\mathfrak{a})^{-s} = \prod_{\mathfrak{p}} (1 - N(\mathfrak{p})^{-s})^{-1},$$

where $\sum'$ is over all non-zero integral ideals of F. In the following sections, we will see L-functions constructed from modular forms and Galois representations and We shall also consider zeta functions for quaternion algebras in Chapter 3.

2.2 Modular Forms and L-functions

Now let us recall the concept of modular forms and their attached L-functions. For our purpose, we shall focus on the case of congruence subgroups $\Gamma_0(N)$. For modular forms with respect to $SL_2(\mathbb{Z})$, see Serre's famous short book [30] and refer to Miyake's book [18] or Shimura's book [32] in the case of congruence subgroups or general groups.

2.2.1 Modular Forms

Let $\mathbb{H} = \{z \in \mathbb{C} : Imz > 0\}$ be the upper half plane and $GL_2(\mathbb{R})^+$ be the group of 2×2 real matrices with positive determinant. Define the action of $GL_2(\mathbb{R})^+$ on $\mathbb{H}$ by fractional linear transformations, namely

$$\gamma(z) = \frac{a_\gamma z + b_\gamma}{c_\gamma z + d_\gamma}, \text{ if } z \in \mathbb{H}, \gamma = \begin{pmatrix} a_\gamma & b_\gamma \\ c_\gamma & d_\gamma \end{pmatrix} \in GL_2(\mathbb{R})^+.$$

For the weight k action of $GL_2(\mathbb{R})^+$ on functions on $\mathbb{H}$, we use the traditional notation

$$(f|_k\gamma)(z) = det(\gamma)^{k/2}(c_\gamma z + d_\gamma)^{-k} f(\gamma(z)).$$

For an integer N, the following congruence subgroups are defined:

$$\Gamma_0(N) = \{\gamma \in SL_2(\mathbb{Z}) : \ c_\gamma \equiv 0 \bmod N\},$$

$$\Gamma_1(N) = \{\gamma \in \Gamma_0(N) : \ a_\gamma \equiv d_\gamma \equiv 1 \bmod N\},$$

$$\Gamma(N) = \{\gamma \in SL_2(\mathbb{Z}) : \ \gamma \equiv I_{2\times 2} \bmod N\}.$$

And generally, a **congruence subgroup** is a subgroup of $SL_2(\mathbb{Z})$ which contains $\Gamma(N)$ for some N.

Definition 2.2.1 *Let $\Gamma \supset \Gamma(N)$ be a congruence subgroup. A holomorphic function $f : \mathbb{H} \to \mathbb{C}$ is called a **modular form** of weight k ($\in \mathbb{Z}$) with respect to Γ if it satisfies*

1. *Automorphy condition: $(f|_k\gamma)(z) = f(z)$ for any $\gamma \in \Gamma$;*
2. *Regularity at cusps: f is regular at all cusps $z \in \mathbb{Q} \cup i\infty$.*

Roughly speaking, the regularity condition above is the same as to say that for all $\gamma \in SL_2(\mathbb{Z})$, $f|_k\gamma$ admits a Fourier expansion over only non-negative powers of $q^{1/N}$ with $q = e(z) = \exp(2\pi i z)$.

A modular form is called a **cusp form** or **cuspidal** if it vanishes at all cusps, namely the above Fourier expansions contain only positive powers of $q^{1/N}$.

The complex vector space of all modular (resp. cusp) forms of weight k with respect to Γ is denoted by $\mathcal{M}_k(\Gamma)$ (resp. $\mathcal{S}_k(\Gamma)$). The space $\mathcal{S}_k(\Gamma)$ can be made into an inner product space by introducing the **Petersson inner product**, which is defined as

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

where $\int_{\Gamma(N)\backslash\mathbb{H}}$ means integration over a fundamental domain for $\Gamma(N)\backslash\mathbb{H}$. Recall that a **fundamental domain** for $\Gamma\backslash\mathbb{H}$ is a open connected subset of $\mathbb{H}$ such that distinct points represent distinct orbits in $\Gamma\backslash\mathbb{H}$ and its closure represents all the orbits.

Let χ be a Dirichlet character mod N and put

$$\mathcal{M}_k(N,\chi) = \{f \in \mathcal{M}_k(\Gamma_1(N)) : \ f|_k\gamma = \chi(d_\gamma)f \text{ for all } \gamma \in \Gamma_0(N)\},$$

and

$$\mathcal{S}_k(N,\chi) = \mathcal{M}_k(N,\chi) \cap \mathcal{S}_k(\Gamma_1(N)).$$

We then say forms in $\mathcal{M}_k(N,\chi)$ are of **level** N and **central character** χ. One has the following decomposition

$$\mathcal{M}_k(\Gamma_1(N)) = \bigoplus_{\chi mod N} \mathcal{M}_k(N,\chi), \qquad \mathcal{S}_k(\Gamma_1(N)) = \bigoplus_{\chi mod N} \mathcal{S}_k(N,\chi),$$

where both χ run through all Dirichlet characters mod N.

2.2.2 The Theory of Hecke Operators

For $\Gamma = \Gamma(1) = SL_2(\mathbb{Z})$, recall that the **discriminant modular form** $\Delta(z)$ is the cusp form of smallest weight $k = 12$. It is defined as

$$\Delta(z) = q\prod_{n=1}^{\infty}(1-q^n)^{24} = \sum_{n=1}^{\infty}\tau(n)q^n.$$

The Fourier coefficients $\tau(n)$, known as the **Ramanujan tau function**, have the following multiplicative properties:

$$\tau(mn) = \tau(m)\tau(n), \text{ for } (m,n) = 1,$$

$$\tau(p^{r+1}) = \tau(p)\tau(p^r) - p^{11}\tau(p^{r-1}), \ p \text{ a prime number}, r \geq 1.$$

This is true in general by the **theory of Hecke operators**. We sketch now the theory for the space $\mathcal{S}_k(N,\chi)$, following Miyake [18] or Shimura [32]. Define first

$$\Delta_0(N) := \{\gamma \in M_2(\mathbb{Z}) : c_\gamma \equiv 0 \bmod N, (a_\gamma, N) = 1, \det(\gamma) > 0\}.$$

For any $\alpha \in \Delta_0(N)$, assume $\Gamma_0(N)\alpha\Gamma_0(N) = \coprod_\nu \Gamma_0(N)\alpha_\nu$ and this double coset acts on $\mathcal{S}_k(N,\chi)$ via

$$f \mid_k \Gamma_0(N)\alpha\Gamma_0(N) = \det(\alpha)^{k/2-1} \sum_\nu \overline{\chi(\alpha_\nu)} f \mid_k \alpha_\nu.$$

For any $n \in \mathbb{Z}^+$, define the operator $T(n)$ on $\mathcal{S}_k(N,\chi)$ by

$$T(n) = \sum_{\det(\alpha)=n} \Gamma_0(N)\alpha\Gamma_0(N),$$

where the summation is taken over all double cosets $\Gamma_0(N)\alpha\Gamma_0(N)$ with $\alpha \in \Delta_0(N)$ and $\det(\alpha) = n$.

We collect the main results in the following theorem:

Theorem 2.2.2 *(1) If (m,n)=1, then $T(m)T(n) = T(mn)$;*

(2)

$$T(p)T(p^r) = \begin{cases} T(p^{r+1}) + p^{k-1}T(p^{r-1}) & \text{if } p \nmid N, \\ T(p^{r+1}) & \text{if } p \mid N \end{cases};$$

(3) As operators on $\mathcal{S}_k(N,\chi)$, $T(n)$ with $(n,N) = 1$ are normal and generate a commutative algebra;

(4) The space $\mathcal{S}_k(N,\chi)$ has a basis consisting of common eigenfunctions of all $T(n)$ with $(n,N) = 1$.

(5) Assume $f(z) = \sum_{n=0}^\infty a(n)q^n \in \mathcal{S}_k(N,\chi)$ is a common eigenfunction of all $T(n)$ with $(n,N) = 1$ and $f|_k T(n) = \lambda(n)f$ with $\lambda(n) \in \mathbb{C}$. Then $a(n) = \lambda(n)a(1)$.

So the Fourier coefficients of a common eigenfunction satisfy analogous multiplicative properties as $\Delta(z)$ does. In (3), (4) or (5) of the above theorem, we cannot (in general) eliminate the condition $(n,N) = 1$. However, on a subspace, we are able to do it. This is the theory of newforms which we shall explain in next subsection.

2.2.3 The Theory of Newforms

The theory of newforms was established by Atkin and Lehner ([2]).

Given a function f, denote by f^d the function $f^d(z) = f(dz)$.

Let $M, N \in \mathbb{Z}^+$ be such that $M \mid N$ and let χ be a Dirichlet character mod M. It is easy to see that χ is also defined mod N and $\mathcal{S}_k(M,\chi) \subset \mathcal{S}_k(N,\chi)$. In general, for any positive $d \mid \frac{N}{M}$ and $f \in \mathcal{S}_k(M,\chi)$, $f^d \in \mathcal{S}_k(N,\chi)$. As usual, let c_χ be the conductor of χ.

Definition 2.2.3 *The **subspace of oldforms** in $\mathcal{S}_k(N,\chi)$, denoted by $\mathcal{S}_k^{old}(N,\chi)$, is defined to be the subspace spanned by the set*

$$\bigcup_M \bigcup_d \{f^d : f \in \mathcal{S}_k(M,\chi)\}$$

*where M runs over all positive integers such that $c_\chi | M$, $M | N$, $M \neq N$ and d runs over all positive divisors of $\frac{N}{M}$. Then the **subspace of newforms** is defined to be its orthogonal complement with respect to the Petersson inner product. We denote it by $\mathcal{S}_k^{new}(N,\chi)$.*

By convention, we shall reserve the notion **newforms** for special elements in $\mathcal{S}_k^{new}(N,\chi)$.

Lemma 2.2.4 *(1) $\mathcal{S}_k^{old}(N,\chi)$ and $\mathcal{S}_k^{new}(N,\chi)$ both are stable under Hecke operators $T(n)$ ($(n,N)=1$);*

(2) Let $f(z) = \sum_{n=1}^{\infty} a_n q^n \in \mathcal{S}_k^{new}(N,\chi)$ be a common eigenfunction of $T(n)$ for all n relatively prime to some integer L, then $a_1 \neq 0$.

Definition 2.2.5 *We call an element $f(z) = \sum_{n=1}^{\infty} a_n q^n \in \mathcal{S}_k^{new}(N,\chi)$ a **newform** if $f(z)$ is a common eigenfunction of all $T(n)$ with $(n,N)=1$ and $a_1 = 1$.*

Theorem 2.2.6 *(1) A newform $f(z) = \sum_{n=1}^{\infty} a(n) q^n \in \mathcal{S}_k^{new}(N,\chi)$ is a common eigenfunctions for all $T(n)$ with eigenvalues $a(n)$;*

(2) $\mathcal{S}_k^{new}(N,\chi)$ has a basis consisting of newforms.

2.2.4 L-functions Attached to Modular Forms

Let $f(z) = \sum_{n=0}^{\infty} a(n)q^n \in \mathcal{M}_k(N, \chi)$ and define formally the Dirichlet series

$$L(s, f) = \sum_{n=1}^{\infty} a(n)n^{-s}.$$

Denote by w_N the following matrix

$$\begin{pmatrix} 0 & -1 \\ N & 0 \end{pmatrix}.$$

Since w_N normalizes $\Gamma_0(N)$, it is not hard to see that $f \to f|_k w_N$ induces the isomorphisms

$$\mathcal{M}_k(N, \chi) \simeq \mathcal{M}_k(N, \overline{\chi}), \qquad \mathcal{S}_k(N, \chi) \simeq \mathcal{S}_k(N, \overline{\chi}),$$

$$\mathcal{S}_k^{new}(N, \chi) \simeq \mathcal{S}_k^{new}(N, \overline{\chi}), \qquad \mathcal{S}_k^{old}(N, \chi) \simeq \mathcal{S}_k^{old}(N, \overline{\chi}).$$

Now define $\Lambda_N(s, f) = (2\pi/\sqrt{N})^{-s}\Gamma(s)L(s, f)$ and assume $f|_k w_N(z) = \sum_{n=0}^{\infty} b(n)q^n$.

Theorem 2.2.7 (Hecke) *The function $\Lambda_N(s, f)$ can be meromorphically continued to the whole s-plane, satisfy the functional equation*

$$\Lambda_N(s, f) = i^k \Lambda_N(k - s, f|_k w_N),$$

and the function

$$\Lambda_N(s, f) + \frac{a(0)}{s} + \frac{i^k b(0)}{k - s}$$

is holomorphic on the whole s-plane and bounded on any vertical strip.

Theorem 2.2.8 *Assume $f(z) = \sum_{n=1}^{\infty} a(n)q^n$ is a newform in $\mathcal{S}_k^{new}(N, \chi)$.*

(1) $L(s, f)$ has a Euler product and

$$L(s, f) = \prod_p (1 - a(p)p^{-s} + \chi(p)p^{k-1-2s})^{-1};$$

(2) $g(z) = \overline{f(-\overline{z})}$ is a newform in $\mathcal{S}_k^{new}(N, \overline{\chi})$ and

$$f|_k w_N(z) = cg(z), \text{ for some constant } c \in \mathbb{C}.$$

Given a modular form f, a newform or not, we shall call $L(s, f)$ the **L-function associated to** f.

2.2.5 Automorphic Representations and L-functions

The theory of automorphic forms or representations gives a natural generalization of the theory of modular forms. In this subsection, we shall briefly mention this theory with little details. See Cogdell, Kim and Murty's lecture notes [5] for a reference.

Let F be a number field and $\mathcal{O}_F$ its ring of integers. As usual, F_v denotes the completion of F with respect to a place v. For a non-Archimedean place v, let $\mathcal{O}_v$ be the ring of integers in F_v, ϖ_v a uniformizer and q_v the order of the corresponding residue field. Denote by $\mathbb{A} = \mathbb{A}_F$ the adele ring of F and for simplicity, we will assume $G = GL_n$. We know that $GL_n(\mathbb{A})$ is the direct limit of the topological groups

$$GL_n(\mathbb{A})_S = \prod_{v \in S} GL_n(F_v) \times \prod_{v \notin S} GL_n(\mathcal{O}_v),$$

where S ranges over all finite sets of valuations of F containing all of the Archimedean valuations. Denote by K the standard maximal compact subgroup of $GL_n(\mathbb{A})$, i.e.,

$$K = \prod_{v \text{ complex}} U(n, \mathbb{C}) \times \prod_{v \text{ real}} O(n, \mathbb{R}) \times \prod_{v \text{ discrete}} GL_n(\mathcal{O}_v),$$

and let K_v be the corresponding local factor of K. (see [36] for details.)

For a fixed unitary central character $\omega : F^\times \backslash \mathbb{A}^\times \to \mathbb{C}^\times$, define

$$L^2(\omega) = L^2(GL_n(F) \backslash GL_n(\mathbb{A}), \omega)$$

to be the Hilbert space of square integrable functions φ modulo the center, i.e., $\varphi(zg) = \omega(z)\varphi(g)$ for $z \in Z(\mathbb{A})$ and

$$\int_{Z(\mathbb{A})GL_n(F)\backslash GL_n(\mathbb{A})} |\varphi(g)|^2 dg < \infty.$$

Here Z is the center of GL_n and dg is the Haar measure.

Denote by R, the right regular representation of $GL_n(\mathbb{A})$ on $L^2(\omega)$, i.e., $(R(h)\varphi)(g) = \varphi(gh)$ for $g, h \in GL_n(\mathbb{A})$ and $\varphi \in L^2(\omega)$. Define

$$\begin{aligned} L_0^2(\omega) &= L_0^2(GL_n(F)\backslash GL_n(\mathbb{A}), \omega) \\ &= \left\{ \varphi \in L^2(\omega) \,\middle|\, \int_{(\mathbb{A}/F)^{r(n-r)}} \varphi\left(\begin{pmatrix} I_r & x \\ 0 & I_{n-r} \end{pmatrix} g \right) dx = 0 \text{ , for all } 1 \le r < n \right\}. \end{aligned}$$

This is a closed R-invariant subspace and denote the action on $L_0^2(\omega)$ also by R.

Definition 2.2.9 *An* ***automorphic representation*** *of $GL_n(\mathbb{A})$ is an irreducible constituent of R on $L^2(\omega)$ for some ω and a* ***cuspidal representation*** *of $GL_n(\mathbb{A})$ is an irreducible constituent of R on $L_0^2(\omega)$ for some ω.*

Theorem 2.2.10 *Let π be a cuspidal representation of $GL_n(\mathbb{A})$. Then there is a restricted tensor product decomposition*

$$\pi = \otimes_v{}'\pi_v$$

into irreducible unitary representations of the local groups $GL_n(F_v)$. Hence for almost all the finite places v, π_v has a $GL_n(\mathcal{O}_v)$-fixed vector.

A representation π_v of $GL_n(F_v)$ is called spherical if it has a $GL_n(\mathcal{O}_v)$-fixed vector. Assume that π_v is an irreducible admissible spherical representation of $GL_n(F_v)$. Then it is known that

$$\pi_v = Ind_{B(F_v)}^{GL_n(F_v)}(\mu_{1,v} \otimes \cdots \otimes \mu_{n,v}),$$

i.e., the induced represenation from the Borel subgroup $B(F_v)$ of n uniquely determined unramified characters $\mu_{i,v}$ of $F_v^\times$. Thus the set of n complex numbers

$$\{\mu_{1,v}(\varpi_v), \cdots, \mu_{n,v}(\varpi_v)\}$$

completely determines π_v, since $\mu_{i,v}$'s are unramified.

Definition 2.2.11 *For a finite v where π_v is spherical, we define the local L-factor to be*

$$L_v(s,\pi) = L(s,\pi_v) = \prod_{i=1}^{n}(1-\mu_{i,v}(\varpi_v)q_v^{-s})^{-1}.$$

Let S be a finite set of places containing all the Archimedean places and all the non-spherical places. We define the partial L-function as

$$L_S(s,\pi) = \prod_{v\notin S} L_v(s,\pi).$$

Note that with more efforts we can define local L-factors $L(s, \pi_v)$ for all the places, hence get a completed L-function $L(s, \pi)$ by formally taking the infinite product of all the local L-factors. Since the partial L-function suffices our purpose in this thesis, we will skip this.

2.3 Galois Representations and Artin L-functions

In general, there are three types of Galois representations, namely, mod p, p-adic and complex Galois representations, corresponding to representation spaces over finite fields, p-adic fields and $\mathbb{C}$, respectively. But we note here that in the sequel, we only consider complex Galois representations.

Let F be a number field and $\overline{F} = \overline{\mathbb{Q}}$ be one algebraic closure. With the Krull topology, the absolute Galois group $\mathrm{Gal}(\overline{F}/F)$ is a compact and totally disconnected topological group.

Now let (ρ, V) be a (complex) n-dimensional **Galois representation**, namely, a continuous homomorphism $\rho : \mathrm{Gal}(\overline{F}/F) \to GL(V)$. Note that the continuity is the same as to say that $Im(\rho)$ is finite, for there is no nontrivial group contained in a sufficiently small neighborhood of the identity in $GL_n(\mathbb{C})$. Denote the **determinant character** $\det(\rho)$ by ϵ. In the case of $F = \mathbb{Q}$ and $n = 2$, we call ρ **odd** if $\epsilon(c) = -1$, where c is the complex conjugation in $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ and **even** if $\epsilon(c) = 1$.

Let L/F be a finite Galois extension such that $\mathrm{Gal}(\overline{F}/F) \subset ker(\rho)$, so we can factor ρ through $\mathrm{Gal}(L/F)$. Take any prime ideal $\mathfrak{p}$ of F and $\mathrm{Gal}(L/F)$ permutes all the prime ideals lying above $\mathfrak{p}$. Let $\mathfrak{P}$ be a prime ideal of L lying above $\mathfrak{p}$ and the **decomposition group** $D_{\mathfrak{P}}$ for $\mathfrak{P} \mid \mathfrak{p}$ is defined to be the subgroup of $\mathrm{Gal}(L/F)$ that stabilizes $\mathfrak{P}$. Moreover the **inertia group** $I_{\mathfrak{P}}$ for $\mathfrak{P} \mid \mathfrak{p}$ is the subgroup of $D_{\mathfrak{P}}$ whose elements induce the identity automorphism on the residue field, i.e.,

$$I_{\mathfrak{P}} = \{\sigma \in D_{\mathfrak{P}} : \sigma x \equiv x \bmod \mathfrak{P} \text{ for all } x \in \mathcal{O}_L\}.$$

Similarly we define the **ramification groups** $G_i = G_{\mathfrak{P},i}$ $(i \geq 0)$ by

$$G_i = \{\sigma \in G_0 : \sigma x \equiv x \bmod \mathfrak{P}^{i+1} \text{ for all } x \in \mathcal{O}_L\}.$$

In particular, $G_0 = I_{\mathfrak{P}}$.

We know that $D_{\mathfrak{P}}/I_{\mathfrak{P}} \simeq \mathrm{Gal}(k_{L,\mathfrak{P}}/k_{F,\mathfrak{p}})$, where the right-hand side is the cyclic Galois group of the corresponding residue fields extension generated by the Frobenius automorphism $x \mapsto x^{N(\mathfrak{P})}$.

Now for any $\mathfrak{p}$, take any $\mathfrak{P}$ lying above $\mathfrak{p}$ and any element $\sigma_{\mathfrak{P}} \in D_{\mathfrak{P}}$ that projects to the Frobenius element. Let $V^{I_{\mathfrak{P}}}$ be the subspace of V stabilized by $I_{\mathfrak{P}}$. Then one can show that the characteristic polynomial of $\sigma_{\mathfrak{P}}$ on $V^{I_{\mathfrak{P}}}$ is independent of the above choices of L, $\mathfrak{P}$ and then $\sigma_{\mathfrak{P}}$, so the following definition is well-defined.

Definition 2.3.1 *Define the* ***local factor of the Artin L-function*** *attached to ρ by*

$$L_{\mathfrak{p}}(s, \rho) = \det_{V^{I_{\mathfrak{P}}}}(I - \rho(\sigma_{\mathfrak{P}})N(\mathfrak{p})^{-s})^{-1};$$

and the ***Artin L-funtion*** *attached to ρ is*

$$L(s, \rho) = \prod_{\mathfrak{p}} L_{\mathfrak{p}}(s, \rho).$$

Note that $L(s, \rho)$ is defined on $Re(s) > 1$. If χ_ρ is the character corresponding to the Galois representation ρ of the finite group $\mathrm{Gal}(L/F)$, we shall also write $L(s, \chi_\rho) = L(s, \rho)$. We summarize some fundamental properties of Artin L-functions.

