REALIZATION OVER $\mathbb{Q}$ OF THE GROUPS $\widetilde{A}_5$ AND $\widehat{A}_5$

A. JEHANNE

1. Introduction

Let $\widetilde{A}_5$ and $\widehat{A}_5$ be respectively the only non trivial central extension of A_5 by the cyclic group C_2 of order 2 and the cyclic group C_4 of order 4. These groups can be described as groups of matrices. The group $\widetilde{A}_5$ is isomorphic to $\mathrm{Sl}_2(\mathbb{F}_5)$ and the group $\widehat{A}_5$ to $\{x \in \mathrm{GL}_2(\mathbb{F}_5) \ : \ \det(x) = \pm 1\}$. In this paper, we give an algorithm to construct some $\widetilde{A}_5$ and $\widehat{A}_5$-extensions of $\mathbb{Q}$, given as the splitting fields of polynomials of degree 24. Let us mention that a different approach to this problem has been developed by T. Crespo in [C1] and [C2]. In the last section, we compute the first coefficients of the L-functions of the irreducible 2-dimensional complex representations corresponding to these extensions. One can find tables for such L-functions on the internet at *http:www//math.u-bordeaux.fr/˜jehanne/*.

The results that we describe here take place in the theory of the complex Galois two-dimensional representations (see [F1], §4). For odd 2-dimensional representations, Artin's conjecture has been proved for infinitely many cases (see theorem 1.1) by K. Buzzard, M. Dickinson, N. Shepherd-Barron and R. Taylor ([B-D-SB-T]), and more recently by R. Taylor in [Ta2] (we say that a complex Galois representation ρ is even (resp. odd) if $\det(\rho)(c) = 1$ (resp. -1), where c is the complex conjugation). Hence our algorithm gives an efficient way to compute many modular forms of weight one corresponding to icosahedral representations (see [D-S]). Finally , it can be used for computing bases for spaces of modular forms of weight one. Moreover, in [J-M], a joint work with M. Müller, we use these constructions for giving a new experimental evidence of Artin's conjecture, in an unproved case of odd 2-dimensional representations. Even representations are more mysterious; we intend in another work to use our constructions for experimental comparisons between L-functions of icosahedral representations with Maaß forms.

Consider an irreducible Galois representation

$$\rho \ : \ G_{\mathbb{Q}} \longrightarrow \mathrm{GL}_2(\mathbb{C})$$

and the induced projective representation

$$\overline{\rho} \ : \ G_{\mathbb{Q}} \longrightarrow \mathrm{PGL}_2(\mathbb{C}),$$

where $\overline{\mathbb{Q}}$ is an algebraic closure of $\mathbb{Q}$ and where $G_{\mathbb{Q}}$ is the absolute Galois group $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$. All Galois representations and projective representations considered in this paper will be continuous. Since $\mathrm{Im}(\overline{\rho})$ is finite, it is isomorphic to a dihedral group D_n, or to one of the groups A_4, A_5 or S_4 (the alternating group on four or five letters, and the symmetric group on four letters). Recall that a representation ρ is said icosahedral if $\mathrm{Im}(\overline{\rho}) \simeq A_5$.

It is known that if $\mathrm{Im}(\overline{\rho})$ is isomorphic to D_n, A_4 or S_4, then ρ satisfies Artin's conjecture. It was proved by Artin for D_n, Langlands for A_4 ([L]) and Tunnel for S_4 ([Tu]). We recall here the most recent result we know about the icosahedral case ([B-D-SB-T], theorem A).

Theorem 1.1 (Buzzard, Dickinson, Shepherd-Barron, Taylor). *If the group $Im(\overline{\rho})$ is isomorphic to A_5, if ρ is odd, if $\overline{\rho}$ is unramified in 2 and 5, and if the image under $\overline{\rho}$ of the Frobenius element at 2 has order 3, then ρ satisfies Artin's conjecture.*

It is then known by this theorem that the representation of example 1, in section 5 of our paper satisfies Artin's conjecture. For examples 6 and 7, we cannot apply this theorem, because in these cases, the Frobenius element in 2 has order 5. The representation of example 8 satisfies Artin's conjecture: this was proved by J. Buhler in [B]. The other examples of this paper treat even representations.

¿From now on, we suppose that $\mathrm{Im}(\overline{\rho})$ is isomorphic to A_5 and that $\det(\rho)$ is either trivial or equal to a quadratic character. Then from the exact sequence

$$1 \longrightarrow \mathrm{Im}(\rho) \cap \mathbb{C}^* \mathrm{Id} \longrightarrow \mathrm{Im}(\rho) \longrightarrow \mathrm{Im}(\overline{\rho}) \longrightarrow 1,$$

we deduce the exact sequence

$$1 \longrightarrow C \longrightarrow \mathrm{Im}(\rho) \longrightarrow A_5 \longrightarrow 1$$

where C is isomorphic to C_2 if $\det(\rho)$ is trivial and to C_4 if $\det(\rho)$ is quadratic. In the first case, $\mathrm{Im}(\rho)$ is isomorphic to $\widetilde{A}_5$, while in the second case, $\mathrm{Im}(\rho)$ is isomorphic to $\widehat{A}_5$. Hence, the problem of constructing icosahedral two-dimensional complex representations with trivial (resp. quadratic) determinant reduces to solving an embedding problem $\widetilde{A}_5 \mapsto A_5$ (resp. $\widehat{A}_5 \mapsto A_5$).

We restrict ourselves to liftings with quadratic or trivial determinant only for reasons of simplicity. We observe that if we find a lifting ρ of $\overline{\rho}$, the set of all liftings of $\overline{\rho}$ is given by $\{\rho \otimes \chi$ where χ is a Dirichlet character of $G_{\mathbb{Q}}\}$. This paper deals with all icosahedral representations such that there exists a Dirichlet character χ such that $\det(\rho \otimes \chi)^2 = 1$. We will use the following vocabulary.

Definition 1.2.
(1) *An n-lifting of $\overline{\rho}$ is a lifting ρ of $\overline{\rho}$ such that the order of $\det(\rho)$ is n.*
(2) *A n-lifting ρ of $\overline{\rho}$ is said of minimal ramification if for all n-liftings ρ' of $\overline{\rho}$, the cardinality $|\rho(I_p)|$ is less than of equal to $|\rho'(I_p)|$ for any prime number p (where I_p is the inertia group of p, defined up to conjugation).*

(3) *The minimal conductor of $\overline{\rho}$ is the smallest conductor amongst the conductors of the liftings of $\overline{\rho}$.*

We observe that if there exists an n-lifting for a given integer n, there exists an n-lifting with minimal ramification (theorem 2.1). For the determination of the minimal conductor, see [K].

Our methods of construction are described in section 5 through eight examples. In each case, given a projective representation $\overline{\rho}$ that has a 1-lifting or a 2-lifting, we produce a polynomial corresponding to such a lifting with minimal ramification. More precisely, we describe an algorithm to determine an element γ such that $\sqrt{\gamma}$ is of degree 24 and the Galois closure of $\mathbb{Q}(\sqrt{\gamma})$ is a solution of the embedding problem $\widetilde{A}_5 \mapsto A_5$ or $\widehat{A}_5 \mapsto A_5$. Using some ramification conditions, this algorithm starts by describing a finite set $\mathcal{E}'$ which contains such an element. Then we need a test to check whether the Galois closure of $\mathbb{Q}(\sqrt{\gamma})$ has Galois group $\widetilde{A}_5$ or $\widehat{A}_5$. This test is given by the theorem 4.3.1. It plays the key role in our work.

Subsection 5.1 gives a general algorithm, that uses the same kind of method than constructions of $\widetilde{A}_4 \simeq \mathrm{SL}_2(\mathbb{F}_3)$ (resp. $\widetilde{S}_4 \simeq \mathrm{GL}_2(\mathbb{F}_3)$) given in [H-K] and [Ba-Kw] (resp. [CN-J]).

In subsection 5.2, working with odd representations, we show how one can use Serre's conjecture on modular forms to accelerate the determination of γ. This method uses the Artin L-function of our representation. In fact, every computation of coefficients of this L-fuction shall permit such an acceleration of the algorithm; for example, subsection 5.3 uses the computations described in [B].

For these constructions, we always start with a polynomial of degree 5 of Galois group A_5, and with one of the two associated projective representations (corresponding to the two different embeddings $A_5 \hookrightarrow \mathrm{PGL}_2(\mathbb{C})$). For these polynomials, we refer to [Bas-Ki] and [B] in the odd case. Michael Müller, from the university of Essen, sent me the polynomials corresponding to the even case (personal communication).

The plan of the paper is the following. The section 2 is based on [S1]. It recalls some results about the lifting of projective representations. We give in this section a simple criterion to know if there exists a lifting ρ of $\overline{\rho}$ such that $\det(\rho)$ is equal to a given character ε. One can find in section 3 the 2-dimensional complex representations of $\widetilde{A}_5$ and $\widehat{A}_5$. Section 4 describes the Hasse diagrams of $\widetilde{A}_5$ and $\widehat{A}_5$ and gives the test (theorem 4.3.1) for computing the Galois group in our examples. Section 5 contains the constructions and the last section the computation of the Artin L-functions.

Acknowledgements. It is a pleasure to thank Nils Skoruppa for his help with modular forms. The author is also grateful for useful discussions with and comments from Philippe Cassou-Noguès, Gerhard Frey, Jacques Martinet and Michael Müller.

2. Local conditions

In this section, we recall some results about the lifting of projective representations (for these results, we refer to [S1], [B] and [K]).

Let k be a global or a local field (we assume throughout that our non-archimedean local fields have finite residue field). Let $\overline{k}$ be a separable closure of k; we write

$$G_k = \mathrm{Gal}(\overline{k}/k).$$

Let $\overline{\rho} : G_k \longrightarrow \mathrm{PGL}_2(\mathbb{C})$ be a projective representation. By a theorem of Tate, we know that there exists a Galois representation

$$\rho \ : \ G_k \longrightarrow \mathrm{GL}_2(\mathbb{C})$$

such that the induced projective representation of ρ is equal to $\overline{\rho}$. We call such a representation ρ a lifting of $\overline{\rho}$.

Now we restrict ourselves to the case $k = \mathbb{Q}$. We fix a projective representation $\overline{\rho} : G_{\mathbb{Q}} \longrightarrow \mathrm{PGL}_2(\mathbb{C})$. It is possible to specify the lifting of $\overline{\rho}$ on the inertia groups of prime numbers of $\mathbb{Q}$. Let p be a prime number, and let I_p and D_p ($I_p \subset D_p \subset G_{\mathbb{Q}}$) be respectively the inertia and decomposition groups of a place of $\overline{\mathbb{Q}}$ above p. These groups are uniquely determined up to conjugation, and D_p may be identified with $G_{\mathbb{Q}_p}$. For a proof of the next result, see [S1] p. 228.

Theorem 2.1 (Tate). *For each prime number p, let ρ'_p be a lifting of the restriction $\overline{\rho}|_{D_p}$ of $\overline{\rho}$ to D_p. Suppose that the restriction $\rho'_p|_{I_p}$ is trivial for almost all p. Then there exists a unique lifting ρ of $\overline{\rho}$ such that $\rho|_{I_p} = \rho'_p|_{I_p}$ for all p.*

Now we fix a character $\varepsilon : G_{\mathbb{Q}} \longrightarrow \mathbb{C}^*$. We want to get a lifting ρ of $\overline{\rho}$ with determinant ε. We can discuss the existence of such a lifting by local considerations. Since $\det(\chi \otimes \rho) = \chi^2.\det(\rho)$ for any abelian character χ of $G_{\mathbb{Q}}$, we see that $\overline{\rho}$ determines the determinant of a lifting up to multiplication by the square of a character.

We consider ε as an idèle class character of $\mathbb{Q}$, we denote by ε_v the restriction of ε to $\mathbb{Q}_v^*$, for every place v of $\mathbb{Q}$, and we define

$$(\varepsilon, v) = \varepsilon_v(-1).$$

We have the product formula $\prod_{v\in S}(\varepsilon, v) = 1$, where S denotes the set of places of $\mathbb{Q}$.

