Computing finite Galois groups arising from automorphic forms

Edward Leonardo Coto Mora

edward.coto-mora@universite-paris-saclay.fr

Advised by Prof. Gaëtan Chenevier

Algant Master Thesis - August 2020

Universiteit Leiden and Université Paris Sud

Computing finite Galois groups arising from automorphic forms

Edward Leonardo Coto Mora

August 28, 2020

Acknowledgments

I am deeply grateful to the ALGANT program that made this thesis possible. I am deeply indebted to my professors at Universiteit Leiden and at Université Paris-Saclay for influencing my mathematical career. First of all, I am sincerely grateful to my supervisor, Professor Gaëtan Chenevier, for suggesting the topic and for his constant supervision and patience in dealing with me, helping me during the development of this thesis and answering my questions when necessary. Also, I would like to thank the people who shared with me my last two years in Leiden and Paris, for their support and for sharing the long days of hard work. Finally and most importantly, I want to express my deepest gratitude to my family and girlfriend for their constant unconditional support during these two years.

Contents

Introduction

The inverse Galois problem asks if given a finite group G, there exists a Galois extension $L/\mathbb{Q}$ with Galois group isomorphic to G. This remains an open problem. In 1892, Hilbert proved that the symmetric group S_n and the alternating group A_n are Galois groups over $\mathbb{Q}$, for all n. It has also been shown to be true for some other families of finite groups. For instance, all finite solvable groups and all sporadic simple groups, except the Mathieu group M_{23}, are known to be Galois groups over $\mathbb{Q}$.

In this thesis we study a paper by Kay Magaard and Gordan Savin [17] on computing finite Galois groups arising from automorphic forms. The main objective is to construct $G_2(p)$ as a Galois group over $\mathbb{Q}$, where $G_2(p)$ is the exceptional group of type G_2 over the finite field of p elements, for p prime.

Theorem 0.1. *There is a set of primes S of density 1, such that for all $p \in S$, there exists an extension of $\mathbb{Q}$ with $G_2(p)$ as its Galois group which ramifies only at 5 and p.*

This is done by reducing, modulo p, the p-adic representation attached to a suitable regular, cuspidal automorphic representation of GL_7. To get such a representation, we start from an automorphic representation π that was constructed on an anisotropic form of G_2 by Gross and Savin [10], where it was also shown that π lifts to a regular, self-dual cuspidal automorphic representation σ on Sp_6, and then using some recent results of Arthur [1], σ can be lifted to a regular, self-dual cuspidal automorphic representation Π on GL_7.

Using a result of Harris and Taylor [11], we get attached to Π a compatible system of representations $\rho_p : \mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q}) \to GL_7(\bar{\mathbb{Q}}_p)$ for all p. The local components Π_2 and Π_3 of Π are unramified and using their Satake parameters, computed by Lansky and Pollack [14], we are able to know the conjugacy classes of $\rho_p(Fr_2)$ and $\rho_p(Fr_3)$ where Fr_2 and Fr_3 are the Frobenius at 2 and 3. Using this we get that the Zariski closure of the image of ρ_p is $G_2(\mathbb{Q}_p)$ for all $p \neq 5$. Thus for $p \neq 5$ the image of ρ_p is an open compact subgroup of $G_2(\mathbb{Q}_p)$ so it is reasonable to expect $G_2(p)$ to appear as a quotient of the image for all but finitely many primes.

The thesis is divided into six chapters. The first chapter aims to give the definition and basic properties concerning the exceptional group of type G_2. However, the main objective of this thesis is not to study G_2 itself, so we do not cover this in much detail. Apart from the basic properties we give a criterion for when two elements generate $G_2(p)$, this is done based on Ascbacher's classification of maximal subgroups of $G_2(p)$ [2].

In chapters 2 and 3 we will recall notions from algebraic groups, Galois theory and algebraic number theory. Our goal is to establish the theory with enough generality so that we can work with it later. It is worth mentioning that within these chapters we sometimes treat theory more generally than is necessary to achieve our goal. In chapter 2 we develop a notion of reduction, modulo $\mathfrak{p}$, of rational conjugacy classes, which is done in a generality of split reductive groups. Also, in Chapter 3 we study the Galois group of palindromic polynomials, which appear naturally when dealing with the group G_2.

In chapter 4 and 5 we deal with Galois representations and automorphic forms, again we would like to set up the theory to work with it later. In particular we care about studying the image of a Galois Representation, and to understand the implications of Harris and Taylor's theorem on Galois representations attached to automorphic forms [11], an instance of the general Langlands correspondence which still remains conjectural.

Finally in chapter six is where the main theorem is proven. This is divided into studying the Galois representations attached to a certain automorphic representation Π and constructing such a representation starting from a representation π of G_2. Among the steps for completing the proof we will take two theorems for granted, which exceed the purpose of the thesis, firstly the local Langlands correspondence for GL_n over a p-adic field, proven by Harris and Taylor in [11], and secondly the fact that a cuspidal automorphic representation on $Sp_{2n}(\mathbb{A})$ such that σ_q is the Steinberg representation for a prime q, lifts to a cuspidal automorphic representation Π of $GL_{2n+1}(\mathbb{A})$, such that Π_q is the Steinberg representation [1] and [17].

1 Exceptional Group of Type G_2

There are five exceptional algebraic groups, namely, the groups of type F_4, E_6, E_7, E_8, and G_2. The exceptional groups can be constructed from their Lie algebras or from their root systems. This chapter contains a survey about the smallest of the exceptional Lie groups G_2 and their Lie Algebras. Up to isomorphism there is a unique complex Lie algebra of type G_2 and two real Lie algebras of type G_2, the split real form and the compact real form. We will be interested in the compact real form. Finally, we will also include a criterion for when two elements of $G_2(p)$ generates the whole group.

1.1 Octonions

Let K be a field of characteristic zero. A Hurwitz algebra over K is a finite K-algebra A (not necessarily commutative) together with a non-degenerate quadratic form $N : A \to K$ such that $N(xy) = N(x)N(y)$ for all $x, y \in A$. It is well known that the only possible dimensions of A are actually $1, 2, 4$, and 8. A Hurwitz algebra of dimension 8 is also known as an Octonion algebra or Cayley algebra.

An (real) octonion algebra $\mathbb{O}$ can be built from the quaternions by taking 7 mutually orthogonal square roots of 1, labelled $e_1, ..., e_7$ (with subscripts understood modulo 7), subject to the condition that for each t, the elements e_t, e_{t+1}, e_{t+3} satisfy the same multiplication rules as i, j, k (respectively) in the quaternion algebra $\mathbb{H}$.

It is easy to see that this defines all multiplications, and that this multiplication is non-associative. The following is the multiplication table of $\{1, e_1, \ldots, e_7\}$

$\times$	1	e_1	e_2	e_3	e_4	e_5	e_6	e_7
1	1	e_1	e_2	e_3	e_4	e_5	e_6	e_7
e_1	e_1	-1	e_3	$-e_2$	e_5	$-e_4$	$-e_7$	e_6
e_2	e_2	$-e_3$	-1	e_1	e_6	e_7	$-e_4$	$-e_5$
e_3	e_3	e_2	$-e_1$	-1	e_7	$-e_6$	e_5	$-e_4$
e_4	e_4	$-e_5$	$-e_6$	$-e_7$	-1	e_1	e_2	e_3
e_5	e_5	e_4	$-e_7$	e_6	$-e_1$	-1	$-e_3$	e_2
e_6	e_6	e_7	e_4	$-e_5$	$-e_2$	e_3	-1	$-e_1$
e_7	e_7	$-e_6$	e_5	e_4	$-e_3$	$-e_2$	e_1	-1

There is a natural norm N, under which $\{1, e_1, \ldots, e_7\}$ is an orthonormal basis, and $N(x) = \bar{x}x$, where $-$ (called octonion conjugation) is the K-linear map fixing 1 and negating $e_1, \ldots, e_7$. One can check that $N(xy) = N(x)N(y)$. The norm N is positive-definite quadratic form, so $\mathbb{O}$ is an octonion division algebra.

Remark 1.1. *Just as with the quaternions, an octonion algebra $\mathbb{O}$ may be defined by the same rules over any field K of characteristic not 2.*

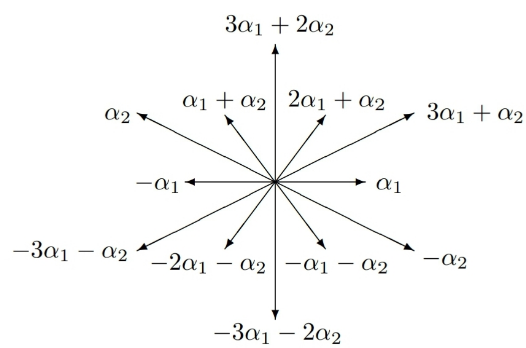
Remark 1.2. *Over the real numbers, the split-octonions, unlike the standard octonions, contain non-zero elements which are non-invertible. Up to isomorphism, the octonions and the split-octonions are the only two 8-dimensional algebras over $\mathbb{R}$.*

1.2 The group G_2

Among root systems in a two dimensional real vector space, there is an irreducible root system called of type G_2, which corresponds to

$$\Phi_{G_2} = \pm\{\alpha_1, \alpha_2, \alpha_1 + \alpha_2, 2\alpha_1 + \alpha_2, 3\alpha_1 + \alpha_2, 3\alpha_1 + 2\alpha_2\}$$

.



Let $\bar{K}$ be an algebraic closure of K and put $\mathbb{O}_{\bar{K}} = \bar{K} \otimes_K \mathbb{O}$. The automorphism group $G = Aut(\mathbb{O}_{\bar{K}})$ is a linear algebraic group. Since automorphisms leave the norm invariant, G is a closed subgroup of the algebraic group $\mathbf{O}(N)$ (the orthogonal group of the quadratic form on $\mathbb{O}_{\bar{K}}$ defined by N).

Proposition 1.1. *The algebraic group G is a connected, simple algebraic group of type G_2 of dimension* 14.

Proof. [22] Proposition 2.3.5.

Definition 1.1. We will call from now on G_2, to the automorphism group of the division octonions algebra over $\mathbb{R}$, and $G_2(q)$ to the automorphism group of the (unique) octonions algebra over the field of q elements.

Corollary 1.1. *G_2 is a subgroup of the rotation group $\mathbf{SO}(N)$.*

Proof. G_2 is contained in $\mathbf{O}(N)$. The connectedness of G_2 implies that it must be contained in the connected component of the identity in $\mathbf{O}(N)$, which is $\mathbf{SO}(N)$. $\square$

Proposition 1.2. *The automorphism group G_2 is defined over K.*

Proof. [22] Proposition 2.4.6.

Remark 1.3. *G_2 is $\mathbb{R}$-anisotropic (compact) and split over $\mathbb{Q}_p$ for all primes p ([8] Lemma 5.1).*

If $char(K) \neq 2$, G_2 acts on the 7-dimensional vector space $1^{\perp}$; the orthogonal complement of the identity. Moreover this action is faithful and irreducible. This yields the following proposition.

Proposition 1.3. *The algebraic group G_2 (over K of characteristic $\neq 2$) has a (unique) 7-dimensional faithful irreducible representation.*

Proposition 1.4. *$G_2(K)$ has rank two, and $G_2(K)$ has Weyl Group $W \cong D_6$.*

Proof. ([28], Section 4.3.5) We can also figure out the Weyl group geometrically from the root system above. The twelve roots are the twelve axes of symmetry of the polygon, and we can get rotations by first reflecting across one root and then across another. For example, rotating by a sixth of a turn can be effected by reflecting with the basic short root, and by reflecting with the basic long root. $\square$

Remark 1.4. *The above interpretation of G_2 as the automorphism group of $\mathbb{O}_{\bar{K}}$ only holds for char$(K) \neq 2$. One can find a definition of $G_2(2^a)$ in [28] Section 4.4.3.*

We end this section by mentioning some general properties of G_2.

Proposition 1.5. - *The order of $G_2(q)$, with q odd is $|G_2(q)| = q^6(q^6-1)(q^2-1)$.*

- *$G_2(q) < Sp_6(q)$ where $Sp_6(q)$ is the Symplectic group.*

- *$G_2(q)$ is simple for all q except for $q = 2$.*

Proof. [28], Sections 4.3.3, 4.3.4, 4.3.7.

1.3 Subgroups of $G_2(q)$

Maximal subgroups of $G_2(p)$ have been classified by Aschbacher. We extract the information from ([2], Corollary 11, p199).

Theorem 1.1. *Assume $p > 3$. The maximal subgroups of $G_2(p)$ are as follows:*

(1) maximal parabolic subgroups.

(2) $SL_3(p).2$ and $SU_3(p).2$.

(3) $SO_4^+(p)$.

(4) $PGL_2(p)$ if $p > 5$, acting on V like on homogeneous polynomials in two variables of degree 6.

(5) $2^3.L_3(2)$*, the stabilizer of an orthonormal basis of* V*; the order is* $2^6 \cdot 3 \cdot 7$

(6) $L_2(13)$ *if* $\mathbb{F}_p$ *is a splitting field for* $T^2 - 13$*; the order is* $2^2 \cdot 3 \cdot 7 \cdot 13$

(7) $G_2(2)$*; the order is* $2^6 \cdot 3^3 \cdot 7$

(8) $L_2(8)$ *if* $\mathbb{F}_p$ *is a splitting field for* $T^2 - 3T + 1$*; the order is* $2^3 \cdot 3^2 \cdot 7$

(9) J_1 *if* $p = 11$*; the order is* $2^3 \cdot 3 \cdot 5 \cdot 7 \cdot 11 \cdot 19$*.*

Corollary 1.2. *Assume that* $p > 3$*. Let* u *and* t *be two elements in* $G_2(p)$ *of orders* > 3*. If the order of* u *divides* $p^2 + p + 1$ *and the order of* t *divides* $p^2 - p + 1$ *then* u *and* t *are not contained in any maximal subgroup except, perhaps, the five groups of bounded order labeled (5) - (9).*

Proof. Let $\Phi_n(x)$ be the n-th cyclotomic polynomial. In particular:

$$\phi_1(p) = p - 1,\ \phi_2(p) = p + 1,\ \phi_3(p) = p^2 + p + 1 \text{ and } \phi_6(p) = p^2 - p + 1.$$

For any finite group G, let $|G|_{p'}$ be the prime to p part of the order of G. Then we get the following table:

G	$SL_3(p)$	$SU_3(p)$	$SO_4^+(p)$	$GL_2(p)$
$\lvert G\rvert_{p'}$	$\Phi_1(p)^2\Phi_3(p)$	$\Phi_1(p)\Phi_2(p)\Phi_6(p)$	$\Phi_1(p)^2\Phi_2(p)^2$	$\Phi_1(p)^2\Phi_2(p)$

We can easily check that all $\Phi_2(p)^2, \Phi_2(p)^2, \Phi_3(p)$ and $\Phi_6(p)$ are pairwise relatively prime. Note that $\Phi_3(p)$ and $\Phi_6(p)$ are also odd. Hence, by Lagrange's theorem, t is contained in $SU_3(p).2$ and in no other maximal subgroups labeled (1)-(4). But u cannot be contained in $SU_3(p).2$. Thus, if u and t are contained in a maximal subgroup, this must be one among the groups labeled (5)-(9) $\square$

2 Algebraic Number Theory

In this section we will study some notions from algebraic number theory and Galois theory. Our goal is to set up the theory in sufficient generality so that we can work with it later. There is a section on the Galois group associated to palindromic polynomials which is of particular importance for the main theorem. We must mention that many of the topics covered are well known, so we will not get into much detail. However, we encourage the reader to also read up on Algebraic Number Theory from Neukirch's book [20].

