

Galois representations associated to
some simple Shimura varieties

Dhruva Rasesh Kelkar

A Thesis
in
The Department
of
Mathematics and Statistics

Presented in Partial Fulfillment of the Requirements
for the degree of
Master of Science
Mathematics (With Thesis)
at
Concordia University
Montreal, Quebec, Canada

August 2021

© Dhruva Kelkar, 2021

CONCORDIA UNIVERSITY
School of Graduate Studies

This is to certify that the thesis prepared

By: Mr. Dhruva Rasesh Kelkar

Entitled: Galois representations associated to some simple Shimura varieties

and submitted in partial fulfillment of the requirements for the degree of

Master of Science

complies with the regulations of the University and meets the accepted standards with respect to originality and quality.

Signed by the final examining committee:

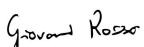


Dr. Chantal David Chair




Dr. Hershy Kisilevsky Examiner


Examiner



Dr. Giovanni Rosso Thesis Supervisor(s)



Dr. Adrian Iovita Thesis Supervisor(s)


with permission

Approved by _____
Dr. Galia Dafni Chair of Department or Graduate Program Director

Dean

ABSTRACT

Galois representations associated to
some simple Shimura varieties

Dhruva Kelkar

The aim of this thesis is to present the paper [1] of Kottwitz with the same title. The first 4 chapters are a rapid review of the prerequisites and the main result of the paper is presented in chapter 5 and some ideas of the proof are given in chapter 6.

The objective of the paper [1] is to construct Galois representations associated to cohomological automorphic representations i.e. automorphic representations occurring in the cohomology of a certain Shimura variety. The difficult part lies in proving that this association matches up the local Satake parameter of the automorphic representations with the local Frobenius conjugacy class of the Galois representation at places of good reduction.

We try to present the material with as much detail as possible, except at some places we either restrict ourselves to providing references for further details or work instead with the case of GL_2 , where the associated Shimura varieties (modular curves) have a much simpler moduli interpretation.

ACKNOWLEDGEMENTS

I would like to thank my advisors Giovanni Rosso and Adrian Iovita for their guidance throughout my year in Concordia. In addition to answering my questions every week, Prof. Rosso's mentorship and constant support helped me overcome several difficulties. I enjoyed the discussions with Prof. Iovita, unfortunately not many because of his sabbatical, and his unique style of explaining things.

I had very interesting courses and seminars with Vytautas Paskunas, Jan Kohlhaase, Marc Levine and Daniel Greb during my first year in Essen which gave me a good foundation to start working on this thesis. Their help in finding a PhD position in Amsterdam was invaluable.

I would also like to thank my (future) PhD supervisor Arno Kret for suggesting this topic for the masters thesis and also for inviting me to Amsterdam on several occasions for discussions regarding this thesis. His in-depth explanation helped me greatly to gain clarity regarding the topic.

The ALGANT coordinators, particularly Vytautas Paskunas and Giovanni Rosso, provided lot of assistance to deal with several bureaucratic issues arising as a result of the pandemic, which helped me to be focused on my work despite several disruptions.

Finally, I would like to thank my family for their encouragement in pursuing this program and my friends for their company.

Contents

1	Linear Algebraic Groups	1
1.1	Algebraic Groups	1
1.2	Reductive groups	3
1.3	Derived subgroup and solvable groups	3
1.4	Maximal tori and Borel subgroups	4
1.5	Lie algebra of a Lie group	5
1.6	Hyperspecial subgroups and models	5
2	Shimura Varieties	7
2.1	Hermitian symmetric domains	7
2.2	Automorphisms of Hermitian symmetric domain	9
2.3	The homomorphism u_p	9
2.4	Shimura Datum	10
3	Representations of td groups	12
3.1	Hecke algebras	13
3.2	Smooth representations	13
3.3	Admissible representations	14
3.4	Unramified Hecke algebra	15
4	Automorphic Representations	16
4.1	Motivation for automorphic forms	16
4.2	Automorphic forms	17
5	Main Theorem	19
5.1	A particular algebraic group	19
5.2	A particular Shimura datum	20
5.3	Local systems on $S_K(\mathbb{C})$	21
5.4	Hecke correspondences	22
5.5	Construction of the Galois representation	22
5.6	Places of good reduction	23
5.7	Satake isomorphism	24
5.8	Statement of the main theorem	24

6 Proof of Main Theorem	26
6.1 Outline of the proof	26
6.2 Modular curves as moduli spaces	28
6.3 Tate module and Dieudonne module	29
6.4 Point counting	30
Bibliography	33

Chapter 1

Linear Algebraic Groups

This chapter is meant to be a collection of facts about algebraic groups which we will need and not meant to be an introduction to the theory of algebraic groups in itself. The treatment of this subject is kept as brief as possible for this thesis.

1.1 Algebraic Groups

The chapter on algebraic groups in [2] gives a rapid introduction to the subject with a view towards the theory of automorphic representations, which will be our primary concern. The books [3] and [4] provide a more detailed treatment of the topic addressing the more subtle aspects.

In this chapter, let k denote a commutative Noetherian ring with identity, unless specified otherwise.

Definition 1 (Affine group schemes). An affine group scheme G over k is a functor

$$G : k\text{-alg} \rightarrow \mathbf{Grp}$$

that is representable by a finite type k -alg i.e. a finite type k -algebra A such that $G(R) = \mathrm{Hom}_k(A, R)$. For a k -alg R , the group $G(R)$ is also referred to as the R -points of the group scheme G .

If A is the k -alg representing the functor G , by abuse of notation we will also use G to denote $\mathrm{Spec}(A)$. We say that the affine group schemes G is smooth (resp. connected) if the corresponding scheme $\mathrm{Spec}(A)$ is smooth (resp. connected). In the case when k is a field and G is smooth, G is called an affine algebraic group. We will often refer to an affine algebraic group also as just an algebraic group, omitting the word affine.

A morphism of affine group schemes $H \rightarrow G$ is a natural transformation of functors and, by Yoneda's lemma, thus induces a map $H \rightarrow G$ of affine schemes.

Moreover we define H to be a subgroup scheme of G if there is a morphism $H \rightarrow G$ such that $H(R)$ is a subgroup of $G(R)$ for all k -algebras R . We also remark that if k is a field then the affine group subschemes are also closed.

We say an affine group scheme H is a *normal subgroup* of G if $H(R)$ is a normal subgroup of $G(R)$ for every k -algebra R .

If $H \xrightarrow{g} G$ is a map of affine group schemes, we define $\ker(f)$ to be the affine group scheme whose R points are given by $\ker(H(R) \rightarrow G(R))$.

Example 1 (Multiplicative group \mathbf{G}_m). The multiplicative group \mathbf{G}_m is a functor assigning to each k -alg R its multiplicative group R^\times . It is represented by $k[x, y]/(xy - 1)$.

Example 2. Let V be a rank n , free k -module. For a k -algebra R , we define the functor $\mathrm{GL}_V(R) := \{R\text{-module automorphisms } V \otimes_k R \rightarrow V \otimes_k R\}$. This functor is representable by $(k[x_{ij}]_{1 \leq i, j \leq n})[y]/(\det(x_{ij}) \cdot y - 1)$.

Definition 2 (Representations of affine group schemes). A representation of an affine group scheme G over k is a morphism of affine groups schemes $r : G \rightarrow \mathrm{GL}_V$ for some V (a finite, free module over k). A representation is *faithful* if r is a closed embedding.

Definition 3. An affine group scheme G is said to be linear if it is smooth and admits a faithful representation $G \rightarrow \mathrm{GL}_V$, for some V .

It is a theorem that all affine algebraic groups are linear. We let LAG_k denote the category of linear algebraic groups over k .

Let k'/k be an extension of rings. If G is an affine group scheme over k , then we define the *extension of scalars* $G_{k'}$ by the functor:

$$G_{k'} : k'\text{-alg} \rightarrow \mathrm{Grp}$$

$$A \mapsto G(A).$$

If the representing object for G is given by the k -alg A then the representing object for $G_{k'}$ is given by the k' -alg $A \otimes_k k'$.

If G is an affine group scheme over k' then we define the *restriction of scalars* $\mathrm{Res}_k^{k'} G$ by the functor:

$$\mathrm{Res}_k^{k'} G : k\text{-alg} \rightarrow \mathrm{Grp}$$

$$A \mapsto G(A \otimes_k k').$$

To show that this functor is representable, one needs additional hypothesis on the extension k'/k . For example, assuming that k'/k is a finite extension of fields suffices.

1.2 Reductive groups

Definition 4. Let k be a perfect field. An element $x \in M_n(\bar{k})$ is said to be *semisimple* if there exists $g \in \mathrm{GL}_n(\bar{k})$ such that $g^{-1}xg$ is diagonal, *nilpotent* if there exists a positive integer n such that $x^n = 0$ and *unipotent* if $(x - I)$ is nilpotent. For an arbitrary linear group G , we say that $x \in G(\bar{k})$ is unipotent if $r(x)$ is so for some faithful representation $r : G \rightarrow \mathrm{GL}_V$.

It turns out that the above properties of being semisimple or unipotent do not depend on the choice of the faithful representation r . These properties are also functorial, in the sense that if $f : H \rightarrow G$ is a morphism of algebraic groups and $x \in H(\bar{k})$ is semisimple (resp. unipotent), then $f(x) \in G(\bar{k})$ is also semisimple (resp. unipotent).

Theorem 1 (Jordan Decomposition). Let G be an algebraic group over a perfect field k . Given $x \in G(k)$, there exists unique $x_s, x_u \in G(k)$ such that x_s is semisimple, x_u is unipotent and $x = x_s x_u = x_u x_s$.

The Jordan decomposition is also functorial in the sense that, if $f : H \rightarrow G$ is a morphism of algebraic groups with $x \in H(\bar{k})$ then $f(x_s) = f(x)_s$ and $f(x_u) = f(x)_u$.

With this theorem in mind, we can make the following definition:

Definition 5 (Unipotent group). A smooth algebraic group G over a perfect field k is said to be unipotent, if every $x \in G(\bar{k})$ is unipotent i.e. $x = x_u$.

Definition 6. Let G be a smooth algebraic group. The *unipotent radical* $\mathcal{R}_u(G)$ is the maximal connected unipotent normal subgroup of G .

Further details regarding the existence of a maximal connected unipotent normal subgroup are explained on Pg. 10 of [3].

Now we arrive at the most important definition of this subsection.

Definition 7 (Reductive algebraic group). A smooth connected algebraic group G is said to be reductive if $\mathcal{R}_u(G) = \{1\}$.

1.3 Derived subgroup and solvable groups

In this section we let k denote a perfect field.

Definition 8. Let G be an algebraic group over k . The *derived subgroup* of G , denoted by G^{der} or $\mathcal{D}G$, is defined as the intersection of all normal subgroups $N \subset G$ such that G/N is commutative.

