# MODULAR FORMS AND GALOIS REPRESENTATIONS

by

Cihan SOYLU

A Thesis Submitted to the

Graduate School of Sciences and Engineering

in Partial Fulfillment of the Requirements for

the Degree of Master of Science

in Mathematics

Koç University

June 2012

Koç University

Graduate School of Sciences and Engineering

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

by

Cihan Soylu

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.

Thesis Committee Members:

Asst. Prof. Kazım Büyükboduk (Advisor) ......................................

Assoc. Prof. Sinan Ünver .................................................................

Prof. K. İlhan İkeda ........................................................................

Date: 12 June 2012

# ABSTRACT

This study aims at explaining the Modularity Theorem which states that every rational elliptic curve arises from modular forms.

First we introduce modular forms, complex elliptic curves and modular curves, and study these objects. More precisely, we see how modular curves parametrize the complex elliptic curves and torsion data as solutions of a moduli problem, and there is a correspondence between the functions on the moduli spaces satisfying certain conditions and the modular forms.

Then we define the Hecke operators acting on the space of modular forms and using them construct a canonical basis, consisting of newforms, of the space of cusp forms, and give the duality between the Hecke algebra and the space of modular forms.

We, then, give the definition of the Jacobian of a modular curve and prove that Fourier coefficients of weight 2 eigenforms of the Hecke operators are algebraic integers and conjugate of a weight 2 normalized eigenform is also a normalized eigenform. Then we define the Abelian variety that comes from a weight 2 eigenform. After that we study the algebraic model of modular curves and give the Eichler-Shimura relation.

Finally, we construct the Galois representations attached to an elliptic curve and a normalized eigenform $f \in S_2(N, \chi)$. Then we give a very brief skecth of Wiles's proof of the Modularity theorem and study the relation of Modularity theorem with the Fermat's last theorem.

# ÖZET

Bu çalışmada, rasyonel eliptik eğrilerin modüler formlardan geldiğini söyleyen modülerlik teoremini anlamaya calıştık.

İlk olarak modüler formlar, kompleks eliptik eğriler ve modüler eğriler arasindaki ilişkileri inceledik ve modüler eğrilerin kompleks elliptik eğrileri nasıl parametrize ettiğini gösterdik. Daha sonra modüler form uzayına etki eden Hecke operatörlerini tanimladık ve cusp form uzayı için bir baz elde ettik. Ayrıca modüler eğrilerin Jakobiyanlarını kullanarak Hecke operatörlerinin özvektörlerinin Fourier katsayılarının cebirsel sayılar olduğunu gösterdik. Sonrasında modüler eğrilerin rasyoneller üzerindeki modelini ve Eichler-Shimura ilişkisini inceledik.

Son olarak eliptik eğrilere ve modüler formlara ilişkilendirilen Galois temsillerini inşa ettik ve modülerlik teoreminin ispatında kullanılan metodun kısa bir özetini verdik. Ayrıca modülerlik teoremi ve Fermat'ın son teoremi arasındaki ilişkiyi inceledik.

# ACKNOWLEDGEMENTS

I want to thank to my advisor Prof. Kazım Büyükboduk for his supports and guidance during my studies. I would like to thank to Altan Erdoğan for helpful conversations. I want to thank TUBİTAK for their financial support.

# Contents

# 1 Introduction

In this chapter we give definitions of modular forms, complex elliptic curves and modular curves. Then we analyze the relations between these objects.

## 1.1 Definitions

We start with the definition of the modular group, the group of 2-by-2 matrices with integer entries and determinant 1;

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

Modular group acts on the Riemann sphere $\widehat{\mathbb{C}} = \mathbb{C} \cup \{\infty\}$ via fractional linear transformations

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix}(\tau) = \frac{a\tau + b}{c\tau + d}, \qquad \tau \in \widehat{\mathbb{C}}.$$

This means that if $\gamma = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right)$ and $c \neq 0$ then $\gamma(-d/c) = \infty$ and $\gamma(\infty) = a/c$; if $c = 0$ then $\gamma(\infty) = \infty$. Note that $-\gamma$ gives the same transformation as $\gamma$. Modular group is generated by the following elements

$$\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \text{ and } \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$$

[**?**, Theorem 2.1]. Hence the transformation group on $\widehat{\mathbb{C}}$ defined by the modular group is generated by the transformations,

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

The upper half plane will be denoted by $\mathcal{H} = \{\tau \in \mathbb{C} : \mathrm{Im}(\tau) > 0\}$. It is easy to see that

$$\mathrm{Im}(\gamma(\tau)) = \frac{\mathrm{Im}(\tau)}{|c\tau + d|^2}, \qquad \gamma = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \mathrm{SL}_2(\mathbb{Z}).$$

Hence modular group maps $\mathcal{H}$ to itself. It is also easy to see that $(\gamma\gamma')(\tau) = \gamma(\gamma'(\tau))$ for all $\gamma, \gamma' \in \mathrm{SL}_2(\mathbb{Z})$. Thus $\mathrm{SL}_2(\mathbb{Z})$ acts on $\mathcal{H}$.

**Definition 1.1.1.** *Let $k$ be an integer. A meromorphic function $f : \mathcal{H} \to \mathbb{C}$ is weakly modular of weight $k$ if*

$$f(\gamma(\tau)) = (c\tau + d)^k f(\tau)$$

*for $\gamma = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \mathrm{SL}_2(\mathbb{Z})$ and $\tau \in \mathcal{H}$.*

In the above definition $\gamma = -I$ gives $f = (-1)^k f$, hence the only weakly modular function of odd weight is zero. Also multiplying weakly modular functions of even weights $m$ and $n$ gives a weakly modular function of weight $m + n$. Since the factor $(c\tau + d)^k$ has neither pole nor zeros on $\mathcal{H}$, $f(\tau)$ and $f(\gamma(\tau))$ has the same zeros and poles.

**Definition 1.1.2.** *Let $k$ be an integer. A function $f : \mathcal{H} \to \mathbb{C}$ is a modular form of weight $k$ if*

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

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

Let us explain what does it mean being holomorphic at $\infty$. Consider the holomorphic map $\tau \mapsto q = e^{2\pi i \tau}$. This map takes $\mathcal{H}$ to open punctured unit disk $D$. Now let $g : D \to \mathbb{C}$ be the function defined by $g(q) = f(\log(q)/(2\pi i))$. $g$ is well defined as being weakly modular $f$ is $\mathbb{Z}$-periodic. Since $f$ is holomorphic on $\mathcal{H}$, $g$ is holomorphic on $D$. Thus $g$ has a Laurent series expansion $g(q) = \sum_{n \in \mathbb{Z}} a_n q^n$ for

$q \in D$. Define $f$ to be holomorphic at $\infty$ if $g$ extends holomorphically to $q = 0$, that is, if $f$ has a Fourier expansion

$$f(\tau) = \sum_{n=0}^{\infty} a_n(f) q^n, \qquad q = e^{2\pi i \tau}.$$

Since $q \to 0$ if and only if $\mathrm{Im}(\tau) \to \infty$, in order to show that $f$ is holomorphic at $\infty$ it suffices to show that $f(\tau)$ is bounded as $\mathrm{Im}(\tau) \to \infty$.

It is easy to see that $\mathcal{M}_k(\mathrm{SL}_2(\mathbb{Z}))$ is a vector space over $\mathbb{C}$. Now we give some examples of modular forms. The trivial example is the zero function on $\mathcal{H}$ which is a modular form of every weight. A nontrivial example is Eisenstein series. Let $k > 2$ be an even integer and define the Eisenstein series of weight $k$

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

where primed summation sign means to sum over nonzero integer pairs $(c, d) \in \mathbb{Z}^2 - \{(0,0)\}$. The sum is absolutely convergent and converges uniformly on compact subsets of $\mathcal{H}$ [?], so $G_k$ is holomorphic on $\mathcal{H}$. For any $\gamma = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \mathrm{SL}_2(\mathbb{Z})$, it is easy to see that $G_k(\gamma(\tau)) = (c\tau + d)^k G_k(\tau)$ so $G_k$ is weakly modular of weight $k$. We also need to check that $G_k$ is holomorphic at $\infty$. i.e. $G_k(\tau)$ is bounded as $\mathrm{Im}(\tau) \to \infty$. As $G_k(\tau + 1) = G_k(\tau)$ it suffices to take the limit in the domain $|\mathrm{Re}(\tau)| \leqslant 1$ and $\mathrm{Im}(\tau) \geqslant 1$. Since $G_k$ is absolutely convergent rearranging gives

$$G_k(\tau) = 2\sum_{d=1}^{\infty} \frac{1}{d^k} + \sum_{c \neq 0, d} (c\tau + d)^{-k}$$

Since $G_k$ converges uniformly taking the limit as $\mathrm{Im}(\tau) \to \infty$ gives

$$\begin{aligned}
\lim_{\mathrm{Im}(\tau)\to\infty} G_k(\tau) &= \lim_{\mathrm{Im}(\tau)\to\infty} \left( 2\sum_{d=1}^{\infty} \frac{1}{d^k} + \sum_{c\neq 0,d} (c\tau + d)^{-k} \right) \\
&= 2\sum_{d=1}^{\infty} \frac{1}{d^k} + \sum_{c\neq 0,d} \lim_{\mathrm{Im}(\tau)\to\infty} (c\tau + d)^{-k} \\
&= 2\sum_{d=1}^{\infty} \frac{1}{d^k}.
\end{aligned}$$

Thus $G_k$ is a modular form of weight $k$. The Fourier expansion of $G_k$ can be obtained by using the identity

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

Differentiating $(k-1)$ times gives

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

Using this formula we have

$$G_k(\tau) = 2\zeta(k) + 2\frac{(2\pi i)^k}{(k-1)!} \sum_{c=1}^{\infty} \sum_{m=1}^{\infty} m^{k-1} q^{cm},$$

and this gives the Fourier expansion of $G_k$

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

where the coefficient $\sigma_{k-1}(n)$ is the arithmetic function

$$\sigma_{k-1}(n) = \sum_{\substack{m|n \\ m>0}} m^{k-1}.$$

Dividing by the leading coefficient gives a series with rational coefficients with a common denominator. The resulting series $G_k(\tau)/(2\zeta(k))$ is called normalized Eisenstein series and denoted by $E_k(\tau)$.

**Definition 1.1.3.** *A cusp form of weight $k$ is a modular form of weight $k$ such that the leading coefficient $a_0$ in the Fourier expansion is zero, i.e.,*

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

*The set of cusp forms is denoted by $\mathcal{S}_k(\mathrm{SL}_2(\mathbb{Z}))$.*

Note that a modular form is a cusp form when $\lim_{\mathrm{Im}(\tau)\to\infty} f(\tau) = 0$. $\mathcal{S}_k(\mathrm{SL}_2(\mathbb{Z}))$ is a subspace of $\mathcal{M}_k(\mathrm{SL}_2(\mathbb{Z}))$. An example of a cusp form is the discriminant function, $\Delta : \mathcal{H} \to \mathbb{C}$ defined by

$$\Delta(\tau) = (g_2(\tau))^3 - 27(g_3(\tau))^2$$

where $g_2(\tau) = 60G_4(\tau)$ and $g_3(\tau) = 140G_6(\tau)$. Now $\Delta$ is weakly modular of weight 12 and holomorphic on $\mathcal{H}$. We have seen above that $\lim_{\mathrm{Im}(\tau)\to\infty} G_k(\tau) = 2\zeta(k)$, hence $\lim_{\mathrm{Im}(\tau)\to\infty} \Delta(\tau) = (60(2\zeta(4)))^3 - 27(140(2\zeta(6)))^2 = 0$ since $\zeta(4) = \pi^4/90$ and $\zeta(6) = \pi^6/945$. Thus $a_0 = 0$ in the Fourier expansion of $\Delta$ and so $\Delta \in \mathcal{S}_k(\mathrm{SL}_2(\mathbb{Z}))$. We will prove later that $\Delta$ is non vanishing on $\mathcal{H}$ hence we can define $j : \mathcal{H} \to \mathbb{C}$ by

$$j(\tau) = 1728\frac{(g_2(\tau))^3}{\Delta(\tau)}.$$

$j$ is clearly holomorphic on $\mathcal{H}$ and as the weights of $g_2(\tau)^3$ and $\Delta(\tau)$ are the same $j$ is $\mathrm{SL}_2(\mathbb{Z})$ invariant, $j(\gamma(\tau)) = j(\tau)$, for every $\gamma \in \mathrm{SL}_2(\mathbb{Z})$ and $\tau \in \mathcal{H}$. $j$ is called the modular invariant.

## 1.2 Congruence subgroups

In the definition of weak modularity the condition $f(\gamma(\tau)) = (c\tau + d)^k f(\tau)$ for $\gamma = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \mathrm{SL}_2(\mathbb{Z})$ can be generalized by replacing $\mathrm{SL}_2(\mathbb{Z})$ by a subgroup $\Gamma$. In this section we explain how to do this.

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

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

In particular $\Gamma(1) = \mathrm{SL}_2(\mathbb{Z})$. Note that $\Gamma(N)$ is the kernel of the natural homomorphism $\mathrm{SL}_2(\mathbb{Z}) \to SL_2(\mathbb{Z}/N\mathbb{Z})$ and so is normal in $\mathrm{SL}_2(\mathbb{Z})$. It is not hard to see that this map is surjective. Hence we have an isomorphism $\mathrm{SL}_2(\mathbb{Z})/\Gamma(N) \xrightarrow{\sim} SL_2(\mathbb{Z}/N\mathbb{Z})$. Hence $[\mathrm{SL}_2(\mathbb{Z}) : \Gamma(N)]$ is finite.

**Definition 1.2.1.** *A subgroup $\Gamma$ of $\mathrm{SL}_2(\mathbb{Z})$ is a congruence subgroup if $\Gamma(N) \subset \Gamma$ for some $N \in \mathbb{Z}^+$ and $\Gamma$ is called a congruence subgroup of level $N$.*

Note that for every congruence subgroup $\Gamma$, $[\mathrm{SL}_2(\mathbb{Z}) : \Gamma]$ is finite. The most important congruence subgroups are

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

and

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

Note that $\Gamma(N) \subset \Gamma_1(N) \subset \Gamma_0(N) \subset \mathrm{SL}_2(\mathbb{Z})$. The map $\Gamma_1(N) \to \mathbb{Z}/N\mathbb{Z}$ that is given by $\left( \begin{smallmatrix} a & b \\ c & d \end{smallmatrix} \right) \mapsto b \mod N$ is a surjection with kernel $\Gamma(N)$. Hence $\Gamma(N) \lhd \Gamma_1(N)$ and $\Gamma_1(N)/\Gamma(N) \xrightarrow{\sim} \mathbb{Z}/N\mathbb{Z}$. Similarly the map $\Gamma_0(N) \to (\mathbb{Z}/N\mathbb{Z})^*$ defined by $\left( \begin{smallmatrix} a & b \\ c & d \end{smallmatrix} \right) \mapsto d \mod N$ is a surjection with kernel $\Gamma_1(N)$ giving $\Gamma_0(N)/\Gamma_1(N) \xrightarrow{\sim} (\mathbb{Z}/N\mathbb{Z})^*$.

Now we introduce some notation. For any matrix $\gamma = \left( \begin{smallmatrix} a & b \\ c & d \end{smallmatrix} \right) \in \mathrm{SL}_2(\mathbb{Z})$ we define the factor of automorphy $j(\gamma, \tau) \in \mathbb{C}$ by $j(\gamma, \tau) = c\tau + d$ and for any $\gamma \in \mathrm{SL}_2(\mathbb{Z})$ the weight-$k$ operator $[\gamma]_k$ on functions $f : \mathcal{H} \to \mathbb{C}$ by

$$(f\,[\gamma]_k)(\tau) = j(\gamma, \tau)^{-k} f(\gamma(\tau)), \qquad \tau \in \mathcal{H}.$$

A meromorphic function $f : \mathcal{H} \to \mathbb{C}$ is called weakly modular of weight $k$ with respect to $\Gamma$ if $f\,[\gamma]_k = f$ for every $\gamma \in \Gamma$. Basic properties of factor of automorphy and weight-$k$ operator are given in the following lemma.

**Lemma 1.2.1.** *For all $\gamma, \gamma' \in \mathrm{SL}_2(\mathbb{Z})$ and $\tau \in \mathcal{H}$,*

1. $j(\gamma\gamma', \tau) = j(\gamma, \gamma'(\tau))j(\gamma', \tau)$,
2. $(\gamma\gamma')(\tau) = \gamma(\gamma'(\tau))$,
3. $[\gamma\gamma']_k = [\gamma]_k [\gamma']_k$,
4. $\mathrm{Im}(\gamma(\tau)) = \frac{\mathrm{Im}(\tau)}{|j(\gamma,\tau)|^2}$,
5. $\frac{d\gamma(\tau)}{d\tau} = \frac{1}{j(\gamma,\tau)^2}$

*Proof.* [**?**, Lemma 1.2.2]. □

The property 3 of the above lemma implies that if a function $f : \mathcal{H} \to \mathbb{C}$ is weakly modular of weight k with respect to a subset $S$ of $\mathrm{SL}_2(\mathbb{Z})$ the $f$ is weakly modular of weight k with respect to the subgroup generated by $S$.

Now we give the definition of a modular form with respect to a congruence subgroup $\Gamma$. Let $k$ be an integer. A function $f : \mathcal{H} \to \mathbb{C}$ is a modular form of weight $k$ with respect to $\Gamma$ if it is weakly modular of weight $k$ with respect to $\Gamma$ and satisfies certain holomorphy condition: As $\Gamma(N) \subset \Gamma$ form some $N$, $\Gamma$ contains a matrix of the form $\left(\begin{smallmatrix} 1 & h \\ 0 & 1 \end{smallmatrix}\right) : \tau \mapsto \tau + h$ for some minimal $h \in \mathbb{Z}^+$. If $f : \mathcal{H} \to \mathbb{C}$ is weakly modular of weight $k$ with respect to $\Gamma$, $f$ is $h\mathbb{Z}$-periodic. Similarly to the first section there is a function $g : D \to \mathbb{C}$ such that $f(\tau) = g(q_h)$ where $q_h = e^{2\pi i\tau/h}$ and $D$ is again the punctured unit disk. As before $g$ is holomorphic on $D$ since $f$ is holomorphic on $\mathcal{H}$ hence $g$ has a Laurent expansion. $f$ is defined to be holomorphic at $\infty$ if $g$ extends holomorphically to $q_h = 0$. If this is the case $f$ has a Fourier expansion

$$f(\tau) = \sum_{n=0}^{\infty} a_n q_h^n.$$

A $\Gamma$-equivalence class of points in $\mathbb{Q} \cup \{\infty\}$ is called a cusp of $\Gamma$. $\mathrm{SL}_2(\mathbb{Z})$ has only one cusp as all rational points are equivalent to $\infty$. Each $s \in \mathbb{Q}$ is of the form $s = \alpha(\infty)$ for some $\alpha \in \mathrm{SL}_2(\mathbb{Z})$ hence the number of cusps is at most the number of cosets $\Gamma\alpha$ in $\mathrm{SL}_2(\mathbb{Z})$. A modular form with respect to $\Gamma$ should be holomorphic at cusps. Holomorphy at $s \in \mathbb{Q}$ is defined in terms of holomorphy at $\infty$: Write $s \in \mathbb{Q}$ as $s = \alpha(\infty)$. $f$ is holomorphic at $s$ if $f\,[\alpha]_k$ is holomorphic at $\infty$. This makes sense since $f\,[\alpha]_k$ is holomorphic on $\mathcal{H}$ and weakly modular with respect to $\alpha^{-1}\Gamma\alpha$ which is again a congruence subgroup of $\mathrm{SL}_2(\mathbb{Z})$.

**Definition 1.2.2.** *Let $\Gamma$ be a congruence subgroup of $\mathrm{SL}_2(\mathbb{Z})$ and $k$ be an integer. A function $f : \mathcal{H} \to \mathbb{C}$ is a modular form of weight $k$ with respect to $\Gamma$ if*
*(1) $f$ is holomorphic,*
*(2) $f$ is weight-$k$ invariant under $\Gamma$,*
*(3) $f\,[\alpha]_k$ is holomorphic at $\infty$ 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 said to be a cusp form of weight $k$ with respect to $\Gamma$.*

The modular forms(resp. cusp forms) of weight k with respect to $\Gamma$ are denoted by $\mathcal{M}_k(\Gamma)$(resp. $\mathcal{S}_k(\Gamma)$). Since $f[\gamma\alpha]_k = f[\alpha]_k$ for all $\gamma \in \Gamma$, condition (3) and (4) in the above definition need to be checked for only finitely many coset representatives of $\Gamma$ in $\mathrm{SL}_2(\mathbb{Z})$.

Let $\chi$ be a Dirichlet character modulo $N$. The $\chi$-eigenspace of $\mathcal{M}_k(\Gamma_1(N))$ is defined as the set

$$\mathcal{M}_k(N, \chi) = \{f \in \mathcal{M}_k(\Gamma_1(N)) : f[\gamma]_k = \chi(d)f \text{ for all } \gamma = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \Gamma_0(N)\}.$$

The vector space $\mathcal{M}_k(\Gamma_1(N))$ decomposes as

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

We will use this fact frequently.

## 1.3 Complex Tori

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

**Lemma 1.3.1.** *Consider two lattices $\Lambda = \omega_1\mathbb{Z} \oplus \omega_2\mathbb{Z}$ and $\Lambda' = \omega_1'\mathbb{Z} + \omega_2'\mathbb{Z}$. Then $\Lambda = \Lambda'$ if and only if $\left(\begin{smallmatrix} \omega_1' \\ \omega_2' \end{smallmatrix}\right) = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right)\left(\begin{smallmatrix} \omega_1 \\ \omega_2 \end{smallmatrix}\right)$ for some $\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \mathrm{SL}_2(\mathbb{Z})$.*

*Proof.* [**?**, Theorem 1.2] □

A complex torus is a quotient of the complex plane by a lattice, $\mathbb{C}/\Lambda = \{z + \Lambda : z \in \mathbb{C}\}$. It is a compact Riemann surface. The following proposition characterize the holomorphic maps between complex tori.

**Proposititon 1.3.1.** *Suppose $\varphi : \mathbb{C}/\Lambda \to \mathbb{C}/\Lambda'$ is a holomorphic map between complex tori. Then there exist $m, b \in \mathbb{C}$ with $m\Lambda \subset \Lambda'$ such that $\varphi(z + \Lambda) = mz + b + \Lambda'$. $\varphi$ is invertible if and only if $m\Lambda = \Lambda'$.*

*Proof.* Since $\mathbb{C}$ is the universal covering space of $\mathbb{C}/\Lambda$, $\varphi$ lifts to a holomorphic map $\tilde{\varphi} : \mathbb{C} \to \mathbb{C}$.

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

Let $\lambda \in \Lambda$ and consider the function $f_\lambda(z) = \tilde{\varphi}(z + \lambda) - \tilde{\varphi}(z)$. By the commutativity of the above diagram we have $p'(\tilde{\varphi}(z + \lambda)) = \varphi(p(z + \lambda)) = \varphi(p(z)) = p'(\tilde{\varphi}(z))$ and so $\tilde{\varphi}(z+\lambda) - \tilde{\varphi}(z) \in \Lambda'$. Hence $f_\lambda$ maps $\mathbb{C}$ to $\Lambda'$ and since $f_\lambda$ is continuous, it is constant. Therefore differentiating gives $\tilde{\varphi}'(z+\lambda) = \tilde{\varphi}'(z)$ and so $\tilde{\varphi}'$ is a holomorphic, $\Lambda$ periodic function. This makes $\tilde{\varphi}'$ bounded and by Liouville's theorem it is constant. Hence $\tilde{\varphi}(z) = mz + b$. Since $\tilde{\varphi}$ lifts a map between quotients, we have $m\Lambda \subset \Lambda'$ and $\varphi$ has the form given in the proposition. □

**Corollary 1.3.1.** *Suppose $\varphi : \mathbb{C}/\Lambda \to \mathbb{C}/\Lambda'$ is a holomorphic map between complex tori, $\varphi(z+\Lambda) = mz + b + \Lambda'$ with $m\Lambda \subset \Lambda'$. Then the following are equivalent:*

1. *$\varphi$ is a group homomorphism,*

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

3. *$\varphi(0) = 0$.*

Now we give an example of an isomorphism between complex tori. Let $\Lambda = \omega_1\mathbb{Z} \oplus \omega_2\mathbb{Z}$ 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 $\tau$ and 1. $\tau$ is not unique but if $\tau' \in \mathcal{H}$ 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 **??** $\tau' = \gamma(\tau)$ for some $\gamma \in \mathrm{SL}_2(\mathbb{Z})$. Thus each complex torus determines a complex number $\tau \in \mathcal{H}$ up to action of $\mathrm{SL}_2(\mathbb{Z})$.

**Definition 1.3.1.** *A nonzero holomorphic homomorphism between complex tori is called an isogeny.*

**Examples**

1. Every holomorphic isomorphism is an isogeny.

2. Multiply by integer maps: Let $N$ be a positive integer and $\Lambda$ 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 $\mathbb{Z}/N\mathbb{Z} \times \mathbb{Z}/N\mathbb{Z}$. The kernel is denoted by $E[N]$.

3. 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 $\Lambda$. The cyclic quotient map $\pi : \mathbb{C}/\Lambda \to \mathbb{C}/C$ given by $z+\Lambda \mapsto z+C$ is an isogeny with kernel $C$.

Every isogeny can be written in terms of the above examples. Indeed; let $\varphi : \mathbb{C}/\Lambda \to \mathbb{C}/\Lambda', \quad z + \Lambda \mapsto mz + \Lambda'$ and let $K = \ker\varphi$. Then $K = m^{-1}\Lambda'/\Lambda$. $K$ can also be viewed as a superlattice $K = m^{-1}\Lambda'$ of $\Lambda$. Let $N$ be the order of $K$, hence $K \subset E[N] \cong \mathbb{Z}/N\mathbb{Z} \times \mathbb{Z}/N\mathbb{Z}$ and so $K \cong \mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/nn'\mathbb{Z}$ for some $n, n' \in \mathbb{Z}^+$. Then $nK$ is a cyclic subgroup isomorphic to $\mathbb{Z}/n'\mathbb{Z}$ and the quotient isogeny $\pi : \mathbb{C}/\Lambda \to \mathbb{C}/nK$ has kernel $nK$. Now consider the map $\mathbb{C}/nK \to \mathbb{C}/\Lambda'$ given by $z+nK \mapsto (m/n)z+\Lambda'$. This map is an isomorphism since $(m/n)nK = mK = \Lambda'$. Thus we have

$$\varphi : \ \mathbb{C}/\Lambda \xrightarrow{[n]} \mathbb{C}/\Lambda \xrightarrow{\pi} \mathbb{C}/nK \ \xrightarrow{\sim} \mathbb{C}/\Lambda'.$$

Let $\Lambda$ be a lattice. The $N$-torsion subgroup of $\mathbb{C}/\Lambda$ is

$$E[N] = \{P \in \mathbb{C}/\Lambda : [N]P = 0\} = \langle \omega_1/N + \Lambda \rangle \times \langle \omega_2/N + \Lambda \rangle.$$

Let $\mu_N$ denote the complex $N$th roots of unity $\mu_N = \{z \in \mathbb{C} : z^N = 1\}$. We define the Weil pairing $e_N : E[N] \times E[N] \to \mu_N$ as follows: Let $P$ and $Q$ be points in $E[N]$. If $\Lambda = \omega_1\mathbb{Z} \oplus \omega_2\mathbb{Z}$ then $\left(\begin{smallmatrix} P \\ Q \end{smallmatrix}\right) = \gamma \left(\begin{smallmatrix} \omega_1/N+\Lambda \\ \omega_2/N+\Lambda \end{smallmatrix}\right)$ for some $\gamma \in M_2(\mathbb{Z}/N\mathbb{Z})$. The Weil pairing of $P$ and $Q$ is $e_N(P, Q) = e^{2\pi i \det\gamma/N}$.

Now we show that how complex tori can be viewed as elliptic curves. Given a lattice $\Lambda$ and let $E = \mathbb{C}/\Lambda$. The meromorphic functions $f : \mathbb{C}/\Lambda \to \widehat{\mathbb{C}}$ can be identified with the $\Lambda$-periodic meromorphic functions $f : \mathbb{C} \to \widehat{\mathbb{C}}$. These $\Lambda$-periodic functions are called elliptic functions. Let $P = \{x_1\omega_1 + x_2\omega_2 : x_1, x_2 \in [0,1]\}$ be the parallelogram representing $E$ and $\partial P$ be the counterclockwise boundary of $P$. Since $f$ has finitely many poles and zeros, $t + \partial P$ does not contain any poles or zeros for some $t$. The following lemma gives some basic properties of these functions that we will need later.

**Lemma 1.3.2.** *Let $f : \mathbb{C} \to \widehat{\mathbb{C}}$ be an elliptic function. Then*

1. $1/(2\pi i) \int_{t+\partial P} f(z)dz = 0$*, hence the sum of the residues of $f$ on $E$ is zero,*
2. $1/(2\pi i) \int_{t+\partial P} \frac{f'(z)}{f(z)} dz = 0$*, hence $f$ takes each value $N$ times, where $N$ is the order of $f$,*
3. $1/(2\pi i) \int_{t+\partial P} z\frac{f'(z)}{f(z)} dz = 0$*, hence $\sum_{x \in E} \nu_x(f)x = 0$ in $E$, where $\nu_x(f)$ is the order of $f$ at $x$.*

*Proof.* [**?**, Chapter 3]. □

The most important example of these functions is the Weierstrass $\wp$-function

$$\wp(z) = \frac{1}{z^2} + \sum_{\omega\in\Lambda}{}' \left( \frac{1}{(z-\omega)^2} + \frac{1}{\omega^2} \right), \qquad z \in \mathbb{C},\ z \notin \Lambda.$$

The sum converges absolutely and uniformly on compact subsets of $\mathbb{C}$ away from $\Lambda$ [**?**]. The derivative

$$\wp'(z) = -2 \sum_{\omega\in\Lambda} \frac{1}{(z-\omega)^3}$$

is clearly $\Lambda$-periodic. i.e. $\wp'(z+\omega) = \wp'(z)$ for all $\omega \in \Lambda$. Hence $\wp(z+\omega) - \wp(z)$ is constant. When $z = -\omega/2$, $\wp(\omega/2) - \wp(-\omega/2) = 0$ as $\wp$ is an even function. This makes $\wp(z+\omega) = \wp(z)$ for all $\omega \in \Lambda$. Thus $\wp$ is $\Lambda$-periodic. This example is important since the field of meromorphic functions on $\mathbb{C}/\Lambda$ is $\mathbb{C}(\wp, \wp')$, the rational expressions in these two functions.

Eisenstein series generalize to functions whose variable is a lattice, $G_k(\Lambda) = \sum_{\omega\in\Lambda}{}' \frac{1}{\omega^2}$, $k > 2$ even. Hence the function $G_k(\tau)$ from before can be written as $G_k(\Lambda_\tau)$.

**Proposititon 1.3.2.** *Let $\wp$ be the Weierstrass function with respect to a lattice $\Lambda$. Then*

1. *The Laurent expansion of $\wp$ is*

$$\wp(z) = \frac{1}{z^2} + \sum_{\substack{n=2 \\ n \text{ even}}}^{\infty} (n+1)G_{n+2}(\Lambda)z^n$$

*for all $z$ such that $0 < |z| < \inf\{|\omega| : \omega \in \Lambda - \{0\}\}$.*

2. *The functions $\wp$ and $\wp'$ satisfy the relation*

$$(\wp'(z))^2 = 4(\wp(z))^3 - g_2(\Lambda)\wp(z) - g_3(\Lambda)$$

*where $g_2(\Lambda) = 60G_4(\Lambda)$ and $g_3(\Lambda) = 140G_6(\Lambda)$.*

3. *Let $\Lambda = \omega_1\mathbb{Z} \bigoplus \omega_2\mathbb{Z}$ and $\omega_3 = \omega_1 + \omega_2$. Then the cubic equation satisfied by $\wp'$ and $\wp$ is*

$$y^2 = 4(x - e_1)(x - e_2)(x - e_3), \qquad e_i = \wp(\omega_i/2) \textit{ for } i = 1, 2, 3.$$

*$e_i$'s are distinct.*

*Proof.* (1) Let $r = \inf\{|\omega| : \omega \in \Lambda - \{0\}\}$. If $0 < |z| < r$, then $|z/\omega| < 1$ and we have

$$\frac{1}{(z-\omega)^2} = \frac{1}{\omega^2\left(1 - \frac{z}{\omega}\right)^2} = \frac{1}{\omega^2}\left(1 + \sum_{n=1}^{\infty}(n+1)\left(\frac{z}{\omega}\right)^n\right).$$

Hence we have

$$\wp(z) = \frac{1}{z^2} + \sum_{n=1}^{\infty}(n+1)\sum_{\omega\neq 0}\frac{1}{\omega^{n+2}}z^n = \frac{1}{z^2} + \sum_{n=1}^{\infty}(n+1)G_{n+2}(\Lambda)z^n.$$

When $n$ is odd $G_{n+2}(\Lambda) = 0$ so (1) follows.

(2) Using part (1) we have

$$(\wp'(z))^2 = 4/z^6 - 24G_4(\Lambda)/z^2 - 80G_6(\Lambda) + \mathcal{O}(z^2)$$

and

$$4(\wp(z))^3 - g_2(\Lambda)\wp(z) - g_3(\Lambda) = 4/z^6 - 24G_4(\Lambda)/z^2 - 80G_6(\Lambda) + \mathcal{O}(z^2)$$

hence the difference is a holomorphic $\Lambda$-periodic function, hence bounded and therefore constant making it zero. This proves part (2).

(3) Since $\wp'$ is odd, it has zeros at the order two points of $\mathbb{C}/\Lambda$. The order two points are $z_i = \omega_i/2$ for $i = 1, 2, 3$. Hence by part (2), $e_i = \wp(\omega_i/2)$ are the roots of the cubic polynomial $4x^3 - g_2(\Lambda)x - g_3(\Lambda)$ and this proves the factorization in part (3). Now let $f_i(z) = \wp(z) - e_i$. $f_i$ is an elliptic function of order 2. Since $f_i(\omega_i/2) = f_i'(\omega_i/2) = 0$, $f_i$ has double zeros at $\omega_i/2$ and so has no other zeros. Hence $f_i(\omega_j/2) \neq 0$ for $i \neq j$. This shows that $e_i$'s are distinct. □

Part (3) of the above proposition shows that the map $z \mapsto (\wp(z), \wp'(z))$ takes the nonlattice points of $\mathbb{C}$ to points $(x, y) \in \mathbb{C}^2$ satisfying the cubic equation $y^2 = 4x^3 - g_2(\Lambda)x - g_3(\Lambda)$. This map is bijective. It extends to lattice points by mapping them to a point at infinity. Thus we have shown that for every lattice the associated Weierstrass $\wp$-function gives a bijection

$$(\wp, \wp') : \text{complex torus} \to \text{elliptic curve}.$$

Under this map the group law on complex torus is transferred to the elliptic curve. Indeed, let $z_1 + \Lambda$ and $z_2 + \Lambda$ be nonzero points of the torus. The image points $(\wp(z_1), \wp'(z_1))$ and $(\wp(z_2), \wp'(z_2))$ determine a tangent or secant line of the curve. Let $ax + by + c = 0$ denote this line and consider the function

$$f(z) = a\wp(z) + b\wp'(z) + c.$$

Now $f$ is meromorphic on $\mathbb{C}/\Lambda$. If $b \neq 0$, $f$ has a triple pole at $0 + \Lambda$ and zeros at $z_1 + \Lambda$ and $z_2 + \Lambda$. By Lemma **??** the third zero of $f$ is at $z_3 + \Lambda$ such that $z_1 + z_2 + z_3 + \Lambda = 0 + \Lambda$. If $b = 0$, $f$ has a double pole at $0 + \Lambda$ and zeros at $z_1 + \Lambda$ and $z_2 + \Lambda$, and again by lemma **??** $z_1 + z_2 + \Lambda = 0 + \Lambda$. In this case let $z_3 + \Lambda = 0 + \Lambda$ and so we have $z_1 + z_2 + z_3 + \Lambda = 0 + \Lambda$. Thus the points of the elliptic curve on the line $ax + by + c = 0$ are the points $(x_i, y_i) = (\wp(z_i), \wp'(z_i))$ for $i = 1, 2, 3$. Since $z_1 + z_2 + z_3 + \Lambda = 0 + \Lambda$ the group law on the curve is that collinear triples sum to zero.

We have seen that a holomorphic isomorphism of complex tori is of the form $z + \Lambda \mapsto mz + \Lambda'$ for $m\Lambda = \Lambda'$. Since $\wp_{\Lambda'}(mz) = m^{-2}\wp_{\Lambda}(z)$ and $\wp'_{\Lambda'}(mz) = m^{-3}\wp'_{\Lambda}(z)$ the corresponding isomorphism of elliptic curves is $(x, y) \mapsto (m^{-2}x, m^{-3}y)$. This transforms the cubic equation $y^2 = 4x^3 - g_2x - g_3$ into $y^2 = 4x^3 - m^{-4}g_2x - m^{-6}g_3$.

The following corollary of Proposition **??** shows that the discriminant function $\Delta$ is nonvanishing.

**Corollary 1.3.2.** *The discriminant function $\Delta$ is non vanishing on $\mathcal{H}$.*

*Proof.* Let $\tau \in \mathcal{H}$. Consider the lattice $\Lambda_\tau$ and the resulting cubic polynomial $4x^3 - g_2(\tau)x - g_3(\tau)$. By Proposition **??** this polynomial has distinct roots. Since $\Delta(\tau)$ is the discriminant of this polynomial, $\Delta(\tau) \neq 0$ □

Up to this point we have seen that every complex torus lead to an elliptic curve

$$y^2 = 4x^3 - a_2x - a_3, \qquad a_2^3 - 27a_3^2 \neq 0 \tag{1.1}$$

via the Weierstrass $\wp$-function. The converse is also true.

**Propositon 1.3.3.** *For every elliptic curve (**??**), there exists a lattice $\Lambda$ such that $a_2 = g_2(\Lambda)$ and $a_3 = g_3(\Lambda)$.*

*Proof.* If $a_2 = 0$ take $\Lambda = \Lambda_{\mu_3}$ where $\mu_3$ is the third root of unity. If $a_3 = 0$ take $\Lambda = \Lambda_i$. Now assume that $a_2 \neq 0$ and $a_3 \neq 0$. Since $j : \mathcal{H} \to \mathbb{C}$ surjects, there exists $\tau \in \mathcal{H}$ such that $j(\tau) = 1728a_2^3/(a_2^3 - 27a_3^2)$. Hence

$$\frac{g_2(\tau)}{g_2(\tau)^3 - 27g_3(\tau)^2} = \frac{a_2^3}{a_2^3 - 27a_3^2},$$

and so

$$\frac{a_2^3}{g_2(\tau)^3} = \frac{a_3^2}{g_3(\tau)^2} \tag{1.2}$$

Choose $\omega_2 \in \mathbb{C}$ such that $\omega_2^{-4} = a_2/g_2(\tau)$ and so $\omega_2^{-12} = a_2^3/g_2(\tau)^3$. By (**??**), $\omega_2^{-6} = \pm a_3/g_3(\tau)$. Replacing $\omega_2$ by $i\omega_2$ if necessary we may assume $\omega_2^{-6} = a_3/g_3(\tau)$. Let $\omega_1 = \tau\omega_2$ and $\Lambda = \omega_1\mathbb{Z} \oplus \omega_2\mathbb{Z}$. Then $a_2 = g_2(\Lambda)$ and $a_3 = g_3(\Lambda)$. □

Thus we may identify complex tori and elliptic curves.

## 1.4 Modular curves and moduli spaces

In this section we explain how modular curves parametrize the complex elliptic curves together with $N$-torsion data.

Let $N$ be a positive integer. An enhanced elliptic curve for $\Gamma_0(N)$ is an ordered pair $(E, C)$ where $E$ is a complex elliptic curve and $C$ is a cyclic subgroup of $E$ of order $N$. Two such pairs $(E, C)$ and $(E', C')$ are equivalent if there exists an isomorphism $E \xrightarrow{\sim} E'$ taking $C$ to $C'$. The set of equivalence classes is denoted by $S_0(N)$.

An enhanced elliptic curve for $\Gamma_1(N)$ is a pair $(E, Q)$ where $E$ is a complex elliptic curve and $Q$ is a point of order $N$. Two such pairs $(E, Q)$ and $(E', Q')$ are equivalent if there exists an isomorphism $E \xrightarrow{\sim} E'$ taking $Q$ to $Q'$. The set of equivalence classes is denoted by $S_1(N)$.

An enhanced elliptic curve for $\Gamma(N)$ is a pair $(E, (P, Q))$ where $E$ is a complex elliptic curve and $(P, Q)$ is a pair of points that generates $E[N]$ with $e_N(P, Q) = e^{2\pi i/N}$. Two such pairs $(E, (P, Q))$ and $(E', (P', Q'))$ are equivalent if there exists an isomorphism $E \xrightarrow{\sim} E'$ taking $P$ to $P'$ and $Q$ to $Q'$. The set of equivalence classes is denoted by $S(N)$.

Each of $S_0(N)$, $S_1(N)$, and $S(N)$ is a moduli space of isomorphism classes of complex elliptic curves and $N$-torsion data. If $N = 1$ then all moduli spaces above reduce to the isomorphism classes of complex elliptic curves.

For any congruence subgroup $\Gamma$ of $\mathrm{SL}_2(\mathbb{Z})$ acting on the upper half plane $\mathcal{H}$, the modular curve $Y(\Gamma)$ is defined as the quotient space of the orbits under the action of $\Gamma$, $Y(\Gamma) = \Gamma\backslash\mathcal{H} = \{\Gamma\tau : \tau \in \mathcal{H}\}$. The topology on the upper half plane $\mathcal{H}$ is the subspace topology induced from $\mathbb{R}^2$. The quotient map $\pi : \mathcal{H} \to Y(\Gamma)$ defined by $\pi(\tau) = \Gamma\tau$ gives $Y(\Gamma)$ the quotient topology. Under this topology $\pi$ is an open mapping and $Y(\Gamma)$ is Hausdorff. The modular curves for $\Gamma_0(N)$, $\Gamma_1(N)$ and $\Gamma(N)$ are denoted by $Y_0(N)$, $Y_1(N)$ and $Y(N)$ respectively.

Let $\mathcal{H}^* = \mathcal{H} \cup \mathbb{Q} \cup \{\infty\}$ and define $X(\Gamma) = \Gamma\backslash\mathcal{H}^* = Y(\Gamma) \cup \Gamma\backslash(\mathbb{Q} \cup \{\infty\})$. To define the topology on $\mathcal{H}^*$, let $\mathcal{N}_M = \{\tau \in \mathcal{H} : \mathrm{Im}(\tau) > M\}$ for $M > 0$. Use the sets $\alpha(\mathcal{N}_M \cup \{\infty\})$ for $\alpha \in \mathrm{SL}_2(\mathbb{Z})$ and $M > 0$ as a base of neighborhoods of the cusps and use the usual topology for points $\tau \in \mathcal{H}$. Hence we have a topology on $\mathcal{H}^*$. Give $X(\Gamma)$ the quotient topology induced by the natural map $\pi : \mathcal{H}^* \to X(\Gamma)$. Under this topology $X(\Gamma)$ is a compact connected and Hausdorff. Moreover $X(\Gamma)$ is compact Riemann surface. For details see [**?**, Chapter 2].