2.1 Profinite groups

As we shall see later on, the Galois group of an infinite Galois extension E/F is a profinite group. Thus in this section, we cover some generalities of profinite groups. which will be applied to infinite Galois theory.

Definition 2.1. A group (G, m) is called a topological group if the underlying set G is equipped with the structure of a topological space such that the multiplication map $m : G \times G \to G, (g, h) \to g \cdot h$ and the inversion map $G \to G, g \to g^{-1}$ are continuous.

Remark 2.1. *Equivalently a topological group is a group object in the category of topological spaces.*

Example 2.1. The following groups are all topological groups (for their obvious topology):

- $(\mathbb{R}^n, +)$, $(\mathbb{C}^n, +)$, $(\mathbb{R}^*, \times)$, $(\mathbb{R}_{>0}, \times)$, $(GL_n(\mathbb{R}), \times)$, $(GL_n(\mathbb{C}), \times)$.
- Any finite group for the discrete topology.

Proposition 2.1. *Let G be a topological group. The following conditions are equivalent:*

1. *G is a projective limit of finite discrete groups.*

2. *The topological space underlying to G is Hausdorff, totally disconnected and compact.*

3. *The identity element $e \in G$ has a basis of open neighborhoods which are open subgroups of finite index in G.*

If they are satisfied, we call the G a profinite group. (We will consider any as the definitions of profinite group)

Proof. [13], Chapter 6, Proposition 2.8.

Example 2.2. The following are profinite groups:

- $\mathbb{Z}_p$ the additive group of p-adic integers.
- The group of profinite integers $\hat{\mathbb{Z}} = \varprojlim_{n \in \mathbb{Z} \geqslant 1} \mathbb{Z}/n\mathbb{Z}$.

  By the Chinese remainder theorem the mapping $\hat{\mathbb{Z}} \xrightarrow{\sim} \prod_p \mathbb{Z}_p$, given by

$$(x_n)_{n \geqslant 1} \to \prod_{p\, prime} (x_{p^n})_{n \geqslant 1}$$

  is an isomorphism

Definition 2.2. Let G be a totally disconnected locally compact topological group, then G is called locally profinite. Equivalently, a topological group is locally profinite if and only if there exists an open profinite subgroup $K \subset G$.

Proof: [6] Chapter 5, Section 1.4 Theorem 1.

Example 2.3. The following are examples of locally profinite groups:

- $\mathbb{Q}_p$, the field of p-adic numbers, with open profinite subgroup $\mathbb{Z}_p \subset \mathbb{Q}_p$.
- $GL_n(\mathbb{Q}_p)$, with $GL_n(\mathbb{Z}_p)$ as profinite open subgroup. These groups, as we will see, play an important role in describing the prime factor components of automorphic representations.

2.2 Infinite algebraic extensions

In this section we consider infinite Galois extensions. The usual Galois correspondence between subgroups of Galois groups of finite Galois extensions and intermediate fields is not valid for infinite Galois extensions.

Example 2.4. Let $\mathbb{F}_p$, be the field of p elements, p prime, and let $G = \mathrm{Gal}(\bar{\mathbb{F}}_p/\mathbb{F}_p)$ be its absolute Galois group (see section 2.3). Then G contains Fr_p, the Frobenius automorphism. Let $H = \langle Fr_p \rangle$, we claim that there is no intermediate field K such that $H = \mathrm{Gal}(\bar{\mathbb{F}}_p/K)$. Indeed, we know $H \neq G$ because Fr_p generates the cyclic dense subgroup $\mathbb{Z}$ inside $\bar{\mathbb{Z}}$ but the fixed fields of H and G are the same, namely $\mathbb{F}_p$.

The Galois theory of field extensions of infinite degree gives rise naturally to Galois groups that are profinite. Specifically, if L/K is a Galois extension, we consider the group $G = Gal(L/K)$ consisting of all field automorphisms of L which keep all elements of K fixed. This group is the inverse limit of the finite groups $Gal(F/K)$, where F ranges over all intermediate fields such that F/K is a finite Galois extension. For the limit process, we use the restriction homomorphisms $Gal(F_1/K) \to Gal(F_2/K)$, where $F_2 \subset F_1$. The topology we obtain on $Gal(L/K)$ is known as the Krull topology.

We have an analogous of the correspondence theorem for infinite Galois theory:

Theorem 2.1. *Let L/K be a (finite or infinite) Galois extension with Galois group G.*

1. *G is profinite.*
2. *The map $M \to Gal(L/K)$ is an inclusion-reversing bijection between the intermediate fields of L/K and the closed subgroups of G with the inverse map given by $H \to E^H$.*
3. *For any intermediate field M of L/K, M/K is finite if and only if $Gal(L/M)$ is an open subgroup of G.*
4. *If M/K is a normal sub-extension of L/K, then the restriction map $Gal(L/K) \to Gal(M/K)$ gives rise to the following isomorphism of topological groups:*

$$Gal(L/K)/Gal(L/M) \cong Gal(M/K).$$

Proof. [13], Chapter 6, Theorem 6.2.

Let K be any (not necessarily finite) algebraic extension of $\mathbb{Q}$. As in the case where K is a number field, we define the ring of integers $\mathcal{O}_K$ as the ring of elements $x \in K$ that are integral over $\mathbb{Q}$. If K is infinite over $\mathbb{Q}$, the ring $\mathcal{O}_K$ is not noetherian, and hence is not a Dedekind domain. In general, $\mathcal{O}_K$ equals the union of all rings $\mathcal{O}_L$, where L runs over the number fields contained in K, and hence is a 'limit' of Dedekind domains. By reducing to Galois theory on number fields, we can easily deduce the following lemma.

Lemma 2.1. *Let K be an algebraic extension of $\mathbb{Q}$, and M an algebraic extension of K.*

1. *For any prime ideal $\mathfrak{p}$ in $\mathcal{O}_K$ there exists a prime ideal $\mathfrak{P} \subset \mathcal{O}_M$ such that $\mathfrak{P} \cap \mathcal{O}_K = \mathfrak{p}$.*
2. *Let $\mathfrak{p}$ be a non-zero prime ideal of $\mathcal{O}_K$ above the prime number p. $\mathcal{O}_K/\mathfrak{p}$ is an algebraic extension of F_p.*
3. *If M/K is a Galois extension, then the action of the Galois group $G = Gal(M/K)$ on the set of primes of M lying above a prime p of K is transitive.*

Remark 2.2. *In contrast to the finite case, unique factorization of ideals fails for infinite algebraic extensions of $\mathbb{Q}$.*

2.3 Absolute Galois group

Definition 2.3. Let F be a field and $\bar{F}$ a separable algebraic closure of F, we call $G_F := Gal(\bar{F}/F)$ the absolute Galois group of F.

On G_F a system of neighborhoods around 1 is given by $\{Gal(\bar{K}/L)\}_L$ as L runs over all Galois extensions of K in $\bar{K}$

Example 2.5. The following are examples of Absolute Galois groups:

1. The absolute Galois group of an algebraically closed field is trivial.

2. The absolute Galois group of $\mathbb{R}$ is a cyclic group of two elements (complex conjugation and the identity map), since $\mathbb{C}$ is the separable closure of $\mathbb{R}$ and $[\mathbb{C} : \mathbb{R}] = 2$.

3. The absolute Galois group of a finite field k is isomorphic to the group $\hat{\mathbb{Z}}$. This will be explained in more detail later.

Remark 2.3. *No direct description is known for the absolute Galois group of the rational numbers $\mathbb{Q}$. A major goal of number theory is to understand this absolute Galois group. Understanding this group would help to answer questions like the inverse Galois problem.*

Absolute galois group of a finite field

Consider the finite field $\mathbb{F}_q$ of $q = p^r$ elements. The algebraic closure of $\mathbb{F}_q$ is the union $\bigcup_{n=1}^{\infty} \mathbb{F}_{q^n}$. We study the Absolute Galois group $Gal(\bar{\mathbb{F}}_q/\mathbb{F}_q)$.

Proposition 2.2.

$$Gal(\bar{\mathbb{F}}_q/\mathbb{F}_q) \cong \varprojlim_{i \geqslant 1} Gal(\mathbb{F}_{q^i}/\mathbb{F}_q) \cong \hat{\mathbb{Z}}$$

.

Proof: The Frobenius automorphism: $Fr_q : x \to x^q$, allows us to identify $\hat{\mathbb{Z}}$ with $Gal(\bar{\mathbb{F}}_q/\mathbb{F}_q)$ via the isomorphism $x \to Fr_q^x$, where Fr_q^x is as follows: note that any $t \in \bar{\mathbb{F}}_q$ actually lies in a finite extension $\mathbb{F}_q^n \subset \bar{\mathbb{F}}_q$ for $N \in \mathbb{Z}_{\geqslant 1}$ sufficiently large. Then for $x = (x_n)_n \in \hat{\mathbb{Z}}$, the power Fr_q^x acts on t as $Fr_q^{x_N}$, which by the divisibility relations does not depend on the choice of N. □

Definition 2.4. A topological generator of a topological group G is just an element that generates a dense subgroup of G.

The frobenius is a topological generator of $Gal(\bar{\mathbb{F}}_q/\mathbb{F}_q)$ as it generates the cyclic dense subgroup $\mathbb{Z}$ inside $\hat{\mathbb{Z}}$. If you think of $\hat{\mathbb{Z}}$ as the direct product $\prod_p \mathbb{Z}_p$, then the Frobenius can be thought of as the ∞-tuple $(1, 1, 1, \cdots)$ all componentes being 1. In fact, any (multiplicative) unit of $\mathbb{Z}_p$ is a topological generator of the additive group $\mathbb{Z}_p$.

2.4 Frobenius elements

Let K be a number field. Recall that the places of K are either finite, corresponding to the prime ideals of K, or infinite, corresponding to embeddings $K \to \mathbb{C}$ up to complex conjugation. If v is a place of K, and K_v the corresponding completion of K, then K_v is a finite extension of $\mathbb{Q}_p$, for some prime number p, is v is finite, and $\mathbb{R}$ or $\mathbb{C}$ if v is infinite. We let k_v denote the corresponding residue field for the place v of K.

Whenever L/K is Galois, Lemma 2.1 implies that $Gal(L/K)$ acts transitively on the places of L extending v. We define $D_w = \{\sigma \in Gal(L/K) | \sigma w = w\}$ called the decomposition group of w, it is well known that $D_w = Gal(L_w/K_v)$ and that if w, w' extend v then D_w and $D_{w'}$ are conjugate subgroups of $Gal(L/K)$.

The projective system for the absolute Galois group G_K is given by the restriction maps $Gal(\bar{K}/K) \to Gal(L/K)$, where L runs over the Galois extension of K inside $\bar{K}$. If we fix a place v of K. For each Galois extension L of K, we can choose a compatible sequence of places $w|v$, consider the inclusion $D_w \to Gal(L/K)$, and take limits to get the map $\iota_v : G_{K_v} \to G_K$ (note that any finite extension of K_v is L_w for some w).

This map will be important as we can study G_K by studying its representations and how they restrict to G_{K_v}. Nevertheless, the map is not well-defined since we chose particular w's, however, it is well-defined up to conjugacy.

Whenever $w|v$, there is a surjective continuous group homomorphism $r : D_w \to Gal(k(w)/k(v))$. topologically generated by the Frobenius element Fr_v. The kernel of r is called the inertia group of w over v.

Definition 2.5. Any element in $D_w \subset Gal(L/K)$ mapping to Fr_v is called a Frobenius element at w and denoted by Fr_w.

Let v be a place of K such that the extension L/K is unramified at v. Then any place w of L lying over v determines a unique element $Fr_w \in Gal(L/F)$. Any other prime of L over v has the form σw with $\sigma \in Gal(L/K)$, and we have $D_{\sigma w} = \sigma D_w \sigma^{-1}$

and $Fr_{\sigma w} = \sigma Fr_w \sigma^{-1}$. Thus, the set of all Fr_w with w a place of L over v is a conjugacy class in $Gal(L/K)$, called the Frobenius conjugacy class at v. If there is no confusion, any element of this conjugacy class is denoted by Fr_v.

If we consider the exact sequences associated with the decomposition groups, then taking limits, for each finite place v, we get an exact sequence

$$0 \to I_v \to G_{K_v} \to \langle Fr_v \rangle \to 0$$

Definition 2.6. Let K be a number field, S a finite set of finite places of K. Then we define $G_{K,S}$ as the quotient of G_K by the smallest closed normal subgroup of G_K containing all inertia groups I_v for v finite, $v \notin S$. Note that normality of the subgroup both ensures that the quotient is a group and makes irrelevant the fact that the map $G_{K_v} \to G_K$ is only defined up to conjugacy.

If v is a finite place of K, then we have a composite map

$$\iota_v : G_{K_v} \to G_K \to G_{K,S}$$

Clearly for $v \notin S$, we have $\iota_v(I_v) = 1$ and thus $\iota_v : \langle Fr_v \rangle \to G_{K,S}$ is well-defined up to conjugacy class. The image of Fr_v under this map is also called Fr_v.

2.5 Chebotarev's density theorem

Definition 2.7. Let K be a number field, and let P be the set of prime ideals corresponding to the places of K. For any subset $S \subset P$, the natural density of S is defined by the following limit (provided it exists):

$$d_0(S) = \lim_{x\to\infty} \frac{\#\{\mathfrak{p} \in S | N(\mathfrak{p}) \leqslant x\}}{\#\{\mathfrak{p} \in P | N(\mathfrak{p}) \leqslant x\}}.$$

Definition 2.8. The Dirichlet density of S is defined by

$$d(S) = \lim_{s\to 1} \frac{\sum_{\mathfrak{p}\in S} N(\mathfrak{p})^{-s}}{\sum_{\mathfrak{p}\in P} N(\mathfrak{p})^{-s}},$$

where the limit is taken over positive real numbers s tending to 1 from above.

Theorem 2.2. *Let K be a number field, and let L be a finite Galois extension of K. Let X be a subset of $G = Gal(L/K)$ that is stable under conjugation. The set of places v of K that are unramified in L and whose associated Frobenius conjugacy class Fr_v is contained in X has natural density $\frac{\#X}{\#G}$.*

Proof: ([19], Chapter V, Theorem 6.4.)

There is also a version for infinite extensions.

Theorem 2.3. *Let K be a number field, and let L be a (possibly infinite) Galois extension of K that is unramified outside a finite set S of places of K. In this case, the Galois group G of L/K is a profinite group equipped with the Krull topology. Since G is compact in this topology, there is a unique Haar measure μ on G. Let X be a subset of G that is stable under conjugation and whose boundary has measure* 0 *Then, the set of primes v of K not in S such that $Fr_v \subset X$ has natural density $\frac{\mu(X)}{\mu(G)}$.*

Corollary 2.1. *The conjugacy classes of the Fr_v for $v \notin S$ are dense in $G_{K,S}$.*

Proof. This is a consequence of Cebotarev density theorem. The open normal subgroups of finite index form a basis for the topology of $G_{K,S}$ at the identity. If $\sigma \in G_{K,S}$, then a basis of neighborhoods of σ is the set of σU for U a finite index open normal subgroup of $G_{K,S}$. So it is enough to prove that each σU contains a conjugate of some Fr_v for $v \notin S$. For each U, let K_U to be the extension of K inside $\bar{K}$ (a fixed separable closure) that is fixed by U; which is Galois since U is normal, and $G_{K,S}/U = Gal(K_U/K)$. Given $\sigma U \in Gal(K_U/K)$, Chebotarev's theorem implies that there is some $v \notin S$ such that $Fr_v \in Gal(K_U/K)$ is conjugate to σU, thus, some conjugate of Fr_v is in σU, in $G_{K,S}$.