Note that, we have not yet discussed the notion of a quotient of two algebraic groups, which we take as a black box for the above definition. We can also inductively define $\mathcal{D}^n G := \mathcal{D}(\mathcal{D}^{n-1}G)$.

Definition 9 (Solvable groups). A group G over k is said to be solvable if $\mathcal{D}^n G$ is the trivial group for sufficiently large n .

1.4 Maximal tori and Borel subgroups

In this section, we use k to denote a perfect field.

Definition 10 (Torus). A *torus* is a linear algebraic group T over k such that $T_{\bar{k}} \simeq \mathbb{G}_m^n$ for some n . The integer n is known as the rank of the torus.

Next, we want to explain the notion of a split algebraic group. But first, we need to make some more definitions.

Definition 11. A torus T over a field k is said to be split if $T \simeq \mathbb{G}_m^n$ (here the isomorphism is over k).

Definition 12 (Maximal torus). Let G be an algebraic group over k . A torus $T \subset G$ is said to be a maximal torus of G if $T_{\bar{k}}$ is maximal among all tori of $G_{\bar{k}}$.

Finally we state the following fundamental theorem regarding existence of maximal tori:

Theorem 2. Every connected algebraic group admits a maximal torus. All maximal tori in $G_{\bar{k}}$ are conjugate under $G(\bar{k})$.

Finally, we come to the definition of a split group:

Definition 13. An algebraic group G over k is said to be split if there exists a maximal torus of G that is split.

Analogously, the group G over k is said to be split over an extension k' if the group $G_{k'}$ is split.

Next, we come to the definition of parabolic subgroups:

Definition 14. A closed subgroup $B \subset G$ is a *Borel subgroup* if $B_{\bar{k}}$ is a maximal smooth connected solvable subgroup of $G_{\bar{k}}$. A smooth subgroup $P \subset G$ is said to be a *parabolic subgroup* if $P_{\bar{k}}$ contains a Borel subgroup of $G_{\bar{k}}$.

Unlike maximal tori, Borel subgroups may not exist in a general reductive algebraic group G . Hence, we make the following definition:

Definition 15. A reductive group G is *quasi-split* if it contains a Borel subgroup.

We remark here that the notion of being quasi-split is weaker than the notion of being split i.e. quasi-split groups are also split.

1.5 Lie algebra of a Lie group

Definition 16 (Lie algebra). Let k be a ring. A Lie algebra over k is a free k -module \mathfrak{g} together with a bilinear pairing (called the Lie bracket)

$$[\cdot, \cdot] : \mathfrak{g} \times \mathfrak{g} \rightarrow \mathfrak{g}$$

satisfying the following assumptions:

1. $[X, X] = 0$ for all $X \in \mathfrak{g}$.
2. For $X, Y, Z \in \mathfrak{g}$, $[[X, Y], Z] + [[Y, Z], X] + [[Z, X], Y] = 0$.

Morphisms of Lie algebras are k -module maps preserving $[\cdot, \cdot]$. We let \mathbf{LieAlg}_k denote the category of Lie algebras over k .

The "tangent space" at identity element of a linear algebraic group (\mathbf{LAG}_k) has the natural structure of a Lie algebra. This is the content of the following theorem:

Theorem 3. Let k be a field. There exists a functor $\mathbf{Lie} : \mathbf{LAG}_k \xrightarrow{t \mapsto 0} \mathbf{LieAlg}_k$ defined by:

$$\mathbf{Lie} G = \ker(G(k[t]/(t^2)) \rightarrow G(k)).$$

Note that the theorem doesn't specify the Lie bracket structure on $\mathbf{Lie} G$ and we will omit this.

Let G be an algebraic group over k . We will now describe a representation of G , known as the adjoint representation.

Let R be a k -algebra. Define

$$\mathfrak{g}(R) := \ker(G(R[t]/(t^2)) \xrightarrow{t \mapsto 0} G(R)).$$

Hence, $\mathfrak{g}(k) = \mathbf{Lie} G$. Note that the group $G(R[t]/(t^2))$ acts on $\mathfrak{g}(R)$ by conjugation. As $G(R)$ is a subgroup of $G(R[t]/(t^2))$, it also acts on $\mathfrak{g}(R)$ and thus we have a map:

$$G(R) \rightarrow \mathrm{Aut}(\mathfrak{g}(R)).$$

This map is functorial in R and hence defines a representation $\mathrm{Ad} : G \rightarrow \mathrm{GL}_{\mathfrak{g}}$, which is the adjoint representation.

1.6 Hyperspecial subgroups and models

In this section, we want to restrict our attention to algebraic groups G over a p -adic field F . We want to highlight certain aspects of this particular type of algebraic groups.

We want to explore the possibility of the group G arising as a restriction of an algebraic group defined over \mathcal{O} , where \mathcal{O} denotes the ring of integers in F . Hence, we first start with the following definition.

Definition 17. Let Y be an affine scheme over F . A *model* \mathcal{Y} of Y over \mathcal{O} is an affine scheme, say $\text{Spec}(A)$, of finite type over \mathcal{O} , such that $Y \simeq \text{Spec}(A \otimes_{\mathcal{O}} F)$.

If \mathcal{Y} is a scheme over \mathcal{O} , then we call $\mathcal{Y} \times_{\text{Spec}(\mathcal{O})} \text{Spec}(F)$ as the *generic fibre* and $\mathcal{Y} \times_{\text{Spec}(\mathcal{O})} \text{Spec}(\mathcal{O}/m)$ as the *special fibre*, where m denotes the maximal ideal of \mathcal{O} (recall that \mathcal{O} is a DVR). Hence, according to this terminology, in Definition 17, Y is the generic fibre of \mathcal{Y} .

Next we have the notion of a group G over a p-adic field F being unramified:

Definition 18 (Unramified group). The reductive group G over F is called *unramified* if there exists a model \mathcal{G} of G over \mathcal{O} such that the special fibre of \mathcal{G} is reductive.

The nice thing about being unramified is the existence of a canonical maximal compact subgroup, which is as follows:

Definition 19 (Hyperspecial subgroup). Let the reductive group G over the p-adic field F be unramified. Let \mathcal{G} be a model of G over \mathcal{O} . Then the subgroup $\mathcal{G}(\mathcal{O}) \subset G(F)$ is a maximal compact subgroup of $G(F)$ and is called a *hyperspecial subgroup*.

We also remark that we have the following theorem, which is sometimes also taken as the definition of an unramified group:

Theorem 4. A reductive group G over a p-adic field F is unramified if and only if it is quasi-split and there is a finite degree unramified extension E/F over which G is split.

Chapter 2

Shimura Varieties

Here we will use [5] as the primary reference. We will treat this topic in more detail than what is needed to understand the paper [1], for the purpose of enriching our understanding of this interesting topic.

2.1 Hermitian symmetric domains

First, we recall some notions from differential geometry, assuming familiarity with the notions of smooth and complex manifolds and their tangent bundles. Let M be a smooth manifold. Let $\mathcal{T}(M) \xrightarrow{p} M$ denote the tangent bundle of M and $\mathcal{T}_p(M)$ denote the tangent space of M at point p . A vector field on an open subset $U \subset M$ is a section of the map p .

A Riemannian manifold is a smooth manifold M endowed with a Riemannian metric i.e. a family $(g_p)_{p \in M}$ of symmetric, positive definite bilinear maps $g_p : \mathcal{T}_p(M) \times \mathcal{T}_p(M) \rightarrow \mathbb{R}$ such that for smooth vector fields X_1, X_2 on any open subset $U \subset M$, $p \mapsto g_p(X_1, X_2)$ is a smooth function on U .

If M additionally has the structure of a complex manifold, then $\mathcal{T}(M)$ gets an additional structure of a family $(J_p)_{p \in M}$ of maps $J_p : \mathcal{T}_p(M) \rightarrow \mathcal{T}_p(M)$ such that $J_p^2 = -1$ for all $p \in M$. Then $(\mathcal{T}_p(M), J_p)$ becomes a complex vector space ($i \in \mathbb{C}$ acts via J_p). We want to define a notion of a metric on this complex manifold which is compatible with this extra structure on $\mathcal{T}(M)$. This motivates the following definition.

Definition 20 (Hermitian forms). Let V be a \mathbb{R} -vector space with an endomorphism $J : V \rightarrow V$ such that $J^2 = -\text{Id}$. A Hermitian form on (V, J) is an \mathbb{R} -bilinear mapping $(|) : V \times V \rightarrow \mathbb{C}$ such that $(Ju|v) = i(u|v)$ and $(v|u) = \overline{(u|v)}$.

We can write $(u|v) = \phi(u, v) - i\psi(u, v)$. We call ϕ as the *real part* of the Hermitian form $(|)$. Note that ϕ is symmetric and satisfies $\phi(Ju, Jv) = \phi(u, v)$. Also, observe that $\psi(u, v) = -\phi(u, Jv)$.

Conversely, if we have a bilinear mapping $\phi : V \times V \rightarrow \mathbb{R}$ that is symmetric and satisfies $\phi(Ju, Jv) = \phi(u, v)$, then setting $(u|v) = \phi(u, v) + i\phi(u, Jv)$ defines a Hermitian form.

Definition 21 (Hermitian manifolds). A *Hermitian metric* on a complex manifold is a Riemannian metric g such that $g(JX, JY) = g(X, Y)$ for all vector fields X, Y . Hence, at each $p \in M$, g_p is the real part of a unique Hermitian form on $\mathcal{T}_p(M)$. A *Hermitian manifold* (M, g) is a complex manifold M with a Hermitian metric g .

Now we turn our attention to the concept of a Hermitian symmetric space. A connected (Hermitian) manifold M (with a metric g) is said to be homogeneous if its automorphism group (automorphisms preserving the complex structure and the Hermitian metric) acts transitively on M i.e. for every $p, q \in M$ there exist an automorphism sending p to q .

Definition 22 ((Hermitian) symmetric spaces). A connected (Hermitian) manifold M (with a metric g) is symmetric if it is homogeneous and at some point p there is an involution s_p (i.e. an automorphism satisfying $s_p^2 = 1$) having p as an isolated fixed point. s_p is called as the *symmetry at p* . By homogeneity, there is then a symmetry at every point of M .

We finally give a family of examples, which will of particular interest to us, of Hermitian symmetric spaces.

Let $D \subset \mathbb{C}^n$ be a bounded domain. By a theorem of Bergmann, every bounded domain has a canonical hermitian metric, called the Bergmann metric.

Now further assume that D is such that the group of holomorphic automorphisms $\text{Hol}(D)$ of D acts transitively and for some point there exists a holomorphic symmetry i.e. D is a *bounded symmetric domain*. As the Bergmann metric is canonical, it is invariant under the action of $\text{Hol}(D)$ and hence D becomes a Hermitian symmetric space with respect to the Bergmann metric.

