On The Modularity of Galois Representations

by

Uğur Doğan

A Thesis Submitted to the
Graduate School of Science and Engineering
in Partial Fulfillment of the Requirements for
the Degree of

Master of Science
in
Mathematics

Koç University

July 2013

Koç University

Graduate School of Science and Engineering

This is to certify that I have examined this copy of a master's thesis by

Uğur Doğan

and have found that it is complete and satisfactory in all respects,

and that any and all revisions required by the final

examining committee have been made.

Committee Members:

Asst. Prof. Kazım Büyükboduk (Advisor)..

Assoc. Prof. Emre Alkan...

Prof. K. İlhan İkeda...

Date: 03 July 2013

Abstract

This study aims to understand a result called the *Modularity Theorem*:

All rational elliptic curves arise from modular forms

Taniyama first suggested in the 1950's that a statement along these lines might be true and a precise conjecture was formulated by Shimura. A paper of Weil ([W67]) provides strong theoretical evidence for the conjecture. The theorem was proved for a large class of elliptic curves by Wiles ([W95]) with a key ingredient supplied by joint work with Taylor ([TW95]), completing the proof of Fermat's Last Theorem after 350 years. The Modularity Theorem was proved completely by Breuil, Conrad, Taylor and Diamond ([BCDT01]). This thesis is devoted to understand the work of these mathematicians and there is no new claim in this thesis.

In this study we will first introduce modular forms and study some properties of these mathematical objects, such as some basic properties of them, their behaivour as vector spaces and topological spaces. Then we introduce Hecke operators, these are the operators between the vector spaces of modular forms. Using Hecke operators we will construct a basis, consisting of newforms. Then we will introduce Jacobians of modular curves and define Abelian variety which comes from weight-2 eigenforms. In the last part, we introduce Galois representations and we will give a brief skecth of the work done by Wiles.

Özet

Bu çalışma *Modülarite Teoremi* adıyla bilinen bir sonucu anlamayı amaçlamaktadır:

Bütün rasyonel eliptik eğriler modüler formlardan gelir.

İlk kez Taniyama tarafından 1950'lerde bu ifadeye çok yakın bir olgunun doğru olabileceği ifade edildi. Sonradan bu teorem, sanı olarak Shimura tarafından ortaya atıldı. Weil'in bir makalesi ([W67]) bu sanının doğruluğu konusunda güçlü teorik ipuçları vermişti. Teorem Wiles tarafından büyük bir eliptik eğri sınıfı için Taylor ile ortak bir çalışma ile kanıtlandı ([W95], [TW95]) ve Fermat'ın son teoremi 350 yıl aradan sonra çözüldü. Modülarite teoremi Breuil, Conrad, Taylor ve Diamond tarafından tamamıyla kanıtlanmıştır ([BCDT01]). Bu tez bu matematikçilerin çalışmalarını anlamaya adanmıştır ve bu tezde yeni bir iddia yoktur.

Bu çalışmada öncelikle modüler formları tanıtacağız ve vektör uzayı, topolojik uzay olarak sağladığı birtakım temel özelliklerini inceleyeceğiz. Sonra modüler formların oluşturduğu vektör uzayları arasında olan Hecke operatörlerini tanıtacağız. Hecke operatörlerini kullanarak, yeniformlardan oluşan bir baz inşa edeceğiz. Sonra modüler eğrilerin Jacobian'larını ve 2-ağırlıklı yeniformlardan gelen abelyen varyeteleri tanımlayacağız. Son kısımda ise, Galois temsillerini tanıtacağız ve Wiles'in yapmış olduklarının kısa bir özetini vereceğiz.

Contents

Chapter 1

Introduction

1.1 Modular Forms

Definition 1.1. The modular group, $SL_2(\mathbb{Z})$ is the set of 2-by-2 matrices with integer entries and with determinant 1:

$$\mathrm{SL}_2(\mathbb{Z}) = \left\{ \begin{bmatrix} a & b \\ c & d \end{bmatrix} : a, b, c, d \in \mathbb{Z}, ad - bc = 1 \right\}$$

The group $\mathrm{SL}_2(\mathbb{Z})$ is generated by the two matrices $\begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix}$ and $\begin{bmatrix} 0 & -1 \\ 1 & 0 \end{bmatrix}$. Each element of the modular group can also be viewed as an automorphism of the Riemann sphere $\hat{\mathbb{C}} = \mathbb{C} \cup \{\infty\}$ given by the fractional linear transformation

$$\begin{bmatrix} a & b \\ c & d \end{bmatrix}(\tau) = \frac{a\tau + b}{c\tau + d} \quad \text{for } \tau \in \mathbb{C}$$

Note that, if $c = 0$ then ∞ maps to ∞, if $c \neq 0$ then $\frac{-d}{c}$ maps to ∞ and ∞ maps to $\frac{a}{c}$.

For $\gamma \in \mathrm{SL}_2(\mathbb{Z})$, the matrices γ and $-\gamma$ give the same transformation.

Since $\mathrm{SL}_2(\mathbb{Z})$ is generated by $\begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix}$ and $\begin{bmatrix} 0 & -1 \\ 1 & 0 \end{bmatrix}$ we have the group of these transformations is generated by the maps

$$\tau \mapsto \tau + 1 \text{ and } \tau \mapsto -1/\tau$$

.

Let $\mathbb{H}$ denote the upper half plane; $\mathbb{H} = \{\tau \in \mathbb{C} : \mathrm{Im}(\tau) > 0\}$. It is easy to verify the equality:

$$\mathrm{Im}(\gamma(\tau)) = \frac{\mathrm{Im}(\tau)}{|c\tau + d|^2} \quad \text{for } \gamma \in \mathrm{SL}_2(\mathbb{Z})$$

so that $\mathbb{H}$ is closed under the action of the modular group.

Definition 1.2. Let k be an integer. A meromorphic function $f : \mathbb{H} \to \mathbb{C}$ is called *weakly modular of weight k* if

$$f(\gamma(\tau)) = (c\tau + d)^k f(\tau) \quad \text{for } \gamma \in \mathrm{SL}_2(\mathbb{Z}) \text{ and } \tau \in \mathbb{H}$$

Lemma 1.3. *Let f be a meromorphic function. f is weakly modular of weight k if $f(\tau + 1) = f(\tau)$ and $f(-1/\tau) = \tau^k f(\tau)$ for $\tau = \begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix}$ and $\tau = \begin{bmatrix} 0 & -1 \\ 1 & 0 \end{bmatrix}$.*

Proof. □

Note that, letting $\gamma = -I$ in the definition 1.2 we see that $f = (-1)^k f$, this implies that the only weakly modular function of odd weight is the zero function. Note also that, $f(\tau)$ and $f(\gamma(\tau))$ have the same zeros and poles since the factor $(c\tau + d)$ doesnot have any zero or pole.

Let $f : \mathbb{H} \to \mathbb{C}$ be a function. f is said to be holomorphic at ∞ if $f(\tau)$ is bounded as $\mathrm{Im}(\tau) \to \infty$.

Definition 1.4. Let k be an integer. A function $f : \mathbb{H} \to \mathbb{C}$ is called a *modular form of weight k* if,

1. f is holomorphic on $\mathbb{H}$,
2. f is weakly modular of weight k,
3. f is holomorphic at ∞.

The set of modular forms of weight k is denoted by $\mathcal{M}_k(\mathrm{SL}_2(\mathbb{Z}))$

$\mathcal{M}_k(\mathrm{SL}_2(\mathbb{Z}))$ forms a vector space over $\mathbb{C}$. If f is a modular form of weight k and g is a modular form of weight l then the product fg is a modular form of weight $k + l$. Hence the direct sum $\bigoplus_{k \in \mathbb{Z}} \mathcal{M}_k(\mathrm{SL}_2(\mathbb{Z}))$ forms a graded ring, and it is denoted by $\mathcal{M}(\mathrm{SL}_2(\mathbb{Z}))$.

Examples:

1. The zero function is a modular form of every weight and a constant function is a modular of weight zero. These are trivial examples of modular forms.

2. We also have a concrete nontrivial example of modular forms which are called *Eisenstein series*. Let $k > 2$ be an even integer, for $\tau \in \mathbb{H}$ define the Eisenstein series of weight k,

$$G_k(\tau) = \sum_{(c,d)}{}' \frac{1}{(c\tau + d)^k}$$

where he sum is taken over all $(c, d) \in \mathbb{Z}^2 \setminus (0, 0)$, this is what the primed sum means. This sum is absolutely convergent and converges uniformly on compact subsets of $\mathbb{H}$. For any $\gamma \in \mathrm{SL}_2(\mathbb{Z})$, if we compute;

$$\begin{aligned} G_k(\gamma(\tau)) &= \sum{}'_{(c',d')} \frac{1}{(c'(\frac{a\tau+b}{c\tau+d}) + d')^k} \\ &= (c\tau + d)^k \sum{}'_{(c',d')} \frac{1}{((c'a + d'c)\tau + (c'b + dd'))^k} \end{aligned}$$

(Here)As (c', d') runs through $\mathbb{Z}^2 \backslash \{(0, 0)\}$ do does $((c'a + d'c)\tau + (c'b + dd'))$. So the right side of the equality is $(c\tau + d)G_k(\tau)$, hence G_k is weakly modular of weight k. Finally, it is easy to see that G_k is bounded as $\mathrm{Im}(\tau) \to \infty$. So G_k is a modular form.

Definition 1.5. A **cusp form** of weight k is a modular form of weight k whose Fourier expansion has leading coefficient $a_0 = 0$, i.e. $f(\tau) = \sum_{i=1}^{\infty} a_n(e^{2\pi i\tau})^n$. The set of cusp forms is denoted by $\mathcal{S}_k(\mathrm{SL}_2(\mathbb{Z}))$. A modular form is a cusp form when $\lim_{\mathrm{Im}(\tau)\to\infty} f(\tau) = 0$

Remark 1.6. The cusp forms $\mathcal{S}_k(\mathrm{SL}_2(\mathbb{Z}))$ form a vector subspace of the modular forms $\mathcal{M}_k(\mathrm{SL}_2(\mathbb{Z}))$ and the graded ring $\mathcal{S}_k(\mathrm{SL}_2(\mathbb{Z})) = \sum_{k\in\mathbb{Z}} \mathcal{S}_k(\mathrm{SL}_2(\mathbb{Z}))$ is an ideal in $\mathcal{M}_k(\mathrm{SL}_2(\mathbb{Z}))$

1.2 Congruence Subgroups

In the definition 1.2, it is stated that f is weakly modular if $f(\gamma(\tau)) = (c\tau + d)^k f(\tau)$ for all $\gamma \in \mathrm{SL}_2(\mathbb{Z})$. If we replace $\mathrm{SL}_2(\mathbb{Z})$ by a subgroup Γ, it would generalize the notion of weak modularity and allow more examples of weakly modular functions.

Let N be a positive integer. The *principal congruence subgroup of level N* is;

$$\Gamma(N) = \left\{ \begin{bmatrix} a & b \\ c & d \end{bmatrix} \in \mathrm{SL}_2(\mathbb{Z}) : \begin{bmatrix} a & b \\ c & d \end{bmatrix} \equiv \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} (mod\, N) \right\}$$

Here, the matrix congruence is entrywise, i.e. $a \equiv 1, b \equiv 0, c \equiv 1$ and $d \equiv 0$ in modulo N. In particular $\Gamma(1) = \mathrm{SL}_2(\mathbb{Z})$.

Consider the natural surjective homomorphism $\varphi : \mathrm{SL}_2(\mathbb{Z}) \to \mathrm{SL}_2(\mathbb{Z}/N\mathbb{Z})$. $\Gamma(N)$ is exactly the kernel of this natural homomorphism, which means $\Gamma(N)$ is a normal subgroup of $\mathrm{SL}_2(\mathbb{Z})$ and it induces an isomorphism

$$\mathrm{SL}_2(\mathbb{Z})/\Gamma(N) \xrightarrow{\sim} \mathrm{SL}_2(\mathbb{Z}/N\mathbb{Z})$$

So, this implies that for every positive integer N, the subgroup $\Gamma(N)$ is a normal subgroup of finite index in $\mathrm{SL}_2(\mathbb{Z})$

Definition 1.7. A subgroup Γ of $\mathrm{SL}_2(\mathbb{Z})$ is a **congruence subgroup** is $\Gamma(N) \subset \Gamma$ for some positive $N \in \mathbb{Z}$, in which case Γ is a congruence subgroup of level N.

By the remarks above every congruence subgroup of $\mathrm{SL}_2(\mathbb{Z})$ has finite index. Besides, the principal congruence subgroups, the most important subgroups are;

$$\Gamma_0(N) = \left\{ \begin{bmatrix} a & b \\ c & d \end{bmatrix} \in \mathrm{SL}_2(\mathbb{Z}) : \begin{bmatrix} a & b \\ c & d \end{bmatrix} \equiv \begin{bmatrix} * & * \\ 0 & * \end{bmatrix} (mod\, N) \right\}$$

and

$$\Gamma_1(N) = \left\{ \begin{bmatrix} a & b \\ c & d \end{bmatrix} \in \mathrm{SL}_2(\mathbb{Z}) : \begin{bmatrix} a & b \\ c & d \end{bmatrix} \equiv \begin{bmatrix} 1 & * \\ 0 & 1 \end{bmatrix} (mod\, N) \right\}$$

These subgroups satisfy the relations;

$$\Gamma(N) \subset \Gamma_1(N) \subset \Gamma_0(N) \subset \mathrm{SL}_2(\mathbb{Z})$$

Consider the map $\Gamma_1(N) \to \mathbb{Z}/N\mathbb{Z}$ defined by $\begin{bmatrix} a & b \\ c & d \end{bmatrix} \mapsto b \bmod(N)$, which is a surjection with kernel $\Gamma(N)$. It shows that $\Gamma(N) \trianglelefteq \Gamma_1(N)$ and

$$\Gamma_1(N)/\Gamma(N) \xrightarrow{\sim} \mathbb{Z}/N\mathbb{Z} \quad \text{with} \quad [\Gamma_1(N) : \Gamma(N)] = N$$

Similarly the map, $\Gamma_0(N) \to (\mathbb{Z}/N\mathbb{Z})^*$ defined by $\begin{bmatrix} a & b \\ c & d \end{bmatrix} \to d \bmod(N)$ is a surjection with kernel $\Gamma_1(N)$, so that $\Gamma_1(N) \trianglelefteq \Gamma_0(N)$ and,

$$\Gamma_1(N)/\Gamma_0(N) \xrightarrow{\sim} (\mathbb{Z}/N\mathbb{Z})^* \quad \text{with} \quad [\Gamma_1(N) : \Gamma(N)] = \phi(N)$$

where ϕ is the Euler totient function.

Now, before continuing further we will introduce a notatin. For any matrix $\gamma = \begin{bmatrix} a & b \\ c & d \end{bmatrix} \in \mathrm{SL}_2(\mathbb{Z})$ define the factor of automorphy $j(\gamma, \tau) \in \mathbb{C}$ for any $\tau \in \mathbb{H}$ to be

$$j(\gamma, \tau) = c\tau + d$$

for any $\gamma \in \mathrm{SL}_2(\mathbb{Z})$ and for any integer k define the *weight-k operator* $[\gamma]_k$ on functions $f\mathbb{H} \to \mathbb{C}$ by

$$(f[\gamma]_k)(\tau) = j(\gamma, \tau)^{-k} f(\gamma(\tau)) \qquad \text{for any } \tau \in \mathbb{H}$$

Now, we can say that a meromorphic function f on $\mathbb{H}$ is *weakly modular of weight k* if

$$f[\gamma]_k = f \qquad \text{for all } \gamma \in \Gamma$$

The next lemma can be proven by easy calculations. It gives the basic properties of the factor of automorphy and weight-k operator:

Lemma 1.8. *For all $\gamma, \gamma' \in SL_2(\mathbb{Z})$ and $\tau \in \mathbb{H}$,*

(a) $j(\gamma\gamma', \tau) = j(\gamma, \gamma'(\tau))j(\gamma', \tau)$

(b) $(\gamma\gamma')(\tau) = \gamma(\gamma'(\tau))$

(c) $[\gamma\gamma']_k = [\gamma]_k[\gamma']_k$

(d) $Im(\gamma(\tau)) = \frac{Im(\tau)}{|j(\gamma,\tau)|^2}$

(e) $\frac{d\gamma(\tau)}{d\tau} = \frac{1}{j(\gamma,\tau)^2}$

A Γ-equivalence class of points in $\mathbb{Q} \cup \{\infty\}$ is called a *cusp* of Γ. If $\Gamma = \mathrm{SL}_2(\mathbb{Z})$, all rational numbers are Γ-equivalent to ∞ and so $\mathrm{SL}_2(\mathbb{Z})$ has only one cusp, represented by ∞. A modular form with respect to a congruence subgroup Γ should be holomorphic at the cusps. Writing any $s \in \mathbb{Q} \cup \{\infty\}$ as $s = \alpha(\infty)$, holomorphy at s is naturally defined in terms of holomorphy at ∞ via the $[\alpha]_k$ operator. f is holomorphic at s if $f[\alpha]_k$ is holomorphic at ∞. This makes sense since $f[\alpha]_k$ is holomorphic on $\mathbb{H}$ and weakly modular with respect to $\alpha^{-1}\Gamma\alpha$ which is again a congruence subgroup of $\mathrm{SL}_2(\mathbb{Z})$.