2.6 Adeles

Let K be a number field. We introduce the adele ring of K. It is a topological ring $\mathbb{A}_K$, that admits every completion K_v as a quotient, but behaves better than the product

$\prod_v K_v$ of topological rings. For example, $\mathbb{A}_F$ is locally compact, while $\prod_v F_v$ is not. $\mathbb{A}_F^\times$ is a central object in class field theory. Moreover its generalisations $GL_n(\mathbb{A}_F)$ are central objects in the theory of automorphic forms.

First we assume $K = \mathbb{Q}$. We define the ring of finite adeles $\mathbb{A}^f = \mathbb{A}_{\mathbb{Q}}^f$ as the tensor product $\mathbb{Q} \otimes_{\mathbb{Z}} \hat{\mathbb{Z}}$, where we view $\mathbb{Q}$ and $\hat{\mathbb{Z}}$ as $\mathbb{Z}$-modules. $\mathbb{A}^f$ inherits a multiplication map, given explicitly by

$$(\sum_{i=1}^{n} q_i \otimes z_i) \cdot (\sum_{j=1}^{m} q'_j \otimes z'_j) = \sum_{i,j} q_i q'_j \otimes z_i z'_j$$

for all $\sum_{i=1}^{n} q_i \otimes z_i$ and $\sum_{j=1}^{m} q'_j \otimes z'_j$ in $\mathbb{A}^f$.

The ring $\mathbb{A}^f$ is equipped with the strongest topology such that the map

$$\mathbb{Q} \times \hat{\mathbb{Z}} \to \mathbb{A}^f,\ (x, z) \to x + z$$

is continuous, where $\mathbb{Q}$ is given the discrete topology. The subsets of the form $U_{x,y} = x \cdot \hat{\mathbb{Z}} + y \subset \mathbb{A}^f$ with $x \in \mathbb{Q}^\times$ and $y \in \mathbb{Q}$ form a basis for the topology on $\mathbb{A}^f$. This definition implies that $\mathbb{A}^f$ is a locally profinite topological ring containing $\hat{\mathbb{Z}}$ as an open subring.

Definition 2.9. The adele ring $\mathbb{A} = \mathbb{A}_{\mathbb{Q}}$ is the product ring $\mathbb{A}^f \times \mathbb{R}$, equipped with the product topology

The ring $\mathbb{A}$ is often introduced as a "restricted product" ranging over all prime numbers p, of the fields $\mathbb{Q}_p$ with respect to the subrings $\mathbb{Z}_p \subset \mathbb{Q}_p$.

$$\mathbb{A}^f = \prod_{p\,prime}{}' (\mathbb{Q}_p, \mathbb{Z}_p) = \{(\alpha_p)_p \in \prod_{p\,prime} \mathbb{Q}_p : \text{ for almost all primes } p \text{ we have } \alpha_p \in \mathbb{Z}_p\}$$

A basis for the topology on the restricted product is given by the sets

$$U_{x,y} = \{(\alpha_p) \in \mathbb{A}^f | v_p(\alpha_p - y) \geqslant v_p(x)\}$$

with $x \in \mathbb{Q}^\times$ and $y \in \mathbb{Q}$. The full adele ring is obtained from $\mathbb{A}^f$ by also attaching a component for the infinite place.

As a restricted product, we have

$$\mathbb{A}_{\mathbb{Q}} = \prod_{\mathbb{Q}-\text{places } v}{}^{\prime} (\mathbb{Q}_v, \mathbb{Z}_v)$$

where for v the infinity place, we take by definition $\mathbb{Z}_v = \mathbb{Q}_v = \mathbb{R}$.

More generally, if F is a number field, in the same way as for the adele ring of $\mathbb{Q}$, we can write $\mathbb{A}_F$ as a restricted direct product:

$$\mathbb{A}_{\mathbb{F}} = \prod_{\mathbb{F}-\text{places } v}{}^{\prime} (F_v, \mathcal{O}_{F_v})$$

.

2.7 Galois theory of palindromic polynomials

In this section we study the Galois group associated to a palindromic polynomial. These often come into play when dealing with G_2.

Assume that K is a field of characteristic 0. Let $P(x) \in K[x]$ be an irreducible palindromic polynomial of degree $2n$. Let $P(x) = x^{2n}P(\frac{1}{x})$. Thus the roots of $P(x)$ come in pairs. Let $x_1^{\pm 1}, x_2^{\pm 1}, \ldots, x_n^{\pm 1}$ be the roots of $P(x)$. Let

$$P(x) = a_{2n}x^{2n} + \ldots + a_1 x + a_0 \text{ such that } a_{2n-i} = a_i.$$

Then we can write

$$x^{-n}P(x) = b_n(x^n + x^{-n}) + \ldots + b_1(x^1 + x^{-1}) + b_0, \text{ where } b_{n-i} = a_i = a_{2n-i}.$$

Now both sets

$$\{x^n + x^{-n}, \ldots, x + x^{-1}, 1\} \text{ and } \{(x + x^{-1})^n, \ldots, x + x^{-1}, 1\}$$

generate the same space over K thus we can write

$$x^{-n}P(x) = c_n(x + x^{-1})^n + \ldots + c_1(x + x^{-1})^1 + c_0 \text{ for some } c_n, \ldots, c_0.$$

We get $x^{-n}P(x) = Q(y)$ where Q is a polynomial of degree n in $y = x + x^{-1}$.

Definition 2.10. For any palindromic polynomial $P(x)$ of even degree, and $Q(y)$ as above, we call $Q(y)$ the palindromic reduction of $P(x)$.

If $y_1, \ldots, y_n$ are the roots of $Q(y)$ then the roots of $P(x)$ are found by solving the equations $x + x^{-1} = y_i$ for $i = 1, 2, \cdots, n$. Let E, F be the splitting fields of $P(x)$ and $Q(y)$ respectively, then E/K and F/K are both Galois extensions. Let $\mathrm{Gal}(E/K)$ and $\mathrm{Gal}(F/K)$ be their Galois groups respectively.

$Gal(F/K)$ is a subgroup of S_n, where S_n is the group of permutations of $y_1, \ldots, y_n$ and $Gal(E/F)$ is a subgroup of C_2^n, the elementary 2-group of order 2^n which acts by permuting x_i and $1/x_i$. This implies $Gal(E/K)$ is contained in the semi-direct product $C_2^n \rtimes S_n$.

Let Δ be the discriminant of $Q(y)$. Let ϵ be the sign character of S_n. By restriction to $\mathrm{Gal}(F/K)$ and then inflation we can view ϵ as a character of $Gal(E/K)$.

Now let ϵ' be the character on $Gal(E/K)$ defined as follows: Let

$$\Delta' = \prod_{i=1}^{n} (x_i - x_i^{-1})^2$$

then for every $\sigma \in Gal(E/K)$, we define ϵ' such that $\sigma(\sqrt{\Delta'}) = \epsilon'(\sigma)\sqrt{\Delta'}$.

Note ϵ' takes only values ± 1. Moreover, if we restrict ϵ' to $Gal(E/F) \subset C_2^n$, we get $\epsilon'(a_1, \ldots, a_n) = a_1 \cdots a_n$ where $a_i \in C_2$. Also $(x_i - x_i^{-1})^2 = y_i^2 - 4$ so Δ' can easily be computed:

$$\Delta' = \prod_{i=1}^{n} (x_i - x_i^{-1})^2 = \prod_{i=1}^{n} (y_i^2 - 4) = Q(2)Q(-2)$$

Proposition 2.3. *Let $P(x) \in K[x]$ be a palindromic polynomial of degree $2n$. Let $Q(y)$ be the polynomial of degree n obtained by the palindromic reduction from $P(x)$. Let Δ be the discriminant of $Q(y)$. Then the polynomial $P(x)$ is separable if and only if $\Delta \neq 0$ and $\Delta' \neq 0$.*

Proof: The roots of $P(x)$ come in pairs (x_i, x_i^{-1}). If $P(x)$ is not separable then $x_i = x_i^{-1}$ for some i, which would imply $\Delta' = 0$ or $x_i = x_j$ (or x_j^{-1}) for some $i \neq j$, and thus $y_i = y_j$, implying $\Delta = 0$. $\square$

Corollary 2.2. *Let K be a number field. Let $\mathfrak{p}$ be a prime ideal of $\mathcal{O}_K$, such that $P(x) \in \mathcal{O}_{K,\mathfrak{p}}$. If Δ, Δ' are in $\mathcal{O}_{K,\mathfrak{p}}^{\times}$, then $P(x)$ is unramified at $\mathfrak{p}$*

Proof. This is just a consequence of the fact that a prime ideal is ramified if and only if the prime divides the discriminant. $\square$

Lemma 2.2. *K is a totally real field and all roots of $Q(y)$ lie in the interval $(-2, 2)$ if and only if, the roots of $P(x)$ are pairs of complex conjugates on the unit circle.*

Proof: Suppose all roots of $P(x)$ are pairs of complex conjugates on the unit circle. The equality $y_i = x_i + x_i^{-1}$ between the roots mentioned at the beginning of this section shows that if $x_i = \cos(\theta) + i\mathrm{sen}(\theta)$ then $y_i = 2\cos(\theta)$ lies in the interval $(-2, 2)$. On the other hand if y_i is in the interval $(-2, 2)$ then $y_i = 2\cos(\theta)$ for some θ and the equation $y_i = x + x^{-1}$ is satisfied by both $\cos(\theta) + i\mathrm{sen}(\theta)$ and $\cos(\theta) - i\mathrm{sen}(\theta)$. $\square$

Remark 2.4. *When K is a totally real field. Complex conjugation, given by the element $c = (-1, -1, \ldots, -1) \in C_2^n$ is in the center of $Gal(E/K)$.*

Proposition 2.4. *Assume that K is a totally real field, that the Galois group of $Q(y)$ is S_n, and that the roots of $Q(y)$ are all in the interval $(-2, 2)$. Assume that Δ' is not a square in K and $K(\sqrt{\Delta'}) \neq K(\sqrt{\Delta})$. Then the Galois group of $P(x)$ is isomorphic to the semi-direct product of C_2^n and S_n or if n is odd, to the direct product $\langle c \rangle \times S_n$ where c corresponds to the complex conjugation.*

Proof: As before, we let E and F be the splitting fields of $P(x)$ and $Q(y)$, respectively. Now, since Δ' is not a square, the character ϵ' of $\mathrm{Gal}(E/K)$ is non-trivial. If the restriction of ϵ' to $\mathrm{Gal}(E/F)$ is trivial, then it induces a non-trivial character of $\mathrm{Gal}(F/K) = S_n$. But the unique non-trivial character of S_n is ϵ, thus $\epsilon' = \epsilon$, which would contradict $K(\sqrt{\Delta'}) \neq K(\sqrt{\Delta})$. Thus there is $(a_1, a_2, \ldots, a_n) \in \mathrm{Gal}(E/F) \subset C_2^n$ such that $\epsilon'(a_1, a_2, \ldots, a_n) = -1$.

Note that C_2^n is S_n-generated by any element outside the kernel of ϵ' except when n is odd and the element is c. Thus either $\mathrm{Gal}(E/F) = C_2^n$ and $\mathrm{Gal}(E/K)$ is isomorphic to the semi-direct product of C_2^n and S_n or $\mathrm{Gal}(E/K)$ is the extension of S_n by $\langle c \rangle$, which would have to split, as given by ϵ'. $\square$

Let $P_i(x) \in K[x], i = 1, 2$ be two palindromic polynomials satisfying the conditions of Proposition 2.3, and let Δ_i, Δ_i', be the two discriminants discussed before.

Corollary 2.3. *Let E_1 and E_2, be the splitting fields of $P_1(x)$ and $P_2(x)$, respectively. Then E_1 and E_2 are linearly independent over K if and only if the bi-quadratic fields $K(\sqrt{\Delta_1}, \sqrt{\Delta_1'})$ and $K(\sqrt{\Delta_2}, \sqrt{\Delta_2'})$ are.*

Proof: Since E_1 and E_2 are Galois, it is enough to show that $E_1 \cap E_2 = K$. Note that $E_1 \cap E_2$ is Galois in both E_1 and E_2. One easily sees that any non-trivial normal subgroup of the semi-direct product of C_2^n and S_n (and of $\langle c \rangle \times S_n$) is contained in a kernel of one of the three characters: ϵ, ϵ' and $\epsilon\epsilon'$. Thus if $E_1 \cap E_2$ is strictly bigger than K, it must contain a quadratic field common to $K(\sqrt{\Delta_1}, \sqrt{\Delta_1'})$ and $K(\sqrt{\Delta_2}, \sqrt{\Delta_2'})$ $\square+$

Corollary 2.4. *Assume that $n = 3, P(x)$ satisfies the conditions of Proposition 2.3, and that the roots $x_1^{\pm 1}, x_2^{\pm 1}, x_3^{\pm 1}$ of $P(x)$ satisfy $x_1 x_2 x_3 = 1$. Then the Galois group of $P(x)$ is isomorphic to $\langle c \rangle \times S_3 \equiv D_6$, the dihedral group of order* 12.

Proof: According to Proposition 2.3 there are two possibilities. Since there is a relation between the roots, the degree of E cannot be 48. Thus the Galois group must be $\langle c \rangle \times S_3 \equiv D_6$. $\square$

3 Algebraic Groups

The main porpuse of this chapter is to develop a notion of reduction mod $\mathfrak{p}$ of rational conjugacy classes. We will do this in a generality of split reductive groups. We assume however that the reader is familiar with the theory of Algebraic Groups. We encourage the interested reader to also read up on Milne's book [18], for a more detailed content than the presented here. We will also include some remarks concerning the group G_2 of particular importance for the proof of our main theorem in the final chapter.

3.1 Rational semi-simple conjugacy classes

In this section we characterize strongly regular K-rational conjugacy classes.

Let K denote any field and K_s a separable closure of K. Let G be a connected reductive group split over K, and fix a faithful algebraic representation (ρ, V) of G. Let T be a maximal split torus of G, defined over K.

Definition 3.1. Any rational representation over K of an K-split torus is a direct sum of one dimensional representations over K in each of which an element $t \in T$ acts as multiplication by $\chi(t)$, where χ is a character of T. The characters so obtained are the weights (of T in V), and the non-zero subspaces

$$V_\chi = \{v \in V : \rho(t)v = \chi(t)v$$

for all $t \in T\}$ are the weight spaces.

Let $\{\chi_i\}$ be the multi-set of weights of V where every weight χ_i appears with multiplicity $\dim(V_{\chi_i})$. Now, consider $g \in G(K_s)$ a semi-simple element, and let $R_g(x) \in K_s[x]$ denote the characteristic polynomial of g acting on $V \otimes_K K_s$. The eigenvalues of the endomorphism corresponding to an element $t \in T$ are precisely the $\chi_i(t)$. Hence the characteristic polynomial for every $t \in T(K_s)$ is:

$$R_t(x) = \prod_{i=1}^{n}(x - \chi_i(t))$$

where $\dim(V) = n$. If n_0 is the dimension of the trivial weight space. We can write

$$R_t(x) = P_t(x)(x-1)^{n_0}.$$

Now as G is connected, every semi-simple element is contained in a maximal torus, and as any two maximal torus are conjugates, then any semi-simple element g is conjugated to an element in $T(K_s)$, thus the polynomial $P_g(x)$ is well defined for any semi-simple element and it is an invariant of the conjugacy class $C(K_s)$ of g (the characteristic polynomial is invariant under conjugation). Hence we can also write $P_C(x) = P_g(x)$.

Definition 3.2. We call a class C as above K-rational if $\sigma(C) = C$ for all σ in $Gal(K_s/K)$.