We are only interested in the Hermitian symmetric spaces which are isomorphic to bounded symmetric domains. Such Hermitian symmetric spaces are called *Hermitian symmetric domains*. We remark that there is an alternative way of defining Hermitian symmetric domains, as is done in [5], as the Hermitian symmetric spaces of negative curvature.

Example 3 (Upper half plane \mathfrak{h}). The upper half plane \mathfrak{h} is isomorphic to the punctured open unit disc and hence is a bounded domain. $\text{SL}_2(\mathbb{R})$ acts transitively on \mathfrak{h} via Mobius transformation $\begin{pmatrix} a & b \\ c & d \end{pmatrix}.z = \frac{az+b}{cz+d}$. The map $z \mapsto 1/z$ is a symmetry at i . Hence, \mathfrak{h} is a bounded symmetric domain. The Bergmann metric on \mathfrak{h} is given by the hyperbolic metric $\frac{dx^2+dy^2}{y^2}$.

2.2 Automorphisms of Hermitian symmetric domain

An interesting aspect about the theory of Hermitian symmetric domains lies in its connections with the theory of algebraic groups. This is what we want to explain next. Let (M, g) be a Hermitian symmetric domain. Let $\text{Is}(M, g)$ denote the group of holomorphic automorphisms of M which preserve g . It is a theorem that $\text{Is}(M, g)$ has the natural structure of a Lie group and its connected component containing identity $\text{Is}(M, g)^+$ has the following properties:

1. $\text{Is}(M, g)^+$ acts transitively on M .
2. The stabilizer K_p of $p \in M$ is compact.
3. $\text{Is}(M, g)^+$ is non-compact.

Theorem 5. Let (M, g) be a Hermitian symmetric domain, and let \mathfrak{h} denote the Lie algebra of $\text{Is}(M, g)^+$. There is a unique connected algebraic subgroup G of $\text{GL}(\mathfrak{h})$ such that

$$G(\mathbb{R})^+ = \text{Is}(M, g)^+ \subset \text{GL}(\mathfrak{h}) \text{ via the adjoint representation.}$$

2.3 The homomorphism u_p

Recall that $U_1 = \{z \in \mathbb{C} \mid |z| = 1\}$. We have the following result.

Theorem 6. Let D be a Hermitian symmetric domain. For each $p \in D$, there exists a unique homomorphism $u_p : U_1 \rightarrow \text{Hol}(D)$ such that $u_p(z)$ fixes p and acts on $\mathcal{T}_p(D)$ as multiplication by z .

We need one more definition before we can state the main result of this section.

Definition 23 (Cartan involution). Let G be a connected algebraic group over \mathbb{R} and let $g \mapsto \bar{g}$ denote the complex conjugation on $G(\mathbb{C})$. An involution θ of G is said to be Cartan if the group

$$G^{(\theta)}(\mathbb{R}) := \{g \in G(\mathbb{C}) \mid g = \theta(\bar{g})\}$$

is compact.

Now we state the main result of this section.

Theorem 7. Let D be a Hermitian symmetric domain, and let G be the associated real adjoint algebraic group. The homomorphism $u_p : U_1 \rightarrow G$ attached to a point p of D has the following properties:

1. only the characters $z, 1, z^{-1}$ occur in the representation of U_1 on $\text{Lie}(G)_{\mathbb{C}}$ defined by $\text{Ad} \circ u_p$.
2. $\text{Ad}(u_p(-1))$ is a Cartan involution.
3. $u_p(-1)$ does not project to 1 in any simple factor of G .

Conversely, let G be a real adjoint algebraic group, and let $u : U_1 \rightarrow G$ satisfy the above three conditions. Then the set D of conjugates of u by elements of $G(\mathbb{R})^+$ has a natural structure of a Hermitian symmetric domain for which $G(\mathbb{R})^+ = \text{Hol}(D)^+$ and $u(-1)$ is the symmetry at u (regarded as a point of D).

This theorem is the motivation for the following definition of a Shimura datum.

2.4 Shimura Datum

We let $\mathbb{S} := \text{Res}_{\mathbb{R}}^{\mathbb{C}} \mathbb{G}_m$. \mathbb{S} will be referred to as the Deligne torus.

Definition 24 (Shimura Datum). A Shimura datum is a pair (G, X) consisting of a reductive algebraic group G defined over \mathbb{Q} and X to be a $G(\mathbb{R})$ -conjugacy class of homomorphisms $h : \mathbb{S} \rightarrow G_{\mathbb{R}}$ satisfying the following properties:

1. For any $h \in X$ only the weights $(0, 0), (1, -1), (-1, 1)$ may occur in $\mathfrak{g}_{\mathbb{C}} := \mathfrak{g} \otimes_{\mathbb{R}} \mathbb{C}$ i.e. we have the following decomposition

$$\mathfrak{g}_{\mathbb{C}} = \mathfrak{l} \oplus \mathfrak{p}^+ \oplus \mathfrak{p}^-$$

where for $z \in \mathbb{S}$, $h(z)$ acts trivially on \mathfrak{l} , via z/\bar{z} (resp. \bar{z}/z) on \mathfrak{p}^+ (resp. \mathfrak{p}^-).

2. The adjoint action of $h(i)$ induces a Cartan involution on the adjoint group of $G_{\mathbb{R}}$.
3. The adjoint group of $G_{\mathbb{R}}$ does not admit a factor H defined over \mathbb{Q} such that the projection of h on H is trivial.

It follows from the additional conditions that X has a canonical structure of a complex manifold and it has a natural action of $G(\mathbb{R})$.

If (G, X) is a Shimura datum then we can define for each compact open subgroup $K \subset G(\mathbb{A}_f)$ consider the following complex algebraic variety

$$S_K(\mathbb{C}) := G(\mathbb{Q}) \backslash X \times G(\mathbb{A}_f) / K.$$

The left action of $g \in G(\mathbb{Q})$ on $(x, g') \in X \times G(\mathbb{A}_f)$ is given by $g.(x, g') = (g.x, gg')$ where in the first component we interpret $g \in G(\mathbb{Q})$ as an element of

$G(\mathbb{R})$ and use the natural action of $G(\mathbb{R})$ on X , and in the second component we view $g \in G(\mathbb{Q})$ as an element of $G(\mathbb{A}_f)$ and use the group operation of $G(\mathbb{A}_f)$. The right action of $k \in K$ on $(x, g') \in X \times G(\mathbb{A}_f)$ is given by $(x, g') \cdot k = (x, g'k)$. Moreover, we have that S_K is defined over a finite extension E of \mathbb{Q} and E is independent of K . The field E is called the *reflex field*.

Chapter 3

Representations of *td* groups

We want to study the representation theory of groups like $G(F)$ where G is an algebraic group over \mathbb{Q} and $F = \mathbb{Q}_p$ or $F = \mathbb{A}^\infty$, where \mathbb{A}^∞ denotes the ring of finite adeles over \mathbb{Q} . We will encounter such representations mainly while studying the cohomology of Shimura varieties associated with the group G . The main reference for this chapter is [2].

First, the following allows us to define a topology on $G(F)$:

Fact 1. Let R be a topological ring. There exists a unique way to topologize $X(R)$ for all affine schemes X of finite type over R such that:

1. For a morphism $X \rightarrow Y$ of affine schemes of finite type over R , the induced map on points $X(R) \rightarrow Y(R)$ is continuous.
2. If $X \rightarrow Y$ and $Z \rightarrow Y$ are morphisms of affine schemes of finite type over R , then the topology on $(X \times_Y Z)(R) \simeq X(R) \times_{Y(R)} Z(R)$ is exactly the fibre product topology.
3. If $X \hookrightarrow Y$ is a closed immersion of affine schemes of finite type over R , then the induced map $X(R) \rightarrow Y(R)$ is a topological embedding.
4. If $X = \text{Spec}(R[t])$ then $X(R)$ is homeomorphic with R under the natural identification $X(R) \simeq R$.

The following definition captures the essence of the topology on $G(F)$:

Definition 25. A topological group is *td* if every neighbourhood of the identity contains a compact open subgroup.

A *td* group is totally disconnected (i.e. connected components are singletons), hence the terminology. They are also Hausdorff and locally compact.

Fact 2. Let G be an algebraic group over \mathbb{Q} and $F = \mathbb{Q}_p$ or $F = \mathbb{A}^S$ where \mathbb{A}^S is the ring of adeles away from the finite set S of places containing ∞ . Then $G(F)$, according to the topology defined by Fact 1 is *td*.

3.1 Hecke algebras

We want to study representations of groups like $G(F)$ as described above. Recall that, in the representation theory of finite groups G , there is an equivalence between representations of G over \mathbb{C} with modules over the group algebra $\mathbb{C}[G]$. We want to have an analogue of the group algebra for groups like $G(F)$. This analogue is known as the Hecke algebra, which is what we want to introduce next.

Let G be a td group in everything that follows in this section.

Definition 26 (Smooth functions). A function $f : G \rightarrow \mathbb{C}$ is *smooth* if it is locally constant. The complex vector subspace of \mathbb{C} -valued functions on G consisting of compactly supported smooth functions is denoted by $\mathcal{C}_c^\infty(G)$.

We want to $\mathcal{C}_c^\infty(G)$ into an algebra. Note that, if G is reductive, then $G(F)$ is unimodular i.e. the left and right Haar measures coincide. We define convolution of two smooth functions as the following integral w.r.t. a Haar measure: Let $f_1, f_2 \in \mathcal{C}_c^\infty(G)$, then we define:

$$(f_1 * f_2)(g) = \int_{G(F)} f_1(gh^{-1})f_2(h)dh.$$

Thus, $\mathcal{C}_c^\infty(G)$ is an algebra under convolution and it is known as the *Hecke algebra* of G . However, note that this algebra does not have an identity element.

For $K \subset G$ a compact open subgroup, we define the following subalgebra of the Hecke algebra consisting of K bi-invariant functions:

$$\mathcal{C}_c^\infty(G//K) = \{f \in \mathcal{C}_c^\infty(G) \mid f(k_1 g k_2) = f(g) \text{ for all } k_1, k_2 \in K\}.$$

The function $e_K := \frac{1}{\text{meas}(K)} \mathbb{1}_K$ is the identity element of $\mathcal{C}_c^\infty(G//K)$ and moreover we have:

Theorem 8. Any element $f \in \mathcal{C}_c^\infty$ is in $\mathcal{C}_c^\infty(G//K)$ for some compact open subgroup K . If $f \in \mathcal{C}_c^\infty(G//K)$, then f is a finite \mathbb{C} linear combination of elements of the form $\mathbb{1}_{K\gamma K}$ for $\gamma \in G$.

3.2 Smooth representations

In this section, we will describe the kind of representations of td groups that we will be interested in. Let G be a td group.

Definition 27. A representation (π, V) of G on a complex vector space V is *smooth* if the stabilizer of any vector in V is open in G .