Definition 1.9. Let Γ be a congruence subgroup of $\mathrm{SL}_2(\mathbb{Z})$, and let k be a positive integer. A function $f : \mathbb{H} \to \mathbb{C}$ is a **modular form of weight k with respect to** Γ if

(1) f is holomorphic

(2) f is weight-k invariant under Γ

(3) $f[\alpha]_k$ is holomorphic at ∞ for all $\alpha \in \mathrm{SL}_2(\mathbb{Z})$

If in addition,

(4) $a_0 = 0$ in the Fourier expansion of $f[\alpha]_k$ for all $\alpha \in \mathrm{SL}_2(\mathbb{Z})$

then f is a **cusp form** of weight-k with respect to Γ. The modular forms of weight k with respect to Γ are denoted by $\mathcal{M}_k(\Gamma)$, the cusp forms $\mathcal{S}_k(\Gamma)$.

1.3 Complex Tori

This section gives a sketch of results about complex tori, also known as complex elliptic curves. This material is covered in details in many books, such as [JS87].

A lattice in $\mathbb{C}$ is a set $\Lambda = \omega_1\mathbb{Z} \oplus \omega_2\mathbb{Z}$ with $\{\omega_1, \omega_2\}$ a basis of $\mathbb{C}$ over $\mathbb{R}$. We make the normalizing condition $\omega_1/\omega_2 \in \mathbb{H}$. We have the following relation between lattices.

Lemma 1.10. *Let $\Lambda = \omega_1\mathbb{Z} \oplus \omega_2\mathbb{Z}$ and $\Lambda' = \omega_1'\mathbb{Z} \oplus \omega_2'\mathbb{Z}$ be two lattices with $\omega_1/\omega_2 \in \mathbb{H}$ and $\omega_1'/\omega_2' \in \mathbb{H}$. Then $\Lambda = \Lambda'$ if and only if*

$$\begin{bmatrix} \omega_1' \\ \omega_2' \end{bmatrix} = \begin{bmatrix} a & b \\ c & d \end{bmatrix} \begin{bmatrix} \omega_1 \\ \omega_2 \end{bmatrix} \quad \textit{for some} \begin{bmatrix} a & b \\ c & d \end{bmatrix} \in SL_2(\mathbb{Z})$$

Proof. See [DS05] - Lemma 1.3.1 □

A complex torus is the quotient of the complex plane by a lattice,

$$\mathbb{C}/\Lambda = \{z + \Lambda : z \in \mathbb{C}\}$$

Algebraically a complex torus is an Abelian group (under the complex addition). Geometrically a complex torus is a parallelogram spanned by ω_1 and ω_2 (in the definition of a lattice) with its sides identified in opposite pairs.

Proposition 1.11. *Suppose $\varphi : \mathbb{C}/\Lambda \to \mathbb{C}/\Lambda'$ is a holomorphic map between complex tori. Then there exist complex numbers m, b with $m\Lambda \subset \Lambda'$ such that $\varphi(z + \Lambda) = mz + b + \Lambda'$. The map is invertible if and only if $m\Lambda = \Lambda'$.*

Proof. We will use algebraic topology methods to prove this proposition. Since $\mathbb{C}$ is the universal covering space of $\mathbb{C}/\Lambda$, φ lifts to a holomorphic map $\tilde{\varphi} : \mathbb{C} \to \mathbb{C}$. (See [H01] for detailed information). So we have the following commutative diagram:

$$\begin{tikzcd}
\mathbb{C} \arrow[r, "\tilde{\varphi}"] \arrow[d, "p"] & \mathbb{C} \arrow[d, "p'"] \\
\mathbb{C}/\Lambda \arrow[r, "\varphi"] & \mathbb{C}/\Lambda'
\end{tikzcd}$$

Let $\lambda \in \Lambda$ and consider the function $f_\lambda(z) = \tilde{\varphi}(z + \lambda) - \tilde{\varphi}(z)$. By the commutativity of the diagram above we have $p'(\tilde{\varphi}(z + \lambda)) = \varphi(p(z + \lambda)) = \varphi(p(z)) = p'(\tilde{\varphi}(z))$ and thus $\tilde{\varphi}(z + \lambda) - \tilde{\varphi}(z) \in \Lambda'$. Hence f_λ maps $\mathbb{C}$ to Λ' and since f_λ is continuos, it must be constant. Therefore differentiating both sides would give us; $\tilde{\varphi}'(z + \lambda) = \tilde{\varphi}'(z)$ so that $\tilde{\varphi}'$ is a holomorphic, Λ-periodic function. This makes $\tilde{\varphi}'$ bounded and by Liouville's Theorem (from complex analysis) it must be constant. Hence $\tilde{\varphi}(z) = mb + z$. Since $\tilde{\varphi}$ lifts a map between the quotients, we have $m\Lambda \subset \Lambda$ and φ has the form given in the proposition. □

Corollary 1.12. *$\varphi : \mathbb{C}/\Lambda \to \mathbb{C}/\Lambda'$ is a holomorphic map between complex tori, $\varphi(z + \Lambda) = mz + b + \Lambda'$ with $m\Lambda \subset \Lambda'$. Then the following are equivalent:*

(i) *φ is a group homomorphism.*

(ii) *$b \in \Lambda'$, so $\varphi(z + \Lambda) = mz + \Lambda'$*

(iii) *$\varphi(0) = 0$*

In particular, there exists a nonzero holomorphic group homomorphism between complex tori $\mathbb{C}/\Lambda$ and $\mathbb{C}/\Lambda'$ if and only if there exists a nonzero $m \in \mathbb{C}$ such that $m\Lambda \subset \Lambda'$, and there exists a holomorphic group isomorphism between complex tori $\mathbb{C}/\Lambda$ and $\mathbb{C}/\Lambda'$ if and only if there exists some $m \in \mathbb{C}$ such that $m\Lambda = \Lambda'$.

Now, given any example of an isomorphism between complex tori. Let $\Lambda = \omega_1\mathbb{Z} \oplus \omega_2$ be a lattice and $\tau = \omega_1/\omega_2$. Let $\Lambda_\tau = \tau\mathbb{Z} \oplus \mathbb{Z}$. Since $(1\omega_2)\Lambda = \Lambda_\tau$, by the above corollary the map $\varphi_\tau := \mathbb{C}/\Lambda \to \mathbb{C}/\Lambda_\tau$ given by $\varphi(z + \Lambda) = z/\omega_2\Lambda_\tau$ is an isomorphism. Thus every complex torus is isomorphic to a complex torus whose lattice is generated by a complex number τ and 1. τ is not unique but if $\tau' \in \mathbb{H}$ is another such number, i.e. $\Lambda = \omega_1'\mathbb{Z} \oplus \omega_2'\mathbb{Z}$ and $\tau' = \omega_1'/\omega_2'$ then by Lemma 1.10 on page 12, $\tau' = \gamma(\tau)$ for some $\gamma \in \mathrm{SL}_2(\mathbb{Z})$. Thus each complex torus determines a complex number $\tau \in \mathbb{H}$ up to action of $\mathrm{SL}_2(\mathbb{Z})$.

Definition 1.13. A nonzero holomorphic homomorphism between complex tori is called an isogeny.

Examples:

(i) Every holomorphic isomorphism is an isogeny.

(ii) Multiply with integer maps. Let N be a positive integer and Λ be a lattice. Consider the map $[N] : \mathbb{C}/\Lambda \to \mathbb{C}/\Lambda$ given by $z + \Lambda \mapsto Nz + \Lambda$. As $N\Lambda \subset \Lambda$ this is an isogeny. Its kernel is the set of N-torsion points of $\mathbb{C}/\Lambda$ isomorphic to $\mathbb{Z}/N\mathbb{Z} \times \mathbb{Z}/N\mathbb{Z}$. This kernel is denoted by $E[N]$

(iii) Cyclic quotient maps: Let N be a positive integer and C be a cyclic subgroup of $E[N]$ isomorphic to $\mathbb{Z}/N\mathbb{Z}$. As a set, C is a superlattice of Λ. The cyclic quotient map $\pi : \mathbb{C}/\Lambda \to \mathbb{C}/C$ is an isogeny with kernel C.

Chapter 2

Hecke Operators

In this chapter, we will introduce Hecke operators and we will find a basis for the space $\mathcal{S}_k(\Gamma_1(N))$.

2.1 The Double Coset Operator

Let Γ_1 and Γ_2 be two congruence subgroups of $\mathrm{SL}_2(\mathbb{Z})$. So, Γ_1 and Γ_2 are subgroups of $\mathrm{GL}_2^+(\mathbb{Q})$ (this is the group of 2×2 matrices with rational entries and positive determinant). For each $\alpha \in \mathrm{GL}_2^+(\mathbb{Q})$ the set,

$$\Gamma_1\alpha\Gamma_2 = \{\gamma_1\alpha\gamma_2 : \gamma_1 \in \Gamma_1, \gamma_2 \in \Gamma_2\}$$

is a double coset in $\mathrm{GL}_2^+(\mathbb{Q})$. Such a double coset transforms modular forms with respect to Γ_1 into modular forms with respect to Γ_2.

The group Γ_1 acts on the double coset $\Gamma_1\alpha\Gamma_2$ via left multiplication and partitions it into orbits. An orbit is $G_1\beta$ where β is a representative $\beta = \gamma_1\alpha\gamma_2$ and the orbit space $\Gamma_1 \setminus \Gamma_1\alpha\Gamma_2$ becomes a disjoint union $\bigcup \Gamma_1\beta_j$ for some choice of representatives β_j's. The next two lemmas show that this union is in fact a finite union.

Lemma 2.1. *Let Γ be a congruence subgroup of $SL_2(\mathbb{Z})$ and α be an element of $GL_2^+(\mathbb{Q})$. Then $\alpha^{-1}\Gamma\alpha \cap SL_2(\mathbb{Z})$ is again a congruence subgroup of $SL_2(\mathbb{Z})$.*

Proof. There exists $\tilde{N} \in \mathbb{Z}^+$ satisfying the conditions $\Gamma(\tilde{N}) \subset \Gamma$, $\tilde{N}\alpha \in \mathrm{M}_2(\mathbb{Z})$ and

$\tilde{N}\alpha^{-1} \in \mathrm{M}_2(\mathbb{Z})$. Set $N = \tilde{N}^3$. Consider;

$$\begin{aligned}\alpha\Gamma(N)\alpha^{-1} &\subset \alpha(I + \tilde{N}^3\mathrm{M}_2(\mathbb{Z}))\alpha^{-1} \\ &= I + \tilde{N}.\tilde{N}\alpha\mathrm{M}_2(\mathbb{Z}).\tilde{N}\alpha^{-1} \\ &\subset I + \tilde{N}\mathrm{M}_2(\mathbb{Z})\end{aligned}$$

and the observation that $\alpha\Gamma(N)\alpha^{-1}$ consist only the matrices with determinant 1 combine to show that $\alpha\Gamma(N)\alpha^{-1} \subset \Gamma(\tilde{N})$. Hence, $\Gamma(N) \subset \alpha^{-1}\Gamma(\tilde{N})\alpha \subset \alpha^{-1}\Gamma\alpha$, intersecting with $\mathrm{SL}_2(\mathbb{Z})$ completes the proof. □

Lemma 2.2. *Let Γ_1 and Γ_2 be two congruence subgroups of $SL_2(\mathbb{Z})$. Let α be an element of $GL_2^+(\mathbb{Q})$. Set $\Gamma_3 = \alpha^{-1}\Gamma_1\alpha \cap \Gamma_2$. Then left multiplication by α: $\Gamma_2 \to \Gamma_1\alpha\Gamma_2$ given by $\gamma_2 \to \alpha\gamma_2$, induces a natural bijection from the coset space $\Gamma_3 \setminus \Gamma_2$ to the orbit space $\Gamma_2 \setminus \Gamma_1\alpha\Gamma_2$.*

Proof. The map $\Gamma_2 \to \Gamma_1 \setminus \Gamma_1\alpha\Gamma_2$ taking γ_2 to $\Gamma_1\alpha\gamma_2$ clearly surjects. It takes the elements γ_2, γ_2' to the same orbit when $\Gamma_1\alpha\gamma_2 = \Gamma_1\alpha\gamma_2'$, i.e. $\gamma_2\gamma_2^{-1} \in \alpha^{-1}\Gamma_1\alpha$, and of course $\gamma_2'\gamma_2^{-1} \in \Gamma_2$ as well. So the definition $\Gamma_3 = \alpha^{-1}\Gamma_1\alpha \cap \Gamma_2$ gives a bijection $\Gamma_2 \setminus \Gamma_2 \to \Gamma_1 \setminus \Gamma_1\alpha\Gamma_2$ from cosets $\Gamma_3\gamma_2$ to orbits $\Gamma_1\alpha\gamma_2$. And the last statement follows easily. □

Remark 2.3. Let Γ_1 and Γ_2 be two congruence subgroups of $\mathrm{SL}_2(\mathbb{Z})$. Then $[\Gamma_1 \cap \Gamma_2]$ is finite. In particular, since $\alpha^{-1}\Gamma_1\alpha \cap \mathrm{SL}_2(\mathbb{Z})$ is a congruence subgroup by Lemma 2.1 and the coset space $\Gamma_3 \setminus \Gamma_2$ is Lemma 2.2 is finite and hence so is the orbit space $\Gamma_1 \setminus \Gamma_1\alpha\Gamma_2$.

Now, we will define the double coset operator.

Definition 2.4. For $\beta \in \mathrm{GL}_2^+(\mathbb{Q})$ and $k \in \mathbb{Z}$, **weight-k β operator** on functions $f : \mathbb{H} \to \mathbb{C}$ is defined by, for $\tau \in \mathbb{H}$;

$$f([\beta]_k)(\tau) = (det\beta)^{k-1} j(\beta, \tau)^k f(\beta(\tau))$$

Definition 2.5. For congruence subgroups Γ_1 and Γ_2 of $\mathrm{SL}_2(\mathbb{Z})$ and $\alpha \in \mathrm{GL}_2^+(\mathbb{Q})$, the **weight-$k$ $\Gamma_1\alpha\Gamma_2$-operator** (or **the double coset operator**) is defined from $\mathcal{M}_k(\Gamma_1)$ (into $\mathcal{M}_k(\Gamma_2)$) given by; for $f \in \mathcal{M}_k(\Gamma_1)$,

$$f[\Gamma_1\alpha\Gamma_2]_k = \sum_j f[\beta_j]_k$$

Remark 2.6. The double coset operator is independent from the choice of orbit representatives β_j's, i.e. it is well-defined.

Remark 2.7. The double coset operator takes modular forms with respect to Γ_1 to the modular forms with respect to Γ_2 and it takes cusp forms with respect to G_1 to the cusp forms with respect to Γ_2.

Remark 2.8. These are some special cases of double coset operators:

- If $\Gamma_2 \subseteq \Gamma_2$ then taking $\alpha = I$ (the identity matrix) makes the double coset operator $f[\Gamma_1\alpha\Gamma_2]_k = f$. It is the natural inclusion from from the subspace $\mathcal{M}_k(\Gamma_1)$ into $\mathcal{M}_k(\Gamma_2)$.