**Theorem 1.4.1.** *Let $N$ be a positive integer.*

1. *The moduli space for $\Gamma_0(N)$ is*

   $$S_0(N) = \{[E_\tau, \langle 1/N + \Lambda_\tau\rangle] : \tau \in \mathcal{H}\}.$$

   *Two points $[E_\tau, \langle 1/N + \Lambda_\tau\rangle]$ and $[E_{\tau'}, \langle 1/N + \Lambda_{\tau'}\rangle]$ are equal if and only if $\Gamma_0(N)\tau = \Gamma_0(N)\tau'$.Thus there is a bijection $\psi_0 : S_0(N) \xrightarrow{\sim} Y_0(N)$ given by,*

   $$[\mathbb{C}/\Lambda_\tau, \langle 1/N + \Lambda_\tau\rangle] \mapsto \Gamma_0(N)\tau.$$

2. *The moduli space for $\Gamma_1(N)$ is*

   $$S_1(N) = \{[E_\tau, 1/N + \Lambda_\tau] : \tau \in \mathcal{H}\}.$$

   *Two points $[E_\tau, 1/N+\Lambda_\tau]$ and $[E_{\tau'}, 1/N+\Lambda_{\tau'}]$ are equal if and only if $\Gamma_1(N)\tau = \Gamma_1(N)\tau'$.Thus there is a bijection $\psi_1 : S_1(N) \xrightarrow{\sim} Y_1(N)$ given by,*

   $$[\mathbb{C}/\Lambda_\tau, 1/N + \Lambda_\tau] \mapsto \Gamma_1(N)\tau.$$

3. *The moduli space for $\Gamma(N)$ is*

   $$S(N) = \{[E_\tau, (\tau/N + \Lambda_\tau, 1/N + \Lambda_\tau)] : \tau \in \mathcal{H}\}.$$

   *Two points $[E_\tau, (\tau/N + \Lambda_\tau, 1/N + \Lambda_\tau)]$ and $[E_{\tau'}, (\tau'/N + \Lambda_{\tau'}, 1/N + \Lambda_{\tau'})]$ are equal if and only if $\Gamma(N)\tau = \Gamma(N)\tau'$.Thus there is a bijection $\psi : S(N) \xrightarrow{\sim} Y(N)$ given by,*

   $$[\mathbb{C}/\Lambda_\tau, (\tau/N + \Lambda_\tau, 1/N + \Lambda_\tau)] \mapsto \Gamma(N)\tau.$$

*Proof.* We only prove part (2). Part (1) and (3) follows from similar arguments. Let $[E, Q] \in S_1(N)$. Since $E$ is isomorphic to $\mathbb{C}/\Lambda_{\tau'}$ for some $\tau' \in \mathcal{H}$, we may assume $E = \mathbb{C}/\Lambda_{\tau'}$. Then $Q = (c\tau' + d)/N + \Lambda_{\tau'}$ for some $c, d \in \mathbb{Z}$. As the order of $Q$ is $N$, $\gcd(c, d, N) = 1$. i.e. $ad - bc - kN = 1$ for some $a, b, k \in \mathbb{Z}$. Consider the matrix $\gamma = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in M_2(\mathbb{Z})$. Note that $\gamma \mod N \in SL_2(\mathbb{Z}/N\mathbb{Z})$. Since changing $\gamma$ modulo $N$ does not change $Q$ and $\mathrm{SL}_2(\mathbb{Z})$ surjects to $SL_2(\mathbb{Z}/N\mathbb{Z})$ we may take $\gamma = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \mathrm{SL}_2(\mathbb{Z})$. Let $\tau = \gamma(\tau')$ and $m = c\tau' + d$. Hence $m\tau = a\tau' + b$ and so

$$m\Lambda_\tau = m(\tau\mathbb{Z} \oplus \mathbb{Z}) = (a\tau' + b)\mathbb{Z} \oplus (c\tau' + d)\mathbb{Z}.$$

Since $\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \mathrm{SL}_2(\mathbb{Z})$ by Lemma **??**

$$(a\tau' + b)\mathbb{Z} \oplus (c\tau' + d)\mathbb{Z} = \tau'\mathbb{Z} \oplus \mathbb{Z} = \Lambda_{\tau'}.$$

We also have

$$m\left(1/N + \Lambda_\tau\right) = (c\tau' + d)/N + \Lambda_{\tau'} = Q.$$

This proves that $[E, Q] = [\mathbb{C}/\Lambda_\tau, 1/N + \Lambda_\tau]$.

Suppose $\Gamma_1(N)\tau = \Gamma_1(N)\tau'$ for some $\tau, \tau' \in \mathcal{H}$. Hence $\tau = \gamma(\tau')$ for some $\gamma = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \Gamma_1(N)$. Thus $(c, d) \equiv (0, 1) \mod N$ and so $m(1/N + \Lambda_\tau) = (1/N + \Lambda_{\tau'})$. Thus $[\mathbb{C}/\Lambda_\tau, 1/N + \Lambda_\tau] = [\mathbb{C}/\Lambda_{\tau'}, 1/N + \Lambda_{\tau'}]$. Therefore $\psi_1$ is injective.

Now suppose $[\mathbb{C}/\Lambda_\tau, 1/N + \Lambda_\tau] = [\mathbb{C}/\Lambda_{\tau'}, 1/N + \Lambda_{\tau'}]$ with $\tau, \tau' \in \mathcal{H}$. Then there exists $m \in \mathbb{C}$ such that $m\Lambda_\tau = \Lambda_{\tau'}$ and $m(1/N + \Lambda_\tau) = 1/N + \Lambda_{\tau'}$. Thus by Lemma **??** we have

$$\left(\begin{smallmatrix} m\tau \\ m \end{smallmatrix}\right) = \gamma\left(\begin{smallmatrix} \tau' \\ 1 \end{smallmatrix}\right) \quad \text{for some } \gamma = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \mathrm{SL}_2(\mathbb{Z}), \tag{1.3}$$

so $m = c\tau' + d$. Thus from above we have

$$\frac{c\tau' + d}{N} + \Lambda_{\tau'} = \frac{1}{N} + \Lambda_{\tau'}.$$

Therefore $(c,d) \equiv (0,1) \mod N$ and $\gamma \in \Gamma_1(N)$. Since by (**??**) $\tau = \gamma(\tau')$, $\Gamma_1(N)\tau = \Gamma_1(N)\tau'$. □

Taking $N = 1$ in the above theorem shows that isomorphism classes of complex elliptic curves are in one-to-one correspondence with $\mathrm{SL}_2(\mathbb{Z})\backslash\mathcal{H}$. Hence we associate an orbit $\mathrm{SL}_2(\mathbb{Z})\tau$ to each isomorphism class. Since the modular invariant $j$ is $\mathrm{SL}_2(\mathbb{Z})$-invariant function on $\mathcal{H}$, each isomorphism class has a well-defined invariant $j(\mathrm{SL}_2(\mathbb{Z})\tau)$. This value is denoted by $j(E)$ for any complex elliptic curve $E$ in the isomorphism class.

The bijections in Theorem **??** give more examples of modular forms as follows: Let $k$ be an integer and $\Gamma = \Gamma_1(N)$. A complex valued function $F$ of enhanced elliptic curves for $\Gamma$ is degree-$k$ homogeneous with respect to $\Gamma$ if for every $m \in \mathbb{C}^*$,

$$F(\mathbb{C}/m\Lambda, mQ) = m^{-k}F(\mathbb{C}/\Lambda, Q). \tag{1.4}$$

Given such $F$ define $f : \mathcal{H} \to \mathbb{C}$ by

$$f(\tau) = F(\mathbb{C}/\Lambda_\tau, 1/N + \Lambda_\tau).$$

Then $f$ is weight-$k$ invariant with respect to $\Gamma$.

Conversely, let $f$ be weight-$k$ invariant with respect to $\Gamma$. Then define $F$ on enhanced elliptic curves by

$$F(\mathbb{C}/\Lambda_\tau, 1/N + \Lambda_\tau) = f(\tau).$$

If $(\mathbb{C}/\Lambda_{\tau'}, 1/N + \Lambda_{\tau'}) = (\mathbb{C}/m\Lambda_\tau, m/N + \Lambda_\tau)$ then $\tau = \gamma(\tau')$ and $m = c\tau' + d$ for some $\gamma = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \Gamma$. Hence $F$ satisfies (**??**)

$$F(\mathbb{C}/\Lambda_{\tau'}, 1/N + \Lambda_{\tau'}) = f(\tau') = m^{-k}f(\tau) = m^{-k}F(\mathbb{C}/m\Lambda_\tau, 1/N + \Lambda_\tau).$$

Since every enhanced elliptic curve is equivalent to an enhanced elliptic curve of the special type given above $F$ extends to all of $S_1(N)$.

# 2 Hecke Operators

In this section we define the Hecke operators and find a canonical basis for the space $\mathcal{S}_k(\Gamma_1(N))$.

## 2.1 The $\langle d \rangle$ and $T_p$ operators

Let $\Gamma_1$ and $\Gamma_2$ be congruence subgroups of $\mathrm{SL}_2(\mathbb{Z})$. For each $\alpha \in GL_2^+(\mathbb{Q})$ the set $\Gamma_1\alpha\Gamma_2 = \{\gamma_1\alpha\gamma_2 : \gamma_1 \in \Gamma_1, \gamma_2 \in \Gamma_2\}$ is said to be a double coset in $GL_2^+(\mathbb{Q})$. $\Gamma_1$ acts on $\Gamma_1\alpha\Gamma_2$ by left multiplication. Hence the orbit space is

$$\Gamma_1\backslash\Gamma_1\alpha\Gamma_2 = \bigcup_j \Gamma_1\beta_j \tag{2.1}$$

where $\beta_j$ are orbit representatives.

**Lemma 2.1.1.** *For any congruence subgroup $\Gamma$ of $\mathrm{SL}_2(\mathbb{Z})$ and $\alpha \in GL_2^+(\mathbb{Q})$, the set $\alpha^{-1}\Gamma\alpha \cap \mathrm{SL}_2(\mathbb{Z})$ is a congruence subgroup of $\mathrm{SL}_2(\mathbb{Z})$.*

*Proof.* [**?**, Lemma 5.1.1] □

**Lemma 2.1.2.** *Let $\Gamma_1$ and $\Gamma_2$ be two congruence subgroups of $\mathrm{SL}_2(\mathbb{Z})$ and $\alpha \in GL_2^+(\mathbb{Q})$. Let $\Gamma_3 = \alpha^{-1}\Gamma_1\alpha \cap \Gamma_2$. Then the map $\Gamma_2 \to \Gamma_1\alpha\Gamma_2$ given by $\gamma_2 \mapsto \alpha\gamma_2$ induces a natural bijection form the coset space $\Gamma_3\backslash\Gamma_2$ to the orbit space $\Gamma_1\backslash\Gamma_1\alpha\Gamma_2$.*

*Proof.* Consider the surjective map $\Gamma_2 \to \Gamma_1\backslash\Gamma_1\alpha\Gamma_2$ given by $\gamma_2 \mapsto \Gamma_1\alpha\gamma_2$. Let $\gamma_2, \gamma_2' \in \Gamma_2$. Then $\Gamma_1\alpha\gamma_2 = \Gamma_1\alpha\gamma_2'$ if and only if $\gamma_2'\gamma_2^{-1} \in \alpha^{-1}\Gamma_1\alpha \cap \Gamma_2 = \Gamma_3$ if and only if $\Gamma_3\gamma_2' = \Gamma_3\gamma_2$. Thus the above map induces a bijection $\Gamma_3\backslash\Gamma_2 \to \Gamma_1\backslash\Gamma_1\alpha\Gamma_2$. □

We need one more lemma to go further

**Lemma 2.1.3.** *Let $\Gamma_1$ and $\Gamma_2$ be two congruence subgroups of $\mathrm{SL}_2(\mathbb{Z})$. Then $[\Gamma_1 : \Gamma_1 \cap \Gamma_2]$ is finite.*

*Proof.* There exists $N_1, N_2 \in \mathbb{Z}^+$ such that $\Gamma(N_1) \subset \Gamma_1$ and $\Gamma(N_2) \subset \Gamma_2$. Let $N_3 = \operatorname{lcm}(N_1, N_2)$. Hence $\Gamma(N_3) \subset \Gamma_1 \cap \Gamma_2$. Thus $[\Gamma_1 : \Gamma_1 \cap \Gamma_2] \leqslant [\Gamma_1 : \Gamma(N_3)] \leqslant [\mathrm{SL}_2(\mathbb{Z}) : \Gamma(N_3)] < \infty$. □

By Lemma **??**, $\alpha^{-1}\Gamma_1\alpha \ \cap \ \mathrm{SL}_2(\mathbb{Z})$ is a congruence subgroup of $\mathrm{SL}_2(\mathbb{Z})$ and by Lemma **??**, the index $[\Gamma_2 : \Gamma_3]$ is finite, where $\Gamma_3 = \alpha^{-1}\Gamma_1\alpha \ \cap \ \Gamma_2$. Hence by Lemma **??**, the orbit space $\Gamma_1\backslash\Gamma_1\alpha\Gamma_2$ is finite. Thus the union (**??**) is finite.

Now we can define the $\Gamma_1\alpha\Gamma_2$ operator. Let $\Gamma_1$ and $\Gamma_2$ be congruence subgroups of $\mathrm{SL}_2(\mathbb{Z})$ and $\alpha \in GL_2^+(\mathbb{Q})$. The weight-k $\Gamma_1\alpha\Gamma_2$ operator on $\mathcal{M}_k(\Gamma_1)$ is defined by

$$f[\Gamma_1\alpha\Gamma_2]_k = \sum_j f[\beta_j]_k, \qquad f \in \mathcal{M}_k(\Gamma_1),$$

where $\{\beta_j\}$ are orbit representatives. By the above discussion the sum is finite. The $[\Gamma_1\alpha\Gamma_2]_k$ operator is well-defined. Indeed; let $\beta$ and $\beta'$ represent the same orbit, i.e. $\Gamma_1\beta = \Gamma_1\beta'$. Then $\beta' = \gamma\beta$ for some $\gamma \in \Gamma_1$. As $f \in \mathcal{M}_k(\Gamma_1)$, $f[\beta']_k = f[\gamma\beta]_k = (f[\gamma]_k)[\beta]_k = f[\beta]_k$.

Our claim is that $f[\Gamma_1\alpha\Gamma_2]_k \in \mathcal{M}_k(\Gamma_2)$ for $f \in \mathcal{M}_k(\Gamma_1)$. To see this first let $\gamma_2 \in \Gamma_2$ and consider the map $\Gamma_1\backslash\Gamma_1\alpha\Gamma_2 \to \Gamma_1\backslash\Gamma_1\alpha\Gamma_2$ defined by $\Gamma_1\beta \mapsto \Gamma_1\beta\gamma_2$. This map is well-defined and bijective. Thus if $\{\beta_j\}$ is a set of orbit representatives then $\{\beta_j\gamma_2\}$ is also a set of orbit representatives. Hence we have

$$(f[\Gamma_1\alpha\Gamma_2]_k)[\gamma_2]_k = (\sum_j f[\beta_j]_k)[\gamma_2]_k = \sum_j f[\beta_j\gamma_2]_k = f[\Gamma_1\alpha\Gamma_2]_k.$$

This proves that $f[\Gamma_1\alpha\Gamma_2]_k$ is weight-$k$ invariant under $\Gamma_2$.

Now we need to show that $f[\Gamma_1\alpha\Gamma_2]_k$ is holomorphic at the cusps. For any $\gamma \in GL_2^+(\mathbb{Q})$ extend the definition of weight-$k$ operator to $GL_2^+(\mathbb{Q})$ by $(f[\gamma]_k)(\tau) = (\det\gamma)^{k-1}j(\gamma,\tau)^{-k}f(\gamma(\tau))$ where $f : \mathcal{H} \to \mathbb{C}$. It is easy to see that $[\gamma\gamma']_k = [\gamma]_k[\gamma']_k$ for all $\gamma, \gamma' \in GL_2^+(\mathbb{Q})$.

**Lemma 2.1.4.** *Let $\gamma \in GL_2^+(\mathbb{Q})$ and $\Gamma$ be a congruence subgroup of $\mathrm{SL}_2(\mathbb{Z})$. Let $f \in \mathcal{M}_k(\Gamma)$. Then $f[\gamma]_k$ has a Fourier expansion.*

*Proof.* Let $\gamma = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right)$. Suppose $c = 0$. Then $\gamma = r\left(\begin{smallmatrix} a' & b' \\ 0 & d' \end{smallmatrix}\right)$ for some $r \in \mathbb{Q}^+$ and $a', b', d' \in \mathbb{Z}$ with $\gcd(a', b', d') = 1$. Now suppose $c \neq 0$. Let $a/c = a'/c'$ with $\gcd(a', c') = 1$. Let $\gamma' = \left(\begin{smallmatrix} * & * \\ c' & -a' \end{smallmatrix}\right) \in \mathrm{SL}_2(\mathbb{Z})$. Then $\gamma'\gamma = \left(\begin{smallmatrix} * & * \\ 0 & * \end{smallmatrix}\right) \in GL_2^+(\mathbb{Q})$ and as above $\gamma'\gamma = r\left(\begin{smallmatrix} a' & b' \\ 0 & d' \end{smallmatrix}\right)$. Thus in both cases $\gamma$ can be written as $\gamma = \alpha\gamma'$ for some $\alpha \in \mathrm{SL}_2(\mathbb{Z})$ and $\gamma' = r\left(\begin{smallmatrix} a' & b' \\ 0 & d' \end{smallmatrix}\right)$ with $a', b', d' \in \mathbb{Z}$ are relatively prime. Since $f \in \mathcal{M}_k(\Gamma)$, $f[\alpha]_k$ has a Fourier expansion. Hence $f[\gamma]_k = (\det\gamma')^{k-1}(rd')^{-k}(f[\alpha]_k)(\frac{a'\tau+b'}{d'})$ has a Fourier expansion. If $f[\alpha]_k$ has period $h \in \mathbb{Z}^+$ then we have

$$(f[\gamma]_k)(\tau) = (\det\gamma')^{k-1}(rd')^{-k}\sum_{n \geqslant 0} a_n e^{2\pi i(a'\tau+b')n/d'h}.$$

This proves that if constant term of $f[\alpha]_k$ is zero then constant term of $f[\gamma]_k$ is also zero. □

Now let $\delta \in \mathrm{SL}_2(\mathbb{Z})$. We have to show that $(f[\Gamma_1\alpha\Gamma_2]_k)[\delta]_k$ is holomorphic at $\infty$. $(f[\Gamma_1\alpha\Gamma_2]_k)[\delta]_k$ is a sum of the functions $g_j = f[\beta_j\delta]_k$. Since $\beta_j\delta \in GL_2^+(\mathbb{Q})$, by Lemma **??**, $g_j$ is holomorphic at $\infty$. Let $h_j$ be the period of $g_j$ and let $h = \mathrm{lcm}(h_j)$. Then the sum $(f[\Gamma_1\alpha\Gamma_2]_k)[\delta]_k$ has period $h$. Each $g_j$ has a Fourier expansion

$$g_j(\tau) = \sum_{n \geqslant 0} b_n(g_j)q_h^n.$$

Thus the sum $(f[\Gamma_1\alpha\Gamma_2]_k)[\delta]_k$ has a Fourier expansion. Hence we proved that $f[\Gamma_1\alpha\Gamma_2]_k$ is holomorphic at cusps and this shows that the weight-$k$ $\Gamma_1\alpha\Gamma_2$ operator is

$$[\Gamma_1\alpha\Gamma_2]_k : \mathcal{M}_k(\Gamma_1) \to \mathcal{M}_k(\Gamma_2).$$

Moreover, if $f \in \mathcal{S}_k(\Gamma_1)$ then by the last part of the proof of Lemma **??** and above discussion combines to show that $f[\Gamma_1\alpha\Gamma_2]_k \in \mathcal{S}_k(\Gamma_2)$, that is,

$$[\Gamma_1\alpha\Gamma_2]_k : \mathcal{S}_k(\Gamma_1) \to \mathcal{S}_k(\Gamma_2).$$

**Remarks**

1. Suppose $\Gamma_1 \supset \Gamma_2$ and take $\alpha = I$. Then $f[\Gamma_1\alpha\Gamma_2]_k = f$ and so the operator $[\Gamma_1\alpha\Gamma_2]_k$ is the natural inclusion of the subspace $\mathcal{M}_k(\Gamma_1)$ into $\mathcal{M}_k(\Gamma_2)$.

2. Suppose $\alpha^{-1}\Gamma_1\alpha = \Gamma_2$. Then $\Gamma_1\alpha\Gamma_2 = \Gamma_1\alpha$ and so $f[\Gamma_1\alpha\Gamma_2]_k = f[\alpha]_k$. Let $f \in \mathcal{M}_k(\Gamma_2)$ and $\gamma_1 \in \Gamma_1$. Then $(f[\alpha^{-1}]_k)[\gamma_1]_k = f[\alpha^{-1}\gamma_1]_k = (f[\alpha^{-1}\gamma_1\alpha]_k)[\alpha^{-1}]_k = f[\alpha^{-1}]_k$ as $\alpha^{-1}\gamma_1\alpha \in \Gamma_2$. The holomorphy conditions are also satisfied by Lemma **??** and so $f[\alpha^{-1}]_k \in \mathcal{M}_k(\Gamma_1)$. Hence $[\Gamma_2\alpha^{-1}\Gamma_1]_k$ is the inverse of $[\Gamma_1\alpha\Gamma_2]_k$ and so in this case

$$[\Gamma_1\alpha\Gamma_2]_k : \mathcal{M}_k(\Gamma_1) \xrightarrow{\sim} \mathcal{M}_k(\Gamma_2).$$

3. Suppose $\Gamma_1 \subset \Gamma_2$ and take $\alpha = I$. Let $\{\gamma_j\}$ be coset representatives of $\Gamma_1\backslash\Gamma_2$ and so $f[\Gamma_1\alpha\Gamma_2]_k = \sum_j f[\gamma_j]_k$. In this case $[\Gamma_1\alpha\Gamma_2]_k$ is the projection of $\mathcal{M}_k(\Gamma_1)$ onto its subspace $\mathcal{M}_k(\Gamma_2)$.

Let $\Gamma_1$ and $\Gamma_2$ be any two congruence subgroups and $\alpha \in GL_2^+(\mathbb{Q})$. Then the double coset operator $[\Gamma_1\alpha\Gamma_2]_k$ can be written as a composition of the above cases. To see this, let $\Gamma_3 = \alpha^{-1}\Gamma_1\alpha \cap \Gamma_2$ and $\Gamma_3' = \alpha\Gamma_3\alpha^{-1} = \Gamma_1 \cap \alpha\Gamma_2\alpha^{-1}$. Then we have $\Gamma_3' \subset \Gamma_1$, $\alpha^{-1}\Gamma_3'\alpha = \Gamma_3$ and $\Gamma_3 \subset \Gamma_2$. Thus the corresponding double coset operators gives

$$\begin{tikzcd}
\mathcal{M}_k(\Gamma_1) \arrow[r, hook, "{[\Gamma_1\alpha\Gamma_3']_k}"] & \mathcal{M}_k(\Gamma_3') \arrow[r, "{[\Gamma_3'\alpha\Gamma_3]_k}"] & \mathcal{M}_k(\Gamma_3) \arrow[r, two heads, "{[\Gamma_3\alpha\Gamma_2]_k}"] & \mathcal{M}_k(\Gamma_2)
\end{tikzcd}$$

$f \longmapsto f \longmapsto f[\alpha]_k \longmapsto \sum_j f[\alpha\gamma_j]_k$ , where $\gamma_j$ are coset representatives of $\Gamma_3\backslash\Gamma_2$. By Lemma **??**, $\alpha\gamma_j$ are the orbit representatives of $\Gamma_1\backslash\Gamma_1\alpha\Gamma_2$ and so the composition is the double coset operator $[\Gamma_1\alpha\Gamma_2]_k$.

The double coset operator $[\Gamma_1\alpha\Gamma_2]_k$ has an interpretation in terms of modular curves and their divisor groups. First note that we have

$$\begin{tikzcd}
\Gamma_3 \arrow[r] \arrow[d] & \Gamma_3' \arrow[d] \\
\Gamma_2 & \Gamma_1
\end{tikzcd}$$

where the top row is the isomorphism $\gamma \mapsto \alpha\gamma\alpha^{-1}$ and the other maps are inclusions. Thus in terms of modular curves we have

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

where the top row is the isomorphism $\Gamma_3\tau \mapsto \Gamma_3'\alpha(\tau)$ and $\pi_1$ and $\pi_2$ are natural maps. Considering modular curves as compact Riemann surfaces the maps in the above diagram are holomorphic. Let $\Gamma_3\backslash\Gamma_2 = \bigcup_j \Gamma_3\gamma_j$ and $\beta_j = \alpha\gamma_j$ for all $j$ and so $\Gamma_1\alpha\Gamma_2 = \bigcup_j \Gamma_1\beta_j$. Each point of $X_2$ is mapped by $\pi_1 \circ \alpha \circ \pi_2^{-1}$ to a set of points of $X_1$

$$\begin{tikzcd}
\{\Gamma_3\gamma_j(\tau)\} \arrow[r] & \{\Gamma_3'\beta_j(\tau)\} \arrow[d, "\pi_1"] \\
\Gamma_2\tau \arrow[u, "\pi_2^{-1}"] & \{\Gamma_1\beta_j(\tau)\}
\end{tikzcd}$$

In terms of divisors the composition $[\Gamma_1\alpha\Gamma_2]_k : X_2 \to \mathrm{Div}(X_1)$ is given by $\Gamma_2\tau \mapsto \sum_j \Gamma_1\beta_j(\tau)$. Extend this linearly to $\mathrm{Div}(X_2)$ to obtain a homomorphism between divisor groups

$$[\Gamma_1\alpha\Gamma_2]_k : \mathrm{Div}(X_2) \to \mathrm{Div}(X_1).$$

**Remarks**

1. Suppose $\Gamma_2 \subset \Gamma_1$. Then corresponding group homomorphism between divisor groups is a surjection.

2. Suppose $\alpha^{-1}\Gamma_1\alpha = \Gamma_2$. Then divisor groups of $\Gamma_1$ and $\Gamma_2$ are isomorphic under $[\Gamma_1\alpha\Gamma_2]_k$.

3. Suppose $\Gamma_2 \supset \Gamma_1$. Then $[\Gamma_1\alpha\Gamma_2]_k$ is an injection.

Now we are ready to define $\langle d\rangle$ and $T_p$ operators. Recall from Section **??** that we have an isomorphism $\Gamma_0(N)/\Gamma_1(N) \xrightarrow{\sim} (\mathbb{Z}/N\mathbb{Z})^*$ defined by $\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \mapsto d \mod N$. Let $\alpha \in \Gamma_0(N)$ and consider the double coset operator

$$[\Gamma_1(N)\alpha\Gamma_1(N)]_k : \mathcal{M}_k(\Gamma_1(N)) \to \mathcal{M}_k(\Gamma_1(N))$$

given by $f[\Gamma_1(N)\alpha\Gamma_1(N)]_k = f[\alpha]_k$ for $f \in \mathcal{M}_k(\Gamma_1(N))$. Hence $f[\alpha]_k \in \mathcal{M}_k(\Gamma_1(N))$ and so $\Gamma_0(N)$ acts on $\mathcal{M}_k(\Gamma_1(N))$. Since $\Gamma_1(N)$ acts trivially the quotient $(\mathbb{Z}/N\mathbb{Z})^*$ acts on $\mathcal{M}_k(\Gamma_1(N))$. Hence we have an operator

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

given by $\langle d\rangle f = f[\alpha]_k$ for any $\alpha = \left(\begin{smallmatrix} a & b \\ c & \delta \end{smallmatrix}\right) \in \Gamma_0(N)$ such that $\delta \equiv d \mod N$. This operator is called diamond operator. Now for any Dirichlet character $\chi : (\mathbb{Z}/N\mathbb{Z})^* \to \mathbb{C}^*$ the $\chi$-eigenspace is

$$\mathcal{M}_k(N, \chi) = \{f \in \mathcal{M}_k(\Gamma_1(N)) : \langle d\rangle f = \chi(d)f \text{ for all } d \in (\mathbb{Z}/N\mathbb{Z})^*\}$$

Thus $\langle d\rangle$ acts on the eigenspace of $\chi$ by multiplication by $\chi(d)$.

To define $T_p$ let $\alpha = \left(\begin{smallmatrix} 1 & 0 \\ 0 & p \end{smallmatrix}\right)$ for $p$ prime. Then $T_p$ is defined to be the double coset operator $[\Gamma_1(N)\alpha\Gamma_1(N)]_k$. Thus

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

is defined by $f \mapsto f[\Gamma_1(N)\alpha\Gamma_1(N)]_k$. The following proposition gives the explicit representation of $T_p$.

**Propositition 2.1.1.** *$T_p$ defined as above is given by*

$$T_p f = \begin{cases} \sum\limits_{j=0}^{p-1} f[\left(\begin{smallmatrix} 1 & j \\ 0 & p \end{smallmatrix}\right)]_k & if\ p|N \\ \sum\limits_{j=0}^{p-1} f[\left(\begin{smallmatrix} 1 & j \\ 0 & p \end{smallmatrix}\right)]_k + f[\left(\begin{smallmatrix} m & n \\ 0 & p \end{smallmatrix}\right)\left(\begin{smallmatrix} p & 0 \\ 0 & 1 \end{smallmatrix}\right)]_k & if\ p \nmid N,\ where\ mp - nN = 1 \end{cases}$$

*Proof.* Let $\Gamma^0(p) = \{\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \mathrm{SL}_2(\mathbb{Z}) : \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \equiv \left(\begin{smallmatrix} * & 0 \\ * & * \end{smallmatrix}\right) (\text{mod } p)\}$ and define $\Gamma_1^0(N,p) = \Gamma_1(N) \cap \Gamma^0(p)$. Let $\Gamma_3 = \alpha^{-1}\Gamma_1(N)\alpha \cap \Gamma_1(N)$. First we show that $\Gamma_3 = \Gamma_1^0(N,p)$. Let $\gamma \in \Gamma_3$. Then $\gamma \in \Gamma_1(N)$ and $\gamma = \alpha^{-1}\gamma_3\alpha$ for some $\gamma_3 \in \Gamma_1(N)$. An easy computation shows that $\alpha^{-1}\gamma_3\alpha \in \Gamma^0(p)$ hence $\gamma \in \Gamma_1(N) \cap \Gamma^0(p) = \Gamma_1^0(N,p)$. Conversely, let $\gamma = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \Gamma_1^0(N,p)$. Then $\alpha\gamma\alpha^{-1} = \left(\begin{smallmatrix} a & b/p \\ pc & d \end{smallmatrix}\right) \in \Gamma_1(N)$ and so $\gamma \in \alpha^{-1}\Gamma_1(N)\alpha$.

Let $\gamma_j = \left(\begin{smallmatrix} 1 & j \\ 0 & 1 \end{smallmatrix}\right)$ for $0 \leqslant j < p$. Given $\gamma \in \Gamma_1(N)$, then $\gamma \in \Gamma_3\gamma_j$ if $\gamma\gamma_j^{-1} \in \Gamma_3 = \Gamma_1(N) \cap \Gamma^0(p)$. Clearly $\gamma\gamma_j^{-1} \in \Gamma_1(N)$ for all $j$. But we also need the upper right entry $b - aj$ of $\gamma\gamma_j^{-1} = \left(\begin{smallmatrix} a & b-aj \\ c & d-cj \end{smallmatrix}\right)$ to be 0 (mod $p$). Suppose $p \nmid a$. Then let $j = ba^{-1}$ (mod $p$) and so $\gamma\gamma_j^{-1} \in \Gamma_3$. Now suppose $p \mid a$. Then $b - ja \not\equiv 0$ (mod $p$) since otherwise $p \mid b$ and $p \mid ad - bc = 1$. $p \mid a$ if and only if $p \nmid N$. In this case let $\gamma_\infty = \left(\begin{smallmatrix} mp & n \\ N & 1 \end{smallmatrix}\right)$ where $mp - nN = 1$. Now $\gamma\gamma_\infty^{-1} \in \Gamma_3$. Thus $\gamma_0, ..., \gamma_{p-1}$ are coset representatives of $\Gamma_3 \backslash \Gamma_1(N)$ when $p \mid N$ and $\gamma_\infty$ is also required when $p \nmid N$. Hence the corresponding orbit representatives of $\Gamma_1(N) \backslash \Gamma_1(N)\alpha\Gamma_1(N)$ are

$$\beta_j = \alpha\gamma_j = \left(\begin{smallmatrix} 1 & j \\ 0 & p \end{smallmatrix}\right) \text{ for } 0 \leqslant j < p, \quad \beta_\infty = \left(\begin{smallmatrix} m & n \\ N & p \end{smallmatrix}\right)\left(\begin{smallmatrix} p & 0 \\ 0 & 1 \end{smallmatrix}\right) \text{ if } p \nmid N. \tag{2.2}$$

This finishes the proof. □

The next proposition describes the effect of $T_p$ on the Fourier coefficients. Before that we need the following lemma.

**Lemma 2.1.5.** *Let $f \in \mathcal{M}_k(\Gamma_1(N))$. Then $\langle d\rangle(T_pf) = T_p(\langle d\rangle f)$. That is the two kinds of Hecke operator commute.*

*Proof.* Let $\alpha = \left(\begin{smallmatrix} 1 & 0 \\ 0 & p \end{smallmatrix}\right)$ and $\gamma \in \Gamma_0(N)$. Then a simple computation shows that $\gamma\alpha\gamma^{-1} \equiv \left(\begin{smallmatrix} 1 & * \\ 0 & p \end{smallmatrix}\right) \pmod N$. The double coset $\Gamma_1(N)\alpha\Gamma_1(N)$ is

$$\Gamma_1(N)\alpha\Gamma_1(N) = \left\{\gamma \in \mathrm{M}_2(\mathbb{Z}) : \gamma \equiv \left(\begin{smallmatrix} 1 & * \\ 0 & p \end{smallmatrix}\right) \pmod N,\ \det\gamma = p\right\}.$$

For the proof of this see [**?**, Chapter 3]. If $\Gamma_1(N)\alpha\Gamma_1(N) = \bigcup_j \Gamma_1(N)\beta_j$ then by the above description of $\Gamma_1(N)\alpha\Gamma_1(N)$ we have $\Gamma_1(N)\alpha\Gamma_1(N) = \Gamma_1(N)\gamma\alpha\gamma^{-1}\Gamma_1(N) = \gamma\Gamma_1(N)\alpha\Gamma_1(N)\gamma^{-1} = \bigcup_j \Gamma_1(N)\gamma\beta_j\gamma^{-1}$. Thus

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

This is true for all $\gamma \in \Gamma_0(N)$. Choose $\gamma \in \Gamma_0(N)$ with lower right entry $\delta \equiv d \pmod N$ and so we have

$$\langle d\rangle T_pf = \sum_j f[\beta_j\gamma]_k = \sum_j f[\gamma\beta_j]_k = T_p\langle d\rangle f.$$

□

**Proposititon 2.1.2.** *Let $f \in \mathcal{M}_k(\Gamma_1(N))$. Since $\left(\begin{smallmatrix} 1 & 1 \\ 0 & 1 \end{smallmatrix}\right) \in \Gamma_1(N)$, $f$ has period 1 and hence has a Fourier expansion*

$$f(\tau) = \sum_{n=0}^{\infty} a_n(f)q^n, \qquad q = e^{2\pi i\tau}.$$

*Then*

1. *Let $\mathbf{1_N} : (\mathbb{Z}/N\mathbb{Z})^* \to \mathbb{C}^*$ be the trivial character modulo $N$. Then $T_pf$ has Fourier expansion*

$$(T_pf)(\tau) = \sum_{n=0}^{\infty}(a_{np}(f) + \mathbf{1_N}(p)p^{k-1}a_{n/p}(\langle d\rangle f))q^n$$

*That is*

$$a_n(T_pf) = a_{np}(f) + \mathbf{1_N}(p)p^{k-1}a_{n/p}(\langle d\rangle f) \tag{2.3}$$

*for $f \in \mathcal{M}_k(\Gamma_1(N))$.*

*2. Let $\chi : (\mathbb{Z}/N\mathbb{Z})^* \to \mathbb{C}^*$ be any character. If $f \in \mathcal{M}_k(N,\chi)$ then $T_pf \in \mathcal{M}_k(N,\chi)$ and the Fourier expansion is*

$$(T_pf)(\tau) = \sum_{n=0}^{\infty}(a_{np}(f) + \chi(p)p^{k-1}a_{n/p}(f))q^n$$

*That is*

$$a_n(T_pf) = a_{np}(f) + \chi(p)p^{k-1}a_{n/p}(f) \tag{2.4}$$

*for $f \in \mathcal{M}_k(N,\chi)$.*

*Proof.* For part (1), let $0 \leqslant j < p$. Then

$$f[\left(\begin{smallmatrix} 1 & j \\ 0 & p \end{smallmatrix}\right)]_k(\tau) = \frac{1}{p}f\left(\frac{\tau+j}{p}\right) = \frac{1}{p}\sum_{n=0}^{\infty}a_n(f)e^{2\pi i n(\tau+j)/p} = \frac{1}{p}\sum_{n=0}^{\infty}a_n(f)q_p^n\mu_p^{nj}.$$

Suppose $p \mid N$. Since $\sum_{j=0}^{p-1}\mu_p^{nj}$ is equal to $p$ when $p \mid n$ and $0$ when $p \nmid n$, summing over $j$ gives $(T_pf)(\tau) = \sum_{j=0}^{p-1} f[\left(\begin{smallmatrix} 1 & j \\ 0 & p \end{smallmatrix}\right)]_k(\tau) = \sum_{p|n} a_n(f)q_p^n = \sum_{n=0}^{\infty} a_{np}(f)q^n$. Suppose $p \nmid N$. Then we have an additional term

$$f[\left(\begin{smallmatrix} m & n \\ N & p \end{smallmatrix}\right)\left(\begin{smallmatrix} p & 0 \\ 0 & 1 \end{smallmatrix}\right)]_k(\tau) = (\langle p\rangle f)[\left(\begin{smallmatrix} p & 0 \\ 0 & 1 \end{smallmatrix}\right)]_k(\tau) = p^{k-1}(\langle p\rangle f)(p\tau) = p^{k-1}\sum_{n=0}^{\infty}a_n(\langle p\rangle f)q^{np}.$$

This proves part (1) of the proposition.

For part (b) note that by Lemma **??** we have $\langle d\rangle T_pf = T_p\langle d\rangle f = T_p\chi(d)f = \chi(d)T_pf$. Thus $T_pf \in \mathcal{M}_k(N,\chi)$. Formula (**??**) follows from (**??**). □

We have seen that the two types of Hecke operator commute. It is also true that they commute with themselves.

**Propositon 2.1.3.** *Let $d, e \in (\mathbb{Z}/N\mathbb{Z})^*$ and $p$ and $q$ be primes. Then*

1. $\langle d\rangle\langle e\rangle = \langle e\rangle\langle d\rangle = \langle de\rangle$

2. $T_pT_q = T_qT_p$

*Proof.* Since $\langle d\rangle$ and $T_p$ operators preserve the decomposition $\mathcal{M}_k(\Gamma_1(N)) = \bigoplus_{\chi} \mathcal{M}_k(N,\chi)$ it is enough to check the above equalities for $f \in \mathcal{M}_k(N,\chi)$. Let $f \in \mathcal{M}_k(N,\chi)$. Then $\langle d\rangle\langle e\rangle f = \langle d\rangle\chi(e)f = \chi(d)\chi(e)f = \chi(ed)f = \langle ed\rangle f$. For the second equality by formula (**??**) of Proposition **??** we have

$$\begin{aligned}
a_n(T_p(T_qf)) &= a_{np}(T_qf) + \chi(p)p^{k-1}a_{n/p}(T_qf)\\
&= a_{npq}(f) + \chi(q)q^{k-1}a_{np/q}(f) + \chi(p)p^{k-1}(a_{nq/p}(f) + \chi(q)q^{k-1}a_{n/pq}(f))\\
&= a_{npq}(f) + \chi(q)q^{k-1}a_{np/q}(f) + \chi(p)p^{k-1}a_{nq/p}(f) + \chi(pq)(pq)^{k-1}a_{n/pq}(f))\\
&= a_n(T_q(T_pf))
\end{aligned}$$

The last equality follows from the symmetry between $p$ and $q$. □

As we have seen before the double coset operators has a modular curve interpretation so does $T_p$

$$T_p : \mathrm{Div}(X_1(N)) \to \mathrm{Div}(X_1(N)), \qquad \Gamma_1(N)\tau \mapsto \sum_j \Gamma_1(N)\beta_j(\tau) \tag{2.5}$$

where $\beta_j$ are coset representatives from (**??**).

$T_p$ also has an interpretation in terms of the moduli space $S_1(N)$ from Section **??**. To construct this let $\Lambda_\tau = \tau\mathbb{Z} \oplus \mathbb{Z}$ and $E_\tau = \mathbb{C}/\Lambda_\tau$ for $\tau \in \mathcal{H}$. For each $j$ let $C_j = c\Lambda_{\beta_j(\tau)}$ where $c \in \mathbb{C}$.

**Lemma 2.1.6.** *Using the above notation $C_j = \langle(\tau + j)/p\rangle + \Lambda_\tau$ for $0 \leqslant j < p$ and $C_j = \langle 1/p\rangle + \Lambda_\tau$ for $j = \infty$.*

*Proof.* Let $0 \leqslant j < p$. Note that $\langle(\tau + j)/p\rangle + \Lambda_\tau = (\tau + j)/p\mathbb{Z} + \tau\mathbb{Z} \oplus \mathbb{Z}$ and $\Lambda_{\beta_j(\tau)} = (\tau + j)/p\mathbb{Z} \oplus \mathbb{Z}$. Clearly we have $\Lambda_{\beta_j(\tau)} \subset \langle(\tau + j)/p\rangle + \Lambda_\tau$. Conversely let $\alpha \in \langle(\tau + j)/p\rangle + \Lambda_\tau$. Hence $\alpha = n(\tau + j)/p + \tau m + k$ for some $n, m, k \in \mathbb{Z}$. Since $\tau = p(\tau + j)/p - j$ we have $\alpha = n(\tau + j)/p + (p(\tau + j)/p - j)m + k \in \Lambda_{\beta_j(\tau)}$.

Now let $j = \infty$ and $\gamma = \left(\begin{smallmatrix} m & n \\ N & p \end{smallmatrix}\right)$. Then $(Np\tau + p)\Lambda_{\gamma(p\tau)} = \Lambda_{p\tau}$. Multiply by $1/p$ and so $(N\tau + 1)\Lambda_{\beta_\infty(\tau)} = \tau\mathbb{Z} \oplus (1/p)\mathbb{Z} = \langle 1/p\rangle + \Lambda_\tau$. □

By Lemma **??** we have $C_j \cong \mathbb{Z}/p\mathbb{Z}$ as a subgroup of $E_\tau$ and $C_j \cap (\langle 1/N\rangle + \Lambda_\tau) = \{0\}$. Now the groups $C_j$ are subgroups of $E_\tau[p]$ and $C_i \cap C_j = \{0\}$ when $i \neq j$. Hence $\bigcup_j C_j$ is a subset of $E_\tau[p]$ with $p^2$ elements. Thus $E_\tau[p] = \bigcup_j C_j$. Any subgroup of $E_\tau$ isomorphic to $\mathbb{Z}/p\mathbb{Z}$ lie in $E_\tau[p]$ and equal to one of the $C_j$. Now we define

$$T_p : \mathrm{Div}(S_1(N)) \to \mathrm{Div}(S_1(N)), \qquad [E, Q] \mapsto \sum_C [E/C, Q + C] \tag{2.6}$$

where the sum is over all order $p$ subgroups $C$ of $E$ such that $C \cap \langle Q\rangle = \{0\}$. If $p \mid N$ the $C_\infty$ does not appear in the above sum.

