Galois Representations and Theta Operators for Siegel Modular Forms

Author:
Angus McAndrew

Supervisor:
Dr. Alex Ghitza

Submitted in total fulfillment of the requirements of the degree of Master of Philosophy

School of Mathematics and Statistics, The University of Melbourne

Abstract

Modular forms are powerful number theoretic objects, having attracted much study and attention for the last 200 years. In the modern area, one of their primary points of interest is their role in the *Langlands program*. The work of Deligne (see [Del71]) and Serre (see [S$^+$87]) provided a connection between modular forms and Galois representations. An integral piece of this connection is the *theta operator*, which allows tight manipulation of the modular forms and Galois representations.

There is a larger picture, in which modular forms are merely a special instance of objects known as *Siegel modular forms*. In this thesis, we describe generalisations of the above concepts and theories to the Siegel case. We first demonstrate some generalisations of the theta operator, and subsequently describe the connection between Siegel modular forms and Galois representations. Finally we give a description of the effect of the theta operator on the Galois representations which are conjecturally arising from these Siegel modular forms.

Declaration

This is to certify that

(i) the thesis comprises only my original work towards the MPhil except where indicated in the Preface,

(ii) due acknowledgement has been made in the text to all other material used,

(iii) the thesis is less than 50 000 words in length, exclusive of tables, maps, bibliographies and appendices.

Angus McAndrew

Preface

This thesis expects no more background than could be reasonably acquired through some introductory material on algebraic geometry, Galois theory and representation theory. There are several sections to cover background and necessary definitions to give the reader a sufficient understanding of the context of the work.

- Chapter 1 (Introduction) describes the problem we considered.
- Chapter 2 provides preliminaries for the theory of modular forms.
- Chapter 3 generalises this to Siegel modular forms
- Chapter 4 discusses some representation theory of algebraic groups. This is largely done to set up the language required for chapters 7 and 8.
- Chapter 5 defines the Hecke operators and describes the structure of the Hecke algebra.
- Chapter 6 defines the Theta operator on modular forms, as well as some generalisations for Siegel modular forms. Commutation relations with the Hecke operator are described here.
- Chapter 7 demonstrates the connection between Galois representations and modular forms, and the role the theta operator plays in this.
- Chapter 8 is focused on the Satake isomorphism, which links a Hecke algebra to a representation ring. From this we define the Satake parameters attached to a modular form.
- Chapter 9 is the culmination of the above in providing a connection between Galois representations and *Siegel* modular forms. We further demonstrate how the generalisations of the theta operator interact with this connection.

Acknowledgements

I would like to thank Alex Ghitza for suggesting the project and being a source of help and inspiration throughout this work. All of the research and results I have achieved in mathematics has been because of him, and I am truly grateful. I hope that we will have many opportunities to continue to work together in the future.

Thank you also to Arun Ram and Lawrence Reeves for their positions on my supervisory panel. It was a great help to have additional minds to bounce my work off, and more people to push me to my best during our review meetings.

I'd like to thank all my friends and family for giving me the life that has led to this moment. It's because of all of you that I'm able to be the person I am and do the work that I do, and you're all important to me in so many ways.

Finally, I'd like to thank my wonderful girlfriend Mai. For being the guiding light that kept me on course, and making sure that I was the happiest and strongest person I could be at all times. You are wonderful and I love you so much. Thank you for being a part of me. Always know that anything I can achieve is because of you.

Contents

Chapter 1

Introduction

We begin by considering the set of algebraic numbers $\overline{\mathbb{Q}}$. This is a grand and mysterious object in mathematics, puzzling number theorists for centuries. Its structure is fascinating and much has been done in an attempt to study it. Galois theory leads us to consider the automorphism group $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$, also known as the *absolute Galois group of* $\mathbb{Q}$. Then, to understand this group, representation theory leads us to consider group homomorphisms of the form $\rho : \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \to \mathrm{GL}(V)$. These are known as *Galois representations*, and connect to many other objects in mathematics. In particular, they are closely related to *modular forms*. This thesis will be devoted to the use of modular forms to understand Galois representations.

Modular forms are one of the most powerful objects in modern number theory. Originally viewed as objects which were both analytic and highly arithmetic, modern advances in the theory have given them a place in algebra and geometry. Perhaps the most remarkable property is their position in the Langlands program, the far-reaching suite of conjectures relating objects from various areas of mathematics. Part of this is the connection to the aforementioned Galois representations. Specifically, fix a prime p and we will consider modular forms and Galois representations in the circumstance where the coefficients are taken $\pmod p$. Now, given a modular eigenform

f, Deligne in [Del71] proved that there exists a Galois representation ρ_f with properties inherited from f.

The truly powerful nature of this correspondence is that it goes both ways. From this point on we will make things slightly more precise by fixing a prime p. Originally conjectured by Serre, see [S$^+$87], we have the following.

Theorem 1.1 (Serre's Conjecture)**.** *Let $\rho : \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \to \mathrm{GL}_2(\overline{\mathbb{F}}_p)$ be a semisimple, odd Galois representation. Then there exists a modular form f such that $\rho_f \cong \rho$.*

This is now known, proved by Khare and Wintenberger, see [KW10]. So we can fully exploit the theory of modular forms in our goal to understand, fundamentally, $\overline{\mathbb{Q}}$. Some of the critical features of modular forms that affect this correspondence are the Hecke eigenvalues a_ℓ and the weight k. One of the primary tools for manipulating these is the *theta operator* θ on modular forms. Then, one has the following remarkable and useful theorem.

Theorem 1.2.

$$\rho_{\theta f} = \chi \otimes \rho_f, \tag{1.1}$$

where χ is the Cyclotomic character (mod p).

This forms an important part of the proof of Serre's conjecture.

The unfortunate thing to notice is that we are fairly limited in the representations we can produce in this way. For example, they always take image in GL_2, which is due to modular forms being automorphic objects related to the algebraic group GL_2. They are generalised by objects called *Siegel modular forms*, which are attached to the algebraic group GSp_{2g}, which for $g = 1$ is precisely GL_2. In this case, the correspondence is conjectural, sending a Siegel modular eigenform f to a homomorphism $\rho_f : \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \to \mathrm{GSpin}_{2g+1}(\overline{\mathbb{F}}_p)$, since GSpin_{2g+1} is the dual group of GSp_{2g}. The construction uses the Satake parameters attached to a form f via the Satake isomorphism.

Now, how can we generalise the theta operator? It turns out that there are multiple generalisations, any of which can be fruitfully studied:

- Boecherer-Nagaoka have defined an operator in [BN07], which we denote $\theta_{BN} : M_k \to M_{k+p+1}$, using Rankin-Cohen brackets.

- Flander-Ghitza have defined an operator in [Fla13], which we denote $\theta_{FG} : M_\kappa \to M_{\kappa\otimes\mathrm{Sym}^2\otimes\det^{p-1}}$, using algebraic geometry.

- In the case $g = 2$, Yamauchi uses algebraic geometry in [Yam14] to define analogues of both operators above.

We look at the effect of some of the operators above on Galois representations, and attain the following result.

Theorem 1.3. *Let λ be a dominant coweight of* GSp_{2g}.
Let η be the symplectic similitude character of GSp_{2g} *and $\eta^\vee$ the corresponding cocharacter of* GSpin_{2g+1}.

(1) Let $f \in M_\kappa(\Gamma; \mathbb{F}_p)$ be a degree g, weight κ, level N Siegel eigenform. Then

$$\rho_{\theta_{FG} f} = (\eta^\vee \circ \chi) \otimes \rho_f, \tag{1.2}$$

where χ is the cyclotomic character (mod p).

(2) Let $f \in M_k(\Gamma; \mathbb{F}_p)$ be a degree g, weight k, level N Siegel eigenform. Then

$$\rho_{\theta_{BN} f} = (\eta^\vee \circ \chi)^g \otimes \rho_f, \tag{1.3}$$

with χ as above.

There are other results from other authors on the theta operators above.

- There are results studying *theta cycles* for θ_{BN} in [CCR11], [DR10], and [RR14].

- Yamauchi in [Yam14] has generalised some *weight in Serre's conjecture*-type results to $g = 2$, looking at the algebro-geometric theta operators mentioned above.

Chapter 2

Modular Forms

Modular forms are examples of *automorphic forms*. Modularity refers to special transformation rules coming from the action of so called "modular groups". For modular forms, we are interested in functions on the upper-half plane $\mathfrak{G}_1 = \{z \in \mathbb{C} |\, \mathrm{Im}(z) > 0\}$ with action coming from the group $\mathrm{SL}_2(\mathbb{Z})$. (For the reasoning behind this nonstandard notation, see chapter 3.)

Specifically, we will consider the action

$$\gamma z = \frac{az+b}{cz+d}, \tag{2.1}$$

where $z \in \mathfrak{G}_1$ and $\gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{SL}_2(\mathbb{Z})$. We also have the following *factor of automorphy* for the above action:

$$j_\gamma(z) = cz + d, \tag{2.2}$$

with γ and z as above.

2.1 Modular Forms of Level 1

We are now in a position to give the basic definition of our craft.

Definition 2.1 (Modular Form)**.** A *modular form of weight k and level 1* is a holomorphic function $f : \mathfrak{H}_1 \to \mathbb{C}$ such that

$$f(\gamma z) = j_\gamma^k(z) f(z), \tag{2.3}$$

and f is *holomorphic at infinity.*

Note that choosing $\gamma = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$ we see that a modular form is $\mathbb{Z}$-periodic, and thus has a Fourier expansion

$$f(q) = \sum_{n=-\infty}^{\infty} a(n) q^n, \quad \text{where} \quad q = e^{2\pi i z}. \tag{2.4}$$

The words *holomorphic at infinity* mean that $a(n) = 0$ for all $n < 0$.

Remark 2.2. One may wonder from whence equation (2.3) arises. One way is to think of a modular form as a *differential form*, rather than a function. Given f, a modular form of weight k, one can show

$$f(\gamma z)(d(\gamma z))^{k/2} = f(z)(dz)^{k/2}. \tag{2.5}$$

We will return to this idea in section 2.4.

We also introduce some special types of modular forms:

Definition 2.3 (Cusp Form)**.** A *cusp form* is a modular form which *vanishes at ∞*, i.e. $a(0) = 0$.

Remark 2.4. For a fixed weight k, the set $M_k(\mathrm{SL}_2(\mathbb{Z}))$ of modular forms of weight k is a $\mathbb{C}$-vector space, and the set $S_k(\mathrm{SL}_2(\mathbb{Z}))$ of cusp forms of weight k is a subspace. Further

$$M_*(\mathrm{SL}_2(\mathbb{Z})) = \bigoplus_{k \in \mathbb{Z}} M_k(\mathrm{SL}_2(\mathbb{Z})) \tag{2.6}$$

is a graded $\mathbb{C}$-algebra and

$$S_*(\mathrm{SL}_2(\mathbb{Z})) = \bigoplus_{k \in \mathbb{Z}} S_k(\mathrm{SL}_2(\mathbb{Z})) \tag{2.7}$$

is an ideal.

We now turn to some examples of modular forms.

Example 2.5.

- Consider the *Eisenstein series of weight k*

$$G_k(z) = \sum_{m,n \in \mathbb{Z}^2 \setminus \{(0,0)\}} \frac{1}{(mz+n)^k}. \tag{2.8}$$

  This is a modular form of weight k as long as $k \geq 4$ is even. It has Fourier expansion

$$G_k(q) = 2\zeta(k) \left(1 - \frac{2k}{B_k} \sum_{n=1}^{\infty} \sigma_{k-1}(n) q^n \right), \tag{2.9}$$

  where B_k is the kth Bernoulli number, and σ_{k-1} is the divisor function. It is often convenient to rescale it to

$$E_k(q) = 1 - \frac{2k}{B_k} \sum_{n=1}^{\infty} \sigma_{k-1}(n) q^n. \tag{2.10}$$

- Consider the *modular discriminant*

$$\Delta(z) = \frac{1}{1728} \left(E_4(z)^3 - E_6(z)^2 \right). \tag{2.11}$$

  This is a cusp form of weight 12. It has Fourier expansion

$$\Delta(q) = q \prod_{j=1}^{\infty} (1-q^n)^{24} = \sum_{n=1}^{\infty} \tau(n) q^n, \tag{2.12}$$

  where $\tau(n)$ is the *Ramanujan tau function*.

As it turns out, we can build all modular forms of level 1 from these examples:

Theorem 2.6.

$$M_*(\mathrm{SL}_2(\mathbb{Z})) = \mathbb{C}[E_4, E_6] \quad \textit{and} \quad S_*(\mathrm{SL}_2(\mathbb{Z})) = \Delta \cdot \mathbb{C}[E_4, E_6]. \tag{2.13}$$

Proof. See [DS05], §3.5, Theorem 3.5.2. □

2.2 Modular forms of level N

Let $N \in \mathbb{Z}$. Consider the reduction (mod N) map

$$\mathrm{SL}_2(\mathbb{Z}) \longrightarrow \mathrm{SL}_2(\mathbb{Z}/N\mathbb{Z}). \tag{2.14}$$

Then we define the *principal congruence subgroup* of $\mathrm{SL}_2(\mathbb{Z})$,

$$\begin{aligned}\Gamma(N) &= \ker\left(\mathrm{SL}_2(\mathbb{Z}) \longrightarrow \mathrm{SL}_2(\mathbb{Z}/N\mathbb{Z})\right) \qquad (2.15)\\ &= \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{SL}_2(\mathbb{Z}) \;\middle|\; \begin{pmatrix} a & b \\ c & d \end{pmatrix} \equiv \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \pmod{N} \right\}.\end{aligned}$$

More generally:

Definition 2.7 (Congruence Subgroup)**.** Let $N \in \mathbb{Z}$. A *congruence subgroup of level* N of $\mathrm{SL}_2(\mathbb{Z})$ is a subgroup $\Gamma \subseteq \mathrm{SL}_2(\mathbb{Z})$ such that $\Gamma(N) \subseteq \Gamma$.

Example 2.8. Besides the principal congruence subgroup, the most important congruence subgroups of $\mathrm{SL}_2(\mathbb{Z})$ are

$$\begin{aligned}\Gamma_0(N) &= \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{SL}_2(\mathbb{Z}) \;\middle|\; \begin{pmatrix} a & b \\ c & d \end{pmatrix} \equiv \begin{pmatrix} * & * \\ 0 & * \end{pmatrix} \pmod{N} \right\},\\ \Gamma_1(N) &= \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{SL}_2(\mathbb{Z}) \;\middle|\; \begin{pmatrix} a & b \\ c & d \end{pmatrix} \equiv \begin{pmatrix} 1 & * \\ 0 & 1 \end{pmatrix} \pmod{N} \right\}. \qquad (2.16)\end{aligned}$$

Note that $\Gamma(N) \subseteq \Gamma_1(N) \subseteq \Gamma_0(N)$. To apply these to modular forms, we introduce the *weight k slash operator* [1]

$$(f|_k\gamma)(z) = j_\gamma(z)^{-k} f(\gamma z) \tag{2.17}$$

for $\gamma \in \mathrm{SL}_2(\mathbb{Z})$. We are now in a position to define modular forms with what is known as a *level structure* as follows:

Definition 2.9 (Modular form of level N)**.** Let $N \in \mathbb{Z}$ and let Γ be a congruence subgroup of level N. A *modular form of level N and weight k* is a holomorphic function $f : \mathfrak{G}_1 \to \mathbb{C}$ such that

$$f(\gamma z) = j_\gamma^k(z) f(z), \quad \text{for} \quad \gamma \in \Gamma \tag{2.18}$$

and $(f|_k\gamma)(z)$ is holomorphic at infinity for all $\gamma \in \mathrm{SL}_2(\mathbb{Z})$.

[1] There is a more general action that we don't need here, see chapter 5, definition 5.1

Remark 2.10. Note that $(f|_k\gamma)(z) = f(z)$ if $\gamma \in \Gamma$.

Further, despite the above definition referring universally to *level* N forms, these are in fact distinct spaces for different choices of group Γ. There are good reasons to choose to work with any of the groups described above, and when we wish to discuss specific spaces, we will make clear our choice of group Γ.

There are some subtleties to this definition. First of all, the matrix $T = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$ is not generally an element of Γ. Specifically with the cases above, $T \in \Gamma_0(N), \Gamma_1(N)$, but $T \notin \Gamma(N)$. So when we don't have the matrix T in our group Γ, then f is not $\mathbb{Z}$-periodic and doesn't have an expansion in terms of q. However, the matrix $\begin{pmatrix} 1 & N \\ 0 & 1 \end{pmatrix} \in \Gamma$, and thus f will have a Fourier expansion in the variable $q^{1/N}$ as

$$f(q) = \sum_{n=-\infty}^{\infty} a(n) q^{n/N}. \tag{2.19}$$

Holomorphicity at infinity is the same, $a(n) = 0$ for all $n < 0$, we now just add that it must hold for certain other series expansions, since in general $f|_k\gamma \neq f$.

Remark 2.11. The spaces of modular forms for a group Γ are denoted $M_k(\Gamma)$. We also have cusp forms in the same way as above, with the spaces denoted $S_k(\Gamma)$. Further, the above inclusions of groups is reversed for spaces of modular forms, that is

$$M_k(\Gamma_0(N)) \subseteq M_k(\Gamma_1(N)) \subseteq M_k(\Gamma(N)). \tag{2.20}$$

Note that $\Gamma_0(N)/\Gamma_1(N) \cong (\mathbb{Z}/N\mathbb{Z})^\times$. Thus, given an element $\gamma \in \Gamma_0(N)$ and a form $f \in M_k(\Gamma_1(N))$ we can compute $f|\gamma$. By the above quotient, this can be expressed as action by an element $d \in (\mathbb{Z}/N\mathbb{Z})^\times$, which is called the *diamond operator* and written $\langle d \rangle f$.

Definition 2.12 (Modular form of type (N, ε))**.** Let $\varepsilon : (\mathbb{Z}/N\mathbb{Z})^\times \to \mathbb{C}^\times$ be a character. A *modular form of type* (N, ε) is a form $f \in M_k(\Gamma_1(N))$ such that $\langle d\rangle f = \varepsilon(d)f$. The space of modular forms of type (N, ε) is denoted $M_k(\Gamma_1(N), \varepsilon)$.

Proposition 2.13. *We have decompositions*

$$M_k(\Gamma_1(N)) = \bigoplus_{\varepsilon:(\mathbb{Z}/N\mathbb{Z})^\times \to \mathbb{C}^\times} M_k(\Gamma_1(N), \varepsilon)$$
$$S_k(\Gamma_1(N)) = \bigoplus_{\varepsilon:(\mathbb{Z}/N\mathbb{Z})^\times \to \mathbb{C}^\times} S_k(\Gamma_1(N), \varepsilon),$$

where the sums run over all characters of $(\mathbb{Z}/N\mathbb{Z})^\times$.

Proof. See Lemma 4.3.1 in [Miy06]. □

Remark 2.14. One of the summands above corresponds to the trivial character, i.e. forms in that summand satisfy $\langle d\rangle f = f$. This means that they are fixed not just under $\Gamma_1(N)$, but under all of $\Gamma_0(N)$. Thus we have $M_k(\Gamma_1(N), \mathrm{triv}) = M_k(\Gamma_0(N))$.

Results on modular forms of level N often rely heavily on the group $\Gamma_1(N)$ and a choice of character ε. To pass to a result on $\Gamma_0(N)$, one can use the same result, but merely consider the character to be trivial. Passing to a result on $\Gamma(N)$ (often referred to as *full* level structure) is more subtle, since $M_k(\Gamma(N))$ is a larger space. For that, we have the following group homomorphism,

$$\begin{array}{ccc} \Gamma_1(N^2) & \longrightarrow & \Gamma(N) \\ \begin{pmatrix} a & b \\ c & d \end{pmatrix} & \longmapsto & \begin{pmatrix} a & bN \\ c/N & d \end{pmatrix}. \end{array} \tag{2.21}$$

This allows us to compare forms for Γ and Γ_1, though the actual level N may change.

2.3 Modular forms (mod p)

One often writes $M_k(\Gamma)$ above as $M_k(\Gamma; \mathbb{C})$, and the definition we have provided above is often referred to as the definition "over $\mathbb{C}$". One way to generalise this is to consider the rings in which the Fourier coefficients reside. For each k, we have the *q-expansion map*,

$$\begin{array}{rccc} Q_k: & M_k(\Gamma;\mathbb{C}) & \longrightarrow & \mathbb{C}[[q]] \\ & f & \longmapsto & f(q). \end{array} \tag{2.22}$$

With this, we now define the following:

Definition 2.15 (Modular forms over R)**.** Let $R \subseteq \mathbb{C}$ be a subring of $\mathbb{C}$. The set of *modular forms of weight k over R* is

$$M_k(\Gamma; R) := Q_k^{-1}(R[[q]]). \tag{2.23}$$

With this we can choose $R = \mathbb{Z}$ and get the set of modular forms with integral coefficients. Now we can construct modular forms with coefficients in any $\mathbb{Z}$-algebra B by

$$M_k(\Gamma; B) := B \otimes_{\mathbb{Z}} M_k(\Gamma; \mathbb{Z}). \tag{2.24}$$

Specifically, we can choose $B = \mathbb{F}_p$ or $B = \overline{\mathbb{F}}_p$ and this gives the theory of modular forms (mod p). The reason to choose the algebraic closure will be discussed in chapter 5.

At this stage, we'd like to note that the q-series $E_{p-1}(q) \pmod p = 1$.

Definition 2.16 (Hasse Invariant)**.** The *Hasse Invariant* is the form $A = E_{p-1} \in M_*(\Gamma; \overline{\mathbb{F}}_p)$.

This turns out to be on of the more remarkable features of the theory of (mod p) modular forms. In particular, it will play a role in chapter 6.

2.4 Algebraic Geometry

This section primarily follows [Kat73]. We will not revise basic scheme-theoretic definitions, but invite the reader to consider [Har77] for the background material.

One may wonder at the motivation behind the study of these modular forms we have defined. In fact, they relate in a very deep way to many powerful and interesting number-theoretic objects. One major area of interest in number theory is the study of *elliptic curves*. These may be familiar in the guise below (see Example 2.21), but we will begin by viewing them more generally.