- If $\alpha^{-1}\Gamma_1\alpha = \Gamma_2$ then $f[\Gamma_1\alpha\Gamma_2]_k = f[\alpha]_k$. It is a natural isomorphism from $\mathcal{M}_k(\Gamma_1)$ to $\mathcal{M}_k(\Gamma_2)$.

- If $\Gamma_1 \subseteq \Gamma_2$, take $\alpha = I$ (the identity matrix). If $\{\gamma_{2,j}\}$ are the coset representatives of the action $\Gamma_1 \setminus \Gamma_2$ then $f[\Gamma_1\alpha\Gamma_2]_k = \sum_j f[\gamma_{2,j}]_k$. In this case, $f[\Gamma_1\alpha\Gamma_2]_k$ is the projection of $\mathcal{M}_k(\Gamma_1)$ onto its subspace $\mathcal{M}_k(\Gamma_2)$.

2.2 The $< d >$ and T_p Operators

Recall the congruence subgroups:

$$\Gamma_0(N) = \left\{ \begin{bmatrix} a & b \\ c & d \end{bmatrix} \in \mathrm{SL}_2(\mathbb{Z}) : \begin{bmatrix} a & b \\ c & d \end{bmatrix} \equiv \begin{bmatrix} * & * \\ 0 & * \end{bmatrix} (mod\, N) \right\}$$

and

$$\Gamma_1(N) = \left\{ \begin{bmatrix} a & b \\ c & d \end{bmatrix} \in \mathrm{SL}_2(\mathbb{Z}) : \begin{bmatrix} a & b \\ c & d \end{bmatrix} \equiv \begin{bmatrix} 1 & * \\ 0 & 1 \end{bmatrix} (mod\, N) \right\}$$

Note thet since $\Gamma_1(N) \subset \Gamma_0(N)$ we habe $\mathcal{M}_k(\Gamma_0(N)) \subset \mathcal{M}_k(\Gamma_1(N))$. We will introduce two operators on the space $\mathcal{M}_k(\Gamma_1(N))$.

To define the first type of Hecke operator, take any $\alpha \in \Gamma_0$ and take $\Gamma_1 = \Gamma_2 = \Gamma_1(N)$. Consider the weight-$k$ double coset operator $[\Gamma_1\alpha\Gamma_1]_k$. Since $\Gamma_1 \trianglelefteq \Gamma_0$, by Remark 2.8 on page 17 this operator translates each function $f \in \mathcal{M}_k(\Gamma_1(N))$ to (for every $\alpha \in \Gamma_0(N)$);

$$f[\Gamma_1(N)\alpha\Gamma_1(N)]_k = f[\alpha]_k$$

So $f[\alpha]_k \in \mathcal{M}_k(\Gamma_1(N))$ and it means $\Gamma_0(N)$ acts on $\mathcal{M}_k(\Gamma_1(N))$. Hence we have an operator

$$\langle d\rangle : \mathcal{M}_k(\Gamma_1(N)) \to \mathcal{M}(\Gamma_1(N))$$

given by $\langle d\rangle f = f[\alpha]_k$ for any $\alpha = \begin{bmatrix} a & b \\ c & \delta \end{bmatrix}$ where $\delta \equiv d \pmod N$. This first type Hecke operator is called the *diamond* operator.

The second kind of Hecke operaor is also a weight-k double coset operator $[\Gamma_1\alpha\Gamma_2]_k$ where again $\Gamma_1 = \Gamma_2 = \Gamma_1(N)$, but now $\alpha = \begin{bmatrix} 1 & 0 \\ 0 & p \end{bmatrix}$ with p is a prime integer. This operator is denoted by T_p. So, we have

$$T_p : \mathcal{M}_k(\Gamma_1(N)) \to \mathcal{M}_k(\Gamma_1(N))$$

given by

$$T_p f = f[\Gamma_1(N)\begin{bmatrix} 1 & 0 \\ 0 & p \end{bmatrix}\Gamma_1(N)]_k$$

Lemma 2.9. *These two kind of Hecke operators commute.*

Proof. Note that by the definition of a double coset we have;

$$\Gamma_1(N)\begin{bmatrix} 1 & 0 \\ 0 & p \end{bmatrix}\Gamma_1(N) = \left\{\gamma \in M_2(\mathbb{Z}) : \gamma \equiv \begin{bmatrix} 1 & * \\ 0 & p \end{bmatrix}(modN), \quad \det\gamma = p\right\}$$

Let $\alpha = \begin{bmatrix} 1 & 0 \\ 0 & p \end{bmatrix}$ and $\gamma \in \Gamma_0(N)$. By an easy computation, we get $\gamma\alpha\gamma^{-1} \equiv \begin{bmatrix} 1 & * \\ 0 & p \end{bmatrix} \pmod N$

Suppose $\Gamma_1(N)\alpha\Gamma_1(N) = \bigcup_j \Gamma_1(N)\beta_j$ for some coset representatives β_j's. Then by the above description of $\Gamma_1(N)\begin{bmatrix} 1 & 0 \\ 0 & p \end{bmatrix}\Gamma_1(N)$, we have $\Gamma_1(N)\begin{bmatrix} 1 & 0 \\ 0 & p \end{bmatrix}\Gamma_1(N) = \Gamma_1(N)\gamma\alpha\gamma^{-1}\Gamma_1(N) = \gamma\Gamma_1(N)\alpha\Gamma_1(N)\gamma^{-1} = \bigcup_j \Gamma_1(N)\gamma\beta_j\gamma^{-1}$, so that

$$\bigcup_j \Gamma_1(N)\beta_j\gamma = \bigcup_j \Gamma_1(N)\gamma\beta_j$$

This equality is true for all $\gamma \in \Gamma_0(N)$. If we choose $\gamma = \begin{bmatrix} a & b \\ c & \delta \end{bmatrix} \in \Gamma_0(N)$ such that

$\delta \equiv d \pmod{N}$, we get;

$$(\langle d\rangle T_p)(f) = \sum_j f[\beta_j\gamma]_k = \sum_j f[\gamma\beta_j]_k = (T_p\langle d\rangle)(f)$$

□

Moreover, we have:

Theorem 2.10. *Let d and e be elements of $(\mathbb{Z}/N\mathbb{Z})^*$ and let p and q be prime. Then;*

(i) $\langle d\rangle\langle e\rangle = \langle e\rangle\langle d\rangle = \langle de\rangle$

(ii) $T_pT_q = T_qT_p$

Proof. See [DS05], Proposition 5.2.4. □

2.2.1 $\langle n\rangle$ and T_n Operator

Now, we will extend the definitions of $\langle d\rangle$ and T_p operators to $\langle n\rangle$ and T_n, for all $n \in \mathbb{Z}^+$.

For $n \in \mathbb{Z}^+$ with $(n, N) = 1$, $\langle n\rangle$ is determined by $n \pmod{N}$. For $n \in \mathbb{Z}^+$ with $(n, N) > 1$, we define $\langle n\rangle = 0$-the zero operator on $\mathcal{M}_k(\Gamma_1(N))$. So that the mapping $n \mapsto \langle n\rangle$ is completely multiplicative.

For defining the operator T_n, we will use an inductive definition. Set $T_1 = 1$-the identity operator on $\mathcal{M}_k(\Gamma_1(N))$. We have already defined T_p. For prime powers, define inductively

$$T_{p^r} = T_pT_{p^{r-1}} - p^{k-1}\langle p\rangle T_{p^{r-2}}$$

for all $r \geq 2$. Now, let $n \in \mathbb{Z}^+$ be any integer, write $n = \prod p_i^{e_i}$ and define;

$$T_n = \prod T_{p_i^{e_i}}$$

So that by Theorem 2.10 on page 19 for all $n, m \in \mathbb{Z}^+$ with the property that $(n, m) = 1$ we have $T_nT_m = T_mT_n$.

2.3 Petersson Inner Product

In this section to make the space of cusp forms $\mathcal{S}_k(\Gamma_1(N))$ an inner product space, we will define an inner product called the Petersson Inner Product. It will be defined as an integral which may not be convergent on the larger space $\mathcal{M}_k(\Gamma_1(N))$, so the inner product is restricted to the cusp forms.

The *hyperbolic measure* on the upper half plane is defined by $d\mu(\tau) = \frac{dxdy}{y^2}$ for all $\tau \in \mathbb{H}$. This is invariant under the action of the automorphism group $\mathrm{SL}_2(\mathbb{Z})$, which means $d\mu(\gamma(\tau)) = d\mu\tau$ for all $\gamma \in \mathrm{SL}_2(\mathbb{Z})$. Since $\mathbb{Q} \cup \{\infty\}$ is a countable set it has measure zero and so $d\mu$ suffices for integrating over the extended upper half plane $\mathbb{H}^* = \mathbb{H} \cup \mathbb{Q} \cup \{\infty\}$.

The *fundamental domain of* $\mathbb{H}^*$ under the action of $\mathrm{SL}_2(\mathbb{Z})$ is the set

$$\mathcal{D}^* = \{\tau \in \mathbb{H} : \mathrm{Re}(\tau) \leq 1/2, |\tau| \geq 1\} \cup \{\infty\}$$

. This means, for every point $\tau' \in \mathbb{H}$ there exists an element $\gamma \in \mathrm{SL}_2(\mathbb{Z})$ such that $\gamma(tau)$ maps into the connected domain $\mathcal{D}^*$. Putting some certain baoundary conditions on $\mathcal{D}^*$ the mapping is unique. Every point of $\mathbb{Q} \cup \{\infty\}$ maps to ∞ under the action of $\mathrm{SL}_2(\mathbb{Z})$. (See [M76], Chapter 1 for details)

Lemma 2.11. *For any continuos bounded function $\varphi : \mathbb{H} \to \mathbb{C}$ and any $\alpha \in SL_2(\mathbb{Z})$, the integral $\int_{\mathcal{D}^*} \varphi(\alpha(\tau))d\mu(\tau)$ converges.*

Proof. Say f is bounded by M. Then we have;

$$\begin{aligned}\left|\int_{\mathcal{D}^*} \varphi(\alpha(\tau))d\mu(\tau)\right| &\leq \int_{\mathcal{D}^*} |\varphi(\alpha(\tau))|\, d\mu(\tau)\\ &\leq M \int_{\mathcal{D}^*} \frac{dxdy}{y^2}\\ &\leq M \int_{-1/2}^{1/2} \int_{1/2}^{\infty} \frac{dy}{y^2} dx\\ &\leq \int_{1/2}^{\infty} \frac{dy}{y^2} < \infty\end{aligned}$$

□

Let $\Gamma \subset \mathrm{SL}_2(\mathbb{Z})$ be a congruence subgroup and let $\{\alpha_j\}$ be some representations of the coset space $\{\pm I\}\Gamma/\mathrm{SL}_2(\mathbb{Z})$, which means the disjoint union $\mathrm{SL}_2(\mathbb{Z}) = \bigcup_j \{\pm I\}\Gamma\alpha_j$. If the function φ is Γ-invariant then the sum $\sum_j \int_{\mathcal{D}^*} \varphi(\alpha_j(\tau))d\mu(\tau)$ is independent of the choice of the coset representatives α_j's. Since $d\mu$ is $\mathrm{SL}_2(\mathbb{Z})$-invariant the sum is $\int_{\cup\alpha_j(\mathcal{D}^*)} \varphi(\tau)d\mu(\tau)$. For some reasons we denote (up to some boundary identification) this union as $X(\Gamma)$ (*the modular curve of* Γ, see [DS05], Chapter 2 for details). So may make the definition

$$\int_{X(\Gamma)} \varphi(\tau) d\mu(\tau) = \int_{\bigcup \alpha_j(\mathcal{D}^*)} \varphi(\tau) d\mu(\tau) = \sum_j \int_{\mathcal{D}^*} \varphi(\alpha_j(\tau)) d\mu(\tau)$$

In particular, taking $\varphi = 1$, the volume of $X(\Gamma)$ is given by $V_\Gamma = \int_{X(\Gamma)} d\mu(\tau)$ and the volume and index of a congruence subgroup are related by

$$V_\Gamma = [\mathrm{SL}_2(\mathbb{Z}) : \{\pm I\}\Gamma] V_{\mathrm{SL}_2(\mathbb{Z})}$$

.

Now, to construct inner product; let $f, g \in \mathcal{S}_k(\Gamma)$ and consider (for $\tau \in \mathbb{H}$) the continuos function

$$\varphi(\tau) = f(\tau)\overline{g(\tau)}(\mathrm{Im}(\gamma(\tau)))^k$$

Moreover;

Lemma 2.12. *φ is Γ-invariant.*

Proof. Let $\gamma \in \Gamma$ be any. Then

$$\begin{aligned} \varphi(\gamma(\tau)) &= f(\gamma(\tau))\overline{g(\gamma(\tau))}(\mathrm{Im}(\gamma(\tau)))^k \\ &= (f[\gamma]_k)(\tau) j(\gamma,\tau)^k \overline{(g[\gamma]_k)(\tau) j(\gamma,\tau)}^k (\mathrm{Im}(\tau))^k |j(\gamma,\tau)|^{-2k} \\ &= (f[\gamma]_k)(\tau)\overline{(g[\gamma]_k)(\tau)}(\mathrm{Im}(\tau))^k \\ &= \varphi(\tau) (\text{since } f \text{ and } g \text{ are weight-}k \text{ invariant under } \Gamma) \end{aligned}$$

□

Definition 2.13. Let $\Gamma \subset \mathrm{SL}_2(\mathbb{Z})$ be a congruence subgroup. The **Petersson Inner Product**;

$$\langle , \rangle_\Gamma : \mathcal{S}_k(\Gamma) \times \mathcal{S}_k(\Gamma) \to \mathbb{C},$$

is given by

$$\langle f, g \rangle_\Gamma = \frac{1}{V_\Gamma} \int_{X(\Gamma)} f(\tau)\overline{g(\tau)}(\mathrm{Im}(\tau)^k) d\mu(\tau)$$

Remark 2.14. Petersson Inner Product is linear in the first coordinate, conjegate linear in the sesond coordinate, Hermitian-symmetric and positive definite. The normalizing factor $1/V_\Gamma$ ensures that if $\Gamma' \subset \Gamma$ then $\langle , \rangle_{\Gamma'} = \langle , \rangle_\Gamma$ on $\mathcal{S}_k(\Gamma)$

2.4 Adjoints of Hecke Operators

In this section we will find the adjoints of Hecke operators. Recall that if V is an inner product space and T is a linear operator on V, then the *adjoint* T^* is the linear operator on V defined by the condition that for all $v, w \in V$; $\langle Tv, w\rangle = \langle v, T^* w\rangle$. An operator T is called *normal* if T commutes with its adjoint T^*.

The next proposition will help us computing the adjoints of the Hecke operators.

Proposition 2.15. *Let $\Gamma \subset SL_2(\mathbb{Z})$ be a congruence subgroup. Let $\alpha \in GL_2^+(\mathbb{Q})$ be any element. Set $\alpha' = \det \alpha\alpha^{-1}$. Then;*

(i) If $\alpha^{-1}\Gamma\alpha \subset SL_2(\mathbb{Z})$ then for all $f \in \mathcal{S}_k(\Gamma)$ and $g \in \mathcal{S}_k(\alpha^{-1}\Gamma\alpha)$,

$$\langle f[\alpha]_k, g\rangle_{\alpha^{-1}\Gamma\alpha} = \langle f, g[\alpha']_k\Gamma$$

(ii) For all $f, g \in S_k(\Gamma)$,

$$\langle f[\Gamma\alpha\Gamma]_k, g\rangle = \langle f, g[\Gamma\alpha'\Gamma]_k$$

In particular, if $\alpha^{-1}\Gamma\alpha = \Gamma$ then $[\alpha]_k^* = [\alpha']_k$ and in any case $[\Gamma\alpha\Gamma]_k^* = [\Gamma\alpha'\Gamma]_k$.