Theorem 2.3.2 *(1) If ρ_1 and ρ_2 are two Galois representations over F, then*

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

(2) Let ρ be a Galois representation over L with L/F an arbitrary finite extension and let $Ind_L^F(\rho)$ be the induced Galois representation over F. Then

$$L(s, \rho) = L(s, Ind_L^F(\rho)).$$

Let us recall the notion of Artin conductor. Fix a Galois representation (ρ, V), a prime ideal p of F and a prime ideal $\mathfrak{P}$ of L above $\mathfrak{p}$. Let us define

$$n(\rho, \mathfrak{p}) = \sum_{i=0}^{\infty} \frac{g_i}{g_0} codim(V^{G_i}),$$

where g_i is the order of G_i, $i \geq 0$. It is easy to see that the summation is finite and $n(\rho, \mathfrak{p})$ is independent of the choice of $\mathfrak{P}$. Artin proved that this rational number $n(\rho, \mathfrak{p})$ is actually an integer. Note also that if $\mathfrak{p}$ is unramified in L/F, $n(\rho, \mathfrak{p}) = 0$. These facts allow us to define the **Artin conductor** $\mathfrak{f}(\rho)$ of ρ as follows:

$$\mathfrak{f}(\rho) = \prod_{\mathfrak{p}} \mathfrak{p}^{n(\rho, \mathfrak{p})}.$$

In the case of $F = \mathbb{Q}$, we also call the positive generator of $\mathfrak{f}(\rho)$ the Artin conductor.

We end this section with the functional equation of $L(s, \rho)$. We need to complete the L-function by adding some γ-factors.

Put $\gamma(s) = \pi^{-s/2}\Gamma(s/2)$. For any complex place v of F, define

$$\gamma_\rho^v(s) = (\gamma(s)\gamma(s+1))^{\dim V}.$$

Consider a real place v. Take any place w of L lying above v and the decomposition group D_w is of order 1 or 2. Decompose $V = V_v^+ \oplus V_v^-$ corresponding the the eigenvalues 1 and -1 of $\rho(\sigma_w)$ and we put

$$\gamma_\rho^v(s) = \gamma(s)^{\dim V_v^+} \gamma(s+1)^{\dim V_v^-}.$$

We note here that $\gamma_\rho^v(s)$ does not depend on the choice of w. Finally let $\gamma_\rho(s) = \prod_v \gamma_\rho^v(s)$, where the product is over all the infinite places of F.

Let $A(\rho) = |d_F|^{\dim V} N_{F/\mathbb{Q}}(\mathfrak{f}(\rho))$ where d_F is the absolute discriminant of F. Define $\Lambda(s, \rho) = A(\rho)^{s/2}\gamma_\rho(s)L(s, \rho)$. Then we have the following theorem:

Theorem 2.3.3 *The function $\Lambda(s, \rho)$ has a meromorphic continuation to the whole complex plane and satisfies the functional equation*

$$\Lambda(1-s, \rho) = W(\rho)\Lambda(s, \overline{\rho}),$$

where $\overline{\rho}$ is the dual (or contragredient) representation of ρ and $W(\rho)$ is a constant of absolute value 1.

The $W(\rho)$ in the above theorem is known as the **Artin root number**.

Chapter 3

Divisor Function over Quaternion Algebras

As a preparation for the next chapter, we will define and investigate the divisor functions for quaternion algebras. In this chapter and the next, except some slight generalizations, we will mainly follow the joint paper [13] with H.H.Kim.

3.1 Introduction

We review the basic knowledge and some important facts on quaternion algebras in this section. See Reiner's book [29] or Weil's book [36] for a reference on the general theory. For the theory over $\mathbb{Q}$, see also the introduction of Pizer's paper [24].

3.1.1 General Notions

Let K be a finite extension of $\mathbb{Q}$ or $\mathbb{Q}_v$ for some place v of $\mathbb{Q}$.

A **quaternion algebra** $\mathfrak{A}$ over K is a central simple algebra of dimension 4 over K, i.e., a 4-dimensional K-algebra with center K and no nontrivial double-sided ideals.

Example. Let $a, b \in K^\times$ be arbitrary and define $\mathfrak{A}$ as the vector space spanned by

$\{1, i, j, k\}$ whose ring structure is subject to $i^2 = a, j^2 = b$ and $ij = -ji = k$. Then $\mathfrak{A}$ is a quaternion algebra over K, denoted by $(a, b)_K$. Actually, it is known that any quaternion algebra over K is isomorphic to one of $(a, b)_K$. Note that $(-1, -1)_{\mathbb{R}}$ is the Hamiltonian quaternion algebra.

Assume K is not $\mathbb{R}$ or $\mathbb{C}$ and denote by S its ring of integers.

A **full S-lattice** M in $\mathfrak{A}$ is a finitely generated S-submodule which contains a K-basis of $\mathfrak{A}$. We will just say **lattice** for short, since we will only deal with full S-lattices. The notion **ideal** will share the same definition as lattice, which should cause no confusion since we are not interested in ideals of $\mathfrak{A}$ itself. Indeed, unless $\mathfrak{A} \simeq M_2(K)$, there are no non-trivial ideals.

An **order** $\mathcal{O}$ in $\mathfrak{A}$ is a subring of $\mathfrak{A}$ with the same identity element such that it is also a lattice. An order is called **maximal** if it is not contained in any other order.

For a lattice M, define the **left order** $\mathcal{O}_l(M)$ and the **right order** $\mathcal{O}_r(M)$ of M as follows:

$$\mathcal{O}_l(M) = \{\alpha \in \mathfrak{A} : \alpha M \subset M\},\ \mathcal{O}_r(M) = \{\alpha \in \mathfrak{A} : M\alpha \subset M\}.$$

It is easy to check that they are orders. Given an order $\mathcal{O}$ and a lattice M, we call M a **left $\mathcal{O}$-ideal** if $\mathcal{O} = \mathcal{O}_l(M)$.[1] The obvious analogous definitions hold for **right $\mathcal{O}$-ideal** and **two-sided $\mathcal{O}$-ideal**. An **integral ideal** $\mathfrak{a}$ is a lattice such that $\mathfrak{a} \subset \mathcal{O}_l(\mathfrak{a})$ or equivalently $\mathfrak{a} \subset \mathcal{O}_r(\mathfrak{a})$. An ideal $\mathfrak{a}$ is **normal**, if $\mathcal{O}_l(\mathfrak{a})$ is maximal or equivalently $\mathcal{O}_r(\mathfrak{a})$ is maximal. An integral ideal $\mathfrak{a}$ is a **maximal** ideal if $\mathfrak{a}$ is a maximal left ideal in $\mathcal{O}_l(\mathfrak{a})$, or equivalently, $\mathfrak{a}$ is a maximal right ideal in $\mathcal{O}_r(\mathfrak{a})$. An ideal is called **principal** if $\mathfrak{a} = \mathcal{O}_l(\mathfrak{a})\alpha$ or equivalently $\mathfrak{a} = \alpha\mathcal{O}_r(\mathfrak{a})$ for some $\alpha \in \mathfrak{A}^\times$.

If M, N are two lattices of $\mathfrak{A}$, define the **product** MN as

$$MN = \left\{ \sum_{i=1}^{n} \alpha_i \beta_i : \alpha_i \in M, \beta_i \in N, n \in \mathbb{Z}^+ \right\},$$

[1] In the literature, a different definition of left $\mathcal{O}$-ideal is given by $\mathcal{O} \subset \mathcal{O}_l(M)$. However, if $\mathcal{O}$ is maximal, they coincide.

which is certainly a lattice. The product MN is called **proper** if $\mathcal{O}_r(M) = \mathcal{O}_l(N)$. If $\mathfrak{a}, \mathfrak{b}$ are two normal ideals, then $\mathfrak{ab}$ is normal with $\mathcal{O}_l(\mathfrak{ab}) = \mathcal{O}_l(\mathfrak{a})$ and $\mathcal{O}_r(\mathfrak{ab}) = \mathcal{O}_r(\mathfrak{b})$. A proper product of integral normal ideals is again integral.

For a lattice M in $\mathfrak{A}$, define the **inverse** of M as

$$M^{-1} = \{\alpha \in \mathfrak{A} : M\alpha M \subset M\}.$$

Then M^{-1} is a lattice. If $\mathfrak{a}$ is a normal ideal, $\mathfrak{a}^{-1}$ is also normal, with left order $\mathcal{O}_r(\mathfrak{a})$ and right order $\mathcal{O}_l(\mathfrak{a})$; moreover if $\mathfrak{b}$ is also normal and $\mathfrak{ab}$ is proper,

$$\mathfrak{a}\mathfrak{a}^{-1} = \mathcal{O}_l(\mathfrak{a}),\ \mathfrak{a}^{-1}\mathfrak{a} = \mathcal{O}_r(\mathfrak{a}),\ (\mathfrak{a}^{-1})^{-1} = \mathfrak{a},\ (\mathfrak{ab})^{-1} = \mathfrak{b}^{-1}\mathfrak{a}^{-1}.$$

As a consequence, the cancellation law holds for proper products of normal ideals.

Let $\mathfrak{a}, \mathfrak{b}$ be two ideals. We call $\mathfrak{b}$ **divides** $\mathfrak{a}$ **from the left**, denoted $\mathfrak{b} \mid_l \mathfrak{a}$, if there exists an integral ideal $\mathfrak{c}$ such that $\mathfrak{bc}$ is proper and equal to $\mathfrak{a}$. If $\mathfrak{a}, \mathfrak{b}$ are normal of the same left order, then $\mathfrak{a} \subset \mathfrak{b}$ if and only if $\mathfrak{b} \mid_l \mathfrak{a}$. The divisibility from the right is similarly defined.

Let $\alpha \in \mathfrak{A}$ be any element and α is algebraic over K whose minimal polynomial $m_\alpha(X)$ over K is of degree 2 if $\alpha \notin K$. Assume $m_\alpha(X) = X^2 - tX + n$ with $t, n \in K$. We call the other root of $m_\alpha(X)$ as the **conjugate** of α, denoted by $\overline{\alpha}$, and define the **reduce trace** $Tr(\alpha) = \alpha + \overline{\alpha} = t$ and the **reduced norm** $N(\alpha) = \alpha\overline{\alpha} = n$. In the case of $\alpha \in K$, $N(\alpha) = \alpha^2$ and $Tr(\alpha) = 2\alpha$. Explicitly, in $(a, b)_K$, let $\alpha = x + yi + zj + wk$ be any element. We have $\overline{\alpha} = x - yi - zj - wk$, and

$$Tr(\alpha) = 2x, \quad N(\alpha) = x^2 - ay^2 - bz^2 + abw^2.$$

The quadratic form

$$q(X, Y, Z, W) = X^2 - aY^2 - bZ^2 + abW^2$$

is called the **norm form** of $(a, b)_K$. If M is a lattice, define its **conjugate** $\overline{M} = \{\overline{\alpha} : \alpha \in M\}$. Thus, $\mathcal{O}_l(\overline{M}) = \mathcal{O}_r(M)$ and $\mathcal{O}_r(\overline{M}) = \mathcal{O}_l(M)$.

Define the **reduced norm** of a lattice M, $N(M)$, be to the (fractional) ideal in K generated by the set $\{N(\alpha) : \alpha \in M\}$. For any two normal ideals $\mathfrak{a}, \mathfrak{b}$ with $\mathfrak{ab}$ proper, it is true that

$$N(\mathfrak{ab}) = N(\mathfrak{a})N(\mathfrak{b}), \quad N(\mathfrak{a}^{-1}) = N(\mathfrak{a})^{-1}, \quad N(\overline{\mathfrak{a}}) = N(\mathfrak{a}).$$

If $\mathfrak{a}$ is an integral normal ideal of $\mathfrak{A}$, $N(\mathfrak{a})$ is an integral ideal of K.

Example. If $\mathcal{O}$ is a maximal order and $\alpha \in \mathfrak{A}^\times$, then $\alpha^{-1}\mathcal{O}\alpha$ is a maximal order and $\mathcal{O}\alpha$ is a normal ideal. Specifically, $\mathcal{O}\alpha$ is a left $\mathcal{O}$-ideal and a right $\alpha^{-1}\mathcal{O}\alpha$-ideal with $N(\mathcal{O}\alpha) = SN(\alpha)$. Moreover, $\mathcal{O}\alpha$ is integral if and only if $\alpha \in \mathcal{O}$.

3.1.2 Local and Global Theory

From now on till the end of this chapter, we fix a number field F and a quaternion algebra $\mathfrak{A}$ over F. To avoid confusion with orders in $\mathfrak{A}$, we use $R = R_F$ to denote the ring of integers of F. If v is a place of F, then F_v is the completion of F at v and if v is finite, R_v is the ring of integers in F_v. Set $\mathfrak{A}_v = \mathfrak{A} \otimes_F F_v$ and $\mathfrak{A}_v$ is a quaternion algebra over F_v. For a finite place $v = v_\mathfrak{p}$, when there is no danger of confusion, we will also denote $R_v \cap F$ by R_v and the maximal ideal in $R_\mathfrak{p}$, namely $\mathfrak{p}R_\mathfrak{p}$, by $\mathfrak{p}$. Let $N(\mathfrak{p}) = N_{F/\mathbb{Q}}(\mathfrak{p})$ denote the cardinality of $R/\mathfrak{p}$.

Let us first see the classification of quaternion algebras. Locally, if F_v is $\mathbb{C}$, then there is a unique quaternion algebra over F_v up to isomorphism, namely the two-by-two matrix algebra $M_2(F_v)$. If F_v is $\mathbb{R}$ or p-adic, there are precisely two quaternion algebras over F_v up to isomorphism, namely, the two-by-two matrix algebra $M_2(F_v)$ and a unique division quaternion algebra. This division quaternion algebra can be constructed explicitly as follows. If $F_v = \mathbb{R}$, the division algebra is given by

$$(-1,-1)_\mathbb{R} \simeq \left\{ \begin{pmatrix} \alpha & \beta \\ -\overline{\beta} & \overline{\alpha} \end{pmatrix} : \alpha, \beta \in \mathbb{C} \right\}.$$

If F_v is a p-adic field, let L/F_v be the unique unramified field extension of degree 2. Assume $\mathrm{Gal}(L/F_v) = \langle \sigma \rangle$ and let ϖ be a uniformizer of F_v. Then the division quaternion

algebra over F_v is isomorphic to the subalgebra of $M_2(L)$ given by

$$\left\{ \begin{pmatrix} \alpha & \beta \\ \varpi\beta^\sigma & \alpha^\sigma \end{pmatrix} : \alpha, \beta \in L \right\},$$

where $\alpha^\sigma = \sigma(\alpha)$.

Globally, for a quaternion algebra $\mathfrak{A}$ over F, we say that $\mathfrak{A}$ is **unramified** or **splits** at a place v if $\mathfrak{A}_v$ is isomorphic to $M_2(F_v)$, and **ramified** otherwise. From the theory of Hilbert symbols, we know that the number of ramified places of $\mathfrak{A}$ over F must be finite and even. Conversely, given any finite set S of real or finite places of F of even cardinality, there is a unique quaternion algebra, up to isomorphism, that ramifies precisely at places in S. So we obtain a one-to-one correspondence between the set of isomorphism classes of $\mathfrak{A}$ over F and the set of even finite sets of real or finite places of F.

For a lattice M in $\mathfrak{A}$ and a finite place $\mathfrak{p}$ of F, denote $M_\mathfrak{p} = M \otimes_R R_\mathfrak{p}$, called the localization of M at $\mathfrak{p}$. Obviously $M_\mathfrak{p}$ is a lattice in $\mathfrak{A}_\mathfrak{p}$. Moreover, given any two lattices M, N, we have $M_\mathfrak{p} = N_\mathfrak{p}$ for almost all $\mathfrak{p}$. There is a local-global correspondence in the context of lattices; namely, if M is a lattice of $\mathfrak{A}$ and $N_{(\mathfrak{p})}$ is a lattice in $\mathfrak{A}_\mathfrak{p}$ for every $\mathfrak{p}$ such that for almost all $\mathfrak{p}$, $M_\mathfrak{p} = N_{(\mathfrak{p})}$, then there exists a unique lattice N of $\mathfrak{A}$ such that $N_\mathfrak{p} = N_{(\mathfrak{p})}$. Actually $N = \bigcap_\mathfrak{p}(\mathfrak{A} \cap N_{(\mathfrak{p})})$. (cf. [36, Theorem 2] on page 84.) Replacing lattice with order, we obtain the local-global correspondence for orders.

If M is a lattice, then

$$\mathcal{O}_l(M_\mathfrak{p}) = \mathcal{O}_l(M)_\mathfrak{p}, \quad \mathcal{O}_r(M_\mathfrak{p}) = \mathcal{O}_r(M)_\mathfrak{p}.$$

If $\mathfrak{a}$ is a normal ideal, $N(\mathfrak{a}_\mathfrak{p}) = N(\mathfrak{a})_\mathfrak{p}$, hence $N(\mathfrak{a}) = \prod_\mathfrak{p} N(\mathfrak{a}_\mathfrak{p})$. If $\mathfrak{b}$ is also normal, we have $(\mathfrak{a}\mathfrak{b})_\mathfrak{p} = \mathfrak{a}_\mathfrak{p}\mathfrak{b}_\mathfrak{p}$ and $\mathfrak{a}\mathfrak{b}$ is proper if and only if $\mathfrak{a}_\mathfrak{p}\mathfrak{b}_\mathfrak{p}$ is proper for any $\mathfrak{p}$.

Any order of $\mathfrak{A}$ or $\mathfrak{A}_\mathfrak{p}$ is contained in a maximal order. An order $\mathcal{O}$ of $\mathfrak{A}$ is maximal if and only if $\mathcal{O}_\mathfrak{p}$ is maximal for all $\mathfrak{p}$. Locally, if $\mathfrak{A}_\mathfrak{p}$ is a division algebra, there is a unique maximal order; if, on the other hand, $\mathfrak{A}_\mathfrak{p} = M_2(F_\mathfrak{p})$, all maximal orders are conjugate to $M_2(R_\mathfrak{p})$ by elements in $\mathfrak{A}_\mathfrak{p}^\times$. Globally, there are non-conjugate maximal orders; actually the number of conjugacy classes of maximal orders is called the **type number** of $\mathfrak{A}$.

Locally, let $\mathcal{O}_\mathfrak{p}$ be a maximal order in $\mathfrak{A}_\mathfrak{p}$. All the one-sided ideals of $\mathcal{O}_\mathfrak{p}$ are principal, all maximal ideals have norm $\mathfrak{p}$; there is a unique maximal two-sided ideal $\mathfrak{m}_\mathfrak{p}$ and $\mathfrak{m}_\mathfrak{p}$ generates the set of two-sided $\mathcal{O}_\mathfrak{p}$-ideals as an infinite cyclic group. Specifically, if $\mathfrak{A}_\mathfrak{p} = M_2(F_\mathfrak{p})$ and $\mathcal{O}_\mathfrak{p} = M_2(R_\mathfrak{p})$, then $\mathfrak{m}_\mathfrak{p} = \mathcal{O}_\mathfrak{p}\varpi$; if, on the other hand, $\mathfrak{A}_\mathfrak{p}$ is the division algebra constructed above, and $\mathcal{O}_\mathfrak{p}$ is the unique maximal order, that is,

$$\mathcal{O}_\mathfrak{p} = \left\{ \begin{pmatrix} \alpha & \beta \\ \varpi\beta^\sigma & \alpha^\sigma \end{pmatrix} : \alpha, \beta \in R_L \right\},$$

then

$$\mathfrak{m}_\mathfrak{p} = \mathcal{O}_\mathfrak{p} \begin{pmatrix} 0 & 1 \\ \varpi_\mathfrak{p} & 0 \end{pmatrix}.$$

It follows that $N(\mathfrak{m}_\mathfrak{p}) = \mathfrak{p}$ and all one-sided ideals of $\mathcal{O}_\mathfrak{p}$ are also double-sided, hence integer powers of $\mathfrak{m}_\mathfrak{p}$.

Let us consider the global situation now. For convenience, let us introduce the adeles and ideles over $\mathfrak{A}$. The ring of adeles $\mathfrak{A}_\mathbb{A} = \prod_v' \mathfrak{A}_v$, the restricted product of $\mathfrak{A}_v$ over all the places of F with respect to $\{\mathcal{O}_\mathfrak{p}\}$ for any given order $\mathcal{O}$. Similarly, the group of ideles $\mathfrak{A}_\mathbb{A}^\times = \prod_v' \mathfrak{A}_v^\times$ is the restricted product of $\mathfrak{A}_v^\times$ with respect to $\{\mathcal{O}_\mathfrak{p}^\times\}$. They are independent on the order $\mathcal{O}$. Denote the finite part of the adeles and ideles by $\mathfrak{A}_{\mathbb{A},f}$ and $\mathfrak{A}_{\mathbb{A},f}^\times$, respectively. Now if $\mathfrak{a}$ is left $\mathcal{O}$-ideal, then there exists $\alpha_\mathfrak{p} \in \mathfrak{A}_\mathfrak{p}^\times$ for each $\mathfrak{p}$, such that $\mathfrak{a}_\mathfrak{p} = \mathcal{O}_\mathfrak{p}\alpha_\mathfrak{p}$ and for almost all $\mathfrak{p}$, $\alpha_\mathfrak{p} \in \mathcal{O}_\mathfrak{p}^\times$. So $\alpha = (\alpha_\mathfrak{p}) \in \mathfrak{A}_{\mathbb{A},f}^\times$. By abuse of language, we write $\mathfrak{a} = \mathcal{O}\alpha$. If $\mathfrak{a} = \mathcal{O}\alpha$ and $\mathfrak{b} = \mathcal{O}'\beta$ with $\alpha, \beta \in \mathfrak{A}_{\mathbb{A},f}^\times$, then $\mathfrak{ab}$ is proper if and only if $\mathcal{O}' = \alpha^{-1}\mathcal{O}\alpha$, in which case $\mathfrak{ab} = \mathcal{O}\alpha\beta$.

Two left $\mathcal{O}$-ideals $\mathfrak{a}, \mathfrak{b}$ are called **left-equivalent**, if there exists $\alpha \in \mathfrak{A}^\times$ such that $\mathfrak{a} = \mathfrak{b}\alpha$, denoted $\mathfrak{a} \sim_l \mathfrak{b}$. The equivalence relation $\sim_r$ for right $\mathcal{O}$-ideals is similarly defined. For an order $\mathcal{O}$, the map $\mathfrak{a} \to \mathfrak{a}^{-1}$ induces a bijection between the set of left $\mathcal{O}$-ideal classes and the set of right $\mathcal{O}$-ideal classes. We define the **class number** of $\mathcal{O}$ as the cardinality of the set of left or right $\mathcal{O}$-ideal classes, denoted by $H(\mathcal{O})$. Maximal orders have the same class number and call this the class number of $\mathfrak{A}$, denoted by $H = H(\mathfrak{A})$.

3.2 Divisor Function over Quaternion Algebras

We fix a number field F and a quaternion algebra $\mathfrak{A}$ over F. Let all the notations be the same as those in the introduction of this chapter.