Note that V is smooth if and only if $V = \bigcup_{K \subset G} V^K$ where the union is over all compact open $K \subset G$ and V^K denotes the subspace of V fixed by elements of K .

Now, we want to justify our earlier claim of how a smooth representation V can be given the structure of a module over the Hecke algebra of G .

Consider $f \in \mathcal{C}_c^\infty(G)$ and $v \in V$. We want to explain the action of f on v . As V is smooth, $V = \bigcup V^K$ and hence $v \in V^{K_1}$ for some K_1 . By Theorem 8, we also have that $f \in \mathcal{C}_c^\infty(G//K_2)$ for some K_2 . Define the compact open subset $K := K_1 \cap K_2$, then $v \in V^K$ and $f \in \mathcal{C}_c^\infty(G//K)$.

Again, by Theorem 8 we have that $f = \sum_\gamma \mathbb{1}_{K\gamma K}$ and hence it suffices to define the action of $\mathbb{1}_{K\gamma K}$ on v . We define $\mathbb{1}_{K\gamma K} \cdot v := \gamma v$. Note that this is well defined as $v \in V^K$. In this way, we now can view V as a module over $\mathcal{C}_c^\infty(G)$.

We can now ask the converse question of which $\mathcal{C}_c^\infty(G)$ -modules arise from a smooth representation of G . For this, we need the following definition:

Definition 28. A module M over an algebra A is *non-degenerate* if every element of M can be written as a finite sum $a_1 m_1 + a_2 m_2 + \cdots + a_n m_n$ for $a_i \in A$ and $m_i \in M$.

This definition is a triviality if the algebra A contains an identity, but we want to set A to be the Hecke algebra of G which does not have the identity element.

Theorem 9. There is an equivalence of categories between nondegenerate $\mathcal{C}_c^\infty(G)$ -modules and smooth representations of G .

Note that if V is a $\mathcal{C}_c^\infty(G)$ -module then V^K is a $\mathcal{C}_c^\infty(G//K)$ -module. This is because $\mathcal{C}_c^\infty(G//K) = e_K * \mathcal{C}_c^\infty(G) * e_K$ and $V^K = e_K V$ where we recall that $e_K = \frac{1}{\text{meas}(K)} \mathbb{1}_K$.

3.3 Admissible representations

We do not want to study all the smooth representations of a td group G as they can be quite big. We want to restrict to a smaller class of representations known as the admissible representations, by imposing certain finiteness conditions. The key point to have in mind, is that all irreducible smooth representations of $G(F)$ are admissible and hence restricting by restricting attention to admissible representations does not exclude any irreducible objects.

Definition 29 (Admissible representations). A representation V of G is admissible if it is smooth and V^K is finite dimensional for every compact open subgroup $K \subset G$. Analogously, a $\mathcal{C}_c^\infty(G)$ -module is admissible if it is non degenerate and $e_K V$ is finite dimensional.

We once again reiterate the statement made in the opening of this section:

Theorem 10. Let F be a p-adic field and let G be a reductive algebraic group over F . Then an irreducible, smooth representation of $G(F)$ is admissible.

3.4 Unramified Hecke algebra

In general, $\mathcal{C}_c^\infty(G//K)$ may not be commutative, as convolutions of arbitrary functions do not commute. But in this section, we turn our attention to a particular case of interest when this does happen.

Let G be an unramified reductive group over a p-adic field F . Hence, as discussed earlier, we have a hyperspecial subgroup $K \subset G(F)$. Then we have that:

Theorem 11. If G is unramified over F , and K is a hyperspecial subgroup then $\mathcal{C}_c^\infty(G(F)//K)$ is commutative. The algebra $\mathcal{C}_c^\infty(G(F)//K)$ is also known as the spherical Hecke algebra.

The spherical Hecke algebra can be made more explicit in the case when G is split over F as follows:

Theorem 12 (Satake Isomorphism). If G is unramified and split over F , then we have an isomorphism of algebras (where K is a hyperspecial subgroup)

$$\mathcal{C}_c^\infty(G(F)//K) \simeq \mathbb{C}[\hat{T}]^{W(\hat{G}, \hat{T})(\mathbb{C})}$$

where \hat{G} is the complex dual of G and $\hat{T} \subset \hat{G}$ is a maximal torus. $\mathbb{C}[\hat{T}]$ denotes the ring of global regular functions on the algebraic variety $\hat{T}(\mathbb{C})$ and hence has an action of $W(\hat{G}, \hat{T})(\mathbb{C})$ (the superscript denotes taking invariants).

We can state this in another equivalent way, we which now go on to describe.

Definition 30. Assume that G is unramified with hyperspecial subgroup $K \subset G(F)$. An irreducible admissible representation (π, V) of $G(F)$ is unramified if $V^K \neq 0$.

Theorem 13 (Satake Isomorphism). If G is unramified and split over F , then we have a bijection:

$$\begin{array}{c} \{\text{isom. classes of unramified representations of Weil group } W_F \rightarrow \hat{G}(\mathbb{C})\} \\ \updownarrow \\ \{\text{isom. classes of unramified representations of } G(F)\} \end{array}$$

Chapter 4

Automorphic Representations

4.1 Motivation for automorphic forms

We first recall the classical definition of a modular form. Let \mathfrak{h} denote the upper half plane and let $f : \mathfrak{h} \rightarrow \mathbb{C}$ be a function. Recall the notation of the *slash- k operator*:

$$(f|_k \gamma)(z) := (cz + d)^k f(z) \text{ for all } \gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{SL}_2(\mathbb{Z}) \text{ and } z \in \mathfrak{h}.$$

Recall the *congruence subgroup*:

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

Definition 31 (Modular forms). We have a function $f : \mathfrak{h} \rightarrow \mathbb{C}$. Let k be an integer and $\Gamma_1(N)$ be as before. We say that f is a modular form of *weight* k and *level* $\Gamma_1(N)$ if the following conditions are satisfied:

1. (Differential equation.) f is holomorphic. We think about holomorphic functions on \mathfrak{h} as smooth functions satisfying the Cauchy-Riemann equations.
2. (Transformation property.) $f|_k \gamma = f$ for all $\gamma \in \Gamma_1(N)$.
3. (Growth condition.) $f|_k \gamma$ is holomorphic at infinity for all $\gamma \in \mathrm{SL}_2(\mathbb{Z})$.

To motivate automorphic forms, we start by giving an alternative description of modular forms. Let f be a cuspidal modular form of weight k and level $\Gamma_1(N)$, for $N \geq 3$ and let $s \in \mathbb{C}$. Let

$$K_1(N) = \left\{ g \in \mathrm{GL}_2(\hat{\mathbb{Z}}) \mid g \equiv \begin{pmatrix} 1 & * \\ 0 & * \end{pmatrix} \pmod{N} \right\}.$$

It is a fact that we have the following decomposition

$$\mathrm{GL}_2(\mathbb{A}) = \mathrm{GL}_2(\mathbb{Q})K_1(N)\mathrm{GL}_2^+(\mathbb{R}).$$

Define

$$\begin{aligned}\phi_{f,s} : \mathrm{GL}_2(\mathbb{Q}) \backslash \mathrm{GL}_2(\mathbb{A}) &\rightarrow \mathbb{C} \\ \phi_{f,s}(\gamma k_1 h) &= (f|_k h)(i) \times (\det h)^s\end{aligned}$$

where $\gamma \in \mathrm{GL}_2(\mathbb{Q})$, $k_1 \in K_1(N)$ and $h \in \mathrm{GL}_2^+(\mathbb{R})$.

Next, note that the function $\phi_{f,s}$ is smooth and has the following properties:

1. $\phi_{f,s}(gk_1) = \phi_{f,s}(g)$ for all $k_1 \in K_1(N)$. The right $K_1(N)$ invariance of the function $\phi_{f,s}$ encodes that the function $\phi_{f,s}$ comes from a modular form f of level $\Gamma_1(N)$.
2. For $k_\infty \in O_2(\mathbb{R})$ (a maximal compact subgroup of $\mathrm{GL}_2(\mathbb{R})$) $\phi(gk_\infty) = \chi(k_\infty)\phi(g)$, where χ is the character $O_2(\mathbb{R}) \rightarrow \mathbb{C}^*$. The weight of the modular form f can be recovered from this character χ .

An automorphic form will vaguely be a smooth function

$$\psi : \mathrm{GL}_2(\mathbb{Q}) \backslash \mathrm{GL}_2(\mathbb{A}) \rightarrow \mathbb{C}$$

such that for some compact open $K_f \subset G(\mathbb{A}_f)$ we have $\psi(gk_f) = \psi(g)$ for all $k \in K_f$ and for a maximal compact subgroup $K_\infty \subset G(\mathbb{R})$ we have $\{\phi(gk_\infty) \mid k_\infty \in K_\infty\}$ spans a finite dimensional space. Automorphic forms also need to satisfy additional conditions (differential equation, growth condition). Moreover, we restrict attention to cuspidal automorphic forms.

If ψ is an automorphic form, and $g \in G(\mathbb{A}_f)$ then $\gamma \mapsto \psi(\gamma g)$ is also an automorphic form. Hence, the space of automorphic forms is a representation of $G(\mathbb{A}_f)$. An automorphic representation will vaguely be an irreducible $G(\mathbb{A}_f)$ subrepresentation of the space of automorphic forms. In the next section, we will give more precise definitions of these concepts.

4.2 Automorphic forms

Let G be an algebraic group over \mathbb{Q} . Let K_∞ be a maximal compact subgroup of $G(\mathbb{R})$. An function $\phi : G(\mathbb{Q}) \backslash G(\mathbb{A}) \xrightarrow{C}$ is called an automorphic form if it satisfies the following conditions:

1. ϕ is smooth. We recall that this means the following: write $(x, y) \in G(\mathbb{A}) = G(\mathbb{A}_f) \times G(\mathbb{R})$, then for a fixed x , ϕ is smooth function of y and for a fixed y , ϕ as a function of x is locally constant.
2. There exists some compact open subgroup $K \subset G(\mathbb{A}_f)$ such that $\phi(gk) = \phi(g)$ for all $k \in K$.

3. The \mathbb{C} -vector space spanned by $g \mapsto \phi(gk_\infty)$ is finite dimensional as $k_\infty \in K_\infty$.
4. There exists an ideal $I \subset Z(U(\mathfrak{g}_\mathbb{C}))$ of finite codimension such that it annihilates the function $y \mapsto \phi(x, y)$ for all $x \in G(\mathbb{A}_f)$.
5. For each $x \in G(\mathbb{A}_f)$, the function on $G(\mathbb{R})$ defined by $y \mapsto f(xy)$ is *slowly increasing*. Where we say that a function $\alpha : G(\mathbb{R}) \rightarrow \mathbb{C}$ is slowly increasing if there exists C and n such that for all $y \in G(\mathbb{R})$ we have $|\alpha(y)| \leq C \|y\|^n$.