Since $\mathrm{PSl}_2(\mathbb{C}) = \mathrm{PGL}_2(\mathbb{C})$, the obstruction to $\overline{\rho}$ having a lifting with determinant 1 is an element λ of $H^2(G_{\mathbb{Q}}, \{\pm 1\})$. For all places v of $\mathbb{Q}$, the restriction λ_v of λ to $\mathbb{Q}_v$ is an element of $H^2(D_v, \{\pm 1\}) \simeq \{\pm 1\}$. This element is the obstruction to $\overline{\rho}|_{D_v}$ having a lifting with determinant 1. Let $(\overline{\rho}, v)$ for all places v of S be the image of λ_v in $\{\pm 1\}$. We have still a product formula: $\prod_{v\in S}(\overline{\rho}, v) = 1$.

Theorem 2.2 (Serre). *The projective representation $\overline{\rho}$ has a lifting ρ such that $\det(\rho) = \varepsilon$ if and only if $(\varepsilon, v) = (\overline{\rho}, v)$ for all places v of $\mathbb{Q}$, that is, by* *the product formula, if and only if $(\varepsilon, v) = (\overline{\rho}, v)$ for all places v of $\mathbb{Q}$, except possibly one.*

Theorem 2.3. *If $\overline{\rho}$ is unramified in a finite place p, then $(\overline{\rho}, p) = 1$.*

Proof. The restriction $\overline{\rho}|_{D_p}$ factors in this case through a homomorphism

$$\varphi : \mathrm{Gal}(\mathbb{Q}_p^{\mathrm{nr}}/\mathbb{Q}_p) \longrightarrow \mathrm{PGL}_2(\mathbb{C}),$$

where $\mathbb{Q}_p^{\mathrm{nr}}$ denotes the maximal unramified extension of $\mathbb{Q}_p$. We can view this homomorphism as an homomorphism with image in $\mathbb{C}^*$. By local class field theory, $\mathrm{Gal}(\mathbb{Q}_p^{\mathrm{nr}}/\mathbb{Q}_p)$ is isomorphic to $\widehat{\mathbb{Z}} = \varprojlim (\mathbb{Z}/n\mathbb{Z})$. Let g be a topological generator of $\widehat{\mathbb{Z}}$ and let γ be a square root of $\varphi(g)$ in $\mathbb{C}^*$. We define the homomorphism $\widetilde{\varphi} : \widehat{\mathbb{Z}} \longrightarrow \mathrm{GL}_2(\mathbb{C})$ by setting:

$$\widetilde{\varphi}(g) = \begin{pmatrix} \varphi(g)\gamma^{-1} & 0 \\ 0 & \gamma^{-1} \end{pmatrix}.$$

This homomorphism defines a lifting of $\overline{\rho}|_{D_p}$ with trivial determinant. $\square$

We suppose now, and until the end of the paper, that $\mathrm{Im}(\overline{\rho})$ is isomorphic to A_5. Let M be the subfield of $\overline{\mathbb{Q}}$ fixed by $\mathrm{Ker}(\overline{\rho})$, and let K be a quintic subfield of M. We denote by $\mathcal{O}_K$ the ring of integers of K. In the following proposition, $\mathfrak{p}_i$ is a prime ideal of $\mathcal{O}_K$ with residual index i.

Proposition 2.4. *The projective representation $\overline{\rho}$ has a lifting ρ with determinant ε if and only if the signature of the field K is equal to $(5, 0)$ (resp. $(1, 2)$) if ε is even (resp. odd) and for all odd prime numbers p, we have the following properties.*
(1) If p is unramified in K, then $(\varepsilon, p) = 1$.
(2) If $p\mathcal{O}_K = \mathfrak{p}_1^2\mathfrak{p}_1'^2\mathfrak{p}_1''$, then $(\varepsilon, p) = (-1)^{\frac{p-1}{2}}$.
(3) If $p\mathcal{O}_K = \mathfrak{p}_1^3\mathfrak{p}_1'\mathfrak{p}_1''$, $\mathfrak{p}_1^3\mathfrak{p}_2'$ or $\mathfrak{p}_1^5$, then $(\varepsilon, p) = 1$.
(4) If $p\mathcal{O}_K = \mathfrak{p}_2^2\mathfrak{p}_1'$, then $(\varepsilon, p) = (-1)^{\frac{p+1}{2}}$.
(5) If $3\mathcal{O}_K = \mathfrak{p}_1^2\mathfrak{p}_1'^3$, then $(\varepsilon, 3) = -1$.

Proof. First look at the condition at infinity: a lifting ρ of $\overline{\rho}$ is even if and only if $\overline{\rho}(c) = 1$, where c is the complex conjugation, that is, if and only if K is totally real.

For the finite places, a study of A_5 shows that if an odd prime number p is unramified, the only possibilities for $(\rho(D_p), \rho(I_p))$ are (C_2, C_2), (C_3, C_3), (D_6, C_3), (D_{10}, C_5), (C_5, C_5), (D_4, C_2) and (D_6, D_6). Couple (C_2, C_2) (resp. (D_4, C_2), (D_6, D_6)) corresponds to (2) (resp. (4), (5)). Couples (C_3, C_3), (D_6, C_3), (D_{10}, C_5), (C_5, C_5) correspond to (3) (see table 3.1 in [B]). If the image of $\overline{\rho}|_{D_p}$ is cyclic, then $\overline{\rho}|_{D_p}$ defines a cyclic character χ_0 with image in $\mathbb{C}^*$. All lifting of $\overline{\rho}|_{D_p}$ has a determinant $\chi^2\chi_0$, where χ is an abelian character. We have $(\overline{\rho}, p) = (\chi_0, p)$. Hence, the local condition is satisfied if and only if $(\chi_0, p) = (\varepsilon, p)$. For example, if $p\mathcal{O}_K = \mathfrak{p}_1^2\mathfrak{p}_1'^2\mathfrak{p}_1''$, the order of the character χ_0 is 2. By the local class field theory, we can see χ_0 as a character

$\chi_0 : \mathbb{Q}_p^* \longrightarrow \mathbb{C}^*$. Since χ_0 is ramified, we see that $\chi_0(\mu_{p-1}) = \{\pm 1\}$ (where μ_{p-1} is the group of the $(p-1)^{\text{th}}$ of the unity). Hence we obtain $(\chi_0, p) = (-1)^{\frac{p-1}{2}}$. In the other cases, we find the corresponding local conditions by the same kind of arguments. In fact, these conditions are particular cases of [K], theorem 1. Now, the proposition is a consequence of the theorem 2.2. $\square$

Corollary 2.5. *A projective representation $\overline{\rho}$ has a 1-lifting or a 2-lifting if and only if for all odd prime numbers $p \equiv 1$ mod 4, $p\mathcal{O}_K \neq \mathfrak{p}_2^2\mathfrak{p}_1'$.*

3. The 2-dimensional representations of $\widetilde{A}_5$ and $\widehat{A}_5$

Let ρ be a Galois representation of icosahedral type and trivial or quadratic determinant. We denote by M' the subfield of $\overline{\mathbb{Q}}$ fixed by $\mathrm{Ker}(\rho)$ and G' the group $\mathrm{Gal}(M'/\mathbb{Q})$. We denote $M = \overline{\mathbb{Q}}^{\mathrm{Ker}(\overline{\rho})}$, G the group $\mathrm{Gal}(M/\mathbb{Q})$ and K a subfield of M of degree 5. The group G' is isomorphic to $\widetilde{A}_5$ or $\widehat{A}_5$.

The group $\widetilde{A}_5$ has nine irreducible characters: the trivial character, two conjugated characters of degree 2, two conjugated characters of degree 3, two characters of degree 4 and two characters of respective degrees 5 and 6 (see [B], page 135). From these characters, we easily get the eighteen irreducible characters of the group $\widehat{A}_5$. Let α be a generator of the center of $\widehat{A}_5$. We denote $\omega = \alpha^2$. We consider A_5 as the alternating group over $\{1, 2, 3, 4, 5\}$, and for all elements $\tau \neq 1$ in A_5, we fix a lifting $\widetilde{\tau} \in \widetilde{A}_5$ with minimal order. Let ψ be the character of degree 2 of $\widehat{A}_5$ such that $\psi(\alpha) = 2i$ with a restriction to $\widetilde{A}_5$ as in table 3.1 below.

s	1	ω	$\widetilde{(12)(34)}$	$\widetilde{(123)}$	$\omega\widetilde{(123)}$	$\widetilde{(12345)}$	$\omega\widetilde{(12345)}$	$\widetilde{(12354)}$	$\omega\widetilde{(12354)}$
$\psi(s)$	2	-2	0	-1	1	$\frac{-1+\sqrt{5}}{2}$	$\frac{1-\sqrt{5}}{2}$	$\frac{-1-\sqrt{5}}{2}$	$\frac{1+\sqrt{5}}{2}$

Table 3.1.

In this table, nine of the eighteen conjugation classes of $\widehat{A}_5$ are represented. To get the other ones, we only have to multiply these representatives by α.

4. $\widetilde{A}_5$ and $\widehat{A}_5$-extensions

Let $M'/\mathbb{Q}$ be a Galois extension with Galois group $\widetilde{A}_5$ or $\widehat{A}_5$. The field M' contains a unique A_5-extension M of $\mathbb{Q}$. If $\mathrm{Gal}(M'/\mathbb{Q})$ is isomorphic to $\widehat{A}_5$, there exists a unique quadratic extension k of $\mathbb{Q}$ contained in M'. If $\mathrm{Gal}(M'/\mathbb{Q})$ is isomorphic to $\widetilde{A}_5$, there is no quadratic field contained in M'. We observe that the groups $\widetilde{A}_5$ and $\widehat{A}_5$ are transitive permutation groups of degree 24. In our constructions (section 5), we will get the field M' as the splitting field of polynomials of degree 24.

In this section, we give in 4.1 and 4.2 some informations on the Hasse diagram of $\widetilde{A}_5$ and $\widehat{A}_5$. In 4.3, we give a test to recognize whether an element of degree 24 (choosen in a set that we will describe) gives or not an $\widetilde{A}_5$ or an $\widehat{A}_5$-extension.

4.1. **$\widetilde{A}_5$-extensions.** For reasons of simplicity, we give an incomplete Hasse diagram for an $\widetilde{A}_5$-extension. With the notations of this diagram, the group $\mathrm{Gal}(M/K)$ is isomorphic to A_4. In this diagram, S and T are respectively the fields fixed by the cyclic group of order 5 generated by $\widetilde{(12345)}$ and the cyclic group of order 3 generated by $\widetilde{(123)}$.

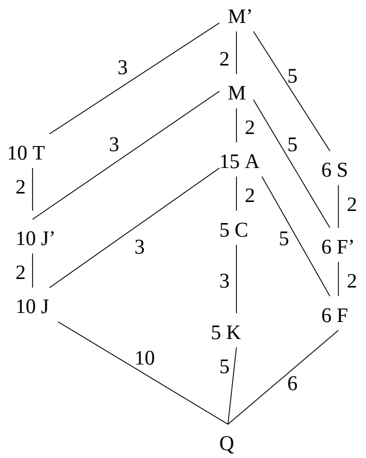

Diagram 4.1.1.

4.2. **$\widehat{A}_5$-extensions.** The Hasse diagram of an $\widehat{A}_5$-extension is more intricate. Here is an incomplete Hasse diagram. In this diagram, S (resp. S', T and T') is the field fixed by the dihedral groups of order 10 generated by $\widetilde{(12345)}$ and $\omega\widetilde{(25)(34)}$ (resp. the dihedral group of order 10 generated by $\widetilde{(12345)}$ and $\omega^3\widetilde{(25)(34)}$, the dihedral group of order 6 generated by $\widetilde{(123)}$ and $\omega\widetilde{(12)(45)}$ and the dihedral group of order 6 generated by $\widetilde{(123)}$ and $\omega^3\widetilde{(12)(45)}$).