Proof. See [DS05], Proposition 5.5.2. □

Theorem 2.16. *In the inner product space $\mathcal{S}_k\Gamma_1(N)$, the Hecke operator $\langle p\rangle$ and T_p for $p \nmid N$ have adjoints;*

$$\langle p\rangle^* = \langle p\rangle^{-1} \quad \textit{and} \quad {T_p}^* = \langle p\rangle^{-1} T_p$$

Thus the Hecke operators $\langle n\rangle$ and T_n for n relatively prime to N are normal.

Proof. Let $f, g \in \mathcal{S}_k(\Gamma_1(N))$ be any. Note that $\Gamma_1(N) \trianglelefteq \Gamma_0(N)$, so by Proposition 2.15 (i),

$$\begin{aligned} \langle p\rangle^* &= [\alpha]_k^* \text{ for any } \alpha \in \Gamma_0(N) \text{ such that } \alpha \equiv \begin{bmatrix} * & * \\ 0 & p \end{bmatrix} \text{ (mod N)} \\ &= [\alpha^{-1}]_k = \langle p\rangle^{-1} \end{aligned}$$

For the second formula using Proposition 2.15-(ii) we get;

$$T_p{}^* = \left[\Gamma_1(N)\begin{bmatrix}1 & 0\\ 0 & p\end{bmatrix}\Gamma_1(N)\right]_k^* = \left[\Gamma_1(N)\begin{bmatrix}p & 0\\ 0 & 1\end{bmatrix}\Gamma_1(N)\right]_k$$

Let m and n be two integers such that $mp - nN = 1$, then by an easy calculation we get $\begin{bmatrix}p & 0\\ 0 & 1\end{bmatrix} = \underbrace{\begin{bmatrix}1 & n\\ N & mp\end{bmatrix}^{-1}}_{\in\Gamma_1(N)}\begin{bmatrix}1 & 0\\ 0 & p\end{bmatrix}\underbrace{\begin{bmatrix}p & n\\ N & m\end{bmatrix}}_{\in\Gamma_0(N)}$. Therefore;

$$\Gamma_1(N)\begin{bmatrix}p & 0\\ 0 & 1\end{bmatrix}\Gamma_1(N) = \Gamma_1(N)\begin{bmatrix}1 & 0\\ 0 & p\end{bmatrix}\Gamma_1(N)\begin{bmatrix}p & n\\ N & m\end{bmatrix}$$

.

Now, suppose $\Gamma_1(N)\begin{bmatrix}p & 0\\ 0 & 1\end{bmatrix}\Gamma_1(N) = \bigcup_j \Gamma_1(N)\beta_j$ is the decomposition of the double coset describing T_p, then we have

$$\Gamma_1(N)\begin{bmatrix}p & 0\\ 0 & 1\end{bmatrix}\Gamma_1(N) = \bigcup_j \Gamma_1(N)\beta_j\begin{bmatrix}p & n\\ N & m\end{bmatrix}$$

as the decomposition for T_p^*.

Hence, we get $T_p^* = \langle p\rangle^{-1}T_p$ since $m \equiv p^{-1} \pmod N$. □

From the Spectral Theorem of linear algebra (see [K89], Chapter 9 for details), given commuting family of normal operators on a finite dimensional inner product space, the space has an orthogonal basis of simultaneous eigenvectors for the operators. Since each vector is a modular form we say *eigenform* instead. So, we have the result:

Theorem 2.17. *The space $\mathcal{S}_k(\Gamma_1(N))$ has an orthogonal basis of simultaneous eigenforms for the Hecke operators $\{\langle n\rangle, T_n : (n,N) = 1\}$.*

2.5 Oldforms and Newforms

If $M \mid N$, then we know that $\mathcal{S}_k(\Gamma_1(M)) \subseteq \mathcal{S}_k(\Gamma_1(N))$ since $\Gamma_1(N) \subseteq \Gamma_1(M)$. This is one way to move between levels. Another way to embed $\mathcal{S}_k(\Gamma_1(M))$ into $\mathcal{S}_k(\Gamma_1(N))$ is by composing with the multiple-by-d map, where d is any factor of N/M. For any such d, let $\alpha_d = \begin{bmatrix}d & 0\\ 0 & 1\end{bmatrix}$ so that, $(f[\alpha_d]_k)(\tau) = d^{k-1}f(d\tau)$ for $f : \mathbb{H} \to \mathbb{C}$. The injective linear map $[\alpha_d]_k$ takes $\mathcal{S}_k(\Gamma_1(M))$ to $\mathcal{S}_k(\Gamma_1(N))$ and lifts the level M to the level N.

Definition 2.18. For each divisor d of N, let i_d be the map;

$$i_d : \mathcal{S}_k(\Gamma_1(Nd^{-1})) \times \mathcal{S}_k(\Gamma_1(Nd^{-1})) \to \mathcal{S}_k(\Gamma_1(N))$$

given by

$$(f, g) \mapsto f + g[\alpha_d]_k$$

The subspace of **oldforms at level N** is

$$\mathcal{S}_k(\Gamma_1(N))^{\text{old}} = \sum_{\substack{p|N \\ p \text{ prime}}} i_p\left(\left(\mathcal{S}_k(\Gamma_1(Np^{-1}))\right)^2\right)$$

and the subspace of **newforms at level** N is the orthogonal complement with respect to the Petersson inner product

$$\mathcal{S}_k(\Gamma_1(N))^{\text{new}} = \left(\mathcal{S}_k(\Gamma_1(N))^{\text{old}}\right)^{\text{old}}$$

Proposition 2.19. *The subspace $\mathcal{S}_k(\Gamma_1(N))^{old}$ and $\mathcal{S}_k(\Gamma_1(N))^{new}$ are stable under the Hecke operators T_n and $\langle n\rangle$ for all $n \in \mathbb{Z}^+$.*

Proof. See [DS05], Proposition 5.6.2. □

Corollary 2.20. *The spaces $\mathcal{S}_k(\Gamma_1(N))^{old}$ and $\mathcal{S}_k(\Gamma_1(N))^{new}$ have orthogonal bases of eigenforms for the Hecke operators away from the level, $\{T_n, \langle n\rangle : (n, N) = 1\}$.*

2.6 Eigenforms

By Corollary 2.20 on page 24 the spaces $\mathcal{S}_k(\Gamma_1(N))^{\text{old}}$ and $\mathcal{S}_k(\Gamma_1(N))^{\text{new}}$ have orthogonal bases of eigenforms for the Hecke operators $\{T_n, \langle n\rangle : (n, N) = 1\}$. In this section we show that if $f \in \mathcal{S}_k(\Gamma_1(N))^{\text{new}}$ is such an eigenform then in fact f is an eigenform for all T_n and $\langle n\rangle$. Note that if $(n, N) > 1$ then $\langle n\rangle = 0$ hence f is an eigenform for all $\langle n\rangle$, so we only need to check T_n.

Definition 2.21. A nonzero modular form $f \in \mathcal{M}_k(\Gamma_1(N))$ that is an eigenform for the Hecke operators T_n and $\langle n\rangle$ for all $n \in \mathbb{Z}^+$ is a **Hecke eigenform** or simply an **eigenform**. The eigenform $f(\tau) = \sum_{n=0}^{\infty} a_n(f)(e^{2\pi i\tau})^n$ is **normalized** when $a_1(f) = 1$. A **newform** is a normalized eigenform in $\mathcal{S}_k(\Gamma_1(N))^{\text{new}}$.

Now, we will show that $\mathcal{S}_k(\Gamma_1(N))^{\text{new}}$ has an orthogonal basis of newforms.

Suppose $f \in \mathcal{S}_k(\Gamma_1(N))^{\text{new}}$ and $f \neq 0$. Then $f \notin \mathcal{S}_k(\Gamma_1(N))^{\text{old}}$ and $a_1(f) \neq 0$, so we may assume that f is normalized to $a_1(f) = 1$. For any $m \in \mathbb{Z}^+$ define $g_m = T_m(f) - a_m(f)(f) \in \mathcal{S}_k(\Gamma_1(N))^{\text{new}}$. Then g_m is an eigenform for the Hecke operators T_n and $\langle n \rangle$ for $(n, N) = 1$. Indeed, for $\langle n \rangle$, we have $\langle n \rangle(g_m) = \langle n \rangle(T_m(f)) - \langle n \rangle(a_m(f)(f)) = T_m(\langle n \rangle(f)) - a_m(f)(\langle n \rangle(f)) = T_m(d_n(f)) - a_m(f)(d_n(f)) = d_n(T_m(f) - a_m(f)(f)) = d_n(g_m)$ and for T_n we have $T_n(g_m) = T_n(T_m(f)) - T_n(a_m(f)(f)) = T_m(T_n(f)) - a_m(f)T_n(f) = T_m(a_n(f)f) - a_m(f)a_n(f)f = a_n(f)g_m$. The first Fourier coefficient of g_m is $a_1(g_m) = a_1(T_m(f)) - a_1(a_m(f)f) = a_m(f) - a_1(f)a_m(f) = 0$. Thus $g_m \in \mathcal{S}_k(\Gamma_1(N))^{\text{old}}$ and hence $g_m \in \mathcal{S}_k(\Gamma_1(N))^{\text{old}} \cap \mathcal{S}_k(\Gamma_1(N))^{\text{new}} = \{0\}$, so that $T_m(f) = a_m(f)f$. We have the following theorem:

Theorem 2.22. *Let $f \in \mathcal{S}_k(\Gamma_1(N))^{new}$ be a nonzero eigenform for the Hecke operators T_n and $\langle n \rangle$ for all n with $(n, N) = 1$. Then;*

(i) f is a Hecke eigenform, i.e. an eigenform for T_n and $\langle n \rangle$ for all $n \in \mathbb{Z}^+$. A suitable scalar multiple of f is a newform.

(ii) If $\tilde{f}$ satisfies the same conditions as f and has the same T_n-eigenvalues then $\tilde{f} = cf$ for some constant c.

The set of all newforms in the space $f \in \mathcal{S}_k(\Gamma_1(N))^{new}$ is an orthogonal basis of the space.

Proof. We have already proven part (i). For part (ii), let $\tilde{f}$ and f be as above. Then $c\tilde{f}$ and df are newforms for some constants c and d. Let d_n be T_n-eigenvalue of f and $\tilde{f}$. Then;

$$a_n(c\tilde{f})c\tilde{f} = T_n(c\tilde{f})c\tilde{f} = cd_n\tilde{f}$$

and

$$a_n(df)df = T_n(df)df = dd_n(f)$$

Thus $a_n(\tilde{f}) = \frac{d_n}{c}$ and $a_n(f) = \frac{d_n}{d}$ and we are done. □

The following theorem gives a basis for the space $\mathcal{S}_k(\Gamma_1(N))$.

Theorem 2.23. *The set*

$$\mathcal{B}_k(N) = \{f(n\tau) = f \text{ is a newform of level } M \text{ and } nM|N\}$$

is a basis for $\mathcal{S}_k(\Gamma_1(N))$.

Proof. See [DS05], Theorem 5.8.3. □

Chapter 3

Jacobians and Abelian Varieties

In this chapter we define Jacobians and Abelian varieties that come form a weight-2 eigenform.

3.1 Introduction

We begin with some preliminaries. Note that modular curves are compact Riemann surfaces. We, now introduce some basic information about compact Riemann surfaces.

Let X be a compact Riemann surface of genus g. It is a sphere with g handles. The holomorphic differentials on X will be denoted by $\Omega^1_{\text{hol}}(X)$. It basicly is a g-dimensional vector space over $\mathbb{C}$. Let $A_1, \ldots, A_g$ be the longitudinal loops and $B_1, \ldots, B_g$ be the latitudinal loops. The group of integer sums of integration over loops is the free abelian group generated by integration over the loops A_i and B_i and this group is called the first homology group of X denoted by $\mathrm{H}_1(X, \mathbb{Z})$, which is;

$$\mathrm{H}_1(X, \mathbb{Z}) = \mathbb{Z}\int_{A_1} \oplus \ldots \oplus \mathbb{Z}\int_{A_g} \oplus \mathbb{Z}\int_{B_1} \oplus \ldots \oplus \mathbb{Z}\int_{B_g} \simeq \mathbb{Z}^{2g}$$

The homology group is the subgroup of the dual space $\Omega^1_{\text{hol}}(X)^\wedge = \mathrm{Hom}_{\mathbb{C}}(\Omega^1_{\text{hol}}(X), \mathbb{C})$ and the dual space is;

$$\Omega^1_{\text{hol}}(X)^\wedge = \mathbb{R}\int_{A_1} \oplus \ldots \oplus \mathbb{R}\int_{A_g} \oplus \mathbb{R}\int_{B_1} \oplus \ldots \oplus \mathbb{R}\int_{B_g}$$

hence $\mathrm{H}_1(X, \mathbb{Z})$ is a lattice in $\Omega^1_{\text{hol}}(X)^\wedge$.

Definition 3.1. The *Jacobian* of X is defined as

$$\mathrm{Jac}(X) = \Omega^1_{\mathrm{hol}}(X)^\wedge / \mathrm{H}_1(X, \mathbb{Z})$$

Since the homology is a $2g$ dimensional lattice in $\Omega^1_{\mathrm{hol}}(X)^\wedge$, the Jacobian is a g dimensional complex torus $\mathbb{C}^g/\Lambda_g$

Let $\mathbb{C}(X)$ denote the field of meromorphic functions on X. The degree-0 divisor group of X is

$$\mathrm{Div}^0(X) = \left\{ \sum_{x \in X} n_x x : n_x \in \mathbb{Z}, n_x = 0 \text{ for almost all } x, \text{ and } \sum_{x \in X} n_x = 0 \right\}$$

The subgroup of principal divisors is

$$\mathrm{Div}^\ell(X) = \{\delta \in \mathrm{Div}^0(X) : \delta = \mathrm{div}(f) \text{ for some } f \in \mathbb{C}(X)\}$$

where the divisor of a meromorphic function $f \in \mathbb{C}(X)$ is defined as

$$\mathrm{div}(f) = \sum_{x \in X} v_x(f) x$$

The degree-0 Picard group of X is

$$\mathrm{Pic}^0(X) = \mathrm{Div}^0(X)/\mathrm{Div}^\ell(X)$$

If X has genus $g > 0$ and $x_0 \in X$ then X embeds into its Picard group

$$X \to \mathrm{Pic}^0(X), \quad \text{given by } x \mapsto [x - x_0]$$

Indeed, suppose $x, x' \in X$ maps to the same equivalence class then we have $x - x' = \mathrm{div}(f)$ for some $f \in \mathbb{C}(X)$. Considering f as a holomorphic function $f : X \to \hat{\mathbb{C}}$ we see that f has degree 1. Since $g > 0$ by Riemann-Hurwitz formula (see [H83] for details) it is impossible. Hence the map is injective.

We also have a map from degree-0 divisors to the Jacobian

$$\mathrm{Div}^0(X) \to \mathrm{Jac}(X), \quad \text{given by } \sum_x n_x x \mapsto \sum_x n_x \int_{x_0}^x$$

Abel's Theorem states that this map induces an isomorpism between the Picard group and the Jacobian

Theorem 3.2. Abel's Theorem *The above map induces an isomorphism* $Pic^0(X) \to Jac(X)$ *given by* $[\sum_x n_x x] \mapsto \sum_x n_x \int_{x_0}^{x}$

Abel's Theorem states that principal divisors maps to trivial integration on $\Omega^1_{\text{hol}}(X)$ modulo integration over loops. If X has genus $g > 0$ then its embedding into its Picard group followed by the isomorphism of Abel's Theorem shows that the map

$$X \to \text{Jac}(X), \qquad x \mapsto \int_{x_0}^{x}$$

emdeds the Riemann surface in its Jacobian. Abel's Theorem also implies the fact that

$$\Omega^1_{\text{hol}}(X)^{\wedge} = \left\{ \sum_{\gamma} n_\gamma \int_\gamma : \sum_{\gamma} n_\gamma = 0 \right\}$$

3.2 Modular Jacobians and Hecke Operators

The Hecke operators give rise to holomorphic maps between modular curves which are compact Riemann surfaces. They lead to maps between Jacobians of modular curves and Picard groups.