The relation between (**??**) and (**??**) is given in the following commutative diagram:

$$\begin{tikzcd}
\mathrm{Div}(S_1(N)) \arrow[r, "T_p"] \arrow[d, "\psi_1"] & \mathrm{Div}(S_1(N)) \arrow[d, "\psi_1"] \\
\mathrm{Div}(Y_1(N)) \arrow[r, "T_p"] & \mathrm{Div}(Y_1(N))
\end{tikzcd} \tag{2.7}$$

where $\psi_1$ is the bijection between $S_1(N)$ and $Y_1(N)$ given in Section **??** and the maps are given as

$$\begin{tikzcd}
{[E_\tau, 1/N + \Lambda_\tau]} \arrow[r, "T_p"] \arrow[d, "\psi_1"] & \sum_C [E_\tau/C, 1/N + C] \arrow[d, "\psi_1"] \\
\Gamma_1(N)\tau \arrow[r, "T_p"] & \sum_j \Gamma_1(N)\beta_j(\tau)
\end{tikzcd}$$

To see that this diagram commutes it is enough to check that given $\tau \in \mathcal{H}$, for each $j$ we have $\psi_1([E_\tau/C_j, 1/N + C_j]) = \Gamma_1(N)\beta_j(\tau)$. For $0 \leqslant j < p$ by Lemma **??**,

$C_j = \Lambda_{\beta_j(\tau)}$ and so $[E_\tau/C_j, 1/N + C_j] = [E_{\beta_j(\tau)}, 1/N + \Lambda_{\beta_j(\tau)}]$. In the case $p \nmid N$, $j = \infty$ is also included and again by Lemma **??**, $C_\infty = \langle 1/p \rangle + \Lambda_\tau$ and so as a lattice $C_\infty = \tau\mathbb{Z} \oplus (1/p)\mathbb{Z}$. Now considering $C_\infty$ as a subgroup of $E_\tau$, $E_\tau/C_\infty \cong E_{p\tau}$ under multiplication by $p$ map. Thus $[E_\tau/C_\infty, 1/N + C_\infty] = [E_{p\tau}, p/N + \Lambda_{p\tau}]$ and so by the proof of Theorem **??** we have $[E_{p\tau}, p/N + \Lambda_{p\tau}] = [E_{\beta_j(\tau)}, 1/N + \Lambda_{\beta_j(\tau)}]$. Thus $\psi_1([E_\tau/C_\infty, 1/N + C_\infty]) = \Gamma_1(N)p\tau = \Gamma_1(N)\beta_\infty(\tau)$.

There is a similar commutative diagram for the diamond operator

$$\begin{tikzcd} S_1(N) \arrow[r, "\langle d \rangle"] \arrow[d, "\psi_1"] & S_1(N) \arrow[d, "\psi_1"] \\ Y_1(N) \arrow[r, "\langle d \rangle"] & Y_1(N) \end{tikzcd} \tag{2.8}$$

where the maps are given by

$$\begin{tikzcd} {[E_\tau, 1/N + \Lambda_\tau]} \arrow[r, "\langle d \rangle"] \arrow[d, "\psi_1"] & {[E_\tau, d/N + \Lambda_\tau]} \arrow[d, "\psi_1"] \\ \Gamma_1(N)\tau \arrow[r, "\langle d \rangle"] & \Gamma_1(N)\alpha(\tau) \end{tikzcd}$$

where $\alpha = \left(\begin{smallmatrix} a & b \\ c & \delta \end{smallmatrix}\right) \in \Gamma_0(N)$ with $\delta \equiv d \pmod{N}$.

## 2.2 The $\langle n \rangle$ and $T_n$ operators

In this section we extend the definition of $\langle d \rangle$ and $T_p$ operators to all of $\mathbb{Z}^+$.

For $n \in \mathbb{Z}^+$ with $(n, N) = 1$, $\langle n \rangle$ is determined by $n(\text{mod } N)$. For $(n, N) > 1$ define $\langle n \rangle = 0$. Then the map $n \mapsto \langle n \rangle$ is multiplicative.

Defining $T_n$ is more complicated. First set $T_1 = 1$. We have already defined $T_p$ for primes $p$. For prime powers, inductively

$$T_{p^r} = T_p T_{p^{r-1}} - p^{k-1}\langle p \rangle T_{p^{r-2}}, \qquad r \geqslant 2 \tag{2.9}$$

By Proposition **??** and induction, for distinct primes $p$ and $q$ we have $T_{p^r}T_{q^s} = T_{q^s}T_{p^r}$ and so we can extend the prime power definition (**??**) to $T_n$ multiplicatively using

$$T_n = \prod_i T_{p^{e_i}}, \qquad n = \prod_i p^{e_i}.$$

Thus $T_nT_m = T_mT_n$ for all $m, n \in \mathbb{Z}^+$ by Proposition **??** and $T_{mn} = T_mT_n$ if $(n, m) = 1$.

Proposition **??** generalizes to

**Propositition 2.2.1.** *Let $f \in \mathcal{M}_k(\Gamma_1(N))$ have Fourier expansion*

$$f(\tau) = \sum_{m=0}^{\infty} a_m(f)q^m.$$

*Then for all $n \in \mathbb{Z}^+$, $T_nf$ has the following Fourier expansion*

$$(T_nf)(\tau) = \sum_{m=0}^{\infty} a_m(T_nf)q^m$$

*where*

$$a_m(T_nf) = \sum_{d|(m,n)} d^{k-1}a_{mn/d^2}(\langle d\rangle f). \tag{2.10}$$

*If $f \in \mathcal{M}_k(N, \chi)$ then*

$$a_m(T_nf) = \sum_{d|(m,n)} \chi(d)d^{k-1}a_{mn/d^2}(f). \tag{2.11}$$

*Proof.* As in the proof of Proposition **??** we may assume $f \in \mathcal{M}_k(N, \chi)$ and so it suffices to check formula (**??**). The case $n = 1$ is trivial. Now let $n = p$ be a prime. Then

$$\sum_{d|(m,p)} \chi(d)d^{k-1}a_{mp/d^2}(f) = a_{mp}(f) + \chi(p)p^{k-1}a_{m/p}(f) = a_m(T_pf)$$

where the second equality follows from Proposition **??**.

Now let $r \geqslant 2$ and assume (**??**) holds for $n = 1, p, ..., p^{r-1}$. Then

$$\begin{aligned}
a_m(T_{p^r} f) &= a_m(T_p(T_{p^{r-1}} f)) - p^{k-1} a_m(\langle p \rangle)(T_{p^{r-2}} f) && \text{by (\textbf{??})} \\
&= a_{mp}(T_{p^{r-1}} f) + \chi(p) p^{k-1} a_{m/p}(T_{p^{r-1}} f) - \chi(p) p^{k-1} a_m(T_{p^{r-2}} f) && \text{by (\textbf{??})} \\
&= \sum_{d|(mp,p^{r-1})} \chi(d) d^{k-1} a_{mp^r/d^2}(f) \\
&+ \chi(p) p^{k-1} \sum_{d|(m/p,p^{r-1})} \chi(d) d^{k-1} a_{mp^{r-2}/d^2}(f) \\
&- \chi(p) p^{k-1} \sum_{d|(m,p^{r-2})} \chi(d) d^{k-1} a_{mp^{r-2}/d^2}(f) && \text{by induction hypothesis}
\end{aligned}$$

The first sum above is $a_{mp^r}(f) + \sum_{\substack{d|(mp,p^{r-1}) \\ d>1}} \chi(d) d^{k-1} a_{mp^r/d^2}(f)$ and

$$\sum_{\substack{d|(mp,p^{r-1}) \\ d>1}} \chi(d) d^{k-1} a_{mp^r/d^2}(f) = \chi(p) p^{k-1} \sum_{d|(m,p^{r-2})} \chi(d) d^{k-1} a_{mp^{r-2}/d^2}(f).$$

Thus $a_m(T_{p^r} f) = a_{mp^r}(f) + \chi(p) p^{k-1} \sum_{d|(m/p,p^{r-1})} \chi(d) d^{k-1} a_{mp^{r-2}/d^2}(f)$. Now it is easy to see that the right-hand side is formula (**??**) with $n = p^r$.

Now let $n_1, n_2 \in \mathbb{Z}^+$ be such that $(n_1, n_2) = 1$. Then

$$\begin{aligned}
a_m(T_{n_1}(T_{n_2} f)) &= \sum_{d|(m,n_1)} \chi(d) d^{k-1} a_{mn_1/d^2}(T_{n_2} f) \\
&= \sum_{d|(m,n_1)} \chi(d) d^{k-1} \sum_{e|(mn_1/d^2,n_2)} \chi(e) e^{k-1} a_{mn_1 n_2/d^2 e^2}(f)
\end{aligned}$$

and this is formula (**??**) with $n = n_1 n_2$. This finishes the proof. □

## 2.3 The Petersson inner product

In this section we define an inner product on $\mathcal{S}_k(\Gamma_1(N))$ which makes it an inner product space.

The hyperbolic measure on $\mathcal{H}$ is defined as

$$d\mu(\tau) = \frac{dxdy}{y^2}, \qquad \tau = x + iy \in \mathcal{H}.$$

$d\mu$ is $\mathrm{SL}_2(\mathbb{Z})$-invariant. Since $\mathbb{Q} \cup \{\infty\}$ is countable its measure is zero and so $d\mu$ is enough to integrate on $\mathcal{H}^*$. The fundamental domain of $\mathcal{H}^*$ is defined as the set

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

That is every point $\tau \in \mathcal{H}^*$ is $\mathrm{SL}_2(\mathbb{Z})$ equivalent to a point in $\mathcal{D}^*$.

**Lemma 2.3.1.** *For any bounded function $\varphi : \mathcal{H} \to \mathbb{C}$ and any $\alpha \in \mathrm{SL}_2(\mathbb{Z})$, the integral $\int_{\mathcal{D}^*} \varphi(\alpha(\tau))d\mu(\tau)$ converges.*

*Proof.* $\left|\int_{\mathcal{D}^*} \varphi(\alpha(\tau))d\mu(\tau)\right| \leqslant \int_{\mathcal{D}^*} |\varphi(\alpha(\tau))|d\mu(\tau) \leqslant M \int_{\mathcal{D}^*} \frac{dxdy}{y^2} = M \int_{1/2}^{\infty} \frac{dy}{y^2} < \infty$ □

Let $\Gamma$ be a congruence subgroup of $\mathrm{SL}_2(\mathbb{Z})$ and $\{\alpha_j\}$ be representatives of the coset space $\{\pm I\}\Gamma\backslash\mathrm{SL}_2(\mathbb{Z})$, i.e. $\mathrm{SL}_2(\mathbb{Z}) = \bigcup_j \{\pm I\}\Gamma\alpha_j$. Let $\varphi : \mathcal{H} \to \mathbb{C}$ be a $\Gamma$-invariant function. Then $\sum_j \int_{\mathcal{D}^*} \varphi(\alpha_j(\tau))d\mu(\tau)$ is independent of the choice if representatives $\alpha_j$. Since $d\mu$ is $\mathrm{SL}_2(\mathbb{Z})$-invariant

$$\sum_j \int_{\mathcal{D}^*} \varphi(\alpha_j(\tau))d\mu(\tau) = \int_{\bigcup_j \alpha_j(\mathcal{D}^*)} \varphi(\tau)d\mu(\tau).$$

Now $\bigcup_j \alpha_j(\mathcal{D}^*)$ represents the modular curve $X(\Gamma)$ hence we can make the following definition

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

Now we are ready to construct the Petersson inner product. Let $f, g \in \mathcal{S}_k(\Gamma)$ and define $\varphi(\tau) = f(\tau)\overline{g(\tau)}(\mathrm{Im}(\tau))^k$, for $\tau \in \mathcal{H}$. Then $\varphi$ is continuous and $\Gamma$-invariant. Let us see that $\varphi$ is bounded on $\mathcal{H}$. Since $\varphi$ is $\Gamma$-invariant it suffices to check that $\varphi$ is bounded on the union $\bigcup_j \alpha_j(\mathcal{D})$ and since the union is finite it suffices to show that $\varphi \circ \alpha$ is bounded on $\mathcal{D}$ for any $\alpha \in \mathrm{SL}_2(\mathbb{Z})$. Since $\varphi \circ \alpha$ is continuous, it is bounded on any compact subset of $\mathcal{D}$. Note that we have the following Fourier expansions for $f$ and $g$,

$$(f[\alpha]_k)(\tau) = \sum_{n=1}^{\infty} a_n(f[\alpha]_k)q_h^n, \qquad (g[\alpha]_k)(\tau) = \sum_{n=1}^{\infty} a_n(g[\alpha]_k)q_h^n$$

for some $h \in \mathbb{Z}^+$. Hence we have

$$\varphi(\alpha(\tau)) = (f[\alpha]_k)(\tau)\overline{(g[\alpha]_k)(\tau)}(\mathrm{Im}(\tau))^k = \mathcal{O}(q_h)^2(\mathrm{Im}(\tau))^k$$

as $\mathrm{Im}(\tau) \to 0$. Because of the exponential decay $\varphi(\alpha(\tau)) \to 0$ as $\mathrm{Im}(\tau) \to 0$ and so $\varphi \circ \alpha$ is bounded on $\mathcal{D}$. Thus the integral in the next definition makes sense.

**Definition 2.3.1.** *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 defined by*

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

*where $V_\Gamma = \int_{X(\Gamma)} d\mu(\tau)$ is the volume of $X(\Gamma)$.*

The Petersson inner product defined as above is linear in $f$, conjugate linear in $g$ and positive definite.

Now we compute the adjoints of the Hecke operators $T_n$ and $\langle n\rangle$. Let $\Gamma \subset \mathrm{SL}_2(\mathbb{Z})$ be a congruence subgroup and $\mathrm{SL}_2(\mathbb{Z}) = \bigcup_j \{\pm I\}\Gamma\alpha_j$. Then for $\alpha \in GL_2^+(\mathbb{Q})$ we have a bijection $\alpha^{-1}\Gamma\alpha\backslash\mathcal{H}^* \to X(\Gamma)$ given by $\alpha^{-1}\Gamma\alpha\tau \mapsto \Gamma\alpha(\tau)$. Thus the space $\alpha^{-1}\Gamma\alpha\backslash\mathcal{H}^*$ is represented by $\bigcup_j \alpha^{-1}\alpha_j(\mathcal{D}^*)$ up to some boundary identification. Similar to the definition of the above integral we can define for continuous, bounded, $\alpha^{-1}\Gamma\alpha$-invariant functions $\varphi : \mathcal{H} \to \mathbb{C}$

$$\int_{\alpha^{-1}\Gamma\alpha\backslash\mathcal{H}^*} \varphi(\tau)d\mu(\tau) = \sum_j \int_{\mathcal{D}^*} \varphi(\alpha^{-1}\alpha_j(\tau))d\mu(\tau).$$

We need the following lemma to go further.

**Lemma 2.3.2.** *Let* $\Gamma \subset \mathrm{SL}_2(\mathbb{Z})$ *be a congruence subgroup and* $\alpha \in GL_2^+(\mathbb{Q})$*.*

1. *If* $\varphi : \mathcal{H} \to \mathbb{C}$ *is continuous, bounded, and* $\Gamma$*-invariant, then*
$$\int_{\alpha^{-1}\Gamma\alpha\backslash\mathcal{H}^*} \varphi(\alpha(\tau))d\mu(\tau) = \int_{X(\Gamma)} \varphi(\tau)d\mu(\tau).$$

2. *If* $\alpha^{-1}\Gamma\alpha \subset \mathrm{SL}_2(\mathbb{Z})$ *then* $V_{\alpha^{-1}\Gamma\alpha} = V_\Gamma$ *and* $[\mathrm{SL}_2(\mathbb{Z}) : \alpha^{-1}\Gamma\alpha] = [\mathrm{SL}_2(\mathbb{Z}) : \Gamma]$*.*

3. *There exists* $\beta_1, ..., \beta_n \in GL_2^+(\mathbb{Q})$*, where* $n = [\Gamma : \alpha^{-1}\Gamma\alpha \cap \Gamma] = [\Gamma : \alpha\Gamma\alpha^{-1} \cap \Gamma]$*, such that*
$$\Gamma\alpha\Gamma = \bigcup_j \Gamma\beta_j = \bigcup_j \beta_j\Gamma$$

*Proof.* For part (1) note that since $\varphi$ is $\Gamma$-invariant, $(\varphi\circ\alpha)(\alpha^{-1}\gamma\alpha)(\tau) = \varphi(\gamma(\alpha(\tau))) = \varphi(\alpha(\tau))$ and so $\varphi \circ \alpha$ is $\alpha^{-1}\Gamma\alpha$-invariant. Thus
$$\int_{\alpha^{-1}\Gamma\alpha\backslash\mathcal{H}^*} \varphi(\alpha(\tau))d\mu(\tau) = \sum_j \int_{\mathcal{D}^*} \varphi(\alpha_j(\tau))d\mu(\tau) = \int_{X(\Gamma)} \varphi(\tau)d\mu(\tau).$$

For part (2) by the definition of the volume and part (1) we have
$$V_{\alpha^{-1}\Gamma\alpha} = \int_{\alpha^{-1}\Gamma\alpha\backslash\mathcal{H}^*} d\mu(\tau) = \int_{X(\Gamma)} d\mu(\tau) = V_\Gamma.$$

The volume and the index of $\Gamma$ are related $V_\Gamma = [\mathrm{SL}_2(\mathbb{Z}) : \{\pm I\}\Gamma]V_{\mathrm{SL}_2(\mathbb{Z})}$. The second equality in part (2) follows from this.

For part (3) apply part (2) with $\Gamma$ is replaced by $\alpha\Gamma\alpha^{-1} \cap \Gamma$ hence we get
$$[\mathrm{SL}_2(\mathbb{Z}) : \alpha\Gamma\alpha^{-1} \cap \Gamma] = [\mathrm{SL}_2(\mathbb{Z}) : \alpha^{-1}\Gamma\alpha \cap \Gamma].$$

Thus $[\Gamma : \alpha\Gamma\alpha^{-1} \cap \Gamma] = [\Gamma : \alpha^{-1}\Gamma\alpha \cap \Gamma]$. Hence there exists $\gamma_1, ..., \gamma_n, \tilde{\gamma}_1, ..., \tilde{\gamma}_n \in \Gamma$ such that
$$\Gamma = \bigcup_j (\alpha^{-1}\Gamma\alpha \cap \Gamma)\gamma_j = \bigcup_j (\alpha\Gamma\alpha^{-1} \cap \Gamma)\tilde{\gamma}_j^{-1}.$$

Now by Lemma **??** with $\Gamma_1 = \Gamma_2 = \Gamma$ we have $\Gamma\alpha\Gamma = \bigcup_j \Gamma\alpha\gamma_j$ and $\Gamma\alpha^{-1}\Gamma = \bigcup_j \Gamma\alpha^{-1}\tilde{\gamma}_j^{-1} = \bigcup_j \tilde{\gamma}_j\alpha\Gamma$. For each $j$, $\Gamma\alpha\gamma_j \cap \tilde{\gamma}_j\alpha\Gamma \neq \varnothing$ since otherwise $\Gamma\alpha\gamma_j \subset \bigcup_{i\neq j} \tilde{\gamma}_j\alpha\Gamma$ and so $\Gamma\alpha\Gamma \subset \bigcup_{i\neq j} \tilde{\gamma}_j\alpha\Gamma$ which is a contradiction. Hence we can choose $\beta_j \in \Gamma\alpha\gamma_j \cap \tilde{\gamma}_j\alpha\Gamma$ for each $j$. Then $\Gamma\alpha\Gamma = \bigcup_j \Gamma\beta_j = \bigcup_j \beta_j\Gamma$. □

Now we are ready to compute the adjoints of the Hecke operators.

**Propositition 2.3.1.** *Let $\Gamma \subset \mathrm{SL}_2(\mathbb{Z})$ be a congruence subgroup and $\alpha \in GL_2^+(\mathbb{Q})$. Set $\alpha' = \det(\alpha)\alpha^{-1}$. Then*

1. *If $\alpha^{-1}\Gamma\alpha \subset \mathrm{SL}_2(\mathbb{Z})$ the for all $f \in \mathcal{S}_k(\Gamma)$ and $g \in \mathcal{S}_k(\alpha^{-1}\Gamma\alpha)$,*

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

2. *For all $f, g \in \mathcal{S}_k(\Gamma)$,*

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

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

*Proof.* For part (1), using Lemma **??** and noting that $\alpha'(\tau) = \alpha^{-1}(\tau)$ for all $\tau \in \mathcal{H}^*$ we have

$$\begin{aligned}
\langle f[\alpha]_k, g\rangle_{\alpha^{-1}\Gamma\alpha} &= \frac{1}{V_{\alpha^{-1}\Gamma\alpha}} \int_{\alpha^{-1}\Gamma\alpha\backslash\mathcal{H}^*} (f[\alpha]_k)(\tau)\overline{g(\tau)}\mathrm{Im}(\tau)^k d\mu(\tau) \\
&= \frac{1}{V_\Gamma} \int_{\alpha^{-1}\Gamma\alpha\backslash\mathcal{H}^*} f(\alpha(\tau))j(\alpha,\tau)^{-k}\det(\alpha)^{k-1}\overline{g(\tau)}\mathrm{Im}(\tau)^k d\mu(\tau) \\
&= \frac{1}{V_\Gamma} \int_{X(\Gamma)} f(\tau)j(\alpha,\alpha'(\tau))^{-k}\det(\alpha)^{k-1}\overline{g(\alpha'(\tau))}\mathrm{Im}(\alpha'(\tau))^k d\mu(\tau) \\
&= \frac{1}{V_\Gamma} \int_{X(\Gamma)} f(\tau)\overline{(g[\alpha']_k)(\tau)}\mathrm{Im}(\tau)^k d\mu(\tau) \\
&= \langle f, g[\alpha']_k\rangle_\Gamma
\end{aligned}$$

In the last equality we use the identities $j(\alpha\alpha', \tau) = j(\alpha, \alpha'(\tau))j(\alpha', \tau)$ and $\mathrm{Im}(\alpha'(\tau)) = \det(\alpha')\mathrm{Im}(\tau)|j(\alpha', \tau)|^{-2}$.

For part (2), by Lemma **??** $\Gamma\alpha\Gamma = \bigcup_j \Gamma\beta_j$ hence $f[\Gamma\alpha\Gamma]_k = \sum_j f[\beta_j]_k$. For each $j$ set $\beta'_j = \det\beta_j\beta_j^{-1}$. Then noting that $\det\alpha = \det\beta_j$ for each $j$ we have $\Gamma\alpha'\Gamma = \bigcup_j \Gamma\beta'_j$. Hence $f[\Gamma\alpha'\Gamma]_k = \sum_j f[\beta'_j]_k$. Since $\Gamma \cap \beta_j\Gamma\beta_j^{-1}$ is a subgroup of $\Gamma$ we have $\langle f, g\rangle_\Gamma = \langle f, g\rangle_{\Gamma\cap\beta_j\Gamma\beta_j^{-1}}$. Now using part (1) we get $\langle f[\Gamma\alpha\Gamma]_k, g\rangle_\Gamma = \sum_j\langle f[\beta_j]_k, g\rangle_\Gamma = \sum_j\langle f[\beta_j]_k, g\rangle_{\Gamma\cap\beta_j\Gamma\beta_j^{-1}} = \langle f, g[\beta'_j]_k\rangle_{\Gamma\cap\beta_j^{-1}\Gamma\beta_j} = \langle f, g[\Gamma\alpha'\Gamma]_k\rangle_\Gamma$. □

Using Proposition **??** we can find the adjoints of the Hecke operators

**Theorem 2.3.1.** *In the inner product space $\mathcal{S}_k(\Gamma_1(N))$, the Hecke operators $\langle p\rangle$ and $T_p$ for $p \nmid N$ have adjoints*

$$\langle p\rangle^* = \langle p\rangle^{-1} \qquad \text{and} \qquad T_p^* = \langle p\rangle^{-1}T_p.$$

*Thus the Hecke operators $\langle n\rangle$ and $T_n$ for $(n, N) = 1$ are normal.*

*Proof.* Let $f, g \in \mathcal{S}_k(\Gamma_1(N))$. Since $\Gamma_1(N) \lhd \Gamma_0(N)$, for any $\alpha \in \Gamma_0(N)$, $\alpha^{-1}\Gamma_1(N)\alpha = \Gamma_1(N)$. Hence by part (1) of Proposition **??** we have $\langle p\rangle^* = [\alpha]_k^* = [\alpha^{-1}]_k = \langle p\rangle^{-1}$. For $T_p$ by part (2) of Propposition **??** we have $T_p^* = [\Gamma_1(N)\left(\begin{smallmatrix}1 & 0\\ 0 & p\end{smallmatrix}\right)\Gamma_1(N)]_k^* = [\Gamma_1(N)\left(\begin{smallmatrix}p & 0\\ 0 & 1\end{smallmatrix}\right)\Gamma_1(N)]_k$. Since $p \nmid N$ there exists $m, n \in \mathbb{Z}^+$ such that $mp - nN = 1$ and $\left(\begin{smallmatrix}p & 0\\ 0 & 1\end{smallmatrix}\right) = \left(\begin{smallmatrix}1 & n\\ N & mp\end{smallmatrix}\right)^{-1}\left(\begin{smallmatrix}1 & 0\\ 0 & p\end{smallmatrix}\right)\left(\begin{smallmatrix}p & n\\ N & m\end{smallmatrix}\right)$. Note that $\left(\begin{smallmatrix}1 & n\\ N & mp\end{smallmatrix}\right)^{-1} \in \Gamma_1(N)$ and $\left(\begin{smallmatrix}p & n\\ N & m\end{smallmatrix}\right) \in \Gamma_0(N)$. Thus $\Gamma_1(N)\left(\begin{smallmatrix}p & 0\\ 0 & 1\end{smallmatrix}\right)\Gamma_1(N) = \Gamma_1(N)\left(\begin{smallmatrix}1 & 0\\ 0 & p\end{smallmatrix}\right)\Gamma_1(N)\left(\begin{smallmatrix}p & n\\ N & m\end{smallmatrix}\right)$. If $\Gamma_1(N)\left(\begin{smallmatrix}p & 0\\ 0 & 1\end{smallmatrix}\right)\Gamma_1(N) = \bigcup_j \Gamma_1(N)\beta_j$ then $\Gamma_1(N)\left(\begin{smallmatrix}1 & 0\\ 0 & p\end{smallmatrix}\right)\Gamma_1(N) = \bigcup_j \Gamma_1(N)\beta_j\left(\begin{smallmatrix}p & n\\ N & m\end{smallmatrix}\right)$ gives the decomposition for $T_p^*$. Thus

$$T_p^* f = \sum_j f[\beta_j\left(\begin{smallmatrix}p & n\\ N & m\end{smallmatrix}\right)]_k = \left(\sum_j f[\beta_j]_k\right)\left(\begin{smallmatrix}p & n\\ N & m\end{smallmatrix}\right) = \langle p\rangle^{-1}T_p$$

as $m \equiv p^{-1} \pmod{N}$. □

By the above result and the Spectral theorem of linear algebra for normal operators we have the following theorem

**Theorem 2.3.2.** *The space $\mathcal{S}_k(\Gamma_1(N))$ has an orthogonal basis of simultaneous eigenforms for the Hecke operators $\{\langle n\rangle, T_n : (n,N) = 1\}$.*

We will need the following lemma later.

**Lemma 2.3.3.** *For any Hecke operator $T = T_n$ or $T = \langle n\rangle$, $T^* = w_N T w_N^{-1}$ where $w_N = [\left(\begin{smallmatrix} 0 & -1 \\ N & 0 \end{smallmatrix}\right)]_k$.*

*Proof.* Let $p$ be a prime such that $p \nmid N$ and $\gamma = \left(\begin{smallmatrix} 0 & -1 \\ N & 0 \end{smallmatrix}\right)$. Then $\gamma^{-1}\left(\begin{smallmatrix} a & b \\ Nc & d \end{smallmatrix}\right)\gamma = \left(\begin{smallmatrix} d & -c \\ -Nb & a \end{smallmatrix}\right)$ and so $\gamma^{-1}\Gamma_1(N)\gamma = \Gamma_1(N)$. Hence $w_N = [\gamma]_k$ is the double coset operator $[\Gamma_1(N)\gamma\Gamma_1(N)]_k$ and by Proposition **??**, $w_N^* = [\gamma]_k^* = [\gamma^{-1}]_k$. Let $\alpha = \left(\begin{smallmatrix} a & b \\ Nc & d \end{smallmatrix}\right) \in \Gamma_0(N)$ with $d \equiv p \pmod N$. Hence $\langle p\rangle = [\alpha]_k$. Now we have $[\gamma\alpha\gamma^{-1}]_k^* = [\gamma^{-1}]_k^*[\alpha]_k^*[\gamma]_k^* = [\gamma\alpha^{-1}\gamma^{-1}]_k$. Since $\gamma\alpha^{-1}\gamma^{-1} = \left(\begin{smallmatrix} a & b \\ Nc & d \end{smallmatrix}\right)$, $[\gamma\alpha^{-1}\gamma^{-1}]_k = \langle p\rangle$ and so $[\gamma\alpha^{-1}\gamma^{-1}]_k = [\gamma\alpha^{-1}\gamma^{-1}]_k^{**} = \langle p\rangle^{-1}$ by Theorem **??**. This proves that $w_N\langle n\rangle w_N = \langle n\rangle^*$ for $(n,N) = 1$. Since $\langle n\rangle = 0$ when $(n,N) > 1$, the equality is true for all $n$.

For $T = T_p$, let $\Gamma_1(N)\left(\begin{smallmatrix} 1 & 0 \\ 0 & p \end{smallmatrix}\right)\Gamma_1(N) = \bigcup_j \Gamma_1(N)\beta_j$. Then $T_p = \sum_j [\beta_j]_k$. Note that $\left(\begin{smallmatrix} p & 0 \\ 0 & 1 \end{smallmatrix}\right) = \gamma^{-1}\left(\begin{smallmatrix} 1 & 0 \\ 0 & p \end{smallmatrix}\right)\gamma$. Hence $\Gamma_1(N)\left(\begin{smallmatrix} p & 0 \\ 0 & 1 \end{smallmatrix}\right)\Gamma_1(N) = \bigcup_j \Gamma_1(N)\gamma^{-1}\beta_j\gamma$. By using these representatives and Proposition **??**,

$$T_p^* = [\Gamma_1(N)\left(\begin{smallmatrix} 1 & 0 \\ 0 & p \end{smallmatrix}\right)\Gamma_1(N)]_k^* = [\Gamma_1(N)\left(\begin{smallmatrix} p & 0 \\ 0 & 1 \end{smallmatrix}\right)\Gamma_1(N)]_k = \sum_j [\gamma^{-1}\beta_j\gamma]_k = w_N^{-1}T_p w_N.$$

Thus $T_n^* = w_N^{-1}T_n w_N$. □

## 2.4 Oldforms and Newforms

Let $M \mid N$. Then $\mathcal{S}_k(\Gamma_1(M))$ embeds into $\mathcal{S}_k(\Gamma_1(N))$ since $\Gamma_1(N) \subset \Gamma_1(M)$. We see that there is another way embed $\mathcal{S}_k(\Gamma_1(M))$ into $\mathcal{S}_k(\Gamma_1(N))$. Let $d \mid (N/M)$ and define $\alpha_d = \left(\begin{smallmatrix} d & 0 \\ 0 & 1 \end{smallmatrix}\right)$. Hence for $f : \mathcal{H} \to \mathbb{C}$, $(f[\alpha_d]_k)(\tau) = d^{k-1}f(d\tau)$.

**Lemma 2.4.1.** *Let $\Gamma_1$ and $\Gamma_2$ be two congruence subgroups of* $\mathrm{SL}_2(\mathbb{Z})$, $\gamma \in GL_2^+(\mathbb{Q})$ *and* $f \in \mathcal{M}_k(\Gamma_1)$. *Suppose that* $\Gamma_1 \supset \gamma\Gamma_2\gamma^{-1}$. *Then* $f[\gamma]_k \in \mathcal{M}_k(\Gamma_2)$.

*Proof.* Let $\beta \in \Gamma_2$. By hypothesis, for some $\alpha \in \Gamma_1$ we have $(f[\gamma]_k)[\beta]_k = f[\gamma\beta]_k = f[\alpha\gamma]_k = f[\gamma]_k$. Thus $f[\gamma]_k$ is weight-$k$ invariant under $\Gamma_2$. To prove holomorphy at the cusps, let $\alpha \in \mathrm{SL}_2(\mathbb{Z})$. Then by the proof of Lemma **??**, $\gamma\alpha = \alpha'\gamma'$ for some $\alpha' \in \mathrm{SL}_2(\mathbb{Z})$ and $\gamma' \in GL_2^+(\mathbb{Q})$ and so $(f[\gamma]_k)[\alpha]_k = (f[\alpha']_k)[\gamma']_k$. Since $f[\alpha']_k$ has Fourier expansion, again by Lemma **??**, $(f[\alpha']_k)[\gamma']_k = (f[\gamma]_k)[\alpha]_k$ has a Fourier expansion. This proves that $f[\gamma]_k \in \mathcal{M}_k(\Gamma_2)$. □

The above lemma is also true if we replace modular forms with cusp forms. Taking $\Gamma_1 = \Gamma_1(M)$, $\Gamma_2 = \Gamma_1(N)$ and $\gamma = \alpha_d$ in the above lemma gives $f[\alpha_d]_k \in \mathcal{S}_k(\Gamma_1(N))$ for $f \in \mathcal{S}_k(\Gamma_1(M))$. Clearly the operator $[\alpha_d]_k$ is injective.

These two types of embeddings show that some of the cusp forms in $\mathcal{S}_k(\Gamma_1(N))$ comes from lower levels.

**Definition 2.4.1.** *For each divisor $d$ of $N$, let $i_d$ be the map*

$$i_d : (\mathcal{S}_k(\Gamma_1(Nd^{-1})))^2 \to \mathcal{S}_k(\Gamma_1(N))$$

*defined by* $(f, g) \mapsto f + g[\alpha_d]_k$. *The subspace of oldforms of level $N$ is*

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

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

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

Now we prove the Hecke operators respect the decomposition of $\mathcal{S}_k(\Gamma_1(N))$ into oldforms and new forms.

**Propositon 2.4.1.** *The subspaces $\mathcal{S}_k(\Gamma_1(N))^{\text{old}}$ and $\mathcal{S}_k(\Gamma_1(N))^{\text{new}}$ are stable under the Hecke operators $T_n$ and $\langle n\rangle$ for all $n \in \mathbb{Z}^+$.*

*Proof.* Let $p \mid N$, $p' \neq p$ be a prime and $T = T_{p'}$ or $T = \langle d\rangle$ for $(d, N) = 1$. Then we have the following commutative diagram

$$\begin{tikzcd}[ampersand replacement=\&]
(\mathcal{S}_k(\Gamma_1(Np^{-1})))^2 \arrow[r, "\left(\begin{smallmatrix} T_{(Np^{-1})} & 0 \\ 0 & T_{(Np^{-1})} \end{smallmatrix}\right)"] \arrow[d, "i_p"'] \& (\mathcal{S}_k(\Gamma_1(Np^{-1})))^2 \arrow[d, "i_p"] \\
\mathcal{S}_k(\Gamma_1(N)) \arrow[r, "T_{(N)}"] \& \mathcal{S}_k(\Gamma_1(N))
\end{tikzcd}$$

where the index of $T$ denote the level. To prove that the diagram commutes it suffices to check that $T_{(Np^{-1})}f = T_{(N)}f$ and $(T_{(Np^{-1})}g)[\alpha_p]_k = T_{(N)}(g[\alpha_p]_k)$. For $T = \langle d\rangle$, $T_{(N)}f = f[\alpha]_k$ for any $\alpha \equiv \left(\begin{smallmatrix} * & * \\ 0 & d \end{smallmatrix}\right) \pmod N$ .Choose such an $\alpha$ with bottom right entry $d$. Then $\alpha$ also satisfies $\alpha \equiv \left(\begin{smallmatrix} * & * \\ 0 & d \end{smallmatrix}\right) \pmod{Np^{-1}}$ hence $T_{(Np^{-1})}f = f[\alpha]_k$ and so $T_{(Np^{-1})}f = T_{(N)}f$. Since $\alpha_p\alpha\alpha_p^{-1} \in \Gamma_0(Np^{-1})$ has bottom right entry $d$ and so $T_{(Np^{-1})} = [\alpha_p]_k T_{(N)}[\alpha_p^{-1}]_k$. This proves the case $T = \langle d\rangle$.

For $T = T_{p'}$, by part (1) of Proposition **??**, $T_{(Np^{-1})}$ is the restriction of $T_{(N)}$ to level $Np^{-1}$. Let $g \in \mathcal{S}_k(Np^{-1}, \chi)$ for some character $\chi : (\mathbb{Z}/Np^{-1}\mathbb{Z})^* \to \mathbb{C}^*$. Since $\Gamma_0(N) \subset \Gamma_0(Np^{-1})$ we have $g[\alpha_p]_k(\tau) = p^{k-1}g(p\tau) \in \mathcal{S}_k(N, \chi')$ where $\chi'$ is a lift of $\chi$ to $(\mathbb{Z}/N\mathbb{Z})^*$. Now by part (2) of Proposition **??**,

$$\begin{aligned}
a_n(T_{(N)}(g[\alpha_p]_k)) &= a_{np'}(g[\alpha_p]_k) + \chi'(p'){p'}^{k-1}a_{n/p'}(g[\alpha_p]_k) \\
&= p^{k-1}a_{np'/p}(g) + \chi'(p'){p'}^{k-1}p^{k-1}a_{n/p'p}(g) \\
&= p^{k-1}a_{n/p}(T_{(Np^{-1})}g) \\
&= a_n((T_{(Np^{-1})}g)[\alpha_p]_k)
\end{aligned}$$

Thus the diagram commutes.

We also have the following commutative diagram

$$\begin{tikzcd}
(\mathcal{S}_k(\Gamma_1(Np^{-1})))^2 \arrow[r, "\left(\begin{smallmatrix} T_p & p^{k-1} \\ -\langle p\rangle & 0 \end{smallmatrix}\right)"] \arrow[d, "i_p"'] & (\mathcal{S}_k(\Gamma_1(Np^{-1})))^2 \arrow[d, "i_p"] \\
\mathcal{S}_k(\Gamma_1(N)) \arrow[r, "T_p"] & \mathcal{S}_k(\Gamma_1(N))
\end{tikzcd}$$

Let $f, g \in \mathcal{S}_k(Np^{-1}, \chi)$ where $\chi$ is a character modulo $Np^{-1}$. To prove that this diagram commutes it is enough to check that $T_pf - (\langle p\rangle f)[\alpha_p]_k = T_pf$ and $p^{k-1}g = T_p(g[\alpha_p]_k)$ where the operator $T_p$ on the left-hand side is of level $Np^{-1}$. Considering the Fourier coefficients gives $a_n(T_pf - (\langle p\rangle f)[\alpha_p]_k) = a_{np}(f) + \chi(p)p^{k-1}a_{n/p}(f) - a_n((\langle p\rangle f)[\alpha_p]_k) = a_{np}(f) = a_n(T_pf)$ and $a_n(T_p(g[\alpha_p]_k)) = a_{np}(g[\alpha_p]_k) = p^{k-1}a_n(g) = a_n(p^{k-1}g)$.

The above two diagram shows that $\mathcal{S}_k(\Gamma_1(N))^{\text{old}}$ is stable under all $T_n$ and $\langle n\rangle$. When $(n, N) = 1$ we have the adjoints $T_n^* = \langle n\rangle^{-1}T_n$ and $\langle n\rangle^* = \langle n\rangle^{-1}$. Hence the above diagrams shows that $\mathcal{S}_k(\Gamma_1(N))^{\text{old}}$ is also stable under the adjoints of the Hecke operators in the case $(n, N) = 1$. For $(n, N) > 1$, $\langle n\rangle^* = 0$ hence this is also true for all $\langle n\rangle$. For $T_n$, note that by Lemma **??**, $T_n^* = w_NT_nw_N^{-1}$. Consider the commutative diagram

$$\begin{tikzcd}
(\mathcal{S}_k(\Gamma_1(Np^{-1})))^2 \arrow[r, "\left(\begin{smallmatrix} 0 & p^{k-2}w_{Np^{-1}} \\ w_{Np^{-1}} & 0 \end{smallmatrix}\right)"] \arrow[d, "i_p"'] & (\mathcal{S}_k(\Gamma_1(Np^{-1})))^2 \arrow[d, "i_p"] \\
\mathcal{S}_k(\Gamma_1(N)) \arrow[r, "w_N"] & \mathcal{S}_k(\Gamma_1(N))
\end{tikzcd}$$

where $w_N = [\gamma]_k$ and $w_{Np^{-1}} = [\gamma']_k$ with $\gamma = \left(\begin{smallmatrix} 0 & 1 \\ -N & 0 \end{smallmatrix}\right)$, $\gamma' = \left(\begin{smallmatrix} 0 & 1 \\ -Np^{-1} & 0 \end{smallmatrix}\right)$. Let $f, g \in \mathcal{S}_k(Np^{-1}, \chi)$.To see that this diagram commutes it is enough to check that $f[\gamma]_k = (f[\gamma']_k)[\alpha_p]_k$ and $(g[\alpha_p]_k)[\gamma]_k = p^{k-2}g[\gamma']_k$. The first equality is clear as $\gamma'\alpha_p = \gamma$. The second can easily be seen from the identity $\alpha_p\gamma = \left(\begin{smallmatrix} 0 & p \\ -N & 0 \end{smallmatrix}\right)$.

Finally let $f \in \mathcal{S}_k(\Gamma_1(N))^{\text{new}}$. Then $\langle f, g\rangle = 0$ for any $g \in \mathcal{S}_k(\Gamma_1(N))^{\text{old}}$. Let $T = T_n$ or $T = \langle n\rangle$. Then $\langle Tf, g\rangle = \langle f, T^*g\rangle = 0$ since $\mathcal{S}_k(\Gamma_1(N))^{\text{old}}$ is stable under the adjoint of $T$. Thus $Tf \in \mathcal{S}_k(\Gamma_1(N))^{\text{new}}$ and this finishes the proof of the proposition. □

Combining Proposition **??** with Theorem **??** we get the following corollary.