Definition 2.17 (Elliptic Curve)**.** An *elliptic curve* over a scheme S is a proper smooth morphism $p : E \to S$ such that the geometric fibres are connected curves of genus 1, and a section $e : S \to E$.

These objects are endowed with much more structure than is immediately apparent from the definition. In fact, they form a commutative group scheme over the base S (see [KM85] Theorem 2.1.2). We will now explore the structure that is useful to the definition of modular forms.

Remark 2.18. Let $\Omega^1_{E/S}$ be the sheaf of differential 1-forms on E relative to S. We can push this forward to a sheaf on S via p. We thus define the (invertible) sheaf $\underline{\omega}_{E/S} = p_*(\Omega^1_{E/S})$.

For simplicity, we will consider the case for which the scheme S is in fact $\operatorname{Spec}(R)$ for a ring R. In this context, we will often write E/R to refer to the elliptic curve $E/\operatorname{Spec}(R)$ in the notation above. We can now define modular forms of level 1, as follows.

Definition 2.19 (Modular Form)**.** An *modular form of weight k and level 1* is a function which associates to each pair $(E/R, \omega)$, where ω is a global section of the sheaf $\underline{\omega}_{E/R}$ on $\operatorname{Spec}(R)$, an element $f(E/R, \omega) \in R$ such that

(1) If $E'/R \cong E/R$, then $f(E/R, \omega) = f(E'/R, \omega')$.

(2) If $\lambda \in R^\times$ (the multiplicative group of R), then

$$f(E/R, \lambda\omega) = \lambda^{-k} f(E/R, \omega) \tag{2.25}$$

(3) If $g : R \to R'$ is a morphism of rings, then

$$f(E_{R'}/R', \omega_{R'}) = g(f(E/R, \omega)). \tag{2.26}$$

Remark 2.20. (1) If we only consider rings defined over a fixed ring R_0 (i.e. only R_0-algebras), then the set of weight k modular forms for all such rings R is the *R_0-module of weight k level 1 modular forms over R_0*.

(2) Compared to the modular forms we defined in definition 2.1, the forms defined here are not necessarily *holomorphic at infinity.* To ensure that, as above, we have to introduce a notion of a series expansion of a form. We can do this abstractly by considering an elliptic curve over the R_0-algebra $R = \mathbb{Z}((q)) \otimes_{\mathbb{Z}} R_0$. To get the expansion above, we consider the *Tate curve*, $\mathrm{Tate}(q)$, with its canonical differential form ω_{can}. Given a modular form f, evaluating $f(\mathrm{Tate}(q), \omega_{\mathrm{can}})$ gives us a Laurent series in $R = \mathbb{Z}((q)) \otimes_{\mathbb{Z}} R_0$ with finitely many terms of negative index. We can now say that the form is *holomorphic at infinity* if $f(\mathrm{Tate}(q), \omega_{\mathrm{can}}) \in \mathbb{Z}[[q]] \otimes_{\mathbb{Z}} R_0$.

We have now recovered a definition of modular forms similar to the one above. This point of view is a powerful one, and allows useful results to be produced using algebro-geometric techniques, rather than analysis. However, there are certain pieces of the original definition that we have not yet reproduced here. Let us attempt to recover the original definition in full.

Example 2.21. Let $R_0 = \mathbb{C}$. So $S = \mathrm{Spec}(R_0) = \{\mathrm{pt}\}$, i.e. a single point. Thus an elliptic curve E/S (or $E/\mathbb{C}$) is a smooth projective curve of genus 1, with a distinguished point O (this is determined by the section). In fact, we can give it a precise equation as a projective variety in $\mathbb{P}^2(\mathbb{C})$ with

$$E \cong \{[X : Y : Z] \in \mathbb{P}^2(\mathbb{C}) \mid Y^2Z = X^3 + aXZ^2 + bZ^3\}, \tag{2.27}$$

where $a, b \in \mathbb{C}$ such that the *discriminant* $\Delta(a, b) = -16(4a^3 + 27b^2)$ is nonzero. Further, this holds over any field K with characteristic $\mathrm{char}(K) \neq 2, 3$, see [Sil09] Proposition III.3.1.

Returning to the case over $\mathbb{C}$, we have yet another description of elliptic curves as *complex tori.* This can be seen by their abelian group structure making them examples of *abelian varieties*; the dimension 1 examples arise as quotients of the complex plane $\mathbb{C}$ by a rank 2 $\mathbb{Z}$-lattice, denoted Λ, see [Sil09] Corollary IV.5.1.1. So, for an elliptic curve $E/\mathbb{C}$, the set of $\mathbb{C}$-points $E(\mathbb{C}) \cong \mathbb{C}/\Lambda$, where $\Lambda = \mathbb{Z}\omega_1 \oplus \mathbb{Z}\omega_2$ with $\omega_1, \omega_2 \in \mathbb{C}$ such that $\omega_1/\omega_2 \notin \mathbb{R}$. By appropriate transformations, one can in fact find an isomorphic curve $\mathbb{C}/\Lambda$ where $\Lambda = \mathbb{Z}z \oplus \mathbb{Z}1$, where $z \in \mathfrak{H}_1$. Thus we can index elliptic curves over $\mathbb{C}$ by elements $z \in \mathfrak{H}_1$. So when are two curves E_1 and E_2 defined as tori isomorphic? Precisely when there exists an invertible (over $\mathbb{Z}$) change of basis between the lattices Λ_1 and Λ_2. Thinking of an element $\alpha z + \beta \in \Lambda$ as a column vector $\begin{pmatrix} \alpha z \\ \beta \end{pmatrix}$, these changes of bases are given by elements of $\mathrm{SL}_2(\mathbb{Z})$.

So, considering our new definition of modular forms of weight k, we see that they are differential k-forms on isomorphism classes of elliptic curves. Over $\mathbb{C}$, these isomorphism classes are in bijection with elements of $\mathrm{SL}_2(\mathbb{Z})\backslash\mathfrak{H}_1$, and thus we recover our original definition.

One final note on this topic is to introduce the notion of a *modular form of level N* in this way. In the world of elliptic curves, this arises from a *level N structure* on a curve E. For the remainder of this section, we will assume that N is invertible in our base scheme, i.e. that S is a scheme over $\mathbb{Z}[1/N]$. Now we introduce the set of N-torsion points on E,

$$E[N] = \{P \in E \mid N \cdot P = O\}. \tag{2.28}$$

This is a group scheme, and we have $E[N](\mathbb{C}) \cong (\mathbb{Z}/N\mathbb{Z})^2$. There are many choices of level N structure on E, which we will categorise as follows:

- S_0: A cyclic subgroup $C \subseteq E$ of order N,
- S_1: A point $Q \in E$ of order N,
- S: Two points $P, Q \in E$ of order N which generate $E[N]$.

Remark 2.22. An alternate description of S is to say that we have a choice of isomorphism $\alpha_N : E[N](\mathbb{C}) \xrightarrow{\sim} (\mathbb{Z}/N\mathbb{Z})^2$.

When we consider an elliptic curve along with a level N structure, we now ask that our morphisms preserve the level N structure (and thus we will in general have more isomorphism classes). So a modular form of level N is as above, but rather than taking an elliptic curve E/R we take a pair either $(E/R, C)$, $(E/R, Q)$, $(E/R, \alpha_N)$ depending on the type of level N structure. We require as above that the modular form only depend on the isomorphism class of curve with level N structure. We will write

$$Y_0(N; R) = \left\{ \begin{array}{c} \text{Isomorphism classes of elliptic curves over } R \\ \text{with level structure } S_0(N) \end{array} \right\}$$

$$Y_1(N; R) = \left\{ \begin{array}{c} \text{Isomorphism classes of elliptic curves over } R \\ \text{with level structure } S_1(N) \end{array} \right\}$$

$$Y(N; R) = \left\{ \begin{array}{c} \text{Isomorphism classes of elliptic curves over } R \\ \text{with level structure } S(N) \end{array} \right\}$$

Finally, to align this fully with the original theory, we have the following theorem.

Theorem 2.23. *Let $N \in \mathbb{N}$. Let $\Gamma_0(N), \Gamma_1(N), \Gamma(N)$ be as in equations* (2.15)*,* (2.16)*. We have bijections*

(1) $Y_0(N; \mathbb{C}) \xrightarrow{\sim} \Gamma_0(N) \backslash \mathfrak{H}_1$

(2) $Y_1(N; \mathbb{C}) \xrightarrow{\sim} \Gamma_1(N) \backslash \mathfrak{H}_1$

(3) $Y(N; \mathbb{C}) \xrightarrow{\sim} \Gamma(N) \backslash \mathfrak{H}_1$

Proof. See [DS05], Theorem 1.5.1. □

This now aligns our original theory fully with this algebro-geometric theory. Note that while we have demonstrated how the groups Γ and the space $\mathfrak{H}_1$ arise for forms over $\mathbb{C}$, this does not explain why this was our starting point for forms (mod p). In fact, this is due to the fact that if we begin with elliptic curves over $\mathbb{C}$, we can restrict our actual points to lie over subrings, in particular $\mathbb{Z}[1/N]$. From this point we can tensor over $\mathbb{Z}[1/N]$ with various rings (as above, our interest lies with $\mathbb{F}_p$ and $\overline{\mathbb{F}}_p$) to retrieve the theory we had initially. However, our original definition of modular forms in this section allowed you to choose any ring R, and to see that this aligns with this *tensoring over* $\mathbb{Z}[1/N]$ idea we have the following.

Theorem 2.24 ([Kat73], Theorem 1.7.1)**.** *Let $N \geq 3$, and then let $k \geq 2$ or $k = 1$ and $N \leq 11$. Let B be a $\mathbb{Z}[1/N]$-algebra. Then we have an isomorphism*

$$B \otimes M_k(\Gamma(N); \mathbb{Z}[1/N]) \xrightarrow{\sim} M_k(\Gamma(N); B). \tag{2.29}$$

We would now like to provide one final modification to this point of view. We have chosen to think of modular forms as functions which take as input both an elliptic curve E/R and a differential form ω and output an element in R. Instead, compared to definition 2.19, we can say that a modular form takes as input an elliptic curve E/R and gives $f(E/R) = f(E/R, \omega) \cdot \omega^k \in \underline{\omega}_{E/R}$. Now, we have assembled these elliptic curves into a space $Y(N; R)$ (note that one can use other level structures, but for brevity we will stick to $S(N)$), and the powerful notion is that there exists an elliptic curve E defined over $Y(N; R)$. This is known as the *universal elliptic curve*, $E/Y(N; R)$. Then we can define the sheaf $\underline{\omega}_{E/Y(N;R)} = p_*(\Omega^1_{E/Y(N;R)})$. We can now think of modular forms as sections of the sheaf $\underline{\omega}_{E/Y(N;R)}$, and in fact since they are defined for *all* elliptic curves, this is in fact a *global* section. This space of global sections is denoted $H^0(Y(N; R), \underline{\omega}^{\otimes k})$, where we take the kth tensor power to get weight k forms. So we are currently motivated to say that this is our space of modular forms of weight k and level N. However, recall that at this stage the definition does not include the "holomorphic at infinity" requirement. Above we resolved this via evaluation at the Tate curve. There is a slightly neater way, which comes from noting that the space $Y(N; R)$ is not compact. The *compactification* of this space is denoted $X(N; R)$, and the sheaf $\underline{\omega}_{E/Y(N;R)}$ can be extended to $\underline{\omega} = \underline{\omega}_{E/X(N;R)}$. This leads us to define

$$M_k(\Gamma(N); R) = H^0(X(N; R), \underline{\omega}^{\otimes k}). \tag{2.30}$$

Chapter 3

Siegel Modular Forms

Modular forms have proven to be an extremely powerful tool in various areas of number theory. Many of the problems which they handle have generalisations to higher dimensions, or simply more variables. For example, modular forms are connected to elliptic curves, whereas in general one may consider *abelian varieties*. That is, projective algebraic varieties which have the structure of an abelian group on their points.

3.1 Siegel Modular Forms

Here we have the *Siegel upper half plane*

$$\mathfrak{S}_g = \{\mathbf{z} \in M_g(\mathbb{C}) \mid \mathbf{z}^\top = \mathbf{z}, \Im(\mathbf{z}) \text{ is positive-definite } \} \tag{3.1}$$

and the *symplectic group*

$$\begin{aligned} \mathrm{Sp}_{2g}(\mathbb{Z}) &= \{\gamma \in \mathrm{GL}_{2g}(\mathbb{Z}) \mid \gamma^\top J \gamma = J\}, \quad \text{where } J = \begin{pmatrix} 0 & I \\ -I & 0 \end{pmatrix} \qquad (3.2) \\ &= \left\{ \gamma = \begin{pmatrix} A & B \\ C & D \end{pmatrix} \middle| \begin{array}{c} A, B, C, D \in \mathrm{GL}_g(\mathbb{Z}), \\ AB^\top = BA^\top, CD^\top = DC^\top, AD^\top - BC^\top = I \end{array} \right\}. \end{aligned}$$

The first observation that one should make is that if one chooses $g = 1$, we have $\mathfrak{H}_1$ (our usual upper half plane) and $\mathrm{Sp}_2(\mathbb{Z}) \cong \mathrm{SL}_2(\mathbb{Z})$. As for the action, we have

$$\gamma \cdot \mathbf{z} = (A\mathbf{z} + B)(C\mathbf{z} + D)^{-1} \qquad \text{where } \gamma = \begin{pmatrix} A & B \\ C & D \end{pmatrix}, \tag{3.3}$$

which again reduces to the usual action in the case $g = 1$. The fact that $C\mathbf{z} + D$ is invertible follows from $\mathbf{z}$ having positive-definite imaginary part.

This is the corresponding domain and group action from which we will define our modular forms. The weight is an algebraic representation

$$\kappa : \mathrm{GL}_g(\mathbb{C}) \longrightarrow \mathrm{GL}_m(\mathbb{C}), \tag{3.4}$$

The factor of automorphy is

$$j_\gamma(\mathbf{z}) = C\mathbf{z} + D, \tag{3.5}$$

with γ and $\mathbf{z}$ as above. We now can turn to the full definition.

Definition 3.1 (Siegel Modular Form)**.** A *Siegel modular form of weight κ and level 1* is a holomorphic function $f : \mathfrak{H}_g \to \mathbb{C}^m$ such that

$$f(\gamma \cdot \mathbf{z}) = \kappa(j_\gamma(\mathbf{z}))f(\mathbf{z}), \quad \text{for} \quad \gamma \in \mathrm{Sp}_{2g}(\mathbb{Z}). \tag{3.6}$$

Remark 3.2. (1) As a function on $\mathfrak{H}_g$, a Siegel modular form can be interpreted as a function of $g(g+1)/2$ complex variables.

(2) If $\kappa = \kappa_1 \oplus \kappa_2$, then $M_\kappa = M_{\kappa_1} \oplus M_{\kappa_2}$, so it is sufficient to consider irreducible representations.

(3) It is not necessary to explicitly ask that Siegel modular forms be "holomorphic at infinity" for $g > 1$ due to the *Koecher principle*, see [vdG06] Theorem 4.4.

Let us now consider the weights that arise for low degrees g.

- If $g = 1$, then $\mathfrak{H}_1$ is the upper half plane and the irreducible representations of $\mathrm{GL}_1(\mathbb{C}) = \mathbb{C}^\times$ are of the form $z \mapsto z^k$. Thus we recover the usual modular forms.

- If $g = 2$, we consider the standard representation std, which is the usual matrix action of $\mathrm{GL}_2(\mathbb{C})$ on $\mathbb{C}^2$. Then all irreducible representations of $\mathrm{GL}_2(\mathbb{C})$ are of the form $\mathrm{Sym}^j(\mathrm{std}) \otimes \det(\mathrm{std})^k$. So one can represent weights for $g = 2$ as a pair (j, k), which some references do.

- In general, the irreducible representations of $\mathrm{GL}_g(\mathbb{C})$ are in bijection with tuples of integers $(\lambda_1, \dots, \lambda_g)$, where $\lambda_i \geq \lambda_{i+1}$.

However, we always have the representation $\det(\mathrm{std})^k$, and we can consider Siegel modular forms with that weight. These are known as *scalar-valued Siegel modular forms*.

As with modular forms, for a fixed weight these form a vector space. We write

$$M_\kappa(\mathrm{Sp}_{2g}(\mathbb{Z})) = \{ \text{ Siegel modular forms of weight } \kappa \ \}, \tag{3.7}$$

and we set $M_k(\mathrm{Sp}_{2g}(\mathbb{Z})) = M_{\det(\mathrm{std})^k}(\mathrm{Sp}_{2g}(\mathbb{Z}))$.

As with modular forms, we can extend past level 1 to general level N by the introduction of *congruence subgroups*. Here, we will focus on just one such group, $\Gamma^g(N)$, which is

$$\begin{aligned} \Gamma^g(N) &= \ker(\mathrm{Sp}_{2g}(\mathbb{Z}) \longrightarrow \mathrm{Sp}_{2g}(\mathbb{Z}/N\mathbb{Z})) \\ &= \left\{ \begin{pmatrix} A & B \\ C & D \end{pmatrix} \in \mathrm{Sp}_{2g}(\mathbb{Z}) \;\middle|\; \begin{pmatrix} A & B \\ C & D \end{pmatrix} \equiv \begin{pmatrix} I & 0 \\ 0 & I \end{pmatrix} \pmod{N} \right\}. \end{aligned}$$

We will often simply refer to Siegel modular forms for some general finite index subgroup $\Gamma^g \subseteq \mathrm{Sp}_{2g}(\mathbb{Z})$ when we do not wish to be precise.

3.2 Fourier Expansion

We begin with the level 1 case.

In the case of modular forms, we acted by a particular matrix to show that the form is periodic and thus has a Fourier expansion. Consider the matrix

$$\gamma = \begin{pmatrix} I & S \\ 0 & I \end{pmatrix}, \tag{3.8}$$

where S is a $g \times g$ symmetric matrix with integer entries. Computing the modularity condition above with this γ gives us

$$f(\mathbf{z} + S) = f(\mathbf{z}). \tag{3.9}$$

Recall that $\mathbf{z}$ is itself a symmetric matrix in $g(g+1)/2$ complex variables, and thus suitable choices of S give us that f is periodic in its variables. Let $\mathbf{z} = (\mathbf{z}_{ij})$ and then write $q_{ij} = e^{2\pi i \mathbf{z}_{ij}}$. From this, we get the Fourier expansion as

$$f(q_{11}, \ldots, q_{gg}) = \sum_{n_{11}, \ldots, n_{gg} \in \mathbb{Z}} a(n_{11}, \ldots, n_{gg}) q_{11}^{n_{11}} \ldots q_{gg}^{n_{gg}}. \tag{3.10}$$

We will not generally make use of this notation, as there is a more concise and helpful way of packaging these expansions. Here we will make the notation $\mathbf{q} = (q_{ij})$.

Let $\mathbf{n}$ be a $g \times g$ symmetric matrix. We say $\mathbf{n}$ is *half-integral* if $a_{ij} \in \frac{1}{2}\mathbb{Z}$ and $a_{ii} \in \mathbb{Z}$. Then we have

$$\mathrm{Tr}(\mathbf{nz}) = \sum_{i=1}^{g} \mathbf{n}_{ii}\mathbf{z}_{ii} + 2 \sum_{1 \leq i < j \leq g} \mathbf{n}_{ij}\mathbf{z}_{ij}, \tag{3.11}$$

so one can see that the choice of $\mathbf{n}$ being half-integral is to make up for the repetition of certain entries due to the symmetry of the matrices. Thus, we can express the earlier Fourier expansion as

$$f(\mathbf{q}) = \sum_{\mathbf{n}} a(\mathbf{n})\mathbf{q}^{\mathbf{n}}, \tag{3.12}$$

where $\mathbf{q}^{\mathbf{n}} = e^{2\pi i \,\mathrm{Tr}(\mathbf{nz})}$.

As for general level N, we need to modify the above in an analogous way that we do for $g = 1$. Here, the matrix available to us is of the form

$$\gamma = \begin{pmatrix} I & NS \\ 0 & I \end{pmatrix}, \tag{3.13}$$

with S as above. So, we have N-periodicity and we obtain a Fourier expansion of the form

$$f(\mathbf{q}) = \sum_{\mathbf{n}} a(\mathbf{n}) \mathbf{q}_N^{\mathbf{n}}, \tag{3.14}$$

where $\mathbf{q}_N^{\mathbf{n}} = e^{\frac{1}{N} 2\pi i \operatorname{Tr}(\mathbf{nz})}$ and $a(\mathbf{n}) \in \mathbb{C}^m$.

3.3 The Φ Operator and Cusp Forms

Definition 3.3 (The Siegel Φ Operator)**.** We define an operator Φ on $M_\kappa(\Gamma^g)$ by

$$(\Phi f)(\mathbf{z}') = \lim_{t \to \infty} f \begin{pmatrix} \mathbf{z}' & 0 \\ 0 & it \end{pmatrix}, \quad \text{with } \mathbf{z}' \in \mathfrak{H}_{g-1}, t \in \mathbb{R}. \tag{3.15}$$

Or, one can view this as

$$(\Phi f)(\mathbf{q}') = \sum_{\mathbf{n}'} a \begin{pmatrix} \mathbf{n}' & 0 \\ 0 & 0 \end{pmatrix} (\mathbf{q}')^{\mathbf{n}'}, \tag{3.16}$$

where $(\mathbf{q}')^{\mathbf{n}'} = e^{2\pi i \operatorname{Tr}(\mathbf{n}'\mathbf{z}')}$.

In fact, the image of Φf in $\mathbb{C}^m$ gives you a subspace $\mathbb{C}^{m-1} \subseteq \mathbb{C}^m$ that is invariant under $\begin{pmatrix} \gamma' & 0 \\ 0 & 1 \end{pmatrix} \in \mathrm{GL}_g(\mathbb{C})$ for $\gamma' \in \mathrm{GL}_{g-1}(\mathbb{C})$. Thus we arrive at a representation $\kappa' : \mathrm{GL}_{g-1}(\mathbb{C}) \to \mathrm{GL}_{m-1}(\mathbb{C})$. Thus the Siegel operator defines a map

$$\Phi : M_\kappa(\Gamma^g) \longrightarrow M_{\kappa'}(\Gamma^{g-1}). \tag{3.17}$$

The primary use of this definition is the following.

