Special Frobenius Traces in Galois Representations

Thesis by

Liubomir Chiriac

In Partial Fulfillment of the Requirements

for the Degree of

Doctor of Philosophy

California Institute of Technology

Pasadena, California

2015

(Defended May 26, 2015)

To my family

Acknowledgments

The greatest intellectual debt I owe is to my advisor, Dinakar Ramakrishnan. The vast majority of the ideas in this thesis were born during our numerous discussions, which have taught me more than any paper or textbook I have read. This work would not have been possible without his continuous input, at every step of my mathematical journey at Caltech.

During my time as a graduate student I have benefited a great deal from interacting with a number of people. I would like to thank Michael Aschbacher for many valuable suggestions and comments, especially on Chapter 2 of my thesis. Special thanks are due to Andrei Jorza for helpful conversations on various occasions that led to improvements in the final draft. I would also like to acknowledge an active exchange of ideas with Iurie Boreico and Hadi Hedayatzadeh.

I am eternally grateful to my parents, Eugenia and Liubomir Chiriac, for their unwavering love, support and encouragement since the day I was born. I am truly blessed to have them in my life and I love them with all my heart.

Finally, it is with immense pleasure that I thank my beloved wife, Natalia, for her candid smile that lightens up my world every day.

Abstract

This thesis studies Frobenius traces in Galois representations from two different directions. In the first problem we explore how often they vanish in Artin-type representations. We give an upper bound for the density of the set of vanishing Frobenius traces in terms of the multiplicities of the irreducible components of the adjoint representation. Towards that, we construct an infinite family of representations of finite groups with an irreducible adjoint action.

In the second problem we partially extend for Hilbert modular forms a result of Coleman and Edixhoven that the Hecke eigenvalues a_p of classical elliptical modular newforms f of weight 2 are never extremal, i.e., a_p is strictly less than $2\sqrt{p}$. The generalization currently applies only to prime ideals $\mathfrak{p}$ of degree one, though we expect it to hold for $\mathfrak{p}$ of any odd degree. However, an even degree prime can be extremal for f. We prove our result in each of the following instances: when one can move to a Shimura curve defined by a quaternion algebra, when f is a CM form, when the crystalline Frobenius is semi-simple, and when the strong Tate conjecture holds for a product of two Hilbert modular surfaces (or quaternionic Shimura surfaces) over a finite field.

Contents

Chapter 1

Introduction

The study of Galois representations coming from arithmetic geometry is of primary importance in modern number theory. In particular, the traces of the images of the Frobenius elements under these representations carry a wealth of information that can be examined in various contexts. The focus of this thesis is to investigate two types of Frobenius traces of special nature: (i) those that vanish and (ii) the ones that are extremal.

The first question we consider is how often the traces of Frobenius vanish. In other words, we are interested in the density of the set $\Sigma = \{v \mid a_v = 0\}$, where v is a finite place of a field F and $a_v = \operatorname{tr} \rho(\mathrm{Frob}_v)$ for an irreducible representation ρ of the Galois group $\Gamma_F = \mathrm{Gal}(\overline{F}/F)$.

One motivation for considering this problem comes from a paper by Serre ([30], Prop. 16), where he treats the case of ℓ-adic Galois representations. If n is the dimension of such an irreducible representation ρ, he provides a sharp upper bound of $1 - 1/n^2$ for the density of Σ. He raises a similar question on the automorphic side, which was recently studied by Walji [36].

For Artin-type representations we can give a density estimate independent of the dimension n, once we assume that the adjoint action is irreducible. More precisely, denote by Ad the composition of the natural projection of

GL_n onto PGL_n with the (n^2-1)-dimensional adjoint representation. Under the assumption that $\mathrm{Ad}(\rho)$ is irreducible, we show that in finite Galois groups the Frobenius traces are nonzero for at least half of the primes.

In this context, the question naturally arises as to whether for every n there exists a finite group G and an n-dimensional irreducible complex representation ρ of G such that its adjoint is irreducible. Following an idea of M. Aschbacher, for every prime power n, we construct a representation ρ of degree n such that $\mathrm{Ad}(\rho)$ irreducible. All this is explained in Chapter 2, which is a detailed version of the author's article [8].

The main results of Chapter 2 (Theorem 2.1.1 and Theorem 2.1.2) can be summarized as follows:

Theorem A. *Let p be a prime and $n = p^r$, for some integer $r \geq 1$. There exists a number field F and an n-dimensional irreducible $\mathbb{C}$-representation ρ of the absolute Galois group Γ_F such that:*

(i) $\mathrm{Ad}(\rho)$ *is irreducible.*

(ii) *The image of Γ_F under ρ is the normalizer of a Heisenberg p-group H, and there is a surjection $\Gamma_F \twoheadrightarrow \mathrm{Sp}_{2r}(\mathbb{F}_p)$ whose kernel is H times its centralizer.*

(iii) *The set*

$$\Sigma = \{v \text{ finite place of } F \mid a_v = 0\}$$

has density at most 1/2.

Theorem 2.1.1 furnishes examples of non essentially self-dual representations, whereas many known examples of Galois representations coming from arithmetic geometry tend to be essentially self-dual. In general, without any

restrictions on $\mathrm{Ad}(\rho)$, Theorem 2.1.2 gives an upper bound for the density of Σ in terms of the multiplicities of the irreducible constituents of $\mathrm{Ad}(\rho)$.

The second part of our thesis is concerned with the non-existence of extremal Frobenius traces in Galois representations. The first interesting examples outside those with finite image are given by the representations associated to Hilbert modular forms of weight $k \geq 2$. To explain the notion of extremality we need to introduce some notation.

Let ρ be a 2-dimensional Galois representation attached to a Hilbert modular newform f of parallel weight k and trivial character. For any prime ideal $\mathfrak{p}$ at which ρ is unramified, we have

$$\operatorname{tr}\rho(\mathrm{Frob}_{\mathfrak{p}}) = a_{\mathfrak{p}} \text{ and } \det\rho(\mathrm{Frob}_{\mathfrak{p}}) = N(\mathfrak{p})^{k-1},$$

where $a_{\mathfrak{p}}$ is the Fourier coefficient of f at $\mathfrak{p}$ and $N(\mathfrak{p})$ is the norm of $\mathfrak{p}$. Since the roots of the Hecke polynomial $x^2 - a_{\mathfrak{p}}x + N(\mathfrak{p})$ have absolute value equal to $N(\mathfrak{p})^{(k-1)/2}$, one knows that

$$|a_{\mathfrak{p}}| \leq 2N(\mathfrak{p})^{(k-1)/2}.$$

We call $a_{\mathfrak{p}}$ extremal if the previous relation is in fact an equality, i.e., if the Hecke polynomial has a double root. Further, by the degree of $\mathfrak{p}$ we mean the exponent in $N(\mathfrak{p})$ of the rational prime below it.

When f is classical cuspidal normalized eigenform of weight 2, Coleman and Edixhoven [9] prove that a_p is never extremal. Moreover, modulo a semi-simplicity hypothesis, they show a similar result for higher weight forms. Another observation they make concerns the case $k = 1$, where Chebotarev's density theorem implies the existence of infinitely many primes p at which

$\rho(\mathrm{Frob}_p)$ is the identity, so the Hecke polynomial has a double root at 1.

The object of Chapter 3 is to extend their result for Hilbert modular forms of weight $k = 2$. It is important to note that this generalization applies at the moment only to primes $\mathfrak{p}$ of degree one, though we expect it to hold for any $\mathfrak{p}$ of odd degree. As it turns out, if the degree of $\mathfrak{p}$ is even then the Hecke polynomial at $\mathfrak{p}$ may have a double root (see section 3.3.1).

The cases in which we prove the non-extremality of the $a_\mathfrak{p}$ coefficients are explained below.

Theorem B. *Let F be a totally real number field of degree n over $\mathbb{Q}$. Let f be a normalized Hilbert cuspidal eigenform for F of parallel weight 2, level $\mathfrak{n}$ and trivial character. Denote by π the automorphic representation generated by f. Then for any degree one prime $\mathfrak{p} \nmid \mathfrak{n}$ the Hecke polynomial*

$$x^2 - a_\mathfrak{p} x + N(\mathfrak{p})$$

has distinct roots, if any of the following conditions hold:

(i) *n is odd.*

(ii) *n is even and there exists a finite place v at which π_v is square integrable.*

(iii) *f is a CM form.*

(iv) *The crystalline Frobenius ϕ is semi-simple.*

(v) *The strong Tate conjecture is true for a product of two Hilbert modular surfaces (or quaternionic Shimura surfaces) over a finite field.*

We remark that part (iv) is implied by part (v), whereas the weak Tate conjecture does not suffice to obtain semi-simplicity. For divisors (algebraic cycles of codimension one) it is known that the strong form of the Tate conjecture is equivalent to the weak form, which asserts that all Tate classes are algebraic (cf. Ulmer [34], Prop. 9.4). In this case, the Tate conjecture for Hilbert modular surfaces of a finite field was proved by Langer ([21], [22]).

The strong Tate conjecture for a product of two Hilbert modular surfaces over a solvable number field is also known (at least for non-CM motives; see Virdol [35]). However, the analogous situation over finite fields is more subtle, since typically there are more Tate classes to consider in that case.

Finally, we note that the non semi-simplicity of Frobenius restricts the number of Tate classes. Therefore, if by geometry one could produce enough algebraic cycles, the weak Tate conjecture may be established, which is an interesting result of independent interest.

Chapter 2

Irreducible adjoint representations in prime power dimensions

2.1 Introduction

Let $n \geq 2$ be an integer. Consider the representation

$$\mathrm{Ad} : \mathrm{GL}_n(\mathbb{C}) \to \mathrm{GL}_{n^2-1}(\mathbb{C}),$$

obtained by composing the natural projection of $\mathrm{GL}_n(\mathbb{C})$ onto $\mathrm{PGL}_n(\mathbb{C})$ with the (n^2-1)-dimensional adjoint representation of $\mathrm{PGL}_n(\mathbb{C})$. Henceforth, given a representation ρ, we shall to refer to $\mathrm{Ad}(\rho)$ as the adjoint of ρ. The main question we address is whether for every n there exists a finite group G and an n-dimensional irreducible $\mathbb{C}$-representation (ρ, V) of G such that $\mathrm{Ad}(\rho)$ is irreducible. We will then apply our conclusion to Galois representations of Artin-type, i.e., those having finite image.

This chapter is a detailed version of the author's paper [8].

For $n \leq 4$ we find all the groups G with the required property using Blichfeldt's classifications (cf. [7]) of the finite subgroups of $\mathrm{PGL}_n(\mathbb{C})$ for $n \leq 4$. In Proposition 2.3.1 we show that if $n = 2$ then $\mathrm{Ad}(\rho) = \mathrm{Sym}^2(\rho) \otimes \det(\rho)^{-1}$ is irreducible unless ρ is of cyclic or dihedral type. In Proposition 2.3.2 we prove that for $n = 3$, $\mathrm{Ad}(\rho)$ is irreducible in precisely four cases; two of which yield simple groups and the remaining two yield solvable groups. Similarly, Proposition 2.3.3 shows that for $n = 4$ there are two instances when $\mathrm{Ad}(\rho)$ is irreducible. Note that for $n \geq 3$, $\mathrm{Ad}(\rho)$ will be reducible if ρ were essentially self-dual. On the other hand, many examples of Galois representations coming from arithmetic geometry tend to be essentially self-dual.

If we restrict our attention to quasisimple groups G (i.e., perfect central extensions of simple groups), then there is a complete answer in a paper of Magaard, Malle and Tiep [24] to whether there are irreducible representations ρ of G with $\mathrm{Ad}(\rho)$ irreducible. As it turns out, the only infinite family of examples are the Weil representations for $\mathrm{SU}_n(\mathbb{F}_2)$ and $\mathrm{Sp}_{2n}(\mathbb{F}_3)$ of degrees $(2^n - (-1)^n)/3$ and $(3^n - (-1)^n)/2$, respectively (see also [25]). This will not provide examples in the generic prime power case, forcing us to consider more general groups.

We also mention that if we do not require the irreducibility of $\mathrm{Ad}(\rho)$, then the prime power degree $\mathbb{C}$-representations ρ of quasisimple groups have been classified, partially by Malle and Zalesskii [26], where they omit the alternating groups and their double covers, and completed by Balog, Bessenrodt, Olsson and Ono [4] (for alternating groups) and Bessenrodt and Olsson [5] (for their double covers). The generic examples of such representations are given by the Steinberg characters of finite groups of Lie type.