Hereafter, all ideals of $\mathfrak{A}$ will be normal integral ideals and all products of ideals will be proper unless otherwise stated.

Fix any maximal order $\mathcal{O}$ in $\mathfrak{A}$.

Definition 3.2.1 *Define the* ***divisor function*** $d : \{\text{integral ideals of } \mathfrak{A}\} \to \mathbb{Z}^+$ *by*

$$d(\mathfrak{a}) = |\{(\mathfrak{b}, \mathfrak{c}) : \mathfrak{a} = \mathfrak{b}\mathfrak{c}\}|.$$

For any non-zero integral ideal $\mathfrak{n}$ in R, put

$$A(\mathfrak{n}) = \{\mathfrak{a} : \mathcal{O} = \mathcal{O}_l(\mathfrak{a}), N(\mathfrak{a}) = \mathfrak{n}\},$$

and define $a(\mathfrak{n}) = |A(\mathfrak{n})|$.

Lemma 3.2.2 *Assume $N(\mathfrak{a}) = \mathfrak{n}\mathfrak{m}$ with $\mathfrak{n}, \mathfrak{m}$ relatively prime. Then there exists a unique pair $(\mathfrak{b}, \mathfrak{c})$ of integral ideals such that $\mathfrak{a} = \mathfrak{b}\mathfrak{c}$, $N(\mathfrak{b}) = \mathfrak{n}$ and $N(\mathfrak{c}) = \mathfrak{m}$.*

Proof. The existence follows trivially from the theorem in (22.28) of [29]. The theorem states that for any preassigned order in the factorization of $N(\mathfrak{a})$ into product of prime ideals, there exists a corresponding factorization of $\mathfrak{a}$ into maximal ideals. Note that such a factorization is not unique in general.

For the uniqueness, assume $\mathfrak{a} = \mathfrak{b}_1\mathfrak{c}_1 = \mathfrak{b}_2\mathfrak{c}_2$. Because of the local-global correpondence for lattices, it suffices to show it locally, that is, $\mathfrak{b}_{1,\mathfrak{p}} = \mathfrak{b}_{2,\mathfrak{p}}$ for all $\mathfrak{p}$. This is true, since for $\mathfrak{p} \mid \mathfrak{n}$ both are equal to $\mathfrak{a}_\mathfrak{p}$ and for $\mathfrak{p} \nmid \mathfrak{n}$ both are trivial. Done. □

Proposition 3.2.3 *Both of the functions d and a are multiplicative, in the sense that if $\mathfrak{n}$, $\mathfrak{m}$ are relatively prime, then $a(\mathfrak{n}\mathfrak{m}) = a(\mathfrak{n})a(\mathfrak{m})$, and if $\mathfrak{b}\mathfrak{c}$ is proper and $N(\mathfrak{b})$, $N(\mathfrak{c})$ are relatively prime, then $d(\mathfrak{b}\mathfrak{c}) = d(\mathfrak{b})d(\mathfrak{c})$.*

Proof. For the function a, let us define a bijective function $\phi : A(\mathfrak{nm}) \to A(\mathfrak{n}) \times A(\mathfrak{m})$ as follows. Given $\mathfrak{a} \in A(\mathfrak{nm})$, by Lemma 3.2.2, we can find a unique pair $(\mathfrak{b}, \mathfrak{c})$ of integral ideals such that $\mathfrak{bc}$ is proper and equal to $\mathfrak{a}$ and $N(\mathfrak{b}) = \mathfrak{n}$, $N(\mathfrak{c}) = \mathfrak{m}$. Assume $\mathfrak{b} = \mathcal{O}\beta$ and $\mathfrak{c} = (\beta^{-1}\mathcal{O}\beta)\gamma$ for some $\beta, \gamma \in \mathfrak{A}_{\mathbb{A},f}^{\times}$. Then define $\phi(\mathfrak{a}) = (\mathcal{O}\beta, \mathcal{O}\beta\gamma\beta^{-1}) \in A(\mathfrak{n}) \times A(\mathfrak{m})$. It is easy to see that ϕ is surjective and the injectivity follows from the uniqueness in Lemma 3.2.2.

For the divisor function, assume $N(\mathfrak{b}) = \mathfrak{n}$ and $N(\mathfrak{c}) = \mathfrak{m}$. Let

$$A = \{(\mathfrak{a}_1, \mathfrak{a}_2) : \mathfrak{a} = \mathfrak{a}_1\mathfrak{a}_2\}$$

and similarly B and C be the sets of decompositions for $\mathfrak{b}$ and $\mathfrak{c}$, respectively.

Now we define a map $\phi : B \times C \to A$ as follows. For any pair of decompositions $\mathfrak{b} = \mathfrak{b}_1\mathfrak{b}_2$ and $\mathfrak{c} = \mathfrak{c}_1\mathfrak{c}_2$, we have $N(\mathfrak{b}_2), N(\mathfrak{c}_1)$ are relatively prime, and by Lemma 3.2.2, there exist unique ideals $\mathfrak{b}_2'$ and $\mathfrak{c}_1'$ such that $\mathfrak{b}_2\mathfrak{c}_1 = \mathfrak{b}_2'\mathfrak{c}_1'$ and $N(\mathfrak{b}_2') = N(\mathfrak{c}_1)$, $N(\mathfrak{c}_1') = N(\mathfrak{b}_2)$. Now

$$\mathfrak{a} = \mathfrak{bc} = \mathfrak{b}_1\mathfrak{b}_2\mathfrak{c}_1\mathfrak{c}_2 = (\mathfrak{b}_1\mathfrak{b}_2')(\mathfrak{c}_1'\mathfrak{c}_2)$$

gives us a decomposition of $\mathfrak{a}$.

Suppose $\mathfrak{b} = \mathfrak{b}_1\mathfrak{b}_2 = \mathfrak{d}_1\mathfrak{d}_2$ and $\mathfrak{c} = \mathfrak{c}_1\mathfrak{c}_2 = \mathfrak{e}_1\mathfrak{e}_2$ give the same decompositions of $\mathfrak{a}$. Then we have $\mathfrak{b}_1\mathfrak{b}_2' = \mathfrak{d}_1\mathfrak{d}_2'$ and $\mathfrak{c}_1'\mathfrak{c}_2 = \mathfrak{e}_1'\mathfrak{e}_2$. So $N(\mathfrak{b}_1)N(\mathfrak{b}_2') = N(\mathfrak{d}_1)N(\mathfrak{d}_2')$ which, by construction, is the same as $N(\mathfrak{b}_1)N(\mathfrak{c}_1) = N(\mathfrak{d}_1)N(\mathfrak{e}_1)$. But since $N(\mathfrak{b})$ and $N(\mathfrak{c})$ are relatively prime, we have $N(\mathfrak{b}_1) = N(\mathfrak{d}_1)$. Now $\mathfrak{b}_1\mathfrak{b}_2' = \mathfrak{d}_1\mathfrak{d}_2'$ implies, by Lemma 3.2.2, that $\mathfrak{b}_1 = \mathfrak{d}_1$. Similarly we obtain $\mathfrak{c}_2 = \mathfrak{e}_2$. So we get the injectivity.

For the surjectivity of ϕ, let $\mathfrak{a} = \mathfrak{a}_1\mathfrak{a}_2$ be any decomposition. By Lemma 3.2.2, there exist unique decompositions $\mathfrak{a}_1 = \mathfrak{b}_1\mathfrak{c}_1$ and $\mathfrak{a}_2 = \mathfrak{b}_2\mathfrak{c}_2$ where in $N(\mathfrak{b}_1)$ and $N(\mathfrak{b}_2)$ only prime divisors of n appear and in $N(\mathfrak{c}_1)$ and $N(\mathfrak{c}_2)$ only prime divisors of m appear. Let $\mathfrak{b}_2'$ and $\mathfrak{c}_1'$ be the unique ideals that $\mathfrak{b}_2'\mathfrak{c}_1' = \mathfrak{c}_1\mathfrak{b}_2$. Then it is obvious that $(\mathfrak{a}_1, \mathfrak{a}_2) = \phi((\mathfrak{b}_1, \mathfrak{b}_2'), (\mathfrak{c}_1', \mathfrak{c}_2))$. Done. $\square$

Proposition 3.2.3 is the key to work on the functions d and a and it says we only need

to proceed locally.

Fix any finite place $\mathfrak{p}$ where $\mathfrak{A}$ ramifies, that is, $\mathfrak{A}_\mathfrak{p}$ is the division algebra over $F_\mathfrak{p}$. Let $L/F_\mathfrak{p}$ be the unique unramified quadratic extension of $F_\mathfrak{p}$, $\varpi_\mathfrak{p}$ be a uniformizer of $\mathfrak{p}$ and σ be the generator of $\mathrm{Gal}(L/F_\mathfrak{p})$. We have

$$\mathfrak{A}_\mathfrak{p} \simeq \left\{ \begin{pmatrix} a & b \\ \varpi_\mathfrak{p} b^\sigma & a^\sigma \end{pmatrix} : a, b \in L \right\}.$$

Without loss of generality, we assume the equality in the above isomorphism, so we have

$$\mathcal{O}_\mathfrak{p} = \left\{ \begin{pmatrix} a & b \\ \varpi_\mathfrak{p} b^\sigma & a^\sigma \end{pmatrix} : a, b \in R_L \right\},$$

where R_L is the ring of integers in L.

Proposition 3.2.4 *For any $n \in \mathbb{N}$, $a(\mathfrak{p}^n) = 1$, that is, there exists a unique integral ideal of norm $\mathfrak{p}^n$, which is given by $\mathfrak{m}_\mathfrak{p}^n$. As a consequence, if $\mathfrak{a}$ has norm $\mathfrak{p}^n$, then $d(\mathfrak{a}) = n+1$.*

Proof. The statement on the divisor function d follows trivially from that on a. Note that there exists a unique maximal left $\mathcal{O}_\mathfrak{p}$-ideal, $\mathfrak{m}_\mathfrak{p}$, which is also a two-sided normal ideal. So any integral proper left $\mathcal{O}$-ideal is contained in, hence divisible by $\mathfrak{m}_\mathfrak{p}$. This implies that all integral ideals take the form $\mathfrak{m}_\mathfrak{p}^n$ with $n \in \mathbb{N}$ and the proposition follows since $N(\mathfrak{m}_\mathfrak{p}) = \mathfrak{p}$. $\square$

Suppose now $\mathfrak{A}$ splits at $\mathfrak{p}$, so $\mathfrak{A}_\mathfrak{p} \simeq M(2, F_\mathfrak{p})$, the two-by-two matrix algebra over $F_\mathfrak{p}$. Without loss of generality we assume that they are equal. One of the maximal orders is $\mathcal{O}_\mathfrak{p} = M(2, R_\mathfrak{p})$ and all others are conjugate to this one by elements in $\mathfrak{A}_\mathfrak{p}^\times$. An integral left $\mathcal{O}_\mathfrak{p}$-ideal $\mathfrak{a}$ is **primitive** if $\mathcal{O}_\mathfrak{p}\mathfrak{p}$ does not divide $\mathfrak{a}$ from the left.

Let us determine $a(\mathfrak{p}^n)$ using $\mathcal{O}_\mathfrak{p} = M(2, R_\mathfrak{p})$.

Lemma 3.2.5 *(1) All integral left $\mathcal{O}_\mathfrak{p}$-ideals of norm $\mathfrak{p}^n$ are*

$$\left\{ \mathcal{O}_\mathfrak{p} \begin{pmatrix} \varpi_\mathfrak{p}^l & b \\ 0 & \varpi_\mathfrak{p}^{n-l} \end{pmatrix} : b \in R_\mathfrak{p}/\mathfrak{p}^{n-l}, 0 \le l \le n \right\};$$

hence $a(\mathfrak{p}^n) = (N(\mathfrak{p})^{n+1} - 1)/(N(\mathfrak{p}) - 1)$.

(2) All primitive left $\mathcal{O}_\mathfrak{p}$*-ideals of norm* $\mathfrak{p}^n$ *are*

$$\left\{\mathcal{O}_\mathfrak{p}\begin{pmatrix} 1 & b \\ 0 & \varpi_\mathfrak{p}^n \end{pmatrix} : b \in R_\mathfrak{p}/\mathfrak{p}^n\right\} \bigcup \left\{\mathcal{O}_\mathfrak{p}\begin{pmatrix} \varpi_\mathfrak{p}^n & 0 \\ 0 & 1 \end{pmatrix}\right\}$$
$$\bigcup \left\{\mathcal{O}_\mathfrak{p}\begin{pmatrix} \varpi_\mathfrak{p}^l & b \\ 0 & \varpi_\mathfrak{p}^{n-l} \end{pmatrix} : b \in (R_\mathfrak{p}/\mathfrak{p}^{n-l})^\times, 1 \le l \le n-1\right\};$$

the total number of them are $N(\mathfrak{p})^{n-1}(N(\mathfrak{p}) + 1)$.

In this lemma, $b \in R_\mathfrak{p}/\mathfrak{p}^n$ means that b suns over a fixed complete representative set for $R_\mathfrak{p}/\mathfrak{p}^n$ and similarly $b \in (R_\mathfrak{p}/\mathfrak{p}^n)^\times$ means that b suns over a fixed complete representative set for the group $(R_\mathfrak{p}/\mathfrak{p}^n)^\times$.

Proof. The second part follows from the first part trivially by noting that $\mathfrak{a} = \mathcal{O}_\mathfrak{p}\alpha$ is primitive if and only if at least one of the four entries of α is in $R_\mathfrak{p}^\times$.

Let $\mathfrak{a} = \mathcal{O}_\mathfrak{p}\alpha$ be any integral ideal of norm $\mathfrak{p}^n$ and assume

$$\alpha = \begin{pmatrix} a & b \\ c & d \end{pmatrix}, a, b, c, d \in R_\mathfrak{p}.$$

If $v_\mathfrak{p}(a) \ge v_\mathfrak{p}(c)$, then let

$$\beta = \begin{pmatrix} 0 & 1 \\ 1 & -c^{-1}a \end{pmatrix} \in \mathcal{O}_\mathfrak{p}^\times$$

and $\beta\alpha$ has zero left lower element. If on the other hand $v_\mathfrak{p}(a) < v_\mathfrak{p}(c)$, then let

$$\beta = \begin{pmatrix} 1 & 0 \\ -a^{-1}c & 1 \end{pmatrix} \in \mathcal{O}_\mathfrak{p}^\times$$

and $\beta\alpha$ also has zero left lower element. So we may assume $c = 0$. Assume $v_\mathfrak{p}(a) = l$ and hence $v_\mathfrak{p}(d) = n - l$. Let

$$\beta = \begin{pmatrix} a^{-1}\varpi_\mathfrak{p}^l & 0 \\ 0 & d^{-1}\varpi_\mathfrak{p}^{n-l} \end{pmatrix} \in \mathcal{O}_\mathfrak{p}^\times$$

and $\beta\alpha$ has diagonal elements $\varpi_{\mathfrak{p}}^{l}$ and $\varpi_{\mathfrak{p}}^{n-l}$ respectively. We can assume $a = \varpi_{\mathfrak{p}}^{l}$ and $d = \varpi_{\mathfrak{p}}^{n-l}$. There is a unique x mod $\mathfrak{p}^{n-l}$ such that $b - x = -y\varpi_{\mathfrak{p}}^{n-l} \in \mathfrak{p}^{n-l}$ with $y \in R_{\mathfrak{p}}$. Let

$$\beta = \begin{pmatrix} 1 & y \\ 0 & 1 \end{pmatrix} \in \mathcal{O}_{\mathfrak{p}}^{\times} \text{ and } \beta\alpha = \begin{pmatrix} \varpi_{\mathfrak{p}}^{l} & x \\ 0 & \varpi_{\mathfrak{p}}^{n-l} \end{pmatrix}.$$

Now it suffices to show that all ideals in (1) are distinct. Suppose

$$\beta = \begin{pmatrix} a_1 & b_1 \\ c_1 & d_1 \end{pmatrix} \in \mathcal{O}_{\mathfrak{p}}^{\times} \text{ and } \beta \begin{pmatrix} \varpi_{\mathfrak{p}}^{l} & b \\ 0 & \varpi_{\mathfrak{p}}^{n-l} \end{pmatrix} = \begin{pmatrix} \varpi_{\mathfrak{p}}^{l'} & b' \\ 0 & \varpi_{\mathfrak{p}}^{n-l'} \end{pmatrix}.$$

Comparing the left lower elements gives us $c_1 = 0$, hence $a_1, d_1 \in R_{\mathfrak{p}}^{\times}$. Now equalities of the diagonal elements imply that $a_1 = d_1 = 1$ and $l = l'$. Finally the right upper elements equal and implies $b \equiv b'$ mod $\mathfrak{p}^{n-l}$; so by the choices of b and b', they must be the same. Done.□

Lemma 3.2.6 *(1) The maximal left $\mathcal{O}_{\mathfrak{p}}$-ideals are precisely the norm $\mathfrak{p}$ ideals;*

(2) Any primitive left $\mathcal{O}_{\mathfrak{p}}$-ideal $\mathfrak{a}$ has a unique decomposition into a proper product of maximal ideals; hence if $N(\mathfrak{a}) = \mathfrak{p}^m$, $d(\mathfrak{a}) = m + 1$.

Proof. As before, assume the left order of $\mathfrak{a}$ is $M(2, R_{\mathfrak{p}})$. We claim that $\mathfrak{a}$ is left divisible by a unique norm $\mathfrak{p}$ ideal; indeed, using the explicit generators in Lemma 3.2.5 and passing to right divisibility of corresponding generators, this is easy to verify directly. We will skip this calculation. As a consequence, the norm $\mathfrak{p}$ ideals are precisely the maximal ideals. The uniqueness of the lemma follows from the cancelation law. Done. □

Lemma 3.2.7 *Suppose $N(\mathfrak{a})$ is a $\mathfrak{p}$-power. Assume $\mathfrak{a} = \mathfrak{b}\mathfrak{c}$ with $\mathfrak{b}$ and $\mathfrak{c}$ primitive but $\mathfrak{a}$ non-primitive. If $\mathfrak{b} = \mathfrak{b}_r \cdots \mathfrak{b}_1$ and $\mathfrak{c} = \mathfrak{c}_1 \cdots \mathfrak{c}_s$ are decompositions into maximal ideals, then $\mathfrak{b}_1\mathfrak{c}_1 = \mathfrak{p}$, i.e., $\mathfrak{b}_1 = \overline{\mathfrak{c}}_1$.*

Here the $\mathfrak{p}$ in $\mathfrak{b}_1\mathfrak{c}_1 = \mathfrak{p}$ actually means the two-sided ideal in $\mathcal{O}_l(\mathfrak{b}_1)$ generated by $\mathfrak{p}$.

Proof. Let us first prove the lemma in the case of $s = 1$, that is, $\mathfrak{c}$ is maximal, hence primitive. First note that in the matrix algebra $\mathcal{O}_{\mathfrak{p}}$, $\overline{\alpha}$ is nothing but the adjoint matrix of α. Then from Lemma 3.2.5, we obtain that $\mathfrak{c}\overline{\mathfrak{c}} = \mathfrak{p}$. Now since $\mathfrak{a}$ is not primitive, there exists a normal integral ideal $\mathfrak{a}_1$ such that $\mathfrak{a} = \mathfrak{p}\mathfrak{a}_1 = \mathfrak{b}\mathfrak{c}$. Multiply the ideal $\overline{c}$ on the right and we obtain $\mathfrak{p}\mathfrak{a}_1\overline{\mathfrak{c}} = \mathfrak{p}\mathfrak{b}$, hence $\mathfrak{a}_1\overline{\mathfrak{c}} = \mathfrak{b}$ and $\overline{\mathfrak{c}} \mid_r \mathfrak{b}$. Since $\mathfrak{b}$ is primitive, by Lemma 3.2.6, $\mathfrak{b}_1 = \overline{\mathfrak{c}}$ and $\mathfrak{b}_1\mathfrak{c} = \mathfrak{p}$.

For the general case, let j be the smallest integer such that $\mathfrak{b}_r \cdots \mathfrak{b}_1\mathfrak{c}_1 \cdots \mathfrak{c}_j$ is not primitive. So $\mathfrak{b}_r \cdots \mathfrak{b}_1\mathfrak{c}_1 \cdots \mathfrak{c}_{j-1}$ is primitive. Apply the result on the case of $s = 1$, and we obtain $\overline{\mathfrak{c}}_j|_r\mathfrak{b}_r \cdots \mathfrak{b}_1\mathfrak{c}_1 \cdots \mathfrak{c}_{j-1}$. If $j > 1$, by the uniqueness in Lemma 3.2.6, $\overline{\mathfrak{c}}_j = \mathfrak{c}_{j-1}$. It contradicts to the fact that $\mathfrak{c}$ is primitive. So $j = 1$ and we are done. $\square$

We say an ideal is of signature $(\mathfrak{p}; n, m)$ if $N(\mathfrak{a}) = \mathfrak{p}^{2n+m}$ and $\mathfrak{p}^n \|_l \mathfrak{a}$. Here $\mathfrak{p}^n \|_l \mathfrak{a}$ means that $\mathfrak{p}^n$ is the highest power of $\mathfrak{p}$ that divides $\mathfrak{a}$. For such an $\mathfrak{a}$, we put

$$c(\mathfrak{a}) = c(\mathfrak{p}; n, m) = |\{(\mathfrak{b}, \mathfrak{c}) : \mathfrak{a} = \mathfrak{b}\mathfrak{c} \text{ with } \mathfrak{b}, \mathfrak{c} \text{ primitive}\}|.$$

We will see in the following lemma that this number only depends on the signature, which justifies the notation we used here. Similarly we will use $d(\mathfrak{p}; n, m) = d(\mathfrak{a})$. See also Lemma 3.2.11 below for the independence on the maximal order $\mathcal{O}$.

Lemma 3.2.8 *Let $\mathfrak{a}$ be of signature $(\mathfrak{p}; n, m)$.*

$$c(\mathfrak{p}; n, m) = \begin{cases} N(\mathfrak{p})^{n-1}((m+1)(N(\mathfrak{p})-1)+2) & n \geq 1, \\ m+1 & n = 0. \end{cases}$$

Proof. If $n = 0$, then $\mathfrak{a}$ is primitive and by Lemma 3.2.6, we can write $\mathfrak{a} = \mathfrak{a}_1 \cdots \mathfrak{a}_m$ as a unique decomposition into maximal ideals. So we $m + 1$ decompositions into product of two factors and of course all of them are primitive. Hence $c(\mathfrak{p}; 0, m) = m + 1$.