Definition 3.4 (Cusp Form)**.** A Siegel modular form $f \in M_\kappa(\Gamma^g)$ is a *cusp form* if $\Phi f = 0$.

One can readily check that for $g = 1$ the Φ operator simply maps to the Fourier coefficient $a_f(0)$, and thus this definition gives the usual idea of a cusp form when $g = 1$.

3.4 Siegel modular forms (mod p), from characteristic zero

As with modular forms, we have so far been focused on the spaces $M_\kappa(\Gamma^g;\mathbb{C})$. Here we have a $\mathbf{q}$-*expansion map*,

$$\begin{array}{rccc} \mathbf{Q}_\kappa: & M_\kappa(\Gamma^g;\mathbb{C}) & \longrightarrow & \mathbb{C}^m[[\mathbf{q}]] \\ & f & \longmapsto & f(\mathbf{q}). \end{array} \tag{3.18}$$

Now, we define:

Definition 3.5 (Siegel modular forms over R)**.** Let $R \subseteq \mathbb{C}$ be a subring of $\mathbb{C}$. The set of *Siegel modular forms of weight κ over R* is

$$M_\kappa(\Gamma^g;R) := \mathbf{Q}_\kappa^{-1}(R^m[[\mathbf{q}]]). \tag{3.19}$$

As before, if B is a $\mathbb{Z}$-module then set

$$M_\kappa(\Gamma^g;B) := B \otimes M_\kappa(\Gamma^g;\mathbb{Z}). \tag{3.20}$$

Then to get Siegel modular forms (mod p) we pick $B = \mathbb{F}_p$ or $\overline{\mathbb{F}}_p$. We will later see a notion of Siegel modular forms arising from algebraic geometry, which will give us an more *intrinsic* notion of forms (mod p). Compared to that, we will say that the above definition gives us Siegel modular forms (mod p) which are reduced from characteristic 0.

Again here, we desire a notion of a *Hasse invariant*, i.e. the reduction of a scalar-valued Siegel modular form $f \in M_{p-1}(\Gamma^g;\mathbb{Z}_{(p)})$ such that $f(q) \equiv 1 \pmod p$. Note here that we are considering $\mathbb{Z}_{(p)}$, so we are allowing fractions so long as their denominators are coprime to p. The existence of this form is in general conjectural, however, we have the following.

Theorem 3.6 ([BN07], Corollary 1)**.** *There exists a form $f \in M_{p-1}(\Gamma^g;\mathbb{Z}_{(p)})$ such that $f(\mathbf{q}) \equiv 1 \pmod p$ as long as any of the following hold:*

- $p \geq g+3$
- $p \equiv 1 \pmod 4$

- $p \geq g/2 + 3$ *and* p *is a* regular prime.

Note that although we are working with $\mathbb{Z}_{(p)}$ rather than $\mathbb{Z}$, we still have $\mathbb{F}_p$ and $\overline{\mathbb{F}}_p$ as modules so we can still reduce (mod p) as desired.

3.5 Algebraic Geometry

We now wish to perform an analogous geometric construction to the one in chapter 2. In section 2.4, we saw that modular forms arise as global sections of the compactified moduli space of elliptic curves. These are the 1-dimensional case of objects called *abelian varieties*, or more generally *abelian schemes*. These are defined as follows.

Definition 3.7 (Abelian Scheme)**.** Let S be a scheme. A *g-dimensional abelian scheme A over S* is a group scheme, which is a smooth proper morphism $p : A \to S$ with section $e : S \to A$ such that the geometric fibres are connected of dimension g.

As usual if we simply wish to take the definition over some ring R, take $S = \mathrm{Spec}(R)$. Note that the case $g = 1$ corresponds precisely to the elliptic curves defined earlier. For general g we require further structure to capture the desired theory and properties.

Definition 3.8 ((Principal) Polarization)**.** Let A be an abelian scheme, with dual $A^\vee = \mathrm{Pic}^0(A/S)$. A *polarization* is an S-homomorphism $\lambda : A \to A^\vee$ such that if s is a geometric point of S then $\lambda_s : A_s \to A_s^\vee$ is of the form $\lambda_s(a) = t_a^*\mathcal{L}_s \otimes \mathcal{L}_s^{-1}$ for some ample invertible sheaf $\mathcal{L}_s$ on A_s. A *principal polarization* is a polarization which is also an isomorphism.

Then, a *principally polarized abelian variety* is a pair (A, λ) where λ is a principal polarization of A. These are the objects with which we will concern ourselves.

We will now introduce levels, and as earlier in this chapter, we will only consider the so-called *full* level structure, which corresponds to the group $\Gamma^g(N)$, above. Let S be a scheme over $\mathbb{Z}[1/N]$, i.e. N is invertible in S, and let A be an abelian scheme over S. A *level N structure* on (A, λ) is an isomorphism $\alpha : A[N] \to (\mathbb{Z}/N\mathbb{Z})^{2g}$ under which the *Weil pairing*[1] corresponds to the standard symplectic pairing on $(\mathbb{Z}/N\mathbb{Z})^{2g}$. If we now consider isomorphism classes of these tuples (A, λ, α), we can assemble these into a scheme $\mathcal{A}_{g,N}$. Just as for elliptic curves, we have here a *universal abelian scheme* $Y/\mathcal{A}_{g,N}$ on which we will consider the sheaf of relative differentials, known as the *Hodge bundle* $\mathbb{E} = e^*(\Omega_{Y/\mathcal{A}_{g,N}})$.

For modular forms, we took the sheaf of differentials $\underline{\omega}$ to a tensor power to find general weights. For the sheaf $\mathbb{E}$ on $\mathcal{A}_{g,N}$, we take an algebraic representation $\kappa : \mathrm{GL}_g \to \mathrm{GL}_m$ and *twist the sheaf of differentials* $\mathbb{E}$ *by* κ, which results in the sheaf $\mathbb{E}_\kappa$. For details on this, see [Ghi03], §3.1. At this point for modular forms we introduced a compactification X, however if $g > 1$ this is not necessary due to the Koecher principle.

Finally, we come to the following expression for the space of weight κ Siegel modular forms:

$$M_\kappa(\Gamma^g(N)) = H^0(\mathcal{A}_{g,N}, \mathbb{E}_\kappa). \tag{3.21}$$

That is, Siegel modular forms of weight κ are global sections of the sheaf $\mathbb{E}_\kappa$ over the moduli space $\mathcal{A}_{g,N}$.

This gives an *intrinsic* notion of Siegel modular forms (mod p) where you could pick, a scheme over $\overline{\mathbb{F}}_p$. To relate this to the previous construction, we have the following result.

Theorem 3.9 ([Str13], Theorem 1.3)**.** *Let κ be the representation given by the tuple $(k_1, \ldots, k_g)$. Let $N > 12$, and either*

- *$p > g(g+1)/2)$, or*
- *$k_g > g + 1$ and $\sum_i (k_i - k_g) < p - g(g+1)/2$.*

Then any Siegel modular form (mod p) of weight κ and level N exists as the reduction of a form in characteristic 0.

[1] which arises from a pairing between A and $A^\vee$, which for us are isomorphic

Chapter 4

Representation Theory of GSp and GSpin

4.1 Definitions and Setup

We have seen now modular forms attached to SL_2 and Siegel modular forms attached to Sp_{2g}. In fact, there is a more general group action on modular forms, coming from GL_2 and GSp_{2g}, respectively. Note that we will generally discuss properties of GSp_{2g} only, since $\mathrm{GSp}_2 = \mathrm{GL}_2$. We would like to understand some of the properties of these groups in a wider context so we can obtain some interesting results on modular forms. Specifically, we would like to understand the following objects:

- The *local Hecke algebra* $\mathcal{H}(\mathrm{GSp}_{2g}(\mathbb{Q}_\ell), \mathrm{GSp}_{2g}(\mathbb{Z}_\ell))$
- The dual group $\hat{\mathrm{GSp}}_{2g} = \mathrm{GSp}_{2g+1}$

To get these properties, we need the view of GSp_{2g} as a *group scheme* over $\mathbb{Z}$ so we can define it over the various rings $\mathbb{Q}_\ell$ and $\mathbb{Z}_\ell$ above.

Much of the interesting data attached to modular forms can be extracted by examining these groups. Mainly our interest will be an analysis of the *Hecke* *algebra* of *Hecke operators*. These act on modular forms via the group action coming from GSp_{2g}. It is helpful to restrict to the data at various primes ℓ, which corresponds to considering the groups $\mathrm{GSp}_{2g}(\mathbb{Q}_\ell)$ and $\mathrm{GSp}_{2g}(\mathbb{Z}_\ell)$. Given that we are predominantly interested in modular forms (mod p), it transpires that we will consider the above for $\ell \neq p$.

We will now explore these groups before leading into a more detailed discussion of Hecke operators in chapter 5.

First, we will define the primary of group of interest for an arbitrary ring R.
Definition 4.1. The reductive group scheme GSp_{2g} over $\mathbb{Z}$ is the linear group such that for all rings R the set of R-points is given by

$$\begin{aligned} \mathrm{GSp}_{2g}(R) = \{\gamma \in \mathrm{GL}_{2g}(R) \mid \gamma^\top J \gamma = \eta(\gamma) J\}, \\ \text{where } \eta(\gamma) \in R^\times \quad \text{and} \quad J = \begin{pmatrix} 0 & I \\ -I & 0 \end{pmatrix}. \end{aligned} \tag{4.1}$$

Remark 4.2. One should think that GSp is to Sp as GL is to SL. That is, we have allowed this symplectic similitude factor η that was equal to 1 for $\gamma \in \mathrm{Sp}_{2g}(R)$ to now in general just be a unit. In fact, for $\gamma \in \mathrm{GSp}_{2g}(R)$ we have that $\det(\gamma) = \eta(\gamma)^g$.

So we are studying here examples of *reductive group schemes*. We will not go into the full details of their definitions and properties here, but necessary set up can be found in [Con14].

4.2 Root Datum

Given the group scheme $G = \mathrm{GSp}_{2g}$, we fix the split torus

$$T = \left\{ \begin{array}{ll} t & = t(u_1, \ldots, u_{g+1}) \\ & = \mathrm{diag}(u_1, \ldots, u_g; u_{g+1}u_1^{-1}, \ldots, u_{g+1}u_g^{-1}) \end{array} \;\middle|\; u_1, \ldots, u_{g+1} \in \mathbb{G}_m \right\},$$

where $\mathbb{G}_m$ is the multiplicative group. From this, we can compute the *character lattice* and *cocharacter lattice*, which are

$$X(T) = \mathrm{Hom}_{\mathrm{GrpSchm}}(T, \mathbb{G}_m) \qquad X^\vee(T) = \mathrm{Hom}_{\mathrm{GrpSchm}}(\mathbb{G}_m, T). \tag{4.2}$$

So, for our case of GSp_{2g} we have

$$\begin{aligned} X(T) &= \mathbb{Z}e_1 \oplus \ldots \oplus \mathbb{Z}e_{g+1} \cong \mathbb{Z}^{g+1} \\ X^\vee(T) &= \mathbb{Z}f_1 \oplus \ldots \oplus \mathbb{Z}f_{g+1} \cong \mathbb{Z}^{g+1}, \end{aligned}$$

where

$$\begin{aligned} &e_i : t(u_1, \ldots, u_{g+1}) \longmapsto u_i, && \text{for } i \in \{1, \ldots, g+1\}, \\ &f_i : u \longmapsto t(1, \ldots, 1, u, 1, \ldots, 1), && \text{for } i \in \{1, \ldots, g+1\}, \end{aligned}$$

where u is in the ith position above. So we can express

$$f_i(u) = \begin{cases} \mathrm{diag}(1, \ldots, 1, u, 1, \ldots, 1; 1, \ldots, 1, u^{-1}, 1, \ldots, 1), & \text{if } 1 \leq i \leq g, \\ \mathrm{diag}(1, \ldots, 1 : u, \ldots, u), & \text{if } i = g+1. \end{cases}$$

Note that we write X and $X^\vee$ additively, while in fact they are multiplicative groups. So, for example, if $\lambda, \mu \in X$, then $(\lambda + \mu)(x) = \lambda(x)\mu(x)$ for $x \in T$.

Remark 4.3. Characters and cocharacters of the torus are often called *weights* and *coweights*, respectively. There are deep connections between group schemes and Lie algebras, and the representation theory makes use of this connection. Thus the weights here correspond closely to the weights in the Lie algebra.

These also have a pairing

$$\begin{array}{cccccc} \langle , \rangle : & X \times X^\vee & \longrightarrow & \mathrm{Hom}_{\mathrm{GrpSchm}}(\mathbb{G}_m, \mathbb{G}_m) & \xrightarrow{\sim} & \mathbb{Z} \\ & (\alpha, \lambda) & \longmapsto & \left(\begin{array}{cccc} \alpha \circ \lambda : & \mathbb{G}_m & \to & \mathbb{G}_m \\ & x & \mapsto & x^n \end{array} \right) & \longmapsto & \langle \alpha, \lambda \rangle = n, \end{array} \tag{4.3}$$

so in particular $\langle e_i, f_j \rangle = \delta_{ij}$.

At this point, we will introduce two special sets of characters and cocharacters, called the *roots* and *coroots*. These are both of deep significance and give a great deal of information regarding the representation theory of group schemes. We will not provide the definitions for these in a general setting, merely give them here explicity as certain combinatorial objects.

In this case, the roots have $\mathbb{Z}$-basis $\Delta = \{\alpha_1, \ldots, \alpha_g\}$ and the coroots have $\mathbb{Z}$-basis $\Delta^\vee = \{\alpha_1^\vee, \ldots, \alpha_g^\vee\}$ where

$$\begin{aligned} \alpha_1 &= e_1 - e_2 & \alpha_1^\vee &= f_1 - f_2 \\ \alpha_2 &= e_2 - e_3 & \alpha_2^\vee &= f_2 - f_3 \\ &\vdots & &\vdots \\ \alpha_{g-1} &= e_{g-1} - e_g & \alpha_{g-1}^\vee &= f_{g-1} - f_g \\ \alpha_g &= 2e_g - e_{g+1} & \alpha_g^\vee &= f_g. \end{aligned}$$

We can use these to define some useful objects for us. Firstly, the set of *dominant weights* and *dominant coweights* by

$$\{\lambda \in X \mid \langle \alpha, \lambda \rangle \geq 0, \text{ for all } \lambda \in \Delta^\vee\} \subseteq X$$
$$\{\lambda \in X^\vee \mid \langle \alpha, \lambda \rangle \geq 0, \text{ for all } \alpha \in \Delta\} \subseteq X^\vee$$

Secondly, orderings on X and $X^\vee$ by

$$\begin{aligned} &\lambda \geq \mu \;\text{ if }\; \lambda - \mu = \sum c_i \alpha_i && \text{(in } X) \\ &\lambda \geq \mu \;\text{ if }\; \lambda - \mu = \sum c_i \alpha_i^\vee && \text{(in } X^\vee) \end{aligned} \tag{4.4}$$

for $c_i \in \mathbb{Z}_{\geq 0}$.

Remark 4.4. One important observation we will make now for $\ell \in \mathbb{Z}$ a prime is that

$$\begin{aligned} \eta(\alpha_i^\vee(\ell)) &= \begin{cases} \eta(f_i(\ell) f_{i+1}(\ell)^{-1}), & \text{if } 1 \leq i \leq g-1 \\ \eta(f_g(\ell)), & \text{if } i = g \end{cases} \\ &= 1, \end{aligned}$$

where $1 \leq i \leq g$ and η is as in (4.1). Or, using the notation of the pairing, we can say $\langle \eta, \alpha_i^\vee \rangle = 0$.

This in fact implies a slightly stronger statement as we will see in section 4.5.

So, attached to the group scheme GSp_{2g}, we have a tuple $(X, X^\vee, \Delta, \Delta^\vee)$, called the *root datum* of the group. From this data, one can attach the *dual group*, $\hat{\mathrm{GSp}}_{2g}$, which is the group scheme with root datum $(X^\vee, X, \Delta^\vee, \Delta)$.

In fact, we have that $\hat{\mathrm{GSp}}_{2g} = \mathrm{GSpin}_{2g+1}$. For our purposes, this is the only feature of GSpin_{2g+1} of interest to us. Any structure we require will occur purely from the fact that it is dual to GSp_{2g}. A more direct construction of GSpin_{2g+1} coming from Clifford algebras can be found in [Con14], appendix C.4.

Now, to see some of the use for all these definitions, we have the following remarkable result.

Theorem 4.5. *Let λ be a dominant weight of GSp_{2g}. Then there exists an irreducible representation $\mathrm{GSp}_{2g}(\mathbb{Z}) \to \mathrm{GL}(\mathbb{Z}^{d_\lambda})$.*

Proof. The above is originally attributed to Chevalley, and the fact that it is over $\mathbb{Z}$ allows us to extend scalars (i.e. tensor by $\mathbb{Z}$-algebras) to our rings of choice. This is particularly valuable for us, since our primary interest will be representations (mod p). See [Jan07], II, Corollary 2.7. □

Corollary 4.6. *Let λ be a dominant coweight of GSp_{2g}. Then there exists an irreducible representation $\mathrm{GSpin}_{2g+1}(\mathbb{Z}) \to \mathrm{GL}(\mathbb{Z}^{d_\lambda})$.*

Proof. By duality, a dominant coweight of GSp_{2g} is a dominant weight of GSpin_{2g+1}. Then apply the theorem above. □

Now we will begin to get into the main topics of interest.

4.3 The Hecke Algebra

The reason we have explored these concepts above is the information they give us for the Hecke algebra. We will now introduce this object formally, but its significance will not be clear until chapter 5.

The Hecke algebra is generated by elements known as *double cosets*, which we will now introduce.

Definition 4.7 (Double Coset)**.** Let G be a group and $K \subseteq G$ a subgroup. Let $g \in G$, then we have the *double coset*

$$KgK = \{k_1 g k_2 \mid k_1, k_2 \in K\}. \tag{4.5}$$

The set of all double cosets of K in G is denoted $K\backslash G/K$.

Remark 4.8. Given a double coset KgK in G, one can decompose it into left (or right) cosets by simply decomposing G and intersecting the resulting cosets with KgK, i.e. if $G = \bigcup_{i \in I} Kg_i$, then $KgK = \bigcup_{j \in J_g}(KgK \cap Kg_j)$, where $J_g = \{j \in I \mid KgK \cap Kg_j \neq \emptyset\}$.

These decompositions can in general be infinite, so we will want the following

Definition 4.9 (Hecke Pair)**.** A *Hecke pair* is a pair (G, K) with G a group and $K \subseteq G$ a subgroup such that every double coset KgK, where $g \in G$, is a finite union of right cosets.

We can give these double cosets the structure of an algebra with formal summation, as follows

Definition 4.10 (Hecke Algebra)**.** Let (G, K) be a Hecke pair. The *Hecke algebra* of (G, K) is the algebra $\mathcal{H}(G, K) = \mathbb{Z}[K\backslash G/K]$, with product

$$KgK \cdot KhK = \sum_{i \in J_g, j \in J_h} Kg_i h_j, \tag{4.6}$$

for $KgK = \sum_{i \in J_g} Kg_i$, $KhK = \sum_{j \in J_h} Kh_j$.

We now make a choice as to the groups G and K in which we are interested.

Lemma 4.11. *Let G be a reductive group scheme over $\mathbb{Z}$. Let $\mathbb{F}$ be a local field with ring of integers $\mathcal{O}_\mathbb{F}$. Then $(G(\mathbb{F}), G(\mathcal{O}_\mathbb{F}))$ is a Hecke pair.*

Proof. See Proposition 6.1 in [Lan01]. □

Remark 4.12. 1. Note that our group of interest, GSp_{2g}, with field $\mathbb{Q}_\ell$ and ring of integers $\mathbb{Z}_\ell$, satisfies the required conditions.

2. Since we have chosen $\mathbb{F}$ to be a local field, the resulting Hecke algebra would often be referred to as a *local Hecke algebra*. We will see in chapter 5 how this corresponds to a piece of a *global* Hecke algebra at a particular prime ℓ.

One application of the above definitions is the ability to precisely formulate a basis for a Hecke algebra, as follows.

Proposition 4.13. *Let ℓ be a prime. Let $G = \mathrm{GSp}_{2g}(\mathbb{Q}_\ell)$ and $K = \mathrm{GSp}_{2g}(\mathbb{Z}_\ell)$ with the torus T as above giving us the set of dominant coweights in $X^\vee$.*

$$G = \coprod_{\substack{\lambda \in X^\vee \\ \lambda \text{ dominant}}} K\lambda(\ell)K \tag{4.7}$$

Further, the double cosets $T_{\lambda(\ell)} = K\lambda(\ell)K$ give a $\mathbb{Z}$-basis for $\mathcal{H}$.

Proof. This is the Cartan decomposition. See, for example, Proposition 2.6 in [Gro98b]. □

4.4 The case of GL_2

We now provide an example, the case of the usual elliptic modular forms.

Example 4.14. Let $g = 1$, so $\mathrm{GSp}_{2g} = \mathrm{GSp}_2 \cong \mathrm{GL}_2$.

We have the torus of diagonal matrices,

$$T = \left\{ \begin{pmatrix} u_1 & 0 \\ 0 & u_2 u_1^{-1} \end{pmatrix} \right\}.$$

The above representatives are chosen to align with our earlier choices for GSp_{2g}, though in this specific case they are not the most natural options. Now we have

$$e_1 : \begin{pmatrix} u_1 & 0 \\ 0 & u_2 u_1^{-1} \end{pmatrix} \longmapsto u_1, \qquad f_1 : u \longmapsto \begin{pmatrix} u & 0 \\ 0 & u^{-1} \end{pmatrix},$$
$$e_2 : \begin{pmatrix} u_1 & 0 \\ 0 & u_2 u_1^{-1} \end{pmatrix} \longmapsto u_2, \qquad f_2 : u \longmapsto \begin{pmatrix} 1 & 0 \\ 0 & u \end{pmatrix},$$

and thus

$$X(T) = \left\{ \begin{pmatrix} u_1 & 0 \\ 0 & u_2 u_1^{-1} \end{pmatrix} \longmapsto u_1^a u_2^b \right\} = \mathbb{Z}e_1 \oplus \mathbb{Z}e_2 \cong \mathbb{Z}^2,$$

$$X^\vee(T) = \left\{ u \longmapsto \begin{pmatrix} u^a & 0 \\ 0 & u^{b-a} \end{pmatrix} \right\} = \mathbb{Z}f_1 \oplus \mathbb{Z}f_2 \cong \mathbb{Z}^2,$$

with pairing the usual dot product on $\mathbb{Z}^2$, i.e. still just $\langle e_i, f_j \rangle = \delta_{ij}$.