Let Γ_1 and Γ_2 be two congruence subgroups of $\text{SL}_2(\mathbb{Z})$ and $\alpha \in \text{GL}_2^+(\mathbb{Q})$. The double coset operator $[\Gamma_1\alpha\Gamma_2]_2$ induces a map between divisor groups of modular curves

$$[\Gamma_1\alpha\Gamma_2]_2 : \text{Div}(X_2) \to \text{Div}(X_1)$$

which is the $\mathbb{Z}$-linear extension of the map $\Gamma_2\tau \to \sum_j \Gamma_1\beta_j(\tau)$, where β_j are orbit representatives of $\Gamma_1\alpha\Gamma_2$ under the action of Γ_1. This map comes from the composition of the maps in the following diagram:

$$\begin{tikzcd}
X_3 \arrow[r] \arrow[d, "\pi_2"] & X_3' \arrow[d, "\pi_1"] \\
X_2 & X_1
\end{tikzcd}$$

where the top row is the isomorphism given by $\Gamma_3\tau \to \Gamma_3'\alpha(\tau)$. $[\Gamma_1\alpha\Gamma_2]_2$ descends to map of Picard groups;

$$[\Gamma_1\alpha\Gamma_2]_2 = (\pi_1)_P \circ \alpha_P(\pi_2)^P : \text{Pic}^0(X_2) \to \text{Pic}(X_1)$$

given by

$$\left[\sum_{\tau}\Gamma_2\tau\right] \mapsto \left[\sum_{\tau} n_\tau \sum_{j}\Gamma_1\beta_j(\tau)\right]$$

We need the following result to define the action of the double coset operator on the Jacobians;

Proposition 3.3. *Let Γ be a congruence sungroup of $SL_2(\mathbb{Z})$. Then the holomorphic differentials $\Omega^1_{hol}(X(\Gamma))$ and the weight-2 cusp forms $\mathcal{S}_2(\Gamma)$ are isomorphic as vector spaces over $\mathbb{C}$,*

$$\omega : \mathcal{S}_2(\Gamma) \xrightarrow{\sim} \Omega^1_{hol}(X(\Gamma)), \qquad f \rightarrow (\omega_j)_{j\in J}$$

where ω_j pulls back to $f(\tau)d\tau \in \Omega^1_{hol}(\mathcal{H})$

Proof. (See: [DS05], Theorem 3.3.1) □

By the proposition above we can identify $\Omega^1_{\text{hol}}(X(\Gamma))$ and $\mathcal{S}(\Gamma)$. So we can also identify $\Omega^1_{\text{hol}}(X(\Gamma))^\wedge$, $\mathcal{S}(\Gamma)^\wedge$. Let $\mathrm{H}_1(X(\Gamma), \mathbb{Z})$ denote the corresponding subgroup of $\mathcal{S}(\Gamma)^\wedge$. Then we can identify the Jacobian of $X(\Gamma)$ in terms of the dual space of weight-2 cusp forms.

Definition 3.4. Let Γ be a congruence subgroup of $\mathrm{SL}_2(\mathbb{Z})$. The *Jacobian* of the modular curve $X(\Gamma)$ is

$$\mathrm{Jac}(X(\Gamma)) = \mathcal{S}_2(\Gamma)^\wedge / \mathrm{H}_1(X(\Gamma), \mathbb{Z})$$

Now, let X and Y be the modular curves whose congruence subgroups are Γ_X and Γ_Y. Let $\alpha \in \mathrm{GL}_2^+(\mathbb{Q})$ be such that $\alpha\Gamma\alpha^{-1} \subset \Gamma_Y$ and consider the corresponding holomorphic map $h : X \rightarrow Y$, given by $\Gamma_X\tau \mapsto \Gamma_Y\alpha(\tau)$.

Denote the isomorphism between $\Omega^1_{\text{hol}}(X)$ (respectively $\Omega^1_{\text{hol}}(Y)$) and $\mathcal{S}_2(\Gamma_X)$ (respectively $\mathcal{S}_2(\Gamma_Y)$) by ω_X (respectively ω_Y). Then we have the following commutative diagram:

$$\begin{tikzcd}
\mathcal{S}_2(\Gamma_Y) \arrow[r, "{[\alpha]_2}"] \arrow[d, "\omega_Y"] & \mathcal{S}_2(\Gamma_X) \arrow[d, "\omega_X"] \\
\Omega^1_{\text{hol}}(Y) \arrow[r, "h^*"] & \Omega^1_{\text{hol}}(X)
\end{tikzcd}$$

To see this, it is enough to check that $f([\alpha]_2)(\tau)d\tau = f(\alpha(\tau))d(\alpha(\tau))$. But it is clear that it holds.

The induced map on the dual space is

$$h_* : \mathcal{S}_2(\Gamma_X)^\wedge \to \mathcal{S}_2(\Gamma_X)^\wedge \qquad \varphi \mapsto \varphi \circ [\alpha]_2$$

.

Suppose, $\alpha\Gamma_X\alpha^{-1} \setminus \Gamma_Y = \bigcup_j \alpha\Gamma_X\alpha^{-1}[\gamma_{Y,j}]_2$ then the following diagram is commutative;

$$\begin{tikzcd}
\mathcal{S}_2(\Gamma_X) \arrow[r, "\sum_j[\Gamma_{Y,j}]_2"] \arrow[d, "\omega_X"] & \mathcal{S}_2(\Gamma_Y) \arrow[d, "\omega_Y"] \\
\Omega^1_{\text{hol}}(X) \arrow[r, "\text{tr}_h"] & \Omega^1_{\text{hol}}(X)
\end{tikzcd}$$

Letting tr_h also denote the top map the induced map on the dual space is

$$\text{tr}_h^\wedge : \mathcal{S}_2(\Gamma_Y)^\wedge \to \mathcal{S}_2(\Gamma_X)^\wedge, \qquad \psi \mapsto \psi \circ \sum_j [\gamma_{Y,j}]_2$$

Now, h_* and and $\text{tr}_h^\wedge$ descends to Jacobians.

Recall that the double coset operator $[\Gamma_1\alpha\Gamma_2]_2 : \mathcal{S}(\Gamma_1) \to \mathcal{S}(\Gamma_2)$ given by $f[\Gamma_1\alpha\Gamma_2]_2 = \sum_j f[\beta_j]_2$. Its dual map denoted as the same is

$$[\Gamma_1\alpha\Gamma_2]_2 : \mathcal{S}_2(\Gamma_2)^\wedge \to \mathcal{S}_2(\Gamma_1)^\wedge \qquad \varphi \mapsto \varphi \circ [\Gamma_1\alpha\Gamma_2]_2$$

which can be realized as $(\pi_1)_* \circ \alpha \circ \text{tr}_{\pi_2}^\wedge$. Thus the double coset operator on Jacobians is

$$[\Gamma_1\alpha\Gamma_2]_2 = (\pi_1)_J \circ \alpha_J \circ (\pi_2)^J : \text{Jac}(X_2) \to \text{Jac}(X_1), \qquad [\psi] \mapsto [\psi \circ [\Gamma_1\alpha\Gamma_2]_2]$$

Let $J_1(N)$ denote the Jacobian of the modular curve $X_1(N)$. The following proposition which is a special case of the above discussion describes the action of the Hecke operator on $J_1(N)$

Proposition 3.5. *The Hecke operators $T = T_p$ and $T = \langle d \rangle$ act by composition on the Jacobian of $X_1(N)$,*

$$T : J_1(N) \to J_1(N), \qquad [\varphi] \mapsto [\varphi \circ T]$$

for $\varphi \in \mathcal{S}_2(\Gamma_1(N))^\wedge$.

Thus the Hecke operators acts as endomorphisms on the homology $H_1(X_1(N), \mathbb{Z})$ which is a finitely generated Abealian group. Hence the characteristic polynomial $f(x)$ of T_p has integer coefficients and it is monic. T_p satisfies its characteristic polynomial and so $f(T_p) = 0$ on . Since T_p is $\mathbb{C}$-linear $f(T_p) = 0$ on $\mathcal{S}_2(\Gamma_1(N))^\wedge$ and so $f(T_p) = 0$ on $\mathcal{S}_2(\Gamma_1(N))$. Therefore the minimal polynomial of T_p on $\mathcal{S}_2(\Gamma_1(N))$ divides $f(x)$ and the eigenvalues of T_p satisfies $f(x)$ which makes them algebraic integers. Hence we have proved the following theorem:

Theorem 3.6. *Let $f \in \mathcal{S}_2(\Gamma_1(N))$ be a normalized eigenform. Then the eigenvalues $a_n(f)$ are algebraic integers.*

Definition 3.7. The Hecke algebra over $\mathbb{Z}$ is the algebra of endomorphisms of $\mathcal{S}_2(\Gamma_1(N))$ generated over $\mathbb{Z}$ by the Hecke operators,

$$\mathbb{T}_{\mathbb{Z}} = \mathbb{Z}[\{T_n, \langle n \rangle : n \in \mathbb{Z}^+\}]$$

The Hecke algebra over $\mathbb{C}$ is defined similarly.

Being a ring of endomorphisms of finitely generated free $\mathbb{Z}$-module $\mathrm{H}_1(X_1(N), \mathbb{Z})$, $\mathbb{T}_{\mathbb{Z}}$ is finitely generated as well. Let $f(\tau) = \sum_{n=1}^{\infty} a_n(f) q^n$ be a normalized eigenform. Define the homomorphism

$$\lambda_f : \mathbb{T}_{\mathbb{Z}} \to \mathbb{C}, \qquad Tf = \lambda_f(T) f$$

The image of λ_f is a finitely generated $\mathbb{Z}$-module. Actually, the image of λ_f is $\mathbb{Z}[a_n(f) : n \in \mathbb{Z}^+]$. This ring is a finite extension of $\mathbb{Q}$ and the extension degree is the rank $\mathbb{T}_{\mathbb{Z}}/\mathcal{I}_f$.

Definition 3.8. Let $f \in \mathcal{S}_2(\Gamma_1(N))$ be a normalized eigenform and suppose $f(\tau) = \sum a_n(f) q^n$. The field $K_f = \mathbb{Q}(\{a_n(f)\})$ is called the *number field of f*.

Any embedding $\sigma : K_f \hookrightarrow \mathbb{C}$ conjugates f by acting on its coefficients

$$f^\sigma(\tau) = \sum_{n=1}^{\infty} a_n(f)^\sigma q^n$$

So, we may ask the question whether f^σ is an eigenform or not. The following theorem clarifies this result.

Theorem 3.9. *Let f be a weight-2 normalized eigenform for the Hecke operators then f^σ is also a newform.*

Proof. (See: [DS05], Theorem 6.5.4) □

Corollary 3.10. *The space $\mathcal{S}_2(\Gamma_1(N))$ has a basis of forms with rational integer coefficients.*

Proof. Let f be a a newform at level M with $M \mid N$. Let $K = K_f$ and $\{\alpha_1, \ldots, a_d\}$ be a basis of O_K as a $\mathbb{Z}$-module. Let $\{\sigma_1, \ldots, \sigma_d$ be the embedding of K into $\mathbb{C}$. Consider the matrix

$$A = \begin{pmatrix} {\alpha_1}^{\sigma_1} & \ldots & {\alpha_1}^{\sigma_d} \\ \vdots & \ddots & \vdots \\ {\alpha_d}^{\sigma_1} & \ldots & {\alpha_d}^{\sigma_d} \end{pmatrix}$$

and let

$$f = \begin{pmatrix} f^{\sigma_1} \\ \vdots \\ f^{\sigma_d} \end{pmatrix}$$

Set $g = Af$, so that

$$g_i = \sum_{j=1}^{d} {\alpha_i}^{\sigma_j} f^{\sigma_j}$$

Since A is invertible, $\operatorname{span}(\{g_1, \ldots, g_d\}) = \operatorname{span}(\{f^{\sigma_1}, \ldots, f^{\sigma_d}\})$. Let $g_i(\tau) = \sum a_n(g_i)q^n$ with $a_n(g_i) \in \bar{\mathbb{Z}}$. For any automorphism $\sigma : \mathbb{C} \to \mathbb{C}$ as σ_j runs through the embeddings of K_f into $\mathbb{C}$ so does $\sigma_j\sigma$ (composing left to right), and so

$$g_i^{\sigma} = \sum_{j=1}^{d} \alpha_j^{\sigma_j\sigma} f^{\sigma_j\sigma} = g$$

That is, each $a_n(g_i)$ is fixed by all automorphisms of $\mathbb{C}$, showing that each $a_n(g_i)$ lies in $\bar{\mathbb{Z}} \cap \mathbb{Q} = \mathbb{Z}$. Repeating this argument for each newform f whose level divides N gives the result.

□

3.3 Abelian Varieties

Let $f \in \mathcal{S}_2(\Gamma_1(M_f))$ be a newform at some level M_f. Recall the map $\lambda_f : \mathbb{T}_{\mathbb{C}}$, $Tf = \lambda_f f$. This induces a $\mathbb{T}_{\mathbb{Z}}$-module isomorphism $\mathbb{T}_{\mathbb{Z}}/\mathcal{I}_f \simeq \mathbb{Z}[\{a_n(f)\}]$ and note that $\mathbb{Z}[\{a_n(f)\}]$ has rank $[K_f : \mathbb{Q}]$. Also, we know that $\mathbb{T}_{\mathbb{Z}}$ acts on $J_1(M_f)$.

Definition 3.11. The *Abelian variety* associated to f is defined as the quotient

$$A_f = J_1(M_f)/\mathcal{I}_f J_1(M_f)$$

By definition, $\mathbb{T}_{\mathbb{Z}}$ acts on A_f and so $\mathbb{Z}[\{a_n(f)\}]$ acts on A_f as well. We have the following commutative diagram:

$$\begin{tikzcd}
J_1(M_f) \arrow[r, "T_p"] \arrow[d] & J_1(M_f) \arrow[d] \\
A_f \arrow[r, "a_p(f)"] & A_f
\end{tikzcd}$$

where $a_p(f)$ acts on A_f as T_p. Let $\varphi \in A_f$ and $\sigma : K_f \to \mathbb{C}$ be an embedding. Then, by Theorem 3.9 on page 32;

$$(a_p(f)\varphi)(f^\sigma) = \varphi(\circ T_p)(f^\sigma) = \varphi(a_p(f^\sigma)f^\sigma) = a_p(f)^\sigma \varphi(f^\sigma)$$

If $a_p(f) \in \mathbb{Z}$ then it acts on A_f as multiplication.

Define the following equivalence relation on newforms:

$$\tilde{f} \sim f \Leftrightarrow \tilde{f} = f^\sigma \text{ for some automorphism } \sigma : \mathbb{C} \to \mathbb{C}$$

Let f denote the equivalence class of f. Again by Theorem 3.9 on page 32 each $f^\sigma \in [f]$ is a newform at level M_f, so that the subspace

$$V_f = \text{span}([f]) \subset \mathcal{S}_2(\Gamma_1(M_f))$$

has dimension $[K_f : \mathbb{Q}]$. Restricting the elements of $\mathrm{H}_1(X_1(M_f), \mathbb{Z})$ to functions on V_f gives the subgroup of the dual $V_f^\wedge$,

$$\Lambda_f = \mathrm{H}_1(X_1(M_f), \mathbb{Z})|_{V_f}$$

and so we have a well defined homomorphism $J_1(M_f) \to V_f^\wedge/\Lambda_f$, given by $[\varphi] \mapsto \varphi|_{V_f} + \Lambda_f$ for $\varphi \in \mathcal{S}_2(\Gamma_1(M_f))^\wedge$

Proposition 3.12. *Let $f \in \mathcal{S}_2(\Gamma_1(M_f))$ be a newform with some number field K_f. Then restricting to V_f induces an isomorphism*

$$A_f \to {V_f}^\wedge/\Lambda_f \text{ given by } [\varphi] + \mathcal{I}_f J_1(M_f) \mapsto \varphi|_{V_f} + \Lambda_f \text{ for } \varphi \in \mathcal{S}_2(\Gamma_1(M_f))^\wedge$$

Proof. (See: [DS05], Proposition 6.6.4) □

Recall the definition;

Definition 3.13. An *isogeny* is a holomorphic homomorphism between complex tori that surjects and has finite kernel.

The next theorem gives us a decomposition of $J_1(N)$,

Theorem 3.14. *$J_1(N)$ is isogeneous to a direct sum of Abelian varieties associated to equivalence classes of newforms;*

$$J_1(N) \to \oplus_f A_f^{m_f}$$

where the direct sum is taken over a set of representatives $f \in \mathcal{S}_2(\Gamma_1(N))$ at levels $M_f \mid N$ and each m_f is the number of divisors of N/M_f.