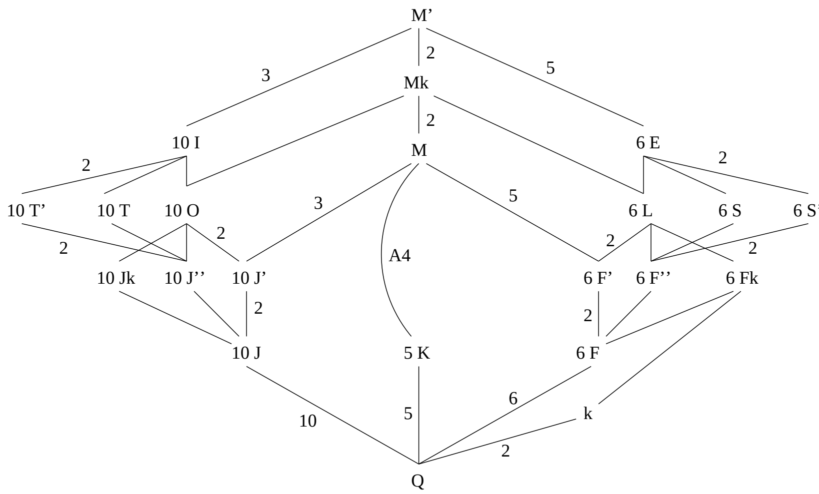

Diagram 4.2.1.

Of course, the group Gal(M/K) is still isomorphic to A_4. If A is a subfield of M such that the degree (M/A) is 2, the group Gal(M'/A) is isomorphic to $C_4 \times C_2$. Here, the group Gal(M'/M) is cyclic of order 4. Moreover, the extensions E/F and I/J are Galois, and their Galois groups are isomorphic to $C_4 \times C_2$.

If we study these fields closely, we obtain the following interesting property.

Property 4.2.2. *The fields S and S' (resp. T and T') are arithmetically equivalent, but not conjugate. We recall that number fields are said to be arithmetically equivalent if they have the same Dedekind ζ-function.*

Property 4.2.2 is a consequence of the following theorem ([G] or [C-D-O], theorem 3)

Theorem 4.2.3. *Let K_1 and K_2 be two number fields in $\overline{\mathbb{Q}}$. The fields K_1 and K_2 are arithmetically equivalent if and only if the following two conditions are satisfied.*
(1) *The fields have a common Galois closure N.*
(2) *Let $G = Gal(N/\mathbb{Q})$, $G_1 = Gal(N/K_1)$ and $G_2 = Gal(N/K_2)$. Then for each conjugacy class C in G, we must have $|G_1 \cap C| = |G_2 \cap C|$.*

4.3. **A test for constructions.** In this subsection, we want to treat as the same time the cases of extensions with Galois group $\widetilde{A}_5$ and $\widehat{A}_5$. We adopt the following notations: A_5' will denote either $\widetilde{A}_5$ or $\widehat{A}_5$ and k will be the unique quadratic extention in M' (resp. the field of rational numbers) when $A_5' = \widehat{A}_5$ (resp. $\widetilde{A}_5$). The notations for the fields correspond either to the diagram 4.1.1 if $A_5' = \widetilde{A}_5$ or to the diagram 4.2.1 if $A_5' = \widehat{A}_5$. Let d be a rational integer such that $k = \mathbb{Q}(\sqrt{d})$. We can write $F' = F(\sqrt{t})$, where $t \in \mathcal{O}_F$. Let $F'' = F(\sqrt{dt})$. The field S is an extension of F'' defined by the square root of an integer $a + b\sqrt{dt}$ of F'', where a and b belong to F. Then one can easily prove that the field M' is the Galois closure of S.

We now are interested in the converse of this property. More precisely, let $M/\mathbb{Q}$ be a Galois extension of A_5 type and $k = \mathbb{Q}(\sqrt{d})$ or $\mathbb{Q}$ a quadratic or rational number field. We denote by L the compositum of F' and k. Let a and b be elements of F such that $\gamma = a + b\sqrt{dt}$ is an integer of F'', and let M'' be the Galois closure of $F''(\sqrt{\gamma})$. The following theorem provides a test to check whether $M''/\mathbb{Q}$ is an extension of Galois group A'_5 having k for quadratic subfield. The field L is the compositum of F' and k. If $\mathrm{Gal}(M'/\mathbb{Q})$ is isomorphic to $\widetilde{A}_5$, we have $L = F'' = F'$.

Theorem 4.3.1. *Suppose that $\gamma \notin \mathbb{Q}^* L^{*2}$. Let σ_i ($i \in \{1, \ldots, 6\}$) be the embeddings of F in $\mathbb{C}$. For $i \in \{1, \ldots, 6\}$, let $a_i = \sigma_i(a)$, $b_i = \sigma_i(b)$, $t_i = \sigma_i(t)$, let θ_i be a square root of t_i and let γ_i and γ'_i be respectively equal to $a_i + b_i\theta_i\sqrt{d}$ and $a_i - b_i\theta_i\sqrt{d}$. The respective degrees of*

$$\Phi = \gamma_1\gamma_2(\gamma_1 - \gamma_2)^2 d \qquad \text{and} \qquad \Phi' = \gamma_1\gamma'_2(\gamma_1 - \gamma'_2)^2 d$$

over $\mathbb{Q}$ divide 30. Moreover, if these degrees both are equal to 30, then $\mathrm{Gal}(M''/\mathbb{Q})$ is isomorphic to A'_5 if and only if $\sqrt{\Phi}$ and $\sqrt{\Phi'}$ both are elements of degree 30 over $\mathbb{Q}$.

Remark 4.3.2. When Φ and Φ' both are elements of degree 30 over $\mathbb{Q}$, our theorem gives us a necessary and sufficient condition in order to get an extension of Galois group A'_5. This is the case for all the examples treated in section 5. Nevertheless if either Φ or Φ' fails to have the required degree one can multiply γ by an element of $(F'')^{*2}$ and try again with this element as a "new γ".

Proof of theorem 4.3.1. The Galois group of $M''/\mathbb{Q}$ is isomorphic to A'_5 if and only if $M'' = Mk(\sqrt{\gamma})$. Indeed, if M'' is a quadratic extension of Mk, we get the exact sequence

$$1 \longrightarrow C_2 \longrightarrow \mathrm{Gal}(M''/\mathbb{Q}) \longrightarrow A_5 \longrightarrow 1$$

if $k = \mathbb{Q}$ or the exact sequence

$$1 \longrightarrow C_2 \longrightarrow \mathrm{Gal}(M''/\mathbb{Q}) \longrightarrow A_5 \times C_2 \longrightarrow 1$$

if not. Since $\gamma \notin \mathbb{Q}^* (F'')^{*2}$, the group $\mathrm{Gal}(M''/\mathbb{Q})$ is neither isomorphic to $A_5 \times C_2$ nor $A_5 \times C_2 \times C_2$. Moreover, if $\mathrm{Gal}(M''/\mathbb{Q})$ is isomorphic to $\widetilde{A}_5 \times C_2$ or $A_5 \times C_4$, the field F'' has a unique quadratic extension L in M''. Hence, the only possibility for $\mathrm{Gal}(M''/\mathbb{Q})$ is A'_5.

Let Φ and Φ' as above, and let $\varphi = \sqrt{\Phi}$ and $\varphi' = \sqrt{\Phi'}$. Here, we consider A_5 as a permutation group on $\{t_1, \ldots, t_6\}$. Let τ and τ' be the two elements of order 2 in A_5 that interchange t_1 and t_2. Since the degree of θ_1 and θ_2 is 12, we get that $\tau\tau'(\theta_1) = -\theta_1$ and $\tau\tau'(\theta_2) = -\theta_2$. We choose τ and τ' such that $\tau(\theta_1) = \theta_2$ and $\tau'(\theta_1) = -\theta_2$. Elements Φ and Φ' belong to Mk. Let $\mathrm{Gal}(k/\mathbb{Q}) = \{e, a\}$, with $e(\sqrt{d}) = \sqrt{d}$ and $a(\sqrt{d}) = -\sqrt{d}$. We denote elements of $\mathrm{Gal}(Mk/\mathbb{Q})$ by couples (g, g'), where $g \in\mathrm{Gal}(M/\mathbb{Q})$ and

$g' \in \mathrm{Gal}(k/\mathbb{Q})$. We compute $(\tau, e)(\Phi) = (\tau', a)(\Phi) = \Phi$ and $(\tau', e)(\Phi') = (\tau, a)(\Phi') = \Phi'$. We suppose now that the degree of Φ and Φ' is 30. For $i \in \{1, \dots, 6\}$, let y_i (resp. y'_i) be a given square root of γ_i (resp. γ'_i). If the degree of elements $y_i y_j (\gamma_i - \gamma_j)\sqrt{d}$ (resp. $y_i y'_j (\gamma_i - \gamma'_j)\sqrt{d}$) for $i \neq j$ is 30, then $y_1 y_i$ and $y_1 y'_i$ belong to Mk for all $i \in \{1, \dots, 6\}$ and $Mk(\sqrt{\gamma})$ is Galois over $\mathbb{Q}$. Conversely, if $\mathrm{Gal}(M''/\mathbb{Q})$ is isomorphic to $\widehat{A}_5$. Let $\widetilde{\tau}$ and $\widetilde{\tau}'$ be some liftings of τ and τ' in $\widetilde{A}_5$. Let α be as in the section 3. We choose the elements y_i and y'_i such that $\alpha(y_i) = y'_i$ for all i. Since $\widetilde{\tau}^2 = \widetilde{\tau}'^2 = \omega$ and $(\alpha\widetilde{\tau})^2 = (\alpha\widetilde{\tau}')^2 = 1$, we have the equalities $\widetilde{\tau}(y_1 y_2) = -y_1 y_2$, $\widetilde{\tau}'(y_1 y_2) = y'_1 y'_2$, $\widetilde{\tau}'(y_1 y'_2) = -y_1 y'_2$ and $\alpha\widetilde{\tau}(y_1 y'_2) = y_1 y'_2$. We compute then $\widetilde{\tau}(\varphi) = \alpha\widetilde{\tau}'(\varphi) = \varphi$ and $\widetilde{\tau}'(\varphi') = \alpha\widetilde{\tau}(\varphi') = \varphi'$. It proves that φ and φ' both have degree 30. The proof for $\widetilde{A}_5$ is left to the reader. $\square$

Corollary 4.3.3 below is a translation of theorem 4.3.1 in terms of polynomials. We use this corollary for our computations. Now let $\mathcal{R}$ (resp. $\mathcal{R}'$) be a system of representatives of cosets of $\mathrm{Gal}(Mk/\mathbb{Q})/ < (\tau, e), (\tau', a) >$ (resp. $\mathrm{Gal}(Mk/\mathbb{Q})/ < (\tau', e), (\tau, a) >$), where τ and τ' are defined in proof of theorem 4.3.1. For all $g \in \mathrm{Gal}(Mk/\mathbb{Q})$, we define $\Phi_g = g(\Phi)$ and $\Phi'_g = g(\Phi')$.

Corollary 4.3.3. *Suppose that $\gamma \notin \mathbb{Q}^* L^{*2}$. The polynomials of degree 30*

$$P_1(X) = \prod_{g \in \mathcal{R}} (X - \Phi_g) \qquad \text{and} \qquad P_2(X) = \prod_{g \in \mathcal{R}'} (X - \Phi'_g)$$

belong to $\mathbb{Z}[X]$. Moreover, if these polynomials are irreducible in $\mathbb{Z}[x]$, then $\mathrm{Gal}(M''/\mathbb{Q})$ is isomorphic to A'_5 if and only if the polynomials $P_1(X^2)$ and $P_2(X^2)$ both are reducible in $\mathbb{Z}[X]$.