If $n = 1$, then $\mathfrak{a} = \mathfrak{p}\mathfrak{b}$ with $\mathfrak{b}$ primitive. For any primitive decomposition $\mathfrak{a} = \mathfrak{a}_1\mathfrak{a}_2 = \mathfrak{a}_{1,r}\mathfrak{a}_{1,r-1} \cdots \mathfrak{a}_{1,1}\mathfrak{a}_{2,1}\mathfrak{a}_{2,2} \cdots \mathfrak{a}_{2,s}$, since $\mathfrak{a}_1$ and $\mathfrak{a}_2$ are primitive but $\mathfrak{a}$ is not, by Lemma 3.2.7, we know that $\mathfrak{a}_{1,1}\mathfrak{a}_{2,1} = \mathfrak{p}$. Canceling $\mathfrak{p}$ from both sides, we get a primitive decomposition

of $\mathfrak{b}$. Therefore, this defines a map from the set of all primitive decompositions (into products of two factors) for $\mathfrak{a}$, to the set of all those decompositions for $\mathfrak{b}$.

Let us look at this map more closely. From the case $n = 0$, we know that $\mathfrak{b}$ has $m+1$ decompositions. Let $\mathfrak{b} = \mathfrak{b}_1\mathfrak{b}_2 = \mathfrak{b}_{1,r} \cdots \mathfrak{b}_{1,1}\mathfrak{b}_{2,1} \cdots \mathfrak{b}_{2,s}$ be any of them with both factors nontrivial and $\mathfrak{b}_{i,j}$ maximal. There are $m-1$ of them. Now we can factor $\mathfrak{p} = \mathfrak{b}_{1,0}\mathfrak{b}_{2,0}$ and there are $N(\mathfrak{p})+1$ possible choices by Lemma 3.2.5. For each of them, we produce $\mathfrak{a}_1 = \mathfrak{b}_{1,r} \cdots \mathfrak{b}_{1,0}$, $\mathfrak{a}_2 = \mathfrak{b}_{2,0} \cdots \mathfrak{b}_{2,s}$ and $\mathfrak{a} = \mathfrak{a}_1\mathfrak{a}_2$. But this decomposition is primitive if and only if $\mathfrak{b}_{1,0} \neq \overline{\mathfrak{b}}_{1,1}$ and $\mathfrak{b}_{2,0} \neq \overline{\mathfrak{b}}_{2,1}$, hence if and only if $\mathfrak{b}_{1,0} \neq \overline{\mathfrak{b}}_{1,1}$,$\mathfrak{b}_{2,1}$, since $\mathfrak{b}_{1,0} = \overline{\mathfrak{b}}_{2,0}$. That $\mathfrak{b}$ is primitive implies $\overline{\mathfrak{b}}_{1,1} \neq \mathfrak{b}_{2,1}$. So among those $N(\mathfrak{p})+1$ choices of $\mathfrak{b}_{1,0}$, only $N(\mathfrak{p})-1$ of them give primitive decompositions of $\mathfrak{a}$. So if both $\mathfrak{b}_1$ and $\mathfrak{b}_2$ are nontrivial, $(\mathfrak{b}_1, \mathfrak{b}_2)$ has $N(\mathfrak{p})-1$ preimages, $(m-1)(N(\mathfrak{p})-1)$ in total. If one of $\mathfrak{b}_1$ and $\mathfrak{b}_2$ is trivial, i.e., equals to the left or right order of $\mathfrak{b}$, we argue in the same way as above, except that in this case we only have one restriction on the factorization of $\mathfrak{p}$. Consequently, either of them has $N(\mathfrak{p})$ preimages and hence we have $2N(\mathfrak{p})$ more choices. Finally, we have $c(\mathfrak{p}; 1, m) = (N(\mathfrak{p})-1)(m-1) + 2N(\mathfrak{p}) = (N(\mathfrak{p})-1)(m+1) + 2$.

Now we are left to show $c(\mathfrak{p}; n, m) = N(\mathfrak{p})c(\mathfrak{p}; n-1, m)$ if $n > 1$. Again let $\mathfrak{a} = \mathfrak{p}\mathfrak{b}$.Note here $\mathfrak{b}$ is not primitive anymore since $n > 1$. We follow exactly the same argument as above, except that each decomposition of $\mathfrak{b}$ will give us exactly $N(\mathfrak{p})$ preimages. (For nontrivial decompositions of $\mathfrak{b}$, this is because $\mathfrak{b}$ is not primitive, which implies $\overline{\mathfrak{b}}_{1,1} = \mathfrak{b}_{2,1}$, hence only excludes one choice among $N(\mathfrak{p})+1$ of them.) So in this case, the above map is $N(\mathfrak{p})$-to-1 and surjective and our conclusion follows. Done. □

Proposition 3.2.9 *Let $\mathfrak{a}$ be of signature $(\mathfrak{p}; n, m)$.*

$$d(\mathfrak{a}) = d(\mathfrak{p}; n, m) = \frac{N(\mathfrak{p})^{n+1} - 1}{N(\mathfrak{p}) - 1}(m+1) - \frac{2(n+1)}{N(\mathfrak{p}) - 1} + \frac{2(N(\mathfrak{p})^{n+1} - 1)}{(N(\mathfrak{p}) - 1)^2}.$$

Proof. Any decomposition of $\mathfrak{a} = \mathfrak{p}^n\mathfrak{a}_1$ can be written uniquely as $\mathfrak{a} = (\mathfrak{p}^r\mathfrak{b})(\mathfrak{p}^t\mathfrak{c})$ with $\mathfrak{b}$ and $\mathfrak{c}$ primitive and $r, t \geq 0$, $r + t \leq n$. So it is produced by primitively decomposing

$\mathfrak{p}^{n-r-t}\mathfrak{a}_1$, followed by assigning the $r+t$ $\mathfrak{p}$-factors. So we have

$$d(\mathfrak{a}) = \sum_{k=0}^{n}(k+1)c(m, n-k).$$

By Lemma 3.2.8 and elementary calculations, we get the identity for $d(\mathfrak{a})$. Done. □

Let us denote by $a(\mathfrak{p}; n, m)$ the number of left $\mathcal{O}_{\mathfrak{p}}$-ideals with signature $(\mathfrak{p}; n, m)$. Then

Proposition 3.2.10

$$a(\mathfrak{p}; n, m) = \begin{cases} N(\mathfrak{p})^{m-1}(N(\mathfrak{p})+1) & m \geq 1 \\ 1 & 0 \end{cases}$$

Proof. It is obvious that $a(\mathfrak{p}; 0, m) = a(\mathfrak{p}; n, m)$ because of the bijectivity of the map $\mathfrak{a} \to \mathfrak{p}^n\mathfrak{a}$ and the formula for $a(\mathfrak{p}; 0, m)$ is given by Lemma 3.2.5. Done. □

Lemma 3.2.11 *(1) The divisor function $d(\mathfrak{a})$ depends only on the norm and the signature of $\mathfrak{a}$ at each $\mathfrak{p}$;*

(2) The functions $a(\mathfrak{n})$, $a(\mathfrak{p}; n, m)$ are independent of the fixed maximal order $\mathcal{O}$.

Proof. Let $\mathcal{O}'$ be another maximal order in $\mathfrak{A}$ and let $\mathfrak{c} = \mathcal{O}\mathcal{O}'$. It is trivial that $\mathfrak{c}$ is an ideal and the fact that $\mathcal{O}$ and $\mathfrak{O}'$ are maximal implies that $\mathfrak{c}$ is normal with left order $\mathcal{O}$ and right order $\mathcal{O}'$. Choose $\alpha \in \mathfrak{A}^{\times}_{\mathbb{A},f}$ such that $\mathfrak{c} = \mathcal{O}\alpha$, so $\mathcal{O}' = \alpha^{-1}\mathcal{O}\alpha$.

It is not hard to check that the map $\mathfrak{a} \to \alpha^{-1}\mathfrak{a}\alpha$ induces a bijective map from the set of integral left $\mathcal{O}$-ideals of signature $(\mathfrak{p}; n, m)$ to the set of integral left $\mathcal{O}'$-ideals of signature $(\mathfrak{p}; n, m)$, hence a bijective map from the set of integral left $\mathcal{O}$-ideals of norm $\mathfrak{n}$ to the set of integral left $\mathcal{O}'$-ideals of norm $\mathfrak{n}$. The independence of $d(\mathfrak{a})$, $a(\mathfrak{n})$ and $a(\mathfrak{p}; n, m)$ on the maximal order O follows from this by easy verifications.

Part (1) follows by Proposition 3.2.9. Done. □

There should be no danger of confusion between the norm of ideals of F and that of ideals of $\mathfrak{A}$. However, we will use $N_{F/\mathbb{Q}}$ to denote the norm of ideals of F in the following.

Define the zeta function for the maximal order $\mathcal{O}$ as follows:

$$\zeta_{\mathcal{O}}(s) = \sum_{\mathfrak{a}} N_{F/\mathbb{Q}}(N(\mathfrak{a}))^{-s},$$

where the sum is over all integral left $\mathcal{O}$-ideals. Since both norms are multiplicative, by Lemma 3.2.2, we can write the zeta function as an Euler product

$$\zeta_{\mathcal{O}}(s) = \prod_{\mathfrak{p}} \zeta_{\mathcal{O},\mathfrak{p}}(s),$$

where

$$\zeta_{\mathcal{O},\mathfrak{p}}(s) = \sum_{\mathfrak{a}} N_{F/\mathbb{Q}}(N(\mathfrak{a}))^{-s},$$

and the sum is taken over all integral left $\mathcal{O}$-ideals of norm $\mathfrak{p}$-powers. By Lemma 3.2.11, $\zeta_{\mathcal{O}}$ and its local factors do not depend on the choice of $\mathcal{O}$.

Proposition 3.2.12

$$\zeta_{\mathcal{O}}(s) = \zeta_F(s)\zeta_F(s-1) \prod_{\textit{ramified } \mathfrak{p}} (1 - N_{F/\mathbb{Q}}(\mathfrak{p})^{1-s}),$$

where $\zeta_F(s)$ is the Dedekind zeta function for F and the product is over all ramified finite places.

Proof. If $\mathfrak{p}$ ramifies in $\mathfrak{A}$, by localization and by Proposition 3.2.4,

$$\zeta_{\mathcal{O},\mathfrak{p}}(s) = \sum_{n=0}^{\infty} N_{F/\mathbb{Q}}(\mathfrak{p})^{-ns} = (1 - N_{F/\mathbb{Q}}(\mathfrak{p})^{-s})^{-1};$$

if $\mathfrak{p}$ splits in $\mathfrak{A}$, by Lemma 3.2.5,

$$\zeta_{\mathcal{O},\mathfrak{p}}(s) = \sum_{n=0}^{\infty} \frac{N_{F/\mathbb{Q}}(\mathfrak{p})^{n+1} - 1}{N_{F/\mathbb{Q}}(\mathfrak{p}) - 1} N_{F/\mathbb{Q}}(\mathfrak{p})^{-ns} = (1 - N_{F/\mathbb{Q}}(\mathfrak{p})^{-s})^{-1}(1 - N_{F/\mathbb{Q}}(\mathfrak{p})^{1-s})^{-1}.$$

Our proposition follows. Done. □

The following theorem is the main theorem of this chapter, which is a quaternion analogue of the well-known formula

$$\sum_{n=1}^{\infty} d(n)^2 n^{-s} = \frac{\zeta(s)^4}{\zeta(2s)},$$

where $d(n)$ is the divisor function for the rational integers and $\zeta(s)$ is the Riemann zeta function.

Theorem 3.2.13

$$\sum_{\mathfrak{a}} d(\mathfrak{a})^2 N_{F/\mathbb{Q}}(N(\mathfrak{a}))^{-s} = \frac{\zeta_{\mathcal{O}}(s)^4}{\zeta_{\mathcal{O}}(2s)},$$

where the sum is over all integral left $\mathcal{O}$-ideals.

Proof. By Proposition 3.2.12, we know that the right-hand side has an Euler product. Explicitly, if $\mathfrak{p}$ splits, the local factor at $\mathfrak{p}$ is

$$(1 + N_{F/\mathbb{Q}}(\mathfrak{p})^{-s})(1 - N_{F/\mathbb{Q}}(\mathfrak{p})^{1-2s})(1 - N_{F/\mathbb{Q}}(\mathfrak{p})^{-s})^{-3}(1 - N_{F/\mathbb{Q}}(\mathfrak{p})^{1-s})^{-4},$$

and if $\mathfrak{p}$ ramifies, the local factor at $\mathfrak{p}$ is

$$(1 - N_{F/\mathbb{Q}}(\mathfrak{p})^{-2s})(1 - N_{F/\mathbb{Q}}(\mathfrak{p})^{-s})^{-4}.$$

We now show that the left-hand side also has an Euler product. The left-hand side equals

$$\sum_{\mathfrak{n}}{}' \sum_{\mathfrak{a} \in A(\mathfrak{n})} d(\mathfrak{a})^2 N_{F/\mathbb{Q}}(\mathfrak{n})^{-s} = \sum_{\mathfrak{n}}{}' a_{\mathfrak{n}} N_{F/\mathbb{Q}}(\mathfrak{n})^{-s},$$

where $\mathfrak{n}$ runs through the non-zero integral ideals in F and $a_{\mathfrak{n}} = \sum_{\mathfrak{a} \in A(\mathfrak{n})} d(\mathfrak{a})^2$. Now for any relatively prime pair $(\mathfrak{m}, \mathfrak{n})$, by Lemma 3.2.2, we have a bijection on the two sets:

$$\{\mathfrak{a} : \mathcal{O}_l(\mathfrak{a}) = \mathcal{O}, N(\mathfrak{a}) = \mathfrak{m}\mathfrak{n}\} \longrightarrow \bigcup_{\mathfrak{b} \in A(\mathfrak{m})} \{(\mathfrak{b}, \mathfrak{c}) : \mathcal{O}_l(\mathfrak{c}) = \mathcal{O}_r(\mathfrak{b}), N(\mathfrak{c}) = \mathfrak{n}\}.$$

It follows that

$$\begin{aligned}
a_{\mathfrak{m}\mathfrak{n}} &= \sum_{\mathfrak{a} \in A(\mathfrak{m}\mathfrak{n})} d(\mathfrak{a})^2 \\
&= \sum_{\mathfrak{b} \in A(\mathfrak{m})} \sum_{\mathcal{O}_l(\mathfrak{c}) = \mathcal{O}_r(\mathfrak{b}), N(\mathfrak{c}) = \mathfrak{n}} d(\mathfrak{b}\mathfrak{c})^2 \\
&= \sum_{\mathfrak{b} \in A(\mathfrak{m})} \sum_{\mathcal{O}_l(\mathfrak{c}) = \mathcal{O}_r(\mathfrak{b}), N(\mathfrak{c}) = \mathfrak{n}} d(\mathfrak{b})^2 d(\mathfrak{c})^2 \\
&= \sum_{\mathfrak{b} \in A(\mathfrak{m})} d(\mathfrak{b})^2 \sum_{\mathcal{O}_l(\mathfrak{c}) = \mathcal{O}_r(\mathfrak{b}), N(\mathfrak{c}) = \mathfrak{n}} d(\mathfrak{c})^2 \\
&= \sum_{\mathfrak{b} \in A(\mathfrak{m})} d(\mathfrak{b})^2 \sum_{\mathfrak{c} \in A(\mathfrak{n})} d(\mathfrak{c})^2 \\
&= a_{\mathfrak{m}} a_{\mathfrak{n}},
\end{aligned}$$

where in the second last equality we used the Lemma 3.2.11. Then we have a Euler product for the left-hand side, that is,

$$\prod_{\mathfrak{p}}(\sum_{m=0}^{\infty}\sum_{\mathfrak{a}\in A(\mathfrak{p}^m)} d(\mathfrak{a})^2 N_{F/\mathbb{Q}}(N(\mathfrak{a}))^{-s}).$$

Hence to show the equality, it suffices to prove that the corresponding local factors coincide.

If $\mathfrak{p}$ ramifies, we need to prove

$$\sum_{m=0}^{\infty}\sum_{\mathfrak{a}\in A(\mathfrak{p}^m)} d(\mathfrak{a})^2 N_{F/\mathbb{Q}}(N(\mathfrak{a}))^{-s} = (1-N_{F/\mathbb{Q}}(\mathfrak{p})^{-2s})(1-N_{F/\mathbb{Q}}(\mathfrak{p})^{-s})^{-4}.$$

By Proposition 3.2.4,

$$\begin{aligned}
&\sum_{m=0}^{\infty}\sum_{\mathfrak{a}\in A(\mathfrak{p}^m)} d(\mathfrak{a})^2 N_{F/\mathbb{Q}}(N(\mathfrak{a}))^{-s}\\
=\ &\sum_{m=0}^{\infty}(m+1)^2 N_{F/\mathbb{Q}}(\mathfrak{p})^{-ms}\\
=\ &(1-N_{F/\mathbb{Q}}(\mathfrak{p})^{-2s})(1-N_{F/\mathbb{Q}}(\mathfrak{p})^{-s})^{-4}.
\end{aligned}$$

On the other hand, if $\mathfrak{p}$ splits, we need to show

$$\begin{aligned}
&\sum_{m=0}^{\infty}\sum_{\mathfrak{a}\in A(\mathfrak{p}^m)} d(\mathfrak{a})^2 N_{F/\mathbb{Q}}(N(\mathfrak{a}))^{-s}\\
=\ &(1+N_{F/\mathbb{Q}}(\mathfrak{p})^{-s})(1-N_{F/\mathbb{Q}}(\mathfrak{p})^{1-2s})(1-N_{F/\mathbb{Q}}(\mathfrak{p})^{-s})^{-3}(1-N_{F/\mathbb{Q}}(\mathfrak{p})^{1-s})^{-4}.
\end{aligned}$$

By Lemma 3.2.11, Proposition 3.2.9 and Proposition 3.2.10,

$$\begin{aligned}
&\sum_{m=0}^{\infty}\sum_{\mathfrak{a}\in A(\mathfrak{p}^m)} d(\mathfrak{a})^2 N_{F/\mathbb{Q}}(N(\mathfrak{a}))^{-s}\\
=\ &\sum_{m=0}^{\infty}\sum_{n=0}^{\infty}\sum_{\mathfrak{a},(\mathfrak{p};n,m)} d(\mathfrak{a})^2 N_{F/\mathbb{Q}}(N(\mathfrak{a}))^{-s}\\
=\ &\sum_{m=0}^{\infty}\sum_{n=0}^{\infty} a(\mathfrak{p};n,m)d(\mathfrak{p};n,m)^2 N_{F/\mathbb{Q}}(\mathfrak{p})^{-(2n+m)s}\\
=\ &\cdots\cdots\\
=\ &(1+N(\mathfrak{p})^{-s})(1-N(\mathfrak{p})^{1-2s})(1-N(\mathfrak{p})^{-s})^{-3}(1-N(\mathfrak{p})^{1-s})^{-4},
\end{aligned}$$

where the last summation in the second term is over all integral left $\mathcal{O}$-ideals of signature $(\mathfrak{p}; n, m)$ and the dots stand for a rather tedious but elementary process of calculations. It is exactly the same calculations as in Duke ([7], p.829) and could be done by hand. We checked it using the software Mathematica. Done. □

Corollary 3.2.14 *As $x \to \infty$,*

$$\sum_{N_{F/\mathbb{Q}}(N(\mathfrak{a}))\leq x} d(\mathfrak{a})^2 \sim Ax^2 \log^3(x),$$

for some positive A.

Proof. Define the Dirichlet series $f(s)$ by

$$f(s) = \sum_{n=1}^{\infty} a_n n^{-s} := \sum_{\mathfrak{a}} d(\mathfrak{a})^2 N_{F/\mathbb{Q}}(N(\mathfrak{a}))^{-s}.$$

Since $\zeta_F(s)$ only has a simple pole at $s = 1$ on the right half plane $Re(s) > 1 - 1/N$ where $N = [F : \mathbb{Q}]$, $\zeta_{\mathcal{O}}(s)$ only has a simple pole at $s = 2$ on the right half plane $Re(s) > 2 - 1/N$. Moreover $\zeta_F(2s)$ is regular and non-vanishing there, so by Theorem 3.2.13, $f(s)$ is regular on $Re(s) > 2 - 1/N$ except a unique pole at $s = 2$ of order 4. Apply Perron's formula to $f(s)$, and we obtain

$$\sum_{N_{F/\mathbb{Q}}(N(\mathfrak{a}))\leq x} d(\mathfrak{a})^2 = \sum_{n\leq x} a_n \sim Ax^2 \log^3(x), \text{ as } x \to \infty,$$

for some positive constant A. Done. □

For a more precise asymptotic result for the summatory function in Corollary 3.2.14 in the case of $F = \mathbb{Q}$, please see Corollary 17 of our paper [13].

In the following chapter, we shall see an application of this asymptotic result on a fourth moment problem of L-functions associated to newforms.

Chapter 4

Fourth Moments of L-functions Associated to Cusp Forms

In this chapter, we will follow Duke's method ([7]) to obtain an bound for fourth moments of L-functions of newforms of level N on average, where N is square-free. As mentioned before, this chapter and Chapter 3 are mainly a joint work of Kim and the author ([13]).

4.1 Introduction

The identity for the divisor function of rational quaternion algebra, proved in the last chapter, provides us with one of the two main ingredients in Duke's method. Due to the fact that the class number of the quaternion algebra is no longer one in general, we need to generalize Maass correspondence theorem to a system of automorphic functions and a system of Dirichlet series; this gives us the other main ingredient.

Throughout this chapter, let us fix a square-free positive integer N which has an odd number prime divisors, and fix $\mathfrak{A}$ as the rational definite quaternion algebra that ramifies precisely at all prime divisors of N and ∞.

4.2 Brandt Matrices and Newforms of Level N

Let $\mathcal{O}$ be a maximal order in $\mathfrak{A}$ and denote by H be the class number of $\mathfrak{A}$. Let $I_1, ..., I_H$, not necessarily integral, be a complete set of representatives of all distinct left $\mathcal{O}$-ideal classes. Let $\mathcal{O}_j = \mathcal{O}_r(I_j)$, the right order of I_j. Then $I_j^{-1}I_1, ..., I_j^{-1}I_H$, is a complete set of representatives of all distinct left $\mathcal{O}_j$-ideal classes. Here note that $I_j^{-1}I_j = \mathcal{O}_j$, and $\{\mathcal{O}_j\}$ exhausts (with multiplicity in general) all types of maximal orders in $\mathfrak{A}$. Let e_j be the number of units in $\mathcal{O}_j$.

Since $\mathfrak{A}$ ramifies at ∞, $\mathfrak{A}_\infty \simeq (-1,-1)_\mathbb{R}$, the Hamiltonian quaternion algebra. The two dimensional complex representation of $(-1,-1)_\mathbb{R}$ (see Section 3.1.2) induces a two dimensional complex representation of $\mathfrak{A}$ from the embedding $\mathfrak{A} \hookrightarrow (-1,-1)_\mathbb{R}$. Denote the matrix representation by $X = X_1$. By taking symmetric powers, for any $m \in \mathbb{N}$, we obtain a $(m+1)$-dimensional matrix representation $X_m = Sym^m(X_1)$ with $X_0 = 1$ for the trivial one dimensional representation. We know that the entries of $X_m(\alpha)$ are harmonic homogeneous polynomials $P(x_1, x_2, x_3, x_4)$ of degree m where x_i's are the coordinates of α with respect to the canonical basis of $(-1,-1)_\mathbb{R}$ (see [8], Proposition 6, page 104).