Lemma 3.1. *If the class C is K-rational then $P_C(x) \in K[x]$:*

Proof: C is a conjugacy class of a semi-simple element $g \in G(K_s)$ thus $P_C(x) = P_g(x) = P_t(x)$ for some $t \in T(K_s)$. When applying one of the embeddings σ in $\mathrm{Gal}(K_s/K)$ to t, as C is K-rational, we get $\sigma(t) \in C \cap T(K_s)$. Moreover we notice that:

$$P_{\sigma(t)}(x) = \prod_{\chi \neq 1}(x - \chi(\sigma(t))) = \prod_{\chi \neq 1}(x - \sigma(\chi(t))) \text{ and } P_t(x) = \prod_{\chi \neq 1}(x - \chi(t)).$$

$P_{\sigma(t)}(x)$ and $P_t(x)$ must coincide, which means that after applying σ to the coefficients of P, they remain the same. Thus, all the coefficients are in K and we conclude $P_C(x) \in K[x]$. □

Definition 3.3. Let $t \in C(K_s) \cap T(K_s)$. We say that t is strongly regular if the centralizer of t in $G(K_s)$ is $T(K_s)$, i.e. $\{x \in G(K_s) | xtx^{-1} = t\} = T(K_s)$.

If t is strongly regular then we can call C strongly regular as any element on C would be strongly regular.

Lemma 3.2. *If $t \in C \cap T(K_s)$ is strongly regular then any element in $C \cap T(K_s)$ is a conjugate of t by a unique element in the Weyl group W.*

Proof: First note that, as t is strongly regular, if we conjugate t by any representative in $N(T)$ of the same class in W, we get the same element. Indeed, for any $t_0 \in T(K_s)$, $(gt_0)t(gt_0)^{-1} = gtg^{-1}$. Now suppose there are two elements $g, h \in N(T)$ such that $gtg^{-1} = hth^{-1}$ this implies $(h^{-1}g)t = t(h^{-1}g)$ but t is strongly regular which means $h^{-1}g \in T(K_s)$, this means they both belong to the same class of equivalence in the Weyl Group, which proves the uniqueness. Now if we let $t_0 \in C \cap T(K_s)$ then as it is in the same class as t there should be some $g \in G$ such that $gt_0g^{-1} = t$. Now $t_0 = g^{-1}tg \in T(K_s)$ and

$$Z(T(K_s)) = T(K_s) \implies T(K_s) \subset Z(g^{-1}tg) = g^{-1}Z(t)g = g^{-1}T(K_s)g.$$

Since $T(K_s)$ is a maximal torus it follows that $T(K_s) = g^{-1}T(K_s)g \implies g \in N(T(K_s))$. $\square$

Lemma 3.3. *If C is a K-rational conjugacy class. Then $C \cap T(K_s)$ is $Gal(K_s/K)$-stable*

Proof: This follows, from the fact that T is a K-split maximal torus and that C is K-rational. For any $\sigma \in \mathrm{Gal}(K_s/K)$, when applied to $T(K_s)$ and $C(K_s)$, σ preserves each of them so for all $\sigma \in \mathrm{Gal}(K_s/K)$, $\sigma(C \cap T(K_s)) = C \cap T(K_s)$. $\square$

We can conlude that for every $\sigma \in Gal(K_s/K)$ there exists a unique element $w \in W$ such that $\sigma(t) = t^w$. Moreover to the K-rational conjugacy class C of strongly regular elements we can assigned a homomorphism

$$\phi_C : Gal(K_s/K) \to W$$

unique up to conjugation by W.

Remark 3.1. *The map above depends on the choice of a strongly regular element t. So different choices differ by conjugations on W.*

Let $E = E_C$ be the finite field extension of K corresponding to the kernel of ϕ_C, i.e. $E_C = \{x \in K_s |\ \sigma(x) = x \ for\ all\ \sigma\ such\ that\ \sigma(t) = t\}$

Proposition 3.1. *Let C be a strongly regular and K-rational conjugacy class. The field E_C is the splitting field of the polynomial $P_C(x)$.*

Proof: Since $R_C(x) = \Pi_{i=1}^{n}(x - \chi_i(t))$ is clearly determined by the $\chi_i(t)$ and t is also determined by the values $\chi_i(t) \in K_s^\times$ (as the representation (ρ, V) is faithful), the subgroup of $Gal(K_s/K)$ fixing the splitting field of $R_C(x)$ (= the splitting field of $P_C(x)$) is indeed the kernel of ϕ_C as if σ preserves t it preserves all the $\chi_i(t)$ and conversely. □

Remark 3.2. *If G is simply connected, such as the exceptional G_2, then regular semi-simple elements are strongly regular. ([24], 2.14)*

3.2 Finite tori

In this section we study the split torus in a split reductive group over a finite field. We assume that k is a finite field of order q. Then $k_s = \bar{k}$ and $Gal(\bar{k}/k)$ is generated (topologically) by Fr_q. Let T be the maximal split torus contained in the split reductive group as in the previous section, this time defined over k.

Theorem 3.1. *[Lang-Steinberg] if G is a connected smooth algebraic group over k, then if $Fr_q : G \to G$, $x \mapsto x^q$ is the Frobenius, the morphism of varieties: $G \to G$ given by $x \mapsto x^{-1}Fr_q(x)$ is surjective.*

Proof. A quick proof is presented in [8].

Let W be the Weyl group, and take any $w \in W$, then let $n \in N(T(\bar{k}))$ be any representative of w in the normalizer. By the previous theorem, there exists $g \in G$ such that $n = g^{-1}Fr_q(g)$. Let $T^g(\bar{k}) = gT(\bar{k})g^{-1}$ and $T^g(k)$ be the set

$$\{gtg^{-1} : t \in T(\bar{k}) \text{ such that } Fr_q(gtg^{-1}) = gtg^{-1}\} = \{gtg^{-1} : t \in T(\bar{k}) \text{ such that } n^{-1}tn = Fr_q(t)\}.$$

Then the map $H : T(\bar{k}) \to T^g(\bar{k})$, such that $t \to gtg^{-1}$ induces a group isomorphism

$$\{t \in T(\bar{k}) : n^{-1}tn = Fr_q(t)\} \to T^g(k)$$

Notice that the left hand side of this isomorphism does not depend on g or n, just the class on the Weyl group, where n belongs.

Definition 3.4. Let W be the Weyl group. For every $w \in W$ let $T_w(k) \subset T(\bar{k})$ be the group of k-points in a torus T_w, but the action of Fr_q is twisted by w^{-1}. Explicitly $T_w(k) = \{t \in T(\bar{k}) : n^{-1}tn = Fr_q(t)\} = \{t \in T(\bar{k}) : w^{-1}(t) = Fr_q(t)\}$.

Remark 3.3. *A priori T^g is defined over $\bar{k}$ only, but*

$$Fr_q(T^g) = Fr_q(g)Fr_q(T)Fr_q(g^{-1}) = Fr_q(T)^{Fr_q(g)} = T^{Fr_q(g)}.$$

Thus $Fr_q(T^g) = T^g$ if and only if

$$gFr_q(T)g^{-1} = Fr_q(g)TFr_q(g^{-1})$$

which is equivalent to $g^{-1}Fr_q(g) = n \in N(T)$, so it is defined also over k.

Proposition 3.2. *Let X be the lattice of characters of T, and $A = X \otimes_{\mathbb{Z}} \mathbb{R}$. Let Φ_w be the characteristic polynomial of w acting on A. Then $|T_w(k)| = \Phi_w(q)$.*

Proof: Let X_0, Y_0 be the group of characters and co-characters of $T(\bar{k})$. We choose for w, one possible g as in Theorem 3.1. Let X_1, Y_1 be the group of characters and co-characters of $T^g(\bar{k})$. Then X_0 and X_1 (resp Y_0 and Y_1) are related by conjugation. We must calculate $|\{t \in T(\bar{k}) : t = nFr_q(t)n^{-1}\}| = |T^g(k)|$.

From ([23], Prop 3.2.2) we can relate $T^g(k)$ and $Y_1/(Fr_q - 1)Y_1$. Also by applying the conjugation relating Y_0 and Y_1 we have:

$$T^g(k) \cong Y_1/(Fr_q - 1)Y_1 \cong Y_0/(w^{-1} \circ Fr_q - 1)Y_0.$$

Arguing as in the structure theorem of a finite free module over a PID

$$|T^g(k)| = |Y_0/(w^{-1} \circ Fr_q - 1)Y_0| = |det_A(w^{-1} \circ Fr_q - 1)|$$

Moreover $Fr_q(\chi)(t) = \chi(Fr_q(t)) = \chi(t^q) = q\chi(t)$ and $|det(w^{-1})| = 1$ implies

$$|det_A(w^{-1} \circ Fr_q - 1)| = |det_A(w^{-1} \circ (q \cdot 1 - w))| = |det_A(q \cdot 1 - w)|$$

We show finally that the determinant on the left is positive. The linear transformation $(q \cdot 1 - w)$ is a real transformation and so its eigenvalues will either be real or occur in complex conjugate pairs. Let λ be a real eigenvalue corresponding to an eigenvector v. Then $(q \cdot 1 - w)(v) = \lambda v$ and so $(q - \lambda)(v) = w(v)$

The vector $w(v)$ has the same length as v and so $|q - \lambda| = 1$. Since $q > 1$ this implies that $\lambda > 0$. Thus all real eigenvalues are positive. It follows that the product of the eigenvalues is positive. Finally we conclude the formula $|T_w(k)| = \Phi_w(q)$. $\square$

Case G_2

Now we do the corresponding calculations for the case $G = G_2$. Recall that the Weyl group W for G_2, is the dihedral group D_6.

The conjugacy classes in D_6 are as the following:

C	1a	2a	2b	2c	3a	6a
$\|C\|$	1	3	3	1	2	2

where the number in the first row is the order of any element in the class and the number in the second row is the number of elements in the class.

(i) There is one trivial class 1a with only one element of order 1.

(ii) There are 3 classes of elements of order 2:

- The class of reflections about long roots, denoted by $2a$.
- The class of reflections about short roots is denoted $2b$.
- The class of the $180°$-rotation (-1) denoted by $2c$.

(iii) There is one class of elements of order 3, denoted $3a$, the $\pm 120°$-rotation.

(iv) There are two classes of elements of order 6, denoted $6a$, the $\pm 60°$-rotations.

Corollary 3.1. *The order of the corresponding tori for* G_2 *are:*

w	*1a*	*2a*	*2b*	*2c*	*3a*	*6a*
$\|T_w\|$	$(q-1)^2$	q^2-1	q^2-1	$(q+1)^2$	q^2+q+1	q^2-q+1

Proof: This table is easily deduced from Proposition 3.2 above, and the root system associated to G_2 as shown in Section 1.2.

3.3 Reduction mod $\mathfrak{p}$ of conjugacy classes

In this section we deal with number fields, and define and characterize reduction mod $\mathfrak{p}$ of elements and conjugacy classes, where $\mathfrak{p}$ is a prime ideal of the corresponding ring of integers.

Let K be a number field and A its ring of integers. As before we assume G is a connected reductive group split over K. Let $L \subset V$ be a Chevalley-Steinberg A-lattice. This means that L is a direct sum of it weight components $L_\chi = L \cap V_\chi$, and that L is preserved by a Chevalley A-lattice in the derived subalgebra of the Lie algebra of G. This exists by ([16], Lemma 4.18) and defines a group scheme structure on G over A such that, for every ring R, $A \subset R \subset K_s$:

$$G(R) = \{g \in G(K_s) | g \cdot L \otimes_A R = L \otimes_A R\}.$$

Since L is a direct sum of the weigth components L_χ, we can characterize the group $T(R)$ as follows:

$$T(R) = \{t \in T(K_s) : \chi(t) \in R^\times \text{ for all weights } \chi \text{ of } V\}.$$

Consider E a finite Galois extension of K, with ring of integers B, let $\mathfrak{q}$ be any maximal ideal in B, with $k_\mathfrak{q}$ the corresponding residue field and let $B_\mathfrak{q}$ be the localization of B at $\mathfrak{q}$.

Definition 3.5. Any element $g \in G(B_\mathfrak{q})$ acts naturally on the quotient

$$L \otimes_A k_\mathfrak{q} = (L \otimes_A B)/(L \otimes_A \mathfrak{q})$$

as an element in $G(k_\mathfrak{q})$ denoted by $\bar{g}$ and is called the reduction of g modulo $\mathfrak{q}$.

For the reminder of this section we fix C, a strongly regular and K-rational conjugacy class. We recall that C is strongly regular if for every $t \in C \cap T(K_s)$. The centralizer of t in $G(K_s)$ is $T(K_s)$. Let $P_C(x)$ be the corresponding characteristic polynomial. Then by Lemma 3.1 $P_C(x) \in K[x]$.

Let E be the finite field extension of K corresponding to the kernel of the homomorphism $\phi_C : \mathrm{Gal}(K_s/K) \to W$ constructed by means of $t \in C \cap T(K_s)$, then by Proposition 3.1, we get $t \in T(E)$.

Now let B be the ring of integers in E, and let $S = S_C$ be the set of prime ideals of A such that:

(1) the field E is unramified outside S

(2) $P_C(x) \in A_{\mathfrak{p}}[x]$ for every $\mathfrak{p} \notin S$, where $A_{\mathfrak{p}}$ is the localization of A at $\mathfrak{p}$.

In particular the set S is finite since only a finite number of primes ramifies, and $P_C(x) \in A_{\mathfrak{p}}[x]$ for all but finitely many primes

Let $\mathfrak{q}$ be a prime in B such that $\mathfrak{p} = \mathfrak{q} \cap A \notin S$.

Since $P_C(x)$ is a monic polynomial and as B is the ring of integers in E, (2) implies that the roots of $P_C(x)$, that is the $\chi(t)$'s, are in $B_{\mathfrak{q}}$, the localization of B_q at $\mathfrak{q}$. Hence, $t \in T(B_{\mathfrak{q}})$ and $\bar{t} \in T(k_{\mathfrak{q}})$, thus the reduction of t modulo $\mathfrak{q}$ is well defined.

Also (1) implies that E is unramified at $\mathfrak{q}$, thus the inertia group $I(\mathfrak{q})$ is trivial and $D(\mathfrak{q}) \cong \mathrm{Gal}(B_{\mathfrak{q}}/A_{\mathfrak{p}})$ which is cyclic since it corresponds to an extension of finite fields, hence generated by the Frobenius Fr_q.