In general, following a suggestion of Michael Aschbacher, we construct an infinite family of representations of prime power degree with irreducible adjoint representations. In this case, the groups G are taken to be the normalizers of certain extraspecial groups (the analogue of the Heisenberg groups over finite fields). More precisely, we establish the following:

Theorem 2.1.1. *Let $p \geq 3$ be a prime, r a positive integer, and P an extraspecial group of order p^{2r+1} and exponent p. Let (ρ, V) be an irreducible $\mathbb{C}$-representation of degree p^r of P, which is necessarily faithful. If G is the normalizer in $\mathrm{SL}(V)$ of P then $\mathrm{Ad}(\rho)$ is an irreducible representation of G.*

Note that this gives new cases of prime power dimensions where G is not quasisimple. Moreover, due to the geometric nature of the Heisenberg groups, we remark that for some values of p, the groups G constructed above are known to have geometric interpretations. For instance, when $p = 5$ and $r = 1$, Decker [10] has proved that the group G is the full symmetry group of the Horrocks-Mumford bundle constructed in [17], which is an indecomposable rank 2 bundle on $\mathbb{P}^4$. In addition, for $p = 3$ and $r = 1$, as noted in [1], the image of G in PGL_3 is the group of projective automorphisms preserving the one-dimensional linear system of plane cubic curves in $\mathbb{P}^2$ given by

$$t_0(x^3 + y^3 + z^3) + t_1 xyz = 0, (t_0, t_1) \in \mathbb{P}^1.$$

Since every finite group appears as a Galois group over a number field F, our construction furnishes examples of non essentially self-dual representations of the absolute Galois groups G_F (for suitable number fields). Given a continuous Galois $\mathbb{C}$-representation ρ of G_F, for any finite place v at which ρ is unramified, consider the Frobenius class Frob_v attached to v, and denote by a_v the trace of $\rho(\mathrm{Frob}_v)$. The interest in $\mathrm{Ad}(\rho)$ stems from the following result:

Theorem 2.1.2. *Let (ρ, V) be a continuous irreducible n-dimensional complex representation of the absolute Galois group G_F of a number field F. Let $\sum_{i=1}^{N} m_i\sigma_i$ be the decomposition of $\mathrm{Ad}(\rho)$ into irreducible components σ_i, such that $\sigma_i \not\cong \sigma_j$ if $i \neq j$, $1 \leq i, j \leq N$. Then the density $\delta(\Sigma)$ of the set Σ of places $\{v \text{ finite} \mid a_v = 0\}$ satisfies*

$$\delta(\Sigma) \leq 1 - \frac{1}{1 + \sum_{i=1}^{N} m_i^2}.$$

In particular, if $\mathrm{Ad}(\rho)$ is irreducible then $\delta(\Sigma) \leq 1/2$.

Note that this is independent of the dimension n of the representation ρ, which contrasts well with the sharp upper bound of $1 - 1/n^2$ given by Serre in [30] for ℓ-adic Galois representations.

After completing [8], the author learned of a paper of Guralnick and Tiep [14] that, in effect, contains Theorem 2.1.1, albeit arranged in a different way and studied in a different context. Our focus is on the application Theorem 2.1.2 to lacunarity.

2.2 Preliminaries

An initial observation shows that if $\rho^\vee$ is the dual representation of ρ then $\rho \otimes \rho^\vee$ is an n^2-dimensional representation that contains the trivial representation. Moreover, by Schur's Lemma, ρ is irreducible if and only if $\rho \otimes \rho^\vee$ contains the trivial representation $\mathbf{1}$ with multiplicity one. In fact, one knows that

$$\mathrm{End}(\rho) \cong \rho \otimes \rho^\vee = \mathbf{1} \oplus \mathrm{Ad}(\rho).$$

Lemma 2.2.1. *Given an irreducible representation (ρ, V), its adjoint $\mathrm{Ad}(\rho)$ is irreducible if and only if both its symmetric square $\mathrm{Sym}^2(\rho)$ and its alternating square $\Lambda^2(\rho)$ are irreducible.*

Proof. As noticed above, ρ is irreducible if and only if $\mathbf{1}$ is not contained in $\mathrm{Ad}(\rho)$, so $\mathrm{Ad}(\rho)$ is irreducible if and only if $\mathbf{1}$ is not contained in $\mathrm{Ad}(\mathrm{Ad}(\rho))$. However, $\mathrm{Ad}(\rho)$ is readily seen to be self-dual, since $\rho \otimes \rho^\vee$ and $\mathbf{1}$ are. Therefore,

$$\mathrm{Ad}(\rho)^{\otimes 2} = \mathrm{Ad}(\rho) \otimes \mathrm{Ad}(\rho)^\vee = \mathbf{1} \oplus \mathrm{Ad}(\mathrm{Ad}(\rho)).$$

Consider

$$\sigma = (\rho \otimes \rho^\vee) \otimes (\rho \otimes \rho^\vee).$$

On one hand, we get

$$\sigma = (\mathbf{1} \oplus \mathrm{Ad}(\rho))^{\otimes 2} = \mathbf{1} \oplus \mathrm{Ad}(\rho)^{\oplus 2} \oplus \mathrm{Ad}(\rho)^{\otimes 2}.$$

This shows that $\mathrm{Ad}(\rho)$ is irreducible if and only if $\mathbf{1}$ is contained in σ with multiplicity 2, i.e., $\dim \mathrm{Hom}_G(\mathbf{1}, \sigma) = 2$.

On the other hand, we can write

$$\sigma = (\rho \otimes \rho) \otimes (\rho \otimes \rho)^\vee = (\mathrm{Sym}^2(\rho) \oplus \Lambda^2(\rho)) \otimes (\mathrm{Sym}^2(\rho) \oplus \Lambda^2(\rho))^\vee,$$

which implies that $\dim \mathrm{Hom}_G(\mathbf{1}, \sigma)$ is greater than or equal to

$$\dim \mathrm{Hom}_G(\mathbf{1}, \mathrm{Sym}^2(\rho) \otimes (\mathrm{Sym}^2(\rho))^\vee) + \dim \mathrm{Hom}_G(\mathbf{1}, \Lambda^2(\rho) \otimes (\Lambda^2(\rho))^\vee) \geq 2.$$

The equality takes place if and only if both $\mathrm{Sym}^2(\rho)$ and $\Lambda^2(\rho)$ are irreducible, so the conclusion follows. □

Recall that a representation ρ is said to be essentially self-dual if $\rho^\vee = \rho \otimes \chi$, for some character χ. Note than when ρ is essentially self-dual there is a direct sum decomposition

$$\rho \otimes \rho^\vee = \mathrm{Sym}^2(\rho) \otimes \chi \oplus \Lambda^2(\rho) \otimes \chi.$$

Since $\dim \Lambda^2(\rho) = \frac{n(n-1)}{2}$ it follows that if $n \geq 3$ and ρ is essentially self-dual then $\mathrm{Ad}(\rho)$ is reducible. Therefore, for $n \geq 3$ the irreducibility of $\mathrm{Ad}(\rho)$ forces ρ to be non essentially self-dual (i.e., ρ is not essentially self-dual).

2.2.1 Primitivity

Recall that an irreducible representation (ρ, V) of G is called *imprimitive* if V can be written as a direct sum

$$V = V_1 \oplus \cdots \oplus V_m$$

for $m > 1$ subspaces V_i (forming a system of imprimitivity), on which G acts transitively. We call V *primitive*, if it is not imprimitive. We shall prove that primitivity is a necessary condition for $\mathrm{Ad}(\rho)$ to be irreducible.

The next known lemma (cf. [19]) shows how imprimitive representations can be viewed as inductions.

Lemma 2.2.2. *(a) Let H be a proper subgroup of G and let (σ, W) be a representation of H. Then the induced representation $\mathrm{Ind}_H^G(W)$ is imprimitive.*

(b) Every imprimitive representation (ρ, V) of G is induced from a representation of a proper subgroup H of G.

Proof. (a) Let $m > 1$ be the index $[G : H]$ and $T = \{t_1, \ldots, t_m\}$ be a (left) transversal for H in G. Then

$$\mathrm{Ind}_H^G(W) = (t_1 \otimes W) \oplus \cdots \oplus (t_m \otimes W).$$

Now for any $g \in G$, and any fixed $1 \leq i \leq m$, pick t_j such that $g(t_i H) = t_j H$. Then we have that $g(t_i \otimes W) = t_j \otimes W$, so $\{t_1 \otimes W, \ldots t_m \otimes W\}$ is a system of imprimitivity for $\mathrm{Ind}_H^G(W)$ and the action of G is transitive.

(b) Write $V = V_1 \oplus \cdots \oplus V_m$, and let $H := \{g \in G : gV_1 = V_1\}$ be the stabilizer of V_1. Since the action of G is transitive it follows that $m = [G : H]$, so we can choose a transversal $T = \{t_1, \ldots, t_m\}$ for H such that $V_i = t_i V_1$ $(1 \leq i \leq m)$ and

$$V = t_1 V_1 \oplus \ldots t_m V_m.$$

For $v_1, \ldots, v_m \in V_1$, the map f given by

$$f : \sum_{i=1}^{m} t_i \otimes v_i \mapsto \sum_{i=1}^{m} t_i v_i$$

is an isomorphism of $\mathrm{Ind}_H^G(V_1)$ onto V.

Moreover, note that f is also a G-equivariant map. Indeed, for $g \in G$ and $t_i \in T$, there exist uniquely determined $t_j \in T$ and $h \in H$ such that $gt_i = t_j h$. Then

$$\begin{aligned} f(g(t_i \otimes v_i)) &= f(t_j h \otimes v_i) = f(t_j \otimes h v_i) = t_j h v_i \\ &= g t_i v_i = g f(t_i \otimes v_i). \end{aligned}$$

In conclusion, f is a G-equivariant isomorphism and therefore $\mathrm{Ind}_H^G(V_1) \simeq V$. $\square$

Proposition 2.2.3. *Let (ρ, V) be an irreducible representation of G such that* $\mathrm{Ad}(\rho)$ *is irreducible. Then (ρ, V) is primitive.*

Proof. Suppose that V is imprimitive. Then by Lemma 2.2.2: $\rho = \mathrm{Ind}_H^G(\tau)$ for some proper subgroup H of G, and a representation τ of H. As a result

$$\rho \otimes \rho^\vee = \mathrm{Ind}_H^G(\tau) \otimes \mathrm{Ind}_H^G(\tau^\vee) = \mathrm{Ind}_H^G\left(\mathrm{Res}_G^H(\mathrm{Ind}_H^G(\tau)) \otimes \tau^\vee\right),$$

where for the second equality we have used the push-pull formula:

$$\sigma_1 \otimes \mathrm{Ind}\,\sigma_2 = \mathrm{Ind}(\mathrm{Res}(\sigma_1) \otimes \sigma_2).$$

By Mackey's Decomposition Theorem we know that

$$\mathrm{Res}_G^H(\mathrm{Ind}_H^G(\tau)) = \bigoplus_{s \in H\backslash G/H} \mathrm{Ind}_{H \cap sHs^{-1}}^H(\tau^s),$$

where s runs through a set of representatives of (H, H) double coset of G and $\tau^s(h)$ is defined to be $\tau(s^{-1}hs)$, for $h \in H$. Hence

$$\rho \otimes \rho^\vee = \bigoplus_{s \in H\backslash G/H} \mathrm{Ind}_H^G\left(\mathrm{Ind}_{H \cap sHs^{-1}}^H(\tau^s) \otimes \tau^\vee\right).$$

Using s as the identity in the above summation, we note that the induction is reducible, so in order for $\mathrm{Ad}(\rho)$ to be irreducible there can be no more summands, i.e, $|H\backslash G/H| = 1$. However, since G is the disjoint union of HsH for $s \in H\backslash G/H$, it follows that $G = H$, which contradicts the assumption that H is a proper subgroup. □

2.3 Low dimensions

2.3.1 The case $n = 2$

Let $\mathfrak{sl}_2(\mathbb{C})$ be the 3-dimensional Lie algebra of 2×2 matrices with trace zero, and let

$$\left\{ \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}, \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}, \begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix} \right\}$$

be an ordered basis for $\mathfrak{sl}_2(\mathbb{C})$. The group $\mathrm{GL}_2(\mathbb{C})$ acts on $\mathfrak{sl}_2(\mathbb{C})$ by conjugation, and the corresponding representation can be explicitly described (with respect to the chosen basis) as

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \mapsto \frac{1}{ad - bc} \begin{pmatrix} ad + bc & -ac & bd \\ -2ab & a^2 & -b^2 \\ 2cd & -c^2 & d^2 \end{pmatrix}.$$

The kernel of this representation is composed only of the scalar matrices, so the representation factors through

$$\mathrm{GL}_2(\mathbb{C})/\mathbb{C}^\star \cong \mathrm{PGL}_2(\mathbb{C}).$$

Hence, the aforementioned representation is the 3-dimensional adjoint representation

$$\mathrm{Ad} : \mathrm{GL}_2(\mathbb{C}) \to \mathrm{GL}_3(\mathbb{C}).$$

Moreover, $\mathrm{GL}_2(\mathbb{C})$ also acts on the space of 2×2 symmetric matrices by

$$g \cdot x = gxg^t,$$

where $g \in GL_2(\mathbb{C})$, g^t is its transpose, and x is a symmetric 2×2 matrix.

This action with respect to the ordered basis

$$\left\{ \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} \right\}$$

is given by

$$\mathrm{Sym}^2 \colon \begin{pmatrix} a & b \\ c & d \end{pmatrix} \mapsto \begin{pmatrix} ad+bc & ac & bd \\ 2ab & a^2 & b^2 \\ 2cd & c^2 & d^2 \end{pmatrix}.$$

Thus, in fact, Ad and $\mathrm{Sym}^2 \otimes \det^{-1}$ are equivalent representations.

For an irreducible 2-dimensional representation $\rho : G \to \mathrm{GL}_2(\mathbb{C})$, the projective image $\overline{G}$ is a finite subgroup of $\mathrm{PGL}_2(\mathbb{C}) \cong \mathrm{SO}_3(\mathbb{C})$. The group $\mathrm{SO}_3(\mathbb{C})$ has five finite subgroups: the cyclic group C_n, the dihedral group D_n, the tetrahedral group A_4, the octahedral group S_4, and the icosahedral group A_5.

Proposition 2.3.1. *Let $\rho : G \to \mathrm{GL}_2(\mathbb{C})$ be an irreducible 2-dimensional representation of a finite group G, and let $\overline{G}$ be its projective image in $\mathrm{PGL}_2(\mathbb{C})$. Then $\mathrm{Ad}(\rho)$ is irreducible if and only if $\overline{G} \simeq A_4, S_4$ or A_5.*

Proof. We rule out C_n and D_n since these groups do not have 3-dimensional irreducible representations. The group A_4 has three 1-dimensional and one 3-dimensional irreducible representations. Thus $\mathrm{Ad}(\rho)$ is the unique irreducible 3-dimensional representations (as the trivial representation is not contained in $\mathrm{Ad}(\rho)$). The irreducibility of $\mathrm{Ad}(\rho)$ when $\overline{G} = S_4$ follows by restricting to the normal subgroup A_4.