Next, we want to define the notion of an automorphic representation. For this, we consider the space $\mathcal{A}(G)$ of automorphic forms on G . Note that $G(\mathbb{A}_f)$ acts on the left on $\mathcal{A}(G)$ as $(g * \phi)(\gamma) = \phi(\gamma g)$. Similarly, K_∞ acts on $\mathcal{A}(G)$ and also $\mathfrak{g}_\mathbb{C}$ acts, thus making $\mathcal{A}(G)$ a (\mathfrak{g}, K_∞) -module.

Hence, $\mathcal{A}(G)$ is a $G(\mathbb{A}_f) \times (\mathfrak{g}, K)$ -module. However, $\mathcal{A}(G)$ is still too big to work with. We need to impose some further conditions, which we will now explain.

Let us first define the notion of a *cuspidal automorphic form*. Let P be a maximal proper parabolic subgroup of G . Let $P = M \otimes N$ where M is a Levi subgroup and N is unipotent. We say that an automorphic form $\phi : G(\mathbb{Q}) \backslash G(\mathbb{A}) \rightarrow \mathbb{C}$ is cuspidal if

$$\int_{N(\mathbb{Q}) \backslash N(\mathbb{A})} \phi(xn) dn = 0.$$

Let us denote by Z , the centre of G . Fix some central character $\chi : Z(\mathbb{Q}) \backslash Z(\mathbb{A}) \rightarrow \mathbb{C}^*$.

We now define $\mathcal{A}_0(G, \chi) := \{\phi \in \mathcal{A}(G) \mid \phi \text{ is cuspidal and } \phi(gz) = \chi(z)\phi(g), \forall z \in Z(\mathbb{A}), \forall g \in G(\mathbb{A})\}$. We finally arrive at our main definition.

Definition 32 (Cuspidal automorphic representation). A cuspidal automorphic representation π of $G(\mathbb{A})$ is an irreducible subrepresentation of $\mathcal{A}_0(G, \chi)$ for some χ . We also denote by $m(\pi)$ the multiplicity with which π occurs in the space $\mathcal{A}_0(G, \chi)$.

Chapter 5

Main Theorem

5.1 A particular algebraic group

Let F_0 be a totally real number field and let F be a totally imaginary quadratic extension of F_0 .

Let D be a division algebra with centre F of dimension, say n^2 , equipped with an involution $*$ which restricts to the non trivial automorphism of F/F_0 .

We define an algebraic group G over \mathbb{Q} whose points over any commutative \mathbb{Q} -algebra R are given by:

$$G(R) = \{x \in D \otimes_{\mathbb{Q}} R \mid xx^* \in 1 \otimes R^\times\}.$$

We will continue to denote by G the group defined above throughout this chapter.

Example 4. For drawing an analogy, consider the algebra $M_n(\mathbb{R})$ with an involution $*$ defined as taking the transpose of a matrix. Then, the group of unitary similitudes $GU(n)$ can be described as

$$GU(n)(R) = \{x \in M_n(\mathbb{R}) \otimes_{\mathbb{Q}} R \mid xx^* \in 1 \otimes R^\times\}.$$

Later, we will define a Shimura datum associated to this group G which will give Shimura variety over a reflex field, which we denote by E . Postponing the discussion of the Shimura datum to the later section, right now we will give a way of determining the reflex field E from the group G .

We consider a morphism of algebraic groups $c : G \rightarrow \mathbb{G}_m$ over \mathbb{Q} given by the following map on points:

For a \mathbb{Q} -algebra R we consider $x \in G(R)$. We have the map from $G(R) \rightarrow R^\times$ given by sending $x \mapsto xx^*$. This defines a natural transformation from G to \mathbb{G}_m , which is the desired map.

Let G_0 denote the kernel of the map c . Then $G_0 \simeq \prod_j U(n(i), n(i'))$, where j runs over the set of \mathbb{Q} -embeddings of $F_0 \rightarrow \mathbb{R}$ and i, i' are two embeddings $F \rightarrow \mathbb{C}$ that extend j . The map $i \mapsto n(i)$ defines a map $I \rightarrow \mathbb{N}$ where I is the set of \mathbb{Q} -embeddings of F . The Galois group $\text{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ naturally acts continuously on I and hence also on the set of functions $I \rightarrow \mathbb{N}$.

The stabilizer of the function $i \rightarrow n(i)$ is closed in $\text{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ and hence corresponds to an intermediate field extension, which is the reflex field E .

5.2 A particular Shimura datum

A Shimura datum consists of a pair (G, X) where G is a reductive algebraic group and X is a $G(\mathbb{R})$ conjugacy class of homomorphisms $h : \mathbb{S} \rightarrow G_{\mathbb{R}}$. They should satisfy certain additional conditions which we have explained in the chapter on Shimura varieties.

It follows from the additional conditions that X has a canonical structure of a complex manifold and it has a natural action of $G(\mathbb{R})$. The important consequence of having a Shimura datum is that it associates to each compact open $K \subset G(\mathbb{A}_f)$, a variety S_K over the reflex field E such that $S_K(\mathbb{C}) = G(\mathbb{Q}) \backslash X \times G(\mathbb{A}_f)/K$. The field E is a finite extension of \mathbb{Q} .

In the previous section, we described what G we want to take. We now describe the map h . To begin with, choose an \mathbb{R} -algebra homomorphism

$$h_0 : \mathbb{C} \rightarrow D \otimes \mathbb{R}$$

satisfying the property that $h_0(z)^* = h_0(\bar{z})$ for $z \in \mathbb{C}$. Note that here the involution $*$ is an involution on $D \otimes \mathbb{R}$ which is induced by the involution on D (and acts trivially on \mathbb{R}).

We now want to define a map

$$h : \text{Res}_{\mathbb{R}}^{\mathbb{C}} \mathbb{G}_m \rightarrow G_{\mathbb{R}}.$$

Consider an \mathbb{R} -algebra R . For $z \otimes r \in (\mathbb{C} \otimes R)^*$ then h is defined by the map $z \otimes r \mapsto h_0(z^{-1}) \otimes r \in (D \otimes R)^*$.

Let X_{∞} denote the $G(\mathbb{R})$ conjugacy class of h . We need to impose one final condition which will make (G, X_{∞}) a Shimura datum.

Using h_0 we define the following involution on $D \otimes \mathbb{R}$

$$x \mapsto h_0(i)^{-1} x^* h_0(i).$$

We need to assume that this involution is positive and this gives us a Shimura datum.

It is interesting to give yet another way of describing the reflex field E of the Shimura variety in terms of the map h , which we do now.

From h_0 we get a \mathbb{C} -algebra homomorphism

$$h_{0,\mathbb{C}} : \mathbb{C} \otimes_{\mathbb{R}} \mathbb{C} \rightarrow D \otimes_{\mathbb{Q}} \mathbb{C}.$$

Recall that we have the totally real field F_0 and a totally imaginary quadratic extension F as in the earlier section. Once again, let I denote the

set of embeddings of F in \mathbb{C} and for $i \in I$, denote by i' the composition of i with the non trivial automorphism of F/F_0 . Then

$$D \otimes_{\mathbb{Q}} \mathbb{C} = \prod_{i \in I} D \otimes_{F,i} \mathbb{C}$$

and hence for $i \in I$ we have the maps:

$$h_i : \mathbb{C} \otimes \mathbb{C} \xrightarrow{h_{0,\mathbb{C}}} D \otimes_{\mathbb{Q}} \mathbb{C} \rightarrow D \otimes_{F,i} \mathbb{C}.$$

Choose a simple $D \otimes_{F,i} \mathbb{C}$ module V , then $\dim_{\mathbb{C}} V = n$. The map h_i gives D the structure of a $\mathbb{C} \otimes_{\mathbb{R}} \mathbb{C}$ module. Note that $\mathbb{C} \otimes_{\mathbb{R}} \mathbb{C} \simeq \mathbb{C} \times \mathbb{C}$ via the isomorphism $z_1 \otimes z_2 \mapsto (z_1 z_2, \bar{z}_1 z_2)$. Hence, as a $\mathbb{C} \times \mathbb{C}$ module, V decomposes as $V = V_1 \oplus V_2$. We let $n(i) = \dim_{\mathbb{C}} V_1$ and once again E is the fixed field of the stabilizer in $\text{Gal}(\bar{\mathbb{Q}}/\mathbb{Q})$ of the function $i \mapsto n(i)$.

5.3 Local systems on $S_K(\mathbb{C})$

Let L be a number field. Let $\zeta : G \rightarrow \text{GL}_V$ be a representation of G , where V is a L -vector space (we again denote by G the group defined at the beginning of the chapter). Assume that ζ is irreducible over \bar{L} .

Consider the vector bundle:

$$G(\mathbb{Q}) \backslash X \times V \times G(\mathbb{A}_f) / K \rightarrow G(\mathbb{Q}) \backslash X \times G(\mathbb{A}_f) / K = S_K(\mathbb{C})$$

where the actions defining the double quotients are as defined before in addition to the $G(\mathbb{Q})$ acting on V via ζ and K acting trivially on V .

We denote by \mathcal{F} to be sheaf of section of this bundle. Then \mathcal{F} is a local system (i.e. locally constant sheaf) on $S_K(\mathbb{C})$ of L vector spaces.

In our case, $S_K(\mathbb{C})$ is in fact compact and hence $H^i(S_K(\mathbb{C}), \mathcal{F})$ are finite dimensional L vector spaces.

Additionally, note that for every finite place λ of L the local system $\mathcal{F} \otimes L_\lambda$ on $S_K(\mathbb{C})$ comes from a smooth L_λ sheaf on S_K over E , which we will denote by \mathcal{F}_λ .

For the variety S_K over the reflex field E and a smooth L_λ sheaf of abelian groups \mathcal{F}_λ , the Etale cohomology $H_{et}^i(S_K, \mathcal{F}_\lambda)$ has the structure of a $\text{Gal}(\bar{E}/E)$ representation, which we will now describe.

For $g \in \text{Gal}(\bar{E}/E)$ the action on the cohomology is given by:

$$\begin{array}{c} H_{et}^i(S_K \times_{\text{Spec}(E)} \text{Spec}(\bar{E}), \mathcal{F}_\lambda \otimes \bar{L}_\lambda) \\ \downarrow 1 \times g \\ H_{et}^i(S_K \times_{\text{Spec}(E)} \text{Spec}(\bar{E}), (1 \times g)^* \mathcal{F}_\lambda \otimes \bar{L}_\lambda) \\ \downarrow \simeq \\ H_{et}^i(S_K \times_{\text{Spec}(E)} \text{Spec}(\bar{E}), \mathcal{F}_\lambda \otimes \bar{L}_\lambda) \end{array}$$

It is a standard fact that once we fix an isomorphism of $L_\lambda \simeq \mathbb{C}$ we have the following isomorphism:

$$H_{\text{et}}^i(S_K, \mathcal{F}_\lambda) \simeq H^i(S_K(\mathbb{C}), \mathcal{F} \otimes L_\lambda).$$

Hence, via this isomorphism, $H^i(S_K(\mathbb{C}), \mathcal{F} \otimes L_\lambda)$ also gets the structure of a $\text{Gal}(\overline{E}/E)$ representation.

