Universität Regensburg - Università degli Studi di Padova

Fakultät für Mathematik - Dipartimento di Matematica

ALGANT Master Program

The Herbrand-Ribet Theorem

Candidate:
Chiara Sabadin
2003562

Supervisors:
Prof. Dr. Guido Kings
Prof. Remke Kloosterman

July 2022

Acknowledgments

I would like to thank the ALGANT consortium that allowed me to join the ALGANT program. It has been an incredible, thrilling, challenging and awesome experience that has allowed me to get to know different approaches into my beloved math. I met lots of new people and new cultures, an incredibly joyful human experience.
I would like to thank in particular Universität Regensburg and Università di Padova and their always helpful and expert staffs and professors. They made me always feeling home.

I would strongly thank my supervisor Professor Guido Kings, he has always followed me and my studies with authentic interest and constant math discussions. His wide math knowledge and life experience continues inspiring me everyday.

I would like to thank my ALGANT companions, in particular Ludovico, Hari, Pier, Elena, Giacomo, Angela. It has been a pleasure being able to talk about math and life in such a beautiful and easy way. Thanks also to Roberto Gualdi, whose ALGANT and math experience has helped me with my choices.

Vorrei ringraziare i miei compagni di Padova che, dal primo anno, mi hanno accompagnato ogni giorno rendendo gli anni universitari pieni di bei ricordi.
Grazie a Giacomo, con cui parlare di ogni argomento è sempre stato spontaneo, con te si cresce sempre. Grazie a Sara, Alessia e Irene, siete le sorelle che non ho mai avuto. Grazie agli amici veneziani Elena, Marco e Venice, dimostrate che non importa essere nella stessa città per essere vicini. Grazie a Giovanni, hai reso la fatica un immenso piacere, ne varrai sempre la pena. Danke fürs gemeinsame Kochen, unterschiedliche Sprachen, aber in der Freundschaft vereint. Grazie a mamma, papà, Giacomo, Giorgio, Nicola e tutta la mia famiglia, siete sempre il mio porto sicuro. Grazie a tutte le persone che ci sono state, se ne sono andate o sono rimaste, avete contribuito a rendere la mia vita uno spettacolo. Grazie a tutte le persone che mi hanno insegnato cosa significa l'impegno, l'onestà, la semplicità e la bontà. Prima o poi riuscirò a mettere in pratica questi insegnamenti.
Grazie a Chi mi ha donato tutto quello che ho e sono, grazie per quello che verrà.

Contents

Introduction

The aim of this thesis is to give an exhaustive explanation of the paper "A modular construction of unramified p-extensions of $\mathbb{Q}(\mu_p)$" by Kenneth A. Ribet [19].
Let us consider the cyclotomic extension $\mathbb{Q}(\mu_p)$ of $\mathbb{Q}$ for μ_p a primitive p-th root of unity, p an odd prime. Recall that the class number of $\mathbb{Q}(\mu_p)$ is the (finite) number of ideal classes $[I]_\sim$ for I a fractional ideal in $\mathbb{Q}(\mu_p)$ (where $I \sim J$ if, and only if, there exist non-zero $a, b \in \mathbb{Q}(\mu_p)$ such that $(a)I = (b)J$). We say that p is *irregular* if p divides the class number of $\mathbb{Q}(\mu_p)$. An important criterion, due to Kummer, states that p is irregular if, and only if, there exists an even integer k, $2 \leq k \leq p-3$, such that $p \mid B_k$ where B_k is the k-th Bernoulli number defined by

$$\frac{x}{e^x - 1} + \frac{x}{2} - 1 = \sum_{n \geq 2} \frac{B_n}{n!} x^n.$$

The aim of Ribet's paper is to give a stronger version of the Kummer's criterion involving the Galois representation of $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ over the $\mathbb{F}_p$-vector space A/A^p for A the ideal class group of $\mathbb{Q}(\mu_p)$. To prove this criterion we will show that, given a particular representation, the criterion is proved and then we will construct such a particular representation using tools of arithmetic geometry. In Chapter 1, after stating the stronger version of Kummer's criterion, we state two theorems: the first one is equivalent to the criterion and involves unramified p-extension of $\mathbb{Q}(\mu_p)$ while the second, and main one, deals with Galois representations. We prove that the last one implies Kummer's criterion and we use all the remaining of the thesis for the proof of this main theorem. In Chapter 2 we begin studying the properties of reductions of reducible representations while in Chapter 3 we will study particular Eisenstein series that are congruent to some cusp forms. Then such a cusp form defined in Chapter 3 will be used in Chapter 4 to construct, via the Shimura variety attached to it, the Galois representation required in the main theorem of Chapter 1. Finally, in Chapter 5 we end the proof of such a theorem. All the needing tools used in these chapters are stated in the two appendices at the end of this thesis.

Chapter 1

A stronger version of the Kummer's criterion

Let us consider the (finite) ideal class group A of the cyclotomic field $\mathbb{Q}(\mu_p)$ and let us define C to be the $\mathbb{F}_p$-vector space A/A^p such that $\dim_{\mathbb{F}_p} C = p$-rank of A. Let us notice that the Galois group $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ acts on the vector space C via the Galois group $\Delta = \mathrm{Gal}(\mathbb{Q}(\mu_p)/\mathbb{Q})$, then consider the Galois representation

$$\rho : \Delta = \mathrm{Gal}(\mathbb{Q}(\mu_p)/\mathbb{Q}) \to \mathrm{GL}(C)$$

and the standard cyclotomic character

$$\chi : \Delta \to \mathbb{F}_p^* \text{ given by } \sigma \mapsto \chi(\sigma)$$

where $\sigma(\mu_p) = \mu_p^{\chi(\sigma)}$. Then, since all characters of Δ are powers of the standard character χ, χ generates the character group of Δ. Hence we may notice that, since $\Delta \cong (\mathbb{Z}/p\,\mathbb{Z})^*$, $|\Delta| = p-1$ is coprime with the characteristic p of $\mathbb{F}_p$ then, by Maschke's Theorem ([11] Corollary 1.6), we have that C may be written in a canonical way as the direct sum

$$C = \bigoplus_{i \bmod p-1} C(\chi^i)$$

where $C(\chi^i) = \{c \in C \mid \sigma(c) = \chi^i(\sigma)(c) \text{ for every } \sigma \in \Delta\}$.

Let us now state the stronger version of the Kummer 's criterion.

Theorem 1.1. *Let k be an even integer such that $2 \leq k \leq p-3$. Then $p \mid B_k$ if, and only if, $C(\chi^{1-k}) \neq 0$.*

The statement $C(\chi^{1-k}) \neq 0$ implies $p \mid B_k$ is known as Herbrand's Theorem and its proof, that we are now going to show, does not involve any further construction.

DEFINITION 1.2. Let $\chi : (\mathbb{Z}/n\mathbb{Z})^* \to \mathbb{C}$ be a Dirichlet character and $f \in \mathbb{Z}_{\geq 0}$ be the conductor of χ (i.e. the smallest positive integer such that χ factors through $(\mathbb{Z}/f\mathbb{Z})^*$). For $n \geq 0$, let us define the generalized Bernoulli numbers $B_{n,\chi}$ by

$$\sum_{a=1}^{f} \frac{\chi(a) x e^{ax}}{e^{fx} - 1} = \sum_{n=0}^{\infty} B_{n,\chi} \frac{x^n}{n!}$$

Lemma 1.3 ([23] (Corollary 5.15))**.** *Let χ be the standard cyclotomic character and let n be an odd integer, $n \not\equiv -1 \pmod{p-1}$. Then the following equivalence holds*

$$B_{1,\chi^n} \equiv \frac{B_{n+1}}{n+1} \ mod\ p.$$

Proof (of Herbrand's Theorem). Let us consider the generalized Bernoulli number $B_{1,\chi^{k-1}}$ then, by [15] Theorem 2.3, we have that $B_{1,\chi^{k-1}}$ annihilates $C(\chi^{1-k})$ [1]. Now, by Lemma 1.3, we have that

$$B_{1,\chi^{k-1}} \equiv \frac{B_k}{k} \bmod p$$

then, if $p \nmid B_k$, we obtain that $B_{1,\chi^{k-1}} \equiv a \pmod{p}$ for some $a \in \mathbb{F}_p^*$ and so $C(\chi^{1-k}) = 0$. □

The main purpose of this paper is to prove the converse statement of the Herbrand's Theorem but, instead of proving it directly, we will prove an equivalent theorem.

Theorem 1.4. *Let $p \mid B_k$. Then there exists a Galois extension $E/\mathbb{Q}$ containing $\mathbb{Q}(\mu_p)$ such that:*

1. *The extension $E/\mathbb{Q}(\mu_p)$ is unramified;*
2. *The group $H = \mathrm{Gal}(E/\mathbb{Q}(\mu_p))$ is a non-zero abelian group of type $(p, \ldots, p)$;*
3. *If $\sigma \in G = \mathrm{Gal}(E/\mathbb{Q})$, $\tau \in H$, then $\sigma\tau\sigma^{-1} = \chi(\sigma)^{1-k}\tau$.*

Let us now show the equivalence between Theorem 1.1 and Theorem 1.4.

Proof. Let us show that 1. and 2. of Theorem 1.4 are equivalent to $C \neq 0$.
By definition of the Hilbert class field of $\mathbb{Q}(\mu_p)$ we have that it is the maximal unramified abelian extension E of $\mathbb{Q}(\mu_p)$ such that $\mathrm{Gal}(E/\mathbb{Q}(\mu_p)) \cong A$, where A is the ideal class group. Then the Artin map $A \to \mathrm{Gal}(E/\mathbb{Q}(\mu_p))$ is obviously an isomorphism. Let us now prove that 3 is equivalent to $C(\chi^{1-k}) \neq 0$.
($\Rightarrow$) Let us consider the tower $E/\mathbb{Q}(\mu_p)/\mathbb{Q}$ of field extensions where, by assumption, $E/\mathbb{Q}$ is a Galois extension and $E/\mathbb{Q}(\mu_p)$ is an unramified abelian extension. Then there is a well-known ([22], Theorem 11.5) functoriality formula for the Artin symbol

$$\left[\frac{E/\mathbb{Q}(\mu_p)}{\cdot}\right] : A \to \mathrm{Gal}(E/\mathbb{Q}(\mu_p))$$

[1] That means that $B_{1,\chi^{k-1}} C(\chi^{1-k}) = 0$.

given by

$$\sigma \left[\frac{E/\mathbb{Q}(\mu_p)}{a} \right] \sigma^{-1} = \left[\frac{E/\mathbb{Q}(\mu_p)}{\sigma a} \right] \tag{1.1}$$

where a is a fractional ideal of $\mathbb{Q}(\mu_p)$, $\sigma \in \mathrm{Gal}(E/\mathbb{Q})$. Let us consider $\tau \in \mathrm{Gal}(E/\mathbb{Q}(\mu_p))$ and let H be the Hilbert class field of $\mathbb{Q}(\mu_p)$ then the Artin symbol for $E/\mathbb{Q}(\mu_p)$ is a quotient of the Artin symbol for $H/\mathbb{Q}(\mu_p)$ and hence it is surjective. Therefore there exists a fractional ideal a of $\mathbb{Q}(\mu_p)$ such that

$$\left[\frac{E/\mathbb{Q}(\mu_p)}{a} \right] = \tau.$$

By 3 we have that there exists k such that

$$\sigma\tau\sigma^{-1} = \chi^{1-k}(\sigma)\tau$$

then, by (1.1), we have

$$\begin{aligned} \left[\frac{E/\mathbb{Q}(\mu_p)}{\sigma a} \right] &= \sigma\tau\sigma^{-1} \\ &= \chi^{1-k}(\sigma)\tau \\ &= \chi^{1-k}(\sigma) \left[\frac{E/\mathbb{Q}(\mu_p)}{a} \right] \\ &= \left[\frac{E/\mathbb{Q}(\mu_p)}{\chi^{1-k}(\sigma)a} \right] \end{aligned}$$

Then $\chi^{1-k}(\sigma)a$ belongs to the same ideal class of σa modulo the kernel of the Artin symbol that is A^p. Then we obtain that $C(\chi^{1-k}) \neq 0$.
($\Leftarrow$) Let us assume that $C(\chi^{1-k}) \neq 0$ then there exists a fractional ideal a of $\mathbb{Q}(\mu_p)$ such that $\sigma a = \chi^{1-k}(\sigma)a$ for every $\sigma \in G$ then, we have that

$$\left[\frac{E/\mathbb{Q}(\mu_p)}{\sigma a} \right] = \left[\frac{E/\mathbb{Q}(\mu_p)}{\chi^{1-k}(\sigma)a} \right]$$

and so, setting again $\tau = \left[\frac{E/\mathbb{Q}(\mu_p)}{a} \right]$, we obtain using (1.1), that $\sigma\tau\sigma^{-1} = \chi^{1-k}(\sigma)\tau$. □

Now, instead of proving Theorem 1.4, we will state (and then prove in the remaining part of the paper) a Theorem involving Galois representations that implies 1.4.

Theorem 1.5. *Let $p \mid B_k$. Then there exists a finite field $\mathbb{F} \supseteq \mathbb{F}_p$ and a continuous representation*

$$\overline{\rho} : \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \to \mathrm{GL}_2(\mathbb{F})$$

such that:

i. $\overline{\rho}$ *is unramified at all primes* $l \neq p$*;*

ii. The representation $\overline{\rho}$ *is reducible over* $\mathbb{F}$ *such that it is isomorphic to a representation of the form* $\begin{pmatrix} 1 & * \\ 0 & \chi^{k-1} \end{pmatrix}$ *i.e.* $\overline{\rho}$ *is an extension of the* 1*-dimensional representation with character* χ^{k-1} *by the trivial* 1*-dimensional representation;*

iii. The image of $\overline{\rho}$ *has order divisible by* p *i.e.* $\overline{\rho}$ *is not diagonalizable;*

iv. Let D_p *be a decomposition group for* p *in* $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$*, then* $\overline{\rho}(D_p)$ *has order prime to* p *i.e.* $\overline{\rho}|D_p$ *is diagonalizable.*

Let us now prove that this Theorem implies Theorem 1.4 where we substitute $\mathbb{Q}(\mu_p)$ with its subfield $\mathbb{Q}(\mu_p^{1-k})$ of degree $(p-1)/(p-1,k-1)$ that is fixed by $\ker \chi^{1-k}$.Then this version of Theorem 1.4 obviously will imply the initial version of it.

Proof. • Let us show that there exists a Galois extension $E/\mathbb{Q}$ containing $\mathbb{Q}(\mu_p^{1-k})$. Since $\ker \overline{\rho}$ is an open in $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$, then, by definition of Krull topology, $\ker \overline{\rho}$ contains $\mathrm{Gal}(\overline{\mathbb{Q}}/E)$ for $E/\mathbb{Q}$ a Galois extension. Then we may write $\overline{\rho} : \mathrm{Gal}(E/\mathbb{Q}) \hookrightarrow \mathrm{GL}_2(\mathbb{F}_p)$ with $\chi : \mathrm{Gal}(E/\mathbb{Q}) \hookrightarrow \mathbb{F}_p$ factoring through $\Delta = \mathrm{Gal}(\mathbb{Q}(\mu_p)/\mathbb{Q})$ and so, by ii), $\mathbb{Q}(\mu_p^{1-k}) \subseteq E$.

- Let us show that $E/\mathbb{Q}(\mu_p^{1-k})$ is Galois. Let $\sigma \in \mathrm{Gal}(E/\mathbb{Q})$ such that σ fixes $\mathbb{Q}(\mu_p^{1-k})$. Then

$$\overline{\rho}(\sigma) = \begin{pmatrix} 1 & * \\ 0 & \chi^{k-1} \end{pmatrix}(\sigma) = \begin{pmatrix} 1 & * \\ 0 & \chi^{k-1}(\sigma) \end{pmatrix} = \begin{pmatrix} 1 & * \\ 0 & 1 \end{pmatrix}$$

  where we use that $\chi^{k-1} = \overline{\chi^{1-k}}$ and that the fixed field of $\ker \chi^{1-k}$ is $\mathbb{Q}(\mu_p^{1-k})$. Then, since the matrices of the type $\begin{pmatrix} 1 & * \\ 0 & 1 \end{pmatrix}$ form a normal subgroup of $\overline{\rho}(\mathrm{Gal}(E/\mathbb{Q}))$, we have that $E/\mathbb{Q}(\mu_p^{1-k})$ is a Galois extension. Moreover, $\mathrm{Gal}(E/\mathbb{Q}(\mu_p^{1-k}))$ is obviously abelian.