**Corollary 2.4.1.** *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 $\{T_n, \langle n\rangle : (n, N) = 1\}$*

Now we give a characterization of oldforms in terms of the Fourier coefficients. Let $M \mid N$ and $d \mid (N/M)$. Normalizing the scalar in the operator $i_d$ to 1 gives

$$\iota_d = d^{1-k}[\alpha_d]_k : \mathcal{S}_k(\Gamma_1(M)) \to \mathcal{S}_k(\Gamma_1(N)), \qquad (\iota_d f)(\tau) = f(d\tau).$$

$\iota_d$ acts on the Fourier expansion as $\iota_d : \sum_{n=1}^{\infty} a_n q^n \mapsto \sum_{n=1}^{\infty} a_n q^{dn}$. Suppose $f \in \mathcal{S}_k(\Gamma_1(N))$ is of the form $\sum_{p|N} \iota_p f_p$ with $f_p \in \mathcal{S}_k(\Gamma_1(Np^{-1}))$. Choose $p \mid N$ and let $f_p(\tau) = \sum_{n=1}^{\infty} a_n(f_p)q^n$ be the Fourier expansion of $f_p$. Then $(\iota_p f_p)(\tau) = \sum_{n=1}^{\infty} a_n(f_p)q^{np}$. If $(n, N) = 1$ then also $(p, n) = 1$ and so $a_n(f_p) = 0$. Thus $a_n(f) = 0$ for such $n$. The following Theorem proves that the converse is also true.

**Theorem 2.4.1.** *If $f \in \mathcal{S}_k(\Gamma_1(N))$ has Fourier expansion $f(\tau) = \sum a_n(f)q^n$ with $a_n(f) = 0$ for $(n, N) = 1$, then $f$ takes the form $f = \sum_{p|N} \iota_p f_p$ with each $f_p \in \mathcal{S}_k(\Gamma_1(Np^{-1}))$.*

See [**?**, Chapter 5.7] for the proof of this theorem.

## 2.5 Eigenforms

From Corollary **??** 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 $f$ is an eigenform for all $T_n$ and $\langle n \rangle$. For $(n, N) > 1$, $\langle n \rangle = 0$ hence $f$ is an eigenform for all $\langle n \rangle$. Hence we only need to check $T_n$.

**Definition 2.5.1.** *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 just eigenform). The eigenform $f(\tau) = \sum a_n(f)q^n$ is normalized when $a_1(f) = 1$. A normalized eigenform $f \in \mathcal{S}_k(\Gamma_1(N))^{\text{new}}$ is called newform.*

Now we show that $\mathcal{S}_k(\Gamma_1(N))^{\text{new}}$ has an orthogonal basis of newforms. Let $f \in \mathcal{S}_k(\Gamma_1(N))$ be an eigenform for the Hecke operators $T_n$ and $\langle n \rangle$ with $(n, N) = 1$. Hence for all such $n$ there exist $c_n, d_n \in \mathbb{C}$ such that $T_n f = c_n f$ and $\langle n \rangle f = d_n f$. By Lemma **??** the map $n \mapsto d_n$ defines a Dirichlet character $\chi : (\mathbb{Z}/N\mathbb{Z})^* \to \mathbb{C}^*$ and $f \in \mathcal{S}_k(N, \chi)$. By formula (**??**), $a_1(T_n f) = a_n(f)$ for all $n \in \mathbb{Z}^+$. Since $f$ is an eigenform we also have

$$a_1(T_n f) = c_n a_1(f) \qquad \text{when } (n, N) = 1.$$

The above two formulas together shows that

$$a_n(f) = c_n a_1(f) \qquad \text{when } (n, N) = 1.$$

Thus if $a_1(f) = 0$ then $a_n(f) = 0$ when $(n, N) = 1$ and so by Theorem **??**, $f \in \mathcal{S}_k(\Gamma_1(N))^{\text{old}}$.

Now 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 so $a_1(f) \neq 0$ so we may assume $f$ 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 $g_m \in \mathcal{S}_k(\Gamma_1(N))^{\mathrm{old}}$ by the above discussion. Hence $g_m \in \mathcal{S}_k(\Gamma_1(N))^{\mathrm{old}} \cap \mathcal{S}_k(\Gamma_1(N))^{\mathrm{new}} = \{0\}$ and so $T_m f = a_m(f) f$. Putting these together we have the following theorem,

**Theorem 2.5.1.** *Let $f \in \mathcal{S}_k(\Gamma_1(N))^{\mathrm{new}}$ be a nonzero eigenform for the Hecke operators $T_n$ and $\langle n \rangle$ with $(n, N) = 1$. Then*

1. *$f$ is a Hecke eigenform.*
2. *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 newforms in $\mathcal{S}_k(\Gamma_1(N))^{\mathrm{new}}$ is an orthogonal basis of the space. Each such newform lies in $\mathcal{S}_k(N, \chi)$ for some $\chi$ and its Fourier coefficients are its $T_n$-eigenvalues.*

*Proof.* Part (1) is proved above. For part (2) 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

$$a_n(c\tilde{f}) c\tilde{f} = T_n(c\tilde{f}) c\tilde{f} = c d_n \tilde{f} \quad \text{and} \quad a_n(df) df = T_n(df) df = d d_n f.$$

Thus $a_n(\tilde{f}) = d_n/c$ and $a_n(f) = d_n/d$. This proves part (2). □

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

**Theorem 2.5.2.** *The set*

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

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

*Proof.* Consider the decomposition

$$\mathcal{S}_k(\Gamma_1(N)) = \mathcal{S}_k(\Gamma_1(N))^{\text{new}} \oplus \sum_{p \mid N} i_p((\mathcal{S}_k(\Gamma_1(N/p)))^2).$$

Now $\mathcal{S}_k(\Gamma_1(N))^{\text{new}}$ is spanned by $\{f(\tau) : f \textit{ is a newform of level } N\} \subset \mathcal{B}_k(N)$. Each summand in the sum is spanned by

$$\{f(\tau), f(p\tau) : f \textit{ is a newform of level dividing } N/p\}.$$

Thus $\mathcal{B}_k(N)$ generates $\mathcal{S}_k(\Gamma_1(N))$.

To see that $\mathcal{B}_k(N)$ forms a basis suppose there is a nontrivial relation

$$\sum_{i,j} c_{i,j} f_i(n_{i,j}\tau) = 0 \qquad c_{i,j} \in \mathbb{C}$$

where $f_i \in \mathcal{S}_k(M_i, \chi_i)$ with $M_i \mid N$ and $n_{i,j} \mid (N/M_i)$ and $\chi_i$ is a Dirichlet character modulo $M_i$. Assume that the relation has as few terms as possible. It has at least two terms. Each character $\chi_i$ lifts to a character $\tilde{\chi}_i$ modulo N and so $f \in \mathcal{S}_k(N, \tilde{\chi}_i)$. In fact $\tilde{\chi}_i$ is the same character for all $i$. Indeed, if $\tilde{\chi}_1(d) \neq \tilde{\chi}_2(d)$ for some $d \in (\mathbb{Z}/N\mathbb{Z})^*$ then applying $\langle d \rangle - \tilde{\chi}_1(d)$ to the relation gives

$$\begin{aligned} (\langle d \rangle - \tilde{\chi}_1(d)) \sum_{i,j} c_{i,j} f_i(n_{i,j}\tau) &= \sum_{i,j} c_{i,j} \langle d \rangle f_i(n_{i,j}\tau) - \sum_{i,j} c_{i,j} \tilde{\chi}_1(d) f_i(n_{i,j}\tau) \\ &= \sum_{i,j} c_{i,j} \tilde{\chi}_i(d) f_i(n_{i,j}\tau) - \sum_{i,j} c_{i,j} \tilde{\chi}_1(d) f_i(n_{i,j}\tau) \\ &= \sum_{i,j} c_{i,j} (\tilde{\chi}_i(d) - \tilde{\chi}_1(d)) f_i(n_{i,j}\tau) \end{aligned}$$

which is a nontrivial relation with fewer terms. Similarly all $f_i$ have the same Fourier coefficients away from $N$. Indeed, if $a_p(f_1) \neq a_p(f_2)$ for some $p \nmid N$ then applying $T_p - a_p(f_1)$ to the relation gives

$$\begin{aligned}(T_p - a_p(f_1)) \sum_{i,j} c_{i,j} f_i(n_{i,j}\tau) &= \sum_{i,j} c_{i,j} T_p f_i(n_{i,j}\tau) - \sum_{i,j} c_{i,j} a_p(f_1) f_i(n_{i,j}\tau) \\ &= \sum_{i,j} c_{i,j}(a_p(f_i)a_p(f_1) -) f_i(n_{i,j}\tau)\end{aligned}$$

which is a nontrivial relation with fewer terms. Thus all $a_p(f_i)$ are equal for $p \nmid N$ and so all $f_i$ are equal contradicts with the number of terms in the relation. □

**Propositition 2.5.1.** *Let $g \in \mathcal{S}_k(\Gamma_1(N))$ be a normalized eigenform. Then there is a newform $f \in \mathcal{S}_k(\Gamma_1(M))^{\text{new}}$ for some $M \mid N$ such that $a_p(f) = a_p(g)$ for all $p \nmid N$.*

*Proof.* Suppose for each newform $f_i$ of level dividing $N$ there exists a prime $p_i \nmid N$ such that $a_{p_i}(f_i) \neq a_{p_i}(g)$. By Theorem **??**, we can write $g$ as

$$g = \sum_{i,j} c_{i,j} f_i(n_{i,j}\tau)$$

Applying $\prod_i (T_{p_i} - a_{p_i}(f_i))$ to this relation we get $\prod_i (T_{p_i} - a_{p_i}(f_i)) \sum_{i,j} c_{i,j} f_i(n_{i,j}\tau) = 0$ but $\prod_i (T_{p_i} - a_{p_i}(f_i))g \neq 0$ by assumption. This contradiction finishes the proof. □

# 3 Jacobians and Abelian Varieties

In this section we define the Jacobian of the modular curves and Abelian variety comes from a weight-2 eigenform.

## 3.1 Preliminaries

We have noted in Section **??** that modular curves are compact Riemann surfaces. Hence we begin with recalling some general facts about compact Riemann surfaces. For details see [**?**, **?**].

Let $X$ be a compact Riemann surface of genus $g$. It is a sphere with $g$ handles. The holomorphic differntials on $X$ will be denoted by $\Omega^1_{\text{hol}}(X)$. It has $g$ dimensional vector space over $\mathbb{C}$. Let $A_1, ..., A_g$ be the longitudinal loops and let $B_1, ..., B_g$ 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 $H^1(X, \mathbb{Z})$, that is

$$H^1(X, \mathbb{Z}) = \mathbb{Z}\int_{A_1} \oplus \cdots \mathbb{Z}\int_{A_g} \oplus \mathbb{Z}\int_{B_1} \oplus \cdots \mathbb{Z}\int_{B_g} \cong \mathbb{Z}^{2g}.$$

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

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

hence $H^1(X, \mathbb{Z})$ is a lattice in $\Omega^1_{\text{hol}}(X)^\wedge$. The Jacobian of $X$ is defined as

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

Since the homology is a $2g$ dimensional lattice in $\Omega^1_{\text{hol}}(X)^\wedge$, 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

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

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

$$X \to \mathrm{Pic}^0(X), \qquad x \mapsto [x - x_0]. \tag{3.1}$$

Indeed, suppose $x, \tilde{x} \in X$ maps to the same equivalence class. Hence $x - \tilde{x} \in \mathrm{Div}^\ell(X)$. That is $x - \tilde{x} = \mathrm{div}(f)$ for some $f \in \mathbb{C}(X)$. Considering $f$ as a holomorphic function $f : X \to \widehat{\mathbb{C}}$ we see that $f$ has degree 1. Since $g > 0$ by Riemann-Hurwitz formula it is not possible. Thus the map is injective.

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

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

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

**Theorem 3.1.1.** *The above map induces an isomorphism*

$$\mathrm{Pic}^0(X) \xrightarrow{\sim} \mathrm{Jac}(X), \qquad \left[\sum_x n_x x\right] \mapsto \sum_x n_x \int_{x_0}^x . \tag{3.2}$$

Abel's Theorem says that principal divisors maps to trivial integration on $\Omega^1_{\text{hol}}(X)$ modulo integration over loops. The maps (**??**) and (**??**) shows that $X$ embeds into its Jacobian via

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

By Abel's Theorem we also have $\Omega^1_{\text{hol}}(X)^\wedge = \left\{\sum_\gamma n_\gamma \int_\gamma : \sum_\gamma n_\gamma = 0\right\}$.

Let $h : X \to Y$ be a nonconstant holomorphic map between compact Riemann surfaces. Now we define the the corresponding maps between Jacobians and Picard groups. The pullback map induced by $h$ is

$$h^* : \mathbb{C}(Y) \to \mathbb{C}(X), \qquad g \mapsto g \circ h.$$

$h^*$ is injective. For $g \in \mathbb{C}(Y)$ the orders of vanishing of $h^*g$ is $\nu_x(h^*g) = e_x \nu_{h(x)}(g)$, where $e_x$ is the ramification degree of $h$ at $x$. Indeed, let $x \in X$ and $z$ be the local coordinate centered at $x$ and $\omega$ be the local coordinate centered at $h(x)$. Then $\nu_0(\omega \circ h \circ z^{-1}) = e_x$, $\nu_0(g \circ \omega^{-1}) = \nu_{h(x)}(g)$ and $\nu_0(g \circ h \circ z^{-1}) = \nu_x(h^*g)$. Considering the compsitions proves the equality.

The pullback extends to holomorphic differentials $h^* : \Omega^1_{\text{hol}}(Y) \to \Omega^1_{\text{hol}}(X)$. Given $\lambda \in \Omega^1_{\text{hol}}(Y)$. Let $\varphi_j : U_j \to V_j$ and $\tilde{\varphi}_j : \tilde{U}_j \to \tilde{V}_j$ be local coordinates on $X$ and $Y$ such that $h(U_j) = \tilde{U}_j$. Let $h_j = \tilde{\varphi}_j h \varphi_j : V_i \to \tilde{V}_j$. Define the pullback of $\lambda$ locally as

$$(h^*\lambda)_j = h_j^* \lambda_j \in \Omega^1_{\text{hol}}(V_j), \quad \lambda_j \in \Omega^1_{\text{hol}}(\tilde{V}_j).$$

This map induces a dual map between dual spaces, denoted $h_*$,

$$h_* : \Omega^1_{\text{hol}}(X)^\wedge \to \Omega^1_{\text{hol}}(Y)^\wedge, \qquad \varphi \mapsto \varphi \circ h^*.$$

Now let $\alpha$ be a loop in $X$ and $\varphi = \int_\alpha \in \Omega^1_{\text{hol}}(X)^\wedge$. Then $h_*\varphi = \int_\alpha h^* = \int_{h(\alpha)} \in \Omega^1_{\text{hol}}(Y)^\wedge$. Since $h(\alpha)$ is a loop in $Y$, $h_*$ takes homology to homology and induces a map between Jacobians.

**Definition 3.1.1.** *The forward map of Jacobians is the holomorphic homomorphism*

$$h_J : \mathrm{Jac}(X) \to \mathrm{Jac}(Y), \qquad [\varphi] \mapsto [h_* \varphi] = [\varphi \circ h^*].$$

In terms of Theorem **??** this map is defined as

$$h_J(\sum_x n_x \int_{x_0}^{x}) = \sum_x n_x \int_{h(x_0)}^{h(x)}$$

There is also a forward map between Picard groups induced by $h : X \to Y$. First define the norm map

$$\mathrm{norm}_h : \mathbb{C}(X) \to \mathbb{C}(Y), \qquad (\mathrm{norm}_h f)(y) = \prod_{x \in h^{-1}(y)} f(x)^{e_x}.$$

The order of vanishing of norm of a function $f \in \mathbb{C}(X)^*$ is

$$\nu_y(\mathrm{norm}_h f) = \sum_{x \in h^{-1}(y)} \nu_x(f)$$

and so

$$\mathrm{div}(\mathrm{norm}_h f) = \sum_y \left( \sum_{x \in h^{-1}(y)} \nu_x(f) \right) y = \sum_x \nu_x(f) h(x).$$

Thus at the level of principal divisors the norm map is $\sum_x \nu_x(f) x \mapsto \sum_x \nu_x(f) h(x)$ and the map between divisors that extend this is

$$h_D : \mathrm{Div}(X) \to \mathrm{Div}(Y), \qquad \sum_x n_x x \mapsto \sum_x n_x h(x)$$

which takes degree-0 divisors to degree-0 divisors.

**Definition 3.1.2.** *The forward map of Picard groups is the homomorphism*

$$h_P : \mathrm{Pic}^0(X) \to \mathrm{Pic}^0(Y), \qquad \left[ \sum_x n_x x \right] \mapsto \left[ \sum_x n_x h(x) \right]$$

Under the isomorphism of Theorem **??** we have a commutative diagram

$$\begin{tikzcd}
\mathrm{Pic}^0(X) \arrow[r, "h_P"] \arrow[d] & \mathrm{Pic}^0(Y) \arrow[d] \\
\mathrm{Jac}(X) \arrow[r, "h_J"] & \mathrm{Jac}(Y)
\end{tikzcd}$$

So far we have defined forward maps. Now we define the reverse maps between Jacobians and Picard groups. Let $S = \{x \in X : e_x > 1\}$, $Y' = Y - h(S)$ and $X' = h^{-1}(Y')$. If $\deg(h) = d$ then the restriction of $h$ to $X'$ is a $d$-fold covering map. Given a path $\delta$ in $Y'$ and $x \in h^{-1}(\delta(0)) \subset X'$ then there exists a unique lift $\gamma$ of $\delta$ to $X'$ such that $\gamma(0) = x$. If $\delta$ is a path in $Y$ and only endpoints of $\delta$ lie in $h(S)$ then for each $x \in h^{-1}(\delta(0))$ there exist $e_x$ lifts of $\gamma$ starting at $x$. By perturbing paths in $Y$ any path integral of holomorphic differentials on $Y$ can be taken over a path $\delta$ such that only the endpoints of $\delta$ might lie in $h(S)$. Define the trace map induced by h

$$\mathrm{tr}_h : \Omega^1_{\mathrm{hol}}(X) \to \Omega^1_{\mathrm{hol}}(Y)$$

as follows: If $\delta$ is a path in $Y'$ lifting to a path in $X'$ and $h_i^{-1}$ is a local inverse of $h$ about $\delta(0)$. Then $h_i^{-1}$ has an analytic continuation along $\delta$. Let $\omega \in \Omega^1_{\mathrm{hol}}(X)$. Suppose $y \in Y'$ such that $h$ has local inverses $h_i^{-1} : \tilde{U} \to U_i$, $i = 1, ..., d$. The trace is defined on $\tilde{U}$ is

$$(\mathrm{tr}_h\omega)|_{\tilde{U}} = \sum_{i=1}^{d} (h_i^{-1})^*(\omega|_{U_i}).$$

This extends holomorphically to $Y$. We have a dual map

$$\mathrm{tr}_h^\wedge : \Omega^1_{\mathrm{hol}}(Y)^\wedge \to \Omega^1_{\mathrm{hol}}(X)^\wedge, \qquad \psi \mapsto \psi \circ \mathrm{tr}_h.$$

For paths $\delta$ in $Y'$ we have

$$\int_\delta \mathrm{tr}_h\omega = \sum_{\text{lifts } \gamma} \int_\gamma \omega.$$

This extends to paths in $Y$ such that only the endpoints might lie in $h(S)$. Let us see that the dual map takes homology to homology. Let $\beta$ be a loop in $Y'$ and $\psi = \int_\beta \in \Omega^1_{\text{hol}}(Y)^\wedge$ then $\text{tr}_h^\wedge \psi = \int_\beta \text{tr}_h = \sum_{\text{lifts } \gamma} \int_\gamma \in \Omega^1_{\text{hol}}(X)^\wedge$. Since $\beta$ lifts to a concatenation of loops in $X$ $\text{tr}_h^\wedge$ takes homology to homology and induces a map between Jacobians.

**Definition 3.1.3.** *The reverse map of Jacobians is the holomorphic homomorphism*

$$h^J : \text{Jac}(Y) \to \text{Jac}(X), \qquad [\psi] \mapsto [\psi \circ \text{tr}_h].$$

In terms of Theorem **??**, $h^J$ is given by

$$h^J(\sum_y n_y \int_{y_0}^{y}) = \sum_y n_y \sum_{x \in h^{-1}(y)} e_x \int_{x_0}^{x}.$$

**Propositititon 3.1.1.** *For any nonconstant holomorphic map $h : X \to Y$ of compact Riemann surfaces*

$$(\text{tr}_h \circ h^*)(\lambda) = \deg(h)\lambda, \qquad \lambda \in \Omega^1_{\text{hol}}(Y)$$

*Proof.* Let $\tilde{U}$ be a local chart on $Y$ such that the inverse image is a disjoint union of local charts $U_1, ..., U_d$ and the restrictions $h_i : U_i \to \tilde{U}$ are invertible. Then locally

$$(\text{tr}_h \circ h^*)(\lambda)|_{\tilde{U}} = \sum_{i=1}^{d} (h_i^{-1})^*(h^*\lambda|_{U_i}) = \sum_{i=1}^{d} (h_i^{-1})^*(h_i^*(\lambda|_{\tilde{U}})) = \sum_{i=1}^{d} \lambda|_{\tilde{U}} = d\lambda|_{\tilde{U}}$$

where $d = \deg(h)$. □

By the above Proposition the composition $h_J \circ h^J$ is multiplication by $\deg(h)$ in $\text{Jac}(Y)$. Finally we define the reverse map between Picard groups. Recall the pull back map $h^* : \mathbb{C}(Y) \to \mathbb{C}(X)$ and the formula $\nu_x(h^*g) = e_x \nu_{h(x)}(g)$ for $g \in \mathbb{C}(Y)$. Hence we have

$$\text{div}(h^*g) = \sum_x e_x \nu_{h(x)}(g)x = \sum_y \nu_y(g) \sum_{x \in h^{-1}(y)} e_x x.$$

Thus the action of pullback on the principal divisors is $\sum_y \nu_y(g)y \mapsto \sum_y \nu_y(g) \sum_{x\in h^{-1}(y)} e_x x$. The map between divisor groups that extends this is

$$h^D : \mathrm{Div}(Y) \to \mathrm{Div}(X), \qquad \sum_y n_y y \mapsto \sum_y n_y \sum_{x\in h^{-1}(y)} e_x x$$

which is taking degree-0 divisors to degree-0 divisors.

**Definition 3.1.4.** *The reverse map of Picard groups is*

$$h^P : \mathrm{Pic}^0(Y) \to \mathrm{Pic}^0(X), \qquad \left[\sum_y n_y y\right] \mapsto \left[\sum_y n_y \sum_{x\in h^{-1}(y)} e_x x\right].$$

As in the case of forward maps by Theorem **??** we have the following commutative diagram

$$\begin{tikzcd}
\mathrm{Pic}^0(Y) \arrow[r, "h^P"] \arrow[d] & \mathrm{Pic}^0(X) \arrow[d] \\
\mathrm{Jac}(Y) \arrow[r, "h^J"] & \mathrm{Jac}(X)
\end{tikzcd}.$$

## 3.2 Modular Jacobians

The Hecke operators give rise to holomorphic maps between modular curves which are compact Riemann surfaces. Thus by the preceding section they lead to maps between Jacobians of modular curves and Picard groups.

Let $\Gamma_1$ and $\Gamma_2$ be two congruence subgroups of $\mathrm{SL}_2(\mathbb{Z})$ and $\alpha \in GL_2^+(\mathbb{Q})$. Recal from Section **??** that the double coset operator $[\Gamma_1\alpha\Gamma_2]_2$ induces a map between divisor groups of modular curves

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

which is the $\mathbb{Z}$-linear extension of the map $\Gamma_2\tau \mapsto \sum_j \Gamma_1\beta_j(\tau)$, where $\beta_j$ are orbit representatives of $\Gamma_1\alpha\Gamma_2$ under the action of $\Gamma_1$. 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 $\Gamma_3\tau \mapsto \Gamma_3'\alpha(\tau)$. In terms of the previous section the $[\Gamma_1\alpha\Gamma_2]_2 = (\pi_1)_D \circ \alpha_D \circ (\pi_2)^D$. Thus $[\Gamma_1\alpha\Gamma_2]_2$ descends to a map of Picard groups,

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

which is given by

$$[\sum_\tau n_\tau \Gamma_2\tau] \mapsto [\sum_\tau n_\tau \sum_j \Gamma_1\beta_j(\tau)].$$

To define the action of the double coset operator on the Jacobians we need the following result,

**Proposititon 3.2.1.** *Let $\Gamma$ be a congruence subgroup of $\mathrm{SL}_2(\mathbb{Z})$. Then the holomorphic differentials $\Omega^1_{\mathrm{hol}}(X(\Gamma))$ and the weight 2 cusp forms $\mathcal{S}_2(\Gamma)$ are isomorphic as vector spaces over $\mathbb{C}$,*

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

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

*Proof.* [**?**, Theorem 3.3.1] □

By the above proposition we can identify $\Omega^1_{\mathrm{hol}}(X(\Gamma))$ and $\mathcal{S}_2(\Gamma)$. Thus we can also identify the dual spaces $\Omega^1_{\mathrm{hol}}(X(\Gamma))^\wedge$ and $\mathcal{S}_2(\Gamma)^\wedge$ and let $H^1(X(\Gamma), \mathbb{Z})$ denote the corresponding subgroup of $\mathcal{S}_2(\Gamma)^\wedge$. Therefore we can define the Jacobian of $X(\Gamma)$ in terms of the dual space of weight-2 cusp forms.

**Definition 3.2.1.** *Let $\Gamma$ be a congruence subgroup of $\mathrm{SL}_2(\mathbb{Z})$. The Jacobian of the modular curve $X(\Gamma)$ is*

$$\mathrm{Jac}(X(\Gamma)) = \mathcal{S}_2(\Gamma)^\wedge / H_1(X(\Gamma), \mathbb{Z}).$$

By the above definition the maps of the previous section can be written in terms of functions. Let $X$ and $Y$ be modular curves whose congruence subgroups are $\Gamma_X$ and $\Gamma_Y$. Let $\alpha \in GL_2^+(\mathbb{Q})$ be such that $\alpha\Gamma_X\alpha^{-1} \subset \Gamma_Y$ and consider the corresponding holomorphic map

$$h : X \to Y, \qquad \Gamma_X\tau \mapsto \Gamma_Y\alpha(\tau).$$

Denote the isomorphism between $\Omega^1_{\mathrm{hol}}(X)$ (reps. $\Omega^1_{\mathrm{hol}}(Y)$) and $\mathcal{S}_2(\Gamma_X)$ (resp. $\mathcal{S}_2(\Gamma_Y)$) by $\omega_X$ (resp. $\omega_Y$). Then we have the following commutative diagram,

$$\begin{tikzcd}
\mathcal{S}_2(\Gamma_Y) \arrow[r, "{[\alpha]_2}"] \arrow[d, "\omega_Y"] & \mathcal{S}_2(\Gamma_X) \arrow[d, "\omega_X"] \\
\Omega^1_{\mathrm{hol}}(Y) \arrow[r, "h^*"] & \Omega^1_{\mathrm{hol}}(X)
\end{tikzcd} \tag{3.3}$$

To see this we need to check that $(f[\alpha]_2)(\tau)d\tau = f(\alpha(\tau))d(\alpha(\tau))$ which clearly holds. The induced map on the dual spaces is

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

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

$$\begin{tikzcd}
\mathcal{S}_2(\Gamma_X) \arrow[r, "{\sum_j [\gamma_{Y,j}]_2}"] \arrow[d, "\omega_Y"] & \mathcal{S}_2(\Gamma_Y) \arrow[d, "\omega_X"] \\
\Omega^1_{\mathrm{hol}}(X) \arrow[r, "\mathrm{tr}_h"] & \Omega^1_{\mathrm{hol}}(Y)
\end{tikzcd} \tag{3.4}$$

Denoting the top map as $\mathrm{tr}_h$, the induced map on dual spaces is

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

Now $h_*$ and $\mathrm{tr}_h^\wedge$ descend to Jacobians.

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

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

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

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

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 operators on $J_1(N)$.

**Proposititon 3.2.2.** *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 act as endomorphisms on the homology $H_1(X_1(N), \mathbb{Z})$ which is a finitely generated Abelian 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 $H_1(X_1(N), \mathbb{Z})$. 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

**Theorem 3.2.1.** *Let $f \in \mathcal{S}_2(\Gamma_1(N))$ be a normalized eigenform. Then the eigenvalues $a_n(f)$ are algebraic integers.*

**Definition 3.2.2.** *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 $H_1(X_1(N), \mathbb{Z})$, $\mathbb{T}_{\mathbb{Z}}$ is finitely generated as well. Let $f(\tau) = \sum_{n=1}^{\infty} a_n(f) q^n$ be a normalized eigenform and define the homomorphism

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

The image of $\lambda_f$ is finitely generated $\mathbb{Z}$-module. The image of $\lambda_f$ is $\mathbb{Z}[\{a_n(f) : n \in \mathbb{Z}^+\}]$. To see this, suppose $f \in \mathcal{S}_2(N, \chi)$ for some Dirichlet character $\chi$ and note that for any $d \in (\mathbb{Z}/N\mathbb{Z})^*$ we have $\lambda_f(\langle d \rangle) = \chi(d)$. Hence the image is $\mathbb{Z}[\{a_n(f), \chi(d)\}]$. Let $p$ and $p'$ be two distinct primes congruent to $d$ modulo $N$. Then using formula (**??**) we can write $\chi(d)$ in terms of $a_p(f), a_{p^2}(f), a_{p'}(f), a_{p'^2}(f)$. Hence adjoining $\chi(d)$ is not needed. Thus the ring generated by the eigenvalues $a_n(f)$ has finite rank as a $\mathbb{Z}$-module. Let $I_f = \ker(\lambda_f) = \{T \in \mathbb{T}_{\mathbb{Z}} : Tf = 0\}$ and so we have a ring and $\mathbb{Z}$-module isomorphism $\mathbb{T}_{\mathbb{Z}}/I_f \xrightarrow{\sim} \mathbb{Z}[\{a_n(f)\}]$. The ring $\mathbb{Z}[\{a_n(f)\}]$ is in a finite extension of $\mathbb{Q}$ and the extension degree is the rank of $\mathbb{T}_{\mathbb{Z}}/I_f$.

**Definition 3.2.3.** *Let $f \in \mathcal{S}_2(\Gamma_1(N))$ be a normalized eigenform, $f(\tau) = \sum a_n(f) q^n$. 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:

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

It is natural to ask that whether $f^{\sigma}$ is also an eigenform or not.

**Theorem 3.2.2.** *Let $f$ be a weight-2 normalized eigenform for the Hecke operators, so that $f \in \mathcal{S}_2(N, \chi)$ for some $N$ and $\chi$. For any embedding $\sigma : K_f \hookrightarrow \mathbb{C}$ the conjugated $f^\sigma$ is also a normalized eigenform in $\mathcal{S}_2(N, \chi^\sigma)$. If f is a newform then so is $f^\sigma$.*

For the proof of this we need the following two lemmas:

**Lemma 3.2.1.** *Let $A$ be a commutative ring with unity and $J$ be an ideal of $A$. Suppose that $M$ is an $A$-module and a finite dimensional vector space over some field* k. *Then there exists $A$-module isomorphisms*

$$(M/JM)^\wedge \cong M^\wedge[J], \qquad M^\wedge/JM^\wedge \cong M[J]^\wedge$$

*where M[J] denotes the elements of M annihilated by $J$ and similarly for $M^\wedge[J]$.*

*Proof.* Let $\varphi \in (M/JM)^\wedge$ then the map $\tilde{\varphi} : m \mapsto \varphi(m + JM) \in M^\wedge[J]$. Conversely, let $\psi \in M^\wedge[J]$ then the map $\tilde{\psi} : m + JM \mapsto \psi(m) \in (M/JM)^\wedge$. Note that $\tilde{\tilde{\varphi}} = \varphi$ and $\tilde{\tilde{\psi}} = \psi$. Thus the first isomorphism follows. □

**Lemma 3.2.2.** *Let $f \in \mathcal{S}_k(\Gamma_1(N))$ be an eigenform. Then $f$ is old or new.*

*Proof.* If $a_1(f) = 0$ then $f = 0$ by Section **??**. If $a_1(f) \neq 0$ we may assume $a_1(f) = 1$. Hence $T_n f = a_n(f)f$ for all $(n, N) = 1$. Let $f = g + h$ with $g$ is old and $h$ is new. Applying $T_n$ to $f$ gives, $a_n(f)f = T_n g + T_n h$. Since $T_n$ preserves the decomposition of $\mathcal{S}_k(\Gamma_1(N))$ as a direct sum of old and new subspaces we have $T_n g = a_n(f)g$ and $T_n h = a_n(f)h$. Similarly $g$ and $h$ are eigenforms for $\langle n \rangle$ for all $n \in \mathbb{Z}^+$ and so $g$ and $h$ are eigenforms with $T_n$-eigenvalues $a_n(f)$. If $h = 0$, then $f = g$ is old. If $h \neq 0$ then $a_1(h) \neq 0$ and $T_n h = (a_n(h)/a_1(h))h$ and so $a_n(f) = a_n(h)/a_1(h)$ and thus $f = h/a_1(h)$ is new. □

*Proof of Theorem* **??**. We need to show that the conjugated coefficients $\{a_n^\sigma\}$ are also a system of eigenvalues for $T_n$. We know that the Hecke algebra $\mathbb{T}_{\mathbb{Z}}$ acts on the homology $H_1(X_1(N), \mathbb{Z})$. The homology is a free $\mathbb{Z}$-module of rank $2g$ where $g$ is the genus of $X_1(N)$ and the dimension of $\mathcal{S}_2(\Gamma_1(N))$. Let

$$H_1(X_1(N), \mathbb{Z}) = \mathbb{Z}\varphi_1 \oplus \cdots \oplus \mathbb{Z}\varphi_{2g}.$$

With respect to this basis $\sum n_j\varphi_j$ is represented by the row vector $v = [n_j] \in \mathbb{Z}^{2g}$ each element $T \in \mathbb{T}_{\mathbb{Z}}$ is represented by a $2g$-by-$2g$ matrix $[T] \in \mathrm{M}_{2g}(\mathbb{Z})$ and the action of $T$ is $T : v \mapsto v[T]$. This action extends linearly to the complex vector space

$$V = \mathbb{C}\varphi_1 \oplus \cdots \oplus \mathbb{C}\varphi_{2g}.$$

Suppose $\{\lambda(T) : T \in \mathbb{T}_{\mathbb{Z}}\}$ is a system of eigenvalues of $\mathbb{T}_{\mathbb{Z}}$ on $V$. Let $\sigma : \mathbb{C} \to \mathbb{C}$ be any automorphism extending the given embedding $\sigma : K_f \hookrightarrow \mathbb{C}$. Then

$$v^\sigma[T] = (v[T])^\sigma = (\lambda(T)v)^\sigma = \lambda(T)^\sigma v^\sigma, \qquad T \in \mathbb{T}_{\mathbb{Z}}.$$

Thus $\{\lambda(T)^\sigma : T \in \mathbb{T}_{\mathbb{Z}}\}$ is also a system of eigenvalues on $V$.

Denote $\mathcal{S}_2(\Gamma_1(N))$ by $\mathcal{S}_2$. $\mathcal{S}_2$ is isomorphic to its dual space

$$\mathcal{S}_2^\wedge = \mathbb{C}\varphi_1 + \cdots + \mathbb{C}\varphi_{2g}.$$

Since the dimension of $\mathcal{S}_2$ is $g$ the map $V \to \mathcal{S}_2^\wedge$ given by $(z_1\varphi_1, \ldots, z_{2g}\varphi_{2g}) \mapsto \sum z_j\varphi_j$ has $g$ dimensional kernel. Let $w_N = [\left(\begin{smallmatrix} 0 & 1 \\ -N & 0 \end{smallmatrix}\right)]_2$. Then by Section **??**, $w_N T = T^* w_N$ for all $T \in \mathbb{T}_{\mathbb{Z}}$. For any $g \in \mathcal{S}_2$ define

$$\psi_g : \mathcal{S}_2 \to \mathbb{C}, \qquad h \mapsto \langle w_N g, h\rangle.$$

Then $\psi_g(h + \tilde{h}) = \psi_g(h) + \psi_g(\tilde{h})$ and $\psi_g(zh) = \overline{z}\psi_g(h)$. Thus $\psi_g$ is a conjugate linear function on $\mathcal{S}_2$. Denote the set of conjugate linear functions by $\overline{\mathcal{S}_2^\wedge}$. Then $\overline{\mathcal{S}_2^\wedge}$ is the conjugate of the dual space $\mathcal{S}_2^\wedge$ and it is a complex vector space. Since $\psi_{g+\tilde{g}} = \psi_g + \psi_{\tilde{g}}$ and $\psi_{zg} = z\psi_g$ for all $g, \tilde{g} \in \mathcal{S}_2$ and $z \in \mathbb{C}$, the map

$$\Psi : \mathcal{S}_2 \to \overline{\mathcal{S}_2^\wedge}, \qquad g \mapsto \psi_g$$

is $\mathbb{C}$-linear. The kernel of $\Psi$ is trivial hence considering the dimensions $\Psi$ is an isomorphism. $\mathbb{T}_\mathbb{Z}$ acts on $\overline{\mathcal{S}_2^\wedge}$ by right composition and so $\overline{\mathcal{S}_2^\wedge}$ is a $\mathbb{T}_\mathbb{Z}$-module. Since

$$\psi_{Tg} = \langle w_N Tg, h\rangle = \langle T^* w_N g, h\rangle = \langle w_N g, Th\rangle = (\psi_g \circ T)(h)$$

$\Psi$ is $\mathbb{T}_\mathbb{Z}$-linear. Thus $\mathcal{S}_2$ and $\overline{\mathcal{S}_2^\wedge}$ are also isomorphic as $\mathbb{T}_\mathbb{Z}$-modules. Thus $\{\lambda(T) : T \in \mathbb{T}_\mathbb{Z}\}$ is a system of eigenvalues on $\mathcal{S}_2$ if and only if it is a system of eigenvalues on $\overline{\mathcal{S}_2^\wedge}$.

Now let us see that $\{\lambda(T) : T \in \mathbb{T}_\mathbb{Z}\}$ is a system of eigenvalues on $\mathcal{S}_2$ if and only if it is a system of eigenvalues on $\mathcal{S}_2^\wedge$. Let $f \in \mathcal{S}_2$ and consider the map

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

Let $J_f = \ker(\lambda_f) = \{T \in \mathbb{T}_\mathbb{C} : Tf = 0\}$. Then $J_f$ is a prime ideal of $\mathbb{T}_\mathbb{C}$. Let $A$ be the localization of $\mathbb{T}_\mathbb{C}$ at the prime ideal $J_f$. Then the ideal $J = J_f A$ is the unique maximal ideal in $A$. Also let $M$ be the localization of $\mathcal{S}_2$ at $J_f$. Then $M$ is an $A$-module and $M \neq 0$ as $f/U \neq 0$ for any $U \in \mathbb{T}_\mathbb{C} - J_f$. Hence by Nakayama's Lemma $JM \neq M$ and so $J_f\mathcal{S}_2 \neq \mathcal{S}_2$. Thus the quotient $\mathcal{S}_2/J_f\mathcal{S}_2$ is nontrivial. By Lemma **??** we have

$$\mathcal{S}_2^\wedge[J_f] = \{\varphi \in \mathcal{S}_2^\wedge : \varphi \circ T = 0 \text{ for all } T \in J_f\} \neq 0.$$

Since $T_1$ is the identity operator, $T - \lambda_f(T)T_1 \in J_f$ for all $T \in \mathbb{T}_\mathbb{C}$ and so for any nonzero $\varphi \in \mathcal{S}_2^\wedge[J_f]$ we have

$$\varphi \circ T = \varphi \circ (T - \lambda_f(T)T_1) + \lambda_f(T)\varphi = \lambda_f(T)\varphi, \quad T \in \mathbb{T}_\mathbb{C}.$$

Restricting to $\mathbb{T}_{\mathbb{Z}}$, $\{\lambda_f(T) : T \in \mathbb{T}_{\mathbb{Z}}\}$ is a system of eigenvalues on $\mathcal{S}_2^{\wedge}$. The converse follows from the fact that double dual of finite dimensional vector spaces isomorphic to itself as a $\mathbb{T}_{\mathbb{Z}}$-module. Thus the cusp forms $\mathcal{S}_2$ and the sum $\mathcal{S}_2^{\wedge} \oplus \overline{\mathcal{S}_2^{\wedge}}$ have the same systems of eigenvalues.

Now consider the $\mathbb{C}$-linear map

$$V \to \mathcal{S}_2^{\wedge} \oplus \overline{\mathcal{S}_2^{\wedge}}, \qquad (z_1\varphi_1, \dots, z_{2g}\varphi_{2g}) \mapsto (\sum z_j\varphi_j, \sum z_j\overline{\varphi_j}).$$

This map is also a $\mathbb{T}_{\mathbb{Z}}$-module homomorphism as $\overline{\varphi_j \circ T} = \overline{\varphi_j} \circ T$. Suppose $\sum z_j\varphi_j = 0$ in $\mathcal{S}_2^{\wedge}$ and $\sum z_j\overline{\varphi_j} = 0$ in $\overline{\mathcal{S}_2^{\wedge}}$. Then $\sum \overline{z_j}\varphi_j = 0$ in $\mathcal{S}_2^{\wedge}$. Thus $\sum \mathrm{Re}(z_j)\varphi_j = 0$ and $\sum \mathrm{Im}(z_j)\varphi_j = 0$ in $\mathcal{S}_2^{\wedge}$. Since $\{\varphi_j\}$ are linearly independent over $\mathbb{R}$, $z_j = 0$ for all $j$. Thus the kernel of the above map is trivial and considering the dimensions of the domain and codomain it is an isomorphism of $\mathbb{T}_{\mathbb{Z}}$-modules.

Now we have seen that if $\{\lambda(T) : T \in \mathbb{T}_{\mathbb{Z}}\}$ is a system of eigenvalues on $V$ then $\{\lambda(T)^\sigma : T \in \mathbb{T}_{\mathbb{Z}}\}$ is also a system of eigenvalues on $V$. By the above isomorphism this is also true for the sum $\mathcal{S}_2^{\wedge} \oplus \overline{\mathcal{S}_2^{\wedge}}$. But we have also seen that $\mathcal{S}_2^{\wedge} \oplus \overline{\mathcal{S}_2^{\wedge}}$ and $\mathcal{S}_2$ have the same systems of eigenvalues and so the result is also true for $\mathcal{S}_2$. This proves that $f^\sigma(\tau) = \sum a_n^\sigma q^n$ is a normalized eigenform in $\mathcal{S}_2(N, \chi^\sigma)$.

For the last part of the theorem, suppose that $f$ is a newform. Then by Theorem **??**, $f^\sigma(\tau) = \sum_i a_i f_i(n_i\tau)$ where each $f_i$ is a newform of level $M_i$ such that $n_iM_i \mid N$. Let $\gamma = \sigma^{-1} : \mathbb{C} \to \mathbb{C}$. Then $\gamma|_{K_f}$ is another embedding of $K_f$ into $\mathbb{C}$. Then $f = (f^\sigma)^\gamma = \sum_i a_i^\gamma f_i^\gamma(n_i\tau)$. Assume that $f^\sigma$ is not a newform. Then by Lemma **??** it has to be an oldform which makes all $M_i$ strictly less than $N$. Since each $f_i^\gamma$ is also a modular form of level $M_i$ this shows that $f$ is an old form, contradiction. Thus $f^\sigma$ is a newform. □

**Corollary 3.2.1.** *The space $\mathcal{S}_2(\Gamma_1(N))$ has a basis of forms with rational integer coefficients.*

*Proof.* Let $f$ be a newform of level $M$ with $M \mid N$. Let $K = K_f$ and $\{\alpha_1, \ldots, \alpha_d\}$ be a basis of $\mathcal{O}_K$ as a $\mathbb{Z}$-module. Let $\{\sigma_1, \ldots, \sigma_d\}$ be the embeddings of $K$ into $\mathbb{C}$. Consider the matrix

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

and let

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

Let $\vec{g} = A\vec{f}$. That is

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

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 all $a_n(g_i) \in \overline{\mathbb{Z}}$. For any automorphism $\sigma : \mathbb{C} \to \mathbb{C}$ we have

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

Thus each $a_n(g_i)$ is fixed by all automorphisms of $\mathbb{C}$ which proves that $a_n(g_i) \in \overline{\mathbb{Z}} \cap \mathbb{Q} = \mathbb{Z}$. □

## 3.3 Abelian variety associated to a newform

In this section we define the Abelian variety associated to a newform and decompose the Jacobian $J_1(N)$ into a direct sum of complex tori.