To use this corollary 4.3.3, we need to know explicitely the elements θ_i. For our constructions, we always start with a polynomial of degree 5 with Galois group A_5. Let $x_1, \dots x_5$ be the roots of this polynomial. We define these elements θ_i as below.

$$\left\{ \begin{aligned} \theta_1 &= (x_1 - x_2)(x_2 - x_3)(x_3 - x_4)(x_4 - x_5)(x_1 - x_5), \\ \theta_2 &= (x_2 - x_5)(x_3 - x_5)(x_3 - x_4)(x_1 - x_4)(x_1 - x_2), \\ \theta_3 &= (x_1 - x_5)(x_1 - x_3)(x_3 - x_4)(x_2 - x_4)(x_2 - x_5), \\ \theta_4 &= (x_2 - x_4)(x_2 - x_3)(x_3 - x_5)(x_1 - x_5)(x_1 - x_4), \\ \theta_5 &= (x_2 - x_5)(x_2 - x_3)(x_1 - x_3)(x_1 - x_4)(x_4 - x_5), \\ \theta_6 &= (x_1 - x_3)(x_3 - x_5)(x_4 - x_5)(x_2 - x_4)(x_1 - x_2). \end{aligned} \right. \tag{4.3.4}$$

Indeed, θ_1 is fixed by (12345) (here we consider $\mathrm{Gal}(M/\mathbb{Q})$ as a permutation group on the roots $x_1, \dots, x_5$) and we have the equality $(14)(23)\theta_1 = -\theta_1$. Let F and F' be respectively the subfields of M fixed by the subgroups $< (12345), (14)(23) >$ and $< (12345) >$ of A_5. Then we have $\theta_1 \in F' \setminus F$ and $\theta_1^2 \in F^2$. We deduce the other elements θ_i by translation under the right cosets of the subgroup $< (12345), (14)(23) >$ of A_5.

5. Explicit constructions

We consider an A_5-extension M of $\mathbb{Q}$. We suppose that there exists a square free integer d and a quadratic extension $M'/M(\sqrt{d})$ such that M' is Galois over $\mathbb{Q}$ with Galois group isomorphic to $\widehat{A}_5$ (resp. $\widetilde{A}_5$) when $d \neq 1$ (resp. $d = 1$). The aim of this section is to show how to use theorem 4.3.1 to construct the field M'. One has to notice that in all our examples, the field M' we obtain has minimal ramification.

In terms of representations, if G is the group $\mathrm{Gal}(M/\mathbb{Q})$, we define $\overline{\rho}$ as the composition of the canonical surjection $G_{\mathbb{Q}} \mapsto G$ with an injection $G \hookrightarrow \mathrm{PGL}_2(\mathbb{C})$. There are two different embeddings $A_5 \hookrightarrow \mathrm{PGL}_2(\mathbb{C})$, and then there are two inequivalent possibilities for $\overline{\rho}$. We suppose that $\overline{\rho}$ has a 1-lifting or a 2-lifting and we choose such a 1-lifting or 2-lifting ρ with minimal ramification. Then, the integer d is such that $\det(\rho) = \chi_d$ and M' is the field fixed by $\mathrm{Ker}(\rho)$.

If we keep the notations of the diagrams 4.1.1 and 4.2.1, we show how to find a primitive element for the field S, choosen as the square root of an integer γ of F''. Using the ramification conditions in the extension S/F'', we know that we only have to look for such a γ in a finite set $\mathcal{E}$. Indeed, suppose that $F''(\sqrt{\pi})$ has the required ramification. Let $\mathcal{S}$ be a fixed finite set $\{1, \alpha_1, \ldots, \alpha_s\}$ such that for for all i, the element α_i is a generator of an ideal $\mathfrak{I}_i^2$, and such that the set $\{\mathcal{O}_{F''}, \mathfrak{I}_1, \ldots, \mathfrak{I}_s\}$ gives the 2-torsion of the class group $\mathrm{Cl}(F'')$. Then there exists an unit ε and an element α in $\mathcal{S}$ such that $S = F''(\sqrt{\pi\varepsilon\alpha})$. We use then ramification conditions at the real places (given by theorem 5.1.1) to get a subset $\mathcal{E}'$ containing the right γ.

Subsection 5.1 describes through five examples the general algorithm to find γ. Subsection 5.2 uses the L-functions of representations to accelerate the algorithm.

Each example begins by a table, that gives the following datas: the coefficients $(a_1, a_2, a_3, a_4, a_5)$ of a polynomial $X^5 + a_1X^4 + a_2X^3 + a_3X^2 + a_4X + a_5$ defining K, the signature of K, its discriminant d_K, the decomposition of each ramified prime number in K, the integer d, the conductor of ρ, the class group of F'' and the ramification of each prime number that has to be ramified in S/F''. Recall that if $d = 1$, the field F'' is equal to F'.

The notation $p = \prod_{i=1}^{s} f_i^{e_i}$ means that the ideal (p) factorises as $(p) = \prod_{i=1}^{s} \mathfrak{p}_i^{e_i}$, where the residue degree of the prime ideal $\mathfrak{p}_i$ is f_i. For all integers n, we denote by χ_n the quadratic character associated to $\mathbb{Q}(\sqrt{n})$ and ϕ_n a cyclotomic character of conductor n.

5.1. General algorithm.

In this subsection, we select the right γ by a systematic research in a "good" set $\mathcal{E}'$ that we will describe. We use the following result.

Proposition 5.1.1. *The signature of the field S is $(24, 0)$ or $(0, 12)$ in the even case and $(4, 10)$ in the odd case.*

Proof. Let σ_i (where $i \in \{1, \dots, 12\}$ in the even case and $i \in \{1, \dots, 4\}$ in the odd case) be the real embeddings of F''. In the even case, the field M is totally real. Since $M(\sqrt{\gamma})$ is Galois over $\mathbb{Q}$, each product $\sigma_1(\gamma)\sigma_i(\gamma)$ is positive. In the odd case, we use the three following facts. The real places of F split in F''/F (because the fields F' and Fk are totally imaginary), the extension E/F'' has a Galois group isomorphic to $C_2 \times C_2$ and the arithmetically equivalent fields S and S' have the same signature. □

The representation of the example 1 is odd. The other ones described in this subsection are even.

Example 1. *Minimal conductor:* $1161 = 3^3.43$ *(example 10 in [Bas-Ki]).*

P	$\mathrm{sgn}(K)$	d_K	ram. in K	d	$\mathfrak{F}(\rho)$	$\mathrm{Cl}(F'')$	ram. in F''
(0,3,48,108,72)	(1,2)	$3^4.43^2$	$3{=}1^2 1^3$ $43{=}1^1 1^1 1^3$	-3	$3^3.43^2$	C_3	$3{=}2^3 2^3$

Proposition 5.1.2. (A polynomial for the example 1) *The projective representation $\overline{\rho}$ has two 2-liftings with minimal ramification: say ρ and $\rho \otimes \chi_{-3}$. The determinant of these 2-liftings are χ_{-3} and their conductor is $3^3.43^2$. Moreover, the field $\overline{\mathbb{Q}}^{\mathrm{Ker}(\rho)}$ is the splitting field of the polynomial*

$$\begin{aligned}&X^{24} - 129X^{22} + 220584X^{20} - 1667231X^{18} + 150502275X^{16}\\&+87739404X^{14} + 1277550617X^{12} - 556689348X^{10} + 164566755X^8\\&+2058993X^6 - 6862320X^4 + 422091X^2 + 729.\end{aligned}$$

We can choose ϕ_{43} such that the representation $\rho \otimes \phi_{43}^{14}$ is a lifting with minimal conductor.

Proof. We use the notations of the diagram 4.2.1. The field F'' is the root field of the polynomial

$$\begin{aligned}P_{F''}(X) = \ & X^{12} - 48504X^{10} + 496567440X^8 - 1769385077568X^6\\&+1743382397325312X^4 - 655520855603281920X^2\\&+77314002626581364736.\end{aligned}$$

Indeed, the roots of this polynomial are $\theta_i\sqrt{-3}/9$ $(i = 1, \dots, 6)$, where the elements θ_i are the ones of theorem 4.3.1, defined by (4.3.4). The only prime ideals that could be ramified in the quadratic extensions S/F'' divide 3. Since the valuation $v_3(\mathfrak{F}(\rho))$ is 3, the ramification index of 3 in M' is 6. We check that $3\mathcal{O}_{F''} = \mathfrak{p}^3\mathfrak{p}'^3$. The ideals $\mathfrak{p}$ and $\mathfrak{p}'$ are the only prime ideals ramified in E/F''. Since S and S' are arithmetically equivalent, one, and only one of these ideals is ramified in the extension S/F'' and the other is ramified in S'/F''. Using the system [PARI], we check that $\mathfrak{p}$ and $\mathfrak{p}'$ have order 3 in $\mathrm{Cl}(F'')$ and we find a generator π for the ideal $\mathfrak{p}^3$. We look for an element $\gamma \in \mathcal{O}_{F''}$ such that $S = F''(\sqrt{\gamma})$. Since the field F'' has 7 fundamental units $\{\varepsilon_i \ : i \in \{1, \cdots, 7\}\}$, we can choose γ in the set

$$\mathcal{E} = \left\{ \pm\pi \prod_{i=1}^{7} \varepsilon_i^{\delta_i} \ : \ \forall i \in \{1, \cdots, 7\}, \delta_i \in \{0, 1\} \right\}.$$

In this set, we find a subset $\mathcal{E}'$ of 96 elements x with the required signature, that is, such that in $\{\sigma_1(x),\dots,\sigma_4(x)\}$ (where $\sigma_1,\dots,\sigma_4$ are the real embeddings of F''), there are two positive reals and two negative reals (see proposition 5.1.1). If $Mk(\sqrt{x})/\mathbb{Q}$ is Galois, then $Mk(\sqrt{-x})/\mathbb{Q}$ is Galois. Hence, we have only to look for an element x such that $Mk(\sqrt{x})/\mathbb{Q}$ is Galois in a set of 48 elements. Using theorem 4.3.1, we find such an element. Then γ is x or $-x$. To choose the right one, we use the fact that the discriminant of $F''(\sqrt{\gamma})$ is odd and that the one of $F''(\sqrt{-\gamma})$ is even. To get the representation with minimal conductor, we only have to see that the restriction of ρ on the inertia group I_3 is conjugated to a matrix

$$\begin{pmatrix}\phi_{43}^{14} & 0\\ 0 & \phi_{43}^{28}\end{pmatrix}. \ \square$$

Example 2. *Minimal conductor:* $7947 = 3^2.883$.

P	$\mathrm{sgn}(K)$	d_K	ram. in K	d	$\mathfrak{F}(\rho)$	$\mathrm{Cl}(F')$	ram. in F'
$(0,-17,30,-4,-7)$	$(5,0)$	$3^2.883^2$	$3{=}1^1 2^2$ $883{=}1^1 1^1 1^3$	1	$3^2.883^2$	C_{15}	$3{=}2^2 2^2 2^2$

Proposition 5.1.3. (A polynomial for the example 2) *The projective representation $\overline{\rho}$ has two 1-liftings with minimal ramification. We note them ρ and $\rho\otimes\chi_{-3}$. The determinant of these representations is 1 and their conductor is $3^2.883^2$. Moreover, we can choose ρ such that the field $\overline{\mathbb{Q}}^{\mathrm{Ker}(\rho)}$ is the splitting field of the polynomial*

$$\begin{aligned}&X^{24}-1719X^{22}+1033803X^{20}-247759929X^{18}+18891275922X^{16}\\ &-520186579740X^{14}+4132529834850X^{12}-12489586256925X^{10}\\ &+17037668338668X^{8}-10424803822722X^{6}+2281972718133X^{4}\\ &-481611663X^{2}+729.\end{aligned}$$

We can choose ϕ_{883} such that the representation $\rho\otimes\phi_{883}^{294}$ is a lifting with minimal conductor.

Proof. Since $d=1$, $\mathrm{Gal}(M'/\mathbb{Q})$ is isomorphic to $\widetilde{A}_5$ and $F''=F'$. We write the decomposition of 3 in F': $3\mathcal{O}_{F'}=\mathfrak{p}^2\mathfrak{p}'^2\mathfrak{p}''^2$. The ideal $\mathfrak{p}\mathfrak{p}'\mathfrak{p}''$ is principal because $\mathrm{Cl}(F')\simeq C_{15}$. The extension S/F' has to be ramified in $\mathfrak{p}$, $\mathfrak{p}'$ and $\mathfrak{p}''$. Using the system [PARI], we get a generator π for $\mathfrak{p}\mathfrak{p}'\mathfrak{p}''$. We have to find a totally positive element in the set

$$\mathcal{E}=\left\{\pm\pi\prod_{i=1}^{11}\varepsilon_i^{\delta_i}\ :\ \forall i\in\{1,\cdots,11\},\delta_i\in\{0,1\}\right\},$$

where $\{\varepsilon_i\ :\ i\in\{1,\dots,11\}\}$ is a system of fondamental units of F'. There are such elements x and y. The discriminant of $F'(\sqrt{x})$ is odd, then we can take $\gamma=x$. If this choice corresponds to ρ, the choice $\gamma=-y$ corresponds to $\rho\otimes\chi_{-3}$. $\square$

Example 3. *Minimal conductor:* $8164 = 2^2.13.157$.