Proof. (See: [DS05] Theorem 6.6.6) □

Remark 3.15. We have the following commutative diagram;

$$\begin{tikzcd}
J_1(N) \arrow[r, "T_p"] \arrow[d] & J_1(N) \arrow[d] \\
\bigoplus_{f,n} A_f \arrow[r, "\prod_{f,n} a_p(f)"] & \bigoplus_{f,n} A_f
\end{tikzcd}$$

where p is a prime not dividing N and the vertical maps are isogenies. To see that this diagram commutes; let $\varphi \in J_1(N)$. Then

$$a_p(f) \circ \Psi_{f,n}(\varphi)(f^\sigma(\tau)) = a_p(f)(n\varphi(f^\sigma(n\tau))) = n\varphi(T_p(f^\sigma(n\tau))$$

and

$$(\Psi_{f,n} \circ T_p)(\varphi)(f^\sigma(\tau)) = \Psi_{f,n}(\varphi(T_p f^\sigma(\tau))) = n\varphi((T_p f^\sigma)(n\tau))$$

Computing the Fourier coefficients we see that these two are the same. Thus the diagram commutes.

Chapter 4

Galois Representations

In this chapter we construct Galois representations attached to elliptic curves and modular forms. Then we will give an overview of the method of Wiles's proof of modularity theorem.

4.1 Galois Number Fields

Recall that a number field is a field $F \subset \bar{\mathbb{Q}}$-the algebraic closure of $\mathbb{Q}$, such that the degree of the extension F over $\mathbb{Q}$; $[F : \mathbb{Q}]$ is finite. We will only take the extensions which are Galois over $\mathbb{Q}$. Each number field has its ring of algebraic integers $\mathcal{O}_F$. In this section we will illustrate some results form algebraic number theory in the Galois case without proof and we will give some spesific examples. (For detailed information about the topic see: [L96] or [L00])

Let F is a Galois number field and $p \in \mathbb{Z}$ be a prime. There are positive integers e, f and g such that we could describe the ideal $p\mathcal{O}_F$ as a product of maximal ideals of $\mathcal{O}_F$;

$$p\mathcal{O}_F = (\mathbf{p}_1 \dots \mathbf{p}_g)^e$$

where

$$\mathcal{O}_F/\mathbf{p}_i \simeq \mathbb{F}_{p^f} \quad \text{for all } i = 1, 2, \dots, g$$

and

$$efg = [F : \mathbb{Q}]$$

The *ramification degree e* says how many times each maximal ideal $\mathbf{p}$ of $\mathcal{O}_F$ that lies over p repeats as a factor of $p\mathcal{O}_F$. There are only finitely many p such that

$e > 1$, those are the primes that *ramify* in F. The residue degree f, is the dimension of the residue field $\mathbf{f_p} = O_F/\mathbf{p}$ (a finite field) as a vector space over $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$ for any $\mathbf{p}$ over p. The *decomposition index* g, is the number of distinct $\mathbf{p}$ over p. The condition $efg = [F : \mathbb{Q}]$ implies that the net measure of ramification degree, and the decomposition index associated to each rational prime p is the field extension degree or equivalently $efg = [\mathrm{Gal}(F/\mathbb{Q})]$.

Example: A (family of) simple Galois number fields are the cyclotomic fields.

Let N be a positive integer. Let $F = \mathbb{Q}(\mu_N)$ where μ_N is a primitive N-th root of unity. We may take $\mu_N = e^{2\pi i/N}$. Then we have $[F : \mathbb{Q}] = \Phi(N)$ where Φ is the Euler totient function and the Galois group of the extension F over $\mathbb{Q}$ is a group isomorphic to $(\mathbb{Z}/N\mathbb{Z})^*$. The isomorphism is given by;

$$\mathrm{Gal}(F/\mathbb{Q}) \to (\mathbb{Z}/N\mathbb{Z})^*, \qquad (\mu_N \mapsto \mu_N^a) \to a(\bmod N)$$

The cyclotomic integers are;

$$O_F = \mathbb{Z}[\mu_N] = \{a_0 + a_1\mu_N + \ldots + a_{N-1}\mu^{N-1} : a_0, \ldots, a_{N-1} \in \mathbb{Z}\}$$

In this case each rational prime not dividing N is unramified in F,

$$pO_F = \mathbf{p}_1 \ldots \mathbf{p}_g, \qquad (\text{where} p \nmid N)$$

and its residue degree f is the order of $p \bmod N$ in $(\mathbb{Z}/N\mathbb{Z})^*$. Note that the primes dividing N ramify in $\mathbb{Q}(\mu_N)$.

Example: For a spesific example let d be a cubefree integer, let $d^{1/3}$ denote the real cube root of d, and let $F = \mathbb{Q}(d^{1/3}, \mu_3)$.

In this case, $[F : \mathbb{Q}] = 6$ and $\mathrm{Gal}(F/\mathbb{Q})$ is isomorphic to Sym(3)- the symmetric group on three letters. The Galois group is generated by

$$\sigma : \begin{pmatrix} d^{1/3} \mapsto \mu_3 d^{1/3} \\ \mu_3 \mapsto \mu_3 \end{pmatrix}, \qquad \tau : \begin{pmatrix} d^{1/3} \mapsto d^{1/3} \\ \mu_3 \mapsto \mu_3^2 \end{pmatrix}$$

and the isomorphism is given by

$$\mathrm{Gal}(F/\mathbb{Q}) \to \mathrm{Sym}(3), \qquad \sigma \mapsto (123), \quad \tau \mapsto (23)$$

The rational primes not dividing $3d$ are unramified in F, and we have:

$$pO_F = \begin{cases} \mathbf{p}_1 \ldots \mathbf{p}_6 & \text{if } p \equiv 1(\text{mod } 3) \text{ and } d \text{ is a cube modulo } p, \\ \mathbf{p}_1\mathbf{p}_2 & \text{if } p \equiv 1(\text{mod } 3) \text{ and } d \text{ is not a cube modulo } p, \\ \mathbf{p}_1\mathbf{p}_2\mathbf{p}_3 & \text{if } p \equiv 1(\text{mod } 2) \end{cases}$$

Now, we continue to the general case. Let F be a Galois number field and let p be a rational prime. For each maximal ideal $\mathbf{p}$ of O_F lying over p be a rational prime. For each maximal ideal $\mathbf{p}$ of O_F lying over p, the *decomposition group* of $\mathbf{p}$ is the subgroup of the Galois group that fixes $\mathbf{p}$ as a set;

$$\mathcal{D}_{\mathbf{p}} = \{\sigma \in \text{Gal}(F/\mathbb{Q}) : \mathbf{p}^{\sigma} = \mathbf{p}\}$$

The decomposition group has order ef, so its index in $\text{Gal}(F/\mathbb{Q})$ is indeed the decomposition index g. By its definition it acts on the residue field $\mathbf{f}_{\mathbf{p}} = O_F/\mathbf{p}$,

$$(x + \mathbf{p})^{\sigma} = x^{\sigma} + \mathbf{p}, \qquad \text{where } x \in O_F, \quad \sigma \in \mathcal{D}_{\mathbf{p}}$$

.

The *inertia group* of $\mathbf{p}$ is the kernel of this action,

$$\mathcal{I}_{\mathbf{p}} = \{\sigma \in \mathcal{D}_{\mathbf{p}} : x^{\sigma} \equiv x\,(\text{mod } \mathbf{p}) \text{ for all } x \in O_F\}$$

The inertia group has order e, so it is trivial for all $\mathbf{p}$ lying over an unramified p. The Frobenius map $\sigma_p : x \rightarrow x^p$ in characteristic p is an automorphism which is called the *Frobenius automorphim.* If we view $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$ as a subfield of $\mathbf{f}_{\mathbf{p}} = O_F/\mathbf{p} \simeq \mathbb{F}_{p^f}$ then there is an injection

$$\mathcal{D}_{\mathbf{p}}/\mathcal{I}_{\mathbf{p}} \rightarrow \text{Gal}(\mathbf{f}/\mathbb{F}_p) = \langle \sigma_p \rangle$$

Since both groups have order f, the injection is an isomorphism and the quotient $\mathcal{D}_{\mathbf{p}}/\mathcal{I}_{\mathbf{p}}$ has a generator that maps to σ_p. Any representative of this generator in $\mathcal{D}_{\mathbf{p}}$ is called a *Frobenius element* of $\text{Gal}(F/\mathbb{Q})$ and denoted by $\text{Frob}_{\mathbf{p}}$. That is, $\text{Frob}_{\mathbf{p}}$ is any element of a particular coset $\sigma\mathcal{I}_{\mathbf{p}}$ in the subgroup $\mathcal{D}_{\mathbf{p}}$ of $\text{Gal}(F/\mathbb{Q})$. Its action on F, restricted to O_F, descends to the residue field $\mathbf{f}_{\mathbf{p}} = O_F/\mathbf{p}$, where it is the action of σ_p. If p is unramified the inertia group $\mathcal{I}_{\mathbf{p}}$ is trivial and $\text{Frob}_{\mathbf{p}}$ is unique.

Definition 4.1. Let $F/\mathbb{Q}$ be a Galois extension. Let p be a rational prime and let $\mathbf{p}$ be a maximal ideal of O_F lying over p. A **Frobenius element** of $\text{Gal}(F/\mathbb{Q})$ is any element $\mathrm{Frob}_{\mathbf{p}}$ satisfying the condition

$$x^{\mathrm{Frob}_{\mathbf{p}}} \equiv x^p \,(\mathrm{mod}\; p), \qquad \text{for all } p \in O_F$$

Thus $\mathrm{Frob}_{\mathbf{p}}$ acts on the residue field $\mathbf{f_p}$ as the Frobenius automorphism σ_p.

When the extension $F/\mathbb{Q}$ is Galois, the Galois group acts transitively on the maximal ideals lying over $\mathbf{p}$, i.e. given any two such ideals $\mathbf{p}$ and $\mathbf{p}'$ there is an automorphism $\sigma \in \mathrm{Gal}(F/\mathbb{Q})$ such that

$$p^{\sigma} = p'$$

The associated decomposition and inertia groups satisfy

$$\mathcal{D}_{\mathbf{p}^{\sigma}} = \sigma^{-1}\mathcal{D}_{\mathbf{p}}\sigma \quad \text{and} \quad \mathcal{I}_{\mathbf{p}^{\sigma}} = \sigma^{-1}\mathcal{I}_{\mathbf{p}}\sigma$$

and the relation between corresponding Frobenius element is

$$\mathrm{Frob}_{\mathbf{p}^{\sigma}} = \sigma^{-1}\mathrm{Frob}_{\mathbf{p}}\sigma$$

If p is unramified then this means that the conjugatate of a Frobenius is a Frobenius of the conjugate. And note that this relation shows that if the Galois group is abelian then $\mathrm{Frob}_{\mathbf{p}}$ for any $\mathbf{p}$ lying over p can be denoted by Frob_p.

We have the following theorem to be used later which is called **Tchebotarov Density Theorem, weak version**:

Theorem 4.2. *Let F be a Galois number fied. Then every element of Gal$(F/\mathbb{Q})$ takes the form Frob$_{\mathbf{p}}$ for infinitely many maximal ideals $\mathbf{p}$ of O_F.*

4.2 The ℓ-adic integers and the ℓ-adic numbers

In this section we introduce and give some basic facts about the ℓ-adic integers and the ℓ-adic numbers where ℓ is prime positive integer, without proofs. (For detailed information see: [K96])

For the rest of this chapter; let ℓ denote a prime number. Consider the affine algebraic curve over $\mathbb{Q}$:

$$C : xy = 1$$

The points of C are identified with the abelian group $\bar{\mathbb{Q}}^*$ via $(x, y) \mapsto x$, this implies C has an Abelian group structure. For each $n \in \mathbb{Z}^+$ the points of order ℓ^n form a subgroup $C[\ell^n]$. Since this is identified with the cyclic group $\mathbb{Z}/\ell^n\mathbb{Z}$, there is an isomorphism

$$C[\ell^n] \to \mathbb{Z}/\ell^n\mathbb{Z} \quad \text{given by } \mu_{\ell^n}^a \mapsto a$$

So there is an isomorphism

$$\mathrm{Aut}(C[\ell^n]) \to (\mathbb{Z}/\ell^n\mathbb{Z})^* \quad \text{given by } (\mu_{\ell^n} \mapsto \mu_{\ell^n}^m) \mapsto m$$

This isomorphism gives us the following isomorphism

$$\mathrm{Gal}(\mathbb{Q}(\mu_{\ell^n})/\mathbb{Q}) \to (\mathbb{Z}/\ell^n\mathbb{Z})^* \quad \text{given by } (\mu_{\ell^n} \mapsto \mu_{\ell^n}^m) \mapsto m$$

If we take the union of all number fields $\mathbb{Q}(\mu_{\ell^n})$ we get:

$$\mathbb{Q}(\mu_{\ell^\infty}) = \bigcup_{n=1}^{\infty} \mathbb{Q}(\mu_{\ell^n})$$

This is a subfield of $\bar{\mathbb{Q}}$ which has infinite degree over $\mathbb{Q}$. Set $G_{\mathbb{Q},\ell} = \mathrm{Aut}\mathbb{Q}(\mu_{\ell^\infty})$. Every element $\sigma \in G_{\mathbb{Q},\ell}$ restricts to $\sigma_n \in \mathrm{Gal}(\mathbb{Q}(\mu_{\ell^n})/\mathbb{Q})$ for each integer n. The restriction form a sequence $(\sigma_1, \sigma_2, \ldots, \sigma_n, \ldots)$ such that $\sigma_{n+1}\mid_{\mathbb{Q}(\mu_{\ell^n})} = \sigma_n$ for all n. Conversely, if $(\sigma_1, \sigma_2, \ldots)$ is such a compatible sequence, defining $\sigma \in \mathrm{Aut}(\mathbb{Q}(\mu_{\ell^\infty}))$ by $\sigma(x) = \sigma_n(x)$ if $x \in \mathbb{Q}(\mu_{\ell^n})$. By compability this definition is well-defined. Thus $G_{\mathbb{Q},\ell}$ can be viewed as a group of compatible sequences, where the group operation is componentwise composition. Each sequence acts componentwise on the group of compatible sequences of ℓ-power roots of unity.

The *ℓ-adic Tate module of C*,

$$\mathrm{Ta}_\ell(C) = \{(\mu_\ell^{a_1}, \mu_{\ell^2}^{a_2}, \mu_{\ell^3}^{a_3}, \ldots) : \mu_{\ell^n}^{a_{n+1}} = \mu_{\ell^n}^{a_n} \text{ for all } n\}$$

where the group operation is componentwise multiplication. $\mathrm{Ta}_\ell(C)$ is isomorphic to the abelian group of sequences

$$\{(a_1, a_2, a_3, \ldots) : a_n \in \mathbb{Z}/\ell^n\mathbb{Z} \text{ and } a_{n+1} \equiv a_n \pmod{\ell^n} \text{ for all } n\}$$

where the group operation is componentwise addition and $G_{\mathbb{Q},\ell}$ is isomorphic to the abelian group of sequences

$$\{(m_1, m_2, m_3, \ldots) : m_n \in (\mathbb{Z}/\ell^n\mathbb{Z})^* \text{ and } m_{n+1} \equiv m_n \pmod{\ell^n} \text{ for all } n\}$$

where the group operation is componentwise multiplication.

Definition 4.3. Let ℓ be a prime. An **ℓ-adic integer** is a sequence $\alpha = (a_1, a_2, a_3, \ldots)$ with $a_n \in \mathbb{Z}/\ell^n\mathbb{Z}$ and $a_{n+1} \equiv a_n \pmod{\ell^n\mathbb{Z}}$ for each $n \in \mathbb{Z}^+$. The ring of ℓ-adic integers, where the operations are componentwise addition and multiplication. It is denoted as $\mathbb{Z}_\ell$.