For any $n \in \mathbb{Z}^+$, $m \in \mathbb{Z}^+ \cup \{0\}$, and $1 \le i, j \le H$, define

$$b_{ij}^m(n) = e_j^{-1} \sum X_m^t(\alpha)$$

where the sum is over all $\alpha \in I_j^{-1}I_i$ with $N(\alpha) = nu_{ij}^{-1}$ and the superscript t denotes "transpose". Further, let $b_{ij}^0(0) = e_j^{-1}$ and $b_{ij}^m(0) = 0$ for any $m > 0$.

Definition 4.2.1 *Let the notations be as above. For $m, n \in \mathbb{N}$, the **Brandt matrix** $B_m(n)$ is given by*

$$B_m(n) = B_m(n; N) = (b_{ij}^m(n))_{H(m+1)\times H(m+1)}.$$

*The **theta series** attached to the Brandt matrices is defined to be*

$$\Theta_m(\tau) = \Theta_m(\tau; N) = \sum_{n=0}^{\infty} B_m(n) \exp(n\tau) = (\theta_{ij}^m(\tau))_{H(m+1)\times H(m+1)},$$

where as usual $\exp(\tau) = e^{2\pi i\tau}$. *Moreover, the* ***shifted L-series*** *attached to Brandt matrices are*

$$\Psi_m(s) = \Psi_m(s;N) = \sum_{n=1}^{\infty} B_m(n) n^{-(s+\frac{m}{2})} = (\psi_{ij}^m(s))_{H(m+1)\times H(m+1)}.$$

It is known that the entries of $\Theta_m(\tau)$ are modular forms of weight $k = m+2$ and level N. Moreover if $m > 0$, they are cusp forms. Please refer to Theorem 1 on page 105 in [8] for details. Here are some properties of the Brandt matrices (Theorem 2, page 106, [8]),

(1) $B_m(n)^t = D^{-1}B_m(n)D$ with $D = \mathrm{diag}\{e_1N(I_1)^{-1}E_{m+1}, \cdots, e_HN(I_H)^{-1}E_{m+1}\}$, the partitioned diagonal matrix with blocks $e_iN(I_i)^{-1}E_{m+1}$. Here E_{m+1} is the identity matrix of size $m+1$.

(2) $B_m(n_1n_2) = B_m(n_1)B_m(n_2)$ if $(n_1, n_2) = 1$.

(3) If $p \nmid N$, then for any $r, t \in \mathbb{N}$,

$$B_m(p^r)B_m(p^t) = \sum_{l=0}^{\min\{r,t\}} p^{(m+1)l} B_m(p^{r+t-2l}).$$

(4) If $p \mid N$, then for any $r, t \in \mathbb{N}$,

$$B_m(p^r)B_m(p^t) = B_m(p^{r+t}).$$

So the Brandt matrices for fixed m generate a commutative semisimple algebra. Hence they can be simultaneously diagonalized. A striking result is the connection between the Hecke operator and Brandt matrices. Observe first that the above identities for Brandt matrices are exactly the identities satisfied by the Hecke operators. Moreover, The action of $T_{m+2}(n)$, $(n, N) = 1$, on entries of $\Theta_m(\tau)$ is given formally by left multiplication by $B_m(n)$, namely, $T_{m+2}(n)\Theta_m(\tau) = (T_{m+2}(n)\theta_{ij}^m(\tau)) = B_m(n)\Theta_m(\tau)$ as matrices (Proposition, page 138, [8]). We can diagonalize $\Theta_m(\tau)$ and get $\mathrm{diag}\{\theta_1(\tau), \cdots, \theta_{(m+1)H}(\tau)\}$. Denote by $\mathcal{S}_m$ the direct sum of the one dimensional complex vector spaces spanned by

non-zero $\theta_i(\tau)$. So $T_{m+2}(n)$ acts on this space for any n relatively prime to N through the diagonalization of $B_m(n)$, hence θ_i, if not zero, is an eigenfunction for all $T_{m+2}(n)$ with $(n, N) = 1$.

Denote by $\mathbb{T} = \mathbb{T}_{m+2}$ the Hecke algebra generated by $T_{m+2}(n)$ with $(n, N) = 1$.

Remark. (1) In Eichler's fundamental work [8], on page 138, the $\mathbb{T}$-module $\theta_l(D, H)$ should be replaced by the direct sum of the one-dimensional complex vector spaces spanned by the non-zero theta series θ_i, where θ_i's are the cuspidal diagonal entries of the matrix obtained from $\theta_l(z; D, H)$ by diagonalization. This is due to the fact that θ_i's could be linearly dependent in general. See Pizer's observation on this, page 112 of [23].

(2) If $k = m + 2 = 2$, then all the diagonal entries of the diaganolized matrix are non-zero. This can be shown by comparing the dimensions. While if $k > 2$, some of the θ_i's might be zero. For example, when $N = 2$ and $k = 4$, we have $H = 1$. Since we know that there is no nonzero cusp form of level 2 weight k, the two cusp forms θ_1 and θ_2 are zeros. This can also be shown by comparing the dimensions in general. So some of the "one-dimensional" vector spaces in Theorem 2.28 and Corollary 2.29 in [24] could be zero spaces.

We present a theorem as follows. See [26] for the weight two case, namely $m = 0$.

Theorem 4.2.2 *Fix any even $m > 0$ and we have $\mathcal{S}_m \cong \mathcal{S}^{new}_{m+2}(N)$ as $\mathbb{T}$-modules. In particular, the θ_i's are newforms of level N and of weight $m + 2$.*

Proof. Since the Hecke algebra $\mathbb{T}$ is semisimple, to show that the two finitely generated $\mathbb{T}$-modules are isomorphic, it suffices to show that the traces of T coincide for any element $T \in \mathbb{T}$. Let $T'_{m+2}(n)$ denote the action of $T_{m+2}(n)$ on the space of newforms $\mathcal{S}^{\text{new}}_{m+2}(N)$ and let T''_{m+2} be the action of $T_{m+2}(n)$ on $\mathcal{S}_m$. So we only need to show $tr(T'_{m+2}(n)) = tr(T''_{m+2}(n))$ for any $(n, N) = 1$. Since the action of T_{m+2} on $\mathcal{S}_m$ is given formally by $B_m(n; N)$ and $tr(T''_{m+2}(n)) = tr(B_m(n; N))$, we only need to show $tr(T'_{m+2}(n)) = tr(B_m(n; N))$ for $(n, N) = 1$.

The traces of Hecke operators and Brandt matrices are well-known, see [8] for example. Here we use Pizer's notations and quote the formulas in Theorem 1 and 2 in [22] where you can see the meaning of the notations. Recall that $k = m+2 > 2$ and N is square-free.

$$tr_N T_k(n) = -\sum_s a_k(s) \sum_f b(s,f) \prod_{p|N} c'(s,f,p) + \delta(\sqrt{n}) \frac{k-1}{12} N \prod_{p|N} (1 + \frac{1}{p}),$$

and

$$trB_{k-2}(n;N) = \sum_s a_k(s) \sum_f b(s,f) \prod_{p|N} c(s,f,p) + \delta(\sqrt{n}) \frac{k-1}{12} N \prod_{p|N} (1 - \frac{1}{p}).$$

Let us first calculate $tr_N T'_k(n)$. From the theory of newforms in [2], we know that

$$\mathcal{S}_k(\Gamma_0(N)) = \bigoplus_{M|N} \bigoplus_{d|\frac{N}{M}} \mathcal{S}_k^{\text{new}}(\Gamma_0(M))^d,$$

where $\mathcal{S}_k(\Gamma_0(M))^d = \{f^d : f \in \mathcal{S}_k(\Gamma_0(M))\}$. For any two positive divisors d, d' of N/M, as H-modules,

$$\mathcal{S}_k^{\text{new}}(\Gamma_0(M))^d \cong \mathcal{S}_k^{\text{new}}(\Gamma_0(M))^{d'},$$

hence $T_k(n)$ has the same traces on them. Define $\lambda(n)$ to be the number of distinct prime divisors of n. We obtain

$$tr_N(T_k(n)) = \sum_{M|N} \sum_{d|\frac{N}{M}} tr_M(T'_k(n)) = \sum_{M|N} 2^{\lambda(N)-\lambda(M)} tr_M(T'_k(n)).$$

Apply Möbius inversion formula, we have

$$tr_N(T'_k(n)) = \sum_{M|N} 2^{\lambda(N)-\lambda(M)} \mu(N/M) tr_M(T_k(n)) = \sum_{M|N} (-2)^{\lambda(N)-\lambda(M)} tr_M(T_k(n)).$$

By above expression of $tr_N(T_k(n))$, we have $tr_N(T'_k(n)) = S_1 + S_2$ where

$$S_1 = \sum_{M|N} (-2)^{\lambda(N)-\lambda(M)} (-\sum_s a_k(s) \sum_f b(s,f) \prod_{p|M} c'(s,f,p))$$

and

$$S_2 = \sum_{M|N} (-2)^{\lambda(N)-\lambda(M)} \delta(\sqrt{n}) \frac{k-1}{12} M \prod_{p|M} (1 + \frac{1}{p}).$$

By explicit verification using the tables in [22], we have $c(s,f,p)+c'(s,f,p)=2$ for any p and any pair of (s,f). Now

$$\begin{aligned} S_1 &= -\sum_s a_k(s)\sum_f b(s,f)\sum_{M|N}(-2)^{\lambda(N)-\lambda(M)}\prod_{p|M}c'(s,f,p) \\ &= -\sum_s a_k(s)\sum_f b(s,f)\prod_{p|N}(c'(s,f,p)-2) \\ &= \sum_s a_k(s)\sum_f b(s,f)\prod_{p|N}c(s,f,p), \end{aligned}$$

where the last equality is true because $\lambda(N)$ is odd. Similarly,

$$\begin{aligned} S_2 &= \delta(\sqrt{n})\frac{k-1}{12}\sum_{M|N}(-2)^{\lambda(N)-\lambda(M)}\prod_{p|M}(p+1) \\ &= \delta(\sqrt{n})\frac{k-1}{12}\prod_{p|N}(p+1-2) \\ &= \delta(\sqrt{n})\frac{k-1}{12}N\prod_{p|N}(1-\frac{1}{p}). \end{aligned}$$

Now it is clear that $tr(T'_{m+2}(n))=tr(B_m(n;N))$ for $(n,N)=1$. Done. □

Let us end this section with a description of the action of the canonical involution (given by w_N) on the theta series above. See Pizer's work [25] (Section 9) on this.

First, let us define an two-sided integral ideal as follows. Assume $\mathcal{O}$ is the maximal order such that $\mathcal{O}_p=M_2(\mathbb{Z}_p)$ if $p\nmid N$ and

$$\mathcal{O}_p=\left\{\begin{pmatrix}\alpha & \beta\\ p\beta^\sigma & \alpha^\sigma\end{pmatrix}:\alpha,\beta\in R_L\right\},\quad \text{if } p\mid N.$$

For the meaning of these notations, please see Section 3.1.2. Define $\omega\in\mathfrak{A}^\times_{\mathbb{A},f}$ by $\omega_p=1$ if $p\nmid N$ and

$$\omega_p=\begin{pmatrix}0 & 1\\ p & 0\end{pmatrix},\quad \text{if } p\mid N.$$

Let $J=\mathcal{O}\omega$ be the integral left $\mathcal{O}$-ideal, determined by the local-global correspondence. It is easy to see that J is two-sided and $N(J)=N$. For other maximal orders, J is also defined by conjugation of some element in $\mathfrak{A}^\times_{\mathbb{A},f}$.

Now fix as before a complete representative set of left $\mathcal{O}$-ideal classes, $\{I_i\}_{i=1}^H$. Since J is two-sided, $\{JI_i\}_{i=1}^H$ gives another representative set. So $JI_i = I_{\sigma(i)\alpha_i}$ for a unique $\sigma(i)$ and some $\alpha_i \in \mathfrak{A}^\times$. Obviously, σ is a permutation of $\{1, \cdots, H\}$ of order 2. We define an $H(m+1) \times H(m+1)$ matrix $\widetilde{W}_m(N)$ by setting $\widetilde{W}_m(N) = N^{-m/2}(\rho_{ij})$, where ρ_{ij} is the $(m+1) \times (m+1)$ matrix

$$\rho_{ij} = \begin{cases} X_m^t(\alpha_i) & \text{if } j = \sigma(i) \\ 0 & \text{otherwise.} \end{cases}$$

We will need the following results in Section 4.4.

Proposition 4.2.3 *(1) $\widetilde{W}_m(N)$ commutes with $B_m(n)$ for any $n \in \mathbb{N}$;*

(2) $\widetilde{W}_m(N)^2 = I$, the identity matrix of size $H(m+1)$;

(3) $\Theta_m \mid_{w_N} (\tau) = -\widetilde{W}_m(N)\Theta_m(\tau)$, where w_N acts on $\Theta_m(\tau)$ by acting on each entry.

Proof. The verifications of (1) and (2) are straightforward. For (3), although Pizer's treatment in [25] carries the restriction that $\mathfrak{A}$ ramifies at only one finite prime, the same procedure can be applied in our situation. We shall omit the identical proof. Done. □

4.3 Maass Correspondence Theorem

In this section, we generalize Maass correspondence theorem [17] and Duke's result [7] to a system of Dirichlet series and a system of automorphic functions.

Let us denote $\mathcal{P}_m$ the space of all degree m spherical harmonic polynomials, and let $\sum_{\mathcal{P}_m}^*$ denote the summation over any orthonormal basis for $\mathcal{P}_m$ with respect to the metric on S^{n-1}.

Definition 4.3.1 *For $i = 1, ..., M$, let $\Lambda_i \subset \mathbb{R}^n$ be a full lattice, and*

$$\phi_i(s) = \sum_{\beta \in \Lambda_i}{}' a_i(\beta)|\beta|^{-2s},$$

be a Dirichlet series. Let $C = (c_{ij})$ be an $M \times M$ constant matrix and $r \in \mathbb{R}$ a constant. Then we say $\phi(s) = (\phi_1(s), ..., \phi_M(s))$ has signature $\langle \Lambda_1, ..., \Lambda_M, n, r, C \rangle$ if

(1) $(s-\frac{n+ir}{2})(s-\frac{n-ir}{2})\phi_i(s)$ *is entire and bounded in vertical strips, and for any* $P_m \in \mathcal{P}_m$*, the twist of* $\phi_i(s)$ *by* P_m*,*

$$\phi_i(s,P_m)=\sum_{\beta\in\Lambda_i}{}' a_i(\beta)P_m(\frac{\beta}{|\beta|})|\beta|^{-2s},$$

is entire and bounded in vertical strips for $m\geq 1$*.*

(2) For any P_m *with* $m\geq 0$ *and*

$$R_i(s,P_m)=\pi^{-2s}\Gamma(s+\frac{m+ir}{2})\Gamma(s+\frac{m-ir}{2})\phi_i(s,P_m),$$

we have

$$R_i(s,P_m)=(-1)^m\sum_{k=1}^{M}c_{ik}R_k(\frac{n}{2}-s,P'_m)$$

where the conjugate P'_m *is defined to be*

$$P'_m(w_1,w_2,\cdots,w_n)=P_m(w_1,-w_2,\cdots,-w_n).$$

When $M=1$, the above Dirichlet series were first considered by Maass [17] who proved a non-holomorphic, $(n+1)$-dimensional version of Hecke correspondence. Namely, there is one to one correspondence between the functions of signature $\langle\Lambda,n,r\rangle$ and certain automorphic functions on hyperbolic $(n+1)$-space. We note that $Spin(1,n)$ acts on the hyperbolic $(n+1)$-space. It is easy to generalize to a system of Dirichlet series. We use the notation in [7].

Let $\mathfrak{C}_{n+1}$ be the Clifford algebra, generated by $i_1,...,i_n$ subject to the relations $i_hi_k=-i_ki_h$ for $k\neq h$, $i_h^2=-1$, and no others. The $(n+1)$-dimensional subspace

$$V^{n+1}=\{x=x_0+x_1i_1+\cdots+x_ni_n : x_i\in\mathbb{R}\},$$

contains $H^{n+1}=\{x\in V^{n+1} : x_n>0\}$, a model for hyperbolic $(n+1)$-space when endowed with the metric $ds^2=x_n^{-2}|dx|^2$. Let Λ be a lattice in V^n, and let Λ' be its dual lattice with respect to the inner product $Re(\bar{x}y)$. Let Γ be the group of isometries of H^{n+1} generated by $x\to x+\alpha$ for all $\alpha\in\Lambda'$ and $x\to -x^{-1}$. We say that $f\in C^2(H^{n+1})$ is an automorphic function for Γ if

(1) $\Delta_{n+1}f + (r^2 + \frac{n^2}{4})f = 0$ for some $r \in \mathbb{R}$, where $\Delta_{n+1} = x_n^{n+1} \sum_{h=0}^{n} \frac{\partial}{\partial x_h}(x_n^{1-n} \frac{\partial}{\partial x_h})$,

(2) $f(x) \ll x_n^A$ as $x_n \to \infty$, and $f(x) \ll x_n^{-A}$ as $x_n \to 0+$ uniformly in $x_0, ..., x_{n-1}$,

(3) $f(\gamma x) = f(x)$ for all $\gamma \in \Gamma$.

Then we have the following Fourier expansion of $f(x)$:

$$f(x) = u(x_n) + \sum_{\beta \in \Lambda}{}' a(\beta) x_n^{\frac{n}{2}} K_{ir}(2\pi|\beta|x_n) e^{2\pi i Re(\bar{\beta}x)},$$

where

$$u(x_n) = \begin{cases} a_1 x_n^{\frac{n}{2}+ir} + a_2 x_n^{\frac{n}{2}-ir} & \text{if } r \neq 0, \\ x^{\frac{n}{2}}(a_1 + a_2 \log x_n) & \text{if } r = 0. \end{cases}$$

For the constants a_1 and a_2, please see [17] or [7].

Now let us consider the case of a family of automorphic functions. Let $\Lambda_1, ..., \Lambda_M$ be lattices in V^n, and let $\Lambda_1', ..., \Lambda_M'$ be its dual lattices. Let Γ_i be the group of isometries of H^{n+1} generated by $x \to x + \alpha$ for all $\alpha \in \Lambda_i'$ and $x \to -x^{-1}$ for each i. We say that $(f_1, ..., f_M)$ is a system of automorphic functions for $\langle \Gamma_1, ..., \Gamma_M, n, r, C \rangle$ where $r \in \mathbb{R}$ and $C = (c_{ij})$ is a constant $M \times M$ matrix, if

(1) for each i, $\Delta_{n+1}f_i + (r^2 + \frac{n^2}{4})f_i = 0$,

(2) for each i, $f_i(x) \ll x_n^A$ as $x_n \to \infty$, and $f_i(x) \ll x_n^{-A}$ as $x_n \to 0+$ uniformly in $x_0, ..., x_{n-1}$,

(3) $f_i(x + \alpha_i) = f_i(x)$ for all $\alpha_i \in \Lambda_i'$, and

(4) $f_i(x) = \sum_{k=1}^{M} c_{ik} f_k(-x^{-1})$.

Now we can prove

Theorem 4.3.2 *(Maass Correspondence Theorem for a system of Dirichlet series) Fix any constant matrix $C = (c_{ij})_{M \times M}$ and suppose, for $i = 1, ..., M$,*

$$f_i(x) = u_i(x_n) + \sum_{\beta \in \Lambda_i}{}' a_i(\beta) x_n^{\frac{n}{2}} K_{ir}(2\pi|\beta|x_n) e^{2\pi i Re(\bar{\beta}x)},$$

and

$$\phi_i(s) = \sum_{\beta\in\Lambda_i}{}' a_i(\beta)|\beta|^{-2s}.$$

The following are equivalent:

(1) $(\phi_1(s), ..., \phi_M(s))$ *has signature* $\langle \Lambda_1, ..., \Lambda_M, n, r, C\rangle$,

(2) $(f_1, ..., f_M)$ *is a system of automorphic functions for* $\langle \Gamma_1, ..., \Gamma_M, n, r, C\rangle$.

Proof. This is a straightforward generalization of [17]. For $i = 1, ..., M$, $y \in \mathbb{R}^+$, Let

$$F_{mi}(y, P_m) = u_{mi}(y) + \sum_{\beta\in\Lambda_i}{}' a_i(\beta)P_m(\beta)y^{\frac{n}{2}}K_{ir}(2\pi|\beta|y),$$

where

$$u_{mi}(y) = \begin{cases} u_i(y) & \text{if } m = 0, \\ 0 & \text{if } m > 0. \end{cases}$$

We can show as in [17] that $f_i(x) = \sum_{k=1}^M c_{ik}f_k(-x^{-1})$ if and only if $F_{mi}(y, P_m) = (-1)^m \sum_{k=1}^M c_{ik}F_{mk}(\frac{1}{y}, P'_m)$ for each m.

By the integral formula

$$4\int_0^\infty K_{ir}(2x)x^{2s}\,\frac{dx}{x} = \Gamma(s + \frac{ir}{2})\Gamma(s - \frac{ir}{2}),$$

we have

$$R_i(s, P_m) = 4\int_0^\infty (F_{mi}(y, P_m) - u_{mi}(y))y^{2s+m-\frac{n}{2}}\,\frac{dy}{y}.$$

By Mellin inversion,

$$4(F_{mi}(y, P_m) - u_{mi}(y))y^{m-\frac{n}{2}} = \frac{1}{2\pi i}\int_{Re(s)\gg 0} R_i(\frac{s}{2}, P_m)y^{-s}\,ds.$$

Note that $R_i(s, P_m)$ is entire for $m > 0$. In that case, by moving the contour to $Re(s) = \frac{n}{4}$, we have

$$4F_{mi}(y, P_m) = \frac{1}{2\pi i}\int_{Re(s)=\frac{n}{4}} R_i(\frac{s}{2}, P_m)y^{\frac{n}{2}-m-s}\,ds.$$

Hence the functional equation $F_{mi}(y, P_m) = (-1)^m \sum_{k=1}^M c_{ik}F_{mk}(\frac{1}{y}, P'_m)$ and $R_i(s, P_m) = (-1)^m \sum_{k=1}^M c_{ik}R_k(\frac{n}{2} - s, P'_m)$ are equivalent.

When $m = 0$, the integrand has a pole. By calculating the residues, we have

$$4(F_i(y,1) - u_i(y) - u_i(y^{-1})) = \frac{1}{2\pi i}\int_{Re(s)=\frac{n}{4}} R_i(\frac{s}{2},1)y^{\frac{n}{2}-s}\,ds.$$

We again obtain the same result. □

It is straightforward to generalize Duke's result ([7], Theorem 2) to a system of Dirichlet series and we skip the proof.