Here, there is no ramification in the extension S/F'. This is why there is no column "ram. in F'" in this table.

P	$\mathrm{sgn}(K)$	d_K	ram. in K	d	$\mathfrak{F}(\rho)$	$\mathrm{Cl}(F')$
$(1,-17,-13,52,52)$	$(5,0)$	$2^2.13^2.157^2$	$2{=}2^1 1^3$ $13{=}1^1 1^1 1^3$ $157{=}1^1 1^1 1^3$	1	$2^2.13^2.157^2$	$C_3{\times}C_{30}$

Proposition 5.1.4. (A polynomial for the example 3) *The projective representation $\overline{\rho}$ has one 1-lifting ρ with minimal ramification. The determinant of this representation is 1 and its conductor is $2^2.13^2.157^2$. Moreover, the field $\overline{\mathbb{Q}}^{\mathrm{Ker}(\rho)}$ is the splitting field of the polynomial*

$$X^{24} - 13770X^{22} + 52469365X^{20} - 55431544302X^{18}$$
$$+10080960908026X^{16} - 137975364303634X^{14} + 511570114282349X^{12}$$
$$-577445967946818X^{10} + 133560924783322X^{8} - 1067593607742X^{6}$$
$$+1354808661X^{4} - 440826X^{2} + 1.$$

We can choose ϕ_{13} and ϕ_{157} such that the representation $\rho \otimes \phi_{13}^4\phi_{157}^{52}$ is a lifting with minimal conductor.

Proof. The extension S/F' has to be unramified. The class number of F' is even. Using [PARI], we found a generator α of the square of a non principal ideal $\mathcal{I}$. We have to find an element $\gamma = \varepsilon$ or $\alpha\varepsilon$, where ε is an unit. By the same way than in the example 3, we found two elements γ and $-\gamma$ (in fact, the good element γ is a totally positive unit). □

Example 4. *Minimal conductor:* $11457 = 3^2.19.67$.

P	$\mathrm{sgn}(K)$	d_K	ram. in K	d	$\mathfrak{F}(\rho)$	$\mathrm{Cl}(F')$	ram. in F'
$(2,-13,-2,$ $34,-19)$	$(5,0)$	$3^2.19^2.67^2$	$3{=}1^1 2^2$ $19{=}1^1 1^1 1^3$ $67{=}1^1 1^1 1^3$	1	$3^2.19^2.67^2$	$C_3{\times}C_{15}$	$3{=}2^2 2^2 2^2$

We obtain by the same way than in the example 2 the following result.

Proposition 5.1.5. (A polynomial for the example 4) *The projective representation $\overline{\rho}$ has two 1-liftings with minimal ramification. We note them ρ and $\rho \otimes \chi_{-3}$. The determinant of these representations is 1 and their conductor is $3^2.19^2.67^2$. Moreover, we can choose ρ such that the field $\overline{\mathbb{Q}}^{\mathrm{Ker}(\rho)}$ is the splitting field of the polynomial*

$$X^{24} - 67617X^{22} + 208285650X^{20} - 181081858005X^{18}$$
$$+42471530348796X^{16} - 2223530218411317X^{14} + 9799325198387037X^{12}$$
$$-13938846510860316X^{10} + 6265339227190755X^{8}$$
$$-689994490005738X^{6} + 2045970070074X^{4} - 1385748081X^{2} + 729.$$

We can choose ϕ_{19} and ϕ_{67} such that the representation $\rho \otimes \phi_{19}^6\phi_{67}^{22}$ is a lifting with minimal conductor.

Example 5. *Minimal conductor:* $8705 = 5.1741$.

P	$\mathrm{sgn}(K)$	d_K	ram. in K	d	$\mathfrak{F}(\rho)$	$\mathrm{Cl}(F')$	ram. in F'
(11,−19,−15, 16,−3)	(5,0)	5^2,1741^2	$5=1^1 1^2 1^2$ $1741=1^1 1^1 1^3$	1	$5^2.1741^2$	C_{30}	$5=\prod_{i=1}^6 1^2$

Proposition 5.1.6. (A polynomial for the example 5) *The projective representation $\overline{\rho}$ has two* 1*-liftings with minimal ramification. We note them ρ and $\rho \otimes \chi_5$. The determinant of these representations is* 1 *and their conductor is* $5^2.1741^2$. *Moreover, we can choose ρ such that the field $\overline{\mathbb{Q}}^{\mathrm{Ker}(\rho)}$ is the splitting field of the polynomial*

$$\begin{aligned}&X^{24} - 6714790X^{22} + 3329994844015X^{20} - 446704398093907750X^{18}\\&+6925323485608502066875X^{16} - 35988214906835348972777500X^{14}\\&+80579487352740009781758640000X^{12}\\&-77379984051244890484351881671875X^{10}\\&+24397137781407868886109290073109375X^{8}\\&-522042591873097725430275471015625X^{6}\\&+13373799357158206196045321875X^{4} - 20698283863183388265625X^{2}\\&+16777216000000.\end{aligned}$$

We can choose ϕ_{1741} such that the representation $\rho \otimes \phi_5 \phi_{1741}^{580}$ is a lifting with minimal conductor.

In this example, the shape of the element for γ, where α generates the square of a non principal ideal and where π generates the product of the six prime ideals of $\mathcal{O}_{F'}$ dividing 5.

Remark 5.1.7. This projective representation has a lifting $\rho \otimes \phi_5$ with determinant χ_5 and conductor 5.1741^2. We prefer to give a polynomial with Galois group $\widetilde{A}_5$ instead of $\widehat{A}_5$.

5.2. **Acceleration of the algorithm, using Serre's conjecture.** In subsection 5.1, we found a general algorithm to solve our embedding problem. In this algorithm, we have to select a right element γ in a field F'' of degree 12. For this aim, this algorithm uses factorisations of polynomials of degree 60. These factorisations can take a long time when the discriminant of the quintic field increases. In even case, conditions at infinity are so strong that the number of such factorisations we have to compute is small (in fact, in examples 2, 3 and 4, we do not need to compute any such factorisation). We propose here a method based on the utilisation of the L-function of the representation: if we know some coefficients a_l (l prime) of this representation, then we deduce the order of the corresponding decomposition groups. We will use such informations to select our element γ.

In fact, we propose here a method using Serre's conjecture on modular forms. This method deals with odd representations. Indeed, Serre's conjecture on modular forms gives a way to compute *conjectural* coefficients of the L-function. We can then select a conjectural element γ. Finally, we prove that the extension $Mk(\sqrt{\gamma})/\mathbb{Q}$ we obtain is Galois by theorem 4.3.1. This method is illustrated by examples 6 and 7. If Serre's conjecture is false, then the method doesn't work: we might not find anything in the space of modular forms mod p, or we might find an eigenform whose coefficients look like the traces of representation only for small p. In this case, the method would give a counter example to the conjecture.

In order to explain how to use Serre's conjecture on modular forms (conjecture 5.2.1 below), we have to fix our notations for modular forms in characteristic p. For definitions and results on these forms, see [S2].

Let p be a prime number, N' an integer, $N' \geq 1$, coprime to p and χ a character $(\mathbb{Z}/N'\mathbb{Z})^* \mapsto \overline{\mathbb{F}}_p^*$. For any integer k, $k > 1$, we denote by $\widetilde{S}_k(N', \chi)$ the space of modular forms with coefficients in $\overline{\mathbb{F}}_p$ of type (k, N', χ), as defined in [S2] (it is the reduction modulo p of the space of complex cusp forms $S_k(N', \chi_0)$, where χ_0 is the only lifting of χ with values in the complex roots of the unity of order prime to p). For all prime numbers ℓ, we note $\widetilde{T}_\ell$ the Hecke operator corresponding to ℓ in such spaces.

In each of examples 6 and 7, we consider a projective representation $\overline{\rho}$ given by a quintic polynomial P. Let N and χ be respectively an integer and a character $(\mathbb{Z}/N\mathbb{Z})^* \mapsto \mathbb{C}^*$ such that there exists a lifting ρ of $\overline{\rho}$ with conductor N and determinant χ. We want to compute some coefficients of the L-function $L(\rho, s)$ of ρ.

Up to conjugation, the representation ρ may be viewed as a representation $\rho : G_{\mathbb{Q}} \longrightarrow \mathrm{GL}_2(\overline{\mathbb{Z}})$, where $\overline{\mathbb{Z}}$ denotes the integral closure of $\mathbb{Z}$ in $\overline{\mathbb{Q}}$. Let p be a prime number. We define by reduction a representation

$$\widetilde{\rho} \;:\; G_{\mathbb{Q}} \longrightarrow \mathrm{GL}_2(\overline{\mathbb{F}}_p),$$

and a character

$$\widetilde{\chi} \;:\; G_{\mathbb{Q}} \longrightarrow \overline{\mathbb{F}}_p^*.$$

Conjecture 5.2.1 (Serre). *There exists two integers $N' \geq 1$, $1 < k \leq p^2$ and an eigenform for the Hecke operators $f = \sum_{n \geq 1} a_n q^n$ in $\widetilde{S}_k(N', \widetilde{\chi})$ such that for all prime numbers $\ell \not| pN'$, we have:*

$$Tr(Frob_{\ell,\widetilde{\rho}}) = a_\ell \qquad and \qquad det(Frob_{\ell,\widetilde{\rho}}) = \widetilde{\chi}(l) l^{k-1}.$$

Moreover, J.-P. Serre gave a recipe (in [S2]) to compute the integers k and N'. If we can compute a basis of $S_k(N', \chi_0)$, we restrict ourselves to a simple problem of linear algebra: computing eigenvectors in a vector space of finite dimension. Dimension of this space, and then complexity of the computation of the basis increases like kN'. Since N' divides N divided by its p-part, we see that it could be good to choose the prime number p either small or such that p^2 divides N (for the choice of p, see also remark 5.2.9). Moreover, it is sometimes useful (as in example 6) to lower the weight k, in order to restrict ourselves to a simpler vector space. For this aim, we can use theorem 5.2.2 below, due to S. Edixhoven ([E]).

In order to write theorem 5.2.2, we have to introduce the derivation θ. If $f = \sum a_n q^n$ is a formal series, we define the series θf by setting $\theta f = \sum n a_n q^n$. If f is a modular form with coefficients in $\overline{\mathbb{F}}_p$, then θf is such a modular form too. Moreover, the application θ does neither change the level nor the character, but it increases the weight by $p+1$ (see [E]).

Theorem 5.2.2 (Edixhoven)**.** *Let f be an eigenform in a space $\widetilde{S}_k(N,\chi)$ of modular forms with coefficients in $\overline{\mathbb{F}}_p$. Then there exists integers n and k' with $0 \leq n \leq p-1$, $k' \leq p+1$, and an eigenform g in $\widetilde{S}_{k'}(N,\chi)$ such that f and $\theta^n g$ have the same eigenvalues for all $\widetilde{T}_\ell$ ($\ell \neq p$).*

Example 6. *Minimal conductor:* $5203 = 11^2.43$ *(Example 16 in [Bas-Ki]).*

P	sgn(K)	d_K	ram. in K	d	$\mathfrak{F}(\rho)$	Cl(F'')	ram. in F''
(0,0,5,−6,27)	(1,2)	$11^2.43^2$	$11=1^3 2^1$ $43=1^2 1^2 1^1$	-43	$11^2.43$	1	$43=2^2 2^2 2^1 2^1$

Let $\overline{\rho}$ be one of the two projective representations associated to the splitting field M of P. This representation has a lifting ρ_0 with odd quadratic character χ_{-43}, and unramified outside $\{11,43\}$. The conductor $\mathfrak{F}(\rho_0)$ of such a representation is equal to $5203 = 11^2.43$. Moreover, the only liftings of $\overline{\rho}$ of determinant χ_{-43} and conductor 5203 are ρ_0, $\rho_0 \otimes \chi_{-43}$, $\rho_0 \otimes \chi_{-11}$ and $\rho_0 \otimes \chi_{43.11}$. In $\{\rho_0, \rho_0 \otimes \chi_{-11}\}$, there is a unique representation ρ such that $\rho(I_{11})$ has cardinal 3. The 2-liftings of $\overline{\rho}$ with minimal ramification are ρ and $\rho \otimes \chi_{-43}$. These representations are conjugated by complex conjugation.