Let $f \in \mathcal{S}_2(\Gamma_1(M_f))$ be a newform at some level $M_f$. Recall the map

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

This induces a $\mathbb{T}_{\mathbb{Z}}$-module isomorphism $\mathbb{T}_{\mathbb{Z}}/I_f \cong \mathbb{Z}[\{a_n(f)\}]$ and $\mathbb{Z}[\{a_n(f)\}]$ has rank $[K_f : \mathbb{Q}]$. Also we have seen that $\mathbb{T}_{\mathbb{Z}}$ acts on $J_1(M_f)$.

**Definition 3.3.1.** *The Abelian variety associated to $f$ is defined as the quotient*

$$A_f = J_1(M_f)/I_f J_1(M_f).$$

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 **??**, $(a_p(f)\varphi)(f^\sigma) = (\varphi \circ T_p)(f^\sigma) = \varphi(a_p(f^\sigma)f^\sigma) = a_p(f)^\sigma \varphi(f^\sigma)$. 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 $f$. By Theorem **??** each $f^\sigma \in [f]$ is a newform at level $M_f$ and so by Theorem **??** the subspace

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

has dimension $[K_f : \mathbb{Q}]$. Restricting the elements of $H_1(X_1(M_f), \mathbb{Z})$ to functions on $V_f$ gives a subgroup of the dual space $V_f^\wedge$,

$$\Lambda_f = H_1(X_1(M_f), \mathbb{Z})|_{V_f}$$

and so we have a well defined homomorphism

$$J_1(M_f) \to V_f^\wedge/\Lambda_f, \qquad [\varphi] \mapsto \varphi|_{V_f} + \Lambda_f \text{ for } \varphi \in \mathcal{S}_2(\Gamma_1(M_f))^\wedge.$$

**Proposititon 3.3.1.** *Let $f \in \mathcal{S}_2(\Gamma_1(M_f))$ be a newform with number field $K_f$. Then restricting to $V_f$ induces an isomorphism*

$$A_f \xrightarrow{\sim} V_f^\wedge/\Lambda_f, \qquad [\varphi] + I_f J_1(M_f) \mapsto \varphi|_{V_f} + \Lambda_f \text{ for } \varphi \in \mathcal{S}_2(\Gamma_1(M_f))^\wedge,$$

*and the right side is a complex torus of dimension $[K_f : \mathbb{Q}]$.*

*Proof.* Let $\mathcal{S}_2 = \mathcal{S}_2(\Gamma_1(M_f))$ and $H_1 = H_1(X_1(M_f), \mathbb{Z})$. Then

$$\begin{aligned} A_f &= J_1(M_f)/I_f J_1(M_f) = (\mathcal{S}_2^\wedge/H_1)/I_f(\mathcal{S}_2^\wedge/H_1) \\ &= \mathcal{S}_2^\wedge/(I_f\mathcal{S}_2^\wedge + H_1) \cong (\mathcal{S}_2^\wedge/I_f\mathcal{S}_2^\wedge)/(\text{image of } H_1 \text{ in } \mathcal{S}_2^\wedge/I_f\mathcal{S}_2^\wedge). \end{aligned}$$

By Lemma **??** we have $\mathcal{S}_2^\wedge/I_f\mathcal{S}_2^\wedge \cong \mathcal{S}_2[I_f]^\wedge$ where the isomorphism is given by $\varphi + I_f\mathcal{S}_2 \mapsto \varphi|_{\mathcal{S}_2[I_f]}$ for $\varphi \in \mathcal{S}_2^\wedge$. Hence

$$A_f \xrightarrow{\sim} \mathcal{S}_2[I_f]^\wedge/H_1|_{\mathcal{S}_2[I_f]}, \qquad [\varphi] + I_f J_1(M_f) \mapsto \varphi|_{\mathcal{S}_2[I_f]} + H_1|_{\mathcal{S}_2[I_f]}.$$

Let us see that $V_f = \mathcal{S}_2[I_f]$. Clearly $V_f \subset \mathcal{S}_2[I_f]$. For the reverse inclusion consider the pairing

$$\mathbb{T}_\mathbb{C} \times \mathcal{S}_2 \to \mathbb{C}, \qquad (T, g) \mapsto a_1(Tg).$$

This is a perfect pairing. It is clearly linear. For the nondegeneracy suppose $T \in \mathbb{T}_\mathbb{C}$ and $a_1(Tg) = 0$ for all $g \in \mathcal{S}_2$. Then for all $n \in \mathbb{Z}^+$ we have $a_n(Tg) = a_1(T_nTg) = a_1(TT_ng) = 0$. Hence $Tg = 0$ for all $g \in \mathcal{S}_2$ which implies $T = 0$. Similarly suppose $g\mathcal{S}_2$ and $a_1(Tg) = 0$ for all $T \in \mathbb{T}_\mathbb{C}$. Then $0 = a_1(T_ng) = a_n(g)$ and so $g = 0$. Thus the pairing is perfect. Therefore we have a vector space and $\mathbb{T}_\mathbb{Z}$-module isomorphism $\mathcal{S}_2 \cong \mathbb{T}_\mathbb{C}$ given by $g \mapsto (T \mapsto a_1(Tg))$. By using the above pairing and Lemma **??** we get

$$\dim(\mathcal{S}_2[I_f]) = \dim(\mathcal{S}_2[I_f]^\wedge) = \dim(\mathcal{S}_2^\wedge/I_f\mathcal{S}_2^\wedge) = \dim(\mathbb{T}_\mathbb{C}/I_f\mathbb{T}_\mathbb{C}).$$

Note that we have a surjection $\mathbb{T}_{\mathbb{Z}} \otimes \mathbb{C} \to \mathbb{T}_{\mathbb{C}}$ that is given by $\sum_i U_i \otimes z_i \mapsto \sum_i z_i U_i$. Viewing $z_i = z_i T_1 \in \mathbb{T}_{\mathbb{C}}$ we see that the image of $I_f \otimes \mathbb{C}$ lies in $I_f \mathbb{T}_{\mathbb{C}}$ hence we have a surjection $(\mathbb{T}_{\mathbb{Z}} \otimes \mathbb{C})/(I_f \otimes \mathbb{C}) \to \mathbb{T}_{\mathbb{C}}/I_f \mathbb{T}_{\mathbb{C}}$ and this gives

$$\begin{aligned} \dim(\mathcal{S}_2[I_f]) &\leqslant \dim((\mathbb{T}_{\mathbb{Z}} \otimes \mathbb{C})/(I_f \otimes \mathbb{C})) = \dim(\mathbb{T}_{\mathbb{Z}}/I_f \otimes \mathbb{C}) \\ &= \operatorname{rank}(\mathbb{T}_{\mathbb{Z}}/I_f) = [K_f : \mathbb{Q}] = \dim(V_f). \end{aligned}$$

This proves that $V_f = \mathcal{S}_2[I_f]$. Now we need to show that $\Lambda_f$ is a lattice in $V_f^\wedge$. It suffices to prove that $\mathbb{R}$-span of $\Lambda_f$ is $V_f^\wedge$ and $\operatorname{rank}(\Lambda_f) \leqslant \dim_{\mathbb{R}}(V_f^\wedge)$. Since $V_j \subset \mathcal{S}_2$ we have a surjection $\pi : \mathcal{S}_2^\wedge \to V_f^\wedge$ that is given by $\varphi \mapsto \varphi|_{V_f}$. Since the $\mathbb{R}$-span of $H_1$ is $\mathcal{S}_2^\wedge$, the $\mathbb{R}$-span of $\Lambda_f = \pi(H_1)$ is $\pi(\mathcal{S}_2^\wedge) = V_f^\wedge$. Moreover considering the dimensions over $\mathbb{R}$ we have

$$\begin{aligned} \dim(V_f^\wedge) &= \dim(\mathcal{S}_2[I_f]^\wedge) = \dim(\mathcal{S}_2^\wedge / I_f \mathcal{S}_2^\wedge) \\ &= \dim((H_1 \otimes \mathbb{R})/I_f(H_1 \otimes \mathbb{R})) \\ &= \dim((H_1 \otimes \mathbb{R})/(I_f H_1 \otimes \mathbb{R})) \\ &= \dim(H_1/I_f H_1 \otimes \mathbb{R}) \\ &= \operatorname{rank}(H_1/I_f H_1). \end{aligned}$$

Note that $\Lambda_f = \pi(H_1) \cong H_1/(H_1 \cap \ker(\pi))$ and $I_f H_1 \subset (H_1 \cap \ker(\pi))$. Hence we have a surjection $H_1/I_f H_1 \to \Lambda_f$ and so $\operatorname{rank}(\Lambda_f) \leqslant \operatorname{rank}(H_1/I_f H_1) = \dim_{\mathbb{R}}(V_f^\wedge)$. □

**Definition 3.3.2.** *An isogeny is a holomorphic homomorphism between complex tori that subjects and has finite kernel.*

The next theorem gives the decomposition of $J_1(N)$ that we have mentioned above.

**Theorem 3.3.1.** *$J_1(N)$ is isogeneous to a direct sum of Abelian varieties associated to equivalence classes of newforms,*

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

*where the 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.* Denote $\mathcal{S}_2(\Gamma_1(N))$ by $\mathcal{S}_2$ and $H_1(X_1(N), \mathbb{Z})$ by $H_1$. By Theorem **??** and **??**,

$$\mathcal{B}_2(N) = \bigcup_f \bigcup_n \bigcup_\sigma f^\sigma(n\tau)$$

is a basis of $\mathcal{S}_2$ where the first union is over equivalence class representatives, the second is over divisors of $N/M_f$ and the last one is over embeddings $\sigma : K_f \to \mathbb{C}$. For each pair $(f, n)$ let $d = [K_f : \mathbb{Q}]$ and $\sigma_1, \ldots, \sigma_d$ be embeddings of $K_f$ into $\mathbb{C}$ and consider

$$\Psi_{f,n} : \mathcal{S}_2^\wedge \to V_f^\wedge, \qquad \varphi \mapsto (\psi : \sum_{j=1}^d z_j f^{\sigma_j}(\tau) \mapsto \sum_{j=1}^d z_j n \varphi(f^{\sigma_j}(n\tau))).$$

Let $\varphi = \int_\alpha$ for some loop $\alpha$ in $X_1(N)$. Identifying the holomorphic differential $\omega(f^\sigma(n\tau))$ with its pullback to $\mathcal{H}$ and $\alpha$ with some lift to $\mathcal{H}$ we get

$$\Psi_{f,n}(\varphi)(f^\sigma(\tau)) = \psi(f^\sigma(\tau)) = n \int_\alpha f^\sigma(n\tau) d\tau = \int_{\tilde{\alpha}} f^\sigma(\tau) d\tau$$

where $\tilde{\alpha}(t) = n\alpha(t)$. Thus $\psi = \int_{\tilde{\alpha}}$ and so $\Psi_{f,n}$ takes $H_1$ to $\Lambda_f$.

Taking the product map gives

$$\Psi = \prod_{f,n} \Psi_{f,n} : \mathcal{S}_2^\wedge \to \bigoplus_{f,n} V_f^\wedge = \bigoplus_f (V_f)^{m_f}.$$

$\Psi$ is surjective. To see this let $\varphi \in \mathcal{S}_2^\wedge$ be such that $\varphi(f^\sigma(n\tau)) = 1$ and it is zero at the other basis elements of $\mathcal{S}_2^\wedge$. Then the map $\Psi_{f,n}(\varphi) = \psi$ takes $f^\sigma(\tau)$ to n and other basis elements of $V_f$ to 0. Thus as $\sigma$ changes the corresponding $\psi$ generate $V_f^\wedge$ which proves that $\Psi$ is surjective. Considering the basis of the each component of the direct sum we see that both sides have the same dimension and so $\Psi$ is an isomorphism. Hence we have the following isomorphism of quotients

$$\overline{\Psi} : J_1(N) \xrightarrow{\sim} \bigoplus_f (V_f^\wedge)^{m_f}/\Psi(H_1).$$

Since $\Psi(H_1) \subset \bigoplus_f (\Lambda_f)^{m_f}$ and they are Abelian groups of the same rank the surjection

$$\pi : \bigoplus_f (V_f)^{m_f}/\Psi(H_1) \to \bigoplus_f (V_f/\Lambda_f)^{m_f}$$

has finite kernel. By Proposition **??** we have the following isomorphism

$$i : \bigoplus_f (V_f/\Lambda_f)^{m_f} \xrightarrow{\sim} \bigoplus_f (A_f)^{m_f}.$$

Putting these together $i \circ \pi \circ \overline{\Psi} : J_1(N) \to \bigoplus_f (A_f)^{m_f}$ is an isogeny. □

Using the isogeny of Theorem **??** we can construct 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 the isogenies of Theorem **??**. 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.

# 4 Modular curves as algebraic curves and Eichler-Shimura relation

In this chapter we show that the modular curves $X_1(N)$ and $X_0(N)$ are algebraic curves over $\mathbb{Q}$.

## 4.1 Weil pairing

We start with recalling some facts about elliptic curves. For more details see [**?**]. Let $k$ be a field of characteristic 0 and $E$ be an elliptic curve over $k$. The set of $N$-torsion points of $E$ is a subgroup, $E[N]$, of $E$ isomorphic to $(\mathbb{Z}/N\mathbb{Z})^2$. The map

$$\mathrm{Div}(E) \to E, \qquad \sum n_P(P) \mapsto \sum [n_P]P$$

induces an isomorphism $\mathrm{Pic}^0(E) \xrightarrow{\sim} E$. Hence principal divisors on $E$ are characterized by

$$\sum n_P(P) \in \mathrm{Div}^\ell(E) \Leftrightarrow \sum n_P = 0 \text{ and } \sum [n_P]P = 0_E.$$

Let $\mu_N$ denote the group of $N$th roots of unity in $\bar{k}$, $\mu_N = \{x \in \bar{k} : x^N = 1\}$. The Weil pairing

$$e_N : E[N] \times E[N] \to \mu_N$$

is defined as follows: Let $P, Q \in E[N]$. Then by the above characterization of principal divisors, there exists a function $f = f_Q \in \bar{k}(E)$ such that $\mathrm{div}(f) = N(Q) - N(0_E)$. Since the map $[N] : E \to E$ is unramified and $\nu_P(f \circ [N]) = e_P([N])\nu_{[N]P}(f)$ we have

$$\mathrm{div}(f \circ [N]) = \sum_{[N]R=Q} N(R) - \sum_{[N]S=0_E} N(S).$$

Let $Q' \in E[N^2]$ be any point such that $[N]Q' = Q$. Then

$$\operatorname{div}(f \circ [N]) = N \sum_{S \in E[N]} \{(Q' + S) - (S)\}.$$

By the above characterization of principal divisors again the above sum is again a principal divisor for some $g = g_Q \in \bar{k}(E)$ and so

$$\operatorname{div}(f \circ [N]) = N\operatorname{div}(g).$$

This shows that $f \circ [N]$ and $g^N$ has the same divisors and so $\operatorname{div}(f \circ [N] - g^N) = 0$ which makes $cf \circ [N] = g^N$ for some constant $c \in \bar{k}^*$. For any point $X \in E$ we have

$$g(X + P)^N = cf([N]X + [N]P) = cf([N]X) = g(X)^N.$$

Thus the $N$th power of the rational function $g(X + P)/g(X) \in \bar{k}(E)$ the image of this function is a subset of $\mu_N$. Since the map is not surjective from $E \to \mathbb{P}^1(\bar{k})$ it is constant. The image point is the Weil pairing of $P$ and $Q$,

$$e_N(P, Q) = \frac{g(X + P)}{g(X)} \in \mu_N.$$

Next proposition proves the basic properties of the Weil pairing.

**Proposititon 4.1.1.** *1. The Weil pairing is bilinear,*

$$e_N(aP + bP', cQ + dQ') = e_N(P, Q)^{ac} e_N(P, Q')^{ad} e_N(P', Q)^{bc} e_N(P', Q')^{bd}.$$

*2. The Weil pairing is alternating*

$$e_N(Q, Q) = 1, \qquad e_N(Q, P) = e_N(P, Q)^{-1}.$$

*3. The Weil pairing is nondegenerate*

$$if\ e_N(P, Q) = 1\ for\ all\ P \in E[N]\ then\ Q = 0_E.$$

*Hence $e_N$ is surjective.*

*4. The Weil pairing is Galois invariant*

$$e_N(P,Q)^\sigma = e_N(P^\sigma, Q^\sigma) \text{ for all } \sigma \in \mathrm{Gal}(\bar{k}/k).$$

*Proof.* 1. Let $g = g_Q$. Then

$$\begin{aligned} e_N(P_1+P_2,Q) &= \frac{g(X+P_1+P_2)}{g(X)} = \frac{g(X+P_1+P_2)}{g(X+P_2)}\frac{g(X+P_2)}{g(X)} \\ &= e_N(P_1,Q)e_N(P_2,Q). \end{aligned}$$

Hence $e_N$ is linear in the first argument. For linearity in the second argument let $f_1, f_2, f_3$ and $g_1, g_2, g_3$ be the functions associated to $Q_1, Q_2$ and $Q_1 + Q_2$. There exists a function $h \in \bar{k}(E)$ such that

$$\mathrm{div}(h) = (Q_1+Q_2) - (Q_1) - (Q_2) + (0_E).$$

Then $\mathrm{div}(f_3/f_1f_2) = N\mathrm{div}(h)$ and so $f_3 = cf_1f_2h^N$ for some $c \in \bar{k}^*$. Thus $g_3^N = c(g_1g_2(h \circ [N]))^N$. Therefore we have

$$\begin{aligned} e_N(P,Q_1+Q_2) &= \frac{g_3(X+P)}{g(X)} \\ &= \frac{g_1(X+P)g_2(X+P)h([N]X+[N]P)}{g_1(X)g_2(X)h([N]X)} \\ &= e_N(P,Q_1)e_N(P,Q_2). \end{aligned}$$

2. Let $f = f_Q$ and $g = g_Q$. Then

$$\mathrm{div}(\prod_{n=0}^{N-1} f(X+[n]Q)) = \sum_{n=0}^{N-1} N([1-n]Q) - N([-n]Q) = 0.$$

Hence $\prod_{n=0}^{N-1} f(X+[n]Q)$ is constant and so if $Q = [N]Q'$ then $\prod_{n=0}^{N-1} g(X + [n]Q')$ is constant. Thus

$$\prod_{n=0}^{N-1} g(X+[n]Q') = \prod_{n=0}^{N-1} g(X+Q'+[n]Q')$$

which implies that $g(X) = g(X+[N]Q') = g(X+Q)$ and so $e_N(Q,Q) = 1$.

3. Suppose $e_N(P,Q) = 1$ for all $P \in E[N]$ and let $g = g_Q$. Hence $g(X+P) = g(X)$ for all $P \in E[N]$. Consider the map $\tau^* : E[N] \to \mathrm{Aut}(\bar{k}(E))$, defined by $P \mapsto (\tau_P^* : f(X) \mapsto f(X+P))$. Then $\tau^*$ is a homomorphism. Let $P \in \ker(\tau^*)$. Then $\tau_P^*(f) = f$ for all $f \in \bar{k}(E)$ and so $f(0_E) = \tau_P^*(f(0_E)) = f(P)$ for all $f \in \bar{k}(E)$. Thus $P = 0_E$ and $\tau^*$ is injective. Now $\bar{k}(E)$ is a Galois extension of its subfield fixed by $\tau^*(E[N])$ with Galois group isomorphic to $E[N]$. The fixed field contains $[N]^*(\bar{k}(E))$ and the degree of $[N]$ is $N^2 = [\bar{k}(E) : [N]^*(\bar{k}(E))]$. Since $|E[N]| = N^2$ the fixed field is exactly $[N]^*(\bar{k}(E))$. This shows that $g = h \circ [N]$ for some $h \in \bar{k}(E)$. Hence

$$\mathrm{div}(h \circ [N]) = \mathrm{div}(g) = \sum_{S \in E[N]} \{(Q' + S) - (S)\}$$

where $[N]Q' = Q$. Thus $\mathrm{div}(h) = Q - 0_E$ and so $Q = 0_E$.

4. Let $\sigma \in \mathrm{Gal}(\bar{k}/k)$. Then $f_{Q^\sigma} = f_Q^\sigma$ and $g_{Q^\sigma} = g_Q^\sigma$. Hence

$$e_N(P^\sigma, Q^\sigma) = \frac{g^\sigma(X^\sigma + P^\sigma)}{g(X^\sigma)} = \left(\frac{g(X+P)}{g(X)}\right)^\sigma = e_N(P,Q)^\sigma.$$

□

**Corollary 4.1.1.** *Let $P, Q, P', Q' \in E[N]$ and $\binom{P}{Q} = \gamma\binom{P'}{Q'}$ for some $\gamma \in M_2(\mathbb{Z}/N\mathbb{Z})$. Then $e_N(P', Q') = e_N(P,Q)^{\det\gamma}$. Therefore if $(P,Q)$ is an ordered basis then $e_N(P,Q)$ is a primitive $N$th root of unity.*

*Proof.* This follows from the properties (1) and (2) of the Proposition **??**. □

## 4.2 Modular curves and function fields over $\mathbb{C}$

The field of meromorphic functions on $\mathrm{SL}_2(\mathbb{Z})\backslash\mathcal{H}^* = X(1)$ over $\mathbb{C}$ is generated by the modular invariant j from Section **??**, $\mathbb{C}(X(1)) = \mathbb{C}(j)$. In this section we describe the function fields of the curves $X(N)$, $X_1(N)$ and $X_0(N)$. For each element $v = (c_v, d_v) \in \mathbb{Z}^2$ such that $\bar{v} \neq 0$ where $\bar{v} \equiv v (\text{mod } N)$. Let

$$f_0^{\bar{v}}(\tau) = \frac{g_2(\tau)}{g_3(\tau)} \wp_\tau \left( \frac{c_v \tau + d_v}{N} \right).$$

Then $f_0^{\bar{v}}$ is weight-0 invariant under $\Gamma(N)$ and $f_0^{\bar{v}} \in \mathbb{C}(X(N))$. Let $d \not\equiv 0 (\text{mod } N)$ and define

$$f_0^{\bar{d}}(\tau) = f_0^{\overline{(0,d)}}(\tau), \qquad f_0(\tau) = \sum_{d=1}^{N-1} f_0^{\bar{d}}(\tau).$$

These functions are weight-0 invariant under $\Gamma_1(N)$ and $\Gamma_0(N)$, respectively and so $f_0^{\bar{d}}(\tau) \in \mathbb{C}(X_1(N))$ and $f_0(\tau) \in \mathbb{C}(X_0(N))$. Denote $f_0^{\pm\overline{(1,0)}}$ by $f_{1,0}$ and $f_0^{\pm\overline{(0,1)}}$ by $f_{0,1}$. Let $j_N(\tau) = j(N\tau)$. Then $j_N \in \mathbb{C}(X_0(N))$.

**Proposititon 4.2.1.** *The fields of meromorphic functions on $X(N)$, $X_1(N)$ and $X_0(N)$ are*

$$\mathbb{C}(X(N)) = \mathbb{C}(j, f_{1,0}, f_{0,1}),\ \mathbb{C}(X_1(N)) = \mathbb{C}(j, f_{0,1}),\ \mathbb{C}(X_0(N)) = \mathbb{C}(j, f_0) = \mathbb{C}(j, j_N).$$

*Proof.* Since $\wp_\tau(z) = \wp_\tau(z')$ if and only if $z \equiv \pm z' (\text{mod } N)$, $f_0^{\bar{v}} = f_0^{-\bar{v}}$ and all $f_0^{\bar{v}}$ are distinct otherwise. We have the containments $\mathbb{C}(X(1)) = \mathbb{C}(j) \subset \mathbb{C}(j, \{f_0^{\pm\bar{v}}\}) \subset \mathbb{C}(X(N))$. Now consider the homomorphism

$$\theta : \mathrm{SL}_2(\mathbb{Z}) \to \mathrm{Aut}(\mathbb{C}(X(N))), \qquad f^{\theta(\gamma)} = f \circ \gamma.$$

$f \circ \gamma \in \mathbb{C}(X(N))$ since $\Gamma(N) \lhd \mathrm{SL}_2(\mathbb{Z})$. Clearly we have $\{\pm I\}\Gamma(N) \subset \ker(\theta)$. Let $\gamma \in \ker(\theta)$. Then $\gamma$ fixes the subfield $\mathbb{C}(j, \{f_0^{\pm\bar{v}}\})$. Since $f_0^{\bar{v}} \circ \gamma = f_0^{\overline{v\gamma}}$ and $f_0^{\pm\bar{v}}$ are distinct, $\gamma \in \{\pm I\}\Gamma(N)$. Thus $\{\pm I\}\Gamma(N) = \ker(\theta)$ and so $\theta(\mathrm{SL}_2(\mathbb{Z})) \cong \mathrm{SL}_2(\mathbb{Z})/\{\pm I\}\Gamma(N)$. The subfield of $\mathbb{C}(X(N))$ that is fixed by $\theta(\mathrm{SL}_2(\mathbb{Z}))$ is $\mathbb{C}(X(1))$ hence $\mathbb{C}(X(N))/\mathbb{C}(X(1))$ is Galois with Galois group $\theta(\mathrm{SL}_2(\mathbb{Z}))$. The subfields $\mathbb{C}(j, \{f_0^{\pm\bar{v}}\})$ and $\mathbb{C}(j, f_{1,0}, f_{0,1})$ both have trivial fixing subgroup and thus they are equal to $\mathbb{C}(X(N))$.

For the second equality consider the set $\{f_0^{\bar{d}} : \bar{d} \in (\mathbb{Z}/N\mathbb{Z} - 0)/\pm\}$ and the containments $\mathbb{C}(X(1)) \subset \mathbb{C}(j, \{f_0^{\bar{d}}\}) \subset \mathbb{C}(X_1(N)) \subset \mathbb{C}(X(N))$. Since $f_0^{\bar{d}} \circ \gamma = f^{\overline{(0,d)\gamma}}$ for $\gamma \in \mathrm{SL}_2(\mathbb{Z})$, the subfields $\mathbb{C}(j, \{f_0^{\bar{d}}\})$ and $\mathbb{C}(j, f_{0,1})$ have fixing subgroup $\{\pm I\}\Gamma_1(N)/\{\pm I\}\Gamma(N)$ which is the fixing subgroup of $\mathbb{C}(X_1(N))$. This proves that $\mathbb{C}(X_1(N)) = \mathbb{C}(j, \{f_0^{\bar{d}}\}) = \mathbb{C}(j, f_{0,1})$. This also shows that

$$\theta^{-1}(\mathrm{Gal}(\mathbb{C}(X(N))/\mathbb{C}(X_1(N)))) = \left\{\pm\left(\begin{smallmatrix} 1 & b \\ 0 & 1 \end{smallmatrix}\right) \in SL_2(\mathbb{Z}/N\mathbb{Z})/\{\pm I\}\right\}.$$

The last equality is similar. □

By the above proposition and the correspondence between algebraic curves and function fields, $X_1(N)$ is birationally equivalent to the plane curve defined by the complex polynomial $\varphi \in \mathbb{C}[x, y]$ such that $\varphi(j, f_{0,1}) = 0$.

The map $\theta$ in the proof of Proposition **??** gives the isomorphism

$$\theta^{-1} : \mathrm{Gal}(\mathbb{C}(X(N))/\mathbb{C}(X(1))) \xrightarrow{\sim} SL_2(\mathbb{Z}/N\mathbb{Z})/\{\pm I\}, \qquad f^\sigma = f \circ \theta^{-1}(\sigma)$$

where $f \in \mathbb{C}(X(N))$ and $\sigma \in \mathrm{Gal}(\mathbb{C}(X(N))/\mathbb{C}(X(1)))$.

Recall from Section **??** that $(\wp_\tau, \wp_\tau') : \mathbb{C}/\Lambda_\tau \to E_\tau$ where $E_\tau : y^2 = 4x^3 - g_2(\tau)x - g_3(\tau)$. Fix $\tau \in \mathcal{H}$ such that $j(\tau) \notin \{0, 1728\}$. Hence $g_2(\tau)$ and $g_3(\tau)$ are nonzero. Let $u = (g_3(\tau)/g_2(\tau))^{1/2}$ be one of the complex root and consider the map

$$\left(u^2\wp_\tau, u^3\wp_\tau'\right) : \mathbb{C}/\Lambda_\tau \to \mathbb{C}^2 \cup \{\infty\}.$$

This differs from $(\wp_\tau, \wp_\tau')$ by an admissible change of variable. The corresponding cubic equation is

$$E_{j(\tau)} : y^2 = 4x^3 - \frac{g_2(\tau)^3}{g_3(\tau)^2}x - \frac{g_2(\tau)^3}{g_3(\tau)^2}.$$

Since $g_2^3/g_3^2 = 27j/(j - 1728)$ we have

$$E_{j(\tau)} : y^2 = 4x^3 - \frac{27j(\tau)}{j(\tau) - 1728}x - \frac{27j(\tau)}{j(\tau) - 1728}$$

The map $\mathbb{C}/\Lambda_\tau \xrightarrow{\sim} E_{j(\tau)}$ gives an isomorphism of $N$-torsion subgroups. Under this isomorphism the canonical generators $\tau/N + \Lambda_\tau$ and $1/N + \Lambda_\tau$ of $(\mathbb{C}/\Lambda_\tau)[N]$ maps to

$$P_\tau = \left( \frac{g_2(\tau)}{g_3(\tau)} \wp_\tau(\tau/N), \frac{g_2(\tau)}{g_3(\tau)}^{3/2} \wp'_\tau(\tau/N) \right),$$

$$Q_\tau = \left( \frac{g_2(\tau)}{g_3(\tau)} \wp_\tau(1/N), \frac{g_2(\tau)}{g_3(\tau)}^{3/2} \wp'_\tau(1/N) \right).$$

Hence $(P_\tau, Q_\tau)$ is a canonical ordered basis of $E_{j(\tau)}[N]$ over $\mathbb{Z}/N\mathbb{Z}$. Observe that the $x$-coordinates of $P_\tau$ and $Q_\tau$ are $f_{1,0}(\tau)$ and $f_{0,1}(\tau)$ respectively and the nonzero points of $E_{j(\tau)}[N]$ have $x$-coordinates $\{f_0^{\pm\bar{v}}(\tau)\}$. Thus knowing $j(\tau)$, $f_{1,0}(\tau)$ and $f_{0,1}(\tau)$ describes an enhanced elliptic curve for $\Gamma(N)$, $(E_{j(\tau)}, (P_\tau, Q_\tau))$ which represents a point $[\mathbb{C}/\Lambda_\tau, (\tau/N + \Lambda_\tau, 1/N + \Lambda_\tau)]$ of the moduli space $S(N)$. Similarly knowing $j(\tau)$ and $f_{0,1}$ describe $(E_{j(\tau)}, Q_\tau)$ representing a point of $S_1(N)$.

Now change $\tau$ to a variable. Hence we get a family of elliptic curves $E_{j(\tau)}$ and putting this family together we get a universal elliptic curve

$$E_j : y^2 = 4x^3 - \frac{27j}{j-1728}x - \frac{27j}{j-1728}$$

with $j$-invariant equal to variable $j$. The universal $N$-torsion $x$-coordinates are $\{f_0^{\pm\bar{v}}\}$. Let $x(E_j[N])$ denote the set of $x$-coordinates of the nonzero points of $E_j[N]$. Viewing $E_j$ as an elliptic curve over $\mathbb{C}(j)$, we have $x(E_j[N]) \subset \overline{\mathbb{C}(j)}$. With this terminology Proposition **??** says that $\mathbb{C}(X(N)) = \mathbb{C}(j, x(E_j[N]))$ and

$$\mathrm{Gal}(\mathbb{C}(j, x(E_j[N]))/\mathbb{C}(j)) \cong SL_2(\mathbb{Z}/N\mathbb{Z})/\{\pm I\}.$$

Let $y(E_j[N])$ denote the set of $y$-coordinates of nonzero $N$-torsion points of $E_j$. These are the functions

$$g_0^{\bar{v}}(\tau) = \frac{g_2(\tau)}{g_3(\tau)}^{3/2} \wp'_\tau\left(\frac{c_v\tau + d_v}{N}\right), \qquad v = (c_v, d_v).$$

Let $E_j[N] = x(E_j[N]) \cup y(E_j[N])$ and consider the field containments

$$\mathbb{C}(j) \subset \mathbb{C}(j, x(E_j[N])) \subset \mathbb{C}(j, E_j[N]) \subset \overline{\mathbb{C}(j)}$$

**Propositon 4.2.2.** *The field extension $\mathbb{C}(j, E_j[N])/\mathbb{C}(j)$ is Galois with Galois group* $\mathrm{Gal}(\mathbb{C}(j, E_j[N])/\mathbb{C}(j)) \cong SL_2(\mathbb{Z}/N\mathbb{Z})$.

*Proof.* Let $\sigma : \mathbb{C}(j, E_j[N]) \to \overline{\mathbb{C}(j)}$ be an embedding which fixes $\mathbb{C}(j)$ point wise. Since the extension $\mathbb{C}(j, x(E_j[N]))/\mathbb{C}(j)$ is Galois by Proposition **??**, $\sigma$ restricts to an element of $\mathrm{Gal}(\mathbb{C}(j, x(E_j[N]))/\mathbb{C}(j))$. Elements of the set $y(E_j[N])$ consists of square roots of elements of $\mathbb{C}(j, x(E_j[N]))$ which are permuted by $\sigma$ and so $\sigma$ also permutes the elements of $y(E_j[N])$. Hence $\sigma$ is an automorphism of $\mathbb{C}(j, E_j[N])$. Thus the extension $\mathbb{C}(j, E_j[N])/\mathbb{C}(j)$ is Galois.

Let $H = \mathrm{Gal}(\mathbb{C}(j, E_j[N])/\mathbb{C}(j))$. The ordered basis $(P_\tau, Q_\tau)$ of $E_j[N]$ over $\mathbb{Z}/N\mathbb{Z}$ gives an injective representation

$$\rho : H \to GL_2(\mathbb{Z}/N\mathbb{Z}), \qquad \left(\begin{smallmatrix} P_\tau^\sigma \\ Q_\tau^\sigma \end{smallmatrix}\right) = \rho(\sigma)\left(\begin{smallmatrix} P_\tau \\ Q_\tau \end{smallmatrix}\right).$$

Hence $H \cong \rho(H)$. Let $\sigma \in H$. By Proposition **??** and Corollary **??** we have $e_N(P_\tau, Q_\tau)^\sigma = e_N(P_\tau^\sigma, Q_\tau^\sigma) = e_N(P_\tau, Q_\tau)^{\det \rho(\sigma)}$. Since $e_N(P_\tau, Q_\tau) \in \mu_N$ it is fixed by $\sigma$ and so $e_N(P_\tau, Q_\tau) = e_N(P_\tau, Q_\tau)^{\det \rho(\sigma)}$. Since $e_N(P_\tau, Q_\tau)$ is a primitive $N$th root of unity, $\det \rho(\sigma) = 1$ inr $(\mathbb{Z}/N\mathbb{Z})^*$. Thus $\rho(H) \subset SL_2(\mathbb{Z}/N\mathbb{Z})$.

Let $K = \mathrm{Gal}(\mathbb{C}(j, E_j[N])/\mathbb{C}(j, x(E_j[N])))$ be the subgroup of $H$ fixing the $x$-coordinates of the elements of $E_j[N]$. Hence if $\sigma \in K$ then $P_\tau^\sigma = \pm P_\tau$ and $Q_\tau^\sigma = \pm Q_\tau$. Since $\rho(\sigma) \in SL_2(\mathbb{Z}/N\mathbb{Z})$, $\rho(\sigma) \in \{\pm I\}$. Now suppose $\sigma \in H$ and $\rho(\sigma) \in \{\pm I\}$. Then $P^\sigma = \pm P$ for all $P \in E_j[N]$ and so $\sigma \in K$. Thus $K = \rho^{-1}(\{\pm I\})$. This shows that $|K| \leqslant 2$. Since $\mathrm{Gal}(\mathbb{C}(j, x(E_j[N]))/\mathbb{C}(j)) \cong SL_2(\mathbb{Z}/N\mathbb{Z})/\{\pm I\}$ we have $|H| = |SL_2(\mathbb{Z}/N\mathbb{Z})/\{\pm I\}||K|$ and so $[SL_2(\mathbb{Z}/N\mathbb{Z}) : \rho(H)] \leqslant 2$. $[SL_2(\mathbb{Z}/N\mathbb{Z}) :$

$\rho(H)] = 2$ if and only if $|K| = 1$ which means $-I \notin \rho(H)$. If this is the case then $\{\pm I\}\rho(H) = SL_2(\mathbb{Z}/N\mathbb{Z})$ and so either $\left(\begin{smallmatrix} 0 & 1 \\ -1 & 0 \end{smallmatrix}\right)$ or $-\left(\begin{smallmatrix} 0 & 1 \\ -1 & 0 \end{smallmatrix}\right)$ is in $\rho(H)$. This implies that $\left(\pm\left(\begin{smallmatrix} 0 & 1 \\ -1 & 0 \end{smallmatrix}\right)\right)^2 = -I \in \rho(H)$, contradiction. Thus $\rho(H) = SL_2(\mathbb{Z}/N\mathbb{Z})$. □

## 4.3 Modular curves and function fields over $\mathbb{Q}$

In this section we examine the function fields of the previous section where the underlying field is changed to be $\mathbb{Q}$.

Recall the universal elliptic curve $E_j$ from the previous section. $E_j$ can be viewed as a curve over $\mathbb{Q}(j)$. The nonzero points of $E_j[N]$ over $\mathbb{C}$ lie in $\overline{\mathbb{Q}(j)}^2$ and so we have the containments $\mathbb{Q}(j) \subset \mathbb{Q}(j, E_j[N]) \subset \overline{\mathbb{Q}(j)}$. Now the extension $\mathbb{Q}(j, E_j[N])/\mathbb{Q}(j)$ is Galois. Consider the Galois group $H_Q = \mathrm{Gal}(\mathbb{Q}(j, \mu_N, E_j[N])/\mathbb{Q}(j))$ and the corresponding representation

$$\rho : H_Q \to GL_2(\mathbb{Z}/N\mathbb{Z}) \qquad \left(\begin{smallmatrix} P_\tau^\sigma \\ Q_\tau^\sigma \end{smallmatrix}\right) = \rho(\sigma)\left(\begin{smallmatrix} P_\tau \\ Q_\tau \end{smallmatrix}\right)$$

where $(P_\tau, Q_\tau)$ is an ordered basis of $E_j[N]$.

**Lemma 4.3.1.** *For any $\mu \in \mu_N$, $\sigma \in H_Q$ we have $\mu^\sigma = \mu^{\det\rho(\sigma)}$.*

*Proof.* Since $(P_\tau, Q_\tau)$ is an ordered basis $e_N(P_\tau, Q_\tau)$ is a primitive $N$th root of unity and so given $\mu \in \mu_N$ and $\sigma \in H_Q$ we have

$$\begin{aligned} \mu^\sigma &= ((e_N(P_\tau, Q_\tau))^a)^\sigma = ((e_N(P_\tau, Q_\tau))^\sigma)^a = (e_N(P_\tau^\sigma, Q_\tau^\sigma))^a \\ &= e_N(P_\tau, Q_\tau)^{a\det\rho(\sigma)} = \mu^{\det\rho(\sigma)}. \end{aligned}$$

□

Suppose $\sigma \in H_Q$ fixes $E_j[N]$ that is $\sigma \in \ker\rho$. Hence $\sigma \in \ker(\det\rho)$. By Lemma **??**, $\sigma$ acts on $\mu_N$ as identity. Thus $\mu_N \subset \mathbb{Q}(j, E_j[N])$ and so $H_Q$ is the Galois group of the extension $\mathbb{Q}(j, E_j[N])/\mathbb{Q}(j)$. Hence we have the following tower of field extensions and Galois groups

$$\begin{tikzcd}
\mathbb{Q}(j, E_j[N]) \arrow[d, dash, "H_{\mathbb{Q}(\mu_N)}"] \\
\mathbb{Q}(j, \mu_N) \arrow[d, dash, "(\mathbb{Z}/N\mathbb{Z})^*"] \\
\mathbb{Q}(j)
\end{tikzcd}$$

As before $\rho$ is injective and by Lemma **??** it restricts to

$$\rho : H_{\mathbb{Q}(\mu_N)} \to SL_2(\mathbb{Z}/N\mathbb{Z}).$$

Since $\mathrm{Gal}(\mathbb{C}(j, E_j[N])/\mathbb{C}(j)) = SL_2(\mathbb{Z}/N\mathbb{Z})$, by Galois theory $SL_2(\mathbb{Z}/N\mathbb{Z})$ injects into $H_{\mathbb{Q}(\mu_N)}$ under the restriction map. This shows that the map $\rho$ is an isomorphism

$$\rho : H_{\mathbb{Q}(\mu_N)} \xrightarrow{\sim} SL_2(\mathbb{Z}/N\mathbb{Z}).$$

Therefore $|H_{\mathbb{Q}}| = |SL_2(\mathbb{Z}/N\mathbb{Z})||(\mathbb{Z}/N\mathbb{Z})^*| = |GL_2(\mathbb{Z}/N\mathbb{Z})|$ which proves that

$$\rho : H_{\mathbb{Q}} \xrightarrow{\sim} GL_2(\mathbb{Z}/N\mathbb{Z}).$$

Now let $\mathbf{K}$ be an intermediate field of the extension $\mathbb{Q}(j, E_j[N])/\mathbb{Q}(j)$ and $K = \mathrm{Gal}(\mathbb{Q}(j, E_j[N])/\mathbf{K})$.

**Lemma 4.3.2.** *Let* $\mathbf{K}$ *be as above. Then*

$$\mathbf{K} \cap \overline{\mathbb{Q}} = \mathbb{Q} \Leftrightarrow \mathbf{K} \cap \mathbb{Q}(\mu_N) = \mathbb{Q} \Leftrightarrow \det \rho : K \to (\mathbb{Z}/N\mathbb{Z})^* \textit{ surjects}$$

*Proof.* The first implication is clear. For the second implication suppose $\mathbf{K} \cap \mathbb{Q}(\mu_N) = \mathbb{Q}$. Let $a \in (\mathbb{Z}/N\mathbb{Z})^*$ and $\mu \in \mu_N$ be a primitive root of unity. Then $\mu \notin \mathbf{K}$ and so there exists $\sigma \in K$ such that $\sigma : \mu \mapsto \mu^a$. By Lemma **??**, $\det \rho(\sigma) = a$. Coversely, assume that $\mathbf{K} \cap \mathbb{Q}(\mu_N) \neq \mathbb{Q}$. Then there exists an $N$th root of unity $\mu \in K - \mathbb{Q}$. Since $\det \rho$ subjects there exists $\sigma \in K$ such that $\det \rho \neq 1$. Since $\rho$ is injective $\mu^\sigma \neq \mu$ and so $\mu \notin \mathbf{K}$, contradiction. □

Since any such intermediate field $\mathbf{K}$ is a finite extension of $\mathbb{Q}(j)$, we have a criterion for which intermediate fields $\mathbf{K}$ are function fields of an algebraic curve over $\mathbb{Q}$.