Theorem 4.3.3 *Suppose $(\phi_1(s),...,\phi_M(s))$ has signature $\langle\Lambda_1,...,\Lambda_M,n,r,C\rangle$, n is even, and that*

$$\sum_{i=1}^{M}\sum_{|\beta|\le x,\beta\in\Lambda_i}{}'|a_i(\beta)|^2 = Ax^n\log^c x + O(x^n\log^{c-1}x).$$

Then as $\theta\to\frac{\pi}{2}^-$,

$$\sum_{m>0}\sum_{\mathcal{P}_m}{}^*\sum_{i=1}^{M}\int_{-\infty}^{\infty}|M(2it,\theta)|^2|\phi_i(\frac{n}{2}+it,P_m)|^2\,dt = A'\log^{c+1}(\sec\theta) + O(\log^c(\sec\theta)),$$

for some constant A', where

$$M(s,\theta) = \frac{i^m}{4}\pi^{-s-\frac{n}{2}}(\tan\theta)^m(\cos\theta)^{-s}\frac{\Gamma(\frac{n}{2})\Gamma(a)\Gamma(b)}{\Gamma(m+\frac{n}{2})}F(a,b;m+\frac{n}{2},-\tan^2\theta),$$

$a = \frac{s+m+\frac{n}{2}+ir}{2}, b = \frac{s+m+\frac{n}{2}-ir}{2}$.

If $\sum_{i=1}^{M}\sum_{|\beta|\le x,\beta\in\Lambda_i}{}'|a_i(\beta)|^2 \asymp x^n\log^c x$, then we have

$$\sum_{m>0}\sum_{\mathcal{P}_m}{}^*\sum_{i=1}^{M}\int_{-\infty}^{\infty}|M(2it,\theta)|^2|\phi_i(\frac{n}{2}+it,P_m)|^2\,dt \asymp \log^{c+1}(\sec\theta).$$

Letting $T = \tan\theta$, as in [7], page 823, we have

Corollary 4.3.4 *Suppose $(\phi_1(s),...,\phi_M(s))$ has signature $\langle\Lambda_1,...,\Lambda_M,n,r,C\rangle$, n is even, and that $\sum_{i=1}^{M}\sum_{|\beta|\le x,\beta\in\Lambda_i}{}'|a_i(\beta)|^2 \asymp x^n\log^c x$. Then as $T\to\infty$,*

$$\sum_{0<m\le T}\sum_{\mathcal{P}_m}{}^*\sum_{i=1}^{M}\int_{-T}^{T}|\phi_i(\frac{n}{4}+it,P_m)|^2\,dt \ll T^n\log^{c+1}T.$$

In the application to the fourth moments of L-functions of newforms, $n = 4$; the main work is to relate the Dirichlet series $\phi(s, P_m)$ to the Dirichlet series formed from quaternion algebras and establish the estimate

$$\sum_{i=1}^{M} \sum_{|\beta| \le x, \beta \in \Lambda_i}{}' |a_i(\beta)|^2 = Ax^4 \log^3 x + O(x^4 \log^2 x).$$

4.4 Application to Fourth Moments of L-functions

Let $N \in \mathbb{Z}^+$ be square-free, which has an odd number of prime divisors, and let $\mathfrak{A}$ be a rational definite quaternion algebra that ramifies precisely at the prime divisors of N. We maintain all the notations as before.

For any $1 \le i, j \le H$, we may also define the divisor function for any $\gamma \in I_j^{-1} I_i$ by

$$d(\gamma) = \sum_{l=1}^{H} e_l^{-1} \#\{(\alpha, \beta) \in I_l^{-1} I_i \times I_j^{-1} I_l : \beta\alpha = \gamma\}.$$

It is easy to see that $\gamma \in I_j^{-1} I_i$ if and only if $I_i^{-1} I_j \gamma$ is integral, and if and only if $\gamma I_i^{-1} I_j$ is integral. The following lemma shows that two divisor functions coincide.

Lemma 4.4.1 *Let $\gamma \in I_j^{-1} I_i$ and let $\mathfrak{a} = I_i^{-1} I_j \gamma$, $\mathfrak{a}' = \gamma I_i^{-1} I_j$. Then $d(\gamma) = d(\mathfrak{a}) = d(\mathfrak{a}')$.*

Proof. The above remark says that $\mathfrak{a}$ is integral and $d(\mathfrak{a})$ makes sense. Here we only show $d(\gamma) = d(\mathfrak{a})$ and the other equality follows in the same way.

It is enough to show that for any l,

$$e_l^{-1} \#\{(\alpha, \beta) \in I_l^{-1} I_i \times I_j^{-1} I_l : \beta\alpha = \gamma\} = \#\{\mathfrak{b} \sim_l I_i^{-1} I_l : \mathfrak{b} |_l \mathfrak{a}\}.$$

We define a map ϕ:

$$\begin{array}{ccc} \{(\alpha, \beta) \in I_l^{-1} I_i \times I_j^{-1} I_l : \beta\alpha = \gamma\} & \longrightarrow & \{\mathfrak{b} \sim_l I_i^{-1} I_l : \mathfrak{b} |_l \mathfrak{a}\} \\ (\alpha, \beta) & \longmapsto & I_i^{-1} I_l \alpha \end{array}$$

First, ϕ is well-defined. Indeed, $\alpha \in I_l^{-1}I_i$ implies $I_i^{-1}I_l\alpha$ is integral; $\beta \in I_j^{-1}I_l$ and $\beta\alpha = \gamma$ imply that $I_l^{-1}I_j\beta$ is integral and so is $\alpha^{-1}(I_l^{-1}I_j\beta)\alpha$. So $(I_i^{-1}I_l\alpha)(\alpha^{-1}(I_l^{-1}I_j\beta)\alpha) = \mathfrak{a}$.

Furthermore, ϕ is surjective. For any $\mathfrak{b}|_l\mathfrak{a}$ with $\mathfrak{b} \sim_l I_i^{-1}I_l$, assume $\mathfrak{a} = \mathfrak{b}\mathfrak{c}$ and $\mathfrak{b} = I_i^{-1}I_l\alpha$. Then $\alpha\mathfrak{c}\alpha^{-1}$ has left order $\mathcal{O}_l$. So for a unique k and for some $\beta \in I_l^{-1}I_k$, $\alpha\mathfrak{c}\alpha^{-1} = I_l^{-1}I_k\beta$. Then $\mathfrak{a} = I_i^{-1}I_k\beta\alpha$, which implies $k = j$ and there exists $\epsilon \in \mathcal{O}_j^\times$, such that $\gamma = \epsilon\beta\alpha$. So $\phi((\alpha, \epsilon\beta)) = \mathfrak{a}$.

Finally, it is enough to show that ϕ is e_l-to-1. Actually, the preimage set of any element is nonempty by surjectivity and if (α, β) is one, then so is $(\epsilon\alpha, \beta\epsilon^{-1})$ for any $\epsilon \in \mathcal{O}_l^\times$. Conversely, if (α_1, β_1) and (α_2, β_2) have the same image, then $I_i^{-1}I_l\alpha_1 = I_i^{-1}I_l\alpha_2$ and there exists $\epsilon \in \mathcal{O}_l^\times$ such that $\alpha_1 = \epsilon\alpha_2$. Done. $\square$

Let the Brandt matrices, theta series and shifted L-functions be defined as in Definition 4.2.1, and we shall drop the superscript 0 if $m = 0$ as we always do in the following, that is, $\theta_{ij}(\tau) = \theta_{ij}^0(\tau)$ and

$$\begin{aligned} b_{ij}(n) &= b_{ij}^0(n) = \frac{1}{e_j}|\{\alpha \in I_j^{-1}I_i : N(\alpha) = nu_{ij}^{-1}\}| \\ &= |\{\mathfrak{a} : N(\mathfrak{a}) = n, \mathfrak{a} \sim_l I_i^{-1}I_j\}|. \end{aligned}$$

We know $\theta_{ij}(\tau)$ is a modular form of weight 2 on $\Gamma_0(N)$, and

$$\psi_{ij}(s) = \sum_{n=1}^{\infty} b_{ij}(n)n^{-s} = e_j^{-1}u_{ij}^{-s} \sum_{\alpha \in I_j^{-1}I_i} N(\alpha)^{-s} = \sum_{\mathfrak{a} \sim_l I_i^{-1}I_j} N(\mathfrak{a})^{-s},$$

which is exactly the zeta function $\zeta_{ij}(s)$ for the ideal class $I_i^{-1}I_j$.

Let $\Phi_m(s) = (\phi_{ij}^m(s)) = (\frac{N}{4})^s(\Psi_m(s))^2$, and in particular for $m = 0$

$$\phi_{ij}(s) = (\frac{N}{4})^s \sum_{l=1}^{H} \psi_{il}(s)\psi_{lj}(s).$$

Lemma 4.4.2

$$\begin{aligned} \phi_{ij}(s) &= (\frac{N}{4})^s \sum_{\mathfrak{a} \sim_l I_i^{-1}I_j} d(\mathfrak{a})N(\mathfrak{a})^{-s} = e_j^{-1}(\frac{N}{4})^s \sum_{\alpha \in I_j^{-1}I_i} d(I_i^{-1}I_j\alpha)N(I_i^{-1}I_j\alpha)^{-s} \\ &= \sum_{\beta \in \Lambda_{ij}} a_{ij}(\beta)|\beta|^{-2s} \end{aligned}$$

where Λ_{ij} *is the lattice* $2\sqrt{u_{ij}N^{-1}}I_j^{-1}I_i$ *and* $a_{ij}(\beta) = e_j^{-1}d(I_i^{-1}I_j\beta/(2\sqrt{u_{ij}N^{-1}}))$. *Moreover, as* $x \to \infty$, *for each* $i = 1, ..., H$,

$$\sum_{i,j=1}^{H} \sum_{\beta\in\Lambda_{ij},|\beta|\leq x} a_{ij}(\beta)^2 \asymp x^4 \log^3 x.$$

Proof. Given any pair $\mathfrak{b} \sim_l I_i^{-1}I_l$ and $\mathfrak{c} \sim_l I_l^{-1}I_j$, we know that $\mathfrak{b} = I_i^{-1}I_l\alpha$ and $\mathfrak{c} = I_l^{-1}I_j\beta$ for some α, $\beta \in \mathfrak{A}$; actually, to make them integral, $\alpha \in I_l^{-1}I_i$ and $\beta \in I_j^{-1}I_l$. So $\mathfrak{b}(\alpha^{-1}\mathfrak{c}\alpha) \sim_l I_i^{-1}I_j$. Since α is unique up to units in $\mathcal{O}_l$, we get a well-defined map

$$\bigcup_{l=1}^{H}\{\mathfrak{b} : \mathfrak{b} \sim_l I_i^{-1}I_l\} \times \{\mathfrak{c} : \mathfrak{c} \sim_l I_l^{-1}I_j\} \longrightarrow \{\mathfrak{a} : \mathfrak{a} \sim_l I_i^{-1}I_j\}.$$

Let $\mathfrak{a} \sim_l I_i^{-1}I_j$ and $\mathfrak{a} = \mathfrak{b}\mathfrak{c}$ be any decomposition into integral ideals. Then $\mathfrak{b} \sim_l I_i^{-1}I_l$ for a unique l, hence $\mathfrak{b} = I_i^{-1}I_l\alpha$ for some α. Then $(\mathfrak{b}, \alpha\mathfrak{c}\alpha^{-1})$ has image $\mathfrak{a}$ and the preimage set of $\mathfrak{a}$ are in one to one correspondence with the set of decompositions of $\mathfrak{a}$. So this map is surjective and for any $\mathfrak{a} \sim_l I_i^{-1}I_j$, there are precisely $d(\mathfrak{a})$ preimages. This proves the first part.

Now

$$\begin{aligned}\sum_{j=1}^{H} \sum_{\beta\in\Lambda_{ij},|\beta|\leq x} a_{ij}(\beta)^2 &= \sum_{j=1}^{H} \sum_{\alpha\in I_j^{-1}I_i, N(\alpha)\leq pu_{ij}^{-1}x^2/4} e_j^{-2}d(I_i^{-1}I_j\alpha)^2 \\ &= \sum_{j=1}^{H} e_j^{-1} \sum_{\mathfrak{a}\sim_l I_i^{-1}I_j, N(\mathfrak{a})\leq Nx^2/4} d(\mathfrak{a})^2.\end{aligned}$$

Since e_j is bounded, by Corollary 3.2.14, we conclude that

$$\sum_{i,j=1}^{H} \sum_{\beta\in\Lambda_{ij},|\beta|\leq x} a_{ij}(\beta)^2 \asymp \sum_{i=1}^{H} \sum_{\mathcal{O}_l(\mathfrak{a})=\mathcal{O}_i, N(\mathfrak{a})\leq Nx^2/4} d(\mathfrak{a})^2 \sim Ax^4 \log^3 x.$$

□

Let $\{v_{ij} : 1 \leq i, j \leq H\}$ be a basis for $\mathbb{R}^{H^2}$ and let C be the $H^2 \times H^2$ matrix that represents the linear transformation which sends v_{ij} to $e_j^{-1}e_iv_{ji}$.

Proposition 4.4.3 *The system of the Dirichlet series* $(\phi_{11}(s), \cdots, \phi_{ij}(s), \cdots, \phi_{HH}(s))$ *is of signature*

$$\langle \Lambda_{11}, \cdots, \Lambda_{ij}, \cdots, \Lambda_{HH}, 4, 0, C\rangle.$$

Proof. Direct calculation gives us $\phi_{ij}^m(s) = \phi_{ij}(s, X_m)$. The fact that $\psi_{ij}(s)$ has only one pole, that is a simple pole at $s = 2$, implies that $(s-2)^2\phi_{ij}(s)$ is entire and bounded in vertical strips. For $m \geq 1$, it follows from [33] (on page 54) that all entries of $\psi_{ij}^m(s)$ are entire and bounded on vertical strips, hence so are those of $\phi_{ij}(s, X_m)$.

Now it suffices to show the functional equations. Denote $L(s, \Theta_m(\tau))$ to be the matrix whose entries are L-functions for corresponding entries of $\Theta_m(\tau)$, and $\Theta_m(\tau)|_{w_N}$ the resulting matrix where w_N acts on each entry. Hence $\Psi_m(s) = L(s + \frac{m}{2}, \Theta_m)$. Since entries of $\Theta_m(\tau)$ are modular forms of level N and weight $m+2$,

$$(2\pi)^{-s}\Gamma(s)L(s, \Theta_m) = i^{m+2}N^{1-s+\frac{m}{2}}(2\pi)^{s-m-2}\Gamma(m+2-s)L(m+2-s, \Theta_m|_{w_N}).$$

By changing the variable $s \to s + \frac{m}{2}$, we get

$$(2\pi)^{-s}\Gamma(s+\frac{m}{2})L(s+\frac{m}{2}, \Theta_m) = i^{m+2}N^{1-s}(2\pi)^{s-2}\Gamma(2-s+\frac{m}{2})L(2-s+\frac{m}{2}, \Theta_m|_{w_N}).$$

By taking squares,

$$\begin{aligned} & (2\pi)^{-2s}\Gamma(s+\frac{m}{2})^2 L(s+\frac{m}{2}, \Theta_m)^2 \\ = \; & (-1)^m N^{2-2s}(2\pi)^{2s-4}\Gamma(2-s+\frac{m}{2})^2 L(2-s+\frac{m}{2}, \Theta_m|_{w_N})^2. \end{aligned}$$

By Proposition 4.2.3, $\Theta_m|_{w_N} = -\widetilde{W}_m(N)\Theta_m$ and $\widetilde{W}_m(N)^2 = I$, which gives us $L(s, \Theta_m|_{w_N}) = -\widetilde{W}_m(N)L(s, \Theta_m)$. Since $\widetilde{W}_m(N)$ commutes with all $B_m(n)$, we have $L(s, \Theta_m|_{w_N})^2 = L(s, \Theta_m)^2$. Then the above equation implies

$$(2\pi)^{-2s}\Gamma(s+\frac{m}{2})^2 L(s+\frac{m}{2}, \Theta_m)^2 = (-1)^m N^{2-2s}(2\pi)^{2s-4}\Gamma(2-s+\frac{m}{2})^2 L(2-s+\frac{m}{2}, \Theta_m)^2,$$

and

$$\pi^{-2s}\Gamma(s+\frac{m}{2})^2\Phi_m(s) = (-1)^m\pi^{2s-4}\Gamma(2-s+\frac{m}{2})^2\Phi_m(2-s),$$

since $\Psi_m(s) = L(s+\frac{m}{2}, \Theta_m)$. This implies $R_{ij}(s, P_m) = (-1)^m R_{ij}(2-s, P_m)$ for any i, j and any P_m, where $R_{ij}(s, P_m) = \pi^{-2s}\Gamma(s+\frac{m}{2})^2\phi_{ij}(s, P_m)$.

Since entries of X_m form a basis for $\mathcal{P}_m$ (see [35], page 160), it is enough to show that $\phi_{ij}(s, X_m) = e_j^{-1}e_i\phi_{ji}(s, X_m')$, where X_m' is the one obtained by taking conjugation

on each entry. Indeed,

$$\begin{aligned}
\phi_{ji}(s, X'_m) &= \sum_{\beta\in\Lambda_{ji}} a_{ji}(\beta) X'_m(\frac{\beta}{|\beta|})|\beta|^{-2s} \\
&= e_i^{-1}(\frac{N}{4})^s u_{ji}^{-s} \sum_{\alpha\in I_i^{-1}I_j} d(I_j^{-1}I_i\alpha) X'_m(\frac{\alpha}{|\alpha|})N(\alpha)^{-s} \\
&= e_i^{-1}(\frac{N}{4})^s u_{ji}^{-s} \sum_{\mathfrak{a}\sim_l I_j^{-1}I_i} d(\mathfrak{a}) \sum_{\alpha,\mathfrak{a}=I_j^{-1}I_i\alpha} X'_m(\frac{\alpha}{|\alpha|})N(\alpha)^{-s} \\
&= e_i^{-1}(\frac{N}{4})^s u_{ji}^{-s} \sum_{\mathfrak{a}\sim_l I_j^{-1}I_i} d(\mathfrak{a}) \sum_{\alpha,\mathfrak{a}=I_j^{-1}I_i\alpha} X_m(\frac{\overline{\alpha}}{|\alpha|})N(\alpha)^{-s}.
\end{aligned}$$

By changing $\alpha \to \overline{\alpha}$ in the second summation and then $\mathfrak{a} \to \overline{\mathfrak{a}}$ in the first summation, we have

$$\begin{aligned}
\phi_{ji}(s, X'_m) &= e_i^{-1}(\frac{N}{4})^s u_{ji}^{-s} \sum_{\mathfrak{a}\sim_l I_j^{-1}I_i} d(\mathfrak{a}) \sum_{\alpha,\mathfrak{a}=I_j^{-1}I_i\overline{\alpha}} X_m(\frac{\alpha}{|\alpha|})N(\alpha)^{-s} \\
&= e_i^{-1}(\frac{N}{4})^s u_{ji}^{-s} \sum_{\mathfrak{a}\sim_l I_j^{-1}I_i} d(\mathfrak{a}) \sum_{\alpha,\overline{\mathfrak{a}}=\alpha\overline{I}_i\overline{I}_j^{-1}} X_m(\frac{\alpha}{|\alpha|})N(\alpha)^{-s} \\
&= e_i^{-1}(\frac{N}{4})^s u_{ji}^{-s} \sum_{\mathfrak{a}\sim_r \overline{I}_i\overline{I}_j^{-1}} d(\overline{\mathfrak{a}}) \sum_{\alpha,\mathfrak{a}=\alpha\overline{I}_i\overline{I}_j^{-1}} X_m(\frac{\alpha}{|\alpha|})N(\alpha)^{-s}.
\end{aligned}$$

It is obvious that $d(\overline{\mathfrak{a}}) = d(\mathfrak{a})$ by Lemma 3.2.11; moreover, since $\overline{I}_j = I_j^{-1}N(I_j)$ and $\overline{I}_i^{-1} = I_iN(I_i)^{-1}$, we have $\overline{I}_j\overline{I}_i^{-1} = u_{ij}I_j^{-1}I_i$ and $\alpha \in \overline{I}_j\overline{I}_i^{-1}$ if and only if $\beta = u_{ij}^{-1}\alpha \in I_j^{-1}I_i$. So

$$\begin{aligned}
\phi_{ji}(s, X'_m) &= e_i^{-1}(\frac{N}{4})^s u_{ji}^{-s} \sum_{\alpha\in\overline{I}_j\overline{I}_i^{-1}} d(\overline{I}_i\overline{I}_j^{-1}\alpha) X_m(\frac{\alpha}{|\alpha|})N(\alpha)^{-s} \\
&= e_i^{-1}(\frac{N}{4})^s u_{ji}^{-s} \sum_{u_{ij}^{-1}\alpha\in I_j^{-1}I_i} d(I_i^{-1}I_ju_{ij}^{-1}\alpha) X_m(\frac{\alpha}{|\alpha|})N(\alpha)^{-s} \\
&= e_i^{-1}e_j\phi_{ij}(s, X_m), \quad \text{by setting } \beta = u_{ij}^{-1}\alpha.
\end{aligned}$$

Done. □

Now we prove our theorem on the fourth moment of L-functions associated to newforms as a corollary of Corollary 4.3.4.