The root basis is $\Delta = \{\alpha = e_1 - e_2\}$, with coroot basis $\Delta^\vee = \{\alpha^\vee = f_1 - f_2\}$. Note now that $X = X^\vee$ and $\Delta = \Delta^\vee$, and thus

$$(X, X^\vee, \Delta, \Delta^\vee) = (X^\vee, X, \Delta^\vee, \Delta), \tag{4.8}$$

and thus GL_2 is its own dual group, i.e. $\hat{\mathrm{GL}}_2 = \mathrm{GL}_2$. Now the set of dominant coweights is

$$\begin{aligned} &\{\lambda = af_1 + bf_2 \in X^\vee \mid \langle \alpha, \lambda \rangle \geq 0, \text{ for all } \alpha \in \Phi^+\} \\ &= \{\lambda = af_1 + bf_2 \in X^\vee \mid \langle e_1 - e_2, af_1 + bf_2 \rangle \geq 0\} \\ &= \{\lambda = af_1 + bf_2 \in X^\vee \mid a - b \geq 0\} \\ &= \{\lambda = af_1 + bf_2 \in X^\vee \mid a \geq b\}. \end{aligned}$$

Thus our Hecke algebra can be expressed as

$$\begin{aligned} \mathcal{H}_{\mathrm{GL}_2} &= \mathbb{Z}\text{- span}\{\mathrm{GL}_2(\mathbb{Z}_\ell)\lambda(\ell)\,\mathrm{GL}_2(\mathbb{Z}_\ell) \mid \lambda \text{ dominant}\} \\ &= \mathbb{Z}\text{- span}\left\{ \mathrm{GL}_2(\mathbb{Z}_\ell) \begin{pmatrix} \ell^a & 0 \\ 0 & \ell^{b-a} \end{pmatrix} \mathrm{GL}_2(\mathbb{Z}_\ell) \;\middle|\; a \geq b \right\} \end{aligned}$$

The above Hecke algebra corresponds to the Hecke Operators on elliptic modular forms.

4.5 Some Useful Facts

Proposition 4.15. *If $\beta^\vee$ is a coroot of GSp_{2g}, then*

$$\eta\left(\beta^\vee(\ell)\right) = 1, \tag{4.9}$$

i.e. $\langle \eta, \beta^\vee \rangle = 0$.

Proof. We've seen that the statement holds for the choice of simple coroots $\{\alpha_1^\vee, \ldots, \alpha_g^\vee\}$ from remark 4.4. These coroots form a basis for the set of coroots. Thus

$$\beta^\vee = \sum_{i=1}^{g} c_i \alpha_i^\vee \tag{4.10}$$

where $c_i \in \mathbb{Z}$ for $1 \leq i \leq g$. Recalling that this addition actually represents multiplication on the images of the coroots, we have

$$\beta^\vee(\ell) = \prod_{i=1}^{g} \left(\alpha_i^\vee(\ell)\right)^{c_i}. \tag{4.11}$$

Thus

$$\begin{aligned} \eta\left(\beta^\vee(\ell)\right) &= \eta\left(\prod_{i=1}^{g} \left(\alpha_i^\vee(\ell)\right)^{c_i}\right) \\ &= \prod_{i=1}^{g} \eta\left(\alpha_i^\vee(\ell)\right)^{c_i} = \prod_{i=1}^{g} 1^{c_i} = 1. \end{aligned}$$

Thus for any coroot $\beta^\vee$ of GSp_{2g}, we have $\eta(\beta^\vee(\ell)) = 1$, as required. □

Corollary 4.16. *If $\lambda, \mu \in X^\vee$ are coweights of GSp_{2g} such that $\lambda \geq \mu$, then $\eta(\lambda(\ell)) = \eta(\mu(\ell))$, or $\langle \eta, \lambda \rangle = \langle \eta, \mu \rangle$.*

Proof. If $\lambda \geq \mu$, then by the definition of the ordering we have

$$\lambda - \mu = \sum_{i=1}^{g} c_i \alpha_i^\vee, \tag{4.12}$$

for $\alpha_i^\vee \in \Delta^\vee$ and $c_i \in \mathbb{Z}_{\geq 0}$. However by the above, we have $\eta\left(\alpha_i^\vee(\ell)\right) = 1$. Thus

$$\eta(\lambda(\ell))\eta(\mu(\ell))^{-1} = \eta\left(\prod_{i=1}^{g} \alpha_i^\vee(\ell)^{c_i}\right) = 1,$$

so we have that $\eta(\lambda(\ell)) = \eta(\mu(\ell))$, as required. □

Remark 4.17. This corollary may seem independent of the prior result, since we had established that the determinant of $\alpha_i^\vee(\ell)$ is 1 already. The result above makes this corollary independent on the choice of simple coroots in remark 4.4. Further, note that it holds equally for $\lambda \geq \mu$ and $\mu \geq \lambda$. The requirement is that λ and μ differ only by coroots.

Another thing to note is that therefore any power of η is trivial on coroots. In particular, $\det = \eta^g$, and thus det is also fixed when $\lambda \geq \mu$ or $\mu \geq \lambda$.

Chapter 5

Hecke Operators and Hecke Algebras

5.1 Double Coset Action

Siegel modular forms have a standard action from the group $\mathrm{Sp}_{2g}(\mathbb{Z})$. The Hecke operators arise from an action of

$$\mathrm{GSp}^+_{2g}(\mathbb{Q}) = \{\gamma \in \mathrm{GSp}_{2g}(\mathbb{Q}) \mid \det(\gamma) > 0\}. \tag{5.1}$$

The reason we choose the subgroup of positive determinant matrices is that we wish to preserve the action on $\mathfrak{H}_g$, i.e. for $\gamma \in \mathrm{GSp}^+_{2g}(\mathbb{Q})$ and $\mathbf{z} \in \mathfrak{H}_g$,

$$\gamma \mathbf{z} = (A\mathbf{z} + B)(C\mathbf{z} + D)^{-1}, \tag{5.2}$$

where $\gamma = \begin{pmatrix} A & B \\ C & D \end{pmatrix}$. The resulting image is only within the upper-half space if $\det \gamma > 0$. Using this, we now have the following

Definition 5.1 (Slash Operator). The *weight κ slash operator* is

$$\begin{array}{rccc} \cdot\,|_\kappa \gamma : & M_\kappa(\mathrm{Sp}_{2g}(\mathbb{Z})) & \longrightarrow & M_\kappa(\mathrm{Sp}_{2g}(\mathbb{Z})) \\ & f & \longmapsto & f|_\kappa \gamma, \end{array} \tag{5.3}$$

where

$$(f|_\kappa\gamma)(\mathbf{z}) = \eta(\gamma)^{\sum\lambda_i - g(g+1)/2}\kappa(C\mathbf{z}+D)^{-1}f(\gamma\mathbf{z}), \tag{5.4}$$

for κ the irreducible representation with highest weight $(\lambda_1 \geq \ldots \geq \lambda_g)$.

Remark 5.2. Note that if $\gamma \in \mathrm{Sp}_{2g}(\mathbb{Z})$, then

$$\begin{aligned}(f|_\kappa\gamma)(\mathbf{z}) &= \eta(\gamma)^{\sum\lambda_i - g(g+1)/2}\kappa(C\mathbf{z}+D)^{-1}f(\gamma\mathbf{z}) \\ &= 1^{\sum\lambda_i - g(g+1)/2}\kappa(C\mathbf{z}+D)^{-1}\kappa(C\mathbf{z}+D)f(\mathbf{z}) \\ &= f(\mathbf{z}),\end{aligned}$$

so $\mathrm{Sp}_{2g}(\mathbb{Z})$ fixes $M_\kappa(\mathrm{Sp}_{2g})$ pointwise under the slash operator.

In section 4.3 we defined a Hecke algebra of double cosets. We will now apply this to the specific case of the groups acting on Siegel modular forms.

Proposition 5.3. *The pair* $(\mathrm{GSp}^+_{2g}(\mathbb{Q}), \mathrm{Sp}_{2g}(\mathbb{Z}))$ *is a Hecke pair.*

Proof. See [And86], §3.3 Lemma 3.3.1. □

We can now introduce an action of double cosets on modular forms. For an element $\gamma \in \mathrm{GSp}^+_{2g}(\mathbb{Q})$, we will say that

$$(f|_\kappa \mathrm{Sp}_{2g}(\mathbb{Z})\gamma\,\mathrm{Sp}_{2g}(\mathbb{Z}))(\mathbf{z}) = \sum_{j\in J_\gamma}(f|_\kappa\gamma_j)(\mathbf{z}), \tag{5.5}$$

where J_γ is as in remark 4.8.

Proposition 5.4. *Let* $f \in M_\kappa(\mathrm{Sp}_{2g}(\mathbb{Z}))$ *and* $\gamma \in \mathrm{GSp}_{2g}(\mathbb{Q})^+$. *Then*

$$f|_\kappa \mathrm{Sp}_{2g}(\mathbb{Z})\gamma\,\mathrm{Sp}_{2g}(\mathbb{Z}) \in M_\kappa(\mathrm{Sp}_{2g}(\mathbb{Z})). \tag{5.6}$$

Proof. See [vdG06], page 31. □

Definition 5.5 (Hecke Operator)**.** Let $\gamma \in \mathrm{GSp}^+_{2g}(\mathbb{Q})$. The *Hecke operator* T_γ is the map

$$\begin{array}{rccc} T_\gamma : & M_\kappa(\mathrm{Sp}_{2g}(\mathbb{Z})) & \longrightarrow & M_\kappa(\mathrm{Sp}_{2g}(\mathbb{Z})) \\ & f & \longmapsto & f|_\kappa \mathrm{Sp}_{2g}(\mathbb{Z})\gamma\,\mathrm{Sp}_{2g}(\mathbb{Z}) \end{array} \tag{5.7}$$

Remark 5.6. We will often interchange between the double coset and the function that acts upon modular forms.

Further, note that though the above definition refers to a specific γ, in the Hecke algebra one can take sums and product of such operators and as a result have Hecke operators T which do not correspond to a specific matrix γ. The action of such operators is simply the sum and product of the actions of the individual T_γ's.

Definition 5.7 (Hecke Eigenform/Eigensystem)**.** Let $f \in M_\kappa(\mathrm{Sp}_{2g}(\mathbb{Z}); B)$ be a Siegel modular form. We say f is an *eigenform* if it is an eigenvector for all the Hecke operators simultaneously, i.e. if T is a Hecke operator, then there exists $\Psi_f(T) \in B$ such that

$$Tf = \Psi_f(T)f. \tag{5.8}$$

When the eigenvalues are contained in B, the function

$$\begin{array}{rccc} \Psi_f: & \mathcal{H} & \longrightarrow & B \\ & T & \longmapsto & \Psi_f(T) \end{array} \tag{5.9}$$

is called the *Hecke eigensystem* of the eigenform f.

For calculation purposes, it is useful to have a concrrete description of the action of Hecke operators on Fourier expansions. We recall the case $g = 1$ below, and refer to [And86], §4.2 for the general case.

Example 5.8. Consider

$$\Delta_m = \{\gamma \in \mathrm{GSp}_{2g}^+(\mathbb{Q}) \mid \det(\gamma) = m\}. \tag{5.10}$$

Then we define the Hecke operator T_m by

$$T_m = \sum_{\gamma \in \Delta_m} T_\gamma, \tag{5.11}$$

i.e. the sum of all operators corresponding to matrices of a fixed determinant m. We can compute the action of the Hecke operators T_m on Fourier expansions. Consider the case $g = 1$, and take $f(q) = \sum a(n)q^n$. Then we have

$$(T_m f)(q) = \sum_{n=0}^{\infty} \left(\sum_{d|\gcd(m,n)} d^{k-1} a(mn/d^2) \right) q^n. \tag{5.12}$$

Now, consider an eigenform $f(q) = \sum a(n)q^n$ for $g = 1$. If $a(1) = 1$, then we say f is a *normalised eigenform*. Then, if one has the Hecke operator T_n acting on f a normalised eigenform, we have

$$T_n f = a(n)f. \tag{5.13}$$

That is, the eigenvalue of T_n is precisely the nth Fourier coefficient. Now, if one thinks back to sections 2.3 and 3.4 we saw that we ocassionally want coefficients in $\overline{\mathbb{F}}_p$. We can now understand this as necessary when the coefficients may occur as eigenvalues of these Hecke operators.

Remark 5.9. One thing to note is that many results about modular forms are stated in terms of their Fourier coefficients. However, in many cases one should imagine that these coefficients in truth are referring to Hecke eigenvalues. The reason to think this is that when one, say, attempts to generalise a result to the Siegel case, one may look for a parallel result in the Fourier coefficients, when really one should have been considering the Hecke eigenvalues.

Remark 5.10. We have chosen to look at the above for Siegel modular forms attached to $\mathrm{Sp}_{2g}(\mathbb{Z})$, that is, level 1 forms. In general, the above theory can be restated for any level N.

5.2 Hecke Algebra Structure

Here we'd like to make explicit some statements about the coset representatives for our Hecke algebras. This will make clear a connection between the various local Hecke algebras and the global algebra containing all the Hecke operators defined above.

Proposition 5.11 (Elementary Divisors)**.** *Let* $\gamma \in \mathrm{GSp}_{2g}^{+}(\mathbb{Q})$*. The double coset* $\mathrm{Sp}_{2g}(\mathbb{Z})\gamma \,\mathrm{Sp}_{2g}(\mathbb{Z})$ *has a unique representative of the form*

$$\mathrm{diag}(d_1, \ldots, d_g, e_1, \ldots, e_g), \tag{5.14}$$

where $d_i, e_j > 0$*,* $d_i | d_{i+1}$*,* $e_{i+1} | e_i$*,* $d_i e_i = \eta(\gamma)$*.*

Proof. This turns out to be equivalent to the Cartan decomposition, which we stated for $\mathbb{Q}_\ell$ in Proposition 4.13. If one makes the statement for $\mathbb{Q}$ and $\mathbb{Z}$, as we have done here, the Cartan decomposition still holds.

A precise proof can be found in [And86], Lemma 3.3.6. $\square$

Remark 5.12. (1) We get the same structure with $\gamma \in \mathrm{GSp}_{2g}(\mathbb{Q})$ and the double coset $\mathrm{GSp}_{2g}(\mathbb{Z})\gamma \,\mathrm{GSp}_{2g}(\mathbb{Z})$.

(2) Note that given a matrix of the form above, we can write it as a product of diagonal matrices each of whose non-zero entries are powers of a single fixed prime. This gives a decomposition

$$\mathcal{H}(\mathrm{GSp}_{2g}^{+}(\mathbb{Q}), \mathrm{Sp}_{2g}(\mathbb{Z})) = \bigotimes_{\ell \text{ prime}} \mathcal{H}_\ell(\mathrm{GSp}_{2g}^{+}(\mathbb{Q}), \mathrm{Sp}_{2g}(\mathbb{Z})), \tag{5.15}$$

where $\mathcal{H}_\ell$ is called the *local Hecke algebra* at the prime ℓ.

This local Hecke algebra is very useful, because it informs the structure of the algebra (since one is often able to prove desired results on the local pieces) and yet is simpler to work with, as one need only worry about a single prime at a time.

Remark 5.13. Specifically, when we refer to an *eigenform*, as above, we will often think of an eigenform *at the prime* ℓ. So we have an eigensystem for each prime ℓ, i.e. $\Psi_{f,\ell} : \mathcal{H}_\ell \to B$.

As it turns out, these local algebras are also Hecke algebras in their own right, as the following lemma demonstrates

Lemma 5.14. *Let* $\gamma \in \mathrm{GSp}_{2g}(\mathbb{Q}_\ell)$*. The double coset* $\mathrm{GSp}_{2g}(\mathbb{Z}_\ell)\gamma \,\mathrm{GSp}_{2g}(\mathbb{Z}_\ell)$ *has a unique representative of the form*

$$\mathrm{diag}(\ell^{k_1}, \ldots, \ell^{k_g}, \ell^{k'_1}, \ldots, \ell^{k'_g}), \tag{5.16}$$

where $k_i, k'_j \in \mathbb{Z}$, $k_i \leq k_{i+1}$, $k'_{i+1} \leq k'_i$, $\ell^{k_i+k'_i} = \eta_\ell(\gamma)$.

Proof. As above, this is equivalent to the Cartan decomposition. In this case, our choice of groups aligns precisely with what we stated in Proposition 4.13.

A proof can be constructed from a minor alteration of the above, i.e. Lemma 3.3.6 in [And86]. The entries arise as gcds of entries in any other choice of representative. The point here is that since we are working with ℓ-adic numbers, all such gcds will be a power of ℓ. $\square$

Corollary 5.15. *The local algebra above is the same as the Hecke algebra coming from ℓ-adic numbers, i.e.*

$$\mathcal{H}_\ell(\mathrm{GSp}_{2g}^+(\mathbb{Q}), \mathrm{Sp}_{2g}(\mathbb{Z})) \cong \mathcal{H}(\mathrm{GSp}_{2g}(\mathbb{Q}_\ell), \mathrm{GSp}_{2g}(\mathbb{Z}_\ell)). \tag{5.17}$$

Proof. We produced the local Hecke algebra by decomposing the matrix representatives in Proposition 5.11 into pieces that are products of a single power. So, consider a matrix

$$\mathrm{diag}(d_1, \ldots, d_g, e_1, \ldots, e_g), \tag{5.18}$$

where $d_i, e_j \in \mathbb{Z}_{>0}$, $d_i | d_{i+1}$, $e_{i+1} | e_i$, $d_i e_i = \eta(\gamma)$. Let k_i and k'_i be maximal such that $\ell^{k_i} | d_i$ and $\ell^{k'_i} | e_i$, for all $i \in \{1, \ldots, g\}$. Then $k_i \leq k_{i+1}$ and $k'_i \leq k'_{i+1}$. So the representative for the local algebra is

$$\mathrm{diag}(\ell^{k_1}, \ldots, \ell^{k_g}, p^{k'_1}, \ldots, p^{k'_g}), \tag{5.19}$$

where $k_i, k'_j \in \mathbb{Z}$, $k_i \leq k_{i+1}$, $k'_{i+1} \leq k'_i$, $p^{k_i+k'_i} = \eta_\ell(\gamma)$. Thus the algebras have the same coset representatives, and thus the double cosets are in bijection, which leads to the isomorphism, as desired. $\square$

Chapter 6

Theta Operators

We have just looked at a family of operators on modular forms called the Hecke operators. To that, we will add an additional theory of operators known as *theta operators*. These are differential operators, one of which is a classical object of study on modular forms. We will present some generalisations to the case of Siegel modular forms.

6.1 Modular Forms (i.e. $g = 1$)

6.1.1 Level 1

We begin with the level 1 case, where we can exploit the structure of the algebra of modular forms to prove some basic results. This method was discussed by Serre in [Ser73].

Definition 6.1 (Theta Operator on Power Series)**.** Let R be a commutative ring, and $R[[q]]$ be the ring of formal power series. The *theta operator* is

$$\begin{array}{cccc} \theta : & R[[q]] & \longrightarrow & R[[q]] \\ & f = \sum a_n q^n & \longmapsto & q\frac{d}{dq} f = \sum n a_n q^n. \end{array} \tag{6.1}$$

We know that modular forms have Fourier expansions, and can view operators on those expansions. However, not all power series arise from modular forms, and thus one should not expect that any function on series will result in a function on modular forms.

First, recall the Eisenstein series E_k defined in example 2.5, which is a non-cusp form of weight k. We have the following (we will work over $\mathbb{C}$ for level 1 so we can make use of the first definition of modular forms).

Lemma 6.2. *(1) Let $f \in M_k(\mathrm{SL}_2(\mathbb{Z}); \mathbb{C})$. Then $\theta f - \frac{k}{12} E_2 \cdot f$ is a modular form of weight $k+2$.*

(2) The ring $\mathbb{C}[E_2, E_4, E_6]$ is closed under the action of θ.

Proof. (1) Over $\mathbb{C}$, one can write $\theta = \frac{1}{2\pi i}\frac{d}{dz}$. Since f is a modular form, we have $f(-1/z) = z^k f(z)$. However, E_2 is not a modular form, and instead satisfies $E_2(-1/z) = z^2 E_2(z) + \frac{12z}{2\pi i}$. Now we compute

$$\begin{aligned} \frac{d}{dz}(f(-1/z)) &= \frac{d}{dz}(z^k f(z)) \\ \frac{1}{z^2} f'(-1/z) &= k z^{k-1} f(z) + z^k f'(z) \\ f'(-1/z) &= k z^{k+1} f(z) + z^{k+2} f(z), \end{aligned}$$

and thus

$$\begin{aligned} &\left(\theta f - \frac{k}{12} E_2 f\right)(-1/z) \\ &= \frac{1}{2\pi i} f'(-1/z) - \frac{k}{12} E_2(-1/z) f(-1/z) \\ &= \frac{1}{2\pi i}\left(k z^{k+1} f(z) + z^{k+2} f'(z)\right) - \frac{k}{12}\left(z^2 E_2(z) + \frac{12z}{2\pi i}\right) z^k f(z) \\ &= z^{k+2}\left(\frac{1}{2\pi i} f'(z) - \frac{k}{12} E_2(z) f(z)\right), \end{aligned}$$

as required.

(2) For this we have Ramanujan's formulae

$$\theta E_2 = (E_2^2 - E_4)/12 \qquad\qquad \theta E_4 = (E_2 E_4 - E_6)/3$$

$$\theta E_6 = (E_2 E_6 - E_4^2)/2$$

which can be confirmed explicitly on Fourier expansions.