**Theorem 4.3.1.** *Let $\mathbf{K}$ be an intermediate field as above with the corresponding Galois group $K$. Then $\mathbf{K}$ is a function field of an algebraic curve over $\mathbb{Q}$ if and only if* $\det \rho$ *is surjective.*

Consider the following intermediate fields of the extension $\mathbb{Q}(j, E_j[N])/\mathbb{Q}(j)$

$$\mathbf{K}_0 = \mathbb{Q}(j, f_0), \qquad \mathbf{K}_0' = \mathbb{Q}(j, j_N), \qquad \mathbf{K}_1 = \mathbb{Q}(j, f_1)$$

and let $K_0, K_0'$ and $K_1$ be the corresponding subgroups of $H_{\mathbb{Q}}$. Then

$$\rho(K_0) = \rho(K_0') = \left\{ \left( \begin{smallmatrix} a & b \\ 0 & d \end{smallmatrix} \right) \in GL_2(\mathbb{Z}/N\mathbb{Z}) \right\}$$

and

$$\rho(K_1) = \left\{ \pm \left( \begin{smallmatrix} a & b \\ 0 & 1 \end{smallmatrix} \right) \in GL_2(\mathbb{Z}/N\mathbb{Z}) \right\}.$$

This implies that $\mathbf{K}_0 = \mathbf{K}_0'$ and $\det \rho : K_j \to (\mathbb{Z}/N\mathbb{Z})^*$ is surjective for $j = 0, 1$. Thus by Theorem **??**, $\mathbf{K}_0$ and $\mathbf{K}_1$ are function fields of nonsingular projective algebraic curves over $\mathbb{Q}$. Denote these curves $X_0(N)_{\text{alg}}$ and $X_1(N)_{\text{alg}}$. We need the following theorem from algebraic geometry to relate the algebraic curves over $\mathbb{C}$ and over $\mathbb{Q}$

**Theorem 4.3.2.** *Let $C$ be a nonsingular projective algebraic curve over a field $k$ defined by the polynomials $\varphi_1, \ldots, \varphi_m \in k[x_1, \ldots, x_n]$, and let the function field of $C$ be $k(C) = k(t)[u]/(p(u))$. Let $K$ be a field containing $k$. Then the polynomials*

*$\varphi_i \in K[x_1, \ldots, x_n]$ define a nonsingular algebraic curve $C'$ over $K$ and its function field is $K(C') = K(t)[u]/(p(u))$.*

Now let $k = \mathbb{Q}$ and $C = X_1(N)_{\mathrm{alg}}$, and $p_1 \in \mathbb{Q}(j)[x]$ be the minimal polynomial of $f_{0,1}$ over $\mathbb{Q}(j)$. Thus $\mathbb{Q}(C) = \mathbb{Q}(j, f_{0,1}) = \mathbb{Q}(j)[x]/(p_1(x))$. Let $K = \mathbb{C}$. Then Theorem **??** says that there exists a curve $C' = X_1(N)_{\mathrm{alg},\mathbb{C}}$ over $\mathbb{C}$ with function field $\mathbb{C}(C') = \mathbb{C}(j)[x]/(p_1(x))$ and the minimal polynomials of $f_{0,1}$ over $\mathbb{C}(j)$ and over $\mathbb{Q}(j)$ are the same. Therefore the function field $\mathbb{C}(j, f_{0,1})$ of the Riemann surface $X_1(N)$ is

$$\mathbb{C}(X_1(N)) = \mathbb{C}(j, f_{0,1}) = \mathbb{C}(j)[x]/(p_1).$$

Since the two function fields are the same $X_1(N) = X_1(N)_{\mathrm{alg}}$ up to isomorphism over $\mathbb{C}$. For $X_0(N)$ the argument is similar with $f_{0,1}$ is replaced by $f_0$.

## 4.4 Hecke operators algebraically

In Section **??** we have seen the action on $T_p$ on the complex analytic moduli space $S_1(N)$

$$T_p[E, Q] = \sum_C [E/C, Q + C],$$

where the sum is over all order $p$ subgroups $C$ of $E$ with $C \cap \langle Q \rangle = \{0\}$. The complex elliptic curve $E$ in the definition of $S_1(N)$ was a complex torus. In this section we describe the action of $T_p$ when $E$ is an algebraic elliptic curve over $\mathbb{Q}$.

An enhanced complex algebraic elliptic curve for $\Gamma_1(N)$ is an ordered pair $(E, Q)$ where $E$ is an algebraic elliptic curve over $\mathbb{C}$ and $Q \in E$ is a point of order $N$. Two such pairs $(E, Q)$ and $(E', Q')$ are equivalent if some isomorphism $E \xrightarrow{\sim} E'$ over $\mathbb{C}$ takes $Q$ to $Q'$. The complex algebraic moduli space for $\Gamma_1(N)$ is

$$S_1(N)_{\mathrm{alg},\mathbb{C}} = \{enhanced\ complex\ algebraic\ elliptic\ curves\ for\ \Gamma_1(N)\}/\sim.$$

The complex analytic moduli space $S_1(N)$ defined in Section **??** and $S_1(N)_{\mathrm{alg},\mathbb{C}}$ are in bijective correspondence where the correspondence is given by

$$[\mathbb{C}/\Lambda_\tau, 1/N + \Lambda_\tau] \mapsto [E_\tau, (\wp_\tau(1/N), \wp'_\tau(1/N))].$$

Thus $T_p$ can be defined on $S_1(N)_{\mathrm{alg},\mathbb{C}}$ by

$$T_p[E, Q] = \sum_C [E/C, Q + C].$$

where now $E/C$ is viewed as an algebraic object namely the image of the quotient isogeny.

An enhanced algebraic elliptic curve for $\Gamma_1(N)$ is an ordered pair $(E, Q)$ where $E$ is an algebraic elliptic curve over $\overline{\mathbb{Q}}$ and $Q \in E$ is a point of order $N$. Two such pairs $(E, Q)$ and $(E', Q')$ are equivalent if some isomorphism $E \xrightarrow{\sim} E'$ over $\overline{\mathbb{Q}}$ takes $Q$ to $Q'$. The algebraic moduli space for $\Gamma_1(N)$ is

$$S_1(N)_{\mathrm{alg}} = \{enhanced\ algebraic\ elliptic\ curves\ for\ \Gamma_1(N)\}/\sim .$$

The intersection of an equivalence class in $S_1(N)_{\mathrm{alg},\mathbb{C}}$ with $S_1(N)_{\mathrm{alg}}$ is an equivalence class in $S_1(N)_{\mathrm{alg}}$. Thus $S_1(N)_{\mathrm{alg}}$ can be viewed as a subset of $S_1(N)_{\mathrm{alg},\mathbb{C}}$. If $E$ is an elliptic curve over $\overline{\mathbb{Q}}$ then its order $p$ subgroups $C \subset E$ are the same as such subgroups of the complex curve $E_{\mathbb{C}}$. Hence the definition of $T_p$ on $\mathrm{Div}(S_1(N)_{\mathrm{alg},\mathbb{C}})$ restricts to $\mathrm{Div}(S_1(N)_{\mathrm{alg}})$. This is the desired version of $T_p$ over $\mathbb{Q}$.

In Section **??** we have seen the action of $T_p$ on $\mathrm{Div}(X_1(N))$. Now we give an algebraic description of this action. For this purpose, identify $X_1(N)$ with the complex points of $X_1(N)_{\mathrm{alg}}$, $X_1(N)_{\mathrm{alg},\mathbb{C}}$. Now we can view the action of $T_p$ on $X_1(N)_{\mathrm{alg},\mathbb{C}}$,

$$T_p : \mathrm{Div}(X_1(N)_{\mathrm{alg},\mathbb{C}}) \to \mathrm{Div}(X_1(N)_{\mathrm{alg},\mathbb{C}})$$

Let us see that this action is defined over $\mathbb{Q}$. First consider the diamond operator $\langle d \rangle$. To see that $\langle d \rangle$ is defined over $\mathbb{Q}$ we need to check that $\langle d \rangle^*$ takes $\mathbb{Q}(X_1(N)_{\mathrm{alg}})$ to

$\mathbb{Q}(X_1(N)_{\text{alg}})$. $\mathbb{Q}(X_1(N)_{\text{alg}}) = \mathbb{Q}(j, f_{0,1})$. Since $\langle d\rangle(\Gamma_1(N)\tau) = \Gamma_1(N)\gamma(\tau)$ where $\gamma = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \Gamma_0(N)$, it suffices to check that $j(\gamma(\tau)), f_{0,1}(\gamma(\tau)) \in \mathbb{Q}(X_1(N)_{\text{alg}})$. $j(\gamma(\tau)) = j(\tau) \in \mathbb{Q}(X_1(N)_{\text{alg}})$. For $f_{0,1}(\gamma(\tau))$ compute that

$$f_{0,1}(\gamma(\tau)) = f_0^{\pm\overline{(0,1)}}(\gamma(\tau)) = f_0^{\pm\overline{(0,1)\gamma}}(\tau) = f_0^{\pm\overline{(0,d)}}(\tau).$$

Thus $f_{0,1}(\gamma(\tau))$ is the $x$-coordinate of $\pm[d]Q_\tau \in E_{j(\tau)}$. Hence $f_{0,1}(\gamma(\tau)) \in \mathbb{Q}(j(\tau), E_{j(\tau)}[N])$. Now $\mathbb{Q}(X_1(N)_{\text{alg}})$ is the fixed field of the Galois group $K_1$ and

$$\rho(K_1) = \left\{\pm\left(\begin{smallmatrix} a & b \\ 0 & 1 \end{smallmatrix}\right) \in GL_2(\mathbb{Z}/N\mathbb{Z})\right\}.$$

This group fixes $\pm[d]Q_\tau$ and so it also fixes $f_{0,1}(\gamma(\tau))$ which implies that $f_{0,1}(\gamma(\tau)) \in \mathbb{Q}(X_1(N)_{\text{alg}})$. Thus $\langle d\rangle$ is defined over $\mathbb{Q}$ and therefore $\langle d\rangle$ restricts to

$$\langle d\rangle : \text{Div}(X_1(N)_{\text{alg}}) \to \text{Div}(X_1(N)_{\text{alg}}).$$

Now consider the description of $T_p$ on the modular curve $X_1(N)$ as a double coset operator: Let $\alpha = \left(\begin{smallmatrix} 1 & 0 \\ 0 & p \end{smallmatrix}\right)$, and $\Gamma_3 = \Gamma_1^0(N,p) = \Gamma_1(N) \cap \Gamma^0(p)$, and $X_1^0(N,p) = X(\Gamma_1^0(N,p))$. Define $\Gamma_{1,0}(N,p) = \Gamma_1(N) \cap \Gamma_0(Np)$ and $X_{1,0}(N,p) = X(\Gamma_{1,0}(N,p))$. Then $\Gamma_{1,0}(N,p) = \alpha\Gamma_1^0(N,p)\alpha^{-1}$. Thus $T_p$ is described as the pullback of the map

$$X_{1,0}(N,p) \to X_1(N), \qquad \Gamma_{1,0}(N,p)\tau \mapsto \Gamma_1(N)p\tau \tag{4.1}$$

followed by the pushforward of the map

$$X_{1,0}(N,p) \to X_1(N), \qquad \Gamma_{1,0}(N,p)\tau \mapsto \Gamma_1(N)\tau. \tag{4.2}$$

Let us see that these maps are defined over $\mathbb{Q}$. Note that $\Gamma_1(Np) \subset \Gamma_{1,0}(N,p) \subset$

$\Gamma_0(Np)$. Thus we have the following tower of field extensions

$$\begin{tikzcd}
\mathbb{C}(X_1(Np)) \arrow[d, dash] & \mathbb{Q}(X_1(Np)) \arrow[d, dash] \\
\mathbb{C}(X_{1,0}(N,p)) \arrow[d, dash] & \mathbf{K} \arrow[d, dash] \\
\mathbb{C}(X_0(Np)) & \mathbb{Q}(X_0(Np))
\end{tikzcd}$$

where $\mathbf{K}$ corresponds to the field $\mathbb{C}(X_{1,0}(N,p))$ and it is function field of a curve over $\mathbb{Q}$. Denote this curve by $X_{1,0}(N,p)_{\mathrm{alg}}$ so that $\mathbb{Q}(X_{1,0}(N,p)_{\mathrm{alg}}) = \mathbf{K}$. The Galois groups on the tower are

$$\mathrm{Gal}(\mathbb{C}(X_1(Np))/\mathbb{C}(X_0(Np))) = \mathrm{Gal}(\mathbb{Q}(X_1(Np))/\mathbb{Q}(X_0(Np))) \cong (\mathbb{Z}/Np\mathbb{Z})^*/\{\pm 1\}$$

Since $X_1(Np)_{\mathrm{lag},\mathbb{C}}$ is isomorphic over $\mathbb{C}$ to $X_1(Np)$ and similarly for $X_0(Np)$ we have the following diagram

$$\begin{tikzcd}
\mathbb{C}(X_1(Np)) \arrow[d, dash] & \mathbb{Q}(X_1(Np)) \arrow[d, dash] \\
\mathbb{C}(X_{1,0}(N,p)_{\mathrm{alg},\mathbb{C}}) \arrow[d, dash] & \mathbb{Q}(X_{1,0}(N,p)_{\mathrm{alg}}) \arrow[d, dash] \\
\mathbb{C}(X_0(Np)) & \mathbb{Q}(X_0(Np))
\end{tikzcd}$$

Thus we have the following injections

$$\mathrm{Gal}(\mathbb{C}(X_1(Np))/\mathbb{C}(X_{1,0}(N,p)_{\mathrm{alg},\mathbb{C}})) \hookrightarrow \mathrm{Gal}(\mathbb{Q}(X_1(Np))/\mathbb{Q}(X_{1,0}(N,p)_{\mathrm{alg}}))$$

and

$$\mathrm{Gal}(\mathbb{C}(X_{1,0}(N,p)_{\mathrm{alg},\mathbb{C}})/\mathbb{C}(X_0(Np))) \hookrightarrow \mathrm{Gal}(\mathbb{Q}(X_{1,0}(N,p)_{\mathrm{alg}})/\mathbb{Q}(X_0(Np)))$$

This shows that the order of $\mathrm{Gal}(\mathbb{C}(X_1(Np))/\mathbb{C}(X_{1,0}(N,p)))$ is the same as the order of $\mathrm{Gal}(\mathbb{C}(X_1(Np))/\mathbb{C}(X_{1,0}(N,p)_{\mathrm{alg},\mathbb{C}}))$. Since these are subgroups of the cyclic group they must be the same and so $\mathbb{C}(X_{1,0}(N,p)_{\mathrm{alg},\mathbb{C}}) = \mathbb{C}(X_{1,0}(N,p))$ which implies that $X_{1,0}(N,p)_{\mathrm{alg},\mathbb{C}} = X_{1,0}(N,p)$ up to isomorphism over $\mathbb{C}$. Thus $X_{1,0}(N,p)$ is defined over $\mathbb{Q}$.

The maps (**??**) and (**??**) correspond to the following function field injections

$$\mathbb{C}(X_1(N)) \to \mathbb{C}(X_{1,0}(N,p)), \qquad f(\tau) \mapsto f(p\tau)$$

and

$$\mathbb{C}(X_1(N)) \to \mathbb{C}(X_{1,0}(N,p)), \qquad f(\tau) \mapsto f(\tau).$$

Since $\mathbb{C}(X_1(N)) = \mathbb{C}(j, f_{0,1})$ the image of the nontrivial map is $\mathbb{C}(j(p\tau), f_{0,1}(p\tau))$. Since $j(p\tau), f_{0,1}(p\tau) \in \mathbb{Q}(X_{1,0}(N,p)_{\mathrm{alg}})$, these injections restrict to function fields over $\mathbb{Q}$. Thus $T_p$ is defined over $\mathbb{Q}$ and so $T_p$ restricts to

$$T_p : \mathrm{Div}(X_1(N)_{\mathrm{alg}}) \to \mathrm{Div}(X_1(N)_{\mathrm{alg}}).$$

From Section **??** we have the following map

$$\psi_1 : S_1(N) \to X_1(N), \qquad [\mathbb{C}/\Lambda_\tau, 1/N + \Lambda_\tau] \mapsto \Gamma_1(N)\tau$$

and this map extends to divisor groups. We need to make $\psi_1$ algebraic. For this purpose consider the following commutative diagram,

$$\begin{tikzcd}
S_1(N) \arrow[r] \arrow[d, "\psi_1"] & S_1(1) \arrow[d] \\
X_1(N) \arrow[r] & X_1(1)
\end{tikzcd}
\qquad
\begin{tikzcd}
{[\mathbb{C}/\Lambda_\tau, 1/N + \Lambda_\tau]} \arrow[r, mapsto] \arrow[d, mapsto] & {[\mathbb{C}/\Lambda_\tau]} \arrow[d, mapsto] \\
\Gamma_1(N)\tau \arrow[r, mapsto] & \mathrm{SL}_2(\mathbb{Z})\tau
\end{tikzcd}$$

Note that we have identified the complex analytic moduli space $S_1(N)$ with the complex algebraic moduli space $S_1(N)_{\mathrm{alg},\mathbb{C}}$ and the Riemann surface $X_1(N)$ with the complex points $X_1(N)_{\mathrm{alg},\mathbb{C}}$ of the algebraic modular curve. For $N = 1$, the complex algebraic moduli space is the set of equivalence classes of complex algebraic elliptic curves and the complex points of the algebraic modular curve are the complex projective line $\mathbb{P}^1(\mathbb{C})$. Therefore the above diagram becomes

$$\begin{tikzcd}
S_1(N)_{\mathrm{alg},\mathbb{C}} \arrow[r] \arrow[d, "\psi_{1,\mathrm{alg}}"] & S_1(1)_{\mathrm{alg},\mathbb{C}} \arrow[d] & {[E,Q]} \arrow[r, mapsto] \arrow[d, mapsto] & {[E]} \arrow[d, mapsto] \\
X_1(N)_{\mathrm{alg},\mathbb{C}} \arrow[r] & X_1(1)_{\mathrm{alg},\mathbb{C}} & P \arrow[r, mapsto] & j(\tau)
\end{tikzcd}$$

Now an element $[E,Q]$ of $S_1(N)_{\mathrm{alg},\mathbb{C}}$ describes an element of the algebraic moduli space $S_1(N)_{\mathrm{alg}}$ if and only if $j(E) \in \overline{\mathbb{Q}}$. Thus mapping down and then across takes $S_1(N)_{\mathrm{alg}}$ to $\mathbb{P}^1(\overline{\mathbb{Q}})$. This shows that $P \in X_1(N)_{\mathrm{alg}}$. Therefore the left side of the diagram restricts to

$$\psi_{1,\mathrm{alg}} : S_1(N)_{\mathrm{alg}} \to X_1(N)_{\mathrm{alg}}.$$

Putting all the things together so far we get the following commutative diagram which is the algebraic version of the diagram given in (**??**),

$$\begin{tikzcd}
\mathrm{Div}(S_1(N)_{\mathrm{alg}}) \arrow[r, "T_p"] \arrow[d, "\psi_{1,\mathrm{alg}}"] & \mathrm{Div}(S_1(N)_{\mathrm{alg}}) \arrow[d, "\psi_{1,\mathrm{alg}}"] \\
\mathrm{Div}(X_1(N)_{\mathrm{alg}}) \arrow[r, "T_p"] & \mathrm{Div}(X_1(N)_{\mathrm{alg}})
\end{tikzcd}$$

and so we have the following commutative diagram

$$\begin{tikzcd}
\mathrm{Div}^0(S_1(N)_{\mathrm{alg}}) \arrow[r, "T_p"] \arrow[d, "\psi_{1,\mathrm{alg}}"] & \mathrm{Div}^0(S_1(N)_{\mathrm{alg}}) \arrow[d, "\psi_{1,\mathrm{alg}}"] \\
\mathrm{Pic}^0(X_1(N)_{\mathrm{alg}}) \arrow[r, "T_p"] & \mathrm{Pic}^0(X_1(N)_{\mathrm{alg}})
\end{tikzcd} \tag{4.3}$$

For the Hecke operator $\langle d \rangle$ we have the following similar diagram,

$$\begin{tikzcd}
\mathrm{Div}^0(S_1(N)_{\mathrm{alg}}) \arrow[r, "\langle d \rangle"] \arrow[d, "\psi_{1,\mathrm{alg}}"] & \mathrm{Div}^0(S_1(N)_{\mathrm{alg}}) \arrow[d, "\psi_{1,\mathrm{alg}}"] \\
\mathrm{Pic}^0(X_1(N)_{\mathrm{alg}}) \arrow[r, "\langle d \rangle_*"] & \mathrm{Pic}^0(X_1(N)_{\mathrm{alg}})
\end{tikzcd} \tag{4.4}$$

## 4.5 Eichler-Shimura Relation

Let $X_1(N)$ denotes the nonsingular algebraic curve over $\mathbb{Q}$ with the function field $\mathbb{Q}(X_1(N)) = \mathbb{Q}(j, f_{0,1})$ and $S_1(N)$ denotes the algebraic moduli space for $\Gamma_1(N)$. We also identify the Jacobians and Picard groups of a compact Riemann surface $X$ and denote both of them by $\mathrm{Pic}^0(X)$.

Let $p$ be a prime not dividing $N$. Let $\mathfrak{p}$ be a maximal ideal of $\overline{\mathbb{Q}}$ lying over $p$. Let $\overline{\mathbb{Z}}_{(\mathfrak{p})}$ denote the localization of $\overline{\mathbb{Z}}$ at $\mathfrak{p}$. Since $\overline{\mathbb{Z}}/\mathfrak{p} \xrightarrow{\sim} \overline{\mathbb{Z}}_{(\mathfrak{p})}/\mathfrak{p}\overline{\mathbb{Z}}_{(\mathfrak{p})}$ and $\overline{\mathbb{Z}}/\mathfrak{p}$ is an algebraic closure of $\mathbb{F}_p$, we have a reduction map $\tilde{}: \overline{\mathbb{Z}}_{(\mathfrak{p})} \to \overline{\mathbb{F}}_p$.

An elliptic curve $E$ over $\overline{\mathbb{Q}}$ has good reduction at $\mathfrak{p}$ if and only if $j(E) \in \overline{\mathbb{Z}}_{(\mathfrak{p})}$ and so $j(E)$ reduces to $\widetilde{j(E)} \in \overline{\mathbb{F}}_p$. Restrict the moduli space $S_1(N)$ over $\mathbb{Q}$ to

$$S_1(N)'_{\mathrm{gd}} = \{[E,Q] \in S_1(N) : E \text{ has good reduction at } \mathfrak{p},\ \widetilde{j(E)} \notin \{0, 1728\}\}.$$

Let $\tilde{S}_1(N)$ denote the moduli space over $\overline{\mathbb{F}}_p$ and restrict it to

$$\tilde{S}_1(N)' = \{[E,Q] \in \tilde{S}_1(N) : j(E) \notin \{0, 1728\}\}.$$

Now we have the following reduction map

$$S_1(N)'_{\mathrm{gd}} \to \tilde{S}_1(N)', \qquad [E_j, Q] \mapsto [\tilde{E}_j, \tilde{Q}]$$

and it is surjective. Indeed, any elliptic curve over $\overline{\mathbb{F}}_p$ lifts to an elliptic curve over $\overline{\mathbb{Z}}$. Since reduction map gives an isomorphism between $N$-torsion subgroups of an elliptic curve with good reduction at $\mathfrak{p}$ and its reduction, $N$-torsion point has a lift. Thus the above map is surjective.

Now we define the reduction $\tilde{X}_1(N)$ of $X_1(N)$ at $p$. Remember the universal elliptic curve from Section **??**. Viewing this as an elliptic curve over $\mathbb{F}_p(j)$ and using an admissible change of variable we get

$$\tilde{E}_j : y^2 + xy = x^3 - \left(\frac{36}{j - 1728}\right) x - \left(\frac{1}{j - 1728}\right).$$

Let $Q$ be a point of $\tilde{E}_j$ of order $N$ and $\varphi_1 \in \mathbb{F}_p(j)[x]$ be the minimal polynomial of its $x$-coordinate $x(Q)$. Let $K_1(N) = \mathbb{F}_p(j)[x]/(\varphi_1(x))$. Then $K_1(N) \cap \overline{\mathbb{F}}_p = \mathbb{F}_p$ and so $K_1(N)$ is a function field over $\mathbb{F}_p$. The following theorem of Igusa says that reducing the moduli space is compatible with reducing the modular curve.

**Theorem 4.5.1.** *The modular curve $X_1(N)$ has good reduction at p and there is an isomorphism of function fields $\mathbb{F}_p(\tilde{X}_1(N)) \xrightarrow{\sim} K_1(N)$. Also the following diagram commutes,*

$$\begin{tikzcd}
S_1(N)'_{\mathrm{gd}} \arrow[r, "\psi_1"] \arrow[d] & X_1(N) \arrow[d] \\
\tilde{S}_1(N)' \arrow[r, "\tilde{\psi}_1"] & \tilde{X}_1(N)
\end{tikzcd}$$

By the above diagram we have

$$\begin{tikzcd}
\mathrm{Div}^0(S_1(N)'_{\mathrm{gd}}) \arrow[r] \arrow[d] & \mathrm{Pic}^0(X_1(N)) \arrow[d] \\
\mathrm{Div}^0(\tilde{S}_1(N)') \arrow[r] & \mathrm{Pic}^0(\tilde{X}_1(N))
\end{tikzcd}$$

Now we give the description of the Hecke operator $T_p$ on the Picard groups of the reduced modular curves,

$$\tilde{T}_p : \mathrm{Pic}^0(\tilde{X}_1(N)) \to \mathrm{Pic}^0(\tilde{X}_1(N)).$$

For the Hecke operator $\langle d \rangle$ it is easy since the pushforward of a morphism and pushforward of its reduction are compatible. Thus we have the following commutative diagram,

$$\begin{tikzcd}
\mathrm{Pic}^0(X_1(N)) \arrow[r, "\langle d \rangle_*"] \arrow[d] & \mathrm{Pic}^0(X_1(N)) \arrow[d] \\
\mathrm{Pic}^0(\tilde{X}_1(N)) \arrow[r, "\widetilde{\langle d \rangle}_*"] & \mathrm{Pic}^0(\tilde{X}_1(N))
\end{tikzcd}$$

We assert without proof that such a commutative diagram exists for $T_p$,

$$\begin{tikzcd}
\mathrm{Pic}^0(X_1(N)) \arrow[r, "T_p"] \arrow[d] & \mathrm{Pic}^0(X_1(N)) \arrow[d] \\
\mathrm{Pic}^0(\tilde{X}_1(N)) \arrow[r, "\tilde{T}_p"] & \mathrm{Pic}^0(\tilde{X}_1(N))
\end{tikzcd}$$

The action of $T_p$ on the moduli space $S_1(N)$ was given by

$$T_p[E, Q] = \sum_C [E/C, Q + C].$$

Let $\mathfrak{p}$ be a maximal ideal of $\overline{\mathbb{Z}}$ lying over $p$. If the curve $E$ has ordinary reduction at $\mathfrak{p}$, then all the curves $E/C$ on the right side also have ordinary reduction at $\mathfrak{p}$. Let $E$ be an elliptic curve over $\overline{\mathbb{Q}}$ with ordinary reduction at $\mathfrak{p}$ and $Q \in E$ be a point of order $N$. Let $C_0$ be the kernel of the reduction map $E[p] \to \tilde{E}[p]$. Then $C_0$ is an order p subgroup of $E$ since the reduction map subjects and $E$ has ordinary reduction.

**Lemma 4.5.1.** *For any order $p$ subgroup $C$ of $E$,*

$$[\widetilde{E/C}, \widetilde{Q+C}] = \begin{cases} [\tilde{E}^{\sigma_p}, \tilde{Q}^{\sigma_p}], & \text{if } C = C_0, \\ [\tilde{E}^{\sigma_p^{-1}}, [p]\tilde{Q}^{\sigma_p^{-1}}], & \text{if } C \neq C_0. \end{cases}$$

*Proof.* Suppose $C = C_0$. Let $E' = E/C$ and $Q' = Q + C = \varphi(Q)$ where $\varphi : E \to E'$ is the quotient isogeny. Let $\psi : E' \to E$ be the dual isogeny of $\varphi$. We have a commutative diagram

$$\begin{tikzcd}
E'[p] \arrow[r, "\psi"] \arrow[d] & E[p] \arrow[d] \\
\widetilde{E'}[p] \arrow[r, "\tilde{\psi}"] & \widetilde{E}[p]
\end{tikzcd}$$

Since $E$ has ordinary reduction at $\mathfrak{p}$, it is isogenous image $E'$ also has ordinary reduction at $\mathfrak{p}$ and so $|\widetilde{E'}[p]| = p$. The image $\psi(E'[p])$ has order $p$ since $|\ker(\psi)| =$

$\deg(\psi) = p$ and it is a subgroup of $C$ since $\varphi(\psi(E'[p])) = [p]E'[p] = \{0\}$. Thus $C_0 = C = \psi(E'[p])$. Since the map $E'[p] \to \widetilde{E'}[p]$ surjects the map at the bottom is the zero map, i.e. $\widetilde{E'}[p] \subset \ker \tilde{\psi}$. Conversely, since $\tilde{\varphi} \circ \tilde{\psi} = [p]$, we have $\ker(\tilde{\psi}) \subset \widetilde{E'}[p]$. Thus $\ker(\tilde{\psi}) = \widetilde{E'}[p]$.

Since reduction at $\mathfrak{p}$ preserves the degrees, by the relation $[p] = \psi \circ \varphi$, $\deg([p]) = p^2$, $\deg(\tilde{\varphi}) = p$ and $\deg(\tilde{\psi}) = p$. Since $\ker([p]) = \widetilde{E'}[p] = \ker(\tilde{\psi})$ we have

$$\deg_{\text{sep}}([p]) = p, \qquad \deg_{\text{ins}}([p]) = p$$

and

$$\deg_{\text{sep}}(\tilde{\psi}) = p, \qquad \deg_{\text{ins}}(\tilde{\psi}) = 1.$$

Thus

$$\deg_{\text{sep}}(\tilde{\varphi}) = 1, \qquad \deg_{\text{ins}}(\tilde{\varphi}) = p.$$

This shows that $\tilde{\varphi}$ is of the form $\tilde{\varphi} = i \circ \sigma_p$ where $i : \tilde{E}^{\sigma_p} \to \widetilde{E'}$ is an isomorphism taking $\tilde{Q}^{\sigma_p}$ to $\widetilde{Q'}$. Thus

$$[\widetilde{E'}, \widetilde{Q'}] = [\tilde{E}^{\sigma_p}, \tilde{Q}^{\sigma_p}].$$

Now suppose $C \neq C_0$. Let $C' = \ker(\psi)$ and $C_0'$ be the kernel of the reduction map $E'[p] \to \widetilde{E'}[p]$ and so $C_0'$ is an order $p$ subgroup of $E'[p]$. Consider the following commutative diagram,

$$\begin{tikzcd}
E[p] \arrow[r, "\varphi"] \arrow[d] & E'[p] \arrow[d] \\
\tilde{E}[p] \arrow[r, "\tilde{\varphi}"] & \widetilde{E'}[p]
\end{tikzcd}$$

The subgroup $\varphi(C_0)$ of $E'[p]$ is an order $p$ subgroup since $C_0 \neq C = \ker(\varphi)$. and $\varphi(C_0)$ is a subgroup of $C' = \ker(\psi)$. Since both have order $p$, they must be equal. Also $\varphi(C_0)$ is a subgroup of $C_0'$ and so $\varphi(C_0) = C_0'$. Thus $C' = c_0'$ and by the first part of this proof we have $\tilde{\psi} = i \circ \sigma_p$ where $i : \widetilde{E'}^{\sigma_p} \to \tilde{E}$ is an isomorphism taking

$\widetilde{Q'}^{\sigma_p}$ to $[p]\tilde{Q}$. Apply $\sigma_p^{-1}$ to $i$ gives an isomorphism $i^{\sigma_p^{-1}} : \widetilde{E'} \to \tilde{E}^{\sigma_p^{-1}}$ taking $\widetilde{Q'}$ to $[p]\tilde{Q}^{\sigma_p^{-1}}$. Thus

$$[\widetilde{E'}, \widetilde{Q'}] = [\tilde{E}^{\sigma_p^{-1}}, [p]\tilde{Q}^{\sigma_p^{-1}}].$$

□

Similarly, if $E$ is an elliptic curve over $\overline{\mathbb{Q}}$ with supersingular reduction at $\mathfrak{p}$ and $Q$ is an element of order $N$, then for any order $p$ subgroup of $E$,

$$[\widetilde{E/C}, \widetilde{Q+C}] = [\tilde{E}^{\sigma_p}, \tilde{Q}^{\sigma_p}] = [\tilde{E}^{\sigma_p^{-1}}, [p]\tilde{Q}^{\sigma_p^{-1}}].$$

Let $d$ be an integer prime to $N$ and define the moduli space diamond operator in characteristic $p$,

$$\widetilde{\langle d \rangle} : \tilde{S}_1(N) \to \tilde{S}_1(N), \qquad [E, Q] \mapsto [E, [d]Q].$$

Since there are $p+1$ order $p$ subgroups of $E$ one of which is $C_0$, by Lemma **??** we have

$$\sum_C [\widetilde{E/C}, \widetilde{Q+C}] = (\sigma_p + p\widetilde{\langle p \rangle}\sigma_p^{-1})[\tilde{E}, \tilde{Q}].$$

This also holds for curves with supersingular reduction at $\mathfrak{p}$ and therefore it holds for all curves with good reduction at $\mathfrak{p}$. If an elliptic curve $\tilde{E}$ over $\overline{\mathbb{F}}_p$ has invariant $j \notin \{0, 1728\}$ then it also holds for $\tilde{E}^{\sigma_p}$ and $\tilde{E}^{\sigma_p^{-1}}$. Thus by the description above we have the following commutative diagram

$$\begin{tikzcd}
S_1(N)'_{\mathrm{gd}} \arrow[r, "T_p"] \arrow[d] & \mathrm{Div}(S_1(N)'_{\mathrm{gd}}) \arrow[d] \\
\tilde{S}_1(N)' \arrow[r, "\sigma_p + p\widetilde{\langle p \rangle}\sigma_p^{-1}"] & \mathrm{Div}(\tilde{S}_1(N)')
\end{tikzcd}$$

and this gives

$$\begin{tikzcd}
\mathrm{Div}^0(S_1(N)'_{\mathrm{gd}}) \arrow[r, "T_p"] \arrow[d] & \mathrm{Div}^0(S_1(N)'_{\mathrm{gd}}) \arrow[d] \\
\mathrm{Div}^0(\tilde{S}_1(N)') \arrow[r, "\sigma_p + p\widetilde{\langle p \rangle}\sigma_p^{-1}"] & \mathrm{Div}^0(\tilde{S}_1(N)')
\end{tikzcd} \tag{4.5}$$

**Lemma 4.5.2.** *The following diagram commutes*

$$\begin{tikzcd}
\mathrm{Div}^0(\tilde{S}_1(N)') \arrow[r, "\sigma_p+p\widetilde{\langle p\rangle}\sigma_p^{-1}"] \arrow[d] & \mathrm{Div}^0(\tilde{S}_1(N)') \arrow[d] \\
\mathrm{Pic}^0(\tilde{X}_1(N)) \arrow[r, "\sigma_{p,*}+\widetilde{\langle p\rangle}_*\sigma_p^*"] & \mathrm{Pic}^0(\tilde{X}_1(N))
\end{tikzcd}$$

*Proof.* Note that we have the following commutative diagrams

$$\begin{tikzcd}
\mathrm{Div}^0(\tilde{S}_1(N)') \arrow[r, "\sigma_p"] \arrow[d] & \mathrm{Div}^0(\tilde{S}_1(N)') \arrow[d] \\
\mathrm{Div}^0(\tilde{X}_1(N)^{\mathrm{planar}}) \arrow[r, "\sigma_{p,*}"] & \mathrm{Div}^0(\tilde{X}_1(N)^{\mathrm{planar}})
\end{tikzcd} \tag{4.6}$$

and

$$\begin{tikzcd}
\mathrm{Div}^0(\tilde{S}_1(N)') \arrow[r, "p\sigma_p^{-1}"] \arrow[d] & \mathrm{Div}^0(\tilde{S}_1(N)') \arrow[d] \\
\mathrm{Div}^0(\tilde{X}_1(N)^{\mathrm{planar}}) \arrow[r, "\sigma_p^*"] & \mathrm{Div}^0(\tilde{X}_1(N)^{\mathrm{planar}})
\end{tikzcd} \tag{4.7}$$

where the maps on the left and right are given by $[E_j, Q] \mapsto [j, x(Q)]$. There is a birational equivalence $h$ from $\tilde{X}_1(N)^{\mathrm{planar}}$ to $\tilde{X}_1(N)$ hence we have the following diagram

$$\begin{tikzcd}
\mathrm{Div}^0(\tilde{X}_1(N)^{\mathrm{planar}}) \arrow[r, "\sigma_{p,*}"] \arrow[d, "h_*"] & \mathrm{Div}^0(\tilde{X}_1(N)^{\mathrm{planar}}) \arrow[d, "h_*"] \\
\mathrm{Div}^0(\tilde{X}_1(N)) \arrow[r, "\sigma_{p,*}"'] & \mathrm{Div}^0(\tilde{X}_1(N))
\end{tikzcd}$$

and similarly

$$\begin{tikzcd}
\mathrm{Div}^0(\tilde{X}_1(N)^{\mathrm{planar}}) \arrow[r, "\sigma_p^*"] \arrow[d, "h_*"] & \mathrm{Div}^0(\tilde{X}_1(N)^{\mathrm{planar}}) \arrow[d, "h_*"] \\
\mathrm{Div}^0(\tilde{X}_1(N)) \arrow[r, "\sigma_p^*"'] & \mathrm{Div}^0(\tilde{X}_1(N))
\end{tikzcd}$$

Now the bottom rows of these two diagrams descend to Picard groups. Combining these two diagrams with the diagrams (**??**) and (**??**) we get the following diagrams

$$\begin{tikzcd}
\mathrm{Div}^0(\tilde{S}_1(N)') \arrow[r, "\sigma_p"] \arrow[d] & \mathrm{Div}^0(\tilde{S}_1(N)') \arrow[d] \\
\mathrm{Pic}^0(\tilde{X}_1(N)) \arrow[r, "\sigma_{p,*}"] & \mathrm{Pic}^0(\tilde{X}_1(N))
\end{tikzcd} \tag{4.8}$$

and

$$\begin{tikzcd}
\mathrm{Div}^0(\tilde{S}_1(N)') \arrow[r, "p\sigma_p^{-1}"] \arrow[d] & \mathrm{Div}^0(\tilde{S}_1(N)') \arrow[d] \\
\mathrm{Pic}^0(\tilde{X}_1(N)) \arrow[r, "\sigma_p^*"] & \mathrm{Pic}^0(\tilde{X}_1(N))
\end{tikzcd} \tag{4.9}$$

Consider the cube-shaped diagram,

$$\begin{tikzcd}
& \mathrm{Pic}^0(X_1(N)) \arrow[rr, "\langle d\rangle^*"] \arrow[dd] & & \mathrm{Pic}^0(X_1(N)) \arrow[dd] \\
\mathrm{Div}^0(S_1(N)'_{\mathrm{gd}}) \arrow[ur] \arrow[rr, "\langle d\rangle"] \arrow[dd] & & \mathrm{Div}^0(S_1(N)'_{\mathrm{gd}}) \arrow[ur] \arrow[dd] & \\
& \mathrm{Pic}^0(\tilde{X}_1(N)) \arrow[rr, "\widetilde{\langle d\rangle}_*"] & & \mathrm{Pic}^0(\tilde{X}_1(N)) \\
\mathrm{Div}^0(\tilde{S}_1(N)') \arrow[ur] \arrow[rr, "\widetilde{\langle d\rangle}"] & & \mathrm{Div}^0(\tilde{S}_1(N)') \arrow[ur] &
\end{tikzcd}$$

Note that the bottom row is the diagram

$$\begin{tikzcd}
\mathrm{Div}^0(\tilde{S}_1(N)') \arrow[r] \arrow[d] & \mathrm{Div}^0(\tilde{S}_1(N)') \arrow[d] \\
\mathrm{Pic}^0(\tilde{X}_1(N)) \arrow[r] & \mathrm{Pic}^0(\tilde{X}_1(N))
\end{tikzcd}$$

and all other diagrams commute and left front vertical map is surjective and so the bottom diagram also commutes. Hence by the diagram (**??**) we get the following commutative diagram

$$\begin{tikzcd}
\mathrm{Div}^0(\tilde{S}_1(N)') \arrow[r, "p\sigma_p^{-1}"] \arrow[d] & \mathrm{Div}^0(\tilde{S}_1(N)') \arrow[r, "\widetilde{\langle d\rangle}"] \arrow[d] & \mathrm{Div}^0(\tilde{S}_1(N)') \arrow[d] \\
\mathrm{Pic}^0(\tilde{X}_1(N)) \arrow[r, "\sigma_p^*"] & \mathrm{Pic}^0(\tilde{X}_1(N)) \arrow[r, "\widetilde{\langle d\rangle}_*"] & \mathrm{Pic}^0(\tilde{X}_1(N))
\end{tikzcd}$$

Now by the diagram (**??**) we get the commutetive diagram in the lemma. □

Now we are ready to give the Eichler-Shimura relation,

**Theorem 4.5.2.** *Let $p \nmid N$. Then the following diagram commutes:*

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

*Proof.* Consider the following cube-shaped diagram,

$$\begin{tikzcd}
 & \mathrm{Pic}^0(X_1(N)) \arrow[rr, "T_p"] \arrow[dd] & & \mathrm{Pic}^0(X_1(N)) \arrow[dd] \\
\mathrm{Div}^0(S_1(N)'_{\mathrm{gd}}) \arrow[ur] \arrow[rr, "T_p"] \arrow[dd] & & \mathrm{Div}^0(S_1(N)'_{\mathrm{gd}}) \arrow[ur] \arrow[dd] & \\
 & \mathrm{Pic}^0(\tilde{X}_1(N)) \arrow[rr, "\sigma_{p,*}+\widetilde{\langle p\rangle}_*\sigma_p^*"] & & \mathrm{Pic}^0(\tilde{X}_1(N)) \\
\mathrm{Div}^0(\tilde{S}_1(N)') \arrow[ur] \arrow[rr, "\sigma_p+p\widetilde{\langle p\rangle}\sigma_p^{-1}"] & & \mathrm{Div}^0(\tilde{S}_1(N)') \arrow[ur] &
\end{tikzcd}$$

Note that the left and right sides of the cube are commutative diagrams from Theorem **??**. The top square is the commutative diagram (**??**). The front square is the commutative diagram (**??**) and the bottom square is the commutative diagram from Lemma **??**. Let $\sigma$ denote the map $\sigma_{p,*} + \widetilde{\langle p\rangle}_*\sigma_p^*$. Consider the following chain of maps

$$\begin{tikzcd}
\mathrm{Div}^0(S_1(N)'_{\mathrm{gd}}) \arrow[r] & \mathrm{Div}^0(\tilde{S}_1(N)') \arrow[r] & \mathrm{Pic}^0(\tilde{X}_1(N)) \arrow[r, "\sigma"] & \mathrm{Pic}^0(\tilde{X}_1(N))
\end{tikzcd} \tag{4.10}$$

where the first two maps are surjective. By commutativity of the left side (**??**) is

$$\begin{tikzcd}\mathrm{Div}^0(S_1(N)'_{\mathrm{gd}}) \arrow[r] & \mathrm{Pic}^0(X_1(N)) \arrow[r] & \mathrm{Pic}^0(\tilde{X}_1(N)) \arrow[r, "\sigma"] & \mathrm{Pic}^0(\tilde{X}_1(N))\end{tikzcd} \tag{4.11}$$

where the composition of the first two maps is surjective. Since the bottom, front and top squares are commutative (**??**) becomes

$$\begin{tikzcd}\mathrm{Div}^0(S_1(N)'_{\mathrm{gd}}) \arrow[r] & \mathrm{Pic}^0(X_1(N)) \arrow[r, "T_p"] & \mathrm{Pic}^0(X_1(N)) \arrow[r] & \mathrm{Pic}^0(\tilde{X}_1(N))\end{tikzcd} \tag{4.12}$$

We know that there exists a map $\tilde{T_p} : \mathrm{Pic}^0(\tilde{X}_1(N)) \to \mathrm{Pic}^0(\tilde{X}_1(N))$ such that the back square of the cube commutes and so we have

$$\begin{tikzcd}\mathrm{Div}^0(S_1(N)'_{\mathrm{gd}}) \arrow[r] & \mathrm{Pic}^0(X_1(N)) \arrow[r] & \mathrm{Pic}^0(X_1(N)) \arrow[r, "\tilde{T_p}"] & \mathrm{Pic}^0(\tilde{X}_1(N))\end{tikzcd} \tag{4.13}$$

Now this is the same chain with (**??**) and since the composite of the first two maps is surjective, $\tilde{T_p} = \sigma$. □

Thus the Hecke operator $T_p$ is now described in characteristic $p$ in terms of the Frobenius map $\sigma_p$.