With this definition we see that each entry a_n in an ℓ-adic integer determines the preceding entries down to a_1, while the entry a_{n+1} to its right is one of its ℓ lifts from $\mathbb{Z}/\ell^n\mathbb{Z}$ to $\mathbb{Z}/\ell^{n+1}\mathbb{Z}$. This makes the ℓ-adic integer a special case of an algebraic construct called the *inverse limit*. In this case the inverse limit of the rings $\mathbb{Z}/\ell^n\mathbb{Z}$ for $n \in \mathbb{Z}^+$,

$$\mathbb{Z}_\ell = \varprojlim \{\mathbb{Z}/\ell^n\mathbb{Z}\}$$

The ring $\mathbb{Z}_\ell$ is an integral domain. The natural map

$$\mathbb{Z} \to \mathbb{Z}_\ell, \quad a \mapsto (a + \ell\mathbb{Z}, a + \ell^2\mathbb{Z}, a + \ell^3\mathbb{Z}, \ldots)$$

is a ring injection, so we may view $\mathbb{Z}$ as a subring of $\mathbb{Z}_\ell$. This maps induces a natural isomorphism

$$\mathbb{Z}/\ell\mathbb{Z} \to \mathbb{Z}_\ell/\ell\mathbb{Z}_\ell, \text{ given by } (a + \mathbb{Z}_\ell \mapsto a + \ell\mathbb{Z}_\ell)$$

so we may identify $\mathbb{Z}/\ell\mathbb{Z}$ and $\mathbb{Z}_\ell/\ell\mathbb{Z}_\ell$. As the inverse limit of a system of finite groups, $\mathbb{Z}_\ell$ is *profinite*.

The multiplicative group of units of $\mathbb{Z}_\ell$ is

$$\mathbb{Z}_\ell^* = \{(a_1, a_2, a_3, \ldots) \in \mathbb{Z}_\ell : a_n \in (\mathbb{Z}/\ell^n\mathbb{Z})^* \text{ for all } n\}$$

for given such a compatible sequence, the sequence of inverses modulo ℓ^n is again compatible. Every ℓ-adic integer α with $a_1 \neq 0$ in $\mathbb{Z}/\ell^n\mathbb{Z}$ is invertible.

The ideal $\ell\mathbb{Z}_\ell$ is the unique maximal ideal of $\mathbb{Z}_\ell$, and $\mathbb{Z}_\ell^* = \mathbb{Z}_\ell \setminus \ell\mathbb{Z}_\ell$. The ideal structure of $\mathbb{Z}_\ell$ is

$$\mathbb{Z}_\ell \supset \ell\mathbb{Z}_\ell \supset \ell^2\mathbb{Z}_\ell \supset \ldots \supset \ell^n\mathbb{Z}_\ell \supset \ldots$$

4.3 Galois Representations

The automorphism group of $\bar{\mathbb{Q}}$ form the *absolute Galois group* of $\mathbb{Q}$;

$$G_\mathbb{Q} = \mathrm{Aut}(\bar{\mathbb{Q}})$$

This section defines ℓ-adic Galois representations as homomorphisms from $G_{\mathbb{Q}}$ into ℓ-adic matrix groups.

As described in the previous section we may see $G_{\mathbb{Q}}$ as an inverse limit;

$$G_{\mathbb{Q}} = \varprojlim_{F}\{\mathrm{Gal}(F/\mathbb{Q})\}$$

Since these Galois groups are all finite, $G_{\mathbb{Q}}$ is a profinite group.

For each $\sigma \in G_{\mathbb{Q}}$ and each Galois number field F, define $U_{\sigma}(F) = \sigma.\mathrm{ker}(G_{\mathbb{Q}} \to \mathrm{Gal}(F/\mathbb{Q}))$. The topology on $G_{\mathbb{Q}}$ which has the basis

$$\{U_{\sigma}(F) : \sigma \in G_{\mathbb{Q}}, F \text{ is a Galois number field}\}$$

is called the *Krull topology*, so that every $U(F)$ is an open normal subgroup of $G_{\mathbb{Q}}$ and it is a fact that every open normal subgroup of $G_{\mathbb{Q}}$ takes the form $U(F)$ for some Galois number field F and as the inverse limit of finite groups, the topological group $G_{\mathbb{Q}}$ is compact.

Complex conjugation is an element of $G_{\mathbb{Q}}$. For a family of elements, let $p \in \mathbb{Z}$ be a prime and let $\mathbf{p} \subset \bar{\mathbb{Z}}$ be any maximal ideal over p. The decomposition group of $\mathbf{p}$ is

$$\mathcal{D}_{\mathbf{p}} = \{\sigma \in G_{\mathbb{Q}} : \mathbf{p}^{\sigma} = \mathbf{p}\}$$

Thus each $\sigma \in \mathcal{D}_{\mathbf{p}}$ acts on $\bar{\mathbb{Z}}/\mathbf{p}$ as $(x + \mathbf{p})^{\sigma} = x^{\sigma} + \mathbf{p}$ so that this can be viewed as an action of $\bar{\mathbb{F}}_p$. If we set $G_{\mathbb{F}_p}$ as the absolute Galois group $\mathrm{Aut}(\bar{\mathbb{F}}_p)$ of $\mathbb{F}_p$. The reduction map $\mathcal{D}_{\mathbf{p}} \to G_{\mathbb{F}_p}$ is surjective. An *absolute Frobenius element over p* is any preimage $\mathrm{Frob}_{\mathbf{p}} \in \mathcal{D}_{\mathbf{p}}$ of the Frobenius automorphism $\sigma_p \in G_{\mathbb{F}_p}$. Thus $\mathrm{Frob}_{\mathbf{p}}$ is defined only up to the kernel of the reduction map, the *inertia group* of $\mathbf{p}$;

$$\mathcal{I}_{\mathbf{p}} = \{\sigma \in \mathcal{D}_{\mathbf{p}} : x^{\sigma} \equiv x \pmod{\mathbf{p}} \text{ for all} x \in \bar{\mathbb{Z}}\}$$

For each Galois number field F the restriction map $G_{\mathbb{Q}} \to \mathrm{Gal}(F/\mathbb{Q})$ takes an absolute Frobenius element to a corresponding Frobenius element for F,

$$\mathrm{Frob}_{\mathbf{p}}|_F = \mathrm{Frob}_{\mathbf{p}\cap F}$$

All maximal ideals of $\bar{\mathbb{Z}}$ over p are conjugate to $\mathbf{p}$ and the definition of $\mathrm{Frob}_{\mathbf{p}}$ shows that analously before

$$\mathrm{Frob}_{\mathbf{p}^{\sigma}} = \sigma^{-1}\mathrm{Frob}_{\mathbf{p}}\sigma, \quad \sigma \in G_{\mathbb{Q}}$$

Theorem 4.4. *For each maximal ideal* $\mathbf{p}$ *of* $\bar{\mathbb{Z}}$ *lying over any but finite set of rational primes* p*, chose an absolute Frobenius element* $Frob_{\mathbf{p}}$*. The set of such elements form a dense subset of* $G_{\mathbb{Q}}$*.*

Proof. Let $U = U_\sigma(F)$ be any basis element of the Krull topology on $G_{\mathbb{Q}}$. It suffices to show that there exists $\mathrm{Frob}_{\mathbf{p}} \in U$. By the remarks above $\sigma|_F \in \mathrm{Gal}(F/\mathbb{Q})$ takes the form $\mathrm{Frob}_{\mathbf{p}_F}$ for some maximal ideal $\mathbf{p}_F \in O_F$. Lifting $\mathbf{p}_F$ to a maximal ideal $\mathbf{p}$ of $\bar{\mathbb{Z}}$, we get $\mathbf{p} \cap F = \mathbf{p}_F$. Thus $\mathrm{Frob}_{\mathbf{p}}|_F = \mathrm{Frob}_{\mathbf{p}_F} = \sigma|_F$. Hence $\mathrm{Frob}_{\mathbf{p}}.\sigma^{-1} \in \ker(G_{\mathbb{Q}} \to \mathrm{Gal}(F/\mathbb{Q}))$ and this implies that $\mathrm{Frob}_{\mathbf{p}} \in U_\sigma(F)$. □

Definition 4.5. Let d be a positive integer. A *d-dimensional ℓ-adic Galois representation* is a continuous homomorphism

$$\rho : \Gamma_{\mathbb{Q}} \to \mathrm{GL}_d(L)$$

where L is a finite extension field of $\mathbb{Q}_\ell$. If $\rho' : G_{\mathbb{Q}} \to \mathrm{GL}_d(L)$ is another such representation and there is a matrix $m \in \mathrm{GL}_d(L)$ such that $\rho'(\sigma) = m^{-1}\rho(\sigma)m$ for all $\sigma \in G_{\mathbb{Q}}$ then ρ and ρ' are equivalent. This equivalence is denoted as $\rho \sim \rho'$.

Given a Galois representation ρ we want to know the values $\rho(\sigma)$ for $\sigma \in G_{\mathbb{Q}}$. Especially at absolute Frobenius elements $\mathrm{Frob}_{\mathbf{p}}$. $\mathrm{Frob}_{\mathbf{p}}$ is defined up to the inertia group $\mathcal{I}_{\mathbf{p}}$ and so $\rho(\mathrm{Frob}_{\mathbf{p}})$ is well-defined if and only if $\mathcal{I}_p \subset \ker\rho$. Let $\mathbf{p}$ and $\mathbf{p}'$ be two maximal ideals lying over the same prime p. Then we have seen that $\mathcal{I}_{\mathbf{p}'} = \tau^{-1}\mathcal{I}_{\mathbf{p}}\tau$ for some $\tau \in G_{\mathbb{Q}}$. Since $\ker\rho \trianglelefteq G_{\mathbb{Q}}$, the condition $\mathcal{I}_{\mathbf{p}} \subset \ker\rho$ depends only on the underlying prime p. Let ρ and ρ' be two representations such that $\rho \sim \rho'$. Then $\ker\rho = \ker\rho'$ hence the condition $\mathcal{I}_{\mathbf{p}} \subset \ker$ makes sense for an equivalence class of representations. Now $\rho(\mathrm{Frob}_{\mathbf{p}})$ depends on the choice of $\mathbf{p}$. Since every conjugate of $\rho(\mathrm{Frob}_{\mathbf{p}})$ has the same characteristic polynomial as $\rho(\mathrm{Frob}_{\mathbf{p}})$ and $\mathrm{Frob}_{\mathbf{p}^\sigma} = \sigma^{-1}\mathrm{Frob}_{\mathbf{p}}\sigma$, the characteristic polynomial depends only on p.

Definition 4.6. Let ρ be a Galois representation and p be a prime. Then ρ is *unramified at p* if $\mathcal{I}_{\mathbf{p}} \subset \ker\rho$ for any maximal ideal $\mathbf{p} \subset \bar{\mathbb{Z}}$ lying over p.

Definition 4.7. Let d be a positive integer. A *d-dimensional l-adic Galois representation* is a d-dimensional topological vector space V over L, where L is a finite extension field of $\mathbb{Q}_\ell$, that is also a $G_{\mathbb{Q}}$-module such that the action

$$V \times G_{\mathbb{Q}} \to V, \qquad (v, \sigma) \mapsto v^\sigma$$

is continuos. If V' is such an another representation and there is a continuos $G_{\mathbb{Q}}$-module isomorphism of L-vector spaces $V \longrightarrow V'$ then V and V' are *equivalent*.

Proposition 4.8. *Let $\rho : G_{\mathbb{Q}} \longrightarrow GL_d(L)$ be a Galois representation. Then ρ is similar to a Galois representation $\rho' : G_{\mathbb{Q}} \rightarrow GL_d(O_L)$*

Proof. Set $V = L^d$ and $\Lambda = O_L^d$. Then we have Λ as a lattice of V, hence a finitely generated $\mathbb{Z}_\ell$-module, hence compact. Since $G_{\mathbb{Q}}$ is also compact, we have the image Λ' of $\Lambda \times G_{\mathbb{Q}}$ under the map $V \times G_{\mathbb{Q}} \rightarrow V$ is also compact. Thus the image lies in $\lambda^{-r}\Lambda$ for some $r \in \mathbb{Z}^+$. The image is finitely generated, it contains Λ so its rank is at least d. It is taken to itself by $G_{\mathbb{Q}}$. These remarks combine to show that O_L-basis of Λ' gives the desired ρ'. □

4.4 Galois Representations and Elliptic Curves

This section aims is to construct two dimensional Galois representations attached to elliptic curves. We begin with some facts about elliptic curves.

Let $\mathbf{k}$ be a field of characteristic zero. Every field has an algebraic closure and any two algebraic closures of a field are isomorphic.

A *Weierstrass equation* over $\mathbf{k}$ is any cubic equation of the form

$$E : y^2 = 4x^3 - g_2x^2 - g_3, \qquad g_2, g_3 \in \mathbf{k}$$

We define the *discriminant* of this equation to be

$$\Delta = g_2^3 - 27g_3^2 \in \mathbf{k}$$

Definition 4.9. Let $\bar{\mathbf{k}}$ be the algebraic closure of the field $\mathbf{k}$. When a Weierstrass equation E has nonzero discriminant Δ it is called *nonsingular* and the set

$$\varepsilon = \{(x, y) \in \bar{\mathbf{k}} \text{ satisfying } E(x, y)\} \cup \{\infty\}$$

is called an *elliptic curve over* $\mathbf{k}$.

Now, let E be an elliptic curve over $\mathbb{Q}$ and let ℓ be a prime. Multiplication by ℓ between ℓ-power torsion subgroups of E gives the maps

$$E[\ell] \longleftarrow E[\ell^2] \longleftarrow E[\ell^3] \longleftarrow \dots$$

The ℓ-adic Tate module of E is

$$\mathrm{Ta}_\ell(E) = \varprojlim_n E[\ell^n]$$

Choose a basis (P_n, Q_n) of $E[\ell^n]$ for each $n \in \mathbb{Z}^+$ such that $[\ell]P_{n+1} = P_n$ and $[\ell]Q_{n+1} = Q_n$. Each basis gives an isomorphism $E[l^n] \to (\mathbb{Z}/\ell^n\mathbb{Z})^2$ and since the basis are compatible with the transition maps we can pass to the limit which gives $\mathrm{Ta}_\ell(E) \simeq \mathbb{Z}_\ell^2$. Note that for each n, $\mathbb{Q}(E[\ell^n])$ is a Galois number field. Hence we have a restriction map

$$G_\mathbb{Q} \to \mathrm{Gal}(\mathbb{Q}(E[\ell^n])/\mathbb{Q})$$

and we also have an injection $\mathrm{Gal}(\mathbb{Q}(E[\ell^n]/\mathbb{Q}) \to \mathrm{Aut}(E[\ell^n])$ Composing these maps gives

$$G_\mathbb{Q} \to \mathrm{Aut}(E[\ell^n]) \quad \text{for each } n$$

For each n, consider the following commutative diagram;

$$\begin{tikzcd}
G_\mathbb{Q} \arrow[d] \arrow[dr] & \\
\mathrm{Aut}(E[\ell^n]) & \mathrm{Aut}(E[\ell^{n+1}]) \arrow[l]
\end{tikzcd}$$

This shows that $G_\mathbb{Q}$ acts on the Tate module of E and so $\mathrm{Ta}_\ell(E)$ is a $G_\mathbb{Q}$-module. Each basis (P_n, Q_n) determines an isomorphism $\mathrm{Aut}(E[\ell^n]) \to \mathrm{GL}_2(\mathbb{Z}/\ell^n\mathbb{Z})$ and by the choice of the basis the following diagram commutes for all n,

$$\begin{tikzcd}
\mathrm{Aut}(E[\ell^n]) \arrow[r] \arrow[d] & \mathrm{GL}_2(\mathbb{Z}/\ell^n\mathbb{Z}) \arrow[d] \\
\mathrm{Aut}(E[\ell^{n+1}]) \arrow[r] & \mathrm{GL}_2(\mathbb{Z}/\ell^{n+1}\mathbb{Z})
\end{tikzcd}$$

Thus we have $\mathrm{Aut}(\mathrm{Ta}_\ell(E)) \simeq \mathrm{GL}_2(\mathbb{Z}/\ell^n\mathbb{Z})$. Combining this isomorphism with the action of $G_\mathbb{Q}$ on $\mathrm{Ta}_\ell(E)$ we get a homomorphism $\rho_{E,\ell} : G_\mathbb{Q} \to \mathrm{GL}_2(\mathbb{Z}_\ell) \subset \mathrm{GL}_2(\mathbb{Q}_\ell)$.