- Let us show that $E/\mathbb{Q}(\mu_p^{1-k})$ has type $(p,\dots,p)$. Indeed, the elements $\begin{pmatrix} 1 & * \\ 0 & 1 \end{pmatrix}$ of $\overline{\rho}(\mathrm{Gal}(E/\mathbb{Q}(\mu_p^{1-k})))$ are such that

$$\begin{pmatrix} 1 & * \\ 0 & 1 \end{pmatrix}^p = \begin{pmatrix} 1 & p* \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}.$$

- Let us show that $E/\mathbb{Q}(\mu_p^{1-k})$ is non trivial. By iii) we have that $\overline{\rho}$ has image of order divisible by p then there exists a matrix of order p, then, as $\mathrm{Gal}(\mathbb{Q}(\mu_p^{1-k})/\mathbb{Q})$ has order $(p-1)/(p-1,k-1)$ coprime to p, we have that the matrices of order p belong to $\overline{\rho}(\mathrm{Gal}((E/\mathbb{Q}(\mu_p^{1-k}))))$. Hence $E/\mathbb{Q}(\mu_p^{1-k})$ is non-trivial.

- Let us show that $\mathbb{Q}(\mu_p^{1-k})/\mathbb{Q}$ is totally ramified at p. Let us consider the extension $\mathbb{Q}(\mu_p^{1-k})/\mathbb{Q}$, then we have that $gef = [\mathbb{Q}(\mu_p^{1-k}) : \mathbb{Q}] = \frac{p-1}{(p-1,k-1)}$ where e and f are the ramification index and the inertia degree of p in $\mathbb{Q}(\mu_p^{1-k})$ and g the number of factors in which p splits. We claim that $e = \frac{p-1}{(p-1,k-1)}$ i.e. p is totally ramified in $\mathbb{Q}(\mu_p^{1-k})$. Let $\mathfrak{P}$ a prime in $\mathbb{Q}(\mu_p)$ over p, then $e(\mathfrak{P}|p) = \varphi(p) = p-1$. Since the ramification index is multiplicative in tower we have that, for P a prime over p in $\mathbb{Q}(\mu_p^{1-k})$, $e(\mathfrak{P}|p) = e(\mathfrak{P}|P)e(P|p)$ then, if we assume by contradiction that $e(P|p) < \frac{p-1}{(p-1,k-1)}$, then $e(\mathfrak{P}|P) > (p-1, k-1) = [\mathbb{Q}(\mu_p) : \mathbb{Q}(\mu_p^{1-k})]$, contradiction.

- Let us show that $E/\mathbb{Q}(\mu_p^{1-k})$ is unramified. By i) we have that $\overline{\rho}$ is unramified at every prime $l \neq p$ then it remains to show only that $E/\mathbb{Q}(\mu_p^{1-k})$ is unramified at p, then let us show that $E/\mathbb{Q}(\mu_p^{1-k})$ is totally unramified at the unique prime P over p. By iv) we have that the decomposition group D_p at p is such that $\overline{\rho}(D_p)$ has order prime to p i.e. D_p has order prime to p. But the ramification index $e(Q|p)$ of p in E divides the order of D_p and the ramification index $e(Q|P)$ of P in E divides p then, by the tower multiplicativity of the ramification index we have that $E/\mathbb{Q}(\mu_p^{1-k})$ is totally unramified also at p.

- Let $\sigma \in \mathrm{Gal}(E/\mathbb{Q})$, $\tau \in \mathrm{Gal}(E/\mathbb{Q}(\mu_p^{1-k}))$, then we show that $\sigma\tau\sigma^{-1} = \chi(\sigma)^{1-k}\tau$. Let us notice that

$$\overline{\rho}(\sigma) = \begin{pmatrix} 1 & a_\sigma \\ 0 & \chi^{k-1}(\sigma) \end{pmatrix} \text{ and } \overline{\rho}(\tau) = \begin{pmatrix} 1 & a_\tau \\ 0 & 1 \end{pmatrix}$$

since $\ker \chi^{1-k}$ fixes $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}(\mu_p^{1-k})) \supseteq \mathrm{Gal}(E/\mathbb{Q}(\mu_p^{1-k}))$, then we have to show that the following equality holds

$$\overline{\rho}(\sigma)\overline{\rho}(\tau)\overline{\rho}(\sigma)^{-1} = \chi^{1-k}(\sigma)\overline{\rho}(\tau).$$

We have

$$\begin{aligned}
\overline{\rho}(\sigma)\overline{\rho}(\tau)\overline{\rho}(\sigma)^{-1} &= \begin{pmatrix} 1 & a_\sigma \\ 0 & \chi^{k-1}(\sigma) \end{pmatrix} \begin{pmatrix} 1 & a_\tau \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & -a_\sigma\chi^{1-k}(\sigma) \\ 0 & \chi^{1-k}(\sigma) \end{pmatrix} \\
&= \begin{pmatrix} 1 & a_\sigma \\ 0 & \chi^{k-1}(\sigma) \end{pmatrix} \begin{pmatrix} 1 & 0 \\ 0 & \chi^{1-k}(\sigma) \end{pmatrix} \\
&= \begin{pmatrix} 1 & a_\sigma\chi^{1-k}(\sigma) \\ 0 & 1(\sigma) \end{pmatrix} \\
&= \begin{pmatrix} 1 & a_\sigma \\ 0 & 1 \end{pmatrix}^{\chi^{1-k}(\sigma)} \\
&= \chi(\sigma)^{1-k} \cdot \overline{\rho}(\tau)
\end{aligned}$$

□

Chapter 2

Reductions of Reducible Representations

The aim of this section is to define the notion of reduction of a representation and to study its structure.

Let us consider a finite extension K of the p-adic numbers $\mathbb{Q}_p$ and let $\mathcal{O}$ be its ring of integers with residue field F and uniformizing parameter π. Let us consider a free module V of rank 2 over K.

DEFINITION 2.1. With notations as above, a *lattice* T in V is a free $\mathcal{O}$-module of rank 2 in V such that it generates V over K, i.e. $T \cdot K = V$.

To give the definition of reduction of a representation we firstly have to study the stability of lattices under the action of groups.

DEFINITION 2.2. Let $\rho : G \to \mathrm{GL}(V)$ be a representation of a group G in V. A lattice T in V is said to be *stable* if $\rho(g)(T) = T$ for every $g \in G$.

For p-adic Galois representations we have the following result about stable lattices.

Proposition 2.3. *Let $\rho : G \to \mathrm{GL}(V)$ be a p-adic Galois representation. Then there exists at least one lattice T of V stable under the action of G.*

Proof. Let L be a lattice in V and define H to be the stabilizer of L in G, i.e.

$$H = \{g \in G \mid g.L = L\}$$

where

$$G \times V \to V \text{ given by } (g, v) \mapsto g.v$$

is a 2-dimensional p-adic representation as in Definition B.32 [1]. Then H is open in G. Indeed, let $\{l_1, l_2\}$ be a basis of L and, for $i = 1, 2$, let $f_i : G \to V$ given by $g \mapsto g.l_i$. Then

$$H = \{g \in G \mid g.l_1 \in L\} \cap \{g \in G \mid g.l_2 \in L\} = f_1^{-1}(L) \cap f_2^{-1}(L).$$

[1] equivalent to the one in Definition B.31

Hence, since G is compact and H is open, G/H is finite. Therefore the lattice $T = \bigcup_{g\in G/H} \rho(g)L$ is, by construction, stable under the action of G. □

Now, since T is G-stable, also πT is G-stable by linearity. Then we may define an action of G on $T/\pi T$ by $g(t+\pi T) = \rho(g)(t) + \pi T$. It is well-defined since, if we consider t' in the same coset of t, $t - t' \in \pi T$ and so $\rho(g)(t-t') \in \pi T$. Let us notice that $T/\pi T$ is free of rank 2 over F.

Let us now introduce the notion of reduction of a representation.

DEFINITION 2.4. Let $\rho : G \to \mathrm{GL}(V)$ be a p-adic Galois representation, T a G-stable lattice in V. With notations as above, the map $\overline{\rho} : G \to \mathrm{GL}(T/\pi T)$ is called the *reduction* of ρ attached to T.

Let us now give the definition of semisimplification of a representation.

DEFINITION 2.5. Let $\rho : G \to \mathrm{GL}(V)$ be a representation as above. A filtration $0 = V_0 \subseteq V_1 \subseteq \cdots \subseteq V_n = V$ of V is called a *Jordan-Hölder series* if, for every $j = 1, \ldots, n$, V_j is a subrepresentation and V_j/V_{j-1} is simple. Then the *semisimplification* of V is $\bigoplus_{j=1}^{n} V_j/V_{j-1}$.

By the Brauer-Nesbitt theorem ([5] Theorem 30.16) we have that the semisimplification of the reduction $\overline{\rho}$ does not depend on the choice of the lattice T. Hence, up to semisimplifications, reductions of p-adic representations are unique and so, $\overline{\rho}$ is unique if one reduction (and thus any reduction) is simple.

Let us recall that we want to prove Theorem 1.5 and so let us consider the opposite situation, i.e. let us assume that the reduction $\overline{\rho} : G \to \mathrm{GL}_2(F)$ of $\rho : G \to \mathrm{GL}(V)$ is reducible. Then the semisimplifications of $\overline{\rho}$ are described by $\varphi_1 \oplus \varphi_2$, where $\varphi_1, \varphi_2 : G \to F^*$ are characters not depending on the choice of the lattice T. Hence a reduction $\overline{\rho}$ of a representation ρ may be written, in a matricial way, as

$$\begin{pmatrix} \varphi_1 & * \\ 0 & \varphi_2 \end{pmatrix} \text{ or } \begin{pmatrix} \varphi_1 & 0 \\ * & \varphi_2 \end{pmatrix}.$$

Let us now study a criterion for the semisimplicity of such a reduction. It will be useful in the next chapters.

Lemma 2.6. *Let F be a field of characteristic p. A representation $\overline{\rho} : G \to \mathrm{GL}_2(F)$ is diagonalizable, i.e. semisimple, if, and only if, its image has order prime to p.*

Proof. Let α be an element in the image of $\overline{\rho}$, i.e. $\alpha \in \mathrm{GL}_2(F)$. Then, in the algebraic closure $\overline{F}$, α has a Jordan form of the type

$$A = \begin{pmatrix} a & 1 \\ 0 & a \end{pmatrix} \text{ or } B = \begin{pmatrix} a & 0 \\ 0 & d \end{pmatrix}$$

for $a, d \in \overline{F}^*$. Let us now take $n \geq 1$, then we have that

$$A^n = \begin{pmatrix} a^n & na^{n-1} \\ 0 & a^n \end{pmatrix} \text{ and } B^n = \begin{pmatrix} a^n & 0 \\ 0 & d^n \end{pmatrix}.$$

Then we may notice that A is not semisimple but has order divisible by p (since otherwise $na^{n-1} \not\equiv 0 \bmod p$) while B is semisimple but has order not divisible by p (otherwise $a^n = a^p a^{n-p} = aa^{n-p}$). □

Recalling that we are considering representations such that their reductions are reducible, let us study the form of these reductions.

Proposition 2.7. *Let $\rho : G \to \mathrm{GL}_2(K)$ be a simple representation with all its reductions that are reducible. Let φ_1, φ_2 be the characters associated to the reductions of ρ. Then G leaves stable some lattice $T \subseteq V$ for which the associated reduction is of the form $\begin{pmatrix} \varphi_1 & * \\ 0 & \varphi_2 \end{pmatrix}$ but is not semisimple.*

Proof. Let us begin the proof with two observations that will be useful in the following.

1. Let T be a G-stable lattice of V with an $\mathcal{O}$-basis, then the representation $\rho : G \to \mathrm{GL}_2(K)$ can be seen as $\rho : G \to \mathrm{GL}_2(\mathcal{O})$ and any $M \in \mathrm{GL}_2(K)$ such that $M\rho(G)M^{-1} \subseteq \mathrm{GL}_2(\mathcal{O})$ defines another G-stable lattice MT together with a basis of it. Hence the reduction attached to this new lattice is the map
$$G \to M\rho(G)M^{-1} \hookrightarrow \mathrm{GL}_2(\mathcal{O}) \to \mathrm{GL}_2(F).$$

2. Let $P = \begin{pmatrix} 1 & 0 \\ 0 & \pi \end{pmatrix}$, where π is the uniformizer defined at the beginning of this chapter. Then, doing some obvious computations, we have that the following equality holds.
$$P \begin{pmatrix} a & \pi b \\ c & d \end{pmatrix} P^{-1} = \begin{pmatrix} a & b \\ \pi c & d \end{pmatrix} \tag{2.1}$$

Let us now start the proof.

1. We may assume that the reduction $\overline{\rho}$ is always of the form $\begin{pmatrix} \varphi_1 & * \\ 0 & \varphi_2 \end{pmatrix}$. Indeed, with the same notations as above, let $\rho : G \to \mathrm{GL}_2(\mathcal{O})$ be the representation, T a G-stable lattice in V with an $\mathcal{O}$-basis and assume that $\overline{\rho}$ has the form $\begin{pmatrix} \varphi_1 & 0 \\ * & \varphi_2 \end{pmatrix}$, then, using (2.1), we obtain
$$\begin{pmatrix} \varphi_1 & 0 \\ * & \varphi_2 \end{pmatrix} \equiv \begin{pmatrix} \varphi_1 & \pi b \\ * & \varphi_2 \end{pmatrix} \overset{(2.1)}{\Rightarrow} \begin{pmatrix} \varphi_1 & b \\ \pi * & \varphi_2 \end{pmatrix} \equiv \begin{pmatrix} \varphi_1 & b \\ 0 & \varphi_2 \end{pmatrix}.$$

2. Let us now assume by contradiction that every reduction $\overline{\rho}$ of the form $\begin{pmatrix} \varphi_1 & * \\ 0 & \varphi_2 \end{pmatrix}$ is semisimple. Then, if we prove that ρ is reducible, the proof is complete because we obtain a contradiction (indeed, ρ was by assumption

simple). To prove that ρ is reducible, starting with $M_0 = \mathbb{I}_2$ the identity matrix, we will construct inductively a convergent sequence of matrices $M_i = \begin{pmatrix} 1 & t_i \\ 0 & 1 \end{pmatrix}$ such that $M_i \rho(G) M_i^{-1} \subseteq \mathrm{GL}_2(\mathcal{O})$ consists of matrices whose lower-left corner entries are divisible by π and whose upper-right corner entries are divisible by π^i. Then, with such a converging sequence, we will obtain that the matrix $M = \begin{pmatrix} 1 & t \\ 0 & 1 \end{pmatrix}$, where $t = \lim_i t_i$, is such that $M\rho(G)M^{-1}$ are matrices with upper-right corner entries equal to 0. Hence the representation ρ will be reducible. Let us now show that the sequence $\{M_i\}_i$ above converges. Let us notice that we can reformulate the induction in the following way. Let us assume that $M_i \rho(G) M_i^{-1}$ consists of matrices of the form $\begin{pmatrix} a & \pi^i b \\ \pi c & d \end{pmatrix}$ for $a, b, c, d \in \mathcal{O}$. Using equation (2.1) we then obtain

$$P^i M_i \rho(G) M_i^{-1} P^{-i} = \begin{pmatrix} a & b \\ \pi^{i+1} & d \end{pmatrix}.$$

Hence the representation given by

$$g \mapsto P^i M_i \rho(g) M_i^{-1} P^{-1} (\mathrm{mod}\ \pi)$$

is of the form $\begin{pmatrix} \varphi_1 & * \\ 0 & \varphi_2 \end{pmatrix}$ since the representation $g \mapsto \rho(g)(\ \mathrm{mod}\ \pi)$ is of this form. By assumption we have that this representation is semisimple then we may choose an element $u \in \mathcal{O}$ such that the mod π representation is diagonalized by the matrix $U = \begin{pmatrix} 1 & u \\ 0 & 1 \end{pmatrix}$. This means that there exists an element $u \in \mathcal{O}$ such that $UP^i M_i \rho(G) M_i^{-1} P^{-i} U^{-1}$ consists of matrices of the form $\begin{pmatrix} \alpha & \pi\beta \\ \pi^{i+1}\gamma & \delta \end{pmatrix}$. Then, conjugating by P^{-i} we obtain

$$(P^{-i}UP^i M_i)\rho(G)(P^{-i}UP^i M_i)^{-1} = \begin{pmatrix} \alpha & \pi^{i+1}\beta \\ \pi c & d \end{pmatrix}$$

and so, setting

$$M_{i+1} = P^{-i}UP^i M_i = \begin{pmatrix} 1 & t_i + \pi^i u \\ 0 & 1 \end{pmatrix},$$

we may continue the induction. Using this last formula we may also notice that the sequence $\{M_i\}_i$ converges.