Proposition 3.3. *Assume $\mathfrak{q} \cap A \notin S$. Let $Fr_{\mathfrak{q}}$ be the Frobenius generator of the decomposition subgroup $D_{\mathfrak{q}} \subset Gal\ (E/K)$. Let $w = \phi_C(Fr_{\mathfrak{q}})$. The element $\bar{t}$ is contained in the finite torus $T_w(k_{\mathfrak{p}}) \subset T(k_{\mathfrak{q}}) \subset G(k_{\mathfrak{q}})$.*

Proof. This follows from the contruction. Let n be a representative of w in the Weyl group. The element $\bar{t}$ satisfies $n^{-1}tn = Fr_q(t)$ by definition of ϕ and w. $\square$

Proposition 3.4. *Let $\bar{k}_{\mathfrak{p}}$ be the algebraic closure of $k_{\mathfrak{p}}$, and chose an embedding of $k_{\mathfrak{q}}$ into $\bar{k}_{\mathfrak{p}}$. This gives an embedding $i : G(k_{\mathfrak{q}}) \to G(\bar{k_{\mathfrak{p}}})$. Let $\bar{C}$ be the conjugacy class of $i(\bar{t})$ in $G(\bar{k_{\mathfrak{p}}})$. Then $\bar{C}$ is a $k_{\mathfrak{p}}$-rational conjugacy class.*

Proof: By Proposition 3.3 the action of $Fr_{\mathfrak{q}}$ on $\bar{t}$ is the action of $\phi_C(Fr_{\mathfrak{q}}) \in W$ on $\bar{t}$, it follows that $\bar{C}$ is independent of the choice of the embedding of $k_{\mathfrak{q}}$ and that $\bar{C}$ is a $k_{\mathfrak{p}}$-rational conjugacy class. □

Remark 3.4. *As a consequence of $\bar{C}$ being $k_{\mathfrak{p}}$-rational. The characteristic polynomial $P_{\bar{C}(x)} \in k_{\mathfrak{p}}[x]$ is the reduction of $P_C(x)$ modulo $\mathfrak{p}$. Furthermore, $\bar{C}$ does not depend on the choice of the prime ideal $\mathfrak{q}$ dividing $\mathfrak{p}$ since $Gal(E/K)$ acts transitively on such ideals. A priory the class $\bar{C}$ may depend on the ideal $\mathfrak{q}$ however it does not. Indeed, if $\mathfrak{q}'$ is another prime ideal in B such that $\mathfrak{q} \cap A = \mathfrak{p}$ then there exist $\sigma \in Gal(E/K)$ such that $\sigma(\mathfrak{q}') = \mathfrak{q}$. $Gal(E/K)$ acts transitively on the primes above $\mathfrak{p}$ Replacing $\mathfrak{q}$ by $\mathfrak{q}'$ is equivalent to replacing t by t^w where $w = \phi_C(\sigma)$. Summarizing, the following definition is independent of the choice of t.*

Definition 3.6. For every $\mathfrak{p} \notin S$ let $\bar{C}$ be the $G(\bar{k}_{\mathfrak{p}})$-conjugacy class of $\bar{t}$. The class $\bar{C}$ is called the reduction of C modulo $\mathfrak{p}$.

Proposition 3.5. *Let m be a positive integer. Assume that the roots of $P_C(x)$ are not roots of 1. Then there exists a finite set of primes $S \subset S_m$ such that for every $\mathfrak{p} \notin S_m$ the elements in $\bar{C}$, the reduction of C modulo $\mathfrak{p}$, do not have the order dividing m.*

Proof. The polynomials $P_C(x)$ and $x^m - 1$ are relatively prime. In particular, there exists polynomials $P(x)$ and $Q(x) \in K[x]$ such that $P(x)P_C(x) + Q(x)(x^m - 1) = 1$. Let $S \subset S_m$ be a set of primes such that for every $\mathfrak{p} \notin S_m$ the coefficients of $P(x)$ and $Q(x)$ are in $A_{\mathfrak{p}}$. Note that the denominators of the coefficients of $P_(x)$ and $Q(x)$ can be contained independently only on a finite set of primes, then we can take S_m to be finite. Now, we can reduce the equation modulo every such prime. It follows that $\bar{P}_C(x)$ is relatively prime to $x^m - 1$ in $k_{\mathfrak{p}}[x]$. Hence the eigenvalues of $\bar{t}$ do not have the order dividing m. For if there was one eigenvalue of $\bar{t}$ with order dividing m then it would be a root of $x^m - 1$ in $k_{\mathfrak{p}}$. □

Let $K_{\mathfrak{p}}$ be the $\mathfrak{p}$-adic completion of K. Let $g \in C(K_{\mathfrak{p}})$, where $C(K_{\mathfrak{p}})$ is a conjugacy class over $K_{\mathfrak{p}}$. Let Λ be a lattice in $V \otimes_K K_{\mathfrak{p}}$ such that $g \cdot \Lambda = \Lambda$.

Definition 3.7. Let

$$\bar{g} : \Lambda/\mathfrak{p}\Lambda \to \Lambda/\mathfrak{p}\Lambda$$

be the map induced by g. We call $\bar{g}$ the "naive" reduction of g modulo $\mathfrak{p}$.

In view of Propositions 3.4 and 3.5 we have certain control of the order of elements in the class $\bar{C}$. We shall now relate this order to the order in "naive" reduction modulo $\mathfrak{p}$.

Let $|g|_{\mathfrak{p}'}$ be the prime to $\mathfrak{p}$-part of the order of $\bar{g}$. This is the order of the semi-simplification of $\bar{g}$. In particular, it does not depend on the choice of the lattice Λ. For our applications we shall need the following:

Proposition 3.6. *Let $\mathfrak{p} \notin S$. Let $g \in C(K_{\mathfrak{p}})$, where $K_{\mathfrak{p}}$ be the $\mathfrak{p}$-adic completion of K. Then $|g|_{\mathfrak{p}'}$ is equal to the order of elements in $\bar{C}$, the reduction of C modulo $\mathfrak{p}$.*

Proof: It is enough to prove this statement after taking an unramified extension of $K_{\mathfrak{p}}$. In particular, we can extend by $E_{\mathfrak{q}}$, the completion of E at a prime $\mathfrak{q} \subset B$ such that $\mathfrak{q} \cap A = \mathfrak{p}$. Recall that $C(K_s)$ contains $t \in T(E) \subset T(E_{\mathfrak{q}})$ so g is conjugated to t over a separable extension of $E_{\mathfrak{q}}$. We claim that g is conjugated to t over a $E_{\mathfrak{q}}$. Note that the centralizer of t in G is T, thus, the possible obstruction lies in the Galois cohomology $H^1(E_{\mathfrak{q}}, T)$. However, since $T(E_{\mathfrak{q}})$ is a split torus, its Galois cohomology is trivial by the Hilbert Theorem 90. Thus s is conjugated to t over $E_{\mathfrak{p}}$. Now it suffices to prove the statement for t and a lattice invariant under multiplication by t. We may choose the lattice to be the $\mathfrak{p}$-adic completion of the lattice L. With this choice of the lattice, $\bar{t}$ defines the class $\bar{C}$, and the proposition follows. $\square$

3.4 Remark on the group G_2

Theorem 3.2. *Let $C_1, \ldots, C_n$ be semi-simple, regular, conjugacy classes in $G_2(\mathbb{Q})$. Assume that the Galois groups of the splitting fields E_{C_i} of the characteristic polyno-*

mials $P_{C_i}(x)$ are all isomorphic to the dihedral group D_6 and that they are linearly independent, i.e. the composite of all these fields has degree 12^n. Assume that for almost all primes p we are given $g_i \in C_i(\mathbb{Q}_p), i = 1, \ldots, n$, and a maximal compact subgroup U_p in $G_2(\mathbb{Q}_p)$ containing g_i. Then, for a set of primes of density at least

$$1 - 2(\frac{5}{6})^n + 4(\frac{4}{6})^n$$

the group U_p is hyperspecial and the projections of g_i generate the reductive quotient of U_p isomorphic to $G_2(p)$.

Proof: Remember that the Weyl group W of G_2 is isomorphic to D_6. Thus the assumption on the Galois groups of the fields E_{C_i} implies that the maps ϕ_{C_i} : $\mathrm{Gal}(E_{C_i}/\mathbb{Q}) \to W$ introduced in Section 3.1 are all isomorphisms. Recall from section 3.2 that $6a$ and $3a$ are the conjugacy classes in W, consisting of two elements of order 6 and 3, respectively. Let Λ be a lattice, in the 7-dimensional representation of G_2, preserved by U_p. Then $\Lambda/p\Lambda$ is a U_p-module. The group U_p acts on a semi simplification of $\Lambda/p\Lambda$ through its reductive quotient: $G_2(p)$, $SL_3(p)$ or $SO_4(p)^+$. Let $\bar{g}_i$ be the projection of g_i to the reductive quotient of U_p. Let $\bar{C}_i$ be the reduction modulo p of the rational conjugacy class C_i, as in Section 3.3. By Proposition 3.6 the prime to p-part of the order of $\bar{g}_i$ is the same as the order of elements in $\bar{C}_i$. Moreover, the order of elements in $\bar{C}_i$ can be arranged to be as large as needed, by Proposition 3.5, provided p is large enough. By Proposition 3.3, the order of elements in $\bar{C}_i$ divides the order of the finite torus T_w where $w = \phi_{C_i}(Fr_p)$. Assume that there exist j and k such that $\phi_{C_j}(Fr_p) = 6a$ and $\phi_{C_k}(Fr_p) = 3a$. Then prime to p order of $\bar{g}_j$ divides $p^2 - p + 1$ and prime to p order of $\bar{g}_k$ divides $p^2 + p + 1$. This forces the reductive quotient of U_p to be isomorphic to $G_2(p)$, i.e. U_p is hyperspecial, and $\bar{g}_j$ and $\bar{g}_k$ generate the quotient $G_2(p)$ by Corollary 3.1. Thus, by contraposition, if $G_2(p)$ is not a quotient of the image of ρ_p, then $\phi_{C_i}(Fr_p) = 6a$ for all $i = 1, \ldots, n$ or $\phi_{C_i}(Fr_p) = 3a$ for all $i = 1, \ldots, n$. By Chebotarev's density theorem the set of primes p such that $\phi_{C_i}(Fr_p) = 6a$ for all $i = 1, \ldots, n$ and the set of primes p such that $\phi_{C_i}(Fr_p) = 3a$ for all $i = 1, \ldots, n$ each has density $(\frac{5}{6})^n$. The intersection of these two sets of primes has density $(\frac{4}{6})^n$. Finally observe that the density of the set of primes such that $G_2(p)$ appears as a quotient approaches 1 as $n \to \infty$. $\square$

4 Galois Representations

In this chapter, we will set up the basic theory of Galois representations. We will be interested in l-adic Galois representations.

4.1 Some representation theory

This section is intended to provide a brief description of the most important concepts in representation theory necessary for our purposes.

Let G be a group, and let A be a commutative ring. An A-linear representation of G consists of a free A-module V and a group morphism $\rho_V : G \to Aut_A(V)$.

Definition 4.1. The group algebra $A[G] = \bigoplus_{g \in G} A$ is the A-algebra consisting of finite formal A-linear combinations of elements of G.

An A-linear representation of G is the same as a left $A[G]$-module V that is free as an A-module. More precisely, the category of A-linear representations of G is isomorphic to the category of left $A[G]$-modules V that are free over A.

Definition 4.2. A morphism between two A-linear representations of G, from V to W is an $A[G]$-linear map $V \to W$. Equivalently, a morphism $V \to W$ is an A-linear map that is compatible with the G-actions on both sides. The representations V and W are called isomorphic or equivalent if they are isomorphic as left $A[G]$-modules.

We consider now the case where A is a field K. Let V be a K-linear representation of G. We say that V is simple or irreducible if V is simple as a $K[G]$-module, i.e. if V has exactly two $K[G]$-submodules, namely 0 and V. Furthermore, we say that V is semi-simple if V is a direct sum of simple $K[G]$-modules.

Theorem 4.1 (Maschke)**.** *Let G be a finite group, and let K be a field such that $|G|$ is not divisible by $char(K)$. If V is a $K[G]$-module of finite K-dimension. Then V is a direct sum of simple $K[G]$-modules.*

Proof. [27] Theorem 1.2.1.

Remark 4.1. *We recall that the semi-simplification of a representation of a group G on a finite dimensional vector space V over a field k is the direct sum of all the Jordan-Hölder constituents of the $k[G]$-module V*

Lemma 4.1 (Schur). *Let K be a field, and let G be a group*

(i) Let V and W be two simple $K[G]$-modules, and let $f : V \to W$ be a $K[G]$-linear map. Then f is either the zero map or an isomorphism

(ii) Let V be a simple $K[G]$-module. Then the K-algebra $End_{K[G]}V$ of $K[G]$-linear endomorphisms of V is a division algebra.

(iii) Let V be a simple $K[G]$-module, where K is algebraically closed and V is finite dimensional. Then $End_{K[G]}(V) = K$.

Proof. [27] Theorem 2.1.1.

Proposition 4.1. *Let A be an algebra over a field K of characteristic zero, and let ρ_1, ρ_2 be two A-modules of finite K-dimension. Assume that ρ_1 and ρ_2 are semi-simple and $Tr_K(\rho_1(\lambda))$ equals $Tr_K(\rho_2(\lambda))$ for all $\lambda \in A$. Then ρ_1 is isomorphic to ρ_2.*

Proof. [4] Chapter 8, Proposition 12.1.3.

4.2 l-adic Galois representations

We start by recalling the definition of the absolute Galois group.

Definition 4.3. Let F be a field and $\bar{F}$ a separable algebraic closure of F, we call $G_F := Gal(\bar{F}/F)$ the absolute Galois group of F. By theorem 2.2, G_F is profinite and it is isomorphic to the projective limit

$$\varprojlim_{F \subset K \subset \bar{F}} \mathrm{Gal}(K/F),$$

where K runs over each finite Galois extension K of F inside $\bar{F}$. The projective system is given by the restriction maps $Gal(\bar{F}/F) \to Gal(K/F)$. By theorem 2.2, the subgroups of the form $Gal(\bar{F}/K)$ with $F \subset K \subset \bar{F}$ a finite extension, are open and moreover they form a fundamental system of neighborhoods of $1 \in G_F$.

Definition 4.4. Let l be a prime number. Let F be a number field, and G_F its absolute Galois group. Let $E \subset \bar{\mathbb{Q}}_l$ be a closed subfield. We call a Galois l-adic representation a continuous representation of G_F in a finite-dimensional E-vector space V

$$\rho : Gal(\bar{F}/F) \to GL_E(V).$$

We will be mostly looking at the case where either E is $\mathbb{Q}_l$ or $\bar{\mathbb{Q}}_l$. The following is a well known example of a l-adic Galois representation, known as the cyclotomic character.

Example 4.1. Let l be a prime number. The following is an example of a one dimensional l-adic representation. We write μ_l^∞ for the set of l^n-roots of unity for every $n \geqslant 0$. There is a unique continuous morphism of groups $\chi_l : G_{\mathbb{Q}} \to \mathbb{Z}_l^\times \subset \bar{\mathbb{Q}}_l^\times$, such that for all l^n-th roots of unity $\zeta \in \mu_l^\infty$ and all $\sigma \in G_{\mathbb{Q}}$ we have $\sigma(\zeta) = \zeta^{\chi_l(\sigma)}$. This morphism is the cyclotomic character. Through the character χ_l we may let $G_{\mathbb{Q}}$ act on $\bar{\mathbb{Q}}_l$ via multiplication.

Let $\rho : G_F \to GL_E(V)$ be a l-adic Galois representation. The normal subgroup $Ker\rho = \rho^{-1}(\{1\})$ is closed, hence of the form $Gal(\bar{F}/F(\rho))$ for a unique Galois extension $F(\rho)$ of F inside $\bar{F}$. Its Galois group $Gal(F(\rho)/F) \cong \rho(G_F)$ is a closed subgroup of $GL_E(V)$.

If L is a finite extension of $\mathbb{Q}_l$, we denote by $\mathcal{O}_L$ its ring of l-adic integers, by π_L a uniformizer of $\mathcal{O}_L$, and by $k_L = \mathcal{O}_L/(\pi_L)$ its residue field.

For an l-adic representations (ρ, V) over L, there is the notion of a lattice in vector space V over $\mathbb{Q}_l$, i.e., a finitely generated free $\mathcal{O}_L$-submodule Λ of V such that $\Lambda \otimes_{\mathcal{O}_L} L \cong V$. For reduction $mod(\pi_L)$, one needs to choose an $\mathcal{O}_L$-lattice Λ invariant under the finite group G acting on V.