Let us see that this is a continuos homomorphism. It suffices to check that $\rho_{E,\ell}^{-1}(U(n))$ is open for each n where $U(n) = \ker(\mathrm{GL}_2(\mathbb{Z}_\ell)) \to \mathrm{GL}_2(\mathbb{Z}/\ell^n\mathbb{Z})$. Now we have;

$$\begin{aligned}\sigma \in \rho_{E,\ell}^{-1}(U(n)) &\Leftrightarrow \rho_{E,\ell}(\sigma) \in U(n)\\ &\Leftrightarrow (P_n^\sigma, Q_n^\sigma) = (P_n, Q_n)\\ &\Leftrightarrow \sigma|_{\mathbb{Q}(E[\ell^n])} = \mathrm{id}\\ &\Leftrightarrow \sigma \in \ker(G_\mathbb{Q} \to \mathrm{Gal}(\mathbb{Q}(E[\ell^n]))/\mathbb{Q})\\ &\Leftrightarrow \sigma \in U(\mathbb{Q}(E[\ell^n]))\end{aligned}$$

Hence, $\rho_{E,\ell}^{-1}(U(n)) = U(\mathbb{Q}(E[\ell^n]))$ and so it is open for all n. $\rho_{E,\ell}$ is the 2-dimensional Galois representation attached to E.

Theorem 4.10. *Let ℓ be a prime and E be an elliptic curve over $\mathbb{Q}$ with conductor N. The Galois representation $\rho_{E,\ell}$ is unramified at every prime $p \nmid \ell N$. For any such p, let $\mathbf{p} \subset \bar{\mathbb{Z}}$ be any maximal ideal over p. Then the characteristic equation of $\rho_{E,\ell}(Frob_\mathbf{p})$ is*

$$x^2 - a_p(E)x + p = 0$$

where $a_p(E) = p + 1 - |E(\mathbb{F}_p)|$.

Proof. (See [DS05], Theorem 9.4.1) □

It is also true that $\rho_{E,\ell}$ is an irreducible representation but this will not be proven here. Galois representations attached to isogenous elliptic curves E and E' are equivalent. To see this, $\varphi : E \to E'$ be an isogeny. Then φ induces a map between Tate modules and so we have a map $V_\ell(E) \to V_\ell(E')$. Similarly, the dual isogeny also gives a map $V_\ell(E') \to V_\ell(E)$ and the composition is multiplication by $\deg(\varphi)$ which is an automorphism as $V_\ell(E)$ and $V_\ell(E')$ are vector spaces over $\mathbb{Q}_\ell$ and $\mathbb{Q}_\ell$ has characteristic zero.

4.5 Galois Representations and Modular Forms

This section associates Galois representations to modular curves and then decomposes them into representations attached to modular forms.

Let N be a positive integer and ℓ be a prime. $X_1(N)$ is a projective nonsingular algebraic curve over $\mathbb{Q}$. Let g be the genus of $X_1(N)$. The Jacobian of the complex curve $X_1(N)$ is

$$J_1(N) = \mathrm{Jac}(X_1(N)_\mathbb{C}) = \mathcal{S}_k(\Gamma_1(N))^\wedge / H_1(X_1(N)_\mathbb{C}, \mathbb{Z}) \simeq \mathbb{C}^g/\Lambda^g$$

The Picard group of the modular curve is the abelian group of the divisor classes on the points of $X_1(N)$;

$$\mathrm{Pic}^0(X_1(N)) = \mathrm{Div}^0(X_1(N))/\mathrm{Div}^\ell(X_1(N))$$

$\mathrm{Pic}^0(X_1(N))$ can be identified with a subgroup of the complex Picard group $\mathrm{Pic}^0(X_1(N)_\mathbb{C})$ which is isomorphic to the Jacobian by Abel's Theorem (See:[FK80]) Thus there is an inclusion of ℓ^n-torsion;

$$i_n : \mathrm{Pic}^0(X_1(N))[\ell^n] \to \mathrm{Pic}^0(X_1(N)_\mathbb{C})[\ell^n] \simeq (\mathbb{Z}/\ell^n\mathbb{Z})^{2g}$$

We have a surjective reduction map $\mathrm{Pic}^0(X_1(N)) \to \mathrm{Pic}^0(\tilde{X}_1(N))$. Restricting it to ℓ^n-torsion;

$$\pi_n : \mathrm{Pic}^0(X_1(N))[\ell^n] \to \mathrm{Pic}^0(\tilde{X}_1(N))[\ell^n]$$

Note that if a curve C over a field $\mathbf{k}$ has genus g and N is coprime to char($\mathbf{k}$) then $\mathrm{Pic}^0(C)[N] \simeq (\mathbb{Z}/N\mathbb{Z})^{2g}$ and if C is a curve over $\mathbb{Q}$ has a good reduction at prime $p \nmid N$ then the reduction map is injective on $\mathrm{Pic}^0(C)[N]$. Hence i_n and π_n are actually isomorphism for $p \nmid \ell N$.

The ℓ-adic Tate module of $X_1(N)$ is ;

$$\mathrm{Ta}(\mathrm{Pic}^0(X_1(N))) = \varprojlim_n \mathrm{Pic}^0(X_1(N))[\ell^n]$$

Choosing a compatible family of basis of $\mathrm{Pic}^0(X_1(N))[\ell^n]$, for all n, we have

$$\mathrm{Ta}(\mathrm{Pic}^0(X_1(N))) \simeq \mathbb{Z}_\ell^{2g}$$

.

$G_\mathbb{Q}$ acts on $\mathrm{Div}^0(X_1(N))$ as

$$\left(\sum n_p(P)\right)^\sigma = \sum n_p(P^\sigma), \quad \text{for } \sigma \in G_\mathbb{Q}$$

and this action descends to $\mathrm{Pic}^0(X_1(N))$,

$$\mathrm{Pic}^0(X_1(N)) \times G_\mathbb{Q} \to \mathrm{Pic}^0(X_1(N))$$

The field extension $\mathbb{Q}(\mathrm{Pic}^0(X_1(N))[\ell^n])/\mathbb{Q}$ is Galois for each $n \in \mathbb{Z}^+$, so the action restricts to $\mathrm{Pic}^0(X_1(N))[\ell^n]$. For each n there is a commutative diagram;

$$\begin{tikzcd}
G_{\mathbb{Q}} \arrow[d] \arrow[dr] & \\
\mathrm{Aut}(\mathrm{Pic}^0(X_1(N))[\ell^n]) & \mathrm{Aut}(\mathrm{Pic}^0(X_1(N))[\ell^{n+1}]) \arrow[l]
\end{tikzcd}$$

Thus $G_{\mathbb{Q}}$ acts on $\mathrm{Ta}_\ell(\mathrm{Pic}^0(X_1(N)))$ and gives us the representation

$$\rho_{X_1(N),\ell} : G_{\mathbb{Q}} \to \mathrm{Aut}(\mathrm{Ta}(\mathrm{Pic}^0(X_1(N))) \simeq \mathrm{Gl}_{2g}(\mathbb{Z}_\ell) \subset \mathrm{Gl}_{2g}(\mathbb{Q}_\ell)$$

This is the $2g$-dimensional Galois representation associated to $X_1(N)$

Theorem 4.11. *Let ℓ be a prime and let N be a positive integer. The Galois representation $\rho_{X_1(N),\ell}$ is unramified at every prime $p \nmid \ell N$. For any such p, let $\mathbf{p} \subset \bar{\mathbb{Z}}$ be any maximal ideal over p. Then $\rho_{X_1(N),\ell}(Frob_{\mathbf{p}})$ satisfies the polynomial equation*

$$x^2 - T_p x + \langle p \rangle p = 0$$

Proof. Let $p \nmid \ell N$ and $\mathbf{p}$ lies over p. We have the following commutative diagram;

$$\begin{tikzcd}
\mathcal{D}_p \arrow[r] \arrow[d] & \mathrm{Aut}(\mathrm{Pic}^0(X_1(N))[\ell^n]) \arrow[d] \\
G_{\mathbb{F}_p} \arrow[r] & \mathrm{Aut}(\mathrm{Pic}^0(\tilde{X}_1(N))[\ell^n])
\end{tikzcd}$$

The map on the right side is the isomorphism induced by π_n from the beginning of the section. As we seen before; $\mathcal{I}_p \subset \ker\rho_{X_1(N),\ell}$

Now for the second part, using the Euler-Schimura relation (see [DS05] Chapter 8 for details), we have the restrictions to ℓ^n-torsion and it gives the following commutative diagram;

$$\begin{tikzcd}
\mathrm{Pic}^0(X_1(N))[\ell^n] \arrow[r, "T_p"] \arrow[d] & \mathrm{Pic}^0(X_1(N))[\ell^n] \arrow[d] \\
\mathrm{Pic}^0(\tilde{X}_1(N))[\ell^n] \arrow[r, "\sigma_{p,*}+\langle \tilde{p} \rangle_* \sigma_p^*"] & \mathrm{Pic}^0(\tilde{X}_1(N))[\ell^n]
\end{tikzcd}$$

We also have the following commutative diagram;

$$\begin{tikzcd}
\mathrm{Pic}^0(X_1(N))[\ell^n] \arrow[r, "\mathrm{Frob}_{\mathbf{p}}+\langle p\rangle p\mathrm{Frob}_{\mathbf{p}}^{-1}"] \arrow[d] & \mathrm{Pic}^0(X_1(N))[\ell^n] \arrow[d] \\
\mathrm{Pic}^0(\tilde{X}_1(N))[\ell^n] \arrow[r, "\sigma_{p,*}+\langle\tilde{p}\rangle_*\sigma_p^*"] & \mathrm{Pic}^0(\tilde{X}_1(N))[\ell^n]
\end{tikzcd}$$

Since the vertical arrows are isomorphisms, $T_p = \mathrm{Frob}_{\mathbf{p}} + \langle p\rangle p\mathrm{Frob}_{\mathbf{p}}^{-1}$ on $\mathrm{Pic}^0(X_1(N))[\ell^n]$. This holds for all n, so the equality extends to $\mathrm{Ta}_\ell(\mathrm{Pic}^0(\tilde{X}_1(N))[\ell^n])$ and the result follows.

□

4.6 Galois Representations and Modularity

This last section states the Modularity Theorem in terms of Galois representations.

Definition 4.12. An irreducible Galois representation

$$\rho : G_{\mathbb{Q}} \to \mathrm{GL}_2(\mathbb{Q}_\ell)$$

such that $\det\rho$ is modular if there exists a newform $f \in \mathcal{S}_2(\Gamma_0(M_f))$ such that $\mathbf{K}_{f,\lambda} = \mathbb{Q}_\ell$ for some maximal ideal λ of O_{K_f} lying over ℓ and such that $\rho_{f,\lambda} \sim \rho$.

In particular, if E is an elliptic curve over $\mathbb{Q}$ and ℓ is prime then the Galois representation $\rho_{E,\ell}$ is a candidate to be modular.

Theorem 4.13. Modularity Theorem *Let E be an elliptic curve over $\mathbb{Q}$. Then $\rho_{E,\ell}$ is modular for some ℓ.*

This is the version that was proved, for semistable curves in [W95] and [TW95] and then for all curves in [BCDT01].

Theorem 4.14. Modularity Theorem, strong version *Let E be an elliptic curve over $\mathbb{Q}$ with conductor N. Then for some newform $f \in \mathcal{S}_2(\Gamma_0(N))$ with number field $\mathbf{K}_f = \mathbb{Q}$,*

$$\rho_{f,\ell} = \rho_{E,\ell} \quad \textit{for all } \ell$$

Proposition 4.15. *Let E be an elliptic curve over $\mathbb{Q}$. Then if $\rho_{E,\ell}$ is modular for some ℓ, then $\rho_{E,\ell}$ is modular for all ℓ.*

Proof. Since $\rho_{E,\ell}$ is modular, there exists a newform $f \in \mathcal{S}_2(\Gamma_0(M_f))$ such that $K_{f,\lambda} = \mathbb{Q}_\ell$ for some maximal ideal λ lying over ℓ and $\rho_{f,\lambda} \sim \rho_{E,\ell}$. Using the characteristic polynomials of $\rho_{f,\lambda}(\mathrm{Frob}_{\mathbf{p}})$ and $\rho_{E,\ell}(\mathrm{Frob}_{\mathbf{p}})$ we get; $a_p(f) = a_p(E)$ for almost all p. Now, since $K_f = \mathbb{Q}$ the Galois representation associated to f takes the form $\rho_{f,\ell} : G_{\mathbb{Q}} \to \mathrm{GL}_2^+(\mathbb{Q})_2(\mathbb{Q}_\ell)$ for all ℓ. Thus, $\rho_{E,\ell} \sim \rho_{f,\ell}$ for all ℓ and hence $\rho_{E,\ell}$ is modular for all ℓ. □

Remark 4.16. Modulo ℓ representations are essential for the proof of the Modularity Theorem. Let $f \in \mathcal{S}_2(\Gamma_1(M_f))$ be a newform and $\lambda \subset \mathcal{O}_{K_f}$ be a maximal ideal lying over ℓ. We may assume that $\rho_{f,\lambda} : G_{\mathbb{Q}} \to \mathrm{GL}_2^+(\mathbb{Q})_2(\mathcal{O}_{K_f}, \lambda)$, so that $\rho_{f,\lambda}$ has a good ℓ reduction

$$\bar{\rho}_{f,\lambda} : G_{\mathbb{Q}} \to \mathrm{GL}_2^+(\mathbb{Q})_2(\mathcal{O}_{K_f,\lambda})/\lambda\mathcal{O}_{K_f,\lambda}$$

Bibliography

[A90] Tom M. Apostol, Modular Functions and Dirichlet Series in Number Theory, Springer, 1990

[BCDT01] C. Breuil, B. Conrad, F. Diamond, R. Taylor - On The Modularity of Elliptic Curves over $\mathbb{Q}$: wild 3-adic exercises. Journal of American Mathematical Society 14(4):843-939, 2001

[CR01] Brian David Conrad, Karl Rubin - Aritmetic Algebraic Geometry, American Mathematical Society, 2001

[DS05] Fred Diamond, Jerry Shurman - A First In Modular Forms, Springer, 2005.

[FK80] Hershel M. Farkas, Irwin Kra - Riemann Surfaces, Graduate Texts in Mathematics 71, Springer-Verlag, 1980.

[Gou] Fernando Q. Gouvea - Deformations of Galois Representations, Arithmetic Algebraic Geometry (IAS Park City Mathematics)

[H01] Allen Hatcher - Algebraic Topology, 2001

[H83] Robin Hartshorne - Algebraic Geometry, Springer, 1983

[J96] Gerald J. Janusz -Algebraic Number Fields, American Mathematical Society,1996

[JS87] Gareth A. Jones, David Singerman - Complex Functions, an Algebraic and Geometric Viewpoint, Cambridge University Press, 1987

[K89] Erwin Kreyszig - Introductory Functional Analysis with Applications, 1989

[K93] Neal I. Koblitz - Introduction to Elliptic Curves and Modular Forms, Springer, 1993

[K96] Neal Koblitz - *p*-adic Numbers, *p*-adic Analysis and Zeta Functions, Springer, 1996

[L00] Serge Lang - Algebraic Number Theory, Springer, 2000.

[M76] Toshitsune Miyake - Modular Forms, Springer, 1976

[M95] Rick Miranda - Algebraic Curves and Riemann Surfaces, American Mathematical Society, 1995.

[S96] Jean Pierre Serre - A Course In Arithmetic, 1996

[S09] Joseph H. Silverman - Arithmetic of Elliptic Curves, Springer, 2009

[TW95] Richard Taylor, Andrew Wiles - Ring Theoretic Properties of certain Hecke Algebras. Ann. of Math. 141(3): 553-572, 1995

[W95] Andrew Wiles - Modular Elliptic Curves and Fermat's Last Theorem. Ann. of Math. 141(3): 443-551, 1995

[W67] Andr Weil - Über die Bestimmung Dirichletscher Reihen durch Funktionalgeichungen, Math Annalen, 168:149-156, 1967