We will give in proposition 5.2.6 the field $\overline{\mathbb{Q}}^{\mathrm{Ker}(\rho)}$ as the splitting field of a polynomial of degree 24 by using Serre's conjecture on modular forms, as it is explained below.

Conjecture 5.2.1 says that representation ρ corresponds with an eigenform in $S_{41}(43,\chi_{-43})$. By theorem 5.2.2, we restrict ourselves to the space $S_5(43,\chi_{-43})$. We note that $\mathrm{Tr}(\rho)$ takes values in the field $\mathbb{Q}(\sqrt{5},i)$, hence $\mathrm{Tr}(\widetilde{\rho})$ takes values in $\mathbb{F}_{11^2}$. We now have to compute a basis of $S_5(43,\chi_{-43})$ and to find the eigenforms corresponding to the eigenvalues with reduction in $\mathbb{F}_{11^2}$. Using [C-Œ], theorem 1 page 71, we find that dim $S_5(43,\chi_{-43}) = 13$. On a table containing the cusps forms of this space (found in [C-S-Z]), we saw that there is in $S_5(43,\chi_{-43})$ one eigenform with rational eigenvalues. This eigenform has no interest for us, since we are looking for an eigenform with eigenvalues in $\mathbb{F}_{11^2}$ (and that has necessarily some eigenvalues in $\mathbb{F}_{11^2} \smallsetminus \mathbb{F}_{11}$). To compute the other eigenforms, there are different classic ways. We propose a construction (that had been suggested to the author by N. Skoruppa). This construction uses the functions described below.

Let Q be the quadratic form $Q(x,y) = x^2 + xy + 11y^2$; it is known that the associated series

$$\Theta_Q = \sum_{(x,y)\in\mathbb{Z}^2} q^{Q(x,y)} = 1 + 2\sum_{n=1}^{\infty}\left(\sum_{d|n}\chi_{-43}(d)\right)q^n$$

belongs to $M_1(43,\chi_{-43})$. We recall the classic notations $\sigma_1(n) = \sum_{d|n} d$ (for $n \in \mathbb{N}$) and $E_2 = 1 - 24\sum_{n=1}^{\infty}\sigma_1(n)q^n$. We define moreover the function $E(z) = E_2(z) - 43E_2(43z) \in M_2(43)$ (with always $q = e^{2i\pi z}$).

Lemma 5.2.3. *The function* $F = 2\theta(\Theta_Q)E - \Theta_Q\theta(E)$ *belongs to* $S_5(43, \chi_{-43})$.

Proof. Let
$$A = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$$
such that $c \equiv 0 \bmod 43$. Then $\Theta_Q(Az) = \chi_{-43}(d)(cz+d)\Theta_Q(z)$ and $E(Az) = \chi_{-43}(d)(cz+d)^2\Theta_Q(z)$. By derivation, we find
$$\Theta'_Q(Az) = \chi_{-43}(d)((cz+d)^3\Theta'_Q(z) + c(cz+d)^2\Theta_Q(z))$$
and
$$E'(Az) = \chi_{-43}(d)((cz+d)^4E'(z) + 2c(cz+d)^3E(z)).$$
Then we have $F(Az) = \chi_{-43}(d)(cz+d)^5F(z)$. Moreover, it is clear that F vanishes at cusps. $\square$

Let $\mathcal{S}$ be the set consisting in the cusp form F with its images by the Hecke operators T_ℓ, where $\ell \in \{2,3,5,7,11,13,17,19,23,29,31\}$, and let $\mathcal{V}$ be the subspace generated by $\mathcal{S}$ in $S_5(43, \chi_{-43})$. We check that $\mathcal{S}$ is a linearly independant family of $S_5(43, \chi_{-43})$ and that $\mathcal{V}$ is invariant under T_2. We can now compute the characteristic polynomial P_2 of the restriction of T_2 to $\mathcal{V}$:
$$X^{12} + 142X^{10} + 7173X^8 + 157368X^6 + 1510016X^4 + 5098688X^2 + 90352.$$
This polynomial is irreducible on $\mathbb{Z}$ but its reduction in $\mathbb{F}_{11}$ factorises in four factors: $X^4+3X^3+2X^2+3X+5$, $X^4+8X^3+2X^2+8X+5$, X^2+1 and X^2+3. In the $\mathbb{F}_{11}$-vector space generated by the reductions modulo 11 of the elements of $\mathcal{S}$, we have now to compute $\mathrm{Ker}(\widetilde{T}_2^2 + 3\mathrm{Id})$ and $\mathrm{Ker}(\widetilde{T}_2^2 + \mathrm{Id})$. If $\sum b_n q^n$ (resp. $\sum b'_n q^n$) is an eigenform in $(\widetilde{T}_2^2 + 3\mathrm{Id})$ (resp. $\mathrm{Ker}(\widetilde{T}_2^2 + \mathrm{Id})$), then we find the same values for $l^3 b_l$ and $l^3 b'_l$, for all prime number $l \notin \{11, 43\}$ lower than 1000. In $\mathrm{Ker}(\widetilde{T}_2^2 + 3\mathrm{Id})$, The eigenforms are $f_1 \pm 5\tilde{\iota} f_2$, where f_1 and f_2 are the reduction modulo 11 of the modular forms in $\mathcal{V}$ with respective coordinates in $\mathcal{S}$: $(1,9,0,9,0,10,9,0,0,6,10,7)$ and $(2,4,0,4,0,9,7,0,0,1,2,3)$. We write below the first coefficients of f_1 and f_2.
$$f_1 = q + 2q^4 + q^6 + q^{10} + 6q^{11} + 6q^{13} + 10q^{14} + \cdots$$
$$f_2 = q^2 + 7q^3 + 7q^5 + 4q^7 + 7q^8 + 3q^{12} + 3q^{20} + \cdots$$

We find the few first coefficients of a normalized eigenform $\sum b_n q^n$ (in our computation, we got one thousand coefficients). The table 5.2.4 below gives the reduction in $\mathbb{F}_{11}$ of the b_ℓ until $\ell = 29$. This table also gives the coefficients $\ell^3 b_\ell$ (where $\ell \neq 11$) of $\theta^3(g)$ and conjecturally the complex numbers $\mathrm{Tr}(\mathrm{Frob}_{\ell,\rho})$, obtained by lifting in $\mathbb{Q}(\sqrt{5}, i)$ of the previous elements. We observe that we obtain two eigenforms $f_1 + 5\tilde{\iota} f_2$ and $f_1 - 5\tilde{\iota} f_2$. These eigenforms correspond (conjecturally) to ρ and $\rho \otimes \chi_{-43}$.

ℓ	2	3	5	7	13	17	19	23	29
$\widetilde{b_\ell}$	$5\widetilde{\imath}$	$2\widetilde{\imath}$	$2\widetilde{\imath}$	$9\widetilde{\imath}$	6	8	0	7	0
$\widetilde{\ell^3 b_\ell}$	$-4\widetilde{\imath}$	$-\widetilde{\imath}$	$8\widetilde{\imath}$	$-4\widetilde{\imath}$	4	1	0	-4	0
$\mathrm{Tr}(\mathrm{Frob}_{\ell,\rho})$	$i\frac{-1+\sqrt{5}}{2}$	$-i$	$i\frac{1+\sqrt{5}}{2}$	$i\frac{-1+\sqrt{5}}{2}$	$\frac{1-\sqrt{5}}{2}$	1	0	$\frac{-1+\sqrt{5}}{2}$	0

Table 5.2.4.

One can find other such computations in [S2] of course, and in [Lar] (resp. [D]) for some Galois representations corresponding to elliptic curves (resp. corresponding to $\widetilde{S}_4$-extensions).

By this method, we compute for prime numbers $\ell \notin \{11, 43\}$ lower than 1000 the conjectural complex numbers $\mathrm{Tr}(\mathrm{Frob}_{\ell,\rho})$. We give these numbers in the table 5.2.5. For all prime numbers ℓ, we denote by $\widehat{\pi}_\ell$ a representative of the conjugacy class in $\widehat{A}_5$ of the Frobenius element corresponding to ℓ.

ℓ	$\widehat{\pi}_\ell$	a_ℓ
	1	2
	α	$2i$
	ω	-2
	$\alpha\omega$	$-2i$
19,29,41,101,181,191,193,211,223,251,263, 271,311,397,431,433,439,467,479,487,557,569,593, 617,619,643,653,673,691,701,709,757,823,839,863	$\widetilde{(12)(34)}$ or $\alpha\widetilde{(12)(34)}$	0
31,59,103,269,307,317,509,541,769,787,809,821,827,877,907	$\widetilde{(123)}$	-1
3,37,131,277,313,373,419,449,491,571,577,587,607,677,727,811,829	$\alpha\widetilde{(123)}$	$-i$
17,47,67,109,167,173,229,239,283,337,659,797,883	$\omega\widetilde{(123)}$	1
61,71,89,163,241,463,499,503,521,601,631,641,733,761,953	$\alpha\omega\widetilde{(123)}$	i
23,139,353,359,367,401,443,563,919,967,977	$\widetilde{(12345)}$	$\frac{-1+\sqrt{5}}{2}$
2,7,113,199,389,409,457,887	$\alpha\widetilde{(12345)}$	$i\frac{-1+\sqrt{5}}{2}$
13,127,379,461,719,857	$\omega\widetilde{(12345)}$	$\frac{1-\sqrt{5}}{2}$
137,179,257,331,383,739,911,937,997	$\alpha\omega\widetilde{(12345)}$	$i\frac{1-\sqrt{5}}{2}$
79,83,97,107,547,661,853,947,971	$\widetilde{(12354)}$	$\frac{-1-\sqrt{5}}{2}$
73,149,157,227,233,347,349,523,751,983,991	$\alpha\widetilde{(12354)}$	$i\frac{-1-\sqrt{5}}{2}$
53,197,281,293,599,613,683,881,941	$\omega\widetilde{(12354)}$	$\frac{1+\sqrt{5}}{2}$
5,151,421,647,743,773,859,929	$\alpha\omega\widetilde{(12354)}$	$i\frac{1+\sqrt{5}}{2}$

Table 5.2.5.

We have now more informations about ρ than we need to get a polynomial for the field $\overline{\mathbb{Q}}^{\mathrm{Ker}(\rho)}$.