□

Chapter 3

A congruence between a cusp form and an Eisenstein series

First of all, let us warning the reader that all the needing definitions and results related to modular forms are given, without proofs, in Appendix A.

Let p be an odd prime and let us consider a Dirichlet character modulo p $\varepsilon : (\mathbb{Z}/p\mathbb{Z})^* \to \mathbb{C}$ that could be also the trivial character. For a modular form f of weight k on $\Gamma_1(p)$, let us now give a definition regarding the character.

DEFINITION 3.1. With notations as above, let us define the modular form $f \in \mathcal{M}_k(\Gamma_1(p))$, $k = 1, 2$, to be *of type* ε if it satisfies

$$f\left[\begin{pmatrix} a & b \\ c & d \end{pmatrix}\right]_k = \varepsilon(d)f$$

for every $\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Gamma_0(p)$.

REMARK 3.2. For a modular form $f \in \mathcal{M}_k(\Gamma_1(p))$, being of type ε is equivalent to say that

$$\langle d \rangle f = \varepsilon(d)f$$

for every $\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Gamma_0(p)$ where $\langle d \rangle$ is the Diamond operator defined in Definition A.36 for $(d, p) = 1$.

We are interested in particular types of modular forms of type ε called cusp forms and semi-cusp forms.

DEFINITION 3.3. Let f be a modular form. For every $\tau \in \mathcal{H}$ the *q-expansion* of $f(\tau)$ is the series $\sum_{n\geq 0} a_n(f)q^n$ where $q = e^{2\pi i\tau}$.

With this definition we can define the notions of cusp forms and semi-cusp forms.

DEFINITION 3.4. Let $f \in M_k(\Gamma_1(p))$ be a modular form of type ε. It is called a *cusp form* if its q-expansion and that of $f[\begin{pmatrix} 0 & -1 \\ p & 0 \end{pmatrix}]_k$ both have the coefficient a_0 equal to 0. If only the q-expansion of f begins with 0 then f is called a *semi-cusp form*.

REMARK 3.5. Let us notice that the definition above agrees with the one in Definition A.17 since the two q-expansions considered above are the two q-expansions related to the two cusp forms (0 and ∞) of $\Gamma_0(p)$.

Let us now associate to the character ε some Eisenstein series.

First of all let us recall a usual definition about characters.

DEFINITION 3.6. A character ε is said to be *even* (resp. *odd*) if $\varepsilon(-1) = 1$ (resp. $\varepsilon(-1) = -1$).

Then, thanks to Theorem A.30, we know that for a non-trivial even[1] character ε of modulo p there exist two Eisenstein series of weight 2 and type ε on $\Gamma_1(p)$. Indeed, $\mathcal{E}_2(p, \varepsilon)$ has basis $\{G_{2,\varepsilon} = E_2^{\mathbf{1},\varepsilon,1}, s_{2,\varepsilon} = E_2^{\varepsilon,\mathbf{1},1}\}$ given by

$$G_{2,\varepsilon} = E_2^{\mathbf{1},\varepsilon,1}(\tau) = E_2^{\mathbf{1},\varepsilon}(\tau) = L(-1,\varepsilon)/2 + \sum_{n\geq 1}\sum_{d|n} \varepsilon(d)dq^n,$$

$$s_{2,\varepsilon} = E_2^{\varepsilon,\mathbf{1},1}(\tau) = E_2^{\varepsilon,\mathbf{1}}(\tau) = \sum_{n\geq 1}\sum_{d|n} \varepsilon(n/d)dq^n$$

where $L(s,\chi) = \sum_{n\geq 1} \frac{\chi(n)}{n^s}$, for χ a Dirichlet character and $s \in \mathbb{C}$ such that $\operatorname{Re} s > 1$, is the L-Dirichlet function.

REMARK 3.7. Let us notice that the Eisenstein series $s_{2,\varepsilon}$ is only a semi-cusp form since it vanishes only at the cusp of $\Gamma_0(p)$ corresponding to ∞.

Then, by Proposition A.27, the space of modular forms of weight 2 and type ε is generated by the cusp forms and the two Eisenstein series $G_{2,\varepsilon}$ and $s_{2,\varepsilon}$.

Again by Theorem A.31, we have that there exists only one Eisenstein series of weight 1 and type ε given by

$$G_{1,\varepsilon} = E_1^{\varepsilon,\mathbf{1},1}(\tau) = L(0,\varepsilon)/2 + \sum_{n\geq 1}\sum_{d|n} \varepsilon(d)q^n$$

where ε is an odd character[2].

Let us notice that by Theorem A.42, the Eisenstein series of weight 2 defined above are eigenforms for the Hecke operators T_n, when $(n,p) = 1$, with eigenvalues

$$T_n G_{2,\varepsilon} = T_n E_2^{\mathbf{1},\varepsilon,1} = (1 + n\varepsilon(n))G_{2,\varepsilon},$$

$$T_n s_{2,\varepsilon} = T_n E_2^{\varepsilon,\mathbf{1},1} = (\varepsilon(n) + n)s_{2,\varepsilon}.$$

[1] Indeed, by Theorem A.30, $\varepsilon \cdot \mathbf{1}(-1) = 1$.

[2] Indeed, by Theorem A.31, $\varepsilon \cdot \mathbf{1}(-1) = -1$.

In order to construct the cusp form that will be used in the proof of Theorem 1.5, we firstly have to study some results about congruences of some Eisenstein series.

From now on, let us fix a prime $\mathfrak{p}$ of $\mathbb{Q}(\mu_{p-1})$ lying over p, with p splitting completely in $\mathbb{Q}(\mu_{p-1})$[3] and μ_{p-1} the group of complex $(p-1)$-th roots of unity. Then let us consider the unique character

$$\omega : (\mathbb{Z}/p\,\mathbb{Z})^* \overset{\cong}{\to} \mu_{p-1}$$

such that $\omega(d) \equiv d \bmod \mathfrak{p}$ for every $d \in \mathbb{Z}$[4].

Let us now study the form of the two Eisenstein series $G_{1,\omega^{k-1}}$ and $G_{2,\omega^{k-2}}$ defined above.

Lemma 3.8. *Let k be an even integer, $2 \leq k \leq p-3$. Then the modular forms $G_{2,\omega^{k-2}}$ and $G_{1,\omega^{k-1}}$ have $\mathfrak{p}$-integral q-expansions in $\mathbb{Q}(\mu_{p-1})$ which are congruent modulo $\mathfrak{p}$ to the q-expansion*

$$G_k = -\frac{B_k}{2k} + \sum_{n\geq 1}\sum_{d|n} d^{k-1}q^n.$$

Proof. From the definitions of Eisenstein series given above we have

$$G_{2,\omega^{k-2}} = \frac{L(-1,\omega^{k-2})}{2} + \sum_{n\geq 1}\sum_{d|n}\omega^{k-2}(d)dq^n$$

$$G_{1,\omega^{k-1}} = \frac{L(0,\omega^{k-1})}{2} + \sum_{n\geq 1}\sum_{d|n}\omega^{k-1}(d)q^n.$$

Then, if we consider the terms for $n \geq 1$, their coefficients are respectively $\omega^{k-2}(d)d$ and $\omega^{k-1}(d)$. But ω is defined such that $\omega(d) \equiv d \bmod \mathfrak{p}$ and so we obtain $\omega^{k-2}(d)d \equiv d^{k-1} \equiv \omega^{k-1}(d) \bmod \mathfrak{p}$. Hence it remains to prove the congruence only for the constant terms of the two series. Let us recall that the Dirichlet L-function $L(s,\varepsilon) = \sum_{n\geq 1}\frac{\varepsilon(n)}{n^s}$, where ε is a character mod k, may be written as

$$L(s,\varepsilon) = \frac{1}{k^s}\sum_{r=1}^{k}\varepsilon(r)\zeta(s,\frac{r}{k})$$

where $\zeta(s,a)$ is the Hurwitz-zeta function such that

$$\zeta(0,a) = \frac{1}{2} - a \text{ and } \zeta(-n,a) = -\frac{B_{n+1}(a)}{n+1}$$

[3]Indeed, p splits completely in the cyclotomic field $\mathbb{Q}(\mu_{p-1})$ if, and only if, $p \equiv 1 \bmod p-1$.

[4]It is known also as Teichmüller character.

for $B_{n+1}(a)$ the $(n+1)$-Bernoulli polynomial. Since in our situation we are considering characters modulo p, we obtain

$$\begin{aligned} L(0,\varepsilon) &= \sum_{n=1}^{p} \varepsilon(n)\zeta(0,\frac{n}{p}) \\ &= \sum_{n=1}^{p-1} \varepsilon(n)(\frac{1}{2}-\frac{n}{p}) + \varepsilon(p)\zeta(0,1) \\ &= -\frac{1}{p}\left(\sum_{n=1}^{p-1}\varepsilon(n)(n-\frac{p}{2})\right) \end{aligned}$$

and

$$\begin{aligned} L(-1,\varepsilon) &= p\sum_{n=1}^{p}\varepsilon(n)\zeta(-1,\frac{n}{p}) \\ &= p\sum_{n=1}^{p}\varepsilon(n)\left(-\frac{B_2(n/p)}{2}\right) \\ &= p\left(\sum_{n=1}^{p-1}\varepsilon(n)(-\frac{\sum_{k=0}^{2}\binom{2}{k}B_{2-k}\cdot(n/p)^k}{2})\right) + p\varepsilon(p)\left(-\frac{B_2(1)}{2}\right) \\ &= p\left(\sum_{n=1}^{p-1}-\frac{\varepsilon(n)}{2}\left(\frac{1}{6}-\frac{n}{p}+(\frac{n}{p})^2\right)\right) \\ &= -\frac{1}{2p}\sum_{n=1}^{p-1}\left(\frac{p^2}{6}-np+n^2\right)\varepsilon(n). \end{aligned}$$

Now, by a consequence of the Hensel's lemma ([3] Section 3.2)[5], we have that $\omega(n) \equiv n^p \bmod \mathfrak{p}^2$ and so, applying this equivalence in the above equalities for $\varepsilon = \omega^{k-1}$ and ω^{k-2} respectively, we obtain

$$pL(0,\omega^{k-1}) \equiv -\sum_{n=1}^{p-1} n^{p(k-1)+1} \bmod \mathfrak{p}^2$$

$$pL(-1,\omega^{k-2}) \equiv -\frac{1}{2}\sum_{n=1}^{p-1} n^{p(k-2)+2} \bmod \mathfrak{p}^2.$$

Moreover, by [1] result 8.8 pag.385, we have that

$$pB_t \equiv \sum_{n=1}^{p-1} n^t \bmod p^2$$

and, by the Kummer's congruences ([23] Corollary 5.14),

$$\frac{B_t}{t} \equiv \frac{B_{t+p-1}}{t+p-1} \bmod p.$$

[5] Applied to the polynomial $f(x) = x^{p-1}-1$ and the element n^p.

Hence we obtain

$$L(0,\omega^{k-1}) \equiv -B_{p(k-1)+1} \equiv -(p(k-1)+1)\frac{B_{k+p-1}}{k+p-1} \equiv -\frac{B_k}{k} \bmod \mathfrak{p}$$

$$L(-1,\omega^{k-2}) \equiv -\frac{1}{2}B_{2+p(k-2)} \equiv -\frac{1}{2}(2+p(k-2))\frac{B_{p(k-1)+1}}{p(k-1)+1} \equiv -\frac{B_k}{k} \bmod \mathfrak{p}$$

where we used also that $1+p(k-1) \equiv k \equiv 2+p(k-2) \bmod (p-1)$. □

This lemma has an immediate corollary.

Corollary 3.9. *Let k,m,n be even integers, $2 \leq k,m,n \leq p-3$, such that $n+m \equiv k \bmod (p-1)$. Then the product*

$$G_{1,\omega^{n-1}}G_{1,\omega^{m-1}}$$

is a modular form of weight 2 and type ω^{k-2} with a $\mathfrak{p}$-integral q-expansion in $\mathbb{Q}(\mu_{p-1})$. Moreover, its constant term is a $\mathfrak{p}$-unit provided that neither B_n nor B_m are divisible by p.

Proof. The product $G_{1,\omega^{n-1}}G_{1,\omega^{m-1}}$ is clearly a modular form of weight 2 and type $\omega^{n-1}\omega^{m-1} \equiv \omega^{k-2} \bmod (p-1)$. Then, by Lemma 3.8, we have that it has a $\mathfrak{p}$-integral q-expansion in $\mathbb{Q}(\mu_{p-1})$ and its constant term is a $\mathfrak{p}$-unit if $p \nmid B_n, B_m$. □

Let us now construct a particular modular form of weight 2 and type ω^{k-2} that will be used to define a semi-cusp form.

Theorem 3.10. *Let k be an even integer, $2 \leq k \leq p-3$. Then there exists a modular form g of weight 2 and type ω^{k-2} whose q-expansion coefficients are $\mathfrak{p}$-integers in $\mathbb{Q}(\mu_{p-1})$ and whose constant term is 1.*

Proof. Let us notice that it suffices to construct such a g with constant term being a $\mathfrak{p}$-unit. Then, multiplying by another unit, we will obtain constant term equal to 1. Let us divide our proof in cases.

1. Let $p \nmid B_k$. Then, by Lemma 3.8, we may choose $g = G_{2,\omega^{k-2}}$.
2. Let $p \nmid B_nB_m$ for m,n even integers as in Corollary 3.9. Then we may choose $g = G_{1,\omega^{n-1}}G_{1,\omega^{m-1}}$.
3. Let $p \mid B_nB_m$, where n,m are defined as in Corollary 3.9, and let t be the number of even integers n, $2 \leq n \leq p-3$, such that $p \mid B_n$. Since there exist $(p-1)/2$ Bernoulli numbers B_n for $2 \leq n \leq p-3$ even, to show the theorem it suffices to show that p divides less than $(p-1)/4$ of them, i.e. we want to show that $t < \frac{p-1}{4}$. Let us now show that $p^t \mid h^-$, where h^-

is the negative part of the class number of $\mathbb{Q}(\mu_p)$[6]. By [12] pag. 250, we have that the negative part h^- may be written as

$$h^- = \alpha p \prod_{k=2k \text{ even}}^{p-1} L(0, \omega^{k-1}).$$

Then, arguing as in the proof of Lemma 3.8, we obtain that

$$h^- = \alpha p \prod_{k=2k \text{ even}}^{p-1} -\frac{B_k}{2k}.$$

Hence, by definition of t, $p^t \mid h^-$.
Then, since by the claim $p^t \mid h^-$, it will suffice to show that $h^- < p^{(p-1)/47}$.
By [2] result 1.7 pag. 266, we may write

$$h^- = \pm \frac{D}{p^{(p-3)/2}}$$

where D is a determinant of dimension $(p-1)/2$ whose entries are integers between 1 and $p-1$. Then, by Hadamard's inequality[8], we have that

$$|D| \leq (p-1)^{(p-1)/2} (\frac{p-1}{2})^{(p-1)/4}$$

and so we obtain that

$$\begin{aligned} h^- &\leq (p-1)^{(p-1)/2} (\frac{p-1}{2})^{(p-1)/4} p^{-(p-3)/2} \\ &< p^{(p-1)/2} (p/2)^{(p-1)/4} p^{-(p-3)/2} \\ &= p^{(p+3)/4} 2^{-(p-1)/4}. \end{aligned}$$

If $p \leq 19$ then, by [23] Chap. II, $h^- = 1$ and so obviously $h^- < p^{(p-1)/4}$.
If $p > 19$ then, since $p \leq 2^{(p-1)/4}$, $h^- < p^{(p+3)/4} 2^{-(p-1)/4} \leq p^{(p-1)/4}$.

□

From now on, let us fix an even integer k, $2 \leq k \leq p-3$, such that $p \mid B_k$ and let us set $\varepsilon = \omega^{k-2}$. By the fact that $B_2 = \frac{1}{6}$, we may refine the limitation for k and consider even k such that $4 \leq k \leq p-3$, hence ε will be a non-trivial even character. Moreover, all the modular forms that we will consider will be of weight 2 and type ε.

Under these assumption, let us now notice that the previous results give us a semi-cusp form equivalent to the Eisenstein series $G_{2,\varepsilon}$.

[6] Recall that the negative part h^- of the class number h of $\mathbb{Q}(\mu_p)$ is defined by $h^- h^+ = h$, where h^+ is the class number of the real cyclotomic field of $\mathbb{Q}(\mu_p)$.