Finally, A_5 has one 1-dimensional, two 3-dimensional, one 4-dimensional and one 5-dimensional irreducible representations. Hence any 3-dimensional representation, and in particular $\mathrm{Ad}(\rho)$, must be irreducible. □

2.3.2 The case $n = 3$

Here we make use of Hambleton and Lee's modern geometric account ([16]) of Blichfeldt's classification for the finite subgroups of $\mathrm{PGL}_3(\mathbb{C})$ ([7]). Using the primitivity condition proved in the previous section, we can restrict our attention to the primitive subgroups only. There are three primitive simple subgroups of $\mathrm{PGL}_3(\mathbb{C})$, namely: $A_5, \mathrm{PSL}_2(\mathbb{F}_7)$ and A_6. The remaining three primitive subgroups of $\mathrm{PGL}_3(\mathbb{C})$ are all solvable. We describe them in terms of the following 3×3 matrices in $\mathrm{GL}_3(\mathbb{C})$:

$$S = \begin{pmatrix} 1 & 0 & 0 \\ 0 & \omega & 0 \\ 0 & 0 & \omega^2 \end{pmatrix} \ (\omega^3 = 1) \ , U = \begin{pmatrix} \epsilon & 0 & 0 \\ 0 & \epsilon & 0 \\ 0 & 0 & \epsilon\omega \end{pmatrix} \ (\epsilon^3 = \omega^2) \ ,$$

$$T = \begin{pmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ 1 & 0 & 0 \end{pmatrix}, \ V = \frac{1}{\sqrt{-3}} \begin{pmatrix} 1 & 1 & 1 \\ 1 & \omega & \omega^2 \\ 1 & \omega^2 & \omega \end{pmatrix}.$$

With this notation, the primitive, solvable subgroups of $\mathrm{PGL}_3(\mathbb{C})$ are:

(i) G_{216}, the Hessian group of order 216, generated by S, T, V, U;

(ii) G_{72}, a subgroup of G_{216} of order 72, generated by S, T, V, UVU^{-1};

(iii) G_{36}, a subgroup of G_{216} of order 36, generated by S, T, V.

Proposition 2.3.2. *Let $\rho : G \to \mathrm{GL}_3(\mathbb{C})$ be an irreducible 3-dimensional representation of a finite group G, and let $\overline{G}$ be its projective image in $\mathrm{PGL}_3(\mathbb{C})$. Then $\mathrm{Ad}(\rho)$ is irreducible if and only if $\overline{G} \simeq \mathrm{PSL}_2(\mathbb{F}_7), A_6, G_{72}$ or G_{216}.*

Proof. As we have already seen, the icosahedral group A_5 has no irreducible 8-dimensional representations. The group $\mathrm{PSL}_2(\mathbb{F}_7)$ has one 1-dimensional, two

3-dimensional, one 6-dimensional, one 7-dimensional and one 8-dimensional irreducible representations. The trivial representation is not contained in $\mathrm{Ad}(\rho)$, so $\mathrm{Ad}(\rho)$ is irreducible. Finally, the Valentiner group A_6 has one 1-dimensional, two 5-dimensional, two 8-dimensional, one 9-dimensional, and one 10-dimensional irreducible representations. Thus $\mathrm{Ad}(\rho)$ is irreducible in this case.

For the remaining three groups (which are all solvable) we use [13] to investigate their character tables. The group G_{36} has four 1-dimensional representations and two 4-dimensional irreducible representations, hence $\mathrm{Ad}(\rho)$ must be the sum of the two 4-dimensional irreducible representations. The character table of G_{72} shows that it has four 1-dimensional representations, one 2-dimensional irreducible representation and one 8-dimensional irreducible representation. By the aforementioned arguments, $\mathrm{Ad}(\rho)$ is induced from either of the two 4-dimensional representations of the normal subgroup G_{36} and therefore $\mathrm{Ad}(\rho)$ is irreducible. Likewise, G_{216} has four 1-dimensional representations, one 2-dimensional representation, eight 3-dimensional representations, two 6-dimensional representations, and one 8-dimensional representation. It is not hard to see that $\mathrm{Ad}(\rho)$ is induced from non-normal extensions of degrees 4 and 8, and it is irreducible. □

2.3.3 The case $n = 4$

We refer to the list of the finite primitive subgroups of $\mathrm{PGL}_4(\mathbb{C})$ given by Blichfeldt in [7]. The simple groups on this list are $A_5, A_6, A_7, \mathrm{PSL}_2(\mathbb{F}_7)$ and $\mathrm{PSp}_4(\mathbb{F}_3)$. We remark that all the solvable groups on the list are mapped by ρ into either $\mathrm{GO}_4(\mathbb{C})$ or $\mathrm{GSp}_4(\mathbb{C})$, i.e., ρ is either orthogonal or symplectic.

Proposition 2.3.3. *Let $\rho : G \to \mathrm{GL}_4(\mathbb{C})$ be an irreducible 4-dimensional representation of a finite group G, and let $\overline{G}$ be its projective image in $\mathrm{PGL}_4(\mathbb{C})$. Then $\mathrm{Ad}(\rho)$ is irreducible if and only if $\overline{G} \simeq A_7$ or $\mathrm{PSp}_4(\mathbb{F}_3)$.*

Proof. We first show that if ρ is either orthogonal or symplectic then ρ is self-dual. Indeed, given an action of G on a quadratic (or symplectic) vector space W we have an action of G on the dual space $W^\vee$ given by

$$(gf)(x) = f(g^{-1}x),$$

for all $g \in G, f \in W^\vee, x \in W$. Any bilinear form $\beta : W \times W \to \mathbb{C}$ induces an isomorphism $\phi : W \to W^\vee$ given by

$$x \mapsto (\phi_x : y \mapsto \beta(x, y)), y \in W.$$

Since $\beta(gx, gy) = \beta(x, y)$ it follows that ϕ is a G-equivariant isomorphism and hence the action of G is self-dual. However, we know from Section 2.2 that $\mathrm{Ad}(\rho)$ must be reducible in this case. Thus, $\mathrm{Ad}(\rho)$ cannot be irreducible if $\overline{G}$ is solvable.

The three simple groups, A_5, A_6 and $PSL_2(\mathbb{F}_7)$ have no irreducible 15-dimensional representations. The group A_7 has one 1-dimensional, one 6-dimensional, two 10-dimensional, two 14-dimensional, one 15-dimensional, one 21-dimensional and one 35-dimensional irreducible representations, so in this case $\mathrm{Ad}(\rho)$ is irreducible. Finally, as mentioned in the introduction, the adjoint of the Weil representation of $\mathrm{Sp}_{2n}(\mathbb{F}_3)$ is irreducible. In particular, if $\overline{G} \cong \mathrm{PSp}_4(\mathbb{F}_3)$ then $\mathrm{Ad}(\rho)$ is irreducible. □

2.4 An infinite family for $n = p^r$

Let p be an odd prime and r a positive integer. The object of this section is to construct an infinite family of groups G with irreducible representations (ρ, V) of degree $n = p^r$, whose adjoint $\mathrm{Ad}(\rho)$ is irreducible. In this case, the group G will arise as the normalizer in $\mathrm{SL}(V)$ of a suitable extraspecial p-group P.

Recall that a finite p-group P is called *extraspecial* if its center $Z(P)$ is a cyclic group of order p which coincides with the commutator group $[P, P]$, such that $P/Z(P)$ is elementary abelian (i.e, every nontrivial element has order p). Up to isomorphism there are two nonabelian extraspecial groups of order p^3: one of exponent p and one of exponent p^2. We will be mainly interested in the groups of exponent p. Their isomorphism class is represented by the Heisenberg group of 3×3 upper-triangular matrices over $\mathbb{F}_p$ with 1's on the main diagonal:

$$\left\{ \begin{pmatrix} 1 & a & c \\ 0 & 1 & b \\ 0 & 0 & 1 \end{pmatrix} : a, b, c \in \mathbb{F}_p \right\}.$$

Below we collect some classical results about the extraspecial groups. Further properties of these groups can be found in [3].

Lemma 2.4.1. *Let P be an extraspecial p-group. Then there exists $r \geq 1$ such that $|P| = p^{2r+1}$ and P is the central product of r non-abelian subgroups of order p^3, i.e., there exist normal subgroups $N_1, \ldots, N_r$ such that*

(i) $P = N_1 \ldots N_r$;

(ii) $[N_i, N_j] = 1$, *whenever* $i \neq j$;

(iii) $N_1 \dots N_{i-1} N_{i+1} \dots N_r \cap N_i = Z, \forall\ i.$

Proof. Denote by Z the center $Z(P)$ of P, and let z be a generator of this cyclic group of order p. Then P/Z can be naturally viewed as a vector space W over $\mathbb{F}_p$, the finite field of integers modulo p. We define a map

$$\beta : W \times W \to Z$$

as follows: for any pair $x, y \in P$, if their commutator $[x, y] = x^{-1}y^{-1}xy$ equals z^a (with $0 \leq a \leq p-1$), we set $\beta(xZ, yZ) = a$. It is easy to check that β is nondegenerate, bilinear and skew-symmetric, which gives W the structure of a nondegenerate symplectic space over $\mathbb{F}_p$. Then W has a *symplectic basis*

$$\{\overline{x_1}, \overline{y_1}, \dots, \overline{x_r}, \overline{y_r}\}$$

such that

$$\beta(\overline{x_i}, \overline{y_i}) = 1, \beta(\overline{x_i}, \overline{y_j}) = 0 \text{ for } i \neq j$$

and

$$\beta(\overline{x_i}, \overline{x_j}) = \beta(\overline{y_i}, \overline{y_j}) = 0 \text{ for all } 1 \leq i, j \leq r.$$

Hence $W = \oplus \overline{N_i},$ where $\overline{N_i} = \langle \overline{x_i}, \overline{y_i} \rangle$. Letting N_i be the preimages of $\overline{N_i}$ in P we obtain the desired characterization for P. □

Lemma 2.4.2. *Let P be an extraspecial group of order p^{2r+1}. Then P has exactly $p^{2r} + p - 1$ inequivalent irreducible representations over $\mathbb{C}$:*

- *p^{2r} are representations of degree 1.*
- *$p - 1$ are faithful representations of degree p^r, which are completely determined by their restriction on the center Z.*

Proof. Since P/Z is an elementary abelian group, we infer that the centralizer $C_P(x)$ of any element $x \in P \setminus Z$ has order p^{2r}, showing that the class of x has $[P : C_P(x)] = p$ elements. By the class equation, it follows that there are $(p^{2r+1} - p)/p = p^{2r} - 1$ conjugacy classes in $P \setminus Z$. Considering that every element of the center is its own conjugacy class, we conclude that there are exactly $p^{2r}+p-1$ conjugacy classes in P, which is also the number of irreducible complex representations of P. The number of 1-dimensional representations is equal to the index in P of the commutator group $[P, P] = Z$, so it is $[P : Z] = p^{2r}$.

Since P/N is abelian for any nontrivial normal subgroup N of P, all irreducible representations of P of dimension greater than 1 are faithful. Let $\lambda_1, \ldots, \lambda_{p-1}$ be all faithful linear characters of Z, let μ_i be an extension of λ_i to a maximal normal abelian subgroup A of G (of order p^{r+1}). Then, as shown in [18], $\mathrm{Ind}_A^P \mu_1, \ldots, \mathrm{Ind}_A^P \mu_{p-1}$ are all distinct faithful irreducible characters of P and

$$\mathrm{Ind}_A^P \mu_i(x) = \begin{cases} p^r \lambda_i(x) & \text{if } x \in Z, \\ 0 & \text{if } x \notin Z. \end{cases}$$

□

Lemma 2.4.3. ([38]) *Let P be an extraspecial group of order p^{2r+1} and exponent p. If*

$$\tilde{G} = \{\alpha \in Aut(P) : \alpha|_Z = 1\}$$

and $Inn(P)$ is the group of inner automorphisms then

$$\tilde{G}/Inn(P) \simeq \mathrm{Sp}_{2r}(\mathbb{F}_p).$$

2.4.1 The main construction

Now we have all the tools to prove Theorem 2.1.1, the first main result of this chapter. Recall that G is taken to be the normalizer in $\mathrm{SL}(V)$ of an extraspecial group P with a faithful irreducible representation (ρ, V) of degree p^r. Note that for $p = 5$ and $r = 1$, this group $G \simeq P \rtimes \mathrm{SL}_2(\mathbb{F}_5)$ is used in [17] to construct an indecomposable rank 2 vector bundle on $\mathbb{P}^4$ with 15000 symmetries (the order of G).