Proposition 5.2.6. (A polynomial for example 6) *Let ρ be a 2-lifting of $\overline{\rho}$ with minimal ramification (then the other one is $\rho \otimes \chi_{-43}$). The conductor $\mathfrak{F}(\rho) = 43.11^2$ is minimal and its determinant is χ_{-43}. Moreover, the field*

$\overline{\mathbb{Q}}^{\mathrm{Ker}(\rho)} = \overline{\mathbb{Q}}^{\mathrm{Ker}(\rho\otimes\chi_{-43})}$ *is the splitting field of the polynomial*

$$X^{24} + 24X^{22} + 59952X^{20} - 496386X^{18} + 1882872X^{16} - 3827348X^{14} \\ +4261919X^{12} - 2093369X^{10} + 312688X^{8} + 170324X^{6} - 66944X^{4} \\ -3225X^{2} + 1849.$$

Proof. Let $\mathfrak{p}$ be an unramified ideal of $\mathcal{O}_{F''}$ dividing 43. By local consideration, we see that we can choose S such that the extension S/F'' is ramified at $\mathfrak{p}$ and unramified outside. As in example 1, we use ramification conditions to get a set $\mathcal{E}'$ containing γ. This set has 96 elements. To find the right γ, we use the table 5.2.4. We see that in the field S, the prime ideals dividing 31, 59 and 103 have (conjecturally) a residual index equal to 3. Using the factorisation modulo these prime numbers of the minimal polynomials of all the $\sqrt{\gamma}$ ($\gamma \in \mathcal{E}$), we find one, and only one γ which agrees with Serre's conjecture on modular forms. We prove that the Galois closure of the field $F''(\sqrt{\gamma})$ has a Galois group isomorphic to $\widehat{A}_5$ by using theorem 4.3.1. The polynomial of proposition 5.2.6 is the minimal polynomial of γ. $\square$

Example 7. *Minimal conductor:* $7047 = 3^5.29$ *(example 46 in [Bas-Ki]).*

P	sgn(K)	d_K	ram. in K	d	$\mathfrak{F}(\rho)$	Cl(F'')	ram. in F''
(0,0,39,−108,81)	(1,2)	$3^6.29^2$	$3=1^21^3$ $29=1^21^21^1$	-3.29	$3^5.29$	1	$3=2^32^3$ $29=2^22^22^12^1$

Projective representation $\overline{\rho}$ has four liftings with quadratic determinant $\chi_{-3.29}$, with minimal ramification and conductor $3^5.29$. Let ρ be one of these liftings, the other ones are $\rho\otimes\chi_{-3.29}$, $\rho\otimes\chi_{29}$ and $\rho\otimes\chi_{-3}$.

Remark 5.2.7. Let ϕ_{29} be a cyclotomic character of conductor 29. The representation $\rho\otimes\phi_{29}^7$ is a lifting of $\overline{\rho}$ with determinant quadratic χ_{-3} and with conductor $3^5.29^2$.

Proposition 5.2.8. (A polynomial for example 7) *The projective representation $\overline{\rho}$ has four 2-liftings ρ with minimal ramification and conductor* 7047. *This conductor is minimal and their determinant is $\chi_{-3.29}$. We can choose ρ such that $\overline{\mathbb{Q}}^{Ker(\rho)}$ is the splitting field of the polynomial*

$$X^{24} - 30X^{22} + 243X^{20} + 1526X^{18} - 40059X^{16} + 140280X^{14} \\ -220630X^{12} + 153126X^{10} + 17046X^{8} - 72420X^{6} + 10368X^{4} \\ +34452X^{2} + 7569.$$

Proof. Consider the following decompositions $3\mathcal{O}_{F''} = \mathfrak{p}_2^3\mathfrak{p}_2'^3$ and $29\mathcal{O}_{F''} = \mathfrak{P}_2\mathfrak{P}_2'\mathfrak{P}_2''^2\mathfrak{P}_2'''^2$. Let π_3, π_3', π_{29} and π_{29}' be respective generators of $\mathfrak{p}_2$, $\mathfrak{p}_2'$, $\mathfrak{P}_2$ and $\mathfrak{P}_2'$. By local considerations, we see that ρ and $\rho\otimes\chi_{-3.29}$ are given by $F''(\sqrt{\varepsilon_1\pi_3\pi_{29}})$ (or by the arithmetically equivalent field $F''(\sqrt{-3.29\varepsilon_1\pi_3\pi_{29}})$, equal to $F''(\sqrt{\varepsilon_2\pi_3'\pi_{29}'})$), and that $\rho\otimes\chi_{29}$ and $\rho\otimes\chi_{-3}$ are given by a field $F''(\sqrt{\varepsilon_3\pi_3\pi_{29}'})$ (or $F''(\sqrt{\varepsilon_4\pi_3'\pi_{29}})$), where the ε_i are units of F''.

We reduce the representation ρ modulo 3. We have to look for an eigenform in $\widetilde{S}_4(29,\chi_{29})$. The dimension of the complex vector space $S_4(29,\chi_{-29})$

is equal to 6. We found in [C-S-Z] a table with the eigenforms of $S_4(29,\chi_{-29})$. The corresponding eigenvalues are in the splitting field of the minimal polynomial of $\widetilde{T}_2$. This polynomial is $X^6+38X^4+301X^2+560$. Its reduction modulo 3 is $(X-1)(X+1)(X^2+X-1)(X^2-X-1)$. We have to deal with the eigenforms of V_1 =Ker$(\widetilde{T}_2^2+\widetilde{T}_2-\mathrm{Id})$ and V_2 =Ker$(\widetilde{T}_2^2-\widetilde{T}_2-\mathrm{Id})$. We choose for example an eigenform in V_2. Here, we have not a one to one correspondance between the values of the character ψ (described in the table 3.1) and their reduction in $\mathbb{F}_9$, but we have such a correspondance between the values of ψ on $\{\widetilde{(123)},\omega\widetilde{(123)},\alpha\widetilde{(123)},\alpha^3\widetilde{(123)}\}$ and their reductions in $\mathbb{F}_9$. It gives us the decomposition of enough prime numbers to eliminate one of the two possibilities for the field S (say $F''(\sqrt{\varepsilon_3\pi_3\pi'_{29}})$), and to select the right element γ of the shape $\varepsilon_1\pi_3\pi_{29}$. Then we prove the proposition by using theorem 4.3.1. Note that if we choose an eigenform in V_1, we find a field S of the shape $F''(\sqrt{\varepsilon_3\pi_3\pi'_{29}})$. $\square$

Remark 5.2.9. In example 6, we used a specific computation to get a basis of space $S_5(43,\chi_{-43})$. Moreover, in example 7, we used a table of [C-S-Z] to get $S_4(29,\chi_{-29})$. In fact, there is an algorithm for such computations: let's choose $p=3$. Then we have to compute an eigenform $\sum a_n q^n$ in a space of cusp forms with a small weight ($k\le 5$). Decomposition of prime numbers in quintic field K gives so many primes numbers ℓ we want such that $a_\ell\equiv 0$ mod 3. Then M. Müller has an algorithm to compute an eigenform satisfying such properties. His algorithm uses the modular symbol method for higher weight (see [M] or [W]).

5.3. **Buhler's example.** This subsection deals with the example of [B] and uses the computation of the L-function described in this book.

Example 8. *Minimal conductor:* $800=2^5.5^2$ *(example of [B]).*

P	sgn(K)	d_K	ram. in K	d	$\mathfrak{F}(\rho)$	Cl(F'')	ram. in F''
(0,10,−10,35,−18)	(1,2)	$2^6.5^8$	$2{=}1^41^1$ $5{=}1^5$	-1	$2^5.5^4$	1	$2{=}3^4$

The projective representation $\overline{\rho}$ has a lifting ρ of conductor $20000=2^5.5^4$, and determinant χ_{-1} ([B] p. 62). Up to multiplication by χ_5, we obtain ρ such that $|\rho(I_5)|=5$. We can choose the cyclotomic character ϕ_{25} such that the restriction of ρ on the inertia group I_5 is conjugated to

$$\begin{pmatrix}\phi_{25}^4 & 0\\ 0 & \phi_{25}^{16}\end{pmatrix}.$$

The conductor $\mathfrak{F}(\rho\otimes\phi_{25}^4)=2^5.5^2$ is then minimal.

Proposition 5.3.1. (A polynomial for example 8) *The field* $\overline{\mathbb{Q}}^{\mathrm{Ker}(\rho)}$ *is the splitting field of the polynomial*

$$X^{24}+334X^{20}+5600X^{18}-19935X^{16}+1336320X^{14}-124170X^{12}$$
$$-425920X^{10}-148310X^8-16800X^6-1396X^4+1.$$

We can choose ϕ_{25} such that the representation $\rho \otimes \phi_{25}^4$ is a lifting of $\overline{\rho}$ with minimal conductor.

Proof. The table 4.4 of [B] (p. 68) gives the decomposition for all prime numbers less than 331. The extension S/F'' is unramified outside the only place $\mathfrak{p}$ of F'' above 2. Since $\mathrm{Cl}(F'') = \{1\}$, we can choose γ as an unit or as a generator of $\mathfrak{p}$. Using the coefficients of the L-function given in [B], we found γ by the same way than in the previous examples. For this example, it is not necessary to use the theorem 4.3.1, because here, the coefficients of the L-function are not conjectural. □

6. Computation of the L-function

One can use the computation of the elements γ described in the previous section to get the first coefficients of the L-functions $L(\rho, s) = \sum_{n \geq 1} a_n n^{-s}$. In this section, we use the fields described in the diagrams 4.1.1 and 4.2.1.

Let ℓ be a prime number where ρ is unramified. Let $\widetilde{\pi}_\ell$ (resp. $\widehat{\pi}_\ell$) be an element of the conjugacy class of the Frobenius element of ℓ if $\mathrm{Gal}(M'/\mathbb{Q})$ is isomorphic to $\widetilde{A}_5$ (resp. $\widehat{A}_5$) which is mapped to the conjugacy class of $\pi_\ell \in A_5$. Then the following table holds.

	$\ell\mathcal{O}_K$	π_l	$\lvert a_\ell \rvert$	$\widetilde{\pi}_\ell$	$\widehat{\pi}_\ell$
1	$\prod_{k=1}^5 1^1$	1	2	$1, \omega$	$1, \omega, \alpha, \alpha^3$
2	$1^1 2^1 2^1$	(12)(34)	0	$\widetilde{(12)(34)}$	$\widetilde{(12)(34)}, \alpha\widetilde{(12)(34)}$
3	$1^1 1^1 3^1$	(123)	1	$\widetilde{(123)}, \omega\widetilde{(123)}$	$\widetilde{(123)}, \omega\widetilde{(123)}, \alpha\widetilde{(123)}, \alpha^3\widetilde{(123)}$
4	5^1	(12345)	$\frac{-1+\sqrt{5}}{2}$	$\widetilde{(12345)}, \omega\widetilde{(12345)}$	$\widetilde{(12345)}, \omega\widetilde{(12345)}, \alpha\widetilde{(12345)}, \alpha^3\widetilde{(12345)}$
5	5^1	(12354)	$\frac{1+\sqrt{5}}{2}$	$\widetilde{(12354)}, \omega\widetilde{(12354)}$	$\widetilde{(12354)}, \omega\widetilde{(12354)}, \alpha\widetilde{(12354)}, \alpha^3\widetilde{(12354)}$

Table 6.1.

In this table, the second column gives the decomposition of the prime number ℓ in the quintic field K and the third one gives the modulus $|a_\ell|$ of the complex coefficient a_ℓ. In fact, a_ℓ is determined by π_ℓ up to multiplication by a fourth root of the unit. This element π_ℓ is given by the decomposition of ℓ in K, except in cases 4 and 5. To distinguish between these cases, we use the following idea due to Serre ([B] p. 53). Let f be a quintic polynomial whose root field is K. Then in these cases 4 and 5, this polynomial is irreducible in $\mathbb{Q}_\ell$. Let D^2 and y be respectively the discriminant and a root of f in the unramified extension of degree 5 of $\mathbb{Q}_\ell$. Then

$$\prod_{0 \leq j < k \leq 4} (\pi_l^j(y) - \pi_l^k(y)) = \pm D \text{ in } \mathbb{Q}_\ell$$

and the sign of this expression distinguishes between the two conjugation classes of 5-cycles.

We have to decide which element $\widetilde{\pi}_\ell$ (resp. $\widehat{\pi}_\ell$) occurs in cases 1, 3, 4 and 5. For $\widetilde{A}_5$-extensions, this conjugation class is determined by the order of $\widetilde{\pi}_l$, hence by the decomposition of ℓ in S. For $\widehat{A}_5$-extension, this criterion can not be used when the order of $\widehat{\pi}_\ell$ is 4, 12 or 20. In these cases, we have to distinguish between $\alpha\tau$ and $\alpha^3\tau$, where $\tau \in \widehat{A}_5$ has order 1 (resp. 3, 5).

Let γ be an element of F'' such that $S = F''(\sqrt{\gamma})$. We have: $\gamma^{\frac{\alpha^3}{2}} = -\gamma^{\frac{\alpha}{2}}$. We distinguish between α and α^3 by choosing $\gamma^{\frac{\alpha}{2}}$.