[7] Indeed, if $h^- \mid p^{(p-1)/4}$ then, as $p^t \mid h^-$, $p^t < p^{(p-1)/4}$ and so $t < (p-1)/4$.

[8] Let A be a $n \times n$ matrix whose entries are bounded by C, then $|\det(A)| \leq C^n n^{n/2}$.

Proposition 3.11. *There exists a semi-cusp form $f = \sum_{n\geq 1} a_n q^n$ such that:*

1. *The coefficients a_n are $\mathfrak{p}$-integers in $\mathbb{Q}(\mu_{p-1})$*
2. *$f \equiv G_k \equiv G_{2,\varepsilon}$ (mod $\mathfrak{p}$) in q-expansions.*

Proof. Let c be the constant term of the Eisenstein series $G_{2,\varepsilon}$ and let us define f as $f = G_{2,\varepsilon} - c \cdot g$, where g is the g defined in Theorem 3.10. Then, as the constant term of g is 1, the constant term of the q-expansion of f will be 0 and so f is, by definition, a semi-cusp form. Moreover, by Lemma 3.8, we have that $G_{2,\varepsilon} \equiv G_k \pmod{\mathfrak{p}}$ and so, in particular, $c \equiv -\frac{B_k}{2k} \pmod{\mathfrak{p}}$. Since by assumption $p \mid B_k$, then $\mathfrak{p} \mid c$ and so $f \equiv G_{2,\varepsilon} \pmod{\mathfrak{p}}$. □

Let us now prove that the semi-cusp form defined in Proposition 3.11 is actually a cusp form that is also an eigenform for some Hecke operators.

Proposition 3.12. *There exists a non-zero cusp form f' of type ε which is an eigenform for all the Hecke operators T_n with $(n,p) = 1$ and which has the property that for each prime $l \neq p$ the eigenvalue $\lambda(l)$ of T_l acting on f' satisfies*

$$\lambda(l) \equiv 1 + l^{k-1} \equiv 1 + \varepsilon(l)l \,(\mathrm{mod}\, \mathcal{M}),$$

where $\mathcal{M}$ is a certain prime (independent from l) lying over $\mathfrak{p}$ in the field $\mathbb{Q}(\mu_{p-1}, \lambda(n))$ generated by the eigenvalues over $\mathbb{Q}(\mu_{p-1})$.

Proof. Let us prove this proposition by steps.

1. Let us consider the semi-cusp form f defined in Proposition 3.11. By loc.cit. we have that $f \equiv G_{2,\varepsilon} \pmod{\mathfrak{p}}$ and so, by Theorem A.42, it is a (mod $\mathfrak{p}$)-eigenform for the Hecke operators T_n, $(n,p) = 1$.

2. We have already noticed before Lemma 3.8 that, for primes $l \neq p$, $T_l G_{2,\varepsilon} = (1 + \varepsilon(l)l)G_{2,\varepsilon}$ hence, by the previous step, $T_l f \equiv (1 + \varepsilon(l)l)f \pmod{\mathfrak{p}}$. Let us now recall that $\varepsilon = \omega^{k-2}$ is a non-trivial even character such that $\omega(l) \equiv l \pmod{\mathfrak{p}}$, hence $\omega^{k-2}(l)l \equiv l^{k-1} \pmod{\mathfrak{p}}$ that means that the eigenvalue $\lambda(l)$ of f under T_l is $\lambda(l) \equiv 1 + l^{k-1} \pmod{\mathfrak{p}}$.

3. By the Deligne-Serre's lemma [8] 6.11, we obtain a semi-cusp form f' as in the statement.

4. It remains only to show that such a semi-cusp form f' is indeed a cusp form. Since we have already noticed that the space of the semi-cusp forms is generated by the cusp forms and the semi-cusp form $s_{2,\varepsilon}$, it suffices to show that $f' \neq s_{2,\varepsilon}$. Again thanks to the facts before Lemma 3.8, we have that $T_l s_{2,\varepsilon} = (l + \varepsilon(l))s_{2,\varepsilon}$ hence we would have $l + \varepsilon(l) \equiv 1 + l\varepsilon(l)$ (mod $\mathfrak{p}$) but this cannot happen since $\varepsilon(l) \not\equiv 1$ (indeed, ε is non-trivial by assumption).

□

In the next proposition we will see that the cusp-form f' defined in Proposition 3.12 is an eigenform for T_n for every n and not only for the n's not divisible by p.

Proposition 3.13. *Let f' be a form as in the statement of Proposition 3.12. Then f' is an eigenform for all Hecke operators T_n (including those for which $p \mid n$). Hence, after replacing f' by a multiple $\tilde{f}$ of f', we have*

$$\tilde{f} = \sum_{n=1}^{\infty} \lambda(n) q^n$$

with $T_n \tilde{f} = \lambda(n) \tilde{f}$.

Proof. Let f' be defined as in Proposition 3.12, then it is an eigenform for T_n when $(n, p) = 1$ and so, by [9] Exercise 5.8.4, f' is an oldform or a newform. If we assume that f' is an oldform, then f' has to belong to $\mathcal{S}_2(\Gamma_1(p))^{old}$ that is the trivial space since $\mathcal{M}_2(\mathrm{SL}_2(\mathbb{Z}))$ is the trivial space by Remark A.8. Hence f' is a newform. Applying [9] Theorem 5.8.2 a), we then obtain that f' is a Hecke eigenform for every positive $n \in \mathbb{Z}$ such that a suitable scalar multiple $\tilde{f}$ is a newform of weight 2 and type ε with the property that $T_n \tilde{f} = \lambda(n) \tilde{f}$ where $\tilde{f} = \sum_{n=1}^{\infty} \lambda(n) q^n$. □

We can then summarize all the previous propositions in the statement of the next theorem.

Theorem 3.14. *There exists a cusp form $f = \sum_{n \geq 1} a_n q^n$ of weight 2 and some type ε which is a normalized, i.e. $a_1 = 1$, eigenform for all Hecke operators T_n and which satisfies*

$$a_l \equiv 1 + l^{k-1} \equiv 1 + \varepsilon(l) l \ (mod\ \mathfrak{p})$$

for all primes $l \neq p$, where $\mathfrak{p}$ is a certain prime ideal over p in the field K generated by the coefficients of f, which does not depend on l.

Chapter 4

Construction and study of the (mod p) representation

In Chapter 3 we have studied particular cusp forms that turned out to be eigenforms for every Hecke operator of the type T_n. In this chapter we will use such results to construct the mod p representation Theorem 1.5.

By Theorem B.40 we have that the representation ρ associated to the cusp form f is unramified at every prime $l \neq p$. Then, to prove Theorem 1.5 points ii) and iii), it remains only to show that there exists a lattice in the representation such that the associated reduction of ρ is of the form $\begin{pmatrix} 1 & * \\ 0 & \chi^{k-1} \end{pmatrix}$ and it's not semisimple. But thanks to Proposition 2.7 we have only to show that the representation ρ is irreducible and to find a lattice such that the associated reduction is reducible. Then we will only have to prove that this reduction has semisimplification of the form $1 \oplus \chi^{k-1}$.

Let us now assume $p \mid B_k$ for some k even integer, $2 \leq k \leq p-3$, and consider the cusp eigenform $f \in \mathcal{S}_2(p, \varepsilon = \omega^{k-2})$ defined in Theorem 3.14. Let

$$\rho : G_{\mathbb{Q}} = \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \to \mathrm{GL}(V_p(A_f))$$

be the representation defined in Theorem B.40. By construction we have that $f \equiv G_k \bmod \mathfrak{p}$, then, by Theorem 3.14, $a_l \equiv 1 + l^{k-1} \bmod \mathfrak{p}$. Hence, by Theorem B.40, we have that an absolute Frobenius element Frob_l over l acts on $V_p(A_f)$ with

$$\mathrm{Tr}(\mathrm{Frob}_l) = a_l \text{ and } \det(\mathrm{Frob}_l) = l\varepsilon(l). \tag{4.1}$$

By Theorem B.28 we have that any system of absolute Frobenius elements F is dense in $G_{\mathbb{Q}}$ hence, since ρ, and then its determinant, is continuous, the determinant may be uniquely extended from $F \subseteq G_{\mathbb{Q}}$ to a continuous homomorphism $G_{\mathbb{Q}} \to K_{\mathfrak{p}}$, where $K_{\mathfrak{p}}$ is the completion of the field K at $\mathfrak{p}$. Then $\mathrm{Frob}_l \to l$ is extended uniquely by the standard cyclotomic character

$$\chi_* : G_{\mathbb{Q}} \to \mathbb{Z}_p^{\times} \subseteq K_{\mathfrak{p}}^{\times}.$$

Hence the character ε may be seen as a character of $G_{\mathbb{Q}}$ via $\varepsilon : \sigma \mapsto \varepsilon(\chi_*(\sigma))$. Therefore, $\det \rho = \chi_* \varepsilon$.

Let us now show that the representation ρ is irreducible.

Proposition 4.1. *The $K_{\mathfrak{p}}$-representation ρ is irreducible.*

Proof. Let us assume by contradiction that the representation ρ is reducible. Then its semisimplification, that is unique by the Jordan-Hölder theorem, is abelian and described by two characters $\rho_1, \rho_2 : G_{\mathbb{Q}} \to K_{\mathfrak{p}}^*$. By [21] Theorem pag.III-20, ρ is then locally algebraic and so, by loc. cit. pag.III-4, there exist integers n_i, $i = 1, 2$, such that $\rho_i = \chi_*^{n_i}$ on an open subgroup of an inertia group for p in $G_{\mathbb{Q}}$. Then we may write $\rho_i = \chi_*^{n_i} \varepsilon_i$ where ε_i is a character of finite order ramified only at p. Hence, regarding ε_i as Dirichlet characters, we obtain from (4.1) that for every $l \neq p$ the following equivalence hold

$$l\varepsilon(l) = l^{n_1+n_2}\varepsilon_1(l)\varepsilon_2(l) \tag{4.2}$$

$$a_l = l^{n_1}\varepsilon_1(l) + l^{n_2}\varepsilon_2(l). \tag{4.3}$$

Hence, from (4.2), we obtain that $n_1 + n_2 = 1$ that means that, without loss of generality, $n_1 \geq 1$ and $n_2 \leq 0$. From (4.3) we get that $|a_l| \geq l - 1$[1] for every $l \neq p$. But if $l \geq 7$, since, by [6], we have that $|a_l| \leq 2\sqrt{l}$, then we get a contradiction. □

We have just showed that the representation ρ is irreducible then, by Proposition 2.7, it remains to show that there exists a lattice such that the associated reduction is of the form of Proposition 2.7.

The next proposition will prove that any $G_{\mathbb{Q}}$-invariant lattice would suffice for our aim. But, before it, let us denote by χ the reduction modulo p of χ_*, i.e.

$$\chi : G_{\mathbb{Q}} \xrightarrow{\chi_*} \mathbb{Z}_p^* \to \mathbb{F}_p^* \hookrightarrow \mathbb{F}^*.$$

Proposition 4.2. *There exists an $\mathcal{O}_{\mathfrak{p}}$-lattice $T \subseteq V_p(A_f)$ invariant by $G_{\mathbb{Q}}$ for which the action of $G_{\mathbb{Q}}$ on $T/\pi T$ may be described matricially by*

$$\begin{pmatrix} 1 & * \\ 0 & \chi^{k-1} \end{pmatrix}$$

and is furthermore not semisimple.

Proof. By Proposition 4.1 we have that ρ is irreducible and so, by Proposition 2.7, it suffices to find a lattice such that the reduction is reducible and so the representation ρ will not be semisimple. By Brauer-Nesbitt theorem [5], we have that the reduction has a well-defined semisimplification, then it suffices to find a lattice T such that the associated reduction has semisimplification of the form $1 \oplus \chi^{k-1}$. Let T be a $G_{\mathbb{Q}}$-stable lattice then, by Theorem B.40, for every

[1] Indeed, $|a_l| = |\varepsilon_1(l)l^{n_1} + \varepsilon_2(l)l^{n_2}| \geq |\varepsilon_1(l)l^{n_1}| - |\varepsilon_2(l)l^{n_2}| \geq l - 1$ since $\varepsilon_i(l)$ is a root of unity.

prime $l \neq p$, there exists an absolute Frobenius element for l acting on $T/\pi T$ such that

$$\mathrm{Tr}(\mathrm{Frob}_l) \equiv a_l \text{ and } \det(\mathrm{Frob}_l) \equiv l\varepsilon(l) \pmod{\pi}.$$

By Theorem 3.14 we have that $f \equiv G_k \pmod{\pi}$ and so we obtain

$$a_l \equiv l^{k-1} + 1 \text{ and } l\varepsilon(l) \equiv l^{k-1} \pmod{\pi}.$$

Hence, since by construction $l^{k-1} \equiv \chi^{k-1} \pmod{\pi}$ and by the fact that the set of Frobenius element is dense in $G_{\mathbb{Q}}$, we have that $G_{\mathbb{Q}}$ acts on $T/\pi T$ with

$$\mathrm{Tr} \equiv 1 + \chi^{k-1} \text{ and } \det \equiv \chi^{k-1} \pmod{\pi}$$

and so every $\sigma \in G_{\mathbb{Q}}$ has the same characteristic roots as a representation of the form $1 \oplus \chi^{k-1}$[2]. Hence, by Brauer-Nesbitt theorem, these two representations have the same semisimplification. Hence the reduction associated to the lattice T has semisimplification $1 \oplus \chi^{k-1}$ as wanted. □

It remains only to prove point iv) of Theorem 1.5. This will be done in the next chapter.

[2]Indeed, the characteristic polynomial of $\sigma \in G_{\mathbb{Q}}$ is $x^2 - \mathrm{Tr}\, x + \det$ and it's the same one of that of $1 \oplus \chi^{k-1}$ since $\mathrm{Tr}(1 \oplus \chi^{k-1}) = 1 + \chi^{k-1}$ and $\det(1 \oplus \chi^{k-1}) = \chi^{k-1}$.

Chapter 5

Diagonalizability of the (mod p) restriction

Let us set $M = T/\pi T$ as in Proposition 4.2. We want to show that M is the representation space for the representation $\overline{\rho}$ of Theorem 1.5 for which point iv) is satisfied.

Let us consider the subgroup $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}(\mu_p)^+)$ of $G_{\mathbb{Q}}$ corresponding to the real cyclotomic field $\mathbb{Q}(\mu_p)^+ = \mathbb{Q}(\mu_p + \mu_p^{-1})$. Now, since the ramification index of p in $\mathbb{Q}(\mu_p)$ is $e(\mathcal{P}|p) = \varphi(p) = p - 1$, then p is totally ramified in $\mathbb{Q}(\mu_p)$ and so also in its subfield $\mathbb{Q}(\mu_p)^+$. Then let $\mathfrak{p}$ be the unique prime in $\mathbb{Q}(\mu_p)^+$ lying over p and consider its decomposition group D in $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}(\mu_p)^+)$. To verify point iv) of Theorem 1.5 it is then sufficient to show that the action of D on M is semisimple, i.e. that $\mathrm{Im}(D) \subseteq \mathrm{Aut}(M)$ has order prime to p (thanks to Lemma 2.6). Indeed, if it is true, then, by the fact that $p \nmid [\mathbb{Q}(\mu_p)^+ : \mathbb{Q}]$, we have that also p does not divide the order of the decomposition group for $G_{\mathbb{Q}}$.

To prove this claim it will be convenient to let E be the completion of the real cyclotomic field $\mathbb{Q}(\mu_p)^+$ at p and to identify D with the Galois group $\mathrm{Gal}(\overline{E}/E)$. We will, at first, show that the $\mathrm{Gal}(\overline{E}/E)$-module M has some properties and then, using them, we will prove the claim.

Let us first give the notion of Neron model for an abelian variety.

Definition 5.1. Let A be an abelian variety over the field E. The *Neron model* of A over E is the the smooth separated scheme $\mathcal{A}$ over the ring of integers $\mathcal{R}$ with fiber A, i.e. such that the following diagram commutes

$$\begin{array}{ccc} A & \longrightarrow & \mathcal{A} \\ \downarrow & & \downarrow \\ \mathrm{Spec}\, E & \longrightarrow & \mathrm{Spec}\, \mathcal{R} \end{array} .$$

Remark 5.2. Since A is an abelian variety, the Neron model $\mathcal{A}$ is unique, up to isomorphism, and it's a commutative group scheme over $\mathcal{R}$.

Let us now study the properties of the Galois module M.