# 5 Galois Representations

In this section we construct Galois representations attached to Elliptic curves and modular forms. Then give a brief overview of the method of Wiles's proof of modularity theorem.

## 5.1 Galois number fields

Let $F$ be a Galois number field, i.e. a finite Galois extension of $\mathbb{Q}$. Let $p$ be a rational prime. Then we have a factorization $p\mathcal{O}_F = (\mathfrak{p}_1 ... \mathfrak{p}_g)^e$, where $e$ is the ramification degree of $p$, $g$ is the decomposition index. Let $f$ be the residue degree, i.e. the dimension of $\mathcal{O}_F/\mathfrak{p}$ over $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$. Then we have $|\mathrm{Gal}(F/\mathbb{Q})| = efg$.

The decomposition group of a maximal ideal $\mathfrak{p}$ of $\mathcal{O}_F$ lying over $p$ is the set

$$D_{\mathfrak{p}} = \{\sigma \in \mathrm{Gal}(F/\mathbb{Q}) : \mathfrak{p}^\sigma = \mathfrak{p}\}.$$

Since $\mathrm{Gal}(F/\mathbb{Q})$ acts transitively on the set of maximal ideals in the factorization of $p\mathcal{O}_F$, the order of $D_{\mathfrak{p}}$ is $ef$. Note that $D_{\mathfrak{p}}$ acts on the residue field $\mathbf{f}_{\mathfrak{p}} = \mathcal{O}_F/\mathfrak{p} \cong \mathbb{F}_{p^f}$,

$$(x + \mathfrak{p})^\sigma = x^\sigma + \mathfrak{p}, \qquad x \in \mathcal{O}_F,\ \sigma \in D_{\mathfrak{p}}.$$

The kernel of this action is called the inertia group of $\mathfrak{p}$,

$$I_{\mathfrak{p}} = \{\sigma \in D_{\mathfrak{p}} : x^\sigma \equiv x \mod \mathfrak{p} \text{ for all } x \in \mathcal{O}_F\}.$$

The order of $I_{\mathfrak{p}}$ is $e$. Consider $\mathbb{F}_p$ as a subfield of $\mathbf{f}_{\mathfrak{p}}$. Hence we have an injection $D_{\mathfrak{p}}/I_{\mathfrak{p}} \to \mathrm{Gal}(\mathbf{f}_{\mathfrak{p}}/\mathbb{F}_p) = \langle \sigma_p \rangle$, where $\sigma_p$ is the Frobenius automorphism in characteristic $p$. Since both sides has order $f$ the injection is actually an isomorphism. Therefore $D_{\mathfrak{p}}/I_{\mathfrak{p}}$ has an element that maps to $\sigma_p$. Any representative of this element in $D_{\mathfrak{p}}$ is called a Frobenius element of $\mathrm{Gal}(F/\mathbb{Q})$ denoted by $\mathrm{Frob}_{\mathfrak{p}}$. Hence $\mathrm{Frob}_{\mathfrak{p}}$ is defined up to inertia and so when $p$ is unramified $\mathrm{Frob}_{\mathfrak{p}}$ is unique. The action of $\mathrm{Frob}_{\mathfrak{p}}$ descends to the residue field as

$$x^{\mathrm{Frob}_{\mathfrak{p}}} \equiv x^p \mod \mathfrak{p} \qquad \text{for all } x \in \mathcal{O}_F.$$

Let $\mathfrak{p}'$ and $\mathfrak{p}$ be two maximal ideals lying over $p$. Since $\mathrm{Gal}(F/\mathbb{Q})$ acts transitively on the maximal ideals lying above $p$, there exists an automorphism $\sigma \in \mathrm{Gal}(F/\mathbb{Q})$ such that $\mathfrak{p}^{\sigma} = \mathfrak{p}'$. It is easy to see that the decomposition group associated to $\mathfrak{p}'$ is $D_{\mathfrak{p}'} = D_{\mathfrak{p}^{\sigma}} = \sigma^{-1} D_{\mathfrak{p}} \sigma$, and the inertia group of $\mathfrak{p}'$ is $I_{\mathfrak{p}'} = I_{\mathfrak{p}^{\sigma}} = \sigma^{-1} I_{\mathfrak{p}} \sigma$. The relation between the corresponding Frobenius elements is $\mathrm{Frob}_{\mathfrak{p}'} = \mathrm{Frob}_{\mathfrak{p}^{\sigma}} = \sigma^{-1} \mathrm{Frob}_{\mathfrak{p}} \sigma$. Therefore if the Galois group is abelian the $\mathrm{Frob}_{\mathfrak{p}}$ depends only on the underlying prime and so can be denoted by $\mathrm{Frob}_p$.

We state the following theorem without proof which we use later.

**Theorem 5.1.1.** *Let $F$ be a Galois number field. Then every element of* $\mathrm{Gal}(F/\mathbb{Q})$ *takes the form* $\mathrm{Frob}_{\mathfrak{p}}$ *for infinitely many maximal ideals $\mathfrak{p}$ of $\mathcal{O}_F$.*

Let $\ell$ be a prime number. Consider the affine algebraic curve over $\mathbb{Q}$, $C : xy = 1$. Under the map $(x, y) \mapsto x$, the points of $C$ are identified with the Abelian group $\overline{\mathbb{Q}}^{*}$. This induces an Abelian group structure on points of $C$ where the group operation is point wise multiplication. Let $n \in \mathbb{Z}^{+}$. The points of $C$ of order $\ell^n$ form a subgroup $C[\ell^n]$ which is identified with the $\ell^n$th roots of unity by the above identification. Thus we have an isomorphism $C[\ell^n] \xrightarrow{\sim} \mathbb{Z}/\ell^n\mathbb{Z}$ given by $\mu_{\ell^n}^{a} \mapsto a$. Therefore we also have

$$\mathrm{Aut}(C[\ell^n]) \xrightarrow{\sim} (\mathbb{Z}/\ell^n\mathbb{Z})^{*}$$

given by $(\mu_{\ell^n} \mapsto \mu_{\ell^n}^{m}) \mapsto m$. This extends to the following isomorphism

$$\mathrm{Gal}(\mathbb{Q}(\mu_{\ell^n})/\mathbb{Q}) \xrightarrow{\sim} (\mathbb{Z}/\ell^n\mathbb{Z})^{*}, \qquad (\sigma : \mu_{\ell^n} \mapsto \mu_{\ell^n}^{m}) \mapsto m.$$

Put the number fields $\mathbb{Q}(\mu_{\ell^n})$ together for all $n$ and define $\mathbb{Q}(\mu_{\ell^\infty}) = \bigcup_{n=1}^{\infty} \mathbb{Q}(\mu_{\ell^n})$. This is a subfield of $\overline{\mathbb{Q}}$ and has infinite degree over $\mathbb{Q}$. Let $G_{\mathbb{Q},\ell} = \mathrm{Aut}(\mathbb{Q}(\mu_{\ell^\infty}))$. Every element $\sigma \in G_{\mathbb{Q},\ell}$ restricts to $\sigma_n \in \mathrm{Gal}(\mathbb{Q}(\mu_{\ell^n})/\mathbb{Q})$ for each $n$. The restrictions form a sequence $(\sigma_1, \sigma_2, ...)$ such that $\sigma_{n+1}|_{\mathbb{Q}(\mu_{\ell^n})} = \sigma_n$ for all $n$. Conversely, let $(\sigma_1, \sigma_2, ...)$ be a compatible sequence as described above. Define $\sigma \in \mathrm{Aut}(\mathbb{Q}(\mu_{\ell^\infty}))$ by $\sigma(x) = \sigma_n(x)$ if $x \in \mathbb{Q}(\mu_{\ell^n})$. The compatibility guarantee that $\sigma$ is well-defined.

Thus $G_{\mathbb{Q},\ell}$ is the group of compatible sequences where the group operation is componentwise composition. Thus $G_{\mathbb{Q},\ell} = \varprojlim_n \mathrm{Gal}(\mathbb{Q}(\mu_{\ell^n})/\mathbb{Q})$. Hence $G_{\mathbb{Q},\ell} \cong \mathbb{Z}_\ell^*$.

The $\ell$-adic Tate module of $C$ is

$$\mathrm{Ta}_\ell(C) = \{(\mu_\ell^{a_1}, \mu_2^{a_2}, ...) : \mu_{\ell^n}^{a_{n+1}} = \mu_{\ell^n}^{a_n} \text{ for all } n\} \cong \mathbb{Z}_\ell.$$

$G_{\mathbb{Q},\ell}$ acts on $\mathrm{Ta}_\ell(C)$ componentwise.

## 5.2 Galois representations

The absolute Galois group of $\mathbb{Q}$ will be denoted by $G_{\mathbb{Q}} = \mathrm{Aut}(\overline{\mathbb{Q}})$ where $\overline{\mathbb{Q}}$ denote the algebraic closure of $\mathbb{Q}$. $\overline{\mathbb{Q}}$ is the union of all Galois number fields. Let $\sigma \in G_{\mathbb{Q}}$ be an automorphism of $\overline{\mathbb{Q}}$. For any Galois number field $F$, $\sigma$ restricts to $\sigma|_F \in \mathrm{Gal}(F/\mathbb{Q})$. If $F$ and $F'$ are two Galois number fields such that $F \subset F'$ then we have $\sigma_F = \sigma_{F'}|_F$. Conversely, every system of automorphisms $\{\sigma_F\}$ satisfying the above compatibility criterion defines an automorphism $\sigma$ of $\overline{\mathbb{Q}}$ as follows: Let $x \in \overline{\mathbb{Q}}$. Then $x \in F$ for some Galois number field $F$. Define $\sigma(x) = \sigma_F(x)$. $\sigma$ is well-defined as $\{\sigma_F\}$ is compatible. This shows that

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

Being the inverse limit of finite groups, $G_{\mathbb{Q}}$ is profinite.

For each $\sigma \in G_{\mathbb{Q}}$ and each Galois number field $F$ let $U_\sigma(F) = \sigma \cdot \ker(G_{\mathbb{Q}} \to \mathrm{Gal}(F/\mathbb{Q}))$. 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. As $G_{\mathbb{Q}}$ is profinite, it is compact. For $\sigma = 1$, denote $U_\sigma(F)$ by $U(F)$. Note that $U(F)$ is an open normal subgroup for every Galois number field $F$. Conversely, every open normal subgroup of $G_{\mathbb{Q}}$ is of the form $U(F)$ for some $F$. Indeed; let $U$ be an open normal subgroup of $G_{\mathbb{Q}}$. Since $1 \in U$, $U(F) \subset U$ for some $F$. Hence

$$\mathrm{Gal}(F/\mathbb{Q}) \cong G_{\mathbb{Q}}/U(F) \twoheadrightarrow G_{\mathbb{Q}}/U.$$

Thus $G_{\mathbb{Q}}/U$ is isomorphic to a quotient of $\mathrm{Gal}(F/\mathbb{Q})$ and so $G_{\mathbb{Q}}/U = \mathrm{Gal}(F'/\mathbb{Q})$ for some $F' \subset F$. This shows that $U = \ker(G_{\mathbb{Q}} \twoheadrightarrow \mathrm{Gal}(F'/\mathbb{Q})) = U(F')$.

Let $p \in \mathbb{Z}$ be a prime and $\mathfrak{p} \subset \overline{\mathbb{Z}}$ be a maximal ideal over $p$, where $\overline{\mathbb{Z}}$ denotes the integral closure of $\mathbb{Z}$ in $\overline{\mathbb{Q}}$. The decomposition group of $\mathfrak{p}$ is

$$D_{\mathfrak{p}} = \{\sigma \in G_{\mathbb{Q}} : \mathfrak{p}^\sigma = \mathfrak{p}\}.$$

Hence $D_{\mathfrak{p}}$ acts on $\overline{\mathbb{Z}}/\mathfrak{p}$ as $(x + \mathfrak{p})^\sigma = x^\sigma + \mathfrak{p}$. Since $\overline{\mathbb{Z}}/\mathfrak{p} \cong \overline{\mathbb{F}}_p$, this action can be viewed as an action on $\overline{\mathbb{F}}_p$. Hence we have a map $D_{\mathfrak{p}} \to \mathrm{G}_{\mathbb{F}_p}$, where $\mathrm{G}_{\mathbb{F}_p}$ denotes the absolute Galois group of $\mathbb{F}_p$. This map is surjective since it is surjective at each finite level. An absolute Frobenius element over $p$ is an element $\mathrm{Frob}_{\mathfrak{p}} \in D_{\mathfrak{p}}$ that maps to the Frobenius automorphism $\sigma_p \in \mathrm{G}_{\mathbb{F}_p}$. Note that $\mathrm{Frob}_{\mathfrak{p}}$ is defined up to the kernel of the action, the inertia group

$$I_{\mathfrak{p}} = \{\sigma \in D_{\mathfrak{p}} : x^\sigma \equiv x \mod \mathfrak{p} \text{ for all } x \in \overline{\mathbb{Z}}\}.$$

The restriction map $G_{\mathbb{Q}} \to \mathrm{Gal}(F/\mathbb{Q})$ takes $\mathrm{Frob}_{\mathfrak{p}}$ to a Frobenius element in $\mathrm{Gal}(F/\mathbb{Q})$, i.e. $\mathrm{Frob}_{\mathfrak{p}}|_F = \mathrm{Frob}_{\mathfrak{p}_F}$ where $\mathfrak{p}_F = \mathfrak{p} \cap F$.

The following theorem illustrate why we are interested in Frobenius elements.

**Theorem 5.2.1.** *The set*

$$\{\mathrm{Frob}_{\mathfrak{p}} : \mathfrak{p} \subset \overline{\mathbb{Z}} \text{ is maximal ideal lying over any but finite set of primes } p\}$$

*is dense in* $G_{\mathbb{Q}}$

*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 $\mathrm{Frob}_{\mathfrak{p}} \in U$. By Theorem **??**, $\sigma|_F \in \mathrm{Gal}(F/\mathbb{Q})$ takes the form $\mathrm{Frob}_{\mathfrak{p}_F}$ for some maximal ideal $\mathfrak{p}_F \in \mathcal{O}_F$. Lift $\mathfrak{p}_F$ to a maximal ideal $\mathfrak{p}$ of $\overline{\mathbb{Z}}$, i.e. $\mathfrak{p} \cap F = \mathfrak{p}_F$. Thus $\mathrm{Frob}_{\mathfrak{p}}|_F = \mathrm{Frob}_{\mathfrak{p}_F} = \sigma|_F$. Hence $\mathrm{Frob}_{\mathfrak{p}} \cdot \sigma^{-1} \in \ker(G_{\mathbb{Q}} \to \mathrm{Gal}(F/\mathbb{Q}))$ which implies $\mathrm{Frob}_{\mathfrak{p}} \in U_\sigma(F)$. □

Let $\chi : (\mathbb{Z}/N\mathbb{Z})^* \to \mathbb{C}^*$ be a primitive Dirichlet character. Then we have

$$\begin{tikzcd} G_{\mathbb{Q}} \arrow[r, "\pi_N"] & \mathrm{Gal}(\mathbb{Q}(\mu_N)/\mathbb{Q}) \arrow[r, "\varphi"] & (\mathbb{Z}/N\mathbb{Z})^* \arrow[r, "\chi"] & \mathbb{C}^* \end{tikzcd}$$

where $\pi_N$ is just the restriction map and $\varphi$ is the isomorphism which is defined by $(\mu_N \mapsto \mu_N^a) \mapsto a$. This shows that $\chi$ determine a homomorphism

$$\rho_\chi = \chi \circ \varphi \circ \pi_N : G_{\mathbb{Q}} \to \mathbb{C}^*.$$

It is easy to see that $\rho_\chi(\mathrm{conj}) = -1$ and $\rho_\chi(\mathrm{Frob}_{\mathfrak{p}}) = \chi(p)$, where conj denotes the complex conjugation. Let us see that $\rho_\chi$ is continuous. To see this we use the following standard result

**Lemma 5.2.1.** *Let $\rho : G \to H$ be a homomorphism of topological groups. $\rho$ is continuous if and only if $\rho^{-1}(V)$ is open for each $V$ in a basis of neighborhoods of identity $1_H$.*

Suppose $\rho_\chi^{-1}(1)$ is open in $G_{\mathbb{Q}}$. Let $V$ be an element of basis of neighborhoods of 1 and let $g \in \rho_\chi^{-1}(V) \supseteq \rho_\chi^{-1}(1)$. Thus $\rho_\chi(g \cdot \rho_\chi^{-1}(1)) \subset V$. Since $\rho_\chi^{-1}(1)$ is open,

$g \cdot \rho_\chi^{-1}(1)$ is open and $g \in g \cdot \rho_\chi^{-1}(1) \subset \rho_\chi^{-1}(V)$. Therefore $\rho_\chi^{-1}(V)$ is open and by the above lemma $\rho_\chi$ is continuous. Therefore we only need to check that $\rho_\chi^{-1}(1)$ is open. To see this note that $\pi_N(\rho_\chi^{-1}(1)) \lhd \mathrm{Gal}(\mathbb{Q}(\mu_N)/\mathbb{Q})$. This is because $\pi_N$ is surjective. Thus Galois theory implies that there exists a subextension $F \subset \mathbb{Q}(\mu_N)$ such that $\mathrm{Gal}(\mathbb{Q}(\mu_N)/F) = \pi_N(\rho_\chi^{-1}(1))$. Our claim is that $\rho_\chi^{-1}(1) = U(F)$. To see this let $\sigma \in U(F)$. Hence $\sigma|_{\mathbb{Q}(\mu_N)} \in \mathrm{Gal}(\mathbb{Q}(\mu_N)/F)$ and so $\pi_N(\sigma) \in \pi_N(\rho_\chi^{-1}(1)) \subset \ker(\chi \circ \varphi)$. Thus $\chi \circ \varphi \circ \pi_N(\sigma) = 1$ which proves $\sigma \in \rho_\chi^{-1}(1)$. Coversely, let $\sigma \in \rho_\chi^{-1}(1)$. Then $\pi_N(\sigma) \in \mathrm{Gal}(\mathbb{Q}(\mu_N)/F)$ and so $\sigma|_F = \mathrm{id}_F$, i.e. $\sigma \in U(F)$. Therefore $\rho_\chi^{-1}(1) = U(F)$ which is open. Thus $\rho_\chi^{-1}(1)$ is open. This finishes the proof of $\rho_\chi$ is continuous.

Conversely, every continuous homomorphism $\rho : G_{\mathbb{Q}} \to \mathbb{C}^*$ arise from a Dirichlet character. First let us see that any such homomorphism has finite image. The following lemma proves more.

**Lemma 5.2.2.** *Any continuous homomorphism $\rho : G_{\mathbb{Q}} \to GL_d(\mathbb{C})$ factors through $\mathrm{Gal}(F/\mathbb{Q}) \to GL_d(\mathbb{C})$ for some Galois number field $F$. Thus the image of $\rho$ is finite.*

*Proof.* Take a neighborhood $V$ of $I \in GL_d(\mathbb{C})$ containing no nontrivial subgroup. Let $U = \rho^{-1}(V)$. Since $U$ is a neighborhood of $1 \in G_{\mathbb{Q}}$, $U(F) \subset U$ for some Galois number field $F$. We have $\ker \rho \subset U$ and if there exists $\sigma \in U(F) \backslash \ker \rho$, then $\rho(U(F))$ gives a nontrivial subgroup of $V$ which contradicts the choice of $V$. Thus $U(F) \subset \ker \rho$. Hence we have a surjective map

$$\mathrm{Gal}(F/\mathbb{Q}) \cong G_{\mathbb{Q}}/U(F) \twoheadrightarrow G_{\mathbb{Q}}/\ker \rho.$$

This proves the lemma. □

Now since $\ker \rho$ is a closed normal subgroup of $G_{\mathbb{Q}}$, it corresponds to a Galois extension $L/\mathbb{Q}$ with $\mathrm{Gal}(L/\mathbb{Q}) \cong \mathrm{Im}\rho$. Thus $\rho$ factors through some Abelian Galois extension $F/\mathbb{Q}$ and by Kronecker-Weber Theorem, we may take $F = \mathbb{Q}(\mu_N)$ for some $N$. Thus we have

$$\begin{tikzcd}
G_{\mathbb{Q}} \arrow[r, "\pi_N"] & \mathrm{Gal}(\mathbb{Q}(\mu_N)/\mathbb{Q}) \arrow[r] \arrow[d, "\varphi"] & \mathbb{C}^* \\
 & (\mathbb{Z}/N\mathbb{Z})^* \arrow[ur, dashed, "\chi"'] &
\end{tikzcd}$$

This shows that $\rho = \rho_\chi$ and so we have seen that there is a correspondence between continuous homomorphisms $\rho : G_{\mathbb{Q}} \to \mathbb{C}^*$ and Dirichlet characters.

**Definition 5.2.1.** *Let $d$ be a positive integer. A $d$-dimensional $\ell$-adic Galois representation is a continuous homomorphism*

$$\rho : G_{\mathbb{Q}} \to GL_d(\mathbf{L})$$

*where $\mathbf{L}$ is a finite extension of $\mathbb{Q}_\ell$. If $\rho' : G_{\mathbb{Q}} \to GL_d(\mathbf{L})$ is another such representation and there exists $m \in GL_d(\mathbf{L})$ such that $\rho'(\sigma) = m^{-1}\rho(\sigma)m$ for all $\sigma \in G_{\mathbb{Q}}$ then $\rho$ and $\rho'$ are equivalent, denoted as $\rho \sim \rho'$.*

An example of a one dimensional $\ell$-adic Galois representation is the $\ell$-adic cyclotomic character: We have seen that $\mathrm{Gal}(\mathbb{Q}(\mu_{\ell^\infty})/\mathbb{Q}) \cong \mathbb{Z}_\ell^*$. The containment $\mathbb{Q}(\mu_{\ell^\infty}) \subset \overline{\mathbb{Q}}$ gives a surjection $G_{\mathbb{Q}} \twoheadrightarrow G_{\mathbb{Q},\ell}$. Combining this map with the isomorphism above we get

$$\chi_\ell : G_{\mathbb{Q}} \to \mathbb{Z}_\ell^*$$

given by $\sigma \mapsto (m_1, m_2, ...)$ such that $\mu_{\ell^n}^{\sigma} = \mu_{\ell^n}^{m_n}$ for all $n$. Thus $\chi_\ell$ arises from the $G_{\mathbb{Q}}$-module structure of the Tate module of C given before. We need to check that $\chi_\ell$ is continuous. By Lemma **??** it suffices to check that $\chi_\ell^{-1}(U(n))$ is open for all $n$. Here $U(n) = \ker(\mathbb{Z}_\ell^* \to (\mathbb{Z}/\ell^n\mathbb{Z})^*)$. We have $\chi_\ell(\sigma) \in U(n) \Leftrightarrow \mu_{\ell^n}^{\sigma} = \mu_{\ell^n} \Leftrightarrow \sigma|_{\mathbb{Q}(\mu_{\ell^n})} = \mathrm{id} \Leftrightarrow \sigma \in \ker(G_{\mathbb{Q}} \to \mathrm{Gal}(\mathbb{Q}(\mu_{\ell^n})/\mathbb{Q})) \Leftrightarrow \sigma \in U(\mathbb{Q}(\mu_{\ell^n}))$. This shows that $\chi_\ell^{-1}(U(n)) = U(\mathbb{Q}(\mu_{\ell^n}))$ and so it is open which proves $\chi_\ell$ is continuous.

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

**Definition 5.2.2.** *Let $\rho$ be a Galois representation and $p$ be a prime. Then $\rho$ is unramified at $p$ if $I_{\mathfrak{p}} \subset \ker \rho$ for any maximal ideal $\mathfrak{p} \subset \overline{\mathbb{Z}}$ lying above $p$.*

If the Galois representation $\rho$ is unramified at all but finitely many primes $p$, then the values $\rho(\mathrm{Frob}_{\mathfrak{p}})$ for $\mathfrak{p}$ lying over unramified primes $p$ determine $\rho$ everywhere by continuity of $\rho$ and Theorem **??**.

We have seen that $\chi_\ell$ arises from the $G_{\mathbb{Q}}$-module structure of $\mathrm{Ta}_\ell(C)$. Let $V_\ell(C) = \mathrm{Ta}_\ell(C) \otimes \mathbb{Q}$. This is a one dimensional vector space over $\mathbb{Q}_\ell$. Consider the commutative diagram

$$\begin{tikzcd}
V_\ell(C) \times G_{\mathbb{Q}} \arrow[r] \arrow[d, "\chi_\ell"] & V_\ell(C) \arrow[d] \\
\mathbb{Q}_\ell \times \mathbb{Q}_\ell^* \arrow[r] & \mathbb{Q}_\ell
\end{tikzcd}$$

The action of $G_{\mathbb{Q}}$ on $V_\ell(C)$ is continuous since the other maps in the diagram are continuous.

**Definition 5.2.3.** *Let $d$ be a positive integer. A $d$-dimensional $\ell$-adic Galois representation is a $d$-dimensional vector space $V$ over $\mathbf{L}$ where $\mathbf{L}$ is a finite extension 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 continuous. If $V'$ is another such representation and there is a continuous $G_{\mathbb{Q}}$-module isomorphism $V \xrightarrow{\sim} V'$ then $V$ and $V'$ are equivalent.*

This definition is compatible with the Definition **??** given earlier. To see this let $\rho : G_{\mathbb{Q}} \to GL_d(\mathbf{L})$ be a Galois representation as in Definition **??**. Now $\mathbf{L}^d$ is a $d$ dimensional vector space over $\mathbf{L}$. Consider the map

$$\mathbf{L}^d \times G_{\mathbb{Q}} \to \mathbf{L}^d \qquad (v, \sigma) \mapsto v\rho(\sigma).$$

This map is continuous since $\rho$ is continuous and so $\mathbf{L}^d$ is a d-dimensional Galois representation as in the Definition **??**.

Conversely, let $V$ be a d-dimensional Galois representation as in Definition **??**. By fixing a basis of $V$ we can identify $\mathrm{Aut}(V)$ with $GL_d(\mathbf{L})$. Then the map

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

induces a map

$$\rho : G_{\mathbb{Q}} \to GL_d(\mathbf{L}).$$

and $\rho$ is continuous.

In the above examples of Galois representations we have seen that the image of the representation lies in $GL_d(\mathcal{O}_L)$. The following proposition shows that this is true in general.

**Propositition 5.2.1.** *Let $\rho : G_{\mathbb{Q}} \to GL_d(L)$ be a Galois representation. Then $\rho$ is similar to a Galois representation $\rho' : G_{\mathbb{Q}} \to GL_d(\mathcal{O}_L)$.*

*Proof.* See [**?**, Proposition 9.3.5]. □

## 5.3 Galois representations and elliptic curves

Our aim in this section is to construct two dimensional Galois representations attached to elliptic curves. Let $E$ be an elliptic curve over $\mathbb{Q}$ and $\ell$ be a prime. Multiplication by $\ell$ between $\ell$-power torsion subgroups of $E$ gives maps

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

The $\ell$-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 $E[\ell^n] \xrightarrow{\sim} (\mathbb{Z}/\ell^n\mathbb{Z})^2$ and since the bases are compatible with the transition maps we can pass to the limit which gives $\mathrm{Ta}_\ell(E) \cong \mathbb{Z}_\ell^2$. 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

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

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 $(P_n, Q_n)$ determine an isomorphism $\mathrm{Aut}(E[\ell^n]) \xrightarrow{\sim} GL_2(\mathbb{Z}/\ell^n\mathbb{Z})$ and by the choice of the basis the following diagram commutes for all $n$

$$\begin{tikzcd}
\mathrm{Aut}(E[\ell^n]) \arrow[r] \arrow[d] & GL_2(\mathbb{Z}/\ell^n\mathbb{Z}) \arrow[d] \\
\mathrm{Aut}(E[\ell^{n+1}]) \arrow[r] & GL_2(\mathbb{Z}/\ell^{n+1}\mathbb{Z})
\end{tikzcd} .$$

Thus we have $\mathrm{Aut}(\mathrm{Ta}_\ell(E)) \xrightarrow{\sim} GL_2(\mathbb{Z}_\ell)$. Combining this isomorphism with the action of $G_{\mathbb{Q}}$ on $\mathrm{Ta}_\ell(E)$ we get a homomorphism

$$\rho_{E,\ell} : G_{\mathbb{Q}} \to GL_2(\mathbb{Z}_\ell) \subset GL_2(\mathbb{Q}_\ell).$$

Let us see that this is a continuous homomorphism. It suffices to check that $\rho_{E,\ell}^{-1}(U(n))$ is open for each $n$ where $U(n) = \ker(GL_2(\mathbb{Z}_\ell) \to GL_2(\mathbb{Z}/\ell^n\mathbb{Z}))$. Now we have

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

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 5.3.1.** *Let $\ell$ 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 $\mathfrak{p} \subset \overline{\mathbb{Z}}$ be any maximal ideal over $p$. Then the characteristic equation of $\rho_{E,\ell}(\mathrm{Frob}_{\mathfrak{p}})$ is*

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

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

*Proof.* Let $p \nmid \ell N$ and $\mathfrak{p}$ lies over $p$. Let $G_{\mathbb{F}_p}$ be the absolute Galois group of $\mathbb{F}_p$. We have a commutative diagram for all $n$,

$$\begin{tikzcd}
D_{\mathfrak{p}} \arrow[r] \arrow[d] & \mathrm{Aut}(E[\ell^n]) \arrow[d] \\
G_{\mathbb{F}_p} \arrow[r] & \mathrm{Aut}(\tilde{E}[\ell^n])
\end{tikzcd}$$

where the map $D_{\mathfrak{p}} \to G_{\mathbb{F}_p}$ is induced by the action of $D_{\mathfrak{p}}$ on $\overline{\mathbb{F}}_p$, the map $D_{\mathfrak{p}} \to \mathrm{Aut}(E[\ell^n])$ is just the restriction of the action of $G_{\mathbb{Q}}$ and the map $G_{\mathbb{F}_p} \to \mathrm{Aut}(\tilde{E}[\ell^n])$ is given by the action of $G_{\mathbb{F}_p}$ on $\tilde{E}$. Now $I_{\mathfrak{p}} \subset \ker(D_{\mathfrak{p}} \to G_{\mathbb{F}_p} \to \mathrm{Aut}(\tilde{E}[\ell^n]))$. Note that $p \nmid \ell N$ implies that $E$ has good reduction at $p$ making $\mathrm{Aut}(E[\ell^n]) \xrightarrow{\sim} \mathrm{Aut}(\tilde{E}[\ell^n])$. Therefore $I_{\mathfrak{p}} \subset \ker(D_{\mathfrak{p}} \to \mathrm{Aut}(E[\ell^n]))$ for all $n$. Thus $I_{\mathfrak{p}} \subset \ker(G_{\mathbb{Q}} \to \mathrm{Aut}(E[\ell^n]))$. Since this is true for all $n$ by definition of $\rho_{E,\ell}$, $I_{\mathfrak{p}} \subset \ker \rho_{E,\ell}$ and so $\rho_{E,\ell}$ is unramified at $p$.

For the characteristic equation of $\rho_{E,\ell}(\mathrm{Frob}_{\mathfrak{p}})$ we need to compute $\det \rho_{E,\ell}(\mathrm{Frob}_{\mathfrak{p}})$ and $\mathrm{tr}\rho_{E,\ell}(\mathrm{Frob}_{\mathfrak{p}})$. Let $\rho_n : G_{\mathbb{Q}} \to \mathrm{Aut}(E[\ell^n]) \xrightarrow{\sim} GL_2(\mathbb{Z}/\ell^n\mathbb{Z})$ be the $n$th entry of $\rho_{E,\ell}$. Considering the Weil pairing of the basis $(P_n, Q_n)$ gives

$$e_{\ell^n}(P_n, Q_n)^{\sigma} = e_{\ell^n}(P^{\sigma}_n, Q^{\sigma}_n) = e_{\ell^n}(P_n, Q_n)^{\det \rho_n(\sigma)}.$$

The second equality comes from the fact that $\left(\begin{smallmatrix} P^{\sigma}_n \\ Q^{\sigma}_n \end{smallmatrix}\right) = \rho_n(\sigma)\left(\begin{smallmatrix} P_n \\ Q_n \end{smallmatrix}\right)$. Since $e_{\ell^n}(P_n, Q_n) = \mu_{\ell^n}$, $\sigma$ acts on $\mu_{\ell^n}$ by $\mu^{\sigma}_{\ell^n} = \mu_{\ell^n}^{\det \rho_n(\sigma)}$. We also have $\mu^{\sigma}_{\ell^n} = \mu_{\ell^n}^{\chi_{\ell,n}(\sigma)}$ where $\chi_{\ell,n}(\sigma)$ denotes the $n$th component of $\chi_{\ell}(\sigma)$. Thus we have $\det \rho_n(\sigma) = \chi_{\ell,n}(\sigma)$ in $(\mathbb{Z}/\ell^n\mathbb{Z})^*$. Since this is true for all $n$, $\det \rho_{E,\ell}(\sigma) = \chi_{\ell}(\sigma)$ in $\mathbb{Z}^*_{\ell}$, and so $\det \rho_{E,\ell}(\mathrm{Frob}_{\mathfrak{p}}) = \chi_{\ell}(\mathrm{Frob}_{\mathfrak{p}}) = p$. For the trace let $A = \rho_{E,\ell}(\mathrm{Frob}_{\mathfrak{p}})$. Since $A$ satisfies its characteristic polynomial we have $\mathrm{tr}(A) = A + pA^{-1}$. As endomorphisms of $\mathrm{Pic}^0(\tilde{E})$, $\sigma_{p,*} + \sigma^*_p = a_p(E)$, where $\sigma_{p,*}$ and $\sigma^*_p$ forward and reverse maps of $\mathrm{Pic}^0(\tilde{E})$ induced by $\sigma_p$. $\sigma_{p,*}$

acts on $\mathrm{Pic}^0(\tilde{E})$ as $\sigma_p$ and $\sigma_p^*$ acts as $p\sigma_p^{-1}$. By the above diagram $\sigma_p$ acts on $\tilde{E}[\ell^n]$ as $\mathrm{Frob}_{\mathfrak{p}_n}$ acts on $E[\ell^n]$ where $\mathrm{Frob}_{\mathfrak{p}_n}$ is the $n$th component of $\mathrm{Frob}_{\mathfrak{p}}$. Thus $A + pA^{-1} \equiv a_p(E) \mod \ell^n$ for all $n$. Therefore

$$\mathrm{tr}\rho_{E,\ell}(\mathrm{Frob}_{\mathfrak{p}}) = a_p(E).$$

□

It is also true that $\rho_{E,\ell}$ is an irreducible representation but we will not give a proof of this. Galois representations attached to isogenous elliptic curves $E$ and $E'$ are equivalent. To see this, $\varphi : E \to E'$ be an isogeny. Then $\varphi$ 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.

## 5.4 Galois representations and modular forms

The aim of this section is associating Galois representations to modular curves and decompose them into representations attached to modular forms.

Let $N$ be a positive integer and $\ell$ be a prime. We have seen that $X_1(N)$ is a projective nonsingular algebraic curve over $\mathbb{Q}$. Let $g$ be the genus of $X_1(N)$. The Jacobian of the complex curve $X_1(N)_{\mathbb{C}}$ is

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

$\mathrm{Pic}^0(X_1(N))$ 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 Theorem **??**. Thus we have an inclusion of $\ell^n$ torsion

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

By Theorem **??**, $X_1(N)$ has good reduction at $p$ and we have a surjective reduction map $\mathrm{Pic}^0(X_1(N)) \to \mathrm{Pic}^0(\tilde{X}_1(N))$ restricting to $\ell^n$ torsion

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

We state without proof that if a curve $C$ over a field $\mathbf{k}$ has genus $g$ and $N$ is coprime to $\mathrm{char}(\mathbf{k})$ then $\mathrm{Pic}^0(C)[N] \cong (\mathbb{Z}/N\mathbb{Z})^{2g}$ and if $C$ is a curve over $\mathbb{Q}$ has good reduction at a prime $p \nmid N$ then the reduction map is injective on $\mathrm{Pic}^0(C)[N]$. Thus $i_n$ and $\pi_n$ are actually isomorphisms for $p \nmid \ell N$.

The $\ell$-adic Tate module of $X_1(N)$ is

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

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

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

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

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

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

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

Since $\mathbb{Q}(\mathrm{Pic}^0(X_1(N))[\ell^n])/\mathbb{Q}$ is a Galois extension the action of $G_\mathbb{Q}$ restricts to $\mathrm{Pic}^0(X_1(N))[\ell^n]$ and we have the following commutative diagram

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

for all $n$. Thus $G_{\mathbb{Q}}$ acts on $\mathrm{Ta}_\ell(\mathrm{Pic}^0(X_1(N)))$ and this gives a representation

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

One can show similarly to the Galois representation attached to an elliptic curve, $\rho_{X_1(N),\ell}$ is continuous. It is the $2g$-dimensional Galois representation associated to $X_1(N)$. By the diagrams (**??**) and (**??**), the Hecke algebra $\mathbb{T}_{\mathbb{Z}}$ acts on $\mathrm{Pic}^0(X_1(N))$,

$$\mathbb{T}_{\mathbb{Z}} \times \mathrm{Pic}^0(X_1(N)) \to \mathrm{Pic}^0(X_1(N)).$$

This action restricts to $\ell$-power torsion and then extends to $\mathrm{Ta}_\ell(\mathrm{Pic}^0(X_1(N)))$. Since the Hecke action on $\mathrm{Pic}^0(X_1(N))$ is defined over $\mathbb{Q}$, it commutes with the action of $G_{\mathbb{Q}}$. Thus the actions on $\mathrm{Ta}_\ell(\mathrm{Pic}^0(X_1(N)))$ also commute.

**Theorem 5.4.1.** *Let $\ell$ be a prime and $N$ 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 $\mathfrak{p} \subset \overline{\mathbb{Z}}$ be any maximal ideal over $p$. Then $\rho_{X_1(N),\ell}(\mathrm{Frob}_{\mathfrak{p}})$ satisfies the polynomial equation*

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

*Proof.* We have the following commutative diagram

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

The map on the right side is the isomorphism induced by $\pi_n$ from the beginning of this section. Similarly to the proof of Theorem **??**, $I_{\mathfrak{p}} \subset \ker \rho_{X_1(N),\ell}$ and so $\rho_{X_1(N),\ell}$ is unramified at $p$. The Eichler-Shimura relation given in Theorem **??** restricts to

$\ell$-torsion and we have the following commutative diagram,

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

We also have the following commutative diagram

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

Since the vertical maps are isomorphisms $T_p = \mathrm{Frob}_{\mathfrak{p}}+\langle p\rangle p\mathrm{Frob}_{\mathfrak{p}}^{-1}$ on $\mathrm{Pic}^0(X_1(N))[\ell^n]$ for all $n$. Thus they are equal on $\mathrm{Ta}_\ell(\mathrm{Pic}^0(X_1(N)))$. This proves the second part of the theorem. □

Let $f \in \mathcal{S}_2(N,\chi)$. We have defined $\mathcal{O}_f = \mathbb{Z}[\{a_n(f) : n \in \mathbb{Z}^+\}]$. We have the following isomorphism from Section **??**, $T_{\mathbb{Z}}/I_f \xrightarrow{\sim} \mathcal{O}_f$. Under this isomorphism $a_p(f)$ acts on $A_f$ as $T_p$ and $\chi(p)$ acts on $A_f$ as $\langle p\rangle$. The dimension of $A_f$ as a complex torus is the degree $d = [K_f : \mathbb{Q}]$. The Tate module of the Abelian variety is

$$\mathrm{Ta}_\ell(A_f) = \varprojlim_n A_f[\ell^n] \cong \mathbb{Z}_\ell^{2d}.$$

The action of $\mathcal{O}_f$ descends to the $\ell$-power torsion and then extends to $\mathrm{Ta}_\ell(A_f)$.

**Lemma 5.4.1.** *The map* $\mathrm{Pic}^0(X_1(N))[\ell^n] \to A_f[\ell^n]$ *is a surjection. Its kernel is stable under* $G_{\mathbb{Q}}$*.*

*Proof.* Multiplication by $\ell^n$ is surjective on $J_1(N)$. Let $y \in I_f J_1(N)$. Then $y = \sum_i T_i y_i$, $T_i \in I_f$ and $y_i \in J_1(N) = \ell^n J_1(N)$. Thus $y_i = \ell^n x_i$ for some $x_i \in J_1(N)$ for each $i$. Then $y = \sum_i T_i(\ell^n x_i) = \ell^n \sum_i T_i x_i \in \ell^n I_f J_1(N)$. Thus multiplication by $\ell^n$ is surjective on $I_f J_1(N)$.

Let $y \in A_f[\ell^n]$. Then $y = x + I_f J_1(N)$ for some $x \in J_1(N)$ such that $\ell^n x \in I_f J_1(N)$. Thus $\ell^n x = \ell^n x'$ for some $x' \in I_f J_1(N)$. Then $x - x' \in J_1(N)[\ell^n] = \mathrm{Pic}^0(X_1(N))[\ell^n]$ and $x - x' \mapsto y$.