Lemma 4.2. *Let L be a finite extension of $\mathbb{Q}_l$ and $\rho : G_F \to GL_n(L)$ a Galois representation. There are $\mathcal{O}_L$-lattices $\Lambda \subset L^n$ which are stable by G_F . The semisimplification of the representation of G_F on $\Lambda/\pi_L\Lambda \cong k_L^n$ does not depend on the choice of Λ.*

Remark 4.2. *In fact, in the statement above G_F could be replaced by any profinite group.*

Proof: Let Λ be any $\mathcal{O}_L$-lattice inside L^n. Then $\{g \in GL_n(L), g(\Lambda) = \Lambda\}$ is an open subgroup of $GL_n(L)$. Now G_F is compact and ρ is continuous so $G = \rho(G_F)$ is a compact subgroup of $GL_n(L)$, hence its intersection H with Λ is an open subgroup of G. Let $\Lambda' = \sum_{g\in G} g(\Lambda)$, it is a finite sum over a set of representative of G/H which is G-stable.

If Λ is a G-stable lattice, so is $\Lambda' = \pi_L^i\Lambda$ for all i, moreover there is a $k_L[G]$-isomorphism $\Lambda/\pi_L\Lambda \cong \Lambda'/\pi_L\Lambda'$. Let now Λ_1 and Λ_2 be two G-stable lattices. Then so are the $L_i := \Lambda_1 + \pi_L^i\Lambda_2$ for $i \in \mathbb{Z}$. Note that $L_i = \Lambda_1$ for $i >> 0$, $L_i = \pi_L^i\Lambda_2$ for $-i >> 0$, and $\pi_L L_i \subset L_{i+1} \subset L_i$ for each $i \in \mathbb{Z}$ so we may assume that $\pi_L\Lambda_1 \subset \Lambda_2 \subset \Lambda_1$ and $\Lambda_2 \subset \Lambda_1 \subset \pi_L^{-1}\Lambda_2$. There is an exact sequence of $k[G]$-modules:

$$0 \to \Lambda_2/\pi L_{\Lambda_1} \to \Lambda_1/\pi L_{\Lambda_1} \to \Lambda_1/\Lambda_2 \to 0.$$

so the $k_L[G]$-module $\Lambda_2/\pi_L\Lambda_2 \cong \pi_L^{-1}\Lambda_2/\Lambda_2$ is as well an extension of $\pi_L^{-1}\Lambda_2/\Lambda_1 \cong \Lambda_2/\pi_L\Lambda_1$ by Λ_1/Λ_2. In other words the the semisimplification of G_F on on $\Lambda/\pi_L\Lambda \cong k_L^n$ does not depend on the choice of Λ. □

Definition 4.5. Let L be a finite extension of $\mathbb{Q}_l$ and $\rho : G_F \to GL_n(L)$ a Galois representation. We denote by $\bar{\rho} : G_F \to GL_n(k_L)$ the semi-simple representation defined by the previous lemma. It is called the residual representation of ρ.

4.3 Ramification

Definition 4.6. Let $(\rho, V\ )$ be a Galois representation of F. Let v be a finite place of F. Then ρ is unramified at v if $\rho(I_v) = 1$; that is, if $I_v \subset \ker\rho$. (Note that I_v is defined only up to conjugacy, but $\ker\rho$ is normal, so all conjugates of any element $\sigma \in I_v$ are also in $ker\rho$ if σ is).

Definition 4.7. (ρ, V) is unramified outside of S if it is unramified at each place $v \notin S$. (ρ, V) is unramified almost everywhere if there is a finite set S of finite places of F such that ρ is unramified outside of S.

Proposition 4.2. *If ρ has finite image, then ρ is unramified almost everywhere (that is, ρ is unramified outside of a finite set of primes).*

Proof. Since ρ has finite image, it factors through a finite quotient of G_F, which is a finite group that is the Galois group of a finite Galois extension L/F. ρ is ramified at v iff $\rho(I_v) \neq 1$, which happens iff v ramifies in L. Thus ρ is ramified precisely where $L|F$ ramifies, which is at most at a finite number of places. □

Proposition 4.3. *If S is a finite set of primes and ρ is unramified outside of S, then ρ factors through $G_{K,S}$:*

$$\begin{tikzcd}
 & G_{K,S} \arrow[dr, "\rho"] & \\
G_K \arrow[ur] \arrow[rr, "\rho"] & & GL_L(V)
\end{tikzcd}$$

Proof. The kernel of the map $G_K \to G_{K,S}$ is the smallest normal subgroup containing all I_v for $v \notin S$, and this subgroup is in the kernel of ρ. □

Remark 4.3. *If ρ is unramified outside of S and $v \notin S$, then $\rho(Fr_v)$ is an element of $GL_L(V)$ well-defined up to conjugacy class. This means that $tr\rho(Fr_v)$, $det\rho(Fr_v)$, and $\chi_\rho(Fr_v)$ (the characteristic polynomial of $\rho(Fr_v)$) are all well-defined.*

Theorem 4.2. *Let $(\rho_V, V), (\rho_{V'}, V')$ be two semi-simple Galois representations over E of $Gal(\bar{F}/F)$. Let S be a finite set finite of F-places v such that S contains all finite F-places where V or V' is ramified. Assume $Tr(Fr_v, V) = Tr(Fr_v, V')$ for all finite F-places v such that $v \notin S$. Then $V \cong V'$.*

Proof. The field $K = \bar{\mathbb{Q}}^{ker(\rho_V) \cap ker(\rho_{V'})}$ is a Galois extension of F which is unramified at almost all F-places. By Chebotarev's density theorem the set of Frobenius elements in $Gal(K/F)$ is a dense subset. Hence the equality $Tr(Fr_v, V) = Tr(Fr_v, V')$ extends to an equality $Tr(\sigma, V) = Tr(\sigma, V')$ for all $\sigma \in Gal(\bar{F}/F)$. Hence the theorem follows from Proposition 4.1. □

5 Automorphic forms and representation

In this chapter, we will introduce the most basic notions needed to understand admissible and automorphic representations, and its local components, we encourage the reader to also read up [3] for a detailed survey on automorphic representations.

5.1 Haar measures and Hecke algebras

Let G be a locally compact topological group (for example $Gl_n(\mathbb{A}_F)$). We define

$$C_c(G) = \{f : G \to \mathbb{R} \text{ continuous with compact support}\}$$

and we let $C_c(G)^\vee$ denote the $\mathbb{R}$-linear dual of $C_c(G)$.

Definition 5.1. A measure on G is an element $\mu \in C_c(G)^\vee$ such that if f is non-negative everywhere and not identically zero, then $\mu(f) > 0$. A left Haar measure on G is a measure μ which is invariant under the canonical left action of G on $C_c(G)^\vee$. A right Haar measure on G is a measure ν which is invariant under the canonical right action of G on $C_c(G)^\vee$.

Proposition 5.1. *There exists a unique left (resp. right) Haar measure on G, up to scaling by a positive constant.*

Proof. [7], Theorem 9.2.2 and Theorem 9.2.6.

If μ is a measure on G and S is a compact open subset of G, we write $\mu(S) = \mu(\mathbf{1}_S)$, where $\mathbf{1}_S$ is the characteristic function of S. For μ either a left or a right Haar measure and $f \in C_c(G)$, we use the notations:

$$\int_G f d\mu = \int_{x \in G} f(x) d\mu(x) = \mu(f)$$

The left invariance of μ and the right invariance of ν can be expressed as

$$\int_{x \in G} f(x) d\mu(x) = \int_{x \in G} f(gx) d\mu(x) \text{ and } \int_{x \in G} f(x) d\nu(x) = \int_{x \in G} f(xg) d\nu(x).$$

Definition 5.2. Let G be a locally compact group G. Let μ be a left Haar measure on G, and ν be a right Haar measure on G. We say that G is unimodular if there is a (positive) constant C such that $\mu = C\nu$.

Suppose now that G is a locally profinite group. Consider the set of smooth compactly supported functions on G:

$$\mathcal{H}(G) = \{f : G \to \mathbb{C} | f \text{ is locally constant and has compact support}\}.$$

If we fix a right Haar measure ν on G. On $\mathcal{H}(G)$, we define a $\mathbb{C}$-bilinear multiplication map by

$$(f * g)(x) = \int_{y \in G} f(xy^{-1})g(y)d\nu(y).$$

Which turn $\mathcal{H}(G)$ into an algebra.

Lemma 5.1. *Let G be a locally profinite group, and let ν be a right Haar measure on G. Then the multiplication defined above is associative. Moreover there is a unit for this multiplication if and only if G is discrete.*

Proof: [7], Proposition 9.4.6.

Remark 5.1. *For any compact open subgroup $K \subset G$, we write*

$$\mathcal{H}(G, K) = \{f \in \mathcal{H}(G) \text{ such that } f \text{ is left and right } K\text{-invariant}\}.$$

With this definition we can write $\mathcal{H}(G)$ as a direct limit $\mathcal{H}(G) = \varinjlim_K \mathcal{H}(G, K)$ with K ranging over the set of compact open subgroups of G.

Also for any open compact subgroup $K \subset G$, we define an element $e_K \in \mathcal{H}(G)$ as $\nu(K)^{-1}$ times $\mathbf{1}_K$. Then we have $e_K * e_K = e_K$ and $\mathcal{H}(G, K) = e_K * \mathcal{H}(G) * e_K$.

5.2 Admissible representations

Among the complex representations of a locally profinite group, we will be interested in the well-behaved representations. These will be the ones satisfying certain conditions, namely smoothness and admissibility.

Definition 5.3. Let G be a locally profinite group, let V be a $\mathbb{C}$-vector space, which may be infinite-dimensional, and let $\pi : G \to GL_{\mathbb{C}}(V)$ be a group homomorphism. We say that (π, V) is smooth if every $v \in V$ is fixed by a compact open subgroup K of G.

Definition 5.4. We say that (π, V) is admissible if it is smooth and for every open compact subgroup $K \subset G$ the space:

$$V^K = \{v \in V | \pi(k)v = v \text{ for all } k \in K\}$$

is finite-dimensional.

Definition 5.5. Let (π, V) and (π', V') be smooth representations of G. A morphism from (π, V) to (π', V') is a $\mathbb{C}$-linear map $t : V \to V'$ satisfying $t(\pi(g)v) = \pi'(g)(t(v))$ for all $g \in G$ and $v \in V$.

We now introduce a similar notion for Hecke algebras.

Definition 5.6. A representation of $\mathcal{H}(G)$ is a homomorphism : $\mathcal{H}(G) \to End_{\mathbb{C}}(V)$ of (non-unital) $\mathbb{C}$-algebras, where V is a $\mathbb{C}$-vector space. We say that a representation (π, V) of $\mathcal{H}(G)$ is smooth if $\mathcal{H}(G)V$ is equal to V , i.e. if for every $v \in V$ there exists $f \in \mathcal{H}(G)$ such that $\pi(f)v = v$.

Both the smooth representations of G, and the smooth representations of $\mathcal{H}(G)$ form a category. In fact,they are equivalent categories.

Theorem 5.1. *Let G be a locally profinite group. Then every smooth representation of G can be given the structure of a smooth representation of $\mathcal{H}(G)$ which gives an equivalence of categories*

$$\{\textit{smooth representations of } G\} \sim \{\textit{ smooth representations of } \mathcal{H}(G)\}.$$

Proof: [5] Section 1.4.

5.3 Ramification

Let F be a finite extension of $\mathbb{Q}_p$, with ring of integers $\mathcal{O}_F$, and let $G = GL_n(F)$. If (π, V) is an irreducible, admissible representation of G, for any vector $v \neq 0 \in V$, the stabilizer K of v in G is open. Moreover, the subspace $\mathbb{C}[G \cdot v] \subset V$ spanned by the translates gv of v, is G-invariant and non-zero. By irreducibility of π, the above inclusion is equality. Thus π is generated by its K-invariant vectors. To V we can try to attach the largest subgroup K such that V^K is non-zero. This group K is then a measure for "how ramified" π is

Let G be a connected reductive group over F. Let $G = G(F)$, and K be a maximal compact (hence open) subgroup of G. In case $G = GL_n(F)$, the maximal compact subgroup would be $GL_n(\mathcal{O}_F)$.

Definition 5.7. A smooth representation (π, V) of G is called spherical (or unramified) with respect to K if it contains a nonzero K-fixed vector, i.e. if $V^K \neq 0$. The Hecke algebra $\mathcal{H}(G, K)$ is called the spherical Hecke algebra with respect to K.

Remark 5.2. *The interest of the group $GL_n(\mathcal{O}_F) \subset GL_n(F)$ is that it is a so-called hyperspecial group.*

We recall the definition of hyperspecial group.

Definition 5.8. Let F be a nonarchimedean local field, $\mathcal{O}_F$ its ring of integers, k its residue field and G a reductive group over F. A compact subgroup K of $G(F)$ is called hyperspecial if there exists a smooth group scheme Γ over $\mathcal{O}_F$ such that $\Gamma_F = G$, Γ_k is a connected reductive group and $\Gamma(\mathcal{O}_F) = K$.

Remark 5.3. *The unramified representations π of G correspond to simple modules over the $\mathcal{H}(G, K)$. So to study the unramified representations, it is natural to try to understand $\mathcal{H}(G, K)$. Using the Cartan decomposition it can be proven that the algebra $\mathcal{H}(G, K)$ is commutative.*

One way to study spherical representations is through the Satake isomorphism which allows us to analyze the structure of $\mathcal{H}(G, K)$. To state the most general form of the Satake isomorphism, for an arbitrary connected reductive group G, we need to be careful about the choice of K, we refer to [12] for more information about the Satake isomorphism.

For a proper K, if G is split, let $\hat{G}$ be the complex dual reductive group with maximal torus $\hat{T}$. The Satake isomorphism then says $\mathcal{H}(G, K) \cong \mathcal{H}(T, T(O_F))^W$. Characters of $\mathcal{H}(G, K)$ are therefore identified with elements of $\hat{T}/W$, i.e. semi-simple conjugacy classes in $\hat{G}$. This is called the Satake parameter of the corresponding spherical representation.

We now discuss an example on a ramified representation, called the Steinberg representation. This an more examples of ramified representations may be found in Peter Bruin, Arno Kret's notes on Galois Representations and Automorphic Forms.

The Steinberg representation

Every reductive group has such a representation, but for simplicity we will study such a representation for the group $GL_n(\mathbb{Q}_p)$. A parabolic subgroup $P \subset GL_n$ is by definition a connected subgroup such that the quotient variety GL_n/P is projective; whenever P is minimal with this property, we call it a Borel subgroup. In GL_n the standard example of a Borel subgroup is the group B of upper triangular matrices B^+, for any $g \in GL_n(\mathbb{Q})$, the subgroup $gBg^{-1} \subset GL_n$ is a Borel subgroup as well. In fact, all Borel subgroups are conjugate, so they are all of this form. A connected subgroup of GL_n is parabolic if and only if it contains a Borel subgroup. Let $B = B^+ \subset GL_n$ the group of upper triangular matrices. We will call a parabolic subgroup P of GL_n standard if $B \subset P$. For any such $P \subset GL_n(F)$ the quotient GL_n/P is projective and the space $GL_n/P(F)$ is compact. We can consider the space C_P of locally constant functions $f : GL_n/P(F) \to \mathbb{C}$ on it. This space C_P again carries a representation of $GL_n(F)$, acting by translations on the right. If P, P_0 are two parabolic subgroups of GL_n such that the partition corresponding to P is a refinement of the partition corresponding to P_0, we have an inclusion $P \subset P_0$, a map $GL_n/P(F) \to GL_n/P_0(F)$ and an induced map $C_{P_0} \to C_P$. In particular, the spaces C_P are not irreducible if P has a refinement. To define the Steinberg representation St of $GL_n(F)$, we consider the space C_B and let U be the subspace of C_B generated (as a representation) by all the subspaces C_P, where $P \subset GL_n$ runs over all the standard parabolic groups with $P \neq B$. Then $U \subset C_B$ is a stable subspace, and the quotient C_B/U turns out to be irreducible. This is the Steinberg representation.