□

Corollary 6.3. *Let ∂ be the derivation of $M_k(\mathrm{SL}_2(\mathbb{Z}); \mathbb{C})$ defined by $\partial E_4 = -4E_6$ and $\partial E_6 = -6E_4^2$. If f is a modular form of weight k, then ∂f is a modular form of weight $k+2$ and*

$$12\theta f = kE_2 f + \partial f. \tag{6.2}$$

Above we were looking at forms over $\mathbb{C}$, and since we require the series E_2 here, the theta operator does not give an operator on modular forms. We will now consider forms (mod p), i.e. $f \in M_k(\mathrm{SL}_2(\mathbb{Z}); \mathbb{F}_p)$ (or $\overline{\mathbb{F}}_p$, which is often our preference). Recall that here we have the *Hasse invariant* $A = E_{p-1}$ which has Fourier expansion $A(q) = 1$. Proofs of the following facts are straightforward, and can be found in [Ser73].

Lemma 6.4. *(1) $E_2(q) \equiv E_{p+1}(q) \pmod p$. Let $B = E_{p+1}$.*

(2) We have $\partial A = B$ and $\partial B = -E_4 A$.

Corollary 6.5. *Viewed as polynomials in the generators E_4 and E_6, the forms A and B are relatively prime. Further, A has no repeated factors.*

Note that we can now write

$$12\theta f = kBf + A\partial f. \tag{6.3}$$

Given all the above, we now can state the following.

Theorem 6.6. *Let $f \in M_k(\mathrm{SL}_2(\mathbb{Z}); \mathbb{F}_p)$. Then $\theta f \in S_{k+p+1}(\mathrm{SL}_2(\mathbb{Z}); \mathbb{F}_p)$.*

That is, if one takes a modular form and simply computes the θ map on its power series, the resulting power series is indeed a modular form (mod p).

6.1.2 Level N

When we pass to general level N, we no longer have an explicit set of generators we can exploit in the same way, so the methods of Serre do not apply. There are two alternate methods available, one using the Rankin-Cohen bracket and the other using algebraic geometry.

Rankin-Cohen Bracket

This exposition can be found in [Zag08], §5. Again, we begin with an operator on power series.

Theorem 6.7. *Let $\Gamma \subseteq \mathrm{SL}_2(\mathbb{Z})$ be a congruence subgroup. Let $f \in M_{k_1}(\Gamma; \mathbb{C}), g \in M_{k_2}(\Gamma; \mathbb{C})$, with Fourier expansions $f(q)$ and $g(q)$, respectively. Then the series*

$$[f(q), g(q)] = k_1 f(q) \cdot q\frac{d}{dq}g(q) - k_2 g(q) \cdot q\frac{d}{dq}f(q) \tag{6.4}$$

is in fact the Fourier expansion $[f, g](q)$ of a modular form $[f, g] \in M_{k_1+k_2+2}(\Gamma; \mathbb{C})$.

Proof. Compute the modularity of $k_1 f \cdot \frac{d}{dz}g - k_2 \cdot \frac{d}{dz}fg$ and recall the connection between $\frac{d}{dz}$ and $q\frac{d}{dq}$. □

This leads us to the following definition.

Definition 6.8 (Rankin-Cohen Bracket)**.** Let $\Gamma \subseteq \mathrm{SL}_2(\mathbb{Z})$ be a congruence subgroup. Let $f \in M_{k_1}(\Gamma; \mathbb{C}), g \in M_{k_2}(\Gamma; \mathbb{C})$, with Fourier expansions $f(q)$ and $g(q)$, respectively. The *first Rankin-Cohen bracket of f and g* is $[f, g] \in M_{k_1+k_2+2}(\Gamma; \mathbb{C})$ such that $[f, g](q) = [f(q), g(q)]$.

There are in fact n-th Rankin-Cohen brackets, but we do not require them here.

Remark 6.9. Note that the bracket preserves the ring of coefficients of f and g. For example, if they both have coefficients in $\mathbb{Z}$, then so will $[f, g]$.

From this we can define a theta operator as follows.

Theorem 6.10. *Let $p \geq 5$ be a prime, $k \geq 2$, and $\Gamma \subseteq \mathrm{SL}_2(\mathbb{Z})$ be a congruence subgroup. There exists a derivation*

$$\theta : M_k(\Gamma; \overline{\mathbb{F}}_p) \longrightarrow S_{k+p+1}(\Gamma; \overline{\mathbb{F}}_p) \tag{6.5}$$

whose effect on Fourier expansions is

$$(\theta f)(q) = q\frac{d}{dq}f(q), \quad i.e. \quad \theta\left(\sum a_n q^n\right) = \sum n a_n q^n. \tag{6.6}$$

Proof. Let $f \in M_k(\Gamma; \overline{\mathbb{F}}_p)$ and, by [Kat73] Theorem 1.7.1, fix a lift $F \in M_k(\Gamma; \mathbb{C})$ such that $F(q) \equiv f(q) \pmod p$. Define

$$\theta f = \overline{[f, A]} \in M_{k+p+1}(\Gamma; \overline{\mathbb{F}}_p), \tag{6.7}$$

where $A \in M_{p-1}(\Gamma; \overline{\mathbb{F}}_p)$ is the Hasse invariant and $\overline{[f, A]}$ is the reduction $\pmod p$ of $[f, A]$. As for the Fourier expansions,

$$(\theta f)(q) = [f, A](q) = kf(q) \cdot 0 - (p-1)A(q) \cdot q\frac{d}{dq}f(q) = q\frac{d}{dq}f(q). \tag{6.8}$$

□

Algebraic Geometry

This particular setup is due to Katz in [Kat77], and one should look there for full details and results. We will present a brief overview of the main points and the primary theorem, with the congruence subgroup chosen to be $\Gamma_1(N)$.

In chapter 2 we saw that the space of modular forms of weight k for $\Gamma_1(N)$ can be viewed as $H^0(Y_1(N), \omega^{\otimes k})$. That is, global sections of the line bundle $\omega^{\otimes k}$ of relative differential forms on $Y_1(N)$, which can be constructed from a *universal elliptic curve* E_{univ} over the scheme $Y_1(N)$. As we are considering differential forms, we are motivated to look at the relative de Rham cohomology, $H^1_{\text{dR}}(E_{\text{univ}}/Y_1(N))$. On this we have the *Gauss-Manin connection*

$$\nabla : H^1_{\text{dR}}(E_{\text{univ}}/Y_1(N)) \to \Omega^1_{Y_1(N)/\mathbb{F}_p} \otimes_{\mathcal{O}_{Y_1(N)}} H^1_{\text{dR}}(E_{\text{univ}}/Y_1(N)), \tag{6.9}$$

and from this we can build the composite map

$$\begin{aligned}\tilde{\theta} : \omega^{\otimes k} &\hookrightarrow \operatorname{Sym}^k H^1_{\text{dR}}(E_{\text{univ}}/Y_1(N)^h) \\ &\xrightarrow{\operatorname{Sym}^k \nabla} \Omega^1_{Y_1(N)^h/\mathbb{F}_p} \otimes_{\mathcal{O}_{Y_1(N)^h}} \operatorname{Sym}^k H^1_{\text{dR}}(E_{\text{univ}}/Y_1(N)) \\ &\twoheadrightarrow \omega^{\otimes(k+2)}.\end{aligned}$$

The notation $Y_1(N)^h$ indicates that we have picked a maximal open subset that ensures we have a decomposition of $\Omega^1_{Y_1(N)^h/\mathbb{F}_p} \otimes_{\mathcal{O}_{Y_1(N)^h}} H^1_{\mathrm{dR}}(E_{\mathrm{univ}}/Y_1(N))$. This gives us the final projection. Moving now to modular forms, we define the theta operator by

Definition 6.11 (Theta operator)**.** The *theta operator* is defined by

$$\begin{array}{rccc} \theta: & H^0(Y_1(N)^h, \omega^{\otimes k}) & \longrightarrow & H^0(Y_1(N), \omega^{\otimes(k+p+1)}) \\ & f & \longmapsto & A \cdot \tilde{\theta}(f). \end{array} \tag{6.10}$$

Theorem 6.12. *Let $f \in M_k(\Gamma; \overline{\mathbb{F}}_p)$ have Fourier expansion $f(q) = \sum a_n q^n$. Then we have*

$$(\theta f)(q) = q\frac{d}{dq}f(q) = \sum n a_n q^n. \tag{6.11}$$

Proof. See the theorem in [Kat77]. □

6.2 Commutation with Hecke Operator

One of the powerful applications of the theta operator is the commutation relation it shares with the Hecke operator.

Theorem 6.13. *Let $m \in \mathbb{Z}_{>0}$. Then $T_m \circ \theta = m\theta \circ T_m$, where T_m on the left is an operator on $M_{k+p+1}(\Gamma; \overline{\mathbb{F}}_p)$ and on the right on $M_k(\Gamma; \overline{\mathbb{F}}_p)$.*

Proof. Recalling the formula in Example 5.8, we compute

$$\begin{aligned} (\theta \circ T_m f)(q) &= \sum_{n=0}^{\infty} n \left(\sum_{d \mid \gcd(m,n)} d^{k-1} a(mn/d^2) \right) q^n \\ (T_m \circ \theta f)(q) &= \sum_{n=0}^{\infty} \left(\sum_{d \mid \gcd(m,n)} d^{(k+p+1)-1} mn/d^2 a(mn/d^2) \right) q^n \\ &= m \sum_{n=0}^{\infty} n \left(\sum_{d \mid \gcd(m,n)} d^{k-1} d^{p-1} a(mn/d^2) \right) q^n \end{aligned}$$

$$= m \sum_{n=0}^{\infty} n \left(\sum_{d \mid \gcd(m,n)} d^{k-1} a(mn/d^2) \right) q^n,$$

since we have $d^{p-1} \cong 1 \pmod{p}$ by Fermat's Little Theorem. Thus

$$T_m \circ \theta = m\theta \circ T_m, \tag{6.12}$$

as required. □

Remark 6.14. As we saw in chapter 5, the Hecke action is defined by the slash operator for individual double cosets. So an alternate method of proof is to show the commutation relation with a single matrix.

Corollary 6.15. *Let Γ be a congruence subgroup of level N. Let $\ell \nmid N$ be a prime. Let $f \in M_k(\Gamma; \overline{\mathbb{F}}_p)$ be an eigenform for the Hecke algebra at ℓ, $\mathcal{H}_\ell$ with eigensystem Ψ_f. If $\theta f \neq 0$,[1] then θf is also an eigenform for $\mathcal{H}_\ell$ with eigensystem*

$$\begin{aligned} \Psi_{\theta f} : \ \mathcal{H}_\ell &\longmapsto \overline{\mathbb{F}}_p \\ T_\ell &\longmapsto \ell \Psi_f(T_\ell). \end{aligned} \tag{6.13}$$

So given an eigenform with a system of eigenvalues, the image under θ is also an eigenform and it simply has the eigenvalues associated to T_ℓ multiplied by ℓ for each $\ell \nmid N$.

6.3 Siegel Modular Forms

We have seen many views of the theta operator, as well as some interesting properties. We will see in chapter 7 some of the direct applications of these results and their power. When one passes to Siegel modular forms, there are multiple ways to generalise the above theta operator. We will explore two such constructions:

- One arising from a particular bracket of Siegel modular forms.

[1] The only Hecke eigenvectors in the kernel of θ are powers of the Hasse invariant A, see Proposition 2 in [CG13]

- Another arising from algebraic geometry, in an analogous way to Katz.

6.3.1 Boecherer-Nagaoka

This section follows [BN07]. An extension of this is developed in [BN13].

We are now working with degree g scalar-valued Siegel modular forms. Here, we begin by considering $R, S \in M_{g\times g}$, a pair of $g \times g$ matrices. From these, consider

$$\det(R + xS) = \sum_{i=0}^{g} P_i(R, S)x^i. \tag{6.14}$$

That is, take the determinant of the matrix $R+xS$, with x a formal variable. This can be expanded as a polynomial in x, with coefficients being polynomials $P_i(R, S)$ in R and S. We now define a new polynomial, for k_1, k_2 such that $2k_1, 2k_2 \geq g$, by

$$Q^{(g)}_{k_1,k_2}(R, S) = \sum_{i=0}^{g}(-1)^i i!(g-i)!\binom{2k_2 - i}{g-i}\binom{2k_1 - g + i}{i}P_i(R, S). \tag{6.15}$$

The idea now is to substitute in certain matrices of differential operators to build one large differential operator. Specifically, consider

$$\partial_{\mathbf{q}} = \begin{pmatrix} \partial_{11} & \frac{1}{2}\partial_{12} & \cdots & \frac{1}{2}\partial_{1g} \\ \frac{1}{2}\partial_{21} & \partial_{22} & \cdots & \vdots \\ \vdots & \vdots & \ddots & \vdots \\ \frac{1}{2}\partial_{g1} & \cdots & \cdots & \partial_{gg} \end{pmatrix}, \tag{6.16}$$

where $\partial_{ij} = q_{ij}\frac{\partial}{\partial q_{ij}}$. Such objects were studied by Eholzer and Ibukiyama[2] in [EI98], and when the polynomials take the appropriate form the result is indeed an operator on Siegel modular forms. Then we construct the operator

$$D^{(g)}_{k_1,k_2} = Q^{(g)}_{k_1,k_2}(\partial_{\mathbf{q}_1}, \partial_{\mathbf{q}_2}). \tag{6.17}$$

This leads to the following

[2] Along with many others - there is a vast literature on Rankin-Cohen brackets.

Theorem 6.16 ([BN07] Thm 3,[EI98] Thm 2.3)**.** *Let $F \in M_{k_1}(\Gamma;\mathbb{C}), G \in M_{k_2}(\Gamma;\mathbb{C})$ such that $2k_1, 2k_2 \geq g$. Let*

$$[F,G] = D^{(g)}_{k_1,k_2}(\partial_{\mathbf{q}_1}, \partial_{\mathbf{q}_2})(FG)|_{\mathbf{q}=\mathbf{q}_1=\mathbf{q}_2}. \tag{6.18}$$

Then $[F,G] \in S_{k_1+k_2+2}(\Gamma;\mathbb{C})$, i.e. $[F,G]$ is a Siegel cusp form of weight k_1+k_2+2.

Definition 6.17 (Generalised Rankin-Cohen Bracket)**.** Let $F \in M_{k_1}(\Gamma;\mathbb{C}), G \in M_{k_2}(\Gamma;\mathbb{C})$ such that $2k_1, 2k_2 \geq g$. The *first generalised Rankin-Cohen bracket of F and G* is $[F,G] \in S_{k_1+k_2+2}(\Gamma;\mathbb{C})$ as defined in Theorem 6.16.

Remark 6.18. As in 6.8 we only consider the *first* bracket, although there are many more.

Note that we can make this into an operator with input a single form F if we fix a choice of G and construct the map

$$\begin{array}{rccc} [\cdot, G]: & M_{k_1}(\Gamma;\mathbb{C}) & \longrightarrow & S_{k_1+k_2+2}(\Gamma;\mathbb{C}) \\ & F & \longmapsto & [F,G]. \end{array} \tag{6.19}$$

We would now like to make a "nice" choice of G. In particular, we'd like a form whose reduction (mod p) has Fourier expansion $G(\mathbf{q}) = 1$. We saw in Theorem 3.6 that such a form often exists (mod p), called the *Hasse invariant*, and indeed it does arise from the reduction of some form over $\mathbb{Z}_{(p)}$. The difficulty is that the bracket is defined over $\mathbb{C}$, but the desired form only exists (mod p). So we will begin (mod p), choose a lift of the Hasse invariant (denoted G), take the bracket and reduce (mod p) again.

Thanks to the choice of renormalisation, the bracket above preserves subrings $B \subseteq \mathbb{C}$, and so we can choose, say, $B = \mathbb{Z}_{(p)}$. Thus when we take our lift, we are assured that the resulting form can be reduced (mod p), as desired.

Theorem 6.19. *Let $g > 1$, $p > g(g+1)/2$ and $k > g+1$. There is a linear map*

$$\theta_{BN} : M_k(\Gamma;\overline{\mathbb{F}}_p) \longmapsto M_{k+p+1}(\Gamma;\overline{\mathbb{F}}_p) \tag{6.20}$$

which is defined by the following commutative diagram:

$$\begin{tikzcd}
F \arrow[r] \arrow[d, "(mod\ p)"] & \frac{(-1)^g}{(g+1)!}[F,A] \arrow[d, "(mod\ p)"] \\
f \arrow[r] \arrow[u, bend left, dotted, "lift"] & \theta_{BN} f
\end{tikzcd}$$

Further, if $f(\mathbf{q}) = \sum a(\mathbf{n})\mathbf{q}_N^{\mathbf{n}}$ *then*

$$(\theta_{BN} f)(\mathbf{q}) = \frac{1}{N^g} \sum \det(\mathbf{n}) a(\mathbf{n}) \mathbf{q}_N^{\mathbf{n}}. \tag{6.21}$$

Proof. The things to be proven above are that the form f can indeed be lifted to characteristic 0, and the statement about the $\mathbf{q}$-expansion. For the first, one can simply require that you look at the subspace of Siegel modular forms (mod p) which exist as the reduction of something in characteristic 0. However, if we want such a statement to be true of the entire space, we restrict to $k > g + 1$, due to [Str13], Theorem 1.3.

Now, this operator is some polynomial in the derivations $\partial_{\mathbf{q}_1}$ and $\partial_{\mathbf{q}_2}$. However, we have chosen that our form G is a lift of the Hasse invariant, so

$$\begin{aligned}
\partial_{\mathbf{q}_2}(F(\mathbf{q}_1)G(\mathbf{q}_2)) &= F(\mathbf{q}_1)\partial_{\mathbf{q}_2}G(\mathbf{q}_2) \\
&\equiv F(\mathbf{q}_1)\partial_{\mathbf{q}_2}(1) = 0 \qquad \pmod{p}.
\end{aligned}$$

Thus, any terms in the polynomial that have a factor of $\partial_{\mathbf{q}_2}$ will reduce to 0 in the image. So, we have that the only term that contributes anything (mod p) is $P_0(R, S) = \det(R)$, i.e. $\det(\partial_{\mathbf{q}_1})$. Thus the resulting effect on $\mathbf{q}$-expansions is

$$(\theta_{BN} f)(\mathbf{q}) = \frac{(-1)^g}{(g+1)!} g! \binom{2p-2}{g} \det(\partial_{\mathbf{q}}) f(\mathbf{q}). \tag{6.22}$$

Which one can compute to be equal to the expression desired. $\square$

Now we wish to compute the commutation relation between θ_{BN} and the Hecke operators. Our main tool for θ_{BN} is the action on Fourier expansions.

Thus we would like a similar $\mathbf{q}$-expansion expression for a general Hecke operator, which is unfortunately generally ugly.

Recall that at a given prime ℓ, Hecke operators are double cosets KMK, where $K = \mathrm{GSp}_{2g}(\mathbb{Z}_\ell)$. To get the action on modular forms, we decompose $KMK = \coprod_i KM_i$ and then act by each of the matrices M_i via the slash operator. So we must see precisely how to decompose in this way for a given matrix M.

Proposition 6.20. *Let $r \geq 0$ and let $M \in \mathrm{GSp}_{2g}(\mathbb{Q}_\ell)$ such that $\eta(M) = \ell^r$. There exists a g-tuple $b = (b_1, \ldots, b_g) \in \mathbb{Z}^g$ with*

$$r \geq b_1 \geq \ldots \geq b_g \geq 0 \tag{6.23}$$

such that

$$KMK = K \begin{pmatrix} \ell^{r-b} & 0 \\ 0 & \ell^b \end{pmatrix} K, \quad \textit{where} \quad K = \mathrm{GSp}_{2g}(\mathbb{Z}_\ell). \tag{6.24}$$

Moreover, KMK can be decomposed into right cosets of the form

$$K \begin{pmatrix} \ell^r (D^\top)^{-1} & B \\ 0 & D \end{pmatrix}. \tag{6.25}$$

Proof. See [RS08], Proposition 2.10. $\square$

So we have the structure of the matrices appearing in the right coset decomposition. We will now compute the commutation with matrices of that form.