The kernel of the map is $\mathrm{Pic}^0(X_1(N))[\ell^n] \cap I_f J_1(N) = (I_f J_1(N))[\ell^n]$. Clearly we have $(I_f \mathrm{Pic}^0(X_1(N)))[\ell^n] \subset (I_f J_1(N))[\ell^n]$. The reverse inclusion is also true. Indeed, let $\mathcal{S}_2 = \mathcal{S}_2(\Gamma_1(N))$ and $H_1 = H_1(X_1(N)_\mathbb{C}, \mathbb{Z}) \subset \mathcal{S}_2^\wedge$. Thus $J_1(N) = \mathcal{S}_2^\wedge / H_1$ and we have

$$I_f J_1(N) = (I_f \mathcal{S}_2^\wedge + H_1)/H_1 \cong I_f \mathcal{S}_2/(H_1 \cap I_f \mathcal{S}_2^\wedge).$$

$I_f H_1$ is a subgroup of $H_1 \cap I_f \mathcal{S}_2^\wedge$ with some finite index $M$. Thus $M(H_1 \cap I_f \mathcal{S}_2^\wedge) \subset I_f H_1$. Let $y \in (I_f J_1(N))[\ell^n]$. Then $y = x + H_1 \cap I_f \mathcal{S}_2^\wedge$ for some $x \in I_f \mathcal{S}_2$. Since $\ell^n y = 0$, $\ell^n x \in H_1 \cap I_f \mathcal{S}_2^\wedge$. Then $M \ell^n x \in I_f H_1$ and so $x \in I_f(M^{-1} \ell^{-n} H_1)$. Thus $y \in I_f(J_1(N)[M\ell^n]) \subset I_f \mathrm{Pic}^0(X_1(N))$. Since $\ell^n y = 0$, $y \in (I_f \mathrm{Pic}^0(X_1(N)))[\ell^n]$. Since the Hecke action and Galois actions commute, the kernel is stable under $G_\mathbb{Q}$. □

By the above lemma, $G_\mathbb{Q}$ acts on $A_f[\ell^n]$ and therefore acts on $\mathrm{Ta}_\ell(A_f)$. This action commutes with the action of $\mathcal{O}_f$ since the Hecke action and Galois actions on $\mathrm{Ta}_\ell(\mathrm{Pic}^0(X_1(N)))$ commute. Choosing a compatible family of basis we have a Galois representation

$$\rho_{A_f,\ell} : G_\mathbb{Q} \to GL_{2d}(\mathbb{Q}_\ell)$$

This is continuous. To see this let $U(n,g) = \ker(GL_{2g}(\mathbb{Z}_\ell) \to GL_{2g}(\mathbb{Z}/\ell^n\mathbb{Z}))$. By definition of the Galois action on $A_f[\ell^n]$ we have

$$\rho_{X_1(N),\ell}^{-1}(U(n,g)) \subset \rho_{A_f,\ell}^{-1}(U(n,d)).$$

Since $\rho_{X_1(N),\ell}$ is continuous, $\rho_{A_f,\ell}$ is also continuous.

Since $\ker(\rho_{X_1(N),\ell}) \subset \ker(\rho_{A_f,\ell})$, $\rho_{A_f,\ell}$ is unramified at all primes $p \nmid \ell N$. Let $\mathfrak{p} \subset \overline{\mathbb{Z}}$ be a maximal ideal lying over such $p$. Since $T_p$ and $\langle p \rangle$ act on $A_f$ as $a_p(f)$ and $\chi(p)$, respectively, $\rho_{A_f,\ell}(\mathrm{Frob}_{\mathfrak{p}})$ satisfies

$$x^2 - a_p(f)x + \chi(p)p = 0.$$

Before going further we give some definitions. Let $K$ be a number field and $\mathcal{O}_K$ be its ring of integers. For a prime $\ell$ we have the following factorization of $\ell\mathcal{O}_K$ into maximal ideals $\lambda$ of $\mathcal{O}_K$ lying over $\ell$

$$\ell\mathcal{O}_K = \prod_{\lambda|\ell} \lambda^{e_\lambda}.$$

For each $\lambda$ define the ring of $\lambda$-adic integers as

$$\mathcal{O}_{K,\lambda} = \varprojlim_n \mathcal{O}_K/\lambda^n$$

and the field of $\lambda$-adic numbers is the quotient field $K_\lambda$ of $\mathcal{O}_{K,\lambda}$. $\mathbb{Z}_\ell$ may be viewed as a subring of $\mathcal{O}_{K,\lambda}$. To see this, first observe that $\lambda^{ne_\lambda} \cap \mathbb{Z} = \ell^{n'}\mathbb{Z}$ for some $n' \leqslant n$. Since

$$\ell^m \in \lambda^{ne_\lambda} \Leftrightarrow \prod_{\lambda|\ell} \lambda^{me_\lambda} \subset \lambda^{ne_\lambda} \Leftrightarrow m \geqslant n,$$

$n' \geqslant n$. Thus $n = n'$, i.e. $\lambda^{ne_\lambda} \cap \mathbb{Z} = \ell^n\mathbb{Z}$. This shows that the map $\mathbb{Z} \to \mathcal{O}_K/\lambda^{ne_\lambda}$ has kernel $\ell^n\mathbb{Z}$. Thus $\mathbb{Z}/\ell^n\mathbb{Z} \to \mathcal{O}_K/\lambda^{ne_\lambda}$ is an injection for all $n$ and this gives an injection $\mathbb{Z}_\ell \to \mathcal{O}_{K,\lambda}$ for all $\lambda$. Thus $\mathbb{Q}_\ell$ may be viewed as a subfield of $K_\lambda$. The containments $\mathbb{Z}_\ell \subset \mathcal{O}_{K,\lambda}$ and $\mathbb{Q}_\ell \subset K_\lambda$ are equalities when $e_\lambda f_\lambda = 1$ and $[K_\lambda : \mathbb{Q}_\ell] = e_\lambda f_\lambda$. We have the following ring isomorphism

$$K \otimes_{\mathbb{Q}} \mathbb{Q}_\ell = \prod_{\lambda|\ell} K_\lambda. \tag{5.1}$$

To see this first note that

$$\mathcal{O}_K \otimes \mathbb{Z}_\ell \cong \varprojlim_n (\mathcal{O}_K \otimes \mathbb{Z}/\ell^n\mathbb{Z}) \cong \varprojlim_n \mathcal{O}_K/\ell^n\mathcal{O}_K.$$

By Chinese Remainder Theorem, $\mathcal{O}_K/\ell^n\mathcal{O}_K = \mathcal{O}_K/\prod_\lambda \lambda^{ne_\lambda} \cong \prod_\lambda \mathcal{O}_K/\lambda^{ne_\lambda}$. Thus

$$\mathcal{O}_K \otimes \mathbb{Z}_\ell \cong \varprojlim_n (\prod_\lambda \mathcal{O}_K/\lambda^{ne_\lambda}) \cong \prod_\lambda \varprojlim_n \mathcal{O}_K/\lambda^{ne_\lambda} \cong \prod_\lambda \mathcal{O}_{K,\lambda}.$$

Using this we get

$$K \otimes_\mathbb{Q} \mathbb{Q}_\ell \cong \mathcal{O}_K \otimes \mathbb{Q}_\ell \cong \mathcal{O}_K \otimes \mathbb{Z}_\ell \otimes_{\mathbb{Z}_\ell} \mathbb{Q}_\ell \cong \prod_\lambda (\mathcal{O}_{K,\lambda} \otimes_{\mathbb{Z}_\ell} \mathbb{Q}_\ell) \cong \prod_\lambda K_\lambda.$$

The Tate module of $A_f$, $\mathrm{Ta}_\ell(A_f)$ has rank $2d$ over $\mathbb{Z}_\ell$. Since it is also a $\mathcal{O}_f$-module, $V_\ell(A_f) = \mathrm{Ta}_\ell(A_f) \otimes \mathbb{Q}$ is an $\mathcal{O}_f \otimes \mathbb{Q}_\ell = K_f \otimes_\mathbb{Q} \mathbb{Q}_\ell$-module.

**Lemma 5.4.2.** *$V_\ell(A_f)$ is a free module of rank 2 over $K_f \otimes_\mathbb{Q} \mathbb{Q}_\ell$.*

See [**?**] for the proof of this lemma. $G_\mathbb{Q}$ acts on $V_\ell(A_f)$ and this action is $K_f \otimes_\mathbb{Q} \mathbb{Q}_\ell$-linear. By the above lemma $V_\ell(A_f) = (K_f \otimes_\mathbb{Q} \mathbb{Q}_\ell)^2$. Choosing a basis of $V_\ell(A_f)$ we get a homomorphism $G_\mathbb{Q} \to GL_2(K_f \otimes_\mathbb{Q} \mathbb{Q}_\ell)$. By equation (**??**) we have $K_f \otimes_\mathbb{Q} \mathbb{Q}_\ell = \prod_{\lambda|\ell} K_{f,\lambda}$. Thus composing the above homomorphism with the projection maps we get a homomorphism

$$\rho_{f,\lambda} : G_\mathbb{Q} \to GL_2(K_{f,\lambda})$$

for each $\lambda$.

**Theorem 5.4.2.** *Let $f \in \mathcal{S}_2(f, \chi)$ be a normalized eigenform with number field $K_f$. Let $\ell$ be a prime. For each maximal ideal $\lambda \subset \mathcal{O}_{K_f}$ lying over $\ell$ there is a 2-dimensional Galois representation*

$$\rho_{f,\lambda} : G_\mathbb{Q} \to GL_2(K_{f,\lambda})$$

*This representation is unramified at every prime $p \nmid \ell N$. For any such $p$ let $\mathfrak{p} \subset \overline{\mathbb{Z}}$ be any maximal ideal lying over $p$. Then $\rho_{f,\lambda}(\mathrm{Frob}_{\mathfrak{p}})$ satisfies*

$$x^2 - a_p(f)x + \chi(p)p = 0.$$

*Proof.* We have already construct the representation $\rho_{f,\lambda}$ above. We need to check that it is continuous. Let $i : K_f \otimes_{\mathbb{Q}} \mathbb{Q}_\ell \to \prod_{\lambda|\ell} K_{f,\lambda}$ be the isomorphism of (**??**). Let $e_\lambda$ be the element of $K_f \otimes_{\mathbb{Q}} \mathbb{Q}_\ell$ that maps to $(0, \dots, 0, 1_{K_{f,\lambda}}, 0, \dots, 0)$ and $V_{f,\lambda} = e_\lambda V_\ell(A_f)$. $K_{f,\lambda}$ acts on $V_{f,\lambda}$ via $i^{-1}$ and $V_{f,\lambda} = e_\lambda V_\ell(A_f) \cong e_\lambda(K_f \otimes_{\mathbb{Q}} \mathbb{Q}_\ell)^2 \cong K_{f,\lambda}^2$. Thus $V_{f,\lambda}$ is a 2-dimensional vector space over $K_{f,\lambda}$. Let us see that $V_\ell(A_f) = \bigoplus_\lambda V_{f,\lambda}$. Any $v \in V_\ell(A_f)$ can be written as $v = \sum_\lambda e_\lambda v$, so the the sum spans $V_\ell(A_f)$. Suppose $\sum_\lambda e_\lambda v_\lambda = 0$. Applying $e_\lambda$ for each $\lambda$ gives $v_\lambda = 0$ for all $\lambda$. Thus the sum is direct. Since the $G_{\mathbb{Q}}$ action on $V_\ell(A_f)$ commutes with $e_\lambda$, $V_{f,\lambda}$ is invariant under the $G_{\mathbb{Q}}$ action. Let $B$ be the basis that we chose to define $\rho_{f,\lambda}$. Then $e_\lambda B$ is a basis of $V_{f,\lambda}$ over $K_{f,\lambda}$ and $\rho_{f,\lambda}$ is defined by the action of $G_{\mathbb{Q}}$ on $V_{f,\lambda}$. Thus to show that $\rho_{f,\lambda}$ is continuous it suffices to check that the action

$$V_{f,\lambda} \times G_{\mathbb{Q}} \to V_{f,\lambda}$$

is continuous. Viewing $V_{f,\lambda}$ as a vector space over $K_{f,\lambda}$ or over $\mathbb{Q}_\ell$ gives the same topology on $V_{f,\lambda}$. Since $\rho_{A_f,\ell}$ is continuous,

$$V_\ell(A_f) \times G_{\mathbb{Q}} \to V_\ell(A_f)$$

is continuous and $V_{f,\lambda}$ is a $\mathbb{Q}_\ell$-subspace of $V_\ell(A_f)$. Thus viewing $V_{f,\lambda}$ as a $\mathbb{Q}_\ell$-space, $\rho_{f,\lambda}$ is continuous.

Since the action of $G_{\mathbb{Q}}$ on $V_{f,\lambda}$ is defined by the action of $G_{\mathbb{Q}}$ on $V_\ell(A_f)$, $\ker(\rho_{A_f,\ell}) \subset \ker(\rho_{f,\lambda})$. This shows that $\rho_{f,\lambda}$ is unramified for all primes $p \nmid \ell N$. □

The following theorem is a generalization of the above theorem to weights other than 2.

**Theorem 5.4.3.** *Let $f \in \mathcal{S}_k(f, \chi)$ be a normalized eigenform with number field $K_f$. Let $\ell$ be a prime. For each maximal ideal $\lambda \subset \mathcal{O}_{K_f}$ lying over $\ell$ there is an irreducible 2-dimensional Galois representation*

$$\rho_{f,\lambda} : G_{\mathbb{Q}} \to GL_2(K_{f,\lambda})$$

*This representation is unramified at every prime $p \nmid \ell N$. For any such $p$ let $\mathfrak{p} \subset \overline{\mathbb{Z}}$ be any maximal ideal lying over $p$. Then $\rho_{f,\lambda}(\mathrm{Frob}_{\mathfrak{p}})$ satisfies*

$$x^2 - a_p(f)x + \chi(p)p^{k-1} = 0.$$

This theorem is due to Deligne [**?**] for $k > 2$ and due to Deligne and Serre [**?**] for $k = 1$. The characteristic equation shows that $\det \rho_{f,\lambda}(\mathrm{Frob}_{\mathfrak{p}}) = \chi(p)p^{k-1}$. Since det is continuous and $\{\mathrm{Frob}_{\mathfrak{p}}\}$ is dense in $G_{\mathbb{Q}}$, $\det \rho_{f,\lambda} = \chi\chi_\ell^{k-1}$ where $\chi$ is identified with the Galois representation $\rho_\chi$.

## 5.5 Galois representations and Modularity

In this section we state the Modularity Theorem in the language of Galois representations.

**Definition 5.5.1.** *An irreducible Galois representation*

$$\rho : G_{\mathbb{Q}} \to GL_2(\mathbb{Q}_\ell)$$

*such that* $\det \rho = \chi_\ell$ *is modular if 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 $\lambda \subset \mathcal{O}_{K_f}$ lying over $\ell$ and $\rho_{f,\lambda} \sim \rho$.*

An example of an irreducible Galois representation with $\det \rho = \chi_\ell$ is the representation $\rho_{E,\ell}$ for an elliptic curve $E$ over $\mathbb{Q}$. Modularity theorem states that it is in fact modular.

**Theorem 5.5.1.** *Let $E$ be an elliptic curve over $\mathbb{Q}$. Then $\rho_{E,\ell}$ is modular for some $\ell$.*

This is proved for semistable curves in [**?**, **?**] and then for all curves in [**?**]. The next proposition shows that a stronger version of the Modularity theorem is also true.

**Propositon 5.5.1.** *Let $E$ be an elliptic curve over $\mathbb{Q}$. Then if $\rho_{E,\ell}$ is modular for some $\ell$, then $\rho_{E,\ell}$ is modular for all $\ell$.*

*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 $\lambda$ lying over $\ell$ and $\rho_{f,\lambda} \sim \rho_{E,\ell}$. By the characteristic polynomials of $\rho_{f,\lambda}(\mathrm{Frob}_\mathfrak{p})$ and $\rho_{E,\ell}(\mathrm{Frob}_\mathfrak{p})$, $a_p(f) = a_p(E)$ for almost all $p$. Now by Strong Multiplicity One $K_f = \mathbb{Q}$ and so the Galois representation associated to $f$ takes the form $\rho_{f,\ell} : G_\mathbb{Q} \to GL_2(\mathbb{Q}_\ell)$ for all $\ell$. Thus $\rho_{E,\ell} \sim \rho_{f,\ell}$ for all $\ell$ and so $\rho_{E,\ell}$ is modular for all $\ell$. □

To each Galois representation $\rho : G_\mathbb{Q} \to GL_n(\mathbb{C})$ we associate an L-function

$$L(\rho, s) = \prod_{p \text{ unramified}} \det(I - \rho(\mathrm{Frob}_\mathfrak{p})p^{-s})^{-1}$$

This is called Artin L-function. Entirity of this L-function is the conjecture of Artin.

**Conjecture 5.5.1.** *The L-function of any continuous representation*

$$\rho : G_\mathbb{Q} \to GL_n(\mathbb{C})$$

*is an entire function on all $\mathbb{C}$, except possibly at 1.*

This conjecture plays an important role in the proof of the Modularity theorem. The simple pole at $s = 1$ correspond to the trivial representation. In fact the L-function is the Riemann Zeta function in this case. Assume that $\rho$ is odd. If $n = 1$, then any such representation comes from a Dirichlet character $\chi$ as we have seen before. Hence the conjecture is known in this case.

If $n = 2$ the image of $\rho$ followed by the projection $GL_2(\mathbb{C}) \to PGL_2(\mathbb{C})$ in $PGL_2(\mathbb{C})$ is isomorphic to one of the followings: a cyclic group, a dihedral group, $A_4$, $S_4$ and $A_5$. The representation $\rho$ is called cyclic, dihedral, tetrahedral, octahedral or icosahedral according to this image. The proof of the cyclic and dihedral cases can be found in [**?**]. The tetrahedral case is proven by Langlands [**?**] and the octahedral case is proven by Tunnell [**?**]. Finally the case of the unsolvable image $A_5$ is proved by Taylor and others in [**?**, **?**, **?**] under some hypotheses. The case $n = 2$ is completely solved by Khare and Wintenberger in [**?**] where they proved Serre's modularity conjecture.

Let $f \in \mathcal{S}_1(N, \chi)$ be a normalized newform. Then due to Deligne and Serre [**?**] we have a Galois representation $\rho_f : G_{\mathbb{Q}} \to GL_2(\mathbb{C})$. If $f = \sum_{n=1}^{\infty} a_n q^n$, then $L(\rho_f, s) = \sum_{n=1}^{\infty} a_n n^{-s}$ and $\rho$ is irreducible, odd and $L(\rho_f \otimes \chi, s)$ has an analytic continuation to all of $\mathbb{C}$ for all continuous characters $\chi : G_{\mathbb{Q}} \to \mathbb{C}^*$. The following theorem states that the converse is also true. See [**?**].

**Theorem 5.5.2.** *Let $\rho : G_{\mathbb{Q}} \to GL_2(\mathbb{C})$ be an irreducible, odd Galois representation with Artin L-function $L(\rho, s) = \sum_{n=1}^{\infty} a_n n^{-s}$ such that $L(\rho \otimes \chi, s) = \sum_{n=1}^{\infty} \chi(n) a_n n^{-s}$ has an alanytic continuation to all of $\mathbb{C}$ for all continuous characters $\chi : G_{\mathbb{Q}} \to \mathbb{C}^*$, then $f = \sum_{n=1}^{\infty} a_n q^n$ is a normalized newform in $S_1(N, \chi)$ where $\chi = \det \rho$.*

By the above theorem the statement that any irreducible, odd, 2-dimensional Galois representation with finite image is modular is a version of Artin's conjecture.

Theorem **??** and the paragraph preceding it shows that there is a bijection between the set of normalized newforms $f \in \mathcal{S}_1(N, \chi)$ and the isomorphism classes of 2-dimensional representations satisfying the hypotheses of the theorem.

Mod $\ell$ 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 $\ell$. By Proposition **??** we may assume that $\rho_{f,\lambda} : G_{\mathbb{Q}} \to GL_2(\mathcal{O}_{K_f,\lambda})$. Then $\rho_{f,\lambda}$ has a mod $\ell$ reduction

$$\overline{\rho}_{f,\lambda} : G_{\mathbb{Q}} \to GL_2(\mathcal{O}_{K_f,\lambda}/\lambda\mathcal{O}_{K_f,\lambda}).$$

Consider the representations $\overline{\rho} : G_{\mathbb{Q}} \to GL_2(\overline{\mathbb{F}}_\ell)$ where $\overline{\mathbb{F}}_\ell$ has discrete topology.

**Definition 5.5.2.** *An irreducible representation $\overline{\rho} : G_{\mathbb{Q}} \to GL_2(\overline{\mathbb{F}}_\ell)$ is modular of level $M$ if there exists a newform $f \in \mathcal{S}_2(\Gamma_1(M))$ and a maximal ideal $\lambda \subset \mathcal{O}_{K_f}$ lying over $\ell$ such that $\overline{\rho} \sim \overline{\rho}_{f,\lambda}$.*

A modularity conjecture for mod $\ell$ representations due to Serre which is proved by Khare and Wintenberger [**?**] is the following:

**Theorem 5.5.3.** *Let $\overline{\rho} : G_{\mathbb{Q}} \to GL_2(\overline{\mathbb{F}}_\ell)$ be irreducible and odd. Then $\overline{\rho}$ is modular of level $M(\overline{\rho})$.*

$M(\overline{\rho})$ is a minimal level depending on $\overline{\rho}$.

$$M(\overline{\rho}) = \prod_{p \neq \ell} p^{n(p)}$$

where $n(p)$ depends on the ramification of $\overline{\rho}$. In particular, $n(p) = 0$ if and only if $\overline{\rho}$ is unramified at $p$. It is known due to Ribet [**?**] that if $\overline{\rho}$ is modular then $\overline{\rho}$ is modular of level $M(\overline{\rho})$. For more details about Serre's conjecture see [**?**].

Now given a nontrivial solution of the Fermat equation

$$a^\ell + b^\ell + c^\ell = 0$$

Then it gives the following Frey curve

$$E_F : y^2 = x(x - a^\ell)(x + b^\ell).$$

Then it turns out that $M(\overline{\rho}_{E_F,\ell}) = 2$. However $\mathcal{S}_2(\Gamma_1(2)) = \{0\}$ since the corresponding modular curve has genus 0, see [**?**]. This shows that $\overline{\rho}_{E_F,\ell}$ is not modular of level $M(\overline{\rho}_{E_F,\ell})$ and so it is not modular. Thus $\rho_{E_F,\ell}$ is not modular, contradicting the Modularity Theorem. This proves Fermat's Last Theorem.

The proof of the Modularity Theorem due to Wiles starts with any elliptic curve $E$ over $\mathbb{Q}$ and considers the mod 3 representation

$$\overline{\rho}_{E,3} : G_{\mathbb{Q}} \to GL_2(\mathbb{F}_3).$$

Suppose that $\overline{\rho}_{E,3}$ is irreducible. The following proposition shows that $\overline{\rho}_{E,3}$ is modular.

**Proposititon 5.5.2.** *$\overline{\rho}_{E,3}$ is modular in the sense of Definition* **??**.

*Proof.* Let $K = \mathbb{Q}(\sqrt{-2})$. Then $\mathcal{O}_K = \mathbb{Z}[\sqrt{-2}]$. Consider the embedding

$$i : GL_2(\mathbb{F}_3) \to GL_2(\mathbb{Z}[\sqrt{-2}])$$

given by

$$\left(\begin{smallmatrix} -1 & 1 \\ -1 & 0 \end{smallmatrix}\right) \mapsto \left(\begin{smallmatrix} -1 & 1 \\ -1 & 0 \end{smallmatrix}\right), \qquad \left(\begin{smallmatrix} 1 & -1 \\ 1 & 1 \end{smallmatrix}\right) \mapsto \left(\begin{smallmatrix} 1 & -1 \\ -\sqrt{-2} & -1+\sqrt{-2} \end{smallmatrix}\right)$$

The orders of the elements are 3 and 8 respectively hence they generate a subgroup $H$ of $GL_2(\mathbb{F}_3)$ whose order is divisible by 24. Since $PGL_2(\mathbb{F}_3)$ is isomorphic to $S_4$ and the only order 12 subgroup of $S_4$ is $A_4$, $SL_2(\mathbb{F}_3)$ is the only order 24 subgroup of $GL_2(\mathbb{F}_3)$. Since $\left(\begin{smallmatrix} 1 & -1 \\ 1 & 1 \end{smallmatrix}\right) \notin SL_2(\mathbb{F}_3)$, $H = GL_2(\mathbb{F}_3)$. The ideal $\lambda = \langle 1 + \sqrt{-2} \rangle$ is a maximal ideal of $\mathcal{O}_K$ lying over 3. Consider the composition $i \circ \overline{\rho}_{E,3}$. Since $GL_2(\mathbb{F}_3)$ is solvable by Langland's and Tunnell's result, $i \circ \overline{\rho}_{E,3}$ is modular, i.e. there exists a newform $f \in \mathcal{S}_1(M_f, \psi)$ such that $\rho_{f,\lambda} \sim i \circ \overline{\rho}_{E,3}$. As before we may assume that the image of $\rho_{f,\lambda}$ lies in $GL_2(\mathcal{O}_K)$. Since $i$ followed by reduction modulo $\lambda$ is identity, the reduction of $\rho_{f,\lambda}$ modulo $\lambda$, $\overline{\rho}_{f,\lambda}$ is $\overline{\rho}_{E,3}$. Since $\psi = \det \rho_{f,\lambda}$ is a lift of $\det \overline{\rho}_{E,3} = \chi_3 \mod 3$ and this is surjective, $\psi$ is a quadratic character and has conductor 3. Thus $\psi(p) \equiv p \mod \lambda$ for all $p$. Now for $p \nmid 3M_fN_E$ we have modulo $\lambda$

$$a_p(f) \equiv \mathrm{tr}\overline{\rho}_{f,\lambda}(\mathrm{Frob}_{\mathfrak{p}}) = \mathrm{tr}\overline{\rho}_{E,3}(\mathrm{Frob}_{\mathfrak{p}}) \equiv a_p(E).$$

Consider the weight 1 Eisenstein series $E_1^{\psi,\mathbf{1}} \in \mathcal{M}_1(3, \psi)$. Then

$$3E_1^{\psi,\mathbf{1}} = 1 + \sum_{n=1}^{\infty} a_n q^n$$

where $a_n \in 3\mathbb{Z}$. Let $g = 3E_1^{\psi,\mathbf{1}} f$. Then $g \in \mathcal{S}_2(\Gamma_0(3M_f))$ and $f \equiv g \mod \lambda$. Observe that the action of $T_p$ on $\mathcal{S}_1(M_f, \psi)$ and $\mathcal{S}_2(\Gamma_0(M_f))$ are congruent modulo $\lambda$. This is because $\psi(p) \equiv p \mod \lambda$. Thus $T_p g \equiv T_p f = a_p(f) f \mod \lambda$. The right side is equal to $a_p(E)g$ modulo $\lambda$ for all but finitely many $p$ and so $T_p g \equiv a_p(E) g \mod \lambda$. The right side is also equal to $a_p(g)g = a_1(T_p g)g$ modulo $\lambda$ for all $p$ and so $Tg \equiv a_1(Tg)g \mod \lambda$ for all $T \in \mathbb{T}_{\mathbb{Z}}$. Now define the homomorphism

$$\phi : \mathbb{T}_{\mathbb{Z}} \to \mathbb{F}_3, \qquad T \mapsto a_1(Tg) \mod \lambda$$

By the above observations $\phi(T_p) = a_p(E) \mod 3$ and $\phi(\langle p \rangle) = 1$ for all but finitely many $p$.

Let $m = \ker \phi$ and $P$ be a minimal prime ideal contained in $m$. Since $\mathbb{T}_{\mathbb{Z}}$ is a finitely generated $\mathbb{Z}$-module, $\mathbb{T}_{\mathbb{Z}}/P$ is an integral domain which is finitely generated $\mathbb{Z}$-module. Since $\mathbb{T}_{\mathbb{Z}}$ is a free module over $\mathbb{Z}$ no rational prime $p$ is a zero divisor in $\mathbb{T}_{\mathbb{Z}}$ and so no rational prime is contained in $P$ as $P$ is a subset of the set of zero divisors. Therefore $\mathbb{Z}$ is contained in $\mathbb{T}_{\mathbb{Z}}/P$ and so $\mathbb{T}_{\mathbb{Z}}/P$ has characteristic zero. Its field of quotients is a number field $K'$ and $\mathbb{T}_{\mathbb{Z}}/P$ is contained in the ring of integers $\mathcal{O}_{K'}$. Hence there is a homomorphism

$$\phi' : \mathbb{T}_{\mathbb{Z}} \to \mathcal{O}_{K'}.$$

Let $\lambda'$ be a maximal ideal of $\mathcal{O}_{K'}$ containing $\phi'(m)$. We have seen that for all but finitely many primes $p$, $\phi(T_p) \equiv a_p(E) \mod \lambda$. Hence $T_p - a_p(E) \in \ker \phi = m$ and so $\phi'(T_p) - a_p(E) \in \phi'(m) \subset \lambda'$. Thus $\phi'(T_p) \equiv a_p(E) \mod \lambda'$ for all but finitely many primes $p$. Similarly $\phi'(\langle p \rangle) \equiv 1 \mod \lambda'$.

Note that we have an isomorphism

$$\pi : \mathbb{T}_{\mathbb{Z}} \otimes \mathbb{C} \xrightarrow{\sim} \mathbb{T}_{\mathbb{C}}, \qquad \sum_i T_i \otimes z_i \mapsto \sum_i z_i T_i.$$

Using this identification we may extend $\phi'$ to a homomorphism $\phi' : \mathbb{T}_{\mathbb{C}} \to \mathbb{C}$ given by $\phi'(\sum_i T_i \otimes z_i) = \sum_i z_i \phi'(T_i)$. By the pairing from Section **??**, there exists an eigenform $g' \in \mathcal{S}_2(\Gamma_0(3M_f))$ with coefficients in $\mathcal{O}_{K'}$ such that

$$\phi'(T) = a_1(Tg'), \qquad T \in \mathbb{T}_{\mathbb{Z}}.$$

Compute that $a_p(g') = a_1(T_p g') = \phi'(T_p) \equiv a_p(E) \mod \lambda'$ and $\chi_{g'}(p) \equiv 1 \mod \lambda'$ for all but finitely many $p$.

By Proposition **??** there exists a newform $g''$ of level dividing $3M_f$ associated to $g'$ such that $a_p(g'') = a_p(g')$ for all $p \nmid 3M_f$. Let $L$ be a finite Galois extension of $\mathbb{Q}$ such that $K_{g'}$ and $K_{g''}$ are contained in $L$. Let $\sigma \in \mathrm{Gal}(L/\mathbb{Q})$. Then $(g'')^\sigma$ is the newform associated to $(g')^\sigma$. Hence if $\sigma$ fixes $K_{g'}$ then it fixes $K_{g''}$. Thus $K_{g''} \subset K_{g'}$. Let $\lambda'' = K_{g''} \cap \lambda'$. Then $a_p(g'') \equiv a_p(E) \mod \lambda''$ for all but finitely many $p$. This shows that characteristic polynomials of $\overline{\rho}_{g'',\lambda''}$ and $\overline{\rho}_{E,3}$ are the same making them equivalent. Thus $\overline{\rho}_{E,3}$ is modular. $\square$

Note that the modularity of $\overline{\rho}_{E,3}$ also follows from Theorem **??**. After that the proof shows the following modularity lifting result: under some hypotheses, for any representation $\rho : G_{\mathbb{Q}} \to GL_2(\mathbb{Z}_\ell)$ with mod $\ell$ reduction $\overline{\rho}$, if $\overline{\rho}$ is modular, then $\rho$ is modular. We will explain the method of the proof of this later. The hypotheses apply when $E$ s semistable and $\rho = \rho_{E,3}$. Thus $\rho_{E,3}$ is modular.

Note that we have assumed that $\overline{\rho}_{E,3}$ is irreducible. If it is not irreducible, the proof use $\overline{\rho}_{E,5}$ and show that for any semistable elliptic curve E one of $\overline{\rho}_{E,3}$ or $\overline{\rho}_{E,5}$ is modular.

Now we will briefly explain the method of proving the modularity lifting theorem. In order to prove the modularity lifting result Wiles used the deformation theory of Galois representations which is introduced by Mazur in [**?**]. We first give some background of the subject.

A complete noetherian local ring with finite residue field of characteristic $p$ is called a coefficient ring. Let $A$ be a coefficient ring with maximal ideal $m_A$ and $k_A = A/m_A$. Let $\rho : G_{\mathbb{Q}} \to GL_2(A)$ be a Galois representation. The residual representation of $\rho$ is the representation $\overline{\rho} : G_{\mathbb{Q}} \to GL_2(k_A)$ obtained by composing $\rho$ with $GL_2(A) \to GL_2(k_A)$.

Given a Galois representation $\rho_0 : G_{\mathbb{Q}} \to GL_2(k)$. A Galois representation $\rho : G_{\mathbb{Q}} \to GL_2(A)$ is said to be a lift of $\rho_0$ if $k = k_A$ and $\overline{\rho} = \rho_0$. Two lifts $\rho, \rho'$ of $\rho_0$ are said to be equivalent if $\rho = M\rho' M^{-1}$ for some $M \in \ker(GL_2(A) \to GL_2(k))$. A deformation of $\rho_0$ to $A$ is an equivalence class of liftings of $\rho_0$ to $A$.

Let $\mathcal{C}$ be the category of coefficient rings where the morphisms are local homomorphisms inducing identity on $k$. Consider the deformation functor $\mathcal{D}$ from $\mathcal{C}$ to the category of sets,

$$\mathcal{D} : \mathcal{C} \to SETS, \qquad R \mapsto \{\text{deformations of } \rho_0 \text{ to } R\}$$

This functor is representable. i.e. there exists a coefficient ring $\mathcal{R} = \mathcal{R}(\rho_0)$ such that $\mathcal{D}(R) = \mathrm{Hom}_{\mathcal{C}}(\mathcal{R}, R)$ for any $R \in \mathrm{Obj}(\mathcal{C})$. $\mathcal{R}$ is called the universal deformation ring of $\rho_0$. The deformation $\rho_{\mathrm{univ}} : G_{\mathbb{Q}} \to GL_2(\mathcal{R})$ that corresponds to the identity homomorphism $\mathrm{id}_{\mathcal{R}} \in \mathrm{Hom}(\mathcal{R}, \mathcal{R})$ is called the universal deformation of $\rho_0$. $\mathcal{R}$ together with $\rho_{\mathrm{univ}}$ satisfy the following universal property: Given a deformation $\rho$ of $\rho_0$ to $R$. Then there exists a morphism $\varphi : \mathcal{R} \to R$ such that the following diagram commutes,

$$\begin{tikzcd}
G_{\mathbb{Q}} \arrow[rr, "\rho"] \arrow[dr, "\rho_{\mathrm{univ}}"'] & & GL_2(R) \\
& GL_2(\mathcal{R}) \arrow[ur, "\varphi"'] &
\end{tikzcd}$$

One might want to consider the deformations that satisfy certain property. This can be done by imposing deformation conditions to the deformation functor. By this way one gets another functor. Given a condition $\mathcal{P}$. Then we can define

$$\mathcal{D}_{\mathcal{P}} : \mathcal{C} \to SETS, \qquad R \mapsto \{\text{deformations of } \rho_0 \text{ to } R \text{ satisfying our condition } \mathcal{P}\}$$

We want that this functor will be a subfunctor of $\mathcal{D}$ and representable whenever $\mathcal{D}$ is. The conditions that satisfy these are called deformation conditions. For the definition and details see [**?**]. An example of such a condition is to consider the deformations that have a fixed determinant. The Galois representations that are coming from Elliptic curves has determinant equal to the cyclotomic character. Hence to show that an elliptic curve is modular it suffices to consider the deformations with determinant equal to cyclotomic character.

Another example of such a condition is to consider deformations that are ordinary at p.

**Definition 5.5.3.** *Let $R \in \mathrm{Obj}(\mathcal{C})$, $G$ be a profinite group and $I \subset G$ be a closed subgroup. Let $\rho : G \to GL_2(R)$ be a representation and $M = R \times R$. We say that*

*$\rho$ is $I$-ordinary if the $R$-submodule $M^I \subset M$ is free of rank 1 over $R$ and a direct summand of $M$. $\rho$ is said to be ordinary at $p$ if $I = I_p$.*

The functor $\mathcal{D}^0(R) = \{$deformations to R which are ordinary at $p\}$ is representable and the representing object is called the universal ordinary deformation ring.

Note that Serre's conjecture implies that any irreducible odd 2-dimensional representation $\overline{\rho} : G_{\mathbb{Q}} \to GL_2(k)$ is attached to a modular form. Hence one can ask whether the deformations are modular too. It turns out that if one does not impose deformation conditions or extend the meaning of being modular this is not true.

Let $\overline{\rho} : G_{\mathbb{Q}} \to GL_2(k)$ be a residual representation. Assume that $\overline{\rho}$ satisfies the following hypotheses:

1. $\overline{\rho}$ has determinant equal to $\chi_p$.

2. $\overline{\rho}$ is absolutely irreducible.

3. $\overline{\rho}$ is semistable at every prime $\ell$: for $\ell = p$, $\overline{\rho}$ is either flat at $p$ or ordinary at $p$ and for $\ell \neq p$, $\overline{\rho}|_{I_\ell} = \left(\begin{smallmatrix} 1 & * \\ 0 & 1 \end{smallmatrix}\right)$.

4. $\overline{\rho}$ is modular.

Let $S = \{\ell \neq p : \overline{\rho}$ is ramified at $\ell\}$. Let $\Sigma$ be a set of primes distinct from $S$. We say that a deformation $\rho$ of $\overline{\rho}$ is of type $\mathcal{P}$ if it satisfies the following conditions:

1. $\rho$ has determinant $\chi_p$.

2. $\rho$ is unramified outside $S \cup \{p\} \cup \Sigma$.

3. $\rho$ is semistable outside $\Sigma$.

4. If $p \notin \Sigma$ and $\overline{\rho}$ is flat at $p$ then $\rho$ is flat at $p$.

As we have explained above $\mathcal{P}$ gives a universal deformation ring $\mathcal{R}_{\mathcal{P}}$ and a universal deformation

$$\rho_{\mathcal{P}} : G_{\mathbb{Q}} \to GL_2(\mathcal{R}_{\mathcal{P}})$$

such that $\rho_{\mathcal{P}}$ satisfies the following universal property: For every deformation $\rho : G_{\mathbb{Q}} \to GL_2(R)$ of $\overline{\rho}$ to $R$ of type $\mathcal{P}$ there exists a unique homomorphism $\mathcal{R}_{\mathcal{P}} \to R$ such that the following diagram commutes,

$$\begin{tikzcd}
G_{\mathbb{Q}} \arrow[rr, "\rho"] \arrow[dr, "\rho_{\mathcal{P}}"'] & & GL_2(R) \\
& GL_2(\mathcal{R}_{\mathcal{P}}) \arrow[ur] &
\end{tikzcd}$$

The aim is to control the deformations which are modular hence we need to find a way of parametrizing the modular deformations. At this point Wiles defines a coefficient ring $T_{\mathcal{P}}$, the universal modular deformation ring and a universal modular deformation

$$\rho_{\mathcal{P},\text{mod}} : G_{\mathbb{Q}} \to GL_2(T_{\mathcal{P}})$$

of $\overline{\rho}$. $\rho_{\mathcal{P},\text{mod}}$ satisfies a similar universal property as above: For every modular deformation $\rho : G_{\mathbb{Q}} \to GL_2(R)$, there exists a unique homomorphism $T_{\mathcal{P}} \to R$ such that the following diagram commutes,

$$\begin{tikzcd}
G_{\mathbb{Q}} \arrow[rr, "\rho"] \arrow[dr, "\rho_{\mathcal{P},\text{mod}}"'] & & GL_2(R) \\
& GL_2(T_{\mathcal{P}}) \arrow[ur] &
\end{tikzcd}$$

$T_{\mathcal{P}}$ is the completed Hecke algebra. Now by the universal property of $\mathcal{R}_{\mathcal{P}}$ there exists a unique homomorphism $\varphi : \mathcal{R}_{\mathcal{P}} \to T_{\mathcal{P}}$ such that $\varphi_{\mathcal{P}} \circ \rho_{\mathcal{P}} = \rho_{\mathcal{P},\text{mod}}$. Wiles's main theorem states that $\varphi$ is an isomorphism. This proves that any deformation of type $\mathcal{P}$ is modular.

# References

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

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

[3] F. Diamond, J. Shurman *A First Course in Modular Forms* Springer, 2005.

[4] Gareth A. Jones, D. Singerman *Complex Functions: An Algebraic and Geometric Viewpoint* Cambridge University Press, 1987.

[5] R. Miranda, *Algebraic Curves and Riemann Surfaces* Americam Mathematical Soc., 1995.

[6] Hershek M. Farkas, I. Kra, *Riemann Surfaces* Springer, 1992.

[7] Joseph H. Silverman, *Arithmetic of Elliptic Curves* Springer, 2009.

[8] A. Wiles. *Modular elliptic curves and Fermat's last theorem. Ann. of Math.*, 141(3):443-551, 1995.

[9] R. Taylor, A. Wiles. *Ring theoretic properties of certain Hecke algebras. Ann. of Math.*, 141(3):553-572, 1995.

[10] C. Beruil, B. Conrad, F. Diamond, R. Taylor. *On the modularity of elliptic curves over $\mathbb{Q}$: wild 3-adic exercises. J. Amer. Math. Soc.*, 14(4):843-939, 2001.

[11] P. Deligne. *Forms modulaires et representations $\ell$-adiques. Lecture Notes in Math.*, volume 179, pages 139-172. Springer-Verlag, 1971.

[12] P. Deligne, J.-P. Serre. *Formes modulaires de poids 1. Ann. Sci. Ecole Norm. Sup.*, 7:507Ğ530, 1975.

[13] Rogawski, J. *Functoriality and the Artin conjecture. Proc. Symp. Pure Math.,* 61, Amer. Math. Soc., Providence, RI, 1997.

[14] R. P. Langlands. *Base change for* GL(2), *Annals of Math. Studies.* Princeton Univ. Press, 1980.

[15] J. Tunnell. *Artin's conjecture for representations of the octahedral type. Bull. Amer. Math. Soc.,* 5:173-175, 1981.

[16] R. Taylor. *On icosahedral representations, II. Amer. J. Math.,* 125(3):549-566, 2003.

[17] K. Buzzard, M. Dickinson, N. Shepard-Barron, R. Taylor. *On icosahedral Artin representations. Duke Math. J.,* 109(2):283-318, 2001.

[18] K. Buzzard, R. Taylor. *Companion forms and weight one forms. Ann. of Math.* 149(2):905-919, 1999

[19] C. Khare, J.-P. Wintenberger. *Serre's modularity conjecture. Proceedings of the International Congress of Mathematicians.* Volume II, 280Ğ293, Hindustan Book Agency, New Delhi, 2010.

[20] J.-P. Serre. *Modular forms of weight one and galois representations.* Algebraic number fields: L-functions and Galois properties (Proc. Sympos., Univ. Durham, Durham, 1975), pp. 193Ğ268. Academic Press, London, 1977.

[21] K. Ribet. *On modular representations of* $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ *arising from modular forms. Invent. Math.*, 100:431-476, 1990.

[22] K. Ribet, W. Stein. *Lectures on Serre's conjectures.* Arithmetic algebraic geometry (Park City, UT, 1999), 143Ğ232, IAS/Park City Math. Ser., 9, Amer. Math. Soc., Providence, RI, 2001.

[23] B. Mazur. *Deforming Galois representations Galois groups over* $\mathbb{Q}$, (Berkeley, CA, 1987), 385-437.

[24] F. Q. Gouvea. *Deformations of Galois representations*, Arithmetic Algebraic Geometry (IAS Park City Mathematics)