Proof of Theorem 2.1.1. First we relate G to the symplectic group $\mathrm{Sp}_{2r}(\mathbb{F}_p)$ by the means of the following lemma:

Lemma 2.4.4. *Let E be the centralizer in $\mathrm{SL}(V)$ of P. Then*

$$G/EP \simeq \mathrm{Sp}_{2r}(\mathbb{F}_p).$$

Proof. The automorphisms $\mathrm{Aut}_{\mathrm{SL}(V)}(P)$ of P induced by $\mathrm{SL}(V)$ are given by G/E. Let $\tilde{G}$ be the group introduced in Lemma 2.4.3, i.e., $\tilde{G}$ is the normal subgroup of $\mathrm{Aut}(P)$ that acts trivially on Z. Then

$$\tilde{G} \supseteq \mathrm{Aut}_{\mathrm{SL}(V)}(P).$$

If $\alpha \in \tilde{G}$ then considering that the irreducible representation of dimension p^n have distinct central characters (by Stone-von Neumann Theorem) it follows that $\rho \cong \rho \circ \alpha$, showing that $\alpha \in \mathrm{Aut}_{\mathrm{SL}(V)}(P)$. Consequently, $\tilde{G} = \mathrm{Aut}_{\mathrm{SL}(V)}(P)$ and Lemma 2.4.3 assures that

$$G/EP \simeq \tilde{G}/\ \mathrm{Inn}(P) \simeq \mathrm{Sp}_{2r}(\mathbb{F}_p).$$

□

We know from Lemma 2.4.1 that P/Z can be viewed as a $2r$-dimensional symplectic space W over $\mathbb{F}_p$. The corresponding symplectic form β gives an isomorphism $\phi : W \to W^\vee$ between W and its dual space $W^\vee$, sending

$$x \mapsto (\phi_x : y \mapsto \beta(x, y)).$$

Since $\mathrm{Sp}_{2r}(\mathbb{F}_p)$ preserves β, so does G (by Lemma 2.4.4), which implies that ϕ is a G-equivariant isomorphism. Furthermore, the group $\mathrm{Sp}_{2r}(\mathbb{F}_p)$ is transitive on $W\backslash\{0\}$, while the dual group $W^\vee$ can be identified with the group of characters $\mathrm{Hom}(W, \mathbb{C})$ of W. Therefore, G acts transitively on the set $\mathrm{Hom}^\star(W, \mathbb{C})$ of nontrivial characters of W.

Given $x \in W$, consider a lift $\tilde{x}$ to P and put $x \cdot M = \tilde{x}M\tilde{x}^{-1}$, which is independent of the choice of the lift. Since W is an elementary abelian group, we can decompose $\mathrm{Ad}(\rho)$ according to the eigenspaces corresponding to the characters of W. For $\chi \in \mathrm{Hom}(W, \mathbb{C})$ consider the corresponding weight space for W on $\mathrm{Ad}(\rho)$:

$$A_\chi = \{M \in \mathrm{Ad}(\rho) \ : \ \mathrm{tr}\, M = 0 \text{ and } x \cdot M = \chi(x)M, \forall\ x \in W\}.$$

If

$$\Lambda = \{\chi \in \mathrm{Hom}(W, \mathbb{C}) : A_\chi \neq 0\}$$

is the set of weights then $\mathrm{Ad}(\rho)$ decomposes as $\mathrm{Ad}(\rho) = \bigoplus_{\chi\in\Lambda} A_\chi$. The group G permutes the weight spaces by $gA_\chi = A_{g\chi}$, $g \in G$, $\chi \in \Lambda$. Since $\mathrm{Ad}(\rho)$ does not contain the trivial representation, it follows that $\Lambda \subseteq \mathrm{Hom}^\star(W, \mathbb{C})$. Moreover, since G is transitive on $\mathrm{Hom}^\star(W, \mathbb{C})$ we obtain that $\Lambda = \mathrm{Hom}^\star(W, \mathbb{C})$. The dimensions of the $p^{2r} - 1$ weight spaces add up to the dimension of $\mathrm{Ad}(\rho)$, which is $p^{2r} - 1$. Therefore, each space A_χ is of dimension 1.

If $W' \subset \mathrm{Ad}(\rho)$ is a G-invariant subspace then W' restricted to W is contained in $\oplus_{\chi \in \Lambda} A_\chi$, and since each summand is 1-dimensional it follows that $A_\chi \subset W'$ for some χ. However, in that case

$$\mathrm{Ad}(\rho) = G \cdot A_\chi \subset G \cdot W' = W',$$

which is a contradiction. Consequently, G is irreducible on $\mathrm{Ad}(\rho)$.

□

Remark 2.4.5. (i) *When $p = 3$ and $r = 1$ the projective image $\overline{G}$ in $\mathrm{PGL}_3(\mathbb{C})$ of the group G constructed above is the Hessian group G_{216} found in Proposition 2.3.2. One can check that (cf. [1], Proposition 4.1)*

$$\overline{G} = G_{216} \simeq (\mathbb{Z}/3\mathbb{Z})^2 \rtimes \mathrm{SL}_2(\mathbb{F}_3),$$

with the natural action of $\mathrm{SL}_2(\mathbb{F}_3)$ on $(\mathbb{Z}/3\mathbb{Z})^2$.

(ii) *Theorem 2.1.1 also holds for $p = 2$, however in that case one needs to take P to be the central product of a cyclic group of order 4 with an extraspecial group of order 2^{2r+1}.*

2.5 An application to Galois representations of Artin-type

We start with a brief discussion on the Artin L-functions before proving Theorem 2.1.2, the second main result of this chapter.

Let F be a number field and let $\rho : G_F \to GL(V)$ be a continuous representation of the absolute Galois group $G_F = \mathrm{Gal}(\overline{F}/F)$ on a n-dimensional $\mathbb{C}$-vector space V. The continuity implies that ρ has finite image, so it factors through the projection $\mathrm{Gal}(\overline{F}/F) \to \mathrm{Gal}(K/F)$, for some finite extension K/F. The Artin L-function attached to ρ is the Euler product

$$L(\rho, s) = \prod_v L_v(\rho, s),$$

with the local factors defined as

$$L_v(\rho, s) = \det([1 - \rho(\mathrm{Frob}_v)q_v^{-s}]|_{V^{I_v}})^{-1}.$$

Here $\mathrm{Frob}_v \in \mathrm{Gal}(\overline{F_v}/F_v)$ is a Frobenius element at a place v, V^{I_v} is the subspace of V fixed by the inertia group I_v at v, and q_v is the order of the residue field of F_v.

Let S be the finite set of places outside which ρ is unramified. Then for $v \notin S$, since the Frobenius conjugacy class $\{\rho(\mathrm{Frob}_v)\}$ is semi-simple, the eigenvalues $\alpha_{1,v}, \ldots, \alpha_{n,v}$ of the corresponding linear transformation are roots of unity. Accordingly, the local factor can be written as

$$L_v(\rho, s) = \prod_{j=1}^{n}(1 - \alpha_{j,v}q_v^{-s})^{-1}.$$

Denote by a_v the trace of the Frobenius at v, i.e., $a_v = \sum_{j=1}^{n} \alpha_{j,v}$. Notice that

$$\log L_v(\rho, s) = \frac{a_v}{q_v^s} + \sum_{m \geq 2} \frac{\sum_{j=1}^{n} \alpha_{j,v}^m}{q_v^{ms}}.$$

Using the fact that $|\alpha_{j,v}| = 1$ we obtain for real $s > 1$

$$\sum_{m \geq 2} \frac{|\sum_{j=1}^{n} \alpha_{j,v}^m|}{q_v^{ms}} \leq n \sum_{m \geq 2} \frac{1}{q_v^{ms}},$$

which implies that

$$\log L(\rho, s) \sim \sum_{v \notin \Sigma} \frac{a_v}{q_v^s} \text{ as } s \to 1^+,$$

where the relation $\sim$ means that the two sides agree up to a function of s which is $o(\log(\frac{1}{s-1}))$, and

$$\Sigma = \{v \text{ finite} \mid a_v = 0\}.$$

Proof of Theorem 2.1.2. Consider the Artin L-function $L(\rho, s)$ attached to a continuous irreducible n-dimensional representation (ρ, V) of the absolute Galois group G_F, and let Σ as defined above.

The order of the pole at $s = 1$ of $L(\rho, s)$ is the multiplicity of the trivial representation in ρ. Therefore, if ρ is irreducible then $-ord_{s=1} L(\rho \otimes \rho^\vee, s) = 1$. Since $\rho \otimes \rho^\vee = \mathbf{1} \oplus \mathrm{Ad}(\rho)$ we have

$$\rho \otimes \rho^\vee \otimes (\rho \otimes \rho^\vee)^\vee = \mathbf{1} \oplus 2\,\mathrm{Ad}(\rho) \oplus \mathrm{Ad}(\rho)^{\otimes 2}.$$

The key observation is that the trivial representation is contained in $\mathrm{Ad}(\rho)^{\otimes 2}$

with multiplicity $\sum_{i=1}^{N} m_i^2$, therefore

$$-ord_{s=1}L(\rho \otimes \rho^{\vee} \otimes \rho \otimes \rho^{\vee}, s) = 1 + \sum_{i=1}^{N} m_i^2.$$

Since ρ is a $\mathbb{C}$-representation of a finite group, the dual representation $\rho^{\vee}$ is isomorphic to the complex conjugate representation $\overline{\rho}$, and so the Frobenius trace of v on $\rho \otimes \rho^{\vee}$ is given by $a_v \cdot \overline{a}_v = |a_v|^2$. Therefore we get

$$\log L(\rho \otimes \rho^{\vee}, s) \sim \sum_{v \notin \Sigma} \frac{|a_v|^2}{q_v^s} \sim \log\Big(\frac{1}{s-1}\Big)$$

and similarly

$$\log L(\rho \otimes \rho^{\vee} \otimes (\rho \otimes \rho^{\vee})^{\vee}, s) \sim \sum_{v \notin \Sigma} \frac{|a_v|^4}{q_v^s} \sim \Big(1 + \sum_{i=1}^{N} m_i^2\Big) \log\Big(\frac{1}{s-1}\Big).$$

Consider the sequence $\{b_v\}$, with $b_v = 1$ if $v \notin \Sigma$ and $b_v = 0$, otherwise. By the Cauchy-Schwarz inequality, it follows that

$$\sum_{v \notin \Sigma} \frac{|a_v|^2}{q_v^s} = \sum_{v} \frac{|a_v^2 b_v|}{q_v^s} \leq \left(\sum_{v} \frac{|a_v|^4}{q_v^s}\right)^{1/2} \left(\sum_{v} \frac{b_v}{q_v^s}\right)^{1/2}.$$

If $\delta(\Sigma)$ is the density of the set Σ then by construction

$$\sum_{v} \frac{b_v}{q_v^s} \sim (1 - \delta(\Sigma)) \log\Big(\frac{1}{s-1}\Big)$$

and so the previous inequality reads as

$$1 \leq (1 + \sum_{i=1}^{N} m_i^2)(1 - \delta(\Sigma)).$$

This yields

$$\delta(\Sigma) \leq 1 - \frac{1}{1 + \sum_{i=1}^{N} m_i^2}.$$

As a consequence, it follows that when Ad is irreducible (i.e., $N = 1$ and $m_1 = 1$) the traces of Frobenius classes in finite Galois groups are nonzero for at least half of the primes. □

2.5.1 Some examples

As previously seen in the preliminaries, the irreducibility of $\mathrm{Ad}(\rho)$ forced ρ to be non essentially self-dual in dimension $n \geq 3$. Since the density estimate in Theorem 2.1.2 depends only on the multiplicity of the irreducible constituents of $\mathrm{Ad}(\rho)$, one could also consider self-dual representations ρ for which $\mathrm{Ad}(\rho)$ has only two inequivalent simple components (and thus $\delta(\Sigma) \leq 2/3$ by Theorem 2.1.2). We provide two examples of such representations.

Example 2.5.1. (*based on* [29]) *Take* $G = \mathrm{SL}_2(\mathbb{F}_5)$ *and let*

$$\pi : G \to \mathrm{GL}_2(\mathbb{C})$$

be an irreducible 2-dimensional representation. By Proposition 2.3.1, since the projective image of G *in* $\mathrm{PGL}_2(\mathbb{C})$ *is* A_5*, we infer that* $\mathrm{Ad}(\pi)$ *is an irreducible 3-dimensional representation. If* $\rho = \mathrm{Ad}(\pi)$ *then using the fact that*

$$\mathrm{Ad}(\pi) = \mathrm{Sym}^2(\pi) \otimes \det(\pi)^{-1}$$

it follows that

$$\mathrm{Sym}^2(\rho) = \mathrm{Sym}^4(\pi) \otimes \det(\pi)^{-2} \oplus \mathbf{1}.$$

Now, $\mathrm{Ad}(\rho)$ *is the sum of* ρ *and* $\mathrm{Sym}^4(\pi) \otimes \det(\pi)^{-2}$*, which are both irreducible.*

Example 2.5.2. *Take* $G = \mathrm{SL}_2(\mathbb{F}_9)$ *(the double cover of* A_6*) and let*

$$\rho : G \to \mathrm{GL}_4(\mathbb{C})$$

be an irreducible 4-dimensional representation. Using [23] (Proposition 3.1) we find that $\mathrm{Sym}^2(\rho)$ *is an irreducible 10-dimensional representation. Furthermore,* $\Lambda^2(\rho)$ *contains the trivial representation with multiplicity one, so we can write*

$$\Lambda^2(\rho) = \mathbf{1} \oplus \tau,$$

where τ *is a 5-dimensional representation that factors through* A_6*. By the character table of* $\mathrm{SL}_2(\mathbb{F}_9)$ *it has one 1-dimensional, two 4-dimensional, two 5-dimensional, four 8-dimensional, one 9-dimensional and three 10-dimensional irreducible representations. Thus,* τ *must be irreducible and* $\mathrm{Ad}(\rho)$ *is the sum of* τ *and* $\mathrm{Sym}^2(\rho)$*.*

Chapter 3

Non-extremality of Frobenius traces in Hilbert modular forms

3.1 Introduction

Let F be a totally real number field of degree n over $\mathbb{Q}$, with ring of integers $\mathcal{O}_F$. Let f be a Hilbert modular newform of parallel weight 2, level $\mathfrak{n}$ and trivial character. The Fourier coefficients $a_{\mathfrak{m}}$, as $\mathfrak{m}$ runs over ideals in $\mathcal{O}_F$ are the eigenvalues of f relative to Hecke operators $T_{\mathfrak{m}}$ (i.e., $T_{\mathfrak{m}}(f) = a_{\mathfrak{m}} f$). These eigenvalues generate a finite extension E over F. By Taylor [33] and Blasius-Rogawski [6], for every prime ideal $\mathfrak{q}$ of E over a rational prime q, one can attach to f a continuous 2-dimensional Galois representation

$$\rho := \rho_{f,\mathfrak{q}} : \mathrm{Gal}(\overline{\mathbb{Q}}/F) \to \mathrm{GL}_2(E_{\mathfrak{q}})$$

that is unramified outside the set of primes dividing $\mathfrak{n}q$. For any prime ideal $\mathfrak{p} \nmid \mathfrak{n}q$, the characteristic polynomial of the (geometric) Frobenius $\mathrm{Frob}_{\mathfrak{p}}$ of $\mathrm{Gal}(\overline{\mathbb{Q}}/F)$at $\mathfrak{p}$ is the Hecke polynomial

$$x^2 - a_{\mathfrak{p}} x + N(\mathfrak{p}),$$

where $N(\mathfrak{p})$ is the norm of $\mathfrak{p}$.

We shall call the Fourier coefficient $a_{\mathfrak{p}}$ *extremal* if $a_{\mathfrak{p}}^2 = 4N(\mathfrak{p})$. This is equivalent to the fact that the Hecke polynomial has a double root. If $\mathfrak{p} \in \mathcal{O}_F$ is a prime ideal above a rational prime p then the degree of the finite extension $\mathcal{O}_F/\mathfrak{p}$ over the prime field $\mathbb{F}_p$ is called the degree of $\mathfrak{p}$. The primary purpose of this chapter is to prove in a number of cases (explained below) that for degree one primes $\mathfrak{p}$ the Fourier coefficient $a_{\mathfrak{p}}$ is never extremal, i.e., the Hecke polynomial at such $\mathfrak{p}$ has always distinct roots.

The analogous statement for classical elliptical modular forms has been been known for some time by the work of by Coleman and Edixhoven ([9]), which has been a source of inspiration for us. Our methods extend theirs, while employing some new ideas in the Hilbert setting.

It is known that such a Hilbert newform f generates a cuspidal automorphic representation $\pi = \otimes_v \pi_v$ of $\mathrm{GL}_2(\mathbb{A}_F)$, where $\mathbb{A}_F$ is the ring of adeles of F and π_v is a representation of $\mathrm{GL}_2(F_v)$ for each finite place v of F, unramified for almost all v. Suppose that one of the following two situations holds: (i) the degree n of the extension $F/\mathbb{Q}$ is odd or (ii) n is even and there exists a finite place v of F at which π_v is square integrable (special or supercuspidal). Then we prove in Theorem 3.3.1 that for any unramified prime $\mathfrak{p}$ of degree one the Fourier coefficient $a_{\mathfrak{p}}$ is not extremal. This is achieved by transferring to a quaternionic Shimura curve via the Jacquet-Langlands correspondence and adapting the approach in [9]. When f is a CM form we obtain in Theorem 3.4.1 an unconditional result for any prime $\mathfrak{p}$ of degree one, even if one may not be able to move directly to a Shimura curve

We expect $a_{\mathfrak{p}}$ not to be extremal for any odd degree prime $\mathfrak{p}$. In section 3.3.1 we show that for certain primes $\mathfrak{p}$ of even degree the coefficients $a_{\mathfrak{p}}$ may be

extremal. One can see this by taking f to be a base change of a classical modular form, and $\mathfrak{p}$ a prime ideal above a rational prime of supersingular reduction.

In general, the non-extremality of the $a_{\mathfrak{p}}$ coefficients (for degree one $\mathfrak{p}$) follows from the semi-simplicity of the Frobenius element in the crystalline cohomology. This is done in Theorem 3.5.1. There, we consider the motivic piece $W(\pi)$ corresponding to π in the cohomology group $H^2(X)$ (here X is a Shimura surface, or an appropriate compactification of a Hilbert modular surface), and show that it is the tensor induction of $V(\pi)$ (determined by ρ). The main ingredient is to use the weak-admissibility of the crystalline realization of W to deduce the semi-simplicity of $\mathrm{Frob}_{\mathfrak{p}}$ on $V(\pi)$.

Finally, in Section 3.6 we explain how the above semi-simplicity condition can be obtained from the strong form of the Tate conjecture for a product of two surfaces over a finite field. More precisely, if $\tilde{X}$ is the reduction of X modulo a good prime $\mathfrak{p}$ and we assume that the order of the pole of the zeta function $\zeta(\tilde{X} \times \tilde{X}, 2)$ is equal to the rank of the group of codimension 2 cycles on $\tilde{X} \times \tilde{X}$ up to numerical equivalence, then we show that the Hecke polynomial at $\mathfrak{p}$ has distinct roots.

3.2 Quaternion algebras

In this section we give a brief overview of some aspects of the theory of quaternion algebras that we will use throughout the chapter.

Let F be a field. A *quaternion algebra* B over F is a central simple F-algebra of dimension 4. When the characteristic of F is not 2, a quaternion algebra B is given by some $a, b \in F^{\times}$, as the F-algebra of basis $1, i, j, k$ with

$i, j \in B$, $k = ij$ and

$$i^2 = a, j^2 = b, ij = -ji.$$

Such a quaternion algebra will be denoted by $B = \left(\frac{a,b}{F}\right)$. For example, if $a = b = -1$ and $F = \mathbb{R}$ then $\left(\frac{-1,-1}{\mathbb{R}}\right)$ is just the division algebra $\mathbb{H}$ of Hamilton quaternions. Any quaternion algebra that is not a division algebra is isomorphic to $M_2(F)$, the algebra of 2×2 matrices over F.

A quaternion algebra $B = \left(\frac{a,b}{F}\right)$ is endowed with an anti-involution $\theta \mapsto \overline{\theta}$ called conjugation, such that $\theta\overline{\theta} \in F$ for $\theta \in B$. The map $\mathrm{nrd}(\theta) = \theta\overline{\theta}$ is referred to as the *reduced norm*. One can also define the *reduced trace* as $\mathrm{trd}(\theta) = \theta + \overline{\theta}$. Explicitly, if $\theta = x + yi + zj + wij \in B$ then

$$\begin{aligned} \overline{\theta} &= x - yi - zj - wij \\ \mathrm{nrd}(\theta) &= x^2 - ay^2 - bz^2 + abw^2 \\ \mathrm{trd}(\theta) &= 2x \in F, \end{aligned}$$

and thus the characteristic equation $\theta^2 - \mathrm{trd}(\theta)\theta + \mathrm{nrd}(\theta) = 0$ is satisfied.

Now let F be a number field contained in a larger field K, then by tensoring we get a quaternion algebra over K

$$\left(\frac{a,b}{F}\right) \otimes_F K \cong \left(\frac{a,b}{K}\right).$$

We say that K *splits* B if

$$B \otimes_F K \cong M_2(K).$$

For any place v of F let F_v denote the completion of F at v. Clearly, if v is a complex place then $B_v = B \otimes_F F_v$ necessarily splits. For a non-complex

place v, we say that B is *ramified* at v if B_v is a division ring. Otherwise, $B_v \cong M_2(F_v)$ and we say that B is *unramified* (or split) at v.

The set of places at which a quaternion algebra B ramifies is finite and of even cardinality. Conversely, given an even number of (non-complex) places there exists a quaternion algebra that ramifies at precisely those places. Two quaternion algebras are isomorphic if and only if they are ramified at the same places. The product of the finite ramified places is an ideal in the ring of integers $\mathcal{O}_F$ of F, called the *discriminant* $\mathrm{disc}(B)$ of B.

An *order* of B is a subring $\mathcal{O} \subset B$ (containing 1) which is a finitely generated $\mathcal{O}_F$-module generating B over F. If $\mathcal{O} = \mathcal{O}_F \oplus \mathfrak{a}i \oplus \mathfrak{b}j \oplus \mathfrak{c}k$ then the reduced discriminant of $\mathcal{O}$ is the ideal

$$\mathfrak{d}(\mathcal{O}) = \mathfrak{abc}\ \mathrm{trd}((ij - ji)\overline{k}),$$

whose square is called the discriminant $\mathrm{disc}(\mathcal{O})$ of $\mathcal{O}$, i.e., $\mathrm{disc}(\mathcal{O}) = \mathfrak{d}(\mathcal{O})^2$.

An order $\mathcal{O}$ that is not properly contained in any other order is called a *maximal order*. Equivalently, $\mathcal{O}$ is maximal if and only if $\mathfrak{d}(\mathcal{O}) = \mathrm{disc}(B)$. If $\mathcal{O}$ is the intersection of two (not necessarily distinct) maximal orders then it is called an *Eichler order*. The *level* of an Eichler order $\mathcal{O}$ is the ideal $\mathfrak{n} \subset \mathcal{O}_F$ satisfying $\mathrm{disc}(\mathcal{O}) = \mathfrak{n}\,\mathrm{disc}(B)$.

To construct an Eichler order of a given level $\mathfrak{n}$ (coprime to $\mathrm{disc}(B)$) one can choose a maximal order $\mathcal{O} \subset B$ and an embedding $\iota_{\mathfrak{n}} : \mathcal{O} \hookrightarrow M_2(\mathcal{O}_{F,\mathfrak{n}})$, with $\mathcal{O}_{F,\mathfrak{n}}$ the completion of $\mathcal{O}_F$ at $\mathfrak{n}$. Then

$$\mathcal{O}(\mathfrak{n}) = \{\theta \in \mathcal{O} : \iota_{\mathfrak{n}}(\theta) \mod \mathfrak{n} \text{ is upper triangular}\}$$

is an Eichler order of level $\mathfrak{n}$.

3.3 The Shimura curve case

Let F be a totally real number field of degree $n = [F : \mathbb{Q}]$ and let $\mathcal{O}_F$ be its ring of integers. Let f be a Hilbert cuspidal eigenform for F of parallel weight 2, level $\mathfrak{n}$ (an ideal of $\mathcal{O}_F$), and trivial character. We associate to f an automorphic representation $\pi = \otimes_v \pi_v$ of $\mathrm{GL}_2(\mathbb{A}_F)$, where $\mathbb{A}_F$ is the ring of adeles of F and π_v is a representation of $\mathrm{GL}_2(F_v)$ for each finite place v of F.

Recall that the degree of a prime ideal $\mathfrak{p} \in \mathcal{O}_F$ above some rational prime p is the power of p in the norm $N(\mathfrak{p})$ of $\mathfrak{p}$ (i.e., the cardinality of the quotient ring $\mathcal{O}_F/\mathfrak{p}$). Let $a_\mathfrak{p}$ be the Hecke eigenvalue at a prime $\mathfrak{p}$. Occasionally, we will use the notation $a_\mathfrak{p}(f)$ or $a_\mathfrak{p}(\pi)$ for $a_\mathfrak{p}$ to emphasize the underlying eigenform or the automorphic representation.

The purpose of this section is to prove that for primes of degree one the Hecke roots are distinct, provided that one can transfer to a quaternionic Shimura curve via the Jacquet-Langlands correspondence. More precisely, we establish the following result.

Theorem 3.3.1. *Let $F, n, f, \mathfrak{n}$ and π be as above. When n is even, suppose in addition that there is a finite place v' of F such that the local component $\pi_{v'}$ is square integrable (i.e., special or supercuspidal). Then for any degree one prime $\mathfrak{p} \nmid \mathfrak{n}$ the Hecke polynomial*

$$x^2 - a_\mathfrak{p} x + N(\mathfrak{p})$$

has distinct roots.

Proof. We first describe how to obtain a Shimura curve using an appropriate quaternion algebra B over F. Then we adapt the methods of Coleman-Edixhoven from [9] to our setting.

Let $\rho_1, \ldots, \rho_n : F \to \mathbb{R}$ be the real embeddings of F. We distinguish two possible cases:

- If n is odd, we let B be the unique quaternion algebra that is split at the archimedean place corresponding to ρ_1 and ramified at the places corresponding to $\rho_2, \ldots, \rho_n$.
- If n is even, we let B be the unique quaternion algebra that is ramified at v' and at the $n-1$ places corresponding to $\rho_2, \ldots, \rho_n$.

Denote by $\mathrm{ram}(B)$ the set of places at which B is ramified, and by $\mathrm{disc}(B)$ the product of all the finite places in $\mathrm{ram}(B)$ (which, by definition, is the discriminant of B).

Let $\mathfrak{n}'$ be an ideal such that $\mathfrak{n} = \mathfrak{n}' \mathrm{disc}(B)$. By the Jacquet-Langlands correspondence, given any Hilbert modular newform f of weight 2 and level $\mathfrak{n}$ of the type above, there exists a unique newform g of weight 2 on the upper half-plane relative to a congruence subgroup $\Gamma^B(\mathfrak{n}')$ (see below), such that $a_v(f) = a_v(g)$ for any finite place $v \nmid \mathfrak{n}$. Let π' be the cuspidal automorphic representation of $B(\mathbb{A}_F)^\times$ generated by g. Then $\pi_v \simeq \pi'_v$, for any $v \notin \mathrm{ram}(B)$.

Now we shall construct an arithmetic group that generalizes the modular group $\mathrm{SL}_2(\mathbb{Z})$. To get the prescribed level structure, we take an Eichler order $\mathcal{O}(\mathfrak{n}')$ in B of level $\mathfrak{n}'$ and consider the group

$$\mathcal{O}^1(\mathfrak{n}') = \{\theta \in \mathcal{O}(\mathfrak{n}') \mid \mathrm{nrd}(\theta) = 1\}.$$

Since our B is split at exactly one real place, there is a map

$$B \hookrightarrow B \otimes_{\mathbb{Q}} \mathbb{R} \simeq M_2(\mathbb{R}) \times \mathbb{H}^{n-1}.$$

Letting $\iota : B \hookrightarrow M_2(\mathbb{R})$ be the projection onto the first factor, we obtain an arithmetic Fuchsian group (i.e., a discrete subgroup of $\mathrm{PSL}_2(\mathbb{R})$)

$$\Gamma^B(\mathfrak{n}') = \iota(\mathcal{O}^1(\mathfrak{n}')) \subset \mathrm{GL}_2^+(\mathbb{R}).$$

This group acts by linear fractional transformations on the upper half-plane $\mathfrak{H}$ and the (compact) quotient $\Gamma^B(\mathfrak{n}')\backslash\mathfrak{H}$ can be viewed as the complex points of the connected component of a Shimura curve C_B, which has a canonical model defined over F.

Let $E_f = \mathbb{Q}(\{a_\mathfrak{p}\})$ be the field generated over $\mathbb{Q}$ by all the coefficients $a_\mathfrak{p}$ of f. There exists an abelian variety associated to π' (and hence to π) defined over F of dimension $[E_f : \mathbb{Q}]$, arising (uniquely up to F-isogeny) as a quotient of the Jacobian of C_B. We shall call it A_g.

Consider the ℓ-adic Tate module of A_g

$$T_\ell(A_g) = \varprojlim_k A_g[\ell^k],$$

which is the inverse limit of the torsion subgroups $A_g[\ell^k]$ (of $A_g(\overline{F})$) of order dividing ℓ^k. One can attach to π' a rank two $E \otimes \mathbb{Q}_\ell$-module

$$V_\ell = T_\ell(A_g) \otimes_{\mathbb{Z}_\ell} \mathbb{Q}_\ell.$$

Again, by the Jacquet-Langlands correspondence $L(s, f) = L(s, \pi')$ so V_ℓ is also attached to f. More precisely, for any prime ℓ and any ideal $\mathfrak{p}$ (over some rational prime p) not dividing $\mathfrak{n}\ell$ we have

$$a_\mathfrak{p} = \mathrm{tr}(\mathrm{Frob}_\mathfrak{p} \,|V_\ell).$$

Assume by contradiction that the Hecke polynomial $x^2 - a_{\mathfrak{p}}x + N(\mathfrak{p})$ has a double root λ. Then $a_{\mathfrak{p}} = 2\lambda$ and $N(\mathfrak{p}) = \lambda^2 = p$ (recall that $\mathfrak{p}$ is taken to be a prime of degree one).

Let $\mathcal{O}_{\mathfrak{p}} = \mathcal{O}_{F,\mathfrak{p}}$ be the the completion of $\mathcal{O}_F$ at $\mathfrak{p}$, $\mathbb{F}_q = \mathcal{O}_{\mathfrak{p}}/\mathfrak{p}\mathcal{O}_{\mathfrak{p}}$ and $\widetilde{A_g}$ the reduction of A_g over $\mathbb{F}_q$. Since A_g has good reduction at $\mathfrak{p}$, the inertia group at $\mathfrak{p}$ acts trivially on $H^1(A_g \times \overline{F}, \mathbb{Q}_\ell)$, and the inertial invariants are known to be identified with the H^1 of the reduction. Hence, the dual of V_ℓ satisfies:

$$H^1(A_g \times \overline{F}, \mathbb{Q}_\ell) \cong H^1(\widetilde{A_g} \times \overline{\mathbb{F}}_q, \mathbb{Q}_\ell).$$

The endomorphism ring $\mathrm{End}(\widetilde{A_g})$ of $\widetilde{A_g}$ is semi-simple (in fact, it is a division algebra if $\widetilde{A_g}$ is simple). Therefore, the Frobenius endomorphism of $\widetilde{A_g}$ acts as a semi-simple operator. On the other hand, by the Eichler-Shimura congruence relations:

$$(\mathrm{Frob}_{\mathfrak{p}} - \lambda)^2 = 0,$$

as endomorphisms over the residue field. Now applying the semi-simplicity of $\mathrm{Frob}_{\mathfrak{p}}$ we get that

$$\mathrm{Frob}_{\mathfrak{p}} = \lambda \text{ in } \mathrm{End}(\widetilde{A_g}). \qquad (\star)$$

To get a contradiction from $(\star)$, we need to also consider (as in [9]) the first de Rham cohomology group M of the associated Néron model $\mathcal{A}$ of A_g over $\mathcal{O}_{\mathfrak{p}}$, with its Hodge filatration

$$\mathrm{Fil}^1 M := H^0(\mathcal{A}, \Omega^1) \subset M.$$

Since $\mathrm{Fil}^1(M)$ is locally isomorphic to $\mathcal{O}_E \otimes \mathcal{O}_{\mathfrak{p}}$ and $\lambda^2 = p$ we get that p does not divide λ, so $\mathrm{Fil}^1(M) \otimes \mathbb{F}_q$ is not annihilated by λ. However, $\mathrm{Frob}_{\mathfrak{p}} = \lambda$ has

differential zero, implying that λ annihilates $H^0(\widetilde{A_g}, \Omega^1) = \mathrm{Fil}^1(M) \otimes \mathbb{F}_q$. In conclusion, the Hecke polynomial has distinct roots.

□

Remark 3.3.2. *The condition requiring $\mathfrak{p}$ to be a degree one prime is crucial. Indeed, if $\mathfrak{p}$ were a prime of degree two, then $\lambda^2 = p^2$ would imply that $\lambda = \pm p$. Accordingly, p would divide λ and hence the above argument would not work.*

3.3.1 An example

It is important to mention that there are examples of Hilbert modular forms obtained by base-changing classical newforms, for which the Hecke roots at certain primes are the same. We present below one such example due to R. Kottwitz, which we learnt about from M. Emerton:

Let f be the unique cusp form of weight 2 and level

$$\Gamma_0(11) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{SL}_2(\mathbb{Z}) \mid c \equiv 0 \pmod{11} \right\}.$$

For convenience, we will denote by E the corresponding elliptic curve

$$X_0(11) = \Gamma_0(11) \backslash \mathfrak{H}.$$

It is known that E has conductor 11 and it is given by the equation (for more details see [37])

$$y^2 + y = x^3 - x^2 - 10x - 20.$$

By a result of Elkies (which holds true for any elliptic curve over $\mathbb{Q}$, cf. [11]), we know that there are infinitely many primes p such that $a_p(f) = 0$ (i.e., E

has supersingular reduction at p). For instance, the first odd prime of this type is $p = 19$.

Fix an odd supersingular prime p and choose a real quadratic extension F of $\mathbb{Q}$ such that p remains inert in F. Denote by $\mathfrak{p}$ the prime of F lying above p. Under the base-change from $\mathbb{Q}$ to F, one can lift f to a (parallel) weight 2 Hilbert modular form $\widetilde{f}$ for F. (The level of $\widetilde{f}$ will be the product of primes of F dividing 11. In particular, it is prime to p.)

Since p is inert, it follows that $N(\mathfrak{p}) = p^2$ and

$$a_{\mathfrak{p}} = a_p^2 - 2p = -2p.$$

Therefore, the polynomial

$$x^2 - a_{\mathfrak{p}}x + N(\mathfrak{p}) = (x + p)^2$$

has a double root at $-p$. This gives an example of an *even* degree prime $\mathfrak{p}$, for which the coefficient $a_{\mathfrak{p}}$ of $\widetilde{f}$ is *extremal* (i.e., $a_{\mathfrak{p}}^2 = 4N(\mathfrak{p})$).

3.3.2 Further analysis

The example presented above is not an isolated situation. To generate similar constructions start with an elliptic curve E over $\mathbb{Q}$ and a prime p of good supersingular reduction. Pick any real quadratic field F in which p is inert. Let f be a newform associated to E by the modularity theorem. If $\widetilde{f}$ denotes the base-change of f to F, then at the prime $\mathfrak{p}$ of degree 2 over p, one has that $a_{\mathfrak{p}}(\widetilde{f})$ is extremal.

Note also that given a prime p, there exist infinitely many real quadratic fields F such that p is inert in F.

Finally, we can fix a real quadratic field F, and a prime $\mathfrak{p}$ of degree 2 over a rational prime p. Take an elliptic curve E over $\mathbb{Q}$ with CM by an order $\mathcal{O}$ in an imaginary quadratic field K in which p is inert. Then E has good supersingular reduction at p, and the same phenomenon happens.

A closer analysis between the coefficients leads to the following observation.

Proposition 3.3.3. *Let K/F be a quadratic extension of totally real fields. Let f be a Hilbert newform for F of weight 2 and trivial character, and $\mathfrak{P}$ a prime of K (away from the level of f), which is of degree 2 over a prime $\mathfrak{p}$ of F. Suppose $\pi_{\mathfrak{P}}$ is a base change of the representation $\pi_{0,\mathfrak{p}}$ of $\mathrm{GL}_2(F_{\mathfrak{p}})$. Then $a_{\mathfrak{P}}$ is extremal if and only if either $a_{\mathfrak{p}}$ is extremal or $a_{\mathfrak{p}} = 0$.*

Proof. If $\mathfrak{p}$ is inert in K (i.e., $\mathfrak{p} = \mathfrak{P}\mathcal{O}_K$) then

$$a_{\mathfrak{P}} = a_{\mathfrak{p}}^2 - 2N(\mathfrak{p}).$$

Since $N(\mathfrak{P}) = N(\mathfrak{p})^2$, note that $a_{\mathfrak{P}}$ is extremal if and only if

$$a_{\mathfrak{P}} = \pm 2N(\mathfrak{P})^{1/2} = \pm 2N(\mathfrak{p}).$$

Combining the last two relations it follows that the extremality condition of $a_{\mathfrak{P}}$ is equivalent to $a_{\mathfrak{p}}^2$ being equal to either $4N(\mathfrak{p})$ (in which case $a_{\mathfrak{p}}$ is extremal) or to 0, as desired.

If $\mathfrak{p}$ splits in K then $a_{\mathfrak{P}} = a_{\mathfrak{p}}$, and the conclusion follows.

□

3.4 The CM case

We maintain the setting of f being a weight 2 Hilbert modular eigenform of level $\mathfrak{n}$ for a totally real field F of degree $n = [F : \mathbb{Q}]$, with trivial character.

In this section we will assume that f is a CM form associated to a character χ of an imaginary quadratic extension K/F. Under this assumption we will settle the case not covered by the last section: namely, when n is even and the automorphic representation π has no discrete series component at a finite place (so one can not move to a Shimura curve directly).

For any unramified prime $\mathfrak{p}$, we will show that $a_\mathfrak{p}$ is not extremal by constructing a certain character μ defined by some local relations. As a result, the automorphic representation π' corresponding to $\chi\mu$ will have the following two properties:

(P_1) $a_\mathfrak{p}(\pi)$ and $a_\mathfrak{p}(\pi')$ have the same Hecke polynomial.

(P_2) π' has a discrete series representation at some auxiliary finite place v'.

This way, by switching from π to π' we reduce the problem to the situation treated in the previous section.

Theorem 3.4.1. *Let $F, n, f, \mathfrak{n}$ and π be as above. Assume f is associated to a Hecke character χ of an imaginary quadratic extension K of F, so that $L(s, f) = L(s, \chi)$ (viewed as degree two Euler products over $\mathbb{Q}$). Then for any degree one prime $\mathfrak{p} \nmid \mathfrak{n}$ the Hecke polynomial*

$$x^2 - a_\mathfrak{p} x + N(\mathfrak{p})$$

has distinct roots.

Remark 3.4.2. *Note that Theorem 3.4.1 holds for any degree n without any further restrictions on π. Evidently, this also includes the case when n is even and the associated automorphic representation π has no square integrable component at a finite place, which was not addressed in Theorem 3.3.1.*

Proof. Since f is a CM form, there exists a quadratic character ε of F corresponding to K/F such that $f = f \otimes \varepsilon$. By hypothesis, π has trivial central character, i.e., $\chi|_F = \varepsilon$.

Fix an unramified prime $\mathfrak{p}$ of F. If $\mathfrak{p}$ is inert in K then $a_\mathfrak{p} = 0$ (recall that f is a CM form), so $a_\mathfrak{p}$ can not be extremal. Therefore, we can assume that $\mathfrak{p}$ splits in K. Denote by $\mathfrak{q}$ and $\mathfrak{q}'$ the primes above $\mathfrak{p}$ in K.

If π has a discrete series component π_u, we are done by Theorem 3.3.1. So assume otherwise, and pick an auxiliary finite place v' of F that remains inert in K. Consider the set

$$S = \{\mathfrak{q}, \mathfrak{q}', v'\}$$

of places of K. To each element of S we shall associate a local character as follows:

- For $\mathfrak{q}$ and $\mathfrak{q}'$, simply take the trivial characters of $K_\mathfrak{q}^\times$ and $K_{\mathfrak{q}'}^\times$.
- For v', choose λ to be a quadratic character of $K_{v'}^\times$ such that $\lambda \neq \lambda \circ c$, where c is the non-trivial element of $\mathrm{Gal}(K_{v'}/F_{v'})$. More concretely, we will tale λ to be the quadratic character of $K_{v'}^\times$ attached to its unique unramified quadratic extension.

By the Grunwald-Wang theorem (see [2], Theorem 5) there exists a (finite order) global character μ of K such that

$$\mu_\mathfrak{q} = \mu_{\mathfrak{q}'} = 1, \mu_{v'} = \lambda \text{ and } \mu_\infty = 1.$$

Take π' to be the induced representation $\mathrm{Ind}_K^F(\chi\mu)$.

Lemma 3.4.3. *π' satisfies the properties (P_1) and (P_2).*

Proof. Since $\mathfrak{p} = \mathfrak{q}\mathfrak{q}'$, the coefficient $a_\mathfrak{p}$ can be written as $a_\mathfrak{p}(\pi) = \chi_\mathfrak{q}(\omega)+\chi_{\mathfrak{q}'}(\omega)$, where ω is an uniformizer of $F_\mathfrak{p} \cong K_\mathfrak{q} \cong K_{\mathfrak{q}'}$. The condition $\mu_\mathfrak{q} = \mu_{\mathfrak{q}'} = 1$ implies that $\chi_\mathfrak{q}\mu_\mathfrak{q} = \chi_\mathfrak{q}$ and $\chi_{\mathfrak{q}'}\mu_{\mathfrak{q}'} = \chi_{\mathfrak{q}'}$. Hence

$$a_\mathfrak{p}(\pi) = a_\mathfrak{p}(\pi').$$

To establish property (P_1) it suffices to show that π' has trivial character at $\mathfrak{p}$. This is equivalent to showing that $\chi_\mathfrak{p}\mu_\mathfrak{p} = \varepsilon_\mathfrak{p}$, which is true because $\mathfrak{p}$ splits.

Moreover, by our construction it follows that

$$\pi'_{v'} = \mathrm{Ind}_{K_{v'}}^{F_{v'}}(\chi_{v'}\mu_{v'}) = \mathrm{Ind}_{K_{v'}}^{F_{v'}}(\chi_{v'}\lambda).$$

Since π has no supercuspidal component, we get that $\chi_{v'} = \chi_{v'} \circ c$. Therefore, since λ was chosen such that $\lambda \neq \lambda \circ c$, we obtain

$$\chi_{v'}\lambda \neq \chi_{v'}\lambda \circ c.$$

This means that the local Galois representation at v' is irreducible. By local-global compatibility, known for CM forms, one gets the local component $\pi'_{v'}$ to be supercuspidal and so (P_2) also holds. □

In view of the lemma, one can change π and look at a related π', for which Theorem 3.3.1 can be applied. As a result, the coefficient $a_\mathfrak{p}(\pi')$ is not extremal. Consequently, the same is true for $a_\mathfrak{p}(\pi)$, since we showed that $a_\mathfrak{p}(\pi)$ and $a_\mathfrak{p}(\pi')$ have the same Hecke polynomial. □

3.5 Semi-simplicity of Frobenius

3.5.1 Cohomology decomposition

Let F be a totally real quadratic extension of $\mathbb{Q}$. We will denote by $\mathbb{A}_{F,f}$ the ring of finite adeles of F, and by $G = R_{F/\mathbb{Q}}\,\mathrm{GL}_2$ the Weil restriction of scalars.

For an arbitrary compact open subgroup K of $G(\mathbb{A}_{F,f})$ consider the associated Shimura variety

$$Y = S_K = G(F)\backslash(F \otimes \mathbb{C} - F \otimes \mathbb{R})^2 \times G(\mathbb{A}_{F,f})/K.$$

We denote by $Y^\star$ its Bailey-Borel compactification over $\mathbb{Q}$. Then for a finite set of cusps Y^∞ we have

$$Y^\star = Y \cup Y^\infty.$$

A rational cone decomposition defines a smooth toroidal compactification

$$X := \tilde{Y} = Y \cup \tilde{Y}^\infty,$$

which we choose to be minimal. The Hecke operators (acting as correspondences) preserve $Y^\star$ but not X, so we consider the intersection cohomology $IH^2(Y^\star)$ that appears in the decomposition

$$H^2(X) = IH^2(Y^\star) \oplus H^2_{\tilde{Y}^\infty}(\tilde{Y}^\infty).$$

The semi-simple action of the Hecke algebra $\mathcal{H}$ commutes with the action of the Galois group $\Gamma_Q = \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ on $IH^2(Y^\star)$. Now $IH^2(Y^\star)$ has a motivic

decomposition

$$IH^2(Y^\star) = IH^2_{\text{res}}(Y^\star) \oplus IH^2_{\text{cusp}}(Y^\star)$$

into a residual part IH^2_{res} and, what will be of main interest to us, a cuspidal part IH^2_{cusp}. The automorphic representations that appear in the cuspidal part are of the form $D_2 \otimes \pi_f$, with D_2 the lowest discrete series of $\mathrm{GL}_2(\mathbb{R})$ of weight 2 with trivial character, and π_f is an irreducible admissible representation of $G(\mathbb{A}_{F,f})$ (cf.[28]). Furthermore, we have a $\mathcal{H} \times \Gamma_{\mathbb{Q}}$-equivariant decomposition:

$$IH^2_{\text{cusp}}(Y^\star) = \bigoplus_{\pi_f} W(\pi)^{m(\pi_f, K)}.$$

Given π_f there is a suitable K (associated to the conductor of π) such that the multiplicity $m(\pi_f, K) = 1$.

Each isotypic component $W(\pi)$ can be thought of as a motivic summand $H^2(X)[\pi]$ of $H^2(X)$ corresponding to π and this motive is of rank 4 over its field of coefficients. So it makes sense in various realizations, such as Betti ($W_B(\pi)$), De Rham ($W_{dR}(\pi)$), and étale ($W_\ell(\pi)$).

3.5.2 Galois representations

For the remainder of this section, f will be a Hilbert modular newform of weight 2 and level $\mathfrak{n}$, with associated automorphic representation π of trivial central character.

By the work of Taylor ([33]) and Blasius-Rogawski ([6]), there exists a 2-dimensional irreducible representation $V_\ell(\pi)$ of $\Gamma_F = \mathrm{Gal}(\overline{\mathbb{Q}}/F)$ that satisfies $L(s, \pi) = L(s, V_\ell(\pi))$. More precisely, for any prime $\mathfrak{p} \nmid \mathfrak{n}\ell$:

$$a_{\mathfrak{p}}(\pi) = \mathrm{tr}(\mathrm{Frob}_{\mathfrak{p}} \,|V_\ell(\pi)).$$

One can decompose W_ℓ into a tensor product of two 2-dimensional representations of Γ_F. Since X is a surface, $H^2(X)$ admits a symmetric bilinear form under intersection, which preserves $IH^2(Y^\star)$. This leads to the Γ_Q representation on $W_\ell(\pi)$ landing in the group of orthogonal transformations $\mathrm{O}(W_\ell)$. Using Harder-Langlands-Rapoport [15], the restriction to Γ_F lands in $\mathrm{SO}(W_\ell)$, which is surjected on by $\mathrm{GL}_2 \times \mathrm{GL}_2$:

$$W_\ell(\pi)|_{\Gamma_F} \simeq V^1(\pi) \otimes V^2(\pi).$$

The choice of the pair $(V^1(\pi), V^2(\pi))$ is not unique, for it can be replaced by the pair $(V^1(\pi) \otimes \nu, V^2(\pi) \otimes \nu^{-1})$, for some character ν. However, by the semi-simplicity of W_ℓ and V_ℓ, one can choose $V^1(\pi) = V_\ell(\pi)$ and $V^2(\pi) = V_\ell(\pi)^\theta$ (here θ is the non-trivial automorphism of F over $\mathbb{Q}$), so that

$$W_\ell(\pi)|_{\Gamma_F} \simeq V_\ell(\pi) \otimes V_\ell(\pi)^\theta.$$

This way

$$W_\ell(\pi) \simeq {}^{\otimes}\mathrm{Ind}_{\Gamma_F}^{\Gamma_\mathbb{Q}}(V_\ell(\pi)),$$

where ${}^{\otimes}\mathrm{Ind}$ is the tensor induction.

3.5.3 Shimura surface

Let E be a totally real number field, and let B be a quaternion algebra over E that is split at exactly two infinite places w and w'. Consider the algebraic group G over E, so that for any E-algebra A:

$$G(A) = (B \otimes_E A)^\times.$$

There exists a Shimura surface S defined over a subfield

$$H := \{\sigma : \mathrm{Hom}(E, \overline{\mathbb{Q}}) \mid \sigma \text{ preserves } \{w, w'\}\},$$

such that

$$S(\mathbb{C}) = G(E)\backslash(\mathbb{C} - \mathbb{R})^2 \times G(\mathbb{A}_{E,f}).$$

Moreover, for every compact open subgroup K of $G(\mathbb{A}_{E,f})$ we get an actual projective surface S_K defined over E, such that

$$S_K(\mathbb{C}) = S(\mathbb{C})/K.$$

One advantage of working with the Shimura surface instead of the Hilbert surface is that the former is already compact. In this case, one avoids the technicalities associated with the appropriate compactification, since the intersection cohomology IH^2 coincides with the usual cohomology H^2. Another advantage constitutes the fact that we have such a Shimura surface over any totally real E, so one does not have to restrict only to the (totally) real quadratic case, as in section 3.5.1.

3.5.4 Non-extremality when Frobenius is semi-simple

The motivic piece $W(\pi)$ of $H^2(X)$ corresponding to π has a crystalline realization M of rank 4 over the field E_f of coefficients of f (here X is taken to be a Shimura surface, or the minimal smooth toroidal compactification of a Hilbert modular surface).

Consider the reduction $\tilde{X}$ modulo a good prime $\mathfrak{p}$. The Galois representation is then unramified at $\mathfrak{p}$, and the intertial invariants of the cohomology

of X in characteristic zero can be identified with the cohomology of $\tilde{X}$. The p-adic Galois representation W is crystalline since it comes from a smooth projective variety with good reduction at $\mathfrak{p}$. This means that W has the same dimension as the space of Galois invariants of $W \otimes_{\mathbb{Q}_p} B_{\text{cris}}$, where B_{cris} is Fontaine's crystalline ring of periods. Accordingly, we have an induced action of the crystalline Frobenius ϕ of M.

Moreover, the comparison map between étale and crystalline cohomology is functorial for the action of algebraic correspondences, and our motive M is cut out of $H^2(X)$ using a projector coming from algebraic correspondences. In addition, by [20], we know that $\text{Frob}_{\mathfrak{p}}$ and ϕ have the same characteristic polynomial, namely $x^2 - a_{\mathfrak{p}}x + N(\mathfrak{p})$.

Theorem 3.5.1. *Let f be a Hilbert modular newform for a totally real number field F of weight 2, level $\mathfrak{n}$ and trivial character. Suppose that the crystalline Frobenius ϕ is semi-simple on M. Then the polynomial*

$$x^2 - a_{\mathfrak{p}}x + N(\mathfrak{p})$$

has distinct roots, for any degree one prime $\mathfrak{p} \nmid \mathfrak{n}$.

Proof. Consider a totally real quadratic extension E of F in which $\mathfrak{p}$ splits as $\mathfrak{q}$ and $\mathfrak{q}'$. Let π be the automorphic representation of $\text{GL}_2(\mathbb{A}_F)$ generated by f and write π_E for the base change of π to GL_2 over E. By construction

$$\pi_{E,\mathfrak{q}} = \pi_{E,\mathfrak{q}'} = \pi_{\mathfrak{p}}$$

and so

$$a_{\mathfrak{q}} = a_{\mathfrak{q}'} = a_{\mathfrak{p}}.$$

Let Σ_F and Σ_E be the set of all the archimedean places of F and E, respectively. We can assume (by Theorem 3.3.1) that $[F : \mathbb{Q}]$ is even, so that both Σ_F and Σ_E have even cardinality.

Fix and element $w \in \Sigma_F$ and let $\tilde{w}, \tilde{w}' \in \Sigma_E$ be the places above w in E. Consider the (indefinite) quaternion algebra B over E that is ramified only at $\Sigma_E - \{\tilde{w}, \tilde{w}'\}$. Then

$$B \otimes_Q \mathbb{R} \simeq M_2(\mathbb{R}) \times M_2(\mathbb{R}) \times \mathbb{H}^{[E:\mathbb{Q}]-2}.$$

By the Jacquet-Langlands correspondence, π_E transfers to a cuspidal automorphic representation Π of $B(\mathbb{A}_F)^\times$ with the same central character, such that for all finite primes $\mathcal{P}$, $a_\mathcal{P}(\Pi) = a_\mathcal{P}(\pi_E)$.

Consider the Shimura surface $S_K(\mathbb{C})$ defined over E (here K is the level subgroup), which is obtained from B as in section 3.5.3. Take the component W corresponding to Π in $H^2(S_K)$ as in section 3.5.1:

$$W := H^2(S_K)[\Pi].$$

Arguing as for the Hilbert surface case in section 3.5.2, one can write

$$W = V \otimes V' \text{ as } \Gamma_E\text{-modules},$$

where V can be chosen to be the restriction of Γ_E of the 2-dimensional representation V_0 associated to f by Taylor and Blasius-Rogawski. Also, V' is obtained from V by applying the non-trivial automorphism of E/F. As a result

$$V' \simeq V_0|_{\Gamma_E} = V, \text{ so } W = V^{\otimes 2}.$$

Since W occurs in the cohomology of a smooth projective variety with good reduction at $\mathfrak{p}$, it is crystalline. The comparison isomorphism relating de Rham and crystalline cohomology allows us to consider a Hodge filtration Fil° on M (recall that M was defined to be the crystalline realization of W):

$$M = \mathrm{Fil}^0(M) \supset \mathrm{Fil}^1(M) \supset \mathrm{Fil}^2(M) \supset \mathrm{Fil}^3(M) = 0,$$

where $\mathrm{Fil}^1(M)$ and $\mathrm{Fil}^2(M)$ are of rank 3 and 1, respectively. (Over $\mathbb{C}$, the Hodge structure M_B has Hodge weight 2, with Hodge numbers $h^{2,0}(M_B) = h^{0,2}(M_B) = 1$, and $h^{1,1}(M_B) = 2$.)

By a theorem of Faltings (see [12], Theorem 5.6), M is admissible, which is now known to be equivalent to weakly admissible (as a ϕ-module). This means that the Newton polygon of every subobject M' of M (in the category of filtered ϕ-modules) lies on or above its Hodge polygon (also, both polygons share the same endpoint). Recall the Hodge number $t_H(M)$ defined as

$$t_H(M) := \sum_{i \in \mathbb{Z}} i \cdot \dim \mathrm{Fil}^i(M)/\mathrm{Fil}^{i+1}(M),$$

and the Newton number $t_N(M)$ defined as

$$t_N(M) := v_p(\det(\phi)),$$

where v_p is the p-adic valuation. Then the condition that M is weakly admissible can be restated as follows:

$$t_N(M') \geq t_H(M') \text{ for any subobject } M' \text{ of } M, \text{ and } t_N(M) = t_H(M).$$

Now, assume by contradiction that the polynomial $x^2 - a_\mathfrak{p} x + N(\mathfrak{p})$ has a

double root α (such that $\alpha^2 = N(\mathfrak{p}) = p$), then we would get that $(\mathrm{Frob}_\mathfrak{p} - \alpha)^2 = 0$. We know (by assumption) that ϕ is semi-simple on M, which is equivalent (by [20]) to saying that $\mathrm{Frob}_\mathfrak{p}$ is semi-simple on $W = V^{\otimes 2}$. Consequently, applying a result of Serre ([31]), we see that $\mathrm{Frob}_\mathfrak{p}$ is semi-simple on V. Hence, the identity $(\mathrm{Frob}_\mathfrak{p} - \alpha)^2 = 0$ gives that $\mathrm{Frob}_\mathfrak{p} = \alpha$ on V. Thus $\mathrm{Frob}_\mathfrak{p}$ acts by α^2 on W, implying that ϕ acts by α^2 on M.

The filtration Fil° is preserved by ϕ, so ϕ also acts by α^2 on the rank 1 subobject $\mathrm{Fil}^2(M) \subset M$. Therefore, the Newton number is just

$$t_N(\mathrm{Fil}^2(M)) = \left(\frac{1}{2} + \frac{1}{2}\right)[E_f : \mathbb{Q}] = [E_f : \mathbb{Q}].$$

However, since $t_H(\mathrm{Fil}^2(M)) = 2[E_f : \mathbb{Q}]$ we obtain that

$$t_H(\mathrm{Fil}^2(M)) > t_N(\mathrm{Fil}^2(M)),$$

which contradicts the weak-admissibility condition for the subobject $\mathrm{Fil}^2(M)$. In conclusion, $a_\mathfrak{p}$ cannot be extremal.

□

3.6 The Tate conjectures

As we have seen in Theorem 3.5.1, the non-extremality of the trace $a_\mathfrak{p}$ of Frobenius at a good prime $\mathfrak{p}$ of odd degree is implied by the semi-simplicity of the crystalline Frobenius ϕ. This leads us to the Tate conjectures that contain such semi-simplicity statements for $\mathrm{Frob}_\mathfrak{p}$ on the étale cohomology, which correspond by Katz-Messing to ϕ. In this section we provide a non-extremality criterion, as a consequence of the Tate conjecture for a product of

two surfaces over a finite field.

Let X be a smooth projective variety of dimension d over a field k, which is finitely generated over its prime field. Let

$$\overline{X} = X \otimes_k \overline{k}$$

be the base change of X to the algebraic closure of k. We have a Galois action of Γ_k on $\overline{X}$ via the second factor.

Fix a prime ℓ, different from the characteristic of k. The Galois group Γ_k acts on the ℓ-adic cohomology $H^j(\overline{X}, \mathbb{Q}_\ell)$ by a representation ρ_j. Denote by $H^j(\overline{X}, \mathbb{Q}_\ell(r))$ (known as the r-th Tate twist) the representation of Γ_k on $H^j(\overline{X}, \mathbb{Q}_\ell)$ defined by $\rho_j \otimes \chi_\ell^r$, where χ_ℓ is the ℓ-adic cyclotomic character. A *Tate class* on X over k is an element of $H^{2r}(\overline{X}, \mathbb{Q}_\ell(r))^{\Gamma_k}$.

An algebraic cycle of codimension $r \leq d$ is an element of the free abelian group (denoted $Z^r(X)$) generated by the irreducible closed subvarieties of X of codimension r. By ℓ-adic Poincaré duality, to every algebraic cycle $Z \in Z^r(X)$ we can associate (via the class map) a class in $H^{2r}(\overline{X}, \mathbb{Q}_\ell(r))$ that is invariant under Γ_k. Such a cohomology class is said to be *algebraic*.

One version of the Tate conjecture (sometimes referred to as the *weak* Tate conjecture) asserts that every Tate class on X is algebraic, i.e,

- $(T_1(X, r))$ The $\mathbb{Q}_\ell$ subspace of $H^{2r}(\overline{X}, \mathbb{Q}_\ell(r))$ generated by the algebraic classes is precisely the space $H^{2r}(\overline{X}, \mathbb{Q}_\ell(r))^{\Gamma_k}$ left fixed by the Galois action.

For our purposes, we will also need a stronger version of the Tate conjecture that involves the zeta function $\zeta(X, r)$ of X over a finite field. Henceforth, we will assume that $k = \mathbb{F}_q$ is a finite field. In this case, the zeta function of X

over k has the form

$$\zeta(X,s) = \frac{P_1(q^{-s})P_3(q^{-s})\dots P_{2d-1}(q^{-s})}{P_0(q^{-s})\dots P_{2d}(q^{-s})},$$

where $P_j(q^{-s})$ is the characteristic polynomial of the geometric Frobenius on $H^j(\overline{X}, \mathbb{Q}_\ell)$.

The *strong* Tate conjecture can be stated as follows:

- $(T_2(X,r))$ The order of the pole of $\zeta(X,s)$ at $s=r$ is equal to the rank of the group of numerical equivalence classes of codimension r cycles on X.

As is to be expected, one knows that $T_2(X,r)$ implies $T_1(X,r)$ (cf. [32]).

Proposition 3.6.1. *Let $\tilde{X}$ be the reduction modulo a good prime $\mathfrak{p}$ of a compact Shimura surface or of the minimal smooth toroidal compactification of a Hilbert modular surface as in section 3.5.4. Assume that $T_2(\tilde{X}\times\tilde{X}, 2)$ holds. Then the polynomial $x^2 - a_{\mathfrak{p}}x + N(\mathfrak{p})$ has distinct roots.*

Proof. An observation of Milne (see [27], Remark 8.6), tells us that the semi-simplicty of the Frobenius element on $H^j(\overline{X}, \mathbb{Q}_\ell(r))$ is implied by the strong Tate conjecture $T_2(\tilde{X}\times\tilde{X}, 2)$. Therefore (since ℓ is distinct from the characersitic of k) if $T_2(\tilde{X}\times\tilde{X}, 2)$ is true, then the crystalline Frobenius ϕ is semi-simple on $H^j(\overline{X}, \mathbb{Q}_\ell)$. It remains to apply Theorem 3.5.1 to get the desired conclusion. □

While the semi-simplicity condition follows from $T_2(X,r)$, one may find it easier to approach $T_1(X,r)$ instead. If we specialize to case $r=1$ (then $Z^1(X)$ is the group of divisors on X) the two conjectures are shown to be equivalent (e.g., [34], Proposition 9.4). We also remark that $T_1(X,1)$ is known for Hilbert-Blumenthal surfaces over finite fields (see [21], [22]).

Bibliography

[1] M. Artebani and I. Dolgachev, The Hesse pecil of plane cubic curves, Enseign. Math (2) **55** (2009), no. 3-4, 235-273.

[2] E. Artin, J. Tate, *Class Field Theory*, Benjamin (1967), 93-103.

[3] M. Aschbacher, *Finite Group Theory*, Cambridge University Press (1986), 108-116.

[4] A. Balog, C. Bessenrodt, J.B. Olsson, K. Ono, *Prime power degree representations of the symmetric and alternating groups*, J. London Math. Soc. (2) **64** (2001), no. 2, 344-356.

[5] C. Bessenrodt, J.B. Olsson, *Prime power degree representations of the double covers of the symmetric and alternating groups*, J. London Math. Soc. (2) **66** (2002), no. 2, 313-324.

[6] D. Blasius, J. Rogawski, *Motives for Hilbert modular forms*, Invent. Math. **114** (1993), no. 1, 55-87.

[7] H.F. Blichfeldt, *Finite collineation groups*, University of Chicago Press 1917.

[8] L. Chiriac, *Irreducible adjoint representations in prime power dimensions, with an application*, J. Ramanujan Math. Soc. **30**, no. 2 (2015), 205-218.

[9] R.F. Coleman, B. Edixhoven, *On the semi-simplicity of the U_p-operator on modular forms*, Math. Ann. **310** (1998), no. 1, 119-127.

[10] W. Decker, *Das Horrocks-Mumford Bündel und das Modul-Schema für stabile 2-Vectorbündel über $\mathbb{P}_4$ mit $c_1 = -1$, $c_2 = 4$*, Matt. Z. **188** (1984), no. 1, 101-110.

[11] N. Elkies, *The existence of infinitely many supersingular primes for every elliptic curve over $\mathbb{Q}$*, Invent. Math. **89** (1987), no. 3, 561-567.

[12] G. Faltings, *Crystalline cohomology and p-adic Galois- representations*, Algebraic analysis, geometry, and number theory, Johns Hopkins Univ. Press, Baltimore, MD (1989), 25-80.

[13] W. Grimus and P.O. Ludl, *Principal series of finite subgroups of SU(3)*, J. Phys. A: Math. Theor. **43** (2010) 445209.

[14] R.M. Guralnick and P.H. Tiep, *Decompositions of small tensor powers and Larsen's conjecture*, Represent. Theory **9** (2005), 138-208.

[15] G. Harder, R. Langlands, M. Rapoport, *Algebraische Zycklen auf Hilbert-Blumenthal-Flächen*, J. Reine. Angew. Math. **366** (1986), 53-120.

[16] I. Hambleton and R. Lee, *Finite Group Actions on $\mathbb{P}^2(\mathbb{C})$*, J. Algebra **116** (1988), no. 1, 227-242.

[17] G. Horrocks and D. Mumford, *A rank 2 vector bundle on $\mathbb{P}^4$ with 15000 symmetries*, Topology **12** (1973), 63-81.

[18] G. Karpilovsky, *Group Representations*, North-Holland Mathematics Studies (1992), vol 1, part B, 808-813.

[19] G. Karpilovsky, *Induced Modules over Group Algebras*, North-Holland Mathematics Studies (1990), 45-48.

[20] N.M. Katz, W. Messing, *Some consequnces of the Riemann hypothesis for varieties over fiite fields*, Invent. Math. **23** (1974), 73-77.

[21] A. Langer, *On the Tate-conjecture for Hilbert modular surfaces in finite characteristic*, J. reine angew. Math. **570** (2004), 219-228.

[22] A. Langer, *Zero-cycles on Hilbert-Blumenthal surfaces*, Duke Math. J. **103** (2000), no. 1, 131-163.

[23] K. Magaard, G. Malle, *Irreducibility of alternating and symmetric squares*, Manuscripta Math. **95** (1998), 169-180.

[24] K. Magaard, G. Malle and P.H. Tiep, *Irreducibility of tensor squares, symmetric squares and alternating sqaures*, Pacific J. Math. **202** (2002), no. 2, 379-427.

[25] G. Malle, *Almost irreducible tensor squares*, Comm. Algebra **27** (1999), no. 3, 1033-1051.

[26] G. Malle and A. E. Zalesskii, *Prime power representations of quasi-simple groups*, Arch. Math. **77** (2001), 461-468.

[27] J.S. Milne, *Values of zeta functions of varieties over finite fields*, Amer. J. Math. **108** (1986), no.2, 297-360.

[28] V.K. Murty, D. Ramakrishnan, *Period relations and the Tate conjecture for Hilbert modular surfaces*, Invent. Math. **89** (1987), 319-345.

[29] D. Ramakrishnan, *An exercise concerning the selfdual cusp forms on GL(3)*, Indian J. Pure Appl. Math. **45** (2014), no. 5, 777-784.

[30] J.P. Serre, *Quelques applications du théoremè de densité de Chebotarev*, Inst. Hautes Études Schi. Publ. Math. No. **54** (1981), 323-401.

[31] J.P. Serre, *Semisimplicity and tensor products of group representations: converse theorems*, J. Algebra **194** (1997), no.2, 496-520.

[32] J. Tate, *Conjectures on algebraic cycles in ℓ-adic cohomology*, Proc. Sympos. Pure Math. **55**, part 1 (1994), 71-83.

[33] R. Taylor, *On Galois representations associated to Hilbert modular forms*, Invent. Math. **98** (1989), 265-280.

[34] D. Ulmer, *Elliptic curves over function fields*, Arithmetic of L-functions, Amer. Math. Soc., Providence, RI (2011), 211-280.

[35] C. Virdol, *Algebraic cycles ina product of two Hilbert modular surfaces*, Trans. Amer. Math. Soc. **362** (2010), no. 7, 3691-3703.

[36] N. Walji, *On the Hecke eigenvalues and a lacunarity question of Serre*, Math. Res. Lett. **21** (2014), no. 6, 1465-1482.

[37] T. Weston, *The modular curves $X_0(11)$ and $X_1(11)$*, expository paper.

[38] D. L. Winter, *The automorphism group of an extraspecial p-group*, Rocky Mountain J. of Math. **2** (1972), no. 2, 159-168.