Theorem 4.4.4 *As $T \to \infty$,*

$$\sum_{2<k\leq T} \sum_{f\in\mathcal{S}_k^{new}(N)} \int_{-T}^{T} |L(\frac{k}{2}+it,f)|^4 dt \ll T^3 \log^4 T.$$

Proof. Lemma 4.4.2 and Proposition 4.4.3 provide the assumptions in Corollary 4.3.4. So as $\theta \to \frac{\pi}{2}^-$,

$$\sum_{m>0,\ m \text{ even}} \sum_{\mathcal{P}_m}^{*} \sum_{i,j} \int_{-\infty}^{\infty} |M(2it,\theta)|^2 |\phi_{ij}(1+it,P_m)|^2\, dt \asymp \log^4(\sec\theta).$$

As we know (see [35], page 160), entries of $\sqrt{m+1}X_m$ constitute an orthonormal basis of $\mathcal{P}_m$, so entries of $\phi_{ij}^m(s)$ are exactly those $\frac{1}{\sqrt{m+1}}\phi_{ij}(s,P_m)$, where P_m's are entries of $\sqrt{m+1}X_m$. Hence

$$LHS = \sum_{m>0,\ m \text{ even}} (m+1) \sum_{i,j} \int_{-\infty}^{\infty} |M(2it,\theta)|^2 tr(\phi_{ij}^m(1+it)(\phi_{ij}^m(1+it))^*)\, dt,$$

which can be further simplified to

$$\sum_{m>0,\ m \text{ even}} (m+1) \int_{-\infty}^{\infty} |M(2it,\theta)|^2 tr(\Phi_m(1+it)(\Phi_m(1+it))^*)\, dt,$$

then to

$$\sum_{m>0,\ m \text{ even}} (m+1) \int_{-\infty}^{\infty} |M(2it,\theta)|^2 tr(\Psi_m^2(1+it)(\Psi_m^2(1+it))^*)\, dt.$$

For fixed $m > 0$, the Brandt matrices $B_m(n)$ $(n = 0, 1, 2...)$ are simultaneously diagonalizable and the resulting non-zero diagonal entries are the n-th coefficients of all new forms of level N, weight $m+2$, by Theorem 3.2.2. So there is a unitary matrix U, such that $U\Theta_m(\tau)U^{-1} = \text{diag}\{f_1, \cdots, f_{H(m+1)}\}$ and the subset of non-zero f_i's is $\mathcal{S}_{m+2}^{\text{new}}(N)$. As a result,

$$U\Psi_m(s)U^{-1} = UL(s+\frac{m}{2},\Theta_m)U^{-1} = \text{diag}\{L(s+\frac{m}{2},f_1),\cdots,L(s+\frac{m}{2},f_{H(m+1)})\},$$

so we have (setting $k = m+2$)

$$LHS = \sum_{k>2,\ k \text{ even}} (k-1) \sum_{f\in\mathcal{S}_k^{\text{new}}(N)} \int_{-\infty}^{\infty} |M(2it,\theta)|^2 |L(\frac{k}{2}+it,f)|^4\, dt.$$

By setting $T = \tan\theta$, as in [7], page 823, we obtain

$$\sum_{2<k\leq T}(k-1)\sum_{f\in\mathcal{S}_k^{\text{new}}(N)}\int_{-T}^{T}|L_f(\frac{k}{2}+it)|^4dt \ll T^4\log^4 T.$$

The theorem follows easily from this. $\square$

Chapter 5

Critical Values of Two-dimensional Artin L-functions

In this chapter, we will generalize a result of Moreno ([20]), which relates the critical value of some Artin L-functions to the Petersson inner product by means of Strong Artin Conjecture.

5.1 Introduction

Let $K/\mathbb{Q}$ be a Galois extension with $Gal(K/\mathbb{Q}) = S_3$ and $\rho : S_3 \longrightarrow GL_2(\mathbb{C})$ be the irreducible two dimensional representation. Then in [20, Theorem 7], Moreno gave the identity (the notations are slightly different from his original paper) for some nonzero constant c

$$cL(1/2, \chi_2)L(1/2, \rho) =< f^* f_\rho, f_\rho \rangle,$$

where χ_2 is the nontrivial linear character of S_3, f_ρ is the cusp form associated to ρ by Strong Artin Conjecture, f^* is the derivative of a Eisenstein series and the inner product is the Petersson inner product. See Section 5.2 for details.

So such an equality connects the vanishing of the value of an L-function at 1/2 with

the existence of f_ρ in the spectral decomposition of the function $f^* f_\rho$.

Although he assumed that ρ is odd, Moreno showed, in another paper [19], that the technique also works in the even case.

In this paper, we follow the same idea and formulate the general equality in Section 5.2. Then in Section 5.3 we apply it to the case of $\widetilde{S}_4$ and we remark here that all other cases can be similarly treated.

5.2 General Equality

Before we state the general equality, let us first set up the notations.

Let $\mathbb{H}$ be the upper half plane, $S = \{z \in \mathbb{H} : |x| \leq 1/2\}$ and let N be a positive integer.

Choose a fundamental domain of $\Gamma_0(N)\backslash\mathbb{H}$ in S and denote it by $\mathcal{F}(N)$. Then we can choose a complete set of representatives $\{\sigma\}$ for $\Gamma_0(N)_\infty\backslash\Gamma_0(N)$ s.t. $S = \coprod_\sigma \sigma\mathcal{F}(N)$ in the sense that two sides differ by a measure zero set. Here $\Gamma_0(N)_\infty$ is the stabilizer of the cusp ∞ in $\Gamma_0(N)$, namely

$$\Gamma_0(N)_\infty = \left\{ \begin{pmatrix} a & b \\ 0 & d \end{pmatrix} : ad = 1, a, b, d \in \mathbb{Z} \right\}.$$

Let $E(z, s, \Gamma_0(N))$ be the Eisenstein series defined by

$$E(z, s, \Gamma_0(N)) = \sum_{\sigma \in \Gamma_0(N)_\infty \backslash \Gamma_0(N)} Im(\sigma z)^{\frac{s+1}{2}}.$$

Recall that $E(z, s, \Gamma_0(N)) = f^*(z)s + O(s^2)$ where $f^*(z) = f^*(z; N)$ satisfies

$$f^*(\sigma z) = f^*(z), \text{ for any } \sigma \in \Gamma_0(N), \quad \text{and} \quad \Delta f^* = \frac{1}{4} f^*.$$

For a modular form f, let us introduce the K operator, i.e., $K(f)(z) = \overline{f(-\overline{z})}$. If $f, h \in \mathcal{S}_1(N, \epsilon)$, then the Petersson inner product takes the form

$$\langle f, h \rangle = \frac{1}{[\Gamma(1) : \Gamma_0(N)]} \int_{\mathcal{F}(N)} y f(z) \overline{h(z)} \frac{dxdy}{y^2};$$

If f and h are two Maass cusp forms of weight 0 and level N, then the Petersson inner product is

$$\langle f, h\rangle = \frac{1}{[\Gamma(1) : \Gamma_0(N)]} \int_{\mathcal{F}(N)} f(z)\overline{h(z)}\frac{dxdy}{y^2}.$$

Let $K/\mathbb{Q}$ be a finite Galois extension with Galois group G. Assume $\rho : G \to GL_2(\mathbb{C})$ is an irreducible Galois representation. Let N be the Artin conductor and $\epsilon = \det(\rho)$. Then we know that its Artin L-function is of the form:

$$L(s, \rho) = \sum_{n=1}^{\infty} a(n)n^{-s} = \prod_{p|N}(1 - a(p)p^{-s})^{-1} \prod_{p\nmid N}(1 - a(p)p^{-s} + \epsilon(p)p^{-2s})^{-1}.$$

Denote $L_p(s, \rho)$ the p-factor above and let $L_M(s, \rho) = \prod_{p|M} L_p(s, \rho)$, for any positive integer M. Similarly $\zeta_M(s) = \prod_{p|M}(1 - p^{-s})^{-1}$.

Let us first work on the calculations on the automorphic side. There are two lemmas.

Lemma 5.2.1 *Let $f(z) = \sum_{n=1}^{\infty} a(n)q^n \in \mathcal{S}_1(N_1, \epsilon_1)$ and $h(z) = \sum_{n=1}^{\infty} b(n)q^n \in \mathcal{S}_1(N_2, \epsilon_2)$. Let $N = N_1N_2$ and $f^*(z) = f^*(z; N)$. Then*

(a) if $\epsilon_1 = \epsilon_2$,

$$(4\pi)^{-\frac{1+s}{2}}\Gamma(\frac{1+s}{2})\sum_{n=1}^{\infty} a(n)\overline{b(n)}n^{-\frac{1+s}{2}} = [\Gamma(1) : \Gamma_0(N)]\langle f^*f, h\rangle s + O(s^2); \tag{5.1}$$

(b) if $\epsilon_1 = \epsilon_2^{-1}$,

$$(4\pi)^{-\frac{1+s}{2}}\Gamma(\frac{1+s}{2})\sum_{n=1}^{\infty} a(n)b(n)n^{-\frac{1+s}{2}} = [\Gamma(1) : \Gamma_0(N)]\langle f^*f, K(h)\rangle s + O(s^2). \tag{5.2}$$

Proof. Consider the following integral

$$I = \int_S y^{1+\frac{1+s}{2}} f(z)\overline{h(z)}\frac{dxdy}{y^2}.$$

On one hand,

$$\begin{aligned} I &= \int_0^\infty \int_{-1/2}^{1/2} y^{1+\frac{1+s}{2}} (\sum_{n=1}^\infty a(n)q^n)(\sum_{n=1}^\infty \overline{b(n)}\overline{q}^n)\frac{dxdy}{y^2} \\ &= \sum_{m=1}^\infty \sum_{n=1}^\infty \int_0^\infty y^{1+\frac{1+s}{2}} a(m)\overline{b(n)} \int_{-1/2}^{1/2} q^m \overline{q}^n dx \frac{dy}{y^2} \\ &= \sum_{n=1}^\infty a(n)\overline{b(n)} \int_0^\infty y^{\frac{1+s}{2}} e^{-4\pi n y} \frac{dy}{y} \\ &= (4\pi)^{-\frac{1+s}{2}} \Gamma(\frac{1+s}{2}) \sum_{n=1}^\infty a(n)\overline{b(n)} n^{-\frac{1+s}{2}} \end{aligned}$$

which is the same as the left-hand side of (4.1).

On the other hand,

$$\begin{aligned} I &= \sum_\sigma \int_{\sigma\mathcal{F}(N)} y^{1+\frac{1+s}{2}} f(z)\overline{h(z)} \frac{dxdy}{y^2} \\ &= \sum_\sigma \int_{\mathcal{F}(N)} Im(\sigma z)^{1+\frac{1+s}{2}} f(\sigma z)\overline{h(\sigma z)} \frac{dxdy}{y^2} \end{aligned}$$

where σ runs through the chosen set of representatives for $\Gamma_0(N)_\infty \backslash \Gamma_0(N)$.

By automorphy of f and h,

$$\begin{aligned} Im(\sigma z) f(\sigma z)\overline{h(\sigma z)} &= \frac{y}{|cz+d|^2} \epsilon(d)(cz+d) f(z) \overline{\epsilon}(d)(c\overline{z}+d)\overline{h(z)} \\ &= y f(z)\overline{h(z)}. \end{aligned}$$

Moreover, we know the measure $y^{-2}dxdy$ is invariant under $\Gamma_0(N)$, hence

$$\begin{aligned} I &= \sum_\sigma \int_{\mathcal{F}(N)} Im(\sigma z)^{\frac{1+s}{2}} y f(z)\overline{h(z)} \frac{dxdy}{y^2} \\ &= \int_{\mathcal{F}(N)} E(z,s,\Gamma_0(N)) y f(z)\overline{h(z)} \frac{dxdy}{y^2} \\ &= (\int_{\mathcal{F}(N)} y(f^* f)(z)\overline{h(z)} \frac{dxdy}{y^2})s + O(s^2) \end{aligned}$$

which is right-hand side of (4.1).

We can prove (4.2) along the same lines above except that we use the integral

$$I' = \int_S y^{1+\frac{1+s}{2}} f(z) h(-\overline{z}) \frac{dxdy}{y^2},$$

instead of I above. We are done. $\square$

Next lemma deals with the real analytic case. Let $s' = \frac{s+1}{2}$.

Lemma 5.2.2 *Let*

$$f(z) = \sum_{n\neq 0} a(n) y^{1/2} K_0(2\pi|n|y) e^{2\pi i n x}$$
$$h(z) = \sum_{n\neq 0} b(n) y^{1/2} K_0(2\pi|n|y) e^{2\pi i n x}$$

be two Maass cusp forms (weight 0) of eigenvalues $\frac{1}{4}$ with central characters ϵ_1, ϵ_2, and levels N_1, N_2, respectively. Let $N = N_1 N_2)$ and $f^*(z) = f^*(z; N)$. Assume further that f, h have the same parity, i.e., $a(-n)b(-n) = a(n)b(n)$. Then

(a) if $\epsilon_1 = \epsilon_2$,

$$\frac{(\Gamma(\frac{s'}{2}))^4}{4\pi^{s'}\Gamma(s')} \sum_{n=1}^{\infty} a(n)\overline{b(n)} n^{-s'} = [\Gamma(1) : \Gamma_0(N)]\langle f^* f, h\rangle s + O(s^2); \tag{5.3}$$

(b) if $\epsilon_1 = \epsilon_2^{-1}$,

$$\frac{(\Gamma(\frac{s'}{2}))^4}{4\pi^{s'}\Gamma(s')} \sum_{n=1}^{\infty} a(n)b(n) n^{-s'} = [\Gamma(1) : \Gamma_0(N)]\langle f^* f, K(h)\rangle s + O(s^2). \tag{5.4}$$

Proof. Consider the integral

$$J = \int_S f(z)\overline{h(z)} y^{s'} \frac{dxdy}{y^2}.$$

As we did in the holomorphic case, we shall compute J in two different ways.

On one hand,

$$\begin{aligned} J &= \int_0^\infty \Big(\int_{-1/2}^{1/2} f(z)\overline{h(z)} dx\Big) y^{s'-2} dy \\ &= \int_0^\infty \sum_{m\neq 0, n\neq 0} a(m)\overline{b(n)} y^{s'-1} K_0(2\pi|m|y) K_0(2\pi|n|y) \Big(\int_{-1/2}^{1/2} e^{2\pi i(m-n)x} dx\Big) dy \\ &= \sum_{n\neq 0} a(n)\overline{b(n)} \int_0^\infty K_0(2\pi|n|y) K_0(2\pi|n|y) y^{s'-1} dy \end{aligned}$$

Now the identity, with $Re(\alpha) > 0$ and $Re(1 - \rho \pm r \pm r') > 0$,

$$\begin{aligned} &\int_0^\infty K_r(\alpha t) K_{r'}(\alpha t) t^{-\rho} dy \\ = \; & \frac{\alpha^{\rho-1}}{2^{\rho+2}\Gamma(1-\rho)} \Gamma\Big(\frac{1-\rho+r+r'}{2}\Big)\Gamma\Big(\frac{1-\rho+r-r'}{2}\Big)\Gamma\Big(\frac{1-\rho-r+r'}{2}\Big)\Gamma\Big(\frac{1-\rho-r-r'}{2}\Big) \end{aligned}$$

implies

$$J = \frac{(\Gamma(\frac{s'}{2}))^4}{4\pi^{s'}\Gamma(s')} \sum_{n=1}^{\infty} a(n)\overline{b(n)}n^{-s'}$$

which is the left-hand side of (4.3). This is where we need the parity condition.

On the other hand,

$$\begin{aligned}
J &= \sum_{\sigma} \int_{\sigma\mathcal{F}(N)} f(z)\overline{h(z)}y^{s'}\frac{dxdy}{y^2} \\
&= \sum_{\sigma} \int_{\mathcal{F}(N)} f(\sigma z)\overline{h(\sigma z)}Im(\sigma z)^{s'}\frac{dxdy}{y^2} \\
&= \sum_{\sigma} \int_{\mathcal{F}(N)} \epsilon(d)(\frac{c\overline{z}+d}{|cz+d|})^{-1}f(z)\overline{\epsilon}(d)\overline{(\frac{c\overline{z}+d}{|cz+d|})^{-1}h(z)}Im(\sigma z)^{s'}\frac{dxdy}{y^2} \\
&= \sum_{\sigma} \int_{\mathcal{F}(N)} f(z)\overline{h(z)}Im(\sigma z)^{s'}\frac{dxdy}{y^2} \\
&= \int_{\mathcal{F}(N)} E(z,s,\Gamma_0(N))f(z)\overline{h(z)}\frac{dxdy}{y^2} \\
&= (\int_{\mathcal{F}(N)} (f^*f)(z)\overline{h(z)}\frac{dxdy}{y^2})s + O(s^2)
\end{aligned}$$

which is exactly the right-hand side of (4.3). So we are done with (a).

For (4.4), we carry out the same process except we replace J with

$$J' = \int_S f(z)h(-\overline{z})y^{s'}\frac{dxdy}{y^2}.$$

We are done. □

On the Galois side, we have an analogous lemma. Let us first recall an elementary result:

Lemma 5.2.3 *Assume we have*

$$\sum_{n=1}^{\infty} A(n)T^n = (1-\alpha_1 T)^{-1}(1-\alpha_2 T)^{-1},$$

$$\sum_{n=1}^{\infty} B(n)T^n = (1-\beta_1 T)^{-1}(1-\beta_2 T)^{-1}.$$

Then we have

$$\sum_{n=1}^{\infty} A(n)B(n)T^n = (1-\alpha_1\alpha_2\beta_1\beta_2 T^2)\prod_{i,j=1,2}(1-\alpha_i\beta_j T)^{-1}.$$

Proof. See Lemma 1.6.1 in Bump's book [4]. □

Lemma 5.2.4 *Let $\rho_1, \rho_2 : Gal(\overline{\mathbb{Q}}/\mathbb{Q}) \to GL_2(\mathbb{C})$ be two irreducible Galois representations with determinant characters ϵ_1 and ϵ_2 respectively. Assume*

$$L(s, \rho_1) = \sum_{n=1}^{\infty} a(n)n^{-s} \quad \text{and} \quad L(s, \rho_2) = \sum_{n=1}^{\infty} b(n)n^{-s}.$$

Then

(a) if $\epsilon_1 = \epsilon_2$, there is a nonzero constant c, s.t.

$$\sum_{n=1}^{\infty} a(n)\overline{b(n)}n^{-\frac{1+s}{2}} = cL(1/2, \rho_1 \otimes \overline{\rho_2})s + O(s^2); \tag{5.5}$$

(b) if $\epsilon_1 = \epsilon_2^{-1}$, there is a nonzero constant c, s.t.

$$\sum_{n=1}^{\infty} a(n)b(n)n^{-\frac{1+s}{2}} = cL(1/2, \rho_1 \otimes \rho_2)s + O(s^2). \tag{5.6}$$

Proof. Assume $\epsilon_1 = \epsilon_2$. Let N be the least common multiple of the conductors of ρ_1,ρ_2 and $\rho_1 \otimes \overline{\rho_2}$. For $p \nmid N$, by Lemma 5.2.3, we have the formal identity

$$\frac{1}{1-T^2} \sum_{n=1}^{\infty} a(p^n)\overline{b(p^n)}T^n = det(I - \rho_1 \otimes \overline{\rho_2}(\sigma_p)T)^{-1}.$$

By setting $T = p^{-s}$ above, we have

$$\begin{aligned}
& \zeta(2s)\zeta_N(2s)^{-1} \sum_{n=1}^{\infty} a(n)\overline{b(n)}n^{-s} \\
= \; & \prod_{p \nmid N} \frac{1}{1-p^{2s}} \prod_{p|N} (\sum_{n=1}^{\infty} a(p^n)\overline{b(p^n)}p^{-ns}) \prod_{p \nmid N} (\sum_{n=1}^{\infty} a(p^n)\overline{b(p^n)}p^{-ns}) \\
= \; & L_N(s, \rho_1, \overline{\rho_2}) \prod_{p \nmid N} (\frac{1}{1-p^{2s}} \sum_{n=1}^{\infty} a(p^n)\overline{b(p^n)}p^{-ns}) \\
= \; & L_N(s, \rho_1, \overline{\rho_2}) \prod_{p \nmid N} det(I - \rho_1 \otimes \overline{\rho_2}(\sigma_p)T)^{-1} \\
= \; & \frac{L_N(s, \rho_1, \overline{\rho_2})}{L_N(s, \rho_1 \otimes \overline{\rho_2})} L(s, \rho_1 \otimes \overline{\rho_2})
\end{aligned}$$

where $L_N(s, \rho_1, \overline{\rho_2}) = \prod_{p|N} (\sum_{n=1}^{\infty} a(p^n)\overline{b(p^n)}p^{-ns})$. Again by the Lemma 5.2.3, we know it is a product of factors in the form of $(1 - \lambda p^{-s})^{-1}$ where by basic representation theory $|\lambda| = 1$.

Let

$$C(s) = \frac{L_N(s, \rho_1, \overline{\rho_2})\zeta_N(2s)}{L_N(s, \rho_1 \otimes \overline{\rho_2})},$$

so again $C(s)$ is a product of factors in the form of $(1 - \lambda p^{-s})^{-1}$ or $(1 - \lambda p^{-s})$. Since $|\lambda| = 1$, so they have no zeros at $\frac{1}{2}$. And

$$\sum_{n=1}^{\infty} a(n)\overline{b(n)}n^{-s} = C(s)\zeta(2s)^{-1}L(s, \rho_1 \otimes \overline{\rho_2}). \tag{5.7}$$

We know that $\zeta(1+s)^{-1} = s + O(s^2)$, and by changing variable $s \to \frac{1+s}{2}$ and setting $s = 0$ in other factors in the right-hand side of (4.7), we obtain

$$\sum_{n=1}^{\infty} a(n)\overline{b(n)}n^{-\frac{1+s}{2}} = C(1/2)L(1/2, \rho_1 \otimes \overline{\rho_2})s + O(s^2).$$

Set $c = C(1/2)$ which is not zero and we are done with (a). Proof of (b) is exactly the same as that of (a). Done. □

Putting together what we have done above, we obtain the following theorem.

Theorem 5.2.5 *Let $\rho_1, \rho_2 : \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \longrightarrow GL_2(\mathbb{C})$ be two irreducible representations with determinant characters ϵ_1, ϵ_2, respectively. Assume they are both odd or even and both modular, corresponding to newforms f and h respectively. Let N be any positive integer divisible by the conductors of ρ_1 and ρ_2, and $f^*(z) = f^*(z; N)$.*

(a) If $\epsilon_1 = \epsilon_2$, then $\exists\ c \neq 0$, s.t.,

$$\langle f^* f, h\rangle = cL(1/2, \rho_1 \otimes \overline{\rho_2});$$

(b) If $\epsilon_1 = \epsilon_2^{-1}$, then $\exists\ c \neq 0$, s.t.,

$$\langle f^* f, K(h)\rangle = cL(1/2, \rho_1 \otimes \rho_2);$$

Proof. If ρ_1, ρ_2 are both odd, i.e. f and h are holomorphic, and $\epsilon_1 = \epsilon_2$, then Lemma 5.2.1(a) and Lemma 5.2.4(a) together imply that $\exists\ c_1 \neq 0$ s.t.

$$[\Gamma(1) : \Gamma_0(N)]\langle f^* f, h\rangle = c_1(4\pi)^{-1/2}\Gamma(1/2)L(1/2, \rho_1 \otimes \overline{\rho_2}).$$

Here all factors except the inner product and the L-function factor are nonzero and we obtain the existence of c, which proves one of the two cases in (a).

All other cases can be shown similarly by simply combining Lemma 5.2.1, Lemma 5.2.2 and Lemma 5.2.4. Done. □

5.3 Applications

Now we can apply Theorem 5.2.5 to any modular irreducible 2-dimensional Galois representation ρ. In particular, it applies to all cases except the icosahedral case, the last unproven case in Strong Artin Conjecture. Since all these cases are similar, we shall only deal with the example when the image of ρ is isomorphic to $\widetilde{S}_4$.

Let us look at the character table of $\widetilde{S}_4$ in Appendix A.3.