Lemma 6.21. *If $M = \begin{pmatrix} A & B \\ 0 & D \end{pmatrix} \in \mathrm{GSp}_{2g}(\mathbb{Q}_\ell)$, then*

$$(\cdot|_{k+p+1} M) \circ \theta_{BN} = \eta(M)^g \theta_{BN} \circ (\cdot|_k M) = \det(M) \theta_{BN} \circ (\cdot|_k M). \tag{6.26}$$

Proof. Since $M \in \mathrm{GSp}_{2g}(\mathbb{Q}_\ell)$, we have $A = \eta(M)(D^\top)^{-1}$. We will compute the commutation between the slash operator and the operator $[\cdot, G]$ in characteristic zero, before reducing (mod p). Here, let $F \in M_k(\Gamma^g(N); \mathbb{Z}[1/N]_{(p)})$

with

$$F(\mathbf{q}) = \sum_{\mathbf{n}} a(\mathbf{n})\mathbf{q}_N^{\mathbf{n}}, \quad \text{where } \mathbf{q}_N^{\mathbf{n}} = e^{\frac{2\pi i}{N}\operatorname{Tr}(\mathbf{n}Z)}. \tag{6.27}$$

We have

$$[F, G](\mathbf{q}) = \frac{1}{N^g}\sum_{\mathbf{n}} \det(\mathbf{n})a(\mathbf{n})\mathbf{q}_N^{\mathbf{n}} + pB_0(\mathbf{q}), \tag{6.28}$$

where G is a lift of the Hasse invariant, and $B_0(\mathbf{q})$ is a power series in $\mathbf{q}$ with p-integral coefficients. Now as for the slash operator, we can compute the action on the Fourier expansion as

$$\begin{aligned}
(F|_k M)(\mathbf{z}) &= \eta(M)^{kg-g(g+1)/2}\det(D)^{-k}F((A\mathbf{z}+B)D^{-1}) \\
&= \eta(M)^{kg-g(g+1)/2}\det(D)^{-k}\sum_{\mathbf{n}} a(\mathbf{n})c(\mathbf{n})e^{2\pi i\operatorname{Tr}(\mathbf{n}\eta(M)(D^\top)^{-1}\mathbf{z}D^{-1})/N} \\
&= \eta(M)^{kg-g(g+1)/2}\det(D)^{-k}\sum_{\mathbf{n}} a(\mathbf{n})c(\mathbf{n})\mathbf{q}_N^{\mathbf{n}'},
\end{aligned}$$

where $\mathbf{n}' = \eta(M)D^{-1}\mathbf{n}(D^\top)^{-1}$ and $c(\mathbf{n}) = e^{2\pi i\operatorname{Tr}(\mathbf{n}BD^{-1})/N}$. From this, note that

$$\det(\mathbf{n}') = \eta(M)^g\det(D)^{-2}\det(\mathbf{n}). \tag{6.29}$$

From this we now compute that

$$\begin{aligned}
([F, G]|_{k+p+1}M)(\mathbf{q}) &= \frac{1}{N^g}\eta(M)^{(k+p+1)g-g(g+1)/2}\det(D)^{-(k+p+1)} \\
&\quad\times\sum_{\mathbf{n}}\det(\mathbf{n})a(\mathbf{n})c(\mathbf{n})\mathbf{q}_N^{\mathbf{n}'} + pB_0(\mathbf{q})|_k M \\
&= \left(\eta(M)^g\det(D)^{-1}\right)^{p-1}\eta(M)^g \\
&\quad\times\frac{1}{N^g}\eta(M)^{(k+1)g-g(g+1)/2}\det(D)^{-(k+2)} \\
&\quad\times\sum_{\mathbf{n}}\det(\mathbf{n})a(\mathbf{n})c(\mathbf{n})\mathbf{q}_N^{\mathbf{n}'} + pB_0(\mathbf{q})|_k M \\
([F|_k M, G])(\mathbf{q}) &= \frac{1}{N^g}\eta(M)^{(k+1)g-g(g+1)/2}\det(D)^{-(k+2)} \\
&\quad\times\sum_{\mathbf{n}}\det(\mathbf{n})a(\mathbf{n})c(\mathbf{n})\mathbf{q}_N^{\mathbf{n}'} + pB_1(\mathbf{q}).
\end{aligned}$$

When we reduce (mod p), note that the terms including B_0 and B_1 are preceeded by p and thus reduce to zero. Further, the term with exponent

$p-1$ is congruent to 1 (mod p). Thus, reducing (mod p) gives us

$$(\cdot|_{k+p+1}M)\circ\theta_{BN}=\eta(M)^g\theta_{BN}\circ(\cdot|_k M), \tag{6.30}$$

as required. □

Theorem 6.22. *If* $M\in\mathrm{GSp}_{2g}(\mathbb{Q}_\ell)$ *then*

$$(KMK)\circ\theta_{BN}=\det(M)\theta_{BN}\circ(KMK). \tag{6.31}$$

Proof. By Proposition 6.20, we can decompose

$$KMK=\coprod_i KM_i \tag{6.32}$$

where the M_i are of the form used in Lemma 6.21 and $\det(M)=\det(M_i)$. The result now follows by Lemma 6.21. □

6.3.2 Flander-Ghitza

Here we are making use of the algebro-geometric set up of Siegel modular forms we saw in Section 3.5. This mirrors the approach of Katz for $g=1$ which we discussed in section 6.1.2. Full details can be found in [Fla13], and we direct the reader there for definitions and proofs. The space of Siegel modular forms of weight κ can be expressed as

$$M_\kappa(\Gamma^g(N))=H^0(Y^g(N),\mathbb{E}_\kappa). \tag{6.33}$$

As in section 6.1.2, we consider the relative de Rham cohomology $H^1_{\mathrm{dR}}(\mathbb{A}_{g,N}/Y^g(N))$ with its Gauss-Manin connection

$$\nabla_{\mathbb{A}_{g,N}/Y^g(N)}:H^1_{\mathrm{dR}}(\mathbb{A}_{g,N}/Y^g(N))\longrightarrow H^1_{\mathrm{dR}}(\mathbb{A}_{g,N}/Y^g(N))\otimes\Omega^1_{Y^g(N)}. \tag{6.34}$$

Let λ be a highest weight vector for κ. There is a *sheaf-theoretic Schur functor* arising from λ, and we consider $(H^1_{\mathrm{dR}})^\lambda$, the image of the de Rham cohomology under λ. We have an induced connection

$$\nabla^\lambda_{\mathbb{A}_{g,N}/Y^g(N)}:(H^1_{\mathrm{dR}}(\mathbb{A}_{g,N}/Y^g(N)))^\lambda\longrightarrow(H^1_{\mathrm{dR}}(\mathbb{A}_{g,N}/Y^g(N)))^\lambda\otimes\Omega^1_{Y^g(N)}. \tag{6.35}$$

We can now construct the theta operator θ_{FG} as a composite map

$$\begin{aligned}\theta_{FG} : \mathbb{E}_\kappa &\hookrightarrow (H^1_{\mathrm{dR}})^\lambda \\ &\xrightarrow{\nabla^\lambda} (H^1_{\mathrm{dR}})^\lambda \otimes \Omega^1 \\ &\xrightarrow{\mathrm{id}\otimes\kappa^{-1}\otimes h} (\mathbb{E} \oplus \mathbb{E}^\vee)^\lambda \otimes \mathrm{Sym}^2 \mathbb{E} \otimes \omega^{\otimes(p-1)} \\ &\longrightarrow \mathbb{E}_\kappa \otimes \underline{\omega}^{(p-1)} \otimes \mathrm{Sym}^2 \mathbb{E}.\end{aligned}$$

One can see that this effects the weight by sending $M_\kappa \to M_{\kappa\otimes\det^{(p-1)}\otimes\mathrm{Sym}^2}$. As for the effect on Fourier expansions, we have the following.

Theorem 6.23. *Let $f \in M_\kappa$ such that $f(\mathbf{q}) = \sum a(\mathbf{n})\mathbf{q}^{\mathbf{n}}$. Then we have*

$$(\theta_{FG} f)(\mathbf{q}) = \sum_{\mathbf{n}} (\mathbf{n} \otimes a(\mathbf{n}))\mathbf{q}^{\mathbf{n}}. \tag{6.36}$$

Proof. See [Fla13], Theorem 4.2.1. □

The other main feature that we have explored above with the theta operators is the commutation with the Hecke operators, in particular the operators T_ℓ.

Theorem 6.24. *Let $\ell \in \mathbb{Z}_{>0}$ be a prime. Then*

$$T_\ell \circ \theta_{FG} = \ell\theta_{FG} \circ T_\ell. \tag{6.37}$$

Proof. See [Fla13], Theorem 4.5.2. □

Chapter 7

Galois Representations and Serre's Conjecture

One of the main motivating factors in the theory of modular forms is their connection to various interesting Number Theoretic objects. We have seen in section 2.4 that modular forms are closely connected with elliptic curves. In fact, this is part of a much larger picture known as the *Langlands program*. Another object in this picture of associated objects are *Galois representations*. Here we will discuss the Galois group $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ and its representations, and specifically the correspondence in the case of degree 1 modular forms.

7.1 Infinite Galois Theory

As stated, our goals are to study the algebraic numbers $\overline{\mathbb{Q}}$, in particular via the group $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$. There is some detail in the construction of this group, since classical Galois theory focuses largely on *finite* extensions of a field K. So to work with this group, we will first need to see how to pass from the Galois groups of finite extensions to this infinite extension. We first require the following notion.

Definition 7.1 (Inverse/Projective System & Limit)**.** Let $(I, \leq)$ be a partially ordered set. Let $(A_i)_{i\in I}$ be a collection of groups such that if $i \leq j$ we have a homomorphism $f_{ij} : A_j \to A_i$ such that

(1) f_{ii} is the identity on A_i, and

(2) $f_{ik} = f_{ij} \circ f_{jk}$ for all $i \leq j \leq k$.

The pair $A = ((A_i)_{i\in I}, (f_{ij})_{i\leq j\in I})$ is called an *inverse (or projective) system.*

Given an inverse system, the *inverse (or projective) limit* is

$$\varprojlim_{i\in I} A = \left\{ \vec{a} \in \prod_{i\in I} A_i \;\middle|\; a_i = f_{ij}(a_j) \text{ for all } i \leq j \in I \right\}. \tag{7.1}$$

The value of this for us is it allows us to pass from the family of Galois groups attached to finite extensions of a base field K to a larger collection. The above limit means for us to take the product of all the finite Galois groups, but the homomorphisms f_{ij} keep track of how related Galois groups interact. In particular, consider two Galois extensions L_1/K and L_2/K such that L_2/L_1 is also a Galois extension. Then we have a natural map $\phi_{L_1}^{L_2} : \mathrm{Gal}(L_2/K) \to \mathrm{Gal}(L_1/K)$ which is simply restriction of all the automorphisms $\omega \in \mathrm{Gal}(L_2/K)$ to the domain L_1. These are then also automorphisms of L_1, and thus we have an inverse system of groups. This leads us to the following definition.

Definition 7.2 (Absolute Galois Group)**.** Let K be a field. Let $\mathcal{K}$ be the set of Galois extensions of K. The *absolute Galois group of* K is the group

$$G_K = \varprojlim_{L\in\mathcal{K}} \mathrm{Gal}(L/K). \tag{7.2}$$

We would like to connect the absolute Galois group with the algebraic closure, however there are some minor technical obstacles. Consider the Galois extensions of K as splitting fields of various polynomials f. So the effect of the Galois groups of these extensions is to permute the roots of these polynomials. However, the polynomials can in general have repeated roots, and the Galois group cannot distinguish these. We therefore are motivated to introduce the following.

Definition 7.3 (Separable Polynomial/Extension)**.** A polynomial is *separable* if it has distinct roots. An extension L/K is *separable* if its minimal polynomial is separable.

Further, we can introduce the following.

Definition 7.4 (Separably Closed)**.** A field K is *separably closed* if for all separable polynomials f over K, then if $f(x) = 0$ then $x \in K$.

We can construct a *separable closure* of a field K, similarly to how we can construct an algebraic closure $\overline{K}$, which we denote K^{sep}. This is the object that the Galois group is able to determine, and in fact we have this result.

Proposition 7.5.

$$G_K = \mathrm{Gal}(K^{sep}/K). \tag{7.3}$$

Proof. See [Mil03], Example 7.24. □

We are primarily interested in the case $K = \mathbb{Q}$, in which case we in fact have $\mathbb{Q}^{\text{sep}} = \overline{\mathbb{Q}}$, and thus

$$G_{\mathbb{Q}} = \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}). \tag{7.4}$$

We now have a definition of the group $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$. However, we still have very little idea of its structure. One of the most powerful ways to study a group is to study its representations, i.e. consider ways of having said group act on a vector space. We now consider how one can construct such representations and how they may be classified.

7.2 Galois representations

There are many available references for Galois representations, but we are particularly interested in the connection with modular forms. Thus, particularly favourite references for the following are [Rib95] and [RS99].

A *representation* of the group $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ is a group homomorphism

$$\rho : \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \longrightarrow \mathrm{GL}(V). \tag{7.5}$$

However, we can endow $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ with additional structure, and thereby restrict to particular representations of interest. Specifically, we can view $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ as a *topological group*. This topology arises from the definition as the inverse limit of the finite Galois groups $\mathrm{Gal}(L/\mathbb{Q})$. Each of these finite groups is endowed with the discrete topology. From this, and the inverse limit construction, we arrive at a topology on $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ called a *profinite topology*. Groups arising as inverse limits of systems of finite groups are called *profinite groups*. From this point on, we will be considering *continuous* representations of $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$. That is, topological group homomorphisms, where the topology on $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ is the profinite topology discussed above and the topology on $\mathrm{GL}(V)$ comes from a topology on V.

We will now look at some special elements of $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$, which will later be our main focus when considering these representations. To begin, let $K/\mathbb{Q}$ be a Galois extension. Let $\mathcal{O}_K$ be the ring of integers of K, i.e. elements of K which are roots of *monic* polynomials with coefficients in $\mathbb{Z}$. In fact, the Galois group $\mathrm{Gal}(K/\mathbb{Q})$ fixes $\mathcal{O}_K$ (not pointwise), so given $\sigma \in \mathrm{Gal}(K/\mathbb{Q}), x \in \mathcal{O}_K$, we have that $\sigma(x) \in \mathcal{O}_K$. Further, since the Galois action is via ring automorphisms, it induces an action on the ideals, and further an action on the set of prime ideals containing a prime p. Any two prime ideals $\mathfrak{p}_1$ and $\mathfrak{p}_2$ containing p are conjugate under the action of $\mathrm{Gal}(K/\mathbb{Q})$.
Definition 7.6 (Decomposition Group)**.** Let $\mathfrak{p} \in \mathcal{O}_K$ such that $p \in \mathfrak{p}$. The *decomposition group of* $\mathfrak{p}$ is the subgroup $D_{\mathfrak{p}} \subseteq \mathrm{Gal}(K/\mathbb{Q})$ consisting of σ such that $\sigma(\mathfrak{p}) = \mathfrak{p}$.

Recall that the prime ideal associated to p in $\mathbb{Z}$ is simply $p\mathbb{Z}$. However, in $\mathcal{O}_K$ we make a choice of $\mathfrak{p}$, since p can be contained in more than one prime ideal. In fact, the ideal $p\mathcal{O}_K = \mathfrak{p}_1^{e_1} \dots \mathfrak{p}_n^{e_n}$ for some prime ideals $\mathfrak{p}_i \in \mathcal{O}_K$ with exponents $e_i \in \mathbb{Z}_{>0}$.

Definition 7.7 (Ramification)**.** Let $K/\mathbb{Q}$ be an extension with ring of integers $\mathcal{O}_K$, and $p \in \mathbb{Z}$. Then $p\mathcal{O}_K = \mathfrak{p}_1^{e_1} \ldots \mathfrak{p}_n^{e_n}$, for $\mathfrak{p}_i$ prime ideals in $\mathcal{O}_K$ and $e_i \in \mathbb{Z}_{>0}$.

(1) p is *ramified* in $\mathcal{O}_K$ if there exists some i such that $e_i > 1$.

(2) p is *tamely ramified* in $\mathcal{O}_K$ if it is ramified and $\gcd(e_i, p) = 1$ for all $1 \leq i \leq n$.

(3) p is *split* in $\mathcal{O}_K$ if $e_i = 1$ for all $1 \leq i \leq n$.

(4) p is *inert* in $\mathcal{O}_K$ if $n = 1$ and $e_1 = 1$, i.e. $p\mathcal{O}_K$ is a prime ideal of $\mathcal{O}_K$.

Remark 7.8. We are often only interested in whether or not the prime is ramified, so scenarios (3) and (4) above are often collectively referred to as *unramified.*

For a prime ideal $\mathfrak{p}$ in $\mathcal{O}_K$, we denote $\mathbb{F}_\mathfrak{p} = \mathcal{O}_K/\mathfrak{p}$. This can in fact be viewed as an extension $\mathbb{F}_\mathfrak{p}/\mathbb{F}_p$.

Proposition 7.9. *Let $K/\mathbb{Q}$ be an extension with ring of integers $\mathcal{O}_K$, and $p \in \mathbb{Z}$. Let $\mathfrak{p}$ be a prime ideal in $\mathcal{O}_K$ such that $p \in \mathfrak{p}$. The homomorphism*

$$D_\mathfrak{p} \longrightarrow \mathrm{Gal}(\mathbb{F}_\mathfrak{p}/\mathbb{F}_p) \tag{7.6}$$

is surjective. We call the kernel the inertia group*, $I_\mathfrak{p}$. Further, if p is unramified in $\mathcal{O}_K$, then $I_\mathfrak{p} = 1$ (and thus the above map is an isomorphism).*

Proof. See [Mil98], page 140. □

So we can think of the decomposition group (which is a subgroup of $\mathrm{Gal}(K/\mathbb{Q})$) in terms of the group $\mathrm{Gal}(\mathbb{F}_\mathfrak{p}/\mathbb{F}_p)$. In fact, all extensions of $\mathbb{F}_p$ are of the form $\mathbb{F}_{p^n}/\mathbb{F}_p$, and thus $\mathrm{Gal}(\mathbb{F}_\mathfrak{p}/\mathbb{F}_p)$ is just the cyclic group of order n. It is generated by the *Frobenius automorphism*

$$x \longmapsto x^p. \tag{7.7}$$

So, if p is unramified in $\mathcal{O}_K$, we can consider the preimage of this automorphism under the map above, $\sigma_\mathfrak{p} \in D_\mathfrak{p}$. Since the $\mathfrak{p}$ are all conjugate, we will simply express this element as σ_p, recalling that it is only defined by p up to conjugation.

Let's take this a step further. We can find an element of $\mathrm{Gal}(K/\mathbb{Q})$ which arises from this Frobenius automorphism for some $K/\mathbb{Q}$ Galois, but our true interest is in $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$. Let $\mathfrak{p}$ be a prime ideal in $\mathcal{O}_{\overline{\mathbb{Q}}}$ containing p. One should think of this as a choice of $\mathfrak{p}$ in $\mathcal{O}_K$ for all finite extensions $K/\mathbb{Q}$ such that inclusions are preserved. Again we have a decomposition group $D_\mathfrak{p}$ and a field $\mathbb{F}_\mathfrak{p}$, which in this case is a choice of algebraic closure for $\mathbb{F}_p$. In this way we can consider the same surjective map $D_\mathfrak{p} \to \mathrm{Gal}(\mathbb{F}_\mathfrak{p}/\mathbb{F}_p)$ and the Frobenius automorphism $(x \mapsto x^p)$. We can thus choose a preimage of this in $D_\mathfrak{p} \subseteq \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$.

Definition 7.10 (Frobenius Element)**.** Let $p \in \mathbb{Z}$ be a prime. Let $\mathfrak{p}$ be a prime ideal in $\mathcal{O}_{\overline{\mathbb{Q}}}$ containing p. The *Frobenius element* Frob_p is the preimage of $(x \mapsto x^p)$ under the map

$$D_\mathfrak{p} \longrightarrow \mathrm{Gal}(\mathbb{F}_\mathfrak{p}/\mathbb{F}_p). \tag{7.8}$$

Proposition 7.11. *The elements* Frob_p *for each prime* p *generate the group* $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ *topologically, i.e. they generate a dense subgroup.*

Remark 7.12. Really it is very poor to refer to this as *the* Frobenius element Frob_p, for two reasons.

(1) As discussed above, it is only defined up to conjugacy in $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$, but this is no obstacle as long as we take it to be defined up to conjugacy.

(2) The inertia subgroup for this choice of $\mathfrak{p}$, $I_\mathfrak{p}$, is very large and thus we cannot generally make a coherent choice of preimage of $(x \to x^p)$. We require a notion of unramified that can work for all choices of $\mathfrak{p}$ in our finite extensions simultaneously.

Definition 7.13 (Unramified Representation)**.** Let

$$\rho : \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \longrightarrow \mathrm{GL}(V) \tag{7.9}$$

be a representation. We say ρ is *unramified at* p if for all $\mathfrak{p}$ containing p we have that $\rho(I_\mathfrak{p}) = 1$.

Remark 7.14. Recalling that all $\mathfrak{p}$ are conjugate in $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$, we in fact only need to ensure the above holds for one choice of $\mathfrak{p}$.

So if ρ is unramified at p, then the image of Frob_p is well defined up to conjugation. Further, since these topologically generate $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$, a given representation ρ is uniquely determined by the images of Frob_p for all p such that ρ is unramified at p. Further, when referring to the decomposition/inertia group at any prime ideal $\mathfrak{p}$ containing p, we will simply write D_p or I_p, respectively.

Example 7.15 (Mod p Cyclotomic Character)**.** Let μ_p be the group of pth roots of unity. As elements of $\overline{\mathbb{Q}}$, these are permuted by $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$. Since μ_p is the cyclic group of order p, any automorphism is a power map. Thus we have an isomorphism

$$\begin{array}{rccc} \varphi : & \mathrm{GL}(\mu_p) & \xrightarrow{\sim} & \mathbb{F}_p^\times \\ & (\zeta \mapsto \zeta^m) & \longmapsto & m. \end{array} \tag{7.10}$$

We can now define the *mod p cyclotomic character* as

$$\begin{array}{rccc} \chi : & \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) & \longrightarrow & \mathbb{F}_p^\times \\ & \sigma & \longmapsto & \chi(\sigma), \end{array} \tag{7.11}$$

where $\sigma \cdot \zeta = \zeta^{\chi(\sigma)}$, for $\sigma \in \mu_p$.

This has a number of interesting properties:

(1) χ is unramified at all primes $\ell \neq p$.

(2) $\chi(\mathrm{Frob}_\ell) = \ell$, for all primes $\ell \neq p$.

7.3 Modular Forms and Serre's Conjecture

Now we have the language of Galois representations, we wish to see how to build them. This is where the theory of modular forms becomes strongly interlinked. Specifically, given a modular form (for $g = 1$), one can construct from it a Galois representation. This is a result of Deligne, as given below.

Theorem 7.16 (Deligne). *Let $f \in M_k(\Gamma_1(N), \varepsilon; \overline{\mathbb{F}}_p)$ be a normalised eigenform* (mod p) *such that $f(q) = \sum a(n)q^n$. There exists a semi-simple continuous Galois representation*

$$\rho_f : \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \longrightarrow \mathrm{GL}_2(\overline{\mathbb{F}}_p) \tag{7.12}$$

which is unramified for all primes $\ell \not| pN$ and such that

$$\mathrm{charpoly}(\rho_f(\mathrm{Frob}_\ell)) = X^2 - a(\ell)X + \varepsilon(\ell)\ell^{k-1} \tag{7.13}$$

for all $\ell \nmid pN$.

Proof. See [G$^+$90], Proposition 11.1. □

Note that this result is highly dependent on the choice of congruence subgroup $\Gamma_1(N)$ and character ε. However, we have seen that if one is considering such things, picking ε to be the trivial character recovers the group $\Gamma_0(N)$, so that appears as a subresult of the above. The group $\Gamma(N)$ is more difficult, since it is a subgroup of $\Gamma_1(N)$, and thus the space of modular forms attached to it is larger and we cannot extend results to it in general. However, we noted this already in chapter 2, specifically the homomorphism (2.21). This injection allows us to view $\Gamma_1(N^2)$ as a subgroup of $\Gamma(N)$, and thus the above holds for $\Gamma(N)$, though the level changes to N^2. Furthermore, the formula for the characteristic polynomial is unaffected since the Fourier expansion is unchanged.