5.4 Hecke correspondences

Let $K \subset G(\mathbb{A}_f)$ be a compact open subgroup as before. For $g \in G(\mathbb{A}_f)$, define $K' = K \cap gKg^{-1}$.

A diagram of the form $X \leftarrow Y \xrightarrow{\simeq} X$ is called a correspondence on X . We have the following correspondence on $S_K(\mathbb{C})$ defined by g : (Recall: $S_K(\mathbb{C}) = G(\mathbb{Q}) \backslash (X \times (G(\mathbb{A}_f)/K))$.)

$$\begin{array}{c} S_K(\mathbb{C}) \\ \uparrow (x, hK') \mapsto (x, hK) \\ S_{K'}(\mathbb{C}) \\ \downarrow (x, hK') \mapsto (x, hgK) \\ S_K(\mathbb{C}) \end{array}$$

We can check that g, g' define the equivalent correspondences if $KgK = Kg'K$. Moreover, Hecke correspondence defined by the double coset KgK induces an endomorphism of $H^i(S_K(\mathbb{C}), \mathbb{C})$.

Let $\mathcal{C}^\infty(G(\mathbb{A}_f)//K)_L$ denote the Hecke algebra of compactly supported K -bi-invariant functions L -valued functions on $G(\mathbb{A}_f)$. Note that, as explained before, every $f \in \mathcal{C}^\infty(G(\mathbb{A}_f)//K)_L$ is of the form $f = \sum_{i=1}^n \mathbb{1}_{Kg_iK}$. Hence, using the above Hecke correspondences, by linear extension we have an action of the Hecke algebra $\mathcal{C}^\infty(G(\mathbb{A}_f)//K)_L$ acts on $H^i(S_K(\mathbb{C}), \mathcal{F})$.

5.5 Construction of the Galois representation

We have now described actions of $\text{Gal}(\overline{E}/E)$ on $H^i(S_K(\mathbb{C}), \mathcal{F} \otimes L_\lambda)$ for a finite place λ of L and the action of $\mathcal{C}^\infty(G(\mathbb{A}_f)//K)_L$ on $H^i(S_K(\mathbb{C}), \mathcal{F})$ (and hence the induced action on $H^i(S_K(\mathbb{C}), \mathcal{F} \otimes L_\lambda)$). Note that these actions commute, making $H^i(S_K(\mathbb{C}), \mathcal{F} \otimes L_\lambda)$ into a $\mathcal{C}^\infty(G(\mathbb{A}_f)//K)_L \times \text{Gal}(\overline{E}/E)$ module.

Next, fix an admissible representation π_f of $G(\mathbb{A}_f)$ and define the L -vector space:

$$W^i(\pi_f) := \text{Hom}_{\mathcal{C}^\infty(G(\mathbb{A}_f)//K)_L}(\pi_f^K, H^i(S_K(\mathbb{C}), \mathcal{F}))$$

where, recall that by π_f^K we mean the subspace of K -invariants of π_f . Note that we have omitted K from our notation $W^i(\pi_f)$, although $W^i(\pi_f)$ as defined above a priori depends on K . However, there is an equivalent way to define $W^i(\pi_f)$ using the Shimura variety at infinite level, which makes the independence on K more explicit.

As $H^i(S_K(\mathbb{C}), \mathcal{F} \otimes L_\lambda)$ is a $\mathcal{C}^\infty(G(\mathbb{A}_f)//K)_L \times \text{Gal}(\overline{E}/E)$ module, we get that the L_λ -vector space $W^i(\pi_f)_\lambda := W^i(\pi_f) \otimes L_\lambda$ has the structure of a $\text{Gal}(\overline{E}/E)$ representation. We want to describe $W^i(\pi_f)_\lambda$ in terms of the automorphic representations of $G(\mathbb{A})$, at places of good reduction. We now proceed to define the places of good reduction in this context.

5.6 Places of good reduction

As our Shimura varieties are compact, we recall that $H^i(S_K(\mathbb{C}), \mathcal{F})$ is a finite dimensional representation of $\mathcal{C}^\infty(G(\mathbb{A}_f)//K)_L$ and that $H^i(S_K(\mathbb{C}), \mathcal{F})$ is zero unless $0 \leq i \leq 2 \dim S_K$. Hence, there exists $f^\infty \in \mathcal{C}^\infty(G(\mathbb{A}_f)//K)_L$ such that f^∞ acts by 0 on all the irreducible subrepresentations of $H^i(S_K(\mathbb{C}), \mathcal{F})$ (for all i) except those isomorphic to π_f^K , where it acts by a non-zero scalar (only finitely many classes of irreducible representations can occur in these cohomologies). Further, after a suitable normalization, we may assume that $\text{tr} \pi_f^K(f^\infty) = 1$ (to be interpreted as the trace of the operator f^∞ acting on the vector space π_f^K).

Now, we are ready to describe the cofinite set of primes S_{good} , which will be our places of good reduction. A prime $p \in S_{\text{good}}$ if the following three conditions hold:

1. the group G is quasi-split over \mathbb{Q}_p and split over an unramified extension of \mathbb{Q}_p OR EQUIVALENTLY G as a group over \mathbb{Q}_p is unramified.
2. the compact open subgroup K of $G(\mathbb{A}_f)$ is a product $K^p K_p$, where K^p is a compact open subgroup of $G(\mathbb{A}_f^p)$ (the finite adeles away from the prime p) and K_p is a hyperspecial maximal compact subgroup of $G(\mathbb{Q}_p)$.
3. the function f^∞ can be written as the product of a function $f^p \in \mathcal{C}^\infty(G(\mathbb{A}_f^p)//K^p)_L$ times the unit element of $\mathcal{C}^\infty(G(\mathbb{Q}_p)//K_p)_L$.

We can now state more precisely the goal of the main theorem. For all $p \in S_{\text{good}}$ and all places v of E over p and all places λ of L over primes different from p , we want to describe the representations $W^i(\pi_f)_\lambda$ of $\text{Gal}(\overline{E}_v/E_v)$ in terms of automorphic representations of $G(\mathbb{A})$.

5.7 Satake isomorphism

By Flath's theorem, we can decompose the irreducible admissible representation π_f as a restricted tensor product $\pi_f = \bigotimes'_p \pi_p$, where π_p is an irreducible admissible representation of $G(\mathbb{Q}_p)$. Following our first assumption, we know that π_p is an unramified representation of $G(\mathbb{Q}_p)$. Now, we describe how to associate an unramified \bar{L} representation $V(\pi_p, E_v)$ of the Weil group W_{E_v} to π_p .

Note that the Satake isomorphism associates an unramified admissible L -parameter $\phi(\pi_p) : W_{\mathbb{Q}_p} \rightarrow {}^L(G_{\mathbb{Q}_p})$, where ${}^L(G_{\mathbb{Q}_p})$ denotes the Langlands dual of $G_{\mathbb{Q}_p}$.

Next, we note that the homomorphism $h : \text{Res}_{\mathbb{R}}^{\mathbb{C}}(\mathbb{G}_m) \rightarrow G_{\mathbb{R}}$ gives rise to a conjugacy class of co-characters $\mu : \mathbb{G}_m \rightarrow G_{E_v}$. Referring to Lemma 2.1.2 of [6], we have a \bar{L} representation r of ${}^L(G_{\mathbb{Q}_p})$ such that as a \hat{G} representation, r is irreducible with highest weight $\hat{\mu} : \hat{G} \rightarrow \mathbb{G}_m$ (the dual of μ).

The unramified representation $V(\pi_p, E_v)$ of W_{E_v} is defined as:

$$V(\pi_p, E_v) = (r \circ \phi(\pi_p)) \otimes \chi$$

where χ is the unramified quasi-character of W_{E_v} whose value on geometric Frobenius element Φ_v of $W_{E_v}^{\text{unr}}$ is $(\sqrt{p})^{[E_v:\mathbb{Q}_p] \dim S_K}$ (we assume that there exist a square root of p in L and we choose one of them and denote it by \sqrt{p}). The χ is only present to take care of certain normalizations.

We denote by $P(\pi_p, E_v)$ the characteristic polynomial of Φ_v acting on $V(\pi_p, E_v)$.

5.8 Statement of the main theorem

Recall that we started with the local system $\zeta : G \rightarrow \text{GL}_V$ and an irreducible admissible representation π_f of $G(\mathbb{A}_f)$. Let $\zeta_{\mathbb{C}} = \zeta \otimes_L \mathbb{C}$ and $\pi_{f,\mathbb{C}} = \pi_f \otimes_L \mathbb{C}$. Choose a discrete series representation π_{∞}^0 of $G(\mathbb{R})$ having the same central and infinitesimal character as the contragredient of $\zeta_{\mathbb{C}}$ and let f_{∞} be $(-1)^{\dim S_K}$ times a pseudo-coefficient for π_{∞}^0 . For an automorphic representation π with central character χ_{π} of $G(\mathbb{A})$ we introduce the notation $m(\pi)$ to denote the multiplicity of π in the space of automorphic forms on $G(\mathbb{Q}) \backslash G(\mathbb{A})$ transforming by χ_{π} under the center of $G(\mathbb{A})$. We also introduce the integer $a(\pi_f)$ which is defined as follows:

$$a(\pi_f) = \sum_{\pi_{\infty}} m(\pi_{f,\mathbb{C}} \otimes \pi_{\infty}) \text{tr } \pi_{\infty}(f_{\infty}).$$

As in [7], the map $h : \text{Res}_{\mathbb{R}}^{\mathbb{C}} \mathbb{G}_m \rightarrow G$ determines a weight, which we denote by $w : \mathbb{G}_m \rightarrow \text{Center}(G)$. The composition $\zeta \circ w$ determines a scalar (element of center of GL_V), which we denote by $w(\zeta)$.