Proposition 5.3. *The* $\mathrm{Gal}(\overline{E}/E)$*-module* M *is the Galois module attached to a finite flat commutative group scheme of type* $(p, \dots, p)$ *over the ring of integers* $\mathcal{R}$ *of* E*.*

Proof. Let $A_{\mathfrak{p}}$ be the abelian variety associated to the modular form f via the Eichler-Shimura relation and let us replace $A_{\mathfrak{p}}$ by A where A is an abelian variety that is $\mathbb{Q}$-isogeneous to $A_{\mathfrak{p}}$ and such that its ring of $\mathbb{Q}$-endomorphisms is the ring of integers $\mathcal{O}$ of K. Hence we have that $M = T/\pi T$ is isomorphic to $A[\mathfrak{p}]$, where $A[\mathfrak{p}] = \{a \in A \mid \mathfrak{p}a = 0_A\}$ is the "kernel of $\mathfrak{p}$" on A. Let us now recall that the module of the p-division points of an abelian variety is the module whose elements are the points of A of order p. Then, since $\mathfrak{p} \mid p$, M is a submodule of the module N of p-division points of A. By the Deligne-Rapoport Theorem ([7] Example 3.7), the abelian variety A acquires good reduction everywhere over E and so there exists a unique, up to isomorphism, Neron model $\mathcal{A}$ over A. Let us now consider the map "multiplication by p" on the Neron model, i.e. the map

$$m : \mathcal{A} \to \mathcal{A}$$

(defined over points as $a \mapsto pa$) and let us set $\mathcal{A}_p$ to be the scheme-theoretic kernel of the map m, i.e.

$$\begin{array}{ccc} \mathcal{A} & \xrightarrow{\quad m \quad} & \mathcal{A} \\ \uparrow & & \uparrow{\scriptstyle e_{\mathcal{A}}} \\ \mathcal{A}_p = \ker m & \longrightarrow & \operatorname{Spec} \mathcal{R} \end{array} .$$

Let us notice that, since the Neron model $\mathcal{A}$, by Remark 5.2, is a group scheme over $\mathcal{R}$, also its scheme-theoretic kernel $\mathcal{A}_p$ is a group scheme over $\mathcal{R}$. Moreover, since the map m is an isogeny ([17] Theorem 7.2), its kernel $\mathcal{A}_p$ is finite flat of type $(p, \dots, p)$. Then N is the Galois module attached to $\mathcal{A}_p$, i.e.

$$\begin{array}{ccc} N & \longrightarrow & \mathcal{A}_p \\ \downarrow & & \downarrow \\ \operatorname{Spec} E & \longrightarrow & \operatorname{Spec} \mathcal{R} \end{array} .$$

Let us consider the closure $\mathcal{M}$ of M in $\mathcal{A}_p$, where $\mathcal{M}$ is the smallest closed subscheme of $\mathcal{A}_p$ such that $M = \mathcal{M} \otimes_{\operatorname{Spec} \mathcal{R}} \operatorname{Spec} E$[1], then M is the Galois module associated to $\mathcal{M}$, that is

$$\begin{array}{ccc} M \subseteq A & \longrightarrow & \mathcal{M} \subseteq \mathcal{A}_p \\ \downarrow & & \downarrow \\ \operatorname{Spec} E & \longrightarrow & \operatorname{Spec} \mathcal{R} \end{array} .$$

□

[1] [18] Chapter 2

Thanks to this last proposition and by the previous observations done in this work, we can write down some properties of the module M:

1. By Chapter 2, M is free of rank 2 over the residue field $\mathbf{F}$ of $\mathcal{O}_{\mathfrak{p}}$ where $\mathcal{O}_{\mathfrak{p}}$ is the completion of $\mathcal{O}$ at $\mathfrak{p}$.
2. Since the reduction of the representation constructed in Chapter 4 has the form $\begin{pmatrix} 1 & * \\ 0 & \chi^{k-1} \end{pmatrix}$, D acts trivial on a 1-dimensional subspace X of M and via the character χ^{k-1} on the quotient $Y = M/X$.
3. By Proposition 5.3, M is the Galois module attached to a finite flat group scheme $\mathcal{M}$ of type $(p, \dots, p)$ over $\mathcal{R}$.

Let us now finally end the proof of Theorem 1.5 by proving that the image of D is diagonalizable, i.e., by Lemma 2.6, it has a prime-to-p order.

Theorem 5.4. *The image of D in $\operatorname{Aut} M$ has prime-to-p order.*

Proof. Let $\mathcal{X}$ be the closure of X in $\mathcal{M}$, i.e. $X = \mathcal{X} \otimes_{\operatorname{Spec} \mathcal{R}} \operatorname{Spec} E$. Then, by fact 2 above, the D-module attached to $\mathcal{X}$ is the trivial module X. Moreover, since the real cyclotomic field $\mathbb{Q}(\mu_p)^+ = \mathbb{Q}(\mu_p + \mu_p^{-1})$ of degree $[\mathbb{Q}(\mu_p)^+ : \mathbb{Q}] = (p-1)/2$ is totally ramified over p, we have that the absolute ramification index of p in the completion E is $(p-1)/2 < p-1$. Since E has characteristic 0, $\mathcal{X}$ is a non-zero constant étale group scheme and, by [18] Theorem 3.3.3, $\mathcal{X}$ is a group scheme over $\mathcal{R}$. Hence $\mathcal{M}$ cannot be connected. Indeed, if $\mathcal{M}$ would be connected, then, by the short exact sequence

$$0 \to \mathcal{M}^0 \to \mathcal{M} \to \mathcal{M}^{et} \to 0,$$

we would have that $\mathcal{M}^0 = \mathcal{M}$ and $\mathcal{M}^{et} = 0$ where $\mathcal{M}^{et}$ is the largest étale quotient of $\mathcal{M}$. But $\mathcal{M}$ has the non-zero étale subgroup $\mathcal{X}$, contradiction.
Let us now consider the canonical exact sequence of D-modules

$$0 \to M^0 \to M \to M^{et} \to 0 \tag{5.1}$$

where M^0 is associated to the largest connected subgroup of $\mathcal{M}$ and M^{et} to the largest étale quotient of $\mathcal{M}$. Since M has a Galois-compatible $\mathbf{F}$-vector space structure, by [18] Proposition 3.3.2, $\mathcal{M}$ is a group scheme in $\mathbf{F}$-vector spaces and so, in particular, the sequence (5.1) is an exact sequence of $\mathbf{F}$-vector spaces. Let us notice that $M^0 \neq M$, being $\mathcal{M}$ not connected, and that $M^{et} \neq M$ being M^{et} unramified (as it is étale) but M not unramified (since it has the quotient $Y = M/X$). Hence, by fact 1, M^0 has dimension 1 and has image in M distinct from X[2]. Therefore, D leaves stable X (by 2) and the line M^0 distinct from X. Let us eventually notice that every element of order p in $\operatorname{Aut} M$, that is of the form $\begin{pmatrix} 1 & * \\ 0 & \chi^{k-1} \end{pmatrix}$, leaves stable a unique line in M, hence D has order prime-to-p in $\operatorname{Aut} M$. □

[2]Indeed, $M/M^0 \cong M^{et} \neq Y$, being Y not unramified, hence $M^0 \neq X$.

Appendix A

Modular forms and Hecke operators

In this chapter we will state all the needing facts about modular forms and Hecke operators that will be used in the work above. All the results are taken from [9].

A.1 Modular forms and cusp forms

Definition A.1. The *modular group* is the group

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

with generators the two matrices

$$\gamma_1 = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \text{ and } \gamma_2 = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}.$$

Remark A.2.

1. Every element of the modular group $\mathrm{SL}_2(\mathbb{Z})$ can be viewed as an automorphism of the Riemann sphere $\widehat{\mathbb{C}} = \mathbb{C} \cup \{\infty\}$. Hence it is of the form
$$\begin{pmatrix} a & b \\ c & d \end{pmatrix}(\tau) = \frac{a\tau + b}{c\tau + d}, \tau \in \widehat{\mathbb{C}}.$$

2. Every pair $\pm\gamma \in \mathrm{SL}_2(\mathbb{Z})$ gives the same transformation in $\widehat{\mathbb{C}}$, i.e. the modular group may be seen as $\mathrm{SL}_2(\mathbb{Z})/\{\pm 1\}$;

3. The group of such transformations is generated by $\tau \mapsto \tau + 1$ and $\tau \mapsto \frac{-1}{\tau}$.

Definition A.3. The *upper half plane* is the space $\mathcal{H} = \{\tau \in \mathbb{C} \mid \mathrm{Im}\,\tau > 0\}$.

Remark A.4. Let $\gamma \in \mathrm{SL}_2(\mathbb{Z})$ and $\tau \in \mathcal{H}$. Then $\mathrm{Im}(\gamma(\tau)) = \frac{\mathrm{Im}\,\tau}{|c\tau+d|^2} > 0$ and so $\gamma(\tau) \in \mathcal{H}$. Hence the modular group $\mathrm{SL}_2(\mathbb{Z})$ maps $\mathcal{H}$ to itself.

DEFINITION A.5. 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 every $\gamma \in \mathrm{SL}_2(\mathbb{Z}), \tau \in \mathcal{H}$.

REMARK A.6.
1. If $f(\gamma(\tau)) = (c\tau + d)^k f(\tau)$ for γ_1, γ_2 the two generators of $\mathrm{SL}_2(\mathbb{Z})$ then it holds for every $\gamma \in SL_2(\mathbb{Z})$. Hence it suffices to check if $f(\tau + 1) = f(\tau)$ and $f(-1/\tau) = \tau^k f(\tau)$.
2. $f(\tau)$ and $f(\gamma(\tau))$ have the same zeros and poles.

DEFINITION A.7. Let k be an integer. A function $f : \mathcal{H} \to \mathbb{C}$ is a *modular form of weight* k if:

i. f is holomorphic on $\mathcal{H}$;

ii. f is weakly modular of weight k;

iii. f is holomorphic at ∞, i.e. the function $\tilde{f}$, expressing f as a function in $q = e^{2\pi i\tau}$, can be extended to a holomorphic function in 0.

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

REMARK A.8. The set of modular forms $\mathcal{M}_k(\mathrm{SL}_2(\mathbb{Z}))$ is a vector space of finite dimension and, by [9] Theorem 3.5.2, $\mathcal{M}_k(\mathrm{SL}_2(\mathbb{Z})) = \{0\}$ for $k \leq 4$ even integer.

DEFINITION A.9. Let us define the set of modular forms $\mathcal{M}(\mathrm{SL}_2(\mathbb{Z}))$ as

$$\mathcal{M}(\mathrm{SL}_2(\mathbb{Z})) = \bigoplus_{k \in \mathbb{Z}} \mathcal{M}_k(\mathrm{SL}_2(\mathbb{Z})).$$

It is a graded ring.

DEFINITION A.10. Let k be an integer. A *cusp form of weight* k is a modular form of weight k whose Fourier expansion has leading coefficient $a_0 = 0$, i.e.

$$f(\tau) = \sum_{n=1}^{\infty} a_n q^n, q = e^{2\pi i\tau}.$$

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

REMARK A.11.
1. A modular form is a cusp form if $\lim_{\mathrm{Im}\,\tau \to \infty} f(\tau) = 0$;
2. $\mathcal{S}_k(\mathrm{SL}_2(\mathbb{Z}))$ is a vector subspace of $\mathcal{M}_k(\mathrm{SL}_2(\mathbb{Z}))$;
3. $\mathcal{S}(\mathrm{SL}_2(\mathbb{Z})) = \bigoplus_{k \in \mathbb{Z}} \mathcal{S}_k(\mathrm{SL}_2(\mathbb{Z}))$ is an ideal in $\mathcal{M}(\mathrm{SL}_2(\mathbb{Z}))$.

A.2 Congruence subgroups

DEFINITION A.12. Let N be a positive integer. The *principal congruence subgroup of level* N is

$$\Gamma(N) = \{\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{SL}_2(\mathbb{Z}) \mid \begin{pmatrix} a & b \\ c & d \end{pmatrix} \equiv \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \bmod N\}.$$

REMARK A.13. 1. $\Gamma(1) = \mathrm{SL}_2(\mathbb{Z})$;

2. Let us consider the surjection $\varphi : \mathrm{SL}_2(\mathbb{Z})) \to \mathrm{SL}_2(\mathbb{Z}/N\mathbb{Z}))$. Then $\Gamma(N) = \ker(\varphi)$ and so $\Gamma(N) \trianglelefteq \mathrm{SL}_2(\mathbb{Z})$.

DEFINITION A.14. Let Γ be a subgroup of $\mathrm{SL}_2(\mathbb{Z})$. It is a *congruence subgroup* if there exists an $N \in \mathbb{Z}_{>0}$ such that $\Gamma(N) \subseteq \Gamma$. Then Γ is a *congruence subgroup of level* N.

REMARK A.15. The fact that $[\mathrm{SL}_2(\mathbb{Z}) : \Gamma(N)]$ is finite implies that Γ has finite index in $\mathrm{SL}_2(\mathbb{Z})$.

EXAMPLE 1. Let us now consider some important congruence subgroups that are not principal.

1. $\Gamma_0(N) = \{\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{SL}_2(\mathbb{Z}) \mid \begin{pmatrix} a & b \\ c & d \end{pmatrix} \equiv \begin{pmatrix} * & * \\ 0 & * \end{pmatrix} \bmod N\}$.

2. $\Gamma_1(N) = \{\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{SL}_2(\mathbb{Z}) \mid \begin{pmatrix} a & b \\ c & d \end{pmatrix} \equiv \begin{pmatrix} 1 & * \\ 0 & 1 \end{pmatrix} \bmod N\}$

Then we may notice that $\Gamma(N) \subseteq \Gamma_1(N) \subseteq \Gamma_0(N) \subseteq \mathrm{SL}_2(\mathbb{Z})$.
Moreover, let us consider the surjective maps

$$\psi_1 : \Gamma_1(N) \to \mathbb{Z}/N\mathbb{Z} \text{ given by } \begin{pmatrix} a & b \\ c & d \end{pmatrix} \mapsto b \bmod N$$

and

$$\psi_2 : \Gamma_0(N) \to (\mathbb{Z}/N\mathbb{Z})^* \text{ given by } \begin{pmatrix} a & b \\ c & d \end{pmatrix} \mapsto d \bmod N,$$

then $\Gamma(N) = \ker(\psi_1) \trianglelefteq \Gamma_1(N)$ (with $[\Gamma(N) : \Gamma_1(N)] = N$) and $\Gamma_1(N) = \ker(\psi_2) \trianglelefteq \Gamma_0(N)$ (with $[\Gamma_0(N) : \Gamma_1(N)] = \varphi(N)$, where φ is the Euler function).

DEFINITION A.16. 1. Let $\gamma \in \mathrm{SL}_2(\mathbb{Z})$. The *factor of automorphy* is $j(\gamma, \tau) = c\tau + d \in \mathbb{C}^*$.

2. Let $\gamma \in \mathrm{SL}_2(\mathbb{Z})$ and k be an integer. The *weight-k operator* $[\gamma]_k$ on functions $f : \mathcal{H} \to \mathbb{C}$ is defined by

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

(Let us notice that if f is meromorphic then $f[\gamma]_k$ is also meromorphic with same zeros and poles of f).

DEFINITION A.17. Let Γ be a congruence subgroup of $\mathrm{SL}_2(\mathbb{Z})$, k an integer. A function $f : \mathcal{H} \to \mathbb{C}$ is a *modular form of weight k with respect to* Γ if:

i. f is holomorphic;

ii. f is weight-k invariant under Γ, i.e. $f[\gamma]_k = f$ for every $\gamma \in \Gamma$;

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

If, in addition, $a_0 = 0$ in the Fourier expansion of $f[\alpha]_k$ for every $\alpha \in \mathrm{SL}_2(\mathbb{Z})$, then f is a *cusp form of weight k with respect to* Γ.
The modular forms (resp. cusp forms) of weight k with respect to Γ are denoted by $\mathcal{M}_k(\Gamma)$ (resp. $\mathcal{S}_k(\Gamma)$).

REMARK A.18. Let us notice that $\mathcal{S}(\Gamma) = \bigoplus_{k\in\mathbb{Z}} \mathcal{S}_k(\Gamma) \trianglelefteq \mathcal{M}(\Gamma) = \bigoplus_{k\in\mathbb{Z}} \mathcal{M}_k(\Gamma)$.

DEFINITION A.19. Let Γ be a congruence subgroup of $\mathrm{SL}_2(\mathbb{Z})$. The *cusps* of Γ are the Γ-equivalence classes of $\mathbb{Q} \cup \{\infty\}$.