So we now have the ability to construct certain representations of $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ from modular forms. While this is a powerful way of generating nice examples, it turns out there is a far more powerful relationship at work here. That is, *all* Galois representations of the above type are isomorphic to one constructed from a modular form. This was conjectured by Serre in [S$^+$87], and proved by Khare-Wintenberger (see [KW10]). First we will make clear what we mean by "the above type".

Definition 7.17 (Odd Representation). A Galois representation $\rho : \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \to \mathrm{GL}(V)$ is *odd* if $\det(\rho(c)) = -1$, where c is a complex conjugation.

The point of this is that all representations arising from modular forms are odd representations.

Theorem 7.18 (Serre's Conjecture)**.** *Let* $\rho : \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \to \mathrm{GL}_2(\overline{\mathbb{F}}_p)$ *be an irreducible, odd representation.*

(1) There exist k*,* N*,* ε *and a cusp form* $f \in S_k(\Gamma_1(N), \varepsilon; \overline{\mathbb{F}}_p)$ *which is an eigenform, such that* $\rho \cong \rho_f$*, where* ρ_f *is the Galois representation attached to* f *by Theorem 7.16.*

(2) There exists an cusp form $f \in S_{k_\rho}(\Gamma_1(N_\rho), \varepsilon_\rho; \overline{\mathbb{F}}_p)$ *which is an eigenform, such that* $\rho \cong \rho_f$ *as above, where* N_ρ*,* k_ρ *and* ε_ρ *are given by explicit formulas from* ρ*.*

Statement (1) above is known as *Serre's weak conjecture*, since it makes no statement about the data of the eigenform. Statement (2), the *strong conjecture*, by comparison gives precise formulas for N_ρ, ε_ρ and k_ρ, that is the level, character and weight of the form that gives rise to that particular representation.

7.4 Theta Operator

We explored the theta operator in some depth in chapter 6. In particular, we gathered some data about its commutation with the Hecke operators T_ℓ. The Hecke operators are of particular relevance here, since the Galois representation ρ_f above is dependent on the values $a(\ell)$, but since f is a normalised eigenform, these are precisely the Hecke eigenvalues, i.e. $\Psi_f(T_\ell) = a(\ell)$. The commutation we have proved leads to the following.

Theorem 7.19.

$$\rho_{\theta f} = \chi \otimes \rho_f \tag{7.14}$$

Proof. First note that if f is a a normalised eigenform with $f(q) = \sum a(n)q^n$, then θf is a normalised eigenform with $(\theta f)(q) = \sum na(n)q^n$. Further, θf is of weight $k+p+1$. So one can construct the Galois representation attached to θf, and we have

$$\operatorname{charpoly}(\rho_{\theta f}(\mathrm{Frob}_\ell)) = X^2 - \ell a(\ell) + \varepsilon(\ell)\ell^{(k+p+1)-1} = X^2 - \ell a(\ell) + \varepsilon(\ell)\ell^{k+p}. \tag{7.15}$$

As for $\chi \otimes \rho f$, pick a basis for $\overline{\mathbb{F}}_p^2$ such that

$$\rho_f(\mathrm{Frob}_\ell) = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \quad \text{and thus} \quad (\chi \otimes \rho_f)(\mathrm{Frob}_\ell) = \begin{pmatrix} \ell a & \ell b \\ \ell c & \ell d \end{pmatrix}. \tag{7.16}$$

So if $\operatorname{charpoly}(\rho_f(\mathrm{Frob}_\ell)) = X^2 - a(\ell)X + \varepsilon(\ell)\ell^{k-1}$, then

$$\begin{aligned} \operatorname{charpoly}((\chi \otimes \rho_f)(\mathrm{Frob}_\ell)) &= X^2 - \ell a(\ell)X + \ell^2\varepsilon(\ell)\ell^{k-1} \\ &= X^2 - \ell a(\ell)X + \varepsilon(\ell)\ell^{k+1}. \end{aligned} \tag{7.17}$$

However note that $\varepsilon(\ell)\ell^{k+p} \equiv \varepsilon(\ell)\ell^{k+1} \pmod p$, by Fermat's Little theorem. Thus since we have two irreducible Galois representations which have the same characteristic polynomial for Frob_ℓ for all primes ℓ at which they are unramified, they are isomorphic, as required. □

This turns out to be an extremely powerful tool for studying Galois representations attached to modular forms. In particular, we can combine it with the following result.

Theorem 7.20 ([Edi92], Theorem 3.4)**.** *Let $f \in S_k(\Gamma_1(N), \varepsilon; \overline{\mathbb{F}}_p)$ be an eigenform. There exist integers $0 \le \alpha \le p-1$, $k' \le p+1$ such that there exists an eigenform $g \in S_{k'}(\Gamma_1(N), \varepsilon; \overline{\mathbb{F}}_p)$ such that*

$$\Psi_f(T_\ell) = \Psi_{\theta^\alpha g}(T_\ell) \tag{7.18}$$

for all primes $\ell \neq p$.

That is, up to the application of a power of θ, all systems of (mod p) eigenvalues occur in weights $\le p+1$. This is a critical tool in many proofs concerning modular forms and Galois representations. One extremely direct corollary is the following.

Corollary 7.21. *Let ρ be a Galois representation such that there exists $f \in S_k(\Gamma_1(N), \varepsilon; \overline{\mathbb{F}}_p)$ such that $\rho \cong \rho_f$. Then there exists $g \in S_{k'}(\Gamma_1(N), \varepsilon; \overline{\mathbb{F}}_p)$ with $k' \leq p+1$ such that*

$$\rho_f \cong \chi^\alpha \otimes \rho_g \tag{7.19}$$

for some $0 \leq \alpha \leq p-1$.

7.5 Weight in Serre's Conjecture

A major step in understanding Serre's conjecture was the work done passing from the weak conjecture to the strong conjecture. That is, given a representation which one assumes is arising from a modular form f, is there a form g with specified weight, level and character which also gives rise to this representation?

The most difficult step is the determination of the weight k_ρ of the form which we can be assured to give the representation ρ. A formula for k_ρ can be found in [Edi92], Definition 4.3. The claim is then as follows.

Theorem 7.22 (See [Edi92], Theorem 4.5)**.** *Let $\rho : \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \to \mathrm{GL}_2(\overline{\mathbb{F}}_p)$ be an irreducible, odd representation. Suppose there exists $g \in S_k(N, \varepsilon; \overline{\mathbb{F}}_p)$ where $p \nmid N$ such that $\rho \cong \rho_g$. Then there exists an eigenform $f \in S_{k(\rho)}(N, \varepsilon; \overline{\mathbb{F}}_p)$ such that the f and g have the same eigenvalues for T_ℓ where $\ell \neq p$, and thus $\rho \cong \rho_f$.*[1] *Further, this is the minimal such weight of a cusp form that gives rise to ρ.*

Proof. The proof uses many tricks and congruences which become available when one restricts to weights $k \leq p+1$. Fortunately, Theorem 7.20 tells us that given any form f there exists a form g such that $f = \theta^\alpha g$ and the weight of g is $\leq p+1$, so we can work with that.

Another remarkable way the theta operator plays a role here is via the theory of *theta cycles*, which are displayed in [Edi92], Proposition 3.3. One can

[1] For a definition of $k(\rho)$, see [Edi92], Definition 4.3.

readily observe that $\theta^p = \theta$, so the sequence generated by recurring applications of θ is cyclical. The powerful notion is in fact that the intermediate steps of the sequence follow very precise patterns, particularly if one focuses on the weights of the forms in the sequence. Knowledge of these patterns gives one precise information about what possible weights can arise, and this is exploited in the proof of the above theorem.

For full details, see [Edi92], the proof of Theorem 4.5. $\square$

Chapter 8

Satake Isomorphism

8.1 The Isomorphism

To set this up, we must turn our attentions back to the definitions and concepts we discussed in chapter 4. One may notice there are certain features in common between the group GSp_{2g} and dual group GSpin_{2g+1} we defined. For example, the dominant coweights index useful data for both groups. Specifically, from Proposition 4.13 the Hecke algebra attached to GSp_{2g} has basis $\{T_{\lambda(\ell)}\}$, while from Corollary 4.6 each λ gives and irreducible representation of GSpin_{2g+1}.

So one can expect that these Hecke algebras have a rather direct connection to the representation ring of the dual group. This is expressed in a map called the Satake isomorphism. This is given by the following

Theorem 8.1 (Satake Isomorphism)**.** *Let $\mathbb{F}$ be a local field with ring of integers $\mathcal{O}_{\mathbb{F}}$, and uniformizing parameter π. Let q be the cardinality of the residue field $\mathcal{O}_{\mathbb{F}}/\pi\mathcal{O}_{\mathbb{F}}$. Let $R(\hat{G})$ be the representation ring of the dual group of G. Then we have an isomorphism of rings*

$$\mathcal{S}_{\mathbb{Z}} : \mathcal{H}(G(\mathbb{F}), G(\mathcal{O}_{\mathbb{F}})) \otimes \mathbb{Z}[q^{1/2}, q^{-1/2}] \ \xrightarrow{\sim}\ R(\hat{G}) \otimes \mathbb{Z}[q^{1/2}, q^{-1/2}]. \quad (8.1)$$

Proof. See [Gro98b] Proposition 3.6, or [Car79] Theorem 4.1. □

Remark 8.2. Recall that our case of interest is $G = \mathrm{GSp}_{2g}$, $F = \mathbb{Q}_\ell$ being the local Hecke algebra at ℓ acting on the space of forms $\pmod p$. So we are interested in the map

$$\mathcal{S}_{p,\ell} : \mathcal{H}_\ell \otimes \overline{\mathbb{F}}_p \longrightarrow R(\mathrm{GSpin}_{2g+1}) \otimes \overline{\mathbb{F}}_p. \tag{8.2}$$

Note that this remains an isomorphism since we only need to be able to invert ℓ, and this is possible in $\overline{\mathbb{F}}_p$ because $\ell \neq p$.

We have two choices of basis for the ring $R(\hat{G})$, one being the characters χ_λ indexed by $\lambda \in X^\vee$ dominant, the other being the images $\mathcal{S}(T_{\lambda(\ell)})$, where $T_{\lambda(\ell)}$ is a basis for the Hecke algebra, also indexed by $\lambda \in X^\vee$ dominant. We have the change of basis formulas

$$\mathcal{S}(T_{\lambda(\ell)}) = \ell^{\langle \rho, \lambda \rangle} \chi_\lambda + \sum_{\mu} b_\lambda(\mu) \ell^{\langle \rho, \mu \rangle} \chi_\mu$$

$$\chi_\lambda = \ell^{-\langle \rho, \lambda \rangle} \left(\mathcal{S}(T_{\lambda(\ell)}) + \sum_{\mu} d_\lambda(\mu) S(T_{\mu(\ell)}) \right),$$

with $b_\lambda(\mu), d_\lambda(\mu) \in \mathbb{F}_p$. In fact, we have the following result about these formulas.

Proposition 8.3. *We have*

$$\mathcal{S}(T_{\lambda(\ell)}) = \ell^{\langle \rho, \lambda \rangle} \chi_\lambda + \sum_{\mu < \lambda} b_\lambda(\mu) \ell^{\langle \rho, \mu \rangle} \chi_\mu$$

$$\chi_\lambda = \ell^{-\langle \rho, \lambda \rangle} \left(\mathcal{S}(T_{\lambda(\ell)}) + \sum_{\mu < \lambda} d_\lambda(\mu) S(T_{\mu(\ell)}) \right),$$

i.e. the sums are indexed by cocharacters which are less than λ via the ordering in equation (4.4).

Proof. See [Car79], pg 148 and Theorem 4.1. □

Remark 8.4. The crucial feature is that the only differences between the indexed cocharacters and λ are coroots, which will be useful for us in the future.

8.2 Satake Parameters

Lemma 8.5. *There is a bijection*

$$\begin{array}{ccc} \left\{ \begin{array}{c} \textit{Semisimple conjugacy} \\ \textit{classes in } \hat{G}(\overline{\mathbb{F}}_p) \end{array} \right\} & \longleftrightarrow & \left\{ \begin{array}{c} \textit{Ring homomorphisms} \\ R(\hat{G}) \otimes \overline{\mathbb{F}}_p \to \overline{\mathbb{F}}_p \end{array} \right\} \\ s & \longmapsto & \left(\begin{array}{cccc} \omega_s : & R(\hat{G}) \otimes \overline{\mathbb{F}}_p & \to & \overline{\mathbb{F}}_p \\ & \chi & \mapsto & \chi(s). \end{array} \right) \end{array}$$

Proof. For the same statement over $\mathbb{C}$, see Theorem 8 in [Fre07]. We will now give a brief description of how this correspondence works.

The first point of note is that any semisimple element is conjugate to an element in a maximal torus, so we can view semisimple conjugacy classes as elements of $\hat{T}/W$. From this point, one interesting way to see this correspondence is to consider the functor Spec applied to the ring $R(\hat{G}) \otimes \overline{\mathbb{F}}_p$. Since the right hand side is the set $\mathrm{Hom}_{\mathsf{Ring}}(R(\hat{G}) \otimes \overline{\mathbb{F}}_p, \overline{\mathbb{F}}_p)$, we have a bijection to the set $\mathrm{Hom}_{\mathsf{Scheme}}(\mathrm{Spec}(\overline{\mathbb{F}}_p), \mathrm{Spec}(R(\hat{G}) \otimes \overline{\mathbb{F}}_p))$. There is an isomorphism $R(\hat{G}) \cong R(\hat{T})^W$, where $W = N(T)/T$, for instance see [Ser68], Theorem 4. From this, we can deduce that $\mathrm{Spec}(R(\hat{G})) \cong \mathrm{Spec}(R(\hat{T})^W) \cong \hat{T}/W$. So we have a bijection

$$\mathrm{Hom}_{\mathsf{Ring}}(R(\hat{G}) \otimes \overline{\mathbb{F}}_p, \overline{\mathbb{F}}_p) \longrightarrow \mathrm{Hom}_{\mathsf{Scheme}}(\mathrm{Spec}(\overline{\mathbb{F}}_p), \hat{T}/W \otimes \overline{\mathbb{F}}_p). \tag{8.3}$$

However, a map of schemes $\mathrm{Spec}(k) \to X$ gives precisely the set of k-points in X. Thus we have a bijection between the desired set of ring homomorphisms and the set of $\overline{\mathbb{F}}_p$-points in $\hat{T}/W$, which is precisely the set of semisimple conjugacy classes, as required. $\square$

Corollary 8.6. *The $\overline{\mathbb{F}}_p$-valued characters of the Hecke algebra $\mathcal{H}_\ell$ are indexed by semi-simple conjugacy classes in $\hat{G}(\overline{\mathbb{F}}_p)$.*

Proof. Given a character $\Psi : \mathcal{H}_\ell \otimes \overline{\mathbb{F}}_p \to \overline{\mathbb{F}}_p$, we can construct a character of $R(\hat{G}) \otimes \overline{\mathbb{F}}_p$ by $\Psi \circ \mathcal{S}_{p,\ell}^{-1}$, which is associated to a semisimple conjugacy class.

Given a semisimple conjugacy class s, we associate a character $\omega_s : R(\hat{G}) \otimes \overline{\mathbb{F}}_p \to \overline{\mathbb{F}}_p$, and then can construct a character of $\mathcal{H}_\ell \otimes \overline{\mathbb{F}}_p$ by $\omega_s \circ \mathcal{S}_{p,\ell}$. $\square$

From this, we can come to the following concept.

Definition 8.7 (Satake Parameter)**.** Given an $\overline{\mathbb{F}}_p$-valued character Ψ of $\mathcal{H}_\ell$, the *Satake Parameter of* Ψ*, often denoted* s_Ψ*,* is the semisimple conjugacy class in $\hat{G}$ given by corollary 8.6.

8.3 Modular Forms

We wish to use this theory for our area of interest, that is, Siegel modular forms. The useful idea is that explored in chapter 5, that the Hecke operators can be viewed as one large Hecke algebra, and this is precisely the Hecke algebra we wish to consider here. As it transpires, given a Siegel modular form and a choice of prime ℓ for our Hecke algebra $\mathcal{H}_\ell$ we will be able to associate to it a conjugacy class in $\mathrm{GSpin}_{2g+1}(\overline{\mathbb{F}}_p)$ with the machinery above.

Proposition 8.8. *Given an eigenform f for the Hecke algebra at ℓ, $\mathcal{H}_\ell$, we can construct a Satake parameter attached to it, denoted $s_{f,\ell} \in \mathrm{GSpin}_{2g+1}(\overline{\mathbb{F}}_p)$.*

Proof. Consider an eigenform f such that $Tf = \Psi_f(T)f$, where $\Psi_f(T) \in \overline{\mathbb{F}}_p$. Let ℓ be a prime and let $\mathcal{H}_\ell$ be the local Hecke algebra at ℓ. Then

$$\begin{array}{rccc} \Psi_{f,\ell}: & \mathcal{H}_\ell & \longrightarrow & \overline{\mathbb{F}}_p^\times \\ & T & \longmapsto & \Psi_{f,\ell}(T) \end{array} \tag{8.4}$$

is a character of the local Hecke algebra at ℓ, $\mathcal{H}_\ell$. We now construct a character of the representation ring by $\omega_{f,\ell} = \Psi_{f,\ell} \circ \mathcal{S}_{p,\ell}^{-1}$. As above, this corresponds to a semisimple conjugacy class $s_{f,\ell} \in \mathrm{GSpin}_{2g+1}(\overline{\mathbb{F}}_p)$. We have that

$$\omega_{f,\ell}(\chi) = \left(\Psi_{f,\ell} \circ \mathcal{S}_{p,\ell}^{-1}\right)(\chi) = \chi(s_{f,\ell}). \tag{8.5}$$

$\square$

Chapter 9

Galois Representations and Theta Operators for Siegel Modular Forms

We now come to the main goal of this thesis. That is, to address the issue of extending some of the theory discussed in chapter 7 to the Siegel case. Recall that there we explored the connection between modular forms and Galois representations. There are many reasons one may wish to extend this. Firstly, and most simplistically, if Siegel modular forms are to serve as a good generalisation of modular forms, one should expect that all data associated to them should have some similar generalisation. Secondly, one may have noticed that all representations arising in chapter 7 were 2-dimensional. This is highly restrictive, and in general one would hope to have a theory which could encompass the higher-dimensional representations. Since Siegel modular forms are a higher dimensional generalisation of modular forms, this is where we choose to look.

The ultimate goal would be to extend the theory of chapter 7 fully to the case of Siegel modular forms of any degree g. That is, to precisely formulate a method of producing a Galois representation from a Siegel modular form, and vice versa. We have focused our attention on a few key points.

(1) How do we associate a Galois representation to a Siegel modular form?

(2) What are some generalisations of the Theta Operator?

(3) How does the Theta action affect the Galois representation?

We will begin with an analysis of the degree 2 case. While not entirely classical, this case is quite well developed, certainly significantly more so than $g > 2$, as we will see below.

9.1 Degree 2

Here we are considering Siegel modular forms of degree 2. That is, modular forms attached to the group GSp_4.

This case has been approached in [T$^+$91], [Lau97], and [Wei05]. Here one has a result in a pleasingly similar format to Theorem 7.16. It can be expressed in the following

Theorem 9.1. *Let $\Gamma \subseteq \mathrm{Sp}_4(\mathbb{Z})$ be a congruence subgroup of level N, and let $f \in M_k(\Gamma; \overline{\mathbb{F}}_p)$ be a Siegel modular eigenform for all T_ℓ such that $\ell \nmid pN$, with eigenvalues $a(\ell), a(\ell^2) \in \overline{\mathbb{F}}_p$. Then there exists a unique semisimple continuous representation*

$$\rho_f : \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \longrightarrow \mathrm{GSp}_4(\overline{\mathbb{F}}_p) \tag{9.1}$$

which is unramified outside pN and such that for all $\ell \nmid pN$, the characteristic polynomial of the image of the Frobenius element Frob_ℓ is

$$\begin{aligned}\operatorname{charpoly} \rho_f(\mathrm{Frob}_\ell) = X^4 - a(\ell)X^3 + \left(a(\ell)^2 - a(\ell^2) - \ell^{2k-4}\right) X^2 \\ - \ell^{2k-3}a(\ell)X + \ell^{4k-6}.\end{aligned}$$

Proof. This statement is a special case of a much larger and more powerful result which was the culmination of the work across [T$^+$91], [Lau97], and

[Wei05]. In particular, the above is a consequence of Theorem 2 in [T$^+$91], Theorem 7.5 in [Lau97], and Theorem 1 in [Wei05].

The result stated here is for scalar-valued Siegel modular forms (mod p), but the results that lead to it are in general for vector-valued forms in characteristic zero. Scalar-valued forms are a special case of vector valued, so that part can easily follow from a more general result. To get the result (mod p), one takes the form f, lifts it to F in characteristic zero (See [Str13] for when we can lift), computes the result for F, and then reduces the result (mod p). $\square$

One observation of interest here is that we do not get just any 4-dimensional representations from this procedure. The image of a representation arising from a degree to Siegel modular form has image contained in $\mathrm{GSp}_4(\overline{\mathbb{F}}_p)$. This is intrinsically related to the fact that these forms are defined with respect to the group GSp_4, and we will see this more clearly when we pass to the case of general g.

The existence of such a formula makes computation and proving results very neat. For example, we can see features like the weight k appearing explicitly. However, passing to $g > 2$ such formulas will not be available in general, as we shall see.

9.2 Degree g

Beyond $g = 2$, the connection between modular forms and Galois representations descends into pure conjecture. We would like to see how to associate a Galois representation to a modular form. To define the representation, we have seen that it is sufficient to determine the image $\rho_f(\mathrm{Frob}_\ell)$ for each prime $\ell \nmid pN$. So we should be able to produce an image (up to conjugacy), when provided with a prime ℓ and a Siegel modular form f. Here we consider the isomorphism discussed in chapter 8. There we had proposition 8.8

which associated to a Siegel modular form f (mod p) and a local Hecke algebra $\mathcal{H}_\ell$ (determined by a choice of prime ℓ) a semisimple conjugacy class in $\mathrm{GSpin}_{2g+1}(\overline{\mathbb{F}}_p)$. This leads us to the following conjecture for general g.