Recalling that we have the decomposition $\pi_f = \bigotimes'_p \pi_p$, we are now ready to state the main theorem:

- Theorem 14.**
1. The integer $a(\pi_f)$ is non-zero iff $W^i(\pi_f)$ is non zero for some i .
 2. Suppose $a(\pi_f)$ is non-zero. Let v be a place of E lying over a prime $p \in S_{\text{good}}$. Then π_p is unramified. Let α be a root of $P(\pi_p, E_v)$. If $a(\pi_f)$ is positive (resp. negative), there exists an even (resp. odd) integer i between 0 and $2 \dim S_K$ such that α is an algebraic number all of whose complex absolute values are equal to $q_v^{(i+w(\zeta))/2}$ (where q_v is the cardinality of the residue field of E_v). The polynomial $P(\pi_p, E_v)$ can be written uniquely as a product

$$\prod_{i=0}^{2 \dim S_K} P^i(\pi_p, E_v)$$

of monic polynomials with coefficients in L having the property that every root of $P^i(\pi_p, E_v)$ has weight $i+w(\zeta)$. Let λ be a place of L lying over a prime other than p . Then $W^i(\pi_f)_\lambda$ is an unramified representation of $\text{Gal}(\overline{E_v}/E_v)$ and the characteristic polynomial of the Frobenius Φ_v on $W^i(\pi_f)_\lambda$ is equal to the $|a(\pi_f)|$ -th power of $P^i(\pi_p, E_v)$.

Chapter 6

Proof of Main Theorem

6.1 Outline of the proof

We continue with the notation of the previous chapter, where we recall that λ was a place of L above a prime $p \in S_{\text{good}}$ and v was a place of E above a prime $l \neq p$.

We let $W(\pi_f)_\lambda$ denote the virtual representation $\bigoplus_{i=0}^{2 \dim S_K} (-1)^i W^i(\pi_f)_\lambda$ of $\text{Gal}(\overline{E}/E)$ and similarly define H_λ . To prove our main theorem that:

$$P(W(\pi_f)) = P(\pi_p, E_v)^{a(\pi_f)}$$

it suffices to show that:

$$\text{tr}(\Phi_v^i; W(\pi_f)) = a(\pi_f) \text{tr}(\Phi_v^i; V(\pi_p, E_v)).$$

Recall that we chose $f^\infty \in \mathcal{C}^\infty(G//K)_L$ such that:

$$\text{tr}(\Phi_v; W(\pi_f)_\lambda) = \text{tr}(f^\infty \times \Phi_v^j; H_\lambda).$$

Outline of the point counting method of [8]. The Shimura varieties S_K have a moduli interpretation as the moduli space of abelian varieties with certain extra structures (which we do not make precise). Using this moduli interpretation, one can show that S_K is defined over $(o_E)_v$ (i.e. the ring of integers of E localized at the place v). Once we have this, we can base change to $\text{Spec } r_v$ where r_v is the residue field of $(o_E)_v$ and obtain the Shimura variety "mod v " \overline{S}_K (a variety over the finite field r_v). Using the Grothendieck-Lefschetz trace formula, computation of $\text{tr}(f^\infty \times \Phi_v^j; H_\lambda)$ can be reduced to computing the r_v points on \overline{S}_K , the Shimura variety mod v . Invoking the moduli interpretation once again, counting points is equivalent to counting the number of (isomorphism classes of) abelian varieties over r_v with certain extra structures.

This counting is done in [8], and the final result is that $\text{tr}(f^\infty \times \Phi_v^j; H_\lambda)$ equals the following (we won't explain all the terms involved in this formula, but instead explain later the analogous formula for the group $G = \text{GL}_2$):

$$\tau(G) \sum_{\gamma_0} \sum_{(\gamma, \delta)} e(\gamma, \delta) O_\gamma(f_{\mathbb{C}}^{\infty, p}) TO_\delta(\phi_j) \operatorname{tr} \zeta_{\mathbb{C}}(\gamma_0) \cdot \operatorname{vol}(A_G(\mathbb{R})^0 \backslash I(\infty)(\mathbb{R})^{-1}) \quad (6.1)$$

where the first sum is over a set of representatives γ_0 for the stable conjugacy classes in $G(\mathbb{Q})$ and the second sum is over equivalence classes of pairs $(\gamma, \delta) \in G(\mathbb{A}_f^p) \times G(E_j)$ satisfying certain conditions.

In this formula, ϕ_j denotes an element of $\mathcal{C}^\infty(G(E_j)//K_j)_L$ where E_j is the unramified extension of E_v of degree j and K_j is a hyperspecial subgroup $G(E_j)$ lying over K_p . We can apply the *base change homomorphism* as given in [6] to obtain a function $f_j \in \mathcal{C}^\infty(G(\mathbb{Q}_p)//K_p)_L$ which has the property that:

$$\operatorname{tr} \pi_p(f_j) = \operatorname{tr}(\Phi_v^j; V(\pi_p, E_v)).$$

Applying the fundamental lemma of Clozel [9], we get that for every semisimple $\gamma_p \in G(\mathbb{Q}_p)$ we have:

$$SO_{\gamma_p}(f_j) = \sum_{\delta} e(\delta) TO_\delta(\phi_j) \quad (6.2)$$

where δ runs over a set of representatives for the σ conjugacy classes of $G(E_j)$ such that $\delta\sigma(\delta) \cdots \sigma^{r-1}(\delta)$ is conjugate to $\gamma_p \in G(\mathbb{Q}_p)$ (where $r := [E_j : \mathbb{Q}_p]$).

Along with the above, we need to know the computation of another orbital integral, of the function f_∞ defined in the earlier section:

$$SO_{\gamma_\infty}(f_\infty) = \operatorname{tr} \zeta_{\mathbb{C}}(\gamma_\infty) \cdot \operatorname{vol}(A_G(\mathbb{R})^0 \backslash I(\infty)(\mathbb{R})^{-1}) \cdot e(I) \quad (6.3)$$

Plugging 6.2 and 6.3 into the expression 6.1 we see that it simplifies to:

$$\tau(G) \sum_{\gamma_0} SO_{\gamma_0}(f_{\mathbb{C}}^p \cdot f_j \cdot f_\infty). \quad (6.4)$$

Next, we recall the Arthur-Selberg trace formula for a smooth function f on $G(\mathbb{A})$:

$$\sum_{\gamma} \tau(G_\gamma) O_\gamma(f) = \sum_{\pi} m(\pi) \operatorname{tr} \pi(f)$$

and also the stabilized Arthur-Selberg trace formula as given in [10]:

$$\sum_{\gamma_0} \tau(G) SO_{\gamma_0}(f) = \sum_{\pi} m(\pi) \operatorname{tr} \pi(f).$$

Apply the stabilized Arthur-Selberg trace formula to the function $f_{\mathbb{C}}^p \cdot f_j \cdot f_\infty$ we obtain that 6.4 equals:

$$\sum_{\pi} m(\pi) \operatorname{tr} \pi(f_{\mathbb{C}}^p \cdot f_j \cdot f_\infty).$$

We temporarily change the notation for our fixed representation π_f in the previous chapter to π_f^0 . From the definition of $a(\pi_f)$ as given in the previous chapter, we get that the above expression further simplifies to:

$$\sum_{\pi_f} \operatorname{tr} \pi_f(f_{\mathbb{C}}^p f_j) a(\pi_f) \quad (6.5)$$

(here the sum ranges over all irreducible representations of $G(\mathbb{A}_f)$).

Since f_j is bi-invariant under K_p , the number $\operatorname{tr} \pi_f(f_{\mathbb{C}}^p f_j)$ vanishes unless the component π_p of π_f at \mathbb{Q}_p is unramified, in which case:

$$\operatorname{tr} \pi_f(f_{\mathbb{C}}^p f_j) = \operatorname{tr} \pi_f(f_{\mathbb{C}}^p) \operatorname{tr} \pi_p(f_j).$$

From this, we see that every summand of 6.5 vanishes except the one indexed by $\pi_f = \pi_f^0 \otimes \mathbb{C}$.

Now, we can drop the superscript on π_f^0 and denote it once again by π_f . Since $\operatorname{tr}(\Phi_v^j; W(\pi_f)_\lambda) = 0$ unless the p-adic component π_p of π_f is unramified, we get our desired result:

$$\operatorname{tr}(\Phi_v^i; W(\pi_f)) = a(\pi_f) \operatorname{tr}(\Phi_v^i; V(\pi_p, E_v)).$$

The formula 6.1 simplifies for the group $G = \operatorname{GL}_2$ and becomes easier to work with. The ideas used to prove the formula for the group G in consideration in the paper [8] are analogous to the case of GL_2 . In the next few sections, we will turn our attention to the GL_2 case for obtaining a better understanding of the situation. Our main reference is [11].

6.2 Modular curves as moduli spaces

The Shimura variety associated to the group GL_2 is the modular curve. We proceed to describe the modular curve as the moduli of elliptic curves with level structure. Note that the Shimura variety in consideration in the paper [1] also can be described as the moduli of abelian varieties with extra structures, however this description is much more technical.

Definition 33 (Elliptic curve). A morphism $p : E \rightarrow S$ of schemes with a section $e : S \rightarrow E$ is said to be an elliptic curve over S if p is proper, flat and all geometric fibres are elliptic curves with zero section given by e .

Definition 34 (level-m-structure). A level-m-structure on an elliptic curve E/S is an isomorphism of group schemes over S

$$\alpha : (\mathbb{Z}/m\mathbb{Z})_S^2 \rightarrow E[m]$$

where $(\mathbb{Z}/m\mathbb{Z})_S^2$ is a constant group scheme over S and $E[m]$ is the base change of the closed embedding e under the multiplication-by- m map $E \xrightarrow{\times m} E$.

It follows that if E/S has a level- m -structure then m is invertible in S (i.e. invertible in the ring of global sections).

Theorem 15. Consider the following functor for $m \geq 3$

$$\mathcal{M}_m : \text{Sch} / \mathbb{Z}[m^{-1}] \rightarrow \text{Sets}$$

$S \rightarrow \{(E/S, \alpha) \text{ elliptic curve } E \text{ over } S \text{ with level-}m\text{-structure } \alpha, \text{ upto isomorphism}\}.$

Then this functor is representable by a smooth affine curve over $\mathbb{Z}[m^{-1}]$, which we again denote by \mathcal{M}_m .

As m will be fixed from now on, by abuse of notation, we will omit the subscript and write \mathcal{M}_m simply as \mathcal{M} .

Recall from the overview of the point counting method of previous section that we want to count the isomorphism classes of elliptic curves over a finite field k with level- m -structure, where $\text{char } k \nmid m$.

6.3 Tate module and Dieudonne module

Tate module.

Let E be an elliptic curve over a finite field k of order $q = p^r$. Let $l \neq p$ be a prime.

Define $T_l(E) := \varprojlim_n E_{\bar{k}}[l^n]$, where we recall that $E_{\bar{k}}[l^n] = \{P \in E(\bar{k}) \mid N \cdot P = 0\}$. Note that as $E_{\bar{k}}[l^n]$ is a free $\mathbb{Z}/l^n\mathbb{Z}$ module of rank 2, we get that $T_l(E)$ is a free \mathbb{Z}_l module of rank 2.

The \mathbb{Z}_l module $T_l(E)$ is also equipped with a $\text{Gal}(\bar{k}/k)$ action as follow: $\text{Gal}(\bar{k}/k)$ acts on $E(\bar{k})$ and hence also acts on $E_{\bar{k}}[l^n]$ for all n . Thus, we have an induced action of $\text{Gal}(\bar{k}/k)$ on $T_l(E)$.