5.4 $(\mathfrak{g}, K)$-modules

Let G be a reductive group over an archimedean local field F (i.e. $\mathbb{R}$ or $\mathbb{C}$) and K be a maximal compact subgroup of $G(F)$. We define $\mathfrak{g} = Lie(Res_{F/\mathbb{R}}G)$ the Lie algebra of $Res_{F/\mathbb{R}}G(F)$ (here the restriction of scalars is employed so that $\mathfrak{g}$ is a Lie algebra over $\mathbb{R}$). There is a natural representation $G \times \mathfrak{g} \to \mathfrak{g}$ $(g, x) \to (Ad\mathfrak{g})x$, where $Ad : \mathfrak{g} \to Aut_{\mathbb{R}}\mathfrak{g}$ is the adjoint representation.

In the case where $G = GL_n(\mathbb{R})$, we can identify $(Ad\mathfrak{g})$x with gxg^{-1} in $M_n(\mathbb{R})$. Recall that there is an exponential map $exp : \mathfrak{g} \to G$ The complexification of $\mathfrak{g}$ is the complex Lie algebra $\mathfrak{g}_{\mathbb{C}} = \mathfrak{g} \otimes_{\mathbb{R}} \mathbb{C}$.

Definition 5.9. A $(\mathfrak{g}, K)$-module is a complex vector space V equipped with representations of the group K and of the Lie algebra $\mathfrak{g}$, both denoted by π, such that

- The space V is a countable algebraic direct sum $V = \bigotimes_i V_i$ with each V_i a finite dimensional K-invariant vector space
- for all x in the Lie algebra $Lie(K) \subset \mathfrak{g}$, the limit

  $$\frac{d}{dt}(\pi(exp(tx))v)|_{t=0} = lim_{t\to 0}t^{-1}(\pi(exp(tx))vv).$$

  (where $exp : \mathfrak{g} \to G$ is the exponential map) exists and is equal to $\pi(x)v$;
- for all $k \in K$ and $x \in g$, we have $\pi(k) \circ \pi(x)\pi(k^{-1}) = \pi((Adk)x)$.

We observe that the representation of $\mathfrak{g}$ on a $(\mathfrak{g}, K)$-module V can be extended in a canonical way to a representation of the complexified Lie algebra $\mathfrak{g}_{\mathbb{C}}$

Definition 5.10. A$(\mathfrak{g}, K)$-module (π, V) is admissible if every irreducible continuous finite-dimensional representation of K occurs only finitely many times in V (up to isomorphism).

Before moving to the next section, let $U(\mathfrak{g}_{\mathbb{C}})$ be the universal enveloping of $\mathfrak{g}_{\mathbb{C}}$. This is an associative unital $\mathbb{C}$-algebra together with a homomorphism $\iota : \mathfrak{g}_{\mathbb{C}} \to U(\mathfrak{g}_{\mathbb{C}})$ of complex Lie algebras (i.e. a $\mathbb{C}$-linear map satisfying $\iota([x, y]) = \iota(x)\iota(y) - \iota(y)\iota(x))$ such that for every associative unital $\mathbb{C}$-algebra A and every Lie algebra homomorphism $f : \mathfrak{g}_{\mathbb{C}} \to A$ there is a unique extension of f to a homomorphism $U(\mathfrak{g}_{\mathbb{C}}) \to A$ of associative unital $\mathbb{C}$-algebras. In particular, every representation of $\mathfrak{g}$ on a $\mathbb{C}$-vector space V extends uniquely to a $U(\mathfrak{g}_C)$-module structure on V.

5.5 Automorphic Representations

The main purpose of this section is to discuss the notions of automorphic forms and automorphic representations of adelic groups.

Let F be a number field, $\mathcal{O}_F$ the ring of integers of F, V (resp. V_∞ ,resp. V_f) the set of places (resp. archimedean places, resp. nonarchimedean places) of F and F_v the completion of F at $v \in V$. Let K_v be the standard maximal compact subgroup of $G(F_v)$ and define $K_\infty = \prod_{v \text{ infinite}} K_v$

Definition 5.11. A function $\phi : G(\mathbb{A}_F) \to \mathbb{C}$ is smooth if is satisfies:

- There exists a compact open subgroup $K \subset G(\mathbb{A}_F^\infty)$ such that $\phi(gk) = \phi(g)$ for all $g \in G(\mathbb{A}_F)$ and $k \in K$
- For every $g^\infty \in G(\mathbb{A}_F^\infty)$, the function $G(F \otimes_{\mathbb{Q}} \mathbb{R}) \to \mathbb{C}$, $g_\infty \to \phi(g_\infty, g^\infty)$ is smooth

Definition 5.12. Given an F-morphism $\rho : G \to GL_n$ with finite kernel define, for $x \in G(\mathbb{A})$

$$||x|| = \text{sup}_{v\in V}\text{max}_{i,j}|\rho(g)_{ij}|_v|\rho(g^{-1})_{ij}|_v$$

Let $\phi : G(F)\backslash G(\mathbb{A}_F) \to \mathbb{C}$ be a smooth function. Then ϕ is said to be of moderate growth if there exist real numbers B, $C > 0$ such that $|\phi(g)| \leqslant C||g||^B$ for all $g \in G(\mathbb{A}_F)$.

Definition 5.13. An automorphic form for G is a smooth function $\phi : G(F)\backslash G(\mathbb{A}_F) \to \mathbb{C}$ (or equivalently a smooth function $\phi : G(\mathbb{A}_F) \to \mathbb{C}$ satisfying $\phi(g_0 g) = \phi(g)$ for all $g_0 \in G(F)$ and $g \in G(\mathbb{A}_F)$) such that:

- ϕ is K_∞-finite, i.e. the $\mathbb{C}$-vector space spanned by the smooth functions $G(\mathbb{A}_F) \to \mathbb{C}$, $g \to \phi(gk)$ for $k \in K_\infty$ is finite-dimensional.
- ϕ is $Z(U(\mathfrak{g}_\mathbb{C}))$-finite, i.e. the $\mathbb{C}$-vector space $Z(U(\mathfrak{g}_\mathbb{C}))\phi$ is finite-dimensional, where the action of $\mathfrak{g}_\mathbb{C}$, and hence of $U(\mathfrak{g}_\mathbb{C})$ and $Z(U(\mathfrak{g}_\mathbb{C}))$, on the space of smooth functions $G(\mathbb{A}_F) \to \mathbb{C}$ is defined through the right action of $G(F \otimes_\mathbb{Q} \mathbb{R})$ on $G(\mathbb{A}_F)$.
- ϕ is of moderate growth.

The $\mathbb{C}$-vector space of automorphic forms for G is denoted by $A(G)$.

Definition 5.14. An admissible representation of $G(\mathbb{A}_F)$ is a pair (π, V) where V is a $\mathbb{C}$-vector space equipped with the structure of both a smooth representation of $G(\mathbb{A}_F^\infty)$ and a $(\mathfrak{g}, K_\infty)$-module, both denoted by π, such that the two actions commute and such that every irreducible continuous finite-dimensional representation of the compact group $K = K_\infty \times G(\mathcal{O}_F)$ occurs only finitely many times in V (up to isomorphism). We say that (π, V) is irreducible if (π, V) has exactly two subrepresentations (namely the zero subspace and V itself).

Definition 5.15. An automorphic representation of $G(\mathbb{A}_F)$ is an irreducible admissible representation of $G(\mathbb{A}_F)$ that is isomorphic to a subquotient of $A(G)$.

Definition 5.16. We call an automorphic form $f \in A(G)$ a cuspform, if for every strict standard parabolic subgroup $P = MN \subset G$, and all $g \in G(\mathbb{A}_F)$

$$\int_{n \in N(\mathbb{A}_F)} f(gn) = 0.$$

We call an automorphic representation π of $G(\mathbb{A}_F)$ cuspidal if it appears in the space of cusp forms on G.

5.6 Decomposition of representation into tensor products

The study of the representations of adelic groups, which are infinite restricted products of groups, requires the notion of restricted tensor product of vector spaces. Here we establish some generalizations of the classical theorem which classifies the irreducible representations of the direct product of two finite groups in terms of those of the factors will be discussed.

Theorem 5.2. *Let G_1, G_2 be locally compact, totally disconnected groups and let $G = G_1 \times G_2$.*

- *If π_i is an admissible irreducible representation of G_i, $i = 1, 2$, then $\pi_1 \times \pi_2$ is an admissible irreducible representation of G.*
- *If π is an admissible irreducible representation of G, then there exist admissible irreducible representations π_i; of G_i; such that $\pi = \pi_1 \otimes \pi_2$.*

Proof. [9] Theorem 1.

Now we introduce the notion of restricted tensor product. The ordinary constructions with finite tensor products extend easily to restricted tensor products.

Definition 5.17. Let $\{W_v | v \in V\}$ be a family of vector spaces. Let V_0 be a finite subset of V. For each $v \in V \backslash V_0$, let x_v be a nonzero vector in W_v. For each finite subset S of V containing V_0, let $V_S = \bigotimes_v W_v$, and if $S \subset S'$, let $f_S : W_S \to W_{5'}$, be defined by $\bigotimes_{v \in S} w_s \to \bigotimes_{v \in S} w_v \bigotimes_{v \in S' \backslash S} x_v$. Then $W = \bigotimes_{x_v} W_v$; the restricted tensor product of the w_v with respect to the x_v, is defined by $W = \varinjlim_S W_S$. The space W is spanned by elements written in the form $w = \otimes w_v$, where $w_v = x_v$ for almost all $v \in V$.

Let $G = \prod'_{K_v} G_v$ be the restricted product of locally compact totally disconnected groups G_v, restricted with respect to the compact open subgroups K_v. Then G itself is locally compact and totally disconnected, and $\mathcal{H}(G)$ is isomorphic to $\bigotimes_{e_{K_v}} \mathcal{H}(G_v)$.

For each $v \in V$ let W_v be an admissible G_v-module. Assume that $dim W_v^{K_v} = 1$ for almost all v. Choosing for almost all v a nonzero vector $x_v \in W_v^{K_v}$, we may form the G-module $W = \bigotimes_{x_v} W_v$. The isomorphism class of W is in fact independent of the choice of $x_v \in W_v^{K_v}$ and will be called the tensor product of the representations W_v. One sees that W is admissible, and that it is irreducible if and only if each W_v is.

Definition 5.18. The admissible irreducible representations of G isomorphic to ones constructed as above are said to be factorizable.

Let G be a connected reductive algebraic group over a number F. Let $\mathbb{A} = \mathbb{A}_F$ be the adele ring of F, and let V be the set of places of F. The adelic group $G(\mathbb{A})$ is isomorphic to a restricted product $\prod'_{K_v} G(F_v)$, where the subgroups K_v are defined for all finite v and are certain maximal compact subgroups of $G(F_v)$. For almost all finite $v \in V$, K_v is a hyperspecial compact subgroup. For these places v, $\mathcal{H}(G(F_v), K.)$ is commutative.

We end this section by stating Flath's decomposition theorem.

Theorem 5.3 (Flath, 1979)**.** *Let (π, V) be an irreducible admissible representation of $G(\mathbb{A}_F)$. Then there exist*

- *an irreducible admissible $(\mathfrak{g}, K_\infty)$-module (π_∞, V_∞),*
- *an irreducible admissible representation (π_v, V_v) for every finite place v of F.*
- *a non-zero element $\epsilon_v \in K_v$, for all but finitely many v such that π is isomorphic to the restricted tensor product of the V_v with respect to the ϵ_v. Furthermore, each (π_v, V_v) is unique up to isomorphism.*

Proof. [9] Theorem 3.

6 Galois groups arising from automorphic representations

In this chapter we study the system of compatible irreducible Galois representations attached to certain automorphic representation Π of $GL_m(\mathbb{A})$, we rely on the results of Harris, Taylor and Yoshida in [11] and [26] to get such system. The automorphic representation is obtained by considering an example of an automorphic representation π on G_2. Finally, by studying the image of the Galois representations, we can conclude the main theorem.

6.1 Galois representations attached to automorphic forms

If $\mathbb{A}$ be the ring of adelés of $\mathbb{Q}$ and Π a cuspidal automorphic representation of $GL_m(\mathbb{A})$ where $m = 2n+1$. Fix a prime q and assume that Π is unramified for all primes $l \neq q$. Let $R_l(x)$ denote the characteristic polynomial of the Satake parameter of the local component Π_l. We assume that Π satisfies the following properties:

(1) The infinitesimal character of Π_∞ is the infinitesimal character of the trivial representation of $GL_m(\mathbb{R})$

(2) Π_q is the Steinberg representation.

(3) $R_l(x)$ the characteristic polynomial of ϕ_{Π_l} factors as $R_l(x) = P_l(x)(x-1)$, with $P_l(x)$ palindromic in $\mathbb{Z}[\frac{1}{l}][x]$.

This means the local components are lifts from Sp_{2n}. In particular, Π is self dual. In [11] Harris and Taylor explain how to attach to Π Galois representations. Moreover by Corollary B in [26], for every prime p there exists a continuous representation

$$\rho_p : \mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q}) \to GL_m(\bar{\mathbb{Q}}_p)$$

unramified at all primes $l \neq p, q$ such that $R_l(x)$ is the characteristic polynomial of $\rho_p(Fr_l)$, where Fr_l is the Frobenius at l, and if $p \neq q$ then the image of the inertia subgroup I_q contains the regular unipotent class implying ρ_p is irreducible.

Proposition 6.1. *If $p \neq q$ then ρ_p is defined over $\mathbb{Q}_p$.*

Proof: Let Γ be the image of ρ_p and consider the algebra $A = \mathbb{Q}_p[\Gamma] \subset M_m(\bar{\mathbb{Q}}_p)$. Then A is simple as ρ_p is irreducible. Wedderburn's theorem implies A is isomorphic to $M_r(D)$ where D is a division Algebra. The center of D is equal to the field of reduced traces of A. A is a finite simple $\mathbb{Q}_p$ algebra thus reduced traces are defined, and these are invariant by extension of scalars. The reduced trace is simply the restriction to A of the usual trace on $M_m(\bar{\mathbb{Q}}_p)$. By (3) the field of reduced traces of A is $\mathbb{Q}_p$. This follows because ρ_p factors through $G_{\mathbb{Q},\{p,q\}}$ by proposition 4.3 and by corollary 2.1 the Frobenius elements form a dense set of $G_{\mathbb{Q},\{p,q\}}$. As the image of these elements have traces on $\mathbb{Q}$, by continuity, all other elements as well. This implies that D is a central simple algebra over $\mathbb{Q}_p$. The algebra $M_r(D)$ acts on D^r from the left. This action commutes with the action of D on D^r on the right. Let $\sigma \in M_r(D)$ be an element of order 2 (the image of complex conjugation). We can decompose then D^r as a sum of the two eigenspaces for σ with eigenvalues 1 and -1 (The characteristic polynomial is a product of linear factors). Each of these two eigenspaces is a D-module for the right action of D. Hence the reduced trace of σ is a multiple of the degree of D. In [25] Taylor has shown that $Tr(\rho_p(c)) = \pm 1$, where c is complex conjugation. By computing the trace of the identity and since $A \otimes \bar{\mathbb{Q}}$ has same dimension as $M_m(\bar{\mathbb{Q}}_p)$, $D = \mathbb{Q}_p$ and $m = r$. Finally Skolem-Noether implies that $g\Gamma g^{-1}$ is inside $GL_m(\mathbb{Q}_p)$ for some g in $GL_m(\bar{\mathbb{Q}})$, it is therefore only a matter of taking a conjugation of ρ. □

In order to keep the notation simple, henceforth we use ρ_p to denote $\rho_p^{\mathbb{Q}}$.