Conjecture 9.2. *Let $\Gamma \subseteq \mathrm{Sp}_{2g}(\mathbb{Z})$ be a congruence subgroup of level N, and let $f \in M_\kappa(\Gamma; \overline{\mathbb{F}}_p)$ be a Siegel modular form of weight κ. Suppose that f is a Hecke eigenform for each local Hecke algebra $\mathcal{H}_\ell$ such that $\ell \nmid pN$. Then there exists a representation*

$$\begin{array}{rccc} \rho_f: & \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) & \longrightarrow & \mathrm{GSpin}_{2g+1}(\overline{\mathbb{F}}_p) \\ & \mathrm{Frob}_\ell & \longmapsto & s_{f,\ell} \end{array} \tag{9.2}$$

which is unramified away from pN, where $s_{f,\ell}$ is the Satake parameter of f at ℓ.

Remark 9.3. In terms of calculation, we will regularly pass to representations of GSpin_{2g+1}, since that is the way one defines Satake parameters. Though in the end our final result will not be dependent on a choice representation.

One may wonder that the above conjecture does not seem to capture the known cases, in which the representation has image in GL_2 and GSp_4, respectively. In fact, in the cases $g = 1$ and $g = 2$ we have that

$$\mathrm{GSpin}_5 \cong \mathrm{GSp}_4 \qquad\qquad \mathrm{GSpin}_3 \cong \mathrm{GSp}_2 \cong \mathrm{GL}_2\,.$$

The above isomorphisms are known as "accidental isomorphisms", and can be interpreted as a peculiarity amongst root data for small g. This allows the above conjecture to indeed align with the known cases for $g = 1$ and $g = 2$.

Some motivation for this definition can be found in the comparison to the case of algebraic modular forms, studied by Gross in [Gro98a]. Further, one can think of a general Langlands-type philosophy, which suggests an association between automorphic objects on G and Galois representations into $\hat{G}$. The Satake isomorphism is a large part of this, tying these two groups together very directly. Thus leading us to the conjecture above.

Example 9.4. Let us now consider the case $g = 1$ explicitly and see how it compares to Theorem 7.16. In general, if one wanted to make comments regarding characteristic polynomials, this is difficult since GSpin is not generally a matrix group. In the cases $g = 1, 2$, we have by the above remark that GSpin_{2g+1} is in fact a matrix group, and thus we can take V to be the standard representation. However, there is reason to consider other representations, as these correspond to other interesting data attached to a modular form. So even in the $g = 1$ and $g = 2$ cases, one may be interested in the full generality of the result.

We will follow [Gro98b], from which get that the characteristic polynomial of the Frobenius element is

$$\operatorname{charpoly}(\rho(\mathrm{Frob}_\ell)) = \det(X - s_\ell|V) = \sum_{k=0}^{g}(-1)^k \ell^{k(k-1)/2} \cdot \alpha_k \cdot X^{g-k} \tag{9.3}$$

where α_i is the eigenvalue of the element $T_{\lambda_i(\ell)} = \mathrm{GSp}_{2g}(\mathbb{Z}_\ell)\lambda_i(\ell)\,\mathrm{GSp}_{2g}(\mathbb{Z}_\ell)$, where

$$\lambda_i(\ell) = \begin{pmatrix} \ell I_i & \\ & I_{g-i} \end{pmatrix}, \tag{9.4}$$

with I_n being the $n \times n$ identity matrix.

For the case of GL_2, we have $\mathcal{H}_\ell = \mathcal{H}(\mathrm{GL}_2(\mathbb{Q}_\ell), \mathrm{GL}_2(\mathbb{Z}_\ell))$. Thus we have

$$\operatorname{charpoly}(\rho(\mathrm{Frob}_\ell)) = \det(X - s_\ell|V) = X^2 - \alpha_1 X + \ell\alpha_2, \tag{9.5}$$

In the case $i = 1$, we have $T_{\lambda_1(\ell)} = T_\ell$, with eigenvalue $\alpha_1 = \lambda(\ell)$. Now consider the effect of the operator defined by $i = 2$, i.e.

$$T_{\lambda_2(\ell)} = \mathrm{GL}_2(\mathbb{Z}_\ell)\begin{pmatrix} \ell & 0 \\ 0 & \ell \end{pmatrix}\mathrm{GL}_2(\mathbb{Z}_\ell) = \mathrm{GL}_2(\mathbb{Z}_\ell)\begin{pmatrix} \ell & 0 \\ 0 & \ell \end{pmatrix} \tag{9.6}$$

Then

$$\begin{aligned} f\left|\mathrm{GL}_2(\mathbb{Z}_\ell)\begin{pmatrix} \ell & 0 \\ 0 & \ell \end{pmatrix}\mathrm{GL}_2(\mathbb{Z}_\ell)\right. &= f\left|\begin{pmatrix} \ell & 0 \\ 0 & \ell \end{pmatrix}\right. \\ &= \det\left(\begin{pmatrix} \ell & 0 \\ 0 & \ell \end{pmatrix}\right)^{k-1} (0z+\ell)^{-k} f\left(\frac{\ell z + 0}{0z + \ell}\right) \\ &= \ell^{2k-2}\ell^{-k} f(\ell z/\ell) = \ell^{k-2} f(z), \end{aligned}$$

which thus can be seen to have eigenvalue $\alpha_2 = \ell^{k-2}$. Thus we have that

$$\begin{aligned}\operatorname{charpoly}(\rho(\mathrm{Frob}_\ell)) = \det(X - s_\ell|V) = X^2 - \alpha_1 X + q\alpha_2 &= X^2 - \lambda(\ell)X + \ell\cdot\ell^{k-2}\\ &= X^2 - \lambda(\ell)X + \ell^{k-1},\end{aligned}$$

which is precisely the formula defining ρ in the classical case.

9.3 Theta Operator and Cyclotomic Character

In chapter 7, we saw that the theta operator on modular forms was related to the cyclotomic character. This was a useful tool for many proofs relating to Galois representations attached to modular forms.

We wish to relate the various theta operators on Siegel modular forms to the cyclotomic character. Since the representation is defined in terms of the Satake parameters, which are data attached to the Hecke eigenvalues, we would like to understand the effect of the theta operator on these eigenvalues. In chapter 6, we saw two theta operators on Siegel modular forms, θ_{BN} and θ_{FG}. These both had commutation relations with the Hecke operators, which lead to the following results on eigenvalues.

Theorem 9.5. *Let f be a Hecke eigenform for $\mathcal{H}_\ell$. Let $K = \mathrm{GSp}_{2g}(\mathbb{Z}_\ell)$.*

(1) If $\theta_{BN}f \neq 0$, then $\theta_{BN}f$ is a Hecke eigenform $\mathcal{H}_\ell$. Further, the eigensystem of $\theta_{BN}f$ satisfies

$$\Psi_{\theta_{BN}f}(T_{\lambda(\ell)}) = \det(\lambda(\ell))\Psi_f(T_{\lambda(\ell)}), \tag{9.7}$$

where λ is a dominant coweight.

(2) If $\theta_{FG}f \neq 0$, then $\theta_{FG}f$ is a Hecke eigenform $\mathcal{H}_\ell$. Further, the eigensystem of $\theta_{FG}f$ satisfies

$$\Psi_{\theta_{FG}f}(T_{\lambda(\ell)}) = \eta(\lambda(\ell))\Psi_f(T_{\lambda(\ell)}), \tag{9.8}$$

where λ is a dominant coweight.

Proof. (1) This follows from Theorem 6.22.

(2) This follows from Theorem 6.24.

□

Remark 9.6. Going with our earlier notation, note that

$$\det(\lambda(\ell)) = \ell^{\langle \det, \lambda \rangle}$$
$$\eta(\lambda(\ell)) = \ell^{\langle \eta, \lambda \rangle}.$$

Further recall that $\det = \eta^g$, so both the results above can be stated in terms of powers of η. We can therefore focus on results on η, and results on det will follow from repeatedly applying the below g times.

Now, how to relate this to our Galois representations? Well in fact, the results we have gathered thus far around Satake parameters allow us to say something more, which will then allow us to discuss the effects of θ_{BN} and θ_{FG}. We now state a first result which depends on a choice of algebraic representation ω_λ.

Theorem 9.7. *Let λ be a dominant coweight of GSp_{2g}. Let $\omega_\lambda : \mathrm{GSpin}_{2g+1}(\overline{\mathbb{F}}_p) \to \mathrm{GL}(V)$ be the representation with highest weight λ. Let $f \in M_\kappa(\Gamma; \mathbb{F}_p)$ be a degree g, weight κ level N Siegel eigenform. Then*

$$\omega_\lambda \circ \rho_{\theta_{FG} f} = \chi^{\langle \eta, \lambda \rangle} \otimes (\omega_\lambda \circ \rho_f), \tag{9.9}$$

where χ is the cyclotomic character (mod p).

Proof. Let $\ell \nmid p$ be a prime. Then we have

$$\begin{aligned}
(\omega_\lambda \circ \rho_{\theta_{FG} f})(\mathrm{Frob}_\ell) &= \omega_\lambda(s_{\vartheta f, \ell}) \\
&= \left(\Psi_{\theta_{FG} f} \circ \mathcal{S}_{p,\ell}^{-1}\right)(\omega_\lambda) \\
&= \left(\Psi_{\theta_{FG} f} \circ \mathcal{S}_{p,\ell}^{-1}\right)\left(\sum_{\mu \le \lambda} d_\lambda(\mu) \mathcal{S}_{p,\ell}(T_{\mu(\ell)})\right) \qquad (9.10) \\
&= \sum_{\mu \le \lambda} d_\lambda(\mu) \Psi_{\theta_{FG} f}(T_{\mu(\ell)})
\end{aligned}$$

$$
\begin{aligned}
&= \sum_{\mu \le \lambda} d_\lambda(\mu)\eta(\mu(\ell))\Psi_{f,\ell}(T_{\mu(\ell)}) \\
&= \sum_{\mu \le \lambda} d_\lambda(\mu)\eta(\lambda(\ell))\Psi_{f,\ell}(T_{\mu(\ell)}) \qquad (9.11) \\
&= \eta(\lambda(\ell)) \sum_{\mu \le \lambda} d_\lambda(\mu)\Psi_{f,\ell}(T_{\mu(\ell)}) \\
&= \ell^{\langle \eta, \lambda \rangle} \sum_{\mu \le \lambda} d_\lambda(\mu)\Psi_{f,\ell}(T_{\mu(\ell)}) \\
&= \ell^{\langle \eta, \lambda \rangle} \omega_\lambda(s_{f,\ell}) \\
&= \ell^{\langle \eta, \lambda \rangle} (\omega_\lambda \circ \rho_f)(\mathrm{Frob}_\ell),
\end{aligned}
$$

where (9.10) follows from Proposition 8.3 and (9.11) follows from Corollary 4.16. Thus the image of Frob_ℓ has been multiplied by $\ell^{\langle \eta, \lambda \rangle}$. Thus

$$\omega_\lambda \circ \rho_{\theta_{FG} f} = \chi^{\langle \eta, \lambda \rangle} \otimes (\omega_\lambda \circ \rho_f), \qquad (9.12)$$

as required. □

This leads to the main result.

Theorem 9.8. *Let $\eta^\vee$ be the cocharacter of GSpin_{2g+1} corresponding to η by duality. Let f and χ be as above. Then*

$$\rho_{\theta_{FG} f} = (\eta^\vee \circ \chi) \otimes \rho_f. \qquad (9.13)$$

Proof. First note that for each ω_λ corresponding to a dominant coweight λ we have

$$
\begin{aligned}
\omega_\lambda \circ ((\eta^\vee \circ \chi) \otimes \rho_f) &= (\omega_\lambda \circ \eta^\vee)(\chi) \otimes (\omega_\lambda \circ \rho_f) \\
&= \chi^{\langle \eta, \lambda \rangle} \otimes (\omega_\lambda \circ \rho_f).
\end{aligned}
$$

Now, by the previous theorem, for each ω_λ corresponding to a dominant coweight λ we have

$$\omega_\lambda \circ \rho_{\theta_{FG} f} = \chi^{\langle \eta, \lambda \rangle} \otimes (\omega_\lambda \circ \rho_f). \qquad (9.14)$$

However, recalling Lemma 8.5, we know that the Satake parameters (that is, the image of ρ_f and $\rho_{\theta_{FG}f}$ are defined by their images under the representations ω_λ. Thus the above two equalities tell us

$$\omega_\lambda \circ \rho_{\theta_{FG}f} = \omega_\lambda \circ ((\eta^\vee \circ \chi) \otimes \rho_f) \tag{9.15}$$

and thus

$$\rho_{\theta_{FG}f} = (\eta^\vee \circ \chi) \otimes \rho_f, \tag{9.16}$$

as required. □

As for θ_{BN}, we can now say the following.

Corollary 9.9. *Let $\eta^\vee$ and $\det^\vee$ be the cocharacters of GSpin_{2g+1} corresponding to η and $\det$ by duality. Let f and χ be as above. Then*

$$\rho_{\theta_{BN}f} = (\eta^\vee \circ \chi)^g \otimes \rho_f = (\det{}^\vee \circ \chi) \otimes \rho_f. \tag{9.17}$$

Proof. Since $\det = \eta^g$, simply apply theorem 9.8 g times. □

Bibliography

[And86] Anatolij N Andrianov. *Quadratic forms and Hecke operators.* Springer-Verlag New York, Inc., 1986.

[AS01] Mahdi Asgari and Ralf Schmidt. Siegel modular forms and representations. *manuscripta mathematica*, 104(2):173–200, 2001.

[BN07] Siegfried Boecherer and Shoyu Nagaoka. On mod p properties of Siegel modular forms. *Mathematische Annalen*, 338(2):421–433, 2007.

[BN13] Siegfried Boecherer and Shoyu Nagaoka. On p-adic properties of Siegel modular forms. *arXiv preprint arXiv:1305.0604*, 2013.

[Car79] Pierre Cartier. Representations of p-adic groups: a survey. In *Automorphic forms, representations and L-functions (Proc. Sympos. Pure Math., Oregon State Univ., Corvallis, Ore., 1977), Part*, volume 1, pages 111–155, 1979.

[CCR11] Dohoon Choi, Youngju Choie, and Olav K Richter. Congruences for Siegel modular forms. *Ann. Inst. Fourier (Grenoble)*, 61(4):1455–1466, 2011.

[CG13] Craig Citro and Alexandru Ghitza. Computing level one Hecke eigensystems (mod p). *LMS Journal of Computation and Mathematics*, 16:246–270, 2013.

[Con14] Brian Conrad. Reductive group schemes. In *Autour des schémas en groupes. Vol. I*, volume 42/43 of *Panor. Synthèses*, pages 93–444. Soc. Math. France, Paris, 2014.

[Del71] Pierre Deligne. Formes modulaires et representations ℓ-adiques. In *Séminaire Bourbaki vol. 1968/69 Exposés 347-363*, pages 139–172. Springer, 1971.

[DR10] Michael Dewar and Olav K Richter. Ramanujan congruences for Siegel modular forms. *International Journal of Number Theory*, 6(07):1677–1687, 2010.

[DS05] Fred Diamond and Jerry Michael Shurman. *A first course in modular forms*, volume 228. Springer, 2005.

[Edi92] Bas Edixhoven. The weight in Serre's conjectures on modular forms. *Inventiones mathematicae*, 109(1):563–594, 1992.

[EI98] Wolfgang Eholzer and Tomoyoshi Ibukiyama. Rankin-Cohen type differential operators for Siegel modular forms. *International Journal of Mathematics*, 9(04):443–463, 1998.

[Fla13] Max Flander. *A theta operator for Siegel modular forms (mod p)*. PhD thesis, The University of Melbourne, 2013.

[Fre07] Edward Frenkel. Lectures on the Langlands program and conformal field theory. In *Frontiers in number theory, physics, and geometry II*, pages 387–533. Springer, 2007.

[G$^+$90] Benedict H Gross et al. A tameness criterion for Galois representations associated to modular forms (mod p). *Duke Mathematical Journal*, 61(2):445–517, 1990.

[Ghi03] Alexandru Ghitza. Siegel modular forms (mod p) and algebraic modular forms. *arXiv preprint math/0306224*, 2003.

[Gro98a] Benedict H Gross. Modular forms (mod p) and Galois representations. *International Mathematics Research Notices*, 1998(16):865–875, 1998.

[Gro98b] Benedict H Gross. On the Satake isomorphism. *Galois representations in arithmetic algebraic geometry*, 254:223, 1998.

[Gro99] Benedict H Gross. Algebraic modular forms. *Israel Journal of Mathematics*, 113(1):61–93, 1999.

[H$^+$09] Florian Herzig et al. The weight in a Serre-type conjecture for tame n-dimensional Galois representations. *Duke Mathematical Journal*, 149(1):37–116, 2009.

[Har77] Robin Hartshorne. *Algebraic geometry*, volume 52. Springer Science & Business Media, 1977.

[HW02a] J Hafner and L Walling. Siegel modular forms and Hecke operators in degree 2. In *Millennial Conference on Number Theory, AK Peters*, 2002.

[HW02b] James Lee Hafner and Lynne H Walling. Explicit action of Hecke operators on Siegel modular forms. *Journal of Number Theory*, 93(1):34–57, 2002.

[Jan07] Jens Carsten Jantzen. *Representations of algebraic groups*, volume 107. American Mathematical Soc., 2007.

[Joc82] Naomi Jochnowitz. A study of the local components of the Hecke algebra mod p. *Transactions of the American Mathematical Society*, 270(1):253–267, 1982.

[Kat73] Nicholas M Katz. p-adic properties of modular schemes and modular forms. In *Modular functions of one variable III*, pages 69–190. Springer, 1973.

[Kat77] Nicholas M Katz. A result on modular forms in characteristic p. In *Modular Functions of one Variable V*, pages 53–61. Springer, 1977.

[KM85] Nicholas M Katz and Barry Mazur. *Arithmetic moduli of elliptic curves*. Princeton University Press, 1985.

[KW10] Chandrashekhar Khare and Jean-Pierre Wintenberger. Serre's modularity conjecture. In *Proceedings of the International Congress of Mathematicians. Volume II*, pages 280–293. Hindustan Book Agency, New Delhi, 2010.

[Lan01] Joshua M Lansky. Decomposition of double cosets in p-adic groups. *Pacific Journal of Mathematics*, 197(1):97–117, 2001.

[Lau97] Gérard Laumon. Sur la cohomologie à supports compacts des variétés de Shimura pour $\mathrm{GSp}(4)_{\mathbb{Q}}$. *Compositio Mathematica*, 105(3):267–359, 1997.

[Mil98] James S Milne. Algebraic number theory. *Lecture Notes in Math*, 676, 1998.

[Mil03] James S Milne. Fields and galois theory. *Courses Notes, Version*, 4, 2003.

[Mil12] James S Milne. Reductive groups. *Courses Notes, Version*, 1, 2012.

[Miy06] Toshitsune Miyake. *Modular forms*. Springer Science & Business Media, 2006.

[Rib95] Kenneth A Ribet. Galois representations and modular forms. *Bulletin of the American Mathematical Society*, 32(4):375–402, 1995.

[Ric08] Olav Richter. On congruences of Jacobi forms. *Proceedings of the American Mathematical Society*, 136(8):2729–2734, 2008.

[Ric09] Olav Richter. The action of the heat operator on Jacobi forms. *Proceedings of the American Mathematical Society*, 137(3):869–875, 2009.

[RR14] M Raum and O Richter. The structure of Siegel modular forms (mod p) and $U(p)$ congruences. *Mathematical Research Letters*, 2014.

[RS99] Kenneth A Ribet and William A Stein. Lectures on Serre's conjectures. *Arithmetic algebraic geometry (Park City, UT, 1999)*, 9:143–232, 1999.

[RS08] Nathan C Ryan and Thomas R Shemanske. Inverting the Satake map for Sp_n and applications to Hecke operators. *The Ramanujan Journal*, 17(2):219–244, 2008.

[S+87] Jean-Pierre Serre et al. Sur les représentations modulaires de degré 2 de $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$. *Duke Mathematical Journal*, 54(1):179–230, 1987.

[SD73] Henry Peter Francis Swinnerton-Dyer. On ℓ-adic representations and congruences for coefficients of modular forms. In *Modular functions of one variable III*, pages 1–55. Springer, 1973.

[SD77] H Peter F Swinnerton-Dyer. On ℓ-adic representations and congruences for coefficients of modular forms (ii). In *Modular functions of one variable V*, pages 63–90. Springer, 1977.

[Ser68] Jean-Pierre Serre. Groupe de Grothendieck des schémas en groupes réductifs déployés. *Publications Mathématiques de l'IHÉS*, 34:37–52, 1968.

[Ser73] Jean-Pierre Serre. Congruences et formes modulaires. In *Séminaire Bourbaki vol. 1971/72 Exposés 400–417*, pages 319–338. Springer, 1973.

[Sil09] Joseph H Silverman. *The arithmetic of elliptic curves*. Springer-Verlag New York, 2009.

[Sko92] Nils-Peter Skoruppa. Computations of Siegel modular forms of genus two. *Mathematics of Computation*, 58(197):381–398, 1992.

[Str13] Benoît Stroh. Classicité en théorie de Hida. *American Journal of Mathematics*, 135(4):861–889, 2013.

[T$^+$91] Richard Taylor et al. Galois representations associated to Siegel modular forms of low weight. *Duke Mathematical Journal*, 63(2):281–332, 1991.

[vdG06] Gerard van der Geer. Siegel modular forms. In *The 1-2-3 of Modular Forms*. Springer, 2006. arXiv:math/0605346.

[Wei05] Rainer Weissauer. Four dimensional Galois representations. *Astérisque*, 302:67–150, 2005.

[Yam14] Takuya Yamauchi. The weight in Serre's conjecture for GSp_4. *arXiv preprint arXiv:1410.7894*, 2014.

[Zag08] Don Zagier. Elliptic modular forms and their applications. In *The 1-2-3 of modular forms*, pages 1–103. Springer, 2008.