Lemma A.20. *If $\Gamma = \Gamma_0(p)$, where p is a prime, then its cusps are only the two classes of ∞ and 0.*

DEFINITION A.21. Let $\chi : (\mathbb{Z}/N\mathbb{Z})^* \to \mathbb{C}$ be a Dirichlet character[1]. Then the *χ-eigenspace* of $\mathcal{M}_k(\Gamma_1(N))$ is

$$\mathcal{M}_k(N,\chi) = \{f \in \mathcal{M}_k(\Gamma_1(N)) \mid f[\gamma]_k = \chi(d_\gamma)f \text{ for every } \gamma = \begin{pmatrix} a_\gamma & b_\gamma \\ c_\gamma & d_\gamma \end{pmatrix} \in \Gamma_0(N)\}.$$

Analogously,

$$\mathcal{S}_k(N,\chi) = \{f \in \mathcal{S}_k(\Gamma_1(N)) \mid f[\gamma]_k = \chi(d_\gamma)f \text{ for every } \gamma = \begin{pmatrix} a_\gamma & b_\gamma \\ c_\gamma & d_\gamma \end{pmatrix} \in \Gamma_0(N)\}.$$

REMARK A.22. The vector space $\mathcal{M}_k(\Gamma_1(N))$ of modular forms decomposes as the direct sum of the eigenspaces, i.e.

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

The same holds also for the space $\mathcal{S}_k(\Gamma_1(N))$ of cusp forms.

A.3 Modular curves

DEFINITION A.23. Let Γ be a congruence subgroup of $\mathrm{SL}_2(\mathbb{Z})$ acting from the left on the upper half plane $\mathcal{H}$. The *modular curve* is

$$Y(\Gamma) = \Gamma\backslash\mathcal{H} = \{\Gamma\tau \mid \tau \in \mathcal{H}\}.$$

Let now Γ be a congruence subgroup of $\mathrm{SL}_2(\mathbb{Z})$. We want to compactify the modular curve $Y(\Gamma)$.

DEFINITION A.24. Let $\mathcal{H}^* = \mathcal{H} \cup \mathbb{Q} \cup \{\infty\}$. Than the *compact modular curve associated to* Γ is

$$X(\Gamma) = \Gamma\backslash\mathcal{H}^* = Y(\Gamma) \cup \Gamma\backslash(\mathbb{Q} \cup \{\infty\}).$$

For the congruence subgroups $\Gamma_0(N), \Gamma_1(N)$ and $\Gamma(N)$ we write $X_0(N), X_1(N)$ and $X(N)$.

[1] i.e. $\chi : (\mathbb{Z}/N\mathbb{Z})^* \to \mathbb{C}^*$ is a homomorphism of multiplicative groups.

A.4 Eisenstein series of weight 1 and 2

In this section we will study Eisenstein series of weight 1 and 2 for the congruence subgroup $\Gamma_1(N)$ of $\mathrm{SL}_2(\mathbb{Z})$.

Definition A.25. Let Γ be a congruence subgroup of $\mathrm{SL}_2(\mathbb{Z})$ and k an integer. The *weight-k Eisenstein space for* Γ is the quotient space of the modular forms by the cusp forms, i.e.

$$\mathcal{E}_k(\Gamma) = \mathcal{M}_k(\Gamma)/\mathcal{S}_k(\Gamma).$$

Let now χ be a Dirichlet character modulo N, then we define the χ-eigenspace of the Eisenstein space $\mathcal{E}_k(\Gamma_1(N))$ in the following way.

Definition A.26. Let χ be a Dirichlet character modulo N. The *χ-eigenspace of the Eisenstein series* $\mathcal{E}_k(\Gamma_1(N))$ is

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

Proposition A.27. *Let Γ be a congruence subgroup of $\mathrm{SL}_2(\mathbb{Z})$. Then the Eisenstein space is linearly disjoint from the cusp forms, i.e.*

$$\mathcal{M}_k(\Gamma) = \mathcal{S}_k(\Gamma) \oplus \mathcal{E}_k(\Gamma).$$

Moreover, if χ is a Dirichlet character modulo N, the χ-eigenspace of the Eisenstein space is linearly disjoint from that of the cusp forms, i.e.

$$\mathcal{M}_k(N,\chi) = \mathcal{S}_k(N,\chi) \oplus \mathcal{E}_k(N,\chi).$$

Remark A.28. The decomposition in Remark A.22 holds also for the Eisenstein space of $\Gamma_1(N)$, i.e.

$$\mathcal{E}_k(\Gamma_1(N)) = \bigoplus_k \mathcal{E}_k(N,\chi).$$

For the aim of this paper we are interested only in the Eisenstein series of weight 1 and 2 then let us start studying the Eisenstein space of $\Gamma_1(N)$ of weight 2.

Let $A_{N,2}$ be the set of triples (ψ,φ,t) such that ψ and φ are primitive[2] Dirichlet characters modulo u and v with $(\psi\varphi)(-1) = 1$ and t is an integer such that $1 < tuv \mid N$.

Definition A.29. For any triple $(\psi,\varphi,t) \in A_{N,2}$ let us define

$$E_2^{\psi,\varphi,t}(\tau) = \begin{cases} E_2^{\psi,\varphi}(t\tau) & \text{unless } \psi = \varphi = \mathbf{1}, \\ E_2^{\mathbf{1},\mathbf{1}}(\tau) - tE_2^{\mathbf{1},\mathbf{1}}(t\tau) & \text{if } \psi = \varphi = \mathbf{1} \end{cases}$$

where

$$E_2^{\psi,\varphi}(\tau) = \delta(\psi)L(-1,\varphi) + 2\sum_{n\geq 1} \sigma_1^{\psi,\varphi}(n)q^n,\ q = e^{2\pi i\tau}$$

[2] A Dirichlet character modulo N is called primitive if it is not induced by any other character except itself, i.e. there exists no Dirichlet character $\chi_2 \neq \chi$ of modulo $N_2 \mid N$ such that $\chi_2(n) = \chi(n)$ for $n \in (\mathbb{Z}/N\mathbb{Z})^*$.

with

$$\delta(\psi) = \begin{cases} 1 & \psi = \mathbf{1} \\ 0 & \text{otherwise} \end{cases}, \ \sigma_{k-1}^{\psi,\varphi}(n) = \sum_{0<d|n} \psi(n/d)\varphi(d)d^{k-1}.$$

Then:

Theorem A.30. *Let N be a positive integer. The set*

$$\{E_2^{\psi,\varphi,t} \mid (\psi,\varphi,t) \in A_{N,2}\}$$

is a basis of the Eisenstein space $\mathcal{E}_2(\Gamma_1(N))$. Moreover, for any character χ modulo N, the set

$$\{E_2^{\psi,\varphi,t} \mid (\psi,\varphi,t) \in A_{N,2}, \psi\varphi = \chi\}$$

is a basis of the χ-eigenspace $\mathcal{E}_k(N,\chi)$.

Let us study the Eisenstein space of weight 1. Analogously to the case $k = 2$, let $A_{N,1}$ be the set of triples $(\{\psi,\varphi\},t)$ such that $\{\psi,\varphi\}$ is an unordered pair of primitive Dirichlet characters modulo u and v such that $(\psi\varphi)(-1) = -1$ and t is a positive integer such that $1 < tuv \mid N$. For any triple $(\{\psi,\varphi\},t) \in A_{N,1}$ let us define

$$E_1^{\psi,\varphi,t}(\tau) = E_1^{\psi,\varphi}(t\tau)$$

where

$$E_1^{\psi,\varphi}(\tau) = \delta(\varphi)L(0,\psi) + \delta(\psi)L(0,\varphi) + 2\sum_{n\geq 1} \sigma_0^{\psi,\varphi}(n)q^n, \ q = e^{2\pi i\tau}$$

with $\delta(\psi), \delta(\varphi)$ and $\sigma_0^{\psi,\varphi}(n)$ defined as in Definition A.29. Then,

Theorem A.31. *Let N be a positive integer. The set*

$$\{E_1^{\psi,\varphi,t} \mid (\{\psi,\varphi\},t) \in A_{N,1}\}$$

is a basis of the Eisenstein space $\mathcal{E}_1(\Gamma_1(N))$. Moreover, for any character χ modulo N, the set

$$\{E_1^{\psi,\varphi,t} \mid (\{\psi,\varphi\},t) \in A_{N,1}, \psi\varphi = \chi\}$$

is a basis for the χ-eigenspace $\mathcal{E}_1(N,\chi)$.

A.5 Hecke operators

Definition A.32. Let $\Gamma_1, \Gamma_2 \subseteq \mathrm{SL}_2(\mathbb{Z})$ be congruence subgroups so that, in particular,

$$\Gamma_1, \Gamma_2 \subseteq \mathrm{GL}_2^+(\mathbb{Q}) = \{\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{GL}_2(\mathbb{Q}) \mid ad - bc > 0\}.$$

Then, for every $\alpha \in \mathrm{GL}_2^+(\mathbb{Q})$, the set

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

is a double coset in $\mathrm{GL}_2^+(\mathbb{Q})$.

REMARK A.33. i. The double cosets defined above transform modular forms with respect to Γ_1 into modular forms with respect to Γ_2.

ii. $\Gamma_1 \backslash \Gamma_1 \alpha \Gamma_2$ is finite.

Using Remark A.33 we may give the following definition.

DEFINITION A.34. Let $\alpha \in \mathrm{GL}_2^+(\mathbb{Q})$ and $\Gamma_1, \Gamma_2 \in \mathrm{SL}_2(\mathbb{Z})$ be congruence subgroups. Then the *weight-k* $\Gamma_1 \alpha \Gamma_2$ *operator* takes $f \in \mathcal{M}_k(\Gamma_1)$ to

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

where the $\{\beta_j\}$ are orbit representatives, i.e. $\Gamma_1 \alpha \Gamma_2 = \bigcup_j \Gamma_1 \beta_j$ disjoint union.

REMARK A.35. The weight-k $\Gamma_1 \alpha \Gamma_2$ operator sends $\mathcal{M}_k(\Gamma_1)$ to $\mathcal{M}_k(\Gamma_2)$ and $\mathcal{S}_k(\Gamma_1)$ to $\mathcal{S}_k(\Gamma_2)$.

DEFINITION A.36. Let $\Gamma_1 = \Gamma_2 = \Gamma_1(N)$ and $\alpha \in \Gamma_0(N)$. Let us consider the weight-k double coset operator $[\Gamma_1 \alpha \Gamma_2]_k$ sending $f \in \mathcal{M}_k(\Gamma_1(N))$ to $f[\Gamma_1(N) \alpha \Gamma_1(N)]_k = f[\alpha]_k$. Then we define an Hecke operator, called *diamond operator*,

$$\langle d \rangle : \mathcal{M}_k(\Gamma_1(N)) \to M_k(\Gamma_1(N)) \text{ given by } f \mapsto \langle d \rangle f = f[\alpha]_k$$

for any $\alpha = \begin{pmatrix} a' & b' \\ c' & d' \end{pmatrix} \in \Gamma_0(N)$ with $d' \equiv d \pmod{N}$.

REMARK A.37. Let $\chi : (\mathbb{Z}/N\mathbb{Z})^* \to \mathbb{C}$ be a character. Then the space $\mathcal{M}_k(N, \chi)$ (defined in A.21), is the χ-eigenspace of the diamond operator, i.e.

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

Hence the diamond operator $\langle d \rangle$ respects the decomposition $\mathcal{M}_k(\Gamma_1(N)) = \oplus_\chi \mathcal{M}_k(N, \chi)$, operating on the eigenspace associated to each character χ as multiplication by $\chi(d)$.

DEFINITION A.38. Let $\Gamma_1 = \Gamma_2 = \Gamma_1(N)$ and $\alpha = \begin{pmatrix} 1 & 0 \\ 0 & p \end{pmatrix}$, p a prime number. Then we define another Hecke operator given by the weight-k double coset operator

$$T_p : \mathcal{M}_k(\Gamma_1(N)) \to \mathcal{M}_k(\Gamma_1(N)) \text{ given by } f \mapsto T_p f = f[\Gamma_1(N) \begin{pmatrix} 1 & 0 \\ 0 & p \end{pmatrix} \Gamma_1(N)]_k$$

where the double coset is

$$\Gamma_1(N) \begin{pmatrix} 1 & 0 \\ 0 & p \end{pmatrix} \Gamma_1(N) = \left\{ \gamma \in M_2(\mathbb{Z}) \mid \gamma \equiv \begin{pmatrix} 1 & * \\ 0 & p \end{pmatrix} \pmod{N}, \det \gamma = p \right\}.$$

REMARK A.39. The two Hecke operators defined in A.36 and A.38 commute, i.e.

$$\langle d \rangle T_p f = T_p \langle d \rangle f.$$

Proposition A.40. *Let N be a positive integer, $\Gamma_1 = \Gamma_2 = \Gamma_1(N)$ and $\alpha = \begin{pmatrix} 1 & 0 \\ 0 & p \end{pmatrix}$ for p a prime. Then the operator $T_p = [\Gamma_1 \alpha \Gamma_2]_k$ on $\mathcal{M}_k(\Gamma_1(N))$ is given by*

$$T_p f = \begin{cases} \sum_{j=0}^{p-1} f \left[\begin{pmatrix} 1 & j \\ o & p \end{pmatrix} \right]_k & \text{if } p \mid N \\ \sum_{j=0}^{p-1} f \left[\begin{pmatrix} 1 & j \\ 0 & p \end{pmatrix} \right]_k + f \left[\begin{pmatrix} m & n \\ N & p \end{pmatrix} \begin{pmatrix} p & 0 \\ 0 & 1 \end{pmatrix} \right]_k & \text{if } p \nmid N, \text{ where } mp - nN = 1. \end{cases}$$

Proposition A.41. *Let $f \in \mathcal{M}_k(\Gamma_1(N))$. Since $\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \in \Gamma_1(N)$, then f has period 1 and so it has a Fourier expansion*

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

Moreover, let $\chi : (\mathbb{Z}/N\mathbb{Z})^* \to \mathbb{C}^*$ be a character. If $f \in \mathcal{M}_k(N, \chi)$, then also $T_p f \in \mathcal{M}_k(N, \chi)$ and its Fourier expansion is

$$(T_p f)(\tau) = \sum_{n=0}^{\infty} (a_{np}(f) + \chi(p) p^{k-1} a_{n/p}(f)) q^n, \quad q = e^{2\pi i \tau}$$

where $a_{n/p} = 0$ if $n/p \notin \mathbb{Z}$.

Let us now study how these Hecke operators act on Eisenstein series of weight k.

Let χ be a Dirichlet character modulo N, ψ, φ primitive characters modulo u and v such that $(\psi\varphi)(-1) = (-1)^k$, t be a positive integer such that $tuv \mid N$ and p a prime. Then,

Theorem A.42. *Excluding the case $k = 2, \psi = \varphi = \mathbf{1}$, we have that*

$$T_p E_k^{\psi,\varphi,t} (\psi(p) + \varphi(p) p^{k-1}) E_k^{\psi,\varphi,t} \text{ if } uv = N \text{ or if } p \nmid N.$$

Moreover,

$$T_p E_2^{\mathbf{1},\mathbf{1},t} = (1 + \mathbf{1}(p)p) E_2^{\mathbf{1},\mathbf{1},t} \text{ if } t \text{ is a prime and } N \text{ is a power of } t \text{ or if } p \nmid N.$$

In addition,

$$\langle d \rangle E_k^{\psi,\varphi,t} = \chi(d) E_k^{\psi,\varphi,t} \text{ for all } d \text{ relatively prime to } N.$$

The last proposition hence shows that Eisenstein series are also eigenvectors of the Hecke operators.

Let us now give the definitions A.36 and A.38 for n a positive integer, not necessarily a prime number.

DEFINITION A.43. Let n be a positive integer.

1. $\begin{cases} \langle n \rangle = n \bmod N & \text{if } (n,N)=1 \\ \langle n \rangle = 0 & \text{if } (n,N)>1; \end{cases}$
2. $T_1 = 1$, $T_{p^r} = T_p T_{p^{r-1}} - p^{r-1}\langle p \rangle T_{p^{r-2}}$ for $r \geq 2$ so that $T_n = \prod T_{p_i^{e_i}}$ for $n = \prod p_i^{e_i}$.

The Hecke operators defined above define an algebra of endomorphisms of $\mathcal{S}_2(\Gamma_1(N))$.