It is trivial to check that $\chi_3 = \mathrm{Sym}^2(\chi_2)$, $\mathrm{Sym}^2(\chi_2') = \chi_2' + \chi_1$, $\chi_2'' = \chi_2\chi_1'$, $\chi_3' = \chi_3\chi_1'$ and $\chi_4 = \chi_2\chi_2'$. Explicitly, χ_2 corresponds to ρ where

$$\begin{aligned} \rho : \qquad & GL_2(\mathbb{F}_3) \longrightarrow GL_2(\mathbb{Z}[-\sqrt{2}]) \subset GL_2(\mathbb{C}) \\ & \begin{pmatrix} -1 & 1 \\ -1 & 0 \end{pmatrix} \longmapsto \begin{pmatrix} -1 & 1 \\ -1 & 0 \end{pmatrix} \\ & \begin{pmatrix} 1 & -1 \\ 1 & 1 \end{pmatrix} \longmapsto \begin{pmatrix} 1 & -1 \\ -\sqrt{-2} & -1+\sqrt{-2} \end{pmatrix}. \end{aligned}$$

So $\det \chi_2 = \det \chi_2''$ is not trivial, hence must be χ_1'. Consequently,

$$\chi_2^2 = \chi_3 + \chi_1' \quad \text{and} \quad \chi_2\chi_2'' = \chi_3' + \chi_1.$$

Moreover, the representation corresponds to χ_2' is obtained by the irreducible 2-dimensional representation of S_3 via the surjective homomorphisms: $\widetilde{S}_4 \to S_4 \to S_3$. The determinant of that of S_3 is not trivial and we know $\det(\chi_2') = \chi_1'$ too.

We know that the strong Artin conjecture is true for all those two dimensional representations. Apply Theorem 5.2.5, and we obtain

Theorem 5.3.1 *Let f_i $(i = 1, 2, 3)$ be the three modular forms (either all holomorphic or all real analytic) for χ_2, χ_2' and χ_2'', resp.. Then there exist non-zero constants c_j, $j = 1, 2, 3$, such that*

$$\langle f^* f_1, f_1 \rangle = c_1 L(1/2, \chi_1') L(1/2, \chi_3),$$

$$\langle f^* f_1, f_3 \rangle = c_2 L(1/2, \chi_3'),$$

$$\langle f^* f_1, f_2 \rangle = c_3 L(1/2, \chi_4).$$

Proof. By the above observations, we can directly apply Theorem 5.2.5 for each pair, (f_1, f_1), (f_1, f_3) and (f_1, f_2). Using the above decompositions and grouping all non-zero constants together, the theorem follows. □

In applying these results to non-vanishing result at $\frac{1}{2}$, calculating the Petersson inner products on the left hand sides becomes crucial. It is totally mysterious how the multiplication of f^* affects the spectrum decomposition.

Chapter 6

Modularity of S_5-Galois Representations

In this chapter, we shall give a sufficient condition for the modularity of irreducible 4-dimensional Galois representations ρ with image S_5, the permutation group on five letters. Roughly speaking, it reduces the modularity of ρ to the modularity of an icosahedral representation over a quadratic field. Please see Appendix for the character tables involved.

6.1 Introduction

Given a number field F, denote by G_F the absolute Galois group of F, that is $G_F = \mathrm{Gal}(\bar{F}/F)$.

Let $\rho : G_F \to GL_4(\mathbb{C})$ be a four dimensional Galois representation with image isomorphic to S_5. This makes sense since we know there are two four dimensional representations for S_5 (see Table A.2 in Appendix).

Let K/F be the S_5-Galois extension fixed by $ker(\rho)$, so $ker(\rho) = G_K$. We say K/F has a double cover $\widetilde{K}$, if $\widetilde{K}/K$ is Galois and $\mathrm{Gal}(\widetilde{K}/K) = \widetilde{S}_5$, where $\widetilde{S}_5$ is the one of the two C_2-central extensions in which a transposition in S_5 has preimages of order 2 in $\widetilde{S}_5$.

Here C_2 is the group of order 2.

Assume this is the case, and denote E the subfield of K which is quadratic over F. Then $\mathrm{Gal}(K/E) = A_5$ and $\widetilde{K}/E$ is Galois with $\mathrm{Gal}(\widetilde{K}/E) \simeq \widetilde{A}_5$, the unique double cover of A_5. Hence we have a two dimensional (icosahedral) Galois representation σ of G_E with $ker(\sigma) = G_{\widetilde{K}}$. Here is the picture:

$$\begin{tikzcd}
 & \widetilde{K} \arrow[dd, dash, "\widetilde{A}_5"] \\
K \arrow[ur, dash, "2"] \arrow[dr, dash, "A_5"] \arrow[dd, dash, "S_5"'] & \\
 & E \arrow[dl, dash, "2"] \\
F &
\end{tikzcd}$$

In this chapter, we consider the modularity of ρ and our main theorem says that the modularity of σ implies that of ρ. The idea of the proof is to connect ρ with the Asai lift of σ by simple computations of characters.

In the last section, we will discuss an open problem, namely, how to construct an affirmative example for the Langlands Functoriality Conjecture in this case.

6.2 Modularity of ρ and σ

Before we get to our main theorem, let us first recall the concept of Asai lift (see [28] or [11] for details). Let E/F be a quadratic extension of number fields with ring of adeles $\mathbb{A}_E$, $\mathbb{A}_F$, respectively.

On the Galois side, let $\sigma : \mathrm{Gal}(\overline{F}/E) \to GL_2(\mathbb{C})$ be an irreducible representation. The Asai lift of σ, denoted by $As(\sigma)$, is given by

$$\wedge^2(Ind_E^F(\sigma)) = (As(\sigma) \otimes \omega_{E/F}) \oplus Ind_E^F(det(\sigma)),$$

where $\omega_{E/F}$ is the quadratic grösencharacter of F attached to E/F by class field theory.

On the automorphic side, let $\mathbf{G} = Res_{K/F}GL_n$ be quasi-split group obtained by

restriction of scalars and we know the L-group is

$$^L\mathbf{G} = (GL_2(\mathbb{C}) \times GL_2(\mathbb{C})) \rtimes \mathrm{Gal}(E/F),$$

where the generator θ of $\mathrm{Gal}(E/F)$ acts by changing the two factors. One defines a representation

$$r : {}^L\mathbf{G} \to GL_4(\mathbb{C}) = GL(\mathbb{C}^2 \otimes \mathbb{C}^2) \cong {}^LGL_4,$$

by setting, for $x, y \in \mathbb{C}^2$,

$$r(g, g'; 1)(x \otimes y) = g(x) \otimes g'(y); r(1, 1; \theta)(x \otimes y) = y \otimes x.$$

Let $\pi = \otimes_v \pi_v$ be a cuspidal automorphic representation of $\mathbf{G}(\mathbb{A}_F) = GL_2(\mathbb{A}_E)$ where each Π_v has the local parametrization $\phi_v : W_{F_v} \times SL_2(\mathbb{C}) \to {}^L\mathbf{G}$ by local Langlands correspondence. Let $As(\pi_v)$ be the irreducible admissible representation of $GL_4(F_v)$ attached to $r \circ \phi_v$, and then $As(\pi) = \otimes_v As(\pi_v)$ is an irreducible admissible representation of $GL_4(\mathbb{A}_{\mathbb{F}})$. The following theorem is first proved by Ramakrishnan [28] and then by Krishnamurthy [14] and Kim [11] using different methods.

Theorem 6.2.1 (Ramakrishnan [28]) *The Asai lift of π is automorphic.*

Let the notations be the same as those in the introduction of this chapter. Now we can state and prove our main theorem.

Theorem 6.2.2 *Assume K has a double cover. Then if σ is modular, so is ρ.*

Proof. Now σ is one of the two dimensional representations of $\widetilde{A}_5$ corresponding to χ_2 or χ_2' in Table A.4, Appendix. Direct calculation shows that $Ind_{\widetilde{A}_5}^{\widetilde{S}_5}\sigma$ has character $\widetilde{\chi}_4$ in Table A.5, Appendix. Moreover, $\Lambda^2(Ind_{\widetilde{A}_5}^{\widetilde{S}_5}\sigma)$ has character row

$$6 \quad 6 \quad 2 \quad 3 \quad 3 \quad 0 \quad 0 \quad 2 \quad -1 \quad -1 \quad 1 \quad 1 \cdot$$

Of course $det(\sigma) = \Lambda^2(\sigma)$ is trivial since the only one dimensional character of $\widetilde{A}_5$ is the trivial one (see Table A.4). So we can get the character row of $Ind_{\widetilde{A}_5}^{\widetilde{S}_5}(det(\sigma))$ as follows:

$$2 \quad 2 \quad 0 \quad 2 \quad 2 \quad 0 \quad 0 \quad 2 \quad 0 \quad 0 \quad 2 \quad 2 \cdot$$

As we know(here χ_1' is the one in Table A.5),

$$\Lambda^2(Ind_{\widetilde{A}_5}^{\widetilde{S}_5}\sigma) = As(\sigma) \otimes \chi_1' \oplus Ind_{\widetilde{A}_5}^{\widetilde{S}_5}(det(\sigma)).$$

And finally we get the character row of $As(\sigma) \otimes \chi_1'$

$$4 \quad 4 \quad 2 \quad 1 \quad 1 \quad 0 \quad 0 \quad 0 \quad -1 \quad -1 \quad -1 \quad -1$$

which is exactly χ_4 of $\widetilde{S}_5$.

So if we know that σ is modular, then so is $As(\sigma)$ and ρ, since the character of ρ is either χ_4 or $\chi_4' = \chi_4\chi_1'$. We are done. $\square$

6.3 An Open Problem

The proof of the modularity of general ρ may be too much to ask for the moment. However, just as Buhler did for an icosahedral representation in [3], it is natural and also interesting to ask the following question:

Open Problem: Can we find an affirmative example, that is, a modular four-dimensional S_5-Galois representation over $\mathbb{Q}$?

Theorem 6.2.2 suggests that we find an S_5-field K that has double cover and then it reduces to show that the corresponding two dimensional icosahedral representation is modular. Let us see some results that may be helpful for solving this problem.

Let us assume from now on $F = \mathbb{Q}$ and let $f \in \mathbb{Q}[X]$ be a irreducible quintic polynomial whose splitting field is K and $\mathrm{Gal}(K/\mathbb{Q}) \cong S_5$. Assume L is one of the root fields for f, so K is the Galois closure of L.

Let Q_L be the trace form of $L/\mathbb{Q}$. Let d_L denote the discriminant of the field $L/\mathbb{Q}$. We quote the following result from [31], which is Proposition 1 therein.

Theorem 6.3.1 (Serre) *$\widetilde{K}$ exists if and only if Q_L is equivalent to $I_3 \oplus \langle 2, 2d_L \rangle$.*

Suppose $\widetilde{K}$ exists and we want to attach a Hilbert modular form to the resulting σ. We need $d_L > 0$, since the quadratic subfield needs to be real. Then based on the corollary to Proposition 7 in [31] and some simple calculations, we know that for the splitting field of the quintic polynomials $X^5 + aX + b$ with $a, b \in \mathbb{Q}$ to have a double cover, d_L must be negative. So we need more terms in the polynomials. Among some examples that we worked on, let us note down the following:

$$f(X) = X^5 - 6X^3 - X^2 + 4X - 1.$$

It is irreducible and has splitting field an S_5-field with double cover. The discriminant is 36497; 36497 is a prime and the narrow class number of $\mathbb{Q}(\sqrt{36497})$ is one.

Now the main difficulty is the modularity of σ and we do not have many results on the general theory or explicit constructions. The idea of Achimescu and Saha in [1] seems not feasible in practice.

Appendix: Character Tables

In this appendix, we will present some character tables for some finite groups that appear in this thesis. In those tables, the first row gives some typical representative of each conjugacy class and the second row consists of the sizes of all conjugacy classes.

A.1 : Character Table of A_5

As usual, A_5 is considered as the group of even permutations on five letters. Here $u = \frac{1+\sqrt{5}}{2}$, $v = \frac{1-\sqrt{5}}{2}$. This table is available in many references, for example [9].

Class	1	(123)	(12)(34)	(12345)	(13452)
Size	1	20	15	12	12
χ_1	1	1	1	1	1
χ_4	4	1	0	-1	-1
χ_5	5	-1	1	0	0
χ_3	3	0	-1	u	v
$\chi_3^{'}$	3	0	-1	v	u

A.2 : Character Table of S_5

As usual, S_5 is the group of permutations on five letters. This table is also available in [9].

Class	1	(12)	(123)	(1234)	(12345)	(12)(34)	(12)(345)
Size	1	10	20	30	24	15	20
χ_1	1	1	1	1	1	1	1
$\chi_1^{'}$	1	-1	1	-1	1	1	-1
χ_4	4	2	1	0	-1	0	-1
$\chi_4^{'}$	4	-2	1	0	-1	0	1
χ_6	6	0	0	0	1	-2	0
χ_5	5	1	-1	-1	0	1	1
$\chi_5^{'}$	5	-1	-1	1	0	1	-1

A.3 : Character Table of $\widetilde{S}_4$

Here S_4 is the permutation group on 4 letters and $\widetilde{S}_4$ is the degree 2 non-trivial central extension of S_4, up to isomorphism, where a transposition has only preimages of order 2. Degree 2 non-trivial central extension means that

$$1 \to C_2 \to \widetilde{S}_4 \to S_4 \to 1$$

is a non-split exact sequence and C_2 is in the center of $\widetilde{S}_4$. Here C_2 is the cyclic group of order 2. It turns out that $\widetilde{S}_4 \simeq GL_2(\mathbb{F}_3)$. See [12] for this table.

class	I	$-I$	$\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$	$\begin{pmatrix} 2 & 1 \\ 0 & 2 \end{pmatrix}$	$\begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$	$\begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$	$\begin{pmatrix} 1 & 2 \\ 1 & 1 \end{pmatrix}$	$\begin{pmatrix} 2 & 2 \\ 1 & 2 \end{pmatrix}$
size	1	1	8	8	12	6	6	6
χ_1	1	1	1	1	1	1	1	1
χ_1'	1	1	1	1	-1	1	-1	-1
χ_2	2	-2	-1	1	0	0	$-\sqrt{-2}$	$\sqrt{-2}$
χ_2'	2	2	-1	-1	0	2	0	0
χ_2''	2	-2	-1	1	0	0	$\sqrt{-2}$	$-\sqrt{-2}$
χ_3	3	3	0	0	1	-1	-1	-1
χ_3'	3	3	0	0	-1	-1	1	1
χ_4	4	-4	1	-1	0	0	0	0

A.4 : Character Table of $\widetilde{A}_5$

$\widetilde{A}_5$ is the unique degree 2 non-trivial central extension of A_5, up to isomorphism. It turns out that $\widetilde{A}_5 \simeq SL_2(\mathbb{F}_5)$. See [9] for the computation of this table and also Table App7.1 in [3]. Note that there are some misprints in the latter table.

Class	(1^5)	$(1^5)'$	$(5)_1$	$(5)_2$	$(5)'_1$	$(5)'_2$	(12^2)	(13^2)	$(13^2)'$
Order	1	1	12	12	12	12	30	20	20
χ_1	1	1	1	1	1	1	1	1	1
χ_5	5	5	0	0	0	0	1	-1	-1
χ_6	6	-6	1	1	-1	-1	0	0	0
χ_3	3	3	u	v	u	v	-1	0	0
χ_3'	3	3	v	u	v	u	-1	0	0
χ_4	4	4	-1	-1	-1	-1	0	1	1
χ_4'	4	-4	-1	-1	1	1	0	-1	1
χ_2	2	-2	-u	-v	u	v	0	1	-1
χ_2'	2	-2	-v	-u	v	u	0	1	-1

As before $u = \frac{1+\sqrt{5}}{2}$, $v = \frac{1-\sqrt{5}}{2}$. We use the subscripts $_{1,2}$ to distinguish the possible two classes in A_5 belonging to the given partition and use the superscript $'$ to distinguish the possible two classes in $\widetilde{A}_5$ with the same projection in A_5.

A.5 : Character Table of $\widetilde{S}_5$

$\widetilde{S}_5$ is one of the two degree 2 non-trivial central extension of S_5, up to isomorphism, where a transposition has only preimages of order 2. Some authors denote it by $\widetilde{S}_5^+$ and denote the other one by $\widetilde{S}_5^-$. The character tables of them are closely related and can be computed from each other easily. See [21] for the computations.

Class	(1^5)	$(1^5)'$	$(1^3 2)$	$(1^2 3)$	$(1^2 3)'$	(14)	$(14)'$	(12^2)	(23)	$(23)'$	(5)	$(5)'$
Order	1	1	20	20	20	30	30	30	20	20	24	24
χ_1	1	1	1	1	1	1	1	1	1	1	1	1
χ_1'	1	1	-1	1	1	-1	-1	1	-1	-1	1	1
χ_4	4	4	2	1	1	0	0	0	-1	-1	-1	-1
χ_4'	4	4	-2	1	1	0	0	0	1	1	-1	-1
χ_5	5	5	1	-1	-1	-1	-1	1	1	1	0	0
χ_5'	5	5	-1	-1	-1	1	1	1	-1	-1	0	0
χ_6	6	6	0	0	0	0	0	-2	0	0	1	1
$\widetilde{\chi}_4$	4	-4	0	2	-2	0	0	0	0	0	1	-1
$\widetilde{\chi}_{4,1}'$	4	-4	0	-1	1	0	0	0	$\sqrt{3}$	$-\sqrt{3}$	1	-1
$\widetilde{\chi}_{4,2}'$	4	-4	0	-1	1	0	0	0	$-\sqrt{3}$	$\sqrt{3}$	1	-1
$\widetilde{\chi}_{6,1}'$	6	-6	0	0	0	$\sqrt{2}$	$-\sqrt{2}$	0	0	0	-1	1
$\widetilde{\chi}_{6,2}'$	6	-6	0	0	0	$-\sqrt{2}$	$\sqrt{2}$	0	0	0	-1	1

Bibliography

[1] S. Achimescu and A. Saha. Hilbert modular forms of weight 1/2 and theta functions. *Journal of Number Theory*, 128(12):3037–3062, 2008.

[2] A.O.L Atkin and J. Lehner. Hecke operators on $\Gamma_0(m)$. *Mathematische Annalen*, 185(2):134–160, 1970.

[3] J.P. Buhler. *Icosahedral galois representations.* Springer, 1978.

[4] D. Bump. *Automorphic forms and representations.* Cambridge University Press, 1998.

[5] J.W. Cogdell, H.H. Kim, and M.R. Murty. *Lectures on automorphic L-functions.* AMS, 2004.

[6] P. Deligne and J.P. Serre. Formes modulaires de poids 1. *Ann. Sci. Ecole Norm. Sup.*, 7(4):507–530, 1974.

[7] W. Duke. Fourth moments of L-functions attached to newforms. *Communications on Pure and Applied Mathematics*, 41(6):815–831, 1988.

[8] M. Eichler. The basis problem for modular forms and the traces of the Hecke operators. *Lecture Notes in Math*, 320:75–151, 1973.

[9] W. Fulton and J. Harris. *Representation theory: A first course.* Springer, 2004.

[10] H. Iwaniec and P. Sarnak. Perspectives on the analytic theory of L-functions. *Geometric and Functional Analysis*, 10:705–741, 2000.

[11] H.H. Kim. An application of exterior square functoriality of GL_4; Asai lift. *CRM Proceedings and Lecture Notes*, 36:197–202, 2004.

[12] H.H. Kim. On Symmetric Powers of Cusp Forms on GL_2. In *The Conference on L-Functions: Fukuoka, Japan, 18-23 February 2006*, pages 95–114. World Scientific Pub Co Inc, 2007.

[13] H.H. Kim and Y. Zhang. Divisor function for quaternion algebras and application to fourth moments of L-functions. *Journal of Number Theory*, 129(2):3000–3019, 2009.

[14] M. Krishnamurthy. The Asai transfer to GL_4 via the Langlands-Shahidi method. *International Mathematics Research Notices*, 2003(41):2221–2254, 2003.

[15] S. Lang. *Introduction to modular forms.* Springer, 2001.

[16] R.P. Langlands. *Base change for GL(2).* Princeton University Press, 1980.

[17] H. Maass. Automorphe Funktionen von mehreren Veränderlichen und Dirichletsche Reihen. *Abh. Math. Sem. Univ. Hamburg*, 16:72–100, 1949.

[18] T. Miyake. *Modular forms.* Springer Verlag, 2006.

[19] C.J. Moreno. Explicit formulas in the theory of automorphic forms. In *Number theory day: proceedings of the conference held at Rockefeller University, New York, 1976*, pages 73–216. Springer, 1977.

[20] C.J. Moreno. The value of $L(\frac{1}{2}, \chi)$ for Abelian L-functions of complex quadratic fields. *Journal of Number Theory*, 18(3):269–288, 1984.

[21] A.O. Morris. The spin representation of the symmetric group. *Proceedings of the London Mathematical Society*, 3(1):55–76, 1962.

[22] A. Pizer. The representability of modular forms by theta series. *Journal of Math. Soc. Japan*, 28(4):689–698, 1976.

[23] A. Pizer. The action of the canonical involution on modular forms of weight 2 on $\Gamma_0(M)$. *Mathematische Annalen*, 226(2):99–116, 1977.

[24] A. Pizer. An algorithm for computing modular forms on $\Gamma_0(N)$. *Journal of algebra*, 64(2):340–390, 1980.

[25] A. Pizer. Theta series and modular forms of level p^2M. *Compositio Math*, 40(2):177–241, 1980.

[26] P. Ponomarev. Newforms of squarefree level and theta series. *Mathematische Annalen*, 345(1):185–193, 2009.

[27] H.S.A. Potter. The mean values of certain Dirichlet series, II. *Proceedings of the London Mathematical Society*, 47(1):1–19, 1942.

[28] D. Ramakrishnan. Modularity of solvable Artin representations of GO(4)-type. *Int. Math. Res. Not.*, 2002(1):1–54, 2002.

[29] I. Reiner. *Maximal orders*. Academic Press New York, 1975.

[30] J.P. Serre. *A course in arithmetic*. Springer Verlag, 1973.

[31] J.P. Serre. L'invariant de Witt de la forme $\mathrm{Tr}(x^2)$. *Commentarii Mathematici Helvetici*, 59(1):651–676, 1984.

[32] G. Shimura. *Introduction to the arithmetic theory of automorphic functions*. Princeton University Press, 1994.

[33] C.L. Siegel. *Lectures on advanced analytic number theory.* Tata Institute of Fundamental Research, 1965.

[34] J. Tunnell. Artins conjecture for representations of octahedral type. *Bull. AMS*, 5:173–175, 1981.

[35] N.I.A. Vilenkin. *Special functions and the theory of group representations.* Amer Mathematical Society, 1968.

[36] A. Weil. *Basic number theory.* Springer Berlin-Heidelberg-New York, 1973.