Proposition 6.2. *If $p \neq q$ then the image of ρ_p is contained in a split orthogonal group $SO_m(\mathbb{Q}_p)$.*

Proof: The representation ρ_p is self dual, thus it has an invariant non-degenerate bilinear form. As ρ is irreducible and self-dual, then such a form is unique up to a scalar multiple. A G-invariant bilinear form is either symmetric or alternate. Since m is odd, the form has to be alternate. moreover Since ρ_p is defined over $\mathbb{Q}_p$, the orthogonal form can be re-scaled so that it is also defined over $\mathbb{Q}_p$. Finally since the determinant of $\rho_p(Fr_l) = 1$ for all primes $l \neq p, q$ and these elements are dense in the image (by the same density argument as before), the image is contained in $SO_n(\mathbb{Q}_p)$. There are two isomorphism classes of odd orthogonal groups over $\mathbb{Q}_p$, but only the split isomorphism class contains the regular unipotent conjugacy class. □

Assume now that $n = 3$. For every prime $l \neq q$ let $Q_l(y) = y^3 - a_l y^2 + b_l y - c_l$ be the palindromic reduction of $P_l(x)$, with roots $y_1^{\pm 1}, y_2^{\pm 1}, y_3^{\pm 1}$. If Π_l is a local lift from $G_2(\mathbb{Q}_l)$ then $y_1 y_2 y_3 = 1$. This imposes a condition on the coefficients of $P_l(x)$ which translates to $a_l^2 = c_l + 2b_l + 4$.

Definition 6.1. We say that Π is locally a lift from G_2 if the relation above hols for every $l \neq q$.

Corollary 6.1. *If $n = 3$ and Π is locally a lift from G_2 and $Gal(E_l/\mathbb{Q}) \cong D_6$ for one prime $r \neq q$. Let G be the Zarisky closure of the image of ρ_p. Then $G(\mathbb{Q}_p) = G_2(\mathbb{Q}_p)$ for all primes $p \neq q, r$.*

Since G acts irreducibly on the 7-dimensional representation, G is a reductive group. Also, since $a^2 = c^2 + 2b + 4$ is an algebraic condition, and $\rho_p(Fr_l)$ are dense in the image, this condition holds for all elements in G. Thus the rank of G is at most 2. The image of the inertia I_q contains the regular unipotent element. Since 1 is contained in the closure of any unipotent class, it follows that the connected component G^0 of 1 contains all the regular unipotent class. Thus G^0 is either $G_2(\mathbb{Q}_p)$ or its principal $PGL_2(\mathbb{Q}_p)$. Since these two groups are self-normalizing in $SO_7(\mathbb{Q}_p)$, it follows that $G(\mathbb{Q}_p) \cong G_2(\mathbb{Q}_l)$ or $PGL_2(\mathbb{Q}_p) \cong G_2(\mathbb{Q}_l)$. Now if the latter happens, for every $l \neq p, q$, the roots of $P(x)$ are z^i, where $-3 \leqslant i \leqslant 3$, for some $z \in \mathbb{C}^\times$.Therefore $Gal(E_l/\mathbb{Q})$ would be contained in the cyclic group C_6. Which contradicts the hypothesis $Gal(E_l/\mathbb{Q}) \cong D_6$. □

6.2 An automorphic representation on G_2

Let G be the unique form over $\mathbb{Q}$, of the exceptional Lie group of type G_2 such that $G(\mathbb{R})$ is compact and $G(\mathbb{Q}_p)$ is split for all primes p .

Savin and Gross [10] proved the existence of an (unique) automorphic representation π of $G(\mathbb{A})$ such that:

(i) $\pi_\infty \cong \mathbb{C}$

(ii) π_5 is the Steinberg Representation

(iii) π_l is unramified for all primes $l \neq 5$.

Moreover the characteristic polynomial $R_l(x)$ of the Satake parameter $s_l \in G_2(\mathbb{C})$ of π_l, acting on the 7-dimensional representation has coefficients in $\mathbb{Z}[\frac{1}{l}]$.

In [14] Lansky and Pollack have calculated the polynomials $R_l(x)$ for $l = 2$ and $l = 3$:

$$R_2(x) = x^7 + \frac{1}{4}x^6 - x^5 - \frac{13}{16}x^4 + \frac{13}{16}x^3 + x^2 - \frac{1}{4}x - 1$$

$$R_3(x) = x^7 + \frac{29}{3^3}x^6 - \frac{175}{3^5}x^5 - \frac{1099}{3^6}x^4 + \frac{1099}{3^6}x^3 + \frac{175}{3^5}x^2 - \frac{29}{3^3}x - 1$$

After factoring $R_l(x) = P_l(X)(x-1)$, the two palindromic polynomials $P_l(x)$ are reduced to:

$$Q_2(y) = y^3 + \frac{5}{4}y^2 - \frac{11}{4}y - \frac{49}{16}$$
$$Q_3(y) = y^3 - \frac{2}{3^3}y^2 - \frac{572}{3^5}y - \frac{520}{3^6}$$

If Δ_l is the discriminant of Q_l. We have the following numerical values:

$$Q_2(2) = \frac{71}{16} \qquad Q_2(-2) = \frac{-9}{16} \qquad \Delta_2 = \frac{71 \cdot 199}{2^8}$$

$$Q_3(2) = \frac{2^7 \cdot 13}{3^6} \qquad Q_3(-2) = \frac{-2^6 \cdot 7^2}{3^6} \qquad \Delta_3 = \frac{2^{14} \cdot 13 \cdot 7321}{3^16}$$

Proposition 6.3. *The local components π_2 and π_3 are tempered. The splitting fields of $P_2(x)$ and $P_3(x)$ have the Galois group isomorphic to D_6 and are algebraically independent.*

Proof: First notice that since $\Delta_l > 0$, the polynomials $Q_l(y)$ have 3 real roots, each. Since

$$\begin{aligned} Q_2'(-2) &= \frac{17}{4} > 0, & Q_3'(-2) &= \frac{2416}{3^5} > 0, & \\ Q_2'(0) &= \frac{-11}{4} < 0, & Q_3'(0) &= \frac{-572}{3^5} < 0 & \text{and} \\ Q_2'(2) &= \frac{57}{4} > 0, & Q_3'(2) &= \frac{2272}{3^5} > 0 & \end{aligned}$$

the inflection points are in the segment $(-2, 2)$. Moreover since $Q(-2) < 0$ and $Q(2) > 0$ the roots are in the segment $(-2, 2)$. This shows that the roots of $P_2(x)$ and $P_3(x)$ lie on the unit circle.

Since Δ_2 and Δ_3 are not rational squares, it follows that the Galois group of, both, $Q_2(y)$ and $Q_3(y)$ is S_3. By corollary 2.4, the Galois group of, both, $P_2(x)$ and $P_3(x)$ is isomorphic to D_6. Moreover, the two splitting fields are linearly independent by corollary 2.3. $\square$

In [10] it is also shown that π lifts to a cuspidal automorphic representation on $Sp_6(\mathbb{A})$ such that:

(1) σ_∞ is a holomorphic discrete series representation.

(2) σ_5 is the Steinberg representation.

(3) σ_l is an unramified representation, a lift from $G_2(\mathbb{Q}_l)$, for $l \neq 5$.

(4) σ_2 and σ_3 are tempered with Satake parameters given by $R_2(x)$ and $R_3(x)$.

Now Kay Magaard and Gordan Savin, using recent results from Arthur [1] lift σ to a cuspidal form on $GL_7(\mathbb{A})$.

Proposition 6.4. *Let σ be a cuspidal automorphic representation on Sp_{2n}, such that σ_q is the Steinberg representation for a prime q. Let Π be the automorphic representation of GL_{2n+1}, the lift of σ as in Theorem 1.5.2 in [1]. Then Π_q is the Steinberg Representation and Π is cuspidal. Moreover Π is a functorial lift of σ.*

Proof. [17] Proposition 8.2. □

6.3 Proof of the main theorem

Summarizing the previous two sections, there exits a cusp form on $GL_7(\mathbb{A})$ to which we can apply corollary 6.1.

Theorem 6.1. *There exists a compatible system of p-adic representations*

$$\rho_p : Gal(\bar{\mathbb{Q}}/\mathbb{Q}) \to GL_7(\mathbb{Q}_p)$$

such that for all $p \neq 5$ the Zariski closure of the image is $G_2(\mathbb{Q}_p)$.

Lemma 6.1. *There exists an infinite sequence of primes $l_1, l_2, \ldots$ such that $Gal(E_{l_j}/\mathbb{Q}) \cong D_6$ and the fields E_j are linearly independent, i.e. the composite of any n of them has degree 12^n*

Proof: We proceed by induction. The base case follows from proposition 6.3. Now suppose there are primes $l_1, l_2, \ldots l_n$ satisfying the properties of the Lemma. Let p be a prime that splits completely in the composite $E_{l_1} \cdots E_{l_n}$. Let F and K be a cubic and a quadratic étale algebras over $\mathbb{Q}_p$, respectively. Let $L = F \otimes_{\mathbb{Q}_p} K$. Let $T_{F,K}$ be the torus consisting of all $x \in L^\times$ such that $N_{L/F}(x) = N_{L/K}(x) = 1$. Every maximal torus in $G_2(\mathbb{Q}_p)$ is isomorphic to $T_{F,K}$ for some pair (F, K) and each pair arises in this way. Now assume that F is a non-Galois cubic field, and K a quadratic field not contained in the Galois closure of F. Then the Galois closure of L is a field E such that $\mathrm{Gal}(E/\mathbb{Q}_p) \cong D_6$. Let $T(\mathbb{Q}_p)$ be a maximal torus in $G_2(\mathbb{Q}_p)$ group isomorphic to $T_{F,K}(\mathbb{Q}_p)$. Then the splitting field of the characteristic polynomial of any regular element in $T(\mathbb{Q}_p)$ is E. By Proposition (7.1) in [15], the set of regular elements in $G_2(\mathbb{Q}_p)$ which are conjugated to an element in $T(\mathbb{Q}_p)$ is an open subset of $G_2(\mathbb{Q}_p)$ that contains the identity element in its closure.Also by Proposition 2 in [21], the image of ρ_p is an open subgroup of $G_2(\mathbb{Q}_p)$. Thus the two open subsets have a non-trivial intersection. Since the set of all $\rho_p(Fr_l)$ is dense in the image of ρ_p, it follows that there exists l such that $\rho_p(Fr_l)$ is conjugated to a regular element in $T(\mathbb{Q}_p)$. Since the p-adic localization of E_l is E, it is clear that $\mathrm{Gal}(E_l/\mathbb{Q}_p) \cong D_6$ and there is a unique prime in E_l dividing p. On the other hand, p splits completely in the composite $E_{l_1} \cdots E_{l_n}$. Then the intersection of the two Galois extension is $\mathbb{Q}$, which means they are linearly independent. We let this l be the next prime in the sequence. □

Theorem 6.2. *There exists an extension of* $\mathbb{Q}$ *with* $G_2(p)$ *as the Galois group, ramified at* 5 *and* p *only, for a set of primes* p *of density* 1.

Proof: Let $l \neq 5$ be a prime. The characteristic polynomial $R_l(x) \in \mathbb{Z}[\frac{1}{l}][x]$ of $\rho_p(Fr_l)$ does not depend on $p \neq l$, and call E_l its splitting field. Then by lemma 6.2 and theorem 3.2 the result follows. □

References

[1] J. Arthur. *The Endoscopic Classification of Representations Orthogonal and Symplectic Groups.* Colloquium Publications. American Mathematical Society, 2013.

[2] M. Aschbacher. Chevalley groups of type g2 as the group of a trilinear form. *Journal of Algebra*, 109(1):193 – 259, 1987.

[3] A. Borel, W. Casselman, Symposium in Pure Mathematics, B. Casselman, and American Mathematical Society. *Automorphic Forms, Representations and L-Functions: Automorphic Forms, Representations and L-functions.* Automorphic Forms, Representations, and L-functions. American Mathematical Society, 1979.

[4] N. Bourbaki. *Lie Groups and Lie Algebras: Chapters 7-9.* Number pts. 7-9 in Elements of mathematics. Springer Berlin Heidelberg, 2004.

[5] P. Cartier. Representations of p-adic groups: a survey. 1977.

[6] J.W.S. Cassels and A. Fröhlich. *Algebraic Number Theory: Proceedings of an Instructional Conference Organized by the London Mathematical Society (a NATO Advanced Study Institute) with the Support of the International Mathematical Union.* London Mathematical Society, 2010.

[7] D.L. Cohn. *Measure Theory: Second Edition.* Birkhäuser Advanced Texts Basler Lehrbücher. Springer New York, 2013.

[8] B. Conrad and B. Gross. Non-split reductive groups over z. *Autour des schémas en groupes. Vol. II, Panor. Synthèses*, 46, 05 2012.

[9] D. Flath. Decomposition of representations into tensor products. *Proc. Sympos. Pure Math.*, 33, 01 1979.

[10] B. Gross and G. Savin. Motives with galois group of type g_2: an exceptional theta-correspondence. *Compositio Mathematica*, 114(2):153–217, 1998.

[11] M. Harris, R. Taylor, and V.G. Berkovich. *The Geometry and Cohomology of Some Simple Shimura Varieties. (AM-151).* Princeton University Press, 2001.

[12] G. Henniart and M-F. Vigneras. A satake isomorphism for representations modulo p of reductive groups over local fields. *Journal fur die Reine und Angewandte Mathematik*, 2015:33–75, 04 2015.

[13] G. Karpilovsky. *Topics in Field Theory*. Number no. 155 in Developments in Water Science. North-Holland, 1989.

[14] J. Lansky and D. Pollack. Hecke algebras and automorphic forms. *Compositio Mathematica*, 130(1):21–48, 2002.

[15] M. Larsen. On ‘-independence of algebraic monodromy groups in compatible systems of representations. 1992.

[16] M. Lopuhaä-Zwakenberg. Integral models of reductive groups and integral mumford-tate groups, 2017.

[17] K. Magaard and G. Savin. Computing finite galois groups arising from automorphic forms, 2014.

[18] J. S. Milne. *Algebraic Groups: The Theory of Group Schemes of Finite Type over a Field*. Cambridge Studies in Advanced Mathematics. Cambridge University Press, 2017.

[19] J. Neukirch. *Class Field Theory*. Grundlehren der mathematischen Wissenschaften. Springer Berlin Heidelberg, 1985.

[20] J. Neukirch and N. Schappacher. *Algebraic Number Theory*. Grundlehren der mathematischen Wissenschaften. Springer Berlin Heidelberg, 2013.

[21] J-P. Serre. Sue les groupes de galois attaches aux groupes p-divisibles. 01 2003.

[22] T. Springer and F. Veldkamp. *Octonions, Jordan algebras and exceptional groups. Revised English version of the original German notes.* 01 2000.

[23] T. A. Springer. Review: Roger w. carter, finite groups of lie type. conjugacy classes and complex characters. *Bull. Amer. Math. Soc. (N.S.)*, 17(1):145–148, 07 1987.

[24] R. Steinberg. Regular elements of semi-simple algebraic groups. *Publications Mathématiques de l'IHÉS*, 25:49–80, 1965.

[25] R. Taylor. The image of complex conjugation in l-adic representations associated to automorphic forms. *Algebra Number Theory*, 6:405–435, 2012.

[26] R. Taylor and T. Yoshida. Compatibility of local and global langlands correspondences. *Journal of the American Mathematical Society*, 20:467–493, 2004.

[27] P. Webb. *Representations, Maschke's Theorem, and Semisimplicity*, page 1–14. Cambridge Studies in Advanced Mathematics. Cambridge University Press, 2016.

[28] R. Wilson. *The Finite Simple Groups*. Graduate Texts in Mathematics. Springer London, 2009.