DEFINITION A.44. 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, i.e. it is

$$\mathbb{T}_{\mathbb{Z}} = \mathbb{Z}[\{T_n, \langle n \rangle \mid n \in \mathbb{Z}_{>0}\}].$$

Analogously, we may define the Hecke algebra $\mathbb{T}_{\mathbb{C}}$ over $\mathbb{C}$.

A.6 Eigenforms

Let us provide the space $\mathcal{S}_k(\Gamma_1(N))$ of cusp forms with an inner product, called Petersson inner product. Then, on this space, let us notice that the two Hecke operators $\langle n \rangle$ and T_n, for $(n,N)=1$, are normal, i.e. they both have an adjoint operator that commutes with them.
Hence, from the Spectral Theorem of linear algebra, we obtain that, given a commutative family of normal operators on a finite dimensional space provided with an inner product, the space has an orthogonal basis of simoultaneous eigenvectors for the operators. Since each such vector is a modular form then it's called *eigenform*.

Theorem A.45. *The space $\mathcal{S}_k(\Gamma_1(N))$ of cusp forms has an orthogonal basis of simoultaneous eigenforms for the Hecke operators $\{\langle n \rangle, T_n \mid (n,N)=1\}$.*

A.7 Oldforms and newforms

DEFINITION A.46. Let d be a divisor of N and consider the map

$$i_d : \mathcal{S}_k(\Gamma_1(Nd^{-1})) \times \mathcal{S}_k(\Gamma_1(Nd^{-1})) \to \mathcal{S}_k(\Gamma_1(N)) \text{ given by } (f,g) \mapsto f + g[\alpha_d]_k$$

where $\alpha_d = \begin{pmatrix} d & 0 \\ 0 & 1 \end{pmatrix}$.

1. The subspace of $\mathcal{S}_k(\Gamma_1(N))$ of the *oldforms at level N* is

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

2. The subspace of $\mathcal{S}_k(\Gamma_1(N))$ of the *newforms at level N* is the orthogonal complement of the space of oldforms with respect to the Petersson inner product, i.e.
$$\mathcal{S}_k(\Gamma_1(N))^{new} = (\mathcal{S}_k(\Gamma_1(N))^{old})^{\perp}.$$

Proposition A.47. *The subspaces $\mathcal{S}_k(\Gamma_1(N))^{old}$ and $\mathcal{S}_k(\Gamma_1(N))^{new}$ are stable under the Hecke operators $\langle n\rangle$ and T_n for every positive integer n.*

A.8 Hecke eigenforms

Definition A.48. Let $f \in \mathcal{M}_k(\Gamma_1(N))$ be a non-zero modular form.

i. If f is an eigenform for the Hecke operators $\langle n\rangle$ and T_n for every positive integer n, then it is called a *(Hecke) eigenform*;

ii. The eigenform $f(\tau) = \sum_{n=0}^{\infty} a_n(f)q^n$ is said to be *normalized* if $a_1(f) = 1$;

iii. A normalized eigenform in $\mathcal{S}_k(\Gamma_1(N))^{new}$ is called a *newform*.

Remark A.49. Let $f \in \mathcal{S}_k(\Gamma_1(N))$ be an eigenform for the Hecke operators $\langle n\rangle$ and T_n for $(n, N) = 1$. Then, for every such an n, there exist eigenvalues $c_n, d_n \in \mathbb{C}$ such that $\langle n\rangle f = c_n f$ and $T_n f = d_n f$. Hence $d_n = a_n(f)/a_1(f)$ for $f(\tau) = \sum_{m=0}^{\infty} a_m(f)q^m$ Fourier expansion of f.

Appendix B

The Eichler-Shimura relation

In this appendix we will state all the definitions and theorems that will be useful for Chapter 4. All the results are taken from [9] Chapters 6-9.

B.1 Jacobian and abelian varieties

Let us consider X to be a compact Riemann surface of genus g, then we may see X as a sphere with g handles. Let $A_1, \dots, A_g$ be longitudinal loops around each handle and $B_1, \dots, B_g$ be latitudinal loops around each handle.

DEFINITION B.1. The *(first) homology group* $H_1(X, \mathbb{Z})$ *of* X is the free abelian group generated by integration over the A_i and the B_i of rank $2g$, i.e.

$$H_1(X, \mathbb{Z}) = \mathbb{Z}\int_{A_1} \oplus \cdots \oplus \mathbb{Z}\int_{A_g} \oplus \mathbb{Z}\int_{B_1} \oplus \cdots \oplus \mathbb{Z}\int_{B_g} \cong \mathbb{Z}^{2g}\,.$$

Hence the elements of $H_1(X, \mathbb{Z})$ are maps that sends holomorphic differentials on X to complex numbers. In fact, the homology group $H_1(X, \mathbb{Z})$ is a subgroup of the dual space $\Omega^1_{hol}(X)^\vee = \mathrm{Hom}_{\mathbb{C}}(\Omega^1_{hol}(X), \mathbb{C})$, where $\Omega^1_{hol}(X)$ is the space of the holomorphic differentials.

Then we may define the Jacobian of X.

DEFINITION B.2. The *Jacobian* of X is the quotient group

$$\mathrm{Jac}(X) = \Omega^1_{hol}(X)^\vee / H_1(X, \mathbb{Z}).$$

Moreover, this quotient is, complex analytically, a g-dimensional complex torus $\mathbb{C}^g/\Lambda_g$.

Let us now consider the function field $\mathbb{C}(X)$ of the compact Riemann surface X.

DEFINITION B.3. The *degree-0 divisor group of X* is

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

and the *subgroup of principal divisors* is

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

Then the *degree-0 divisor class group of X* (or the *degree-0 Picard group of X*) is

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

Let us consider the well-defined map

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

Then we have the following theorem.

Theorem B.4 (Abel's theorem)**.** *The map defined above descends to divisor classes inducing an isomorphism*

$$\mathrm{Pic}^0(X) \xrightarrow{\cong} \mathrm{Jac}(X) \text{ given by } [\sum_x n_x x] \mapsto \sum_x n_x \int_{x_0}^{x}.$$

Let us consider the compact modular curve $X_0(N)$ associated to the congruence subgroup $X_0(N)$. We denote its Jacobian by

$$J_0(N) = \mathrm{Jac}(X_0(N)).$$

Let Γ be congruence subgroup of $\mathrm{SL}_2(\mathbb{Z})$. By [9] Section 3.3, there exists a linear isomorphism $\varphi : \mathcal{S}_2(\Gamma) \to \Omega^1_{hol}(X(\Gamma))$, then, passing to the dual spaces, we obtain

$$\mathcal{S}_2(\Gamma)^\wedge = \varphi^\wedge(\Omega^1_{hol}(X(\Gamma))^\wedge).$$

Let now $H_1(X(\Gamma), \mathbb{Z})$ be denoting $\varphi^\wedge(\Omega^1_{hol}(X(\Gamma), \mathbb{Z}))$ for Γ a congruence subgroup of $\mathrm{SL}_2(\mathbb{Z})$ and let us define the Jacobian of $X(\Gamma)$.

DEFINITION B.5. The *Jacobian of $X(\Gamma)$* is

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

Since the double coset operator acts on Jacobians as composition with its action on modular forms[1] then we may state the following proposition for the double coset operators given by the Hecke operators T_n and $\langle d\rangle$.

Proposition B.6. *The Hecke operators $T = T_p, \langle d\rangle$ act by composition on the Jacobian associated to $\Gamma_1(N)$ as*

$$T : J_1(N) \to J_1(N) \text{ given by } [\psi] \mapsto [\psi \circ T] \text{ for } \psi \in \mathcal{S}_2(\Gamma_1(N))^\wedge$$

and similarly for T_p on $J_0(N)$.

[1] [9] pag.228 for details.

Hence we have that the Hecke algebra defined in A.44 consists of endomorphisms of the free finitely generated $\mathbb{Z}$-module $H_1(X_1(N), \mathbb{Z})$ and this leads to some facts.

Proposition B.7. *1. The Hecke algebra is a finitely generated $\mathbb{Z}$-module.*

2. Let $f(\tau) = \sum_{n\geq 1} a_n(f)q^n$, $q = e^{2\pi i\tau}$, be a normalized eigenform in $\mathcal{S}_2(\Gamma_1(N))$. Then the image $\mathbb{Z}[a_n(f)]$ of the homomorphism

$$\lambda_f : \mathbb{T} \to \mathbb{C} \text{ such that } Tf = \lambda_f(T)f$$

is a finitely-generated $\mathbb{Z}$-module. Hence it lies in the number field K_f generated by the Fourier coefficients of f. Then, if we set $I_f = \ker(\lambda_f) = \{T \in \mathbb{T}_{\mathbb{Z}} \mid Tf = 0\}$, we have $\mathbb{T}/I_f \cong \mathbb{Z}[a_n(f)] =: \mathcal{O}_f$ of rank $[K_f : \mathbb{Q}]$.

We are now ready to define the notion of abelian varieties associated to a normalized eigenform.

Definition B.8. Let f be a normalized eigenform in $\mathcal{S}_2(\Gamma_1(N))$. The *abelian variety associated to f* is defined as the quotient

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

Proposition B.9. *The abelian variety A_f is isomorphic to a complex torus of dimension $[K_f : \mathbb{Q}]$ where K_f is the number field of the newform $f \in \mathcal{S}_2(\Gamma_1(N))$.*

Then $\mathbb{T}_{\mathbb{Z}}/I_f$, and so its isomorphic image $\mathbb{Z}[\{a_n\}]$, acts on A_f. Moreover, since by Proposition B.7 $\lambda_f(T_p) = a_p(f)$, the following diagram commutes

$$\begin{array}{ccc} J_1(N) & \xrightarrow{T_p} & J_1(N) \\ \downarrow & & \downarrow \\ A_f & \xrightarrow{a_p(f)} & A_f \end{array}$$

where the map $a_p(f)$ is given by $(a_p(f)\varphi)(f^\sigma) = (a_p(f))^\sigma(\varphi(f))^\sigma$ for $\varphi \in A_f$, $\sigma : K_f \to \mathbb{C}$ embedding and $f^\sigma = \sum_{n\geq 1} a_n(f)^\sigma q^n$.

Then it is natural to expect that Jacobian factors through abelian varieties. For this, let us firstly give the notion of an isogeny.

Definition B.10. An *isogeny* is a holomorphic homomorphism between complex tori that surjects and has finite kernel.

Let us now define an equivalence relation $\sim$ on newforms given by $f' \sim f$ if, and only if, $f' = f^\sigma$ for some automorphism $\sigma : \mathbb{C} \to \mathbb{C}$. Every class $[f]$ has cardinality $[K_f : \mathbb{Q}]$ and it consists of newforms. Then:

Theorem B.11. *There exists an isogeny between the Jacobian associated to $\Gamma_1(N)$ and 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 $f \in \mathcal{S}_2(\Gamma_1(M_f))$ for M_f dividing N and m_f the number of divisors of N/M_f.

B.2 Modular curves as algebraic curves

Let us consider the modular curve $X_1(N)$ defined in A.24. This section shows that it can be seen as an algebraic curve over $\mathbb{Q}$.

Proposition B.12. *The field of meromorphic functions on $X_1(N)$ is*

$$\mathbb{C}(X_1(N)) = \mathbb{C}(j, f_1)$$

where $f_1(\tau) = \frac{g_2(\tau)}{g_3(\tau)}\wp_\tau(1/N)$, with g_2, g_3 suitable multiple of Eisenstein series and $\wp$ the Weierstrass function.

Let us now define the notion of a universal elliptic curve.

DEFINITION B.13. The *universal elliptic curve* E_j over $\mathbb{Q}(j)$ is given by

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

and has j-invariant the variable j.

Let $\mathcal{E}$ be an elliptic curve. For any positive integer N let us define the map

$$[N] : \mathcal{E} \to \mathcal{E} \text{ given by } [N]P = P + \cdots + P.$$

Then we denote by $\mathcal{E}[N]$ the group of N-torsion points of $\mathcal{E}$, i.e.

$$\mathcal{E}[N] = \{P \in \mathcal{E} \mid [N]P = 0_\mathcal{E}\}.$$

It is isomorphic to $(\mathbb{Z}/N\mathbb{Z})^2$.

Let us now consider the Galois group $H_\mathbb{Q} = \mathrm{Gal}(\mathbb{Q}(\mu_N, j, E_j[N])/\mathbb{Q}(j))$, where μ_N is the group of complex N-th roots of unity and $\mathbb{Q}(j)$ is the field of rational functions of j. Then the representation

$$\rho : H_\mathbb{Q} \to \mathrm{GL}_2(\mathbb{Z}/N\mathbb{Z}),$$

defined by

$$\begin{bmatrix} P_\tau^\sigma \\ Q_\tau^\sigma \end{bmatrix} = \rho(\sigma) \begin{bmatrix} P_\tau \\ Q_\tau \end{bmatrix}, \sigma \in H_\mathbb{Q},$$

describes how $H_\mathbb{Q}$ permutes $E_j[N]$.
Since μ_N is fixed by $\sigma \in H_\mathbb{Q}$, then we have that $H_\mathbb{Q} = (\mathbb{Q}(j, E_j[N])/(\mathbb{Q}(j))$.

Theorem B.14. *Let $H_\mathbb{Q}$ be the Galois group* $\mathrm{Gal}(\mathbb{Q}(j, E_j[N])/\mathbb{Q}(j))$. *Then there exists an isomorphism*

$$\rho : H_\mathbb{Q} \xrightarrow{\cong} \mathrm{GL}_2(\mathbb{Z}/N\mathbb{Z})$$

and every intermediate field K, with corresponding group $H_K \leq H_\mathbb{Q}$, is the function field of an algebraic curve over $\mathbb{Q}$ if, and only if, $\det\rho : H_K \to (\mathbb{Z}/N\mathbb{Z})^*$ *is surjective.*

Then, by [9] Section 7.7, we may see the modular curve $X_1(N)$ as an algebraic curve over $\mathbb{Q}$.

B.3 Reduction of curves to finite fields

In this section we will show that we can reduce algebraic curves over $\mathbb{Q}$ to algebraic curves over finite fields.

First of all, let us recall that the localization of $\mathbb{Z}$ at p is

$$\mathbb{Z}_{(p)} = \{x/y \mid x, y \in \mathbb{Z}, y \notin p\,\mathbb{Z}\},$$

that is a local subring of $\mathbb{Q}$ with maximal ideal $p\,\mathbb{Z}_{(p)}$. Since there exists a natural isomorphism $\mathbb{Z}/p\,\mathbb{Z} \cong \mathbb{Z}_{(p)}/p\,\mathbb{Z}_{(p)}$, then the reduction map

$$\sim\colon \mathbb{Z}_{(p)} \to \mathbb{F}_p \text{ given by } \tilde{\alpha} = \alpha + p\,\mathbb{Z}_{(p)}$$

is a well-defined surjective map.

Then, the definition of reducing an algebraic curve over $\mathbb{Q}$ to an algebraic curve over $\mathbb{F}_p$ uses the localization $\mathbb{Z}_{(p)}$.

Definition B.15. Let C be a non-singular affine algebraic curve over $\mathbb{Q}$, defined by polynomials $\varphi_1, \ldots, \varphi_m \in \mathbb{Z}_{(p)}[x_1, \ldots, x_n]$. Then C has *good reduction modulo p (or at p)* if

1. the ideal $I = (\varphi_1, \ldots, \varphi_m)$ of $\mathbb{Z}_{(p)}[x_1, \ldots, x_n]$ is prime;
2. the reduced polynomials $\tilde{\varphi_1}, \ldots, \tilde{\varphi_m} \in \mathbb{F}_p[x_1, \ldots, x_n]$ define a non-singular affine algebraic curve $\tilde{C}$ over $\mathbb{F}_p$.

In this case $\tilde{C}$ is the *reduction of C at p*.

Theorem B.16. *Let C be a non-singular projective algebraic curve over $\mathbb{Q}$ with good reduction at p. Then the reduction map $C \to \tilde{C}$ is surjective.*

Let us now study how maps between reductions work.