Note that a map of elliptic curves $f : E \rightarrow E'$ over k induces a map of Tate modules $f^* : T_l(E) \rightarrow T_l(E')$.

We also define $V_l(E) := T_l(E) \otimes_{\mathbb{Z}_l} \mathbb{Q}_l$. The $\text{Gal}(\bar{k}/k)$ action on $T_l(E)$ induces an action on $V_l(E)$.

A fundamental property of the Tate module is the following:

Theorem 16 (Tate Isogeny theorem). The induced map

$$\phi : \text{Hom}_k(E, E') \otimes_{\mathbb{Z}} \mathbb{Z}_l \rightarrow \text{Hom}_{\text{Gal}(\bar{k}/k)}(T_l(E), T_l(E'))$$

is an isomorphism.

Dieudonne module. The Tate module $T_l(E)$ uniquely characterizes the inverse system of finite group schemes $\varprojlim E[l^n]$ only when $l \neq p$ (as in this case the finite group schemes are etale). For dealing with the inverse system of group schemes $\varprojlim E[p^n]$, we need a different approach. This leads us to the notion of the Dieudonne module $D(E)$ of the elliptic curve E .

We will not provide a construction of the Dieudonne module, but restrict ourselves to stating some properties of it.

Recall that E is defined over a finite field k or order $q = p^r$. We denote by \mathbb{Z}_{p^r} the ring of integers of \mathbb{Q}_{p^r} , the degree r unramified extension of \mathbb{Z}_p . The Dieudonne module $D(E)$ is a free module of rank 2 over \mathbb{Z}_{p^r} .

Additionally, note that as \mathbb{Q}_{p^r} is an unramified extension of \mathbb{Q}_p , we have that $\text{Gal}(\mathbb{Q}_{p^r}/\mathbb{Q}_p) \simeq \text{Gal}(k/\mathbb{F}_p)$. We denote by σ the element of $\text{Gal}(\mathbb{Q}_{p^r}/\mathbb{Q}_p)$ corresponding to the Frobenius $x \mapsto x^p$ under this isomorphism.

Analogous to the Galois action on the Tate module, we have some extra structures on $D(G)$. We have a σ semilinear operator F ("Frobenius") and a σ^{-1} semilinear operator V ("Verschiebung") on the \mathbb{Z}_{p^r} -module $D(E)$, such that $FV = VF = (p)$ (multiplication-by- p). Thus, we may define a ring D_k as the \mathbb{Z}_{p^r} algebra generated by F and V subject to the relations:

1. $FV = VF = p$.
2. $Fw = \sigma(w)F$ for all $w \in \mathbb{Z}_{p^r}$.
3. $wV = V\sigma(w)$ for all $w \in \mathbb{Z}_{p^r}$.

Thus, we have that $D(G)$ has an action of D_k .

A map of elliptic curves $f : E \rightarrow E'$ induces a map $f^* : D(E) \rightarrow D(E')$.

We also define $V_p(E) := D(E) \otimes_{\mathbb{Z}_{p^r}} \mathbb{Q}_{p^r}$.

Similar to the Tate Isogeny theorem, we have that:

Theorem 17. The natural map is an isomorphism:

$$\text{Hom}_k(E, E') \otimes_{\mathbb{Z}} \mathbb{Z}_p \rightarrow \text{Hom}_{D_k}(D(E), D(E')).$$

6.4 Point counting

Fix an elliptic curve E_0 over \mathbb{F}_{p^r} . We want to count the number of elements of:

$$\mathcal{M}(k)(E_0) := \{x \in \mathcal{M}(k) \mid E_0 \text{ is } k\text{-isogenous to } E_x\}.$$

Denote by $H^p := \prod_{l \neq p} T_l(E) \otimes \mathbb{A}_f^p$, a \mathbb{A}_f^p -module and by $H_p := V_p(E)$, a \mathbb{Q}_{p^r} -module. Choosing a k -isogeny $f : E_x \rightarrow E_0$ we get the following:

1. A $\text{Gal}(\bar{k}/k)$ invariant $\hat{\mathbb{Z}}^p$ lattice

$$L = f^*\left(\prod_{l \neq p} T_l(E_x)\right) \subset H^p.$$

2. A F, V -invariant \mathbb{Z}_{p^r} -lattice

$$\Lambda = f^*(D(E_x)).$$

3. Finally, the level structure: a $\text{Gal}(\bar{k}/k)$ invariant map

$$\phi : \mathbb{Z}/m\mathbb{Z} \rightarrow L \otimes \mathbb{Z}/m\mathbb{Z}$$

where $\mathbb{Z}/m\mathbb{Z}$ has the trivial $\text{Gal}(\bar{k}/k)$ action.

Let Y^p denote the set of pairs (L, ϕ) satisfying the first and the third conditions and let Y_p be the set Λ satisfying the second condition. Dividing by the choice of f we get a map:

$$\mathcal{M}(k)(E_0) \rightarrow \Gamma \backslash Y^p \times Y_p$$

where $\Gamma = (\text{End}(E_0) \otimes \mathbb{Q})^\times$. We state the following whose proof can be found in [11].

Theorem 18. This map is a bijection.

Hence, it remains to count the cardinality of $\Gamma \backslash Y^p \times Y_p$ and express it in terms of orbital integrals.

We know that H^p is a two dimensional \mathbb{A}_f^p vector space and that H_p is a two dimensional \mathbb{Q}_{p^r} vector space. Choose bases for both these vector spaces.

Note that from the $\text{Gal}(\bar{k}/k)$ action on the Tate modules, we have that the Frobenius of k ($x \mapsto x^{p^r}$) acts on H^p . Let $\gamma \in \text{GL}_2(\mathbb{A}_f^p)$ be this Frobenius endomorphism w.r.t. the chosen basis. Note that changing the basis of H^p , doesn't change the conjugacy class of γ .

Recall the notation from the section on Dieudonne modules: σ is the Frobenius on \mathbb{Q}_{p^r} and F is the σ semi-linear operator on $H_p = D(E) \otimes \mathbb{Q}_{p^r}$ (induced from F on $D(E)$).

From the chosen basis of H_p we have an isomorphism $H_p \simeq \mathbb{Q}_{p^r}^2$. We next define an element $\delta \in \text{GL}_2(\mathbb{Q}_{p^r})$ such that the following diagram commutes.

$$\begin{array}{ccc} H_p & \xrightarrow{\simeq} & \mathbb{Q}_{p^r}^2 \\ \downarrow & & \downarrow \sigma \\ F \curvearrowright H_p & \xrightarrow{\simeq} & \mathbb{Q}_{p^r}^2 \\ \downarrow & & \downarrow \delta \\ H_p & \xrightarrow{\simeq} & \mathbb{Q}_{p^r}^2 \end{array}$$

From this definition, it can indeed be checked that δ defines a linear map. It can also be checked that that changing the basis of H_p doesn't change the σ -conjugacy class of δ .

Next we define the following:

1. $G_\gamma(\mathbb{A}_f^p) = \{g \in \text{GL}_2(\mathbb{A}_f^p) \mid g^{-1}\gamma g = \gamma\}$.

2. $G_{\delta,\sigma}(\mathbb{Q}_p) = \{h \in \mathrm{GL}_2(\mathbb{Q}_{p^r}) \mid h^{-1}\delta h^\sigma = \delta\}$.
3. f^p is the characteristic function of the following set divided by its volume

$$K^p = \{g \in \mathrm{GL}_2(\hat{\mathbb{Z}}^p) \mid g \equiv 1 \pmod{m}\}.$$
4. $\phi_{p,0}$ is the characteristic function of the following set divided by the volume of $\mathrm{GL}_2(\mathbb{Z}_{p^r})$

$$\mathrm{GL}_2(\mathbb{Z}_{p^r}) \begin{pmatrix} p & 0 \\ 0 & 1 \end{pmatrix} \mathrm{GL}_2(\mathbb{Z}_{p^r}).$$

We finally arrive at the expression for the number of points in terms of orbital integrals:

Theorem 19. The cardinality of $\mathcal{M}(k)(E_0)$ is

$$\mathrm{vol}(\Gamma \backslash G_\gamma(\mathbb{A}_f^p) \times G_{\delta,\sigma}(\mathbb{Q}_p)) O_\gamma(f^p) T O_{\delta,\sigma}(\phi_{p,0}).$$

Bibliography

- [1] Robert E. Kottwitz. “On the λ -adic representations associated to some simple Shimura varieties”. In: *Invent. Math.* 108.3 (1992), pp. 653–665. ISSN: 0020-9910. DOI: [10.1007/BF02100620](https://doi.org/10.1007/BF02100620).
- [2] Heekyoung Hahn Jayce R. Getz. *An Introduction to Automorphic Representations*.
- [3] Brian Conrad. “Reductive Group Schemes”. In: (). URL: <http://math.stanford.edu/~conrad/papers/luminysga3.pdf>.
- [4] J. S. Milne. *Algebraic Groups*. URL: <https://www.jmilne.org/math/CourseNotes/iAG200.pdf>.
- [5] J. S. Milne. *Introduction to Shimura Varieties*. URL: <https://www.jmilne.org/math/xnotes/svi.pdf>.
- [6] Robert E. Kottwitz. “Shimura varieties and twisted orbital integrals”. In: *Math. Ann.* 269.3 (1984), pp. 287–300. ISSN: 0025-5831. DOI: [10.1007/BF01450697](https://doi.org/10.1007/BF01450697).
- [7] Pierre Deligne. “Variétés de Shimura: interprétation modulaire, et techniques de construction de modèles canoniques”. French. In: (1979), pp. 247–289.
- [8] Robert E. Kottwitz. “Points on some Shimura varieties over finite fields”. In: *J. Amer. Math. Soc.* 5.2 (1992), pp. 373–444. ISSN: 0894-0347. DOI: [10.2307/2152772](https://doi.org/10.2307/2152772).
- [9] Laurent Clozel. “The fundamental lemma for stable base change”. In: *Duke Math. J.* 61.1 (1990), pp. 255–302. ISSN: 0012-7094. DOI: [10.1215/S0012-7094-90-06112-5](https://doi.org/10.1215/S0012-7094-90-06112-5).
- [10] Robert E. Kottwitz. “Stable trace formula: elliptic singular terms”. In: *Math. Ann.* 275.3 (1986), pp. 365–399. ISSN: 0025-5831. DOI: [10.1007/BF01458611](https://doi.org/10.1007/BF01458611).
- [11] Peter Scholze. “The Langlands-Kottwitz approach for the modular curve”. In: *Int. Math. Res. Not. IMRN* 15 (2011), pp. 3368–3425. ISSN: 1073-7928. DOI: [10.1093/imrn/rnq225](https://doi.org/10.1093/imrn/rnq225).