Proposition 6.2. (Case 1) *We suppose that $\pi_\ell = 1$, and that the order of $\widehat{\pi}_l$ is 4. Let $\mathfrak{l}_1$ a prime ideal of $\mathcal{O}_F$ dividing ℓ and $\mathfrak{L}_4$ aprime ideal of $\mathcal{O}_S$ dividing $\mathfrak{l}_1$ (where the index is the residual index). Since the valuation $v_{\mathfrak{L}_4}(\gamma)$ is even, we may suppose after multiplication by a square of K that $\gamma \notin \mathfrak{L}_4$. We have then, in case 1 of table 6.1:*

- $a_\ell = 2i$ *if and only if* $N_{S/F}(\gamma^{\frac{\ell}{2}} - \gamma^{\frac{\alpha}{2}}) \in \mathfrak{l}_1$.
- $a_\ell = -2i$ *if and only if* $N_{S/F}(\gamma^{\frac{\ell}{2}} + \gamma^{\frac{\alpha}{2}}) \in \mathfrak{l}_1$.

Proof. The element a_ℓ is the trace of $\mathrm{Frob}_{\ell,\rho}$. Since has order 4 and a trivial projective image, we have

$$\mathrm{Frob}_{\ell,\rho} = \pm \begin{pmatrix} i & 0 \\ 0 & i \end{pmatrix}$$

and $a_\ell = \pm i$. We choose to put $a_\ell = i$ if $\widehat{\pi} = \alpha$ and $a_\ell = -i$ if $\widehat{\pi} = \alpha^3$. Since $\gamma^{\frac{\widehat{\pi}}{2}} \equiv \gamma^{\frac{\ell}{2}} \bmod \mathfrak{L}_4$, we have $a_\ell = 2i$ if and only if $\gamma^{\frac{\ell}{2}} - \gamma^{\frac{\alpha}{2}} \in \mathfrak{L}_4$ and $a_\ell = -2i$ if and only if $\gamma^{\frac{\ell}{2}} + \gamma^{\frac{\alpha}{2}} \in \mathfrak{L}_4$. $\square$

Proposition 6.3. (Cases 4 and 5) *The order of $\widehat{\pi}_\ell$ is 20 if and only if $\ell\mathcal{O}_S = \mathfrak{L}_4\mathfrak{L}'_{20}$. In this case, $\ell\mathcal{O}_F = \mathfrak{l}_1\mathfrak{l}'_5$. Since the valuation $v_{\mathfrak{L}_4}(\gamma)$ is even, we may suppose after multiplication by a square of K that $\gamma \notin \mathfrak{L}_4$. We then have, in case 4 (resp, 5) of table 6.1:*

- $a_\ell = i\frac{-1+\sqrt{5}}{2}$ *(resp.* $i\frac{-1-\sqrt{5}}{2}$*) if and only if* $N_{S/F}(\gamma^{\frac{\ell}{2}} - \gamma^{\frac{\alpha}{2}}) \in \mathfrak{l}_1$.
- $a_\ell = -i\frac{-1+\sqrt{5}}{2}$ *(resp.* $i\frac{1+\sqrt{5}}{2}$*) if and only if* $N_{S/F}(\gamma^{\frac{\ell}{2}} + \gamma^{\frac{\alpha}{2}}) \in \mathfrak{l}_1$.

In order to decide whether $\widehat{\pi}_\ell$ is in the class of $\alpha\widetilde{(123)}$ or $\alpha^3\widetilde{(123)}$, that is whether $a_\ell = \pm i$ when the order of $\widehat{\pi}_\ell$ is 12, we consider $\delta = \gamma_1\gamma'_5\gamma'_6$, with notations of theorem 4.3.1. This element is in the field T of degree 10 fixed by the group $< \widetilde{(123)}, \omega\widetilde{(12)(45)} >$.

Proposition 6.4. (Case 3) *The order of $\widehat{\pi}_\ell$ is 12 if and only if $\ell\mathcal{O}_T = \mathfrak{L}_4\mathfrak{L}'_{12}\mathfrak{L}''_{12}\mathfrak{L}'''_{12}$. In this case, $\ell\mathcal{O}_J = \mathfrak{l}_1\mathfrak{l}'_3\mathfrak{l}''_3\mathfrak{l}'''_3$. Since the valuation $v_{\mathfrak{L}_4}$ is even, we may suppose after multiplication by a square of J that $\delta \notin \mathfrak{L}_4$. We have then:*

- $a_\ell = -i$ *if and only if* $N_{T/J}(\delta^{\frac{\ell}{2}} - \delta^{\frac{\alpha}{2}}) \in \mathfrak{l}_1$.
- $a_\ell = i$ *if and only if* $N_{T/J}(\delta^{\frac{\ell}{2}} + \delta^{\frac{\alpha}{2}}) \in \mathfrak{l}_1$.

Remark 6.5. For $\ell = 2$, we have the same result if we take another primitive element x of S (resp. T) instead of $\sqrt{\gamma}$ (resp. $\sqrt{\delta}$). Such an element has to be chosen such that its reduction modulo the ideal $\mathfrak{L}_4$ of proposition 6.2 or 6.3 (resp. 6.4) spans $\mathbb{F}_8$. We can find such an element by using function "polred" of [PARI].

To complete the study, we have to give a_ℓ for a ramified prime ℓ. If ℓ is such a prime, then $a_\ell \neq 0$ if and only if $\overline{\rho}(I_\ell)$ has order 2 (and then if $\ell\mathcal{O}_F = \mathfrak{l}_1\mathfrak{l}'_1\mathfrak{l}''^2_1\mathfrak{l}'''^2_1$), because if not, the subspace invariant by I_ℓ is $\{0\}$. In this case, $a_\ell = 1$, -1, i or $-i$. The decomposition of p in S gives a_ℓ, except if $\ell\mathcal{O}_S = \mathfrak{L}_4\mathfrak{L}'^2_2\mathfrak{L}''^2_2\mathfrak{L}'''^2_2$. If ℓ has such a decomposition (it only occurs if $\mathrm{Gal}(M'Q)$ is isomorphic to $\widehat{A}_5$), then $a_\ell = i$ or $-i$.

Proposition 6.6. *Suppose that the decompositions of ℓ in F and S are given by $\ell\mathcal{O}_F = \mathfrak{l}_1\mathfrak{l}'_1\mathfrak{l}''^2_1\mathfrak{l}'''^2_1$ and $\ell\mathcal{O}_S = \mathfrak{L}_4\mathfrak{L}'^2_2\mathfrak{L}''^2_4\mathfrak{L}'''^2_4$, where $\mathfrak{L}_4$ divides $\mathfrak{l}_1$. Then:*

- *$a_\ell = i$ if and only if $N_{S/F}(\gamma^{\frac{\ell}{2}} - \gamma^{\frac{\alpha}{2}}) \in \mathfrak{l}_1$.*
- *$a_\ell = -i$ if and only if $N_{S/F}(\gamma^{\frac{\ell}{2}} + \gamma^{\frac{\alpha}{2}}) \in \mathfrak{l}_1$.*

For example 6, we found the coefficients given in table 5.2.5, for the unramified primes. For ramified primes, we found $a_{11} = 0$ and $a_{43} = i$.

Bibliography

[Bac-Kw] . Bachoc and S.-H. Kwon, *Sur les extensions de groupe de Galois $\widetilde{A}_4$*, Acta Arith. 62 (1992), 1–10.

[Bas-Ki] J. Basmaji and I. Kiming, *A table of A_5-fields*, in [F2], 37–46.

[B] J. Buhler, *Icosahedral Galois representations*, Lecture note in math. **654** (1978), Springer–Verlag.

[B-D-SB-T] K. Buzzard, M. Dickinson, N. Shepherd-Barron and R. Taylor *On icosahedral Artin representations*, Preprint.

[B-T] K. Buzzard and R. Taylor *Companion forms and weight one forms*, Annals of Math, 149 (1999), p. 905–919.

[CN–J] Ph. Cassou-Noguès et A. Jehanne, *Formes primitives et représentations galoisiennes de type octaédral,* Exp. Math., 5.4 (1996), p. 275–290.

[C-D-O] H. Cohen, F. Diaz y Diaz and M. Olivier, *Tables of octic fields with a quartic subfield*, preprint.

[C-O] H. Cohen et J. Oesterlé, *Dimensions des espaces de formes modulaires*, in *Modular functions of one variable VI*, edited by J.-P. Serre and D.B. Zagier, Lecture note in math. **627** (1976), Springer–Verlag, p. 69–78.

[C-S-Z] H. Cohen, N. Skoruppa and D.B. Zagier, *Bases of modular forms*, temporary version.

[C1] T. Crespo *Explicit construction of $\widetilde{A}_n$-type fields* J. of Algebra, 127 (1989), p. 452–461.

[C2] T. Crespo *Extensions de $\widetilde{A}_n$ par C_4 comme groupes de Galois*, CRAS, t. 315, Série I, (1992), p. 625–628.

[D-S] P. Deligne et J.-P. Serre, *Formes modulaires de poids* 1, Ann. scient. Éc. Norm. Sup., 4e série t. 7 (1974), p. 507–530.

[D] D. Doud, *S_4 and $\widetilde{S}_4$-extensions of $\mathbb{Q}$ ramified at only one prime*, J. of Number Theory, Vol 75 N° 2 (1999), p. 185–197.

[E] S. Edixhoven, *The weight in Serre's conjecture on modular forms*, Invent. math. 109 (1992), p. 563–594.

[F1] G. Frey *Construction and arithmetical applications of modular forms of low weight* CRM Proceeding and Lecture Notes 4 (1994), p. 1–21.

[F2] G. Frey, *On Artin's conjecture for odd 2-dimensional representations*, Lecture note in math. **1585** (1994), Springer–Verlag.

[G] F. Gassmann, *Bemerkungen zur Vorstehenden Arbeit von Hurwitz*, Math. Z. 25 (1926), p. 665–675.

[H-K] F.-P. Heider and P. Kolvenbach, *The construction of $SL(2,3)$-polynomials*, J. Number Theory, 19 (1984), p. 392–411.

[J-M] A. Jehanne and M. Müller *Modularity of an odd icosahedral representation*, to appear in J. Théorie des nombres de Bordeaux.

[K] I. Kiming, *On the experimental verification of the Artin conjecture for 2-dimensional odd Galois representations over $\mathbb{Q}$. Lifting of 2-dimensional projective Galois representations over $\mathbb{Q}$*, in [F2], p. 1–36.

[Lan] R.-P. Langlands *Base change for $GL(2)$* Annals of Math. Studies 96 (1980), Princeton Univ. Press, Princeton.

[Lar] J.-C Lario, *Representacions de Galois i corbes el.líptiques*, Memòria, Universitat de Barcelona (1991).

[M] L. Merel *Universal Fourier expansions of modular forms*, in [F2], p. 59–94.

[PARI] C. Batut, K. Belabas, D. Bernardi, H. Cohen and M. Olivier, computation system.

[S1] J.-P. Serre, *Modular forms of weight one and Galois representations*, in *Algebraic number fields*, Academic Press (London), edited by A. Fröhlich (1977), p. 193–268.

[S2] J.-P. Serre, *Sur les représentations modulaires de degré 2 de $Gal(\overline{\mathbb{Q}}/\mathbb{Q})$*, Duke Math, Journal (1987), Vol. 54, p. 179–230.

[SB-T] N. Shepherd-Barron and R. Taylor, *Mod 2 and mod 5 icosahedral representations* J. AMS (1997), Vol. 10, p. 283–298.

[Ta1] R. Taylor *Icosahedral Galois representations* Pacific Jour. of Math., Olga Taussky-Todd memorial issue (1997), p. 337–347.

[Ta2] R. Taylor *On icosahedral Artin representations II*, preprint.

[Tu] J. Tunnel *Artin's conjecture for representations of octahedral type* Bull. AMS (1981), Vol. 5, p. 173–175.

[W] X. Wang *The Hecke operators on the cusp forms of $\Gamma_0(N)$ with nebentype.* in [F2], p. 95–108.