Theorem B.17. *Let C and C' be non-singular projective algebraic curves over $\mathbb{Q}$ with good reduction at p, C' with positive genus. Then, for any morphism $h : C \to C'$ over $\mathbb{Q}$ of non-singular projective algebraic curves over $\mathbb{Q}$ with good reduction at p, the following diagram commutes*

$$\begin{array}{ccc} C & \xrightarrow{h} & C' \\ \downarrow & & \downarrow \\ \tilde{C} & \xrightarrow{\tilde{h}} & \tilde{C}' \end{array}$$

Theorem B.18. *Let C be a non-singular projective algebraic curve over $\mathbb{Q}$ with good reduction at p. Then the map induced by reduction on degree-0 divisors*

$$\mathrm{Div}^0(C) \to \mathrm{Div}^0(\tilde{C}) \text{ given by } \sum n_P(P) \mapsto \sum n_P(\tilde{P})$$

induces a surjective map of Picard groups

$$\mathrm{Pic}^0(C) \to \mathrm{Pic}^0(\tilde{C}) \text{ given by } [\sum n_P(P)] \mapsto [\sum n_P(\tilde{P})].$$

B.4 The Eichler-Shimura relation

Let N be a positive integer, $p \nmid N$ a prime. In this section we will describe the Hecke operator T_p at the level of Picard groups of reduced modular curves, i.e.

$$\widetilde{T_p} : \mathrm{Pic}^0(\widetilde{X_1}(N)) \to \mathrm{Pic}^0(\widetilde{X_1}(N)).$$

Let us first define the notion of an enhanced elliptic curve for $\Gamma_1(N)$ and its moduli space.

DEFINITION B.19. An *enhanced elliptic curve for* $\Gamma_1(N)$ is an ordered pair (E, Q) where E is an elliptic curve and $Q \in E$ is a point of order N^2. Two such pairs (E, Q) and (E', Q') are equivalent if there exists an isomorphism $E \xrightarrow{\cong} E'$ taking Q to Q'.
The *moduli space* $S_1(N)$ *for* $\Gamma_1(N)$ is the set of equivalence classes $[E, Q]$.

Theorem B.20. *The moduli space $S_1(N)$ for $\Gamma_1(N)$ is in bijection with the modular curve $Y_1(N)$.*

Let now $\mathrm{Div}(S_1(N))$ be the divisor group of the moduli space $S_1(N)$. Then the Hecke operator T_p acts on it in the following way.

Proposition B.21. *There exists a map*

$$T_p : \mathrm{Div}(S_1(N)) \to \mathrm{Div}(S_1(N)) \text{ given by } [E, Q] \mapsto \sum_C [E/C, Q + C]$$

where the sum is taken over all order p subgroups $C \subseteq E$ such that $C \cap \langle Q \rangle = \{0_E\}$.

REMARK B.22. Since we are considering $p \nmid N$, in Proposition B.21 C is taken over all order p subgroups of E.

Moreover, let us define the reduction of an elliptic curve over the field of algebraic numbers $\overline{\mathbb{Q}}$.
The localization of the ring of algebraic integers $\overline{\mathbb{Z}}$ at a maximal ideal $\mathfrak{p}$ is

$$\overline{\mathbb{Z}}_{(\mathfrak{p})} = \{x/y \mid x, y \in \overline{\mathbb{Z}}, y \notin \mathfrak{p}\}.$$

Proposition B.23. *Let E be an elliptic curve over $\overline{\mathbb{Q}}$, $\mathfrak{p}$ be a maximal ideal of $\overline{\mathbb{Z}}$. Then the reduction $\tilde{E}$ is ordinary if $\tilde{E}[p] \cong \mathbb{Z}/p\mathbb{Z}$.*

Let us now study how reduction of equivalence classes in the moduli space $S_1(N)$ works.

Lemma B.24. *Let E be an elliptic curve over $\overline{\mathbb{Q}}$ with ordinary reduction at $\mathfrak{p}$, $Q \in E$ a point of order N, $p \nmid N$. Let C_0 be the kernel of the reduction map*

[2] i.e. $NQ = 0$ but $nQ \neq 0$ for every $0 < n < N$.

$E[p] \to \tilde{E}[p]$, i.e. an order-p-subgroup of E. Then, for any order-p-subgroup C of E, we have

$$[\widetilde{E/C}, \widetilde{Q/C}] = \begin{cases} [\widetilde{E}^{\sigma_p}, \widetilde{Q}^{\sigma_p}] & \text{if } C = C_0, \\ [\widetilde{E}^{\sigma_p^{-1}}, [p]\widetilde{Q}^{\sigma_p^{-1}}] & \text{if } C \neq C_0 \end{cases}$$

where $\sigma_p : x \to x^p$ is the Frobenius map.

REMARK B.25. By [9] Exercise 8.7.1, Lemma B.24 may be extended also to elliptic curves with supersingular reduction.

We are now ready to state the Eichler-Shimura relation.

Theorem B.26 (Eichler-Shimura relation)**.** *Let $p \nmid N$. Then the following diagram commutes*

$$\begin{array}{ccc} \mathrm{Pic}^0(X_1(N)) & \xrightarrow{T_p} & \mathrm{Pic}^0(X_1(N)) \\ \downarrow & & \downarrow \\ \mathrm{Pic}^0(\widetilde{X_1}(N)) & \xrightarrow{\widetilde{T_p}=\sigma_{p*}+\widetilde{\langle p \rangle}_* \sigma_p^*} & \mathrm{Pic}^0(\widetilde{X_1}(N)). \end{array}$$

where the upper and lower stars mean the pullback and pushforward maps.

B.5 Galois representations

Let now $\overline{\mathbb{Q}}$ be the algebraic closure of $\mathbb{Q}$ and $G_{\mathbb{Q}}$ the absolute Galois group $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$. For a prime $p \in \mathbb{Z}$, let $\mathfrak{p} \in \overline{\mathbb{Z}}$ be a maximal ideal over it and consider the reduction map $\overline{\mathbb{Z}} \to \overline{\mathbb{F}}_p$. Let now $G_{\mathbb{F}_p}$ be the absoulte Galois group of $\mathbb{F}_p$, then the reduction map

$$D_{\mathfrak{p}} = \{\sigma \in G_{\mathbb{Q}} \mid \sigma(\mathfrak{p}) = \mathfrak{p}\} \to G_{\mathbb{F}_p}$$

is surjective.

DEFINITION B.27. An *absolute Frobenius element over p* is any preimage $\mathrm{Frob}_{\mathfrak{p}} \in D_{\mathfrak{p}}$ of the Frobenius automorphism $\sigma_p \in G_{\mathbb{F}_p}$. It is defined up to the inertia group $I_{\mathfrak{p}} = \{\sigma \in D_{\mathfrak{p}} \mid \sigma(x) \equiv x \pmod{\mathfrak{p}} \text{ for all } x \in \overline{\mathbb{Z}}\}$ of $\mathfrak{p}$.

Theorem B.28. *For each maximal ideal $\mathfrak{p}$ of $\overline{\mathbb{Z}}$ lying over any but a finite set of rational primes p, choose an absolute Frobenius element $\mathrm{Frob}_{\mathfrak{p}}$. Then the set of such elements forms a dense subset of $G_{\mathbb{Q}}$.*

Let us now give the definition of a p-adic Galois representation.

DEFINITION B.29. Let d be a positive integer. A *d-dimensional p-adic Galois representation* is a continuous homomorphism

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

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

REMARK B.30. Every finite extension field L of $\mathbb{Q}_p$ is of the form K_λ for some number field K and maximal ideal $\lambda \mid p$ of $\mathcal{O}_K$. For such an L, the ring $\mathcal{O}_L = \mathcal{O}_{K,\lambda}$ is independent from K and λ. Moreover, the ring $\mathcal{O}_L$ is a lattice in L, i.e. there exists a $\mathbb{Z}_p$-basis of $\mathcal{O}_L$ that is also a $\mathbb{Q}_p$-basis of L.

DEFINITION B.31. Let ρ be a Galois representation and let p be a prime. Then ρ is unramified at p if $I_\mathfrak{p} \subseteq \ker \rho$ for any maximal ideal $\mathfrak{p} \subseteq \overline{\mathbb{Z}}$ lying over p.

Let us now give a second definition of p-adic Galois representation, where it is seen as a vector space over $\mathbb{Q}_p$ with $G_\mathbb{Q}$-module structure.

DEFINITION B.32. Let d be a positive integer. A *d-dimensional p-adic Galois representation* is a d-dimensional topological vector space V over L, where L is a finite extension field of $\mathbb{Q}_p$, that is also a $G_\mathbb{Q}$-module such that the action

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

is continuous. If V' is another such representation and there exists a continuous $G_\mathbb{Q}$-module isomorphism of L-vector spaces $V \xrightarrow{\cong} V'$, then V and V' are equivalent.

Using Definition B.32, we have

Proposition B.33. *Let $\rho : G_\mathbb{Q} \to \mathrm{GL}_d(L)$ be a Galois representation. Then ρ is similar to a Galois representation $\rho' : G_\mathbb{Q} \to \mathrm{GL}_d(\mathcal{O}_L)$.*

B.6 Galois representations and modular forms

In this section we will associate Galois representations to modular curves and then we will decompose them into 2-dimensional representations associated to modular forms.

Let N be a positive integer, p a prime and $X_1(N)$ a modular curve, i.e. a projective non-singular algebraic curve over $\mathbb{Q}$, with genus g.

DEFINITION B.34. The *p-adic Tate module of $X_1(N)$* is

$$\mathrm{Tal}_p(\mathrm{Pic}^0(X_1(N))) = \varprojlim_n \{\mathrm{Pic}^0(X_1(N))[p^n]\}.$$

REMARK B.35. The p-adic Tate module $\mathrm{Tal}_p(\mathrm{Pic}^0(X_1(N)))$ is isomorphic to $\mathbb{Z}_p^{2g}$.

Since for every n there exists a commutative diagram of the form

$$\begin{array}{ccc} & G_\mathbb{Q} & \\ \swarrow & & \searrow \\ \mathrm{Aut}(\mathrm{Pic}^0(X_1(N))[p^n]) & \longleftarrow & \mathrm{Aut}(\mathrm{Pic}^0(X_1(N))[p^{n+1}]) \end{array},$$

we have a continuous homomorphism

$$\rho_{X_1(N),p} : G_\mathbb{Q} \to \mathrm{GL}_{2g}(\mathbb{Z}_p) \subseteq \mathrm{GL}_{2g}(\mathbb{Q}_p)$$

that is the $2g$-dimensional Galois representation attached to $X_1(N)$.

Let us now study how the Hecke operator acts on Tate modules.

Theorem B.36. *Let p be a prime, N a positive integer. The Galois representation $\rho_{X_1(N),p}$ is unramified at every prime $l \nmid pN$. For any such p, let $\mathfrak{p} \subseteq \overline{\mathbb{Z}}$ be any maximal ideal over p. Then $\rho_{X_1(N),p}(\mathrm{Frob}_{\mathfrak{p}})$ satisfied the polynomial equation*

$$x^2 - T_l x + \langle l \rangle l = 0.$$

Up to this point we have defined Tate modules for Picard groups. Let us now study Tate modules for modular forms.

DEFINITION B.37. Let $f \in \mathcal{S}_2(N, \chi)$ be a normalized eigenform. The *p-adic Tate module* for the abelian variety A_f is

$$\mathrm{Tal}_p(A_f) = \varprojlim_n \{A_f[p^n]\} \cong \mathbb{Z}_p^{2d}$$

where $d = [K_f : \mathbb{Q}]$.

Let us now notice that the absolute Galois group $G_{\mathbb{Q}}$ acts on $\mathrm{Tal}_p(A_f)$.

Lemma B.38. *The map $\mathrm{Pic}^0(X_1(N))[p^n] \to A_f[p^n]$ is a surjection and its kernel is stable under $G_{\mathbb{Q}}$.*

Hence $G_{\mathbb{Q}}$ acts on $A_f[p^n]$ and so also on $\mathrm{Tal}_p(A_f)$. Choosing coordinates appropriately we obtain a Galois representation

$$\rho_{A_f,p} : G_{\mathbb{Q}} \to \mathrm{GL}_{2d}(\mathbb{Q}_p)$$

unramified at all primes $l \nmid pN$. Moreover, for every maximal ideal $\mathfrak{p} \subseteq \overline{\mathbb{Z}}$ over l, we have that $\rho_{A_f,p}(\mathrm{Frob}_{\mathfrak{p}})$ satisfies the polynomial equation

$$x^2 - a_p(f)x + \chi(p)p = 0.$$

The Tate module $\mathrm{Tal}_p(A_f)$ has rank $2d$ over $\mathbb{Z}_p$ and the tensor product $V_p(A_f) = \mathrm{Tal}_p(A_f) \otimes \mathbb{Q}$ is a module over $K_f \otimes_{\mathbb{Q}} \mathbb{Q}_p = \prod_{\lambda|l} K_{f,\lambda}$. Moreover:

Lemma B.39. *$V_p(A_f)$ is a free module of rank 2 over $K_f \otimes_{\mathbb{Q}} \mathbb{Q}_p$.*

Then the absolute Galois group $G_{\mathbb{Q}}$ acts linearly on $V_p(A_f) \cong (K_f \otimes_{\mathbb{Q}} \mathbb{Q}_p)^2$. Finally, we have the 2-dimensional representation associated to modular forms.

Theorem B.40. *Let $f \in \mathcal{S}_2(N, \chi)$ be a normalized eigenform with number field K_f. Let p be a prime. For each maximal ideal λ of $\mathcal{O}_{K_f}$ lying over p there exists a 2-dimensional Galois representation*

$$\rho_{f,\lambda} : G_{\mathbb{Q}} \to \mathrm{GL}_2(K_{f,\lambda}).$$

This representation is unramified at every prime $l \nmid pN$ and for every maximal ideal $\mathfrak{p} \subseteq \overline{\mathbb{Z}}$ over l we have that $\rho_{f,\lambda}(\mathrm{Frob}_{\mathfrak{p}})$ satisfies the polynomial equation

$$x^2 - a_l(f)x + \chi(l)l = 0.$$

In particular, if $f \in \mathcal{S}_2(\Gamma_0(N))$, then the relation is $x^2 - a_p(f)x + p = 0$.

Bibliography

[1] Z.I. Borevich, I.R. Shafarevich, Number theory. New York: Academic Press 1966

[2] L. Carlitz, F. Olson, Maillet's determinant. A.M.S. 6, 265-269 (1955)

[3] C. Chevalley, Introduction to the theory of algebraic functions of one variable. A.M.S. 6 (1951)

[4] G. Cornell, J.H. Silverman, G. Stevens, Arithmetic Geometry. Springer-Verlag 1986

[5] C. Curtis, I. Reiner, Representation theory of finite groups and associative algebras. A.M.S. 2006

[6] P. Deligne, La conjecture de Weil: I. Publications Mathématiques de l'IHÉS, Tome 43 (1974), pp. 273-307

[7] P. Deligne, M. Rapoport, Les schémas de modules de courbes elliptiques. International Summer School on Modular Functions, Antwerp 1972

[8] P. Deligne, J-P. Serre, Formes modulaires de poids 1. Annales scientifiques de l'É.N.S. 4e série, tome 7, no 4 (1974), p. 507-530

[9] F. Diamond, J. Shurman, A first course in modular forms. Springer 2005

[10] C. Ericson, Ribet's converse to Herbrand's Theorem. Unpublished notes (2008)

[11] W. Fulton, J. Harris, Representation theory, a first course. Springer 2004

[12] R. Greenberg, A generalization of Kummer's criterion. Inventiones math. 21,247- 254 (1973)

[13] J. Herbrand, Sur les classes des corps circulaires. J. Math. Pures et Appliquées, 9 série 11,417-441 (1932)

[14] C. Khare, Notes on Ribet's converse to Herbrand. Online notes

[15] S. Lang, Cyclotomic fields 1 and 2. Springer 1990

[16] S. Lang, Introduction to modular forms. Springer 1976

[17] J.S. Milne, Abelian varieties. Online notes (2008)

[18] M. Raynaud, Schémas en groups de type $(p, \ldots, p)$. Bull. Soc. Math. France 102, 241-280 (1974)

[19] K.A. Ribet, A modular construction of unramified p-extension of $\mathbb{Q}(\mu_p)$. Inventiones math. 34, 151-162 (1976)

[20] A. Saikia, Ribet's construction of a suitable cusp eigenform. arXiv:0910.1408 [math.NT]

[21] J.P. Serre, Abelian l-adic representations and elliptic curves. New York: Benjamin 1968

[22] J. Tate, Global class field theory. In: Algebraic number theory. Washington: Thompson 1967

[23] L. Washington, Introduction to cyclotomic fields. Springer 1997

Ich habe die Arbeit selbständig verfasst, keine anderen als die angegebenen Quellen unf Hilfsmittel benutzt und bisher keiner anderen Prüfungsbehörde vorgelegt. Außerdem bestätige ich hiermit, dass die vorgelegten Druckexemplare und die vorgelegte elektronische Version der Arbeit identisch sind und dass ich von den in §26 Abs. 6 vorgesehenen Rechtsfolgen Kenntnis habe.

Unterschrift: