Modular Galois Realizations of Linear Groups

Memoria presentada
para optar al grado de
Doctor en Matemáticas
por

Luis Victor Dieulefait[1]
Departamento de Álgebra y Geometría
Universitat de Barcelona

April 25, 2001

[1]supported by TMR - Marie Curie Fellowship ERBFMBICT983234

Departamento de Álgebra y Geometría
Programa de Doctorado de Álgebra y Geometría, Bienio 1996-1998.
Doctorando: Luis Victor Dieulefait
Directora de Tesis: Dra. Núria Vila Oliva

Núria Vila Oliva, Profesora Titular de Álgebra
de la Facultad de Matemáticas de la Universitat de Barcelona,
HAGO CONSTAR
que el señor Luis Victor Dieulefait ha realizado esta memoria
para optar al grado de Doctor en Matemáticas bajo mi dirección.

Barcelona, abril del 2001.

Firmado: Núria Vila Oliva

To those whose infinite curiosity and endless imagination have produced a secret world of whispering thoughts. To Pierre de Fermat, Évariste Galois, Beppo Levi, Yutaka Taniyama and Robert Langlands.

"Escribimos
porque no sabemos
de allí
por qué
o para...
aunque persiste
¿qué decir?
Aldebarán en el ojo del toro
o la luna
que nosotros los antiguos
la llamamos
el ojo de la noche.
Y aunque hollada por el pie
quebrado su silencio
dice
que al fin de cuentas,
bajo cualquier operatoria
yace el uno,
lo que es mucho decir
para nombrar
y uno nada más.
Es suficiente."
Víctor Zenobi

Contents

Chapter 1

Prolegomena

1.1 Foreword

In this thesis we investigate the problem of giving criteria for the images of a compatible family of ℓ-adic Galois representations to be generically large, meaning that for almost every prime the images are as large as they can possibly be. The families of Galois representations that we will consider will be modular or geometric, attached to a modular form or to a smooth projective variety. Through the different chapters we will deal with the cases of two, three and four dimensional such families of representations. We will also give effective methods to bound the set of exceptional primes (those where the image is not as large as possible) and we will derive the corresponding consequences from the point of view of inverse Galois theory.
The maximal possible image is defined taking into account the intrinsic restrictions in each case. For example, in the case of principally polarized abelian surfaces (chapter 5) we know a priori that the Galois representations on Tate's modules are symplectic.
The results obtained in this thesis suggest that for algebraic modular forms on an arbitrary reductive group, the images of the attached (in most cases conjectural) compatible family of Galois representations will be generically large if and only if the modular form does not come from any smaller reductive group.

In the two-dimensional case we will concentrate on Galois representations attached to weight 2 modular forms without Complex Multiplication (CM). In this case Momose and Ribet have proved that the images are generically large. In chapter two we concentrate on the case of newforms without CM and without inner twists. We reproduce in detail Ribet's proof that the set of primes such that the image is not maximal is finite. This close examination allows us to give an algorithm for an explicit determination of the exceptional set, and we apply it to many examples, most of them of newforms with $\mathbb{Q}_f$ abelian of degree up to 4. This provides a large number of new families of projective linear groups realized as Galois groups over $\mathbb{Q}$.

In chapter three we again review the results of Momose and Ribet but now for the more general case of newforms with inner twists. We generalize the algorithm of the previous chapter to this case. For simplicity, we will only consider newforms with a single inner twist. Applying the resulting algorithm to certain "well-posed" examples we obtain new families of projective linear groups as Galois groups over $\mathbb{Q}$.

In chapter four we study the case of compatible families of three-dimensional Galois representations constructed in the étale cohomology of a smooth projective variety. We prove a theorem asserting that the images will be generically large if certain easy to check conditions are satisfied. In this case it is only conjectured, but not yet proved, that such a compatible family of Galois representations will have a uniformly bounded conductor; so instead of proving the result on the images for all but finitely many primes we can only prove it for all primes outside a density 0 set. All conditions are necessary in the strong sense that if any of them is not satisfied then the images become smaller for all primes. For instance, we have to avoid selfdual or reducible representations. Non-selfduality implies that the representations will be defined over an imaginary field, and all known examples (with any chance of having large images) have coefficients in imaginary quadratic fields. We will assume from the beginning that this is the case. For primes inert in the field of definition, the representations (if irreducible) will be unitary. We give an explicit description of our result, and apply it to an example constructed by van Geemen and Top. As a consequence we obtain a family of special linear groups and one of special unitary groups as Galois groups over $\mathbb{Q}$.
We will also consider the case of a cohomological modular form for a congruence subgroup of $\mathrm{SL}(3, \mathbb{Z})$ and we will assume Clozel's conjecture stating that a geometric family of three-dimensional Galois representations can be attached to it. We will give conditions on the modular form guaranteeing the validity of the result on the largeness of the images of the Galois representations. We will apply this result to several examples (satisfying the required

conditions and with imaginary quadratic field of coefficients) obtaining as a consequence new families of special linear/unitary groups as Galois groups over $\mathbb{Q}$ (assuming Clozel's conjecture).

In chapter five we give an effective version of a result reported by Serre asserting that the images of the Galois representations attached to an abelian surface with $\mathrm{End}(A) = \mathbb{Z}$ are as large as possible for almost every prime. The proof given by Serre depends on ineffective results of Faltings, so new and different arguments are needed. Our algorithm depends on the truth of Serre's conjecture for two dimensional odd irreducible Galois representations. Assuming this conjecture we determine the finite set of primes with exceptional image. We also give infinite sets of primes for which we can prove (unconditionally) that the images of the corresponding Galois representations are large.

In chapter six we address the similar problem of the determination of the images of the Galois representations attached to genus 2 Siegel cusp forms of level 1 and having multiplicity one. These representations are symplectic. We prove that the images are as large as possible for almost every prime, if the Siegel cusp form is not a Maass spezialform and verifies two easy to check conditions. Assuming Serre's conjecture we give an algorithm for the determination of the finitely many exceptional primes. We also obtain infinite sets of primes for which we can prove (unconditionally) that the images of the corresponding Galois representations are large.

Through all the chapters there are two tools whose use is fundamental in the proof of the results (sometimes they are hidden, but they are always present), namely: the classification of all maximal proper subgroups of the corresponding projective linear, unitary or symplectic group (the results of Dickson and Mitchell) and the description of the image of the inertia subgroup at ℓ, and its relation with Hodge-Tate decompositions (the results of Raynaud, Fontaine-Laffaille, and Fontaine-Messing).

Notation: When a reference is made to a section in another chapter, the number of the chapter is explicitly stated. For example, when a reference to section 4.6.3 is made in chapter 6 we put "see chapter 4, section 6.3". For references to a section in the same chapter, the number of the chapter is omitted. For example, when a reference to section 4.6.3 is made in chapter 4 we put "see section 6.3". Theorems, lemmas, and all other propositions are numbered according to the chapter where they belong. Note that each chapter has a separate bibliography.

The contents of chapter 2 have been published as "Projective Linear Groups as Galois Groups over $\mathbb{Q}$ via Modular Representations" (joint work with N. Vila), Journal of Symbolic Computation (2000) **30** 799-810 (Special Issue on Algorithmic Methods in Galois Theory; editors: Matzat, McKay, Yokoyama). The contents of chapter 3 have been accepted for publication in the Journal de Théorie des Nombres de Bordeaux.

Agradecimientos: Este trabajo no hubiera ni tan siquiera sido imaginado si no fuera por el empuje y la constancia de Virginia. Gracias por arriesgarte. Gracias a mi familia y amigos, por soportar estoicamente mis embistes matemáticos, y por todos los buenos momentos.
No quiero olvidar en esta ocasión a todos los que sembraron en mí la inquietud, la insaciedad, el goce de la búsqueda, el gusto por el reto. A vos mamá, a papá, a mis tíos y a mis profesores, en especial a Randazzo, Chacho Pereira, Aranda, Kantor, Z. Marcas, Scarparo, Verdes y muy especialmente a Pedro Marangunic.

Agradezco enormemente al profesor Juan Tena por su generosidad al abrirme las puertas para realizar estudios de doctorado en la Universidad de Valladolid, su apoyo fue esencial para mí. De igual modo agradezco a la profesora Pilar Bayer por el cálido recibimiento y por introducirme al Seminari de Teoria de Nombres de Barcelona (STNB). Muy valiosas fueron las charlas con X. Xarles, B. Plans, F. Bars, P. Bayer, W. Stein, A. Brumer, D. Prasad, A. Pacheco, C. Infante, D. Maisner, K. Ribet, F. Holgado, V. Rotger y J. C. Lario. Gracias a todos ellos por sus sugerencias y correcciones.

Sobra decir que por encima y por detrás de toda esta tesis está la mano de mi directora. Gracias a ella, Núria Vila, no sólo por el apoyo, si no también por apostar por este proyecto.

Diferentes partes de esta tesis han sido expuestas en congresos y seminarios sea por mí, sea por mi directora. Agradezco a este respecto en particular a K. Ribet por darme la posibilidad de exponer (una versión preliminar de) el capítulo 4 en el Seminario de Representaciones de Galois en el MSRI, Berkeley, USA, en octubre de 1999.

1.2 Resumen

En esta tesis investigamos el problema de dar criterios para que las imágenes de una familia compatible de representaciones de Galois sean"tan grande como es posible" para casi todo primo. Las familias de representaciones de Galois que consideraremos serán modulares o geométricas, asociadas a ciertas formas modulares o a alguna variedad lisa y proyectiva. A través de los diferentes capítulos trataremos los casos de tales familias de representaciones de dimensión dos, tres y cuatro. En cada caso también daremos métodos efectivos para acotar el conjunto de primos excepcionales, es decir, aquellos para los cuales la imagen no es "tan grande como es posible", y sacaremos las consecuencias correspondientes desde el punto de vista del problema inverso de la teoría de Galois. La imagen más grande posible se define teniendo en cuenta las restricciones intrínsecas en cada caso, por ejemplo en el caso de superficies abelianas principalmente polarizadas (capítulo 5) sabemos a priori que las representaciones de Galois en los módulos de Tate son simplécticas.

Los resultados obtenidos en esta tesis sugieren que para formas modulares algebraicas en un grupo reductivo G arbitrario, las imágenes de las familias compatibles de representaciones de Galois asociadas (en la mayoría de los casos estas representaciones sólo existen conjeturalmente) serán "tan grande como es posible" para casi todo primo si y solo si la forma modular no proviene de un grupo reductivo menor.

A lo largo de los capítulos hay dos herramientas cuya utilización es fundamental en la demostración de los resultados principales (algunas veces no se las menciona explícitamente, pero siempre están allí) que son: la clasificación de todos los subgrupos propios maximales del correspondiente grupo proyectivo lineal, unitario o simpléctico (resultados de Dickson y Mitchell) y la descripción de la imagen del subgrupo de inercia en ℓ y su relación con la descomposición de Hodge-Tate (resultados de Raynaud, Fontaine-Laffaille, Fontaine-Messing y Faltings).

1.2.1 Imágenes de representaciones de Galois asociadas a formas nuevas sin Multiplicación Compleja - Capítulos 2 y 3

El objetivo de los capítulos dos y tres es el de aplicar un resultado de Momose y Ribet acerca de las imágenes de representaciones de Galois asociadas a for-

mas modulares nuevas a la realización de grupos proyectivos lineales como grupos de Galois sobre $\mathbb{Q}$.
El resultado de Momose y Ribet dice que las imágenes de estas representaciones ℓ-ádicas son "tan grande como es posible" para casi todo primo ℓ, siempre que la forma nueva no tenga Multiplicación Compleja (MC) ni twists internos.

En el capítulo dos nos concentramos en este caso. Hemos obtenido un algoritmo que permite acotar el conjunto finito de primos excepcionales, es decir, aquellos para los que la imagen de la correspondiente representación no es maximal, suponiendo que la forma nueva es de peso 2 y de nebentypus trivial. Hemos calculado algunos ejemplos de formas nuevas f con $\mathbb{Q}_f$ abeliano de grado $2, 3$ y 4. Aplicándoles el algoritmo a estas formas nuevas, obtenemos varias familias de grupos proyectivos lineales sobre cuerpos finitos realizados como grupos de Galois sobre $\mathbb{Q}$, por ejemplo ($\ell \geq 5$):

$$\mathrm{PSL}(2, \mathbb{F}_{\ell^2}), \quad \ell \not\equiv \pm 1 \pmod{120} \quad \text{o} \quad \ell \not\equiv \pm 1, \pm 4 \pmod{17};$$

$$\mathrm{PGL}(2, \mathbb{F}_{\ell^3}), \quad \ell \not\equiv \pm 1 \pmod{7} \quad \text{o} \quad \ell \not\equiv \pm 1 \pmod{9};$$

$$\mathrm{PSL}(2, \mathbb{F}_{\ell^4}), \quad \ell \equiv 2, 3 \pmod{5} \quad \text{o} \quad \left(\frac{17}{\ell}\right) = -1.$$

Además, combinando nuestro resultado con otro de Reverter-Vila hemos probado que los grupos:

$$\mathrm{PSL}(2, \mathbb{F}_{\ell^2}), \quad \text{para todo} \quad 5 \leq \ell \leq 5000000 \quad \text{y}$$

$$\mathrm{PGL}(2, \mathbb{F}_{\ell^3}), \quad \text{para todo} \quad 5 \leq \ell \leq 500000$$

son grupos de Galois sobre $\mathbb{Q}$.

En el capítulo tres consideramos el caso de formas nuevas con twists internos, siempre bajo las condiciones: peso 2, nebentypus trivial y sin MC. En este caso las imágenes de las representaciones restringidas a un cierto subgrupo abierto H de $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ que se define en término de los caracteres que aparecen en los twists, vienen dadas por matrices con coeficientes en (la completación ℓ-ádica de) el subcuerpo de $\mathbb{Q}_f$ fijo por los twists internos, para casi todo ℓ. Nuevamente estas imágenes son "tan grande como es posible" para casi todo ℓ. También se tiene, gracias a un resultado de Papier, una descripción de la imagen de todo $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ para estos primos. Hemos obtenido condiciones que nos permiten hacer explícito el conjunto de primos excepcionales en este caso y las hemos aplicado a ejemplos de formas nuevas con un solo twist interno.

En los ejemplos, probamos que no hay primos excepcionales de entre los primos con índice de inercia prefijado. Como consecuencia realizamos los grupos ($\ell \geq 5$):

$$\mathrm{PGL}(2, \mathbb{F}_{\ell^5}), \quad \ell \not\equiv \pm 1, 0 \pmod{11} \quad \text{y}$$

$$\mathrm{PGL}(2, \mathbb{F}_{\ell^2}), \quad \ell \not\equiv \pm 1 \pmod{48} \quad \text{o} \quad \ell \not\equiv \pm 1 \pmod{5} \qquad (*)$$

como grupos de Galois sobre $\mathbb{Q}$.

Obsérvese que la familia de grupos (*) no podría haberse obtenido usando formas nuevas sin twists internos. Con dichas formas nuevas solo pueden obtenerse grupos de la forma $\mathrm{PXL}(2, \mathbb{F}_{\ell^r})$, con $X = S$ si r es par y $X = G$ si r es impar. Pero en el caso de una forma nueva con twists internos, probamos que si ℓ es un primo tal que la imagen de la restricción de la representación a H es $\mathrm{PSL}(2, \mathbb{F}_{\ell^{2t}})$ y ℓ verifica una condición adicional, usando la descripción de la imagen de $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ se obtiene el grupo $\mathrm{PGL}(2, \mathbb{F}_{\ell^{2t}})$. Este resultado se utilizó para obtener la familia de grupos (*).

1.2.2 Representaciones de Galois de dimensión tres - Capítulo 4

La conjetura de Clozel predice la existencia de una familia compatible de representaciones de Galois tridimensionales asociadas a una forma propia de Hecke en la cohomología de un subgrupo congruencial de $\mathrm{SL}(3, \mathbb{Z})$. En particular los autovalores de la forma propia de Hecke coincidirían con las trazas de las imágenes de los correspondientes elementos de Frobenius.
van Geemen y Top han construido ejemplos de representaciones de Galois geométricas tridimensionales, que vienen dadas por la acción del grupo de Galois en los ciclos transcendentes de una superficie proyectiva y lisa. Algunos de estos ejemplos dan evidencia experimental para la conjetura de Clozel debido a que (luego de hacer un twist apropiado a estas representaciones para que se cumpla la condición necesaria de que su determinante

sea el carácter ciclotómico al cubo) todos los valores calculados de trazas de imágenes de elementos de Frobenius coinciden con los autovalores de una forma propia de Hecke.
En todos los ejemplos las representaciones de Galois vienen dadas por espacios vectoriales de dimensión tres sobre $\mathbb{Q}_\ell(i)$.
Hemos estudiado las imágenes de estas representaciones geométricas y hemos obtenido resultados similares a los de Serre, Momose y Ribet en el caso de dimensión dos.

Nuestro resultado principal es que si las trazas de las imágenes de los elementos de Frobenius y la filtración de Hodge del motivo de rango tres en el que estamos representando satisfacen ciertas condiciones (que pueden ser efectivamente verificadas), entonces las imágenes de las representaciones residuales serán "tan grande como es posible" para todo primo fuera de un conjunto de densidad de Dirichlet 0. Esta imagen será (luego de hacer un adecuado twist): $\mathrm{SL}(3,\mathbb{F}_\ell)$ si $\ell \equiv 1 \pmod 4$ (primos que descomponen) y $\mathrm{SU}(3,\mathbb{F}_\ell)$ si $\ell \equiv 3 \pmod 4$ (primos inertes). El hecho de que para primos inertes con imagen irreducible esta sea unitaria es consecuencia de la hipótesis de Riemann.

Si supiéramos que existe un conductor uniforme (acotado independientemente de ℓ) para estas familias compatibles de representaciones podríamos reemplazar el conjunto de densidad 0 posiblemente excepcional por un conjunto finito de primos, el cual podría calcularse explícitamente si se conociera el valor de este conductor.

En el caso de los primos $\ell \equiv 1 \pmod 4$, con el propósito de dar resultados explícitos, hemos excluido un conjunto de densidad pequeña (aunque no nula) que contiene al conjunto de densidad 0 que debe excluirse (y a fortiori contiene a todos los primos excepcionales). En el caso de primos $\ell \equiv 3 \pmod 4$ hemos logrado describir explícitamente un conjunto de densidad 0 que contiene a todos los primos excepcionales.
Las técnicas que se utilizan en la demostración del teorema principal incluyen la clasificación de subgrupos maximales de $\mathrm{PSL}(3,\mathbb{F}_q)$ debida a Mitchell, el teorema de comparación entre cohomologías étale y cristalina de Fontaine-Messing y su aplicación a la determinación de la imagen del subgrupo de inercia en ℓ (resultado previamente conjeturado por Serre), los resultados de Fontaine y Laffaille relacionando la filtración de Hodge con los pesos del

subgrupo de inercia en ℓ y las técnicas ya utilizadas por Serre y Ribet en el tratamiento de representaciones de Galois de dimensión dos.

Las condiciones que la familia de representaciones de Galois ha de verificar para que le sea aplicable el teorema son fácilmente verificables y están destinadas a excluir casos de representaciones para las que claramente la imagen no sería maximal: representaciones autoduales, reducibles o monomiales (inducidas por un carácter de una extensión de $\mathbb{Q}$). También hay restricciones sobre la filtración de Hodge del motivo que da las representaciones.
La información sobre la filtración de Hodge se utiliza para poder decir que la imagen del subgrupo de inercia en ℓ proporciona un subgrupo no trivial cuyo orden crece con ℓ, no solo de la representación residual si no también de su proyectivización. Esta información será esencial a la hora de eliminar la posibilidad de que la imagen coincida con uno de los grupos excepcionales si ℓ es suficientemente grande y, bajo la hipótesis de que la familia de representaciones no es monomial, la posibilidad de que sea el normalizador de un grupo abeliano.

Hemos aplicado el teorema a uno de los ejemplos de van Geemen y Top (uno de los que está conjeturalmente asociado a formas modulares) y calculado los primos excepcionales. Esto automáticamente se aplica a la realización de grupos lineales y unitarios como grupos de Galois sobre $\mathbb{Q}$. El resultado obtenido es el siguiente:

Los grupos $\mathrm{SL}(3, \mathbb{F}_\ell)$ son grupos de Galois sobre $\mathbb{Q}$ para todo primo

$$\ell \equiv 1 \pmod 4,\ \ell \not\equiv 1 \pmod{64},\ \ell > 5.$$

Más aún, lo mismo es cierto para todo $\ell \equiv 1 \pmod 4$, excepto a lo sumo por un conjunto de primos de densidad de Dirichlet 0.
Los grupos $\mathrm{SU}(3, \mathbb{F}_\ell)$ son grupos de Galois sobre $\mathbb{Q}$ para todo primo

$$\ell \equiv 3 \pmod 4,\ \ell \not\equiv -1 \pmod{2^{13}},\ \ell > 3,$$

y para todo $\ell \equiv 3 \pmod 4$, $(\frac{33}{\ell}) = -1$, $\ell > 3$. Más aún, lo mismo vale para todo $\ell \equiv 3 \pmod 4$, excepto a lo sumo por un conjunto de primos de densidad de Dirichlet 0 (y podemos describir explícitamente un tal conjunto de densidad 0).

Versión fuerte de la conjetura de Clozel y aplicaciones

También hemos aplicado las técnicas ya descritas al caso de una familia compatible de representaciones de Galois asociadas a una forma propia de Hecke cuspidal según lo predice la conjetura de Clozel. Con este propósito damos una versión más fuerte de esta conjetura que afirma que estas representaciones de Galois han de ser motívicas, la restricción al subgrupo de inercia en ℓ ha de estar relacionada con el "peso" de la forma modular, como en la definición de peso que se da en la conjetura de Serre, y el conductor de la familia de representaciones de Galois ha de dividir al nivel de la forma propia. La descripción de la restricción al subgrupo de inercia en ℓ concuerda con la generalización de la conjetura de Serre a dimensiones mayores hecha por Ash y Sinnot. La relación entre el conductor y el nivel es como en el caso de formas modulares clásicas y evita tener que trabajar con conductor indeterminado, permitiendo así obtener los resultados para casi todo primo y no solamente para todo primo fuera de un conjunto de densidad 0.

Asumiendo esta versión fuerte de la conjetura hemos obtenido ejemplos de familias de representaciones de Galois sobre diferentes cuerpos cuadráticos imaginarios. Las condiciones sobre las representaciones de Galois que se necesitan para garantizar imágenes grandes se traducen en condiciones (gracias a que se corresponden con casos de funtorialidad de Langlands ya resueltos) sobre la forma modular. La conclusión es que para formas propias de Hecke cuspidales no autoduales ni inducidas por un carácter de Hecke de (la clausura normal de) una extensión cúbica de $\mathbb{Q}$, las imágenes de las representaciones de Galois asociadas son "tan grande como es posible" para casi todo primo, es decir, un grupo lineal si el primo descompone en el cuerpo cuadrático imaginario $\mathbb{Q}_f$ y un grupo unitario en caso contrario. Aplicando a ejemplos concretos de formas propias de Hecke las técnicas ya aplicadas a representaciones geométricas se obtiene una determinación explícita del conjunto finito de primos excepcionales y se prueba que nuevas familias de grupos lineales y unitarios sobre cuerpos finitos aparecen como grupos de Galois sobre $\mathbb{Q}$ (asumiendo la conjetura fuerte de Clozel).

Por ejemplo, usando una forma propia de Hecke f de nivel 88 con $\mathbb{Q}_f = \mathbb{Q}(\sqrt{-7})$ y una de nivel 128 con $\mathbb{Q}_f = \mathbb{Q}(i)$ se realizan como grupos de Galois sobre $\mathbb{Q}$ los siguientes grupos:

$$\mathrm{SL}(3, \mathbb{F}_\ell) \quad \text{para todo} \quad \ell \equiv 1, 2, 4 \pmod 7,\ \ell \geq 13 \quad \text{y}$$

$$\mathrm{SU}(3,\mathbb{F}_\ell) \quad \text{para todo} \quad \ell \equiv 3,5,6 \pmod 7,\ \ell \geq 5.$$

Usando una forma propia de Hecke f de nivel 53 con $\mathbb{Q}_f = \mathbb{Q}(\sqrt{-11})$ y una de nivel 128 con $\mathbb{Q}_f = \mathbb{Q}(i)$ se realizan como grupos de Galois sobre $\mathbb{Q}$ los grupos:

$$\mathrm{SL}(3,\mathbb{F}_\ell) \quad \text{para todo} \quad \ell \equiv 1,3,4,5,9 \pmod{11},\ \ell > 5 \quad \text{y}$$

$$\mathrm{SU}(3,\mathbb{F}_\ell) \quad \text{para todo} \quad \ell \equiv 2,6,7,8,10 \pmod{11},\ \ell \geq 5.$$

1.2.3 Representaciones de Galois asociadas a superficies abelianas - Capítulo 5

Sea A una superficie abeliana principalmente polarizada definida sobre $\mathbb{Q}$ con $\mathrm{End}(A) = \mathbb{Z}$. Serre probó que las imágenes de las representaciones de Galois asociadas son "tan grande como es posible" para casi todo primo, es decir, $\mathrm{GSp}(4,\mathbb{Z}_\ell)$. Para todo ℓ esto equivale al hecho de que la imagen de la representación de Galois residual es $\mathrm{GSp}(4,\mathbb{F}_\ell)$. Serre propuso el problema de calcular efectivamente el conjunto finito de primos excepcionales en ejemplos concretos de jacobianas de curvas de género dos dadas. Su demostración depende de resultados no efectivos de Faltings y por lo tanto no permite efectuar esta determinación.

En este capítulo se dará un método para realizar dicha determinación explícita si se asume la validez de la conjetura de Serre para representaciones dos dimensionales irreducibles e impares. Las técnicas utilizadas incluyen la clasificación de subgrupos maximales de $\mathrm{PSp}(4,\mathbb{F}_q)$ obtenida por Mitchell y el mismo tipo de argumentos ya aplicados en el caso de dimensión tres. Todos los casos de imagen no maximal se corresponden con ciertas congruencias que han de verificar los polinomios característicos de las imágenes de los elementos de Frobenius, y esto permite la determinación de los primos excepcionales.

En el caso de una representación residual que reduce y su semi-simplificación es la suma de dos representaciones impares irreducibles dos dimensionales, puede ocurrir que ambas estén relacionadas (usando la propiedad de reciprocidad de las raíces de matrices simplécticas), en cuyo caso obtenemos congruencias para los polinomios característicos. De no ser así, puede aplicarse la conjetura de Serre para concluir que ambas representaciones deben coincidir con las reducciones de sendas formas cuspidales clásicas de peso dos con nivel dividiendo al conductor de la variedad abeliana. De este modo obtenemos un procedimiento que en un número finito de pasos calcula los primos que podrían caer en este caso comparando los polinomios característicos correspondientes a la acción del grupo de Galois en los módulos de Tate de la variedad abeliana con productos de dos polinomios característicos correspondientes a formas cuspidales verificando las condiciones indicadas.

Es de fundamental importancia que el conductor de la familia de representaciones de Galois asociadas a la jacobiana de una curva de género dos dada puede calcularse efectivamente (o al menos acotarse).

Por ejemplo, considérese la curva de género dos:

$$y^2 = x^6 - x^3 - x + 1.$$

Si llamamos σ_ℓ a la representación de Galois asociada al ℓ-ésimo módulo de Tate de su jacobiana, entonces σ_ℓ es no ramificada fuera de $2 \cdot 5 \cdot 23 \cdot \ell$. Más aún, si calculamos el conductor c de esta jacobiana obtenemos que $c \mid 2^{12} \cdot 23 \cdot 5$. Aplicando el algoritmo a este ejemplo no encontramos primos no ramificados excepcionales, por lo que concluimos que la imagen de σ_ℓ es $\mathrm{GSp}(4, \mathbb{Z}_\ell)$ para todo $\ell > 5$, $\ell \neq 23$ (asumiendo la conjetura de Serre).

En otros ejemplos, también damos conjuntos infinitos de primos para los cuales podemos probar el resultado sobre las imágenes en forma incondicional, es decir sin asumir la conjetura de Serre. Este tipo de resultados han sido obtenidos recientemente por Le Duff con otros métodos, pero solo bajo la hipótesis de que la superficie abeliana considerada debía tener reducción semi-abeliana en algún primo. Comparativamente, nuestro método presenta dos ventajas: no impone restricción alguna sobre el tipo de reducción de la variedad abeliana y aún en el caso de reducción semi-abeliana da una prueba del resultado sobre las imágenes para conjuntos más grandes de primos, siempre trabajando incondicionalmente.

Un ejemplo que verifica la condición de reducción semi-abeliana viene dado por la curva de género dos:

$$C_2 : \quad y^2 = x^5 - x + 1.$$

El conductor de la jacobiana de C_2 divide a $2^8 \cdot 19 \cdot 151$.
Aplicando nuestro método (asumiendo la conjetura de Serre) probamos que

las imágenes de las representaciones de Galois asociadas a $J(C_2)$ son:

$$\mathrm{GSp}(4, \mathbb{Z}_\ell) \quad \text{para todo } \ell > 2.$$

También probamos incondicionalmente (sin apelar a la conjetura de Serre) que el resultado anterior es válido para todo $\ell > 3$ tal que $(\frac{5}{\ell}) = -1$.

Un ejemplo que no verifica la condición de reducción semi-abeliana viene dado por la curva de género dos:

$$C_3: \quad y^2 = x(x^4 + 32x^3 + 336x^2 + 1152x - 64).$$

El conductor de la jacobiana de C_3 divide a 2^{20}.
Nuevamente en este ejemplo aplicando nuestro método (asumiendo la conjetura de Serre) vemos que las imágenes de las representaciones de Galois asociadas a $J(C_3)$ son: $\mathrm{GSp}(4, \mathbb{Z}_\ell)$ para todo $\ell > 3$.
Incondicionalmente, probamos que el resultado anterior es válido para todo $\ell > 3$ tal que $(\frac{3}{\ell}) = -1$.

1.2.4 Representaciones de Galois asociadas a formas de Siegel de género 2 - Capítulo 6

En éste capítulo aplicamos las mismas técnicas que en el anterior al estudio de las imágenes de las familias compatibles de representaciones de Galois asociadas a formas modulares de Siegel cuspidales de género 2 respecto al grupo modular de Siegel $\mathrm{Sp}(4, \mathbb{Z})$ de peso par k que son formas propias de Hecke. Dichas representaciones de Galois de dimensión cuatro han sido construidas por Taylor y Weissauer.
Nos restringimos al caso en que la representación automorfa correspondiente a la forma modular de Siegel tiene multiplicidad uno. En este caso las representaciones de Galois son simplécticas.

Consideramos ejemplos explícitos de estas formas de Siegel para los que los primeros coeficientes de Fourier han sido calculados por Skoruppa y probamos que las imágenes son "tan grande como es posible" para casi todo primo. Los ejemplos de Skoruppa no corresponden a Maass spezialformen (formas modulares de Siegel en la imagen del levantamiento de Saito-Kurokawa) ni tampoco a series de Eisenstein-Klingen. Para los casos excluidos es sabido que la imagen no es maximal para ningún primo.

Como en el capítulo previo, se utiliza fuertemente la clasificación de subgrupos maximales de $\mathrm{PSp}(4, \mathbb{F}_q)$ (esta vez sobre un cuerpo finito arbitrario). Para la determinación explícita del conjunto finito de primos excepcionales se asume la conjetura de Serre sobre representaciones de Galois irreducibles e impares de dimensión dos.

Para obtener resultados explícitos sin asumir la conjetura de Serre procedemos como en el capítulo anterior. A cada polinomio característico de la imagen de un elemento de Frobenius le asociamos un cierto discriminante d_p. Si d_p no es un cuadrado obtenemos el resultado incondicional de imagen maximal para "la mitad" de los primos.

El algoritmo que resulta, sea asumiendo la conjetura de Serre o no, es muy similar al obtenido en el capítulo anterior, y algunas diferencias numéricas se deben al hecho de que los pesos de la acción de la inercia son diferentes y el conductor de la familia de representaciones de Galois es ahora 1. Además, el hecho de que en este capítulo las representaciones estén definidas sobre extensiones de $\mathbb{Q}_\ell$ trae complicaciones del tipo que se encuentran en los capítulos 2 y 3. Aparte de estas diferencias y otros cambios menores, las ideas utilizadas para obtener el algoritmo de cálculo de primos excepcionales son las mismas en ambos capítulos.

Asumiendo la conjetura de Serre, se demuestra que para toda forma cuspidal de Siegel de género 2 para todo el grupo modular de Siegel, de peso par, con multiplicidad uno, que no sea una Maass spezialform y verifique una condición adicional (similar a la condición de no tener twists internos impuesta en el capítulo 2 a formas modulares clásicas), las imágenes de las representaciones de Galois correspondientes serán "tan grande como es posible" para casi todo primo (el grupo simpléctico maximal que corresponda).

Más aún, en la última sección se prueba un resultado más fuerte utilizando la teoría de pseudorepresentaciones: con las hipótesis anteriores, el resultado anterior sigue siendo cierto aún sin asumir la conjetura de Serre, si imponemos la condición adicional:

$$\mathbb{Q}(d_p) = E \qquad \text{y} \qquad \sqrt{d_p} \notin E$$

para algún primo p. Aquí E denota el cuerpo de números generado por los autovalores de la forma cuspidal de Siegel y d_p es un discriminante asociado

al polinomio característico de la imagen de Frob p.
Esta condición se cumple en los ejemplos considerados. Presumiblemente se trata de una condición que se cumple siempre.

Aplicamos el algoritmo de determinación de los primos excepcionales al ejemplo dado por $\Upsilon 20$, forma de Siegel cuspidal de peso 20 que verifica todas las condiciones anteriores y tiene autovalores racionales. Sus primeros autovalores han sido calculados por Skoruppa. Nuestro algoritmo no funciona para primos $\ell \leq 2k-2 = 38$. Además de esta cota inferior, hallamos que $\ell = 71$ es excepcional. Concluimos asumiendo la conjetura de Serre que las imágenes de las representaciones de Galois asociadas a $\Upsilon 20$ son "tan grande como es posible" para todo $\ell > 37$, $\ell \neq 71$. En particular para todo $\ell > 37$, $\ell \neq 71$, los grupos $\mathrm{PGSp}(4, \mathbb{F}_\ell)$ se realizan como grupos de Galois sobre $\mathbb{Q}$, y la correspondiente representación de Galois sólo ramifica en ℓ.
Sin asumir la conjetura de Serre, el mismo resultado vale para casi todo primo, pero no sabemos calcular explícitamente el conjunto finito excepcional.
El resultado de imagen maximal es válido incondicionalmente para todos los primos que verifiquen: $\ell > 37$, $\ell \neq 71$ y $(\frac{d_p}{\ell}) = -1$, para $p = 2, 3, 5$ o 7, donde:
$d_2 = 2^{14} \cdot 3^2 \cdot 7 \cdot 13 \cdot 19 \cdot 241$,
$d_3 = 2^6 \cdot 3^{10} \cdot 19 \cdot 47 \cdot 150628997$,
$d_5 = 2^8 \cdot 3^2 \cdot 5^6 \cdot 19 \cdot 47 \cdot 1396135808326877$,
$d_7 = 2^8 \cdot 3^6 \cdot 7^6 \cdot 29 \cdot 1097 \cdot 41713094306662453$.

En modo análogo, aplicamos nuestro algoritmo a una forma cuspidal de Siegel de peso 28 donde el cuerpo E generado por los autovalores es un cuerpo cúbico. Este ejemplo ha sido considerado recientemente por Dettweiler, Kühn y Reiter. Aplicando nuestras técnicas a este ejemplo demostramos la maximalidad de las imágenes para casi todo primo, acotamos explícitamente (asumiendo la conjetura de Serre) el conjunto de primos excepcionales y obtenemos un resultado explícito incondicional similar al obtenido en el ejemplo anterior.
En particular, si se consideran sólo los primos inertes es E, se tiene como corolario la realización de los grupos $\mathrm{PGSp}(4, \mathbb{F}_{\ell^3})$ como grupos de Galois sobre $\mathbb{Q}$, para casi todos los primos inertes en $E/\mathbb{Q}$. Los primos inertes en el intervalo $53 < \ell \leq 197$ son:

$$59, 67, 71, 101, 103, 137, 151, 157, 181, 191, 197$$

y probamos (incondicionalmente) la maximalidad de la imagen, y por lo tanto realizamos el grupo simpléctico correspondiente como grupo de Galois sobre $\mathbb{Q}$, para todos ellos excepto el 151.

Chapter 2

On the images of the Galois representations attached to newforms without inner twists

2.1 Introduction

The images of the ℓ-adic Galois representations attached to a newform $f = \sum_{n=1}^{\infty} a_n q^n$ of weight 2 on $\Gamma_0(N)$ are known to be "as large as possible" for almost every ℓ, with the sole condition that f does not have complex multiplication (CM), thanks to the work of Momose [Mo 81] and Ribet [Ri 85]. Actually, if f has inner twists, this is only true for the restriction of these representations to a certain open subgroup of $G_{\mathbb{Q}} = \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ defined in terms of the twisting characters. Even in this case, thanks to a theorem of Papier, something can be said about the image of $G_{\mathbb{Q}}$ (see [Ri 85] and the next chapter).

In this chapter we will restrict ourselves to newforms without inner twists and without CM. We will give an algorithm for an explicit determination of the finitely many primes ℓ (that seem to be) exceptional, i.e., such that the image of the corresponding representation is not "as large as possible". As a consequence, we will be able to realize many new families of projective linear groups over finite fields as Galois groups over $\mathbb{Q}$.

We concentrate on newforms f such that $\mathbb{Q}_f$, the number field generated by its coefficients a_n, is an abelian extension of $\mathbb{Q}$, to obtain a simple characterization of primes with a prescribed residue class degree. The examples are designed to realize, for high density sets of primes, the following groups: $\mathrm{PSL}(2, \mathbb{F}_{\ell^2})$, $\mathrm{PGL}(2, \mathbb{F}_{\ell^3})$ and $\mathrm{PSL}(2, \mathbb{F}_{\ell^4})$ as Galois groups over $\mathbb{Q}$.

The groups $\mathrm{PSL}(2, \mathbb{F}_{\ell^2})$ have been previously realized as Galois groups over $\mathbb{Q}$ only in [Me 88] for primes $\ell \equiv 2, 3 \pmod 5$, $\ell > 3$, and in [Ri 75], [R-V 95] for, almost all, the inert primes in six quadratic fields of large discriminant. Applying our algorithm, we will realize these groups for every prime $\ell > 3$ such that $\ell \not\equiv \pm 1 \pmod{120}$ or $(\frac{p}{\ell}) = -1$ for a prime $p \leq 19$.
The groups $\mathrm{PGL}(2, \mathbb{F}_{\ell^3})$ and $\mathrm{PSL}(2, \mathbb{F}_{\ell^4})$ have been realized as Galois groups over $\mathbb{Q}$ only in [R-V 95] for almost all the inert primes in certain cubic and quartic non-abelian fields, and so these primes cannot be expressed in terms of congruences. We will realize the groups $\mathrm{PGL}(2, \mathbb{F}_{\ell^3})$ as Galois groups over $\mathbb{Q}$, for every prime $\ell > 3$ such that $\ell \not\equiv \pm 1 \pmod 7$ or $\ell \not\equiv \pm 1 \pmod 9$, and the groups $\mathrm{PSL}(2, \mathbb{F}_{\ell^4})$ for every $\ell > 3$ such that $(\frac{5}{\ell}) = -1$ or $(\frac{17}{\ell}) = -1$.

In particular, the groups $\mathrm{PSL}(2, \mathbb{F}_{\ell^2})$ appear as Galois groups over $\mathbb{Q}$ for every prime $\ell < 5000000$, and the groups $\mathrm{PGL}(2, \mathbb{F}_{\ell^3})$ for every prime ℓ such that $3 < \ell < 500000$.

2.2 The Algorithm

Let $f \in S_2(N) = S_2(\Gamma_0(N))$ be a newform, i.e., a normalized eigenform for the whole Hecke algebra which is new of level N. We assume from now on that f does not have CM nor inner twists. Let $\mathbb{Q}_f$ be the number field generated by its Fourier coefficients a_n and $\mathcal{O}$ its ring of integers. For every prime ℓ put $\mathcal{O}_\ell = \mathcal{O} \otimes_{\mathbb{Z}} \mathbb{Z}_\ell$ and $\mathbb{Q}_{f,\ell} = \mathbb{Q}_f \otimes_{\mathbb{Q}} \mathbb{Q}_\ell$.

By Deligne's theorem, there exists a continuous Galois representation

$$\rho_\ell : \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \to \mathrm{GL}(2, \mathcal{O}_\ell) \subseteq \mathrm{GL}(2, \mathbb{Q}_{f,\ell}),$$

unramified outside ℓN, satisfying for every prime $p \not| \ell N$,

$$\mathrm{trace}(\rho_\ell(\mathrm{Frob}\ p)) = a_p, \qquad \det(\rho_\ell(\mathrm{Frob}\ p)) = p.$$

Let $G_{\mathbb{Q}} = \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ and $G_\ell = \rho_\ell(G_{\mathbb{Q}})$, closed subgroup of $\mathrm{GL}(2, \mathcal{O}_\ell)$. From the decompositions $\mathbb{Q}_{f,\ell} = \prod_{\lambda|\ell} \mathbb{Q}_{f,\lambda}$ and $\mathcal{O}_\ell = \prod_{\lambda|\ell} \mathcal{O}_\lambda$ we obtain a decomposition of ρ_ℓ as a direct sum of representations

$$\rho_\lambda : G_\mathbb{Q} \to \mathrm{GL}(2, \mathcal{O}_\lambda) \subseteq \mathrm{GL}(2, \mathbb{Q}_{f,\lambda}).$$

Let λ be a prime in $\mathbb{Q}_f$. Consider the reduction $\overline{\rho}_\lambda$ of ρ_λ, obtained by composing ρ_λ with the reduction map $\mathrm{GL}(2, \mathcal{O}_\lambda) \to \mathrm{GL}(2, \mathbb{F}_\lambda)$, where $\mathbb{F}_\lambda$ is the residue field of λ. Let $\ell = \ell(\lambda)$ be the rational prime such that $\lambda \mid \ell$ and let $\overline{G}_\lambda$ be the image of $\overline{\rho}_\lambda$.
In order to compute the images of the representations $\overline{\rho}_\lambda$, we will use the following results of Ribet [Ri 85]:

Theorem 2.1 *For all but finitely many λ we have:*

(a) *The representation $\overline{\rho}_\lambda$ is an irreducible 2-dimensional representation over $\mathbb{F}_\lambda$.*
(b) *The order of the group $\overline{G}_\lambda = \overline{\rho}_\lambda(G_\mathbb{Q})$ is divisible by ℓ.*

In the next section we will give an algorithm to compute a set of primes containing those that do not verify these two conditions.

Theorem 2.2 *Let $A_\ell = \{x \in \mathrm{GL}(2, \mathcal{O}_\ell) \mid \det(x) \in \mathbb{Z}_\ell^*\}$.*
The equality $G_\ell = A_\ell$ holds for almost every prime. In fact, this equality holds whenever all the following conditions are satisfied:

(0) *ℓ does not ramify in $\mathbb{Q}_f/\mathbb{Q}$.*
(1) *The determinant map $G_\ell \to \mathbb{Z}_\ell^*$ is surjective.*
(2) *$\ell \geq 5$.*
(3) *G_ℓ contains an element x_ℓ such that $(\mathrm{trace}(x_\ell))^2$ generates $\mathcal{O}_\ell$ as a $\mathbb{Z}_\ell$-algebra.*
(4) *For each $\lambda \mid \ell$, the group $\overline{G}_\lambda$ is an irreducible subgroup of $\mathrm{GL}(2, \mathbb{F}_\lambda)$ whose order is divisible by ℓ.*

To see that these conditions hold for almost every prime we follow [Ri 85]. Theorem 2.1 is applied, to deal with condition (4). It is proved that there exists an integer v such that v is relatively prime to N and a_v^2 generates $\mathbb{Q}_f$ over $\mathbb{Q}$, which gives condition (3). Finally, since the determinant of ρ_ℓ coincides on $G_\mathbb{Q}$ with the ℓ-adic cyclotomic character χ_ℓ, we have condition (1).

This result allows us to realize projective linear groups over finite fields as Galois groups over $\mathbb{Q}$. Let ℓ be a prime verifying the conditions of theorem 2.2, and λ a prime in $\mathcal{O}$ over ℓ. From the equality $A_\ell = G_\ell$ it follows that

$$\overline{G}_\lambda = \{x \in \mathrm{GL}(2, \mathbb{F}_\lambda) \mid \det(x) \in \mathbb{F}_\ell^*\}.$$

Let $\mathbb{P}(\overline{G}_\lambda)$ be the image of $\overline{G}_\lambda$ in $\mathrm{PGL}(2, \mathbb{F}_\lambda)$. Then we can see that $\mathbb{P}(\overline{G}_\lambda)$ is $\mathrm{PSL}(2, \mathbb{F}_\lambda)$, if $[\mathbb{F}_\lambda : \mathbb{F}_\ell]$ is even, and $\mathrm{PGL}(2, \mathbb{F}_\lambda)$, otherwise (cf. [R-V 95]).

2.2.1 The exceptional primes for theorem 2.1

Reducible representations

Let $\lambda \in \mathcal{O}$ be a prime dividing ℓ and $\ell \not| N$. Assume that $\overline{G}_\lambda = \overline{\rho}_\lambda(G_\mathbb{Q})$ is a reducible subgroup of $\mathrm{GL}(2, \mathbb{F}_\lambda)$. Then

$$\overline{\rho}_\lambda \cong \begin{pmatrix} \phi_1 & * \\ 0 & \phi_2 \end{pmatrix},$$

with $\phi_i = \epsilon_i \overline{\chi}_\ell^{m_i}$, for $i = 1, 2$, where ϵ_1, ϵ_2 are Dirichlet characters unramified outside N, with image in $\mathbb{F}_\lambda$, and $\overline{\chi}_\ell$ is the cyclotomic character mod ℓ.
By Deligne's theorem, for every prime $p \not| \ell N$ we have:

$$a_p = \mathrm{trace}(\rho_\lambda(\mathrm{Frob}\ p)) \equiv^{\mathrm{mod}\ \lambda} \phi_1(\mathrm{Frob}\ p) + \phi_2(\mathrm{Frob}\ p) = \epsilon_1(p)\ p^{m_1} + \epsilon_2(p)\ p^{m_2},$$

$$p = \det(\rho_\lambda(\mathrm{Frob}\ p)) \equiv^{\mathrm{mod}\ \lambda} \phi_1(\mathrm{Frob}\ p)\ \phi_2(\mathrm{Frob}\ p) = \epsilon_1(p)\ \epsilon_2(p)\ p^{m_1+m_2}.$$

Take $p \not| N$ a primitive root modulo ℓ such that $\epsilon_1(p) = \epsilon_2(p) = 1$, from the last formula we see that $m_1 + m_2 \equiv 1 \pmod{\ell - 1}$ and we can choose $0 \le m_1 < m_2 < \ell - 1$.
Generalizing results of Swinnerton-Dyer [Sw 73] to the case of general level, Faltings and Jordan [F-J 95] proved the following result, which we will state for general weight, i.e., when the representation comes from a newform $f \in S_k(N)$.

Theorem 2.3 *Suppose that the representation $\overline{\rho}_\lambda$ is reducible. If $\ell > k$ and $\ell \not| N$, then $\overline{\rho}_\lambda = \epsilon_1 \oplus \epsilon_2 \overline{\chi}_\ell$, with the characters ϵ_1, ϵ_2 unramified outside N.*

Carayol (cf. [Ca 89]) and Livné (cf. [Li 89]) have given bounds for the conductors of modular Galois representations. Using these results, together with those of [F-J 95], we have

Corollary 2.4 *Let f be a newform of weight 2 and level N and $\lambda \mid \ell$ a prime in $\mathcal{O}$ such that $\overline{\rho}_\lambda$ is reducible. If $\ell > 2, \ell \not| N$, then for every $p \not| \ell N$, we have*

$$a_p \equiv \epsilon(p) + p\,\epsilon^{-1}(p) \pmod{\lambda},$$

where ϵ is a character unramified outside N whose conductor c verifies $c^2 \mid N$.

In the algorithm, we will only use the following two cases of this corollary:
a) if $p \neq \ell, p \equiv 1 \pmod{c}$, then $a_p \equiv 1 + p \pmod{\lambda}$.
b) if $p \neq \ell, p \equiv -1 \pmod{c}$, then $a_p \equiv \pm(1 + p) \pmod{\lambda}$.

These congruences cannot be equalities, because $|a_p| \leq 2\sqrt{p}$. So, only finitely many λ can satisfy them.

In the case of prime level N, a better criterion for reducibility was given by Mazur in [Ma 77]. Here the condition $\ell \not| N$ can be removed and the reducible primes are the Eisenstein primes.

Definition 2.5 *Let N be a prime. Let $\mathbf{T}$ be the Hecke algebra generated by the Hecke operators T_l $(l \neq N)$ and w, acting on $J_0(N)$. The Eisenstein ideal $\Im \subseteq \mathbf{T}$ is the one generated by the elements $1 + l - T_l$ $(l \neq N)$ and $1 + w$. An Eisenstein prime is a prime ideal $\beta \subseteq \mathbf{T}$ in the support of $\Im$.*

Let $n = \mathrm{num}(\frac{N-1}{12})$. We have a one-to-one correspondence between Eisenstein primes β and prime factors p of n. Besides, for every Eisenstein prime β, $\mathbf{T}/\beta = \mathbb{F}_p$. In particular, whenever the inertia is nontrivial the prime will not be Eisenstein.

Corollary 2.6 *Let f be a newform of weight 2 and prime level N. Let $\lambda \mid \ell$, $\ell \geq 5$, be a prime in $\mathcal{O}$ such that $\overline{\rho}_\lambda$ is reducible. Then $\ell \mid N - 1$.*

Representations with image of order not divisible by ℓ

We now turn to the second condition in theorem 2.1. Let λ and ℓ be as before and suppose that the order of $\overline{G}_\lambda$ is not divisible by ℓ. As the reducible case has already been treated, we will also assume that $\overline{\rho}_\lambda$ is irreducible. We consider $\mathbb{P}(\overline{G}_\lambda)$, its image in $\mathrm{PGL}(2,\mathbb{F}_\lambda)$. The image can only be (cf. [Se 72]):

1) cyclic,

2) dihedral, or

3) isomorphic to one of the following special groups : A_4, S_4, A_5.

• In case 1) $\overline{\rho}_\lambda$ would be reducible, contradicting our assumption.

• In case 2) there exists a Cartan subgroup C_λ of $\mathrm{GL}(2,\mathbb{F}_\lambda)$ such that $\overline{G}_\lambda$ is contained in the normalizer N_λ of C_λ, but not in C_λ. Let $\varphi_\lambda : G_\mathbb{Q} \to \{\pm 1\}$ be the composition

$$G_\mathbb{Q} \to \overline{G}_\lambda \subseteq N_\lambda \to N_\lambda / C_\lambda \cong \{\pm 1\}.$$

The kernel of φ_λ is an open subgroup of $G_\mathbb{Q}$ of index 2, so its fixed field K_λ is a quadratic field unramified outside ℓN.
We now consider the restriction of $\overline{\rho}_\lambda$ to I, an inertia subgroup of $G_\mathbb{Q}$ for ℓ. Its semisimplification can be described in terms of fundamental characters as in [Se 87]. Using the fact that the weight of f is 2, it follows that the image of I in $\mathrm{PGL}(2,\mathbb{F}_\lambda)$ is cyclic of order $\ell \pm 1$ (cf. [Ri 97]). So this is a cyclic subgroup of the dihedral group $\mathbb{P}(\overline{G}_\lambda)$ with order, if $\ell > 3$, greater than 2, and therefore must be contained in its center. This implies that the quadratic field K_λ does not ramify at ℓ, if $\ell > 3$.

This is enough to make the dihedral case computable, but there is another observation that will simplify the computations if N has any prime factor q such that $q \parallel N$. In this case, the ramification subgroup of $\overline{G}_\lambda$ for the prime q is unipotent, if q divides the conductor of $\overline{\rho}_\lambda$, and trivial otherwise. This, together with the assumption that the order of $\overline{G}_\lambda$ is prime to ℓ, implies that these ramification groups are in fact trivial for all these primes.
We conclude that the field K_λ can only ramify at those prime factors r of N (if any) such that $r^2 \mid N$. Let N' be the product of these prime factors. If we call α the quadratic character corresponding to K_λ we have proved the following:

Lemma 2.7 *Suppose that $\overline{\rho}_\lambda$ falls in case (2). If $\ell > 3$, we have*

$$a_p \equiv \alpha(p)\, a_p \pmod{\lambda},$$

for every $p \not| \ell N$, where α is a quadratic character unramified outside N'. In particular, if N is squarefree, no λ verifies the hypothesis of this lemma.

• In case 3) it is known that for every $p \not| \ell N$,

$$a_p^2 \equiv 0,\ p,\ 2p \ \text{ or } \ 4p \pmod{\lambda}, \quad \text{or} \ \ a_p^4 - 3pa_p^2 + p^2 \equiv 0 \pmod{\lambda}. \tag{2.1}$$

Actually, we will need to apply (2.1) only to the prime $\ell = 5$ because in the case of weight 2 and irreducible $\overline{\rho}_\lambda$, again using the description of the semisimplification of the restriction of $\overline{\rho}_\lambda$ to an inertia subgroup for the prime ℓ in terms of fundamental characters, it follows that there is an element of order $\ell \pm 1$ in the projective image of this inertia subgroup, and therefore in $\mathbb{P}(\overline{G}_\lambda)$. This rules out case 3) if $\ell \geq 7$ (cf. [Se 72] , [Ri 97]).
It is proved in [Ri 97] that in the squarefree level case, 3) cannot hold even for 5, so in this case the following result holds:

Theorem 2.8 *Let f be a newform of weight 2 and level N squarefree. Let $\lambda \mid \ell$, $\ell \geq 5$, be a prime in $\mathcal{O}$ such that $\overline{\rho}_\lambda$ is irreducible. Then the image of $\overline{\rho}_\lambda$ has order multiple of ℓ.*

2.2.2 Description of the algorithm

At this point we can give a complete description of the algorithm to compute the exceptional primes in theorem 2.2. Suppose that we have a newform $f \in S_2(N)$ without CM or inner twists, and we consider the representation ρ_ℓ for a prime $\ell \geq 5$. The conditions of theorem 2.2 are treated as follows:

- Step (i): It is enough, in order to verify conditions 0) and 3), to find a coefficient a_p with $p \not| \ell N$ such that a_p^2 (and a fortiori a_p) generates $\mathbb{Q}_f$ over $\mathbb{Q}$ and $\ell \not| \operatorname{disc}(a_p^2)$, where $\operatorname{disc}(a_p^2)$ denotes the discriminant of the minimal polynomial of a_p^2 over $\mathbb{Q}$.

- Step (ii): Find the maximal c such that $c^2 \mid N$, and a coefficient a_p with $p \equiv 1 \pmod{c}$ such that

$$p \not| \ell N \ \text{ and } \ a_p - (1+p) \not\equiv 0 \pmod{\lambda},$$

for every $\lambda \mid \ell$. Then, if $\ell \not| N$, the reducible case is excluded. To verify the congruences, it is enough to compute the norm of $a_p - (1+p)$ and check that $\ell \not| \mathrm{Norm}(a_p - (1+p))$.

Similarly, we can take a prime $p \equiv -1 \pmod{c}$ with

$$p \not| \ell N \text{ and } a_p \not\equiv \pm(1+p) \pmod{\lambda}.$$

It suffices to verify that $\ell \not| \mathrm{Norm}(a_p \pm (1+p))$.

In the prime level case the reducible primes $\ell \geq 5$ are among those that $\ell \mid N-1$. In particular, the prime N, which cannot be dealt with using the other approach, is not reducible.

Remark. The remaining conditions do not have to be verified in the case of squarefree level. In this case, all exceptional primes $\ell \geq 5$ are detected with steps (i) and (ii).

- Step (iii): For every quadratic character α ramifying only at the primes q such that $q^2 \mid N$, find a coefficient a_p with

  $$p \not| N\ell, \quad a_p \neq 0, \quad \alpha(p) = -1 \text{ and } a_p \not\equiv -a_p \pmod{\lambda},$$

  for every $\lambda \mid \ell$. Then, the dihedral case is excluded. To verify the congruences, it suffices to check that $\ell \not| \mathrm{Norm}(a_p)$.

- Step (iv): Take a prime $p \not| 5N$ and compute the resultants of Q, the minimal polynomial of a_p , and the polynomials P_i, $i = 1, ..., 5$,

  $$x^2, \quad x^2 - p\,, \quad x^2 - 2p\,, \quad x^2 - 4p\,, \quad x^4 - 3px^2 + p^2,$$

  following (2.1). If $5 \not| \mathrm{Res}(P_i, Q)$, for $i = 1, ..., 5$, we have that none of the P_i has a_p as a root mod $\widehat{5}$, for every $\widehat{5} \mid 5$. Then, the case of special images is excluded.

We conclude the section with a brief explanation of how, for the newforms in the examples, we have determined the corresponding number fields and checked that the newforms have no CM or inner twists.

Determination of the number field $\mathbb{Q}_f$: Let f be a newform in $S_2(N)$. If f has a coefficient a_p, $p \not| N$, which is a simple root of the characteristic polynomial of the Hecke operator T_p acting on $S_2^{new}(N)$, then it follows that $\mathbb{Q}(a_p) = \mathbb{Q}_f$.

CM-Inner Twists: It is known (cf. [Ri 80]) that a newform $f \in S_2(N)$ does not have CM or inner twists if the level is squarefree. Moreover, we can see that if there exists a prime q strictly dividing the level N, i.e., $q \parallel N$, then in $S_2(N)$ there is no newform with CM. In any case, to avoid CM one has to check that for every character α ramifying only at primes dividing the level N, there exists a coefficient a_p with $\alpha(p) = -1$, $a_p \neq 0$. Finally, to avoid inner twists in the non-squarefree level case, one has to find a coefficient a_p with $\mathbb{Q}(a_p^2) = \mathbb{Q}_f$, as in step (i) of the algorithm.

2.3 Examples: $\mathbb{Q}_f$ quadratic or abelian quartic

All the examples of newforms have been computed with an algorithm implemented by W. Stein based on ideas of J. Cremona.
The algorithm described in the previous section and all other computations have been done with PARI GP.

2.3.1 Applying the algorithm

In this section we look for newforms f of weight 2 such that the field $\mathbb{Q}_f$ is quadratic or quartic abelian.
We found that exactly 10 distinct quadratic or quartic abelian fields occur as $\mathbb{Q}_f$ for some weight 2 newforms of level up to 640. We verified that these newforms have no CM nor inner twists.

We applied the algorithm to find the exceptional primes for the representations attached to each one. The results are summarized in table 1.

	[Level / $\mathbb{Q}_f$]	[Step (i) : $p,\ a_p$]
1	$23/\ x^2-5$	$2,\ x^2+x-1$
2	$29/\ x^2-2$	$2,\ x^2+2x-1$
3	$410/\ x^2-3$	$3,\ x^2-2x-2$
4	$410/\ x^2-17$	$7,\ x^2-2x-16$ // $11,\ x^2-2x-16$
5	$414/\ x^2-7$	$5,\ x^2+2x-6$ // $11,\ x^2-2x-6$
6	$496/\ x^2-33$	$5,\ x^2-3x-6$ // $13,\ x^2-2x-32$
7	$418/\ x^2-13$	$3,\ x^2+3x-1$
8	$546/\ x^2-57$	$5,\ x^2+x-14$ // $11,\ x^2-3x-12$
9	$226/\ F_{20}$	$3,\ x^4-2x^3-6x^2+12x-4$ // $5,\ x^4-4x^3-4x^2+16x-4$
10	$358/\ V_{17}$	$3,\ x^4+2x^3-7x^2-8x-1$ // $5,\ x^4+7x^3+12x^2-3x-13$

	[Step (i) : ℓ]	[Step (ii):$p,\ a_p$]	[Step (ii) : ℓ]	[Step (iii) : $p,\ a_p$]
1	5	—-	11	—-
2	empty	—-	7	—-
3	empty	3	$5, 41$	—-
4	17	3, 2	$5, 41$	—-
5	7	7, 2	23	5 and 11
6	11	$3,\ -2$	31	3 or // 5 and 13
7	13	3	$11, 19$	—-
8	19	5 // 11	$7, 13$	—-
9	5	from 3 to 17	$113, 19$	—-
10	17	3 // 5	179	—-

	[Step (iii): ℓ]	[Step (iv) : $p,\ a_p$]	[Step (iv) :5?]	[Results]
1	—-	—-	—-	$5, 11$
2	—-	—-	—-	7
3	—-	—-	—-	$5, 41$
4	—-	—-	—-	$5, 41$
5	empty	11	NO	$7, 23$
6	empty	13	NO	$11, 31$
7	—-	—-	—-	$11, 13, 19$
8	—-	—-	—-	$7, 13, 19$
9	—-	—-	—-	$5, 19, 113$
10	—-	—-	—-	$17, 179$

Table 1

Explanation of Table 1: In the table we exhibit 10 cusp forms and the result of the algorithm of the previous section applied to them. The first eight are newforms with quadratic number field, and the last two examples correspond to the abelian quartic field case. F_{20} denotes the maximal real subfield of the cyclotomic field of 20-th roots of unity, and V_{17} a totally real subfield of the cyclotomic field of 17-th roots of unity.
The minimal polynomials of the coefficients used at each step are included, but the value is not repeated if it has already appeared in a previous column. Multiple pairs p and a_p are used in order to save some primes ℓ. In every odd column, the exceptional primes found at the corresponding step are listed, and they are put together in the last column.
Here exceptional primes are those for which the algorithm was not able to prove that the image is "as large as possible". However, it may be so for some of them. For instance all primes appearing in the fifth column are primes dividing the level, except for the Eisenstein primes 11 and 7 in the first and second row and the prime 19 appearing in the ninth row. In this last case, having computed the coefficients from a_3 to a_{17}, the corresponding representation seems to be reducible.

2.3.2 Galois realizations of groups $\mathrm{PSL}(2, \mathbb{F}_{\ell^2})$

For each of the examples in Table 1, we consider primes with residue class degree 2. The condition for this is easily given in terms of congruences, or using Legendre's symbols. So, from Table 1 and the discussion following theorem 2.2, we conclude that for the following sets of primes the groups $\mathrm{PSL}(2, \mathbb{F}_{\ell^2})$ are Galois groups over $\mathbb{Q}$: $\ell \geq 5$ and

$\ell \equiv 2, 3 \pmod 5$ (already proved in [Me 88]),
$\ell \not\equiv \pm 1 \pmod 8$,
$(\frac{3}{\ell}) = -1, \quad \ell \neq 5, 41$,
$\ell \equiv \pm 3, \pm 5, \pm 6, \pm 7 \pmod{17}, \quad \ell \neq 5, 41$,
$(\frac{7}{\ell}) = -1, \quad \ell \neq 23$,
$(\frac{33}{\ell}) = -1$,
$(\frac{13}{\ell}) = -1, \quad \ell \neq 11, 19$,
$(\frac{57}{\ell}) = -1, \quad \ell \neq 13$,
$\ell \equiv 9, 11 \pmod{20}$, or
$\ell \equiv \pm 2, \pm 8 \pmod{17}, \quad \ell \neq 179$.

Observe that the primes listed as exceptional at some of the rows:

$$5, 41, 23, 11, 19, 13, 179$$

are covered by another row. After some other elementary simplifications, we obtain

Theorem 2.9 *The group* $\mathrm{PSL}(2, \mathbb{F}_{\ell^2})$ *is a Galois group over* $\mathbb{Q}$ *whenever* ℓ *is a prime greater than* 3 *satisfying one of the following conditions:*

(a) $\ell \not\equiv \pm 1 \pmod{120}$.
(b) $\ell \not\equiv \pm 1, \pm 4 \pmod{17}$.
(c) $(\frac{7}{\ell}) = -1$ *or* $(\frac{11}{\ell}) = -1$ *or* $(\frac{13}{\ell}) = -1$ *or* $(\frac{19}{\ell}) = -1$.

In [R-V 95], using the Galois representations attached to cusp forms of weight k and level $N = 1$, other projective linear groups are realized as Galois groups. In particular, for $k = 24, 28, 30, 32, 34, 38$, there is a cusp form f with a quadratic $\mathbb{Q}_f$, and it is proved that, except for a few computed exceptions, for every prime ℓ inert in some of these quadratic fields, the group $\mathrm{PSL}(2, \mathbb{F}_{\ell^2})$ is a Galois group over $\mathbb{Q}$.
We determine the primes $\ell \geq 5$ up to 5000000 not covered by the result of [R-V 95] or by theorem 2.9. We found only 6:

$$620759, \quad 878641, \quad 1782959, \quad 3747241, \quad 3871921, \quad 4490639.$$

To cover these primes, we consider three newforms of prime level:

Level	a_2
41	$x^3 + x^2 - 5x - 1$
59	$x^5 - 9x^3 + 2x^2 + 16x - 8$
79	$x^5 - 6x^3 + 8x - 1.$

In each case the coefficient a_2 generates $\mathbb{Q}_f$. The 6 primes not yet covered have the property that in some of these three $\mathbb{Q}_f$ there is a prime above them with residue class degree 2. Applying the algorithm, it is easy to see that none of them is exceptional.
On the other hand, $\mathrm{PSL}(2, \mathbb{F}_4)$ is isomorphic to the alternating group A_5 and $\mathrm{PSL}(2, \mathbb{F}_9)$ to A_6, then we have

Theorem 2.10 *For every prime* $\ell < 5000000$, *the group* $\mathrm{PSL}(2, \mathbb{F}_{\ell^2})$ *is a Galois group over* $\mathbb{Q}$.

2.3.3 Galois realizations of groups $\mathrm{PSL}(2, \mathbb{F}_{\ell^4})$

Let us consider the inert primes in the two examples of quartic abelian number field F_{20} and V_{17}, which are given by the conditions $\ell \equiv 2, 3 \pmod 5$ and $\ell \equiv \pm 3, \pm 5, \pm 6, \pm 7 \pmod{17}$, respectively. Among the exceptional primes obtained in these two examples, the only one satisfying these conditions is 113 in the first example. But $113 \equiv -6 \pmod{17}$, so that it is covered by the second example.

Theorem 2.11 *The group* $\mathrm{PSL}(2, \mathbb{F}_{\ell^4})$ *is a Galois group over* $\mathbb{Q}$ *for every prime* $\ell \geq 5$ *satisfying one of the following conditions:*

(a) $\ell \equiv 2, 3 \pmod 5$.
(b) $\ell \equiv \pm 3, \pm 5, \pm 6, \pm 7 \pmod{17}$.

2.4 Three examples designed for realizing $\mathrm{PGL}(2, \mathbb{F}_{\ell^3})$ for many ℓ

In this section we consider three examples. The first two are examples of newforms whose corresponding number fields are abelian cubic fields, namely, $\mathbb{Q}_f = F_7$ and $\mathbb{Q}_f = F_9$, where $F_n = \mathbb{Q}(\zeta_n + \zeta_n^{-1})$, with ζ_n a primitive n-root of unity. The third example is the only example in all this chapter involving relatively large numbers. It consists of a newform whose corresponding number field has degree 27, and is a cubic extension of F_{27}.
Using the algorithm, we will compute all exceptional primes in each case, and we will apply the result to the realization of groups $\mathrm{PGL}(2, \mathbb{F}_{\ell^3})$ as Galois groups over $\mathbb{Q}$. The following result [Br 95] helped us to find these examples:

Theorem 2.12 *Let* $f \in S_2(N)$ *be a newform without CM. Suppose that* $p^{r_p} \parallel N$. *Let* $s_p = \left\lceil \frac{r_p}{2} - 1 - \frac{1}{p-1} \right\rceil$ *and* ζ *a primitive* p^{s_p}*-root of unity. Then* $\mathbb{Q}_f \supseteq \mathbb{Q}(\zeta + \zeta^{-1})$, *if* $p > 2$ *(resp.* $\mathbb{Q}(\zeta^2 + \zeta^{-2})$, *if* $p = 2$*).*

We looked for newforms without CM with corresponding number field F_7 and F_9 in the spaces $S_2^{new}(343)$ and $S_2^{new}(243)$, respectively, and found them. We will not use the one at level 343, because there is also a newform $f \in S_2(97)$ with $\mathbb{Q}_f = F_7$ and it is easier to apply the algorithm to the latter, as it has prime level.

2.4.1 Applying the algorithm

First example: There is a newform $f \in S_2(97)$ with $\mathbb{Q}_f = F_7$. We will only need the following two coefficients, given by their minimal polynomials

$$a_2 : \quad x^3 + 4x^2 + 3x - 1 \quad \text{and} \quad a_{17} : \quad x^3 + 3x^2 - 4x - 13.$$

Running the algorithm, we find, using both a_2 and a_{17}, that 7 is the only exceptional prime at step (i). There is no exceptional (Eisenstein) prime at step (ii). The level being prime, we conclude that 7 is the only exceptional prime $\ell \geq 5$.

Second example: There is a newform $f \in S_2(243)$ without CM or inner twists, with $\mathbb{Q}_f = F_9$. We apply the algorithm to find the exceptional primes $\ell \geq 5$. At step (i), we use the coefficient $a_2 : \quad x^3 - 3x^2 + 3$ to see that there is no exceptional prime. At step (ii), we first observe that we have to take $c = 9$ because $N = 243 = 3^5$. Then we use the coefficients

$$a_{19} : \quad x^3 + 3x^2 - 24x + 1, \qquad a_{53} : \quad x^3 - 18x^2 + 81x - 81,$$

and a_{37}, which is Galois conjugate to a_{19}, to see that there is no exceptional prime. Finally, we again use a_2 to see that there is no exceptional prime at step (iii) and that 5 is not exceptional at step (iv). So that, in this example, there is no prime $\ell \geq 5$ exceptional.

Third example: In the space $S_2^{new}(2187)$ we did not find a newform f with $\mathbb{Q}_f = F_{27}$ but we did find one with $\mathbb{Q}_f$ of degree 27 being a cubic extension of F_{27}. This newform has no CM nor inner twists. The field $\mathbb{Q}_f$ is NOT a Galois field. It is generated by the coefficient a_2, with minimal polynomial

$$\begin{aligned} A_2(x) = \; & x^{27} + 9x^{26} - 222x^{24} - 459x^{23} + 2133x^{22} + 7362x^{21} - 9045x^{20} \\ & -55485x^{19} + 4047x^{18} + 241677x^{17} + 128898x^{16} - 643257x^{15} \\ & -609714x^{14} + 1040283x^{13} + 1377729x^{12} - 957987x^{11} \\ & -1758753x^{10} + 410742x^{9} + 1285227x^{8} - 5184x^{7} - 520830x^{6} \\ & -53136x^{5} + 106434x^{4} + 14094x^{3} - 8262x^{2} - 972x + 27. \end{aligned}$$

To apply step (i) of the algorithm we will also use the coefficient a_5, given by the polynomial

$$\begin{aligned} A_5(x) = {} & x^{27} + 18x^{26} + 81x^{25} - 399x^{24} - 4347x^{23} - 4077x^{22} + 72270x^{21} \\ & +216621x^{20} - 480411x^{19} - 2883570x^{18} - 56565x^{17} + 19123614x^{16} \\ & +20821662x^{15} - 67078422x^{14} - 137250288x^{13} + 98869950x^{12} \\ & +423746154x^{11} + 82935981x^{10} - 662094576x^{9} - 503302086x^{8} \\ & +423203940x^{7} + 625539429x^{6} + 37164501x^{5} - 254848680x^{4} \\ & -101328894x^{3} + 21227994x^{2} + 18844893x + 2847447. \end{aligned}$$

Instead of factoring the discriminants of a_2^2 and a_5^2, we compute their greatest common divisor (and check that $5 \not| \operatorname{disc}(a_2^2)$). This gives the following exceptional primes: 811 and 7655551041527. We also compute the discriminant of the field $\mathbb{Q}_f$ and we found that these two primes ramify.

Now we turn to step (ii). We have $c = 27$ because the level is $2187 = 3^7$. We use the coefficient a_{53} given by

$$\begin{aligned} & x^{27} + 90x^{26} + 3321x^{25} + 58986x^{24} + 286659x^{23} - 8402130x^{22} \\ & -173468061x^{21} - 997212708x^{20} + 8609338368x^{19} + 174882898125x^{18} \\ & +879497766396x^{17} - 3839798343339x^{16} - 72574129126800x^{15} \\ & -322522524201888x^{14} + 507275006736879x^{13} + 11881100841555393x^{12} \\ & +50880136840412436x^{11} + 32267290657623723x^{10} \\ & -583118269440460587x^{9} - 2803147835818522302x^{8} \\ & -6056528831138196135x^{7} - 5328052040331553149x^{6} \\ & +4040855350703314974x^{5} + 14364803283290718444x^{4} \\ & +11649146213084963013x^{3} + 205986024736020486x^{2} \\ & -3863232567933946101x - 1195010794014230997, \end{aligned}$$

and the coefficient a_{109} given by

$$\begin{aligned} & x^{27} - 1161x^{25} + 1143x^{24} + 552258x^{23} - 943704x^{22} - 141492546x^{21} \\ & +288666909x^{20} + 21785693796x^{19} - 42415128438x^{18} - 2149133334543x^{17} \\ & +3249157564620x^{16} + 140451320065959x^{15} - 118337820691194x^{14} \\ & -6119920386937629x^{13} + 286365050094708x^{12} + 174146647974621273x^{11} \\ & +137088225897636096x^{10} - 3067205587844711523x^{9} \\ & -4979500588408020255x^{8} + 29948677258338999450x^{7} \\ & +76790301210845625861x^{6} - 119349417294626396391x^{5} \\ & -535760443536103781838x^{4} - 167198875027467682545x^{3} \\ & +1273594079757375456489x^{2} + 1827054356350586351796x \\ & +769405689432892210627. \end{aligned}$$

We found no exceptional prime at step (ii). We finally check, using only a_2, that there are no exceptional primes at step (iii) and that 5 is not exceptional at step (iv). We conclude that the only exceptional primes are 811 and 7655551041527.

2.4.2 Galois realizations

We will now apply these three examples to the realization of groups $\mathrm{PGL}(2, \mathbb{F}_{\ell^3})$ as Galois groups over $\mathbb{Q}$. We restrict, in each of the examples, to those primes $\ell \geq 5$ unramified in $\mathbb{Q}_f$ such that there exists a place λ in $\mathbb{Q}_f$ above them having residue class degree 3 . In the first two examples, this is equivalent to saying that ℓ is inert, and this gives $\ell \not\equiv \pm 1, 0 \pmod 7$ and $\ell \not\equiv \pm 1 \pmod 9$. In the third example, these primes can be characterized in terms of the decomposition of the polynomials A_2 and A_5. The fact that $[\mathbb{Q}_f : F_{27}] = 3$ implies that all these primes ℓ verify $\ell \equiv \pm 1 \pmod 9$, i.e., they are in the complement of the set of primes covered by the second example.

We have already shown that in our examples the only exceptional primes are those that ramify in $\mathbb{Q}_f$. Thus, we have

Theorem 2.13 *The group* $\mathrm{PGL}(2, \mathbb{F}_{\ell^3})$ *is a Galois group over* $\mathbb{Q}$ *for every prime* $\ell \geq 5$ *satisfying one of the following conditions:*

(a) $\ell \not\equiv \pm 1 \pmod 7$.
(b) $\ell \not\equiv \pm 1 \pmod 9$.
(c) $\ell \nmid \mathrm{disc}(A_2)$ *and* A_2 *has a cubic factor when reduced* mod ℓ.
(d) $\ell \nmid \mathrm{disc}(A_5)$ *and* A_5 *has a cubic factor when reduced* mod ℓ.

As in the previous section, we will combine this result with the one obtained in [R-V 95] using cusp forms f for $\mathrm{SL}(2, \mathbb{Z})$ with cubic $\mathbb{Q}_f$ and weight $k =$ 36, 40, 42, 44, 46 and 50. For these cases they computed the few exceptional inert primes.
We determine the primes $\ell \geq 5$ up to 500000 such that the groups $\mathrm{PGL}(2, \mathbb{F}_{\ell^3})$ are not covered by this result of [R-V 95] nor by theorem 2.13 and we found only 12:

11087, 97649, 176597, 202987, 237691, 297793, 358273,
368803, 394631, 407287, 408437 and 496817.

To cover these primes, we introduce four newforms of squarefree level

Level	a_2
71	x^3+x^2-4x-3
87	x^3-2x^2-4x+7
91	x^3-x^2-4x+2
97	$x^4-3x^3-x^2+6x-1.$

In each case the coefficient a_2 generates $\mathbb{Q}_f$. The 12 primes not yet covered have the property that in some of these four $\mathbb{Q}_f$ there is a prime above them with residue class degree 3. Applying the algorithm, it is easy to see that none of them is exceptional. Then, we have

Theorem 2.14 *For every prime $5 \le \ell < 500000$, the group $\mathrm{PGL}(2, \mathbb{F}_{\ell^3})$ is a Galois group over $\mathbb{Q}$.*

2.5 Bibliography

[Br 95]- Brumer, A., *The rank of $J_0(N)$*, S.M.F. Astérisque **228** (1995) 41-68

[Ca 89]- Carayol, H., *Sur les représentations galoisiennes modulo ℓ attachées aux formes modulaires*, Duke Math. J. **59** (1989), no. 3, 785-801

[F-J 95]- Faltings, G. and Jordan, B., *Crystalline cohomology and $GL(2,\mathbb{Q})$*, Israel J. Math. **90** (1995), no. 1-3, 1-66

[Li 89]- Livné, R., *On the conductors of* mod ℓ *Galois representations coming from modular forms*, J. Number Theory **31** (1989), no. 2, 133-141

[Ma 77]- Mazur, B., *Modular curves and the Eisenstein ideal*, Publ. Math. IHES **47** (1977), 33-186

[Me 88]- Mestre, J.F., *Courbes hyperelliptiques à multiplications réelles*, C.R. Acad. Sci. Paris **307** (1988) 721-724

[Mo 81]- Momose, F., *On the ℓ-adic representations attached to modular forms*, J. Fac. Sci. Univ. Tokyo, Sect. IA Math. **28**:1 (1981) 89-109

[R-V 95]- Reverter, A. and Vila, N., *Some projective linear groups over finite fields as Galois groups over $\mathbb{Q}$* , Contemporary Math.**186** (1995) 51-63

[Ri 75]- Ribet, K.A., *On ℓ-adic representations attached to modular forms*, Invent. Math. **28** (1975) 245-275

[Ri 80]- ________, *Twists of modular forms and endomorphisms of Abelian Varieties*, Math. Ann. **253** (1980) 43-62

[Ri 85]- ________, *On ℓ-adic representations attached to modular forms II*, Glasgow Math. J. **27** (1985) 185-194

[Ri 97]- ________, *Images of semistable Galois representations*, Pacific J. of Math. **181**, 3 (1997)

[Se 72]- Serre, J.P., *Propriétés galoisiennes des points d'ordre fini des courbes elliptiques*, Invent. Math. **15** (1972) 259-331

[Se 87]- ________, *Sur les représentations modulaires de degré* 2 *de* $Gal(\overline{\mathbb{Q}}/\mathbb{Q})$, Duke Math. J. **54** (1987) 179-230

[St]- Stein, W., Hecke: The Modular Forms Calculator, available at: http://shimura.math.berkeley.edu/~was/Tables/hecke.html

[Sw 73]- Swinnerton-Dyer, H., *On ℓ-adic representations and congruences for coefficients of modular forms*, Lecture Notes in Math. **350** (1973) 1-55

Chapter 3

On the images of the Galois representations attached to newforms with inner twists

3.1 Introduction

In this chapter we will apply the results of Momose, Ribet and Papier ([Mo 81], [Ri 85]) to newforms with inner twists and without CM. We keep the notation of the previous chapter and we restrict ourselves again to newforms of weight 2 and trivial nebentypus. After reviewing the definition and properties of inner twists, we will recall the result of Momose and Ribet stating that the restriction to a certain open subgroup H of $G_{\mathbb{Q}}$ (defined in terms of the twisting characters) of the Galois representations ρ_ℓ attached to a newform has an image "as large as possible" for almost every prime ℓ. This theorem is the natural generalization of theorem 2.2 to the inner twist case. A result of Papier tells us how to reconstruct from this the image of the full Galois group $G_{\mathbb{Q}}$.

We will restrict ourselves to the case of newforms with a single inner twist. We will show that the algorithm described in chapter 2, section 2, plus some easy to check technical conditions, make it possible to determine the finite set of exceptional primes, i.e., those primes ℓ such that the image of $\rho_\ell|_H$ is not "as large as possible".

As a consequence, we will be able to realize new families of projective linear groups over finite fields as Galois groups over $\mathbb{Q}$.

We concentrate on newforms f such that F_f, the subfield of $\mathbb{Q}_f$ fixed by the inner twists (see the next section for a precise definition), is an abelian extension of $\mathbb{Q}$, in order to obtain a simple characterization of primes with a prescribed residue class degree. The examples are designed to realize the groups $\mathrm{PGL}(2, \mathbb{F}_{\ell^2})$ and $\mathrm{PGL}(2, \mathbb{F}_{\ell^5})$ as Galois groups over $\mathbb{Q}$ for explicitly given infinite sets of primes.
Observe that the groups $\mathrm{PGL}(2, \mathbb{F}_{\ell^2})$ could not have been obtained using newforms without inner twists because in such a case if the residual degree is 2 the maximal possible image of the projective residual representation is $\mathrm{PSL}(2, \mathbb{F}_{\ell^2})$ (see chapter 2, section 2, or [R-V 95]). Applying our algorithm, we will realize these groups for every prime $\ell > 3$ such that $\ell \not\equiv \pm 1 \pmod{48}$ or $\ell \not\equiv \pm 1 \pmod 5$.
The groups $\mathrm{PGL}(2, \mathbb{F}_{\ell^5})$ will be realized as Galois groups over $\mathbb{Q}$, for every prime $\ell > 3$ such that $\ell \not\equiv \pm 1, 0 \pmod{11}$.

3.2 Determination of the images

Let $f = \sum_{n=1}^{\infty} a_n q^n \in S_2(N) = S_2(\Gamma_0(N))$ be a newform without CM. The main result to control the image of the residual Galois representations $\overline{\rho}_\lambda$ attached to f is due to Ribet ([Ri 85]):

Theorem 3.1 *Let C be an open subgroup of $G_{\mathbb{Q}}$. Then for almost every λ we have:*

a) The representation $\overline{\rho}_\lambda|_C$ is an irreducible 2-dimensional representation of C over $\mathbb{F}_\lambda$.

b) The order of the group $\overline{C}_\lambda = \overline{\rho}_\lambda(C)$ is divisible by ℓ.

Remark: Theorem 2.1 is a particular case of this theorem.

For every automorphism γ of the field $\mathbb{Q}_f$ consider the newform:

$$\gamma f = \sum_{n=1}^{\infty} \gamma(a_n) q^n.$$

Suppose that there exists a Dirichlet character χ such that:

$$\gamma(a_p) = \chi(p) a_p$$

for almost every p. This character must be unique (because we are assuming that f does not have CM) and we will call it χ_γ. In general, for a cusp form $f \in S_2(\Gamma_0(N), \varepsilon)$ $\varepsilon\chi_\gamma^2 = \gamma(\varepsilon)$ holds. In our particular case ($\varepsilon = 1$) this implies that χ_γ is a quadratic character. When such a character exists we say that γf is an **inner twist** of f.
Let Γ be the set of those γ giving an inner twist. We recall some properties of Γ (see [Ri 77] , [Ri 80]) :

- For every $\gamma \in \Gamma$ the conductor of χ_γ is divisible only by the primes dividing N.
- Γ is an abelian elementary 2-group.
- Let $F_f = \mathbb{Q}_f^\Gamma$, the fixed field of Γ. Then F_f is the field generated by $\{a_p^2\}$, with $p \nmid N$ ranging over a density one set of primes.
- Whenever N is square-free, no $f \in S_2(N)$ has CM or inner twists, so $\Gamma = \{1\}$.

Every character χ_γ may be thought of as a character on the Galois group $G_\mathbb{Q}$, so its kernel H_γ is an open subgroup of $G_\mathbb{Q}$. Let H be the intersection of the H_γ, $\gamma \in \Gamma$, and let K be its fixed field.
Let $H_\ell = \rho_\ell(H)$ and let

$$A_\ell = \{x \in \mathrm{GL}(2, R_\ell) \quad / \ \det(x) \in \mathbb{Z}_\ell^*\}, \qquad (2.1)$$

where R is the ring of integers of F_f and $R_\ell = R \otimes_\mathbb{Z} \mathbb{Z}_\ell$.
The following theorem of Momose ([Mo 81], [Ri 85]) determines the image of the restriction to H of the modular ℓ-adic Galois representations ρ_ℓ :

Theorem 3.2 *For almost every prime ℓ we have $H_\ell = A_\ell$.*

What is known for every prime ℓ is that ρ_ℓ restricted to H gives a map:

$$\rho_\ell : H \to (D \otimes_\mathbb{Q} \mathbb{Q}_\ell)^*,$$

where D is a quaternion division algebra over F_f (this quaternion algebra is related to a central simple algebra over F_f defined by a certain 2-cocycle on Γ with values in $\mathbb{Q}_f^*$). This implies that, first of all, we should restrict ourselves to those primes ℓ such that:

$$0) \qquad D \otimes_\mathbb{Q} \mathbb{Q}_\ell \cong M(2, F_f \otimes_\mathbb{Q} \mathbb{Q}_\ell).$$

For these primes, H_ℓ is an open subgroup of A_ℓ. Condition (0) holds for almost every ℓ, the exceptions being the primes dividing the discriminant of D.
Then the theorem is proved after applying a result of [Ri 75] stating that $H_\ell = A_\ell$ if the following hold:

1) The determinant map $H_\ell \to \mathbb{Z}_\ell^*$ is surjective.

2) $\ell \geq 5$.

3) H_ℓ contains an element x_ℓ such that: $(\mathrm{trace}(x_\ell))^2$ generates R_ℓ as a $\mathbb{Z}_\ell$-algebra.

4) For each $\lambda \mid \ell$, the group $\overline{\rho}_\lambda(H)$ is an irreducible subgroup of $\mathrm{GL}(2, \mathbb{F}_\lambda)$ whose order is divisible by ℓ.

Observe that when applied to a newform without inner twists, theorem 3.2 becomes theorem 2.2. To see that these conditions hold for almost every prime, theorem 3.1 is applied to deal with condition (4) together with the following facts (cf. [Ri 85]):
• There exists an integer v such that v is relatively prime to N, a_v^2 generates F_f over $\mathbb{Q}$ and Frob $v \in H$ (condition (3)).
• The determinant of ρ_ℓ agrees on H with the ℓ-adic cyclotomic character χ_ℓ (condition (1)).

For $g \in G_\mathbb{Q}$ let $\alpha(g) \in \mathbb{Q}_f^*$ be an element such that $\gamma(\alpha(g)) = \chi_\gamma(g)\alpha(g)$ for all $\gamma \in \Gamma$. Its existence is guaranteed by Hilbert's Satz 90, and $\alpha(g)$ does not depend on ℓ. Moreover, it only depends on the image $\overline{g}$ of g in $G_\mathbb{Q}/H$. Therefore, there are only a finite number of $\alpha(g)$, and they belong to $\mathcal{O}_\ell^*$ for almost every ℓ.
The following theorem of E. Papier (cf. [Ri 85]) follows from theorem 3.2 and the equality of the representations $\gamma(\rho_\ell)$ and $\rho_\ell \otimes \chi_\gamma$:

Theorem 3.3 *For almost every prime ℓ, the image G_ℓ of ρ_ℓ is the subgroup of $\mathrm{GL}(2, \mathcal{O}_\ell)$ generated by the group A_ℓ and the finite set of matrices:*

$$\begin{pmatrix} \alpha(g) & 0 \\ 0 & 1/\alpha(g) \end{pmatrix}$$

with $g \in G_{\mathbb{Q}}/H$.

Given a prime ℓ verifying the conditions 0) to 4) needed for theorem 3.2 to hold and such that the elements $\alpha(g)$ are invertible modulo ℓ then the image of G_ℓ is as in theorem 3.3. Condition (0) ensures that $H_\ell \subseteq A_\ell$. In [Qu 98] J. Quer gives a formula for the quaternion algebra D (see also [Cr 92]) and condition (0) holds for all primes ℓ such that:

$$\ell \nmid \operatorname{disc}(D). \qquad (i)$$

We want the prime ℓ to verify:

$$\alpha(g) \in \mathcal{O}_\ell^*, \text{ for every } g \in G_{\mathbb{Q}}/H. \qquad (ii)$$

From now on we will also assume that f is a newform with a single inner twist.

So, the subgroup H has index 2 in $G_{\mathbb{Q}}$. In this case from the definition of inner twist and of the elements $\alpha(g)$ it is clear that we can take as $\alpha(g)$ for $g \notin H$ (there is just one such coset) any coefficient a_p of f such that $a_p \notin F_f$.

We look for the element in H_ℓ such that condition 3) holds. Then if v is such that $v \nmid N$, Frob $v \in H$ and a_v^2 generates F_f over $\mathbb{Q}$, ℓ must verify:

$$\ell \nmid v \text{ and } a_v^2 \text{ generates } R_\ell \text{ as a } \mathbb{Z}_\ell - \text{algebra}. \qquad (iii)$$

The condition Frob $v \in H$ is equivalent in the case of a single inner twist to $\chi_\gamma(v) = 1$, thus to $a_v \in F_f$ (if $a_v \neq 0$).
Recall that K denotes the fixed field of H. Then if we impose

$$\ell \nmid \operatorname{disc}(K) \qquad (iv)$$

the determinant of H_ℓ is exhaustive, i.e., condition 1) holds.
We still have to deal with condition 4), i.e., to give an algorithm to detect the finitely many primes such that theorem 3.1 applied to the open subgroup H fails.
It is clear that the two conditions in theorem 3.1 applied to H hold for a prime $\ell > 2$ if and only if they hold for ℓ when applied to $G_{\mathbb{Q}}$. Therefore, the determination of the exceptional primes for theorem 3.1 can be performed applying the algorithm of the previous chapter.

Theorem 3.4 *Let $\ell \geq 5$ be a prime such that for every place λ of $\mathbb{Q}_f$ lying above ℓ, $\overline{G}_\lambda$ is an irreducible subgroup of* $\mathrm{GL}(2, \mathbb{F}_\lambda)$ *whose order is a multiple of ℓ. If, furthermore, ℓ satisfies conditions (i), (ii), (iii) and (iv) above, then: G_ℓ is the subgroup of* $\mathrm{GL}(2, \mathcal{O}_\ell)$ *generated by the group A_ℓ and the finite set of matrices:*

$$\begin{pmatrix} \alpha(g) & 0 \\ 0 & 1/\alpha(g) \end{pmatrix}$$

with $g \in G_{\mathbb{Q}}/H$.

Remark: This result applies to almost every prime.

Let ℓ be a prime such that the conclusion of the previous theorem holds for ℓ. The inclusion $A_\ell \subseteq G_\ell$ implies:

$$\mathbb{P}(\overline{\rho}_\lambda(G_{\mathbb{Q}})) \supseteq \mathrm{PXL}(2, \mathbb{F}_{\lambda'}), \qquad (2.2)$$

where $\lambda' = \lambda \cap R$, and PXL = PSL if $r = [\mathbb{F}_{\lambda'} : \mathbb{F}_\ell]$ is even and PXL = PGL if r is odd.

Notation: Let us denote by $[x, y]$ the matrix

$$\begin{pmatrix} x & 0 \\ 0 & y \end{pmatrix}.$$

Now observe that as elements of $\mathrm{PGL}(2, \mathbb{F}_\lambda)$ the matrices $[\overline{\alpha(g)}, \overline{\alpha^{-1}(g)}]$ and $[\overline{\alpha^2(g)}, 1]$ can be identified, and this is useful because $\alpha^2(g) \in R_\ell$ implies $[\overline{\alpha^2(g)}, 1] \in \mathrm{PGL}(2, \mathbb{F}_{\lambda'})$. From this and formula (2.2) we see that if r is odd we already have:

$$\mathbb{P}(\overline{\rho}_\lambda(G_{\mathbb{Q}})) = \mathrm{PGL}(2, \mathbb{F}_{\lambda'}). \qquad (2.3)$$

If r is even, we have to determine whether all the matrices $[\overline{\alpha^2(g)}, 1]$ are in $\mathrm{PSL}(2, \mathbb{F}_{\lambda'})$, in which case we will have:

$$\mathbb{P}(\overline{\rho}_\lambda(G_{\mathbb{Q}})) = \mathrm{PSL}(2, \mathbb{F}_{\lambda'}), \qquad (2.4)$$

or whether any of them is not in $\mathrm{PSL}(2, \mathbb{F}_{\lambda'})$, in which case we will again have (2.3).
The determinant of these matrices being $\overline{\alpha^2(g)}$, we easily distinguish between these two cases, and we obtain:

Proposition 3.5 *Let ℓ, λ, λ' and r be as in the previous discussion. Then*

$$\mathbb{P}(\overline{\rho}_\lambda(G_\mathbb{Q})) = \begin{cases} \mathrm{PSL}(2, \mathbb{F}_{\lambda'}), & \textit{if } r \textit{ is even } \textbf{and } \overline{\alpha^2(g)} \in \mathbb{F}_{\lambda'}^2 \text{ for every } g \in G_\mathbb{Q}/H. \\ \mathrm{PGL}(2, \mathbb{F}_{\lambda'}), & \textit{if either of these conditions fails.} \end{cases}$$

3.3 Description of the algorithm

Now we give a detailed description of the algorithm to compute the exceptional primes in theorem 3.4. Suppose that we have a newform $f \in S_2(N)$ with a single inner twist and without CM, and we consider the representation ρ_ℓ for a prime $\ell \geq 5$. The first four steps of the algorithm are the same as the algorithm given in chapter 2, section 2.2 for the case of newforms without inner twists, except for a slight change at step (i). We refer to chapter 2 for an explanation of why steps (ii), (iii) and (iv) give an effective determination of the exceptional primes for theorem 2.1.
The fifth and last step takes care of the technical conditions (i), (ii) and (iv) of theorem 3.4.

- Step (i): It is enough, in order to verify condition (iii), to find a coefficient a_p with $p \not| \ell N$ such that a_p^2 generates F_f over $\mathbb{Q}$, $a_p \in F_f$ and $\ell \not| \mathrm{disc}(a_p^2)$.

- Step (ii): Find the maximal c such that $c^2 \mid N$, and a coefficient a_p with $p \equiv 1 \pmod{c}$ such that

  $$p \not| \ell N \quad \text{and} \quad a_p - (1+p) \not\equiv 0 \pmod{\lambda},$$

  for every $\lambda \mid \ell$. Then, if $\ell \not| N$, the reducible case is excluded. To verify the congruences, it is enough to compute the norm of $a_p - (1+p)$ and check that $\ell \not| \mathrm{Norm}(a_p - (1+p))$.

  Similarly, we can take a prime $p \equiv -1 \pmod{c}$ with

  $$p \not| \ell N \text{ and } a_p \not\equiv \pm(1+p) \pmod{\lambda}.$$

  It suffices to verify that $\ell \not| \mathrm{Norm}(a_p \pm (1+p))$.

- Step (iii): For every quadratic character α ramifying only at the primes q such that $q^2 \mid N$, find a coefficient a_p with

  $$p \not| N\ell, \quad a_p \neq 0, \quad \alpha(p) = -1 \text{ and } a_p \not\equiv -a_p \pmod{\lambda},$$

  for every $\lambda \mid \ell$. Then, the dihedral case is excluded. To verify the congruences, it suffices to check that $\ell \not| \mathrm{Norm}(a_p)$.

- Step (iv): Take a prime $p \not| 5N$ and compute the resultants of Q, the minimal polynomial of a_p , and the polynomials P_i, $i = 1, ..., 5$,

  $$x^2, \quad x^2 - p\,, \quad x^2 - 2p\,, \quad x^2 - 4p\,, \quad x^4 - 3px^2 + p^2.$$

  If $5 \not| \mathrm{Res}(P_i, Q)$, for $i = 1, ..., 5$, we have that none of the P_i has a_p as a root mod $\widehat{5}$, for every $\widehat{5} \mid 5$. Then, the case of special images is excluded.

- Step (v): To verify conditions (i), (ii) and (iv) it is enough to find a coefficient a_p with $p \nmid \ell N$ such that $a_p \notin F_f$,

  $$\ell \nmid \mathrm{Norm}(a_p^2) \quad \text{and} \quad \ell \nmid \mathrm{disc}(K)$$

  where K is the fixed field of H.

Explanation of step (v): The conditions at this step imply that the prime ℓ verify condition (i) because the quaternion algebra D is given by $(a_p^2\,, \mathrm{disc}(K))$ for any p such that $a_p \notin F_f$ (see [Qu 98]). They also imply that condition (ii) is verified because if $a_p \notin F_f$ we can take a_p as $\alpha(g)$ for g in the only non trivial coset of $G_{\mathbb{Q}}/H$.

3.4 The Examples

We will study examples of newforms without CM having a single inner twist. Our goal is to apply to them the algorithm of the previous section to compute the exceptional primes for theorem 3.4. In our examples F_f will be a quadratic or a real cyclotomic field, in order to obtain an expression of primes with a prescribed residue class degree in terms of congruences. The examples below have been computed with an algorithm implemented by W. Stein [St] based on ideas of J. Cremona.

- $f \in S_2^{new}(1024)$ a newform without CM with $\mathbb{Q}_f = \mathbb{Q}(\sqrt{2+\sqrt{2}})$ and $a_2 = 0$ (because $4 \mid N$, see [A-L 70]) and with the following coefficients, given by their minimal polynomials:
  $a_3 : x^4 - 8x^2 + 8$,
  $a_5 : x^2 - 4x + 2$,
  $a_{13} : x^2 - 4x + 2$,
  $a_{31} : x^4 - 64x^2 + 512$,
  $a_{97} : x^2 - 16x + 56$,
  $a_{127} : x^4 - 320x^2 + 25088$.

  When we computed the characteristic polynomial of the Hecke operator T_3 acting on $S_2^{new}(1024)$ we observed also that the polynomial defining a_3 appears in this characteristic polynomial with multiplicity 2. This means that the eigenspaces corresponding to the eigenvalue a_3 and its Galois conjugates are all 2-dimensional. This fact, a comparison of the first eigenvalues and theorem 3.64 in [Shi 71] prove the equality:

  $$f^\sigma = \chi f,$$

  with $\sigma \in \mathrm{Gal}(\mathbb{Q}_f/\mathbb{Q}(\sqrt{2}))$ an involution and $\chi_\sigma = \chi$ the mod 4 character corresponding to $\mathbb{Q}(i)$ ($-a_3 = a_3^\sigma$ is a common eigenvalue with respect to the action of T_3 of f^σ, χf and ψf, with ψ the character corresponding to $\mathbb{Q}(\sqrt{2})$). Thus, f has a (single) inner twist, $F_f = \mathbb{Q}(\sqrt{2})$ and $K = \mathbb{Q}(i)$.
  We apply the algorithm of the previous section using only the above coefficients. To be more precise, let us list the coefficients used at each step:
  Step (i): a_5 and a_{13}.
  Step (ii): a_{31}, a_{97} and a_{127}.
  Step (iii): a_3, a_5 and a_{13}.
  Step (iv): a_3.
  Step (v): a_3.

The only possibly exceptional prime greater than 3 that we find is $\ell = 17$ at step (ii).

- $f \in S_2^{new}(1331)$ a newform without CM with $\mathbb{Q}_f$ a quadratic extension of the real cyclotomic field $L_{11} = \mathbb{Q}(\zeta + \zeta^{-1})$, where ζ is a primitive 11-th root of unity.
Remark: As in the previous chapter, theorem 2.12 helped us to find these examples.
The following are the coefficients of f that we will use:
$a_2 : x^{10} - 16x^8 + 98x^6 - 285x^4 + 390x^2 - 199$,
$a_3 : x^5 + x^4 - 4x^3 - 3x^2 + 3x + 1$,
$a_7 : x^{10} - 31x^8 + 303x^6 - 1080x^4 + 1313x^2 - 199$,
$a_{17} : x^{10} - 59x^8 + 1146x^6 - 8531x^4 + 19523x^2 - 199$,
$a_{23} : x^5 + x^4 - 37x^3 - 14x^2 + 289x - 263$,
$a_{43} : x^{10} - 253x^8 + 16665x^6 - 87483x^4 + 93170x^2 - 24079$,
$a_{67} : x^5 + 12x^4 - 48x^3 - 663x^2 + 476x + 4049$.
We show as in the previous example that
$$f^\sigma = \omega f,$$
where σ is the involution in $\mathrm{Gal}(\mathbb{Q}_f/L_{11})$ and ω the quadratic character corresponding to $\mathbb{Q}(\sqrt{-11})$.
Thus, f has a (single) inner twist, $F_f = L_{11}$ and $K = \mathbb{Q}(\sqrt{-11})$.
We apply the algorithm. Let us list the coefficients used at each step:
Step (i): a_3.
Step (ii): a_{23} and a_{67}.
Step (iii): a_2, a_7, a_{17} and a_{43}.
Step (iv): a_3.
Step (v): a_2.
The possibly exceptional primes greater than 3 that we find are $\ell = 11$ at steps (i), (ii) and (v) and $\ell = 199$ at steps (iii) and (v).

- $f \in S_2^{new}(361)$ a newform without CM. We will use the following coefficients:
$a_2 : x^4 - 5x^2 + 5$,
$a_3 : x^4 - 5x^2 + 5$,
$a_7 : x^2 + 4x - 1$,
$a_{11} : x^2 + 5x + 5$,
$a_{37} : x^4 - 85x^2 + 1805$,

$a_{113} = 0$.
This newform has a single inner twist given by the quadratic character of conductor 19, $\mathbb{Q}_f = \mathbb{Q}(a_2)$, $F_f = \mathbb{Q}(\sqrt{5})$ and $K = \mathbb{Q}(\sqrt{-19})$.
We use coefficients a_7, a_{11} at step (i), a_{37}, a_{113} at step (ii), and a_2, a_3, a_{37} at steps (iii) and (v). We do not execute step (iv) because the prime 5 is already exceptional at other steps.
We find the possibly exceptional primes $\ell = 5$ at steps (i), (iii) and (v) and $\ell = 19$ at steps (ii) and (v).

- $f \in S_2^{new}(333)$ a newform without CM. We will use the following coefficients:
  $a_2 : x^4 - 6x^2 + 3$,
  $a_7 = 2$,
  $a_{13} = 2$,
  $a_{19} : x^2 - 4x - 20$,
  $a_{31} : x^2 - 4x - 20$.
  This newform has a single inner twist given by the quadratic character of conductor 3, $\mathbb{Q}_f = \mathbb{Q}(a_2)$, $F_f = \mathbb{Q}(\sqrt{6})$ and $K = \mathbb{Q}(\sqrt{-3})$.
  We use coefficients a_{19}, a_{31} at step (i), a_7, a_{13} at step (ii), a_2 at steps (iii) and (v) and a_{13} at step (iv).
  We find no exceptional primes greater than 3. Nevertheless, observe that our algorithm does not apply to $\ell = 37$ because this prime divides the level $N = 333$.

The determination of the exceptional primes in the four above examples has an immediate application to inverse Galois theory. With this aim, we restrict ourselves in each case to those primes ℓ inert in $F_f/\mathbb{Q}$.
In the first and third examples observe that we can take as $\alpha(g)$ for $g \notin H$ the coefficient a_3. This coefficient verifies $\mathrm{Norm}(a_3) = 8$ in the first example and $\mathrm{Norm}(a_3) = 5$ in the third. This implies that $\bar{a}_3^2 \notin \mathbb{F}_{\ell^2}^2$, for every ℓ inert in $F_f = \mathbb{Q}(\sqrt{2})$, $F_f = \mathbb{Q}(\sqrt{5})$, respectively. Recall that the only possibly exceptional primes greater than 3 that we have found are $\ell = 17$ in the first example and $\ell = 5, 19$ in the third. None of them is inert in the corresponding quadratic field. An application of proposition 3.5 gives:

Theorem 3.6 *The newform $f \in S_2(1024)$ of the first example has a single inner twist, $F_f = \mathbb{Q}(\sqrt{2})$ and for every*

$$\ell \equiv 3, 5 \pmod 8, \quad \ell > 3$$

and $\lambda \in \mathcal{O}$, $\lambda \mid \ell$, we have:

$$\mathbb{P}(\overline{\rho}_\lambda(G_\mathbb{Q})) = \mathrm{PGL}(2, \mathbb{F}_{\ell^2}).$$

The newform $f \in S_2(361)$ of the third example has a single inner twist, $F_f = \mathbb{Q}(\sqrt{5})$ and for every

$$\ell \equiv 2, 3 \pmod 5, \quad \ell > 3$$

and $\lambda \in \mathcal{O}$, $\lambda \mid \ell$, we have:

$$\mathbb{P}(\overline{\rho}_\lambda(G_\mathbb{Q})) = \mathrm{PGL}(2, \mathbb{F}_{\ell^2}).$$

Corollary 3.7 *For every $\ell \equiv 3, 5 \pmod 8$ or $\ell \equiv 2, 3 \pmod 5$, $\ell > 3$, $\mathrm{PGL}(2, \mathbb{F}_{\ell^2})$ is a Galois group over $\mathbb{Q}$.*

To apply proposition 3.5 to the second example observe that $F_f = L_{11}$ is a degree 5 extension of $\mathbb{Q}$, so inert primes have odd residue class degree. The possibly exceptional primes greater than 3 found for this example are $\ell = 11, 199$. None of them is inert in L_{11}, so we have

Theorem 3.8 *The newform $f \in S_2(1331)$ of the second example has a single inner twist, $F_f = L_{11}$ and for every*

$$\ell \not\equiv \pm 1 \pmod{11}, \quad \ell \neq 2, 3, 11$$

and $\lambda \in \mathcal{O}$, $\lambda \mid \ell$, we have:

$$\mathbb{P}(\overline{\rho}_\lambda(G_\mathbb{Q})) = \mathrm{PGL}(2, \mathbb{F}_{\ell^5}).$$

Corollary 3.9 *For every $\ell \not\equiv \pm 1 \pmod{11}$, $\ell \neq 2, 3, 11$, $\mathrm{PGL}(2, \mathbb{F}_{\ell^5})$ is a Galois group over $\mathbb{Q}$.*

In the fourth example, we have $F_f = \mathbb{Q}(\sqrt{6})$. The inert primes in F_f are the primes ℓ such that $(\frac{6}{\ell}) = -1$. For such a prime ℓ, there are two possibilities, either $(\frac{2}{\ell}) = -1$ or $(\frac{2}{\ell}) = 1$. In the first case, the group $\mathrm{PGL}(2, \mathbb{F}_{\ell^2})$ is a Galois group over $\mathbb{Q}$ as follows from corollary 3.7. In the second case we have $(\frac{3}{\ell}) = -1$. In this example we can take as $\alpha(g)$ for $g \notin H$ the coefficient a_2. This coefficient verifies $\mathrm{Norm}(a_2) = 3$, and this implies that $\bar{a}_2^2 \notin \mathbb{F}_{\ell^2}^2$, for every ℓ such that $(\frac{3}{\ell}) = -1$. An application of proposition 3.5 to these primes together with corollary 3.7 gives

Theorem 3.10 *For every* $\ell \not\equiv \pm 1 \pmod{24}$, $\ell > 3$, $\mathrm{PGL}(2, \mathbb{F}_{\ell^2})$ *is a Galois group over* $\mathbb{Q}$.

Remark: The prime $\ell = 37$ verifies $\ell \equiv 5 \pmod 8$, so it is covered by corollary 3.7.

To conclude, let us mention that there is a newform $f \in S_2(4096)$ whose first coefficients have minimal polynomials ($a_2 = 0$):

$$a_3 : x^8 - 16x^6 + 72x^4 - 96x^2 + 8, \quad a_5 : x^4 - 8x^2 + 8x - 2.$$

This newform has an inner twist, given by the mod 4 character χ, so $F_f = \mathbb{Q}(a_5) = \mathbb{Q}\left(\sqrt{2+\sqrt{2}}\right)$. Consider the primes ℓ with residue class degree 2 in $F_f/\mathbb{Q}$, i.e., $\ell \equiv 7, 9 \pmod{16}$. It can be shown that the 2 places of F_f lying above ℓ are inert in $\mathbb{Q}_f/F_f$. We apply the algorithm to this example and we found no exceptional primes of this type. It follows that for every $\ell \equiv 7, 9 \pmod{16}$, and $\lambda \in \mathcal{O}$, $\lambda \mid \ell$,

$$\mathbb{P}(\overline{\rho}_\lambda(G_{\mathbb{Q}})) = \mathrm{PGL}(2, \mathbb{F}_{\ell^2}).$$

This, together with theorem 3.10, proves that $\mathrm{PGL}(2, \mathbb{F}_{\ell^2})$ is a Galois group over $\mathbb{Q}$, for every $\ell \not\equiv \pm 1 \pmod{48}$, $\ell > 3$.

3.5 Bibliography

[A-L 70]- Atkin, A. and Lehner, J., *Hecke operators on* $\Gamma_0(m)$, Math. Ann. **185** (1970) 134-160

[Br 95]- Brumer, A., *The rank of* $J_0(N)$, S.M.F. Astérisque **228** (1995) 41-68

[Cr 92]- Cremona, J., *Abelian varieties with extra twist, cusp forms, and elliptic curves over imaginary quadratic fields*, J. London Math. Soc. (2) **45** (1992), no. 3, 404-416

[Mo 81]- Momose, F., *On the* ℓ*-adic representations attached to modular forms*, J. Fac. Sci. Univ. Tokyo, Sect. IA Math. **28**:1 (1981) 89-109

[Qu 98]- Quer, J., *La classe de Brauer de l'algèbre d'endomorphismes d'une variété abélienne modulaire*, C. R. Acad. Sci. Paris Sér I Math. **327** (1998) no.3, 227-230

[R-V 95]- Reverter, A. and Vila, N., *Some projective linear groups over finite fields as Galois groups over* $\mathbb{Q}$, Contemporary Math.**186** (1995) 51-63

[Ri 75]- Ribet, K.A., *On* ℓ*-adic representations attached to modular forms*, Invent. Math. **28** (1975) 245-275

[Ri 77]- ________, *Galois representations attached to eigenforms with nebentypus*, LNM 601 (1977), Springer-Verlag

[Ri 80]- ________, *Twists of modular forms and endomorphisms of Abelian Varieties*, Math. Ann. **253** (1980) 43-62

[Ri 85]- ________, *On* ℓ*-adic representations attached to modular forms II*, Glasgow Math. J. **27** (1985) 185-194

[Shi 71]- Shimura, G., *Introduction to the Arithmetic Theory of Automorphic Functions*, Publ. Math. Soc. Japan, Princeton (1971) 199-208

[St]- Stein, W., Hecke: The Modular Forms Calculator, available at: http://shimura.math.berkeley.edu/~was/Tables/hecke.html

Chapter 4

On the images of modular and geometric three-dimensional Galois representations

4.1 Introduction

In this and the next section, we give an account of the theory of modular forms for congruence subgroups of $SL(3, \mathbb{Z})$, Clozel's conjecture predicting a family of Galois representations attached to Hecke eigenforms, and van Geemen and Top's construction of three-dimensional compatible families of geometric Galois representations that experimentally support this conjecture. This provides the motivation and background for the following sections, where we determine the images of these geometric representations and apply this to the realization of three-dimensional special linear and unitary groups over finite fields as Galois groups over $\mathbb{Q}$. See section 3 for more details.
In section 12, assuming Clozel's conjecture in a stronger form, we obtain examples of Galois representations over different fields, and an application of the techniques described in previous sections shows that for eigenforms satisfying some easy to check standard conditions the images of these Galois representations give special linear or unitary groups for all but finitely many primes.
References for the first two sections: [A-G-G 84] , [A-M 92], [vG-T 96], [vG-T 94] and [vG-K-T-V 97].

4.1.1 Modular Forms for congruence subgroups of $\mathrm{SL}(3,\mathbb{Z})$

For classical modular forms, the space $S_2(\Gamma_0(N))$ can be thought of as a subspace of $H^1(\Gamma_0(N),\mathbb{C})$. This inspires an analogous definition of modular forms and Hecke operators in the three dimensional case, i.e., for congruence subgroups of $\mathrm{SL}(3,\mathbb{Z})$. For $N \geq 1$ an integer, let $\Gamma_0(N) \subseteq \mathrm{SL}(3,\mathbb{Z})$ be the subgroup whose elements $M = (m_{ij})$ satisfy:

$$m_{21} \equiv m_{31} \equiv 0 \pmod{N}.$$

Definition 4.1 *A modular form of level N is an element of $H^3(\Gamma_0(N),\mathbb{C})$.*

Definition 4.2 *For every $\alpha \in \mathrm{GL}(3,\mathbb{Q})$, let $\Gamma_\alpha := \Gamma \cap \alpha^{-1}\Gamma\alpha$, where $\Gamma := \Gamma_0(N)$. Γ_α has finite index both in Γ and in $\alpha^{-1}\Gamma\alpha$. We have two natural maps from Γ_α to Γ:*

$$\varphi : \gamma \to \gamma,$$
$$\psi : \gamma \to \alpha\gamma\alpha^{-1}.$$

Consider the restriction $\varphi^* : H^3(\Gamma,\mathbb{C}) \to H^3(\Gamma_\alpha,\mathbb{C})$ and the transfer induced by ψ: $\psi_* : H^3(\Gamma_\alpha,\mathbb{C}) \to H^3(\Gamma,\mathbb{C})$.
We call Hecke operator the $\mathbb{C}$-linear operator:

$$T_\alpha : H^3(\Gamma_0(N),\mathbb{C}) \to H^3(\Gamma_0(N),\mathbb{C})$$

given by the composition $\psi_* \circ \varphi^*$.

Proposition 4.3 *Let $\mathcal{T}(N)$ be the subalgebra of $\mathrm{End}(H^3(\Gamma_0(N),\mathbb{C}))$ generated by the Hecke operators T_α with $\alpha \in \mathrm{GL}(3,\mathbb{Z})^+, (\det(\alpha), N) = 1$. Then $\mathcal{T}(N)$ is commutative and it is generated by the operators T_{α_p} and T_{β_p} with $p \nmid N$ and:*

$$\alpha_p := \begin{pmatrix} p & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}; \quad \beta_p := \begin{pmatrix} p & 0 & 0 \\ 0 & p & 0 \\ 0 & 0 & 1 \end{pmatrix}.$$

$H^3(\Gamma_0(N),\mathbb{C})$ can be decomposed as direct sum of common eigenspaces for the operators in $\mathcal{T}(N)$:

$$H^3(\Gamma_0(N),\mathbb{C}) = \bigoplus_\lambda V_\lambda,$$

with λ homomorphism of algebras $\mathcal{T}(N) \to \mathbb{C}$ and $Tf = \lambda(T)f$, for $T \in \mathcal{T}(N), f \in V_\lambda$.

Given a character λ of $\mathcal{T}(N)$, we define the eigenvalue a_p of the Hecke eigenform $f \in V_\lambda$:

$$a_p := \lambda(T_{\alpha_p}).$$

Then it is known that: $\lambda(T_{\beta_p}) = \bar{a_p}$.
The field generated by the eigenvalues a_p of a Hecke eigenform f is a number field, either totally real or a CM-field. We will denote this field $\mathbb{Q}_f$. The eigenvalues a_p are algebraic integers.

Conjecture 4.4 *(Clozel) Let $f \in H^3(\Gamma_0(N), \mathbb{C})$ be a cuspidal eigenform for the action of the Hecke algebra $\mathcal{T}(N)$ with eigenvalues: $T_{\alpha_p} f = a_p f$ for every $p \nmid N$ (and therefore $T_{\beta_p} f = \bar{a_p} f$) generating the number field $\mathbb{Q}_f$.*
Then, if we take for every rational prime ℓ a prime λ in $\mathbb{Q}_f$ dividing ℓ, there exists a compatible family of λ-adic Galois representations

$$\rho_\lambda : G_\mathbb{Q} \to \mathrm{GL}(3, \mathbb{Q}_{f,\lambda})$$

such that for every λ, ρ_λ is unramified outside ℓN and for every $p \nmid \ell N$ the characteristic polynomial of $\rho_\lambda(\mathrm{Frob}\ p)$ is:

$$x^3 - a_p x^2 + p\bar{a_p} x - p^3.$$

See [Cl 90], [vG-T 94] and [vG-K-T-V 97]. For the definition of cuspidality see [A-G-G 84].
Remark: In [A-M 92], a similar conjecture for mod p modular forms is stated.

We will only consider the case of $\mathbb{Q}_f$ a CM-field. In the other case the family ρ_λ becomes selfdual, and there is a finite index subgroup of the image of these representations contained in $G \cong \mathrm{PGL}(2, \mathbb{Q}_{f,\lambda})$.
Most of the known examples of eigenforms $f \in H^3(\Gamma_0(N), \mathbb{C})$ have imaginary quadratic $\mathbb{Q}_f$, such as $\mathbb{Q}_f = \mathbb{Q}(i)$ for $f \in H^3(\Gamma_0(128), \mathbb{C})$.

4.2 Experimental verification of Clozel's conjecture

A compatible family of three-dimensional λ-adic Galois representations was constructed by van Geemen and Top (see [vG-T 94]) to give experimental

evidence for the previous conjecture for three eigenforms of different levels, all with $\mathbb{Q}_f = \mathbb{Q}(i)$. These representations are geometric, and we summarize their construction:
Let X be an algebraic variety defined over $\mathbb{Q}$, and consider the Galois ℓ-adic representations on étale cohomology:

$$\rho_\ell : G_{\mathbb{Q}} \to \mathrm{GL}(H^n_{et}(X_{\overline{\mathbb{Q}}}, \mathbb{Q}_\ell)).$$

If X is smooth, projective, and with good reduction at p, it is known that the representations ρ_ℓ ($\ell \neq p$), are unramified at p and the characteristic polynomial of $\rho_\ell(\text{Frob } p)$ has coefficients in $\mathbb{Z}$, is independent of ℓ and its roots have absolute value $p^{n/2}$.
Clozel's conjecture predicts the determinant of the representations attached to modular forms to be p^3, so we must take $n = 2$. This also implies $|a_p| \leq 3p$. The examples are constructed using a subspace of $H^2_{et}(S_{\overline{\mathbb{Q}}}, \mathbb{Q}_\ell)$, where S is a surface. The Galois representation decomposes:

$$H^2_{et}(S_{\overline{\mathbb{Q}}}, \mathbb{Q}_\ell) = T_\ell \oplus \mathrm{NS}(S_{\overline{\mathbb{Q}}}) \otimes_{\mathbb{Z}} \mathbb{Q}_\ell,$$

where $\mathrm{NS}(S_{\overline{\mathbb{Q}}})$ is the Nèron-Severi group and T_ℓ its orthogonal complement with respect to the cup product: $H^2_{et} \times H^2_{et} \to H^4_{et} \cong \mathbb{Q}_\ell$.
Eigenvalues of Frobenius on $\mathrm{NS}(S_{\overline{\mathbb{Q}}})$ are roots of unity multiplied by p, so we will look for our family of λ-adic representations inside $T_\ell \otimes_{\mathbb{Q}_\ell} K_\ell$ with $K = \mathbb{Q}(i)$.
If it were dim $T_\ell = 3$ we would have selfdual representations given by three dimensional $\mathbb{Q}_\ell$-vector spaces. We look for three dimensional λ-adic representations $\rho_{f,\lambda}$ associated as in the conjecture to a modular form f with $\mathbb{Q}_f = \mathbb{Q}(i)$. Therefore, we want trace$(\rho_{f,\lambda}(\text{Frob } p)) \in \mathbb{Z}[i]$ and not all these traces in $\mathbb{Z}$. Thus we suppose that the surface has an automorphism defined over $\mathbb{Q}$:

$$\phi : S \to S \quad \text{with} \quad \phi^4 = id_S.$$

The induced map: $\phi^* : H^2_{et} \to H^2_{et}$ commutes with the Galois representations. Suppose that dim $T_\ell = 6$ and $\phi^* : T_\ell \to T_\ell$ has two three dimensional eigenspaces $W_\lambda, W_{\lambda'}$, with eigenvalues $i, -i$ respectively, such that:

$$T_\lambda := T_\ell \otimes_{\mathbb{Q}_\ell} \mathbb{Q}_\ell(i) = W_\lambda \oplus W_{\lambda'}.$$

This decomposition gives us a compatible family of λ-adic three dimensional Galois representations σ'_λ on W_λ, a $\mathbb{Q}(i)_\lambda$ vector space. In general

σ'_λ has to be twisted by a Dirichlet character ϵ to obtain $\epsilon \otimes \sigma'_\lambda = \sigma_\lambda$ with $\det(\sigma_\lambda(\text{Frob } p)) = p^3$.
These are the representations we will consider:

$$\sigma_{S,\lambda} : G_{\mathbb{Q}} \to \mathrm{GL}(W_\lambda).$$

The Example: The family of surfaces constructed by van Geemen and Top is the following: S_a is the smooth, minimal projective model of the singular affine surface defined by:

$$t^2 = xy(x^2-1)(y^2-1)(x^2-y^2+axy).$$

The automorphism ϕ is given by $(x,y,t) \to (y,-x,t)$.
Let $N = N(a)$ be the product of the primes of bad reduction of S_a.
The characteristic polynomials of $\sigma_{S_a,\lambda}(\text{Frob } p)$ will be denoted

$$x^3 - a_p x^2 + p\bar{a}_p x - p^3.$$

In particular, we put $a_p := \mathrm{trace}(\sigma_{S_a,\lambda}(\text{Frob } p)) \in \mathbb{Q}(i)$ for every $p \nmid \ell N$. These traces are determined using Lefschetz trace formula and counting points of S_a over finite fields. Of course these surfaces verify $\dim T_\ell = 6$.
We will illustrate our study of three-dimensional geometric Galois representations with the examples given by the surfaces S_a. This is just to simplify the exposition; the results obtained can be applied to any similar example (see section 11).

In [vG-K-T-V 97] the following result is proved:

Theorem 4.5 *Clozel's conjecture for three examples of modular forms in $H^3(\Gamma_0(N), \mathbb{C})$ with $N = 128, 160, 205$ is experimentally supported by the representations $\sigma_{S_a,\lambda}$ described above, with $a = 2, 1, 1/16$, respectively. More precisely, the eigenvalues of these eigenforms agree with the traces of the images of Frobenius for the corresponding representation, for all $p \nmid 2N, \quad p \leq 173$.*

Remarks: For example, in the case $a = 2$, we have to twist by

$$\epsilon : G_{\mathbb{Q}} \to \mathrm{Gal}(\mathbb{Q}(\sqrt{-2})/\mathbb{Q}) \cong \pm 1,$$

to obtain $\det(\sigma_{S_2,\lambda}) = \chi^3$, χ the ℓ-adic cyclotomic character.
Observe that the properties possessed by a geometric representation that we

will use later are preserved by this twist (description of the restriction to the inertia subgroup at ℓ and absolute value of roots of characteristic polynomials), so no additional difficulties are introduced.

The primes of bad reduction of S_a, which are the only primes other than ℓ where $\sigma_{S_a,\lambda}$ may ramify, are the primes dividing $2a(a^2+4)$. This gives only the prime 2 in the case $a = 2$. It is not known whether the conductor of the representations $\sigma_{S_a,\lambda}$ is bounded independently of ℓ. If this is the case, we call this minimal uniform bound "conductor of the family of representations". The existence of this conductor is conjectured.

4.3 Statement of Purpose

We will consider the compatible family of Galois representations $\sigma_{S_2,\lambda}$ constructed in the previous section from the surface S_2.
We will prove that the image is a special linear group (up to a twist by the cyclotomic character) for the primes decomposing in $\mathbb{Q}(i)$, i.e., $\ell \equiv 1 \pmod 4$, except at most for a set of Dirichlet density 0, and the image of the residual Galois representation is a unitary group for the inert primes $\ell \equiv 3 \pmod 4$, except at most for a set of Dirichlet density 0. Moreover, in the case of inert primes we will give an explicit description of this exceptional density 0 set.
The exceptional density 0 sets, both for decomposing and inert primes, could be replaced by finite sets if we merely knew the existence and value of the conductor of the family $\sigma_{S_2,\lambda}$.
The method works in general for geometric three-dimensional representations over a quadratic imaginary field such as those associated to the surfaces S_a, whenever certain general conditions that we will describe later are satisfied by the traces of Frobenius (see section 6 and 8) and the action of the inertia subgroup at ℓ (see section 5).
The family of representations $\sigma_{S_a,\lambda}$ comes from the action of $G_{\mathbb{Q}}$ on W_λ, the 3-dimensional i-eigenspace (for $\phi^* : T_\ell \to T_\ell$) contained in $T_\ell \subseteq H^2_{et}(S_{a\overline{\mathbb{Q}}}, \mathbb{Q}_\ell)$. T_ℓ also admits a realization $T_{\mathbb{Z}} \subseteq H^2(S_a(\mathbb{C}), \mathbb{Z})$ which is a Hodge structure of weight 2, i.e.: $T_{\mathbb{Z}}$ is a $\mathbb{Z}$-module, free of rank 6 with

$$T_{\mathbb{Z}} \otimes \mathbb{C} = \bigoplus_{p+q=2} T^{p,q} \qquad \overline{T}^{p,q} = T^{q,p},$$

with $\dim T^{p,q} = 2$ and ϕ^* has eigenvalues $i, -i$ on each $T^{p,q}$. In particular $W_\lambda \otimes \mathbb{C}$ intersects non-trivially each $T^{p,q}$ (cf. [vG-T 94] and [vG-T 96]).

4.4 Classification of subgroups of $\mathrm{PSL}(3,\mathbb{F}_q)$

What follows is the classification, due to Mitchell ([Mi 11]), of the maximal subgroups $\mathcal{G}$, up to conjugation, of $\mathrm{PSL}(3,\mathbb{F}_{p^t})$, for $t = 1$ or 2, as groups of collineations of the projective plane over $\mathbb{F}_{p^t}$. See [V-Y 65] for the relevant definitions from plane projective geometry. We include the order of the subgroup $\mathcal{G}$ in each case.

a) the stabilizer of a point: $|\mathcal{G}| = (p^t+1)p^{3t}(p^t-1)^2/\gcd(3,p^t-1)$
b) the stabilizer of a line: $|\mathcal{G}| = (p^t+1)p^{3t}(p^t-1)^2/\gcd(3,p^t-1)$
c) groups that leave invariant a triangle with coordinates in $\mathbb{F}_{p^t}$ and make all six permutations of its vertices: $|\mathcal{G}| = 6(p^t-1)^2/\gcd(3,p^t-1)$
d) groups that leave invariant a triangle with coordinates in $\mathbb{F}_{p^{3t}} \setminus \mathbb{F}_{p^t}$ and permute its vertices cyclically: $|\mathcal{G}| = 3(p^{2t}+p^t+1)/\gcd(3,p^t-1)$
e) the stabilizer of a conic: $|\mathcal{G}| = (p^t+1)p^t(p^t-1)$
f) $\mathrm{PSL}(3,\mathbb{F}_{p^k})$ with $k \le t$:
$|\mathcal{G}| = (p^{2k}+p^k+1)(p^k+1)p^{3k}(p^k-1)^2/\gcd(3,p^k-1)$
g) (only if $t = 2$) group of special unitary transformations $\mathrm{PSU}(3,\mathbb{F}_p)$: $|\mathcal{G}| = (p^2-p+1)(p+1)^2p^3(p-1)/\gcd(3,p+1)$
h) Hessian groups of orders 216 (if $p^t \equiv 1 \pmod 9$), 72 or 36 (if $p^t \equiv 4,7 \pmod 9$)
i) group isomorphic to $\mathrm{PSL}(2,7)$: $|\mathcal{G}| = 168$ (if $t = 2$ or if $t = 1,\ p \equiv 0,1,2,4 \pmod 7$)
j) group isomorphic to A_6 : $|\mathcal{G}| = 360$ (if $t = 2$ or if $t = 1,\ p \equiv 1,4 \pmod{15}$).

We have excluded the case $p = 5$ and $t = 2$. In this case there are more possibilities.

Remarks: In cases a) and b) the subgroup is reducible. Cases c) and d) correspond to the normalizer of the group of diagonal matrices and that of the group of units of the extension $[\mathbb{F}_{p^{3t}} : \mathbb{F}_{p^t}]$ embedded in $\mathrm{SL}(3,\mathbb{F}_{p^t})$ using the regular representation respectively. In particular, inside such a group we have groups that are reducible over $\mathbb{F}_{p^t}$ (over $\mathbb{F}_{p^{3t}}$), namely, a group of

diagonal matrices and a cyclic group of units embedded by the regular representation respectively.
In case h), the group $\mathcal{G}$ fits in the exact sequence

$$1 \to \mathcal{F} \to \mathcal{G} \to \mathcal{U} \to 1,$$

with $\mathcal{U}$ isomorphic to a subgroup of $\mathrm{SL}(2,3)$ or the quaternionic group $\mathcal{D}_8$ and $\mathcal{F}$ of type $(3,3)$ (cf. [Bl 67]).
We will call cases h), i) and j) "exceptional cases".

4.5 Comparison of Étale and Crystalline cohomologies and the action of inertia

As a consequence of the result of Fontaine-Messing in [F-M 87] giving (canonical, functorial) isomorphism between the étale cohomology and the crystalline cohomology for a variety S having good reduction at ℓ and with $\dim(S) < \ell$, the following theorem, conjectured by Serre in [Se 72], holds:

Theorem 4.6 *Let V be a $G_{\mathbb{Q}}$-stable lattice in $H^m_{et}(S_{\overline{\mathbb{Q}}}, \mathbb{Q}_\ell)$ and $\tilde{V}$ the semi-simplification of $V/\ell V$ with respect to the action of $I = I_\ell$. Then, if $\dim(S) < \ell$ and S have good reduction at ℓ, the action of I is given by a character $\Psi : I_t \to \mathbb{F}_q^*$ with $q = \ell^n, n = \dim\ V$, such that*

$$\Psi = \Psi_f^{d_0 + \ell d_1 + \ldots + \ell^{n-1} d_{n-1}}$$

with Ψ_f fundamental character of level n and the exponents verify: $0 \leq d_i \leq m$.

We apply this result to the representations $\sigma_{S_a,\lambda}$. For any λ-adic representation σ_λ, we denote by $\bar{\sigma}_\lambda$ the corresponding residual representation obtained by composing σ_λ with the reduction modulo λ.
Since $\det(\sigma_{S_a,\lambda}) = \chi^3$ and $m = 2$, we have the following possibilities for $\bar{\sigma}_{S_a,\lambda}|_I$, where $\ell > 2$ is a prime of good reduction for S_a :

$$\begin{pmatrix} 1 & * & * \\ 0 & \chi & * \\ 0 & 0 & \chi^2 \end{pmatrix}; \quad \begin{pmatrix} 1 & * & * \\ 0 & \psi_2^{2+\ell} & 0 \\ 0 & 0 & \psi_2^{1+2\ell} \end{pmatrix}; \quad \begin{pmatrix} \chi & * & * \\ 0 & \psi_2^{2} & 0 \\ 0 & 0 & \psi_2^{2\ell} \end{pmatrix};$$

$$\begin{pmatrix} \chi^2 & * & * \\ 0 & \psi_2 & 0 \\ 0 & 0 & \psi_2^\ell \end{pmatrix}; \quad \begin{pmatrix} \psi_3^{1+2\ell} & 0 & 0 \\ 0 & \psi_3^{\ell+2\ell^2} & 0 \\ 0 & 0 & \psi_3^{\ell^2+2} \end{pmatrix}; \quad \begin{pmatrix} \chi & * & * \\ 0 & \chi & * \\ 0 & 0 & \chi \end{pmatrix}$$

with ψ_i a fundamental character of level i.
We want to compare this description with the classification of the previous section. To do so, we first need to exclude the last case, the case with trivial $\mathbb{P}((\bar{\sigma}_\lambda|_I)^{ss})$.
In the examples $\bar{\sigma}_{S_a,\lambda}$ this can be done because of the Hodge structure of $T_{\mathbb{Z}}$. Using again the fact that our representations are crystalline ([F-M 87]), we are free to apply the results of Fontaine-Laffaille (cf. [F-L 82], theorem 5.3), so the knowledge of the Hodge filtration allows us to compute the possible values of the exponents of the fundamental characters describing the action of I_ℓ as in theorem 4.6. In particular the exponent 1 cannot appear three times because dimension $T^{p,q} = 2$ for $(p,q) = (0,2), (1,1)$ and $(2,0)$.
In the other cases we have $\mathbb{P}(\bar{\sigma}_{S_a,\lambda}|_I)$ of the form:

$$\begin{pmatrix} \chi^{-1} & * & * \\ 0 & 1 & * \\ 0 & 0 & \chi \end{pmatrix}; \quad \begin{pmatrix} \chi^{-1} & * & * \\ 0 & \psi_2 & 0 \\ 0 & 0 & \psi_2^\ell \end{pmatrix}; \quad \begin{pmatrix} 1 & * & * \\ 0 & \psi_2^{1-\ell} & 0 \\ 0 & 0 & \psi_2^{\ell-1} \end{pmatrix};$$

$$\begin{pmatrix} \psi_3^{\ell-\ell^2} & 0 & 0 \\ 0 & \psi_3^{\ell^2-1} & 0 \\ 0 & 0 & \psi_3^{1-\ell} \end{pmatrix}.$$

4.6 Determination of the images: totally decomposing primes

4.6.1 Reducible representations

Recall that N denotes the product of the primes of bad reduction of S_a. Suppose that $\ell \equiv 1 \pmod 4$ is a prime such that $\bar{\sigma}_{S_a,\lambda}$ is not irreducible over $\mathbb{F}_{\ell^3}$. In this case there is a character μ unramified outside $N\ell$ with image in $\mathbb{F}_{\ell^3}^*$ such that $\mu(p)$ is a root of $x^3 - a_p x^2 + p\bar{a}_p x - p^3$, for every $p \nmid \ell N$.
Using the description of $\bar{\sigma}_{S_a,\lambda}|_I$ we know that $\mu = \chi^i \varepsilon$, with χ the mod ℓ cyclotomic character, $i = 0, 1, 2$ and ε a character unramified outside N.

The problem is that we cannot bound the value of cond(ε), the conductor of ε, independently of ℓ. We have to exclude a set of primes of small density in order to bound it.

For the family of Galois representations $\bar{\sigma}_{S_2,\lambda}$ of the example, we have $N = 2$ and $\varepsilon : (\mathbb{Z}/2^u\mathbb{Z})^* \to \mathbb{F}_{\ell^3}^*$, with $\ell \equiv 1 \pmod 4$.
We exclude the set $\mathcal{P}$ of primes $\ell \equiv 1 \pmod{64}$ in order to bound the conductor of ε.
What follows only holds for $\ell \equiv 1 \pmod 4$, $\ell \notin \mathcal{P}$.
With this restriction $64 \nmid \ell^3 - 1$ holds, so the image of ε is a cyclic group of order at most 32. Then the conductor of ε is at most 128, because

$$(\mathbb{Z}/128\mathbb{Z})^* \cong \mathbb{Z}/2\mathbb{Z} \times (\mathbb{Z}/32\mathbb{Z}).$$

Thus, $\varepsilon(p) = 1$, for every $p \equiv 1 \pmod{128}$. Moreover, $\varepsilon(p) = 1$ for every $p \equiv -1 \pmod{128}$, except if ε is a character of conductor 4 or 8, in which case $\varepsilon(3) = \pm 1$.
We will use only a_3 and a_{127} because either $\varepsilon(127) = 1$ or $\varepsilon(3) = \pm 1$. We are assuming that $\mu(p) = p^i \varepsilon(p)$, $i = 0, 1$ or 2, is a root of the characteristic polynomials of $\bar{\sigma}_{S_2,\lambda}(\text{Frob } p)$, for every $p \nmid 2\ell$. Taking in particular $p = 127$ or $p = 3$, we know that either $\varepsilon(127) = 1$, thus giving the equation:

$$127^{3i} - a_{127}127^{2i} + 127\bar{a}_{127}127^i - 127^3 \equiv 0 \pmod{\ell},$$

$i = 0, 1$ or 2, with $a_{127} = 161 - 16i$; or $\varepsilon(3) = \pm 1$, giving a similar equation for $p = 3$, $a_3 = 1 + 2i$, except for some $\pm$ signs (the values of the traces a_p that we use are listed in [vG-K-T-V 97]).
From these equations we check that $\bar{\sigma}_{S_2,\lambda}$ may reduce over $\mathbb{F}_{\ell^3}$ only for the primes $\ell = 5, 13, 1901, 105649$. Looking at the characteristic polynomials of $\bar{\sigma}_{S_2,\lambda}(\text{Frob } p)$ for these ℓ and several primes p, we see that the representation $\bar{\sigma}_{S_2,5}$ seems to be reducible (over $\mathbb{F}_5$). For the other three primes it is irreducible (over $\mathbb{F}_{\ell^3}$).

Moreover, for $\ell = 13$ these computations and the classification (section 4) show that the image of $\mathbb{P}(\bar{\sigma}_{S_2,13})$ is $\text{PSL}(3, \mathbb{F}_{13})$. The determination of the image for a single prime using the classification appears in [A-M 92] and [A-A-C 98].
We have proved the following:

Theorem 4.7 *For every* $\ell \equiv 1 \pmod 4$, $\ell \not\equiv 1 \pmod{64}$, $\ell \neq 5$, *the Galois representation* $\bar{\sigma}_{S_2,\lambda}$ *is irreducible over* $\mathbb{F}_{\ell^3}$. *The same holds for* $\mathbb{P}(\bar{\sigma}_{S_2,\lambda})$ *and* $\overline{\chi^{-1} \otimes \sigma_{S_2,\lambda}}$.

This excludes cases a) and b) of the classification, the case of a diagonal group contained in a maximal subgroup in case c), and the case of a cyclic group contained in a maximal subgroup in case d).

The fact that, after excluding a set of primes $\mathcal{P}$, we obtain just a finite number of reducible primes, is general. The only condition that a compatible family of geometric Galois representations (such as those we obtain from the surfaces S_a, $a \in \mathbb{Q}$) has to verify for this to hold is the following:

Condition 1 If c is (a uniform bound for) the conductor of the family $\sigma_{S_a,\lambda}$, then there exists a prime $p \equiv 1 \pmod c$ such that $a_p \notin \mathbb{R}$.

If we do not know c (or even that it exists) we exclude a set of primes $\mathcal{P}$ such that for every prime ℓ decomposing totally in $K := \mathbb{Q}(\{a_p\}) = \mathbb{Q}(i)$ and $\ell \notin \mathcal{P}$ the conductor of ε (a character ramifying only at the primes of bad reduction of S_a with values in $\mathbb{F}^*_{\ell^3}$) is uniformly bounded by d. This is exactly what we have done in the example given by the surface S_2 to obtain the "artificial bound" 128 for the conductor. Then we require:

Condition 1' There exists a prime $p \equiv 1 \pmod d$ with $a_p \notin \mathbb{R}$.

Under condition 1 or 1', we prove that there is a finite number of reducible primes, outside $\mathcal{P}$ and decomposing totally in K, as follows:
Take $p \equiv 1 \pmod d$ (or $p \equiv 1 \pmod c$) with $a_p \notin \mathbb{R}$.
Then $\varepsilon(p) = 1$ and putting $\mu = \varepsilon\chi^i$, $i = 0, 1, 2$ we obtain:

$$p^3 - 1 \equiv p\bar{a}_p - a_p \pmod \ell \qquad (i = 0),$$

$$p^3 - 1 \equiv pa_p - \bar{a}_p \pmod \ell \qquad (i = 2),$$

$$a_p - \bar{a}_p \equiv 0 \pmod \ell \qquad (i = 1).$$

For the finiteness of the set of solutions of the third, use condition 1 or 1'.
For the other two congruences, use $|a_p| \leq 3p$.

4.6.2 Cases c) and d) of the classification

We will now study the non-cyclic case of d) and case c) of the classification (see section 4).

d) Let $G_\lambda := \mathrm{Image}(\bar{\sigma}_{S_a,\lambda})$. If its projective image $\mathbb{P}(G_\lambda)$ is an irreducible group contained in a maximal subgroup in case d), then $\mathbb{P}(G_\lambda)$ is contained in the normalizer of a cyclic group, and it fits in the exact sequence

$$1 \to \mathcal{C} \to \mathbb{P}(G_\lambda) \to C_3 \to 1,$$

where $\mathcal{C}$ is cyclic of order $|\mathcal{C}| \mid p^2 + p + 1$.

c) If $\mathbb{P}(G_\lambda)$ is an irreducible subgroup contained in a maximal group in case c), then $\mathbb{P}(G_\lambda)$ is contained in the normalizer of a diagonal group, and it fits in the exact sequence

$$1 \to \mathcal{R} \to \mathbb{P}(G_\lambda) \to \mathcal{U} \to 1,$$

where $\mathcal{U}$ is isomorphic to a subgroup of S_3 and $\mathcal{R}$ is diagonal of order $|\mathcal{R}| \mid (p-1)^2$.

• Case d): Using the description of the image of the inertia subgroup at ℓ (see section 5), we know that its projective image will be contained in $\mathcal{C}$, because it is cyclic with order greater or equal to $\ell - 1 > 3$, whenever $\ell \geq 5$. Then composing $\mathbb{P}(\bar{\sigma}_{S_a,\lambda})$ with the quotient $\mathbb{P}(G_\lambda) \to C_3$ we obtain a representation

$$G_{\mathbb{Q}} \twoheadrightarrow C_3$$

unramified outside N, because when we take quotient by $\mathcal{C}$ we are trivializing the image of the inertia group at ℓ.
So its kernel gives a cubic character ψ unramified outside N, and if $p \nmid \ell N$:

$$\psi(p) \neq 1 \Rightarrow \mathbb{P}(\bar{\sigma}_{S_a,\lambda})(\mathrm{Frob}\ p) \text{ has trace } 0 \Leftrightarrow a_p \equiv 0 \pmod{\ell}. \qquad (6.1)$$

Here we are using the fact that a matrix obtained by a non trivial cyclic permutation of the columns of a diagonal matrix has trace 0. To control this case we need the following

Definition 4.8 *let N' be the product of primes of bad reduction of S_a except that we put 9 in this product if 3 is a prime of bad reduction. Then we say that the family of representations $\sigma_{S_a,\lambda}$ has cubic Complex Multiplication (or cubic CM) if there exists a character:*

$$\psi : (\mathbb{Z}/N'\mathbb{Z})^* \to C_3$$

such that for every $p \nmid N'$ with $\psi(p) \neq 1$, $a_p = 0$, i.e,

$$a_p = \psi(p) a_p \quad \textit{for every} \quad p \nmid N'.$$

Then, it is clear that only finitely many primes ℓ can fall in case d) if we avoid cubic CM.
In the example $\sigma_{S_2,\lambda}$, $N = 2$ and $3 \nmid (\mathbb{Z}/2^k\mathbb{Z})^*$, so that case d) cannot happen for any ℓ.

• Case c): Again we have $\mathbb{P}(\bar{\sigma}_{S_a,\lambda}|_I)$ contained in the center $\mathcal{R}$, because $\ell - 1 > 3$ for $\ell \geq 5$ and S_3 does not contain cyclic subgroups of order greater than 3. Assuming irreducibility of the representation, we must have $\mathcal{U} = S_3$ or C_3. If $\mathcal{U} = C_3$, the same analysis as in case d) applies.
If $\mathcal{U} = S_3$, consider the quotient $S_3 \twoheadrightarrow C_2$. Composing the epimorphisms

$$G_{\mathbb{Q}} \twoheadrightarrow \mathbb{P}(G_\lambda) \twoheadrightarrow S_3 \twoheadrightarrow C_2$$

we obtain a quadratic character γ unramified outside N. We have that for every $p \nmid \ell N$, $\gamma(p) = -1$ implies that $\mathbb{P}(\bar{\sigma}_{S_a,\lambda})(\text{Frob } p)$ becomes diagonal after an odd permutation of its columns.
These matrices have the following property: If their characteristic polynomial is $x^3 + Ax^2 + Bx + C$, then $AB = C$.
But the characteristic polynomial of $\bar{\sigma}_{S_a,\lambda}(\text{Frob } p)$ is, for every $p \nmid N\ell$:

$$x^3 - a_p x^2 + p\bar{a}_p x - p^3 \qquad \pmod{\ell}.$$

Then $\gamma(p) = -1 \Rightarrow -p a_p \bar{a}_p \equiv -p^3 \pmod{\ell}$ must hold, and therefore:

$$a_p \bar{a}_p \equiv p^2 \pmod{\ell}. \qquad (6.2)$$

Definition 4.9 *We say that the family of representations $\sigma_{S_a,\lambda}$ is dual with respect to a quadratic character γ (ramifying only at the primes of bad reduction of S_a) if, for every prime p,*

$$\gamma(p) = -1 \Rightarrow a_p \bar{a}_p = p^2.$$

Again, it is clear that, assuming that $\sigma_{S_a,\lambda}$ is not dual with respect to any quadratic character, it follows that only finitely many primes ℓ can fall in case c).

Remark: The consideration of the quotient C_2 of S_3 is just to simplify computations. Note that the condition obtained is sufficient to guarantee that only finitely many primes fall in case c), but not necessary. The alternative option is to work with S_3, and we obtain a situation analogous to that encountered in case d). The difference is that now we have to work with the closure L of a non-cyclic cubic extension of $\mathbb{Q}$, instead of with a cyclic cubic field. L only ramifies at primes of bad reduction of S_a (only finitely many possible L thanks to Hermite's theorem). For every $p \nmid \ell N$ we should look at the element in $\mathrm{Gal}(L/\mathbb{Q})$ corresponding to Frob p : if it is a non trivial cyclic permutation then formula (6.1) applies, and (6.2) if is is an odd permutation. Therefore, for case c) to hold for infinitely many primes the representations should be dual respect to a quadratic character and the coefficients a_p should be 0 for "one third" of the primes.

In the example $\sigma_{S_2,\lambda}$, γ would ramify only at 2. Then $\gamma(3) = -1$ or $\gamma(5) = -1$. Using only $a_3 = 1 + 2i$ and $a_5 = -1 - 4i$ we conclude that the representation is not dual respect to γ. Moreover:
$a_3\bar{a}_3 = 5 \equiv 3^2 \pmod{\ell} \Rightarrow \ell = 2$,
$a_5\bar{a}_5 = 17 \equiv 5^2 \pmod{\ell} \Rightarrow \ell = 2$.
So that no prime $\ell \equiv 1 \pmod 4$, $\ell > 5$, falls in case c) .

4.6.3 Case e) : The stabilizer of a conic

Choosing an adequate basis we can write the equation of a general conic as:

$$y^2 = kxz.$$

Then, it is easy to see that the stabilizer of this conic is the group of matrices of the form (cf. [V-Y 65]):

$$\begin{pmatrix} k\alpha^2 & 2\alpha\beta & \beta^2 \\ k\sqrt{k}\alpha\beta & \sqrt{k}(\alpha\delta+\beta\gamma) & \sqrt{k}\beta\delta \\ k\gamma^2 & 2\gamma\delta & \delta^2 \end{pmatrix}.$$

One can check by direct computation that the characteristic polynomial is for such matrices:

$$x^3 - Ax^2 + Bx - C,$$

with $B^3 = CA^3$.
Therefore, if we suppose that the image of $\bar{\sigma}_{S_a,\lambda}$ falls in case e) we must have: $p^3\bar{a}_p^3 \equiv p^3 a_p^3 \pmod{\lambda}$ for every $p \nmid \ell N$, or equivalently:

$$a_p^3 \equiv \bar{a}_p^3 \pmod{\lambda}.$$

The values a_p are all in a quadratic imaginary field K. Then, for a prime p such that $a_p \notin \mathbb{R}$, $a_p^3 \neq \bar{a}_p^3$; provided that $K \neq \mathbb{Q}(\sqrt{-3})$.
Thus, for the representations $\bar{\sigma}_{S_a,\lambda}$ case e) can only happen for finitely many primes.
More generally, this will be the case whenever the representations are non-selfdual in the more general sense that there does not exist any character ν such that $a_p = \nu(p)\bar{a}_p$ for every $p \nmid \ell N$.
In the example, using only a_3 we obtain: $(1+2i)^3 \equiv (1-2i)^3 \pmod{\lambda}$, and this implies $\ell = 2$. We conclude that no prime $\ell \equiv 1 \pmod{4}$ falls in case e) in our example.

4.6.4 The exceptional cases

In these cases $\mathbb{P}(G_\lambda) \subseteq \mathrm{PSL}(3, \mathbb{F}_\ell)$ is a group contained in another group of order $36, 72, 168, 216$ or 360. The description of $\mathbb{P}(\bar{\sigma}_{S_a,\lambda}|_I)$ given in section 5 tells us that in the image of $\mathbb{P}(\bar{\sigma}_{S_a,\lambda})$ there is a cyclic subgroup of order $\ell-1$, $\ell+1$ or $\ell^2+\ell+1$. This gives only a few possibilities for the exceptional primes. Using the structure of the exceptional groups in cases h), i) and j) and the restriction to $\ell \equiv 1 \pmod{4}$ we end up with $\ell = 5$ or 13.
As we already mentioned, we know that $\mathbb{P}(\bar{\sigma}_{S_2,13})$ has image $\mathrm{PSL}(3, \mathbb{F}_{13})$. Then, 5 is the only prime $\ell \equiv 1 \pmod{4}$ not in $\mathcal{P}$ such that the image of $\mathbb{P}(\bar{\sigma}_{S_2,\lambda})$ for $\lambda \mid \ell$ can be a proper subgroup of $\mathrm{PSL}(3, \mathbb{F}_\ell)$.

4.6.5 Conclusion

We have considered all cases in the classification of subgroups of $\mathrm{PSL}(3, \mathbb{F}_\ell)$ given in section 4. Therefore, we conclude:

Theorem 4.10 *The family of representations $\sigma_{S_2,\lambda}$ verifies:*

$$\mathrm{Image}(\mathbb{P}(\bar{\sigma}_{S_2,\lambda})) = \mathrm{PSL}(3, \mathbb{F}_\ell),$$

for every prime $\ell \equiv 1 \pmod 4$, $\quad \ell \not\equiv 1 \pmod{64}$, $\quad \ell > 5$.

Remark: The groups $\mathrm{PSL}(3, \mathbb{F}_\ell)$, for all primes $\ell \equiv 1 \pmod 4$, have been previously realized as Galois groups over $\mathbb{Q}(t)$ using rigidity methods in [Th 84].

Observe that the image of $\overline{\chi^{-1} \otimes \sigma_{S_2,\lambda}}$ is contained in $\mathrm{SL}(3, \mathbb{F}_\ell)$ and

$$\mathbb{P}(\overline{\chi^{-1} \otimes \sigma_{S_2,\lambda}}) = \mathbb{P}(\bar{\sigma}_{S_2,\lambda}).$$

Then we conclude that:

Corollary 4.11

$$\mathrm{Image}(\overline{\chi^{-1} \otimes \sigma_{S_2,\lambda}}) = \mathrm{SL}(3, \mathbb{F}_\ell),$$

for every $\ell \equiv 1 \pmod 4$, $\quad \ell \not\equiv 1 \pmod{64}$, $\quad \ell > 5$. *In particular, for these values of ℓ the groups $\mathrm{SL}(3, \mathbb{F}_\ell)$ are Galois groups over $\mathbb{Q}$. For each ℓ, the corresponding number field is unramified outside 2ℓ.*

Remark: Using a lemma of Serre (see [Se 68]), we also conclude that for these ℓ the image of $\chi^{-1} \otimes \sigma_{S_2,\lambda}$ is $\mathrm{SL}(3, \mathbb{Z}_\ell)$.

4.7 On the density of the exceptional set - Condition 1' revisited

We have proved that the image of $\bar{\sigma}_{S_2,\lambda}$ is "as large as possible" for infinitely many totally decomposed primes. Now we will show that this, together with the Cebotarev density theorem, forces the image of the rest of the totally decomposed primes to be also "as large as possible", except at most for a set of Dirichlet density 0.

Lemma 4.12 *If a compatible family of three-dimensional geometric Galois representations σ_λ verifies*

$$\mathrm{Image}(\bar{\sigma}_\lambda) = \mathrm{PSL}(3, \mathbb{F}_\ell)$$

for an infinite set $\mathbb{L}$ of totally decomposed primes, then condition 1' is satisfied for any d.

Before proving this lemma, let us show its consequences. We denote by $\mathcal{D}$ the set of totally decomposed primes in $\mathbb{Q}(\{a_p\})$. Suppose that for a compatible family of geometric Galois representations we have checked all conditions, as in the previous section, to ensure an image "as large as possible" for those primes in $\mathcal{D}$ that are not in a finite exceptional set $\mathcal{S}$ nor in a certain excluded set $\mathcal{P}$ as in condition 1', and assume that the Dirichlet density of $\mathcal{P}$ is smaller than that of $\mathcal{D}$. Then we apply lemma 4.12 and conclude that condition 1' is still valid for an arbitrarily large d and the corresponding set $\mathcal{P}'$ of arbitrarily small Dirichlet density to be excluded. Therefore, the image must be "as large as possible" for every prime in $\mathcal{D}$ except for the elements of $\mathcal{P}'$ and a finite set $\mathcal{S}'$. Note that $\mathcal{S}'$ may be larger than $\mathcal{S}$, but it is still finite (condition 1' implies that there are only finitely many primes with reducible image in $\mathcal{D} \setminus \mathcal{P}'$). Letting the conductor d go to infinity we conclude that the exceptional set has Dirichlet density 0.
Applying this to the representations $\sigma_{S_2,\lambda}$ we obtain:

Theorem 4.13

$$\mathrm{Image}(\overline{\chi^{-1} \otimes \sigma_{S_2,\lambda}}) = \mathrm{SL}(3, \mathbb{F}_\ell)$$

for every $\ell \equiv 1 \pmod 4$, *except at most for a set of Dirichlet density* 0.

Proof of lemma 4.12: The proof is based on the fact that, whenever a_p is real, the characteristic polynomial of $\sigma_\lambda(\mathrm{Frob}\ p)$ decomposes over $\mathbb{Q}$:

$$x^3 - a_p x^2 + p a_p x - p^3 = (x - p)(x^2 + (p - a_p)x + p^2).$$

Suppose that this happens for every $p \equiv 1 \pmod d$ for some d. Now consider the residual representation $\overline{\chi^{-1} \otimes \sigma_\lambda}$ for a prime $\ell \in \mathbb{L}$. For such a prime the image is $\mathrm{SL}(3, \mathbb{F}_\ell)$. Let $\mathcal{U}_\ell$ be the image of the subgroup of $\mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q})$ topologically generated by the Frobenius elements at primes $p \equiv 1 \pmod d$; it is a subgroup of $\mathrm{SL}(3, \mathbb{F}_\ell)$ and it follows from the Cebotarev density theorem that it is made of (not only generated by) matrices whose characteristic polynomials are reducible over $\mathbb{F}_\ell$. Therefore, it is clear that

$$|\mathcal{U}_\ell| / |\mathrm{SL}(3, \mathbb{F}_\ell)| \leq 1/(\ell^2 + \ell + 1).$$

On the other hand, by the Cebotarev density theorem and the fact that the Dirichlet density of the set of $p \equiv 1 \pmod d$ is $1/\varphi(d)$ (where φ is the Euler function), we must have:

$$|\mathcal{U}_\ell| / |\mathrm{SL}(3, \mathbb{F}_\ell)| \geq 1/\varphi(d).$$

Therefore $\ell^2+\ell+1 \leq \varphi(d)$. But ℓ can be taken to be arbitrarily large, because $\mathbb{L}$ is infinite, so we obtain a contradiction, and this proves the lemma.

4.8 Determination of the images: inert primes

4.8.1 Imitation of section 6

With slight changes, the same ideas used for totally decomposed primes can also be applied to deal with the same cases of the classification for inert primes. In our example these are the primes $\ell \equiv 3 \pmod 4$ and for them the image of the representation $\bar{\sigma}_{S_2,\lambda}$ is a subgroup of $\mathrm{PSL}(3, \mathbb{F}_{\ell^2})$. We briefly describe this procedure:

• Reducible representations: We have a character $\mu = \chi^i \varepsilon$ with $\mu(p)$ a root of the characteristic polynomial of $\bar{\sigma}_{S_2,\lambda}(\mathrm{Frob}\ p)$, $i = 0, 1, 2$ and ε unramified outside 2, as in section 6.1. The difference is that the image of ε is now contained in $\mathbb{F}^*_{\ell^6}$. To bound the conductor we subtract from the set of inert primes the set $\mathcal{P}$ of primes $\ell \equiv -1 \pmod{32}$. We obtain $64 \nmid \ell^6 - 1$, and the same bound for the conductor as in section 6.1. So with the computations of that section, using $\varepsilon(127) = 1$ or $\varepsilon(3) = \pm 1$, and the characteristic polynomials corresponding to these two primes, we prove that the image is irreducible (over $\mathbb{F}_{\ell^6}$) for every $\ell \equiv 3 \pmod 4$, $\ell \not\equiv -1 \pmod{32}$, except of course for $\ell = 3$ and 127. To save the prime 127 we compute the reduction mod 127 of a few characteristic polynomials and this shows that the image of the corresponding representation is irreducible over $\mathbb{F}_{127^2}$ and is not cyclic. We ignore the prime 3 because our method fails for it in cases c) and d), and by direct inspection we cannot determine whether it falls in the exceptional cases or not; so we will assume henceforth that we are dealing only with primes greater than 3.
We have proved that for every $\ell \equiv 3 \pmod 4$, $\ell \not\equiv -1 \pmod{32}$, $\ell > 3$, cases a) , b) and the reducible subcases of c) and d) in the classification are not possible for the image of the corresponding residual Galois representation.

• Cases c), d) and e): All we have done in sections 6.2 and 6.3 applies as well to the inert primes greater than 3 (this inequality being essential in the argument used in cases c) and d)). We conclude that, under the hypothesis of irreducibility, no inert prime greater than 3 falls in these cases (recall that in the computations we have only used a_3 and a_5).

• Exceptional cases: As in section 6.4, we have a cyclic subgroup of the image with order $\ell - 1$, $\ell + 1$ or $\ell^2 + \ell + 1$. Using the structure of the exceptional groups, we see that they have a cyclic subgroup of one of these orders only for $\ell = 7, 11$ and 19, among all primes $\ell \equiv 3 \pmod 4$, $\ell > 3$. Computing the reduction of some characteristic polynomials modulo these three primes, we see that there are elements in the image of the corresponding representation whose orders do not divide the order of those exceptional groups we were suspecting the image could be equal to. We conclude that no inert prime greater than 3 falls in the exceptional cases.

Now we consider the remaining cases in the classification (see section 4):
Case f) with $k = 1$: If, for an inert prime ℓ, the image were contained in $\mathrm{PSL}(3, \mathbb{F}_\ell)$, there should exist for every prime $p \nmid 2\ell$ an element $c(p) \in \bar{\mathbb{F}}_\ell^*$ such that $c(p)^3 p^3 \in \mathbb{F}_\ell^*$ and $c(p) a_p \in \mathbb{F}_\ell$. Therefore, $a_p^3 \in \mathbb{F}_\ell$. This implies that the prime ℓ falls in case e), the stabilizer of a conic.

In his article [Mi 11], Mitchell also classifies the subgroups of $\mathrm{PSU}(3, \mathbb{F}_\ell)$. All of them are subgroups of those appearing in section 4, so we can conclude from the computations above that no proper subgroup of $\mathrm{PSU}(3, \mathbb{F}_\ell)$ will be obtained as the image of $\sigma_{S_2,\lambda}$ for any inert prime ℓ not in the excluded set.

Applying the classification in section 4, for $t = 2$, we obtain:

Theorem 4.14 *The family of representations $\sigma_{S_2,\lambda}$ verifies:*

$$\mathrm{Image}(\mathbb{P}(\bar{\sigma}_\lambda)) = \mathrm{PSU}(3, \mathbb{F}_\ell) \textit{ or } \mathrm{PSL}(3, \mathbb{F}_{\ell^2})$$

for every prime $\ell \equiv 3 \pmod 4$, $\ell \not\equiv -1 \pmod{32}$, $\ell > 3$.

Applying lemma 4.12, and letting the bound of the conductor of the character in the reducible case tend to infinity, we conclude, as in section 7, that the density of the set of inert primes with reducible image (over $\mathbb{F}_{\ell^6}$) is 0. For those with irreducible image, the previous theorem applies:

Corollary 4.15 *The conclusion of theorem 4.14 is valid for every $\ell \equiv 3 \pmod 4$, except at most for a set of Dirichlet density 0.*

4.8.2 Unitariness

In this section we will prove that for those inert primes such that theorem 4.14 or corollary 4.15 applies, the image is in fact unitary. Our reasoning will be by reductio ad absurdum.

Lemma 4.16 *For the family of representation $\sigma_{S_a,\lambda}$, the image of $\mathbb{P}(\bar{\sigma}_{S_a,\lambda})$ can not be $\mathrm{PSL}(3,\mathbb{F}_{\ell^2})$ for any prime $\ell \equiv 3 \pmod 4$.*

This lemma, together with theorem 4.14 and corollary 4.15 gives:

Theorem 4.17 *The family of representations $\sigma_{S_2,\lambda}$ verifies:*

$$\mathrm{Image}(\mathbb{P}(\bar{\sigma}_{S_2,\lambda})) = \mathrm{PSU}(3,\mathbb{F}_\ell)$$

for every prime $\ell \equiv 3 \pmod 4$, except at most for a set of Dirichlet density 0, in particular the result is valid for every prime $\ell \equiv 3 \pmod 4$, $\ell \not\equiv -1 \pmod{32}$, $\ell > 3$.

Proof of lemma 4.16:
Suppose that there is a prime $\ell \equiv 3 \pmod 4$ such that the image of $\mathbb{P}(\bar{\sigma}_{S_a,\lambda})$ is $\mathrm{PSL}(3,\mathbb{F}_{\ell^2})$. In particular, there will be elements in this image of order $\ell^4+\ell^2+1$ (projective classes of generators of the cyclic group of units of $\mathbb{F}_{\ell^6}$ embedded in SL_3 via the regular representation). By the Cebotarev density theorem there will be infinitely many primes p such that $\mathbb{P}(\bar{\sigma}_{S_a,\lambda})(\mathrm{Frob}\ p)$ is an element of this order. In this case, the characteristic polynomial of $\bar{\sigma}_{S_a,\lambda}(\mathrm{Frob}\ p)$ will be irreducible modulo ℓ and its roots will be elements of $\mathbb{F}_{\ell^6}$ of order multiple of $\ell^4+\ell^2+1$. Therefore the polynomial:

$$x^3 - a_p x^2 + p\bar{a}_p x - p^3 \qquad (8.1)$$

is irreducible in characteristics 0 and ℓ, with $a_p \in \mathbb{Q}(i) \setminus \mathbb{Q}$ and its reduction in $\mathbb{F}_{\ell^2} \setminus \mathbb{F}_\ell$.
Let $\alpha = a + bi$ be one of its roots, with $a, b \in \mathbb{R}$. It is an algebraic integer with $[\mathbb{Q}(\alpha):\mathbb{Q}] = 6$ and ℓ is inert in $\mathbb{Q}(\alpha)/\mathbb{Q}$. Let $\mathcal{L}$ be the prime in $\mathbb{Q}(\alpha)$ dividing ℓ and let us denote by $\hat{}$ reduction mod $\mathcal{L}$. Then $[\mathbb{F}_\ell(\hat{\alpha}):\mathbb{F}_\ell] = 6$.
We know (by the Riemann hypothesis) that $|\alpha| = p$, i.e., $a^2+b^2=p^2$. Using this, $\mathbb{Q}(i) \subseteq \mathbb{Q}(\alpha)$ and $a, b \in \mathbb{R}$ we see that:

$$\mathbb{Q}(a,b) \subsetneq \mathbb{Q}(a,b,i) = \mathbb{Q}(a+bi, a-bi) = \mathbb{Q}(\alpha),$$

with $[\mathbb{Q}(\alpha) : \mathbb{Q}(a, b)] = 2$. Thus, $[\mathbb{Q}(a, b) : \mathbb{Q}] = 3$. From this it follows that $[\mathbb{Q}(a) : \mathbb{Q}] \leq 3$ and $[\mathbb{Q}(b) : \mathbb{Q}] \leq 3$ and one of these must be an equality. Using $a^2 + b^2 = p^2 \in \mathbb{Q}$, it easily follows that $[\mathbb{Q}(a) : \mathbb{Q}] = [\mathbb{Q}(b) : \mathbb{Q}] = 3$.
Reducing mod $\mathcal{L}$ we obtain $\hat{\alpha} = \hat{a} + \hat{b}\hat{i} \in \mathbb{F}_{\ell^6}$ with $\hat{a}, \hat{b} \in \mathbb{F}_{\ell^3}$.
Starting from

$$(a + bi)(a - bi) = p^2,$$

and reducing mod $\mathcal{L}$ we obtain:

$$(\hat{a} + \hat{b}\hat{i})(\hat{a} - \hat{b}\hat{i}) = \hat{p}^2.$$

But $\hat{a}, \hat{b} \in \mathbb{F}_{\ell^3}$ and $\hat{i}^{\ell^3} = -\hat{i}$ (because $\ell^3 \equiv 3 \pmod 4$), so the Frobenius morphism "raise to the ℓ^3 " agrees with the reduction of complex conjugation, i.e.,

$$(\hat{a} + \hat{b}\hat{i})(\hat{a}^{\ell^3} + \hat{i}^{\ell^3}\hat{b}^{\ell^3}) = \hat{p}^2.$$

Therefore

$$(\hat{a} + \hat{b}\hat{i})(\hat{a} + \hat{b}\hat{i})^{\ell^3} = (\hat{a} + \hat{b}\hat{i})^{\ell^3+1} = \hat{p}^2,$$

i.e.,

$$\alpha^{\ell^3+1} \equiv p^2 \pmod{\ell}$$

So the order of α divides $(\ell^3 + 1)(\ell - 1) = (\ell^2 - \ell + 1)(\ell + 1)(\ell - 1)$.
But α is a root of the characteristic polynomial (8.1) and, by assumption, its order is a multiple of $\ell^4 + \ell^2 + 1 = (\ell^2 + \ell + 1)(\ell^2 - \ell + 1)$. This is a contradiction. This proves that for every prime inert in $[\mathbb{Q}(i) : \mathbb{Q}]$, the image of the corresponding Galois representation cannot be $\mathrm{PSL}(3, \mathbb{F}_{\ell^2})$.

Remark: The fact that the images of the Galois representations for inert primes, when irreducible, are unitary, can be proved directly using the particular form of the characteristic polynomials, which in turn is a consequence of the Riemann hypothesis (see [A-M 92]).

4.9 Inert primes with reducible image revisited

Up to this point, the fact that the conductor (if it exists) of the compatible family of Galois representations is unknown has forced us to exclude sets of primes of small density, or a not explicitly given set of Dirichlet density 0, in order to deal with reducibility of the image. Now we will show that in the case of inert primes, for the example we are considering, we can give a description of a density 0 set of primes containing the (possibly empty) set of primes with reducible image as those primes dividing the values of a function.

We emphasize that the results of this section apply exclusively to the example $\bar{\sigma}_{S_2,\lambda}$. Recall that the character ε that appears in the reducible case for inert primes (see section 8.1) has its image contained in $\mathbb{F}_{\ell^2}^*$ and ramifies only at 2 (a priori, its image is in $\mathbb{F}_{\ell^6}^*$, but all the elements of this group with order a power of 2 lie in $\mathbb{F}_{\ell^2}^*$).

For ease of notation we put $\sigma_\lambda := \sigma_{S_2,\lambda}$.

4.9.1 The "easy" cases

As in section 8.1, for an inert prime ℓ with reducible image, we have $\varepsilon\chi^i$ as a quotient or subrepresentation of $\bar{\sigma}_\lambda$, with $i = 0, 1, 2$ and ε unramified outside 2 with image in $\mathbb{F}_{\ell^2}$. In this section we deal with the cases $i = 0, 2$.

Case $i = 0$: Let p be a prime such that $\sigma_\lambda(\text{Frob } p)$ has its trace a_p in $\mathbb{Z}$. Thus, $\bar{\sigma}_\lambda(\text{Frob } p)$ has its trace in $\mathbb{F}_\ell$. If we look at the list of the traces we find :

$$(p, a_p) = (17, 7); (31, 1); (41, -5); (97, 7). \tag{9.1}$$

For an inert prime ℓ, $\ell \neq p$ as usual, with reducible image and these values of p we have that the characteristic polynomial of $\bar{\sigma}_\lambda(\text{Frob } p)$ has roots: p and $\varepsilon(p)$.

First of all, let us consider the case when these two are one and the same root. Suppose that $p \equiv \varepsilon(p) \pmod{\lambda}$. In this case we have $\varepsilon(p) \in \mathbb{F}_\ell$, and therefore $(2 \parallel \ell - 1)$ $\varepsilon(p) = \pm 1$. This implies $p \equiv \pm 1 \pmod{\ell}$, i.e.,

$$\ell \mid p \pm 1. \tag{9.2}$$

So except for these finitely many primes, we have:

$$p \not\equiv \varepsilon(p) \pmod{\lambda}.$$

Then these are two different roots of $\bar{\sigma}_\lambda(\text{Frob } p)$, and we can easily compute the third: $p^3/(p\varepsilon(p)) = p^2\varepsilon^{-1}(p)$. So the trace of this matrix is

$$p + \varepsilon(p) + p^2\varepsilon(p)^{-1}$$

and it is an element of $\mathbb{F}_\ell$, because $a_p \in \mathbb{Z}$. This gives

$$\varepsilon(p) + p^2\varepsilon(p)^{-1} \in \mathbb{F}_\ell. \qquad (9.3)$$

Now observe that $\varepsilon(p) \in \mathbb{F}_{\ell^2}^*$ (a cyclic group of order $\ell^2 - 1$) has order a power of 2 , and $2 \parallel \ell - 1$, thus implying that $\varepsilon(p)^{\ell+1} = \pm 1$. Then, $\varepsilon(p)^\ell = \pm\varepsilon(p)^{-1}$. But $\varepsilon(p) + \varepsilon(p)^\ell \in \mathbb{F}_\ell$, so we have: $\varepsilon(p) \pm \varepsilon(p)^{-1} \in \mathbb{F}_\ell$ (for a suitable choice of sign). This together with (9.3) implies:

$$(p^2 \pm 1)\varepsilon^{-1}(p) \in \mathbb{F}_\ell. \qquad (9.4)$$

Therefore, either $\varepsilon(p) \in \mathbb{F}_\ell$, in which case it is $\varepsilon(p) = \pm 1$, or:

$$\ell \mid p^2 \pm 1. \qquad (9.5)$$

Observe that the finite set of primes ℓ verifying (9.5) contains the ones we had to exclude in (9.2). We have proved the following:

Lemma 4.18 *Let $\ell \equiv 3 \pmod 4$ be a prime such that the image of $\bar{\sigma}_\lambda$ is reducible and is in the case "$i = 0$".*
Let p be a prime ($p \nmid 2\ell$) such that $a_p \in \mathbb{Z}$. Then, either

$$\ell \mid (p+1)(p-1)(p^2+1)$$

or

$$\varepsilon(p) = \pm 1.$$

In our example, using $a_{17} = 7$, the only possibility for an inert prime ℓ as in the lemma is $\ell = 3$, or $\varepsilon(17) = \pm 1$. In this latter case, the character ε is defined modulo 32, and this bound implies in particular that the effective computation of reducible inert primes made in section 8.1, for the case "i=0", applies to all inert primes, so no prime $\ell > 3$, $\ell \equiv 3 \pmod 4$ falls in this case.

Case $i = 2$: This case is quite similar to the previous one, and with the same reasoning and computations we reach the same conclusion, so lemma 4.18 and its consequences are also valid for the case $i = 2$.

4.9.2 The "hard" case

Now we consider the case "$i = 1$". In this case the characteristic polynomial for $p \nmid 2\ell$ has $p\varepsilon(p)$ as a root. We will not be able to prove irreducibility for all inert primes; we will fail on a set of density 0, which we will explicitly compute. We make use again of characteristic polynomials with $a_p \in \mathbb{Z}$, together with a concrete formula for the values of the character ε, which are roots of unity of order a power of 2 in $\mathbb{F}_{\ell^2}$.

Let ℓ be an inert prime with $\ell \equiv -1 \pmod{2^u}$ "strictly", i.e., $2^u \parallel \ell+1$. Then, the conductor of ε divides 2^{u+1}, so for every prime $p \nmid 2\ell$ we have: $\varepsilon(p)^{2^{u+1}} = 1$. In this situation, a root of unity of order 2^v in $\mathbb{F}_{\ell^2}$ with $3 \leq v \leq u$ has the form:

$$\pm\left\{\sqrt{2 \pm \sqrt{2 \pm \ldots\sqrt{2 \pm \sqrt{2}}}} \pm i\sqrt{2 \mp \sqrt{2 \pm \ldots\sqrt{2 \pm \sqrt{2}}}}\right\}/2 = c_v + i d_v, \quad (9.6)$$

with the symbol $\sqrt{\ }$ appearing $v-2$ times both in c_v and d_v. The different choices of signs in c_v give different roots of unity of the same order. From the hypothesis $\ell \equiv -1 \pmod{2^u}$ and $v \leq u$ it follows that c_v and d_v are in $\mathbb{F}_\ell$ (this fails for $v > u$). The values of ε on primes $p \equiv 1 \pmod 8$ have order dividing 2^u, and therefore they are of the form (9.6), or $\pm 1, \pm i$.

We will compare (9.6) with the roots of the characteristic polynomials for $p = 17$ and 41, with traces in $\mathbb{Z}$.

For $p = 17$ we have the factorization:

$$(x-17)(x-(-5+2i\sqrt{2}\sqrt{33}))(x-(-5-2i\sqrt{2}\sqrt{33})). \quad (9.7)$$

In virtue of theorem 4.17 we restrict our attention to inert primes $\ell \equiv -1 \pmod 8$. Reducing (9.7) modulo such a prime, we have $2 \in (\mathbb{F}_\ell)^2$, and therefore the equation has all its roots in $\mathbb{F}_\ell$ if $(\frac{33}{\ell}) = -1$. Besides, one of these roots must be equal to $17 \cdot \varepsilon(17)$ under the reducibility assumption for ℓ. In particular, $2 \parallel \ell - 1$ implies that $\varepsilon(17) = \pm 1$ whenever $(\frac{33}{\ell}) = -1$.

If $\varepsilon(17) = \pm 1$ or $\pm i$, it is a character defined modulo 64, so the computation of reducible inert primes for the case "i=1" made in section 8.1 applies, and no $\ell > 3$ appears.

Therefore, we assume that $\varepsilon(17)$ is of the form $c_v + i d_v$ with $3 \leq v \leq u$, and a fortiori $(\frac{33}{\ell}) = 1$. Equating $17 \cdot \varepsilon(17) = 17(c_v + i d_v)$ with a non trivial root of (9.7), we obtain:

$$-5/17 \equiv c_v \pmod{\ell}.$$

Squaring and subtracting 2 from both sides, and repeating this $v-2$ times, this congruence implies that ℓ divides the value $f_{17}(v-2)$, where the function f_{17} is recursively defined as follows:

$$f_{17}(0) = -10,$$
$$f_{17}(n+1) = f_{17}(n)^2 - 2 \cdot 17^{2^{n+1}}.$$

Therefore, if $\ell \equiv -1 \pmod{2^u}$ strictly, it can fall in the reducible case with "i=1" only if

$$\ell \mid f_{17}(j), \quad 1 \leq j \leq u-2. \qquad (9.8)$$

In particular, given u, only finitely many primes of this type appear. Moreover, it is not possible that $\ell \mid f_{17}(j')$ for $j' > u-2$, because reversing the computations this gives $c_{j'+2} \in \mathbb{F}_\ell$, and this is impossible ($j'+2 > u$). Then the set of inert primes dividing some value of f_{17} is a density 0 set of primes and contains those that fall in the reducible case.

We apply the same reasoning to $p = 41$. The corresponding characteristic polynomial has the factorization:

$$(x-41)(x-(-23+24i\sqrt{2}))(x-(-23-24i\sqrt{2})),$$

and inert primes with reducible image in the case "i=1" must divide $f_{41}(j)$ for some positive j (bounded, as in (9.8), in terms of the highest power of 2 in $\ell+1$), where the definition of this function is:

$$f_{41}(0) = -46,$$
$$f_{41}(n+1) = f_{41}(n)^2 - 2 \cdot 41^{2^{n+1}}.$$

Computing $f_{17}(j)$ and $f_{41}(j)$ for $j = 1, 2, ..., 10$, and the greatest common divisors $\gcd(f_{17}(j_1), f_{41}(j_2))$ of these values, the only inert primes that we find in these gcd are: 31 and 1279. Applying (9.8) and the similar result for f_{41} we conclude that these are the only inert primes greater than 3 of the form $\ell \not\equiv -1 \pmod{2^{13}}$ such that the image may fall in the reducible case. The necessary condition $(\frac{33}{\ell}) = 1$ is satisfied by both of them. But computing the reduction of a few characteristic polynomials modulo these two primes, we check that the image is irreducible in both cases.

From the discussion above and the results of sections 8 and 9.1 we deduce the following:

Theorem 4.19 *For $p = 17$ and 41 consider the set of primes:*

$$\mathbb{S}_p = \{\ell : \ell \equiv 3 \pmod 4,\ \ell \mid f_p(j),\ j > 0\},$$

for the functions f_{17} and f_{41} defined above.
These two sets have Dirichlet density 0 and the family of representations $\sigma_\lambda = \sigma_{S_2,\lambda}$ verifies:

$$\mathrm{Image}(\mathbb{P}(\bar{\sigma}_\lambda)) = \mathrm{PSU}(3, \mathbb{F}_\ell)$$

for every prime $\ell > 3,\ \ell \equiv 3 \pmod 4$, except at most for the primes in $\mathbb{S}_{17} \bigcap \mathbb{S}_{41}$.
In particular the result is valid for every prime

$$\ell \equiv 3 \pmod 4,\ \ell \not\equiv -1 \pmod{2^{13}},\ \ell > 3,$$

and for every $\ell \equiv 3 \pmod 4$, $(\frac{33}{\ell}) = -1,\ \ell > 3$.

From this, for the representations $\overline{\chi^{-1} \otimes \sigma_\lambda}$ and for the primes to which the above theorem applies, the following holds:

$$\mathrm{Image}(\overline{\chi^{-1} \otimes \sigma_\lambda}) = \mathrm{SU}(3, \mathbb{F}_\ell).$$

Corollary 4.20 *The groups $\mathrm{SU}(3, \mathbb{F}_\ell)$ are Galois groups over $\mathbb{Q}$ for the primes $\ell > 3,\ \ell \equiv 3 \pmod 4$, except at most for the primes in $\mathbb{S}_{17} \bigcap \mathbb{S}_{41}$. In particular the result is valid for every prime*

$$\ell \equiv 3 \pmod 4,\ \ell \not\equiv -1 \pmod{2^{13}},\ \ell > 3,$$

and for every $\ell \equiv 3 \pmod 4$, $(\frac{33}{\ell}) = -1,\ \ell > 3$.
For each ℓ, the corresponding number field is unramified outside 2ℓ.

Remark: The groups $\mathrm{SU}(3, \mathbb{F}_\ell)$ for all primes $\ell \equiv 3 \pmod 4$, $\ell > 3$, have been realized as Galois groups over $\mathbb{Q}$ using rigidity methods in [Ma 90].

4.10 Final comments on the example

Let $\sigma_\lambda = \sigma_{S_2,\lambda}$ be the compatible family of Galois representations whose images we have determined in the previous sections.
For the prime $\ell = 5$ we have computed the reduction of the characteristic

polynomials of $\sigma_5(\text{Frob } p)$ modulo 5 for $2 < p \leq 97$, $p \neq 5$, and we have found the trivial character 1 as a root of them; so we suspect that the residual representation for 5 is reducible with $\varepsilon = 1$ and "i=0". If this were so, after semi-simplification we also obtain a two-dimensional subrepresentation π over $\mathbb{F}_5$, unramified outside $2 \cdot 5$, with determinant χ^3 (χ the mod 5 cyclotomic character). The semi-simplification of the restriction of π to the inertia group at 5 (see section 5) is the sum of the characters χ and χ^2 or ψ_2^{2+5} and $\psi_2^{1+2\cdot 5}$. The computations also show that π is irreducible. If a_p is the trace of $\bar{\sigma}_5(\text{Frob } p)$ and b_p that of $\pi(\text{Frob } p)$ then we have:

$$a_p \equiv 1 + b_p \pmod 5, \qquad (10.1)$$

for every $p \nmid 10$. Applying Serre's conjecture (see [Se 87]) to π we deduce that there should exist a classical modular form f of level a power of 2 and weight 8 whose Fourier coefficients reduced modulo 5 agree with the b_p. Looking at the space of newforms $S_8(128)$ we have found a newform verifying this for every $p \leq 97$, thus providing more evidence for the fact that $\bar{\sigma}_5$ is reducible. Observe that the congruence (10.1) relates the coefficients of f, an eigenform in $S_8(128)$, with those of an eigenform in $H^3(\Gamma_0(128), \mathbb{C})$.
The values a_p are computed in [vG-T 94] in terms of the number of points of S_2 and other related surfaces over finite fields. The reducibility at 5 would imply congruences modulo 5 involving these numbers of points, depending only on the value modulo 40 of the characteristic p of the finite field.

For an inert prime ℓ greater than 3 such that the image of $\bar{\sigma}_\lambda$ is not as in theorem 4.19, if any, this representation must be reducible and with "i=1". After semi-simplification we would obtain a two dimensional subrepresentation π over $\mathbb{F}_{\ell^2}$.
It can be proved that $\text{Image}(\mathbb{P}(\pi))$ must be conjugated in $\text{PGL}(2, \mathbb{F}_{\ell^4})$ to $\text{PSL}(2, \mathbb{F}_\ell)$. In this case, after conjugation and twisting by an appropriate character, the image of π would be $\text{SL}(2, \mathbb{F}_\ell)$.
To see this we apply the classification of subgroups of $\text{PSL}(2, \mathbb{F}_{\ell^r})$ as in [Ri 75] and [Ri 97] and the techniques of this chapter; unitariness and the Cebotarev density theorem to prove that the reducibility assumption implies that the three roots of the characteristic polynomials of $\bar{\sigma}_\lambda(\text{Frob } p)$ must be in $\mathbb{F}_{\ell^2}$, the techniques of sections 6 and 8 to eliminate the dihedral and special cases for the image of $\mathbb{P}(\pi)$ and the description of the restriction to inertia at ℓ together with the results of section 9.1 to eliminate the possibility that π were reducible.

4.11 On the generality of the previous results

We stress that conclusions such as those of sections 6, 7 and 8 asserting that the images are generically "as large as possible" will still be valid if we perform the computations starting from any other similar geometric three-dimensional compatible family of Galois representations defined over an imaginary quadratic field K (for example, those obtained from the surfaces S_a for any $a \in \mathbb{Z} - \{0\}$) as long as the Hodge structure is as in the example, condition 1' is verified with an "excluded set" of primes of relatively small density, the family of representations is non-selfdual in the general sense (this is automatic if $K \neq \mathbb{Q}(\sqrt{-3}\,)$) and does not have cubic CM, nor is dual with respect to any character.

In particular, Jasper Scholten has communicated to us that with the techniques of [Sc 00] using elliptic surfaces he can produce examples of non-selfdual compatible families of three-dimensional Galois representations defined over $\mathbb{Q}(\sqrt{-3})$. Unfortunately, these examples have not been published and are unavailable. If any of these examples verifies all of the above conditions, then as a consequence we would realize the groups $\mathrm{SL}(3, \mathbb{F}_\ell)$ as Galois groups over $\mathbb{Q}$ for every $\ell \equiv \pm 1 \pmod{12}$, except for a subset of primes of Dirichlet density 0, and the groups $\mathrm{SU}(3, \mathbb{F}_\ell)$ for every $\ell \not\equiv \pm 1 \pmod{12}$ except for a subset of Dirichlet density 0.

The only point where the argument seems to depend on the fact that $K = \mathbb{Q}(i)$ is section 8.2, but it is straightforward to verify that it applies to any imaginary quadratic field. The only step that needs a closer look is the congruence $\hat{i}^{\ell^3} = -\hat{i}$ (in fact an equality even in characteristic 0), a crucial point because it shows that complex conjugation agrees with the Frobenius automorphism. In the general case it becomes $\hat{\xi}^{\ell^3} = -\hat{\xi}$ with $\xi = \sqrt{-D}$ and ℓ inert in $K = \mathbb{Q}(\xi)$. This congruence follows from $(-D)^{\frac{\ell-1}{2}} \equiv -1 \pmod{\ell}$.

4.12 Strong Form of Clozel's conjecture and applications

4.12.1 The Conjecture

In this section we will assume the validity of a strong form of Clozel's conjecture and we will derive consequences for inverse Galois theory. We will give intrinsic conditions on a Hecke eigenform (whose eigenvalues generate an imaginary quadratic field) guaranteeing that the results summarized in the previous section apply to the attached Galois representations, so for those eigenforms verifying these conditions the images of the residual representations will be "as large as possible" for almost every prime: SL_3 or SU_3 (after twisting by χ) depending on the decomposition type of the prime.

Conjecture 4.21 *Let $f \in H^3(\Gamma_0(N), \mathbb{C})$ be a cuspidal Hecke eigenform, then there is a compatible family of Galois representations attached to f as described in conjecture 4.4. These representations ρ_λ arise from the action of $G_{\mathbb{Q}}$ on a rank 3 motive defined over $\mathbb{Q}$ with coefficients in $\mathbb{Q}_f$. For every $\ell \nmid N$ the (semi-simplification of the) restriction of $\bar{\rho}_\lambda$ to the inertia group at ℓ is not the group of scalar matrices $\chi \cdot Id$. Moreover, for every ℓ, the conductor of $\bar{\rho}_\lambda$ divides the level N.*

Remark: The resulting motive has weight 2.
Justification: The geometric or motivic nature of the conjectured Galois representations appears already in [Cl 90] (see also [Ra 94]). The relation between the weight of the modular form and the image of inertia is taken from the generalizations of Serre's conjectures by Ash and Sinnott (see [A-S 00]).
Finally, the relation between the level and the conductor comes from the analogy with the case of classical modular forms. Recently, this relation has been postulated as part of the generalized Serre's conjecture for the case of arbitrary level (see [A-D-P 01]). Removing this last hypothesis would complicate the computations as in the purely geometric example we considered above, and the results on the largeness of the images would hold only outside a density 0 set of primes.
Assuming conjecture 4.21, we can apply the techniques of the previous sections to modular families of Galois representation. The desired result will follow as long as the modular form f verify certain conditions.

4.12.2 Conditions on the Modular Forms

As usual, we consider only the case of Hecke eigenforms $f \in H^3(\Gamma_0(N), \mathbb{C})$ with $\mathbb{Q}_f$ imaginary quadratic. If f is cuspidal, the needed facts, i.e., that the

roots of the characteristic polynomial of the image of Frob p should have absolute value p (Ramanujan's conjecture) and the bound on the eigenvalue a_p that this implies, are known (using the fact that f is a cuspidal automorphic forms on GL(3)). They agree with the geometric hypothesis in conjecture 4.21 (Riemann hypothesis).
The statement about the image of inertia at ℓ in conjecture 4.21 can be replaced by a condition on the Hodge decomposition of the motive, as explained in section 5.

Therefore, in order to apply the techniques of previous sections to these representations and obtain large images, we only need to determine which conditions on f correspond to the fact that the family of Galois representations become:

1) selfdual (in general sense),

2) reducible, or

3) monomial.

Explanation:

2) If the representations $\bar{\rho}_\lambda$ were reducible for infinitely many λ, then thanks to Ramanujan's conjecture we can assume (see sections 6 and 8) that one of the irreducible components is of the form $\varepsilon_\lambda \chi$, where ε_λ is a character with conductor dividing N. Moreover, using the fact that the determinant χ^3 of $\bar{\rho}_\lambda$ is unramified at N, we conclude that it must hold: $\mathrm{cond}(\varepsilon_\lambda)^2 \mid N$.
Let us show that in this situation the representations are reducible also in characteristic 0, independently of ℓ. To see this, observe that from the uniform bound on the conductors of the characters ε_λ, we know that there is a complex character ε with the square of its conductor dividing N such that $\varepsilon(p)p$ is a root of $\rho_\lambda(\mathrm{Frob}\ p)$, for every $p \nmid N$, $\ell \nmid N$.
From this and the reducibility of infinitely many residual representations, an application of the theory of pseudo-representations (see [Ta 91]) proves that the values $\{a_p - \varepsilon(p)p\}$ correspond to the traces of a two-dimensional compatible family of Galois representations $\{\nu'_\lambda\}$.
For an exposition of the standard facts of the theory of pseudo- representations and how to use them to prove reducibility, see chapter 6, section 6.

The only difference is that because we are not dealing with odd residual representations the construction of the representations ν'_λ is done using Taylor's notion of pseudo-representation instead of Wiles' one. Therefore, for every λ there is a λ'-adic Galois representation $\nu_{\lambda'}$ over $\overline{\mathbb{Q}}_{\lambda'}$ (λ' a prime above λ) with $\mathrm{trace}(\nu_{\lambda'}(\mathrm{Frob}\ p)) = a_p - \varepsilon(p)p$, for every $p \nmid \ell N$.
We conclude that if the representations $\bar{\rho}_\lambda$ are reducible for infinitely many λ, then they are so for every prime λ. Furthermore, after a field extension we obtain a reducible family of λ'-adic representations:

$$\rho_{\lambda'}^{ss} = \varepsilon \cdot \chi \oplus \nu_{\lambda'}.$$

The converse is obvious. In what follows, condition 2) refers to either of these two equivalent conditions.

3) As explained in section 6.2, dual respect to a character was a weaker notion introduced to simplify computations, but if the images of the Galois representations fall in case c) or d) (see section 4) for infinitely many primes, the representations are monomial for every $\lambda \nmid N$. In these cases the representations are induced from a character of a cyclic, respectively (Galois closure of a) non-cyclic, cubic extension of $\mathbb{Q}$.

1) "In general sense" means up to multiplication by a character. Recall that this is incompatible with the assumption that $\mathbb{Q}_f$ is imaginary quadratic, except for the case of $\mathbb{Q}_f = \mathbb{Q}(\sqrt{-3})$.

Now let us translate these three conditions to conditions on the Hecke eigenform f, using the language of automorphic forms. This can be done because our space of modular forms can be thought of as being included in that of automorphic forms on $\mathrm{GL}(3)/\mathbb{Q}$, and the cuspidal modular forms correspond to cuspidal automorphic forms (see [A-G-G 84]).

- Condition 1) implies that the automorphic form is selfdual:

$$f \otimes \omega = f^\vee, \qquad (I)$$

  where ω is a Hecke character, i.e., a one dimensional automorphic representation of $\mathrm{GL}(1)/\mathbb{Q}$. This is the case in particular when f is the symmetric square constructed by Gelbart and Jacquet of an automorphic representation on $\mathrm{GL}(2)/\mathbb{Q}$.

- Condition 2) implies that the Galois representations attached to f (assuming they are semisimple) reduce as the sum of the Galois representations associated to a Hecke character and those associated to a certain rank two motive. In this situation, we can apply a result ([Ra 94], prop. 3.2.4) guaranteeing that the property of a motive of being associated to an automorphic form is "closed under subtraction" (this generalizes theorem 4.7 in [J-S 81]), so we have:

$$f = \omega \boxplus g, \qquad (II)$$

where ω is a Hecke character and g an automorphic form on $\mathrm{GL}(2)/\mathbb{Q}$. In this case f cannot be cuspidal (see [J-S 81]).
Remark: The result we are applying is only proved (see [Ra 94]) under the assumption of the analytic Tate conjecture.

- Condition 3) in our case of cubic induction is also a case of Langlands' functoriality solved, i.e., given E (the Galois closure of) a cubic extension of $\mathbb{Q}$ and a Hecke character φ on $\mathrm{GL}(1)/E$ there is an automorphic form on $\mathrm{GL}(3)/\mathbb{Q}$ with the same L-function:

$$f = Ind_E^{\mathbb{Q}}(\varphi). \qquad (III)$$

These are the automorphic representations corresponding to condition 3).

Theorem 4.22 *Assume conjecture 4.21 and the analytic Tate conjecture (cf. [Ra 94]). If a cuspidal Hecke eigenform f with $\mathbb{Q}_f$ imaginary quadratic does not verify either condition (I) or (III) above, then the images of the residual representations $\bar{\rho}_\lambda$ attached to f are "as large as possible" for almost every ℓ. Moreover, if $\mathbb{Q}_f \neq \mathbb{Q}(\sqrt{-3})$ then f does not verify condition (I).*

4.12.3 Examples

First we apply these ideas to the eigenform $f \in H^3(\Gamma_0(128), \mathbb{C})$ appearing in theorem 4.5. As stated there, all coefficients used in the computations agree with the traces of the family of geometric Galois representations studied in detail in previous sections. In particular from the computations done in those sections we conclude that this eigenform does not verify condition (I), (II) or (III). The artificial conductor for condition 1') used in section 6 and 8 was

128, which we are now assuming to be the conductor of the family of Galois representations attached to f, so conditions 1') and 1) become equivalent in this case. Therefore, the conclusions of sections 6 and 8 follow, but now for all primes.

Theorem 4.23 *Assume conjecture 4.21 to be true. Then, if we call σ_λ the family of Galois representations attached to the eigenform $f \in H^3(\Gamma_0(128), \mathbb{C})$, we have*

$$\mathrm{Image}(\overline{\chi^{-1} \otimes \sigma_\lambda}) = \mathrm{SL}(3, \mathbb{F}_\ell),$$

for every $\ell \equiv 1 \pmod 4$, $\ell > 5$ and

$$\mathrm{Image}(\overline{\chi^{-1} \otimes \sigma_\lambda}) = \mathrm{SU}(3, \mathbb{F}_\ell)$$

for every $\ell \equiv 3 \pmod 4$, $\ell > 3$. In particular, these linear and unitary groups are Galois groups over $\mathbb{Q}$.

As our next example we take the eigenform $f \in H^3(\Gamma_0(88), \mathbb{C})$ with $\mathbb{Q}_f = \mathbb{Q}(\sqrt{-7})$ whose coefficients are listed in [vG-K-T-V 97] for $p \leq 173$.
We assume that the conductor of the family of Galois representations attached to f is 88, so condition 1) defined in section 6 is satisfied because $a_{89} = -60 - 4\sqrt{-7}$ is not real. This implies in particular that f does not verify condition (II). Using a_{89} we compute the finitely many primes with (possibly) reducible residual image as described in sections 6 and 8 and we only obtain $\ell = 2, 2879, 48889$ (except for 7 which ramifies in $\mathbb{Q}_f$, 11 which may divide the conductor of the representations and 89). Looking at the reduction of a couple of characteristic polynomials modulo $\ell = 89, 2879, 48889$ we see that for none of them the residual representation is reducible.

Remark: In order to simplify the determination of the primes with reducible image, condition 1) can be improved by using the fact that $\mathrm{cond}(\varepsilon)^2 \mid N$. In particular if N is square-free the character ε becomes trivial. We will use this in the next example.
As explained in section 6, we study cases c) and d) considering all possible cubic (none!) and quadratic characters unramified outside $2 \cdot 11$. Using a couple of coefficients of f for each possible such character and using the equations described in section 6, we see that no prime $\ell > 3$ falls in these cases, i.e., the image of the residual representation is not monomial for any such ℓ. In particular, this implies that f is not an eigenform verifying condition

(III).
Using only $a_3 = -1 + \sqrt{-7}$ we study condition e) as in section 6 and see that no $\ell > 3$ falls in this case, i.e., the image of the residual representation is not selfdual (in general sense) for any such ℓ. It was a priori known that f is not an eigenform verifying condition (I) from the last assertion in theorem 4.22. Finally, as in section 6 and 8, we know from the possible orders of the image of inertia (thanks to the exclusion of the trivial case in conjecture 4.21) that the only primes $\ell > 3$ such that the image may fall in one of the exceptional cases in the classification are: $\ell = 5, 7, 11, 13, 19$. The prime 7 ramifies in $\mathbb{Q}_f$ and 11 may divide the conductor. For the remaining three primes, we compute the reduction of some characteristic polynomials and see that there are elements in the images with orders not corresponding to the order of any element in any of the exceptional groups. So we conclude that the image of the residual Galois representation is not exceptional for any $\ell > 3$.
We remark that for the prime $\ell = 5$, inert in $\mathbb{Q}(\sqrt{-7})$, we have considered (and eliminated) the cases of exceptional image $2 \cdot A_6$ or A_7 that were not listed in section 4 and are the only extra possibilities (see [Mi 11]).
From all this we conclude:

Theorem 4.24 *Assume conjecture 4.21 to be true. Then, if we call σ_λ the family of Galois representations attached to f, we have*

$$\mathrm{Image}(\overline{\chi^{-1} \otimes \sigma_\lambda}) = \mathrm{SL}(3, \mathbb{F}_\ell)$$

for every ℓ such that $(\frac{-7}{\ell}) = 1$, $\ell \geq 13$ and

$$\mathrm{Image}(\overline{\chi^{-1} \otimes \sigma_\lambda}) = \mathrm{SU}(3, \mathbb{F}_\ell)$$

for every ℓ such that $(\frac{-7}{\ell}) = -1$, $\ell \geq 5$.
In particular, these linear and unitary groups are Galois groups over $\mathbb{Q}$.

Combining the last two theorems we also have:

Corollary 4.25 *Assume conjecture 4.21 to be true. Then, the following are Galois groups over $\mathbb{Q}$:*

$$\mathrm{SL}(3, \mathbb{F}_\ell)$$

for every $\ell \equiv 1, 2, 4 \pmod 7$, $\ell \geq 13$; and

$$\mathrm{SU}(3, \mathbb{F}_\ell)$$

for every $\ell \equiv 3, 5, 6 \pmod 7$, $\ell \geq 5$.

Another example: Consider the eigenform $f \in H^3(\Gamma_0(53), \mathbb{C})$ with $\mathbb{Q}_f = \mathbb{Q}(\sqrt{-11})$. To check reducibility we can take the character ε as trivial, because the level is prime. Therefore, the congruences determining reducible primes introduced in section 6.1 now hold with any a_p. This and all other cases of the classification are dealt with as in the previous examples, using just the first few characteristic polynomials. After the computations we find 5 as the only prime greater than 3 (excluding 11 and 53) such that the image seems to be not "as large as possible". For this prime, as in the geometric example, the representation seems to be reducible with the trivial character as one-dimensional constituent (5 decomposes in $\mathbb{Q}_f$).
This example, combined with the one of level 128, gives the corollary:

Corollary 4.26 *Assume conjecture 4.21. Then the following are Galois groups over $\mathbb{Q}$:*

$$\mathrm{SL}(3, \mathbb{F}_\ell)$$

for every $\ell \equiv 1, 3, 4, 5, 9 \pmod{11}$, $\ell > 5$; and

$$\mathrm{SU}(3, \mathbb{F}_\ell)$$

for every $\ell \equiv 2, 6, 7, 8, 10 \pmod{11}$, $\ell \geq 5$.

4.13 Bibliography

[A-A-C 98]- Allison, G., Ash, A., Conrad, E., *Galois Representations, Hecke Operators, and the* mod-p *Cohomology of* $\mathrm{GL}(3, \mathbb{Z})$ *with Twisted Coefficients*, Experimental Math. **7**:4 (1998) 361-390

[A-D-P 01]- Ash, A., Doud, D., Pollack, D., *Galois representations with conjectural connections with arithmetic cohomology*, (2001) preprint

[A-G-G 84]- Ash, A., Grayson, D., Green, P., *Computations of Cuspidal Cohomology of Congruence Subgroups of* $\mathrm{SL}(3, \mathbb{Z})$, J. Number Theory **19** (1984) 412-436

[A-M 92]- Ash, A., McConnell, M., *Experimental indications of three-dimensional Galois representations from the cohomology of* $\mathrm{SL}(3, \mathbb{Z})$, Experimental Math. **1**:3 (1992) 209-223

[A-S 00]- Ash, A., Sinnott, W., *An analogue of Serre's conjecture for Galois representations and Hecke eigenclasses in the* mod-p *cohomology of* $\mathrm{GL}(n, \mathbb{Z})$, Duke Math. J. **105** (2000), 1-24

[A-S 86]- Ash, A., Stevens, G., *Cohomology of arithmetic goups and congruences between systems of Hecke eigenvalues*, J. Reine Angew. Math. **365** (1986) 192-220

[Bl 67]- Bloom, D., *The subgroups of* $\mathrm{PSL}(3, q)$ *for odd* q, Trans. Amer. Math. Soc. **127** (1967) 150-178

[Cl 90]- Clozel, L., *Motifs et formes automorphes: applications du principe de fonctorialité*, in "Automorphic Forms, Shimura Varieties and L-functions", Clozel, L., Milne, J. (eds). Proceedings of the Ann Arbor Conference, (1990) 77-159, Academic Press

[F-L 82]- Fontaine, J.M., Laffaille, G., *Construction de représentations p-adiques*, Ann. Scient. Éc. Norm. Sup., 4^e série, t. **15** (1982) 547-608

[F-M 87]- Fontaine, J.M, Messing, W., *p-adic periods and p-adic étale cohomology*, in "Currents Trends in Arithmetical Algebraic Geometry (Arcata, Calif., 1985)". Contemporary Mathematics **67** (1987) 179-207, American Mathematical Society

[vG-K-T-V 97]- van Geemen, B., van der Kallen, W., Top, J., Verberkmoes, A., *Hecke Eigenforms in the Cohomology of Congruences Subgroups of* $\mathrm{SL}(3, \mathbb{Z})$, Experiment. Math. **6**:2 (1997) 163-174

[vG-T 94]- van Geemen, B., Top, J., *A non-selfdual automorphic representation of* GL_3 *and a Galois representation*, Invent. Math. **117** (1994) 391-401

[vG-T 96]- ______ , *Modular Forms on GL(3) and Galois representations*, notes, 1996

[J-S 81]- Jacquet, H., Shalika, J., *Euler products and the classification of automorphic forms II*, Amer. J. Math. **103** (1981) 777-815

[Ma 90]- Malle, G., *Some unitary groups as Galois groups over* $\mathbb{Q}$, J. Algebra **131** (1990) 476-482

[Mi 11]- Mitchell, H., *Determination of the ordinary and modular ternary linear groups*, Trans. Amer. Math. Soc. **12** (1911) 207-242

[Ra 94]- Ramakrishnan, D., *Pure Motives and Automorphic Forms*, Proc. Sympos. Pure Math. **55** Part 2 (1994) 411-445

[Ri 75]- Ribet, K.A., *On ℓ-adic representations attached to modular forms*, Invent. Math. **28** (1975) 245-275

[Ri 97]- ______ , *Images of semistable Galois representations*, Pacific J. of Math. **181** (1997)

[Sc 00]- Scholten, J., *Mordell-Weil groups of elliptic surfaces and Galois representations*, thesis, Rijksuniversiteit Groningen (2000)

[Se 68]- Serre, J.P., *Abelian ℓ-adic representations and elliptic curves*, (1968) Benjamin

[Se 72]- _____ , *Propriétés galoisiennes des points d'ordre fini des courbes elliptiques*, Invent. Math. **15** (1972) 259-331

[Se 87]- _____ , *Sur les représentations modulaires de degré* 2 *de* $\mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q})$, Duke Math. J. **54** (1987) 179-230

[Ta 91]- Taylor, R., *Galois representations associated to Siegel modular forms of low weight*, Duke Math. J. **63** (1991) 281-332

[Th 84]- Thompson, J., PSL_3 *as Galois groups over* $\mathbb{Q}$, in "Proceedings of the Rutgers group theory year, 1983-1984" Cambridge U.P. (1984) 309-319

[V-Y 65]- Veblen, O., Young, J., *Projective geometry*, (1965) Blaisdell Publishing Company

Chapter 5

On the images of the Galois representations attached to abelian surfaces with $\mathrm{End}(A) = \mathbb{Z}$

5.1 Introduction

Let A be an abelian surface defined over $\mathbb{Q}$ with $\mathrm{End}(A) := \mathrm{End}_{\overline{\mathbb{Q}}}(A) = \mathbb{Z}$. Let $\rho_\ell : G_\mathbb{Q} \to \mathrm{GSp}(4, \mathbb{Z}_\ell)$ be the compatible family of Galois representations given by the Galois action on $T_\ell(A) = A[\ell^\infty](\bar{\mathbb{Q}})$, the Tate modules of the abelian surface (we are assuming that A is principally polarized). Each ρ_ℓ is unramified outside ℓN, where N is the product of the primes of bad reduction of A. If we call G_{ℓ^∞} the image of ρ_ℓ then we have the following result of Serre (cf. [Se 86]):

Theorem 5.1 *If A is an abelian surface over $\mathbb{Q}$ with $\mathrm{End}(A) = \mathbb{Z}$ and principally polarized, then $G_{\ell^\infty} = \mathrm{GSp}(4, \mathbb{Z}_\ell)$ for almost every ℓ.*

Remark: If G_ℓ is the image of $\bar{\rho}_\ell$, the Galois representation on ℓ-division points of $A(\bar{\mathbb{Q}})$ (and the residual mod ℓ representation corresponding to ρ_ℓ), it is enough to show that $G_\ell = \mathrm{GSp}(4, \mathbb{F}_\ell)$ for almost every ℓ (cf. [Se 86]). Serre proposed the problem of giving an effective version of this result: "*...partir de courbes de genre 2 explicites, et tâcher de dire à partir de quand le groupe de Galois correspondant G_ℓ devient égal à* $\mathrm{GSp}(4, \mathbb{F}_\ell)$ ". But Serre's proof depends on certain ineffective results of Faltings and therefore does not solve this problem.

In this chapter, we will give an algorithm that computes a finite set $\mathcal{F}$ of primes containing all those primes (if any) with image of the corresponding Galois representation exceptional, i.e., different from $\mathrm{GSp}(4, \mathbb{F}_\ell)$. The validity of our method depends on the truth of Serre's conjecture for 2-dimensional irreducible odd Galois representations, conjecture (3.2.4$_?$) in [Se 87]. This means that if ℓ is a prime such that $G_\ell \neq \mathrm{GSp}(4, \mathbb{F}_\ell)$ and $\ell \notin \mathcal{F}$, then G_ℓ has a 2-dimensional irreducible (odd) component that violates Serre's conjecture.

The method is inspired by the articles [Se 72], [Ri 75], [Ri 85] and [Ri 97] where the case of 2-dimensional Galois representations is treated.

In the examples, we also give infinite sets of primes for which we can prove the result on the images unconditionally, i.e., without assuming Serre's conjecture. Results of this kind were previously obtained by Le Duff only under the extra assumption of semiabelian reduction of the abelian surface at some prime. Our technique has two advantages: it does not have any restriction on the reduction type of the abelian surface, and in the case of semiabelian reduction it allows us to prove the result on the images (unconditionally) for larger sets of primes.

5.2 Main Tools

5.2.1 Maximal subgroups of $\mathrm{PGSp}(4, \mathbb{F}_\ell)$

In [Mi 14], Mitchell gives the following classification of maximal proper subgroups G of $\mathrm{PSp}(4, \mathbb{F}_\ell)$ (ℓ odd), as groups of transformations of the projective space having an invariant linear complex:

1) a group having an invariant point and plane
2) a group having an invariant parabolic congruence
3) a group having an invariant hyperbolic congruence
4) a group having an invariant elliptic congruence
5) a group having an invariant quadric
6) a group having an invariant twisted cubic
7) a group G containing a normal elementary abelian subgroup E of order 16, with: $G/E \cong A_5$ or S_5
8) a group G isomorphic to A_6, S_6 or A_7.

For the relevant definitions see [Hi 85], see also [Bl 17] and [Os 77] for cases 7) and 8).

From this we obtain a classification of maximal proper subgroups H of $\mathrm{PGSp}(4, \mathbb{F}_\ell)$ with exhaustive determinant. It is similar to the above one, except that cases 7) and 8) change according to the relation between H and G, given by the exact sequence:

$$1 \to G \to H \to \{\pm 1\} \to 1.$$

5.2.2 The action of Inertia

From now on we will assume that ℓ is a prime of good reduction for the abelian surface A. Then it follows from results of Raynaud that the restriction $\bar{\rho}_\ell|_{I_\ell}$ has the following property (cf. [Ra 74], [Se 72]):

Theorem 5.2 *If V is a Jordan-Hölder quotient of the I_ℓ-module $A[\ell](\bar{\mathbb{Q}})$ of dimension n over $\mathbb{F}_\ell$, then V admits an $\mathbb{F}_{\ell^n}$-vector space structure of dimension 1 such that the action of I_ℓ on V is given by a character $\phi : I_{\ell,t} \to \mathbb{F}_{\ell^n}^*$ (t stands for tame) with:*

$$\phi = \phi_1^{d_1} \dots \phi_n^{d_n}, \qquad (2.1)$$

where ϕ_i are the fundamental characters of level n and $d_i = 0$ or 1, for every $i = 1, 2, ..., n$.

All this statement is proved by Serre in [Se 72] except for the last line, which is the result of Raynaud mentioned above, later generalized by Fontaine-Messing.

We will use the following lemmas repeatedly (cf. [Di 1901]):

Lemma 5.3 *Let $M \in \mathrm{Sp}(4, F)$ be a symplectic transformation over a field F. If α is a root of the characteristic polynomial of M, then α^{-1} is also a root.*

In the case of the Galois representations attached to A, we know that $\det(\bar{\rho}_\ell) = \chi^2$, where χ is the mod ℓ cyclotomic character. Therefore, we obtain:

Lemma 5.4 *If α is a root of the characteristic polynomial of $\bar{\rho}_\ell(\mathrm{Frob}\ p) \in G_\ell$, then p/α is also a root ($p \nmid \ell N$).*

Proof: Use lemma 5.3, $G_\ell \subseteq \mathrm{GSp}(4, \mathbb{F}_\ell)$, and the exact sequence:

$$1 \to \mathrm{Sp}(4, \mathbb{F}_\ell) \to \mathrm{GSp}(4, \mathbb{F}_\ell) \to \mathbb{F}_\ell^* \to 1.$$

Remark: The same is true for $\rho_\ell(\mathrm{Frob}\ p) \in G_{\ell^\infty}$. Thus, the characteristic polynomial of $\rho_\ell(\mathrm{Frob}\ p)$ has the form:

$$x^4 - a_p x^3 + b_p x^2 - p a_p x + p^2$$

with $a_p, b_p \in \mathbb{Z}$, $a_p = \mathrm{trace}(\rho_\ell(\mathrm{Frob}\ p))$.

From formula (2.1), we obtain the following possibilities for $\bar{\rho}_\ell|_{I_\ell}$ $(\ell \nmid N)$:

$$\begin{pmatrix} 1 & * & * & * \\ 0 & \chi & * & * \\ 0 & 0 & 1 & * \\ 0 & 0 & 0 & \chi \end{pmatrix}; \quad \begin{pmatrix} \psi_2 & 0 & * & * \\ 0 & \psi_2^\ell & * & * \\ 0 & 0 & \psi_2 & 0 \\ 0 & 0 & 0 & \psi_2^\ell \end{pmatrix};$$

$$\begin{pmatrix} \psi_2 & 0 & * & * \\ 0 & \psi_2^\ell & * & * \\ 0 & 0 & 1 & * \\ 0 & 0 & 0 & \chi \end{pmatrix}; \quad \begin{pmatrix} \psi_4^{\ell+\ell^2} & 0 & 0 & 0 \\ 0 & \psi_4^{\ell^2+\ell^3} & 0 & 0 \\ 0 & 0 & \psi_4^{\ell^3+1} & 0 \\ 0 & 0 & 0 & \psi_4^{1+\ell} \end{pmatrix},$$

where ψ_i is a fundamental character of level i.

5.3 Study of the Images

5.3.1 Reducible case: 1-dimensional constituent

Let c be the conductor of the compatible family $\{\rho_\ell\}$. For the case of the jacobian of a genus 2 curve, it can be computed using an algorithm of Q. Liu except for the exponent of 2 in c, which can easily be bounded using the discriminant of an integral model of the curve (see [Liu 94]).

Suppose that the representation $\bar{\rho}_\ell$ is reducible with a 1-dimensional sub(or quotient) representation given by a character: $\varepsilon\chi^i$, with ε unramified outside N. Clearly $\mathrm{cond}(\varepsilon) \mid c$. From the description of $\bar{\rho}_\ell|_{I_\ell}$ given in section 2.2, we see that the exponent of the cyclotomic character has to be $i = 0$ or 1. After semi-simplification, we have:

$$\bar{\rho}_\ell \cong \varepsilon\chi^i \oplus \pi,$$

for a 3-dimensional representation π with $\det(\pi) = \varepsilon^{-1}\chi^{2-i}$.
Therefore, $\mathrm{cond}(\varepsilon)^2 \mid c$. Let d be the maximal integer such that $d^2 \mid c$. If we take a prime $p \equiv 1 \pmod{d}$, we have $\varepsilon(p) = 1$ so χ^i is a root of the characteristic polynomial of $\bar{\rho}_\ell(\mathrm{Frob}\ p)$. This gives:

$$b_p - a_p(p+1) + p^2 + 1 \equiv 0 \pmod{\ell}, \qquad (3.1)$$

both for $i = 0$ and $i = 1$ (in agreement with lemma 5.4). For large enough p, using the well-known bounds for the absolute values of a_p and b_p, we see that this congruence is not an equality. Therefore, only finitely many primes ℓ may verify (3.1).

Variant: Instead of taking a prime $p \equiv 1 \pmod{d}$, we can work in general with p of order f in $(\mathbb{Z}/d\mathbb{Z})^*$. Let $Pol_p(x)$ be the characteristic polynomial of $\bar{\rho}_\ell(\mathrm{Frob}\ p)$. Then $\varepsilon(p)p^i$ is a root of $Pol_p(x)$, with $i = 0$ or 1, and $\varepsilon(p)^f = 1 \in \mathbb{F}_\ell$. Then

$$\mathrm{Res}(Pol_p(x), x^f - 1) \equiv 0 \pmod{\ell} \qquad (3.2)$$

where Res stands for resultant (again, cases $i = 0$ and 1 agree).
This variant is used in the examples to avoid computing $Pol_p(x)$ for large p.

5.3.2 Reducible case: "related" 2-dimensional constituents

Suppose that, after semi-simplification, $\bar{\rho}_\ell$ decomposes as the sum of two 2-dimensional irreducible Galois representations: $\bar{\rho}_\ell \cong \pi_1 \oplus \pi_2$. Assume also that these two constituents are related by lemma 5.4, i.e., if α, β are the roots of the characteristic polynomial of $\pi_1(\mathrm{Frob}\ p)$, then $p/\alpha, p/\beta$ are the roots of that of $\pi_2(\mathrm{Frob}\ p)$. If not, then it follows from lemma 5.4 that $\alpha = p/\beta$, so $\det(\pi_1) = \det(\pi_2) = \chi$; this case will be studied in the next subsection.
Using the description of $\bar{\rho}_\ell|_{I_\ell}$ given in section 2.2 we see that one of the following must happen (where ε is a character unramified outside N):

- Case 1: $\det(\pi_1) = \varepsilon\chi^2, \quad \det(\pi_2) = \varepsilon^{-1}$.

- Case 2: $\det(\pi_1) = \varepsilon\chi, \quad \det(\pi_2) = \varepsilon^{-1}\chi$.

• Case 1: In this case we have the factorization:

$$Pol_p(x) \equiv (x^2 - rx + p^2\varepsilon(p))\,(x^2 - \frac{rx}{p\varepsilon(p)} + \varepsilon^{-1}(p)) \pmod{\ell}.$$

As in the previous subsection: $\mathrm{cond}(\varepsilon) \mid d$. Eliminating r from the equation, we obtain:

$$Q_p(b_p, a_p, \varepsilon(p)) := (\varepsilon(p)b_p - 1 - p^2\varepsilon(p))(p\varepsilon(p)+1)^2 - a_p p\varepsilon(p)^2 \equiv 0 \pmod{\ell}.$$

If we take $p \equiv 1 \pmod{d}$, we obtain:

$$(b_p - 1 - p^2)\,(p+1)^2 \equiv a_p^2\,p \pmod{\ell}. \qquad (3.3)$$

Again, from the bounds for the coefficients we see that for large enough p this is not an equality. Thus, only finitely many ℓ can satisfy (3.3).

Alternatively, for computational purposes, we may take p with $p^f \equiv 1 \pmod{d}$. Then we have:

$$\mathrm{Res}(Q_p(b_p, a_p, x), x^f - 1) \equiv 0 \pmod{\ell}. \qquad (3.4)$$

• Case 2: This case is quite similar to the previous one. We start with:

$$Pol_p(x) \equiv (x^2 - rx + p\varepsilon(p))\,(x^2 - \frac{rx}{\varepsilon(p)} + p\varepsilon^{-1}(p)) \pmod{\ell}$$

with $\mathrm{cond}(\varepsilon) \mid d$. From this:

$$Q'_p(b_p, a_p, \varepsilon(p)) := (\varepsilon(p)b_p - p - p\varepsilon(p)^2)(\varepsilon(p)+1)^2 - a_p^2\varepsilon(p)^2 \equiv 0 \pmod{\ell}.$$

Thus, if $p \equiv 1 \pmod{d}$,

$$4(b_p - 2p) \equiv a_p^2 \pmod{\ell}. \qquad (3.5)$$

In general, if $p^f \equiv 1 \pmod{d}$,

$$\mathrm{Res}(Q'_p(b_p, a_p, x), x^f - 1) \equiv 0 \pmod{\ell}. \qquad (3.6)$$

In this case, the fact that this holds only for finitely many primes ℓ is non-trivial. It may be thought of as a consequence of theorem 5.1.

5.3.3 The remaining reducible case

As explained above, in the remaining reducible case we have: $\bar{\rho}_\ell^{ss} \cong \pi_1 \oplus \pi_2$ with $\det(\pi_1) = \det(\pi_2) = \chi$. We have described in section 2.2 the possibilities for $\bar{\rho}_\ell|_{I_\ell}$. This gives for $\pi_1|_{I_\ell}$ and $\pi_2|_{I_\ell}$:

$$\begin{pmatrix} 1 & * \\ 0 & \chi \end{pmatrix} \quad \text{or} \quad \begin{pmatrix} \psi_2 & 0 \\ 0 & \psi_2^\ell \end{pmatrix}.$$

Besides, $\mathrm{cond}(\pi_1)\mathrm{cond}(\pi_2) \mid c$.
At this point we invoke Serre's conjecture (3.2.4?) (see [Se 87]) that gives us a control on π_1 and π_2. Both representations should be modular of weight 2, i.e., there exist two cusp forms f_1, f_2 with:

$$\bar{\rho}_{f_1,\ell} \cong \pi_1,\ \bar{\rho}_{f_2,\ell} \cong \pi_2, \quad f_1 \in S_2(N_1),\ f_2 \in S_2(N_2),$$

$N_1N_2 \mid c$ (we are assuming π_1, π_2 to be irreducible; otherwise, they are covered by section 3.1). Both cusp forms have trivial nebentypus.

There are finitely many cusp forms in these finitely many spaces. So we have an algorithm to detect the primes ℓ falling in this case by comparing characteristic polynomials mod ℓ, due to

$$\bar{\rho}_\ell^{ss} \cong \bar{\rho}_{f_1,\ell} \oplus \bar{\rho}_{f_2,\ell}.$$

We take all pairs of integers N_1, N_2 with $N_1N_2 = c$ and all pairs of cusp forms $f_1 \in S_2(N_1),\ f_2 \in S_2(N_2)$ (either newforms or oldforms). If we denote by $Pol_{f_i,p}(x)$ the characteristic polynomial of $\rho_{f_i,\ell}(\mathrm{Frob}\ p)$ $(i = 1, 2)$, we should have for some such pair f_1, f_2:

$$Pol_{f_1,p}(x)Pol_{f_2,p}(x) \equiv Pol_p(x) \pmod{\ell} \qquad (3.7)$$

for every $p \nmid \ell N$.
Theorem 5.1 guarantees that this can only happen for finitely many primes.

Remark: The Galois representations $\rho_{f_i,\ell}$ attached to f_i by Deligne's theorem were introduced in chapter 2. The polynomials $Pol_{f_i,p}(x)$ are of the form

$$Pol_{f_i,p}(x) = x^2 - c_p x + p,$$

where c_p is the eigenvalue of f_i corresponding to the Hecke operator T_p. These eigenvalues, and a fortiori the characteristic polynomials $Pol_{f,p}(x)$ for any cusp form f, can be computed with the algorithm of W. Stein (cf. [St]) already used in chapter 2 and 3.

For computational purposes, we introduce the following variant: observe that either N_1 or N_2 (say N_1) satisfy

$$N_1 \mid c, \ N_1 \leq \sqrt{c}.$$

Consider all divisors of c verifying this, maximal (among divisors of c) with this property. Call S the set of such divisors. Then we are supposing that there exists $f \in S_2(t)$ with $t \in S$ and

$$\mathrm{Res}(Pol_{f,p}(x), Pol_p(x)) \equiv 0 \pmod{\ell},$$

for every $p \nmid \ell N$. Therefore, for some $t \in S$

$$\mathrm{Res}(\prod_{f \in S_2(t)} Pol_{f,p}(x), Pol_p(x) \ ) \equiv 0 \pmod{\ell}, \tag{3.8}$$

for every $p \nmid \ell N$.

With this formula we compute in any given example all primes ℓ falling in this case.

Remark: In all reducible cases (sections 3.1 , 3.2 and 3.3) we have considered reducibility over $\bar{\mathbb{F}}_\ell$.

5.3.4 Stabilizer of a hyperbolic or elliptic congruence

If G_ℓ corresponds to an irreducible subgroup inside (its projective image) some of the maximal subgroups in cases 3) and 4) of Mitchell's classification, there is a normal subgroup of index 2 of G_ℓ such that

$$1 \to M_\ell \to G_\ell \to \{\pm 1\} \to 1,$$

and the subgroup M_ℓ is reducible (not necessarily over $\mathbb{F}_\ell$).
From the description of $\bar{\rho}_\ell|_{I_\ell}$ given in section 2.2 we see that if $\ell > 3$, it is contained in M_ℓ. Therefore, if we take the quotient G_ℓ / M_ℓ we obtain a representation $G_{\mathbb{Q}} \to C_2$ whose kernel is a quadratic field unramified outside

N. Then, there is a quadratic character $\phi : (\mathbb{Z}/c\mathbb{Z})^* \to C_2$ with:
$\phi(p) = -1 \;\Rightarrow\; \bar{\rho}_\ell(\text{Frob } p)$ is of the form:

$$\begin{pmatrix} 0 & 0 & * & * \\ 0 & 0 & * & * \\ * & * & 0 & 0 \\ * & * & 0 & 0 \end{pmatrix}.$$

Therefore, $\text{trace}(\bar{\rho}_\ell(\text{Frob } p)) = 0$, i.e.,

$$a_p \equiv 0 \pmod{\ell}, \qquad (3.9)$$

for every $p \nmid \ell N$ with $\phi(p) = -1$.
Considering all quadratic characters ramifying only at the primes in N we detect the primes ℓ falling in this case.
Once again, from theorem 5.1, it follows that this set is finite (of course, this fact strongly depends on the assumption $\text{End}(A) = \mathbb{Z}$).

5.3.5 Stabilizer of a quadric

This case can be treated exactly as the one above: again there is a normal subgroup of index 2, and we obtain a quadratic character unramified outside N verifying formula (3.9).
In fact, in this case $\bar{\rho}_\ell$ is the tensor product of two irreducible 2-dimensional Galois representations, one of them dihedral, so the matrices in G_ℓ are of the form:

$$\begin{pmatrix} av & 0 & cv & 0 \\ 0 & az & 0 & cz \\ bv & 0 & dv & 0 \\ 0 & bz & 0 & dz \end{pmatrix} \quad \text{or} \quad \begin{pmatrix} 0 & az & 0 & cz \\ av & 0 & cv & 0 \\ 0 & bz & 0 & dz \\ bv & 0 & dv & 0 \end{pmatrix},$$

depending on the value of the quadratic character ϕ.

5.3.6 Stabilizer of a twisted cubic

This case is incompatible with the description of $\bar{\rho}_\ell|_{I_\ell}$ given in section 2.2.
In fact, in this case all upper-triangular matrices are of the form:

$$\begin{pmatrix} a^3 & * & * & * \\ 0 & a^2d & * & * \\ 0 & 0 & ad^2 & * \\ 0 & 0 & 0 & d^3 \end{pmatrix}.$$

In no case is the subgroup of G_ℓ given by $\bar{\rho}_\ell|_{I_\ell}$ of this form.

5.3.7 Exceptional cases

The cases already studied cover all possibilities in the classification except the exceptional groups, i.e., cases 7) and 8).
In these cases, comparing the exceptional group $H \subseteq \mathrm{PGSp}(4, \mathbb{F}_\ell)$ (its order and structure) with the fact that $\mathbb{P}(G_\ell)$ contains the image of $\mathbb{P}(\bar{\rho}_\ell|_{I_\ell})$ described in section 2.2, we end up with the only possibilities ($\ell > 3$):

$$\ell = 5, 7.$$

For these two primes, as for any prime we suspect of satisfying $G_\ell \neq \mathrm{GSp}(4, \mathbb{F}_\ell)$, we compute several characteristic polynomials $Pol_p(x)$ mod ℓ. At the end, either we prove that it must be $G_\ell = \mathrm{GSp}(4, \mathbb{F}_\ell)$ (because the orders of the roots of the computed polynomials do not give any other option) or we reinforce our suspicion that ℓ is exceptional.

5.3.8 Conclusion

Having gone through all cases in the classification (the stabilizer of a parabolic congruence is reducible, it has an invariant line of the complex, cf. [Mi 14]) we conclude that for all primes ℓ except those whose image, according to our algorithm, may fall in a proper subgroup (according to theorem 5.1, only finitely many) the image of $\mathbb{P}(\bar{\rho}_\ell)$ is $\mathrm{PGSp}(4, \mathbb{F}_\ell)$.
From this it easily follows that $G_\ell = \mathrm{GSp}(4, \mathbb{F}_\ell)$ for all these ℓ and applying a lemma of [Se 86] (see also [Se 68]) we obtain $G_{\ell^\infty} = \mathrm{GSp}(4, \mathbb{Z}_\ell)$.
Recall that at one step we have assumed the veracity of Serre's conjecture ($3.2.4_?$).

5.4 An example

We have applied the algorithm to the example given by the jacobian of the genus 2 curve given by the equation:

$$y^2 = x^6 - x^3 - x + 1.$$

The algorithm of Q. Liu computes the prime-to-2 part of the conductor. From this computation and the bound of the conductor in terms of the discriminant of an integral equation (cf. [Liu 94]) we obtain: $c \mid 2^{12} \cdot 23 \cdot 5$.

We exclude a priori the primes dividing the conductor: $2, 5$ and 23.
We sketch some of the computations performed:
• Reducible cases with 1-dimensional constituent or two related 2-dimensional constituents:
The maximal possible value of the conductor of ε is $d = 64$. We compute the characteristic polynomials of $\rho_\ell(\text{Frob } p)$ for the primes $p = 229, 257, 641, 769$ and applying the algorithm (equations (3.2), (3.4) and (3.6)) we easily check that no prime $\ell > 3$ falls in these cases.
Remark: The characteristic polynomials used at this and the remaining steps can be found in section 6.
• Remaining reducible case:
First we describe the set of special divisors of c:

$$S = \{368, 460, 512, 640\}.$$

Then we compute, for each $t \in S$ and each Hecke eigenform $f \in S_2(t)$, the characteristic polynomial $Pol_{f,p}(x)$ for $p = 3, 7, 11, 13, 17, 19$ with the algorithm implemented by W.Stein ([St]). Then, comparing these polynomials with the characteristic polynomials of $\rho_\ell(\text{Frob } p)$ as in formula (3.8) we see that no prime $\ell > 3$ falls in this case.
• Cases "governed" by a quadratic character:
We have to consider all possible quadratic characters ϕ unramified outside c (there are 15) and for each of them take a couple of primes p with $\phi(p) = -1$ and $a_p \neq 0$. Applying the algorithm (formula (3.9)) we see that no prime $\ell > 3$ falls in these cases. At this step we have used the values a_p for the primes $p = 3, 7, 13, 97, 113, 569, 769$.
• Exceptional cases:
We compute the reduction of a few characteristic polynomials modulo 7 and we find elements whose order (in $\mathrm{PGSp}(4, \mathbb{F}_7)$) does not correspond to the structure of any of the exceptional groups.
From all the above computations we conclude:

Theorem 5.5 *Let A be the jacobian of the genus 2 curve:*

$$y^2 = x^6 - x^3 - x + 1.$$

Let G_{ℓ^∞} be the image of $\rho_{A,\ell}$, the Galois representation on $A[\ell^\infty](\bar{\mathbb{Q}})$, whose conductor divides $2^{12} \cdot 5 \cdot 23$. Then, assuming Serre's conjecture ($3.2.4_?$) it holds:

$$G_{\ell^\infty} = \mathrm{GSp}(4, \mathbb{Z}_\ell)$$

for every $\ell > 5$, $\ell \neq 23$.

5.5 Unconditional Results and more examples

5.5.1 The case of semiabelian reduction

For certain genus 2 curves one can prove that the image is large for an infinite set of primes by using the following results of Le Duff [LeD 98]:

Proposition 5.6 *Let A be an abelian surface defined over $\mathbb{Q}$. Suppose that for a prime p of bad reduction of A, $\tilde{A}_p^0$ (the connected component of 0 in the special fiber of the Néron Model of A at p) is an extension of an elliptic curve by a torus. Then, for every prime $\ell \neq p$ with $\ell \nmid \Phi(p)$ (number of connected components of $\tilde{A}_p$), G_ℓ contains a transvection.*

Proposition 5.7 *If $G \subset \mathrm{Sp}(4, \mathbb{F}_\ell)$ is a proper maximal subgroup containing a transvection, all its elements have reducible (over $\mathbb{F}_\ell$) characteristic polynomial. Therefore, a transvection together with a matrix with irreducible characteristic polynomial generate $\mathrm{Sp}(4, \mathbb{F}_\ell)$.*

Remark: We can also find in [Mi 14] the list of maximal subgroups of $\mathrm{PSp}(4, \mathbb{F}_\ell)$ containing central elations, and a central elation is the image in $\mathrm{PSp}(4, \mathbb{F}_\ell)$ of a transvection in $\mathrm{Sp}(4, \mathbb{F}_\ell)$. These groups correspond to cases 1) and 3) in section 2.1 or to a group having an invariant line of the complex, defined over $\mathbb{F}_\ell$.
Recall that $Pol_q(x)$ denotes the characteristic polynomial of $\rho_\ell(\mathrm{Frob}\ q)$ for any prime q of good reduction for the abelian surface A and $\ell \neq p$. From the two previous results it follows:

Theorem 5.8 *(Le Duff) Let p be a bad reduction prime verifying the condition of proposition 5.6 and q a prime with $Pol_q(x)$ irreducible, then for every $\ell \nmid 2pq\Phi(p)$ such that $Pol_q(x)$ is irreducible modulo ℓ, $G_\ell = \mathrm{GSp}(4, \mathbb{F}_\ell)$.*
If Δ_q is the discriminant of $Pol_q(x)$ and Δ_{Q_q} the discriminant of $Q_q(x) := x^2 - a_q x + b_q - 2q$ the irreducibility condition reads:
$(\frac{\Delta_q}{\ell}) = -1$ *and* $(\frac{\Delta_{Q_q}}{\ell}) = -1$.

EXAMPLE (Le Duff): Take the genus 2 curve:

$$C_2 : \quad y^2 = x^5 - x + 1.$$

$A_2 = J(C_2)$ has good reduction outside $2, 19, 151$. For $p = 19, 151$ the condition in proposition 5.6 is satisfied with $\Phi(p) = 1$.
Take $q = 3$, $Pol_3(x)$ is irreducible and theorem 5.8 gives: $G_\ell = \mathrm{GSp}(4, \mathbb{F}_\ell)$ for every $\ell > 3$ with $(\frac{61}{\ell}) = -1$ and $(\frac{5}{\ell}) = -1$.
Remark: Of course, considering more irreducible characteristic polynomials one can obtain the same result for other primes. In particular, $G_\ell = \mathrm{GSp}(4, \mathbb{F}_\ell)$ for $\ell = 19, 151$ (cf. [LeD 98]).
Remark: The example in the previous section also verifies Le Duff's condition.

Let us apply our method to this example. The invariants are:
$c = \mathrm{cond}(A_2) \mid 2^8 \cdot 19 \cdot 151$ (computed with Liu's algorithm), then $\mathrm{cond}(\varepsilon) \mid d = 16$; and the set $S = \{256, 604, 608\}$.
In this example, we only have to worry about those maximal subgroups in Mitchell's classification containing central elations. Therefore, we only have to discard the maximal subgroups considered in sections 3.1, 3.3 and 3.4.

• The reducible case with 1-dimensional constituent is easily handled using the characteristic polynomials (see section 6) $Pol_p(x)$ for $p = 17, 97$ and we conclude that no prime $\ell > 2$ falls in this case.
• Due to the fact that the spaces of modular forms $S_2(t)$ for $t \in S$ are rather large, we decided to save computations and to apply the procedure described in section 3.3, formula (3.8), only to the prime $p = 3$. After computing all resultants of $Pol_3(x)$ with all the characteristic polynomials $Pol_{f,3}(x)$ for $f \in S_2(t)$, $t \in S$, we find the possibly exceptional primes $\ell > 2$:

$$\ell = 3, 5, 11, 19, 29, 31, 41, 61, 109, 151.$$

Having computed the characteristic polynomials

$$Pol_p(x) \quad \text{for} \quad p = 11, 41, 79, 101, 199, 211$$

(see section 6) we checked that for each of the ten possibly exceptional primes ℓ listed above one of these six polynomials is irreducible modulo ℓ. Then, applying theorem 5.8, we conclude that none of these primes is exceptional. Thus, no $\ell > 2$ has reducible image.

• Cases governed by a quadratic character: we have to consider all possible quadratic characters ϕ unramified outside c and for each of them take a couple of primes p with $\phi(p) = -1$ and $a_p \neq 0$. We use the values a_p for $p = 3, 5, 97, 257$ (see section 6) and an application of the algorithm (formula (3.9)) proves that the only possibly exceptional primes $\ell > 2$ are:

$$\ell = 3, 5, 11, 97, 257.$$

We already mentioned that 3, 5 and 11 are not exceptional. Applying theorem 5.8 again we see that 97 and 257 are also non-exceptional because $Pol_{11}(x)$ is irreducible modulo 97 and $Pol_{281}(x)$ is irreducible modulo 257. Then, we conclude:

Theorem 5.9 *Assume Serre's conjecture (3.2.4?) (cf. [Se 87]). Then the images of the Galois representations on the ℓ-division points of A_2 are*

$$G_\ell = \mathrm{GSp}(4, \mathbb{F}_\ell), \quad \textit{for every } \ell > 2.$$

Remark: $\bar{\rho}_2$ is also irreducible over $\mathbb{F}_2$. This irreducibility for all ℓ is equivalent to the fact that A_2 is isolated in its isogeny class in the sense that any abelian variety isogenous to A_2 over $\mathbb{Q}$ is isomorphic to A_2 over $\mathbb{Q}$. Unfortunately, this condition of being isolated is not effectively verifiable.

Among the maximal proper subgroups containing central elations, we have used Serre's conjecture only to eliminate the following one:

$$G_\ell \subseteq \{A \times B \in \mathrm{GL}(2, \mathbb{F}_\ell) \times \mathrm{GL}(2, \mathbb{F}_\ell) : \det(A) = \det(B) = \chi\}. \qquad (*)$$

Take q with $Pol_q(x)$ irreducible. If $(\frac{\Delta_{Q_q}}{\ell}) = -1$ case (*) cannot hold, because the matrices A and B would have their traces in $\mathbb{F}_{\ell^2} \smallsetminus \mathbb{F}_\ell$. This follows from the factorization:

$$Pol_q(x) = \Big(x^2 - (\frac{a_q + \sqrt{\Delta_{Q_q}}}{2})x + q\Big)\Big(x^2 - (\frac{a_q - \sqrt{\Delta_{Q_q}}}{2})x + q\Big).$$

Then, again using $Pol_3(x)$ we prove without using Serre's conjecture the following

Theorem 5.10 *The images of the Galois representations on the ℓ-division points of A_2 are*

$$G_\ell = \mathrm{GSp}(4, \mathbb{F}_\ell), \quad \textit{for every} \quad \ell > 3 \quad \textit{with} \quad \left(\frac{5}{\ell}\right) = -1.$$

Observe that we have obtained an unconditional result that is stronger than the one in [LeD 98], because it only uses the condition on one of the discriminants (thus, it applies to more primes).
We warn the reader that there is a mistake in [LeD 98], pag. 521, the polynomial Pol_{11} corresponding to this example is wrongly computed. It should read:

$$x^4 + 7x^3 + 31x^2 + 77x + 121.$$

5.5.2 Unconditional results in the general case

We will show now that even in the case that the condition of proposition 5.6 is not verified at any prime, we can obtain similar unconditional results.
In an arbitrary example, if we do not use Serre's conjecture, there is another case to consider (in addition to case (*)):

$$G_\ell \subseteq \{M \in \mathrm{GL}(2, \mathbb{F}_{\ell^2}) : \det(M) = \chi\}. \quad (**)$$

The inclusion of this group in $\mathrm{GSp}(4, \mathbb{F}_\ell)$ is given by the map:
$M \to \mathrm{diag}(M, M^{\mathrm{Frob}})$, where Frob is the non-trivial element in $\mathrm{Gal}(\mathbb{F}_{\ell^2}/\mathbb{F}_\ell)$.
Two tricks allow us to discard this case:

i) Suppose that for a prime q, $Pol_q(x)$ decomposes over $\mathbb{Q}$ as follows:

$$Pol_q(x) = (x^2 + Ax + q)(x^2 + Bx + q), \quad A \neq B.$$

Then case (**) cannot hold if $\ell \nmid B - A$ and $\ell \neq q$.

ii) Suppose that $p^{2k+1} \parallel \mathrm{cond}(A)$, then for every $\ell \nmid p\Phi(p)$, case (**) cannot hold. The condition on ℓ is imposed to ensure that for these ℓ $p^{2k+1} \parallel \mathrm{cond}(\bar{\rho}_\ell)$ also holds.

EXAMPLE (Smart): The following curve is taken from the list given in [Sm 97] of all genus 2 curves defined over $\mathbb{Q}$ with good reduction away from 2:

$$C_3: \quad y^2 = x(x^4 + 32x^3 + 336x^2 + 1152x - 64),$$

$A_3 = J(C_3)$, $c \mid 2^{20}$ (this is the uniform bound for the 2-part of the conductor of abelian surfaces over $\mathbb{Q}$, cf. [B-K 94]). Le Duff's method cannot be applied to this example; the condition of proposition 5.6 is not verified at 2.
We eliminate ALL maximal proper subgroups in Mitchell's classification using the characteristic polynomials $Pol_p(x)$ for several primes p and $\mathrm{cond}(\varepsilon) \mid 1024$, $S = \{1024\}$, with the algorithm described in section 3.
To be more precise, the reducible cases treated in section 3.1 and 3.2 are excluded using the polynomials $Pol_p(x)$ for $p = 3, 17, 19, 31$. Assuming Serre's conjecture, the remaining reducible case is excluded using the polynomials $Pol_p(x)$ for $p = 7, 11, 13$. The cases considered in sections 3.4 and 3.5 are excluded using the polynomials $Pol_p(x)$ for $p = 3, 5$. Finally, with the technique described in section 3.7 we check that $\ell = 5, 7$ are non-exceptional.
All characteristic polynomials used are listed in section 6.
After these computations we find no exceptional primes. Then, we conclude

Theorem 5.11 *Assume Serre's conjecture (3.2.4?) (cf. [Se 87]). Then the images of the Galois representations on the ℓ-division points of A_3 are*

$$G_\ell = \mathrm{GSp}(4, \mathbb{F}_\ell), \quad \textit{for every } \ell > 3.$$

Without Serre's conjecture, trick (i) is used to discard case (**). In fact, $Pol_5(x)$ decomposes as in (i) with $A = -2$ and $B = 0$. The same happens to $Pol_{17}(x)$.
To deal with case (*) we check that $Pol_3(x)$ is irreducible and $\Delta_{Q_3} = 12$ (see section 6). We obtain the unconditional result:

Theorem 5.12 *The images of the Galois representations on the ℓ-division points of A_3 are*

$$G_\ell = \mathrm{GSp}(4, \mathbb{F}_\ell), \quad \textit{for every} \quad \ell > 3 \quad \textit{with} \quad \left(\frac{3}{\ell}\right) = -1.$$

5.5.3 Further examples

In [Le 91], Leprévost gives a genus 2 curve over $\mathbb{Q}(t)$ with 13-rational torsion. For $t = 13$ we obtain:

$$C : \quad y^2 = -4x^5 + 300x^4 - 1404x^3 + 5408x^2 - 8788x + 28561,$$

$A = J(C)$ has $\mathrm{cond}(A) = 2^a \cdot 13^3 \cdot 5^2 \cdot 17^2$. Le Duff's condition is not verified at any prime. We can determine the image as in the previous example, with or without assuming Serre's conjecture (in the "reducible case with 1-dimensional constituent" we find $\ell = 13$ as exceptional prime).
Remark: Here trick (ii) eliminates case (**) for every $\ell \neq 13$ because

$$13^3 \parallel \mathrm{cond}(A) \quad \text{and} \quad \Phi(13) = 13.$$

Brumer and Kramer (unpublished) have given examples of jacobians of genus 2 curves with prime conductor. For them our algorithm determines the image with just a few computations. For instance, when applying Serre's conjecture no computation is necessary because we have $S = \{1\}$ and $S_2(1)$ is empty.
One of these examples is given by the jacobian of the genus two curve:

$$C: \quad y^2 = x(x^2+1)(1729x^3 + 45568x^2 + 25088x - 76832).$$

The conductor of $J(C)$ is 709.

Remark: All the examples of abelian surfaces considered in this chapter verify the condition $\mathrm{End}(A) = \mathbb{Z}$. This follows in particular from our result on the images of the attached Galois representations (the condition on the endomorphism algebra is also necessary for this result to hold).

5.6 Computed characteristic polynomials

We list all the characteristic polynomials $Pol_p(x)$ that have been used in the examples of the abelian surface A in section 4 and the abelian surfaces A_2 and A_3 in section 5.
Recall that in any case the polynomial $Pol_p(x)$ is of the form

$$x^4 - a_p x^3 + b_p x^2 - p a_p x + p^2$$

so it is enough to give the values a_p, b_p.

Abelian surface A (section 4):

p	a_p	b_p
3	-3	6
7	-2	6
11	-4	18
13	-5	16
17	0	22
19	-6	42
97	6	154
113	18	250
229	24	534
257	15	148
569	6	-118
641	12	-266
769	-6	402

Abelian surface $A_2 = J(C_2)$ (section 5.1):

p	a_p	b_p
3	-3	7
5	-5	15
17	-3	16
97	-8	86
257	-11	-113
11	-7	31
41	-7	72
79	7	75
101	-8	-16
199	25	338
211	-17	103
281	1	148

Abelian surface $A_3 = J(C_3)$ (section 5.2):

p	a_p	b_p
3	2	4
5	2	10
7	-2	2
11	-2	12
13	-6	18
17	4	22
19	-2	-4
31	4	46

5.7 Bibliography

[B-K 94]- Brumer, A., Kramer, K., *The conductor of an abelian variety*, Compositio Math. **92** (1994) 227-248

[B-K]- ________, *Non-existence of certain semistable abelian varieties*, preprint

[Bl 17]- Blichfeldt, H., *Finite collineation groups*, (1917) University of Chicago Press

[Di 1901]- Dickson, L., *Canonical forms of quaternary abelian substitutions in an arbitrary Galois field*, Trans. Amer. Math. Soc. **2** (1901) 103-138

[Hi 85]- Hirschfeld, J., *Finite projective spaces of three dimensions*, (1985) Clarendon Press - Oxford

[Le 91]- Leprévost, F., *Famille de courbes de genre* 2 *munies d'une classe de diviseurs rationnels d'ordre* 13, C. R. Acad. Sci. Paris **313** Série I (1991) 451-454

[LeD 98]- Le Duff, P., *Représentations Galoisiennes associées aux points d'ordre ℓ des jacobiennes de certains courbes de genre* 2, Bull. Soc. Math. France **126** (1998) 507-524

[Liu 94]- Liu, Q., *Conducteur et discriminant minimal de courbes de genre* 2, Compositio Math. **94** (1994) 51-79

[Mi 14]- Mitchell, H., *The subgroups of the quaternary abelian linear group*, Trans. Amer. Math. Soc. **15** (1914) 379-396

[Os 77]- Ostrom, T., *Collineation groups whose order is prime to the characteristic*, Math. Z. **156** (1977) 59-71

[Ra 74]- Raynaud, M., *Schémas en groupes de type* $(p, ..., p)$, Bull. Soc. Math. France **102** (1974) 241-280

[Ri 75]- Ribet, K.A., *On ℓ-adic representations attached to modular forms*, Invent. Math. **28** (1975) 245-275

[Ri 85]- ________, *On ℓ-adic representations attached to modular forms II*, Glasgow Math. J. **27** (1985) 185-194

[Ri 97]- ______ , *Images of semistable Galois representations*, Pacific J. of Math. **181** (1997)

[Se 68]- Serre, J.P., *Abelian ℓ-adic representations and elliptic curves*, (1968) Benjamin

[Se 72]- ______ , *Propriétés galoisiennes des points d'ordre fini des courbes elliptiques*, Invent. Math. **15** (1972) 259-331

[Se 86]- ______ , *Oeuvres*, vol. 4, 1-55, Springer-Verlag

[Se 87]- ______ , *Sur les représentations modulaires de degré* 2 *de* $\mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q})$, Duke Math. J. **54** (1987) 179-230

[Sm 97]- Smart, N.P., *S-unit equations, binary forms and curves of genus* 2, Proc. Lond. Math. Soc., III. Ser. 75, No.2, (1997) 271-307

[St]- Stein, W., Hecke: The Modular Forms Calculator, available at: http://shimura.math.berkeley.edu/~was/Tables/hecke.html

Chapter 6

On the images of the Galois representations attached to genus 2 Siegel modular forms

6.1 Introduction

In this chapter we apply the same techniques as in the previous one to study the images of the compatible family of Galois representations attached to genus 2 cuspidal Siegel modular forms on the full Siegel modular group $\mathrm{Sp}(4, \mathbb{Z})$ of even weight k that are Hecke eigenforms. These four dimensional Galois representations have been constructed by Taylor and Weissauer (see [Ta 93], [We 00]).
We will restrict ourselves to the case where the automorphic representation corresponding to the Siegel modular form has multiplicity one. In this case the Galois representations are symplectic (cf. [We 00], [D-K-R 00]).

We will consider explicit examples of such Siegel modular forms whose first Fourier coefficients have been computed by Skoruppa (see [Sk 92], [Sk]) and we will show that the images are "as large as possible" (a certain symplectic group) for almost every prime. The examples of Skoruppa do not correspond to Maass spezialformen (Siegel modular forms in the image of the Saito-Kurokawa lift from $S_{2k-2}(\mathrm{SL}_2(\mathbb{Z}))$), and in addition Eisenstein-Klingen series are excluded. For such cases it is known that the image is not maximal for any prime.

As in the previous chapter, our main tools will be Mitchell's classification

([Mi 14]) of maximal subgroups of $\mathrm{PSp}(4, \mathbb{F}_q)$, this time over an arbitrary finite field; the description of the image of the inertia subgroup I_ℓ, this time due to the work of Faltings (see [Fa 90], [C-F 90] and [Ur 98]) on Hodge-Tate decompositions via an application of Fontaine-Laffaille theory (see [F-L 82]); and Serre's conjecture ($3.2.4_?$) (cf. [Se 87]) for odd irreducible two-dimensional Galois representations. This conjecture will only be needed for an explicit determination of the finite exceptional set, the theoretical result in its stronger form will be independent of it. To obtain explicit results without using Serre's conjecture we proceed as in the previous chapter. Given any characteristic polynomial of Frobenius, we associate to it a certain discriminant d_p such that if this discriminant is not a square then we can compute an infinite set of primes such that the image is "as large as possible" for all the primes in this set.

For one of Skoruppa's examples, in a recent preprint of Dettweiler, Kühn and Reiter ([D-K-R 00]), it is shown that the images are "as large as possible" for an infinite set of primes. To choose the primes, they require different types of decomposition at three characteristic polynomials and in this way they obtain elements that generate the whole symplectic group. In particular, their result only holds for certain primes verifying several restrictions. Applying our method to this example we prove that the images are "as large as possible" for almost every prime and we explicitly give a large density set of primes verifying this.

The resulting algorithm, either with or without assuming Serre's conjecture, is quite similar to the one in the previous chapter. Certain numerical differences are based on the fact that the weights of the action of inertia are different and the conductor of the family of Galois representations is now 1, and principally on the fact that now the representations are defined over fields larger than $\mathbb{Q}_\ell$; this causes some complications as those already faced in chapters 2 and 3. Apart from these numerical differences and other minor changes, the main ideas are the same as in chapter 5. This comparison does not include the results of section 6.

Our main result shows, under the assumption of Serre's conjecture ($3.2.4_?$), that given a genus 2 Siegel cusp form for the full Siegel modular group of even weight, if it has multiplicity one, is not a Maass spezialform and verifies an additional condition (similar to the condition "without inner twists" imposed in chapter 2 to classical modular forms), then the images of the cor-

responding Galois representations are "as large as possible" for almost every prime.
In fact, a stronger statement is proved in the last section using the theory of pseudo-representations: the same result holds independently of Serre's conjecture if we further impose the condition that for some prime p: $\mathbb{Q}(d_p) = E$ and $\sqrt{d_p} \notin E$ where E is the number field generated by the eigenvalues of the Siegel cusp form and d_p is defined in section 4.8.
This condition is verified in the examples. Moreover, the condition is harmless, in the sense that one can easily prove (assuming Serre's conjecture) that this condition will always be satisfied.

6.2 The setup

Let f be a cuspidal weight k Siegel modular form for $\mathrm{Sp}(4, \mathbb{Z})$ which is a Hecke eigenform and denote a_n its eigenvalues.
Let

$$Z_f(s) := \zeta(2s - 2k + 4) \sum_{n=1}^{\infty} \frac{a_n}{n^s}$$

be the spinor zeta function. Then Z_f has an Euler product of the form

$$Z_f(s) = \prod Q_p(p^{-s})^{-1},$$

where Q_p is the polynomial:

$$Q_p(x) = 1 - a_p x + (a_p^2 - a_{p^2} - p^{2k-4})x^2 - a_p p^{2k-3} x^3 + p^{4k-6} x^4.$$

Then we have the following result of Taylor [Ta 93], completed by Weissauer [We 00] (see also [D-K-R 00]):

Theorem 6.1 *Let f be a Siegel modular form of even weight k on the full Siegel modular group $\mathrm{Sp}(4, \mathbb{Z})$ which is a cusp form and a simultaneous eigenform for all Hecke operators $T(n)$. Furthermore, assume that the automorphic representation corresponding to f has mutiplicity one. Let E be the number field generated by the eigenvalues a_n. For any prime number ℓ and any extension λ of ℓ to E there exists a continuous Galois representation*

$$\rho_{f,\lambda} : G_{\mathbb{Q}} \to \mathrm{GSp}(4, \overline{E}_\lambda)$$

such that the following holds: the representation $\rho_{f,\lambda}$ is unramified outside ℓ and

$$\det(Id - x\rho_{f,\lambda}(\text{Frob } p)) = Q_p(x)$$

for every $p \neq \ell$. If $\rho_{f,\lambda}$ is absolutely irreducible, then it is defined over E_λ.

For such an f and under the hypothesis of absolute irreducibility, the maximal possible image for $\rho_{f,\lambda}$ is the group

$$A_\lambda^k = \{g \in \mathrm{GSp}(4, \mathcal{O}_{E_\lambda}) : \det(g) \in (\mathbb{Q}_\ell^*)^{4k-6}\},$$

where $\mathcal{O}_{E_\lambda}$ is the ring of integers of E_λ.
If we consider the residual mod λ Galois representation $\bar{\rho}_{f,\lambda}$ (see the remark below), then its image is contained in

$$\{g \in \mathrm{GSp}(4, \mathbb{F}_\lambda) : \det(g) \in (\mathbb{F}_\ell^*)^{4k-6}\}.$$

The image of its projective image $\mathbb{P}(\bar{\rho}_{f,\lambda})$ is contained in $\mathrm{PSp}(4, \mathbb{F}_\lambda)$, if the residual degree of λ is even, and in $\mathrm{PGSp}(4, \mathbb{F}_\lambda)$ if it is odd (see [D-K-R 00]).

Remark: In these assertions the assumption of absolute irreducibility is not needed (fortunately, because we **want to prove** that the images are large, not to assume it). This follows from the fact that E is the field generated by the coefficients of the characteristic polynomials of the images of the Frobenius elements and from a lemma on the reduction of ℓ-adic representations proved in [D-K-R 00]. This lemma tells us that the mod λ residual representation obtained by reducing the coefficients of all the characteristic polynomials of the images of Frobenius elements "agrees" with the reduction of our λ-adic Galois representation that may not be defined over E_λ; actually it is only thanks to this lemma that we can define the residual mod λ representation in general.
Once we have determined that for a prime ℓ the image of $\bar{\rho}_{f,\lambda}$ is as large as possible, an application of a lemma of Serre (cf. [Se 86] and [D-K-R 00]) implies that the image of $\rho_{f,\lambda}$ is A_λ^k (in this case it is evident that we do need the λ-adic representation to be defined over E_λ, but this follows from its absolute irreducibility which in turn is an immediate consequence of the fact that the residual representation has an image as large as possible).

6.3 The tools

6.3.1 Maximal subgroups of $\mathrm{PGSp}(4, \mathbb{F}_q)$

In [Mi 14], Mitchell gives the following classification of maximal proper subgroups G of $\mathrm{PSp}(4, \mathbb{F}_q)$ where $q = p^r$, p odd prime, as groups of transformations of the projective space having an invariant linear complex:

1) a group having an invariant point and plane
2) a group having an invariant parabolic congruence
3) a group having an invariant hyperbolic congruence
4) a group having an invariant elliptic congruence
5) a group having an invariant quadric
6) a group having an invariant twisted cubic
7) a group G containing a normal elementary abelian subgroup E of order 16, with: $G/E \cong A_5$ or S_5
8) a group G isomorphic to A_6, S_6 or A_7
9) a group conjugated under $\mathrm{PSp}(4, \mathbb{F}_{p^r})$ with $\mathrm{PSp}(4, \mathbb{F}_{p^k})$, where r/k is an odd prime
10) a group conjugated under $\mathrm{PGSp}(4, \mathbb{F}_{p^r})$ with $\mathrm{PGSp}(4, \mathbb{F}_{p^k})$, where r is even and $r/k = 2$

Cases 7) and 8) only occur if $r = 1$.
From this we obtain a classification of maximal proper subgroups H of $\mathrm{PGSp}(4, \mathbb{F}_q)$. It is similar to the one above, except that cases 7) and 8) change according to the relation between H and G, given by the exact sequence:

$$1 \to G \to H \to \{\pm 1\} \to 1.$$

6.3.2 The image of inertia at ℓ

In Weissauer's construction, the representations $\rho_{f,\lambda}$ are realized in the étale cohomology of the Siegel variety X_1 of level 1. Applying results of Faltings and Chai-Faltings (see [Fa 90], [C-F 90]), Urban proves (see [Ur 98]) a result that combined with Fontaine-Laffaille theory (see [F-L 82]) gives:

Proposition 6.2 *Let f be a Siegel cusp form as in theorem 6.1. Then $\rho_{f,\lambda}$ is crystalline and has Hodge-Tate weights $\{2k-3, k-1, k-2, 0\}$. Moreover* *if $\ell - 1 > 2k-3$, then we have the following possibilities for the action of the inertia group at ℓ:*

$$\bar{\rho}_{f,\lambda}|_{I_\ell} \simeq \begin{pmatrix} 1 & * & * & * \\ 0 & \chi^{k-2} & * & * \\ 0 & 0 & \chi^{k-1} & * \\ 0 & 0 & 0 & \chi^{2k-3} \end{pmatrix},$$

$$\begin{pmatrix} \psi^{2k-3} & 0 & * & * \\ 0 & \psi^{(2k-3)\ell} & * & * \\ 0 & 0 & \psi^{(k-2)+(k-1)\ell} & 0 \\ 0 & 0 & 0 & \psi^{(k-1)+(k-2)\ell} \end{pmatrix},$$

$$\begin{pmatrix} \psi^{2k-3} & 0 & * & * \\ 0 & \psi^{(2k-3)\ell} & * & * \\ 0 & 0 & \chi^{k-2} & * \\ 0 & 0 & 0 & \chi^{k-1} \end{pmatrix} \textit{ or}$$

$$\begin{pmatrix} 1 & * & * & * \\ 0 & \chi^{2k-3} & * & * \\ 0 & 0 & \psi^{(k-2)+(k-1)\ell} & 0 \\ 0 & 0 & 0 & \psi^{(k-1)+(k-2)\ell} \end{pmatrix},$$

where ψ denotes a fundamental character of level 2.

6.4 Study of the images

6.4.1 Reducible case: 1-dimensional constituent

Let f be a Siegel cusp form verifying all the conditions of theorem 6.1. Suppose that for a prime λ in E the representation $\bar{\rho}_{f,\lambda}$ is reducible with a 1-dimensional sub(or quotient) representation. The representation being unramified outside ℓ we conclude from proposition 6.2 (assume $\ell > 2k-2$) that this 1-dimensional constituent is: χ^i, $i = 0, k-2, k-1$ or $2k-3$.
As in the previous chapter, we will use the fact that symplectic representations have "reciprocal" roots, i.e., that the roots of the characteristic polynomial of $\rho_{f,\lambda}(\text{Frob } p)$ come in pairs $\alpha, p^{2k-3}/\alpha$.
Remark: We have also used this fact in proposition 6.2 to discard many cases, in particular the cases involving fundamental characters of level 3 or 4.

Therefore we can assume that χ^i is a root of the characteristic polynomial $Pol_p(x)$ of $\bar{\rho}_{f,\lambda}(\text{Frob } p)$

$$Pol_p(x) = x^4 - a_p x^3 + (a_p^2 - a_{p^2} - p^{2k-4})x^2 - a_p p^{2k-3} x + p^{4k-6},$$

for every $p \neq \ell$, with $i = 0$ or $k-1$.

For $i = 0$ we obtain the following congruence:

$$b_p - a_p(p^{2k-3} + 1) + p^{4k-6} + 1 \equiv 0 \pmod{\lambda} \qquad (4.1)$$

for every $p \neq \ell$, where $b_p = a_p^2 - a_{p^2} - p^{2k-4}$ is the quadratic coefficient of $Pol_p(x)$.

Weissauer proved (see [We 94]) that any genus 2 Siegel cusp form that is not in the image of the Saito-Kurokawa lift (and more generally any irreducible cuspidal automorphic representations π of $\mathrm{GSp}(4, \mathbb{A})$ such that π is not Cuspidal Associated to Parabolic and π_∞ is a discrete series representation), i.e., not a Maass spezialform, verifies the generalized Ramanujan conjecture, so the roots of $Pol_p(x)$ have all the same absolute value $\sqrt{p^{2k-3}}$.

From now on we will only work with Siegel cusp forms that are not Maass spezialformen, with the twofold intention of obtaining large images and using Ramanujan's conjecture. This is the case for the examples computed by Skoruppa (cf. [Sk 92], [Sk]), where the Siegel cusp forms that are not Maass spezialformen are called "interesting" (as we will call them).

Therefore, if f is an interesting Siegel cusp form, using the bounds for the absolute values of a_p and b_p that follow from Ramanujan's conjecture we conclude that congruence (4.1) is not an equality (for large enough p). Therefore, it can only hold for finitely many primes ℓ.

Similarly, for $i = k-1$ we obtain the congruence:

$$p^{2k-4}(1 + p^2) - a_p p^{k-2}(1 + p) + b_p \equiv 0 \pmod{\lambda} \qquad (4.2)$$

for every $p \neq \ell$.

Again, Ramanujan's conjecture implies that this is not an equality for large enough p. Thus, the reducible case with 1-dimensional constituent can only hold for finitely many primes.

6.4.2 Reducible case: related 2-dimensional constituents

Suppose that, after semi-simplification, $\bar{\rho}_{f,\lambda}$ decomposes as the sum of two 2-dimensional irreducible Galois representations: $\bar{\rho}_{f,\lambda} \cong \pi_1 \oplus \pi_2$. Assume

also that these two constituents are related, i.e., if α, β are the roots of the characteristic polynomial of $\pi_1(\text{Frob } p)$, then $p^{2k-3}/\alpha, p^{2k-3}/\beta$ are the roots of that of $\pi_2(\text{Frob } p)$. If not, then : $\alpha = p^{2k-3}/\beta$, so $\det(\pi_1) = \det(\pi_2) = \chi^{2k-3}$; this case will be studied in the next subsection.
We apply proposition 6.2 (assume $\ell > 2k-2$). There are two cases to consider:

- Case 1 : $\det(\pi_1) = \chi^{k-1}, \quad \det(\pi_2) = \chi^{3k-5}$.

- Case 2: $\det(\pi_1) = \chi^{k-2}, \quad \det(\pi_2) = \chi^{3k-4}$.

• Case 1: In this case we have the factorization:

$$Pol_p(x) \equiv (x^2 - Ax + p^{3k-5})\,(x^2 - \frac{Ax}{p^{k-2}} + p^{k-1}) \qquad (\text{mod } \lambda).$$

Eliminating A from the equation, we obtain:

$$(b_p - p^{k-1} - p^{3k-5})\,(p^{k-2}+1)^2 - a_p^2\,p^{k-2} \equiv 0 \pmod{\lambda} \qquad (4.3)$$

for every $p \neq \ell$.
From the bounds on the coefficients that follow from Ramanujan's conjecture, we see that for large enough p this is not an equality. Thus, only finitely many ℓ can satisfy (4.3).
• Case 2: This case is quite similar to the previous one. We start with:

$$Pol_p(x) \equiv (x^2 - Ax + p^{3k-4})\,(x^2 - \frac{Ax}{p^{k-1}} + p^{k-2}) \qquad (\text{mod } \lambda).$$

From this:

$$(b_p - p^{k-2} - p^{3k-4})\,(p^{k-1}+1)^2 - a_p^2\,p^{k-1} \equiv 0 \pmod{\lambda} \qquad (4.4)$$

for every $p \neq \ell$.
From the bounds on the coefficients we conclude that for an interesting Siegel cusp form the reducible case with related two-dimensional constituents can only hold for finitely many primes.

6.4.3 The remaining reducible case with Serre's conjecture

As explained above, in the remaining reducible case we have: $\bar{\rho}^{ss}_{f,\lambda} \cong \pi_1 \oplus \pi_2$ with $\det(\pi_1) = \det(\pi_2) = \chi^{2k-3}$. Assume $\ell > 2k-2$. In proposition 6.2 we have given a description of $\bar{\rho}_{f,\lambda}|_{I_\ell}$. This gives for $\pi_1|_{I_\ell}$, $\pi_2|_{I_\ell}$:

$$\begin{pmatrix} 1 & * \\ 0 & \chi^{2k-3} \end{pmatrix} \quad \text{or} \quad \begin{pmatrix} \psi^{2k-3} & 0 \\ 0 & \psi^{(2k-3)\ell} \end{pmatrix}$$

and

$$\begin{pmatrix} \chi^{k-2} & * \\ 0 & \chi^{k-1} \end{pmatrix} \quad \text{or} \quad \begin{pmatrix} \psi^{(k-2)+(k-1)\ell} & 0 \\ 0 & \psi^{(k-1)+(k-2)\ell} \end{pmatrix},$$

respectively. Besides, both two-dimensional representations are unramified outside ℓ. At this point we invoke Serre's conjecture (3.2.4?) (see [Se 87]) that gives us a control on π_1 and $\pi_2' := \chi^{-k+2} \otimes \pi_2$. Both representations should be modular of weights $2k-2$ and 2, respectively, and level 1; i.e., there exist two cusp forms f_1, f_2 with:

$$\bar{\rho}_{f_1,\lambda} \cong \pi_1, \; \bar{\rho}_{f_2,\lambda} \cong \pi_2', \quad f_1 \in S_{2k-2}(1), \; f_2 \in S_2(1)$$

(we are assuming that π_1 and π_2 are irreducible; otherwise the results of section 4.1 apply). Both cusp forms have trivial nebentypus.
But the space $S_2(1)$ is empty and we obtain a contradiction.
We conclude, assuming Serre's conjecture, that the reducible case with unrelated two dimensional constituents cannot happen if $\ell > 2k-2$ for genus two Siegel cusp forms for the full Siegel modular group $\mathrm{Sp}(4,\mathbb{Z})$ verifying the conditions of theorem 6.1.
Remark: In all reducible cases (sections 4.1 , 4.2 and 4.3) we have considered reducibility over $\bar{\mathbb{F}}_\lambda$.

6.4.4 Groups with a reducible index 2 subgroup

If G_λ, the image of $\bar{\rho}_{f,\lambda}$, corresponds to an irreducible subgroup inside (its projective image) some of the maximal subgroups in cases 3), 4) and 5) of Mitchell's classification, there is a normal subgroup of index 2 of G_λ:

$$1 \to M_\lambda \to G_\lambda \to \{\pm 1\} \to 1,$$

where the subgroup M_λ is reducible (not necessarily over $\mathbb{F}_\lambda$).
For $\ell > 2k-2$ we apply the description of $\bar{\rho}_{f,\lambda}|_{I_\ell}$ given in proposition 6.2. Observe that χ^{k-2} has order larger than 2 because $\ell - 1 > 2k-3$, and the order of $\psi^{(k-2)+(k-1)\ell}$ is clearly a multiple of $\ell+1$, therefore larger than 2. Then we conclude that the image of I_ℓ is contained in M_λ.
Therefore, if we take the quotient G_λ/M_λ we obtain a representation

$$G_{\mathbb{Q}} \to C_2$$

whose kernel is a quadratic field unramified everywhere; we thus obtain a contradiction.
We conclude that the image of $\bar{\rho}_{f,\lambda}$ never falls in this case if $\ell > 2k-2$.

6.4.5 The stabilizer of a twisted cubic

In this case all upper-triangular matrices are of the form:

$$\begin{pmatrix} a^3 & * & * & * \\ 0 & a^2d & * & * \\ 0 & 0 & ad^2 & * \\ 0 & 0 & 0 & d^3 \end{pmatrix}.$$

Let us compare this with the four possibilities for the image of the inertia subgroup at ℓ for $\ell > 2k-2$ given in proposition 6.2.
In the first case we see that this inertia subgroup has the required form only if: $\chi^{2k-3} \equiv \chi^{3k-6}$, $\chi^{2k-3} \equiv \chi^{3k-3}$, $\chi^{3k-4} \equiv 1$ or $\chi^{3k-4} \equiv \chi^{6k-9}$. But this implies $\ell - 1 \mid k-3$, $\ell-1 \mid k$, $\ell - 1 \mid 3k-5$ or $\ell - 1 \mid 3k-4$, respectively. With the restriction $\ell > 2k-2$, we see that this is impossible.
In the second case, we see that the inertia subgroup has the required form only if:

$$\psi^{(3k-4)+(3k-5)\ell} \equiv \psi^{6k-9} \text{ or } \psi^{(6k-9)\ell},$$

or

$$\psi^{(2k-3)+(4k-6)\ell} \equiv \psi^{(3k-3)+(3k-6)\ell} \text{ or } \psi^{(3k-6)+(3k-3)\ell}.$$

But this implies $\ell+1 \mid 3k-5$, $\ell+1 \mid 3k-4$, $\ell+1 \mid k$ or $\ell+1 \mid k-3$, respectively. Again, this is impossible for $\ell > 2k-2$.
In the third case, we see that the inertia subgroup has the required form only if:

$$\psi^{(2k-3)(1+2\ell)} \equiv \chi^{3k-6} \text{ or } \chi^{3k-3},$$

or

$$\chi^{3k-4} \equiv \psi^{6k-9} \text{ or } \psi^{(6k-9)\ell}.$$

The first congruence implies $\ell+1 \mid 2k-3$, which is impossible for $\ell > 2k-2$. The second congruence implies:

$$\ell^2 - 1 \mid (-3k+5) + (3k-4)\ell, \qquad (\ddagger)$$

which is impossible for every ℓ because $\ell - 1 \mid (-3k+4) + (3k-4)\ell$.
In the fourth and last case, if the inertia subgroup has the required form then:

$$\psi^{(3k-4)+(3k-5)\ell} \equiv 1 \text{ or } \chi^{6k-9},$$

or

$$\chi^{2k-3} \equiv \psi^{(3k-6)+(3k-3)\ell} \text{ or } \psi^{(3k-3)+(3k-6)\ell}.$$

The first congruence again gives ($\ddagger$).
The second implies $\ell+1 \mid (3k-6)+(3k-3)\ell$, and from this: $\ell+1 \mid 3$.
We conclude that the image does not fall inside the stabilizer of a twisted cubic for any $\ell > 2k-2$.
Remark: We are working with even weight. For the case of weight 3, the image of inertia may fall inside the stabilizer of a twisted cubic.

6.4.6 The exceptional groups

We call exceptional groups those appearing in cases 7) and 8) of the classification. In these cases, comparing the exceptional group $H \subseteq \mathrm{PGSp}(4, \mathbb{F}_\lambda)$ or $G \subseteq \mathrm{PSp}(4, \mathbb{F}_\lambda)$, its order and structure, with the fact that the image of $\mathbb{P}(\bar{\rho}_{f,\lambda})$ contains the image of $\mathbb{P}(\bar{\rho}_{f,\lambda}|_{I_\ell})$, and applying proposition 6.2 (assuming $\ell > 2k-2$) we conclude that these cases can never happen for any $\ell > 2k-2$. If $k < 6$ we have to demand also that $\ell > 7$, but there is no interesting Siegel cusp forms for the full Siegel modular group $\mathrm{Sp}(4, \mathbb{Z})$ of weight smaller than 20.

6.4.7 Smaller symplectic groups

To obtain the maximal possible image we need to impose the following condition:

Definition 6.3 *We say that a genus two Siegel cusp form f is untwisted if there exists a prime p such that $a_p \neq 0$ and $\mathbb{Q}(b_p) = E$, where $b_p = a_p^2 - a_{p^2} - p^{2k-4}$.*

Alternatively, we can ask the number field E to be generated by a_p^2 for some prime p (*), both conditions are enough to exclude for almost every prime the case where the image is in a smaller symplectic group. This second condition is essentially the same as that required in the case of classical modular forms to exclude the case of inner twists.
Suppose that the Siegel cusp form f is untwisted and let p be a prime as in definition 6.3. Let ℓ be a prime different from p such that

$$\ell \nmid \mathrm{Norm}(a_p) \quad \text{and} \quad \ell \nmid \mathrm{disc}(b_p). \qquad (4.5)$$

Let λ be a prime of E lying above ℓ. We will show that for such a λ the projective image of $\bar{\rho}_{f,\lambda}$ cannot fall in a proper symplectic subgroup of $\mathrm{PGSp}(4, \mathbb{F}_\lambda)$, i.e., it cannot be a subgroup as in cases 9) and 10) of the classification.
Assume the contrary. Then, there exists $c \in \mathbb{F}_\lambda^*$ such that the polynomial

$$x^4 - ca_p x^3 + c^2 b_p x^2 - c^3 a_p p^{2k-3} x + c^4 p^{4k-6} \mod \lambda$$

has its coefficients in $\mathbb{F}_{\lambda'}$ with $[\mathbb{F}_\lambda : \mathbb{F}_{\lambda'}] > 1$.
This implies that $\frac{c^3 a_p}{c a_p} = c^2 \in \mathbb{F}_{\lambda'}^*$ (recall that $\ell \nmid \mathrm{Norm}(a_p)$). Thus, $c^2 b_p / c^2 = b_p \in \mathbb{F}_{\lambda'}$, contradicting the assumption that $\mathbb{Q}(b_p) = E$ and $\ell \nmid \mathrm{disc}(b_p)$. This contradiction proves that the image does not fall in a proper symplectic group, if ℓ verifies (4.5).
Remark: In a similar way, one can prove under condition (*) that the image does not fall in a proper symplectic group, for every ℓ such that $\ell \nmid \mathrm{Norm}(a_p)$ and $\ell \nmid \mathrm{disc}(a_p^2)$.

6.4.8 Unconditional results without Serre's conjecture

Without using Serre's conjecture we can show that the images are "as large as possible" for large density sets of primes, applying tricks similar to those used in the previous chapter. For λ a prime in E, let r be its residue class degree: $\mathbb{F}_{\ell^r} = \mathbb{F}_\lambda$. Serre's conjecture was used to eliminate the following two possibilities:

i) The image of $\bar{\rho}_{f,\lambda}$ is contained in

$$\{A \times B \in \mathrm{GL}(2, \mathbb{F}_\lambda) \times \mathrm{GL}(2, \mathbb{F}_\lambda) : \det(A) = \det(B) = \chi^{2k-3}\}. \qquad (4.6)$$

ii) The image of $\bar{\rho}_{f,\lambda}$ is contained in

$$\{M \in \mathrm{GL}(2, \mathbb{F}_{\ell^{2r}}) : \det(M) = \chi^{2k-3}\} \quad (4.7)$$

The inclusion of this group in $\mathrm{GSp}(4, \mathbb{F}_\lambda)$ is given by the map:
$M \to \mathrm{diag}(M, M^{\mathrm{Frob}})$, where Frob is the non-trivial element in $\mathrm{Gal}(\mathbb{F}_{\ell^{2r}}/\mathbb{F}_{\ell^r})$.

• Case i): We will use the standard factorization (see [Sk 92]):

$$Pol_p(x) = (x^2 - (a_p/2 + \sqrt{d_p})x + p^{2k-3})(x^2 - (a_p/2 - \sqrt{d_p})x + p^{2k-3}),$$

where $d_p = -3/4a_p^2 + a_{p^2} + p^{2k-4} + p^{2k-3}$.
We impose the condition:

$$\mathbb{Q}(d_p) = E \quad \text{and} \quad \sqrt{d_p} \notin E. \qquad (4.8)$$

Then, if we restrict to the primes λ in E such that

$$\ell \nmid \mathrm{disc}(d_p) \quad \text{and} \quad d_p \notin (\mathbb{F}_\lambda)^2 \qquad (4.9)$$

case i) cannot hold, because the matrices A and B in (4.6) would have their traces in $\mathbb{F}_{\ell^{2r}} \setminus \mathbb{F}_\lambda$.

• Case ii): Assume $\ell > 2k-2$ and apply proposition 6.2. Because $M = M^{\mathrm{Frob}}$ for any $M \in \mathrm{GL}(2, \mathbb{F}_\lambda)$, if the matrices in the image of inertia were in case ii) it should hold:

$$\{1, \chi^{2k-3}\} = \{\chi^{k-2}, \chi^{k-1}\},$$

$$\{\psi^{2k-3}, \psi^{(2k-3)\ell}\} = \{\psi^{(k-2)+(k-1)\ell}, \psi^{(k-1)+(k-2)\ell}\},$$

$$\{\psi^{2k-3}, \psi^{(2k-3)\ell}\} = \{\chi^{k-2}, \chi^{k-1}\} \text{ or}$$

$$\{1, \chi^{2k-3}\} = \{\psi^{(k-2)+(k-1)\ell}, \psi^{(k-1)+(k-2)\ell}\}.$$

The first of these equalities implies $\ell - 1 \mid k-2$ or $\ell - 1 \mid k-1$. The second implies $\ell + 1 \mid k-2$ or $\ell + 1 \mid k-1$. The third implies $\ell + 1 \mid 2k-3$, and the fourth implies $\ell + 1 \mid (k-2) + (k-1)\ell$, impossible for every ℓ. We conclude that no $\ell > 2k-2$ can verify any of these equalities, so case ii) can never happen for such an ℓ.

6.4.9 Conclusion

Having gone through all cases of the classification (see section 3.1), we conclude that under certain conditions on a Siegel cusp form f the images of the attached Galois representations are "as large as possible" for almost every prime, to be more precise:

Theorem 6.4 *Let f be a Siegel cusp form (and Hecke eigenform) of even weight k for the full Siegel modular group* $\mathrm{Sp}(4, \mathbb{Z})$ *verifying the conditions:*
- *Multiplicity one.*
- *Interesting cusp form (not a Maass spezialform).*
- *Untwisted (see definition 6.3).*

Assume Serre's conjecture (3.2.4?). *Then the images of the Galois representations $\rho_{f,\lambda}$ are A_λ^k, for almost every λ.*
Without assuming Serre's conjecture, take a prime p such that (4.8) holds. Then for all but finitely many primes verifying (4.9) the image of $\rho_{f,\lambda}$ is A_λ^k.

Remark: We are using the fact (see section 2) that the maximality of the images of $\rho_{f,\lambda}$, $\bar{\rho}_{f,\lambda}$ and $\mathbb{P}(\bar{\rho}_{f,\lambda})$ are equivalent. In section 6 we will prove, without assuming Serre's conjecture, that the above result applies to almost every prime.
The result, with or without the assumption of Serre's conjecture, is effective, and we can compute the exceptional primes given a Siegel cusp form verifying the above conditions.
In fact, assuming Serre's conjecture, all exceptional primes (more exactly, a finite set containing all exceptional primes) are computed using equations (4.1), (4.2), (4.3), (4.4) and (4.5) (this last condition implies in particular that ℓ is unramified in $E/\mathbb{Q}$) applied to more than one $Pol_p(x)$ with the restrictions $\ell > 2k - 2$ and ℓ "not dividing denominators" (see next section).
Without assuming Serre's conjecture, we also compute several d_p such that (4.8) holds and find the finitely many exceptional primes among the primes verifying (4.9) for any of these d_p.

6.5 Examples

We start by applying our method to an example of Skoruppa (see [Sk 92], [Sk]), the example already investigated in [D-K-R 00]. This example consists

of a Siegel Hecke eigenform Υ of weight $k = 28$ for the full Siegel modular group $\mathrm{Sp}(4, \mathbb{Z})$ such that the space spanned by the Galois conjugates of Υ is the complement of the space spanned by the Eisenstein-Klingen series and the Maass spezialformen, so the automorphic representation corresponding to Υ has multiplicity one.
Using the results of [Sk 92] and the tables in [Sk], we can compute the characteristic polynomials $Pol_p(x)$ for $p = 2, 3$ and 5 as in [D-K-R 00].
The field E generated by the eigenvalues of Υ is the cubic field generated by some root α of $x^3 - x^2 - 294086x - 59412960$.
The required Fourier coefficients of Υ are, in terms of α:

$a(1,1,1) = 12171273932394959959617937200\alpha^2 -$
$3002035657179872135332112844312\alpha -$
$70266648287313346458671196175512$

$a(2,2,2) = 1677984573470531610324138952787599750\alpha^2 -$
$414092621616401798555119241378212012691\alpha -$
$34880020443365867172742066190931257658045/2$

$a(3,3,3) = 40528677650362308810917276328829759765008\alpha^2 -$
$9993582071950239096074929506242070406773384\alpha -$
$387701121613685136327008010073629284610690936$

$a(4,4,4) = 235161576926603374184625090654858223519273152\alpha^2 -$
$57970607100638211602375544449739660532651092576\alpha -$
$2600292663047595132144160876702679248518781706064$

$a(5,5,5) = 78394728033906461782765030942313953784960201600\alpha^2 -$
$19381896022485847701310751066183248396173872804800\alpha -$
$623881080184953876774684605318302039569534324591600$

$a(1,1,7) = -52284558237596655158824348611551189871168\alpha^2 +$
$12898733485281936189063574256312016862462752\alpha +$
$148124054844534130486331188574142123721611552$

$a(3,3,7) = -12288329366640591505065134861374984329216565680\alpha^2 +$
$2985012596172125045826302405366210464924189513560\alpha -$
$100353753844574955659177552284091544322106595000840$

$a(1,1,19) = -12288329366640617801983929133125597308410762800\alpha^2+$
$29850125961721349380946661011468966131536669270000\alpha-$
$100353753844571476278158160325640019107500992436200$

From these coefficients, using the formulas in [Sk 92], the first eigenvalues of Υ are computed (see [D-K-R 00]):

$$a_2 = \frac{a(2,2,2)}{a(1,1,1)}, \qquad a_4 = \frac{a(4,4,4)}{a(1,1,1)},$$

$$a_3 = \frac{a(3,3,3)}{a(1,1,1)} + 3^{k-2}, \qquad a_9 = \frac{a_3 \cdot a(3,3,3) - 3\cdot 3^{k-2} a(1,1,7)}{a(1,1,1)} - 3^{2k-3},$$

$$a_5 = \frac{a(5,5,5)}{a(1,1,1)},$$

$$a_{25} = \frac{a_5 \cdot a(5,5,5) - 3\cdot 5^{k-2} a(3,3,7) - 3\cdot 5^{k-2} a(1,1,19)}{a(1,1,1)} - 5^{2k-3}.$$

These values determine all the coefficients of the characteristic polynomials $Pol_p(x)$ for $p = 2,3$ and 5. From now on let us impose $\ell > 2k-2 = 54$.
We compute the exceptional primes falling in a reducible case using formulas (4.1) to (4.4) with $p = 2$ and 3. To do so just take the norm in these equations and discard the primes ℓ dividing the greatest common divisor of the norms obtained for $p = 2$ and 3. In the example we found no exceptional primes $\ell > 54$ at this step.
As a matter of fact, in this and other steps, we have to exclude the "primes dividing denominators" from consideration. These are the primes dividing the denominators of the norm of a_2, a_3, a_5, a_4, a_9 or a_{25}. In the example, they form the set:

$$\mathbb{D} = \{2, 3, 17, 2063, 8841304187, 1646767084367711\}.$$

We use equation (4.5) for $p = 2,3$ to bound the set of exceptional primes falling in a smaller symplectic group (a_2 and a_3 are not zero and $\mathbb{Q}(b_2) = \mathbb{Q}(b_3) = E$). Excluding the primes in $\mathbb{D}$, we know that any such exceptional prime ℓ has to divide the greatest common divisor of the two numbers:

$$\text{numerator}(\text{Norm}(a_p)) \cdot \text{numerator}(\text{disc}(b_p)), \quad p = 2,3.$$

As the only possible exceptional primes we obtain the primes that ramify in E:

$$\mathbb{R} = \{5, 13, 73693, 1418741\}.$$

Therefore, we have the following result:

Theorem 6.5 *Let Υ be the interesting Siegel cusp form of weight 28 computed by Skoruppa. It is untwisted and has multiplicity one. Let $\rho_{\Upsilon,\lambda}$ be the Galois representations attached to Υ constructed by Weissauer. Then, if we assume Serre's conjecture (3.2.4?), it follows that for every $\ell > 53$, $\ell \notin \mathbb{D} \cup \mathbb{R}$ and every λ in E above ℓ the image of $\rho_{\Upsilon,\lambda}$ is A_λ^{28}. In particular, except for the finitely many primes excluded, the groups $\mathrm{PSp}(4, \mathbb{F}_{\ell^r})$, if r is even, and $\mathrm{PGSp}(4, \mathbb{F}_{\ell^r})$, if r is odd, (where r denotes the residual degree of λ) are realized as Galois group over $\mathbb{Q}$, and the corresponding Galois extension only ramifies at ℓ.*

Without assuming Serre's conjecture, we want to obtain an effective unconditional result for the images of the $\rho_{\Upsilon,\lambda}$. With this aim, we compute the values d_p, for $p = 2, 3$ and 5, and check that (4.8) holds for the three of them. Therefore, applying (4.9) three times, we obtain:

Theorem 6.6 *Let Υ, $\rho_{\Upsilon,\lambda}$ be as in theorem 6.5. Then, for every $\ell > 53$, $\ell \notin \mathbb{D} \cup \mathbb{R}$ and every $\lambda \in E$ above ℓ such that:*

$$\ell \nmid \mathrm{disc}(d_p) \quad \textit{and } d_p \notin (\mathbb{F}_\lambda)^2, \quad p = 2, 3, \textit{ or } 5,$$

the image of $\rho_{\Upsilon,\lambda}$ is A_λ^{28} (with the same consequences for inverse Galois theory as in theorem 6.5).

We want to be more explicit, so we restrict the analysis to the primes ℓ inert in $E/\mathbb{Q}$. For such a prime ℓ, it is easy to see that if

$$\ell \nmid \mathrm{disc}(d_p) \quad \text{and} \quad \left(\frac{\mathrm{Norm}(d_p)}{\ell}\right) = -1 \qquad (**)$$

for $p = 2, 3$ or 5, then $d_p \notin (\mathbb{F}_\lambda)^2$.
The set $\mathbb{D}$ contains no inert prime. To check the first of the two conditions above we list the integers Δ_p, numerators of the discriminant of d_p:

$\Delta_2 = 5^3 \cdot 7^2 \cdot 13 \cdot 73693 \cdot 1418741 \cdot$

48576885698746350591043459700524701301949975126789677610603640786299818519723232500912038016984123895424193002103674818405705062406425520337737704285346902101735718157075956768276035576548097003920963315831289531213652091073215562272216550713688430135841336495116523220883603089684220341436561334014570502306047322471941431053089

$\Delta_3 = 5^3 \cdot 7^2 \cdot 11^2 \cdot 13 \cdot 73693 \cdot 1418741$
559357264621318790364651556177669237482714074283947475016992687327468773482658685160598367034438005722967111621154431655242169310373922583203392584465119651604395653370812637462298472000725513536730789850099746672576641037598023643613047599656205566799688836034169040485082874413011207031465947211222156842614479358456512447246874653384760948969193046419808564158249

$\Delta_5 = 5^{31} \cdot 13 \cdot 73693 \cdot 1418741 \cdot$
43744807031018441203335941462176932588434929153120967447618618877707295793639835144845670493167330803577258063753986273636445797056329809918610220735667535266268450539233315550458887118150112621268919876070794562735796547289608280790275289039482920326919453800010156604115437536262795796046188140883603829432040083388429269520452936979552953490869956775852968658928749822517487926511544828954552011843135857941153340882564161

To check the second condition in (**) we first observe that the denominator of $\mathrm{Norm}(d_p)$ is "almost" a square, namely, it is a square for $p = 3$ and 5 and 3 times a square for $p = 2$, and of course it only contains primes in $\mathbb{D}$.
We list the integers $N_p := \mathrm{numerator}(\mathrm{Norm}(d_p))$:

$N_2 = 645214534637358547808360710086380670675443423138510590484678228674772517906904832210240712636277003099833565736201103431$

$N_3 = 900 \cdot 10 \cdot 1081753423635983898627234533153328916279097631985349685565455333246882553191962731954308003625615905500945223116396054099255206206613$

$N_5 = 5^{12} \cdot 113592026279430325934820668839290533489159573387551245635518195436182514659912239166275376600269259425949700260444908857955701026762399296734848049764154997430110934849$

Now we can state a more explicit version of theorem 6.6 for inert primes:

Corollary 6.7 *Keep the notation of the previous two theorems. Let ℓ be a prime inert in $E/\mathbb{Q}$ greater than 53. Let $N_2' = 3 \cdot N_2$, $N_p' = N_p$ for $p = 3, 5$. If ℓ satisfies:*

$$\ell \nmid \Delta_p \quad \textit{and} \quad \left(\frac{N_p'}{\ell}\right) = -1$$

for $p = 2, 3$ or 5, then the image of $\rho_{\Upsilon,\lambda}$ is A_λ^{28}. In particular for such ℓ the groups $\mathrm{PGSp}(4, \mathbb{F}_{\ell^3})$ are realized as Galois groups over $\mathbb{Q}$.

Remark: Heuristically (and a careful application of the Cebotarev density theorem may confirm this fact) we see that the proportion of inert primes verifying this is $\frac{7}{8}$.

For the prime $\ell = 53$, inert in E, the image is proved to be maximal in [D-K-R 00]. Therefore the group $\mathrm{PGSp}(4, \mathbb{F}_{53^3})$ is realized as Galois group over $\mathbb{Q}$ (and this is the only computed inert prime with this property in [D-K-R 00]).
The first primes $\ell > 53$ inert in E are:

$$59, 67, 71, 101, 103, 137, 151, 157, 181, 191, 197.$$

We apply corollary 6.7 and we verify that except for 151, the other ten primes in this list verify the required conditions for some $p \leq 5$. Therefore we obtain the following corollary:

Corollary 6.8 *The groups $\mathrm{PGSp}(4, \mathbb{F}_{\ell^3})$ are Galois groups over $\mathbb{Q}$ for $\ell = 53, 59, 67, 71, 101, 103, 137, 157, 181, 191, 197$.*

6.5.1 The first interesting Siegel cusp form

Now we apply the algorithm to $\Upsilon 20$, the first example of interesting Siegel cusp form for the full Siegel modular group. $\Upsilon 20$ has weight $k = 20$ and rational Fourier coefficients. Its first eigenvalues were computed by Skoruppa in [Sk 92]. The dimension of the space of interesting Siegel cusp forms of weight 20 is 1, therefore $\Upsilon 20$ has multiplicity one.
The first eigenvalues of $\Upsilon 20$ are:

$$a_2 = -840960, \ a_4 = 248256200704,$$

$$a_3 = 346935960, \ a_9 = -452051040393665991,$$

$$a_5 = -5232247240500, \ a_{25} = -94655785156653029446859375,$$

$$a_7 = 2617414076964400, \ a_{49} = -550162995018478094943498331595 1.$$

Applying equation (4.1) with $p = 2$ and 3 we find no exceptional primes at this step.
Applying equation (4.2) with $p = 2, 3$ and 5 we obtain as (possible) exceptional primes $\ell = 2, 3, 5, 7, 11$. According to the results of Skoruppa (cf. [Sk 92]) these primes are in fact exceptional because $\Upsilon 20$ is congruent modulo these ℓ (and only them) to a Maass spezialform, so equation (4.2) holds, for these ℓ, for every p.
Applying equation (4.3) with $p = 2, 3, 5$ and 7, we obtain as (possible) exceptional primes $\ell = 2, 3, 5, 29, 71$.
Recall that with our algorithm we can show non-exceptionality only for primes $\ell > 2k - 2 = 38$. Here we have the first prime $\ell > 37$ in this example seeming to be exceptional: $\ell = 71$. But Kurokawa proved in [Ku 79] that $\Upsilon 20$ is congruent modulo 71 to an Eisenstein-Klingen series, so 71 is in fact exceptional and (4.3) holds, for $\ell = 71$, for every p.
Applying equation (4.4) with $p = 2, 3, 5$ only gives $\ell = 2, 3, 5$ as possible exceptional primes.

This concludes the application of the algorithm to this example, proving in particular that the image of the Galois representations ρ_ℓ attached to $\Upsilon 20$ are "as large as possible" for every $\ell > 71$, under the assumption of Serre's conjecture. To obtain an unconditional result, we use the first values of d_p:
$d_2 = 2^{14} \cdot 3^2 \cdot 7 \cdot 13 \cdot 19 \cdot 241$,
$d_3 = 2^6 \cdot 3^{10} \cdot 19 \cdot 47 \cdot 150628997$,
$d_5 = 2^8 \cdot 3^2 \cdot 5^6 \cdot 19 \cdot 47 \cdot 1396135808326877$,
$d_7 = 2^8 \cdot 3^6 \cdot 7^6 \cdot 29 \cdot 1097 \cdot 41713094306662453$.

Theorem 6.9 *Let $\Upsilon 20$ be the interesting Siegel cusp form of weight 20 computed by Skoruppa. It has multiplicity one and $E = \mathbb{Q}$. Let ρ_ℓ be the Galois representations attached to $\Upsilon 20$ constructed by Weissauer. Then, if we assume Serre's conjecture (3.2.4?) it follows that for every $\ell > 37$, $\ell \neq 71$ the image of ρ_ℓ is A_ℓ^{20}. In particular for every $\ell > 37$, $\ell \neq 71$, the groups $\mathrm{PGSp}(4, \mathbb{F}_\ell)$ are realized as Galois group over $\mathbb{Q}$, and the corresponding Galois extension of $\mathbb{Q}$ only ramifies at ℓ.*

The same conclusion holds unconditionally (without assuming Serre's conjecture) if we also impose $(\frac{d_p}{\ell}) = -1$ *for* $p = 2, 3, 5$ *or* 7.

Remark: In particular, we have proved that the images are "as large as possible" for an explicitly given set of primes of Dirichlet density $\frac{15}{16}$.

6.6 Improving theorem 6.4

6.6.1 Pseudo-representations

We reproduce Wiles' definition of pseudo-representations and some of its properties (cf. [Wi 88], [Ti 94]). This is a tool used to construct odd two-dimensional representations.
Let A be a ring, G a group, and $c \in G$ an element of order two.

Definition 6.10 *A pseudo-representation of* G *defined over* A *is a quadruple* $\tau = (a, d, t, x)$; $a, d, t : G \to A$, $x : G \times G \to A$ *satisfying the conditions:*
(i) $2a_{g \cdot g'} = a_g a_{g'} + x_{g,g'}$, $2d_{g \cdot g'} = d_g d_{g'} + x_{g',g}$
(ii) $a_g = t_g + t_{cg}$, $d_g = t_g - t_{cg}$
(iii) $t_1 = 2$, $t_c = 0$, $x_{g,c} = x_{c,g} = 0$
(iv) $x_{g,g'} x_{h,h'} = x_{g,h'} x_{h,g'}$,
$4x_{gh,g'h'} = a_g a_{h'} x_{h,g'} + a_{h'} d_h x_{g,g'} + a_g d_{g'} x_{h,h'} + d_h d_{g'} x_{g,h'}$.

Define the trace of τ by $\mathrm{trace}(\tau) = t$, and the determinant by
$\det(\tau)(g) = a_g d_g - x_{g,g}$.
Remarks: (i) If G and A have a topology, all maps are assumed to be continuous.
(ii) If $\rho : G \to \mathrm{GL}(2, A)$, $\rho = (\alpha, \beta, \gamma, \delta)$ is a representation defined over A, with $\rho(c) = (1, 0, 0, -1)$ (an odd representation) it gives rise to a pseudo-representation $\tau = (a, d, t, x)$, where $a = 2\alpha$, $d = 2\delta$, $t = \alpha + \delta$, $x_{g,g'} = 4\beta_g \gamma_{g'}$.
(iii) A pseudo-representation is determined by its trace. If $A' \subset A$ is a subring, if τ is defined over A and $\mathrm{trace}(\tau)$ takes values in A', then τ is defined over A'.
The following are two basic properties that we will use in the sequel (cf. [Wi 88], [Ti 94]):

Lemma 6.11 *("patching lemma") Let $(U_i)_{i>0}$ be a sequence of ideals in A such that $\bigcap_i U_i = \{0\}$. For each i, let τ_i be a pseudo-representation defined over A/U_i. Assume that there exist a dense subset Σ of G and a function $T : \Sigma \to A$ such that for any i, $T \bmod U_i = \mathrm{trace}(\tau_i)$. Then, there exists a pseudo-representation τ defined over A such that for any i, $\tau \bmod U_i = \tau_i$.*

Theorem 6.12 *If A is a field of characteristic different from 2, any pseudo-representation τ corresponds to an odd two dimensional representation ρ.*

Next we reproduce Taylor's definition of pseudo-representation (cf. [Ta 91]). It has the advantage that it is useful to construct representations of any dimension.

Definition 6.13 *If G is a group and R is a ring, a pseudo-representation of G over R of dimension d is a map $T : G \to R$ such that:*
(i) $T(1) = d$
(ii) $T(g_1g_2) = T(g_2g_1)$
(iii) $\sum_{\sigma \in S_{d+1}} \mathrm{sign}(\sigma) T_\sigma(g_1, ..., g_{d+1}) = 0$.
Here S_{d+1} denotes the symmetric group on $d+1$ letters and $T_\sigma : G^{d+1} \to R$ is the function

$$(g_1, ..., g_r) \to T(g^{(1)}_{i_1} ... g^{(1)}_{i_{r_1}}) T(g^{(2)}_{i_1} ... g^{(2)}_{i_{r_2}}) T(g^{(s)}_{i_1} ... g^{(s)}_{i_{r_s}})$$

where σ has cycle decomposition

$$(i^{(1)}_1 ... i^{(1)}_{r_1})(i^{(2)}_1 ... i^{(2)}_{r_2}) ... (i^{(s)}_1 ... i^{(s)}_{r_s}).$$

Note that by property (ii), T_σ is well defined.
To conclude, we state the main properties of d-dimensional pseudo- representations (cf. [Ta 91]).

Lemma 6.14 1. *If $\phi : R \to S$ is a ring homomorphism and $T : G \to R$ is a pseudo-representation then $\phi \circ T$ is a pseudo-representation of the same dimension.*
2. *If $T : G \to R$, if d is a positive integer, if I is an index set, and if for each $i \in I$, $\phi_i : R \to S_i$ is a ring homomorphism such that $\phi_i \circ T$ is a pseudo-representation of dimension d and $\cap_I \ker \phi_i = \{0\}$, then T is a pseudo-representation of dimension d.*

The second property of this lemma generalizes lemma 6.11. Observe that in the case where I is a singleton and ϕ_i an inclusion, it says that we can always restrict the ring of definition to the minimal ring containing the image of T (compare with remark (iii) after definition 6.10).

Theorem 6.15 1. *If R is a ring and $\rho : G \to \mathrm{GL}(d, R)$ a representation, then* $\operatorname{trace}(\rho)$ *is a pseudo-representation of dimension d.*
2. *If R is an algebraically closed field of characteristic* 0 *and $T : G \to R$ is a pseudo-representation of dimension d, then there is a true semisimple representation $\rho : G \to \mathrm{GL}(d, R)$ with* $\operatorname{trace} \rho = T$, *and ρ is unique up to conjugation.*
3. *If G and R have a topology, the above results remain true with continuous pseudo-representations and continuous representations.*

6.6.2 Compatibility

First we want to prove a result about the compatibility of the images of Frobenius elements. Consider a compatible family of Galois representations:

$$\rho_\lambda : G_{\mathbb{Q}} \to \mathrm{GSp}(4, \overline{K}_\lambda),$$

where K is a number field and λ a prime in K. Assume that each ρ_λ is unramified outside $\ell = \ell(\lambda)$ and that $\operatorname{trace}(\rho_\lambda(\mathrm{Frob}\ p)) \in K$ for every λ, p with $p \neq \ell$.
Take $\rho_{\lambda_1}, \rho_{\lambda_2}$, for λ_1, λ_2 primes in K with $\lambda_1 \mid \ell_1$, $\lambda_2 \mid \ell_2$, $\ell_1 \neq \ell_2$ rational primes. We consider the subgroup W of $G_{\mathbb{Q}}$ algebraically (not topologically) generated by the set $\{\mathrm{Frob}\ p\}_{p \neq \ell_1, \ell_2}$.
Remark: In fact, as both representations $\rho_{\lambda_1}, \rho_{\lambda_2}$ are unramified outside $\ell_1 \cdot \ell_2$, we can see them as representations of $G^{\ell_1 \cdot \ell_2}$, the quotient of $G_{\mathbb{Q}}$ corresponding to the maximal extension of $\mathbb{Q}$ unramified outside $\ell_1 \cdot \ell_2$. W must be thought of as a subgroup of $G^{\ell_1 \cdot \ell_2}$.
Restricting the representations ρ_{λ_i} $(i = 1, 2)$ to W, we obtain two representations of W: $\rho_i = \rho_{\lambda_i}|_W$ $(i = 1, 2)$ such that:

$$\rho_i : W \to \mathrm{GSp}(4, \overline{K}_{\lambda_i}), \qquad i = 1, 2,$$

with $\operatorname{trace}(\rho_1(\mathrm{Frob}\ p)) = \operatorname{trace}(\rho_2(\mathrm{Frob}\ p)) \in K$, for every $p \neq \ell_1, \ell_2$. Let $\tilde{\rho}_i$ be the pseudo-representation corresponding to ρ_i, $i = 1, 2$. Then, $\tilde{\rho}_1 = \tilde{\rho}_2$ as

pseudo-representations of W with values in K.
Applying theorem 6.15 we see that there is a semisimple representation

$$\rho : W \to \mathrm{GL}(4, \overline{K})$$

with trace ρ = trace ρ_1 = trace ρ_2, and ρ is unique up to conjugation. Therefore, the representations ρ, ρ_1^{ss} are $\overline{K}_{\lambda_1}$ conjugated, and similarly ρ, ρ_2^{ss} are $\overline{K}_{\lambda_2}$ conjugated.
We conclude that there are matrices $\mu_i \in \mathrm{GL}(4, \overline{K}_{\lambda_i})$ $(i = 1, 2)$ such that for every $p \neq \ell_1, \ell_2$:

$$\mu_i \rho_{\lambda_i}^{ss}(\mathrm{Frob}\ p)\mu_i^{-1} = \rho(\mathrm{Frob}\ p).$$

This equation is a compatibility constraint between ρ_{λ_1} and ρ_{λ_2} that implies the following proposition in the case of reducible residual representations:

Proposition 6.16 *Let $\{\rho_\lambda\}_\lambda$ be a compatible family of Galois representations*

$$\rho_\lambda : G_{\mathbb{Q}} \to \mathrm{GSp}(4, \overline{K}_\lambda)$$

where K is a number field, $\mathrm{trace}(\rho_\lambda(\mathrm{Frob}\ p)) \in K$ *for every λ, p with $p \neq \ell$, the conductor of the family of representations is* 1 *and* $\det(\rho_\lambda) = \chi^{2\theta}$, *with $\theta \in \mathbb{Z}$.*
Suppose that for primes $\lambda_1, \lambda_2 \in K$ the representations $\bar{\rho}_{\lambda_i}$, $i = 1, 2$, are reducible of the form:

$$\bar{\rho}_{\lambda_i}^{ss} = \sigma_i \oplus \pi_i,$$

where σ_i, π_i are two-dimensional representations with $\det(\sigma_i) = \det(\pi_i) = \chi^\theta$, *for $i = 1, 2$.*
Let p_1, p_2 be two rational primes different from ℓ_1, ℓ_2. Let

$$\{\alpha_j, p^\theta/\alpha_j, \beta_j, p^\theta/\beta_j\}$$

be the roots of the characteristic polynomial of $\rho_{\lambda_i}(\mathrm{Frob}\ p_j)$ *(they do not depend on i) for $j = 1, 2$. Suppose that reducing modulo λ_1:*
$\{\alpha_j, p^\theta/\alpha_j\}$ correspond to $\sigma_1(\mathrm{Frob}\ p_j)$ *and $\{\beta_j, p^\theta/\beta_j\}$ correspond to* $\pi_1(\mathrm{Frob}\ p_j)$, *$j = 1, 2$.*
Without loss of generality we may assume that reducing modulo λ_2:
$\{\alpha_1, p^\theta/\alpha_1\}$ correspond to $\sigma_2(\mathrm{Frob}\ p_1)$ *and $\{\beta_1, p^\theta/\beta_1\}$ correspond to* $\pi_2(\mathrm{Frob}\ p_1)$.
Then, it must hold:
$\{\alpha_2, p^\theta/\alpha_2\}$ correspond to $\sigma_2(\mathrm{Frob}\ p_2)$ *and $\{\beta_2, p^\theta/\beta_2\}$ correspond to* $\pi_2(\mathrm{Frob}\ p_2)$.

Remark: "correspond" means that their reduction gives the roots of the corresponding residual representation.

6.6.3 From residual to λ-adic reducibility

Let f be a genus two Siegel cusp form verifying the conditions of theorem 6.4, and consider the Galois representations $\rho_\lambda := \rho_{f,\lambda}$. Suppose that for an infinite set of primes $\{\lambda_i\}_{i=1}^{\infty} = \Lambda$ of E the residual representations $\bar{\rho}_{\lambda_i}$ are reducible of the form described in proposition 6.16. Taking a subset of Λ if necessary, we assume that the density of the set $\mathbb{L}$ of rational primes ℓ_i such that $\lambda_i \mid \ell_i$ is 0.
We want to prove that with this hypothesis of residual reducibility the whole family of λ-adic representations ρ_λ has to be reducible (and a fortiori residually reducible). We know from proposition 6.16 that the decompositions:

$$\bar{\rho}_{\lambda_i}^{ss} = \sigma_i \oplus \pi_i$$

induce a decomposition on the set $\{a_p\}$ of traces of the family ρ_λ: $a_p = u_p + v_p$ for every $p \notin \mathbb{L}$ that is independent of λ_i. That is to say, there exists such a decomposition (fixed) with $\{u_p \bmod \lambda_i\}$ equal to the set of traces of σ_i (restricted to $p \notin \mathbb{L}$) and $\{v_p \bmod \lambda_i\}$ equal to the set of traces of π_i (restricted to $p \notin \mathbb{L}$), for every $\lambda_i \in \Lambda$.
Fix a prime λ of E. As usual, let ℓ be the rational prime such that $\lambda \mid \ell$.
For any set S of rational primes let us denote by $\mathbb{Q}^S$ the maximal extension of $\mathbb{Q}$ unramified outside S and $G^S = \mathrm{Gal}(\mathbb{Q}^S/\mathbb{Q})$. We will work only with Galois representations unramified outside $\mathbb{L} + \ell := \mathbb{L} \bigcup \{\ell\}$, therefore we take the quotient $G^{\mathbb{L}+\ell}$ of $G_{\mathbb{Q}}$ and work with representations of this quotient group.
Consider the subgroup W_λ of $G^{\mathbb{L}+\ell}$ algebraically generated by the elements $\{\mathrm{Frob}\ p\}_{p \notin \mathbb{L}+\ell}$.
Let us consider the function $F : W_\lambda \to \overline{\mathbb{Q}}$ defined on the generators of W_λ by: $F(\mathrm{Frob}\ p) = u_p$ and extended to all W_λ by setting: $F(\omega_1\omega_2) = F(\omega_1)F(\omega_2)$.

Recall that the traces a_p of ρ_λ are the eigenvalues of the Siegel cusp form f. They generate the number field E. The decomposition of the characteristic polynomials Pol_p introduced in section 4.8 shows that it must hold:

$u_p = a_p/2 \pm \sqrt{d_p}$, so we have:

$$E' := \mathbb{Q}(\{u_p\}) = E(\{\sqrt{d_p}\}).$$

Moreover, from the definition of d_p (see section 4.8) and standard properties of the eigenvalues of f it is known that all a_p and a_{p^2} belong to $\mathcal{O}_E[\frac{1}{N}]$ where N is a finite product of primes and all u_p belongs to $\mathcal{O}' := \mathcal{O}_{E'}[\frac{1}{2N}]$, where $\mathcal{O}_X$ denotes "ring of algebraic integers of X".

Therefore, the image of F is inside $\mathcal{O}'$:

$$F : W_\lambda \to \mathcal{O}'. \qquad (6.1)$$

For each $\lambda_i \in \Lambda$ we take a prime λ_i' of E' above λ_i. Composing the function F with the reduction modulo λ_i' for every $\lambda_i \in \Lambda$ gives the functions:

$$F_{\lambda_i'} : W_\lambda \to \mathbb{F}_{\lambda_i'}$$

with $F_{\lambda_i'}(\text{Frob } p) = u_p \bmod \lambda_i'$, for every $p \notin \mathbb{L} + \ell$. This is the restriction to W_λ of the pseudo-representation $\tilde{\sigma}_i$ associated to σ_i , therefore $F_{\lambda_i'}$ is a 2-dimensional pseudo-representation of W_λ for every $\lambda_i \in \Lambda$.
Remark: For every λ_i, σ_i gives a representation of $G^{\mathbb{L}+\ell}$ because it is unramified outside ℓ_i.
Now we apply the patching lemma (see lemma 6.11) and we conclude that F as in (6.1) is a 2-dimensional pseudo-representation. We have already seen (see for example section 4.3) that the representations σ_i have to be odd. An application of theorem 6.12 proves that there exists a representation

$$\sigma : W_\lambda \to \mathrm{GL}(2, E')$$

with trace $\sigma = F$, i.e.,

$$\mathrm{trace}(\sigma(\text{Frob } p)) = u_p$$

for every $p \notin \mathbb{L} + \ell$.
The same argument shows that by patching the representations π_i we construct a representation:

$$\pi : W_\lambda \to \mathrm{GL}(2, E')$$

with

$$\mathrm{trace}(\pi(\text{Frob } p)) = v_p$$

for every $p \notin \mathbb{L} + \ell$.
Now let us compare the semisimplification $(\rho_\lambda|_{W_\lambda})^{ss}$ with $\sigma \oplus \pi$, as representations of W_λ with image in $\mathrm{GSp}(4, \overline{E})$.
Remark: ρ_λ gives a representation of $G^{\mathbb{L}+\ell}$ and W_λ because it is unramified outside ℓ.
Both representations have the same trace at every element of W_λ, so they are conjugated. We conclude that $\rho_\lambda|_{W_\lambda}$ is reducible for every λ.
But the Cebotarev density theorem implies that the subgroup W_λ is dense in $G^{\mathbb{L}+\ell}$, because $\mathbb{L}$ has density 0. Therefore, being continuous, the representation ρ_λ has to be reducible for every prime λ of E, of the form

$$\rho_{f,\lambda}^{ss} = \sigma_\lambda \oplus \pi_\lambda$$

with $\det(\sigma_\lambda) = \det(\pi_\lambda) = \chi^{2k-3}$.

6.6.4 The result

Theorem 6.17 *Let f be a genus 2 Siegel cusp form verifying the conditions of theorem 6.4. Let $\rho_{f,\lambda}$ be the corresponding family of Galois representations. Suppose that the residual representations $\bar{\rho}_{f,\lambda_i}$ are reducible for infinitely many primes λ_i of E. Then, for every prime λ the λ-adic representation $\rho_{f,\lambda}$ is reducible.*

Remark: We do not need to specify the type of reducibility of the representations $\bar{\rho}_{f,\lambda_i}$ because we know from the results of section 4 that for almost all these primes there is just one possibility.

Let f be a Siegel cusp form verifying the conditions of theorem 6.4. Assume that we are in the situation of theorem 6.17. Then we have: $\rho_{f,\lambda}^{ss} = \sigma_\lambda \oplus \pi_\lambda$ for every λ, with $\det(\sigma_\lambda) = \det(\pi_\lambda) = \chi^{2k-3}$. Suppose that condition (4.8) is verified by some prime p. As was shown in section 4.8, this implies that for infinitely many λ with

$$\ell \nmid \mathrm{disc}(d_p) \quad \text{and} \quad d_p \notin (\mathbb{F}_\lambda)^2$$

the representation $\bar{\rho}_{f,\lambda}$ cannot be reducible. Thus we obtain a contradiction with theorem 6.17.
Combining this with the results of section 4 we conclude:

Theorem 6.18 *Let f be a genus 2 Siegel cusp form and Hecke eigenform of even weight k for the Siegel modular group $\mathrm{Sp}(4,\mathbb{Z})$ with multiplicity one, untwisted and not a Maass spezialform.*
Suppose that there is a prime p with $\mathbb{Q}(d_p) = E$ and $\sqrt{d_p} \notin E$. Then the image of the Galois representation $\rho_{f,\lambda}$ is A_λ^k for almost every λ.

This result applies in particular to the examples considered in the previous section, so we have

Corollary 6.19 *If f is an interesting genus 2 Siegel cusp form of weight $k = 20$ or 28, then the images of the Galois representations $\rho_{f,\lambda}$ are "as large as possible", i.e., A_λ^k, for almost every λ.*

6.7 Bibliography

[C-F 90]- Chai, C., Faltings, G., *Degeneration of Abelian Varieties*, (1990) Springer-Verlag

[D-K-R 00]- Dettweiler, M., Kühn, U., Reiter, S., *On Galois representations via Siegel modular forms of genus* 2, (2000) preprint

[Fa 90]- Faltings, G., *Crystalline cohomology and Galois representations*, in Algebraic Analysis, Geometry and Number Theory, Proceedings of JAMI Inaugural Conference, (1990) John Hopkins Univ. Press

[F-L 82]- Fontaine, J.M., Laffaille, G., *Construction de représentations p-adiques*, Ann. Scient. Éc. Norm. Sup., 4^e série, t. **15** (1982) 547-608

[Ku 79]- Kurokawa, N., *Congruences between Siegel Modular Forms of Degree Two*, Proc. Japan Acad. **55**, Ser. A (1979) 417-422

[Mi 14]- Mitchell, H., *The subgroups of the quaternary abelian linear group*, Trans. Amer. Math. Soc. **15** (1914) 379-396

[Se 86]- Serre, J.P., *Oeuvres*, vol. 4, 1-55, Springer-Verlag

[Se 87]- Serre, J.P., *Sur les représentations modulaires de degré* 2 *de* $\mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q})$, Duke Math. J. **54** (1987) 179-230

[Sk 92]- Skoruppa, N., *Computations of Siegel modular forms of genus two*, Math. Computation **58** (1992) 381-398

[Sk]- Skoruppa, N., *Siegel modular eigenforms of even weight on the full Siegel modular group of genus* 2, available at: http://thor.math.u-bordeaux.fr/~modi

[Ta 91]- Taylor, R., *Galois representations associated to Siegel modular forms of low weight*, Duke Math. J. **63** (1991) 281-332

[Ta 93]- Taylor, R., *On the ℓ-adic cohomology of Siegel threefolds*, Invent. Math. **114** (1993) 289-310

[Ti 94]- Tilouine, J., *Galois representations congruent to those coming from Shimura Varieties*, Proc. Sympos. Pure Math. **55** Part 2 (1994) 625-638

[Ur 98]- Urban, E., *Selmer groups and the Eisenstein-Klingen Ideal*, preprint (1998)

[We 94]- Weissauer, R., *The Ramanujan Conjecture for genus two Siegel modular forms (An application of the Trace Formula)*, preprint (1994)

[We 00]- Weissauer, R., *Four dimensional Galois representations*, preprint (2000)

[Wi 88]- Wiles, A., *On nearly ordinary λ-adic representation associated to modular forms*, Invent. Math. **94** (1988) 529-573